iMC BYOD解决方案中关于根据不同终端MAC地址分配不同IP地址的典型配置

BYOD 何颖 2013-06-09 发表

iMC BYOD解决方案中关于根据不同终端MAC地址分配不同IP地址的典型配置

一、 组网需求：

很多网络环境中，需要根据不同的终端MAC分配不同的IP地址，以解决信息安全的某种需求。H3C iMC BYOD解决方案提供了便捷灵活的接入场景策略，可以满足针对不同终端MAC分配不同IP地址的需求，同时还可以利用BYOD本身的丰富特性更加合理的管理各种终端。

二、 组网图：

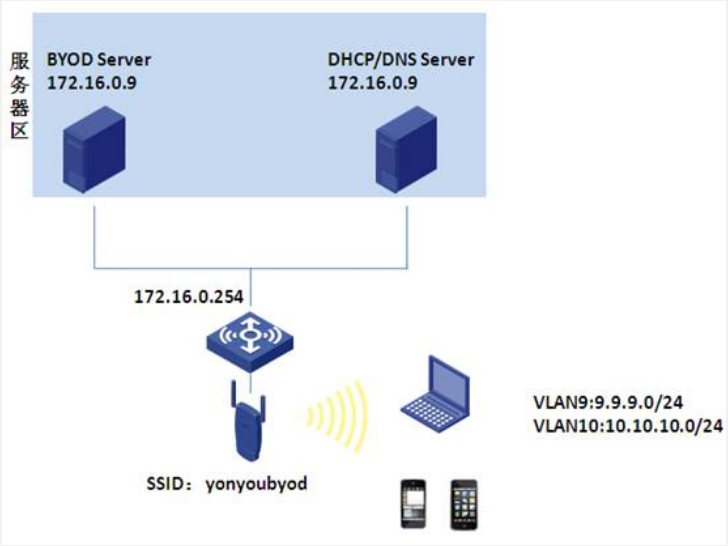

图1 组网图

具体说明如下：

BYOD Server：IP地址为172.16.0.9，测试软件版本为iMC PLAT 5.2 E0401H03+iMC UAM 5.2 E0402P05

DHCP/DNS Server：案例中跟BYOD Server为同一台服务器（实际项目中建议为单独的服务器），划分三个地址池，分别为私网网段地址池9.9.9.0/24、办公网网段地址池10.10.10.0/24。

三、 配置步骤：

案例中服务器区的服务器与AC网络可达。终端通过SSID　yonyoubyod接入无线网络。测试中以两台PC（PCA和PCB）作为测试点。在AC上配置MAC地址认证。

PCA首次接入无线网络，后台自动去往BYOD Server完成MAC认证，DHCP根据BYOD Server上的策略为PCA分配9.9.9.0/24的IP地址。PCA重定向到BYOD界面完成终端注册，关联已知帐号pca，DHCP根据注册后策略重新为其分配10.10.10.0/24网段地址。

办公PCB首次接入无线网络，后台自动去往BYOD Server完成MAC认证，BYOD Server事先导入PCB MAC地址和已知帐号pcb绑定，BYOD Server根据MAC地址判断该终端合法性，根据策略配合DHCP为其分配10.10.10.0/24地址。

具体配置如下：

1. 首先完成DHCP/DNS Server的配置，规划好各类地址池。
2. 完成AC的配置：

[AC]

#

version 5.20, Release 3111P12

#

```
 sysname AC
#
 dhcp relay server-group 1 ip 172.16.0.9
#
 domain default enable ead
#
 telnet server enable
#
 port-security enable
#
 mac-authentication domain byod
#
 sysnetid AC
#
 oap management-ip 192.168.0.101 slot 0
#
 wlan auto-ap enable
#
vlan 1
#
vlan 8 to 11
#
vlan 172
#
radius scheme byod
 server-type extended
 primary authentication 172.16.0.9
 primary accounting 172.16.0.9
 key authentication 123
 key accounting 123
#
domain byod
 authentication lan-access radius-scheme byod
 authorization lan-access radius-scheme byod
 accounting lan-access radius-scheme byod
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
domain system
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#
dhcp server ip-pool ap
 network 8.8.8.0 mask 255.255.255.0
```

```
 gateway-list 8.8.8.254
#
user-group system
#
local-user admin
 password simple admin
 authorization-attribute level 3
 service-type telnet
#
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
#
wlan service-template 1 clear
 ssid yonyoubyod
 bind WLAN-ESS 1
 service-template enable
#
interface NULL0
#
interface Vlan-interface1
#
interface Vlan-interface8
 ip address 8.8.8.254 255.255.255.0
#
interface Vlan-interface9
 description 隔离IP
 ip address 9.9.9.1 255.255.255.0
 dhcp select relay
 dhcp relay server-select 1
#
interface Vlan-interface10
 description 公网IP
 ip address 10.10.10.1 255.255.255.0
 dhcp select relay
 dhcp relay server-select 1
 portal server ead method direct
#
interface Vlan-interface172
 ip address 172.16.0.254 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
```

```
 port trunk permit vlan all
#
interface WLAN-ESS1
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 9 untagged
 port hybrid pvid vlan 9
 mac-vlan enable
 port-security port-mode mac-authentication
#
wlan ap ap1 model WA2220-AG id 1
 serial-id 210235A29E0087000090
 radio 1
  service-template 1
  radio enable
 radio 2
  service-template 1
  radio enable
#
 dhcp enable
#
 load xml-configuration
#
user-interface aux 0
user-interface vty 0 4
 authentication-mode scheme
 user privilege level 3
#
return
```

3. BYOD Server配置

1） 登录BYOD Server界面，点击【业务】|【用户接入管理】|【业务参数配置】|【系统配置】|【BYOD系统参数配置】，选择“启用快速认证功能”。另外，单帐号最多MAC数等其他业务参数根据实际业务需求进行调整。

2） 在【业务】|【用户接入管理】|【接入场景管理】|【接入MAC地址组管理】中增加/批量导入PCB及其他测试终端的MAC地址。预留PCA的MAC地址（24:77:03:90:ED:18）不导入。

图2 接入MAC地址组

3） 创建匿名接入规则、Portal接入规则。其中匿名接入规则指定下发VLAN9（

和DHCP私网网段9.9.9.0/24关联），Portal接入规则下发VLAN10（和DHCP办公网网段10.10.10.0/24关联）。

图3 匿名接入规则配置

图4 Portal接入规则配置

4） 创建服务。注册前服务名为：初次入网服务，注册后服务名为：办公帐号服务。

图5 创建服务

具体每个服务的配置如下：

对于“初次入网服务”，引用缺省接入规则“匿名接入规则”，同时在接入策略列表中增加名为“办公PC免注册”的接入场景，其中“办公PC免注册”场景里引入“办公PC”的接入MAC地址组和“Portal接入规则”。此配置表示，当终端MAC地址属于“办公PC”这个MAC地址组时，按照“Portal接入规则”策略为终端下发VLAN10；当终端（例如智能终端或访客PC）MAC地址不属于“办公PC”这个MAC地址组时，按照缺省接入规则“匿名接入规则”为其下发VLAN9。

图6 初次入网服务的配置

图7 办公帐号服务的配置

5） 添加作MAC认证的接入设备即AC的IP地址及相关Radius参数

图8 在BYOD Server上添加接入设备

6） 创建帐号

在BYOD Server上需创建测试用的pca和公共帐号byodanonymous，pca帐号关联“办公帐号服务”，byodanonymous关联“初次入网服务”。由于配置策略免去终端PCB注册过程，因此pcb帐号无需在BYOD Server上创建。

图9 帐号列表

7） 测试结果如下：

当终端PCA（MAC地址：24:77:03:90:ED:18）连接无线SSID yonyoubyod时，BYOD Server自动完成MAC认证，终端PCA对此无感知，管理员在BYOD Server（IP地址：172.16

.0.9）的在线用户列表中可看到公共帐号byodanonymous在线。如图10所示，登录名为24770390ED18@byod，表明该帐号是通过MAC认证上线，该用户使用服务为“初次入网服务”，用户所属VLAN为VLAN9，IP地址为9.9.9.4，用户MAC地址为24:77:03:90:ED:18。

图10 PCA使用公共帐号初次入网时的在线状态

如图11所示，对于未注册终端，用户访问其他页面时会被重定向到BYOD界面完成终端注册，PCA终端选择访问方式为“使用已存在帐号访问”，输入已知帐号pca和密码，确定后即可完成终端注册。

图11 BYOD注册页面

如图12所示，注册后在BYOD界面上可看到该终端的基本信息。

图12 PCA注册成功后的BYOD界面

此时，BYOD Server会根据该终端注册时关联的已知帐号pca所绑定的策略，重新给终端PCA下发VLAN10，如图13所示，终端PCA获得一个新的IP地址10.10.10.3。

图13 终端PCA的网卡信息

此时在BYOD Server（IP地址：172.16.0.9）的在线用户列表中会看到终端PCA已经使用已知帐号pca在线了。如图14所示，且pca使用的服务为“办公帐号服务”，用户所属VLAN为VLAN10，IP地址为10.10.10.3，用户MAC地址为24:77:03:90:ED:18。

图14 终端PCA注册之后的BYOD Server在线状态

当终端PCB（MAC地址：00:24:D6:9A:5E:D6）连接无线SSID yonyoubyod时，BYOD Server自动完成MAC认证，终端PCB对此无感知，管理员在BYOD Server（IP地址：172.16.0.9）的在线用户列表中可看到公共帐号byodanonymous在线，如图15所示，使用的服务为“初次入网服务”，用户所属VLAN为VLAN10，IP地址为10.10.10.2，用户MAC地址为00:24:D6:9A:5E:D6。

图15 BYOD Server上的在线信息

四、 配置关键点：

1. BYOD参数设置需符合实际需求。
2. 访客参数设置需符合实际需求。