SecBladeIAG支持根据不同SSID指向不同PORTAL RADIUS SERVER实现共享业务地址池的典型配置

wlan接入 Portal AAA **李晨光** 2012-06-26 发表

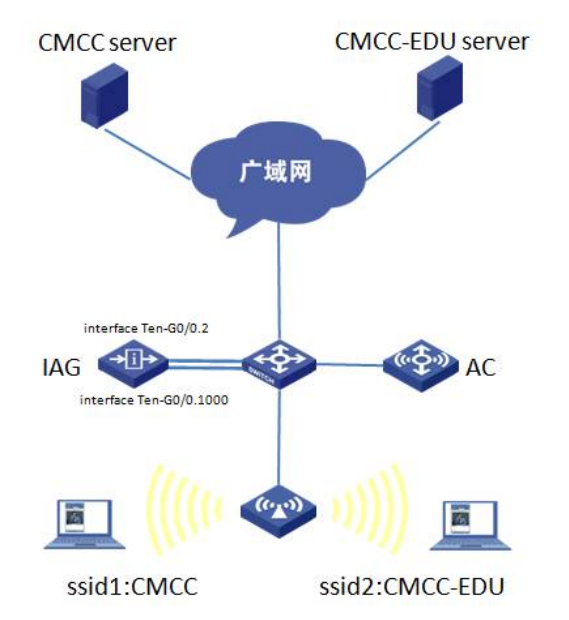
SecBladeIAG支持根据不同SSID指向不同PORTAL/RADIUS SERVER实现共享业务地址池的典型配置

一、组网需求：

WX6000系列无线控制器上开启多个服务，PC接入不同的SSID，业务网关终结到IAG同一子接口下。IAG能根据接入不同的SSID推送不同的PORTAL SERVER并匹配到不同的认证域。不同SSID的用户能共享业务地址池。

IAG必须是7510P06及以上版本，AC建议使用2308P07及以上版本。

二、组网图：



三、配置方法：

1．配置思路

- 在AC配置两个服务模板，SSID为CMCC、CMCC-EDU
- 在IAG上配置业务网关，同时终结CMCC、CMCC-EDU的业务VLAN
- 在IAG上配置portal server、domain，并配置SSID与portal server、domain绑定
- 在IAG上手动portal free-rule放通portal server

2．配置步骤

（1）AC上的配置信息：

```
dis cur
#
 version 5.20, Release 2308P07                    //AC版本建议是2308P07及以上
#
 sysname HAZZ-WLAN-AC135-HSWX6103
#
 clock timezone BEIJING add 08:00:00
#
 domain default enable system
#
dhcp server ip-pool test                          //配置AP的管理地址池
 network 192.168.100.0 mask 255.255.255.240
 gateway-list 192.168.100.1
 option 43 hex 80070000 01C0A864 01
#
user-group system
 group-attribute allow-guest
```

```
#
wlan service-template 1 clear                          //创建CMCC服务模板
 ssid CMCC
 bind WLAN-ESS 1
 user-isolation enable
 service-template enable
#
wlan service-template 4 clear                      //创建CMCC-EDU服务模板
 ssid CMCC-EDU
 bind WLAN-ESS 4
 user-isolation enable
 service-template enable
#
interface NULL0
#
interface Vlan-interface500                          //AC、AP注册三层接口
 ip address 192.168.100.1 255.255.255.240
#
interface Vlan-interface600                          //AC、IAG漫游隧道接口
 ip address 10.206.196.165 255.255.255.248
#
interface M-GigabitEthernet1/0/0
 shutdown
#
interface Ten-GigabitEthernet1/0/1
 description internet
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 2 to 3000
#
interface WLAN-ESS1
 port link-type hybrid
 undo port hybrid vlan 1
 mac-vlan enable
#
interface WLAN-ESS4
 port link-type hybrid
 undo port hybrid vlan 1
 mac-vlan enable
#
wlan ap test model WA2620 id 1
 trap enable
 serial-id 219801A0D1C122005975
 radio 1
 radio 2
  service-template 1 vlan-id 1005                    //绑定CMCC服务模板
  service-template 4 vlan-id 1072                  //绑定CMCC-EDU服务模板
  radio enable
#
wlan mobility-group 1                  //配置AC和IAG之间的lactp漫游隧道
 member ip 10.206.196.163
 source ip 10.206.196.165
 mobility-group enable
#
 ip route-static 0.0.0.0 0.0.0.0 10.206.196.161
#
 snmp-agent proxy ip 10.206.196.163                        //代理IAG网管
#
 snmp-agent
 snmp-agent local-engineid 800063A2033CE5A611BE35
 snmp-agent community write private
 snmp-agent sys-info version all
#
 dhcp enable
```

```
#
load xml-configuration
#
user-interface con 0
user-interface vty 0 4
 acl 2000 inbound
 authentication-mode scheme
 user privilege level 1
 idle-timeout 120 0
#
```

（2）IAG上的配置信息：

```
dis cur
#
 version 5.20, Release 7510P06                    //IAG版本必须是7510P06及以上
#
 sysname HAZZ-WLAN-BAS135-HSWX6103
#
 nas device-id 1
#
 domain default enable system
#
 portal server cmcc ip 10.176.1.140 url http://10.176.1.140/wlan/index.php
                                                  //配置cmcc的portal server
 portal server cmccedu ip 10.138.30.41 url http://10.138.30.41/index.php
                                                  //配置cmcc-edu的portal server
 portal free-rule 0 source any destination ip 10.176.1.140 mask 255.255.255.255
                                                  //必须要手动放通portal server地址
 portal free-rule 1 source any destination ip 10.138.30.41 mask 255.255.255.255
                                                  //必须要手动放通portal server地址
 portal free-rule 2 source any destination ip 211.136.17.107 mask 255.255.255.255
                                                  //放通DNS
 portal free-rule 3 source any destination ip 10.0.0.3 mask 255.255.255.255
                                                  //放通网关
 portal device-id 0135.0371.371.00
 portal wlan ssid CMCC server cmcc domain cmccwlan
                                                  //绑定SSID与portal server & domain
 portal wlan ssid CMCC-EDU server cmccedu domain cmccedu
                                                  //绑定SSID与portal server & domain
#
radius scheme cmccwlan                            //配置CMCC的radius scheme
 server-type extended
 primary authentication 10.176.1.138 1645
 primary accounting 10.176.1.138 1646
 key authentication 8
 key accounting 8
 timer realtime-accounting 30
 user-name-format keep-original
 nas-ip 10.206.196.162
 retry stop-accounting 10
radius scheme cmccedu                             //配置CMCC-EDU的radius scheme
```

```
 server-type extended
 primary authentication 10.206.248.109 1645
 primary accounting 10.206.248.109 1646
 key authentication 8
 key accounting 8
 timer realtime-accounting 30
 user-name-format without-domain
 nas-ip 10.206.196.162
 retry stop-accounting 10
#
aaa nas-id profile yaxin                          //配置nas-id profile
 nas-id 1005037137100460 bind vlan 1005
 nas-id 1072037137100460 bind vlan 1072
#
domain cmccedu                                    //配置CMCC-EDU的domain
 authentication portal radius-scheme cmccedu
 authorization portal radius-scheme cmccedu
 accounting portal radius-scheme cmccedu
 access-limit disable
 state active
 idle-cut enable 15 1024
 self-service-url disable
domain cmccwlan                                   //配置CMCC的domain
 authentication portal radius-scheme cmccwlan
 authorization portal radius-scheme cmccwlan
 accounting portal radius-scheme cmccwlan
 access-limit disable
 state active
 idle-cut enable 15 1024
 self-service-url disable
#
dhcp server ip-pool ac135-01                      //配置用户地址池
 network 10.5.52.0 mask 255.255.252.0
 gateway-list 10.5.52.1
 dns-list 10.138.24.66 10.138.30.66
 expired day 0 hour 1
#
user-group system
#
interface NULL0
#
interface GigabitEthernet0/1
 port link-mode route
#
interface GigabitEthernet0/2
 port link-mode route
#
```

```
interface GigabitEthernet0/3
 port link-mode route
#
interface GigabitEthernet0/4
 port link-mode route
#
interface Ten-GigabitEthernet0/0
 port link-mode route
#
interface Ten-GigabitEthernet0/0.2                    //配置nas-ip接口
 vlan-type dot1q vid 2
 ip address 10.206.196.162 255.255.255.248
#
interface Ten-GigabitEthernet0/0.600                  //配置AC、IAG漫游隧道接口
 vlan-type dot1q vid 600
 ip address 10.206.196.163 255.255.255.248
#
interface Ten-GigabitEthernet0/0.1000                 //配置业务网关接口
 vlan-type dot1q vid 1005 1072
 ip address 192.168.16.1 255.255.248.0
 portal server cmcc method direct          //添加一个缺省的重定向portal server，并开启端口portal 认证功能。该指定的portal server优先级低于全局绑定ssid的portal server
 portal domain cmccwlan
    //允许添加一个缺省的domain，用于兼容老配置。优先级低于全局绑定ssid的domain
 portal nas-id-profile yaxin
 portal nas-port-type wireless
 portal nas-ip 10.206.196.162
 access-user detect type arp retransmit 3 interval 60
#
wlan mobility-group 1                         //配置AC和IAG之间的lactp漫游隧道
 member ip 10.206.196.165
 source ip 10.206.196.163
 mobility-group enable
#
 ip route-static 0.0.0.0 0.0.0.0 10.206.196.161
#
 snmp-agent proxy ip 10.206.196.165    //配置snmp-agent代理，AC从R2308P10版本开始，在IAG+AC组网下为必选配置
 snmp-agent
 snmp-agent local-engineid 800063A2033CE5A613C720
 snmp-agent community write private
 snmp-agent sys-info version all
 snmp-agent target-host trap address udp-domain 10.142.189.59 params securityname public v2c
#
 dhcp enable
#
 load xml-configuration
```

#

user-interface con 0

user-interface aux 0

authentication-mode none

user privilege level 3

user-interface vty 0 4

acl 2000 inbound

authentication-mode scheme

user privilege level 1

#

（3）RADIUS服务器设置：略

3．配置关键点

（1）WX6103上进行配置：

创建WLAN-ESS1接口，并进入该视图。

[WX6103] interface WLAN-ESS 1

#配置端口的链路类型为hybrid

[WX6103-WLAN-ESS1] port link-type hybrid

hybrid端口上使能mac-vlan功能

[WX6103-WLAN-ESS0] mac-vlan enable

创建clear类型的服务模板1。

[WX6103] wlan service-template 1 clear

设置当前服务模板的SSID（服务模板的标识）为CMCC。

[WX6103-wlan-st-1] ssid CMCC

将WLAN-ESS1接口绑定到服务模板1。

[WX6103-wlan-st-1] bind WLAN-ESS 1

使能无线模板。

[WX6103-wlan-st-1] service-template enable

#同样的方法创建SSID为CMCC-EDU的服务模板。

在AC下绑定无线服务模板。

注意：AP的配置需要根据具体AP的型号和序列号进行配置。

创建AP管理模板，其名称为test，型号名称这里选择WA2620。

[WX6103] wlan ap test model WA2620

设置AP的序列号为219801A0D1C122005975。

[WX6103-wlan-ap-test] serial-id 219801A0D1C122005975

进入radio2射频视图。

[WX6103-wlan-ap-test] radio 2

将在AC上配置的服务模板与射频2进行关联,并帮定vlan属性。

[WX6103-wlan-ap-test-radio-2] service-template 1 vlan-id 1005

[WX6103-wlan-ap-test-radio-2] service-template 4 vlan-id 1072

使能test的radio 2

[WX6103-wlan-ap-test-radio-2] radio enable

[WX6103-wlan-ap-test-radio-2] quit

[WX6103-wlan-ap-test] quit

#配置WLAN漫游组

[WX6103] wlan mobility-group 1

#配置源IP地址

[WX6103-wlan-mg-1] source ip 10.206.196.165

#添加漫游组成员

[WX6103-wlan-mg-1] member ip 10.206.196.163

#开启IACTP服务

[WX6103-wlan-mg-1] mobility-group enable

[WX6103-wlan-mg-1] quit

（2）IAG上进行配置：

创建radius方案cmccwlan并进入其视图。

[IAG] radius scheme cmccwlan

配置PEAP认证/计费RADIUS服务器的IP地址。

[IAG-radius-cmccwlan] primary authentication 10.176.1.138 1645

[IAG-radius-cmccwlan] primary accounting 10.176.1.138 1646

配置Device与认证/计费RADIUS服务器交互报文时的共享密钥。

[IAG-radius-cmccwlan] key authentication 8

[IAG-radius-cmccwlan] key accounting 8

#设置设备发送RADIUS报文使用的源地址

[IAG-radius-cmccwlan] nas-ip 10.206.196.162

创建域cmccwlan并进入其视图。

[IAG] domain cmccwlan

配置PORTAL用户使用RADIUS方案cmccwlan进行认证、授权、计费。

[IAG-isp-cmccwlan] authentication portal radius-scheme cmccwlan

[IAG-isp-cmccwlan] authorization portal radius-scheme cmccwlan

[IAG-isp-cmccwlan] accounting portal radius-scheme cmccwlan

关闭该域最多可容纳用户限制功能。

[IAG-isp-cmccwlan] access-limit disable

启动闲置切断功能，并指定正常连接时用户空闲时间超过15分钟，并且最小流量低于1024 Byte时则切断其连接。

[IAG-isp-cmccwlan] idle-cut enable 15 1024

[IAG-isp-cmccwlan] quit

用同样的方法创建cmccedu的radius-scheme和domain

指定域system为缺省的ISP域。如果用户在登录时没有提供ISP域名，系统将把它归于该缺省的ISP域。

[IAG] domain default enable system

创建portal server cmcc

[IAG] portal server cmcc ip 10.176.1.140 url http://10.176.1.140/wlan/index.php

创建portal server cmccedu

[IAG] portal server cmccedu ip 10.138.30.41 url http://10.138.30.41/index.php

创建portal free-rule放通portal server

[IAG] portal free-rule 0 source any destination ip 10.176.1.140 mask 255.255.255.255

[IAG] portal free-rule 1 source any destination ip 10.138.30.41 mask 255.255.255.255

绑定SSID与portal server和认证域domain

[IAG] portal wlan ssid CMCC server cmcc domain cmccwlan

[IAG] portal wlan ssid CMCC-EDU server cmccedu domain cmccedu

在TG0/0.2上配置三层接口，作为nas-ip和服务器交互认证报文。

[IAG] interface Ten-GigabitEthernet0/0.2

[IAG-Ten-GigabitEthernet0/0.2] vlan-type dot1q vid 2

[IAG-Ten-GigabitEthernet0/0.2] ip address 10.206.196.162 255.255.255.248

创建TG0/0.1000接口作为业务网关，并进入该视图。

[IAG] interface Ten-GigabitEthernet 0/0.1000

#配置此端口模糊VLAN终结

[IAG-Ten-GigabitEthernet0/0.1000] vlan-type dot1q vid 1005 1072

#配置此端口的IP地址，作为业务网关

[IAG-Ten-GigabitEthernet0/0.1000] ip address 192.168.16.1 255.255.248.0

#配置重定向portal server。该指定的portal server优先级低于全局绑定ssid的server优先级，即IAG推送PORTAL时先在全局查询该SSID是否绑定PORTAL SERVER，如果是，则推送绑定的SERVER，否则推送接口下配置的缺省SERVER

[IAG-Ten-GigabitEthernet0/0.1000] portal server cmcc method direct

#配置认证域domain。该指定的domain优先级低于全局绑定ssid的domain优先级，即IAG认证时先在全局查询该SSID是否绑定domain，如果是，则匹配绑定的domain，否则匹配接口下配置的缺省domain

[IAG-Ten-GigabitEthernet0/0.1000] portal domain cmccwlan

#配置WLAN漫游组

[IAG] wlan mobility-group 1

#配置源IP地址

[IAG-wlan-mg-1] source ip 10.206.196.163

#添加漫游组成员

[IAG-wlan-mg-1] member ip 10.206.196.165

#开启IACTP服务

[IAG-wlan-mg-1] mobility-group enable

[IAG-wlan-mg-1] quit