H3C WA 系列 PSK 认证典型配置举例

关键词：PSK

摘　要：随着无线网络应用的广泛普及，越来越多无线用户出现，使得无线安全问题凸显出来，PSK 认证可以实现利用共享密钥的方式对无线用户进行控制，对无线数据机密进行保护。

缩略语：

缩略语	英文全名	中文解释
PSK	Preshared Key	预共享密钥

目 录

1 特性简介

PSK（Preshared Key，预共享密钥）用来以预共享密钥的方式对无线用户的接入进行控制，并能够动态产生密钥保护无线局域网中的授权用户所交换的数据的机密性，防止这些数据被随机窃听。

2 应用场合

PSK 对无线报文的一种预共享密钥的认证方式和产生动态密钥对无线数据报文进行加密，该协议适用于接入设备与 Client 点到点的连接方式。通过预共享密钥的方式来进行认证。并产生动态密钥对数据进行加密。

3 配置举例

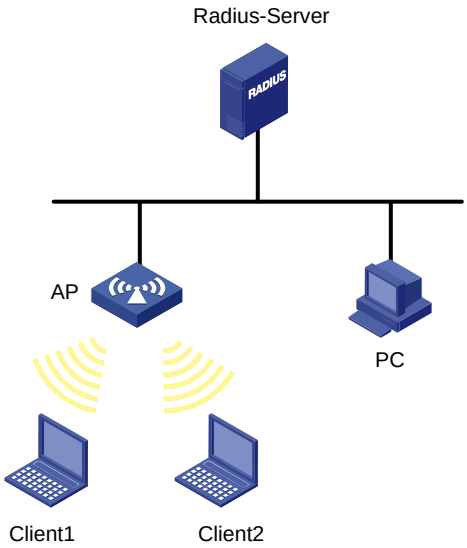
3.1 组网需求

说明

本配置举例中的 AP 使用的是 WA2200 无线局域网接入点。

本典型举例通过在 AP 的 WLAN-BSS 2 端口上启用 PSK 认证来达到对接入点 Client1 进行控制的目的。

图3-1 WA2200 PSK 认证组网图



3.2 配置思路

配置 PSK 认证，需要配置以下内容：

- 创建启用 PSK 认证的无线口；
- 创建启用 PSK 认证的服务模版；
- 在射频口把服务模板和无线口绑定。

3.3 使用版本

```
[AP]display version
H3C Comware Platform Software
Comware Software, Version 5.20, 0001
Copyright (c) 2004-2007 Hangzhou H3C Tech. Co., Ltd. All rights reserved.
WA2200 uptime is 0 week, 0 day, 16 hours, 48 minutes

 CPU type: AMCC PowerPC 266MHz
 64M bytes SDRAM Memory
 8M bytes Flash Memory
 Pcb             Version:  Ver.A
 Basic  BootROM  Version:  1.04
 Extend BootROM  Version:  1.04
 [SLOT  1]CON           (Hardware)Ver.A, (Driver)1.0
 [SLOT  1]RADIO1/0/1    (Hardware)Ver.A, (Driver)1.0
 [SLOT  1]RADIO1/0/1    (Hardware)Ver.A, (Driver)1.0
 [SLOT  1]ETH1/0/1      (Hardware)Ver.A, (Driver)1.0
 [SLOT  1]ETH1/0/2      (Hardware)Ver.A, (Driver)1.0
```

3.4 配置 AP PSK 认证

1. 配置文件

```
<AP>display current-configuration
#
 version 5.00, 0001
#
 sysname AP
#
 configure-user count 1
#
 domain default enable system
#
 port-security enable
#
vlan 1
#
vlan 2 to 4094
```

```
#
radius scheme system
 primary authentication 127.0.0.1
 primary accounting 127.0.0.1
 key authentication h3c
 key accounting h3c
 accounting-on enable
domain system
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#
wlan service-template 2 crypto
 ssid h3c-psk
 authentication-method open-system
 cipher-suite tkip
 security-ie wpa
 service-template enable
#
interface NULL0
#
interface Vlan-interface1
 ip address 192.168.1.50 255.255.255.0
#
interface Ethernet1/0/1
#
interface Ethernet1/0/2
#
interface WLAN-BSS2
 port-security port-mode psk
 port-security tx-key-type 11key
port-security preshared-key pass-phrase 12345678
#
interface WLAN-Radio1/0/1
#
interface WLAN-Radio1/0/2
 service-template 2 interface wlan-bss 2
#
 ip route-static 0.0.0.0 0.0.0.0 192.168.1.1
#
user-interface con 0
 idle-timeout 0 0
user-interface vty 0 4
#
return
```

2. 配置步骤

在 PSK 接入端（AP）配置 PSK

(1) 启用 port-security

```
[AP]port-security enable
```

(2) 配置无线接口，认证方式为 PSK

```
[AP]interface WLAN-BSS2
```

配置无线端口 WLAN-BSS2 的端口安全模式为 psk。

```
[AP-WLAN-BSS2]port-security port-mode psk
```

在接口 WLAN-BSS2 下使能 11key 类型的密钥协商功能。

```
[AP-WLAN-BSS2]port-security tx-key-type 11key
```

在接口 WLAN-BSS2 下配置预共享密钥为 12345678。

```
[AP-WLAN-BSS2]port-security preshared-key pass-phrase 12345678
```

(3) 配置无线服务模板

创建一个 crypto 类型的服务模板 2。

```
[AP-wlan-rp-rp]wlan service-template 2 crypto
```

设置服务模板 2 的 SSID 为 h3c-psk。

```
[AP-wlan-st-2]ssid h3c-psk
```

使能开放式系统认证。

```
[AP-wlan-st-2]authentication-method open-system
```

使能 TKIP 加密套件。

```
[AP-wlan-st-2] cipher-suite tkip
```

配置信标和探查帧携带 WPA IE 信息。

```
[AP-wlan-st-2] security-ie wpa
```

使能服务模板 2。

```
[AP-wlan-st-2]service-template enable
```

(4) 在射频口 WLAN-Radio 1/0/2 绑定无线服务模板 2 和无线口 WLAN-BSS 2。

```
[AP]interface WLAN-Radio 1/0/2
[AP-WLAN-Radio1/0/2]service-template 2 interface WLAN-BSS 2
```

(5) 配置 VLAN 虚接口。

```
[AP1]interface Vlan-interface1
[AP-Vlan-interface1]ip address 192.168.1.50 255.255.255.0
```

(6) 配置缺省路由

```
[AP-Vlan-interface1]ip route-static 0.0.0.0 0.0.0.0 192.168.1.1
```

3.5 验证结果

(1) 在配置错误预共享密钥的情况下，使用 Client1 访问 internet，有结果 1。

(2) 在配置正确预共享密钥的情况下，使用 Client1 访问 internet，有结果 2。

结果 1：Client1 不能访问 Internet 上的资源。

结果 2：Client1 可以成功关联，并且可以正常访问 internet 上的资源。

4 相关资料

4.1 相关协议和标准

表4-1 相关协议与标准

标准号	标题
IEEE 802.11i	802.11i IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements

4.2 其它相关资料

- 《H3C WA 系列无线接入点设备 用户手册》“WLAN 分册”中的“WLAN”。
- 《H3C WA 系列无线接入点设备 用户手册》“安全分册”中的“端口安全”。