



AirCheck™

Testador de Wi-Fi

Manual do Usuário

01/2010, Rev. 4, 08/2013

©2010-2013 Fluke Corporation.

Todos os nomes de produtos são marcas comerciais de suas respectivas companhias.

GARANTIA LIMITADA E LIMITAÇÃO DE RESPONSABILIDADE

Todos os produtos da Fluke Networks são garantidos contra defeitos de material e mão-de-obra, sob condições de uso e serviço normal. O período de garantia da unidade-base (mainframe) é de 1 (um) ano a partir da data da compra. Peças, acessórios, reparos e serviços nos produtos têm garantia de 90 dias, salvo disposto em contrário. As baterias de Ni-Cad, Ni-MH e Li-Ion, cabos ou outros periféricos são todos considerados peças e acessórios. Esta garantia aplica-se apenas ao comprador original ou ao cliente usuário final de um revendedor autorizado da Fluke Networks, e não cobre qualquer produto que, na opinião da Fluke Networks, tenha sido usado de forma inadequada ou descuidada, ou tenha sido alterado, contaminado, ou danificado por acidente ou condições anormais de operação ou manuseio. A Fluke Networks garante que o software funcionará de acordo com as respectivas especificações técnicas pelo período de 90 dias, e que o mesmo foi gravado de forma adequada em meio físico sem defeitos. A Fluke Networks não garante que o software não apresentará erros nem que funcionará ininterruptamente.

Os revendedores Fluke Networks autorizados deverão conceder esta garantia somente para produtos novos e não-usados, mas não estão autorizados a ampliá-la ou modificá-la de nenhuma forma em nome da Fluke Networks. A assistência técnica coberta pela garantia está disponível apenas se o produto houver sido adquirido de uma loja autorizada da Fluke Networks, ou se o Comprador tiver pago o preço internacional aplicável. A Fluke Networks reserva-se o direito de cobrar do Comprador taxas relativas ao custo de importação das peças de reposição/reparos, quando o produto for comprado em um país e remetido a outro país para reparos.

A obrigação da Fluke Networks no que se refere a esta garantia é limitada, a critério da Fluke Networks, à devolução da importância paga pela compra do produto, ao conserto gratuito do produto, ou à reposição do produto que apresente defeito e que seja remetido a um centro de assistência técnica da Fluke Networks dentro do prazo de validade da garantia.

Para receber serviço de assistência técnica coberto pela garantia, entre em contato com o centro de assistência técnica autorizado da Fluke Networks mais próximo ou remeta o produto, com uma descrição do problema e com frete e seguro pagos (FOB no destino), ao centro de assistência técnica mais próximo. A Fluke Networks não se responsabiliza por nenhum dano que possa ocorrer durante o transporte. Após efetuado o conserto coberto pela garantia, o produto será remetido de volta ao Comprador, com frete pago (FOB no destino). Se a Fluke Networks determinar que o problema foi causado por uso inadequado ou descuidado, alteração, acidente ou condições anormais de operação ou manuseio, ou pelo desgaste normal dos componentes mecânicos, a Fluke Networks fará uma estimativa do custo do reparo e obterá a autorização do Comprador antes de efetuá-lo. Após a realização do conserto, o produto será remetido de volta ao Comprador com frete pago. O custo do conserto e da entrega do produto de volta ao Comprador será cobrado do mesmo (FOB no local da remessa).

ESTA GARANTIA É O ÚNICO E EXCLUSIVO RECURSO JURÍDICO DO COMPRADOR, E SUBSTITUI TODAS AS OUTRAS GARANTIAS, EXPRESSAS OU IMPLÍCITAS, INCLUINDO, MAS NÃO SE LIMITANDO A, QUALQUER GARANTIA IMPLÍCITA DE COMERCIALIZABILIDADE OU ADEQUAÇÃO PARA UM DETERMINADO FIM. A FLUKE NETWORKS NÃO SE RESPONSABILIZA POR NENHUM DANO OU PERDA ESPECIAL, INDIRETA, INCIDENTAL OU CONSEQUENTE, INCLUSIVE PERDA DE DADOS, QUE POSSA OCORRER EM DECORRÊNCIA DE QUALQUER CAUSA OU TEORIA JURÍDICA.

Como alguns estados ou países não permitem a exclusão ou limitação dos termos de garantias implícitas, nem de danos incidentais ou consequentes, esta limitação de responsabilidade poderá não se aplicar ao seu caso específico. Se alguma provisão desta garantia for considerada inválida ou inexecutável por algum tribunal ou outro órgão de jurisdição competente, tal decisão judicial não afetará a validade ou executabilidade de nenhuma outra provisão.

4/04

Fluke Networks
PO Box 777
Everett, WA 98206-0777
EUA

Índice

| Título | Página |
|---|---------------|
| Introdução | 1 |
| Registro do produto | 1 |
| Fluke Networks Knowledge Base | 1 |
| Para contatar a Fluke Networks | 2 |
| Informações de segurança | 2 |
| Desembalagem do produto | 4 |
| AirCheck – Testador de Wi-Fi | 4 |
| Kit do AirCheck para identificação e solução de problemas de primeira linha | 4 |
| Características físicas | 5 |
| Carregamento e duração da bateria | 7 |
| Utilize o aplicativo para PC do AirCheck Manager para um melhor desempenho | 8 |
| Informações que você pode obter sobre a sua rede | 9 |
| O que é o estado da minha rede? | 9 |
| O que há na LAN sem fio? | 12 |
| Dispositivos podem se conectar à minha rede? | 14 |
| Qual é a causa de um desempenho lento da rede e das quedas de conexão? | 15 |
| Existe algum risco de segurança na rede? | 16 |
| Como posso documentar minha rede e minha sessão de teste? | 18 |
| Como faço para apagar tudo no meu AirCheck? | 18 |

| | |
|---|----|
| Onde se localiza um ponto de acesso? | 18 |
| Que redes ou pontos de acesso entram na faixa de alcance conforme me movimento? | 18 |
| A tela inicial | 19 |
| Utilizar o AutoTest para diagnosticar o estado da rede | 21 |
| Qualidade do ar | 21 |
| Utilização de canal 802.11 | 21 |
| Utilização de canal não 802.11 | 22 |
| Interferência entre canais | 23 |
| Pontos de acesso não autorizados | 24 |
| Qualidade da rede | 25 |
| Configure o testador | 26 |
| Mudar o idioma e as definições de país | 26 |
| Criar perfil para conexão a redes protegidas | 27 |
| Configurações | 29 |
| Operação em 802.11d | 36 |
| Alterar os limites das cores dos gráficos de barras | 37 |
| Atribuir status de autorização a pontos de acesso | 38 |
| Descobrir redes e pontos de acesso | 39 |
| Anotações para redes e pontos de acesso | 51 |
| Se o testador não conseguir descobrir um ponto de acesso | 54 |
| Uso do canal | 54 |
| Verificar a conectividade | 57 |
| Conectar a uma rede ou ponto de acesso | 57 |
| Inserir credenciais de segurança utilizando "Conectar" | 58 |
| Revisar resultados de conexão | 60 |
| Fazer ping de um dispositivo ou servidor de aplicativos | 63 |
| Descobrir clientes | 65 |
| Descobrimdo clientes através de PAs Meru | 66 |

| | |
|--|----|
| Se o testador não conseguir descobrir um cliente | 70 |
| Localizar um Ponto de Acesso ou um Cliente | 71 |
| Antena direcional externa | 75 |
| Ajuste as medidas de intensidade de sinal para estarem de acordo com outros dispositivos | 78 |
| Salvar uma sessão de teste | 79 |
| Gerenciar arquivos no testador | 80 |
| Sobre os arquivos contidos no testador | 81 |
| Transferir arquivos para um computador | 82 |
| Manutenção | 82 |
| Limpeza do testador | 83 |
| Atualização do software do testador | 83 |
| Restaurar padrões de fábrica | 84 |
| Excluir todos os dados | 84 |
| Informações sobre o dispositivo | 84 |
| Se não for possível desligar o testador | 84 |
| Opcionais e acessórios | 84 |
| Especificações | 86 |
| Especificações ambientais | 86 |
| Especificações gerais | 89 |
| Especificações de conexão sem fio | 90 |
| Declaração sobre interferência para Federal Communication Commission e Industry Canada | 94 |
| Observação importante: Declaração da FCC e da IC sobre exposição à radiação | 94 |
| Declaração de conformidade para a Europa-UE | 95 |

Lista das figuras

| Figura | Página |
|--|-----------|
| 1. Características físicas..... | 6 |
| 2. Como remover a bateria..... | 7 |
| 3. Resultados do AutoTest visualizados no AirCheck Manager | 8 |
| 4. A tela inicial | 19 |
| 5. Tela de resultados do AutoTest | 21 |
| 6. Limites padrão de utilização do canal 802.11 | 22 |
| 7. Limites padrão de utilização do canal não 802.11..... | 23 |
| 8. Limite padrão da qualidade do ar entre canais..... | 23 |
| 9. Limite padrão de nível de sinal | 24 |
| 10. Tela Principal do AutoTest | 26 |
| 11. Analisar a qualidade da rede de um SSID | 26 |
| 12. Mudança dos limites das cores de um gráfico de barras..... | 37 |
| 13. Lista Redes (SSIDs)..... | 41 |
| 14. Lista de pontos de acesso | 45 |
| 15. Tela de detalhes do ponto de acesso..... | 49 |
| 16. Tela de uso do canal | 54 |
| 17. Tela de detalhes do uso do canal..... | 56 |
| 18. Tela de conexão | 61 |
| 19. Log de conexão | 62 |
| 20. Tela de ping..... | 64 |

| | | |
|-----|---|----|
| 21. | Tela Clientes | 67 |
| 22. | Tela de Detalhes do Cliente..... | 69 |
| 23. | Tela de localização de ponto de acesso..... | 72 |
| 24. | Tela Localizar cliente..... | 72 |
| 25. | Padrão de busca da antena omnidirecional do testador..... | 75 |
| 26. | Padrão de busca da antena externa..... | 76 |
| 27. | Como apontar a antena externa..... | 78 |
| 28. | Arquivo oui_abbr.txt..... | 82 |

Testador de Wi-Fi do AirCheck™

Introdução

O Testador de Wi-Fi AirCheck™ garante que as redes LAN sem fio 802.11 estejam disponíveis para usuários móveis, examinar a utilização de canais para melhor analisar as condições da rede, e localizar a origem dos problemas de conexão. O testador opera em redes 802.11 na faixa de 2,4 GHz e em redes 802.11 a/n na faixa de 5 GHz. Ele tem a capacidade de detectar pontos de acesso e redes 802.11 ac.

O detector de PoE opcional indica se há disponibilidade de alimentação PoE (Power over Ethernet) por dispositivos 802.3af e dispositivos de alta potência tipo 802.3at em cabeamentos de rede de pares trançados.

Pode-se salvar os resultados de testes e usar o software AirCheck™ Manager para transferir os resultados a um computador e gerar relatórios de qualidade profissional. Além disso, o AirCheck Manager pode ser usado para comparar informações de diversas sessões de teste e ver as mudanças ocorridas em uma rede LAN sem fio.

Registro do produto

O registro do produto com a Fluke Networks dá ao comprador acesso a importantes informações sobre atualização do produto, procedimentos para solução de problemas e outros serviços. Para fazer o registro, preencha o formulário on-line no site da Fluke Networks em www.flukenetworks.com/fnet/pt-br/MyAccount.

Fluke Networks Knowledge Base

A Fluke Networks Knowledge Base contém respostas a perguntas comuns relacionadas aos produtos da Fluke Networks, além de artigos sobre tecnologia e procedimentos de testes de redes e de cabos. Para ver a Knowledge Base, acesse www.flukenetworks.com e clique em **Suporte > Knowledge Base**.

Para contatar a Fluke Networks



www.flukenetworks.com
support@flukenetworks.com
+1-425-446-4519

- Austrália: 61 (2) 8850-3333 ou 61 (3) 9329 0244
- Pequim: 86 (10) 6512-3435
- Brasil: 11 3759 7600
- Canadá: 1-800-363-5853
- Europa: +31-(0) 40 2675 600
- Hong Kong: 852 2721-3228
- Japão: 03-6714-3117
- Coreia: 82 2 539-6311
- Singapura: +65-6799-5566
- Taiwan: (886) 2-227-83199
- E.U.A.: 1-800-283-5853

Para obter outros números de telefone, visite nosso site.

Informações de segurança

A Tabela 1 apresenta os símbolos referentes a segurança usados no testador e neste manual.

Tabela 1. Símbolos de segurança

| | |
|--|---|
| | Aviso ou Cuidado: risco de danos ou destruição do equipamento ou do software. Veja as explicações no manual. |
| | Aviso: risco de choque elétrico. |
| | Produtos que contêm placas de circuitos não devem ser jogados no lixo comum. Informe-se sobre os procedimentos de descarte necessários de acordo com as regulamentações locais. |
| | Este equipamento contém um rádio de Classe 2. |



Leia todas as informações de segurança antes de usar o Produto.

Utilize o Produto somente conforme especificado, ou a proteção fornecida pelo Produto poderá ser comprometida.

Leia com atenção todas as instruções.

Use apenas adaptadores de energia aprovados da Fluke para carregar a bateria.

Não use o produto em áreas próximas a gases explosivos, vapor ou em ambientes úmidos ou molhados.

Examine o caso antes de usar o produto. Verifique se há alguma rachadura ou algum pedaço de plástico faltando. Analise o isolamento ao redor dos terminais.

Baterias contêm substâncias químicas perigosas que podem causar queimaduras ou explodir. Se houver exposição a produtos químicos, limpe com água e obtenha ajuda médica.

Remova as baterias se o produto não for utilizado por um período prolongado ou se ele for armazenado a temperaturas acima de 50 °C. Se as baterias não forem removidas, o produto poderá ser danificado por vazamento das baterias.

Não provoque curto-circuito nos terminais da bateria juntos.

Não desmonte ou bate nas células de bateria e nos pacotes de baterias. Não coloque pilhas e baterias perto de calor ou fogo. Não as exponha à luz solar.



Ao usar antena externa, use somente a antena fabricada pela Fluke Networks para o testador AirCheck. O testador não funcionará corretamente com outras antenas e poderá infringir os regulamentos locais.

Desembalagem do produto

O Testador de Wi-Fi AirCheck vem com os acessórios relacionados a seguir. Se algum item estiver danificado ou faltando, informe o distribuidor de quem o produto foi adquirido.

AirCheck – Testador de Wi-Fi

- AirCheck com unidade de bateria recarregável
- Adaptador CA
- Cabo USB
- Bolsa
- Guia de introdução
- CD com os manuais do produto
- CD do software AirCheck Manager

Kit do AirCheck para identificação e solução de problemas de primeira linha

- AirCheck com unidade de bateria recarregável
- Pacote adicional de bateria
- LinkRunner™ Pro
- Antena direcional externa com conector RSMA
- Detector de PoE
- Adaptador CA
- Cabo USB
- Bolsa
- Guia de introdução
- CD com os manuais do produto
- CD do software AirCheck Manager

Características físicas

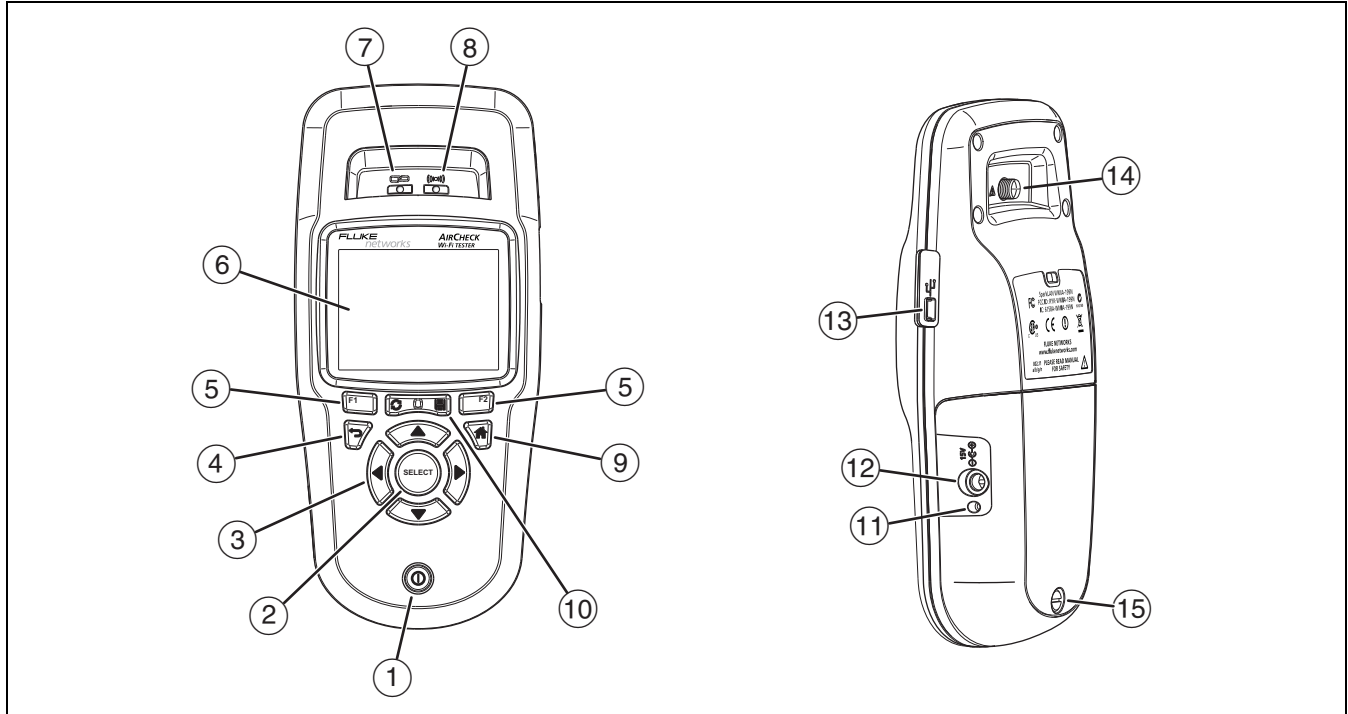




Figura 1. Características físicas

- ① Tecla liga/desliga
- ② Efetua uma seleção na tela.
- ③ Teclas de navegação.
- ④ Exibe a tela anterior.
- ⑤ Teclas de função. A função da tecla é indicada acima dela.
- ⑥ Display de cristal líquido (LCD) em cores (full-color).
- ⑦ O LED pisca quando o testador tenta se conectar a uma rede LAN sem fio. O LED se acende quando o testador está conectado a uma LAN sem fio.
- ⑧ O LED pisca quando o testador está transmitindo dados
- ⑨ Mostra a tela inicial.
- ⑩ : Apaga todos os dados coletados durante a sequência de testes atual. Isso não apaga os resultados gravados na memória.  Salva todos os dados em um arquivo de sessão. Consulte a página 79.
- ⑪ O LED se acende quando um adaptador CA é conectado. Quando a luz do LED está vermelha, significa que a bateria está sendo carregada; quando está verde, a bateria está totalmente carregada.
- ⑫ Conector para o adaptador CA.
- ⑬ Porta USB para conexão a um computador. O AirCheck aparece como um dispositivo de armazenamento em massa.
- ⑭ Conector para a antena direcional externa. Consulte a página 75.
- ⑮ Parafuso para a unidade de bateria.

Carregamento e duração da bateria

Carregue a bateria por 4 horas antes de usá-la pela primeira vez.

Para carregar a bateria, conecte o adaptador CA ao conector da bateria (12) na Figura 1). O testador pode ser usado enquanto a bateria está sendo carregada.

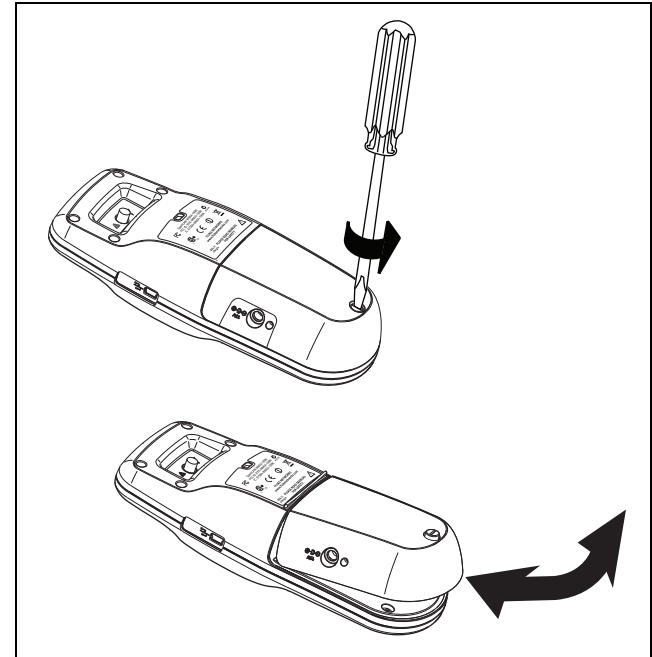
A Figura 2 mostra como trocar a bateria.

Com o testador desligado, a bateria é carregada em aproximadamente 3 horas.

Obs.:

A bateria não é carregada se a temperatura interna do testador estiver acima de 45°C (113°F).

A duração da bateria é de aproximadamente 5,5 horas durante uma operação normal. O nível de carga da bateria é indicado por um ícone no canto superior esquerdo da tela. Veja a figura 4 na página 19.



ffy14.eps

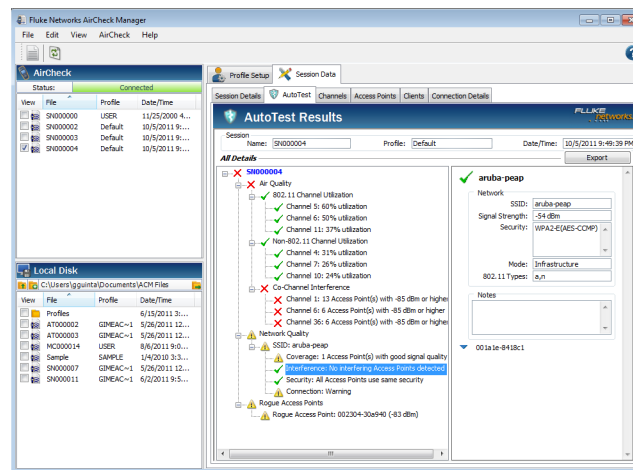
Figura 2. Como remover a bateria

Utilize o aplicativo para PC do AirCheck Manager para um melhor desempenho

Para que o testador apresente o máximo desempenho, utilize o AirCheck Manager para atualizar o firmware do testador AirCheck, para visualizar os resultados salvos como arquivos de sessão, gerar relatórios sobre arquivos de sessão, realizar a configuração do testador e salvá-la em um perfil, e transferir o perfil para o testador. Um perfil permite que o testador realize as seguintes tarefas:

- Conectar a redes que requerem credenciais de segurança. As credenciais de segurança podem ser inseridas no testador ou através do programa do AirCheck Manager.
- Mostrar o status de autorização correto para cada ponto de acesso. Isso permite ver rapidamente quais pontos de acesso são partes autorizadas da rede.
- Configurar os principais dispositivos de rede para executar Ping e um teste de conexão da porta TCP. Você deve configurar as credenciais de segurança para a(s) rede(s) que contenham dispositivos importantes para os quais esteja executando um ping.

Veja a “Utilizar o AutoTest para diagnosticar o estado da rede” na página 20. Utilize também a Ajuda online do AirCheck Manager para obter instruções.



ffy29.bmp




Figura 3. Resultados do AutoTest visualizados no AirCheck Manager


Informações que você pode obter sobre a sua rede

O que é o estado da minha rede?

**Como é a qualidade de ar de minha Wi-Fi?
Os meus canais estão sobrecarregados com pontos de acesso e tráfego de WiFi?
Os meus canais são muito ruidosos?**

Selecione **AutoTest** – Depois de executar o AutoTest, selecione **Qualidade do Ar** para ver os resultados da Utilização do canal 802.11, Utilização do canal não 802.11 e avaliação do estado da interferência entre canais.

Os resultados da Utilização do canal 802.11 incluem os três principais canais com o maior tráfego de Wi-Fi. É exibido o valor da utilização do canal junto com a classificação de  Aprovado,  Alerta ou  Não aprovado. A classificação do teste se baseia em uma comparação do valor real para os limites definidos pelos usuários. Esses limites são configurados em **Ferramentas > Limites/Configurações de AutoTest**.




Para ver os limites do Autoteste atual usados para avaliar os resultados, pressione  **Limites** na tela Autoteste (resultados).

Os resultados da Utilização do canal não 802.11 incluem os três principais canais com a maior interferência e ruído não 802.11. Exibe-se o valor da utilização do canal junto com a classificação de Aprovado, Alerta ou Não aprovado.


Os resultados da Interferência entre canais incluem os três principais canais com mais APs com força mínima do sinal. Exibe-se o número de pontos de acesso junto com a classificação de Aprovado, Alerta ou Não aprovado.


Veja Utilizar o AutoTest para diagnosticar o estado da sua rede, na página 39.

| | |
|--|---|
| <p>Como é a qualidade de ar de minha rede? Posso escutar os pontos de acesso que suportam minhas redes? Existem áreas sem cobertura na região? Existem muitos PAs próximos usando o mesmo canal e deixando minha rede mais lenta? Posso me conectar?</p> | <p>Selecione AutoTest – Depois de executar o AutoTest, selecione Qualidade de rede para ver os resultados de Cobertura, Interferência entre canais, Segurança e Avaliação de estado da conexão.</p> <p>Os resultados da Cobertura incluem a quantidade de pontos de acesso com boa qualidade de sinal com suporte a uma rede (SSID) junto a uma classificação de Aprovado, Alerta ou Não Aprovado. A classificação do teste se baseia em uma comparação dos valores reais para os limites definidos pelos usuários. Os limites de qualidade do sinal e número de APs do nível do sinal e a relação sinal/ruído são definidos nas telas Ferramentas > Limites / Configurações de Autoteste > Cobertura de rede, Nível de sinal e Limite sinal/ruído.</p> <p>Os resultados de Interferência entre canais incluem o número de pontos de acesso que se cruzam em uma rede juntamente com uma classificação entre Aprovado, Alerta ou Não Aprovado. Isso se baseia em uma comparação entre rede única (SSID) com os limites. Os limites para esse teste são definidos na tela Ferramentas > Limites / Configurações de AutoTest > Limites entre canais da qualidade da rede.</p> <p>Os resultados de Segurança informam se todos os pontos de acesso no SSID usam as mesmas credenciais de segurança junto com uma classificação de Aprovado, Alerta ou Não aprovado.</p> <p>O teste de conexão procura se conectar a cada rede configurada em seu perfil (veja página 58). Os resultados do teste indicam se você pode se conectar à sua localização atual. O estado da sua conexão, por exemplo, taxas de transmissão, tentativas de pacotes, e se você pode atingir outros dispositivos em uma rede, por exemplo, ping. Os resultados são apresentados junto a uma classificação de Aprovado, Alerta ou Não aprovado.</p> |
|--|---|

| | |
|---|---|
| <p>Quais pontos de acesso não autorizados ou desconhecidos estão conectados à minha rede Wi-Fi? Representam um risco de segurança?</p> | <p>O teste dos pontos de acesso invasores, um elemento opcional do Autoteste, indica se os pontos de acesso não autorizados ou desconhecidos são detectados com uma classificação  Aprovado,  Alerta ou  Não aprovado. Os resultados incluem uma lista de todos os pontos de acesso não autorizados escutados na sua localização. A identificação dos pontos de acesso não autorizados exige a configuração de uma lista de controle de acesso (ACL). A configuração da ACL está disponível na tela do Autoteste ao selecionar Pontos de acesso invasores > ACL ou Início > Pontos de acesso > ACL.</p> <p>Por padrão, o teste de Ponto de acesso invasor não está ativado. Para ativar o teste e permitir que ele seja executado como parte do Autoteste, selecione Ferramentas > Limites / Configurações de autoteste > Autoteste do ponto de acesso invasor.</p> <p>Veja <i>Utilizar o AutoTest para diagnosticar o estado da sua rede</i>, na página 39.</p> |
|---|---|

O que há na LAN sem fio?


| | |
|---|---|
| <p>Quais LANs sem fio estão disponíveis?</p> | <p>Selecione Redes para ver uma lista de LANs sem fio e os pontos de acesso que se conectam a cada rede. Para ver todos os pontos de acesso disponíveis em seu local, selecione Pontos de acesso. Consulte a página 41.</p> |
| <p>Quais são os pontos de acesso disponíveis? A intensidade do sinal é suficiente?</p> | <p>Selecione Pontos de acesso para ver uma lista de pontos de acesso disponíveis em seu local e a intensidade do sinal dos pontos de acesso. Para ver os gráficos de barra da intensidade do sinal e o ruído de um ponto de acesso, realce o ponto de acesso e depois pressione .</p> |



| | |
|---|--|
| <p>O ponto de acesso está configurado corretamente?</p> | <p>Selecione Pontos de acesso, realce um ponto de acesso e depois pressione . Consulte a página 45.</p> |
| <p>Existem novos pontos de acesso na área? Eles são seus pontos de acesso, vizinhos ou um invasor?</p> | <p>Use o recurso de status de autorização de dispositivo (ACL) para relatar automaticamente quando novos pontos de acesso forem localizados em seu local. Para usar esse recurso, configure status de autorização de ponto de acesso de cada ponto de acesso (por exemplo, autorizado ou vizinho), em seguida defina o status de autorização padrão de ? Desconhecido. Como resultado, o status de autorização padrão ? Desconhecido será atribuído a qualquer ponto de acesso não descoberto anteriormente. Finalmente, selecione Pontos de acesso na tela inicial para ver pontos de acesso marcados como ? Desconhecido.</p> <p>Como alternativa, salve a sessão de teste que contém a lista de pontos de acesso descobertos. Use o AirCheck Manager para comparar a lista de pontos de acesso a um arquivo de sessão previamente salvo para ver se pontos de acesso adicionais foram descobertos.</p> <p>Para especificar uma autorização de dispositivo padrão de desconhecido ou autorizado, selecione Ferramentas > Definir padrão de autorização do dispositivo (ACL).</p> |
| <p>Quais clientes sem fio usam a rede?</p> | <p>Na tela de início, selecione Redes, selecione uma rede e busque a tela de Detalhes do Ponto de Acesso, e selecione Cientes. Você também pode arrastar para a tela de Detalhes do Ponto de Acesso desde vários locais para ver clientes associados a qualquer ponto de acesso específico.</p> <p>Para ver todos os clientes, inclusive os conectados e em teste em todas as redes dentro do alcance do testador: selecione Cientes na tela inicial.</p> |

Dispositivos podem se conectar à minha rede?


Use o testador para verificar a conectividade.

Obs.:



Para conectar-se a uma rede segura, o testador deve ter um perfil que inclua credenciais de segurança. Se as credenciais não estiverem disponíveis, a tecla de função será mostrada como  Conectar. Consulte a página 26.*

| | |
|---|---|
| É possível conectar um dispositivo como cliente à rede (SSID)? | Selecione Redes , realce uma rede e pressione  Conectar . Consulte a página 60. |
| É possível fazer um dispositivo se conectar a um ponto de acesso (BSSID)? | Selecione Pontos de acesso , realce um ponto de acesso e depois pressione  Conectar . Consulte a página 60. |
| Caso não seja possível conectar um dispositivo a uma rede ou ponto de acesso, onde estará a falha neste procedimento de conexão? | Veja o registro de conexão. Consulte a página 62. |
| É possível fazer com que um dispositivo execute um ping em um dispositivo de rede? | Faça um teste de ping. Consulte a página 63. |
| O cartão de interface de rede funciona corretamente em um cliente? | Na tela iniciar, selecione Clientes para verificar se o cliente transmite quadros de solicitação de sonda e para ver as configurações básicas, como o canal e os SSIDs que o cliente usa nas sondas. Consulte a página 67. |

Qual é a causa de um desempenho lento da rede e das quedas de conexão?


| | |
|---|--|
| A intensidade do sinal é suficiente? | Selecione Pontos de acesso . A tela de Pontos de acesso mostra a intensidade do sinal de cada ponto de acesso. Selecione um ponto de acesso para ver mais detalhes sobre a intensidade e o congestionamento do sinal. Consulte a página 49. |
| A rede está muito ocupada? | Selecione Canais para ver um quadro geral da utilização de canais e o número de pontos de acesso e clientes conectados que usam cada canal. Para ver um gráfico, realce o canal e pressione  . Consulte a página 54. |
| Existe alguma interferência que não seja de 802.11 em algum canal? | Selecione Canais . A interferência não 802.11 é a porção cinza da barra do gráfico. Esse ruído pode interferir nas conexões ou no desempenho da WLAN. O ruído não-802.11 pode ser gerado a partir dos fornos de microondas, telefones sem fio, dispositivos Bluetooth®, detectores de movimento, câmeras sem fio e outros dispositivos sem fio. Consulte a página 56. |

Existe algum risco de segurança na rede?



| | |
|--|---|
| As redes apresentam o nível esperado de segurança? | Selecione Redes . Redes com pontos de acesso desprotegidos são indicadas por um cadeado vermelho aberto (). Consulte a página 41. |
| Existe alguma rede ad hoc na área? | Selecione Redes . Redes com clientes ad-hoc são indicadas pelo ícone de rede ad-hoc () na coluna SSID . Clientes ad-hoc podem apresentar riscos de segurança à rede ou infringir as políticas da rede. Consulte a página 41. |
| Existe algum ponto de acesso não controlado na área? Onde eles estão? | <p>O AirCheck pode ser usado para ajudar a rastrear o status de autorização de pontos de acesso descobertos. Por definição padrão, quando são descobertos pontos de acesso, lhes é atribuído um status de autorização de ? Desconhecido. É possível alterar o status de indivíduo ou grupos de pontos de acesso para refletir sua relação com sua rede, por exemplo, autorizado, vizinho, não autorizado.</p> <p>Também existe a opção de alterar o status do dispositivo padrão de ? Desconhecido para ✓ Autorizado. Uma vez alterado, todos os pontos de acesso descobertos serão identificados como ✓ Autorizado. É possível em seguida revisar a lista e atribuir status a pontos de acesso individuais adequadamente. Por exemplo, se você souber que um ponto de acesso não é autorizado, pode dar a ele um o status de ▶ Dispositivo sinalizado ou ⚠ Dispositivo não autorizado. Consulte a página 38.</p> |

| | |
|--|--|
| | <p style="text-align: center;"><i>Obs.:</i></p> <p>O Autoteste inclui, como opção um teste de Ponto de Acesso invasor que detecta e relata pontos de acesso invasores. Para habilitar esta funcionalidade, vá para Ferramentas > Limites/Configurações de autoteste > Autoteste do ponto de acesso invasor. Para obter resultados de teste precisos e significativos, é necessário configurar ACLs de ponto de acesso antes de executar o Autoteste.</p> <p><i>Quando você salva seu perfil, as ACLs designadas também serão salvas como parte desse perfil.</i></p> <p>Também é possível definir uma série de PAs para autorizado ou não autorizado com base no AP BSSID/MAC ou no prefixo MAC do fornecedor, ao selecionar ✓ Definir série PA para Autorizado ou ⚠ Definir série PA para Não autorizado. Essas opções podem reduzir o tempo gasto na configuração e fornecer visibilidade rápida de possíveis problemas. Por exemplo, se o equipamento de um fornecedor específico não tem permissão por sua política de rede, use o prefixo MAC do fornecedor para definir a ACL para não autorizado. Quando esses pontos de acesso são detectados, serão automaticamente encaminhados como não autorizados.</p> |
|--|--|

Onde se localiza um ponto de acesso?

Selecione **Pontos de acesso**, selecione um ponto de acesso e depois pressione  **Localizar** na tela **Detalhes do PA**. Consulte a página 71. Use também a antena direcional externa opcional da Fluke Networks para localizar pontos de acesso com mais rapidez. Consulte a página 71.

Que redes ou pontos de acesso entram na faixa de alcance conforme me movimento?

Classifique a lista em ordem decrescente, na coluna de registro de hora (). Pressione , e movimente-se na área. As redes ou pontos de acesso que entram na faixa de alcance são acrescentados ao começo da lista. Veja a página 42 ou 46.

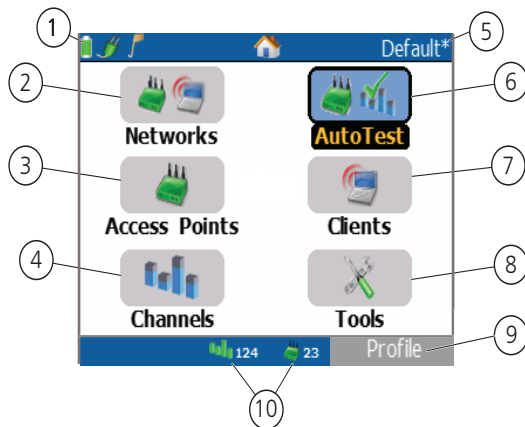
Como posso documentar minha rede e minha sessão de teste?

Salve a sessão (veja a página 71) e, em seguida, use o software AirCheck Manager para transferir os resultados para um computador e gerar um relatório. Consulte a página 82.

Como faço para apagar tudo no meu AirCheck?


Se quiser apagar todas as configurações, dados de sessões e perfis no testador, selecione **Ferramentas > Apagar tudo** – Tudo o que foi salvo ou armazenado no testador AirCheck será apagado.

A tela inicial



Home.eps

Figura 4. A tela inicial

- ①  Mostra o estado da bateria. Quando a carga da bateria estiver baixa, o ícone piscará. Conecte o adaptador CA para carregar a bateria e assegurar que o testador continue a funcionar.



Indica que o adaptador CA está conectado.






Indica que a antena externa está conectada.

Obs.:

O AirCheck não vai transmitir nem se conectar a um ponto de acesso quando a antena externa estiver conectada.

- ② **Redes:** Descobre LANs sem fio. Consulte a página 39.
- ③ **Pontos de acesso:** Descobre pontos de acesso. Consulte a página 39.
- ④ **Canais:** Indica a utilização de canais de WLAN. Consulte a página 54. O nome do perfil usado pelo testador. Se nenhum outro perfil tiver sido carregado, será usado o perfil **Padrão**. O nome tem um asterisco se alguma configuração do testador tiver sido alterada desde que o perfil foi carregado ou salvo. Consulte a página 81.
- ⑤ **Autoteste:** Verifica automaticamente o funcionamento da rede, ao observar a qualidade do ar (utilização dos canais e interferências), qualidade da rede (cobertura da rede e conectividade), e a presença de redes ad hoc. A detecção de ponto de acesso invasor é opcional e requer configuração de ACL.
- ⑥ **Clientes:** Descobre clientes associados e não associados (exemplo: sondagem).

- 7 **Ferramentas:** Permite gerenciar arquivos e configurações.
- 8 **Perfil:** Permite carregar ou salvar um perfil. Na tela Inicial, pressione  **Perfil**.
- 9 À esquerda:  O canal que o testador está monitorando no momento. A cor das barras mostra o status do código do país de um domínio normativo. Um ícone vermelho pode indicar a operação de um canal ilegal da configuração de país atual e/ou a recepção de um código de país diferente. Consulte “Operação em 802.11d” na página 36. À direita

: O número de  pontos de acesso que o testador tem. Esse número é uma contagem dos pontos de acesso físicos quando a opção **Agrupar pontos de acesso virtuais** está ativada. Consulte a página 32.

Até 500 pontos de acesso podem ser armazenados no banco de dados de pontos de acesso do testador. Quando o ícone do ponto de acesso fica amarelo, indica que um número igual ou maior que 400 pontos de acesso foram descobertos. Quando o ícone fica vermelho, indica que 500 pontos de acesso ou mais foram descobertos e o banco de dados de pontos de acesso está cheio. Qualquer ponto de acesso novo encontrado não será incluído na lista.

Utilizar o AutoTest para diagnosticar o estado da rede

O Autoteste verifica automaticamente o funcionamento da rede examinando a qualidade do ar, redes ad hoc, qualidade da rede e o potencial risco de pontos de acesso invasores, se configurado.

Obs.:

Se nenhum SSID foi configurado, isto é, acrescentado ao AirCheck, o AutoTest será executado para todos SSIDs. Se foi acrescentado algum SSID, somente esse será testado. O teste de Conexão será executado somente para os SSIDs que foram configurados com credenciais de segurança.

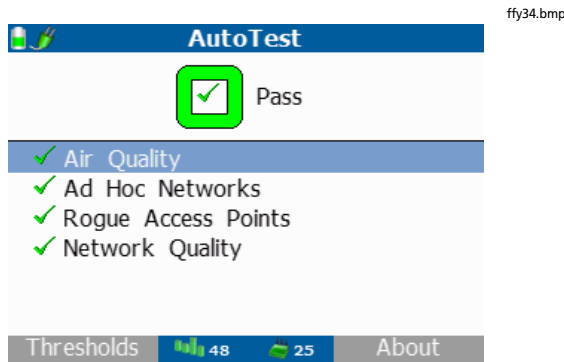


Figura 5. Tela de resultados do AutoTest

Qualidade do ar

A medição da Qualidade do Ar mostra a Utilização do canal 802.11, a Utilização do canal não 802.11 e da Interferência entre canais.

Utilização de canal 802.11

Os resultados da utilização de canal 802.11 incluem três canais de Wi-Fi com maior utilização de 802.11 e são apresentados com o valor medido e o símbolo de classificação: ✓ Aprovado, ⚠ Alerta ou ✗ Não aprovado.

Salve o perfil para que as configurações não se percam quando o testador estiver desligado. Na tela inicial, pressione **F2** **Perfis**, realce e selecione **Salvar perfil**. Também é possível salvar os perfis em **Ferramentas > Gerenciar perfis / senhas da rede > Salvar perfil**.

Essa medida se baseia nos limites configurados na tela **Ferramentas > Limites / Configurações de Autoteste > Limites de utilização de canal 802.11** apresentada nos próxima figura.

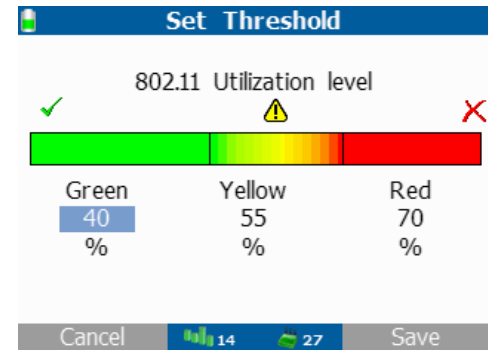


Figura 6. Limites padrão de utilização do canal 802.11

Pressione **F1** **Limites** para ver os valores de limite de do Autoteste usado para relatar a integridade da rede.

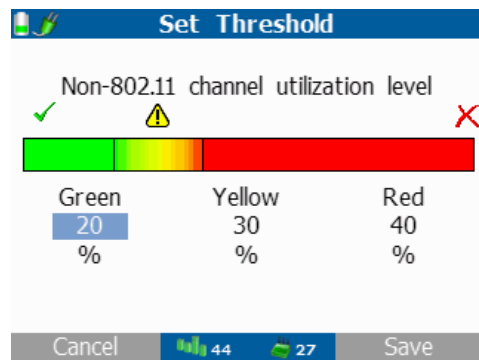
Mude os limites na tela **Ferramentas > Limites / Configurações de Autoteste**.

Utilização de canal não 802.11

Os resultados da utilização do canal não 802.11 incluem os três canais com mais interferência, ou seja, ruído de tipo não 802.11. O valor da utilização do canal juntamente com a classificação **✓** Aprovado, **⚠** Alerta, ou **✗** Não aprovado.

O uso variará dependendo da hora do dia, do número de clientes que passaram da parte da rede com fio para a parte sem fio ou da quantidade de interferência de dispositivos como microondas, filmadoras etc.

Essa medida se baseia nos limites configurados na tela **Ferramentas > Limites / Configurações AutoTest > Limites de utilização de canal não802.11**.

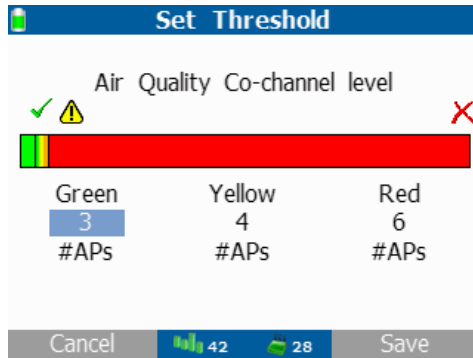


ffj23.bmp

Figura 7. Limites padrão de utilização do canal não 802.11

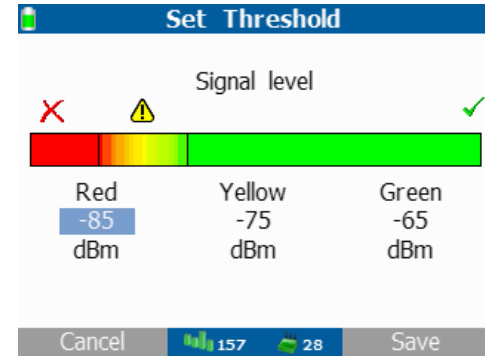
Interferência entre canais

Os resultados da Interferência entre canais incluem o número de pontos de acesso cruzados que ultrapassam o limite de qualidade de sinal e é visto com a classificação de **✓** Aprovado, **⚠** Alerta, ou **✗** Não Aprovado. Os limites para esse teste estão configurados na tela **Ferramentas > Limites / Configurações de Autoteste > Limites entre canais de qualidade da rede**, e o limite de intensidade do sinal do canal é configurado na tela **Ferramentas > Limites / Configurações de Autoteste > Limites de nível de sinal**.



ff24.bmp

Figura 8. Limite padrão da qualidade do ar entre canais






ff25.bmp

Figura 9. Limite padrão de nível de sinal




Essa medida é independente dos SSIDs e verifica somente o número de pontos de acesso e a respectiva qualidade de sinal.

Redes Ad Hoc



Os resultados de teste de redes ad hoc indicam a presença de dispositivos cliente com uma classificação  Aprovado,  Alerta ou  Não aprovado. Os resultados incluem uma lista de todas as estações ad hoc escutadas na sua localização.

Os dispositivos clientes ad hoc se comunicam diretamente com outros clientes, e não por um ponto de acesso. Esses dispositivos podem fornecer aos hackers acesso aos dados transmitidos na rede. (Algumas políticas de TI para redes permitem dispositivos ad hoc).

Pontos de acesso não autorizados

O teste de Pontos de acesso invasores indica se foram detectados pontos de acesso não autorizados com uma classificação de  Aprovado,  Alerta ou  Não aprovado. Os resultados incluem uma lista de todos os pontos de acesso não autorizados escutados na sua localização. A identificação dos pontos de acesso não autorizados exige a configuração da lista de controle de acesso (ACL). O teste de Ponto de acesso invasor é desativado por padrão. Contudo, quando estiver ativado, ele é executado automaticamente como parte do autoteste. Para ativar o teste de ponto de acesso invasor, selecione **Ferramentas > Limite /Configurações de autoteste > Teste de ponto de acesso invasor**.

Inicialmente, todos os pontos de acesso são definidos para um status padrão de **Desconhecido**, mas também podem ser definidos como **Autorizados**. Consulte a página 39.

Para definir o status de ACL, vá à tela inicial, e selecione a tela **Pontos de acesso**. Depois selecione  **ACL**, e edite cada ponto de acesso. Selecione **Definir todos os pontos de acesso para Autorizado** para definir o status de todos os pontos de acesso descobertos para "Autorizado". Isso também pode ser feito na tela **Autoteste > Ponto de acesso invasor** selecionando-se **ACL**, realçando-se o ponto de acesso e selecionando-se **ACL** novamente. Selecione o seguinte tipo de autorização e pressione o botão de retrocesso .

Obs.:

Se você alterar o ACL no AutoTest, você deve executar novamente o AutoTest para que as alterações sejam aplicadas.



Dispositivo não autorizado



Serviço autorizado



Dispositivo vizinho



Dispositivo desconhecido



Dispositivo sinalizado



Definir todos os APs como Autorizados

  **Definir todas as Séries de AP como Autorizadas**

  **Definir todas as Séries de AP como Não autorizadas**

Qualidade da rede

As medidas de Qualidade da Rede verificam a disponibilidade de rede oferecida, a existência de interferência dos pontos de acesso utilizando o mesmo canal que pode comprometer a velocidade da rede, uso do ponto de acesso de métodos de segurança consistentes para uma rede e a capacidade de conectar e usar a rede (acesso a serviços, outros dispositivos) e oferecer qualidade de rede.

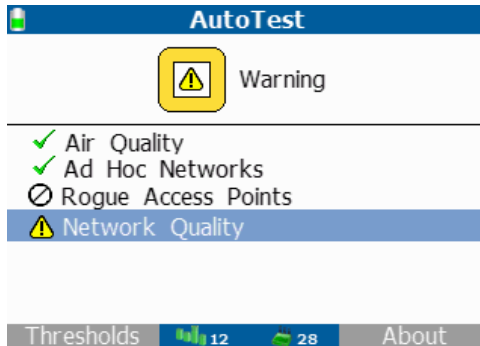



Figura 10. Tela Principal do AutoTest

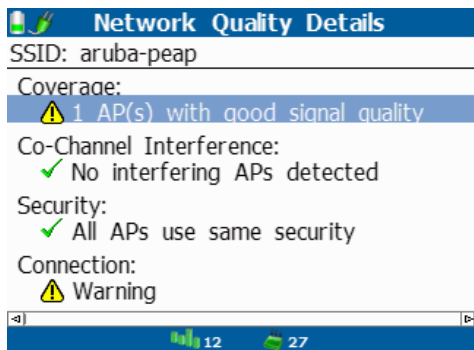
A segurança da rede pode ser configurada na tela inicial selecionando **Redes > Conectar** e passar pelas telas de configuração de segurança. Verifique *Inserir Credenciais de Segurança* na página 58 para ver os procedimentos de **Conexão**.

Os teste de Qualidade da Rede são executados para cada SSID no perfil atual com resultados informados na tela de Qualidade da Rede. Todos os SSIDs descobertos serão testados se nenhum SSID for configurado no perfil.

Os resultados do teste de Conexão indicam se você pode se conectar ao seu local atual. O estado da sua conexão, por exemplo, taxas de transmissão de pacotes, tentativas de pacotes e se você pode atingir outros dispositivos na rede, por exemplo, ping.

Os resultados são apresentados junto a uma classificação de Aprovado, Alerta ou Não aprovado. A fim de executar o teste de Conexão, a segurança SSID deve estar configurada, caso contrário você verá:

Connection:
 Not Tested




ffy27.bmp


Figura 11. Analisar a qualidade da rede de um SSID

Configure o testador

Para mudar as definições do testador, selecione **Ferramentas**, na tela inicial. Veja a Tabela 2 na página 30.

Mudar o idioma e as definições de país

- 1 Selecione **Ferramentas**.
- 2 Para mudar o idioma apresentado na tela, selecione **Definir idioma**. Selecione um idioma, e clique em  **Salvar**.

- 3 Para alterar o país, selecione **Configurar país**, selecione o país onde você usará o testador, e pressione  **Salvar**. Consulte a página 35.

Criar perfil para conexão a redes protegidas

Os perfis são arquivos que contêm configurações de segurança para redes e para o testador. As configurações de redes incluem credenciais de segurança. As credenciais de segurança fazem com que o testador possa se conectar a redes e realize testes de ping, descubra servidores DNS, servidores DHCP, e o roteador padrão.

Os perfis contêm credenciais/definições de segurança de rede para que o testador possa se conectar a redes. O perfil pode ser protegido por senha para que os usuários não autorizados não utilizem o testador para se conectarem a redes seguras, e não tenham acesso às credenciais de segurança de rede no aplicativo para PC AirCheck Manager.

As configurações do testador podem ser salvas na forma de um perfil, ou pode-se usar o AirCheck Manager no computador para criar um perfil.

A tela inicial mostra o nome do perfil usado pelo testador. O nome tem um asterisco se alguma configuração do testador tiver sido alterada desde que o perfil foi carregado ou salvo. O testador salva as alterações em um arquivo temporário. O testador usa o arquivo temporário como perfil atual. Ao salvar o perfil, o testador copia as mudanças no perfil mostrado na tela inicial.

Os perfis criados no AirCheck Manager incluem estas definições:

- Senha do perfil
- Credenciais de segurança para redes (criptografia, nome de usuário, senha, etc..)
- Status de autorização de redes (SSIDs) e pontos de acesso
- Os endereços IP usado para ping ou testes de conexão de porta TCP
- Todas as definições de 802.11 (ex.: **Ativar faixa de 2,4 GHz** e **Ativar faixa de 5 GHz**. Veja a página 32.)
- País
- Configurações de AutoTest

Definições de limites dos gráficos de barras




Se o perfil for salvo enquanto estiver sendo usado, o testador adicionará estas definições ao perfil:

- Definição de som para a função de localização
- Definição de desligamento automático
- Sequências para ordenação de listas de redes, pontos de acesso e clientes



Para transferir um perfil de um computador para o testador

- 1 Utilize o **Configurar Perfil** no AirCheck Manager para criar um perfil.
- 2 Use o cabo USB fornecido com o testador para conectá-lo ao computador.
- 3 Utilize a função de transferência na **Configuração de Perfil** para transferir o perfil ao testador.

Para carregar um perfil contido no testador

- 1 Na tela Inicial, pressione  **Perfis**.
- 2 Realce e pressione  **Carregar perfil**.
- 3 Realce um perfil e pressione  **Carregar**

Ou

- 1 Selecione **Ferramentas > Gerenciar Perfis / senhas de rede**, depois selecione **Carregar perfil**.
- 2 Realce o perfil desejado, pressione  e, em seguida,  **Carregar**.

Obs.:






Se o arquivo não for um perfil válido, ou se a extensão não for “.ACP”, o testador apresentará a mensagem “Não foi possível carregar o perfil selecionado”.

- 3 Se necessário, digite a senha do perfil.

Obs.:









*Você só precisa inserir a senha na primeira vez que você carregar um perfil no testador. Para proteger todos os perfis com senha novamente, selecione **Ferramentas > Restabelecer padrões de fábrica**.*

Para salvar as definições atuais como um perfil


- 1 Selecione **Ferramentas > Gerenciar Perfis / senhas de rede**, depois selecione **Salvar perfil**.
 - Para salvar o perfil com o nome de arquivo mostrado, pressione  **Salvar**. O testador salva o perfil na pasta "PERFIS".
 - Para gravar em cima de um perfil salvo no testador, realce-o e pressione  em seguida  **Salvar**; depois pressione  **OK**.
 - Para editar o nome do arquivo, pressione  **Editar**.

Obs.:

Nomes de arquivo podem ter, no máximo, 8 caracteres e uma extensão de 3 caracteres. Se quiser que o perfil apareça no AirCheck Manager, use a extensão ".ACP".

- Para apagar caracteres do nome do arquivo, pressione  **Excluir**.
- Para acrescentar caracteres ao nome do arquivo, use    para realçar o caractere e pressione .
- Para mover o cursor pelo nome do arquivo, realce o nome do arquivo e pressione  .
- Para salvar o perfil com o nome de arquivo editado, pressione  **Salvar**. O testador salva o perfil na pasta "PERFIS".

Para apagar um perfil

- 1 Selecione **Ferramentas > Gerenciar arquivos**.
- 2 Selecione **Excluir arquivo**.
- 3 Selecione a pasta PERFIS.
- 4 Realce o perfil e pressione .
- 5 Pressione **Excluir**.

Configurações

A tabela 2 descreve as diferentes configurações e telas afetadas. As configurações são acessadas pela tela **Ferramentas**.

Ao mudar uma definição, pressione **F2** **Salvar** para salvar as mudanças efetuadas. Para sair da tela sem salvar as configurações, pressione **F1** **Cancelar**.

Obs.:

*Para salvar as definições em um perfil, selecione **Ferramentas > Gerenciar perfis / senhas de rede > Salvar perfil** ou pressione **F2** **Perfil** na tela inicial e, em seguida, **Salvar perfil**. O nome do perfil aparece no canto superior direito da tela inicial. Caso apareça com um asterisco*, isso indica que uma alteração de configuração foi feita e que o perfil ainda não foi salvo.*

Tabela 2. Definições do menu Ferramentas




| | |
|---|--|
| Configurações de Limites/ AutoTest | <p>Permite que você configure os limites utilizados para o AutoTest e para outras medidas em todo o testador. Consulte a página 37. As medidas podem ser  Aprovado,  Alerta ou  Não Aprovado baseadas nesses limites.</p> <p>O Autoteste não se conecta a SSIDs abertos a menos que sejam adicionados manualmente ao AirCheck Manager e salvos no perfil do AirCheck.</p> <p>Conectar a redes em um perfil – Quando selecionada, a conectividade a SSIDs no perfil atual será testada como parte do Autoteste da Qualidade da Rede. Os SSIDs com segurança configurados e SSIDs abertos/não seguros são incluídos.</p> <p>Autoteste de ponto de acesso invasor - Quando marcado, ativa o teste de ponto de acesso invasor para ser executado como parte do Autoteste. Para obter resultados de testes mais precisos, você deve configurar a ACL antes de executar o teste. Consulte a página 24.</p> <p>Limite de nível de sinal – Indica a distância relativa entre ponto de acesso/cliente. Presente no teste de Qualidade da Rede > AutoTest e na tela de detalhes do cliente. Usado globalmente, não só no AutoTest.</p> <p>Limite de ruído - Nível de ruído detectado. Presente na > Interferência entre canais/Segurança > de Qualidade da Rede ao navegar na tela de Detalhes de PA. Usado globalmente, não só no AutoTest.</p> <p>Limite de sinal-ruído - Mede/prevê a qualidade do sinal de conexão do cliente. Presente na tela de alcance da Qualidade da Rede > do AutoTest. Usado globalmente, não só no AutoTest.</p> <p>Limite de alcance da rede - O número de PAs em um SSID necessários para o alcance do teste da Qualidade de Rede > do AutoTest sob o Alcance.</p> <p>Limite de utilização de 802.11 - Porcentagem de tempo que o canal possui pacotes de 802.11 enquanto o AutoTest colhe os resultados. Presente na tela de Qualidade do Ar.</p> <p>Limite de utilização não 802.11 - Porcentagem de tempo que o canal possui ruído excessivo enquanto o AutoTest colhe os resultados. Presente na tela de Qualidade do Ar.</p> |
|---|--|

Tabela 2. Definições do menu Ferramentas (continuação)


| | |
|---|---|
| Configurações de Limites/ AutoTest (continuação) | <p>Limite de Interferência entre canais da Qualidade de Ar - Múltiplos PAs no mesmo canal causam interferência. Presente na tela de Qualidade do Ar.</p> <p>Limites da Qualidade de Rede entre canais – PAs que coincidem com SSID sobreposto no canal. Presente na tela Qualidade da Rede sob Detalhes de Conexão.</p> |
| | <p>Limite de taxa de tentativa - Porcentagem de pacotes de ping reenviados durante os testes de ping. Presente na tela Qualidade da Rede sob Detalhes de Conexão.</p> <p>Limite do nível de taxa de pacote conectado - Porcentagem da taxa do pacote da taxa máxima de pontos de acesso suportados, isto é, real/máx. = %. Presente na tela Qualidade de Rede em Detalhes de Conexão.</p> <p>Limite mínimo do sinal - Os testes de interferência entre canais ignoram os PAs abaixo desse nível de sinal. Presente na tela Qualidade de Rede em Detalhes de Conexão e nos resultados de Interferência entre canais na Qualidade de Ar.</p> |
| Gerenciar arquivos | <p>Renomear arquivo - Permite renomear arquivos de perfis e de sessão.</p> <p>Excluir arquivo - Permite excluir arquivos de perfis e de sessão.</p> <p style="text-align: center;"><i>Obs.:</i></p> <p style="text-align: center;"><i>As medições atuais são salvas em um arquivo de sessão ao pressionar </i></p> |

Tabela 2. Definições do menu Ferramentas (continuação)

| | |
|--|---|
| <p>Gerenciar configuração s 802.11</p> <p><i>Obs.: Estas configurações mudam a forma pela qual o testador localiza e exibe os pontos de acesso. Antes de usar o testador, é útil saber claramente o que estas configurações determinam.</i></p> | <p>Permite definir opções para listas de pontos de acesso e canais.</p> <ul style="list-style-type: none">• Ativar faixa de 2,4 GHz, Ativar faixa de 5 GHz: Selecione um comprimento de onda ou as duas faixas de frequência para ver as redes e os pontos de acesso de uma ou ambas as faixas.• Transmitir sondas: Para descobrir pontos de acesso, o testador escuta transmissões de SSID em cada canal. O testador pode descobrir somente pontos de acesso que transmitem SSID enquanto o testador estiver no mesmo canal. Para efetuar descobertas mais rapidamente, por padrão, o testador transmite quadros de solicitação de sonda para obter respostas dos pontos de acesso. Como as sondas aumentam a utilização dos canais, o testador não as transmite quando as telas de utilização estão sendo exibidas ou quando há uma antena externa conectada.• Agrupar pontos de acesso virtuais: Quando um ponto de acesso transmite SSIDs múltiplos e/ou endereços MAC (BSSIDs), os MACs são pontos de acesso virtuais. Pontos de acesso virtuais aceitam diversas redes de um mesmo ponto de acesso físico. Um ponto de acesso que usa dois rádios para transmitir vários MACs pode aceitar redes que se encontram em vários canais. Quando a opção Agrupar pontos de acesso virtuais está ativada, os pontos de acesso virtuais aparecem na lista Pontos de acesso como um único ponto de acesso. Se o ponto de acesso transmite um nome (apresentado na coluna Nome/MAC), o número de SSIDs que ele suporta aparece na coluna SSID. Por exemplo, "2 SSIDs" aparece na coluna. Se um ponto de acesso não transmite um nome, possui um asterisco na coluna ou colunas onde o BSID é diferente de um ponto de acesso virtual ao outro. Para ver os endereços MAC e os SSIDs dos pontos de acesso virtuais, selecione o ponto de acesso na lista Pontos de acesso. Por padrão, essa configuração está habilitada. |
|--|---|








Tabela 2. Definições do menu Ferramentas (continuação)

| | |
|---|---|
| Gerenciar configurações de 802.11 (continuação) | <ul style="list-style-type: none">• Deixar pontos de acesso inaudíveis em cinza: Se o testador não capta nada de um ponto de acesso durante quatro ciclos de todos os canais, o ponto de acesso aparece em cinza na lista Pontos de acesso. Esta é a definição padrão.• Excluir pontos de acesso inaudíveis: Se o testador não capta nada de um ponto de acesso durante quatro ciclos de todos os canais, ele apaga o ponto de acesso da lista Pontos de acesso.• Usar ajustes de sinal personalizados: As medidas de intensidade de sinal de modelos diferentes de testadores de rede sem fio ou de clientes utilizados como referência nem sempre estão de acordo. As diferenças são provocadas principalmente pelas diferenças nas antenas. Para fazer com que os dispositivos coincidam, você pode acrescentar um desvio às medidas do AirCheck na tela. |
|---|---|

Tabela 2. Definições do menu Ferramentas (continuação)

| | |
|---|--|
| Gerenciar senhas de perfis/redes | <p>Permite a alteração da senha do perfil (definida como nenhuma por padrão), e a edição de credenciais/definições de segurança de rede que você configurou anteriormente. A senha do perfil evita acesso não autorizado a credenciais de segurança de rede utilizadas anteriormente. Para alterar a senha do perfil, selecione Alterar senha do perfil, insira a senha e selecione Alterar. Ou selecione Excluir para remover a senha.</p> <p>Para alterar as credenciais de segurança de rede, selecione Editar redes, e selecione a rede a ser editada. O AirCheck suporta os seguintes formatos de criptografia: Aberto, WEP, Legacy 802.1X, WPA Personal, WPA2 Personal, WPA Enterprise e WPA2 Enterprise.</p> <p style="text-align: center;"><i>Obs.:</i></p> <p style="text-align: center;"><i>O AirCheck não permite a autenticação Cisco LEAP ou Cisco PPK (Per-Packet Keying) (Codificação Pré-Pacote).</i></p> <p>Carregar perfil - Carrega um perfil salvo anteriormente. Os perfis contêm todas as configurações do testador incluindo credenciais de segurança SSID.</p> <p>Salvar Perfil - Salva as configurações atuais em um arquivo de perfil. Você pode alterar o nome padrão apresentado na parte inferior da tela pressionando Editar.</p> <p>Editar destinos - Permite para selecionar ou desmarcar destinos com ping ao executar o autoteste. Os destinos disponíveis são: gateway padrão, servidor DHCP, DNS primário e secundário. O gateway padrão e o servidor DHCP são selecionados por padrão.</p> <p>Você tem a capacidade para adicionar seus próprios destinos de IP. Selecione <input type="text" value="F1"/> Adicionar para fornecer um nome de host ou um endereço IP diretamente no testador. O AirCheck Manager também permite que você adicione um número de porta designado. Consulte a ajuda on-line do AirCheck para obter informações adicionais.</p> |
|---|--|

Tabela 2. Definições do menu Ferramentas (continuação)

| | |
|---------------------------------------|---|
| Definir data e hora | Permite a configuração de hora e data. Use   para selecionar uma configuração, e use   para alterar a configuração que o testador inclui nos resultados salvos. |
| Definir país | Os canais que são ilegais no país selecionado são indicados em vermelho nas telas Uso do canal , Detalhes do uso do canal e Detalhes de pontos de acesso . Veja a “Operação em 802.11d” na página 36. Os pontos de acesso que transmitem um código de país que não corresponde a esta definição são indicados por barras vermelhas na coluna 802.11 . |
| Definir idioma | Define o idioma a ser usado na interface do usuário. |
| Exibir informações do AirCheck | Mostra o número de série do testador, endereço MAC, versão do software, versão USB, e versão para rádio. |
| Brilho e Deslig. Automático | <p>Visualização de baixo brilho – Permite a configuração do brilho para pouco uso de energia. Marque a caixa e selecione  Salvar para alterar a configuração</p> <p>Desligamento automático to ativado - Quando ativada, o testador se desliga automaticamente após 10 minutos de inatividade (sem pressionamento de tecla). Ao se desligar automaticamente, o testador não salva a sessão de teste. Salva, contudo, as mudanças efetuadas no perfil. O testador não se desliga automaticamente se o adaptador CA estiver conectado. Para salvar a configuração, pressione  Salvar.</p> <p>Para sair da tela sem salvar as definições, pressione  Cancelar.</p> |
| Restaurar padrões fábrica | Restabelece todas as definições pré-configuradas na fábrica. Veja o Apêndice . |
| Apagar tudo | Apaga todos os dados no testador incluindo os perfis e os dados salvos da sessão. |


Operação em 802.11d


Quando um ponto de acesso usa o padrão 802.11d, ele transmite um código de país ISO nos beacons e respostas de sondas. Quando o testador recebe esse código, ele efetua transmissões apenas pelos canais que são legais no país, e usa apenas os níveis de potência legalmente permitidos.


Se o testador não receber um código de país, ele funcionará no "modo mundial":

- Nesse modo, o testador só usa canais e níveis de potência legalmente permitidos em todos os países. Na faixa de 2,4 GHz, os canais são: 1 a 11.
- O testador não transmitirá sondas nos canais 12, 13 e 14 na faixa de 2.4 GHz.
- O testador não transmitirá na faixa de 5 GHz a menos que detecte pontos de acesso que operam nessa faixa.
- O testador usa a potência mínima de transmissão permitida legalmente em todos os países.

As barras na parte inferior da tela e os ícones nas telas de redes e pontos de acesso indicam o status do código do país:

 Barras verdes: O testador recebeu um código de país de um ou mais pontos de acesso. Todos os códigos de país recebidos são iguais e correspondem à configuração encontrada em **Ferramentas > Definir país**. O testador usa canais e níveis de potência que são legalmente permitidos no país definido.

 Barras brancas: O testador não recebeu nenhum código de país. O testador usa o modo mundial.

 Barras vermelhas: O testador recebeu um código de país que não corresponde ao país definido em **Ferramentas > Definir país**. Para identificar a rede ou ponto de acesso que transmitiu o código, selecione **Redes** ou **Pontos de acesso** e procure as barras vermelhas na coluna **802.11**.

A tela **Detalhes do ponto de acesso** mostra o código de país de 802.11d transmitido pelo ponto de acesso. O Apêndice mostra os países correspondentes aos códigos.

Alterar os limites das cores dos gráficos de barras

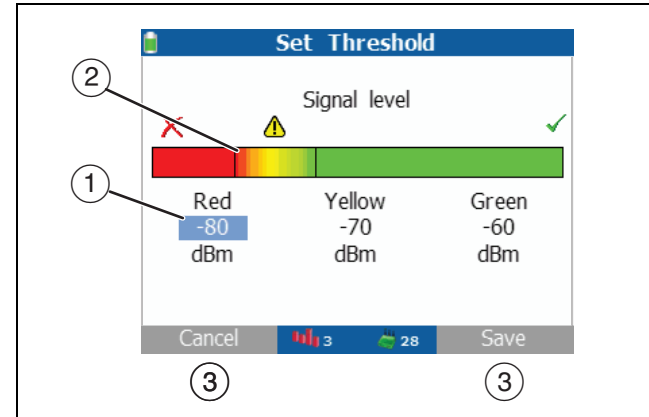
Os gráficos de barra mostram se a força do sinal, o ruído, Proporção Sinal-Ruído (Signal to Noise Ratio - SNR) estão acima ou abaixo dos limites especificados. São representados em vermelho, amarelo ou verde. Você pode alterar os limites para que atendam às exigências da sua rede.

Para alterar limites

- 1 Selecione **Ferramentas**.
- 2 Selecione **Limites / Configurações de Autoteste**.
- 3 Selecione um item. A Figura 12 mostra como mudar os limites das cores.

Obs.:

No AutoTest, os resultados em verde ou melhor aprovam, os que estão em vermelho ou abaixo são retidos, e os que estão entre vermelho ou verde emitem um alerta.



ffy05.eps




Figura 12. Mudança dos limites das cores de um gráfico de barras


- ① Use para selecionar uma cor. Use para aumentar ou diminuir o valor medido da cor.
- ② As linhas mostram em que ponto do gráfico de barras o valor se encontra.
- ③ Para salvar essas definições, pressione **Salvar**. Para sair da tela sem salvar as definições, pressione **Cancelar**.


Atribuir status de autorização a pontos de acesso

Ao definir o status de autorização a cada ponto de acesso, pode-se ver rapidamente se o ponto de acesso em questão é autorizado a fazer parte da rede. Os pontos de acesso apresentam **Desconhecido** (?) na coluna da lista de controle de acesso (ACL) até que o status seja alterado. Você pode selecionar um ponto de acesso de cada vez e alterar o seu status. Você também pode selecionar **Definir todos os pontos de acesso para Autorizados** e trabalhar de trás para frente identificando cada ponto de acesso que não terá o status de autorização.


Para atribuir um status de autorização a um ponto de acesso


- 1 Selecione **Pontos de acesso**.
- 2 Se um ponto de acesso tiver mais de um endereço MAC e você quiser atribuir diferentes status de autorização aos diversos MACs, selecione o ponto de acesso.
- 3 Realce o ponto de acesso desejado e pressione  **ACL**.
- 4 Realce um status na tela **Status de autorização**, pressione  e, em seguida, .


 **Dispositivo não autorizado:** O ponto de acesso não tem um status de autorização.



 **Dispositivo autorizado:** O ponto de acesso está autorizado a se conectar à rede.



 **Dispositivo Vizinho:** Pontos de acesso descobertos que são propriedade de uma empresa vizinha ou indivíduo.



 **Dispositivo desconhecido:** O ponto de acesso não foi descoberto anteriormente ou o status de autorização não foi definido para refletir o relacionamento com sua rede.

 **Dispositivo sinalizado:** Este símbolo pode ser usado para indicar pontos de acesso que você deseja monitorar. Por exemplo, se achar que determinado ponto de acesso está fora do controle, pode marcá-lo até saber mais a seu respeito.


  **Definir todos os pontos de acesso para Autorizado:** Define todos os pontos de acesso no testador para Autorizado.

  **Definir todas as Séries de ponto de acesso para Autorizado:** Permite definir uma série de ponto de acesso para autorizado com base no endereço BSSID/MAC ou prefixo MAC do fornecedor.

  **Definir todas as Séries de ponto de acesso para Não autorizado:** Permite definir uma série de ponto de acesso para Não autorizado com base em **um prefixo BSSID/MAC** ou **prefixo MAC do fornecedor**. Utilize esta opção quando precisar excluir (cancelar autorização de) um fornecedor específico ou BSSID da rede.

As opções para definir uma série de pontos de acesso economiza o tempo de configuração e oferece visibilidade rápida nas questões de segurança ou políticas em potencial. Por exemplo, se o equipamento de um fornecedor específico não tiver permissão por sua política de rede, use o prefixo MAC do fornecedor para definir a ACL para não  autorizado ou  sinalizado. Quando detectados, os pontos de acesso serão indicados como tal.

Para definir um status de autorização padrão

- 1 Selecione **Ferramentas**.
- 2 Selecione **Definir o padrão de autorização do dispositivo (ACL)**
- 3 Escolha **Definir status para "Desconhecido"** ou **Definir status para "Autorizado"** e pressione  ou **Salvar**.

Obs.:




Se um ponto de acesso não estiver transmitindo mas você souber o seu endereço MAC, use o AirCheck Manager para atribuir um status de autorização ao ponto de acesso. Salve o status em um perfil no computador, depois transfira o perfil para o testador.

Descobrir redes e pontos de acesso

Obs.:

*Por padrão, o testador detecta sinais sem fio nas faixas de frequência de 2,4 GHz (b/g/n) e 5 GHz (a/n/ac). Para mudar esta definição, selecione **Ferramentas** e, em seguida, **Gerenciar configurações de 802.11**.*

Para efetuar a descoberta de redes ou pontos de acesso

- 1 Na tela inicial, selecione **Redes** ou **Pontos de acesso**. O testador mostra a lista de **Redes** ou **Pontos de acesso** (Figuras 13 e 14).
- 2 Para ver detalhes sobre um ponto de acesso (Figura 15), use   para realçar o ponto de acesso e, em seguida, pressione .



Obs.:s

*Um SSID estará em texto preto se a rede (ou ponto de acesso) estiver no alcance. Um texto de SSIDs ficará cinza para indicar que uma rede (ou um ponto de acesso) não foi ouvida recentemente ou está agora fora do alcance (se **Deixar pontos de acesso inaudíveis** estiver ativado). Um texto de SSIDs fica roxo para indicar que existe uma nota à direita com informações adicionais sobre o status da rede (ou ponto de acesso).*

Procurando um dispositivo específico



É possível procurar um ponto de acesso específico na lista de pontos de acesso descobertos.

Para procurar um ponto de acesso específico

- 1 Na tela inicial, realce o ícone **Pontos de acesso** e pressione  **Pesquisar**.
- 2 Realce e selecione **BSSID/MAC**, **MAC de fornecedor** ou **Nome**
- 3 Insira as formações e pressione  **Pesquisar**.

Se o dispositivo de pesquisa estiver dentro da área de alcance descoberta, o dispositivo será realçado na tela de Pontos de acesso.

Para procurar um cliente específico

- 1 Na tela inicial, realce o ícone **Clientes** e pressione  **Pesquisar**.
- 2 Realce e selecione **BSSID/MAC** ou **fornecedor MAC**.
- 3 Insira as formações e pressione  **Pesquisar**.

Se o dispositivo de pesquisa foi descoberto, o dispositivo será realçado na tela de Pontos de acesso.






| Networks (SSIDs) | | | | | | | | |
|------------------|-----|----------|------|------|----|----------|--------|------------------------------|
| Time | ACL | Signal | SNR | Lock | Ch | SSID | 802.11 | Notes |
| 22:29:30 | ✓ | [Signal] | 45 | 🔒 | 1 | [Hidden] | b g | Possible Interference - over |
| 22:29:30 | ✓ | [Signal] | 28 | 🔒 | 1 | [Hidden] | b g | Possible Interference - over |
| 22:29:30 | ✓ | [Signal] | 30 | 🔒 | 1 | [Hidden] | b g | Possible Interference - over |
| 22:29:30 | ✓ | [Signal] | 49 | 🔒 | 1 | [Hidden] | b g | Possible Interference - over |
| 22:29:29 | ✓ | [Signal] | -128 | 🔒 | 1 | [Hidden] | b g | |
| 22:29:30 | ✓ | [Signal] | 30 | 🔒 | 1 | 2WIRE127 | b g | Possible Interference - over |
| 22:29:30 | ✓ | [Signal] | 29 | 🔒 | 1 | 2WIRE484 | b g | |
| 22:29:30 | ✓ | [Signal] | 29 | 🔒 | 1 | 2WIRE953 | b g | |






10 (1) (2) (3) (4) (5) (6) (7) (8) (9)

11 Connect* 12 2 13 27 14 Legend

ffy03.eps

Figura 13. Lista Redes (SSIDs)

- ① : O horário em que o testador detectou a rede pela primeira vez. Para ver as redes que fazem parte do intervalo conforme você navega por uma área, classifique a lista em ordem decrescente na coluna de carimbo de hora.
- Pressione  e, em seguida, navegue por uma área. As redes que fizerem parte do intervalo serão adicionadas ao topo da lista. As redes que ficam fora do intervalo ficarão cinza se Deixar ptos acesso n aud. em cinza (Deixar pontos de acesso não audíveis em cinza) estiver habilitado.
- ② **ACL**: O status de autorização do ponto de acesso. O status padrão é  **Desconhecido**, mas pode ser alterado para  **Autorizado**. Altere o status de cada ponto de acesso para mostrar como ele está relacionado à sua rede. Consulte a página 38.
- (...): Todos os pontos de acesso na rede não têm o mesmo status de autorização.
- ③ : A capacidade máxima do sinal de todos os pontos de acesso de uma rede **SSID**. Você pode mudar os limites das cores dos gráficos de barras. Consulte a página 37.

- ④ **SNR**: Siglas em inglês para Razão sinal-ruído é a medida da capacidade do sinal relativa ao ruído; uma indicação da qualidade do sinal para uma conexão de cliente confiável. A razão é medida em decibéis (dB). Os mesmos limites são utilizados tanto aqui quanto no AutoTest, e são ajustados na tela **Ferramentas > Limites / Configurações de AutoTest**.
- ⑤ : O status de segurança da rede:
-  Cadeado vermelho aberto: A segurança não está habilitada na rede.
 -  Cadeado amarelo fechado: Um ou mais pontos de acesso usam WEP ou protocolo de segurança LEAP da Cisco. Estes protocolos são menos seguros que outros.
 -  Cadeado verde fechado: Todos os pontos de acesso utilizam protocolo de segurança que são mais seguros que o WEP, como por exemplo, WPA ou WPA2.
- (...): Todos os pontos de acesso na rede não usam o mesmo tipo de segurança. Por exemplo, um utiliza o WEP e outro usa o WPA.
- ⑥ : O número de pontos de acesso que o testador detecta em seu local.
- ⑦ **SSID**: Service Set Identifier. O nome da rede sem fio.

As redes em que o testador não captou nenhuma atividade recentemente aparecem em cinza, se a opção **Acinzentar pontos de acesso inaudíveis** estiver ativada (veja a página 33).



: A rede possui dispositivos ad hoc. Dispositivos ad-hoc comunicam-se diretamente com outros dispositivos, sem passar por um ponto de acesso que faz parte da rede. Os dispositivos ad hoc podem fornecer aos hackers acesso aos dados transmitidos na rede. (Algumas políticas de TI para redes permitem dispositivos ad hoc).

[Oculto]: A rede não transmite o seu SSID.

Se um SSID aparece entre colchetes, o testador encontrou o SSID oculto em pacotes de outros clientes sem fio. No AirCheck Manager, esses SSIDs aparecem sem colchetes.

- ⑧ **802.11:** Os padrões 802.11 que os pontos de acesso usam na rede:



802.11a: Usa a banda 5 GHz.



802.11b: Usa a banda 2.4 GHz.



802.11g: Usa a banda 2.4 GHz.



802.11n: Pode ser usado nas bandas 2.4 GHz ou 5 GHz.



802.11ac: Usa a banda 5 GHz.




Barras vermelhas: O testador recebeu um código de país 802.11d do ponto de acesso. Esse país não corresponde ao definido no testador, em **Ferramentas > Definir país**.




Um ou mais pontos de acesso utilizam um canal vinculado. Os pontos de acesso que utilizam o padrão 802.11n podem vincular um canal a um canal de extensão acima de (n 40+) ou abaixo de (n 40-) para compor um canal de 40 MHz. Esse canal mais largo fornece à rede um throughput mais alto.


(...): Todos os pontos de acesso na rede não usam o mesmo padrão 802.11.




Notas: Pressione  para percorrer o campo de notas. O testador adiciona notas automaticamente. Consulte a página 51. As redes que contêm notas são roxas.



(...): A rede contém diversas notas. Para ver todas as anotações, realce a rede e pressione duas vezes  para acessar a tela **Detalhes do ponto de acesso**.











: **Classif 1**, seqüências decrescentes e crescentes


: **Classif 2**, seqüências decrescentes e crescentes

Obs.:


A seta maior  indica **Classif 1**. A seta menor  indica **Classif 2**.


Para colocar a lista em ordem crescente ou decrescente, use  e  para realçar o título da coluna e, em seguida, pressione  ou  **Classif 1**. Por exemplo, para encontrar rapidamente o ponto de acesso que apresenta o sinal mais forte, realce  na parte superior da coluna, depois pressione  ou  **Classif 1**. Isso leva o ponto de acesso com o sinal mais forte para o topo da lista.

Para classificar em uma seqüência secundária, realce um cabeçalho de coluna diferente, depois pressione  **Classif 2**.

- ⑪ Pressione  **Conectar** para conectar-se à rede realçada. Consulte a página 60.

O botão de conexão é mostrado como "**Conectar***" caso o testador não consiga se conectar à rede realçada. Consulte a página 60.




- ⑫  **40** O canal que o testador está monitorando no momento. A cor das barras mostra o status do código do país de um domínio normativo. Veja a "Operação em 802.11d" na página 36.

- ⑬  **23** O número de pontos de acesso que o testador detecta em seu local. Esse número não inclui pontos de acesso virtuais caso **Agrupar pontos de acesso virtuais** esteja selecionado. Consulte a página 32.

Até 500 pontos de acesso podem ser armazenados no banco de dados de pontos de acesso do testador. Quando o ícone do ponto de acesso fica amarelo, indica que um número igual ou maior que 400 pontos de acesso foram descobertos.

Quando o ícone fica vermelho, indica que 500 pontos de acesso ou mais foram descobertos e o banco de dados de pontos de acesso está cheio. Qualquer ponto de acesso novo encontrado não será incluído na lista.






- ⑭ Para ver as descrições dos ícones na tela **Redes**, pressione  **Legenda**.


Para ver detalhes sobre os pontos de acesso em uma rede, use  e  para realçar uma rede, depois pressione  Consulte a Figura 14.

| Time | ACL | Signal | SNR | Name/MAC | SSID | Lock | 802.11 |
|---------|-----|--------|-----|---------------|----------------|-------|--------|
| 2:19:55 | ✓ | 1/149 | 23 | 000b85-66795e | REWIFI3 | 🔒 | (...) |
| 2:19:55 | ✓ | 11/161 | 30 | 000b85-667d91 | REWIFI3 | 🔒 | (...) |
| 2:19:55 | | 11 | 42 | 000ce5-53b6b7 | morganmotorola | 🔒 | (...) |
| 2:19:56 | ? | 11/48 | 40 | 000ce6-09992f | 7 SSIDs | (...) | (...) |
| 2:19:56 | ✓ | 11/48 | 34 | 000ce6-09a522 | 7 SSIDs | (...) | (...) |
| 2:19:56 | ? | 11/48 | 11 | 000ce6-09a538 | 6 SSIDs | (...) | (...) |
| 2:19:55 | ✓ | 6 | 36 | 000f66-9da116 | 8021xTest | 🔒 | (...) |
| 2:20:01 | ✓ | 6 | 23 | 001310-dbd4a3 | kris_linksys | 🔒 | (...) |

1: Time column
 2: ACL column
 3: Signal strength column
 4: SNR column
 5: SNR value
 6: Name/MAC column
 7: SSID column
 8: Lock icon
 9: 802.11 column
 10: List item expansion icon
 11: Arrow pointing to the first row
 12: Connect* button
 13: Signal strength indicator (124)
 14: Wi-Fi icon (25)
 15: ACL label

Figura 14. Lista de pontos de acesso

- ① : O horário em que o testador escutou o ponto de acesso pela primeira vez. Para ver os pontos de acesso que entram na faixa de alcance conforme você se movimenta em uma área, coloque a lista em ordem decrescente, na coluna do registro de hora.
- Pressione  e, em seguida, navegue por uma área. Os pontos de acesso que entram na faixa de alcance são acrescentados ao começo da lista. Os pontos de acesso que ficam fora do intervalo ficarão cinza se **Deixar ptos acesso n aud. em cinza (Deixar pontos de acesso não audíveis em cinza)** estiver habilitado.
- ② **ACL**: O status de autorização do ponto de acesso. O status padrão é  **Desconhecido**, mas pode ser alterado para  **Autorizado** para se adequar às suas necessidades. Altere o status de cada ponto de acesso para mostrar como ele está relacionado à sua rede. Consulte a página 38.
- (...): Pontos de acesso virtuais ou MACs de um mesmo ponto de acesso têm status de autorização diferentes definidos. Geralmente, eles são definidos com o mesmo status de autorização.
- ③ : O canal usado pelo ponto de acesso.
- ④ SNR: Siglas em inglês para Razão sinal-ruído é uma medida da intensidade do sinal relativa ao ruído. A razão é medida em decibéis (dB).

- ⑤ : A intensidade do sinal. Para PAs múltiplos, esta coluna mostra a capacidade do sinal mais forte. Você pode mudar os limites das cores dos gráficos de barras. Consulte a página 37.
- ⑥ **Nome/MAC**: O nome ou endereço MAC do ponto de acesso. O endereço começa com um prefixo correspondente ao nome abreviado do fornecedor, se houver prefixo. Veja “oui_abbr.txt” na página 81.
- *: O ponto de acesso transmite mais de um endereço MAC (BSSID). Para ver os endereços MAC, selecione o ponto de acesso. Veja **“Agrupar pontos de acesso virtuais”** na página 33.
- Os pontos de acesso em que o testador não captou nenhuma atividade recentemente aparecem em cinza, se a opção **Acinzentar pontos de acesso inaudíveis** estiver ativada (veja a página 33).
- ⑦ **SSID**: Service Set Identifier. O nome da rede sem fio.
- Se o ponto de acesso é compatível com mais de um SSID, selecione o ponto de acesso para visualizar os SSIDs. Veja **“Agrupar pontos de acesso virtuais”** na página 33.
- Se você chegou a esta tela a partir da tela **Redes**, ela terá o SSID no topo.
- As redes em que o testador não captou nenhuma atividade recentemente aparecem em cinza, se a opção **Acinzentar pontos de acesso inaudíveis** estiver ativada (veja a página 33).



: As redes Ad hoc são criadas quando os clientes se comunicam diretamente e não através de um ponto de acesso. Esse tipo de rede pode ser considerada um risco de segurança facilitando o acesso não autorizado a dados na rede.

[Oculto]: A rede não transmite o seu SSID.

Se um SSID aparece entre colchetes, o testador encontrou o SSID oculto em pacotes de outros clientes sem fio. No AirCheck Manager, esses SSIDs aparecem sem colchetes.

8 : O status de segurança do ponto de acesso:



Cadeado vermelho aberto: A segurança do ponto de acesso não está habilitada na rede.



Cadeado amarelo fechado: O ponto de acesso utiliza o protocolo de segurança WEP.



Cadeado verde fechado: O ponto de acesso usa um protocolo de segurança mais seguro que o WEP, como, por exemplo, o WPA ou o WPA2.



: Um dispositivo de cliente que funcione em modo ad hoc está incluído na lista de pontos de acesso. Os outros dispositivos de cliente conectados à rede ad hoc estarão na lista na guia "clientes".

(...): Nem todos os pontos de acesso na rede usam o mesmo tipo de segurança. Por exemplo, um utiliza o WEP e outro usa o WPA.

9 **802.11:** Os padrões 802.11 que os pontos de acesso da rede utilizam:



802.11a: Usa a banda de 5 GHz.



802.11b: Usa a banda de 2,4 GHz.



802.11g: Usa a banda de 2,4 GHz.



802.11n: Pode ser usado nas bandas de 2,4 GHz ou 5 GHz.



802.11ac: Usa a banda 5 GHz.




Barras vermelhas: O testador recebeu um código de país 802.11d do ponto de acesso. Esse país não corresponde ao definido no testador em **Ferramentas > Definir país** no testador.




Os pontos de acesso que usam o padrão 802.11n podem vincular um canal a um canal de extensão acima (**n40+**) ou abaixo dele (**n40-**), formando um único canal de 40 MHz. Esse canal mais largo fornece à rede um throughput mais alto.


(...): Nem todos os pontos de acesso da rede utilizam o mesmo padrão 802.11.








10


Notas: Pressione  para percorrer o campo de notas. O testador adiciona notas automaticamente. Consulte a página 51. Os pontos de acesso que contêm anotações são indicados em roxo.

(...): O ponto de acesso possui várias anotações. Para ver todas as anotações, acesse a tela **Detalhes do ponto de acesso**.

⑪ : **Classif 1**, seqüências decrescentes e crescentes

: **Classif 2**, seqüências decrescentes e crescentes


Para colocar a lista em ordem crescente ou decrescente, use  e  para realçar o título da coluna e, em seguida, pressione  ou  **Classif 1**. Por exemplo, para encontrar rapidamente o ponto de acesso que apresenta o sinal mais forte, realce , na parte superior da coluna, depois pressione  ou  **Classif 1**. Isso leva o ponto de acesso com o sinal mais forte para o topo da lista.


Para classificar em uma seqüência secundária, realce um cabeçalho de coluna diferente, depois pressione  **Classif 2**.

⑫ Pressione  **Conectar** para efetuar a conexão ao ponto de acesso realçado. Consulte a página 60.

O botão de conexão aparece como **“Conectar*”**, se o testador não conseguiu se conectar ao ponto de acesso realçado. Consulte a página 60.


Para estabelecer conexão a um ponto de acesso protegido, o testador precisa ter um perfil que tenha credenciais de segurança. Consulte a página 26.


⑬  O canal que o testador está monitorando no momento. A cor das barras mostra o status do código do país de um domínio normativo. Consulte “Operação em 802.11d” na página 36.

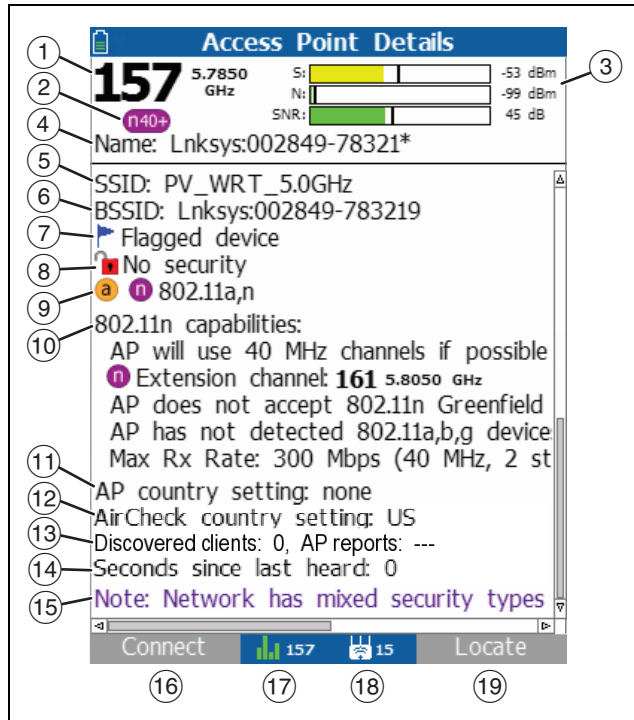
⑭  O número de pontos de acesso encontrados pelo testador no local. Esse número não inclui pontos de acesso virtuais caso **Agrupar pontos de acesso virtuais** esteja selecionado. Consulte a página 33.

Até 500 pontos de acesso podem ser armazenados no banco de dados de pontos de acesso do testador. Quando o ícone do ponto de acesso fica amarelo, indica que um número igual ou maior que 400 pontos de acesso foram descobertos.

Quando o ícone fica vermelho, indica que 500 pontos de acesso ou mais foram descobertos e o banco de dados de pontos de acesso está cheio. Qualquer ponto de acesso novo encontrado não será incluído na lista.

⑮ Pressione  **ACL** para mudar o status de autorização do ponto de acesso realçado. Consulte a página 38.

Para ver os detalhes de um ponto de acesso, realce-o e pressione . Veja a Figura 15.






ffiy06.eps

Figura 15. Tela de detalhes do ponto de acesso

- ① O canal e a frequência do ponto de acesso. O número é vermelho quando o canal é ilegal no país selecionado em **Ferramentas > Definir país**.
 - ② **n40+** **n40-**: O canal principal (①) é vinculado a um canal de extensão acima (**n40+**) ou abaixo (**n40-**) para formar um canal de 40 MHz. Esse canal mais largo fornece à rede um throughput mais alto. O canal de extensão aparece abaixo de **Recursos de 802.11n** (⑩).
 - ③ Intensidade do sinal (**S**), intensidade do ruído (**N**) e razão sinal-ruído (**SNR**). Você pode mudar os limites das cores dos gráficos de barras. As barras são cinzas quando o testador não consegue escutar o ponto de acesso. Consulte a página 37.
 - ④ **Nome**: O nome do ponto de acesso, se houver um nome nos quadros de beacon e de respostas de sondas.
 - ⑤ **SSID**: Service Set Identifier. O nome da rede que usa os pontos de acesso.
 - ⑥ **BSSID**: Basic Service Set Identifier. O endereço MAC do ponto de acesso.
- Obs.:*
- Alguns pontos de acesso têm endereços MAC diferentes para interfaces cabeadas e sem fio.*
- ⑦ Status de autorização do ponto de acesso.
 - ⑧ Status de segurança do ponto de acesso.

- 9 Os padrões 802.11 que podem ser usados pelo ponto de acesso.
- 10 **Recursos 802.11n:** Anotações para pontos de acesso que podem usar o padrão 802.11n. Veja a Tabela 4 na página 52.
- 11 **Configuração do país do ponto de acesso:** código do país que o ponto de acesso transmite. Se a **Configuração de país para PA** não corresponder à **Configuração de país para o AirCheck**, o ponto de acesso terá barras vermelhas na coluna **802.11**. Veja a “Operação em 802.11d” na página 36. O Apêndice mostra os países correspondentes aos códigos.
- 12 **Configuração do país do AirCheck:** O código do país selecionado em **Ferramentas > Definir país**. Veja a “Operação em 802.11d” na página 36. O Apêndice mostra os países correspondentes aos códigos.
- 13 **Clientes descobertos: XX, AP relatórios: XX:** O número de clientes que, no momento, estão descobertos e a quantidade de clientes relatada pelo ponto de acesso. “--” aparece se o ponto de acesso não informa o número de clientes que possui.
- 14 **Segundos desde a última escuta:** O número de segundos desde o testador detectou o ponto de acesso.
- 15 Anotações para o ponto de acesso. Veja a Tabela 3 na página 51.

- 16 Pressione  **Conectar** para efetuar a conexão ao ponto de acesso. Consulte a página 60.
- 17  O canal que o testador está monitorando no momento. A cor das barras mostra o status do código do país de um domínio normativo. Consulte “Operação em 802.11d” na página 36.
- 18  O número de pontos de acesso que o testador detecta em seu local. Esse número não inclui pontos de acesso virtuais caso **Agrupar pontos de acesso virtuais** esteja selecionado. Consulte a página 32.

Até 500 pontos de acesso podem ser armazenados no banco de dados de pontos de acesso do testador. Quando o ícone do ponto de acesso fica amarelo, indica que um número igual ou maior que 400 pontos de acesso foram descobertos.

Quando o ícone fica vermelho, indica que 500 pontos de acesso ou mais foram descobertos e o banco de dados de pontos de acesso está cheio. Qualquer ponto de acesso novo encontrado não será incluído na lista.

- 19 Pressione  **Localizar** para localizar o ponto de acesso. Consulte a página 71.

Anotações para redes e pontos de acesso

As tabelas 3 e 4 explicam as anotações que o testador permite acrescentar às redes e pontos de acesso.

Tabela 3. Anotações para redes e pontos de acesso

| | |
|---|---|
| <p>Rede ad-hoc em operação</p> | <p>Este SSID é de uma rede ad-hoc. A operação no modo ad hoc faz com que os dispositivos sem fio (clientes) dentro do alcance do outro descubram e se comuniquem entre si sem a utilização de um ponto de acesso. As redes ad hoc representam um risco de segurança. Eles normalmente possuem pouca ou nenhuma proteção, e criam uma "ponte" para usuários não autorizados acessarem dados corporativos. Algumas regras de redes de TI permitem redes ad hoc, por exemplo, usuários temporários, como o compartilhamento móvel de um arquivo de um grupo pequeno.</p> |
| <p>Canal ilegal para esse país</p> | <p>O ponto de acesso usa um canal que é ilegal no país selecionado em Ferramentas > Definir país. Verifique se o país selecionado em Ferramentas > Definir país está correto.</p> |
| <p>Possível interferência – sobreposição aos canais padrão</p> | <p>O ponto de acesso usa um canal na faixa de 2,4 GHz que pode se sobrepor aos canais adjacentes. Isso pode produzir interferência nos canais adjacentes.</p> <p style="text-align: center;"><i>Obs.:</i></p> <p style="text-align: center;"><i>Nos EUA, os canais que não se sobrepõem entre si são: 1, 6 e 11.</i></p> |
| <p>A rede misturou os tipos de segurança</p> | <p>Todos os pontos de acesso para este SSID não utilizam o mesmo tipo de segurança.</p> |

Tabela 3. Anotações para redes e pontos de acesso (continuação)

| | |
|---|--|
| Não é recomendado 802.11n de 40 MHz em 2,4 GHz | Não se deve vincular canais na faixa de 2,4 GHz porque essa faixa só tem três canais que não se sobrepõem. Se você vincular dois canais, apenas um canal estará disponível para outros dispositivos. |
| Código inesperado de país para o ponto de acesso | O código de país do ponto de acesso não corresponde ao país selecionado no testador, em Ferramentass > Definir país. |

Tabela 4. Recursos de 802.11n (na tela de detalhes de pontos de acesso)

| | |
|--|--|
| O PA usará can. de 40 MHz se possível | <p>Em certas situações, o ponto de acesso não usa canais de 40 MHz. Exemplos:</p> <ul style="list-style-type: none">• O ponto de acesso captou outros pontos de acesso ou clientes que usam canais que se sobrepõem aos canais de 40 MHz.• Um cliente que usa o ponto de acesso captou esses pontos de acesso ou clientes e informou o ponto de acesso para não usar canais de 40 MHz. <p>Consulte o padrão 802.11n para obter informações sobre todas as situações em que os pontos de acesso não usam canais de 40 MHz.</p> |
| O PA está def p/ can 20 MHz | O usuário definiu o ponto de acesso para usar apenas canais de 20 MHz. |
| O PA adm pac Greenfield 802.11n | O ponto de acesso pode aumentar a velocidade, se usar pacotes Greenfield. |

Tabela 4. Recursos de 802.11n (na tela de detalhes de pontos de acesso) (continuação)

| | |
|---|--|
| O PA não adm pac Greenfield 802.11n | O ponto de acesso não aceita pacotes Greenfield 802.11n. O usuário definiu o ponto de acesso para que nunca use pacotes Greenfield; ou, o ponto de acesso capta clientes a, b ou g e não opera no modo Greenfield 802.11n. |
| PA detectou dispositivos 802.11a,b,g | <p>O ponto de acesso precisa usar proteção para não causar problemas em transmissões a, b ou g. Os procedimentos de proteção diminuem a velocidade da rede 802.11n.</p> <ul style="list-style-type: none"> • O ponto de acesso captou pontos de acesso ou clientes 802.11a, b ou g. • Um cliente que usa o ponto de acesso captou pontos de acesso ou clientes 802.11a, b ou g. |
| PA não detectou dispositivos 802.11a,b,g | O ponto de acesso não precisa usar proteção para evitar problemas nas transmissões a, b ou g. O ponto de acesso pode operar à máxima velocidade. |
| Taxa máx. de Rx | <p>Taxa máxima de recepção de dados do ponto de acesso no momento. A taxa pode mudar conforme o ponto de acesso se ajusta às mudanças no tráfego da comunicação sem fio da área.</p> <ul style="list-style-type: none"> • 20 MHz ou 40 MHz: A largura do canal que é necessária para obter a taxa máxima. • Fluxos X: Número de sequências de dados que o ponto de acesso usa para obter a taxa máxima. • 1/2 GI: O ponto de acesso usa um intervalo de guarda curto (400 ns em vez de 800 ns) para obter a máxima taxa de velocidade. Por exemplo, um intervalo curto de guarda pode aumentar a velocidade de recepção de 270 para 300. |






Se o testador não conseguir descobrir um ponto de acesso

Em certas situações, o testador não descobre determinados pontos de acesso:

- O testador não capta o ponto de acesso porque está muito longe.
- O ponto de acesso não emite beacon quando o testador está escutando o canal usado pelo ponto de acesso.
- O testador não escuta o ponto de acesso porque o sinal não consegue atravessar uma parede ou outro tipo de barreira.
- Há muita interferência no canal usado pelo ponto de acesso. Selecione **Canais** para ver a interferência de fontes não 802.11 no canal.

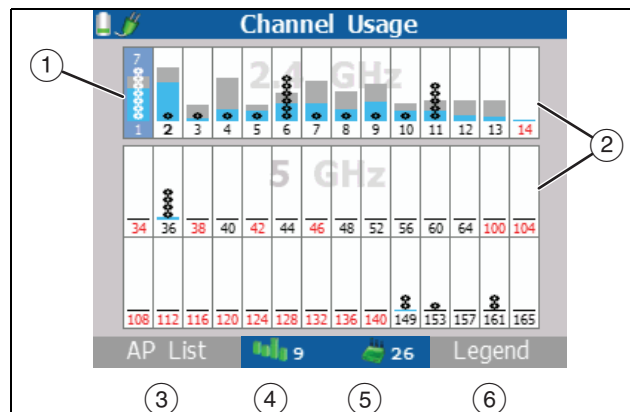
Uso do canal

A função de uso do canal mostra quanto tráfego de comunicação sem fio existe em cada canal. Também mostra as fontes de interferência não 802.11. A Figura 16 mostra a tela **Uso do canal**.

Para ver os detalhes de um canal (Figura 17), use     para realçar um canal, e selecione .

Os círculos nas barras mostram quantos pontos de acesso usam o canal. Ao realçar o canal, o número de

Para selecionar as faixas para esta função, selecione **Ferramentas** e, em seguida, **Gerenciar configurações de 802.11**. Veja a Tabela 2 na página 30.





ffy08.eps


Figura 16. Tela de uso do canal

- 1 Os gráficos de barras mostram quanta capacidade do canal está sendo usada pelos dispositivos 802.11 (em azul) e não 802.11 (em cinza). Quanto mais alta a barra, maior o tráfego no canal.

pontos de acesso ativos é indicado acima do gráfico de barras.


Canais sem pontos de acesso podem indicar uso de 802.11, devido à sobreposição de pontos de acesso nos canais adjacentes.

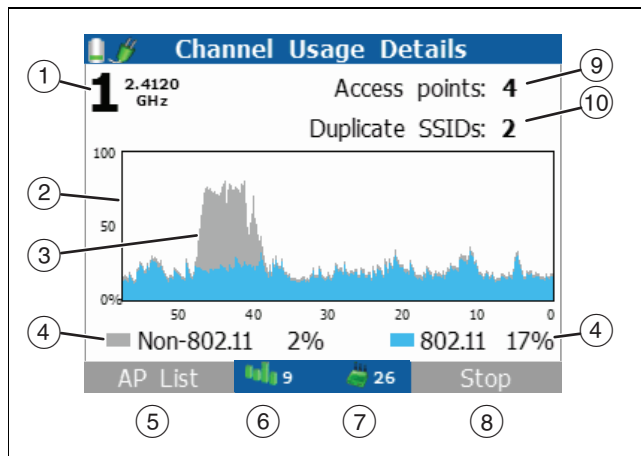
- ② Por padrão, o testador mostra os canais nas faixas de 2,4 GHz e 5 GHz. Para ver apenas uma faixa, mude a definição em **Ferramentas > Gerenciar configurações de 802.11**.
- ③ Pressione  **Lista de PAs** para ver os pontos de acesso que usam o canal realçado.
- ④  O canal que o testador está monitorando no momento. A cor das barras mostra o status do código de país de um domínio normativo. Consulte "Operação em 802.11d" na página 36.

- ⑤  O número de pontos de acesso encontrados pelo testador no local. Quando a opção **Agrupar pontos de acesso virtuais** está selecionada, é mostrado o número de pontos de acesso físicos. Consulte a página 32.

Até 500 pontos de acesso podem ser armazenados no banco de dados de pontos de acesso do testador. Quando o ícone do ponto de acesso fica amarelo, indica que um número igual ou maior que 400 pontos de acesso foram descobertos.

Quando o ícone fica vermelho, indica que 500 pontos de acesso ou mais foram descobertos e o banco de dados de pontos de acesso está cheio. Qualquer ponto de acesso novo encontrado não será incluído na lista.


- ⑥ Para ver as descrições dos ícones da tela **Uso do canal**, pressione  **Legenda**.



ffy09.eps

Figura 17. Tela de detalhes do uso do canal

- ① O número e a frequência do canal que está sendo monitorado. O número é vermelho quando o canal é ilegal no país selecionado em **Ferramentas > Definir país**.

Para alterar o canal, pressione .


- ② Gráfico do uso de 802.11 e da interferência não 802.11 do canal selecionado, ao longo do tempo, em minutos. Quanto maior o uso, mais tráfego existe no canal. Canais com muito tráfego podem causar lentidão na rede ou afetar a conectividade


- ③ Interferência, por exemplo, de um forno microondas.

- ④ **Não 802.11, 802.11:** A porcentagem de sinais no canal que não provém de dispositivos 802.11 (em cinza) e que provém de dispositivos 802.11 (em azul).

O ruído não-802.11 pode ser gerado a partir dos fornos de microondas, telefones sem fio, dispositivos de Bluetooth®, detectores de movimento, câmeras sem fio e outros dispositivos sem fio. Esse ruído pode interferir nas conexões ou no desempenho da WLAN.


- ⑤ Pressione **F1** **Lista de PAs** para ver os pontos de acesso que usam o canal. Veja a Figura 14.

- ⑥  **40** O canal usado pelo ponto de acesso. A cor das barras mostra o status do código do país de um domínio normativo. As barras são vermelhas quando o testador recebe diferentes códigos de país de dois ou mais pontos de acesso. Veja a “Operação em 802.11d” na página 36.

- 7  23 O número de pontos de acesso que o testador detecta em seu local. Quando a opção **Agrupar pontos de acesso virtuais** está selecionada, é mostrado o número de pontos de acesso físicos. Consulte a página 33.

Até 500 pontos de acesso podem ser armazenados no banco de dados de pontos de acesso do testador. Quando o ícone do ponto de acesso fica amarelo, indica que um número igual ou maior que 400 pontos de acesso foram descobertos.

Quando o ícone fica vermelho, indica que 500 pontos de acesso ou mais foram descobertos e o banco de dados de pontos de acesso está cheio. Qualquer ponto de acesso novo encontrado não será incluído na lista.

- 8 Pressione  **Clientes** para visualizar detalhes do cliente.
- 9 **Pontos de acesso:** O número de pontos de acesso que usam o canal. Quando a opção **Agrupar pontos de acesso virtuais** está selecionada, é mostrado o número de pontos de acesso físicos. Consulte a página 33.
- 10 **SSIDs duplicados:** O número de pontos de acesso na mesma área que usam o mesmo canal e a mesma rede. Isso pode constituir um problema, porque os pontos de acesso interferem uns nos outros.

Verificar a conectividade

Use os testes de conectividade para verificar estas funções de redes sem fio:

- Conexão dos clientes à rede.
- Acesso dos clientes aos serviços da rede (ex.: DHCP, DNS e roteadores).
- Comunicação dos clientes com outros dispositivos dentro de um intervalo de tempo razoável.
- Faixa de alcance satisfatória para conexão a clientes.

Os testes também medem parâmetros de desempenho que indicam se há algum problema na rede.

Conectar a uma rede ou ponto de acesso

O testador pode se conectar a uma rede (SSID) ou a um ponto de acesso específico (BSSID) para garantir que a rede ou o ponto de acesso esteja disponível para clientes em fio.

Você também pode usar o testador para estabelecer conexão a uma rede protegida e verificar se as credenciais de segurança estão corretas.

O testador mostra as etapas do procedimento de conexão e um registro dos eventos ocorridos (Figuras 18 e 19).

O botão de conexão aparece como **"Conectar*"**, se o testador não conseguir se conectar à rede ou ao ponto de acesso realçado. Isso ocorre porque a rede usa credenciais de segurança que não estão incluídas no perfil carregado.

Inserir credenciais de segurança utilizando "Conectar"


O testador precisa ter as credenciais de segurança corretas para poder se conectar a redes protegidas. As redes protegidas são indicadas na coluna de segurança por um cadeado amarelo fechado (🔒).



Para inserir credenciais de segurança, utilize o botão do AirCheck **Conectar*** para acessar as telas de configuração de credenciais de segurança. Você também pode utilizar o AirCheck Manager para fazer um perfil que inclua credenciais de segurança. Caso esteja utilizando o AirCheck Manager, é necessário transferir o perfil ao testador e carregá-lo. Consulte a página 26.

Para inserir credenciais de segurança:

Obs.:

*Você também pode acrescentar um SSID e definir suas credenciais de segurança indo a **Ferramentas > Gerenciar Perfis / senhas de rede > Editar redes > Adicionar.***

- 1 Da tela de Redes ou Pontos de Acesso, realce um ponto de acesso/SSID e selecione o botão **Conectar**. Na tela Canais, selecione **Listas de PA**, e selecione o botão **Conectar**.
- 2 Selecione o botão **Conectar*** . A tela instantânea "Esta rede não está configurada - Configurar agora?" é exibida.

Se **Conectar** não tiver um asterisco, é uma rede aberta ou as credenciais de segurança já foram inseridas.
- 3 Pressione **OK**  para seguir para a próxima tela. A janela de popup "Criando uma nova rede no perfil atual" aparece seguida da tela de Selecionar Autenticação.
- 4 Realce o tipo de criptografia apropriado e pressione **Selecionar**.
- 5 Pressione **Seguinte** . Dependendo do tipo de autenticação selecionado, podem aparecer as telas WEP > Configuração WEP Key, Legado 802.1X > Seleção do Tipo EAP, ou WPA/WPA2 > Configurar Criptografia.

Obs.:

O tipo de criptografia WPA/WPA2 foi selecionado para as etapas 6 a 11. WEP e 802.1X têm telas um pouco diferentes.

- 6 Realce o tipo de criptografia, pressione **Selecionar**, clique em **Seguinte**. Aparece a tela de Seleção de Tipo de EAP.
- 7 Realce o tipo de EAP e pressione **Selecionar**.
- 8 Pressione **Seguinte**. A tela Configurar Nome do Usuário/Senha aparecerá.

Obs.:

*Selecione **Concluído** somente depois de ter terminado de inserir o nome de usuário e senha. Se você selecionar **Concluído** e não tiver terminado de inserir as configurações, a conexão falhará. Você terá que selecionar **Ferramentas > Gerenciar perfis / senhas de rede**, selecionar **Editar redes**, selecionar a rede, e terminar de inserir as configurações de segurança.*

- 9 Pressione **Definir nome do usuário**, insira o nome do usuário no teclado na tela, e pressione **Salvar**.
- 10 Pressione **Definir senha**, insira a senha, e pressione **Salvar**.
- 11 Pressione **Concluído** e aparecerá a tela Conectar à rede. O AirCheck tentará então se conectar à rede e executar uma série de testes.

Obs.:

O AirCheck pode usar somente uma configuração de credenciais de segurança por SSID, mesmo se um SSID tiver vários Pontos de Acesso com configurações de segurança diferentes. Portanto, ao pressionar Conectar (sem asterisco), a conexão pode não funcionar.

Para salvar o perfil com as suas credenciais de segurança

Um perfil é um arquivo que contém as configurações feitas por você para o testador. A maioria das configurações é realizada na tela Ferramentas. Você pode ter vários perfis no testador, mas usa apenas um por vez. Assim que inserir as credenciais de segurança para um SSID (ou vários SSIDs), salve-as em um perfil para evitar a perda dessas configurações quando o testador estiver desligado.


- 1 Na tela inicial, selecione **Ferramentas**, depois selecione **Gerenciar Perfis / senhas de rede**.
- 2 Selecione **Salvar perfil**. O nome do perfil aparece na parte inferior da tela.
- 3 Selecione **Salvar** ou selecione **Editar** e altere o nome do arquivo do perfil.

Para carregar um perfil

1 Na tela inicial, selecione **Ferramentas**, depois selecione **Gerenciar Perfis / senhas de rede**.

2 Selecione **Carregar perfil**, realce o perfil desejado, pressione  e, em seguida,  **Carregar**.

Ou

3 Pressione  **Perfil** na tela inicial e, em seguida, **Carregar perfil**.

Para conectar a uma rede

1 Se a rede é protegida, é necessário carregar um perfil de configuração que contenha as devidas credenciais de segurança. Consulte a página 26.


2 Na tela inicial, selecione **Redes**.

3 Realce a rede na lista de **Redes (SSIDs)**, e pressione  **Conectar**.


Para conectar a um ponto de acesso especificado

1 Se o ponto de acesso é protegido, é necessário usar um perfil de configuração que contenha as devidas credenciais de segurança. Consulte a página 26.

2 Na tela inicial, selecione **Pontos de acesso**.

3 Realce o ponto de acesso na lista **Pontos de acesso** e pressione  **Conectar**.

Para realizar um ping ou um teste de conexão de porta TCP


1 Conecte-se à rede ou ao ponto de acesso e depois pressione  **Iniciar testes**.

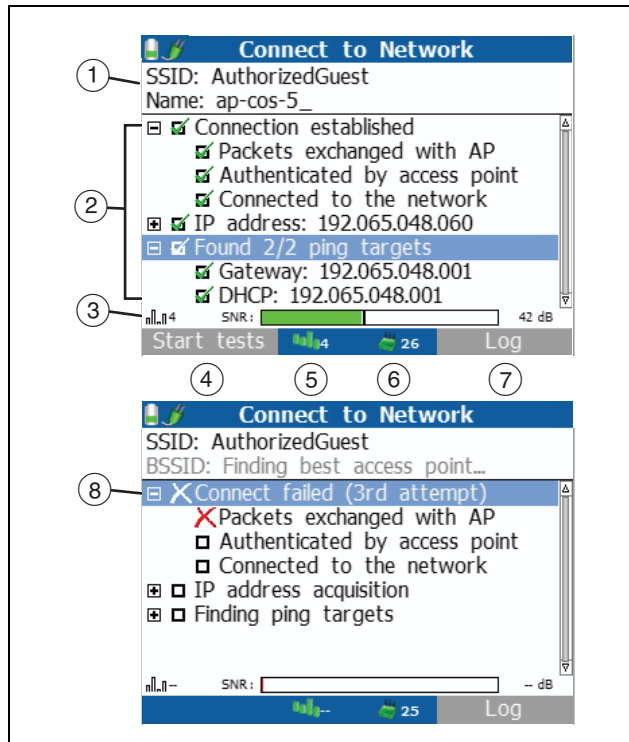
Obs.:

*Os destinos de ping ou teste de conexão de porta TCP podem ser adicionados selecionando-se **Ferramentas > Gerenciar perfis/senhas de rede > Editar destinos de ping > Adicionar**. Você pode adicionar um destino com um endereço IP ou nome de host (URL).*

*Se aparecer um * à direita de **Conectar**, isso indica que a segurança não foi configurado no testador para aquela rede. Pressione **Conectar*** e você será guiado pelas configurações de segurança.*

Revisar resultados de conexão

Após  **Conectar** ser pressionado, o processo para se conectar a uma rede ou um ponto de acesso específico começa e os resultados são apresentados conforme. ficam disponíveis.






ffy04.eps


Figura 18. Tela de conexão

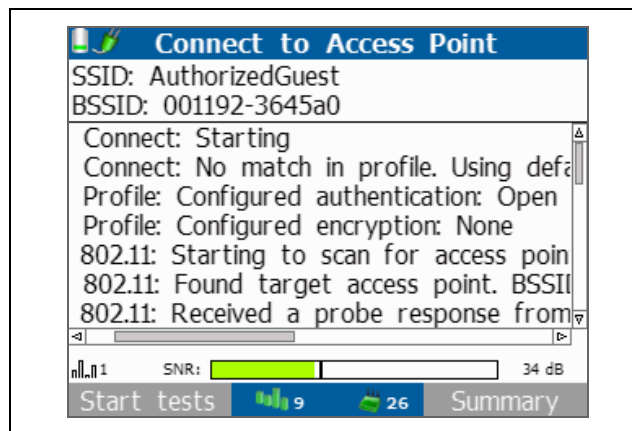
- ① **SSID, BSSID:** O nome da rede e o endereço MAC do ponto de acesso usado pelo testador para a conexão. Ao efetuar a conexão a uma rede, geralmente o testador se conecta por meio do ponto de acesso que tem a razão sinal-ruído mais alta. Se a rede incluir pontos de acesso protegidos e desprotegidos e o testador tiver credenciais de segurança, ele tentará se conectar ao ponto de acesso protegido que apresenta a razão sinal-ruído mais alta. Algumas redes usam um controlador que efetua a conexão ao ponto de acesso que tem o menor volume de tráfego.
- ② Etapas do procedimento de conexão. A lista de cada etapa se fecha quando a etapa é finalizada. Para abrir ou fechar a lista de uma etapa, realce a etapa e pressione **SELECT**.

Como parte do teste de conexão, o testador faz pings dos dispositivos compatíveis para conexão (ex.: servidores DHCP e DNS), executa o teste de conexão de porta TCP (nome de host e endereço IP fornecidos pelo usuário) e de endereços IP incluídos no perfil. O testador mostra uma marca verde (✓) se o dispositivo respondeu, ou um X vermelho (✗) se não houve resposta. Para fazer ping de outros dispositivos, faça um teste de ping. Consulte a página 63.

- ③  **SNR**: O número do canal e a razão sinal-ruído para o ponto de acesso. Você pode mudar os limites das cores dos gráficos de barras. Consulte a página 37.
- ④ Pressione **F1** **Inic testes** para realizar um ping ou teste de conexão de porta TCP que inclui o teste **Alcance de conexão**. Esse teste proporciona visibilidade no alcance da sua conexão e cobertura de ponto de acesso. Consulte a página 64.
- ⑤  **40** O canal usado pelo ponto de acesso. A cor das barras mostra o status do código do país de um domínio normativo. Veja a “Operação em 802.11d” na página 36.
- ⑥  **23** O número de pontos de acesso encontrados pelo testador no local. Quando a opção **Agrupar pontos de acesso virtuais** está selecionada, é mostrado o número de pontos de acesso físicos. Consulte a página 33.
- ⑦ Pressione **F2** **Log** para ver os detalhes do procedimento de conexão. Veja a Figura 19.
- ⑧ Falha na conexão. O testador para o processo de conexão após a terceira tentativa.
O Apêndice apresenta as mensagens exibidas quando a conexão fracassa.

Obs.:

Na tela de registro da conexão, pressione  para rolar e ver os registros de hora de cada entrada do log. Os registros de hora são indicados em segundos.




ffy10.bmp

Figura 19. Log de conexão




Fazer ping de um dispositivo ou servidor de aplicativos

Você pode inserir endereços para fazer ping de outros dispositivos ou servidores de aplicativos (ex.: servidores web). Isso verifica se os outros dispositivos da rede estão acessíveis, e mede o tempo de resposta.

- 1 Conectar a uma rede ou ponto de acesso. Consulte a página 60.
- 2 Quando a conexão estiver estabelecida, pressione  **Iniciar testes.**


Selecione um endereço IP na lista ou digite um novo endereço.

Para inserir um novo endereço

- a. Selecione **Inserir endereço IP.**
- b. Use  para selecionar um valor a ser alterado.
- c. Use  para aumentar ou diminuir o valor realçado.
- d. Para salvar o endereço, pressione  **Concluído.**

Obs.:

Até 10 destinos de ping podem ser configurados no testador.

A tela de ping (Figura 20) mostra os resultados do teste de ping. Para fazer ping de um endereço diferente, pressione  duas vezes, e selecione ou insira um endereço diferente.

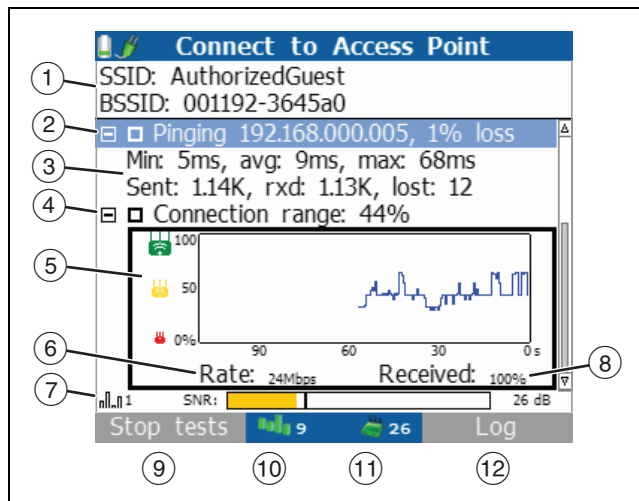






Figura 20. Tela de ping

- ① **SSID, BSSID:** Nome da rede e do ponto de acesso do destino de ping.
- ② **Ping** ou **Conexão (HTTP, FTP):** O endereço IP para o ping ou o destino de conexão da porta TCP e o percentual de respostas não recebidas.

- ③ Os períodos mínimo (**mín**), Médio (**méd**) e máximo (**máx**) para as respostas de ping do dispositivo e o número de pacotes enviados, recebidos e perdidos durante o teste de ping.
- ④ **Alcance de conexão:** O alcance da conexão mostra a probabilidade da melhor conexão possível ao ponto de acesso a partir da sua localização. A melhor conexão possível fornece uma taxa de resposta de 100% e a máxima taxa de dados possível. O valor do alcance de conexão diminuir conforme você se afasta do ponto de acesso. Primeiro, a taxa de dados diminui. Conforme você se afasta do ponto de acesso, a taxa de resposta de ping diminui, assim como a confiabilidade da conexão. Este teste proporciona visibilidade da cobertura de rede de pontos de acesso conectados e o alcance da conexão. Quando conectado a uma rede, o gráfico de resultados do teste indicará quando você faz roaming para um ponto de acesso diferente.
- ⑤ Gráfico do alcance da conexão nos últimos 120 segundos.
- ⑥ **Taxa:** A taxa de transferência de dados.
- ⑦ **SNR:** O número do canal do ponto de acesso e o sinal razão-ruído. Você pode mudar os limites das cores do gráfico de barras. Consulte a página 37.
- ⑧ **Recebido:** Taxa de resposta de ping (número de respostas de ping recebidas dividido pelo número de pings enviados).


- 9) Pressione  **Parar testes** para parar o ping ou testes de conexão de porta TCP.
- 10)  O canal usado pelo ponto de acesso. A cor das barras mostra o status do código do país de um domínio normativo. Consulte “Operação em 802.11d” na página 36.
- 11)  O número de pontos de acesso encontrados pelo testador no local. Quando a opção **Agrupar pontos de acesso virtuais** está selecionada, é mostrado o número de pontos de acesso físicos. Consulte a página 33.
- 12) Pressione  **Log** para ver os detalhes do procedimento de conexão. Veja a Figura 19.

Descobrir clientes

Quando o testador está ligado, ele monitora cada canal dos quadros de solicitação de sonda para descobrir dispositivos clientes. Para visualizar esses clientes, utilize o botão **Clientes** na tela inicial.

Além do endereço MAC do cliente, informações, como os canais usados, taxa de dados, SSIDs sondados, o SSID conectado e o ponto de acesso de um cliente associado são mostrados.


As telas de cliente incluem uma função **Localizar** que ajuda a encontrar clientes. Consulte a página 71.

Quando um cliente associado é realçado no teste. Pressione  **Detalhes do ponto de acesso** para ver os detalhes do Ponto de acesso associados.

Quando você utiliza a função **Clientes** o testador monitora cada canal por mais tempo do que quando você utiliza outras funções. Isso permite que o testador encontre mais clientes em cada canal.

Para descobrir clientes


Na tela inicial, selecione **Clientes**. A Figura 21 mostra a tela **Clientes**.

Para ver mais detalhes sobre um cliente, realce-o e pressione . Veja a Figura 22.


Obs.:

*O testador mostra as informações mais recentes sobre um cliente quando ele transmite dados enquanto o testador monitora o canal que o cliente utiliza. Para obter informações de cliente mais rapidamente, vá para **Ferramentas > Gerenciar configurações de 802.11** e habilite somente uma faixa. Isto diminui o número de canais monitorados pelo testador.*

Para procurar um cliente específico

- 1) Na tela inicial, realce o ícone **Clientes** e pressione  **Pesquisar**.

2 Realce e selecione **BSSID/MAC** ou **fornecedor MAC**.

3 Insira as formações e pressione  **Pesquisar**.

Se o dispositivo de pesquisa foi descoberto, o dispositivo será realçado na tela **Cientes**.

Descobrimdo clientes através de PAs Meru

O testador pode descobrir clientes independente de quantos PAs Meru estão configurados. Se o SSID estiver configurado para uma entrada virtual, ou se a célula virtual estiver desativada, o testador pode se conectar ao PA virtual correto.

Se o PA estiver somente no modo de célula virtual, o testador mostrará um cliente como conectado para todos os PAs virtuais compatíveis com o SSID conectado no canal sendo utilizado por um cliente.

8

| Ch | MAC | SSID | Mbps | Key | AP |
|-------|---------------------|-----------------|-------|-----|---------------|
| 1 -61 | Fluke:02c412-a40017 | [keepout] | 54/1 | 🔒 | cap-fp1-f21 |
| 1 -91 | Apple:041e64-2ba6d9 | [keepout] | 5/1 | 🔒 | cap-fp1-f21 |
| 1 -70 | Intel:00516a-3d4b90 | AuthorizedGuest | 24/24 | 🔓 | cap-fp1-f21 |
| 1 -66 | Intel:0019f0-6eff48 | --- | 48/5 | -- | 001162-8645a0 |
| 1 -88 | Intel:002717-ed0b90 | --- | 6/2 | -- | 001b45-b2cb52 |
| 1 -80 | Fluke:05c017-a40418 | --- | 11/1 | -- | 001152-3645a8 |


1 2 3 4 5 6 7





9 10 11


9 26 Locate



ffy12.eps








Figura 21. Tela Clientes


- ① **Ch**: O canal que o cliente utiliza.
- ② : A intensidade do sinal. Você pode mudar os limites das cores dos gráficos de barras. Consulte a página 37.
- ③ **MAC**: O endereço MAC do cliente. O endereço começa com um prefixo correspondente ao nome abreviado do fornecedor, se houver prefixo. Veja "oui_abbr.txt" na página 81.
- ④ **SSID**: Service Set Identifier. O cliente está conectado a essa rede.
[Oculto]: A rede não transmite o seu SSID.


Se um SSID aparece entre colchetes, o testador encontrou o SSID oculto em pacotes de outros clientes sem fio. No AirCheck Manager, esses SSIDs aparecem sem colchetes.
- ⑤ : As últimas taxas de conexão máxima e mínima do cliente verificadas pelo testador.
- ⑥ : O status de segurança do ponto de acesso:
 -  Cadeado vermelho aberto: A segurança do ponto de acesso não está habilitada na rede.
 -  Cadeado amarelo fechado: O ponto de acesso utiliza o protocolo de segurança WEP.
- ⑨  **23** O número de pontos de acesso que o testador detecta em seu local. Esse número não inclui pontos de

 Cadeado verde fechado: O ponto de acesso usa um protocolo de segurança mais seguro que o WEP, como, por exemplo, o WPA ou o WPA2.

- ⑦ **AP**: O nome ou o BSSID do ponto de acesso que o cliente utiliza para a conexão de rede.
- ⑧ : **Classif 1**, seqüências decrescentes e crescentes
: **Classif 2**, seqüências decrescentes e crescentes

Para colocar a lista em ordem crescente ou decrescente, use  e  para realçar o título da coluna e, em seguida, pressione  ou  **Classif 1**. Por exemplo, para localizar rapidamente o ponto de acesso que tem a maior intensidade de sinal, realce  no topo da coluna e pressione  ou  **Classif 1**. Isso coloca o cliente com sinal de maior intensidade no início da lista.

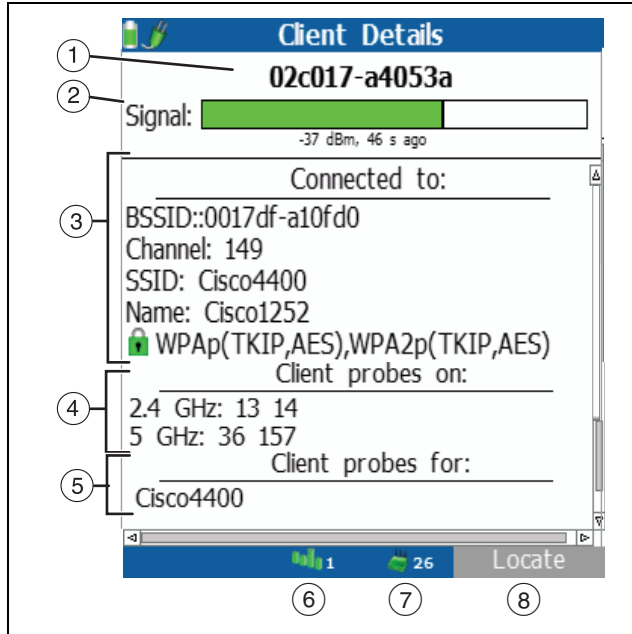
Para classificar em uma seqüência secundária, realce um cabeçalho de coluna diferente, depois pressione  **Classif 2**.

- ⑨  **40** O canal que o testador está monitorando no momento. A cor das barras mostra o status do código do país de um domínio normativo. Consulte "Operação em 802.11d" na página 36.




acesso virtuais caso **Agrupar pontos de acesso virtuais** esteja selecionado. Consulte a página 33.

- 11 Pressione **F2** **Localizar** para localizar o cliente. Consulte a página 71.

Figura 22. Tela de Detalhes do Cliente



- 1 Endereço MAC do cliente. O endereço começa com um prefixo correspondente ao nome abreviado do fornecedor, se houver prefixo. Veja "oui_abbr.txt" na página 81.
- 2 **Sinal:** A intensidade do sinal da última transmissão do cliente e o tempo desde que o testador detectou a transmissão. Após 120 segundos, a unidade passa a ser minutos. Após 120 minutos, a unidade passa a ser horas.
- 3 **Conectado a:** Se o cliente está ou esteve conectado a uma rede ou tentou se conectar recentemente, essa seção mostra informações sobre o ponto de acesso que o cliente utilizou. Se a seção mostra somente o BSSID e o canal para o ponto de acesso, o testador precisa mais tempo para colher as informações.
- 4 **Sondas do cliente em:** Os canais que o cliente sonda. **Sondas do cliente para:** Os SSIDs que o cliente usa para sondas. Quando um cliente conecta-se a uma rede, ele às vezes não sonda outras redes, portanto, a lista não mostra sempre todos os SSIDs que o cliente pode usar. Mais SSIDs mostrarão se o cliente anda aleatoriamente.

- 5  O canal que o testador está monitorando no momento. A cor das barras mostra o status do código do país de um domínio normativo. Veja a “Operação em 802.11d” na página 36.
- 6  O número de pontos de acesso que o testador detecta em seu local. Esse número não inclui pontos de acesso virtuais caso **Agrupar pontos de acesso virtuais** esteja selecionado. Consulte a página 33.
- 7 Pressione  **Localizar** para localizar o cliente. Consulte a página 71.



- O testador não faz varredura da faixa usada pelo cliente. Veja essa configuração em **Ferramentas > Gerenciar configurações de 802.11**.
- O cliente não transmite uma sonda quando o testador está escutando o canal usado por ele.


Se o testador não conseguir descobrir um cliente


Em certas situações, o testador não descobre determinado cliente:

- O cartão wireless do cliente está desativado.
- O testador não consegue captar o cliente porque está muito longe dele.
- O testador não consegue captar o cliente porque o sinal não consegue atravessar uma parede ou outro tipo de barreira.
- Há muita interferência no canal usado pelo cliente. Selecione **Canais** para ver a interferência de fontes não 802.11 no canal.

Localizar um Ponto de Acesso ou um Cliente

- 1 Para localizar um ponto de acesso: Selecione **Pontos de acesso** e, em seguida, use  e  para acessar a tela **Detalhes do ponto de acesso** do ponto de acesso que deseja localizar.

Para localizar um cliente: Na tela inicial, selecione **Clientes**. Use  para realçar o cliente que deseja localizar.

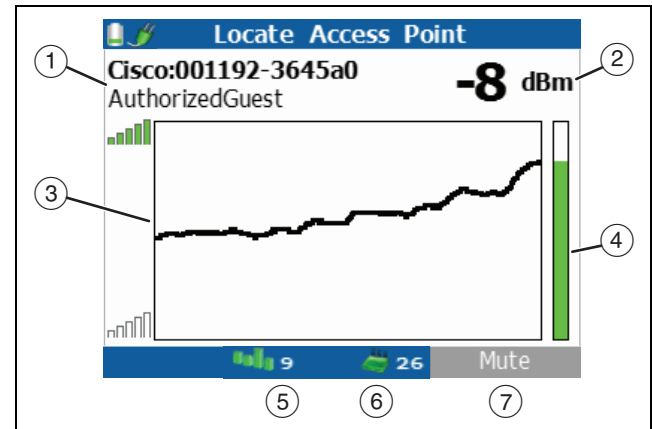
- 2 Pressione  **Localizar**. A Figura 23 mostra a tela **Localizar ponto de acesso**. A Figura 24 mostra a tela **Localizar Clientes**.
- 3 Divida a área que deseja pesquisar em quatro seções, conforme mostrado na Figura 25. Caminhe até um dos cantos da área.
- 4 Anote a intensidade do sinal.
- 5 Vá aos outros três cantos da área e anote a intensidade do sinal de cada um.
- 6 Vá ao primeiro canto da seção que tem o sinal mais forte.
- 7 Realize os passos 4, 5 e 6 novamente até encontrar um ponto de acesso ou um cliente.

Obs.:s

Caso não encontre um ponto de acesso ou um cliente, verifique o andar acima ou abaixo.




Se não conseguir encontrar um cliente, e o cliente mostrar uma conexão à rede, encontre primeiro o ponto de acesso que o cliente utilizou, e depois procure o cliente.

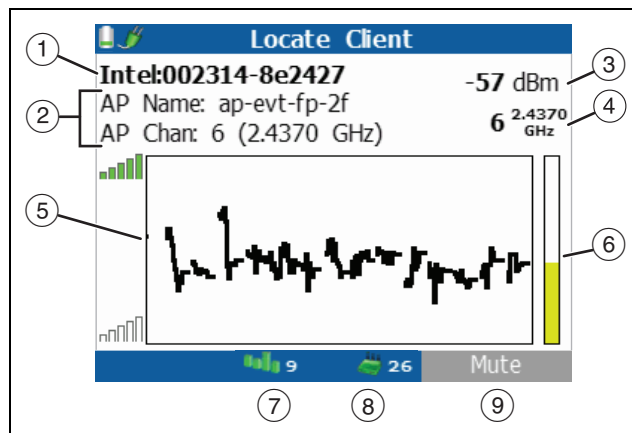
Em áreas abertas e grandes, a antena externa opcional ajuda a localizar pontos de acesso ou clientes mais rapidamente. Consulte a página 75.



ffy07.eps

Figura 23. Tela de localização de ponto de acesso





- 1 Nome da rede (SSID) e endereço MAC do ponto de acesso (BSSID).
- 2 Intensidade de sinal do ponto de acesso. O visor mostra "----" se o testador não consegue captar o ponto de acesso.
- 3 Gráfico da intensidade do sinal ao longo do tempo. Se o testador não conseguir captar o ponto de acesso, a linha não aparecerá.
- 4 Indicador da intensidade do sinal no momento. A barra é cinza quando o testador não consegue escutar o ponto de acesso.
- 5  O canal usado pelo ponto de acesso. A cor das barras mostra o status do código do país de um domínio normativo. Consulte "Operação em 802.11d" na página 36.
- 6  O número de pontos de acesso encontrados pelo testador. Esse número não inclui pontos de acesso virtuais caso **Agrupar pontos de acesso virtuais** esteja selecionado. Consulte a página 32.
- 7 Pressione  **Mudo** para desativar o som.



ffy18.eps

Figura 24. Tela Localizar cliente

- 1 Endereço MAC do cliente. O endereço começa com um prefixo correspondente ao nome abreviado do fornecedor, se houver prefixo. Veja "oui_abbr.txt" na página 81.
- 2 O nome, canal e frequência do ponto de acesso que o cliente utiliza para a conexão de rede.
- 3 Intensidade de sinal do cliente. O visor mostra "----" se o testador não consegue escutar o cliente.

- ④ O canal que o testador está monitorando para a localização.
Para alterar o canal, pressione .
- ⑤ Gráfico da intensidade do sinal ao longo do tempo. Se o testador não conseguir escutar o cliente, a linha não aparecerá.
- ⑥ Indicador da intensidade do sinal no momento. A barra fica cinza quando o testador não consegue escutar o cliente.
- ⑦  O canal que o testador monitora. Veja ④.
A cor das barras mostra o status do código do país de um domínio normativo. Consulte "Operação em 802.11d" na página 36.
- ⑧  O número de pontos de acesso encontrados pelo testador. Esse número não inclui pontos de acesso virtuais caso **Agrupar pontos de acesso virtuais** esteja selecionado. Consulte a página 32.
- ⑨ Pressione  **Mudo** para desativar o som.

 Anote a intensidade do sinal.

? Vá ao primeiro canto da seção que tem o sinal mais forte.

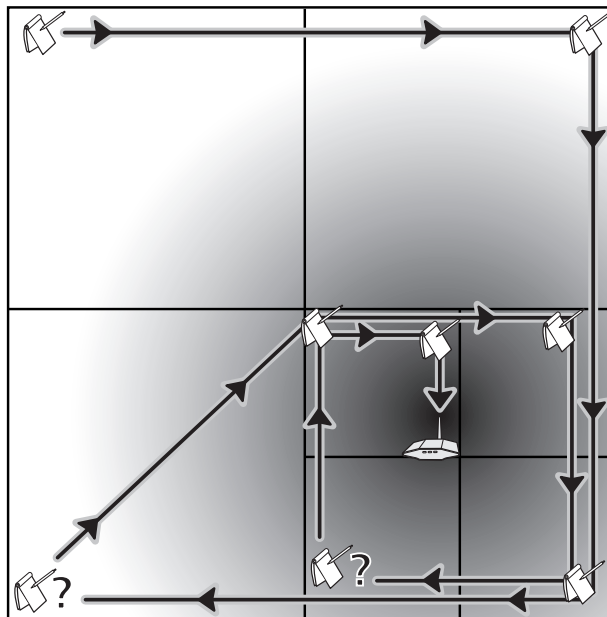


Figura 25. Padrão de busca da antena omnidirecional do testador


Antena direcional externa

Em áreas abertas e grandes, a antena direcional externa pode indicar a direção de uma fonte de sinal com mais precisão do que a antena omnidirecional do testador.

Obs.:



Em áreas com muitas salas, como, por exemplo, escolas ou hospitais, use a antena omnidirecional interna para localizar pontos de acesso.


Para utilizar a antena externa


- 1 Conecte a antena ao conector de antena no painel traseiro do testador. A tela mostra o ícone de antena () quando a antena está conectada. Quando a antena está conectada, o testador usa apenas a antena externa.

Obs.:

Quando a antena externa está conectada, o testador não transmite, portanto, não pode se conectar a uma rede ou ponto de acesso.

- 2 Divida a área em quatro seções, conforme mostrado na Figura 26. Coloque-se no centro da área.
- 3 Para localizar um ponto de acesso: Selecione **Redes** ou **Pontos de acesso** e, em seguida, use  e  para acessar a tela **Detalhes do ponto de acesso** do ponto de acesso que deseja localizar.

Para localizar um cliente: Na tela inicial, selecione **Clientes**. Use  para realçar o cliente que deseja localizar.

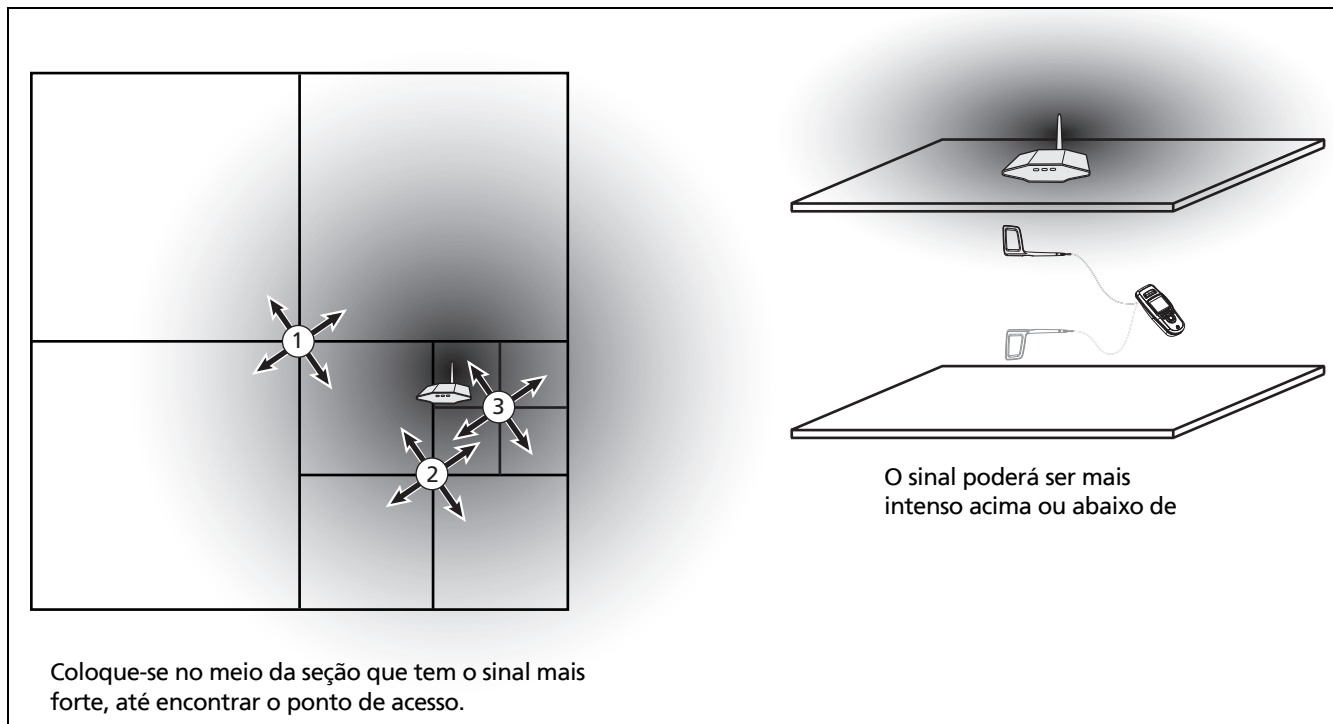
- 4 Pressione  **Localizar**.
- 5 Aponte a antena na direção de cada canto da área. A Figura 27 mostra como apontar a antena.
- 6 Coloque-se no meio da seção que tem o sinal mais forte.
- 7 Realize os passos 2, 5 e 6 novamente até encontrar um ponto de acesso ou um cliente.

Obs.:

Caso não encontre um ponto de acesso ou um cliente, verifique o andar acima ou abaixo.

Siga estas diretrizes ao usar a antena externa:

- Segure a antena mantendo-a em uma altura constante. Segure a antena acima das paredes de cubículos ou divisórias para obter medidas mais estáveis.
- Ao apontar a antena em outra direção, não mova o braço. Segure o testador e a antena na mesma posição enquanto você vira o corpo.



ffy17.eps

Figura 26. Padrão de busca da antena externa

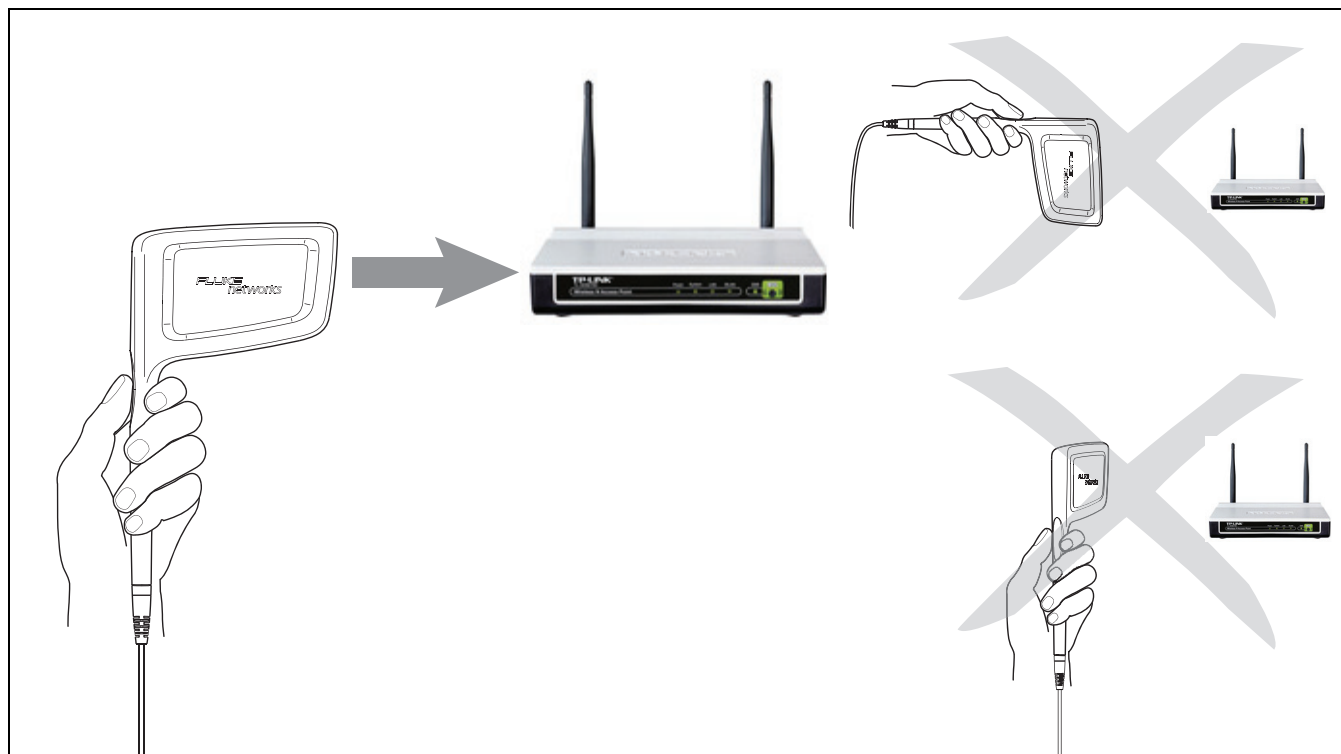


Figura 27. Como apontar a antena externa

Ajuste as medidas de intensidade de sinal para estarem de acordo com outros dispositivos




As medidas de intensidade de sinal de modelos diferentes de testadores de rede sem fio ou de clientes utilizados como referência nem sempre estão de acordo. As diferenças são provocadas principalmente pelas diferenças nas antenas. Para fazer com que os dispositivos estejam de acordo, você pode acrescentar um desvio às medidas do AirCheck na tela.

Para adicionar um desvio às medidas de intensidade de sinal

- 1 Encontre o valor de desvio:

Utilize o testador AirCheck e o outro dispositivo para medir a intensidade do sinal no mesmo local. Registre a diferença na medida de cada canal importante para você.

- 2 Selecione **Ferramentas**.


- 3 Selecione **Gerenciar configurações de 802.11**, depois selecione **Utilizar ajuste de sinal personalizado**.
- 4 Na tela **Deslocamentos do usuário**, use  para selecionar o canal e use  para selecionar um valor de deslocamento.
- 5 Repita o passo 4 conforme necessário para os outros canais.
- 6 Para salvar os valores de desvio, pressione  **Salvar**.

Quando você desliga o testador, ele salva os desvios no perfil. Os desvios também aparecem nos relatórios realizados com o AirCheck Manager.

Atenção







Para evitar futuras medidas inconsistentes, lembre-se de ter ajustado os desvios.

Salvar uma sessão de teste

Você pode salvar as informações coletadas pelo testador desde que ele foi ligado ou desde a última vez em que você salvou uma sessão, pressionou  ou desconectou o cabo USB. Cada sessão inclui as seguintes informações:










- Resultados de AutoTest (se salvos com o AutoTest existente).
- Informações da rede, do ponto de acesso, do cliente e do canal (não inclui os gráficos)
- Uma lista de clientes que transmitiram sondas
- Os resultados da última conexão efetuada
- Os resultados do último teste de ping efetuado
- O log de conexão

Para salvar os dados de uma sessão de teste

- 1 Pressione . O testador mostra um nome de arquivo sequencial padrão na parte inferior da tela.
 - Para salvar a sessão com o nome de arquivo mostrado, pressione  **Salvar**. O testador salva a sessão na pasta "SESSÕES".
 - Para gravar em cima de uma sessão de teste salva no testador, realce-a e pressione , em seguida  **Salvar**; depois pressione  **OK**.
 - Para editar o nome do arquivo, pressione  **Editar**.

Obs.:



Os nomes de sessões podem ter, no máximo, 8 caracteres, e uma extensão de 3 caracteres. Se quiser que a sessão apareça no AirCheck Manager, é necessário usar a extensão ".ACS".

- Para apagar caracteres do nome do arquivo, pressione  **Excluir**.
- Para acrescentar caracteres ao nome do arquivo, use    para realçar o caractere e pressione .
- Para mover o cursor pelo nome do arquivo, realce o nome do arquivo e pressione  .
- Para salvar a sessão com o nome de arquivo editado, pressione  **Concluído** e, em seguida,  **Salvar**.

Para ver o arquivo da sessão, abra-o no AirCheck Manager. Consulte a página 82.









Gerenciar arquivos no testador

Para renomear um arquivo



- 1 Selecione **Ferramentas** e, em seguida, **Gerenciar arquivos**.
- 2 Selecione **Renomear arquivo**.
- 3 Realce um arquivo e pressione .
- 4 Para editar o nome do arquivo, pressione  **Editar**.

Obs.:

Para ver as sessões e perfis no AirCheck Manager, as sessões precisam ter a extensão “.ACS”, e os perfis, a extensão “.ACP”.

- Para excluir caracteres no nome do arquivo, pressione  **Excluir**.
 - Para acrescentar caracteres ao nome do arquivo, use   para realçar o caractere e pressione .
 - Para mover o cursor pelo nome do arquivo, realce o nome do arquivo e pressione  .
- 5 Para renomear o arquivo com o nome que desejar, pressione  **Concluído** e, em seguida,  **Renomear**.

Para excluir um arquivo

- 1 Selecione **Ferramentas** e, em seguida, **Gerenciar arquivos**.
- 2 Selecione **Excluir arquivo**.
- 3 Realce um arquivo e pressione .
- 4 Pressione  **Excluir**.

Para ver quanto espaço está disponível na memória

- 1 Selecione **Ferramentas > Visualizar Informações do AirCheck**.
- 2 Visualizar **Memória utilizada %**.

ou

Use o cabo USB fornecido com o testador para conectar o testador ao computador; em seguida, use um destes procedimentos:

- Inicie o AirCheck Manager, selecione **AirCheck > Visualizar Informações**, depois olhe para o gráfico **Memória utilizada**.
- Use o navegador de arquivos do sistema operacional no computador para ver quanta memória está disponível no testador.

Se a memória estiver cheia, o testador indicará **Memória cheia** quando você tentar salvar um arquivo.

Sobre os arquivos contidos no testador

O testador salva dados no formato XML (Extensible Markup Language). Os dados dos arquivos XML incluem tags de identificação. Um software que lê tags pode usar esses dados. Um navegador web, por exemplo, lê tags e pode exibir os arquivos XML como páginas web.

O testador cria os seguintes tipos de arquivos XML (nomes de arquivos padrão):

- **DEVICE.XML**: Este arquivo contém as informações mostradas ao selecionar **Ferramentas > Exibir informações do AirCheck**.
- **CURRENT.ACP**: Este arquivo contém uma cópia do perfil atual. Também contém as mudanças efetuadas nas definições do testador desde que o perfil foi salvo ou carregado.
- **SNXXXXXX.ACS**: Os arquivos de sessões contêm informações sobre redes sem fio. Veja a "Localizar um Ponto de Acesso ou um Cliente" na página 71. O AirCheck Manager usa os arquivos de sessões para gerar relatórios de sessões.

O arquivo de texto *oui_abbr.txt* contém abreviaturas dos nomes dos fabricantes que fabricam dispositivos de interface para redes. O testador usa essas abreviaturas como prefixos nos endereços MAC.

Para carregar a lista mais recente de prefixos de fornecedores no testador

- 1 Inicie a última versão do AirCheck Manager no computador e conecte o testador ao computador.
- 2 Selecione **AirCheck > Atualizar software** e, em seguida, selecione a guia **Arquivo de prefixos MAC de fornecedores**.
- 3 Clique em **Atualizar baseado no arquivo**, selecione o arquivo de prefixos (*oui_abbr.txt*) e clique em **Abrir**.

Se há uma nova lista no site da Fluke Networks que não está incluída na última versão do AirCheck Manager, copie o arquivo na pasta "VendorPrefix" no AirCheck Manager (no seu computador). Em seguida, efetue as etapas mencionadas para carregar a lista no testador.

Caso deseje adicionar manualmente os prefixos dos fornecedores no arquivo *oui_abbr.txt*, utilize o WordPad da Microsoft e preserve os campos delimitados por tabulações.

```
00000A Omron OMRON TATEISI ELECTRONICS
00000B Matrix          ↑ MATRIX CORPORATION
00000C ← [Tab delimited fields] EMS, INC.
00000D          ↓          RONICS LTD.
00000E Fujitsu          ↓ FUJITSU LIMITED
```

ffy44.bmp

Figura 28. Arquivo oui_abbr.txt

Transferir arquivos para um computador

Para usar o AirCheck Manager para ver sessões de teste ou perfis salvos no testador

- 1 Instale a versão mais recente do software AirCheck Manager no computador. Inicie o software.
- 2 Ligue o testador.
- 3 Use o cabo USB fornecido com o testador para conectá-lo ao computador. A janela do AirCheck mostra os arquivos de sessões contidos no testador.

Para usar o sistema operacional do computador para transferir os arquivos

- 1 Ligue o testador.

- 2 Use o cabo USB fornecido com o testador para conectá-lo ao computador. O sistema operacional do computador mostra o testador como uma unidade de disco.
- 3 Use o sistema operacional do computador para copiar arquivos do testador para uma unidade de disco do computador.

Manutenção



Cuidado

Para evitar risco de incêndio, choque elétrico, lesão física ou dano ao testador:

- **Não abra a parte externa do aparelho. Nenhuma peça interna do testador pode ser consertada ou substituída pelo próprio usuário.**
- **Use apenas peças de reposição aprovadas pela Fluke Networks.**
- **Se substituir uma peça por uma não especificada, a garantia do produto será anulada; além disso, poderá se tornar perigoso usar o produto.**
- **Use apenas os centros de assistência técnica aprovados pela Fluke Networks.**

Limpeza do testador

Para limpar o visor, use um limpador especial para lentes e um pano macio e sem fiapos. Limpe a parte externa da unidade com um pano macio umedecido com água ou água e sabão neutro.

Atenção

Para evitar danos ao visor ou à parte externa da unidade, não use solventes nem produtos de limpeza abrasivos.

Atualização do software do testador

- 1 Baixe o arquivo de atualização do AirCheck no site da Fluke Networks, ou entre em contato com a Fluke Networks para obter uma atualização. Salve o arquivo em disco rígido.
- 2 Baixe a versão mais recente do AirCheck Manager no site da Fluke Networks.
- 3 Inicie o AirCheck Manager no seu computador.
- 4 Ligue o testador.
- 5 Use o cabo USB fornecido com o testador para conectá-lo ao computador.

- 6 No AirCheck Manager, selecione **AirCheck > Atualizar software**.

Obs.:

Também é possível atualizar o arquivo de prefixo MAC (oui_abbr.txt) usado para resolver os MACs do fornecedor na lista de dispositivos do AirCheck.

- 7 Clique em **Selecionar**; localize e selecione o arquivo de atualização (extensão .xlf) e clique em **Abrir**.
- 8 Clique em **Atualizar**.
- 9 Após concluir a transferência, desconecte o cabo USB do testador.
- 10 A tela do testador fica vazia e o testador vai marcando as tarefas realizadas durante a instalação do arquivo de atualização. Após concluir a atualização, a tela inicial será apresentada no testador.



Obs.:

Durante a atualização do software o interruptor liga/desliga é desativado. Se a bateria for removida antes de terminada a atualização, a atualização será reiniciada quando o testador for ligado.

Restaurar padrões de fábrica

O Apêndice apresenta a lista das configurações padrão do testador.



Para restabelecer padrões de fábrica

- 1 Na tela inicial, selecione **Ferramentas** e **Restabelecer padrões de fábrica**; em seguida, pressione  **OK**.
- 2 Para finalizar o processo, pressione  e ligue o testador novamente.

Excluir todos os dados

Excluir todos os dados faz tudo o que **Restabelecer Padrões de Fábrica** faz, além de apagar todos os arquivos no sistema de arquivo.

Para apagar totalmente os perfis e dados da sessão

- 1 Na tela inicial, selecione **Ferramentas** e **Apagar tudo**; em seguida, pressione  **OK**.
- 2 Para finalizar o processo, pressione  e ligue o testador novamente.

Informações sobre o dispositivo

Para ver informações sobre o testador

- 1 Na tela inicial, selecione **Ferramentas** > **Visualizar Informações do AirCheck**.

- 2 Visualizar Memória utilizada %.

- **Número de série:** O número de série também encontra-se sob a unidade de bateria.
- **Endereço MAC:** Endereço Media Access Control. Endereço exclusivo do testador.
- **Versão SW:** Versão do software instalado no testador.
- **Versão do rádio:** Versão do rádio instalado no testador.
- **Versão de USB:** Versão do driver USB instalado no testador.

Se não for possível desligar o testador

Se o testador não desligar, segure o botão verde de ligar por cerca de 10 segundos.

Se mesmo assim o testador não desligar, retire a bateria e instale-a novamente.

Opcionais e acessórios

A Tabela 5 mostra as opções e acessórios disponíveis para o testador de Wi-Fi AirCheck.

Para ver a lista completa de opções e acessórios, acesse o site da Fluke Networks: www.flukenetworks.com.





Tabela 5. Opcionais e acessórios




| Opção ou acessório | Número do modelo da Fluke Networks |
|--|---|
| Antena direcional externa com conector RSMA | EXTANT-RPSMA |
| Unidade de bateria lítio-ion para o testador AirCheck | WBP-LION |
| Detector PoE (Power over Ethernet) | POE-DETECTOR |
| Adaptador/carregador para conexão em acendedor de cigarros de automóveis | MS-Auto-Chg |
| Carregador/adaptador CA universal (120-240 V CA) | DTX-ACUN |

Especificações

Especificações ambientais

| | |
|---|---|
| Temperatura e umidade relativa de operação | 0°C a 45°C ou mais (32°F a 113°F) <i>Obs.: A bateria não é carregada se a temperatura interna do testador estiver acima de 45°C (113°F).</i> |
| Umidade relativa de operação (% de umidade relativa sem condensação) | 90% (50°F a 95°F; 10°C a 35°C) 75% (95°F a 113°F; 35°C a 45°C) |
| Temperatura de armazenagem | -20°C a 60°C ou mais (-4°F a 140°F) |
| Impacto e vibração | Aleatória, 2 g, 5 Hz a 500 Hz (Classe 2); teste de queda de 1 metro |
| Segurança | IEC/EN 61010-1 |
| Altitude | 4.000 m; Armazenagem: 12.000 m |
| EMC (compatibilidade eletromagnética) | FCC Parte 15 Classe A, EN 61326-1 |

| | |
|------------------------------------|---|
| Certificação e conformidade |  Conformidade com as normas pertinentes da União Europeia. |
| |  Conformidade com os padrões pertinentes da Austrália. |
| |  Consta na relação da Canadian Standards Association |
| |  Conformidade com as Regras da FCC, Partes 15.107, 15.109 <i>Observação As alterações ou modificações no rádio wireless não aprovadas expressamente pela Fluke Corporation anularão a autoridade do usuário no uso do equipamento. Esse dispositivo está em conformidade com a Parte 15 das Regras FCC. O uso do equipamento está sujeito às duas condições seguintes: (1) este dispositivo não pode causar interferência e (2) este dispositivo deve aceitar qualquer interferência, incluindo interferência que possam causar funcionamento indesejado do dispositivo. Dispositivos digitais Classe B: Um dispositivo digital que é comercializado para operação em um ambiente residencial, apesar do uso em ambientes comerciais, empresariais e industriais. Exemplos de tais dispositivos incluem, sem limitação, computadores pessoais, calculadoras e dispositivos eletrônicos equivalentes comercializados para operação pelo público em geral. O medidor foi testado e considerado em conformidade com os limites para um dispositivo digital Classe B, de acordo com a Parte 15 das regras do FCC. Esses limites foram estabelecidos para fornecer proteção razoável contra interferência nociva em instalações residenciais. O equipamento gera, usa e pode irradiar energia de radiofrequência e, se não for instalado e usado de acordo com as instruções, pode causar interferência nociva em radiocomunicações.</i> |

| | |
|--|--|
| | <p>Contudo, não há garantia de que não ocorrerá interferência em uma instalação específica. Se este equipamento causar interferência nociva na recepção de rádio ou televisão, o que pode ser verificado desligando-se e ligando-se o equipamento, incentivamos o usuário técnico a tentar corrigir a interferência por meio de uma das seguintes medidas: • Mudar a direção ou o local da antena de recepção. • Aumentar a distância entre o equipamento e o receptor. • Se necessitar de assistência, consulte o revendedor ou um técnico de rádio ou TV experiente. O termo "IC:" antes do número de certificação apenas significa que o dispositivo cumpre as especificações de indústria do Canadá.</p> |
| | <p> ANATEL 1572-10-5988  (01)07898941652029</p> <p>Certificação pela Agência Nacional de Telecomunicações (Anatel)</p> |
| | <p> Em conformidade com os Padrões de EMC relevantes da Coreia do Sul.</p> |
| Informações adicionais sobre o Padrão EMC da Coreia do Sul | |
| Compatibilidade eletromagnética. Aplica-se ao uso somente na Coreia. Equipamento Classe A (Equipamento de Comunicação e Broadcasting Industrial) [1] | <p>[1] Este produto está em conformidade com as exigências para equipamentos industriais de ondas eletromagnéticas (Classe A), e o vendedor ou usuário deve estar ciente disso. Este equipamento é indicado para uso em ambientes empresariais e não deve ser utilizado em ambientes domésticos.</p> |

Especificações gerais

| | |
|--|---|
| Dimensões | 8,9 cm x 19,8 cm x 4,8 cm (3,5 pol x 7,8 pol x 1,9 pol) |
| Peso | 0,4 kg (14 oz) |
| Bateria | Unidade de bateria de lítio-íon; recarregável e removível (18,5 watts-horas) |
| Duração da bateria | A duração sob condições normais é de 5,5 horas de uso. Normalmente, leva 3 horas para carregar a bateria. |
| Carregador/adaptador CA externo | Entrada CA de 90 a 264 V CA; saída CC de alimentação de entrada de 48 a 62 Hz de 15 V CC a 1,2 ampere |
| Tela | Display de cristal líquido (LCD) de 2,8 polegadas, em cores (320 x 240 pixels) |
| Teclado: | 12 teclas, elastomérico |
| LEDs | 2 LEDs (indicadores de transmissão e de conexão) |
| Interface com host | USB mini-B, 5 pinos |
| Antena sem fio | Interna |
| Porta para antena externa | Somente entrada. Conector SMA de polaridade inversa. |

Especificações de conexão sem fio

| | |
|--|---|
| Conformidade das especificações | IEEE 802.11a, 11b, 11g, 11n |
| Conectividade Wi-Fi | 802.11a, 802.11b, 802.11g , 802.11n 802.11b /CA (taxas de 802.11n inferior) |

| | |
|--|---|
| <p>Frequências de operação</p> <p><i>Obs.:</i> <i>Esses são os centros de frequência dos canais com os quais o testador AirCheck é compatível.</i></p> | <p>Frequências dos canais recebidos</p> <p><i>Obs.:</i> <i>O testador capta todas as frequências em todos os canais.</i></p> <p>Faixa de 2,4 GHz: de 2,412 GHz a 2,484 GHz (do canal 1 ao canal 14)</p> <p>Faixa de 5 GHz: de 5,170 GHz a 5,320 GHz, de 5,500 GHz a 5,700 GHz, de 5,745 GHz a 5,825 GHz (canais 34, 36, 38, 40, 42, 44, 46, 48, 52, 56, 60, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 149, 153, 157, 161, 165)</p> <p>Frequências dos canais transmitidos</p> <p><i>Obs.:</i> <i>O testador transmite somente as frequências permitidas no país onde estiver funcionando.</i></p> <p>Faixa de 2,4 GHz</p> <p>802.11b: de 2,412 GHz a 2,484 GHz (do canal 1 ao canal 14)</p> <p>802.11 g/n 20 MHz BW (HT20): de 2,412 GHz a 2,472 GHz (do canal 1 ao canal 13)</p> <p>802.11 n 40 MHz BW (HT40): de 2,422 GHz a 2,462 GHz (inclui todas as combinações de pares de canais legais vinculados)</p> |
|--|---|

| | |
|----------------------------------|---|
| | <p>Frequências dos canais transmitidos (continuação)</p> <p>Faixa de 5GHz</p> <p>802.11 a /n 20 MHz BW (HT20): 5,180 GHz to 5,320 GHz, 5,500 GHz to 5,700 GHz, 5,745 GHz to 5,825 GHz (canais 36, 40, 44, 48, 52, 56, 60, 100, 104, 108, 112, 116, 120, 124, 128, 132, 1, 36, 140, 149, 153, 157, 161, 165)</p> <p>802.11 n 40 MHz BW (HT40): de 5,190 GHz a 5,310 GHz, de 5,510 GHz a 5,670 GHz, de 5,755 GHz a 5,795 GHz (inclui todas as combinações de pares de canais legais vinculados)</p> |
| Domínio regulatório | Modo mundial, conformidade com 802.11d |
| Antena direcional externa | |
| Frequências | Faixa de frequência 2,4 GHz a 2,5 GHz e 4,9 a 5,9 GHz |
| Conector | Ganho mínimo 5,0 dBi na faixa de 2,4 GHz e 7,0 dBi na faixa de 5 GHz Plugue SMA de polaridade reversa |

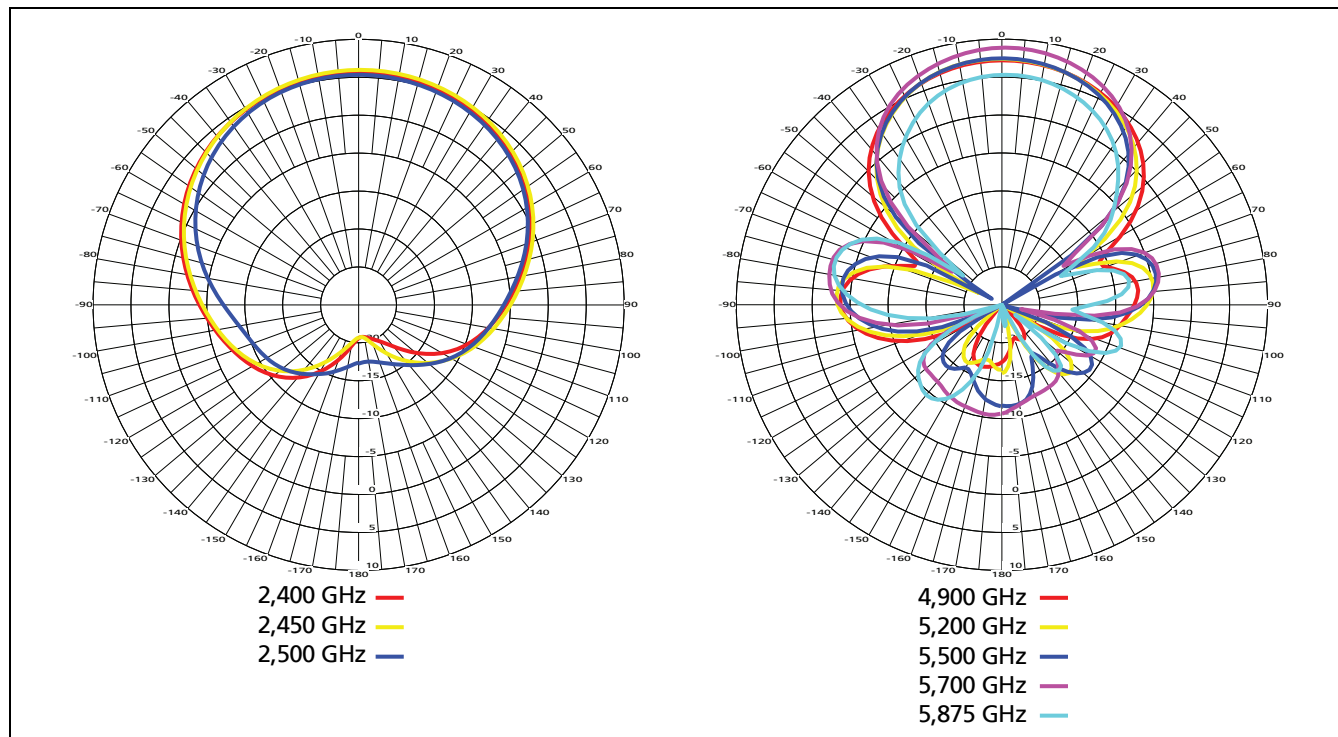


Figura 29. Padrões de antena para antena externa (magnitude (dBi)) vs. azimute (graus)

Declaração sobre interferência para Federal Communication Commission e Industry Canada

Este equipamento foi testado e verificou-se que cumpre os limites definidos para dispositivos digitais de Classe B, de acordo com a Parte 15 das regras da FCC e da IC. Esses limites foram estabelecidos para fornecer proteção razoável contra interferência nociva em instalações residenciais. O equipamento gera, usa e pode irradiar energia de radiofrequência e, se não for instalado e usado de acordo com as instruções, pode causar interferência nociva em radiocomunicações. Contudo, não há garantia de que não ocorrerá interferência em uma instalação específica. Se este equipamento causar interferência nociva na recepção de rádio ou televisão, o que pode ser verificado desligando-se e ligando-se o equipamento, incentivamos o usuário a tentar corrigir a interferência por meio de uma das seguintes medidas:

- Mudar a direção ou o local da antena de recepção.
- Aumentar a distância entre o equipamento e o receptor.
- Conectar o equipamento em uma tomada de outro circuito, que não o circuito em que o receptor está conectado.

- Se necessitar de assistência, consulte o revendedor do equipamento ou um técnico de rádio ou TV experiente.

Aviso da FCC: qualquer mudança ou modificação que não tenha sido expressamente aprovada pela parte responsável pela conformidade regulamentar poderá anular a autoridade do usuário de usar este equipamento.

Este dispositivo cumpre as regras da FCC e IC, Parte 15. O uso do equipamento está sujeito às duas condições seguintes:

- (1) Este dispositivo não pode causar interferência nociva; (2) este dispositivo deve, necessariamente, aceitar qualquer interferência, inclusive interferência que possa causar um funcionamento indesejável.

Observação importante: Declaração da FCC e da IC sobre exposição à radiação

Este equipamento cumpre os limites de exposição à radiação estabelecidos pela FCC e pela IC no que se refere a ambientes não controlados. Este equipamento deve ser instalado e usado com uma distância mínima de 20 cm entre o radiador e o usuário.

É proibido mudar o transmissor de lugar ou operá-lo em conjunto com algum outro transmissor ou antena.

A operação na faixa de 5,15 GHz a 5,25 GHz é restrita a ambientes internos.

A disponibilidade de certos canais ou faixas de frequência operacional específicos variam conforme o país e não é acessível para o usuário final.

Declaração de conformidade para a Europa-UE

Este dispositivo cumpre os requisitos essenciais da Diretiva R&TTE 1999/5/EC. Os seguintes métodos de teste foram empregados para comprovar a premissa de conformidade com os requisitos essenciais da Diretiva R&TTE 1999/5/EC:

- **EN50385: (2002-08)**

Padrão de produto para demonstrar a conformidade de estações-base de rádio e estações de terminais fixos para sistemas de telecomunicações sem fio (wireless) com as restrições básicas ou os níveis de referência relacionados à exposição humana a campos eletromagnéticos de radiofrequência (110 MHz a 40 GHz) – Público em geral

- **EN 300328 V1.7.1: (2006-10)**

Compatibilidade eletromagnética e questões referentes a espectros de rádio (ERM); sistemas de transmissão em banda larga; equipamento de transmissão de dados que opera na faixa ISM de 2,4 GHz e usa técnicas de modulação de espectros dispersos; EN harmonizado, abrangendo os requisitos essenciais constantes no artigo 3.2 da Diretiva R&TTE

- **EN 301 893 V1.4.1: (2007-07)**

Broadband Radio Access Networks (BRAN); RLAN 5 GHz de alto desempenho; sistema EN harmonizado, cobrindo os requisitos essenciais do artigo 3.2 da Diretiva R&TTE

- **EN 301 489-1 V1.6.1: (2005-09)**

Compatibilidade eletromagnética e questões referentes a espectros de rádio (ERM); padrão de compatibilidade eletromagnética (EMC) para serviços e equipamentos de rádio; Parte 1: Requisitos técnicos comuns

- **EN 301 489-17 V1.2.1 (2002-08)**

Compatibilidade eletromagnética e questões referentes a espectros de rádio (ERM); padrão de compatibilidade eletromagnética (EMC) para serviços e equipamentos de rádio; Parte 17: Condições específicas para sistemas de transmissão de 2,4 GHz em banda larga e equipamentos RLAN de 5 GHz de alto desempenho

Este dispositivo é um sistema de transmissão (transceptor) de banda larga em 2,4 GHz produzido para ser usado em todos os estados-membros da UE e países da EFTA, exceto França e Itália, onde se aplicam restrições ao uso.

Na Itália, o usuário final deve requerer uma licença dos órgãos competentes nacionais a fim de obter autorização para usar o dispositivo para estabelecer enlaces de rádio em ambiente externo e/ou para fornecer acesso público a serviços de redes ou de telecomunicações.

É proibido usar este dispositivo para estabelecer enlaces de rádio em ambiente externo na França; em certas áreas, a potência de saída de RF pode se limitar a 10 mW EIRP na faixa de frequência de 2454 MHz a 2483,5 MHz. Para obter informações detalhadas, o usuário final deve contatar o órgão competente encarregado de autorização de espectros na França.

Apêndice : Registro de mensagens referentes a conexões com erros

O registro ou log de conexão é útil para se entender por que determinado dispositivo não conseguiu se conectar à rede. Este apêndice apresenta as mensagens e os possíveis motivos dos erros da conexão.

| Mensagem | Possíveis motivos do erro da conexão |
|--|--|
| 802.11: nenhum ponto de acesso encontrado | O ponto de acesso está fora do alcance, está desativado, ou alguém mudou a faixa de frequência do mesmo. |
| 802.11: aviso: PA com SSID encontrado. Configurações de segurança incompatíveis | O testador não tem os tipos corretos de criptografia/autenticação 802.1X. |

| Mensagem | Possíveis motivos do erro da conexão |
|---|--|
| Falha na autenticação | <p>A lista de controle de acesso e o filtro MAC do ponto de acesso rejeitaram o MAC do testador.</p> <p>O ponto de acesso usa segurança WEP; a autenticação 802.11 de baixo nível (aberta/compartilhada) usada pelo testador é diferente do tipo de autenticação usado pelo ponto de acesso.</p> |
| 802.11 : pacotes de exclusão de autenticação | <p>Quando essa ação segue a mensagem 802.1X : Enviando chave EAP de 4 vias com cliente nonce e info elements, é causada, com frequência, por uma chave pré-compartilhada incorreta (senha).</p> |
| Conectar: falha esperada durante provisionamento do PAC (fase 0) | <p>O testador exibe esta mensagem sempre que usa autenticação EAP-FAST para tentar estabelecer conexão a um ponto de acesso. São necessárias várias fases para estabelecer uma conexão EAP-FAST, e é comum ocorrer erros durante a fase inicial.</p> |
| 802.1X: falha no EAP recebido | <ul style="list-style-type: none">• Quando esta ação segue a mensagem 802.1X TLS: Enviando troca de chave do cliente é causada, com frequência, por um certificado de cliente incorreto.• Quando esta ação segue a mensagem 802.1X EAP-MSCHAPv2: Respondendo ao desafio, é causada, com frequência, por um nome do usuário ou a senha incorreta.• Quando esta ação segue a mensagem 802.1X : NAK, ela ocorre com frequência porque o servidor RADIUS não é compatível com o tipo EAP. |

| Mensagem | Possíveis motivos do erro da conexão |
|--|---|
| 802.1X: certificado de servidor não verificado | Ignore esta mensagem se não tiver selecionado a opção Verificar certificado do servidor no perfil do AirCheck Manager. |
| 802.1X: certificado de servidor inválido | A opção Verificar certificado do servidor foi selecionada no perfil, no AirCheck Manager, mas um certificado incorreto foi carregado no testador. |
| DHCP: tempo esgotado (sem a mensagem DHCP: sucesso após esta opção) | <ul style="list-style-type: none"> • O ponto de acesso não conseguiu se comunicar com o servidor DHCP externo. • O ponto de acesso tem um servidor DHCP interno, mas ele está desativado. • O servidor DHCP alcançou o número limite de usuários. • O testador e o ponto de acesso foram configurados para usar segurança WEP, mas as chaves estão configuradas de forma diferente. |
| DHCP: nenhuma oferta recebida | Quando esta ação segue a mensagem DHCP: tempo esgotado , veja as causas acima. |
| IP estático: ARP recebido. Endereço já está em uso | A opção Manual (estático) foi selecionada no perfil, no AirCheck Manager, mas foi encontrado um endereço IP duplicado na rede. |

Apêndice : Configurações padrão

Este apêndice mostra as configurações padrão do testador quando se seleciona **Ferramentas > Restabelecer padrões de fábrica**.

| Função | Configuração padrão |
|--|---|
| Perfil usado pelo testador | Padrão |
| Desligamento automático | Ligar |
| Idioma | O idioma que foi selecionado por último |
| País | EUA |
| Som para a função de localização de ponto de acesso (PA) | Ligar |

| Limites dos gráficos de barras | |
|---------------------------------------|---------|
| Nível de sinal: Vermelho | -85 dBm |
| Nível de sinal: Amarelo | -75 dBm |
| Nível de sinal: Verde | -65 dBm |
| Nível de ruído: Vermelho | -65 dBm |
| Nível de ruído: Amarelo | -72 dBm |
| Nível de ruído: Verde | -80 dBm |
| Nível de sinal-ruído: Vermelho | 10 dB |
| Nível de sinal-ruído: Amarelo | 17 dB |
| Nível de sinal-ruído: Verde | 25 dB |
| Cobertura de rede: | 2 PAs |

| | |
|--|--------------------|
| Nível de utilização do 802.11: Verde | 40% |
| Nível de utilização do 802.11: Amarelo | 55% |
| Nível de utilização do 802.11: Vermelho | 70% |
| Nível de utilização não 802.11: Verde | 20% |
| Nível de utilização não 802.11: Amarelo | 30% |
| Nível de utilização não 802.11: Vermelho | 40% |
| Nível de qualidade do ar entre canais: Verde | 3 pontos de acesso |
| Nível de qualidade do ar entre canais: Amarelo | 4 pontos de acesso |
| Nível de qualidade do ar entre canais: Vermelho | 6 pontos de acesso |
| Nível de qualidade de rede entre canais: Verde | 2 PAs |

| | |
|--|--------------------|
| Nível de qualidade de rede entre canais: Amarelo | 3 pontos de acesso |
| Nível de qualidade de rede entre canais: Vermelho | 4 pontos de acesso |
| Nível da taxa de tentativa do pacote: Verde | 10% |
| Nível da taxa de tentativa do pacote: Amarelo | 17% |
| Nível da taxa de tentativa do pacote: Vermelho | 25% |
| Nível da taxa de pacote conectado: Vermelho | 10% |
| Nível da taxa de pacote conectado: Amarelo | 20% |
| Nível da taxa de pacote conectado: Verde | 30% |
| Limite mínimo de sinal | -85dBm |
| Configurações de 802.11 | |
| Faixas | 2,4 GHz e 5 GHz |
| Transmitir sondas | Ativar |

| | |
|--|------------|
| Agrupar pontos de acesso virtuais | Ativar |
| Deixar ptos acesso n aud. em cinza | Ativado |
| Excluir ptos de acesso não audíveis | Desativado |
| Desvio do usuário para ajustes de sinal personalizados | 0 dB |
| Lista de redes (SSIDs) | |
| Classif 1 | SSID |
| Classif 2 | SSID |
| Redes individuais | |
| Classif 1 | Nome/MAC |
| Classif 2 | Nome/MAC |
| Pontos de acesso em um canal | |
| Classif 1 | Nome/MAC |
| Classif 2 | Nome/MAC |
| Lista de pontos de acesso | |
| Classif 1 | Nome/MAC |

| | |
|---|----------|
| Classif 2 | Nome/MAC |
| Lista de pontos de acesso virtuais | |
| Classif 1 | SSID |
| Classif 2 | SSID |
| Lista de clientes | |
| Classif 1 | SSID |
| Classif 2 | MAC |

Apêndice : Código 802.11d de países

Este apêndice mostra os países correspondentes aos códigos de país indicados pelo testador na tela **Detalhes do ponto de acesso**.

Os países indicados em negrito podem ser selecionados em **Ferramentas > Definir país**.

Obs.:

O testador pode apresentar um terceiro caractere no código do país. Esse caractere pode ser ignorado ao procurar o código do país na tabela abaixo.

| | |
|-----------|-------------------------------|
| AD | Andorra |
| AE | Emirados Árabes Unidos |
| AF | Afeganistão |
| AG | Antigua e Barbuda |
| AI | Anguilla |
| AL | Albânia |
| AM | Armênia |
| AN | Antilhas Holandesas |
| AO | Angola |
| AQ | Antártica |
| AR | Argentina |
| AS | Samoa Americana |
| AT | Áustria |

| | |
|-----------|-----------------------------|
| AU | Austrália |
| AW | Aruba |
| AX | Aland |
| AZ | Azerbaijão |
| BA | Bósnia e Herzegovina |
| BB | Barbados |
| BD | Bangladesh |
| BE | Bélgica |
| BF | Burkina Fasso |
| BG | Bulgária |
| BH | Bahrein |
| BI | Burundi |
| BJ | Benin |
| BL | Saint Barthelemy |
| BM | Bermuda |
| BN | Brunei Darussalam |
| BO | Bolívia |
| BR | Brasil |
| BS | Bahamas |
| BT | Butão |

| | |
|-----------|--|
| BU | Burma (transição) |
| BV | Ilha Bouvet |
| BW | Botsuana |
| BY | Belarus |
| BZ | Belize |
| CA | Canadá |
| CC | Ilhas Cocos |
| CD | Congo, República Democrática do |
| CF | República Centro-Africana |
| CG | Congo |
| CH | Suíça |
| CI | Costa do Marfim |
| CK | Ilhas Cook |
| CL | Chile |
| CM | Camarões |
| CN | China |
| CO | Colômbia |
| CR | Costa Rica |
| CS | Sérvia e Montenegro (transição) |
| CU | Cuba |

| | |
|-----------|-----------------------------|
| CV | Cabo Verde |
| CX | Ilha Christmas |
| CY | Chipre |
| CZ | República Tcheca |
| DE | Alemanha |
| DJ | Djibuti |
| DK | Dinamarca |
| DM | Dominica |
| DO | República Dominicana |
| DZ | Argélia |
| EC | Equador |
| EE | Estônia |
| EG | Egito |
| EH | Saara Ocidental |
| ER | Eritreia |
| ES | Espanha |
| ET | Etiópia |
| EU | União Europeia |
| FI | Finlândia |
| FJ | Fiji |

| | |
|-----------|-----------------------------|
| FK | Ilhas Falkland (Malvinas) |
| FM | Micronésia |
| FO | Ilhas Faro |
| FR | França |
| FX | França (área metropolitana) |
| GA | Gabão |
| GB | Reino Unido |
| GD | Granada |
| GE | Geórgia |
| GF | Guiana Francesa |
| GG | Guernsey |
| GH | Gana |
| GI | Gibraltar |
| GL | Groenlândia |
| GM | Gâmbia |
| GN | Guiné |
| GP | Guadalupe |
| GQ | Guiné Equatorial |
| GR | Grécia |
| GS | Geórgia do Sul |

| | |
|-----------|---------------------------------------|
| GT | Guatemala |
| GU | Guam |
| GW | Guiné-Bissau |
| GY | Guiana |
| HK | Hong Kong |
| HM | Ilhas Heard e McDonald |
| HN | Honduras |
| HR | Croácia |
| HT | Haiti |
| HU | Hungria |
| ID | Indonésia |
| IE | Irlanda |
| II | Internacional (somente Cisco) |
| IL | Israel |
| IM | Ilha do Homem |
| IN | Índia |
| IO | Território Britânico do Oceano Índico |
| IQ | Iraque |
| IR | Irã |
| IS | Islândia |

| | |
|-----------|---|
| IT | Itália |
| JE | Jersey |
| JM | Jamaica |
| JO | Jordânia |
| JP | Japão |
| KE | Quênia |
| KG | Quirguistão |
| KH | Camboja |
| KI | Kiribati |
| KM | Comoros |
| KN | São Cristóvão e Névis |
| KP | República Popular Democrática da Coreia (Norte) |
| KR | Coreia do Sul |
| KW | Kuait |
| KY | Ilhas Cayman |
| KZ | Cazaquistão |
| LA | Laos |
| LB | Líbano |
| LC | Santa Lúcia |

| | |
|-----------|--------------------------------|
| LI | Liechtenstein |
| LK | Sri Lanka |
| LR | Libéria |
| LS | Lesoto |
| LT | Lituânia |
| LU | Luxemburgo |
| LV | Letônia |
| LY | Líbia, Grande Jamahiriya Árabe |
| MA | Marrocos |
| MC | Mônaco |
| MD | Moldávia, República da |
| ME | Montenegro |
| MF | Saint Martin |
| MG | Madagáscar |
| MH | Ilhas Marshall |
| MK | Macedônia |
| ML | Mali |
| MM | Mianmar |
| MN | Mongólia |
| MO | Macau |

| | |
|------------|--|
| MP | Ilhas Mariana do Norte |
| MQ | Martinica |
| MR | Mauritânia |
| MS | Montserrat |
| MT | Malta |
| MU | Maurício |
| MV | Maldivas |
| MW | Maláui |
| MX | México |
| MY | Malásia |
| MZ | Moçambique |
| NA | Nenhum país selecionado (situação especial para alguns pontos de acesso) |
| NC | Nova Caledônia |
| NE | Níger |
| NF | Ilha Norfolk |
| NG | Nigéria |
| NI | Nicarágua |
| NL | Holanda |
| NÃO | Noruega |

AirCheck – Testador de Wi-Fi
Manual do Usuário

| | |
|-----------|------------------------------------|
| NP | Nepal |
| NR | Nauru |
| NT | Zona neutra (transição) |
| NU | Niue |
| NZ | Nova Zelândia |
| OM | Omã |
| PA | Panamá |
| PE | Peru |
| PF | Polinésia Francesa |
| PG | Papua-Nova Guiné |
| PH | Filipinas |
| PK | Paquistão |
| PL | Polônia |
| PM | Saint Pierre e Miquelon |
| PN | Pitcairn |
| PR | Porto Rico |
| PS | Território Palestino |
| PS | Estados Unidos (segurança pública) |
| PT | Portugal |
| PW | Palau |

| | |
|-----------|-------------------------|
| PY | Paraguai |
| QA | Qatar |
| RE | Reunião |
| RO | Romênia |
| RS | Sérvia |
| RU | Federação Russa |
| RW | Ruanda |
| SA | Arábia Saudita |
| SB | Ilhas Salomão |
| SC | Seychelles |
| SD | Sudão |
| SE | Suécia |
| SF | Finlândia (não oficial) |
| SG | Cingapura |
| SH | Santa Helena |
| SI | Eslovênia |
| SJ | Svalbard e Jan Mayen |
| SK | Eslováquia |
| SL | Serra Leoa |
| SM | San Marino |

| | |
|-----------|------------------------------|
| SN | Senegal |
| SO | Somália |
| SR | Suriname |
| ST | São Tomé e Príncipe |
| SU | União Soviética (antiga) |
| SV | El Salvador |
| SY | Síria, República Árabe da |
| SZ | Suazilândia |
| TC | Ilhas Turks e Caicos |
| TD | Chade |
| TF | Territórios Franceses do Sul |
| TG | Togo |
| TH | Tailândia |
| TJ | Tadjiquistão |
| TK | Tokelau |
| TL | Timor-Leste |
| TM | Turcomenistão |
| TN | Tunísia |
| TO | Tonga |
| TP | Timor Leste (transição) |

| | |
|------------|-------------------------------|
| TR | Turquia |
| TT | Trinidad e Tobago |
| TV | Tuvalu |
| TW | Taiwan |
| TZ | Tanzânia |
| UA | Ucrânia |
| UG | Uganda |
| UK | Reino Unido (não oficial) |
| UM | Territórios Insulares dos EUA |
| EUA | Estados Unidos |
| UY | Uruguai |
| UZ | Uzbequistão |
| VA | Cidade do Vaticano |
| VC | São Vicente e Granadinas |
| VE | Venezuela |
| VG | Ilhas Virgens Britânicas |
| VI | Ilhas Virgens, EUA |
| VN | Vietnã |
| VU | Vanuatu |
| WF | Ilhas Wallis e Futuna |

| | |
|-----------|------------------------|
| WS | Samoa |
| YE | lêmen |
| YT | Mayotte |
| YU | Iugoslávia (transição) |
| ZA | África do Sul |
| ZM | Zâmbia |
| ZR | Zaire (transição) |
| ZW | Zimbábue |

Índice remissivo

Symbols

(...)

lista de pontos de acesso

802.11, 47

ACL, 46

observações, 48

segurança, 47

lista de redes

802.11, 43

ACL, 42

observações, 43

segurança, 42

*

Conectar, 58

nome do perfil, 20, 27

ponto de acesso, 46

Numbers

802.11d, 36

–A–

a, 43, 47

acessórios

opcionais, 84

padrão, 4

ACL, 38

Agrupar pontos de acesso virtuais, 32

AirCheck Manager

atualizar o software no testador, 83

perfil, 27

transferir arquivos para um computador, 82

visão geral, 1

ajuda (como contatar a Fluke Networks), 2

ajuste de sinal personalizado, 78

alcance da conexão, 64

anotações, 51

antena

externa, 75

interna, 75

arquivos

- ACP, 81
- ACS, 81
- excluir, 80
- perfis, 27
- renomear, 80
- sessões, 79
- transferir para um computador, 82
- XML, 81
- arquivos ACP, 81
- arquivos ACS, 81
- arquivos de sessão
 - salvar, 79
- arquivos XML, 81
- atendimento ao cliente, 2
- ativar faixa de 2,4 GHz ou 5 GHz, 32
- atualização de software, 83
- atualizar o software, 83

–B–

- b, 43
- Base de conhecimento, 1
- bateria, 7
- bloquear ícones
 - tela de pontos de acesso, 47, 68
 - tela de redes, 42

–C–

- canais
 - detalhes do uso do canal, 56
 - faixas de frequência, 32
 - interferência
 - no gráfico de uso, 56
 - observação, 51
 - padrão, 36
 - uso do canal, 54
- certificação e conformidade, 90
- classificar uma lista, 44, 68
- códigos, 35
- conectar a uma rede ou ponto de acesso, 57
- configurações, 26
 - 802.11, 32
 - restaurar padrões, 84, 101
- configurações de 802.11, 32
- configurações padrão, 101
- configurações
 - mínimo, 8
- cores dos gráfico de barras, 37
- credenciais de segurança, 27, 58
- CURRENT.ACP, 81

–D–

- data, 35

declaração de conformidade, 94
Deixar ptos acesso n aud. em cinza, 33
descobrir dispositivos
 não é possível descobrir um cliente, 70
 não é possível descobrir um ponto de acesso, 54
desligamento automático, 35
Deslocamentos do Usuário, 78
Detalhes do PA, 49
DEVICE.XML, 81
dispositivo ad hoc
 lista de redes, 24, 43
dispositivo autorizado, 38
dispositivo convidado, 38
dispositivo não autorizado, 38
dispositivo sinalizado, 38
dispositivo vizinho, 38
dispositivos de descoberta
 redes ou pontos de acesso, 39

–E–

energia
 bateria, 7
 desligamento automático, 35
 não é possível desligar, 84
especificações, 86
Excluir ptos de acesso não audíveis, 33

–F–

faixas de frequência, 32
Fluke Networks
 base de conhecimento, 1
 contato, 2

–G–

g, 43
Gerenciar configurações 802.11, 30, 31, 32, 33

–H–

hora, 35

–I–

Idioma, 35
informações de segurança, 2, 82
interferência
 no gráfico de uso, 56
 observação, 51
intervalo de guarda, 53

–L–

LEDs, 6
Limites, 12, 17, 23, 30, 31, 37

limites, 10, 11, 22, 42, 46, 49, 62, 64, 68
limites para gráficos de barras, 37
limpeza, 83
localizar um ponto de acesso ou cliente
 usar a antena interna, 71
log
 tela, 62

–M–

manutenção, 82
memória, 81
modo mundial, 36

–N–

n, 43
n40+, n40-, 43
níveis de potência de transmissão, 36

–O–

observações
 (...), 43, 48
Oculto, 43, 47, 68
opções, 84

–P–

país
 código de pontos de acesso, 36
 códigos, 105
 configuração, 35
perfil, 27
ping
 endereços padrão, 61
 qualquer endereço, 63
ponto de acesso virtual, 32
pontos de acesso
 ACL (status de autorização), 38
 conectar a um ponto de acesso, 57
 lista, 45
 localizar um ponto de acesso, 71, 75
 país 802.11d, 50
 ping, 63
 tela de detalhes, 49

–Q–

quadros de solicitação de sonda
 do testador, 32

–R–

recursos de 802.11n
 , 52

redes

- conectar a uma rede, 57
- credenciais de segurança, 27
- lista, 42
- ping, 63

registro, 1

registro de data e hora

- lista de pontos de acesso, 46
- lista de redes, 42

-S-

salvar um arquivo

- perfil, 28, 29
- sessão de teste, 79

senha

- perfis, 27
- rede, 27

sequências, 53

SNR, 62

SNXXXXXX.ACS

- , 81

status de autorização, 38

-T-

teclas, 6

tela inicial, 19

transferir arquivos para um computador, 82

Transmitir sondas, 32

