802.1X AAA **李洋洋** 2012-05-30 发表



server-type extended

primary authentication 172.16.100.122

primary accounting 172.16.100.122

key authentication h3c

key accounting h3c

user-name-format without-domain

nas-ip 192.168.1.254

#

domain system

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

#

dhcp server ip-pool ap_add network 192.168.1.0 mask 255.255.255.0 gateway-list 192.168.1.254

#

dhcp server ip-pool sta_add network 192.168.2.0 mask 255.255.255.0 gateway-list 192.168.2.254

#

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 crypto ssid test-802.1x bind WLAN-ESS 1 cipher-suite tkip security-ie wpa service-template enable

interface NULL0 # interface Vlan-interface1 ip address 192.168.1.254 255.255.255.0 # interface Vlan-interface2 ip address 192.168.2.254 255.255.255.0 # interface Vlan-interface100 ip address 172.16.100.202 255.255.255.0 # interface GigabitEthernet1/0/1 port link-type trunk port trunk permit vlan all # interface WLAN-ESS1 port access vlan 2 port-security port-mode userlogin-secure-ext port-security tx-key-type 11key undo dot1x handshake dot1x mandatory-domain system # wlan ap ap1 model WA2620E-AGN id 1 serial-id 000F-E233-5500 radio 1 type dot11a radio 2 service-template 1 radio enable # ip route-static 172.16.100.0 255.255.255.0 192.168.1.253 ip route-static 172.16.100.0 255.255.255.0 192.168.2.253 # dhcp enable # load xml-configuration # user-interface aux 0 user-interface vty 0 4 authentication-mode scheme user privilege level 3 # return [WX3010-AC] ocs0 Press CTRL+K to quit. Connected to OAP!

%Sep 18 16:46:11:607 2011 WX3010-SW SHELL/5/LOGIN:- 1 - Console(aux0) in unit1

```
login
dis cu
#
sysname WX3010-SW
#
oap management-ip 192.168.0.100 slot 0
#
radius scheme system
#
domain system
#
local-user admin
password simple admin
service-type telnet
level 3
#
vlan 1 to 2
#
vlan 100
#
interface Vlan-interface1
ip address 192.168.1.253 255.255.255.0
#
interface Vlan-interface2
ip address 192.168.2.253 255.255.255.0
#
interface Vlan-interface100
ip address 172.16.100.201 255.255.255.0
#
interface Aux1/0/0
#
interface GigabitEthernet1/0/1
poe enable
#
interface GigabitEthernet1/0/2
port link-type trunk
port trunk permit vlan all
#
interface GigabitEthernet1/0/3
#
interface GigabitEthernet1/0/4
#
interface GigabitEthernet1/0/5
#
interface GigabitEthernet1/0/6
#
interface GigabitEthernet1/0/7
```

interface GigabitEthernet1/0/8

#

#

interface GigabitEthernet1/0/9

#

interface GigabitEthernet1/0/10

#

interface GigabitEthernet1/0/11

stp disable

port link-type trunk

port trunk permit vlan all

#

interface NULL0

#

user-interface aux 0

user-interface vty 0 4

authentication-mode scheme

user privilege level 3

#

Return

2) 主要配置步骤

(1) 创建RADIUS方案。

创建RADIUS方案imc并进入其视图。

[WX3010-AC] radius scheme imc

设置主认证RADIUS服务器的IP地址172.16.100.122。

[WX3010-AC-radius-h3c] primary authentication 172.16.100.122

设置主计费RADIUS服务器的IP地址172.16.100.122。

[WX3010-WX3010-AC-radius-h3c] primary accounting 172.16.100.122

设置系统与认证RADIUS服务器交互报文时的共享密钥为h3c。

[WX3010-AC-radius-h3c] 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。

[WX3010-AC-radius-h3c] key accounting h3c

#将RADIUS方案h3c的RADIUS服务器类型设置为extended。

[WX3010-AC-radius-h3c] server-type extended

(2) 创建domain域。

创建cams域并进入其视图。

[WX3010-AC] domain system

#为lan-access用户配置认证方案为RADIUS方案,方案名为imc。

[WX3010-AC-isp-system] 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。

[WX3010-AC-isp-system] 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。

[WX3010-AC-isp-system]accounting lan-access radius-scheme imc

(3) 全局使能802.1x。

[WX3010-AC] port-security enable

(4) 设置802.1x用户的认证方式为EAP。

[WX3010-AC] dot1x authentication-method eap

(5) 配置接口WLAN-ESS 1。

#创建接口WLAN-ESS1并进入其视图。

[WX3010-AC] interface WLAN-ESS 1

WLAN-ESS 1 上使能802.1x端口安全模式。

[WX3010-AC-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。

[WX3010-AC-WLAN-ESS1] port-security tx-key-type 11key

(6) 无线服务集设置。

#创建crypto类型的服务模板1并进入其视图。

[WX3010-AC] wlan service-template 1 crypto

设置当前服务模板的SSID (服务模板的标识)为test-802.1x。

[WX3010-AC-wlan-st-1] ssid test-802.1x

#将WLAN-ESS1接口绑定到服务模板1。

[WX3010-AC-wlan-st-1] bind WLAN-ESS 1

设置无线客户端接入该无线服务(SSID)的认证方式为开放式系统认证。

[WX3010-AC-wlan-st-1] authentication-method open-system

#使能TKIP加密套件。

[WX3010-AC-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。

[WX3010-AC-wlan-st-1] security-ie wpa

使能服务模板。

[WX3010-AC-wlan-st-1] service-template enable

2、配置iMC

1) 接入设备配置

在iMC控制界面,点击菜单栏中[业务]->[接入业务] ->[接入设备管理] ->[接入设备配置]的"增加接入设备"。

进入接入设备配置,选择"手工增加"->"手工增加接入设备"后,进入接入设备配置页面。根据设备 上的RADIUS属性配置,对参数进行设置,然后点击"确定"。

Consiger the speed Letter					Siadron D	RB 0 AT 0 88
GRANKE SH	18 RP 25				48-	Ge BITR
* ****	TH OR HEADE H		ARY NO.			047
NITE V	-					
K18# V	RAACE		10050610			
RERMINO V	- H\$EM	AGE	+ 6120MC	1812		
305R# ¥	+ 1159360	1913	业务内裁	しや肥入会務		
NATT V	展入校会内型	H3CrGenetat)	编列开式	78822000		
(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	推入区域	*	air.			
1. 新乐和演学理 1. 株入场後管理	2696	And D				
管算人区地管理			a haspere to	1934) Iosano (Fille)	all A R 🖗 - mirrown 🔍 = 🐹	
GRAPHERT		FIMM		-		
「日本日本日本日日日	-	and the second s	- 305km183	1 182.168.1.254		
······································	1919		ITAL MERICAN	1 102 100 1 254		
 (1) (1) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2				BC .	**	

2) 服务配置

在iMC控制界面,首先进入"业务"、"接入业务"、"业务参数配置"、"证书配置"安装证书。然后进入" 服务配置管理"、"增加服务配置",在服务配置列表中,选择"增加",添加服务名,在计费策略中选 中配置好的计费策略(计费策略配置方法,此处略),这里选择不计费。无线EAP认证方式,iMC 中支持两种: peap、tls。此处选择peap,之后确定即可。



18 RP 25 11 M	A 35TR	Celoral C	
		N9.51	Ge PLT R
THE REAL PROPERTY AND COMPANY			0.45
The second of the second			
M TACKGROWN			
421828	CHHOC 0HOC ST-Some-State C+CH		
医外腺炎 化丁酸	CN+HOC-WLANLO+HOC.ST+Dome-State.C+CN		
BABE SAMAAMM	2010-00-11		
服务课证书在地球止时间	2038-08-08		
证书希望尚者更新方式	impot		
		22 ************************************	W MERICE - NO. CONSCI - N. SALE STOCK PARAMETER - S. W MERICE BASK W MERICE BASK W MERICE BASK BASK NS.FR. CH-MCC CALLST-Stock - Market - CON CH-MCC CALLST-Stock - Market - CON CH-MCC CALLST-STOCK - Market - CON CH-MCC CALLST-STOCK - Market - Market - CON CH-MCC CALLST-STOCK - Market - Market - CON CH-MCC CALLST-STOCK - Market

LIC Internet Measurer's Carlos					Sil admin [] Ro	0 XT 🥥 IIM
		0 K# 5500			(4) *	Go Ride I
****	A	TTT				042
WANER *	The second se					
4CIMM +	WARSACT.					
*	# SILB					
* 201	· ##48	w////ess	84 G G			
ATT V	* 业务分组	#.14tf				
1入安告 A	* 肋道安主策略	干扰用完全制度 💌	- 新省东菜屬拉丁式菜屬	关闭用		
1. 新茶和清常常	计算用电	干计费				
展入场景堂督	RABE					
古田人に相当せ	LOWERS		P 2040			
A WARRANG M	and the second se					
₹ 最人MAC地址管理	NAULE.	101			1.1.1	
● 建盘库剂号管理	* 個人时間	R	HEPHELE	a	100	
Piersene .	TOWN	kay	H F031		Hops	
·····································	优化成		D 8883402			
· LEBYTEMEST	12/44/12	O TER O EXPERING	O www.getuar			
観人会長知り住在	NEWHOLD	ENP PENPUTE N	以证证书子内裁	M5-OH/PV28A	2 =	
Portal#6世世	E TRIAN		TRUber Fridie			
LDW企具管理	D Telling					
全省世界配置	CJ TANF	1				
ES XAME	LJ TRACL					
CONTRACTOR OF	LA MORTAN B					

3) 用户配置

在iMC控制界面,进入"用户",选择"增加用户"输入用户名和密码。此处需要注意将刚才配置的服务选上。

推产管理		B. BP >> MINEP						01	
1000P		While .							
用户附加准备									
展戸設業費店		· #P#5	Substances.		- (7/m-848	121404			
- 4+UTT		18-214-19							
1.00000000		#740			· ROUM				
***	۲.	WHERE .			100 110				
CRPRN		- 51			64				
*实装入管理		1.94	12345		· #B	0			
			1		1 845	1	(m)		
		THE OBSIDE							
		□ N# DB•S.P							
		- MARRAY		i.	NE BR				
		Tranks,		Ē	ME En				
				C	RI En				
		OKADB67		0	#12 E3				
		Offanter,		0	RC En				
		C FROMA		E	NC En				

ISC manager the	persent Centrel		1 admin 13 위한 0 유학 3 경제
C RINKER		教授 現戶 金香 首都 縣東 基集智慧	de land
1.2首席		B.R. MARKER	
ANDER ANDER ANDER ANDER		2 W108/* "www.s." \$25.	
用户指量操作 导入用户		*******	
1 DARK		增加资产标号 增加提入规户电号。	
最大用户推制		WINCRP WINCRP	
0.822	۷.	EXEMAN EXEMAN.	
Incall Page 1		# 64// mills # 60/P#tot/EP2/Wells.	
*完装入管理		edende edensede.	

No. 10. 20 1	* 58 5500	8				(dia *)	Go Auto
	MRARP.						041
WARP							
新 入自由							
 用户推名 	familia .	155 1938/	1				
- 895	ACCOUNTS	Internet and Internet	DEESSE				
- 255			* #55860				
C and the second		The second second	1.12.01.2777		No. B. R. Rokeling		
ANCH ANCH		CTO CHORNE			10.4400000		
A-100							
R.C. Marrie	10000	21.00	(Local Break)				
**/10	Bit #	1	* 時代金額		0		
00.94	10/T	1					
2912742							
NAKS.						_	in provincianty
11/ 15.5	1111	-	NEXT 20	UA.	10.014		SACOUR
0004	408		1803286	29.8	100		
0 11			TRREEME	2,413	70.0		
E 10			子使用完全领域	104.8	不计算		
123123			干扰用空止发展	1043	不计算		
123486			THEREMS	tes	不计量		
			MINING A TANK OF A	Line Transformer		artist Br.	
	Gp 000 000 000 RARD ARRES ARRES 000 RARD - 80% 000 000 SARRAWERS - 80% 000 000 RARD - 80% 000 000 11 11 11 11 11 11 11 11 11 11 11 111 11 11 11	BARD BARD BARD BARD BARD BARD	00 00<	Bit Production of All All All All All All All All All Al	Bit All Control of Statuture State State State State State State State State State State State State State		Bit All

4、验证结果

I在未通过802.1x认证的情况下使用PC1访问internet, PC不能访问Internet上的资源。

| 在PC1上使用802.1x客户端进行认证, PC1可以通过802.1x认证成功, 并且可以正常访问intern et上的资源。需根据不同设置认证方式的不同 (peap、tls) 对无线客户端进行相应的配置。 (1) 添加SSID。 (2)首先在无线网络属性中,添加SSID,并选择相应的加密方式、认证方式。 test-802.1x 居性 2 🔀 关联 验证 连接 网络名(SSID) 00: test-802.1s 即使此网络未广播,也进行连接(8) 无线网络密钥 此网络要求下列密钥: ~ ~ 确认网络密钥(0) 宏明索引 (高雄) (X) [1 💼 回自动力我提供此密钥00 □ 这是一个计算机到计算机的(临时)网络,未使用无线访 (同点 cc) 确定 取消

(3)在验证对话框中,选择EAP类型为PEAP,点击<属性>,去掉验证服务器证书选项(此处不验证服务器证书),点击<配置>,去掉自动使用Windows登陆名和密码选项,然后点击<确定>。

👃 无线网络连接 属性 🛛 🔍 🔍
常规 无线网络配置 高级
☑用 Windows 配置我的无线网络设置(W)
test-802.1x 属性 ? ×
关联 验证 连接
选择此选项以提供访问以太网所需的身份验证。
☑启用此网络的 IEEE 802.1x 验证(E)
EAP 类型(T): 受保护的 EAP (PEAP)
受保护的 EAP 属性 ?×
EAP MSCHAPv2 属性
当连接时: 自动使用 Windows 登录名和密码(以及域, 如果有的话)(A) 确定 取消 ACEDICOM Root A-CERT ADVANCED ACNLB
不提示用户授权新服务器或受信任的证书项发机构(?)。 选择身份验证方法(S): 安全密码(CAP-MSCHAP v2) ② 启用快速重新连接(C) □ 月用隔离检查(Q) □ 如果服务器设有显示加密绑定的TLV则断开连接(T) 确定 取消
□ 如果服务器没有显示加密绑定的 TLV 则断开连接 (T) 确定 取消