Aironetアクセスポイントおよびブリッジでの WEPの設定

内容

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：ワイヤレスLANコントローラ(WLC)のWEP設定の詳細は、『第6章：WLANの設定』の「静的Webキー」セクションを参照してください。

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暗号化では、40または104ビットキーと24ビット初期化ベクトル(IV)を使用したRon's Code 4(RC4)ストリーム暗号が使用されます。

標準で規定されているように、WEPは40ビットまたは104ビットキーと24ビットIVを使用するRC4アルゴリズムを使用します。RC4 ではデータの暗号化と復号化に同一のキーを使用するため、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、主にホームオフィスや、非常に強力なセキュリティを必要としない小規模オフィスで使

用できます。

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：WEPには、いくつかの既知の問題があるため、強力な暗号化方式ではありません。これらの問題には次のようなものがあります。

- 共有WEPキーを維持するには、大量の管理オーバーヘッドがあります。
- WEPには、共有キーに基づくすべてのシステムと同じ問題があります。ある人に与えられた秘密は、一定期間が経過すると公開されます。
- 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チェックサムは線形で予測可能です。

Temporal Key Integrity Protocol(TKIP)は、これらのWEPの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、WEPの既知の脆弱性に対処するために、パケットごとのキーハッシュ、Message Integrity Check(MIC)、およびブロードキャストキーローテーションなどの対策を追加することで、WEPを強化します。TKIPは、暗号化に128ビットキーを使用し、認証に64ビットキーを使用する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準拠のシスコ以外の製品と40ビットの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ました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

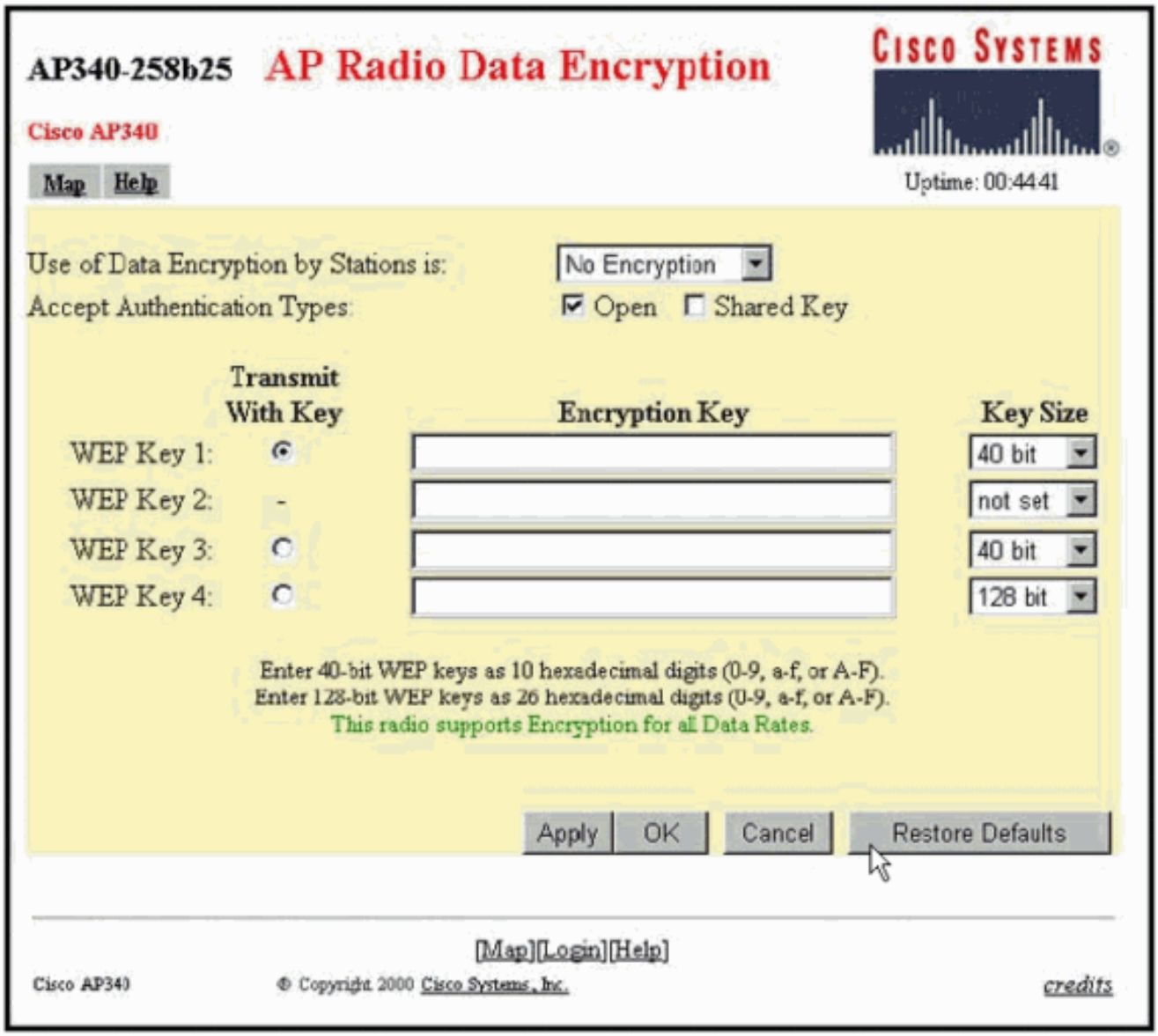
ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

Aironetアクセスポイントでの WEPの設定

VxWorksオペレーティングシステムが稼働するAironetアクセスポイント

次のステップを実行します。

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：このページを変更するには、IDおよび書き込み機能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**



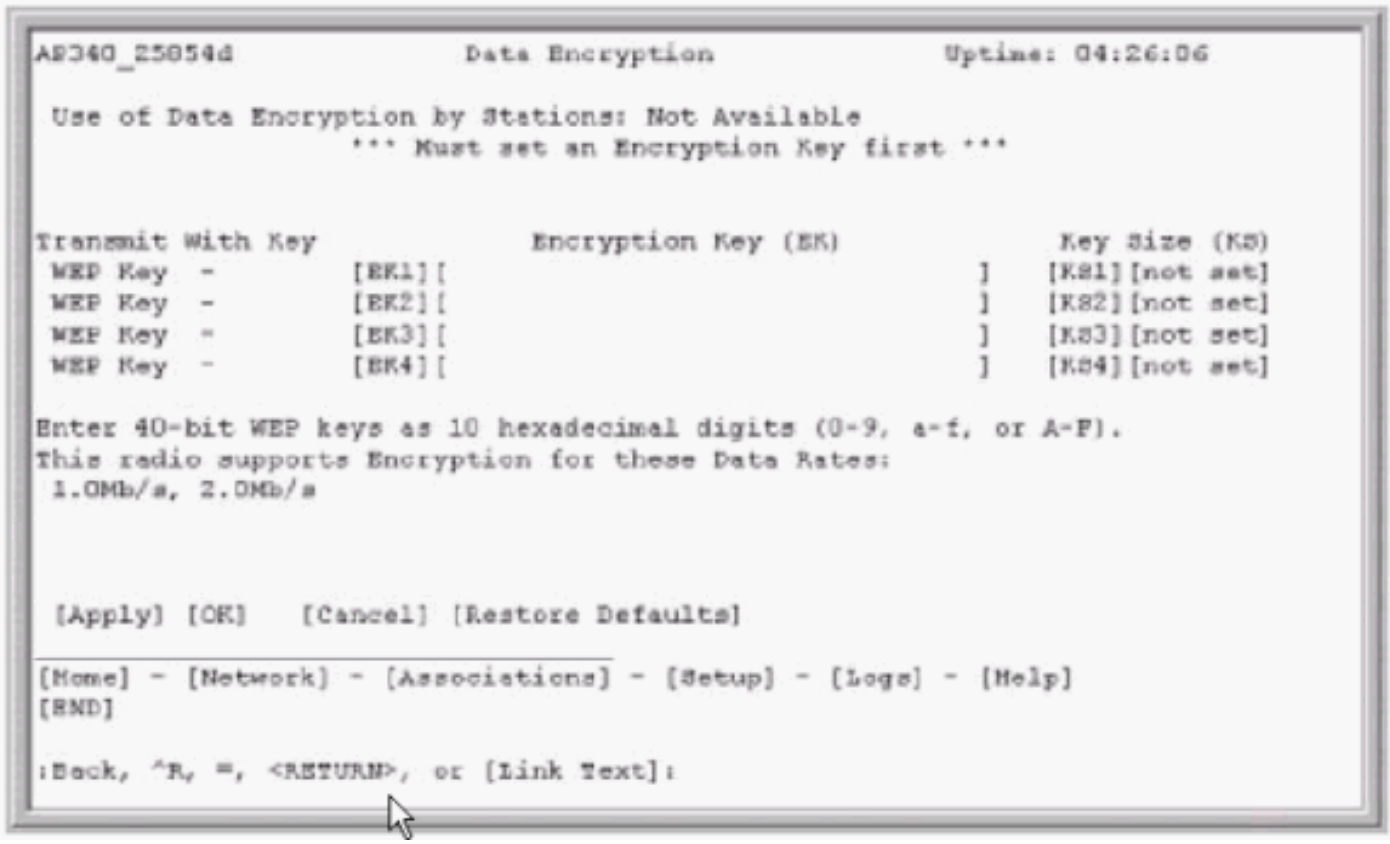
VxWorks の設定

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。**暗号化なし（デフォルト）**：クライアントがデータ暗号化なしでAPと通信することを要求します。この設定は推奨されません。**オプション**：クライアントがデータ暗号化の有無にかかわらずAPと通信できるようにします。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。**完全暗号化（推奨）**：クライアントがAPと通信するときに、データ暗号化を使用する必要があります。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(RECOMMENDED)**：このデフォルト設定では、WEPキーに関係なく、任意のデバイスが認証され、関連付けを試行できます。**Shared Key**：この設定は、APとの関連付けを試みるデバイスにプレーンテキストの共有キークエリを送信するようにAPに指示します。**注：このクエリ**は、APを侵入者からの既知のテキスト攻撃に開放したままにすることができます。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キーの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にプレーンテキストで表示されません。最近のバージョンのAPでは、既存のキーを削除できます。ただし、既存のキーは編集できません。**注：ネ**ットワーク、AP、クライアントデバイスのWEPキーは、まったく同じ方法で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：「設定**なし」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。**適用**：このボタンをクリックすると、新しい値の設定がアクティブになります。ブラウザは、そのページのままです。**OK**：このボタンをクリックすると、新しい設定が適用され、ブラウザがメインのセットアップページに戻ります。**Cancel**：このボタンをクリックすると、設定の変更がキャンセルされ、以前に保存した値に設定が戻されます。Setup のメインページに戻ります。**Restore Defaults**：このボタンをクリックすると、このページのすべての設定が工場出荷時のデフォルト設定に戻ります。

注：最近のCisco IOS®バージョンのAPでは、このページで**は**Applyボタン**と**Cancelボタンだけが使用できます。

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

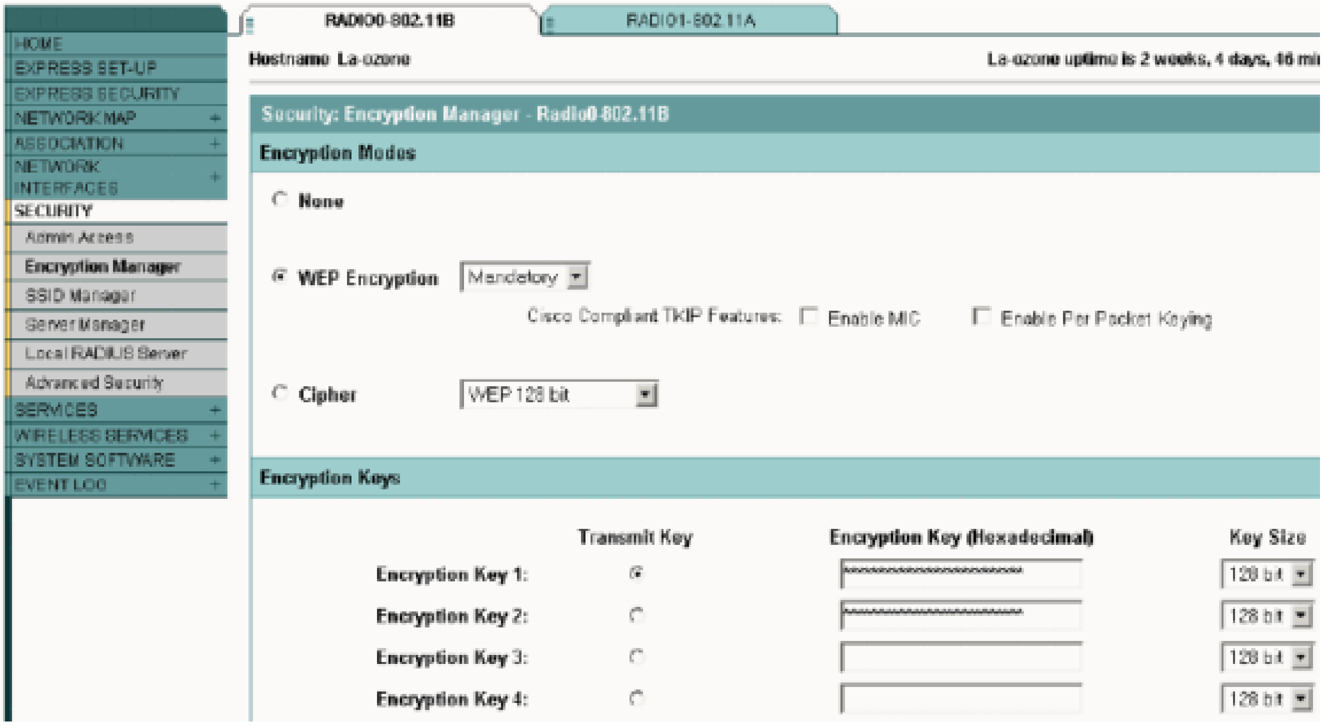
```
La-ozone>
La-ozone>
La-ozone>enable
Password:
La-ozone#
La-ozone#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
La-ozone(config)#interface dot
La-ozone(config)#interface dot11Radio 0
La-ozone(config-if)#encryption key 1 size 128bit 11c0ffeec0ffeec0ffeec0ffee ?
  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ソフトウェアが稼働するAironet AP

次のステップを実行します。

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**



Aironetブリッジの設定

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の順に選択します**。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
   >_
```

CLIモードを使用して1300および1400シリーズブリッジでWEPを設定する方法については、『暗号スイートとWEPの設定 – 1300シリーズブリッジ』および『WEPおよびWEP機能の設定 – 14000000000000000000000000000000000000000000000000000000000000000000000

GUIを使用して1300および1400シリーズブリッジを設定するには、このドキュメントの「Cisco IOSソフトウェアが稼働するAironet AP」セクションで説明されている手順を実行します。

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、次の順序でオプションを設定します。

1. キー
2. トランスミット
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。
- **トランスミット**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。
- **AUTH**Auth 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。**オープン（推奨）**：この認証モードは基本的にヌル操作です。すべてのクライアントが認証を許可されます。**共有キー**：このモードでは、親がクライアントにチャレンジテキストを送信できます。チャレンジテキストは、クライアントが暗号化して親に戻ります。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：共有キー**・モードは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。**オープン（推奨）**：この認証モードは基本的にヌル操作です。すべてのクライアントが認証を許可されます。**共有キー**：このモードでは、親がクライアントにチャレンジテキストを送信できます。チャレンジテキストは、クライアントが暗号化して親に戻ります。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。**Both**：このモードでは、クライアントがどちらかのモードを使用できます。
- **暗号化Off**:[Encryption]オプションを[Off]に設定すると、暗号化は行われません。データはクリア テキストで送信されます。**On (MANDATORY)**:[Encryption]オプションを[On]に設定すると、送信されたすべてのデータパケットが暗号化され、暗号化されていない受信パケットは破棄されます。**混合**：混合モードでは、ルートまたはリピータブリッジは、暗号化がオンまたはオフになっているクライアントからの関連付けを受け入れます。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：混合**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

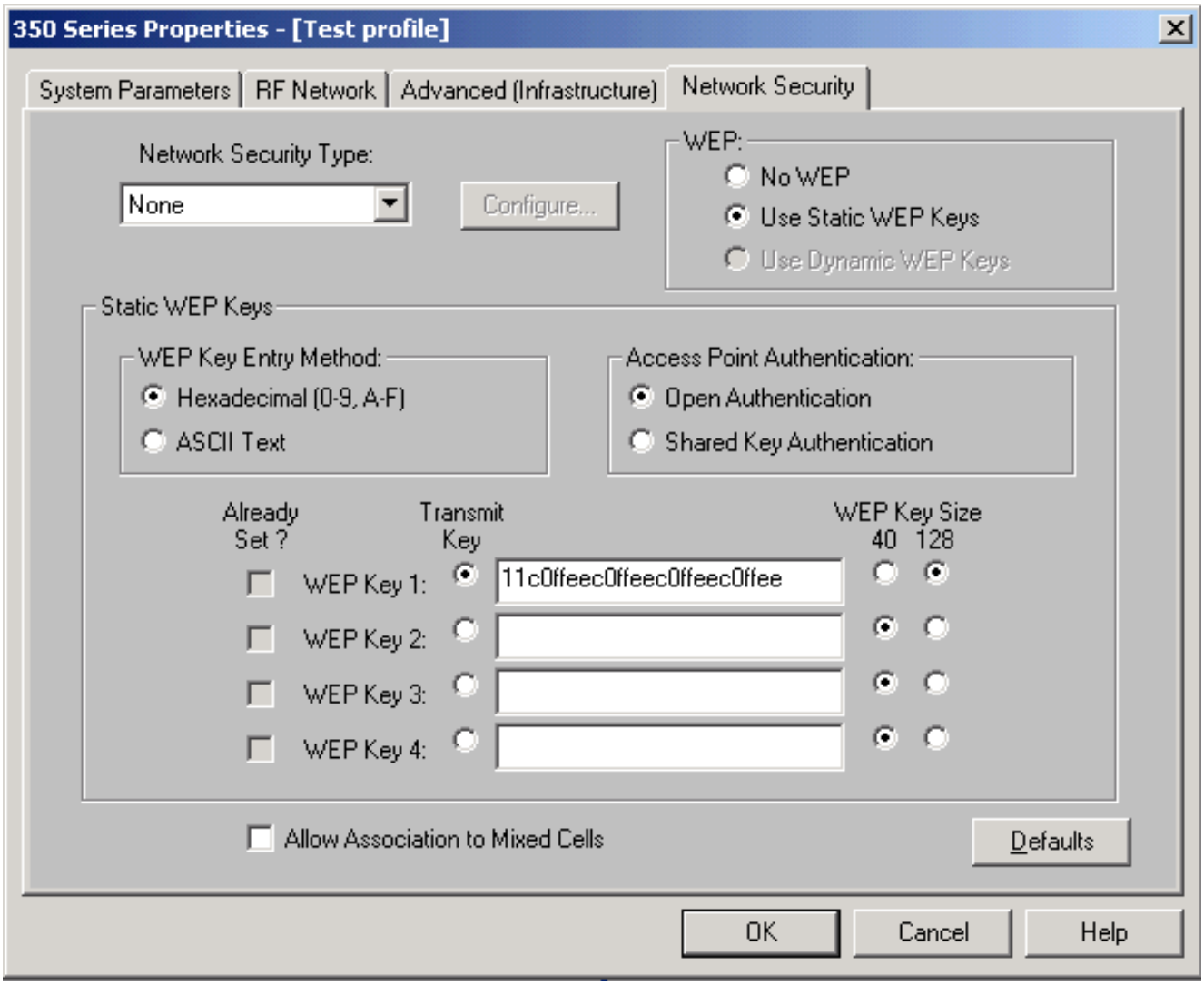
Aironet Client Adapter に WEP を設定するには、次の主な 2 つの手順を実行する必要があります。

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. 作成する WEP Key に対し、ウィンドウ右側の WEP Key Size の下で 40 ビットまたは 128 ビットを選択します。**注：128ビット**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**アントアダプタのWEPキーは、通信に使用する他のWLANコンポーネントのWEPキーと一致している必要があります。複数の WEP Key を使用する場合は、すべてのデバイスで WEP Key に同じ WEP Key 番号を割り当てる必要があります。WEPキーは16進数で構成する必要があり、40ビットWEPキーの場合は10文字、128ビットWEPキーの場合は26文字である必要があります。使用できる 16 進値は次のとおりです。0 ～ 9a ～ fA ～ F**注：**ASCIIテキストのWEPキーは、Aironet APではサポートされていません。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**を作成した後は、それを上書きできます。ただし、編集や削除はできません。**注：ACUの代わりに**新しいバージョンのAironet Desktop Utility(ADU)をクライアントユーティリティとして使用する場合は、作成したWEPキーを削除し、新しいWEPキーに置き換えることもできます。
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。この動作により、アダプタへの電力が遮断されたり、キーがインストールされているコンピュータがリブートされたりした場合も、クライアント アダプタではこの WEP Key を維持できます。このオプションで Temporary を選択すると、クライアント アダプタの電力が失われると WEP Key が失われます。
7. [OK] をクリックします。

WEP の有効化

次のステップを実行します。

1. ACU を開き、メニュー バーから Edit Properties を選択します。
2. [**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ます。
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。

ADUをクライアントユーティリティとして使用してWEPを設定する手順については、『ADUでのWEPの設定』を参照してください。

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を使用するための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じです。ブリッジの設定については、「Aironetブリッジの設定」セクションを参照してください。

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。**[Main] > [Configuration] > [Radio] > [I80211] > [Privacy]を選択して**、[Privacy VxWorks]メニューにアクセスします。

設定

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. トランスミット
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
- **トランスミット**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。伝送に使用できるWEPキーは1つだけです。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。**オープン（ 推奨 ）**：デフォルトのオープン設定では、APのWEP設定に関係なく、任意のAPが認証を行い、ブリッジとの通信を試みることができます。**共有キー**：この設定は、ブリッジと通信を試みるために、プレーンテキストの共有キークエリをAPに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で**は、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。**Off**：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。**オン（推奨）**：この設定では、すべてのデータ転送の暗号化が必要です。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。**Mixed on**：この設定は、ブリッジがAPと通信するために常にWEPを使用することを意味します。ただし、APは、WEPを使用するか、WEPを使用しないかにかかわらず、すべてのデバイスと通信します。**Mixed off**：この設定は、ブリッジがAPと通信するためにWEPを使用しないことを意味します。ただし、APは、WEPを使用するか、WEPを使用しないかにかかわらず、すべてのデバイスと通信します。**注意：WEPカテゴリとして**Onまたは Mixed onを選択し、その無線リンクを通じてブリッジを設定すると、WEPキーを誤って設定すると、ブリッジへの接続が失われます。Workgroup BridgeのWEPキーとWLANの他のデバイスのWEPキーを設定する場合は、まったく同じ設定を使用してください。

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
- シスコワイヤレスLANセキュリティの概要
- ワイヤレス（モビリティ）ワイヤレスネットワークの保護
- 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

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。