H3C 无线控制器

本地 802.1X 认证+本地 MAC 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

本文档介绍本地 802.1X 和本地 MAC 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 MAC 地址认证、WLAN 接入、WLAN 用户接入认证和 802.1X 的相关特性。

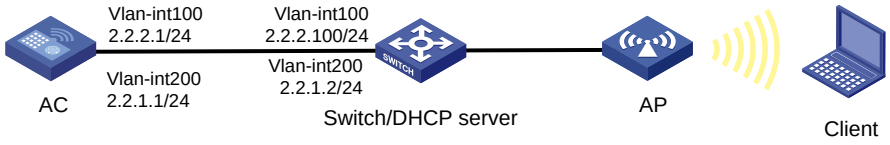
3 配置举例

3.1 组网需求

如 3.1 图 1 所示组网，Switch 通过 PoE 方式给 AP 供电，Switch 作为 DHCP server 为 AP 和 Client 分配 IP 地址，要求：

- 对无线用户先进行 MAC 地址认证，如果失败，再进行 802.1X 认证。如果认证成功，则不进行 802.1X 认证。
- 客户端链路层认证使用开放式系统认证。

图1 本地 802.1X+本地 MAC 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。
- 在 AC 上配置的 MAC 地址认证的用户名、密码需要与 Client 上配置的用户名、密码保持一致，即使用 Client 的 MAC 地址作为用户名和密码进行 MAC 地址认证。
- 目前，无线客户端只支持采用 iNode 智能客户端进行本地 802.1X 认证。

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 IP 地址。AP 将获取该 IP 地址与 AC 建立 CAPWAP 隧道。

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 2.2.2.1 24
[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] ip address 2.2.1.1 24
[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 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 100 200
[AC-GigabitEthernet1/0/1] quit
```

(2) 配置 802.1X 认证本地用户

配置 802.1X 认证本地用户，用户名为 localuser，密码为明文输入的 localpass。

```
[AC] local-user localuser class network
[AC-luser-network-localuser] password simple localpass
```

配置 802.1X 认证本地用户的服务类型为 lan-access。

```
[AC-luser-network-localuser] service-type lan-access
[AC-luser-network-localuser] quit
```

(3) 配置 MAC 认证本地用户

配置一个网络接入类的 MAC 认证本地用户，名称为客户端的 MAC 地址 3ca9f4144c20，密码为明文密码 3ca9f4144c20，并指定用户可以使用 lan-access 服务。

```
[AC] local-user 3ca9f4144c20 class network
[AC-luser-network-3ca9f4144c20] password simple 3ca9f4144c20
[AC-luser-network-3ca9f4144c20] service-type lan-access
[AC-luser-network-3ca9f4144c20] quit
```

(4) 配置本地 MAC 地址认证的用户名格式

配置 MAC 地址认证的用户名和密码均为用户的 MAC 地址。

```
[AC] mac-authentication user-name-format mac-address without-hyphen lowercase
```

(5) 配置 ISP 域

创建名为 bbb 的 ISP 域并进入其视图。

```
[AC] domain bbb
```

为 802.1X 和 MAC 认证用户配置 AAA 认证方法为本地认证、授权和计费。

```
[AC-isp-bbb] authentication lan-access local
[AC-isp-bbb] authorization lan-access local
[AC-isp-bbb] accounting lan-access local
[AC-isp-bbb] quit
```

(6) 配置 802.1X 认证

配置 802.1X 系统的认证方法为 CHAP。

```
[AC] dot1x authentication-method chap
```

(7) 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
```

配置用户接入认证模式为 mac-then-dot1x。

```
[AC-wlan-st-service] client-security authentication-mode mac-then-dot1x
```

配置 802.1X 用户使用认证域为 bbb。

```
[AC-wlan-st-service] dot1x domain bbb
```

配置 MAC 认证用户使用认证域为 bbb。

```
[AC-wlan-st-service] mac-authentication domain bbb
```

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 office，型号名称选择 WA4320i-ACN，并配置序列号 210235A1GQC158004457。

```
[AC] wlan ap office model WA4320i-ACN
[AC-wlan-ap-office] serial-id 210235A1GQC158004457
```

进入 Radio 1 视图。

```
[AC-wlan-ap-office] radio 1
```

将无线服务模板 service 绑定到 radio 1，并开启射频。

```
[AC-wlan-ap-office-radio-1] service-template service
[AC-wlan-ap-office-radio-1] radio enable
[AC-wlan-ap-office-radio-1] quit
[AC-wlan-ap-office] quit
```

3.3.2 配置Switch

开启 DHCP server 功能。

```
<Switch> system-view
[Switch] dhcp enable
```

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

```
[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 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 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 100 接口的 IP 地址。
```
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip address 2.2.2.100 255.255.255.0
[Switch-Vlan-interface100] quit
```
配置 VLAN 200 接口的 IP 地址。
```
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 2.2.1.2 255.255.255.0
[Switch-Vlan-interface200] quit
```
配置 DHCP 地址池 100，用于为 AP 分配 IP 地址。
```
[Switch] dhcp server ip-pool 100
[Switch-dhcp-pool-100] network 2.2.2.0 mask 255.255.255.0
[Switch-dhcp-pool-100] gateway-list 2.2.2.1
[Switch-dhcp-pool-100] quit
```
配置 DHCP 地址池 200，用于为 Client 分配 IP 地址，为 Client 分配的 DNS 服务器地址为网关地址（实际使用过程中请根据实际网络规划配置无线客户端的 DNS 服务器地址），网关地址为 2.2.1.1。
```
[Switch] dhcp server ip-pool 200
[Switch-dhcp-pool-200] network 2.2.1.0 mask 255.255.255.0
[Switch-dhcp-pool-200] gateway-list 2.2.1.1
[Switch-dhcp-pool-200] dns-list 2.2.1.1
[Switch-dhcp-pool-200] quit
```

3.3.3 配置iNode智能客户端

说明

下面以 iNode 为例（使用 iNode 版本为：iNode PC 7.1），说明本地 802.1x 认证中 iNode 的基本配置。

(1) 无线连接

打开 iNode 智能客户端，单击“无线连接”。

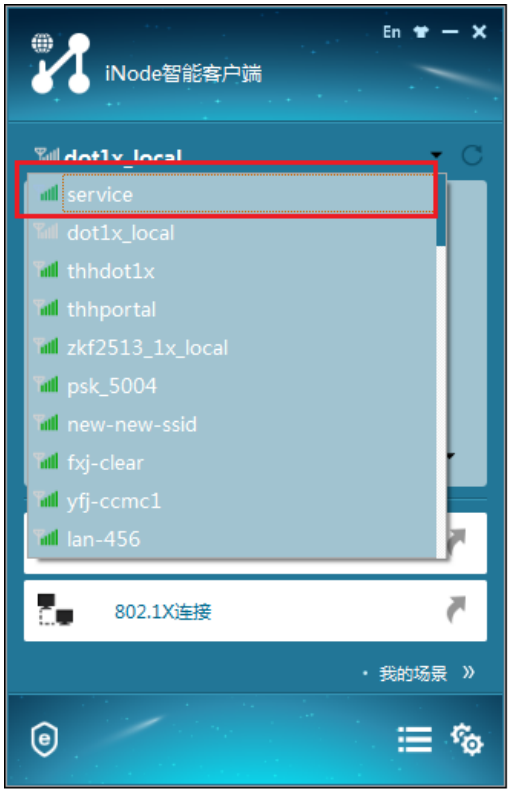
图2 打开 iNode 智能客户端

单击无线连接右上角的小三角按钮，显示可用的无线 SSID。

图3 无线连接

双击 SSID 为 service 的无线服务，进行无线网络连接。

图4 无线网络连接



单击窗口中的<连接>按钮，接入无线网络。

图5 无线网络连接

(2) 配置 802.1X 认证

无线连接成功后，单击“802.1X 连接”，进行 802.1X 认证。

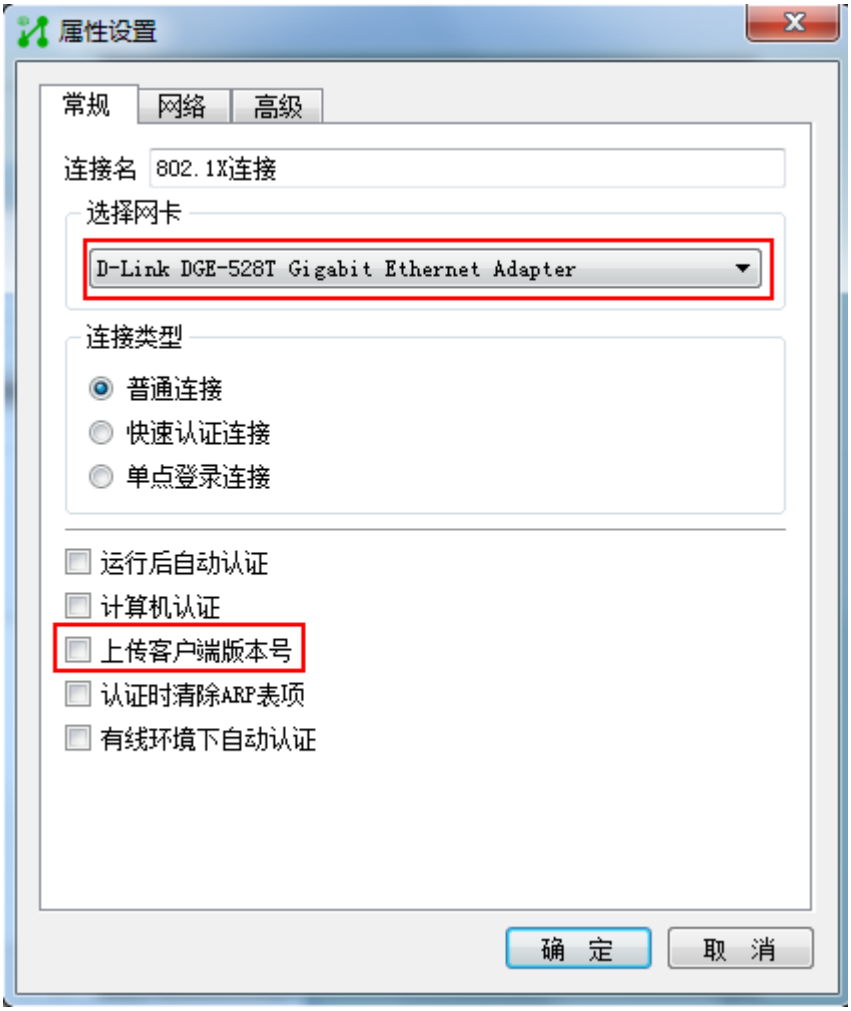
图6 802.1X 连接

输入用户名和密码，用户名和密码应与配置的本地认证用户名和密码相同。

图7 输入用户名和密码

单击“连接”右侧的倒三角，然后单击“属性”，进入属性设置对话框，选择当前使用的无线网卡，然后将“上传客户端版本号”前面的勾去掉，单击<确定>按钮。

图8 属性设置



最后，单击 802.1X 连接页面的<连接>按钮，即可进行 802.1X 认证。

图9 802.1X 认证成功

3.4 验证配置

当无线用户本地 MAC 认证不通过时，就会进行 802.1X 认证，通过 802.1X 认证成功并上线之后，AC 上可以通过 **display dot1x connection** 命令看到上线用户的连接情况。

```
[AC] display dot1x connection
User MAC address           : 0015-00bf-e84d
AP name                    : office
Radio ID                   : 1
SSID                       : service
BSSID                      : 741f-4ad4-1fe0
Username                   : localuser
Authentication domain      : bbb
IPv4 address               : 2.2.1.3
Authentication method      : CHAP
Initial VLAN               : 200
Authorization VLAN         : 200
Authorization ACL number   : N/A
Authorization user profile : N/A
Termination action         : N/A
Session timeout period     : N/A
Online from                : 2015/12/04 17:37:55
Online duration            : 0h 4m 20s
```

当本地 MAC 认证通过时，就不会进行本地 802.1X 认证，在 AC 上通过命令 **display wlan client** 可以看见无线用户 Clientt 从 VLAN 200 上线。

```
[AC] display wlan client
 Total Number of Clients           : 1

MAC address     Username       AP name     RID   IP address      IPv6 address   VLAN
3ca9-f414-4c20  3ca9f4144c20   office      1     2.2.1.3         N/A            200
```

3.5 配置文件

- AC：

```
#
vlan 100
#
vlan 200
#
wlan service-template service
 ssid service
 vlan 200
 client-security authentication-mode mac-then-dot1x
 dot1x domain bbb
mac-authentication domain bbb
 service-template enable
#
interface Vlan-interface100
 ip address 2.2.2.1 255.255.255.0
#
interface Vlan-interface200
 ip address 2.2.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 100 200
#
domain bbb
 authentication lan-access local
 authorization lan-access local
 accounting lan-access local
#
local-user localuser class network
 password cipher $c$3$+5Yra0KsaLci/RxEa4lyYKxxiw6jwMCcOg==
 service-type lan-access
#
local-user 3ca9f4144c20 class network
 password cipher $c$3$KWMkvq/FnQ2opPqBnpSTs3NPhVKrSOvqFPLAECSiDQ==
 service-type lan-access
#
```

```
wlan ap office model WA4320i-ACN
 serial-id 210235A1GQC158004457
 radio 1
  radio enable
  service-template service
#
```

- Switch：

```
#
 dhcp enable
#
vlan 100
#
vlan 200
#
dhcp server ip-pool 100
gateway-list 2.2.2.1
 network 2.2.2.0 mask 255.255.255.0
#
dhcp server ip-pool 200
gateway-list 2.2.1.1
 network 2.2.1.0 mask 255.255.255.0
dns-list 2.2.1.1
#
interface Vlan-interface100
 ip address 2.2.2.100 255.255.255.0
#
interface Vlan-interface200
 ip address 2.2.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 100 200
#
interface GigabitEthernet1/0/2
 port link-type access
 port access permit 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”