BYOD **寻尚岩** 2013-07-26 发表

## iMC UAM BYOD功能与Ac结合实现8021x快速接入认证的典型配 罯 一、组网需求 基于H3C iMC UAM的BYOD可与无线Portal、8021x、无线MAC配合使用。BYOD结合无线 MAC认证无法进行安全检查,8021x认证或者portal认证可以解决这一问题。本文以BYOD结合 8021x认证为例,BYOD结合8021x认证主要是将终端与已有账号绑定,直接使用已有账号认证 并根据终端类型应用不同的安全控制策略,需要注意的是终端第一次接入网络时,由于认证通过前 还未获取IP地址,所以默认接入规则必须为证书认证,等终端MAC地址信息已经写入UAM中时, 默认接入规则将不再起作用。 二、组网图 G1/0/1 G1/0/11 G1/0/1 172.16.2.0/24 172.16.2.0/24 72.16.0.0/2 G1/0/7 **DHCP Server** PC/phone 注: 1: UAM从E0401版本开始支持BYOD; 2: 图中红色区域为WX3010,为便于理解,将其中的交换网板模拟为一交换机; 3: AP属于VLAN 4, 由AC动态分配IP; 4:终端属于VLAN 8,由iMC服务器分配IP;

三、配置步骤

1.交换机配置

划分业务VLAN 2, 15口为与交换板相连接口。

[1234]vlan 2

[1234-vlan2]port g2/0/15

[1234]inter vlan 2

[1234-Vlan-interface2]ip address 172.16.2.3 255.255.255.0

配置静态路由

[1234]ip route-static 172.16.8.0 24 172.16.2.2

2.交换板配置

划分业务VLAN

[H3C]vlan 2,

[H3C-vlan2]port g1/0/1

为vlan2分配IP地址

[H3C-vlan2]inter vlan 2

[H3C-Vlan-interface2]ip address 172.16.2.2 24

G1/0/7口与AP相连,所以需放通VLAN 4,且为AP供电

[H3C-GigabitEthernet1/0/7]poe enable

[H3C-GigabitEthernet1/0/7]port access vlan 4

G1/0/11口为内置与AC互联端口,该端口需配置成trunk类型,且必须允许业务vlan2和AP所属vlan4通过(用户vlan经过ap时会被打上vlan4的标签)

[H3C-GigabitEthernet1/0/7]inter g1/0/11

[H3C-GigabitEthernet1/0/11]port link-type trunk

[H3C-GigabitEthernet1/0/11]port trunk permit vlan 2 4

[H3C-GigabitEthernet1/0/11]port trunk pvid vlan 2

3.AC配置

G1/0/1口为内置与交换板互联端口,该端口需配置成trunk类型,且必须运行业务vlan2和AP所属vlan4通过

[AC]inter g1/0/1

[AC-GigabitEthernet1/0/1]port link-type trunk

[AC-GigabitEthernet1/0/1]port trunk permit vlan 2 4

[AC-GigabitEthernet1/0/1]port trunk pvid vlan 2

[AC-GigabitEthernet1/0/1]vlan 2

为业务vlan分配IP

[AC-vlan2]inter vlan 2

[AC-Vlan-interface2]ip address 172.16.2.1 24

开启DHCP功能为AP分配IP地址

[AC]dhcp enable

[AC]dhcp server ip-pool ap

[AC-dhcp-pool-ap] network 172.16.4.0 mask 255.255.255.0

指定AP网关

[AC-dhcp-pool-ap] gateway-list 172.16.4.1

划分用户vlan

[AC]vlan 8

[AC-vlan8]inter vlan 8

[AC-Vlan-interface8]ip add 172.16.8.1 24

BYOD功能要求用户IP地址由DHCP agent分配,这样UAM才能根据DHCP特征识别终端信息, 所以AC需配置dhcp中继,DHCP服务器IP为iMC服务器地址

[AC]dhcp relay server-group 1 ip 172.16.0.9

配置用户vlan工作在中继模式

[AC-Vlan-interface8]dhcp select relay

指定分配IP的DHCP server,这样终端用户获取IP时,UAM就会从DHCP request请求中提取dhcp 特征识别终端信息

[AC-Vlan-interface8]dhcp relay server-select 1

认证相关信息配置:

使能端口安全,类似于交换机全局dot1x作用:

[H3C]port-security enable

证书认证只能采用eap认证方式

[H3C]dot1x authentication-method eap

配置radius 认证信息

[AC-Vlan-interface8]rad sch h3c

标准模式不支持EAD,尽量选择扩展模式

[AC-radius-h3c]server-type extended

[AC-radius-h3c]primary authentication 172.16.0.9

[AC-radius-h3c]primary accounting 172.16.0.9

[AC-radius-h3c]key authentication h3c

[AC-radius-h3c] key accounting h3c

配置domain 8021x,并引用h3c

[AC]domain 8021x

[AC-isp-8021x] authentication lan-access radius-scheme h3c

[AC-isp-8021x] authorization lan-access radius-scheme h3c

[AC-isp-8021x] accounting lan-access radius-scheme h3c

创建服务模板3,与AP关联后使用密文发送数据

[AC] wlan service-template 3 crypto

创建8021x认证时使用的ssid

[AC-wlan-st-3] ssid x\_dot1x

绑定无线虚拟接口3

[AC-wlan-st-3] bind WLAN-ESS 3

配置在帧加密时使用的加密套件为tkip或者ccmp

[AC-wlan-st-3] cipher-suite tkip

[AC-wlan-st-3] cipher-suite ccmp

设置在AP发送信标和探查响应帧时携带WPA IE,即认证方式为WPA

[H3C-wlan-st-3]security-ie wpa

激活服务模板3(激活前需创建无线接口3)

[AC-wlan-st-3] service-template enable

创建无线虚拟接口3

[AC]inter WLAN-ESS 3

允许用户vlan通过

[AC-WLAN-ESS1]port access vlan 8

对接入用户采用基于MAC的802.1X认证,且允许端口下有多个802.1X用户

[H3C-WLAN-ESS3]port-security port-mode userlogin-secure-ext

开启11key类型的密钥协商功能:

[H3C-WLAN-ESS3]port-security tx-key-type 11key

指定用户的认证域为8021x:

[H3C-WLAN-ESS3]dot1x mandatory-domain 8021x

注册AP并进行设置

[AC]wlan ap x\_byod\_ap

[AC-wlan-ap-x\_byod\_ap] serial-id 210235A29E0087000090

[AC-wlan-ap-x\_byod\_ap] radio 1

[AC-wlan-ap-x\_byod\_ap-radio-1]service-template 3

[AC-wlan-ap-x\_byod\_ap-radio-1]radio enable

[AC-wlan-ap-x\_byod\_ap-radio-1]radio 2

[AC-wlan-ap-x\_byod\_ap-radio-2]service-template 3

[AC-wlan-ap-x\_byod\_ap-radio-2]radio enable

4.DHCP server配置,需安装DHCP server和DNS server,具体安装过程略

	Adunistrator	↓ ↓ 终端服务
	文 当	
· andia	计算机	👣 Internet 信息服务(IIS) 6.0 管理器 💱 Internet 信息服务(IIS)管理器
(cuiro	网络	😪 iSCSI 发起程序
	控制面板	₩ Windows Server Backup 安全配置向导
	管理工具	<ul> <li>→ 本地安全策略</li> <li></li></ul>
	≠R04.10-+-4±	④ 服务

新建IPV4作用域(DHCP server保证已授权)

Q DHCP □ ] win-w5wfplanlih □ ] IPv4 ]	DHCP 作用域向导	Tatua C
<ul> <li>■ 作用域 [172.</li> <li>■ 作用域 [172.</li> <li>■ 服务器选项</li> </ul>	- M	欢迎使用新建作用域向导
€ <b>]</b> Irv6		此向导帮助您设置作用域,在网络上为计算机分配地 址。 若要继续,请单击"下一步"。
		< 上一步(3) <b>下一步(0) &gt; 取</b>

点击下一步输入作用域名称, 配置地址池

win-w5wfplmnlih	起始 IP 地址	结束 IP 地址	描述
(★) 1774 □ □ /5 田村志 [172, 16, 9, 0]	172. 16. 8. 2	172.16.8.254	地址分发范围
·····································			

指定网关为172.16.8.1, dns为8.8.8.8,

Í	作用域选项			
	选项名	供应商	值	
	ℯ	标准	172.16.8.1	
	💞 006 DNS 服务器	标准	8.8.8.8	
	🧓015 DNS 域名	标准	h3c.com	

## 服务器选项再次指定DNS

LO DHCP				. 0
文件(P) 操作(A) 查看(V) 帮助	<b>ђ</b> 0Ю			
(= =) 🖄 📷 😹 🔛 🕷	<i>9</i>			
Ф рись	服务器选项			
E 📑 win-w5wfplmnlih	选项名	供应商	值	
<ul> <li>○ IFv4</li> <li>○ 作用域 [172.16.8.0]</li> <li>○ 地址地</li> <li>○ 地址相用</li> <li>○ 律留</li> <li>○ 作用域 [172.16.9.0]</li> <li>○ 振劳器选项</li> <li>① IFv6</li> </ul>	4006 DNS 服务器 40015 DNS 域名	标准	8.8.8.8 h3c.com	

安装dhcp agent (UAM安装包内有安装文件) 插件,过程略,安装配置完成后启动agent插件:

-goinglett		Agenut	
启用Agent	<b>A</b>		
UAM服务器IP	172 . 16 . 0	. 9	
UAM服务器端口	1810	$\sim$	
日志级别	警告		
Agent消息			
DHCP Server	务已启动。 <sup>委加</sup> 载。		1
	A MIL MORAL MARKED AND AND AND AND AND AND AND AND AND AN	A CONTRACTOR OF A CONTRACTOR O	1997 (1997) (19977) (19977) (19977) (19977) (19977) (1977) (1977) (1977) (1977)

5.iMC侧配置, byod结合8021x认证适用于已经存在接入账号,该账号用不同的终端认证时,接受的安全控制策略也不相同。本例要求PC认证时必须使用iNode客户端且进行安全检查,手机认证上线时只需下发ACL, ACL要求手机不能访问172.16.0.11,具体的配置包括

增加接入设备,和常规配置一致

夏亚乔 20月前入1	世界 >> 株入社会管理 >> 株入	- CARE					*	加入市場
接入设备查询								2.9
设备护地址从	1		¥					
设备名称			職入设备类型				- Ta	11日
入设备列表								
fitta W	(第)		与平台设备两步		697		QANAFERIN QU	1917 FX
具有6条记录,当前第1	1-5+第1/1资。						每页世示: 8	15 [50] 100
	经会中地址	승유성적	TXNZAU	(Fil	下來情報	藏口政委用步结束	7988	語作
Ð	192,168.0.102				未下发	无意用步		~
15	192,168,100,102				*7%	无意料步		-
	172.16.0.11				*75	无菌网步		-
13		1000 1000 50 50	H3CRH		未下生	天靈同步		-
	1.1.1.1	PIGC BIDPCID-20	A CONTRACT OF A DESCRIPTION OF A DESCRIP					
10 E HJU E 1721621	111.1	ICMP	1.000		未下发	无意同步		-

创建三个接入规则,一个匿名接入规则,另外两个 接入规则分别用于不同的接入场景:

匿名接入规则

" 孫人則則名	服名推入规则			
• 计费分组	(未分詞 -			
Sit				
inco				
38 X 8310		- 4380(PH66)	100	
現代の研究	70	- 2014年 - 3044 - 1221年 - 1221年		1
(****	Köps			
UL YEAR		E BRIKSAWE		
证书认证	· 不直用 O EAPERIUE O W	PI证书认证		
认证证书类型	ENGILEDING +			
下发VLAN				
下发User Profile		下发用户组		
C用接入规则				
🖬 业务 >> 用户输入管理 >>	#入规则管理 >> 都改推入规则			
基本信息				
* 權入規則名	1002			
* 业务分组	(未分姐 *)			
橫迷				
授权信息				
推入时段	天 •	- 分解呼地站	2	*
下行遵军	Kbps	上行进军		Kops
优先级		回 启用RSA认证		
证书认证	<ul> <li>不自用 · EAP证书认证 · WAF</li> </ul>	NEHUE		
110000000000	EAP-TLSU .			
BURGERS TOPPOSE				
Trævlan				
TrævLan		下发用户组		0
T发UAN T发UserProfile 手机接入规则:		下发用户间		Ø
T%VLW ■ T%UserProfile 手机接入规则:		TRUCHE		G
T%VLAN ■ T%UserProfile 手机接入规则:	手机输入规则	T52/8,≏H8		Ð
TXXVLAN ■ TXXUser Profile ■ TXXUser Profile ■ TXXUser Profile ■ TXXUser Profile ■ TXXUser Profile	<b>手机接入规则</b> 亦分组 •	TXAPE		G
<ul> <li>下放UAH</li> <li>下放User Profile</li> <li>手机接入规则:</li> <li>● 計入規則為</li> <li>● 当务分組 載述</li> </ul>	<b>手机抽入规则</b> 用分组 -	TRAPA		Ø
TRUUH TRUUH 下RUSHProfit 年机接入规则: * 服入规则集 · 让分别国 能述	<b>羊机除入机器</b> 用分组 *	TRUEAN		0
TRUUH     TRUUH     TRUUH     TRUUH     TRUUH     TRUUH     TRUUH     TRUUH     TRUUH     TRUH     TRUH	<b>羊机抽入规则</b> 原始组 * 	53/0/HB	8	
TRAUAH	手飛線入網70 原分類 ・ 光 ・ Kbps	下水用户组 - 分配户地址 上行在来	(B)	v ktps
TRUUH     TRUUH     TRUUH     TRUUH     TRUUH     TRUH	平統論入統約 掛分祖 - 光 ・ Kbps	下水用户道 - 分配PHS社 上行客军 □ £用RSAUGE	8	C Kbps
TSUUAI	予約時入税28           原分祖           売           売           た              た	下30月中日 - 分配中地址 上行意来 - 創用RSAU王	( <u>6</u>	C) * Kbps
TRU-AN     TRU	∓RHA入RDN 用分明 売 た たひps の不良明 ● EAPETULE ○ WAP EAP-TLSULE ・	ТЗЛЯРНЕ • УКОРНИЕ ⊥ПЕТ ■ едлялисе чатнисе	8	v Kbps
	手和論入版10 用分组 ・ ・ ・ 本記の 単 EAPで正光以変 ・ ・	тжлена • уженые ⊥так с епекание четние	8	v Kbps
TSULAH	平規構入規約 ※分明 ・ 、 た の 、 た の 、 、 た の 、 、 た の の 、 、 た の の 、 、 た の の 、 、 た の の 、 、 た 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	ТХЛАНШ - УЛФРИВШ ⊥1922 ⊡ £АЯКАЧЦЕ ТХЛАНШ ТХЛАНШ	8	× Kbps
TRULAI	手机構入規則者           単点構           売沙相           売沙相           売           ・           ● 元会周 * EAP定于以近 ● WA           EAP-TLS以近 ●           * 手工転入 3000	下北周中道 ・ 分配中地址 上行意来 直相RSA以近 下支用户道 2		T Kbps
TRULAI	子校振入規28 戸分祖     ・	ТХЛРНЕ • УВСРИЗЕ ⊥ПЕХ _ дирозна: четные тедров • тедров	8	v Kbps

#54 允许用户修改密码	1002		株ち状态 自用用户	密码控制策略	正常		
开户日期	2013-05	-17	下次登录	须给改密码	否		
最后下线时间 最大闲置时长	2013-05	-31 13:01	失效日期 在线数型	RV	3		
在线状态 登录提示信息	在线		Portal智慧	<b>5终端最大绑定数</b>	1		
计表信息 帐号类型	杨付弗		当前余额		399 0077		
自助充值	ftif						
服务名	服务后端	缺省安全等略	计表策略	分配的	9 ML	当前计参周期	
1_8021x 發統终端使運動研MA/	8021x 2.纳丽娜家信贝	不使用安全策略	不计费				
置已有账号li 端第一次上约	uo2引用的原 线时,需保证 <b>&gt; ■\$\$\$</b> \$ <b>\$</b>	服务,该服务有 E该规则为证书	有两个接入场景 认证方式,终站	(注意: 缺 湍认证通过/	省接入規 后,则对	见则为匿名拍 I该规则没有	接入规 可要求
【本信息 服务名	k_8021x		服务局级		[0021X		-
业务分组 建备安全策略	未分组	+	<ul> <li>         、設备報入紙         ・         、         、         、</li></ul>	01 8-0/7	蓄名独入规则 不使用	• • 0	
<b>缺省私有属性下发策略</b> 计集制和	不使用	- 0	90, m ( 3 <sup>17</sup> 1/)	10.05	- <b>R</b> /4		
服务描述		0					
☑ 司申请 ☑ ↓入策略列表			🔲 Porta	副影响得快速以近 😡			
增加	持入附制	\$2300	A GEO NAME	ABBARA		¥.00 (1020)	
	luc2	run_disk_pass	不使用	不使用	1	8 1	ж
ecu .	7.0100/00/0	小田田文王市町	কর্মা	小花用		- 1	
C场景对应PC	2接入, 接入	、规则为luo2					
* 接入场景名	你		PC				
★ 接入区域			不限			•	
			-114R			•	
* 接入IP地址约	Ξ.		不限			▼	
* 无线 <mark>SSID</mark> 组			不限			•	
★ 接入MAC地:	址组		不限			•	
★ 厂商分组			微软			•	
* 操作系统分约	闺		办公PC			-	
• {2):出来中国/14	:н		DC				
·秋炳天空刀: 管自	<b>.</b> ш		ru -			·	
* 接入和回问			1002			-	
			1002			•	
* 安全策略			xun_disk_pas	s		•	
* 私有属性下)	发策略		不使用			•	
* 内网外联酚	苦		不使用			•	
eizu场景对应 * 接入场暑空;	立手机接入: <sup>你</sup>		meizu	1			
	na-						
* 接入区域	_		不限			•	
* 接入IP地址约	E		不限			•	
* 无线 <mark>SSID</mark> 组	l		不限			•	
* 接入MAC地	址组		不限			•	
* 厂商分组			魅族			•	
* 操作系统分约	组		安卓 <b>4.1魅</b> 族				
* 终端***刑\-	目		移动物			—, I	
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	<u>.</u> п		12/9/0533前				
* 接入规则			手机接入规则			- T	
* 安全策略			不伸田安全等	18			
→エオペーロ * 利力同時で	七空的		「「以用以主衆」	н			
一個自周住下。	x, 992.WD		小使用			•	

手机接入规则:

* 接入规则名	手机搬入规则			
• 业务分组	未分组	*		
描述				
授权信息				
攘入时段	无		• 分配P地址	a
下行速率		Kbps	上行連案	
优先级			□ 启用RSA认证	
证书认证	● 不启用 ◎ E	EAP证书认证 ① WAPI证:	书认证	
认证证书类型	EAP-TLSINE			
下发VLAN				
□ 下发User Profile			下发用户组	
	● 手工输入	3000	0	
☑ 下发ACL	列表选择		· ·	
	◎ 接入ACL列表	6	*	

设备acl配置:

```
[AC]dis ac
[AC]dis ac] 3000
Advanced ACL 3000, named -none-, 2 rules,
ACL's step is 5
rule 0 deny ip destination 172.16.0.11 0
rule 1 permit ip
```

[AC]

证书配置:

手机、UAM侧分别分别安装证书,具体配置略。

PC认证,由于是802.1x认证,终端第一次认证通过后还未获取到IP,所以UAM无法判断终端类型,即不能应用安全控制策略,所以UAM会强制用户下线并应用新的策略。

SSID	状态	安全类型	信号强度	连接类型	
Tx_dot1x	已连接上,没有通	WPA	极好	普通	
IToIP_1X		WPA	极好	普通	
人证信息					
2013-05-31 12:36:43	正在进行证书验证。				
2013-05-31 12:36:45	您的身份验证成功				
2013-05-31 12:36:45	已连接安全无线网络	5			
2013-05-31 12:36:46	自动获取IP地址				
2013-05-31 12:36:50	当前IP地址是172.16	6.8.3			_
2013-05-31 12:36:52	新识别或更新了终端	(信息,正在下約	就并重新认证以应用	用新的策略。	
2013-05-31 12:36:52	小要水进行安主位重	<u>.</u>			
2013-05-31 12:36:56	无线网络已断开	强制断开。			
2013-05-31 12:37:32	开始连接安全无线网	骆 SSID: x	_dot1x		
2013-05-31 12:37:33	开始进行身份验证。	. [luo208021x	]		
2013-05-31 12:37:34	正在进行证书验证。	11			





a itu	1098														
- 1	ARTRA	優朝	FAR	调除在纸	法规	宝制齐西		RAF							
共有2	亲记录,	当解第1-2-3	6 1/1页+											着页盘示:	8 15 [5
	11号名	0#8	用户推名	國務會	的入时间	放入时候	设备印始社	用户印绘址	无线用户与	90 安全状态	<b>客户法定时时</b>	1111120	机油厂具	经编程合系统 经介质	i len ti
	1002	luo2(88021x	portal	00211	2013- 05-31 13:14:06	66	172 16.2.1	172.16.8.2	x_doftx	元章女全 い正		NIS	us.	Android 4.1.1	
10	1002	1002@80210	portal	0.00213	2013- 05-31 12:36:41	36分钟 17秒	172.10.2.1	172.16.8.3	1_0011	148	2013-05-28 12:23:11	PC	Microsoft	Windows 7	

可以看出UAM已经通过DHCP特征方式识别出终端类型并应用了不同的安全策略,具体的识别过程如下:

终端在向DHCP server获取IP时会发生dhcp request请求,报文如下:从中可以看出该终端的 dhcp 特征码为1,33,3,6,15,28,51,58,59,

Length: 9				
Parameter	Request	List	Iten:	<li>(1) Subnet Mask</li>
Parameter	Request	List	Iten:	(33) Staric Route
Parameter	Request	List	Iten:	(3) Router
Parameter	Request	List	Iten:	(6) Domain Name Server
Parameter	Request	List	Iten:	(15) Domain Name
Parameter	Request	List	Iten:	(28) Broadcast Address
Parameter	Request	List	Iten:	(51) IP Address Lease Time
Parameter	Request	List	Iten:	(58) Renewal Time Value
Parameter	Request	List	Iten:	(59) Rebinding Time Value

而这些特征码是和在UAM中之前预定义的魅族特征码相一致,也就是说只要某个终端的DHCP特征码是这个值,均会被识别为魅族。DHCP特征码中的厂商、终端类型和操作系统信息均需要提前添加。



13:15	記 🗊 🔅 🛈 器
设置 WLAN	
Øwlan	1
网络	
x_dot1x 已连接	(îə
x_byod	((+
x_portal	((1-

## 手机ping172.16.0.9时:

9:41 88.80 7
Ping & DNS
2013-5-31 上午9:41:11
-n IP (rmnet0) 10.10.37.120
IP (eth0) fe80::237:6dff:feeb:
41ab%eth0
IP (eth0) 172.16.8.2
PING 172.16.0.9 (172.16.0.9)
56(84) bytes of data.
64 bytes from 172.16.0.9:
icmp_seq=1 ttl=125 time=14.6 ms
64 bytes from 172.16.0.9:
64 bytes from 172 16 0.9
icmn_seg=3 ttl=125 time=13.0 ms
icmp_seq=0 (ii=120 time=10.0 ms
172.16.0.9 ping statistics 3 packets transmitted, 3 received, 0% packet loss, time 2000ms
Ping 172.16.0.11时:
9:40 🕮 🐯 🎅 📶 🗂
Ping & DNS
2013-5-31 上午9:40:29
-di IP (rmnet0) 10.10.37.120
<ul> <li>IP (eth0) fe80::237:6dff:feeb:</li> </ul>
41ab%eth0
IP (eth0) 172.16.8.2
PING 172.16.0.11 (172.16.0.11)
56(84) bytes of data.

--- 172.16.0.11 ping statistics ---3 packets transmitted, 0 received, 100% packet loss, time 2002ms

可见,已经达到了预期的效果

四、注意事项

1: 该认证方式前提要求已经在UAM侧创建了账号,认证时输入账号信息即可;

2:终端第一次认证上线时,由于未获取IP,所以UAM不会识别终端信息,也不会应用终端的场景信息,等终端认证通过并获取IP后;终端第二次认证时才会匹配场景信息。

3:第一次认证上线时,默认接入规则需为证书认证;

4:客户端证书名称必须与认证账号一至;

5:如果用系统自带客户端认证,则终端第一次认证通过后,终端并不会立即下线,只有等终端打 开域名并跳转至BYOD页面后才会下线并应用新的控制策略。