Configurar WEP em pontos de acesso e bridges Aironet

Contents

Introduction

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

Observação: consulte a seção Static Web Keys do Capítulo 6 - Configuring WLANs para obter mais informações sobre a configuração de WEP em controladores de LAN sem fio (WLCs).

WEP é o algoritmo de criptografia integrado ao padrão 802.11 (Wi-Fi). A criptografia WEP usa a codificação de fluxo RC4 (Code 4) do Ron com chaves de 40 ou 104 bits e um vetor de inicialização (IV) de 24 bits.

Como o padrão especifica, o WEP usa o algoritmo RC4 com uma chave de 40 ou 104 bits e um IV de 24 bits. RC4 é um algoritmo simétrico porque usa a mesma chave para a criptografia e a descriptografia de 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 está embaralhado com a chave apropriada, o pacote é descartado e nunca é entregue ao host.

A WEP pode ser usada principalmente para um escritório doméstico ou um pequeno escritório

que não exige uma segurança muito forte.

A implementação do Aironet WEP está no hardware. Portanto, o impacto mínimo no desempenho é obtido quando você usa WEP.

Observação: há alguns problemas conhecidos com a WEP, o que a torna um método de criptografia não forte. Os problemas são:

- Há muita sobrecarga administrativa para manter uma chave WEP compartilhada.
- A WEP tem o mesmo problema de todos os sistemas baseados em chaves compartilhadas. Qualquer segredo dado a uma pessoa torna-se público após um período de tempo.
- O IV que semeia o algoritmo WEP é enviado em texto claro.
- A soma de verificação WEP é linear e previsível.

O Temporal Key Integrity Protocol (TKIP) foi criado para resolver esses problemas de WEP. Semelhante à WEP, o TKIP usa criptografia RC4. No entanto, o TKIP melhora a WEP adicionando medidas como o hashing de chave por pacote, o Message Integrity Check (MIC) e a rotação de chave de broadcast para tratar das vulnerabilidades conhecidas da WEP. O TKIP usa cifra de fluxo RC4 com chaves de 128 bits para criptografia e chaves de 64 bits para autenticação.

Prerequisites

Requirements

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

Para configurar o WEP padrão de 40 bits, você deve ter duas ou mais unidades de rádio que se comunicam entre si.

Observação: os produtos Aironet podem estabelecer conexões WEP de 40 bits com produtos não compatíveis com IEEE 802.11b da Cisco. Este documento não aborda a configuração de outros dispositivos.

Para a criação de um link WEP de 128 bits, os produtos da Cisco interagem apenas com outros produtos da Cisco.

Componentes Utilizados

Use estes componentes com este documento:

- Duas ou mais unidades de rádio que se comunicam entre si
- Uma conexão administrativa com o dispositivo WLAN

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

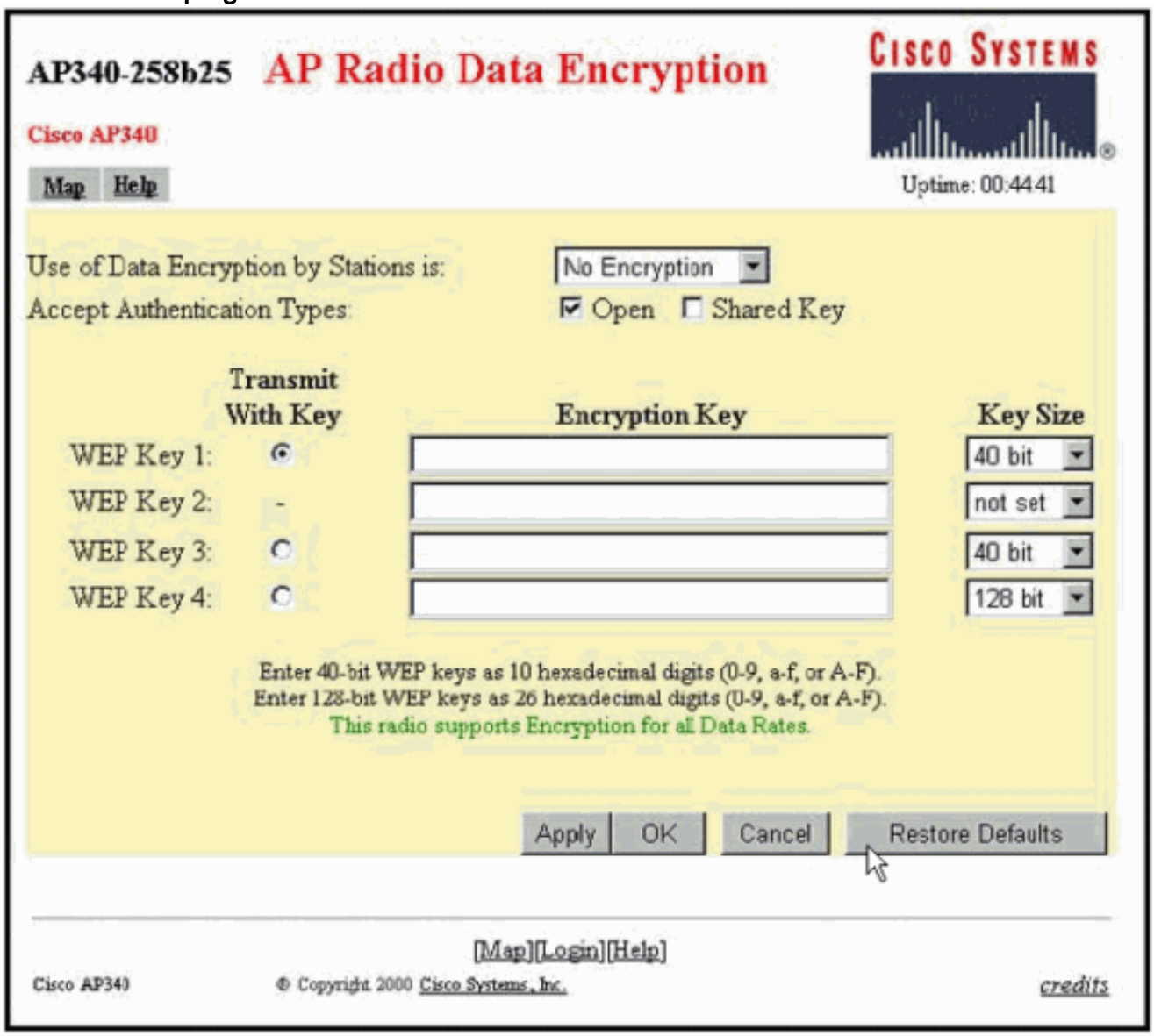
Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Configurar WEP em access points Aironet

Access Points Aironet Que Executam O Sistema Operacional VxWorks

Conclua estes passos:

1. Faça uma conexão com o ponto de acesso (AP).
2. Navegue até o menu Criptografia de rádio AP.Use um destes caminhos:**Status do resumo > Configuração > Hardware/Rádio do AP > Criptografia de Dados de Rádio (WEP) > Criptografia de Dados de Rádio do APStatus do resumo > Configuração > Segurança > Configuração de segurança: Criptografia de dados de rádio (WEP) > Criptografia de dados de rádio APObservação:** para fazer alterações nesta página, você deve ser um administrador com recursos de Identidade e Gravação.**Visualização do navegador da Web do menu de criptografia de dados do rádio AP**



Configurações do VxWorks

A página Criptografia de dados de rádio AP apresenta uma variedade de opções a serem usadas. Algumas opções são obrigatórias para a WEP. Esta seção observa essas opções obrigatórias. Outras opções não são necessárias para que a WEP funcione, mas são recomendadas.

- **O uso da criptografia de dados pelas estações é:**Use essa configuração para escolher se os clientes devem usar a criptografia de dados ao se comunicarem com o AP. O menu suspenso lista três opções:**No Encryption (Sem criptografia) (padrão)** — Requer que os clientes se comuniquem com o AP sem qualquer criptografia de dados. Esta configuração não é recomendada.**Opcional** —Permite que os clientes se comuniquem com o AP com ou sem criptografia de dados. Normalmente, você usa essa opção quando tem dispositivos de cliente que não podem fazer uma conexão WEP, como clientes não-Cisco em um ambiente WEP de 128 bits.**Full Encryption (RECOMENDADO)** — Exige que os clientes usem criptografia de dados quando se comunicam com o AP. Clientes que não usam criptografia de dados não têm permissão para se comunicar. Essa opção é recomendada se você quiser maximizar a segurança da sua WLAN.**Observação:** você deve definir uma chave WEP antes de habilitar o uso da criptografia. Consulte a seção **Chave de Criptografia (OBRIGATÓRIA)** desta lista.
- **Aceitar Tipos de Autenticação**Você pode escolher Open (Abrir), Shared Key (Chave compartilhada) ou ambas as opções para definir as autenticações que o AP reconhecerá.**Abrir (RECOMENDADO)** — Essa configuração padrão permite que qualquer dispositivo, independentemente de suas chaves WEP, autentique e tente se associar.**Chave compartilhada** — Essa configuração instrui o AP a enviar uma consulta de chave compartilhada de texto simples para qualquer dispositivo que tente se associar ao AP.**Observação:** essa consulta pode deixar o AP aberto a um ataque de texto conhecido de invasores. Portanto, essa configuração não é tão segura quanto a configuração Abrir.
- **Transmitir com chave**Esses botões permitem selecionar a chave que o AP usa durante a transmissão de dados. Você pode selecionar apenas uma chave por vez. Qualquer uma ou todas as chaves definidas podem ser usadas para receber dados. Você deve definir a chave antes de especificá-la como a Chave de transmissão.
- **Chave de Criptografia (MANDATORY)**Esses campos permitem inserir as chaves WEP. Insira 10 dígitos hexadecimais para as chaves WEP de 40 bits ou 26 dígitos hexadecimais para as chaves WEP de 128 bits. As teclas podem ser qualquer combinação destes dígitos:0 a 9a fA a FPara proteger a segurança da chave WEP, as chaves WEP existentes não aparecem em texto simples nos campos de entrada. Em versões recentes de APs, você pode excluir chaves existentes. No entanto, não é possível editar as chaves existentes.**Observação:** você deve configurar as chaves WEP para sua rede, APs e dispositivos de cliente exatamente da mesma forma. Por exemplo, se você definir a chave WEP 3 em seu AP como 0987654321 e selecionar essa chave como a chave ativa, também deverá definir a chave WEP 3 no dispositivo cliente com o mesmo valor.
- **Tamanho da chave (OBRIGATÓRIO)**Essa configuração define as teclas para WEP de 40 ou 128 bits. Se "não definido" aparecer para esta seleção, a chave não está definida.**Nota:** Não é possível eliminar uma chave selecionando "não definido".
- **Botões de ação**Quatro botões de ação controlam as configurações. Se o JavaScript estiver habilitado no navegador da Web, uma janela pop-up de confirmação será exibida depois que você clicar em qualquer botão, exceto Cancelar.**Aplicar** — Este botão ativa as novas configurações de valor. O navegador permanece na página.**OK** — Este botão aplica as novas configurações e move o navegador de volta para a página de configuração principal.**Cancelar** — Este botão cancela as alterações de configuração e retorna as configurações aos valores armazenados anteriormente. Em seguida, você retorna à página de configuração

principal.**Restore Defaults** —Este botão altera todas as configurações desta página de volta para as configurações padrão de fábrica.

Observação: nas versões recentes de APs do Cisco IOS®, somente os botões de controle **Aplicar** e **Cancelar** estão disponíveis para esta página.

Vista do emulador de terminal do menu Data Encryption

```
AP340_25054d              Data Encryption              Uptime: 04:26:06

 Use of Data Encryption by Stations: Not Available
                  *** Must set an Encryption Key first ***


Transmit With Key              Encryption Key (EK)              Key Size (KS)
 WEP Key  -         [EK1][                                ]    [KS1][not set]
 WEP Key  -         [EK2][                                ]    [KS2][not set]
 WEP Key  -         [EK3][                                ]    [KS3][not set]
 WEP Key  -         [EK4][                                ]    [KS4][not set]

Enter 40-bit WEP keys as 10 hexadecimal digits (0-9, a-f, or A-F).
This radio supports Encryption for these Data Rates:
 1.0Mb/s, 2.0Mb/s



 [Apply] [OK]    [Cancel] [Restore Defaults]
_____________________________________________
[Home] - [Network] - [Associations] - [Setup] - [Logs] - [Help]
[END]

:Back, ^R, =, <RETURN>, or [Link Text]:
```

Visão do Emulador de Terminal da Sequência de Configuração de Chave WEP (Software Cisco IOS®)

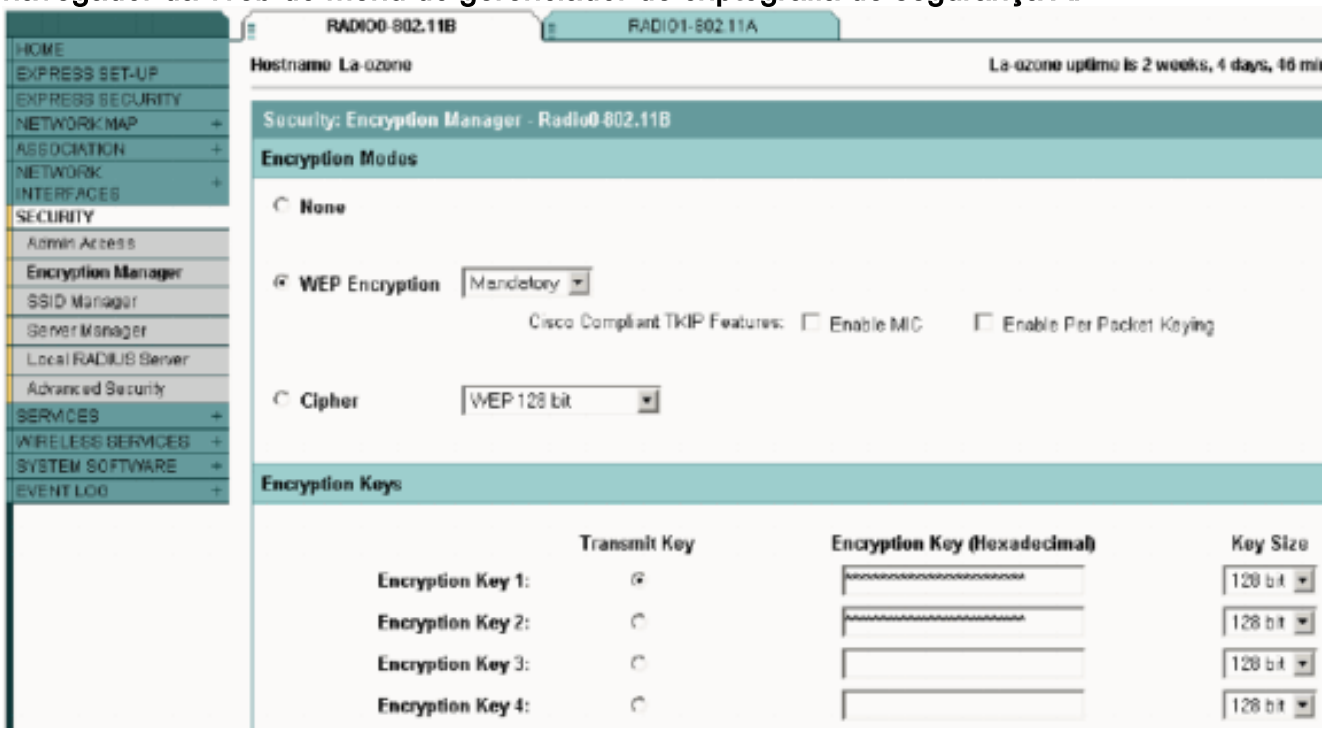
```
La-ozone>
La-ozone>
La-ozone>enable
Password:
La-ozone#
La-ozone#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
La-ozone(config)#interface dot
La-ozone(config)#interface dot11Radio 0
La-ozone(config-if)#encryption key 1 size 128bit 11c0ffeec0ffeec0ffeec0ffee ?
 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

APs Aironet que executam o software Cisco IOS

Conclua estes passos:

1. Faça uma conexão com o AP.
2. Na opção de menu SECURITY no lado esquerdo da janela, escolha **Encryption Manager** para a interface de rádio na qual deseja configurar suas chaves WEP estáticas.**Exibição do**

navegador da Web do menu do gerenciador de criptografia de segurança AP



Configurar as bridges Aironet

Se você usar o VxWorks, faça o seguinte:

1. Faça uma conexão com a ponte.
2. Navegue até o menu Privacidade.Escolha **Main Menu > Configuration > Radio > I80211 > Privacy**.O menu Privacidade controla o uso de criptografia no pacote de dados que é transmitido pelo ar pelos rádios. O algoritmo RSA RC4 e uma das quatro chaves conhecidas são usadas para criptografar os pacotes. Cada nó na célula de rádio deve saber todas as chaves em uso, mas qualquer uma das chaves pode ser selecionada para transmitir os dados.**Vista de simulador terminal do menu 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
>_
```

Consulte Configuração de Conjuntos de Cifras e WEP - 1300 Series Bridge e Configuração de Recursos WEP e WEP - 1400 Series Bridge para obter informações sobre como configurar WEP em 1300 e 1400 Series Bridges através do modo CLI.

Para usar a GUI para configurar as 1300 e 1400 Series Bridges, faça o mesmo procedimento explicado na seção APs Aironet que executam o software Cisco IOS deste documento.

Configurações do VxWorks

O menu Privacidade apresenta um conjunto de opções que você deve configurar. Algumas opções são obrigatórias para a WEP. Esta seção observa essas opções obrigatórias. Outras opções não são necessárias para que a WEP funcione, mas são recomendadas.

Esta seção apresenta as opções de menu na ordem em que aparecem na Visualização do Emulador de Terminal do menu Privacidade. No entanto, configure as opções nesta ordem:

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

A configuração nesta ordem garante que as pré-condições necessárias sejam configuradas à medida que você configura cada configuração.

Estas são as opções:

- **Key (MANDATORY)**A opção Key (Chave) programa as chaves de criptografia na Bridge. Você será solicitado a definir uma das quatro teclas. Você será solicitado duas vezes a inserir a chave. Para definir a chave, você deve digitar 10 ou 26 dígitos hexadecimais, o que depende da configuração da bridge para chaves de 40 bits ou 128 bits. Use qualquer combinação destes dígitos:0 a 9a fA a FAs chaves devem corresponder em ***todos os*** nós na célula de rádio e você deve digitar as chaves na mesma ordem. Você não precisa definir todas as quatro chaves, desde que o número de chaves corresponda em cada dispositivo na WLAN.
- **Transmitir**A opção Transmitir informa ao rádio quais chaves usar para transmitir pacotes. Cada rádio é capaz de descriptografar pacotes recebidos que são enviados com qualquer uma das quatro chaves.
- **Auth**Você usa a opção Auth em bridges repetidores para determinar qual modo de autenticação a unidade usa para se conectar com seu pai. Os valores permitidos são Open (Chave aberta) ou Shared Key (Chave compartilhada). O protocolo 802.11 especifica um procedimento no qual um cliente deve se autenticar com um pai antes que o cliente possa se associar.**Abrir (RECOMENDADO)** — Este modo de autenticação é essencialmente uma operação nula. Todos os clientes têm permissão para autenticar.**Chave compartilhada** — Este modo permite que o pai envie ao cliente um texto de desafio, que o cliente criptografa e retorna ao pai. Se o pai descriptografar com êxito o texto do desafio, o cliente será autenticado.**Cuidado:** não use o modo Chave compartilhada. Quando você o usa, uma versão em texto simples e criptografada dos mesmos dados transmite no ar. Isso não ganha nada. Se a chave do usuário estiver errada, a unidade não descriptografará os pacotes e os pacotes não poderão obter acesso à rede.
- **Cliente**A opção Cliente determina o modo de autenticação que os nós do cliente usam para associar à unidade. Estes são os valores permitidos:**Abrir (RECOMENDADO)** — Este modo de autenticação é essencialmente uma operação nula. Todos os clientes têm permissão para autenticar.**Chave compartilhada** — Este modo permite que o pai envie ao cliente um texto de desafio, que o cliente criptografa e retorna ao pai. Se o pai descriptografar com êxito o texto do desafio, o cliente será autenticado.**Ambos**—Este modo permite que o cliente use qualquer um dos modos.
- **CriptografiaOff** — Se você definir a opção Encryption (Criptografia) como Off (Desativado), nenhuma criptografia será feita. Os dados são transmitidos sem formatação.**On**

(OBRIGATÓRIO) — Se você definir a opção Encryption (Criptografia) como On (Ativada), todos os pacotes de dados transmitidos serão criptografados e todos os pacotes recebidos não criptografados serão descartados.**Mixed** — No modo Mixed, uma bridge raiz ou repetidora aceita associação de clientes que possuem criptografia ativada ou desativada. Nesse caso, somente os pacotes de dados entre os nós compatíveis são criptografados. Os pacotes multicast são enviados sem formatação. Todos os nós podem ver os pacotes.**Cuidado:** não use o modo Misto. Se um cliente com criptografia habilitada envia um pacote multicast para seu pai, o pacote é criptografado. O pai descriptografa o pacote e retransmite-o na célula, e outros nós podem ver o pacote. A capacidade de visualizar um pacote na forma criptografada e não criptografada pode contribuir para quebrar uma chave. A inclusão do modo Misto destina-se apenas à compatibilidade com outros fornecedores.

Configurar adaptadores clientes

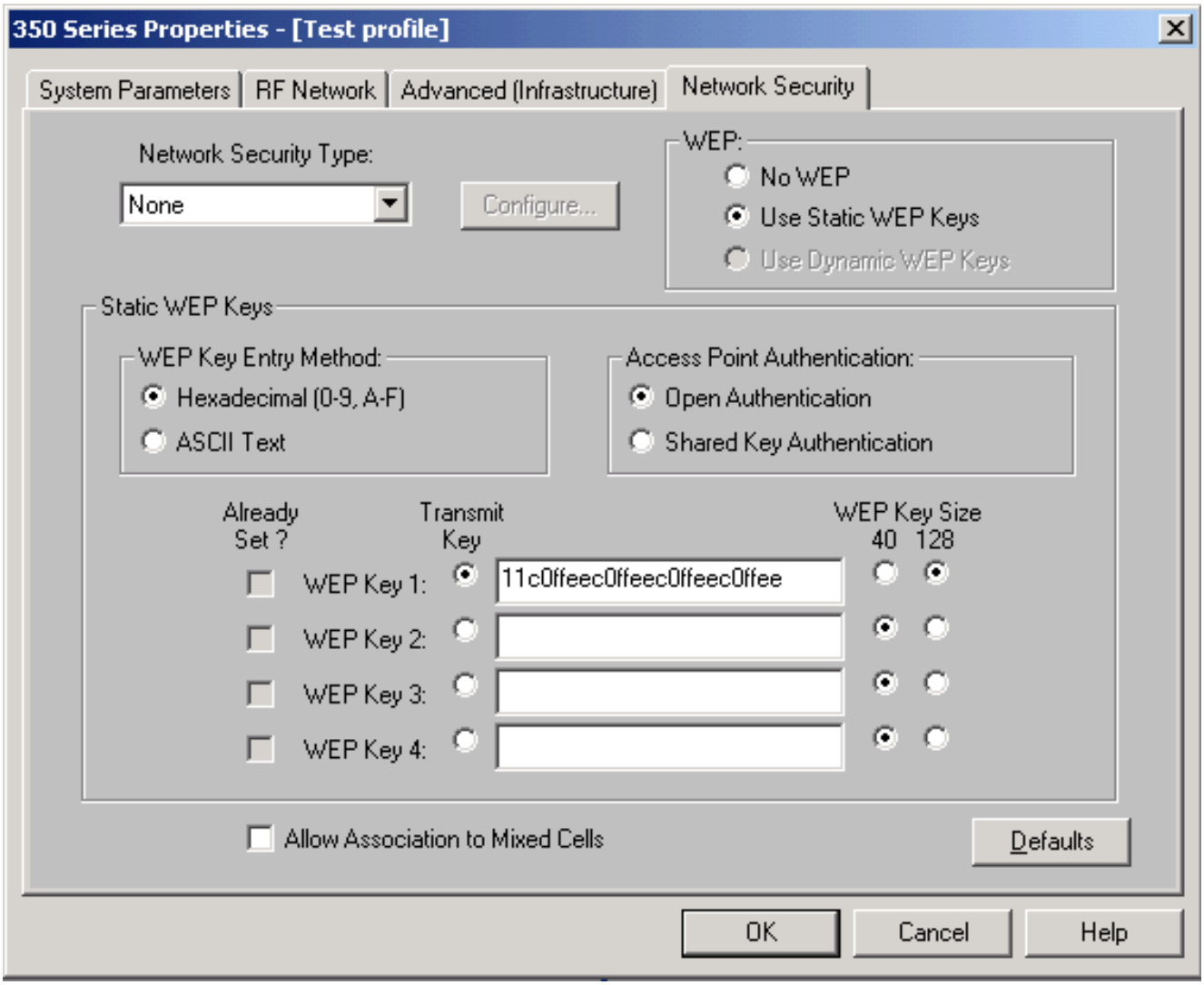
Você deve concluir duas etapas principais para configurar o WEP no adaptador cliente Aironet:

1. Configure as chaves WEP no Client Encryption Manager.
2. Ative o WEP no Aironet Client Utility (ACU).

Defina as chaves WEP

Conclua estes passos para configurar chaves WEP nos adaptadores clientes:

1. Abra a ACU e escolha **Profile Manager**.
2. Escolha o perfil onde deseja habilitar a WEP e clique em **Editar**.
3. Clique na guia **Network Security** para exibir as opções de segurança e clique em **Use Static WEP Keys**.Esta ação ativa as opções de configuração WEP que estão esmaecidas quando Nenhum WEP está
selecionado.



4. Para a chave WEP que você deseja criar, escolha **40** bits ou **128** bits em WEP Key Size (Tamanho da chave WEP) no lado direito da janela.**Nota:** os adaptadores clientes de 128 bits podem usar chaves de 40 ou 128 bits. Mas os adaptadores de 40 bits só podem usar chaves de 40 bits.**Nota:** A chave WEP do adaptador cliente deve corresponder à chave WEP usada pelos outros componentes WLAN com os quais você se comunica.Ao definir mais de uma chave WEP, você deve atribuir as chaves WEP aos mesmos números de chave WEP para todos os dispositivos. As chaves WEP devem ser compostas de caracteres hexadecimais e conter 10 caracteres para chaves WEP de 40 bits ou 26 caracteres para chaves WEP de 128 bits. Os caracteres hexadecimais podem ser:0 a 9a fA a F**Observação:** as chaves WEP de texto ASCII não são suportadas nos APs Aironet. Portanto, você deve escolher a opção Hexadecimal (0-9, A-F) se planeja usar seu adaptador cliente com esses APs.**Observação:** depois de criar a chave WEP, você pode gravá-la. Mas não é possível editá-la ou excluí-la.**Observação:** se você usar uma versão mais recente do Aironet Desktop Utility (ADU) em vez de ACU como um utilitário cliente, você também poderá excluir a chave WEP criada e substituí-la por uma nova.
5. Clique no botão **Transmit Key (Chave de transmissão)** que está ao lado de uma das chaves que você criou.Com essa ação, você indica que essa chave é a chave que deseja usar para transmitir pacotes.
6. Clique em **Persistente** em WEP Key Type (Tipo de chave WEP).Esta ação permite que o adaptador cliente mantenha esta chave WEP, mesmo quando a alimentação do adaptador for removida ou na reinicialização do computador no qual a chave está instalada. Se você escolher Temporário para esta opção, a chave WEP será perdida quando a energia for

removida do adaptador cliente.
7. Click **OK**.

Habilitar WEP

Conclua estes passos:

1. Abra a ACU e escolha **Editar propriedades** na barra de menus.
2. Clique na guia **Segurança de rede** para exibir as opções de segurança.
3. Marque a caixa de seleção **Habilitar WEP** para ativar o WEP.

Consulte Configuração de WEP em ADU para obter as etapas de configuração de WEP usando ADU como utilitário cliente.

Configurar pontes de grupo de trabalho

Há diferenças entre a Aironet 340 Series Workgroup Bridge e a Aironet 340 Series Bridge. No entanto, a configuração da ligação do grupo de trabalho para usar a WEP é quase idêntica à configuração da ponte. Consulte a seção Configure Aironet Bridges para obter informações sobre a configuração da Bridge.

1. Conecte-se à ligação do grupo de trabalho.
2. Navegue até o menu Privacidade.Escolha **Main > Configuration > Radio > I80211 > Privacy** para acessar o menu Privacy VxWorks.

Configurações

O menu Privacidade apresenta as configurações que esta seção lista. Configure as opções na ligação do grupo de trabalho nesta ordem:

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

Estas são as opções:

- **Chave**A opção Key estabelece a chave WEP que a bridge usa para receber pacotes. O valor deve corresponder à chave que o AP ou outro dispositivo com o qual a ligação de grupo de trabalho se comunica utiliza. A chave consiste em até 10 caracteres hexadecimais para criptografia de 40 bits ou 26 caracteres hexadecimais para criptografia de 128 bits. Os caracteres hexadecimais podem ser qualquer combinação destes dígitos:0 a 9a fA a F
- **Transmitir**A opção Transmitir estabelece a chave WEP que a bridge usa para transmitir pacotes. Você pode optar por usar a mesma chave que usou para a opção Key (Chave). Se você escolher uma chave diferente, deverá estabelecer uma chave correspondente no AP.Apenas uma chave WEP pode ser usada de uma vez para transmissões. A chave WEP que você usa para transmitir dados deve ser definida com o mesmo valor no Workgroup Bridge e em outros dispositivos com os quais se comunica.
- **Autenticação (Aut.)**O parâmetro Auth determina qual método de autenticação o sistema usa. As opções são:**Abrir (RECOMENDADO)** — A configuração padrão de Abertura permite que

qualquer AP, independentemente de suas configurações WEP, autentique e tente se comunicar com a bridge.**Chave compartilhada** — Essa configuração instrui a bridge a enviar uma consulta de chave compartilhada de texto simples aos APs na tentativa de se comunicar com a bridge. A configuração Chave compartilhada pode deixar a bridge aberta a um ataque de texto conhecido de invasores. Portanto, essa configuração não é tão segura quanto a configuração Abrir.

- **Criptografia**A opção Encryption define parâmetros de criptografia em todos os pacotes de dados, exceto pacotes de associação e alguns pacotes de controle. Há quatro opções:**Observação:** o AP deve ter criptografia ativa e uma chave definida corretamente.**Off** —Esta é a configuração padrão. Toda criptografia está desligada. A ligação de grupo de trabalho não se comunica com um AP com o uso de WEP.**On (RECOMENDADO)** — Essa configuração exige a criptografia de todas as transferências de dados. A ligação de grupo de trabalho se comunica somente com APs que usam WEP.**Mixed on** — Essa configuração significa que a bridge sempre usa WEP para se comunicar com o AP. No entanto, o AP se comunica com todos os dispositivos, quer eles usem WEP ou não a WEP.**Misto** — Essa configuração significa que a bridge não usa WEP para se comunicar com o AP. No entanto, o AP se comunica com todos os dispositivos, quer eles usem WEP ou não a WEP.**Cuidado:** se você selecionar On (Ativado) ou Mixed (Misto) como a categoria WEP e configurar a bridge por meio de seu link de rádio, a conectividade com a bridge será perdida se você definir a chave WEP incorretamente. Certifique-se de usar exatamente as mesmas configurações ao definir a chave WEP no Workgroup Bridge e a chave WEP em outros dispositivos na WLAN.

Informações Relacionadas

- Associação de Padrões IEEE
- Produtos LAN sem fio do Aironet 340 Series
- 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)
- Guia de configuração do software Cisco IOS para Access Point/Bridge externo Cisco Aironet 1300 Series
- Guia de Configuração do Software Cisco Aironet Access Point para VxWorks
- Guia de configuração do software Cisco Aironet 1400 Series Bridge
- Guias de configuração dos adaptadores de cliente LAN sem fio Cisco Aironet
- Visão geral do Cisco Wireless LAN Security
- Redes sem fio (mobilidade) protegendo redes sem fio
- Exemplo de Configuração de Ponto de Acesso como uma Bridge de Grupo de Trabalho
- Perguntas frequentes sobre a Cisco Aironet Workgroup Bridge
- Procedimento de recuperação de senha para equipamento Cisco Aironet
- Perguntas mais Frequentes sobre o access point Cisco Aironet
- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.