Aironet アクセス ポイントおよびブリッジの Wired Equivalent Privacy（WEP）の設定例

目次

概要

このドキュメントでは、Cisco Aironet Wireless LAN（WLAN）コンポーネントに Wired Equivalent Privacy（WEP）を設定する方法について説明します。

注: 章の第 6 静的な Web キー セクションを-ワイヤレス LAN コントローラ（WLCs）の WEP 設定に関する詳細については WLAN を設定すること参照して下さい。

WEP は 802.11 標準（Wi-Fi）に組み込まれている暗号化アルゴリズムです。 WEP暗号化は 40-と Ron のコード 4 （RC4）ストリーム暗号か 104-bit キーおよび 24 ビット 初期化ベクトル（iv）使用します。

規格が規定 すると同時に、WEP は 40 ビットによって RC4 アルゴリズムを使用しますまたは暗号化のために同じキーおよびデータの復号化を使用するので 104-bit キーおよび 24 ビット IV. RC4 は対称アルゴリズムです。 WEP をイネーブルにすると、各無線「ステーション」にはキーが配備されます。 このキーは、電波を介してデータを送信する前に、データをスクランブルするために使用されます。 あるステーションが適切なキーでスクランブルされていないパケットを受信すると、そのパケットは廃棄され、ホストに配信されません。

WEP は家庭内オフィスか強い セキュリティを非常に必要としないスモールオフィスに主に使用

することができます。

Aironet の WEP はハードウェアで実装されています。 したがって、WEP の使用によるパフォーマンスへの影響は最小限です。

注: それにない強化暗号化 方式をする WEP においてのいくつかの既知の問題があります。 これらの問題には次のようなものがあります。

- 共用 WEPキーを維持する大量の管理上のオーバーヘッドがあります。
- WEP に共有鍵に基づいてすべてのシステムと同じ問題があります。 1 人に与えられるどのシークレットでもしばらくすると公共になります。
- WEP アルゴリズムをシードする IV はクリアテキストで送信 されます。
- WEP チェックサムはリニアおよび予想できます。

Temporal Key Integrity Protocol （ TKIP ）はこれらの WEP 問題に対処するために作成されました。 WEP と同様に、TKIP は RC4 暗号化を使用します。 ただし、TKIP はパケットごとのキーハッシュのような手段の、Message Integrity Check （ MIC ）追加によって WEP を高め、ブロードキャストは WEP の既知の脆弱性に対処するためにローテーションをキー入力します。 TKIP は暗号化のために 128-bit キーおよび認証のために 64 ビット キーによって RC4 ストリーム暗号を使用します。

前提条件

要件

このドキュメントでは、WLAN デバイスへ管理接続できること、また暗号化のない環境でデバイスが正常に機能することが前提となっています。

標準的な 40 ビットの WEP を設定するには、2 つ以上の相互に通信する無線装置が必要です。

注: Aironet 製品は、IEEE 802.11b に準拠するシスコ以外の製品との 40 ビット WEP 接続を確立できます。 このドキュメントでは、他のデバイスの設定は扱われていません。

128 ビット WEP リンクを作成する場合、シスコ製品は他のシスコ製品とだけ相互動作を行います。

使用するコンポーネント

このドキュメントでは、次のコンポーネントを使用します。

- 相互に通信する 2 つ以上の無線装置
- WLAN デバイスへの管理接続

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

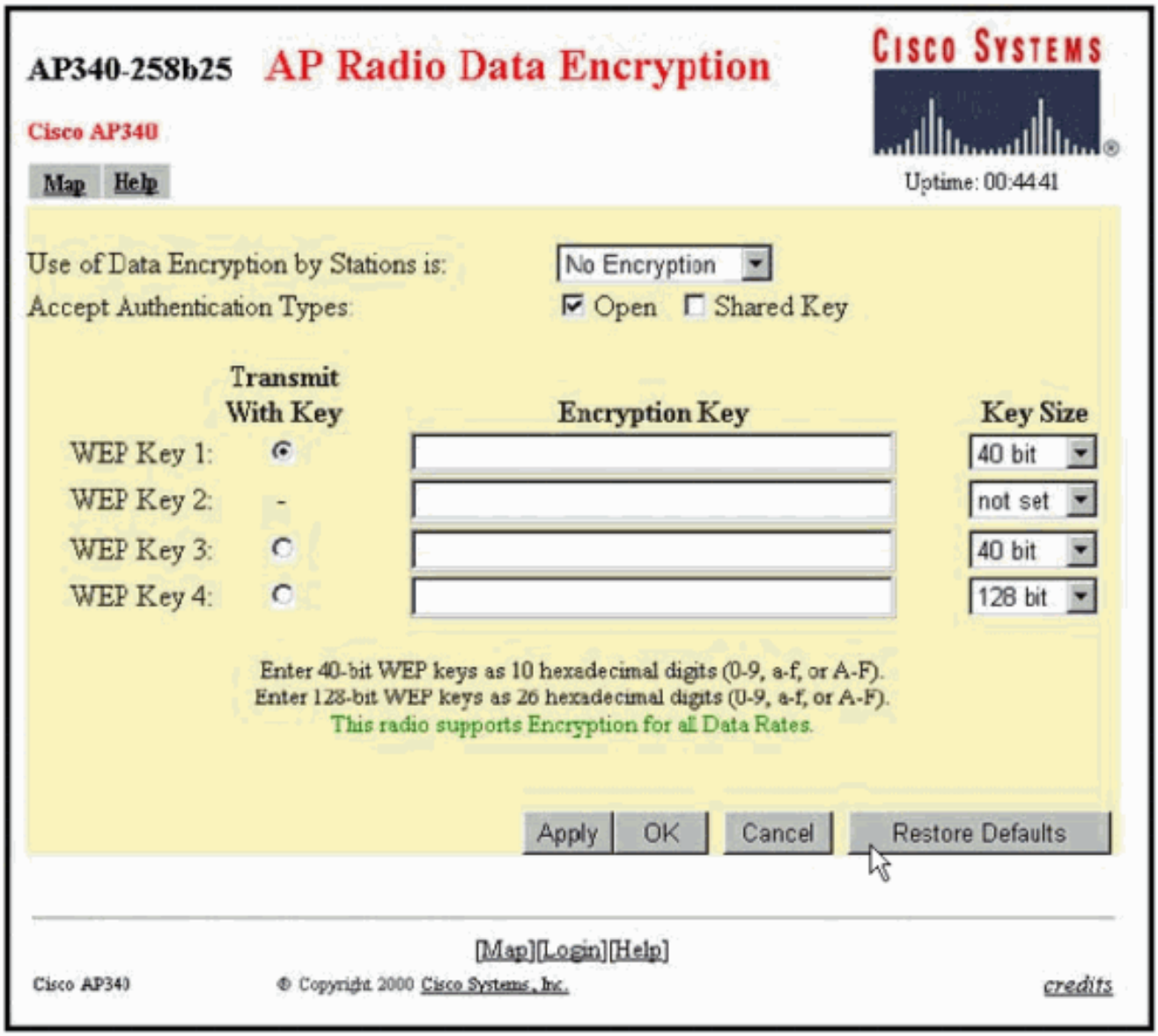
ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

Aironetアクセスポイントの WEP を設定して下さい

VxWorks オペレーティングシステムを実行する Aironetアクセスポイント

次の手順を実行します。

1. アクセス ポイント（AP）へ接続します。
2. AP Radio Encryption メニューへ移動します。次のパスのうち 1 つを使用します。**[Summary Status] > [Setup] > [Security] > [Security Setup:Radio Data Encryption (WEP)] > [AP Radio Data Encryption]Summary Status > Setup > Security > Security Setup: Radio Data Encryption（WEP）> AP Radio Data Encryption注:** このページで変更を行うには、Identity および Write の許可を持つ管理者である必要があります。**AP Radio Data Encryption メニューのブラウザ表示**



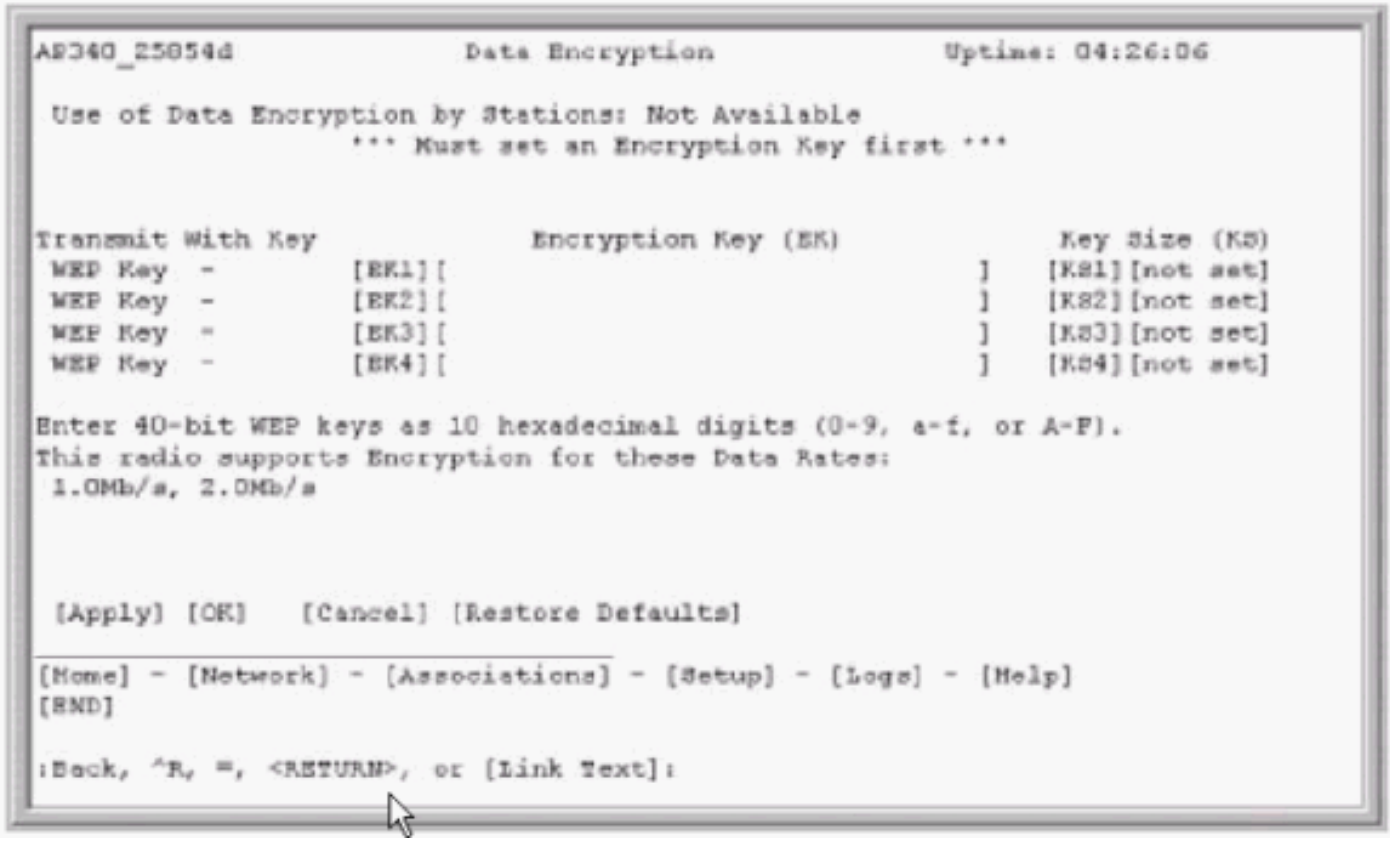
VxWorks の設定

AP Radio Data Encryption ページに、使用できるさまざまなオプションが表示されます。 一部のオプションは WEP に必須です。 このセクションでは、それらの必須オプションを取り上げます。 他のオプションは WEP の機能に必須ではありませんが、推奨されます。

- **[Use of Data Encryption by Stations] とは**この設定は、クライアントが AP との通信でデータ暗号化を使用するかどうかを選択するためのものです。 プルダウン メニューに次の 3 つのオプションが表示されます。**No encryption（デフォルト）**—クライアントがデータ暗号化なしで AP と通信するように要求します。 この設定は推奨されません。[Optional]：クライアントに対しデータ暗号化ありまたはなしで AP と通信することを許可します。 通常、このオプションは、シスコ以外のクライアントなど WEP 接続を行えないクライアント デバイスが 128 ビットの WEP 環境に含まれている場合に使用します。**Full Encryption（推奨）**— AP と通信するときクライアントがデータ暗号化を使用するように要求します。 データ暗号化を使用しないクライアントは通信できません。 この暗号化オプションは、WLAN のセキュリティを最大にする場合に推奨されます。**注:** 暗号化の使用を有効にする前に、WEP キーを設定する必要があります。 詳細については、この箇条書きの「Encryption Key（必須）」を参照してください。
- **Accept Authentication Types**Open、Shared Key、またはその両方のオプションを選択することで、AP にどのように認証を認識させるかを設定できます。**Open（推奨）**—このデフォルト設定は、WEPキーに関係なく、デバイスが認証し、関連付けるように試みるようにします。**共有鍵**—この設定は AP を AP と関連付けるように試みるあらゆるデバイスにプレーンテキストを、共有鍵クエリー 送信 するように告げます。**注:** このクエリによって、AP が侵入者からの既知のテキストによる攻撃にさらされる可能性があります。 したがって、この設定は「Open」ほどセキュアではありません。
- **Transmit With Key**このボタンで、データ送信時に AP が使用するキーを選択できます。 一度に選択できるのは 1 つのキーだけです。 データの受信には、設定されている任意またはすべてのキーを使用できます。 キーを Transmit Key に指定する前に、そのキーを設定しておく必要があります。
- **Encryption Key（必須）**このフィールドを使用して、WEP キーを入力できます。 40 ビット WEP キーには 10 桁の 16 進値、また 128 ビットの WEP キーには 26 桁の 16 進値を入力します。 キーには次の文字を任意に組み合わせることができます。0 ~ 9a 〜 fA ~ FWEPキーセキュリティを保護するために、既存の WEPキーは入力フィールドの平文に書かれていません。 AP の最近のバージョンでは、既存のキーを削除できます。 ただし、既存のキーを編集できません。**注:** ネットワーク、AP、およびクライアント デバイスで、まったく同様に WEP キーを設定する必要があります。 たとえば、AP の WEP キー 3 を 0987654321 に設定し、このキーをアクティブなキーとして選択したら、クライアント デバイスでも WEP Key 3 を同じ値に設定する必要があります。
- **Key Size（必須）**この設定では、キーが 40 ビットまたは 128 ビットの WEP に設定されます。 選択肢に「not set」と表示されていたら、キーは設定されていません。**注:**「not set」を選択してキーを削除することはできません。
- **Action Buttons**4 つのアクション ボタンで設定を管理します。 ブラウザで JavaScript が有効になっている場合は、Cancel 以外のボタンをクリックした後、確認のポップアップ ウィンドウが表示されます。**apply** —このボタンは New 値設定をアクティブにします。 ブラウザは、そのページのままです。OK— このボタンを押すと新規設定を適用し、ブラウザをメインの [Setup] ページに戻します。**キャンセル**—このボタンは設定変更を取り消し、保存 された 値に設定を以前に戻します。 Setup のメインページに戻ります。**復元 デフォルト**—このボタンは工場出荷時のデフォルト設定にこのページのすべての設定を戻します。

注: AP の Cisco 最近の IOS® バージョンでは、**適用だけ**および**キャンセル**制御ボタンはこのページに利用できます。

Data Encryption メニューのターミナル エミュレーション表示



WEP Key Configuration Sequence（Cisco IOS(R) ソフトウェア）のターミナル エミュレーション表示

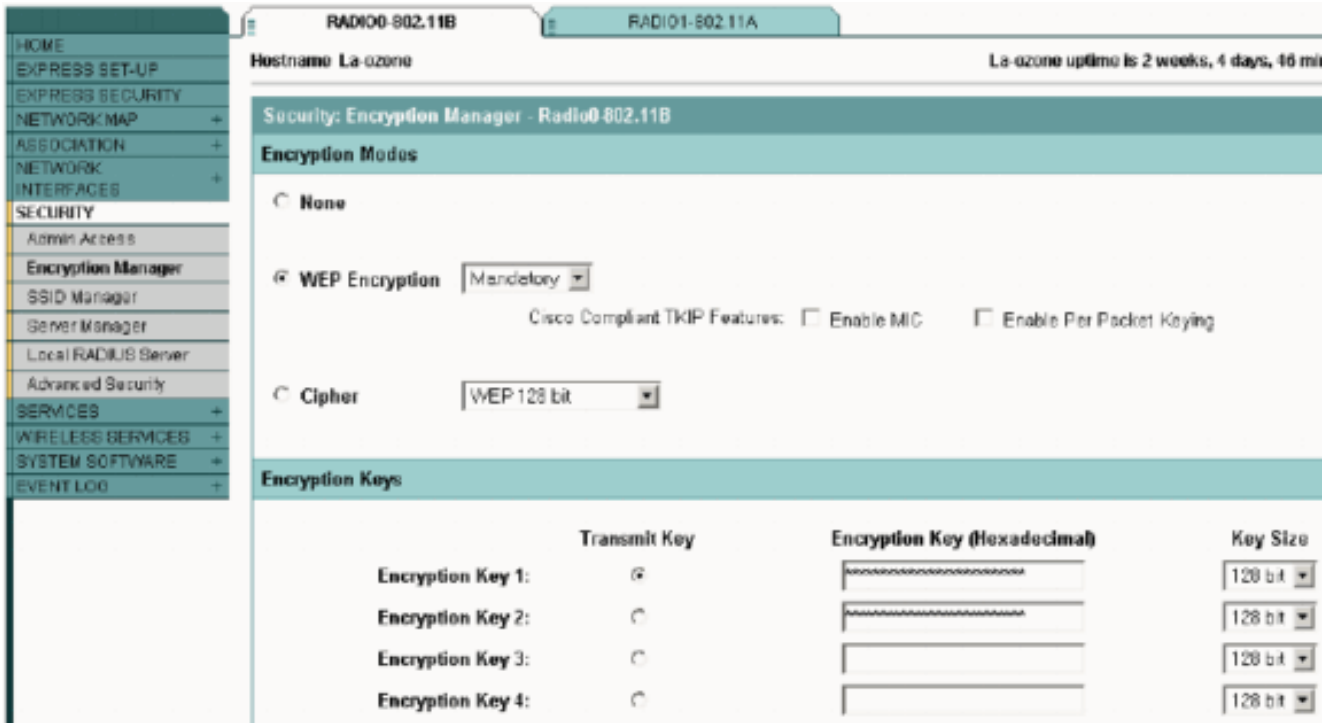
```
La-ozone>
La-ozone>
La-ozone>enable
Password:
La-ozone#
La-ozone#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
La-ozone(config)#interface dot
La-ozone(config)#interface dot11Radio 0
La-ozone(config-if)#encryption key 1 size 128bit 11c0ffeec0ffeec0ffeec0ffee ?
 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

Cisco IOSソフトウェアを実行する Aironet AP

次の手順を実行します。

1. アクセス ポイント（AP）へ接続します。
2. ウィンドウの左側にある SECURITY メニュー オプションから、スタティックな WEP キーを設定する無線インターフェイスに Encryption Manager を選択します。**AP Security Encryption Manager メニューのブラウザ表示**



設定 Aironetブリッジ

VxWorks を使用する場合は、次の手順を実行します。

1. ブリッジへ接続します。
2. Privacy メニューに移動します。Main Menu > Configuration > Radio > I80211 > Privacy の順に選択 して下さい。Privacy メニューは、無線で空中を伝送されるデータ パケットに対する暗号化の使用方法を制御します。 パケットの暗号化には、RSA RC4 のアルゴリズムと、4 つまでの既知のキーのうち 1 つを使用します。 無線セル内の各ノードは、使用中のキーをすべて知っている必要がありますが、そのうちのどのキーをデータ伝送に使用してもかまいません。**Privacy メニューのターミナル エミュレーション表示**

```
        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
>_
```

暗号スイートおよび WEP の設定を- 1300 シリーズ ブリッジおよび WEP および WEP 機能設定すること- CLI モードによって 1300 および 1400 シリーズ ブリッジの WEP を設定する方法の情報に関しては 1400 シリーズ ブリッジ参照して下さい。

GUI をこの資料の Cisco IOSソフトウェア セクションを実行する 1300 および 1400 シリーズ ブリッジを設定するのに使用するために Aironet AP で説明される同じプロシージャを完了して下さい。

VxWorks の設定

Privacy メニューには、設定する一連のオプションが表示されます。 一部のオプションは WEP に必須です。 このセクションでは、それらの必須オプションを取り上げます。 他のオプションは WEP の機能に必須ではありませんが、推奨されます。

このセクションでは、Privacy メニューのターミナル エミュレーション表示に表示される順序でメニュー オプションを紹介します。 ただし、この順序でオプションを設定して下さい:

1. キー
2. 送信側
3. Auth
4. クライアント
5. 暗号化

この順序で設定すると、各設定に従い必要な前提条件が設定されます。

オプションは次のとおりです。

- **Key（必須）**Key オプションは、暗号化キーをブリッジにプログラミングします。 4 つのキーのうち 1 つを設定するように求められます。 キーを二度入力するように求められます。 キーを定義するには、10 桁または 26 桁の 16 進値を入力する必要があります。どちらにするかは、ブリッジの設定が 40 ビットか 128 ビットかによります。 次の文字を任意に組み合わせて使用します。0 ～ 9a ～ fA ～ Fキーは無線セル内のすべてのノードで一致する必要があり、キーは同じ順序で入力する必要があります。 4 つのキーすべてを定義する必要はありませんが、WLAN 内のすべてのデバイスでキーの数が一致している必要があります。
- **送信側**Transmit オプションは、パケットの送信に使用するキーを無線に伝えます。 各無線は、4 つのキーのいずれかで送信された受信パケットを複号化できます。
- AuthAuth オプションはリピータ ブリッジで使用され、装置がどの認証モードを使用して親と接続するかを決定します。 使用できる値は Open または Shared Key です。 802.11 プロトコルは、クライアントがアソシエーションを行う前に親と認証を行う必要のある手続きを規定しています。**Open（推奨）**—認証のこのモードは本質的にヌル オペレーションです。 すべてのクライアントが認証を許可されます。**共有鍵**—このモードは親がクライアントが親に暗号化し、戻すユーザ確認のためのテキスト クライアントを送信 することを可能にします。 親がチャレンジ テキストを復号化できると、そのクライアントは認証されます。**注意**：Shared Key モードを使用しないでください。 Shared Key モードを使用すると、プレーンテキストと、同じデータの暗号化バージョンが空中に伝送されます。 これでは意味がありません。 ユーザのキーが間違っている場合は、装置はパケットを復号化せず、パケットはネットワークへのアクセスを取得できません。
- **クライアント**Client オプションは、クライアントのノードが装置へのアソシエーションに使用する認証モードを決定します。 使用できる値は次のとおりです。**Open（推奨）**—認証のこのモードは本質的にヌル オペレーションです。 すべてのクライアントが認証を許可されます。**共有鍵**—このモードは親がクライアントが親に暗号化し、戻すユーザ確認のためのテキスト クライアントを送信 することを可能にします。 親がチャレンジ テキストを復号化できると、そのクライアントは認証されます。**両方とも**—このモードはクライアントがどちらかのモードを使用することを可能にします。
- 暗号化に Encryption オプションを設定 したら**以外**、no encryption は行われます。 データはクリア テキストで送信されます。**（必須）**—に Encryption オプションを設定 した場合、すべての送信されたデータ パケットは暗号化され、どの非暗号化受け取り パケットでも廃棄されます。**混合された**—ミックス モードでは、ルートかリピータブリッジはオン/オフどちらか回る暗号化があるクライアントからのアソシエーションを許可します。 この場合、ノード間で両方のノードがサポートするデータ パケットだけが暗号化されます。 マルチキャスト パ

ケットはクリア テキストで送信されます。 すべてのノードがパケットを見ることができます。**注意：** Mixed モードは使用しないでください。 暗号化を有効にしたクライアントがマルチキャスト パケットを親へ送信すると、パケットは暗号化されます。 親はそのパケットを復号化し、パケットをクリア テキストでセルへ再送信し、他のノードはパケットを見ることができます。 暗号化された形式とされていない形式の両方のパケットを確認できることで、キーが解読される可能性があります。 Mixed モードが含まれているのは、他のベンダーとの互換性のためだけです。

クライアント アダプタの設定

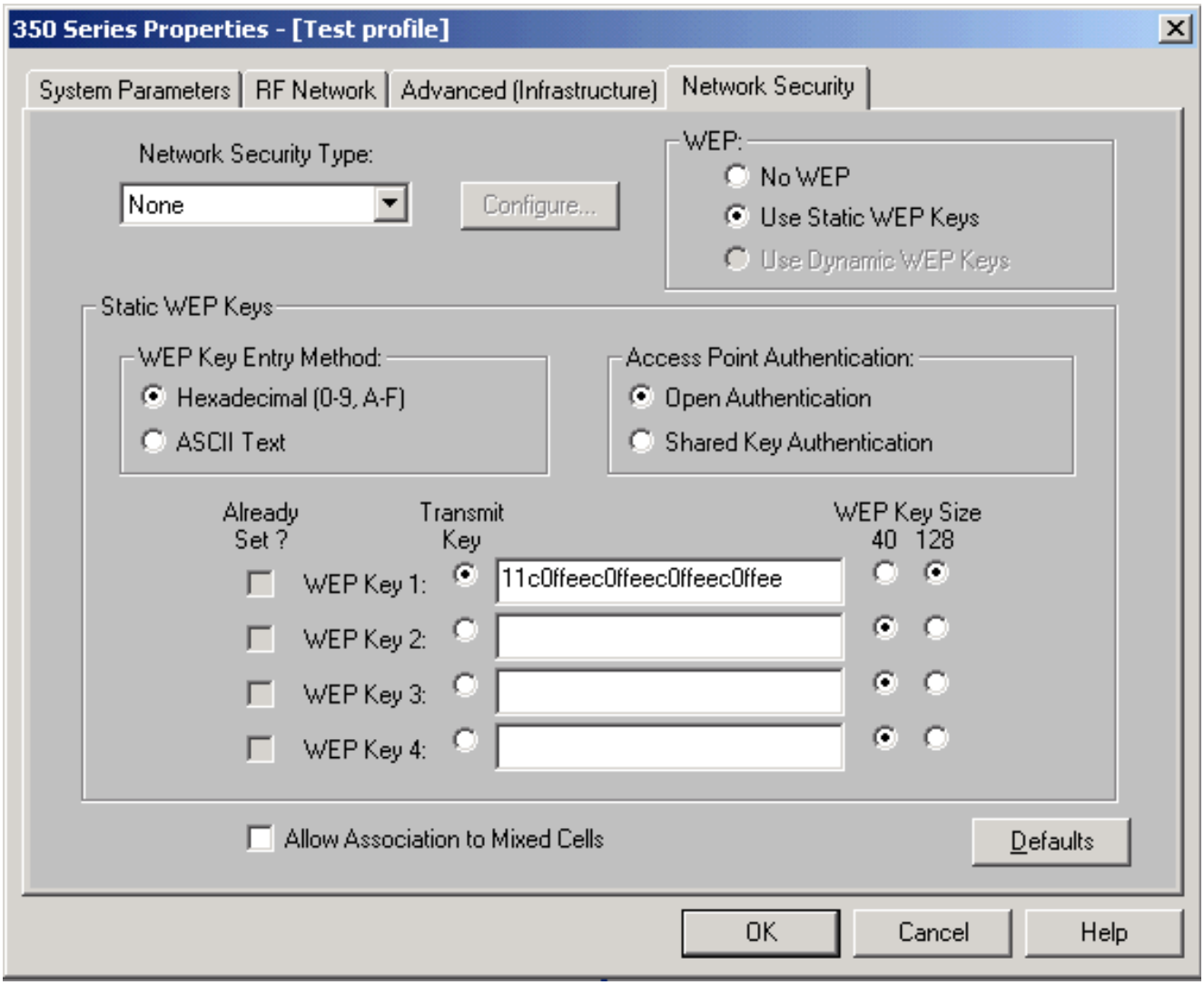
Aironet Client Adapter に WEP を設定するには、次の主な 2 つの手順を実行する必要があります。

1. Client Encryption Manager に WEP キーを 1 つまたは複数設定する。
2. Aironet Client Utility（ACU）で WEP をイネーブルにする。

WEP キーの設定

クライアント アダプタに WEP キーを設定するには、次の手順を実行します。

1. ACU を開き、Profile Manager を選択します。
2. WEP を有効にするプロファイルを選択して、Edit をクリックします。
3. Network Security タブをクリックしてセキュリティ オプションを表示し、Use Static WEP Keys をクリックします。この動作により、No WEP が選択されたときにグレー表示される WEP の設定オプションが有効化されます。



4. 作成したいと思う WEPキーに関しては、ウィンドウの右側の WEPキー サイズの下で **40** ビットか **128** ビットを選択して下さい。**注:** 128 ビットのクライアント アダプタは、40 ビットまたは 128 ビットのキーを使用できます。 ただし、40 ビットのアダプタは、40 ビットのキーしか使用できません。**注:** クライアントアダプタ WEPキーは使用を伝える他の WLANコンポーネント WEPキーを一致する必要があります。複数の WEPキー 設定 されるすべてのデバイスに同じ WEPキー数に WEPキーを割り当てる必要がある時。 WEPキーは 16進文字で構成され、40 ビット WEPキーのための 10 文字か 128-bit WEPキーのための 26 文字が含まれている必要があります。 使用できる 16 進値は次のとおりです。0 ~ 9a ~ fA ~ F**注:** Aironet の AP では、ASCII テキストの WEP キーはサポートされません。 したがって、これらの AP でクライアント アダプタを使用する計画であれば、16 進値 (0-9、A-F) を選択する必要があります。**注:** WEPキーを作成した後、それに書くことができます。ただし、編集や削除はできません。**注:** クライアントユーティリティとして ACU の代りに Aironet デスクトップ ユーティリティ (ADU) の以降のバージョンを使用する場合、また作成された WEPキーを削除し、新しいものと取り替えることができます。
5. 作成したキーの横にある Transmit Key ボタンをクリックします。この動作により、パケットの転送にそのキーを使用することを示します。
6. WEP Key Type の下で、Persistent をクリックします。この操作はアダプタへの電源がキーがインストールされているコンピュータの再度ブートするでまたは取除かれる時でさえクライアントアダプタがこの WEPキーを保つようにします。 このオプションのための一時を選択する場合、WEPキーは電源がクライアントアダプタから取除かれるとき失われます。
7. [OK] をクリックします。

WEP の有効化

次の手順を実行します。

1. ACU を開き、メニュー バーから Edit Properties を選択します。
2. セキュリティオプションを表示するために **Network Security タブを**クリックして下さい。
3. Enable WEP チェック ボックスをチェックし、WEP を有効化します。

クライアントユーティリティでのステップについては ADU の WEP の ADU を使用して WEP を設定するために設定を参照して下さい。

ワークグループ ブリッジの設定

Aironet 340 シリーズ ワークグループ ブリッジと Aironet 340 シリーズ ブリッジには違いがあります。 ただし、WEP を使用するワークグループブリッジの設定はブリッジの設定とほとんど同一です。 ブリッジの設定については設定 Aironetブリッジ セクションを参照して下さい。

1. ワークグループ ブリッジに接続します。
2. Privacy メニューに移動します。プライバシー VxWorks メニューにアクセスするために Main > Configuration > Radio > I80211 > Privacy の順に選択 して下さい。

Settings

Privacy メニューに、このセクションで取り上げる設定が表示されます。 ワークグループ ブリッジでは、この順序でオプションを設定してください。

1. キー
2. 送信側
3. Auth
4. 暗号化

オプションは次のとおりです。

- **キー**Key オプションは、ブリッジがパケットの受信に使用する WEP キーを設定します。 この値は、ワークグループ ブリッジの通信先の AP や他のデバイスが使用するキーと一致する必要があります。 40 ビット暗号化では 10 桁までの 16 進値、128 ビット暗号化では 26 桁の 16 進値でキーを構成します。 次の 16 進値を任意に組み合わせることができます。0 ~ 9a ~ fA ~ F
- **送信側**Transmit オプションは、ブリッジがパケットの送信に使用する WEP キーを設定します。 Key オプションで使用したものと同じキーを使用することもできます。 別のキーを使用する場合は、AP で一致するキーを設定する必要があります。1 つの WEPキーだけ伝達のために一度に使用することができます。 データの送信に使用する WEP キーには、ワークグループ ブリッジとその通信先のデバイスで同じ値を設定する必要があります。
- **Authentication （ Auth ）** Auth パラメータは、システムが使用する認証方法を決定します。 次のオプションがあります。**Open （ 推奨 ）**—デフォルト オープン設定は、WEP設定に関係なく、AP が認証し、次にブリッジと通信するように試みるようにします。**共有鍵**—この設定はブリッジと通信するために AP にプレーンテキストを、共有鍵クエリー 送信 するようにブリッジに指示します。 Shared Key 設定では、ブリッジが侵入者からの既知のテキストによる攻撃にさらされる可能性があります。 したがって、この設定は「Open」ほどセキュアではありません。

- 暗号化Encryption オプションは、アソシエーション パケットと一部の制御パケットを除いたすべてのデータパケットの暗号化パラメータを設定します。 次の 4 つのオプションがあります。**注:** AP の暗号化がアクティブで、キーが正しく設定されている必要があります。**以外**これはデフォルト設定です。 すべての暗号化がオフになります。 ワークグループ ブリッジは、WEP を使用した AP との通信を行いません。（**推奨**）—この設定はすべてのデータ転送の暗号化を必要とします。 ワークグループ ブリッジは、WEP を使用する AP のみと通信を行います。ブリッジが AP と交信するために WEP を常に使用することを**混合されたオン**この設定意味します。 ただし、AP はすべてのデバイスとそれらが WEP を使用するか、または WEP を使用しないかどうか、通信します。**混合された以外は**この設定ブリッジが AP と交信するために WEP を使用しないことを意味します。 ただし、AP はすべてのデバイスとそれらが WEP を使用するか、または WEP を使用しないかどうか、通信します。**注意**：WEP カテゴリに On または Mixed on を使用し、無線リンクからブリッジを設定する場合、WEP キーが誤って設定されているとブリッジとの接続が失われます。 ワークグループブリッジの WEPキーおよび WLAN のその他のデバイスの WEPキーを設定 した時同じ設定を丁度使用することを確かめて下さい。

関連情報

- IEEE Standards Association
- Aironet 340 シリーズ ワイヤレス LAN プロダクト
- ワイヤレスに関するサポート リソース
- ワイヤレス LAN サポートページ
- Cisco Aironet アクセス ポイント用 Cisco IOS ソフトウェア設定ガイド
- Cisco Aironet 1300 シリーズ屋外アクセス ポイント/ブリッジでの Cisco IOS ソフトウェア コンフィギュレーション ガイド
- VxWorks のための Cisco Aironet アクセス ポイント ソフトウェア設定ガイド
- Cisco Aironet 1400 シリーズ ブリッジ ソフトウェアのコンフィギュレーション ガイド
- Cisco Aironet ワイヤレス LAN クライアント アダプタ構成ガイド
- Ciscoワイヤレス LAN セキュリティ 外観
- 無線ネットワークをしっかり止めているワイヤレス（モビリティ）
- ワークグループ ブリッジとしてのアクセス ポイントの設定例
- Cisco Aironet ワークグループ ブリッジに関する FAQ
- Cisco Aironet 機器のパスワード回復手順
- Cisco Aironet アクセス ポイントに関する FAQ
- テクニカルサポートとドキュメント - Cisco Systems