

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

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[配置在Aironet访问接入点的WEP](#)

[运行VxWorks操作系统的Aironet访问接入点](#)

[VxWorks设置](#)

[Aironet运行Cisco IOS软件的AP](#)

[配置Aironet网桥](#)

[VxWorks设置](#)

[配置客户端适配器](#)

[设置WEP密钥](#)

[启用 WEP](#)

[配置工作组网桥](#)

[设置](#)

[相关信息](#)

简介

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)。

注意： 参考[章节6的静态Web密钥](#)部分-[配置WLAN](#)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密钥和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密钥和24位IV. RC4是对称算法，因为使用同一密钥加密和数据的解密。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。如果站点收到没有用appropriate键加扰的数据包，数据包丢弃和从未传送到主机。

WEP可以主要用于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。

注意： 有与WEP的一些已知问题，做它不是强加密方法。这些问题包括：

- 有维护一把共享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。所有机密给对一个人变得公共一段时间以后。
- IV植入的WEP算法在明文发送。
- WEP校验和是线性和可预测的。

临时密钥完整性协议(TKIP)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例如每个信息包密钥哈希算法，Message Integrity Check (MIC)和广播密钥交替针对WEP已知弱点。TKIP以128-bit密钥加密和64位密钥使用RC4流密码验证。

先决条件

要求

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环境通常作用。

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。

注意： 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。

使用的组件

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

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](#)。

配置在Aironet访问接入点的WEP

运行VxWorks操作系统的Aironet访问接入点

完成这些步骤：

1. 建立对接入点(AP)的联系。
2. 导航对Ap无线加密菜单。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 Encryption****Summary Status > Setup > Security > Security Setup**：**无线数据加密> AP Radio Data Encryption****注意：** 为了做对此页的变动，您必须是一个管理员以标识和写入功能。AP Radio Data Encryption菜单的Web浏览器查阅

AP340-258b25 **AP Radio Data Encryption**


Cisco AP340
Uptime: 00:44:41

Map Help

Use of Data Encryption by Stations is: No Encryption

Accept Authentication Types: Open Shared Key

	Transmit With Key	Encryption Key	Key Size
WEP Key 1:	<input checked="" type="radio"/>	<input style="width: 100%;" type="text"/>	40 bit
WEP Key 2:	<input type="radio"/>	<input style="width: 100%;" type="text"/>	not set
WEP Key 3:	<input type="radio"/>	<input style="width: 100%;" type="text"/>	40 bit
WEP Key 4:	<input type="radio"/>	<input style="width: 100%;" type="text"/>	128 bit

Enter 40-bit WEP keys as 10 hexadecimal digits (0-9, a-f, or A-F).
Enter 128-bit WEP keys as 26 hexadecimal digits (0-9, a-f, or A-F).
This radio supports Encryption for all Data Rates.

Apply
OK
Cancel
Restore Defaults

Cisco AP340
© Copyright 2000 Cisco Systems, Inc.
credits

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选项。其它选项不是必要为了WEP能作用，但是推荐他们。

- **由站点的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，当他们通信与AP时。下拉菜单列出三个选项：**不加密(默认)**—要求客户端通信与AP，不用任何数据加密。没有推荐此设置。**可选**—允许客户端通信与AP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)**—，当他们通信与AP时，要求客户端使用数据加密。不使用数据加密的客户端没有允许通信。推荐此选项是否希望最大化您的WLAN安全。**注意：**在您启用加密使用前，您必须设置WEP密钥。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(推荐)**—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，共享的密钥查询到该所有的设备尝试与AP产生关联。**注意：**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。
- **有密钥的平湖**这些按钮允许您选择在数据传输期间，AP使用的密钥。您只能每次选择一密钥。任一或所有集合密钥能使用接收数据。在您指定它作为传送密钥前，您必须设置密钥。
- **加密密钥强制性**这些字段允许您输入WEP密钥。输入40位WEP密钥的10十六进制数字或128-

bit WEP密钥的26十六进制数字。密钥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WEP密钥在纯文本没出现在输入字段。在AP中最新版本，您能删除现有密钥。然而，您不能编辑现有密钥。**注意：**您必须相似地设置您的网络、AP和客户端设备的WEP密钥。例如，如果您在您的AP的集WEP密钥3到0987654321和选择此密钥作为活动密钥，您必须也设置在客户端设备的WEP密钥3为同一个值。

- **密钥大小强制性**此设置设置密钥为40位或128-bit WEP。如果"not set"为此选择出现，密钥没有设置。**注意：**您不能通过选择"not set"删除密钥。
- **操作按钮**四操作按钮控制设置。如果Javascript在您的Web浏览器启用，确认弹出窗口出现，在您点击所有按钮后，除了取消。**应用**—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对存储的值。您然后回到主要设置页。**恢复默认**—此按钮更改在此页的所有设置回到工厂默认设置。

注意：在AP中最近的Cisco IOS版本，仅**应用**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

```
AP340_25854d          Data Encryption          Uptime: 04:26:06

Use of Data Encryption by Stations: Not Available
*** Must set an Encryption Key first ***

Transmit With Key      Encryption Key (EK)      Key Size (KS)
WEP Key - [EK1][          ] [KS1][not set]
WEP Key - [EK2][          ] [KS2][not set]
WEP Key - [EK3][          ] [KS3][not set]
WEP Key - [EK4][          ] [KS4][not set]

Enter 40-bit WEP keys as 10 hexadecimal digits (0-9, a-f, or A-F).
This radio supports Encryption for these Data Rates:
1.0Mb/s, 2.0Mb/s

[Apply] [OK]  [Cancel] [Restore Defaults]

[Home] - [Network] - [Associations] - [Setup] - [Logs] - [Help]
[END]

;Back, ^R, =, <RETURN>, or [Link Text]:
```

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AP](#)

完成这些步骤：

1. 建立对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

The screenshot displays the configuration page for the Security: Encryption Manager on a radio interface (Radio0-802.11B). The left sidebar contains a navigation menu with categories like SECURITY and SERVICES. The main configuration area shows the following settings:

- Encryption Mode:** WEP Encryption (selected), with a dropdown menu set to 'Manualkey'. Below this, there are checkboxes for 'Cisco Compliant TKIP Features' including 'Enable MIC' and 'Enable Per Packet Keying', both of which are currently unchecked.
- Encryption Keys:** A table with four rows for 'Encryption Key 1' through 'Encryption Key 4'. Each row has a radio button for 'Transmit Key', a text input field for the 'Encryption Key (Hexadecimal)', and a dropdown menu for 'Key Size' (all set to 128 bit).

[配置Aironet网桥](#)

如果使用VxWorks，请完成这些步骤：

1. 建立对网桥的联系。
2. 导航对Privacy菜单。选择主菜单> Configuration>收音> I80211 > Privacy。Privacy菜单控制使用在空气传送给无线电的数据包的加密。RSA RC4算法和那个四已知密钥用于加密数据包。每个节点在无线电小区必须认识所有密钥在使用中，但是中的任一密钥能选择传送数据。
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         [ open ]     - Set the keys
5 - Transmit    [ open ]     - Key number for transmit
Enter an option number or name, "=" main menu, <ESC> previous menu
>_
```

参考[配置密码器套件和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](#)本文的[Cisco IOS软件](#)部分的1300和1400系列网桥，请完成在[Aironet](#)解释的同一个步骤[AP](#)。

VxWorks设置

Privacy菜单提交您必须配置的一—组选项。一些选项对于WEP是必需的。此部分注释这些必须选项。其它选项不是必要为了WEP能作用，但是推荐他们。

此部分展示菜单选项按他们在[Privacy菜单的终端仿真器视图](#)出现的顺序。然而，请配置选项按此顺序：

1. 密钥
2. 平湖
3. 验证
4. 客户端
5. 加密

配置按此顺序保证必要的首要条件设置，当您配置每设置。

这些是选项：

- **关键强制性**密钥选项编程加密密钥到网桥。提示您设置四密钥之一。两次提示您输入密钥。为了定义密钥，您必须输入10或26十六进制数字，取决于网桥配置是否是为40位或128-bit密钥。请使用这些位的所有组合：0到9a到fA到F密钥在**所有**节点必须配比在无线电小区，并且您必须输入密钥按同一顺序。只要密钥数量在WLAN的每个设备配比您不需要定义全部四密钥。
- **平湖**平湖选项告诉无线电使用的哪些密钥为了传送数据包。每无线电解密发送与任何四密钥的收到的信息包。
- **验证**您使用中继网桥的验证选项为了确定哪认证模式单元使用其parent连接。允许值是开放或共享密钥。802.11协议指定客户端必须验证与parent的步骤，在客户端能联合前。**打开(推荐)**—验证此模式根本是空操作。所有客户端允许验证。**共享密钥**—此模式允许parent发送客户端质询文本，客户端加密并且返回对parent。如果parent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，同一个数据的明文和已加密版本在空气传送。这不获取什么。如果用户密钥是错误的，单元不解码数据包，并且数据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(推荐)**—验证此模式根本是空操作。所有客户端允许验证。**共享密钥**—此模式允许parent发送客户端质询文本，客户端加密并且返回对parent。如果parent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，不加密完成。数据无危险传送。**在强制性**—如果设置

Encryption选项至开，所有传输的数据数据包加密，并且所有未加密收到的信息包丢弃。**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加密。组播信息包无危险被发送。所有节点能看到数据包。**警告：**请勿使用混合模式。如果安排加密启用的客户端发送组播信息包对其parent，数据包加密。parent解码数据包并且无危险重传数据包到信元，并且其他节点能看到数据包。能力显示在两的一数据包加密和未加密的形式能造成中断密钥。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

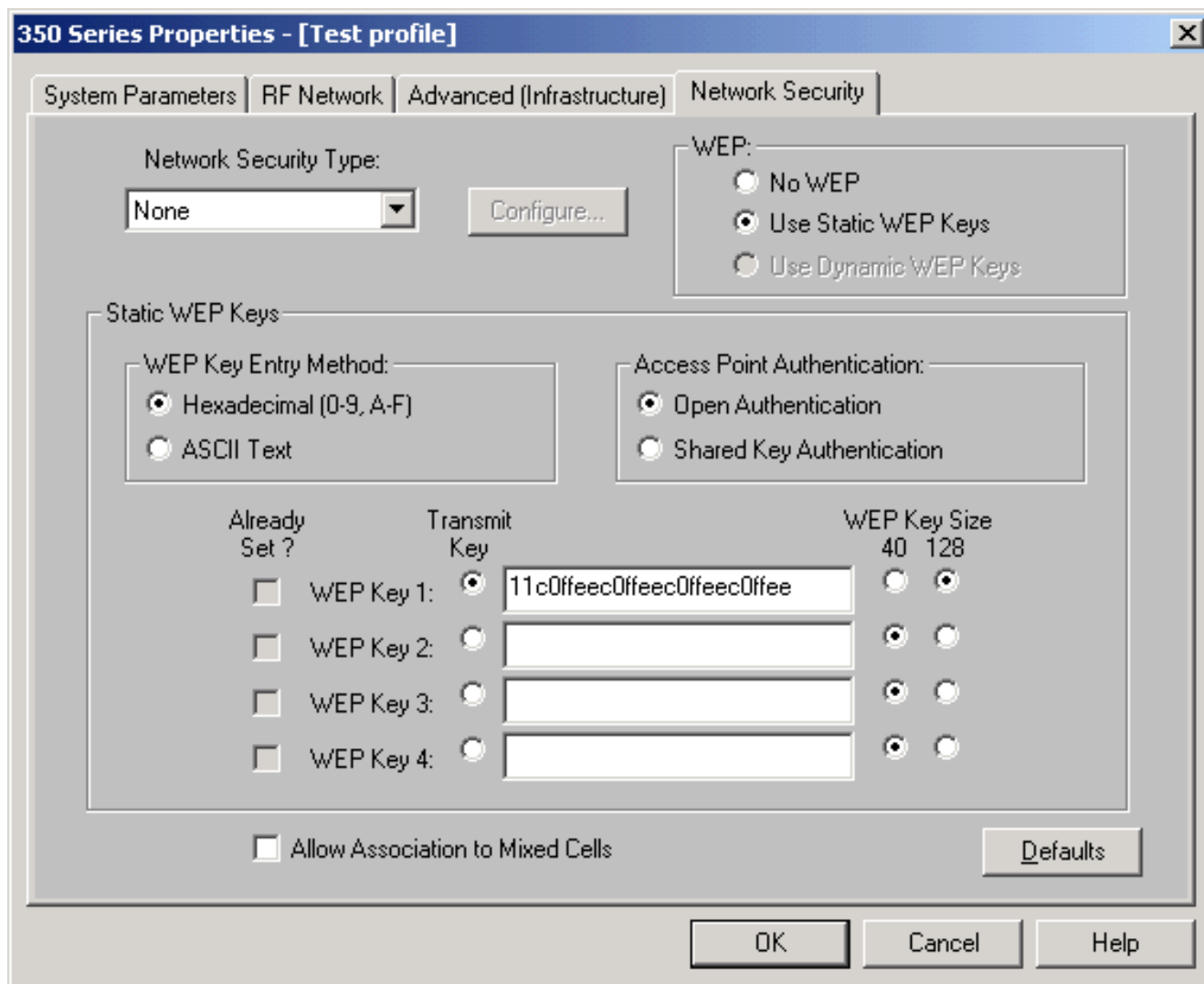
您必须完成两个主要步骤为了设置在Aironet客户端适配器的WEP：

1. 配置WEP密钥/密钥在客户端加密管理器。
2. 启用在Aironet客户端工具(ACU)的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. 选择您要启用WEP并且单击**编辑**的配置文件。
3. 单击**Network Security**选项为了显示安全选项，并且单击**使用静态WEP密钥**。此操作激活黯淡的WEP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个位或128个位在WEP密钥大小下在窗口的右边。**注意**：128-bit客户端适配器能使用40位或128-bit密钥。但是40位适配器能只使用40位密钥。**注意**：您的客户端适配器WEP密钥必须匹配其他WLAN组件您传达使用的WEP密钥。当您集超过一把WEP密钥，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**注意**：Aironet AP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AP。**注意**：在您创建WEP密钥后，您能在它写入。但是您不能编辑或删除它。**注意**：如果使用一个最新版本Aironet Desktop软件(ADU)而不是ACU作为客户端工具，您能也删除已创建WEP密钥和用新的替换它。
5. 点击是在该的密钥之一旁边您创建的**传送密钥**按钮。使用此操作，您表明此密钥是您要使用传送数据包的密钥。
6. 点击**不变**下面WEP密钥类型。此操作允许您的客户端适配器保留此WEP密钥，既使当对适配器的电源删除或在密钥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，当电源从您的客户端适配器时删除。
7. 单击 **Ok**。

启用 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](#)步骤的能配置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. 导航对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. 密钥
2. 平湖
3. 验证
4. 加密

这些是选项：

- **密钥**关键选项设立网桥用途为了收到数据包的WEP密钥。值必须匹配AP或其它设备工作组网桥联络用途的密钥。密钥包括40位加密的10十六进制字符或128-bit加密的26十六进制字符。十六进制字符可以是这些位的所有组合：0到9a到fA到F
- **平湖**平湖选项设立网桥用途为了传送数据包的WEP密钥。您能决定使用您使用关键选项的同一密钥。如果选择不同的密钥，您必须设立在AP的一匹配的密钥。仅一把WEP密钥可以一次使用发射。您使用传送数据的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个值。
- **验证(验证)**验证参数确定哪个验证方法系统使用。选项有：**打开(推荐)**—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AP为用网桥通信。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选项设置在数据包的加密参数，除了关联数据包和一些控制数据包。其中有四个选项：**注意**：AP必须适当地有加密激活和密钥集合。这是默认设置。所有加密被关闭。工作组网桥不连通与与使用的AP WEP。**在(建议使用)**—此设置要求所有数据传输的加密。工作组网桥只连通与使用WEP的AP。**混合**在此设置意味着网桥总是使用WEP为了连通与AP。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为了连通与AP。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。确保您使用同一设置，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。

相关信息

- [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系列户外接入点/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](#)
- [无线\(移动性\)保护的无线网络](#)
- [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](#)