Content

Chapter 1   AP Configuration Management

1.1 Introduction to AP Configuration Management

AP (Access Point)

AP (Access Point) is a very complicated entity which is the important part of wireless network. We should configure and manage AP to make it provide better service for users. This document describes some aspects to configure and manage to AP: AP Reset, AP Image file updating, AP configuration file updating and AP statistic information management.

1.2 AP Management Configuration

AP management configuration task list is as below:

1. AP reset

2. AP Image updating

3. AP configuration files updating

4. AP statistic information management

5. Rate restriction function of ap Ethernet port

6. Configure data forwarding mode of the disconnected AP

7. Configure whether the managed AP supports Aeroscout engine

1. Reset AP manually

Command	Explanation
Admin Mode	
wireless ap reset [<*macaddr*>]	Reset the appointed AP which is at local management status. If local AC is controller, reset AP managed by peer-switch.
wireless ap factory-reset [mac]	Make AP managed by AC reset with factory configuration.

2. Update AP image manually

Command	Explanation
Command	Explanation

Wireless Global Mode	
ap auto-upgrade **no ap auto-upgrade**	Enable/disable the automatical update function of AC.
wireless ap integrated image-type *<1-7>* WORD **no wireless ap integrated image-type *<1-7>***	Appoint the image file for the AP which uses the updating method of Integrated.
wireless ap download image-type *<1-7>* *<word>* **no wireless ap download image-type *<1-7>***	Configure the TFTP or FTP address that a specific AP Image type is in and configure the full path of this file.
wireless ap download group-size *<1-48>*	Configure the number of AP which downloads the Image file at the same time per group.
Admin Mode	
wireless ap download abort	Get over the AP Image update process.
wireless ap download start [image-type *<1-7>*] [*<macaddr>*]	Trigger an AP with specific image type or mac address or both of them to start to download image file configured already

3. AP configuration files updating

Command	Explanation
Wireless Global Mode	
ap profile *<1-1024>* **no ap profile *<1-1024>***	Add a configuration file and enter the AP configuration file mode from the wireless global mode. The no command deletes the appointed configuration file.
ap address A.B.C.D A.B.C.D profile <1-1024> **no ap address A.B.C.D A.B.C.D profile <1-1024>**	Set profile ID for the IP address range interval AP. The no command deletes profile ID that AP specified in the interval.
AP Configuration Mode	

profile *<1-1024>* **no profile** *<1-1024>*	Appoint a profile ID for an AP. The no command deletes the profile ID appointed by AP and recovers it to be the default profile ID.
AP Profile Configuration Mode	
clear	Configure all except AP profile name in profile as default.
hwtype *<1-255>* **no hwtype**	Appoint an AP hardware type for a configuration file or appoint using AP hardware type of profile configuration file as 0
name *<name>* **no name**	Appoint a descriptive name for a configuration file or configure this name as default
ntp server {domain <word>|ipv4 <A.B.C.D>|ipv6 <X:X::X:X>} **no ntp server**	Appoint ntp server domain name or IP address for AP of the profile. The no command cancels this domain name or IP address.
Admin Mode	
ap profile copy *<1-1024> <1-1024>*	Copy content of a configuration file to another configuration file
wireless ap profile apply *<1-1024>*	Issue the appointed profile configuration file to AP which is configured corresponding configuration file
AP profile Configuration Mode	
dns-server {primary|backup} <ipv4/6-address> **no dns-server** {primary|backup }	Appoint a dns server for an ap of the configuration file. The no command deletes it.
management vlan <1-4094> **no management vlan**	Appoint a managed vlan for ap of the configuration file. The no command appoints the vlan as 1.
management vlan priority <0-7> **no management vlan priority**	Appoint the priority of managed vlan for a configuration file. The no command recovers it to 0.

ethernet native-vlan <1-4094> no ethernet native-vlan	Appoint a untagged-vlan for ap of the configuration file. The no command appoints the AP untagged-vlan as 1.

4. AP statistic information management

Command	Explanation
Admin Mode	
clear wireless statistics	Reset the statistics information of global AC.
Wireless Global Mode	
statistics-interval <5-3600> no statistics-interval	Stipulate the time interval of ap reporting the status statistic data. The no command makes the time interval automatic.

5. Rate restriction function of ap Ethernet port

Command	Explanation
AP Configuration Mode	
rate-limit ethernet no rate-limit ethernet	Enable rate restriction function of AP ethernet ingress.
rate-limit ethernet arp<0-1000000> no rate-limit ethernet arp	Configure ARP packets rate restriction of AP ethernet ingress.
rate-limit ethernet broadcast<0-1000000> no rate-limit ethernet broadcast	Configure broadcast packets rate restriction of AP ethernet ingress.
rate-limit ethernet multicast<0-1000000> no rate-limit ethernet multicast	Configure multicast packets rate restriction fof AP ethernet ingress.
rate-limit ethernet timer<10-1000> no rate-limit ethernet timer	Configure speed limit time interval of AP ethernet ingress.
rate-limit ethernet unicast<0-1000000> no rate-limit ethernet unicast	Configure unicast packets rate restriction of AP ethernet ingress.
rate-limit ethernet unicast-promiscuous<0-1000000> no rate-limit ethernet unicast-promiscuous	Configure unicast packets rate restriction of AP ethernet ingress under mix mode.

6. Configure data forwarding mode of the disconnected AP

Command	Explanation

wireless ap profile config	
disconnected-ap forwarding-mode	Enable data forwarding function of
no disconnected-ap forwarding-mode	the disconnected ap.
disconnected-ap management-mode	Enable management mode of the
no disconnected-ap management-mode	ap connected to port.

7. Configure whether the managed AP supports Aeroscout engine

Command	Explanation
wireless ap profile config	
aeroscout	Configure the managed AP
no aeroscout	supports Aeroscout engine.

1.3 AP Configuration Management Examples

Case：

In two wireless controllers, AC1 is controller, AC2 is peer-switch. In two wireless access points, AP1 and AP2 connect to AC1 and AC2 respectively.
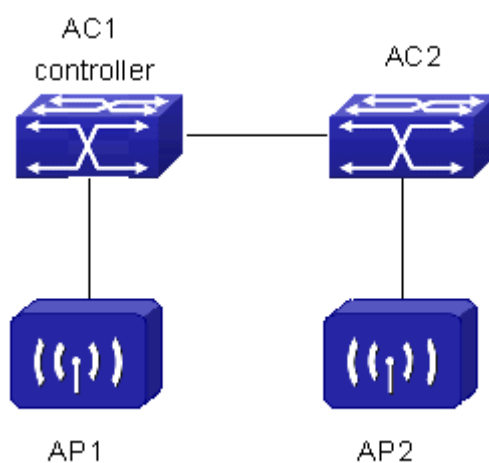

Fig 1-1 AP configuration management

Configuration steps:

1. AP Image updating

1) AP updates AC configuration automatically

AC#copy tftp://192.168.1.100/ap_image.tar ap_image.tar

AC(config-wireless)#ap auto-upgrade

AC(config-wireless)#wireless ap integrated image-type 1 flash:/ap_image.tar

AC#wireless ap reset 00-03-0f-18-ec-b0

Are you sure you want to reset WS managed AP? [Y/N] y

Reset Requested for WS Managed AP.

2) AP updates AC configuration manually (manual control is only on controller)

AC(config-wireless)#wireless   ap   download   image-type   1

tftp://192.168.1.100/ap_image.tar

AC(config-wireless)#wireless ap download group-size 20

AC#wireless ap download start

Wireless system initiated code download for managed AP 00-03-0f-18-ec-b0

2. AP configuration file updating

1) configure profile ID for AP

AC(config-wireless)#ap profile 2

AC(config-wireless)#ap database 00-03-0f-18-ec-b0

AC(config-ap)#profile 2

The valid AP entry is updated. This AP is already managed, to update the managed AP configuration with the new value(s) you need to reset the AP.

AC(config-ap)#end

AC#wireless ap reset 00-03-0f-18-ec-b0

2) configure profile content and issue

AC(config-wireless)#ap profile 2

AC(config-ap-profile)#hwtype 1

AC(config-ap-profile)#name p2

AC(config-ap-profile)#end

AC#wireless ap profile apply 2

All configurations will be send to the aps associated with this profile. Are you sure you want to apply the profile configuration? [Y/N] y

AP Profile apply is in progress.

3) copy profile file

AC#ap profile copy 1 2

All contents in the source profile will be copied to the destination profile. Are you sure you want to copy? [Y/N] y

AP Profile Configuration Copy Successful.

3. Statistic information management

1) reset wireless global statistic information

AC#clear wireless statistics

All the statistics on the switch will be cleared. Are you sure you want to clear all the statistics on the switch? [Y/N] y

Wireless statistics are cleared.

1.4 AP Configuration Management Troubleshooting

If there is something wrong when managing AP configuration, please check out if it is caused with reasons below:

☞ If enable wireless function, all configuration will only be effective when enabling wireless function;

☞ After modifying profile ID of relevant status AP, to see whether the AP is reseted, after reseting, the new configuration will be effective;

☞ After modifying profile file content, to see whether it was issued configuration. After issuing, the new configuration will be effective. During issuing configuration, radio of AP will be reseted and it will cause the client disconnection. In configuration issuing, 3 configurations do not need to be issued, they can be effective automatically, and they are centralized tunnel VLAN list, distributed configuration and client QoS configuration updating. If hwtype of profile is matching to AP hardware type when issuing. If it is not matching, it cannot be issued.

☞ If the AC which is updating manually is controller, only controller can update manually.

☞ If AP completes Image download after stopping manual updating. If AP do not complete downloading image file, it cannot trigger new manual updating.

☞ If it is fail to use the automatic updating method as the AP updating, please check: 1. If the AP hardware type matches the image type, use **show wireless ap capability image-table** command to ensure; 2. If the AP image file which needs updating is put in the flash of AC correctly.

Chapter 2   License Control

2.1 Introduction to License Control

The license control module is used to limit the number of AP managed by wireless controller. License control is an exemplification of authorizing manner, authorizing the users through license can use some specific features of the wireless switches. Users can also buy the specific features of the wireless switches according to their own needs, which making the function of switches meet the users' needs.

When in factory, the controller internal will be pre-installed on a default license file used to achieve the basic functions of the controller and meet the basic requirements of users on controller. Using the controller for a period time, if they find that the basic functions cannot meet the requirements, then they can make requests to the sales staff for updating the controller. Then, the sales staff will presented a paper license file containing the certificate ID which is used for achieving license file. User can use the Certificate ID written in the license file and the extracted MAC address information and factory serial number from controller which needs to be updated to produce a lawful file; user can also send the relevant information to the company through the appointed mailbox according to the explanation in license file. The relevant staff of the company will produce the license file needed by user according to the information user sent and send it to user through email. This License file contains information of the limitations for the controller module and parameters, user installs this License files to the corresponding controller and restarts the controller, it can make the new functions added in license file become effective and meet the the user's needs.

2.2 License Control Configuration

1. Import the license file into wireless controller

Command	Explanation
Admin Mode	
copy license *<source-url>* *<destination-url>*	Import the license file into wireless controller.

2.3 License Control Configuration Examples

Typical Case:

Import new license: abc.lic and make it become effective.

AC configuration list:

AC# copy license ftp://admin:admin@192.168.1.10/abc.lic abc.lic

AC#show license

   License name: abc.lic

   License ap-count: 32

   License module: none

   License total period: forever

AC#show device information

 Controller serial number:abcd23456

 Controller mac:00-03-0f-18-28-28

AC# reload

Process with reboot? [Y/N] y

2.4 License Control Troubleshooting

When you found the new AP cannot be managed, you can examine the number of management AP supported by this license file through the command of **show license**, then examine whether the number of AP had been managed reached the maximum number which license supports through the command of **show wireless switch local status**. If the number of AP reached the maximum number, the new license should be added to make sure the controller can manage a larger number of APs.

Chapter 3   Upgrading Based on AP Group

3.1 Introduction to Upgrading Based on AP Group

At present there are many methods for an AP to upgrade. User can either use the serial port directly for the AP upgrade, and can also use the integrated mode or independent way on the ac to upgrade the AP. But the above methods are not flexible enough to upgrade, each operation can only be for one AP in upgrading the AP on the ac, or upgrade all APs, or upgrade according to the image type of AP. There is a big limitation on the number of APs or combination. The technology of upgrading a group of AP based on the AP group breaks this limitation; it can upgrade any number, any combination of APs.

The upgrading technology based on the AP group is implemented based on AP group technology. It is the expansion to the upgrading of the independent mode. It can be widely used in various time environments, satisfying the different upgrading requirements.

Under the mode of independent upgrading, Image files is stored in the outside TFTP/FTP server, after the AP passes through the AC certification, this mode is triggered by the administrator manually, AC will send Image updating messages to the AP with that MAC, the message contains the name of a particular type of Image file. After all of the APs which need to update the Image download the Image file successfully, AC will send a message of restarting to each AP. After receiving the message of restarting, AP begins to restart.

Upgrade operations can only start on the controller. When entering the CLI command, AC controller will check whether the AP which needs updating is in a state of local management. If so, send the message of updating directly to the AP. If the AP which needs updating is not in a state of local management, the AC controller needs to send the message of Image updating to one or all ACs which need the updated management AP, and then the AC which needs the updated management AP transmits the message of Image updating to those APs.

Upgrade one AP group based on AP group, which mainly can be divided into four steps:

(1) Named the AP which needs to upgrade. AP's default name is its MAC address. In order to the facilitate management, user can name it according to the AP's geographical location or type.

(2) Create an AP group and add the AP which needs to upgrade. User can add

different APs to the same or different AP groups; multiple APs can join into one AP group.

(3) Configure the imgTypeID, file name, the path and the relationship among them. According to show wireless ap capability image –type, the imgTypeID can be gotten, and then configure the imgTypeID, file name, the path and the relationship among them.

(4) Use wireless ap download start ap-group <ap-group-name> to upgrade the AP.

3.2 Upgrading Based on AP Group Configuration

The upgrading based on AP group configuration task list is as below:

1. Name the AP which is waiting for the upgrading
2. Create an ap group and add the ap name into it
3. Configure the tftp (ftp) address and full path of the specific ap image file
4. Use wireless ap download start ap-group <ap-group-name> to trigger the AP upgrading

1. Name the AP which is waiting for the upgrading

Command	Explanation
ap database mode	
name (default-mac-name|WORD) **no name**	Configure/delete the AP name.

2. Create an ap group and add the ap name into it

Command	Explanation
Wireless Global Mode	
ap-group <ap-group-name> **no ap-group <ap-group-name>**	Create/delete the ap group.
ap-group mode	
permit-ap-name <ap-name> **no permit-ap-name <ap-name>**	Add/delete the authorized AP.

3. Configure the tftp (ftp) address and full path of the specific ap image file

Command	Explanation
Wireless Global Mode	
wireless ap download image-type <1-7><url> **no wireless ap download image-type <1-7>**	Configure/delete the tftp (ftp) address and full path of the specific ap image file.

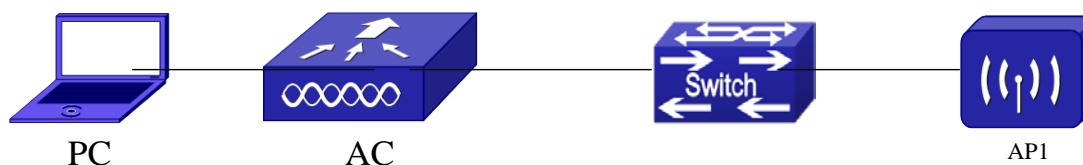4. Use wireless ap download start ap-group <ap-group-name> to trigger the AP upgrading

Command	Explanation
Admin Mode	

wireless ap download start ap-group <ap-group-name>	Trigger all the APs in one ap group to start to download the configured image file.

3.3 Upgrading Based on AP Group Examples

PC   AC   AP1

Create the environment. AC connects to AP through the switch or PoE. AP is managed successfully.

1. Name the AP which is waiting for the upgrading:

Name the ap according to the ap location as below:

AC(config-wireless)#ap database 00-03-0f-1e-58-60

AC(config-ap)#name 1_301R4

AC(config-ap)#exi

AC(config-wireless)#ap database 00-03-0f-26-18-60

AC(config-ap)#name 1_302R4

View the ap name through the command of **sho wireless ap database**:

AC(config-ap)#sho wireless ap database

MAC Address	AP Name	Location	AP Mode
00-03-0f-1e-58-60	1_301R4		ws-managed
00-03-0f-26-18-60	1_302R4		ws-managed

2. Create an ap group and add the ap name into it:

AC(config-wireless)#ap-group 1_1

AC(config-ap-group)#permit-ap-name 1_301R4

AC(config-ap-group)#permit-ap-name 1_302R4

AC#show wireless ap-group

AP-Group Name	AP Name	MAC Address
1_1	1_301R4	00-03-0f-1e-58-60
1_1	1_302R4	00-03-0f-26-18-60

Total ap group count:4

AC#

3. Configure the tftp (ftp) address and full path of the specific ap image file

AC#config

AC(config)#wireless

AC(config-wireless)#wireless   ap   download   image-type   2

tftp://102.1.1.200/upgrade_2_0_5_10.tar

4. Use wireless ap download start ap-group <ap-group-name> to trigger the AP upgrading:

AC#config

AC(config)#wireless

AC#wireless ap download start ap-group 1_1

3.4 Upgrading Based on AP Group Troubleshooting

When trigger the AP upgrading through the command of wireless ap download start ap-group<ap-group-name>, if it is abnormal, please check the following reasons:

☞ Check if the downloaded image file exists. If it does not exist, the image downloading cannot start.

☞ Check if the image file is put on the tftp (ftp) server.

☞ Check if the tftp (ftp) server is started and if the server file path is configured as the path that the image is saved in.

☞ Check if the AP is managed by AC and if the IP address between each AP and tftp (ftp) server is connectivity.

Chapter 4   AP Upgrade Independent Mode Function

4.1 Introduction to AP Upgrade Independent Mode Function

In independent upgrade mode, image file save on external FTP/TFTP server and keep AC and server connected to each other. After AP pass the authencation with AC, administrators trigger the mode manually, AC will send Image upgrade information to AP which have the mac address, the information includes the name of specific type of Image file. According to the set updated AP numbers of every group at the same time, AC manage AP that need to update to update Image file according to group and send Image update information to every group AP in turn, the information includes the name of specific type of Image file. After all AP that need update Image download Image file successfully, AP will send a reboot information to every AP, after AP receive reboot information, AP reboot and finish AP upgrade.

4.2 AP Upgrade Independent Mode Configuration

The configuration of AP upgrade independent mode as follows:

1. Set the AP number of every group download image file at the same time.
2. Show the AP Image type that current system supported.
3. Set the independent upgrade path of specific AP Image type.
4. Trigger specific AP download configured Image file.
5. Show AP global download status.

1.   Set the AP number of every group download image file at the same time

Command	Explanation
Wireless configuration mode	
wireless ap download group-size *<1-48>*	Set the AP number of every group download image file at the same time. The default is 10.

2. Show the AP Image type that current system supported

Command	Explanation
Admin mode	
show wireless ap capability image-table	Show the AP Image type that current system supported.

3. Set the independent upgrade path of specific AP Image type

Command	Explanation
Wireless global mode	
wireless ap download image-type<type WORD> FTP/TFTP	Set the independent upgrade path of specific AP Image type.

4. Trigger specific AP download configured Image file

Command	Explanation
Admin mode	
wireless ap download start[image-type <*1-12*>] [<*macaddr*>]	Trigger specific AP download configured Image file.

5. Show AP global download status

Command	Explanation
Admin mode	
show wireless ap download	Show AP global download status.

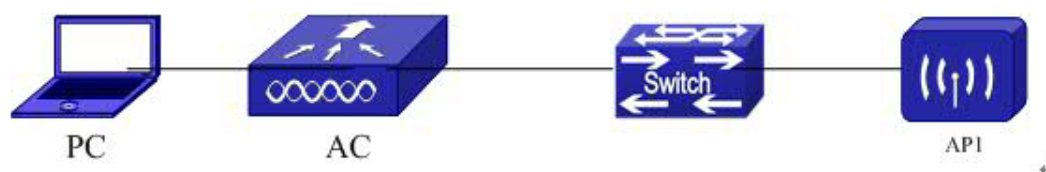# 4.3 AP Upgrade Independent Mode Configuration Examples

Fig 1 the application topology of AP upgrade independent mode

Topology explanation: AP1 managed by AC successfully, PC as TFTP sever connected with AC.

Application: after AP managed by AC, it issue configuration information of AP upgrade independent mode through AC.

1）Show AP Image type that current system supported, in the case of image-table 1 of AP1, every group download AP numbers of Image file is 20 at the same time, after set independent upgrade path, trigger specific AP to download configured Image file to upgrade.

AC#show wireless ap capability image-table

AC(config-wireless)#wireless ap download group-size 20

AC(config-wireless)# wireless ap download image-type 1

tftp://192.168.1.100/.//ap_image.tar

AC#wireless ap download startimage-type 1 00-03-0f-26-18-60

4.4 AP Upgrade Independent Mode Troubleshooting

If there is something wrong when using AP upgrade independent mode configuration, please check out if it is caused with reasons below:

☞ Upgrade AP in independent mode, premise is AP in managed AP table, namely it is managed successfully.

☞ Upgrade operation in controller only, but controller can upgrade their managed AP and peer switch managed AP. PeerSwitch can not upgrade their managed AP directly through independent mode.

☞ If a AP download Image failed during the update, the AP state is set as Failure, the upgrade failed AP require administrator intervention, such as administrator can trigger a specific AP manually to reboot it.

Chapter 5   Access Based on AP Location

5.1 Introduction to Access Based on AP Location

Considering the security and billing, the wireless network operators may need to control the location that the wireless users access the network, it means that the wireless users can access the network in the appointed locations but they cannot access the network in the locations which are not appointed. We can achieve this function through controlling the AP. Users can access the network through the association with the AP in the appointed AP Group. One AP Group can authorize one or more APs.

After the function of access based on AP location is enabled, the server will issue a user profile name property when the wireless user tries to access the network and passes the authentication of AAA Server. AC checks all the authorized AP Groups and the authorized APs in the groups according to the user profile name. As long as any AP Group authorizes the associated AP, the user can be allowed accessing; if the AP that the user accesses is not in the authorized AP Group of the user profile name, the user will be rejected accessing.

After the function of access based on AP location is enabled, user should check the access controlling if there is the roam. If the roam destination AP is the one that the user is allowed accessing, the roam is successful; if the roam destination AP is not the one that the user is allowed accessing, the roam fails.

5.2 Access Based on AP Location Configuration

This section only presents the configuration on AC. Please reference the authentication server manual for how the authentication serverconfigures user's user profile name.

Access based on AP location configuration task list:

1. Configure the name for AP

2. Configure the AP Group and the authorized AP name in the group

3. Configure the user profile and the authorized AP Group under the profile

4. Enable the function of access based on AP location

5. Show the configurations

1. Configure the name for AP

Command	Explanation
ap database Mode	
name <default-mac-name|ap-name> **no name**	Configure the name of AP. The no command deletes the name. it adopts the MAC address of AP as the name of AP.

2. Configure the AP Group and the authorized AP name in the group

Command	Explanation
Wireless Globale Configuration Mode	
ap-group <ap-group-name> **no ap-group <ap-group-name>**	Add an AP group and enter into the ap-group configuration mode. If the ap-group-name exists, enter into the ap-group configuration mode. The command of **no ap-group** can delete one AP group.
ap-group Mode	
permit-ap-name <ap-name> **no permit-ap-name <ap-name>**	Add an authorized AP for AP Group. The no command deletes an authorized AP.

3. Configure the user profile and the authorized AP Group under the profile

Command	Explanation
Wireless Globale Configuration Mode	
user-profile <user-profile-name> **no user-profile <user-profile-name>**	Add a user profile and enter into the user profile configuration mode. If the user profile exists, enter into the user profile configuration mode. The command of **no user-profile <user-profile-name>** can delete one user profile.
user-profile Configuration Mode	
permit-ap-group <ap-group-name> **no permit-ap-group <ap-group-name>**	Add an authorized AP group into the user-profile. The no command deletes an authorized AP group.

4. Enable the function of access based on AP location

Command	Explanation
Wireless Globale Configuration Mode	

user-profile enable no user-profile enable	Enable the function of access based on AP location. The no command disables this function.

5. Show the configurations

Command	Explanation
Admin Mode	
show wireless client ff-ff-ff-ff-ff-ff status	Show the authenticated wireless user's information including the AP name that the user is allowed accessing.
show wireless ap database	Show the AP database including AP name. If the AP name is not configured on AP, the shown content is empty.
show wireless user-profile [<user-profile-name>]	Show the configured user profile and the authorized AP Group under the profile.
show wireless ap-group [<ap-group-name>]	Show the configured AP Groups and the authorized AP name under the Groups.

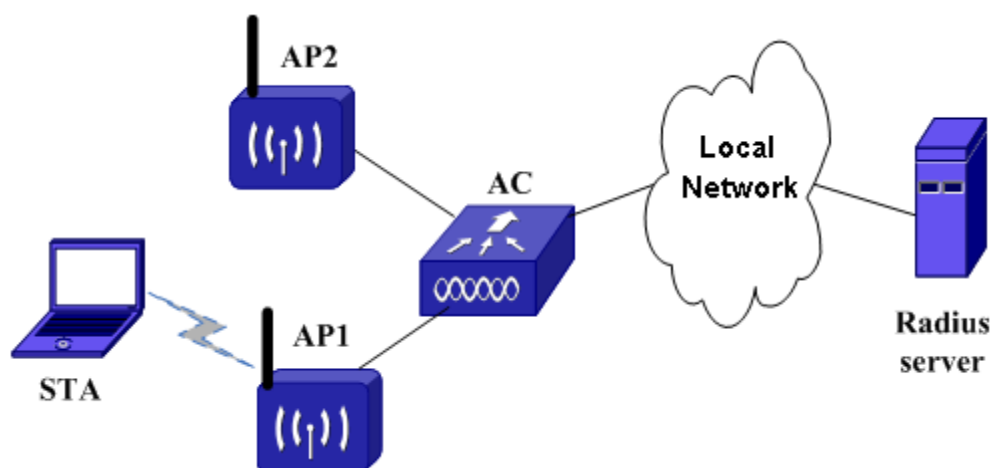# 5.3 Access Based on AP Location Examples

Typical case:

Fig 5-1 typical case of local AP

As shown above, there are AP1 and AP2 close to the STA location. If dose not access based on the AP location, STA can access the network through AP1 and AP2. After enabled the function of access based on AP location, users are limited to access through AP1 only, they are not allowed accessing through AP2.

The configuration is as below:

1 configuration on Radius server:

An account should be created for the STA user on Radius server, and the corresponding user profile name should be configured in the account information. Please reference the authentication server manual for the detailed methods. In this example, we assume the configured user profile name as profile1.

2 Configure the AAA authentication/accounting, network and vap on AC. （below is the simple method; please reference the wireless client access and authentication manual for the detailed methods.）

AC>enable

AC#config

AC(config)#aaa enable

AC(config)#aaa-accounting enable

AC(config)#radius source-ipv4 1.1.1.1 (AC sends the source added of radius packet.)

AC(config)#radius nas-ipv4 1.1.1.1

AC(config)#radius-server key 0 test （RADIUS server key. It should be the same as the one on the server.）

AC(config)#radius-server authentication host 100.1.1.100 （RADIUS server address）

AC(config)#radius-server accounting host 100.1.1.100

AC(config)#aaa group server radius radius_server

AC(config-sg-radius)#server 100.1.1.100

AC(config-sg-radius)#exit

AC(config)#wireless

AC(config-wireless)#radius server-name auth radius_server

AC(config-wireless)#radius server-name acct radius_server

AC(config-wireless)#network 1

AC(config-network)#ssid ssid1

AC(config-network)#security mode wpa-enterprise

AC(config-network)#exit

AC(config-wireless)#ap profile 1

AC(config-ap-profile)#radio 1

AC(config-ap-profile-radio)#vap 0

AC(config- ap-profile-vap)#network 1

AC(config-ap-profile-vap)#enable

AC(config- ap-profile-vap)#exit

AC(config-ap-profile-radio)#exit

AC(config-ap-profile)#exit

AC(config-wireless)#exit

AC(config)#exit

AC#wireless ap profile apply 1

3 Add the database for AP1 and AP2 on AC and configure the AP name.

AC(config-wireless)#ap database 00-00-00-00-01

AC(config-ap)#name ap1

AC(config-ap)#exit

AC(config-wireless)#ap database 00-00-00-00-02

AC(config-ap)#name ap2

4 Create the AP Group of group1 on AC and authorize AP1.

AC(config-wireless)#ap-group group1

AC(config-ap-group)# permit-ap-name ap1

5 Create the user profile on AC and name it as profile1; and authorize the AP Group of group1.

AC(config-wireless)#user-profile profile1

AC(config-user-profile)#permit-ap-group group1

6 Enable the function of access based on AP location.

AC(config-wireless)# user-profile enable

Through the configuration as above, user can access the network through AP1. If user access the network through AP2, it will be rejected.

5.4 Access Based on AP Location Troubleshooting

Please adopt the following method if the function of access based on AP location cannot be effective in using:

- ☞ Check if the configured user profile name on the user data of the server is the same as the user profile name on AC. If they are different, please modify it.
- ☞ Check if the AP name configuration is correct (it is not the name that the administrator assigns.)
- ☞ Check if the AP name joins in the correct AP Group and if the AP Group joins in the correct user profile. If this AP allows the user accessing, it must be joined in

the user profile of the user; if this AP does not allow the user accessing, it cannot be joined in the user profile of the user.

☞ If the above steps have no problems, please check if the access authentication configuration is correct. User can disable the function of access based on AP location first and check if user can access normally. If user cannot access, the configuration should be modified; if user can access, please check as the above steps again.

Chapter 6   LAN Port of Wall AP

6.1 Introduction to LAN Port of Wall AP

The configuration method of wireless function of the wall AP is same to other AP devices, and the issuing method is also same. Bug the LAN port has difference; it should be configured all alone. The LAN port is the layer2 device, user can access in the network directly after connecting to it. Currently, the VLAN and UP/DOWN information of LAN port can be configured through AC, it can be issued by the specific command after the configuration.

6.2 LAN Port Configuration

1. Configure the VLAN ID of LAN port

Command	Explanation
AP Profile Configuration Mode	
lan port vlan<1-4094> **no lan port vlan<1-4094>**	Configure the VLAN ID of LAN port. The no command recovers it to be the default VLAN ID of VLAN 1.

2. Enable/disable the LAN port

Command	Explanation
AP Profile Configuration Mode	
lan port down **no lan port down**	Enable/disable the LAN port, the LAN port is enabled as default.

3. Send the configuration

Command	Explanation
Addmin Mode	
wireless ap lan port configuration apply profile <profileId>	Send the configuration to the LAN port.

6.3 LAN Port Configuration Examples

Configure the LAN port as VLAN 1.

AC>enable

AC#config

AC(config)#wireless

AC(config-wireless)#ap profile 1

AC(config-ap-profile)#lan port vlan 1

Send the above configuration to the LAN port.

AC#wireless ap lan port configuration apply profile 1

Chapter 7   AP Escape Client-persist Function

7.1 Introduction to AP Escape Client-persist Function

Fit AP is working under the managemet of AC, if it disconnected from AC, the associated client will be forced to offline, and it is the worst for working users (no charging case). It will be a good choose if Fit AP can maintain client not dropped like Fat AP. It means Fit AP can adjust itself, when it dropped with AC, it can maintain the online or offline of client; after it create link with AC again, it is maintained by AC as before. So we create an AP escape function, enable it can maintenance the online or offline function of client when Fit AP dropped with AC. Realized AP escape function as follows:

(1) When Fit AP is not being managed, AP escape function enable or disable do not influence the operation of AP.

(2) When Fit AP is managed by AC, AP escape function enable or disable do not influence the operation of AP.

(3) When Fit AP that managed by AC enable escape function, AC-AP keep alive timeout, and turn off TCP link, the results as follows:

AP close TCP socket, open row socket, set rfscan scan interval, statistic report interval and keep alive interval is 0, and set no manage status for AP, enter the status that wait to find relationship with AC;

Keep the current configuration (except tunnel configuration) of AP, radio status is unchanged, the client in normal still can use wireless network;

Changing VAP that configured to centralized transfer to local transfer;

The information which includes client association, authencation, disassociation, pre-authencation are not forward to AC, only modify the record that mapd correspond, and not save error information in log file.

7.2 AP Escape Client-persist Configuration

1. Enable AP escape function.
2. Enable AP escape client-persist function.

1. Enable/Disable AP escape function

Command	Explanation
Ap profile configuration mode	
ap escape **no ap escape**	Enable/disable ap escape function of all AP under the ap profile.

2. Enable/Disable AP escape client-persist function

Command	Explanation
Ap profile configuration mode	
ap escape client-persist **no ap escape client-persist**	Enable/disable AP escape clien-persist function of all AP under the ap profile.

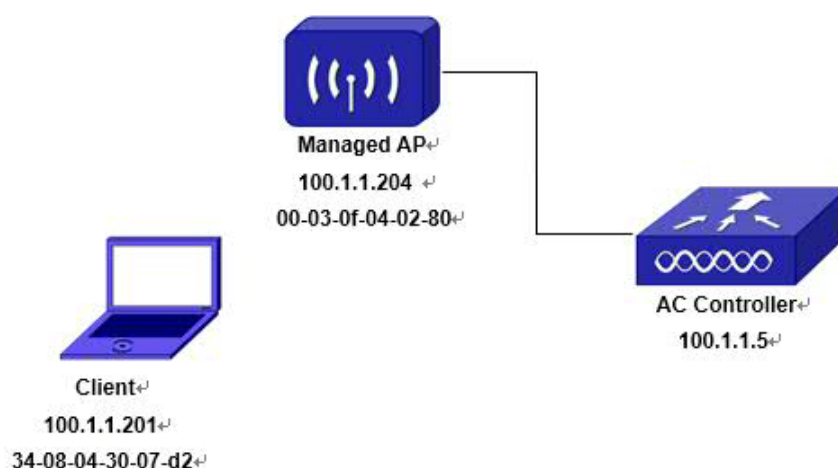# 7.3 AP Escape Client-persist Configuration Example

Fig1 The topology of AP escape client-persist

Topology explanation: AP is managed by profile 1 of AC

Application: After ap is managed by AC, send AP escape client-persist configuration by AC:

1. Enable ap escape client-persist function

AC(config-ap-profile)#ap escape

AC(config-ap-profile)#ap escape client-persist

7.4 AP Escape Client-persist Troubleshooting

When there are problems in using the AP escape client-persist, please check the following reasons:

☞ Before configure AP escape client-persist function, please enable AP escape function

☞ For client-persist when AC, AP associated again, it will skip profile issue automatically after enable escape function, if it update profile configuration when AC, AP turn off, it will work until issue configuration manually in AC.