

H3C 无线控制器

IPv6 802.1X 远程认证典型配置举例(V7)

资料版本：6W100-20191125

Copyright © 2019 新华三技术有限公司 版权所有，保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

本文档中的信息可能变动，恕不另行通知。

目 录

1 简介.....	1
2 配置前提.....	1
3 配置举例.....	1
3.1 组网需求.....	1
3.2 配置注意事项.....	2
3.3 配置步骤.....	2
3.3.1 配置 AC.....	2
3.3.2 配置 Switch.....	4
3.3.3 配置 RADIUS server.....	5
3.3.4 配置客户端.....	8
3.4 验证配置.....	10
3.5 配置文件.....	12
4 相关资料.....	14

1 简介

本文档介绍 IPv6 的 802.1X 远程认证典型配置举例。

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 IPv6 基础、WLAN 接入、WLAN 用户安全、WLAN 用户接入认证和 802.1X 的相关特性。

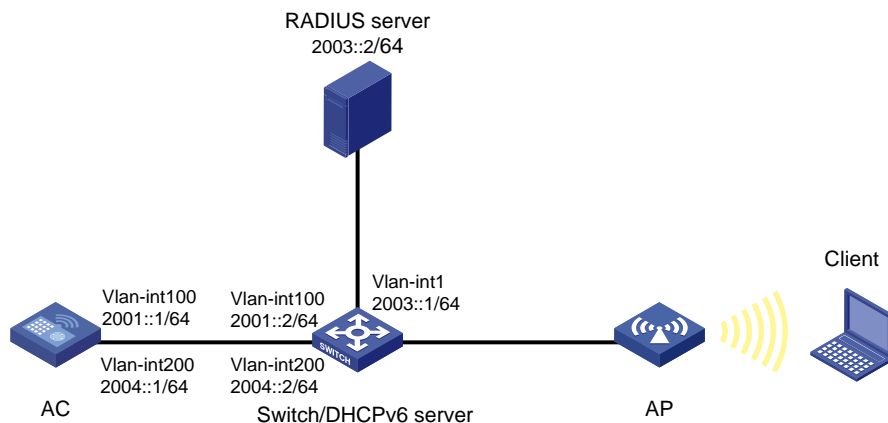
3 配置举例

3.1 组网需求

如图1所示组网，Switch 作为 DHCPv6 server 为 AP 和 Client 分配 IPv6 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。

图1 远程 802.1X 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。
- 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 session control 功能。

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 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] 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) 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 IPv6 地址为 2003::2。

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

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 IPv6 地址为 2001::1。

```
[AC-radius-radius1] nas-ip ipv6 2001::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 RADIUS 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 IPv6 地址为 2003::2，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 ipv6 2003::2 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
# 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
# 创建 AP，配置 AP 名称为 ap1，型号名称选择 UAP300，并配置序列号 219801A15K8171E00166。
[AC] wlan ap ap1 model UAP300
[AC-wlan-ap-ap1] serial-id 219801A15K8171E00166
# 进入 Radio 1 视图。

```

```
[AC-wlan-ap-ap1] radio 1
# 将无线服务模板 service 绑定到 radio 1，并开启射频。
[AC-wlan-ap-ap1-radio-1] service-template service
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] quit
[AC-wlan-ap-ap1] quit
(5) 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

```
# 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
# 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 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
# 使能 PoE 功能。
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
# 配置 VLAN 1 接口的 IPv6 地址。
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] ipv6 address 2003::1 64
[Switch-Vlan-interface1] 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
# 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
# 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 server



说明

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

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。在该页面中单击<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 IPv6 接入设备，添加 IPv6 地址为 2001::1 的接入设备。

图2 增加接入设备页面

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 增加IPv6设备 全部清除

设备名称	设备IP地址	设备型号	备注	删除
未找到符合条件的记录。				

增加接入策略。

选择“用户”页签，单击导航树中的[接入策略管理/接入策略管理]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3 增加服务策略页面

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4 增加接入服务页面

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5 增加接入用户页面

用户 > 接入用户 > 增加接入用户

接入用户

接入信息

用户姓名 *

帐号名 *

预开户用户 缺省BYOD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 启用用户密码控制策略 下次登录须修改密码

生效时间 失效时间

最大闲置时长(分钟) 在线数量限制

Portal无感知认证最大绑定数 *

<input type="checkbox"/>	do1x		不使用	可申请
<input checked="" type="checkbox"/>	dot1x		不使用	可申请
<input type="checkbox"/>	dotpap		不使用	可申请

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 dot1x;
- 密码输入 dot1x123;
- 其它保持缺省配置，然后单击“连接”。

图6 连接无线网络



图7 无线网络连接成功



3.4 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           : 3829-5a40-9589
IPv4 address          : N/A
IPv6 address          : 2004::4
Username              : dot1x
AID                   : 1
AP ID                 : 2
AP name               : ap1
Radio ID              : 1
SSID                  : service
BSSID                 : ac74-090a-6421
VLAN ID               : 200
Sleep count           : 0
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                     : N/A
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                          : 0
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          : N/A
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 1seconds
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             : 3829-5a40-9589
AP name                      : ap1
Radio ID                    : 1
SSID                        : service
BSSID                       : ac74-090a-6421
Username                    : dot1x
Authentication domain        : dom1
IPv6 address                 : 2004::4
Authentication method       : EAP
Initial VLAN                 : 200
Authorization VLAN           : 200
Authorization ACL number     : N/A
Authorization user profile   : N/A
Termination action          : Radius-Request
Session timeout period      : 86401 s
Online from                  : 2018/07/18 10:36:00
Online duration              : 0h 0m 19s

```

3.5 配置文件

- AC:

```
#
 dot1x authentication-method eap
#
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
#
  radius session-control enable
#
radius scheme radius1
  primary authentication ipv6 2003::2
  primary accounting ipv6 2003::2
  key authentication cipher $c$3$Nc0p9aAdeZsigfKkc+BNOVwrlStmtFHa
  key accounting cipher $c$3$1UiOGNVopIKWmUamDZBOPk2pSJ9+C7U5
  nas-ip ipv6 2001::1
#
radius dynamic-author server
  client ipv6 2003::2 key cipher $c$3$mOGMY0tNJT94RiwVyD80JG2zYwsUfpNV
#
```

```

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”。