# H3C无线控制器IPv6的EAD认证典型配置举例(V7)

IPv6 802.1X 王媛媛 2018-08-05 发表

## 组网及说明

**1 组网及说明**

本文档介绍IPv6的EAD认证的典型配置举例。

**1.1 配置前提**

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。

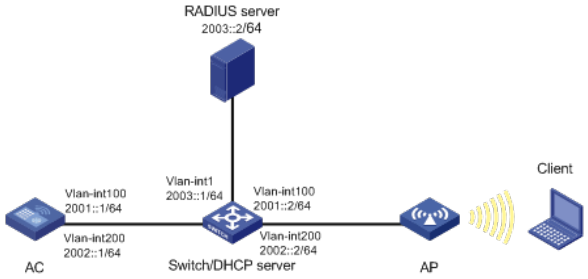
本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文档假设您已了解WLAN接入和EAD认证相关特性。

**1.1 组网需求**

如图1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。

图1 EAD认证组网图




## 配置步骤

**2 配置步骤**

**2.1 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将通过该VLAN与AC建立CAPWAP隧道。

<AC> system-view

[AC] vlan 100

[AC-vlan100] quit

[AC] interface vlan-interface 100

[AC-Vlan-interface100] ipv6 address 2001::1 64

[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] ipv6 address 2002::1 64

[AC-Vlan-interface200] quit

# 配置AC与Switch相连的接口GigabitEthernet1/0/1的属性为Trunk，允许VLAN 1、VLAN 100和VLAN 200通过。

[AC] interface gigabitethernet 1/0/1

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

[ACh-GigabitEthernet1/0/1] port trunk permit vlan 1 100 200

[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2003::2。

[AC-radius-radius1] primary authentication ipv6 2003::2

# 设置主计费RADIUS服务器的IP地址2003::2。

[AC-radius-radius1] primary accounting ipv6 2003::2

# 配置认证报文的共享密钥为明文12345。
[AC-radius-radius1] key authentication simple 12345
# 配置计费报文的共享密钥为明文12345。
[AC-radius-radius1] key accounting simple 12345
# 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2001::1。
[AC-radius-radius1] nas-ip ipv6 2001::1
[AC-radius-radius1] quit
(4) 配置认证域
# 配置认证域为dom1。
[AC] domain dom1
# 配置lan-access用户使用RADIUS方案radius1进行认证、授权和计费。
[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
(5) 配置ACL
# 创建一个序号为3000的IPv6高级ACL，并进入其视图。
[AC] acl ipv6 advanced 3000
# 定义一条规则，允许IPv6报文通过。
[AC-acl-ipv6-adv-3000] rule permit ipv6
[AC-acl-ipv6-adv-3000] quit
# 创建一个序号为3001的IPv6高级ACL，并进入其视图。
[AC] acl ipv6 advanced 3001
# 定义一条规则，允许UDP报文通过。
[AC-acl-ipv6-adv-3001] rule permit udp
# 定义一条规则，禁止TCP报文通过。
[AC-acl-ipv6-adv-3001] rule deny tcp
[AC-acl-ipv6-adv-3001] quit
(6) 配置无线服务
# 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
# 配置无线客户端上线后将被加入到VLAN 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
# 配置加密套件为CCMP，安全信息元素为RSN。
[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dot1x认证的domain域为dom1
[AC-wlan-st-service] dot1x domain dom1
# 开启通过DHCPv6方式学习客户端IPv6地址功能。
[AC-wlan-st-service] client ipv6-snooping dhcpv6-learning enable
# 使能无线服务模板。
[AC-wlan-st-service] service-template enable
[AC-wlan-st-service] quit
(7) 配置AP
# 创建手工AP，名称为ap1，型号名称为UAP300。
[AC] wlan ap ap1 model UAP300
# 设置AP的序列号为219801A15K8171E00166。
[AC-wlan-ap-ap1] serial-id 219801A15K8171E00166
# 进入AP的Radio 1视图，并将无线服务模板service绑定到Radio 1上。
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] service-template service
# 开启Radio 2的射频功能。
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] quit
[AC-wlan-ap-ap1] quit
(8) 配置AC到RADIUS服务器的静态路由

[AC] ipv6 route-static 2003:: 64 2001::2

**2.2 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IPv6地址，用于转发AC和AP间CAPWAP隧道内的流量。

<Switch> system-view

[Switch] vlan 100

[Switch-vlan100] quit

[Switch] interface vlan-interface 100

[Switch-Vlan-interface100] ipv6 address 2001::2 64

[Switch-Vlan-interface100] quit

# 创建VLAN 200及其对应接口，并为该接口配置IPv6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] ipv6 address 2002::2 64

[Switch-Vlan-interface200] quit

# 创建VLAN 1及其对应接口，并为该接口配置IPv6地址，用于与RADIUS服务器通信。

[Switch] vlan 1

[Switch-vlan1] quit

[Switch] interface vlan-interface 1

[Switch-Vlan-interface1] ipv6 address 2003::1 64

[Switch-Vlan-interface1] quit

# 配置Switch与AC相连的GigabitEthernet1/0/1接口的属性为Trunk，允许VLAN 1、VLAN 100和VLAN 200通过。

[Switch] interface gigabitethernet 1/0/1

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

[Switch-GigabitEthernet1/0/1] port trunk permit vlan 1 100 200

[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

# 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

(2) 配置DHCPv6服务

# 配置DHCPv6地址池1，用于为AP分配IPv6地址。

[Switch] ipv6 dhcp pool 1

[Switch-dhcp6-pool-1] network 2001::/64

[Switch-dhcp6-pool-1] gateway-list 2001::1

# 配置Option选项，使AP获取AC的IPv6地址。

[Switch-dhcp6-pool-1] option 52 hex 20010000000000000000000000000001

[Switch-dhcp6-pool-1] quit

[Switch] ipv6 dhcp server forbidden-address 2001::1

# 配置在VLAN 100接口下引用地址池1，并配置该接口工作在DHCPv6服务器模式。

[Switch] interface vlan-interface 100

[Switch-Vlan-interface100] ipv6 dhcp select server

[Switch-Vlan-interface100] ipv6 dhcp server apply pool 1

# 取消VLAN 100接口对RA消息发布的抑制。配置被管理地址的配置标志位为1，即主机通过DHCPv6服务器获取IPv6地址。配置其他信息配置标志位为1，即主机通过DHCPv6服务器获取除IPv6地址以外的其他信息。

[Switch-Vlan-interface100] ipv6 nd autoconfig managed-address-flag

[Switch-Vlan-interface100] ipv6 nd autoconfig other-flag

[Switch-Vlan-interface100] undo ipv6 nd ra halt

[Switch-Vlan-interface100] quit

# 配置DHCPv6地址池2，用于为Client分配IPv6地址。

[Switch] ipv6 dhcp pool 2

[Switch-dhcp6-pool-2] network 2002::/64

[Switch-dhcp6-pool-2] gateway-list 2002::1

[Switch-dhcp6-pool-2] quit

[Switch] ipv6 dhcp server forbidden-address 2002::1

# 配置在VLAN 200接口下引用地址池2，并配置该接口工作在DHCPv6服务器模式。

[Switch] interface Vlan-interface 200

[Switch-Vlan-interface200] ipv6 dhcp select server
[Switch-Vlan-interface200]ipv6 dhcp server apply pool 2
# 取消VLAN 200接口下对RA消息发布的抑制。配置被管理地址的配置标志位为1，即主机通过DHCPv6服务器获取IPv6地址。配置其他信息配置标志位为1，即主机通过DHCPv6服务器获取除IPv6地址以外的其他信息。
[Switch-Vlan-interface200] ipv6 nd autoconfig managed-address-flag
[Switch-Vlan-interface200] ipv6 nd autoconfig other-flag
[Switch-Vlan-interface200] undo ipv6 nd ra halt
[Switch-Vlan-interface200] quit

**2.3 配置RADIUS service（iMC V7)**

· 下面以iMC为例（使用iMC版本为：iMC PLAT 7.1、iMC EAD 7.1），说明RADIUS server的基本配置。
· 在服务器上已经完成证书的安装。

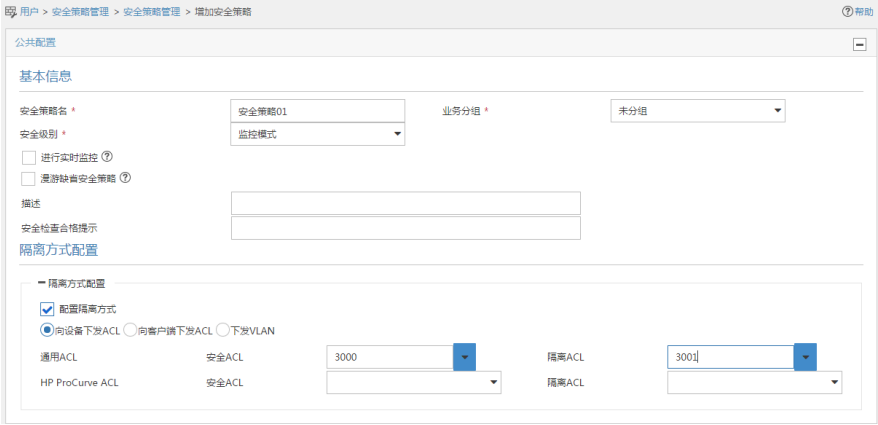
**2.3.1 在iMC上配置MAC认证项**

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。
· 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IPv6接入设备，添加IPv6地址为2001::1的接入设备；


**2.3.2. 配置安全策略**

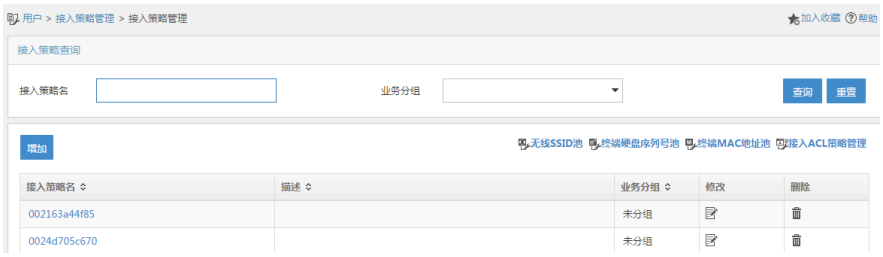
(1) 在iMC“用户>安全策略管理”中选择“安全策略管理”，在“安全策略管理”页面中单击<增加>按钮，增加安全策略。


(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”；
· 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。




**2.3.3 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。



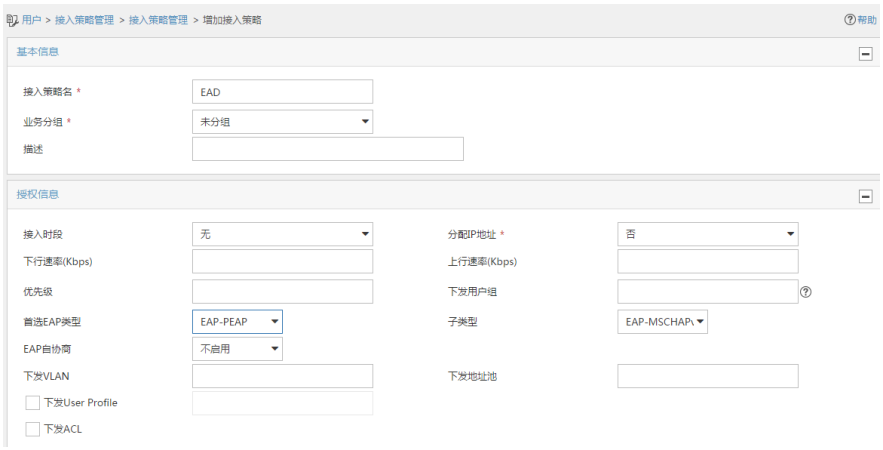

(2) 在弹出的“增加接入策略”页面中：

· 配置接入策略名为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。




### 2.3.4 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。

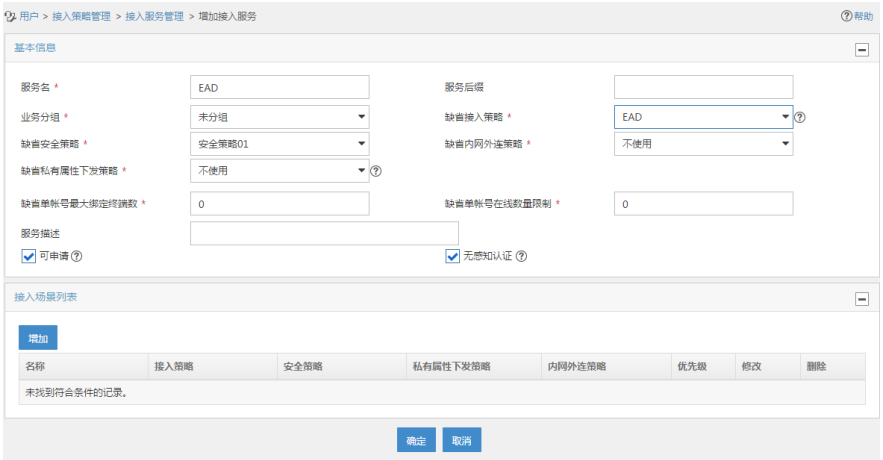

(2) 在弹出的“增加接入服务”页面中，

· 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。



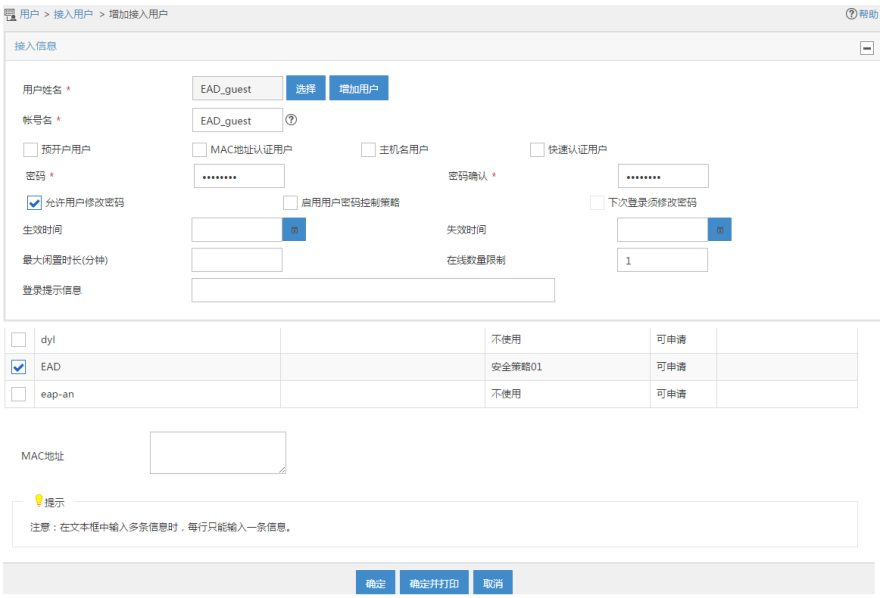

### 2.3.4 配置帐号用户：

(1) 在iMC“用户>接入用户”页面中单击<增加>按钮，增加接入用户。


(2) 在增加接入用户界面，单击<增加用户>。


(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。


(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。




### 2.4 配置客户端

# 打开手机，选择SSID为service无线服务进行连接，然后输入无线网络信息。

· EAP方法选择PEAP；

· 身份输入EAD_guest；

· 密码输入12345678；

· 其它保持缺省配置，然后单击“连接”。

图2 连接无线网络

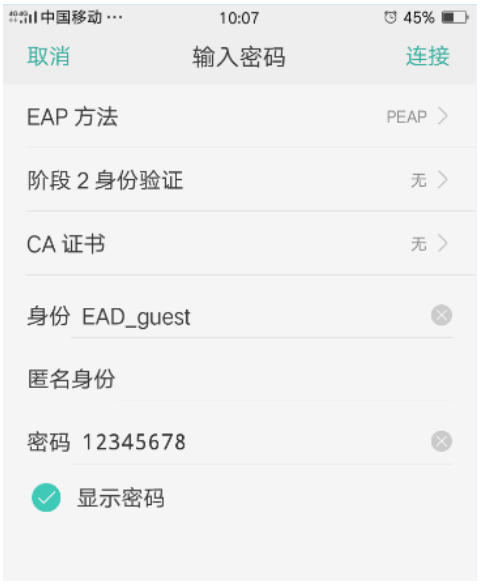



图3 无线网络连接成功


**2.5 验证配置**

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

<AC> display dot1x sessions
AP name: ap1 Radio ID: 1 SSID: service
Online 802.1X users: 1
MAC address Auth state
3829-5a40-9589 Authenticated

(2) 使用**display wlan client verbose**命令查看EAD策略是否下发，查看到ACL3001，由此可知EAD安全策略下发成功

<AC> display wlan client verbose
Total number of clients: 1

MAC address : 3829-5a40-9589
IPv4 address : N/A
IPv6 address : 2002::3
Username : EAD_guest
AID : 1
AP ID : 2
AP name : ap1
Radio ID : 1

```
 SSID                          : service
 BSSID                         : ac74-090a-6421
 VLAN ID                       : 200
 Sleep count                   : 18
 Wireless mode                 : 802.11an
 Channel bandwidth             : 40MHz
 20/40 BSS Coexistence Management  : Supported
 SM power save                 : Enabled
 SM power save mode            : Static
 Short GI for 20MHz            : Supported
 Short GI for 40MHz            : Supported
 STBC RX capability            : Supported
 STBC TX capability            : Not supported
 LDPC RX capability            : Not supported
 Block Ack                     : TID 0  Both
 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               : 2
 RSSI                          : 30
 Rx/Tx rate                    : 0/0 Mbps
 Authentication method         : Open system
 Security mode                 : RSN
 AKM mode                      : 802.1X
 Cipher suite                  : CCMP
 User authentication mode      : 802.1X
 Authorization ACL ID          : 3001
 Authorization user profile    : N/A
 Roam status                   : N/A
 Key derivation                : SHA1
 PMF status                    : N/A
 Forwarding policy name        : Not configured
 Online time                   : 0days 0hours 0minutes 2seconds
 FT status                     : Inactive
```

**2.6 配置文件**

· AC

```
#
 dot1x authentication-method eap
#
 port-security enable
#
vlan 1
#
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
 client ipv6-snooping dhcpv6-learning enable
 service-template enable
#
interface Vlan-interface100
 ipv6 address 2001::1/64
#
interface Vlan-interface200
 ipv6 address 2002::1/64
```

```
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 100 200
#
 ipv6 route-static 2003:: 64 2001::2
#
acl ipv6 advanced 3000
 rule 0 permit ipv6
#
acl ipv6 advanced 3001
 rule 0 permit udp
 rule 5 deny tcp
#
radius scheme radius1
 primary authentication ipv6 2003::2
 primary accounting ipv6 2003::2
 key authentication cipher $c$3$CAoJIYj1WmUo808RrsxOvXcfUpkZLcPY
 key accounting cipher $c$3$9YjVI/VV3rlbbKw7TZOnaGZGY/gD0pKU
 timer realtime-accounting 3
 nas-ip ipv6 2001::1
#
domain dom1
 authentication lan-access radius-scheme radius1
 authorization lan-access radius-scheme radius1
 accounting lan-access radius-scheme radius1
#
wlan ap ap1 model UAP300
 serial-id 219801A15K8171E00166
 radio 1
  radio enable
  service-template service
#
·  Switch
#
 dhcp enable
#
 ipv6 dhcp server forbidden-address 2001::1
 ipv6 dhcp server forbidden-address 2002::1
#
vlan 1
#
vlan 100
#
vlan 200
#
ipv6 dhcp pool 1
 network 2001::/64
 option 52 hex 20010000000000000000000000000001
 gateway-list 2001::1
#
ipv6 dhcp pool 2
 network 2002::/64
 gateway-list 2002::1
#
interface Vlan-interface1
 ipv6 address 2003::1/64
#
interface Vlan-interface100
ipv6 dhcp select server
ipv6 dhcp server apply pool 1
 ipv6 address 2001::2/64
 ipv6 nd autoconfig managed-address-flag
```

```
 ipv6 nd autoconfig other-flag
 undo ipv6 nd ra halt
#
interface Vlan-interface200
 ipv6 dhcp select server
 ipv6 dhcp server apply pool 2
 ipv6 address 2002::2/64
 ipv6 nd autoconfig managed-address-flag
 ipv6 nd autoconfig other-flag
 undo ipv6 nd ra halt
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 100 200
#
interface GigabitEthernet1/0/2
 port access vlan 100
 poe enable
#
```

## 配置关键点

无