Alcatel·Lucent Enterprise

Stellar AP

Deployment & Configuration & Troubleshooting Guide

January 2019

Table of Contents

1 Introduction

1.1 Revision History

Ed.	Date	Descripotion
1.0	Sep-2018	New creation for knowledge transfer with ALE team.
2.0	Jan-2019	Update Software Upgrading for AP1201 and useful CLI Commands New creation for log collection and AP reboot log collection method

1.2 Objective

The objective of this document is to give a brief introduction of Stellar series solution on the features, configurations and troubleshooting, in order to help and guide the TSS team to provide better service to the end customers.

1.3 Glossary

ACS	Auto Channel Selection
ALE	Alcatel-Lucent Enterprise
AP	Access Point
APC	Auto Power Control
BLE	Bluetooth Low Energy

CLI	Command Line Interface
DCM	Dynamic Client Management
DRM	Dynamic Radio Management
IG	Installation Guide
MIMO	Multiple-Input Multiple-Output
MU-MIMO	Multi-User Multiple-Input Multiple-Out
OVC	OmniVista Cirrus
OVE	OmniVista Enterprise
QSG	Quick Start Guide
WBM	Web Based Management
ZTP	Zero Touch Provision

2 Stellar Overview

2.1 Introduction

The high-performance OmniAccess Stellar Series featuring enhanced WLAN technology with RF Radio Dynamic Adjustment, a distributed control Wi-Fi architecture, secure network admission control with unified access, built in application intelligence and analytics, making it ideal for enterprises of all sizes demanding a simple, secure and scalable wireless solution.

Deliver enterprise-grade Wi-Fi to high-density client environments in offices, hospitals, schools, retail stores and warehouses. Achieve our highest speeds and best performance for your network services and applications. Ensure your users have network access anywhere on your campus.

Main features are:

- Seamless roaming and Quality of Service for real-time applications
- VoWLAN support with QoS for each application (Voice, Video, Collaboration, etc..)
- Integrated simple guest management
- Built-in customizable captive portal
- Support of role-based management access (Admin, Viewer and Guest Manager)
- Enhanced RF technology - Radio Dynamic Adjustment with DFS/TPC to deliver reliable, high-performance WLAN access
- OmniVista 2500 managed deployment embeds a visionary controllerless architecture, providing user-friendly workflows for unified access plus an integrated unified policy authentication manager

- Zero-touch provisioning (ZTP)

2.2 Product Matrix

Model	AP1101	AP1220 Series	AP1230	AP1251	AP1201H	AP1201
Product Class	Indoor (Low-end) 802.11ac	Indoor (Mid-end) 802.11ac Wave 2	Indoor (High-end) 802.11ac Wave 2	Outdoor 802.11ac Wave 2	Indoor Hospitality 802.11ac Wave 2	Indoor IoT 802.11ac Wave 2
Form Factor						
Radio	dual-radio, 802.11ac 2x2 MIMO,	dual radio, 5 GHz 802.11ac 4x4:4 MU-MIMO and 2.4 GHz 802.11n 2x2:2 MIMO	tri radio, dual 5 GHz 802.11ac 4x4:4 MU-MIMO and 2.4 GHz 802.11n 4x4:4 MIMO	dual radio, 5 GHz 802.11ac 2x2:2 MU-MIMO and 2.4 GHz 802.11n 2x2:2 MIMO	dual radio, 5 GHz 802.11ac 2x2:2 MU-MIMO, and 2.4 GHz 802.11n 2x2:2 MIMO	dual radio, 5 GHz 802.11ac 2x2:2 MU-MIMO and 2.4 GHz 802.11n 2x2:2 MIMO
Antennas	Built-in 2×2:2, 3.4 dBi @ 2.4 GHz, 2.55 dBi @ 5 GHz	AP1221: Built-in 2×2:2 @ 2.4 GHz, 4x4:4 @ 5 GHz AP1222 External 2×2:2 @ 2.4 GHz, 4x4:4 @ 5 GHz	AP1231: Built-in 4×4:4 @ 2.4 GHz, dual 4x4:4 @ 5 GHz AP1232: External 4×4:4 @ 2.4 GHz,	Built-in 2×2:2 @ 2.4GHz, 2x2:2 @ 5GHz	Built-in 2×2:2 @ 2.4 GHz, 2x2:2 @ 5 GHz	Built-in 2×2:2 @ 2.4 GHz, 2x2:2 @ 5 GHz , BLE antenna

Model	AP1101	AP1220 Series	AP1230	AP1251	AP1201H	AP1201
			dual 4x4:4 @ 5 GHz 8 RP-SMA connectors for external dual band antennas			
Network Interfaces	1× 10/100/1000 Mb/s full/half-duplex Ethernet (RJ-45)	1x 10/100/1000Base-T (RJ-45) 1x USB 2.0 (Type A)	1x 100/1000/2500Base-T(RJ-45) 1x 10/100/1000Base-T 1x BLE radio, integrated	2x 10/100/1000Base-T (RJ-45)	4x10/100/1000Base-T (RJ-45), include 1xPSE 1x USB 2.0 (Type A)	1x 10/100/1000Base-T 1x BLE radio, integrated
Other Interfaces	1x console port (RJ-45)	1x console port (RJ-45)	1x console port (RJ-45)	1x management console port (Micro-USB)	N/A	1x console port (RJ-45)
Power	10 W (802.3at PoE or DC)	<15.6 W (802.3at PoE or DC	27.6 W (PoE or DC)	<11.8W (802.3af PoE)	11W (802.3af PoE w/o PSE)	Supports direct DC power and Power over Ethernet (PoE)

2.3 Working Modes

Three working modes are supported by all Stellar APs:

- **Express mode** - Plug and Play: Secure Web managed (HTTPS) cluster deployment

  Stellar Series APs by default operates in a cluster architecture to provide simplified plug-and-play deployment. The access point cluster is an autonomous system that consists of a group of OmniAccess Stellar APs and a virtual controller, which is a selected access point, for cluster management. One AP cluster supports up to 64 APs. The access point cluster architecture ensures simplified and quick deployment. Once the first AP is configured using the configuration wizard, the remaining APs in the network will come up automatically with an updated configuration. This ensures the whole network is up and functional within a few minutes. Stellar Series APs also supports secure zero-touch provisioning with Alcatel- Lucent OXO Connect R2, a mechanism by which all access points in a cluster will obtain bootstrap data securely from an on premise OXO Connect.

- **OVC mode** - Cloud enabled with OmniVista Cirrus

  Stellar Series APs can be managed by Alcatel-Lucent OmniVista® Cirrus cloud platform. OmniVista® Cirrus powers a secure, resilient and scalable cloud-based network management platform. It offers hassle free network deployment and easy service rollout with advanced analytics for smarter decision making. Offers IT friendly Unified Access with secure authentication and policy enforcement for users and devices.

- **OVE mode** - OmniVista 2500 managed deployment

Stellar Series APs can be managed by Alcatel-Lucent OmniVista® 2500 on premise Network Management System. The access points are managed as one or more access point (AP) groups (a logical grouping of one or more access points). The OmniVista 2500 next generation management suite embeds a visionary controller-less architecture, providing user friendly workflows for unified access together with an integrated unified policy authenticati on manager (UPAM) which helps define authentication strategy and policy enforcement for employees, guest management and BYOD devices. Stellar Series APs has built-in DPI technology providing real-time Application Monitoring and enforcement. The network administrator can obtain a comprehensive view of applications running in the network and apply adequate control to optimize the performance of the network for business critical applications. OmniVista 2500 provides advanced options for RF management, WIDS/WIPS for intrusion detection and prevention, and a heat map for WLAN site planning.

3 Deployment

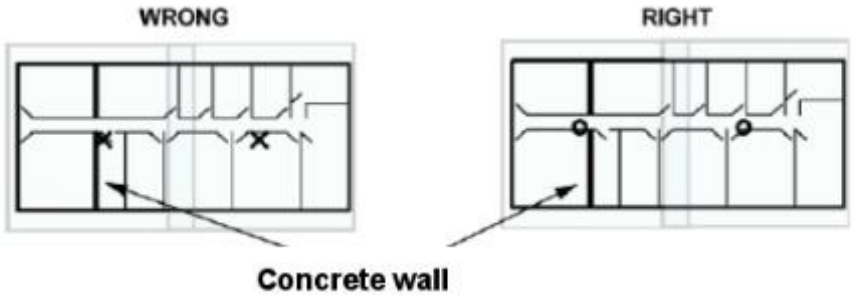
3.1 AP Placement & Guidelines

3.1.1 General Recommendations

- Position the APs above obstructions.
- Position the APs vertically near the ceiling in the center of each coverage area, if possible. APs are designed to be installed vertically, either standing up in a plenum or hanging from a ceiling, to create the largest coverage area per AP. Hanging the AP from the ceiling provides the best coverage.
- Position APs in locations where users are expected to be. For example, large rooms are typically a better location for APs than a hallway.
- Place APs no more than 40 meters apart from each other. Placing APs further apart almost always results in poor coverage.
- Do not mount APs outside buildings.
- Do not mount APs on building perimeter walls unless the operator wants to provide coverage outside the building.
- **Important**: Do not mount AP antennas within one meter (3 feet) of any metal obstructions. The radio frequency waves from the APs are blocked and/or reflected by metal objects, such as ducts, conduit, pipes, bookcases, elevator shafts, stairwells, and walls.

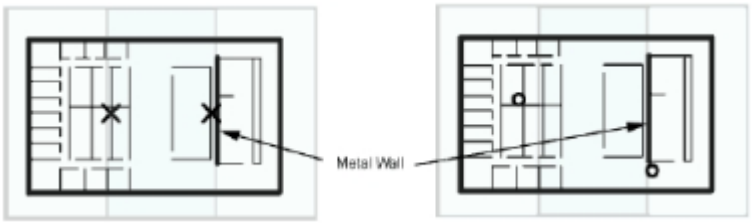
3.1.2 Three Sample Solutions to AP Placement Problems

In the first example, there is a large concrete wall in the middle of one coverage area.



The figure on the left shows a poor installation of two APs indicated with an X. The figure on the right shows a better solution. Both APs are mounted in hallways. The leftmost AP is moved to other side of wall to provide coverage on left side of the wall and the rightmost AP is moved slightly left to provide better coverage to overlap area.

In the second example, there is a large metal wall next to a planned location.



The figure on the left shows a poor installation of two APs indicated with an X. The figure on the right shows a better solution. The right most AP is moved to the hallway slightly to the right of one end of the metal wall. The left most AP is moved up and to the left to provide better coverage to overlap area.

In the third example, the AP needs to be mounted in a right angle corner of a hallway.

In the right angle corner of a hallway, mount the AP at a 45 degree angle to the two hallways as shown in the figure on the right. The Alcatel-Lucent AP internal antennas are not omnidirectional, and will cover a larger area if mounted this way.

3.1.3 Interferers

802.11b/g/n standards share the unlicensed Industrial, Scientific and Medical (ISM) band (2.4 GHz) with a number of other wireless technologies. Bluetooth devices and microwave ovens are the most common ones and can be found on a site where WLAN will be deployed. AP placement should be chosen in order to minimize interferences on the WLAN system' s performance. Interferences by WLAN on other technologies is not discussed, except cohabitation with DECT APs. For more information, see Cohabitation with DECT APs.

Cohabitation with Bluetooth Devices

Bluetooth technology is based on frequency hopping over 79 channels in the 2400 to 2483.5 MHz band.

There are 3 power classes

- Power class 1: max transmit power: +20 dBm (range 100 m)
    - Voice application: do not mount an Alcatel-Lucent AP within 10 meters of a power class 1 Bluetooth AP. The number of maximum simultaneous calls on WLAN AP can decrease significantly if a Bluetooth AP class 1 emits within 10 meters.
    - 802b/g/n data application: for maximum throughput, do not mount an Alcatel-Lucent AP within 10 meters of a power class 1 Bluetooth AP.

      802.11b/g/n data throughput is reduced when a user within 10 meters from a class 1 Bluetooth device in use. To ensure 80% of the maximum

data throughput, users should be at least 10 meters away from a Bluetooth class 1 device.

- Power class 2: maximum transmit power: +4 dBm (range 10m)
    - Voice application: do not mount an Alcatel-Lucent AP within 1 meter of a power class 2 Bluetooth AP. WLAN handset users can experience cuts in the audio when placed less than 1 meter from a Bluetooth class 2 device in use. Cuts are less than 1 second long and can appear in bursts. General audio quality is minimally impacted.
    - 802b/g Data application: for maximum throughput, do not mount an Alcatel-Lucent AP within 10 meters of a power class 2 Bluetooth AP.
    - 802.11b/g data throughput is reduced when a user is within 10 meters from a class 2 Bluetooth device in use. To ensure 80% of the maximum data throughput, users should be at least 3 meters away from a Bluetooth class 2 device.
- Power class 3: max transmit power: 0 dBm (range 10 cm)
    - Not tested, interferences should be minimal on WLAN.

Cohabitation with Microwave Ovens

Microwave ovens emit signals in the ISM band. Depending on how well the oven is shielded, emissions can disturb WLAN applications. To reduce interference from microwave ovens, check the label on the microwave which should provide the central operating frequency. Most microwave ovens operate at a central frequency of 2.45 GHz, Emissions occur in a large band, so typically disturb channels 6 to 11. In this case, an AP close to a microwave oven should be set to channel 1.

Cohabitation with other WLAN APs

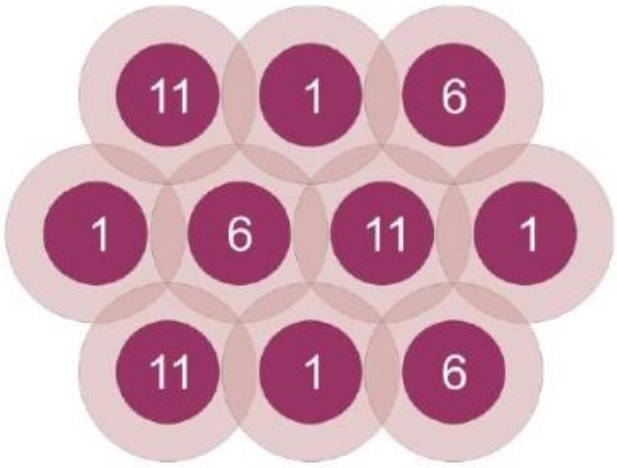
Adjacent APs need to use different radio channels to prevent interference between them. See Channel and Transmission power Considerations.

Cohabitation with DECT APs

Place WLAN APs at least 3.5 meters from DECT APs in order not to disturb DECT communications.

3.1.4 Channel and Transmission power Considerations

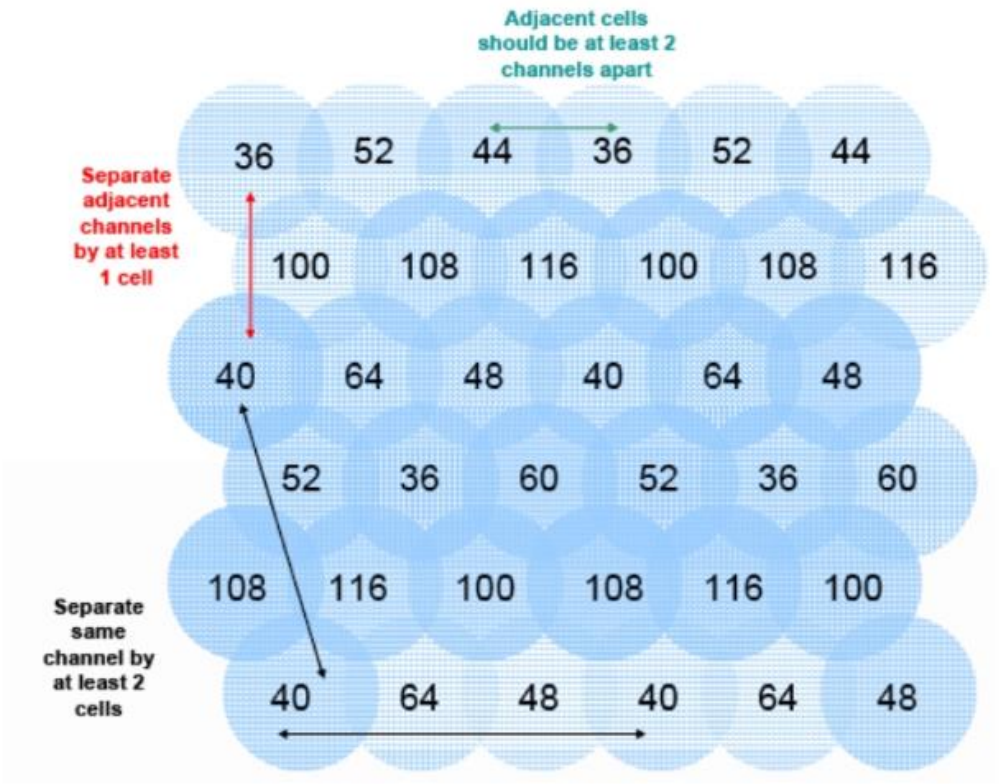
Adjacent APs need to use different radio channels to prevent interference between them. The 802.11b/g/n standard provides for three non-interfering channels: channels 1, 6, and 11. APs within range of each other should always be set to non-interfering channels to maximize the capacity and performance of the wireless infrastructure, as shown in the diagram below.



If adjacent APs are set to the same channel, or use channels with overlapping frequency bands, the resulting interference will cause a significant reduction in the network performance and throughput, and will degrade overall voice quality.

In an 802.11a/n deployment, all 23 channels are considered non-overlapping, since there is 20 MHz of separation between the center frequencies of each channel.

However, since there is some frequency overlap on adjacent 802.11a channel sidebands, there should always be at least one cell separating adjacent channels and two cells separating the same channel, as shown in the diagram below.



For voice only applications: do not use the same channel for APs placed less than 3.5 meters from each other. This distance assumes that the AP's transmit power is 100 mW, For an interfering AP emitting at a different power level, the rule is, the interferer has to be at such a distance that it should not been seen by the system at more than –40 dBm.

For voice and data applications in 802.11b/g band: do not use the same channel for APs placed less than 12 meters from each other. This distance assumes that the AP's transmit power is 100 mW, For an interfering AP emitting at a different power level, the rule is, the interferer has to be at such a distance that it should not been seen by the system at more than –47 dBm.

The transmission power of APs can be increased or decreased to provide more or less AP coverage area. Generally, the transmission power setting should be the same

for all APs in a facility. This minimizes the chance of higher-power APs interfering with nearby lower-power APs and provides consistent coverage.

It is recommended to set AP power output to 100 mW. If this cannot be accommodated, use a 50 mW setting or a minimum of 30 mW. With lower power output settings, special attention must be made to AP placement to ensure there are no frequency reuse issues. Regardless of the selected power level settings, all APs and handsets must be configured with the same settings to avoid channel conflicts and unwanted cross-channel interference.

In mixed 802.11b/g environments, set the power of the 802.11b and 802.11g radios to the same setting, if they are separately configurable. For example, set both radio to 30mW to ensure identical coverage on both radios. For mixed 802.11a/b/g environments, where the AP uses all three radios types, AP placement should first be determined by modeling for the characteristics of 802.11a, since this environment will typically have the shortest range. Then, the transmission power of the 802.11b and 802.11g radios should be adjusted to provide the required coverage levels for those networks, within the already established AP locations.

Where possible, all APs should be set to the same transmission power level within a given radio type. For example, set all 802.11a radios to 50 mW and set all 802.11b and 802.11g radios to 30 mW. It crucial to then set the transmission power of the handset to match the transmission power of the APs. This will ensure a symmetrical communication link. Mismatched transmission power outputs will result in reduced range, poor handoff, one-way audio and other QoS issues.

3.2 Express mode

Stellar APs, by default, are running in “**Express mode**”. To configure the AP out-of-box, connect the AP to the network and powered by POE or power adapter, and ensure the AP could retrieve an IP address from the network.

When the LED on AP would be in "Green Blinking" state, a SSID named with "**AP-xx:xx**" (xx:xx is the last 4 characters of the AP MAC address) will be able to detected and connected. After associated with this WLAN SSID, the AP Web Based Management page would be able to reached via below default URL: http://mywifi.al-enterprise.com:8080/ or http://<AP_IP_Address>:8080/. After login with the default account (user: **Administrator** / Password: **admin**), the "***configuration wizard***" would be displayed on WBM configuration, user may follow the wizard to configure the AP.

For more details, please refer to the QSG document of each AP model.

In case of some abnormal situation, below methods could help to make the AP back to "factory settings":

- Long pressing the "reset" button
- Command "*firstboot*" + "*reboot*" input via Console or SSH connection
- Click "*Clear All Configuration*" from "*WBM -> AP Configuration*"

3.3 OV Cloud Mode

Stellar APs could be centralized managed by OmniVista Cirrus. A default OVC Server URL is built-in AP software. The AP will be switched to OVC mode automatically when below two conditions are met:

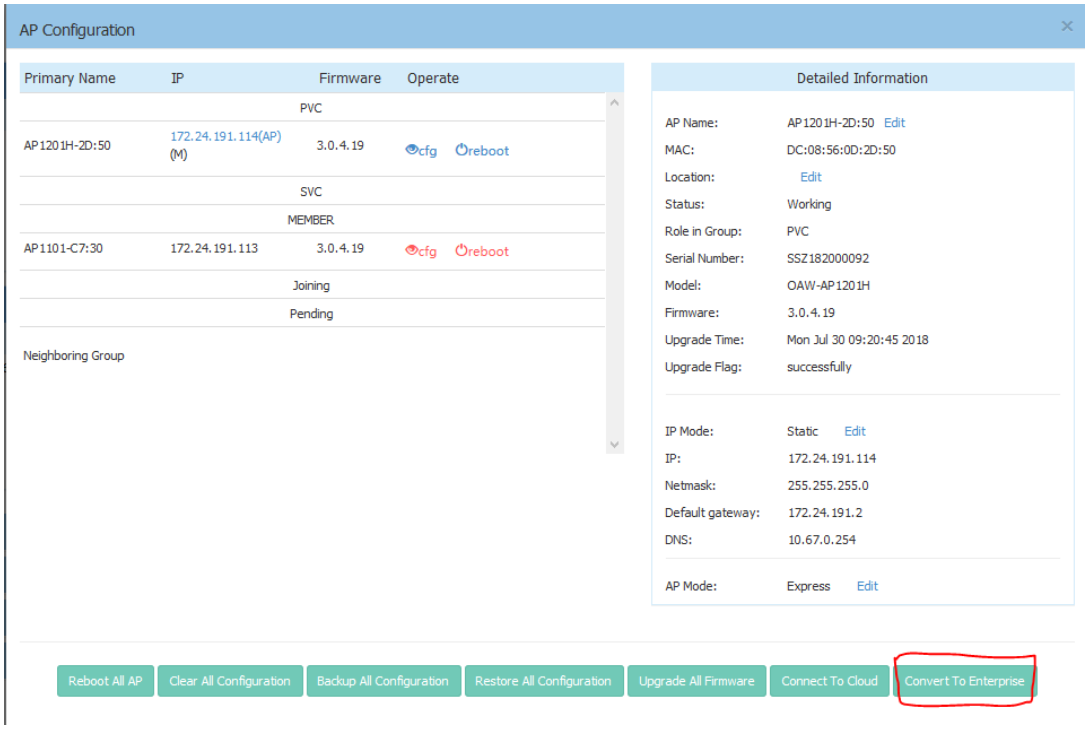
- AP network is able to reach the built-in OVC Server URL
- The AP hardware information has been correctly configured in OVC Server.

For more details, please refer to the related guides or documents of OmniVista Cirrus.

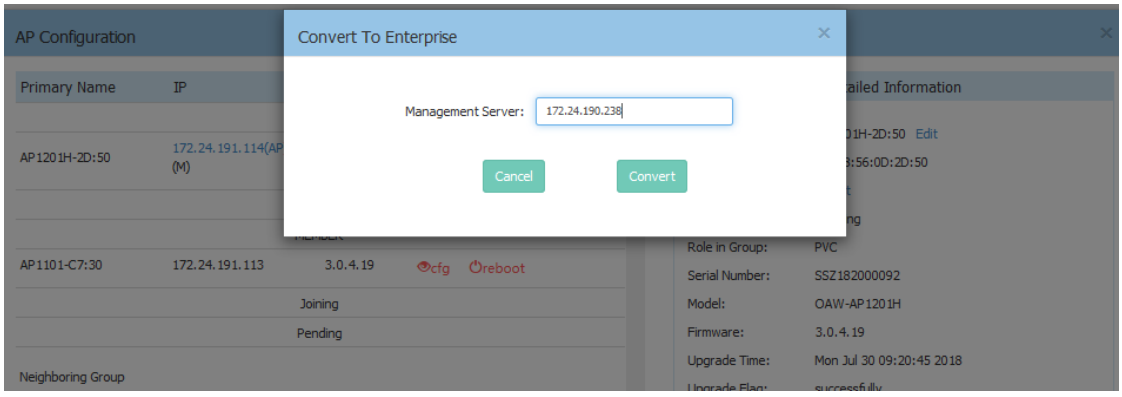
3.4 OV Enterprise mode

Stellar APs could also be centralized managed by OmniVista Enterprise. Below two methods could be used to switch the AP to OVE mode:

- AP receives option 43 or option 138 from the DHCP server specifying the OmniVista IP, the AP will boot up and connect to OmniVista 2500 for management.
- AP in "Express mode" could be switched to OVE mode through Web Based Management as below:
  - Login AP WBM, go to "**AP Configuration**", and click "**Convert To Enterprise**" button.



  - Specify the OVE Server IP address, and press "**Convert**"



For more details, please refer to the related guides or documents of OmniVista Enterprise.

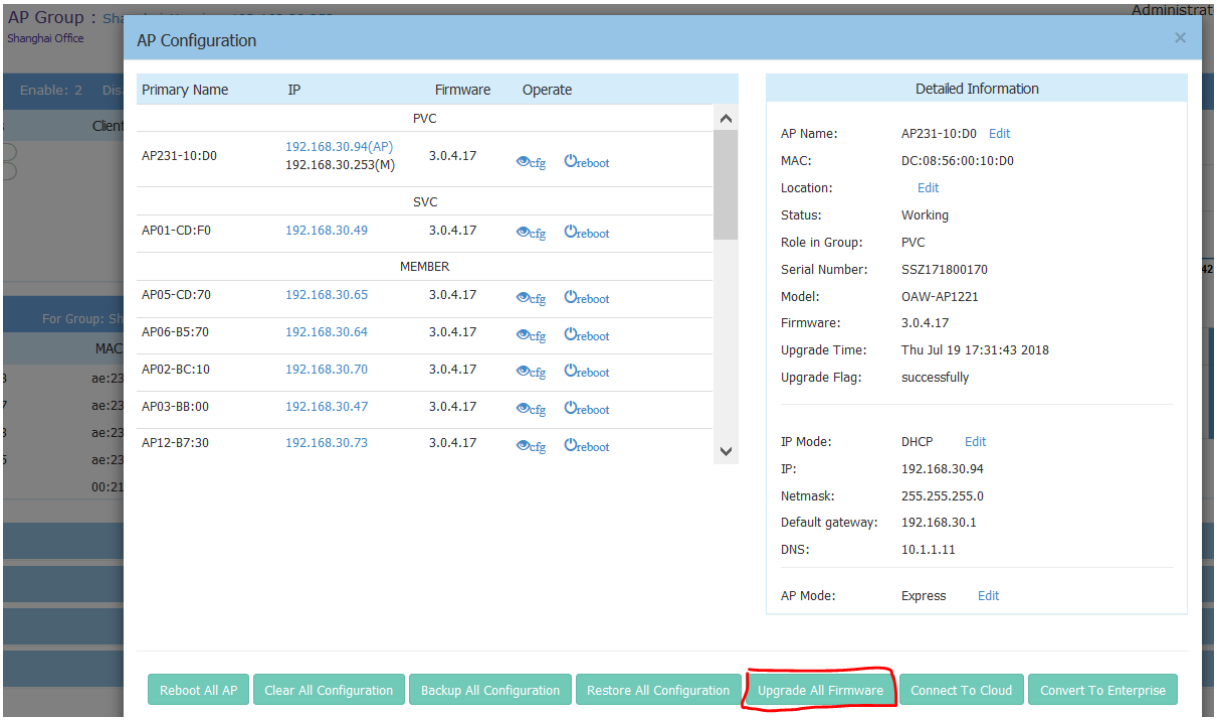
4 Software Upgrading

4.1 Upgrading in Express mode

Working in "Express mode", the AP software upgrading could be managed from the Web Based Management. The software upgrading could be managed either in the whole cluster or per single AP. While to avoid any incompatibility issue, strongly recommend to keep all the APs within the whole cluster in the same software versions.

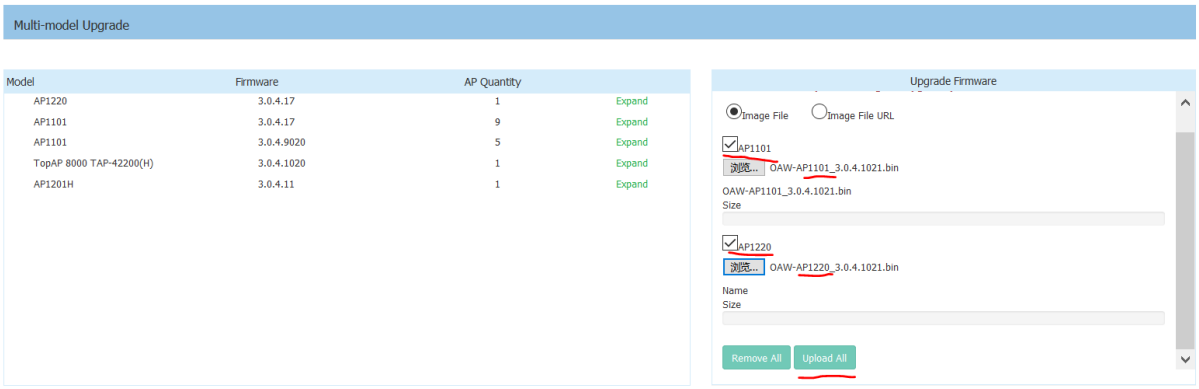
Procedures of AP upgrading in the whole cluster

- Login AP WBM, go to "**AP Configuration**", and click "**Upgrade All Firmware**" button.



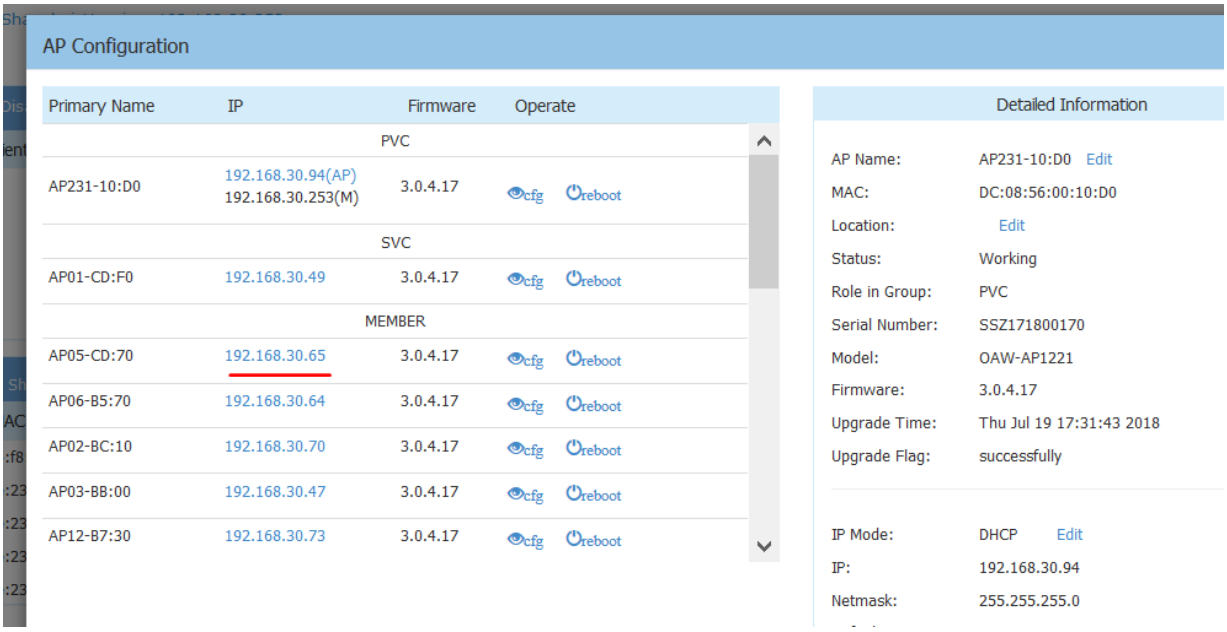
- Click the AP modes need to be upgraded, and select the AP firmware accordingly. Then press "**Upload All**".

Importance: Don't turn off the power during the upgrade process.



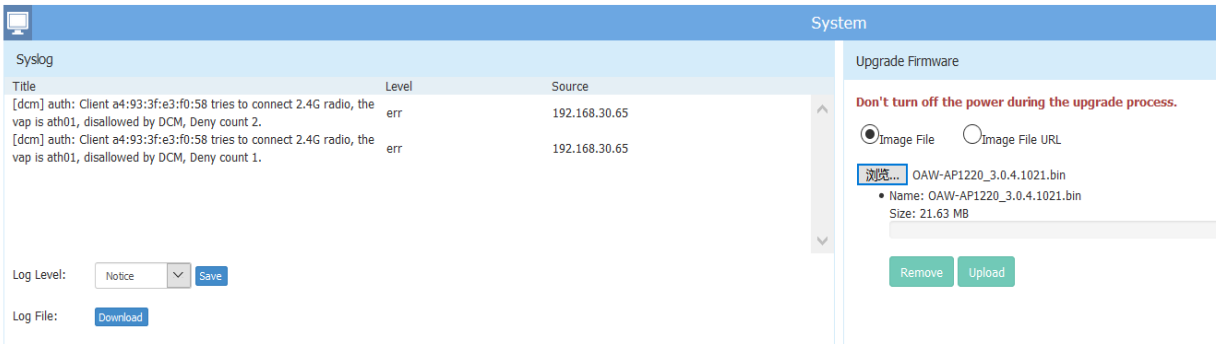
Procedures of Single AP Software Upgrading:

- Login AP Cluster WBM, go to "**AP Configuration**" and Select the IP address of AP which need to be upgraded.



- A new WBM page (apui) will be opened. Click "**Image File**" from "System" and select the AP software according to the AP model. Press "**Upload**" button to start the upgrading.

Importance: Don't turn off the power during the upgrade process.



4.2 Upgrading in OV Cloud mode

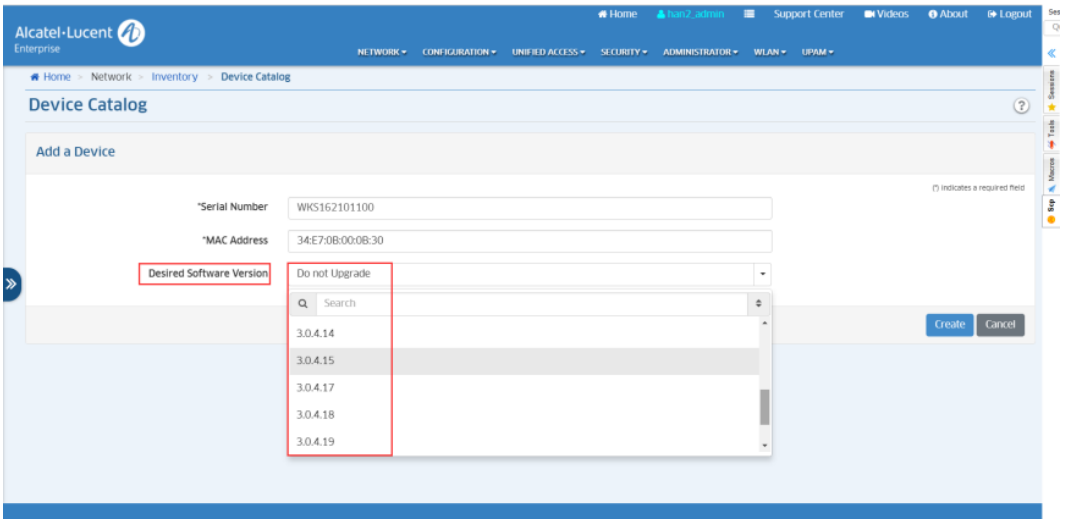
When working in OVC (OmniVista Cloud) mode, the AP software could be centralized managed through OVC management server. Single or all APs could be upgraded as requested.

✎ **Note**: *From AWOS-3.0.4.x and later releases, the AP upgrading will be started in 30 minutes. Regarding the previous releases (AWOS-3.0.3.x), "manual restart" of the AP would be required to trigger the upgrading.*

Procedures of the upgrading in OVC mode:

Upgrade when registering a new AP to OV Cloud

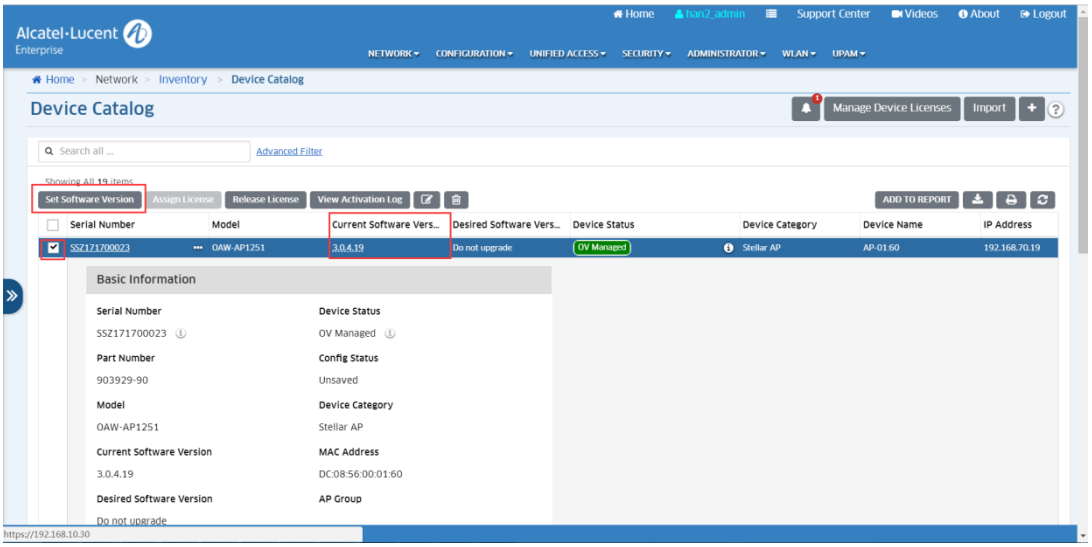
- Log in OV cloud, enter the **Network** -> **inventory** -> **device Catalog** page, click the "**+**" button, enter the MAC and SN, and select the software version that wants to be updated in the "**Desired Software Version**", then click create.

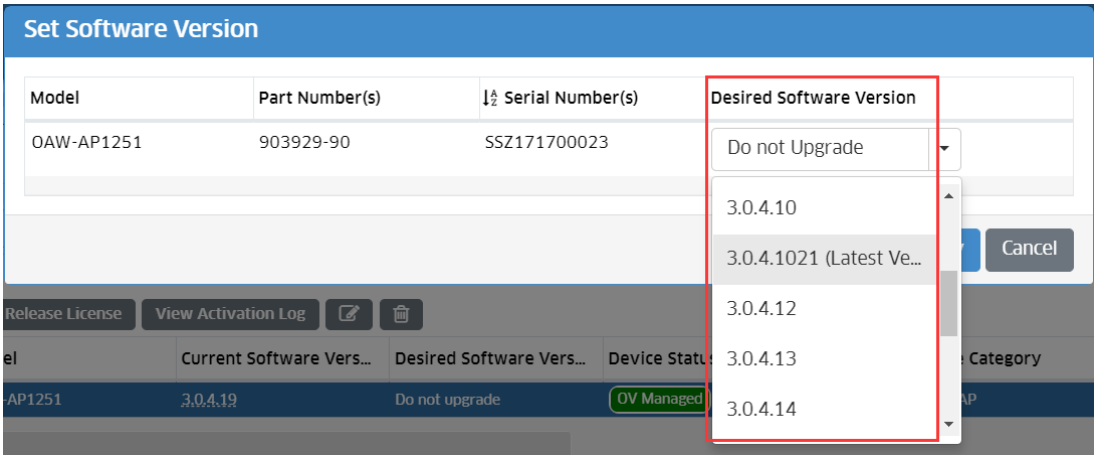


- AP will be registered to OV cloud after upgrading to the selected version.

Upgrade for one registered AP

- Go to the **Network** -> **inventory** -> **device Catalog** page, select the AP need to be upgraded, and click the "**Set Software Version**" button.



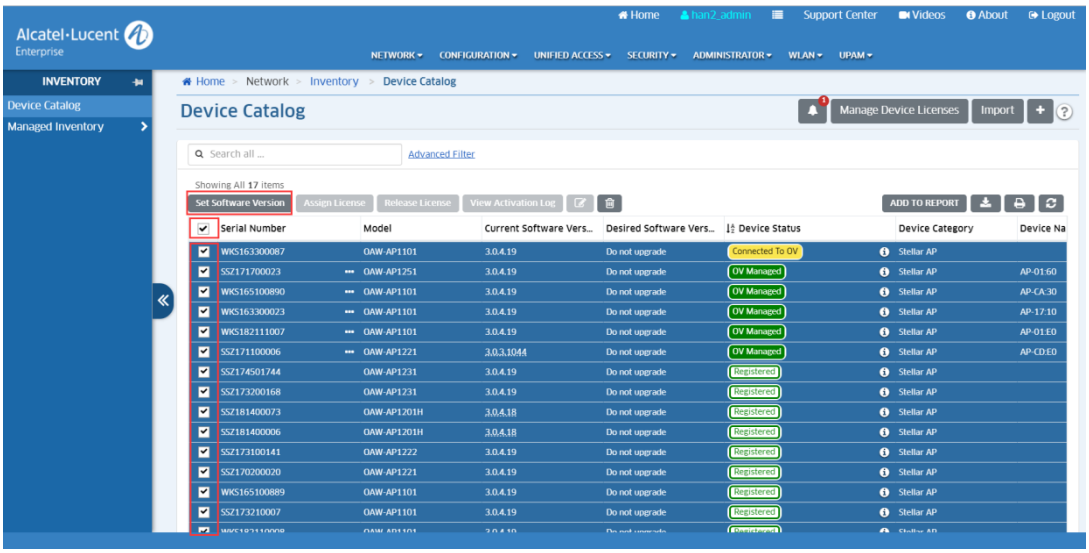


- Select the version you want to upgrade in "**Desired Software Version**" and click **apply**.

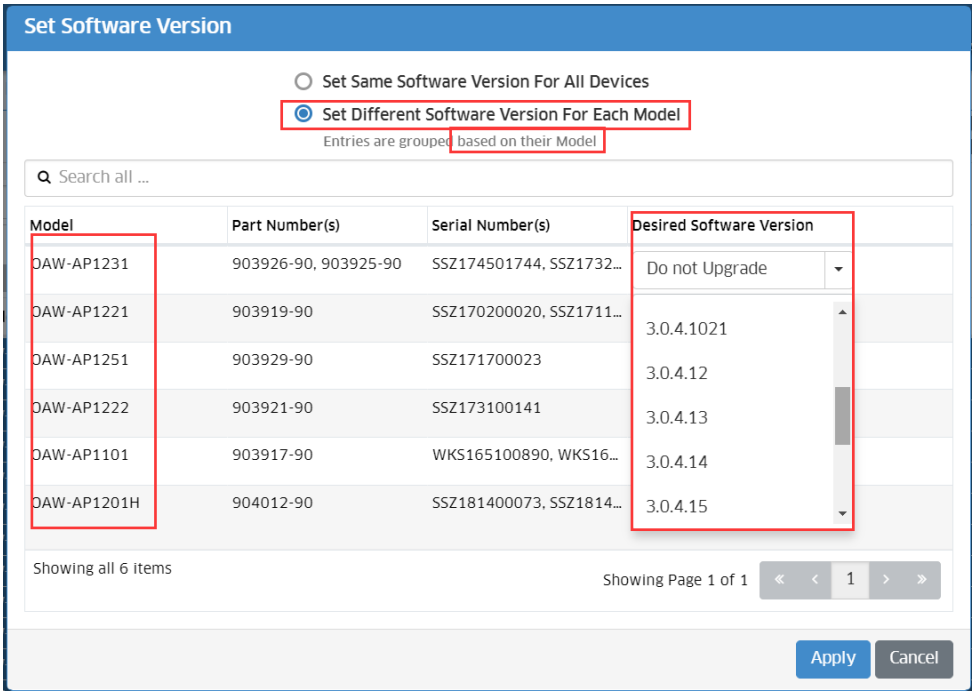
  The AP will start to upgrade when the next callhome is sent.

Upgrade for multiple registered AP

- Go to the **Network** -> **inventory** -> **device Catalog** page, select multiple (or all) AP need to be upgraded, and click the "**Set Software Version**" button



- Select the "**Set Different Software Version For Each Model**" option, select the version to be upgraded in the "**Desired Software Version**" drop-down box, and click apply.



- The APs will start to upgrade when the next callhome is sent.

4.3 Upgrading in OV Enterprise mode

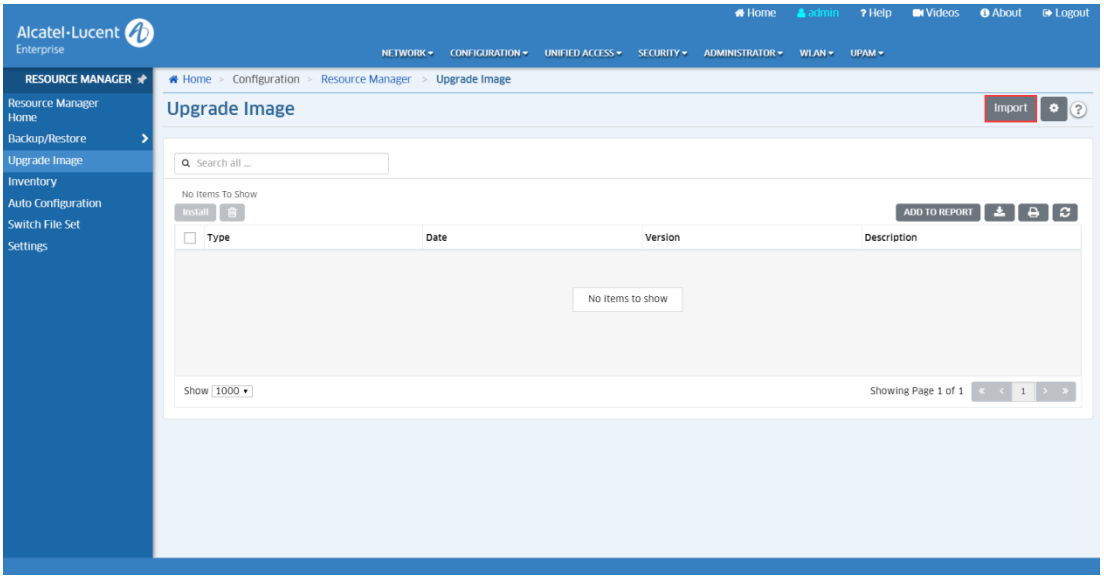
When working in OVE (OmniVista Enterprise) mode, the AP software could be centralized managed through OVE management server. Single or all APs could be upgraded as requested.

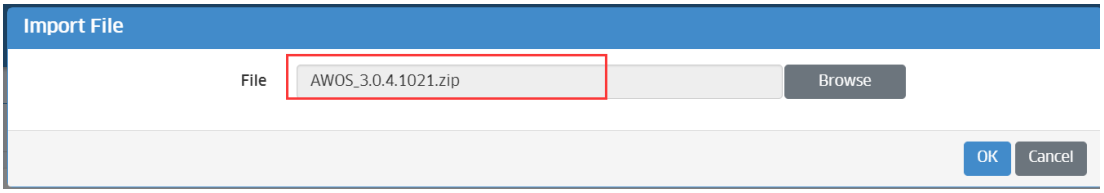
✎ **Note:** *Reboot of the AP is mandatory during the AP upgrading, so no WLAN service at that moment.*

Procedures of the upgrading in OVE mode:

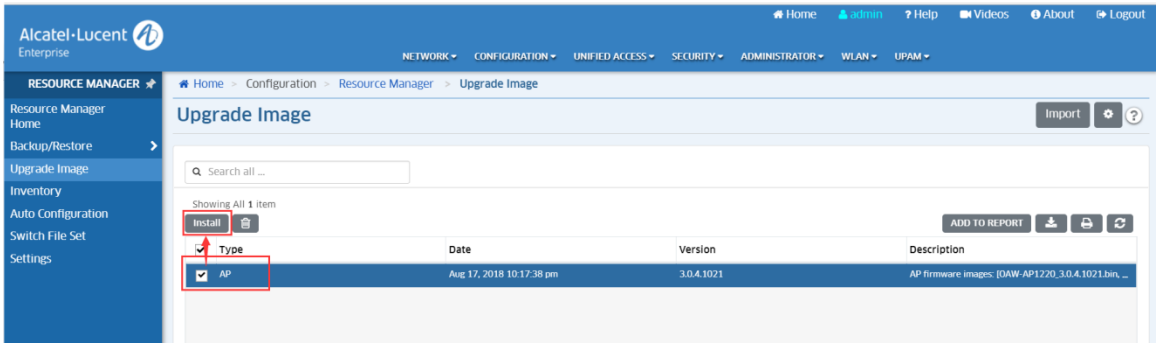
AP Software versions uploading:

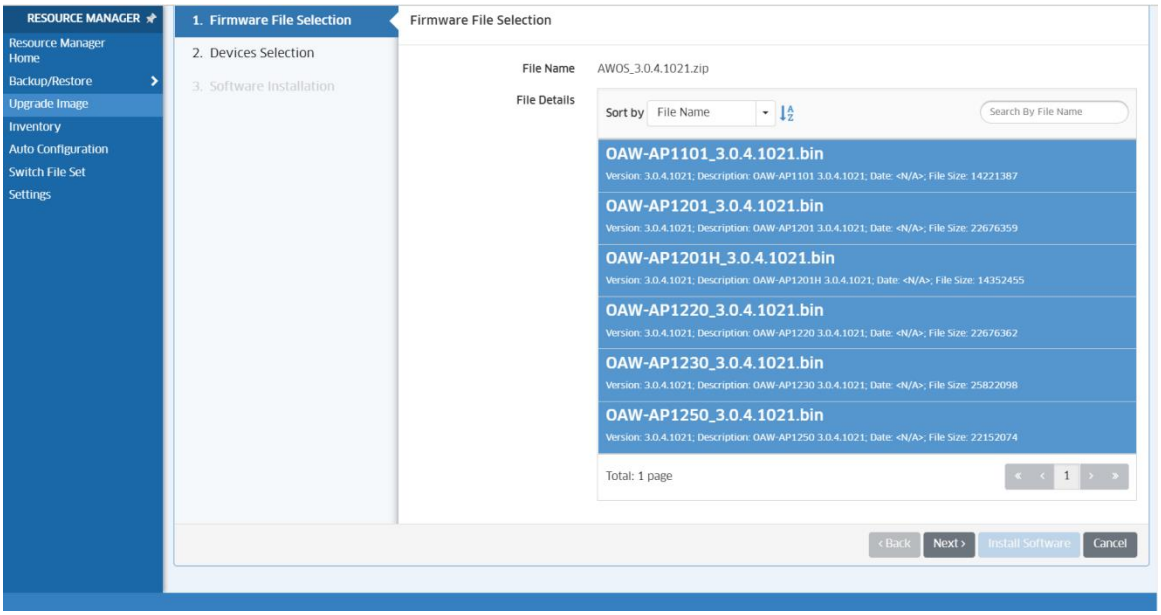
- Log in OV Enterprise, enter the **Configuration--Resource Manager--Upgrade Image** page, click **import** to upload the AP software version to be upgraded.





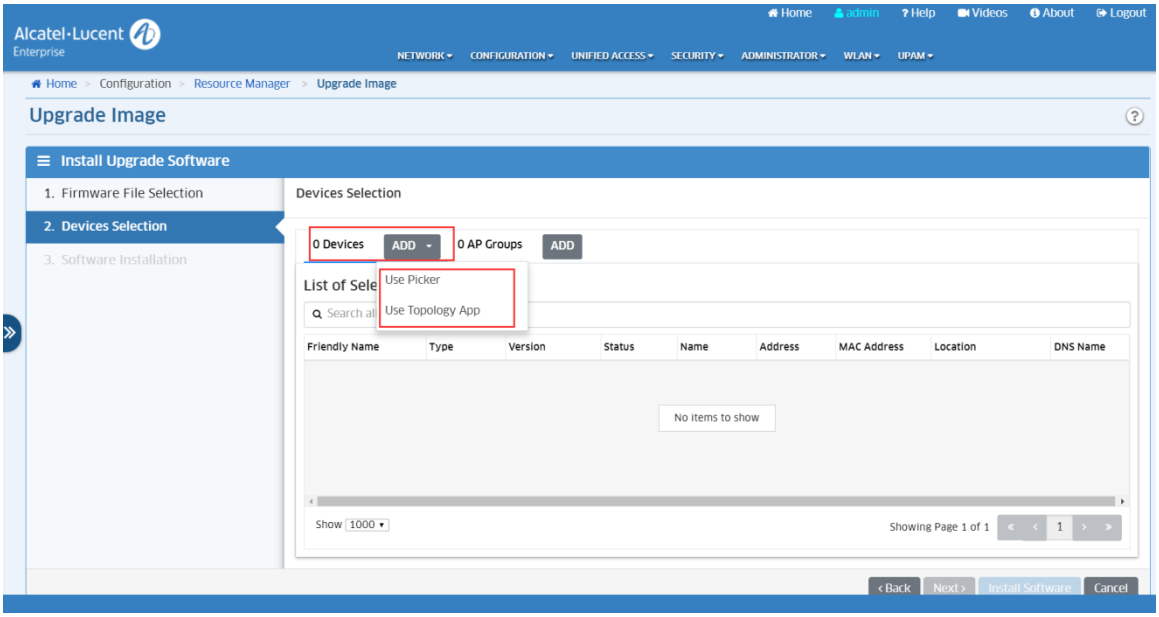
- After uploading the AP software version, select the file, and click the **install** button, and then go to **devices selection** step.



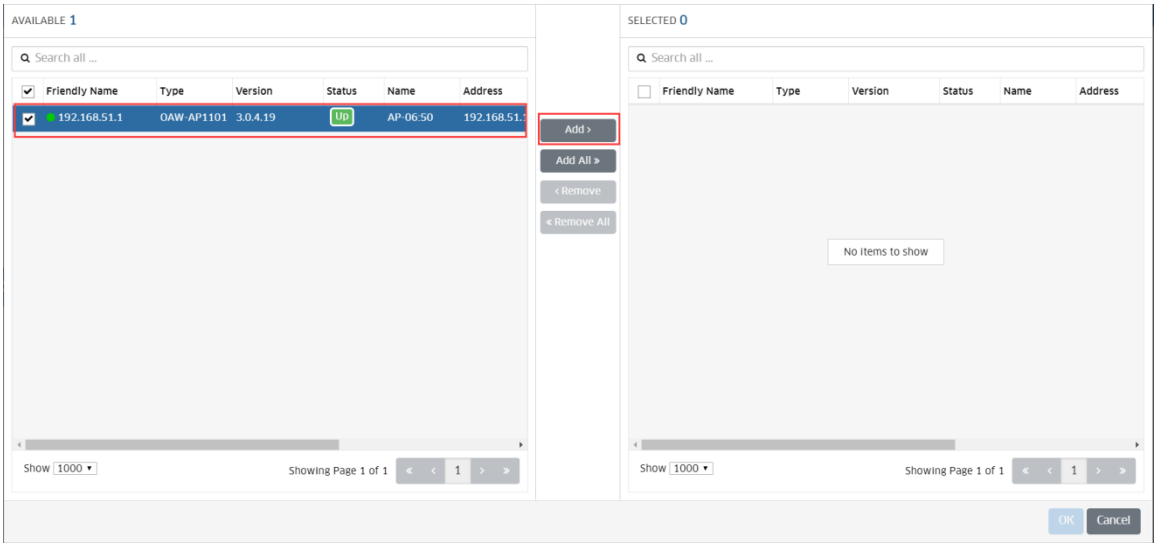


Upgrade per AP/APs

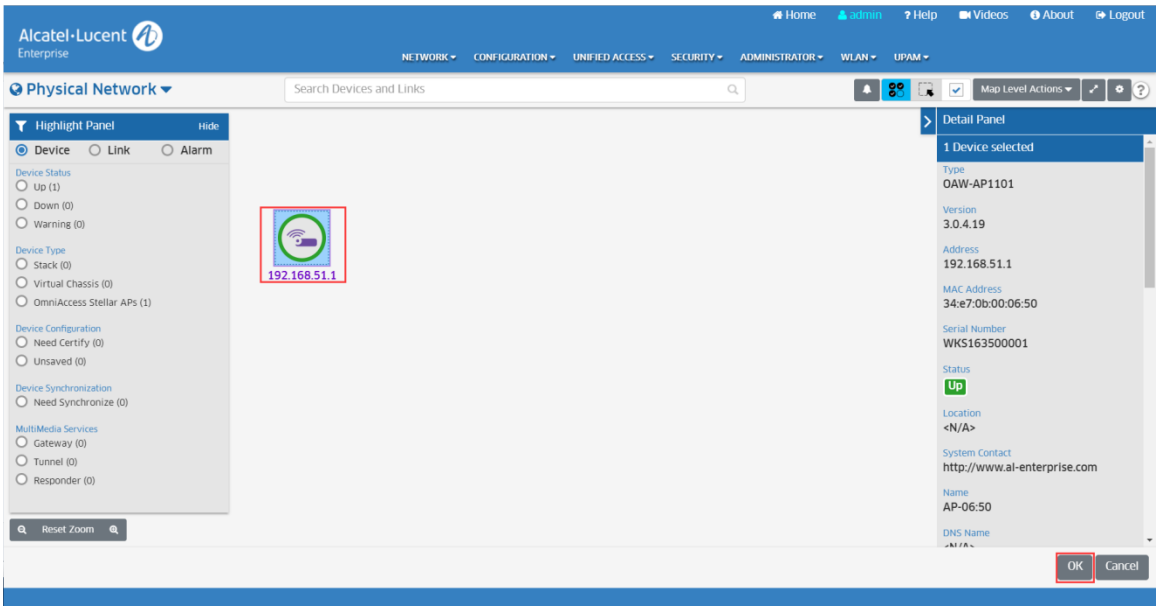
- Click the "**next**" to open the **device selection** window. Click the **ADD** button of device and use "**Use Picker**" or "**Use Topology App**" to select the AP to be upgraded.



- In the "**Use Picker**" page, select the AP, and click the **add** button to add to the selected window, then click **OK**

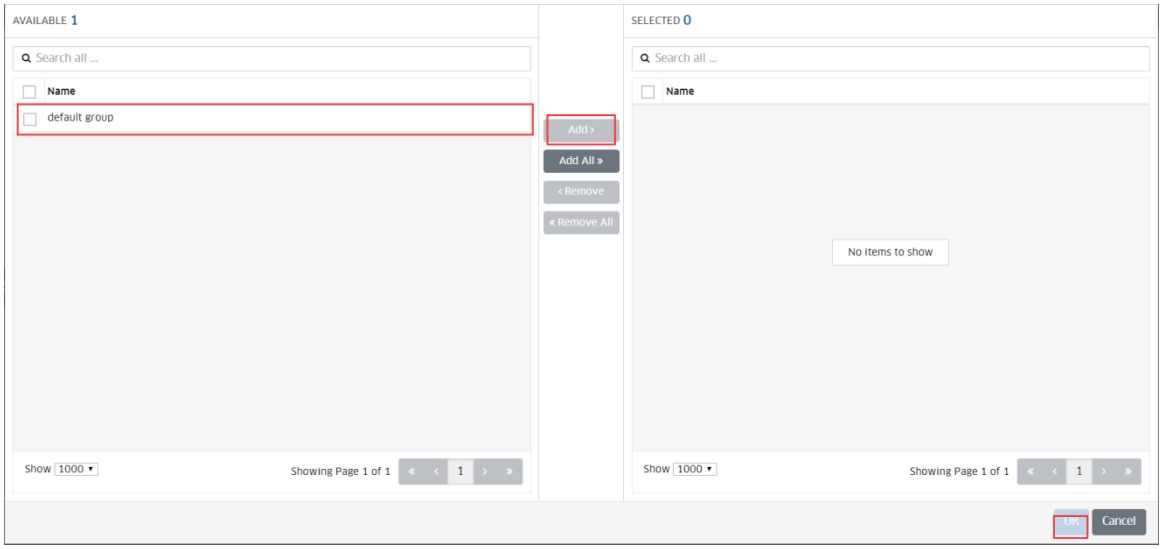


- In the "**Use Topology App**" page, select the AP need to be upgraded and click **OK.**

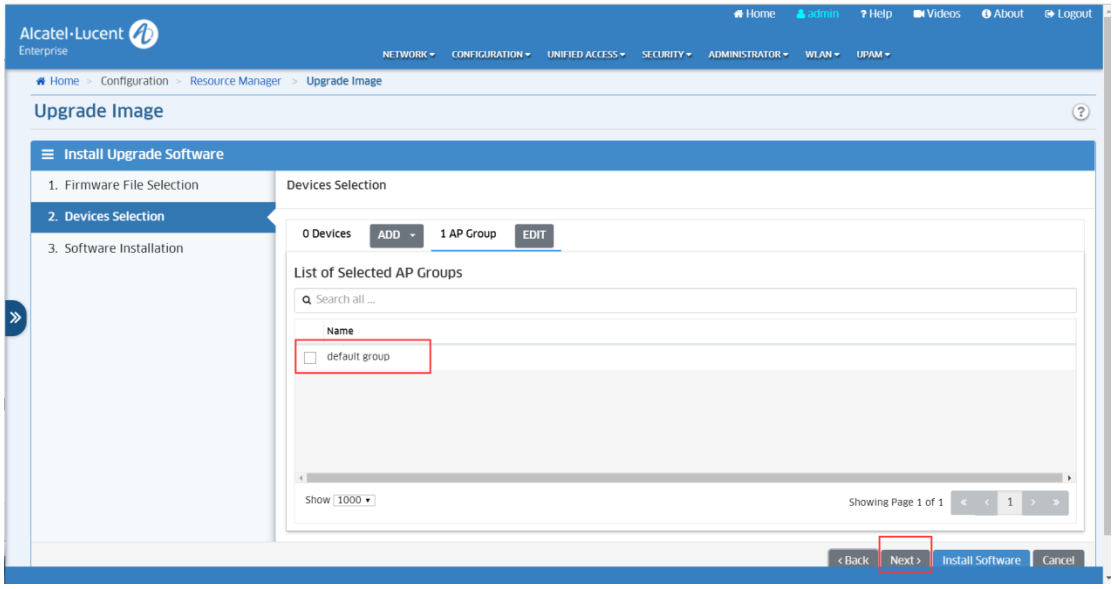


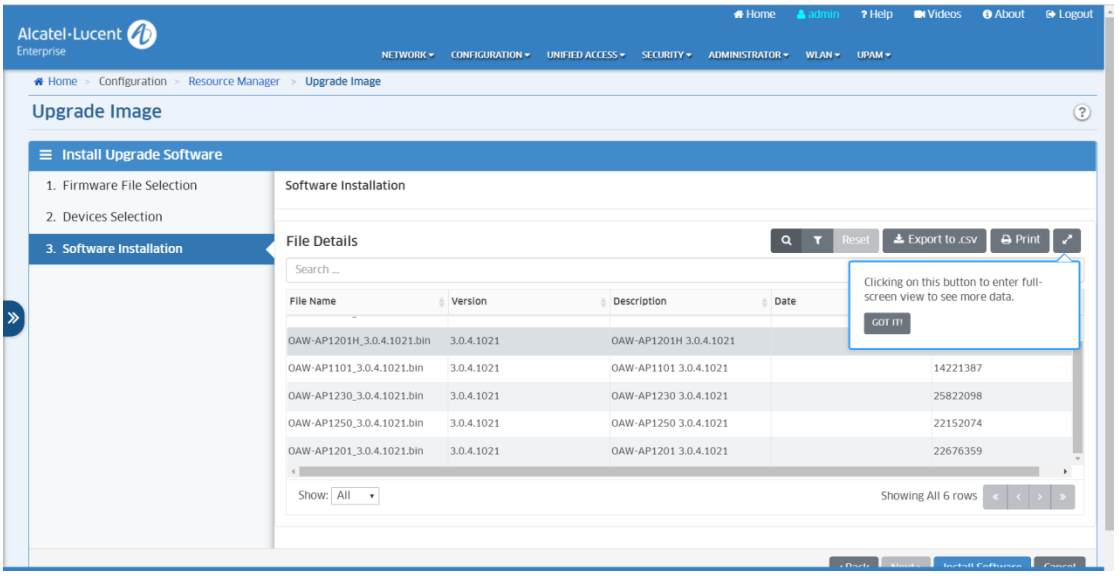
Upgrade per AP Group

- In the **device selection** window, click the **ADD** button of AP Groups, go to the group selection window.
- Select AP Groups, and click the **Add** button, and click OK.

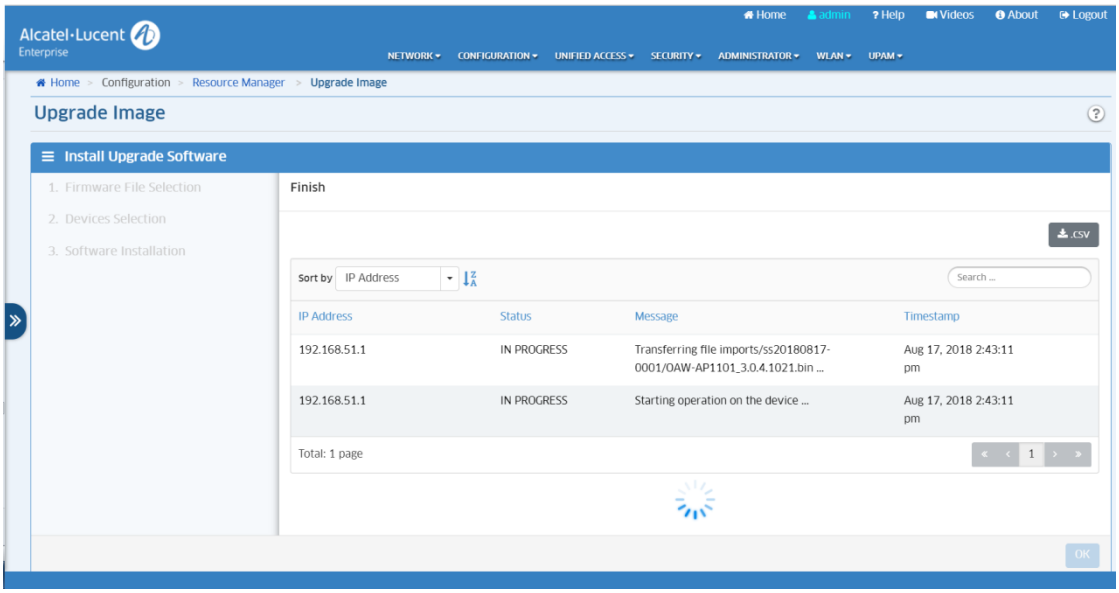


- After selecting the AP, click the "**Next**" to enter the Software Installation page.





- Click the "**install software**" button to enter the upgrade page.



✎ **Note**: *To avoid incompatibility issues, suggest keeping the same AP software version in the AP group. So, it's better to use "AP Group" when upgrading the APs.*

4.4 Upgrading through Bootloader

In some specific cases, the AP may be not in a normal operation state, which cannot be succeeded upgraded though any of the working modes. It will need to upgrade the AP through Bootloader.

4.4.1 Entering Bootloader

To enter the bootloader, it will need to connect the console port and open the console session. During the AP initialization, pressing any key when below words showing on the screen of console:

```
Hit any key to stop autoboot:  0
```

4.4.2 AP1101

Procedure of the upgrading AP1101 through bootloader:

- ✓ To setup a TFTP server on a PC, and put the images on the TFTP server path:
  - OAW-AP1101-UBOOT_KERNEL_**3.0.x.x**.bin
  - OAW-AP1101-UBOOT_ROOTFS_**3.0.x.x**.bin
- ✓ To enter the bootloader during AP initialization, which is described in 4.4.1.
- ✓ Network configuration (IP Address, TFTP Server Address…)

  Example: IP address=***172.16.18.11***; TFTP Server Address=***172.16.18.129***

  # set ipaddr **172.16.18.11**

  # set serverip **172.16.18.129**
- ✓ AP upgrading through bootloader

set bootcmd bootm 0x9f050000

mw 0x18060008 0x0

set lk-aos "tftp 0x80060000 OAW-AP1101-UBOOT_KERNEL_**3.0.x.x**.bin && erase 0x9f050000 +0x180000 &&cp.b 0x80060000 0x9f050000 0x180000"

set lf-aos "tftp 0x80060000 OAW-AP1101-UBOOT_ROOTFS_**3.0.x.x**.bin && erase 0x9f1d0000 +0xc20000 &&cp.b 0x80060000 0x9f1d0000 0xc20000"

run lk-aos && run lf-aos && reset

4.4.3 AP1220 Series

Procedure of the upgrading AP1220 Series through bootloader:

- ✓ To setup a TFTP server on a PC, and put the images on the TFTP server path:
  - OAW-AP1220-UBOOT_FIRMWARE_**3.0.x.x**.bin
- ✓ To enter the bootloader during AP initialization, which is described in 4.4.1.
- ✓ Network configuration (IP Address, TFTP Server Address…)

  Example: IP address=***172.16.18.11***; TFTP Server Address=***172.16.18.129***

  # set ipaddr **172.16.18.11**

  # set serverip **172.16.18.129**

  # save

- ✓ AP upgrading through bootloader

  # tftpboot 0x84000000 OAW-AP1220-UBOOT_FIRMWARE_**3.0.x.x**.bin

  # nand erase 0x0 0x10000000 && nand write 0x84000000 0x0 $filesize

nand read 0x85000000 0x0 $filesize

md5sum 0x85000000 $filesize

reset

✓ After AP reboot, entering below commands to make dual system working.

fm_switch

reboot

4.4.4 AP1230 Series

There’ re two Ethernet ports on AP1230 Series, one is Gigabit Ethernet port, another one is 2.5 Gigabit Ethernet port. We **MUST** use the **Gigabit Ethernet** port for both upgrading AP through bootloader and upgrading UBoot version.

Procedure of the upgrading AP1230 through bootloader:

✓ To setup a TFTP server on a PC, and put the images on the TFTP server path:

- OAW-AP1230-UBOOT_FIRMWARE_**3.0.x.x**.bin

✓ To enter the bootloader during AP initialization, which is described in 4.4.1.

✓ Network configuration (IP Address, TFTP Server Address…)

Example: IP address=***172.16.18.11***; TFTP Server Address=***172.16.18.129***

set ipaddr **172.16.18.11**

set serverip **172.16.18.129**

save

✓ AP upgrading through bootloader

tftpboot 0x42000000 OAW-AP1230-UBOOT_FIRMWARE_**3.0.x.x**.bin

nand erase 0x0 0x10000000 && nand write 0x42000000 0x0 $filesize && nand read 0x42000000 0x3000000 $filesize

nand read 0x43000000 0x0 $filesize && md5sum 0x43000000 $filesize

nand read 0x44000000 0x3000000 $filesize && md5sum 0x44000000 $filesize

reset

✓ After AP reboot, entering below commands to make dual system working.

fm_switch

reboot

4.4.5 AP1251

Procedure of the upgrading AP1250 Series through bootloader:

✓ To setup a TFTP server on a PC, and put the images on the TFTP server path:

- OAW-AP1250-UBOOT_FIRMWARE_**3.0.x.x**.bin

✓ To enter the bootloader during AP initialization, which is described in 4.4.1.

✓ Network configuration (IP Address, TFTP Server Address…)

Example: IP address=***172.16.18.11***; TFTP Server Address=***172.16.18.129***

set ipaddr **172.16.18.11**

set serverip **172.16.18.129**

save

✓ AP upgrading through bootloader

tftpboot 0x84000000 OAW-AP1250-UBOOT_FIRMWARE_**3.0.x.x**.bin

nand erase 0x0 0x10000000 && nand write 0x84000000 0x0 $filesize && nand read 0x84000000 0x03000000 $filesize

nand read 0x85000000 0x0 $filesize && md5sum 0x85000000 $filesize

nand read 0x83000000 0x03000000 $filesize && md5sum 0x83000000 $filesize

reset

✓ After AP reboot, entering below commands to make dual system working.

fm_switch

reboot

4.4.6 AP1201

Procedure of the upgrading AP1201 Series through bootloader:

✓ To setup a TFTP server on a PC, and put the images on the TFTP server path:

- OAW-AP1201-UBOOT_FIRMWARE_3.0.x.x.bin

✓ Network configuration (IP Address, TFTP Server Address…)

Example: IP address=***172.16.18.11***; TFTP Server Address=***172.16.18.129***

set ipaddr **172.16.18.11**

set serverip **172.16.18.129**

✓ AP upgrading through bootloader

tftpboot 0x84000000 OAW-AP1201-UBOOT_FIRMWARE_3.0.x.x.bin

nand erase 0x0 0x8000000 && nand write 0x84000000 0x0 $filesize && nand write 0x84000000 0x03000000 $filesize

nand read 0x85000000 0x0 $filesize && md5sum 0x85000000 $filesize

Second check Md5 Command:

nand read 0x83000000 0x03000000 $filesize && md5sum 0x83000000 $filesize

reset

4.5 Upgrading UBoot

Normally, it' s **NOT** necessary to upgrade UBoot software of APs. While in some very special cases, the new UBoot software version maybe needed to solve some issues.

This chapter describes the procedure of the UBoot upgrading for different AP models.

4.5.1 AP1101

Procedure of UBoot upgrading:

- ✓ To setup a TFTP server on a PC, and put the images on the TFTP server path:
  - hos-r21-boot.bin
- ✓ To enter the bootloader during AP initialization, which is described in 4.4.1.
- ✓ Network configuration (IP Address, TFTP Server Address…)

  Example: IP address=***172.16.18.11***; TFTP Server Address=***172.16.18.129***

  ath> set ipaddr **172.16.18.11**

ath> set serverip **172.16.18.129**

✓ UBoot Upgrading

ath> run lu

4.5.2 AP1220 Series

Procedure of UBoot upgrading:

✓ To setup a TFTP server on a PC, and put the images on the TFTP server path:

- OAW-AP1220-uboot_1.x.bin

✓ To enter the bootloader during AP initialization, which is described in 4.4.1.

✓ Network configuration (IP Address, TFTP Server Address…)

Example: IP address=***172.16.18.11***; TFTP Server Address=***172.16.18.129***

set ipaddr **172.16.18.11**

set serverip **172.16.18.129**

✓ UBoot Upgrading

tftpboot 0x84000000 OAW-AP1220-uboot_1.x.bin

imgaddr=0x84000000 && source $imgaddr:script && reset

4.5.3 AP1230 Series

Procedure of UBoot upgrading:

✓ To setup a TFTP server on a PC, and put the images on the TFTP server path:

- OAW-AP1230-uboot_1.x.bin

✓ To enter the bootloader during AP initialization, which is described in 4.4.1.

✓ Network configuration (IP Address, TFTP Server Address…)

Example: IP address=***172.16.18.11***; TFTP Server Address=***172.16.18.129***

set ipaddr **172.16.18.11**

set serverip **172.16.18.129**

save

✓ UBoot Upgrading

tftpboot 0x42000000 OAW-AP1230-uboot_1.x.bin

imgaddr=0x42000000&&sf probe&&source $imgaddr:script

reset

4.5.4 AP1251

Procedure of UBoot upgrading:

✓ To setup a TFTP server on a PC, and put the images on the TFTP server path:

- OAW-AP1250-uboot_1.x.bin

✓ To enter the bootloader during AP initialization, which is described in 4.4.1.

✓ Network configuration (IP Address, TFTP Server Address…)

Example: IP address=***172.16.18.11***; TFTP Server Address=***172.16.18.129***

set ipaddr **172.16.18.11**

set serverip **172.16.18.129**

save

✓ UBoot Upgrading

tftpboot 0x84000000 OAW-AP1250-uboot_1.x.bin

```
# imgaddr=0x84000000 source $imgaddr:script && reset
```

4.5.5 AP1201

Procedure of UBoot upgrading:

- ✓ To setup a TFTP server on a PC, and put the images on the TFTP server path:
  - OAW-AP1201-uboot_1.x.bin
- ✓ To enter the bootloader during AP initialization, which is described in 4.4.1.

  Example: IP address=172.16.18.11; TFTP Server Address=172.16.18.129

  # set ipaddr 172.16.18.11

  # set serverip 172.16.18.129
- ✓ UBoot Upgrading

  # tftpboot 0x84000000 OAW-AP1201-uboot_1.0.bin

  # imgaddr=0x84000000 source $imgaddr:script

  # reset

Features and Configurations

4.6 ACS & DRM

4.6.1 Feature description

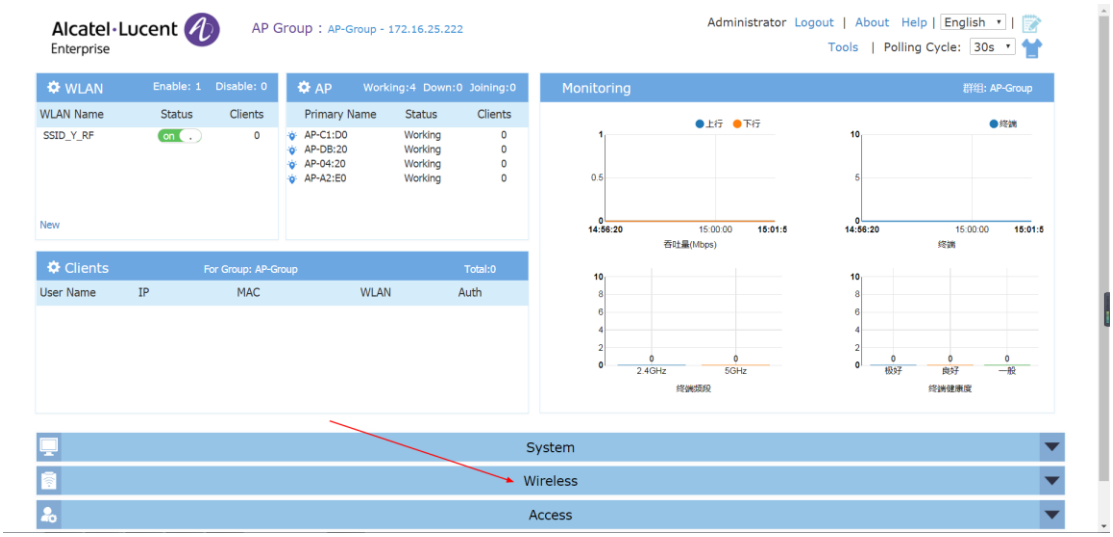
Adjacent APs need to use different radio channels to prevent interference between them. APs within range of each other should always be set to non-interfering channels to maximize the capacity and performance of the wireless infrastructure. Please check chapter 3.1.3 for more detail.

To avoid mutual interference with adjacent APs, ACS (auto channel selection) could be used to make the AP to check and select a best channel under the radio environment automatically. The algorithm will help the AP to find the channel with best radio performance.

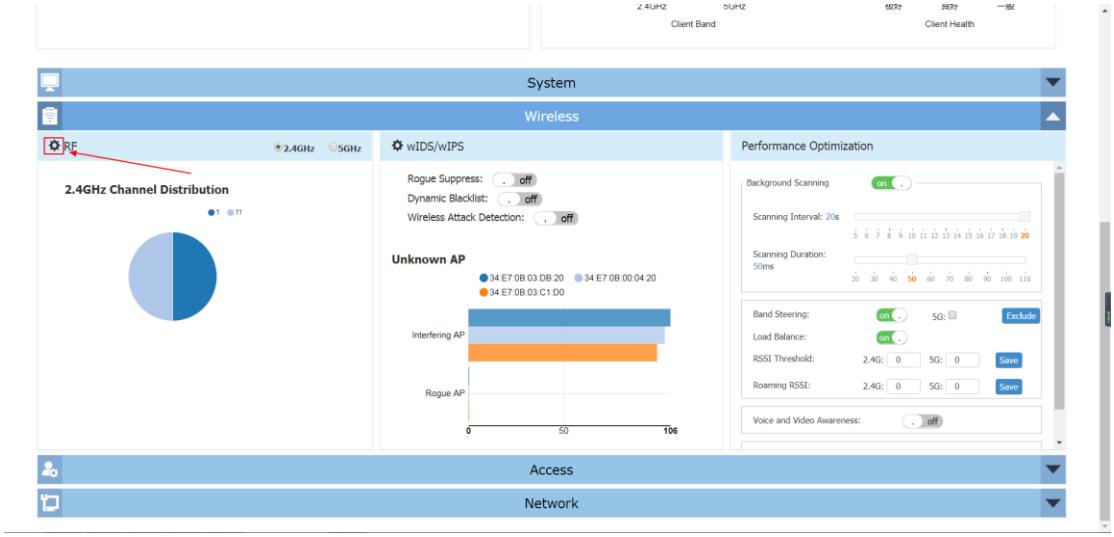
And if working on 5G radio, the DRM could be used to define a "Channel List" to make the AP to select the channels from the list.

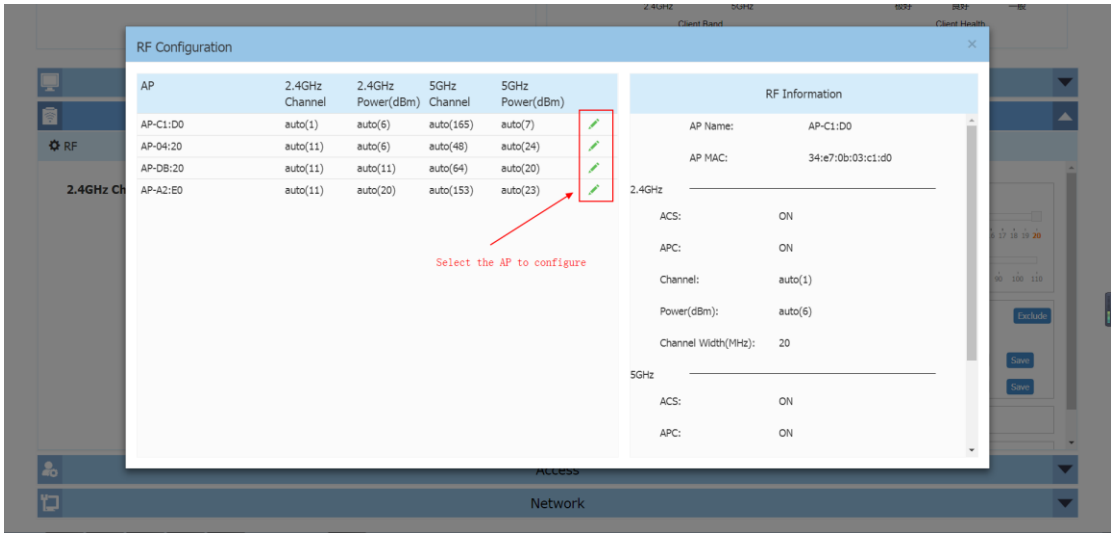
4.6.2 Configuration and Recommendation

- Login the WEB UI and go to "**Wireless**" sub-menu. As below.

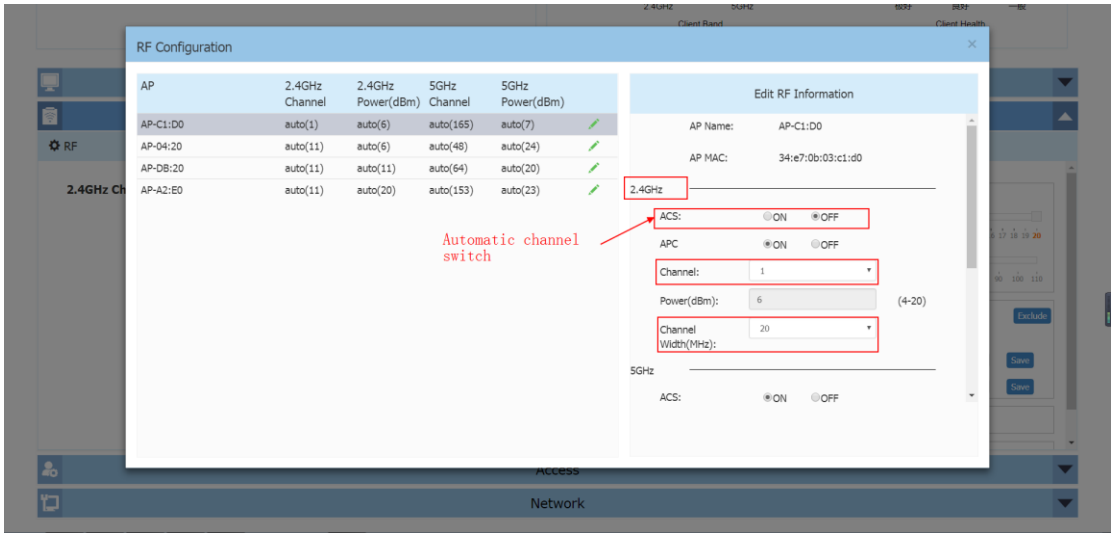


- Go to "**RF**" configuration, and select the AP to be configured.

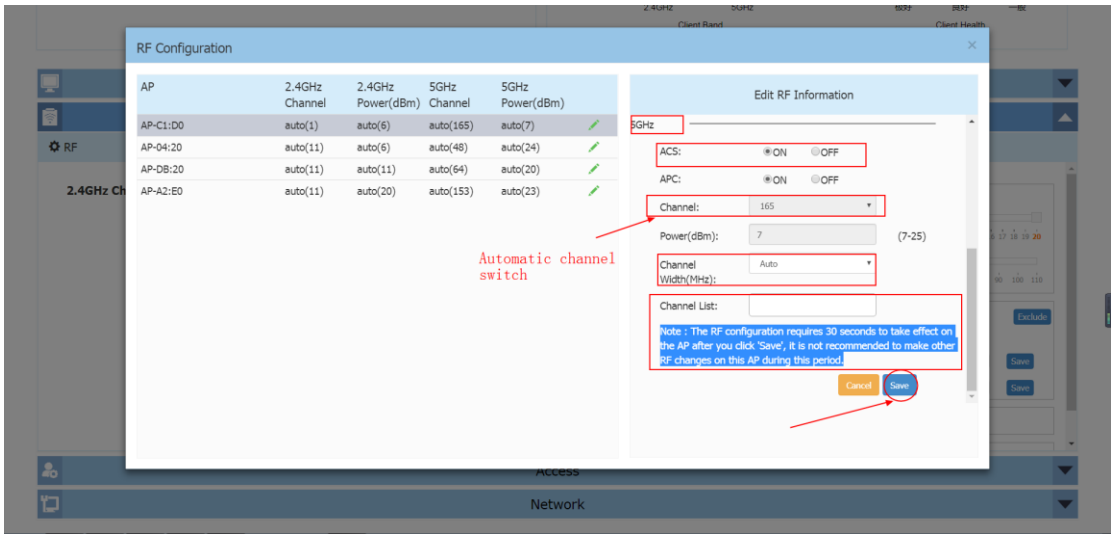




- The **ACS** could be turn **ON/OFF** separately on 2.4GHz or 5GHz.



- On 5GHz radio, the DRM could be configured.



4.7 APC

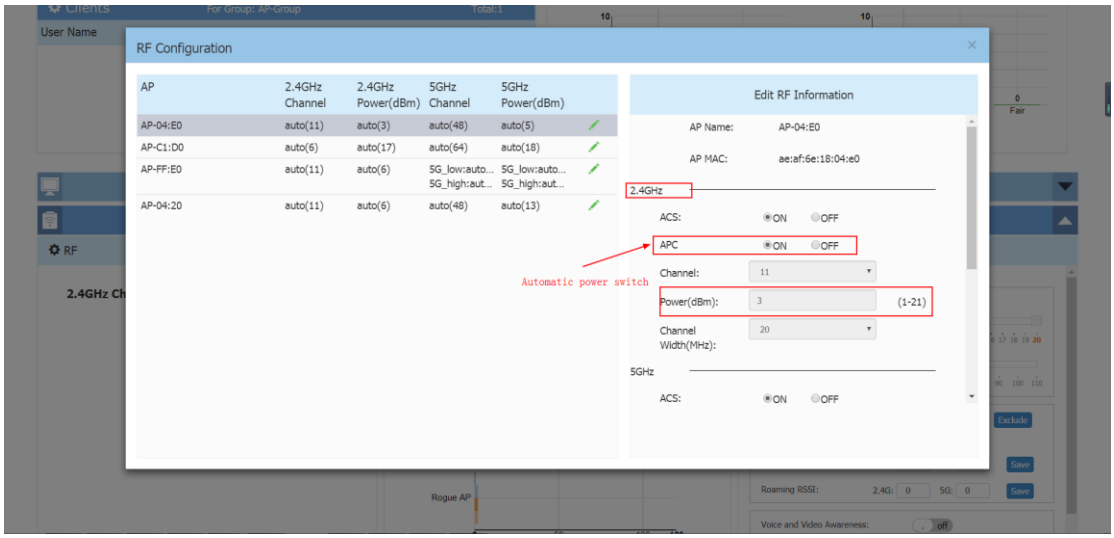
4.7.1 Feature description

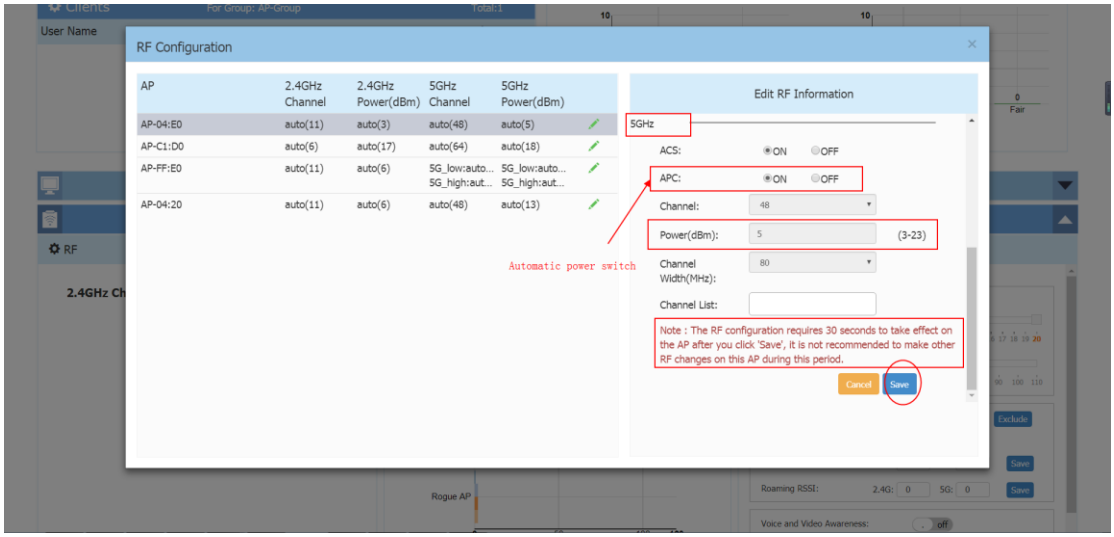
In order to have a better radio coverage, and less mutual interference between the adjacent APs, APC (Auto Power Control) could be used to make the AP to scan the other APs transmission power, and then to calculate and control its owner RF transmission power.

4.7.2 Configuration and Recommendation

APC configuration is similar to ACS, which has been described in 5.1.2.

APC could be turned ON/OFF separately on 2.4GHz or 5GHz as below.





4.8 Load Balancing

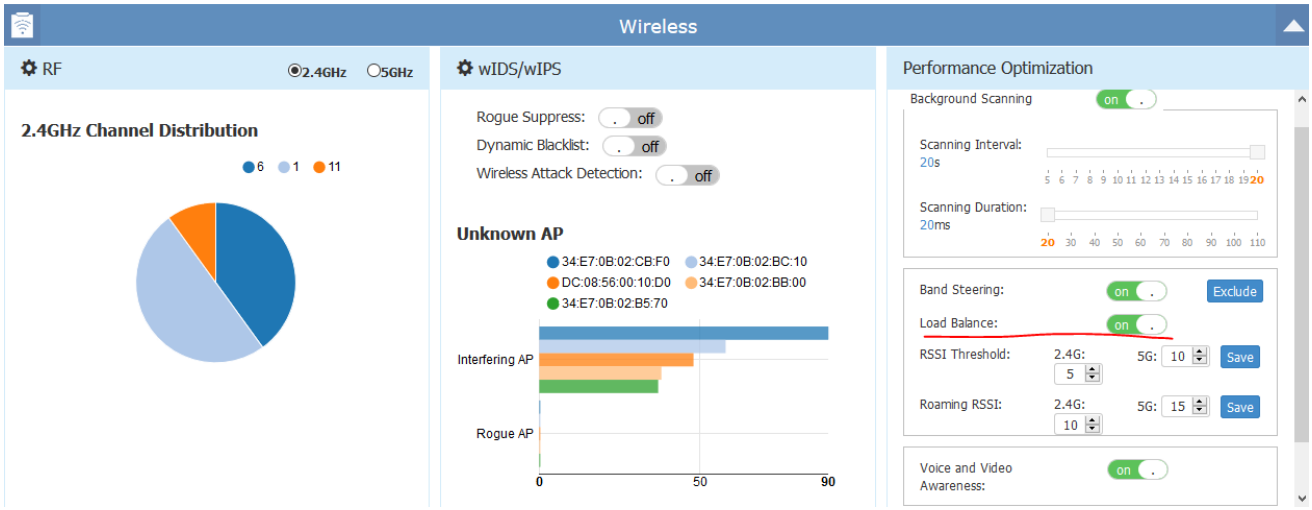
4.8.1 Feature description

Load balancing is used to make the wireless clients could be associated to the AP with good performance, by checking the number clients associated, and uplink RSSI info synchronized between the neighbor APs.

It’ s balancing the clients working on the same radio band.

4.8.2 Configuration and Recommendation

The “load balancing” could be activated from “**WEB UI** -> **Wireless**” page as below:



4.9 Band Steering

4.9.1 Feature description

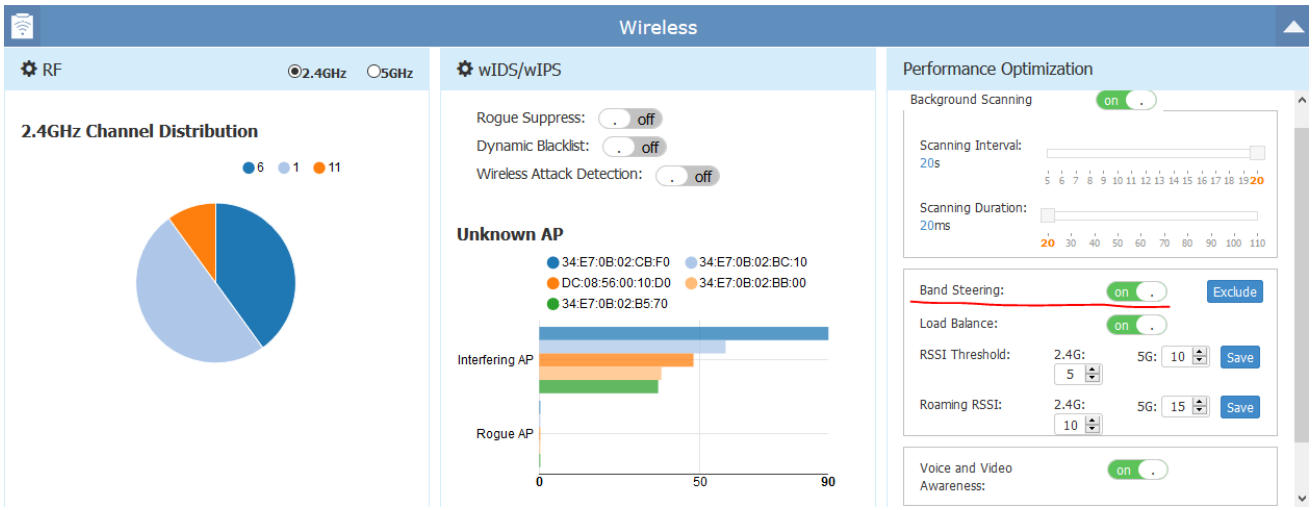
Dual-band devices could be associated with the AP either in 2.4GHz or 5GHz. “Band Steering” feature is able to help this kind of devices to be associated on a better radio band, which is based on:

- RSSI in 5GHz radio.
- RF utilization of the channel of each radio band.
- Number of stations on the radio
- The difference of the stations on the two radio bands.

The band steering feature is handled during “Pre-association” phase.

4.9.2 Configuration and Recommendation

The "load balancing" could be activated from "**WEB UI** -> **Wireless**" page as below:



4.10 Background scanning

4.10.1 Feature description

4.10.2 Configuration and Recommendation

4.11 Voice over WLAN

4.11.1 Feature description

4.11.2 Configuration and Recommendation

4.12 <More features to be introduced>

.....

.....

.....

.....

5 Useful CLI Commands

5.1 System information

✓ ***Free*** ***// To check the memory usage.***

Example:

```
support@AP-C7:20:~$
support@AP-C7:20:~$ free
             total         used         free       shared      buffers
Mem:        245560       143608       101952            0        11420
-/+ buffers:             132188       113372
Swap:            0            0            0
support@AP-C7:20:~$
```

✓ ***Showsysinfo*** ***// To check the AP hardware information.***

Example:

```
support@AP-C7:20:~$
support@AP-C7:20:~$ showsysinfo
    Company Name:ALE USA Inc.
              SN:SSZ170300020
    Device Model:OAW-AP1221
             MAC:34:E7:0B:03:C7:20
         Country:RW
   Software Name:AOS-WNG
Software Version:3.0.0
Hardware Version:1.10
     Part Number:903921-90
        Revision:
    Essid Prefix:mywifi
Cluster Describe:AP Group
         Website:http://www.al-enterprise.com
           Legal:Copyright 1995-2016 ALE USA Inc.   ALL RIGHTS RESERVED WORLDWIDE
        Describe:
support@AP-C7:20:~$
```

✓ ***ps |grep <process>*** ***// To check the status of the related software process.***

Example:

```
support@AP-C7:20:~$ ps |grep cluster
13157 root      5532 S    /sbin/cluster_mgt -I 666 -p ff:ff:ff:ff:ff:ff
13158 root      3144 S    /sbin/cluster_cor -I 666 -p ff:ff:ff:ff:ff:ff
20756 support   1344 S    grep cluster
support@AP-C7:20:~$
support@AP-C7:20:~$
support@AP-C7:20:~$ ps |grep wam
 2846 root      2916 S    wam -g /var/run/wam/global -d -f /var/log/wam.log
22860 support   1344 R    grep wam
support@AP-C7:20:~$
```

✓ ***ps |grep D*** ***// To check if there's any software process in D (dead) state.***

Example:

```
support@AP-C7:20:~$ ps |grep D
  PID USER       VSZ STAT COMMAND
19314 root      4528 S    /usr/sbin/lighttpd -D -f /etc/lighttpd/lighttpd_https.conf
31185 support   1344 R    grep D
support@AP-C7:20:~$
```

- ✓ ***uptime*** ***// To check the AP run time***

Example:

```
support@AP-C7:20:~$ uptime
 21:13:00 up  2:24,  load average: 0.58, 0.39, 0.38
```

- ✓ ***date*** ***// To check AP system date and time***

Example:

```
support@AP-C7:20:~$ date
Wed Nov 22 21:18:17 2017
```

- ✓ ***ssudo passwd*** ***// To modify the password of "support" account***

Example:

```
support@AP-C7:20:~$
support@AP-C7:20:~$ ssudo passwd
Changing password for support
New password:
Bad password: too weak
Retype password:
Password for support changed by root
support@AP-C7:20:~$
support@AP-C7:20:~$
```

- ✓ ***showver*** ***// To check AP firmware version***

Example:

```
support@AP-C7:20:~$
support@AP-C7:20:~$ showver
3.0.0.63
support@AP-C7:20:~$
```

- ✓ ***reset_reason get*** ***// To check the recent reset reasons***

Example:

```
support@AP-78:00:~$ reset_reason get
[1] Fri Nov 17 18:32:32 2017 Update firmware
[1] Mon Nov 20 10:56:04 2017 Clear all configuration
[1] Tue May 30 00:02:39 2017 ZTP-reboot
[1] Tue May 30 00:00:12 2017 Power off reboot
[1] Tue May 30 00:00:12 2017 Power off reboot
[1] Tue May 30 00:00:12 2017 Power off reboot
[1] Mon Nov 20 07:54:43 2017 Restore all configuration
[1] Tue May 30 00:00:11 2017 Power off reboot
[1] Thu Nov 23 16:38:56 2017 Update firmware
[1] Thu Nov 23 18:06:32 2017 Restore all configuration
```

- ***ssudo firstboot // To clear all the settings and reset to factory.***

Example:

```
support@AP-36:D0:~$
support@AP-36:D0:~$ ssudo firstboot
This will erase all settings and remove any installed packages. Are you sure? [N/y]
y
/dev/mtdblock4 is mounted as /overlay, only erasing files
support@AP-36:D0:~$ ssudo reboot
support@AP-36:D0:~$
```

- ***ssudo reboot // To reboot the AP device***

Example:

```
support@AP-36:D0:~$ ssudo reboot
support@AP-36:D0:~$
```

- ***iwpriv wifi0 getCountry //To check the "Country Code" of the AP***

Example:

```
support@AP-78:00:~$
support@AP-78:00:~$ iwpriv wifi0 getCountry
wifi0     getCountry:CN
support@AP-78:00:~$
support@AP-78:00:~$ iwpriv wifi1 getCountry
wifi1     getCountry:CN
support@AP-78:00:~$
```

- ***cat /proc/kes_syslog // To check the system log and filter could be used for specific requests.***

Example:

```
support@AP-78:00:~$
support@AP-78:00:~$ cat /proc/kes_syslog
t txpower= 3]--[atp_control.c:558]
Mon Nov 27 15:32:29 2017 kern.warn kernel: [264341.910000] wmi_unified_vdev_stop_send for vap 0 (864f0000)
Mon Nov 27 15:32:29 2017 kern.warn kernel: [264341.910000] STOPPED EVENT for vap 0 (864f0000)
Mon Nov 27 15:32:29 2017 kern.warn kernel: [264341.950000] OL vap_start +
Mon Nov 27 15:32:29 2017 kern.warn kernel: [264341.950000] wmi_unified_vdev_start_send for vap 0 (864f0000)
Mon Nov 27 15:32:29 2017 kern.warn kernel: [264341.950000] OL vap_start -
Mon Nov 27 15:32:29 2017 daemon.notice [DRM-LOG]: [radio 2 ifname is NULL]--[atp_control.c:453]
Mon Nov 27 15:32:29 2017 kern.warn kernel: [264342.010000] ol_vdev_start_resp_ev for vap 0 (864f0000)
Mon Nov 27 15:32:29 2017 kern.warn kernel: [264342.010000] wmi_unified_vdev_up_send for vap 0 (864f0000)
Mon Nov 27 15:32:30 2017 kern.warn kernel: [264343.110000] [wifi1] FWLOG: [2252392] WAL_DBGID_TX_BA_SETUP ( 0x436980, 0x6, 0x19, 0x10040, 0x7cb0a507 )
Mon Nov 27 15:32:30 2017 kern.warn kernel: [264343.110000] [wifi1] FWLOG: [2252396] WAL_DBGID_TX_BA_SETUP ( 0x436980, 0x0, 0x2c4, 0x10040, 0x7cb0a507 )
Mon Nov 27 15:32:41 2017 user.notice core-mon: timer CORE_TIMER_CHECK_ONLINE_USR_ALIVE
Mon Nov 27 15:32:42 2017 user.notice core-mon: online user = [1], alive = [1]
Mon Nov 27 15:32:42 2017 user.notice core-mon: timer CORE_TIMER_CHECK_WAM
Mon Nov 27 15:32:42 2017 kern.warn kernel: [264355.110000] [wifi1] FWLOG: [2264667] WAL_DBGID_TX_BA_SETUP ( 0x436980, 0x0, 0x0, 0x2, 0x7cb0a507 )
Mon Nov 27 15:32:42 2017 kern.warn kernel: [264355.110000] [wifi1] FWLOG: [2264668] WAL_DBGID_TX_BA_SETUP ( 0x436980, 0x6, 0x0, 0x2, 0x7cb0a507 )
Mon Nov 27 15:32:46 2017 kern.warn kernel: [264359.110000] [wifi1] FWLOG: [2268809] WAL_DBGID_TX_BA_SETUP ( 0x436980, 0x0, 0x2c6, 0x10040, 0x7cb0a507 )
Mon Nov 27 15:32:52 2017 kern.warn kernel: [264365.110000] [wifi1] FWLOG: [2274907] WAL_DBGID_TX_BA_SETUP ( 0x436980, 0x0, 0x0, 0x2, 0x7cb0a507 )
Mon Nov 27 15:32:55 2017 kern.warn kernel: [264368.030000] Inst RSSI value of node-7c:b0:c2:bc:a5:07: 50
Mon Nov 27 15:32:55 2017 kern.warn kernel: [264368.030000] Inst RSSI value of node-7c:b0:c2:bc:a5:07: 50
Mon Nov 27 15:32:55 2017 kern.warn kernel: [264368.030000] Inst RSSI value of node-7c:b0:c2:bc:a5:07: 49
Mon Nov 27 15:32:55 2017 kern.warn kernel: [264368.030000] Inst RSSI value of node-7c:b0:c2:bc:a5:07: 50
Mon Nov 27 15:32:55 2017 kern.warn kernel: [264368.030000] Inst RSSI value of node-7c:b0:c2:bc:a5:07: 51
```

5.2 Wireless Management

✓ ***Iwconfig // To check the wireless configuration***

Example:

```
support@AP-78:00:~$ iwconfig
br-wan    no wireless extensions.

ifb0      no wireless extensions.

ath01     IEEE 802.11ng  ESSID:"test1"
          Mode:Master  Frequency:2.412 GHz  Access Point: DC:08:56:00:78:01
          Bit Rate:144.4 Mb/s   Tx-Power=20 dBm
          RTS thr:off   Fragment thr:off
          Power Management:off
          Link Quality=0/94  Signal level=-95 dBm  Noise level=-95 dBm
          Rx invalid nwid:2  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0

gre0      no wireless extensions.

wifi0     no wireless extensions.

lo        no wireless extensions.

gretap0   no wireless extensions.

teql0     no wireless extensions.

ath11-untag  no wireless extensions.

athscan1  IEEE 802.11ac  ESSID:"athscan1"
          Mode:Monitor  Frequency:5.18 GHz  Access Point: Not-Associated
          Bit Rate:866.7 Mb/s   Tx-Power=23 dBm
          RTS thr:off   Fragment thr:off
          Power Management:off
          Link Quality=0/94  Signal level=-95 dBm  Noise level=-95 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0

imq1      no wireless extensions.

ath01-untag  no wireless extensions.

ath11     IEEE 802.11ac  ESSID:"test1"
          Mode:Master  Frequency:5.18 GHz  Access Point: DC:08:56:00:78:09
          Bit Rate:866.7 Mb/s   Tx-Power=23 dBm
          RTS thr:off   Fragment thr:off
          Power Management:off
          Link Quality=87/94  Signal level=-62 dBm  Noise level=-95 dBm
          Rx invalid nwid:12  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0

athscan0  IEEE 802.11ng  ESSID:"athscan0"
          Mode:Master  Frequency:2.412 GHz  Access Point: DC:08:56:00:78:00
          Bit Rate:144.4 Mb/s   Tx-Power=20 dBm
          RTS thr:off   Fragment thr:off
          Power Management:off
          Link Quality=0/94  Signal level=-95 dBm  Noise level=-95 dBm
          Rx invalid nwid:2503  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0

eth0      no wireless extensions.

imq0      no wireless extensions.

ifb1      no wireless extensions.

wifi1     no wireless extensions.
```

✓ ***cat /etc/config/wireless // To check the wireless configuration***

Example:

```
support@AP-78:00:~$ cat /etc/config/wireless

config wifi-device 'wifi0'
        option type 'qcawifi'
        option channel 'auto'
        option txpower 'auto'
        option bcnburst '1'
        option hwmode '11ng'
        option disabled '0'
        option country 'CN'

config wifi-device 'wifi1'
        option type 'qcawifi'
        option channel 'auto'
        option txpower 'auto'
        option bcnburst '1'
        option hwmode '11ac'
        option disabled '0'
        option country 'CN'

config wifi-iface 'athscan1'
        option device 'wifi1'
        option mode 'ap'
        option ifname 'athscan1'
        option ssid 'athscan1'
        option hidden '1'
        option vif_monitor '1'
        option enable '0'

config wifi-iface 'athscan0'
        option device 'wifi0'
        option mode 'ap'
        option ifname 'athscan0'
        option ssid 'athscan0'
        option hidden '1'
        option vif_monitor '1'
        option athnewind '1'
        option enable '0'

config wifi-global 'global'

config wifi-iface '7465737431_2G_wifi0'
        option ssid 'test1'
        option device 'wifi0'
        option mode 'ap'
        option network 'wan'
        option network_type 'employee'
        option hidden '0'
        option enable '1'
        option maxsta '64'
        option probe_threshold '0'
        option encryption 'psk-mixed+tkip+aes'
        option key '3236e9e1c70a76b5199e60e53e9eaffe'
        option stream_limit_sw '1'

config wifi-iface '7465737431_5G_wifi1'
        option ssid 'test1'
        option device 'wifi1'
        option mode 'ap'
        option network 'wan'
        option network_type 'employee'
        option hidden '0'
        option enable '1'
        option maxsta '64'
        option probe_threshold '0'
        option encryption 'psk-mixed+tkip+aes'
        option key '3236e9e1c70a76b5199e60e53e9eaffe'
```

✓ ***cat /tmp/config/rfprofile.conf // To check the RF configuration***

Example:

```
support@AP-D1:40:~$ cat /tmp/config/rfprofile.conf
{
        "RFService":[
                {
                        "bandSteering":"enable",
                        "LoadBalance":"enable",
                        "backgroundScanning":"enable",
                        "countryCode":"SG",
                        "scanningInterval":20,
                        "scanningDuration":50,
                        "voiceVedioAwareness":"disable",
                        "airtimeFairnessAt2G":"disable",
                        "airtimeFairnessAt5G":"disable",
                        "perBandInfo":{
                                "2.4G":{
                                        "band":"enable",
                                        "channelSetting":"AUTO",
                                        "channelWidth":20,
                                        "powerSetting":"AUTO",
                                        "shortGuardInterval":"enable",
                                        "signalStrengthThreshold":0,
                                        "roamingSignalStrengthThreshold":0
                                },
                                "5G_high":{
                                        "band":"enable",
                                        "channelSetting":"AUTO",
                                        "channelWidth":80,
                                        "powerSetting":"AUTO",
                                        "shortGuardInterval":"enable",
                                        "signalStrengthThreshold":0,
                                        "roamingSignalStrengthThreshold":0
                                },
                                "5G_low":{
                                        "band":"enable",
                                        "channelSetting":"AUTO",
                                        "channelWidth":80,
                                        "powerSetting":"AUTO",
                                        "shortGuardInterval":"enable",
                                        "signalStrengthThreshold":0,
                                        "roamingSignalStrengthThreshold":0
                                },
                                "5G_all":{
                                        "band":"enable",
                                        "channelSetting":"AUTO",
                                        "channelWidth":80,
                                        "powerSetting":"AUTO",
                                        "shortGuardInterval":"enable",
                                        "signalStrengthThreshold":0,
                                        "roamingSignalStrengthThreshold":0
                                }
                        }
                }
        ]
}
support@AP-D1:40:~$
```

- ✓ ***iwlist ath01 channel // To check the cannel of ath01 interface. The same for other interfaces***

  Example:

```
support@AP-78:00:~$ iwlist ath01 channel
ath01     57 channels in total; available frequencies :
          Channel 01 : 2.412 GHz
          Channel 02 : 2.417 GHz
          Channel 03 : 2.422 GHz
          Channel 04 : 2.427 GHz
          Channel 05 : 2.432 GHz
          Channel 06 : 2.437 GHz
          Channel 07 : 2.442 GHz
          Channel 08 : 2.447 GHz
          Channel 09 : 2.452 GHz
          Channel 10 : 2.457 GHz
          Channel 11 : 2.462 GHz
          Channel 12 : 2.467 GHz
          Channel 13 : 2.472 GHz
          Current Frequency:2.437 GHz (Channel 6)
```

```
support@AP-78:00:~$ iwlist ath11 channel
ath11     75 channels in total; available frequencies :
          Channel 36 : 5.18 GHz
          Channel 40 : 5.2 GHz
          Channel 44 : 5.22 GHz
          Channel 48 : 5.24 GHz
          Channel 52 : 5.26 GHz
          Channel 56 : 5.28 GHz
          Channel 60 : 5.3 GHz
          Channel 64 : 5.32 GHz
          Channel 149 : 5.745 GHz
          Channel 153 : 5.765 GHz
          Channel 157 : 5.785 GHz
          Channel 161 : 5.805 GHz
          Channel 165 : 5.825 GHz
          Current Frequency:5.32 GHz (Channel 64)
```

- ✓ ***iwlist ath01 txpower // To check the txpower of ath01 interface. The same for other interfaces***

  Example:

```
support@AP-78:00:~$ iwlist ath01 txpower
ath01     6 available transmit-powers :
          0 dBm          (1 mw)
          3 dBm          (1 mw)
          3 dBm          (1 mw)
          3 dBm          (1 mw)
          3 dBm          (1 mw)
          3 dBm          (1 mw)
          Current Tx-Power=3 dBm        (1 mw)
```

```
support@AP-78:00:~$ iwlist ath11 txpower
ath11     6 available transmit-powers :
          0 dBm          (1 mw)
          3 dBm          (1 mw)
          3 dBm          (1 mw)
          3 dBm          (1 mw)
          3 dBm          (1 mw)
          3 dBm          (1 mw)
          Current Tx-Power=3 dBm        (1 mw)
```

- ✓ ***iwlist ath01 bitrate //To check the bit rate of ath01 interface. The same for other interfaces***

Example:

```
support@AP-78:00:~$
support@AP-78:00:~$ iwlist ath01 bitrate
ath01     12 available bit-rates :
          1 Mb/s
          2 Mb/s
          5.5 Mb/s
          11 Mb/s
          6 Mb/s
          9 Mb/s
          12 Mb/s
          18 Mb/s
          24 Mb/s
          36 Mb/s
          48 Mb/s
          54 Mb/s
          Current Bit Rate:144.4 Mb/s
```

```
support@AP-78:00:~$
support@AP-78:00:~$ iwlist ath11 bitrate
ath11     8 available bit-rates :
          6 Mb/s
          9 Mb/s
          12 Mb/s
          18 Mb/s
          24 Mb/s
          36 Mb/s
          48 Mb/s
          54 Mb/s
          Current Bit Rate:866.7 Mb/s
```

- ✓ ***iwpriv ath01 get_mode //To check the interface mode of ath01. The same for other interfaces***

Example:

```
support@AP-78:00:~$ iwpriv ath01 get_mode
ath01     get_mode:11NGHT20
support@AP-78:00:~$
```

```
support@AP-78:00:~$
support@AP-78:00:~$ iwpriv ath11 get_mode
ath11     get_mode:11ACVHT80
support@AP-78:00:~$
```

- ✓ ***iwpriv wifi0 get_txchainmask or iwpriv wifi1 get_txchainmask //To check the spatial streams quantity supported by the Steller AP***

Example:

```
support@AP-28:C0:~$
support@AP-28:C0:~$ iwpriv wifi0 get_txchainmask
wifi0     get_txchainmask:3
support@AP-28:C0:~$
support@AP-28:C0:~$ iwpriv wifi1 get_txchainmask
wifi1     get_txchainmask:3
support@AP-28:C0:~$
```

- ✓ ***telnet 127.0.0.1:7787 then stadb and s //To check*** the clients supported band currently detected by the AP

Example:

```
support@AP-28:C0:~$ telnet 127.0.0.1:7787
Use `h' and `help' for help messages
Use `dbg here' to see log messages; other dbg cmds for log level
@ stadb
@stadb s
Num entries = 119

MAC Address               Age       Bands     Assoc? (age)                          Active? (age)       Flags
54:9F:13:45:B6:29         31        5         APId 255 ChanId 165 ESSId 0   (3807)  no  (12)            BTM RRM PS  Steer Allowed
@stadb support@AP-28:C0:~$

support@AP-28:C0:~$ telnet 127.0.0.1:7787
Use `h' and `help' for help messages
Use `dbg here' to see log messages; other dbg cmds for log level
@
@ stadb
@stadb s
Num entries = 116

MAC Address               Age       Bands     Assoc? (age)                          Active? (age)       Flags
54:9F:13:45:B6:29         1553      25              (5616)                                              BTM RRM PS  Steer Allowed
@stadb
@stadb support@AP-28:C0:~$
```

Press ctrl+d to exit

- ✓ ***cat /proc/kes_syslog |grep DRM //To check the logs of ACS and APC management***

  Example:

```
support@AP-78:00:~$
support@AP-78:00:~$ cat /proc/kes_syslog |grep DRM
Mon Nov 27 15:27:29 2017 daemon.notice [DRM-LOG]: [base ip=192.168.92.36, max priority neighbor_ip=88.1.1.10]--[atp_control.c:372]
Mon Nov 27 15:27:29 2017 daemon.notice [DRM-LOG]: [wifi0 current channel = 11, current_txpower = 3, min_txpower=3, max_txpower=20;max_rssi neighbor:ip 192.168.92.40, txpower 3, rssi 55, channel 11;other info:dist = 3, best txpower= 3]--
[atp_control.c:558]
Mon Nov 27 15:27:29 2017 daemon.notice [DRM-LOG]: [base ip=192.168.92.36, max priority neighbor_ip=88.1.1.11]--[atp_control.c:372]
Mon Nov 27 15:27:29 2017 daemon.notice [DRM-LOG]: [wifi1 current channel = 165, current_txpower = 5, min_txpower=3, max_txpower=23;max_rssi neighbor:ip 192.168.92.46, txpower 3, rssi 61, channel 165;other info:dist = 3, best txpower= 3]
--[atp_control.c:558]
Mon Nov 27 15:27:29 2017 daemon.notice [DRM-LOG]: [radio 2 ifname is NULL]--[atp_control.c:453]
Mon Nov 27 15:27:59 2017 daemon.notice [DRM-LOG]: [base ip=192.168.92.36, max priority neighbor_ip=88.1.1.10]--[atp_control.c:372]
Mon Nov 27 15:27:59 2017 daemon.notice [DRM-LOG]: [wifi0 current channel = 11, current_txpower = 3, min_txpower=3, max_txpower=20;max_rssi neighbor:ip 192.168.92.48, txpower 3, rssi 55, channel 11;other info:dist = 3, best txpower= 3]--
[atp_control.c:558]
Mon Nov 27 15:27:59 2017 daemon.notice [DRM-LOG]: [base ip=192.168.92.36, max priority neighbor_ip=88.1.1.17]--[atp_control.c:372]
Mon Nov 27 15:27:59 2017 daemon.notice [DRM-LOG]: [wifi1 current channel = 165, current_txpower = 5, min_txpower=3, max_txpower=23;max_rssi neighbor:ip 192.168.92.46, txpower 3, rssi 62, channel 165;other info:dist = 3, best txpower= 3]
--[atp_control.c:558]
Mon Nov 27 15:27:59 2017 daemon.notice [DRM-LOG]: [radio 2 ifname is NULL]--[atp_control.c:453]
Mon Nov 27 15:28:29 2017 daemon.notice [DRM-LOG]: [base ip=192.168.92.36, max priority neighbor_ip=88.1.1.10]--[atp_control.c:372]
Mon Nov 27 15:28:29 2017 daemon.notice [DRM-LOG]: [wifi0 current channel = 11, current_txpower = 3, min_txpower=3, max_txpower=20;max_rssi neighbor:ip 192.168.92.48, txpower 3, rssi 54, channel 11;other info:dist = 3, best txpower= 3]--
[atp_control.c:558]
Mon Nov 27 15:28:29 2017 daemon.notice [DRM-LOG]: [base ip=192.168.92.36, max priority neighbor_ip=88.1.1.17]--[atp_control.c:372]
Mon Nov 27 15:28:29 2017 daemon.notice [DRM-LOG]: [wifi1 current channel = 165, current_txpower = 5, min_txpower=3, max_txpower=23;max_rssi neighbor:ip 192.168.92.46, txpower 3, rssi 62, channel 165;other info:dist = 3, best txpower= 3]
--[atp_control.c:558]
Mon Nov 27 15:28:29 2017 daemon.notice [DRM-LOG]: [radio 2 ifname is NULL]--[atp_control.c:453]
```

5.3 Client Management

- ✓ ***ssudo sta_list // To list all the clients associated with this AP***

  ssudo wam_debug sta_list

  Example:

```
support@AP-D0:A0:~$ ssudo sta_list
SSID:11JP
STA_MAC                IP              OnlineTime          RX          TX          FREQ    AUTH    Final_role                  VLANID  TUNNELID  FARENDIP
SSID:11JP
STA_MAC                IP              OnlineTime          RX          TX          FREQ    AUTH    Final_role                  VLANID  TUNNELID  FARENDIP
54:9f:13:45:b6:29    172.16.18.121         333           95373739    11982277    5GHz    OPEN    1544592109710arp            0       0
support@AP-D0:A0:~$
```

```
support@AP-28:C0:~$ ssudo wam_debug sta_list
{
        "status": "Success!!!",
        "wlanServiceData": [
                {
                        "iface": "ath01",
                        "ssid": "11Su-Ex",
                        "freq": "2.4GHz",
                        "security": "Open",
                        "wlanService": "1546845869291"
                },
                {
                        "iface": "ath11",
                        "ssid": "11Su-Ex",
                        "freq": "5GHz",
                        "security": "Open",
                        "wlanService": "1546845869291",
                        "staData": [
                                {
                                        "staMAC": "54:9f:13:45:b6:29",
                                        "staIP": "172.16.18.121",
                                        "associationTime": 362,
                                        "mappingType": 0,
                                        "assignedVLAN": 0,
                                        "assignedAR": "1546845869291arp",
                                        "assignedPL": "",
                                        "macAuthResult": "",
                                        "ARFromMACAuth": "",
                                        "PLFromMACAuth": "",
                                        "redirectURLFromMACAuth": "",
                                        "ARFrom8021xAuth": "",
                                        "PLFrom8021xAuth": "",
                                        "redirectURLFrom8021xAuth": "",
                                        "CPAuthResult": "FAILED",
                                        "ARFromCPAuth": "",
                                        "PLFromCPAuth": "",
                                        "ARFromRoaming": "",
                                        "PLFromRoaming": "",
                                        "redirectURLFromRoaming": "",
                                        "classificationMatched": "none"
                                }
                        ]
                }
```

- ✓ ***wlanconfig ath11 list // To list all clients on specific AP interface***

Example:

```
support@AP-78:00:~$
support@AP-78:00:~$ wlanconfig ath11 list
ADDR               AID CHAN TXRATE RXRATE RSSI MINRSSI MAXRSSI IDLE  TXSEQ  RXSEQ  CAPS        ACAPS     ERP    STATE MAXRATE(DOT11) HTCAPS ASSOCTIME    IEs   MODE PSMODE
54:9f:13:45:b6:29    1  149 433M    351M   47     35      54    0      0   65535   EP          0         b              0          AWQS 00:02:25 RSN WME IEEE80211_MODE_11AC_VHT80  1
7c:b0:c2:bc:a5:07    2  149 468M    585M   44     44      51    7      0   65535   EPs         0         b              0          AWPSM 00:01:39 RSN WME IEEE80211_MODE_11AC_VHT80  0
support@AP-78:00:~$
```

- ✓ ***cat /proc/kes_syslog |grep tid // To check the OS type of the clients on AP***

Example:

```
support@AP-78:00:~$ sta_list
SSID:test
STA_MAC              IP                  OnlineTime      RX       TX        FREQ    AUTH    Final_role                      VLANID
SSID:test
STA_MAC              IP                  OnlineTime      RX       TX        FREQ    AUTH    Final_role                      VLANID
54:9f:13:45:b6:29    192.168.92.30       859             4199469   70188539   5GHz    PSK    test_arp                        0
support@AP-78:00:~$
support@AP-78:00:~$
support@AP-78:00:~$
support@AP-78:00:~$ cat /proc/kes_syslog |grep tid
Fri Nov 24 17:21:06 2017 daemon.notice tid: [tid]: [TID_DHCP_PROTOCOL] ip:[], mac:[7c:b0:c2:bc:a5:07], hostname:[MS-20161013HMQJ], ostype:[]
Fri Nov 24 17:21:10 2017 daemon.notice tid: [tid]: [TID_DHCP_PROTOCOL] ip:[], mac:[7c:b0:c2:bc:a5:07], hostname:[MS-20161013HMQJ], ostype:[]
Fri Nov 24 17:21:10 2017 daemon.notice tid: [tid]: [TID_DHCP_PROTOCOL] ip:[], mac:[7c:b0:c2:bc:a5:07], hostname:[MS-20161013HMQJ], ostype:[]
Fri Nov 24 17:21:14 2017 daemon.notice tid: [tid]: [TID_DHCP_PROTOCOL] ip:[], mac:[7c:b0:c2:bc:a5:07], hostname:[MS-20161013HMQJ], ostype:[]
Fri Nov 24 17:21:14 2017 daemon.notice tid: [tid]: [TID_DHCP_PROTOCOL] ip:[], mac:[7c:b0:c2:bc:a5:07], hostname:[MS-20161013HMQJ], ostype:[]
Fri Nov 24 17:21:16 2017 daemon.notice tid: [tid]: [TID_NETBIOS_PROTOCOL] ip:[192.168.92.32], mac:[7c:b0:c2:bc:a5:07], hostname:[]
Fri Nov 24 17:21:16 2017 daemon.notice tid: [tid]: [TID_NETBIOS_PROTOCOL] ip:[192.168.92.32], mac:[7c:b0:c2:bc:a5:07], hostname:[]
Fri Nov 24 17:22:29 2017 daemon.notice tid: [tid]: [TID_DHCP_PROTOCOL] ip:[], mac:[7c:b0:c2:bc:a5:07], hostname:[MS-20161013HMQJ], ostype:[]
Fri Nov 24 17:22:29 2017 daemon.notice tid: [tid]: [TID_DHCP_PROTOCOL] ip:[], mac:[7c:b0:c2:bc:a5:07], hostname:[MS-20161013HMQJ], ostype:[]
Fri Nov 24 17:31:16 2017 daemon.notice tid: [tid]: [TID_HTTP_PROTOCOL] ip:[192.168.92.30], mac:[54:9f:13:45:b6:29], os type:[iOS]
Fri Nov 24 17:31:16 2017 daemon.notice tid: [tid]: [TID_HTTP_PROTOCOL] ip:[192.168.92.30], mac:[54:9f:13:45:b6:29], os type:[iOS]
support@AP-78:00:~$
```

- ✓ ***cat /proc/kes_syslog |grep "<MAC>" // To check the access logs of specific client***

Example:

```
support@AP-78:00:~$
support@AP-78:00:~$
support@AP-78:00:~$
support@AP-78:00:~$ cat /proc/kes_syslog |grep "54:9f:13:45:b6:29"
Fri Nov 24 17:20:21 2017 daemon.notice netifd: mvlan add user mac success: 54:9f:13:45:b6:29
Fri Nov 24 17:20:24 2017 daemon.warn um: [um]:um_user_update creat:1 mac: 54:9f:13:45:b6:29 ip:192.168.92.30
Fri Nov 24 17:21:11 2017 kern.warn kernel: [11667.300000] Inst RSSI value of node-54:9f:13:45:b6:29: 50
Fri Nov 24 17:21:11 2017 kern.warn kernel: [11667.300000] Inst RSSI value of node-54:9f:13:45:b6:29: 49
Fri Nov 24 17:21:11 2017 kern.warn kernel: [11667.300000] Inst RSSI value of node-54:9f:13:45:b6:29: 49
Fri Nov 24 17:21:11 2017 kern.warn kernel: [11667.300000] Inst RSSI value of node-54:9f:13:45:b6:29: 48
Fri Nov 24 17:21:11 2017 kern.warn kernel: [11667.300000] Inst RSSI value of node-54:9f:13:45:b6:29: 50
Fri Nov 24 17:21:35 2017 kern.warn kernel: [11691.260000] Inst RSSI value of node-54:9f:13:45:b6:29: 67
Fri Nov 24 17:21:35 2017 kern.warn kernel: [11691.260000] Inst RSSI value of node-54:9f:13:45:b6:29: 67
Fri Nov 24 17:21:35 2017 kern.warn kernel: [11691.270000] Inst RSSI value of node-54:9f:13:45:b6:29: 66
Fri Nov 24 17:21:35 2017 kern.warn kernel: [11691.270000] Inst RSSI value of node-54:9f:13:45:b6:29: 66
Fri Nov 24 17:21:35 2017 kern.warn kernel: [11691.270000] Inst RSSI value of node-54:9f:13:45:b6:29: 66
Fri Nov 24 17:27:56 2017 kern.warn kernel: [12071.790000] Inst RSSI value of node-54:9f:13:45:b6:29: 59
Fri Nov 24 17:27:56 2017 kern.warn kernel: [12071.790000] Inst RSSI value of node-54:9f:13:45:b6:29: 58
Fri Nov 24 17:27:56 2017 kern.warn kernel: [12071.790000] Inst RSSI value of node-54:9f:13:45:b6:29: 58
Fri Nov 24 17:27:56 2017 kern.warn kernel: [12071.790000] Inst RSSI value of node-54:9f:13:45:b6:29: 58
Fri Nov 24 17:27:56 2017 kern.warn kernel: [12071.790000] Inst RSSI value of node-54:9f:13:45:b6:29: 59
Fri Nov 24 17:28:51 2017 kern.warn kernel: [12127.090000] Inst RSSI value of node-54:9f:13:45:b6:29: 60
Fri Nov 24 17:28:51 2017 kern.warn kernel: [12127.090000] Inst RSSI value of node-54:9f:13:45:b6:29: 58
Fri Nov 24 17:28:51 2017 kern.warn kernel: [12127.090000] Inst RSSI value of node-54:9f:13:45:b6:29: 57
Fri Nov 24 17:28:51 2017 kern.warn kernel: [12127.090000] Inst RSSI value of node-54:9f:13:45:b6:29: 57
Fri Nov 24 17:28:51 2017 kern.warn kernel: [12127.090000] Inst RSSI value of node-54:9f:13:45:b6:29: 57
Fri Nov 24 17:30:10 2017 kern.warn kernel: [12206.350000] Inst RSSI value of node-54:9f:13:45:b6:29: 49
Fri Nov 24 17:30:10 2017 kern.warn kernel: [12206.350000] Inst RSSI value of node-54:9f:13:45:b6:29: 49
Fri Nov 24 17:30:10 2017 kern.warn kernel: [12206.350000] Inst RSSI value of node-54:9f:13:45:b6:29: 49
Fri Nov 24 17:30:10 2017 kern.warn kernel: [12206.350000] Inst RSSI value of node-54:9f:13:45:b6:29: 47
Fri Nov 24 17:30:10 2017 kern.warn kernel: [12206.350000] Inst RSSI value of node-54:9f:13:45:b6:29: 46
Fri Nov 24 17:31:16 2017 daemon.notice tid: [tid]: [TID_HTTP_PROTOCOL] ip:[192.168.92.30], mac:[54:9f:13:45:b6:29], os type:[iOS]
Fri Nov 24 17:31:16 2017 daemon.notice tid: [tid]: [TID_HTTP_PROTOCOL] ip:[192.168.92.30], mac:[54:9f:13:45:b6:29], os type:[iOS]
Fri Nov 24 17:31:45 2017 kern.warn kernel: [12300.660000] Inst RSSI value of node-54:9f:13:45:b6:29: 55
Fri Nov 24 17:31:45 2017 kern.warn kernel: [12300.660000] Inst RSSI value of node-54:9f:13:45:b6:29: 54
Fri Nov 24 17:31:45 2017 kern.warn kernel: [12300.660000] Inst RSSI value of node-54:9f:13:45:b6:29: 54
Fri Nov 24 17:31:45 2017 kern.warn kernel: [12300.660000] Inst RSSI value of node-54:9f:13:45:b6:29: 54
Fri Nov 24 17:31:45 2017 kern.warn kernel: [12300.660000] Inst RSSI value of node-54:9f:13:45:b6:29: 54
Fri Nov 24 17:32:01 2017 kern.warn kernel: [12317.040000] Inst RSSI value of node-54:9f:13:45:b6:29: 53
Fri Nov 24 17:32:01 2017 kern.warn kernel: [12317.040000] Inst RSSI value of node-54:9f:13:45:b6:29: 56
Fri Nov 24 17:32:01 2017 kern.warn kernel: [12317.040000] Inst RSSI value of node-54:9f:13:45:b6:29: 53
Fri Nov 24 17:32:01 2017 kern.warn kernel: [12317.040000] Inst RSSI value of node-54:9f:13:45:b6:29: 54
Fri Nov 24 17:32:01 2017 kern.warn kernel: [12317.040000] Inst RSSI value of node-54:9f:13:45:b6:29: 53
Fri Nov 24 17:32:36 2017 kern.warn kernel: [12351.860000] Inst RSSI value of node-54:9f:13:45:b6:29: 54
Fri Nov 24 17:32:36 2017 kern.warn kernel: [12351.860000] Inst RSSI value of node-54:9f:13:45:b6:29: 55
Fri Nov 24 17:32:36 2017 kern.warn kernel: [12351.860000] Inst RSSI value of node-54:9f:13:45:b6:29: 55
Fri Nov 24 17:32:36 2017 kern.warn kernel: [12351.860000] Inst RSSI value of node-54:9f:13:45:b6:29: 54
Fri Nov 24 17:32:36 2017 kern.warn kernel: [12351.860000] Inst RSSI value of node-54:9f:13:45:b6:29: 54
Fri Nov 24 17:32:56 2017 kern.warn kernel: [12372.340000] Inst RSSI value of node-54:9f:13:45:b6:29: 54
Fri Nov 24 17:32:56 2017 kern.warn kernel: [12372.340000] Inst RSSI value of node-54:9f:13:45:b6:29: 55
Fri Nov 24 17:32:56 2017 kern.warn kernel: [12372.340000] Inst RSSI value of node-54:9f:13:45:b6:29: 53
Fri Nov 24 17:32:56 2017 kern.warn kernel: [12372.340000] Inst RSSI value of node-54:9f:13:45:b6:29: 55
Fri Nov 24 17:32:56 2017 kern.warn kernel: [12372.340000] Inst RSSI value of node-54:9f:13:45:b6:29: 55
Fri Nov 24 17:32:56 2017 kern.warn kernel: [12372.340000] Inst RSSI value of node-54:9f:13:45:b6:29: 55
Fri Nov 24 17:33:56 2017 kern.warn kernel: [12431.730000] Inst RSSI value of node-54:9f:13:45:b6:29: 53
Fri Nov 24 17:33:56 2017 kern.warn kernel: [12431.730000] Inst RSSI value of node-54:9f:13:45:b6:29: 53
Fri Nov 24 17:33:56 2017 kern.warn kernel: [12431.730000] Inst RSSI value of node-54:9f:13:45:b6:29: 53
Fri Nov 24 17:33:56 2017 kern.warn kernel: [12431.730000] Inst RSSI value of node-54:9f:13:45:b6:29: 52
Fri Nov 24 17:33:56 2017 kern.warn kernel: [12431.730000] Inst RSSI value of node-54:9f:13:45:b6:29: 53
Fri Nov 24 17:34:43 2017 kern.warn kernel: [12478.430000] Inst RSSI value of node-54:9f:13:45:b6:29: 54
Fri Nov 24 17:34:43 2017 kern.warn kernel: [12478.430000] Inst RSSI value of node-54:9f:13:45:b6:29: 54
Fri Nov 24 17:34:43 2017 kern.warn kernel: [12478.430000] Inst RSSI value of node-54:9f:13:45:b6:29: 54
Fri Nov 24 17:34:43 2017 kern.warn kernel: [12478.430000] Inst RSSI value of node-54:9f:13:45:b6:29: 54
Fri Nov 24 17:34:43 2017 kern.warn kernel: [12478.430000] Inst RSSI value of node-54:9f:13:45:b6:29: 53
Fri Nov 24 17:35:19 2017 daemon.notice netifd: mvlan remove user mac success: 54:9f:13:45:b6:29
Fri Nov 24 17:43:14 2017 daemon.notice netifd: mvlan add user mac success: 54:9f:13:45:b6:29
Fri Nov 24 17:43:16 2017 daemon.warn um: [um]: ip is not find for 54:9f:13:45:b6:29 in arp
Fri Nov 24 17:43:16 2017 daemon.warn um: [um]:um_user_update creat:1 mac: 54:9f:13:45:b6:29 ip:0.0.0.0
Fri Nov 24 17:43:16 2017 daemon.notice tid: [tid]: [TID_DHCP_PROTOCOL] ip:[], mac:[54:9f:13:45:b6:29], hostname:[AdminsdeiPhone], ostype:[iOS]
Fri Nov 24 17:43:16 2017 daemon.notice tid: [tid]: [TID_DHCP_PROTOCOL] ip:[], mac:[54:9f:13:45:b6:29], hostname:[AdminsdeiPhone], ostype:[iOS]
Fri Nov 24 17:43:16 2017 daemon.warn um: [um]: ip is not find for 54:9f:13:45:b6:29 in arp
Fri Nov 24 17:43:17 2017 daemon.warn um: [um]: ip is not find for 54:9f:13:45:b6:29 in arp
Fri Nov 24 17:43:17 2017 daemon.notice tid: [tid]: [TID_DHCP_PROTOCOL] ip:[], mac:[54:9f:13:45:b6:29], hostname:[AdminsdeiPhone], ostype:[iOS]
Fri Nov 24 17:43:17 2017 daemon.notice tid: [tid]: [TID_DHCP_PROTOCOL] ip:[], mac:[54:9f:13:45:b6:29], hostname:[AdminsdeiPhone], ostype:[iOS]
support@AP-78:00:~$
```

5.4 Captive Portal Management

- ✓ ***ps |grep eag // To check if the thread of "eag" is running well.***

  Example:

```
support@AP-78:00:~$
support@AP-78:00:~$ ps |grep eag
 2307 root     10152 S    /usr/sbin/eag_app -c
12087 support   1520 S    grep eag
support@AP-78:00:~$
```

- ✓ ***eag_cli show user all/list // To list the clients authenticated by captive portal***

  Example:

```
support@AP-78:00:~$
support@AP-78:00:~$ eag_cli show user list
user num : 2
ID      UserName        UserIP          UserMAC             SessionTime  OutputFlow      InputFlow       AuthType        ESSID
1       zheng           192.168.92.30   54:9F:13:45:B6:29   0:10:58      32960           133066          PORTAL      test-portal
2       zheng           192.168.92.32   7C:B0:C2:BC:A5:07   0:00:33      520922          1281951         PORTAL      test-portal
support@AP-78:00:~$
support@AP-78:00:~$
support@AP-78:00:~$
support@AP-78:00:~$ eag_cli show user all
user num : 2
ID      UserName        UserIP          UserMAC             SessionTime  OutputFlow      InputFlow       AuthType        ESSID
1       zheng           192.168.92.30   54:9F:13:45:B6:29   0:11:13      32960           133066          PORTAL      test-portal
2       zheng           192.168.92.32   7C:B0:C2:BC:A5:07   0:00:48      659998          1533077         PORTAL      test-portal
support@AP-78:00:~$
```

- ***eag_cli kick user index 1 // To delete a user from Portal authenticated user list.***

Example:

```
support@AP-78:00:~$ eag_cli show user all
user num : 2
ID      UserName          UserIP          UserMAC           SessionTime  OutputFlow      InputFlow       AuthType        ESSID
1       zheng             192.168.92.30   54:9F:13:45:B6:29 0:11:13      32960           133066          PORTAL      test-portal
2       zheng             192.168.92.32   7C:B0:C2:BC:A5:07 0:00:48      659998          1533077         PORTAL      test-portal
support@AP-78:00:~$
support@AP-78:00:~$
support@AP-78:00:~$
support@AP-78:00:~$ eag_cli kick user index 1
the command sucsessful
support@AP-78:00:~$ eag_cli show user list
user num : 1
ID      UserName          UserIP          UserMAC           SessionTime  OutputFlow      InputFlow       AuthType        ESSID
1       zheng             192.168.92.32   7C:B0:C2:BC:A5:07 0:06:05      752317          1595914         PORTAL      test-portal
support@AP-78:00:~$


support@AP-78:00:~$
support@AP-78:00:~$ eag_cli show user list
user num : 2
ID      UserName          UserIP          UserMAC           SessionTime  OutputFlow      InputFlow       AuthType        ESSID
1       zheng             192.168.92.32   7C:B0:C2:BC:A5:07 0:12:27      830670          1608523         PORTAL      test-portal
2       zheng             192.168.92.30   54:9F:13:45:B6:29 0:02:07      34129           132819          PORTAL      test-portal
support@AP-78:00:~$ eag_cli kick user index 2
the command sucsessful
support@AP-78:00:~$
support@AP-78:00:~$ eag_cli show user list
user num : 1
ID      UserName          UserIP          UserMAC           SessionTime  OutputFlow      InputFlow       AuthType        ESSID
1       zheng             192.168.92.32   7C:B0:C2:BC:A5:07 0:12:47      831679          1608631         PORTAL      test-portal
support@AP-78:00:~$
```

- ***tail -f /tmp/log/eag.log***

cat /proc/kes_syslog |grep eag

cat /var/log/eag.log

// To check the related logs of push portal.

Example:

```
support@AP-78:00:~$ tail -f /tmp/log/eag.log
[2017-11-27 15:01:53]:  eag_stamsg.c:771:stamsg_recieve usermac 54:9F:13:45:B6:29,userip 192.168.92.30, OP: 1
[2017-11-27 15:01:53]:  eag_stamsg.c:424:Receive leave msg usermac:54:9F:13:45:B6:29, userip:192.168.92.30, status:NotAuthed, apmac:DC:08:56:00:78:00, apname:, ssid:test-portal, leave_reason:0
[2017-11-27 15:03:01]:  appconn.c:1863:appconn_check_flux userip=192.168.92.32, output_octets=865605, total_octets=2501165
[2017-11-27 15:04:21]:  appconn.c:1863:appconn_check_flux userip=192.168.92.32, output_octets=876811, total_octets=2512990
[2017-11-27 15:05:20]:  appconn.c:1863:appconn_check_flux userip=192.168.92.32, output_octets=892076, total_octets=2538925
[2017-11-27 15:06:20]:  appconn.c:1863:appconn_check_flux userip=192.168.92.32, output_octets=904008, total_octets=2555139
[2017-11-27 15:07:20]:  appconn.c:1863:appconn_check_flux userip=192.168.92.32, output_octets=913383, total_octets=2566678
[2017-11-27 15:08:20]:  appconn.c:1863:appconn_check_flux userip=192.168.92.32, output_octets=925434, total_octets=2579377
[2017-11-27 15:09:11]:  eag_ins.c:2347:eag_cli_cmd_kick_user_index index 2 > total 1
[2017-11-27 15:09:20]:  appconn.c:1863:appconn_check_flux userip=192.168.92.32, output_octets=938610, total_octets=2597656
[2017-11-27 15:09:55]:  eag_stamsg.c:771:stamsg_recieve usermac 54:9F:13:45:B6:29,userip 192.168.92.30, OP: 0
[2017-11-27 15:09:55]:  eag_ins.c:5840:get intf [br-wan]
[2017-11-27 15:09:55]:  eag_ins.c:5842:interface aready be used!
[2017-11-27 15:09:55]:  eag_stamsg.c:255:stamsg_proc, appconn not exist, usermac=54:9F:13:45:B6:29
[2017-11-27 15:09:55]:  appconn.c:1100:bridge : .intf : ath12
[2017-11-27 15:09:55]:  eag_ins.c:5664:ARP test-portal_arp vlanid = 0
[2017-11-27 15:09:55]:  eag_stamsg.c:303:bridge name br-wan ,len  6
[2017-11-27 15:09:55]:  eag_stamsg.c:307:ARP name test-portal_arp,len 15,intf ath12,bridge br-wan
[2017-11-27 15:09:55]:  eag_stamsg.c:374:Receive USER_ADD msg  status:NotAuthed, apmac: DC:08:56:00:78:00,usermac:54:9F:13:45:B6:29,userip 192.168.92.30, wlan service name:test-portal, ssid:test-portal ,ARP name: test-portal_arp, redire
ct URL:
[2017-11-27 15:09:57]:  appconn.c:841:eag_ipinfo_get before userip=192.168.92.30
[2017-11-27 15:09:57]:  appconn.c:845:eag_ipinfo_get after userip=192.168.92.30,usermac=54:9F:13:45:B6:29,interface=br-wan
[2017-11-27 15:09:57]:  appconn.c:848:appconn_check_is_conflict eag_ipinfo_get userip 192.168.92.30, interface(br-wan), usermac(54:9F:13:45:B6:29)
[2017-11-27 15:09:57]:  eag_redir.c:2221:ARP name test-portal_arp,intf ath12,bridge br-wan
[2017-11-27 15:09:57]:  eag_redir.c:1479:PortalRedirect___userIP:192.168.92.30,usrMAC:54-9F-13-45-B6-29,APMAC:DC-08-56-00-78-00,SSID:test-portal,NasIP:192.168.92.36,Interface:ath12,NasID:,redirURL:http://192.168.92.36:8080/internal_por
tal/portal_account_login.html?wlanuserip=192.168.92.30&usermac=54:9F:13:45:B6:29&wlanuserfirsturl=https://www.baidu.com
[2017-11-27 15:10:08]:  appconn.c:841:eag_ipinfo_get before userip=192.168.92.30
[2017-11-27 15:10:08]:  appconn.c:845:eag_ipinfo_get after userip=192.168.92.30,usermac=54:9F:13:45:B6:29,interface=br-wan
[2017-11-27 15:10:08]:  appconn.c:848:appconn_check_is_conflict eag_ipinfo_get userip 192.168.92.30, interface(br-wan), usermac(54:9F:13:45:B6:29)
[2017-11-27 15:10:08]:  eag_redir.c:2221:ARP name test-portal_arp,intf ath12,bridge br-wan
[2017-11-27 15:10:08]:  eag_redir.c:1479:PortalRedirect___userIP:192.168.92.30,usrMAC:54-9F-13-45-B6-29,APMAC:DC-08-56-00-78-00,SSID:test-portal,NasIP:192.168.92.36,Interface:ath12,NasID:,redirURL:http://192.168.92.36:8080/internal_por
tal/portal_account_login.html?wlanuserip=192.168.92.30&usermac=54:9F:13:45:B6:29&wlanuserfirsturl=https://www.baidu.com
[2017-11-27 15:10:15]:  appconn.c:841:eag_ipinfo_get before userip=192.168.92.30
[2017-11-27 15:10:15]:  appconn.c:845:eag_ipinfo_get after userip=192.168.92.30,usermac=54:9F:13:45:B6:29,interface=br-wan
[2017-11-27 15:10:15]:  appconn.c:848:appconn_check_is_conflict eag_ipinfo_get userip 192.168.92.30, interface(br-wan), usermac(54:9F:13:45:B6:29)
[2017-11-27 15:10:15]:  eag_redir.c:2221:ARP name test-portal_arp,intf ath12,bridge br-wan
[2017-11-27 15:10:15]:  eag_redir.c:1479:PortalRedirect___userIP:192.168.92.30,usrMAC:54-9F-13-45-B6-29,APMAC:DC-08-56-00-78-00,SSID:test-portal,NasIP:192.168.92.36,Interface:ath12,NasID:,redirURL:http://192.168.92.36:8080/internal_por
tal/portal_account_login.html?wlanuserip=192.168.92.30&usermac=54:9F:13:45:B6:29&wlanuserfirsturl=https://www.baidu.com
[2017-11-27 15:10:32]:  eag_stamsg.c:771:stamsg_recieve usermac 54:9F:13:45:B6:29,userip 192.168.92.30, OP: 1
[2017-11-27 15:10:32]:  eag_stamsg.c:424:Receive leave msg usermac:54:9F:13:45:B6:29, userip:192.168.92.30, status:NotAuthed, apmac:DC:08:56:00:78:00, apname:, ssid:test-portal, leave_reason:0
[2017-11-27 15:10:34]:  eag_stamsg.c:771:stamsg_recieve usermac 54:9F:13:45:B6:29,userip 192.168.92.30, OP: 0
[2017-11-27 15:10:34]:  eag_ins.c:5840:get intf [br-wan]
[2017-11-27 15:10:34]:  eag_ins.c:5842:interface aready be used!
[2017-11-27 15:10:34]:  eag_stamsg.c:255:stamsg_proc, appconn not exist, usermac=54:9F:13:45:B6:29
[2017-11-27 15:10:34]:  appconn.c:1100:bridge : .intf : ath11
[2017-11-27 15:10:34]:  eag_ins.c:5664:ARP test_arp vlanid = 0
[2017-11-27 15:10:34]:  eag_stamsg.c:303:bridge name br-wan ,len  6
[2017-11-27 15:10:34]:  eag_stamsg.c:307:ARP name test_arp,len 8,intf ath11,bridge br-wan
[2017-11-27 15:10:34]:  eag_stamsg.c:330:The ARP test_arp redirectStatus is disable
[2017-11-27 15:10:34]:  eag_stamsg.c:374:Receive USER_ADD msg  status:Authed, apmac: DC:08:56:00:78:00,usermac:54:9F:13:45:B6:29,userip 192.168.92.30, wlan service name:test, ssid:test ,ARP name: test_arp, redirect URL:
^C
support@AP-78:00:~$
```

```
support@AP-78:00:~$ cat /proc/kes_syslog |grep eag
Mon Nov 27 10:29:53 2017 user.notice core-mon: eag - pid [2307]
Mon Nov 27 10:29:53 2017 user.notice core-mon: eag - process state [S]
Mon Nov 27 10:34:53 2017 user.notice core-mon: eag - pid [2307]
Mon Nov 27 10:34:53 2017 user.notice core-mon: eag - process state [S]
Mon Nov 27 10:39:54 2017 user.notice core-mon: eag - pid [2307]
Mon Nov 27 10:39:54 2017 user.notice core-mon: eag - process state [S]
Mon Nov 27 10:44:54 2017 user.notice core-mon: eag - pid [2307]
Mon Nov 27 10:44:54 2017 user.notice core-mon: eag - process state [S]
Mon Nov 27 10:49:56 2017 user.notice core-mon: eag - pid [2307]
Mon Nov 27 10:49:56 2017 user.notice core-mon: eag - process state [S]
```

```
Mon Nov 27 14:25:18 2017 user.notice core-mon: eag - process state [5]
Mon Nov 27 14:30:19 2017 user.notice core-mon: eag - pid [2307]
Mon Nov 27 14:30:19 2017 user.notice core-mon: eag - process state [5]
Mon Nov 27 14:35:20 2017 user.notice core-mon: eag - pid [2307]
Mon Nov 27 14:35:21 2017 user.notice core-mon: eag - process state [0]
Mon Nov 27 14:35:50 2017 user.notice web: eag_uci add "test-portal" result:success
Mon Nov 27 14:35:54 2017 daemon.err eag: eag_ins.c:7985: json_object_object_get hostName2 no exist
Mon Nov 27 14:35:54 2017 daemon.err eag: eag_ins.c:8008: json_object_object_get ipAddress2 no exist
Mon Nov 27 14:35:54 2017 daemon.err eag: eag_ins.c:7985: json_object_object_get hostName2 no exist
Mon Nov 27 14:35:54 2017 daemon.err eag: eag_ins.c:8008: json_object_object_get ipAddress2 no exist
Mon Nov 27 14:36:57 2017 daemon.notice eag: username:zheng usermac:54-9F-13-45-B6-29 userip:192.168.92.30 ssid:test-portal time:14:36:57 portal_online
Mon Nov 27 14:40:22 2017 user.notice core-mon: eag - pid [2307]
Mon Nov 27 14:40:22 2017 user.notice core-mon: eag - process state [5]
Mon Nov 27 14:45:22 2017 user.notice core-mon: eag - pid [2307]
Mon Nov 27 14:45:22 2017 user.notice core-mon: eag - process state [5]
Mon Nov 27 14:47:22 2017 daemon.notice eag: username:zheng usermac:7C-B0-C2-BC-A5-07 userip:192.168.92.32 ssid:test-portal time:14:47:22 portal_online
Mon Nov 27 14:50:23 2017 user.notice core-mon: eag - pid [2307]
Mon Nov 27 14:50:23 2017 user.notice core-mon: eag - process state [5]
Mon Nov 27 14:53:15 2017 daemon.notice eag: username:zheng usermac:54-9F-13-45-B6-29 userip:192.168.92.30 ssid:test-portal time:14:53:15 portal_offline
Mon Nov 27 14:55:23 2017 user.notice core-mon: eag - pid [2307]
Mon Nov 27 14:55:23 2017 user.notice core-mon: eag - process state [5]
Mon Nov 27 14:57:42 2017 daemon.notice eag: username:zheng usermac:54-9F-13-45-B6-29 userip:192.168.92.30 ssid:test-portal time:14:57:42 portal_online
Mon Nov 27 15:00:03 2017 daemon.notice eag: username:zheng usermac:54-9F-13-45-B6-29 userip:192.168.92.30 ssid:test-portal time:15:00:03 portal_offline
Mon Nov 27 15:00:24 2017 user.notice core-mon: eag - pid [2307]
Mon Nov 27 15:00:24 2017 user.notice core-mon: eag - process state [5]
Mon Nov 27 15:05:24 2017 user.notice core-mon: eag - pid [2307]
Mon Nov 27 15:05:24 2017 user.notice core-mon: eag - process state [5]
Mon Nov 27 15:10:25 2017 user.notice core-mon: eag - pid [2307]
Mon Nov 27 15:10:25 2017 user.notice core-mon: eag - process state [5]
support@AP-78:00:~$
```

```
support@AP-78:00:~$ cat /var/log/eag.log

[2017-11-27 14:36:16]:  appconn.c:1863:appconn_check_flux userip=192.168.92.30, output_octets=3581, total_octets=31969
[2017-11-27 14:36:27]:  eag_stamsg.c:771:stamsg_recieve usermac 54:9F:13:45:B6:29,userip 192.168.92.30, OP: 1
[2017-11-27 14:36:27]:  eag_stamsg.c:424:Receive leave msg usermac:54:9f:13:45:b6:29, userip:192.168.92.30, status:Authed, apmac:DC:08:56:00:78:00, apname:, ssid:test, leave_reason:0
[2017-11-27 14:36:30]:  eag_stamsg.c:771:stamsg_recieve usermac 54:9F:13:45:B6:29,userip 192.168.92.30, OP: 0
[2017-11-27 14:36:30]:  eag_ins.c:5840:get intf [br-wan]
[2017-11-27 14:36:30]:  eag_ins.c:5842:interface aready be used!
[2017-11-27 14:36:30]:  eag_stamsg.c:255:stamsg_proc, appconn not exist, usermac=54:9F:13:45:B6:29
[2017-11-27 14:36:30]:  appconn.c:1100:bridge : ,intf : ath12
[2017-11-27 14:36:30]:  eag_ins.c:5664:ARP test-portal_arp vlanid = 0
[2017-11-27 14:36:30]:  eag_stamsg.c:303:bridge name br-wan ,len  6
[2017-11-27 14:36:30]:  eag_stamsg.c:307:ARP name test-portal_arp,len 15,intf ath12,bridge br-wan
[2017-11-27 14:36:30]:  eag_stamsg.c:374:Receive USER_ADD msg  status:NotAuthed, apmac: DC:08:56:00:78:00,usermac:54:9F:13:45:B6:29,userip 192.168.92.30, wlan service name:test-portal, ssid:test-portal ,ARP name: test-portal_arp, redire
ct URL:
[2017-11-27 14:36:32]:  appconn.c:841:eag_ipinfo_get before userip=192.168.92.30
[2017-11-27 14:36:32]:  appconn.c:845:eag_ipinfo_get after userip=192.168.92.30,usermac=54:9F:13:45:B6:29,interface=br-wan
[2017-11-27 14:36:32]:  appconn.c:848:appconn_check_is_conflict eag_ipinfo_get userip 192.168.92.30, interface(br-wan), usermac(54:9F:13:45:B6:29)
[2017-11-27 14:36:32]:  eag_redir.c:2221:ARP name test-portal_arp,intf ath12,bridge br-wan
[2017-11-27 14:36:32]:  eag_redir.c:1479:PortalRedirect___userIP:192.168.92.30,usrMAC:54-9F-13-45-B6-29,ApMAC:DC-08-56-00-78-00,SSID:test-portal,NasIP:192.168.92.36,Interface:ath12,NasID:,redirURL:http://192.168.92.36:8080/internal_por
tal/portal_account_login.html?wlanuserip=192.168.92.30&usermac=54:9F:13:45:B6:29&wlanuserfirsturl=https://www.baidu.com
[2017-11-27 14:36:38]:  appconn.c:841:eag_ipinfo_get before userip=192.168.92.30
[2017-11-27 14:36:38]:  appconn.c:845:eag_ipinfo_get after userip=192.168.92.30,usermac=54:9F:13:45:B6:29,interface=br-wan
[2017-11-27 14:36:38]:  appconn.c:848:appconn_check_is_conflict eag_ipinfo_get userip 192.168.92.30, interface(br-wan), usermac(54:9F:13:45:B6:29)
[2017-11-27 14:36:38]:  eag_redir.c:2221:ARP name test-portal_arp,intf ath12,bridge br-wan
[2017-11-27 14:36:38]:  eag_redir.c:1479:PortalRedirect___userIP:192.168.92.30,usrMAC:54-9F-13-45-B6-29,ApMAC:DC-08-56-00-78-00,SSID:test-portal,NasIP:192.168.92.36,Interface:ath12,NasID:,redirURL:http://192.168.92.36:8080/internal_por
tal/portal_account_login.html?wlanuserip=192.168.92.30&usermac=54:9F:13:45:B6:29&wlanuserfirsturl=https://www.baidu.com
[2017-11-27 14:36:43]:  appconn.c:841:eag_ipinfo_get before userip=192.168.92.30
[2017-11-27 14:36:43]:  appconn.c:845:eag_ipinfo_get after userip=192.168.92.30,usermac=54:9F:13:45:B6:29,interface=br-wan
[2017-11-27 14:36:43]:  appconn.c:848:appconn_check_is_conflict eag_ipinfo_get userip 192.168.92.30, interface(br-wan), usermac(54:9F:13:45:B6:29)
[2017-11-27 14:36:43]:  eag_redir.c:2221:ARP name test-portal_arp,intf ath12,bridge br-wan
[2017-11-27 14:36:43]:  eag_redir.c:1479:PortalRedirect___userIP:192.168.92.30,usrMAC:54-9F-13-45-B6-29,ApMAC:DC-08-56-00-78-00,SSID:test-portal,NasIP:192.168.92.36,Interface:ath12,NasID:,redirURL:http://192.168.92.36:8080/internal_por
tal/portal_account_login.html?wlanuserip=192.168.92.30&usermac=54:9F:13:45:B6:29&wlanuserfirsturl=https://www.baidu.com
[2017-11-27 14:36:55]:  appconn.c:841:eag_ipinfo_get before userip=192.168.92.30
[2017-11-27 14:36:55]:  appconn.c:845:eag_ipinfo_get after userip=192.168.92.30,usermac=54:9F:13:45:B6:29,interface=br-wan
[2017-11-27 14:36:55]:  appconn.c:848:appconn_check_is_conflict eag_ipinfo_get userip 192.168.92.30, interface(br-wan), usermac(54:9F:13:45:B6:29)
[2017-11-27 14:36:55]:  eag_redir.c:2221:ARP name test-portal_arp,intf ath12,bridge br-wan
```

5.5 Cluster Management

✓ ***cluster_mgt -x show=self // To check the AP Cluster role and status***

Example:

```
support@AP-78:00:~$
support@AP-78:00:~$ cluster_mgt -x show=self
ClusterID   MAC                 role        priority            status
111         dc:08:56:00:78:00   PVC         000461007800        RUN
support@AP-78:00:~$
```

✓ ***cluster_mgt -x show=pvc // To check the PVC of the cluster***

Example:

```
support@AP-78:00:~$
support@AP-78:00:~$ cluster_mgt -x show=pvc
IP              MAC                 priority            status
192.168.92.36   dc:08:56:00:78:00   000465007800        RUN
support@AP-78:00:~$
```

✓ ***show_cluster // To check all the AP members in the cluster***

Example:

```
support@AP-C2:F0:~$
support@AP-C2:F0:~$ show_cluster
mac               ip              prio   state   role   auth    name      version      ptype
34:e7:0b:03:c2:f0   192.168.92.49     0     3     1      1     AP-C2:F0      3.0.0.63       6
34:e7:0b:00:07:e0   192.168.92.40     0     3     3      1     AP-07:E0      3.0.0.63       4
34:e7:0b:00:06:50   192.168.92.48     0     3     3      1     AP-06:50      3.0.0.63       4
34:e7:0b:00:0a:d0   192.168.92.45     0     3     3      1     AP-0A:D0      3.0.0.63       4
34:e7:0b:03:c2:50   192.168.92.44     0     3     3      1     AP-C2:50      3.0.0.63       6
34:e7:0b:03:c6:90   192.168.92.42     0     3     2      1     AP-C6:90      3.0.0.63       6
support@AP-C2:F0:~$
```

✓ ***show_cluster |wc -l // To check the AP numbers in the cluster***

Example:

```
support@AP-C2:F0:~$ show_cluster
mac               ip              prio   state   role   auth    name      version      ptype
34:e7:0b:03:c2:f0   192.168.92.49     0     3     1      1     AP-C2:F0      3.0.0.63       6
34:e7:0b:00:07:e0   192.168.92.40     0     3     3      1     AP-07:E0      3.0.0.63       4
34:e7:0b:00:06:50   192.168.92.48     0     3     3      1     AP-06:50      3.0.0.63       4
34:e7:0b:00:0a:d0   192.168.92.45     0     3     3      1     AP-0A:D0      3.0.0.63       4
34:e7:0b:03:c2:50   192.168.92.44     0     3     3      1     AP-C2:50      3.0.0.63       6
34:e7:0b:03:c6:90   192.168.92.42     0     3     2      1     AP-C6:90      3.0.0.63       6
support@AP-C2:F0:~$ show_cluster |wc -l
7
support@AP-C2:F0:~$
```

The AP numbers is the output value minus one.

✓ ***ps |grep cluster // To check if "cluster" process is working normally***

Example:

```
support@AP-78:00:~$
support@AP-78:00:~$ ps |grep cluster
12181 root      5600 S    /sbin/cluster_mgt -I 111 -p ff:ff:ff:ff:ff:ff
22137 support   1520 S    grep cluster
31545 root      3240 S    /sbin/cluster_cor -I 111 -p ff:ff:ff:ff:ff:ff
support@AP-78:00:~$
```

Two "cluster_mgt" thread existing indicates abnormal behavior as below example:

```
support@AP-0C:E0:~$ ps  | grep cluster
 3484 root      7144 S    /sbin/cluster_mgt -I 100 -p 0
 3485 root      9208 S    /sbin/cluster_cor -I 100 -p 0 -v 10.0.0.1
26955 root      7144 R    /sbin/cluster_mgt -I 100 -p 0
28666 support   1184 S    grep cluster
support@AP-0C:E0:~$
```

5.6 Network Management

✓ ***cat /etc/resolv.conf // To check the DNS server information***

Example:

```
support@AP-78:00:~$
support@AP-78:00:~$ cat /etc/resolv.conf
# Interface wan
nameserver 219.141.136.10
nameserver 219.141.140.10
support@AP-78:00:~$
```

✓ ***cat /tmp/TZ // To check the Timezone configuration***

Example:

```
support@AP-78:00:~$
support@AP-78:00:~$ cat /tmp/TZ
UTC-08
support@AP-78:00:~$
```

✓ ***cat /proc/kes_syslog |grep ntp // To check the NTP logs***

Example:

```
support@AP-78:00:~$
support@AP-78:00:~$ cat /proc/kes_syslog |grep ntp
Mon Nov 27 15:30:09 2017 user.notice root: _GOLSOH_time was synced from pool.ntp.org
Mon Nov 27 15:45:09 2017 user.notice root: _GOLSOH_time was synced from pool.ntp.org
Mon Nov 27 16:00:09 2017 user.notice root: _GOLSOH_time was synced from pool.ntp.org
Mon Nov 27 16:15:09 2017 user.notice root: _GOLSOH_time was synced from pool.ntp.org
Mon Nov 27 16:30:09 2017 user.notice root: _GOLSOH_time was synced from pool.ntp.org
Mon Nov 27 16:45:10 2017 user.notice root: _GOLSOH_time was synced from pool.ntp.org
Mon Nov 27 17:00:08 2017 user.notice root: _GOLSOH_time was synced from pool.ntp.org
Mon Nov 27 17:15:09 2017 user.notice root: _GOLSOH_time was synced from pool.ntp.org
Mon Nov 27 17:30:08 2017 user.notice root: _GOLSOH_time was synced from pool.ntp.org
Mon Nov 27 17:45:08 2017 user.notice root: _GOLSOH_time was synced from pool.ntp.org
Mon Nov 27 18:00:07 2017 user.notice root: _GOLSOH_time was synced from pool.ntp.org
support@AP-78:00:~$
support@AP-78:00:~$
```

✓ ***cat /etc/config/rogueap // To check the "Rogue AP" configuration***

cat /tmp/config/wids.conf

Example:

```
support@AP-78:00:~$
support@AP-78:00:~$ cat /etc/config/rogueap

config rogueap 'RogueAP'
        option Debug '1'
        list wildcard 'dc:08:56:*:*:*'
        option SuppressSwitch '1'
        option BlackSwitch '1'

config rogueap 'Contain'
        list ruleset 'Open'
        list ruleset 'Encrypt'

config ruleset 'Open'
        option ARP '1'
        option Deauth '0'
        option Disassoc '0'

config ruleset 'Encrypt'
        option Deauth '1'
        option Disassoc '0'

support@AP-78:00:~$


support@AP-1B:60:~$ cat /tmp/config/wids.conf
{
        "WidsRules":{
                "condition":{
                        "validssid_filter":1,
                        "prevent_switch":0,
                        "black_switch":0,
                        "detect_switch":0
                },
                "FOUIList":[
                        "34:e7:0b:*:*:*",
                        "dc:08:56:*:*:*"
                ]
        }
}
support@AP-1B:60:~$
```

✓ ***ps|grep light // To check if the WBM service is running***

Example:

```
support@AP-78:00:~$
support@AP-78:00:~$ ps|grep light
 8645 root      4748 S    /usr/sbin/lighttpd -D -f /etc/lighttpd/lighttpd_http
28166 support   1520 S    grep light
support@AP-78:00:~$
```

- ✓ ***cat /etc/cert/serial // To check the serial of the certificate***

Example:

```
support@AP-78:00:~$
support@AP-78:00:~$ cat /etc/cert/serial
DC0856007800000008425A
support@AP-78:00:~$
```

- ✓ ***ifconfig br-wan // To check the IP address configuration of AP***

ssudo ifconfig br-wan

Example:

```
support@AP-36:D0:~$ ifconfig br-wan
br-wan    Link encap:Ethernet  HWaddr DC:08:56:0A:36:D0
          inet addr:172.16.18.167  Bcast:172.16.18.255  Mask:255.255.255.0
          inet6 addr: fe80::de08:56ff:fe0a:36d0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4100 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1313 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:263864 (257.6 KiB)  TX bytes:172549 (168.5 KiB)

support@AP-36:D0:~$ ssudo ifconfig br-wan
br-wan    Link encap:Ethernet  HWaddr DC:08:56:0A:36:D0
          inet addr:172.16.18.167  Bcast:172.16.18.255  Mask:255.255.255.0
          inet6 addr: fe80::de08:56ff:fe0a:36d0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4275 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1352 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:274704 (268.2 KiB)  TX bytes:177581 (173.4 KiB)

support@AP-36:D0:~$
```

- ✓ ***ssudo ping // To check the network connectivity***

Example:

```
support@AP-36:D0:~$ ssudo ping 172.16.18.1
PING 172.16.18.1 (172.16.18.1): 56 data bytes
64 bytes from 172.16.18.1: seq=0 ttl=64 time=0.699 ms
64 bytes from 172.16.18.1: seq=1 ttl=64 time=0.506 ms
64 bytes from 172.16.18.1: seq=2 ttl=64 time=0.510 ms
64 bytes from 172.16.18.1: seq=3 ttl=64 time=0.487 ms
64 bytes from 172.16.18.1: seq=4 ttl=64 time=0.496 ms
64 bytes from 172.16.18.1: seq=5 ttl=64 time=0.479 ms
64 bytes from 172.16.18.1: seq=6 ttl=64 time=0.554 ms
64 bytes from 172.16.18.1: seq=7 ttl=64 time=0.504 ms
64 bytes from 172.16.18.1: seq=8 ttl=64 time=0.517 ms
64 bytes from 172.16.18.1: seq=9 ttl=64 time=0.479 ms
64 bytes from 172.16.18.1: seq=10 ttl=64 time=0.523 ms
64 bytes from 172.16.18.1: seq=11 ttl=64 time=0.487 ms
64 bytes from 172.16.18.1: seq=12 ttl=64 time=0.513 ms
64 bytes from 172.16.18.1: seq=13 ttl=64 time=0.494 ms
^C
--- 172.16.18.1 ping statistics ---
14 packets transmitted, 14 packets received, 0% packet loss
round-trip min/avg/max = 0.479/0.517/0.699 ms
support@AP-36:D0:~$
support@AP-36:D0:~$ ssudo ping www.baidu.com
PING www.baidu.com (220.181.111.188): 56 data bytes
64 bytes from 220.181.111.188: seq=0 ttl=54 time=7.625 ms
64 bytes from 220.181.111.188: seq=1 ttl=54 time=4.199 ms
64 bytes from 220.181.111.188: seq=2 ttl=54 time=6.986 ms
64 bytes from 220.181.111.188: seq=3 ttl=54 time=6.690 ms
64 bytes from 220.181.111.188: seq=4 ttl=54 time=7.491 ms
64 bytes from 220.181.111.188: seq=5 ttl=54 time=3.360 ms
64 bytes from 220.181.111.188: seq=6 ttl=54 time=4.746 ms
^C
--- www.baidu.com ping statistics ---
7 packets transmitted, 7 packets received, 0% packet loss
round-trip min/avg/max = 3.360/5.871/7.625 ms
support@AP-36:D0:~$
```

- ✓ ***ssudo traceroute*** ***// To check the network trace route***

Example:

```
support@AP-36:D0:~$ ssudo traceroute www.baidu.com
traceroute to www.baidu.com (220.181.111.188), 30 hops max, 38 byte packets
 1  bogon (172.16.18.1)  0.164 ms  0.285 ms  0.296 ms
 2  *  *^C
support@AP-36:D0:~$ ssudo traceroute 172.16.18.1
traceroute to 172.16.18.1 (172.16.18.1), 30 hops max, 38 byte packets
 1  bogon (172.16.18.1)  0.212 ms  0.026 ms  0.236 ms
support@AP-36:D0:~$
```

- ✓ ***ssudo tcpdump*** ***// To capture the packets from "br-wan" interface***

tftp ***// To transfer files via TFTP***

Example:

```
support@AP-36:D0:~$
support@AP-36:D0:~$ cd /tmp
support@AP-36:D0:/tmp$ tcpdumcm -i br-wan -s0 -w 1111.pcap
-ash: tcpdumcm: not found
support@AP-36:D0:/tmp$
support@AP-36:D0:/tmp$
support@AP-36:D0:/tmp$ tcpdump -i br-wan -s0 -w 1111.pcap
tcpdump: br-wan: You don't have permission to capture on that device
(socket: Operation not permitted)
support@AP-36:D0:/tmp$
support@AP-36:D0:/tmp$
support@AP-36:D0:/tmp$ ssudo tcpdump -i br-wan -s0 -w 1111.pcap
tcpdump: listening on br-wan, link-type EN10MB (Ethernet), capture size 65535 bytes
^C60 packets captured
61 packets received by filter
0 packets dropped by kernel
support@AP-36:D0:/tmp$
support@AP-36:D0:/tmp$ ls
1111.pcap                cluster_cmd_pipe         cluster_neighbor_dump   dnsmasq.d                ipaddr                   lock                     online-usr-count         sessionId                wifi1.calda
PortalCustom             cluster_config           cluster_socket          echo.fcgi.socket-0       kes_debug.log            log                      overlay                  shm                      wmaagent_re
TZ                       cluster_cor_sock         config                  etc                      kes_dmsg.log             mkca_lock                pvc-info                 spool                    wpa.log
adme_socket              cluster_fifo             configuration_state     fix_mode.log             kes_history_syslog.log   mode                     resolv.conf              state                    zfinal
caldata                  cluster_mgt_pipe         dcm_socket              hos_partool.cfg          lib                      ntp_synced_mark          resolv.conf.auto         sysinfo                  ztp_log
cluster                  cluster_mgt_socket       dhcp.leases             hosts                    lighttpd                 ntpdate_lock             run                      wifi0.caldata
support@AP-36:D0:/tmp$
support@AP-36:D0:/tmp$ tftp -pl 1111.pcap 172.16.18.166
support@AP-36:D0:/tmp$
support@AP-36:D0:/tmp$
```

6 Troubleshooting

6.1 Introduction of the AP Logs

6.1.1 Log files

6.1.2 Log level

6.1.3 Log collection

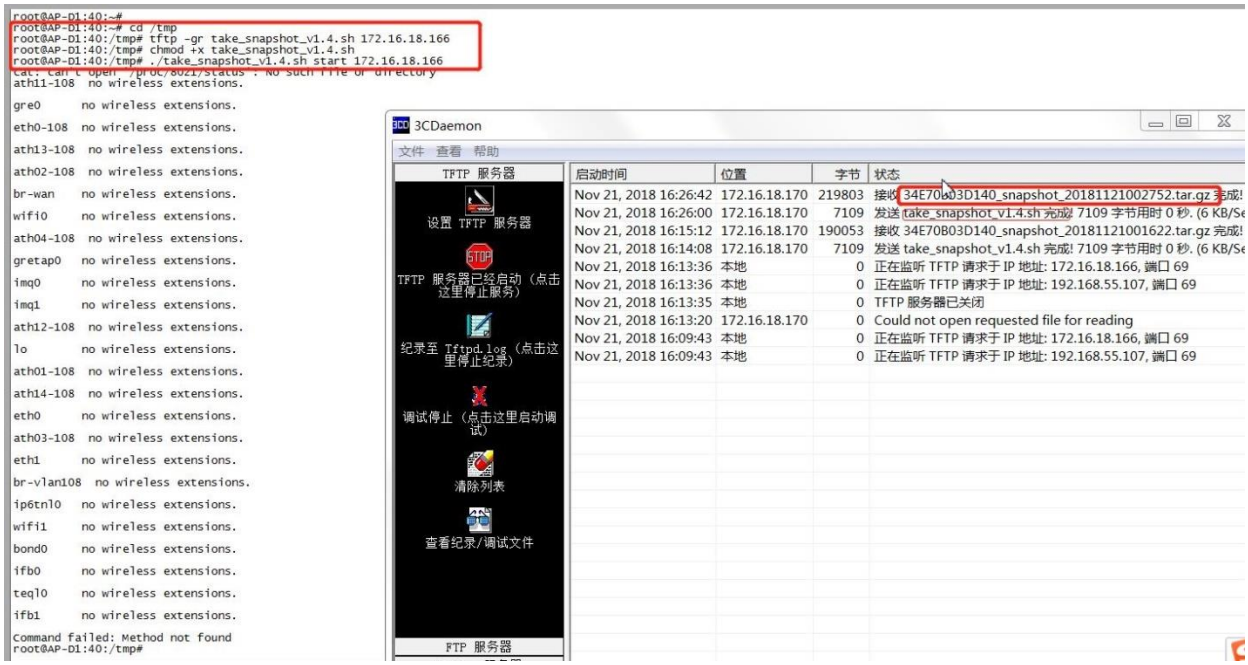
6.1.3.1 For R3.0.3 Build

✓ To setup a TFTP server on a PC, and put the script "take_snapshot_v1.4.sh" on the TFTP server path:

Example: TFTP Server Address=***172.16.18.166***

✓ Log collection through the root account

```
root@AP-D1:40:~#
root@AP-D1:40:~# cd /tmp
root@AP-D1:40:/tmp# tftp -gr take_snapshot_v1.4.sh 172.16.18.166
root@AP-D1:40:/tmp# chmod +x take_snapshot_v1.4.sh
root@AP-D1:40:/tmp# ./take_snapshot_v1.4.sh start 172.16.18.166
```



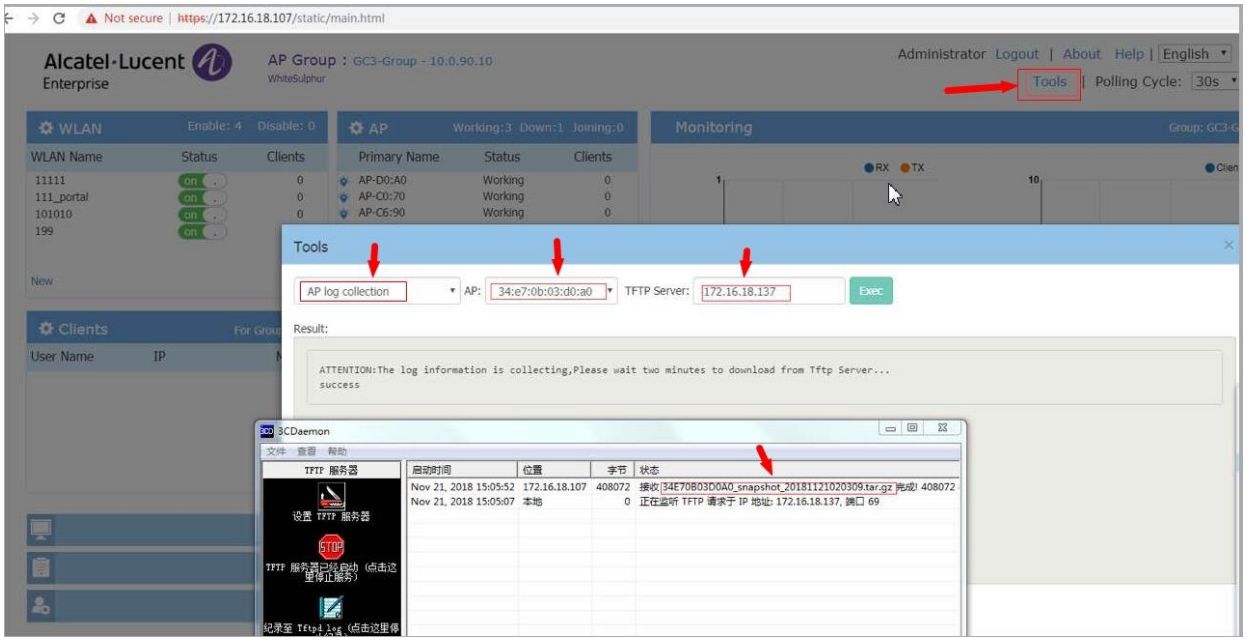
6.1.3.2 For R3.0.4 Build

There are two methods to collect the logs:

A. Use the script "take_snapshot_v1.4.sh", the same as R3.0.3 Build.

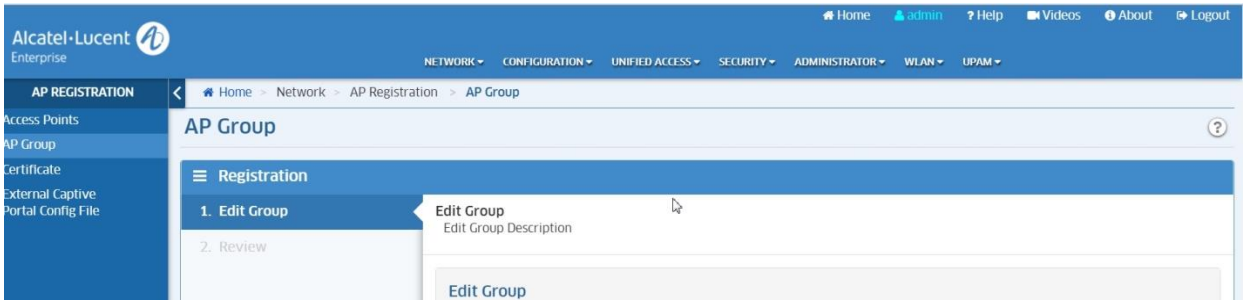
B. Use the GUI Tools.

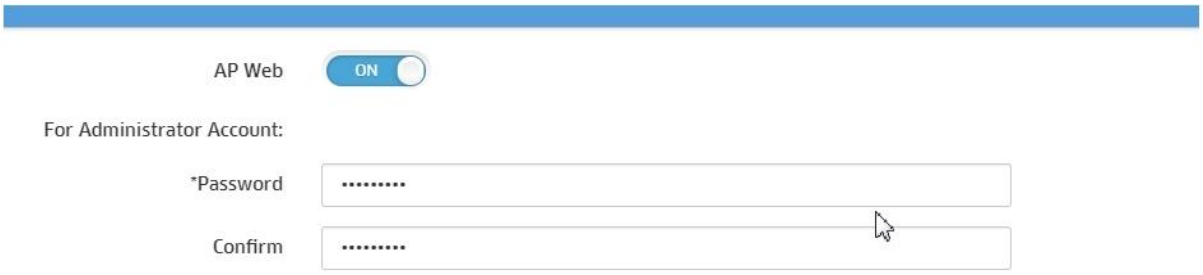
- For Express mode, refer to below screenshot:



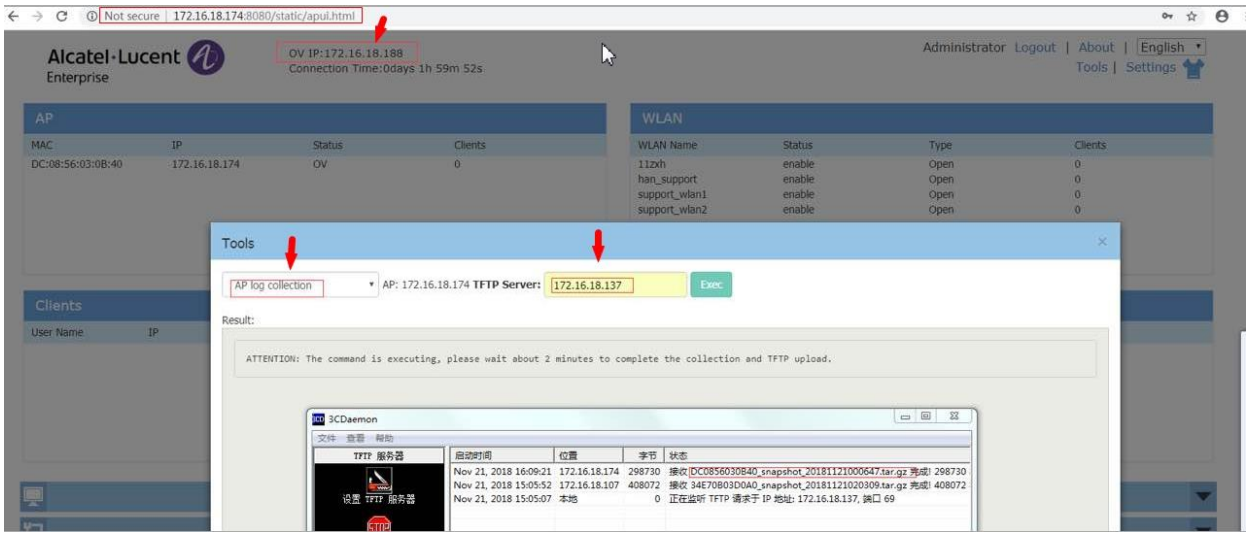
- For Enterprise mode, it supports in R3.0.4MR2 or later build, see below screeshot

  ✓ Enable "AP Web" first.





✓ Login the AP Web with "http://AP_IP:8080" or "https://AP_IP"



6.1.3.3 For long time collection of the log.

For some cases, it needs to collect the logs for hours or days, please use the script "take_snapshot_v1.4.sh" and "get_log_v1.4.sh" together as below:

root@AP-D1:40:/tmp# tftp -gr take_snapshot_v1.4.sh 172.16.18.166

root@AP-D1:40:/tmp# mv take_snapshot_v1.4.sh /usr/bin

root@AP-D1:40:/tmp# tftp -gr get_log_v1.4.sh 172.16.18.166

root@AP-D1:40:/tmp# chmod +x /usr/bin/take_snapshot_v1.4.sh

root@AP-D1:40:/tmp# chmod +x ./get_log_v1.4.sh

root@AP-D1:40:/tmp# sh ./get_log_v1.4.sh 172.16.18.166 &

Note: when finish the log collection, please first type "fg" then press ctrl+c to end the script.

6.2 Troubleshooting for specific features (To be finished)

6.2.1 AP Reboot

Collection the logs under support account:

✓ To setup a TFTP server on a PC, for example: TFTP Server Address=***172.16.18.166***

```
support@AP-CA:70:~$ cd /tmp

support@AP-CA:70:/tmp$

support@AP-CA:70:/tmp$ reset_reason get

support@AP-CA:70:/tmp$ tftp -pl kes_debug.log 172.16.18.166

support@AP-CA:70:/tmp$ tftp -pl kes_dmsg.log 172.16.18.166

support@AP-CA:70:/tmp$ tftp -pl kes_history_syslog.log 172.16.18.166

support@AP-CA:70:/tmp$ tftp -pl kes_history_traps.log 172.16.18.166
```

6.2.2 Band steering

- Related log description
- How to capture this trace
- Necessary analysis.

6.2.3 Throughput issues

6.2.4 Authentication

6.2.5 Portal

……

- END OF DOCUMENT -