wlan接入 MAC地址认证 AAA 杨攀 2015-11-12 发表

一、本地转发MAC快速认证简介

为了加快提升手机用户使用WLAN的便利性,降低使用WLAN的门槛,在浙江移动省公司的牵头下,召集各个厂家包括华三、摩托、大唐、中兴、亚信一起开发了WLAN手机上网MAC快速认证功能。

使用该功能后,手机用户初次登陆WLAN,弹出Portal登陆页面,手工输入用户名和密码进行正常的PORTAL认证,与此同时,AC会将用户MAC等信息传递给后端MAC绑定服务器,以后该手机用户再次上网时就无需输入任何信息,AC会自动将用户信息传递给后台进行认证,从而免去了用户每次手工输入用户名和密码的麻烦,简化了上网流程。同时为了减轻AC对用户数据转发的压力,实现在无线控制器AC上对无线用户进行MAC快速认证,但认证成功后业务数据走AP本地转发。

MAC快速认证本地转发流程如下:

- 1、用户打开应用程序如浏览器, QQ等, 进行上网操作。
- 2、AC检测到流量超过门限,通知MAC绑定服务器进行MAC检查。

3、MAC绑定服务器对MAC进行检查,如果已经绑定,则提取该MAC地址对应的用户名和密码,这时客户端在通过AP进行HTTP重定向发起portal认证。

- 4、AC向集团的AAA服务器进行认证请求,认证通过后,通知绑定服务器。
- 5、当认证完成之后,用户的数据流量通过AP走本地转发

二、组网需求:

如图1-1,总部的AC与分支机构的AP二层关联并作为DHCP server为无线客户端分配地址;wx6 103作为无线客户端的网关并为AP分配地址,具体要求如下:

AC先向服务器发送MAC快速认证请求,如果用户第一次上线,则服务器向AC发起认证请求,用 户认证成功后,AC将用户规则下发到AP设备上,用户报文在AP上直接做转发;如果用户不是第一次 上线,用户不需要进行认证,用户报文在AP上直接转发。

图1-1 AC为无线客户端分配地址配置组网图



三、配置步骤:

3.1配置AC

#创建vlan 1的三层虚机接口,并为该接口配置IP地址,其中VLAN 1用于和IMC服务器之间进行通信

۰

system-view [AC] interface vlan-interface 1 [AC-Vlan-interface10] ip address 192.168.0.4 24 [AC-Vlan-interface10] quit #创建VLAN 10及其对应的VLAN接口,并为该接口配置IP地址,其中VLAN10用于和AP之间进行 通信。 system-view [AC] vlan 10

[AC-vlan10] quit

[AC] interface vlan-interface 10 [AC-Vlan-interface10] ip address 10.1.1.1 24 [AC-Vlan-interface10] guit # 创建VLAN 30及其对应的VLAN接口,并为该接口配置IP地址,其中VLAN 30用于起Portal服务。 [AC] vlan 30 [AC-vlan30] quit [AC] interface vlan-interface 30 [AC-Vlan-interface30] ip address 30.1.1.1 24 [AC-Vlan-interface30] quit # 配置AC的以太网1/0/1口的类型为Trunk口并允许所有VLAN通过,用于与AP、无线客户端、IMC之间 通信。 [AC] interface g1/0/1 [AC-Bridge-Aggregation1] port link-type trunk [AC-Bridge-Aggregation1] port trunk permit vlan all [AC-Bridge-Aggregation1] quit (1) 配置DHCP服务 # 使能DHCP功能。 [AC] dhcp enable #配置DHCP地址池10,用于为AP动态分配地址。 [AC] dhcp server ip-pool vlan10 [AC-dhcp-pool-10] network 10.1.1.0 24 [AC-dhcp-pool-10] gateway-list 10.1.1.1 [AC-dhcp-pool-10] dns-list 10.1.1.1 [AC-dhcp-pool-10] quit # 配置DHCP地址池30,用于为Client动态分配地址。 [AC] dhcp server ip-pool vlan30 [AC-dhcp-pool-30] network 30.1.1.0 24 [AC-dhcp-pool-30] gateway-list 30.1.1.1 [AC-dhcp-pool-30] dns-list 30.1.1.1 [AC-dhcp-pool-30] quit (2) 配置WLAN-ESS接口 #创建接口WLAN-ESS 30。 [AC] interface wlan-ess 30 #配置端口的链路类型为Access, 允许VLAN 30通过。 [AC-WLAN-ESS30] port access vlan 30 [AC-WLAN-ESS30] quit (3)配置无线服务模板 #创建clear类型的服务模板30。 [AC] wlan service-template 30 clear # 设置当前服务模板的SSID为portal-local。 [AC-wlan-st-30] ssid portal-local #将WLAN-ESS30接口绑定到服务模板30。 [AC-wlan-st-30] bind wlan-ess 30 #开启用户本地转发功能。 [AC-wlan-st-30] client forwarding-mode local #开启无线客户端透传DHCP报文到AC的功能。 [AC-wlan-st-30] client dhcp-server centralized # 使能服务模板。 [AC-wlan-st-30] service-template enable [AC-wlan-st-30] quit 在AC下绑定无线服务模板 #创建AP模板,名称为officeap,型号名称选择WA3628i-AGN,并配置序列号。 [AC] wlan ap ap1 model WA3628i-AGN

[AC-wlan-ap-ap1] serial-id 210235A42MB108000002

[AC-wlan-ap-ap1] map-configuration apcfg.txt

#进入radio 1射频视图。

[AC-wlan-ap-ap1] radio 1

#配置射频的工作信道为161。

[AC-wlan-ap-ap1-radio-1] channel 161

#将服务模板30绑定到AP的radio 1口。

[AC-wlan-ap-ap1-radio-1] service-template 30

- [AC-wlan-ap-ap1-radio-1] radio enable
- [AC-wlan-ap-ap1-radio-1] quit
- [AC-wlan-ap-ap1]quit

(4)配置Portal认证

配置Portal服务器地址为172.17.0.100,并指定服务器对应的url。

[AC] portal server imc ip 172.17.0.100 key simple h3c url http://172.17.0.100:8080/portal

配置Portal免认证规则1,用于放行AC上起portal的接口能够与portal服务器通信。

[AC] portal free-rule 1 source interface bridge-aggregation1 destination any

#配置AC通过WLAN获取Portal用户信息。

[AC] portal host-check wlan

配置RADIUS方案portal。

[AC] radius scheme portal

#配置认证、计费和授权服务器的IP地址为172.17.0.100。

[AC-radius-portal] primary authentication 172.17.0.100

[AC-radius-portal] primary accounting 172.17.0.100

配置与认证、计费和授权服务器交互报文时的共享密钥均为h3c。

[AC-radius-portal] key authentication simple h3c

[AC-radius-portal] key accounting simple h3c

#指定发送给RADIUS方案portal中RADIUS服务器的用户名不得携带域名。

[AC-radius-portal] user-name-format without-domain

配置设备发送RADIUS报文使用的源IP地址为192.168.0.4。

[AC-radius-portal] nas-ip 192.168.0.4

[AC-radius-portal] quit

#配置AAA认证域portal。

[AC] domain portal

设置ISP域的认证、授权和计费方法均为RADIUS方式。

[AC-isp-portal] authentication portal radius-scheme portal

[AC-isp-portal] accounting portal radius-scheme portal

[AC-isp-portal] authorization portal radius-scheme portal

[AC-isp-portal] quit

[AC] interface vlan-interface 30

#配置接口VLAN 30为Portal直接认证的接口。

[AC-Vlan-interface30] portal server imc method direct

#指定从接口接入的IPv4 Portal用户使用认证域为portal。

[AC-Vlan-interface30] portal domain portal

配置接口发送Portal报文使用的IPv4源地址为192.168.0.4。

[AC-Vlan-interface30] portal nas-ip 192.168.0.4

#开启Portal本地转发功能。

[AC-Vlan-interface30] portal forwarding-mode local

#配置MAC绑定服务器的IP和UDP端口,缺省值为5010

[AC-Vlan-interface30] portal mac-trigger server ip 172.17.0.100

#配置MAC快速认证功能在接口下使能

[AC-Vlan-interface30] portal mac-trigger enable

[AC-Vlan-interface30] quit

#配置arp-snooping功能。

[AC] arp-snooping enable

#配置learn-ipaddr功能

[AC] wlan client learn-ipaddr enable

3.2配置SW

#为vlan 1配置对应接口IP地址,用于和AC之间通信。

system-view

[SW] interface vlan-interface 1

[SW-Vlan-interface1] ip address 192.168.0.2 24

[SW-Vlan-interface1] quit

配置SW与Router连接的物理接口的类型为Trunk, 允许所有VLAN通过。

[SW] interface gigabitethernet 1/0/1

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

[SW-GigabitEthernet1/0/1] port trunk permit vlan all

[SW-GigabitEthernet1/0/1] quit

配置SW与AP连接的物理接口属性,使能POE为AP供电,类型为Trunk,允许所有VLAN通过,且PV ID设置为10。

[SW] interface gigabitethernet 1/0/2

[SW-GigabitEthernet1/0/2] poe enable

[SW-GigabitEthernet1/0/2] port link-type trunk

[SW-GigabitEthernet1/0/2] port trunk permit vlan all

[SW-GigabitEthernet1/0/2] port trunk pvid vlan 10

[SW-GigabitEthernet1/0/2] quit

#创建VLAN20,并配置对应接口的IP地址,用于和IMC服务器之间通信。

[SW] vlan 20

[SW-vlan30] quit

[SW] interface vlan-interface 20

[SW-Vlan-interface30] ip address 172.17.0.254 24

[SW-Vlan-interface30] quit

3.2 map.txt配置文件

编辑AP的配置文件map.txt。

system-view #http://172.17.0.100:8080/portal/配置portal服务器地址为 172.17.0.100,并指定服务器对应的url portal server imc ip 172.17.0.100 key simple h3c url #destination any/配置portal免认证规则1,用于放行AP上起portal 的接口能够与portal服务器通信 portal free-rule 1 source interface GigabitEthernet 1/0/1 #配置ap通过WLAN获取Portal用户信息。 portal host-check wlan #创建vlan 30 vlan 30

#创建VLAN30对应接口,并接入接口VLAN30视图

interface vlan 30

#接口下指定portal服务器并配置为直接认证方式

portal server imc method direct

#配置接口发送portal报文使用的源地址为AC的地址

portal nas-ip 192.168.0.4

#配置MAC快速认证功能在接口下使能

portal mac-trigger enable

#进入到AP的物理接口

interface GigabitEthernet 1/0/1

#配置接口GigabitEthernet1/0/1类型为Trunk

port link-type trunk port

配置接口GigabitEthernet1/0/1允许所有VLAN通过

四、 IMC的配置

4.1配置Portal服务器。

登录进入iMC管理平台,选择"用户"页签,单击导航树中的[接入策略管理/Portal服务管理/服务器 配置]菜单项,进入服务器配置页面,使用缺省配置。

2. 用户 > 接入策略管理 > Portal服务管理 > 服务器配置						
Portal服务器配置						
基本信息						
日志级别*	调试	•				
Portal Server						
报文请求超时时长(秒)*	4	0	逃生心跳间隔时长(秒)	e	20	?
用户心跳间隔时长(分钟)*	5	0	LB设备地址			
Portal Web						
请求报文题时时长(秒)*	15	0	交互报文编码			?
校验终端用户请求报文	문 •	•	使用缓存		문	•
HTTP心跳界面展示方式	新页面	•	HTTPS心跳界面展示?	ਤੇਸ਼	原页面	•
	http://172.17.0.1 https://172.17.0.	100:8080/portal/ 100:8443/portal/				
Portal主页						

配置IP地址组。

选择"用户"页签,单击导航树[接入策略管理/Portal服务管理/IP地址组配置]菜单项,进入IP地址组配置 页面,在该页面中单击<增加>按钮,进入增加IP地址组配置页面。

- · 输入IP地址组名: test5;
- · 输入起始地址: 30.1.1.1;
 - 输入终止地址: 30.1.1.100;

其他采用缺省配置, 单击<确定>按钮完成操作

プ用户 > 接入策略管理 > Portal 服务管理 > IP地址组配置 > 增加IP地址组						
增加IP地址组						
IP地址组名 *	test5					
起始地址 *	30.1.1.1					
终止地址 *	30.1.1.100					
业务分组	未分组	-				
类型 *	普通	•				
				确定取消		

增加Portal设备。

选择"用户"页签,单击导航树中的[接入策略管理/Portal服务管理/设备配置]菜单项,进入设备配置页面 。在该页面中单击<增加>按钮,进入增加设备信息配置页面。

- · 输入设备名: test5;
- · 输入IP地址:即AC上配置的portal bas-ip地址, 192.168.0.4;
- · 输入密钥:h3c,与AC上配置的portal server密钥一致;
- · 组网方式改为"直连"类型;
- · 其他采用默认配置,单击<确定>按钮完成操作。

UP用户 > 接入策略管理 > Portal服务管理 > 设备配置	> 増加设备信息		
增加设备信息			
设备信息			
设备名 *	test5	业务分组 *	未分组 🔻
版本 *	Portal 2.0 🔻	IP地址 *	192.168.0.4
监听端口 *	2000	本地Challenge *	否 🔻
认证重发次数 *	0	下线重发次数 *	1
支持逃生心跳 *		支持用户心跳 *	否 🔻
密钥 *	•••	确认密钥 *	•••
组网方式*	直连 ▼		
设备描述			
		· 御寺 - 取消	

增加端口组信息。

在Portal设备配置页面中的设备信息列表中,单击""图标,进入端口组信息配置页面。

・ 用户> 接入策略管理 > P	Portal服务管理 > 设备配置					者加入依藏 ④	
设备信息查询							
设备名			版本		-		
下没结果		-	业务分组		-	2 59 22	
#ttin							
设备名 ≎	版本 🗘	业务分组 ≎	IP地址	最近一次下发时间 ≎	下发结果	要作	
test1	Portal 2.0	未分组	192.168.0.7		未下汝	V B B B	
test	Portal 2.0	未分组	192.168.0.4		未下发		
local11	Portal 2.0	未分组	192.168.0.24		未下发	S B B B	
local	Portal 2.0	未分组	192.168.0.100		未下发	V B B B	
共有4条记录,当前第1	共称4元法、当相第1-4,第1/1页。						

在端口组信息配置页面中点击<增加>按钮,进入增加端口组信息配置页面。

- · 输入端口组名: test5;
- · 选择IP地址组: test5;
- · 选择支持无感知认证;
- · 其他采用默认配置,单击<确定>按钮完成操作。

♥用户> 接入策略管理 > Portal服务管理 > 设备	配置 > 靖口组信息配置 > 增加消口组	信息		
增加納口組備應				
端□组名 [•]	testS		提示语言 *	动态检测
开始第二	0		终止講□ *	222222
协议类型 *	HTTP	-	快速认证 *	* *
是否NAT *	否	-	错误透传 *	是 🔻
认证方式 *	CHAPIAIE	-	IP地址组*	test5 💌
心期间隔(分钟) *	0		心跳超时(分钟) *	0
用户域名			第口组描述	
无感知认证	支持	-	畜户;請防破解 ★	杏 ▼
页面推送策略		-	缺省认证页面	•
			确定 取消	

4.2 配置接入服务

增加接入设备

选择"资源"标签,单击导航树中的[增加设备]菜单项,进入增加设备视图下。 设置设备的IP地址为192.168.0.4,也就是和设备交互报文的地址。

点击配置Telnet选项

们名或IP地址 *	192.168.0.4		Nozilla Firefox	- 0 - X -
重标签			172.17.0.100:8080/imc/res/paratemplate/telnet/select.jsf?beanName=resDeviceBean	
A		Ŷ	●手工编辑Telnet参数 从已有的Telnet参数模板中选取	
新 分组		• ?	认证权式 用户名 + 密码 ▼	
蒙方式	Telnet	• (?)	用户名 * admin	
将设备的Trap发送到本网管系统				
设备支持Ping操作⑦			密码 •••••	
Ping不通也加入⑦			超时时间(1-60秒)* 4	
将LoopBack地址作为管理IP			約 2315	
E置SNMP参数				
R置Teinet参数			-	
設置				
证模式		无用户名 + 无密码		
1919年1月(1957)		4		

选择"用户"标签,单击导航树中的[接入策略管理/接入设备管理/接入设备配置]菜单项,进入接入设备配置页面。在该页面中单击<增加>按钮,进入增加接入设备页面。

- I 设置与AC交互报文时使用的认证、计费共享密钥为"h3c",该密码与AC配置RADIUS方案时的地址 一致;
- I选择接入设备类型为"H3C(General)";
- | 其它参数采用缺省值,并单击<确定>按钮完成操作

| 点击"选择"按钮;

🔁 > 用户 > 接入策略管理 > 接入设备	管理 > 接入设备配置 > 增加接入设备			
接入配置				
认证朔□ *	1812	it	-费请□ *	1813
组网方式	不启用混合组网	41	务类型	LAN接入业务
接入设备类型	H3C(General)	44	务分组	未分组
共愿密明 *	•••	确	认共享密明 *	•••
接入设备分组	无			
设备列表 选择 手工增加 全部渐渐				
设备名称	设备IP地址	设备型号	备注	1
未找到符合条件的记录。				
共有0条记录。				
		and	ROH	

点击"IP视图",选择自己要添加的设备,点击向下添加按钮

入配置								
		🧶 H3C 智能管理中心 - Mozilla Firefox						
认证端口 *	1812	🕙 172.17.0.100:8080/imc/res/devicese	elect/gwt/DeviceSelect.jsf	?locale=zh_CN&bea	inName=acmAcces	sDevice&sele	ectType=null&viev	
组网方式	不启用	查询条件	《 可选择的	的设备 - 已自动过城不去	转的设备			 家入业
		我國 查询	状态	设备标签 🔺	设备P	设备类型	设备系列	
接入设置荣望	H3C(G	4 🥼 PRE	● 严重	192.168.0.1	192.168.0.1	PC	ICMP	8
共享密钥 *		192.168.0.0/24[5]	 未知 	НЗС	192.168.0.4	无线设备	H3C WX	
		▶ 💋 设备视图						
	-							Ŀ
香列表								
	_		14 4	第1 页共1页)	• M 🕹 🔤		显示1-2,共2条	
选择 手工增加 全部清除						F 🕇 🎕	4	
			已选择的	的设备		_		
设备名称			状态	设备标签	设备P	设备类型	设备系列	
长找到符合条件的记录。								
	_							E
共有0条记录。								
	-							
			没有数据	國需要显示				

#增加接入策略。

选择"用户"标签,单击导航树中的[接入策略管理/接入策略管理]菜单项,进入接入策略配置页面。在接入策略列表中点击<增加>按钮,进入增加接入策略页面。

接入策略名输入"test5";

· 业务分组"未分组";

其它参数采用缺省值,并单击<确定>按钮完成操作

ī.				
	3. 用户 > 按入策略管理 > 按入策略管理 > 增加接入策略			
	基本信息			
	接入策略名*	test5		
	业务分组*	未分组 マ		
	描述			
	授权信息			
	接入时段	无	分配IP地址 *	否 •
	下行速率(Kbps)		上行速率(Kbps)	
	优先级		启用RSA认证	
	证书认证	●不启用 ─EAP证书认证 ─WAPf证书认证		
	认证证书类型	EAP-TLS认证 💌		
	下发VLAN			
	下发User Profile		下发用户组	0
	下发ACL			

增加接入服务。

.

选择"用户"标签,单击导航树中的[接入策略管理/接入服务管理]菜单项,进入接入服务配置页面。在接入服务列表中点击<增加>按钮。

- · 服务名输入"test5";
- · 缺省接入策略"test5";
 - 勾选portal无感知认证;

其它参数采用缺省值,并单击<确定>按钮完成操作。

Q4用户 > 接入策略管理 > 接入服务管理 > 增加接入服务					
基本信息					
服务名 *	test5	٦	服务后缴		
业务分组 *	未分组	•	缺盲接入策略 *	test5	• 0
缺資私有属性下发策略*	不使用	• ?			
缺貨单帐号在线数量限制*	0				
服务描述					
✓ 可申请 ?			✓ Portal无感知认证 ⑦		
接入场展列表					
mita					
名称	接入策略		私有属性下发策略	优先级	462X
未找到符合条件的记录。					
			確定 取消		

4.3增加接入用户。

#选择"用户"标签,单击导航树中的[接入用户管理/接入用户]菜单项,进入到接入用户配置页面。在接入用户列表中点击<增加>按钮,进入增加接入用户页面。

- · 在增加接入用户页面,单击<增加用户>按钮弹出增加用户窗口;
- · 输入用户名"test5";
- · 输入证件号码"01022171414";
- · 单击<检查是否可用>按钮;
- · 如用户姓名和证件号码可用,单击<确定>按钮完成操作。

♣o 用户 > 增加用户						
増加用户						
基本信息						
用户姓名 *	test5	1	证件号码 *	01022171414	1	检查是否可用
通讯地址			电话		?	
电子邮件		?	用户分组 ★	未分组	ບໍ່ໃ	
□开通自助帐户						
			确定	取消		

点击"确定"按钮,选择"增加接入用户"。

€o用户 > 増加用户结果	
增加用户完成,您可继续选择如下操作:	
増加接入用户 返回用户列表 查看用户详细信息 继续增加用户	增加接入用户帐号。 返回用户列表。 查看刚刚增加的用户的详细信息。 继续增加新的用户。

- · 账号名输入"test5";
- · 密码输入"test5";
- · 强portal无感知认证最大数设置为10;
- · 勾选接入服务"test5";

用户 > 接入用户 > 增加接入用户						
接入用户						
接入信息						
用户姓名 *	test5 选择	境加用户				
₩号名 *	test5					
预开户用户	缺省BYOD用户	MAC地址认证用户		主机名用户		快速认证用户
密码 *	•••••		密码确认*		•••••	
✔ 允许用户修改密码		启用用户密码控制策略			下次豐景须修改密码	
生效时间			失败时间			
最大闲暨时长(分钟)			在线数量限制		10	
Portal无题如认证最大绑定数 *	10					
登录提示信息						
接入服务						

服务名	服务后缀	状态	分配IP地址
123		可申请	
dotlx		可申请	
Icoal		可申请	
mac		可申请	
macpsk	cams	可申请	
portal		可申请	
test		可申请	
test2		可申请	
test3		可申请	
test4		可申请	
test5		可申请	
test6	portal	可申请	

单击<确定>按钮完成操作。

五、验证配置

(1)用户使用智能终端通过浏览器访问网络,重定向到Portal认证页面。用户输入用

户名、密码、服务等认证信息,进行上线认证。

(2)认证成功后,用户下线。

(3)用户再次使用该智能终端访问网络,这时不需要输入用户名和密码,直接上线。

(4)此时可在iMC上观察到绑定该智能终端MAC地址信息

(別か > Ponteの語名の記念 (別の > Noteの語名の記念 (別の > Noteの語名の記念								
无感知认证用户查询								
※号名 場合服务名]	MAC地址 天感知认证状态		0			
息用/蒙用时间		0	¥.		8		<u>-</u> 28 -22	
Leen Articlevic Articlevic Theory								
	MACIELE 0	株号名 ▲	用户姓名 ♀	服务名 0	无感知认证状态 0	启用/禁用时间 ◊	详细信息	
	F4:8E:92:E0:4D:CF	local	local	lcoal	启用	2015-11-12 14:35:42	袤	
共有1条记录,当前第1。	-1,第1/1页。					« <	1 → » 50 •	

配置思路:

- · 为实现AC与Portal服务器通信,在AC上配置到portal服务器的静态路由;
- · 在AC上配置DHCP功能,使得AC统一分配、集中管理无线客户端的地址;
- · 为实现MAC快速认证,在AC和AP上配置MAC快速认证;
- · 为了使AP能够直接转发Client报文,需要在AC的服务模板下开启本地转发功

能,同时通过下发map-configuration文件来对AP进行配置实现本地转发。

配置注意事项:

- · AC和AP上都要配置从WLAN获取用户信息的功能;
- · AC和AP上都需要配置触发无感知认证的功能。
- · 配置AP的序列号时请确保该序列号与AP唯一对应, AP的序列号可以通过AP设备 背面的标签获取。
- · 配置MAC认证服务器必须在使能三层Portal认证的接口下使能。
- 为使MAC快速认证功能生效,必须保证配置了MAC绑定服务器的IP和UDP端口信
- 息,且接口使能了Portal。