SecBladeIAG支持PEAP认证并和PORTAL共享业务地址池典型配置

wlan接入 Portal 802.1X AAA DHCP **李晨光** 2012-06-26 发表

SecBladeIAG支持PEAP认证并和PORTAL共享业务地址池典型配置

一、应用环境

中国移动现网局点大量采用AC/IAG分离架构,已有的PORTAL认证点位于IAG板卡上。中国移动要求在原PORTAL业务的基础上新增无感知认证业务，即EAP-SIM/PEAP认证业务。为满足中国移动无感知业务需求，且保持认证点的统一，和节省NAS-IP，我司IAG在7510P06版本新增支持EAP-SIM/PEAP认证。在AC/IAG组网下，IAG完成EAP认证交互，AC完成空口的加密。

同时，PORTAL和PEAP业务可以在IAG同一子接口下配置，能实现PORTAL和PEAP共享业务地址池。

二、注意事项

（1）IAG上的EAP-SIM/PEAP业务目前不支持双机热备；

（2）需要IAG与AC特定版本配合使用；IAG：7510P06及以上、AC：2308P07及以上；

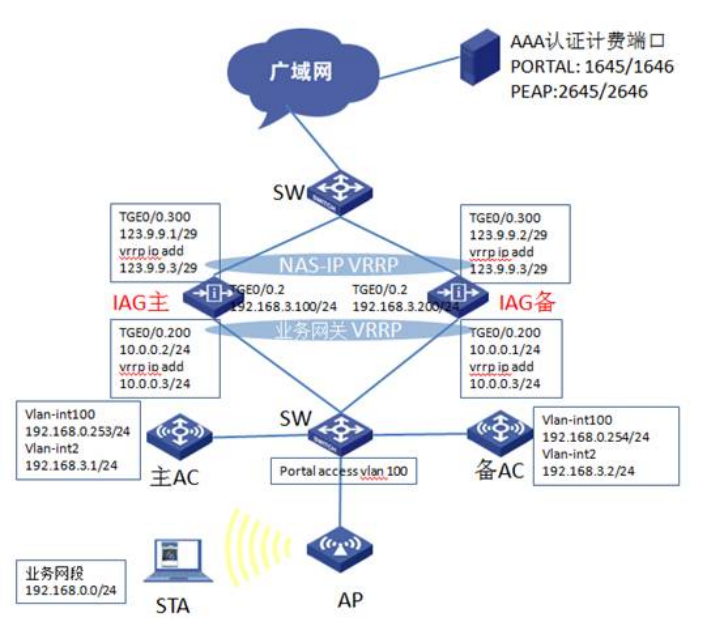
（3）PEAP建议采用单一业务vlan，规避部分终端漫游不通问题；

（4）一般组网建议采用AC做PEAP认证点。IAG支持PEAP应用为次选方案，不推荐！！！

三、组网需求：

按照IAG 1+1备份（PEAP冷备，PORTAL双机热备）进行组网。AC使用的是WX6000系列无线控制器(WX6103)。Client和AP通过DHCP服务器获取IP地址(DHCP服务器配置略)。各设备和接口情况如下图，AP使用vlan100上线, sta的业务vlan为vlan 200（10.0.0.0/24），WX6103和IAG之间的IACTP隧道使用vlan2建立。

四、组网图：



五、配置方法：

1．配置思路

- 在AC上配置漫游组、端口安全代理模式等
- 在IAG上配置RADIUS方案、doamin、端口安全模式、VRRP等
- 配置radius服务器
- 关于nas-id：PORTAL业务的nas-id建议沿用原来的nas-id profile配置；PEAP业务的nas-id通过漫游隧道取自AC。即IAG上配置portal的nas-id，AC上配置PEAP的nas-id。

2．配置步骤

(1) 主AC上的配置信息:

```
dis cur
#
 version 5.20, Release 2308P07
#
 sysname WX6103
#
 domain default enable system
#
 telnet server enable
#
 port-security enable                                    //端口安全
#
 dot1x authentication-method eap                         //dot1x  EAP模式
#
 wlan backup-ac ip 192.168.0.254                         //配置备份AC
 hot-backup vlan 2
 hot-backup enable domain 1
#
 wlan rfid-tracking enable
#
acl number 2001
 rule 0 permit source 192.168.0.0 0.0.0.255
 rule 1 permit
#
vlan 1
#
vlan 2
#
vlan 100
#
vlan 200
#
dhcp server ip-pool vlan100                              //配置AP管理地址pool
 network 192.168.0.0 mask 255.255.0.0
 network ip range 192.168.0.1 192.168.0.253
 gateway-list 192.168.0.254
#
local-user admin
 authorization-attribute level 3
 service-type ssh telnet
 service-type web
#
wlan rrm
 dot11a mandatory-rate 6 12 24
 dot11a supported-rate 9 18 36 48 54
 dot11b mandatory-rate 1 2
 dot11b supported-rate 5.5 11
 dot11g mandatory-rate 1 2 5.5 11
 dot11g supported-rate 6 9 12 18 24 36 48 54
 dot11n protection enable
#
wlan service-template 1 crypto                           //CMCC-AUTO 服务模板
 ssid CMCC-AUTO
 bind WLAN-ESS 1
 cipher-suite ccmp
 security-ie rsn
 service-template enable
#
wlan service-template 2 clear                            //CMCC 服务模板
 ssid CMCC
 bind WLAN-ESS 2
service-template enable
#
```

```
interface NULL0
#
interface Vlan-interface100                          //AP隧道三层接口
 ip address 192.168.0.253 255.255.255.0
#
interface Vlan-interface2                    //和IAG iactp漫游隧道接口
 ip address 192.168.3.1 255.255.255.0
#
interface M-GigabitEthernet1/0/0
#
interface Ten-GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan all
 flow-interval 5
#
interface WLAN-ESS1                          //CMCC-AUTO ESS虚接口
 port link-type hybrid
 undo port hybrid vlan 1
 mac-vlan enable
 port-security port-mode userlogin-secure-ext
 port-security tx-key-type 11key
 port-security remote-auth-proxy enable          //配置dot1x代理认证
 undo dot1x multicast-trigger
 undo dot1x handshake
#
interface WLAN-ESS2                          //CMCC ESS虚接口
 port link-type hybrid
 undo port hybrid vlan 1
 mac-vlan enable
#
wlan ap testap1 model WA2610E-AGN id 2                  //AP服务模板
 priority level 7
 serial-id 210235A35U0087000023
 undo broadcast-probe reply
 radio 1
  service-template 1 vlan 200 nas-id 3507071027000460
 //关联CMCC-AUTO服务模板，绑定nas-id
  service-template 2 vlan 200
//关联CMCC服务模板，nas-id不配置.IAG上的nas-id profile配置生效
  radio enable
#
wlan mobility-group 1
//配置到IAG漫游组，用于上传ssid、bssid、nas-id，代理1x认证加密key下发，
 member ip 192.168.3.100
 member ip 192.168.3.200
 source ip 192.168.3.1
 authentication-mode MD5 simple 123456
 mobility-group enable
#
wlan rrm-calibration-group 1
#
 ip route-static 0.0.0.0 0.0.0.0 192.168.3.100
#
 dhcp enable
#
 arp-snooping enable
#
user-interface con 0
user-interface vty 0 4
 authentication-mode none
 user privilege level 3
#
return
```

（2）备AC上的配置信息：略

（3）主IAG上的配置信息：

```
dis cur
#
 version 5.20, Release 7510P06
#
 sysname IAG
#
 super password level 3 cipher X7A'-%9#+WZ/3:L02.;;!Q!!
#
 configure-user count 8
#
 nas device-id 1              //portal  1+1热备份，主备device-id分别为1和2
#
 domain default enable system
#
 user-isolation vlan 200 enable                          //用户隔离
 user-isolation vlan 200 permit-mac 0000-5e00-0102
#
 portal server cmcc ip 221.176.1.140 url http://221.176.1.140/wlan/index.php
                                  //portal server
 portal free-rule 1 source any destination ip 211.136.17.107 mask 255.255.255.255
                                  //放通DNS
 portal free-rule 2 source any destination ip 10.0.0.3 mask 255.255.255.255
                        //放通网关
 portal device-id 0004.0431.431.00                       //配置AC NAME
#
 port-security enable                                    //端口安全
#
 dot1x authentication-method eap                         //EAP模式
#
radius scheme cmcc-auto                                  //eap的radius策略
 server-type extended
 primary authentication 221.176.1.138 2645               //peap认证端口号2645
 primary accounting 221.176.1.138 2646                   //peap计费端口号2646
 key authentication 88----89
 key accounting 88----89
 timer realtime-accounting 3
 user-name-format keep-original
 nas-ip 123.9.9.3                        //eap的nas-ip，使用vrrp虚地址
 retry stop-accounting 10
#
radius scheme cmcc                                       //portal的radius策略
 server-type extended
 primary authentication 221.176.1.138 1645               //认证端口号1645
 primary accounting 221.176.1.138 1646                   //计费端口号1646
 key authentication cipher abQuGU4cQTpZL8rzyG52eg==
 key accounting cipher abQuGU4cQTpZL8rzyG52eg==
 timer realtime-accounting 3
 user-name-format keep-original
 nas-ip 123.9.9.3
 retry stop-accounting 10
#
aaa nas-id profile mobile                //配置portal业务radius的nas-id，与peap的nas-id无关，pe
ap业务的nas-id 通过lactp隧道取自AC上的配置
 nas-id 0010043143100460 bind vlan 200
 nas-id 0011043143100460 bind vlan 201
 nas-id 0012043143100460 bind vlan 202
#
domain cmcc-auto                                         //eap的domain域
 authentication lan-access radius-scheme cmcc-auto
 authorization lan-access radius-scheme cmcc-auto
 accounting lan-access radius-scheme cmcc-auto
```

```
 access-limit disable
 state active
 idle-cut enable 15 10000                    //按需要配置，集团暂时没有规范
 self-service-url disable
#
domain cmcc                                  //portal的domain域
 authentication portal radius-scheme cmcc
 authorization portal radius-scheme cmcc
 accounting portal radius-scheme cmcc
 access-limit disable
 state active
 idle-cut enable 15 10000
 self-service-url disable
#
dhcp server ip-pool userclient_dhcp_server      // cmcc、cmcc-auto业务地址池
 network 10.0.0.0 mask 255.255.255.0
 gateway-list 10.0.0.3
 dns-list 211.137.58.20 211.136.17.107
 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-GigabitEthernet0/0.300            //nas-ip接口
 vlan-type dot1q vid 100
 ip address 123.9.9.1 255.255.255.248
 vrrp vrid 1 virtual-ip 123.9.9.3
 vrrp vrid 1 priority 150
#
interface Ten-GigabitEthernet0/0.2          //iag、ac漫游lactp隧道接口
 vlan-type dot1q vid 2
 ip add 192.168.3.100 255.255.255.0
#
interface Ten-GigabitEthernet0/0.200            //业务网关接口
 vlan-type dot1q vid 200 to 207 221             //模糊vlan终结
 ip address 10.0.0.2 255.255.255.0              //配置实ip地址
 vrrp dot1q vid 200                             //配置vrrp控制vlan
 vrrp vrid 1 virtual-ip 10.0.0.3                //配置vrrp虚地址
 vrrp vrid 1 priority 150                       //配置vrrp优先级
 arp authorized enable                          //使能授权arp
 arp send-gratuitous-arp interval 60000         //配置免费arp发送间隔
 dhcp update arp                                //配置授权arp
 port-security port-mode userlogin-secure-ext   //配置dot1x
 port-security vrrp-virtual-ip 123.9.9.3        //配置由vrrp主设备处理认证报文
 port-security wlan-access                      //配置无线1x代理认证
 dot1x mandatory-domain cmcc-auto               //配置1x强制认证域
 undo dot1x handshake
 undo dot1x multicast-trigger
```

```
 portal server cmcc method direct                    //指定portal server
 portal domain cmcc                                  //配置portal强制认证域
 portal nas-id-profile mobile                        //绑定portal nas-id-profile
 portal nas-port-type wireless
 portal nas-ip 123.9.9.3                             //指定portal nas-ip
 portal backup-group 1                               //portal备份组
 access-user detect type arp retransmit 5 interval 30          //在线用户检测
#
wlan mobility-group 1                                //配置漫游组
 member ip 192.168.3.1
 member ip 192.168.3.2
 source ip 192.168.3.100
 authentication-mode MD5 123456                      //配置漫游隧道md5验证
 mobility-group enable
#
 ip route-static 0.0.0.0 0.0.0.0 123.9.9.4
#
 undo info-center enable
#
 snmp-agent
 snmp-agent local-engineid 800063A203000FE2000001
 snmp-agent community read ^%dsU!!
 snmp-agent community write ^%dsU!!
 snmp-agent sys-info version all
 snmp-agent target-host trap address udp-domain 221.9.0.11 params securityname public
v2c
#
 nqa schedule cl2topo ping start-time now lifetime 630720000
#
 arp timer aging 1440
#
 load xml-configuration
#
user-interface con 0
 idle-timeout 35791 0
user-interface aux 0
user-interface vty 0 4
 authentication-mode scheme
#
return
```

（4）备IAG上的配置信息：

```
dis cur
#
 version 5.20, Release 7510P06
#
 sysname IAG
#
 super password level 3 cipher X7A'-%9#+WZ/3:L02.;;!Q!!
#
 configure-user count 8
#
 nas device-id 2                //portal  1+1热备份，主备device-id分别为1和2
#
 domain default enable system
#
 user-isolation vlan 200 enable                      //用户隔离
 user-isolation vlan 200 permit-mac 0000-5e00-0102
#
 portal server cmcc ip 221.176.1.140 url http://221.176.1.140/wlan/index.php
                                                     //portal server
 portal free-rule 1 source any destination ip 211.136.17.107 mask 255.255.255.255
                                                     //放通DNS
 portal free-rule 2 source any destination ip 10.0.0.3 mask 255.255.255.255
```

```
                                                    //放通网关
 portal device-id 0004.0431.431.00                  //配置AC NAME
#
 port-security enable                               //端口安全
#
 dot1x authentication-method eap                    //EAP模式
#
radius scheme cmcc-auto                             //eap的radius策略
 server-type extended
 primary authentication 221.176.1.138 2645          //peap认证端口号2645
 primary accounting 221.176.1.138 2646              //peap计费端口号2646
 key authentication 88----89
 key accounting 88----89
 timer realtime-accounting 3
 user-name-format keep-original
 nas-ip 123.9.9.3                                  //eap的nas-ip，使用vrrp虚地址
 retry stop-accounting 10
#
radius scheme cmcc                                  //portal的radius策略
 server-type extended
 primary authentication 221.176.1.138 1645          //认证端口号1645
 primary accounting 221.176.1.138 1646              //计费端口号1646
 key authentication cipher abQuGU4cQTpZL8rzyG52eg==
 key accounting cipher abQuGU4cQTpZL8rzyG52eg==
 timer realtime-accounting 3
 user-name-format keep-original
 nas-ip 123.9.9.3
 retry stop-accounting 10
#
aaa nas-id profile mobile                           //配置portal业务radius的nas-id
 nas-id 0010043143100460 bind vlan 200
 nas-id 0011043143100460 bind vlan 201
 nas-id 0012043143100460 bind vlan 202
#
domain cmcc-auto                                    //eap的domain域
 authentication lan-access radius-scheme cmcc-auto
 authorization lan-access radius-scheme cmcc-auto
 accounting lan-access radius-scheme cmcc-auto
 access-limit disable
 state active
 idle-cut enable 15 10000                           //按需要配置，集团暂时没有规范
 self-service-url disable
#
domain cmcc                                         //portal的domain域
 authentication portal radius-scheme cmcc
 authorization portal radius-scheme cmcc
 accounting portal radius-scheme cmcc
 access-limit disable
 state active
 idle-cut enable 15 10000
 self-service-url disable
#
dhcp server ip-pool userclient_dhcp_server          // cmcc、cmcc-auto业务地址池
 network 10.0.0.0 mask 255.255.255.0
 gateway-list 10.0.0.3
 dns-list 211.137.58.20 211.136.17.107
 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-GigabitEthernet0/0.300                    //nas-ip接口
 vlan-type dot1q vid 100
 ip address 123.9.9.2 255.255.255.248
 vrrp vrid 1 virtual-ip 123.9.9.3
 vrrp vrid 1 priority 100
#
interface Ten-GigabitEthernet0/0.2          //iag、ac漫游lactp隧道接口
 vlan-type dot1q vid 2
 ip address 192.168.3.200 255.255.255.0
#
interface Ten-GigabitEthernet0/0.200                    //业务网关接口
 vlan-type dot1q vid 200 to 207 221                     //模糊vlan终结
 ip address 10.0.0.1 255.255.255.0                      //配置实ip地址
 vrrp dot1q vid 200                                  //配置vrrp控制vlan
 vrrp vrid 1 virtual-ip 10.0.0.3                        //配置vrrp虚地址
 vrrp vrid 1 priority 100                            //配置vrrp优先级
 arp authorized enable                                  //使能授权arp
 arp send-gratuitous-arp interval 60000                 //配置免费arp发送间隔
 dhcp update arp                                        //配置授权arp
 port-security port-mode userlogin-secure-ext                   //配置dot1x
 port-security vrrp-virtual-ip 123.9.9.3        //配置由vrrp主设备处理认证报文
 port-security wlan-access                          //配置无线1x代理认证
 dot1x mandatory-domain cmcc-auto                       //配置1x强制认证域
 undo dot1x handshake
 undo dot1x multicast-trigger
 portal server cmcc method direct                       //指定portal server
 portal domain cmcc                                  //配置portal强制认证域
 portal nas-id-profile mobile                   //绑定portal nas-id-profile
 portal nas-port-type wireless
 portal nas-ip 123.9.9.3                            //制定portal nas-ip
 portal backup-group 1                                  //portal备份组
 access-user detect type arp retransmit 5 interval 30           //在线用户检测
#
wlan mobility-group 1                                   //配置漫游组
 member ip 192.168.3.1
 member ip 192.168.3.2
 source ip 192.168.3.200
 authentication-mode MD5 123456                         //配置漫游隧道md5验证
 mobility-group enable
#
 ip route-static 0.0.0.0 0.0.0.0 123.9.9.4
#
 undo info-center enable
#
 snmp-agent
 snmp-agent local-engineid 800063A203000FE2000001
 snmp-agent community read ^%dsU!!
 snmp-agent community write ^%dsU!!
 snmp-agent sys-info version all
 snmp-agent target-host trap address udp-domain 221.9.0.11 params securityname public
v2c #
```

```
 nqa schedule cl2topo ping start-time now lifetime 630720000
#
 arp timer aging 1440
#
 load xml-configuration
#
user-interface con 0
 idle-timeout 35791 0
user-interface aux 0
user-interface vty 0 4
 authentication-mode scheme
#
return
```

（5）RADIUS服务器设置：略

3．配置关键点

（1）WX6103上进行配置：

启用端口安全port-security。

[WX6103] port-security enable

创建WLAN-ESS1接口，并进入该视图。

[WX6103] interface WLAN-ESS 1

设置端口的安全模式为userlogin-secure-ext。

[WX6103-WLAN-ESS1] port-security port-mode userlogin-secure-ext

在接口WLAN-ESS1下使能11key类型的密钥协商功能。

[WX6103-WLAN-ESS1]port-security tx-key-type 11key

在接口WLAN-ESS1下使能端口安全代理功能。

[WX6103-WLAN-ESS1] port-security remote-auth-proxy enable

关闭802.1X的组播触发功能。

[WX6103-WLAN-ESS1] undo dot1x multicast-trigger

#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crypto类型的服务模板1。

[WX6103] wlan service-template 1 crypto

设置当前服务模板的SSID（服务模板的标识）为CMCC-AUTO。

[WX6103-wlan-st-1] ssid CMCC-AUTO

将WLAN-ESS1接口绑定到服务模板1。

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

使能ccmp加密套件。

[WX6103-wlan-st-1] cipher-suite ccmp

[WX6103-wlan-st-1] security-ie rsn

使能无线模板。

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

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testap1，型号名称这里选择WA2620E-AGN。

[WX6103] wlan ap testap1 model WA2620E-AGN

设置AP的序列号为210235A35VB095000042。

[WX6103-wlan-ap-testap1] serial-id 210235A35VB095000042

进入radio2射频视图。

[WX6103-wlan-ap-testap1] radio 2

将在AC上配置的服务模板1与射频2进行关联,并帮定vlan和nas-id属性。

[WX6103-wlan-ap-testap1-radio-2] service-template 1 vlan 200 nas-id 3507071027000460

#手动指定信道为11

[WX6103-wlan-ap-testap1-radio-2] channel 11

使能testap1的radio 2

[WX6103-wlan-ap-testap1-radio-2] radio enable

[WX6103-wlan-ap-testap1-radio-2] quit

[WX6103-wlan-ap-testap1] quit

#配置WLAN漫游组

[WX6103] wlan mobility-group 1

#配置源IP地址

[WX6103-wlan-mg-1] source ip 192.168.3.1

#添加漫游组成员（包含IAG1和IAG2）

[WX6103-wlan-mg-1] member ip 192.168.3.100

[WX6103-wlan-mg-1] member ip 192.168.3.200

#配置IACTP控制消息完整性认证模式(可选)

[WX6103-wlan-mg-1] authentication-mode MD5 simple 123456

#开启IACTP服务

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

[WX6103-wlan-mg-1] quit

（2）IAG1上进行配置：

启用端口安全port-security，配置Dot1x认证方式为EAP。

[IAG1] port-security enable

[IAG1] dot1x authentication-method eap

创建radius方案system并进入其视图。

[IAG1] radius scheme cmcc-auto

配置PEAP认证/计费RADIUS服务器的IP地址。

[IAG1-radius-cmcc-auto] primary authentication 221.176.1.138 2645

[IAG1-radius-cmcc-auto] primary accounting 221.176.1.138 2646

配置Device与认证/计费RADIUS服务器交互报文时的共享密钥。

[IAG1-radius-cmcc-auto] key authentication 88----89

[IAG1-radius-cmcc-auto] key accounting 88----89

#设置设备发送RADIUS报文使用的源地址

[IAG1-radius-cmcc-auto] nas-ip 123.9.9.3

配置发送给RADIUS服务器的用户名不携带域名。

[IAG1-radius-cmcc-auto] user-name-format without-domain

[IAG1-radius-cmcc-auto] quit

创建域cmcc-auto并进入其视图。

[IAG1] domain cmcc-auto

配置802.1X用户使用RADIUS方案system进行认证、授权、计费。

[IAG1-isp-cmcc-auto] authentication lan-access radius-scheme cmcc-auto

[IAG1-isp-cmcc-auto] authorization lan-access radius-scheme cmcc-auto

[IAG1-isp-cmcc-auto] accounting lan-access radius-scheme cmcc-auto

关闭该域最多可容纳用户限制功能。

[IAG1-isp-cmcc-auto] 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10000 Byte时则切断其连接。（此配置项根据实际情况可选,集团暂时没有统一规范）

[IAG1-isp-cmcc-auto] idle-cut enable 15 10000

[IAG1-isp-cmcc-auto] quit

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。

[IAG1] domain default enable system

在TG0/0.100上配置VRRP，使主备IAG都使用相同的源IP地址和radius server进行报文交互。

[IAG1] interface Ten-GigabitEthernet0/0.10

[IAG1-Ten-GigabitEthernet0/0.100] vlan-type dot1q vid 100

[IAG1-Ten-GigabitEthernet0/0.100] ip address 123.9.9.1 255.255.255.248

[IAG1-Ten-GigabitEthernet0/0.100] vrrp vrid 1 virtual-ip 123.9.9.3

[IAG1-Ten-GigabitEthernet0/0.100] vrrp vrid 1 priority 150

创建TG0/0.200接口作为业务网关，并进入该视图。

[IAG1] interface Ten-GigabitEthernet 0/0.200

#配置此端口模糊VLAN终结

[IAG1-Ten-GigabitEthernet0/0.200] vlan-type dot1q vid 200 to 207 221

#配置此端口的实IP地址

[IAG1-Ten-GigabitEthernet0/0.200] ip address 10.0.0.1 255.255.255.0

#配置VRRP控制VLAN

[IAG1-Ten-GigabitEthernet0/0.200] vrrp dot1q vid 200

#配置VRRP虚地址

[IAG1-Ten-GigabitEthernet0/0.200] vrrp vrid 1 virtual-ip 10.0.0.3

#配置VRRP优先级

[IAG1-Ten-GigabitEthernet0/0.200] vrrp vrid 1 priority 150

#配置授权ARP和免费ARP发送间隔

[IAG1-Ten-GigabitEthernet0/0.200] arp authorized enable

[IAG1-Ten-GigabitEthernet0/0.200] arp send-gratuitous-arp interval 60000

[IAG1-Ten-GigabitEthernet0/0.200] dhcp update arp

设置端口的安全模式为userlogin-secure-ext。

[IAG1-Ten-GigabitEthernet0/0.200] port-security port-mode userlogin-secure-ext

在此端口下配置NAS IP（IAG 1+1备份时使用，通过这个ip区分那个是vrrp主设备，由主设备处理认证报文）。

[IAG1-Ten-GigabitEthernet0/0.200] port-security vrrp-virtual-ip 123.9.9.3

在此端口下配置端口安全无线接入。

[IAG1-Ten-GigabitEthernet0/0.200] port-security wlan-access

配置1x强制认证域。

[IAG1-Ten-GigabitEthernet0/0.200] dot1x mandatory-domain cmcc-auto

取消1x认证握手功能和组播触发功能

[IAG1-Ten-GigabitEthernet0/0.200] undo dot1x handshake

[IAG1-Ten-GigabitEthernet0/0.200] dot1x multicast-trigger

#配置portal认证

[IAG1-Ten-GigabitEthernet0/0.200] portal server cmcc method direct

[IAG1-Ten-GigabitEthernet0/0.200] portal domain cmcc

[IAG1-Ten-GigabitEthernet0/0.200] portal nas-id-profile mobile

[IAG1-Ten-GigabitEthernet0/0.200] portal nas-port-type wireless

[IAG1-Ten-GigabitEthernet0/0.200] portal nas-ip 123.9.9.3

[IAG1-Ten-GigabitEthernet0/0.200] portal backup-group 1

[IAG1-Ten-GigabitEthernet0/0.200] access-user detect type arp retransmit 5 interval 30

#配置WLAN漫游组

[IAG1] wlan mobility-group 1

#配置源IP地址

[IAG1-wlan-mg-1] source ip 192.168.3.100

#添加漫游组成员

[IAG1-wlan-mg-1] member ip 192.168.3.1

[IAG1-wlan-mg-1] member ip 192.168.3.2

#配置IACTP控制消息完整性认证模式(可选)

[IAG1-wlan-mg-1] authentication-mode MD5 simple 123456

#开启IACTP服务

[IAG1-wlan-mg-1] mobility-group enable

[IAG1-wlan-mg-1] quit

（3）IAG2上进行配置：

启用端口安全port-security，配置Dot1x认证方式为EAP。

[IAG2] port-security enable

[IAG2] dot1x authentication-method eap

创建radius方案system并进入其视图。

[IAG2] radius scheme cmcc-auto

配置PEAP认证/计费RADIUS服务器的IP地址。

[IAG2-radius-cmcc-auto] primary authentication 221.176.1.138 2645

[IAG2-radius-cmcc-auto] primary accounting 221.176.1.138 2646

配置Device与认证/计费RADIUS服务器交互报文时的共享密钥。

[IAG2-radius-cmcc-auto] key authentication 88----89

[IAG2-radius-cmcc-auto] key accounting 88----89

#设置设备发送RADIUS报文使用的源地址

[IAG2-radius-cmcc-auto] nas-ip 123.9.9.3

配置发送给RADIUS服务器的用户名不携带域名。

[IAG2-radius-cmcc-auto] user-name-format without-domain

[IAG2-radius-cmcc-auto] quit

创建域cmcc-auto并进入其视图。

[IAG2] domain cmcc-auto

配置802.1X用户使用RADIUS方案system进行认证、授权、计费

[IAG2-isp-cmcc-auto] authentication lan-access radius-scheme cmcc-auto

[IAG2-isp-cmcc-auto] authorization lan-access radius-scheme cmcc-auto

[IAG2-isp-cmcc-auto] accounting lan-access radius-scheme cmcc-auto

关闭该域最多可容纳用户限制功能。

[IAG2-isp-cmcc-auto] 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10000 Byte时则切断其连接。（此配置项根据实际情况可选,集团暂时没有统一规范）

[IAG2-isp-cmcc-auto] idle-cut enable 15 10000

[IAG2-isp-cmcc-auto] quit

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。

[IAG2] domain default enable system

在TG0/0.100上配置VRRP，使主备IAG都使用相同的源IP地址和radius server进行报文

交互。

[IAG2] interface Ten-GigabitEthernet0/0.100

[IAG2-Ten-GigabitEthernet0/0.100] vlan-type dot1q vid 100

[IAG2-Ten-GigabitEthernet0/0.100] ip address 123.9.9.2 255.255.255.248

[IAG2-Ten-GigabitEthernet0/0.100] vrrp vrid 1 virtual-ip 123.9.9.3

[IAG2-Ten-GigabitEthernet0/0.100] vrrp vrid 1 priority 100

创建TG0/0.200接口作为业务网关，并进入该视图。

[IAG2] interface Ten-GigabitEthernet 0/0.200

#配置此端口模糊VLAN终结

[IAG2-Ten-GigabitEthernet0/0.200] vlan-type dot1q vid 200 to 207 221

#配置此端口的实IP地址

[IAG2-Ten-GigabitEthernet0/0.200] ip address 10.0.0.2 255.255.255.0

#配置VRRP控制VLAN

[IAG2-Ten-GigabitEthernet0/0.200] vrrp dot1q vid 200

#配置VRRP虚地址

[IAG2-Ten-GigabitEthernet0/0.200] vrrp vrid 1 virtual-ip 10.0.0.3

#配置VRRP优先级

[IAG2-Ten-GigabitEthernet0/0.200] vrrp vrid 1 priority 100

#配置授权ARP和免费ARP发送间隔

[IAG2-Ten-GigabitEthernet0/0.200] arp authorized enable

[IAG2-Ten-GigabitEthernet0/0.200] arp send-gratuitous-arp interval 60000

[IAG2-Ten-GigabitEthernet0/0.200] dhcp update arp

设置端口的安全模式为userlogin-secure-ext。

[IAG2-Ten-GigabitEthernet0/0.200] port-security port-mode userlogin-secure-ext

在此端口下配置NAS IP（IAG 1+1备份时使用，通过这个ｉｐ区分那个是ｖｒｒｐ主设备，由主设备处理认证报文）。

[IAG2-Ten-GigabitEthernet0/0.200] port-security vrrp-virtual-ip 123.9.9.3

在此端口下配置端口安全无线接入。

[IAG2-Ten-GigabitEthernet0/0.200] port-security wlan-access

配置1x强制认证域。

[IAG2-Ten-GigabitEthernet0/0.200] dot1x mandatory-domain cmcc-auto

取消1x认证握手功能和组播触发功能

[IAG2-Ten-GigabitEthernet0/0.200] undo dot1x handshake

[IAG2-Ten-GigabitEthernet0/0.200] dot1x multicast-trigger

#配置portal认证

[IAG2-Ten-GigabitEthernet0/0.200] portal server cmcc method direct

[IAG2-Ten-GigabitEthernet0/0.200] portal domain cmcc

[IAG2-Ten-GigabitEthernet0/0.200] portal nas-id-profile mobile

[IAG2-Ten-GigabitEthernet0/0.200] portal nas-port-type wireless

[IAG2-Ten-GigabitEthernet0/0.200] portal nas-ip 123.9.9.3

[IAG2-Ten-GigabitEthernet0/0.200] portal backup-group 1

[IAG2-Ten-GigabitEthernet0/0.200] access-user detect type arp retransmit 5 interval 30

#配置WLAN漫游组

[IAG2] wlan mobility-group 1

#配置源IP地址

[IAG2-wlan-mg-1] source ip 192.168.3.200

#添加漫游组成员

[IAG2-wlan-mg-1] member ip 192.168.3.1

[IAG2-wlan-mg-1] member ip 192.168.3.2

#配置IACTP控制消息完整性认证模式(可选)

[IAG2-wlan-mg-1] authentication-mode MD5 simple 123456

#开启IACTP服务

[IAG2-wlan-mg-1] mobility-group enable

[IAG2-wlan-mg-1] quit

六、验证结果：

（1）在IAG上使用命令行display connection查看是否有用户在线。

```
display  connection
index=5   ,Username=client@cmcc-auto
MAC=00-19-5B-EC-7A-E9
IP=N/A
IPv6=N/A
 Total 1 connection(s) matched.
```

（2）在IAG上通过命令行display connection ucibindex查看用户的较详细信息

```
display  connection  ucibindex  5
Index=5   , Username=client@cmcc-auto
MAC=00-19-5B-EC-7A-E9
IP=N/A
IPv6=N/A
Access=8021X   ,AuthMethod=EAP
Port Type=Wireless-802.11,Port Name=WLAN-DBSS0:2
Initial VLAN=200, Authorization VLAN=N/A
ACL Group=Disable
User Profile=N/A
CAR=Disable
Priority=Disable
Start=2011-10-14 15:24:21 ,Current=2011-10-14 18:29:24 ,Online=03h05m03
s
 Total 1 connection matched
```

（3）如果有Dot1x用户在线，在无线控制器上通过命令display wlan client verbose查看相应用户

```
display  wlan  client verbose
 Total Number of Clients          : 1
                          Client Information
-------------------------------------------------------------------------------
 MAC Address                    : 0019-5bec-7ae9
 User Name                      : client
 AID                           : 1
 AP Name                         : testap01
 Radio Id                       : 1
 SSID                           : CMCC-AUTO
 BSSID                           : 0023-8998-0450
 Port                           : WLAN-DBSS0:2
 VLAN                            : 200
 State                          : Running
 Power Save Mode                  : Active
 Wireless Mode                    : 11a
 QoS Mode                        : WMM
 Listen Interval (Beacon Interval) : 10
 RSSI                           : 32
 Rx/Tx Rate                      : 54/54
 Client Type                     : WPA2(RSN)
 Authentication Method             : Open System
 AKM Method                      : Dot1X
 4-Way Handshake State             : PTKINITDONE
 Group Key State                  : IDLE
 Encryption Cipher                : AES-CCMP
 Roam Status                     : Normal
```

```
Roam Count                    : 0
Up Time (hh:mm:ss)            : 00:54:47
--------------------------------------------------------------------------------
```