wlan接入 802.1X AAA 李晨光 2016-06-21 发表

本文档介绍802.1X远程认证典型配置举例。

本文档适用于使用Comware V7软件版本的无线控制器和接入点产品,不严格与具体硬件版本对 应,如果使用过程中与产品实际情况有差异,请参考相关产品手册,或以设备实际情况为准。 本文档中的配置均是在实验室环境下进行的配置和验证,配置前设备的所有参数均采用出厂时的 缺省配置。如果您已经对设备进行了配置,为了保证配置效果,请确认现有配置和以下举例中的 配置不冲突。

本文档假设您已了解WLAN接入、WLAN用户安全、WLAN用户接入认证和802.1X的相关特性。 如图1所示组网,Switch作为DHCP server为AP和Client分配IP地址,采用iMC作为RADIUS服务 器对用户进行认证、授权和计费,要求:

- 对无线用户进行远程802.1X认证。
- · 客户端链路层认证使用开放式系统认证。
- · 通过配置客户端和AP之间的数据报文采用802.1X身份认证与密钥管理来确保用户数据的传输安全。
- · 加密套件采用CCMP。



1.1 配置步骤

1.1.1 配置AC

(1) 配置AC的接口 #创建VLAN 100以及对应的VLAN接口,并为该接口配置IP地址。AP将获取该IP地址与AC建立 CAPWAP隧道。 system-view [AC] vlan 100 [AC-vlan100] quit [AC] interface vlan-interface 100 [AC-Vlan-interface100] ip address 10.1.1.46 24 [AC-Vlan-interface100] quit # 创建VLAN 200及其对应的VLAN接口,并为该接口配置IP地址。Client将使用该VLAN接入无线 网络。 [AC] vlan 200 [AC-vlan200] quit [AC] interface vlan-interface 200 [AC-Vlan-interface200] ip address 10.1.2.1 24 [AC-Vlan-interface200] quit (2) 配置RADIUS方案 #创建RADIUS方案radius1并进入其视图。 [AC] radius scheme radius1 # 配置主认证/计费RADIUS服务器的IP地址为10.1.1.3。 [AC-radius-radius1] primary authentication 10.1.1.3 [AC-radius-radius1] primary accounting 10.1.1.3 # 配置AC与认证/计费RADIUS服务器交互报文时的共享密钥为明文字符串12345。 [AC-radius-radius1] key authentication simple 12345 [AC-radius-radius1] key accounting simple 12345 # 配置设备发送RADIUS报文使用的源IP地址为10.1.2.1。 [AC-radius-radius1] nas-ip 10.1.2.1

[AC-radius-radius1] quit

#创建名为dom1的ISP域并进入其视图。

[AC] domain dom1

#配置802.1X用户使用RADIUS方案radius1进行认证、授权、计费。

[AC-isp-dom1] authentication lan-access radius-scheme radius1

[AC-isp-dom1] authorization lan-access radius-scheme radius1

[AC-isp-dom1] accounting lan-access radius-scheme radius1

[AC-isp-dom1] quit

使能RADUIS session control功能。

[AC] radius session-control enable

#开启RADIUS DAE服务,并进入RADIUS DAE服务器视图。

[AC] radius dynamic-author server

设置RADIUS DAE客户端的IP地址为10.1.1.3,与RADIUS DAE客户端交互DAE报文时使用的

共享密钥为明文12345。

[AC-radius-da-server] client ip 10.1.1.3 key simple 12345

[AC-radius-da-server] quit

(3) 配置802.1X认证

#配置802.1X系统的认证方法为EAP。

[AC] dot1x authentication-method eap

(4) 配置无线服务模板

创建无线服务模板service,并进入无线服务模板视图。

[AC] wlan service-template service

配置SSID为service。

[AC-wlan-st-service] ssid service

#配置无线服务模板VLAN为200。

[AC-wlan-st-service] vlan 200

#配置身份认证与密钥管理的模式为802.1X。

[AC-wlan-st-service] akm mode dot1x

#配置CCMP为加密套件,配RSN为安全信息元素。

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

[AC-wlan-st-service] security-ie rsn

#配置用户接入认证模式为802.1X。

[AC-wlan-st-service] client-security authentication-mode dot1x

配置802.1X用户使用认证域为dom1。 [AC-wlan-st-service] dot1x domain dom1

#使能无线服务模板。

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

[AC-wlan-st-service] quit

创建AP, 配置AP名称为office,型号名称选择WA4320i-ACN,并配置序列号210235A1GQC1 58004457。

[AC] wlan ap office model WA4320i-ACN

[AC-wlan-ap-office] serial-id 210235A1GQC158004457

#进入Radio 1视图。

[AC-wlan-ap-office] radio 1

#将无线服务模板service绑定到radio 1,并开启射频。

[AC-wlan-ap-office-radio-1] service-template service

[AC-wlan-ap-office-radio-1] radio enable

[AC-wlan-ap-office-radio-1] quit

[AC-wlan-ap-office] quit

1.1.2 配置Switch

创建VLAN 100,用于转发AC和AP间CAPWAP隧道内的流量。 system-view [Switch] vlan 100 [Switch-vlan100] quit # 创建VLAN 200,用于转发Client无线报文。 [Switch] vlan 200 [Switch-vlan200] quit # 配置Switch与AC相连的GigabitEthernet1/0/1接口的属性为Trunk,允许VLAN 100和VLAN 200 [Switch] interface gigabitethernet 1/0/1 [Switch-GigabitEthernet1/0/1] port link-type trunk [Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200 [Switch-GigabitEthernet1/0/1] quit # 配置Switch与AP相连的GigabitEthernet1/0/2接口属性为Access,并允许VLAN 100通过。 [Switch] interface gigabitethernet 1/0/2 [Switch-GigabitEthernet1/0/2] port link-type access [Switch-GigabitEthernet1/0/2] port access vlan 100 #使能PoE功能。 [Switch-GigabitEthernet1/0/2] poe enable [Switch-GigabitEthernet1/0/2] quit # 配置VLAN 100接口的IP地址。 [Switch] interface vlan-interface 100 [Switch-Vlan-interface100] ip address 10.1.1.47 24 [Switch-Vlan-interface100] quit # 配置VLAN 200接口的IP地址。 [Switch] interface vlan-interface 200 [Switch-Vlan-interface200] ip address 10.1.2.2 24 [Switch-Vlan-interface200] quit #配置DHCP地址池100,用于为AP分配IP地址。 [Switch] dhcp server ip-pool 100 [Switch-dhcp-pool-100] network 10.1.1.0 mask 255.255.255.0 [Switch-dhcp-pool-100] gateway-list 10.1.1.46 [Switch-dhcp-pool-100] quit #配置DHCP地址池200,用于为Client分配IP地址。 [Switch] dhcp server ip-pool 200 [Switch-dhcp-pool-200] network 10.1.2.0 mask 255.255.255.0 [Switch-dhcp-pool-200] gateway-list 10.1.2.1 [Switch-dhcp-pool-200] guit

1.1.3 配置RADIUS server

通过.

下面以IMC为例(使用IMC版本为: IMC PLAT 7.1(E0302)、IMC UAM 7.1(E0302)), 说明AAA 服务器的基本配置。

增加接入设备。

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/接入设备管理/接入设备配置]菜单项,进入接入配置管理页面。在该页面中点击<增加>按钮,进入增加接入设备页面

•

- · 设置认证、计费共享密钥为12345,其它保持缺省配置;
- 选择或手工增加接入设备,添加IP地址为10.1.2.1的接入设备。

图1 增加接入设备页面

₽2>	用户 > 接入策略管理 > 掛	度入设备管理 > 接入设备配置 > 増加接入	设备				
接	入配置						
	认证端口 *	1812		计费端口 *		1813	
	组网方式	不启用混合组网		业务类型		LAN接入业务	•
	接入设备类型	H3C(General)		业务分组		未分组	•
	共享密钥 *			确认共享密钥 *		•••••	
	接入设备分组	无					
设	备列表						
	选择 手工增加 5	增加IPv6设备 全部清除					
i	设备名称	设备IP地址	设备型号		备注		删除
		10.1.2.1					â
;	共有1条记录。						
			确定	取消			

选择"用户"页签,单击导航树中的J接入策略管理/接入策略管理J菜单项,进入接入策略管理页面,在该页面中单击<增加>按钮,进入增加接入策略页面。

- · 设置接入策略名输入dot1x;
- · 选择证书认证为EAP证书认证;
- · 选择认证证书类型为EAP-PEAP认证,认证证书子类型为MS-CHAPV2认证。认证证书子类型需要与 客户端的身份验证方法一致。

图2 增加服务策略页面

即用户 > 接入策略管理 > 接入策略管	理 > 増加接入策略		
基本信息			
接入策略名 *	dot1x		
业务分组 *	未分组 マ		
描述			
运机信白			
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 ○WAPI证书认证		
认证证书类型	EAP-PEAP认证 ▼	认证证书子类型	MS-CHAPV2认 ▼
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"页签,单击导航树[接入策略管理/接入服务管理]菜单项,进入接入服务管理页面,在 该页面中单击<增加>按钮,进入增加接入服务页面。

- · 设置服务名为dot1x;
- · 设置缺省接入策略为已经创建的dot1x策略。

图3 增加接入服务页面

本信息										
服务名 *		dot1x			服务后缀					
业务分组 *		未分组		-	缺省接入策略 *		dot1x			• ?
快省安全策略 *		不使用		•	缺省内网外连策略*		不使用			•
读省私有属性下发策略 *		不使用		• ?						
缺首单帐号最大绑定终端数 *		0			缺盲单帐号在线数量	限制 *	0			
服务描述										
✓ 可申请 ?					Portal无感知认识	E (?)				
入场暴列表										
101-0										
夕称	控λ ^{倍8}	8	安全策略		私有属性下发简略	内网外连常略		优先级	修改	
主我到符合条件的记录。	1367 (3464	н	жтяки		TATIBILE PASSAN	P3P3/1723806		PETCAX	13HA	
And Add and the act in the second										

增加接入用户。

选择"用户"页签,单击导航树中的|接入用户管理/接入用户]菜单项,进入接入用户页面,在该页面中单击<增加>按钮,进入增加接入用户页面。

- · 添加用户user;
- · 添加账号名为dot1x, 密码为dot1x123;
- · 选中之前配置的服务dot1x。

图4 增加接入用户页面

🖳 用户 > 接入用户 > 増加接入用户					0
接入用户					
接入信息					
用户姓名 *	user 选择	增加用户			
帐号名 *	dot1x				
预开户用户	缺省BYOD用户	MAC地址认证用户	主机名用户	1	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	イ	次登录须修改密码	
生效时间	0	失效时间			
最大闲置时长(分钟)		在线数量限:	制	1	
Portal无感知认证最大绑定数*	1				
dolx			不使用	可申请	
dot1x			不使用	可申请	
dotpap			不使用	可申请	

1.1.4 配置客户端

#配置无线网卡

- · 下面以Windows 7 Service Pack 1为例,说明无线网卡的配置。
- 在客户端上已经完成证书安装。

打开"开始"菜单,单击"控制面板",进入控制面板窗口。

图5 打开控制面板



#单击"查看网络状态和任务",进入到了"网络和共享中心"。

Statement of the state of the s	
 ・ 控制面板 ・ 	 ▼ 4y / 提案控制面板
调整计算机的设置	查看方式: 类别 ▼
 系统和安全 重量德的计算机状态 备份您的计算机 重找并解决问题 网络孔 Internet 重图网络状态和任务 远程露窗伯和某更或现 	 第二章 ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●
 硬件和声音 量能後報印印机 添加设备 電子 電子 取動程序 获得程序 	时钟、语言和区域 更改健量或其他输入法 轻松访问 使用 Windows 建议的设置 代化视频显示

单击"管理无线网络",进入管理无线网络窗口。

图6 查看网络状态和任务

1.				
]Internet) 管理无线网络	- ↓	搜索 管理无线网络	٩
管理使用(无线网络连接)的 Windows 将尝试按照下面所列的间	无线网络 哼连接这些网络。			
添加 适配器属性 配置文件类型	网络和共享中心			0
您可以查看、修改和重新排序的网络 (1)			-
dh1x	安全: WPA2 - 企业	类型: 任何受支持项	手动连接	
1 个对象				

#单击<添加>按钮,选择"手动创建网络配置文件(M)"。

图8手动添加无线网络

○ 业 手动连接到无线网络		
您想如何添加网络?		
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 件。您需要知道网络名称(SSID)和安全密钥(如果适用)。	置文	
创建临时网络(<u>C</u>) 这个选项创建一个暂时的网络,用于共享文件或 Internet 连接		

#添加无线网络信息。

- · 输入网络名(服务模板中的ssid):service;
- · 选择安全类型:WPA2-企业;
- · 加密类型: AES;
- · 其它保持缺省配置,然后单击"下一步"。

3	手动连接到无线网络	
	输入您要添加的无线	网络的信息
	网络名(E):	service
	安全类型(S):	WPA2 - 企业
	加密类型(<u>R</u>):	AES
	安全密钥(<u>C</u>):	□ 隐藏字符(出)
	☑ 自动启动此连接(工)	
	即使网络未进行广播 警告:如果选择此选择	也连接(Q) 顷,则计算机的隐私信息可能存在风险。
		下一步(N) 取消

图9 无线网络创建成功

④ ····· 手动连接到无线网络	
成功地添加了 service	
→ 更改连接设置(<u>H</u>) 打开连接属性以便更改设置。	
	关闭

网络创建成功后,选择"更改连接设置(H)",进入无线网络属性对话框。

图10 无线网络属性

s	ervice 无	线网络属	性			x
	连接	安全				
	名称: SSID: 网络类 网络可	2型: 1月性: 比网络在 後到更适	service service 访问点 所有用户 范围内时自动连接 合的网络如果可用	(M)) (F)(P)		
	144	£₩##不) 擂兵石称也庄按	(2210) (0)		
				确定	<u>ا</u>	消

- # 单击"安全"页签,在"选择网络身份验证方法"下拉框中选择"Microsoft:受保护的EAP (PEAP)"
- ,然后将"每次登录时记住此连接的凭据"前的复选框中的勾去掉。

图11 网络身份验证配置

service 无线网络属性	x
连接 安全	
安全类型(E): WPA2 - 企业 ▼	
加密类型 (I): AES ▼	
选择网络身份验证方法 (1)	
Microsoft: 受保护的 EAP (PEAP) ▼ 设置(S)	
□ 海次登录时记住此连接的凭据 ®)	
高级设置 (1)	
确定取消	

#单击<设置>按钮,进入"保护的EAP属性"对话框。

- · 去掉"验证服务器证书(V)"前复选框中的勾;
- · 去掉"启用快速重新连接"前复选框中的勾;
- · 单击"选择身份验证方法(S)"后面的<配置>按钮;
- · 在弹出的"EAP MSCHAPv2属性"对话框中,去掉复选框中的勾;
- · 然后单击<确定>按钮,返回"受保护的EAP属性"界面,再单击<确定>按钮。

图12 属性配置

務器证书 (V)
J根证书颁发机构 (R)
EAP MSCHAPv2 届性
当连接时: 自动使用 "indows 登录名和密码 (以及域, 如果有的话) (A)。 确定 取消
;证方法 (S):
(EAP-MSCHAP v2) ▼ 配置 (C)
室重新连接(ᡗ) 〒网络访问保护(Ω) 务器未提供加密绑定的 TLV 则断开连接(Ω) 只隐私(Ω)

#在无线网络属性对话框中,单击<高级设置>按钮,进入高级设置对话框。在802.1X设置页签

中, 勾选"指定身份验证模式", 然后, 在下拉框中选择"用户身份验证"。

图13 高级设置-802.1X设置

用户身份验证	▼ 保存	凭据(C)
□删除所有用户的凭据(0)		
□ 为此网络启用单一登录(S)		
◎ 用户登录前立即执行 (8) ● 用户登录后立即执行 (8)		
最大延迟(秒)(M):	10	W.
最大延迟(秒)(M): ⑦ 允许单一登录期间显示其他	 [对话框 (L)	W
最大延迟(秒)(M): ⑦ 允许单一登录期间显示其他 ② 该网络为计算机和用户身份 LAN(V)		■
最大延迟(砂)(M): ⑦ 允许单一登录期间显示其他 □ 该网络为计算机和用户身份 LAN(V)		的虚拟
最大延迟(砂)(附): ⑦ 允许单一登录期间显示其他 □ 该网络为计算机和用户身份 LAN(V)	10 対话框 (L) 验证使用单独的	的虚拟
最大延迟(砂) ⑾): ☑ 允许单一登录期间显示其他 □ 该网络为计算机和用户身份 LAN (V)	10 奴话框 (L) 验证使用单独的	的虚拟

单击"802.11设置"页签,去掉"启用成对主密钥(PMK)缓存"前的复选框中的勾,然后单击<确定 >按钮。

图14 无线网卡配置过程

802.1X 设置 802.11 设置		
快速漫游		
📄 启用成对主密钥 (PMK)缓存 (K)		
PMK 生存时间(分钟)(L);	720	A.
PMK 缓存中的项目数(N):	128	- A-
□ 此网络使用预身份验证 (P)		
最多尝试预身份验证次数(M):	3	A
□ 为此网络启用联邦信息处理标准 (FIP:	5)兼容(7)	
□ 为此网络启用联邦信息处理标准 (*IP: □ 为此网络启用联邦信息处理标准 (*IP: □ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○	(1) 茶茶 (1)	

1.2 验证配置

客户端通过802.1X认证成功关联AP,并且可以访问无线网络。 在AC上可以通过**display wlan client verbose**命令查看客户端上线情况。

[AC] display wlan client verbose

Total number of clients: 1

MAC address	: cc3a-61a8-fb8c
IPv4 address	: 10.1.2.3
IPv6 address	: N/A
Username	: user
AID	:1
AP ID	: 3
AP name	: office
Radio ID	:1
SSID	: service
BSSID	: 741f-4ad4-1fe0
VLAN ID	: 200
Sleep count	: 0
Wireless mode	:802.11ac
Channel bandwidth	: 80MHz
SM power save	: Disabled
Short GI for 20MHz	: Supported
Short GI for 40MHz	: Supported
Short GI for 80MHz	: Supported
Short GI for 160/80+80MH	z : Not supported
STBC RX capability	: Not supported
STBC TX capability	: Not supported
LDPC RX capability	: Not supported
SU beamformee capability	: Not supported
MU beamformee capability	: Not supported
Beamformee STS capabili	ty : N/A
Block Ack	: N/A
Supported VHT-MCS set	: NSS1 0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Supported HT MCS set	: 0, 1, 2, 3, 4, 5, 6, 7
Supported rates	: 6, 9, 12, 18, 24, 36, 48, 54 Mbps
QoS mode	: WMM

Listen interval	: 10			
RSSI	: 0			
Rx/Tx rate	: 0/0			
Authentication method	: Open system			
Security mode	: RSN			
AKM mode	: 802.1X			
Cipher suite	: CCMP			
User authentication mode	: 802.1X			
Authorization ACL ID	: N/A			
Authorization user profile	: N/A			
Roam status	: N/A			
Key derivation	: SHA1			
PMF status	: N/A			
Forwarding policy name	: N/A			
Online time	: 0days 0hours 0minutes 15seconds			
FT status	: Inactive			
#在AC上可以通过display dot1x connection命令查看dot1x用户上线情况。				

[AC] display dot1x connection

Total connections: 1

User MAC address : cc3a-61a8-fb8c AP name : office : 1 Radio ID SSID : service BSSID : 741f-4ad4-1fe0 Username : user Authentication domain : dom1 : 10.1.2.3 IPv4 address Authentication method : EAP Initial VLAN : 200 Authorization VLAN : 200 Authorization ACL number : N/A Authorization user profile : N/A Termination action : Default Session timeout period : 36000001 s : 2015/12/21 11:27:11 Online from Online duration :0h 1m 1s

1.3 配置文件

· AC: # dot1x authentication-method eap # vlan 100 # vlan 200 # wlan service-template service ssid service vlan 200 akm mode dot1x cipher-suite ccmp security-ie rsn client-security authentication-mode dot1x dot1x domain dom1

```
service-template enable
#
interface Vlan-interface100
ip address 10.1.1.46 255.255.255.0
#
interface Vlan-interface200
ip address 10.1.2.1 255.255.255.0
#
radius scheme radius1
primary authentication 10.1.1.3
primary accounting 10.1.1.3
key authentication cipher $c$3$Bb61SHV2ZsVYPJU2+RFB/8ntk0uCQkmxdA==
key accounting cipher $c$3$w03NfxnBmfDuedv9/xo7ESnoxKjowmmX9A==
nas-ip 10.1.2.1
#
radius dynamic-author server
client ip 10.1.1.3 key cipher $c$3$AkTEB7OgMYnCqsfDeplhoAgXUek/rVrLZw==
#
domain dom1
authentication lan-access radius-scheme radius1
authorization lan-access radius-scheme radius1
accounting lan-access radius-scheme radius1
#
wlan ap office model WA4320i-ACN
serial-id 210235A1GQC158004457
radio 1
 radio enable
  service-template service
#
          Switch:
    .
#
vlan 100
#
vlan 200
#
dhcp server ip-pool 100
network 10.1.1.0 mask 255.255.255.0
gateway-list 10.1.1.46
#
dhcp server ip-pool 200
network 10.1.2.0 mask 255.255.255.0
gateway-list 10.1.2.1
#
interface Vlan-interface100
ip address 10.1.1.47 255.255.255.0
#
interface Vlan-interface200
ip address 10.1.2.2 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 1 100 200
#
interface GigabitEthernet1/0/2
port link-type access
port access vlan 100
poe enable
```

```
#
```

面的标签获取。

· 为了使服务器对用户授权信息进行动态修改或强制用户下线,必须开启RADIUS sess ion control功能。

· 为了防止用户上线过程中,动态授权信息下发失败,需要配置RADIUS DAE服务器功能。