Manual WEB do Usuário

R3005G

Versão deste manual: 1.0.0

R3005G | Manual WEB do Usuário

Parabéns, você acaba de adquirir um produto com a qualidade e segurança Intelbras.

O R3005G é um switch de 5 portas Gigabit Ethernet com 1 porta USB.

Este é um produto homologado pela Anatel, o número de homologação se encontra na etiqueta do produto, para consultas utilize o link sistemas.anatel.gov.br/sch (https://sistemas.anatel.gov.br/sch)

ÍNDICE

EXPORTAR PARA PDF

Para exportar este manual para o formato de arquivo PDF, utilize o recurso de impressão que navegadores como Google Chrome® e Mozilla Firefox® possuem. Para acessá-lo, pressione as teclas *CTRL + P* ou clique aqui. Se preferir, utilize o menu do navegador, acessando a aba *Imprimir*, que geralmente fica no canto superior direito da tela. Na tela que será aberta, execute os passos a seguir, de acordo com o navegador:

Google Chrome®: na tela de impressão, no campo *Destino*, clique em *Alterar*, selecione a opção *Salvar como PDF* na seção *Destinos locais* e clique em *Salvar*. Será aberta a tela do sistema operacional solicitando que seja definido o nome e onde deverá ser salvo o arquivo.

Mozilla Firefox®: na tela de impressão, clique em *Imprimir*, na aba *Geral*, selecione a opção *Imprimir para arquivo*, no campo *Arquivo*, defina o nome e o local onde deverá ser salvo o arquivo, selecione *PDF* como formato de saída e clique em *Imprimir*.

PROTEÇÃO E SEGURANÇA DE DADOS

Observar as leis locais relativas à proteção e uso de tais dados e as regulamentações que prevalecem no país. O objetivo da legislação de proteção de dados é evitar infrações nos direitos individuais de privacidade baseadas no mau uso dos dados pessoais.

Tratamento de dados pessoais

Este sistema utiliza e processa dados pessoais como senhas, registro detalhado de chamadas, endereços de rede e registro de dados de clientes, por exemplo.

Diretrizes que se aplicam aos funcionários da Intelbras

- Os funcionários da Intelbras estão sujeitos a práticas de comércio seguro e confidencialidade de dados sob os termos dos procedimentos de trabalho da companhia.
- É imperativo que as regras a seguir sejam observadas para assegurar que as provisões estatutárias relacionadas a serviços (sejam eles serviços internos ou administração e manutenção remotas) sejam estritamente seguidas. Isso preserva os interesses do cliente e oferece proteção pessoal adicional.

Diretrizes que controlam o tratamento de dados

- Assegurar que apenas pessoas autorizadas tenham acesso aos dados de clientes.
- Usar as facilidades de atribuição de senhas, sem permitir qualquer exceção. Jamais informar senhas para pessoas não autorizadas.
- Assegurar que nenhuma pessoa não autorizada tenha como processar (armazenar, alterar, transmitir, desabilitar ou apagar) ou usar dados de clientes.
- Evitar que pessoas não autorizadas tenham acesso aos meios de dados, por exemplo, discos de backup ou impressões de protocolos.
- Assegurar que os meios de dados que não são mais necessários sejam completamente destruídos e que documentos não sejam armazenados ou deixados em locais geralmente acessíveis.
- O trabalho em conjunto com o cliente gera confiança.

Uso indevido e invasão de hackers

As senhas de acesso permitem o alcance e a alteração de qualquer facilidade, como o acesso externo ao sistema da empresa para obtenção de dados, portanto, é de suma importância que as senhas sejam disponibilizadas apenas àqueles que tenham autorização para uso, sob o risco de uso indevido.

A intelbras não acessa, transfere, capta, nem realiza qualquer outro tipo tratamento de dados pessoais a partir deste produto, com exceção aos dados necessários para funcionamento do próprio produto. Para mais informações, consulte o capítulo sobre métodos de segurança do equipamento.

SOBRE O MANUAL

Quando estiver utilizando esse manual perceba que as funções do switch podem variar sua apresentação dependendo de qual versão de software você estiver executando. Todas as *Screenshots*., imagens, parâmetros e descrições documentadas nesse guia são utilizadas unicamente para demonstração.

As informações deste documento e seu conteúdo podem mudar sem aviso prévio. Todos os esforços foram tomados na preparação desse documento para garantir a precisão do seu conteúdo, porém sob todas as informações e recomendações desse documento não constituem garantia de qualquer gênero. Os usuários devem ter total responsabilidade pela aplicação desse produto.

Este manual contém informações para instalação e gerenciamento do switch R3005G. Por favor, leia-o com atenção antes de operar o produto.

Público destinado para o manual

Esse guia é direcionado para gestores de rede os quais estejam familiarizados com conceitos de TI e terminologias de rede.

Convenções

Neste manual as seguintes convenções serão usadas:

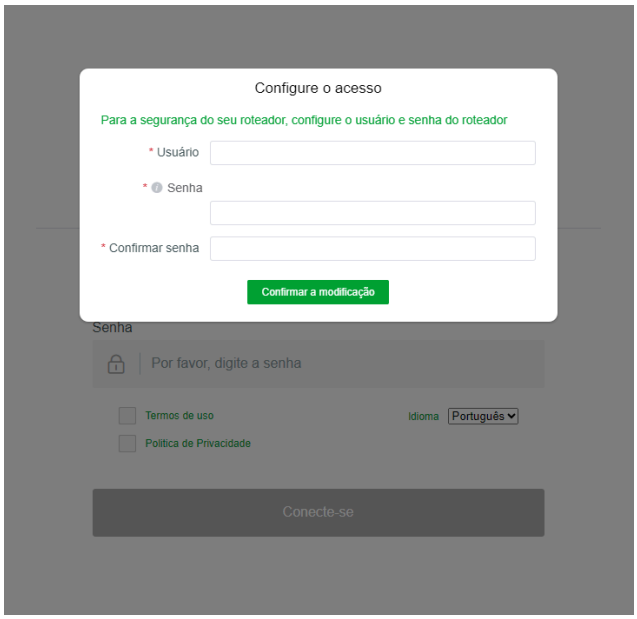
Sistema > Informações > Status: significa que a página Status está dentro do submenu Informações, que está localizada dentro do menu Sistema.

Login na web

Conecte-se

1. Conecte o computador a na porta 1 do R3005G usando um cabo Ethernet.
2. Para acessar o roteador use o endereço IP padrão 192.168.0.1 na web.
3. Inicie um navegador e digite o endereço IP do roteador (padrão: 192.168.0.1) na barra de endereços para acessar a página de login.

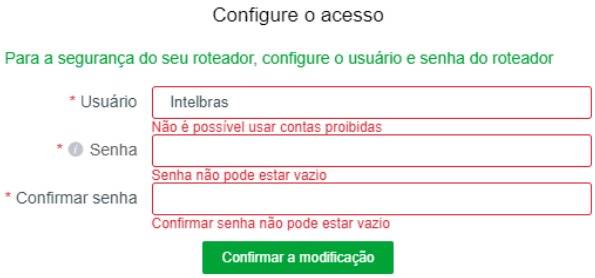
4. Crie seu nome de usuário e senha e clique em confirmar a modificação.



É importante lembrar que não é possível usar as seguintes contas proibidas:

Contas Proibidas			
1001chin	1q2w3e4r	abc123	Admin
admin	Administrador	Administrator	adm
anonymous	asdfgh	author	brasil
Brazil	Changeme	Changeme_123	Changeme@123
Change_Me@123	changeme!@#123	cliente	customer
debug	default	Demo	device
fulano	guest	Intelbras	Intelbras!@#123
Intelbras@123	intelbras	live	lucas123
manager	Master	Mudar@123	none
operator	operations	operacao	password
qwerty	Qwerty123!@#	recover	readonly
role	root	security	senha
senha123	super	superuser	system
sysadmin	taZz@23495859	tech	telecom
telecon	teste	ttnet	user
vizxv	write	zxcvbn	

Se uma conta proibida for inserida, uma notificação será exibida, conforme ilustrado na imagem abaixo:



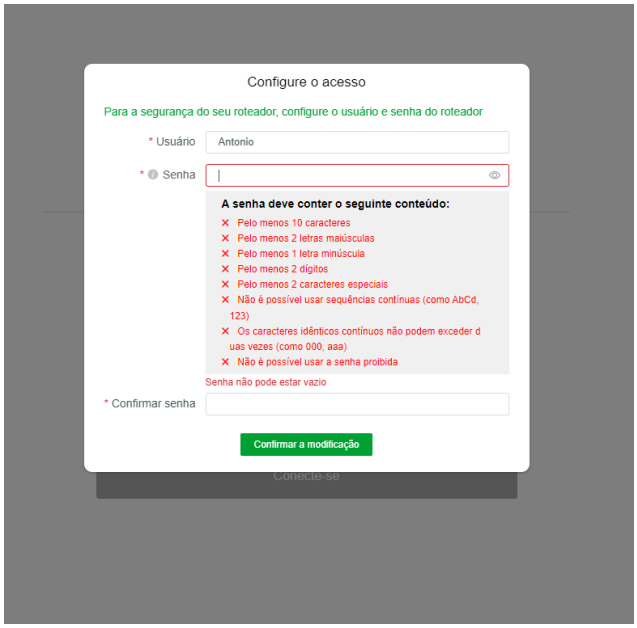
Política de primeiro acesso

- no primeiro acesso ou quando o equipamento for resetado as configurações de fabrica o equipamento estara com todas as portas Wan desabilitadas, somente será possivel acessar pela porta Lan.
- O equipamento não ira se conectar a internet por nenhum protocolo (DHCP, IP estático, PPPoE entre outros) na porta WAN até que a senha seja trocada.

Politica de senhas

Os requisitos mínimos para senhas no R3005G incluem :

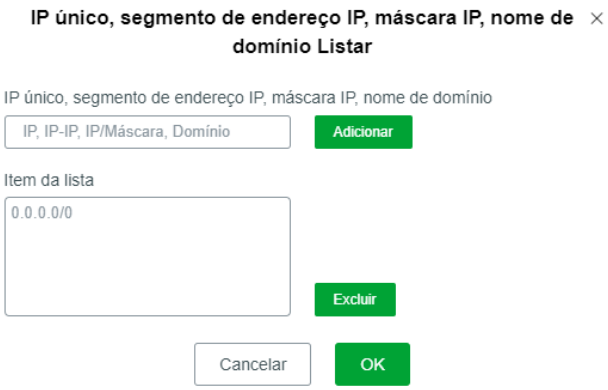
- 10 caracteres
- 2 Letras Maíusculas
- 1 Letra minúscula
- 2 Números
- 2 Caracteres especiais(exemplo: !@#$%¨&*()_+"-='´[~]\,.;/`{^}<>:?).
- Não pode usar Sequências conhecidas (exemplo AbCd, 123, 456).
- Não pode repetir o mesmo caractere por mais de 2x (000, aaa, 222, $$$).
- A senha não pode ser nenhuma das senhas populares (abrir um pop-up ou pagina com a lista de senhas populares e proibidas, a tabela com as principais palavras proibidas está acima).
- Não pode repetir ou ter sido utilizada Anteriormente (esta politica ser aplicada apenas quando a senha for trocada posteriormente).



Implementações de Segurança na Firmware

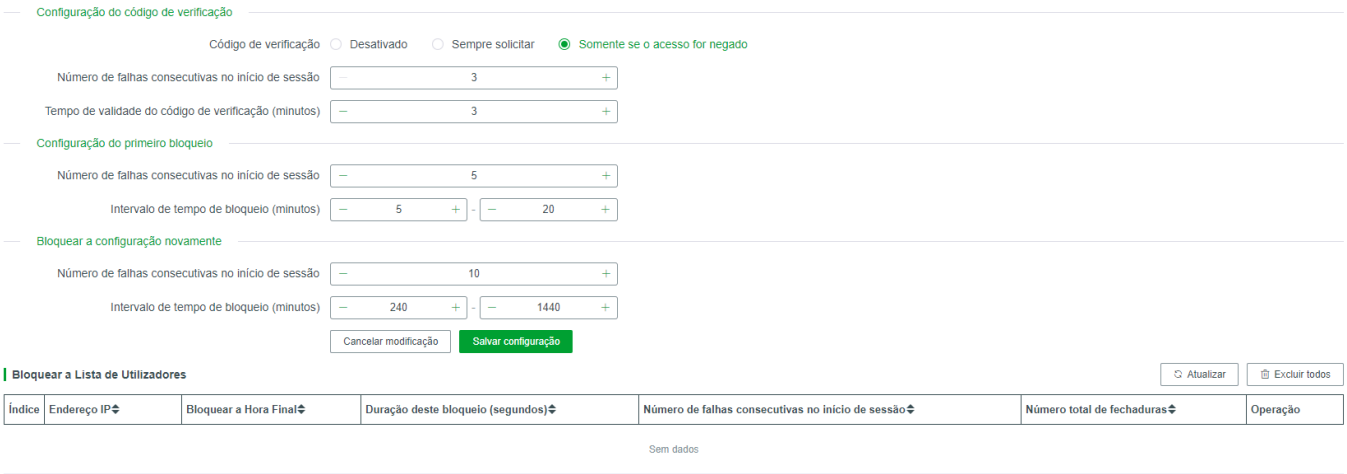
- Por padrão o acesso externo é fechado, bloqueado para todos os endereços. Mesmo o usuário habilitando o acesso remoto da WAN, ele precisa liberar os endereços permitidos (mesmo que seja para especificar liberando o acesso de qualquer lugar).

  Em restrições de origem, adicione o IP, segmento de endereço IP, mascara e nome de dominio para configurar sua ACL.



- Por padrão, qualquer IP que fizer mais de 3 tentativas de acesso deve ser bloqueado por um tempo aleatório entre 10 a 20 minutos, Após esse tempo, o IP fica em uma softlist por 10 minutos.
  - Se houverem múltiplas tentativas de acesso malsucedidas e excederem um limite pré-definido, será necessária uma validação humana com reCAPTCHA.

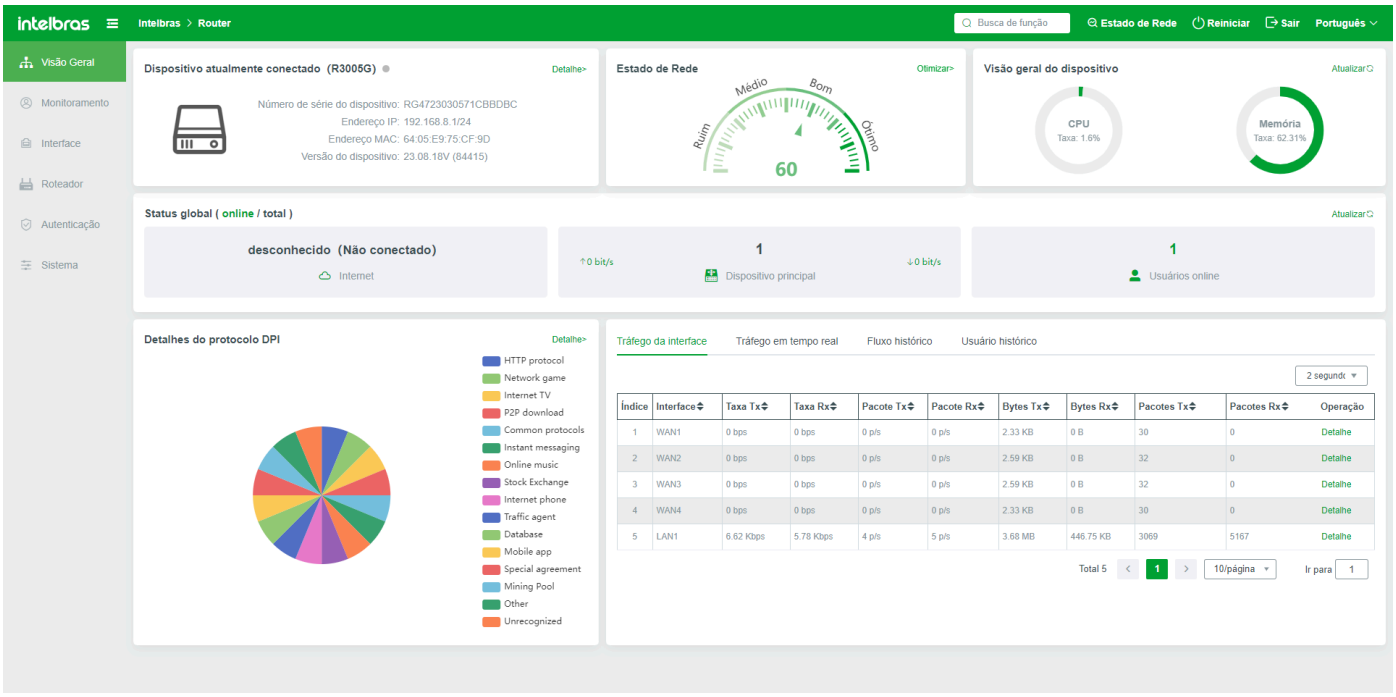
  - Se errar o acesso por mais de 3 vezes durante o período da softlist, o IP deve sera bloqueado por 1 hora.



- A sessão tem um timeout de 60 segundos se não houver nenhuma interação.
- O R3005G irá sugerir a troca de senha a cada 180 dias, sendo este intervalo configurável, e utilizará pop-ups ou outros métodos para notificar o usuário sobre a necessidade de realizar a troca de senha.

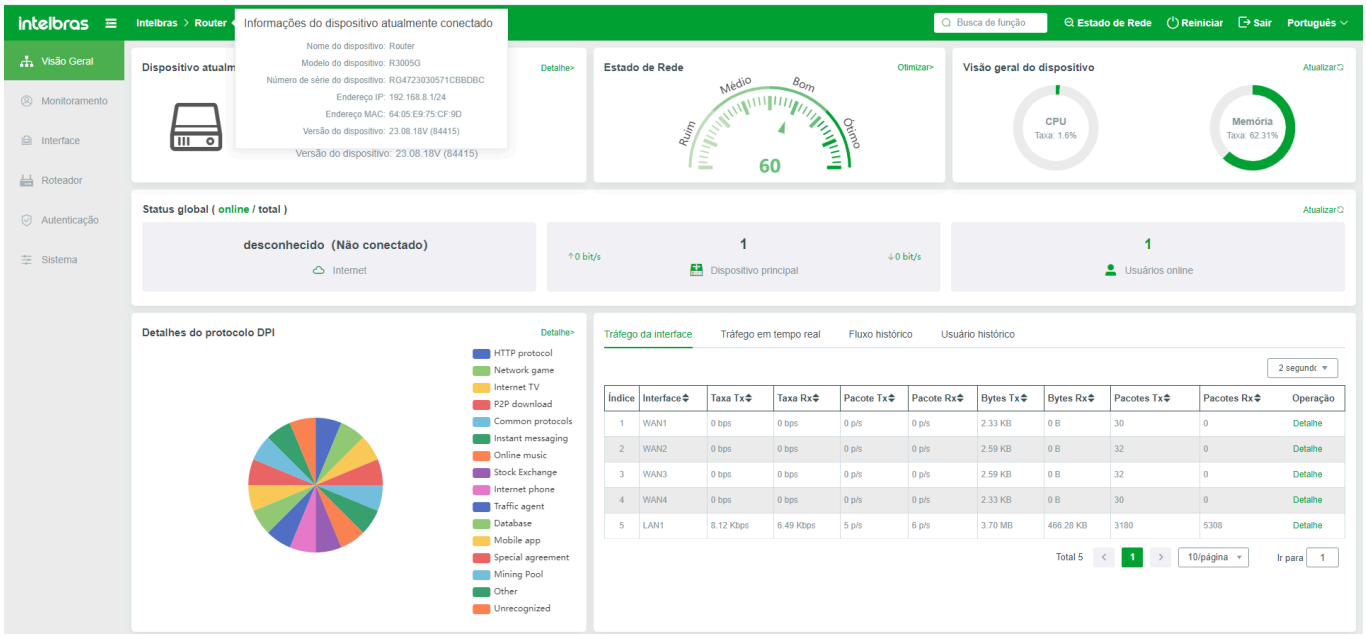
Visão Geral

A página de gerenciamento do sistema de gerenciamento completo do R3005G (página de visão geral) concentra-se principalmente na unificação de dados. As informações do dispositivo, terminal e os dados relevantes de toda a rede são exibidos nesta página. A maioria das seções correspondentes de estatísticas de dados pode ser clicada para acessar a página de detalhes dos dados.

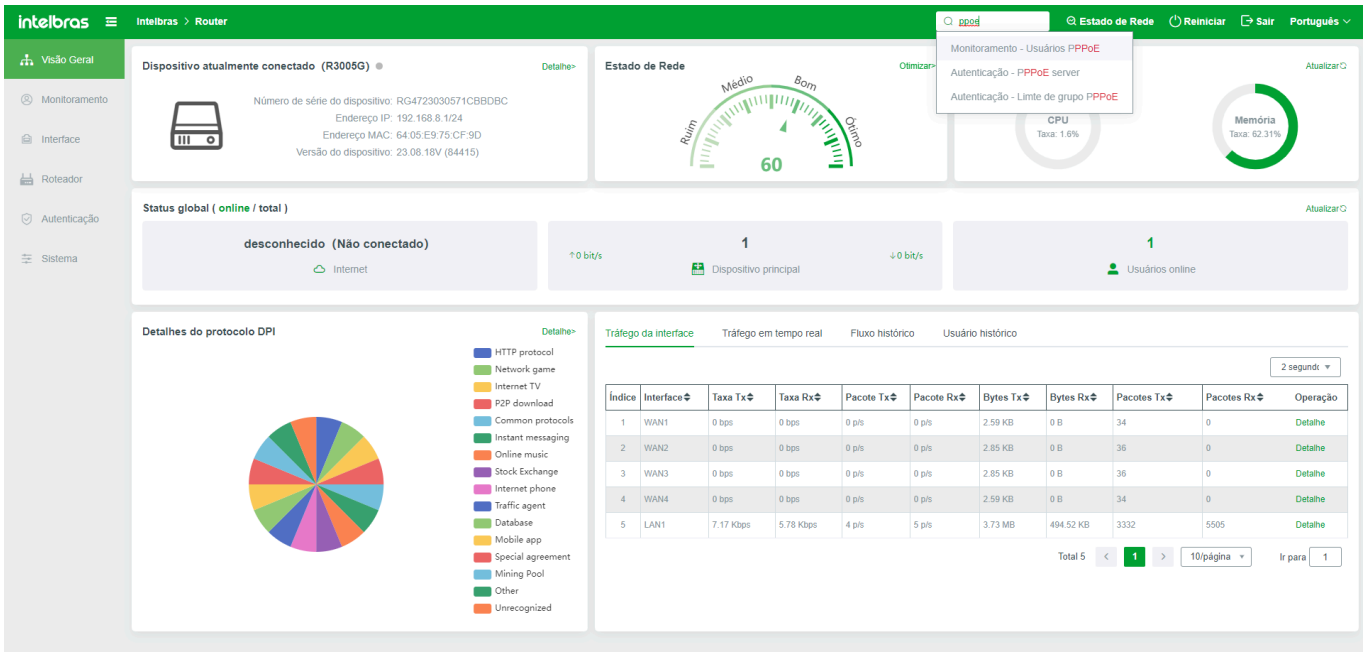


Configuração de Acesso Rápido

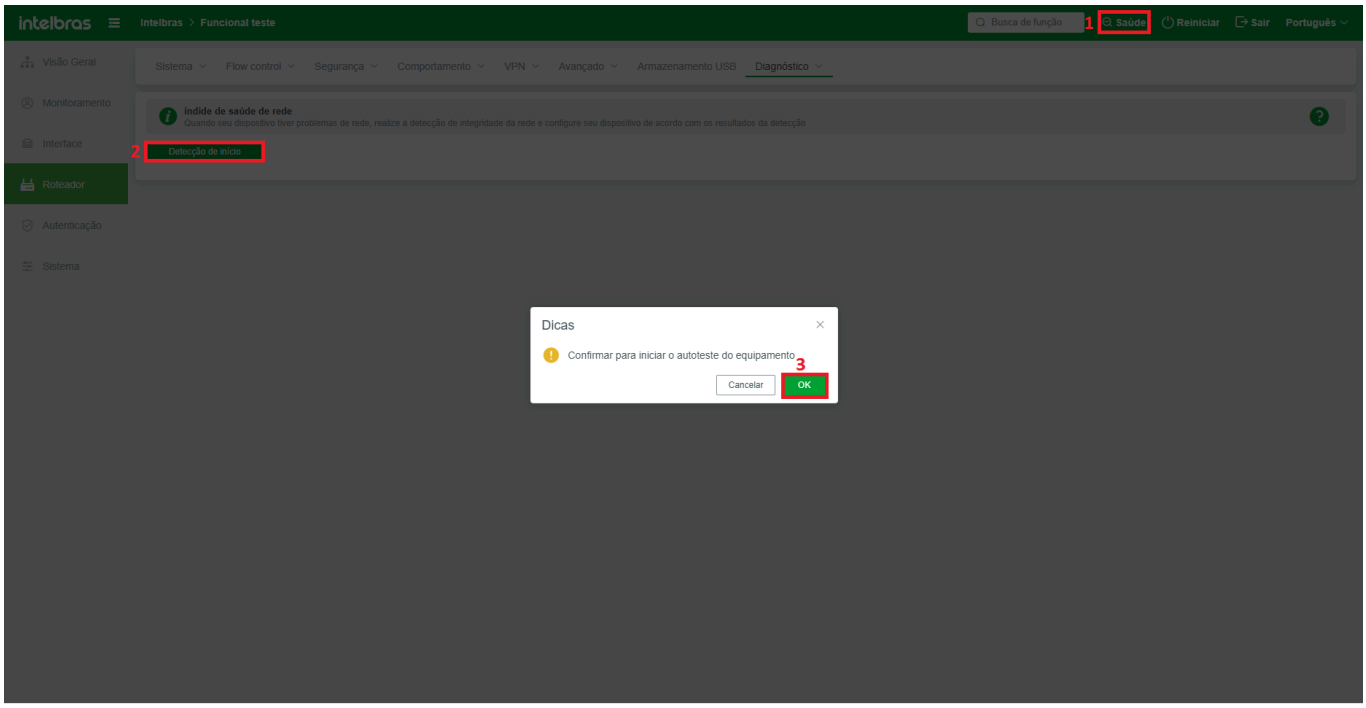
Informações do dispositivo atualmente conectado: Quando o ponteiro do mouse é direcionado para a marca principal (ou secundária) ou marca "i" no topo da página, são exibidas as informações de versão, modelo, SN e endereço do gateway do dispositivo atual.



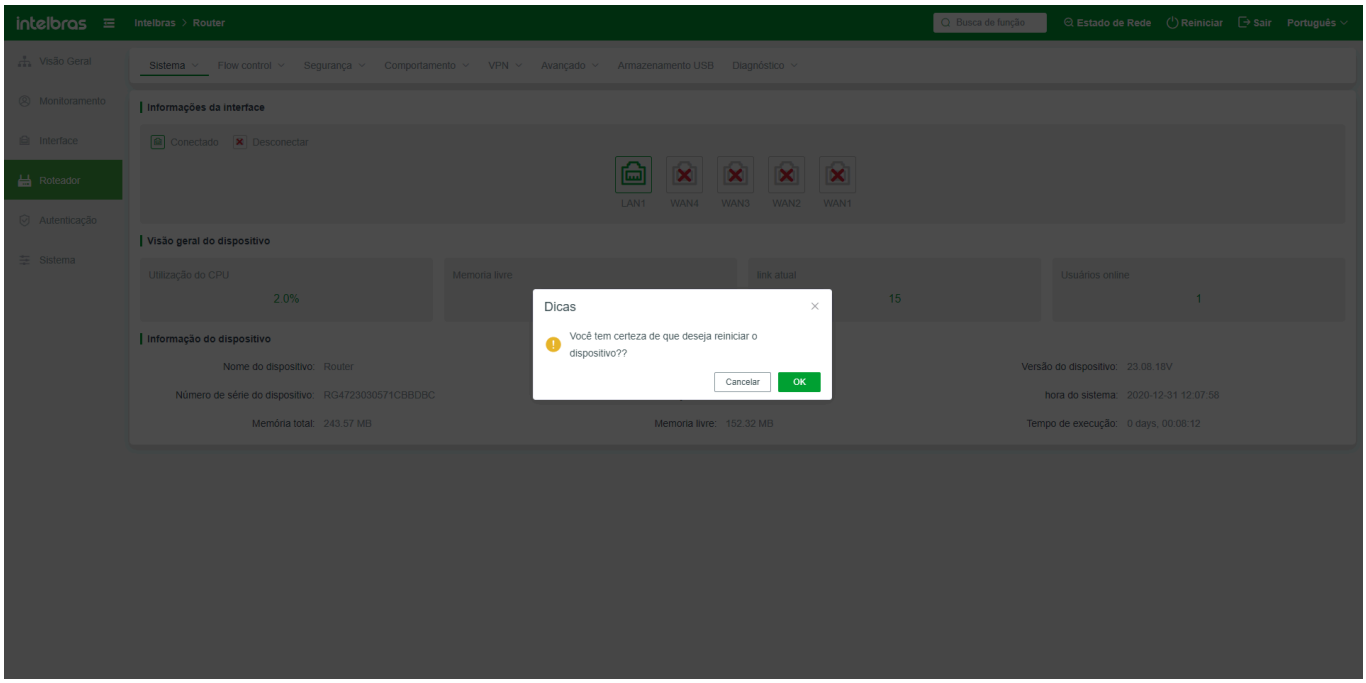
Busca de Função: Se você estiver usando o sistema pela primeira vez e não puder determinar o menu de uma função, pode usar a função de pesquisa de função para inserir uma palavra-chave, por exemplo, PPOE. O sistema exibe automaticamente todas as funções PPOE do sistema atual.



Índice de Saúde: Clique para alternar para a página de verificação da saúde do ambiente de rede do dispositivo atual. As condições de verificação são definidas por padrão, e os resultados da verificação são exibidos na página. Ao retornar à página de visão geral do gerenciamento, o sistema atribui automaticamente uma pontuação ao índice de saúde da rede com base no resultado da detecção. Uma pontuação mais alta indica um índice de saúde de rede melhor.



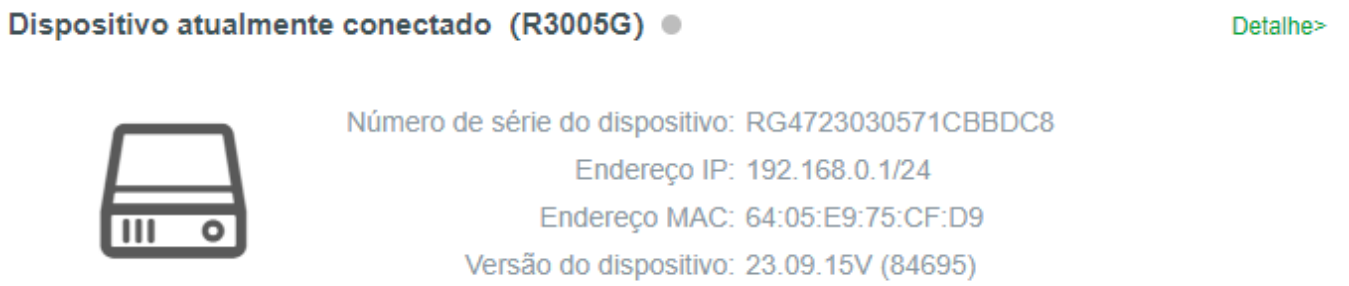
Reiniciar: Clique em Confirmar para reiniciar o dispositivo. O dispositivo reinicia automaticamente com sucesso.

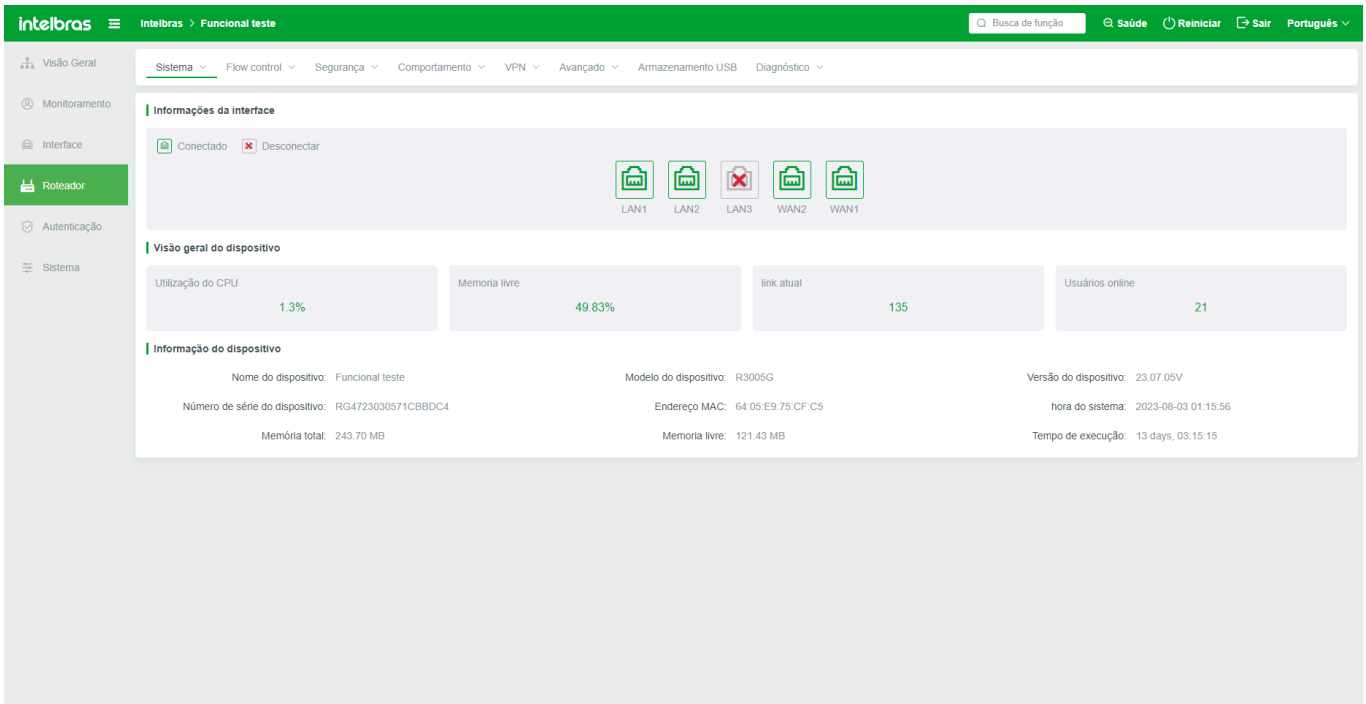


Sair: Clique para fazer logout da página de gerenciamento do sistema.

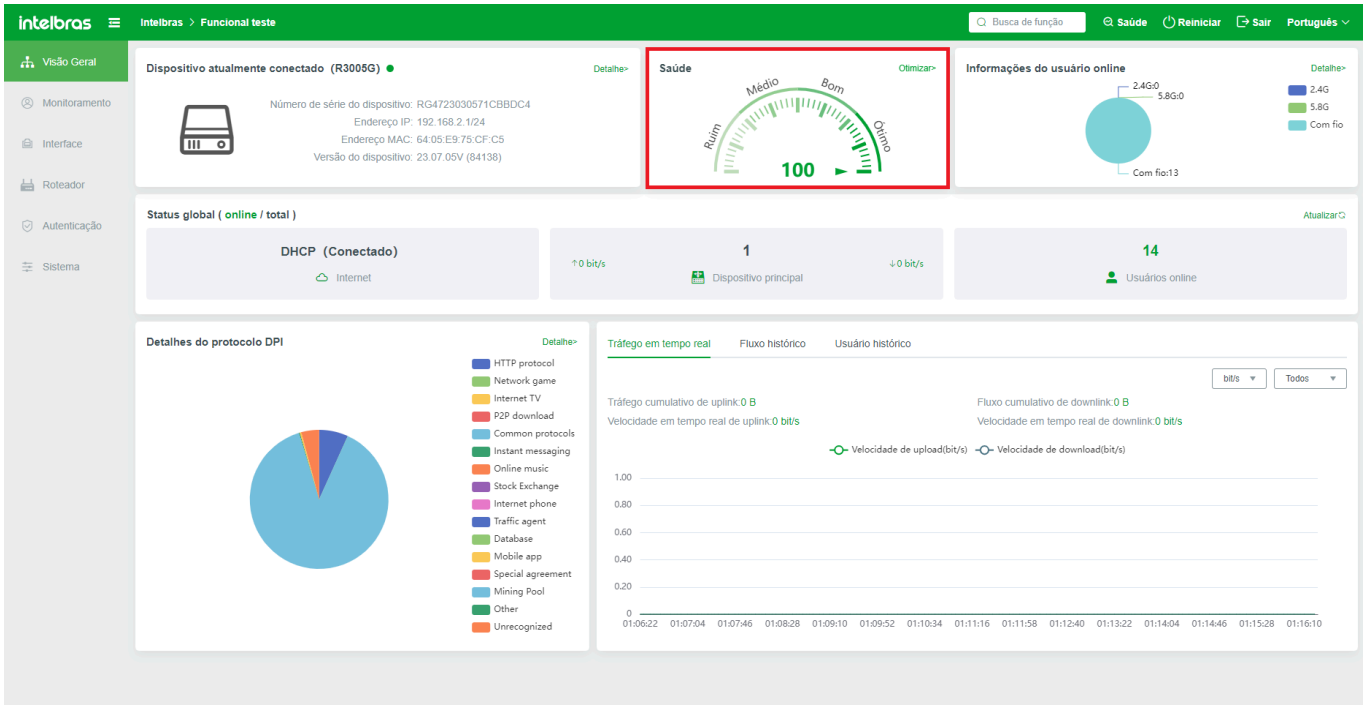
Estatísticas de Dados

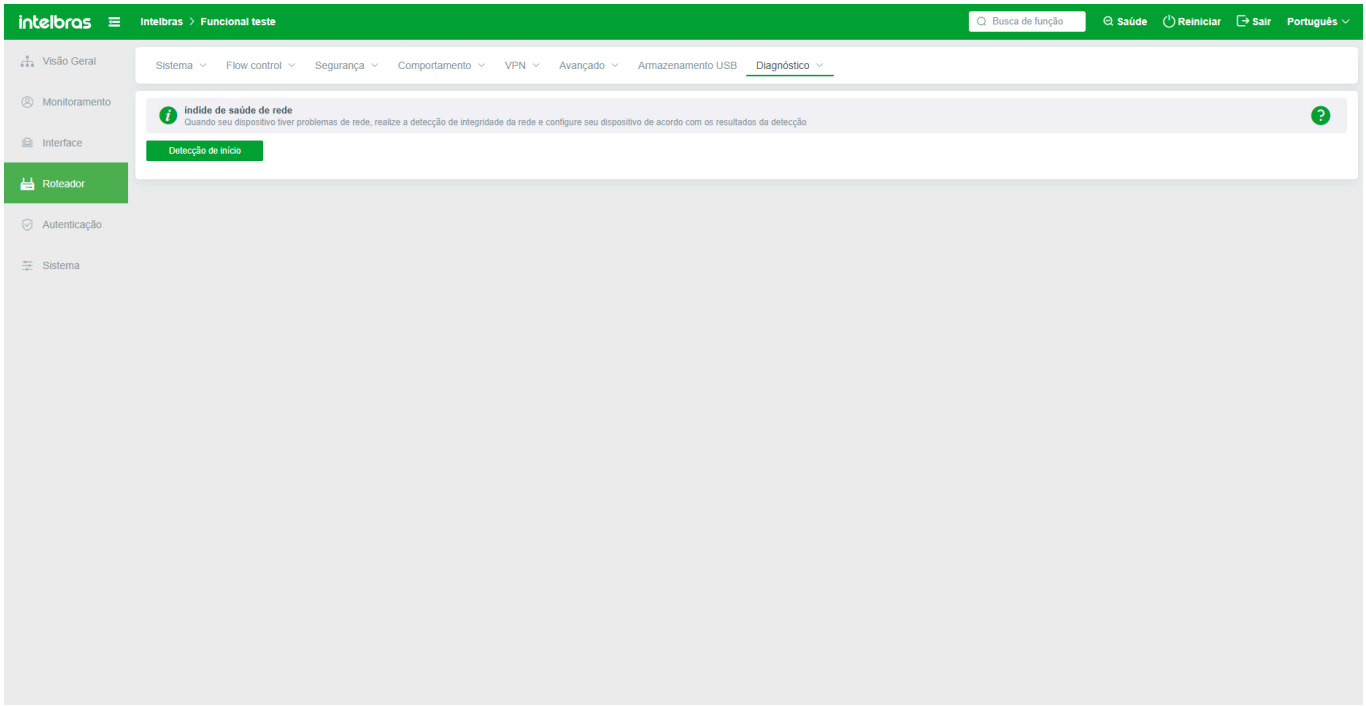
Dispositivo atualmente conectado: Exibe as informações básicas sobre o dispositivo de login atual, incluindo número de série, endereço IP de gerenciamento, endereço MAC e número da versão. Após clicar no botão "Detalhes", a página será redirecionada para a página de status do sistema do dispositivo, onde informações adicionais sobre o dispositivo de login atual são exibidas.





Índice de Saúde: indica o índice de saúde da rede do dispositivo atual. Um índice mais alto indica um dispositivo mais saudável. Se você clicar no botão "Otimizar", a página será redirecionada para a página de detecção automática.

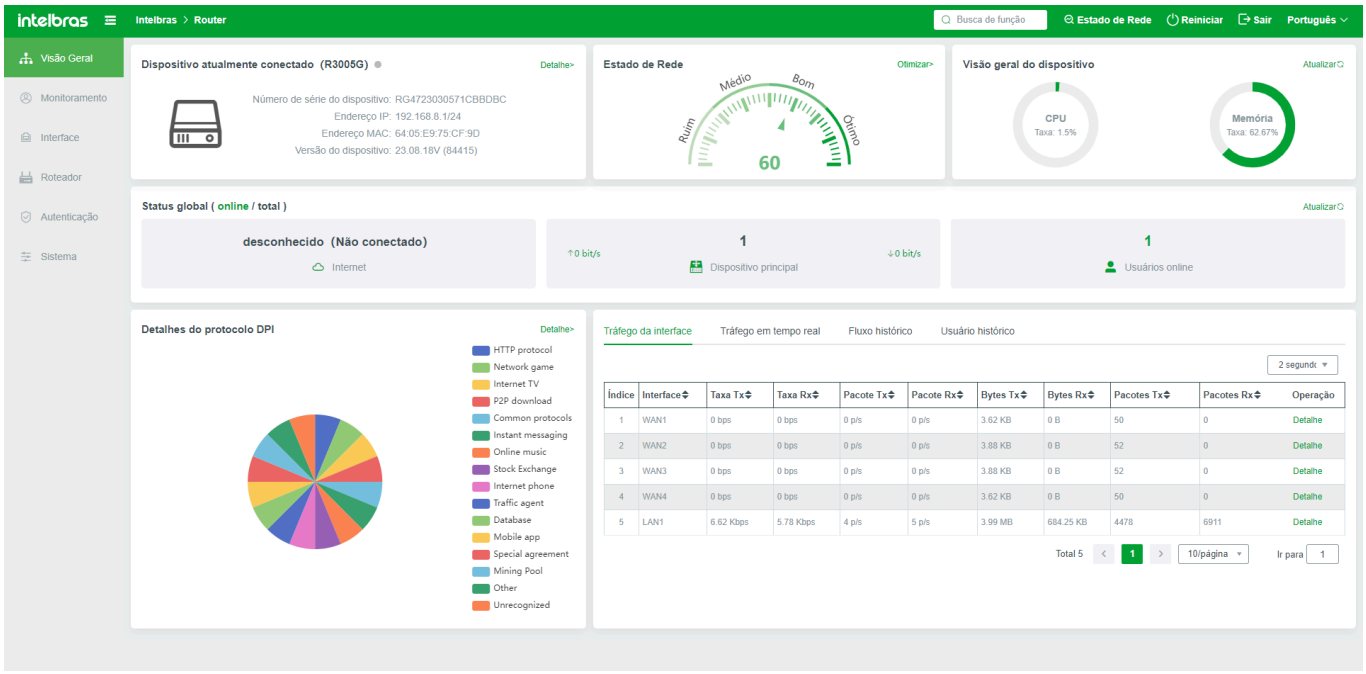




Status Geral da Rede

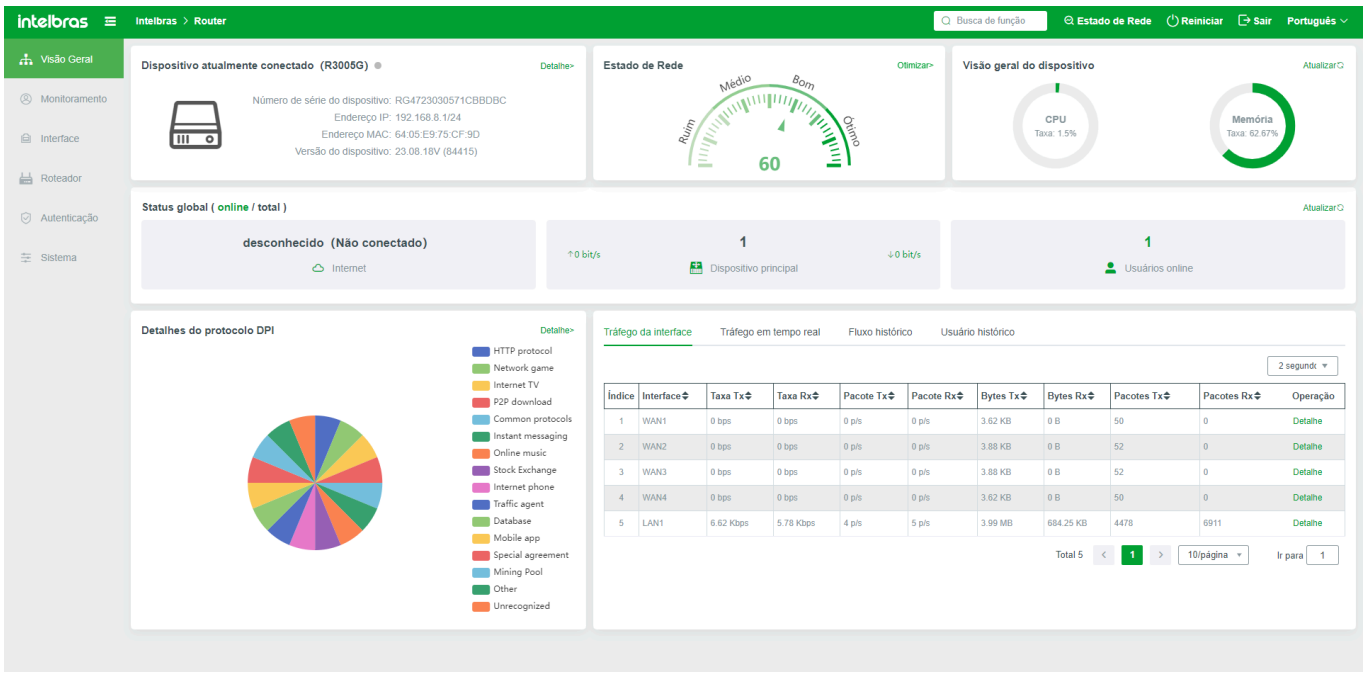
Número de dispositivos online/total:

O modo do dispositivo atual obtém informações da rede externa, número de dispositivos ativos e downlink de saída (em tempo real), e número de usuários online (incluindo usuários com fio e sem fio). Clique no botão "Atualizar" e as estatísticas de status em toda a rede serão atualizadas.

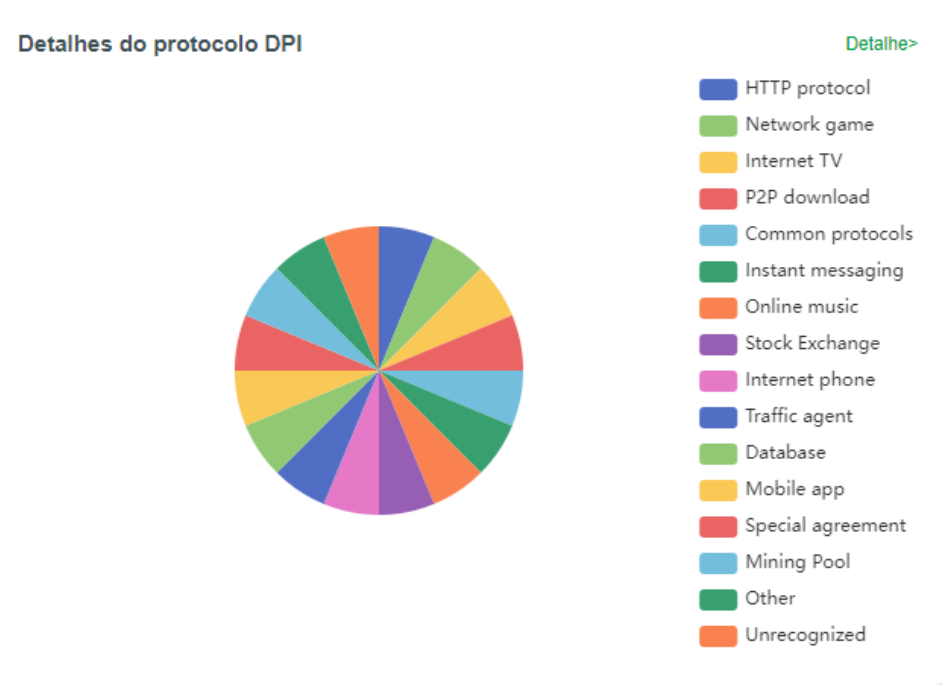


DPI

Coleta estatísticas sobre a porcentagem de uso de protocolos DPI pelos usuários terminais. Os protocolos DPI são exibidos por categorias e níveis. Diferentes cores indicam diferentes protocolos. Se você clicar no cartão de cor à direita do protocolo, o protocolo correspondente não será exibido no gráfico de pizza. Se precisar retomar a exibição, clique novamente no cartão de cor.



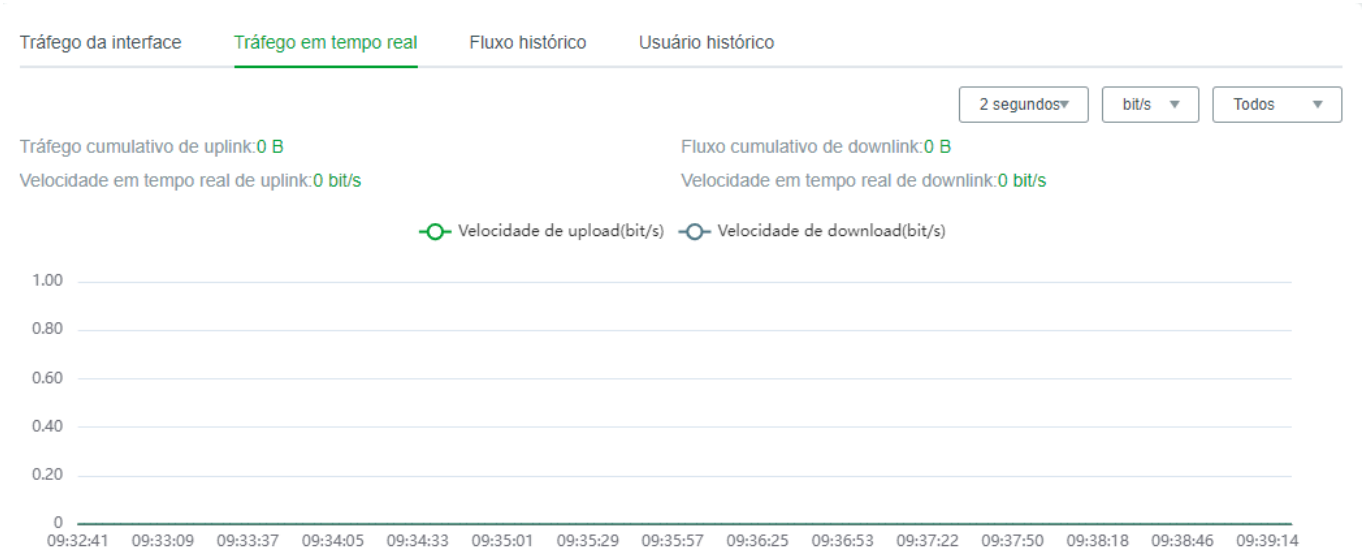
O gráfico de pizza mostra apenas o uso de tráfego do menu de nível 1 do protocolo; cada acordo também contém protocolos secundários ou terciários, como clicar no acordo comum, também inclui o HTTPS, terminal, escritório comum, etc. (terminal é usado ou usa ou acordo), se precisar retornar ao menu de nível superior, clique no nome "Acordo DPI" no final do acordo.



Estatísticas de Tráfego

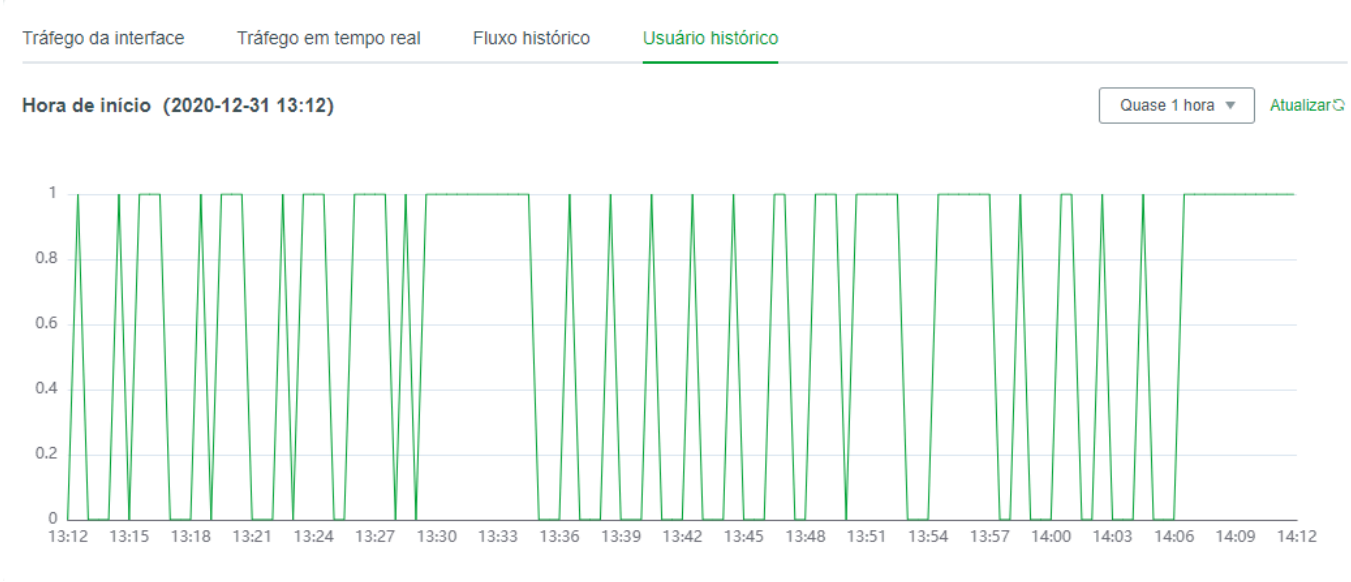
Exibe o uso histórico, em tempo real e de tráfego do usuário do dispositivo.

Tráfego em tempo real: O modo atualiza automaticamente todos os dados de uso de tráfego externo atual. O gráfico de linha abaixo também é atualizado em tempo real com base na situação real. A porta WAN ou a porta óptica;



Fluxo Histórico: Selecione um intervalo de tempo e uma interface WAN conforme necessário para consultar o uso de tráfego da interface WAN em um intervalo de tempo histórico.

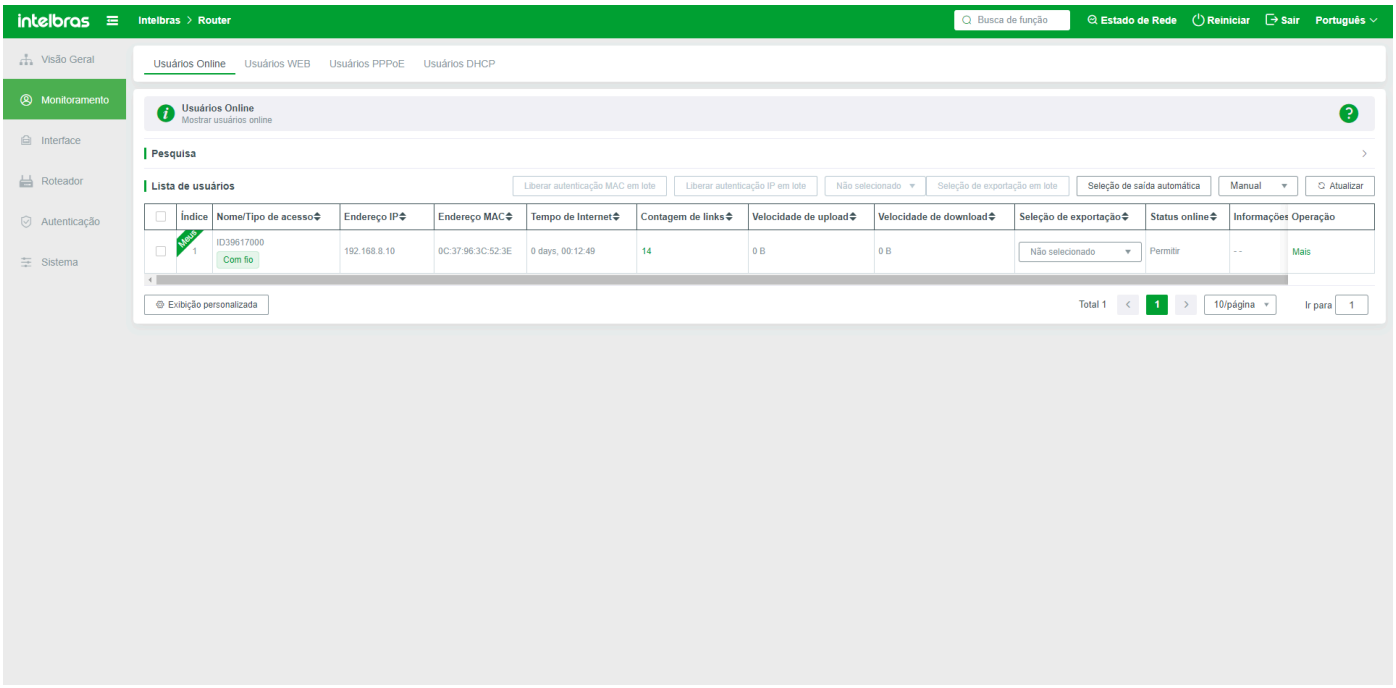
Usuários Históricos: Veja o número de usuários online em um período especificado.



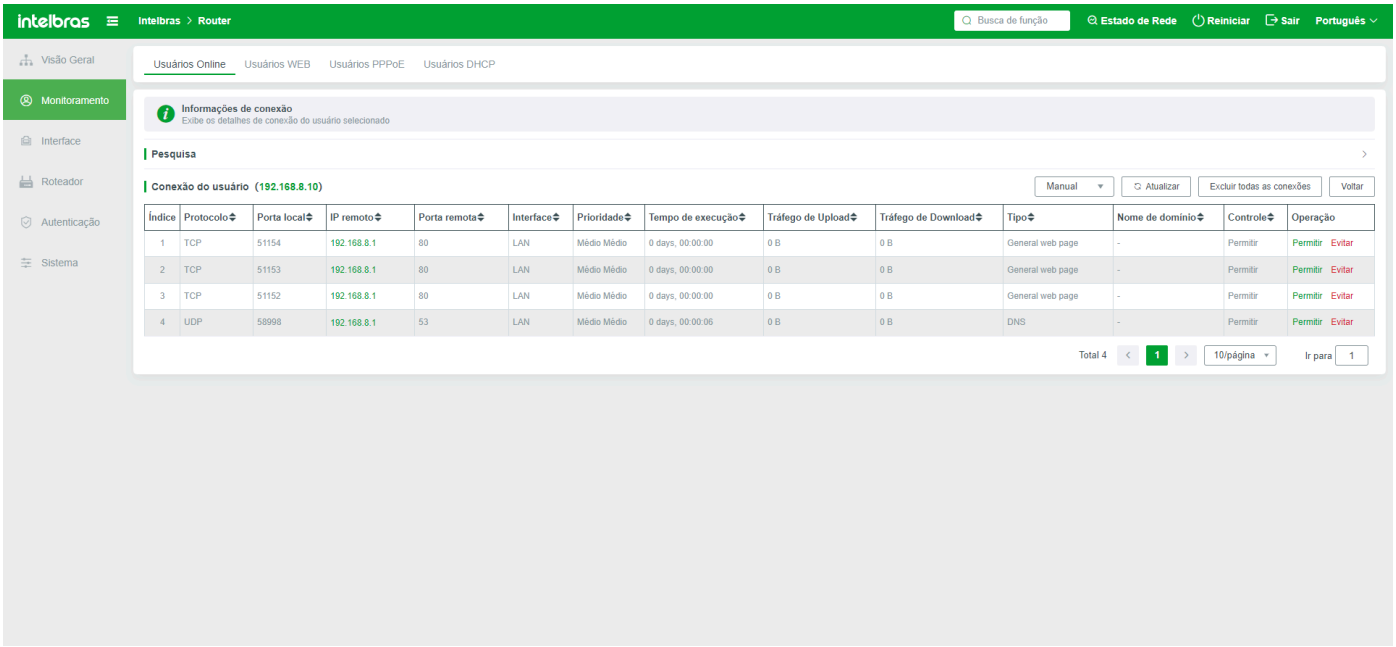
Monitoramento

Usuários Online

Exibe as conexões de rede dos usuários online atuais na Intranet. Os usuários podem ser pesquisados com base em condições. Na lista, é possível visualizar a rede ocupada por cada terminal, informações básicas do terminal e status de acesso à Internet. Operações Comuns podem ser realizadas no terminal, incluindo visualização do uso de tráfego do terminal, isenção de autenticação, vinculação ARP (única por padrão), detecção de ping e controle de acesso. Conforme mostrado na imagem:

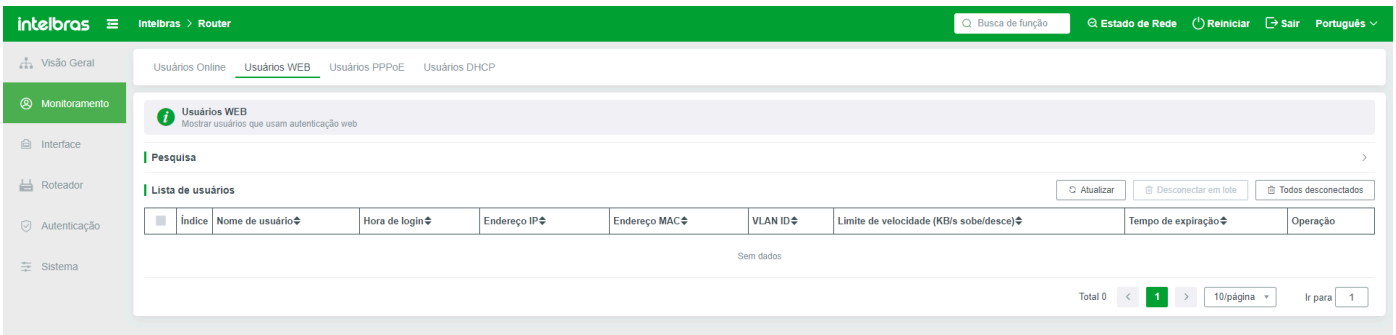


Clique em "Detalhes" embaixo de "Número de Conexão" na lista de terminais para visualizar o protocolo de acesso à rede do terminal. É possível excluir, permitir e bloquear detalhes da conexão.



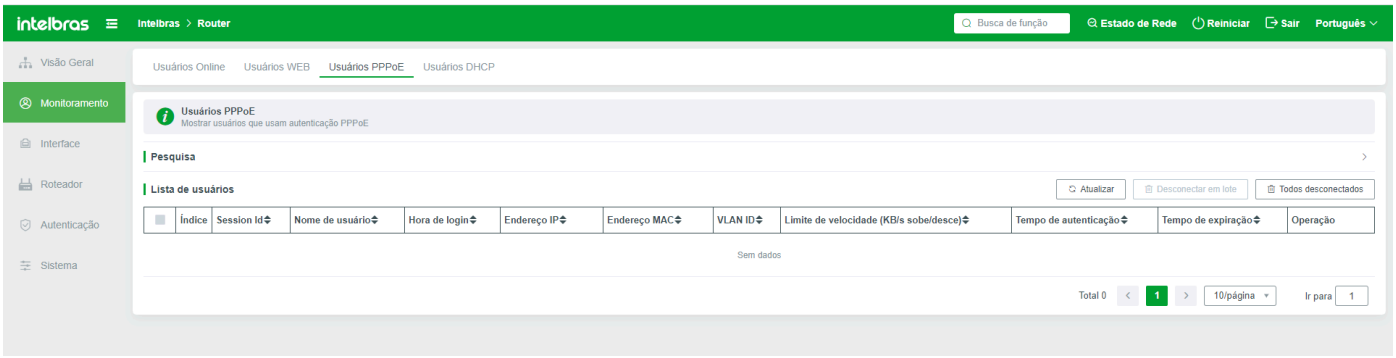
Usuários WEB

Exibe os usuários que passaram com sucesso pela autenticação WEB, incluindo usuários que passaram pela autenticação de contabilidade. Se você clicar em "Desconectar Todos" para o usuário de faturamento ou "Desconectar" para o terminal na lista, o sistema falha.



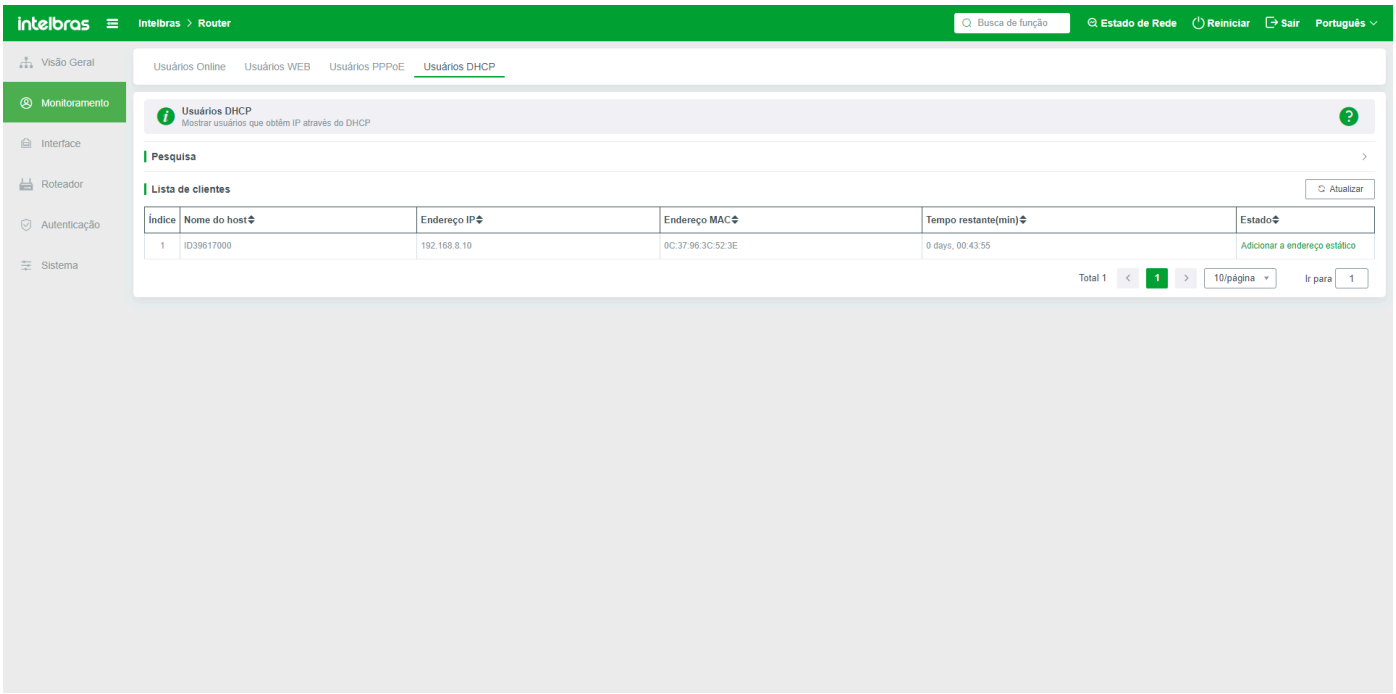
Usuários PPPOE

Exibe os usuários conectados com sucesso por meio da discagem PPPOE.



Usuários DHCP

As informações sobre todos os usuários que obtêm automaticamente endereços IP do DHCP são exibidas. É possível adicionar um endereço estático à lista de usuários DHCP. Você pode visualizar o resultado de vinculação na Lista ARP.



Interface

Configurações da WAN

Configure as funções LAN, WAN, PBR e IPV6 sob este menu.

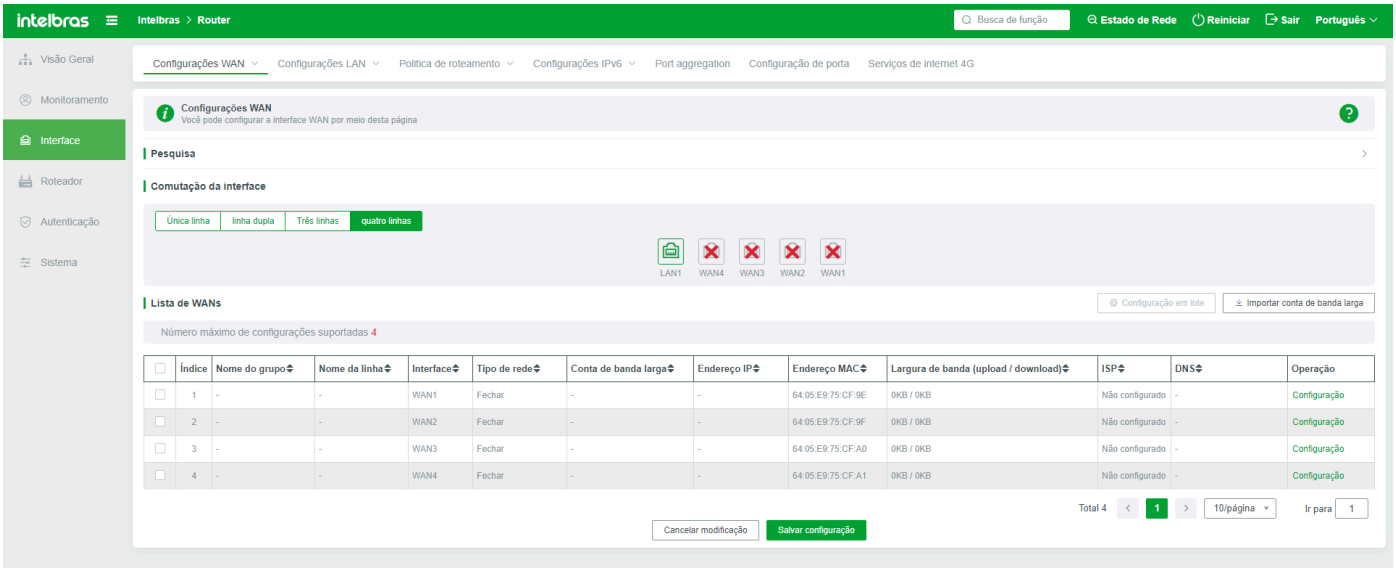
> Aviso Importante: Para assegurar o funcionamento adequado do R3005G, é essencial conectar o dispositivo à Internet assim que possível após a configuração inicial. Esta conexão permite a sincronização automática do relógio interno do produto com os serviços públicos de NTP, garantindo a precisão do horário e a eficiência operacional do produto.

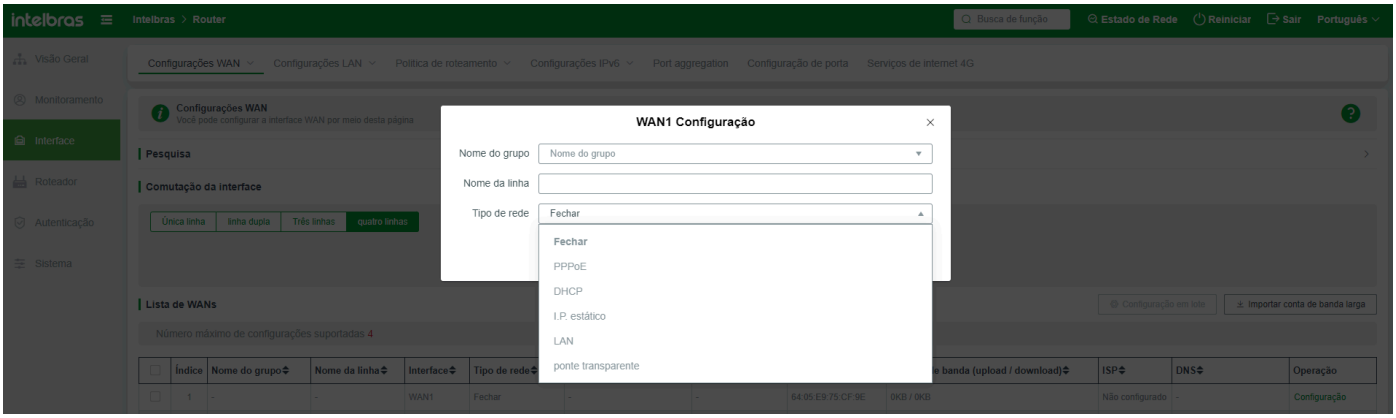
Configurações da WAN

Defina os parâmetros da porta WAN e selecione o tipo de linha do dispositivo. Configure a interface WAN conforme necessário; caso contrário, a rede pode ser afetada.

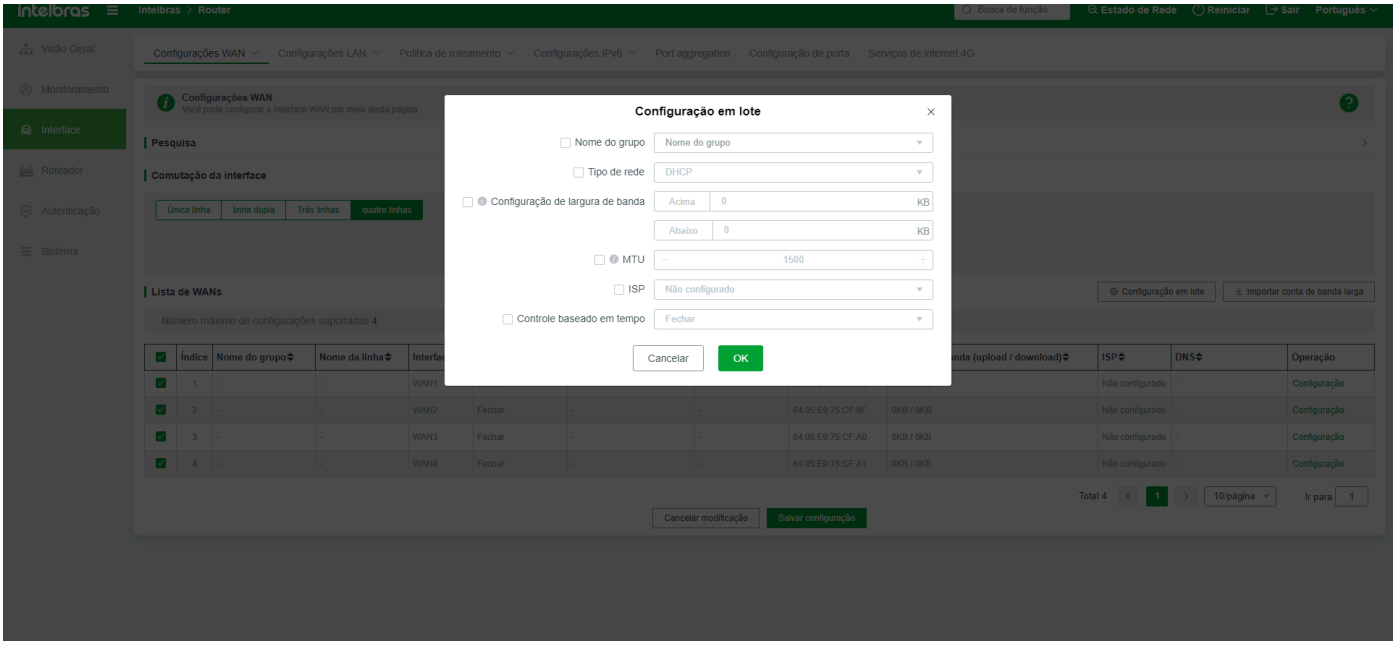
Neste menu, você pode selecionar o número de portas WAN conforme necessário. O número de portas WAN é exibido com base no hardware do dispositivo. Se você precisar configurar mais portas WAN, mova-se para o menu de Extensão WAN para visualizar o método de configuração. O número máximo de interfaces WAN a serem configuradas é afetado pelo número de interfaces WAN autorizadas. Portanto, se precisar configurar mais interfaces WAN, obtenha autorização para expandir as interfaces WAN primeiro.

Por exemplo, o dispositivo R3005G possui cinco portas RJ45, uma porta LAN por padrão e as quatro portas restantes são portas WAN. Se forem necessárias duas portas WAN, clique em "Dual Line" para enviar a configuração. As duas portas RJ45 à direita do dispositivo são portas WAN, e as demais são portas LAN.





Configuração em lote: Selecione as portas WAN na lista para configurar os parâmetros da porta WAN em lotes.



Importar contas de banda larga: Quando a discagem PPPOE é usada para conectar-se através de uma determinada porta WAN, você pode importar contas de banda larga em lotes para adicionar rapidamente senhas. Como mostrado na imagem abaixo: (use vírgulas no estado em inglês)

WAN1, 1111, 1111,

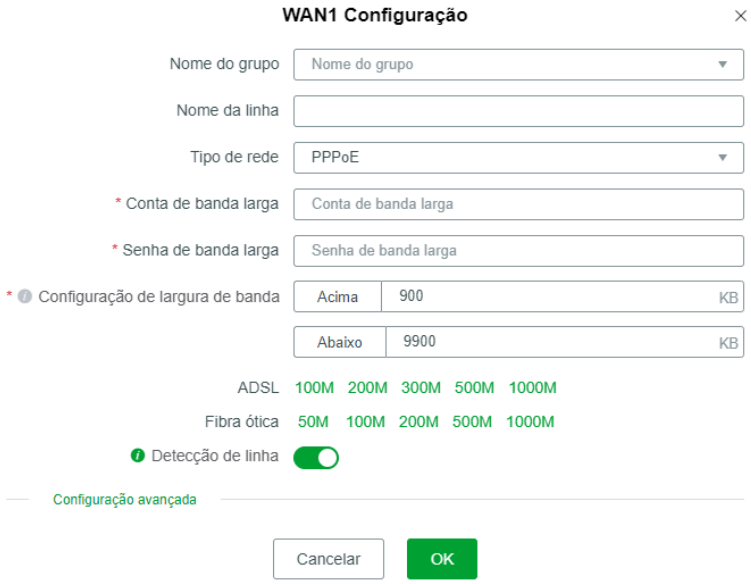
WAN2, 2222, 2222,

WAN3, 3333, 3333,

...

Após concluir a configuração, clique em "OK" e "Salvar configuração

Configuração: Este parâmetro pode ser configurado para uma interface WAN



1. Desligar

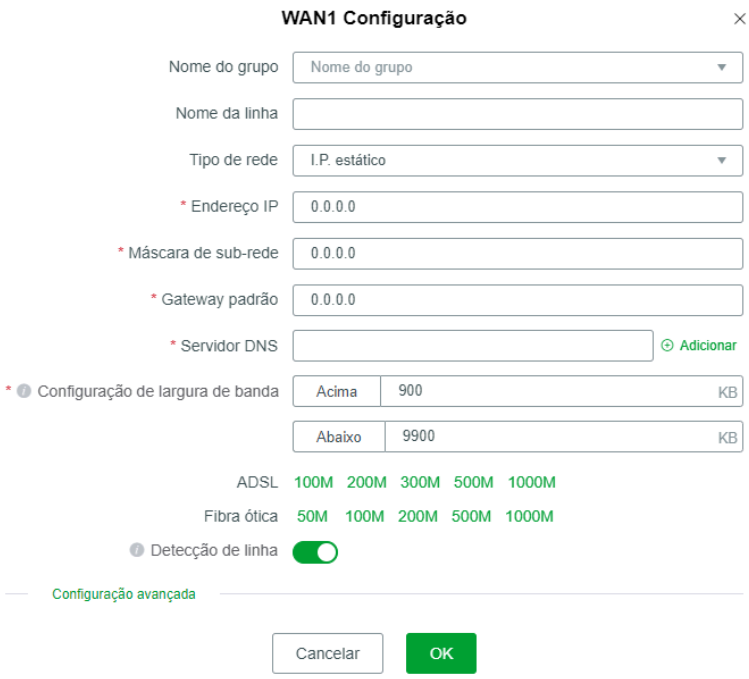
Indica que o status de conexão da interface WAN está desligado. A interface WAN no estado desligado não pode se conectar à Internet.

2.**Acesso à Internet de banda larga**

Indica que a interface usa o modo de discagem. Você precisa inserir a operadora ou conta de largura de banda disponível e salvar a submissão antes de se conectar à interface.

A conta de largura de banda e a senha são obrigatórias. O valor padrão da largura de banda é 0, indicando que o tráfego na rede externa não é restrito.

A porta WAN obtém automaticamente um endereço IP da rede externa. O endereço IP atribuído automaticamente pelo dispositivo de camada superior serve como o endereço IP de rede do dispositivo local. Quando o dispositivo de camada superior reinicia ou reatribui um segmento de endereços IP, o dispositivo local obtém automaticamente um novo endereço IP.



4. IP Estático

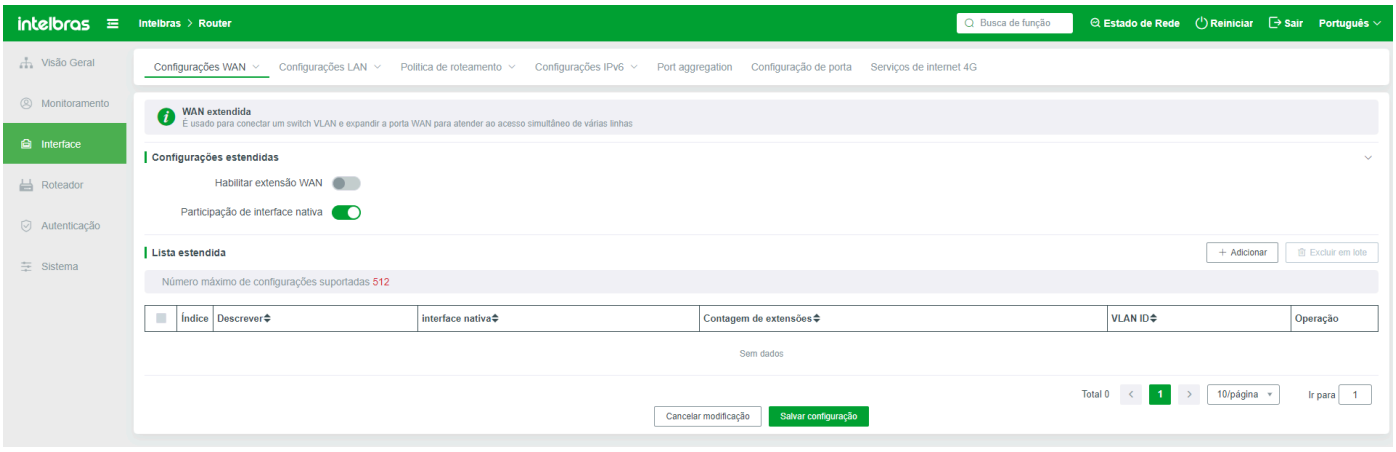
A porta WAN usa um endereço IP estático. Independentemente de a segmentação de rede do dispositivo de camada superior mudar ou o dispositivo reiniciar, a porta WAN no dispositivo local usa o endereço IP estático configurado e não muda automaticamente.

Endereço IP, máscara de sub-rede, endereço do gateway e servidor DNS são obrigatórios. Se você não conhece o endereço do servidor DNS, insira o endereço do gateway. Se houver vários endereços de servidor DNS, clique em + para adicioná-los.

Para Configurações de banda larga, são os valores de largura de banda de saída e entrada da WAN. Se você não conhece a conversão dos valores de largura de banda, pode usar os valores de referência abaixo para inseri-los automaticamente. Se a largura de banda não estiver dentro da faixa de referência, configure manualmente a largura de banda de saída.

Referência de Largura de Banda: Indica o valor de referência de largura de banda para definir a largura de banda de saída da WAN. Se você selecionar algum valor de referência, o valor da largura de banda é inserido automaticamente.

Detectar linha: habilita o roteador a detectar se o status da linha de rede está normal em tempo real.



5. Configurações Avançadas

Configurações avançadas de parâmetros para a configuração de extranet.

Modo de operação: Modo de gateway padrão, NAT é implementado na interface. O modo de roteamento pode ser usado em alguns ambientes especiais (por exemplo, quando todas as máquinas da intranet usam endereços IP públicos).

MTU: indica a unidade máxima de transmissão para pacotes. A Intervalo de endereços IP dinâmicos e estáticos é de 576 a 1500, e a faixa de PPPoE é de 576 a 1492.

Endereço MAC: Endereços MAC aleatórios ou clonados com base na condição da rede. Geralmente, o endereço MAC padrão não precisa ser ajustado.

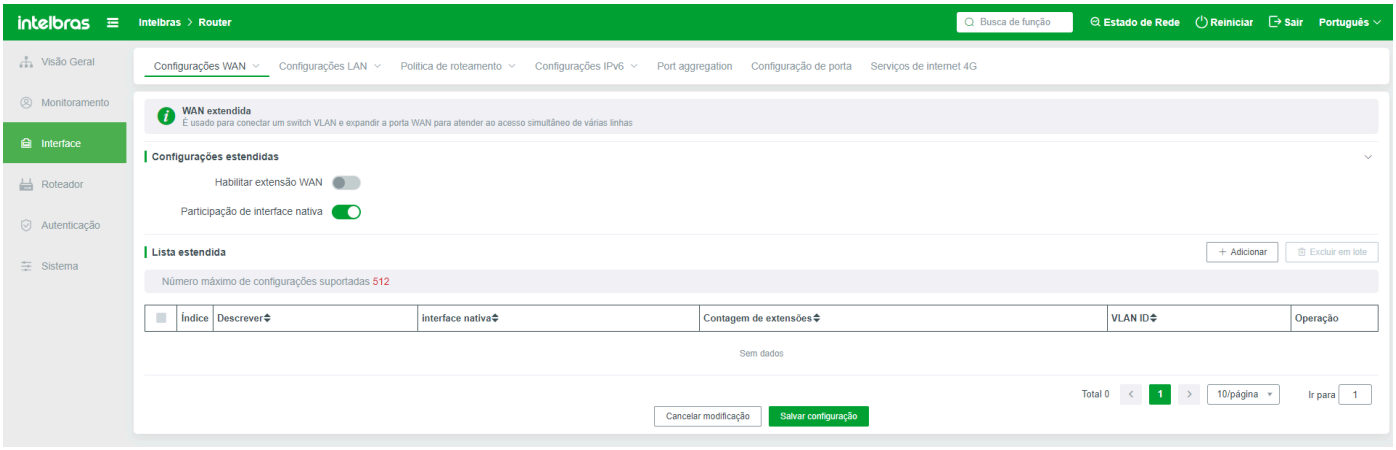
Prioridade de resolução DNS: Para o acesso à porta WAN, o valor determina a prioridade de saída da resolução DNS.

Operadora: Operadora de uma rede de longa distância, como Netcom ou Telecom. Se "Não" for selecionado, a linha deve ser usada com a função de roteamento baseado em políticas. Nenhuma operadora é necessária para acesso de porta WAN única.

Participar do Load balancing: Especifica se participará do Load balancing. Após a ativação dessa função, o sistema participa do Load balancing com base no modo de Load balancing. Desativado não participa na carga padrão.

WAN Extendida

Para usar a função de WAN Extendida, você deve determinar o número de portas WAN suportadas pela autorização atual. A porta WAN expandida aqui tem o mesmo efeito que a porta WAN no hardware.



Status da WAN Extendida: Para expandir a WAN, primeiro ative o interruptor de status. Se este interruptor estiver desativado, a função de WAN Extendida será desativada. Se a regra de WAN Extendida estiver configurada, a regra se tornará inválida quando a função estiver desativada.

Participação na Extensão da Interface Nativa: Especifica se deseja habilitar interfaces nativas para participar da extensão. Interfaces nativas referem-se a interfaces físicas nativas em dispositivos de hardware. Você pode habilitar essa função quando os dispositivos de camada superior são configurados com VLANs ou quando a rede de camada precisa ser isolada. Após a interface nativa ser habilitada para participar da expansão, a interface WAN carrega uma marca e não pode ser usada como uma interface WAN regular. O cabo de rede da interface WAN pode ser conectado à interface de tronco (interface pública) do switch.

Regras para Adicionar

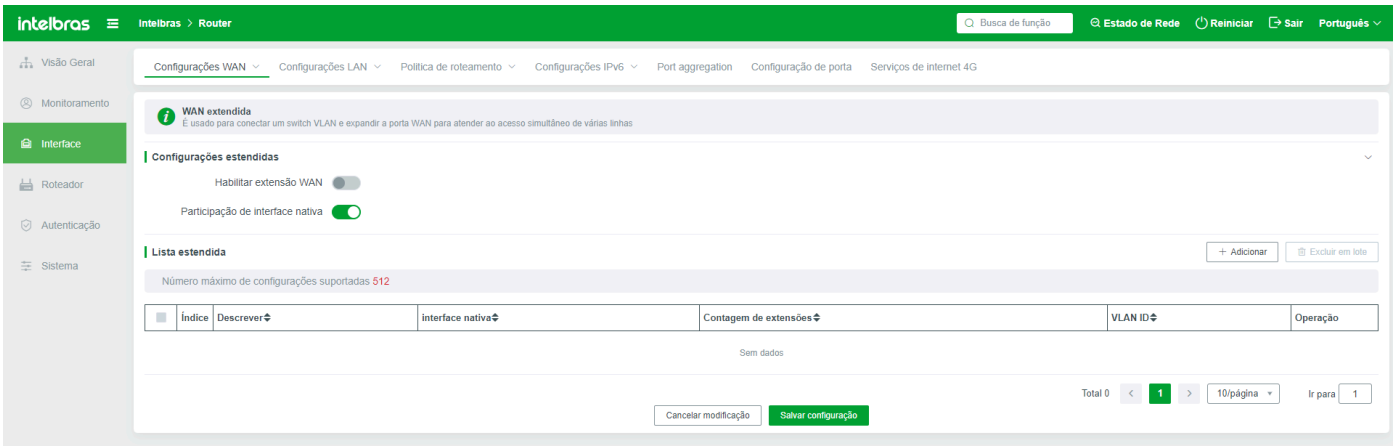
Descrição: Conteúdo de descrição personalizado, fácil de distinguir entre muitas regras;

Interface Nativa: Ou seja, em qual interface WAN estender. Para WAN1, selecione WAN1. Para WAN4, selecione WAN4 (esta porta é usada para conectar à porta pública no switch).

Número de Extensões: É o número de portas WAN a serem estendidas. As portas WAN a serem estendidas estão nas portas do switch sob este roteador. Ou seja, preencha o número necessário de portas para estender na interface do switch (o número da extensão e do equipamento real deve ser menor ou igual à soma do número de autorização da interface WAN). Em teoria, um switch de 24 portas pode estender até 22 portas WAN (uma para a porta pública, outra para compensar a extensão de WAN).

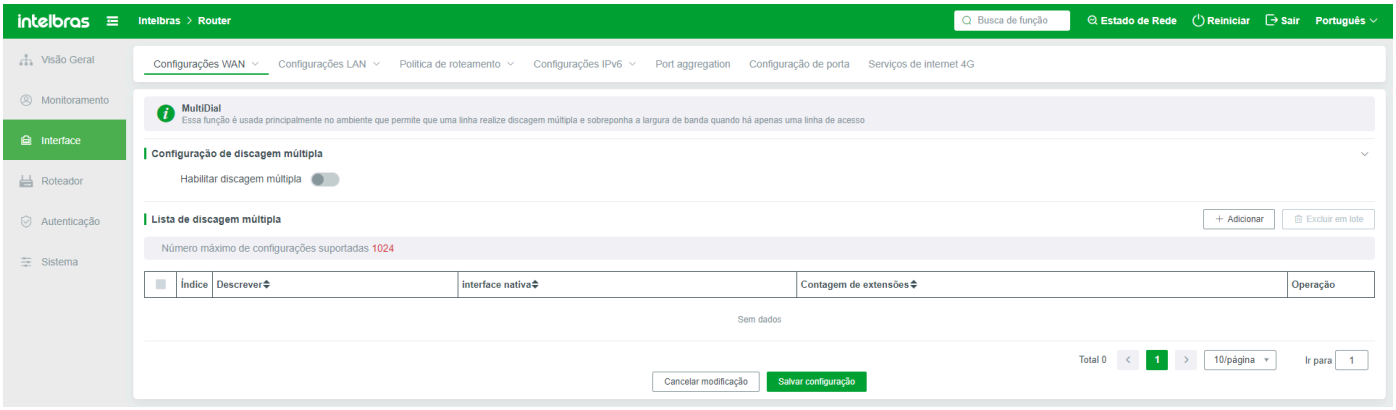
VLanID: Indica o VLanID da WAN configurada no switch. O valor varia de 1 a 4080.

Após as alterações nos switches acima e a configuração ser enviada, o dispositivo reinicia automaticamente para entrar em vigor. A figura a seguir mostra algumas portas WAN após 10 portas WAN serem expandidas.



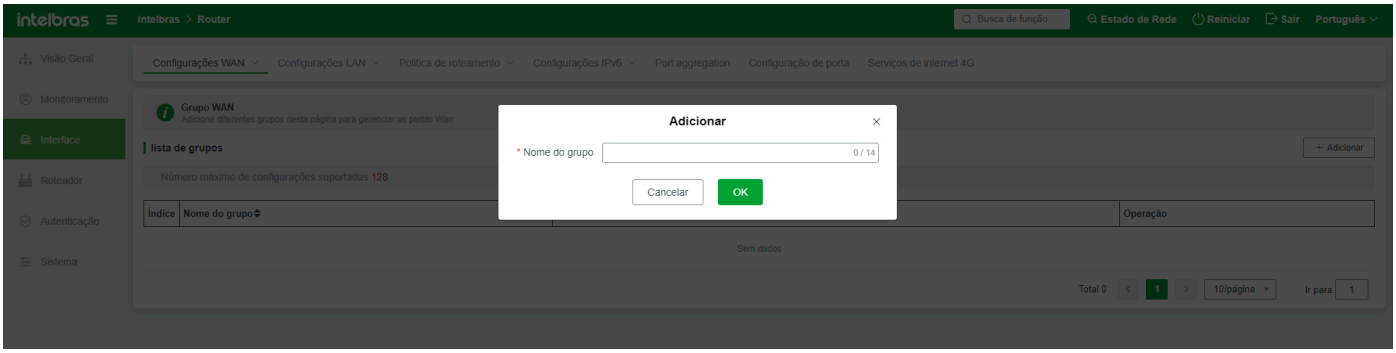
MultiDial

O MultiDial se aplica principalmente ao cenário em que há apenas uma linha de acesso ISP, mas várias contas de discagem são atribuídas ou várias discagens são permitidas em uma linha ISP e a largura de banda é sobreposta.



Grupo de WAN

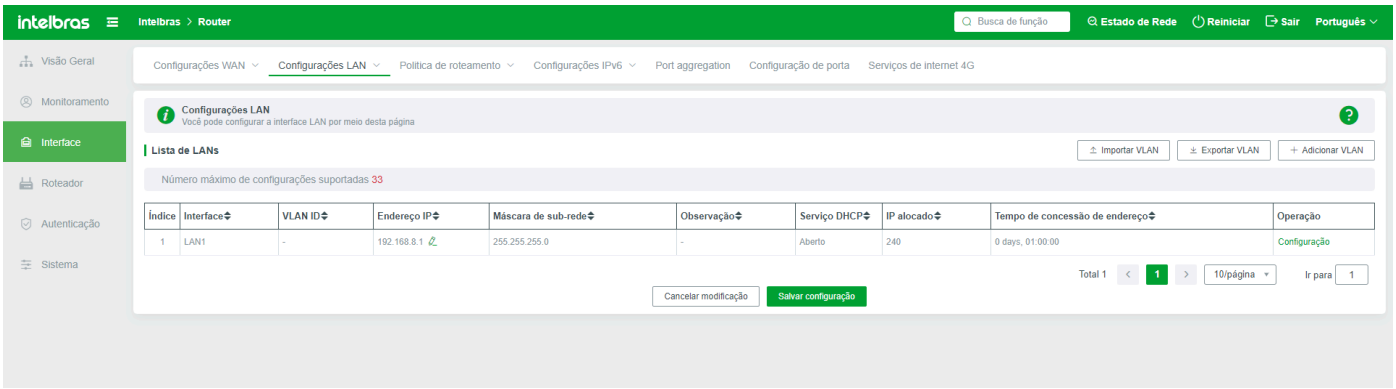
Adicione grupos diferentes nesta página para gerenciar as portas Wan.



Configurações de LAN

Configuração de LAN

Configure os parâmetros da interface LAN, adicione VLANs e exiba o número máximo de interfaces VLAN suportadas pelo dispositivo principal.

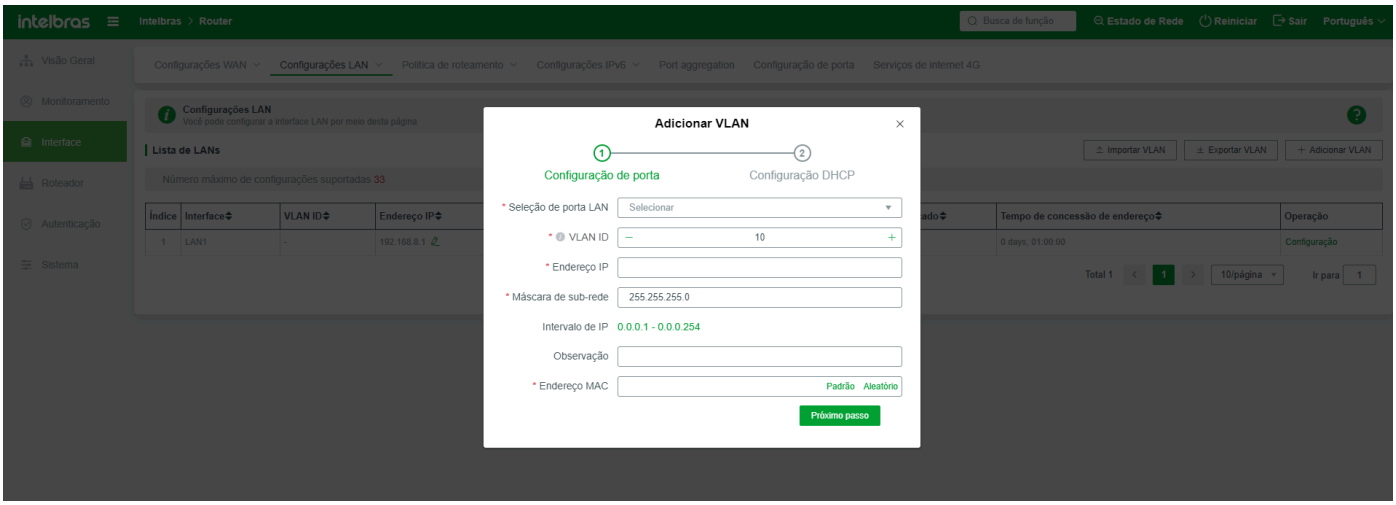


Configurar (porta LAN): Definir os parâmetros da porta LAN, como endereço IP, máscara de sub-rede, endereço MAC e se iniciar várias segmentações de sub-rede.

Endereço IP: Defina o endereço IP da porta de rede no roteador. O endereço IP é configurado como 192.168.1.1 antes da entrega e pode ser alterado conforme necessário. Se o endereço IP for alterado, o dispositivo reiniciará automaticamente após o envio do endereço IP.

Máscara de Sub-rede: Configure uma máscara apropriada com base no número de fitas na Intranet. A máscara de sub-rede padrão usada pelo roteador é 255.255.255.0, que pode ser alterada conforme necessário.

Endereço MAC: Altere o endereço MAC com base na condição da rede Intranet. Geralmente, o endereço MAC padrão é usado e não precisa ser ajustado.

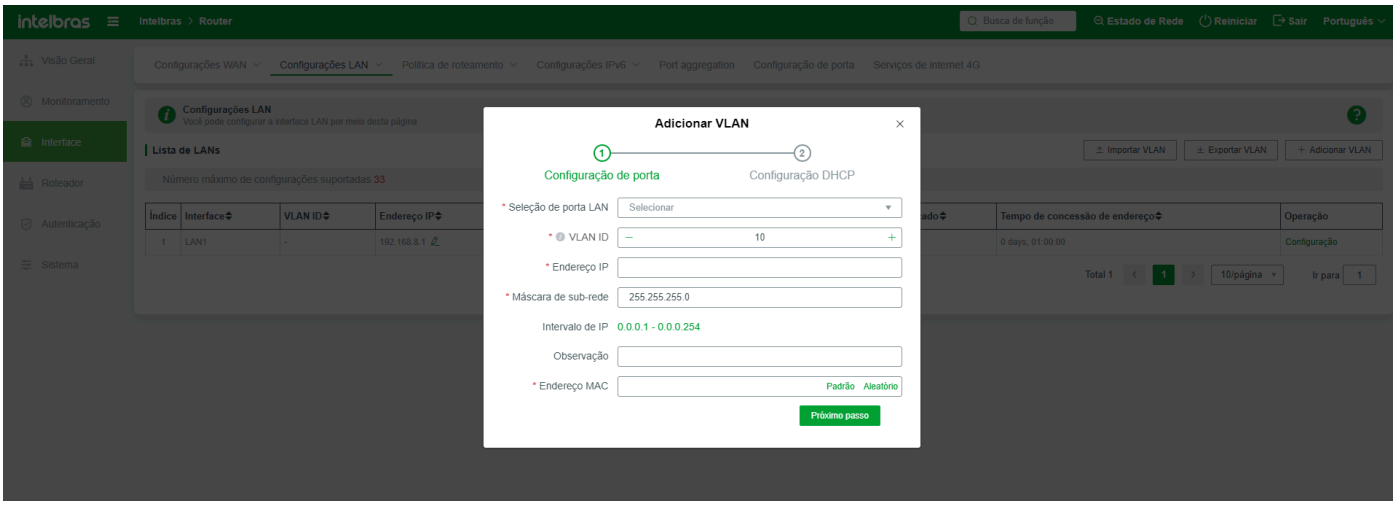


Adicionar uma VLAN: Múltiplas VLANs são suportadas na LAN. As VLANs estão associadas à configuração de uplink. Observe o seguinte durante a configuração:

1. Selecione a porta LAN correspondente para a VLAN.

2. O ID da VLAN é exclusivo e obrigatório.

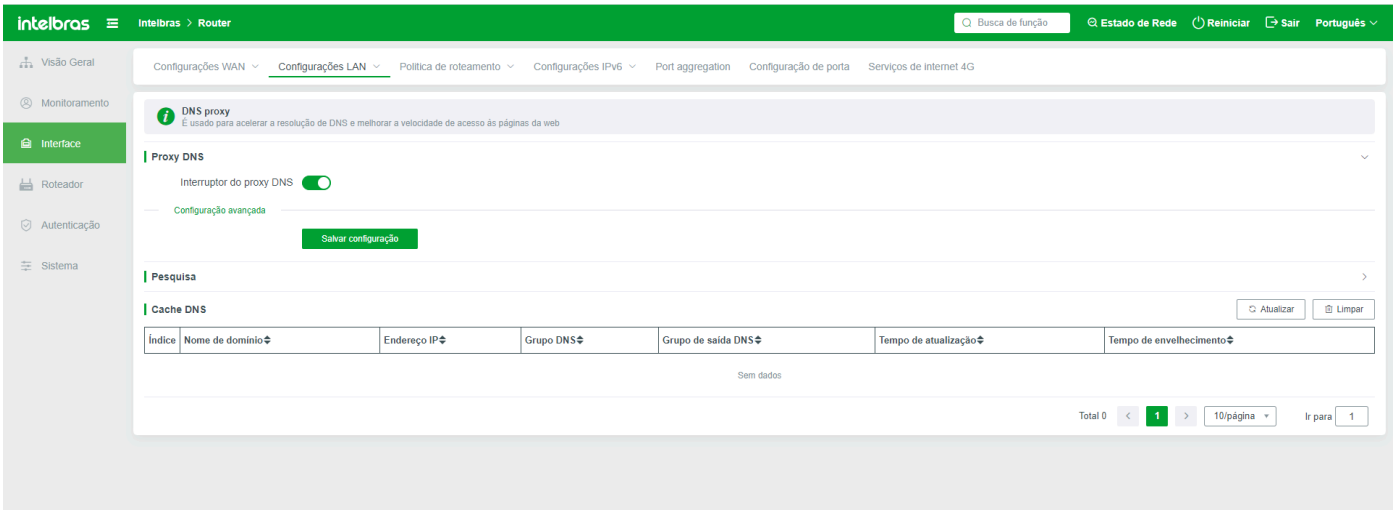
3. O endereço IP deve ser exclusivo e diferente de outros endereços na LAN.



Porta LAN (Endereço IP) Modificação: Na área de Endereço IP da lista de LAN, você pode alterar diretamente o endereço IP da porta LAN. Após a modificação, clique em OK e Salvar Configuração. Após a modificação, o dispositivo reiniciará automaticamente.

DNS Proxy

Ativar o DNS acelera a resolução DNS e melhora a velocidade de acesso às páginas da web.

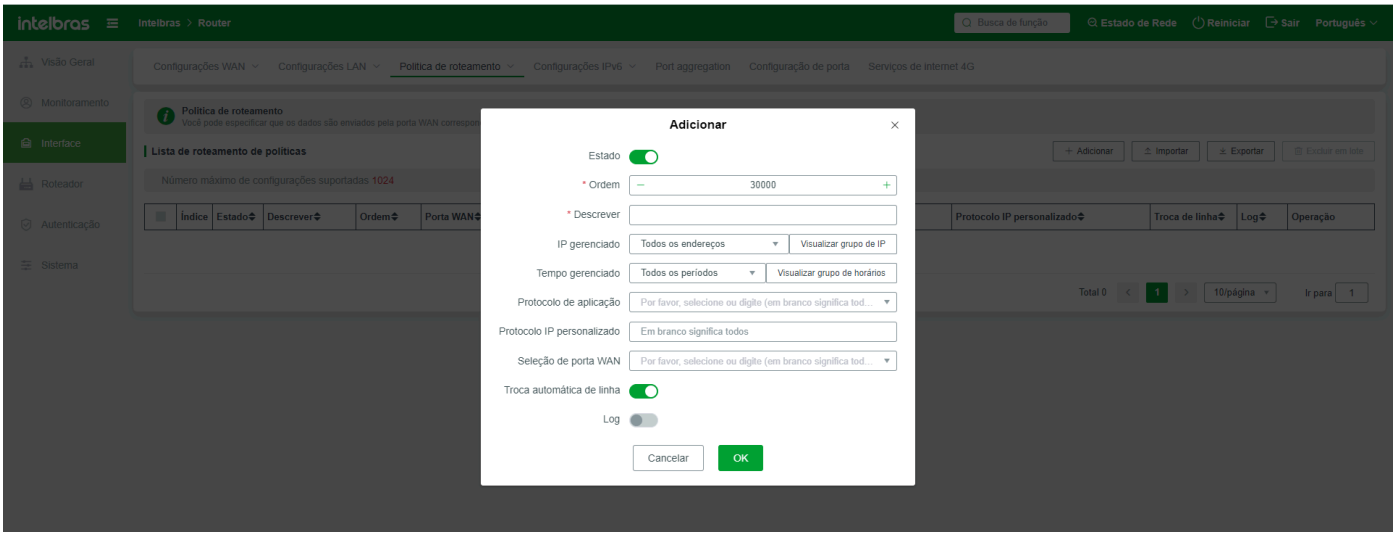


DNS Proxy: Se esta função estiver ativada, acelera a resolução DNS e melhora a velocidade de acesso às páginas da web. Quando ativado, a regra "Configurações Avançadas" também será exibida;

Política de Roteamento

Política de Roteamento

Você precisa configurar as regras de **Roteamento de Políticas** quando é necessário um protocolo específico, linha dedicada ou interface WAN especificada na rede.



Adicionar Regras

Status: Status da regra ligado ou desligado. Quando o status está desativado, a regra criada não entra em vigor.

Ordem de Execução: Indica a prioridade da execução da regra. Quanto maior o valor, maior a prioridade de execução. Se diferentes regras são executadas na mesma ordem, as regras entram em vigor ao mesmo tempo. Se as mesmas regras são criadas e executadas na mesma ordem, o dispositivo aleatoriamente aplica uma delas. Se a mesma regra for criada, mas executada em ordens diferentes, o dispositivo executa a regra com a ordem mais alta.

Endereço IP Gerenciado: Especifica o endereço IP ou segmento de IP para o qual a regra entra em vigor. A regra de política entra em vigor para o endereço IP (segmento) inserido. Todos os Endereços indicam todos os terminais na rede. Você também pode selecionar Personalizado para inserir um determinado endereço IP ou um determinado segmento de endereço IP.

Tempo Gerenciado: Indica o tempo de validade de uma regra PBR. A regra só entra em vigor dentro do tempo especificado. A regra é inválida fora do tempo especificado.

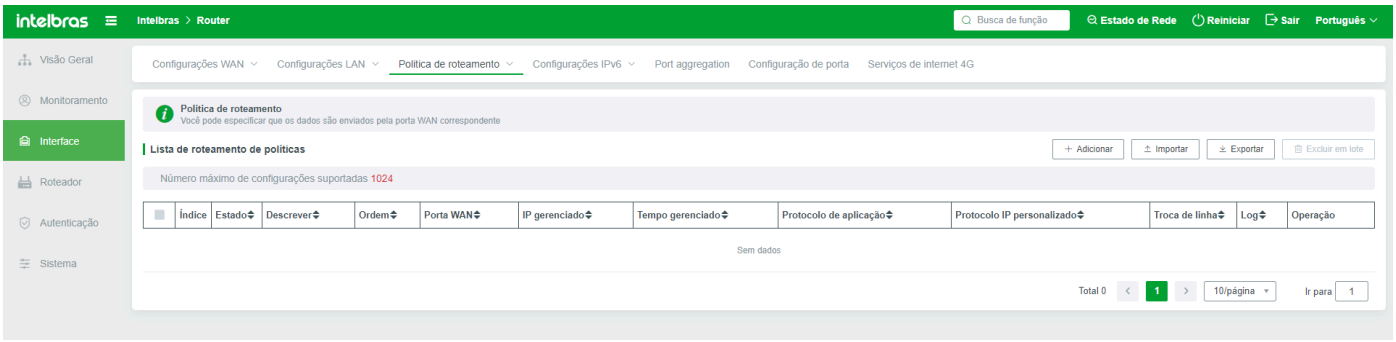
Protocolo de Aplicação: especifica o protocolo da regra, que geralmente é usado com a seleção da interface WAN.

Protocolo IP Personalizado: Se a opção de protocolo de aplicação não tiver um protocolo para definir ou tiver um endereço remoto especial, insira o endereço IP correspondente e a interface de porta. Essa função é usada da mesma forma que o Protocolo de Aplicação.

Seleção de Porta WAN: Seleciona uma ou mais portas de rede externas para as quais a regra entra em vigor. O número de portas WAN está relacionado ao número de portas WAN.

Troca Automática de Linha: se permite que as regras usem outras linhas quando a rede de uma porta WAN nas regras é desconectada ou ocorrem outras falhas.

Log: Ativa ou desativa o log de regras de roteamento lateral. Geralmente, você pode ativar esta função para facilitar a solução de problemas.

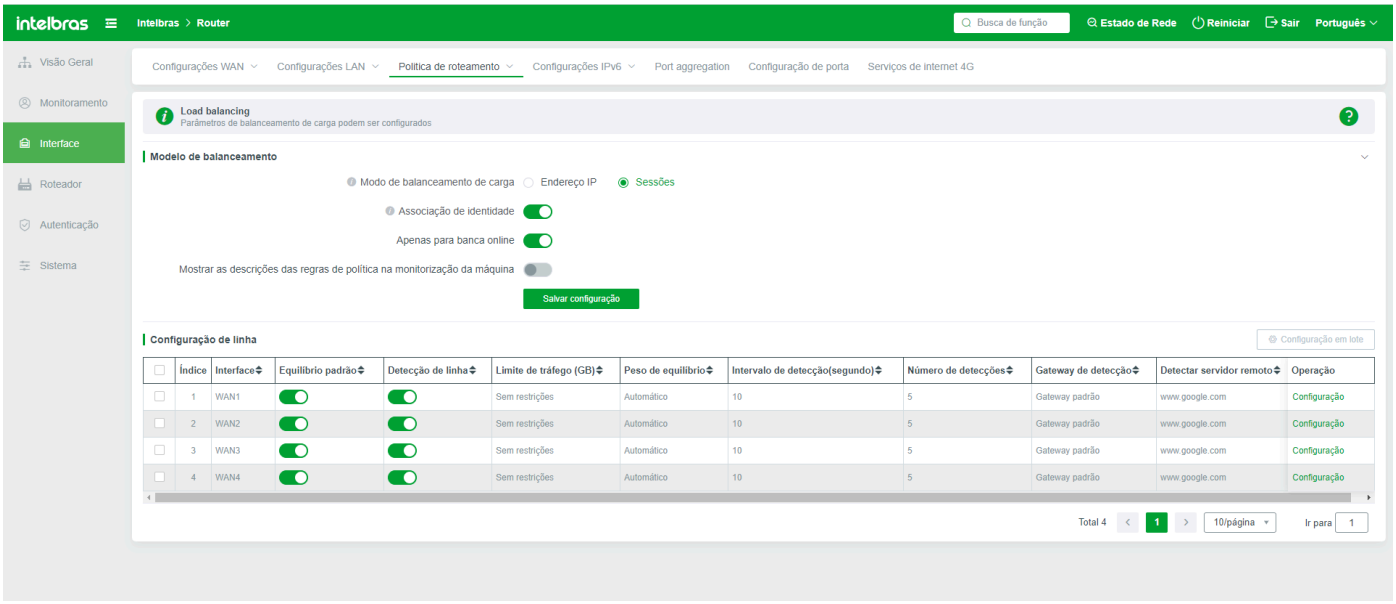


Importar: Importa regras PBR. O arquivo de importação tem requisitos de formato. É recomendável exportar uma PBR antes de usar a função de importação, adicionar ou modificar as regras no arquivo e salvar a importação.

Exportar: As regras PBR podem ser exportadas.

Load balancing

O Load balancing é usado para configurar o modo de balanceamento de linha, modo de detecção e peso do balanceamento.



Load balancing Inteligente: O Load balancing é ativado na maioria dos dispositivos por padrão. Por padrão, uma regra de balanceamento é criada com base no número de sessões e no número de interfaces WAN.

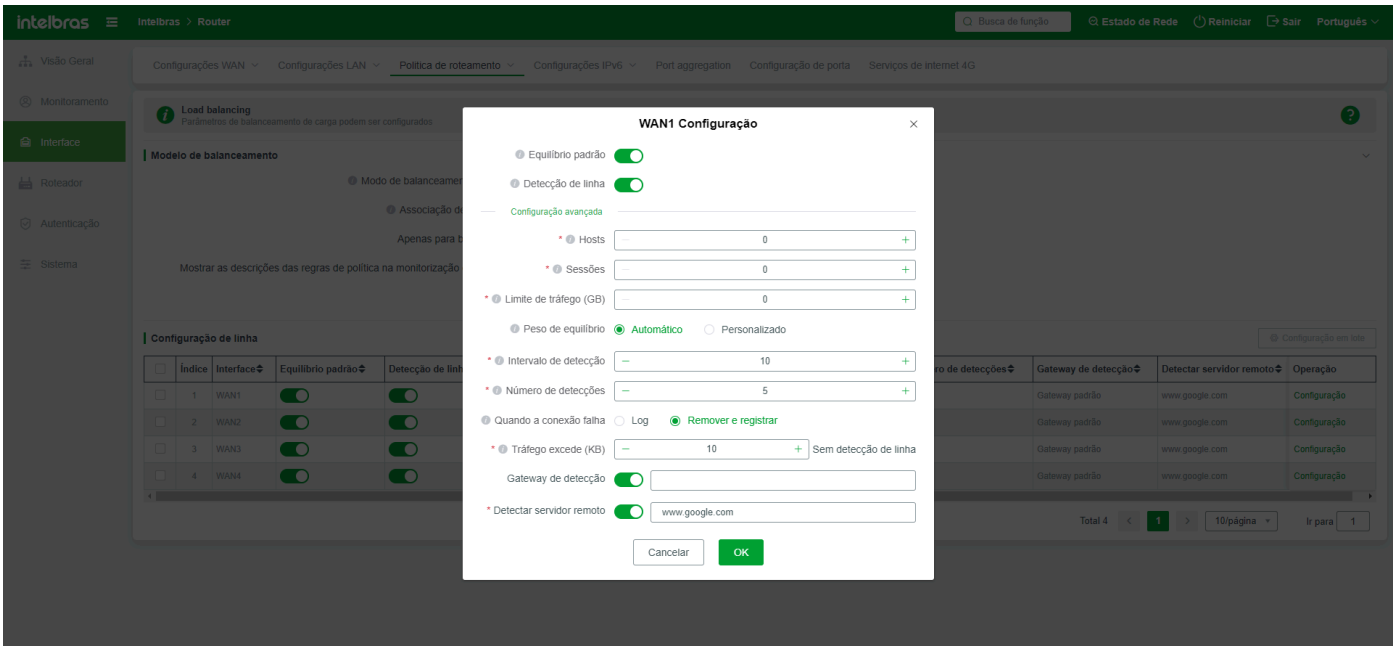
Endereço IP: indica o Load balancing. Se você selecionar o Load balancing com base no número de endereços IP, o sistema equilibra automaticamente o número de endereços IP em diferentes portas WAN. Você pode visualizar o resultado do balanceamento na coluna Status da Linha - Hosts/Sessões.

Balanceamento de Sessão: O sistema equilibra automaticamente o número de sessões em diferentes interfaces WAN.

Função de Vinculação de Identidade: se a configuração de várias linhas, para garantir o uso normal de QQ, internet banking e outros, ative a função de vinculação de identidade;

Apenas para Internet Banking: Apenas para Internet Banking;

Configuração em Lote: Após ativar o Load balancing inteligente, o sistema gera automaticamente regras de lista de balanceamento. Você pode selecionar as regras da lista para configuração em lote.



Participar no Equilíbrio Padrão: Se esta linha estiver marcada, indica participação. Se você não precisar permitir que esta linha participe do equilíbrio, remova a marca. Uma linha que não participa do equilíbrio apenas recebe a direção de dados das regras vinculadas na PBR. Se nenhum dado vinculado na PBR for para a linha, a linha não recebe nenhum tráfego de dados.

Deteção de Linha: Ativa a função de detecção de linha. A opção de parâmetros avançados só pode ser ativada quando ativada, caso contrário, é inválida. A detecção de linha é usada para verificar se uma linha está desobstruída. Em um ambiente de várias linhas, se uma linha falhar na detecção, o sistema remove a linha por padrão, e todas as sessões na linha são transferidas automaticamente para outra linha que é detectada com sucesso e participa do equilíbrio.

Limite de Tráfego (GB): limita o tráfego total de uma interface WAN. Quando o tráfego atinge o valor especificado, a interface WAN não exporta dados.

Peso do Balanceamento: Este valor é usado para comparar com o valor de balanceamento de outras linhas. O sistema determina o tamanho da carga das linhas com base no valor de balanceamento. O valor padrão é determinado automaticamente com base no valor de largura de banda. Se você escolher Personalizado, defina este parâmetro de acordo com a relação de compensação da linha. Quanto maior o parâmetro, mais dados/usuarios passarão.

Intervalo de Detecção: o intervalo intermediário de detecção automática da linha;

Número de Detecções: o número de detecção de linha;

Falha de Conexão: Indica o método de processamento para a linha quando a detecção de linha falha. Remover a linha e registrar - Se esta linha for excluída e registrada no log, todas as conexões nesta linha serão transferidas automaticamente para outras linhas; Registrar Apenas - Registra a linha desconectada apenas no log e não exclui a linha.

Nenhuma detecção de linha quando o tráfego excede o valor especificado: Nenhuma detecção de linha é realizada quando o tráfego na interface WAN excede o valor especificado.

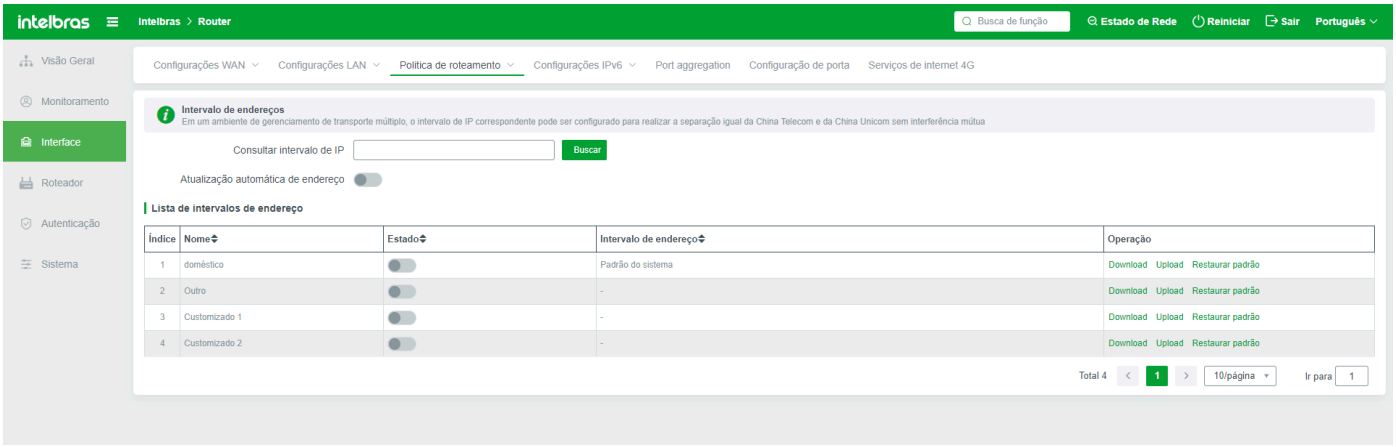
Detectar Gateway Padrão: Se este parâmetro for selecionado, o gateway da extranet desta linha é detectado. Se o conteúdo estiver vazio, o gateway padrão é detectado. O gateway padrão de alguns ISPs pode não permitir ping. Nesse caso, você pode configurar manualmente outros endereços WAN para teste.

Detectar SERVIDOR REMOTO: Insira um nome de domínio estável ou endereço IP WAN para verificar se a linha está ligada ou desligada.

Nota: Por padrão, a detecção de linha usa ping para determinar se uma linha está ligada ou desligada. Portanto, ao preencher o endereço IP de detecção ou o endereço do servidor, selecione um endereço que esteja online de forma estável por um longo período.

Intervalo de endereços (PBR)

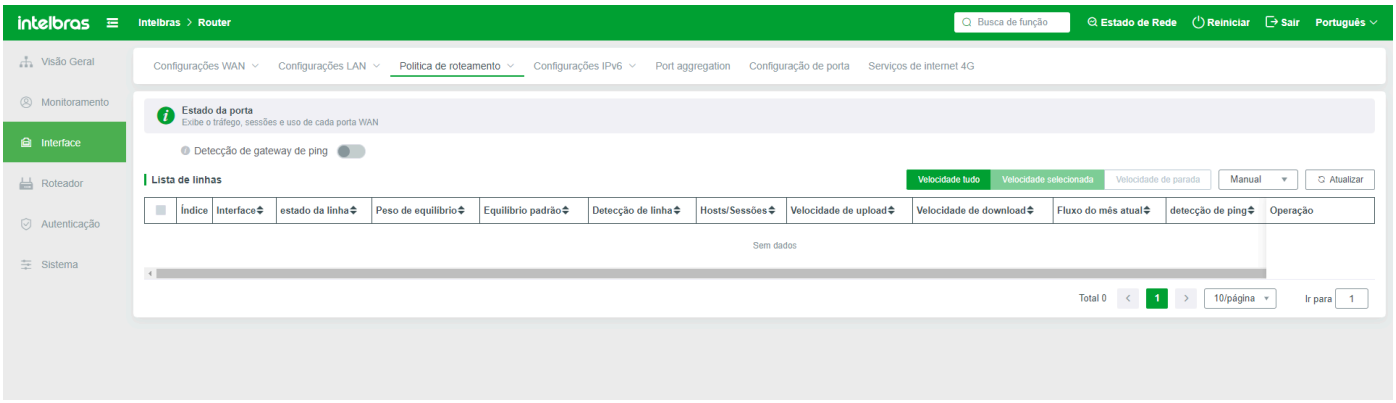
A PBR é usada em um ambiente com várias linhas de operadoras. Contanto que a linha correspondente seja selecionada e o modo de política seja definido, a rede de telecomunicações pode ser separada e afastada sem interferências.



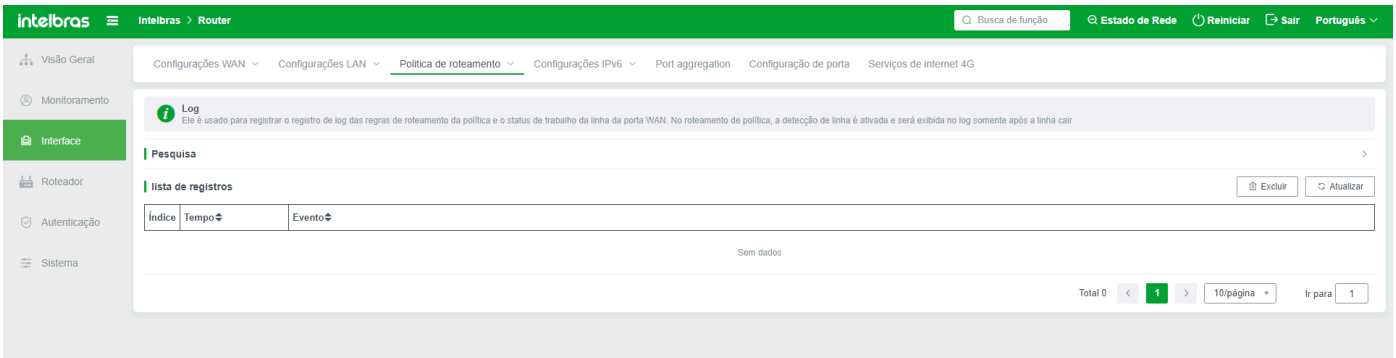
Você pode fazer upload ou download da Intervalo de endereços padrão do sistema atual. Se necessário, você pode adicionar ou excluir a Intervalo de endereços e fazer upload para o sistema.

Status da porta

Status atual de cada extranet. Suporta medição de velocidade e medição de ping.



Verificação de ping do gateway: Após a ativação desta função, o sistema automaticamente faz ping no gateway da porta WAN. Você pode visualizar o resultado do ping. Resultado do teste de ping do gateway Clique no botão "Visualizar Resultado do Ping" na lista.



Todas as medições de velocidade: ou seja, medir a velocidade de todas as portas WAN atuais, a lista da página será atualizada automaticamente com a velocidade de upload e download após todas as medições de velocidade serem enviadas;

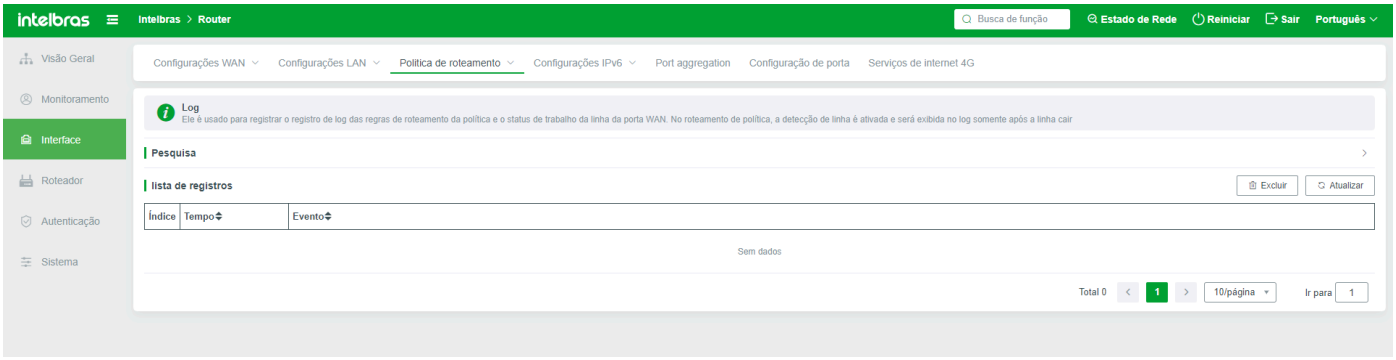
Medição de velocidade: medição de velocidade para porta WAN na caixa;

Suspensão de medição de velocidade: a página será atualizada automaticamente com a velocidade de upload e download após todas as medições de velocidade serem enviadas. Se precisar parar, clique na medição de velocidade e selecione.

Atualização automática: O status da interface WAN pode ser atualizado em intervalos diferentes.

Log

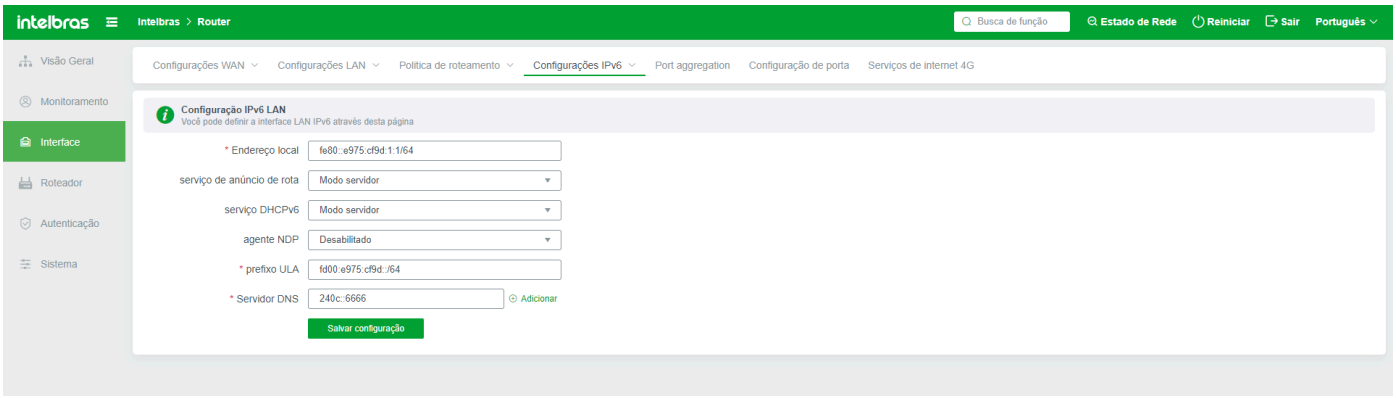
Registra os logs das regras PBR e o status de funcionamento da linha de interface WAN. Na PBR, a detecção de linha está ativada para a linha e a linha é exibida no log apenas quando a linha é desconectada.



Configurações IPv6

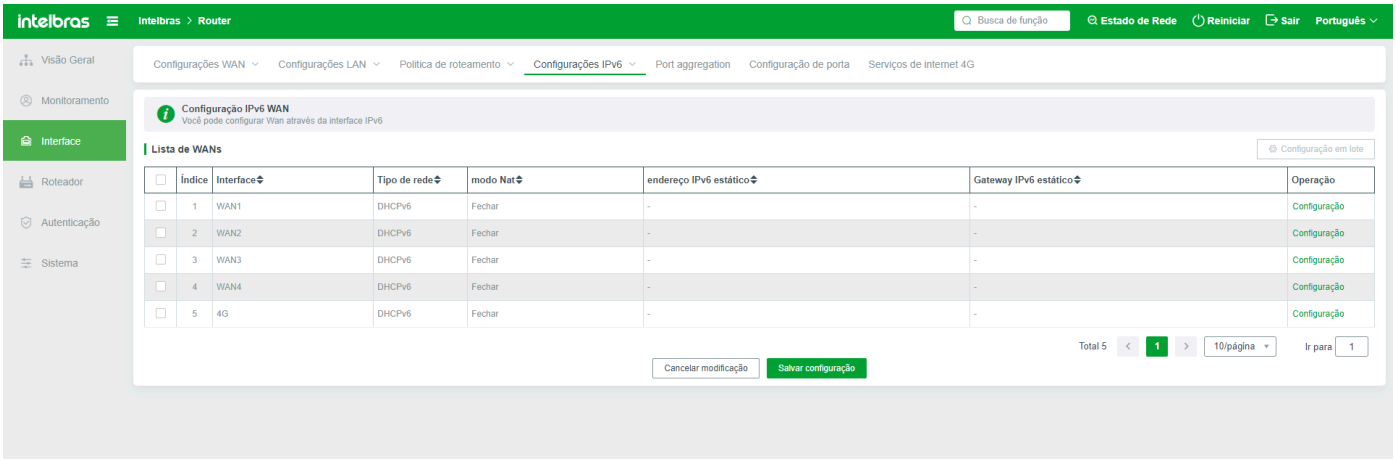
Configuração de LAN IPv6

Configure as interfaces IPv6 conforme necessário.



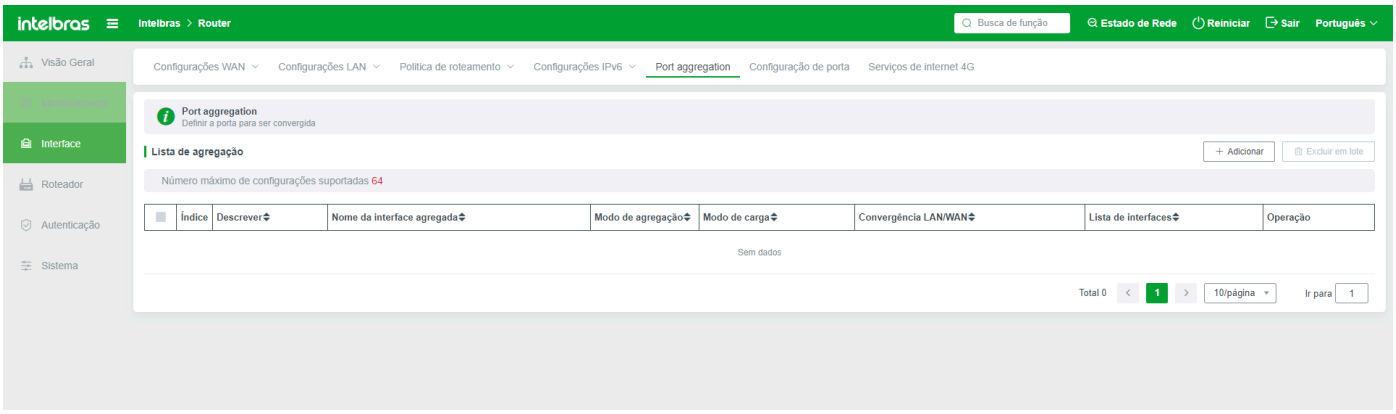
Configurações IPv6 WAN

Configure as interfaces IPv6 WAN conforme necessário.



Port aggregation

Configure a porta a ser agregada

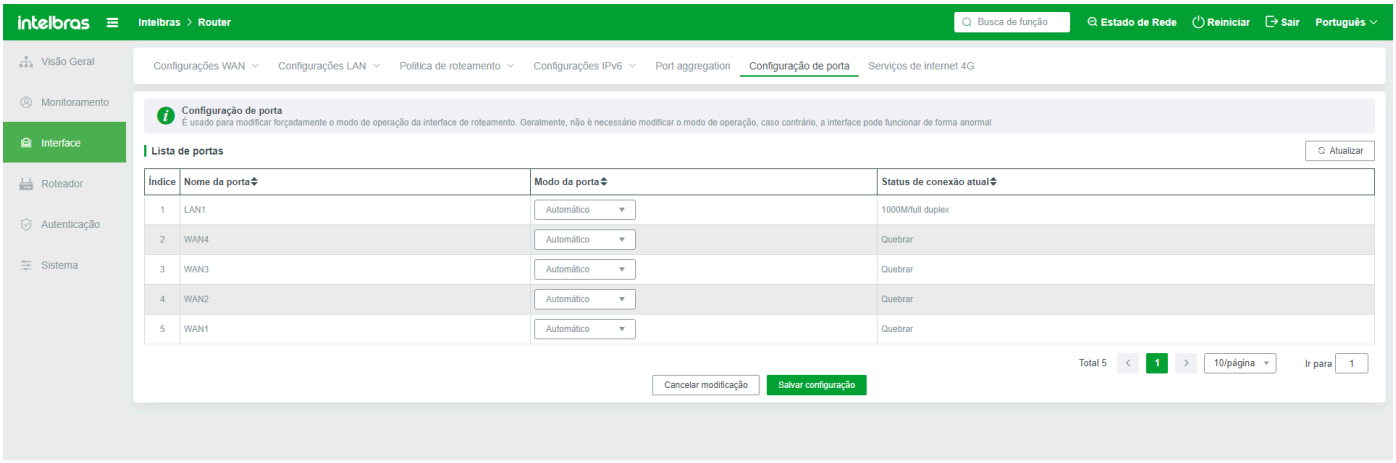


Clique em adicionar para configurar regras detalhadas de agregação de portas.

Agregação LAN/WAN: você pode escolher a porta que precisa ser agregada, seja porta LAN ou porta WAN. Selecione o modo de interface de agregação a ser definido: LACP e agregação manual. O padrão é LACP. Selecione o modo de carga a ser definido: MAC, IP+, MAC+IP. Selecione as interfaces que precisam ser definidas e escolha pelo menos duas interfaces para agregação

Configurações de Porta

Este comando é usado para alterar forçadamente o modo de operação de uma interface de roteamento. Geralmente, não é necessário alterar o modo de operação. Caso contrário, a interface pode não funcionar corretamente.

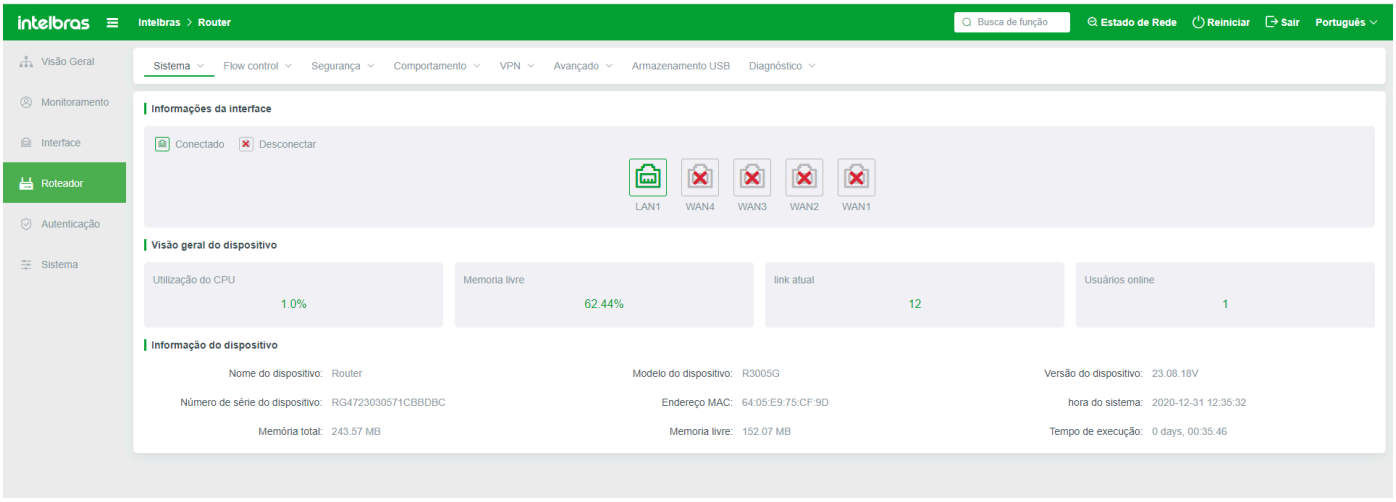


Roteador

Estado do Sistema

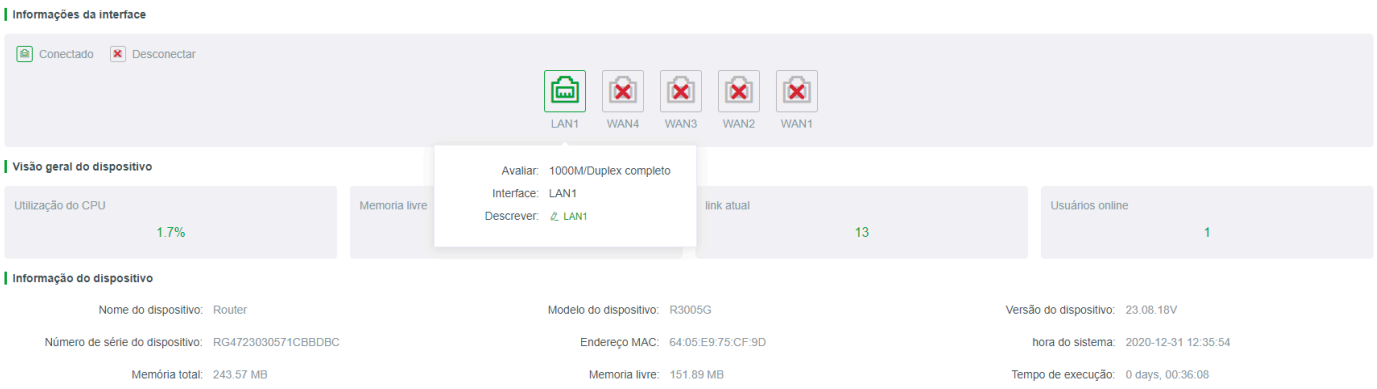
Visão Geral

As informações básicas do dispositivo principal são exibidas, como status de execução do sistema, duração, status atual da interface do dispositivo principal e dados de informações do dispositivo.



Informações da porta. Uma porta verde indica que a porta correspondente no dispositivo está conectada a um cabo de rede. Cinza indica que nenhum cabo de rede está conectado. Se apontar para o ícone de qualquer porta de rede, as informações básicas sobre a porta de rede atual são exibidas acima do ícone, incluindo taxa de porta de rede, status de fornecimento de energia POE (necessário que o hardware do dispositivo suporte fornecimento de energia POE), tipo de interface (LAN/WAN) e Descrição (Você pode personalizar a descrição).

Nota: A descrição contém de 1 a 8 caracteres, letras, dígitos, e apenas os seguintes símbolos são suportados: _-! @ # $% ^ & * ().



Estado da Rede

O status da rede aqui refere-se principalmente ao status da porta WAN, porta óptica. Você pode visualizar ou operar a porta WAN correspondente na barra de operações da lista.

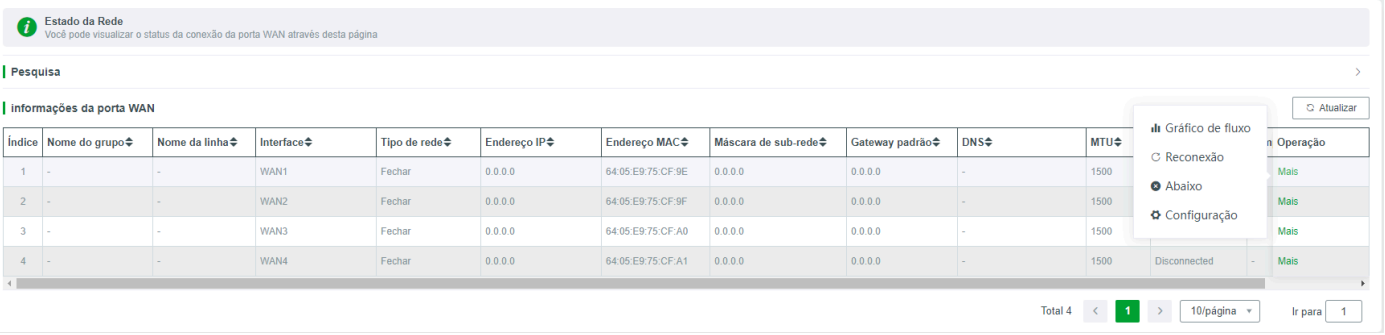
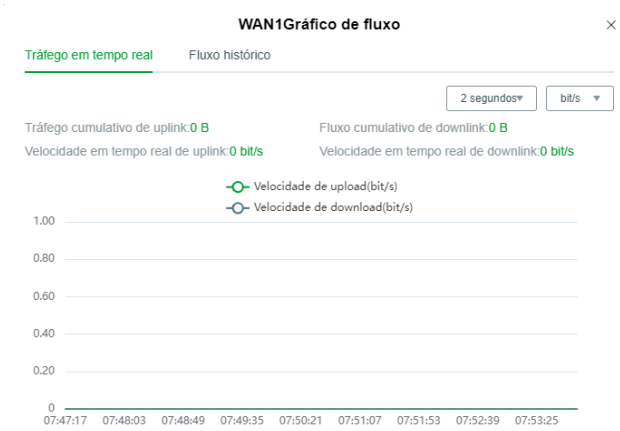
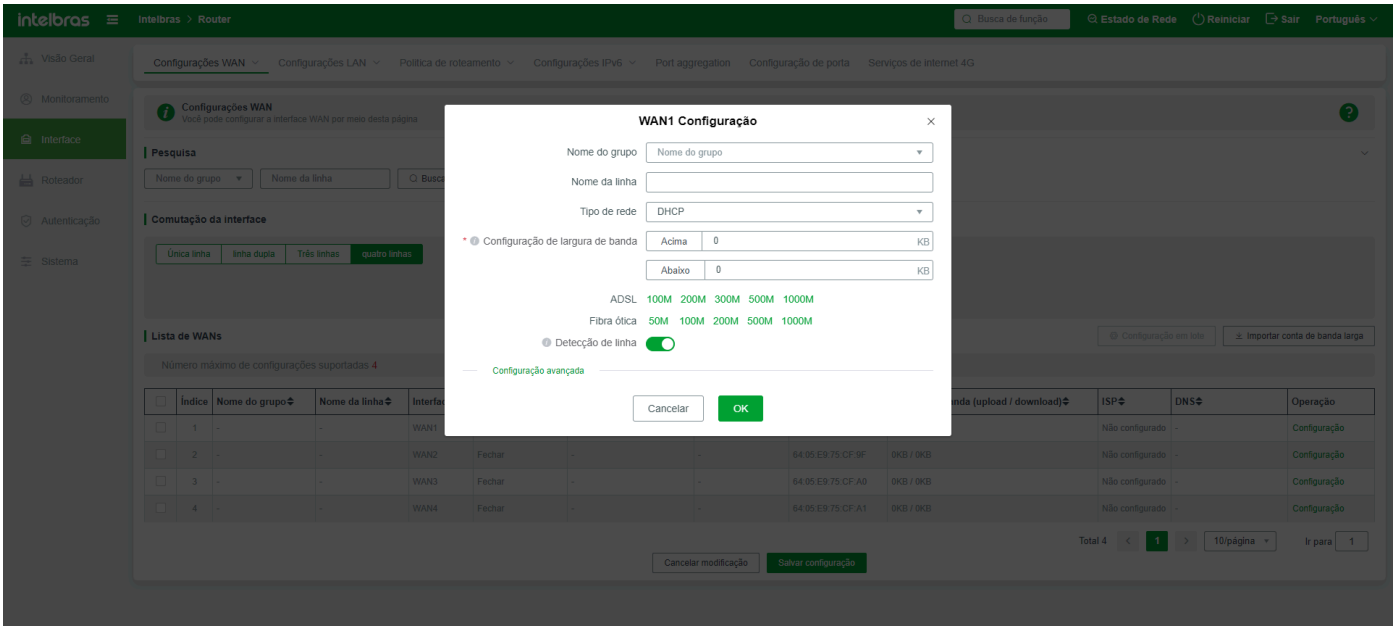


Gráfico de Fluxo: Clique em "Gráfico de Fluxo" para exibir os dados de tráfego em tempo real da WAN atual e o gráfico estatístico de desconto, que geralmente é atualizado e registrado automaticamente a cada 3 segundos.



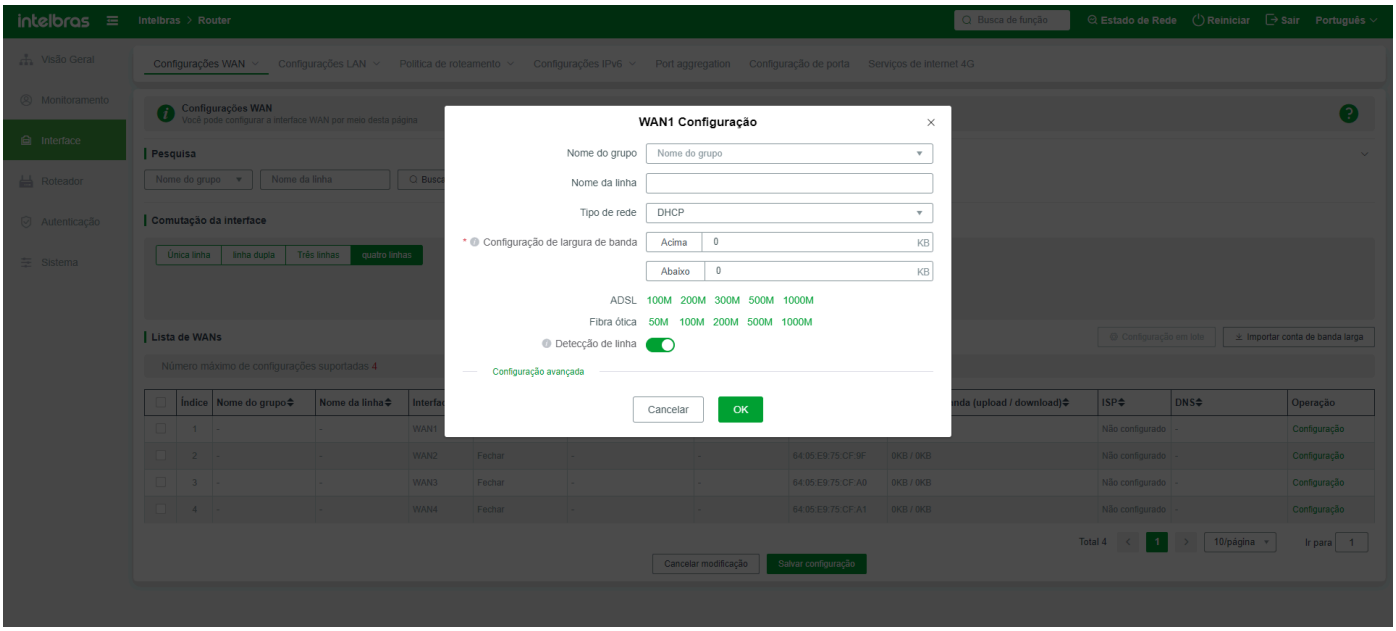
Você também pode visualizar estatísticas de tráfego históricas, incluindo estatísticas de tráfego na última hora, 1 dia e 7 dias.



Reconectar: ou seja, desconectar manualmente a conexão e reconectar automaticamente imediatamente.

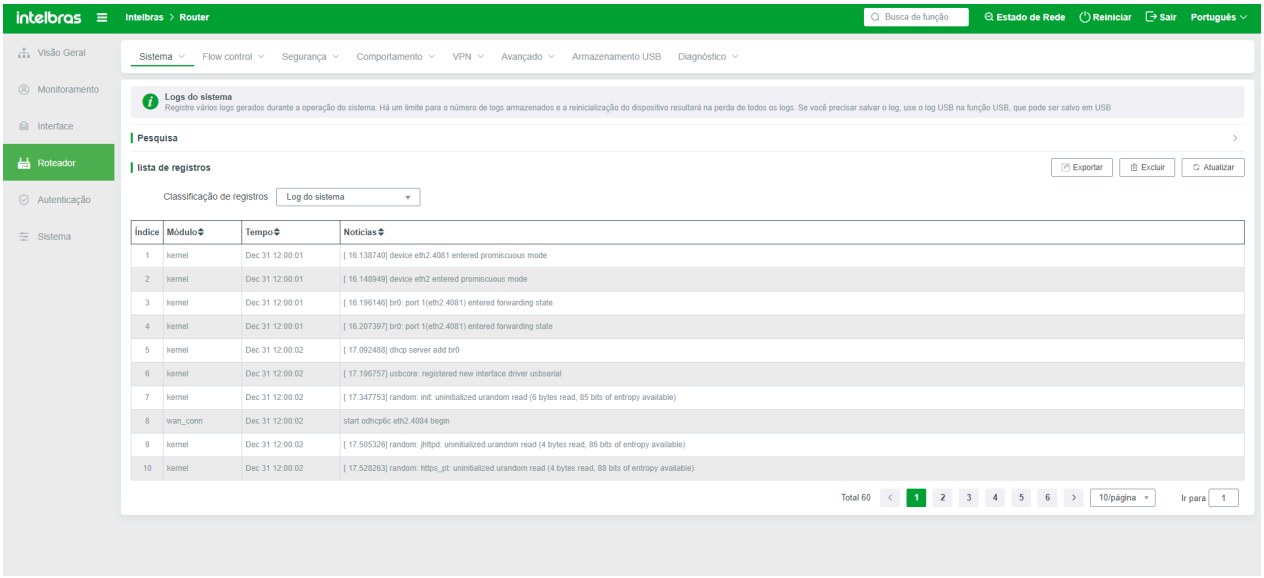
Desconectar: Após clicar, a conexão será desconectada e não será reconectada automaticamente.

Configuração: Configure o modo de conexão com a Internet e selecione o tipo de rede conforme necessário. - O valor padrão é Desligado, Banda larga, endereço IP dinâmico e endereço IP estático.



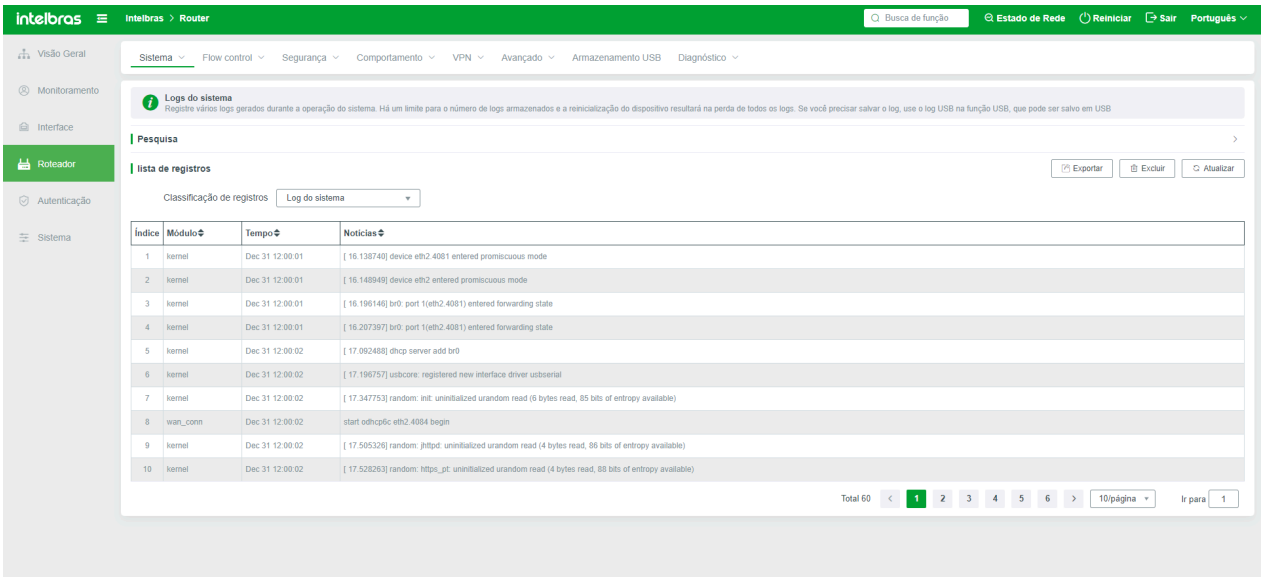
Registro de Login

Registra as informações de login do usuário



Logs do Sistema

Esta seção descreve os logs gerados durante a execução do sistema, incluindo logs do sistema, logs ARP, logs de ataque de tráfego, logs DDos, logs de autenticação WEB, logs PPPoE, logs PBR e logs de controle de acesso. A quantidade de logs armazenados é limitada e todos os logs serão perdidos após o reinício do dispositivo. Se precisar salvar logs, use logs USB na função USB.



Exportar: Selecione o tipo de log a ser exportado e clique em Exportar para exportar os logs.

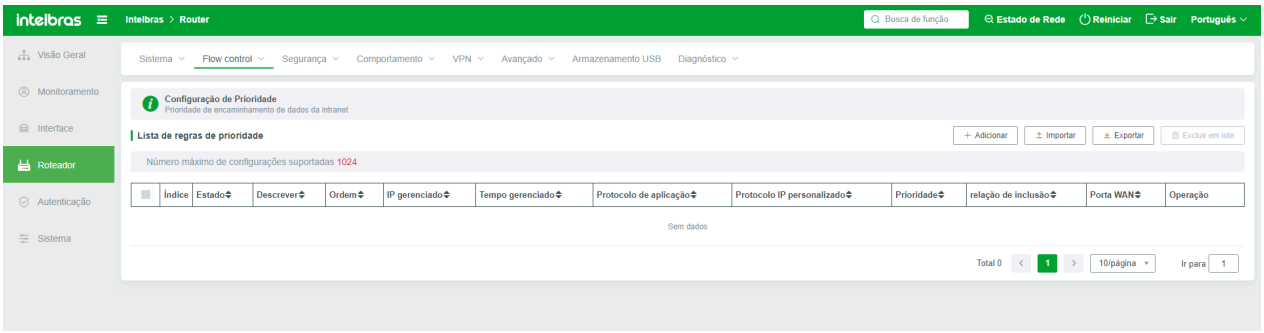
Excluir: Selecione o tipo de logs a serem excluídos e clique em Excluir. Logs excluídos não podem ser restaurados.

Atualizar: indica o registro de log de escovação de linha.

Controle de Fluxo

Configuração de Prioridade

Configure a prioridade para o sistema encaminhar dados da Intranet.



Adicionar: Adiciona regras de prioridade de controle de fluxo conforme necessário

Status: Após a ativação da regra de prioridade de controle de fluxo, ela entra em vigor; se a regra de prioridade de controle de fluxo estiver desativada, ela se torna inválida.

Descrição da Regra: Descrição da regra, equivalente a nomear a regra;

Prioridade de Execução: indica o valor da ordem de execução entre as regras. Quanto maior o valor, mais prioridade as regras têm para serem lidas e executadas.

Endereço IP Gerenciado: indica o endereço IP, segmento de endereço IP ou grupo de endereços IP para os quais a regra entra em vigor. Se selecionar Todos os Endereços, a regra entra em vigor em todos os terminais. Se Custom for selecionado, insira um endereço IP ou segmento de endereço IP.

Tempo Gerenciado: indica o horário em que a regra entra em vigor. O tempo deve ser específico para um determinado período em uma semana. Fora deste período, o trabalho de prioridade não entra em vigor;

Protocolo de Aplicação: Você pode selecionar diferentes ou todos os protocolos de aplicação para entrar em vigor. Os protocolos de aplicação selecionados entram em vigor de acordo com as regras.

Prioridade Global: A prioridade dos dados desta regra em todos os dados na LAN, alta, média e baixa.

Prioridade Local: Em todos os dados deste host, a prioridade de processamento de dados para esta regra é alta, média e baixa.

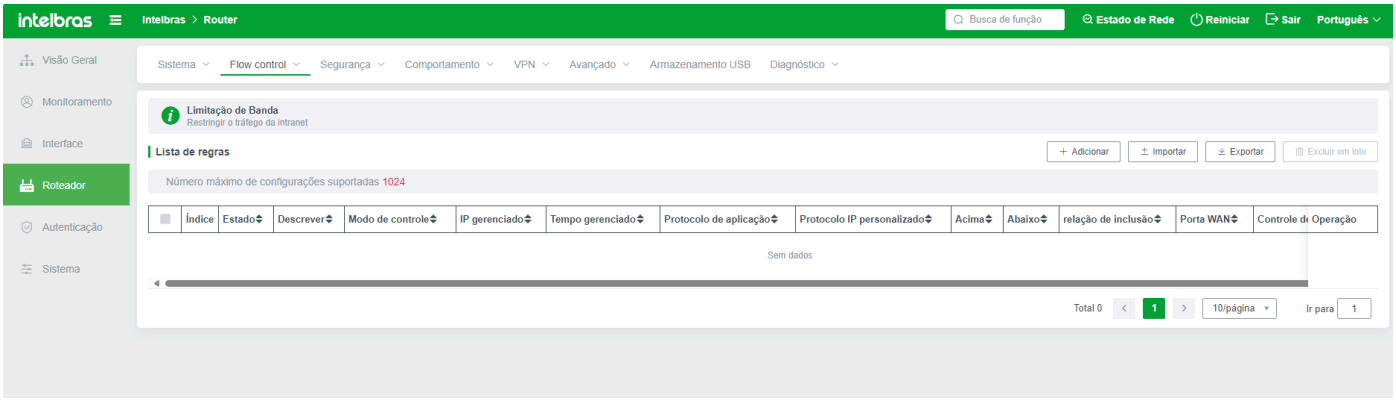
IP Personalizado: Se for necessário atribuir prioridade a um endereço IP remoto específico, mas não existe um aplicativo no protocolo de aplicação, você pode usar a função de endereço IP personalizado.

Relação de Inclusão: A relação de inclusão do protocolo. Tudo: indica que tanto o protocolo de aplicação quanto o protocolo definido pelo usuário correspondem com sucesso e a regra entra em vigor. Parte: indica que qualquer regra de prioridade coincide com o protocolo de aplicação e o protocolo definido pelo usuário e entra em vigor imediatamente.

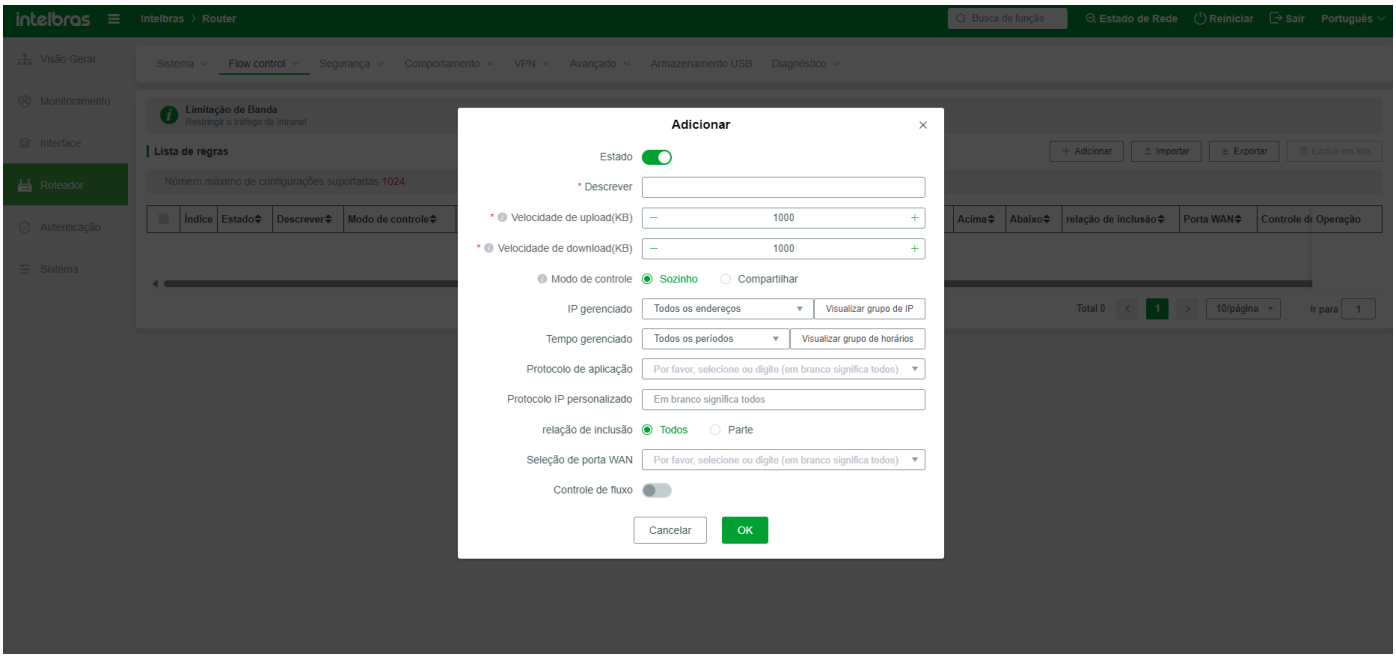
Seleção de Porta WAN: Selecione a porta WAN na qual a regra entra em vigor.

Limitação de Banda Larga

Restrições nas velocidades de upload e download dos terminais da Intranet.



Adicionar: Adiciona uma regra de limitação de largura de banda.



Status: Indica se a regra de controle está em vigor. Se marcado, a regra está em vigor;

Descrição da Regra: Descrição da regra;

Velocidade de Uplink: define o limite máximo de velocidade de upload. Se o valor for definido como 0, indica que não há restrição.

Velocidade de Downlink: define o limite máximo de velocidade de download. Se o valor for definido como 0, indica que não há restrição.

Modo de Controle: (Limite Separado) A velocidade de cada IP nesta faixa será limitada à velocidade definida, ou seja, cada IP na faixa definida será limitado separadamente; (Limite Compartilhado) A velocidade total de todos os endereços IP nesta faixa será limitada à velocidade definida;

Endereço IP Gerenciado: indica o endereço IP, segmento de endereço IP ou grupo de endereços IP para os quais a regra entra em vigor. Se selecionar Todos os Endereços, a regra entra em vigor em todos os terminais. Se Custom for selecionado, insira um endereço IP ou segmento de endereço IP.

Tempo Gerenciado: indica o horário em que a regra entra em vigor. O tempo deve ser específico para um determinado período em uma semana. Fora deste período, o limite de largura de banda não entra em vigor.

Protocolo de Aplicação: Você pode selecionar diferentes ou todos os protocolos de aplicação para entrar em vigor. Os protocolos de aplicação selecionados entram em vigor de acordo com as regras.

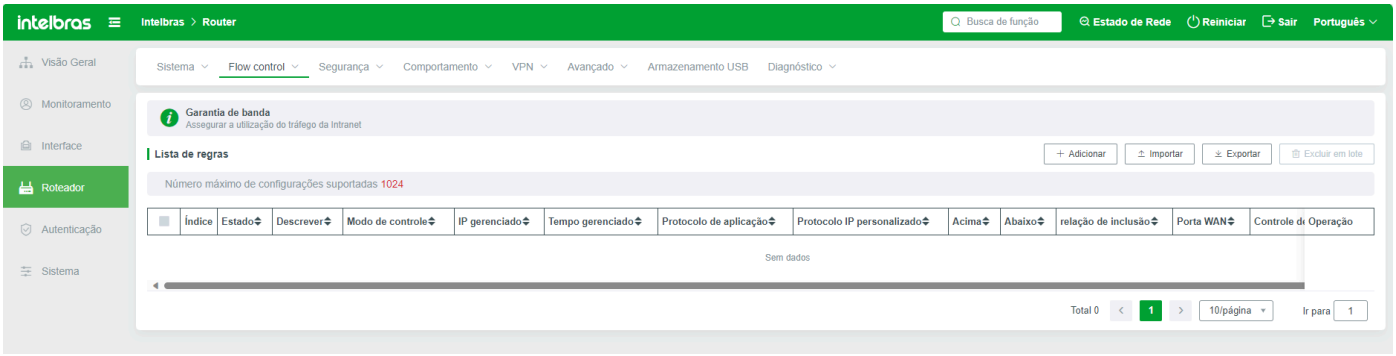
Protocolo IP definido pelo usuário: Você pode definir endereços IP remotos e protocolos de porta e usá-los como objetos de controle.

Relação de Inclusão: A relação de inclusão do protocolo. Tudo: indica que tanto o protocolo de aplicação quanto o protocolo definido pelo usuário correspondem com sucesso e a regra entra em vigor. Parte: indica que qualquer regra de prioridade coincide com o protocolo de aplicação e o protocolo definido pelo usuário e entra em vigor imediatamente.

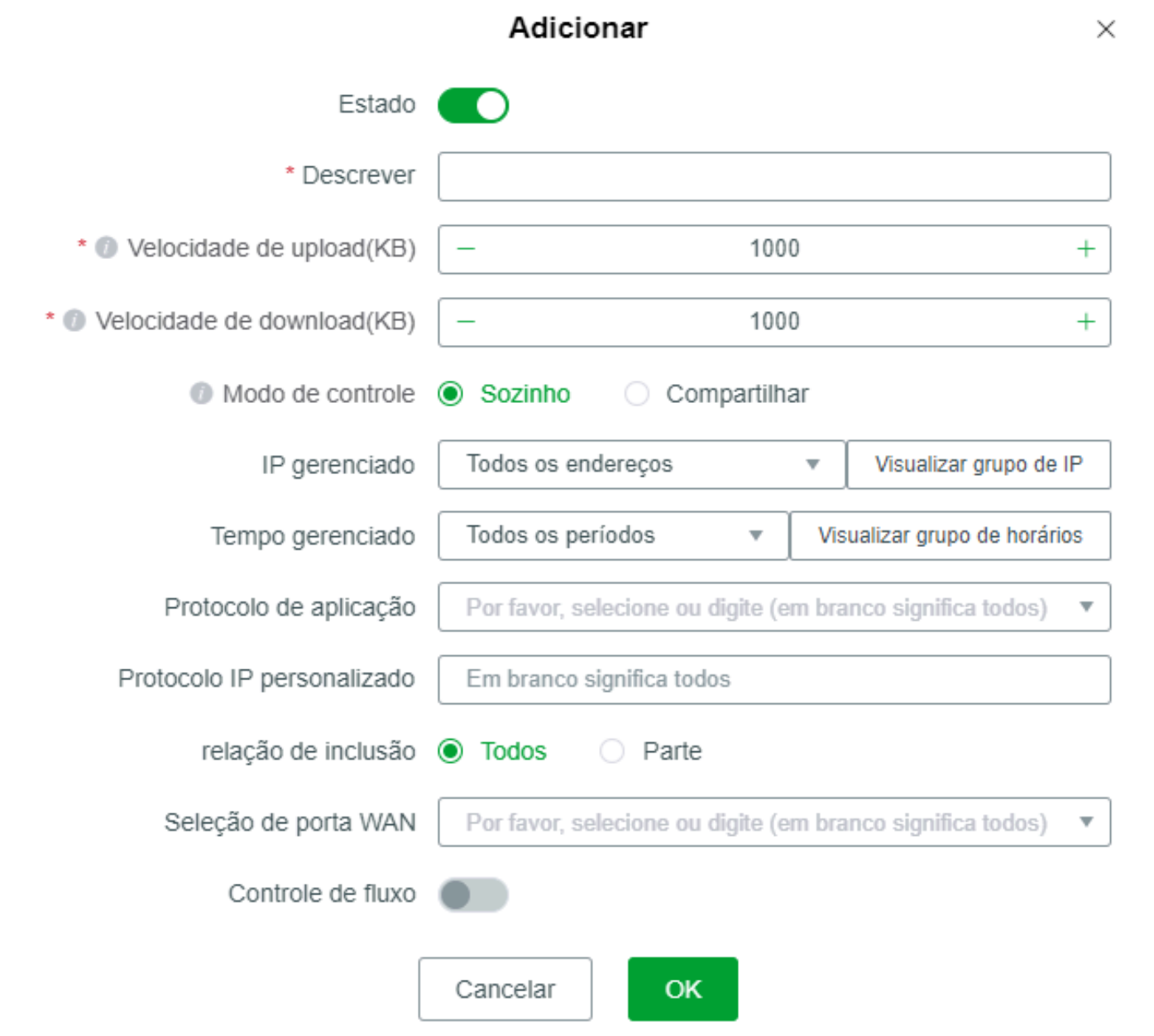
Seleção de Porta WAN: Selecione a porta WAN na qual a regra entra em vigor.

Controle com Base no Tráfego: Quando o tráfego de download total na interface WAN atinge o percentual definido, a regra de limitação de largura de banda é ativada e o tráfego é alocado para terminais de acordo com as regras.

Garantia de Banda



Add: Adiciona uma regra de largura de banda



Status: Se este parâmetro estiver ativado, a regra de garantia de largura de banda entra em vigor; se este parâmetro estiver desativado, ela se torna inválida.

Descrição da Regra: Descrição de uma regra, equivalente a nomear a regra;

Prioridade de Execução: indica o valor da ordem de execução entre as regras. Quanto maior o valor, mais prioridade as regras têm para serem lidas e executadas.

Endereço IP Gerenciado: indica o endereço IP, segmento de endereço IP ou grupo de endereços IP para os quais a regra entra em vigor. Se selecionar Todos os Endereços, a regra entra em vigor em todos os terminais. Se Custom for selecionado, insira um endereço IP ou segmento de endereço IP.

Tempo Gerenciado: indica o horário em que a regra entra em vigor. O tempo deve ser específico para um determinado período em uma semana. Fora deste intervalo de tempo, a função de garantia de largura de banda não entra em vigor.

Protocolo de Aplicação: Você pode selecionar diferentes ou todos os protocolos de aplicação para entrar em vigor. Os protocolos de aplicação selecionados entram em vigor de acordo com as regras.

Prioridade Global: A prioridade dos dados desta regra em todos os dados na LAN, alta, média e baixa.

Prioridade Local: Em todos os dados deste host, a prioridade de processamento de dados para esta regra é alta, média e baixa.

IP Personalizado: Se for necessário garantir a largura de banda para um endereço IP remoto específico, mas não existe um aplicativo no protocolo de aplicação, você pode usar a função de endereço IP personalizado.

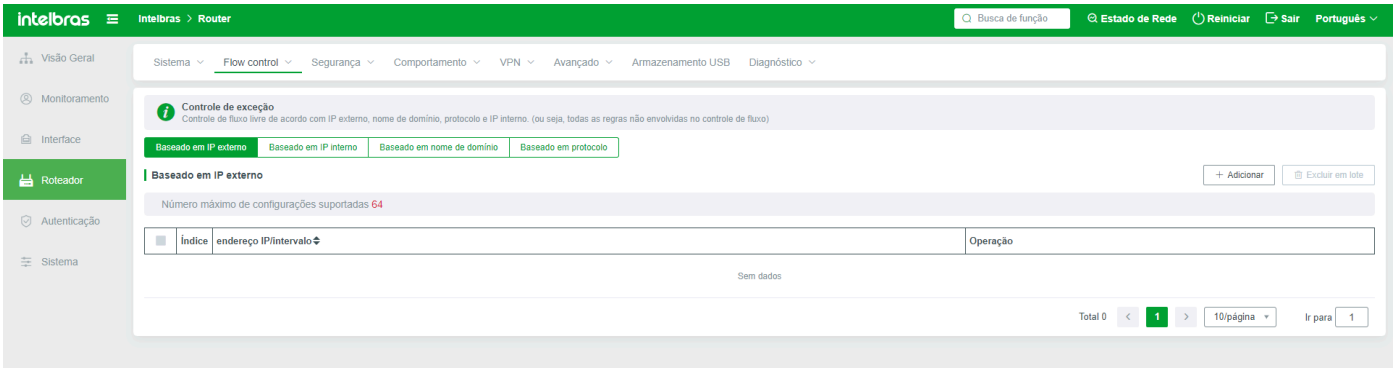
Relação de Inclusão: A relação de inclusão do protocolo. Tudo: indica que tanto o protocolo de aplicação quanto o protocolo definido pelo usuário correspondem com sucesso e a regra entra em vigor. Parte: indica que qualquer regra de prioridade coincide com o protocolo de aplicação e o protocolo definido pelo usuário e entra em vigor imediatamente.

Seleção de Porta WAN: Selecione a porta WAN na qual a regra entra em vigor.

Controle com Base no Tráfego: Quando o tráfego de download total na interface WAN atinge o percentual definido, a regra de garantia de largura de banda é ativada e o tráfego é alocado para os terminais de uplink e downlink de acordo com a regra.

Exceções de Controle

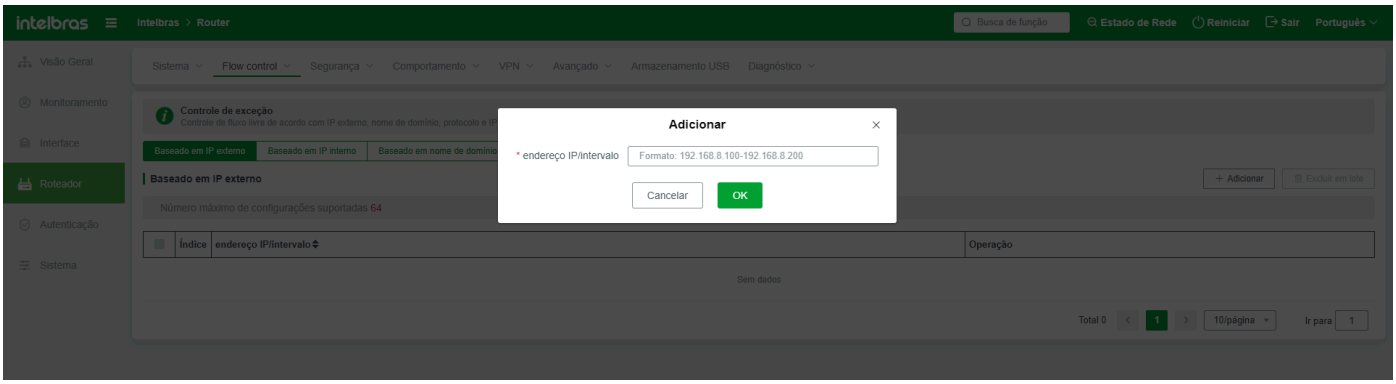
Com base nas regras de garantia e limitação de largura de banda acima, o terminal de exceção não é restrito pelas regras de controle de fluxo.



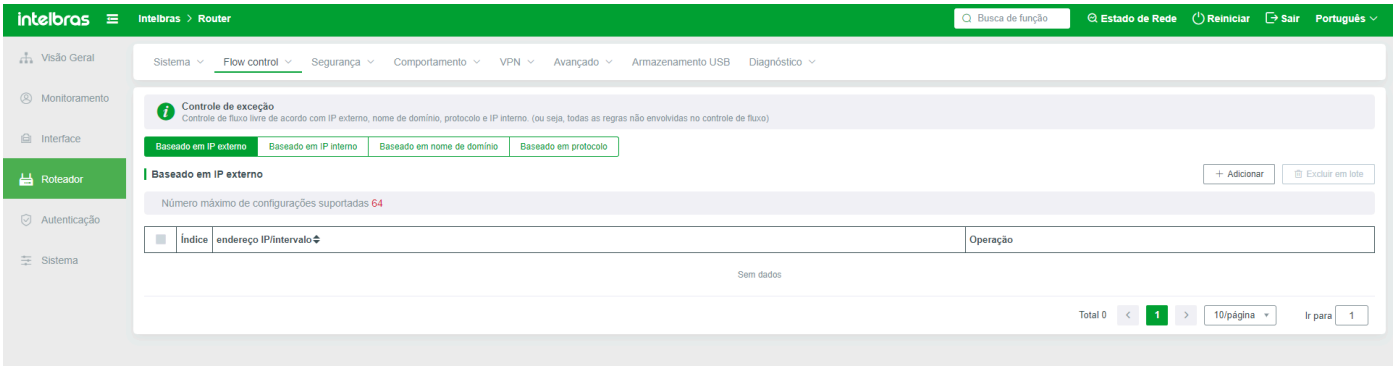
Com Base em IP Externo

Quando um usuário de terminal acessa o endereço IP externo especificado, ele não é restrito pelas regras de controle de fluxo ou garantia de largura de banda. No entanto, a regra de controle de fluxo entra em vigor quando o usuário acessa um endereço IP externo que não está especificado.

Configuração de endereço IP externo É compatível com um único endereço IP ou um segmento de endereço IP. Se inserir um segmento de endereço IP, o segmento de endereço IP deve variar de pequeno para grande; caso contrário, a entrada falha.



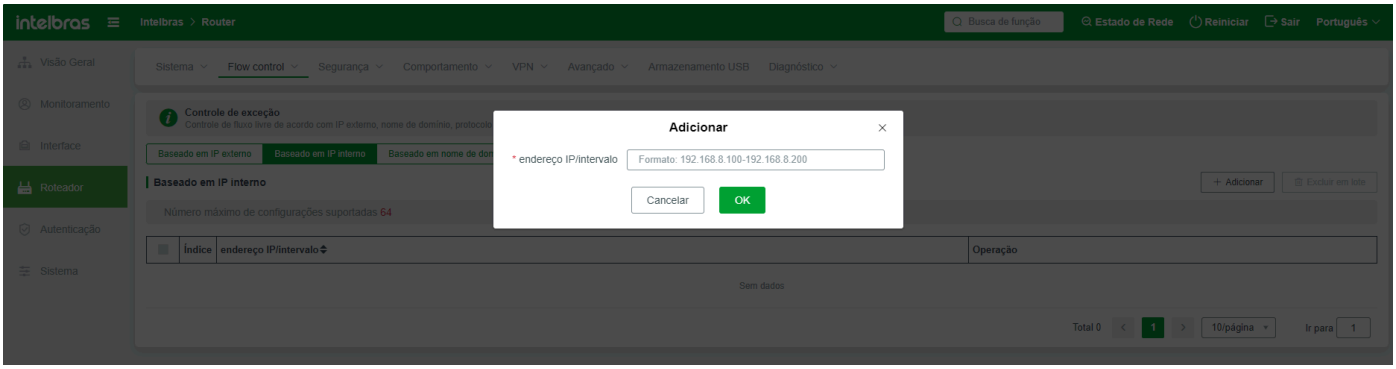
Se uma exceção for necessária para endereços IP com segmentos diferentes, adicione uma regra novamente.



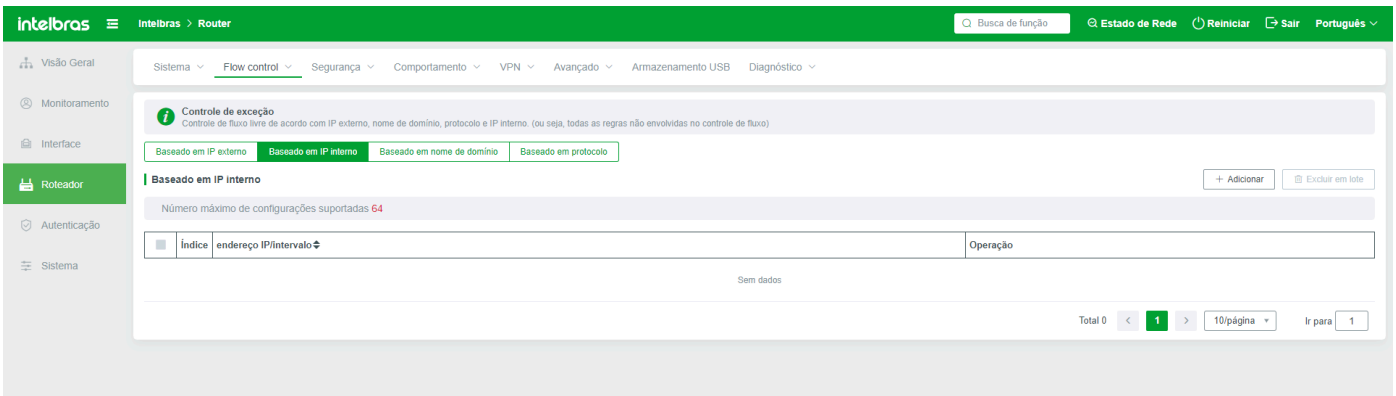
Com Base em IP Interno

É um usuário de terminal de Intranet cuja largura de banda não é restrita ou garantida (insira o endereço IP aqui). Usuários de IP Intranet que não inserem este parâmetro são automaticamente restritos pelas regras de controle de fluxo.

Configuração de endereço IP interno É compatível com um único endereço IP ou um segmento de endereço IP. Se inserir um segmento de endereço IP, o segmento de endereço IP deve variar de pequeno para grande; caso contrário, a entrada falha.



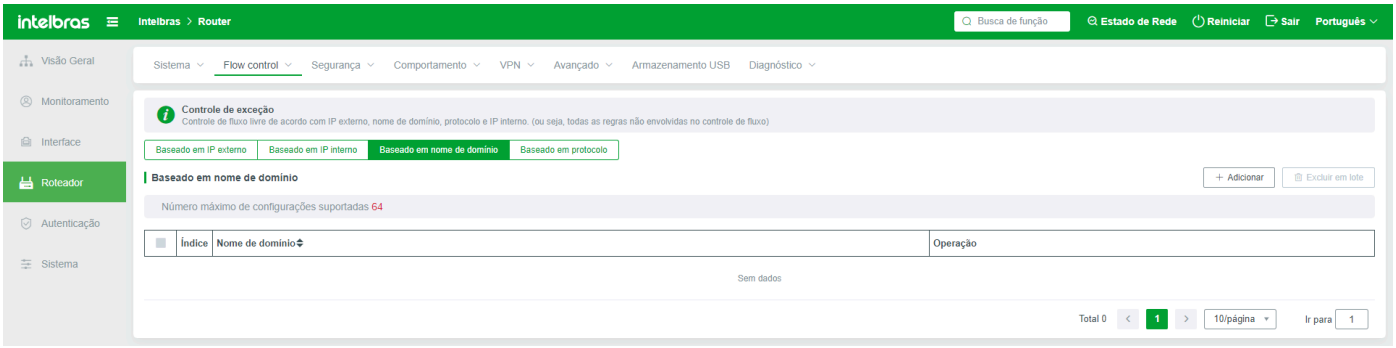
Se uma exceção for necessária para endereços IP com segmentos diferentes, adicione uma regra novamente.



Com Base em Domínio

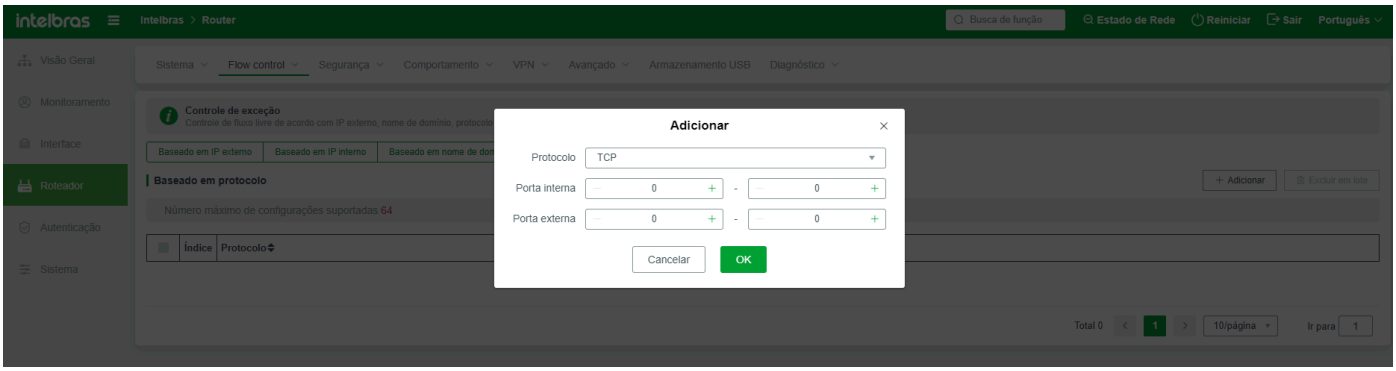
O nome de domínio remoto é uma exceção à regra de controle de fluxo. Quando um terminal interno acessa o nome de domínio inserido neste nome de domínio, ele não é restrito pela restrição ou garantia de largura de banda.

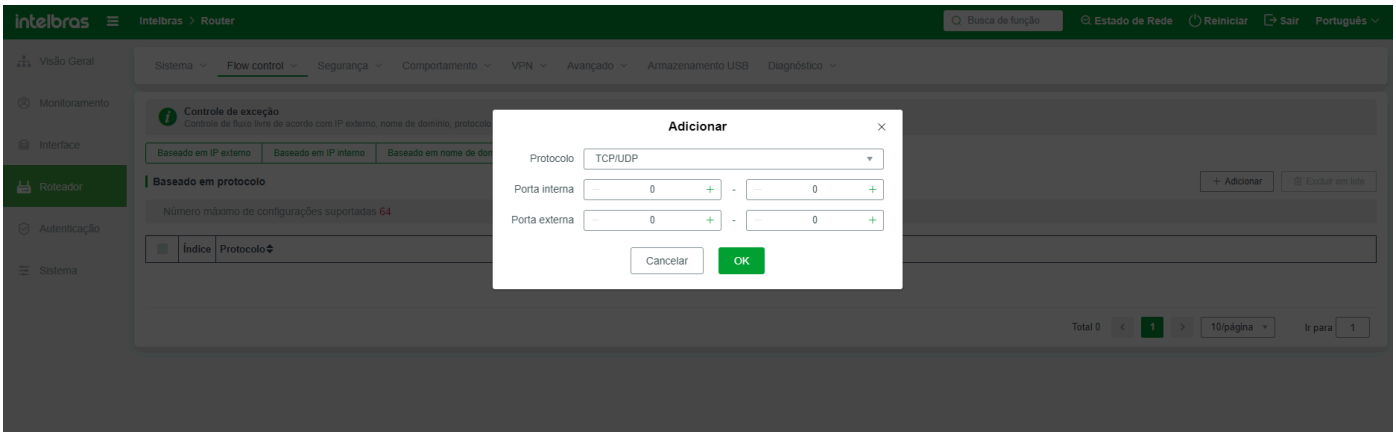
O nome de domínio deve seguir a regra do nome de domínio. Você pode inserir um endereço IP que não segue a regra.



Com Base em Protocolo

É feita uma exceção ao controle de fluxo com base no tipo e porta do protocolo. Da mesma forma, terminais internos não são restritos pelas regras de banda larga e garantia ao acessar o conteúdo do protocolo correspondente.



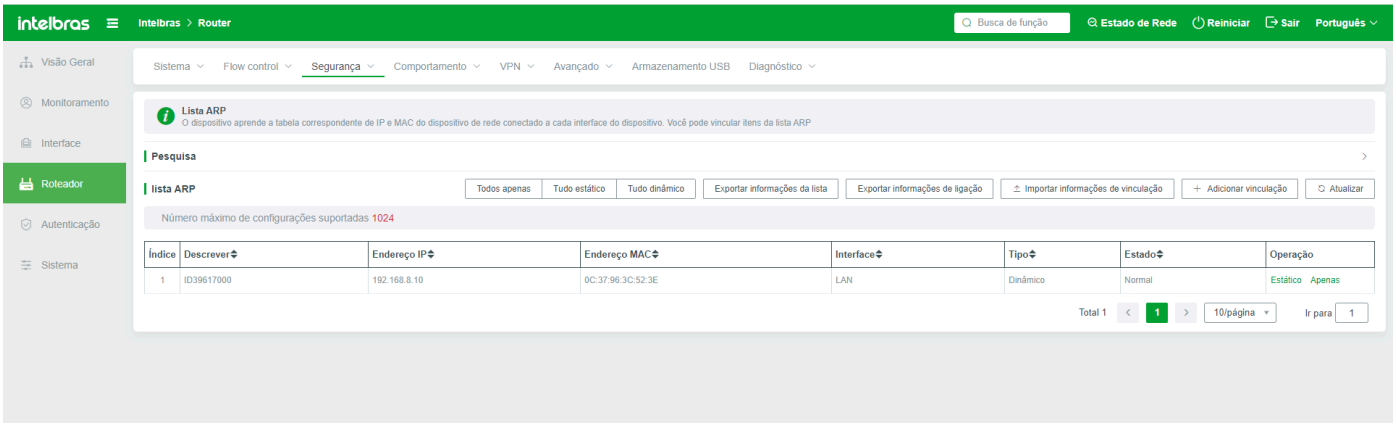


Segurança

Lista ARP

Geralmente, todos os terminais e interfaces WAN na Intranet são exibidos na lista ARP. Se você deseja vincular um endereço IP estaticamente, de forma exclusiva ou desvinculá-lo dinamicamente, defina este parâmetro aqui.

Para confirmar ou visualizar o status de vinculação de um endereço IP, você pode selecionar um terminal pelo endereço IP ou endereço MAC.



Apenas Todos: O atalho de clique único vincula os endereços IP e MAC de todos os terminais da Intranet de forma exclusiva. Quando vinculado como um terminal exclusivo, o dispositivo aprende automaticamente o endereço MAC físico atual e o endereço IP atribuído do terminal na LAN. Quando o terminal se reconecta à rede local, o dispositivo verifica automaticamente se o endereço IP obtido pelo terminal e o endereço MAC vinculado são correspondidos. Se algum dos endereços IP ou MAC não puder ser aprendido, o terminal não poderá usar a rede normalmente.

Todos Estáticos: O atalho de clique único vincula os endereços IP e MAC de todos os terminais da Intranet ao estado estático. A diferença entre vincular como único e vincular como exclusivo é que, ao vincular como único, o endereço IP e o endereço MAC do terminal devem corresponder com sucesso. O endereço IP aprendido pelo mecanismo estático só pode ser usado pelo terminal MAC ao qual o terminal está vinculado. Mesmo que o endereço MAC do terminal não seja atribuído ao endereço IP original vinculado especificado, a rede pode ser usada normalmente. No entanto, o endereço IP vinculado não pode ser atribuído a outros terminais e só pode ser usado em terminais específicos.

Todos Dinâmicos: Todos os terminais da Intranet são dinâmicos e não são afetados pelos endereços MAC e IP. Os endereços IP atribuídos pelo dispositivo de roteamento prevalecem.

Exportar informações de vinculação: Se o sistema não estiver vinculado ao ARP, os dados podem ser exportados. Se o sistema estiver vinculado, os dados podem ser exportados conforme mostrado na figura a seguir:

Adicionar: Adiciona manualmente um endereço de vinculação ARP

Descrição: Conteúdo de descrição personalizado, fácil de distinguir em muitas regras;

Endereço IP: Insira o endereço IP do terminal a ser vinculado. O formato do endereço IP deve ser o mesmo que o formato do endereço IP. Caso contrário, a entrada falha.

Endereço MAC: Insira o endereço MAC do terminal a ser vinculado. O endereço MAC deve ser real e correto.

Tipo: Selecione o tipo de vinculação como único ou estático, conforme descrito acima;

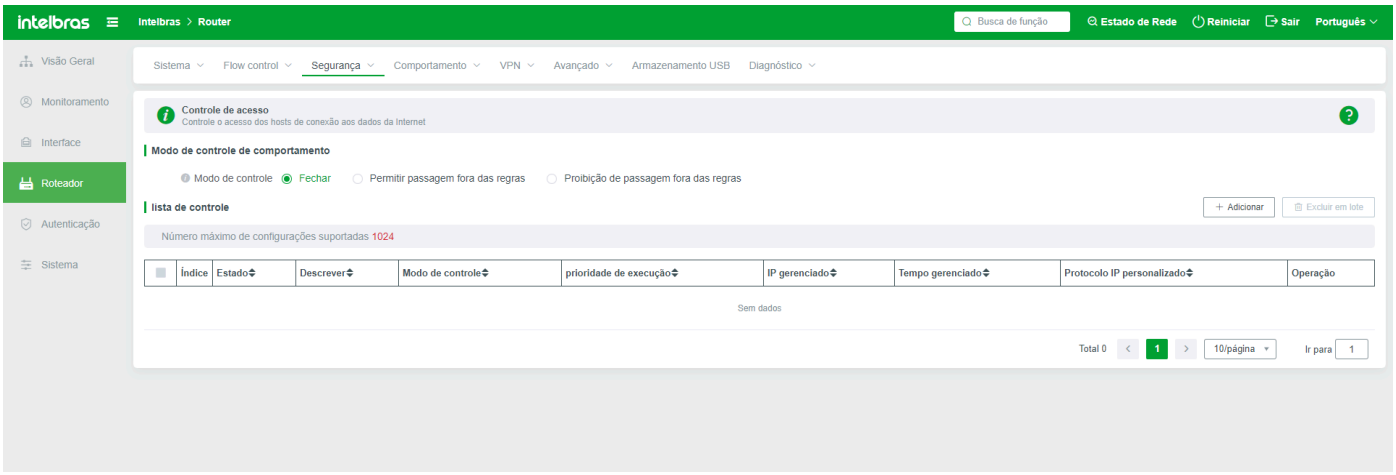
Interface: Indica a interface de endereço vinculada, que está na LAN ou na extranet.

Lista: Indica a lista de usuários vinculados ou não vinculados. A lista exibe informações sobre terminais atuais ou detectados. A vinculação ARP estática, exclusiva ou dinâmica pode ser realizada em um terminal.

O terminal de sondagem refere-se ao terminal que foi conectado à LAN local sem fio, mas está desconectado de outros dispositivos sem fio.

Controle de Acesso

Controla se o terminal pode acessar a Internet ou apenas os protocolos de aplicação.



Modo de Controle de Comportamento: existem três estados: fechar, permitir a passagem fora das regras e proibir a passagem fora das regras

Desativar: Se você selecionar Desativar, todas as regras criadas abaixo não terão efeito.

Permitir a passagem de outras regras: Todas as restrições ou aplicativos, exceto as regras criadas abaixo, podem passar;

Proibir passagem fora das regras: permitir ou proibir apenas o conteúdo das regras abaixo;

Adicionar: Para adicionar regras específicas de controle de acesso, você pode criar regras para terminais, aplicativos e modos de controle

Status: se o estado da regra estiver Ligado ou não. Se o estado da regra for Ligado aqui e desligado acima, então a regra ainda está desligada;

Nome da regra: Personalize o nome da regra para distinguir entre muitas regras.

Modo de Controle: Permitir indica que o conteúdo da regra é permitido. Bloquear indica que o conteúdo da regra é bloqueado.

1) Se a parte superior estiver definida como "Permitir acesso fora das regras", selecione "Permitir" para indicar que todo o acesso passa;

2) Se "permitir passagem fora da regra" estiver definido acima, selecione "Bloquear" aqui para indicar que o conteúdo desta regra está bloqueado e o restante pode ser usado normalmente (passar);

3) Se negar a passagem fora das regras estiver definido acima, selecione Permitir para indicar que apenas o conteúdo nas regras pode passar e o restante (terminais ou protocolos de aplicação) não pode passar;

4) como acima está definido como "nenhuma regra passa", selecione "parar" aqui diz proibido todos os terminais de acesso globais e acordo, esta situação também levará a acessar a rede de todos os terminais não pode acessar à página de gerenciamento WEB do routerr (independentemente de sem fio ou com fio), portanto, é importante observar que as regras de configuração.

Prioridade de Execução: Indica a ordem de prioridade de execução entre as regras. Quanto maior o valor, mais prioridade as regras têm para serem executadas. Se as prioridades forem iguais, uma das regras é executada aleatoriamente.

Controle com Base no Tipo de Endereço do Terminal

Com Base em IP: Se a regra deve entrar em vigor para o endereço IP global do terminal, selecione Todos os endereços. Se desejar controlar o acesso a parte ou a um endereço IP, selecione Personalizado e insira um ou um segmento de endereços IP.

Com Base em Endereço MAC: criar regras de acesso com base no endereço físico do terminal MAC, terminal móvel existente com vários MAC virtuais (diferentes conexões sem fio ao mesmo equipamento podem obter MAC diferentes do terminal, o MAC é o MAC virtual), se desejar alcançar controle total de acesso a um terminal, preencha todos os MAC virtuais do terminal;

Tempo Gerenciado: especifica o período de tempo durante o qual as regras entram em vigor. As regras de controle de acesso não têm efeito fora do período de tempo especificado.

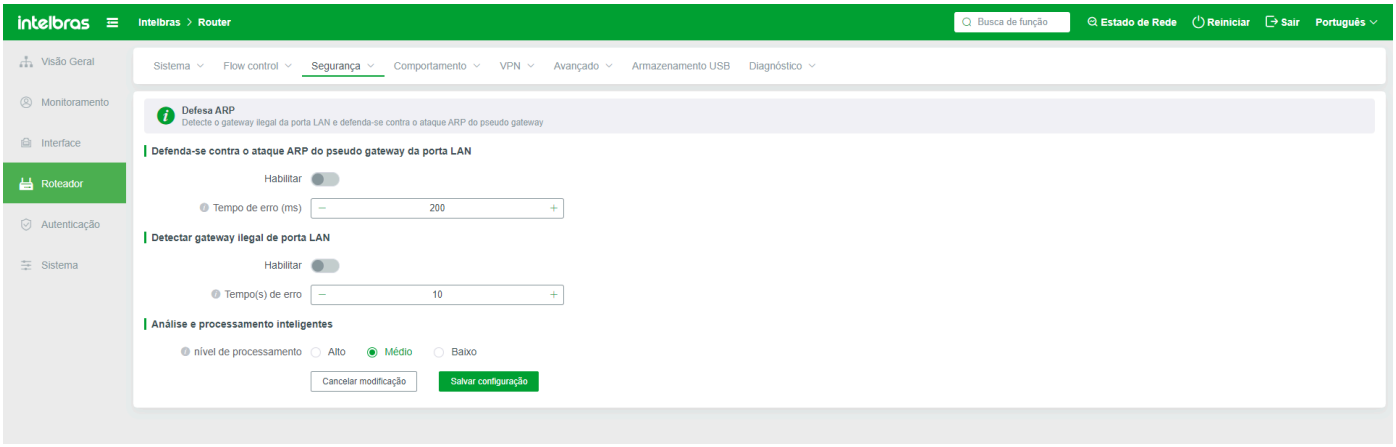
Protocolo de Aplicação: Selecione o tipo de protocolo de aplicação para controle de acesso.

Endereço IP definido pelo usuário: Você pode definir o endereço IP remoto, o nome de domínio e o protocolo de porta e usar o endereço IP remoto como objeto de gerenciamento.

Log: Ativa o registro de log das regras de controle de acesso. Quando um terminal (usuário) aciona a regra, o sistema registra e salva automaticamente os logs. Se a ferramenta de registro estiver desativada, nenhum registro será salvo.

Defesa ARP

Você pode definir regras para detectar gateways ilegítimos nas interfaces LAN e se defender contra ataques ARP em pseudo gateways.



Defender contra ataque ARP no pseudo-gateway na interface LAN: Defenda-se contra software comum de ataque ARP. Se existirem softwares de ataque ARP, como Network Warden, P2P Terminator e outros ataques de gateway de computador, eles são registrados no Log ARP. O intervalo padrão é de 200ms.

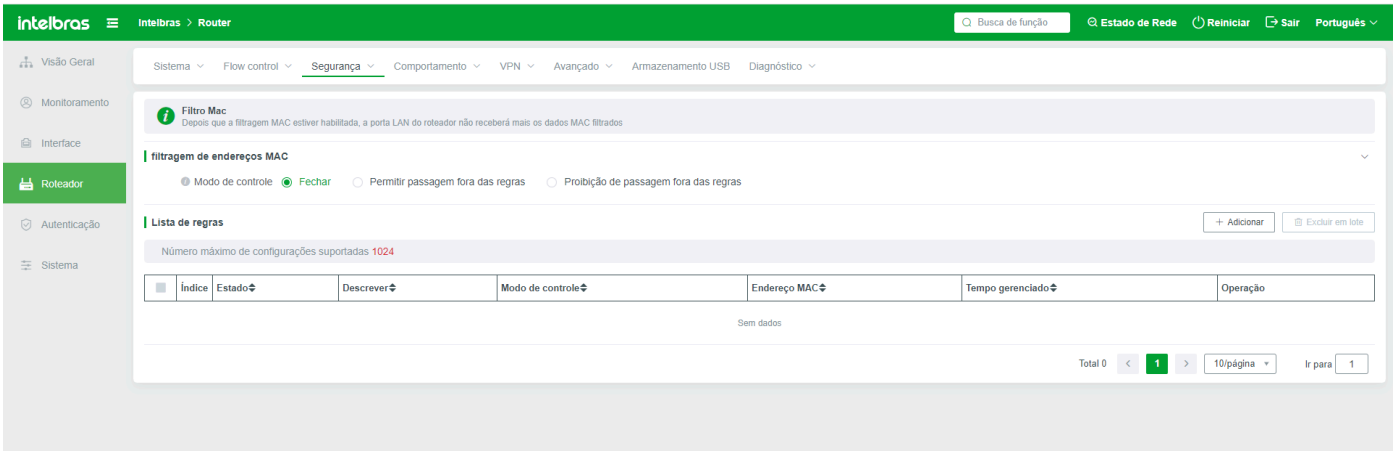
Detectar Gateway LAN ilegítimo: Verifique se algum endereço IP da Intranet é o mesmo que o da LAN do roteador. Se sim, o endereço IP é registrado no Log ARP. O tempo de detecção padrão é de 10 segundos.

Defesa ARP inteligente Indica o nível de processamento do sistema de defesa ARP inteligente. Um nível mais alto indica um nível mais seguro. Pode ser ajustado de acordo com o ambiente de rede.

Você pode visualizar os logs de defesa ARP em Gerenciamento de Sistema - Log de Sistema - Log ARP.

Filtragem de MAC

Ao ativar a filtragem de endereços MAC e definir regras de filtragem, é possível controlar o acesso à Internet do host conectado.



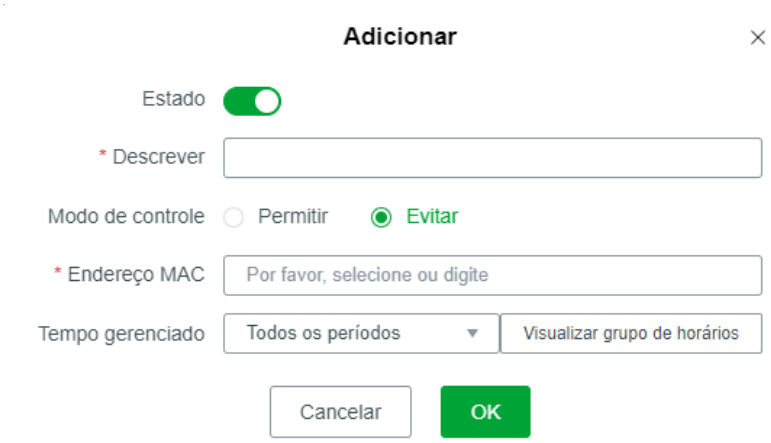
Modo de filtragem de endereço MAC: Há três opções: Não habilitar a filtragem de endereço MAC, permitir que entradas fora das regras passem e proibir que entradas fora das regras passem. Selecione as opções conforme necessário.

Desativar: Indica que a regra de filtragem está desativada. A filtragem de MAC não tem efeito, independentemente de a regra estar configurada abaixo ou se a regra for permitida ou bloqueada.

Os endereços MAC fora das regras são permitidos. As regras adicionadas são executadas de acordo com o modo de controle. Os endereços MAC fora das regras são passados diretamente sem restrições.

As regras na lista são implementadas de acordo com o modo de controle. Todos os endereços MAC fora da lista são bloqueados.

Adicionar: Adiciona regras de filtragem de endereço MAC



Status: Seleciona se deseja habilitar a regra.

Descrição: Uma breve descrição desta regra. O valor padrão é "default". Recomenda-se alterar o valor para algo fácil de identificar.

Modo de Controle: Dividido em 'permitir' e 'prevenir'. Os usuários podem escolher se permitem que esta regra passe.

Endereço MAC: Insira o endereço MAC a ser gerenciado. O formato é: 00:0A:0B:0C:0D:0E.

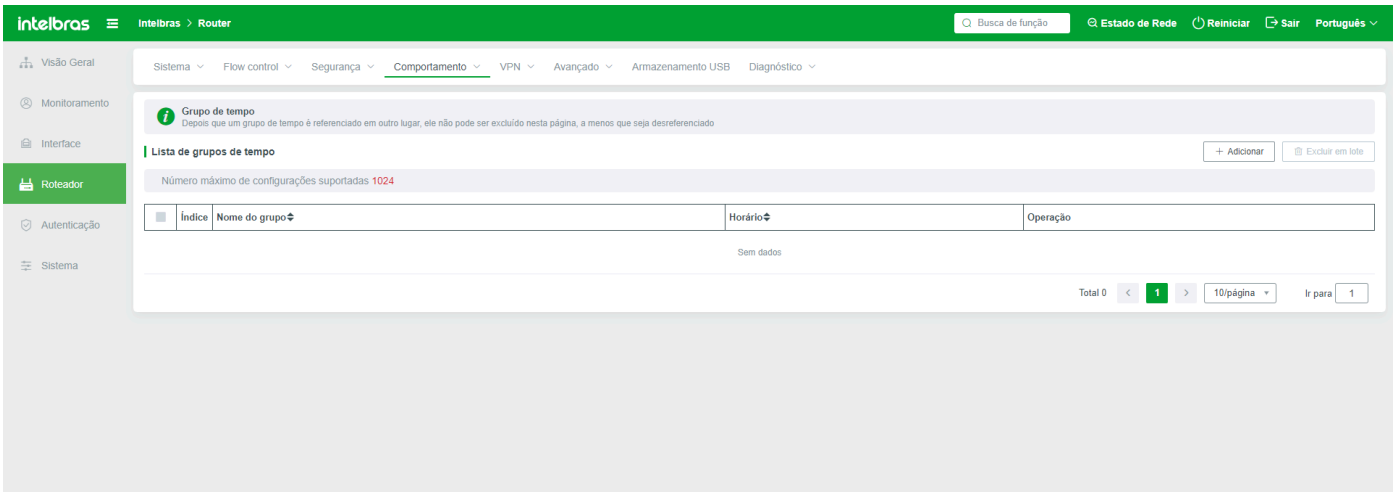
Intervalo de tempo gerenciado: A filtragem de endereço MAC é habilitada no intervalo de tempo especificado. Por padrão, todos os intervalos de tempo têm efeito. Para usar um intervalo de tempo específico, é possível selecionar um intervalo de tempo definido pelo usuário.

Comportamento

Grupo de tempo

É possível criar um grupo de tempo conforme necessário. Se precisar selecionar um tempo para criar uma regra de comportamento ou controle de fluxo, é possível selecionar diretamente o grupo de tempo.

Um grupo de tempo que foi referenciado em outro lugar não pode ser excluído desta página, a menos que seja desreferenciado.



Adicionar: Adiciona grupos de tempo conforme necessário

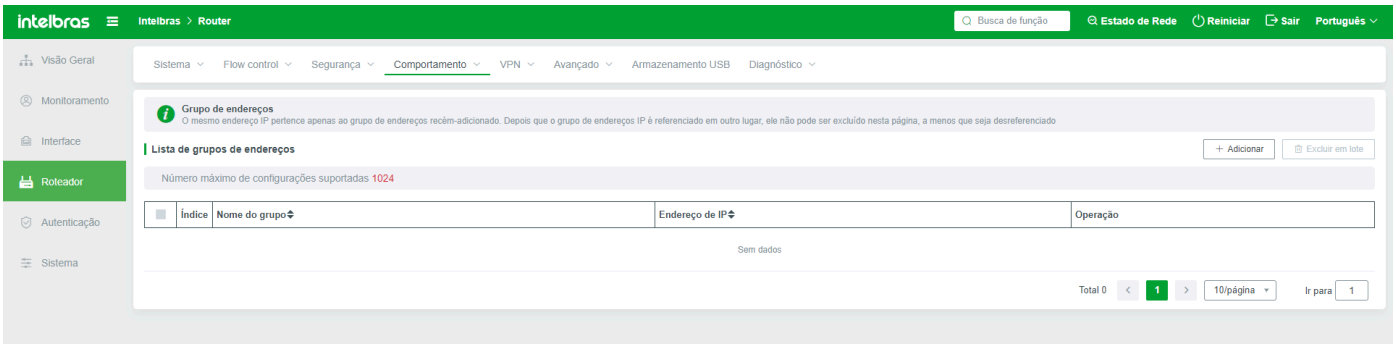
Nome do grupo: especifica o nome de um grupo de tempo definido pelo usuário.

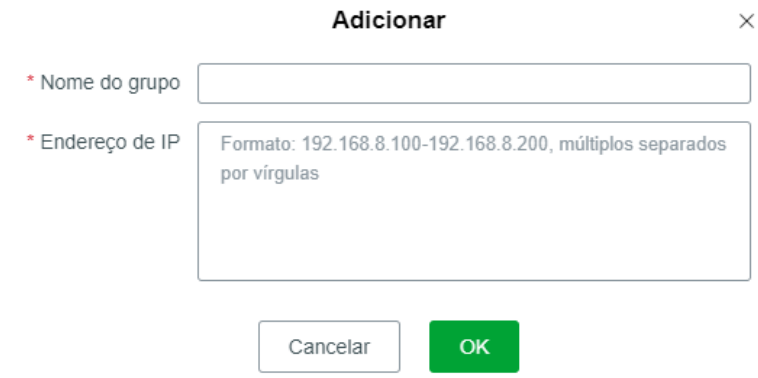
Tempo semanal: Seleciona um tempo semanal. Este parâmetro é obrigatório. Se "todos" for selecionado, todas as semanas são escolhidas. Se não for selecionado, as semanas não escolhidas são selecionadas junto com as escolhidas.

Agenda diária: Configura a agenda diária. Seleciona o horário de início e término, sendo que o horário de início não pode ser posterior ao horário de término. Se houver vários períodos, clique no sinal de mais para adicioná-los.

Excluir em lote: Se vários grupos de tempo precisarem ser excluídos, selecione-os e clique em Excluir em Lote. No entanto, o grupo de tempo referenciado não pode ser excluído.

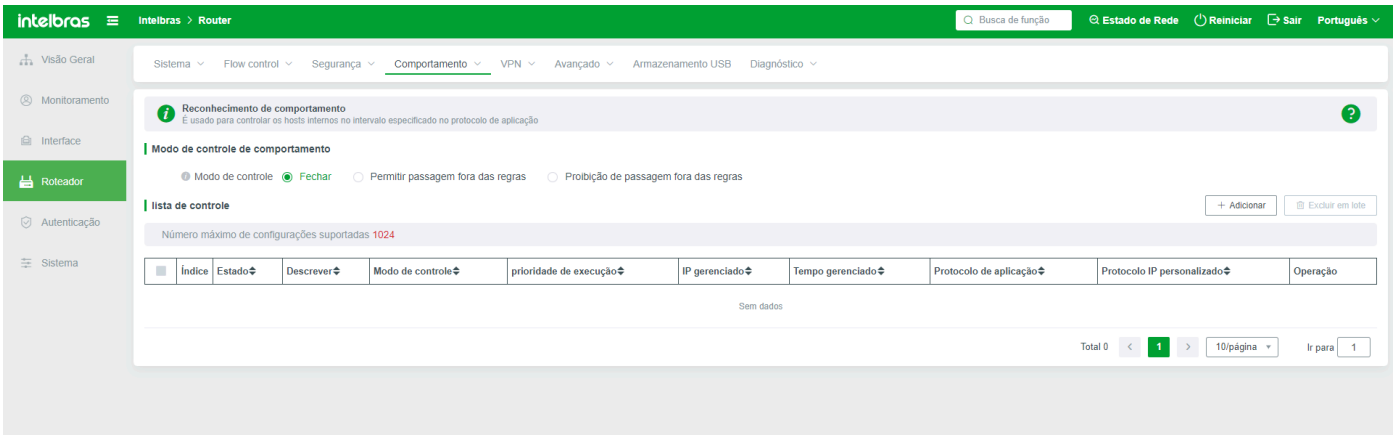
Grupo de endereços





Reconhecimento de Comportamento

Controla se o terminal pode acessar a Internet ou apenas os protocolos de aplicativos.



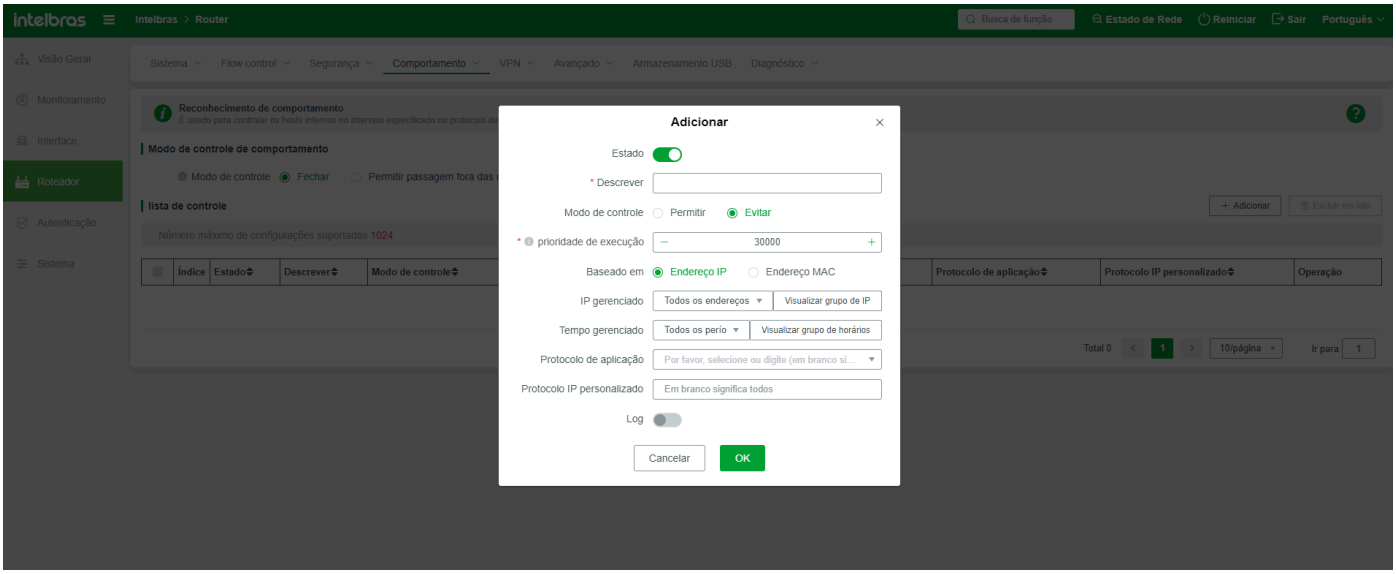
Modo de controle de comportamento: há três estados: fechamento, permitindo a passagem fora das regras e proibindo a passagem fora das regras

Desativar: Se selecionar Desativar, todas as regras criadas abaixo não terão efeito.

Permitir que outras regras passem: Todas as restrições ou aplicativos, exceto as regras criadas abaixo, podem passar;

Proibir passagem fora das regras: permite ou proíbe apenas o conteúdo das regras abaixo;

Adicionar: Para adicionar regras específicas de controle de acesso, é possível criar regras para terminais, aplicativos e modos de controle



Status: se o estado da regra está ligado ou não. Se o estado da regra estiver ligado aqui e desligado acima, a regra ainda estará desligada;

Nome da regra: Personaliza o nome da regra para distinguir entre muitas regras.

Modo de controle: Permitir indica que o conteúdo da regra é permitido. Bloquear indica que o conteúdo da regra é bloqueado.

1) Se a parte superior estiver definida como "Permitir acesso fora das regras", selecione "Permitir" para indicar que todo o acesso é permitido;

2) Se "permitir passar fora da regra" estiver definido acima, selecione "Bloquear" aqui para indicar que o conteúdo desta regra está bloqueado e o restante pode ser usado normalmente (passar);

3) Se negar a passagem fora das regras estiver definido acima, selecione Permitir para indicar que apenas o conteúdo nas regras pode passar e o restante (terminais ou protocolos de aplicativos) não pode passar;

4) Como acima está definido como "sem regras através", selecione "parar" aqui para proibir todos os terminais e acordos de acesso globais, essa situação também levará a todos os terminais não poderem acessar a página de gerenciamento WEB do roteador (independentemente de ser sem fio ou com fio), portanto, é importante observar que a configuração de regras.

Prioridade de execução: Indica a ordem de prioridade de execução entre as regras. Quanto maior o valor, mais prioridade as regras têm. Se as prioridades forem iguais, uma das regras será executada aleatoriamente.

Controle com base no tipo de endereço do terminal

Com base no IP: Se a regra deve ter efeito para o endereço IP global do terminal, selecione Todos os endereços. Se desejar controlar o acesso a parte ou a um endereço IP, selecione Personalizado e insira um ou um segmento de endereços IP.

Com base no endereço MAC: cria regras de acesso com base no endereço físico do terminal MAC, terminal móvel existente possui vários MAC virtuais (conexões sem fio diferentes do mesmo equipamento podem obter MAC diferentes do terminal, o MAC é o MAC virtual), se desejar alcançar controle total de acesso a um terminal, preencha todos os MAC virtuais do terminal;

Tempo gerenciado: especifica o período durante o qual as regras têm efeito. As regras de controle de acesso não têm efeito fora do período de tempo especificado.

Protocolo de Aplicação: Seleciona o tipo de protocolo de aplicação para controle de acesso.

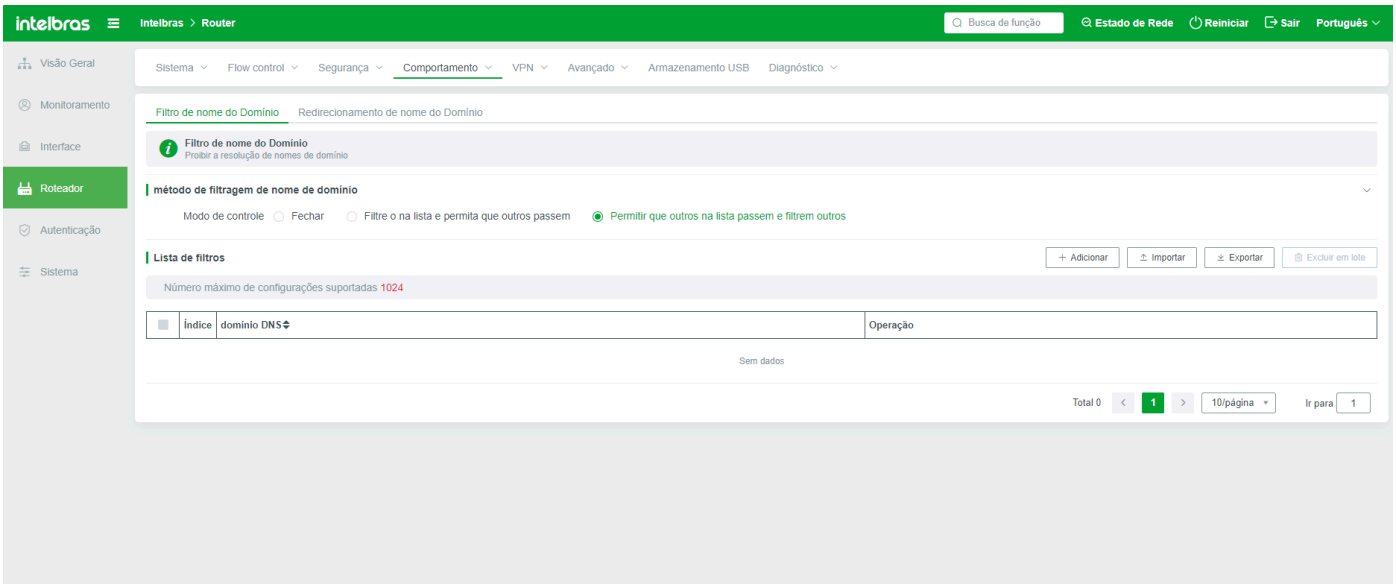
Endereço IP definido pelo usuário: É possível definir o endereço IP remoto, nome de domínio e protocolo de porta e usar o endereço IP remoto como objeto de gerenciamento.

Log: Ativa o registro de logs das regras de controle de acesso. Quando um terminal (usuário) aciona a regra, o sistema registra e salva automaticamente os logs. Se a ferramenta de log estiver desativada, nenhum registro será salvo.

Nome de domínio

Filtragem de nome de domínio

Se definir se adicionar resolução de filtragem de nome de domínio, o nome de domínio bloqueado não pode ser resolvido com sucesso.



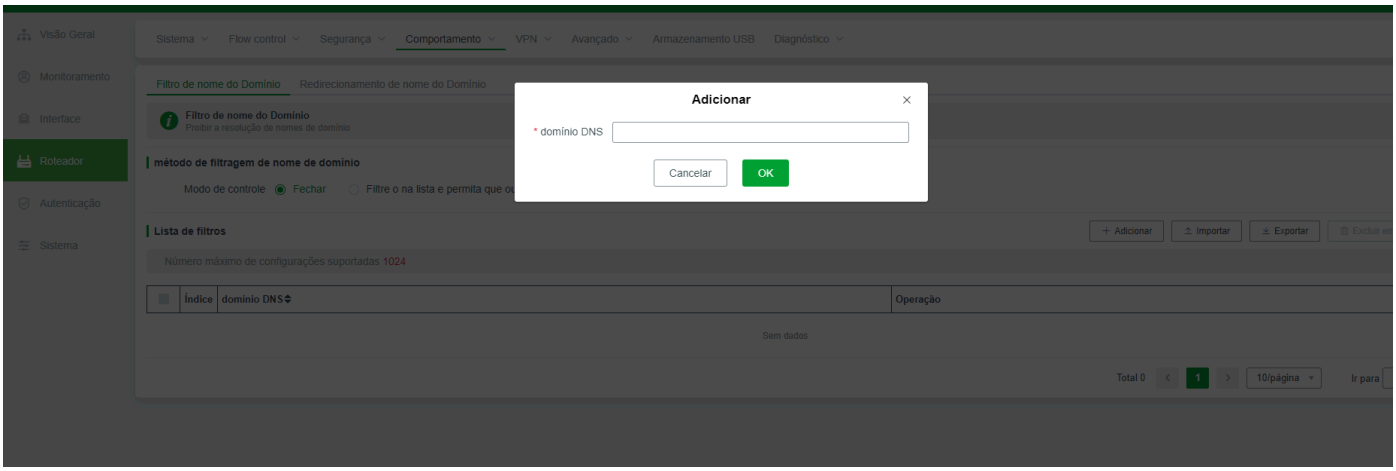
Modo de filtragem de nome de domínio: Desativar, permitir que outros passem e filtrar outros da lista de permissões

Desativar: Se selecionar Desativar, todos os nomes de domínio adicionados abaixo não terão efeito.

Na lista de filtragem, outros domínios podem passar: Todos os nomes de domínio podem ser resolvidos, exceto o nome de domínio adicionado abaixo.

Na lista de permissões, filtrar outros nomes de domínio: Apenas os nomes de domínio adicionados abaixo podem ser resolvidos. Outros nomes de domínio não podem ser resolvidos. Atenção a esta regra de configuração para evitar falhas globais na rede.

Adicionar: Adiciona nomes de domínio que precisam ser gerenciados e resolvidos, como mostrado na figura abaixo:



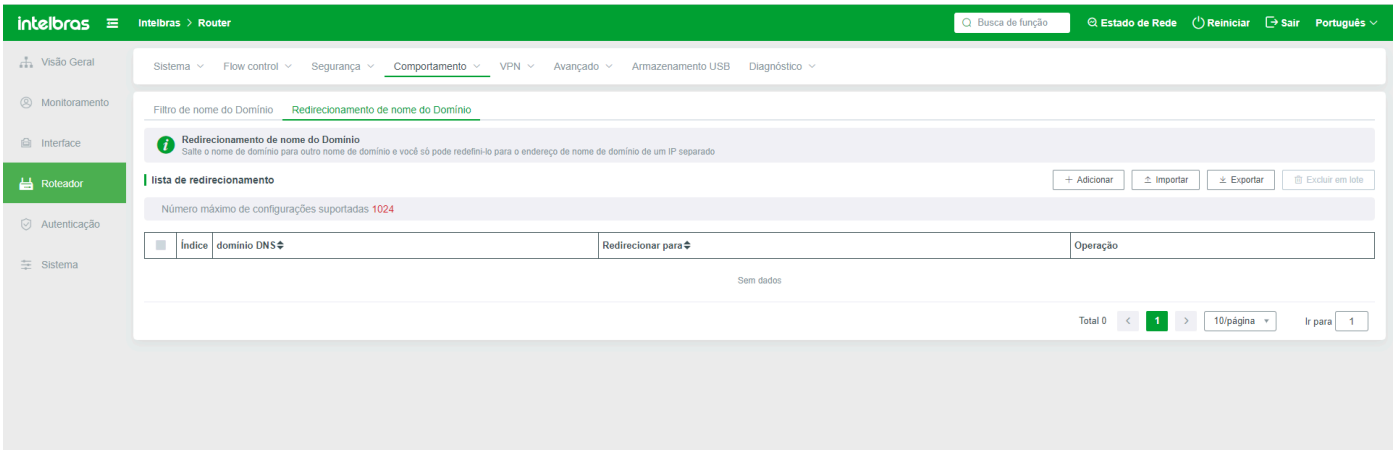
1) Se selecionar Desligar, a resolução de qualquer nome de domínio adicionado abaixo não será bloqueada e o nome de domínio poderá ser acessado e usado normalmente.

2) Se selecionar Permitir que outros passem na lista de filtros, o nome de domínio adicionado não será resolvido (não pode ser acessado), mas o nome de domínio fora da regra pode ser resolvido. Na figura anterior, o nome de domínio é baidu.com. O terminal não consegue acessar o nome de domínio.

Se o acima selecionar "permitir a lista, filtrar os outros", apenas a lista de nomes de domínio pode ser resolvida e acessada, não na lista de nomes de domínio não conseguirá acessar, como o preenchimento acima do baidu.com terminal pode ser normalmente acessado, mas os outros nomes de domínio falharão ao acessar, então visitar qq.com falhará ao acessar.

Redirecionamento de Nome de Domínio

Mesmo se um site http for redirecionado para outro site http, o redirecionamento de nome de domínio não suporta sites https.

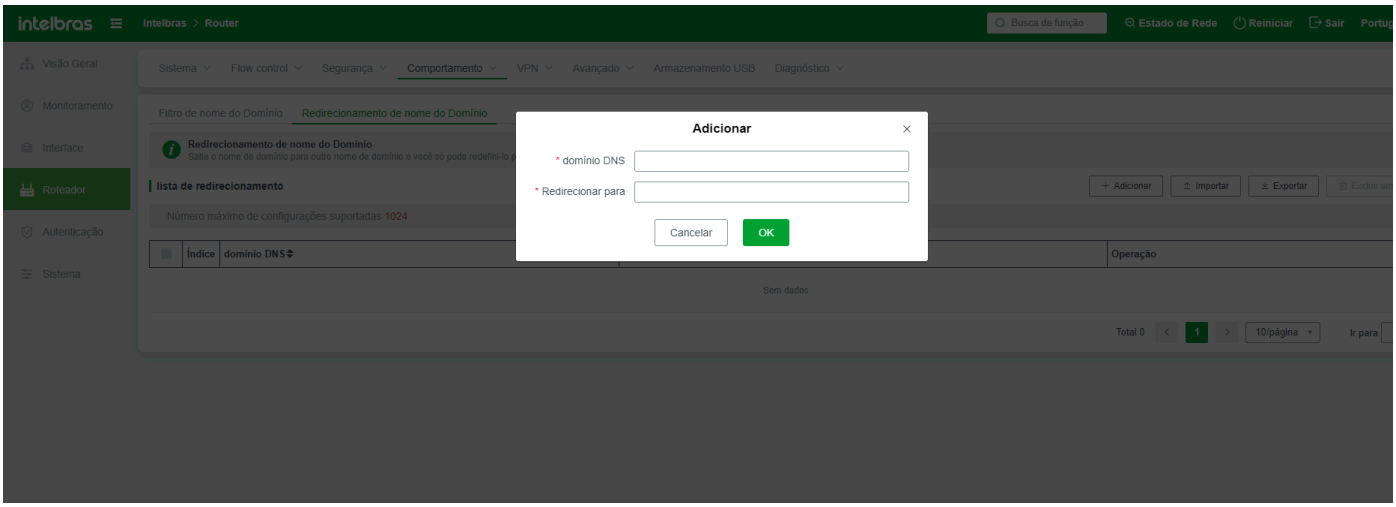


Adicionar regras de redirecionamento conforme necessário

Domínio DNS: Insira o nome de domínio a ser redirecionado. O nome de domínio deve seguir o nome de domínio padrão e deve ser um nome de domínio real de site http.

Redirecionar para: ou seja, será redirecionado para um novo site http.

Por exemplo, redirecione o site www.cac.gov.cn para www.youth.cn, como mostrado abaixo:



O acesso ao endereço é www.qstheory.cn, mas a página da web na verdade salta para www.youth.cn; **Importar:** Redireciona regras com base no formato da regra. Se não souber o formato da regra, é possível adicionar uma regra de redirecionamento primeiro e, em seguida, adicionar ou modificar o conteúdo no arquivo original. (Garanta que o formato do arquivo original seja seguido; caso contrário, a importação da regra falhará.) **Exportar:** É possível exportar regras de redirecionamento criadas. Se nenhuma regra for adicionada, o arquivo exportado estará vazio.

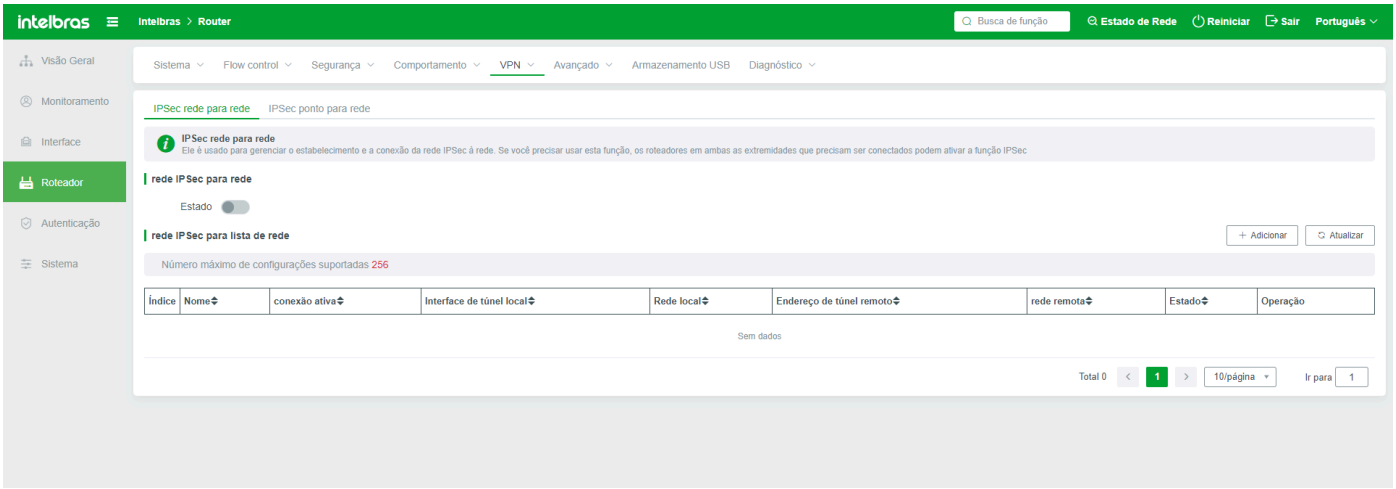
VPN

Configurações IPSec

IPSec de Rede para Rede

Esta função é usada para gerenciar o estabelecimento e a conexão da rede IPSec para a rede. Para usar esta função, certifique-se de que a função IPSec está ativada em ambos os roteadores a serem conectados.

Normalmente, a rede para rede é usada em cenários com alta confiança entre as duas partes, possibilitando o acesso a recursos da intranet.



Configuração IPSec de Rede para Rede (interruptor): Selecione para ativar a rede para rede.

Adicionar uma regra de par de rede IPSec: Adicione uma regra de par de rede ipsec conforme necessário

Nome: Nome de par de rede definido pelo usuário. O valor contém de 1 a 31 letras, dígitos e sublinhados -! @ # $% ^ & * ();

Conexão ativa IPSec NT-para-rede: Após a ativação da conexão ativa IPSec NT-para-rede, o dispositivo inicia ativamente uma solicitação de conexão para se conectar ao dispositivo remoto. Se o final local desativar a conexão ativa NT-para-rede, o dispositivo não se conectará ativamente ao dispositivo remoto. Em vez disso, ele aguarda o dispositivo remoto iniciar uma solicitação de conexão (desde que a conexão ativa esteja ativada no final remoto). Se ambas as partes não selecionarem a conexão ativa, ambas as partes não iniciarão uma solicitação de conexão e só poderão clicar manualmente em "Conectar".

Manter conectado: Se este parâmetro for selecionado, pingue a intranet remota.

Interface de túnel local: Indica qual interface WAN é usada para estabelecer a rede para rede. Se WAN1 for selecionado, o endereço IP do WAN1 local deve ser inserido em Endereço de Túnel Remoto no final remoto (o modo de discagem não é suportado).

Modo: Selecione o modo principal e o modo agressivo conforme necessário. A diferença entre os dois modos é que o modo principal criptografa o ID de identidade, enquanto o modo agressivo não. Outros modos de configuração (o processo é basicamente o mesmo).

Rede local: Indica o endereço da segmentação de rede da intranet local. Por exemplo, se o endereço da intranet local for 192.168.1.1, o formato é 192.168.1.0.

Máscara de sub-rede: O valor padrão é 255.255.255.0. É possível alterar o tamanho da máscara conforme necessário.

Tipo de ID local: O valor padrão é NENHUM. Se NENHUM, não é necessário inserir um ID. Se o ID local tiver outros tipos, selecione FQDN ou USER_FQDN conforme necessário e insira o ID local na caixa abaixo:

Tipo de endereço de túnel remoto: Indica o tipo de conexão de rede externa do dispositivo remoto. O valor pode ser estático ou dinâmico (o tipo de discagem não é suportado ou é possível solicitar um endereço IP público do provedor). São recomendados endereços IP estáticos.

Endereço de túnel remoto: Especifica o endereço IP externo do dispositivo remoto. Recomenda-se que o endereço IP seja um endereço IP público estático. Se uma rede para rede for criada entre uma intranet e uma intranet, insira os endereços IP públicos dos dois dispositivos.

Rede remota: Indica o endereço IP da intranet do dispositivo remoto. Se o dispositivo remoto for 192.168.8.1, defina este parâmetro como 192.168.8.0.

Máscara de sub-rede: O valor padrão é 255.255.255.0 e pode ser alterado conforme necessário.

Tipo de ID remoto: O valor padrão é NENHUM. NENHUM não requer um ID. Se o ID remoto tiver outros tipos, selecione FQDN ou USER_FQDN conforme necessário e insira o ID remoto na caixa abaixo.

Modo de autenticação IKE: O tipo de autenticação padrão é IKE-PSK.

Chave PSK: Defina a chave de autenticação. A autenticação é bem-sucedida apenas quando as chaves em ambas as extremidades são iguais. Caso contrário, a autenticação falha e a rede para rede não é criada.

Nas Configurações avançadas, as Configurações padrão são usadas. Se o dispositivo remoto não for do mesmo sistema de armazenamento, o tipo de criptografia é AES128.

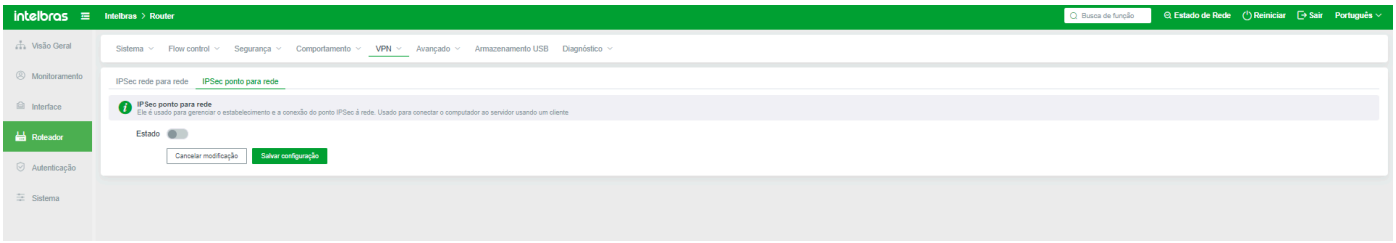
Se nenhuma rede for criada, as regras de rede são exibidas em uma lista. É possível modificar, conectar e excluir as regras na lista.

Se a rede para rede estiver conectada, ela também será exibida como "Conectada" na lista, e o botão na barra de operações mudará para "Modificar, Reiniciar, Desconectar", como mostrado abaixo:

Rede IPSec de Ponto a Ponto

É usado para gerenciar o estabelecimento e a conexão de redes IPSec P2P. Usado para computadores usarem clientes para se conectarem ao servidor. Ou seja, depois que esta função é ativada, o sistema se torna o servidor IPSec P2P.

Serviço IPSec P2P (status): indica se habilitar ou desabilitar o serviço P2P. É possível definir parâmetros de regra somente após o status estar habilitado.



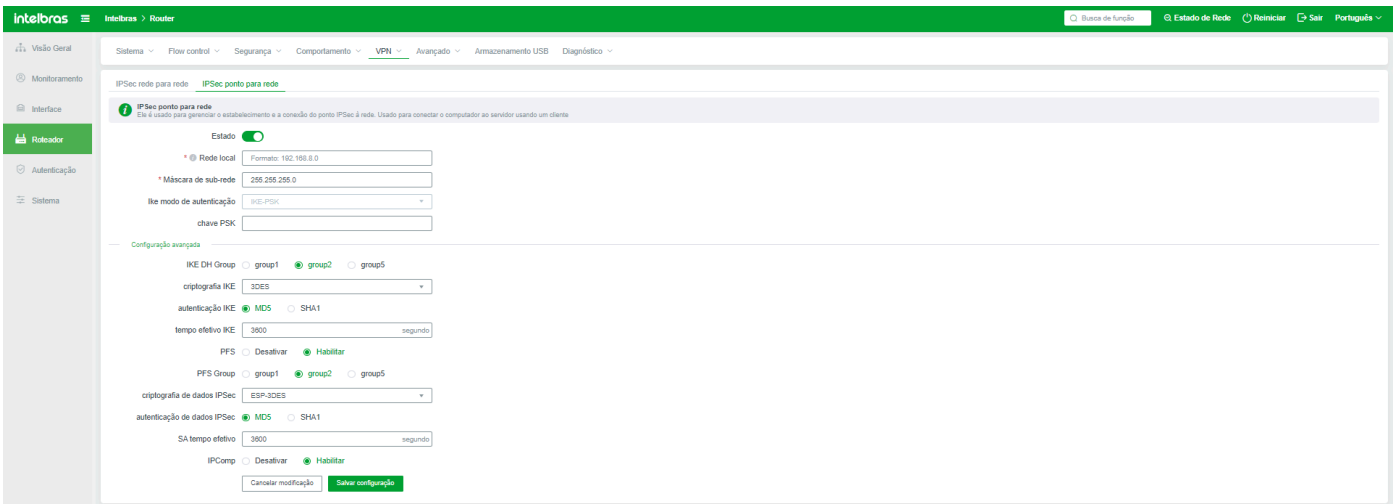
Rede local: indica o endereço da intranet local (servidor). Por exemplo, se o endereço da intranet local for 192.168.1.1, defina este parâmetro como 192.168.1.0.

Máscara de sub-rede: O valor padrão é 255.255.25.0. Altere o segmento da máscara conforme necessário.

Modo de autenticação IKE: Este item não é opcional. Apenas o modo de autenticação IKE-PSK está disponível.

Chave PSK: Defina a chave por conta própria. Quando o cliente se conecta ao servidor, a chave deve ser preenchida corretamente; caso contrário, a conexão falha.

Configurações avançadas: Os parâmetros neste parâmetro não são modificados. No entanto, é necessário defini-los conforme necessário ao se conectar ao cliente para evitar falhas de conexão.

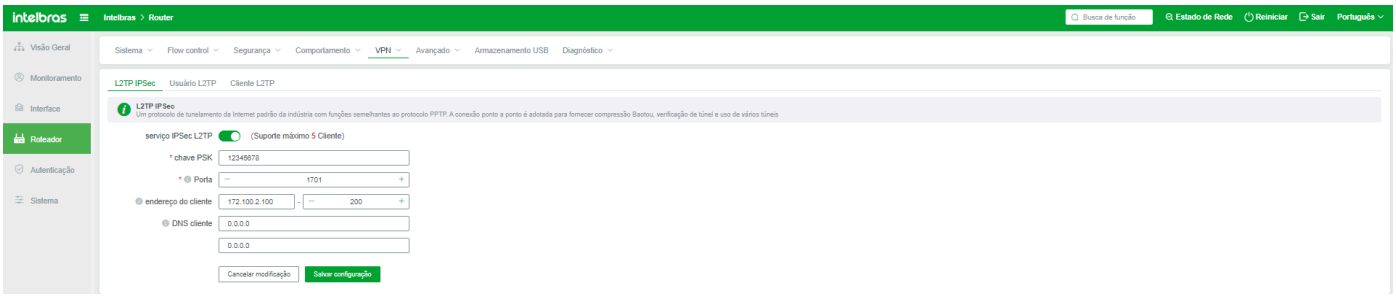


Aviso: É necessário um software de conexão VPN para conexão Client IPsec no computador que for se conectar ao Servidor VPN

L2TP IPSEC

L2TP IPSec

A função L2TP IPSec é semelhante à função de conexão PPTP. Ela adota a conexão ponto a ponto e fornece compressão de cabeçalho de pacote, autenticação de túnel e vários túneis. Neste exemplo, o servidor L2TP IPSec está configurado.



Serviço L2TP IPSec: Ativar ou desativar o serviço L2TP IPSec. Os parâmetros do servidor podem ser configurados somente após o serviço L2TP IPSec ser ativado.

Chave PSK: Definir chave PSK.

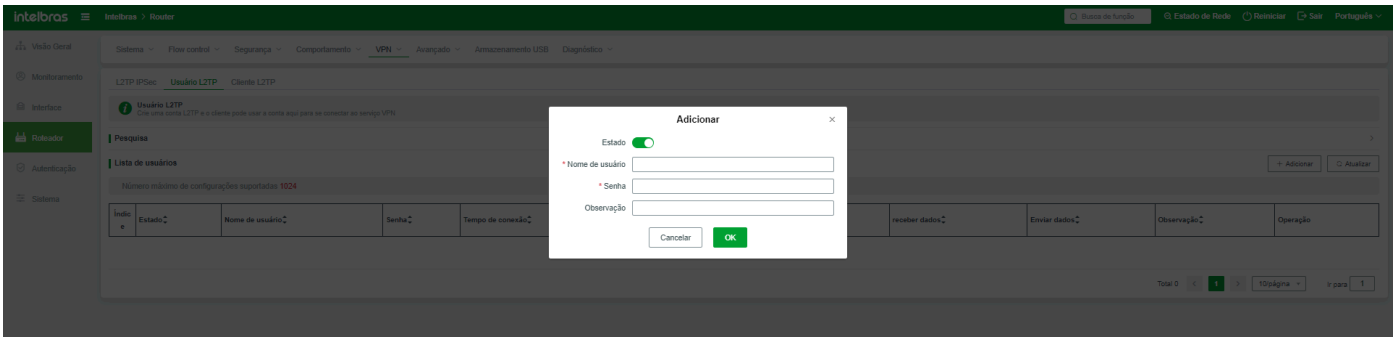
Porta: A porta padrão do L2TP IPSec é 1701.

Endereço do cliente: Indica o intervalo da piscina de endereços DHCP atribuído pelo servidor ao cliente. Este endereço IP é o endereço IP virtual para se conectar ao L2TP. Não defina este endereço IP no mesmo segmento de rede que outros endereços IP do roteador. Caso contrário, pode ocorrer conflito de IP e falhas de rede.

DNS do cliente: Especifica o endereço DNS atribuído ao cliente. É recomendável inserir o endereço DNS local.

Usuário L2TP

O cliente precisa de uma conta e senha para se conectar ao servidor. Neste caso, você pode criar uma conta de usuário. Uma conta L2TP pode ser usada pelo cliente para se conectar ao serviço VPN.



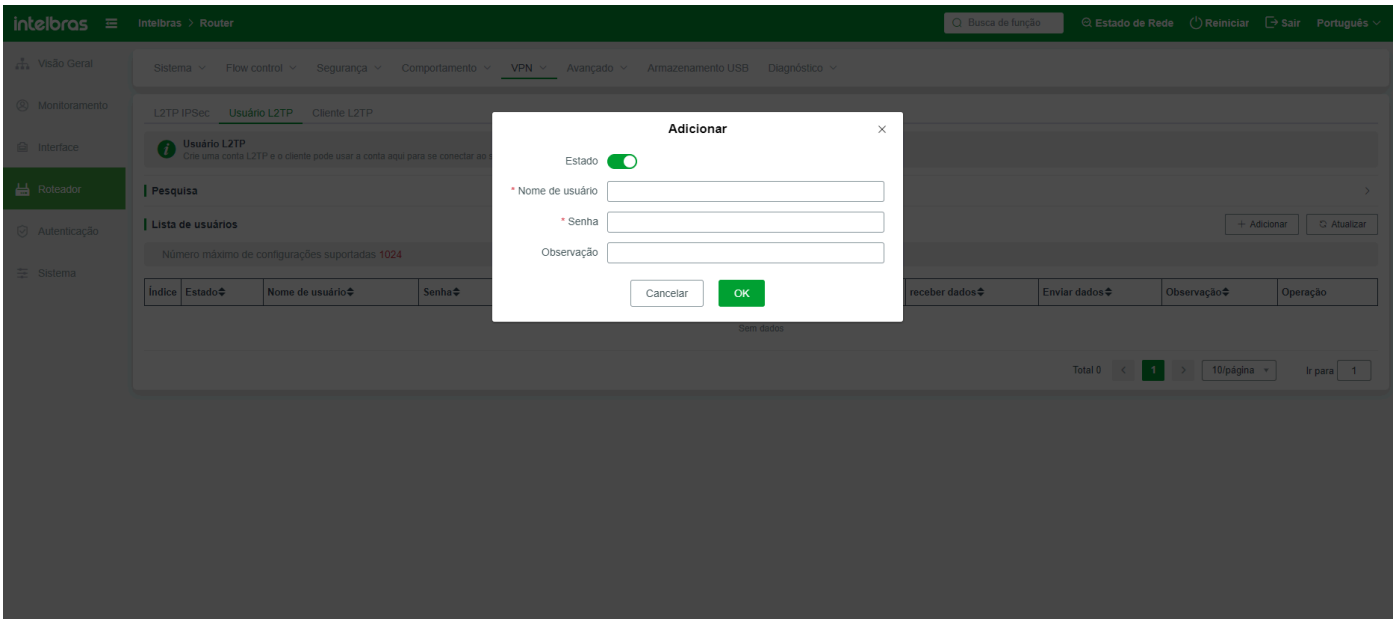
Adicionar: Adiciona uma conta L2TP

Status do usuário: Ativar ou desativar o status da conta de usuário. A conta desativada não pode ser usada normalmente.

Nome do usuário: Define a conta de usuário.

Senha: Define a senha de conexão do usuário.

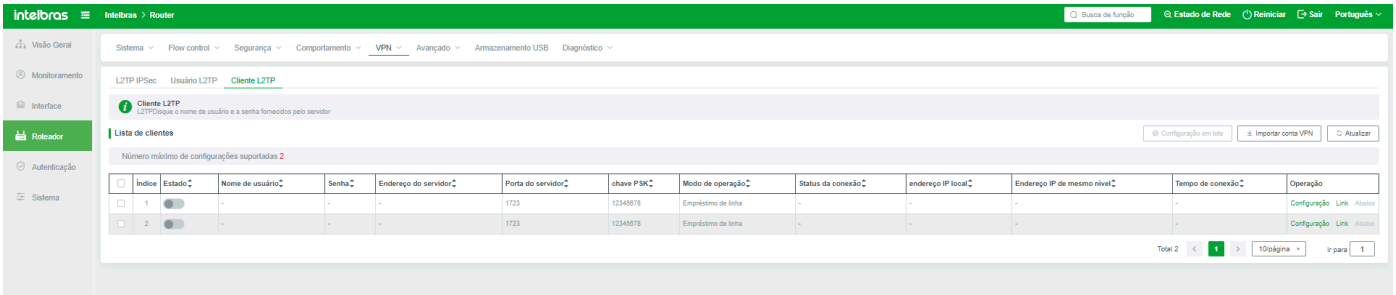
Observação: Selecione um item para definir as observações.



Após a conta ser adicionada, ela é exibida em uma lista. Você pode modificar ou excluir a conta. A lista também exibe o status de conexão e a recepção de dados da conta atual.

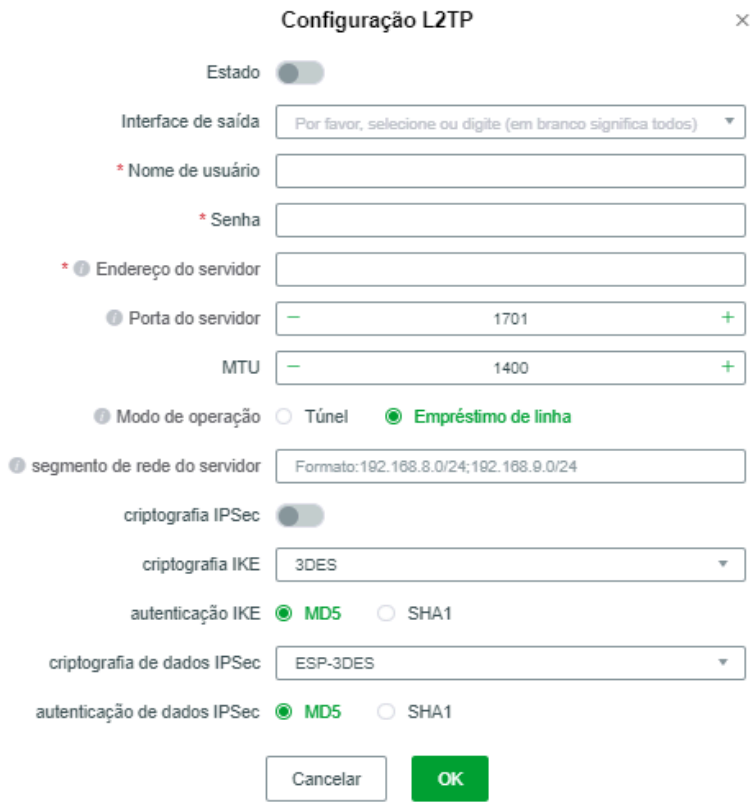
Clientes L2TP

Quando a conta fornecida pelo servidor L2TP é usada para conexão, observe que o cliente no sistema local não pode usar a conta definida no servidor local. O número máximo de clientes suportados depende do modelo do dispositivo. Neste exemplo, o modelo de cliente L2TP suporta apenas um cliente L2TP.



A lista de clientes exibe a conexão da conta L2TP. Observe que a conta de cliente L2TP é compartilhada pela conta de cliente PPTP. Na barra de operações da lista, você pode editar, conectar e desconectar contas.

Editar: Edita contas e parâmetros de regra.



Status: Indica que a conta está em uso. Quando a conta é desativada, a conta não pode ser usada.

Interface de saída: Indica a interface WAN pela qual o cliente L2TP sai. Certifique-se de que a interface WAN está disponível.

Nome de usuário: Indica a conta de usuário.

Senha do usuário: Indica a senha do usuário L2TP.

Endereço do servidor: Insira o endereço IP público do servidor L2TP.

Porta do servidor: Indica a porta no servidor L2TP. O número da porta padrão é 1701. É necessário verificar o número da porta no servidor real e, em seguida, alterar o número da porta.

Configurações MTU: O valor padrão é 1400.

Modo de funcionamento: Selecione o modo de cliente L2TP, modo de túnel e modo de empréstimo

No modo de túnel: os roteadores são usados apenas como conexões VPN. Eles podem compartilhar os recursos internos do segmento de rede virtual, mas não podem acessar os recursos externos do servidor (ou seja, a função de empréstimo de linha não pode ser usada).

Segmento de rede do servidor: Este parâmetro só entra em vigor quando o modo de túnel é selecionado. Insira o segmento de rede interno do servidor (por exemplo, se o endereço IP interno do servidor for 192.168.2.1, insira 192.168.2.0/24). O segmento de rede da intranet do servidor não pode ser o mesmo que o segmento de rede local. Se sim, modifique o segmento de rede local ou o segmento de rede do servidor.

Encriptação IPSEC: Se a encriptação estiver habilitada no servidor e a chave estiver definida, você também deve habilitar a encriptação IPSEC e inserir a senha definida no servidor.

Chave PSK: Insira a chave definida no servidor.

Encriptação IKE: Indica o modo de encriptação. Nossos dispositivos usam 3DES por padrão.

Autenticação IKE: O sistema usa MD5 por padrão. Se o servidor usar SHA1, selecione SHA1.

Encriptação de dados IPSEC: O sistema usa encriptação ESP-3DE5 por padrão. Se precisar modificar os dados IPSEC, confirme a modificação.

Autenticação de dados IPSEC: O sistema padrão é MD5. Se precisar modificar os dados IPSEC, confirme a modificação.

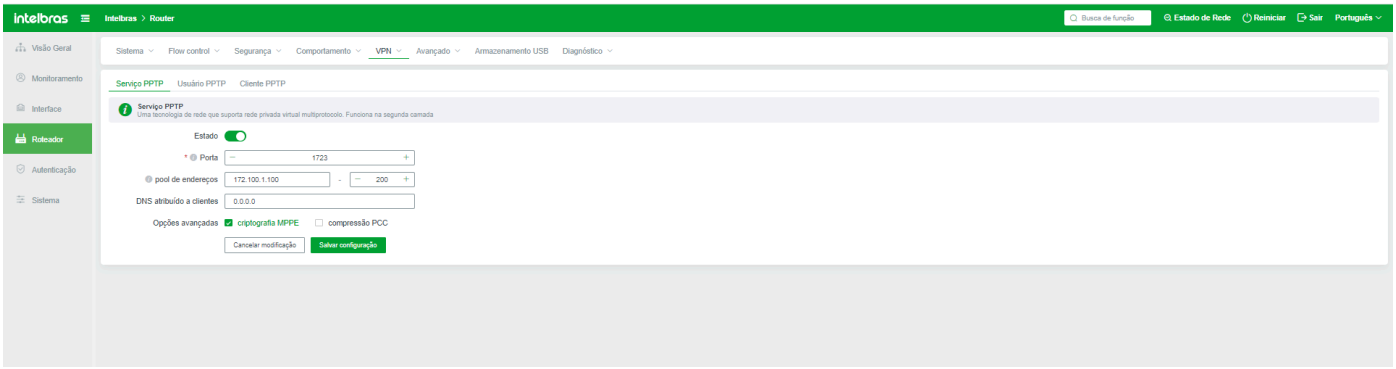
No modo de empréstimo de linha, o cliente do roteador pode usar a rede do servidor para acessar recursos externos, mas não pode acessar recursos internos do servidor.

Importar contas VPN: Se o dispositivo suportar vários clientes L2TP e for necessário importar várias contas L2TP, é possível importar contas VPN em lote. Todas as contas importadas em lote estão no modo de empréstimo de linha.

PPTP

Serviço PPTP

Este comando é usado para configurar o status e os parâmetros do servidor PPTP. Você pode definir parâmetros relacionados somente quando o servidor PPTP estiver habilitado.



Porta: A porta padrão do servidor PPTP é 1723. O sistema geralmente tem configurações fixas para cada porta da VPN e geralmente não as modifica. Se precisar modificá-la, confirme se a porta modificada entra em conflito.

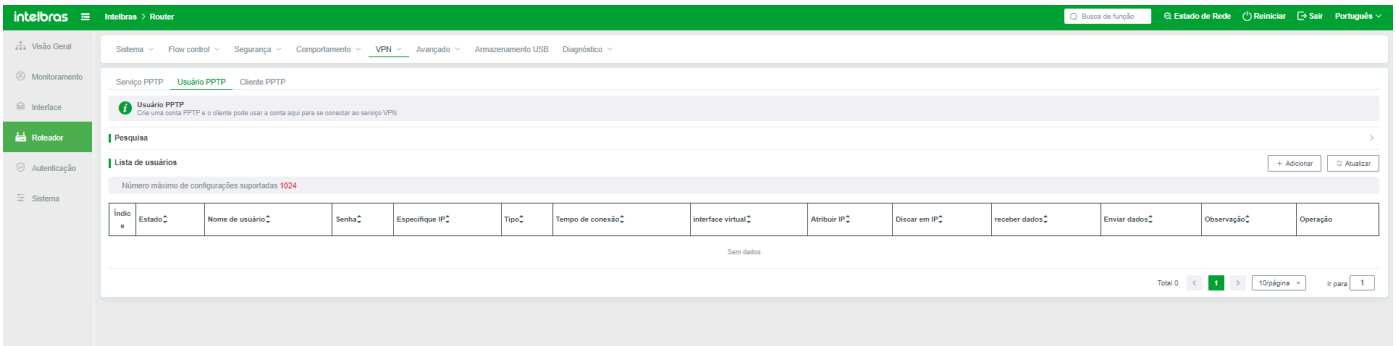
Piscina de endereços: Indica o intervalo disponível de endereços IP atribuídos aos clientes. Insira o endereço IP inicial na primeira caixa e o endereço IP final na segunda caixa, por exemplo, 10.10.10.100-200.

DNS atribuído ao cliente: Especifica o endereço DNS atribuído ao cliente. É recomendável inserir o endereço DNS local.

Opções avançadas: Selecione se suporta a criptografia MPPE e a compressão CCP. Se este parâmetro estiver selecionado, você também deve selecionar o modo de criptografia correspondente durante a configuração do cliente.

Usuário PPTP

Após a criação de uma conta de usuário PPTP e a conexão bem-sucedida, o status de conexão, o tempo e o status de envio e recebimento de dados da conta de usuário PPTP são exibidos na lista.



Adicionar: Adicionar contas de usuário PPTP. Modelos diferentes suportam números diferentes de usuários PPTP, e modelos diferentes suportam números diferentes de usuários PPTP.

Status do usuário: Depois de ativado, a conta pode ser usada normalmente, mas depois de desativado, a conta não pode ser usada (falha na discagem).

Nome de usuário: Especifica a conta de usuário. O valor contém de 1 a 31 letras, dígitos e underscores -! @ # $% ^ & * ();

Senha: Senha de discagem PPTP, a regra limita-se a 4-31 caracteres;

Especificar endereço IP: Especifica um endereço IP privado para a conta. Este endereço IP não pode entrar em conflito com o endereço IP interno do cliente ou servidor. Após a especificação de um endereço IP, somente a conta pode usar este endereço IP e este endereço IP não será atribuído a outras contas. Se o endereço IP especificado for nulo, o cliente começa de 172.100.1.101 por padrão.

Tipo: Selecione o tipo de conta PPTP

A conexão do túnel VPN conecta duas LANs para formar uma LAN virtual, que é usada principalmente para acesso compartilhado à LAN.

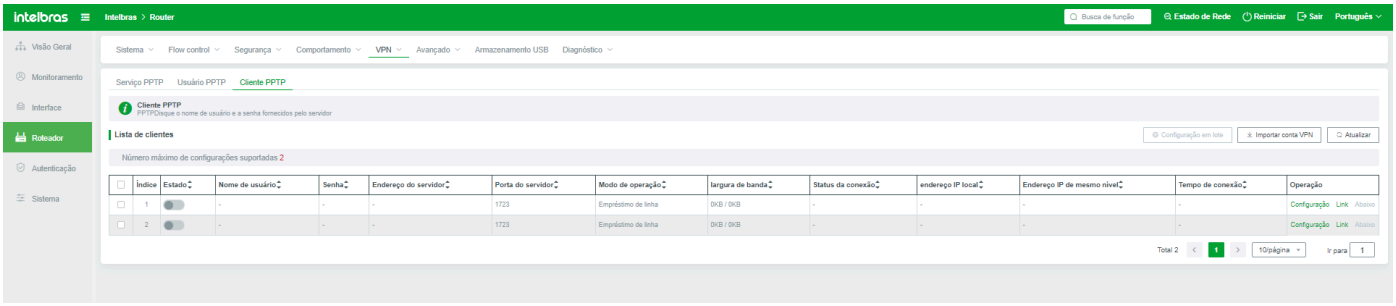
Empréstimo de VPN: O cliente acessa a Internet através da linha de rede externa do servidor, que pode ser entendida como um proxy IP. O cliente pode usar o empréstimo de linha como uma regra de roteamento de política para rotear os dados necessários através do caminho de empréstimo de VPN.

Segmento de rede interno do cliente: No modo de túnel VPN, insira o endereço IP do segmento de rede interno do cliente. Por exemplo, se o endereço IP interno do cliente for 192.168.2.1, insira 192.168.2.0/24. Não é necessário preencher no modo de empréstimo;

Nota: Observações definidas pelo usuário.

Cliente PPTP

Quando o cliente local precisa se conectar ao servidor, use a conta e a senha fornecidas pelo servidor para se conectar. A conta no cliente PPTP é a mesma do cliente L2TP. Portanto, se uma conta editada for adicionada no cliente L2TP, a mesma conta existirá na lista de discagem do cliente PPTP.

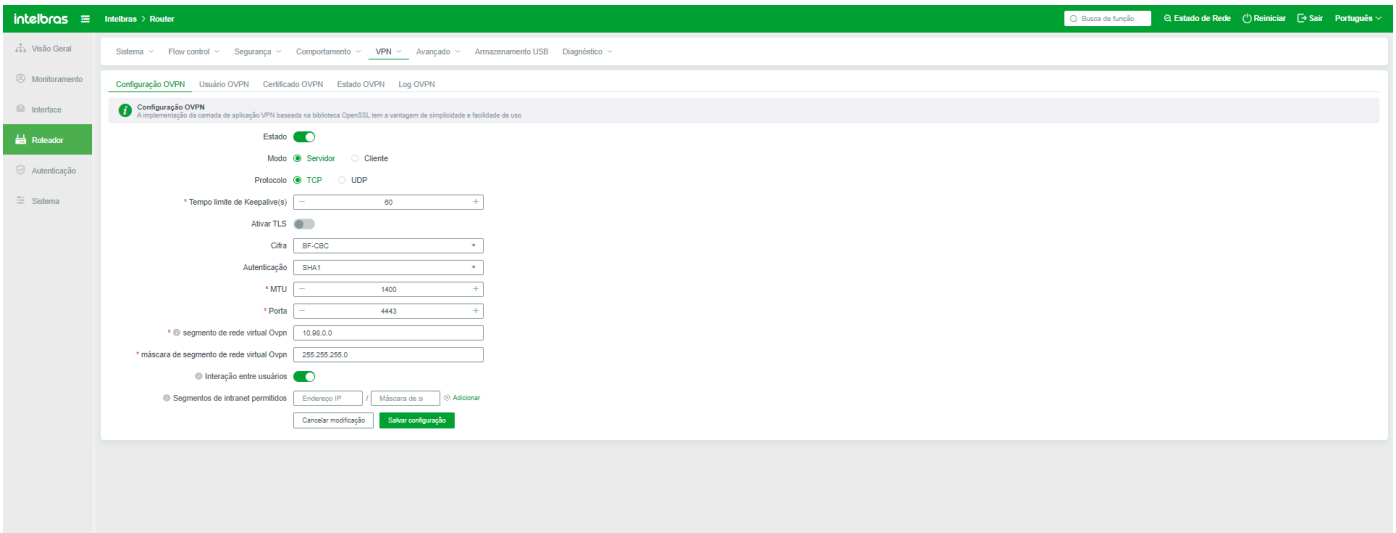


Importando contas de VPN: Se o sistema suportar vários clientes PPTP e for necessário alocar várias VPNs ao mesmo tempo, você pode importar contas de VPN. Por padrão, a conta de VPN importada está no modo de empréstimo. Se o sistema suportar a conexão de apenas um cliente, apenas a primeira conta de VPN poderá ser importada com sucesso, mesmo que várias contas sejam importadas.

OVPN

Configuração do OVPN

Configure os parâmetros do servidor ou cliente OVPN.



Status: Os próximos parâmetros podem ser configurados apenas quando o OVPN está habilitado.

Modo OVPN: Selecione o cliente ou servidor do sistema local como OVPN.

Os lados do serviço

Tipo de Protocolo: Especifica o protocolo usado pelo serviço OVPN. O protocolo padrão é TCP.

Duração da detecção de timeout (s): Se nenhum dado for recebido do cliente dentro do período especificado, a conexão será encerrada.

Configurações de MTU: Define o valor de MTU para a transmissão de dados VPN. Esse valor é usado em ambientes especiais. Mantenha o valor padrão.

Porta: Porta usada pelo serviço OVPN. O valor padrão é 4443. Você pode alterar o valor para uma porta não utilizada. Ao alterar o valor, certifique-se de que não conflita com outras portas.

Endereço do segmento de rede virtual OVPN: Um endereço de segmento de rede virtual definido pelo usuário é usado para se conectar à VPN. O endereço OVPN é atribuído ao cliente neste segmento de rede. Por exemplo, se o segmento de endereços IP for 192.168.x. X, use o segmento de endereços IP 10.X ou 172.

Máscara do segmento de rede virtual OVPN: Personalize uma máscara de segmento de rede virtual para se conectar à VPN.

Comunicação entre usuários: Após a ativação do OVPN, os clientes OVPN se comunicam entre si.

Segmento de intranet permitido: Especifica o segmento de intranet que o cliente VPN tem permissão para acessar. Esse parâmetro é configurado para um segmento de rede na LAN local.

O cliente

Tipo de Protocolo: Configure este parâmetro para o tipo de protocolo usado pela conexão VPN. O tipo de protocolo deve ser o mesmo usado pelo servidor. Caso contrário, a conexão VPN falha.

Duração da detecção de timeout (s): Se nenhum dado for recebido do cliente dentro do período especificado, a conexão será encerrada.

Configurações de MTU: O valor de MTU da conexão VPN pode ser definido pelo usuário. Geralmente, você pode usar o valor padrão.

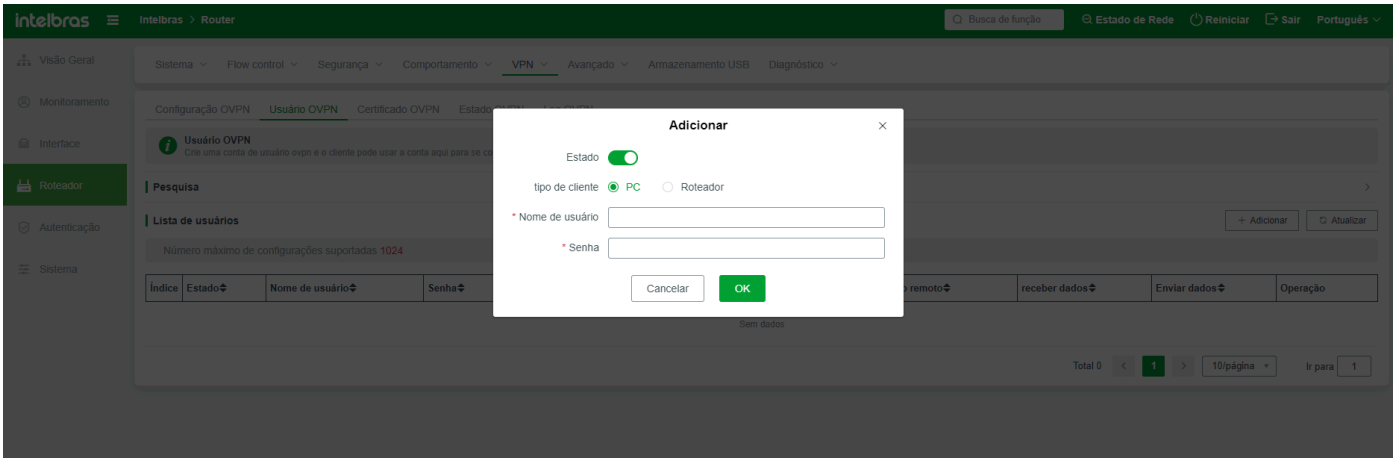
Nome de usuário: Conta OVPN fornecida pelo servidor.

Senha do usuário: Insira a senha OVPN fornecida pelo servidor.

Endereço do servidor: Insira o endereço IP público do servidor OVPN e o número da porta do servidor. Se existirem várias redes públicas no servidor, clique em Adicionar.

Usuário OVPN

Crie uma conta de usuário OVPN e forneça-a ao cliente.



Adicionar: Se precisar adicionar uma nova conta, clique neste botão para adicionar a configuração.

Status do usuário: A conta pode ser usada normalmente apenas quando está habilitada. A conta não pode ser usada normalmente quando está desativada.

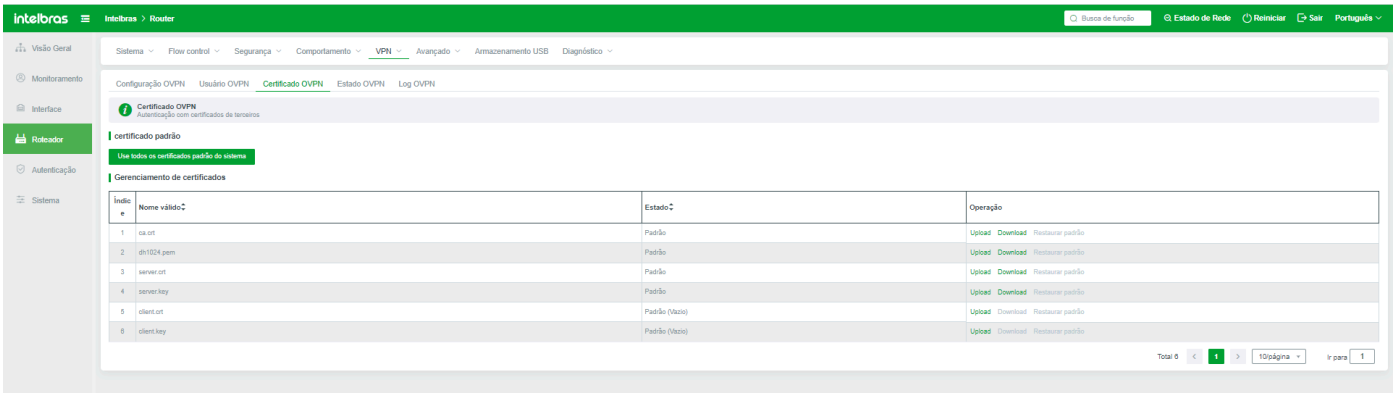
Tipo de usuário: Selecione o tipo de cliente, PC ou roteador. (Diferentes tipos de clientes se comunicam entre si. Por exemplo, se uma conta de PC for usada no cliente de roteamento, o cliente não poderá fazer ping na intranet do servidor.)

Senha: Especifica a senha da conta definida no servidor.

Endereço do segmento de rede interno: Insira o segmento de rede interno do cliente roteador somente quando o cliente for um roteador. Note que o segmento de rede interno do cliente não pode ser o mesmo que o segmento de rede interno do servidor.

Certificado OVPN

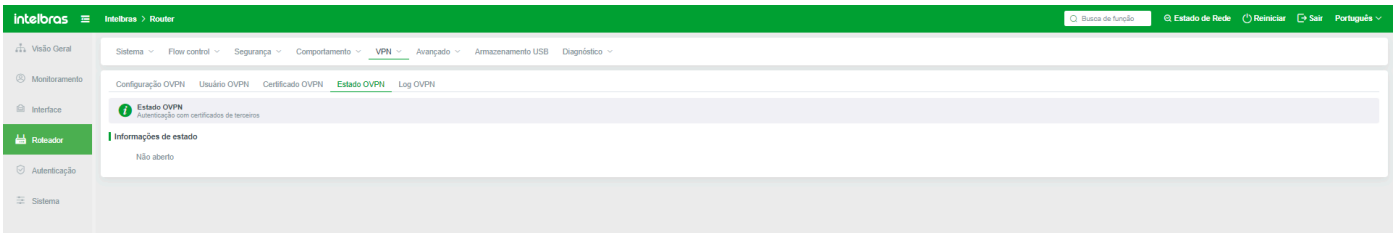
O OVPN requer um certificado OVPN. O sistema tem seu próprio certificado por padrão. Se precisar atualizar o certificado, faça o upload da cópia de atualização correspondente aqui.



Estado OVPN

Quando o cliente se conecta com sucesso ao servidor, o status atual da conexão OVPN pode ser visto no cliente.

O cliente conectado pode clicar no botão "Desconectar" para encerrar a conexão atual.



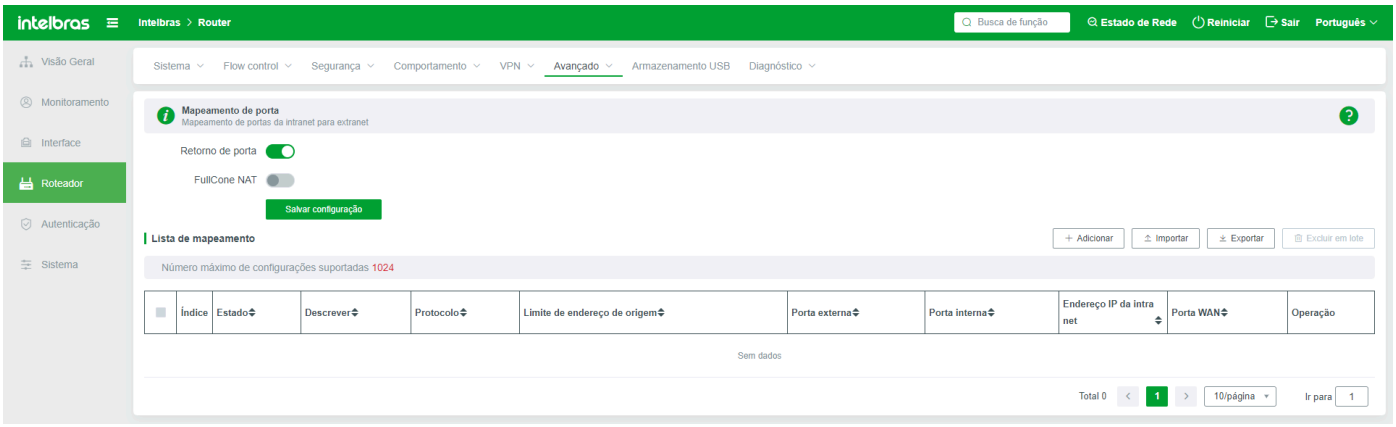
Log OVPN

Registra os logs do OVPN. Se os logs forem excluídos, eles não poderão ser restaurados.

Avançado

Mapeamento de Portas

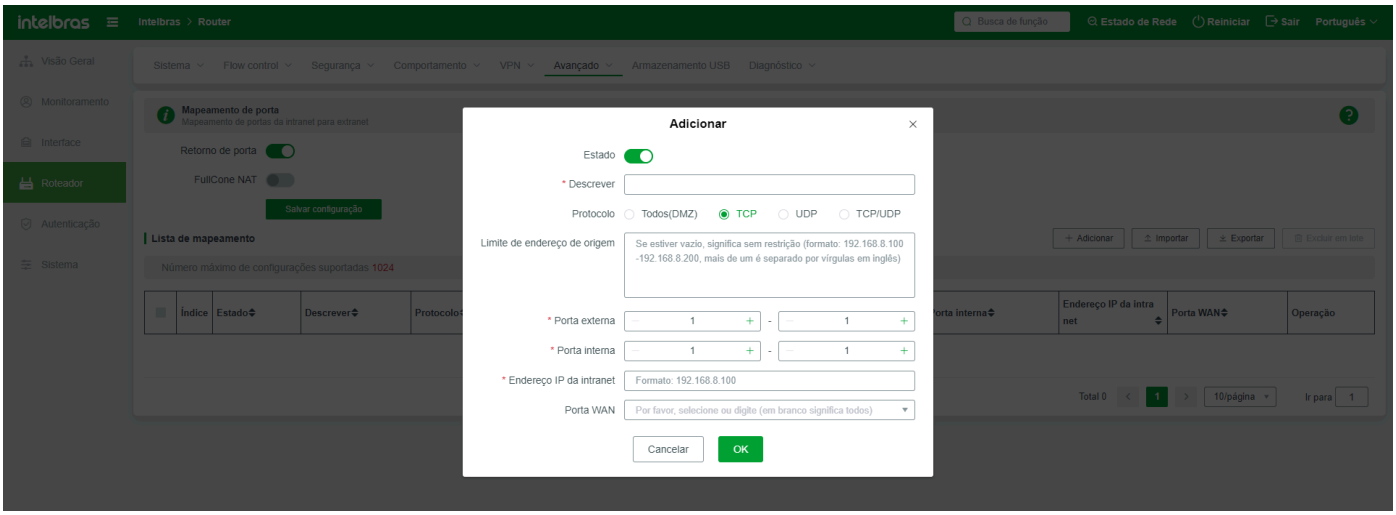
Configure regras de mapeamento para mapear portas da intranet para a internet, permitindo que outros hosts na internet acessem o conteúdo das portas.



Refluxo de Porta: O refluxo de porta está habilitado por padrão.

NAT de Cone Completo: Esta função está desativada por padrão. É aconselhável habilitar esta função em um ambiente de CDN.

Adicionar uma regra de refluxo de porta



Status: Indica se o status da regra está habilitado. Se o status da regra estiver desativado, a regra de mapeamento não terá efeito.

Descrição: Adicione uma descrição das regras para facilitar a distinção entre muitas regras;

Protocolo: Selecione o tipo de protocolo de mapeamento. Protocolos não selecionados não serão mapeados com sucesso.

Restrição de Endereço de Origem: Somente o endereço (ou segmento de endereço) inserido pode acessar o conteúdo mapeado. Se o valor estiver vazio, indica que o conteúdo mapeado não está restrito.

Porta Externa: Esta porta é adicionada ao endereço IP da porta WAN onde o host de mapeamento reside para acessar o conteúdo mapeado. Esta porta não pode entrar em conflito com outras portas.

Porta Interna: Porta usada pela LAN para acessar a máquina de mapeamento. Geralmente, essa porta é determinada pelo software. Se a porta interna a ser mapeada for a mesma que a porta externa, você não precisa inserir a porta interna.

Endereço do Host Interno: Especifica o endereço IP do host interno a ser mapeado. Este parâmetro é obrigatório.

Porta WAN: Selecione a regra de saída de mapeamento de porta. A extremidade de acesso acessa o host ou endereço IP mapeado através do endereço IP e porta especificados da porta WAN.

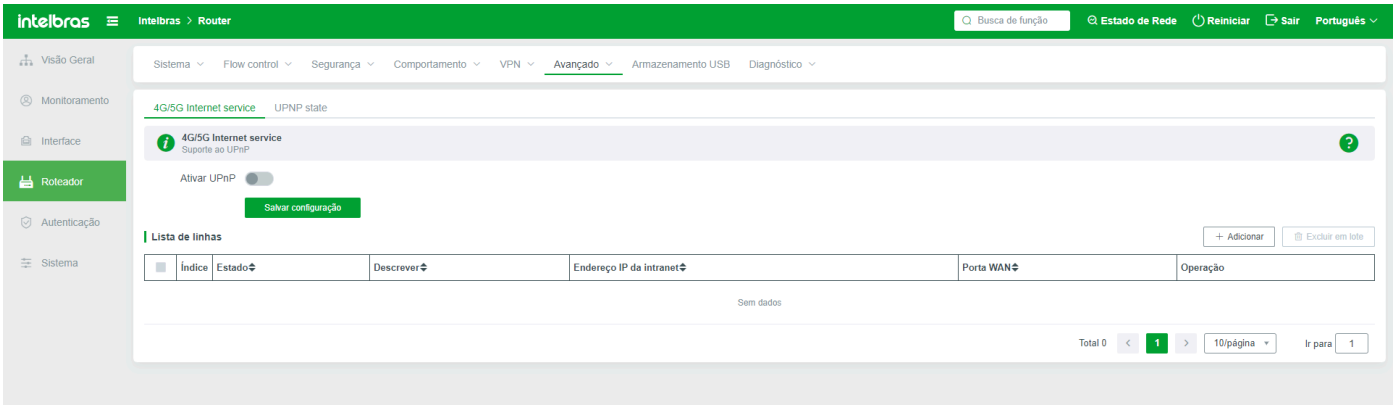
Importar: Você pode importar regras de mapeamento de porta em lotes. Se não tiver certeza sobre o formato do arquivo e as regras, você pode adicionar uma regra de mapeamento e exportá-la. Adicione ou exclua as informações modificadas no arquivo exportado e, em seguida, importe-o.

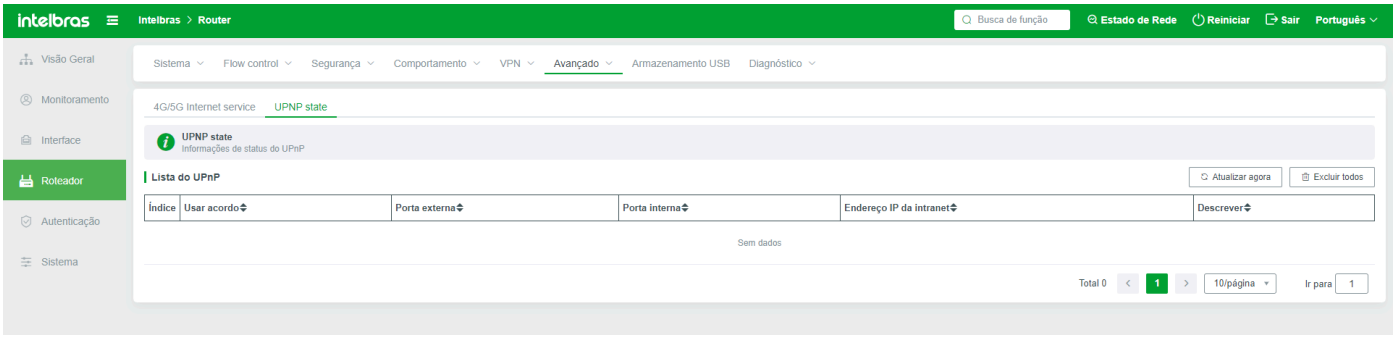
Exportar: Você pode exportar regras de mapeamento criadas no sistema.

Exclusão em lote: Selecione as regras de mapeamento criadas e clique em Excluir em Lote. As regras de mapeamento excluídas não podem ser restauradas.

Configurações UPnP

UPnP é um padrão de protocolo de comunicação. Se o computador suportar o mecanismo UPnP e a função UPnP estiver ativada no computador, a função UPnP pode ser ativada no roteador. Após a ativação do UPnP, os downloads P2P são acelerados até certo ponto, mas a rede é sobrecarregada. Downloads excessivos de P2P afetarão o uso normal da rede. Use essa função adequadamente.





UPnP: A função UPnP está desativada por padrão. As regras podem ser configuradas somente após a ativação do UPnP.

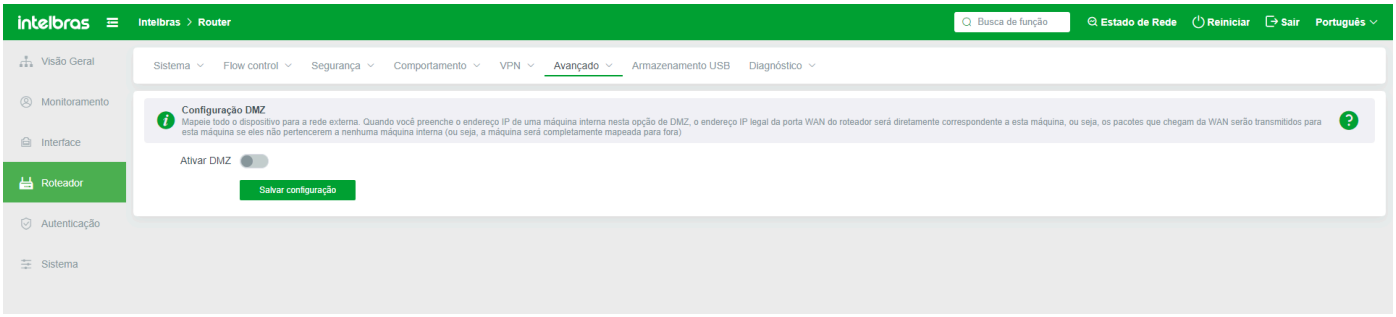
Porta WAN: Selecione a porta WAN mapeada a partir da porta UPnP.

Exibição na rede: Depois de selecionar o software de aplicativo que precisa mapear automaticamente as portas, o software de aplicativo é exibido na lista, para que o administrador possa visualizar o tipo de software usado.

Excluir Tudo: Exclua o UPnP gerado após ser ativado.

Configurações DMZ

Quando o endereço IP de uma máquina interna é inserido nesta opção DMZ, o endereço IP legítimo da interface WAN do roteador corresponde diretamente a esta máquina. Em outras palavras, pacotes da WAN que não pertencem a nenhuma máquina interna serão transmitidos para esta máquina (ou seja, a máquina é completamente mapeada para fora).



Habilitar DMZ: O DMZ está desativado por padrão. Você pode configurar regras apenas quando o DMZ está habilitado.

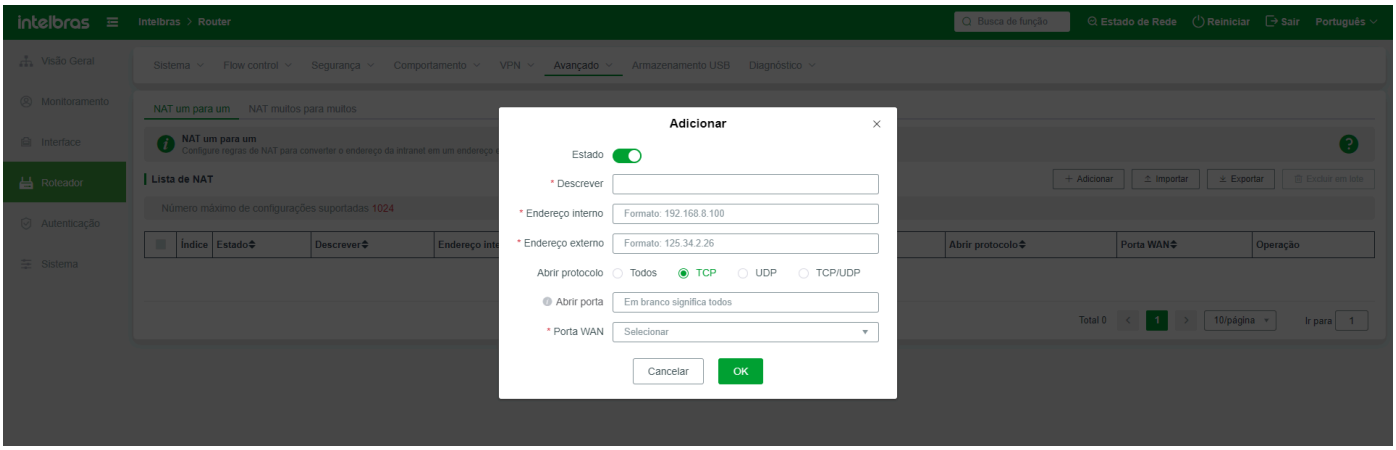
Endereço IP de Destino: Especifica o endereço IP da máquina interna no DMZ.

Limite de Endereço de Origem: Especifica o endereço IP ou segmento de endereço que pode ser acessado por portas WAN externas. Os três formatos "202.103.24.68", "202.103.24.68-202.103.44.150" e "202.103.24.0/24" são permitidos.

NAT

NAT Um para Um

Para traduzir o endereço de origem de onde um host envia dados em um endereço externo correspondente.



Exemplo Adicionar uma regra de tradução um para um

Status: Indica se o status da regra está habilitado. Se o status da regra estiver desativado, a regra de um para um criada não terá efeito.

Descrição: Adicione uma descrição das regras para facilitar a distinção entre muitas regras;

Endereço Interno: Insira o endereço da LAN local para tradução de endereço de rede um para um. Por exemplo, 192.168.1.100.

Endereço Externo: Insira um endereço externo para tradução de endereço de rede um para um. Por exemplo, 218.35.97.7;

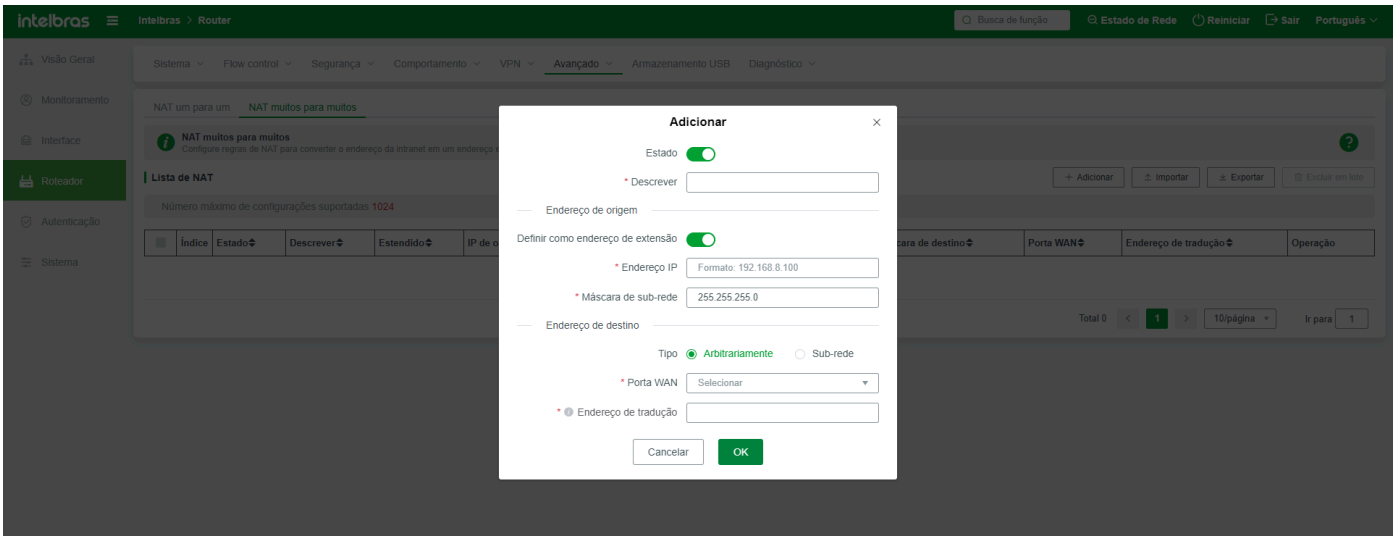
Protocolo Aberto: Selecione o protocolo a ser usado pela transformação aberta;

Porta Aberta: Insira a porta com o endereço externo aberto. Se o valor estiver vazio, significa que está aberto para todos. O formato é 100,200,300:305.

Porta WAN: Selecione uma porta WAN para a saída de dados do host interno um para um.

NAT Um para Muitos

Configure regras NAT para traduzir endereços de intranet em endereços externos, para que os usuários da intranet possam acessar redes externas. Pode ser interpretado como a tradução do endereço de origem dos dados enviados por um host em um endereço externo correspondente.



A regra NAT um para muitos é adicionada

Status: Indica se o status da regra está habilitado. Por exemplo, a regra um para muitos criada para desabilitar a regra não terá efeito.

Descrição: Adicione uma descrição das regras para facilitar a distinção entre muitas regras;

Endereço de Origem

Definir para Endereço de Extensão da Intranet: se o endereço de extensão da rede está bloqueado, o que está habilitado por padrão.

Endereço IP: indica um endereço IP a ser traduzido na intranet. Este parâmetro é obrigatório.

Máscara de Sub-rede: Insira a máscara de sub-rede. O valor padrão é recomendado.

Destino

Tipo: Seleciona o tipo da conversão;

Porta WAN: especifica a saída através da qual os dados são convertidos.

Traduzir Endereço IP: Insira o segmento de endereço IP a ser traduzido. Este segmento de endereço IP suporta um máximo de 16 endereços IP, por exemplo, 221.18.10.6-221.18.10.21.

Configurações do Roteador

Esta unidade é usada para configurar a tabela de roteamento. A tabela de roteamento, uma tabela armazenada em um roteador ou outro dispositivo de rede da Internet que contém caminhos para terminais de rede específicos e, em alguns casos, métricas associadas a esses caminhos. O principal trabalho de um roteador é encontrar um caminho de transmissão ótimo para cada datagrama que passa pelo roteador e transmitir eficientemente os dados para o site de destino.

Tabela de Roteamento

A tabela de roteamento padrão (IPv4) é gerada automaticamente pelo roteador para que os usuários possam visualizá-la e não pode ser modificada.

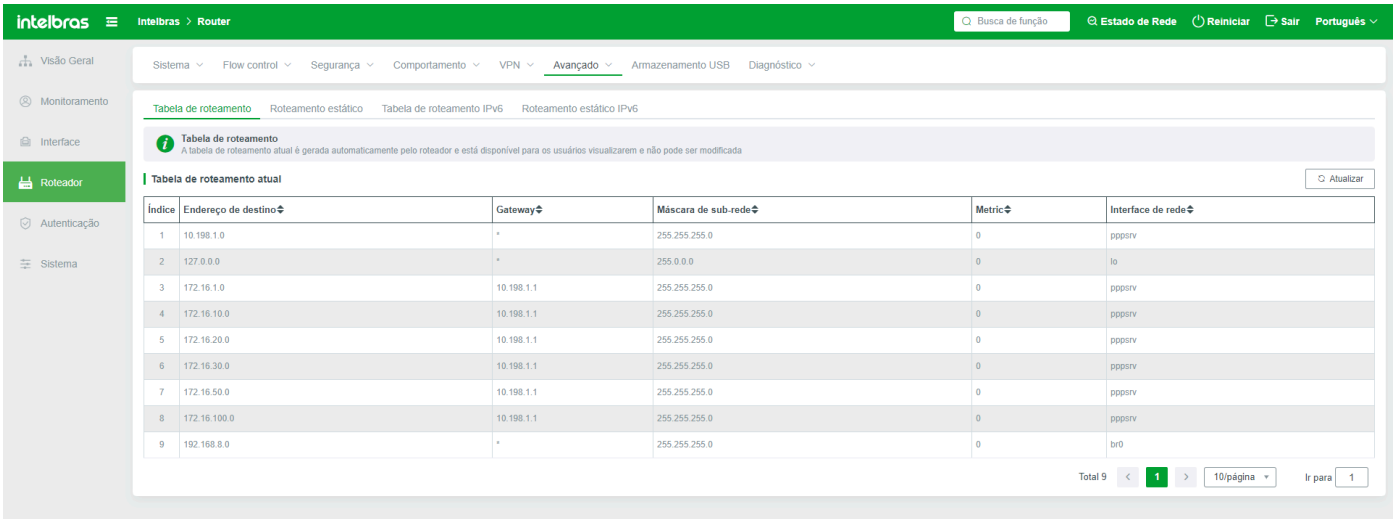
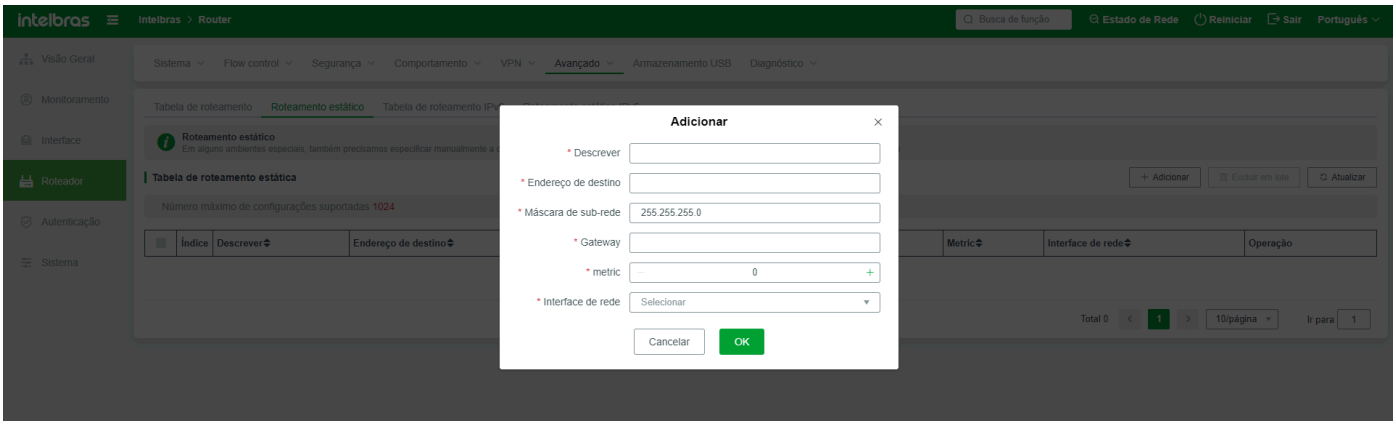


Tabela de Roteamento Estático

Além da tabela de roteamento padrão (IPv4), você precisa adicionar manualmente uma tabela de roteamento estático em alguns ambientes especiais para especificar o roteador do roteador para garantir que alguns dados possam passar.

Adicione uma tabela de roteamento estático conforme necessário



Descrição: Personalize as especificações para distinguir entre regras.

Destino: indica o endereço IP de destino da tabela de roteamento estático.

Máscara de sub-rede: defina a máscara de sub-rede conforme necessário.

Gateway: Insira o endereço do gateway com base na situação real.

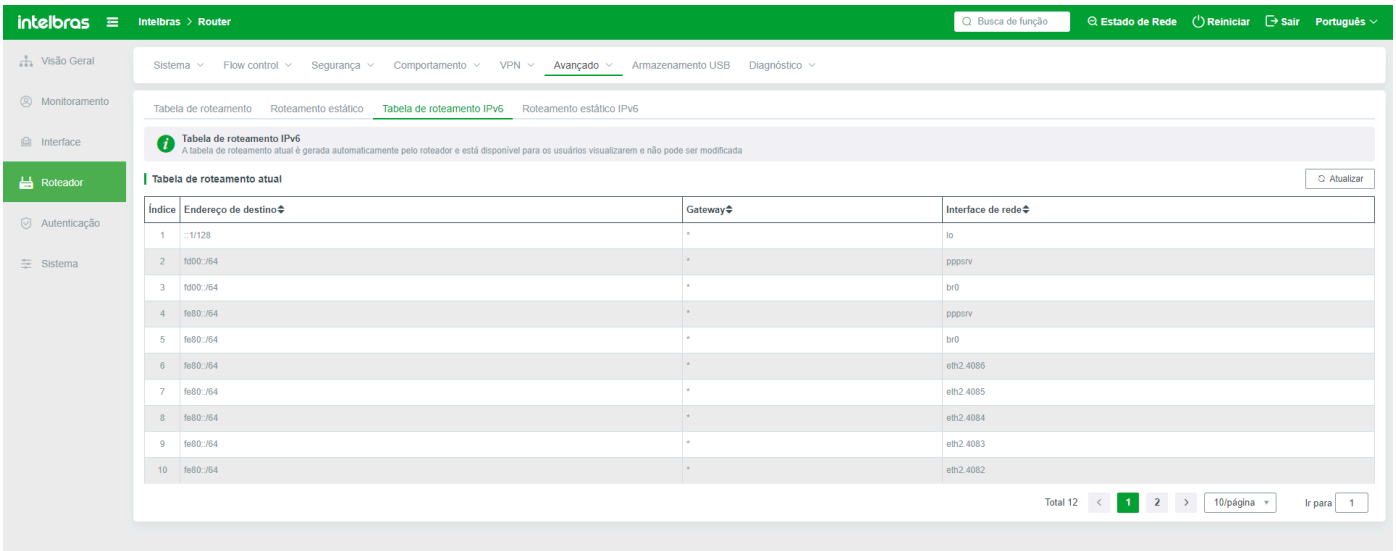
Métrica: O valor da métrica é 0 por padrão.

Interface de rede: Selecione a interface WAN da tabela de roteamento estático.

Exemplo: Por exemplo, o roteador R3005G está conectado a um switch de camada 3 com o endereço IP 192.168.1.244. O switch de camada 3 é atribuído a um segmento de rede 172.15.2.1/24. Os hosts no switch de camada 3 usam endereços IP no segmento de rede 172.15.2.X para acessar a Internet e usam 172.15.2.1 como endereço de gateway. Nesse caso, é necessário adicionar roteadores estáticos conforme mostrado na figura anterior para permitir que os hosts sob o switch de Camada 3 acessem a Internet normalmente.

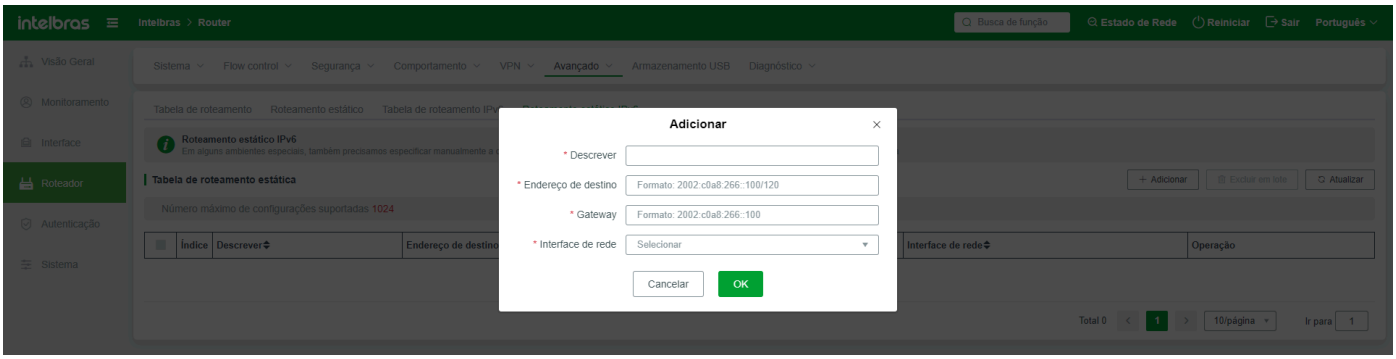
Tabela de Roteamento IPv6

Os princípios e funções da tabela de roteamento são os mesmos da tabela de roteamento anterior, exceto que a tabela de roteamento IPv6 é gerada automaticamente pelo roteador.



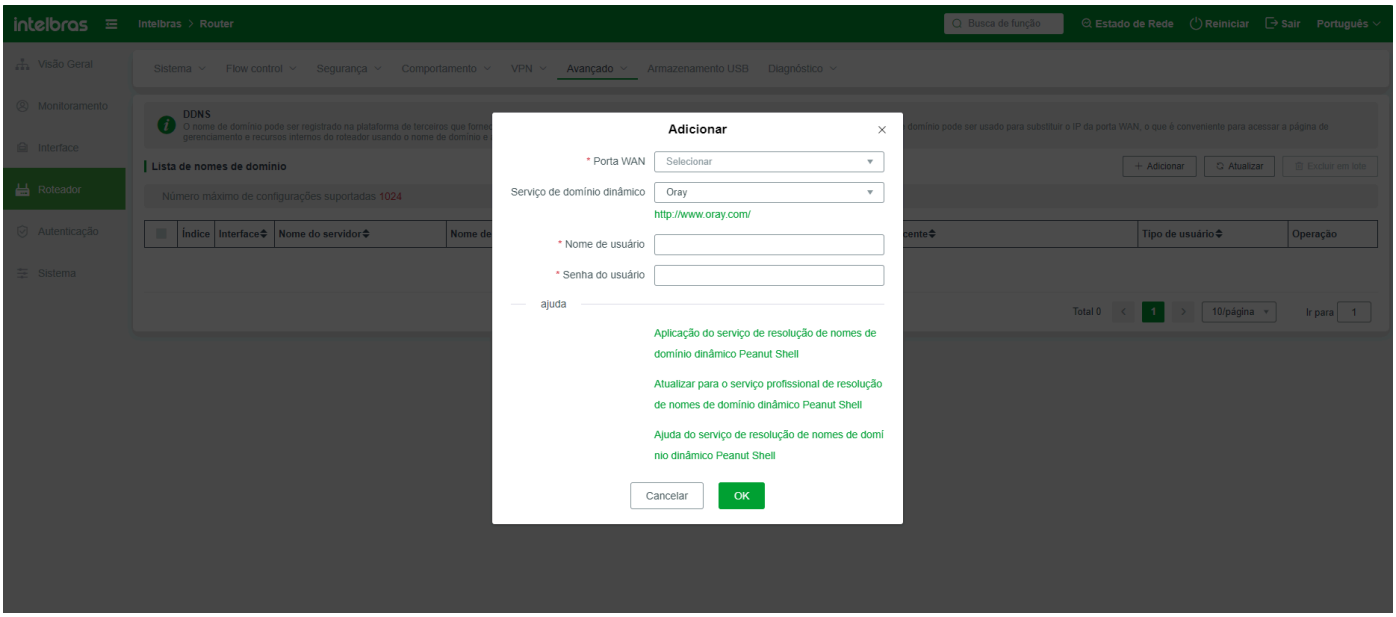
Roteador Estático IPv6

Os princípios e funções são os mesmos do roteador estático (IPv4). Você pode configurar este parâmetro com base nos requisitos e nas exigências do sistema.



Nome de Domínio Dinâmico

Um nome de domínio dinâmico é usado para resolver um endereço IP dinâmico em um nome de domínio estático para que a rede possa acessar. Para usar essa função, solicite um nome de domínio registrado no site de nome de domínio dinâmico de terceiros e resolva automaticamente o nome de domínio para a interface WAN do roteador. Use este nome de domínio para substituir o endereço IP da interface WAN e use o nome de domínio e a porta para acessar a página de gerenciamento e os recursos internos do roteador.



Interface WAN de Trabalho do Nome de Domínio: Selecione a interface WAN que usa o nome de domínio estático.

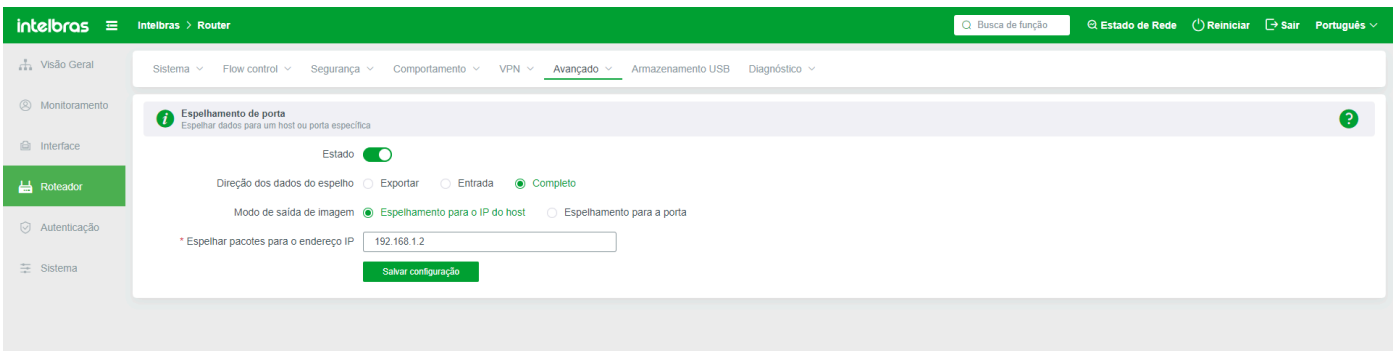
Serviço de Nome de Domínio Dinâmico: Selecione o nome do servidor de nome de domínio registrado e resolvido, clique na tecla de expansão para visualizar o servidor de nome de domínio suportado pelo sistema atual;

Nome de Usuário: Insira o nome do usuário registrado no servidor DNS.

Senha do Usuário: Insira a senha para se registrar no servidor DNS.

Espelhamento de Porta

A função de espelhamento de porta é usada para espelhar dados internos para uma porta ou host específico, facilitando a análise de dados de rede.



Status: A função de espelhamento de porta está desativada por padrão. As regras podem ser configuradas somente após serem habilitadas.

Selecione a Direção de Dados para Espelhamento: Selecione a direção dos dados a serem espelhados, incluindo dados de saída, dados de saída ou dados de saída e dados de saída.

Modo de Saída de Espelhamento: Selecione o modo de saída de dados espelhados. Pode ser simplesmente entendido como onde os dados espelhados são espelhados - para um endereço IP de host ou uma porta.

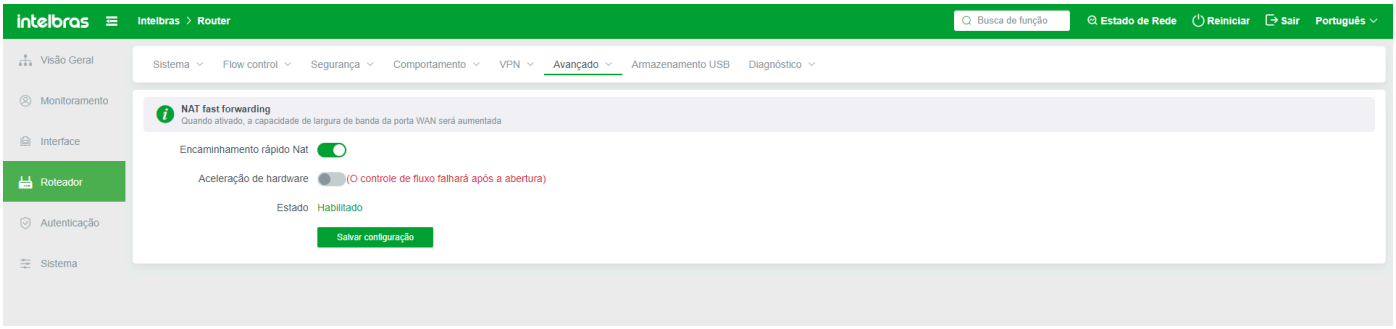
Pacotes de Dados de Espelhamento para o Endereço IP do Host Interno: Se o modo de saída de espelhamento estiver definido como Espelhamento para o endereço IP do host, insira o endereço IP do host.

Porta de Espelhamento: Se o modo de saída de espelhamento estiver definido como Espelhamento para a porta, selecione a porta correspondente.

A função de espelhamento de porta pode ser usada com ferramentas de captura de pacotes, como Collet.

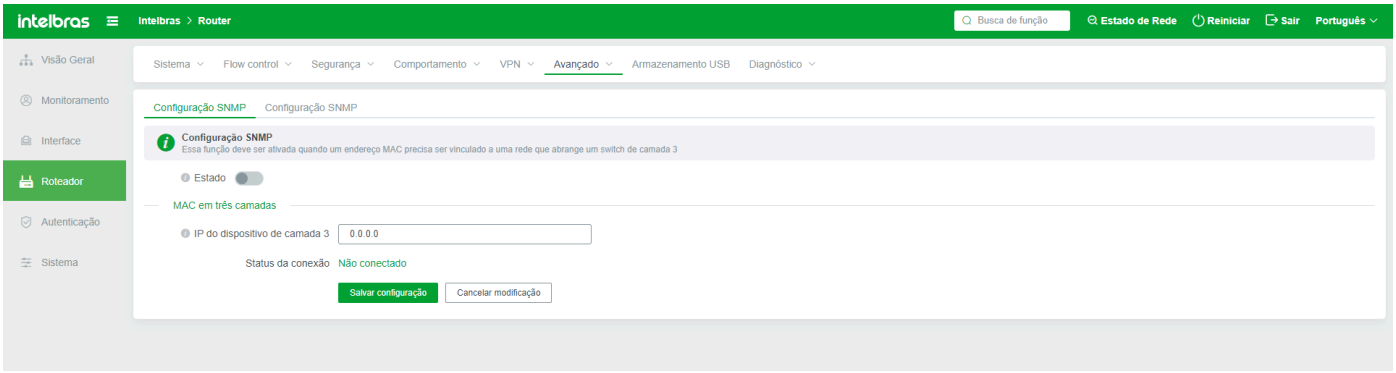
Encaminhamento Rápido NAT

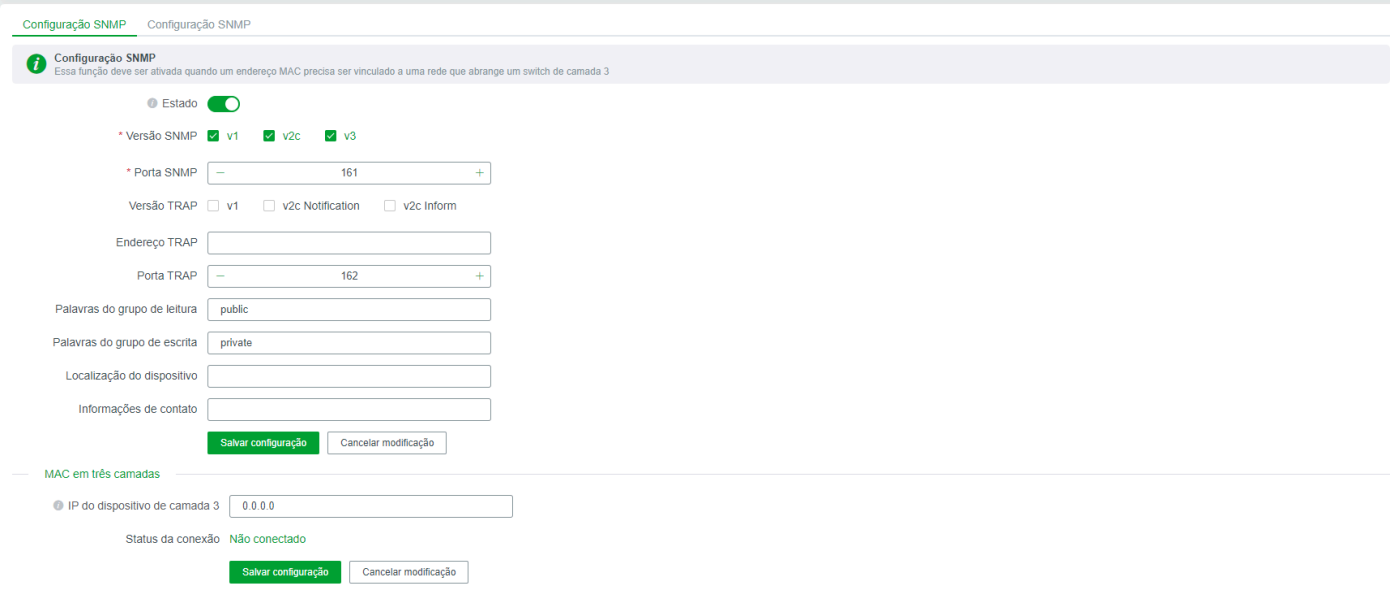
Habilitar o encaminhamento rápido NAT melhora a velocidade de processamento de dados. Após habilitar o encaminhamento rápido NAT, a filtragem de palavras-chave WEB, monitoramento de e-mails.



Configuração SNMP

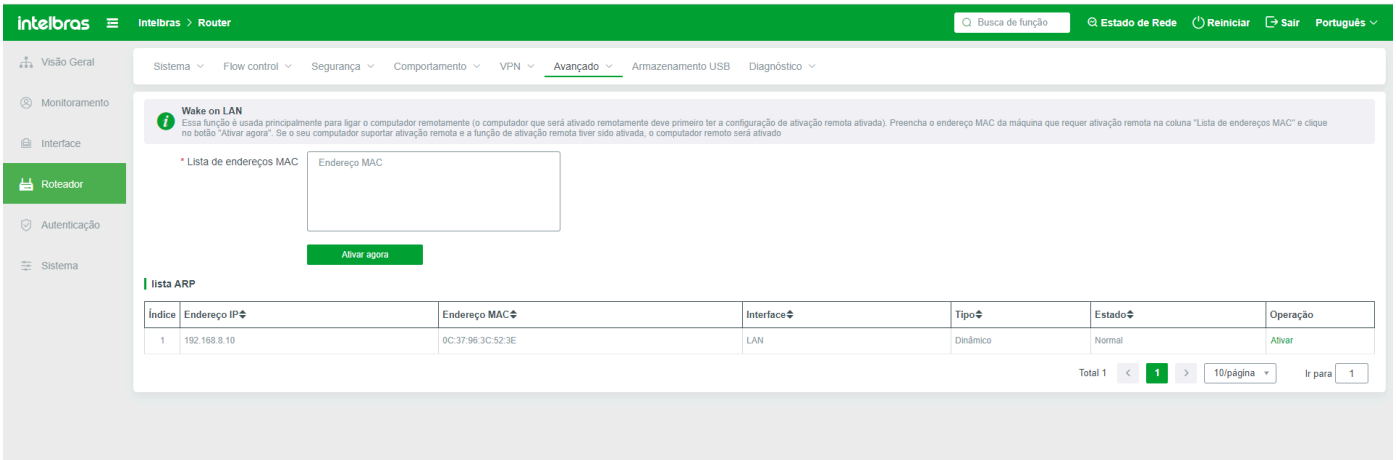
Esta função deve ser ativada quando um endereço MAC precisa ser vinculado a uma rede abrangendo um switch de camada 3.





Wake on LAN

Esta função é usada principalmente para ligar o computador remotamente (o computador acordado deve primeiro ativar a configuração de despertar remoto). Preencha o endereço MAC da máquina que requer despertar remoto na coluna "Lista de endereços MAC" e, em seguida, clique no botão "acordar agora". Se o seu computador suporta o despertar remoto e a função de despertar remoto estiver ativada, o computador remoto será acordado

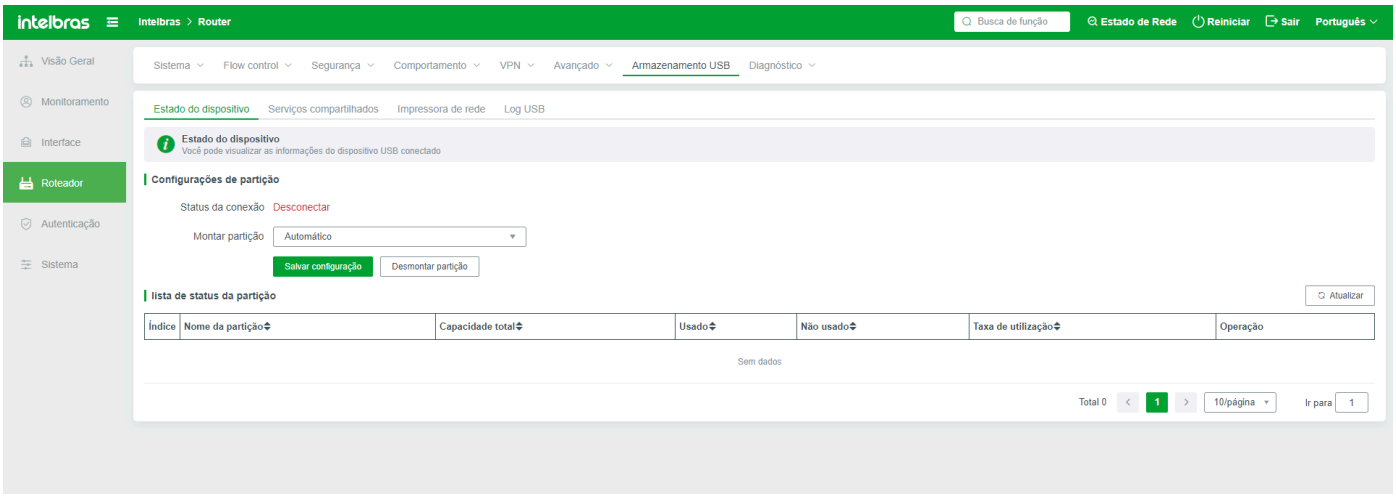


Armazenamento USB

Dispositivos USB são inseridos no roteador para realizar o compartilhamento de arquivos e dados sem a necessidade de configurar um servidor de compartilhamento de arquivos.

Status do Dispositivo

Se o hardware do sistema de roteamento suportar o acesso USB, o status de conexão muda para Conectado na página de status do dispositivo após o hardware USB ser conectado com sucesso. Se nenhum hardware USB estiver conectado ou o hardware USB não for conectado com sucesso, o status de conexão na página será Desconectado.



Status de Conexão: Status de acesso USB, conectado ou não conectado;

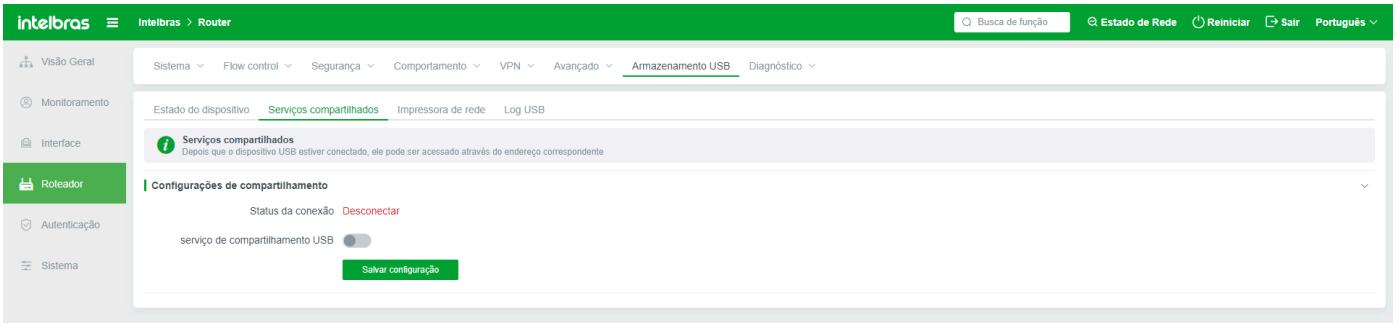
Partição de Montagem: Selecione a partição de montagem de um disco externo. Se dois dispositivos USB estiverem conectados ao disco externo, você pode selecionar a partição automática ou especificar uma delas para ser montada. O dispositivo USB especificado armazenará os dados especificados, como logs.

Desmontar a Partição: Desmonte a partição desconectando a conexão USB. Se precisar remontar a partição, clique em "Salvar configurações".

Lista de Status da Partição: exibe o status dos dispositivos USB conectados e o uso da memória. Se você clicar em Formatar, os dados USB serão formatados e não poderão ser restaurados.

Serviços de Compartilhamento

Decidir se deseja compartilhar uma unidade USB e configurar as regras para acessar diretórios e caminhos de compartilhamento. O serviço de compartilhamento só pode ser usado após a conexão bem-sucedida do USB. Caso contrário, o serviço de compartilhamento não pode ser usado. Por padrão, a função de compartilhamento USB está desativada. Portanto, é necessário ativar manualmente a regra de configuração.



Serviço de Compartilhamento USB: Determina se a função de compartilhamento USB está habilitada. As regras a seguir podem ser configuradas apenas após a função de compartilhamento USB ser ativada.

Permitir que usuários da Internet acessem: Após a ativação dessa função, os usuários da Internet podem acessar os compartilhamentos USB.

Habilitar acesso de autenticação WEB: Se habilitado, a autenticação de acesso refere-se a inserir a conta e senha no endereço de acesso WEB abaixo. Se isso estiver desativado, você pode acessar diretamente o endereço WEB clicando neste endereço WEB. Se a função de acesso WEB estiver habilitada, você precisará inserir a conta e a senha para acessar a página do diretório.

ID do dispositivo: Define o ID do dispositivo. O ID do dispositivo será enviado ao usuário quando o endereço for enviado abaixo.

Nome de usuário: Define a conta para fazer login no diretório compartilhado.

Senha: Define a senha para fazer login no diretório compartilhado.

Super usuário: Define a conta super para fazer login em um diretório compartilhado. As quatro contas comuns podem acessar alguns diretórios. A conta e a senha superiores têm os direitos de acesso mais altos.

Super senha: Define a senha super para fazer login em um diretório compartilhado. A conta e a senha superiores têm os direitos de acesso mais altos.

Diretório compartilhado: Um diretório geralmente compartilhado com outro host. Para acessar um diretório, execute Windows+R primeiro e, em seguida, insira este endereço.

Diretório privado: Diretório USB. Se desejar compartilhá-lo com outros hosts, use o mesmo método do diretório compartilhado.

Acesso WEB: Acesse o diretório no formato do endereço da web, copie o endereço para o acesso à página da web;

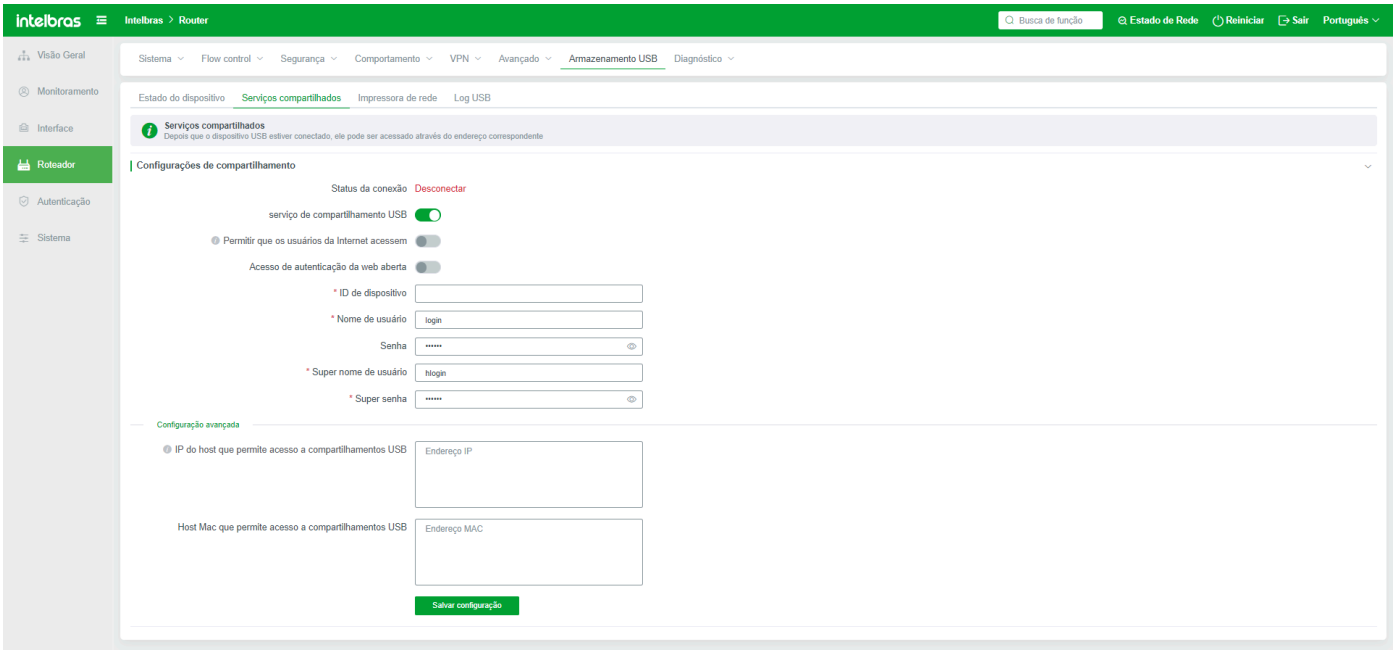
Enviar o URL por e-mail/WeChat para acesso à Internet: Desativado por padrão. Depois de ativado, você pode selecionar "Enviar nome de usuário compartilhado" e "Enviar senha compartilhada" para enviar as Configurações acima (ou o nome de usuário e senha padrão) para o e-mail/WeChat especificado, e as regras de envio são adicionadas abaixo.

Configurações Avançadas

Hosts internos (baseados em IP) que permitem acesso aos compartilhamentos USB: O host IP adicionado pode acessar diretamente o endereço IP compartilhado sem usar o nome de usuário ou senha.

Permitir acesso a hosts internos (baseado em MAC): O host MAC adicionado pode acessar diretamente o endereço compartilhado sem usar o nome de usuário ou senha.

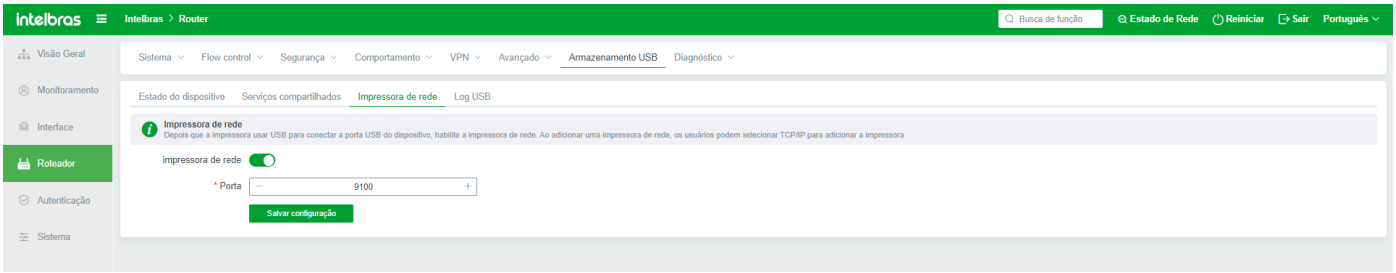
Status: Indica se o status da regra de envio precisa ser habilitado. Se a regra de envio não precisar entrar em vigor, defina seu status como desativado.



Impressoras de Rede

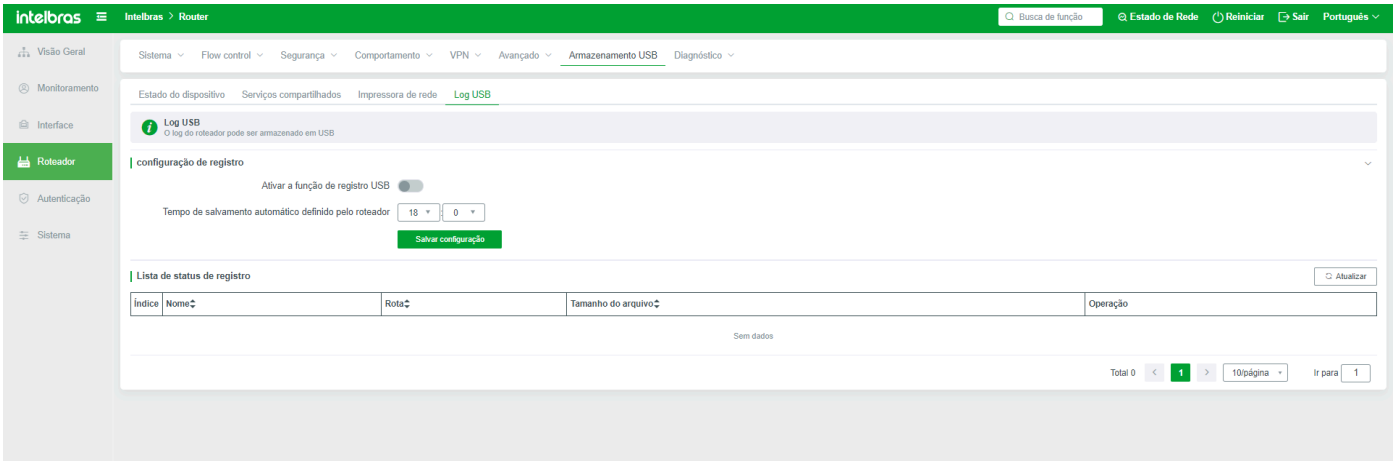
Após a conexão da impressora à porta USB do dispositivo por meio de USB, a impressora de rede pode ser habilitada. Você pode selecionar TCP/IP ao adicionar uma impressora de rede.

O status padrão é desativado. Ative e configure a função quando necessário. Geralmente, as configurações de porta são padrão. Se precisar alterar as configurações de porta, evite conflitos com outras portas.



Log USB

Logs gerados pelo sistema podem ser salvos no USB. Por padrão, a função USB está desativada. Portanto, se precisar salvar logs no USB, ative esta função.



Habilitar função de log USB: Especifica se deseja ativar a função de log USB. Após a ativação da função de log USB, os logs serão salvos no USB no horário especificado.

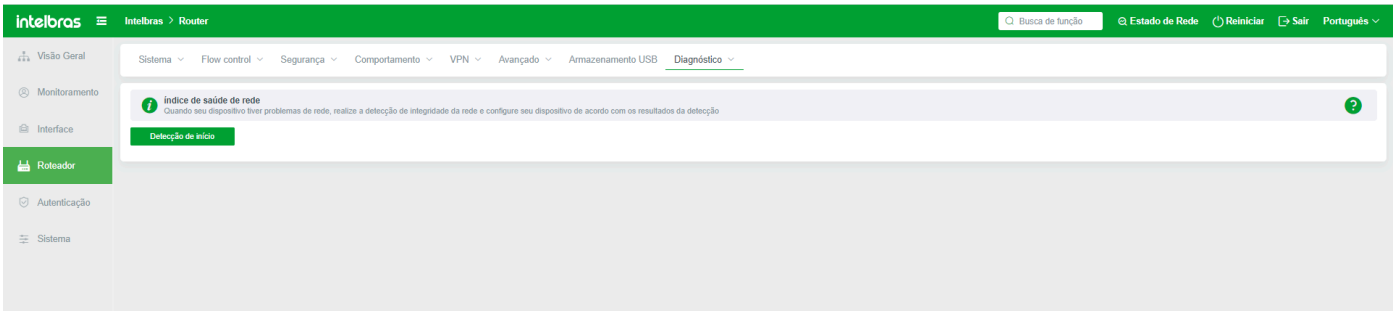
O roteador define o horário de salvamento automático: Define o tempo de armazenamento automático de logs, e os logs não serão armazenados no restante do tempo.

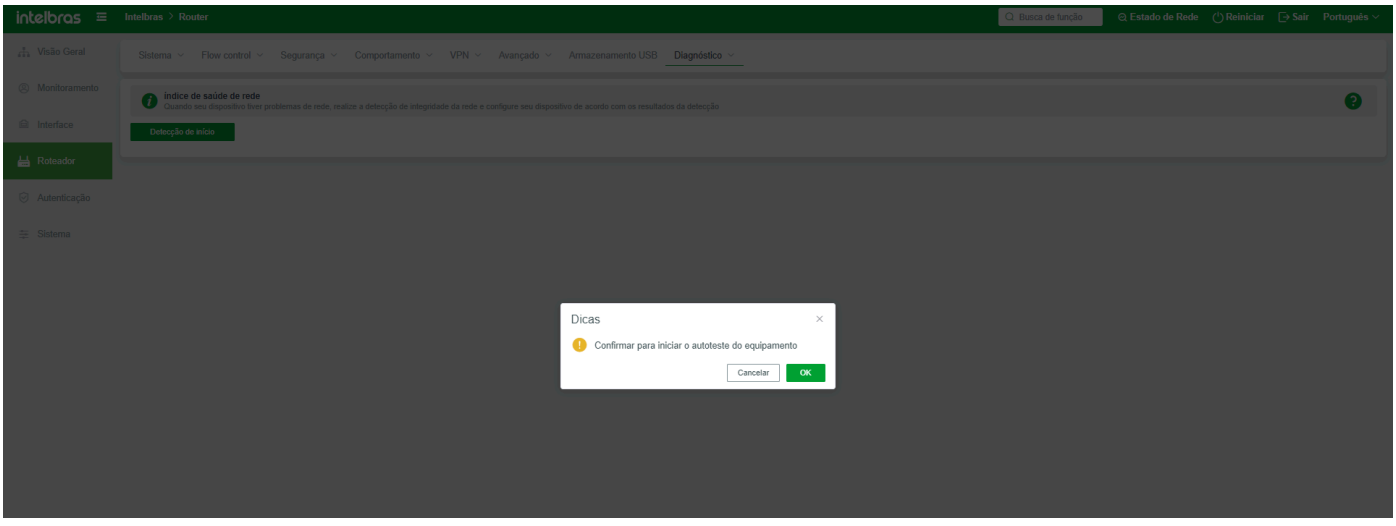
Depois que a função de armazenamento de log é ativada, o log correspondente na lista de status do log tem um botão de limpeza. Se você clicar em "Limpar", o log será excluído e não poderá ser restaurado.

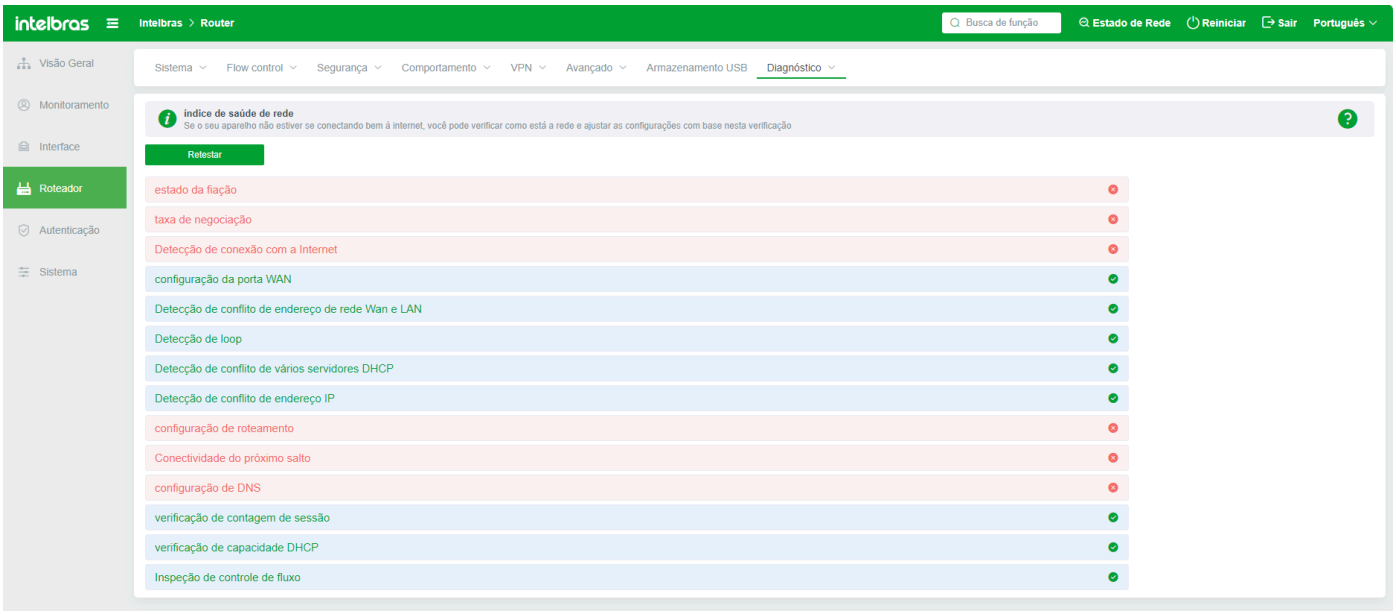
Diagnóstico

Índice de Saúde da Rede

Verificação da saúde da rede: Ative "Iniciar Verificação" para verificar a saúde da rede quando ocorrer uma falha no dispositivo ou na LAN local.







Ferramentas de Rede

Teste de Ping

A função de Ping ajuda o administrador a saber o status online da rede. Você pode usar a função de ping para determinar o status da rede.

Endereço IP/Nome de domínio: Insira o endereço IP ou nome de domínio a ser pingado.

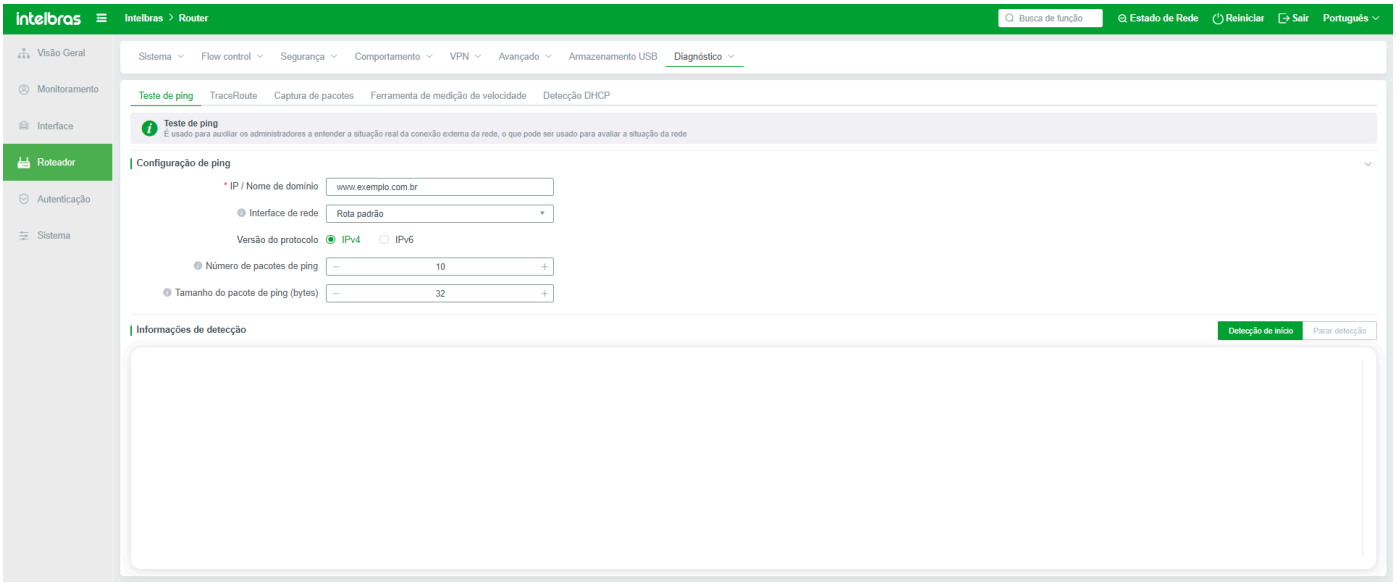
Interface de rede: Selecione a interface da qual o ping verifica.

Versão do protocolo: IPv4 ou IPv6.

Contagem de pacotes Ping: Especifica o número de pacotes detectados por cada Ping. O valor padrão é 20. O valor varia de 1 a 1000.

Tamanho do pacote Ping (bytes): Especifica o tamanho do pacote a ser pingado. O valor padrão é 1024. O valor varia de 1 a 10240.

Depois que as regras são configuradas, clique em "Iniciar Detecção". O resultado da detecção é exibido abaixo. Para interromper a detecção, clique no botão "Parar Detecção".



Rastreamento de Roteador

Usado para determinar o caminho percorrido pelos dados IP até o alvo de acesso

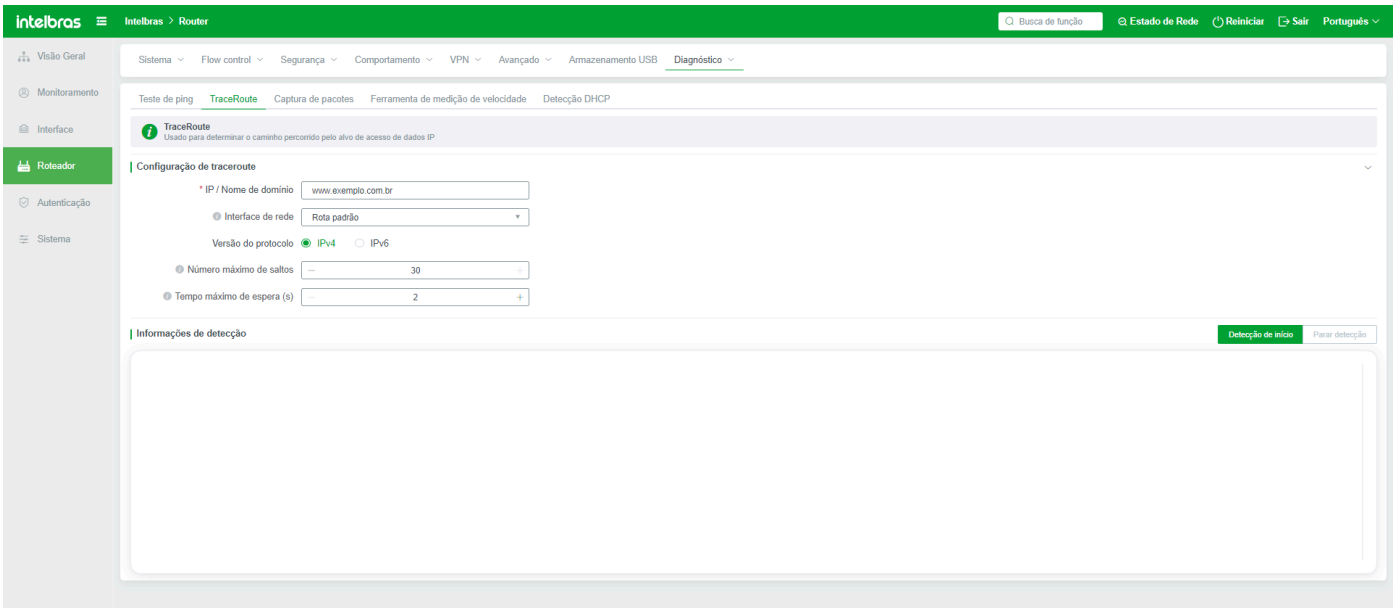
Endereço IP/nome de domínio: Insira o endereço IP ou nome de domínio do caminho a ser determinado.

Interface de rede: Selecione a porta pela qual o caminho de dados sai.

Contagem Máxima de Saltos: Define o número máximo de saltos entre dados. O valor padrão é 30. A faixa é de 2 a 30.

Tempo Máximo de Espera (s): Especifica o tempo máximo de espera. O valor padrão é 2 segundos. O valor varia de 2 a 10.

Depois que as regras são configuradas, clique em "Iniciar Detecção". O resultado da detecção é exibido abaixo. Para interromper a detecção, clique em "Parar Detecção".



Diagnóstico de Captura de Pacotes

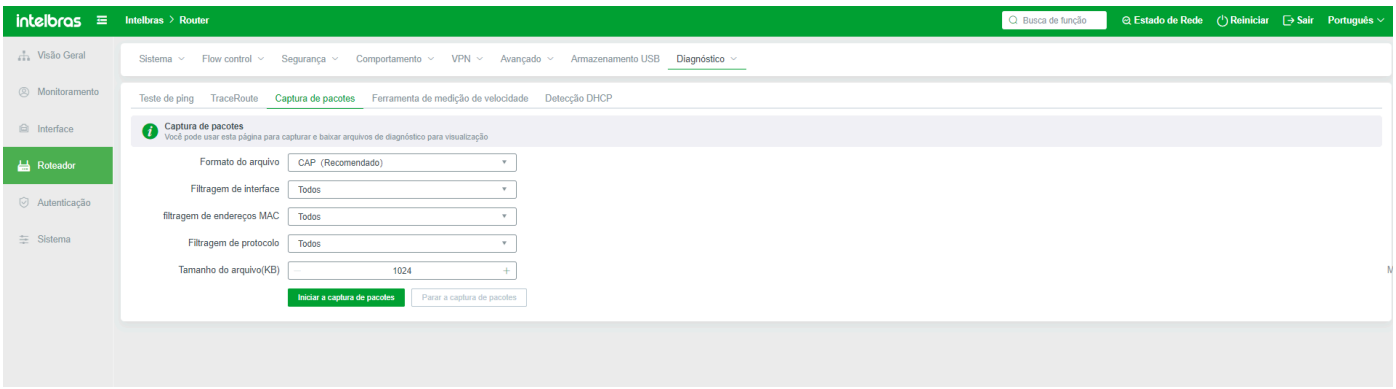
Você pode usar esta página para capturar e baixar arquivos de diagnóstico para visualização

Filtragem de Interface: Filtrar através da interface de rede

Filtragem de Endereço MAC: Filtrar através do MAC

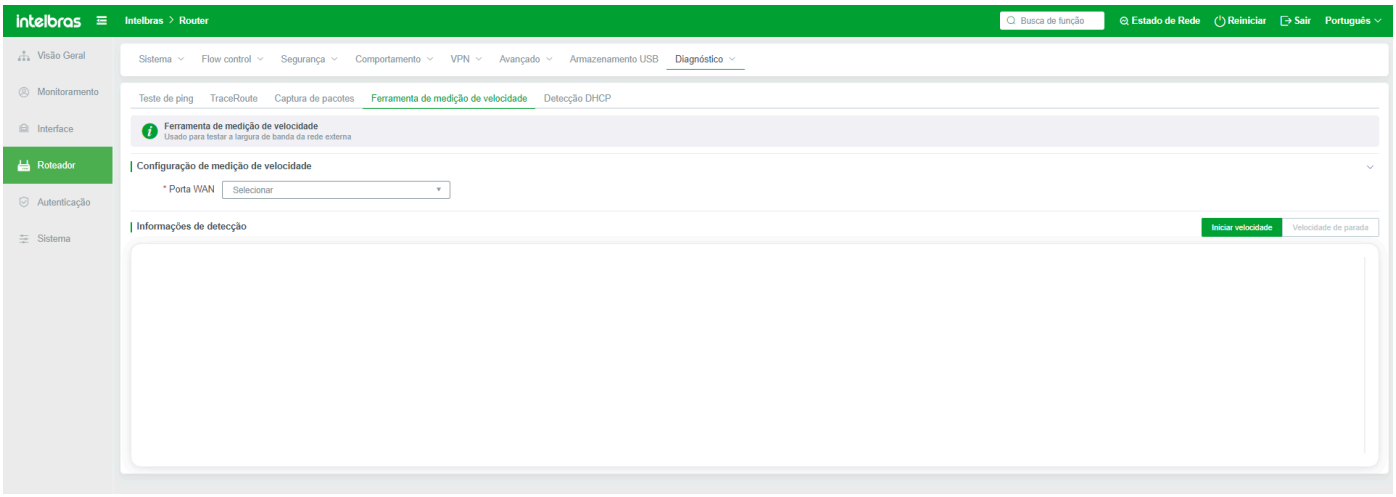
Filtragem de Protocolo: Filtrar através do Protocolo

Tamanho do Arquivo (KB): Tamanho do arquivo salvo



Ferramenta de Medição de Velocidade

Função para verificar as larguras de banda de upload e download nas interfaces WAN. Selecione a porta WAN que precisa de medição de velocidade e clique em "Iniciar medição de velocidade".

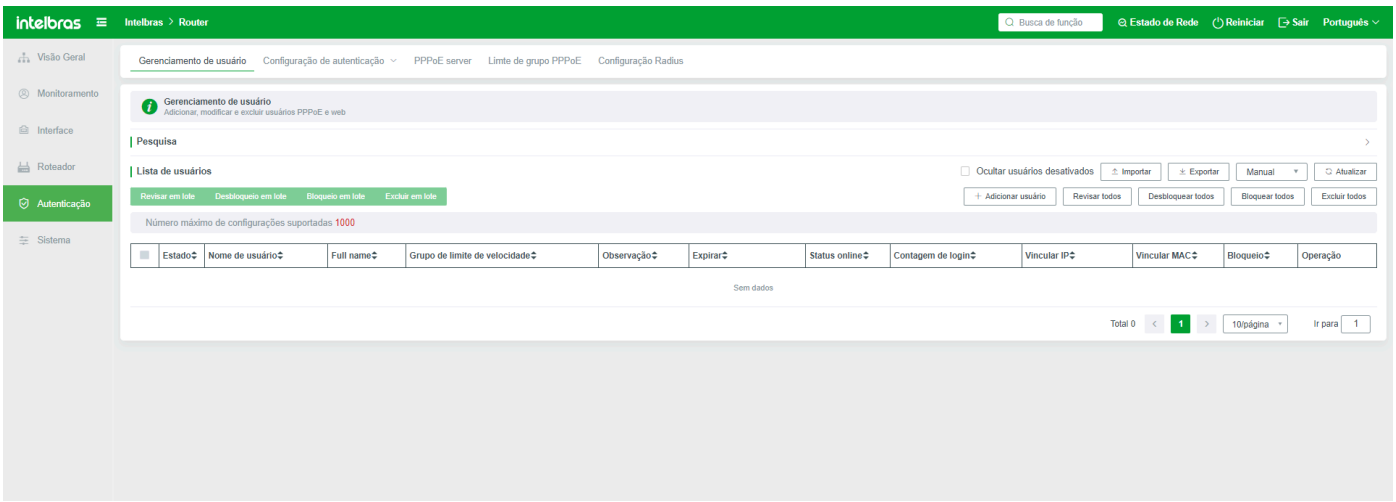


Autenticação

Gerenciamento de Usuários

Quando são necessárias autenticação WEB e funções PPPOE no ambiente de rede, é necessário criar e gerenciar contas de usuário. Este menu é usado para implementar tais funções.

Se uma conta de usuário foi adicionada, você pode visualizar a conta com base nos critérios. Se as condições de filtro estiverem incorretas ou precisarem ser substituídas, clique no botão "Limpar" para limpar as condições de filtro inseridas.



Adicionar (usuário). A autenticação de usuário (conta) adicionada aqui se aplica apenas à autenticação WEB embutida no sistema e à autenticação PPPOE. Não pode ser usado para faturamento em nuvem e autenticação inteligente de WiFi.

Status do usuário: O status da conta do usuário está Ligado ou Desligado. A conta desligada não pode ser usada normalmente.

Trava: Após a seleção deste parâmetro, a conta será bloqueada.

Nome de usuário: Define a conta de usuário. O valor pode conter no máximo 31 caracteres, incluindo letras, dígitos ou uma combinação deles.

Senha: Define a senha de login do usuário.

Modo de login: Seleciona o modo de autenticação para a conta. Uma vez que o modo de autenticação é selecionado, a conta só pode ser usada nesse modo de autenticação. Por exemplo, se a conta usar autenticação WEB, a autenticação de discagem PPPOE não pode ser usada.

Grupo de extensão PPPOE: No modo de discagem PPPOE, pode existir um grupo de extensão PPPOE para o qual a conta pode ser adicionada. Por padrão, o sistema não possui um grupo de extensão. Portanto, é exibido como padrão aqui.

Endereço MAC: Especifica se vincular um endereço MAC à conta. Os endereços MAC podem ser vinculados automaticamente, vinculados manualmente ou não vinculados

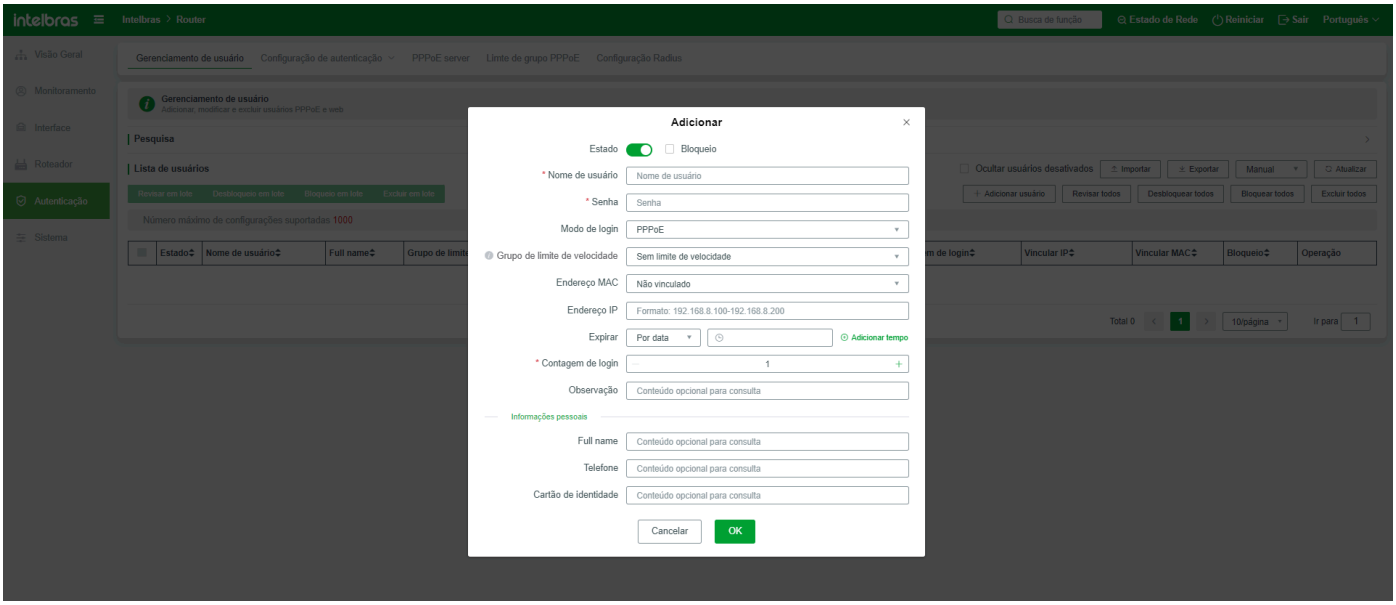
Vinculação automática de MAC: Quando uma conta faz login na Internet pela primeira vez, a conta é automaticamente vinculada ao endereço MAC do terminal em uso. Em seguida, a conta só pode ser usada por terminais com o mesmo endereço MAC. Caso contrário, outros terminais não podem usar a conta.

Vinculação manual de MAC: Insira manualmente o endereço MAC do terminal a ser vinculado. Apenas terminais com este endereço MAC podem usar a conta.

Endereço IP: Se o endereço IP for especificado, a conta só pode ser usada por terminais com este endereço IP. Caso contrário, terminais sem este endereço IP não podem usar esta conta. Se o valor estiver em branco, a conta não está vinculada a um endereço IP.

Expiração (Configuração de tempo): Define o tempo de expiração da conta. Quando a conta expira, a autenticação falha. Você precisa entrar em contato com o administrador para alterar o tempo de expiração. O tempo de expiração pode ser definido de diferentes maneiras, como segue:

Por data: Depois que a data é selecionada na página, a conta expirará na data definida e não poderá ser autenticada para login. Ao selecionar o tempo de expiração rápido, o tempo de expiração é calculado com base na data atual.



Pacote: indica por quanto tempo a conta pode ser usada. A autenticação falha se o período especificado for excedido. Se você selecionar Repetir e definir o intervalo e as vezes, isso indica o intervalo em que a conta pode ser autenticada. Nesse caso, o intervalo é de 5 minutos e o intervalo é de 1 hora, três vezes ao dia. Indica que a conta está disponível por uma hora. Se um terminal desconectar da rede e precisar ser autenticado novamente, só três vezes ao dia pode ser autenticado, e cada intervalo de autenticação deve ser maior ou igual a cinco minutos. Caso contrário, a autenticação falha. Se Repetir não for selecionado, o número de vezes e o intervalo para a conta fazer login novamente não são limitados. Neste tipo de pacote, o tempo não será acumulado após o desligamento da conta, mas apenas quando a conta estiver logada.

Traffic do Pacote: indica o tráfego total disponível da conta. Após o uso do tráfego, não pode ser usado normalmente.

Pacote TIME, tempo offline: igual ao pacote de tempo acima, mas aqui o tempo de pacote

Modo de controle de velocidade: limita a velocidade de upstream e downstream do terminal que usa a conta.

Único: indica que se várias conexões forem permitidas, as velocidades de upstream e downstream dos terminais que fazem login na conta são baseadas no valor definido aqui.

Compartilhamento: Se a conta permitir várias conexões, a soma das velocidades de upstream e downstream de cada terminal prevalece. Ou seja, a soma das velocidades de upstream e downstream não pode exceder o valor definido, e a soma das velocidades de downstream não pode exceder o valor definido.

Limitação de Taxa de Uplink: Define a velocidade de uplink da conta. A velocidade de uplink do terminal que usa a conta é limitada por esse valor.

Limitação de Taxa de Downlink: Define a velocidade de downlink da conta. A velocidade de downlink do terminal que usa a conta é limitada por esse valor.

Número de usuários logados: indica quantos terminais podem fazer login em uma conta ao mesmo tempo. A entrada 2 indica que dois terminais podem fazer login ao mesmo tempo sem afetar um ao outro.

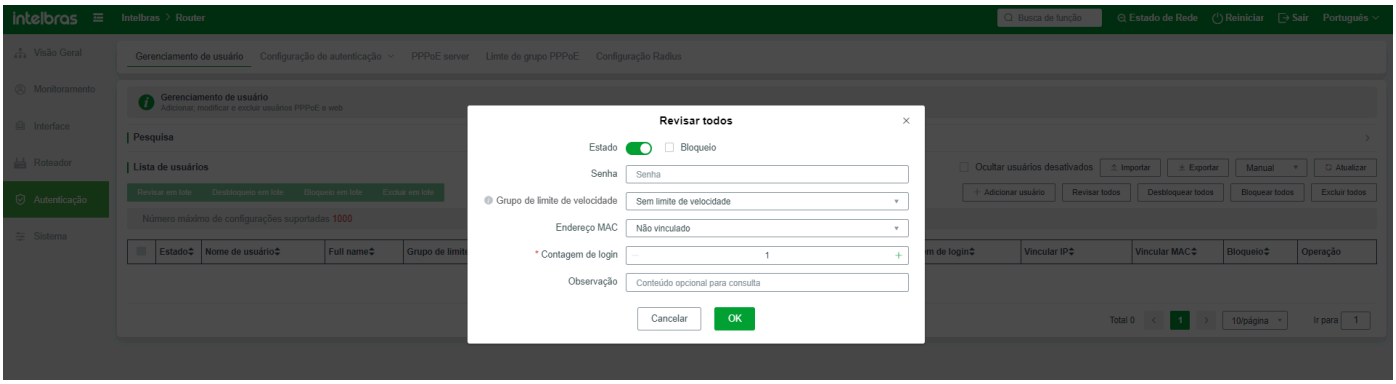
VLANID: Especifica se vincular o VLANID. Se precisar vincular o VLANID, você pode vincular automaticamente ou manualmente. Para mais detalhes, consulte Vinculação de Endereço MAC.

Informações pessoais: Crie uma conta de usuário. Se precisar preencher as informações da conta, você pode preencher o nome, número de telefone, informações de cartão de identificação e observações do titular da conta aqui.

Importar: Importe informações da conta do usuário. Se não houver conta de usuário no sistema, o conteúdo do arquivo exportado estará vazio. Você pode adicionar uma conta aqui e enviá-la antes de exportá-la e adicionar uma nova conta ao arquivo exportado para salvar a importação.

Exportar: Você pode exportar a conta atual.

Modificar todos: Clique neste botão para modificar parte da conta sem verificar a lista de usuários da conta. Veja abaixo:

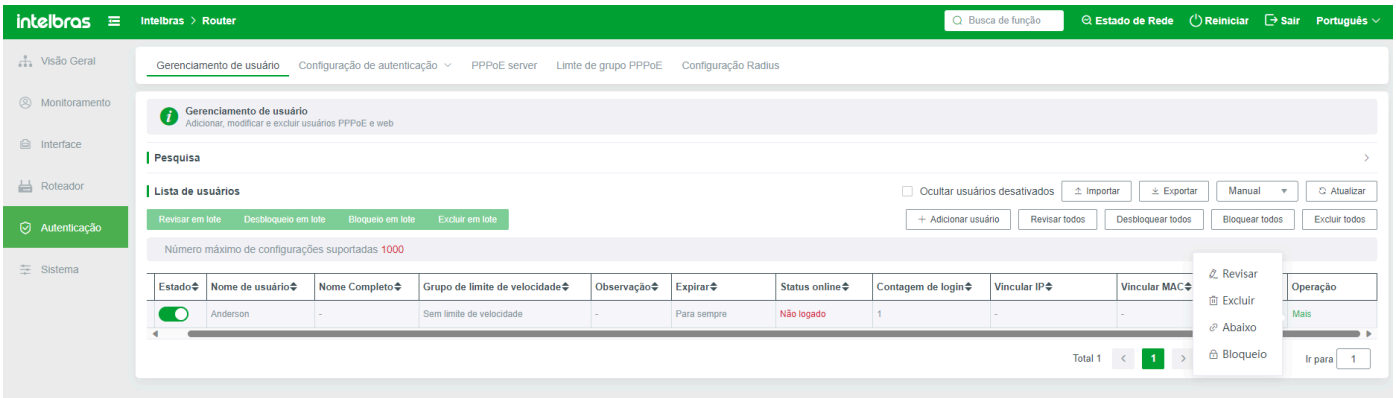


Todos desbloqueados: Uma conta de usuário só pode ser desbloqueada quando estiver bloqueada. A conta desbloqueada pode ser excluída.

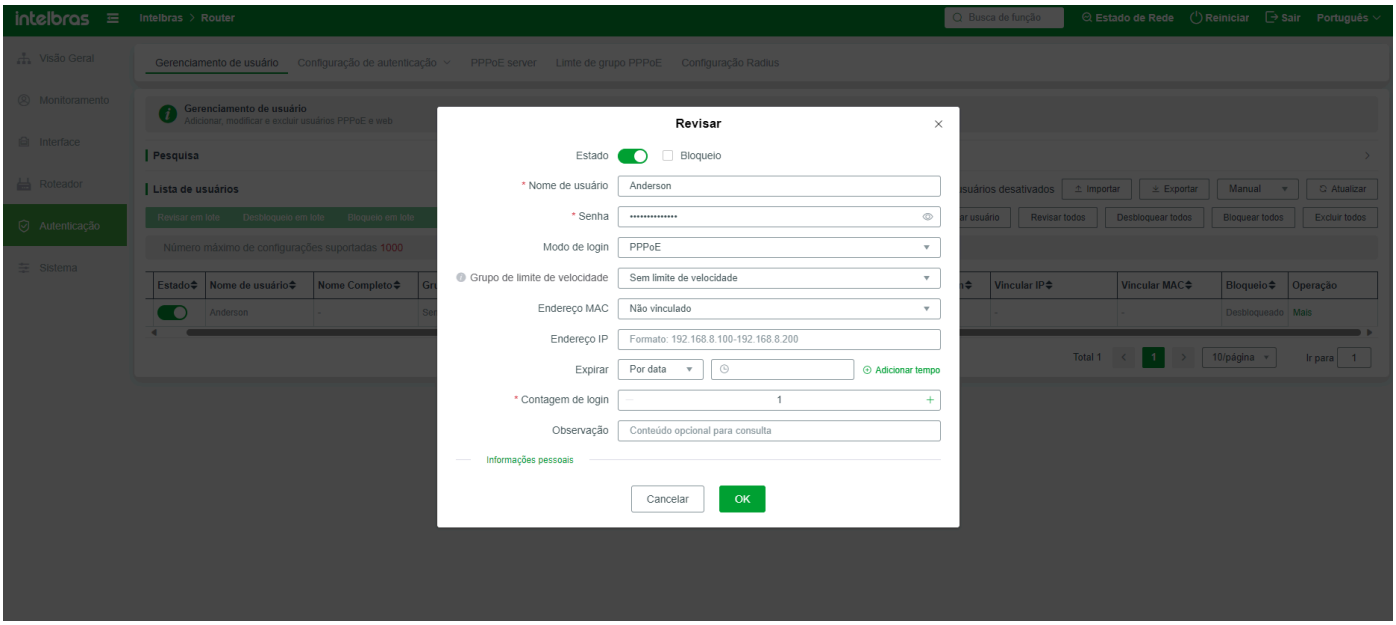
Bloquear todos: A conta bloqueada não pode ser excluída ou restaurada para o padrão.

Excluir todos: Contas online e bloqueadas não podem ser excluídas. Portanto, clicar em Excluir Todos excluirá apenas contas offline, expiradas e desbloqueadas.

A barra de operações do usuário permite que você modifique um único usuário



Modificar usuário: Modifica os parâmetros de configuração da conta. Se você definir o status de um usuário online como desativado ou alterar o nome de usuário ou a senha, a conta será desconectada imediatamente após fazer login no terminal.



Excluir um usuário: Exclui uma conta de usuário. A conta excluída não pode ser restaurada. Contas online e bloqueadas não podem ser excluídas.

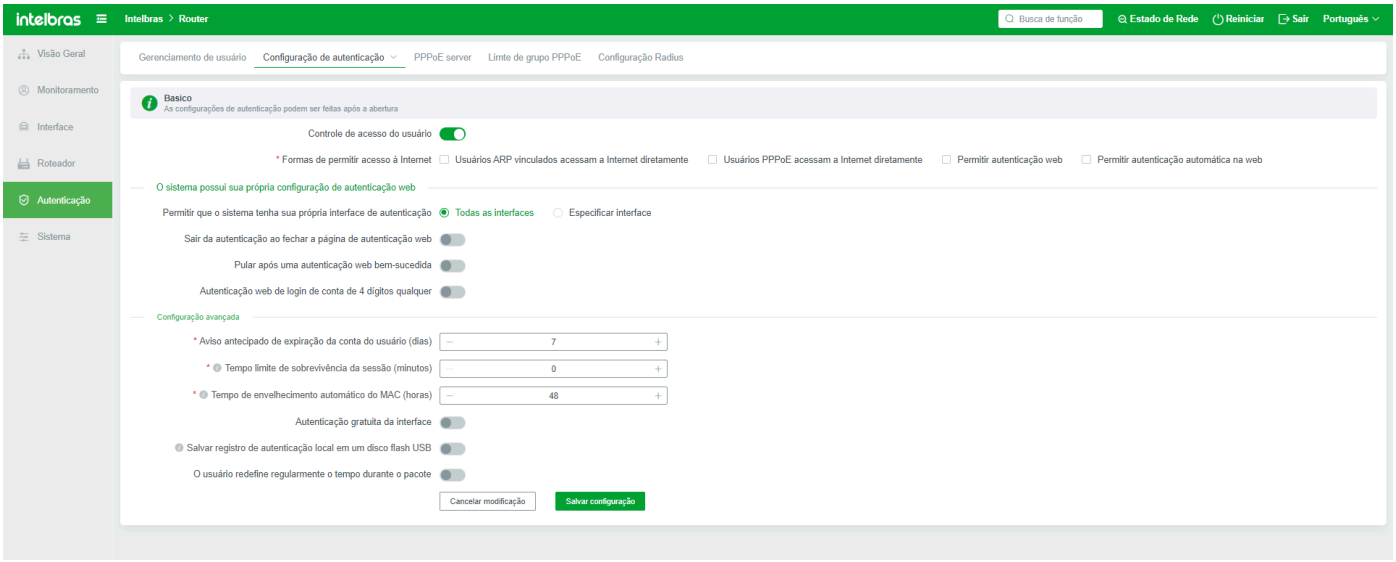
Desconectar o usuário: Se o status de acesso à Internet da conta atual estiver "Login", clique no botão para desconectar o usuário, e o terminal correspondente ficará offline.

Desbloquear um usuário: Se a conta atual estiver bloqueada, clique neste botão para desbloquear a conta.

Configurações de Autenticação

Configurações Básicas

Ative a configuração básica de faturamento ou da função Wi-Fi inteligente após a ativação da função correspondente, a configuração será concluída automaticamente. Se você só precisar usar a função local de autenticação WEB, sem precisar habilitar outras autenticações, apenas selecione "Sistema de Certificação WEB" neste menu para determinar a disposição básica, principalmente para configurações relacionadas à certificação.



Controle do Modo de Acesso à Internet do Usuário: A configuração da próxima regra pode ser realizada somente quando está habilitada. Quando o sistema de faturamento ou a função de Wi-Fi inteligente está ativado, o controle do modo de acesso à Internet do usuário é habilitado automaticamente.

Modo de Acesso à Internet: Configura o modo de acesso à Internet para o usuário. Quando a função de Wi-Fi inteligente ou de faturamento está ativada, o sistema seleciona automaticamente "Acesso Direto do Usuário PPPOE", "Permitir Autenticação WEB para Acesso à Internet" e "Permitir Autenticação Automática WEB para Acesso à Internet".

Geralmente, se a autenticação WEB (página) for usada, selecione "Permitir autenticação WEB para acesso à Internet" e "Permitir autenticação automática WEB para acesso à Internet". Para habilitar a autenticação WEB para acesso à Internet e permitir que o portal WEB seja exibido normalmente, habilitar a autenticação WEB automática para acesso à Internet significa que o terminal se conecta à rede original dentro do intervalo de tempo de envelhecimento do MAC. Não é necessário inserir um nome de usuário ou senha para autenticação.

Tipo de Autenticação WEB: Seleciona um tipo de autenticação WEB

Autenticação WEB Incorporada: O sistema possui autenticação WEB incorporada. Se você selecionar esta opção e selecionar "Permitir Autenticação WEB para Acesso à Internet" e "Permitir Autenticação Automática WEB para Acesso à Internet" no modo de autenticação, o seguinte portal é exibido no terminal conectado à rede local na LAN:

Autenticação WEB de Terceiros: geralmente, refere-se à autenticação da função de faturamento do sistema e à função de autenticação inteligente de Wi-Fi.

O sistema possui autenticação WEB de terceiros: o sistema possui autenticação WEB incorporada, autenticação de faturamento e autenticação inteligente de Wi-Fi.

Configurações Avançadas

Aviso de expiração da conta do usuário com antecedência (dias): Geralmente, é usado para a autenticação WEB fornecida pelo sistema. O aviso de expiração da conta é definido vários dias antes. A página correspondente pode ser personalizada e melhorada.

Tempo limite da sessão (minutos): Se um usuário for detectado como inativo e exceder a duração máxima predefinida, o usuário será desconectado à força e precisará ser autenticado novamente.

Tempo de Envelhecimento da Autenticação Automática MAC (H): Depois que um usuário é autenticado offline, a autenticação é isenta quando o usuário volta a ficar online dentro do tempo de envelhecimento especificado. Se o usuário acessar a rede após o tempo de envelhecimento, o usuário precisará ser autenticado novamente.

Isenção de autenticação de interface: Os usuários terminais que acessam a interface selecionada podem acessar a Internet sem autenticação.

Salvar logs de autenticação local no pen drive USB: Após a ativação desta função, quando um dispositivo de roteamento está conectado ao pen drive USB e a função local de autenticação WEB está ativada, os logs de autenticação WEB local gerados são salvos no pen drive USB.

Duração de Reset do Usuário do Tempo do Pacote: O usuário pode redefinir a duração online em um horário especificado.

Certificação Gratuita

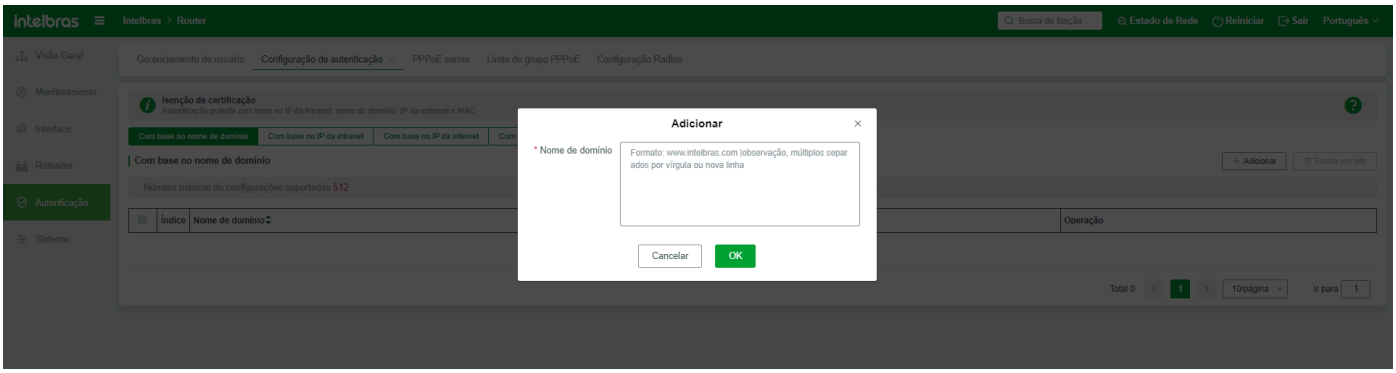
Você pode configurar a lista branca com base no endereço IP da Intranet, nome de domínio, endereço IP da extranet e endereço MAC neste menu. Terminais na lista branca podem acessar a Internet sem autenticação.

1. Com base no nome de domínio

Se algum modo de autenticação (autenticação WEB, Wi-Fi inteligente e sistema de contabilidade) estiver habilitado no sistema, os terminais na LAN não conseguirão acessar todos os endereços da web. No entanto, se o nome de domínio inserido aqui for inserido, os terminais não serão bloqueados e poderão acessar diretamente.

O formato do nome de domínio deve estar em conformidade com o formato padrão. Você pode inserir apenas um nome de domínio por vez no campo de entrada. Se for necessário incluir vários nomes de domínio na lista branca, adicione mais regras.

Se for necessário excluir nomes de domínio da lista branca em lotes, selecione este parâmetro e clique em Excluir em Lote. Os nomes de domínio excluídos não podem ser recuperados.

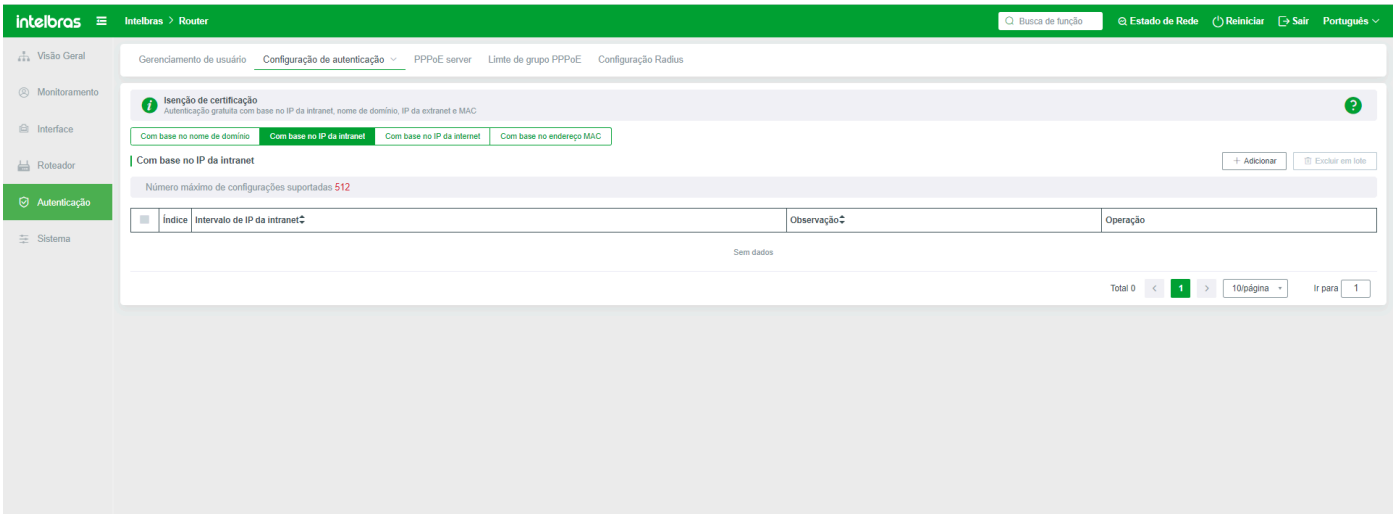


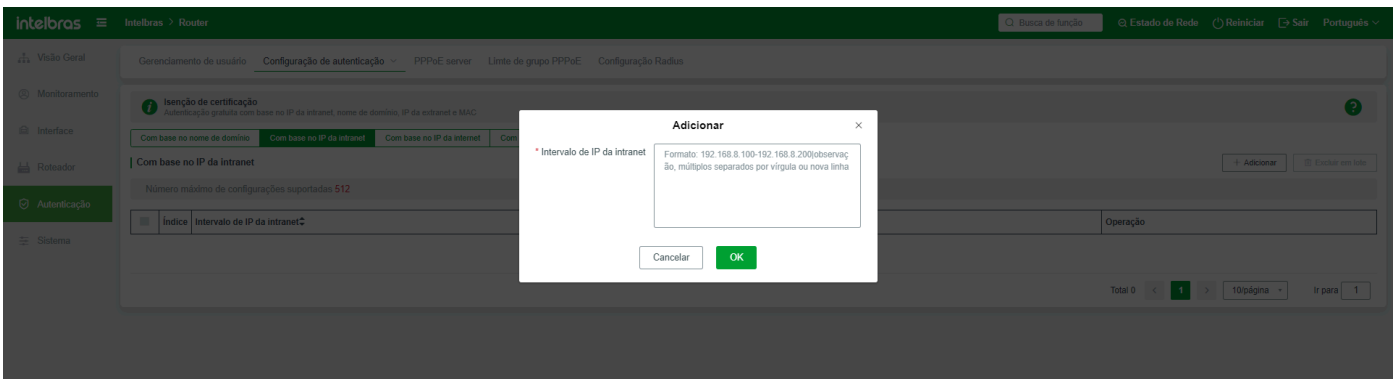
2. Com base no endereço IP da Intranet

Por exemplo, o endereço IP do telefone celular é 192.168.1.101. Após a ativação da função de autenticação, o terminal cujo endereço IP é 1.101 pode ser autorizado a acessar a Internet sem autenticação. O usuário na lista branca é exibido como Permitir no Status Online na Lista de Usuários monitorada pelo host.

O endereço IP da Intranet pode ser um único endereço IP ou um segmento de endereços IP.

Para excluir determinados ou certos endereços IP da Intranet na lista branca, selecione e clique em Excluir em Lote e confirme.



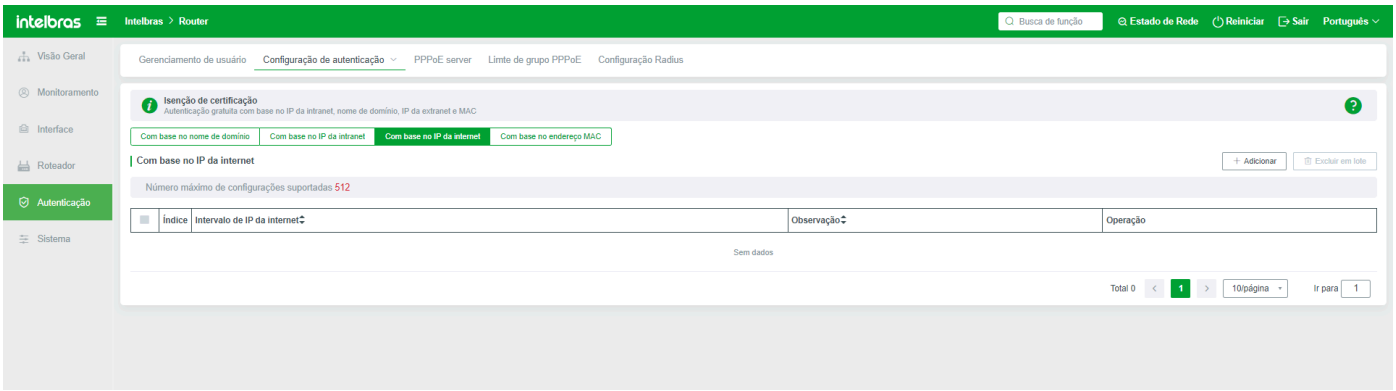


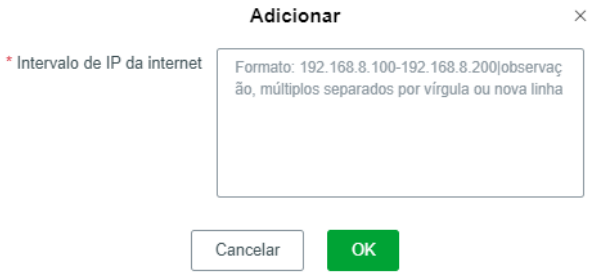
3. Com base no endereço IP da Extranet

Similar à inclusão de endereços IP com base em nomes de domínio, se desejar incluir endereços IP externos na lista branca, insira os endereços IP a serem permitidos neste menu. Você pode inserir um único endereço IP ou um segmento de endereços IP no campo de entrada.

Se desejar excluir a lista branca de endereços IP da rede externa, selecione-a primeiro, clique em Excluir em Lote e clique em OK.

Se for necessário alterar o endereço IP inserido, modifique-o na barra de operações da lista.





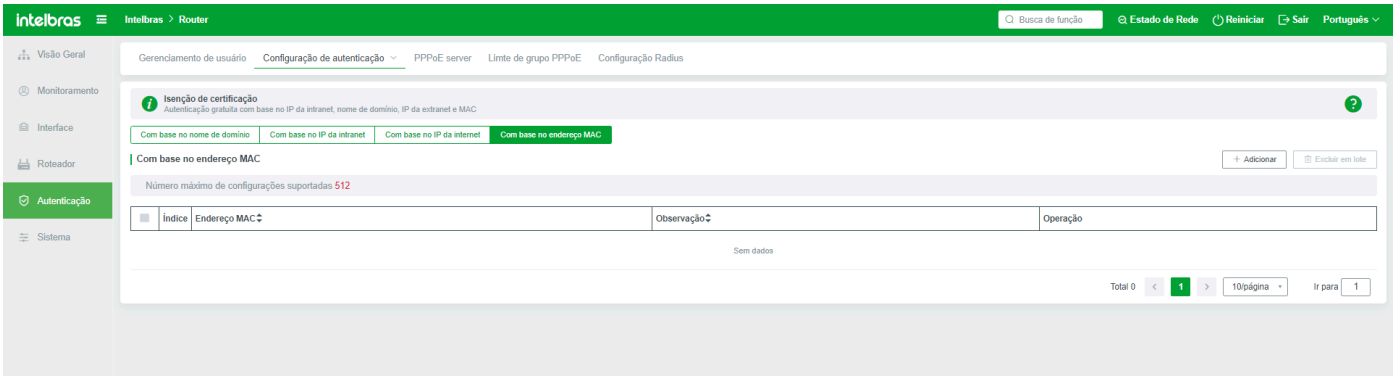
4. Com base no endereço MAC

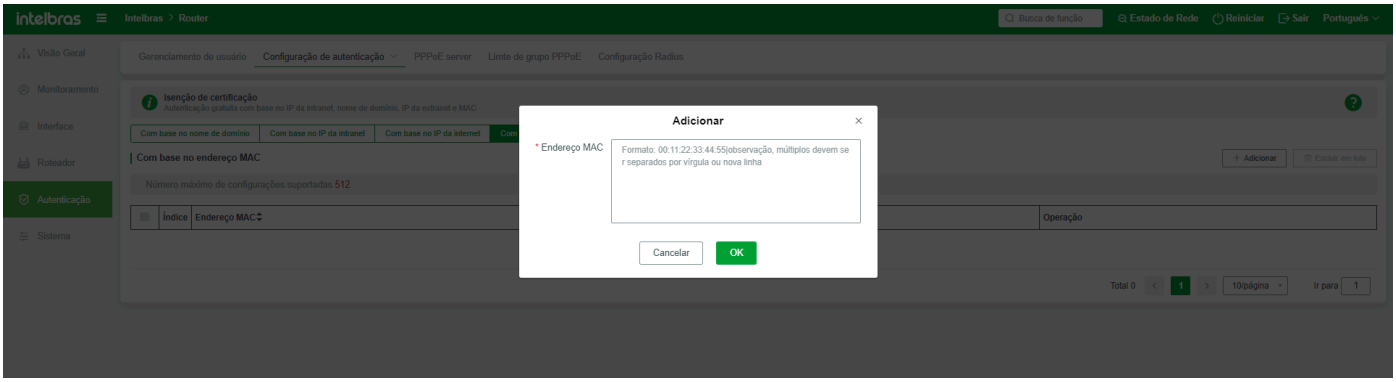
Os endereços IP da Intranet são frequentemente alterados devido ao reacesso dos usuários terminais após a desconexão. Como resultado, a lista branca com base nos endereços IP da Intranet não tem efeito. É criada uma lista branca com base no endereço MAC. O endereço MAC é o endereço MAC do terminal, que não muda.

Da mesma forma, os usuários terminais na lista branca de endereços MAC podem acessar a Internet sem autenticação.

Para excluir a lista branca de endereços MAC, selecione-a, clique em Excluir em Lote e clique em OK.

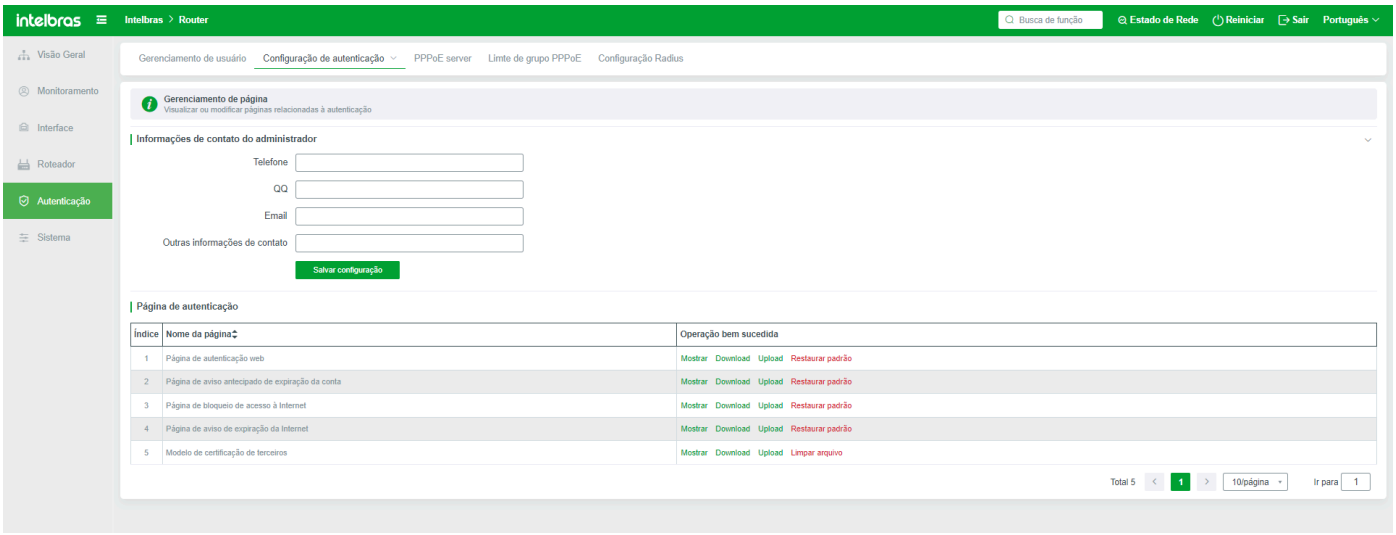
Você pode modificar o endereço MAC na barra de operações da lista de endereços MAC.





Gerenciamento de Páginas

É usado para gerenciar a página de autenticação WEB do sistema, por exemplo, configurar o conteúdo de notificação antecipada de expiração, as informações de contato do administrador e modificar o conteúdo da página de autenticação WEB. Se nenhuma modificação for necessária, use o modelo padrão do sistema.



Informações de Contato do Administrador: Geralmente, as informações de contato do administrador são exibidas na página de aviso de expiração, para que os usuários que usam a autenticação WEB incorporada do sistema possam entrar em contato com o administrador, renovar suas taxas ou resolver outros problemas. As informações de contato incluem telefone, QQ, e-mail e outras informações de contato, que também podem ser deixadas em branco.

Página de Autenticação: Esta página é usada para autenticação WEB.

Página de Notificação de Expiração da Conta: O tempo de notificação de expiração é definido nas Configurações Básicas. Uma vez que a notificação de expiração é acionada, a seguinte mensagem é exibida quando o terminal que usa o sistema de autenticação WEB abre o site http. Onde "0" dia é o tempo antecipado de expiração definido:

Página de aviso para bloquear o acesso à Internet:

Página de notificação de expiração: Quando o tráfego da conta ou os recursos de pacotes são esgotados, a seguinte mensagem é exibida quando o terminal abre a página da web:

Cada barra de operações de página pode ser usada para operar a página correspondente

Visualizar: O mesmo que a função de visualização, você pode visualizar o conteúdo atual da página e o layout;

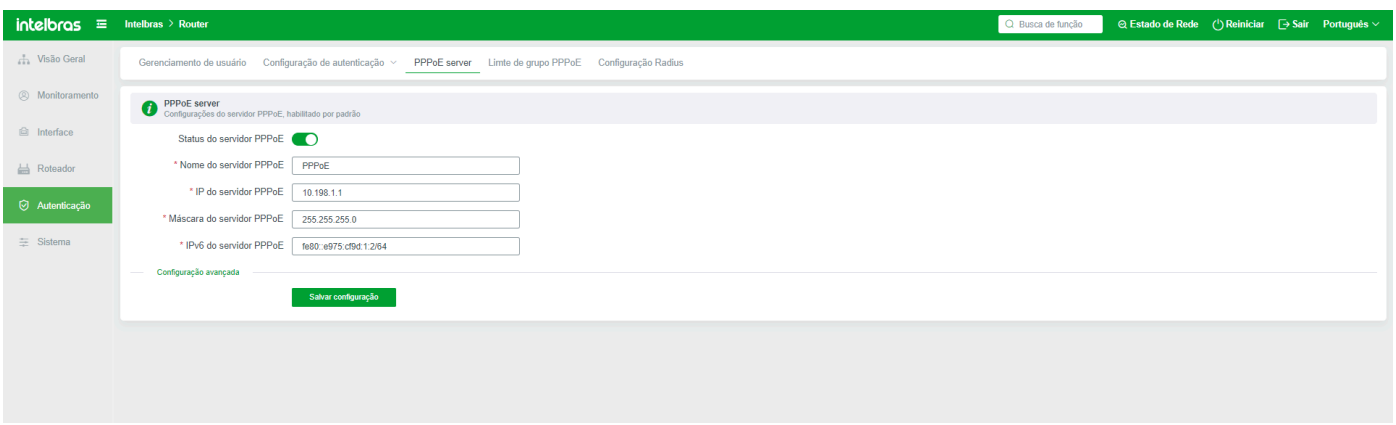
Baixar: Após o download da página atual, você pode modificar o conteúdo de texto na página. Caso contrário, o upload falhará. Salve a modificação antes de fazer o upload.

Upload: Com base no download e na salvação do conteúdo modificado, faça o upload para o sistema, e a página usará o conteúdo modificado no cenário correspondente.

Restaurar o padrão: Para restaurar o conteúdo da página modificado ao status padrão, clique neste botão.

Servidor PPPOE

Se a função PPPOE for necessária na configuração de rede e o servidor funcionar como servidor PPPOE, configure o servidor aqui.



Status do Servidor PPPOE: Geralmente, o sistema habilita o servidor PPPOE por padrão. Se o servidor estiver desativado, o usuário PPPOE não conseguirá discar.

Nome do Servidor PPPOE: Personalize o nome do servidor PPPOE. O nome padrão pode ser usado.

Endereço IP do Servidor PPPOE: Indica o endereço IP do servidor PPOE. Um usuário PPPOE pode acessar a página de login WEB do servidor por meio deste endereço IP. Se o endereço IP do servidor PPPOE de camada inferior for o mesmo que o endereço IP do servidor de camada superior, altere o endereço IP de um dos servidores PPPOE para evitar conflitos.

Máscara de Sub-rede do Servidor PPPOE: Indica a máscara de sub-rede do servidor PPPoE. A máscara de sub-rede pode ser alterada com base nos requisitos do ambiente.

Endereço IPv6 do Servidor PPPOE: Se a função PPPOE IPV6 for necessária, você pode configurar um endereço IPV6 aqui. O endereço padrão pode ser usado. Se ocorrer um conflito de endereço, modifique conforme necessário.

Configurações Avançadas

Permitir acesso a qualquer nome de servidor: Se esta função estiver habilitada, o nome do servidor inserido pelo cliente durante a discagem PPPOE não será verificado. Caso contrário, o nome do servidor precisa ser verificado.

Acesso somente PPPOE: Após esta função ser habilitada, apenas usuários de discagem PPPoE podem acessar o roteador e a Internet. Além disso, apenas os endereços do servidor PPPOE podem acessar a interface WEB do roteador. Se o endereço IP da porta LAN for usado, a interface WEB do roteador não poderá ser acessada.

Servidor DNS Preferencial: Especifica o endereço do servidor DNS atribuído pelo servidor PPPOE ao cliente.

Servidor DNS de Backup: Especifica o endereço do servidor DNS atribuído pelo servidor PPPOE ao cliente.

Tempo de Detecção de Inatividade (s): Após o tempo especificado, se não houver comunicação de dados entre o cliente e o servidor, o sistema começa a detectar se o cliente está offline. O valor padrão é de 3 segundos. O valor varia de 3 a 180 segundos.

Quantas solicitações de detecção não são respondidas antes da desconexão: Após um número definido de solicitações, o cliente é desconectado se não houver resposta à comunicação de dados. O valor padrão é de 3. O valor varia de 3 a 180.

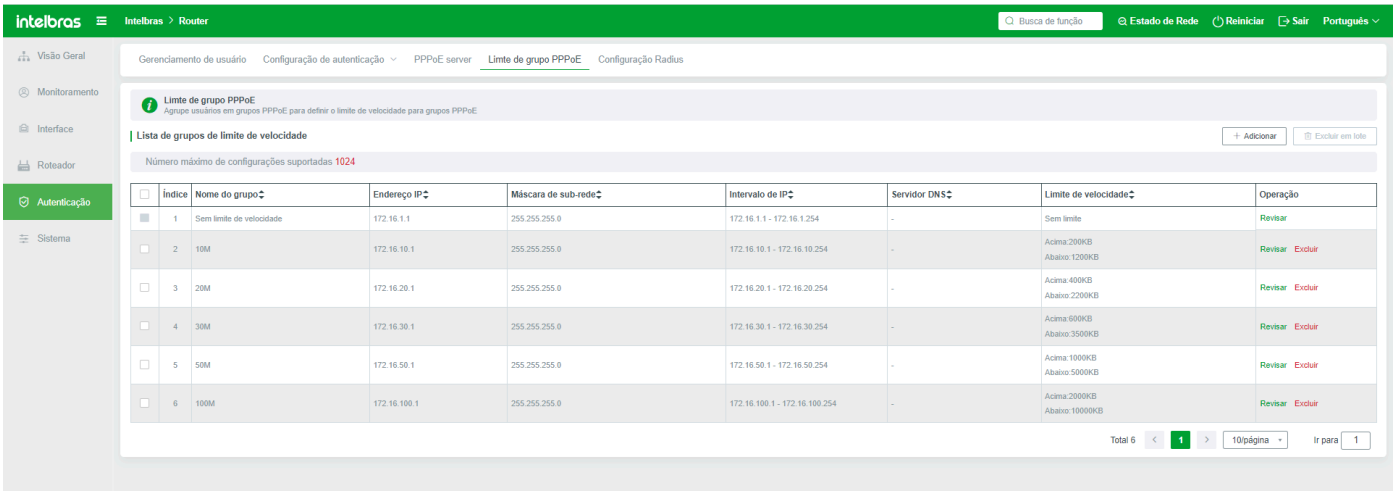
Modo de Autenticação: Modos de autenticação diferentes estão disponíveis para ambientes de aplicativos diferentes. Para PCS gerais, o modo PAP é usado. Se o roteador de nível inferior for usado para discagem, você pode selecionar todos os modos de autenticação.

Login com qualquer conta: Após esta função ser habilitada, o servidor não verificará com precisão as informações da conta de discagem do terminal. Os usuários podem ser autenticados inserindo qualquer conta ou senha.

Grupo de Limite PPPOE

Você pode adicionar vários pools de endereços PPPOE para distinguir diferentes tipos de usuários, facilitando a restrição de largura de banda ou restrição de acesso para diferentes tipos de usuários.

Adicionar um grupo de extensão PPPOE



Nome do Grupo: Nome do grupo definido pelo usuário, configurado conforme necessário.

Endereço IP: Insira o endereço IP do servidor PPPOE. Para um servidor recém-expandido, insira o endereço IP do novo servidor. Observe que o endereço IP do servidor não pode entrar em conflito com o endereço IP de outros locais.

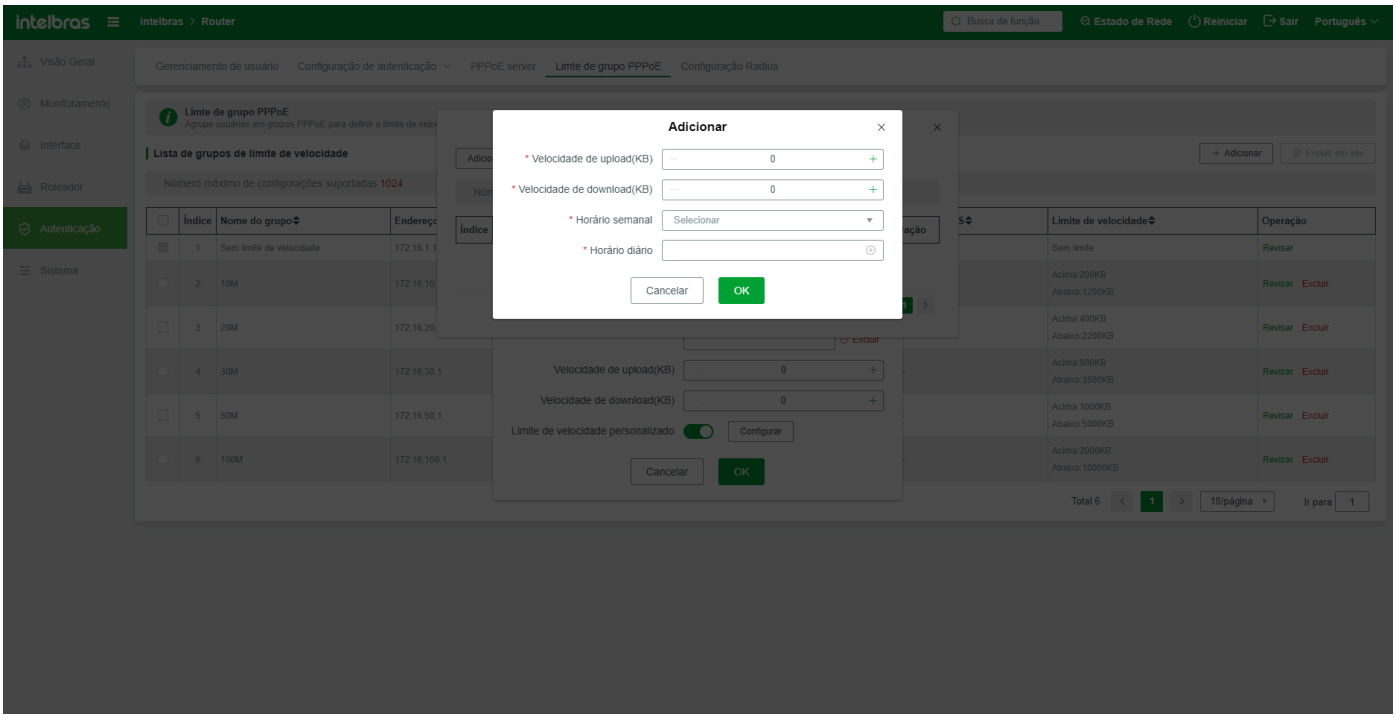
Máscara de Sub-rede: O valor padrão é normal. Se mais de 254 usuários usarem este pool de endereços, você pode alterar o segmento de máscara de sub-rede conforme necessário.

Servidor DNS: Especifica o endereço do servidor DNS atribuído aos usuários terminais.

Velocidade de Uplink: Limita a velocidade de uplink dos usuários no grupo.

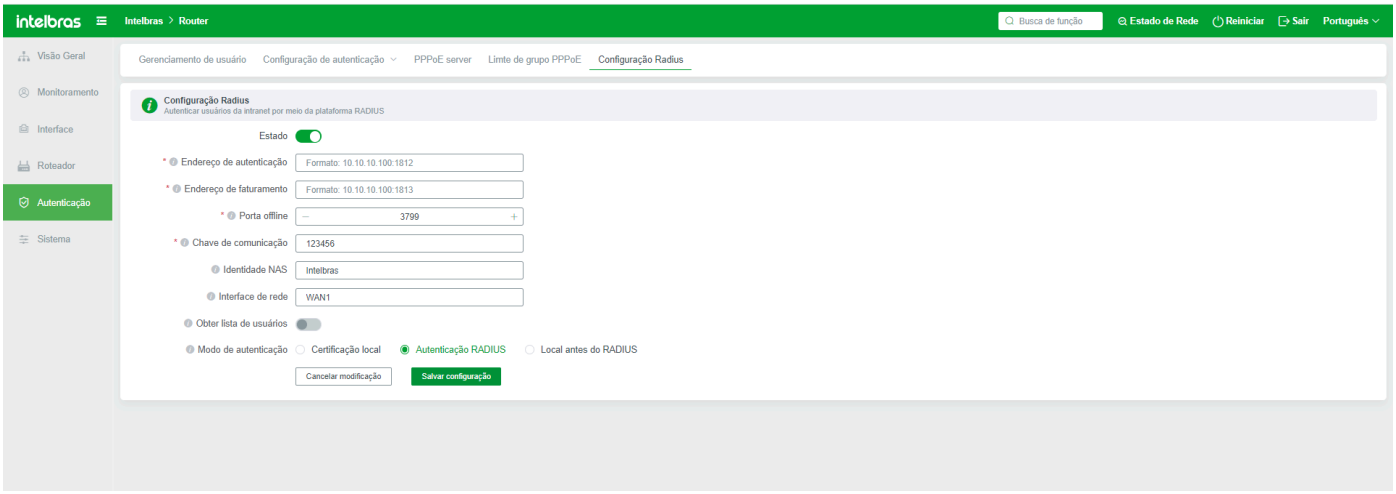
Velocidade de Downlink: Limita a velocidade de downlink dos usuários neste grupo.

Limite de Taxa Definida pelo Usuário: Limita a velocidade de uplink e downlink das contas em um intervalo de tempo especificado.



Configuração do Radius

O protocolo RADIUS fornecido com o protocolo padrão do sistema pode se conectar a servidores RADIUS padrão para autenticação e contabilidade.



Status: A autenticação RADIUS é desativada por padrão. As regras podem ser configuradas apenas depois que a autenticação RADIUS é habilitada. Após a habilitação da autenticação RADIUS, você precisa clicar em Salvar Configuração.

Endereço de Autenticação: Indica o endereço IP e o número da porta do servidor RADIUS. O formato é 10.10.10.1:1812.

Endereço de Contabilidade: Indica o endereço do servidor de contabilidade e a porta do servidor RADIUS. O endereço IP e a porta são os mesmos fornecidos pelo servidor. O formato do endereço IP e da porta é 10.10.10.1:1813.

Porta Offline: O servidor RADIUS envia comandos offline para esta porta. Verifique o número da porta com o servidor ao preencher o comando.

Chave de Comunicação: O valor deve ser o mesmo que a chave de comunicação fornecida pelo servidor e deve ser confirmado pelo servidor.

ID NAS: Insira o ID do servidor de destino.

Interface de Rede: indica a interface pela qual os dados RADIUS fluem para fora do sistema atual. Por exemplo, LAN, WAN1, WAN2, VPN1, VPN2 e OVPN, separe várias interfaces com vírgulas (,).

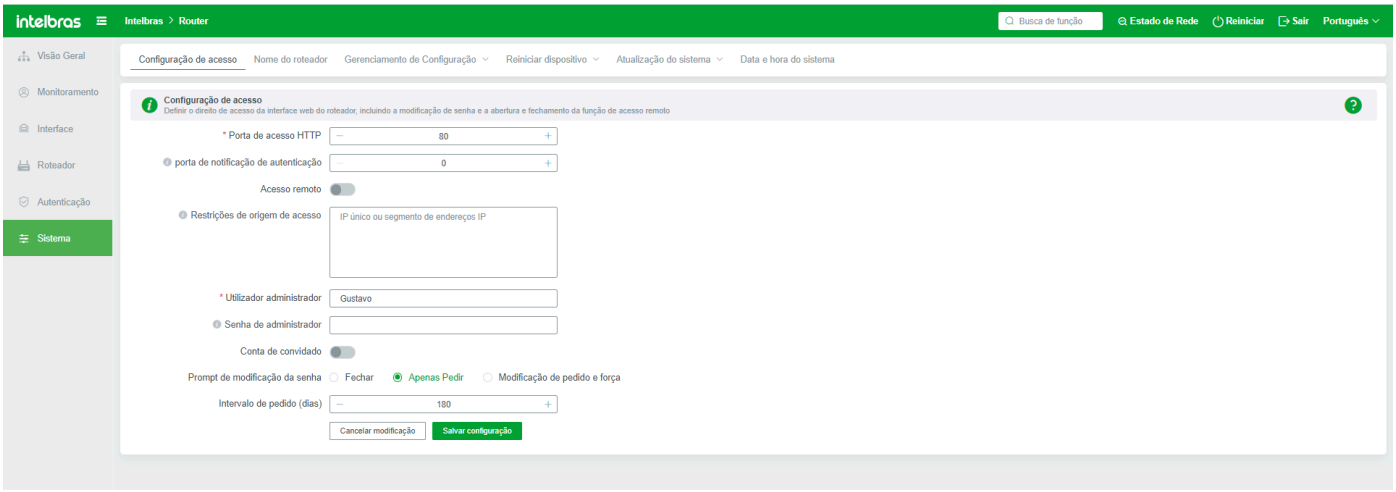
Obtendo a Lista de Usuários: Após a ativação desta função, o sistema obtém a lista de contas de usuário do servidor e suporta apenas a criptografia PAP.

Modo de Autenticação: O próprio roteador ou o servidor Radius pode ser usado para autenticação. A limitação de taxa entregue pelo servidor RADIUS tem prioridade sobre o servidor local.

Sistema

Configurações de Acesso

Defina a permissão de acesso à interface WEB do roteador, incluindo a alteração da senha e a ativação e desativação da função de acesso remoto.



Porta HTTP: Porta usada pela LAN local para acessar o roteador. O valor padrão é 80.

Acesso Remoto: Marque para ativar o acesso remoto. Após a ativação do roteador, a interface de controle WEB do roteador é acessível na WAN, facilitando a manutenção remota pelo administrador. Por padrão, está desativado.

Restrição de Endereço de Origem de Acesso: O endereço inserido não pode acessar o endereço remoto do sistema.

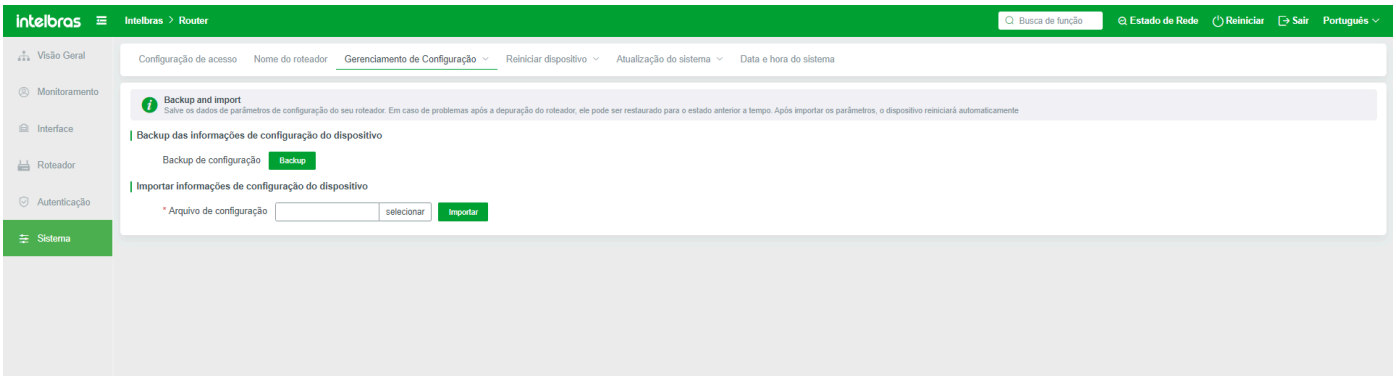
Senha do Administrador: Senha do administrador definida pelo usuário. Esta senha tem a autoridade de gerenciamento mais alta no roteador. Por padrão, o sistema não precisa definir ou modificar a conta, e a conta é root por padrão.

Conta de Visitante: A conta de visitante refere-se a uma conta de administrador comum. A conta de gerenciamento comum original não tem a autoridade mais alta. Portanto, o proprietário desta conta só pode visualizar a configuração do sistema, mas não tem autoridade para modificar o sistema.

Gerenciamento de Configuração

Backup e Importação

Você pode salvar os dados de parâmetros de configuração do roteador para que o roteador possa ser restaurado para o estado de configuração anterior em tempo hábil se ocorrer uma falha após a depuração. Observe que o dispositivo reinicia automaticamente após a importação dos parâmetros.

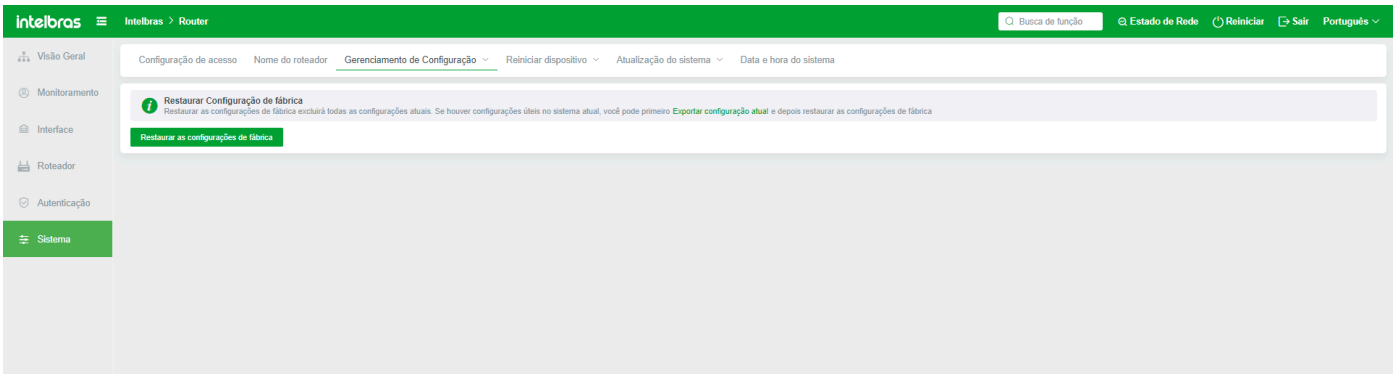


Fazer backup das informações de configuração do dispositivo: Se desejar fazer backup de parâmetros, clique em "Fazer Backup" e os parâmetros serão baixados para o navegador. Você pode visualizar ou mover o arquivo baixado no menu "Download".

Importar informações de configuração do dispositivo: Se precisar restaurar parâmetros após o dispositivo ser restaurado para o padrão, clique em Selecionar para selecionar o arquivo de parâmetros salvo e clique em Importar. Após a restauração dos parâmetros, o dispositivo reinicia automaticamente.

Restaurar Configurações de Fábrica

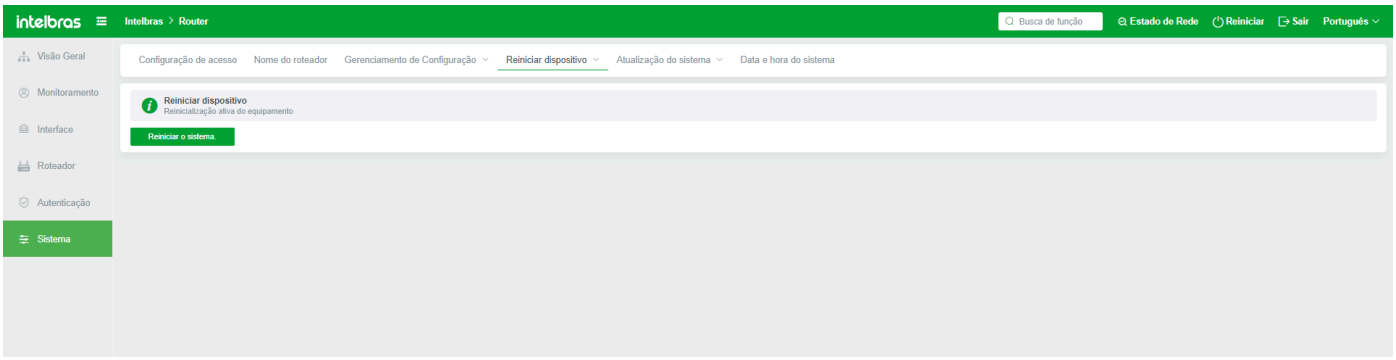
Restaurar as configurações de fábrica exclui todas as configurações atuais. Se o sistema atual tiver configurações úteis, exporte as configurações atuais e restaure as configurações de fábrica.



Reinício do Dispositivo

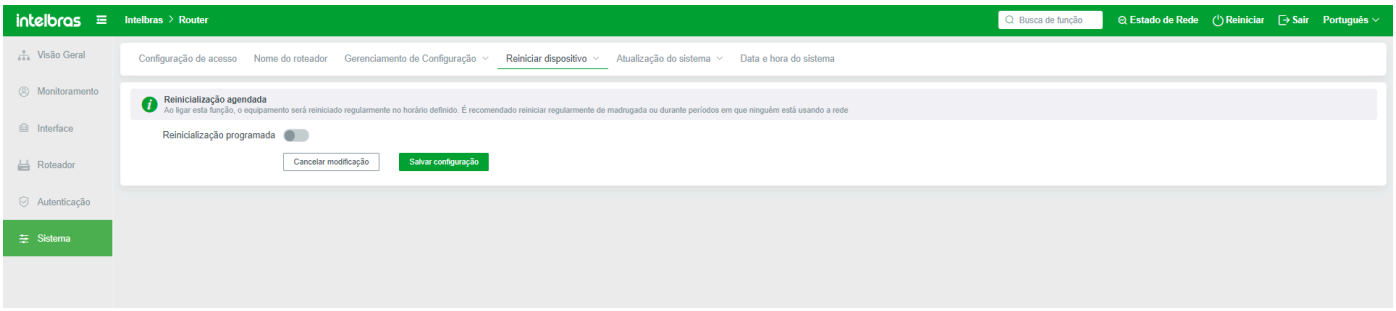
Reiniciar o Dispositivo Manualmente

Reinicie manualmente o dispositivo no software. Reiniciar o dispositivo não limpará os parâmetros configurados. A rede é desconectada automaticamente durante o reinício do dispositivo. Tenha cuidado ao realizar esta operação.

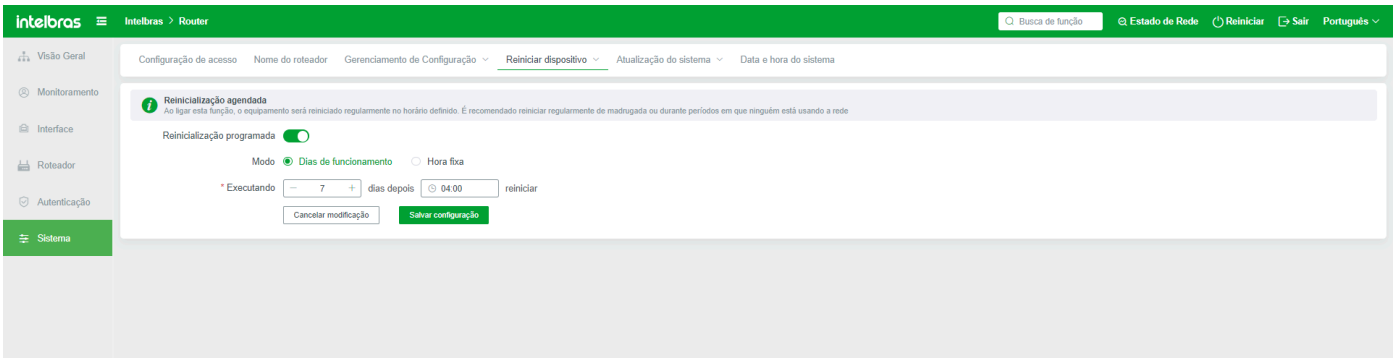


Reinício Agendado

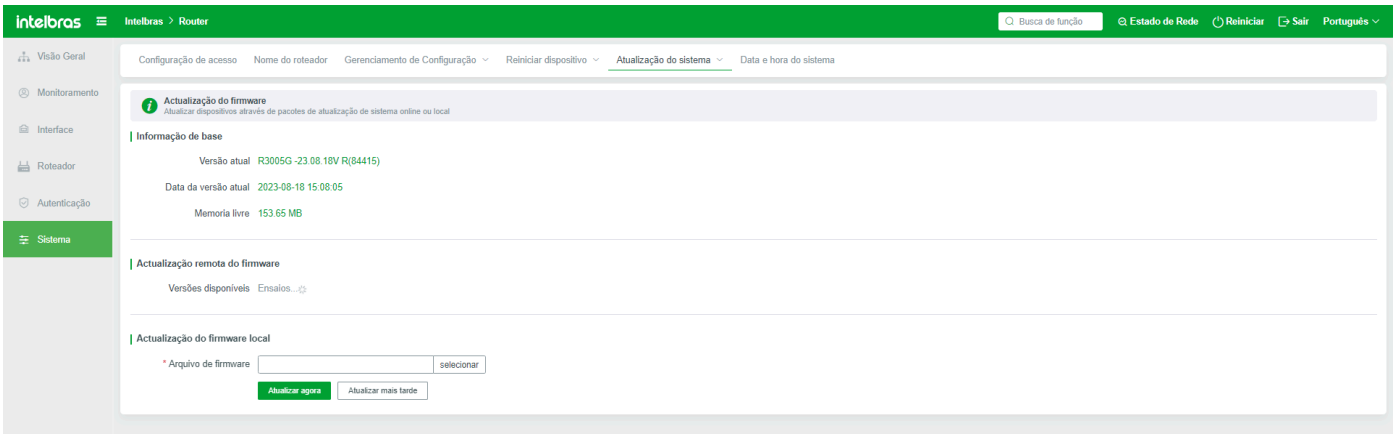
Se esta função estiver habilitada, o sistema reiniciará em um horário especificado. É recomendável reiniciar o sistema ao amanhecer ou quando ninguém estiver usando a rede. Por padrão, o reinício agendado está desativado. Você pode criar uma regra de reinício agendado apenas após ativá-lo.



Modo: Dias de Funcionamento: especifica o número de dias durante os quais o sistema funciona e reinicia o dispositivo em um horário especificado.



Horário Fixo, especifique o horário de reinício fixo, em qual dia da semana;



Após definir a regra de reinício periódico, salve a configuração; caso contrário, a regra não terá efeito. Se o reinício periódico estiver desativado, a regra de reinício periódico não terá efeito.

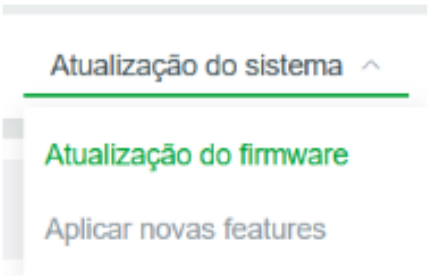
ATUALIZAÇÃO DE SOFTWARE

ATUALIZAÇÃO REMOTA PELA INTERNET

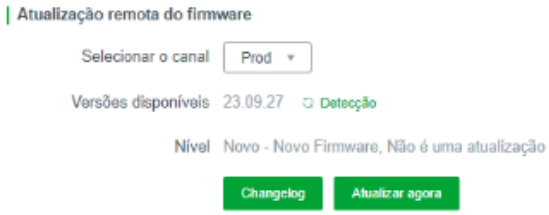
» Acesse a interface WEB do produto.

» No menu lateral esquerdo, clique em “Sistema”.

» Agora no menu superior, vá em “Atualização do sistema” > “Atualização do firmware”.



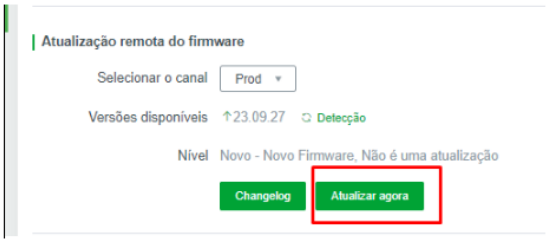
» Em “Atualização remota do firmware”, clique em “detecção”, e aguarde mostrar as versões disponíveis.



» Caso não apareça verifique a sua conectividade de rede com a internet para cronos.intelbras.com.br.

» Ao aparecer a versão, se estiver na última versão, o campo “Versão atual” em “informações de base” ficará em verde. Caso haja uma versão mais nova, ficará em vermelho com a mensagem “Desatualizada!”

» Para atualizar para a última versão, clique em “Atualizar agora” e aguarde o produto reiniciar.



Atualização do Sistema

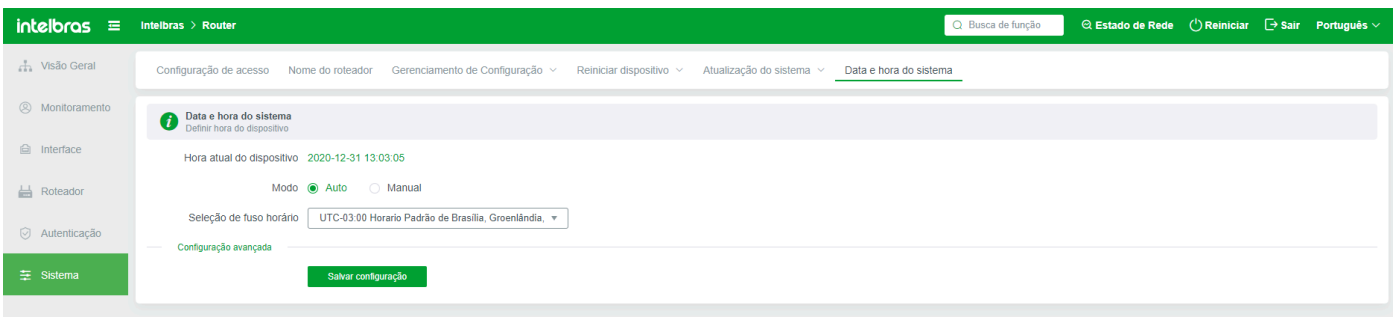
Atualização Local

Se o firmware precisar ser atualizado ou degradado, selecione a opção de atualização local. Selecione o firmware e clique em "Atualizar agora" para aguardar a contagem regressiva ser concluída. "Atualizar Depois" indica que o firmware será atualizado apenas quando o dispositivo for reiniciado (reinicialização de software ou reinicialização por desligamento). Para atualizar o firmware posteriormente, selecione Atualizar firmware e clique em Atualizar Depois.

Status de Atualização: indica se o banco de dados de assinaturas foi atualizado com sucesso.

Data e hora do sistema

Ao definir o horário do sistema, é aconselhável manter o valor padrão.



RECUPERAÇÃO DE DISPOSITIVO TRAVADO

Você ira precisar dos seguintes itens:

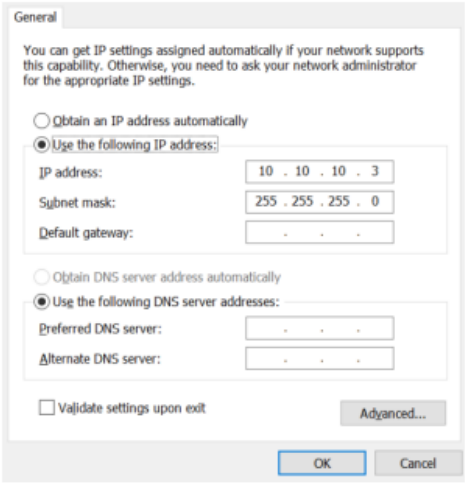
» Cabo de rede RJ45 8 Vias

» Software TFTP64

RECUPERANDO A FIRMWARE VIA MODO DE RECUPERAÇÃO

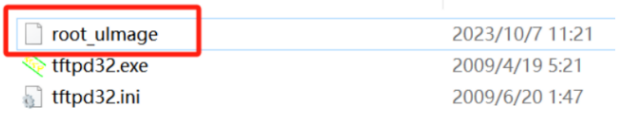
» Configurações no PC:

» Fixe o endereço IP 10.10.10.3 na sua placa de rede cabeada;

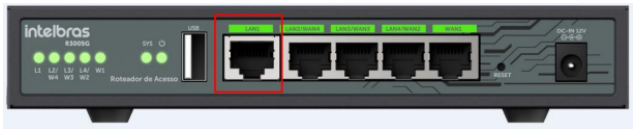


» Realize o Download do firmware de recuperação e salve em uma pasta de fácil acesso (/pt-BR/roteadores/R3005G/changelog.html)

» Renomeie o firmware de recuperação para root_uImage, conforme a imagem abaixo

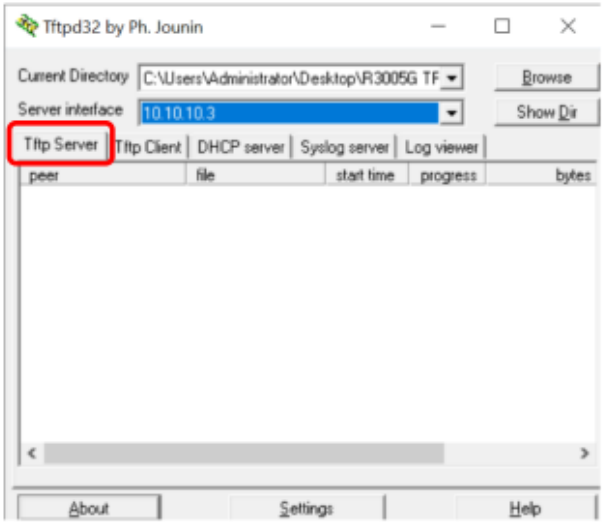


» Conecte o Cabo da interface do computador na interface LAN1



» Configuração no TFTP:

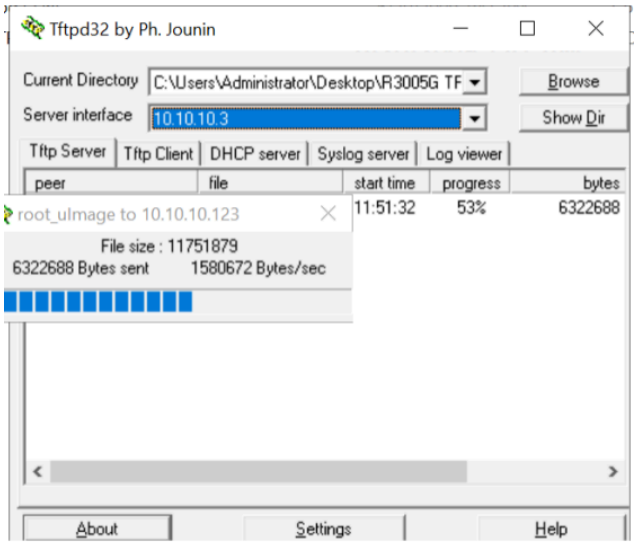
» Abra o software TFTP64 e acesse a aba “TFTP Server”:



» Clique em “Browse” e selecione a pasta onde você salvou o arquivo de recuperação de firmware:

» Pressione e segure o botão reset do dispositivo e ligue o roteador inserindo o conector macho DC no conector fêmea de energia do roteador, aguarde cerca de 5 segundos com o reset pressionado e então solte o botão reset.

» O processo irá iniciar automaticamente. Aguarde o a restauração do firmware completar. (o que deve demorar cerca de 1 a 2 minutos)



» Quando finalizar altere a interface local removendo o IP fixado e habilitando a configuração automática (DHCP)

» Ping o Roteador através do IP 192.168.0.1

» Se houver resposta o procedimento foi bem sucedido.

» Caso não tenha sucesso, você pode resetar o roteador novamente (na condição de boot, basta pressionar o botão por cerca de 3s e soltar) que o dispositivo irá restaurar a configuração default de fábrica.

» Aguarde cerca de 2 minutos para o roteador inicializar e teste o ping novamente.

» Caso o dispositivo não responda, siga para a próxima etapa realizando a recuperação do firmware via conexão serial.

RECUPERANDO A FIRMWARE VIA SERIAL

> A execução do procedimento delineado abaixo acarreta o risco de danos e subsequente inutilização do dispositivo, caso não seja realizada de forma apropriada. Caso o executor não detenha a confiança necessária para conduzir o referido procedimento, é fortemente recomendado que busque os serviços de uma assistência técnica autorizada para sua efetivação. Destaca-se que o procedimento em questão visa prover suporte na recuperação do dispositivo em cenários críticos nos quais uma substituição imediata da unidade corrompida não é imediatamente viável.

» Configurações no PC:

- Fixe o endereço IP 10.10.10.3 na sua placa de rede cabeada;
- Realize o Download do firmware de recuperação e salve em uma pasta de fácil acesso (/pt-BR/roteadores/R3005G/changelog.html)
- Altere o nome do arquivo para img.bin

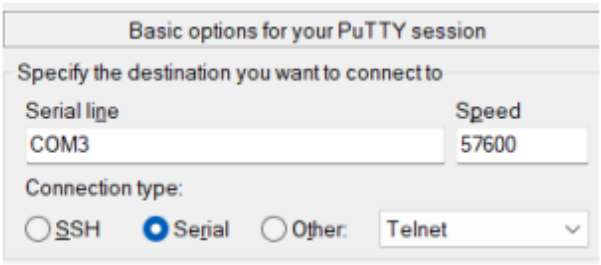
» Configuração serial:

- Realize a conexão serial conforme a imagem abaixo(Para ter acesso aos conectores seriais da placa é necessário retirar a tampa do dispositivo):

Conversor Serial USB	Conector na placa
GND	GND
RX	TX
TX	RX

» Configuração no PuTTY:

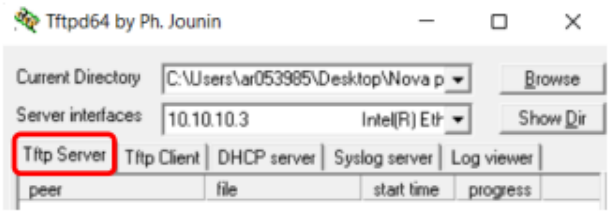
- Realize a configuração conforme a imagem abaixo:



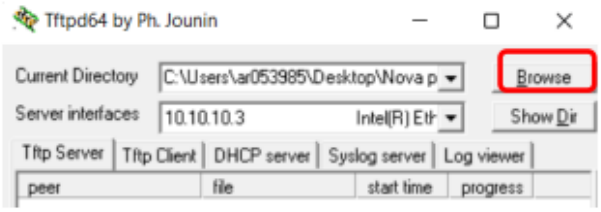
- Serial line: Porta COM onde o produto está conectado. É possível identificar no gerenciador de dispositivos do Windows;
- Speed: 57600;
- Connection type: Serial.

» Configuração no TFTP:

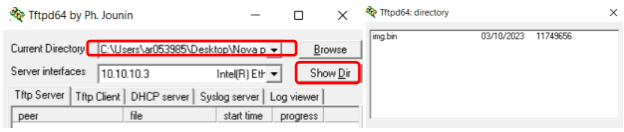
- Abra o software TFTP64 e acesse a aba “TFTP Server”.



- Clique em “Browse” e selecione a pasta onde você salvou o arquivo de recuperação de firmware;



- Clique em “Show Dir” e verifique se o arquivo “img.bin” está na pasta.



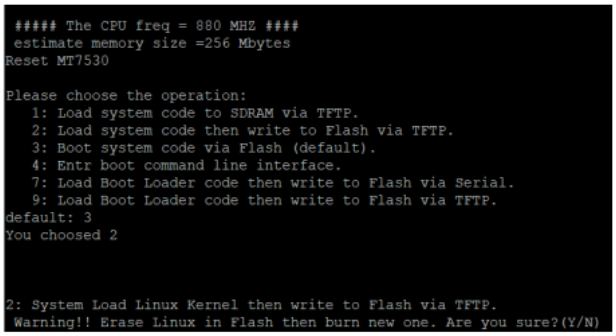
» Após realizar todas as configurações acima, na parte inferior do menu do PuTTY, clique em “Open” para iniciar a conexão serial com o produto.

» Ligue o R3005G na alimentação.

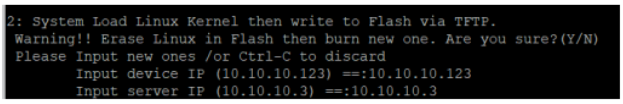
» Na tela da conexão serial, começarão a ser exibidos os dados de boot do produto:

- Caso não haja nenhuma resposta (dados sendo impressos na tela) em até 3 minutos após ligar o R3005G, leve o dispositivo para uma assistência técnica autorizada

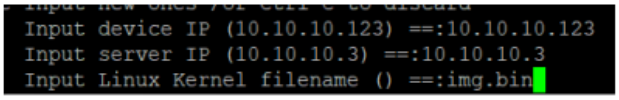
» Logo no início, será exibida a tela abaixo, pressione “2” e depois “Y” para interromper o boot e iniciar o modo de recuperação.



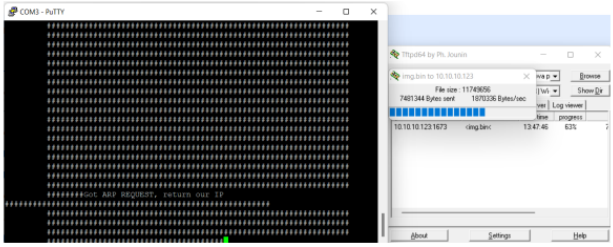
» Caso tenha seguido os passos de configuração anteriores, pressione “Enter” nas próximas duas mensagens.



» Quando for solicitada a informação “Input Linux Kernel filename () ==:”, digite “img.bin” e pressione “Enter”.



» Aguarde enquanto o firmware é enviado via TFTP.



» Assim que finalizar, reconfigure sua placa de rede cabeada para pegar DHCP novamente.

» Realize o acesso ao produto novamente.

- Obs: O produto não retorna aos padrões de fábrica após a recuperação de firmware. Caso não consiga acessar mesmo após o procedimento, realize o reset físico do produto pressionando o botão por cerca de 12s e soltando.
- Se mesmo assim o produto continuar travado, leve o dispositivo para uma assistência técnica autorizada.

Termo de garantia

Para a sua comodidade, preencha os dados abaixo, pois, somente com a apresentação deste em conjunto com a nota fiscal de compra do produto, você poderá utilizar os benefícios que lhe são assegurados.

Nome do cliente:

Assinatura do cliente:

Nº da nota fiscal:

Data da compra:

Modelo:

Nº de série:

Revendedor:

Fica expresso que esta garantia contratual é conferida mediante as seguintes condições:

1. Todas as partes, peças e componentes do produto são garantidos contra eventuais defeitos de fabricação, que porventura venham a apresentar, pelo prazo de 3 (três) anos – sendo 3 (três) meses de garantia legal e 33 (trinta e três) meses de garantia contratual –, contado a partir da data de entrega do produto ao Senhor Consumidor, conforme consta na nota fiscal de compra do produto, que é parte integrante deste Termo em todo o território nacional. Esta garantia contratual compreende a troca gratuita de partes, peças e componentes que apresentarem defeito de fabricação, incluindo a mão de obra utilizada nesse reparo. Caso não seja constatado defeito de fabricação, e sim defeito(s) proveniente(s) de uso inadequado, o Senhor Consumidor arcará com essas despesas.

2. A instalação do produto deve ser feita de acordo com o Manual do Produto e/ou Guia de Instalação. Caso seu produto necessite a instalação e configuração por um técnico capacitado, procure um profissional idôneo e especializado, sendo que os custos desses serviços não estão inclusos no valor do produto.

3. Na eventualidade de o Senhor Consumidor solicitar atendimento domiciliar, deverá encaminhar-se ao Serviço Autorizado mais próximo para consulta da taxa de visita técnica. Caso seja constatada a necessidade da retirada do produto, as despesas decorrentes de transporte e segurança de ida e volta do produto ficam sob a responsabilidade do Senhor Consumidor.

4. Na eventualidade de o Senhor Consumidor solicitar atendimento domiciliar, deverá encaminhar-se ao Serviço Autorizado mais próximo para consulta da taxa de visita técnica. Caso seja constatada a necessidade da retirada do produto, as despesas decorrentes, como as de transporte e segurança de ida e volta do produto, ficam sob a responsabilidade do Senhor Consumidor.

5. A garantia perderá totalmente sua validade na ocorrência de quaisquer das hipóteses a seguir: a) se o vício não for de fabricação, mas sim causado pelo Senhor Consumidor ou por terceiros estranhos ao fabricante; b) se os danos ao produto forem oriundos de acidentes, sinistros, agentes da natureza (raios, inundações, desabamentos, etc.), umidade, tensão na rede elétrica (sobretensão provocada por acidentes ou flutuações excessivas na rede), instalação/uso em desacordo com o manual do usuário ou decorrentes do desgaste natural das partes, peças e componentes; c) se o produto tiver sofrido influência de natureza química, eletromagnética, elétrica ou animal (insetos, etc.); d) se o número de série do produto tiver sido adulterado ou rasurado; e) se o aparelho tiver sido violado.

6. Esta garantia não cobre perda de dados, portanto, recomenda-se, se for o caso do produto, que o Consumidor faça uma cópia de segurança regularmente dos dados que constam no produto.

7. A Intelbras não se responsabiliza pela instalação deste produto, e também por eventuais tentativas de fraudes e/ou sabotagens em seus produtos. Mantenha as atualizações do software e aplicativos utilizados em dia, se for o caso, assim como as proteções de rede necessárias para proteção contra invasões (hackers). O equipamento é garantido contra vícios dentro das suas condições normais de uso, sendo importante que se tenha ciência de que, por ser um equipamento eletrônico, não está livre de fraudes e burlas que possam interferir no seu correto funcionamento.

A garantia contratual deste termo é complementar à legal, portanto, a Intelbras S/A reserva-se o direito de alterar as características gerais, técnicas e estéticas de seus produtos sem aviso prévio.

Sendo estas as condições deste Termo de Garantia complementar, a Intelbras S/A se reserva o direito de alterar as características gerais, técnicas e estéticas de seus produtos sem aviso prévio.

Todas as imagens deste manual são ilustrativas.

Suporte a clientes: (48) 2106 0006

Fórum: forum.intelbras.com.br (http://forum.intelbras.com.br)

Suporte via chat: intelbras.com.br/suporte-tecnico (http://www.intelbras.com.br/suporte-tecnico)

Suporte via e-mail: suporte@intelbras.com.br

SAC: 0800 7042767

Onde comprar? Quem instala?: 0800 7245115

Importado por Intelbras

Rodovia SC 281, km 4,5 – Sertão do Maruim – São José/SC - 88122-001

CNPJ 82.901.000/0014-41 - www.intelbras.com.br (http://www.intelbras.com.br)

Origem: China