

无线PSK认证问题排查



一、开始

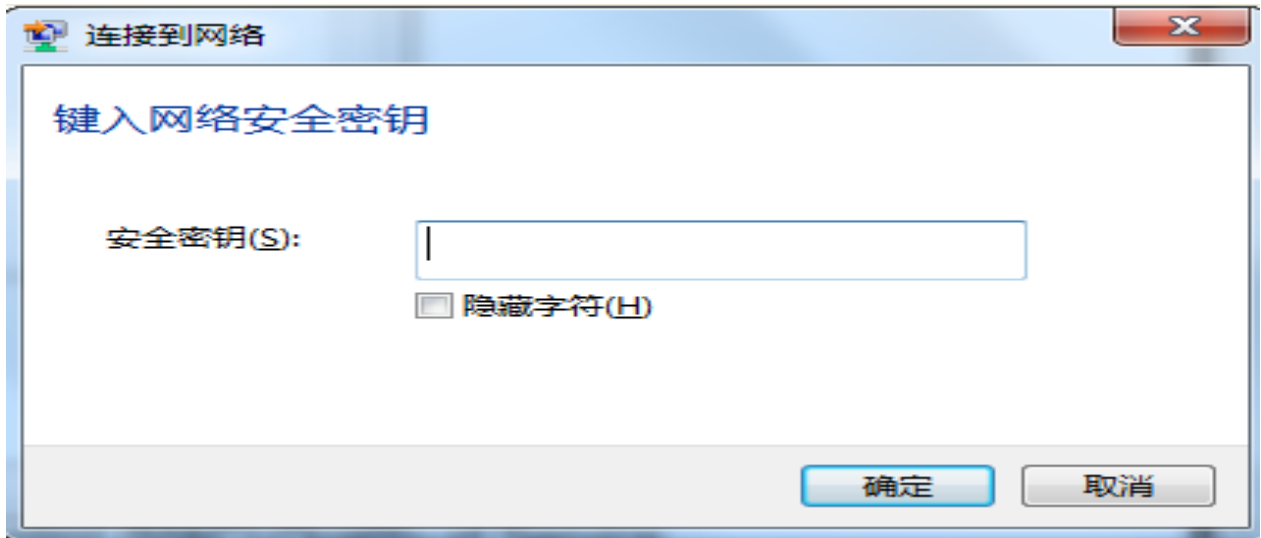
无线PSK（Pre-Shared Key，预共享密钥）认证问题排查的思路是：首先需要实现在无线客户

版权所有：杭州华三通信技术有限公司

端和设备端配置相同的预共享密钥，如果密钥相同，PSK接入认证成功；如果密钥不同，PSK接入认证失败。

1、连接SSID是否显示密码输入页面

如果正确配置了PSK认证，终端连接SSID会显示密钥输入页面，如图分别为win7和IOS的终端密钥输入页面。





2、检查ESS口配置

检查ESS接口是否使能端口安全模式为PSK、使能11key类型的密钥协商功能并设置秘钥。

```
[AC-WLAN-ESS2]display this
#
interface WLAN-ESS2
 port access vlan 2
 port-security port-mode psk //使能端口安全模式为 PSK
 port-security tx-key-type 11key //使能 11key 类型的密钥协商功能
 port-security preshared-key pass-phrase cipher
 $c$3$SHcJ950t8GUuMW7zb96l75T9lwDNjtFzbJ43 //设置密钥
#
```

PSK用户是指通过

preSharedKey安全模式认证上线的用户。不同端口安全模式下，端口可允许接入的最大用户数受到不同的限制，具体情况如下：

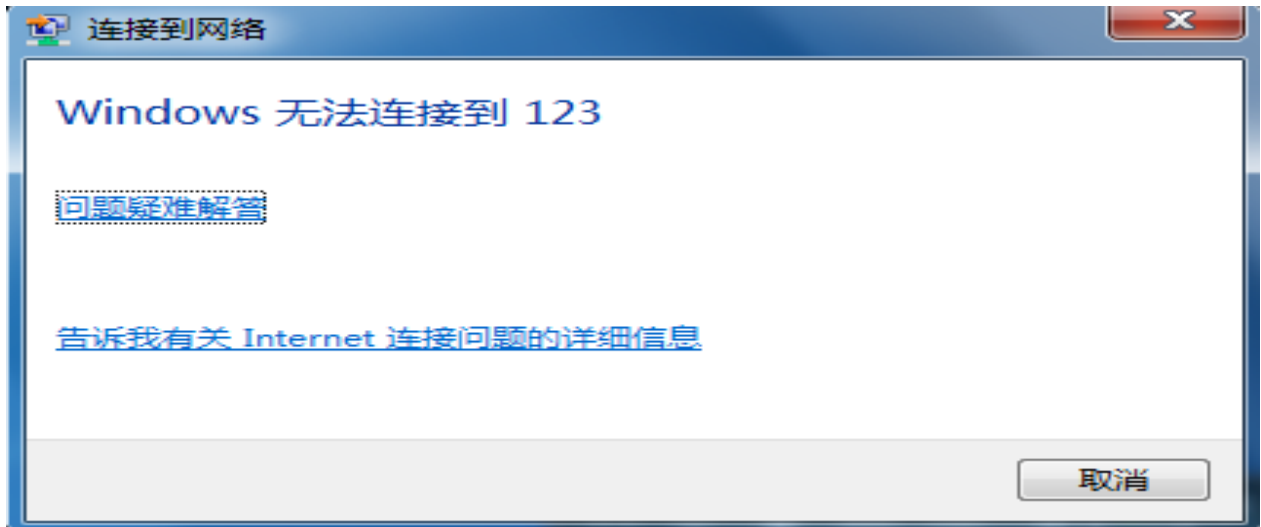
- preSharedKey模式下，单个端口上允许的最大PSK用户数由无线接口可支持的最大用户数决定，如果端口上还设置了端口安全所允许的最大MAC地址数，则端口上的最大 PSK 用户数取两者的最小值。
- macAddressAndPresharedKey模式下，系统所允许的认证用户总数及单个端口上的最大用户数受MAC地址认证接入用户数限制，如果端口上还设置了端口安全所允许的最大 MAC地址数，则端口上的最大用户数取两者的最小值。
- userLoginSecureExtOrPresharedKey模式下，单个端口以及系统所允许的最大PSK用户数限制与preSharedKey模式同；系统所允许的802.1X认证用户总数及单个端口上的用户数受802.1X认证接入用户数限制；此外，如果端口上还设置了端口安全所允许的最大MAC地址数，则允许的PSK用户数及802.1X认证用户数之和不能超过该限制。

3、密钥是否一致

PSK接入用户必须使用设备上预先配置的静态密钥，即PSK（Pre-Shared

Key，预共享密钥）与设备进行协商，协商成功后可访问端口；终端在

密码输入页面输入密钥后，若提示密码不正确，则无法接入无线服务，如图分别为win7和IOS的终端密码错误显示。





4、重置密钥

重新配置预共享密钥秘钥：

```
[AC-WLAN-ESS2]port-security preshared-key ?  
  pass-phrase  Specify port preshare phrase key //以字符串方式设置预共享密钥  
  raw-key      Specify port preshare raw key //以十六进制方式设置预共享密钥  
[AC-WLAN-ESS2]port-security preshared-key pass-phrase 12345678
```

cipher: 以密文方式设置密钥。

simple: 以明文方式设置密钥。

以明文或密文方式设置的共享密钥，均以密文的方式保存在配置文件中。设置的明文密钥或密文密钥，区分大小写。明文密钥为8~63个字符的字符串或者长度为64位的合法十六进制数；密文密钥为8~117个字符的字符串。不指定cipher或simple时，表示以明文方式设置共享密钥。

5、检查WIDS黑白名单配置

查看AC是否配置了WIDS功能，如果配置了则需要注意：

- (1) 配置黑名单中的用户，不能接入无线网络。
- (2) 配置白名单后，非名单内的用户不能接入无线网络。
- (3) 同时配置黑白名单后，先检查白名单，只有白名单内的用户能接入，再检查黑名单，黑名单内的用户不能接入。

display current-configuration

例如：通过命令查看是否有黑白名单相关的配置。

```
[AC] display current-configuration
#
wlan ids
  static-blacklist mac-address 2477-0390-c7c0
#
```

6、收集log、trap及debugging信息

注意：开启debug之前，请检查CPU和内存的使用情况，确保开启debug不会影响设备的正常运行。收集完信息后请及时关闭debug。

(1) 当AC在线用户数少于或等于100时，建议用下面的命令收集信息并使用调试开关进行调试：

```
display logbuffer
```

```
debugging wlan mac all
```

```
terminal monitor
```

```
terminal debugging
```

(2) 当AC在线用户数超过100时，建议等业务闲时关联用户数下降到100以下，再执行上述操作。

请拨打热线400-810-0504