H3C 无线控制器

PSK 加密典型配置举例(V7)

资料版本：6W100-20191125

目录

1 简介

本文档介绍了 PSK 加密的典型配置举例。

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 WLAN 用户安全相关特性。

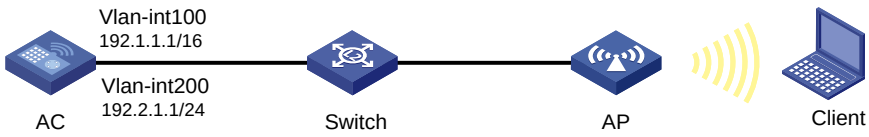
3 配置举例

3.1 组网需求

如图 1 所示，Switch 作为 DHCP 服务器为 AP 和 Client 分配 IP 地址。现要求：

- 在 AC 上配置 PSK 加密方式，使客户端通过该加密方式接入无线网络。
- 客户端链路层认证使用开放式系统认证，用户接入认证使用 Bypass 认证的方式实现客户端可以不需要认证直接接入 WLAN 网络的目的。
- 通过配置客户端和 AP 之间的数据报文采用 PSK 身份认证与密钥管理模式来确保用户数据的传输安全。
- 加密套件采用 CCMP。
- 安全信息元素采用 RSN。

图1 PSK 加密组网图



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。
- 配置身份认证与密钥管理模式为 PSK 模式时，必须配置 PSK 密钥。

3.3 配置步骤

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。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 192.1.1.1 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。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] ip address 192.2.1.1 24
[AC-Vlan-interface200] quit
```

配置 AC 和 Switch 相连的接口 GigabitEthernet1/0/1 为 Trunk 类型，禁止 VLAN 1 报文通过，允许 VLAN 100 和 VLAN 200 通过，当前 Trunk 口的 PVID 为 100。

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[AC-GigabitEthernet1/0/1] port trunk pvid vlan 100
[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
```

配置无线客户端上线后将被加入到 VLAN 200。

```
[AC-wlan-st-1] vlan 200
```

配置身份认证与密钥管理模式为 PSK 模式，配置 PSK 密钥为明文字符串 12345678。

```
[AC-wlan-st-1] akm mode psk
[AC-wlan-st-1] preshared-key pass-phrase simple 12345678
```

配置加密套件为 CCMP，安全信息元素为 RSN。

```
[AC-wlan-st-1] cipher-suite ccmp
[AC-wlan-st-1] security-ie rsn
```

使能无线服务模板。

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

(3) 配置 AP

创建手工 AP，名称为 officeap，型号名称为 WA4320i-ACN。

```
[AC] wlan ap officeap model WA4320i-ACN
```

设置 AP 序列号为 210235A1GQC152001076。

```
[AC-wlan-ap-officeap] serial-id 210235A1GQC152001076
```

进入 AP 的 Radio 2 视图，并将无线服务模板 1 绑定到 Radio 2 上。

```
[AC-wlan-ap-officeap] radio 2
[AC-wlan-ap-officeap-radio-2] service-template 1
```

开启 Radio 2 的射频功能。

```
[AC-wlan-ap-officeap-radio-2] radio enable
[AC-wlan-ap-officeap-radio-2] quit
[AC-wlan-ap-officeap] quit
```

2. 配置 Switch

(1) 配置 Switch 的接口

创建 VLAN 100 和 VLAN 200 及其对应接口，并为该接口配置 IP 地址，其中 VLAN 100 用于转发 AC 和 AP 间 CAPWAP 隧道内的流量，VLAN 200 用于转发 Client 无线报文。

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip address 192.1.1.2 16
[Switch-Vlan-interface100] quit
[Switch] vlan 200
[Switch-vlan200] quit
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 192.2.1.2 24
[Switch-Vlan-interface200] quit
```

配置 Switch 和 AC 相连的接口 GigabitEthernet1/0/1 为 Trunk 类型，禁止 VLAN 1 报文通过，允许 VLAN 100 和 VLAN 200 通过，当前 Trunk 口的 PVID 为 100。

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] quit
```

配置 Switch 和 AP 相连的接口 GigabitEthernet1/0/2 为 Trunk 类型，禁止 VLAN 1 报文通过，允许 VLAN 100 通过，当前 Trunk 口的 PVID 为 100。

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type trunk
[Switch-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[Switch-GigabitEthernet1/0/2] port trunk permit vlan 100
[Switch-GigabitEthernet1/0/2] port trunk pvid 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 DHCP 服务

开启 DHCP 功能。

```
[Switch] dhcp enable
```

创建名为 vlan100 的 DHCP 地址池，为 AP 分配 IP 地址，配置地址池动态分配的网段为 192.1.0.0/16，地址池中不参与自动分配的 IP 地址为 192.1.1.1，网关地址为 192.1.1.2。

```
[Switch] dhcp server ip-pool vlan100
[Switch-dhcp-pool-vlan100] network 192.1.0.0 mask 255.255.0.0
[Switch-dhcp-pool-vlan100] forbidden-ip 192.1.1.1
[Switch-dhcp-pool-vlan100] gateway-list 192.1.1.2
[Switch-dhcp-pool-vlan100] quit
```

创建名为 vlan200 的 DHCP 地址池，为 Client 分配 IP 地址，配置地址池动态分配的网段为 192.2.1.0/24，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），地址池中不参与自动分配的 IP 地址为 192.2.1.1，网关地址为 192.2.1.2。

```
[Switch] dhcp server ip-pool vlan200
[Switch-dhcp-pool-vlan200] network 192.2.1.0 mask 255.255.255.0
[Switch-dhcp-pool-vlan200] forbidden-ip 192.2.1.1
[Switch-dhcp-pool-vlan200] gateway-list 192.2.1.2
[Switch-dhcp-pool-vlan200] dns-list 192.2.1.2
[Switch-dhcp-pool-vlan200] quit
```

3.4 验证配置

在 AC 上使用 **display wlan client verbose** 命令可以看到 Client 通过 PSK 加密方式接入无线网络。

```
[AC] display wlan client verbose
Total number of clients: 1


MAC address                          : 0024-d705-c608
IPv4 address                         : 192.2.1.3
 IPv6 address                         : N/A
 Username                             : N/A
 AID                                  : 1
 AP ID                                : 2
 AP name                              : officeap
 Radio ID                             : 2
 SSID                                 : service
 BSSID                                : 80f6-2eaf-5190
 VLAN ID                              : 200
 Sleep count                          : 137
 Wireless mode                        : 802.11g
 Supported rates                      : 1, 2, 5.5, 6, 9, 11,
                                        12, 18, 24, 36, 48, 54 Mbps
QoS mode                             : WMM
 Listen interval                      : 100
 RSSI                                 : 20
 Rx/Tx rate                           : 2/1
```

```
 Authentication method             : Open system
 Security mode                     : PRE-RSNA
 AKM mode                          : N/A
Security mode                      : RSN
AKM mode                           : PSK
Cipher suite                       : CCMP
 User authentication mode          : Bypass
 Authorization ACL ID              : N/A
 Authorization user profile        : N/A
 Roam status                       : N/A
 Key derivation                    : N/A
 PMF status                        : N/A
 Forwarding policy name            : N/A
 Online time                       : 0days 0hours 21minutes 55seconds
 FT status                         : Inactive
```

3.5 配置文件

- AC：

```
#
vlan 100
#
vlan 200
#
wlan service-template 1
 ssid service
vlan 200
akm mode psk
 preshared-key pass-phrase cipher $c$3$N//5BVbsOqdBTxi+7MJZKT6Zqh5MAmYs2ZzM
 cipher-suite ccmp
 security-ie rsn
service-template enable
#
interface Vlan-interface100
 ip address 192.1.1.1 255.255.0.0
#
interface Vlan-interface200
 ip address 192.2.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 200
 port trunk pvid vlan 100
#
wlan ap officeap model WA4320i-ACN
 serial-id 210235A1GQC152001076
 radio 1
```

```
 radio 2
  radio enable
  service-template 1
#
```

- Switch

```
#
 dhcp enable
#
vlan 100
#
vlan 200
#
dhcp server ip-pool vlan100
 gateway-list 192.1.1.2
 network 192.1.0.0 mask 255.255.0.0
 forbidden-ip 192.1.1.1
#
dhcp server ip-pool vlan200
 gateway-list 192.2.1.2
 network 192.2.1.0 mask 255.255.255.0
 dns-list 192.2.1.2
 forbidden-ip 192.2.1.1
#
interface GigabitEthernet1/0/1
port link-type trunk
undo port trunk permit vlan 1
 port trunk permit vlan 100 200
 port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
port link-type trunk
undo port trunk permit vlan 1
 port trunk permit vlan 100
 port trunk pvid vlan 100
poe enable
#
```

4 相关资料

- 《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”。