Configurazione di WEP su access point e bridge Aironet

Sommario

Introduzione

In questo documento vengono illustrati i metodi per configurare il protocollo WEP (Wired Equivalent Privacy) sui componenti Cisco Aironet Wireless LAN (WLAN).

Nota: per ulteriori informazioni sulla configurazione WEP sui controller WLC, consultare la sezione Chiavi Web statiche del capitolo 6 - Configurazione delle WLAN.

WEP è l'algoritmo di crittografia integrato nello standard 802.11 (Wi-Fi). La crittografia WEP utilizza la crittografia di flusso Ron Code 4 (RC4) con chiavi a 40 o 104 bit e un vettore di inizializzazione a 24 bit (IV).

Come specificato dallo standard, WEP utilizza l'algoritmo RC4 con una chiave a 40 o 104 bit e una IV a 24 bit. RC4 è un algoritmo simmetrico in quanto utilizza la stessa chiave per la crittografia e la decrittografia dei dati. Quando WEP è abilitato, ogni "stazione" radio ha una chiave. La chiave viene utilizzata per codificare i dati prima della loro trasmissione attraverso le onde radio. Se una stazione riceve un pacchetto non codificato con la chiave appropriata, il pacchetto viene scartato e non viene mai consegnato all'host.

WEP può essere utilizzato principalmente per un ufficio domestico o un piccolo ufficio che non

richiede una sicurezza molto elevata.

L'implementazione di Aironet WEP è nell'hardware. Pertanto, l'impatto sulle prestazioni risulta minimo quando si utilizza WEP.

Nota: esistono alcuni problemi noti relativi a WEP, che non lo rendono un metodo di crittografia efficace. Le questioni sono:

- Il mantenimento di una chiave WEP condivisa comporta un notevole sovraccarico amministrativo.
- WEP presenta lo stesso problema di tutti i sistemi basati su chiavi condivise. Qualsiasi segreto dato ad una persona diventa pubblico dopo un periodo di tempo.
- La clausola IV che definisce l'algoritmo WEP viene inviata in testo non crittografato.
- Il checksum WEP è lineare e prevedibile.

Il protocollo TKIP (Temporal Key Integrity Protocol) è stato creato per risolvere questi problemi WEP. Analogamente a WEP, TKIP utilizza la crittografia RC4. Tuttavia, TKIP migliora WEP aggiungendo misure come l'hashing delle chiavi per pacchetto, il controllo dell'integrità dei messaggi (MIC) e la rotazione delle chiavi di trasmissione per affrontare le vulnerabilità note di WEP. TKIP utilizza la cifratura di flusso RC4 con chiavi a 128 bit per la crittografia e chiavi a 64 bit per l'autenticazione.

Prerequisiti

Requisiti

per le successive spiegazioni, si presume che sia possibile stabilire una connessione amministrativa ai dispositivi WLAN e che i dispositivi funzionino normalmente in un ambiente non crittografato.

Per configurare un protocollo WEP standard a 40 bit, è necessario disporre di due o più unità radio che comunichino tra loro.

Nota: i prodotti Aironet possono stabilire connessioni WEP a 40 bit con prodotti non Cisco conformi allo standard IEEE 802.11b. Questo documento non descrive la configurazione di altri dispositivi.

Per la creazione di un collegamento WEP a 128 bit, i prodotti Cisco interagiscono solo con altri prodotti Cisco.

Componenti usati

Utilizzare i seguenti componenti con il presente documento:

- Due o più unità radio che comunicano tra loro
- Una connessione amministrativa al dispositivo WLAN

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

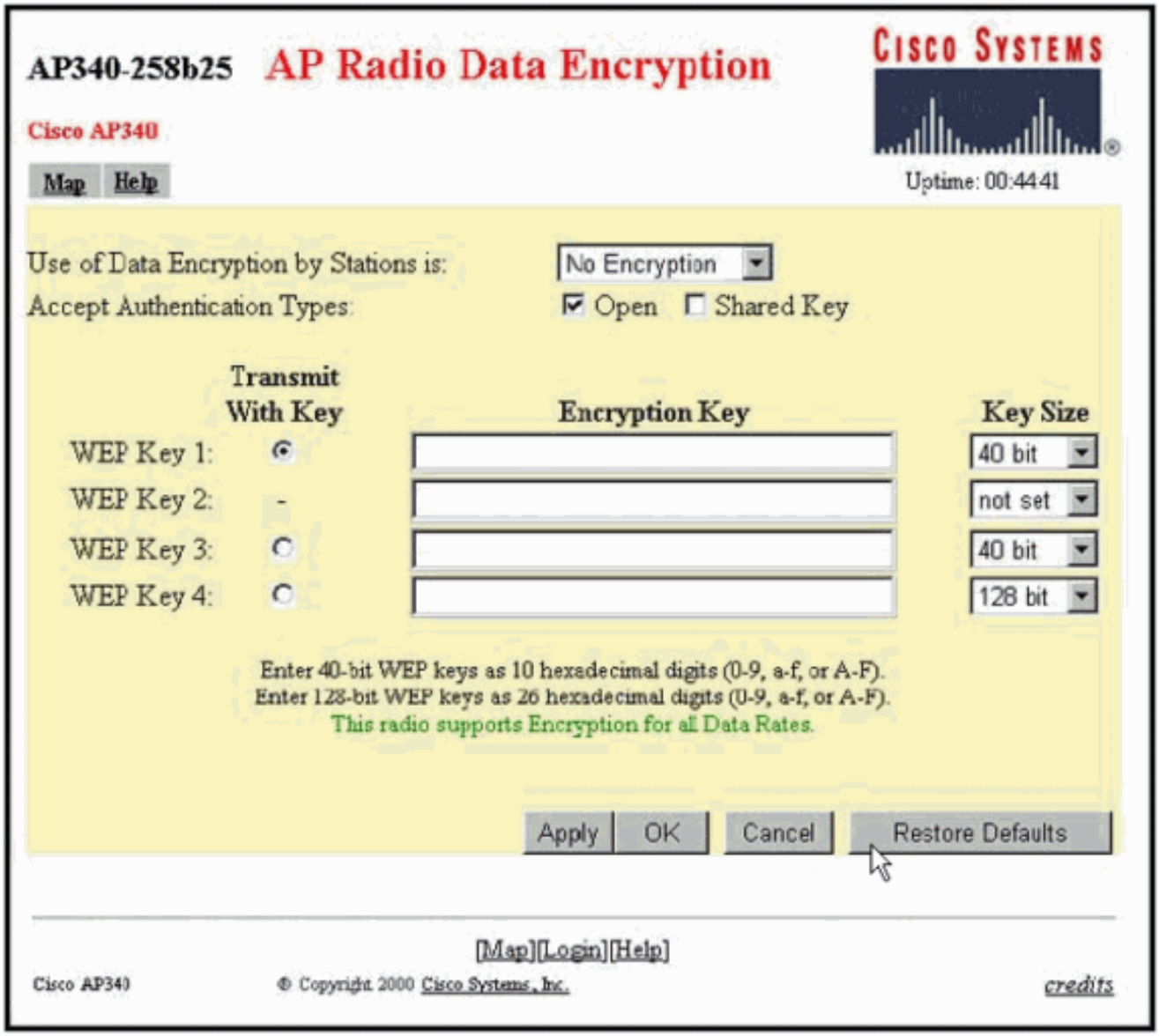
Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Configurazione di WEP sui punti di accesso Aironet

Access Point Aironet Con Sistema Operativo VxWorks

Attenersi alla seguente procedura:

1. Effettuare una connessione al punto di accesso.
2. Passare al menu AP Radio Encryption.Utilizzare uno dei percorsi seguenti:**Summary Status > Setup > AP Radio/Hardware > Radio Data Encryption (WEP) > AP Radio Data EncryptionSintetico Stato > Impostazione > Sicurezza > Impostazione sicurezza: Crittografia dati radio (WEP) > Crittografia dati radio APNota:** per apportare modifiche a questa pagina, è necessario essere un amministratore con funzionalità di identità e scrittura.**Visualizzazione browser Web del menu Crittografia dati radio AP**



Impostazioni di VxWorks

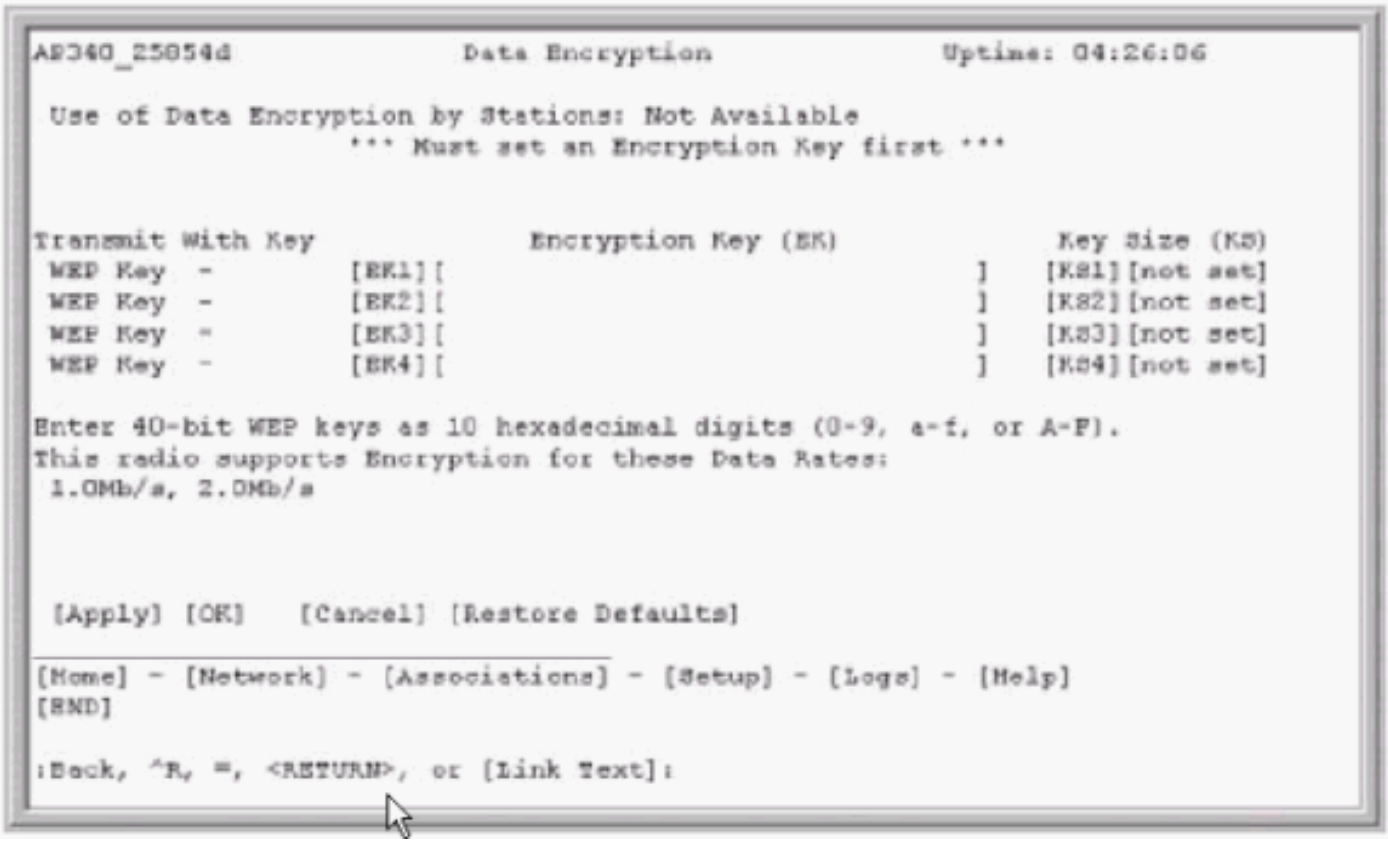
La pagina Crittografia dei dati della radio AP presenta una varietà di opzioni da utilizzare. Alcune opzioni sono obbligatorie per WEP. In questa sezione vengono descritte queste opzioni obbligatorie. Per il funzionamento di WEP non sono necessarie altre opzioni, ma sono consigliate.

- **L'uso della crittografia dei dati da parte delle stazioni è:**Utilizzare questa impostazione per scegliere se i client devono utilizzare la crittografia dei dati quando comunicano con l'access point. Il menu a discesa contiene tre opzioni:**Nessuna crittografia (impostazione predefinita)**: i client devono comunicare con l'access point senza crittografia dei dati. Questa impostazione è sconsigliata.**Facoltativo**: consente ai client di comunicare con l'access point con o senza crittografia dei dati. In genere, questa opzione viene utilizzata quando sono presenti dispositivi client che non possono effettuare una connessione WEP, ad esempio client non Cisco in un ambiente WEP a 128 bit.**Crittografia completa (CONSIGLIATA)**: i client devono utilizzare la crittografia dei dati quando comunicano con l'access point. I client che non utilizzano la crittografia dei dati non possono comunicare. Questa opzione è consigliata se si desidera ottimizzare la sicurezza della WLAN.**Nota:** prima di abilitare l'uso della crittografia, è necessario impostare una chiave WEP. Vedere la sezione **Chiave di crittografia (OBBLIGATORIA)** in questo elenco.
- **Accetta tipi di autenticazione**Èpossibile scegliere Apri, Chiave condivisa o entrambe le opzioni per impostare le autenticazioni che verranno riconosciute dal punto di accesso.**Open (RECOMMENDED)** - Questa impostazione predefinita consente a qualsiasi dispositivo, indipendentemente dalle chiavi WEP, di eseguire l'autenticazione e di tentare l'associazione.**Chiave condivisa**: questa impostazione indica all'access point di inviare una query con chiave condivisa in testo normale a qualsiasi dispositivo che tenti di associarsi all'access point.**Nota:** questa query può lasciare l'access point aperto a un attacco di testo noto da intrusi. Pertanto, questa impostazione non è sicura come l'impostazione Apri.
- **Trasmetti con chiave**Questi pulsanti consentono di selezionare il tasto utilizzato dall'access point durante la trasmissione dei dati. È possibile selezionare un solo tasto alla volta. Per ricevere i dati è possibile utilizzare una o tutte le chiavi set. È necessario impostare la chiave prima di specificarla come chiave di trasmissione.
- **Chiave di crittografia (OBBLIGATORIA)**Questi campi consentono di immettere le chiavi WEP. Immettere 10 cifre esadecimali per le chiavi WEP a 40 bit o 26 cifre esadecimali per le chiavi WEP a 128 bit. I tasti possono essere costituiti da qualsiasi combinazione delle seguenti cifre:Da 0 a 9da a a fDa A a FPer proteggere la protezione delle chiavi WEP, le chiavi WEP esistenti non vengono visualizzate in testo normale nei campi di immissione. Nelle versioni recenti dei punti di accesso è possibile eliminare le chiavi esistenti. Non è tuttavia possibile modificare le chiavi esistenti.**Nota:** è necessario impostare le chiavi WEP per la rete, i punti di accesso e i dispositivi client esattamente allo stesso modo. Ad esempio, se si imposta la chiave WEP 3 del punto di accesso su 0987654321 e si seleziona questa chiave come chiave attiva, è necessario impostare anche la chiave WEP 3 del dispositivo client sullo stesso valore.
- **Dimensione chiave (OBBLIGATORIO)**Questa impostazione imposta le chiavi su WEP a 40 o 128 bit. Se per questa selezione appare "not set" (non impostato), il tasto non è impostato.**Nota:** non è possibile eliminare una chiave selezionando "non impostato".
- **Pulsanti di azione**Quattro pulsanti di azione controllano le impostazioni. Se JavaScript è abilitato sul browser Web, dopo aver fatto clic su un pulsante qualsiasi viene visualizzata una finestra popup di conferma, ad eccezione di Annulla.**Applica (Apply**) - Questo pulsante attiva le nuove impostazioni del valore. Il browser rimane nella pagina.**OK** - Questo pulsante consente di applicare le nuove impostazioni e di riportare il browser alla pagina di

impostazione principale.**Annulla (Cancel)** - Questo pulsante annulla le modifiche apportate alle impostazioni e ripristina i valori memorizzati in precedenza. Quindi si torna alla pagina principale di impostazione.**Ripristina valori predefiniti**: questo pulsante consente di ripristinare le impostazioni predefinite di fabbrica di tutte le impostazioni presenti nella pagina.

Nota: nelle versioni Cisco IOS® recenti degli access point, per questa pagina sono disponibili solo i pulsanti di controllo **Apply** e **Cancel**.

Visualizzazione dell'emulatore di terminale del menu Data Encryption



Visualizzazione emulatore di terminale della sequenza di configurazione tasti WEP (software Cisco IOS®)

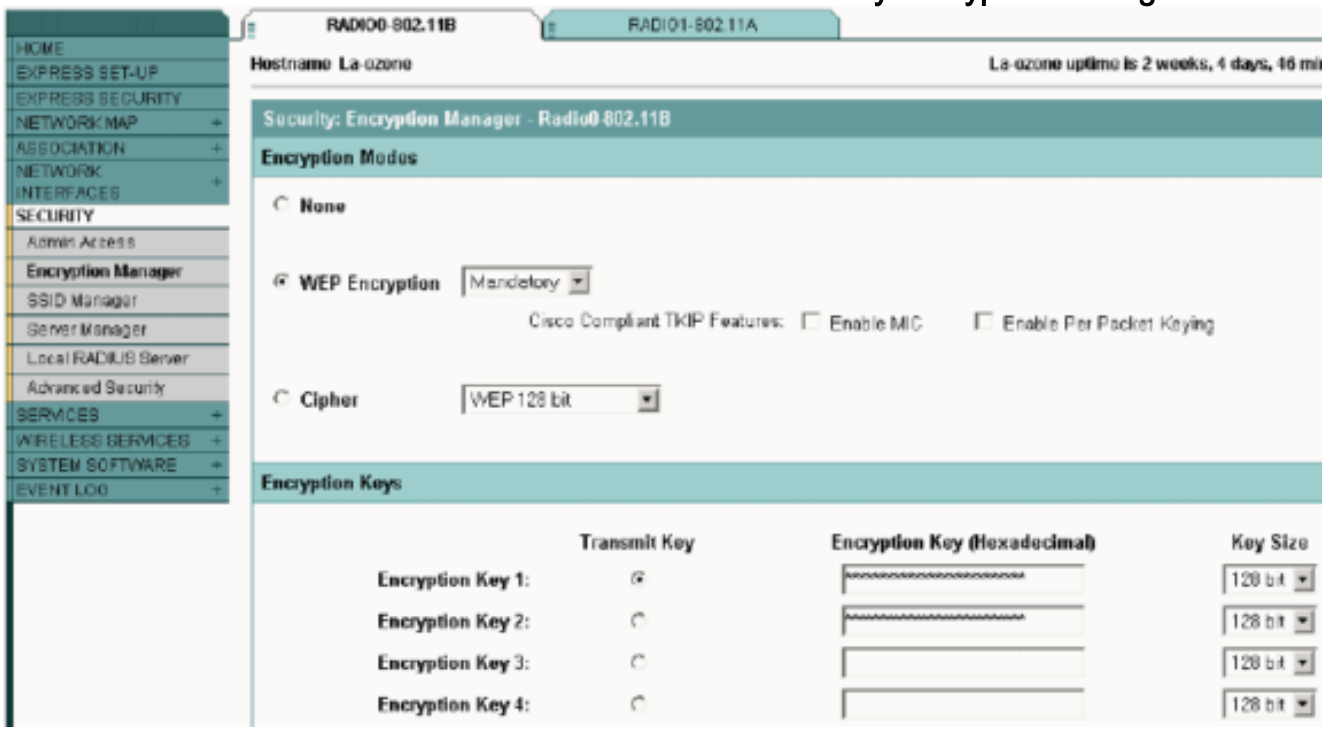
```
La-ozone>
La-ozone>
La-ozone>enable
Password:
La-ozone#
La-ozone#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
La-ozone(config)#interface dot
La-ozone(config)#interface dot11Radio 0
La-ozone(config-if)#encryption key 1 size 128bit 11c0ffeec0ffeec0ffeec0ffee ?
 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

Attenersi alla seguente procedura:

1. Eseguire una connessione all'access point.

2. Dall'opzione del menu SECURITY sul lato sinistro della finestra, scegliere **Encryption Manager** per l'interfaccia radio su cui si desidera configurare le chiavi WEP statiche.**Visualizzazione browser Web del menu di AP Security Encryption Manager**



Configurazione dei bridge Aironet

Se si utilizza VxWorks, attenersi alla seguente procedura:

1. Effettuare una connessione al Bridge.
2. Passare al menu Privacy.Scegliere **Menu principale > Configurazione > Radio > I80211 > Privacy**.Il menu Privacy controlla l'uso della crittografia sul pacchetto dati trasmesso via etere dalle radio. Per crittografare i pacchetti vengono utilizzati l'algoritmo RSA RC4 e una delle quattro chiavi conosciute. Ogni nodo nella cella radio deve conoscere tutte le chiavi in uso, ma è possibile selezionare qualsiasi chiave per trasmettere i dati.**Visualizzazione emulatore terminale del menu Privacy**

```
        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
>_
```

Per informazioni su come configurare il protocollo WEP nei bridge serie 1300 e 1400 in modalità CLI, fare riferimento a Configurazione delle suite di cifratura e del bridge WEP serie 1300 e Configurazione delle funzionalità WEP e WEP - Bridge serie 1400.

Per utilizzare la GUI per configurare i bridge serie 1300 e 1400, completare la stessa procedura descritta nella sezione Access point Aironet con software Cisco IOS di questo documento.

Impostazioni di VxWorks

Il menu Privacy presenta una serie di opzioni che è necessario configurare. Alcune opzioni sono obbligatorie per WEP. In questa sezione vengono descritte queste opzioni obbligatorie. Per il funzionamento di WEP non sono necessarie altre opzioni, ma sono consigliate.

In questa sezione le opzioni di menu vengono presentate nell'ordine in cui appaiono nella visualizzazione Emulatore terminale del menu Privacy. Configurare tuttavia le opzioni nell'ordine seguente:

1. Chiave
2. Trasmissione
3. Auth
4. Cliente
5. Crittografia

La configurazione in questo ordine assicura che le condizioni preliminari necessarie vengano impostate durante la configurazione di ciascuna impostazione.

Queste sono le opzioni:

- **Chiave (OBBLIGATORIA)**L'opzione Chiave (Key) consente di programmare le chiavi di crittografia nel bridge. Viene richiesto di impostare uno dei quattro tasti. Viene richiesto due volte di immettere la chiave. Per definire la chiave, è necessario immettere 10 o 26 cifre esadecimali, a seconda che la configurazione Bridge sia per chiavi a 40 o 128 bit. Utilizzare una qualsiasi combinazione delle cifre seguenti:Da 0 a 9da a a fDa A a FLe chiavi devono corrispondere in ***tutti*** i nodi della cella radio ed è necessario immettere le chiavi nello stesso ordine. non è necessario definire tutte e quattro le chiavi, purché il numero di chiavi corrisponda in ciascun dispositivo della WLAN.
- **Trasmissione**L'opzione Trasmetti indica alla radio le chiavi da utilizzare per trasmettere i pacchetti. Ogni radio è in grado di decrittografare i pacchetti ricevuti che vengono inviati con una qualsiasi delle quattro chiavi.
- **Auth**Sui bridge di ripetitori si utilizza l'opzione Auth per determinare la modalità di autenticazione utilizzata dall'apparecchio per connettersi con il padre. I valori consentiti sono Apri o Chiave condivisa. Il protocollo 802.11 specifica una procedura in cui un client deve autenticarsi con un padre prima di potersi associare.**Aperto (CONSIGLIATO)**: questa modalità di autenticazione è essenzialmente un'operazione Null. Tutti i client possono eseguire l'autenticazione.**Chiave condivisa**: questa modalità consente al padre di inviare al client un testo di richiesta, che il client crittografa e restituisce al padre. Se il documento principale decrittografa correttamente il testo della richiesta di verifica, il client viene autenticato.**Attenzione:** non utilizzare la modalità chiave condivisa. Quando lo si utilizza, una versione in testo normale e crittografata degli stessi dati trasmette via etere. Questo non guadagna nulla. Se la chiave utente non è corretta, l'unità non decrittografa i pacchetti e questi non possono accedere alla rete.
- **Cliente**L'opzione Client determina la modalità di autenticazione che i nodi client utilizzano per associare all'unità. Sono consentiti i valori seguenti:**Aperto (CONSIGLIATO)**: questa modalità di autenticazione è essenzialmente un'operazione Null. Tutti i client possono eseguire l'autenticazione.**Chiave condivisa**: questa modalità consente al padre di inviare al client un testo di richiesta, che il client crittografa e restituisce al padre. Se il documento principale decrittografa correttamente il testo della richiesta di verifica, il client viene autenticato.**Both** -

Questa modalità consente al client di utilizzare entrambe le modalità.

- **CrittografiaOff**: se si imposta l'opzione Encryption su Off, non viene eseguita alcuna crittografia. I dati vengono trasmessi in chiaro.**On (OBBLIGATORIO)**: se si imposta l'opzione Encryption (Crittografia) su On (Attivata), tutti i pacchetti di dati trasmessi vengono crittografati e tutti i pacchetti non crittografati ricevuti vengono scartati.**Misto**: nella modalità Misto, un bridge radice o ripetitore accetta l'associazione dai client in cui la crittografia è attivata o disattivata. In questo caso, vengono crittografati solo i pacchetti di dati tra nodi che supportano entrambi. I pacchetti multicast vengono inviati in chiaro. Tutti i nodi possono visualizzare i pacchetti.**Attenzione:** non utilizzare la modalità mista. Se un client con la crittografia abilitata invia un pacchetto multicast al relativo elemento padre, il pacchetto viene crittografato. Il nodo padre decrittografa il pacchetto e lo trasmette nuovamente alla cella in modo che gli altri nodi possano vedere il pacchetto. La possibilità di visualizzare un pacchetto sia in forma crittografata che non crittografata può contribuire a interrompere una chiave. L'inclusione della modalità mista serve solo per la compatibilità con altri fornitori.

Configura adattatori client

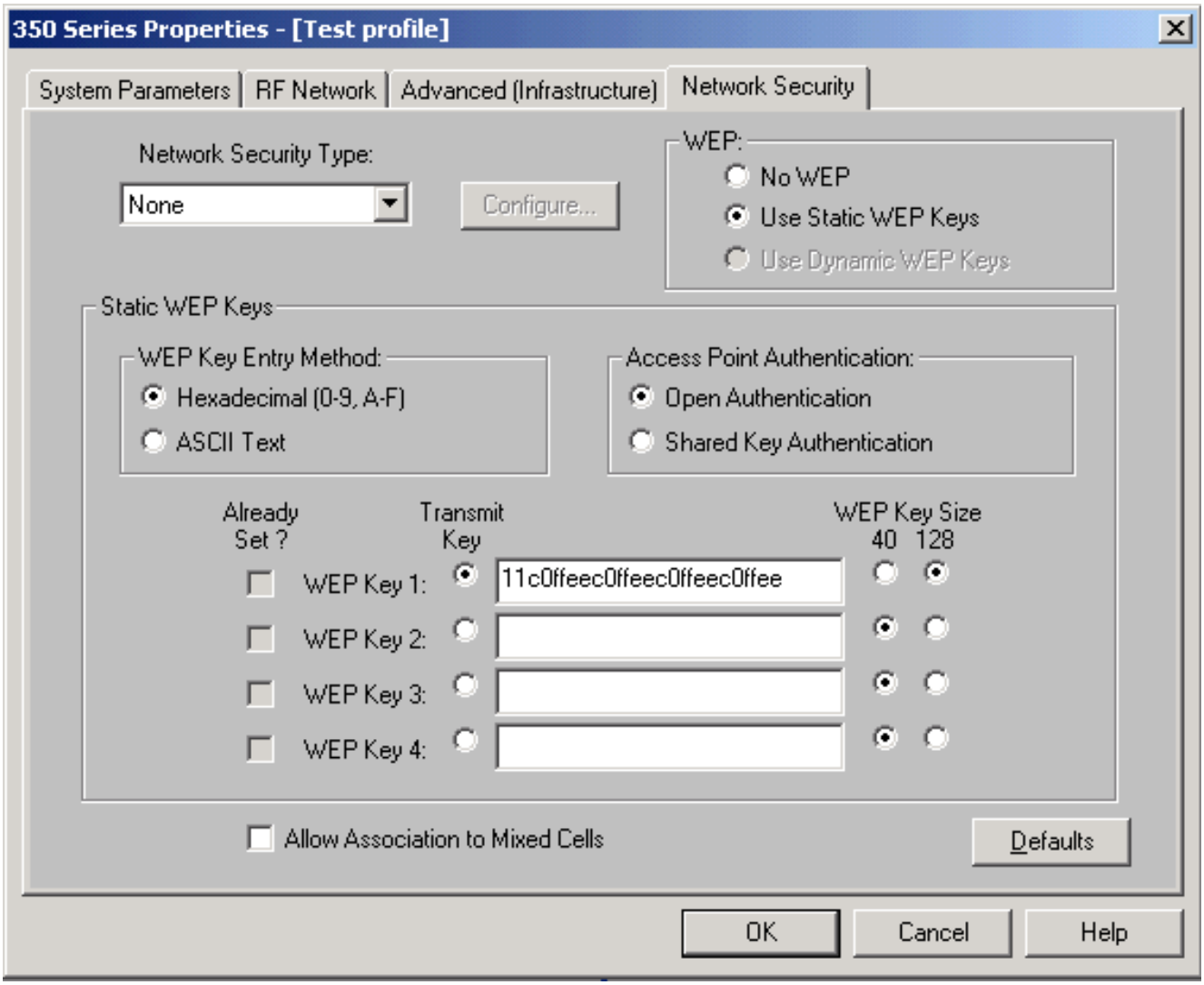
Per configurare WEP su Aironet Client Adapter è necessario completare due passaggi principali:

1. Configurare le chiavi WEP in Client Encryption Manager.
2. Abilitare WEP in Aironet Client Utility (ACU).

Impostazione delle chiavi WEP

Completare questi passaggi per impostare le chiavi WEP sugli adattatori client:

1. Aprire ACU e scegliere **Gestione profili**.
2. Scegliere il profilo in cui si desidera abilitare WEP e fare clic su **Modifica**.
3. Fare clic sulla scheda **Protezione di rete** per visualizzare le opzioni di protezione e fare clic su **Usa chiavi WEP statiche**.Questa azione attiva le opzioni di configurazione WEP che risultano inattive quando è selezionata l'opzione No WEP (Nessun WEP).



4. Per la chiave WEP che si desidera creare, scegliere **40** bit o **128** bit in Dimensione chiave WEP sul lato destro della finestra.**Nota:** le schede client a 128 bit possono utilizzare chiavi a 40 o 128 bit. Tuttavia, le schede a 40 bit possono utilizzare solo chiavi a 40 bit.**Nota:** la chiave WEP della scheda client deve corrispondere alla chiave WEP utilizzata dagli altri componenti WLAN con cui si comunica.Quando si impostano più chiavi WEP, è necessario assegnarle agli stessi numeri di chiave WEP per tutti i dispositivi. Le chiavi WEP devono essere composte da caratteri esadecimali e devono contenere 10 caratteri per le chiavi WEP a 40 bit o 26 caratteri per le chiavi WEP a 128 bit. I caratteri esadecimali possono essere:Da 0 a 9da a a fDa A a F**Nota:** le chiavi WEP in testo ASCII non sono supportate sugli access point Aironet. Pertanto, è necessario scegliere l'opzione Esadecimale (0-9, A-F) se si intende utilizzare l'adattatore client con questi access point.**Nota:** dopo aver creato la chiave WEP, è possibile sovrascriverla. Ma non è possibile modificarlo o eliminarlo.**Nota:** se si utilizza una versione successiva di Aironet Desktop Utility (ADU) anziché ACU come utility client, è possibile anche eliminare la chiave WEP creata e sostituirla con una nuova.
5. Fare clic sul pulsante **Trasmetti** accanto a uno dei tasti creati.Con questa azione, si indica che questa chiave è la chiave che si desidera utilizzare per trasmettere i pacchetti.
6. Fare clic su **Persistent** in Tipo di chiave WEP.Questa azione consente alla scheda di rete del client di conservare la chiave WEP, anche quando l'alimentazione alla scheda viene interrotta o al riavvio del computer in cui la chiave è installata. Se si sceglie Temporaneo per questa opzione, la chiave WEP viene persa quando si rimuove l'alimentazione dalla scheda di rete del client.
7. Fare clic su **OK**.

Abilita WEP

Attenersi alla seguente procedura:

1. Aprire ACU e scegliere **Modifica proprietà** dalla barra dei menu.
2. Per visualizzare le opzioni di protezione, fare clic sulla scheda **Protezione di rete**.
3. Per attivare WEP, selezionare la casella di controllo **Abilita WEP**.

Fare riferimento a Configurazione di WEP in ADU per la procedura di configurazione di WEP utilizzando ADU come utility client.

Configura bridge di gruppi di lavoro

Ci sono differenze tra Aironet serie 340 Workgroup Bridge e Aironet serie 340 Bridge. Tuttavia, la configurazione di Workgroup Bridge per l'utilizzo di WEP è quasi identica a quella di Bridge. Per la configurazione del bridge, vedere la sezione Configurazione dei bridge Aironet.

1. Connettersi a Workgroup Bridge.
2. Passare al menu Privacy.Scegliere **Principale > Configurazione > Radio > I80211 > Privacy** per accedere al menu Privacy VxWorks.

Impostazioni

Il menu Privacy presenta le impostazioni elencate in questa sezione. Configurare le opzioni in Workgroup Bridge nell'ordine seguente:

1. Chiave
2. Trasmissione
3. Auth
4. Crittografia

Queste sono le opzioni:

- **Chiave**L'opzione Chiave stabilisce la chiave WEP utilizzata dal bridge per ricevere i pacchetti. Il valore deve corrispondere alla chiave utilizzata dal punto di accesso o da un'altra periferica con cui comunica il bridge di gruppi di lavoro. La chiave è costituita da un massimo di 10 caratteri esadecimali per la crittografia a 40 bit o di 26 caratteri esadecimali per la crittografia a 128 bit. I caratteri esadecimali possono essere costituiti da qualsiasi combinazione delle seguenti cifre:Da 0 a 9da a a fDa A a F
- **Trasmissione**L'opzione Trasmetti stabilisce la chiave WEP usata dal bridge per trasmettere i pacchetti. È possibile scegliere di utilizzare la stessa chiave utilizzata per l'opzione Chiave. Se si sceglie una chiave diversa, è necessario stabilire una chiave corrispondente nell'access point.Per le trasmissioni è possibile utilizzare una sola chiave WEP alla volta. La chiave WEP utilizzata per la trasmissione dei dati deve essere impostata sullo stesso valore sul dispositivo Workgroup Bridge e sugli altri dispositivi con cui comunica.
- **Autenticazione (Auth)**Il parametro Auth determina il metodo di autenticazione utilizzato dal sistema. Le opzioni sono:**Aperto (CONSIGLIATO)** - L'impostazione predefinita di Apertura consente a qualsiasi access point, indipendentemente dalle impostazioni WEP, di eseguire l'autenticazione e quindi di tentare di comunicare con il bridge.**Chiave condivisa**: questa impostazione indica al bridge di inviare una query con chiave condivisa in testo normale agli

access point nel tentativo di comunicare con il bridge. L'impostazione della chiave condivisa può lasciare il bridge aperto a un attacco di testo noto da intrusi. Pertanto, questa impostazione non è sicura come l'impostazione Apri.

- **Crittografia**L'opzione Encryption imposta i parametri di crittografia su tutti i pacchetti di dati, ad eccezione dei pacchetti di associazione e di alcuni pacchetti di controllo. Sono disponibili quattro opzioni:**Nota:** l'access point deve avere la crittografia attiva e una chiave impostata correttamente.**Off** - Questa è l'impostazione di default. La crittografia è disattivata. Workgroup Bridge non comunica con un punto di accesso tramite WEP.**On (RECOMMENDED)** - Questa impostazione richiede la crittografia di tutti i trasferimenti di dati. Workgroup Bridge comunica solo con i punti di accesso che utilizzano WEP.**Misto attivo (Mixed on**) - Questa impostazione indica che il bridge utilizza sempre WEP per comunicare con l'access point. Tuttavia, l'access point comunica con tutti i dispositivi, indipendentemente dal fatto che utilizzino o meno WEP.**Misto disattivato (Mixed off**) - Questa impostazione indica che il bridge non utilizza WEP per comunicare con l'access point. Tuttavia, l'access point comunica con tutti i dispositivi, indipendentemente dal fatto che utilizzino o meno WEP.**Attenzione:** se si seleziona Attivato o Misto su come categoria WEP e si configura il bridge tramite il relativo collegamento radio, la connettività al bridge viene interrotta se si imposta la chiave WEP in modo errato. Accertarsi di utilizzare esattamente le stesse impostazioni quando si imposta la chiave WEP su Workgroup Bridge e la chiave WEP su altri dispositivi della WLAN.

Informazioni correlate

- Associazione standard IEEE
- Prodotti LAN wireless Aironet serie 340
- Risorse di supporto wireless
- Pagina di supporto per LAN wireless
- Guida alla configurazione software Cisco IOS per Cisco Aironet Access Point
- Guida alla configurazione del software Cisco IOS per Cisco Aironet serie 1300 Outdoor Access Point/Bridge
- Guida alla configurazione di Cisco Aironet Access Point Software per VxWorks
- Guida alla configurazione del software Cisco Aironet serie 1400 Bridge
- Guide alla configurazione degli adattatori client LAN wireless Cisco Aironet
- Panoramica sulla sicurezza delle LAN wireless Cisco
- Wireless (mobilità) protezione delle reti wireless
- Esempio di configurazione di Access Point come bridge per gruppi di lavoro
- Domande frequenti su Cisco Aironet Workgroup Bridge
- Procedura di recupero della password per i dispositivi Cisco Aironet
- Domande frequenti su Cisco Aironet Access Point
- Documentazione e supporto tecnico – Cisco Systems