H3C无线控制器PSK加密典型配置举例(V7)

wlan接入 wlan安全 李晨光 2016-07-06 发表

本文档介绍了PSK加密的典型配置举例。

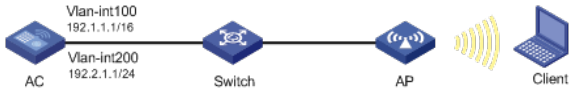
本文档适用于使用Comware V7软件版本的无线控制器和接入点产品，不严格与具体硬件版本对应，如果使用过程中与产品实际情况有差异，请参考相关产品手册，或以设备实际情况为准。

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接入和WLAN用户安全相关特性。

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。



1.1 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。

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。

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，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] quit

1.2 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

1.3 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
 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
#
```

- 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。