在Aironet接入點和網橋上配置WEP

目錄

簡介

本文提供在Cisco Aironet無線LAN(WLAN)元件上設定有線等效保密(WEP)的方法。

註：有關無線LAN控制器(WLC)上的WEP配置的詳細資訊，請參閱[第6章 — 配置WLAN的靜態Web金鑰](#)**部分。**

WEP是802.11(Wi-Fi)標準中內建的加密演算法。WEP加密使用具有40位或104位金鑰和24位初始化向量(IV)的Ron代碼4(RC4)流密碼。

正如標準所規定的，WEP使用RC4演算法和40位或104位金鑰和24位IV。RC4是對稱演算法，因為它使用相同的金鑰對資料進行加密和解密。啟用WEP後，每個電台「電台」都有一個金鑰。該金鑰用於在通過無線電波傳輸資料之前對資料進行加擾。如果站點收到的資料包未使用相應的金鑰進行加擾，則資料包將被丟棄，並且永遠不會傳送到主機。

WEP主要用於不需要強大安全性的家庭辦公室或小型辦公室。

Aironet WEP實施在硬體中。因此，使用WEP時效能影響最小。

注意：WEP存在一些已知問題，因此它不是一種強加密方法。問題是：

- 維護共用WEP金鑰需要大量管理開銷。

- WEP的問題與基於共用金鑰的所有系統相同。任何透露給某人的秘密都會在一段時間後被公之於眾。
- 種子WEP演算法的IV以明文傳送。
- WEP校驗和是線性且可預測的。

臨時金鑰完整性協定(TKIP)已經建立以解決這些WEP問題。與WEP類似，TKIP使用RC4加密。但是，TKIP通過新增諸如每資料包金鑰雜湊、消息完整性檢查(MIC)和廣播金鑰輪替等措施來增強WEP，以解決WEP的已知漏洞。TKIP使用RC4流密碼和128位金鑰進行加密，64位金鑰進行身份驗證。

必要條件

需求

本檔案假設您可以建立與WLAN裝置的管理連線，且裝置在未加密環境中正常運作。

要配置標準40位WEP，您必須有兩個或多個無線電單元相互通訊。

注意：Aironet產品可與符合IEEE 802.11b的非思科產品建立40位WEP連線。本文檔不介紹其他裝置的配置。

為了建立128位WEP連結，思科產品只能與其他思科產品互動。

採用元件

將以下元件與本文檔配合使用：

- 相互通訊的兩個或多個無線電單元
- 到WLAN裝置的管理連線

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

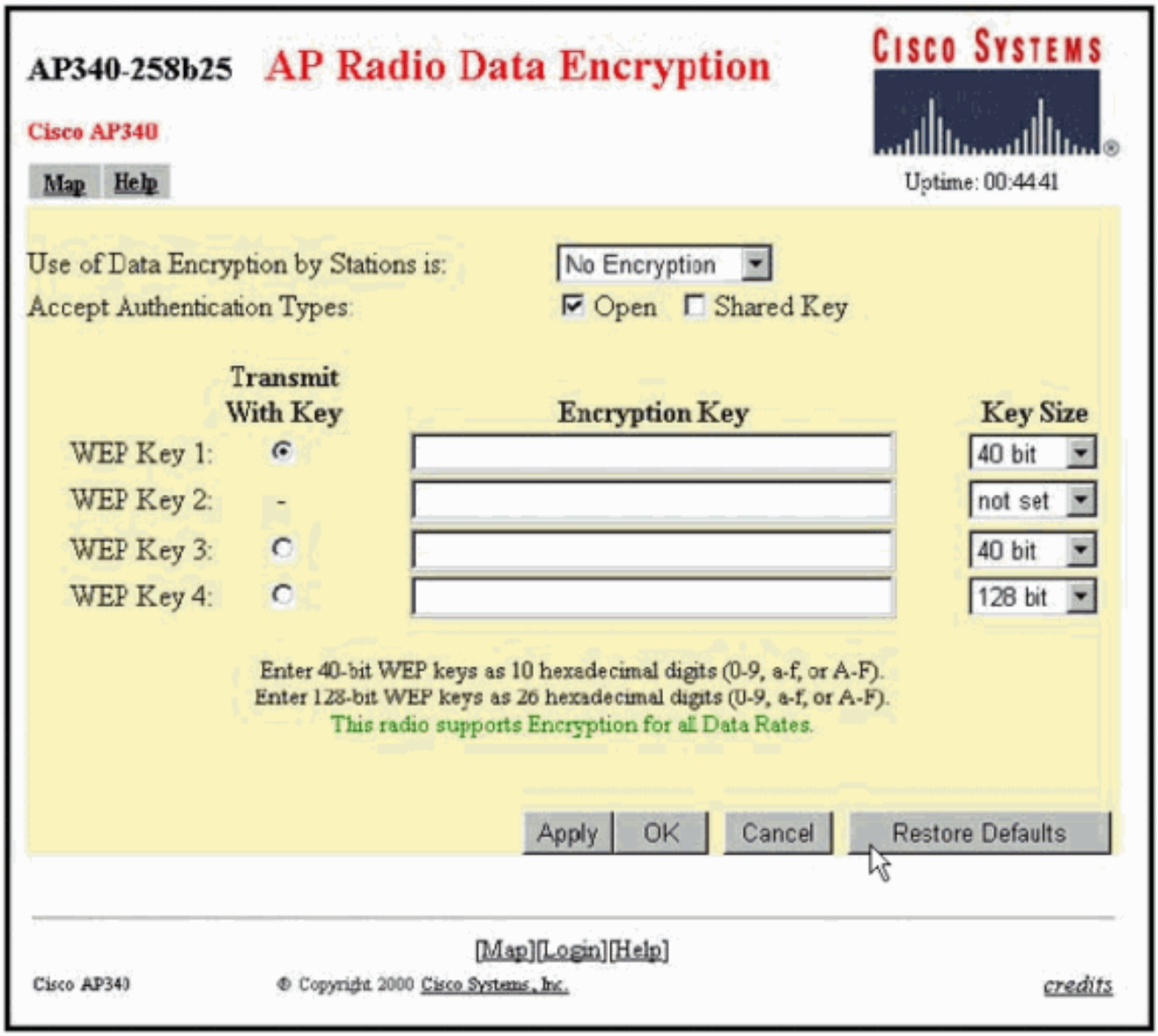
如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

在Aironet接入點上配置WEP

執行VxWorks作業系統的Aironet存取點

請完成以下步驟：

1. 連線到接入點(AP)。
2. 導航到AP無線電加密選單。使用以下路徑之一：**Summary Status > Setup > AP Radio/Hardware > Radio Data Encryption(WEP)> AP Radio Data EncryptionSummary Status > Setup > Security > Security Setup:無線電資料加密(WEP)> AP無線電資料加密注意**：要對此頁面進行更改，您必須是具有身份和寫入功能的管理員。**AP無線電資料加密選單的Web瀏覽器檢視**



VxWorks設定

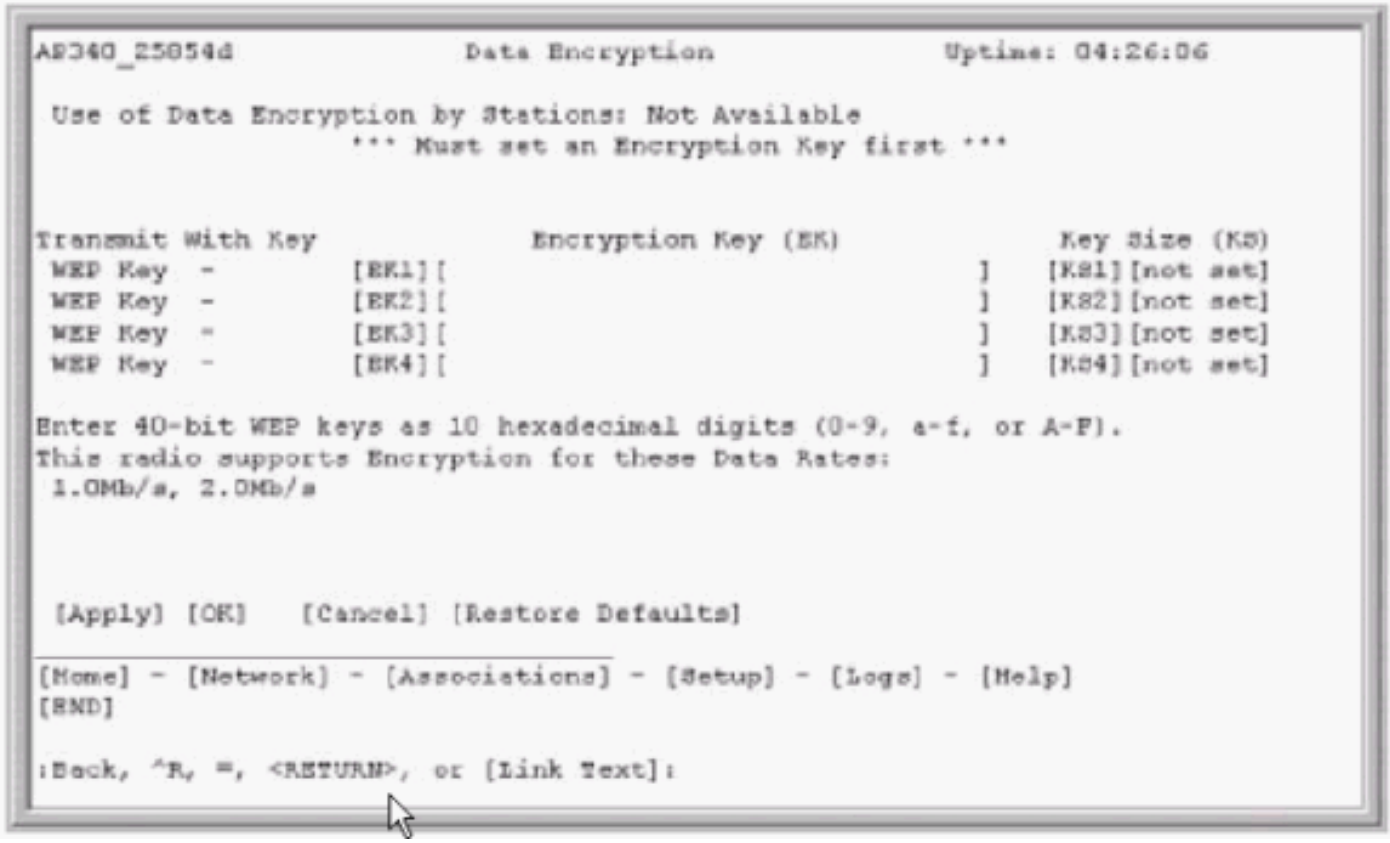
AP Radio Data Encryption頁面提供了各種要使用的選項。某些選項對於WEP是強制性的。本節將註明這些必填選項。其他選項對WEP正常運行不是必需的，但建議使用。

- **工作站對資料加密的使用：**使用此設定可以選擇客戶端與AP通訊時是否必須使用資料加密。下拉選單列出了三個選項：**無加密（預設）** — 要求客戶端在不進行任何資料加密的情況下與AP通訊。不建議使用此設定。**可選** — 允許客戶端使用或不使用資料加密與AP通訊。通常，當您有無法建立WEP連線的客戶端裝置（例如128位WEP環境中的非思科客戶端）時，會使用此選項。**完全加密（推薦）** — 要求客戶端在與AP通訊時使用資料加密。不使用資料加密的客戶端不允許通訊。如果您希望最大限度地提高WLAN的安全性，建議使用此選項。**注意：**啟用加密使用之前，必須設定WEP金鑰。請參見此清單的**加密金鑰(MANDATORY)**部分。
- **接受身份驗證型別**您可以選擇「開啟」、「共用金鑰」或這兩個選項，以設定AP將識別的身份驗證。**Open(RECOMMENDED)** — 此預設設定允許任何裝置（無論其WEP金鑰如何）進行身份驗證並嘗試關聯。**Shared Key** — 此設定指示AP向嘗試與AP關聯的任何裝置傳送純文字檔案共用金鑰查詢。**注意：**此查詢可能使AP處於開啟狀態，容易遭到入侵者的已知文本攻擊。因此，此設定不如開放設定安全。
- **使用金鑰傳輸**這些按鈕允許您選擇AP在資料傳輸期間使用的金鑰。一次只能選擇一個金鑰。任何或全部設定鍵均可用於接收資料。您必須先設定金鑰，然後才能將其指定為Transmit Key。

- **加密金鑰（必填）**這些欄位允許您輸入WEP金鑰。為40位WEP金鑰輸入10個十六進位制數字，為128位WEP金鑰輸入26個十六進位制數字。金鑰可以是以下數字的任意組合：0到9a到fA到F為了保護WEP金鑰安全，現有的WEP金鑰不會以純文字檔案顯示在輸入欄位中。在最新版本的AP中，您可以刪除現有金鑰。但是，不能編輯現有金鑰。**注意：**必須以完全相同的方式為網路、AP和客戶端裝置設定WEP金鑰。例如，如果您將AP上的WEP金鑰3設定為0987654321並選擇該金鑰作為活動金鑰，則還必須將客戶端裝置上的WEP金鑰3設定為相同的值。
- **金鑰大小（必填）**此設定將金鑰設定為40位或128位WEP。如果對此選擇顯示「not set」，則表示未設定金鑰。**注意：**不能通過選擇「not set」刪除金鑰。
- **操作按鈕**四個操作按鈕控制設定。如果在Web瀏覽器上啟用了JavaScript，則在按一下除「取消」之外的任何按鈕後，將出現一個確認彈出視窗。Apply — 此按鈕啟用新值設定。瀏覽器仍保留在頁面上。OK — 此按鈕應用新設定並將瀏覽器移回主設定頁面。Cancel — 此按鈕可取消設定更改並將設定返回到以前儲存的值。然後返回主設定頁。**恢復默**認值 — 此按鈕將此頁面上的所有設定更改回出廠預設設定。

註：在最新版本的Cisco IOS® AP中，此頁只可用Apply和Cancel控制按鈕。

資料加密選單的終端模擬器檢視



WEP金鑰配置序列的終端模擬器檢視(Cisco IOS®軟體)

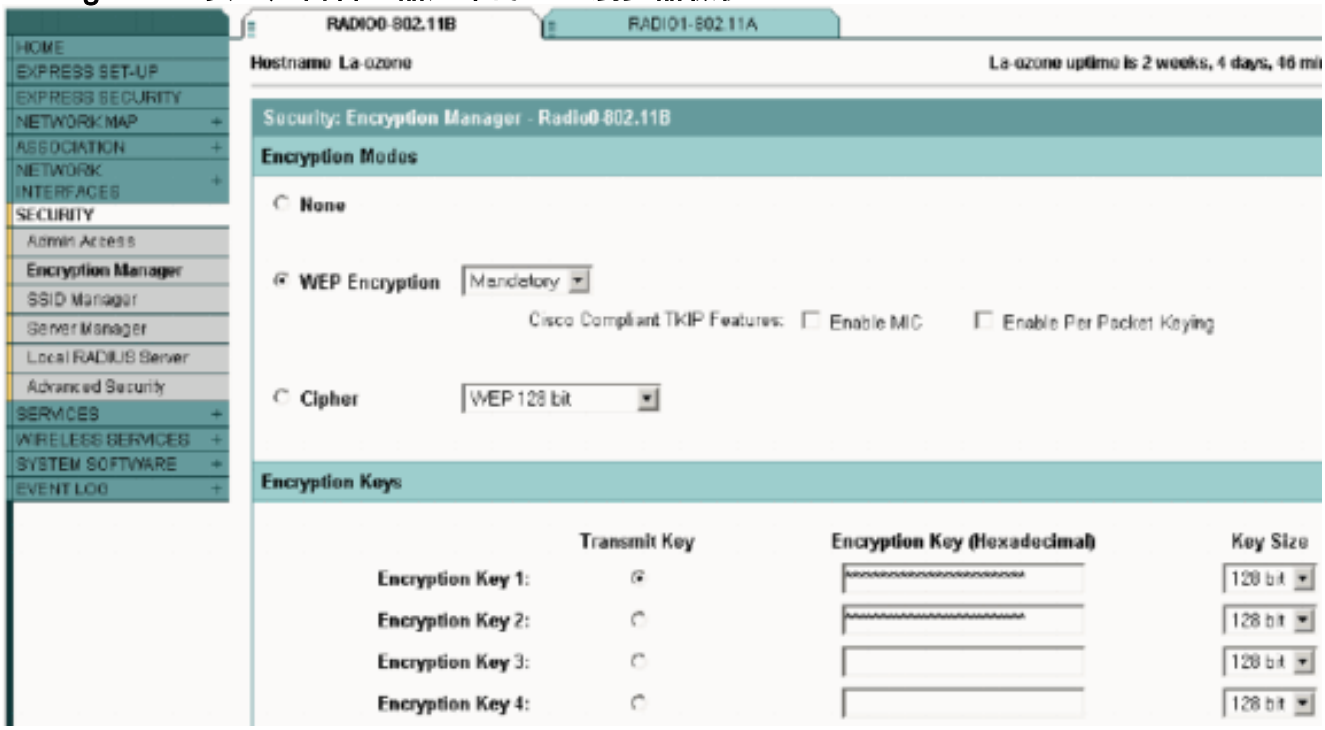
```
La-ozone>
La-ozone>
La-ozone>enable
Password:
La-ozone#
La-ozone#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
La-ozone(config)#interface dot
La-ozone(config)#interface dot11Radio 0
La-ozone(config-if)#encryption key 1 size 128bit 11c0ffeec0ffeec0ffeec0ffee ?
 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

執行Cisco IOS軟體的Aironet AP

請完成以下步驟：

1. 建立與AP的連線。
2. 從視窗左側的SECURITY選單選項中，為要配置靜態WEP金鑰的無線電介面選擇**Encryption Manager**。**AP安全加密管理器選單的Web瀏覽器檢視**



配置Aironet網橋

如果使用VxWorks，請完成以下步驟：

1. 連線到網橋。
2. 導航到「隱私」選單。選擇**Main Menu > Configuration > Radio > I80211 > Privacy**。「隱私」選單控制對無線電通過無線傳輸的資料包使用加密。RSA RC4演算法和最多四個已知金鑰中的一個用於加密資料包。無線電蜂窩中的每個節點必須知道所有正在使用的金鑰，但是可以選擇任何金鑰來傳輸資料。**隱私選單的終端模擬器檢視**

```
        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
>_
```

有關如何通過CLI模式在1300和1400系列網橋中配置WEP的資訊，請參閱配置密碼套件和WEP - 1300系列網橋和配置WEP和WEP功能 — 1400系列網橋。

若要使用GUI設定1300和1400系列橋接器，請完成本檔案執行Cisco IOS軟體的Aironet AP一節中說明的程式。

VxWorks設定

「隱私」選單提供一組必須配置的選項。某些選項對於WEP是強制性的。本節將註明這些必填選項。其他選項對WEP正常運行不是必需的，但建議使用。

本部分按照選單選項在Privacy選單的Terminal Emulator View中的顯示順序顯示這些選單選項。但是，請按以下順序配置選項：

1. 主要
2. 傳輸
3. 身份驗證
4. 使用者端
5. 加密

按此順序配置可確保配置每個設定時設定必要的先決條件。

以下是選項：

- **金鑰（必填）**Key選項將加密金鑰程式設計到網橋中。系統將提示您設定四個鍵之一。系統提示您輸入金鑰兩次。要定義金鑰，必須輸入10或26個十六進位制數字，這取決於網橋配置是用於40位還是128位金鑰。使用以下數字的任意組合：0到9a到fA到F在無線電單元格的所有***節點***中，金鑰必須匹配，並且必須以相同順序輸入金鑰。您無需定義所有四個金鑰，只要WLAN中每台裝置中的金鑰數量匹配。
- **傳輸**Transmit選項告知無線電使用哪些金鑰來傳輸資料包。每個無線電都能夠解密使用四個金鑰中的任何一個金鑰傳送的接收資料包。
- ***身份驗證***您可以在中繼器網橋上使用Auth選項，以確定裝置使用哪種身份驗證模式與其父裝置連線。允許的值為Open或Shared Key。802.11協定指定了一個過程，在該過程中，客戶端必須首先與父級進行身份驗證，然後客戶端才能進行關聯。Open(RECOMMENDED) — 此身份驗證模式本質上是一個空操作。允許所有使用者端進行驗證。**共用金鑰** — 此模式允許父級向客戶端傳送質詢文本，客戶端將加密該文本並返回給父級。如果父級成功解密質詢文本，則對客戶端進行身份驗證。**注意：**請勿使用共用金鑰模式。當您使用它時，相同資料的純文字檔案和加密版本會在空中傳輸。這不會得到任何好處。如果使用者金鑰錯誤，則裝置不會解密資料包，並且資料包無法訪問網路。
- **使用者端**客戶端選項確定客戶端節點用於與裝置關聯的身份驗證模式。以下是允許的值：Open(RECOMMENDED) — 此身份驗證模式本質上是一個空操作。允許所有使用者端進行

驗證。**共用金鑰** — 此模式允許父級向客戶端傳送質詢文本，客戶端將加密該文本並返回給父級。如果父級成功解密質詢文本，則對客戶端進行身份驗證。**Both** — 此模式允許客戶端使用任一模式。

- **加密Off** — 如果將Encryption選項設定為Off，則不執行加密。資料以透明方式傳輸。**On(MANDATORY)**-如果將Encryption選項設定為On ，則所有傳輸的資料包都會被加密，所有未加密的接收資料包都會被丟棄。**Mixed** — 在混合模式下，根網橋或中繼器網橋接受來自開啟或關閉加密的客戶端的關聯。在這種情況下，僅加密兩個支援的節點之間的資料包。組播資料包以明文形式傳送。所有節點都可以看到資料包。**注意：**請勿使用混合模式。如果啟用了加密的客戶端將組播資料包傳送到其父節點，則該資料包將被加密。父節點解密資料包並以明文形式將資料包重新傳輸到信元，其他節點可以看到該資料包。以加密形式和非加密形式檢視資料包的功能都有助於破解金鑰。混合模式僅用於與其他供應商的相容性。

配置客戶端介面卡

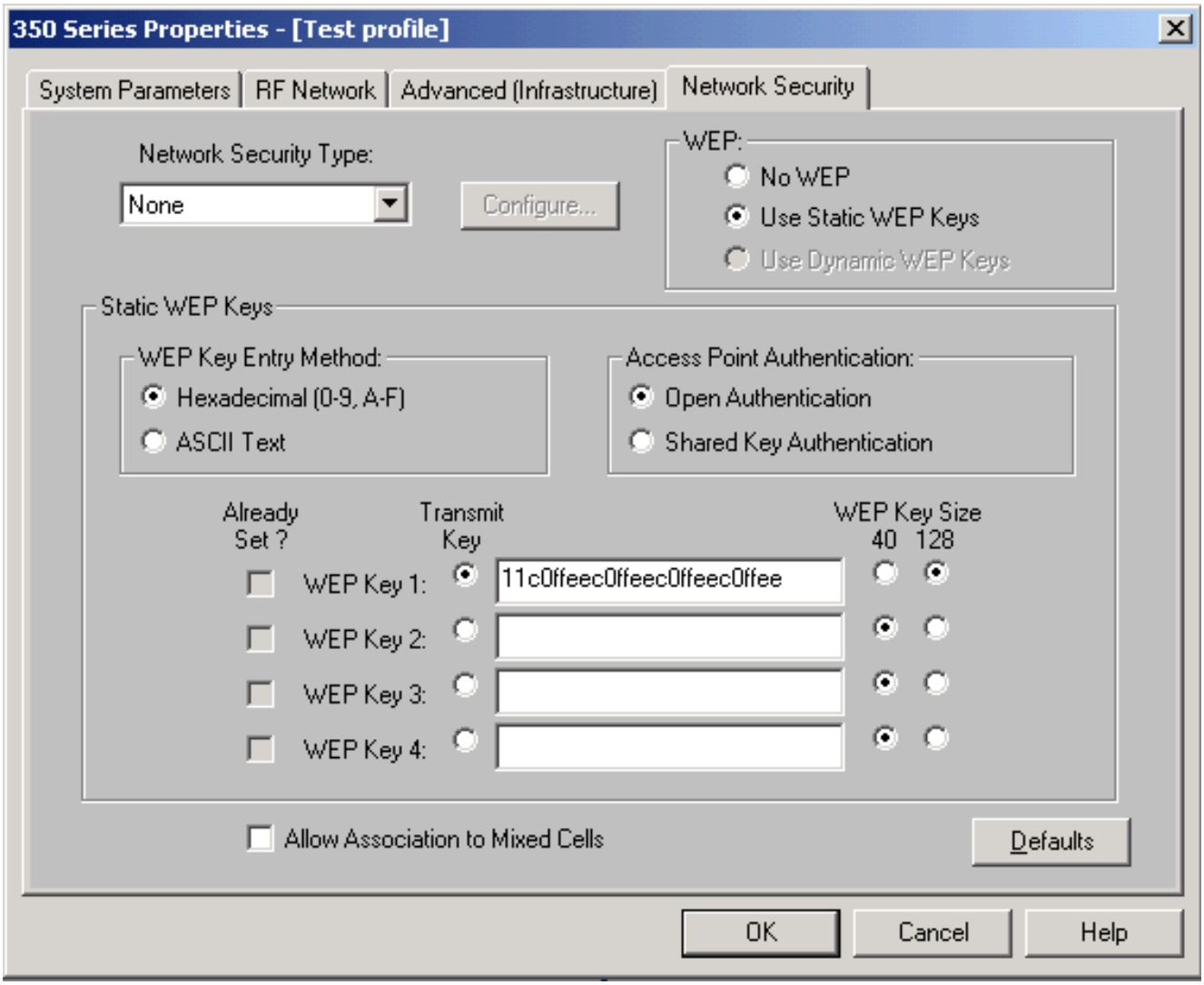
要在Aironet客戶端介面卡上設定WEP，必須完成兩個主要步驟：

1. 在客戶端加密管理器中配置WEP金鑰。
2. 在Aironet客戶端實用程式(ACU)中啟用WEP。

設定WEP金鑰

完成以下步驟，在客戶端介面卡上設定WEP金鑰：

1. 開啟ACU並選擇**Profile Manager**。
2. 選擇要啟用WEP的配置檔案，然後按一下**Edit**。
3. 按一下**Network Security**頁籤以顯示安全選項，然後按一下**Use Static WEP Keys**。此操作會啟用WEP配置選項，如果選擇「無WEP」，這些選項將變暗。



4. 對於要建立的WEP金鑰，在視窗右側WEP金鑰大小下選擇**40**位或**128**位。**注意**：128位客戶端介面卡可以使用40位或128位金鑰。但40位介面卡只能使用40位金鑰。**注意**：您的客戶端介面卡WEP金鑰必須與您與之通訊的其他WLAN元件使用的WEP金鑰匹配。當您設定多個WEP金鑰時，您必須為所有裝置將WEP金鑰分配到相同的WEP金鑰編號。WEP金鑰必須由十六進位制字元組成，對於40位WEP金鑰必須包含10個字元，對於128位WEP金鑰必須包含26個字元。十六進位制字元可以是：0到9a到fA到F**注意**：Aironet AP不支援ASCII文本WEP金鑰。因此，如果計畫對這些AP使用客戶端介面卡，則必須選擇十六進位制(0-9, A-F)選項。**注意**：建立WEP金鑰後，您可以對金鑰進行寫操作。但您不能編輯或刪除它。**注意**：如果您使用較新版本的Aironet Desktop Utility(ADU)而不是ACU作為客戶端實用程式，您還可以刪除建立的WEP金鑰並將其替換為新的WEP金鑰。
5. 按一下您建立的一個金鑰旁邊的**Transmit Key**按鈕。通過此操作，您指示此金鑰是要用於傳輸資料包的金鑰。
6. 按一下WEP Key Type下的**Persistent**。此操作允許您的客戶端介面卡保留此WEP金鑰，即使刪除了介面卡的電源或在安裝了金鑰的電腦重新啟動時也是如此。如果對此選項選擇Temporary（臨時），則從客戶端介面卡上拔下電源時，WEP金鑰將丟失。
7. 按一下「**OK**」（確定）。

啟用WEP

請完成以下步驟：

1. 開啟ACU，然後從選單欄中選擇**Edit Properties**。

2. 按一下**Network Security**頁籤以顯示安全選項。
3. 勾選「**Enable WEP**」覈取方塊以啟用WEP。

有關使用ADU作為客戶端實用程式配置WEP的步驟，請參閱在ADU中配置WEP。

配置工作組網橋

Aironet 340系列工作組網橋和Aironet 340系列網橋之間存在差異。但是，工作組網橋使用WEP的配置與網橋的配置幾乎完全相同。有關網橋的配置，請參閱配置Aironet網橋部分。

1. 連線到工作組橋。
2. 導航到「隱私」選單。選擇**Main > Configuration > Radio > I80211 > Privacy**以訪問Privacy VxWorks選單。

設定

「隱私」選單將顯示此部分列出的設定。按以下順序在工作組橋上配置選項：

1. 主要
2. 傳輸
3. 身份驗證
4. 加密

以下是選項：

- **主要**Key選項建立網橋用於接收資料包時使用的WEP金鑰。該值必須與AP或工作組網橋與之通訊的其他裝置使用的金鑰相匹配。該金鑰最多包含10個十六進位制字元用於40位加密，26個十六進位制字元用於128位加密。十六進位制字元可以是以下數字的任意組合：0到9a到fA到F
- **傳輸**Transmit選項建立網橋用於傳輸資料包的WEP金鑰。您可以選擇使用與「鍵」選項相同的鍵。如果選擇其他金鑰，必須在AP上建立匹配的金鑰。一次只能使用一個WEP金鑰進行傳輸。在工作組橋和其他與其通訊的裝置上，用於傳輸資料的WEP金鑰必須設定為相同的值。
- **驗證(Auth)**Auth引數確定系統使用的身份驗證方法。選項包括：**Open（建議）** — 預設的Open設定允許任何AP（無論其WEP設定如何）進行身份驗證，然後嘗試與網橋通訊。**共用密鑰** — 此設定指示網橋向AP傳送純文字檔案共用金鑰查詢，以嘗試與網橋通訊。Shared Key設定可能會使網橋對入侵者的已知文本攻擊保持開啟狀態。因此，此設定不如開放設定安全。
- **加密**Encryption選項為所有資料包（關聯資料包和一些控制資料包除外）設定加密引數。有四個選項：**注意：**AP必須啟用加密並正確設定金鑰。**Off** — 這是預設設定。所有加密都關閉。工作組網橋無法使用WEP與AP通訊。**開啟（推薦）** — 此設定要求對所有資料傳輸進行加密。工作組橋只與使用WEP的AP通訊。**Mixed on** — 此設定意味著網橋始終使用WEP與AP通訊。但是，AP會與所有裝置通訊，無論它們使用WEP還是不使用WEP。**Mixed off** — 此設定表示網橋不使用WEP與AP通訊。但是，AP會與所有裝置通訊，無論它們使用WEP還是不使用WEP。**注意：如**果選擇On或Mixed on作為WEP類別，並通過網橋的無線電鏈路配置網橋，則當您錯誤設定WEP金鑰時，網橋將失去連線。確保在工作組橋上設定WEP金鑰以及在WLAN上的其他裝置上設定WEP金鑰時使用完全相同的設定。

相關資訊

- IEEE標準協會
- Aironet 340系列無線LAN產品

- 無線支援資源
- 無線LAN支援頁面
- 適用於Cisco Aironet存取點的Cisco IOS軟體組態指南
- 適用於Cisco Aironet 1300系列室外存取點/橋接器的Cisco IOS軟體組態指南
- 適用於VxWorks的Cisco Aironet存取點軟體組態設定指南
- Cisco Aironet 1400系列網橋軟體配置指南
- Cisco Aironet無線區域網客戶端介面卡配置指南
- Cisco無線LAN安全概觀
- 無線（移動）保護無線網路
- 接入點作為工作組網橋的配置示例
- Cisco Aironet Workgroup Bridge常見問題
- Cisco Aironet裝置的密碼復原程式
- Cisco Aironet接入點常見問題
- 技術支援與文件 - Cisco Systems