wlan接入 802.1X AAA 李晨光 2016-07-06 发表

本文档介绍EAD认证的典型配置举例。

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接入和EAD认证相关特性。

如<u>图3-1</u>所示,Switch作为DHCP服务器为AP和Client分配IP地址。现要求在AC上配置EAD认证 ,使客户端通过该认证才可以接入无线网络。



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 192.1.1.1 16 [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 192.2.1.1 24 [AC-Vlan-interface200] quit # 配置AC和Switch相连侧的接口GigabitEthernet1/0/1为Trunk类型,禁止VLAN 1报文通过,允 许VLAN 100和VLAN 200通过,当前Trunk口的PVID为100。 [AC] interface gigabitethernet 1/0/1 [AC-GigabitEthernet1/0/1] port link-type trunk [AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1 [AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200 [AC-GigabitEthernet1/0/1] port trunk pvid vlan 100 [AC-GigabitEthernet1/0/1] quit (2) 开启端口安全功能,并配置802.1X认证方式为eap。 [AC] port-security enable [AC] dot1x authentication-method eap (3) 配置认证策略 # 创建名为radius1的RADIUS方案并进入其视图。 [AC] radius scheme radius1 # 设置主认证RADIUS服务器的IP地址8.1.1.16。 [AC-radius-radius1] primary authentication 8.1.1.16 #设置主计费RADIUS服务器的IP地址8.1.1.16。 [AC-radius-radius1] primary accounting 8.1.1.16 # 配置认证报文的共享密钥为明文example。

[AC-radius-radius1] key authentication simple example # 配置计费报文的共享密钥为明文example。 [AC-radius-radius1] key accounting simple example #配置实时计费的时间间隔为3分钟。 [AC-radius-radius1] timer realtime-accounting 3 #配置设备发送RADIUS报文使用的源IP地址为192.1.1.1。 [AC-radius-radius1] nas-ip 192.1.1.1 (4) 配置认证域 #配置认证域为radius1。 [AC] domain radius1 # 配置lan-access用户使用RADIUS方案radius1进行认证、授权和计费。 [AC-isp-radius1] authentication lan-access radius-scheme radius1 [AC-isp-radius1] authorization lan-access radius-scheme radius1 [AC-isp-radius1] accounting lan-access radius-scheme radius1 (5) 配置ACL #创建一个序号为3000的IPv4高级ACL,并进入其视图。 [AC] acl advanced 3000 # 定义一条规则,允许IP报文通过。 [AC-acl-ipv4-adv-3000] rule permit ip [AC-acl-ipv4-adv-3000] quit #创建一个序号为3001的IPv4高级ACL,并进入其视图。 [AC] acl advanced 3001 # 定义一条规则,允许UDP报文通过。 [AC-acl-ipv4-adv-3001] rule permit udp # 定义一条规则,禁止TCP报文通过。 [AC-acl-ipv4-adv-3001] rule deny tcp [AC-acl-ipv4-adv-3001] quit (6) 配置无线服务 #创建无线服务模板1,并进入无线服务模板视图。 [AC] wlan service-template 1 # 配置SSID为service。 [AC-wlan-st-1] ssid service # 配置无线客户端上线后将被加入到VLAN 200。 [AC-wlan-st-1] vlan 200 # 配置身份认证与密钥管理的模式为802.1X。 [AC-wlan-st-1] akm mode dot1x #配置加密套件为CCMP,安全信息元素为RSN。 [AC-wlan-st-1] cipher-suite ccmp [AC-wlan-st-1] security-ie rsn #配置用户接入认证模式为802.1X。 [AC-wlan-st-1] client-security authentication-mode dot1x #配置dot1x认证的domain域为radius1 [AC-wlan-st-1] dot1x domain radius1 # 使能无线服务模板。 [AC-wlan-st-1] service-template enable [AC-wlan-st-1] quit (7) 配置AP #创建手工AP, 名称为officeap, 型号名称为WA4320i-ACN。 [AC] wlan ap officeap model WA4320i-ACN #设置AP的序列号为210235A1K6C15A003025。 [AC-wlan-ap-officeap] serial-id 210235A1K6C15A003025 #进入AP的Radio 2视图,并将无线服务模板1绑定到Radio 2上。 [AC-wlan-ap-officeap] radio 2 [AC-wlan-ap-officeap-radio-2] service-template 1 #开启Radio 2的射频功能。 [AC-wlan-ap-officeap-radio-2] radio enable [AC-wlan-ap-officeap-radio-2] quit [AC-wlan-ap-officeap] quit

(8) 配置AC到RADIUS服务器的静态路由

1.1.2 配置Switch

(1) 配置Switch的接口 #创建VLAN 100及其对应接口,并为该接口配置IP地址,用于转发AC和AP间CAPWAP隧道内 的流量。 system-view [Switch] vlan 100 [Switch-vlan100] quit [Switch] interface vlan-interface 100 [Switch-Vlan-interface100] ip address 192.1.1.2 16 [Switch-Vlan-interface100] quit # 创建VLAN 200及其对应接口,并为该接口配置IP地址,用于转发Client无线报文。 [Switch] vlan 200 [Switch-vlan200] quit [Switch] interface vlan-interface 200 [Switch-Vlan-interface200] ip address 192.2.1.2 24 [Switch-Vlan-interface200] quit # 创建VLAN 8及其对应接口,并为该接口配置IP地址,用于与RADIUS服务器通信。 [Switch] vlan 8 [Switch-vlan8] quit [Switch] interface vlan-interface 8 [Switch-Vlan-interface8] ip address 8.1.1.2 8 [Switch-Vlan-interface8] quit # 配置Switch和AC相连侧的接口GigabitEthernet1/0/1为Trunk类型,禁止VLAN 1报文通过,允 许VLAN 100和VLAN 200通过,当前Trunk口的PVID为100。 [Switch] interface gigabitethernet 1/0/1 [Switch-GigabitEthernet1/0/1] port link-type trunk [Switch-GigabitEthernet1/0/1] undo port trunk permit vlan 1 [Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200 [Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100 [Switch-GigabitEthernet1/0/1] quit # 配置Switch与AP相连侧的GigabitEthernet1/0/2为trunk类型,禁止VLAN 1报文通过,允许VLA N 100和VLAN 200通过,并设置PVID为VLAN100。 [Switch] interface gigabitethernet 1/0/2 [Switch-GigabitEthernet1/0/2] port link-type trunk [Switch-GigabitEthernet1/0/2] undo port trunk permit vlan 1 [Switch-GigabitEthernet1/0/2] port trunk permit vlan 100 200 [Switch-GigabitEthernet1/0/2] port trunk pvid vlan 100 #开启Switch和AP相连的接口GigabitEthernet1/0/2的PoE供电功能。 [Switch-GigabitEthernet1/0/2] poe enable [Switch-GigabitEthernet1/0/2] quit # 配置Swith与Radius service相连侧的GigabitEthernet1/0/3为trunk类型, 禁止VLAN 1报文通过 , 允许VLAN 100和VLAN 200通过, 并设置PVID为VLAN 8。 [Switch] interface gigabitethernet 1/0/3 [Switch-GigabitEthernet1/0/3] port link-type trunk [Switch-GigabitEthernet1/0/3] undo port trunk permit vlan 1 [Switch-GigabitEthernet1/0/3] port trunk permit vlan 100 200 [Switch-GigabitEthernet1/0/3] port trunk pvid vlan 8 (2) 配置DHCP服务 #开启DHCP功能。 [Switch] dhcp enable # 创建名为vlan100的DHCP地址池,配置地址池动态分配的网段为192.1.0.0/16,地址池中不参 与自动分配的IP地址为192.1.1.1,网关地址为192.1.1.2,为AP分配IP地址。 [Switch] dhcp server ip-pool vlan100 [Switch-dhcp-pool-vlan100] network 192.1.0.0 mask 255.255.255.0 [Switch-dhcp-pool-vlan100] forbidden-ip 192.1.1.1 [Switch-dhcp-pool-vlan100] gateway-list 192.1.1.2

[Switch-dhcp-pool-vlan100] quit

创建名为vlan200的DHCP地址池,配置地址池动态分配的网段为192.2.1.0/24,地址池中不参 与自动分配的IP地址为192.2.1.1,网关地址为192.2.1.2,为Client分配IP地址。 [Switch] dhcpserverip-pool vlan200 [Switch-dhcp-pool-vlan200] network 192.2.1.0 mask 255.255.255.0 [Switch-dhcp-pool-vlan200] forbidden-ip 192.2.1.1 [Switch-dhcp-pool-vlan200] gateway-list 192.2.1.2 [Switch-dhcp-pool-vlan200] quit

1.1.3 配置RADIUSservice (iMC V7)

· 下面以iMC为例(使用iMC版本为: iMC PLAT 7.2、iMC EAD 7.2), 说明RADIUS ser ver的基本配置。

• 在服务器上已经完成证书的安装。

1. 在iMC上配置MAC认证项

接入设备配置:

(1) 在iMC"用户>接入策略管理>接入设备管理"中选择"接入设备配置"页面,在"接入设备 配置"页面中单击<增加>按钮,增加接入设备。

【用户 > 接入策略管	理 > 接入设备管理	> 接入设备配置								加入收藏 ?	明政
接入设备查询										高級直	i 0
设备IP地址从				Ŧ							
设备名称				接	入设备类型			•		查询重置	
増加 删除 🕴	参改 ▼下发配置	同步端口配置	与平台设备同步	批量导入	刷新		ţ	2能从平台中增加:否 🗞	AAA下发结果	國命令行下发结	Ŗ
设备名称	设备IP地址	设备型号	下发配置	类型	备注	下发结药	R	端口配置同步结果	详细信息	操作	
	8.50.1.21					未下发		无需同步	iFo,		
	8.121.1.4		H3C无线	ŧ		未下发		无需同步	iio,		

- (2) 在弹出的"增加接入设备"页面中:
- · 设置认证、计费共享密钥为example,其它保持缺省配置;
- 手工增加接入设备,添加IP地址为192.1.1.1的接入设备;
- 点击<确定>按钮,完成接入设备的添加。

🚏 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				
认证满口 *	1812	计费端口 *	1813	
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 *	example			
接入设备分组	无			
设备列表				
选择 手工増加 堆	制加IPv6设备 全部清除			
设备名称	设备IP地址	设备型号	裔注	删除
	192.1.1.1			1
共有1条记录。				
		确定 取消		

2. 配置安全策略

(1) 在iMC"用户>安全策略管理"中选择"安全策略管理",在"安全策略管理"页面中单击<增加>按钮,增加安全策略。

剪	1 用户 > 安全策略管理 > 安全策略管理									
	14200 AHH									
	安全策略名 ▲	安全级别 \$	隔离方式 \$	安全ACL或VLAN	隔离ACL或VLAN	业务分组 ≎	修改	删除		
	h3c-ead	监控模式	向设备下发ACL	3000	3001	未分组	e	Û		
	共有1条记录。									

- (2) 在弹出的"增加安全策略"页面中:
- | 配置安全策略名为"安全策略01";安全级别选择"监控模式";
- I 配置隔离方式为"向设备下发ACL",并设置安全ACL为3000,隔离ACL为3001;
- | 点击<确定>按钮, 完成安全策略的添加。

殿 ,	用户 > 安全策略管理 > 安全策略管理 >	增加安全策略							(?#I
2	共配置								-
1	基本信息								
9	2全策略名 *	安全策略01		业务分组 *		未分组		•	
9	R全级别 *	监控模式	•						
	进行实时监控 ⑦								
	還游缺盲安全策略 ⑦								
1	苗述								
	安全检查合格提示								
P	鬲离方式配置								
	- 隔离方式配置								
	✓ 配置隔离方式								
	●向设备下发ACL ○向客户遗下发	ACL〇下授VLAN							
	通用ACL	安全ACL	3000	• 7	隔离ACL		3001	- 0	D
	HP ProCurve ACL	安全ACL		•	隔离ACL				•

3. 配置接入策略

(1) 在iMC"用户>接入策略管理"中选择"接入策略管理",在"接入策略管理"页面中单击<增加>按钮,增加接入服务配置。

12.用户 > 接入策略管理 > 接入策略管理					大加入收藏 ②帮
接入策略查询					
接入策略名	业务分组		•		查询 重置
1850		吗。无线SSID池 早	终端硬盘序列号池	终端MAC地址池 早	逻接入ACL策略管理
接入策略名 ≎	描述 ≎		业务分组 😂	修改	删除
002163a44f85			未分组	B	1
0024d705c670			未分组	B	Û
(2) 在弹出的"增加接入贫 · 配置接入策略名为I	策略"页面中: EAD;				

- · 选择首选EAD类型为EAP-PEAP认证,子类型为EAP-MSCHAPv2;
- · 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,其它配置采用缺省值;
- · 点击<确定>按钮,完成接入策略的添加。

12 用户 > 接入策略管理 > 接入策略管理	> 増加接入策略				②帮助
基本信息					-
接入策略名*	EAD				
业务分组 *	未分组 🔻				
描述					
授权信息					-
接入时段	无	5	子爾JIP地址 *	否 •	
下行速率(Kbps)		1	上行速率(Kbps)		
优先级		r	下发用户组		(?)
首选EAP类型	EAP-PEAP 🔻	÷	子类型	EAP-MSCHAP\ 🕶	
EAP自协商	不启用 🔻				
下发VLAN		1	下发地址池		
下发User Profile					
下发ACL					

4. 配置服务策略

(1) 在iMC"用户>接入策略管理"中选择"接入服务管理",在"接入服务管理"页面中单击<增加>按钮,增加接入服务配置。

2	用户 > 接入策略管理 > 接入服务管理				ť	5加入收藏 ②帮助
	増加 刷新					
	服务名 \$	服务描述	服务后缀 \$	业务分组 \$	修改	删除
	whm-1x			未分组	B	Ô
	zkf2513_1x			未分组	B	Û

- (2) 在弹出的"增加接入服务"页面中,
- · 配置服务名为EAD;
- · 缺省安全策略选择安全策略01;
- · 缺省接入策略为EAD,其它配置采用缺省值;
- · 点击<确定>按钮,完成服务配置。

② 用户> 按入無點管理> 按入服务管理> 增加按入服务 ⑦ 開始								②帮助		
基本信息										-
服务名*	EAD			服务后缀						
业务分组 *	未分组	•	•	缺省接入策略 *		EAD		•	?	
缺省安全策略 *	安全策略01	•	•	缺省内网外连策略 *		不使用		•		
缺首私有属性下发策略 *	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网	制 *	0				
服务描述										
✔ 可申请 ?				✔ 无感知认证 ⑦						
接入场景列表										-
均加										
名称 接入第四	8	安全策略		私有属性下发策略	内网外连策略		优先级	修改	删除	
未找到符合条件的记录。										
				确定 取消						

5.配置帐号用户:

۰

(1) 在iMC"用户>接入用户"页面中单击<增加>按钮,增加接入用户。

□ 用户 > 接入用户						参加入	收藏 ⑦ 帮助
接入用户							高级查询
帐号名		用户姓名					
用户分组	្លំរ	服务名	•			查询	重置
增加 批量导入 修改帐号	加入黑名单注销帐号申请服务	注销服务 ▼更多					
● 株号名 \$	用户姓名 ≎			用户分组	开户日期	生效时间 \$	失效时间
fxj-portal	fxj-portal			未分组	2016-03-03		
Ihch001	lhch			未分组	2016-03-03		
12 用户 > 接入用户 > 增加接入用	خ ر!						②帮助
接入信息							-
用户姓名 *	选择	增加用户					
帐号名 *	3						
预开户用户	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	自用用户	密码控制策略	下次登	景须修改密码	₿		
生效时间		失效时间					
最大闲置时长(分钟)		在线数量限制	1				
登录提示信息							

(3) 在弹出增加用户窗体中输入用户名为"EAD_guest",证件号码可以根据需要输入相关 证件号码,然后点击<确定>按钮,提示增加用户成功,并返回增加接入用户界面。

增加用户				
基本信息				
用户姓名 *	EAD_guest	证件号码 *	000	检查是否可用
通讯地址		电话		?
电子邮件		⑦ 用户分组 *	未分组	ພໍ່ນ
		确定 取消		

(4) 页面输入帐号和密码(这里采用的用户名为EAD_guest,密码为12345678),选择前面配置的接入服务为EAD,其它参数可以根据需要配置,然后点击<确定>按钮,完成配置

接入	信息								[
用用	□姓名 *	EAD_guest 选择	增加用户						
帐	5名 *	EAD_guest							
	预开户用户	MAC地址认证用户	主机名用户		快速认证用户				
Elso	码 *			密码确认	(*		•		
v	✔ 允许用户修改密码	启用	用户密码控制策略			下次登录须	修改密码		
纟	波时间	O		失效时间]		t	ž.	
最	大闲置时长(分钟)			在线数量	1限制	1			
登?	灵提示信息								
	dyl				不使用		可申请		
/	EAD				安全策略01		可申请		
	eap-an				不使用		可申请		
MA	Ct地址								
2	▼ 500万 注意:在文本框中输入多条信息时,	每行只能输入一条信息。							
			确定 确定并	FTED I	取消				

1.1.4 iNode客户端配置

iNode客户端配置如下所示:

(1) 打开iNode客户端。



(2) 点击无线连接,出现无线连接界面。



(3) 点击无线连接窗体右侧的倒三角,选择配置的SSID为service的无线服务。



(4) 点击连接右侧的倒三角,选择属性。在属性对话框中选择"安全"页面,选择安全类型为WPA2,加密类型为AES,然后点击"802.1x属性"。

2	service 属性	×
	连接 安全	
	安全类型	WPA2 -
	加密类型	AES 💌
	密钥索引	1 -
		□ 自动连接
		🔲 断线后自动重连
		自动重连次数 3 🔻
		802.1X 属性
		确定取消

(5) 在802.1X属性对话框中选择"网络设置",报文类型为"多播",其他选项采用默认值,点击<确定>。

¥ 802.1X 属性	×
网络设置 连接设置	
- 报文类型	
◎ 单播	
◎ 多播	
用户选项	
□ 上传IP地址	
Selection State S	
- 认证选项	
☑ 上传客户端版本号	
恢复为联制体	
	确定即消

(6) 在"802.1X属性"窗体中选择"连接设置",认证类型为"PEAP",其他选项不动,然后点 击确定。

¥ 802.1X 属性	x
网络设置 连接设置	
◎ 普通连接	
◎ 单点登录连接	
认证类型	
PEAP	
─ EAP-TLS	选择客户端证书
EAP-TTLS	· · · · · · · · · · · · · · · · · · ·
□ 验证服务器证书	
🗌 从证书中读取用户名	
	确定 取消

(7) 关闭属性窗体后,返回iNode无线连接界面,输入用户名为EAD_guest,密码为12345 678。



(9) 点击连接, 连接成功后如下。



1.2 验证配置

(1) 使用display dot1x sessions查看dot1x用户已在线。

display dot1x sessions

AP name: officeap Radio ID: 2 SSID: service

Online 802.1X users: 1

MAC address Auth state

0015-00bf-e84d Authenticated

(2) 使用display wlan client verbose查看EAD是否下发,查看到ACL3000,由此可知EA

D安全策略下发成功

display wlan client verbose

Total number of clients: 1

MAC address	: 0015-00bf-e84d
IPv4 address	: 192.2.1.3
IPv6 address	: N/A
Username	: ead_guest
AID :	: 1
AP ID	:2
AP name	: officeap
Radio ID	:2
SSID	: service
BSSID	: 3891-d58a-8930
VLAN ID	: 200
Sleep count	: 18
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+80	MHz : Not supported
STBC RX capability	: Supported
STBC TX capability	: Not supported
LDPC RX capability	: Not supported
SU beamformee capabi	lity : Not supported
MU beamformee capab	ility : Not supported
Beamformee STS capa	bility : N/A
Block Ack : TID 0 Out	

Supported VHT-MCS set : NSS1 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 NSS2 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 Supported HT MCS set : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15 Supported rates : 6, 9, 12, 18, 24, 36, 48, 54 Mbps : WMM QoS mode Listen interval : 250 RSSI : 34 : 58.5/324 Rx/Tx rate Authentication method : Open system Security mode : RSN AKM mode : 802.1X : CCMP Cipher suite User authentication mode : 802.1X Authorization ACL ID : 3000 Authorization user profile : N/A : N/A Roam status : SHA1 Key derivation PMF status : N/A Forwarding policy name : N/A Online time : 0days 0hours 2minutes 49seconds FT status : Inactive

1.3 配置文件

AC # dot1x authentication-method eap # port-security enable # vlan 100 # vlan 200 # wlan service-template 1 ssid service vlan 200 akm mode dot1x cipher-suite ccmp security-ie rsn client-security authentication-mode dot1x dot1x domain radius1 service-template enable # interface Vlan-interface100 ip address 192.1.1.1 255.255.0.0 # interface Vlan-interface200 ip address 192.2.1.1 255.255.255.0 # interface GigabitEthernet1/0/1 port link-type trunk undo port trunk permit vlan 1 port trunk permit vlan 100 200 port trunk pvid vlan 100 # ip route-static 8.0.0.0 8 192.2.1.2

```
#
acl advanced 3000
rule 0 permit ip
#
acl advanced 3001
rule 0 permit udp
rule 5 deny tcp
#
radius scheme radius1
primary authentication 8.1.1.16
primary accounting 8.1.1.16
key authentication cipher $c$3$YCjREST8/BuXrsEKyY9nY8QQfmrN3w==
key accounting cipher $c$3$yPGJYnF7FE+/36JrXfn+DYGq/8ngZA==
timer realtime-accounting 3
nas-ip 192.1.1.1
#
domain radius1
authentication lan-access radius-scheme radius1
authorization lan-access radius-scheme radius1
accounting lan-access radius-scheme radius1
#
wlan ap officeap model WA4320i-ACN
serial-id 210235A1K6C15A003025
radio2
 radio enable
 service-template 1
#
          Switch
#
dhcp enable
#
vlan8
#
vlan 100
#
vlan 200
#
dhcp server ip-pool vlan100
gateway-list 192.1.1.2
network 192.1.0.0 mask 255.255.0.0
forbidden-ip 192.1.1.1
#
dhcp server ip-pool vlan200
gateway-list 192.2.1.2
network 192.2.1.0 mask 255.255.255.0
forbidden-ip 192.2.1.1
#
interface Vlan-interface8
ip address 8.1.1.2 255.0.0.0
#
interface Vlan-interface100
ip address 192.1.1.2 255.255.255.0
#
interface Vlan-interface200
ip address 192.2.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-type trunk
undo port trunk permit vlan 1
```

port trunk permit vlan 100 200 port trunk pvid vlan 100 # interface GigabitEthernet1/0/2 port link-type trunk undo port trunk permit vlan 1 port trunk permit vlan 100 200 port trunk pvid vlan 100 poe enable # interface GigabitEthernet1/0/3 port link-type trunk undo port trunk permit vlan 1

port trunk permit vlan 100 200

port trunk pvid vlan 8

#

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。