Konfigurationsbeispiel für Wired Equivalent Privacy (WEP) auf Aironet Access Points und Bridges

Inhalt

Einführung

Dieses Dokument enthält Methoden zum Konfigurieren von Wired Equivalent Privacy (WEP) für Cisco Aironet Wireless LAN (WLAN)-Komponenten.

Hinweis: Weitere Informationen zur WEP-Konfiguration auf WLAN-Controllern (WLCs) finden Sie im Abschnitt Statische Web-Schlüssel in Kapitel 6 - Konfigurieren von WLANs.

WEP ist der in den 802.11-Standard (Wi-Fi) integrierte Verschlüsselungsalgorithmus. Die WEP-Verschlüsselung verwendet den Ron's Code 4 (RC4) Stream Cipher mit 40- oder 104-Bit-Schlüsseln und einem 24-Bit-Initialisierungsvektor (IV).

Wie der Standard festlegt, verwendet WEP den RC4-Algorithmus mit einem 40-Bit- oder 104-Bit-Schlüssel und einem 24-Bit-IV. RC4 ist ein symmetrischer Algorithmus, da er denselben Schlüssel für die Verschlüsselung und Entschlüsselung von Daten verwendet. Wenn WEP aktiviert ist, hat jede Funkstation einen Schlüssel. Der Schlüssel wird verwendet, um die Daten vor der Übertragung der Daten durch die Funkwellen zu verwirren. Wenn eine Station ein Paket empfängt, das nicht mit dem entsprechenden Schlüssel verschlüsselt wird, wird das Paket verworfen und nie

an den Host geliefert.

WEP kann in erster Linie für Heimbüros oder kleinere Büros verwendet werden, für die keine besonders hohe Sicherheit erforderlich ist.

Die Aironet WEP-Implementierung befindet sich in der Hardware. Aus diesem Grund werden bei Verwendung von WEP nur minimale Auswirkungen auf die Leistung erzielt.

Hinweis: Es gibt einige bekannte Probleme mit WEP, wodurch es keine starke Verschlüsselungsmethode ist. Es geht um folgende Fragen:

- Der Verwaltungsaufwand für die Beibehaltung eines gemeinsamen WEP-Schlüssels ist enorm.
- WEP hat das gleiche Problem wie alle Systeme, die auf gemeinsam genutzten Schlüsseln basieren. Jedes Geheimnis, das einer Person gegeben wird, wird nach einer bestimmten Zeit öffentlich.
- Die IV, die den WEP-Algorithmus einkerbt, wird als Klartext gesendet.
- Die WEP-Prüfsumme ist linear und vorhersehbar.

Um diese WEP-Probleme zu beheben, wurde das Temporal Key Integrity Protocol (TKIP) erstellt. Ähnlich wie WEP verwendet TKIP die RC4-Verschlüsselung. TKIP verbessert WEP jedoch, indem Maßnahmen wie Hashing pro Paketschlüssel, Message Integrity Check (MIC) und Broadcast Key Rotation hinzugefügt werden, um bekannte Schwachstellen von WEP zu beheben. TKIP verwendet RC4-Stream-Verschlüsselung mit 128-Bit-Schlüsseln für die Verschlüsselung und 64-Bit-Schlüssel für die Authentifizierung.

Voraussetzungen

Anforderungen

In diesem Dokument wird davon ausgegangen, dass Sie eine administrative Verbindung zu den WLAN-Geräten herstellen können und dass die Geräte normal in einer unverschlüsselten Umgebung funktionieren.

Um Standard-40-Bit-WEP zu konfigurieren, müssen Sie über zwei oder mehr Funkeinheiten verfügen, die miteinander kommunizieren.

Hinweis: Die Aironet-Produkte können 40-Bit-WEP-Verbindungen mit nicht von Cisco stammenden IEEE 802.11b-konformen Produkten herstellen. Dieses Dokument behandelt nicht die Konfiguration anderer Geräte.

Für die Erstellung einer 128-Bit-WEP-Verbindung interagieren Cisco Produkte nur mit anderen Cisco Produkten.

Verwendete Komponenten

Verwenden Sie diese Komponenten in diesem Dokument:

- Zwei oder mehr Funkeinheiten kommunizieren miteinander
- Eine administrative Verbindung zum WLAN-Gerät

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten

Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konventionen

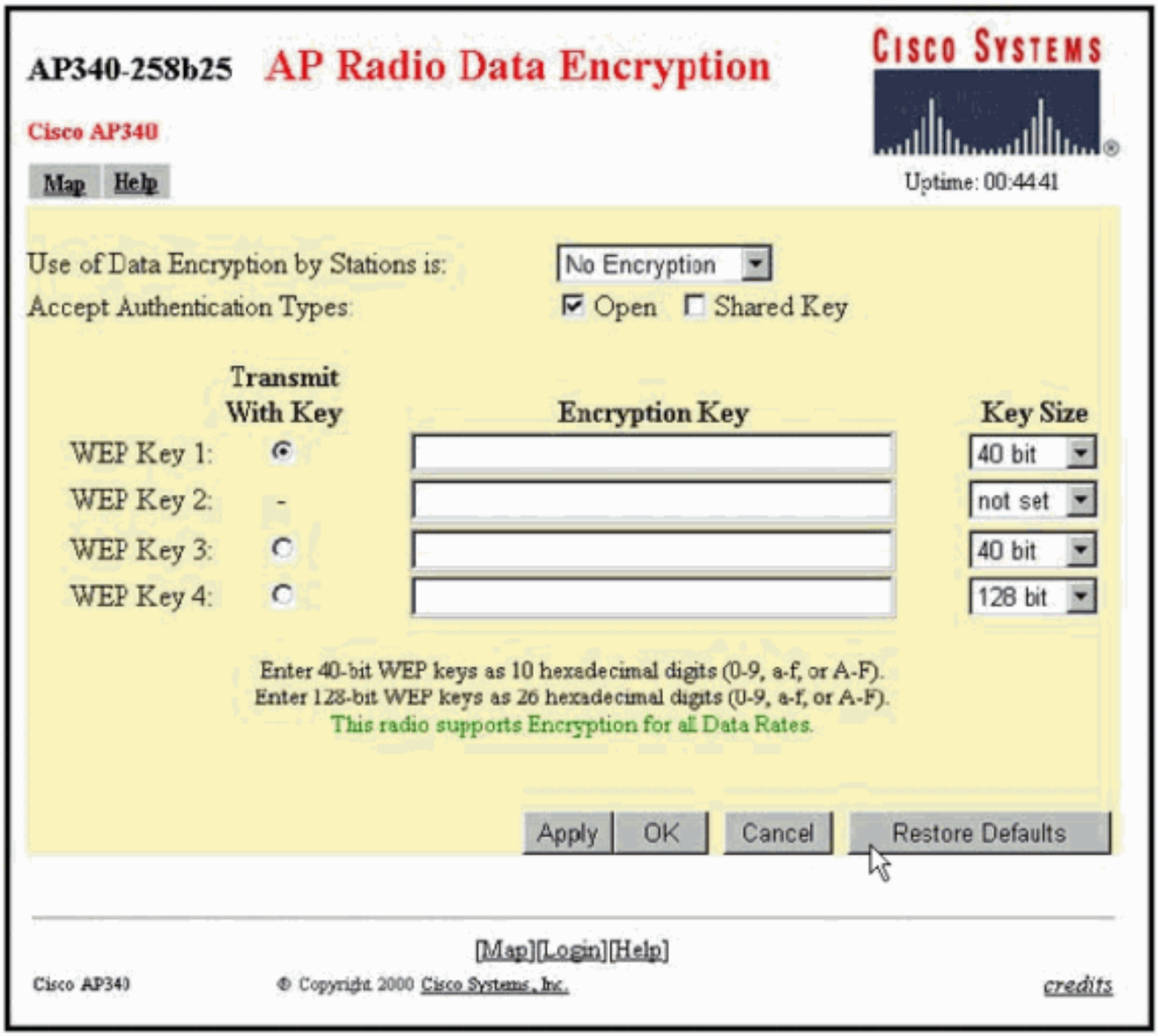
Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

WEP auf Aironet Access Points konfigurieren

Aironet Access Points, die VxWorks-Betriebssystem ausführen

Führen Sie diese Schritte aus:

1. Stellen Sie eine Verbindung zum Access Point (AP) her.
2. Navigieren Sie zum Menü AP Radio Encryption.Verwenden Sie einen der folgenden Pfade:**Zusammenfassender Status > Setup > AP Radio/Hardware > Radio Data Encryption (WEP) > AP Radio Data EncryptionZusammengefasster Status > Setup > Security > Security Setup: Radio Data Encryption (WEP) > AP Radio Data EncryptionHinweis:** Um Änderungen an dieser Seite vornehmen zu können, müssen Sie ein Administrator mit Identitäts- und Schreibfunktionen sein.**Webbrowser-Ansicht des AP Radio Data Encryption-Menüs**



VxWorks-Einstellungen

Die Seite AP Radio Data Encryption (AP-Radio-Datenverschlüsselung) bietet eine Reihe von Optionen zur Verwendung. Einige Optionen sind für WEP obligatorisch. In diesem Abschnitt werden diese obligatorischen Optionen aufgeführt. Andere Optionen sind für die Funktion von WEP nicht erforderlich, werden jedoch empfohlen.

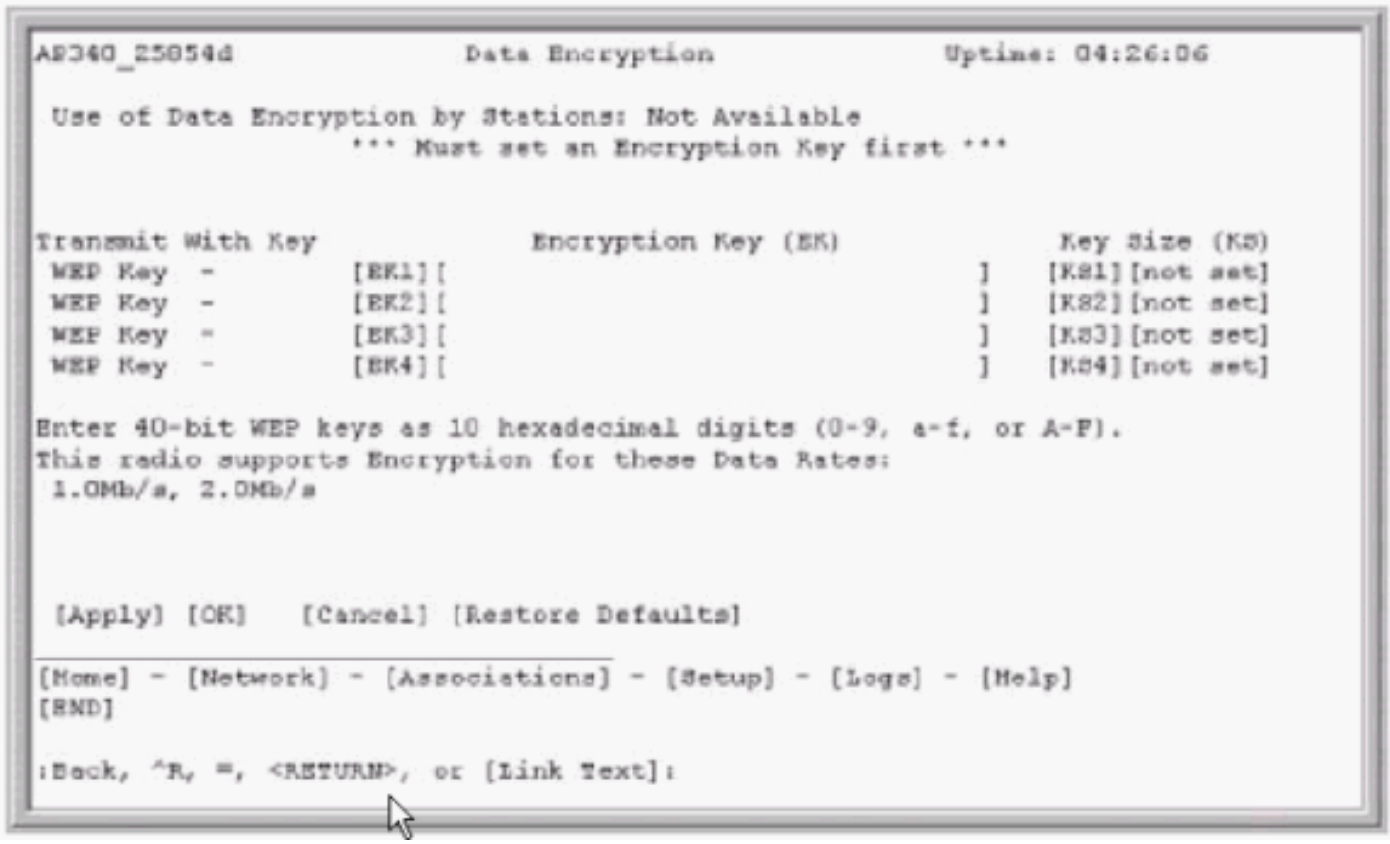
- **Die Datenverschlüsselung nach Stationen wird wie folgt verwendet:**Verwenden Sie diese Einstellung, um festzulegen, ob Clients Datenverschlüsselung verwenden müssen, wenn sie mit dem Access Point kommunizieren. Im Dropdown-Menü sind drei Optionen aufgeführt:**No Encryption (Standard)** - Erfordert Clients, ohne Datenverschlüsselung mit dem AP zu kommunizieren. Diese Einstellung wird nicht empfohlen.**Optional**: Ermöglicht Clients die Kommunikation mit dem Access Point entweder mit oder ohne Datenverschlüsselung. In der Regel verwenden Sie diese Option, wenn Sie über Clientgeräte verfügen, die keine WEP-Verbindung herstellen können, z. B. Clients von anderen Anbietern in einer 128-Bit-WEP-Umgebung.**Full Encryption (EMPFOHLEN)** - Erfordert Clients, die Datenverschlüsselung verwenden, wenn sie mit dem Access Point kommunizieren. Clients, die keine Datenverschlüsselung verwenden, dürfen nicht kommunizieren. Diese Option wird empfohlen, wenn Sie die Sicherheit Ihres WLANs maximieren möchten.**Hinweis:** Sie müssen einen WEP-Schlüssel festlegen, bevor Sie die Verschlüsselung aktivieren. Weitere Informationen finden

Sie im Abschnitt **Verschlüsselungsschlüssel (MANDATORY)** dieser Liste.

- **Authentifizierungstypen akzeptieren**Sie können Open (Öffnen), Shared Key (Gemeinsamer Schlüssel) oder beide Optionen auswählen, um die vom AP erkannten Authentifizierungen festzulegen.**Open (EMPFOHLEN)** - Diese Standardeinstellung ermöglicht jedem Gerät unabhängig von seinen WEP-Schlüsseln die Authentifizierung und den Verbindungsversuch.**Shared Key**: Diese Einstellung weist den Access Point an, eine Abfrage mit einem freigegebenen Schlüssel in Textform an jedes Gerät zu senden, das versucht, eine Verbindung zum Access Point herzustellen.**Hinweis:** Bei dieser Abfrage kann der Access Point einem bekannten Text-Angriff durch Eindringlinge ausgesetzt sein. Daher ist diese Einstellung nicht so sicher wie die Einstellung Öffnen.
- **Mit Schlüssel übertragen**Mit diesen Schaltflächen können Sie die Taste auswählen, die der Access Point bei der Datenübertragung verwendet. Sie können jeweils nur einen Schlüssel auswählen. Sie können alle oder alle Schlüsseln zum Empfangen von Daten verwenden. Sie müssen den Schlüssel festlegen, bevor Sie ihn als Übertragungsschlüssel angeben.
- **Verschlüsselungsschlüssel (OBLIGATORISCH)**Mit diesen Feldern können Sie die WEP-Schlüssel eingeben. Geben Sie 10 Hexadezimalziffern für 40-Bit-WEP-Schlüssel oder 26 Hexadezimalziffern für 128-Bit-WEP-Schlüssel ein. Bei den Tasten kann es sich um eine beliebige Kombination der folgenden Ziffern handeln:0 bis 9a bis fA bis FZum Schutz der WEP-Schlüsselsicherheit werden vorhandene WEP-Schlüssel nicht im Klartext in den Eingabefeldern angezeigt. In den letzten Versionen der APs können Sie vorhandene Schlüssel löschen. Sie können die vorhandenen Schlüssel jedoch nicht bearbeiten.**Hinweis:** Sie müssen die WEP-Schlüssel für Ihr Netzwerk, Access Points und Client-Geräte genau auf die gleiche Weise einrichten. Wenn Sie z. B. den WEP-Schlüssel 3 auf Ihrem AP auf 0987654321 festlegen und diesen Schlüssel als aktiven Schlüssel auswählen, müssen Sie auch den WEP-Schlüssel 3 auf dem Client-Gerät auf den gleichen Wert festlegen.
- **Schlüsselgröße (OBJEKTIV)**Diese Einstellung legt die Schlüssel entweder auf 40-Bit- oder 128-Bit-WEP fest. Wenn für diese Auswahl "not set" (Nicht festgelegt) angezeigt wird, ist der Schlüssel nicht festgelegt.**Hinweis:** Sie können einen Schlüssel nicht löschen, indem Sie "nicht festgelegt" auswählen.
- **Aktionsschaltflächen**Die Einstellungen werden über vier Aktionsschaltflächen gesteuert. Wenn JavaScript in Ihrem Webbrowser aktiviert ist, wird nach dem Klicken auf eine Schaltfläche außer Cancel (Abbrechen) ein Popup-Bestätigungsfenster angezeigt.**Apply** (Übernehmen): Diese Schaltfläche aktiviert die neuen Werteeinstellungen. Der Browser bleibt auf der Seite.**OK** - Mit dieser Schaltfläche werden die neuen Einstellungen übernommen, und der Browser wird wieder zur Haupt-Setup-Seite geleitet.**Cancel (Abbrechen**): Mit dieser Schaltfläche werden Änderungen der Einstellung abgebrochen und die Einstellungen auf die zuvor gespeicherten Werte zurückgesetzt. Kehren Sie dann zur Haupt-Setup-Seite zurück.**Restore Defaults (Standardeinstellungen wiederherstellen**): Mit dieser Schaltfläche werden alle Einstellungen auf dieser Seite auf die werkseitigen Standardeinstellungen zurückgesetzt.

Hinweis: In den letzten Cisco IOS®-Versionen der Access Points sind nur die Schaltflächen **Apply** und **Cancel** für diese Seite verfügbar.

Terminal-Emulatoransicht des Datenverschlüsselungsmenüs



Terminal Emulator View of the WEP Key Configuration Sequence (Cisco IOS® Software)

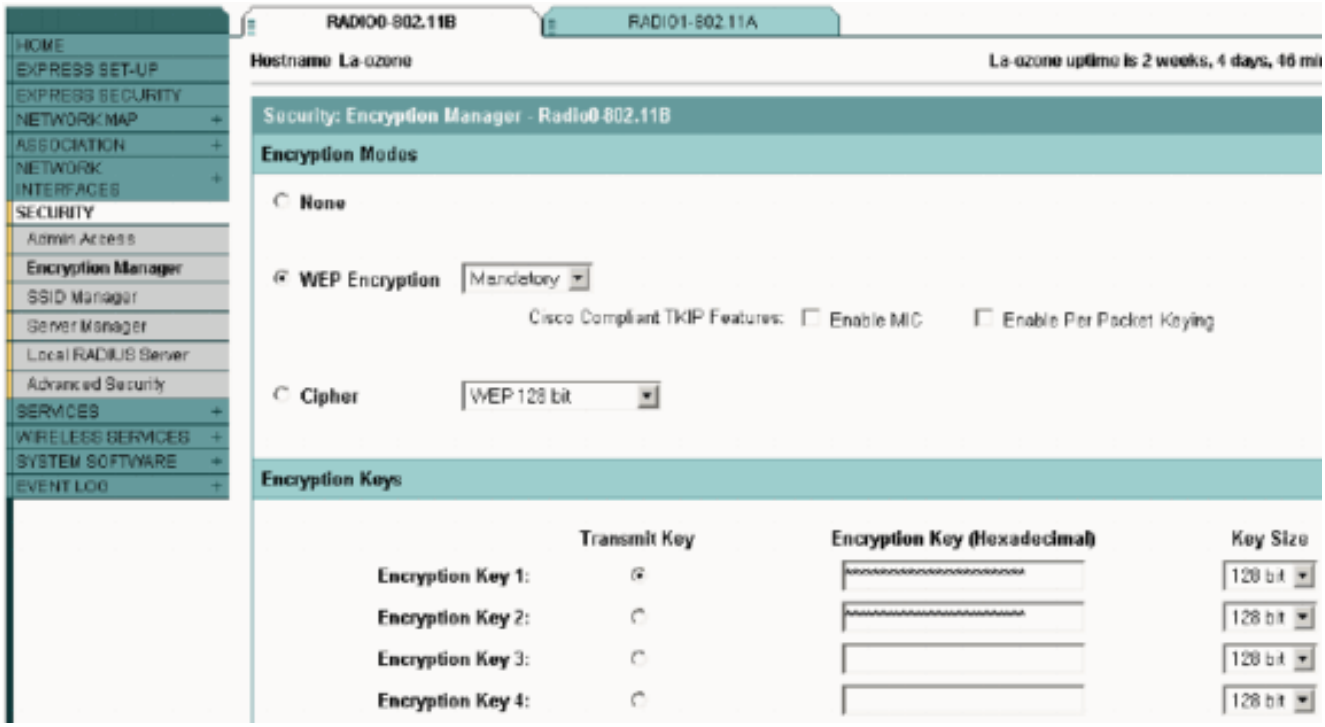
```
La-ozone>
La-ozone>
La-ozone>enable
Password:
La-ozone#
La-ozone#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
La-ozone(config)#interface dot
La-ozone(config)#interface dot11Radio 0
La-ozone(config-if)#encryption key 1 size 128bit 11c0ffeec0ffeec0ffeec0ffee ?
 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

Führen Sie diese Schritte aus:

1. Stellen Sie eine Verbindung zum AP her.
2. Wählen Sie im Menü SECURITY (SICHERHEIT) auf der linken Seite des Fensters **Encryption Manager** für die Funkschnittstelle aus, für die Sie die statischen WEP-Schlüssel konfigurieren möchten.**Webbrowser-Ansicht des AP Security Encryption Manager-Menüs**



Konfigurieren von Aironet Bridges

Wenn Sie VxWorks verwenden, gehen Sie wie folgt vor:

1. Stellen Sie eine Verbindung zur Bridge her.
2. Navigieren Sie zum Menü Datenschutz.Wählen Sie **Hauptmenü > Konfiguration > Radio > I80211 > Privacy (Datenschutz) aus**.Im Menü Datenschutz wird die Verschlüsselung des Datenpakets gesteuert, das von den Funkmodulen über die Luft übertragen wird. Zur Verschlüsselung der Pakete werden der RSA RC4-Algorithmus und einer von bis zu vier bekannten Schlüsseln verwendet. Jeder Knoten in der Funkzelle muss über alle verwendeten Schlüssel verfügen, jedoch können alle Schlüssel für die Datenübertragung ausgewählt werden.**Terminal-Emulator-Ansicht des Datenschutzmenüs**

```
        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
>_
```

Unter Konfigurieren von Cipher Suites und WEP - Bridge der Serie 1300 und Konfigurieren von WEP- und WEP-Funktionen - Bridge der Serie 1400 finden Sie Informationen zur Konfiguration von WEP in Bridges der Serien 1300 und 1400 im CLI-Modus.

Führen Sie zum Konfigurieren von Bridges der Serien 1300 und 1400 über die Benutzeroberfläche die gleichen Schritte aus, die im Abschnitt Aironet APs, die Cisco IOS Software ausführen, beschrieben werden.

VxWorks-Einstellungen

Im Menü "Datenschutz" werden eine Reihe von Optionen angezeigt, die Sie konfigurieren müssen. Einige Optionen sind für WEP obligatorisch. In diesem Abschnitt werden diese obligatorischen Optionen aufgeführt. Andere Optionen sind für die Funktion von WEP nicht erforderlich, werden jedoch empfohlen.

In diesem Abschnitt werden die Menüoptionen in der Reihenfolge dargestellt, in der sie in der Terminalemulatoransicht des Datenschutzmenüs angezeigt werden. Konfigurieren Sie die Optionen jedoch in der folgenden Reihenfolge:

1. Wichtigste
2. Übertragen
3. Auth
4. Kunde
5. Verschlüsselung

Durch die Konfiguration in dieser Reihenfolge wird sichergestellt, dass bei der Konfiguration jeder Einstellung die erforderlichen Vorbedingungen festgelegt werden.

Folgende Optionen stehen zur Verfügung:

- **Schlüssel (OBLIGATORISCH)**Die Option Key programmiert die Verschlüsselungsschlüssel in die Bridge. Sie werden aufgefordert, eine der vier Tasten festzulegen. Sie werden zweimal aufgefordert, den Schlüssel einzugeben. Um den Schlüssel zu definieren, müssen Sie entweder 10 oder 26 Hexadezimalziffern eingeben. Dies hängt davon ab, ob die Bridge-Konfiguration für 40-Bit- oder 128-Bit-Schlüssel gilt. Verwenden Sie eine beliebige Kombination dieser Ziffern:0 bis 9a bis fA bis FDie Schlüssel müssen in ***allen Knoten in der Funkzelle*** übereinstimmen, und Sie müssen die Schlüssel in der gleichen Reihenfolge eingeben. Sie müssen nicht alle vier Schlüssel definieren, solange die Anzahl der Schlüssel in jedem Gerät im WLAN übereinstimmt.
- **Übertragen**Die Option "Senden" teilt dem Funkmodul mit, welche Schlüssel zum Übertragen von Paketen verwendet werden sollen. Jede Funkeinheit kann empfangene Pakete entschlüsseln, die mit einem der vier Schlüssel gesendet werden.
- **Auth**Sie können die Option Auth auf Repeater-Bridges verwenden, um den Authentifizierungsmodus zu bestimmen, den das Gerät für die Verbindung mit dem übergeordneten Gerät verwendet. Zulässige Werte sind Open (Offener) oder Shared Key (Freigegebener Schlüssel). Das 802.11-Protokoll gibt eine Prozedur an, bei der ein Client sich bei einem übergeordneten Element authentifizieren muss, bevor der Client eine Verbindung herstellen kann.**Open (EMPFOHLEN)** - Dieser Authentifizierungsmodus ist im Wesentlichen ein NULL-Vorgang. Alle Clients können sich authentifizieren.**Shared Key** - Dieser Modus ermöglicht es dem übergeordneten Benutzer, dem Client einen Challenge-Text zu senden, den der Client verschlüsselt und an das übergeordnete Element zurückgibt. Wenn das übergeordnete Element den Challenge-Text erfolgreich entschlüsselt, wird der Client authentifiziert.**Vorsicht:** Verwenden Sie nicht den Modus für den gemeinsamen Schlüssel. Wenn Sie diese verwenden, wird eine unverschlüsselte und verschlüsselte Version derselben Daten in die Luft übertragen. Das bringt nichts. Wenn der Benutzerschlüssel falsch ist, entschlüsselt die Einheit die Pakete nicht, und die Pakete können nicht auf das Netzwerk zugreifen.
- **Kunde**Die Client-Option legt den Authentifizierungsmodus fest, den die Client-Knoten verwenden, um der Einheit zuzuordnen. Folgende Werte sind zulässig:**Open (EMPFOHLEN)** - Dieser Authentifizierungsmodus ist im Wesentlichen ein NULL-Vorgang. Alle Clients können

sich authentifizieren.**Shared Key** - Dieser Modus ermöglicht es dem übergeordneten Benutzer, dem Client einen Challenge-Text zu senden, den der Client verschlüsselt und an das übergeordnete Element zurückgibt. Wenn das übergeordnete Element den Challenge-Text erfolgreich entschlüsselt, wird der Client authentifiziert.**Both (Beide**): Dieser Modus ermöglicht dem Client, beide Modi zu verwenden.

- **VerschlüsselungAus**: Wenn Sie die Verschlüsselungsoption auf Off (Aus) setzen, erfolgt keine Verschlüsselung. Daten werden in der Klarheit übertragen.**On (MANDATORY)** - Wenn Sie die Verschlüsselungsoption auf On (Ein) setzen, werden alle übertragenen Datenpakete verschlüsselt und alle nicht verschlüsselten empfangenen Pakete verworfen.**Gemischt** - Im gemischten Modus akzeptiert eine Root- oder Repeater-Bridge die Zuordnung von Clients, deren Verschlüsselung entweder aktiviert oder deaktiviert ist. In diesem Fall werden nur Datenpakete zwischen Knoten verschlüsselt, die beide unterstützen. Multicast-Pakete werden unverschlüsselt gesendet. Alle Knoten können die Pakete sehen.**Vorsicht:** Verwenden Sie nicht den gemischten Modus. Wenn ein Client mit aktivierter Verschlüsselung ein Multicast-Paket an sein übergeordnetes Element sendet, wird das Paket verschlüsselt. Das übergeordnete Element entschlüsselt das Paket und überträgt das Paket erneut in die Zelle, während andere Knoten das Paket sehen können. Die Möglichkeit, ein Paket sowohl in verschlüsselter als auch in unverschlüsselter Form anzuzeigen, kann dazu beitragen, einen Schlüssel zu brechen. Die Aufnahme des gemischten Modus dient nur zur Kompatibilität mit anderen Anbietern.

Konfigurieren von Client-Adaptern

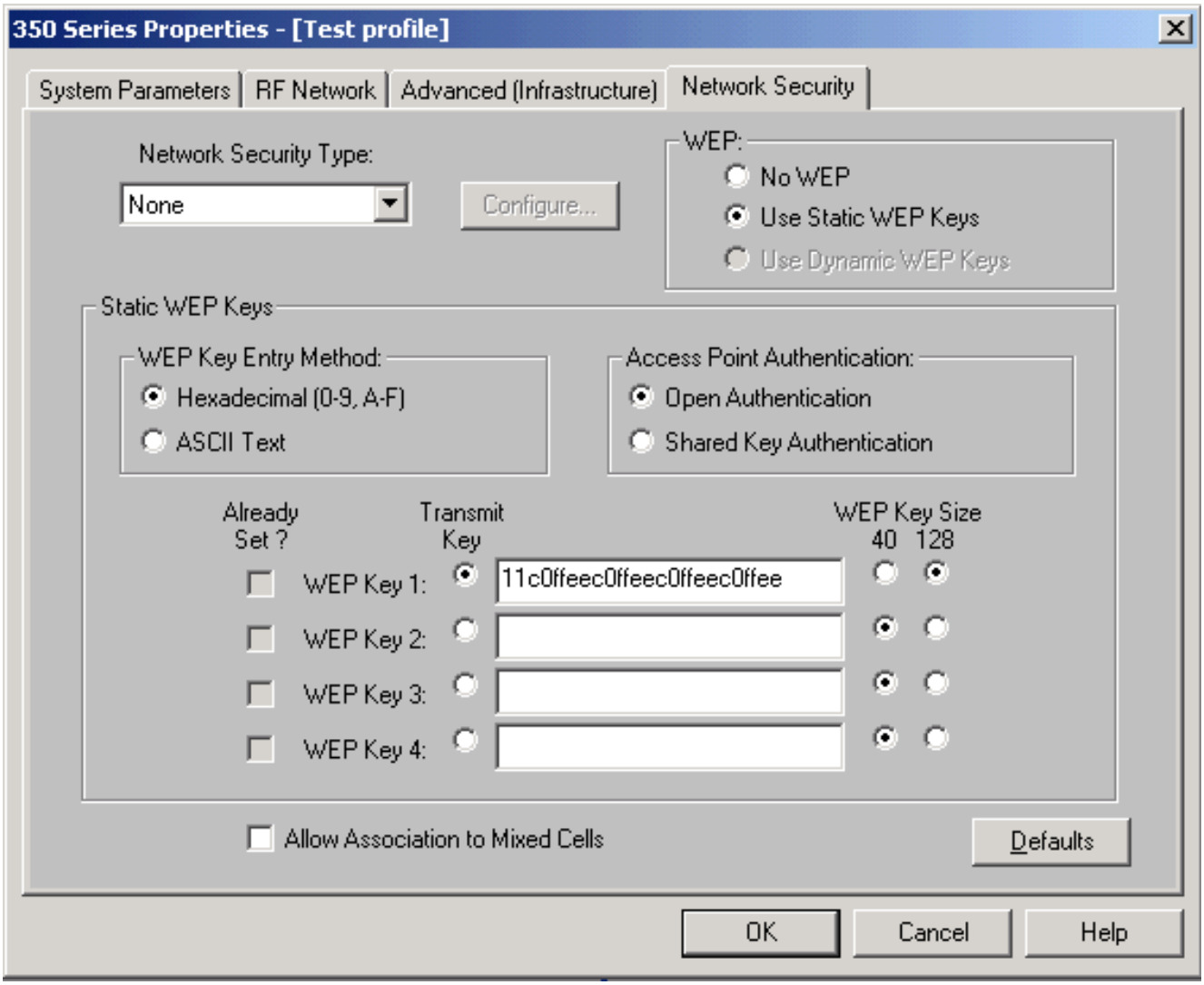
Sie müssen zwei Hauptschritte ausführen, um WEP auf dem Aironet-Client-Adapter einzurichten:

1. Konfigurieren Sie den/die WEP-Schlüssel/Schlüssel im Client Encryption Manager.
2. Aktivieren Sie WEP im Aironet Client Utility (ACU).

Festlegen der WEP-Schlüssel

Gehen Sie wie folgt vor, um WEP-Schlüssel auf den Client-Adaptern einzurichten:

1. Öffnen Sie die ACU, und wählen Sie **Profile Manager aus**.
2. Wählen Sie das Profil aus, in dem WEP aktiviert werden soll, und klicken Sie auf **Bearbeiten**.
3. Klicken Sie auf die Registerkarte **Netzwerksicherheit**, um die Sicherheitsoptionen anzuzeigen, und klicken Sie auf **Statische WEP-Schlüssel verwenden**.Diese Aktion aktiviert WEP-Konfigurationsoptionen, die deaktiviert werden, wenn No WEP ausgewählt ist.



4. Wählen Sie für den WEP-Schlüssel, den Sie erstellen möchten, **40** Bit oder **128** Bit unter WEP Key Size (WEP-Schlüsselgröße) auf der rechten Seite des Fensters aus.**Hinweis:** 128-Bit-Client-Adapter können 40-Bit- oder 128-Bit-Schlüssel verwenden. 40-Bit-Adapter können jedoch nur 40-Bit-Schlüssel verwenden.**Hinweis:** Der WEP-Schlüssel des Client-Adapters muss mit dem WEP-Schlüssel übereinstimmen, mit dem die anderen WLAN-Komponenten, mit denen Sie kommunizieren, verwendet werden.Wenn Sie mehr als einen WEP-Schlüssel festlegen, müssen Sie die WEP-Schlüssel den gleichen WEP-Schlüsselnummern für alle Geräte zuweisen. WEP-Schlüssel müssen aus Hexadezimalzeichen bestehen und 10 Zeichen für 40-Bit-WEP-Schlüssel oder 26 Zeichen für 128-Bit-WEP-Schlüssel enthalten. Hexadezimalzeichen können sein:0 bis 9a bis fA bis F**Hinweis:** ASCII-Text-WEP-Schlüssel werden von den Aironet APs nicht unterstützt. Daher müssen Sie die Hexadezimaloption (0-9, A-F) auswählen, wenn Sie den Client-Adapter mit diesen APs verwenden möchten.**Hinweis:** Nachdem Sie den WEP-Schlüssel erstellt haben, können Sie ihn überschreiben. Sie können sie jedoch nicht bearbeiten oder löschen.**Hinweis:** Wenn Sie statt der ACU als Client-Dienstprogramm eine neuere Version des Aironet Desktop-Dienstprogramms (ADU) verwenden, können Sie auch den erstellten WEP-Schlüssel löschen und durch einen neuen Schlüssel ersetzen.
5. Klicken Sie auf die Schaltfläche **Übertragungsschlüssel** neben einem der von Ihnen erstellten Schlüssel.Bei dieser Aktion geben Sie an, dass dieser Schlüssel der Schlüssel ist, den Sie zum Übertragen von Paketen verwenden möchten.
6. Klicken Sie unter WEP-Schlüsseltyp auf **Persistent**.Dadurch kann der Client-Adapter diesen WEP-Schlüssel beibehalten, selbst wenn die Stromversorgung zum Adapter entfernt oder

der Computer, in dem der Schlüssel installiert ist, neu gestartet wird. Wenn Sie für diese Option Temporary (Temporär) auswählen, geht der WEP-Schlüssel verloren, wenn die Stromversorgung vom Client-Adapter entfernt wird.
7. Klicken Sie auf **OK**.

WEP aktivieren

Führen Sie diese Schritte aus:

1. Öffnen Sie die ACU, und wählen Sie **Eigenschaften bearbeiten** in der Menüleiste aus.
2. Klicken Sie auf die Registerkarte **Netzwerksicherheit**, um die Sicherheitsoptionen anzuzeigen.
3. Aktivieren Sie das Kontrollkästchen **WEP aktivieren**, um WEP zu aktivieren.

Unter Konfigurieren von WEP in ADU finden Sie Anweisungen zum Konfigurieren von WEP mithilfe von ADU als Client-Dienstprogramm.

Konfigurieren von Arbeitsgruppen-Bridges

Zwischen der Aironet Workgroup Bridge der Serie 340 und der Aironet Bridge der Serie 340 bestehen Unterschiede. Die Konfiguration der Workgroup Bridge für die Verwendung von WEP ist jedoch fast identisch mit der Konfiguration der Bridge. Informationen zur Konfiguration der Bridge finden Sie im Abschnitt Konfigurieren von Aironet-Bridges.

1. Herstellen einer Verbindung zur Workgroup Bridge
2. Navigieren Sie zum Menü Datenschutz.Wählen Sie **Main > Configuration > Radio > I80211 > Privacy**, um das Menü Privacy VxWorks aufzurufen.

Einstellungen

Im Menü Datenschutz werden die in diesem Abschnitt aufgeführten Einstellungen angezeigt. Konfigurieren Sie die Optionen für die Workgroup Bridge in der folgenden Reihenfolge:

1. Wichtigste
2. Übertragen
3. Auth
4. Verschlüsselung

Folgende Optionen stehen zur Verfügung:

- **Wichtigste**Die Key-Option legt den WEP-Schlüssel fest, den die Bridge zum Empfangen von Paketen verwendet. Der Wert muss mit dem Schlüssel übereinstimmen, den der Access Point oder ein anderes Gerät, mit dem die Workgroup Bridge kommuniziert, verwendet. Der Schlüssel besteht aus bis zu 10 Hexadezimalzeichen für 40-Bit-Verschlüsselung oder 26 Hexadezimalzeichen für 128-Bit-Verschlüsselung. Die Hexadezimalzeichen können eine beliebige Kombination dieser Ziffern sein:0 bis 9a bis fA bis F
- **Übertragen**Die Übertragungsoption stellt den WEP-Schlüssel her, den die Bridge zum Übertragen von Paketen verwendet. Sie können festlegen, dass derselbe Schlüssel verwendet wird, den Sie für die Option Schlüssel verwendet haben. Wenn Sie einen anderen Schlüssel auswählen, müssen Sie einen passenden Schlüssel auf dem Access Point

festlegen.Für Übertragungen kann jeweils nur ein WEP-Schlüssel verwendet werden. Der WEP-Schlüssel, den Sie zum Übertragen von Daten verwenden, muss auf der Workgroup Bridge und anderen Geräten, mit denen sie kommuniziert, auf den gleichen Wert festgelegt werden.

- **Authentifizierung (Auth)**Der Parameter Auth bestimmt, welche Authentifizierungsmethode das System verwendet. Folgende Optionen sind verfügbar:**Open (EMPFOHLEN)** - Die Standardeinstellung "Open" (Öffnen) ermöglicht jedem Access Point unabhängig von seinen WEP-Einstellungen die Authentifizierung und anschließend die Kommunikation mit der Bridge.**Shared Key**: Diese Einstellung weist die Bridge an, eine universelle, gemeinsam genutzte Schlüsselabfrage an APs zu senden, um mit der Bridge zu kommunizieren. Bei der Einstellung für den gemeinsamen Schlüssel kann die Bridge für einen bekannten Text-Angriff durch Eindringlinge geöffnet bleiben. Daher ist diese Einstellung nicht so sicher wie die Einstellung Öffnen.
- **Verschlüsselung**Die Verschlüsselungsoption legt Verschlüsselungsparameter für alle Datenpakete fest, mit Ausnahme von Zuordnungspaketen und einigen Steuerungspaketen. Es gibt vier Optionen:**Hinweis:** Der Access Point muss über eine aktive Verschlüsselung verfügen, und ein Schlüssel muss korrekt festgelegt sein.**Aus** - Dies ist die Standardeinstellung. Die gesamte Verschlüsselung ist deaktiviert. Die Workgroup Bridge kommuniziert nicht mit einem Access Point, der WEP verwendet.**On (EMPFOHLEN)** - Diese Einstellung erfordert die Verschlüsselung aller Datenübertragungen. Die Workgroup Bridge kommuniziert nur mit APs, die WEP verwenden.**Mixed on (Wird aktiviert)**: Diese Einstellung bedeutet, dass die Bridge immer WEP verwendet, um mit dem Access Point zu kommunizieren. Der AP kommuniziert jedoch mit allen Geräten, unabhängig davon, ob sie WEP verwenden oder WEP nicht.**Mixed off (Gemischt Aus)**: Diese Einstellung bedeutet, dass die Bridge WEP nicht für die Kommunikation mit dem Access Point verwendet. Der AP kommuniziert jedoch mit allen Geräten, unabhängig davon, ob sie WEP verwenden oder WEP nicht.**Vorsicht:** Wenn Sie als WEP-Kategorie "Ein" oder "Gemischt" auswählen und die Bridge über deren Funkverbindung konfigurieren, geht die Verbindung zur Bridge verloren, wenn Sie den WEP-Schlüssel falsch festgelegt haben. Stellen Sie sicher, dass Sie dieselben Einstellungen verwenden, wenn Sie den WEP-Schlüssel auf der Workgroup Bridge und den WEP-Schlüssel auf anderen Geräten im WLAN festlegen.

Zugehörige Informationen

- IEEE Standards Association
- Wireless LAN-Produkte der Aironet Serie 340
- Wireless Support-Ressourcen
- Support-Seite für Wireless LAN
- Cisco IOS Software Configuration Guide Cisco Aironet Access Points
- Cisco IOS Software Configuration Guide for Cisco Aironet Outdoor Access Point/Bridge der Serie 1300
- Cisco Aironet Access Point - Software-Konfigurationsleitfaden für VxWorks
- Cisco Aironet Bridge Software der Serie 1400 - Konfigurationsleitfaden
- Konfigurationsanleitungen für Cisco Aironet Wireless LAN Client Adapter
- Cisco Wireless LAN Security - Übersicht
- Wireless (Mobilität) Sichern von Wireless-Netzwerken
- Konfigurationsbeispiel für Access Point als Workgroup Bridge

- Cisco Aironet Workgroup Bridge - Häufig gestellte Fragen
- Verfahren zur Kennwortwiederherstellung für Cisco Aironet-Geräte
- Häufig gestellte Fragen zu Cisco Aironet Access Points
- Technischer Support und Dokumentation für Cisco Systeme