Wired Equivalent Privacy (WEP) em pontos de acesso Aironet e em exemplo de configuração das pontes

Índice

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Convenções
Configurar o WEP em pontos de acesso Aironet
Pontos de acesso Aironet que executam o sistema operacional vxworks
Ajustes de VxWorks
Aironet AP que executa o Cisco IOS Software
Configurar Aironet Bridge
Ajustes de VxWorks
Configurar adaptadores cliente
Ajuste as chaves de WEP
Permita o WEP
Configurar bridges de grupo de trabalho
Configurações
Informações Relacionadas

Introdução

Este documento fornece métodos para configurar o Wired Equivalent Privacy (WEP) em componentes do Cisco Aironet Wireless LAN (WLAN).

Nota: Refira a seção estática das chaves da Web do capítulo 6 - configurando WLAN para obter mais informações sobre da configuração WEP nos controladores do Wireless LAN (WLC).

O WEP é o algoritmo de criptografia construído no padrão do 802.11 (Wi-fi). A criptografia de WEP usa a cifra de córrego do código 4 do Ron (RC4) com 40- ou chaves do 104-bit e 24-bit um vetor de inicialização (iv).

Enquanto o padrão especifica, o WEP usa o algoritmo RC4 com uma chave 40-bit ou de 104-bit e um 24-bit IV. RC4 é um algoritmo simétrico porque usa a mesma chave para a criptografia e a descriptografia dos dados. Quando a WEP está habilitada, cada "estação" de rádio possui uma chave. A chave é usada para misturar os dados antes da transmissão dos dados através das ondas de rádio. Se uma estação recebe um pacote que não scrambled com a chave apropriada, o pacote é rejeitado e nunca entregado ao host.

O WEP pode primeiramente ser usado para um escritório de casa ou um escritório pequeno que não exija muito o forte segurança.

A implementação WEP de Aironet está no hardware. Consequentemente, o impacto de desempenho mínimo resulta quando você usa o WEP.

Nota: Há alguns problemas conhecidos com WEP, que lhe faz não um método de criptografia forte. As edições são:

- Há muita carga adicional administrativa para manter uma chave de WEP compartilhada.
- O WEP tem o mesmo problema que todos os sistemas baseados em chaves compartilhadas. Todo o segredo dado a uma pessoa torna-se público após um período de tempo.
- O IV que semeia o algoritmo de WEP é enviado no texto claro.
- A soma de verificação WEP é Linear e predizível.

O Temporal Key Integrity Protocol (TKIP) foi criado para endereçar estas edições WEP. Similar ao WEP, o TKIP usa a criptografia RC4. Contudo, o TKIP aumenta o WEP adicionando medidas tais como o pacote per. hashing-chave, a rotação chave do Message Integrity Check (MIC), e da transmissão endereçar vulnerabilidades conhecidas do WEP. O TKIP usa a cifra de córrego RC4 com chaves do 128-bit para a criptografia e chaves 64-bit para a autenticação.

Pré-requisitos

Requisitos

Este documento supõe que você pode fazer uma conexão administrativa aos dispositivos de WLAN e que os dispositivos funcionam normalmente em um ambiente não criptografado.

A fim configurar o padrão 40-bit WEP, você deve ter dois ou mais unidades de rádio que se comunicam um com o otro.

Nota: Os produtos Aironet podem estabelecer as conexões WEP 40-bit com Produtos não-Cisco da IEEE 802.11b-compliant. Este documento não endereça a configuração dos outros dispositivos.

Para a criação de um link do 128-bit WEP, o Produtos da Cisco interage somente com outros produtos Cisco.

Componentes Utilizados

Use estes componentes com este documento:

- Dois ou mais unidades de rádio que se comunicam um com o otro
- Uma conexão administrativa ao dispositivo de WLAN

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

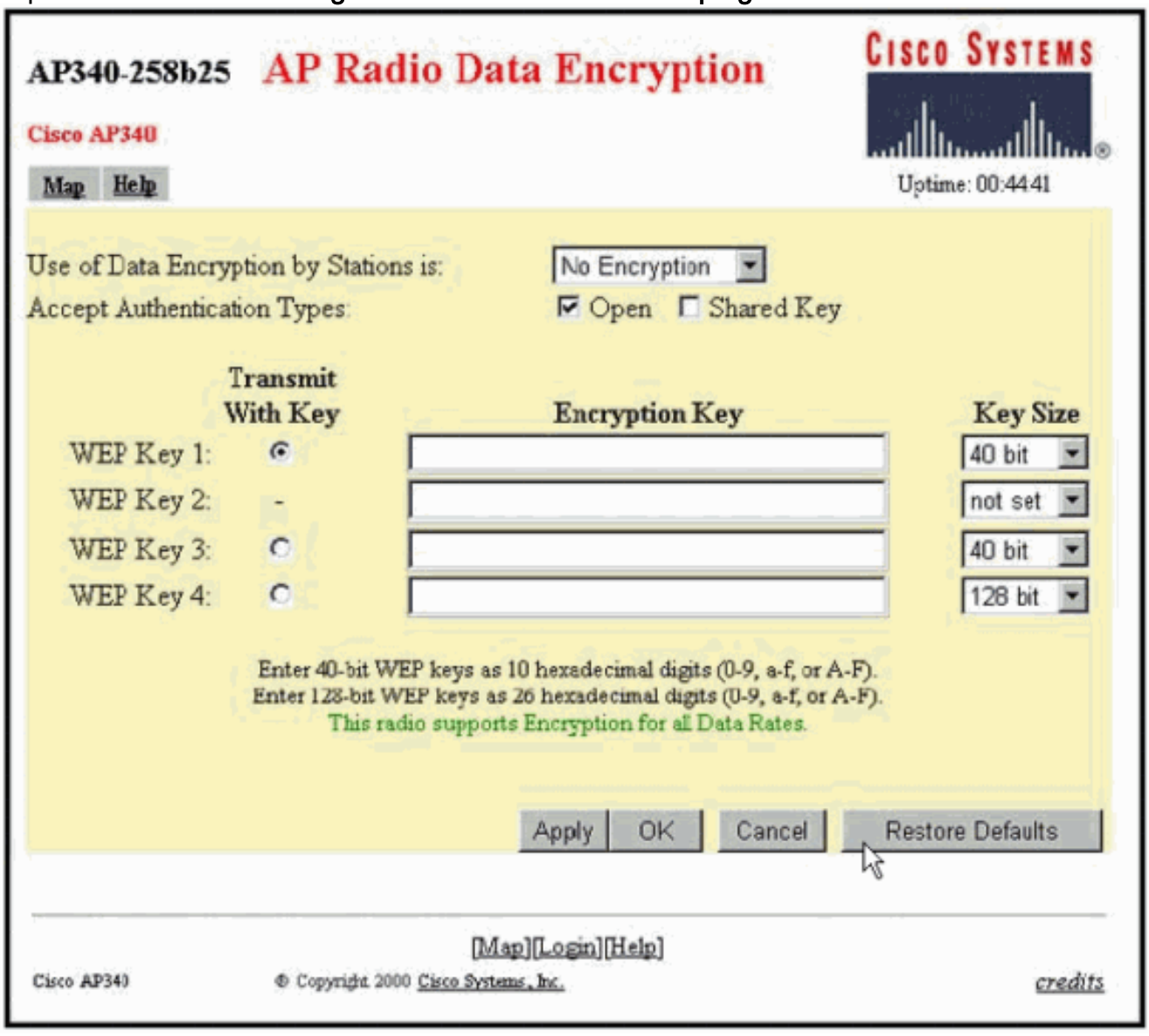
Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Configurar o WEP em pontos de acesso Aironet

Pontos de acesso Aironet que executam o sistema operacional vxworks

Conclua estes passos:

1. Faça uma conexão ao Access Point (AP).
2. Navegue ao menu de criptografia de rádio AP.Use um destes trajetos:**Criptografia de dados do > Rádio do Status de Sumário > Instalação > do rádio AP/hardware (WEP) > criptografia de dados do rádio AP> instalação de segurança do > segurança do Status de Sumário > Instalação: Radio Data Encryption (WEP) > criptografia de dados do rádio APNota:** A fim fazer mudanças a esta página, você deve ser um administrador com identidade e escrever capacidades.**Ideia do navegador da Web do menu de criptografia de dados do rádio AP**



Ajustes de VxWorks

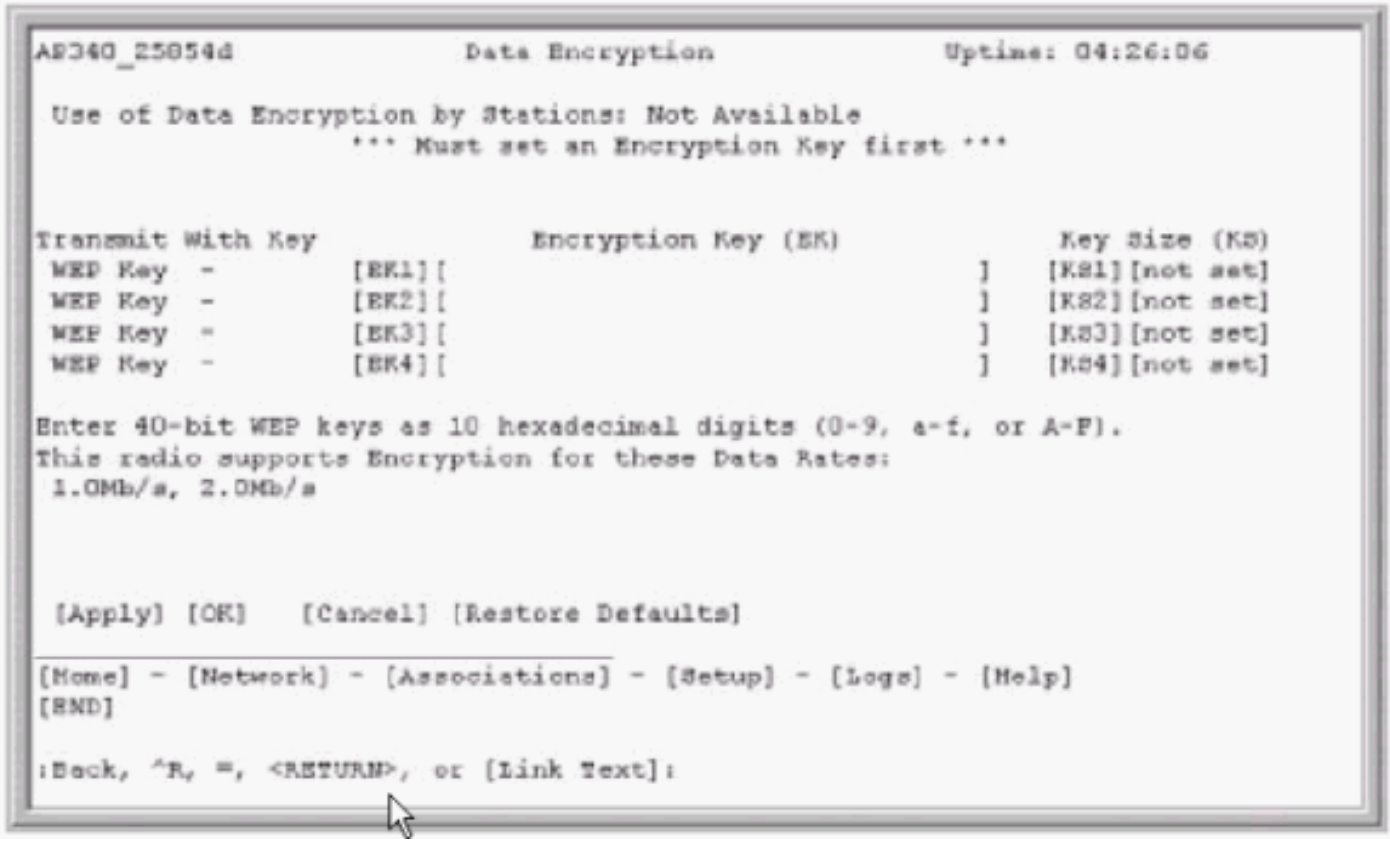
A página da criptografia de dados do rádio AP apresenta uma variedade de opções para usar-se.

Algumas opções são imperativas para o WEP. Esta seção nota estas opções imperativas. As outras opções não são necessárias para que o WEP funcione, mas são recomendadas.

- **O uso da criptografia de dados pelas estações é:**Use este ajuste a fim escolher se os clientes devem usar a criptografia de dados quando se comunicam com o AP. O menu de destruição alista três opções:**No encryption (padrão)** — Requer cliente a comunicar-se com o AP sem alguma criptografia de dados. Este ajuste não é recomendado.**Opcional** — Permite cliente a comunicar-se com o AP um ou outro com ou sem a criptografia de dados. Tipicamente, você usa esta opção quando você tem os dispositivos do cliente que não podem fazer uma conexão WEP, tal como clientes não-Cisco em um ambiente do 128-bit WEP.**Criptografia total (RECOMENDADA)** — Requer cliente para usar a criptografia de dados quando se comunicarem com o AP. Não são permitidos aos clientes que não usam a criptografia de dados comunicar-se. Esta opção é recomendada se você deseja maximizar a Segurança de seu WLAN.**Nota:** Você deve ajustar uma chave de WEP antes que você uso do Enable Encryption. Veja a seção da **chave de criptografia (MANDATORY) d**esta lista.
- **Aceitar Tipos de Autenticação**Você pode escolher aberto, a chave compartilhada, ou as both of these opções a fim ajustar as autenticações que o AP reconhecerá.**Abrir (RECOMENDADO)** — Esta configuração padrão permite que todo o dispositivo, apesar de suas chaves de WEP, autentique e tente associar.**Chave compartilhada** — Este ajuste diz o AP para enviar um texto simples, consulta de chave compartilhada a todo o dispositivo que tentar associar com o AP.**Nota:** Esta pergunta pode sair do AP aberto a um ataque de texto conhecido dos intrusos. Consequentemente, este ajuste não é tão seguro quanto a configuração em aberto.
- **Transmita com chave**Estes botões permitem que você selecione a chave que o AP usa durante a transmissão de dados. Você pode selecionar somente uma chave de cada vez. Alguns ou todas as chaves do grupo podem ser usados para receber dados. Você deve ajustar a chave antes que você a especifique como a chave transmissora.
- **Chave de Criptografia (MANDATORY)**Estes campos permitem que você incorpore as chaves de WEP. Incorpore os dígitos hexadecimais 10 para as chaves de WEP 40-bit ou os 26 dígitos hexadecimais para chaves de WEP do 128-bit. As chaves podem ser toda a combinação destes dígitos:0 a 9àfàFA fim proteger a Segurança da chave de WEP, as chaves de WEP existentes não aparecem no texto simples nos campos de entrada. Nas versões recentes dos AP, você pode suprimir de chaves existentes. Contudo, você não pode editar as chaves existentes.**Nota:** Você deve estabelecer as chaves de WEP para seus rede, AP, e dispositivos do cliente exatamente da mesma forma. Por exemplo, se você ajusta a chave de WEP 3 em seu AP a 0987654321 e seleciona esta chave como a chave ativa, você deve igualmente ajustar a chave de WEP 3 no dispositivo do cliente ao mesmo valor.
- **Tamanho chave (MANDATORY)**Este ajuste ajusta as chaves à 40-bit ou ao 128-bit WEP. Se o " não definido " aparece para esta seleção, a chave não está ajustada.**Nota:** Você não pode suprimir de uma chave selecionando o " não definido ".
- **Botões de ação**Quatro ajustes do controle dos botões de ação. Se o Javascript é permitido em seu navegador da Web, um indicador do pop-up de confirmação aparece depois que você clica todo o botão, exceto o cancelamento.**Aplique** — Este botão ativa as configurações de valor novas. O navegador permanece na página.**APROVAÇÃO** — Este botão aplica os ajustes novos e move o navegador de volta à página de instalação principal.**Cancelamento** — Este botão cancela mudanças do ajuste e retorna os ajustes previamente aos valores armazenados. Você retorna então à página de instalação principal.**Padrões da restauração** — Este botão muda todos os ajustes nesta página de volta às instalações padrão de fábrica.

Nota: Em versões recentes de Cisco IOS® dos AP, do controle somente os botões da **aplicação** e do **cancelamento** estão disponíveis para esta página.

Vista de simulador terminal do menu de criptografia de dados



Vista de simulador terminal da sequência de configuração da chave de WEP (software de Cisco IOS®)

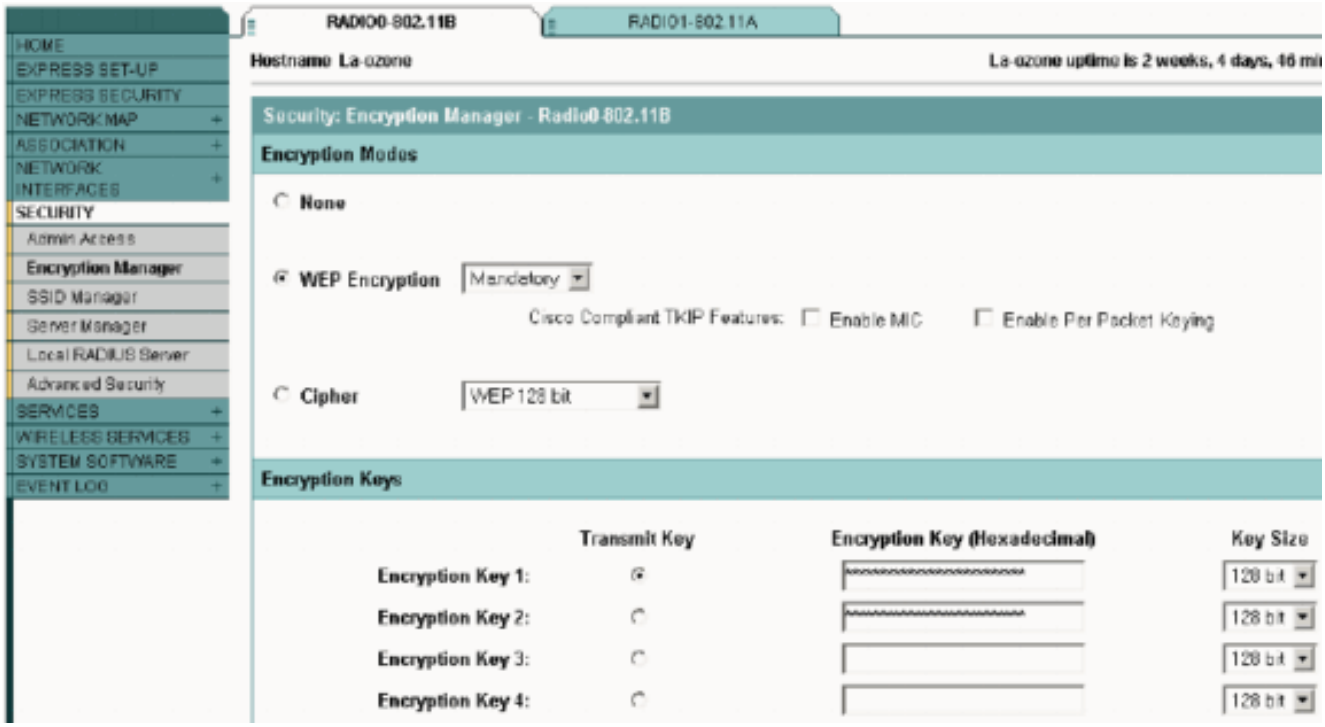
```
La-ozone>
La-ozone>
La-ozone>enable
Password:
La-ozone#
La-ozone#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
La-ozone(config)#interface dot
La-ozone(config)#interface dot11Radio 0
La-ozone(config-if)#encryption key 1 size 128bit 11c0ffeec0ffeec0ffeec0ffee ?
 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

Conclua estes passos:

1. Faça uma conexão ao AP.
2. Da opção do menu Segurança no lado esquerdo do indicador, escolha o **gerenciador de criptografia** para a interface de rádio a que você quer configurar suas chaves de WEP estático.**Opinião do navegador da Web do Menu AP Security Encryption Manager**



Configurar Aironet Bridge

Se você usa VxWorks, termine estas etapas:

1. Faça uma conexão à ponte.
2. Navegue ao menu de privacidade.Escolha o **> Rádio do menu principal > da configuração > o > Privacidade I80211**.Os controles de menu de privacidade o uso da criptografia no pacote de dados que é transmitido sobre o ar pelos rádios. O algoritmo RSA RC4 e essa de até quatro chaves conhecidas são usados para cifrar os pacotes. Cada nó na célula de rádio deve conhecer todas as chaves no uso, mas das chaves pode ser selecionado para transmitir os dados.**Vista de simulador terminal do menu de privacidade**

```
        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
>_
```

Refira configurar séries da cifra e WEP - ponte do 1300 Series e configurar características WEP e WEP - ponte do 1400 Series para obter informações sobre de como configurar o WEP em 1300 e as pontes do 1400 Series com o modo de CLI.

A fim usar o GUI para configurar as pontes do 1300 e 1400 Series, termine o mesmo procedimento explicado em Aironet AP que executam a seção do Cisco IOS Software deste documento.

Ajustes de VxWorks

O menu de privacidade apresenta um conjunto de opções que você deva configurar. Algumas opções são imperativas para o WEP. Esta seção nota estas opções imperativas. As outras opções não são necessárias para que o WEP funcione, mas são recomendadas.

Esta seção apresenta as opções de menu na ordem que aparecem na vista de simulador terminal do menu de privacidade. Contudo, configurar as opções nesta ordem:

1. Chave
2. Transmit
3. Auth
4. Cliente
5. Criptografia

A configuração nesta ordem assegura-se de que as condições prévias necessárias lhe estejam estabelecidas configurem cada ajuste.

Estas são as opções:

- **Key (MANDATORY)**A opção da chave programa as chaves de criptografia na ponte. Você é alertado ajustar uma das quatro chaves. Você é alertado duas vezes incorporar a chave. A fim definir a chave, você deve incorporar o 10 ou os 26 dígitos hexadecimais, que depende sobre se a configuração de bridges é para chaves 40-bit ou de 128-bit. Use toda a combinação destes dígitos:0 a 9àfàFAs chaves devem combinar em ***todos os*** Nós na célula de rádio, e você deve incorporar as chaves à mesma ordem. Você não precisa de definir todas as quatro chaves, enquanto o número de chaves combina em cada dispositivo no WLAN.
- TransmitA opção transmitir diz ao rádio que chaves a se usar a fim transmitir pacotes. Cada rádio pode decifrar os pacotes recebidos que são enviados com as algumas das quatro chaves.
- AuthVocê usa a opção Auth em bridges de repetidor a fim determinar que modo de autenticação a unidade se usa para conectar com seu pai. Os valores permitidos são abertos ou chave compartilhada. O protocolo do 802.11 especifica um procedimento em que um cliente deve autenticar com um pai antes que o cliente possa associar.**Abrir (RECOMENDADO)** — Este modo de autenticação é essencialmente uma operação nula. São permitidos a todos os clientes autenticar.**Chave compartilhada** — Este modo permite que o pai envie ao cliente um texto de desafio, que o cliente cifre e retorne ao pai. Se o pai decifra com sucesso o texto de desafio, o cliente está autenticado.**Cuidado:** Não use o modo da chave compartilhada. Quando você o usa, um texto simples e uma versão cifrada dos mesmos dados transmitem no ar. Isto não ganha qualquer coisa. Se a chave do usuário é errada, a unidade não decifra os pacotes, e os pacotes não podem aceder à rede.
- **Cliente**A opção de cliente determina o modo de autenticação que os nós de cliente se usam para associar à unidade. Estes são os valores que são permitidos:**Abrir (RECOMENDADO)** — Este modo de autenticação é essencialmente uma operação nula. São permitidos a todos os clientes autenticar.**Chave compartilhada** — Este modo permite que o pai envie ao cliente um texto de desafio, que o cliente cifre e retorne ao pai. Se o pai decifra com sucesso o texto de desafio, o cliente está autenticado.**Ambos** — Este modo permite que o cliente use um ou outro modo.
- Criptografia**Fora de** — Se você ajusta a opção de criptografia a fora, o no encryption está feito. Os dados transmitem na claro.**Em (MANDATORY)** — Se você ajusta a opção de criptografia a sobre, todos os pacotes de dados transmitidos estão cifrados e todos os

pacotes recebidos unencrypted são rejeitados.**Misturado** — No modo misturado, uma raiz ou um bridge de repetidor aceitam a associação dos clientes que têm a criptografia girada qualquer um de ligar/desligar. Neste caso, somente os pacotes de dados entre Nós que ambos apoiam são cifrados. Os pacotes de transmissão múltipla são enviados na claro. Todos os Nós podem considerar os pacotes.**Cuidado:** Não use o modo misturado. Se um cliente que tenha a criptografia permitida envia um pacote de transmissão múltipla a seu pai, o pacote está cifrado. O pai decifra o pacote e retransmite o pacote na claro à pilha, e outros Nós podem considerar o pacote. A capacidade para ver um pacote nos ambos formulário criptografado e não criptografado pode contribuir a quebrar uma chave. A inclusão de modo variado é somente para a compatibilidade com outros fornecedores.

Configurar adaptadores cliente

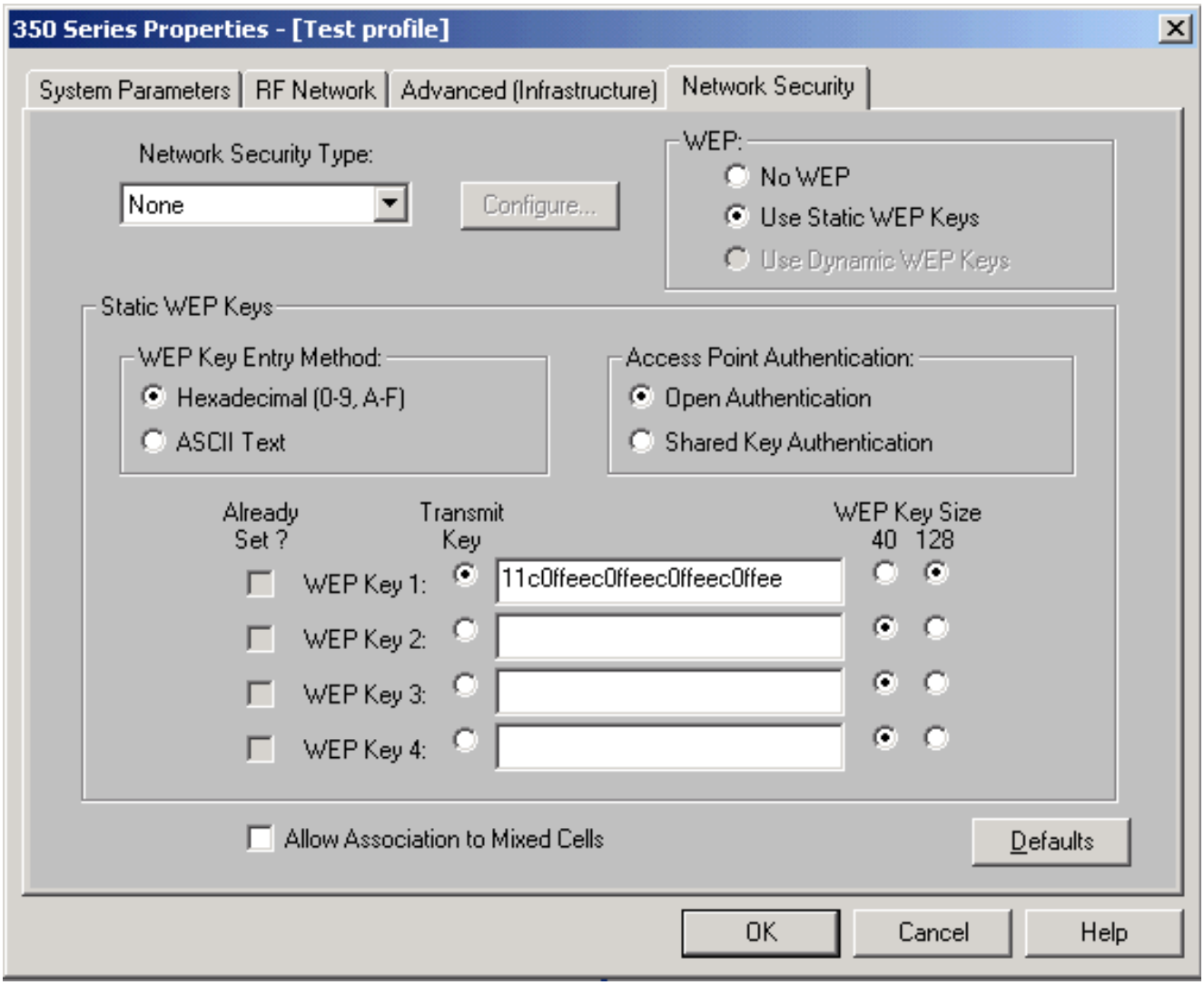
Você deve terminar duas etapas principais a fim estabelecer o WEP no adaptador de cliente Aironet:

1. Configurar a chave de WEP/chaves no gerenciador de criptografia de cliente.
2. Permita o WEP no Aironet Client Utility (ACU).

Ajuste as chaves de WEP

Termine estas etapas a fim estabelecer chaves de WEP nos adaptadores cliente:

1. Abra o ACU e escolha o **gerente do perfil**.
2. Escolha o perfil onde você quer permitir o WEP e o clique **edita**.
3. Clique a **ABA de segurança de rede** a fim indicar as opções de segurança, e clique **chaves de WEP estático do uso**.Esta ação ativa as opções de configuração WEP que são escurecidas quando nenhum WEP é
selecionado.



4. Para a chave de WEP que você quer criar, escolha **40** bit bit ou **128** sob o tamanho da chave de WEP no lado direito do indicador.**Nota:** os adaptadores cliente do 128-bit podem usar chaves 40-bit ou de 128-bit. Mas os adaptadores 40-bit podem somente usar as chaves 40-bit.**Nota:** Sua chave de WEP do adaptador cliente deve combinar a chave de WEP que os outros componentes de WLAN com que você comunica o uso.Quando você ajusta mais de uma chave de WEP, você deve atribuir as chaves de WEP aos mesmos números da chave de WEP para todos os dispositivos. As chaves de WEP devem ser compreendidas dos caracteres hexadecimais e devem conter os caráteres 10 para as chaves de WEP 40-bit ou os 26 caráteres para chaves de WEP do 128-bit. Os caracteres hexadecimais podem ser:0 a 9àfàF**Nota:** As chaves de WEP do texto de ASCII não são apoiadas em Aironet AP. Consequentemente, você deve escolher (0-9, A-F) a opção hexadecimal se você planeia usar seu adaptador cliente com estes AP.**Nota:** Depois que você cria a chave de WEP, você pode escrever sobre ela. Mas você não pode editá-la ou suprimir d.**Nota:** Se você usa uma versão mais atrasada do utilitário de Desktop de Aironet (ADU) em vez do ACU como um utilitário de cliente, você pode igualmente suprimir da chave de WEP criada e substitui-la com um novo.
5. Clique o botão da **chave transmissora** que é ao lado de uma das chaves que você criou.Com esta ação, você indica que esta chave é a chave que você quer usar para transmitir pacotes.
6. Tipo inferior **persistente da** chave de WEP do clique.Esta ação permite que seu adaptador cliente retenha esta chave de WEP, mesmo quando a potência ao adaptador é removida ou na repartição do computador em que a chave está instalada. Se você escolhe provisório para esta opção, a chave de WEP está perdida quando a potência é removida de seu

adaptador cliente.
7. Clique em **OK**.

Permita o WEP

Conclua estes passos:

1. Abra o ACU e escolha-o **Edit Properties da** barra de menus.
2. Clique a **ABA de segurança de rede** a fim indicar as opções de segurança.
3. Verifique a **caixa de verificação de WEP da possibilidade** a fim ativar o WEP.

Refira configurar o WEP no ADU para que as etapas configurem o WEP usando o ADU como o utilitário de cliente.

Configurar bridges de grupo de trabalho

Há umas diferenças entre o bridge de grupo de trabalho do 340 Series de Aironet e a ponte do 340 Series de Aironet. Contudo, a configuração do bridge de grupo de trabalho para usar o WEP é quase idêntica à configuração da ponte. Veja a seção dos Aironet Bridge configurar para a configuração da ponte.

1. Conecte ao bridge de grupo de trabalho.
2. Navegue ao menu de privacidade.Escolha **Main > Configuration > Radio > o > Privacidade I80211** a fim alcançar o menu de VxWorks da privacidade.

Configurações

O menu de privacidade apresenta aos ajustes lista dessa esta seção. Configurar as opções no bridge de grupo de trabalho nesta ordem:

1. Chave
2. Transmit
3. Auth
4. Criptografia

Estas são as opções:

- **Chave**A opção chave estabelece a chave de WEP que os usos da ponte a fim receber pacotes. O valor deve combinar a chave que o AP ou o outro dispositivo com que o bridge de grupo de trabalho comunica usos. A chave consiste até os caracteres hexadecimais 10 para a criptografia 40-bit ou os 26 caracteres hexadecimais para a criptografia do 128-bit. Os caracteres hexadecimais podem ser toda a combinação destes dígitos:0 a 9àfàF
- TransmitA opção transmitir estabelece a chave de WEP que os usos da ponte a fim transmitir pacotes. Você pode eleger para usar a mesma chave que você usou para a opção chave. Se você escolhe uma chave diferente, você deve estabelecer uma chave de harmonização no AP.Somente uma chave de WEP pode ser usada ao mesmo tempo para transmissões. A chave de WEP que você se usa para transmitir dados deve ser ajustada ao mesmo valor em seus bridge de grupo de trabalho e outros dispositivos com que se comunica.
- **Autenticação (AUTH)**O Parâmetro de autenticação determina que método de autenticação o sistema usa. As opções são:**Abrir (RECOMENDADO)** — A configuração em aberto do padrão

permite que todo o AP, apesar de suas configurações de WEP, autentique e tente então comunicar-se com a ponte.**Chave compartilhada** — Este ajuste instrui a ponte para enviar um texto simples, consulta de chave compartilhada aos AP na tentativa de comunicar-se com a ponte. A configuração chave compartilhada pode sair da ponte aberta a um ataque de texto conhecido dos intrusos. Consequentemente, este ajuste não é tão seguro quanto a configuração em aberto.

- CriptografiaA opção de criptografia ajusta parâmetros de criptografia em todos os pacotes de dados, exceto pacotes de associação e alguns pacotes de controle. Há quatro opções:**Nota:** O AP deve ter a criptografia ativa e um key set corretamente.**Fora de** — Esta é a configuração padrão. Toda a criptografia é desligada. O bridge de grupo de trabalho não se comunica com um AP com uso do WEP.**Em (RECOMENDADO)** — Este ajuste exige a criptografia de todas as transferências de dados. O bridge de grupo de trabalho comunica-se somente com os AP que usam o WEP.**Misturado sobre** — Este ajuste significa que a ponte usa sempre o WEP a fim se comunicar com o AP. Contudo, o AP comunica-se com todos os dispositivos, se usam o WEP ou não usam o WEP.**Misturado fora** — Este ajuste significa que a ponte não usa o WEP a fim se comunicar com o AP. Contudo, o AP comunica-se com todos os dispositivos, se usam o WEP ou não usam o WEP.**Cuidado:** Se você seleciona sobre ou misturado sobre enquanto a categoria WEP e você configuram a ponte através de seu link de rádio, a Conectividade à ponte está perdida se você ajusta a chave de WEP incorretamente. Certifique-se de que você usa exatamente os mesmos ajustes quando você ajustar a chave de WEP no bridge de grupo de trabalho e a chave de WEP em outros dispositivos em seu WLAN.

Informações Relacionadas

- Associação dos padrões de IEEE
- Produtos Aironet 340 Series Wireless LAN
- Wireless Support Resources
- Página de Suporte de Wireless LAN
- Cisco IOS Software Configuration Guide for Cisco Aironet Access Points (Guia de Configuração do Software Cisco IOS para Pontos de Acesso do Cisco Aironet)
- Manual de configuração do Cisco IOS Software para a bridge/ponte de acesso exterior do Cisco Aironet série 1300
- Guia de Configuração do Software Cisco Aironet Access Point para VxWorks
- Manual de configuração do software de Bridge do Cisco Aironet série 1400
- Manuais de configuração do Adaptadores de clientes LAN sem fio Cisco Aironet
- Vista geral da Segurança de LAN do Cisco Wireless
- Sem fio (mobilidade) que fixa redes Wireless
- Access point como um exemplo de configuração do bridge de grupo de trabalho
- Bridge de grupo de trabalho FAQ do Cisco Aironet
- Procedimento de recuperação de senha para equipamento Cisco Aironet
- Perguntas freqüentes sobre o ponto de acesso Cisco Aironet
- Suporte Técnico e Documentação - Cisco Systems