H3C无线控制器HTTPS登录典型配置举例(V7)

wlan接入 IP wlan安全 李晨光 2016-06-23 发表

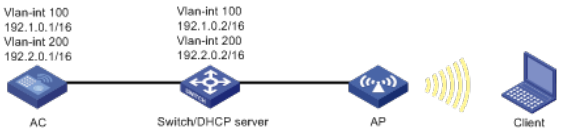
本文档介绍无线用户通过HTTPS登录AC设备的配置举例。

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、HTTPS方式登录设备等相关特性。

如图1所示，用户希望通过Web页面访问和控制AC。为了防止非法用户访问和控制设备，提高设备管理的安全性，要求无线用户以HTTPS的方式登录Web页面，利用SSL协议实现用户身份验证，并保证传输的数据不被窃听和篡改。本例中，Switch作为DHCP服务器，为AP和Client分配IP地址。AP与AC使用VLAN 100建立CAPWAP隧道，Client使用VLAN 200接入无线网络。



1.1 配置步骤

1.1.1 配置AC

(1) 配置AC的接口

创建VLAN 100及其对应的VLAN接口，并为该接口配置IP地址192.1.0.1/16。AP将获取该IP地址与AC建立CAPWAP隧道。

system-view

[AC] vlan 100

[AC-vlan100] quit

[AC] interface vlan-interface 100

[AC-Vlan-interface100] ip address 192.1.0.1 16

[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192.2.0.1/16。AC将使用该接口的IP地址和Client进行通信。

[AC] vlan 200

[AC-vlan200] quit

[AC] interface vlan-interface 200

[AC-Vlan-interface200] ip address 192.2.0.1 16

[AC-Vlan-interface200] quit

配置AC与Switch相连的接口GigabitEthernet 1/0/1的接口类型为Trunk，并允许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) 配置无线服务

创建无线服务模板1，并进入无线服务模板视图。

[AC] wlan service-template 1

配置SSID为service。

[AC-wlan-st-1] ssid service

配置无线服务模板的VLAN为200。

[AC-wlan-st-1] vlan 200

开启无线服务模板。

[AC-wlan-st-1] service-template enable

[AC-wlan-st-1] quit

(3) 配置AP

创建手工AP，配置AP名称为ap1，型号为WA4320-ACN，序列号为210235A1GUC158005091。

[AC] wlan ap ap1 model WA4320-ACN

[AC-wlan-ap-ap1] serial-id 210235A1GUC158005091

进入ap1的Radio 1视图，并将无线服务模板1绑定到Radio 1上。

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] service-template 1

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

(4) 配置通过HTTPS方式登录设备

创建PKI域1，并关闭CRL检查。（是否进行CRL检查，请以实际的使用需求为准）

[AC] pki domain 1

[AC-pki-domain-1] undo crl check enable

[AC-pki-domain-1] quit

向PKI域中导入CA证书，证书文件格式为PEM编码，证书文件名称为root.pem。

[AC] pki import domain 1 pem ca filename root.pem

向PKI域中导入本地证书，证书文件格式为PEM编码，证书文件名称为radius.pem。

[AC] pki import domain 1 pem local filename radius.pem

Please input the password:****

创建SSL服务器端策略myssl，指定该策略使用PKI域1。

[AC] ssl server-policy myssl

[AC-ssl-server-policy-myssl] pki-domain 1

[AC-ssl-server-policy-myssl] quit

配置HTTPS服务与SSL服务器端策略myssl关联。

[AC] ip https ssl-server-policy myssl

开启HTTPS服务

[AC] ip https enable

添加名称为usera的设备管理类本地用户，密码为123，服务类型为https，用户角色为network-admin。

[AC] local-user usera

[AC-luser-manage-usera] password simple 123

[AC-luser-manage-usera] service-type https

[AC-luser-manage-usera] authorization-attribute user-role network-admin

[AC-luser-manage-usera] quit

1.1.2 配置Switch

(1) 配置Switch的接口

创建VLAN 100及其对应的VLAN接口，并为该接口配置IP地址192.1.0.2/16。Switch将使用该接口的IP地址和AC进行通信。

system-view

[Switch] vlan 100

[Switch-vlan100] quit

[Switch] interface vlan-interface 100

[Switch-Vlan-interface100] ip address 192.1.0.2 16

[Switch-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192.2.0.2/16。Switch将使用该接口的IP地址和Client进行通信。

[Switch] vlan 200

[Switch-vlan200] quit

[Switch] interface vlan-interface 200

[Switch-Vlan-interface200] ip address 192.2.0.2 16

[Switch-Vlan-interface200] quit

配置Switch与AC相连的接口GE1/0/1的接口类型为Trunk，并允许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相连的接口GE1/0/2的接口类型为Trunk，缺省VLAN为VLAN100，并允许VLAN 100通过。

[Switch] interface gigabitethernet 1/0/2

[Switch-GigabitEthernet1/0/2] port link-type trunk

[Switch-GigabitEthernet1/0/2] port trunk pvid vlan 100

[Switch-GigabitEthernet1/0/2] port trunk permit vlan 100

开启接口GE1/0/2的PoE接口远程供电功能。

[Switch-GigabitEthernet1/0/2] poe enable

[Switch-GigabitEthernet1/0/2] quit

(2) 配置DHCP服务器

开启DHCP服务。

[Switch] dhcp enable

创建DHCP地址池100，为AP动态分配网段为192.1.0.0/16，网关为192.1.0.2的IP地址。

[Switch] dhcp server ip-pool 100

[Switch-dhcp-pool-100] network 192.1.0.0 16

[Switch-dhcp-pool-100] gateway-list 192.1.0.2

通过自定义选项的方式配置Option 43的内容，为AP指定AC的IP地址192.1.0.1，注意Option 43选项内容中最后四字节为c0010001（192.1.0.1），即为AC的IP地址。

[Switch-dhcp-pool-100] option 43 hex 8007000001c0010001

[Switch-dhcp-pool-100] quit

创建DHCP地址池200，为无线客户端动态分配网段为192.2.0.0/16，网关为192.2.0.2的IP地址。

[Switch] dhcp server ip-pool 200

[Switch-dhcp-pool-200] network 192.2.0.0 16

[Switch-dhcp-pool-200] gateway-list 192.2.0.2

[Switch-dhcp-pool-200] quit

1.2 验证配置

Client连接到无线网络后，打开IE浏览器，输入网址https://192.2.0.1进入登录页面。在登录页面，输入用户名usera，密码123进入AC的Web配置页面，实现对AC的访问和控制。

1.3 配置文件

- AC：

```
#
vlan 100
#
vlan 200
#
wlan service-template 1
 ssid service
 vlan 200
 service-template enable
#
interface Vlan-interface100
 ip address 192.1.0.1 255.255.0.0
#
interface Vlan-interface200
 ip address 192.2.0.1 255.255.0.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 100 200
#
local-user usera class manage
 password hash
$h$6$FOrfdnZ2QRORxu7o$OK/dcQ/N/S7m+zrhpyh+xDm2aerS7vvN8WwFVuhQuk8hdeFjDtqzPJthCen1ylElTkE7OqbCG5YhiRnjHtEr0g==
```

```
 service-type https
 authorization-attribute user-role network-admin
#
pki domain 1
 undo crl check enable
#
ssl server-policy myssl
 pki-domain 1
#
 ip https ssl-server-policy myssl
 ip https enable
#
wlan ap ap1 model WA4320-ACN
 serial-id 210235A1GUC158005091
 vlan 1
 radio 1
  radio enable
  service-template 1
#
```

- Switch：

```
#
 dhcp enable
#
vlan 100
#
vlan 200
#
interface Vlan-interface100
 ip address 192.1.0.2 255.255.0.0
#
interface Vlan-interface200
 ip address 192.2.0.2 255.255.0.0
#
dhcp server ip-pool 100
 network 192.1.0.0 mask 255.255.0.0
 gateway-list 192.1.0.2
 option 43 hex 8007000001C0010001
#
dhcp server ip-pool 200
 network 192.2.0.0 mask 255.255.0.0
 gateway-list 192.2.0.2
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 100 200
#
interface GigabitEthernet1/0/2
 poe enable
 port link-type trunk
 port trunk permit vlan 100
 port trunk pvid vlan 100
#
```

- 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。
- 本举例采用离线导入方式获取证书，需要提前将对应的证书通过FTP、TFTP等方式加载到设备上。证书中包含有效时间，请确保使用的证书在有效期内，以避免证书导入失败。