在Aironet接入点和网桥上配置WEP

目录

简介

本文档提供在Cisco Aironet无线LAN(WLAN)组件上配置有线等效保密(WEP)的方法。

注：有关无线局域网控制器(WLC)上WEP配置的详细信息，请参阅第6章 — 配置WLAN的静态Web密钥部分。

WEP是802.11(Wi-Fi)标准中内置的加密算法。WEP加密使用带有40或104位密钥和24位初始化矢量(IV)的Ron's Code 4(RC4)Stream Cipher（流密码）。

如标准规定的，WEP使用RC4算法和40位或104位密钥和24位IV。RC4是一种对称算法，因为它对数据的加密和解密使用相同的密钥。当WEP被启用时，每个“station”有一个关键字。关键字被用于在数据的发射前通过广播频道加扰数据。如果工作站收到的数据包没有使用适当的密钥进行加扰，则该数据包将被丢弃，并且永远不会被传送到主机。

WEP主要用于家庭办公室或不需要非常强大安全性的小型办公室。

Aironet WEP实施在硬件中。因此，使用WEP时，对性能影响最小。

注意：WEP存在一些已知问题，这使它不是强加密方法。这些问题包括：

- 维护共享WEP密钥需要大量的管理开销。

- WEP与基于共享密钥的所有系统存在相同的问题。给一个人的任何秘密在一段时间后公开。
- WEP算法种子的IV以明文发送。
- WEP校验和是线性的，可预测。

已创建临时密钥完整性协议(TKIP)来解决这些WEP问题。与WEP类似，TKIP使用RC4加密。但是，TKIP通过添加每数据包密钥散列、消息完整性检查(MIC)和广播密钥轮替等措施来增强WEP，以解决WEP的已知漏洞。TKIP使用RC4流加密，128位密钥用于加密，64位密钥用于身份验证。

先决条件

要求

本文档假设您可以与WLAN设备建立管理连接，并且设备在未加密的环境中正常运行。

要配置标准40位WEP，您必须有两个或多个相互通信的无线电设备。

注意：Aironet产品可以与符合IEEE 802.11b的非Cisco产品建立40位WEP连接。本文档不涉及其他设备的配置。

创建128位WEP链路时，思科产品仅与其他思科产品交互。

使用的组件

将以下组件与本文档配合使用：

- 两个或多个相互通信的无线电单元
- 与WLAN设备的管理连接

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。

规则

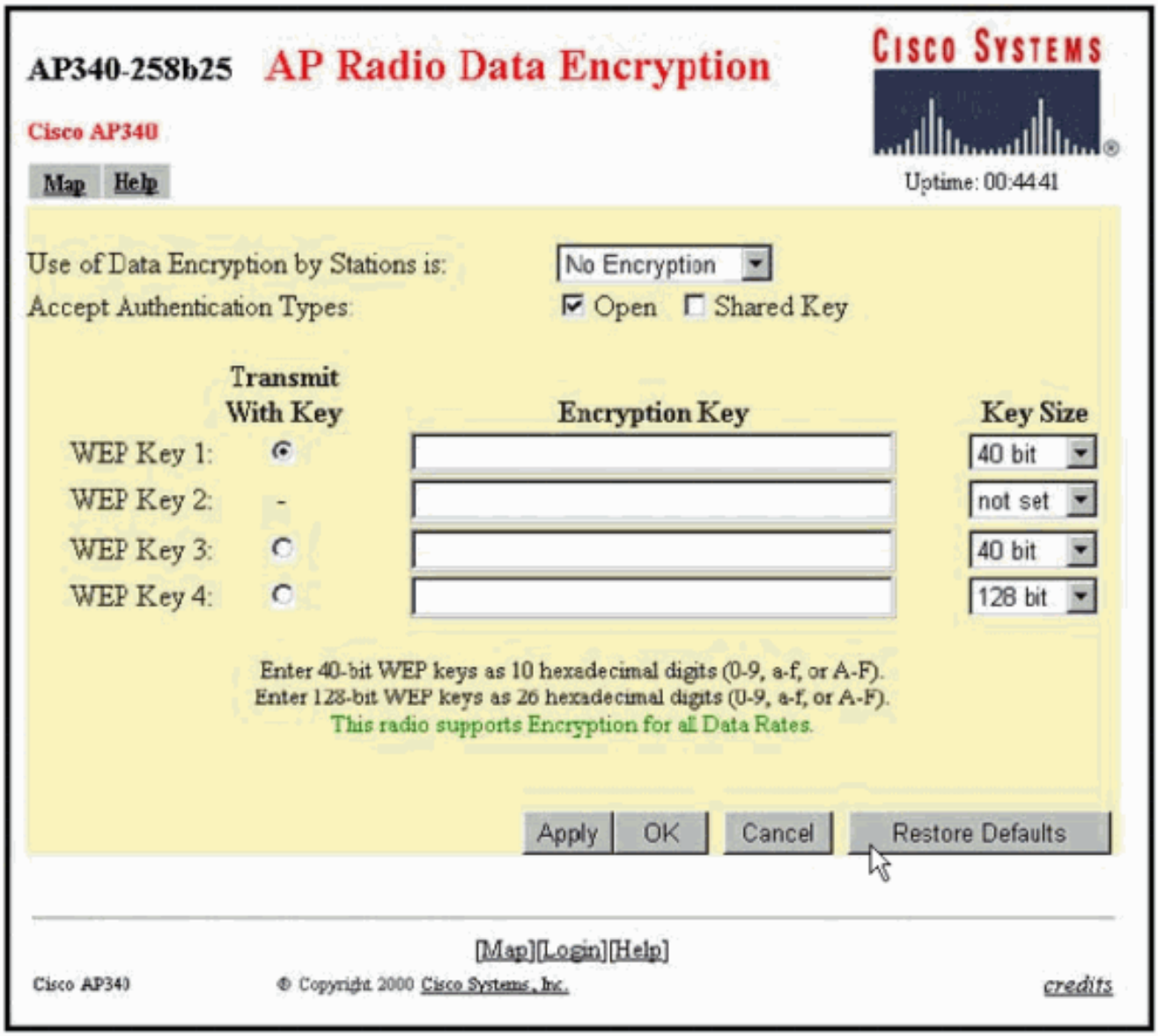
有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

在Aironet接入点上配置WEP

运行VxWorks操作系统的Aironet接入点

请完成以下步骤：

1. 连接到接入点(AP)。
2. 导航至AP Radio Encryption菜单。使用以下路径之一：**Summary Status > Setup > AP Radio/Hardware > Radio Data Encryption(WEP)> AP Radio Data Encryption摘要状态>设置>安全>安全设置：无线数据加密(WEP)> AP无线数据加密注意**：要更改此页面，您必须是具有身份和写入功能的管理员。**AP Radio Data Encryption菜单的Web浏览器视图**



VxWorks设置

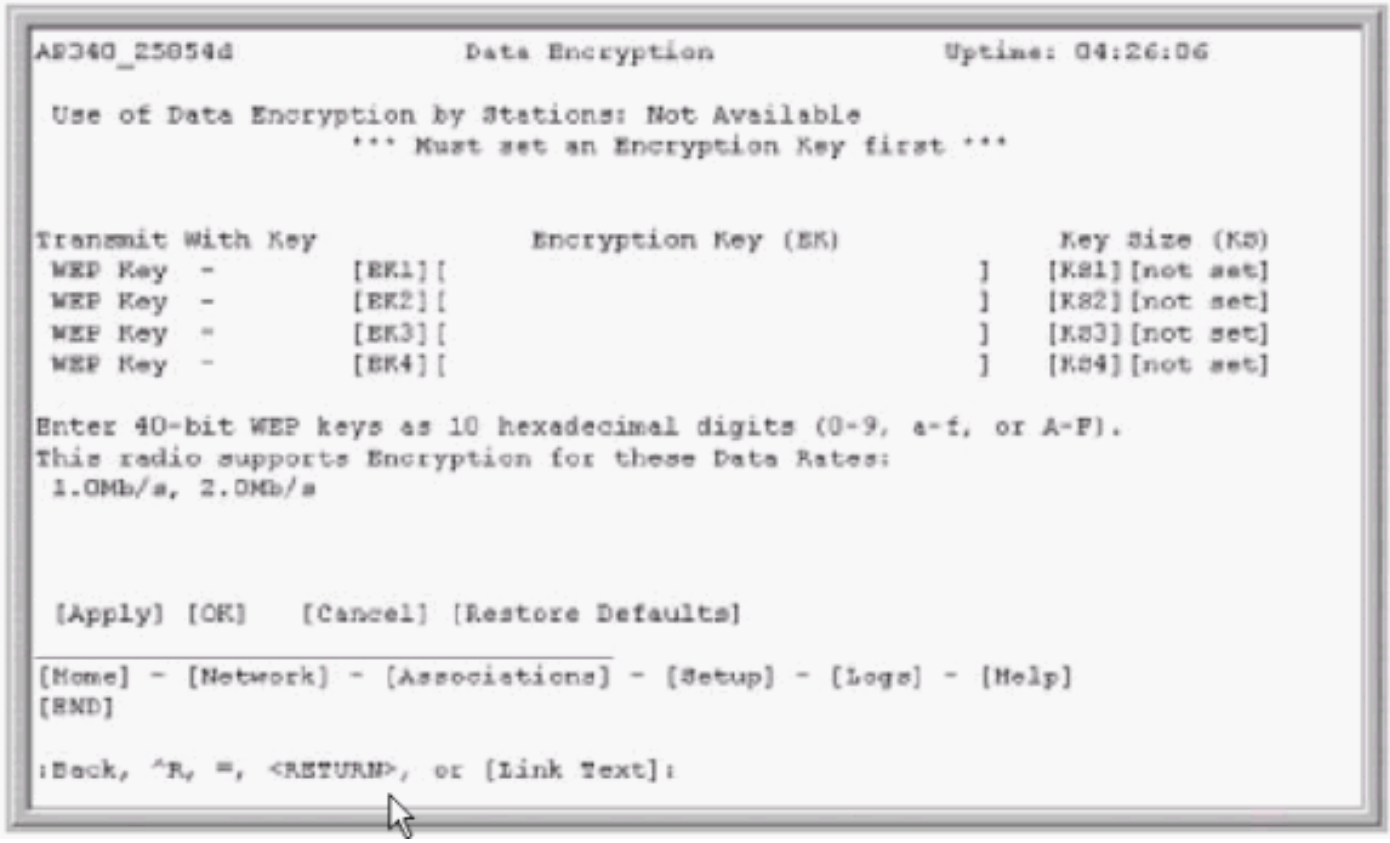
AP Radio Data Encryption页面提供了多种选项。某些选项是WEP的必需选项。本部分将说明这些必选选项。WEP功能不需要其他选项，但建议使用。

- **站点使用数据加密**：使用此设置以选择客户端在与AP通信时是否必须使用数据加密。下拉菜单列出三个选项：**No Encryption（默认）** — 要求客户端与AP通信，而不需要任何数据加密。不建议使用此设置。**可选** — 允许客户端与AP通信，无论是否使用数据加密。通常，当客户端设备无法建立WEP连接时（例如128位WEP环境中的非Cisco客户端），使用此选项。**Full Encryption(RECOMMENDED)** — 要求客户端在与AP通信时使用数据加密。不使用数据加密的客户端不允许通信。如果您希望最大限度地提高WLAN的安全性，建议使用此选项。**注意**：在启用加密使用之前，必须设置WEP密钥。请参阅**此列表的加**密密钥（必填）部分。
- **接受身份验证类型**您可以选择打开、共享密钥或这两个选项，以设置AP将识别的身份验证。**Open(RECOMMENDED)** — 此默认设置允许任何设备（无论其WEP密钥如何）进行身份验证并尝试关联。**共享密钥** — 此设置告知AP向任何尝试与AP关联的设备发送纯文本共享密钥查询。**注意**：此查询可能使AP对入侵者的已知文本攻击保持开放。因此，此设置不像“打开”设置那么安全。
- **使用密钥传输**这些按钮允许您选择AP在数据传输过程中使用的密钥。一次只能选择一个密钥。任何或所有设置的密钥都可用于接收数据。必须先设置密钥，然后才将其指定为传输密钥。

- **加密密钥（必填）**这些字段允许您输入WEP密钥。输入10个十六进制数字表示40位WEP密钥，输入26个十六进制数字表示128位WEP密钥。密钥可以是以下数字的任意组合：0 到 9到fA到F为了保护WEP密钥安全，现有WEP密钥不会以纯文本形式出现在条目字段中。在AP的最新版本中，您可以删除现有密钥。但是，您无法编辑现有密钥。**注意：**您必须以完全相同的方式为网络、AP和客户端设备设置WEP密钥。例如，如果将AP上的WEP密钥3设置为0987654321并选择此密钥作为活动密钥，则还必须将客户端设备上的WEP密钥3设置为相同的值。
- **密钥大小（必填）**此设置将密钥设置为40位或128位WEP。如果此选择显示“未设置”，则未设置密钥。**注意：**不能通过选择“未设置”删除密钥。
- **操作按钮**四个操作按钮控制设置。如果在Web浏览器上启用了JavaScript，则在单击任何按钮（取消除外）后，会出现确认弹出窗口。Apply — 此按钮激活新值设置。浏览器仍保留在页面上。OK — 此按钮应用新设置并将浏览器移回Setup主页。**取消** — 此按钮取消设置更改并将设置返回到以前存储的值。然后返回主Setup页面。**恢复默认**值 — 此按钮将此页上的所有设置重新更改为出厂默认设置。

注意：在最新的Cisco IOS® AP版本中，只有“应用”**和“**取消**”**控制按钮可用于此页。

数据加密菜单的终端仿真器视图



WEP密钥配置序列的终端仿真器视图（Cisco IOS®软件）

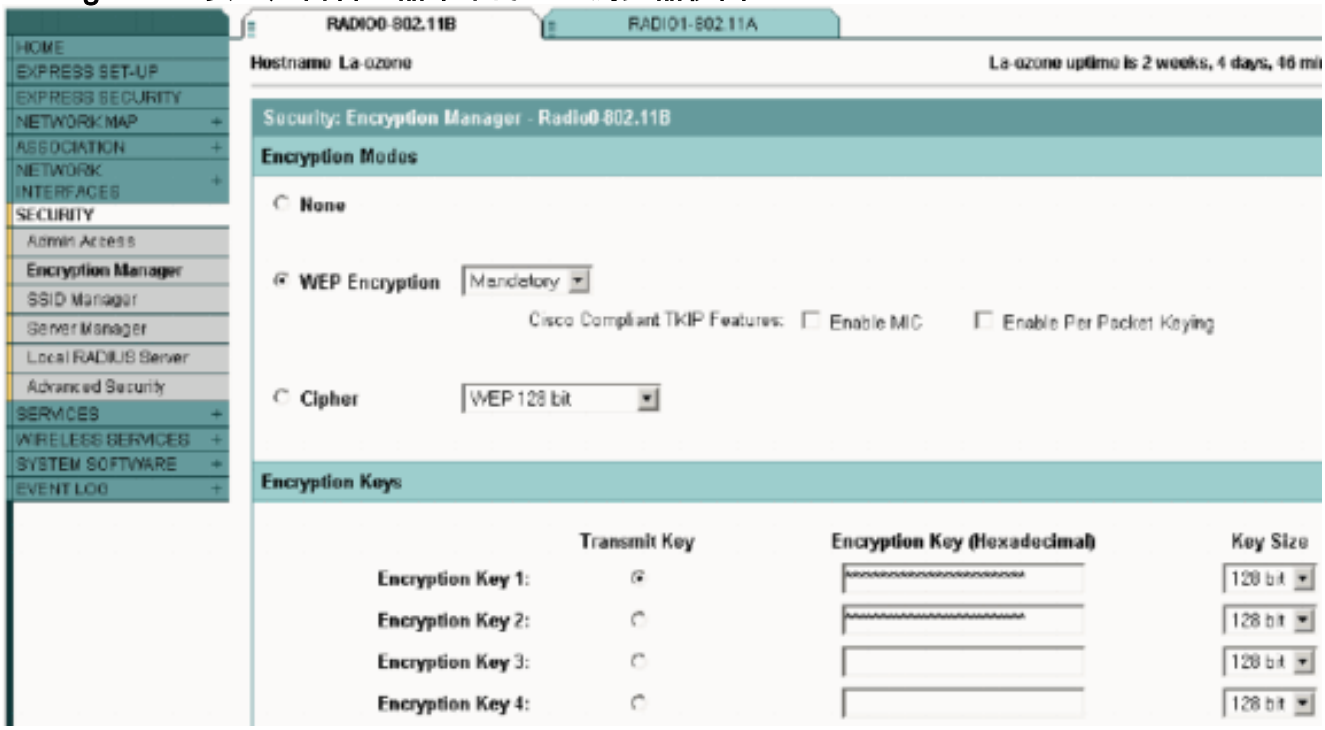
```
La-ozone>
La-ozone>
La-ozone>enable
Password:
La-ozone#
La-ozone#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
La-ozone(config)#interface dot
La-ozone(config)#interface dot11Radio 0
La-ozone(config-if)#encryption key 1 size 128bit 11c0ffeec0ffeec0ffeec0ffee ?
 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

运行Cisco IOS软件的Aironet AP

请完成以下步骤：

1. 连接到AP。
2. 从窗口左侧的SECURITY菜单选项中，为要配置静态WEP密钥的无线电接口选择**Encryption Manager。AP安全加密管理器菜单的Web浏览器视图**



配置Aironet网桥

如果使用VxWorks，请完成以下步骤：

1. 连接网桥。
2. 导航至“隐私”菜单。选择**主菜单>配置>无线电> I80211 >隐私**。“隐私”(Privacy)菜单控制无线电在空中传输的数据包上加密的使用。RSA RC4算法和最多四个已知密钥之一用于加密数据包。无线电单元中的每个节点必须知道正在使用的所有密钥，但可以选择任何密钥来传输数据。**隐私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
>_
```

有关如何通过CLI模式在1300和1400系列网桥中配置WEP的信息，请参阅配置密码套件和WEP - 1300系列网桥和配置WEP和WEP功能 — 1400系列网桥。

要使用GUI配置1300和1400系列网桥，请完成本文档“运行Cisco IOS软件的Aironet AP”部分中介绍的相同步骤。

VxWorks设置

“隐私”菜单提供一组您必须配置的选项。某些选项是WEP的必需选项。本部分将说明这些必选选项。WEP功能不需要其他选项，但建议使用。

本节按菜单选项在“隐私”菜单的“终端仿真器视图”中的显示顺序显示菜单选项。但是，请按以下顺序配置选项：

1. 密钥
2. 传输
3. auth
4. 客户端
5. 加密

按此顺序进行配置可确保在配置每个设置时设置必要的前提条件。

以下是选项：

- **密钥（必填）**密钥选项将加密密钥编程到网桥。系统将提示您设置四个键中的一个。系统将提示您输入两次密钥。要定义密钥，必须输入10或26个十六进制数字，这取决于网桥配置是用于40位还是128位密钥。使用以下数字的任意组合：0 到 9到fA到F密钥在无线电单元***格中***的所有节点中必须匹配，并且您必须按相同顺序输入密钥。只要WLAN中每台设备的密钥数都匹配，您就无需定义全部四个密钥。
- **传输**Transmit选项告知无线电要使用哪些密钥来传输数据包。每个无线电都能够解密使用四个密钥中的任意一个发送的已接收数据包。
- **auth**在中继器网桥上使用身份验证选项，以确定设备使用哪种身份验证模式与其父设备连接。允许的值为Open或Shared Key。802.11协议指定了一个过程，在该过程中，客户端必须向父级进行身份验证，客户端才能进行关联。Open(RECOMMENDED) — 此身份验证模式实质上是空操作。允许所有客户端进行身份验证。**共享密钥** — 此模式允许父级向客户端发送质询文本，客户端对该文本进行加密并返回给父级。如果父设备成功解密质询文本，则客户端将通过身份验证。**注意：**请勿使用共享密钥模式。使用时，同一数据的明文和加密版本会在空中传输。这不会带来任何好处。如果用户密钥错误，设备不解密数据包，并且数据包无法访问网络。
- **客户端**客户端选项确定客户端节点用于与设备关联的身份验证模式。以下是允许的值：Open(RECOMMENDED) — 此身份验证模式实质上是空操作。允许所有客户端进行身份验证。**共享密钥** — 此模式允许父级向客户端发送质询文本，客户端对该文本进行加密并返回给父

级。如果父设备成功解密质询文本，则客户端将通过身份验证。**Both** — 此模式允许客户端使用任一模式。

- **加密关闭** — 如果将“加密”选项设置为“关闭”，则不执行加密。数据以明文传输。**On(MANDATORY)** — 如果将Encryption选项设置为On，则所有传输的数据包都将加密，并丢弃任何未加密的接收数据包。**混合** — 在混合模式下，根网桥或中继器网桥接受来自已打开或关闭加密的客户端的关联。在这种情况下，只加密两个支持的节点之间的数据包。组播数据包以明文形式发送。所有节点都可以看到数据包。**注意：**请勿使用混合模式。如果启用了加密的客户端向其父设备发送组播数据包，则会加密该数据包。父节点解密数据包，然后以明文形式将数据包重新传输给信元，其他节点可以看到数据包。能够以加密和未加密的形式查看数据包可能会破坏密钥。包含混合模式仅用于与其他供应商兼容。

配置客户端适配器

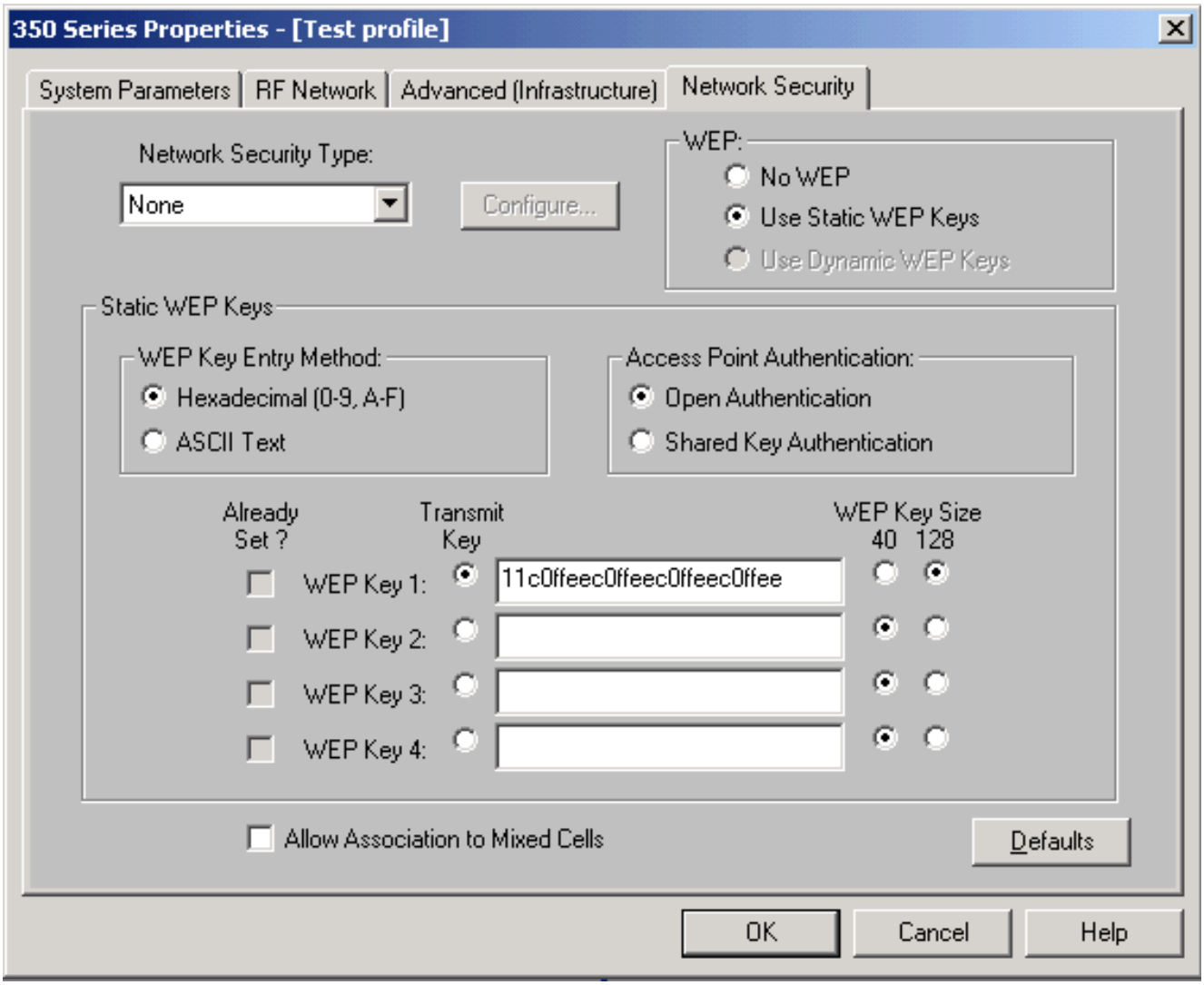
要在Aironet客户端适配器上设置WEP，必须完成两个主要步骤：

1. 在客户端加密管理器中配置WEP密钥/密钥。
2. 在Aironet客户端实用程序(ACU)中启用WEP。

设置WEP密钥

要在客户端适配器上设置WEP密钥，请完成以下步骤：

1. 打开ACU并选择“配置**文件管理器**”。
2. 选择要启用WEP的配置文件，然后单击**Edit**。
3. 单击“**Network Security(网络安**全)”选项卡以显示安全选项，然后单击“**Use Static WEP Keys（使用静态WEP密钥）**”。此操作激活WEP配置选项，当未选择WEP时，这些选项呈灰色显示。



4. 对于要创建的WEP密钥，请在窗口右侧的WEP Key Size（WEP密钥大小）下选择**40**位或**128**位。**注意**：128位客户端适配器可以使用40位或128位密钥。但40位适配器只能使用40位密钥。**注意**：您的客户端适配器WEP密钥必须与您通信时使用的其他WLAN组件的WEP密钥匹配。设置多个WEP密钥时，必须为所有设备分配相同的WEP密钥编号。WEP密钥必须由十六进制字符组成，40位WEP密钥必须包含10个字符，128位WEP密钥必须包含26个字符。十六进制字符可以是：0 到 9到fA到F**注意**：Aironet AP不支持ASCII文本WEP密钥。因此，如果计划将这些AP与客户端适配器配合使用，则必须选择十六进制(0-9, A-F)选项。**注意**：创建WEP密钥后，可以对其进行写入。但您不能编辑或删除它。**注意**：如果使用Aironet桌面实用程序(ADU)的更新版本而不是ACU作为客户端实用程序，您还可以删除创建的WEP密钥，并将其替换为新密钥。
5. 单击**Transmit Key**按钮，该按钮位于您创建的密钥之一旁。通过此操作，您表示此密钥是要用于传输数据包的密钥。
6. 在WEP Key Type（WEP密钥类型）下单击**Persistent**。此操作允许客户端适配器保留此WEP密钥，即使在适配器断电或重新启动安装该密钥的计算机时也是如此。如果为此选项选择“临时”，当从客户端适配器断电时，WEP密钥将丢失。
7. Click **OK**.

启用 WEP

请完成以下步骤：

1. 打开ACU，然后从菜**单栏中**选择“编辑属性”。

2. 单击**Network Security**选项卡以显示安全选项。
3. 选中**Enable WEP**复选框以激活WEP。

有关将ADU用作客户端实用程序配置WEP的步骤，请参阅在ADU中配置WEP。

配置工作组网桥

Aironet 340系列工作组桥和Aironet 340系列桥有所不同。但是，工作组网桥的配置使用WEP几乎与网桥的配置相同。有关网桥的配置，请参阅“配置Aironet网桥”部分。

1. 连接到工作组桥。
2. 导航至“隐私”菜单。选择**Main > Configuration > Radio > I80211 > Privacy**以访问Privacy VxWorks菜单。

设置

“隐私”菜单显示此部分列出的设置。按以下顺序配置工作组桥上的选项：

1. 密钥
2. 传输
3. auth
4. 加密

以下是选项：

- **密钥**Key选项用于建立网桥用于接收数据包的WEP密钥。该值必须与AP或工作组网桥通信使用的其他设备的密钥匹配。密钥最多包含10个十六进制字符（40位加密）或26个十六进制字符（128位加密）。十六进制字符可以是以下数字的任意组合：0 到 9到fA到F
- **传输**Transmit选项建立网桥用于传输数据包的WEP密钥。您可以选择使用与用于Key选项的密钥相同的密钥。如果选择其他密钥，则必须在AP上建立匹配的密钥。一次只能使用一个WEP密钥进行传输。您用于传输数据的WEP密钥必须设置为工作组桥和与其通信的其他设备上的相同值。
- **身份验证（身份验证）**Auth参数确定系统使用哪种身份验证方法。选项有：**Open(RECOMMENDED)** — 默认的Open设置允许任何AP（无论其WEP设置如何）进行身份验证，然后尝试与网桥通信。**共享密**钥 — 此设置指示网桥向AP发送纯文本共享密钥查询以尝试与网桥通信。“共享密钥”设置可让网桥对入侵者的已知文本攻击保持开放。因此，此设置不像“打开”设置那么安全。
- **加密**Encryption选项为所有数据包设置加密参数，但关联数据包和某些控制数据包除外。其中有四个选项：**注意：**AP必须激活加密并正确设置密钥。**关闭** — 这是默认设置。所有加密都已关闭。工作组桥不使用WEP与AP通信。**On(RECOMMENDED)** — 此设置要求对所有数据传输进行加密。工作组桥仅与使用WEP的AP通信。**Mixed on** — 此设置表示网桥始终使用WEP与AP通信。但是，AP与所有设备通信，无论它们使用WEP还是不使用WEP。**Mixed off** — 此设置表示网桥不使用WEP与AP通信。但是，AP与所有设备通信，无论它们使用WEP还是不使用WEP。**注意：**如果选择On或Mixed on作为WEP类别，并且通过其无线链路配置网桥，则如果设置WEP密钥不正确，则与网桥的连接将丢失。在工作组桥上设置WEP密钥时，请确保使用与WLAN上其他设备设置WEP密钥时完全相同的设置。

相关信息

- IEEE标准协会
- 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LAN客户端适配器配置指南
- 思科无线局域网安全概述
- 无线（移动）保护无线网络
- 接入点作为工作组网桥的配置示例
- Cisco Aironet 工作组网桥常见问题
- Cisco Aironet 设备的密码恢复程序
- Cisco Aironet 接入点常见问题
- 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）。