H3C无线控制器远程IPv6的802.1X认证典型配置举例(V7)

802.1X IPv6 王媛媛 2018-08-09 发表

组网及说明

1 组网及说明

本文档介绍IPv6的802.1X远程认证典型配置举例。

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。

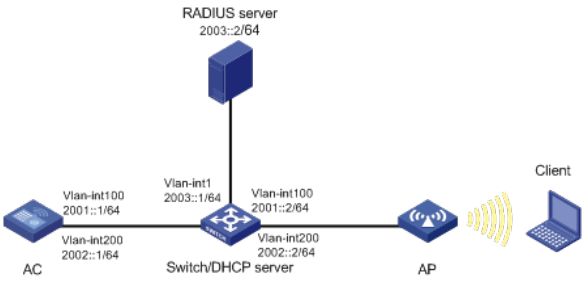
本文档假设您已了解IPv6基础、WLAN接入、WLAN用户安全、WLAN用户接入认证和802.1X的相关特性。

1.2 组网需求

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。**

图1 远程802.1X认证组网图



1.3 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。**

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 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) 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IP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RADUIS session control功能[w12] 。
[AC] radius session-control enable
(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 2001::2

2.2 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 2002::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 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 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
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 server

· 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

增加接入策略。

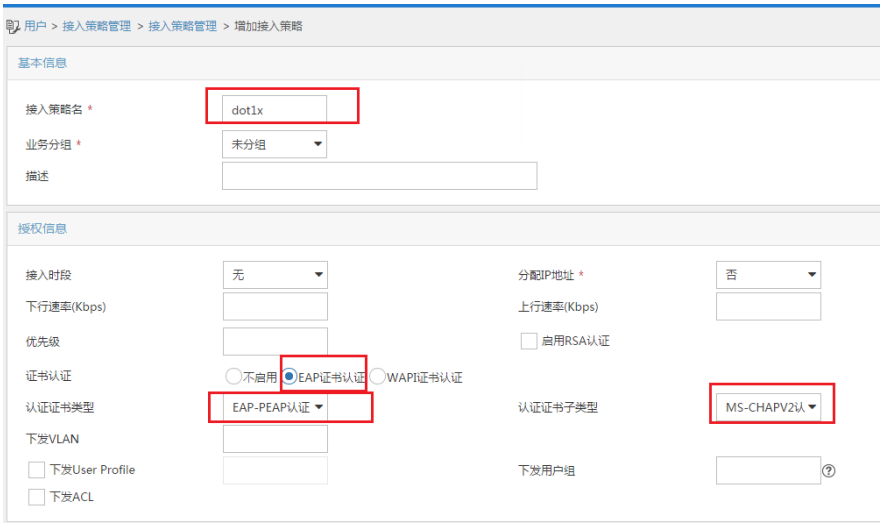
选择“用户”页签，单击导航树中的[接入策略管理/接入策略管理]菜单项，进入接入策略管理页面，在该页面中单击<增加>按钮，进入增加接入策略页面。

· 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



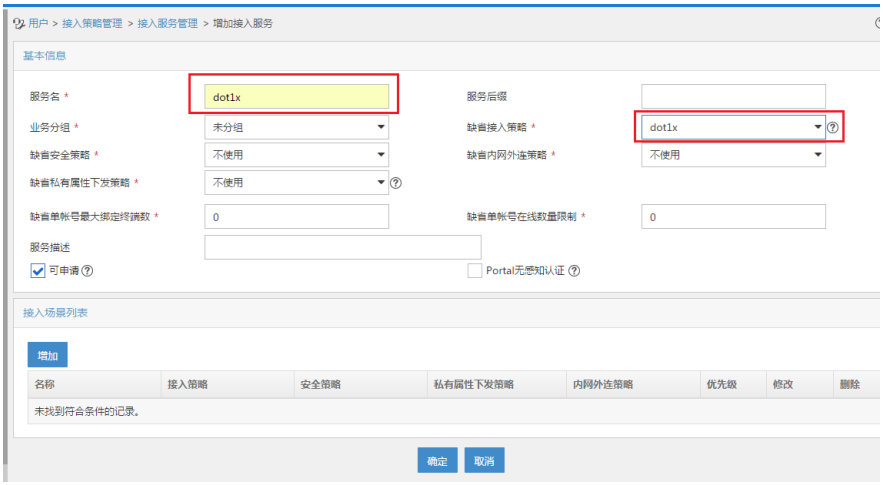
增加接入服务。

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

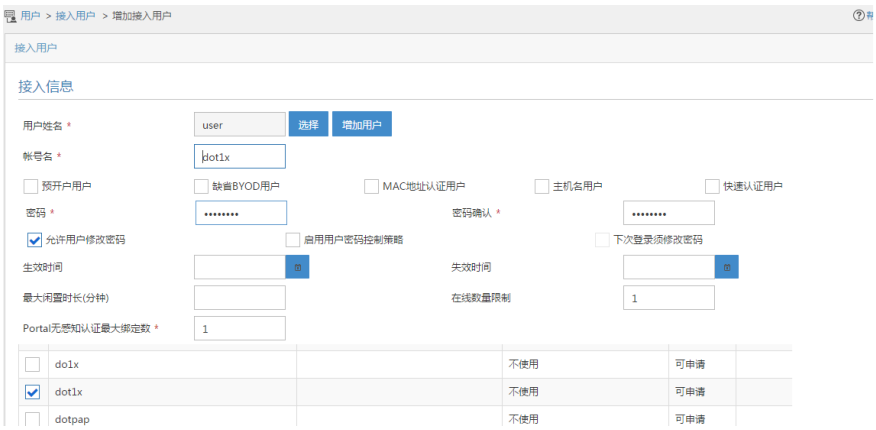


增加接入用户。

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



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

2.5 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 : 2002::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 : 2002::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

2.6 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 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
#
radius scheme radius1
 primary authentication ipv6 2003::2
 primary accounting ipv6 2003::2
 key authentication cipher $c$3$Nc0p9aAdEZsigfKkc+BNOVwr1StmtFHa
 key accounting cipher $c$3$1UiOGNVopIKWmUamDZBOpK2pSJ9+C7U5
 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::3
 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 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 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