在Aironet访问接入点的Wired Equivalent Privacy (WEP)和网桥配置示例

Contents

Introduction

本文提供方法配置在Cisco Aironet无线局域网(WLAN)组件的有线等效保密(WEP)。

Note: 请参见第6的静态Web键部分章-配置WLANs关于在无线局域网控制器(WLCs)的WEP配置的更多信息。

WEP是加密算法被建立到802.11 (Wi-Fi)标准。WEP加密以40-使用Ron's代码4 (RC4)流密码或104-bit键和24位初始化矢量(iv)。

当标准指定， WEP以40位使用RC4算法或104-bit键和24位IV. RC4是对称算法，因为使用同一个键加密和数据的解密。当WEP是启用的时，每个无线电“位置”有一个键。关键字被用于在数据的发射前通过广播频道加扰数据。如果位置收到没有用appropriate键加扰的一个信息包，信息包被丢弃和从未被传送到主机。

WEP可以主要用于一个家庭办公室或不要求非常强有力的安全保障的小型办公室。

Aironet WEP实施在硬件里。所以，当您使用WEP，最小的性能影响发生。

Note: 有WEP的一些已知问题，做它不是强加密方法。问题是：

- 有维护一把被共享的WEP密钥的很多管理开销。
- WEP有问题和根据共享密钥的所有系统一样。所有秘密产生一个人变得公共一段时间以后。
- IV植入的WEP算法在明文被发送。
- WEP校验和是线性和可预测的。

临时密钥完整性协议(TKIP)被创建解决这些WEP问题。类似于WEP， TKIP使用RC4加密。然而，TKIP通过添加测量提高WEP例如每个信息包关键散列， Message Integrity Check (MIC)和广播密钥交替针对WEP的已知弱点。TKIP以128-bit键加密和64位键使用RC4流密码认证。

Prerequisites

Requirements

本文假设，您能做运行联系到WLAN设备，并且设备在一个未加密的环境里通常作用。

为了配置标准的40位WEP，您必须有与彼此联络的两个或多个无线电单元。

Note: Aironet产品能建立40位WEP连接同IEEE 802.11b兼容非Cisco的产品。本文不讨论其它设备的配置。

对于128-bit WEP链路的创建，思科产品与其他思科产品只呼应。

Components Used

以本文使用这些组件：

- 与彼此联络的两个或多个无线电单元
- 对WLAN设备的一运行联系

The information in this document was created from the devices in a specific lab environment.All of the devices used in this document started with a cleared (default) configuration.If your network is live, make sure that you understand the potential impact of any command.

Conventions

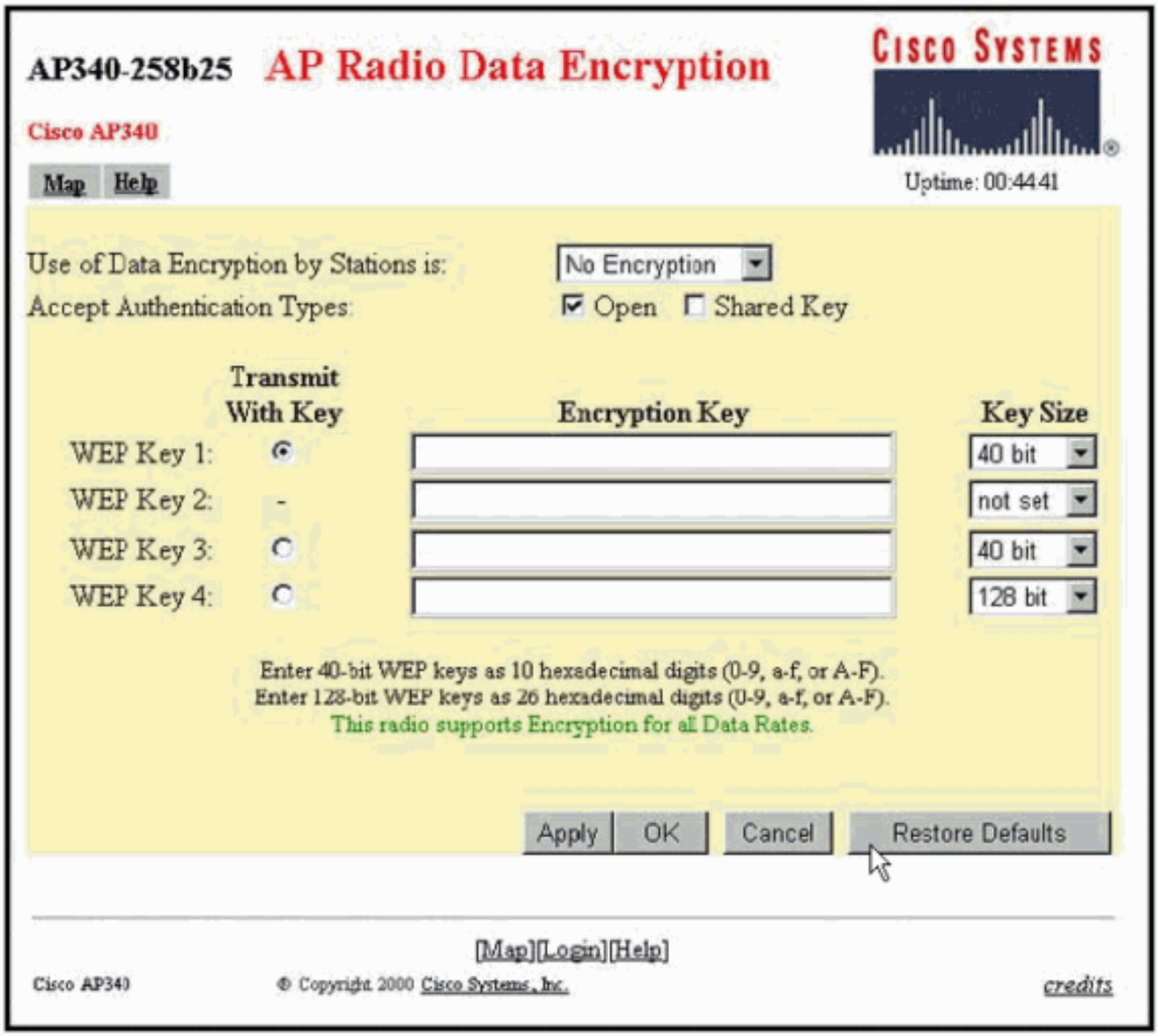
Refer to Cisco Technical Tips Conventions for more information on document conventions.

配置在Aironet访问点访问接入点的WEP

运行VxWorks操作系统的Aironet访问点访问接入点

完成这些步骤：

1. 建立与接入点(AP)的联系。
2. 连接对AP Radio Encryption菜单。请使用这些路径之一：**Summary Status > Setup > AP无线电/硬件> Radio数据加密(WEP) > AP Radio Data EncryptionSummary Status > Setup > Security > Security Setup ：无线数据加密> AP Radio Data EncryptionNote:** 为了做对此页的变动，您必须是一个管理员以身份和写功能。**AP Radio Data Encryption菜单的Web浏览器查阅**



VxWorks设置

AP Radio Data Encryption页展示各种各样的选项使用。一些选项对于WEP是必需的。此部分注释这些必须的选项。其它选项不是必要为了WEP能作用，但是他们是推荐的。

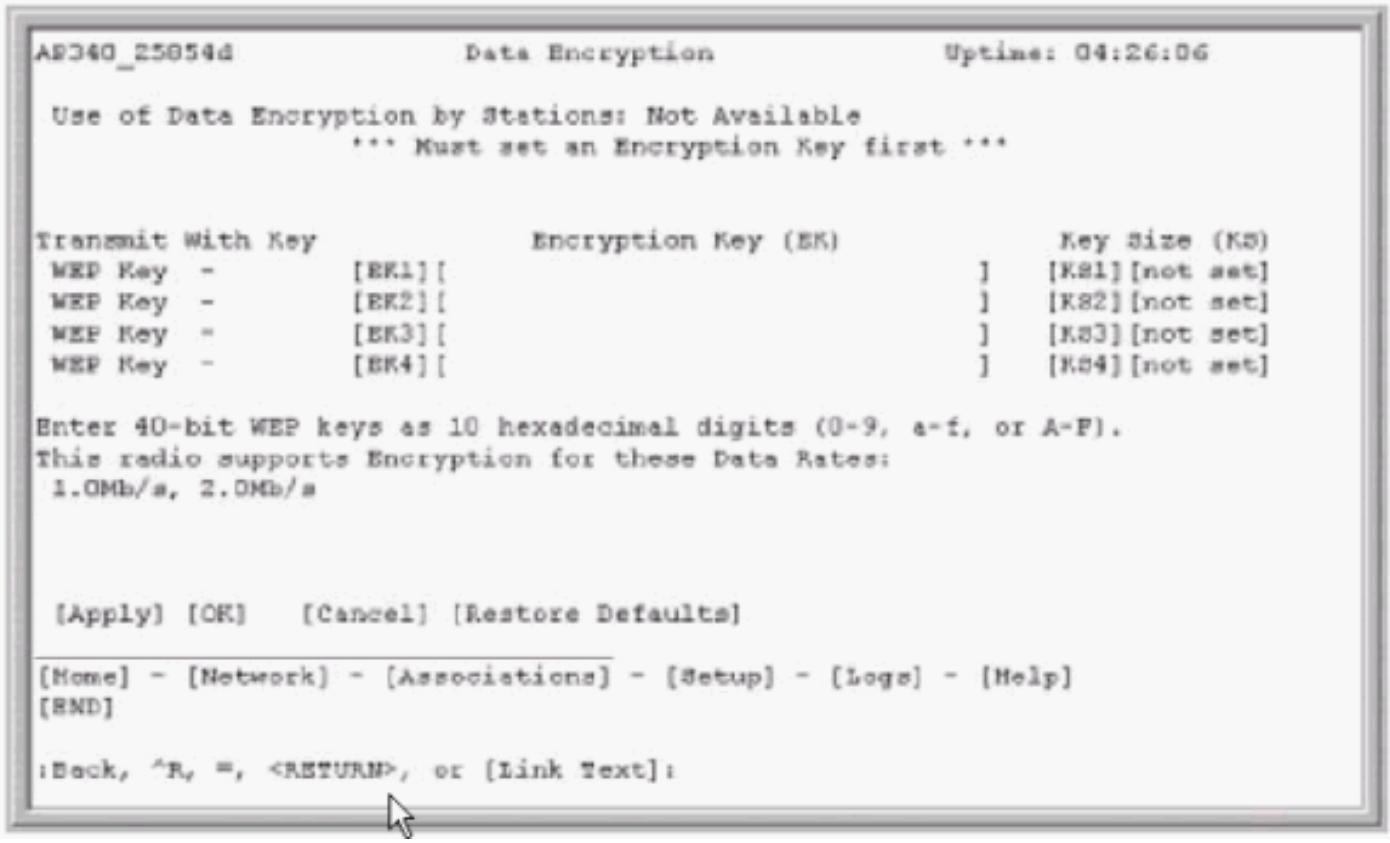
- **由位置的Use of Data Encryption是：**请使用此设置为了选择客户端是否必须使用数据加密，当他们与AP时沟通。下拉菜单列出三个选项：**没有加密(默认值)** —要求客户端与AP沟通，不用任何数据加密。此设置不是推荐的。**可选**—允许客户端与AP沟通任一有或没有数据加密。一般，您使用此选项，当您有不能建立WEP联系时的客户端设备，例如非Cisco的客户端在128-bit WEP环境。**完全加密(建议使用)** —，当他们与AP时，沟通要求客户端使用数据加密。不使用数据加密的客户端不允许沟通。如果希望最大化您的WLAN，安全此选项是推荐的。**Note:** 您必须设置WEP密钥，在您enable (event)加密使用前。请参阅此列表的**加密密钥强制性**部分。
- **Accept Authentication Types**您能选择开放，共享密钥，或者这两个选项为了设置AP将认可的认证。**打开(建议使用)** —不管其WEP密钥，此默认设置允许所有设备，验证和尝试联合。**共享密钥**—此设置告诉AP发送明文，共享的密钥查询到尝试与AP产生关联的所有设备。**Note:** 此查询能打开AP对从入侵者的一次已知文本攻击。所以，此设置不是一样安全象开放设置。
- **传输用键**这些按钮允许您选择在数据传输期间， AP使用的键。您只能每次选择一个键。任一或所有集键能使用接受数据。在您指定它作为传送密钥前，您必须设置键。
- **加密密钥强制性**这些字段允许您输入WEP密钥。进入40位WEP密钥的10个十六进制数字或

128-bit WEP密钥的26个十六进制数字。键可以是这些位的所有组合：0到9a到fA到F为了保护WEP密钥安全，现有的WEP密钥没出现以在条目字段的纯文本。在APs中最新版本，您能删除现有的键。然而，您不能编辑现有的键。**Note:** 您必须相似地设置您的网络、APs和客户端设备的WEP密钥。例如，如果设置在您的AP的WEP密钥3到0987654321并且选择此键作为活动键，您必须也设置在客户端设备的WEP密钥3为同一值。

- **密钥大小强制性**此设置设置键为40位或128-bit WEP。如果"not set"为此选择出现，没有设置键。**Note:** 您不能通过选择"not set"删除键。
- **Action按钮**四Action按钮控制设置。如果Javascript在您的Web浏览器允许，确认弹出窗口出现，在您点击所有按钮后，除了取消。**适用**—此按钮激活新的值设置。浏览器在页。**好**—此按钮应用新的设置并且移动浏览器回到主要设置页。**取消**—此按钮取消设置更改并且以前返回设置到存储的值。您然后回到主要设置页。**恢复默认值**—此按钮更改在此页的所有设置回到工厂默认设置。

Note: 在APs中最近Cisco IOS版本，仅**适用**和**取消**控制按钮为此页是可用的。

数据加密菜单的终端仿真器视图



WEP密钥配置顺序(Cisco IOS软件)的终端仿真器视图

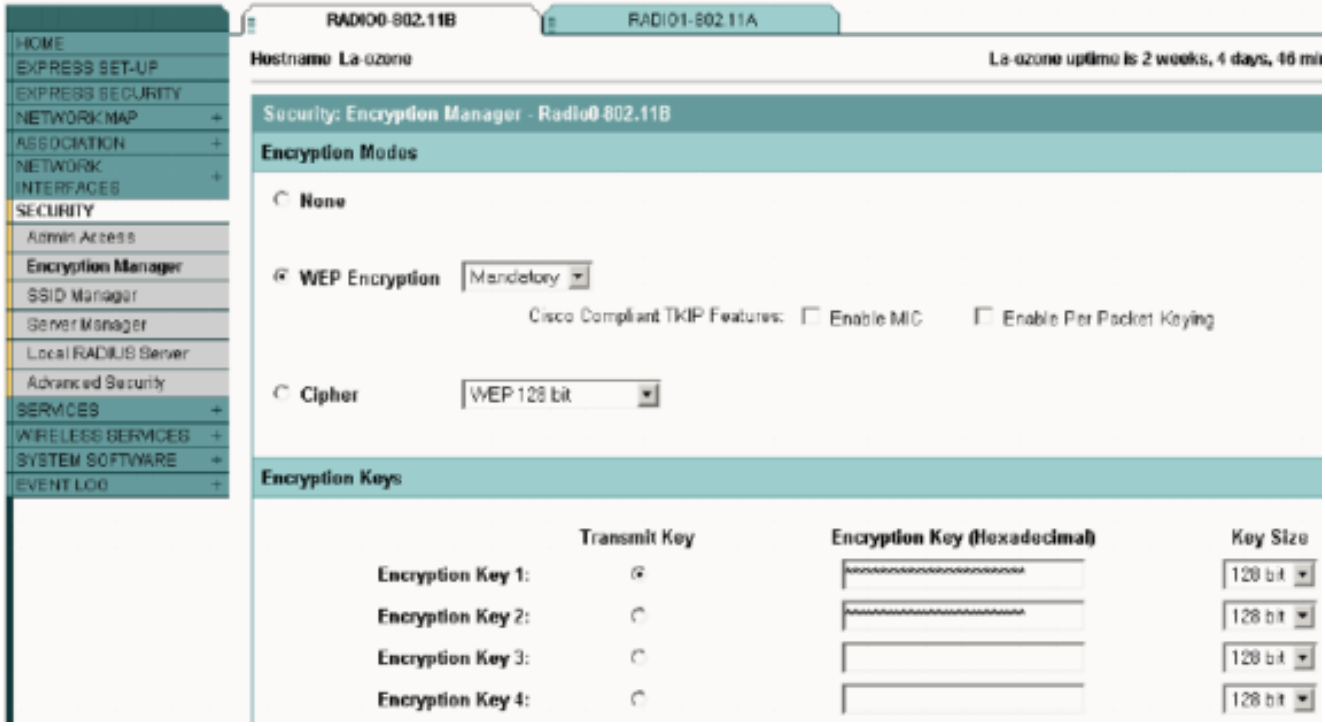
```
La-ozone>
La-ozone>
La-ozone>enable
Password:
La-ozone#
La-ozone#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
La-ozone(config)#interface dot
La-ozone(config)#interface dot11Radio 0
La-ozone(config-if)#encryption key 1 size 128bit 11c0ffeec0ffeec0ffeec0ffee ?
  transmit-key  Set the key as transmit key
  <cr>

La-ozone(config-if)#encryption key 1 size 128bit 11c0ffeec0ffeec0ffeec0ffee transmit-key
La-ozone(config-if)#end
La-ozone#
*Mar 19 00:42:13.893: %SYS-5-CONFIG_I: Configured from console by console
La-ozone#
La-ozone#
```

Aironet运行Cisco IOS软件的APs

完成这些步骤：

1. 建立与AP的联系。
2. 从在窗口的左边Security菜单选项，请选择您要配置您的静态WEP密钥的无线接口的**加密管理器。AP安全加密管理器菜单的Web浏览器查阅**



配置Aironet网桥

如果使用VxWorks，请完成这些步骤：

1. 建立与网桥的联系。
2. 连接对Privacy菜单。选择**主菜单> Configuration>无线电> I80211 > Privacy**。Privacy菜单控制使用在空气传输用无线电的数据包的加密。RSA RC4算法和那个四个已知键用于加密信息包。在无线电电池的每个节点必须认识所有键在使用中，但是中的任一键能选择传输数据。**Privacy菜单的终端仿真器视图**

```
        Configuration Radio I80211 Privacy Menu
      Option          Value       Description
1 - Encryption    [ off  ]    - Encrypt radio packets
2 - Auth          [ open ]    - Authentication mode
3 - Client        [ open ]    - Client authentication modes allowed
4 - Key                       - Set the keys
5 - Transmit                  - Key number for transmit
 Enter an option number or name, "=" main menu, <ESC> previous menu
>_
```

参考配置密码套件和WEP - 1300系列网桥和配置WEP和WEP功能- 1400系列网桥关于如何通过CLI模式配置在1300和1400系列网桥的WEP的信息。

为了使用GUI配置运行本文Cisco IOS软件部分的1300和1400系列网桥，请完成在Aironet解释的同一个程序APs。

VxWorks设置

Privacy菜单提交您必须配置的一套选项。一些选项对于WEP是必需的。此部分注释这些必须的选项。其它选项不是必要为了WEP能作用，但是他们是推荐的。

此部分展示菜单选项按顺序他们出现于Privacy菜单的终端仿真器视图。然而，请配置选项按此顺序：

1. 键
2. 传输
3. Auth
4. 客户端
5. 加密

配置按此顺序保证必要的首要条件设置，当您配置每个设置。

这些是选项：

- **关键强制性**键选项编程加密密钥到网桥。提示您设置四个键之一。两次提示您输入键。为了定义键，您必须进入10个或26个十六进制数字，取决于网桥配置是否是为40位或128-bit键。请使用这些位的所有组合：0到9a到fA到F键在无线电电池的***所有***节点必须配比，并且您必须按同一顺序输入键。只要键的数量在WLAN的每个设备配比您不需要定义全部四个键。
- **传输**传输选项告诉无线电使用的哪些键为了传输信息包。每无线电能解码发送与任何四个键的收到的信息包。
- **Auth**您使用在中继网桥的Auth选项为了确定哪认证模式单元使用用其父母连接。允许的值是开放或共享密钥。802.11协议指定客户端必须验证与父母的程序，在客户端能联合前。**打开(建议使用)** —认证此模式根本是一次空操作。所有客户端允许验证。**共享密钥**—此模式允许父母发送客户端质询文本，客户端加密并且返回到父母。如果父母成功解码质询文本，客户端验证。**警告：** 请勿使用共享密钥模式。当您使用它时，同样数据的明文和被加密的版本在空气传输。这不获取什么。如果用户键是错误的，单元不解码信息包，并且信息包不能获得访问到网络。
- **客户端**客户端选项确定客户端节点使用关联到单元的认证模式。这些是允许的值：**打开(建议使用)** —认证此模式根本是一次空操作。所有客户端允许验证。**共享密钥**—此模式允许父母发送客户端质询文本，客户端加密并且返回到父母。如果父母成功解码质询文本，客户端验证。**两个**—此模式允许客户端使用任一个模式。
- **加密**如果设置Encryption选项对，加密没有完成。数据无危险传输。**在强制性**—如果设置

Encryption选项至开，所有传送的数据信息包被加密，并且丢弃所有未加密的收到的信息包。**混合**—在混合模式，根或中继网桥接受从有加密启用开/关的二者之一的客户端的关联。在这种情况下，在节点之间的仅数据包两个支持被加密。无危险发送组播信息包。所有节点能看到信息包。**警告：** 请勿使用混合模式。如果安排加密被启用的客户端发送一个组播信息包到其父母，信息包被加密。父母解码信息包并且无危险重传信息包到信元，并且其他节点能看到信息包。能力显示在加密的一个信息包和未加密的形式能造成中断键。包括混合模式仅是为与其他供应商的兼容性。

配置客户端适配器

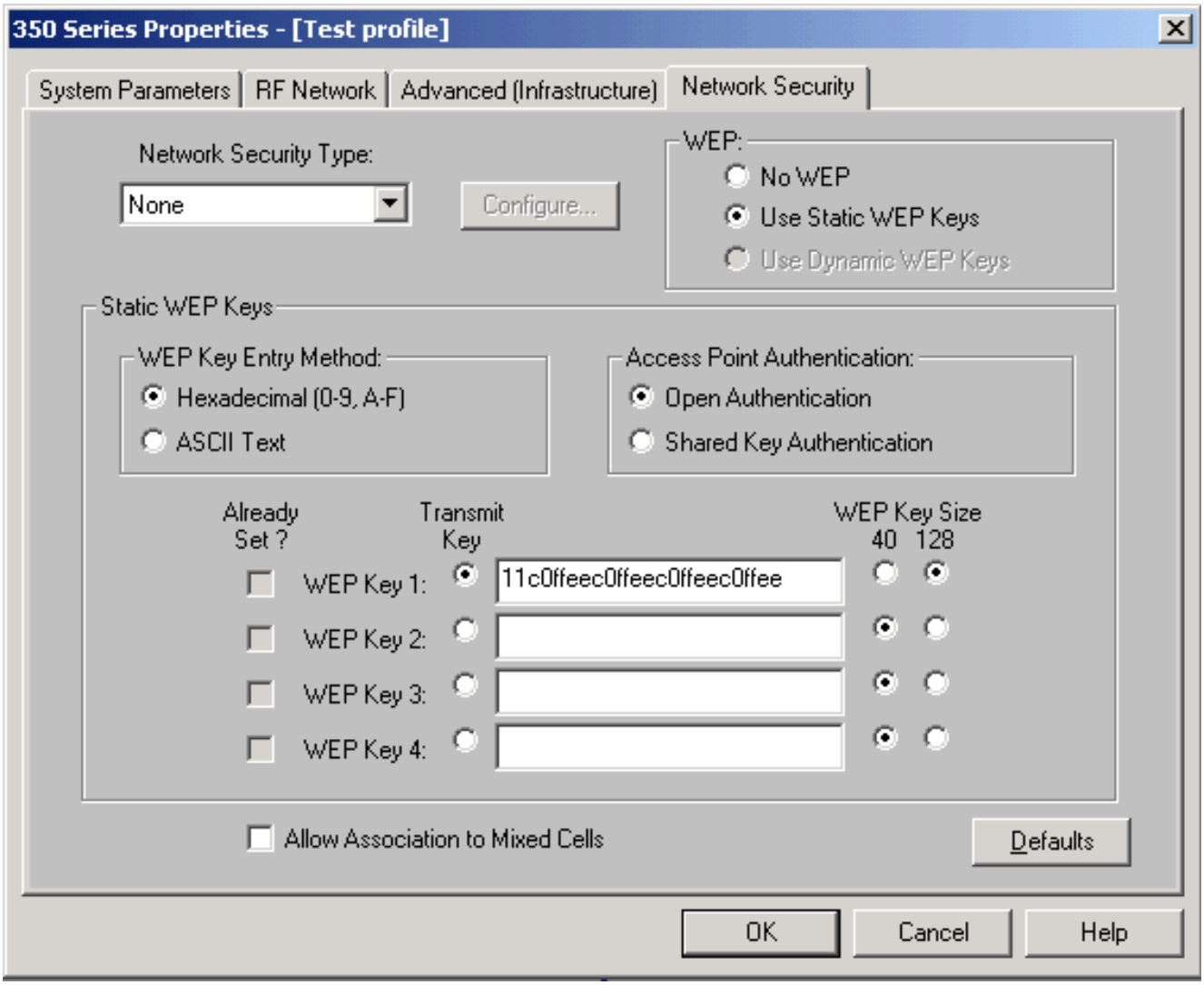
您必须完成两个主要步骤为了设置在Aironet客户端适配器的WEP ：

1. 配置WEP密钥/键在客户端加密管理器。
2. 在Aironet客户端工具(ACU)的Enable (event) WEP。

设置WEP密钥

完成这些步骤为了设置在客户端适配器的WEP密钥：

1. 打开ACU并且选择**配置文件管理器**。
2. 选择您希望对enable (event) WEP并且点击**编辑的**配置文件。
3. 点击**Network Security选项**为了显示安全选项，并且点击**使用静态WEP密钥**。此动作激活WEP黯淡的配置选项，当WEP没有选择时。



4. 对于您要创建的WEP密钥，请选择**40**位或**128**位在WEP密钥大小下在窗口的右边。**Note:** 128-bit客户端适配器能使用40位或128-bit键。但是40位适配器能只使用40位键。**Note:** 您的客户端适配器WEP密钥必须匹配其他无线局域网组件您传达使用的WEP密钥。当您设置超过一把WEP密钥时，您必须分配WEP密钥到同样WEP密钥编号为所有设备。必须包括WEP密钥十六进制字符，并且必须包含40位WEP密钥的10个字符或128-bit WEP密钥的26个字符。十六进制字符可以是：0到9a到fA到F**Note:** Aironet APs不支持ASCII文本WEP密钥。所以，您必须选择十六进制(0-9， A-F)选项，如果计划以这些使用您的客户端适配器APs。**Note:** 在您创建WEP密钥后，您能在它写。但是您不能编辑或删除它。**Note:** 如果使用Aironet Desktop软件(ADU)的一个最新版本而不是ACU作为客户端工具，您能也删除被创建的WEP密钥和用新的替换它。
5. 点击是在其中一个键旁边您创建的**传送密钥**按钮。使用此动作，您表明此键是您要使用传输信息包的键。
6. 点击**不变**下面WEP密钥类型。此动作允许您的客户端适配器保留此WEP密钥，既使当对适配器的功率被免除或在键安装计算机的重新启动。如果选择临时此选项的， WEP密钥丢失，当功率从您的客户端适配器时被免除。
7. 单击 **Ok**。

Enable (event) WEP

完成这些步骤：

1. 打开ACU并且从菜单栏选择**Edit Properties**。

2. 点击**Network Security选项**为了显示安全选项。
3. 检查**Enable WEP复选框**为了激活WEP。

参考配置在ADU的WEP关于步骤配置WEP使用ADU作为客户端工具。

配置工作组网桥

有在Aironet 340系列工作组网桥和Aironet 340系列网桥之间的区别。然而，使用WEP的工作组网桥的配置与网桥的配置是几乎相同的。请参阅配置Aironet网桥部分关于网桥的配置。

1. 连接到工作组网桥。
2. 连接对Privacy菜单。选择**Main > Configuration > Radio > I80211 > Privacy**为了访问保密性VxWorks菜单。

设置

Privacy菜单提交设置该此部分列表。配置在工作组网桥的选项按此顺序：

1. 键
2. 传输
3. Auth
4. 加密

这些是选项：

- **键**关键选项设立网桥用途为了收到信息包的WEP密钥。值必须匹配AP或其它设备工作组网桥联络用途的键。键包括40位加密的10个十六进制字符或128-bit加密的26个十六进制字符。十六进制字符可以是这些位的所有组合：0到9a到fA到F
- **传输**传输选项设立网桥用途为了传输信息包的WEP密钥。您能决定使用您使用关键选项的同一个键。如果选择不同的密钥，您必须设立在AP的配比的键。仅一把WEP密钥可以一次使用发射。您使用传输数据的WEP密钥必须设置为在联络的您的工作组网桥和其它设备的同一值。
- **认证(Auth)**Auth参数确定哪个验证方法系统使用。选项是：**打开(建议使用)** —不管其WEP设置，默认开放设置允许所有AP，验证然后尝试与网桥联络。**共享密钥**—此设置指示网桥发送明文，共享的密钥查询到APs为与网桥沟通。共享密钥设置能打开网桥对从入侵者的一次已知文本攻击。所以，此设置不是一样安全象开放设置。
- **加密**Encryption选项设置在所有数据包的加密参数，除了关联信息包和一些控制数据包。有四个选项：**Note:** AP必须适当地有活动加密和密钥集合。这是默认设置。所有加密被关闭。工作组网桥与与使用的AP不连通WEP。**在(建议使用)** —此设置要求所有数据传输的加密。工作组网桥与使用WEP的APs只连通。**混合在**此设置意味着网桥总是使用WEP为了与AP连通。然而，AP与所有设备联络，他们是否使用WEP或不使用WEP。**混合**此设置意味着网桥不使用WEP为了与AP连通。然而， AP与所有设备联络，他们是否使用WEP或不使用WEP。**警告：** 如果选择或混合，当WEP类别和您通过其无线链路配置网桥，对网桥的连接丢失，如果不正确设置WEP密钥。切记您使用同一个设置，当您设置在工作组网桥的WEP密钥和在其它设备的WEP密钥在您的WLAN。

Related Information

- IEEE标准关联
- Aironet 340系列无线LAN产品

- 无线支持资源
- 无线LAN支持页
- Cisco Aironet接入点的Cisco IOS软件配置指南
- Cisco Aironet 1300系列室外接入点/网桥的Cisco IOS软件配置指南
- 用于 VxWorks 的 Cisco Aironet 接入点软件配置指南
- Cisco Aironet 1400系列网桥软件配置指南
- Cisco Aironet无线局域网客户端适配器配置指南
- Cisco无线LAN安全概述
- 巩固无线网络的无线(移动性)
- 接入点作为工作组网桥配置示例
- Cisco Aironet工作组网桥FAQ
- Cisco Aironet设备的密码恢复流程
- Cisco Aironet接入点FAQ
- Technical Support & Documentation - Cisco Systems