

WPA 配置范例

介绍

本文档提供一个简单的 WPA 配置范例，WPA 是 Wi-Fi 联盟使用的过渡期安全标准

首要条件

需求

在进行配置前，请先满足下列要求：

- (1) 具备无线网络和无线安全问题的知识
- (2) 具备可扩展的认证协议 (EAP) 工作模式的知识

组件构成

在此文档中使用下列软件和硬件版本：

- (1) 基于思科 IOS 的 AP
- (2) 软件版本 12.2 (15) JA 或者以后

【译者注】：尽量使用最新的 IOS 软件，尽管 WPA 也被支持在 12.2 (11) JA，获得更多 IOS 版本软件，请访问以下网址：

http://www.cisco.com/en/US/products/hw/wireless/ps4570/products_configuration_example09_186a00801c40b6.shtml

- (3) 使用支持 WPA 的无线网卡，以及相应的无线客户软件

此文档相关信息都是在实验环境下验证，所有设备都是初始配置，如果在现网下进行配置，请确认理解已使用配置命令的潜在影响。

知识点

WEP 是不安全脆弱的无线加密方式，无线联盟组织（WECA）提出了下一代的无线网络安全方式，并提出了 802.11i 的标准。

新框架建立在使用 EAP 做认证的 802.1x 协议上，通过动态密钥管理的方式提供增强的加密方式，一旦客户端与认证服务器经过 802.1x 认证后，WPA 加密密钥会自动在客户端和服务端之间动态生成。

思科 AP 也提供混合模式的配置方式，以支持基于 WEP 加密的 EAP 客户端，此配置谈论到的过渡模式，是为了向 WPA 转型。本文档暂不涉及到这方面的内容。

WPA 还可以使用 Pre-Shared Key(WPA-PSK)的认证方式，支持小型办公环境、SOHO 和家庭环境中，思科 ACU 客户软件不支持(WPA-PSK)的认证模式，微软的无线客户端支持 PSK 的认证方式，下列软件同样也支持 WPA-PSK：

(1) Meetinghouse 的 AEGIS 客户端

【译者注】：请参考 Meetinghouse 的解决方案

<http://www.mtghouse.com/solutions/index.asp>

(2) Funk 的 Odyssey 客户端

【译者注】：请参考 Juniper 解决方案

<http://www.juniper.net/customers/support/products/oac.jsp>

(3) 其他厂商（OEM）的客户端

可以在以下情况下配置 WPA-PSK 模式：

(1) 使用 TKIP 做加密

(2) 定义 pre-shared key 的认证方式

(3) 不需要配置认证服务器

通过命令行方式配置以上内容：

```
AP(config)#interface dot11Radio 0
```

```
AP(config-if)#encryption mode ciphers tkip
```

```
AP(config-if)#ssid ssid_name
```

```
AP(config-if-ssid)#authentication open
```

```
AP(config-if-ssid)#authentication key-management wpa
```

```
AP(config-if-ssid)#wpa-psk ascii pre-shared_key
```

【译者注】：以上部分只是解释如何配置 WPA-PSK

使用惯例

请参考以下网址：

http://www.cisco.com/en/US/tech/tk801/tk36/technologies_tech_note09186a0080121ac5.shtml

配置

WPA 基于 EAP 的 802.1x 认证方法。此文档假定使用 Light EAP (LEAP), EAP, or Protected EAP (PEAP) 的认证方式实现 WPA。

文档中会详细描述配置步骤

【译者注】： 通过以下网址获得更多信息

<http://www.cisco.com/cgi-bin/Support/Commandlookup/home.pl>

网络 EAP 或者开放的 EAP 认证

在任何基于 EAP 的 802.1x 的认证方法，网络 EAP 与开放的 EAP 有所不同，通过查看管理和关联数据包头的认证算法域的值来体现。大多数无线客户端使用开放的 EAP 认证（此域的值为 0），然后进行 EAP 的认证过程，思科通过设置网络 EAP 标志的不同数值做认证。

可以使用以下认证类型：

- （1） 思科客户端：使用网络 EAP
- （2） 第三方客户端（包括支持 CCX 计划的客户端）：使用开放的 EAP
- （3） 思科和第三方客户端的组合：可以使用网络 EAP 和开放的 EAP

CLI 配置

此文档使用以下配置：

- （1） LEAP 的配置
- （2） 基于 12.2(15)JA 的思科无线 AP

AP

```
ap1#show running-config
Building configuration...

.
.
.
aaa new-model
!
aaa group server radius rad_eap
server 192.168.2.100 auth-port 1645 acct-port 1646
.
.
aaa authentication login eap_methods group rad_eap
.
.
.
!
bridge irb
!
interface Dot11Radio0
no ip address
no ip route-cache
!
encryption mode ciphers tkip

!--- This defines the cipher method that WPA uses. The TKIP
!method is the most secure, with use of the Wi-Fi-defined version of TKIP.

!
ssid WPAlabap1200
authentication open eap eap_methods

!--- This defines the method for the underlying EAP when third-party clients
!are in use.

authentication network-eap eap_methods

!--- This defines the method for the underlying EAP when Cisco clients are
!in use.

authentication key-management wpa
```

!-- This engages WPA key management.

```
!  
speed basic-1.0 basic-2.0 basic-5.5 basic-11.0  
rts threshold 2312  
channel 2437  
station-role root  
bridge-group 1  
bridge-group 1 subscriber-loop-control  
bridge-group 1 block-unknown-source  
no bridge-group 1 source-learning  
no bridge-group 1 unicast-flooding  
bridge-group 1 spanning-disabled
```

```
.  
. .
```

```
interface FastEthernet0  
no ip address  
no ip route-cache  
duplex auto  
speed auto  
bridge-group 1  
no bridge-group 1 source-learning  
bridge-group 1 spanning-disabled  
!  
interface BVI1  
ip address 192.168.2.108 255.255.255.0
```

!-- This is the address of this unit.

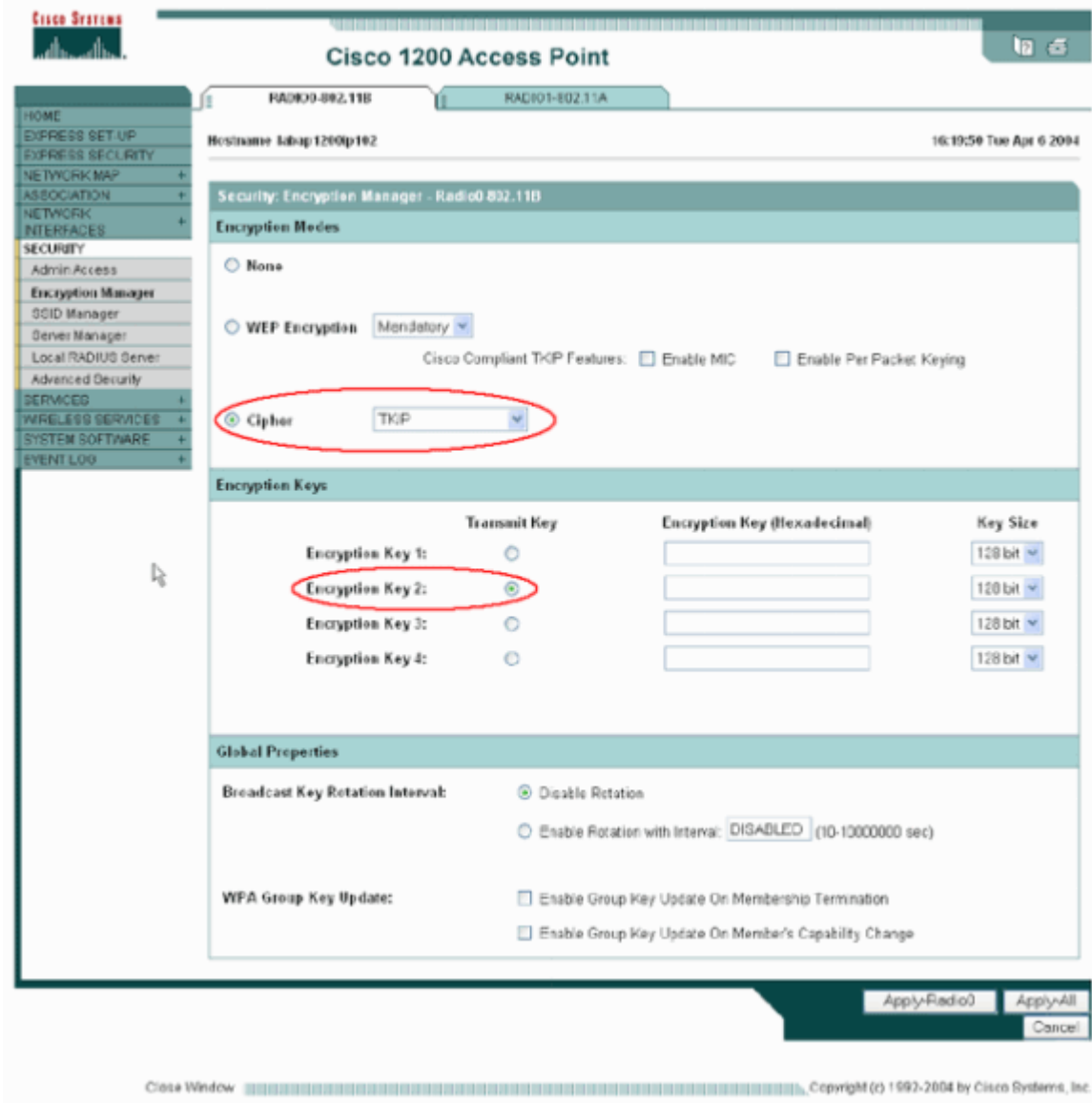
```
no ip route-cache  
!  
ip default-gateway 192.168.2.1  
ip http server  
ip http help-path  
http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag/ivory/1100  
ip radius source-interface BVI1  
snmp-server community cable RO  
snmp-server enable traps tty  
radius-server host 192.168.2.100 auth-port 1645 acct-port 1646 key  
shared_secret
```

!-- This defines where the RADIUS server is and the key between the AP and server.

```
radius-server retransmit 3
radius-server attribute 32 include-in-access-req format %h
radius-server authorization permit missing Service-Type
radius-server vsa send accounting
bridge 1 route ip
!
!
line con 0
line vty 5 15
!
end
!
end
```

图形配置模式

1. 配置加密管理
 - A. 打开 T K I P 加密
 - B. 在加密 1 中清空
 - C. 设置加密 2 中的密钥
 - D. 点击 **Apply-Radio#**.



2. 设置 SSID

A. 选择 SSID 选项

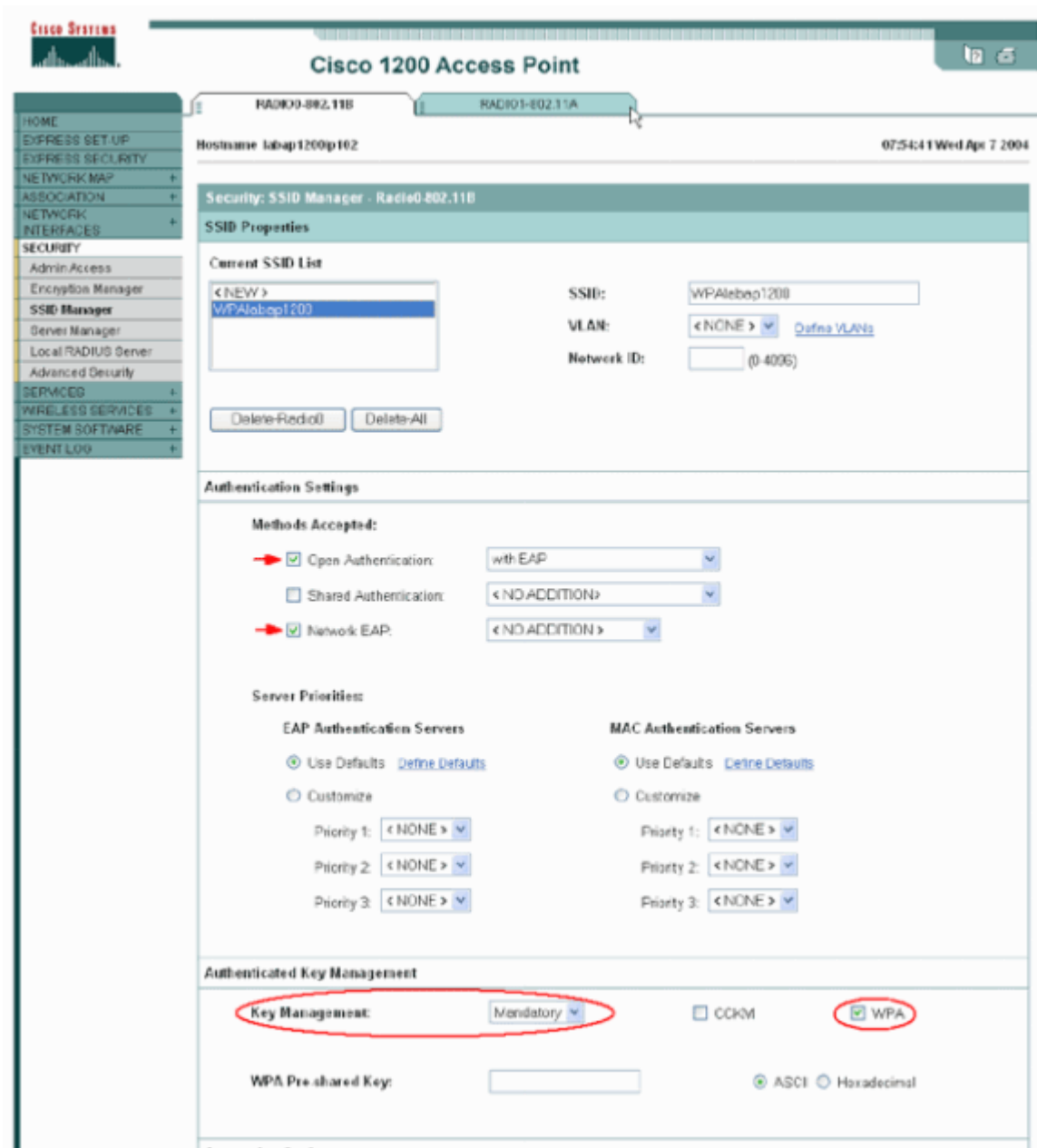
B. 选择认证方法

取决于所使用的无线网卡，参考

[HTTP://WWW.CISCO.COM/EN/US/PRODUCTS/HW/WIRELESS/PS4570/PRODUCTS_CONFIGURATION_EXAMPLE09186A00801C40B6.SHTML#NETEAP](http://www.cisco.com/en/US/products/hw/wireless/ps4570/products_configuration_example09186a00801c40b6.shtml#NETEAP)

C. 开启密钥管理

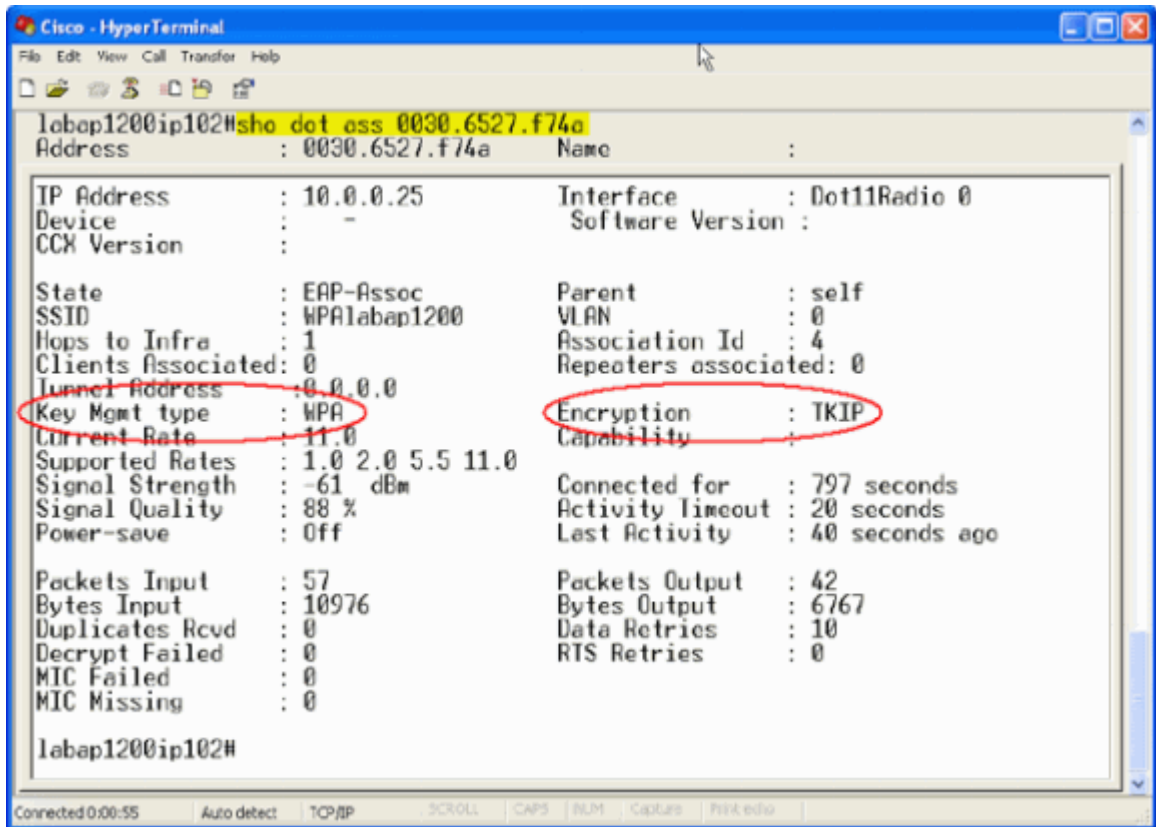
D. 应用 APPLY-RADIO#



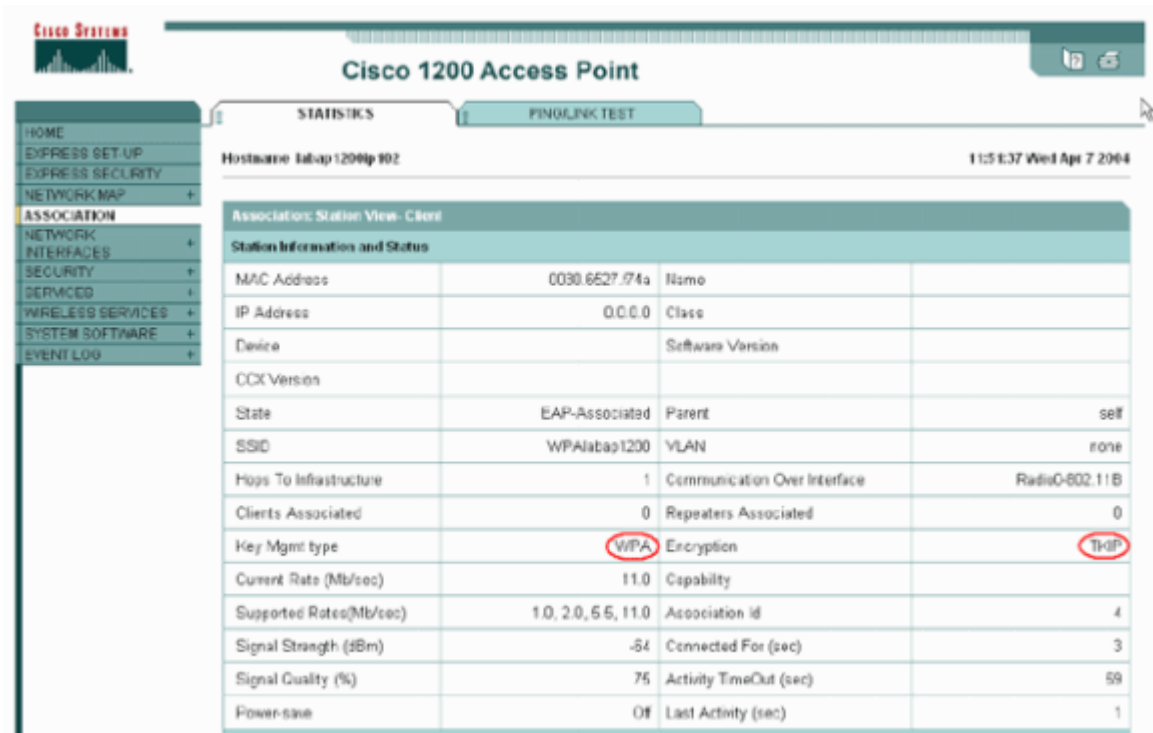
检测

使用以下方法验证配置

- (1) 通过 `show dot11 association mac_address` 命令查看连接状态



(2) 通过图形化界面查看 W P A 密钥管理以及 T K I P



排错

使用以下方式进行排错

排错过程

通过以下方式进行

(1) 如果没有完成 LEAP, EAP, or PEAP 的配置:

- A. 临时关闭 W P A 加密模式
- B. 重新开启 E A P
- C. 确定认证状态

(2) 检测客户端配置

确定客户端的配置是否和 A P 配置相同

排错命令

【译者注】: 在 d e b u g 前, 请参考以下网址

http://www.cisco.com/en/US/tech/tk801/tk379/technologies_tech_note09186a008017874c.shtml

W P A 密钥是在 E A P 认证后通过四次握手完成, 可以通过 d e b u g 查看, 如果 E A P 没有完成认证, 请查看以下状态:

- 1. 临时关闭 W P A
- 2. 重新开启 E A P
- 3. 确定认证

以下显示 d e b u g 信息

(1) 通过 **debug dot11 aaa manager keys** 命令查看密钥协商过程

```
debug dot11 aaa manager keys
```

```
labapl200ip102#
Apr  7 16:29:57.908: dot11_dot1x_build_ptk_handshake: building PTK msg
1 for
0030.6527.f74a
Apr  7 16:29:59.190: dot11_dot1x_verify_ptk_handshake: verifying PTK
msg 2 from
0030.6527.f74a
Apr  7 16:29:59.191: dot11_dot1x_verify_eapol_header: Warning: Invalid
key info
(exp=0x381, act=0x109)
Apr  7 16:29:59.191: dot11_dot1x_verify_eapol_header: Warning: Invalid
key len
(exp=0x20, act=0x0)
Apr  7 16:29:59.192: dot11_dot1x_build_ptk_handshake: building PTK msg
3 for
0030.6527.f74a
Apr  7 16:29:59.783: dot11_dot1x_verify_ptk_handshake: verifying PTK
msg 4 from
0030.6527.f74a
Apr  7 16:29:59.783: dot11_dot1x_verify_eapol_header: Warning: Invalid
key info
(exp=0x381, act=0x109)
Apr  7 16:29:59.783: dot11_dot1x_verify_eapol_header: Warning: Invalid
key len
(exp=0x20, act=0x0)
Apr  7 16:29:59.788: dot11_dot1x_build_gtk_handshake: building GTK msg
1 for
0030.6527.f74a
Apr  7 16:29:59.788: dot11_dot1x_build_gtk_handshake:
dot11_dot1x_get_multicast_key
len 32 index 1
Apr  7 16:29:59.788: dot11_dot1x_hex_dump: GTK: 27 CA 88 7D 03 D9 C4 61
FD 4B BE 71
EC F7 43 B5 82 93 57 83
Apr  7 16:30:01.633: dot11_dot1x_verify_gtk_handshake: verifying GTK
msg 2 from
0030.6527.f74a
Apr  7 16:30:01.633: dot11_dot1x_verify_eapol_header: Warning: Invalid
key info
(exp=0x391, act=0x301)
Apr  7 16:30:01.633: dot11_dot1x_verify_eapol_header: Warning: Invalid
key len
(exp=0x20, act=0x0)
Apr  7 16:30:01.633: %DOT11-6-ASSOC: Interface Dot11Radio0, Station
```

```
0030.6527.f74a
Associated KEY_MGMT[WPA]
labap1200ip102#
```

如果没有 `debug` 输出，请查看

- (1) 是否开启 `term mo`
- (2) 是否开启 `debug`
- (3) 客户端是否连接到 AP

如果看到 PTK 和 GTK 的协商过程，但是无法验证，请升级相应的客户端无线版本

- (1) 通过 `debug dot11 aaa authenticator state-machine` 命令查看客户端和 AP 的各种协商状态，在 12.2 (15) JA 及以后，使用 `debug dot11 aaa dot1x state-machine`
- (2) 通过 `debug dot11 aaa dot1x state-machine` 查看所有客户端和 AP 的各种认证，以及通过 AP 的状态情况
- (3) 通过 `debug dot11 aaa authenticator process` 查看各种协商问题，显示客户端的请求及回复，也可以使用 `debug radius authentication` 查看
- (4) 通过 `debug dot11 aaa dot1x process` 查看认证过程