# *Motorola SURFboard®*

## Gateway de Voz Wireless Série SVG1501

## Guia do Usuário

*SVG1501
SVG1501E
SVG1501U
SVG1501UE

# Informações de segurança e normativas

## INSTRUÇÕES IMPORTANTES DE SEGURANÇA

Quando utilizar o aparelho telefônico, devem ser seguidas sempre as precauções básicas de segurança para reduzir riscos de incêndio, choques elétricos e lesões pessoais, incluindo as seguintes:

- Leia todas as instruções relacionadas aqui e/ou no Manual do Usuário antes de operar este dispositivo. Dê atenção especial a todas as precauções de segurança. Guarde as instruções para referência futura.
- Este dispositivo deve ser instalado e usado rigorosamente de acordo com as instruções do fabricante, conforme descrito na documentação do usuário que acompanha o dispositivo.
- Siga todas as instruções de aviso e cuidado nas instruções. Observe todos os símbolos de aviso e cuidado afixados neste dispositivo.
- Para evitar risco de incêndio ou choque, não exponha este dispositivo à chuva ou à umidade. O dispositivo não deve ficar exposto a gotejamento ou respingos. Não coloque objetos cheios de líquido, como vasos, no dispositivo.
- Este dispositivo foi qualificado sob condições de teste que incluíram a utilização dos cabos fornecidos entre os componentes do sistema. Para garantir o cumprimento de normas legais e de segurança, use apenas os cabos de energia e de interface fornecidos e instale-os adequadamente.
- Podem ser usados outros tipos de cabos para conexões com o circuito de alimentação principal. Use apenas um cabo de alimentação que obedeça a todas as exigências de segurança do dispositivo aplicáveis do país em que será usado.
- A instalação deste dispositivo deve estar de acordo com os códigos nacionais de cabeamento e com as normas locais.
- Opere este dispositivo apenas com o tipo de fonte de alimentação indicada em sua etiqueta. Se você não tiver certeza sobre o tipo de energia fornecido para sua residência, consulte seu revendedor ou a companhia de energia elétrica local.
- Não sobrecarregue tomadas ou extensões, pois isso pode resultar em risco de incêndio ou de choque elétrico. Tomadas de corrente alternada (CA) ou extensões sobrecarregadas, cabos de alimentação desgastados, isolamento de fios danificado ou rompido e plugues quebrados são perigosos. Eles podem resultar em risco de incêndio ou de choque.
- Disponha os cabos de alimentação de forma que não haja possibilidade de serem pisados ou comprimidos por objetos colocados sobre eles ou apoiados neles. Preste atenção especial aos cabos no local, nas partes em que estão ligados a plugues e receptáculos convenientes, e examine o ponto em que saem do dispositivo.
- Coloque este dispositivo em um local próximo de uma tomada elétrica para que o comprimento do cabo de alimentação seja suficiente.
- Coloque o dispositivo em um local que permita fácil acesso ao desconectar o cabo de alimentação do dispositivo da tomada de CA.

- Não conecte o plugue em uma extensão, receptáculo ou outra tomada a menos que possa ser totalmente inserido, sem nenhuma parte dos pinos fique exposta.
- Coloque este dispositivo em uma superfície estável.
- É recomendável que o cliente instale um protetor contra surtos de tensão CA na tomada de CA à qual este dispositivo será conectado. Isso serve para evitar danos ao dispositivo provocados por raios no local e outros surtos elétricos.
- Adie a instalação até que não haja mais risco de tempestade ou raios em sua região.
- Evite usar um telefone (que não seja sem fio) durante uma tempestade elétrica. Pode haver um risco remoto de choque elétrico provocado por raios. Para maior proteção, retire o dispositivo da tomada e desconecte os cabos, para evitar danos provocados por raios e surtos de energia.
- Este produto é destinado somente para uso em ambientes internos. Não deixe o cabo Ethernet ou telefônico em ambientes externos. A exposição dos cabos a raios pode gerar riscos à segurança e danificar o produto.
- Não cubra o dispositivo nem bloqueie o fluxo de ar para o dispositivo com outros objetos. Mantenha o dispositivo afastado de calor umidade e calor excessivos, sem vibração e poeira.
- Utilize somente as baterias e o cabo de alimentação especificados neste manual. Não descarte as baterias no fogo, pois elas podem explodir. Verifique os códigos locais para obter instruções especiais sobre descarte.
- Limpe o dispositivo com um pano limpo e seco. Nunca use líquidos de limpeza ou produtos químicos semelhantes. Não use limpadores em spray diretamente no dispositivo ou ar comprimido para retirar poeira.
- **CUIDADO**: Para reduzir o risco de incêndio, use apenas cabo para telecomunicações no. 26 AWG ou maior (por exemplo, 24 AWG) certificado relacionado pela UL ou certificado pela CSA, ou equivalente nacional.
- Desconecte o(s) conector(es) do circuito TNV antes de desconectar a energia.
- Desconecte o conector do circuito TNV antes de retirar a tampa.
- Não use este produto perto de água: por exemplo, perto de banheira, lavatório, pia de cozinha ou tanque, em porão úmido ou perto de piscina.
- Não use o telefone perto de um vazamento de gás para comunicar sobre o vazamento.
- Ao concluir qualquer serviço ou reparo neste dispositivo, solicite que o técnico de serviço execute verificações de segurança para determinar se o dispositivo está em condições operacionais seguras.
- Não abra o dispositivo. Não realize manutenção que não esteja contida nas instruções de instalação e solução de problemas. Encaminhe toda a manutenção para assistência técnica qualificada.
- Este dispositivo não deve ser usado em ambientes com mais de 40º C.

**GUARDE ESTAS INSTRUÇÕES**

**Observação para o instalador do sistema TV a cabo:** Este lembrete serve para chamar a atenção do instalador do sistema de TV a cabo para o Artigo 820.93 do NEC (National Electric Code, código nacional de eletricidade dos Estados Unidos), que fornece diretrizes para o aterramento adequado e, em particular, especifica que um cabo coaxial blindado deve ser conectado ao sistema de aterramento da edificação, o mais próximo possível do ponto de entrada do cabo.

## CUIDANDO DO MEIO AMBIENTE POR MEIO DA RECICLAGEM

Quando este símbolo estiver em um produto da Motorola, não descarte o produto juntamente com o resíduo residencial ou comercial.

**Reciclagem do seu equipamento da Motorola**

Não descarte este produto juntamente com o resíduo residencial ou comercial. Alguns países ou regiões, como a União Européia, estabeleceram sistemas de coleta e reciclagem de resíduos elétricos e eletrônicos. Entre em contato com as autoridades locais para obter informações sobre as práticas estabelecidas para a sua região. Se não existirem sistemas de coleta disponíveis, ligue para a assistência técnica da Motorola para obter assistência. Visite www.motorola.com/recycle para obter instruções sobre reciclagem.

## INFORMAÇÕES IMPORTANTES SOBRE O SERVIÇO VOIP

Entre em contato com seu ISP (Internet Service Provider, provedor de serviços de Internet) e/ou com sua municipalidade local para obter informações adicionais sobre como fazer ligações de emergência usando o serviço VoIP em sua região.

Ao utilizar este dispositivo VoIP, você NÃO PODERÁ fazer ligações, inclusive ligações de emergência. Os serviços de localização E911 NÃO estarão disponíveis nas seguintes circunstâncias:

- Sua conexão com o provedor de serviços de banda larga cair, for perdida ou falhar de alguma outra forma.
- Houver falha no fornecimento de energia elétrica.

Ao utilizar este dispositivo VoIP, é possível que você consiga fazer uma ligação de emergência para um operador, mas os serviços de localização E911 talvez não estejam disponíveis nas seguintes circunstâncias:

- Você alterou o endereço físico do seu dispositivo VoIP e não atualizou ou informou de alguma outra forma o seu provedor de serviços VoIP sobre essa alteração.
- Você está usando um número de telefone que não é dos E.U.A.
- Existem atrasos na disponibilização das informações sobre sua localização no banco de dados de informações sobre localização automática local ou através dele.

> ***Observação**: Seu provedor de serviços, e não a Motorola, é responsável pelo fornecimento de serviços telefônicos VoIP neste equipamento. A Motorola não é responsável e se isenta expressamente de quaisquer renúncias, responsabilidades diretas ou indiretas, danos, perdas, reivindicações, demandas, ações, causas de ação, riscos ou prejuízos decorrentes ou relacionados aos serviços fornecidos por este equipamento.*

## DECLARAÇÕES DA FCC

### DECLARAÇÃO SOBRE INTERFERÊNCIA DA FCC

Este equipamento foi testado e considerado em conformidade com os limites para um dispositivo digital Classe B, nos termos da parte 15 das normas da FCC. Esses limites foram criados para fornecer uma proteção razoável contra interferências nocivas em um ambiente residencial. Este equipamento gera, utiliza e pode irradiar energia de radiofreqüência e, caso não seja instalado e usado de acordo com as instruções, poderá provocar interferência nociva às comunicações de rádio. Entretanto, não há garantia de que não ocorrerão interferências em uma instalação específica. Se este equipamento vier a provocar interferências nocivas à recepção de rádio ou televisão, o que pode ser determinado ao ligar e desligar o dispositivo, o usuário deve tentar corrigir a interferência seguindo um ou mais dos procedimentos abaixo:

- Reorientar ou reposicionar a antena receptora.
- Aumentar a distância entre o dispositivo e o receptor.
- Conectar o equipamento a uma tomada de um circuito diferente daquele ao qual está conectado o receptor.
- Consultar o revendedor ou um técnico de rádio/TV experiente para obter ajuda.

Este dispositivo é compatível com as normas da FCC, parte 15. A operação está sujeita às duas seguintes condições: 1) Este dispositivo não pode provocar interferência nociva e (2) Este dispositivo deve aceitar qualquer interferência recebida, inclusive interferências que possam provocar operação indesejada.

**AVISO DA FCC:** Quaisquer alterações ou modificações que não sejam expressamente aprovadas pela Motorola por cumprimento das normas poderão fazer com que o usuário perca a autorização para operar o equipamento.

### DECLARAÇÃO DE EXPOSIÇÃO À RADIAÇÃO DA FCC

Este equipamento é compatível com os limites de exposição à radiação da FCC estabelecidos para um ambiente não controlado. Para estar de acordo com as exigências de exposição à RF da FCC, a distância mínima de separação entre a antena e o corpo da pessoa (incluindo mãos, pulsos, pés e tornozelos) deve ser de 20 cm.

Esse transmissor não pode estar situado no mesmo local ou operado em conjunto com outra antena ou transmissor.

A disponibilidade de alguns canais e/ou faixas de freqüência de operação específicos depende do país e é programada no firmware na fábrica de acordo com os destinos desejados. O usuário final não tem acesso à configuração do firmware.

## DECLARAÇÃO DA INDUSTRY CANADA (IC)

Este dispositivo é compatível com a RSS-210 das normas da Industry Canada. A operação está sujeita às duas seguintes condições:

- Este dispositivo não pode causar interferência e
- Este dispositivo deve aceitar qualquer interferência, inclusive as que possam causar operação indesejável do dispositivo.

Este aparelho digital da Classe B atende à norma canadense ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

## DECLARAÇÃO DE EXPOSIÇÃO À RADIAÇÃO DA IC

**OBSERVAÇÃO IMPORTANTE:** Este equipamento é compatível com os limites de exposição à radiação da IC estabelecidos para um ambiente não controlado. Este equipamento deve ser instalado e operado a uma distância mínima de 20 cm entre o radiador e o seu corpo.

## INFORMAÇÕES SOBRE REDES LOCAIS SEM FIO

Este dispositivo é um produto de rede sem fio que usa a tecnologia de rádio DSSS (Direct Sequence Spread Spectrum, espalhamento espectral por seqüência direta) e OFDMA (Orthogonal Frequency-Division Multiple Access, acesso múltiplo de divisão de freqüência ortogonal).
O dispositivo foi projetado para operar com qualquer outro produto DSSS e OFDMA sem fio que seja compatível com:

- A norma IEEE 802.11 sobre Redes Locais Sem Fio (Revisão B e Revisão G), conforme definido e aprovado pelo IEEE (Institute of Electrical and Electronics Engineers)
- A certificação Wireless Fidelity (Wi-Fi) conforme definida pela WECA (Wireless Ethernet Compatibility Alliance).

## RESTRIÇÕES SOBRE O USO DE DISPOSITIVOS SEM FIO

Em algumas situações ou ambientes, o uso de dispositivos sem fio pode ser restringido pelo proprietário da edificação ou pelos representantes responsáveis da organização. Por exemplo, o uso de equipamentos sem fio em ambientes onde o risco de interferência em outros dispositivos ou serviços é percebido ou identificado como prejudicial.

Se você não tiver certeza da política aplicável para a utilização de equipamentos sem fio em uma organização ou ambiente, deverá pedir autorização para usar o dispositivo antes de ligar o equipamento.

O fabricante não é responsável por interferências de rádio e televisão causadas por modificação não autorizada dos dispositivos incluídos neste produto, ou pela substituição ou ligação de cabos de conexão e equipamentos que não os especificados pelo fabricante. A correção da interferência causada por essa modificação, substituição ou ligação não autorizada é de responsabilidade do usuário.

O fabricante e seus revendedores ou distribuidores autorizados estão isentos de responsabilidade por quaisquer danos ou violações das normas governamentais que possam resultar do não cumprimento dessas diretrizes.

**ADVERTÊNCIAS SOBRE SEGURANÇA:** Este dispositivo permite criar uma rede sem fio. As conexões das redes sem fio podem ser acessadas por usuários não autorizados. Para obter mais informações sobre como proteger sua rede, consulte Configuração da sua rede wireless LAN ou visite o website da Motorola.

## DECLARAÇÃO INTERNACIONAL DE CONFORMIDADE

A empresa, Motorola, Inc., 101 Tournament Drive, Horsham, PA 19044, U.S.A., declara sob sua inteira responsabilidade que o Gateway de Voz Wireless SURFboard Série SVG1501 ao qual esta declaração se refere está em conformidade com uma ou mais das seguintes normas:

| | | |
|---|---|---|
| EN60950-1 | EN 300 328 | EN 301 489-1/-17 |
| EN61000-3-2 | EN61000-3-3 | |

As seguintes cláusulas da(s) diretiva(s) do Conselho da União Européia:

- Diretiva EMC 2004/108/EC
- Diretiva sobre baixa tensão 2006/95/EC
- Diretiva R&TTE 1999/5/EC
- Diretiva sobre equipamentos elétricos e eletrônicos descartados (WEEE) 2002/96/EC
- Diretiva sobre a restrição do uso de determinadas substâncias perigosas em equipamentos elétricos (RoHS) 2002/95/EC

# Índice

**Informações de segurança e normativas**

**Visão geral**
Informações de contato....1
Recursos padrão....1
Opções de LAN do SVG1501....2
Conexão USB (apenas SVG1501U)....2
LAN wireless....3
LAN Ethernet com fio....4
Painel frontal....5
Painel traseiro....6
Etiqueta MAC....7

**Primeiros passos**
Dentro da caixa....8
Antes de começar....9
Registro para serviço....9
Requisitos do sistema....9
Conexão do SVG1501....10
Conexão do SVG1501U....11
Montagem em parede do SVG1501....12
Modelo de montagem em parede....14
Configuração do acesso à Internet....15
Configuração do TCP/IP no Windows XP....15
Configuração do TCP/IP no Windows Vista....15
Verificação do endereço IP no Windows XP....16
Verificação do endereço IP no Windows Vista....16
Renovação do endereço IP....17
Configuração de uma rede Wi-Fi....17

**Configuração básica**
Início do Gerenciador de configuração (CMGR, Configuration Manager) do SVG1501....18
Barra de opções dos menus do SVG1501....19
Como obter ajuda....20
Como sair do Gerenciador de configuração do SVG1501....20

**Páginas Status**
Página do software de status....21
Página de conexão do status....21
Página de segurança do status....22
Alteração da senha padrão do SVG1501....22
Restauração dos padrões de fábrica....23

Página de diagnóstico do status ....23
Utilitário ping ....23
Utilitário Traceroute ....24
Página Registro de eventos de status ....25

**Páginas básicas**
Página de configuração básica ....26
Página DHCP básica ....28
Página DDNS básica ....29
Página básica de backup ....30
Restauração da configuração do SVG1501 ....30
Backup da configuração do SVG1501 ....30

**Páginas avançadas**
Página de opções avançadas ....31
Página avançada Filtro de IP ....33
Página avançada Filtro de MAC ....34
Configuração de um filtro de endereço MAC ....34
Página avançada Filtro de porta ....35
Página avançada Encaminhamento de porta ....36
Página avançada Gatilhos de porta ....37
Página avançada Host DMZ ....38
Configuração do host DMZ ....38
Página avançada Configuração do protocolo de informações de roteamento ....39

**Páginas Firewall**
Página Filtro de conteúdo da Web do firewall ....41
Página Registro local do firewall ....42
Página Registro remoto do firewall ....42

**Páginas Controle dos pais**
Página Configuração do usuário para o controle dos pais ....44
Página Configuração básica do controle dos pais ....46
Página Filtro de hora do dia para o controle dos pais ....47
Página Registro local do controle dos pais ....47

**Páginas Wireless**
Página Rádio wireless 802.11 ....48
Página Rede primária wireless 802.11 ....49
Página avançada wireless 802.11 ....51
Página Controle de acesso wireless 802.11 ....53
Página Multimídia Wi-Fi wireless 802.11 ....54
Página Ponte wireless 802.11 ....55
Configuração da LAN wireless ....56
Criptografia das transmissões da LAN wireless ....56
Instalação de clientes wireless ....57
Instalação de um cliente wireless para o WPA ....58

Configuração de um cliente wireless para o WEP ..... 58
Configuração de um cliente wireless com o nome da rede (SSID) ..... 58

**Páginas VPN**

Página básica VPN ..... 59
Página IPsec VPN ..... 60
Página L2TP/PPTP VPN ..... 64
Página Registro de eventos VPN ..... 65

**Páginas MTA**

Página Status MTA ..... 66
Página DHCP MTA ..... 66
Página QoS MTA ..... 67
Página Provisionamento MTA ..... 68
Página Registro de eventos MTA ..... 69

**Solução de problemas**

Soluções ..... 70
LEDs do painel frontal e Condições de erro ..... 71

**Licença de software**

# 1 Visão geral

O Gateway de Voz Wireless Motorola SURFboard® SVG1501 pode ser usado em residências com um ou mais computadores compatíveis com conectividade wireless para acesso remoto ao gateway de voz wireless.

Este guia do usuário oferece visão geral do produto e informações de definição do SVG1501. Também oferece instruções para instalação do gateway de voz wireless e definição das configurações de LAN, Ethernet, roteador, DHCP, wireless e de segurança.

> ***Observação:*** *Todas as referências ao SVG1501 usadas neste guia também se aplicam ao SVG1501U, ao SVG1501E e ao SVG1501UE, a menos que o contrário seja indicado. Todas as referências ao SVG1501U também se aplicam ao SVG1501UE.*

## Informações de contato

- Para dúvidas ou assistência com o Gateway de Voz Wireless SVG1501, entre em contato com seu provedor de serviços de Internet.
- Para obter informações sobre atendimento ao cliente, suporte técnico ou reivindicações de garantia, consulte o cartão de Informações de Licença, Garantia, Segurança e Normativas do Software do Motorola SVG1501 fornecido com o Gateway de Voz Wireless SVG1501.

## Recursos padrão

O Gateway de Voz Wireless SVG1501 oferece os seguintes recursos:

- Combinação de cinco produtos separados em uma unidade compacta: um cable modem DOCSIS® 2.0, um ponto de acesso wireless IEEE 802.11g (certificado pela Wi-Fi©), conexões Ethernet 10/100Base-T, duas conexões telefônicas de Internet VoIP e um firewall.
- Firewall avançado para maior segurança da rede contra ataques indesejáveis na Internet. Oferece suporte para inspeção do estado, detecção de intrusão, DMZ, prevenção contra ataque por recusa de serviço e NAT (Network Address Translation, conversão do endereço de rede).
- Criptografia de dados e controle de acesso à rede para transmissões wireless
- Fácil instalação wireless e assistente de configuração de segurança
- Cable modem de alta velocidade integrado para acesso contínuo de banda larga
- Uma conexão de banda larga para até 245 computadores

- Acesso wireless IEEE 802.11g para rede doméstica ou rede pequena
- Serviço telefônico VoIP (Voice-over-Internet Protocol) com duas linhas telefônicas
- Conexão de banda larga Wi-Fi (Wireless Fidelity) segura para dispositivos ativados para Wi-Fi
- Quatro portas de uplink 10/100Base-T Ethernet oferecendo suporte para conexões half ou full-duplex com o recurso auto-MDIX
- Conexão USB (Universal Serial Bus) para um único PC (modelos SVG1501U apenas)
- Roteamento para uma WLAN (wireless LAN) ou uma LAN Ethernet com fio
- Servidor DHCP integrado para configurar uma LAN particular Classe C combinada com fio e/ou wireless
- Operação de passagem VPN (Virtual Private Network, rede privada virtual) suportando IPSec, PPTP ou L2TP para conexão segura a computadores remotos na Internet.
- Gerenciador de configuração (CMGR, Configuration Manager) do SVG1501, que oferece fácil definição de configurações wireless, Ethernet, roteador, DHCP e de segurança
- Suporte para modem e fax telefônico
- Serviço telefônico VoIP por meio de sua conexão a cabo oferecendo muitos serviços telefônicos tradicionais, como:
  - Ligações locais e de longa distância
  - Ligações de 3 vias
  - Correio de voz
  - Rediscagem do número
  - Discagem rápida
  - ID do chamador, espera, encaminhamento e retorno de chamadas

# Opções de LAN do SVG1501

Você pode conectar até 245 computadores clientes ao SVG1501 usando uma ou qualquer combinação das seguintes conexões de rede:

- USB (Universal Serial Bus) – Modelos SVG1501U apenas
- LAN wireless (WLAN, Wireless LAN)
- LAN (Local Area Network, rede de área local) Ethernet
- Conexões Wi-Fi com dispositivos ativados para Wi-Fi

## Conexão USB (apenas SVG1501U)

Você pode conectar um único computador executando Windows XP ou Windows Vista à porta USB V2.0 do SVG1501U.

# LAN wireless

Uma rede wireless elimina a necessidade de fios para conexão de computadores em casa ou no escritório. Cada computador ou dispositivo em uma WLAN deve estar ativado para Wi-Fi com um adaptador wireless integrado ou externo.

**Laptops** — Use um adaptador para notebook wireless integrado, um adaptador para slot PCMCIA ou um adaptador USB wireless.

**Desktops** — Use um adaptador PCI wireless, um adaptador USB wireless ou um produto compatível no slot PCI ou porta USB, respectivamente.

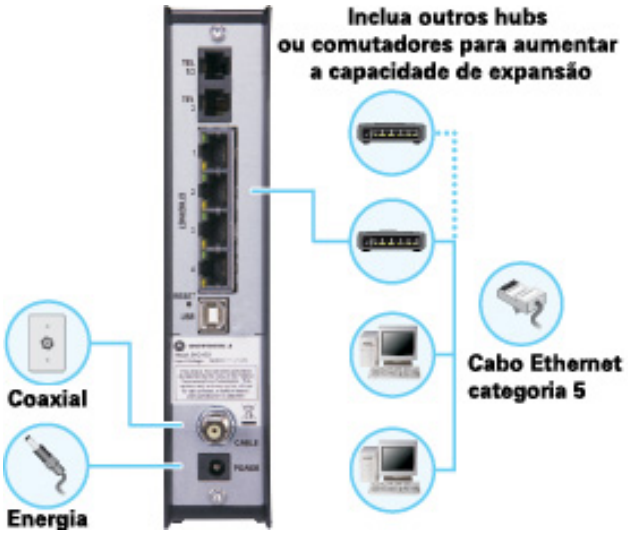

**Amostra de conexões de rede wireless (modelo SVG1501U mostrado)**

Para configurar o SVG1501 em um computador conectado ao SVG1501 via uma Ethernet, execute os procedimentos descritos na seção **Páginas Wireless**. Não tente configurar o SVG1501 usando uma conexão wireless.

A distância máxima de operação wireless depende do tipo de material pelo qual o sinal deve passar e do local do SVG1501 e dos clientes (estações). A Motorola não pode garantir a operação wireless para todas as distâncias suportadas em todos os ambientes.

# LAN Ethernet com fio

Você pode ligar qualquer PC com uma porta LAN Ethernet à conexão Ethernet do SVG1501. Como a porta Ethernet do SVG1501 suporta auto-MDIX, você pode usar um cabo reto ou cruzado para conectar um hub, um comutador ou um computador. Use o cabeamento categoria 5, ou melhor, para todas as conexões Ethernet.



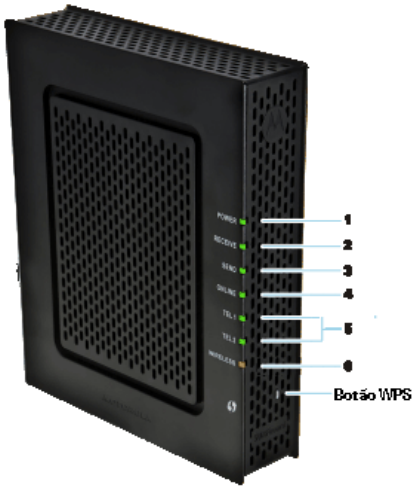

**Amostra de conexão Ethernet com o computador (modelo SVG1501U mostrado)**

Uma LAN Ethernet com fio com mais de quatro computadores requer um ou mais hubs, comutadores ou roteadores. Você pode:

- Conectar um hub ou comutador a qualquer porta Ethernet no SVG1501.
- Usar hubs, comutadores ou roteadores Ethernet para conectar qualquer combinação de até 245 computadores e clientes wireless ao SVG1501.

# Painel frontal

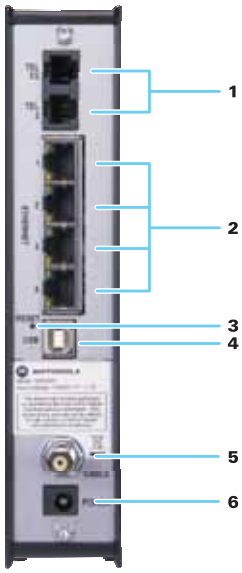
O painel frontal do SVG1501 contém luzes indicadoras e o **botão WPS** que é usado para configurar a WPS (Wi-Fi Protected Security, segurança protegida para Wi-Fi) em clientes compatíveis conectados à rede do SVG1501.




Os indicadores LED do painel frontal do SVG1501 apresentam o seguinte status para energia, comunicações e erros:

| | LED | Piscando | Ligado |
|---|---|---|---|
| 1 | **ENERGIA** | Não aplicável — O LED não pisca | **Verde**: A energia está ligada adequadamente |
| 2 | **RECEBER** | Verificando uma conexão de canal downstream | **Verde**: O canal downstream está conectado |
| 3 | **ENVIAR** | Verificando uma conexão de canal upstream | **Verde**: O canal upstream está conectado |
| 4 | **ON-LINE** | Verificando a conexão com a Internet; transmitindo ou recebendo dados na Internet | **Verde**: Processo de inicialização concluído |
| 5 | **TEL. 1**<br>**TEL. 2** | O telefone está fora do gancho; discagem ou chamada em andamento | **Verde**: O telefone está conectado e ativado; no gancho |
| 6 | **SEM FIO** | **Verde**: Wi-Fi ativado com atividade de dados wireless criptografada. Piscadas longas/curtas indicam emparelhamento wireless com placa do cliente em andamento.<br>**Âmbar**: Wi-Fi ativado com atividade de dados wireless não-criptografada. | **Verde**: Emparelhamento wireless estabelecido com sucesso entre o SVG1501 e outro dispositivo ativado para Wi-Fi em sua rede; telefone celular, PDA, laptop, etc.<br>**Âmbar**: Emparelhamento móvel bem-sucedido. Fica verde após cinco minutos. |

# Painel traseiro




Os painéis traseiros do SVG1501 e do SVG1501U (mostrados abaixo) contêm a seguinte porta e conectores de cabeamento:

| | Item | Descrição |
|---|---|---|
| 1 | **TEL1/2**<br>**TEL 2** | Conexão VoIP para um telefone de uma ou duas linhas<br>Conexão VoIP para um telefone de uma linha |
| 2 | **ETHERNET**<br>**1 2 3 4** | Use qualquer porta Ethernet para conectar um computador equipado com Ethernet, hub, ponte ou comutador usando um cabo RJ-45.<br><br>**LED de atividade** – LED verde define a atividade do conector Ethernet.<br>Quando a LED está LIGADA, não há tráfego de dados e uma conexão está estabilizada.<br>Quando a LED está PISCANDO, os dados estão sendo transmitidos up ou downstream.<br>Quando a LED está DESLIGADA, a unidade não está ligada ou não há conexão Ethernet.<br><br>**LED 10/100** – Indica a taxa de dados da conexão.<br>Quando a LED verde está LIGADA, a conexão está com uma taxa 100Base-T.<br>Quando a LED âmbar está LIGADA, a conexão está com uma taxa 10Base-T. |

| | Item | Descrição |
|---|---|---|
| 3 | **RESET (REDEFINIR)** | Redefine o gateway de voz wireless. Pode demorar de 5 a 30 minutos para encontrar e bloquear os canais de comunicação apropriados.<br><br>Pressione e mantenha pressionado o botão REDEFINIR por cinco segundos ou mais para restaurar as definições padrão de fábrica. |
| 4 | **USB** | Para o Windows apenas, você pode usar a porta USB para conectar um PC ao SVG1501U. Você não pode conectar um computador Macintosh ou UNIX® à porta USB no SVG1501U.<br><br>**Observação**: O conector USB está disponível apenas nos modelos SVG1501U. |
| 5 | **CABLE (CABO)** | Conecta o SVG1501 a uma tomada de cabo. |
| 6 | **POWER (ENERGIA)** | Fornece energia para o SVG1501. |

# Etiqueta MAC

A etiqueta MAC (Media Access Control, controle de acesso a mídia) do SVG1501, localizada na parte inferior do SVG1501, contém um valor exclusivo de 48 bits que identifica cada dispositivo de rede Ethernet. Para receber o serviço de dados, você precisará fornecer o endereço MAC marcado **HFC MAC ID** para seu provedor de serviços de Internet. Para receber o serviço VoIP, você precisa fornecer o **MTA MAC ID** para seu provedor VOIP.

# 2 Primeiros passos

## Dentro da caixa

Verifique se os seguintes itens estão incluídos na caixa com o SVG1501:

| Item | | Descrição |
|---|---|---|
| **Cabo de alimentação** |  | Conecta o SVG1501 a uma tomada elétrica de CA |
| **Cabo 10/100Base-T Ethernet** |  | Conecta o SVG1501 à rede via porta Ethernet. O cabo deve ser um Cat 5 padrão ou maior. |
| **Licença do software e cartão normativo** |  | Contém as informações de licença, garantia e segurança do software para o SVG1501. |
| **CD-ROM de instalação do SVG1501** |  | Contém o Assistente Wi-Fi do SVG1501, o contrato de licença do software, Guias do Usuário do SVG1501 em vários idiomas e drivers USB (apenas para os modelos SVG1501U). |
| **Folha de instalação do SVG1501** |  | Apresenta informações básicas para configuração do SVG1501 |

Será necessário um cabo coaxial de 75 ohm com conectores do tipo F para conectar o SVG1501 à tomada mais próxima. Se a TV estiver conectada à tomada, pode ser necessário um divisor de 5 a 900 MHz de RF e dois cabos coaxiais adicionais para usar a TV e o SVG1501.

# Antes de começar

Tome as seguintes precauções antes de instalar o SVG1501:

- Aguarde até que não haja mais risco de tempestade ou raios em sua região.
- Para evitar possíveis choques, sempre desconecte o cabo de alimentação da tomada ou de outra fonte de alimentação antes de desconectá-lo do painel traseiro do SVG1501.
- Para evitar superaquecimento do SVG1501, não obstrua os orifícios de ventilação nas laterais da unidade. Não abra a unidade. Encaminhe toda a manutenção para o provedor de serviços de Internet.
- Não conecte os cabos Ethernet e USB ao computador ao mesmo tempo. Conecte um ou o outro.

Verifique se você possui os cabos, adaptadores e software do adaptador necessários. Verifique se os drivers corretos estão instalados para o adaptador Ethernet em cada computador da rede. Para obter informações sobre configuração da WLAN, consulte Configuração da LAN wireless.

## Registro para serviço

Você deve se registrar com um provedor de serviços de Internet para acessar a Internet e outros serviços on-line.

- Para o serviço de dados, você precisará fornecer o endereço MAC marcado **HFC MAC ID** na Etiqueta do MAC.

## Requisitos do sistema

Seu computador deve atender aos seguintes requisitos mínimos:

- Computador com processador classe Pentium© ou melhor
- Sistema operacional Windows XP, Windows Vista, Macintosh ou UNIX com CD-ROM disponível do sistema operacional
- Qualquer navegador da Web, como Microsoft Internet Explorer, Netscape Navigator® ou Mozilla® Firefox®

# Conexão do SVG1501

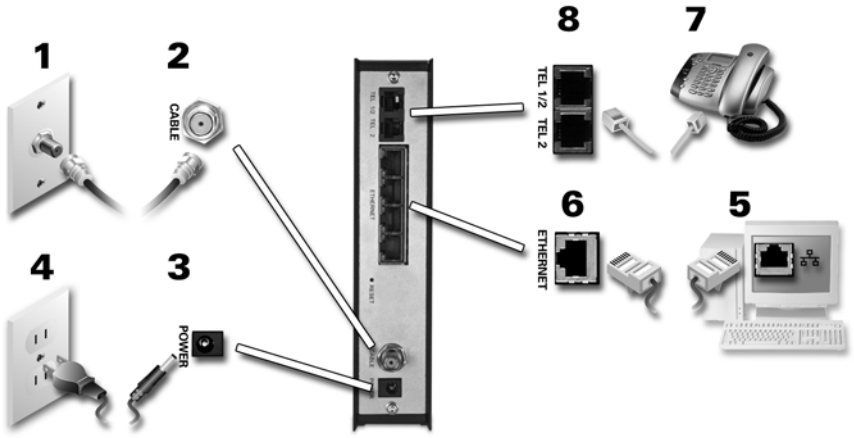
> ***CUIDADO:*** *Para reduzir o risco de incêndio, use apenas cabo para telecomunicações no. 26 ou maior certificado relacionado pela UL ou certificado pela CSA ou equivalente nacional para conectar uma linha telefônica ao SVG1501.*
>
> *Entre em contato com seu provedor de serviços antes de ligar seu Motorola SVG1501 na conexão telefônica existente. Não conecte o fio do telefone a um serviço telefônico tradicional (PSTN).*

Antes de iniciar, verifique se o computador está ligado e se o cabo de alimentação do SVG1501 está desconectado.

1. Conecte o cabo coaxial à tomada ou divisor do cabo e depois ao conector do cabo no SVG1501. Aperte os conectores manualmente para evitar danos.
2. Conecte o cabo de alimentação à porta de energia no SVG1501 e depois a uma tomada de parede elétrica.

   Isso liga o gateway automaticamente. Não é necessário desconectar o gateway quando não estiver em uso. Da primeira vez que você conectar o SVG1501, aguarde de 5 a 30 minutos para encontrar e bloquear os canais de comunicação apropriados.
3. Conecte o cabo Ethernet à porta Ethernet no computador e à porta Ethernet no gateway.
4. Conecte o cabo telefônico de um telefone com uma ou duas linhas ao telefone e depois à porta TEL 1/2 na parte traseira do SVG1501.

> ***Observação****: Entre em contato com um provedor de serviços VoIP para ativar este serviço.*



5. Para um segundo telefone, conecte o fio do telefone de uma linha à porta TEL 2 na parte traseira do SVG1501.
6. Verifique se as LEDs no painel frontal passam pela seguinte seqüência:

**Atividade de LED do SVG1501 durante a inicialização**

| LED | Descrição |
|---|---|
| **POWER (ENERGIA)** | Liga quando a energia de CA é conectada ao SVG1501.<br>Indica que a energia está ligada adequadamente. |
| **RECEIVE (RECEBER)** | Pisca ao verificar o canal de recebimento downstream.<br>Muda para verde constante quando o canal de recebimento está bloqueado. |
| **SEND (ENVIAR)** | Pisca ao verificar o canal de envio upstream.<br>Muda para verde constante quando o canal de envio está bloqueado. |
| **ONLINE (ON LINE)** | Pisca durante o registro e a configuração do SVG1501.<br>Muda para verde constante quando o SVG1501 está registrado. |

# Conexão do SVG1501U

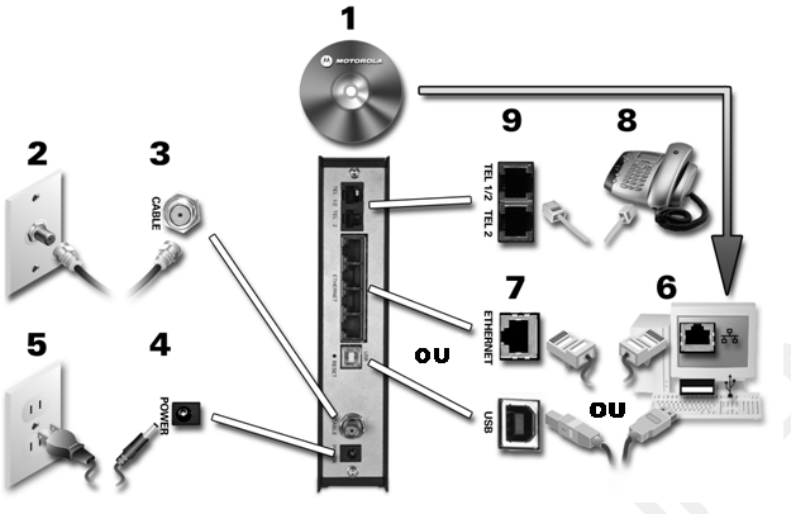
> ***CUIDADO:*** *Antes de conectar o cabo USB ao SVG1501U, carregue o CD-ROM de Instalação do SVG1501 na unidade de CD-ROM.*
>
> *Não conecte os cabos Ethernet e USB ao computador ao mesmo tempo.*

Antes de iniciar, verifique se o computador está ligado e se o cabo de alimentação do SVG1501U está desconectado.

1. Insira o CD-ROM de Instalação do SVG1501 na unidade de CD-ROM e instale os drivers USB aplicáveis.
2. Conecte uma extremidade do cabo coaxial à tomada ou divisor do cabo.
3. Conecte a outra extremidade do cabo coaxial ao conector do cabo no SVG1501U. Aperte os conectores manualmente para evitar danos.
4. Conecte o cabo de alimentação à porta de energia do SVG1501U.
5. Conecte a outra extremidade do cabo de alimentação a uma tomada elétrica.

   Isso liga o gateway automaticamente. Não é necessário desconectar o gateway quando não estiver em uso. Da primeira vez que você conectar o SVG1501U, aguarde de 5 a 30 minutos para encontrar e bloquear os canais de comunicação apropriados.
6. Conecte o cabo USB ou Ethernet à porta apropriada no computador.

7. Conecte a outra extremidade do cabo USB ou Ethernet à porta apropriada no gateway.




8. Conecte o cabo telefônico de uma ou duas linhas ao telefone.
9. Conecte a outra extremidade do cabo telefônico de um telefone com uma ou duas linhas à porta TEL 1/2 na parte traseira do gateway.

> ***Observação***: *Entre em contato com um provedor de serviços VoIP para ativar este serviço.*

10. Para um segundo telefone, conecte o fio do telefone de uma linha à porta TEL 2 na parte traseira do SVG1501.
11. Verifique se as LEDs no painel frontal passam pela seqüência correta; consulte Atividade de LED do SVG1501 durante a inicialização.

# Montagem em parede do SVG1501

Opcionalmente, é possível montar o SVG1501 na parede:

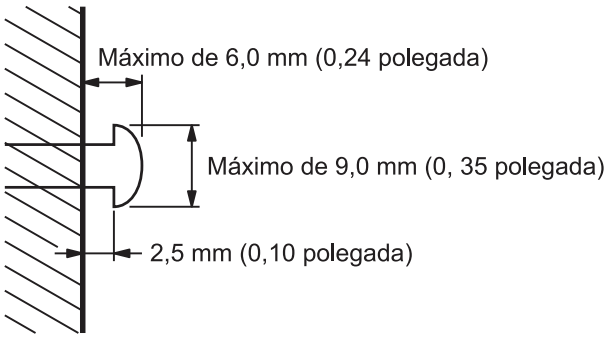
- Localize a unidade, conforme especificado pelos códigos local ou nacional, que controlam os serviços de TV a cabo e comunicações residenciais ou empresariais.
- Siga todos os padrões locais para instalação de uma unidade de interface de rede /dispositivo de interface de rede (NIU/NID, Network Interface Unit/Network Interface Device).
- Verifique se o cabo de alimentação de CA está desconectado da tomada e se todos os cabos foram removidos da parte traseira do SVG1501 antes de iniciar a instalação.
- Decida se deseja montar o SVG1501 horizontal ou verticalmente.

*Se possível, monte a unidade em concreto, alvenaria, um montante de madeira ou algum outro material de parede sólido. Use apoios, se necessário (por exemplo, se precisar montar a unidade em parede de gesso).*

> ***CUIDADO:*** *Antes de fazer furos, verifique a estrutura para saber se não há riscos de danificar as linhas de água, gás ou eletricidade.*

Faça o seguinte para montar o SVG1501 na parede:

1. Imprima uma cópia do Modelo de montagem em parede.
2. Meça o modelo impresso com uma régua para verificar se é do tamanho correto.
3. Use um perfurador central para marcar o centro dos orifícios.
4. Na parede, localize as marcas dos orifícios de montagem.
5. Faça furos com pelo menos 1 ½ polegada de profundidade (3,8 cm). Use parafusos M3,5 x 38 mm (#6 x 11/2 polegada) com uma superfície plana e diâmetro máximo da cabeça de 9,0 mm para montar o SVG1501.
6. Com uma chave de fenda, gire cada parafuso até perfure a parede, conforme mostrado na seguinte ilustração de dimensões do parafuso de montagem em parede.




   Deve haver uma distância de 0,10 polegada (2,5 mm) entre a parede e a parte inferior da cabeça do parafuso.
7. Coloque o SVG1501 de forma que os buracos da fechadura na parte traseira da unidade estejam alinhados acima dos parafusos de montagem.
8. Deslize o SVG1501 para baixo até que pare contra a parte superior da abertura do buraco da fechadura.
9. Após a montagem, reconecte a entrada do cabo coaxial e conexão Ethernet.
10. Conecte o cabo de alimentação ao conector +12VDC no gateway de voz e à tomada elétrica.
11. Roteie os cabos para evitar riscos de segurança.

## Modelo de montagem em parede

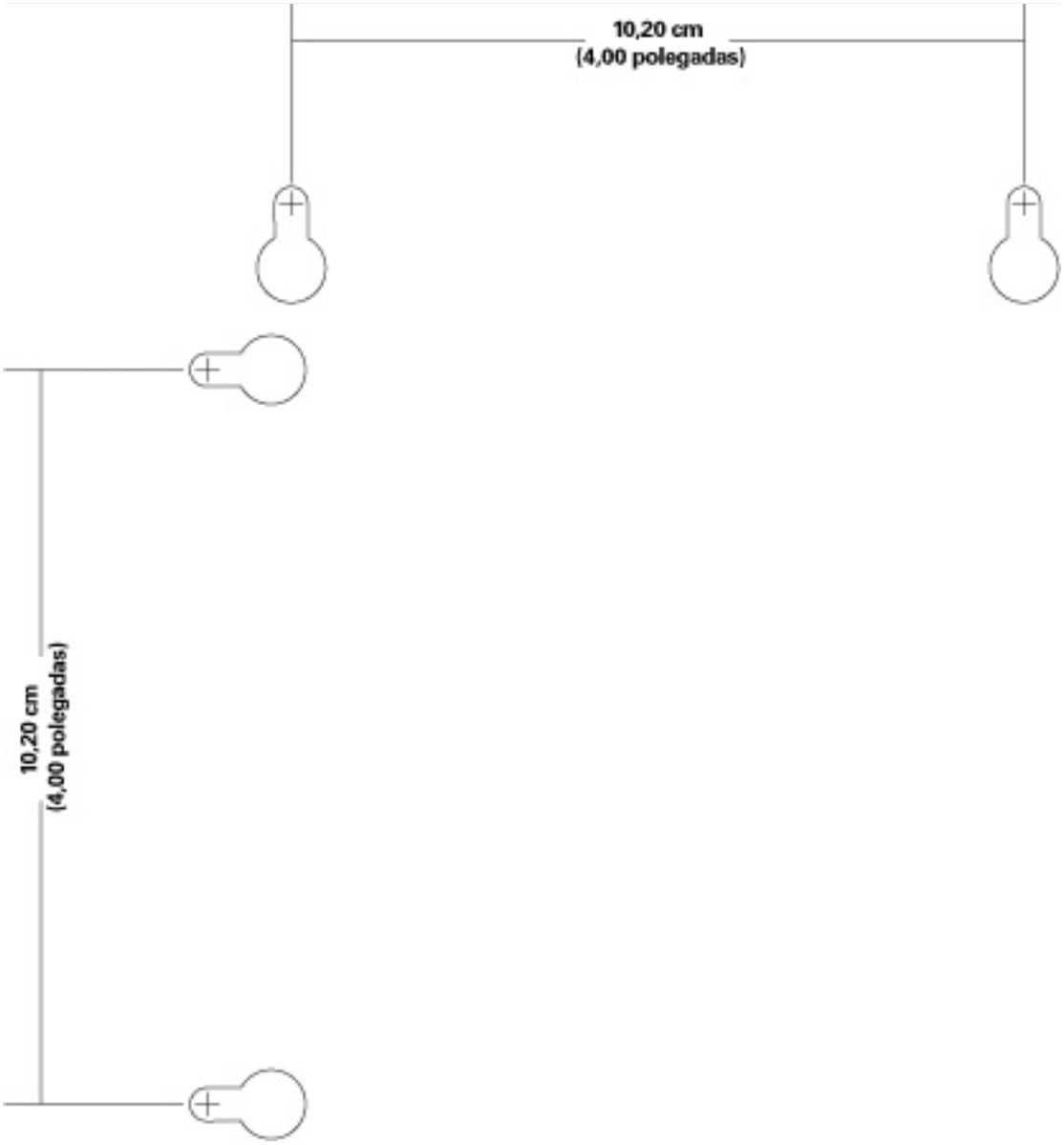



**Figura 1 - Modelo de montagem em parede**

# Configuração do acesso à Internet

Depois de instalar o SVG1501, verifique se é possível se conectar à Internet. Você pode recuperar um endereço IP para a interface de rede de seu computador usando uma das seguintes opções:

- Recuperar o endereço IP e o endereço DNS definidos estaticamente
- Recuperar automaticamente o endereço IP usando o servidor DHCP de rede

O Gateway de Voz Wireless Motorola SVG1501 oferece um servidor DHCP em sua LAN. A Motorola recomenda que você configure a LAN para obter os IPs para a LAN e o servidor DNS automaticamente.

Verifique se todos os computadores na LAN estão configurados para TCP/IP. Depois de configurar o TCP/IP no computador, verifique o endereço IP.

> ***Observação**: Para sistemas UNIX ou Linux, siga as instruções na documentação do usuário aplicável.*

## Configuração do TCP/IP no Windows XP

1. Abra o **Painel de controle**.
2. Clique duas vezes em **Conexões de rede** para listar as conexões discada e LAN ou de Internet de alta velocidade.
3. Clique com o botão direito do mouse na conexão de rede com a interface de rede.
4. Selecione **Propriedades** no menu suspenso para exibir a janela Propriedades da conexão de área local. Verifique se Protocolo da Internet (TCP/IP) está marcado.
5. Selecione **Protocolo da Internet (TCP/IP)** e clique em **Propriedades** para exibir a janela Propriedades do Protocolo da Internet (TCP/IP).
6. Selecione **Obter um endereço IP automaticamente** e **Obter endereço do servidor DNS automaticamente**.
7. Clique em **OK** para salvar as configurações do TCP/IP e saia da janela Propriedades do TCP/IP.
8. Feche a janela Propriedades da conexão de área local e saia do Painel de controle.
9. Ao concluir a configuração do TCP/IP, continue com Verificando o endereço IP no Windows XP.

## Configuração do TCP/IP no Windows Vista

1. Abra o **Painel de controle**.
2. Clique em **Rede e Internet** para exibir a janela Rede e Internet.
3. Clique em **Central de redes e compartilhamento** para exibir a janela Rede e Centro de compartilhamento.
4. Clique em **Gerenciar conexões de rede** para exibir a janela Conexões LAN ou de Internet de alta velocidade.

5. Clique com o botão direito do mouse na conexão de rede com a interface de rede que deseja alterar.
6. Clique em **Propriedades** para exibir a janela Propriedades da conexão de área local.

   O Vista pode solicitar uma senha ou confirmação de administrador. Digite a senha ou confirmação e, em seguida, clique em **Continuar**.
7. Clique na guia **Rede** e, em seguida, selecione **Protocolo da Internet Versão 4 (IPv4)**.
8. Clique em **Propriedades** para exibir a janela Propriedades do Protocolo da Internet Versão 4 (TCP/IPv4).
9. Selecione **Obter um endereço IP automaticamente** e **Obter endereço do servidor DNS automaticamente**.
10. Clique em **OK** para salvar as configurações do TCP/IP e feche a janela Propriedades do Protocolo da Internet Versão 4 (TCP/IPv4).
11. Clique em **OK** para fechar a janela Propriedades da conexão de área local.
12. Feche as janelas restantes e saia do Painel de controle.
13. Ao concluir a configuração do TCP/IP, continue com Verificando o endereço IP no Windows Vista.

## Verificação do endereço IP no Windows XP

Para verificar o endereço IP:

1. No desktop do Windows, clique em **Iniciar**.
2. Selecione **Executar**. A janela Executar é exibida.
3. Digite **cmd** e clique em **OK**.
4. Digite **ipconfig** e pressione **ENTER** para exibir a configuração do IP.

Se for exibido um endereço IP de configuração automática, isso indica possíveis problemas de cabo de rede ou uma conexão inadequada entre o computador e o SVG1501.

Verifique o seguinte:

- Suas conexões de cabo
- Se é possível assistir aos canais da TV a cabo na televisão

Depois de verificar com sucesso as conexões de cabo e se a TV a cabo está funcionando corretamente, você pode renovar seu endereço IP.

## Verificação do endereço IP no Windows Vista

Faça o seguinte para verificar o endereço IP:

1. No desktop do Windows, clique em **Iniciar**.
2. Clique em **Todos os Programas**.
3. Clique em **Acessórios**.
4. Clique em **Prompt de comandos** para abrir uma janela do prompt de comandos.
5. Digite **ipconfig** e pressione **Enter** para exibir o endereço IP.

Se for exibido um endereço IP de configuração automática, isso indica uma conexão inadequada entre o computador e o SVG1501 ou possíveis problemas de cabo de rede.

## Renovação do endereço IP

Para renovar o endereço IP no Windows XP ou Windows Vista:

1. Abra uma janela do prompt de comandos.
2. No prompt de comandos, digite **ipconfig /renew** e pressione **ENTER** para obter um novo endereço IP.
3. Digite **exit** e pressione **ENTER** para fechar a janela do prompt de comandos.

Se mesmo após a execução desse procedimento seu computador ainda não conseguir acessar a Internet, entre em contato com seu provedor de serviços de cabo para obter assistência.

# Configuração de uma rede Wi-Fi

Faça o seguinte para configurar uma rede Wi-Fi usando o botão WPS no SVG1501:

1. Ligue o Gateway de Voz Wireless SVG1501.
2. Ligue os dispositivos ativados para WPS que você deseja que tenham acesso à rede, como um PC, um roteador ou um telefone.

   A rede Wi-Fi detectará automaticamente os dispositivos WPS.
3. Pressione o botão **WPS** no SVG1501.
4. Se aplicável, pressione o botão **WPS** nos outros dispositivos WPS.

# 3 Configuração básica

Para operação normal, não é necessário alterar a maioria das configurações padrão.

> ***CUIDADO:*** *Para impedir configuração não autorizada, altere a senha padrão imediatamente ao configurar o SVG1501 pela primeira vez. Consulte Alteração da senha padrão do SVG1501.*
>
> *Firewalls não são seguros. Escolha a política do firewall mais segura possível. Consulte Páginas Firewall para obter mais informações.*

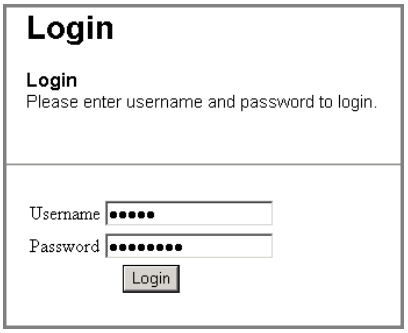
## Início do Gerenciador de configuração (CMGR, Configuration Manager) do SVG1501

Use o Gerenciador de configuração do SVG1501 para alterar e exibir configurações no SVG1501.

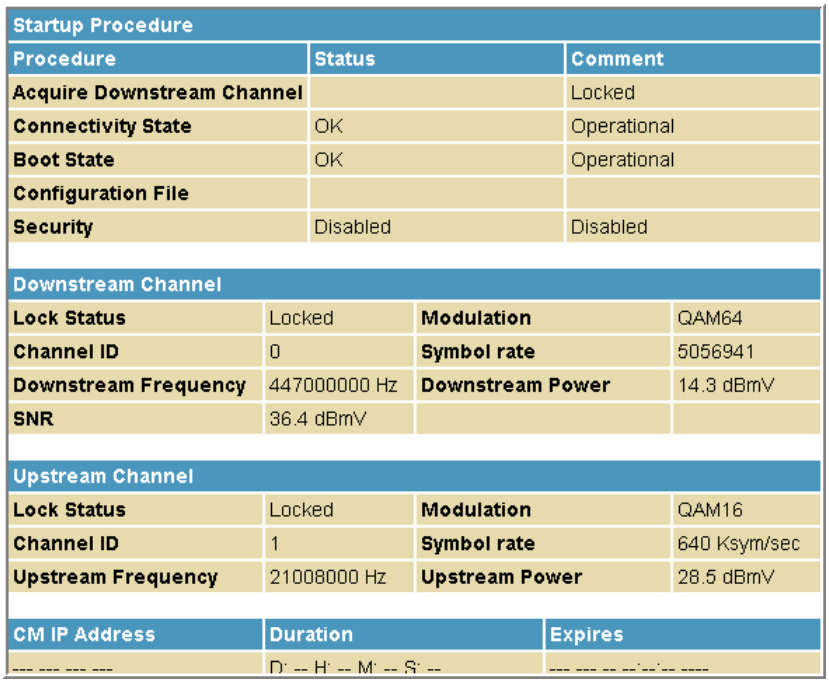
1. Abra o navegador da Web em um computador conectado ao SVG1501 por uma conexão Ethernet.

> ***Nota:*** *Não tente configurar o SVG1501 usando uma conexão wireless.*

2. No campo Address (Endereço) ou Location (Local) do navegador, digite **http://192.168.0.1** e pressione **ENTER**.
3. Digite **admin** no campo Username (Nome de usuário) (este campo diferencia maiúsculas e minúsculas).
4. Digite **motorola** no campo Password (Senha) (este campo diferencia maiúsculas e minúsculas).




5. Clique em **Login** para exibir a página Conexão de status do SVG1501.



| Startup Procedure | | |
|---|---|---|
| **Procedure** | **Status** | **Comment** |
| **Acquire Downstream Channel** | | Locked |
| **Connectivity State** | OK | Operational |
| **Boot State** | OK | Operational |
| **Configuration File** | | |
| **Security** | Disabled | Disabled |

| Downstream Channel | | | |
|---|---|---|---|
| **Lock Status** | Locked | **Modulation** | QAM64 |
| **Channel ID** | 0 | **Symbol rate** | 5056941 |
| **Downstream Frequency** | 447000000 Hz | **Downstream Power** | 14.3 dBmV |
| **SNR** | 36.4 dBmV | | |

| Upstream Channel | | | |
|---|---|---|---|
| **Lock Status** | Locked | **Modulation** | QAM16 |
| **Channel ID** | 1 | **Symbol rate** | 640 Ksym/sec |
| **Upstream Frequency** | 21008000 Hz | **Upstream Power** | 28.5 dBmV |

| CM IP Address | Duration | Expires |
|---|---|---|
| --- --- --- --- | D: -- H: -- M: -- S: -- | --- --- -- --:--:-- ---- |

A página Status Connection (Conexão de status) apresenta informações de status do canal downstream e upstream de RF na conexão de rede do SVG1501.

Se você tiver problemas ao iniciar o Gerenciador de configuração do SVG1501, consulte Solução de problemas para obter mais informações.

# Barra de opções dos menus do SVG1501

A barra de opções dos menus do SVG1501 é exibida na parte superior da janela SVG1501 Configuration Manager (Gerenciador de configuração do SVG1501).


**Barra de opções dos menus do Gerenciador de configuração**

| Páginas de opções de menus | Função |
|---|---|
| **Status** | Apresenta informações sobre o hardware e software do SVG1501, endereço MAC, endereço IP do gateway de voz, número de série e informações relacionadas. Páginas adicionais fornecem ferramentas de diagnóstico e permitem alterar o nome de usuário e senha do SVG1501. |
| **Basic (Básico)** | Exibe e define dados de configuração relacionados ao IP do SVG1501, incluindo Configuração de rede, Tipo de conexão WAN, DHCP e DDNS. |

| Páginas de opções de menus | Função |
|---|---|
| **Advanced (Avançado)** | Configura e monitora como o SVG1501 roteia o tráfego IP |
| **Firewall** | Configura e monitora o firewall do SVG1501 |
| **Parental Control (Controle dos pais)** | Configura e monitora o recurso de controle dos pais do SVG1501 |
| **Wireless** | Configura e monitora os recursos de rede wireless do SVG1501 |
| **VPN** | Configura e monitora a operação do SVG1501 com um VPN |
| **MTA** | Monitora os recursos telefônicos do SVG1501 |
| **Logout** | Sai do Gerenciador de configuração do SVG1501 |

# Como obter ajuda

Para recuperar informações de ajuda para qualquer opção do menu, clique em **Help** (Ajuda) nessa página.

# Como sair do Gerenciador de configuração do SVG1501

Para efetuar logoff e fechar o Gerenciador de configuração do SVG1501:

- Clique em **Logout** na barra de opções do menu do SVG1501.

# 4 Páginas Status

Use as páginas Status do SVG1501 para obter informações sobre o hardware e software, endereço MAC, endereço IP do cable modem e número de série do SVG1501 e para monitorar a conexão do sistema de cabo, acessar ferramentas de diagnóstico adicionais e alterar o nome de usuário e senha do SVG1501.

## Página do software de status

Exibe informações sobre a versão do hardware, versão do software, endereço MAC, endereço IP do cable modem, número de série, tempo de "atividade" do sistema e status de registro da rede.

| Information | |
|---|---|
| Standard Specification Compliant | DOCSIS 2.0 |
| Hardware Version | 1 |
| Software Version | SVG1501E-2.9.9.9-LAB-98-98-SH |
| Cable Modem MAC Address | 00:1e:5a:8c:e1:1a |
| Cable Modem Serial Number | 150100000000000000000003 |
| CM certificate | Installed |
| **Status** | |
| System Up Time | 25 days 04h:59m:58s |
| Network Access | Denied |
| Cable Modem IP Address | ---.---.---.--- |

## Página de conexão do status

Verifique o status da conectividade de rede do HFC e do IP do SVG1501.

- Clique no botão **Refresh** (Atualizar) no navegador da Web para atualizar as informações.

| Startup Procedure | | |
|---|---|---|
| Procedure | Status | Comment |
| Acquire Downstream Channel | | Locked |
| Connectivity State | OK | Operational |
| Boot State | OK | Operational |
| Configuration File | | |
| Security | Disabled | Disabled |

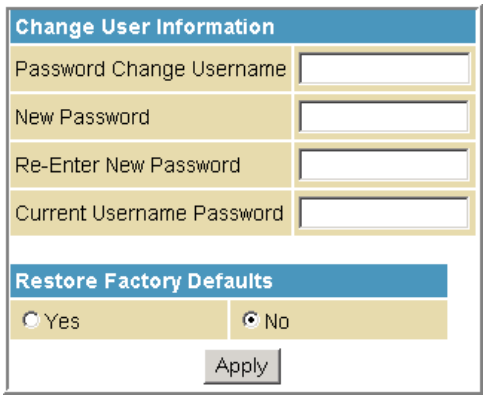
| Downstream Channel | | | |
|---|---|---|---|
| Lock Status | Locked | Modulation | QAM64 |
| Channel ID | 0 | Symbol rate | 5056941 |
| Downstream Frequency | 447000000 Hz | Downstream Power | 13.1 dBmV |
| SNR | 37.7 dBmV | | |

| Upstream Channel | | | |
|---|---|---|---|
| Lock Status | Locked | Modulation | QAM16 |
| Channel ID | 1 | Symbol rate | 640 Ksym/sec |
| Upstream Frequency | 21008000 Hz | Upstream Power | 31.0 dBmV |

| CM IP Address | Duration | Expires |
|---|---|---|
| ---.---.---.--- | D: -- H: -- M: -- S: -- | --- --- -- --:--:-- ---- |

# Página de segurança do status

Define os privilégios de acesso do administrador alterando o nome de usuário e senha do SVG1501 e redefina o nome de usuário e a senha para a definição padrão.




## Alteração da senha padrão do SVG1501

> ***CUIDADO:*** *Para impedir configuração não autorizada, altere a senha padrão imediatamente ao configurar o Motorola SVG1501pela primeira vez.*

1. No campo Password Change Username (Nome de usuário da alteração de senha), digite seu novo Nome de usuário.
2. No campo New Password (Nova senha), digite sua nova senha (este campo diferencia maiúsculas e minúsculas).
3. No campo New Password (Nova senha), digite sua nova senha (este campo diferencia maiúsculas e minúsculas).
4. No campo Current Username Password (Senha do nome de usuário atual), digite a senha antiga.
5. Selecione **Yes** (Sim) se deseja redefinir o nome de usuário e a senha para as configurações originais de fábrica.
6. Clique em **Apply** (Aplicar) para atualizar a senha do nome de usuário.

> ***Nota:*** *Você deve efetuar login com o nome de usuário,* ***admin****, e a senha padrão,* ***motorola****, depois de aplicar alteração Restaurar configurações de fábrica.*

## Restauração dos padrões de fábrica

Para redefinir o nome de usuário e a senha para as configurações originais de fábrica:

1. Selecione **Yes** (Sim) e, em seguida, clique em **Apply** (Aplicar).
2. Efetue login com o nome de usuário, **admin**, e a senha padrão, **motorola**, depois de aplicar esta alteração. Todas as entradas diferenciam maiúsculas e minúsculas.

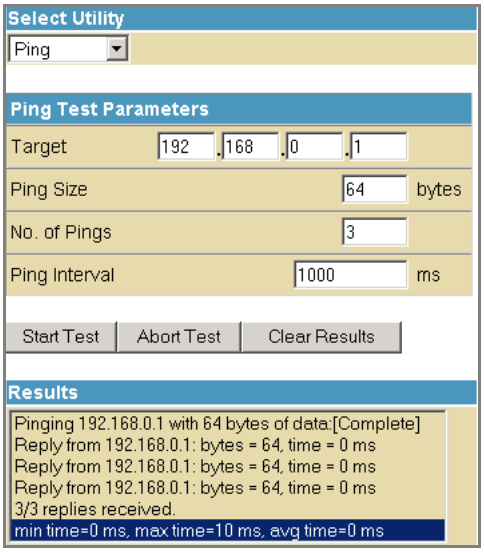
# Página de diagnóstico do status

Use as seguintes ferramentas de diagnóstico para solucionar problemas de conectividade IP:

- Ping (LAN)
- Traceroute (WAN)

## Utilitário ping

Use o Ping (Packet InterNet Groper) para verificar a conectividade entre o SVG1501 e outros dispositivos na LAN do SVG1501 enviando um pequeno pacote de dados e aguardando uma resposta. Uma resposta do Ping confirma que o computador está conectado ao SVG1501.




### Teste da conectividade de rede com o SVG1501

Para verificar a conectividade entre o SVG1501 e outros dispositivos na LAN do SVG1501, execute o seguinte teste:

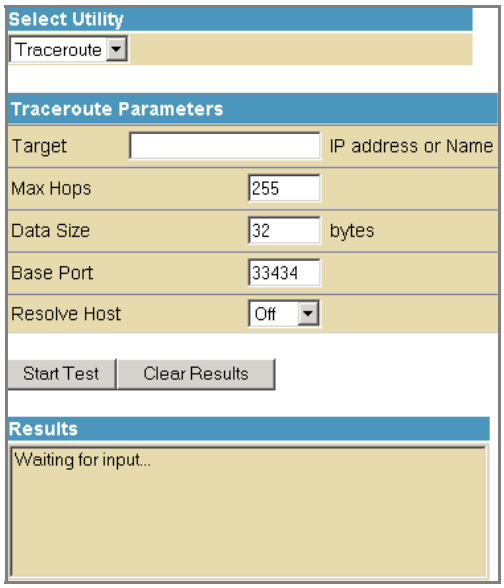
1. Selecione **Ping** na lista suspensa Select Utility (Selecionar utilitário).
2. Digite o endereço IP do computador no qual você deseja executar o Ping no campo Target (Destino).

3. Digite o tamanho do pacote de dados em bytes no campo Ping Size (Tamanho do ping).
4. Digite o número de tentativas de ping no campo No. of Pings (Número de pings).
5. Digite o tempo entre as operações de envio de Ping em milissegundos no campo Ping Interval (Intervalo de ping).
6. Clique em **Start Test** (Iniciar teste) para começar a operação de Ping. Os resultados do Ping serão exibidos no painel Results (Resultados).
7. Você pode clicar em **Abort Test** (Interromper teste) a qualquer momento durante o teste para parar a operação de Ping.
8. Repita as etapas 2 a 6 para cada dispositivo do qual deseja executar ping.

Ao concluir, clique em **Clear Results** (Limpar resultados) para excluir os resultados do Ping no painel Results (Resultados).

## Utilitário Traceroute

Use o Traceroute para mapear o caminho de rede do Gerenciador de configuração do SVG1501 para um host público.




1. Digite o endereço IP ou o Nome do host do computador que deseja usar como destino para a operação Traceroute no campo Target (Destino).
2. Digite o número máximo de hops que a operação Traceroute executa antes de parar no campo Max Hops (Máximo de hops).
3. Digite o tamanho do pacote de dados em bytes no campo Data Size (Tamanho dos dados).
4. Defina o número da porta UDP de base usado pelo Traceroute no campo Base Port (Porta de base). O padrão é **33434**. Se uma porta UDP não estiver disponível, esse campo poderá ser usado para especificar um intervalo de portas não usadas.

5. No campo Resolve Host (Resolver host), selecione **On** (Ativado) para listar os nomes de hosts encontrados durante a operação Traceroute ou selecione **Off** (Desativado) para listar apenas os endereços IP de hosts.
6. Depois de inserir os parâmetros do Traceroute, clique em **Start Test** (Iniciar teste) para iniciar a operação Traceroute. Os resultados do Traceroute serão exibidos no painel Results (Resultados).
7. Ao concluir, clique em **Clear Results** (Limpar resultados) para excluir os resultados do Traceroute no painel Results (Resultados).

# Página Registro de eventos de status

Reveja os eventos críticos do sistema em ordem cronológica no registros de Eventos do SNMP.

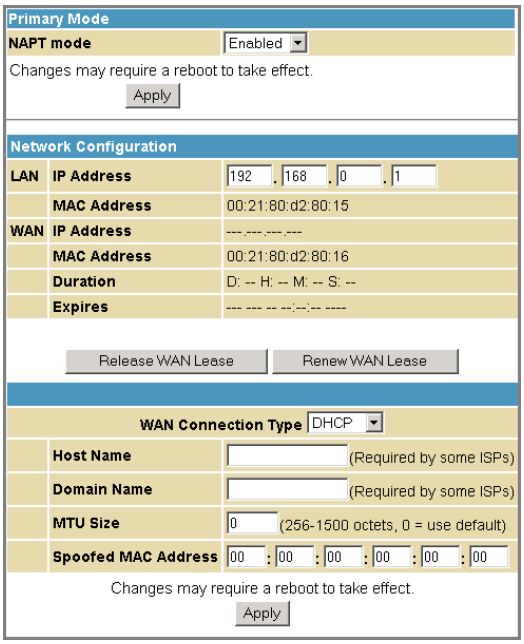
| Time | Priority | Description |
|---|---|---|
| Time Not Established | Critical (3) | SYNC Timing Synchronization failure - Failed to acquire QAM/Q... |
| Time Not Established | Notice (6) | Ds Lock Failed - Reinitialize MAC... |
| Time Not Established | Critical (3) | SYNC Timing Synchronization failure - Failed to acquire QAM/Q... |
| Time Not Established | Notice (6) | Ds Lock Failed - Reinitialize MAC... |
| Time Not Established | Critical (3) | SYNC Timing Synchronization failure - Failed to acquire QAM/Q... |
| Time Not Established | Notice (6) | Ds Lock Failed - Reinitialize MAC... |
| Time Not Established | Critical (3) | SYNC Timing Synchronization failure - Failed to acquire QAM/Q... |
| Time Not Established | Critical (3) | SYNC Timing Synchronization failure - Failed to acquire FEC f... |
| Time Not Established | Critical (3) | SYNC Timing Synchronization failure - Failed to acquire QAM/Q... |
| Time Not Established | Notice (6) | Ethernet link up - ready to pass packets |
| Thu Nov 13 14:47:40 2008 | Notice (6) | Modem Is Shutting Down and Rebooting... |
| Thu Nov 13 14:47:40 2008 | Critical (3) | Received Response to Broadcast Maintenance Request, But no Un... |
| Thu Nov 13 14:47:40 2008 | Critical (3) | SYNC Timing Synchronization failure - Failed to acquire QAM/Q... |
| Thu Nov 13 14:43:54 2008 | Information (7) | Registration Completed |
| Thu Nov 13 14:43:54 2008 | Information (7) | Authorized |
| Thu Nov 13 14:43:54 2008 | Information (7) | Retrieved Time..... SUCCESS |
| Thu Nov 13 14:43:54 2008 | Information (7) | Retrieved TFTP Config sbv5200_cm_dual_1.1_dqos_full_pc_sbvpro... |
| Thu Nov 13 14:43:54 2008 | Information (7) | Retrieved DHCP ..... SUCCESS |
| Thu Nov 13 14:43:47 2008 | Information (7) | Acquired Upstream ..... SUCCESS |
| Thu Nov 13 14:43:43 2008 | Information (7) | Acquired Downstream (651038118 Hz)..... SUCCESS |
| Thu Nov 13 14:43:32 2008 | Notice (6) | Ds Lock Failed - Reinitialize MAC... |
| Thu Nov 13 14:43:32 2008 | Information (7) | Retrieved Time..... SUCCESS |
| Thu Nov 13 14:43:32 2008 | Information (7) | Retrieved TFTP Config sbv5200_cm_dual_1.1_dqos_full_pc_sbvpro... |
| Time Not Established | Information (7) | Retrieved DHCP ..... SUCCESS |
| Time Not Established | Information (7) | Acquired Upstream ..... SUCCESS |

# 5 Páginas básicas

Exibe e define dados de configuração relacionados ao IP do SVG1501, incluindo Configuração de rede, Tipo de conexão WAN, DHCP e DDNS nas Páginas básicas. A opção Backup permite salvar uma cópia da configuração do SVG1501 no computador

## Página de configuração básica

Configure os recursos básicos do gateway do SVG1501 relacionados à conexão ISP.




**Descrições de campos da Página de configuração básica**

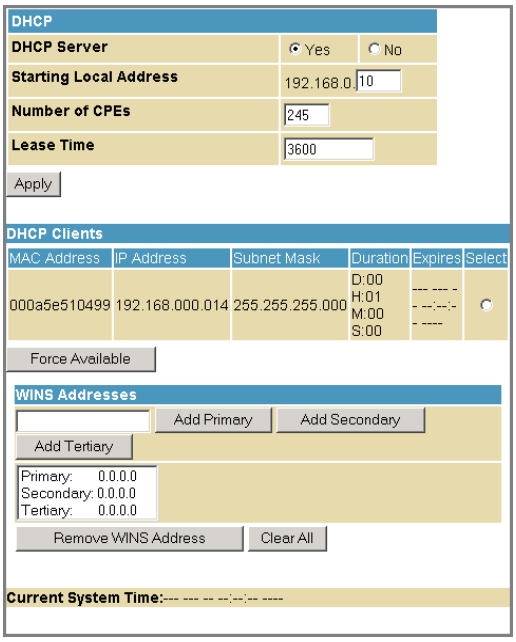
| Campo | Descrição |
|---|---|
| **NAPT mode (Modo NAPT)** | NAPT é um caso especial de NAT, em que muitos números de IP são ocultos em diversos endereços. No entanto, ao contrário do NAT original, isso não significa que pode haver apenas esse número de conexões por vez.<br>No modo NAPT, um número quase arbitrário de conexões é multiplexado usando informações da porta TCP. O número de conexões simultâneas é limitado pelo número de endereços multiplicado pelo número de portas TCP disponíveis. |

| Campo | Descrição |
|---|---|
| **LAN** | |
| **IP Address (Endereço IP)** | Digite o endereço IP do SVG1501 em sua LAN particular. |
| **MAC Address (Endereço MAC)** | Endereço MAC — um conjunto de 12 dígitos hexadecimais atribuído durante a fabricação que identifica exclusivamente o endereço de hardware da Porta de acesso do SVG1501. |
| **WAN** | |
| **IP Address (Endereço IP)** | O endereço IP da WAN pública do dispositivo SVG1501, que é atribuído dinâmica ou estaticamente pelo ISP. |
| **MAC Address (Endereço MAC)** | Endereço MAC — um conjunto de 12 dígitos hexadecimais atribuído durante a fabricação que identifica exclusivamente o endereço de hardware da Porta de acesso do SVG1501. |
| **Duration (Duração)** | Descreve quanto tempo antes sua conexão com a Internet expira. O leasing WAN será renovado automaticamente quando expirar. |
| **Expires (Expira em)** | Exibe a hora e data exatas quando o leasing WAN expira. |
| **Release WAN Lease (Liberar leasing WAN)** | Clique para liberar o leasing WAN. |
| **Renew WAN Lease (Renovar leasing WAN)** | Clique para renovar o leasing WAN. |
| **WAN Connection Type (Tipo de conexão WAN)** | DHCP ou IP estático. Se o ISP usar DHCP, selecione **DHCP** e digite um Nome de host e Nome de domínio, se necessário.<br>Se o ISP usar endereço IP estático, selecione **Static IP** (IP estático) e as insira as informações fornecidas pelo ISP para Endereço IP estático, Máscara IP estática, Gateway padrão, DNS primário e DNS secundário. |
| **Host Name (Nome do host)** | Se o Tipo de conexão WAN for DHCP, digite um Nome de host, se necessário. |
| **Domain Name (Nome do domínio)** | Se o Tipo de conexão WAN for DHCP, digite um Nome de domínio, se necessário. |
| **MTU Size (Tamanho da MTU)** | A MTU (Maximum Transmission Unit, unidade máxima de transmissão) é o maior pacote ou quadro que pode ser enviado. O valor padrão é adequado para a maioria dos usuários. |
| **Spoofed MAC Address (Endereço MAC adulterado)** | Se o Tipo de conexão WAN for IP estático, insira as informações fornecidas pelo ISP para Endereço IP estático, Máscara IP estática, Gateway padrão, DNS primário e DNS secundário. |

Quando terminar, clique em **Apply** (Aplicar) para salvar as alterações.

# Página DHCP básica

Configura e exibe o status do servidor DHCP (Dynamic Host Configuration Protocol) interno opcional do SVG1501 para a LAN.




***CUIDADO:*** *Não modifique essas configurações a menos que seja um administrador de rede experiente com amplo conhecimento de endereço IP, sub-rede e DHCP.*

**Descrições de campos da Página DHCP básica**

| Campo | Descrição |
|---|---|
| **DHCP Server (Servidor DHCP)** | Selecione **Yes** (Sim) para ativar o servidor DHCP do SVG1501.<br>Selecione **No** (Não) para desativar o servidor DHCP do SVG1501. |
| **Starting Local Address (Endereço local inicial)** | Digite o endereço IP inicial a ser atribuído pelo servidor DHCP do SVG1501 para clientes no formato com pontos decimais. O padrão é 192.168.0.2. |
| **Number of CPEs (Número de CPEs)** | Define o número de clientes para o servidor DHCP do SVG1501 para atribuir um endereço IP particular. Existem 245 endereços de clientes possíveis. O padrão é **245**. |
| **Lease Time (Tempo de leasing)** | Define o tempo em segundos que o servidor DHCP do SVG1501 efetua leasing de um endereço IP para um cliente. O padrão é 3600 segundos (60 minutos). |

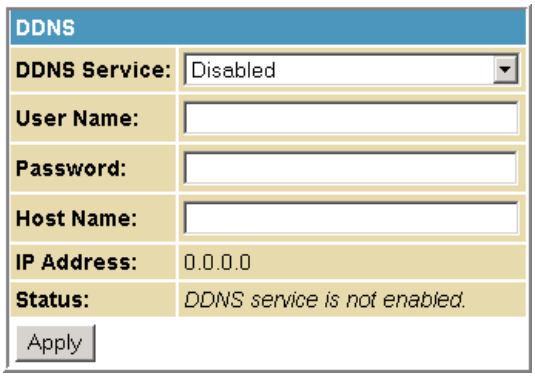
| Campo | Descrição |
|---|---|
| **DHCP Clients (Clientes DHCP)** | Lista informações de dispositivo do cliente DHCP. |
| **WINS Addresses (Endereços WINS)** | Especifica até três endereços de servidor WINS (Windows Internet Name Service). |

Clique em **Apply** (Aplicar) para salvar as alterações.

Para renovar um endereço IP do cliente DHCP, escolha **Select** (Selecionar) e, em seguida, clique em **Force Available** (Forçar disponível).

# Página DDNS básica

Configure o serviço DDNS (Dynamic Domain Name System) para atribuir um nome de domínio de Internet estático para um endereço IP dinâmico. Isso permite que o SVG1501 seja acessado mais facilmente de diversos locais na Internet.



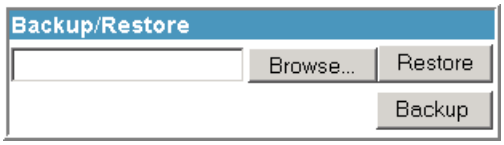

**Descrições de campos da Página DDNS básica**

| Campo | Descrição |
|---|---|
| **DDNS Service (Serviço DDNS)** | Selecione **Disable** (Desativar) ou **wwwDynDNS.org** para ativar o Serviço DDN. |
| **User Name (Nome de usuário)** | Digite seu nome de usuário DynDNS. |
| **Password (Senha)** | Digite sua senha DynDNS. |
| **Host Name (Nome do host)** | Digite seu nome do host DDNS. |
| **IP Address (Endereço IP)** | Lista informações do IP. |
| **Status** | Exibe o status do serviço DDNS: **ativado** ou **desativado** |

Clique em **Apply** (Aplicar) para salvar as alterações.

# Página básica de backup

Salve as definições de configuração atuais do SVG1501 localmente no computador ou restaure as configurações salvas anteriormente.




## Restauração da configuração do SVG1501

1. Digite o caminho com o nome do arquivo onde o arquivo de backup está localizado no computador ou clique em **Browse** (Procurar) para localizar o arquivo.
2. Clique em **Restore** (Restaurar) para restaurar as configurações salvas anteriormente do SVG1501.

## Backup da configuração do SVG1501

1. Digite o caminho com o nome do arquivo onde você deseja armazenar o arquivo de backup no computador ou clique em **Browse** (Procurar) para localizar o arquivo.
2. Clique em **Backup** para criar um backup das configurações do SVG1501.

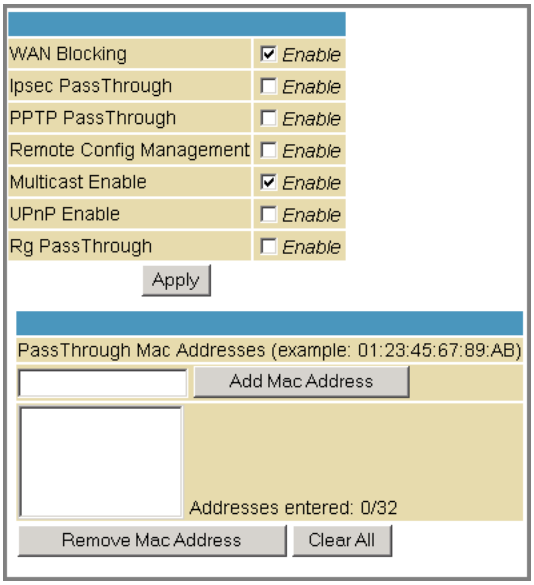
# 6 Páginas avançadas

Defina a configuração de Filtro IP, Filtro MAC, Filtro de porta, Encaminhamento de porta, Gatilhos de porta, Host DMZ e RIP (Routing Information Protocol, protocolo de informações de roteamento).

Clique na opção do menu Advanced (Avançado) para exibir ou alterar as informações avançadas de configuração dessa opção.

## Página de opções avançadas

Defina os modos operacionais para ajustar como o dispositivo SVG1501 roteia o tráfego IP.




**Descrições de campos da Página de opções avançadas**

| Campo | Descrição |
|---|---|
| **WAN Blocking (Bloqueio WAN)** | Impede que o Gerenciador de Configuração do SVG1501 ou os PCs atrás dele fiquem visíveis para outros computadores na WAN do SVG1501.<br>Selecione **Enable** (Ativar) para ativar. |
| **IPsec PassThrough (Passagem IPsec)** | Ativa o protocolo IPsec Pass-Through (Passagem IPsec) a ser usado pelo Gerenciador de configuração do SVG1501 para que um dispositivo (ou software) VPN possa se comunicar adequadamente com a WAN.<br>Selecione **Enable** (Ativar) para ativar. |

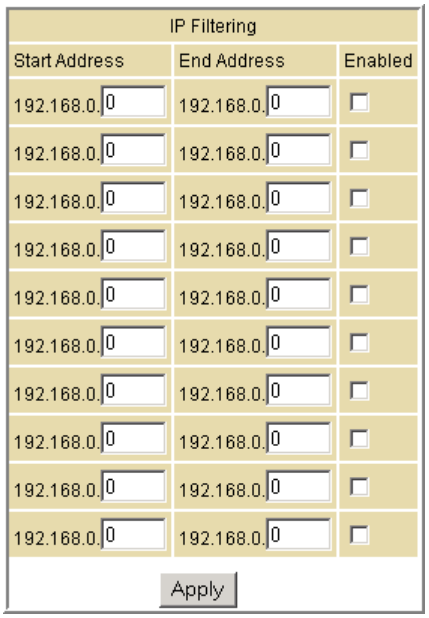
| Campo | Descrição |
|---|---|
| **PPTP PassThrough (Passagem PPTP)** | Ativa o protocolo PPTP (Point-to-Point Tunneling Protocol, protocolo de túnel de ponto a ponto) a ser usado pelo Gerenciador de configuração do SVG1501 para que um dispositivo (ou software) VPN possa se comunicar adequadamente com a WAN.<br>Selecione **Enable** (Ativar) para ativar. |
| **Remote Config Management (Gerenciamento remoto de configuração)** | Permite o acesso remoto ao Gerenciador de configuração do SVG1501. Permite configurar a WAN do SVG1501 acessando o endereço IP da WAN na porta 8080 do gerenciador de configuração de qualquer lugar na Internet. Por exemplo, na janela do URL do navegador, digite **http://WanIPAddress:8080/** para acessar o Gerenciador de configuração do SVG1501 remotamente.<br>Selecione **Enable** (Ativar) para ativar. |
| **Multicast Enable (Ativação multicast)** | Permite que o tráfego específico ao multicast (denotado por um endereço específico multicast) flua entre os PCs na rede particular atrás do gerenciador de configuração.<br>Selecione **Enable** (Ativar) para ativar. |
| **UPnP Enable (Ativação UPnP)** | Ativa o agente do protocolo UpnP (Universal Plug and Play) no gerenciador de configuração. Se você estiver executando um aplicativo CPE (cliente) que requer UPnP, selecione esta caixa.<br>Selecione **Enable** (Ativar) para ativar. |
| **Rg PassThrough (Passagem Rg)** | Desativa a operação NAT permitindo que todos os computadores clientes atuem como clientes de passagem.<br>Selecione **Enable** (Ativar) para ativar. |
| **PassThrough Mac Addresses (Endereços Mac de passagem)** | Especifica até 32 computadores como clientes de passagem não sujeitos ao NAT, usando seus endereços MAC.<br>Para ativar esse recurso, seu operador de cabo talvez precise fornecer endereços IP públicos adicionais. |

Clique em **Apply** (Aplicar) para salvar as alterações.

# Página avançada Filtro de IP

Defina quais PCs locais terão acesso negado ao WAN do SVG1501 configurando filtros de endereço IP para bloquear o tráfego na Internet pra dispositivos de rede específicos na LAN. Digite o LSB (Least-significant byte, byte menos significante) do endereço IP; os bytes superiores do endereço IP são definidos automaticamente a partir do endereço IP do Gerenciador de configuração do SVG1501.

Você pode armazenar as configurações de filtro usadas com freqüência, mas não pode mantê-las ativas.



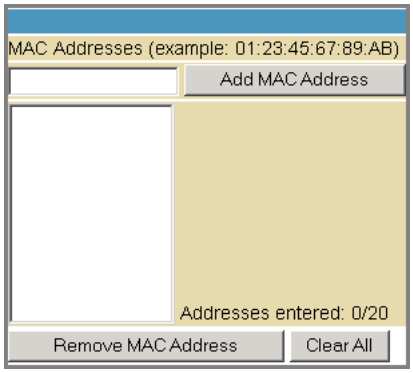

**Descrições de campos da Página avançada Filtro de IP**

| Campo | Descrição |
|---|---|
| **Start Address (Endereço inicial)** | Digite o intervalo de endereços IP iniciais dos computadores para os quais deseja recusar o acesso à WAN do SVG1501.<br>Digite apenas o byte menos significante do endereço IP. |
| **End Address (Endereço final)** | Digite o intervalo de endereços IP finais dos computadores para os quais deseja recusar o acesso à WAN do SVG1501.<br>Digite apenas o byte menos significante do endereço IP. |
| **Enabled (Ativado)** | Ative o filtro de endereço IP.<br>Selecione cada intervalo de endereços IP para os quais deseja recusar o acesso à WAN do SVG1501. |

Clique em **Apply** (Aplicar) para ativar e salvar as configurações.

# Página avançada Filtro de MAC

Defina até 20 filtros de endereço MAC (Media Access Control) para impedir que os PCs enviem tráfego TCP/UDP de saída para a WAN por meio de seus endereços de MAC. O endereço MAC de uma placa NIC específica nunca muda, ao contrário de seu endereço IP que pode ser atribuído por meio do servidor DHCP ou codificado para vários endereços com o tempo.




**Descrições de campos da Página avançada Filtro de MAC**

| Campo | Descrição |
|---|---|
| **MAC Addresses (Endereços MAC)** | Endereço MAC — um conjunto exclusivo de 12 dígitos hexadecimais atribuídos a um PC durante a fabricação. |

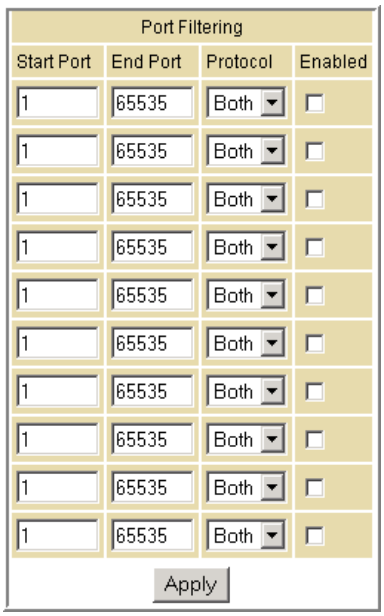
## Configuração de um filtro de endereço MAC

1. Digite o endereço MAC no campo MAC Addresses (Endereços MAC) do PC que deseja bloquear.
2. Clique em **Add MAC Address** (Adicionar endereço MAC).
3. Repita cada etapa para até vinte endereços MAC.

# Página avançada Filtro de porta

Defina filtros de porta para impedir que todos os dispositivos enviem tráfego TCP/UDP de saída para a WAN em números de porta IP específicos. Especifique um intervalo de portas iniciais e finais para determinar qual tráfego TCP/UDP é permitido na WAN de acordo com a porta.

> ***Nota:*** *Os intervalos de porta especificados são bloqueados para TODOS OS PCs. Essa definição não é específica ao endereço IP ou endereço MAC. Por exemplo, para impedir o acesso de todos os PCs na LAN particular a sites HTTP, defina a "Porta inicial" como* ***80****, a "Porta final" como* ***80****, o "Protocolo" como* ***TCP****, selecione* ***Enabled*** *(Ativado) e, em seguida, clique em* ***Apply*** *(Aplicar).*

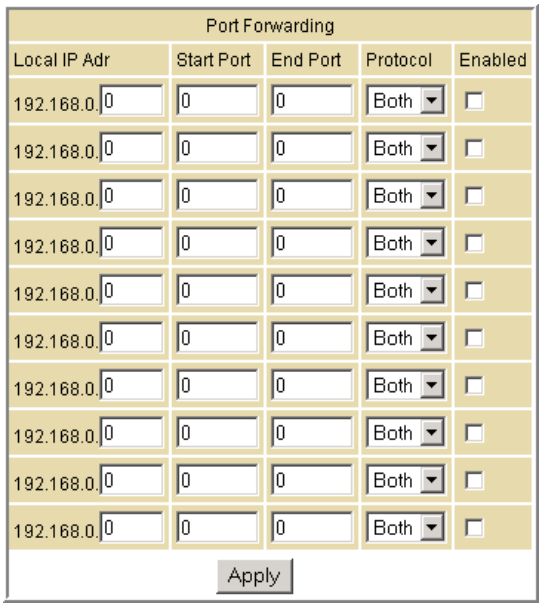



**Descrições de campos da Página avançada Filtro de porta**

| Campo | Descrição |
|---|---|
| **Start Port (Porta inicial)** | Digite o número da porta inicial. |
| **End Port (Porta final)** | Digite o número da porta final. |
| **Protocol (Protocolo** | Selecione **TCP**, **UDP** ou **Both** (Ambos) na lista suspensa. |
| **Enabled (Ativado)** | Selecione para ativar os filtros de porta IP. |

# Página avançada Encaminhamento de porta

Execute um servidor acessível publicamente na LAN especificando o mapeamento de portas TCP/UDP para um PC local. Isso permite que pedidos de entrada em números de porta específicos cheguem aos servidores da Web, servidores FTP, servidores de correio, etc., para que possam ficar acessíveis na Internet pública.




Números de porta usados com freqüência:

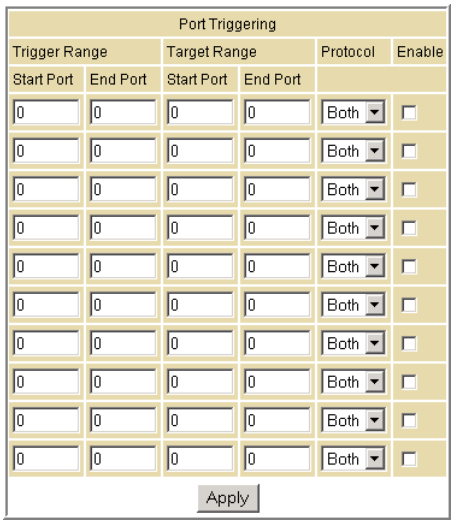
- HTTP: 80
- FTP: 20, 21
- Shell seguro: 22
- Telnet: 23
- E-mail SMTP: 25
- SNMP: 161

Para mapear uma porta, digite o intervalo de números de portas que devem ser encaminhados localmente e o endereço IP para o qual o tráfego para essas portas deve ser enviado. Para mapear uma única porta, digite o mesmo número de porta nos locais "inicial" e "final" desse endereço IP.

# Página avançada Gatilhos de porta

Configure gatilhos dinâmicos para dispositivos específicos na LAN. Isso permite que aplicativos especiais que requerem números de porta específicos com tráfego bidirecional funcionem corretamente. Aplicativos como conferência de vídeo, voz, jogos e alguns recursos do programa de envio de mensagens podem precisar dessas definições especiais.

Os Gatilhos avançados de porta não são portas estáticas mantidas abertas sempre. Quando o Gerenciador de configuração detecta dados de saída em um número de porta IP específico definido no "Intervalo de gatilhos", as portas resultantes definidas no "Intervalo de destino" são abertas para dados de entrada ou bidirecionais. Se nenhum tráfego de saída for detectado nas portas do "Intervalo de gatilhos" durante 10 minutos, as portas do "Intervalo de destino" serão fechadas. Esse é um método mais seguro para abrir portas específicas para aplicativos especiais (por exemplo, programas de conferência de vídeo, jogos interativos, transferência de arquivos em programas de bate-papo, etc.), porque são disparadas dinamicamente e não são mantidas abertas constantemente nem deixadas abertas por engano pelo administrador do roteador e expostas para descoberta por possíveis hackers.




**Descrições de campos da Página avançada Gatilhos de porta**

| Campo | Descrição |
|---|---|
| **Trigger Range Start Port (Porta inicial do intervalo de gatilhos)**<br>**End Port (Porta final)** | Número da porta inicial do intervalo de gatilhos da porta.<br>Número da porta final do intervalo de gatilhos da porta. |
| **Target Range Start Port (Porta inicial do intervalo de destino)**<br>**End Port (Porta final)** | Número da porta inicial do intervalo de gatilhos da porta.<br>Número da porta final do intervalo de gatilhos da porta. |

| Campo | Descrição |
|---|---|
| **Protocol (Protocolo)** | Selecione **TCP**, **UDP** ou **Both** (Ambos) na lista suspensa. |
| **Enable (Ativar)** | Marque a caixa de seleção para ativar os gatilhos de porta IP. |

# Página avançada Host DMZ

Especifique o destinatário padrão do tráfego WAN que o NAT pode converter para um PC local conhecido. A DMZ (De-militarized Zone, zona desmilitarizada) é um computador ou pequena sub-rede fora do firewall, entre a LAN particular interna confiável e a Internet pública não-confiável, que impede acesso direto por usuários externos aos dados particulares.

Por exemplo, você pode configurar um servidor da Web em um computador DMZ para permitir que usuários externos acessem seu website sem expor dados confidenciais na rede.

Uma DMZ também é útil para jogos interativos que podem apresentar problemas ao executar por meio de um firewall. Você pode deixar um computador usado para jogos apenas exposto na Internet, protegendo o restante da rede.


Você pode configurar um PC para ser o host da DMZ. Essa definição geralmente é usada para PCs usando aplicativos com problema que usam números de porta aleatórios e não funcionam corretamente com gatilhos de porta específicos ou com as configurações de encaminhamento de porta. Se você configurar um PC como um host da DMZ, defina novamente como zero ao terminar com o aplicativo necessário, pois esse PC será efetivamente exposto na Internet pública, embora ainda protegida contra ataques DoS (Denial of Service, recusa de serviço) por meio do firewall.

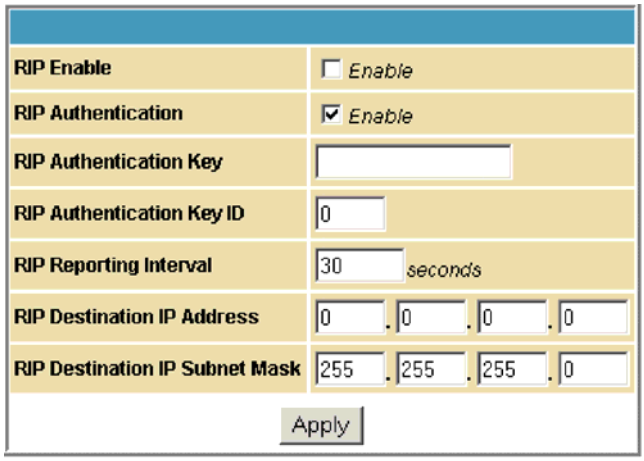
## Configuração do host DMZ

1. Digite o endereço IP do computador.
2. Clique em **Apply** (Aplicar) para ativar o computador selecionado como o host DMZ.

# Página avançada Configuração do protocolo de informações de roteamento

Configure os parâmetros do RIP (Routing Information Protocol, protocolo de informações de roteamento) relacionados a autenticação, endereço IP/máscara de sub-rede de destino e intervalos de geração de relatórios. O RIP identifica e usa automaticamente a melhor rota e mais rápida para qualquer endereço de destino determinado. O protocolo RIP requer negociação de ambos os lados (CMRG e CMTS) da rede. O ISP geralmente define essa opção para corresponder as definições CMTS com a configuração no CMRG.

> ***Nota:*** *As mensagens do RIP são enviadas upstream apenas ao executar no modo Endereço IP estático, na página Configuração básica. Você deve ativar o Endereço IP estático e depois definir as informações de rede IP da WAN! O RIP geralmente é uma função estritamente controlada pelo ISP. As chaves e IDs de autenticação do RIP normalmente são mantidas como informações secretas do usuário final para impedir configurações do RIP não autorizadas.*




**Descrições de campos da Página Configuração avançada do RIP**

| Campo | Descrição |
|---|---|
| **RIP Enable (Ativação do RIP)** | Ativa ou desativa o protocolo RIP.<br>O RIP ajuda o roteador a adaptar-se dinamicamente às alterações na rede. Agora está obsoleto em razão de protocolos de roteamento mais recentes, como OSPF e ISIS. |
| **RIP Authentication (Autenticação do RIP)** | Inclui uma senha de texto sem formatação ou uma chave compartilhada ao pacote RIP do CPE e ao roteador wireless para autenticar um ao outro. |

| Campo | Descrição |
|---|---|
| **RIP Authentication Key (Chave de autenticação do RIP)** | Criptografa a senha de texto sem formatação contida em cada pacote RIP.<br>Se estiver usando a autenticação de chave compartilhada no RIP, você precisa fornecer uma chave. |
| **RIP Authentication Key ID (ID da chave de autenticação do RIP)** | Identifica a chave para criar os dados de autenticação para o pacote RIP e indica o algoritmo de autenticação. |
| **RIP Reporting Interval (Intervalo de geração de relatórios do RIP)** | Determina quanto tempo antes um pacote RIP é enviado para o CPE. |
| **RIP Destination IP Address (Endereço IP de destino do RIP)** | Define o local para o qual o pacote RIP será enviado para atualizar a tabela de roteamento no CPE. |
| **RIP Destination IP Subnet Mask (Máscara de sub-rede IP de destino do RIP)** | Especifica em qual CPE você deseja receber o pacote RIP. |

# 7 Páginas Firewall

Use as Páginas Firewall para configurar os filtros do firewall e as notificações de alerta do firewall. O firewall protege a LAN do SVG1501 de ataques indesejáveis e outras intrusões na Internet. O firewall:

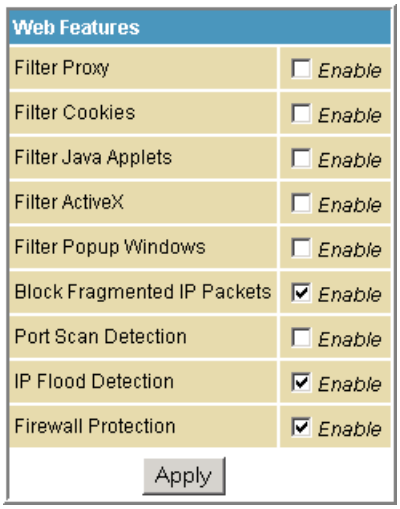
- Mantém os dados de estado para cada sessão TCP/IP na rede OSI e camadas de transporte.
- Monitora todos os pacotes de entrada e saída, aplica a política do firewall a cada um e detecta os pacotes inadequados e tentativas de intrusão.
- Oferece registro abrangente para todos:
  - Autenticações do usuário
  - Pedidos de conexão interna e externa rejeitados
  - Criação e encerramento da sessão
  - Ataques externos (detecção de intrusão)

Você pode configurar os filtros do firewall para definir regras para o uso da porta.

## Página Filtro de conteúdo da Web do firewall

Configure o firewall ativando ou desativando diversos filtros da Web relacionados a bloquear ou permitir exclusivamente tipos diferentes de dados por meio do Gerenciador de configuração da WAN para a LAN.

Você pode bloquear Java Applets, Cookies, controles ActiveX, janelas pop-up e Proxies. A proteção de firewall ativa os recursos do firewall de SPI (Stateful Packet Inspection, inspeção do estado do pacote).



Selecione cada filtro da Web que deseja definir para o firewall e, em seguida, clique em **Apply** (Aplicar). Os filtros da Web serão ativados sem a necessidade de reinicializar o Gerenciador de configuração do SVG1501.

> ***Nota:*** *Pelo menos um filtro ou recurso da Web deve estar ativado para que o firewall esteja ativo. Verifique se o firewall não está desativado.*

# Página Registro local do firewall

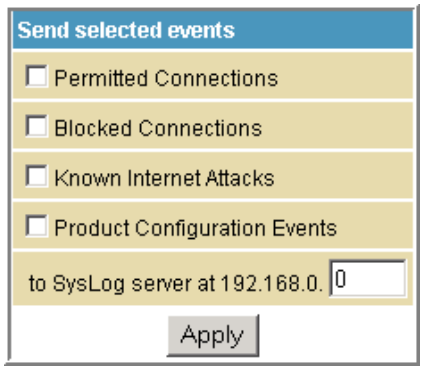
Configure a notificação do registro de eventos do firewall em um dos seguintes formatos:

- Alertas de e-mail individuais enviados toda vez que o firewall é atacado
- Registro local armazenado no modem e exibido na página Registro local

# Página Registro remoto do firewall

Envie relatórios de ataque do firewall para um servidor SysLog padrão para que várias instâncias possam ser registradas em um período. Selecione itens individuais de ataque ou de configuração a serem enviados para o servidor SysLog para que apenas os itens de interesse sejam monitorados. Você pode registrar conexões permitidas, conexões bloqueadas, tipos de ataque à Internet conhecidos e eventos de configuração do CMRG. O servidor SysLog deve estar na mesma rede da LAN particular no Gerenciador de configuração (geralmente, 192.168.0.x).

Para ativar o recurso de monitoramento SysLog, marque todos os tipos de evento desejados para monitorar e insira o último byte do endereço IP do servidor SysLog. Geralmente, o endereço IP desse servidor SysLog é codificado para que o endereço não seja alterado e sempre combine com a entrada nesta página.



**Descrição de campos da Página Registro remoto do firewall**

| Campo | Descrição |
|---|---|
| **Permitted Connections (Conexões permitidas)** | Selecione para que o servidor lhe envie por e-mail registros de quem está conectado à sua rede. |
| **Blocked Connections (Conexões bloqueadas)** | Selecione para que o servidor lhe envie por e-mail registros de quem está bloqueado para conexão à sua rede. |
| **Known Internet Attacks (Ataques à Internet conhecidos)** | Selecione para que o servidor lhe envie por e-mail registros de ataques conhecidos na Internet contra sua rede. |
| **Product Configuration Events (Eventos de configuração do produto)** | Selecione para que o servidor lhe envie por e-mail registros de eventos de configuração básica do produto. |
| **To SysLog server at 192.168.0. (Para o servidor SysLog em 192.168.0.)** | Digite os últimos dígitos de 10 a 254 do endereço IP do seu servidor SysLog. |

Clique em **Apply** (Aplicar).

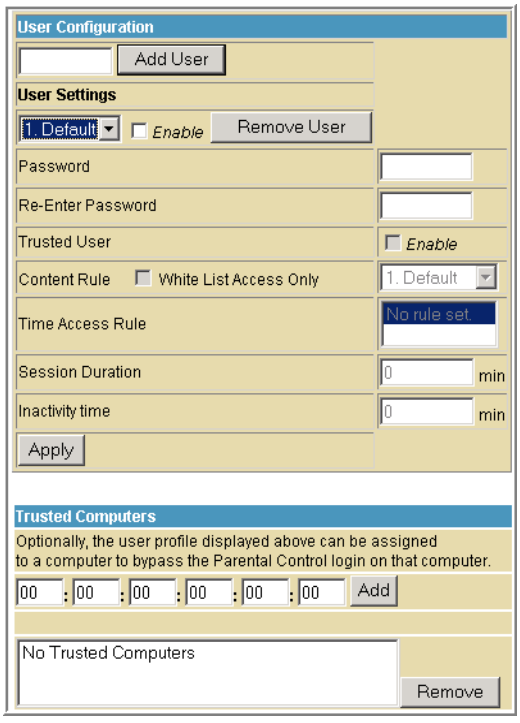
# 8 Páginas Controle dos pais

Use as Páginas Controle dos pais para configurar restrições de acesso a um dispositivo específico conectado à LAN do SVG1501.

## Página Configuração do usuário para o controle dos pais

Vincule cada usuário a uma regra de tempo de acesso especificado, regra de filtro do conteúdo e login. Você também pode especificar um usuário como um "usuário confiável" que terá acesso a todo o conteúdo da Internet, independente dos filtros. Você pode usar a caixa de seleção Usuário confiável como uma sobreposição para conceder acesso total a um usuário, armazenando todas as configurações de filtro para fácil disponibilidade.

Você pode ativar os cronômetros de duração de sessão da Internet, que limitam o tempo para acesso à Internet. Os usuários devem inserir suas senhas da primeira vez que acessam a Internet, mas não toda vez que uma nova página da Web é acessada. Você também pode definir o cronômetro de inatividade para que, se não houver acesso à Internet durante um tempo especificado, o usuário precise efetuar login novamente.



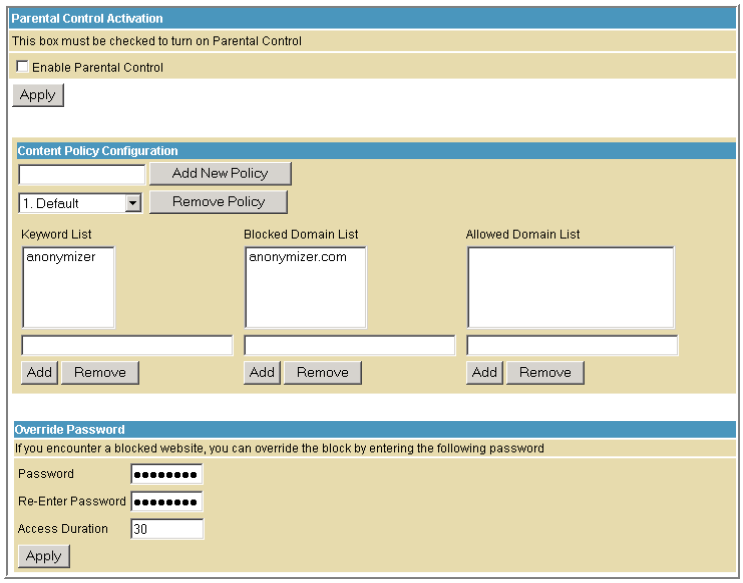
**Descrições de campos da Página Configuração do usuário para o controle dos pais**

| Campo | Descrição |
|---|---|
| **Botão Add User (Adicionar usuário)** | Adiciona um usuário para definir controles dos pais para um usuário específico. |
| **User Settings (Configurações do usuário)** | Selecione o usuário do qual você deseja modificar as restrições de acesso.<br>Selecione **Enable** (Ativar) para selecionar o usuário.<br>Clique em **Remove User** (Remover usuário) para excluir o usuário dos Controles dos pais. |
| **Password (Senha)** | Digite uma senha do usuário para logon na Internet. |
| **Re-Enter Password (Reinserir senha)** | Digite a senha novamente para confirmação. |
| **Trusted User (Usuário confiável)** | Selecione os usuários que terão acesso total ao conteúdo da Internet.<br>Selecione **Enable** (Ativar) para sobrepor os filtros definidos sem precisar desativar as definições do filtro. |
| **Content Rule (Regra do conteúdo)** | Especifique quais websites cada usuário tem permissão para acessar.<br>Selecione **White List Access Only** (Acesso à lista de permissão apenas), e escolha um usuário na lista suspensa. |
| **Time Access Rule (Regra de tempo de acesso)** | Defina uma regra para restringir quando um usuário selecionado pode usar a Internet. |
| **Session Duration (Duração da sessão)** | Defina o tempo que um usuário selecionado pode usar a Internet. |
| **Inactivity time (Tempo de inatividade)** | Defina o tempo de inatividade antes que a Internet seja fechada automaticamente para um usuário selecionado. |
| **Computadores confiáveis** | Digite o endereço MAC CPE de um usuário para que o CPE possa acessar a Internet sem censura pelo Controle dos pais.<br>Quando terminar, clique em **Add** (Adicionar). |

Clique em **Apply** (Aplicar) para ativar e salvar as alterações feitas.

# Página Configuração básica do controle dos pais

Defina regras para bloquear os tipos de conteúdo da Internet e determinados Web sites.



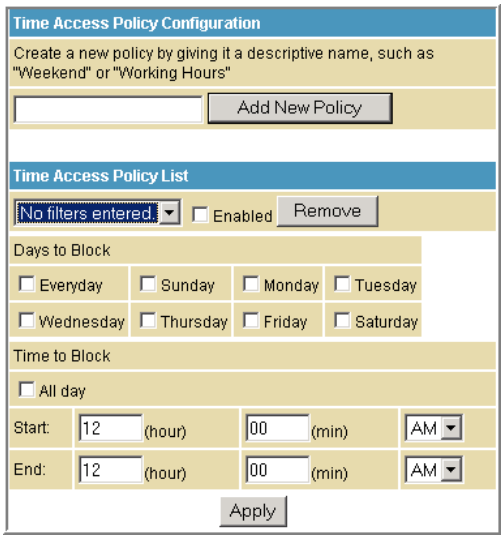

Depois de alterar as configurações do Controle dos pais, clique no botão **Apply** (Aplicar), **Add** (Adicionar) ou **Remove** (Remover) apropriado.

Clique em **Refresh** (Renovar) na janela do navegador da Web para exibir suas configurações atuais.

# Página Filtro de hora do dia para o controle dos pais

Bloqueie todo o tráfego da Internet em dispositivos especificados na rede do SVG1501 com base nas definições de dia e hora. Você pode bloquear o tráfego na Internet durante todo o dia ou em determinadas horas de cada dia para usuários específicos. Você pode adicionar até 30 caracteres de oito caracteres (nomes de filtro) com definições diferentes de dia e hora. Insira um nome para cada filtro de hora no campo **Add New Policy** (Adicionar nova política).

Aplique filtros de hora para acesso limitado à Internet para cada usuário no campo **Time Access Rule** (Regra de tempo de acesso) na Página Configuração do usuário para o controle dos pais.




Depois de criar cada categoria, clique em **Apply** (Aplicar) na parte inferior da página para armazenar e ativar as definições. Os mesmos nomes de categoria para bloquear perfis aparecem na página Configuração do usuário para o controle dos pais, na seção "Regra de tempo de acesso", em que cada usuário pode ser atribuído a até quatro categorias simultaneamente.

# Página Registro local do controle dos pais

Gere um registro de eventos que mostre uma lista de execução das últimas 30 violações de acesso do Controle dos pais, incluindo:

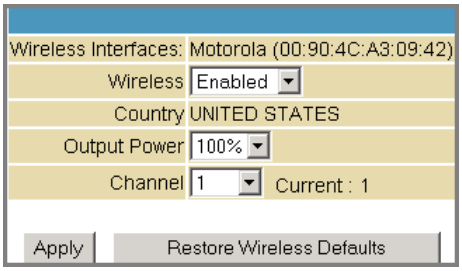
- Se o acesso do usuário à Internet está bloqueado (filtro de hora)
- Se uma palavra-chave bloqueada foi detectada no URL
- Se um domínio bloqueado foi detectado no URL
- Se o serviço de consulta on-line detecta que o URL está em uma categoria bloqueada

# 9 Páginas Wireless

Para configurar sua WLAN, clique em qualquer opção do submenu Wireless para exibir ou alterar as informações de configuração para essa opção. A criptografia WPA ou WPA2 oferece mais segurança que a criptografia WEP, mas placas de cliente wireless mais antigas podem não suportar os métodos de criptografia WPA ou WPA2 mais recentes.

## Página Rádio wireless 802.11

Configure os parâmetros do Rádio wireless, incluindo o número atual do país e do canal.

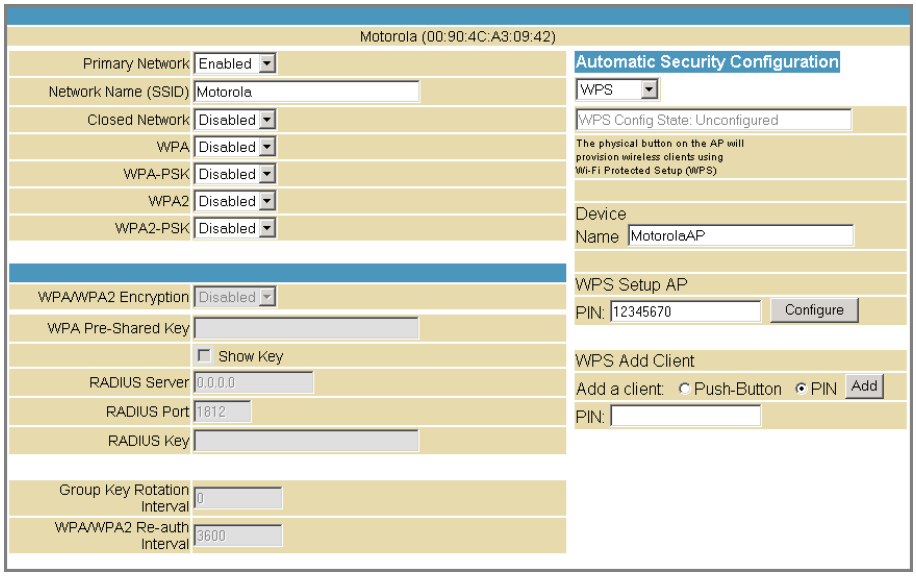



**Descrições de campos da Página Rádio wireless 802.11**

| Campo | Descrição |
|---|---|
| **Wireless Interfaces (Interfaces wireless)** | Mostra o endereço MAC da placa wireless instalada. Não é configurável. |
| **Wireless** | Mostra se a rede wireless está ativada ou desativada |
| **Country (País)** | Restringe o conjunto de canais com base nos requisitos normativos do país. Este é um campo somente exibição. |
| **Output Power (Potência de saída)** | Define uma porcentagem da potência de saída da capacidade máxima do hardware. |
| **Channel (Canal)** | Seleciona o canal para operação do ponto de acesso (AP, Access Point). A lista de canais disponíveis depende do país designado.<br>Para este campo, o canal selecionado nos clientes wireless na WLAN deve ser igual ao canal selecionado no SVG1501. |

# Página Rede primária wireless 802.11

Configure sua rede wireless primária.




**Descrições de campos da Página Rede primária wireless 802.11**

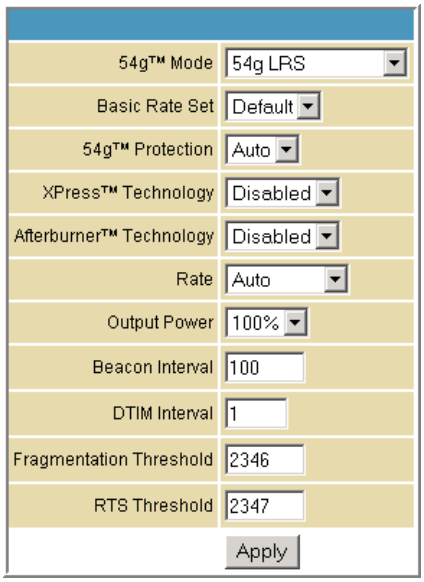
| Campo | Descrição |
|---|---|
| **Primary Network (Rede primária)** | Quando definido como **Enabled** (Ativado), transmite quadros de indicador com o SSID da rede primária. |
| **Network Name (SSID) (Nome da rede (SSID))** | Define o Nome da rede (SSID) da rede wireless primária usando uma seqüência de 1 a 32 caracteres ASCII. |
| **Closed Network (Rede fechada)** | Em uma rede fechada, os usuários digitam o SSID no aplicativo cliente, em vez de selecioná-lo em uma lista. |
| **WPA** | Ativa ou desativa a criptografia de acesso protegido Wi-Fi. |
| **WPA-PSK** | Ativa ou desativa uma passphrase de chave pré-compartilhada WPA local. |
| **WPA2** | Ativa ou desativa a criptografia 2 de acesso protegido Wi-Fi. |
| **WPA2-PSK** | Ativa ou desativa uma passphrase de chave pré-compartilhada WPA2 local. |
| **WPA/WPA2 Encryption (Criptografia WPA/WPA2)** | Define o modo de criptografia como: TKIP, AES ou TKIP + AES. AES. |

| Campo | Descrição |
|---|---|
| **WPA Pre-Shared Key (Chave pré-compartilhada WPA)**<br>**Show Key (Mostrar chave)** | Define a PSK (Pre-Shared Key, chave pré-compartilhada) WPA: uma seqüência de 8 a 63 caracteres ASCII ou um número hexadecimal de 64 dígitos. Isso é especificado quando o método de Autenticação de rede é o WPA-PSK.<br>**Show Key** (Mostrar chave) – exibe a chave pré-compartilhada WPA. |
| **RADIUS Server (Servidor RADIUS)** | Define o endereço IP do servidor RADIUS a ser usado para autenticação do cliente usando o formato com pontos decimais (xxx.xxx.xxx.xxx). |
| **RADIUS Port (Porta RADIUS)** | Defina o número da porta UDP do servidor RADIUS; o padrão é 1812. |
| **RADIUS Key (Chave RADIUS)** | Define o segredo compartilhado para a conexão RADIUS; a chave é uma seqüência ASCII de 0 a 255 caracteres. |
| **Group Key Rotation Interval (Intervalo de rotação da chave do grupo)** | Define o intervalo de rotação da chave do grupo WPA em segundos. Defina como zero para desativar a rotação periódica da chave. |
| **WPA/WPA2 Re-auth Interval (Intervalo de nova criação WPA/WPA2)** | Define o tempo que o roteador wireless pode aguardar antes de estabelecer novamente autenticação com o CPE. |
| **WEP Encryption (Criptografia WEP)** | Ativa ou desativa a criptografia de WEP (Wired Equivalent Privacy, privacidade equivalente com fio). |
| **Shared Key Authentication (Autenticação de chave compartilhada)** | Envia um pedido de autenticação para o ponto de acesso. Depois o ponto de acesso envia um texto de desafio para o CPE.<br>O CPE criptografia o texto de desafio enviado para o ponto de acesso. O ponto de acesso decifra e compara a mensagem com o texto do desafio original. Se forem iguais, o ponto de acesso permitirá a conexão do CPE; se não forem iguais, o ponto de acesso não permitirá a conexão do CPE. |
| **802.1x Authentication (Autenticação 802.1x)** | Usa uma autenticação mais forte que o WEP e pode ser usado adicionalmente. |
| **Network Key 1 – 4 (Chave de rede 1 – 4)** | Define as chaves WEP estáticas quando a criptografia WEP está ativada.<br>• Digite 5 caracteres ASCII ou 10 dígitos hexadecimais para uma chave de 64 bits.<br>• Digite 13 caracteres ASCII ou 26 dígitos hexadecimais para uma chave de 128 bits.<br>Quando a criptografia WPA e WEP estão ativadas ao mesmo tempo, apenas as chaves 2 e 3 são disponibilizadas para criptografia WEP. |

| Campo | Descrição |
|---|---|
| **Current Network Key (Chave de rede atual)** | Selecione a chaves de criptografia (transmissão) quando a criptografia WEP está ativada. |
| **PassPhrase** | Define o texto a ser usado para geração de chaves WEP. |

# Página avançada wireless 802.11

Configure as taxas de dados e os limites Wi-Fi.



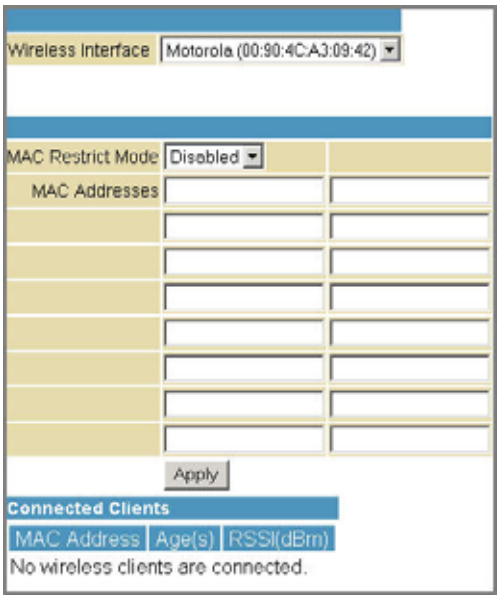

**Descrições de campos da Página avançada wireless 802.11**

| Campo | Descrição |
|---|---|
| **54g™ Mode (Modo 54g™)** | Define estes modos de rede:<br>54g Auto (54g automático)<br>54g Performance (Desempenho 54g)<br>54g LRS (LRS 54g)<br>802.11b only (802.11b apenas)<br>54g Auto (54g automático) aceita clientes 54g, 802.11g e 802.11b, mas otimiza o desempenho com base no tipo de clientes conectados. 54g Performance (Desempenho 54g) aceita apenas clientes 54g e oferece o maior desempenho geral; as redes 802.11b vizinhas podem ter uma diminuição no desempenho. 54g LRS (LRS 54g) interopera com a maior variedade de clientes 54g, 802.11g e 802.11b. 802.11b aceita apenas clientes 802.11b. |

| Campo | Descrição |
|---|---|
| **Basic Rate Set (Conjunto de taxas básicas)** | Determina quais taxas são anunciadas como taxas básicas. O padrão usa os padrões do driver. "All" (Tudo) define todas as taxas disponíveis como taxas básicas. |
| **54g™ Protection (Proteção 54g™)** | Melhora o desempenho no modo Auto usando a proteção RTS/CTS em redes 802.11g + 802.11b mistas. Desative a proteção para maximizar o rendimento 802.11g na maioria das condições. |
| **XPress™ Technology (Tecnologia XPress™)** | Aumenta o rendimento e a eficácia Wi-Fi usadas quando há redes wireless mistas na área adjacentes de redes 802.11a/b/g. |
| **Afterburner™ Technology (Tecnologia Afterburner™)** | Aprimora o padrão Wi-Fi 802.11g aumentando o rendimento em 40%. |
| **Rate (Taxa)** | Impõe a taxa de transmissão para o AP como uma velocidade específica. "Auto" oferece o melhor desempenho em quase todas as situações. |
| **Output Power (Potência de saída)** | Define a potência de saída como uma porcentagem da capacidade máxima do hardware. |
| **Beacon Interval (Intervalo do indicador)** | Define o intervalo do indicador para o AP. O padrão é 100, que é adequado para quase todos os aplicativos. |
| **DTIM Interval (Intervalo DTIM)** | Define o intervalo de ativação para clientes no modo Power Save (Economia de energia). Quando um cliente está executando nesse modo, os valores de Lower SVG1501 bin (Caixa inferior do SVG1501) oferecem melhor desempenho, mas diminuem o tempo de vida da bateria do cliente; valores mais altos oferecem menor desempenho, mas um tempo de vida da bateria do cliente mais longa. |
| **Fragmentation Threshold (Limite de fragmentação)** | Define o limite de fragmentação. Os pacotes que excedam esse limite são fragmentados em pacotes menores que o limites antes da transmissão do pacote. |
| **RTS Threshold (Limite RTS)** | Define o limite RTS. Os pacotes que excedem esse limite fazem com que o AP execute uma troca RTS/CTS para reservar a mídia wireless antes da transmissão do pacote. |

# Página Controle de acesso wireless 802.11

Configure o Controle de acesso para o AP e o status nos clientes conectados.

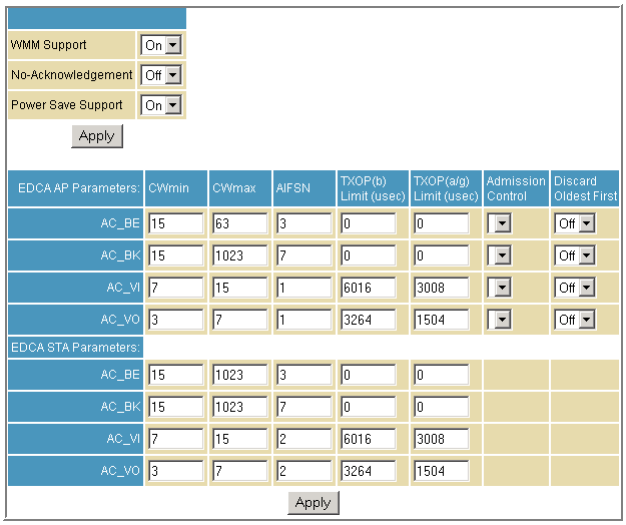



**Descrições de campos da Página Controle de acesso wireless 802.11**

| Campo | Descrição |
|---|---|
| **Wireless Interface (Interface wireless)** | Mostra o endereço MAC da placa wireless instalada. Não é configurável. |
| **MAC Restrict Mode (Modo de restrição MAC)** | Seleciona se os clientes wireless com o endereço MAC especificado têm permissão ou não de acesso wireless.<br>Selecione **Disabled** (Desativado) para permitir todos os clientes. |
| **MAC Address (Endereço MAC)** | Lista os endereços MAC do cliente wireless com ou sem permissão de acesso com base na definição Restrict Mode (Modo de restrição). Formatos de endereço MAC de entrada válidos são XX:XX:XX:XX:XX:XX e XX-XX-XX-XX-XX-XX. |
| **Connected Clients (Clientes conectados)** | Lista os clientes wireless conectados. Quando um cliente se conecta ou sai da rede, isso é adicionado ou removido da lista, Age (Idade) é o tempo desde que os dados foram transmitidos ou recebidos do cliente. |

# Página Multimídia Wi-Fi wireless 802.11

Configure a qualidade de serviço (QoS, Quality of Service) da multimídia Wi-Fi.

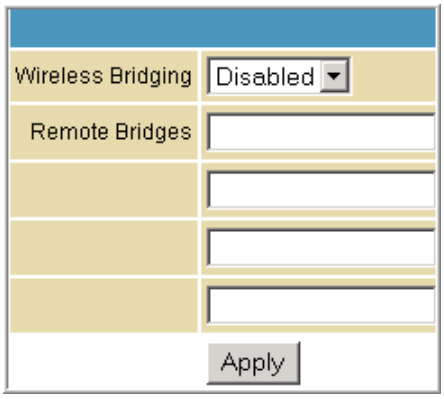



**Descrições de campos da Página Multimídia Wi-Fi wireless 802.11**

| Campo | Descrição |
|---|---|
| **WMM Support (Suporte WMM)** | Define o suporte WMM como Auto (Automático), On (Ligado) ou Off (Desligado).<br>Se ativado (Automático ou Ligado), o Elemento de Informações WME é incluído em quadros do indicador. |
| **No-Acknowledgement (Sem confirmação)** | Define o suporte No-Acknowledgement (Sem confirmação) como On (Ligado) ou Off (Desligado).<br>Quando Ligado, as confirmações de dados não são transmitidas. |
| **Power Save Support (Suporte para economia de energia)** | Define o suporte Power Save (Economia de energia) como On (Ligado) ou Off (Desligado).<br>Quando Ligado, o AP enfileira pacotes para STAs que estejam no modo de economia de energia. Os pacotes enfileirados são transmitidos quando o STA notificado o AP de que deixou no modo Power Save (Economia de energia). |
| **EDCA AP Parameters (Parâmetros AP EDCA)** | Especifica os parâmetros para o tráfego transmitido do AP para o STA em quatro categorias de acesso:<br>Admission control (Controle de admissão) especifica se deve ser forçado para as categorias de acesso. Discard Oldest First (Descartar primeiro mais antigo) especifica a política de descarte para as filas. "On" (Ativado) descarta o primeiro mais antigo; "Off" (Desativado) descarta o primeiro mais recente. |
| **EDCA STA Parameters (Parâmetros STA EDCA)** | Especifica os parâmetros de transmissão para o tráfego transmitido do STA para o AP em quatro categorias de acesso |

# Página Ponte wireless 802.11

Ativa a ponte wireless.




**Descrições de campos da Página Ponte wireless 802.11**

| Campo | Descrição |
|---|---|
| **Wireless Bridging (Ponte wireless)** | Ativa ou desativa a ponte wireless. |
| **Remote Bridges (Pontes remotas)** | Construa uma tabela de endereços MAC de ponte remota autorizados para estabelecer uma ponte wireless. Você pode se conectar a até quatro pontes remotas. Geralmente, você deve inserir seu endereço MAC do AP na ponte remota. |

# Configuração da LAN wireless

Você pode usar o SVG1501 como um ponto de acesso para uma LAN wireless LAN (WLAN) sem alterar as definições padrão.

> ***CUIDADO:*** *Para impedir intromissão ou o acesso não autorizado, ative a segurança wireless quando sua WLAN estiver em funcionamento. As definições padrão não oferecem segurança wireless.*

Para ativar a segurança para sua WLAN:

- Criptografe as transmissões da LAN wireless
- Restrinja o acesso à LAN wireless para impedir intrusões adicionais não autorizadas na WLAN usando a Página Controle de acesso wireless 802

> ***CUIDADO:*** *Nunca forneça sua passphrase SSID, WPA ou WEP, ou chave WEP para uma pessoa que não esteja autorizada a usar sua WLAN.*

Não tente configurar o SVG1501 usando uma conexão wireless.

Conecte pelo menos um computador à porta Ethernet do SVG1501.

Configure cada cliente (estação) wireless para acessar o SVG1501.

Mantenha os componentes wireless afastados de janelas. Isso diminui a força do sinal fora da área desejada.

## Criptografia das transmissões da LAN wireless

Para impedir a exibição não autorizada dos dados transmitidos na WLAN, você deve criptografar as transmissões wireless. Escolha um dos seguintes:

**Criptografia das transmissões da LAN wireless**

| Configure no SVG1501 | Necessário em cada cliente wireless |
|---|---|
| **Se todos os seus clientes wireless suportarem o WPA (Wi-Fi Protected Access, acesso protegido Wi-Fi), a Motorola recomenda a configuração do WPA no SVG1501** | Se você usar uma passphrase de chave pré-compartilhada local (WPA-PSK), deve configurar a passphrase idêntica no SVG1501 e em cada cliente wireless. As definições domésticas e para pequenos escritórios geralmente usam uma passphrase local. |
| **Caso contrário, configure o WEP no SVG1501** | Você deve configurar a chave WEP idêntica no SVG1501 e em cada cliente wireless. |

A Motorola recomenda o uso do WPA, em vez do WEP, se todos os seus clientes wireless suportarem criptografia WPA. As vantagens do WPA incluem:

- Criptografia mais forte e mais segura
- Autenticação para garantir que apenas usuários autorizados possam efetuar login na WLAN
- Configuração mais fácil
- Algoritmo padrão em todos os produtos compatíveis para gerar uma chave a partir de uma passphrase textual
- Incorporação no novo padrão de rede wireless IEEE 802.11i

Para novas LANs wireless, a Motorola recomenda a aquisição de adaptadores clientes que suportem criptografia WPA.

# Instalação de clientes wireless

> ***Observação***: *Use o CD-ROM de Instalação do SVG1501para definir a segurança do cliente. A senha está localizada na etiqueta do gateway.*

Para cada computador cliente wireless, siga as instruções fornecidas com o adaptador e as etapas abaixo para instalar o adaptador wireless:

1. Insira o CD-ROM do adaptador a unidade de CD-ROM no cliente.
2. Instale o software do dispositivo usando o CD.
3. Insira o adaptador no slot PCMCIA ou PCI ou conecte-o à porta USB.
4. Configure o adaptador para obter um endereço IP automaticamente.

Em um PC com o Wireless Client Manager instalado, o ícone  é exibido na barra de tarefas do Windows. Clique duas vezes no ícone para iniciar o utilitário. Talvez seja necessário fazer o seguinte para usar um computador cliente wireless para acessar a Internet:

**Configuração de clientes wireless**

| Se você: | Você precisa fazer isto em cada cliente: |
|---|---|
| **Configurou o WPA no SVG1501** | Configurar um cliente wireless para o WPA ou WPA2 |
| **Configurou o WEP no SVG1501** | Configurar um cliente wireless para o WEP |
| **Configurou o nome da rede wireless no SVG1501** | Configurar um cliente wireless com o nome da rede (SSID) |
| **Configurou uma lista de controle de acesso MAC no SVG1501** | Nenhuma configuração do cliente necessária |

## Instalação de um cliente wireless para o WPA

Se você ativou o WPA e definiu uma passphrase PSK configurando o WPA no SVG1501, deve configurar a mesma passphrase (chave) em cada cliente wireless. O SVG1501 não pode autenticar um cliente se:

- O WPA estiver ativado no SVG1501, mas não no cliente
- A passphrase do cliente não corresponder à passphrase PSK do SVG1501

> ***CUIDADO:*** *Nunca forneça a passphrase PSK para alguém que não esteja autorizado a usar sua WLAN.*

## Configuração de um cliente wireless para o WEP

Se você ativou o WEP e definiu uma chave configurando o WEP no SVG1501, deve configurar a mesma chave WEP em cada cliente wireless. O SVG1501 não pode autenticar um cliente se:

- A Autenticação de chave compartilhada estiver ativada no SVG1501, mas não no cliente
- A chave WEP do cliente não corresponder à chave WEP do SVG1501

Para todos os adaptadores wireless, você deve inserir a chave WEP de 64 ou 128 bits gerada pelo SVG1501.

> ***CUIDADO:*** *Nunca forneça a chave WEP para alguém que não esteja autorizado a usar sua WLAN.*

## Configuração de um cliente wireless com o nome da rede (SSID)

Depois de especificar o nome da rede na Página Básica Wireless, muitas placas ou adaptadores wireless verificam automaticamente um ponto de acesso, como o SVG1501 e o canal e taxas de dados adequados. Se a placa exigir que você inicie manualmente a verificação de um ponto de acesso, siga as instruções na documentação fornecida com a placa. Você deve inserir o mesmo SSID na definição da configuração wireless do dispositivo para comunicação com o SVG1501.

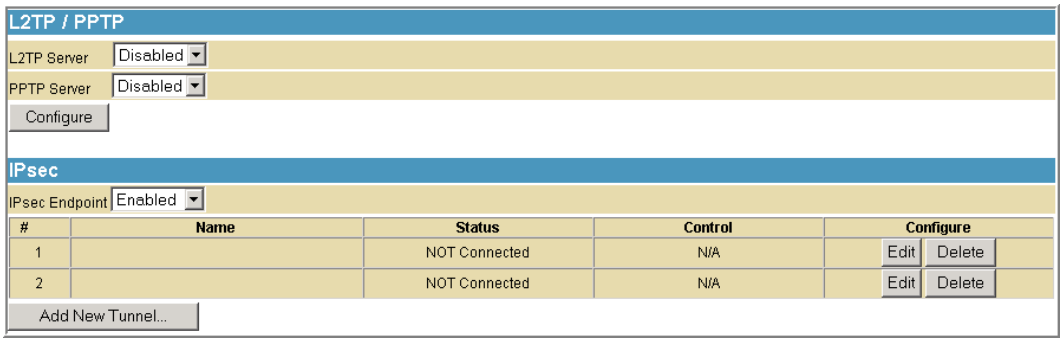
# 10 Páginas VPN

As páginas **VPN** permitem configurar e gerenciar túneis VPN.

Você pode clicar na opção do submenu VPN para exibir ou alterar as informações de configuração dessa opção.

## Página básica VPN

Ative protocolos VPN e gerencie túneis VPN.

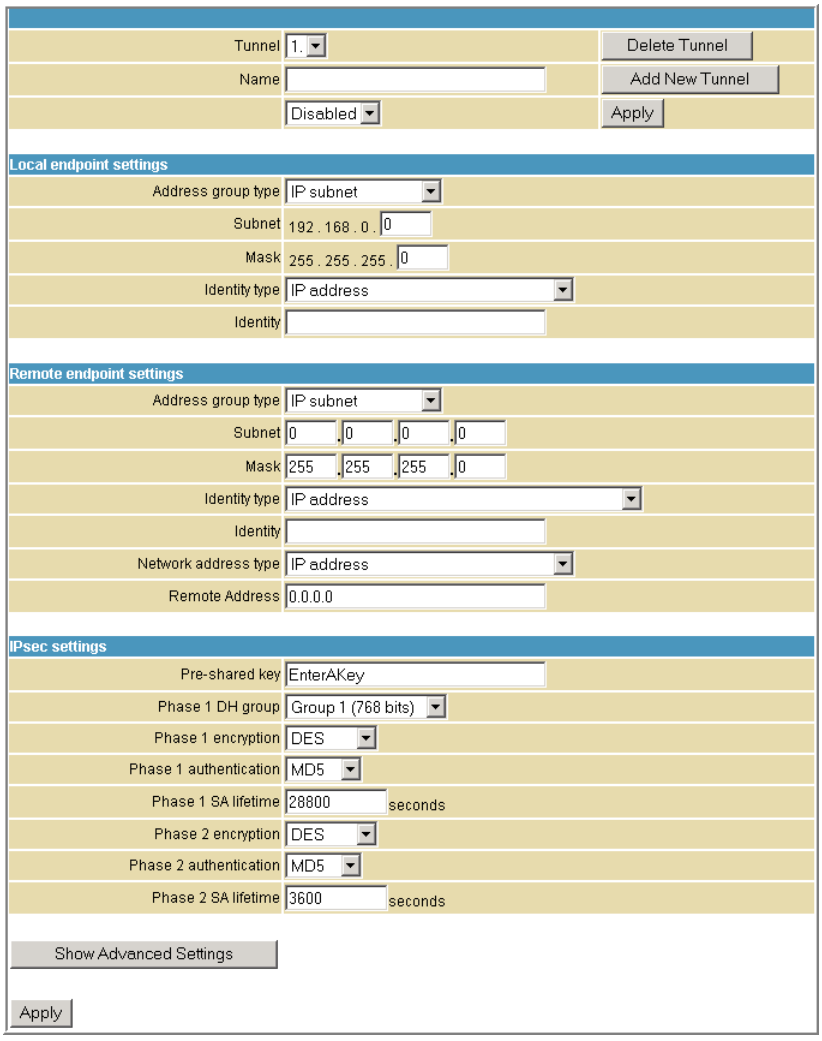



| Campo | Descrição |
|---|---|
| **L2TP Server (Servidor L2TP)** | Ativa ou desativa o Layer 2 Tunneling Protocol |
| **PPTP Server (Servidor PPTP)** | Ativa ou desativa o Point-to-Point Protocol |
| **IPsec Endpoint (Terminal IPsec)** | Ativa ou desativa o protocolo Internet Protocol Security |
| **Add New Tunnel (Adicionar novo túnel)** | Crie uma nova configuração de túnel e anexe-o à tabela.<br>Clique em **Edit** (Editar) para adicionar o nome e constructos desse túnel. |

# Página IPsec VPN

Você pode configurar vários túneis VPN para diversos computadores clientes e armazenar diferentes túneis, mas não pode ativá-los para facilitar o uso com conexões e/ou computadores clientes que não usados constantemente.

Para cada configuração de túnel armazenada, seus parâmetros IPsec exclusivos são armazenados usando a seção IPsec Settings (Configurações de IPsec) na parte inferior da página. Clique em **Show Advanced Settings** (Mostrar configurações avançadas) na parte inferior da página para exibir os recursos avançados que controlam o gerenciamento e a negociação de chave IPSEC com o terminal extremo.



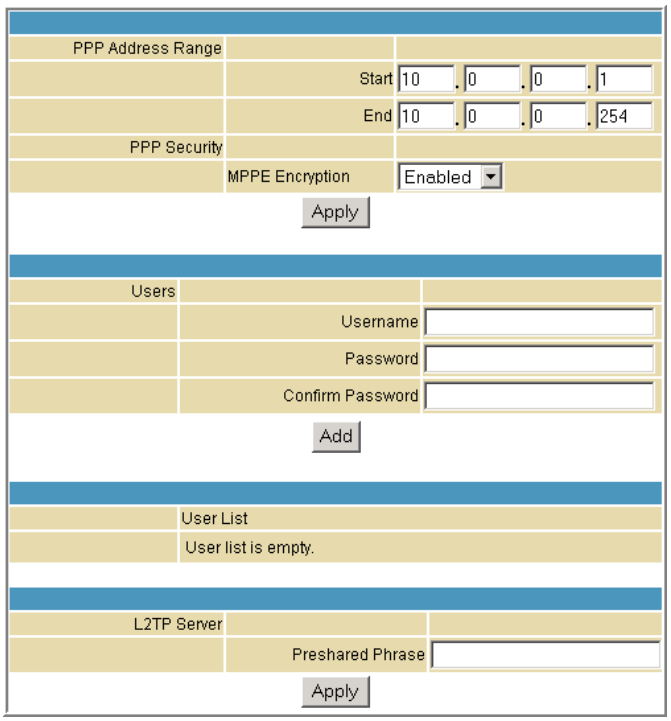
| Campo | Descrição |
|---|---|
| **Tunnel (Túnel)** | Configure cada túnel individualmente. Os túneis predefinidos são listados pelo nome da predefinição. |
| **Name (Nome)** | Atribua um nome genérico para um grupo de definições a um único túnel.<br>Depois de inserir o nome do túnel apropriado pela primeira vez, clique em **Add New Tunnel** (Adicionar novo túnel) para criar um cabeçalho para as configurações do túnel selecionadas na lista suspensa **Tunnel** (Túnel). Se você não atribuir um nome, os túneis são numerados seqüencialmente. |
| **Enable drop-down (Ativar drop-down)** | Depois de nomear e configurar um túnel VPN, você pode armazená-lo como desativado ou ativado na lista suspensa Enable/Disable (Ativar/Desativar).<br>Clique em **Apply** (Aplicar) para alternar entre "Enable/Disable" (Ativar/Desativar). |
| **Configurações do terminal local**<br>**Tipo de grupo de endereços** | Defina o grupo de acesso VPN local como um dos seguintes tipos de grupo:<br>**Endereço IP único** — para um computador, digite o endereço IP do computador específico<br>**Intervalo de endereços IP** — para um pequeno intervalo de computadores, digite os endereços IP inicial e final do grupo de endereços IP consecutivos que terão acesso ao túnel VPN<br>**Sub-rede IP**— para uma sub-rede/rede inteira, digite a sub-rede e máscara do intervalo de endereços IP e sub-rede IP. Digite os endereços IP inicial e final do grupo de endereços IP consecutivos que terão acesso ao túnel VPN. |
| **Identity Type (Tipo de identidade)** | Defina o tipo de identidade do terminal local para usar automaticamente o endereço IP da WAN do roteador ou como um endereço IP especificado pelo usuário, nome completo do domínio (FQDN, Fully Qualified Domain Name) ou endereço de e-mail. O terminal extremo usa isso para identificar o ponto de término e o handshake do VPN.<br>O terminal VPN remoto no outro lado do túnel deve ter as mesmas configurações para as configurações do terminal remoto. |
| **Identity (Identidade)** | Digite a cadeia de identidade.<br>Para o endereço IP, digite *x.x.x.x.*<br>Para o FQDN, digite *seudomínio.com*<br>Para a identidade do endereço de e-mail, digite *seunome@domínio.com*<br>O terminal VPN remoto no outro lado do túnel deve ter as mesmas configurações para as configurações do terminal remoto. |

| Campo | Descrição |
|---|---|
| **Remote Endpoint Settings (Configurações do terminal remoto)**<br>**Address group type (Tipo de grupo de endereços)** | Defina o grupo de acesso VPN remoto para um dos seguintes tipos de grupo:<br>**Endereço IP único** — para um computador, digite o endereço IP do computador específico<br>**Intervalo de endereços IP** — para um pequeno intervalo de computadores, digite os endereços IP inicial e final do grupo de endereços IP consecutivos que terão acesso ao túnel VPN.<br>**Sub-rede IP** — para uma sub-rede/rede inteira, digite a sub-rede e a máscara<br>Para um intervalo de endereços IP e sub-rede IP, digite os endereços IP inicial e final do grupo de endereços IP consecutivos que terão acesso ao túnel VPN.<br>O terminal VPN remoto no outro lado do túnel deve ter as mesmas configurações para as configurações do terminal local. |
| **Identity type (Tipo de identidade)** | Defina o tipo de identidade do terminal remoto para usar automaticamente o endereço IP do terminal remoto ou como um endereço IP especificado pelo usuário, nome completo do domínio ou endereço de e-mail. Essa é a identidade que o terminal extremo usa para identificação do ponto de término e handshake do VPN.<br>O terminal VPN remoto no outro lado do túnel deve ter as mesmas configurações para as configurações do terminal local. |
| **Identity (Identidade)** | Digite a cadeia de identidade:<br>Para o endereço IP, digite **x.x.x.x**.<br>Para o FQDN, digite *seudomínio.com*<br>Para a identidade do endereço de e-mail, digite *seunome@domínio.com*<br>O terminal VPN remoto no outro lado do túnel deve ter as mesmas configurações para as configurações do terminal local. |
| **Network address type (Tipo de endereço de rede)** | Selecione o tipo de endereço da WAN do terminal remoto: endereço IP ou nome completo do domínio |
| **Remote Address (Endereço remoto)** | Digite o endereço IP do terminal remoto ou seu FQDN. |
| **IPsec Settings (Configurações IPsec)** | Associe uma das fases da Associação de Segurança (SA, Security Association) ao túnel VPN. A fase 1 cria um SA IKE. Após a conclusão da fase 1, a fase 2 cria um ou mais Sas IPSEC, que são usados para chavear sessões IPSEC. |
| **Pre-shared key (Chave pré-compartilhada)** | Digite o campo "Pre-shared Key" (Chave pré-compartilhada) se um lado do túnel VPN estiver usando um identificador de firewall exclusivo (ou Chave pré-compartilhada). |

| Campo | Descrição |
|---|---|
| **Phase 1 DH group (Grupo DH fase 1)** | Selecione um dos grupos Diffie-Hellman: 768 bits, 1024 bits ou 1536 bits.<br>Diffie-Hellman é uma técnica de criptografia que usa chaves públicas e privadas para criptorafia e decriptografia. Quanto maior o número de bits, mais segura a criptografia. Opções: Grupo 1 (768 bits), Grupo 2 (1024 bits) ou Grupo 5 (1536 bits). |
| **Phase 1 encryption (Criptografia fase 1)** | Proteja a conexão VPN entre os terminais: DES, 3DES, AES-128, AES-192 ou AES-256.<br>Selecione qualquer criptografia, mas de forma com que os terminais extremos sejam iguais. As configurações comuns de criptografia são 3DES e AES. |
| **Phase 1 authentication (Autenticação fase 1)** | Defina a Autenticação, outro nível de segurança, como SHA ou MD5<br>A Motorola recomenda o SHA, pois é mais seguro, mas você pode usar a autenticação desde que a outra extremidade do túnel VPN use o mesmo método. |
| **Phase 1 SA lifetime (Tempo de vida SA fase 1)** | Especifica o tempo de vida de chaves de rotação individuais.<br>Digite o número de segundos para duração da chave até que uma nova negociação de chave seja feita entre cada terminal. A definição padrão é 28.800 segundos.<br>Um tempo de vida mais curto geralmente é mais seguro, pois daria ao agressor um tempo menor para tentar violar a chave, no entanto a negociação de chave utiliza largura de banda, portanto o rendimento de rede é sacrificado com tempos de vida curtos. As entradas são geralmente em milhares ou dezenas de milhares de segundos. |

# Página L2TP/PPTP VPN

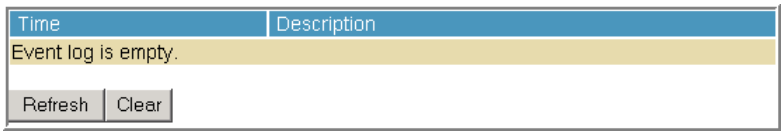
Configure as opções do servidor L2TP e PPTP.




| Campo | Descrição |
|---|---|
| **PPP Address Range (Intervalo de endereços PPP)**<br>**Start (Início)**<br>**End (Fim)** | Especifique o intervalo de endereços IP inicial e final para que, quando o túnel for configurado, o lado do cliente e do servidor obtenham seu endereço IP desse intervalo especificado. |
| **PPP Security**<br>**MPPE Encryption (Criptogafia MPPE de segurança PPP)** | Ative ou desative o Microsoft Point to Point Encryption (MPPE). É um tipo de criptografia de link, significando que os dados enviados juntos com este túnel são criptografados, usados no PPTP. |
| **Username (Nome de usuário)** | Autentica o túnel criado entre o cliente e o servidor |
| **Password (Senha)** | Digite uma senha do usuário para autenticação. |
| **Confirm Password (Confirmar senha)** | Digite a senha novamente para confirmação. |
| **Preshared Phrase (Frase pré-compartilhada)** | Autentica o servidor L2TP (Layer 2 Tunneling Protocol). |

# Página Registro de eventos VPN

Exiba o Registro de eventos VPN, que mostra um histórico de conexões VPN e atividade em ordem cronológica e o endereço IP de terminais remotos e locais no túnel.




- Clique em **Refresh** (Renovar) para atualizar a tabela Registro de eventos para mostrar as alterações desde que a página da Web foi carregada pela última vez.
- Clique em **Clear** (Limpar) para limpar a tabela de registros de seu conteúdo atual. Apenas os dados mais recentes aparecem.

# 11 Páginas MTA

Use a Internet para fazer ligações telefônicas. O MTA (Multimedia Terminal Adapter, adaptador de terminal multimídia) suporta as funções básicas do telefone, como ligações de três vias, correio de voz e transmissões de fax.

## Página Status MTA

Exibe o status de inicialização do MTA.

| Startup Procedure | |
|---|---|
| **Task** | **Status** |
| **Telephony DHCP** | Completed |
| **Telephony Security** | Disabled |
| **Telephony TFTP** | Completed |
| **Telephony Call Server Registration** | L1: Operational / L2: Operational |
| **Telephony Registration Complete** | Pass With Warnings |

| MTA Line State | |
|---|---|
| **Line 1** | On-Hook |
| **Line 2** | On-Hook |

## Página DHCP MTA

Exibe as informações de leasing DHCP do MTA.

| Lease Paramteres | |
|---|---|
| **FQDN** | mta001a66080b06.swdev.net |
| **IP Address/Submask** | 206.19.81.247 / 255.255.255.0 |
| **Gateway** | 206.19.81.1 |
| **Bootfile** | tftp://sbvprov3.swdev.net/001A66080B06.bin |
| **Primary DNS** | 198.102.87.133 |
| **Secondary DNS** | 0.0.0.0 |

| Lease Timers | |
|---|---|
| **Lease Time Remaining** | D: 00 H: 00 M: 27 S: 58 |
| **Rebind Time Remaining** | D: 00 H: 00 M: 12 S: 58 |
| **Renew Time Remaining** | D: 00 H: 00 M: 01 S: 43 |

| PacketCable DHCP Option 122 | |
|---|---|
| **SNMP Entity (Sub-option 3)** | sbvprov3.swdev.net |
| **Kerberos Realm (Sub-option 6)** | |
| **Provisioning Timer (Sub-option 8)** | |

# Página QoS MTA

Esta página exibe os parâmetros de qualidade de serviço (QoS, Quality of Service) do MTA.

| Error Codewords | |
|---|---|
| **Unerrored Codewords** | 128653228 |
| **Correctable Codewords** | 0 |
| **Uncorrectable Codewords** | 0 |

| Payload Header Suppression | |
|---|---|
| **PHS Status** | ON |

**Service Flows**

| SFID | Service Class Name | Direction | Primary Flow | Packets |
|---|---|---|---|---|
| **3543** | | Upstream | No | 23806 |
| **3544** | | Downstream | No | 0 |
| **4133** | | Upstream | No | 6 |
| **4134** | | Downstream | No | 0 |

# Página Provisionamento MTA

Esta seção exibe os detalhes de provisionamento MTA sobre sua conexão telefônica VoIP do SVG1501.

| MTA Config File | |
|---|---|
| **Filename** | tftp://sbvprov3.swdev.net/001A66080B06.bin |
| **Contents** | MTA Config File Contents<br>==========<br>.1.3.6.1.4.1.4491.2.2.1.1.1.7.0 1<br>.1.3.6.1.2.1.2.2.1.7.9 1<br>.1.3.6.1.2.1.2.2.1.7.10 1<br>.1.3.6.1.4.1.4491.2.2.2.1.1.10.0 2<br>.1.3.6.1.4.1.4491.2.2.2.1.1.8.0 24<br>.1.3.6.1.4.1.4491.2.2.2.1.1.9.0 40<br>.1.3.6.1.4.1.4491.2.2.2.1.1.12.0 2427<br>.1.3.6.1.4.1.4491.2.2.2.1.1.5.0 FFC00000<br>.1.3.6.1.4.1.4491.2.2.2.1.1.6.0 FFC00000<br>.1.3.6.1.4.1.4491.2.2.2.1.1.7.0 FFC00000<br>.1.3.6.1.4.1.4491.2.2.2.1.2.1.1.18.9 10<br>.1.3.6.1.4.1.4491.2.2.2.1.2.1.1.18.10 10<br>.1.3.6.1.4.1.4491.2.2.2.1.2.1.1.27.9 1<br>.1.3.6.1.4.1.4491.2.2.2.1.2.1.1.27.10 1<br>.1.3.6.1.4.1.4491.2.2.2.1.2.1.1.28.9 8<br>.1.3.6.1.4.1.4491.2.2.2.1.2.1.1.28.10 8<br>.1.3.6.1.4.1.4491.2.2.2.1.2.1.1.2.9 2427<br>.1.3.6.1.4.1.4491.2.2.2.1.2.1.1.2.10 2427<br>.1.3.6.1.4.1.4491.2.2.2.1.2.1.1.1.9 SBVPROV3-CA.SWDEV.NET<br>.1.3.6.1.4.1.4491.2.2.2.1.2.1.1.1.10 SBVPROV3-CA.SWDEV.NET<br>.1.3.6.1.4.1.1166.1.200.2.36.0 128<br>Vendor Specific TLV (TLV-43) Start: VendorID 0803002040<br>Vendor Specific TLV (TLV-43) End: Num of TLV processed (in hex) 1D |

| Enterprise MIBs | |
|---|---|
| OID | Value |
| **emtaInhibitSwDownloadDuringCall** | false(2) |
| **emtaFirewallEnable** | true(1) |
| **emtaRingWithDCOffset** | false(2) |
| **emtaIncludedInCmMaxCpe** | false(2) |
| **emtaDhcpOption** | packetCableAndCableHomeObsolete(177) |
| **emtaUseAlternateTelephonyRootCert** | false(2) |
| **emtaEnableDQoSLite** | false(2) |
| **emtaInhibitNcsSyslog** | true(1) |
| **emtaMaintenanceWindowBegin** | Thu Jan 01 00:00:00 1970 |
| **emtaMaintenanceWindowDuration** | 0 |
| **emtaMaintenanceControlMask** | 0xfffffffb0 [maintenanceOnCmReset(0) maintenanceOnMtaReset(2) maintenanceOnCMSLoss(3) ] |
| **emtaMaintenanceQuarantineTimeout** | 120 |
| **emtaMaintenanceDisconnectedTimeout** | 120 |
| **emtaMaintenanceRFDisconnectTimeout** | 300 |
| **emtaSignalingAnnouncementCtrl** | 0x00 |
| **emtaSignalingVoiceJitterBufferType** | jitterBufferTypeAdaptive(2) |
| **emtaSignalingVoiceJitterNomValue** | 30 |
| **emtaSignalingVoiceJitterMinValue** | 0 |
| **emtaSignalingVoiceJitterMaxValue** | 60 |
| **emtaSignalingDataJitterNomValue** | 120 |
| **emtaSignalingDtmfToneRelayRFC2833Support** | true(1) |
| **emtaSignalingRtpBaseReceiveUdpPort** | 53456 |
| **emtaSignalingEndptConnectionCleanupTimeout** | 0 |
| **emtaSignalingEmtaResetCleanupTimeout** | 0 |
| **emtaSignalingT38FaxRelaySupport** | true(1) |

# Página Registro de eventos MTA

Esta página exibe as informações do Registro de eventos MTA e mensagens de diagnóstico geradas pelo MTA para técnicos.

| Time | Priority | ID | Text |
|---|---|---|---|
| Endpoint | | | |
| 2007-08-08 16:25:06 | 5-Information | 35 | MTA Last 24 Hours: Count of No ACK rec'd from Call Agent=0 |
| mta001a66080b06.swdev.net/206.19.81.247 | | | |
| 2007-08-08 16:25:06 | 5-Information | 35 | MTA Last 24 Hours: Average Latency for Response to MGCP Messages=0 ms |
| mta001a66080b06.swdev.net/206.19.81.247 | | | |
| 2007-08-08 16:25:06 | 5-Information | 35 | MTA Last 24 Hours: Average Latency via RTCP Packets=0 ms |
| mta001a66080b06.swdev.net/206.19.81.247 | | | |
| 2007-08-08 16:25:06 | 5-Information | 35 | MTA Last 24 Hours: Maximum Jitter Measurements=0 |
| mta001a66080b06.swdev.net/206.19.81.247 | | | |
| 2007-08-08 16:25:06 | 5-Information | 35 | MTA Last 24 Hours: Average Jitter Measurements=0 |
| mta001a66080b06.swdev.net/206.19.81.247 | | | |
| 2007-08-07 16:25:06 | 5-Information | 35 | MTA Last 24 Hours: Count of No ACK rec'd from Call Agent=0 |

# 12 Solução de problemas

Se as soluções listadas aqui não resolverem seu problema, entre em contato com o provedor de serviços.

Antes de ligar, tente pressionar o botão RESET no painel traseiro do SVG1501.

> ***Observação***: *Pressionar RESET restaura as definições padrão. Você perderá suas definições de configuração personalizadas, incluindo as configurações do Controle dos pais, Firewall e Avançadas.*

A redefinição do SVG1501 pode demorar até 30 minutos. Seu provedor de serviços pode solicitar o status da LED do painel frontal; consulte LEDs do painel frontal e Condições de erro.

## Soluções

**Tabela 1 – Soluções de problemas**

| Problema | Possível solução |
|---|---|
| **A luz de energia está desligada** | Verifique se o SVG1501 está conectado adequadamente à tomada elétrica.<br>Verifique se a tomada elétrica está funcionando.<br>Pressione o botão **RESET**. |
| **Não é possível enviar nem receber dados** | Observe o status das LEDs no painel frontal e consulte LEDs do painel frontal e Condições de erro para identificar o erro. Se você tiver TV a cabo, verifique se a TV está funcionando e se a imagem está nítida. Se você não puder receber seus canais de TV normais, seu serviço de dados não funcionará.<br>Verifique o cabo coaxial no SVG1501 e tomada. Aperte com as mãos, se necessário.<br>Verifique o endereço IP. Siga as etapas para verificar o endereço IP de seu sistema descritas em Configuração do TCP/IP. Ligue para seu provedor de serviços se precisar de um endereço IP.<br>Verifique se o cabo Ethernet está conectado adequadamente ao SVG1501 e ao computador.<br>Verifique a conectividade de qualquer dispositivo conectado via porta Ethernet, verificando as LEDs LINK no painel traseiro. |

| Problema | Possível solução |
|---|---|
| **Cliente(s) wireless não pode(m) enviar nem receber dados** | Execute as quatro primeiras verificações em "Não pode enviar nem receber dados".<br>Verifique a definição Security Mode (Modo de segurança) na Página Rede primária wireless:<br>• Se você ativou o WPA e configurou uma passphrase no SVG1501, verifique se cada cliente wireless afetado tem a passphrase idêntica. Se isso não resolver o problema, verifique se o cliente wireless suporta WPA.<br>• Se você ativou o WEP e configurou uma chave no SVG1501, verifique se cada cliente wireless afetado tem a chave WEP idêntica. Se isso não resolver o problema, verifique se o adaptador wireless do cliente suporta o tipo de chave WEP configurado no SVG1501.<br>• Para eliminar temporariamente o Modo de segurança como um possível problema, desative a segurança.<br><br>Depois de resolver o problema, lembre-se de reativar a segurança wireless.<br>• Na Página Controle de acesso wireless, verifique se o endereço MAC para cada cliente wireless afetado está listado corretamente. |
| **Velocidade de transmissão wireless lenta com WPA ativado** | Na Página Rede primária wireless, verifique se o tipo de criptografia WPA é TKIP. Se todos os seus clientes wireless suportarem AES, altere a Criptografia WPA para AES. |

# LEDs do painel frontal e Condições de erro

As LEDs do painel frontal do SVG1501 apresentam informações de status para as seguintes condições de erro:

**Tabela 2 – LEDs do painel frontal e Condições de erro**

| LED | Status | se, Durante a inicialização: | se, Durante a operação normal: |
|---|---|---|---|
| **POWER (ENERGIA)** | DESLIGADA | O SVG1501 não está conectado adequadamente à tomada elétrica | O SVG1501 está desconectado |
| **RECEIVE (RECEBER)** | PISCANDO | Canal de recebimento downstream não pode ser adquirido | O canal downstream foi perdido |
| **SEND (ENVIAR)** | PISCANDO | Canal de envio upstream não pode ser adquirido | O canal upstream foi perdido |
| **ONLINE (ON-LINE)** | PISCANDO | O registro IP não foi bem-sucedido | O registro IP foi perdido |

# A Licença de software

Gateway de Voz Wireless SURFboard SVG1501

Motorola, Inc.
Home & Networks Mobility Solutions Business [Mobilidade de Redes e do Lar] (“Motorola”)
101 Tournament Drive
Horsham, PA 19044

**IMPORTANTE**: LEIA ESTA LICENÇA DE USO DE SOFTWARE (“LICENÇA”) COM CUIDADO ANTES DE INSTALAR, FAZER DOWNLOAD OU USAR QUALQUER SOFTWARE, DRIVER USB, FIRMWARE E DOCUMENTAÇÕES CORRELATAS (“SOFTWARE”) FORNECIDOS COM O PRODUTO PARA TRANSFERÊNCIA DE DADOS VIA CABO DA MOTOROLA (O “PRODUTO PARA TRANSFERÊNCIA DE DADOS VIA CABO”). AO UTILIZAR O PRODUTO PARA TRANSFERÊNCIA DE DADOS VIA CABO E/OU INSTALAR, FAZER DOWNLOAD OU UTILIZAR QUALQUER SOFTWARE, VOCÊ ESTÁ INDICANDO QUE ACEITA CADA UM DOS TERMOS DESTA LICENÇA. UMA VEZ ACEITA, ESTA LICENÇA SE TORNARÁ UM CONTRATO JURÍDICO ENTRE VOCÊ E A MOTOROLA. OS TERMOS DESTA LICENÇA SE APLICAM A VOCÊ E A QUALQUER FUTURO USUÁRIO DESTE SOFTWARE.

SE VOCÊ NÃO CONCORDAR COM TODOS OS TERMOS DESTA LICENÇA: (I) NÃO INSTALE NEM USE O SOFTWARE E (II) DEVOLVA O PRODUTO PARA TRANSFERÊNCIA DE DADOS VIA CABO E O SOFTWARE (COLETIVAMENTE, “PRODUTO”), INCLUSIVE TODOS OS COMPONENTES, A DOCUMENTAÇÃO E OUTROS MATERIAIS FORNECIDOS COM O PRODUTO, PARA O LOCAL ONDE O ADQUIRIU OU PARA O PROVEDOR DE SERVIÇOS, CONFORME O CASO, PARA OBTER REEMBOLSO INTEGRAL. AO INSTALAR OU USAR O SOFTWARE, VOCÊ CONCORDA EM OBEDECER ÀS CONDIÇÕES DESTE CONTRATO DE LICENÇA.

O Software inclui a mídia digital associada, materiais impressos e qualquer documentação eletrônica ou “on-line”. Os softwares fornecidos por terceiros poderão estar sujeitos a outras licenças de uso entre os usuários finais e os fabricantes de tais Softwares.

O software nunca é vendido. A Motorola concede a licença de uso do Software ao cliente original e a qualquer futuro licenciado somente para uso pessoal e nos termos desta Licença. A Motorola e seus licenciadores terceirizados mantêm a propriedade do Software.

Você pode:

USAR o Software somente para a operação do Produto.

TRANSFERIR o Software (inclusive todos os componentes e materiais impressos) em caráter permanente para outra pessoa, mas somente se ela concordar em aceitar todos os termos desta Licença. Se você transferir o Software, deverá transferir simultaneamente o Produto e todas as cópias do Software (se for o caso) para a mesma pessoa ou destruir as cópias não transferidas.

RESCINDIR a presente Licença, destruindo o Software original e (se for o caso) todas as suas cópias na forma em que estiverem.

Você não pode:

(1) Emprestar, distribuir, alugar, fazer "leasing", ceder, sublicenciar ou transferir por qualquer outro método o Software, no todo ou em parte, para qualquer outra pessoa, exceto conforme permitido no parágrafo TRANSFERIR acima. (2) Copiar ou traduzir o Guia do Usuário incluído com o Software, exceto para uso pessoal. (3) Copiar, alterar, traduzir, descompilar, desmontar ou fazer engenharia reversa no Software, incluindo, sem limitações, modificar o Software de modo a fazê-lo funcionar com hardwares não compatíveis. (4) Remover, alterar ou fazer com que não sejam exibidos quaisquer avisos de copyright ou mensagens iniciais contidas nos Softwares ou na documentação. (5) Exportar o Software ou os componentes do Produto de modo a violar qualquer lei de exportação dos Estados Unidos.

O Produto não foi projetado ou previsto para utilização em controle on-line de aeronaves, tráfego aéreo, navegação aérea ou comunicação de aeronaves; ou ainda em projeto, construção, operação ou manutenção de instalações nucleares. A MOTOROLA E SEUS LICENCIADORES TERCEIRIZADOS REJEITAM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS DE ADEQUAÇÃO PARA OS REFERIDOS USOS. VOCÊ DECLARA E GARANTE QUE NÃO UTILIZARÁ O PRODUTO PARA TAIS FINALIDADES.

A propriedade deste Software, inclusive a propriedade de todos os direitos autorais, direitos sobre os originais, patentes, marcas comerciais e todos os outros direitos de propriedade intelectual subsistentes no supracitado, e todas as adaptações e modificações do supracitado sempre serão da Motorola e de seus licenciadores terceirizados. A Motorola mantém todos os direitos não mencionados de forma explícita nesta Licença. O Software, inclusive quaisquer imagens, figuras, fotografias, animação, vídeo, áudio, música e texto incorporados a ele, é de propriedade da Motorola ou de seus licenciadores terceirizados e protegido pelas leis de direitos autorais dos Estados Unidos e pelas cláusulas dos tratados internacionais. Salvo disposições em contrário expressamente indicadas nesta Licença, a cópia, a reprodução, a distribuição ou a preparação de trabalhos derivados do Software, de qualquer parte do Produto ou da documentação são estritamente proibidas por tais leis e cláusulas de tratados. Nada nesta Licença constitui uma desistência de direitos da Motorola sob a lei de direitos autorais dos Estados Unidos.

Esta Licença e seus direitos relativamente a qualquer assunto abordado por ela são regidos pelas leis do Estado da Pensilvânia, sem referência a conflitos de princípios legais. ESTA LICENÇA SERÁ AUTOMATICAMENTE CANCELADA se você deixar de cumprir seus termos.

A Motorola não se responsabiliza por softwares de terceiros fornecidos como um pacote de aplicativos, ou sob outra forma, junto com o Software.

**DIREITOS RESTRITOS DO GOVERNO DOS E.U.A.**

O Produto e a documentação são fornecidos com DIREITOS RESTRITOS. O uso, a duplicação ou a divulgação por parte do Governo estão sujeitos a restrições, conforme estabelecido no item (c)(1)(ii) da cláusula em 52.227-7013 dos "The Rights in Technical Data and Computer Software" [Direitos em dados técnicos e software de computadores]. A contratada/fabricante é a Motorola, Inc., Home and Networks Mobility Business [Mobilidade de Redes e do Lar], 101 Tournament Drive, Horsham, PA 19044.

Motorola, Inc.
101 Tournament Drive
Horsham, PA 19044 U.S.A.

http://www.motorola.com



567299-004-a
05/2009