H3C 无线控制器

IPv6 EAD 认证典型配置举例(V7)

资料版本：6W100-20191125

目录

1 简介

本文档介绍 IPv6 的 EAD 认证的典型配置举例。

2 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。

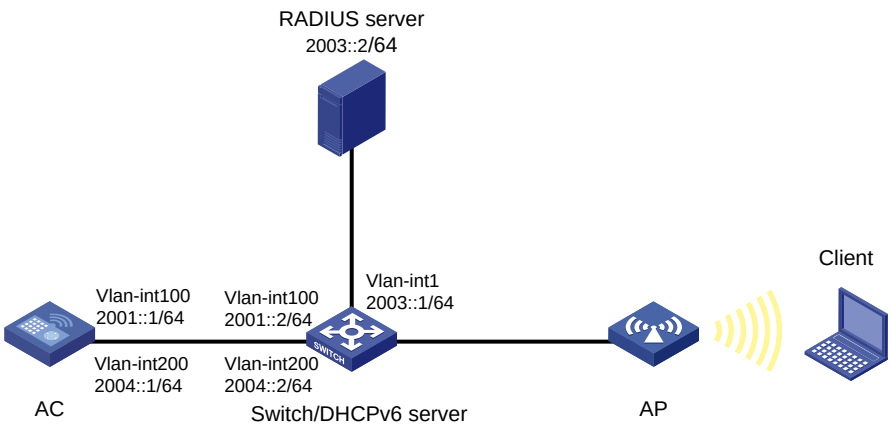
本文档假设您已了解 WLAN 接入和 EAD 认证相关特性。

3 配置举例

3.1 组网需求

如图 1 所示，Switch 作为 DHCPv6 服务器为 AP 和 Client 分配 IPv6 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



3.2 配置注意事项

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。

3.3 配置步骤

3.3.1 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 IPv6 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 IPv6 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 2004::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
[AC-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 IPv6 地址 2003::2。

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

设置主计费 RADIUS 服务器的 IPv6 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 IPv6 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 1 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 2004::2
```

3.3.2 配置Switch

(1) 配置 Switch 的接口

创建 VLAN 100，用于转发 AC 和 AP 间 CAPWAP 隧道内的流量。

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
```

配置 VLAN 100 接口的 IPv6 地址。

```
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ipv6 address 2001::2 64
[Switch-Vlan-interface100] quit
```

创建 VLAN 200，用于转发 Client 无线报文。

```
[Switch] vlan 200
[Switch-vlan200] quit
```

配置 VLAN 200 接口的 IPv6 地址。

```
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ipv6 address 2004::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 server apply pool 1
[Switch-Vlan-interface100] ipv6 dhcp select server
```

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 2004::/64
[Switch-dhcp6-pool-2] gateway-list 2004::2
[Switch-dhcp6-pool-2] quit
[Switch] ipv6 dhcp server forbidden-address 2004::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 server apply pool 2
[Switch-Vlan-interface200] ipv6 dhcp select server
```

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
```

3.3.3 配置RADIUS service（iMC V7）

说明

- 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。

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. 配置安全策略

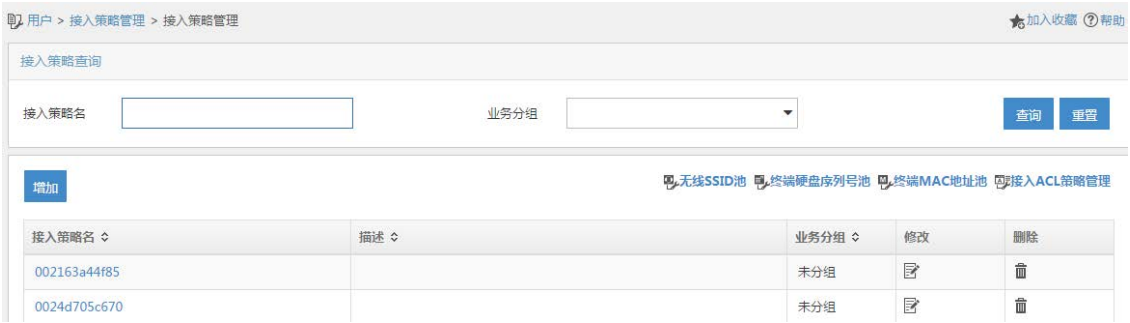
(1) 在 iMC“用户>安全策略管理”中选择“安全策略管理”，在“安全策略管理”页面中单击<增加>按钮，增加安全策略。

(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。

3. 配置接入策略

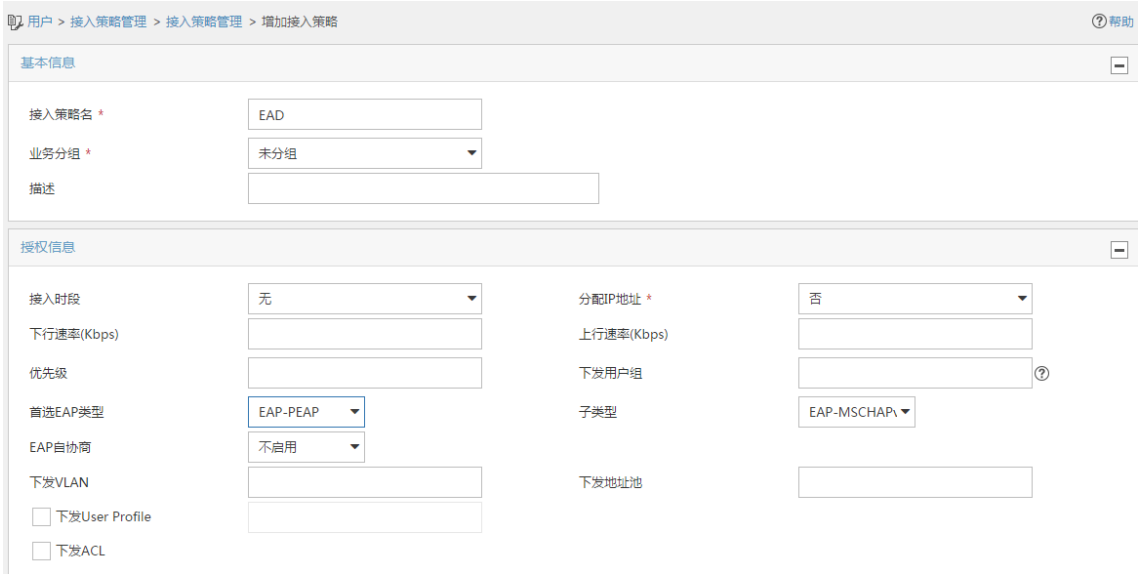
(1) 在 iMC“用户>接入策略管理”中选择“接入策略管理”，在“接入策略管理”页面中单击<增加>按钮，增加接入服务配置。



(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。

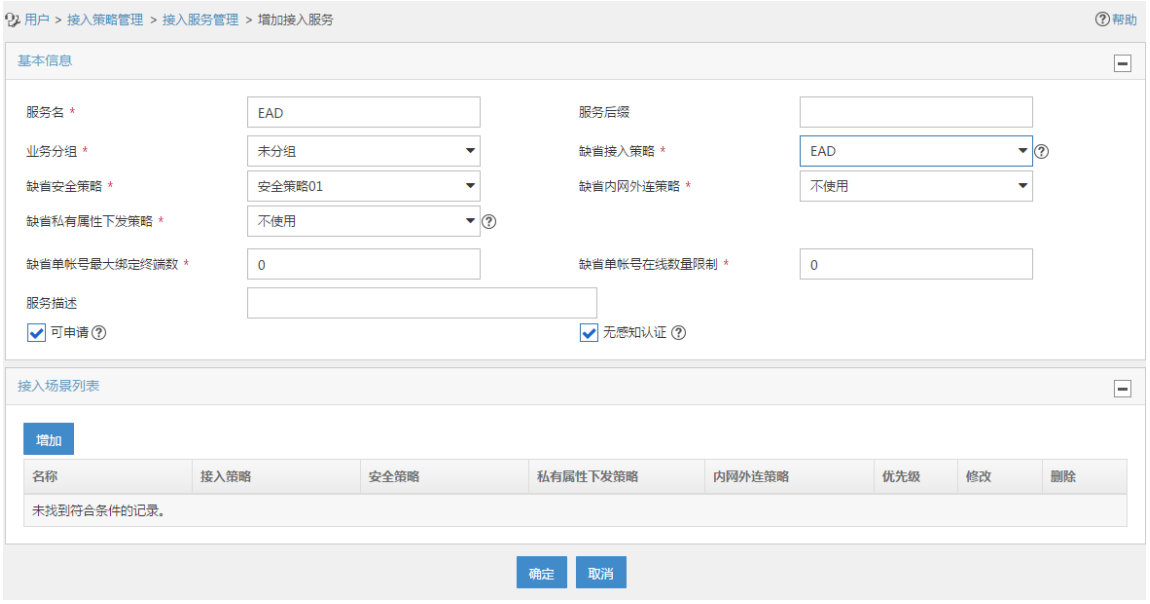


4. 配置服务策略

(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。



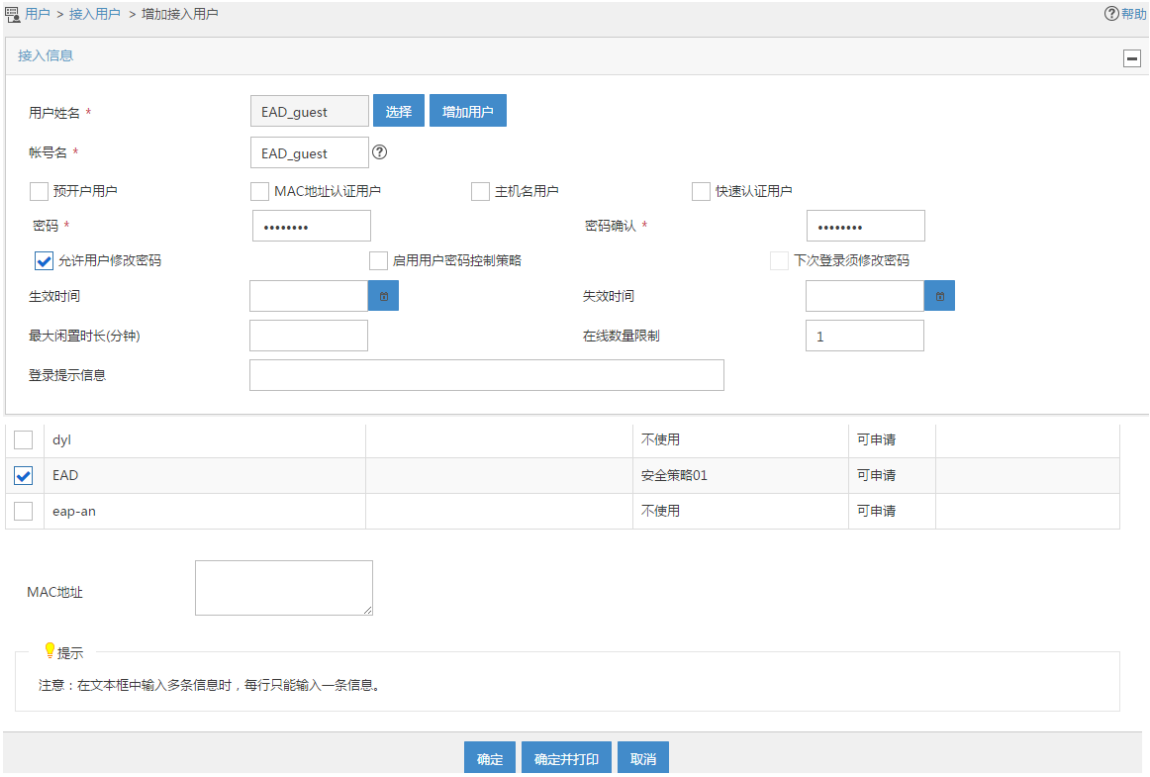
5. 配置帐号用户：

(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。



3.3.4 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

3.4 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                   : 2004::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
```

3.5 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 2004::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 2004::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

```
#
 ipv6 dhcp server forbidden-address 2001::1
 ipv6 dhcp server forbidden-address 2004::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 2004::/64
 gateway-list 2004::2
#
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 2004::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
#
```

4 相关资料

- 《H3C 无线控制器产品 配置指导》中的“用户接入与认证配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“用户接入与认证命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“WLAN 接入配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“WLAN 接入命令参考”。
- 《H3C 无线控制器产品 配置指导》中的“AP 管理配置指导”。
- 《H3C 无线控制器产品 命令参考》中的“AP 管理命令参考”。