802.1X wlan接入 AAA 吴骋骐 2014-04-16 发表

wx系列AC 远程802.1x无线认证和IMCv7配合典型配置案例及认证过程 分析

一、组网需求及背景

1.802.1x认证介绍

802.1x协议通俗意义上是一个通用认证的封装协议,可以封装多种认证,对于WLAN网络比较常用的有PEAP和EAP-TLS,而PAP和CHAP不能使用,因为在WLAN网络中802.1x认证过程还有一个重要的作用就是在客户端和设备侧协商产生一个4-way handshake协商的种子密钥,而PAP和CHAP是无法完成该功能的。

802.1x协议主要实现认证设备和认证终端之间的交互,而对具体的认证报文会通过radius发送给认证服务器。设备首先请求客户端的ID来触发802.1x认证,之后实际上实现了802.1x报文和radius报文之间的一个中继功能,将来自无线客户端的802.1x报文的认证信息进行中继通过radius报文发送给指定的认证服务器;同时将认证服务器回应的radius报文解析转换成802.1x报文并最终发送给无线客户端。

对于802.1x认证本身,无线用户和有线用户没有任何的差别,只是无线用户在认证成功后会使用认证过程中产生的radius key生成后续4-way handshake的种子密钥。

另外,顺带说明4-way handshake可以作为802.1x协议的一部分,是专门为WLAN设计,通过 802.1x的EAPOL-Key报文完成无线客户端和设备之间的密钥协商。WPA2+PSK还是WPA2+802.1x 接入都存在4-way handshake过程协商无线链路的密钥,唯一的区别使用PSK方式的时候前面没 有任何的其他认证,而是在4-Way handshake过程中同步完成PSK认证。

2.认证流程说明:

1.在整个过程之前,还有一个WLAN服务的通告或者搜索过程:AP定期主动的发送Beacon报 文通告可以提供的WLAN服务;无线客户端可以发送Probe request报文搜索周围的WLAN无线网 络;

2.Open-system Authentication过程和Association过程就是802.11链路的协商过程,无论接入 哪种WLAN服务都必须通过这两个过程先建立802.11的无线链路,之后在无线链路建立成功的基础上,才可以完成其他的业务,例如密钥协商、地址申请、访问网络,等等;

3.从"EAPOL Start"到"认证成功"整个过程为802.1x认证过程,整个过程可能有多个报文交互,而且随着使用的EAP认证方式不同,报文的交互有所不同。当802.1x认证成功后,802.1x客户端和Radius server会产生一个相同的Radius key,该Radius key将会生成后面密钥协商的PMK;

4."4次握手Key协商"过程就是通常提到的密钥协商过程,该过程使用802.1x认证产生的PMK 作为种子密钥,在无线客户端和AP之间动态协商出后续无线链路传输数据报文所要使用的各种 密钥;

5.当上面的所有过程完成后,该无线客户端才会认为成功接入到WLAN服务中;如果任何一个环节出现错误都会被认为无线结果失败,AP会主动发送Disassociation报文将该无线客户端断开;

3.802.1x协商过程介绍

802.1x协议实际上在WLAN网络上才真正得到全面的应用,而过去有线网络的802.1x认证只 是使用了802.1x的认证部分的功能。

802.1x协议从功能上可以分为两大部分:认证部分和密钥协商部分。其中,认证部分需要客 户端、设备和认证服务器共同参与,最终完成对客户端的接入认证,特别在WLAN协议中还会在 客户端和认证服务器(包括设备)端协商一个radius key,带密钥将被作为后续密钥协商的种子 密钥。而密钥协商部分(4-way handshake)只是在设备和客户端之间进行交互,完成对称密钥 的协商和生成,生成的密钥最终会作为802.11链路使用的系列密钥。

下面介绍一下802.1x协商过程中的几个关键报文:

认证开始报文: 1、客户端发送EAP-Start报文触发认证; 2、设备侧会发送EAP request报文 请求客户端的用户名信息,启动对客户端的认证。

认证成功报文:当所有的认证成功以后,设备会向客户端发送EAP-Success报文通知客户端 认证成功。协议认为该报文作为消息通知报文,不需要进行重传。

认证下线或者失败报文:客户端也可以发送EAPOL-Logoff报文给设备端,主动要求下线。 设备端把端口状态从授权状态改变成未授权状态,并向客户端发送EAP-Failure报文

密钥协商报文: EAPOL-Key报文,目前仅支持802.11Key方式的密钥协商,可以包括两个协

商过程(4-way handshake和Group Key handshake)。目前该部分功能在WLAN的MAC模块完成,但是报文收发由802.1x模块完成。

根据目前的经验整个802.1x认证过程的协商报文可能超过20多个报文,在这个过程任何的一个报文出现丢失,都需要802.1x协议重传机制进行适当的保护,而这个重传机制直接决定了此次协商所需要的时间。

4.组网需求



本配置举例中,使用WX3010E作为无线控制器,版本号为R3507P14。AC作为AP网关(vla n-interface10:192.168.1.1/24)并配置DHCP server为AP分配IP地址。AC作为STA网关(vlan-interface10: 192.168.10.1/24)并配置DHCP Server为STA分配IP地址。交换机为AP提供POE供电

```
二、配置步骤
1、AC侧配置
[WX3010E]dis cu
#
version 5.20, Release 3507P14
#
sysname WX3010E
#
configure-user count 6
#
domain default enable dot1x
#
telnet server enable
#
port-security enable
#
dot1x authentication-method eap
#
oap management-ip 192.168.0.101 slot 0
#
password-recovery enable
#
vlan 1
```

vlan 10 # vlan 100 # radius scheme imc server-type extended primary authentication 10.153.43.100 primary accounting 10.153.43.100 key authentication cipher \$c\$3\$AlgC2dNmRlbCWNjuhqz3Z5aCVeu6iA== key accounting cipher \$c\$3\$o1Oiwu5dwthrUwlzdk02tCtcTobSMg== user-name-format without-domain nas-ip 10.153.43.141 # domain dot1x authentication lan-access radius-scheme imc authorization lan-access radius-scheme imc accounting lan-access radius-scheme imc 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 192.168.1.0 mask 255.255.255.0 gateway-list 192.168.1.1 # dhcp server ip-pool sta network 192.168.10.0 mask 255.255.255.0 gateway-list 192.168.10.1 dns-list 9.9.9.9 # user-group system group-attribute allow-guest # local-user admin password cipher \$c\$3\$VnWjDhTHgrxykrRnOJv3ANrCmwfBPzB9 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 crypto ssid h3c-1x bind WLAN-ESS 1 cipher-suite tkip security-ie wpa service-template enable # wlan ap-group default_group ap ap1 # interface Bridge-Aggregation1 port link-type trunk port trunk permit vlan all # interface NULL0 # interface Vlan-interface1 ip address 192.168.1.1 255.255.255.0 # interface Vlan-interface10 ip address 192.168.10.1 255.255.255.0 # interface Vlan-interface100 ip address 10.153.43.141 255.255.255.0

interface GigabitEthernet1/0/1 port link-type trunk port trunk permit vlan all port link-aggregation group 1 # interface GigabitEthernet1/0/2 port link-type trunk port trunk permit vlan all port link-aggregation group 1 # interface WLAN-ESS1 port access vlan 10 port-security port-mode userlogin-secure-ext port-security tx-key-type 11key undo dot1x handshake

dot1x mandatory-domain dot1x

#

wlan ap ap1 model WA2620 id 1

serial-id 5866-BA5E-C6E0

radio 1 radio 2

channel 6

max-power 15

service-template 1

radio enable

#

snmp-agent

snmp-agent local-engineid 800063A203000FE2873066

snmp-agent community read public

snmp-agent community write private

snmp-agent sys-info version all

snmp-agent target-host trap address udp-domain 10.153.43.100 params securityname pu

blic v2c

wlan ips malformed-detect-policy default signature deauth_flood signature-id 1 signature broadcast_deauth_flood signature-id 2 signature disassoc_flood signature-id 3 signature broadcast_disassoc_flood signature-id 4 signature eapol_logoff_flood signature-id 5 signature eap_success_flood signature-id 6 signature eap_failure_flood signature-id 7 signature pspoll_flood signature-id 8 signature cts_flood signature-id 9 signature rts_flood signature-id 10 signature-policy default countermeasure-policy default attack-detect-policy default virtual-security-domain default attack-detect-policy default malformed-detect-policy default signature-policy default countermeasure-policy default # dhcp enable # arp-snooping enable # user-interface con 0 user-interface vty 0 4

authentication-mode scheme

user privilege level 3

#

Return

主要配置步骤

(1)创建radius方案imc并进入其视图
#创建radius方案imc并进入其视图
[WX3010E]radius scheme imc
#radius服务器类型设置为extended
[WX3010E-radius-imc]server-type extended
#配置主认证radius服务器的ip地址
[WX3010E-radius-imc]primary authentication 10.153.43.100
#配置主计费radius服务器的ip地址
[WX3010E-radius-imc]primary accounting 10.153.43.100
设置系统与认证RADIUS服务器交互报文时的共享密钥为h3c。
[WX3010E-radius-imc]key authentication h3c
设置系统与计费RADIUS服务器交互报文时的共享密钥为h3c。
[WX3010E-radius-imc]key accounting h3c
#绑定nas-ip
[WX3010E-radius-imc]nas-ip 10.153.43.141

(2)创建domain域

创建dot1x域并进入其视图 [WX3010E]domain dot1x #为lan-access用户配置认证方案为RADIUS方案,方案名为imc [WX3010E-isp-dot1x]authentication lan-access radius-scheme imc #为lan-access用户配置授权方案为RADIUS方案,方案名为imc [WX3010E-isp-dot1x]authorization lan-access radius-scheme imc #为lan-access用户配置计费方案为RADIUS方案,方案名为imc [WX3010E-isp-dot1x]accounting lan-access radius-scheme imc

(3)#**认证缺省域为dot1**x

[WX3010E]domain default enable dot1x #全局使能端口安全 [WX3010E]port-security enable #设置802.1x的认证方式为EAP [WX3010E]dot1x authentication-method eap

(4)#创建AP地址池

[WX3010E]dhcp server ip-pool ap [WX3010E-dhcp-pool-ap]network 192.168.1.0 mask 255.255.255.0 [WX3010E-dhcp-pool-ap]gateway-list 192.168.1.1 #创建客户端地址池 [WX3010E]dhcp server ip-pool sta [WX3010E-dhcp-pool-sta]network 192.168.10.0 mask 255.255.255.0 [WX3010E-dhcp-pool-sta]gateway-list 192.168.10.1 [WX3010E-dhcp-pool-sta]dns-list 9.9.9.9

(5)#配置无线接口WLAN-ESS1

#创建接口WLAN-ESS1并进入其视图 interface WLAN-ESS1 #接口WLAN-ESS1下放通对应的业务vlan [WX3010E-WLAN-ESS1]port access vlan 10 #WLAN-ESS 1 上使能802.1x端口安全模式 [WX3010E-WLAN-ESS1]port-security port-mode userlogin-secure-ext #在接口WLAN-ESS1下使能11key类型的密钥协商功能 [WX3010E-WLAN-ESS1]port-security tx-key-type 11key #关闭dot1x握手模式 [WX3010E-WLAN-ESS1]undo dot1x handshake #dot1x强制认证域为dot1x [WX3010E-WLAN-ESS1]dot1x mandatory-domain dot1x

(6)#无线服务模板配置

#创建crypto类型的服务模板1并进入其视图 [WX3010E]wlan service-template 1 crypto #设置当前服务模板的SSID(服务模板的标识)为h3c-1x [WX3010E-wlan-st-1]ssid h3c-1x #将WLAN-ESS1接口绑定到服务模板1 [WX3010E-wlan-st-1]bind WLAN-ESS 1 #使能TKIP加密套件 [WX3010E-wlan-st-1]cipher-suite tkip #设置在AP发送信标和探查响应帧时携带WPA IE [WX3010E-wlan-st-1]security-ie wpa #使能服务模板 [WX3010E-wlan-st-1]service-template enable

(7)#创建相应的vlan三层虚接口

#创建管理vlan 三层接口 [WX3010E]interface Vlan-interface1 [WX3010E-Vlan-interface1]ip address 192.168.1.1 255.255.255.0 #创建业务vlan 三层接口 [WX3010E]interface Vlan-interface10 [WX3010E-Vlan-interface10]ip address 192.168.10.1 255.255.255.0 #创建连接服务器vlan 三层接口,即nas-ip地址 [WX3010E]interface Vlan-interface100 [WX3010E]interface Vlan-interface100

2、SW侧配置(略)

3、IMC 步骤配置

1. 接入设备配置:

#登录iMC平台,点击"资源"->"增加设备"。

#IP地址10.153.43.141, 并配置SNMP和Telnet参数, 和AC上snmp-agent和local-user(服务类型telnet)配置一致, 点击"确定"。

H3C	Intelligent M	anagement Center		💄 admin 🔹 🕅 🕄 👯 🕄	i 关于 也注销
*	首页 前	党源 用户 业务 计	攀 报表 系统管理	4. 2008	Q, 8
視問管理	~	🔜 提筆 > 增加设备			⑦帮助
洪源管理	~	- 设备基本信息			
终端准入管理	~	主机名弦尸绝处 *	10 153 43 141		
网络资产	~	设备标签			
虚拟网络管理	~	推码	0		
		设备分组	• ⑦		
合快速入门		登录方式	无 • ⑦		
□ 住能稅間 職 监視设置 ② 全局指标设置 ③ 网络括扑设置 ▲ 住能送项 ◎ 只知性能出現 ■ 和約代知	,	●時最新的Trac支送到本同會系统 ●投資支持Pling操作⑦ ●Pling不過也加入⑦ ●時LoopBack地址作力管理P			
应用管理	~	+ 配置 SNMP 參數			
		+ 配置Teinet参数			
		+ 配置SSH参数			
Ta 🐔 🔺	3 🔺 46	▲6 ▲ 138 ± 16	版权所有 @ 2007-2013 杭州华三道信技术有限公司,保留一切权	利。	e K

#点击"用户"->"接入策略管理"->"接入设备管理",选择"选择"。

НЗС	Intellige	nt N	lanagement Cent	er				💄 admin 🛛 🕅 👯 🔃	i 关于 也注册
*	首页		資源 用户	业务 告讐 探護	医二乙酸 化二乙酸 化二乙酸 化二乙酸 化二乙酸 化二乙酸 化二乙酸 化二乙酸 化			1 100 - 室間设备	Q, 8
用户管理		~ .	📅 用户 > 接入编辑	管理 > 接入设备管理 > 接入设备自	置 > 增加接入设备				⑦ 梨肋
接入用户管理		~	接入奠团						
访客管理		~	认证的口 、	1812		计费油口 *	1813		
终端管理		~	组网方式	不直用混合组网	*	业务类型	LAN接入业务	¥	
用户接入日志		~	接入设备类型	H3C(General)	*	接入设备分组	无	*	
接入策略管理		~	共享密辑 *			确认共享密钥。			
12 快速入门 ○ 接入服务管理 □ 接入解明管理		> =	业务分组	未分组	*				
 ・ ・ ・			选择 手	I MI Sifili					
日本 法入设备配	2		设备名称	设备IP地址		동코号	香注	網線	
し 扱入気留英	10月1五 秋彩船配置		未找到符合条件的证	2录。					
▶ LDAP业务管理			共有0条记录。						
 Porta服务管理 ・						前定 取消			
🔯 🐔 🔺	48		<u>4</u> 6 <u>4</u> 139	16		版权所有 @ 2007-2013 杭/	用华三道信技术有限公司,保留	9—切积利。	e K

#输入设备地址10.153.43.141,精确查找,添加对应设备到"已选择的设备中",点击"确定"。

查询条件 《	可选择的	的设备一已自动过滤不支持	的设备		
视图 查询	状态	设备标签 ▲	设备IP	设备类型	设备系列
· 삼종파·					
☑ 精确查询					
10.153.43.141					
×					
设备标金:					
设备状态:	14 4	第1 页共1页 ▶ ▶	&	显	示1-1,共1条
↓ 设备类型:			- 😻 🖡	1 🔶	
×	已选择的	的设备	_		
设备系列:	状态	设备标签	设备₽	设备类型	设备系列
「ビジュ・	●重要	10.153.43.141	10.153.43.141	无线设备	H3C WX3000
位置:					
设备可达性:					
•					
查询 重置	4+++	`- -			
	共有1余	吃來			
	确定	取消			

#选择"确定"。

H3C	Intellig	ent M	anag	ement Cent	ter							👤 admin 🛛	③林昀 i 关于	山注領
*	首页		发源	用户	业务	告讐	报表	系统管理				📲 🗸 查询设备		Q, ¥
用户管理		~ .	17	用户 > 描入編輯	8曾理 ≻ 接入	後音管理 >	搞入设备 配置 >	增加接入设备						⑦林助
接入用户管理		\sim	撞	182 C										
访查管理		~		ilitenno •	1812					计影响口	1813			
经济管理		~		组网方式	不启用	混合组网		+		业务类型	LAN權入业务	*		
用户接入日志		~		接入设备类型	H3C(0	eneral)		-		接入设备分组	无	•		
28 X 9482 1718				共享密钥 '						确认共享密钥"			1	
「望 快速入门 「ジ 接入服务管理 「ジ 接入服务管理		, =		业务分组	该值必 未分组	亦痛驾。		×			波圖必须編写。			
▶ 搜入条件管理			iQ1	劉康										
▼ 接入设备管理	_			选择 手	工増加	全部清除	请单击下方	的~确定>按钮劳	家業置。					
124 接入设备管 124 接入设备类	28 2962		ii ii	设备名称		设备	P地址		设备型号		备注	888		
12:私有属性下	发策略配置		1	0.153.43.141		10.15	i3.43.141		H3C WX3010	E-WCM		Û		
 LDAP业务管理 Portal服务管理 		U	+	H有1条记录。										
> 业务参数配置 Ⅰ 导出任务管理									前定	电消				
To 🐔 🔺		18	<u>+</u> 6	1 39	1.16				版社	2所有 @ 2007-2013 杭州	华三道信技术有限公司,保留	2—切权利。		e K

2.创建dot1x策略

#选择"用户"->"接入策略管理"->"接入策略管理",选择"增加"。

НЗС	Intelligent M	Management Cent	er			👤 admin	②帮助 i 关于 山注销
*	首页	资源 用户	业务 告署	医 报表	系统管理	📲 🗸 查询设备	i Q ×
用户管理	~	102 用户≻接入策略管	理≻接入策略管理				★加入收藏 ⑦帮助
 総 増加用户 協 所有用户 田 用户附加信息 第 用户批量操作 等入用户 	>	握入策略查询 接入策略名 增加			业务分组	•	查询 重置
👪 帐号群组管理		接入策略名 ♀		描述 ≎		业务分组 ♀ 修改	火 删除
接入用户管理	~	未找到符合条件的认	记录。				
访客管理	~	共有0条记录,当前	第0-0,第1/1页。			14 4	08 BO BI 50 💌
终端管理	~						
用户接入日志	~						
接入策略管理	~						
来宾接入管理	~						
🖻 🐔 🔺	3 🔥 46	<u>▲</u> 6 <u>▲</u> 138	1 16		版权所有 © 2007-	2013 杭州华三通信技术有限公司,保留一切权利	t) • 🛛 🕹

#输入策略名h3c-dot1x,选择"EAP证书认证",证书类型"EAP-PEAP",子类型"MS-CHAPV2",点击"确定"。

×	首页	资源	用户	业务	告審	报表	系统管理		■ 查询设备	୍
用户管理		× 92 A	月户 > 接入策略	管理 > 接入策略	管理 > 増加接)	「策略				②帮助
。增加用户 ■新育用户 ■用户附加信息 ■用户批量操作 ■导入用户 ■特許組管理		→ 接 上 道本 単 道本 単 二 二 二 二 二 二 二 二 二 二 二 二 二	信息 入策略名。 5分组。 老	dot1x 未分组	•					-
- 後入用户管理		、 摂切	信息							-
防容管理		~ 接	入时段	无		• ?		分配P地址*	否 *	
《端管理		~ ^{Tri}	亍速军	L		Kbps		上行速率	Kbps	
1.户接入日志		~ (优)	无级					自用RSA认证		
後入策略管理		√ ùE	书认证		不启用 ● 目	APietti (ie	WAP航田书认证	E		
未宾接入管理		✓ 认i 下2	E证书类型 BVLAN	E	VP-PEAP认证			认证证书子类型	MS-CHAPV21/UE +	
]下发User Profi]下发ACL	le				下发用户组	0	
		idit	湖定信息							-

#选择"用户"-> "接入策略管理" -> "接入服务管理",选择"增加"。填写服务名dot1x,接入策略选择"dot1x",点击"确定"。

НЗС	Intelligent M	anagement Center				٩	admin 🕐 👯 😫	i 关于 山注語
*	首页	党派 用户	业务 告讐 报表	系统管理				Q, ×
用户管理	~	② 用户 > 接入策略管的	▶ 接入服务管理 > 增加接入服务					⑦那助
都加用户 部所有用户 目用户附加值用 等用户批量操作 局等入用户 条 等入用户 条 等者報始管理 接入用户管理	>	 基本信息 服务名。 业务分组。 染音私有属性下发策略 染音和有属性下发策略 染音PYOD页面。 	dottx 未分組 v 不使用 v ⑦ PC-缺省页画 v		服劳 后胡 缺省接入碗箱 *	dottx v 🖓		-
访客管理 终间管理	×	■7 単位 「一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一			□Portal无感知认证 ⑦			
用户接入日志 接入策點管理	v	接入场景列表 增加						-
未直接入管理	~	名称	接入策略	私有属性下发策略	BYOD页面	优先级	修改	1088
		未找到符合条件的记录	¢	藏定	取消			
🔯 🐔 🔺	8 🔥 🚹	<u>▲</u> 7 <u>▲</u> 140 <u>▲</u> 1	8	版权)	所有 @ 2007-2013 杭州华三道(由技术有限公司,保留一切权利。		e K

#选择"用户"-> "用户管理" -> "增加用户"。用户姓名dot1x,证件号码01010101,点击"确定"。

*	首页					
		炭源 用户 业务	告聯 报表 系统管理		1 100 - 五田没有	Q, ×
用户管理	~	🐍 用户 > 增加用户				⑦帮助
約一型加用户 「「新有用户 」目 用户附加信息 基、用户附置操作 基、导入用户 動 帐号群细管理	>	增加用户 基本信息 用户姓名" 通讯地址 电子邮件	dottx	证件号码 * 电话 ⑦ 用户分组 *	0101010101 来分组	C
接入用户管理	~					
访客管理	~	□ 开通自助帐户				
终端管理	~					
用户接入日志	~			确定 取消		
接入策略管理	~					
未直接入管理	~					

#选择"增加接入用户",账户名dot1x,密码,勾选"dot1x"服务,点击"确定"。

НЗС	Intelligent M	anagement Center					오 admin ⑦ 제외	i 关于 仏注詞
*	首页	奥源 用户	业务 告讐	报表 系统管理			· 宜田设备	Q ×
用户管理	~	🖳 用户 > 擁入用户 >	增加接入用户					②帮助
🗞 増加用户		接入用户						
葡 新有用户	>	接入信息						
王 用户附加信息 基 用户批型操作 表 号 2 田 白		用户姓名。	dot1x	选择	增加用户			
AL 称号群组管理		帐号名 *	dottx					
接入用户管理	~	□预开户用户	□ 読術Bh	YOD用户	主机名用户	一快速认证用户		
1520019		22時 *	•••		密码确认*	•••		
AT MARKED		✓允许用户给改密码		。启用用户密释	控制策略	下次豐景須總改密码		
SCONING OF	v	生效时间		00	失效时间		00	
用戶機人自志	×	商士运费 924		(2.94	なは砂糖原料			
接入策略管理	~	Design of the second se	7+418+		La constante e a			
未再接入管理	~	Ponal-LiebenAulantet	PERIO	•				
		医水蛭不信息						
		総入協会	_					
		服务名			务后继	状态	分配中地址	
		✓ dot1x				可申请		
Ta 🐔 🔺	8 🔥 51	140 11	8		版权所有 @ 2007-2013	杭州华三道信技术有限公司,保留一切权利	j.	E 5

3. 证书导入配置:

#选择"用户"->"接入策略管理" -> "业务参数配置"->"证书配置",选择"EAP证书配置"。

НЗС	Intelligent M	anagement Cent	er	1	Ladmin ③棘瞰 i 关于 山注阔
*	首页 注	党源 用户	业务 告幣 报表 系统管理		• 亚洲设备 Q ×
用户管理	~	😫 用户 > 接入網驗管	理 > 业务参救政置 > 证书取置		★加入收藏 ⑦耳助
接入用户管理	Ý	证书校验			
访宾管理	~	模板名称	擬述	动作	
终端管理	Ý	EAP证书翻遗	基于EAP接入方式的证书配置	0 ₀	
用户撤入日志	×	WAPI证书配置	基于WAP增入方式的证书概题	0,	
 伝統(1) の) 振入服券管理 ジー振入服券管理 ・ 振入条件管理 ・ 振入条件管理 ・ 進入公園管理 ・ 止入や止券管理 ・ 止入や止券管理 ・ 止入参数局置 、 呉二任务管理 ・ 公核页面定制 	>				
未宾接入管理	~				
🗟 🐔 🔺	46	<u>∎</u> 6 <u>∎</u> 138	1. 16	版权所有 @ 2007-2013 杭州华三道信技术有限公司,保留一切权利。	E K

#选择对应的根证书和服务器证书,选择"下一步",最后点击"确定"。注:根证书和服务器证书选择AC接入设备当前版本匹配的根证书和服务器证书。

НЗС	Intelligent M	lanagement Center	👤 admin	@ #89	i关于 齿注调
*	首页	淡源 用户 业务 告祷 报表 系统管理	📲 🗸 查询设备		Q ¥
用户管理	~	20 证书就图 1. 根证书就图 >>> 2. CRL就图 >>> 3. 服务器证书载置 >>> 4. 服务器证书私胡密码 >>> 5. 证书载图信息接近			() #89
搬入用户管理	~	根正书稿遗			
访查管理	~	根证书文件			
终端管理	~				
用户搬入日志	~	г т			
		IMC支持的报证书文件格式为: perm(base64位编码,文件应照为perm级.cer), der(ded编码,文件应服为.der级.cer), pixcs12(pixcs12编码,文件应	前现为 p0.或 p12)。注意	: 如果证书	格式是ptx
 「望 快速入门 (2) 接入服务管理 (3) 接入限新管理) 推入设备管理) 推入设备管理) 止乃4戶出务管理) 止分析数据置 (2) 导出任务管理 >) 法领域页面控制 未容推入管理 	>	低水。647.58月9446329346822月+			
🗓 🐔 🔺	<u>▲</u> 46	▲ 6 ▲ 138 1 16 版权所有 © 2007-2013 杭州华三道信技术有限公司,保留·	一切权利。		t K

点击"浏览",在PC上找到和AC版本对应的根证书,选择"打开",如我的AC版本号为WX3000-CMW520-R3507P14,内部版本号为V300R005B09D020。

096	ement Gen	GL	🏉 选择要加载的文件						×
原	用户	业务	🔾 🖓 - 📕 « W	(3000-C	• WX3000-CMW520-R3507P14	▼ ⁴ 7	提索 WX3000	0-CMW520-R3	
en :	证书配置 1. 根 词	E书配置 >> 2.0	组织 ▼ 新建文(牛 夾			B		0
根词	正书配置		2 文档	^ <u> </u>	称	修改	日期	类型	
	根证书文件				waz100_upuate.pin	2010	1/2/24 13:20	Ultracult DO	cur
	HOLE DOCT		- = e	ľ	wa2100n_fit.bin	2013	/12/13 11:00	UltraEdit Do	cur
					wa2200_fit.bin	2013	/11/27 12:06	UltraEdit Do	cur
r.	- 🤉		190,290		wa2200_update.bin	2010	/5/24 19:41	UltraEdit Do	cui
	iMC古地的相同	元本文件格式力・	■ 闔片	= [wa2600_fit.bin	2013	/12/13 10:57	UltraEdit Do	cui
	格式,则不支	持pvk格式的私钥	📄 文档	E	wa2600a_fit.bin	2013	/12/13 10:57	UltraEdit Do	cu
			合 音乐	E E	wa3600_fit.bin	2013	/12/13 10:58	UltraEdit Do	cui
-		_			wlan_ca_certificate.cer	2010)/8/11 11:19	安全证书	
			🌉 计算机		🛿 wlan_local_certificate.pfx	2010)/8/11 11:33	Personal Infe	orr
			🌉 本地磁盘 (C:)		WX3000-CMW520-R3507P14.bin	2013	/12/15 10:00	UltraEdit Do	cu
			- 本地磁盘 (D:)						•
							and the second second		-
				又作者(N):	wlan_ca_certificate.cer	•	所有文件(*.*)		
							打开(O)	取消	
			<u> </u>	_		_			

#选择"下一步"。

😫 证书配置 1. 根证书配置 >> 2. C	RL配置 >> 3. 服务器证书配置 >>	4. 服务器证书私钥密码 >>	5. 证书配置信息预览
CRL配置			
启用CRL定时更新			
更新日期(1-30天)			
更新时间(0-23时)			
链接			?
	上一步	测试链接	一步 取消

#点击"浏览",选择服务器证书。

🕄 证书配置 1. 根证书配置 >> 2. CRL配置 >> 3. 服务器证书配置	>> 4.服务器i	正书私钥密码 >>	5. 证书配置(言息预览	
配置服务器证书					
▶ 服务器证书和私钥在同一文件 服务器证书文件				浏览	
MC支持的服务器证书文件格式为:perr(base64位编码,文件后 果证书格式是plot格式,则不支持plot格式的私钢文件:着服务器证	醫为.pem或.cer) E书和私钥在同一	,der(der编码,文 ·个文件, 则不能·	(件后缀为.der 使用der文件。	或.cer),pkcs12	2(pkcs12s
	上一步	下一步	取消		

anagement Center	🍘 选择要加载的文件	
【源 用户 业务 告警 报表	🔾 🖓 « WX3000-C 🕨 WX3000-CMW520-R3507P14	▼ 4 / 提索 WX3000-CMW520-R3 ♀
□〕 证书配置 1. 根证书配置 >> 2. CRL配置 >> 3. 服务器证书配	组织 ▼ 新建文件夹	III • 🔟 🔞
 ■ 股支援委員選任书 ● 服务器证书和私销在同一文件 服务器证书文件 	文価 名称 ※ 席 wal208h20 ft.bin ※ 席 wal200.bin ※ 認知 wal200.pt.bin 》 圖 知道 wal200.pt.bin 》 圖 武術 wal200.pt.bin 》 圖 文術 wal200.pt.bin 》 圖 文術 wal200.pt.bin	参次日期 少田 2013/11/27 12:05 UltraEdit Docum 2013/11/27 12:05 UltraEdit Docum 2010/5/24 19:36 UltraEdit Docum 2013/11/27 12:06 UltraEdit Docum 2013/11/27 12:06 UltraEdit Docum
MC支持的服务器证书文件指式为:pem(base64位编码,文作 po相式,则不支持px相式的纵语文件:希腊务器证书和纠错		2010/5/24 1941 Ultracidt Docum 2013/12/13 10:57 Ultracidt Docum 2013/12/13 10:57 Ultracidt Docum 2013/12/13 10:58 Ultracidt Docum 2010/8/11 11:19 安全语 2010/8/11 11:33 Bresonal Inform 2013/12/15 10:00 Ultracidt Docum -
	文件名(N): wlan_local_certificate.pfx	, 所有文件(*.*) • 打开(0) 取消

#输入服务器私钥密码: h3c, 选择"下一步"。

Ī	🔧 证‡	·配置	1. 根证书配置 >>	2. CRL配置 >>	3. 服务器证书配置 >>	4. 服务器证	[书私钥密码 >>	5. 证书配置	信息预览
	服务器	私钥密码	円						
	服务	器私钥器	密码	•••					
						上一步	下一步	取消	

#选择"确认"。

НЗС	Intelligent Ma	anagement Center		👤 admin 🗇 👯 🚯	i关于 也注调
*	首页 詳	医藻 用户 业务	告祷 报表 系统管理	📲 - 室道设备	Q, ×
用户管理	~	😫 证书配置 1. 根证书配置 >> 2. CRL	截置>> 3.服务器证书截置>> 4.服务器证书私钥密码>> 5.证书配置信息预览		() #89
接入用户管理	~	CDI BUB			
访查管理	~	CHURCH CHURCH			
终端管理	~	板址台版改有 和永慧江北 十 略	CN=H3C,0=H3C,ST=Some-State,C=CN		
用户搬入日志	~	開からない工作	2010-02-11		
		服务器证书有效经计时间	2030-08-06		
12 快速入门 ② 振入服务管理 ③ 振入服务管理 > 推入误称管理理 > 推入设备管理 > LDAP业务管理 > DAP业务管理 > 当务参数能置 码 导流成页面控制 + 本市协会理理	>	为了在中国的内部地址为了式 2017年1月20日	inpol		
	45	▲ 6 ▲ 138 ▲ 16	新約15年点2007-2013 並供化工業後述考慮部分表。 保認	_1107-01.	

三、客户端配置

1.STA配置:

#进入网络和共享中心,选择"管理无线网络"。



#选择"添加",#选择"手动创建网络配置文件"。

③ 业 手动	主接到无线网络
您想如	何添加网络?
2	手动创建网络配置文件(M) 这个选项创建一个新网络配置文件或查找现有网络并在计算机上保存网络的配置文件。您需要知道网络名称(SSID)和安全密钥(如果适用)。
4	创建临时网络(C) 这个选项创建一个暂时的网络,用于共享文件或 Internet 连接

#输入SSID:h3c-1x,安全类型WPA,加密类型TKIP,选择"下一步"。

\bigcirc	手动连接到无线网络	To and the second second
	输入您要添加的无线网	网络的信息
	网络名(E):	h3c-1x
	安全 <u>类型</u> (S):	WPA - 企业
	加密类型(R):	TKIP
	安全密钥(C):	隐藏字符(H)
	自动启动此连接(T)	
	🔽 即使网络未进行广播也	9连接(O)
	警告: 如果选择此选项	,则计算机的隐私信息可能存在风险。
		下一步(N) 取消

#选择"更改连接设置"。

🕞 📶 手动连接到无线网络	_
成功地添加了 h3c-1x	
◆ 更改连接设置(H) 打开连接属性以便更改设置。	
	关闭
#点击"安全"。	
h3c-dot1x 无线网络属性	
连接 安全	
名称: h3c=dot1x	
SSLU: N3c-0011X 网络类型: 访问点 网络可用性: 所有用户	
■ 当此网络在范围内时自动连接(M)	
□ 连接到更适合的网络 (如果可用) (P) □ 即使网络未广播其名称也连接 (SSID) (D)	
h3c-dot1x 无线网络属性	
<u>连接</u> 安全	
安全类型(E): WPA - <u>企业</u> ▼	
加密类型 (X): TKIP	
法择网络身份验证方法 (0):	
Microsoft: 受保护的 EAP (PEAP) ▼ 设置(S) ▼ 每次登录时记住此连接的凭据(R)	
高级设置 (0)	
□	

#选择"设置",进入"配置",去掉所有勾选,并点击"确定"。



#找到ssid=h3c-1x,点击连接即可。

四、实验结果验证

1、认证成功后, AC侧显示客户端信息



<wx3010e>dis wlan client verbose</wx3010e>	
Total Number of Clients	1
Client	Information
MAC Addrocs	6c88 1450 808c
MAC Address	dot1x
TD Addross	
ATD	1
AD Namo	an1
Padio Id	
Antenna Td	0
Service Template Number	1
SSTD	h3c-1x
BSSTD	5866-ba5e-c6f0
Port	WLAN-DB551:2
VLAN	10
State	Running
Power Save Mode	Active
Wireless Mode	11g
QoS Mode	WMM
Listen Interval (Beacon Interval) :	100
RSSI	67
Rx/Tx Rate :	48/54
Client Type :	WPA
Authentication Method :	Open System
Authentication Mode :	Central
AKM Method :	Dot1X
4-Way Handshake State :	PTKINITDONE
Group Key State	REKEYESTABLISHED
Encryption Cipher :	TKIP
Roam Status	Normal
Roam Count	0
Up Time (hh:mm:ss)	00:09:31

2、客户端信息

网络连接详细信息		x
网络连接详细信息(D):		
属性	值	
注接特定的 DNS 后缀 描述 物理地址 已启用 DHCP IFv4 地址 IFv4 子网摘码 获得租约的时间 租约过期的时间 相约过期的时间 IFv4 默认网关 IFv4 DMCP 服务器 IFv4 WINS 服务器 IFv4 WINS 服务器 已启用 NetBIOS ove 注接 本地 IFv6 地路 IFv6 DNS 服务器 <	Intel (R) Centrino (R) Advanced 6C-68-14-59-89-8C 是 192 168 10.3 255.255.255.0 2014年3月13日 14:35:48 2014年3月14日 14:35:48 192.168 10.1 192.168 10.1 9.9.9.9 是 fe80::18a8:c627:b8a0:e592%18	4
	关闭 (0)	

3、认证成功之后,客户端能ping 通网关

