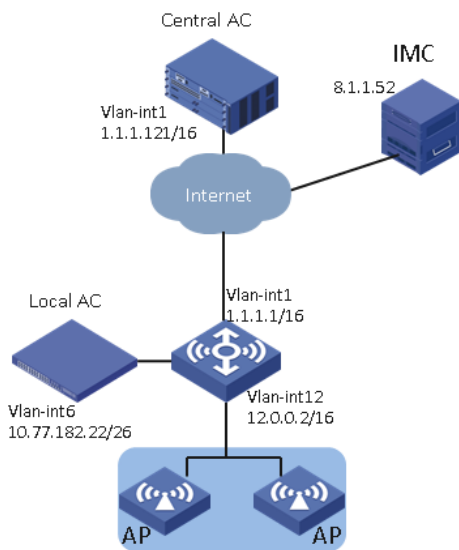


## 知 分层AC组网portal认证典型配置 (Central AC认证+AP转发)

Portal 分层AC 陈铮 2018-09-07 发表

### 组网及说明



总部采用一台WX3520H作为Central AC，分支采用一台WX3510H作为Local AC，Local AC负责管理和接入本地AP和无线客户端。用户的认证授权则由总部Central AC负责，数据流量由AP转发。

具体应用需求如下：

- AP通过DHCP Option43功能获取到Central AC地址，之后通过二次发现方式与Local AC建立CAPWAP连接。
- 使用IMC作为Portal服务器和AAA服务器对用户进行Portal认证。
- AP和用户的地址池配置在交换机上。
- Local AC设备故障后AP直接接入到Central AC上组成普通AC+FITAP组网，变为AC认证AP转发模式。

### 配置步骤

- 在采用本地转发模式的无线组网环境中，AC上没有Portal客户端的ARP表项，为了保证合法用户可以进行Portal认证，需要开启无线Portal客户端合法性检查功能。
- 为了将AP的GigabitEthernet1/0/1接口加入本地转发的VLAN，需要使用文本档编辑AP的配置文件，并将配置文件上传到AC存储介质上。
- 在总部分支组网中，如果不配置二次发现的Local AC的IP地址，则Central AC将当前负载最轻的Local AC的IP地址下发给AP，如果负载最轻的Local AC不是本分支的Local AC，则会导致本分支AP无法上线，所以为了保证本分支的AP能够正确从本分支的Local AC上线，需要配置二次发现的Local AC的IP地址为本分支的Local AC的IP地址。
- 为了保证Local AC设备故障后AP可以接入到Central AC做备份，将AP和用户的地址池配置在交换机上。

配置Central AC

(1) 配置接口

# 创建VLAN1及其接口，用来与Local AC建立管理通道。

```
system-view
```

```
[Central AC] vlan 1
```

```
[Central AC-vlan1] quit
```

```
[Central AC] interface vlan-interface 1
```

```
[Central AC-Vlan-interface1] ip address 1.1.1.121 16
```

```
[Central AC-Vlan-interface1] quit
```

(2) 配置Central AC管理的Local AC

# 创建名称为3510h-1的Local AC，并进入Local AC视图。

```
[Central AC] wlan local-ac name 3510h-1 model WX3510H
```

# 配置Local AC的序列号。

```
[Central AC-wlan-local-ac-3510h-1] serial-id 210235A1JNB166000078
```

```
[Central AC-wlan-local-ac-3510h-1] quit
```

(3) 配置无线客户端的Portal认证功能

- 配置RADIUS方案

```
# 创建RADIUS方案imc1并进入其视图。
[Central AC] radius scheme imc1
# 设置主认证RADIUS服务器的IP地址8.1.1.52。
[Central AC-radius-imc1] primary authentication 8.1.1.52
# 设置主计费RADIUS服务器的IP地址8.1.1.52。
[Central AC-radius-imc1] primary accounting 8.1.1.52
# 设置系统与认证RADIUS服务器交互报文时的共享密钥为12345678。
[Central AC-radius-imc1] key authentication simple 12345678
# 设置系统与计费RADIUS服务器交互报文时的共享密钥为12345678。
[Central AC-radius-imc1] key accounting simple 12345678
# 设置发送给RADIUS服务器的用户名不携带域名。
[Central AC-radius-imc1] user-name-format without-domain
# 设置设备发送RADIUS报文时使用的源IP地址8.183.1.121。
[Central AC-radius-imc1] nas-ip 8.183.1.121
[Central AC-radius-imc1] quit
• 配置认证域
# 创建imc域并进入其视图。
[Central AC] domain imc1
# 为Portal用户配置认证方案为RADIUS方案，方案名为imc1。
[Central AC-isp-imc1] authentication portal radius-scheme imc1
# 为Portal用户配置授权方案为RADIUS方案，方案名为imc1。
[Central AC-isp-imc1] authorization portal radius-scheme imc1
# 为Portal用户配置计费方案为RADIUS方案，方案名为imc1。
[Central AC-isp-imc1] accounting portal radius-scheme imc1
[Central AC-isp-imc1] quit
• 配置Portal认证服务器
# 配置Portal认证服务器imc，IP地址为8.1.1.52，密钥为明文12345678。
[Central AC] portal server hesy1
[Central AC-portal-server-hesy1] ip 8.1.1.52 key simple 12345678
• 配置Portal web服务器
# 配置Portal Web服务器hesy1。
[Central AC] portal web-server hesy1
# 配置Portal Web服务器的URL。
[Central AC-portal-websvr-hesy1] url http://8.1.1.52:8080/portal/
# 配置URL中携带的参数信息。
[Central AC-portal-server-imc] url-parameter apmac ap-mac
[Central AC-portal-websvr-hesy1] url-parameter ssid ssid
[Central AC-portal-websvr-hesy1] url-parameter wlanacname value AC
[Central AC-portal-websvr-hesy1] url-parameter wlanuserip source-address
[Central AC-portal-websvr-hesy1] quit
# 开启无线Portal客户端合法性检查功能
[Central AC] portal host-check enable
(4) 配置无线服务。
# 创建无线服务模板portal。
[Central AC] wlan service-template 1
# 配置SSID。
[Central AC-wlan-st-1] ssid hesy
# 配置用户上线VLAN。
[Central AC-wlan-st-1] vlan 2000
# 配置客户端数据报文转发位置为AP。
[Central AC-wlan-st-1] client forwarding-location ap
# 在无线服务模板上开启直接方式的Portal认证。
[Central AC-wlan-st-1] portal enable method direct
# 在无线服务模板上引用Portal认证域imc。
[Central AC-wlan-st-1] portal domain imc
# 在无线服务模板上配置发送Portal报文的BAS-IP属性值为8.183.1.121。
[Central AC-wlan-st-1] portal bas-ip 8.183.1.121
# 在无线服务模板上引用Portal Web服务器hesy1。
[Central AC-wlan-st-1] portal apply web-server hesy1
# 开启无线服务模板。
[Central AC-wlan-st-1] service-template enable
[Central AC-wlan-st-portal] quit
# 创建手工AP，名称为ap1，配置序列号为210235A1BSC161001186。
[Central AC] wlan ap ap1 model WA4620i-ACN
```

```
[Central AC-wlan-ap-ap1] serial-id 210235A1BSC161001186
# 指定AP的配置文件。
[Central AC-wlan-ap-ap1] map-configuration cfa0:/map.txt
# 开启二次发现AC功能。
[Central AC-wlan-ap-ap1] control-address enable
# 手动指定Local AC的IP地址。
[Central AC-wlan-ap-ap1] control-address ip 10.77.182.22
# 将无线服务模板portal绑定到Radio 1接口。
[Central AC-wlan-ap-ap1] radio 1
[Central AC-wlan-ap-ap1-radio-1] radio enable
[Central AC-wlan-ap-ap1-radio-1] service-template 1
[Central AC-wlan-ap-ap1-radio-1] quit
配置Local AC
(1) 配置接口
# 创建VLAN 6及其接口， Local AC通过此接口上线到Central AC。
[Local AC] vlan 6
[Local AC-vlan6] quit
[Local AC] interface Vlan-interface6
[Local AC-Vlan-interface6] ip address 10.77.182.22 26
[Local AC-Vlan-interface6] quit
(2) 开启Local AC功能
# 开启Local AC功能。
system-view
[Local AC] wlan local-ac enable
# 指定Central AC的IP地址。
[Local AC] wlan central-ac ip 1.1.1.121
# 指定与Central AC建立管理通道的VLAN。
[Local AC] wlan local-ac capwap source-vlan 6
编辑AP配置文件
# 使用文本文档编辑AP的配置文件，将配置文件命名为map.txt，并将配置文件上传到AC存储介质上。
配置文件内容和格式如下：
system-view
vlan 12
vlan 2000
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 1 12 2000
配置交换机：
(1) 配置地址池
# 开启DHCP服务。
[swith] dhcp enable
# 配置地址池，为AP分配IP地址。
[swith] dhcp server ip-pool ap
[swith-dhcp-pool-ap] gateway-list 12.0.0.1
[swith-dhcp-pool-ap] network 12.0.0.0 mask 255.255.0.0
# 通过option43选项指定AC地址为Central AC地址。
[swith-dhcp-pool-ap] option 138 ip-address 1.1.1.121
[swith-dhcp-pool-ap] quit
# 配置地址池，为客户端分配IP地址。
[swith] dhcp server ip-pool vlan2000
[swith-dhcp-pool-vlan2000] gateway-list 183.1.0.2
[swith-dhcp-pool-vlan2000] network 183.1.0.0 mask 255.255.0.0
[swith-dhcp-pool-vlan2000] quit
(2) 配置接口绑定地址池
# 创建VLAN 12及其接口，用于AP接入
[swith] vlan 12
[swith-vlan12] quit
[swith] interface Vlan-interface12
[swith-Vlan-interface12] ip address 12.0.0.1 255.255.0.0
[swith-Vlan-interface12] dhcp server apply ip-pool ap
# 创建VLAN 12及其接口，用于Client接入
[swith] vlan 2000
[swith-vlan2000] quit
[swith] interface Vlan-interface2000
```

```
[swith-Vlan-interface2000]ip address 183.1.0.1 255.255.0.0
[swith-Vlan-interface2000]dhcp server apply ip-pool vlan2000
[swith-Vlan-interface2000]quit
配置Portal服务器
略
```

### 3.6 验证配置

# 在Central AC上可以查看到Local AC是R/M状态, 说明Local AC已在Central AC上线。

```
[Central AC]dis wlan local-ac name 3510h-1
```

Local AC Information

State : I = Idle, J = Join, JA = JoinAck, IL = ImageLoad

C = Config, DC = DataCheck, R = Run

AC name	ACID	State	Model	Serial ID
3510h-1	10	R/M	WX3510H	210235A1JNB166000078

# 在Central AC上可以查看到AP是R/M状态, 说明Local AC已经通过二次发现与Central AC建立管理通道。

```
[Central AC]display wlan ap all
```

Total number of APs: 1

Total number of connected APs: 1

Total number of connected manual APs: 1

Total number of connected auto APs: 0

Total number of connected common APs: 1

Total number of connected WTUs: 0

Total number of inside APs: 0

Maximum supported APs: 512

Remaining APs: 511

Total AP licenses: 512

Local AP licenses: 512

Server AP licenses: 0

Remaining Local AP licenses: 511

Sync AP licenses: 0

AP information

State : I = Idle, J = Join, JA = JoinAck, IL = ImageLoad

C = Config, DC = DataCheck, R = Run, M = Master, B = Backup

AP name	APID	State	Model	Serial ID
ap1	2	R/M	WA4620i-ACN	210235A1BSC161001186

# 在Central AC上可以查看到AP已经连接到Local AC。

```
[Central AC]display wlan ap-distribution all
```

Central AC

Slot : 2

Total Number of APs: 0

AP name :

Local AC

Name : 3510h-1

Total Number of APs: 1

AP name : ap1

```
[Central AC]
```

# 在Central AC上可以查看到无线客户端已经上线。

```
[Central AC]display wlan client
```

Total number of clients: 1

MAC address	User name	AP name	RID	IP address	VLAN
5c03-3940-042b	N/A	ap1	1	183.1.0.4	2000

# 在Central AC上可以查看到用户已经Portal认证成功。

```
[Central AC]display portal user all
```

Total portal users: 1

Username: qcf

AP name: ap1

Radio ID: 1

SSID: hesy

Portal server: hesy1

State: Online

VPN instance: N/A

MAC	IP	VLAN	Interface
5c03-3940-042b	183.1.0.4	2000	WLAN-BSS2/0/46

Authorization information:

DHCP IP pool: N/A

User profile: qucf (active)

Session group profile: N/A

ACL number: 3000 (active)

Inbound CAR: N/A

Outbound CAR: N/A

#Local AC故障AP直接接入到Central AC上做备份, 在Central AC上查看Local AC不在线

[Central AC]display wlan local-ac all

Total number of local ACs: 1

Total number of connected local ACs: 0

#### Local AC Information

State : I = Idle, J = Join, JA = JoinAck, IL = ImageLoad

C = Config, DC = DataCheck, R = Run

AC name	ACID	State	Model	Serial ID
3510h-1	10	I	WX3510H	210235A1JNB166000078

# 在Central AC上可以查看到AP接入到Central AC上。

[Central AC]display wlan ap-distribution all

Central AC

Slot : 2

Total Number of APs: 1

AP name : ap1

# # 在Central AC上可以查看到无线客户端重现上线。

[Central AC]display wlan client

Total number of clients: 1

MAC address	User name	AP name	RID	IP address	VLAN
5c03-3940-042b	N/A	ap1	1	183.1.0.4	2000

# 在Central AC上可以查看到用户重新Portal认证成功。

[Central AC]display portal user all

Total portal users: 1

Username: qucf

AP name: ap1

Radio ID: 1

SSID: hesy

Portal server: hesy1

State: Online

VPN instance: N/A

MAC	IP	VLAN	Interface
5c03-3940-042b	183.1.0.4	2000	WLAN-BSS2/0/47

Authorization information:

DHCP IP pool: N/A

User profile: qucf (active)

Session group profile: N/A

ACL number: 3000 (active)

Inbound CAR: N/A

Outbound CAR: N/A

配置关键点