WPA 配置概述

目录

简介

本文档提供了 Wi-Fi 保护访问 (WPA) 的示例配置，这是 Wi-Fi 联盟成员使用的一种临时安全标准。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 全面了解无线网络和无线安全问题
- 了解可扩展身份验证协议 (EAP) 安全方法

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 基于 Cisco IOS® 软件的接入点 (AP)
- Cisco IOS 软件版本 12.2(15)JA 或更高版本**注意：**最好使用最新的Cisco IOS软件版本，即使Cisco IOS软件版本12.2(11)JA及更高版本支持WPA。要获取最新版本的 Cisco IOS 软件，请参阅下载（仅限注册用户）。
- 与 WPA 兼容的网络接口卡 (NIC) 以及与 WPA 兼容的相应客户端软件

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景理论

无线网络中的安全功能（例如 WEP）较弱。Wi-Fi 联盟（即 WECA）行业组织设计了用于无线网络的下一代临时安全标准。在 IEEE 组织正式批准 802.11i 标准之间，此标准将暂时对安全缺陷提供防御。

这种新的方案建立在当前EAP/802.1x认证和动态密钥管理上，并添加更严格的密码加密。在客户端设备与身份验证服务器建立 EAP/802.1x 关联后，AP 和 WPA 兼容客户端设备之间会对 WPA 密钥管理进行协商。

Cisco AP 产品还提供了混合配置，在这种配置中，两种传统的基于 WEP 的 EAP 客户端（带有传统密钥管理或无密钥管理）都可以与 WPA 客户端配合使用。这种配置称为迁移模式。通过迁移模式可采用分阶段的方法迁移到 WPA。本文档不讨论迁移模式，仅对纯 WPA 保护网络进行概述。

除了考虑到企业或公司级别的安全问题之外，WPA 还提供了用于小型办公室、家庭办公 (SOHO) 或家庭无线网络的预共享密钥版本 (WPA-PSK)。Cisco Aironet 客户端实用程序 (ACU) 不支持 WPA-PSK。Microsoft Windows 无线零配置实用程序支持大多数无线网卡的 WPA-PSK，以下实用程序也同样如此：

- Meetinghouse Communications 的 AEGIS Client**注意：**有关Meetinghouse AEGIS产品线，请参阅EOS和EOL公告。
- Funk Software 的 Odyssey 客户端**注意：请**参阅Juniper Networks客户支持中心 。
- 一些制造商提供的原始设备制造商 (OEM) 客户端实用程序

在以下情形中，您可以配置 WPA-PSK：

- 您在 Encryption Manager 选项卡中将加密模式定义为密码临时密钥完整性协议 (TKIP)。
- 您在 GUI 的 Service Set Identifier (SSID) Manager 选项卡上定义身份验证类型、身份验证密钥管理的使用以及预共享密钥。
- 无需在 Server Manager 选项卡上进行配置。

要通过命令行界面 (CLI) 启用 WPA-PSK，请输入以下命令。从配置模式开始：

```
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
```

注意：本节仅提供与WPA-PSK相关的配置。本部分提供的配置只是为了让您了解如何启用 WPA-PSK，并非本文档的重点内容。本文档解释了如何配置 WPA。

规则

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

配置

WPA 基于当前的 EAP/802.1x 方法。本文档假定您在添加配置以启用 WPA 之前就已经拥有已生效的轻量 EAP (LEAP)、EAP 或受保护的 EAP (PEAP) 配置。

此部分存在信息配置在本文描述的功能中。

注意：使用命令查找工具(仅限注册客户)可获取有关本节中使用的命令的详细信息。

网络 EAP 或采用 EAP 的开放式身份验证

在基于 EAP/802.1x 的身份验证方法中，您可能会问网络 EAP 和采用 EAP 的开放式身份验证之间有何区别。这些项目参考了管理和关联信息包报头中认证算法字段中的数值。大多数无线客户端制造商将该字段的值设置为 0（开放式身份验证），然后传达他们的期望值，以便在关联过程后期进行 EAP 身份验证。Cisco 对该值的设置有所不同（从与网络 EAP 标志的关联开始时）。

如果您的网络客户端为以下类型，请使用下面相应列出的身份验证方法：

- Cisco 客户端 - 使用网络 EAP。
- 第三方客户端（包括与 Cisco Compatible Extensions [CCX] 兼容的产品）- 使用采用 EAP 的开放式身份验证。
- Cisco 客户端与第三方客户端的组合 - 同时选择网络 EAP 和采用 EAP 的开放式身份验证。

CLI 配置

本文档使用以下配置：

- 已经存在且有效的 LEAP 配置
- Cisco IOS 软件版本 12.2(15)JA（适用于基于 Cisco IOS 软件的 AP）

AP

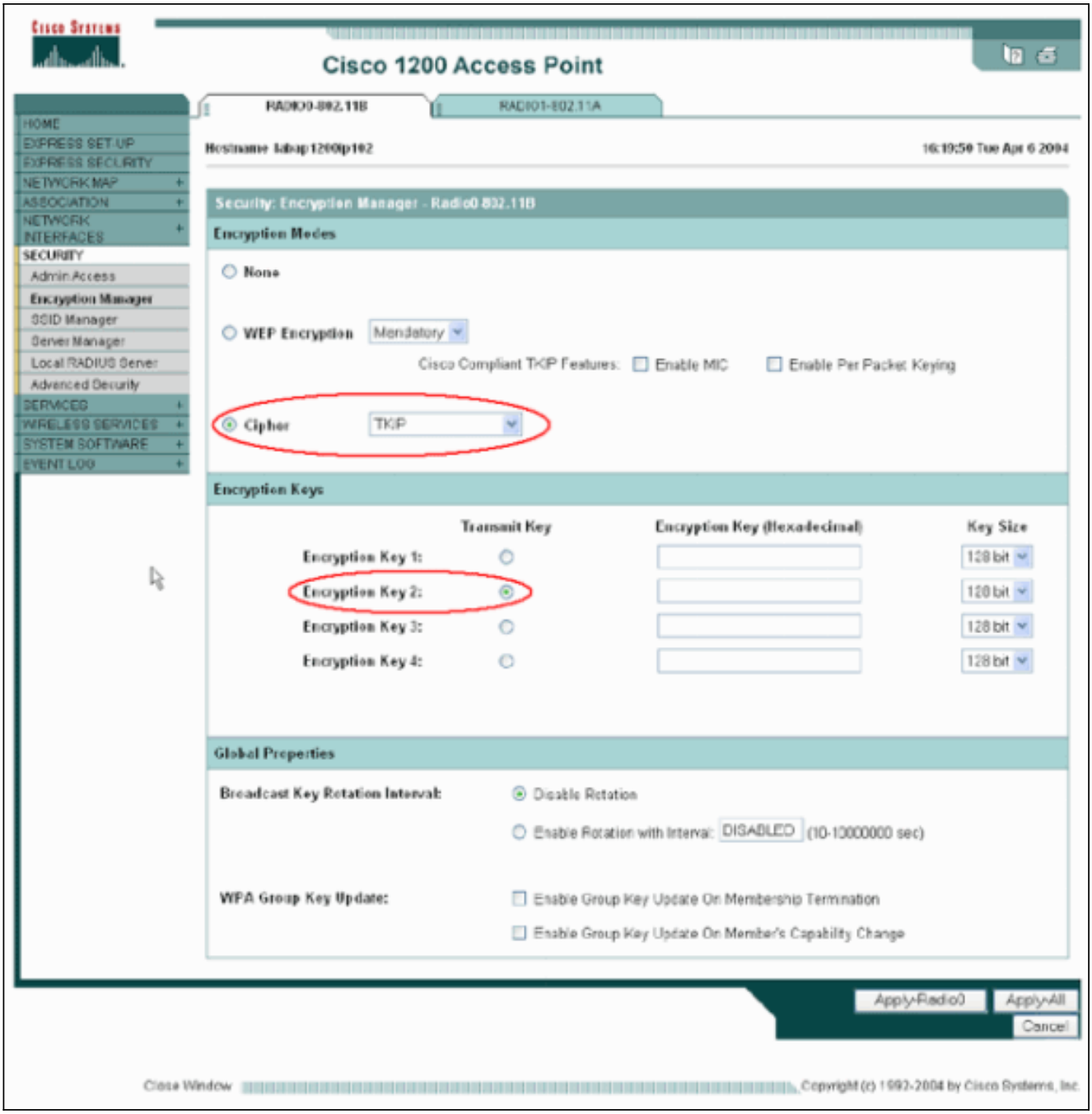
```
ap1#show running-config
 Building configuration...
 .
 .
 .
aaa new-model
!
aaa group server radius rad_eap
 server 192.168.2.100 auth-port 1645 acct-port 1646
.
.
aaa authentication login eap_methods group rad_eap
.
.
.
!
bridge irb
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption 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/he
lp/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
```

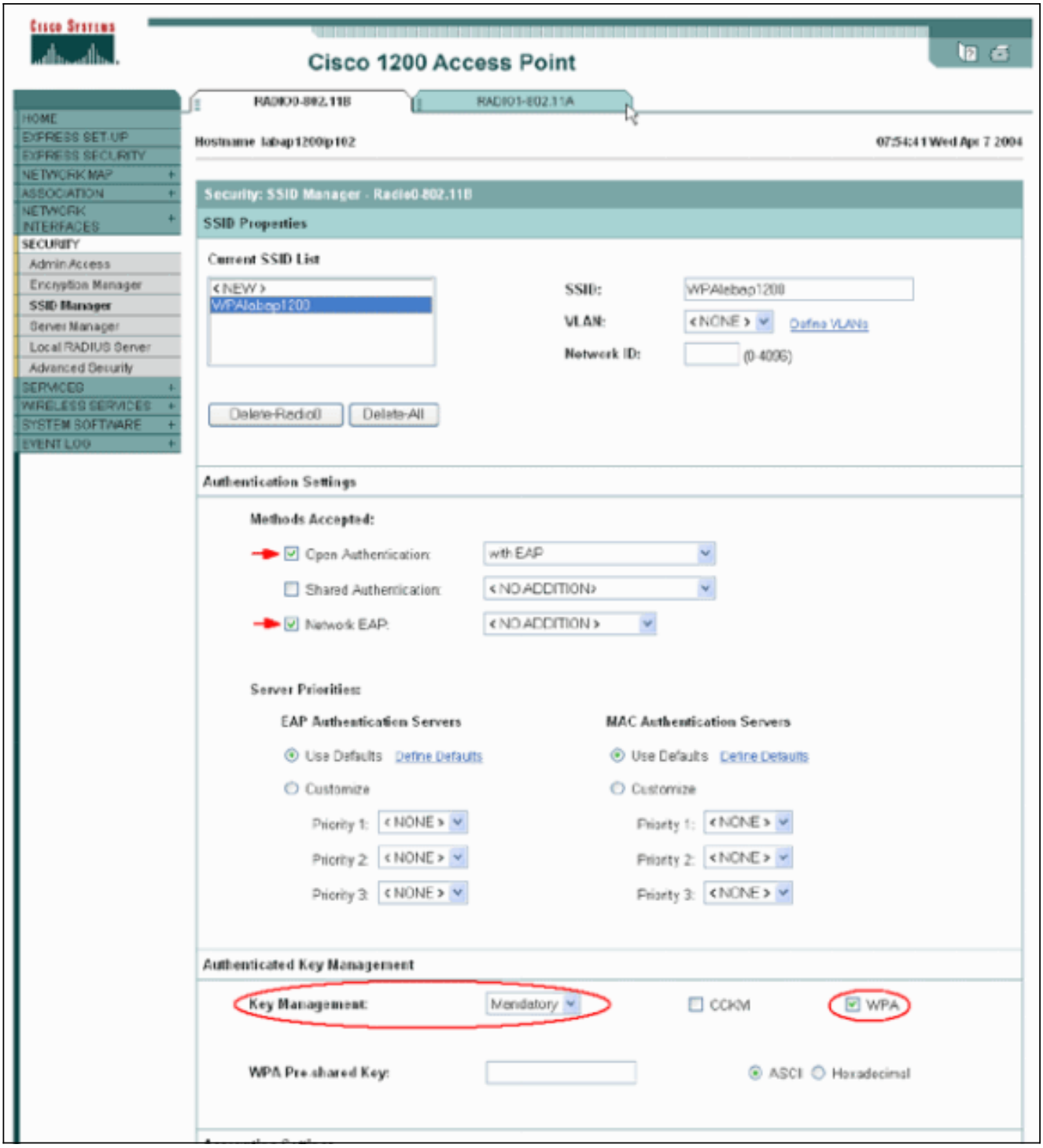
GUI 配置

要配置 WPA 的 AP，请完成以下步骤：

1. 要设置 Encryption Manager，请完成以下步骤：启用 TKIP 的 Cipher。清除 Encryption Key 1 中的值。将 Encryption Key 2 设置为 Transmit Key。单击 Apply-Radio#。



2. 要设置 SSID Manager，请完成以下步骤：从 Current SSID List 中选择所需的 SSID。选择适当的身份验证方法。根据您使用的客户端卡类型进行选择。有关详细信息，请参阅本文档的网络 EAP 或采用 EAP 的开放式身份验证部分。如果在添加 WPA 之前 EAP 已经生效，则可能无需进行更改。要启用密钥管理，请完成以下步骤：从 Key Management 下拉菜单中选择 **Mandatory**。选中 WPA 复选框。单击 **Apply-Radio#**。

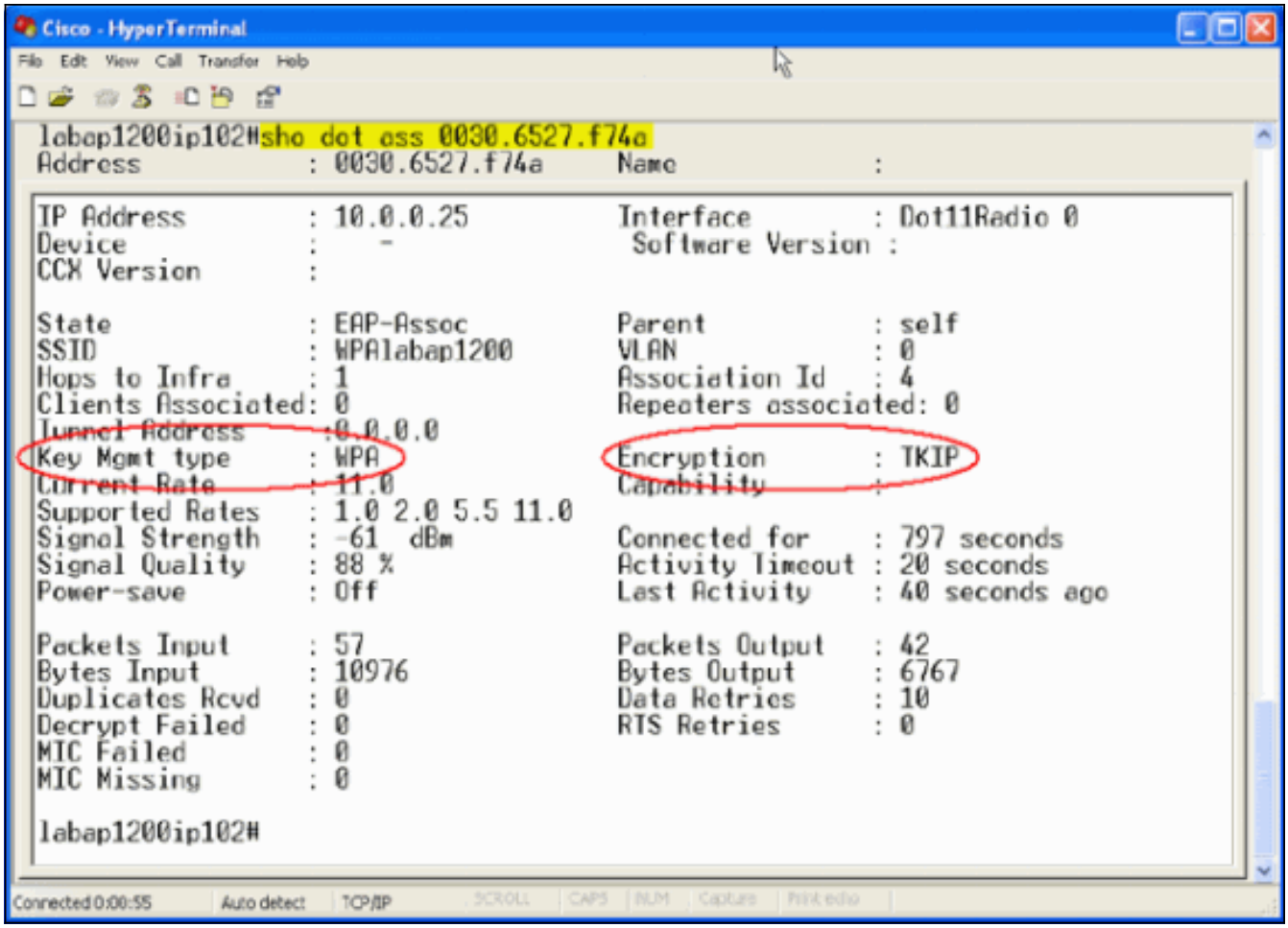


验证

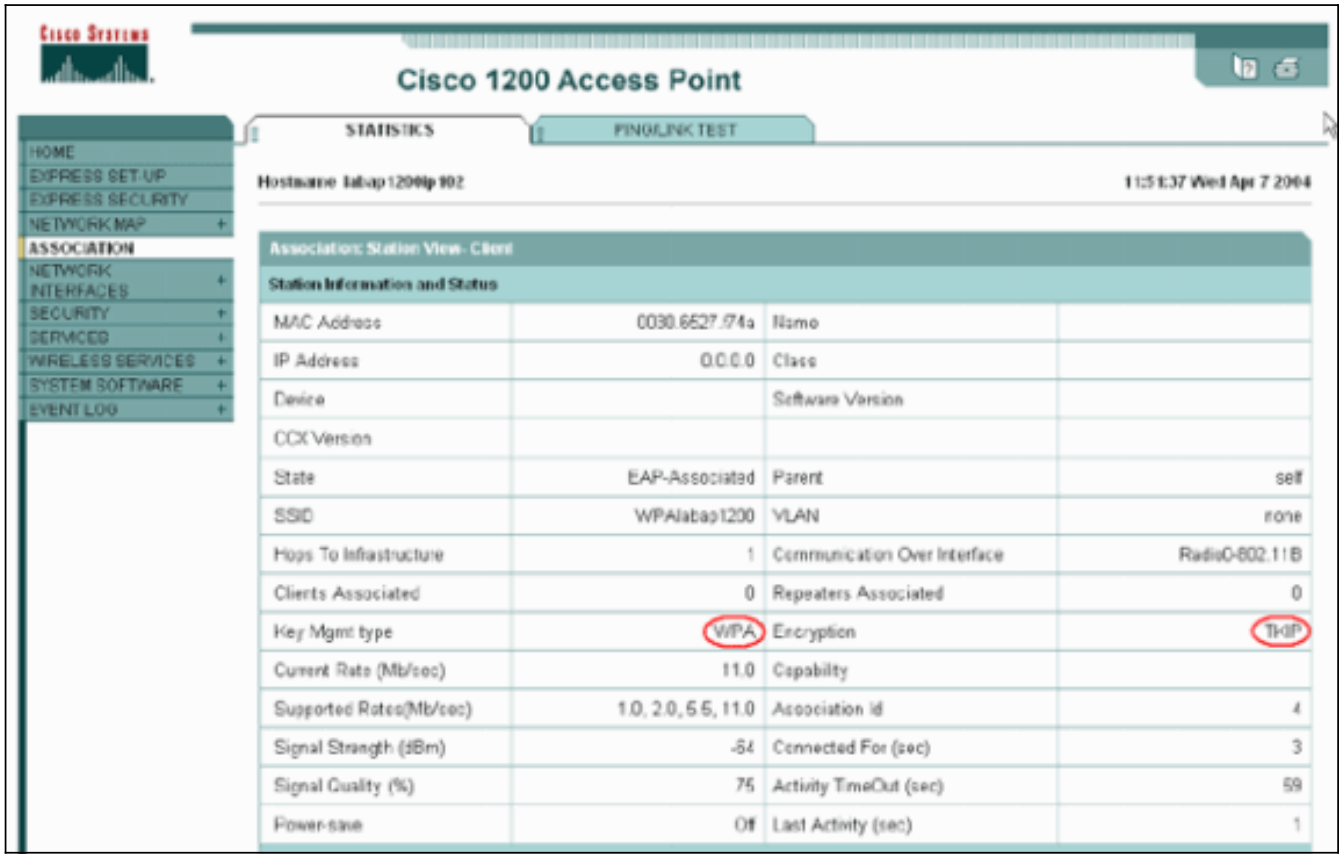
使用本部分可确认配置能否正常运行。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 show 命令。使用 OIT 可查看对 show 命令输出的分析。

- **show dot11 association** *mac_address* - 此命令显示有关专门标识的关联客户端的信息。验证客户端是否将 Key Management 协商为 **WPA 并将 Encryption 协商为 TKIP。**



- 特定客户端的 Association 表条目也必须将 Key Management 指示为 **WPA 并将 Encryption 指示为 TKIP。**在 Association 表中，单击某个客户端的特定 MAC 地址即可查看有关该客户端关联的详细信息。



故障排除

本部分提供的信息可用于对配置进行故障排除。

故障排除步骤

这些信息与该配置相关。要排除配置故障，请完成以下步骤：

1. 如果此 LEAP、EAP 或 PEAP 配置在 WPA 实施前未经过彻底测试，您必须完成以下步骤：暂时禁用 WPA 加密模式。重新启用适当的 EAP。确认身份验证工作正常。
2. 验证客户端的配置是否与 AP 的配置相匹配。例如，当 AP 配置为 WPA 和 TKIP 时，请确认这些设置与客户端中的设置相匹配。

故障排除命令

注意：在使用debug命令之前，请参阅有关Debug命**令的**重要信息。

WPA 密钥管理涉及在 EAP 身份验证成功完成后进行一个四方握手。您可以在 debug 命令输出中看到这四条消息。如果 EAP 没有成功完成对客户端进行的身份验证，或者如果您没有看到这些消息，请完成以下步骤：

1. 暂时禁用 WPA。
2. 重新启用适当的 EAP。
3. 确认身份验证工作正常。

下表对 debug 命令输出进行了说明：

- **debug dot11 aaa manager keys - 该 debug 显示在成对临时密钥 (PTK) 与组临时密钥 (GTK) 进行协商时 AP 与 WPA 客户端之间发生的握手。**这个debug在Cisco IOS软件版本12.2(15)JA介绍过。如果没有出现 debug 输出内容，请验证以下项目：终端监控 **term mon 是否已启用（如果您使用 Telnet 会话）。**debug 是否已启用。客户端是否针对 WPA 进行了适当配置。如果 debug 显示 PTK 和/或 GTK 握手已建立，但没有经过验证，请检查 WPA 请求方软件配置是否正确以及是否为最新版本。
- **debug dot11 aaa authenticator state-machine** - 该 debug 显示客户端在进行关联和身份验证时经过的各种协商状态。状态名称即可表示各种状态。这个debug在Cisco IOS软件版本12.2(15)JA介绍过。在 Cisco IOS 软件版本 12.2(15)JA 及更高版本中，该 debug 命令淘汰了 **debug dot11 aaa dot1x state-machine 命令。**
- **debug dot11 aaa dot1x state-machine** - 该 debug 显示客户端在进行关联和身份验证时经过的各种协商状态。状态名称即可表示各种状态。在低于 Cisco IOS 软件版本 12.2(15)JA 的 Cisco IOS 软件版本中，该 debug 命令也显示了 WPA 密钥管理协商。
- **调试dot11 aaa证明人程序----该调试对于诊断协商通信问题最有帮助。**其详细信息显示了每个协商参与者所发送的内容，并显示了其他参与者的响应。您也可以将该 debug 命令与 **debug radius authentication 命令结合使用。**这个debug在Cisco IOS软件版本12.2(15)JA介绍过。在 Cisco IOS 软件版本 12.2(15)JA 及更高版本中，该 debug 命令淘汰了 **debug dot11 aaa dot1x process 命令。**
- **debug dot11 aaa dot1x process----该调试对于诊断协商通信问题最有帮助。**其详细信息显示了每个协商参与者所发送的内容，并显示了其他参与者的响应。您也可以将该 debug 命令与 **debug radius authentication 命令结合使用。**在低于 Cisco IOS 软件版本 12.2(15)JA 的 Cisco IOS 软件版本中，该 debug 命令也显示了 WPA 密钥管理协商。

相关信息

- 配置密码套件和 WEP
- 配置身份验证类型
- WPA2 - Wi-Fi 保护访问 2
- Wi-Fi 保护访问 2 (WPA 2) 配置
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。