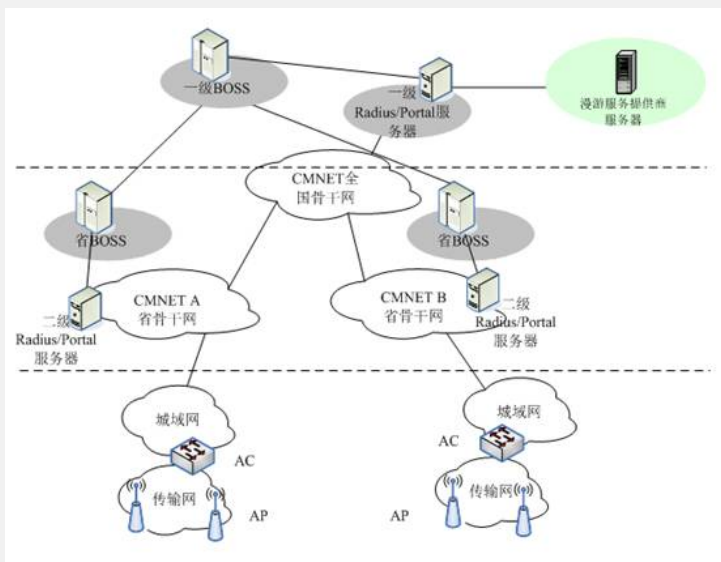


中国移动WLAN二级Portal&多域应用案例

一、中国移动二级Portal架构：

中国移动WLAN用户认证平台架构如下图所示：



Portal设备采用集团、省两级架构。集团一级Portal服务器采用集中建设原则，全网部署一套，面向公众用户及部分省高校用户提供服务。省内二级Portal服务器采用集中建设原则，各省部署一套，面向省内高校用户提供服务。

Radius设备采用集团、省两级Radius架构，集团一级Radius服务器用于中国移动WLAN个人用户、部分集团客户的认证和计费等功能，全网部署一套；省内二级Radius服务器目前仅提供省内高校用户认证、计费等功能，各省部署一套。

二、多域需求：

各省移动为推广自己个性化的业务，在二级Portal上扩充了丰富的业务功能，已经可以完全替代一级Portal。如山东、广东等省已完全弃用集团的一级Portal（除国际漫游业务外），由省内的二级Portal负责所有WLAN业务的Portal页面推送，包括CMCC-EDU、CMCC业务。

省内Portal Server可以负责推送Portal页面，但AAA还是需分流到一级和二级Radius上完成。如果有其他省的漫游用户需要在本省使用WLAN业务，这些外省账号信息就应该送集团Radius处理（注意：移动对WLAN用户账号分层管理，省二级RADIUS只能完成对省内用户的AAA，不能对漫游用户做AAA）。这就需要Portal和AC设备能区分出外省漫游用户和本省用户，并分别上送一级和二级Radius完成认证。认证设备（AC）也需要支持多域功能，即实现对不同的用户（外省漫游、本省用户）分别到不同的Radius认证，当二级Portal Server在向AC设备发起认证时，在用户名信息上携带不同的@后缀名，AC根据后缀名匹配认证域，选择到省内还是集团Radius进行认证。

三、应用案例分析和AC配置说明：

比如某省的WLAN认证平台有如下要求：

1、CMCC的SSID下缺省Portal要求指向省内二级Portal服务器。

2、省内Portal的处理逻辑：

（1）对省内用户，账号加wlan-moni-jituan后缀（如13953110669@wlan-moni-jituan），送给AC，AC需根据此后缀判断送给省内radius认证（且需去掉账号后缀，即@wlan-moni-jituan部分）。

（2）对于外省漫游用户，省内portal不加后缀送给AC，AC送给集团radius认证（不需去掉账号后缀）。

（3）对于国际漫游业务，用户点击后会跳到集团portal，国漫账号带的后缀没有普遍规律，均需送给集团radius认证（不需去掉账号后缀）。

3、AC配置说明，看AC如何适配Portal的处理逻辑。

(1) 强制重定向指向二级Portal服务器，但接口上不指定强制认证域

```
#
portal server cmcc ip 221.176.1.140 url http://221.176.1.140/wlan/index.php server-type cmcc //配置集团一级Portal Server，AC接受来自集团Portal Server的国漫用户认证
portal server shandong ip 211.137.185.106 url http://211.137.185.106:8001/showlogin.do server-type cmcc //配置省内二级Portal Server
portal free-rule 0 source wlan ssid CMCC-AUTO destination any
portal device-id 0344.0531.531.00
#
interface Vlan-interface1101
description GateWay_of_CMCC and CMCC_AUTO
ip address 10.198.0.2 255.255.192.0
vrrp vrid 2 virtual-ip 10.198.0.1
vrrp vrid 2 priority 120
portal server shandong method direct //强制重定向到省内Portal，但接口上不指定强制认证域，认证域根据用户名@后缀域匹配。
portal nas-port-type wireless
portal backup-group 1
portal nas-ip 111.17.233.177
access-user detect type arp retransmit 3 interval 50
#
```

(2) 配置用户名@后缀域和缺省认证域，其中@ wlan-moni-jituan指向省内RADIUS，缺省认证域wlan-jituan指向集团RADIUS

```
#
domain wlan-moni-jituan //省内AAA的认证域，域的名称必须和Portal服务器送过来的@后缀域保持一致
authentication portal radius-scheme wlan-shengnei
authorization portal radius-scheme wlan-shengnei
accounting portal radius-scheme wlan-shengnei
access-limit disable
state active
idle-cut enable 15 10000
self-service-url disable
domain wlan-jituan //集团AAA的认证域，名称自定义
authentication portal radius-scheme wlan-jituan
authorization portal radius-scheme wlan-jituan
accounting portal radius-scheme wlan-jituan
access-limit disable
state active
idle-cut enable 15 10000
self-service-url disable
#
```

(3) 配置省内和集团RADIUS，省内AAA认证时不带账号后缀，集团AAA认证时带账号后缀

```
#
radius scheme wlan-shengnei //省内RADIUS
server-type extended
primary authentication 211.137.185.105
primary accounting 211.137.185.105
```

```
key authentication cipher $c$3$nH3D17gxrRRbVjEB+IUxm5n90btzjjwJrrZ
key accounting cipher $c$3$Bg3tVMVBgSR2Xw26GtPZ1VzGRzLcbqyU7cQi
user-name-format without-domain //省内AAA不带后缀域名认证
nas-ip 111.17.233.177
retry stop-accounting 10
radius scheme wlan-jituan //集团RADIUS
server-type extended
primary authentication 221.176.1.138 1645
primary accounting 221.176.1.138 1646
key authentication cipher $c$3$PwfsSd1eBsbCMOKsxroZcZi9g34g6us87gXt
key accounting cipher $c$3$nMF7zBCyKiJ9/lx/szEDM48AJiDFiLIUjh2i
user-name-format keep-original //集团AAA带后缀域名认证
nas-ip 111.17.233.177
retry stop-accounting 10
```

#

(4) 指定全局缺省认证域，以适配当@后缀域不存在或者无法匹配的情况

#

```
domain default enable wlan-jituan //配置@后缀域不存在的用户到集团AAA认证
```

```
domain if-unknown wlan-jituan //配置当@后缀域无法匹配时到集团AAA认证，如国际漫游用户
```

#

四、AC的域优先级说明：

AC对认证用户需要选择认证策略，即针对用户匹配认证域Domain。设备上有多个地方可以配置认证域信息，各种配置方式的生效优先级有区别。

优先级顺序如下（由高到低）：

(1) 全局根据SSID和AP热点指定使用的Portal认证域；

命令：portal wlan ssid XXXX server YYYY domain ZZZZ

```
<H3C>display current-configuration
#
portal wlan ssid CMCC server cmcc-portal domain cmcc-wlan
```

(2) 三层接口下强制Portal认证域；

命令：portal domain ZZZZ

```
<H3C>display current-configuration
#
interface Vlan-interface1102
portal domain cmcc-wlan
```

(3) 用户名携带的"@后缀名"匹配域；

(4) 全局domain default；

命令：domain default ZZZZ

```
<H3C>display current-configuration
#
domain default cmcc-wlan
```

注意：如果（1）、（2）、（3）按优先级顺序匹配过程中出现指定的域在AC全局并没有定义，则走全局domain if-unknown配置；如果domain if-unknown没有配置则认证失败；

命令：domain if-unknown ZZZZ

```
<H3C>display current-configuration
#
domain if-unknown cmcc-wlan
```

