

访客用户在iMC BYOD解决方案中的典型应用

一、组网需求:

很多企业或其他类型的网络环境中,除了有大量正式常用已知帐号进行认证以外,还存在大量访客访问网络的应用场景。尤其是智能终端广泛应用的今天,接入网络终端的类型丰富多样和对移动办公业务的需求,衍生了BYOD这样的解决方案。为了更好地解决大量访客快捷访问网络且IT部门对访客终端可控的应用场景,本文将详细描述H3C iMC BYOD解决方案在此种场景中的应用。

二、组网图:

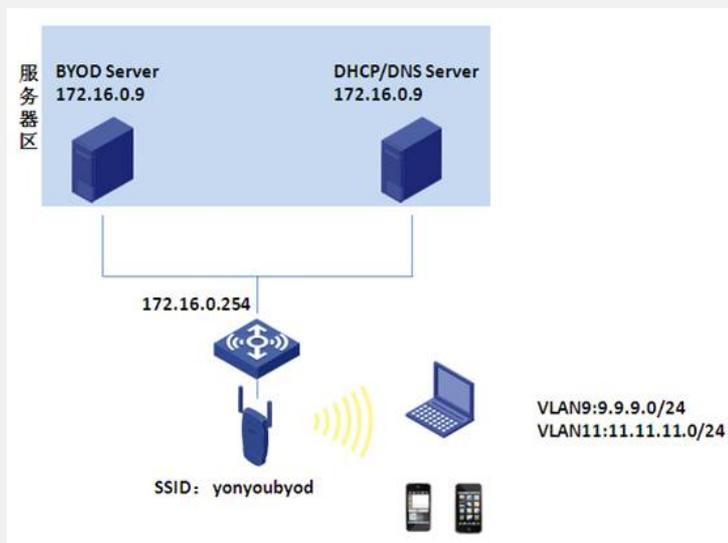


图1 组网图

组网图说明:

- 1) 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
- 2) 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), 划分两个地址池, 分别为隔离网段地址池9.9.9.0/24、访客网段地址池11.11.11.0/24。
- 3) 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。

三、配置步骤:

本案例中访客以智能手机 (iphone) 为终端, 通过H3C AC的无线接入, 以MAC认证为主要认证方式, 所有终端 (含智能终端) 均通过MAC地址认证方式接入无线, iMC BYOD Server对所有终端自动完成MAC认证, 所有终端用户无感知。若是访客终端, 接入无线后BYOD Server先将其划分到隔离VLAN9中, 终端获得一个9.9.9.0/24的地址, 可以在网络设备上配置VLAN9智能访问有限的资源, 不占用企业网络资源。访客终端访问其他网页时被重定向到BYOD注册页面, 访客在此页面完成终端注册后自动完成第二次MAC无感知认证, BYOD Server根据注册后的策略为其下发访客网段IP地址11.11.11.0/24, 访客根据设备上VLAN11的相关配置, 访问其被授权的网络资源。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。如下:

```
[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-interface11
description 访客IP
ip address 11.11.11.1 255.255.255.0
dhcp select relay
dhcp relay server-select 1

#
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。



图2 BYOD参数配置

2) 创建匿名接入规则、访客接入规则。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），访客接入规则下发VLAN11（和DHCP访客网段地址11.11.11.0/24关联）。

业务 >> 用户接入管理 >> 接入规则管理 >> 接入规则详细信息

基本信息	
接入规则名	匿名接入规则
业务分组	未分组
描述	

授权信息	
接入时段	无
下行速率	
优先级	
证书认证	不启用
认证证书类型	
下发VLAN	9

图3 匿名接入规则配置

业务 >> 用户接入管理 >> 接入规则管理 >> 接入规则详细信息

基本信息	
接入规则名	访客接入规则
业务分组	未分组
描述	

授权信息	
接入时段	无
下行速率	
优先级	
证书认证	不启用
认证证书类型	
下发VLAN	11

图4 访客接入规则配置

3) 创建服务：初次入网服务和访客服务。如图5所示。

业务 >> 用户接入管理 >> 服务配置管理

服务列表

增加 刷新

共有3条记录。

服务名	状态	服务描述	服务后缀	业务分组	缺省接入规则	缺省安全策略	计费策略
初次入网服务	可申请		byod	未分组	匿名接入规则	不使用安全策略	不计费
办公外号服务	可申请		byod	未分组	Portal接入规则	不使用安全策略	不计费
访客服务	可申请		byod	未分组	访客接入规则	不使用安全策略	不计费

图5 服务列表

如图6和图7所示，每个服务规则的具体配置如下：

业务 >> 用户接入管理 >> 服务配置管理 >> 增加服务配置

基本信息	
服务名	初次入网服务
业务分组	未分组
缺省安全策略	不使用安全策略
缺省私有属性下发策略	不使用
计费策略	不计费
服务描述	
<input checked="" type="checkbox"/> 可申请	<input type="checkbox"/> Portal智能终端快速认证

接入策略列表	
接入策略	接入规则
安全策略	私有属性下发策略
内网外联配置	优先级

确定 取消

图6 初次入网服务

业务 >> 用户接入管理 >> 服务配置管理 >> 服务配置详细信息

服务配置详细信息	
服务名	访客服务
业务分组	未分组
缺省安全策略	不使用安全策略
缺省私有属性下发策略	不使用
服务描述	
计费策略	不计费
<input checked="" type="checkbox"/> 可申请	<input type="checkbox"/> Portal智能终端快速认证

接入策略列表	
接入策略	接入规则
安全策略	私有属性下发策略
内网外联配置	优先级

图7 访客接入规则

- 4) 在【用户】|【访客管理】中增加创建好的“访客服务”，根据需求选择是否自动转正。本案例以自动转正为例。

服务名	状态	服务描述	服务后号	业务分组	缺省安全策略	计费策略	自动转正
访客服务	可申请		byod	未分组	不使用安全策略	不计费	是

图8 关联访客服务

- 5) 添加作MAC认证的接入设备即AC的IP地址及相关Radius参数

设备名称	设备IP地址
	172.16.0.254
接入区域	
认证端口	1812
计费端口	1813
业务类型	LAN接入业务
接入设备类型	H3C(General)
组网方式	不启用混合组网
共享密钥	*****
业务分组	未分组

图9 在BYOD Server上添加接入设备

- 6) 创建帐号。在BYOD Server上需创建测试用的公共帐号byodanonymous，让其“初次上网服务”。

帐号名	用户姓名	用户分组	帐号类型	当前余额(元)	开户日期
<input type="checkbox"/> pca	pca	未分组	预付费	0.00	2013-06-08
<input type="checkbox"/> byodanonymous	公共帐号	未分组	预付费	0.00	2013-06-07

图10帐号列表

- 7) 测试结果：

手机iphone接入无线SSID yonyoubyod，BYOD Server自动完成MAC认证，可以在BYOD Server上看到在线用户。如图11所示。

帐号名	用户名	用户分组	登录时间	登录IP地址	设备IP地址	用户IP地址	VLAN ID	MAC ID	安全状态	帐号类型	品牌	平台	用户MAC地址
byodanonymous	ec852f73385e@byod	公共帐号	2013-06-08 09:14:11	172.16.0.254	9.9.9.7	9			认证通过	预付费	Apple	iOS	EC852F73385E

图11 智能终端的在线信息

智能终端侧的网络情况如图12所示，此时该终端的IP地址为9.9.9.7。



图12 终端的网络信息

手机进行在BYOD界面完成注册。如图13所示。注册后可以看到该终端的相关信息。

说明：注册的方式有两种，一种是注册为新用户，由访客自己生成访客帐号(密码可自己设置，由iMC管理审批或者iMC后台自动审批)，但此时访客帐号会占用访客管理组件的License；另外一种是关联一个事先在iMC上创建好的专为访客使用的帐号，但需要事先告知用户该专用帐号的帐号信息和密码，此种方式不占用访客组件的License。



图13 终端的注册过程和结果

注册成功后，智能终端根据注册帐号关联的策略，被下发VLAN11，重新获得新的IP地址11.11.11.2。如图14所示。



图14 终端重新分配IP地址

如图15所示，在BYOD Server的在线用户列表中可以看到该终端的新的在线信息：



图15 帐号注册后的在线信息

如图16所示，此时检测终端网络连通情况，能够ping通网关11.11.11地址。



图17 终端的ping操作信息

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。