BYOD 何颖 2013-06-09 发表

# 访客用户在імс вуор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。



#### 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+i MC 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 BY OD 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11.11.11.0/2 4,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。

00系统参数配置				
息用快速认证功能	2	~	· 单张号是多MAC数	900 000
· 智能终端MAC通让老化时长	1	天 O	• 禁止同时在战时长大于等于	0 BOSMACHELEHTHERATE
算止非智能终端认证	Ť	v 0	• 快速认证老化时长	0 天日
终端信息不一致的处理方式	允许认证	v ()	终端信息获取方式	INode DHCP HTTP User Agent MA
息用DNS重定向	4	- 0		

## 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)。

基本信息				
接入規則名		匿名接入规则		
业务分组		未分组		
描述				
超复信白				
按入时代		 <del>*</del>	_	
五八明夜		56		
111124 F				
11.元级		<b>7 a m</b>		
证书认证		小启用		
认证证书类型				
下友VLAN		9		
3 匿名接入规则面	置			
就业务 ≫ 用户接入	管理 >> 接入规则	管理 >> 接入規則详细	自息	
<b>苯华信息</b> 接入投剧 <b>么</b>		访客接入规则		
地名马相				
出分力和		JAC JI SE		
1011年1月				
投权信息 接入时段		无		
武八明夜		50		
优先级				
证书认证		不启用		
认证证书类型				
14 访客接入规则面	置	11		
R&VLAN 3) 创建服务 3) 创建服务	3置 5:初次入网服	11 务和访客服务。如	图5所示。	
	置 5:初次入网服 Rate	11 务和访客服务。如[	图5所示。	
F&VLAN       24 访客接入规则部       3) 创建服务       *** 用P最人管理 * 影易       *** 用P最人管理 * 影易       *** 用P最人管理 * 影易       *** *** 用P最人管理 * 影易       *** *** ***       **** ***	2置 务:初次入网服 1826年	11 务和访客服务。如图	图5所示。	
F&VLAN           日4         访客接入规则画           3)         创建服务           1         小学家           1         小学家 <td>2置 5:初次入网服 配音音度</td> <td>11 务和访客服务。如 ****</td> <td>图5所示。 <u>规制                                    </u></td> <td><b>海 社会</b>第</td>	2置 5:初次入网服 配音音度	11 务和访客服务。如 ****	图5所示。 <u>规制                                    </u>	<b>海 社会</b> 第
F&VLAN           日4         访客接入规则面           3)         创建服务           (1)         (1)           (2)         (2)           (2)         (2)           (2)         (2)           (2)         (2)           (2)         (2)           (2)         (2)           (2)         (2)           (2)         (2)	2置 子:初次入网服 配面变度 Lifestatic Lifestatic Lifestatic Lifestatic Lifestatic Lifestatic Lifestatic Lifestatic	11 务和访客服务。如 * *分组	图5所示。 (M) <u>\$\$</u> \$\$\$\$ (M) 不能現实 (M) 不能現实	<b>16 11 東京</b> 不计愛 第6 不计学
F&VLAN           日4         访客接入规则部           3)         创建服务           1         北京           1         北京 <t< th=""><th>2置 子:初次入网服 配置管理</th><th>11 务和访客服务。如</th><th>图5所示。</th><th><b>減</b> 開発 不計算 開編 不計算 減編 不計算</th></t<>	2置 子:初次入网服 配置管理	11 务和访客服务。如	图5所示。	<b>減</b> 開発 不計算 開編 不計算 減編 不計算
F&VLAN       14 访客接入规则部       3) 创建服务       3) 创建服务       14 访客接入规则部       3) 12 服务       14 访客接入规则部       15 服务列表       1866和图7所示,名       1866和图7所示,名	2置 5:初次入网服: 1 1 1 1 1 1 1 1 1 1 1 1 1	11 务和访客服务。如	<b>255所示。</b>	1 <b>年 计变如</b> 第6 不计变 第6 不计变 第6 不计变
F&VLAN       14 访客接入规则部       3) 创建服务       3) 创建服务       12 #8 >> 用戶集入管理 >> 服务       13 #8       14 访客接入规则部       15 服务列表       1866和图7所示,名       1866和图7所示,名       1866和图7所示,名       1876	2 音:初次入网服 記書を建	11 务和访客服务。如	图5所示。 <u> 現則</u> 秋安全な 現明 不使用史全 現象 不使用史全 1 1 1 1 1 1 1 1 1 1 1 1 1	<ul> <li>14. (注意意味)</li> <li>第時、不计意</li> <li>第時、不计意</li> <li>第時、不计意</li> </ul>
FXVLAN       14 访客接入规则商       3) 创建服务       1 访客接入规则商       3) 创建服务       1 如果       1 1 日       1 1 日       1 1 日       1 1 日       1 1 日       1 1 日       1 1 日       1 1 日       1 1 日       1 1 日       1 1 日       1 1 日       1 1 1 日       1 1 1 1 日       1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	2 音:初次入网服 配音音度	11 务和访客服务。如 *分组 *分组	图5所示。 	<ul> <li>読品 (注意)加引 第二級 不计意 第二級 不计意 期間 不计意</li> <li>byod</li> <li>byod</li> <li>面合類人発明</li> <li>不依明</li> </ul>
FXVLAN       14 访客接入规则部       3) 创建服务       3) 创建服务       14 访客接入规则部       3) 成功       15 服务列表       15 服务列表       186 和图7所示, 名	日 日 日 日 日 日 日 日 日 日 日 日 日 日	11 务和访客服务。如 *分组 ¥3年 *分组 Potal *分组 Potal *分组 235推入 具体配置如下: #未分组 * ¥3页网络	图5所示。 (MN) 秋奇安全第 (Q) 不使用安全 (Q) 不使用安全 (Q) 不使用安全 (Q) 不使用安全 (Q) 不使用安全 (Q) (Q) (Q) (Q) (Q) (Q) (Q) (Q) (Q) (Q)	1年 11章第第 第二章 第二章 第二章 第二章 第二章 第二章 第二章 第二章 第二章
F&VLAN       14 访客接入规则部       3) 创建服务       3) 创建服务       14 访客接入规则部       3) 10 建服务       14 访客接入规则部       15 服务列表       18 6和图7所示,名	2 当 ま ま ま ま ま ま ま ま ま ま ま ま ま	11 务和访客服务。如 *分组 ¥3至 *分组 ¥3至 *分组 23至 *分组 23章 *分组 23章 ************************************	图5所示。 <u>RNI 於5文全部</u> <u>RNI 不使用支土</u> <u>RNI 不使用支土</u>	<ul> <li>第6 子は変第 第6 子は変 第第 子は変 第第 子は変 第6 子はないのである。</li> <li>byod</li> <li>byod</li> <li>医な声入発明</li> <li>不使用</li> </ul>
F&VLAN       14 访客接入规则部       3) 创建服务       3) 创建服务       14 访客接入规则部       3) 10 建服务       14 访客接入報告       15 服务列表       186 和图7所示,名	2 置 ま ま ま ま ま ま ま ま ま ま ま ま ま	11 多和访客服务。如	名5所示。	<ul> <li>1年 は受知 第二 不计会 第二 不计会 第二 不计会</li> <li>1日 不計会</li> <li>1日 不計会</li> <li>1日 不会用</li> </ul>
FXVLAN       A4 访客接入规则部       3) 创建服务       3) 创建服务       125 服务列表       1266和图7所示,在       245%       2586       2586       264%       275       275       286       286       287       288       288       298       298       298       298       298       298       298       298       298       298       298       298       298       298       298       298       299       2010       2011 </td <td>2 当 まままま まままま まままま まままま たまままま たままままま たままままままま などの たままままままままままままままままままままままままままままます。 本の時を、 本の時を、 本の時で、 本ので  本ので、 本ので、 本ので  本ので  本ので  本ので  本ので  本ので  本ので  本ので</td> <td>11 务和访客服务。如</td> <td>図5所示。        305所示。       300</td> <td><ul> <li>14 受加</li> <li>第5 不计章</li> <li>第6 不计章</li> <li>第6 不计章</li> <li>第6 不计章</li> <li>第6 不计章</li> <li>7 代型</li> </ul></td>	2 当 まままま まままま まままま まままま たまままま たままままま たままままままま などの たままままままままままままままままままままままままままままます。 本の時を、 本の時を、 本の時で、 本ので  本ので、 本ので、 本ので  本ので  本ので  本ので  本ので  本ので  本ので  本ので	11 务和访客服务。如	図5所示。        305所示。       300	<ul> <li>14 受加</li> <li>第5 不计章</li> <li>第6 不计章</li> <li>第6 不计章</li> <li>第6 不计章</li> <li>第6 不计章</li> <li>7 代型</li> </ul>
FXVLAN       14 访客接入规则部       3) 创建服务       3) 创建服务       14 访客接入规则部       3) 10 建服务       14 访客接入规则部       15 服务列表       15 服务列表       18 6和图7所示,名       18 6和图7       18 6和图7       18 6和图7       18 6和图7       18 6和图7	2 当:初次入网服 配置すま	11 务和访客服务。如	名うり、 名の 名の 名の 一 本の で 本の の 、 本の の 、 本の の 、 本の の 、 本の の 、 本の の 、 本の の 、 本の の 、 本の の 、 、 本の の 、 、 本の の 、 、 本の の 、 、 本の の 、 、 本の の 、 、 本の の 、 、 本の の 、 、 、 本の の 、 、 、 本の の 、 、 、 本の の 、 、 、 本の の 、 、 、 本の の 、 、 、 本の の 、 、 、 、 、 、 、 、 、 、 、 、 、	1年 11章 第二 第二 不计章 第三 不计章 第三 不计章 第三 不计章 第三 不计章 第三 不计章 第二 第二 "不计章" 第二 "不可章" 第二 "不可章" 第二 "不可章" 第二 "不可章" 第二 "不可章" "" "" "" "" "" "" "" "" "" "" "" "" ""
FXVLAN       14 访客接入规则部       3) 创建服务       3) 创建服务       14 访客接入规则部       3) 创建服务       14 访客接入规则部       15 服务列表       186 和图7所示, 年       186 和次入网服务	2 当 二 二 二 二 二 二 二 二 二 二 二 二 二	11 务和访客服务。如 *分組 *分組 E 382 *分組 E 382 *分組 · 235 *分組 · 235 · 23	名の 名の 名の 名の 名の 子の での での の での での の の での の の での の の での の の での の の での の の での の の での の の での の の での の の での の の での の の での の の での の の の の の の の の の の の の の	
FXVLAN         14       访客接入规则面面         3)       创建服务         14       访客接入规则面面         3)       创建服务         14       小田市山大学校、新会         15       服务列表         16       加方川市大,在         186       和日和大学校、         186       和日和大学校、         186       和日和大学校、         186       和小大大学校、         187       中は         188       日本         188       日本         188       日本         198       日本 <td>2 当 ま ま ま ま ま ま ま ま ま ま ま ま ま</td> <td>11       务和访客服务。如日       ● まる分類       未分類       第の類       第の類       第の類       夏体配置如下:</td> <td>名の方式である。</td> <td><ul> <li>14、11・支払</li> <li>第第6 不计委</li> <li>第第6 不计委</li> <li>第第6 不计委</li> <li>第第6 不计委</li> <li>第6 是入我利</li> <li>万使用</li> <li>14 先点()</li> </ul></td>	2 当 ま ま ま ま ま ま ま ま ま ま ま ま ま	11       务和访客服务。如日       ● まる分類       未分類       第の類       第の類       第の類       夏体配置如下:	名の方式である。	<ul> <li>14、11・支払</li> <li>第第6 不计委</li> <li>第第6 不计委</li> <li>第第6 不计委</li> <li>第第6 不计委</li> <li>第6 是入我利</li> <li>万使用</li> <li>14 先点()</li> </ul>
FXVLAN         A4 访客接入规则部         3) 创建服务         3) 创建服务         2 ±8 >> 用戶集入管理 >> 基条         1 ±72       1 ±72         1 ±72       1 ±72         1 ±72       1 ±72         1 ±72       1 ±72         1 ±72       1 ±72         1 ±72       1 ±72         1 ±72       1 ±72         1 ±72       1 ±72         1 ±72       1 ±72         1 ±72       1 ±72         1 ±72       1 ±72         2 ±75       1 ±72         2 ±75       1 ±72         2 ±75       1 ±72         2 ±75       1 ±72         2 ±75       1 ±72         2 ±75       1 ±72         2 ±75       1 ±72         2 ±75       1 ±72         2 ±75       1 ±72         2 ±75       1 ±72         2 ±75       1 ±72         2 ±75       1 ±72         2 ±75       1 ±72         2 ±75       1 ±72         2 ±75       1 ±72         2 ±75       1 ±72	3 当 二 二 二 二 二 二 二 二 二 二 二 二 二	11         务和访客服务。如目         *分組         *分組         #分組         「「大気量」         *分組         具体配置如下:         「「大気量」         「「大気量」         ● 中の調         * 大規         ● 中の調         * 大規         ● 中の調         ● 中のの調         ● 中のののののののののののののののののののののののののののののののののののの	名しち所示。	3年 11 受知 第6 不计愛 第第 不计愛 第第 不计学 第第 不计学 第第 不计学 第第 不计学 第第 不计学 第第 不计学 第第 不计学 第1 (1) (1) (1) (1) (1) (1) (1) (1) (1) (1
FXVLAN         14 访客接入规则部         3) 创建服务         3) 创建服务         14 访客接入规则部         3) 创建服务         15 服务列表         15 服务列表         18 6和图7所示,4         18 43 243         18 6和图7所示,4         18 58         19 6和图7所示,4         19 884         19 884         19 885         19 6和1877所示,4         19 6和1877所示,4         19 884         19 884         19 984         19 984         19 985         19 885         19 986         19 986         19 986         19 986         19 986         19 986         19 986         19 986         19 986         19 986         19 986         19 987         19 988         19 988         19 988         19 988         19 988         19 988         19 988         19 988         19 988         19 988         19 988         19 988         19	3 ま:初次入网服: 転音音度	11 务和访客服务。如	名しち所示。	1時、「日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日

计费策略

区可申请

缺省私有歷性下发策略 服务描述

不使用

不计费

Portal智能终端快速以证



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。

CONTROL OF THE	onyoubyou		
IP 地址			
DHCP	BootP	静态	
IP 地址		9.9.9.7	
子网掩码	255.255.255.0		
路由器	9.9.9.1		
DNS		172.16.0.9	
搜索域	h3c		
客户端 ID			

### 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。

XC	X			X	2	N
Management 络的方式。这	Center		lanagement	Center		
	新用户注册	§的方式。	-			
	* M98	guest	首。	898	quest	
	25		专输、处	84	1	
	WIELBOX		言息),都	终病类型	Phone	
	10.000	-	5	<b>FR</b>	Apple	
	用户姓名	1.98.8	11日月 加	操作系统	IOS	
		武扫和应的	MAC地社	EC:85:2F:73:36:5E		
	· ###	pca		注册访客成与	5、请保存好您的报号名及密码	b.
	8849.0017					
	操持人员					
	1	#	HEN-			

## 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。

IP 地址		
DHCP	BootP	静态
IP 地址		11.11.11.2
子网掩码	25	5.255.255.0
路由器		11.11.11.1
DNS		172.16.0.9
搜索域		h3c.com
客户端 ID		



# 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11.11.11.1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。