Manual WEB do Usuário

S2050G-A

Versão deste manual: 1.0.0

S2050G-A | Manual WEB do Usuário

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

O S2050G-A é um switch de 48 portas Gigabit Ethernet com 2 portas SFP.

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

- Backup (m_backup)
- Reiniciar (m_reiniciar)
- Configurações de fábrica (m_fabrica)

DIAGNOSTICO

- Teste de ping
- Gerenciamento de nuvem

DHCP snooping

- Visão geral
- Configurar DHCP snooping

Spanning tree

- Visão geral
- Globais
- Configuração da porta
- Estatísticas portuárias
- Informações da instância

CONFIGURAÇÃO LLDP

- Visão geral
- Globais
- Configuração da porta
- Neighbor info

LLDP-MED

- Visão geral
- Básico
- Configurações de TLV
- Informações locais
- Neighbor info

FALE COM A GENTE

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 S3054G-B. 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:

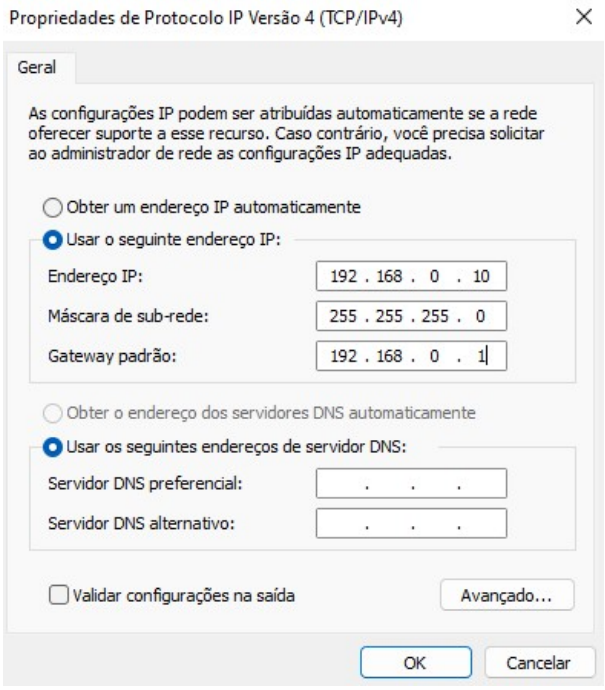
Sistema > Informações > Status: significa que a página Status está dentro do submenu Informações, que está localizada dentro do menu Sistema.

Login na web

Conecte-se

1. Conecte o computador a uma das portas RJ45 do switch usando um cabo Ethernet.
2. Defina o endereço IP de Ethernet (ou Conexão de Área Local) do computador para um não utilizado pertencente ao mesmo segmento de rede do endereço IP do switch.

   > Por exemplo, o endereço IP padrão do switch é 192.168.0.1 , você pode definir o endereço IP do computador como 192.168.0. X (X varia de 2 a 254 excluindo 168 e não está ocupado) e máscara de sub-rede para 255.255.255.0 .



3. Inicie um navegador e digite o endereço IP do switch (padrão: 192.168.0.1) na barra de endereços para acessar a página de login.

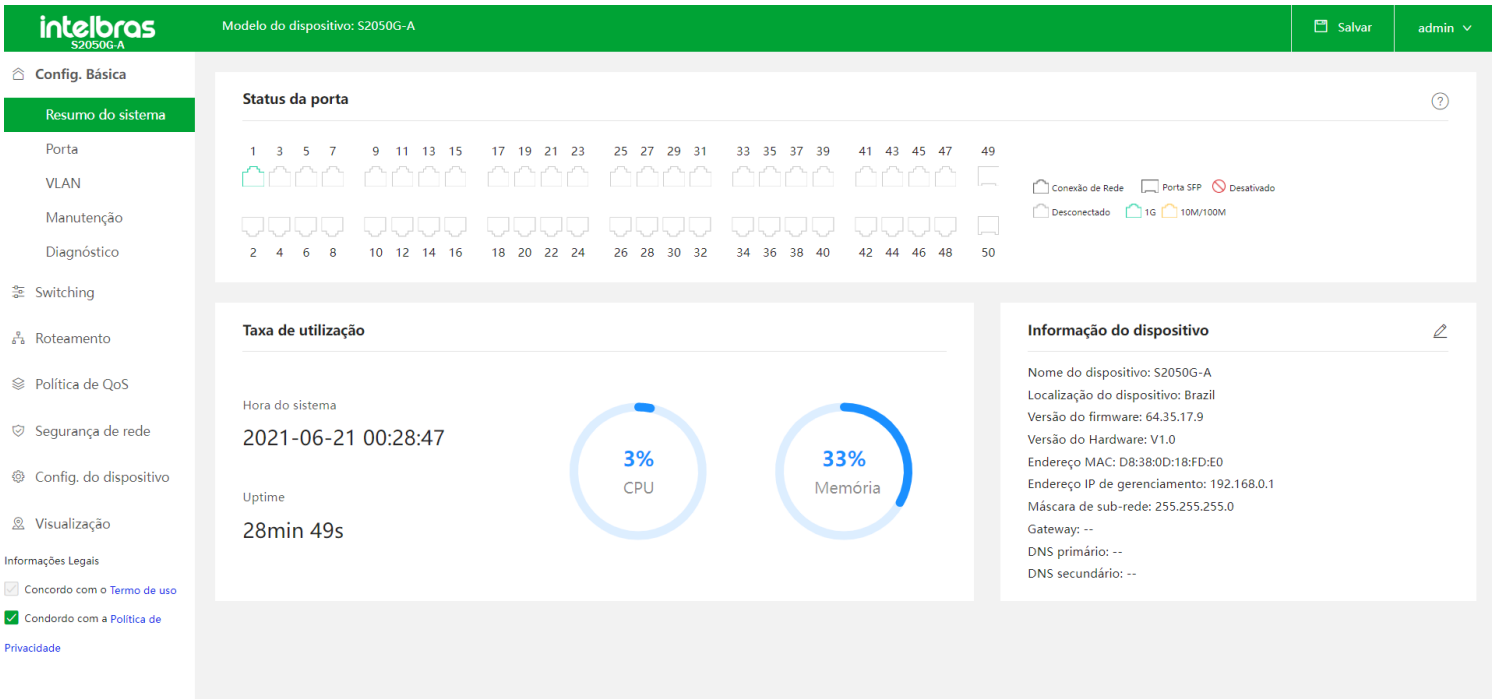
4. Digite seu nome de usuário e senha (ambos são admin por padrão) e clique em Login .

Se a página acima não aparecer, tente as seguintes soluções:

- Verifique se o switch está ligado corretamente: O indicador LED de energia está aceso.
- Verifique se o computador está conectado ao switch corretamente com um cabo Ethernet.
- Verifique se o endereço IP da Ethernet (ou Conexão de Área Local) do computador está definido como 192.168.0. x (X varia de 2 a 254 excluindo 168 e não está ocupado).
- Verifique se existe outro dispositivo com o endereço IP 192.168.0.1 na rede local.
- Limpe o cache do navegador da web ou tente outro navegador da web.
- Se o problema persistir, reinicie o interruptor e tente novamente. Método de reinicialização:

  1. Quando o indicador LED SYS estiver piscando, pressione o botão de reinicialização usando um objeto semelhante a uma agulha (como um alfinete) por cerca de 10 segundos e solte-o
  2. Quando todos os indicadores LED estiverem acesos. o indicador LED SYS IRÁ piscar novamente, então o switch será restauradopara as configurações de fábrica.

Depois de fazer login na interface do usuário da web, você pode começar a configurar o switch.



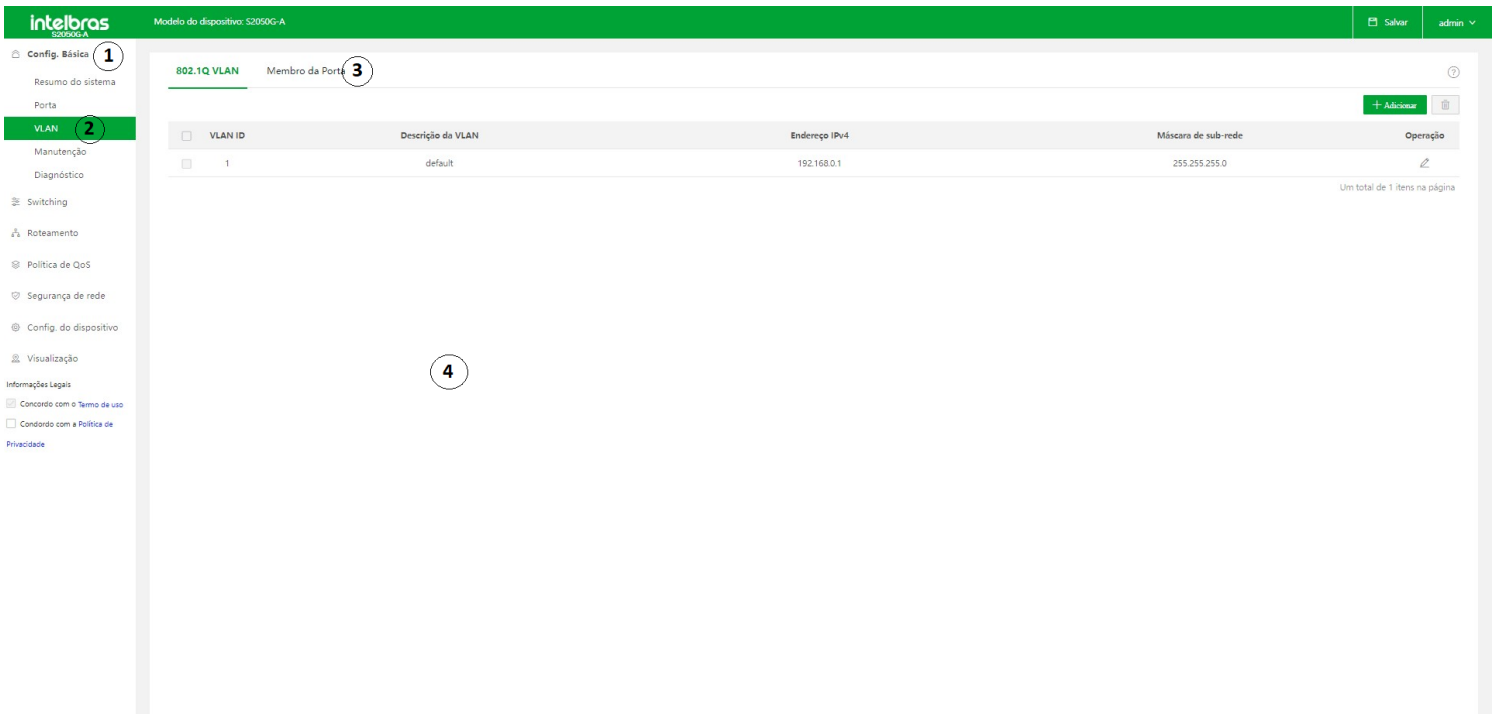
Sair

Depois de fazer login na página de interface do usuário da web do switch, o sistema o desconectará automaticamente se não houver nenhuma operação dentro do Login Timeout . Como alternativa, você pode clicar diretamente no nome do usuário no canto superior direito e, em seguida, clicar em Sair no menu suspenso para sair da página da interface do usuário da web.

Introdução à Interface de Usuário Web

Layout da web

A página da IU da Web pode ser dividida em quatro partes: barra de navegação de nível 1, barra de navegação de nível 2, área de página de guias e área de configuração



Não	Nome	Descrição
1	Barra de navegação de nível 1	As barras de navegação e páginas de guia exibem o menu de funções
2	Interruptor da navegação de nível 2	Quando você seleciona uma função na barra de navegação,da área da página da guia.

Não	Nome	Descrição
3	Configuração	Função aparece na área de configuração
4	Área de configuração	Esta área permite visualizar e modificar a configuração

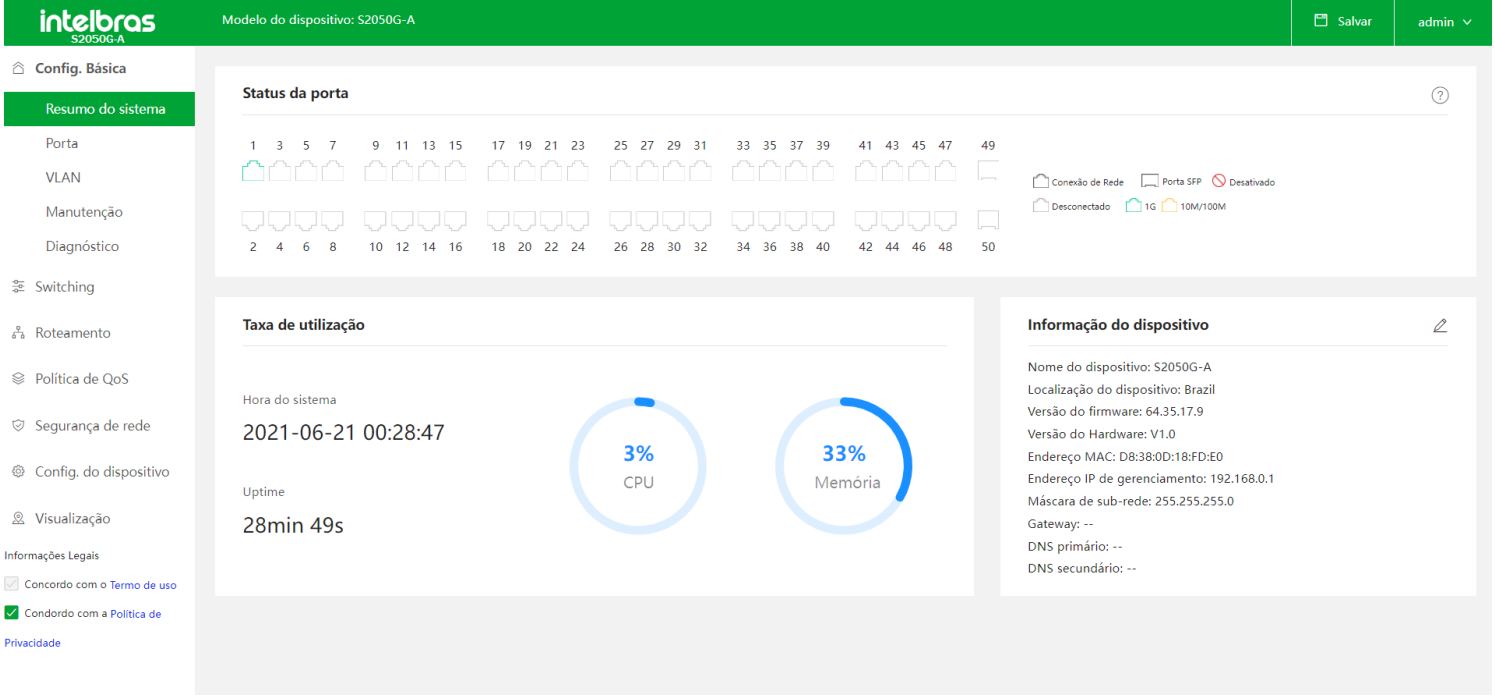
Botões comuns

Botões comuns	Icones	Descrição
Atualizar		Usado para atualizar o conteúdo exibido na página atual.
Editar		Usado para definir as configurações na página atual em lotes.
Confirmar	✓	Usado para salvar as configurações na página atual e permitir que as configurações entrem em vigor se você clicar apenas em confirmar para salvar as configurações modificadas, elas serão apagadas após a reinicialização do switch.
Cancelar	×	Usado para restaurar a configuração original sem as configurações na pagina atual.
Duvida	?	Usado para ajudar em alguma informação corresponde as configurações da pagina.
Adicionar	+	Usado para adicionar novas regras na página atual.
Lixo		Usado para detelar as regras na pagina atual.
Salvar		Usado para salvar toda a configuração atual do switch. se você clicar em salvar as configurações, elas ainda permanecerão após a reinicialização do switch.

Introdução à Interface de Usuário Web

Resumo do sistema

Na página Resumo do sistema , você pode visualizar o status da conexão de cada porta, a taxa de utilização da CPU e da memória, a hora do sistema e as informações do dispositivo.



Nome	Descrição
Status da porta	Exibe o status da conexão de cada porta do switch. Verde - indica que a porta está conectada a um dispositivo e a taxa é de 1000 Mbps. Amarela - indica que a porta está conectada a um dispositivo e a taxa é de 10 ou 100 Mbps. Cinza - indica que a porta não está conectada a um dispositivo. Vermelho - indica que a porta está desabilitada.
Taxa de utilização	Ele exibe a utilização da CPU e da memória do switch.
Hora do Sistema	Exibe a hora do sistema do switch
Tempo de atividade	Ele exibe o tempo durante o qual este switch está operando desde a última reinicialização.

Nome	Descrição
Nome do dispositivo	Ele exibe o nome do switch, que é o modelo do switch por padrão. Você pode clicar para modificá-lo.
Localização do dispositivo	Ele exibe a localização do switch, que é Shenzhen por padrão. Você pode clicar para modificá-lo.
Versão do firmware	Exibe a versão do firmware do switch.
Versão do hardware	Exibe a versão de hardware do switch.
Endereço MAC	Exibe o endereço MAC do switch.
VLAN de gerenciamento	Exibe a VLAN de gerenciamento do switch. Você pode clicar para modificá-lo.
Gerenciamento Endereço de IP	Exibe o endereço IP da VLAN de gerenciamento do switch. Você pode clicar para modificá-lo. Os computadores pertencentes à VLAN de gerenciamento podem fazer login na interface do usuário da Web do switch usando esse endereço IP.

Nome	Descrição
Máscara de sub-rede	Exibe a máscara de sub-rede da VLAN de gerenciamento do switch. Você pode clicar para modificá-lo.
Porta de entrada	Exibe o endereço do gateway da VLAN de gerenciamento do switch. Você pode clicar para modificá-lo.
DNS primário	Exibe o endereço do servidor DNS primário/secundário do switch.
DNS secundário	O tipo de atribuição de DNS inclui Auto e Manual . Você pode clicar em modificá-lo.
SN do dispositivo	Exibe o número de série do switch.
Informação do dispositivo	Exibe se o switch está conectado à plataforma Intelbras CloudFi. Conectado : O switch está conectado à plataforma Intelbras CloudFi. Desconectado : A função de gerenciamento de nuvem está desativada ou o switch não consegue se conectar à plataforma Intelbras CloudFi

Para se conectar à plataforma Intelbras CloudFi, o switch deve estar conectado à internet e pode resolver o nome de domínio corretamente. Portanto, verifique se o endereço do servidor DNS primário inserido está correto e se o endereço do servidor DNS secundário é opcional (recomendado: servidor DNS primário: 114.114.114.114; servidor DNS secundário: 8.8.8.8)..

Porta

Básico

Clique em **Básico > Porta > Básico** para entrar na página. Nesta página, você pode visualizar e configurar os parâmetros básicos das portas

Descrição do parâmetro

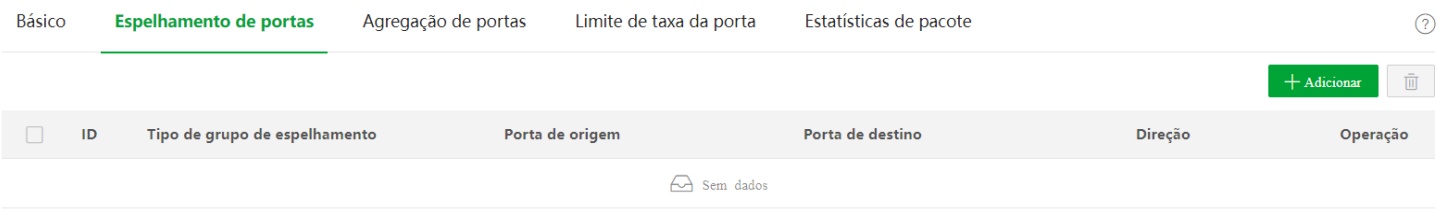
Nome	Descrição
Porta	Ele especifica o ID da porta.
Status da porta	Ele especifica o status atual da conexão da porta, incluindo Connected , Disconnected e Disabled.
Velocidade/Duplex (Taxa/Modo)	Especifica a velocidade de negociação e o modo duplex da porta. Auto-negociação : A porta negocia automaticamente a velocidade e o modo duplex com o dispositivo par. Modo obrigatório : A velocidade e o modo duplex da porta são fixos. Nesse modo, a porta não pode negociar a velocidade e o modo duplex com o dispositivo par. HDX : Modo meio duplex. FDX : Modo full duplex. Auto : A porta pode ajustar automaticamente o modo duplex.
Isolamento de porta	Ele especifica o grupo de isolamento ao qual a porta pertence. As portas pertencentes a diferentes grupos de isolamento podem se comunicar entre si, enquanto as portas pertencentes ao mesmo grupo não podem. As portas que não estão atribuídas a nenhum grupo de isolamento são exibidas no estado Desativado , indicando que podem se comunicar com todas as portas.

Nome	Descrição
Limite de entrada	Com a função habilitada, o fluxo de entrada da porta será monitorado. Quando ocorre congestionamento na porta de entrada, o switch envia um quadro PAUSE para notificar o dispositivo par para parar ou desacelerar a transmissão de dados, de modo a evitar a perda de mensagens recebidas.
Limite de saída	Com a função habilitada, quando o switch recebe um quadro PAUSE do dispositivo peer, o switch interrompe ou desacelera a transmissão de dados da porta para evitar que o dispositivo peer descarte mensagens.
fluxo de entrada	Especifica as estatísticas do tráfego de dados recebidos pela porta.
Fluxo de saída	Especifica as estatísticas do tráfego de dados transmitidos pela porta.

Espelhamento de porta

O espelhamento de porta é um método de copiar e enviar dados de uma ou várias portas (portas de origem) para uma porta especificada (porta de destino) do switch. A porta de destino geralmente é conectada a um dispositivo de monitoramento de dados, permitindo monitorar o tráfego de dados, analisar o desempenho e diagnosticar falhas

> Clique em Básico > Porta > Espelhamento de porta para entrar na página. Nesta página, você pode configurar as regras de espelhamento de porta



Descrição do parâmetro

Nome	Descrição
EU IA	Ele especifica o ID do grupo de espelhamento.
Tipo de grupo de espelhamento	Essa opção oferece suporte apenas a tipos de grupos de espelhamento local.
Porta de origem	Especifica as portas cujos pacotes serão copiados. Múltiplas portas podem ser selecionadas.
Porto de destino	Os pacotes das portas de origem serão copiados para esta porta. Um grupo de espelhamento pode conter apenas uma porta de destino.

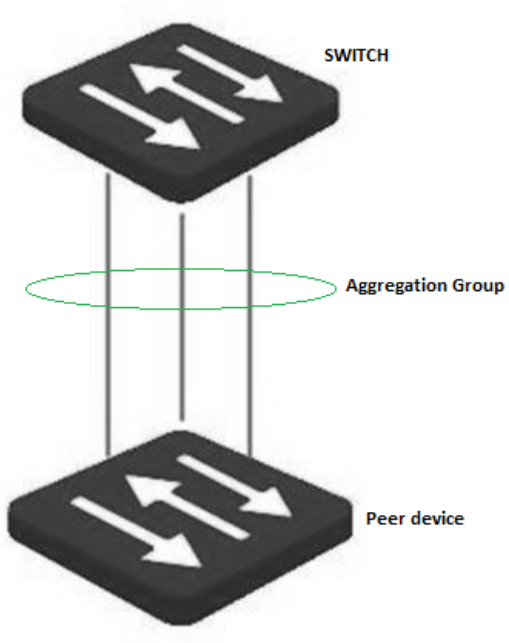
Nome	Descrição
Descrição	• Ele especifica o tipo de pacote. • Ingress : Os pacotes recebidos pelas portas de origem serão copiados para a porta de destino. • Egress : Os pacotes transmitidos pelas portas de origem serão copiados para a porta de destino. • Bidirecional : Os pacotes transmitidos e recebidos pelas portas de origem serão copiados para a porta de destino.

Agregação de Portas

A agregação de porta é usada para convergir várias portas físicas em um grupo de agregação lógica.

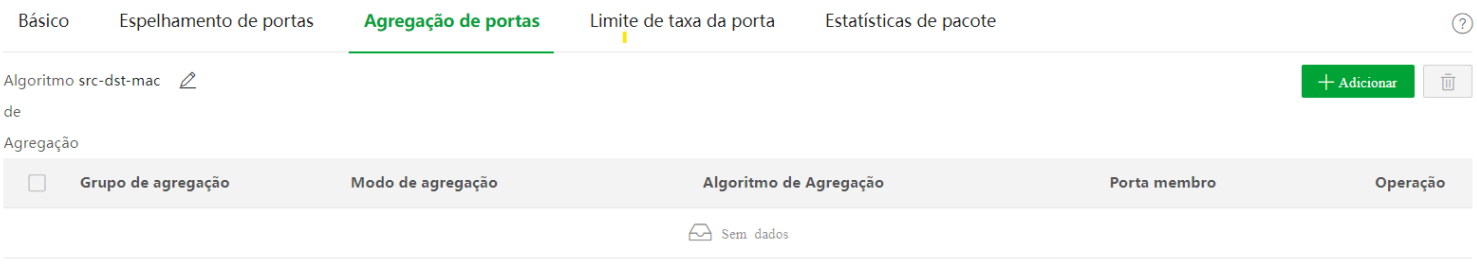
Vários links físicos em um grupo de agregação são considerados como um link lógico. A função Port Aggregation vincula vários links físicos em um link lógico e permite que eles compartilhem a carga de tráfego entre si, aumentando assim a largura de banda entre o switch e o dispositivo par. Enquanto isso, cada membro de um grupo de agregação faz backup dos dados uns dos outros dinamicamente, melhorando a confiabilidade da conexão.

A topologia de rede de agregação de porta é mostrada abaixo.



No mesmo grupo de agregação, todas as portas membros devem ser definidas com as mesmas configurações em relação a STP, QoS, configuração de VLAN e propriedade de porta.

Clique em Básico > Porta > Agregação de porta para entrar na página. Nesta página, você pode configurar as regras de agregação de portas.



Descrição do parâmetro

Nome	Descrição
Grupo de agregação	Ele especifica o ID da porta. • Quando o modo está definido como Estático Agregação,o ID varia de 1 a 8. • Quando o modo é definido como Agregação Dinâmica , o ID varia de 9 a 16.
Modo de agregação	Existem dois modos de agregação: Estático Agregação e Agregação Dinâmica. • Agregação estática : todas as portas membros no grupo de agregação convergem para uma porta lógica. • Agregação Dinâmica : LACP (Link Aggregation Control Protocol) para todos

O modo de agregação do switch precisa ser o mesmo do dispositivo par. Caso contrário, os dados não podem ser encaminhados corretamente ou os loops ocorrem.

Nome	Descrição
Algoritmo de Agregação	Ele especifica os algoritmos de roteamento para o grupo de agregação: • src-dst-mac : As portas membros no grupo de agregação compartilham a carga de acordo com o endereço MAC de origem e o endereço MAC de destino no pacote recebido. • src-dst-ip : As portas membros no grupo de agregação compartilham a carga de acordo com o endereço IP de origem e o endereço IP de destino no pacote recebido. • src-dst-mac-ip-port : As portas membros no grupo de agregação compartilham a carga de acordo com o endereço MAC de origem, endereço MAC de destino, endereço IP de origem, endereço IP de destino, número da porta de origem TCP/UDP e porta de destino TCP/UDP número no pacote recebido

Nome	Descrição
Porta Membro	Ele especifica os membros de um grupo de agregação. • No modo de agregação estática, as portas membros são membros de um grupo de agregação. • No modo de agregação dinâmica, as portas membros são as portas com LACP habilitado e as portas agregadas reais devem ser determinadas junto com o dispositivo de mesmo nível por meio do LACP. • Agregação estática : todas as portas membros no grupo de agregação convergem para uma porta lógica. • Agregação Dinâmica : LACP (Link Aggregation Control Protocol) para todos Do modo de agregação no grupo de agregação estão habilitadas e as portas agregadas reais devem ser determinadas junto com o dispositivo de mesmo nível por meio do LACP.

Limite de taxa de porta

Clique em **Básico > Porta > Limite de taxa de porta** para entrar na página. Nesta página, você pode configurar a taxa de saída da porta e definir o valor de supressão da taxa de recebimento de pacotes broadcast, multicast e unicast desconhecidos para cada porta.

Nome	Descrição
Porta	Ele especifica o ID da porta.
Taxa de saída (Mbps)	Ele especifica a taxa de saída máxima da porta. “ -- ” significa sem limite de taxa.

Nome	Descrição
Pacote de Transmissão	Exibe se a função de supressão de pacote de transmissão está habilitada ou desabilitada.
Pacote Multicast	Exibe se a função de supressão de pacote multicast está habilitada ou desabilitada.
Unicast Desconhecido	Exibe se a função de supressão de pacotes unicast desconhecidos está habilitada ou desabilitada.
Valor de supressão	Ele especifica a taxa máxima na qual os pacotes broadcast, multicast e unicast desconhecidos podem passar quando a função de supressão está habilitada. Quando os pacotes broadcast/multicast/unicast desconhecidos excedem o valor limite definido pelo usuário, o sistema descarta os pacotes em excesso, para diminuir a proporção de pacotes broadcast/multicast/unicast desconhecidos para a operação normal do serviço de rede.

Estatísticas de pacotes

Clique em **Basics > Port > Packet Statistics** para entrar na página. Nesta página, você pode visualizar e excluir as estatísticas de pacotes recebidos e enviados por cada porta.

Descrição do parâmetro

Nome	Descrição
Porta	Ele especifica o ID da porta.
Pacotes Transmitidos	Especifica o total de pacotes enviados por uma porta.
Byte transmitido	Especifica o total de bytes enviados por uma porta.

Nome	Descrição
Pacotes recebidos	Especifica o total de pacotes recebidos por uma porta.
Byte recebido	Especifica o total de bytes recebidos por uma porta.

Para visualizar os detalhes dos pacotes recebidos e enviados por uma porta, clique no botão atrás da porta.

Descrição do parâmetro

Nome	Descrição
Total de bytes	Especifica os bytes recebidos/enviados pela porta.
Pacotes de Transmissão	Especifica o número de pacotes broadcast recebidos/enviados pela porta.
Pacotes Unicast	Especifica o número de pacotes unicast recebidos/enviados pela porta.
Pacotes de erro	Especifica o número de pacotes de erro recebidos/enviados pela porta.
Descartar Pacotes	Especifica o número de pacotes descartados quando a porta está recebendo/enviando pacotes.

VLAN

Visão geral

VLAN (Virtual Local Area Network) é uma tecnologia que divide os dispositivos na LAN em diferentes segmentos de rede lógicos, em vez de físicos, para formar grupos de trabalho virtuais. As VLANs permitem que uma estação de rede constituída por switches seja segmentada logicamente em diferentes domínios para isolamento de broadcast. Todos os membros em uma VLAN são tratados como no mesmo domínio de broadcast e se comunicam como se estivessem no mesmo segmento de rede, independentemente de suas localizações físicas. Diferentes VLANs não podem se comunicar diretamente. A comunicação entre VLANs só pode ser obtida usando um roteador ou outros dispositivos de camada 3 capazes de executar o encaminhamento de camada 3.

O switch suporta 802.1Q VLAN e também pode se comunicar com dispositivos que suportam 802.1Q VLAN em VLAN.

A VLAN 802.1Q é definida pelo protocolo IEEE 802.1q. Com VLAN 802.1Q, o switch pode processar mensagens identificando as tags nas mensagens.

Este switch suporta três tipos de porta VLAN 802.1Q:

- **Acesso:** Uma porta de acesso pertence a apenas 1 VLAN, geralmente usada para conectar o computador.
- **Tronco:** Uma porta de tronco pode receber e enviar mensagens pertencentes a várias VLANs. Normalmente, uma porta de tronco é usada para conexão de switches.
- **Híbrido:** Uma porta híbrida pode receber e enviar mensagens pertencentes a várias VLANs. Normalmente, uma porta híbrida é usada para conexão de switches e pode ser conectada a um computador.

Métodos de cada tipo de porta para processar pacotes são mostrados a seguir:

Tipo de porta	Recebendo dados marcados	Recebendo dados não marcados	Envio de dados
Porta de acesso			As mensagens são encaminhadas após as tags são removidos.

Tipo de porta	Recebendo dados marcados	Recebendo dados não marcados	Envio de dados
Porta tronco	Encaminhar para outras portas no correspondente VLAN de acordo com o VID na tag.	Encaminhar para outras portas no correspondente VLAN de acordo com o PVID nesta porta.	Se o valor VID da mensagem for o igual ao seu valor PVID, a mensagem é encaminhado depois que as tags são removidas. Caso contrário, encaminhe-o com suas tags Permaneceu.
Porta híbrida			Se o valor VID da mensagem pertencer para a VLAN marcada, a mensagem é encaminhado com suas etiquetas restantes; se o O valor VID da mensagem pertence ao VLAN não marcada, a mensagem é encaminhado depois que as tags são removidas

Configuração de VLAN

Configurar regras de VLAN 802.1Q

Uma regra de VLAN é criada por padrão para garantir a comunicação entre os switches nas configurações de fábrica. Todas as portas são definidas para serem membros desta VLAN por padrão com o VLAN ID de 1. Esta regra não pode ser excluída.

Clique em **Basics > VLAN > 802.1Q VLAN** para entrar na página. Nesta página, você pode configurar as regras da VLAN 802.1Q.

Descrição do parâmetro

Nome	Descrição
ID da VLAN	Especifica o VLAN ID, utilizado para identificar a VLAN a qual o pacote pertence.
Descrição da VLAN	É usado para identificar grupos de VLAN. Se não estiver definido, a descrição padrão é "VLAN e ID de VLAN de quatro dígitos". Por exemplo, quando o ID da VLAN é 3, a descrição da VLAN é VLAN0003.

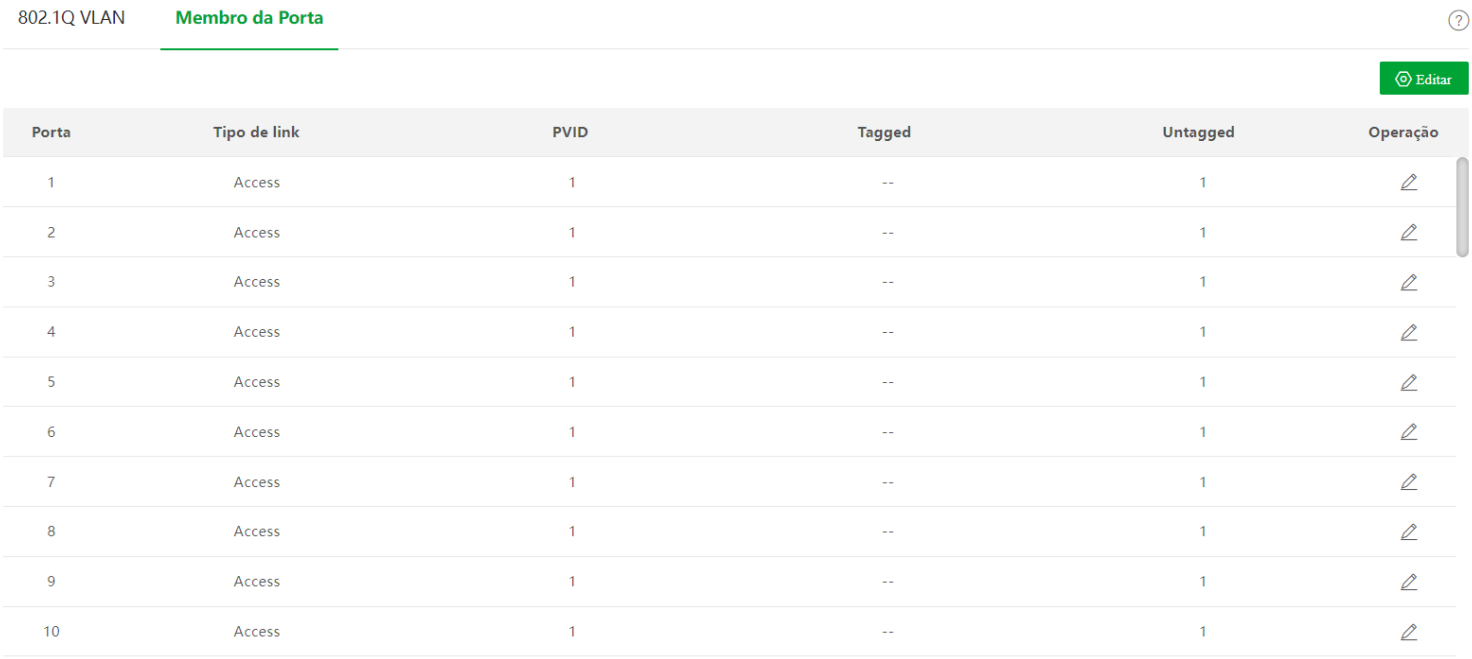
- Ele especifica o tipo que a interface VLAN emprega para obter um endereço IP.
- Manual : Configure manualmente o endereço IP e a máscara de sub-rede para a interface VLAN.
- DHCP : Obtenha automaticamente as informações do endereço IP do servidor DHCP.
- Tipo de obtenção de IP
- Observação
- Quando o tipo de obtenção do endereço IP for definido como DHCP, certifique-se de que haja um servidor DHCP pertencente à VLAN.

Nome	Descrição
Endereço IP/Máscara	Ele especifica o endereço IP e a máscara de sub-rede da VLAN de gerenciamento. Os dispositivos conectados às portas no grupo VLAN podem usar esse endereço IP para fazer login na interface do usuário da web do switch.

Nome	Descrição
Porta de entrada	Ele especifica o endereço do gateway da VLAN de gerenciamento.

Configurar membros da porta

Clique em **Basics > VLAN > Port Member** para entrar na página. Nesta página, você pode configurar as políticas de tratamento PVID e Tag de cada porta para realizar o isolamento de VLAN.



Descrição do parâmetro

Nome	Descrição
Porta	Ele especifica o ID da porta.
Tipo de link	Três tipos de link de VLAN são suportados: Access , Trunk e Hybrid . • Acesso : Uma porta de acesso pertence apenas a 1 VLAN e transmite mensagens não marcadas. É comumente usado para conectar a terminais, como computadores. • Tronco : Uma porta de tronco pode receber e transmitir mensagens pertencentes a várias VLANs, geralmente usadas como uma porta conectada em cascata entre switches. • Híbrido : Uma porta híbrida pode receber e transmitir mensagens pertencentes a várias VLANs. Uma porta híbrida pode ser usada como uma porta conectada em cascata entre switches ou para conectar terminais.
PVID	Ele especifica o ID de VLAN padrão de uma porta. Ao receber pacotes não marcados, a porta os encaminha para a VLAN correspondente com base no PVID da própria porta.
marcado	Se o VID dos pacotes etiquetados recebidos pela porta for o mesmo da VLAN etiquetada, a porta retém as etiquetas dos pacotes e os transmite.
Não etiquetado	Se o VID dos pacotes etiquetados recebidos pela porta for o mesmo da VLAN não etiquetada, a porta remove as etiquetas dos pacotes e os transmite.

Exemplo de configuração de VLAN 802.1Q

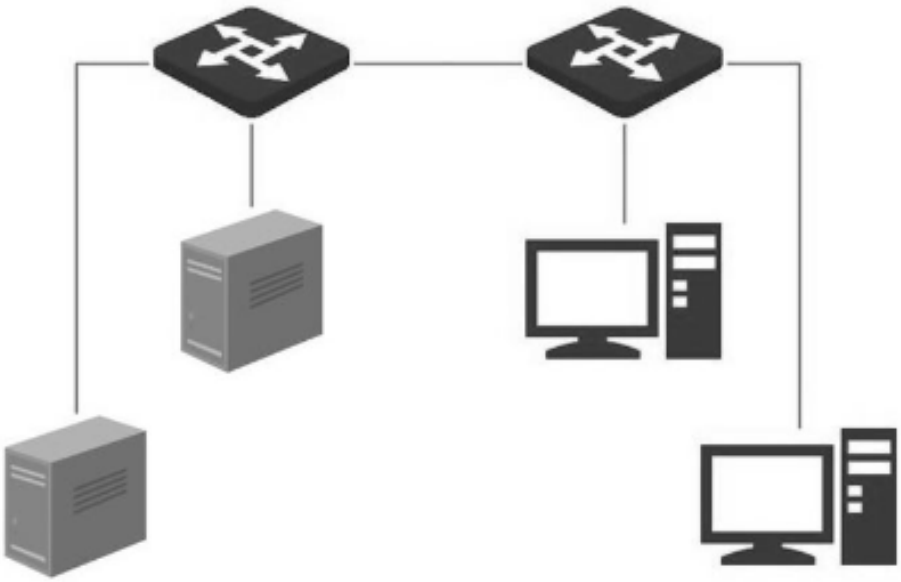
Requisito de rede

Os funcionários do departamento financeiro e do departamento de marketing de uma empresa trabalham no segundo andar, enquanto os servidores desses dois departamentos ficam no terceiro andar. Agora é necessário que a comunicação esteja disponível dentro de cada departamento e os servidores possam ser acessados respectivamente, mas os dois departamentos não podem se comunicar entre si.

Solução

Configure a VLAN 802.1Q para dois switches:

- Crie duas VLANs para os switches. Atribua as portas conectadas aos dispositivos do departamento financeiro à VLAN 5 e as portas aos dispositivos do departamento de marketing à VLAN 7.
- Adicione as portas que conectam dois switches à VLAN 5 e à VLAN 7.



Procedimento de configuração

I .Configurando o Switch A

1.Adicione VLANs.

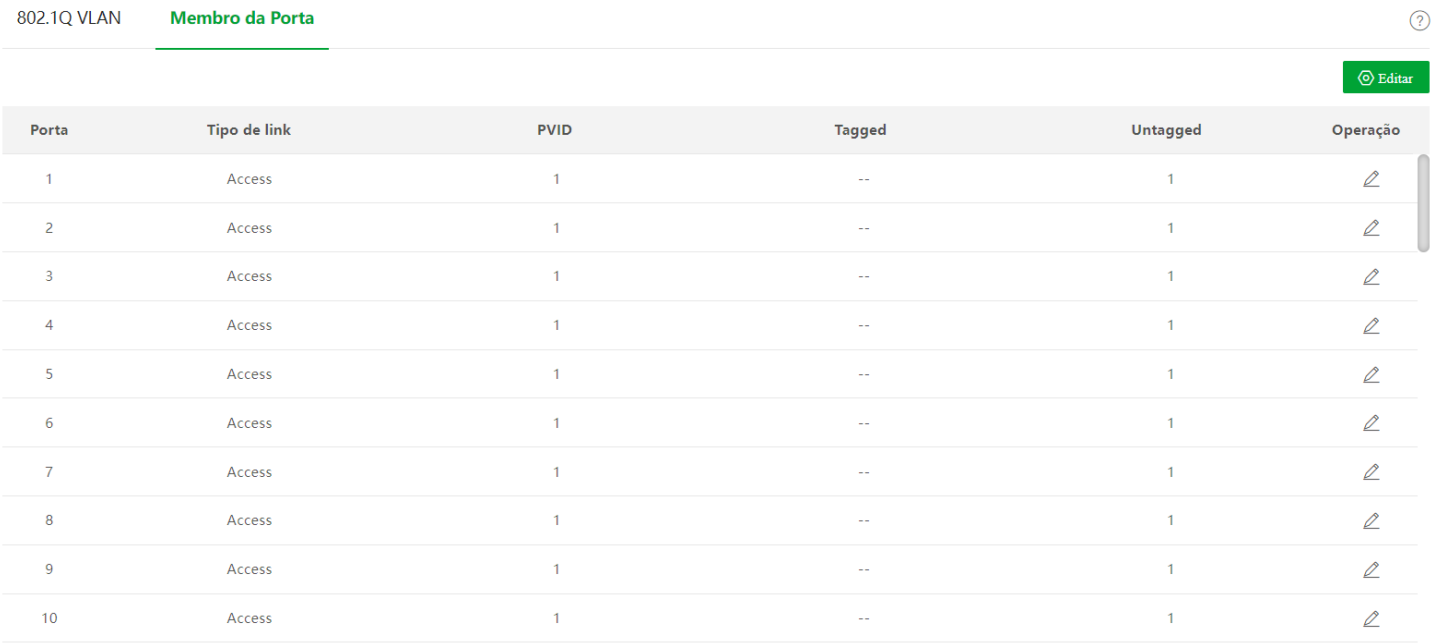
2.Faça login na interface do usuário da web do Switch A e clique em Basics > VLAN >802.1Q VLAN.

- .Clique em Adicionar e insira as seguintes informações na janela pop-up e clique em Confirmar.
- Defina o ID da VLAN como 5.
- Defina a Descrição da VLAN para Finanças .

- Repita a etapa (2) e adicione outra VLAN com VLAN ID 7 e VLAN Description of Marketing .

3. Configurando a propriedade da porta

- clique em **básico > VLAN > membro da porta**
- Clique no botão Atrás da porta 5 e defina PVID como 5
- Clique no botão Atrás da porta 7 e defina PVID como 7
- Clique no botão Atrás da porta 1 para definir o tipo de link para tronco e Tagged para 5,7



II. Configurando o Switch B

Consulte as etapas de configuração do switch A.

Verificação

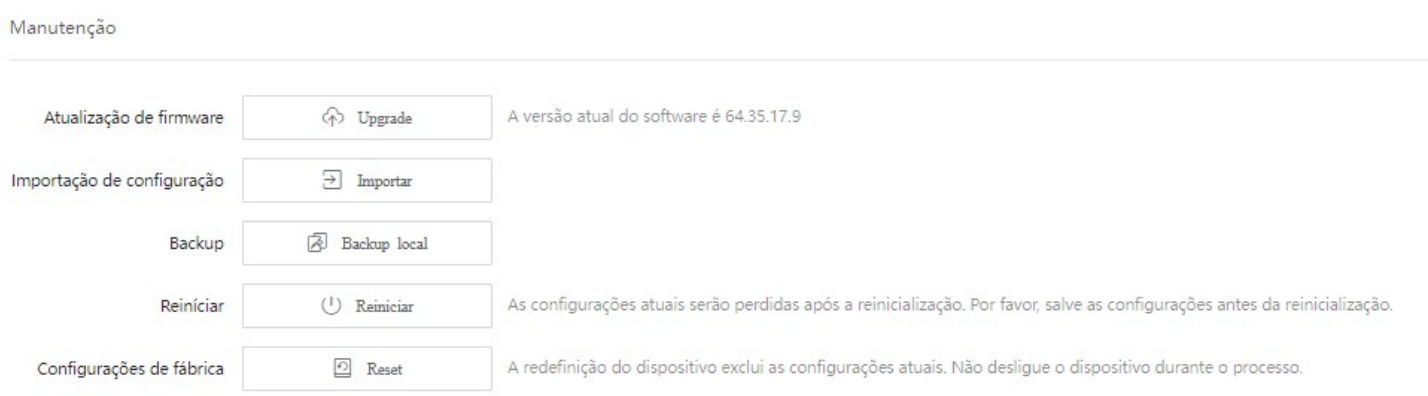
A equipe pode acessar o servidor de seu departamento, mas não pode acessar o servidor do outro departamento. A equipe do mesmo departamento pode se comunicar entre si, mas não pode se comunicar com a equipe de outros departamentos.

Manutenção

Atualização de firmware

Clique em **Básico > Manutenção** para entrar na página. Nesta página, você pode clicar em **Upgrade** para atualizar o firmware do switch, aproveitando uma melhor experiência do usuário

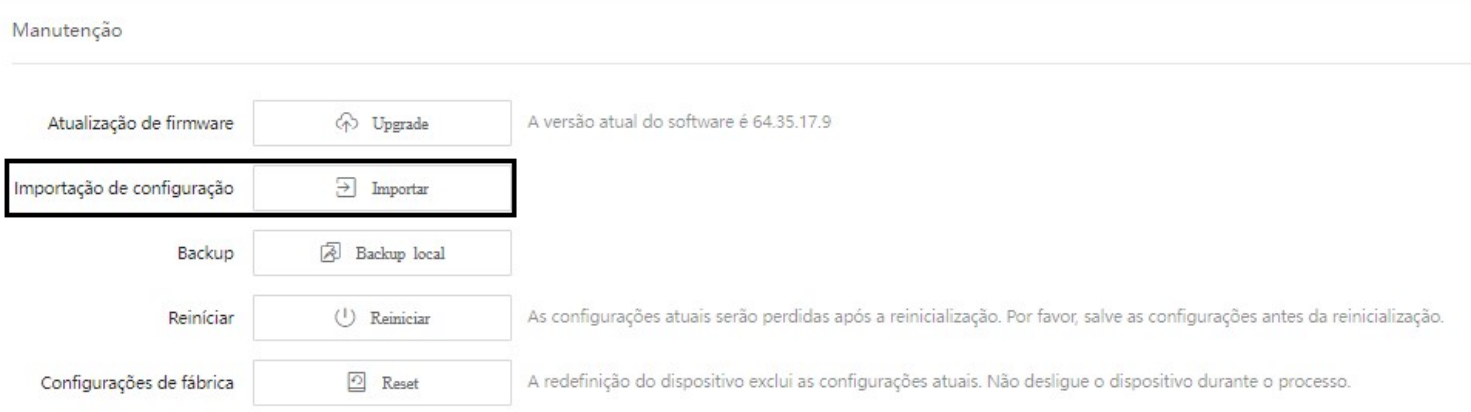
Para evitar danos ao switch, certifique-se de que o switch seja atualizado corretamente.Observe que, antes de atualizar, você pode baixar o firmware mais recente do switch no site oficial da Intelbras, www.intelbras.com geralmente, a extensão do arquivo de atualização é .bin. Durante o processo de atualização, garanta uma fonte de alimentação estável para o switch.



Importar configuração

Clique em **Básico > Manutenção** para entrar na página. Nesta página, você pode clicar em Importar para **importar** o arquivo de configuração de backup para o switch.

O switch não verifica o conteúdo do arquivo de configuração, portanto, certifique-se de que o arquivo esteja correto antes da importação.



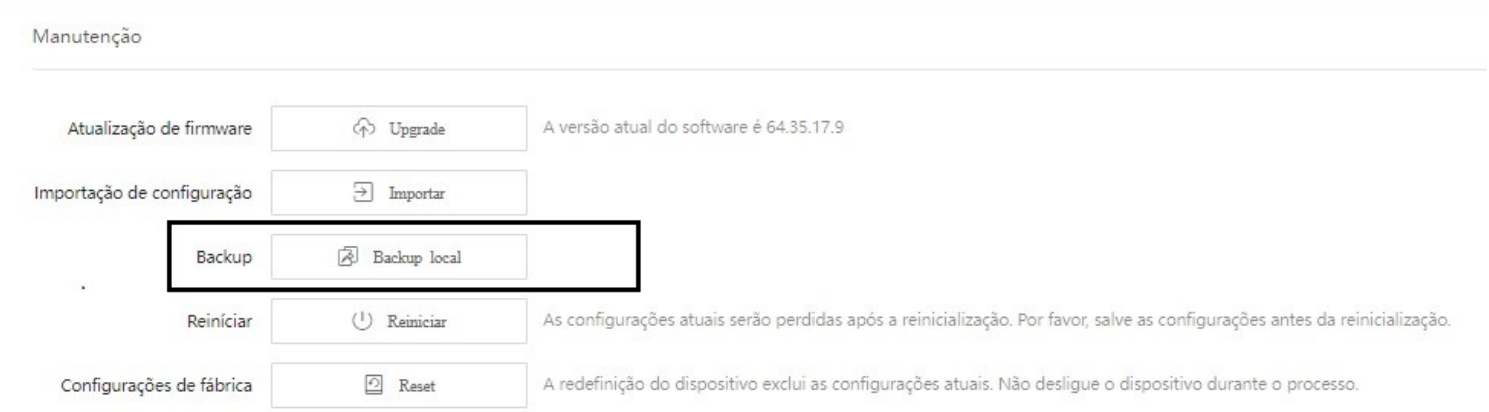
Backup

Se você fez muitas configurações no switch para obter melhor desempenho em um ambiente operacional específico, é recomendável fazer backup das configurações do switch. Depois de atualizar o switch ou restaurá-lo para as configurações de fábrica, você pode importar este arquivo de configuração de backup para restaurar as configurações do switch.

Clique em **Básico > Manutenção** para entrar na página. Nesta página, você pode fazer backup das informações de configuração do switch no computador local ou na plataforma Intelbras CloudFi.

Para salvar as configurações do switch no computador local, clique em Local Backup ; para a plataforma Intelbras CloudFi, clique em Cloud Backup.

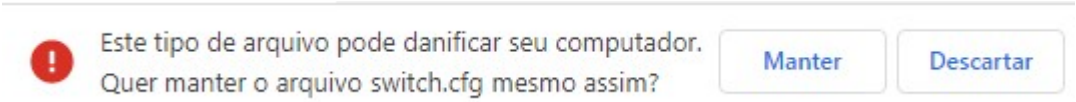
Clique em **Salvar** no canto superior direito da página para salvar todas as configurações antes do backup. Somente quando o switch é gerenciado pela plataforma Intelbras CloudFi é que as configurações podem ser copiadas para a plataforma Intelbras CloudFi.



Backup local

Clique em **Backup local** e um arquivo chamado **switch.cfg** será baixado para um computador local.

Se um prompt de segurança aparecer como abaixo, basta clicar em manter para baixar o arquivo de backup.



Nuvem Cópia de segurança

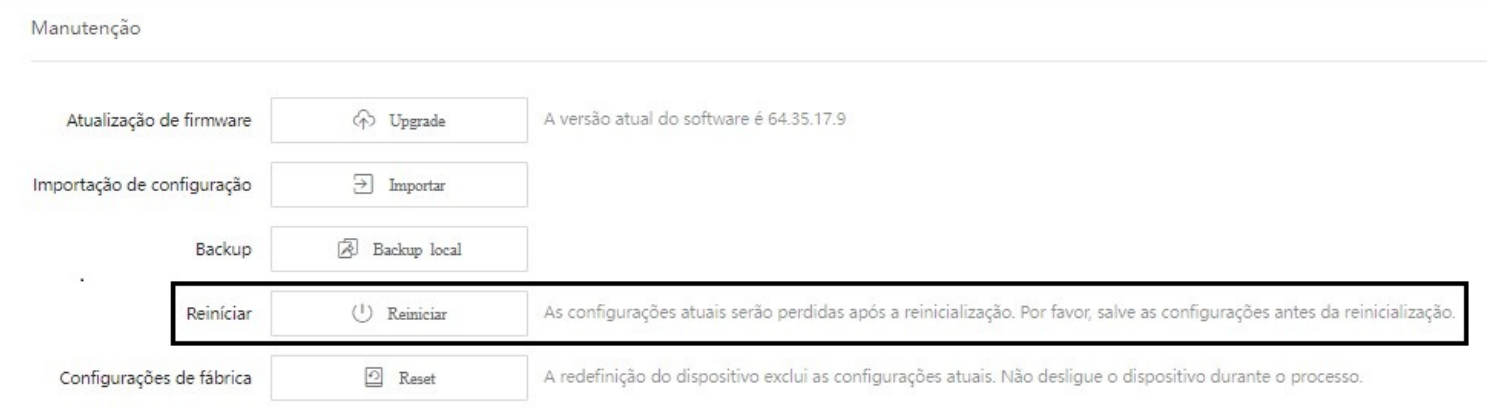
Clique em **Cloud Backup** , você pode fazer backup das configurações do switch para a plataforma Intelbras CloudFi.

Reinício

Quando um parâmetro definido não funciona corretamente, você pode tentar reiniciar o switch para corrigir esse problema

Clique em **Básico > Manutenção** para entrar na página. Nesta página, você pode clicar em Reiniciar para **reiniciar** o switch.

Por favor, clique em **salvar** no canto superior direito para salvar todas as configurações antes de redefinir o switch



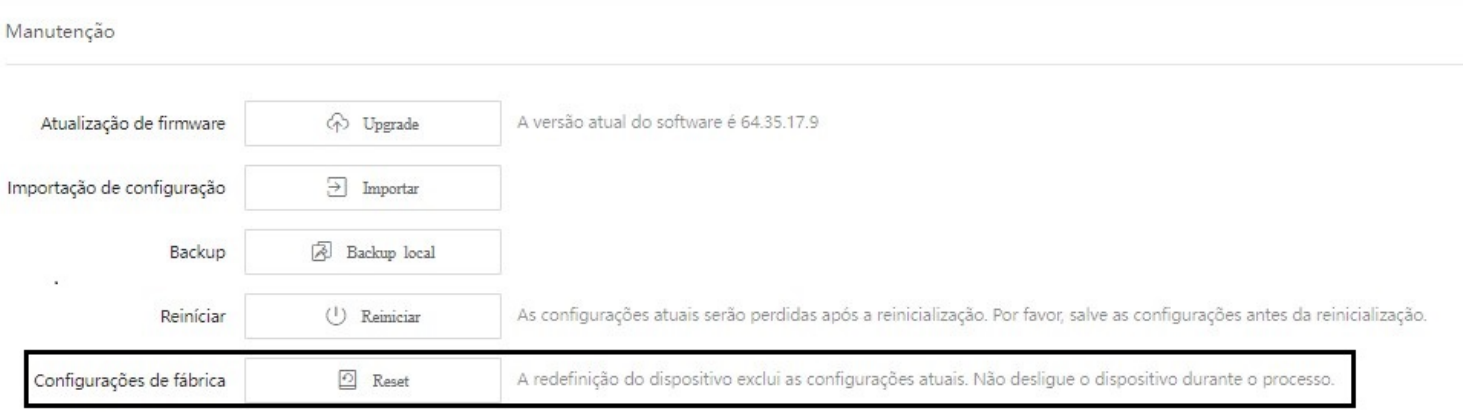
Configurações de fábrica

Se você esquecer seu nome de usuário ou senha ao fazer login na interface do usuário da web do switch, poderá restaurar as configurações de fábrica do switch e, em seguida, usar o nome de usuário e a senha padrão (ambos são admin) para fazer login . e reinicialização de hardware .

Redefinição de software

Clique em **Básico > Manutenção** para entrar na página. Nesta página, você pode clicar em **Redefinir** para restaurar a chave para as configurações de fábrica

> Para evitar quaisquer danos, certifique-se de fornecer uma fonte de alimentação estável ao switch durante o processo de reinicialização.



Redefinição de hardware

Quando o indicador LED **SYS** estiver piscando, pressione o botão de reinicialização por cerca de 10 segundos usando um objeto semelhante a uma agulha (como um alfinete) e solte-o quando todos os indicadores estiverem acesos. Quando o indicador LED SYS piscar novamente, a chave será restaurada para as configurações de fábrica.

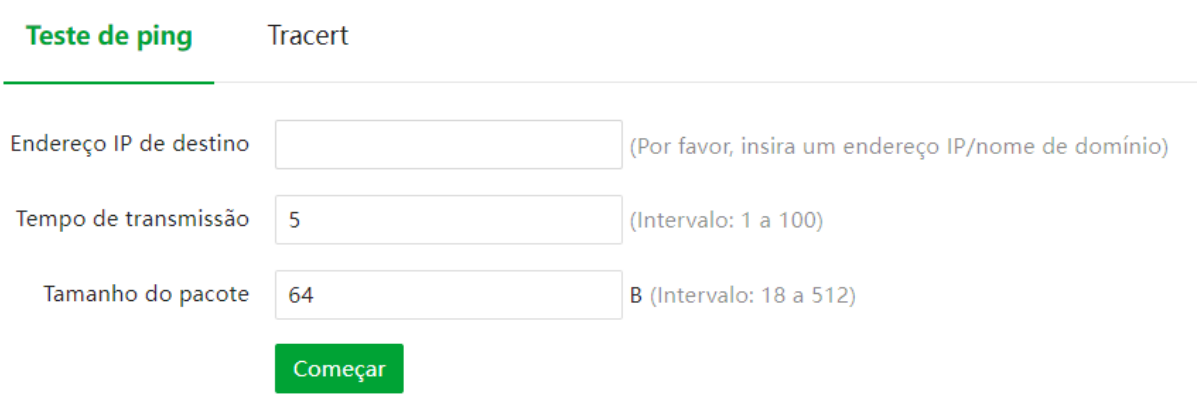
Diagnóstico

Clique em **Básico > Diagnóstico** para entrar na página. Nesta página, você pode executar o teste Ping/Tracert.

- Teste de ping : É usado para testar a conexão de rede e a qualidade da conexão.
- Teste Tracert : É usado para testar as rotas dos pacotes do switch para o host de destino.

Teste de ping

Clique em **Básico > Diagnóstico > Teste de Ping** para entrar na página. Nesta página, você pode testar a conexão de rede e a qualidade da conexão.

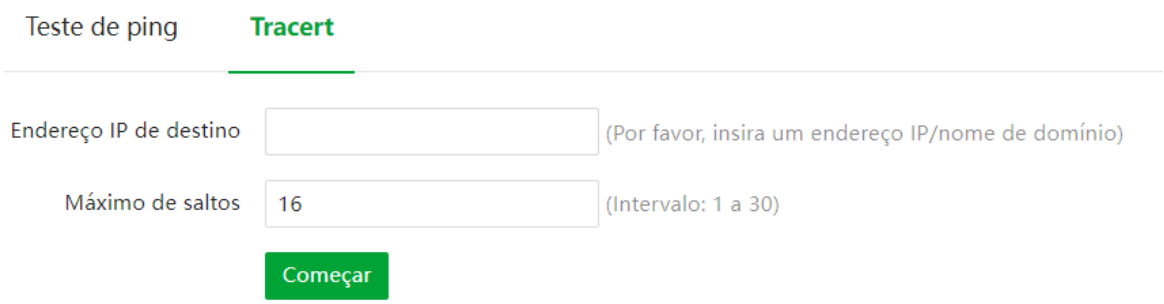


Descrição do parâmetro

Nome	Descrição
Endereço IP de destino	Ele especifica o endereço IP ou nome de domínio do dispositivo de destino para o qual será executado o ping.
Tempos de Transmissão	Especifica o número de pacotes de dados enviados pelo Ping.
Tamanho do pacote	Especifica o tamanho dos pacotes de dados enviados pelo Ping.

Teste tracert

Clique em **Básico > Diagnóstico > Tracert** para entrar na página. Nesta página, você pode testar as rotas dos pacotes que passam do switch para o dispositivo de destino.



Nome	Descrição
Endereço IP de destino	Ele especifica o endereço IP ou nome de domínio do dispositivo de destino a ser testado
Saltos Máximos	Ele especifica o tempo de sobrevivência da mensagem, que é o número máximo de roteadores pelos quais a mensagem pode passar.

Gerenciamento de nuvem

A plataforma Intelbras CloudFi é desenvolvida pela intelbras, fornecendo gerenciamento central para dispositivos que suportam gerenciamento de nuvem.

Clique em **Básico > Gerenciamento de Nuvem** para entrar na página de configuração. Você pode habilitar ou desabilitar a função de gerenciamento de nuvem do switch.

Com o switch gerenciado pela plataforma Intelbras (CloudFi web UI ou CloudFi App), você pode configurar e verificar os parâmetros do switch na plataforma. Você também pode configurar e verificar esses parâmetros na interface do usuário da web do switch.

- Para saber como adicionar o switch à plataforma Intelbras CloudFi, consulte o Guia de Instalação Rápida do switch.

- Com o comutador gerenciado pela plataforma, você pode modificar os parâmetros do comutador na plataforma Intelbras CloudFi ou na IU da web local do comutador. Os parâmetros do switch entram em vigor com base na última modificação

Espionagem DHCP

Visão Geral

DHCP Snooping é um mecanismo de segurança que protege o serviço DHCP.

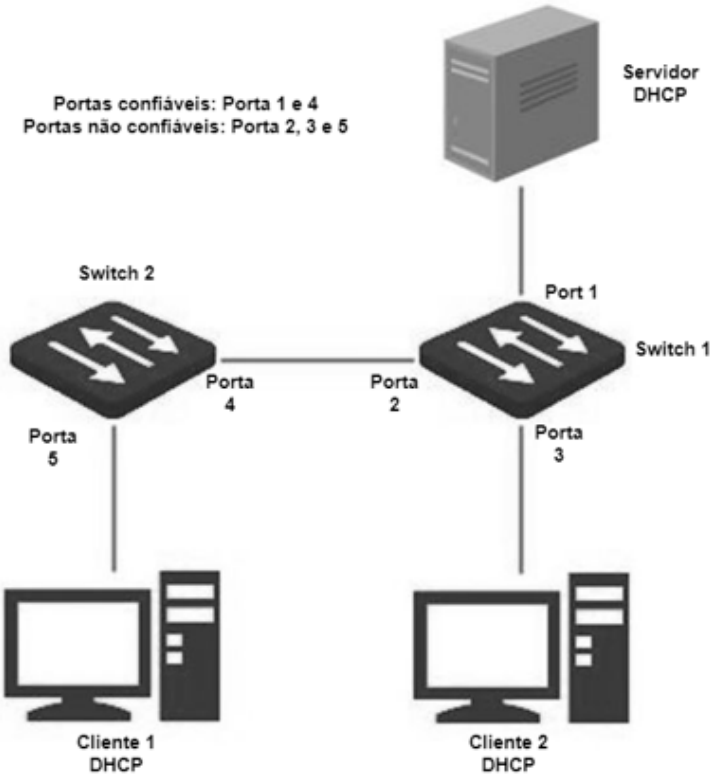
Ele garante que os clientes DHCP possam obter endereços IP dos servidores corretos.

A porta que conecta ao servidor DHCP autorizado é a porta confiável e as outras portas são portas não confiáveis. O switch encaminha as mensagens DHCP recebidas pelas portas confiáveis e descarta as mensagens de resposta recebidas pelas portas não confiáveis do servidor DHCP, de modo a garantir que os clientes DHCP possam obter apenas os endereços IP dos servidores DHCP corretos.

Ele registra as entradas da tabela DHCP Snooping.

Ao espionar a mensagem de solicitação DHCP e a mensagem DHCP-ACK recebida pela porta confiável, o switch estabelece uma tabela de espionagem DHCP, que inclui o endereço MAC do cliente, o endereço IP do cliente DHCP atribuído pelo servidor DHCP, a porta que conecta o cliente DHCP e as informações da VLAN. A tabela DHCP Snooping é uma base importante para a validação ARP.

A topologia de rede do DHCP Snooping é mostrada na figura a seguir. Suponha que a função DHCP Snooping do switch 1 e do switch 2 esteja habilitada.



A função DHCP snooping só está disponível quando esta função está habilitada e o switch está entre o cliente DHCP e o servidor DHCP (ou DHCP relay) na rede de conexão. Quando o switch está entre o servidor DHCP e o relé DHCP, a função de espionagem DHCP não está disponível.

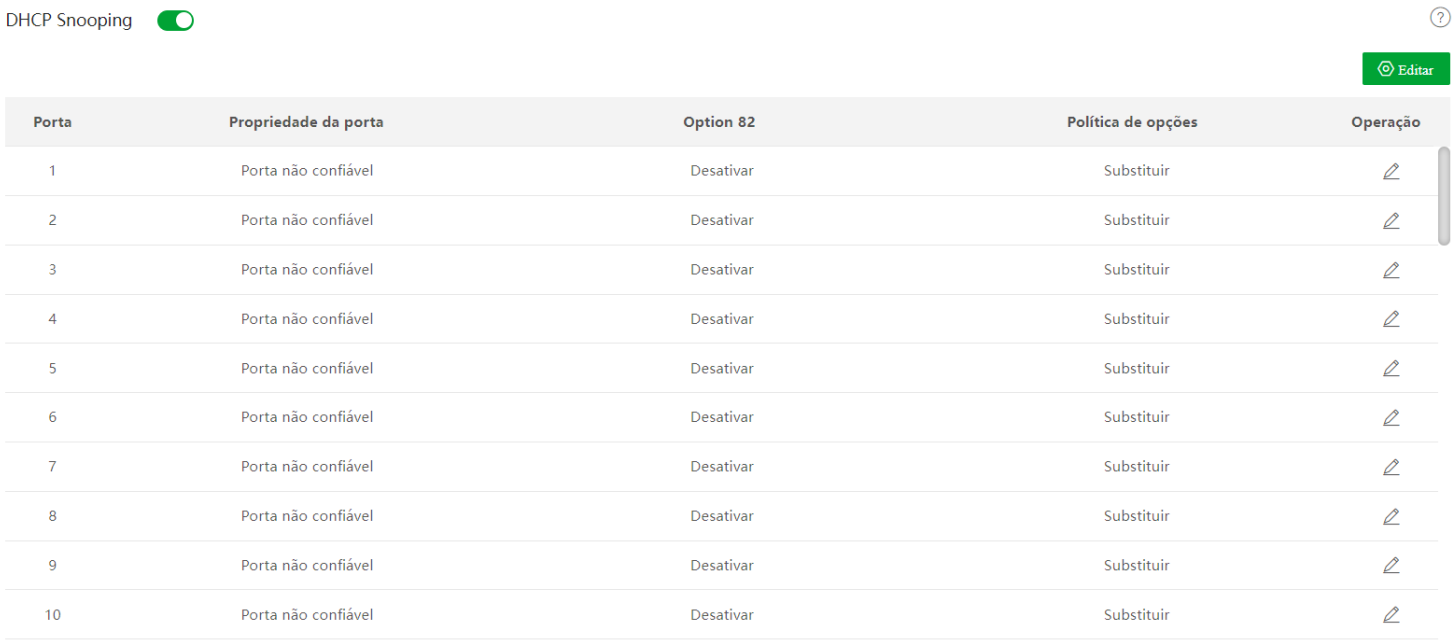
A opção 82, também chamada de opção de informações do agente de retransmissão DHCP, é uma opção na mensagem DHCP que registra as informações de localização dos clientes DHCP. Você pode usar esta opção para localizar o cliente DHCP, implementando assim segurança e controle de cobrança para clientes. O endereço IP correspondente e as políticas de alocação de parâmetros também podem ser configurados no servidor DHCP de acordo com as informações da Opção 82, alocando assim o endereço IP de forma flexível.

Por padrão, a opção 82 dessa opção está desativada. Depois de habilitado, o mecanismo de funcionamento da Opção 82 desta chave é mostrado a seguir:

Tipo de mensagens recebidas	Política de processamento
Mensagem de solicitação DHCP com opção 82	As mensagens de solicitação DHCP são processadas de acordo com as seguintes políticas de configuração • **Substituir** : Substitua as informações originais da Opção 82 na mensagem pelo conteúdo padrão da central e encaminhe-a. • **Reter** : Reter o estado original da Opção 82 na mensagem e encaminhá-la. • **Descartar** : Descarte o pacote de solicitação DHCP com a Opção 82 e encaminhe a mensagem de solicitação DHCP sem a Opção 82.
Mensagem de resposta DHCP	Exclua a opção 82 do pacote de resposta DHCP e encaminhe a mensagem.

DHCP Snooping

Clique em **Switching > DHCP Snooping** para entrar na página. Nesta página, você pode configurar as regras de DHCP Snooping.



Nome	Descrição
Opção 82	Ele especifica o status da Opção 82. Você pode habilitar ou desabilitar a função da Opção 82 clicando em editar. A opção 82 registra as informações de localização do cliente DHCP. A política de opção entra em vigor quando a Opção 82 é habilitada. Por favor, consulte a Opção 82 para seu mecanismo de trabalho.

Nome	Descrição
Política de opções	Três políticas da Opção 82 são suportadas por este switch: • **Substituir** : Quando o DHCP Relay recebe mensagens de solicitação DHCP, ele substitui as informações originais da Opção 82 pelo conteúdo padrão do switch e encaminha as mensagens. • **Retain** : Quando o DHCP Relay recebe mensagens de solicitação DHCP, ele retém o estado original da Opção 82 e encaminha a mensagem. • **Discard** : O DHCP Relay descarta a mensagem de solicitação DHCP com a opção 82 e encaminha a mensagem de solicitação DHCP sem a opção 82.

Spannig tree

Visão geral

Spanning Tree ajuda a evitar loops na rede para proteger a rede de tempestades de transmissão e fornecer backup de redundância de link. Este switch suporta três modos spanning tree: STP (Spanning Tree Protocol), RSTP (Rapid Spanning Tree Protocol) e MSTP (Multi Spanning Tree Protocol).

STP

STP é um protocolo de rede baseado em IEEE 802.1d. É um protocolo que garante uma topologia sem loop para rede local e fornece links redundantes de backup. Os dispositivos sob este protocolo descobrem os loops na rede comunicando-se entre si, e bloqueiam seletivamente algumas portas, e eventualmente estabelecem uma estrutura spanning tree sem loops, de forma a evitar o declínio da capacidade de processamento de mensagens dos dispositivos devido ao proliferação contínua e circulação infinita de mensagens na rede de loop.

Mensagem do protocolo STP

Para implementar a função spanning tree, os switches na rede transferem BPDUs (Bridge Protocol Data Unit) entre si para trocar informações. Os BPDUs carregam as informações necessárias para os switches calcularem a spanning tree.

A topologia da rede é determinada pela transmissão BPDU entre os dispositivos. Existem dois tipos de BPDUs do protocolo STP:

- Configuração BPDU: É usado para cálculo de spanning tree e manutenção da topologia de spanning tree.
- TCN BPDU (Topology Change Notification BPDU): É utilizado para notificar as mudanças na estrutura da topologia da rede.

Conceitos básicos de STP

- **ID da ponte**

  O ID da ponte contém a prioridade da ponte e o endereço MAC, no qual a prioridade da ponte é um parâmetro configurável. Quanto menor o ID da ponte, maior a prioridade da ponte. A ponte raiz é a ponte com o menor ID de ponte.

- **Ponte raiz**

A ponte de raiz atua como a raiz de uma árvore. Existe apenas uma root bridge na rede e ela pode ser alterada de acordo com as mudanças na topologia da rede.

Inicialmente, todos os dispositivos se consideram root bridges. Eles geram seus próprios BPDUs de configuração e os enviam periodicamente. Quando a topologia de rede se torna estável, apenas o dispositivo root bridge pode enviar BPDUs de configuração e outros dispositivos podem apenas encaminhar esses BPDUs.

- **Porta raiz**

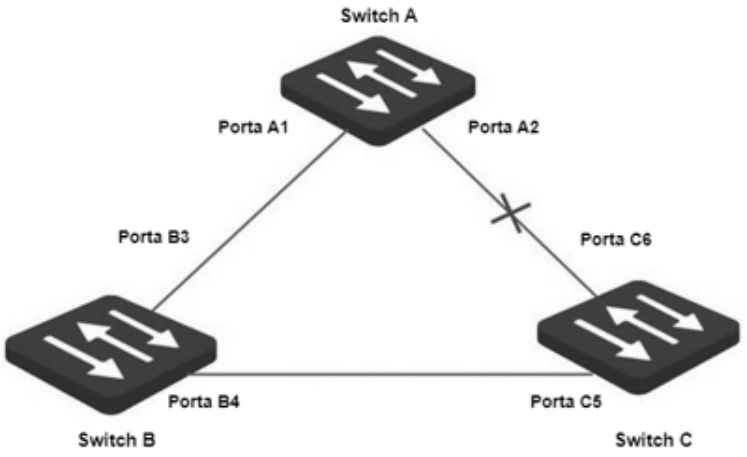
A porta root é a porta em um dispositivo não root bridge que possui o menor custo de caminho da bridge até a root bridge, responsável pela comunicação com a root bridge. Há apenas uma porta raiz no dispositivo não-root bridge e nenhuma porta raiz no dispositivo root bridge.Ponte designada e porto designado

- Ponte designada: Para um switch, a ponte designada é o dispositivo que se conecta e encaminha BPDUs para o switch. Para a LAN, é o dispositivo que encaminha BPDUs no mesmo segmento de rede.
- Em cada segmento de rede, o dispositivo com o menor custo de caminho para a ponte raiz é a ponte designada. Se mais de um switch tiver o mesmo custo de caminho para a ponte raiz, aquele com o menor ID de ponte será a ponte designada.
- Porta designada: Quanto a um dispositivo, é a porta que encaminha BPDUs para o host. Já para uma LAN, é a porta que encaminha BPDUs no mesmo segmento de rede.

Custo do caminho

É um parâmetro para escolha do caminho do link pelo STP. Ao calcular o custo do caminho, o STP escolhe os melhores enlaces e bloqueia os enlaces redundantes, de modo a desmembrar a rede de loops para formar uma rede livre de loops topológicos.

O diagrama de rede básico do STP é mostrado na figura a seguir. Os interruptores A, B e C são conectados sucessivamente.



Após o cálculo, o switch A é selecionado como root bridge e o link entre as portas A2 e C6 é bloqueado.

- Pontes: O switch A é a ponte raiz da rede, enquanto o switch B é a ponte designada do switch C.
- Portas: A porta B3 e a porta C5 são as portas raiz do switch B e do switch C, respectivamente.

- A porta A1 e a porta B4 são as portas designadas do switch A e do switch B, respectivamente.
- A porta C6 é a porta de bloqueio do switch C.

Prioridade BPDU

Quanto menor for o ID da ponte, maior será a prioridade da ponte. Se o ID da ponte raiz for o mesmo, os custos do caminho raiz serão comparados. O método de comparação é assumir que o custo do caminho raiz em BPDU e o custo do caminho correspondente a esta porta são S, então o BPDU com S menor tem maior prioridade.

Se os custos do caminho raiz forem os mesmos, compare o ID da ponte designada, o ID da porta designada e o ID da porta que recebe o BPDU sucessivamente, aquele com o menor ID tem maior prioridade.

Processo de computação STP

1. Estado inicial

Inicialmente, cada porta do switch gera um BPDU considerando o switch como root bridge, com o custo do caminho raiz sendo 0, o ID da ponte designada sendo o switch ID e a porta designada sendo ela mesma.

2. Seleção de BPDU ideal

Cada switch envia seus BPDUs e recebe BPDUs de outros switches. A tabela a seguir mostra o procedimento para selecionar o BPDU ideal.

Etapa	Contente
1	Recebendo BPDU com menor prioridade: Se a prioridade do BPDU recebido por uma porta for menor que a da própria porta, o switch descarta o BPDU recebido e não trata o BPDU dessa porta. Recebendo BPDU com maior prioridade: Se a prioridade do BPDU recebido for maior que a da própria porta, o switch substitui o BPDU da porta pelo recebido.
2	O switch seleciona o melhor BPDU comparando BPDUs em todas as portas.

3. Seleção da ponte raiz

A ponte raiz é selecionada pela troca de BPDU e comparação de ID da ponte raiz. O switch com o menor ID de root bridge é escolhido como root bridge.

4. Porta raiz e seleção de porta designada

O procedimento de seleção é mostrado na tabela a seguir:

Etapa	Contente
1	Para cada switch (exceto o root bridge), a porta que recebe o BPDU ideal é escolhida como a porta raiz do switch.

Etapa	Contente
2	O switch calcula um BPDU de porta designado para cada porta de acordo com o BPDU da porta raiz e o custo do caminho da porta raiz. • O ID da ponte raiz é substituído pelo da porta raiz. • O custo do caminho raiz é substituído pela soma do custo do caminho raiz da porta raiz. BPDU e o custo do caminho correspondente à porta raiz. • O ID da ponte designada é substituído pelo do próprio switch. • O ID da porta designada é substituído pelo próprio ID da porta
3	O switch compara o BPDU calculado com o BPDU da porta cuja função precisa ser determinada e lida com a porta de acordo com diferentes resultados de comparação. • Se o BPDU calculado tiver precedência sobre o BPDU da porta, a porta será escolhida como a porta designada com seu BPDU substituído pelo BPDU calculado e enviará regularmente o BPDU. • Se o BPDU desta ort tiver precedência sobre o BPDU calculado, o BPDU desta porta não será alterado e a porta será bloqueada. A porta recebe apenas BPDUs, mas não pode encaminhar BPDU ou outros dados.

Em uma topologia estável, apenas as portas raiz e as portas designadas podem encaminhar dados, e as outras portas são bloqueadas. As portas bloqueadas podem apenas receber BPDUs, mas não encaminhar dados.

Temporizador STP

- **Alô hora**

Ele especifica o intervalo para a ponte raiz enviar mensagens BPDU para outros switches, usado para testar se os links estão funcionando mal.

- **Tempo Máximo de Envelhecimento**

Ele especifica a duração máxima durante a qual, se um switch não receber uma mensagem BPDU da root bridge, ele enviará pacotes BPDU a todos os outros switches para recalcular o novo STP.

- **Atraso de Encaminhamento**

Ele especifica o tempo de atraso que a migração do estado da porta leva após a alteração da topologia da rede.

O mau funcionamento do link leva ao recálculo do STP na rede; nesse caso, a estrutura do STP será alterada de acordo. No entanto, como os novos BPDUs não podem ser distribuídos para toda a rede imediatamente, os loops temporais podem ocorrer se as novas portas raiz e as portas designadas encaminharem dados de uma só vez. Portanto, o STP adota um mecanismo de migração de estado, ou seja, as novas portas raiz e as portas designadas começam a encaminhar dados após o dobro do atraso de encaminhamento, o que garante que os novos BPDUs sejam espalhados por toda a rede.

RSTP

RSTP é definido pelo padrão IEEE 802.1w e compatível com IEEE 802.1d STP. Além de rede sem loop e links redundantes, apresenta rápida convergência. Se todas as pontes em uma LAN suportarem RSTP, isso permitirá uma rápida geração de árvore de topologia quando a topologia da rede mudar (árvore de topologia STP tradicional:

50 segundos, árvore de topologia RSTP: 1 segundo).

O RSTP determina a topologia da rede trocando BPDUs entre switches. No entanto, o

O formato BPDU do RSTP difere daquele do STP. Quando a topologia está mudando, mensagens RST-BPDU são espalhadas por floods para notificar a mudança para toda a rede.

Condições para migração rápida de estado das portas raiz e portas designadas no RSTP:

- Porta raiz: a porta raiz original do switch para de encaminhar dados e a porta designada do switch upstream começa a encaminhar dados.
- Porta designada: Se a porta designada for uma porta de borda, ela pode transitar diretamente para o estado de encaminhamento; se a porta designada for uma porta P2P, ela poderá transitar para o estado de encaminhamento assim que receber a resposta do switch downstream por meio do handshake.

- **Porta de Borda**

  Uma porta de borda é uma porta designada na borda da rede de comutação. É conectado diretamente aos dispositivos terminais. Uma porta de borda pode transitar para o estado de encaminhamento imediatamente sem passar pelos estados de escuta e aprendizado. Se receber um BPDU, ele imediatamente passa de uma porta de borda para uma porta de spanning tree comum e se junta à geração de STP.

- **Porta P2P**

  Uma porta P2P usada para conectar a outros switches. Sob RSTP/MSTP, todas as portas operando no modo fullduplex são portas P2P.

MSTP

Desvantagens de STP e RSTP em ambientes de trabalho comuns:

- STP: As portas não podem transitar rapidamente pelos estados, e mesmo as portas em links com portas ponto a ponto e portas de borda só podem transitar para os estados de encaminhamento após o dobro do atraso de encaminhamento.
- RSTP: Possui convergência rápida, mas como todas as VLANs na LAN compartilham apenas uma spanning tree e todas as mensagens das VLANs devem ser encaminhadas ao longo desta spanning tree. Portanto, os links redundantes não podem ser bloqueados por VLANs e a carga de tráfego de dados não pode ser balanceada entre as VLANs.

MSTP é definido pelo padrão IEEE 802.1s e compatível com STP e RSTP. Ele não apenas apresenta convergência rápida, mas também permite que fluxos de dados de diferentes VLANs sejam encaminhados ao longo dos caminhos, respectivamente. Essas funções levam a um melhor mecanismo de compartilhamento de carga para links redundantes e compensam as limitações de STP e RSTP.

Características do MSTP:

- O MSTP oferece suporte ao mapeamento de VLANs para as instâncias de spanning tree por meio da tabela de mapeamento de VLAN para instância e realiza o balanceamento de carga mapeando várias VLANs para uma instância.

- O MSTP divide a rede spanning tree em várias regiões, cada uma contendo spanning tree internas independentes umas das outras.
- O MSTP transforma uma rede de loop em uma rede de árvore sem loop para evitar a proliferação contínua e a circulação interminável de mensagens e também fornece vários caminhos redundantes para encaminhamento de dados, garantindo assim o balanceamento de carga no processo de encaminhamento de dados.

- **Região MST**

  As regiões MST (Multiple Spanning Tree Regions) são compostas por vários dispositivos em uma rede de comutação e seus segmentos de rede.

  Esses dispositivos têm as seguintes características:

  - Um protocolo spanning tree ativado
  - Mesmo nome de região
  - Mesmo resumo de configuração (a configuração do relacionamento de mapeamento entre VLAN e MSTI é a mesma)
  - Mesmo nível de revisão MSTP
  - Fisicamente ligados entre si

- **MSTI**

  O MSTP pode gerar várias spanning tree independentes em uma região MST, e cada spanning tree é considerado um MSTI (Multiple Spanning Tree Instance). Na região MST, o MSTP gera várias Spanning Trees de acordo com a tabela de mapeamento de VLAN para instância e mapeia as VLANs para as Spanning Trees. O método de cálculo da spanning tree do MSTP é o mesmo do STP.

- **IST**

  Uma IST (Internal Spanning Tree) é uma spanning tree especial na região MST. É comumente chamado de MSTI 0.

- **CST**

  CST (Common Spanning Tree) é uma única árvore de abrangência que conecta todas as regiões MST dentro da rede. O MSTP considera as regiões MST como dispositivos separados e gera CST conectando-se a todas as regiões.

- **CIST**

  CIST (Common and Internal Spanning Tree) é uma única spanning tree que conecta todos os dispositivos dentro da rede. É composto pelas ISTs de todas as regiões do MST e pela CST.

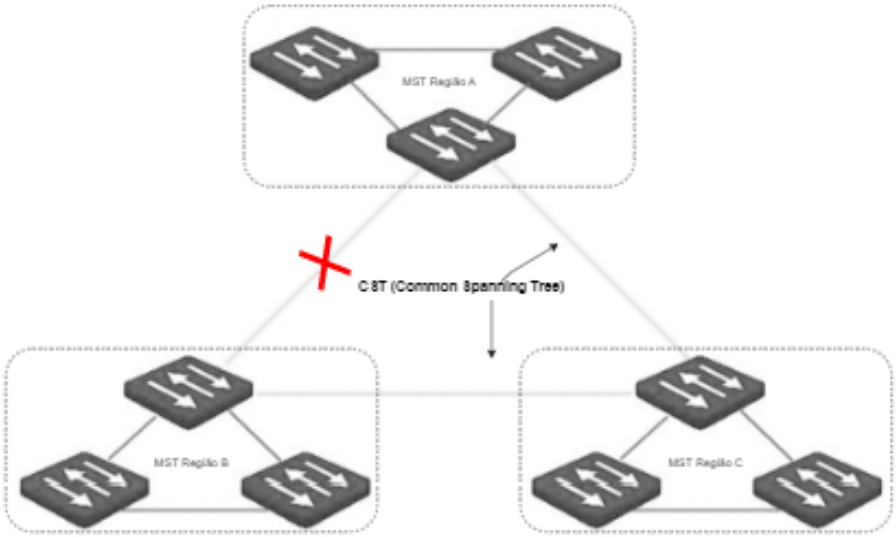
- **Raiz regional**

  Regional Root é a ponte raiz do IST ou MSTI dentro da região MST. As raízes regionais variam com diferentes topologias de spanning tree.

- **Ponte Raiz Comum**

  O Common Root Bridge é o root bridge do CIST. Com base na comparação de BPDUs, o MSTP seleciona um dispositivo ideal como a ponte raiz comum em toda a rede.

Semelhante ao STP, o MSTP usa BPDUs para calcular spanning tree, exceto que os BPDUs carregam informações de configuração do MSTP. O diagrama conceitual básico do MSTP é mostrado a seguir.



Status da porta

No MSTP, o status da porta inclui os quatro tipos a seguir, dependendo se a porta pode encaminhar dados e as formas de processar BPDUs:

- Encaminhamento: a porta recebe e encaminha dados, recebe e envia BPDUs e aprende endereços.
- Learning: A porta não recebe ou encaminha dados, mas recebe e envia BPDUs, também aprende endereços.

Descartando: A porta não recebe ou encaminha dados, nem envia BPDUs ou aprende endereços, mas recebe BPDUs.

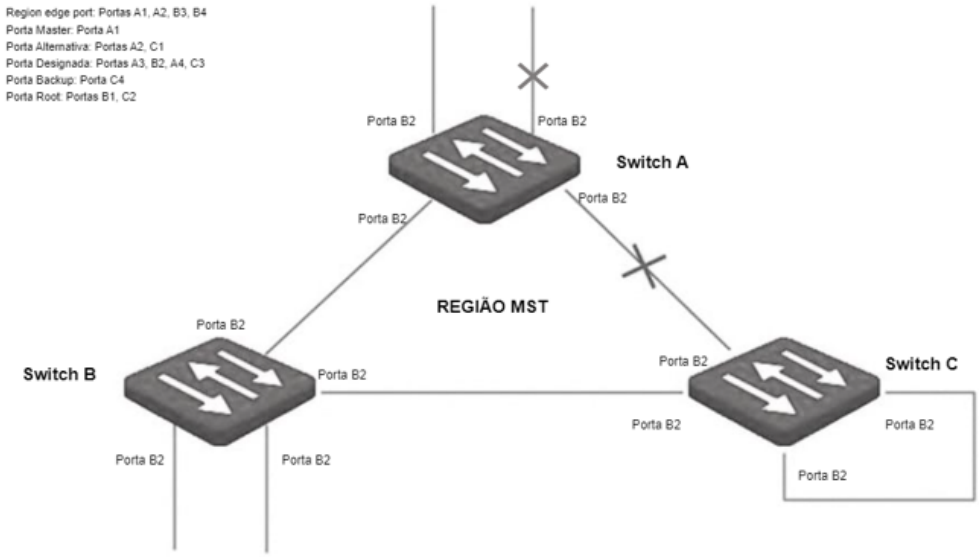
- Disabled: A porta não está conectada fisicamente.

Função da porta

No MSTP, existem diferentes funções das portas:

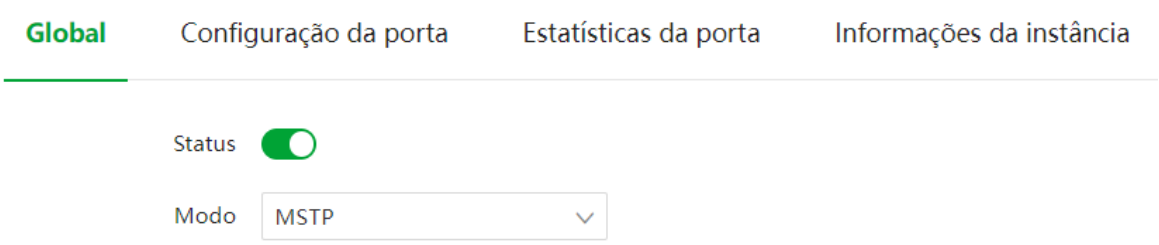
- Porta raiz: tem o menor custo passado para a ponte raiz e é responsável por encaminhar dados de uma ponte não raiz para a ponte raiz.
- Porta designada: encaminha dados para o segmento ou dispositivo de rede downstream.
- Porta master: Está no caminho mais curto da região MST até a common root bridge, conectando a região MST à common root bridge.
- Porta alternativa: Atua como a porta de backup para a porta raiz ou porta mestre.
- Porta de backup: Atua como a porta de backup para a porta designada.
- Desabilitar porta: É uma porta que não está conectada fisicamente.

As funções de porta são mostradas no diagrama a seguir.



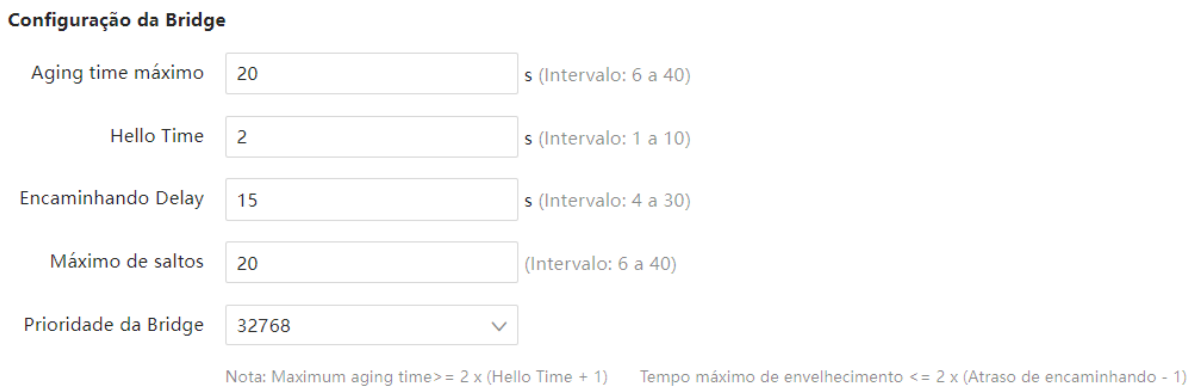
Global

Clique em **Switching > Spanning Tree > Global** para entrar na página. Nesta página, você pode configurar os parâmetros globais da spanning tree.



Nome	Descrição
Status	Ele é usado para habilitar ou desabilitar a função spanning tree.
Modo	O switch suporta três modos spanning tree: STP, RSTP e MSTP. • STP : Spanning Tree Protocol. • RSTP : Rapid Spanning Tree Protocol, compatível com o protocolo STP, apresentando convergência rápida. • MSTP : Multiple Spanning Tree Protocol, compatível com RSTP e STP, proporcionando melhor mecanismo de compartilhamento de carga para links redundantes.

Configuração da Ponte



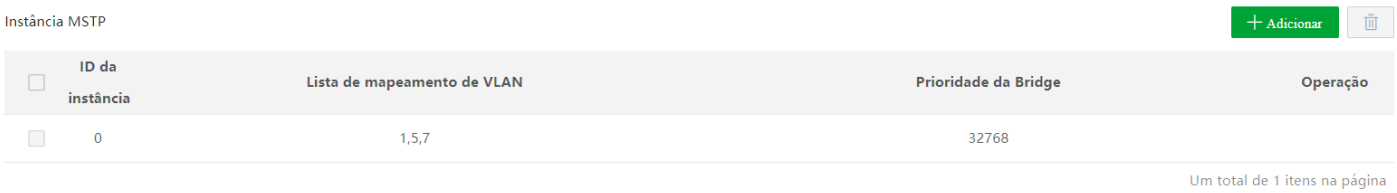
Descrição do parâmetro

Nome	Descrição
Tempo Máximo de Envelhecimento	Especifica a duração máxima durante a qual o BPDU pode ser mantido no switch. A configuração deve atender às seguintes fórmulas: • Tempo Máximo de Envelhecimento ≥ 2 × (Hello Time + 1). • Tempo Máximo de Envelhecimento ≤ 2 × (Atraso de Encaminhamento - 1).
Alô hora	Ele especifica o intervalo no qual o switch envia BPDU, que é definido como 2 segundos por padrão.
Atraso de Encaminhamento	Ele especifica o atraso que a migração do estado da porta leva após as alterações na topologia da rede, que é definido como 15 segundos por padrão.
Saltos Máximos	Especifica o número máximo de BPDU que pode ser encaminhado, usado para limitar a escala da spanning tree.
Ponte Prioridade	Especifica a prioridade do sistema de um switch na participação no cálculo da spanning tree. A prioridade é um critério importante pelo qual a root bridge é determinada. O switch com prioridade mais alta será escolhido como root bridge em igualdade de condições.

Configuração da Região MSTP

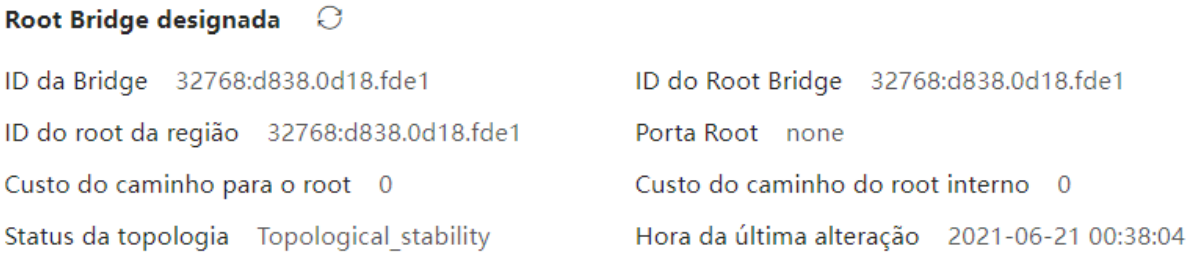
Nome	Descrição
Nome da região	Ele especifica a identidade da região MST. O valor padrão é o endereço MAC do switch.
Revisão	Ele especifica o nível de revisão do MSTP, que é definido como 0 por padrão.
Digerir	Ele especifica a identidade da região MST. O valor padrão é o endereço MAC do switch.

Instância MSTP



Nome	Descrição
ID da instância	Um máximo de 32 instâncias são permitidas. 0 indica spanning tree interno. A spanning tree é calculada por cada instância separadamente.
Lista de mapeamento de VLAN	Ele especifica o nível de revisão do MSTP, que é definido como 0 por padrão.
Ponte Prioridade	Ele especifica a prioridade do sistema de instância usada para eleição de root bridge de instâncias em regiões MST.

Root Bridge especificado

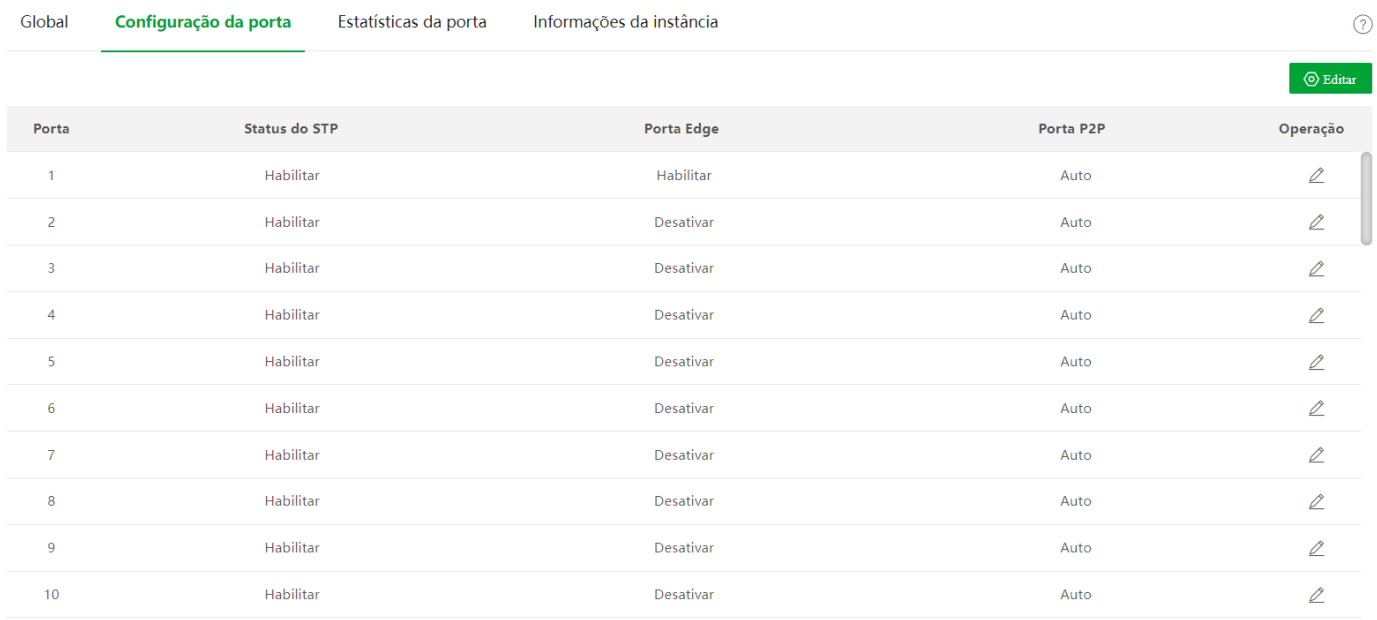


Nome	Descrição
ID da ponte	ID da raiz da região.
Custo do caminho raiz	Ele especifica a soma do custo do caminho da porta raiz e o custo do caminho raiz de todos os switches pelos quais os pacotes passam. O custo do caminho raiz da ponte raiz é 0.

Nome	Descrição
Status da topologia	Ele especifica o status da topologia da spanning tree deste switch. • Topology_calculation : A porta está instável durante o cálculo da spanning tree e os pacotes não podem ser encaminhados. Normalmente, com os parâmetros de tempo padrão, o status Topology_calculation pode durar até 50 segundos quando o modo é STP, enquanto para RSTP e MSTP, a duração do tempo é inferior a 3 segundos. • Topological_stability : A porta está estável e a rede está normal.
ID da ponte raiz	Para STP e RSTP, especifica a prioridade da ponte e o endereço MAC da ponte raiz; enquanto para MSTP, especifica a prioridade da ponte e o endereço MAC da ponte raiz comum.
Porta Raiz	Ele especifica a porta mais próxima da root bridge em um switch sem root bridge.
Custo do Caminho Raiz Interno	Ele especifica o valor de referência usado para escolher o caminho e calcular o custo do caminho no caminho da região MST. É também o critério usado para determinar se a porta é escolhida como a porta raiz. Quanto menor o valor, maior será a prioridade.
Hora da última alteração	Especifica a hora da última mudança de topologia.

Configuração da porta

Clique em **Switching > Spanning Tree > Configuração de porta** . Nesta página, você pode configurar os parâmetros STP das portas.



Descrição do parâmetro

Nome	Descrição
Porta	Ele especifica o ID da porta.
Estado STP	Indica se a função STP está habilitada ou não. a função STP em Global e a configuração da porta estiver habilitada pode o cálculo da spanning tree de junção da porta.
Porta de Borda	A porta de borda pode migrar rapidamente para o estado de encaminhamento do estado de congestionamento. Não há necessidade de esperar pelo tempo de atraso. A porta de borda é comumente conectada a terminais. Ao receber mensagens BPDU, a porta de borda é alterada para uma porta sem borda. Todas as portas são portas non-edge por padrão. • Desativar : Esta porta é uma porta sem borda. • Ativar : esta porta é uma porta de borda.
Porta P2P	Uma porta P2P pode executar uma migração rápida. No modo RSTP/MSTP, todas as portas no modo fullduplex são consideradas portas P2P. A porta padrão identifica links automaticamente. • Auto : A porta P2P pode ser identificada automaticamente. • Habilitar : Esta porta é uma porta P2P. • Disable : Esta porta não é uma porta P2P.

Root Bridge especificado

Clique em **Switching > Spanning Tree > Port Statistics** para entrar na página. Nesta página, você pode visualizar os pacotes spanning tree transmitidos, recebidos e descartados por cada porta.

Porta	Transmitido				Recebido				Descartar	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
1	118	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0

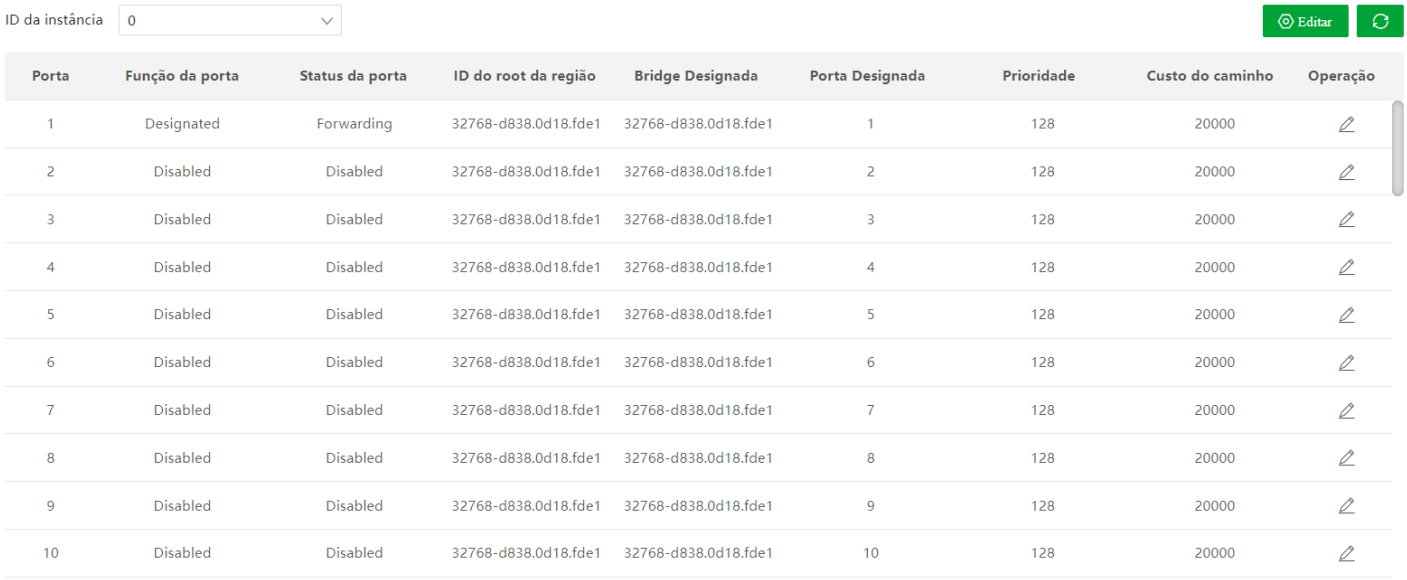
Descrição do parâmetro

Nome	Descrição
Porta	Ele especifica o ID da porta.

Nome	Descrição
MSTP	Especifica o número de BPDUs de configuração com informações RSTP transmitidas ou recebidas pela porta.
STP	Especifica o número de BPDUs de configuração com informações STP transmitidas ou recebidas pela porta.
TCN	Especifica o número de mensagens TCN BPDU transmitidas ou recebidas pela porta.
Desconhecido	Ele especifica o número de pacotes STP desconhecidos descartados.
Ilegal	Ele especifica o número de pacotes STP com erro descartados.

Informações da instância

Clique em **Switching > Spanning Tree > Informações da instância** para entrar na página. Nesta página, você pode visualizar e configurar as informações da instância MSTP.



Porta	Função da porta	Status da porta	ID do root da região	Bridge Designada	Porta Designada	Prioridade	Custo do caminho	Operação
1	Designated	Forwarding	32768-d838.0d18.fde1	32768-d838.0d18.fde1	1	128	20000	
2	Disabled	Disabled	32768-d838.0d18.fde1	32768-d838.0d18.fde1	2	128	20000	
3	Disabled	Disabled	32768-d838.0d18.fde1	32768-d838.0d18.fde1	3	128	20000	
4	Disabled	Disabled	32768-d838.0d18.fde1	32768-d838.0d18.fde1	4	128	20000	
5	Disabled	Disabled	32768-d838.0d18.fde1	32768-d838.0d18.fde1	5	128	20000	
6	Disabled	Disabled	32768-d838.0d18.fde1	32768-d838.0d18.fde1	6	128	20000	
7	Disabled	Disabled	32768-d838.0d18.fde1	32768-d838.0d18.fde1	7	128	20000	
8	Disabled	Disabled	32768-d838.0d18.fde1	32768-d838.0d18.fde1	8	128	20000	
9	Disabled	Disabled	32768-d838.0d18.fde1	32768-d838.0d18.fde1	9	128	20000	
10	Disabled	Disabled	32768-d838.0d18.fde1	32768-d838.0d18.fde1	10	128	20000	

Descrição do parâmetro

Nome	Descrição
ID da instância	Ele é usado para selecionar o ID da instância para verificar as informações do estado STP da instância.
Porta	Ele especifica o ID da porta.
Função da porta	Ele especifica a função que a porta desempenha na instância da spanning tree. Para obter mais detalhes, consulte Função da porta.
Status da porta	Ele especifica o status operacional atual da porta. Para obter mais detalhes, consulte o status da porta.
ID da raiz da região	Ele especifica a prioridade da ponte e o endereço MAC da ponte raiz regional.

Nome	Descrição
Ponte designada	Ele especifica o ID da ponte do switch que se conecta a esse switch e é usado para encaminhar mensagens BPDU para o switch. O ID de ponte designado da porta raiz e da porta de backup é o ID de ponte do switch usado para enviar mensagens BPDU; enquanto o ID de ponte designado da porta designada é o ID de ponte do próprio switch.
Porto Designado	Ele especifica a porta para a qual a ponte designada encaminha as mensagens BPDU.
Prioridade	Ele especifica a prioridade da porta no cálculo da spanning tree. Quando o ID da ponte raiz, o custo do caminho raiz e o ID da ponte são os mesmos, a prioridade é um critério importante para determinar se a porta está selecionada como a porta raiz. Quanto menor o valor da prioridade, maior será a prioridade.
Custo do Caminho	É um valor de referência usado para selecionar os caminhos e calcular os custos do caminho na instância dentro da região do MST, também uma referência para a seleção da porta raiz. Quanto menor o valor, maior será a prioridade.

Configuração LLDP

Visão Geral

Em um ambiente de vários fornecedores, é necessário um protocolo padrão que permita que dispositivos de rede de diferentes fornecedores descubram outros dispositivos, troquem informações de sistema e configuração.

LLDP (Link Layer Discovery Protocol) fornece um método de descoberta de camada de link padrão que organiza os principais recursos, endereço de gerenciamento, identificador de dispositivo e informações de identificador de interface de dispositivos neste lado em diferentes TLVs (Tipo/Comprimento/Valor) e os encapsula em LLDPDUs (Link Layer Discovery Protocol Data Unit) para liberar aos vizinhos aos quais estão diretamente conectados. Depois de receber essas informações, os vizinhos as salvarão como o padrão MIB (Management Information Base) para permitir que o sistema de gerenciamento de rede verifique e julgue as condições de comunicação do link.

Conceitos Básicos

- **Mensagem LLDP**

  A mensagem LLDP é encapsulada com LLDPDU.

- **LLDPDU**

  LLDPDU é uma unidade de dados encapsulada na mensagem LLDP. Cada LLDPDU é uma sequência de estruturas typelength-value (TLV).

- **TLV**

  Um TLV é um elemento de informação do LLDPDU. Cada TLV carrega uma informação.

- **Endereço de gerenciamento**

  O sistema de gerenciamento de rede usa o endereço de gerenciamento para identificar e gerenciar o dispositivo para manutenção de topologia e gerenciamento de rede. O endereço de gerenciamento é encapsulado no endereço de gerenciamento TLV da mensagem LLDP.

Mecanismo de operação

LLDP é um protocolo unidirecional para notificação ou recuperação de informações. Notifica um método de operação sem necessidade de confirmação e indisponível para consulta.

Principais obras do LLDP:

- Inicializar e manter informações no MIB local.
- Obtenha as informações necessárias do MIB local e encapsuleas nos quadros LLDP. Há duas maneiras de acionar o envio de quadros LLDP: uma é acionada pela expiração do cronômetro e a outra é acionada pela mudança de status do dispositivo.
- Identifique e processe os quadros LLDPDU recebidos.
- Mantenha os MIBs LLDP dos dispositivos remotos.
- Notifique as alterações de informações MIB dos dispositivos locais ou remotos.
- **Status operacional LLDP**

Há quatro status operacionais LLDP:

- Send & Receive: Neste modo, o switch pode enviar e receber mensagens LLDP.
- Send Only: Neste modo, o switch só pode enviar mensagens LLDP.
- Receive Only: Neste modo, o switch só pode receber mensagens LLDP.
- Disabled: Neste modo, o switch não pode enviar nem receber mensagens LLDP.

Quando o status operacional do LLDP muda, sua máquina de estado do protocolo LLDP é reinicializada. Você pode configurar o Atraso de inicialização para evitar inicializações frequentes causadas por mudanças frequentes do status operacional. Se você configurou o Atraso de inicialização , o switch deve aguardar o tempo especificado para inicializar o LLDP depois que o status operacional do LLDP mudar.

- **Mecanismo de transmissão de mensagem LLDP**

  Quando o status operacional da porta é Send & Receive ou Send Only, o switch envia periodicamente mensagens LLDP para seus dispositivos vizinhos.

  Quando as informações do dispositivo local são alteradas, o switch notifica imediatamente as alterações aos dispositivos vizinhos enviando mensagens LLDP. Mas, para evitar que as mensagens LLDP sejam enviadas em massa para a rede causadas por alterações frequentes nas informações do dispositivo local, cada mensagem LLDP precisa ser atrasada por um tempo específico após o envio da última mensagem.

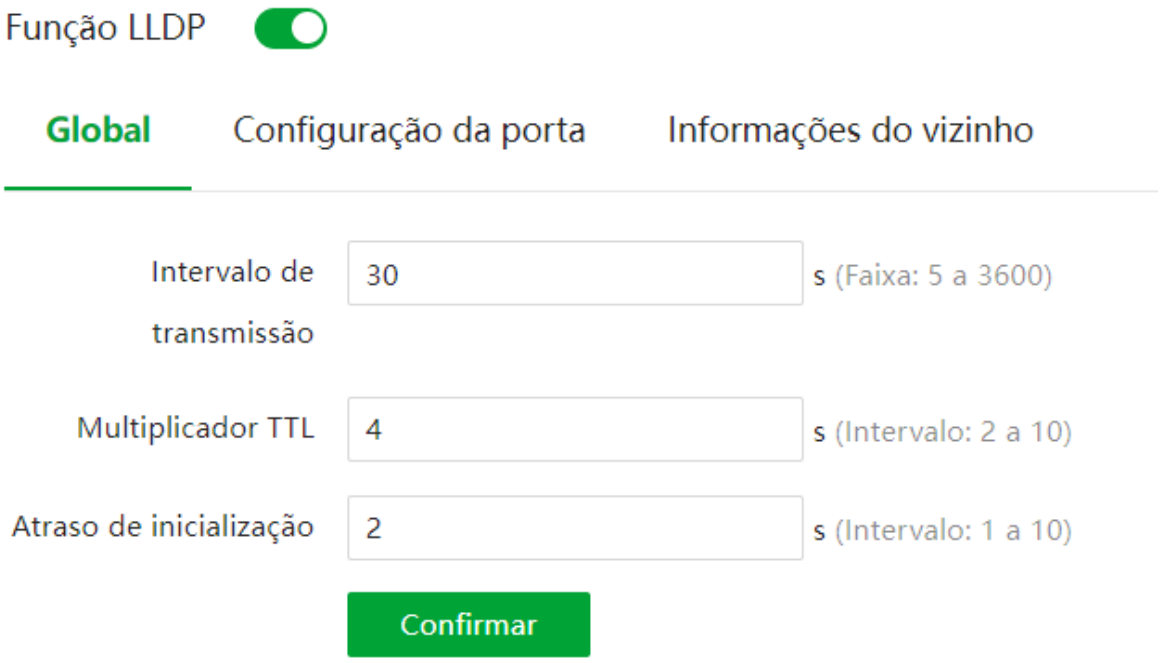
  Quando o status operacional da porta muda de Disabled ou Receive Only para Send & Receive ou Send Only , o switch envia uma mensagem LLDP para seus dispositivos vizinhos imediatamente.

- **Mecanismo de recebimento de mensagens LLDP**

Quando o status operacional da porta é Send & Receive ou Receive Only, o switch confirma a validade de cada mensagem LLDP recebida e seus TLVs. Após a verificação, ele salva as informações do dispositivo vizinho e inicia um temporizador de envelhecimento de acordo com o valor de TTL (Time to Live) no Time to Live TLV. Se o valor for zero, as informações do dispositivo vizinho expiram imediatamente.

Global

Clique em **Comutação > Configuração LLDP Global** para entrar na página. Nesta página, você pode configurar os parâmetros globais do LLDP.

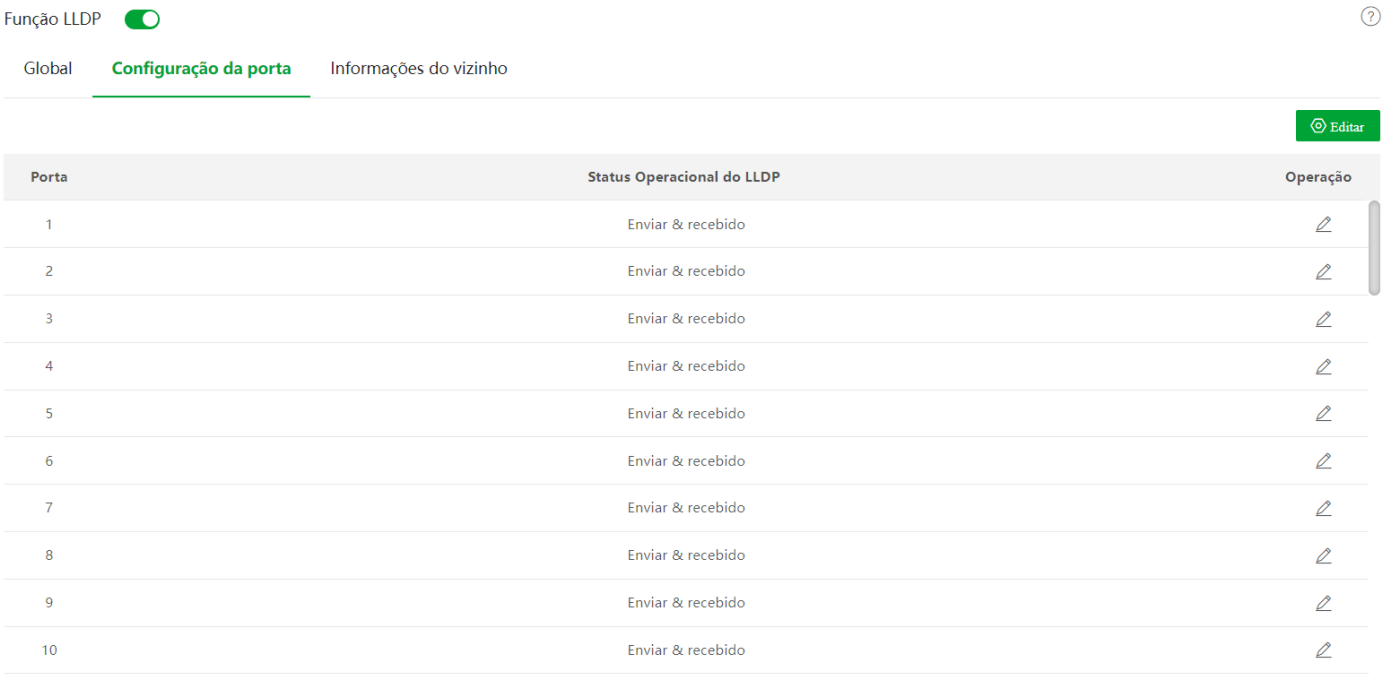


Descrição do parâmetro

Nome	Descrição
Função LLDP	É usado para habilitar ou desabilitar a função LLDP.
Intervalo de transmissão	Ele especifica o intervalo no qual o switch envia LLDPDUs aos vizinhos.
Multiplicador TTL	O Multiplicador TTL é usado para controlar o valor do campo TTL em LLDPDUs transmitidos pelo switch. O TTL é a duração em que as informações locais podem sobreviver nos dispositivos vizinhos. TTL = Min (65535, multiplicador TTL x intervalo de envio LLDPDU), indicando o valor mínimo entre 65535 e o multiplicador TTL × intervalo de envio LLDPDU.
Atraso de inicialização	Para evitar que a porta execute a inicialização continuamente como resultado de alterações frequentes do status operacional, você pode configurar um tempo de atraso de inicialização para a porta que permite que a porta execute a inicialização por um tempo específico após as alterações do status operacional.

Configuração da porta

Clique em **Comutação > Configuração de porta de configuração LLDP** para entrar na página. Nesta página, você pode configurar o status operacional LLDP para cada porta.

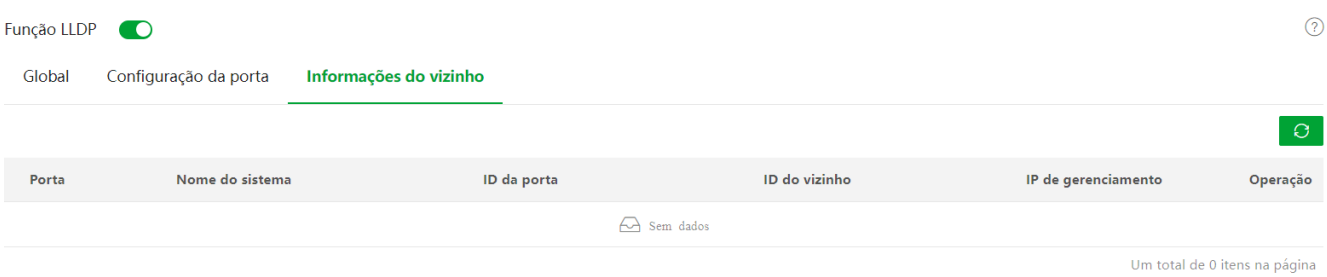


Descrição do parâmetro

Nome	Descrição
Porta	Ele especifica o ID da porta.
Operação LLDP Estado (Porta Propriedade)	Indica o status operacional LLDP de cada porta. • **Disabled** : A função LLDP desta porta está desabilitada. • **Send Only** : A porta apenas envia, mas não recebe mensagens LLDP. • **Receive Only** : A porta apenas recebe, mas não envia mensagens LLDP. • **Send & Receive** : A porta envia e recebe mensagens LLDP. • **No Change** : Mantém a configuração atual.

Informação do vizinho

Clique em **Switching > LLDP Configuration Neighbor Info** para entrar na página. Nesta página, você pode visualizar as informações do vizinho.



Descrição do parametro

Nome	Descrição
Porta	Ele especifica o ID da porta.
Nome do sistema	Ele especifica o nome do sistema do dispositivo vizinho.
Id da porta	Ele especifica as informações da porta do dispositivo vizinho. A informação da porta pode ser um número de porta, endereço MAC ou outra informação, definida pela informação transportada na mensagem LLDP do dispositivo vizinho
Identificação do vizinho	Ele especifica o endereço MAC do dispositivo vizinho.
IP de gerenciamento	Ele especifica o endereço IP de gerenciamento do dispositivo vizinho.
Tempo de sobrevivência	Ele especifica o resto do tempo que as informações do vizinho podem ser salvas e exibidas no switch.
Descrição da porta	Especifica a descrição detalhada da porta usada para transmitir mensagens LLDP no dispositivo vizinho.
Descrição do sistema	Ele especifica a descrição detalhada do dispositivo vizinho.
Desempenho	Ele especifica os recursos suportados pelo dispositivo vizinho.

LLDP-MED

Visão geral

LLDP-MED (Link Layer Discovery Protocol - Media Endpoint Discovery) é uma extensão do LLDP e é usado para anunciar informações entre dispositivos de rede e terminais de mídia. É especialmente utilizado em conjunto com o Auto VoIP (Voice over Internet Protocol) para permitir o acesso à rede e a autoconfiguração dos dispositivos VoIP. Com LLDP-MED, este switch oferece três tipos de TLVs: Capabilities, Network Policy e Location Identification, ajudando os administradores de rede a solucionar as falhas de rede ocorridas e facilitando a implantação e gerenciamento de dispositivos VoIP na Ethernet com custos mais baixos.

Com LLDP-MED, este switch oferece três tipos de TLVs: Capabilities, Network Policy e Location Identification, ajudando os administradores de rede a solucionar as falhas de rede ocorridas e facilitando a implantação e gerenciamento de dispositivos VoIP na Ethernet com custos mais baixos.

Tipo de dispositivo

O LLDP-MED define dois tipos de dispositivos: Dispositivo de conectividade de rede e Dispositivo de ponto final. Este switch é um dispositivo de conectividade de rede.

Dispositivo de conectividade de rede

Dispositivos de conectividade de rede LLDP-MED fornecem acesso à infraestrutura de LAN baseada em IEEE 802 para dispositivos de terminal LLDP-MED. Um dispositivo de conectividade de rede LLDP-MED é um dispositivo de acesso à LAN baseado em qualquer uma das seguintes tecnologias:

- Comutador/Roteador LAN
- Ponte IEEE 802.1
- Repetidor IEEE 802.3
- Ponto de acesso sem fio IEEE 802.11
- Qualquer dispositivo que suporte as extensões IEEE 802.1AB e MED e possa retransmitir quadros IEEE 802 por meio de qualquer método.

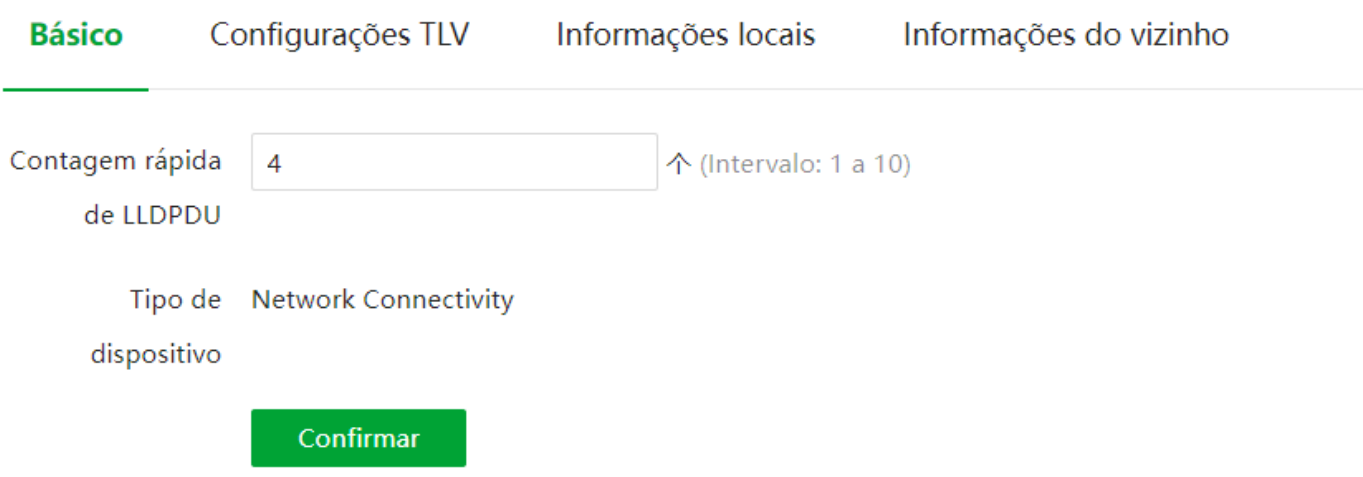
Dispositivo terminal

Os Dispositivos Endpoint LLDP-MED estão localizados na borda da rede LAN IEEE 802 e são divididos em Classe I, Classe II e Classe III.

- Endpoint genérico (Classe I)
- Endpoints participantes básicos em LLDP-MED, como controladores de comunicações IP.
- Terminal de mídia (Classe II)
- Suporta fluxos de mídia IP, como gateways de mídia, pontes de conferência e servidores de mídia.
- Terminal de comunicação (Classe III)
- Suporta usuários finais de comunicação IP, como telefones IP e softphones.

Básico

Clique em **Switching > LLDP-MED > Basic** para entrar na página. Nesta página, você pode configurar os parâmetros básicos do LLDP-MED



Descrição do parâmetro

Nome	Descrição
Contagem rápida de LLDPDU	Ele especifica o número de pacotes LLDP-MED sucessivos que o switch envia quando recebe os pacotes LLDP-MED dos endpoints vizinhos. O padrão é 4.
Tipo de dispositivo	Ele especifica o tipo de dispositivo LLDP-MED atual. O switch é um dispositivo de conectividade de rede.

Configurações TLV

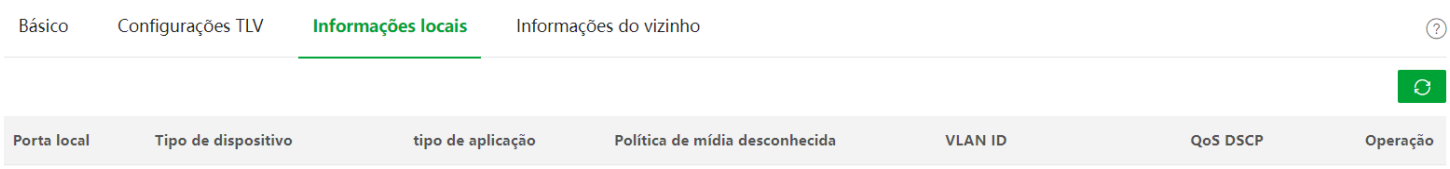
Clique em **Switching > LLDP-MED > TLV Settings** para entrar na página. Nesta página, você pode configurar os parâmetros básicos do LLDP-MED.

Descrição do parâmetro

Nome	Descrição
Porta	Ele especifica o número da porta do switch.
Campo TLV	É usado para selecionar as informações TLV incluídas no LLDPDU. • Capacidades : permite que um dispositivo de rede anuncie os TLVs LLDP-MED que ele suporta. • Política de rede : permite que o switch conectado e os dispositivos de endpoint anunciem configurações de VLAN e atributos associados de Camada 2 e Camada 3 para o aplicativo específico nessa porta. • Identificação do local : é usado para anunciar as informações do identificador de local apropriado de um dispositivo local para um dispositivo vizinho.

Informações locais

Clique em **Switching > LLDP-MED > Local Information** para entrar na página. Nesta página, você pode visualizar as configurações LLDP-MED de todas as portas.

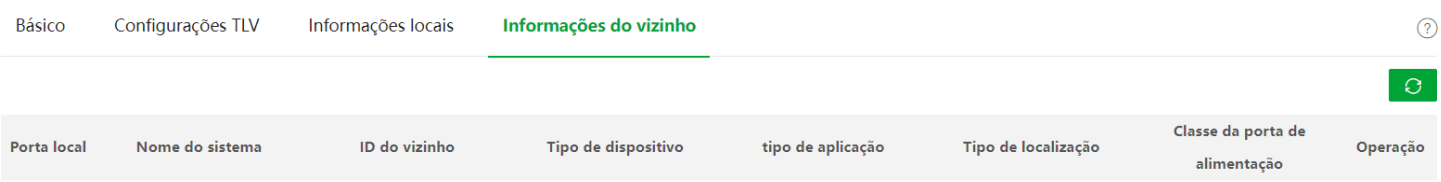


Descrição do parâmetro

Nome	Descrição
Porto Local	Ele especifica o número da porta do switch.
Tipo de dispositivo	Ele especifica os tipos de dispositivos locais definidos pelo LLDP-MED.
Tipo de aplicação	Ele especifica os tipos de aplicativos suportados pelos dispositivos locais.
Política de Mídia Desconhecida	Especifica a configuração da tag desconhecida incluída na política de rede.
ID da VLAN	Ele especifica o ID de VLAN 802.1Q da porta.
QoS DSCP	Ele especifica o valor DSCP de determinado aplicativo.

Informação do vizinho

Clique em **Switching > LLDP-MED > Neighbor Info** para entrar na página. Nesta página, você pode visualizar as informações LLDP-MED dos dispositivos vizinhos em todas as portas.



Descrição do parâmetro

Nome	Descrição
Porto Local	Ele especifica o número da porta deste switch.
Nome do sistema	Ele especifica o nome do sistema do dispositivo vizinho.

Nome	Descrição
Identificação do vizinho	Ele especifica o endereço MAC do dispositivo vizinho.
IP de gerenciamento	Ele especifica o endereço IP de gerenciamento do dispositivo vizinho.
Tempo de sobrevivência	Ele especifica o resto do tempo que as informações do vizinho podem ser salvas e exibidas no switch.
Descrição da porta	Especifica a descrição detalhada da porta usada para transmitir mensagens LLDP no dispositivo vizinho.
Descrição do sistema	Ele especifica a descrição detalhada do dispositivo vizinho.
Desempenho	Ele especifica os recursos suportados pelo dispositivo vizinho.

IGMP Snooping

Visão geral

O IGMP Snooping (internet group management protocol snooping) é um mecanismo de restrição multicast executado nos switches Ethernet da camada 2, que é usado para gerenciar e controlar grupos multicast.

Conforme mostrado na figura abaixo, os dados multicast são transmitidos do dispositivo de camada 2 desativado para IGMP-Snooping; Mas com o IGMP Snooping ativado, o dispositivo de camada 2 estabelecerá uma tabela de mapeamento para portas e endereços MAC multicast analisando as mensagens IGMP recebidas e encaminhando os dados multicast para os receptores específicos.

O IGMP snooping apenas encaminha os dados para os receptores específicos por meio do multicast da camada 2, fornecendo as seguintes vantagens:

- Reduza a transmissão na rede da camada 2 e economize largura de banda da rede.
- Aumente a segurança dos dados multicast.
- Forneça conveniência para o gerenciamento de cobrança para cada host.
- Conforme mostrado na figura a seguir, o roteador A está conectado à fonte multicast, o rastreamento IGMP do switch A e do switch B está ativado, enquanto o host A e o host C são os receptores dos dados multicast.

- Porta do roteador

  De camada 2 habilitado para espionagem IGMP , as portas para dispositivos multicast de camada 3 upstream são chamadas de portas de roteador (portas A1 e B1 na figura acima).

- Porta do host

De camada 2 habilitado para IGMP snooping , as portas para hosts receptores downstream são chamadas de portas de host (Portas A2, A4 e B2 na figura acima).

- Consulta geral

  O consultador IGMP (roteador A na figura acima) envia periodicamente consultas gerais IGMP a todos os hosts e dispositivos no segmento de rede local para verificar os membros do grupo multicast.

  Após receber uma consulta geral IGMP, o dispositivo da camada 2 (switches A e B na figura acima) encaminha a consulta e realiza o seguinte tratamento para as portas de recebimento:

  Se a porta de recebimento estiver incluída na tabela de mapeamento, o dispositivo da camada 2 reinicia o cronômetro de vencimento da porta.

  Se a porta de recebimento for excluída na tabela de mapeamento, o dispositivo da camada 2 adicionará a porta à tabela de mapeamento e iniciará um cronômetro de vencimento para a porta.

- Consulta específica

  Quando um host com IGMPv2 ou IGMPv3 ativado deixa o grupo multicast, ele envia mensagens IGMP para deixar o grupo. Quando as portas dos dispositivos da camada 2 (switches A e B na figura acima) receberem a mensagem IGMP leave group, as seguintes ações serão executadas de acordo com a tabela de mapeamento:

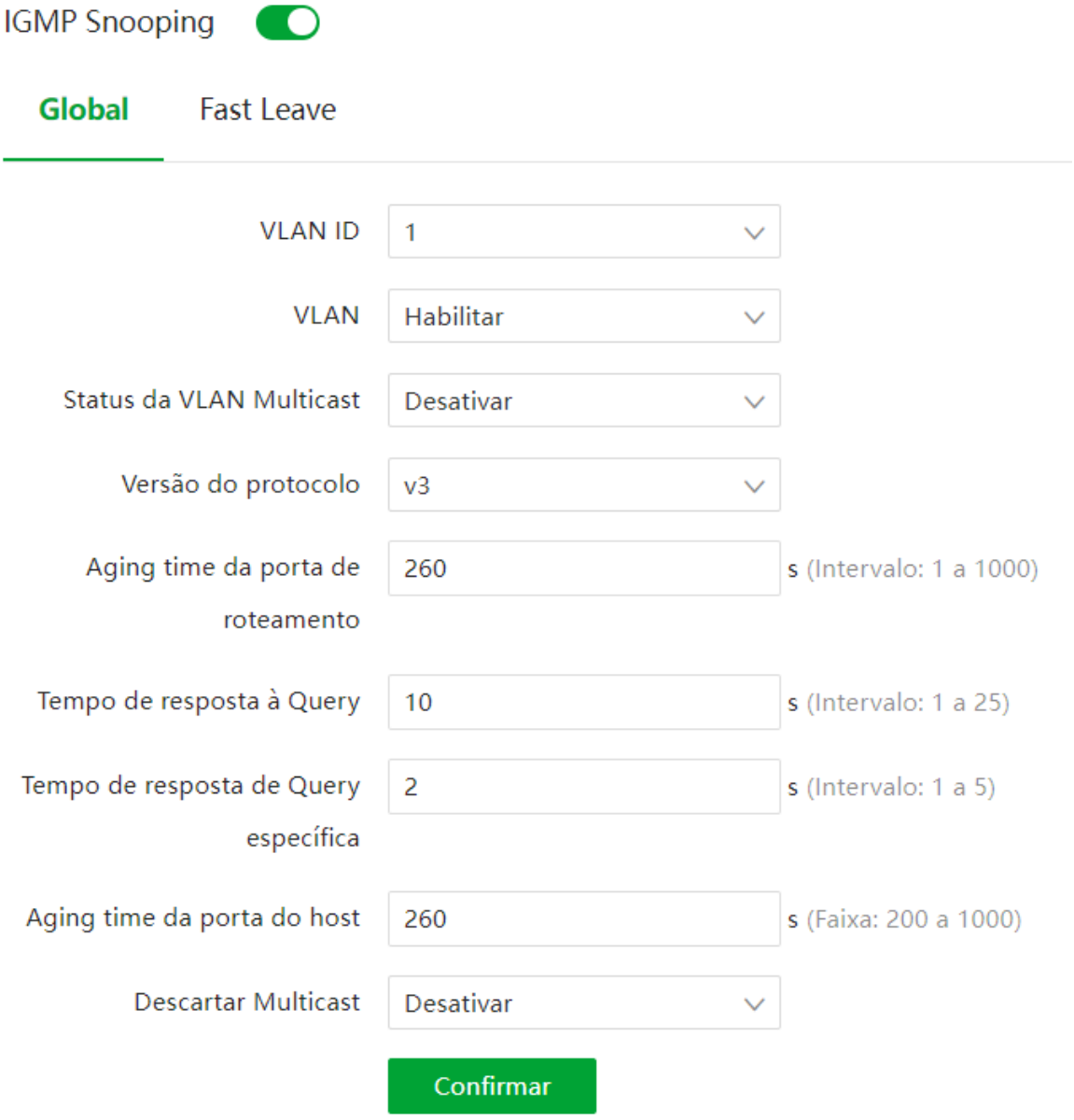
  Se nenhuma entrada de encaminhamento do grupo multicast for encontrada ou a entrada de encaminhamento correspondente não contiver a porta de recebimento, o dispositivo da camada 2 descartará a mensagem do grupo de saída IGMP diretamente, em vez de encaminhá-la para outras portas.

  Se a entrada de encaminhamento do grupo multicast for encontrada e a entrada de encaminhamento correspondente contiver outras portas de host, o dispositivo da camada 2 descartará a mensagem do grupo de saída IGMP diretamente, em vez de encaminhá-la para outras portas, e enviará uma mensagem de consulta específica do IGMP para o host que está saindo .

  Se a entrada de encaminhamento do grupo multicast for encontrada e a entrada de encaminhamento correspondente não contiver outras portas de host, o dispositivo da camada 2 encaminhará a mensagem pela porta do roteador e também enviará uma mensagem de consulta específica IGMP ao host.

Global

Clique em **Switching > IGMP Snooping > Global** para entrar na página. Nesta página, você pode configurar os parâmetros globais de espionagem IGMP.



Descrição do parâmetro

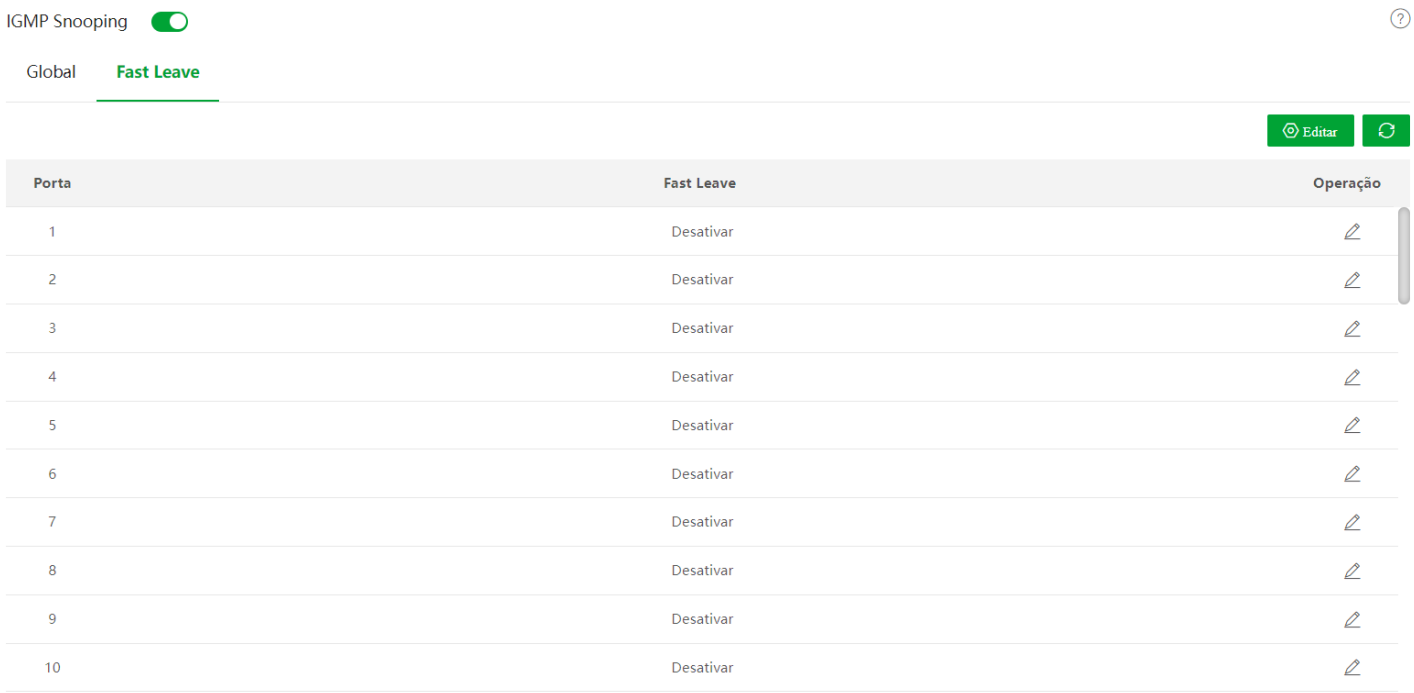
Nome	Descrição
Espionagem IGMP	É usado para habilitar ou desabilitar a função de espionagem IGMP.
ID da VLAN	Ele especifica a VLAN cuja função IGMP Snooping está habilitada.
VLAN	É usado para habilitar ou desabilitar a função IGMP Snooping da VLAN.

Nome	Descrição
Status da VLAN Multicast	É usado para habilitar ou desabilitar a função multicast VLAN da VLAN acima. Por padrão, a função VLAN multicast do switch está desativada. Se dispositivos de diferentes VLANs dentro de uma LAN solicitarem mensagens multicast da mesma fonte multicast, o dispositivo multicast deverá copiar os dados multicast para cada VLAN. Com esta função habilitada, o dispositivo multicast só precisa enviar dados multicast para este switch, e este switch os enviará para os receptores de dados multicast, economizando largura de banda e reduzindo a carga do dispositivo multicast.
Versão do Protocolo	Versões de mensagens IGMP suportadas: • v1 : Processa apenas mensagens de IGMPv1. • v2 : processa apenas mensagens de IGMPv1 e IGMPv2. • v3 : processa mensagens de IGMPv1, IGMPv2 e IGMPv3.
Tempo de Envelhecimento da Porta de Roteamento	Ele especifica o tempo do temporizador de envelhecimento da porta de roteamento. Durante esse período, se a porta de roteamento não receber a mensagem de consulta geral IGMP, o switch excluirá a porta da tabela de mapeamento.
Tempo de resposta da consulta geral	Especifica o tempo máximo de resposta à consulta geral. Após o switch encaminhar a mensagem de consulta geral, e durante esse período, se a porta não receber a mensagem de associação IGMP que responde à consulta geral, a porta será excluída da tabela de mapeamento.
Tempo de resposta de consulta específico	Ele especifica o tempo máximo de resposta para a consulta específica. Após o switch encaminhar a mensagem de consulta específica do IGMP para as portas do host e, durante o período de tempo, se a porta do host não receber a mensagem de associação IGMP que responde à consulta específica do host, o switch exclui a porta na tabela de mapeamento .

Nome	Descrição
Tempo de Envelhecimento da Porta do Host	Ele especifica o tempo do temporizador de envelhecimento da porta do host. Quando a porta do host não recebe a mensagem de associação IGMP durante esse período, o switch exclui a porta da tabela de mapeamento.
Descarte Multicast	Com a função Multicast Discard habilitada, o switch encaminha a mensagem de dados multicast desconhecida apenas para sua porta do roteador e não transmite em VLAN. Se o switch não tiver nenhuma porta de roteador, os dados multicast desconhecidos serão descartados e não encaminhados.

Saída rápida

Clique em **Switching > IGMP Snooping > Fast Leave** para entrar na página. Nesta página, você pode configurar o modo de saída rápida para cada porta.



Descrição do parâmetro

Nome	Descrição
Porta	Ele especifica o ID da porta.
Saída rápida	Com a função habilitada, ao receber as mensagens IGMP leave group desta porta, o switch remove a porta da lista de encaminhamento multicast de snooping IGMP correspondente e não espera até que o tempo de envelhecimento da porta do host expire.

Configurações MAC

Tabela de endereços MAC

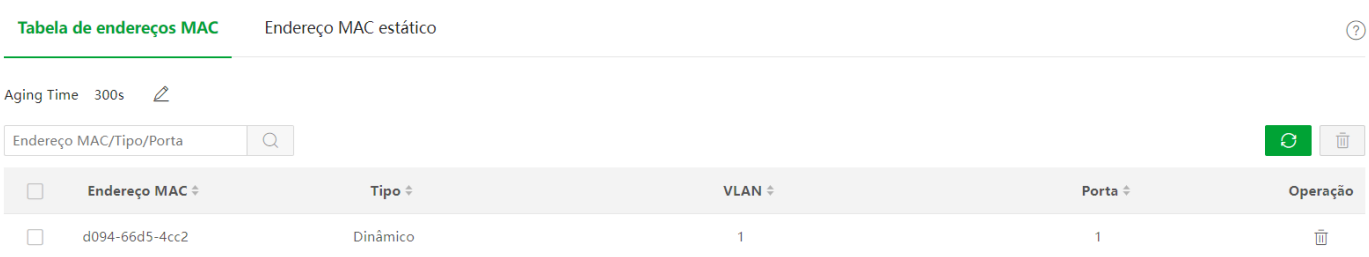
O switch cria a tabela de encaminhamento de endereço MAC pelo mecanismo de aprendizado de endereço. A tabela inclui informações como endereço MAC, ID de VLAN e número da porta. Ao encaminhar uma mensagem, o switch adota um dos dois modos de encaminhamento a seguir com base nas informações da tabela de endereços MAC:

Modo Unicast: Se uma entrada na tabela de encaminhamento de endereços MAC estiver disponível para o endereço MAC de destino, o switch encaminhará a mensagem para a porta indicada pela entrada na tabela de endereços MAC.

Nome	Descrição
Tempo de envelhecimento	Ele especifica o tempo de vencimento das entradas na tabela de endereços MAC, que é efetivo apenas para entradas dinâmicas. Quando o switch não receber mensagens cujo endereço de origem seja consistente com o endereço MAC de origem na tabela dentro do tempo de vencimento, a entrada da tabela de endereços MAC será excluída automaticamente.
Endereço MAC	Endereço MAC, formato: XXXX-XXXX-XXXX.

Modo de transmissão: Se o switch receber uma mensagem com o endereço MAC de destino cujo bit mais baixo do segundo byte é 1, ou se nenhuma entrada na tabela de encaminhamento de endereço MAC estiver disponível para o endereço MAC de destino, o switch encaminhará a mensagem para todas as portas, exceto a porta receptora no modo broadcast. As mensagens de transmissão, mensagens multicast e mensagens unicast desconhecidas serão encaminhadas no modo broadcast.

Clique em **Switching > MAC Settings > MAC Address Table** para entrar na página. Nesta página, você pode visualizar e excluir as entradas da tabela de endereços MAC.

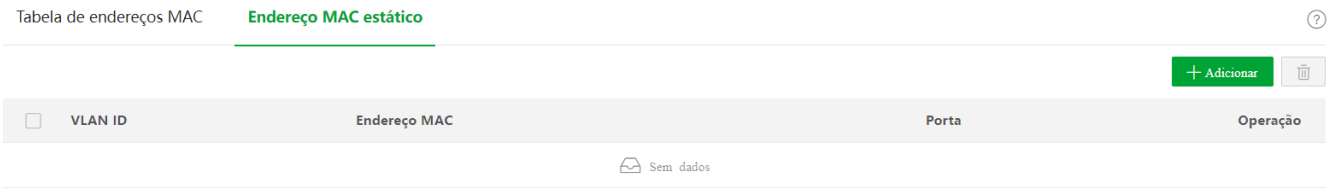


Descrição do parâmetro

Nome	Descrição
Tipo	Ele especifica o tipo do endereço MAC. • Static : Especifica a entrada do endereço MAC configurado manualmente pelo administrador. • Dinâmico : especifica a entrada do endereço MAC gerado automaticamente pelo switch.
VLAN	Ele especifica a VLAN à qual o endereço MAC pertence.
Porta	Ele especifica a porta física do switch à qual o dispositivo com o endereço MAC se conecta.

Endereço MAC estático

Clique em **Switching > MAC Settings > Static MAC Address** para entrar na página. Nesta página, você pode configurar a tabela de endereços MAC estáticos. A configuração existe como entradas estáticas na tabela de endereços MAC, além do controle do tempo de vencimento do MAC.



Descrição do parâmetro

Nome	Descrição
ID da VLAN	Ele especifica a VLAN à qual o endereço MAC pertence.
Endereço MAC	Endereço MAC, formato: XXXX-XXXX-XXXX.
Porta	Ele especifica a porta física do switch à qual o dispositivo com o endereço MAC se conecta.

Política de QoS

Visão geral

Na rede IP tradicional, os pacotes são tratados igualmente. Essa política de serviço de rede é conhecida como Best-effort, que entrega os pacotes aos seus destinos com o melhor esforço, sem nenhuma segurança e garantia de atraso na entrega, confiabilidade e assim por diante. Atualmente, além das aplicações tradicionais como www, FTP e E-mail, surgem novos serviços, como videoconferência, educação remota, Video-on-Demand (VoD) e videotelefone, que necessitam de maiores requisitos de largura de banda, atraso e nervosismo. A política de QoS (Quality of Service) pode atender às demandas acima e melhorar a qualidade do serviço na rede.

Este switch classifica as mensagens de acordo com a prioridade no estágio de entrada, em seguida, mapeia-as para diferentes filas no estágio de saída e, finalmente, encaminha essas mensagens por filas de acordo com o modo de agendamento, de modo a garantir a qualidade do serviço da rede.

Modo de agendamento

O escalonamento de filas é usado para resolver o problema de preempção de recursos por múltiplas mensagens quando a rede está congestionada. Este switch suporta três modos de agendamento: prioridade estrita, prioridade ponderada simples e prioridade ponderada. Cada modo de agendamento possui oito filas com diferentes prioridades de encaminhamento de dados.

Algoritmo de agendamento de prioridade estrito é especialmente projetado para aplicativos de serviço crítico. Uma característica importante dos serviços críticos é que eles exigem atendimento preferencial em congestionamentos para reduzir o atraso de resposta.

No escalonamento de filas, as mensagens são enviadas em filas seguindo rigorosamente a ordem de prioridade de alta para baixa (Fila 8 > Fila 7 > … > Fila 1). Quando a fila com prioridade mais alta estiver vazia, as mensagens na fila com prioridade mais baixa serão enviadas. Você pode colocar mensagens de serviço críticas nas filas com prioridade mais alta e colocar mensagens de serviço não críticas (como e-mail) nas filas com prioridade mais baixa. Desta forma, as mensagens de serviço crítico são enviadas preferencialmente, e as mensagens de serviço não crítico são enviadas quando as mensagens de serviço crítico não são enviadas.

Desvantagem da Prioridade Estrita: Se houver mensagens nas filas de maior prioridade por muito tempo durante o congestionamento, as mensagens nas filas de menor prioridade ficarão presas porque não foram atendidas.

Prioridade Ponderada Simples

Nesse modo, não há prioridade e todas as filas compartilham igualmente a largura de banda.

Prioridade Ponderada

Esse algoritmo de agendamento agenda todas as filas sucessivamente para garantir que cada fila possa receber um determinado tempo de serviço. O valor ponderado representa a proporção do recurso atribuído. Suponha que haja oito filas de saída para uma porta e cada fila seja atribuída a um valor ponderado. Por exemplo, você pode configurar os oito valores ponderados de uma porta de 100 Mbps para 25, 20, 15, 15, 10, 5, 5 e 5, respectivamente. Desta forma, a fila com a prioridade mais baixa pode ter certeza de pelo menos 5 Mbps de largura de banda, evitando assim a desvantagem do algoritmo de escalonamento de filas de Prioridade Simples de que mensagens em filas de baixa prioridade possivelmente não serão servidas por muito tempo. Outra vantagem do algoritmo de escalonamento de filas de Prioridade Ponderada é que, embora as filas sejam escalonadas sucessivamente, o tempo de serviço para cada fila não é fixo, o que significa que se uma fila estiver vazia, a próxima fila será escalonada imediatamente. Desta forma, os recursos de largura de banda podem ser totalmente utilizados.

Prioridade

Este switch suporta três modos de prioridade: 802.1P Priority , DSCP Priority e Port Priority .

Prioridade 802.1P

A prioridade 802.1P está nos cabeçalhos do pacote da Camada 2 e é aplicável a ocasiões em que o cabeçalho do pacote da Camada 3 não precisa de análise, mas a QoS deve ser assegurada na Camada 2. A prioridade 802.1P está disponível apenas em um pacote marcado com 802.1Q.

Por padrão, a prioridade 802.1P, as filas e as palavras-chave desse switch são mapeadas da seguinte maneira.

Prioridade 802.1P	**Fila**	**Palavra chave**
0	1	melhor esforço
1	2	fundo
2	3	poupar
3	4	esforço excelente
4	5	carga controlada
5	6	vídeo
6	7	voz
7	8	Gerenciamento de rede

Prioridade DSCP

RFC2474 redefine o campo ToS (tipo de serviço) no cabeçalho da mensagem IP, que é chamado de campo

Campo DS (Serviços Diferenciados). Os primeiros seis bits (bits 0 a 5) do campo DS indicam a prioridade DSCP (Differentiated Services Code Point) variando de 0 a 63. Os últimos 2 bits (bits 6 e 7) são reservados.

A relação correspondente entre a prioridade DSCP e as palavras-chave são as seguintes.

Prioridade DSCP (Decimal)	**Prioridade DSCP (binário)**	**Palavra chave**
46	101110	ef
10	001010	af11
12	001100	af12
14	001110	af13
Prioridade DSCP (Decimal)	Prioridade DSCP (binário)	Palavra chave
18	010010	af21
20	010100	af22
22	010110	af23
26	011010	af31
28	011100	af32
30	011110	af33
34	100010	af41
36	100100	af42
38	100110	af43
8	001000	cs1
16	010000	cs2
24	011000	cs3
32	100000	cs4
40	101000	cs5

48	110000	cs6
56	111000	cs7
0	000000	ser (padrão)

Por padrão, a prioridade DSCP e as filas desse switch são mapeadas da seguinte maneira.

Prioridade DSCP	**Fila**
0 - 7	1
8 - 15	2
16 - 23	3
24 - 31	4
32 - 39	5
40 - 47	6
48 - 55	7
56 - 63	8

Prioridade de porta

Você pode configurar manualmente a prioridade CoS (Class of Service) das portas físicas para mapear as portas físicas com filas. A porta mapeia mensagens para as filas correspondentes de acordo com o relacionamento de mapeamento configurado quando ocorrem as duas situações a seguir:

- As mensagens recebidas pela porta não carregam as tags de prioridade confiáveis pela porta. Exemplo: Para uma porta com modo de prioridade 802.1P habilitado, as mensagens recebidas não carregam o tag 802.1Q.
- A porta não confia no modo de prioridade 802.1P e no modo de prioridade DSCP.

A prioridade CoS das portas e filas é mapeada da seguinte maneira.

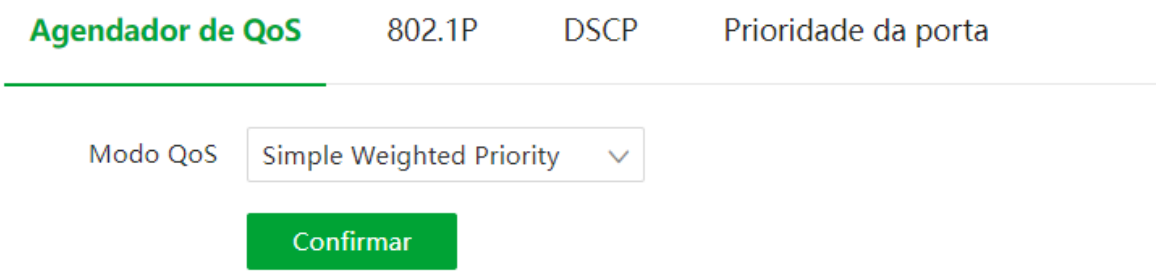
Prioridade CoS	**Fila**
0	1
1	2
2	3
3	4
4	5
5	6
6	7
7	8

Orientação de configuração

Com base na prioridade 802.P

Etapa Tarefa	Descrição
Agendador de QoS	Obrigatório. Selecione o modo de agendamento do switch com base nas demandas reais.
802.1P	Obrigatório. Configure a relação de mapeamento entre a prioridade 802.1P e as filas.
Prioridade de porta	Obrigatório. Defina o modo de prioridade das portas correspondentes para 802.1P Trust e configure a prioridade CoS para todas as portas.
Etapa Tarefa	Descrição
Agendador de QoS	Obrigatório. Selecione o modo de agendamento do switch com base nas demandas reais.
DSCP	Obrigatório. Configure a relação de mapeamento entre a prioridade DSCP e as filas.
Prioridade de porta	Obrigatório. Defina o modo de prioridade das portas correspondentes para DSCP Trust e configure a prioridade CoS para todas as portas.

Clique em **Política de QoS > Agendador de QoS** para entrar na página. Nesta página, você pode configurar o modo de agendamento de QoS e as políticas de controle de congestionamento.



Descrição do parâmetro

Nome	Descrição
Modo QoS	Ele especifica o modo do planejador para o tráfego da porta. • Strict Priority : O switch encaminha as mensagens estritamente com base na prioridade da mensagem de alta para baixa. As mensagens da fila com prioridade mais baixa são encaminhadas apenas quando a fila com prioridade mais alta está vazia. • Prioridade ponderada simples : 8 filas compartilham igualmente a largura de banda. • Prioridade ponderada : você precisa configurar um valor ponderado para cada fila. O valor ponderado indica o peso da obtenção de recursos. Se ocorrer congestionamento na porta, as larguras de banda são atribuídas com base no peso de cada fila.

Configurações da fila	Se o Modo QoS estiver definido como Prioridade ponderada , você precisará configurar o valor ponderado para cada fila.

Quando esta função está habilitada, o switch desativa a função de controle de fluxo para atender aos requisitos de clonagem de rede em vários ambientes.

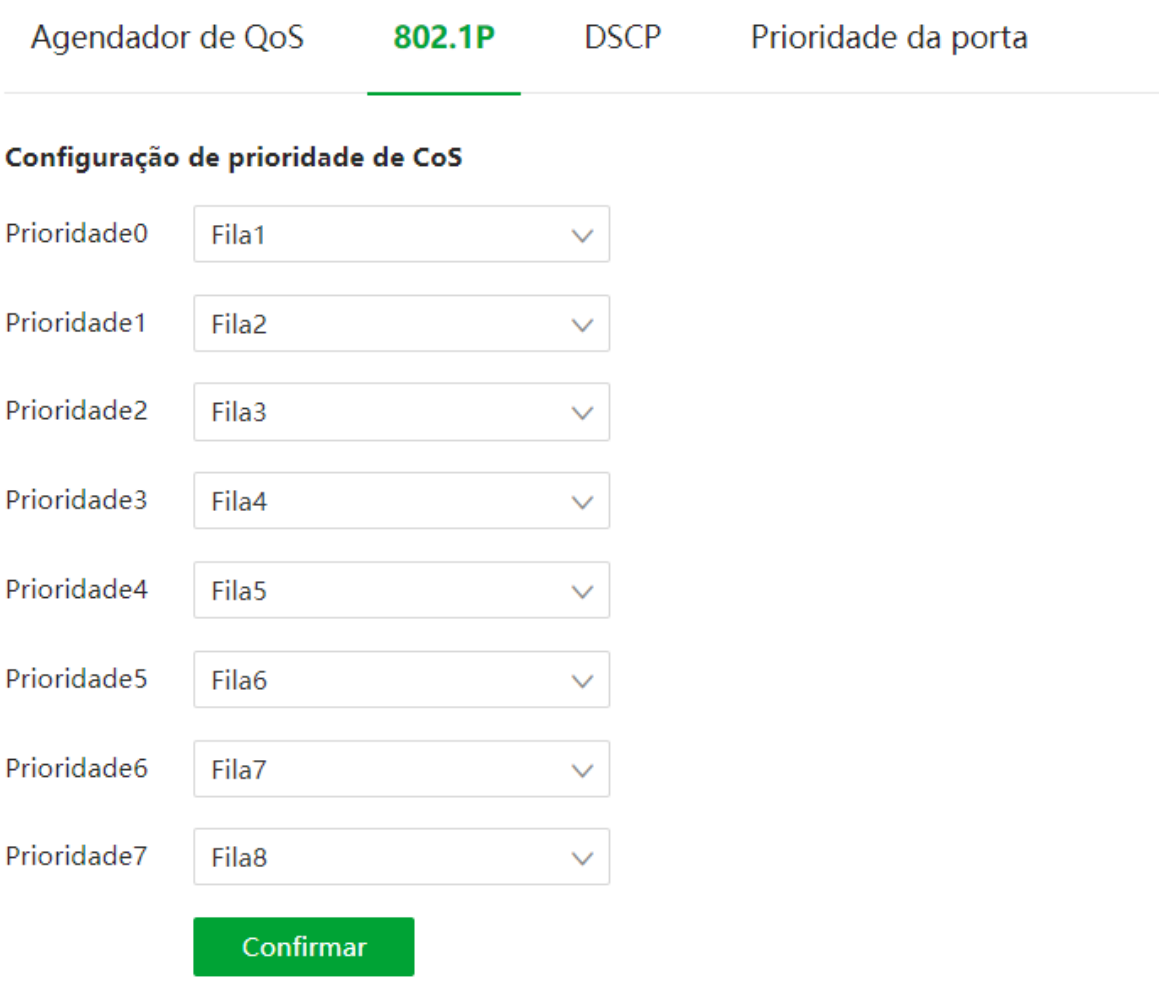
Descarte de Saída

Dica

Esta função se aplica ao cenário de clonagem de rede e não é recomendada em cenários comuns.

802.1P

Clique em **QoS Policy > 802.1P** para entrar na página. Nesta página, você pode configurar o relacionamento de mapeamento entre a prioridade 802.1P e as filas.



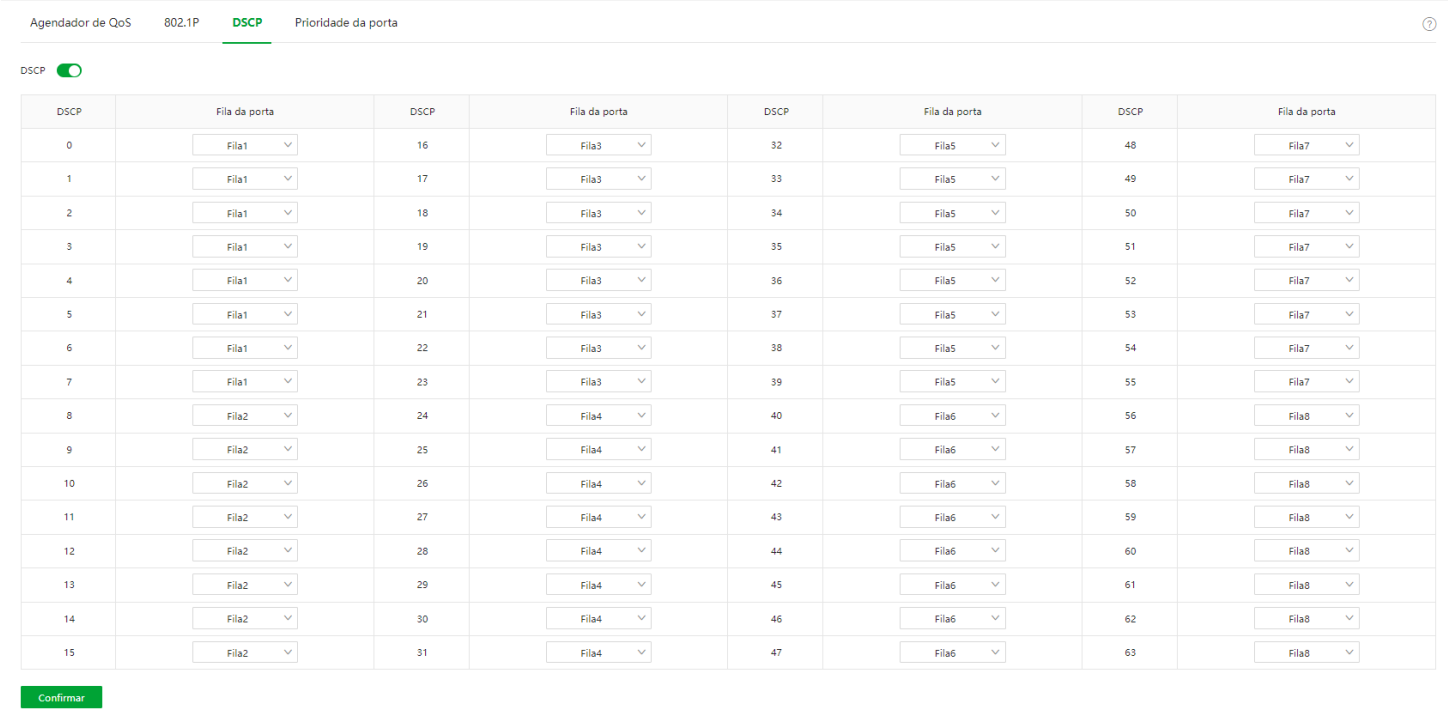
Descrição do parâmetro

Nome	Descrição
Prioridade0	Especifica a fila na qual a prioridade das mensagens é 0.
Prioridade1	Especifica a fila na qual a prioridade das mensagens é 1.
Prioridade2	Especifica a fila na qual a prioridade das mensagens é 2.
Prioridade3	Especifica a fila na qual a prioridade das mensagens é 3.

Prioridade4	Especifica a fila na qual a prioridade das mensagens é 4.
Prioridade5	Especifica a fila na qual a prioridade das mensagens é 5.
Prioridade6	Especifica a fila na qual a prioridade das mensagens é 6.
Prioridade7	Especifica a fila na qual a prioridade das mensagens é 7.

DSCP

Clique em **Política de QoS > DSCP** para entrar na página. Nesta página, você pode configurar o relacionamento de mapeamento entre a prioridade DSCP e as filas.



DSCP	Fila da porta	DSCP	Fila da porta	DSCP	Fila da porta	DSCP	Fila da porta
0	Fila1	16	Fila3	32	Fila5	48	Fila7
1	Fila1	17	Fila3	33	Fila5	49	Fila7
2	Fila1	18	Fila3	34	Fila5	50	Fila7
3	Fila1	19	Fila3	35	Fila5	51	Fila7
4	Fila1	20	Fila3	36	Fila5	52	Fila7
5	Fila1	21	Fila3	37	Fila5	53	Fila7
6	Fila1	22	Fila3	38	Fila5	54	Fila7
7	Fila1	23	Fila3	39	Fila5	55	Fila7
8	Fila2	24	Fila4	40	Fila6	56	Fila8
9	Fila2	25	Fila4	41	Fila6	57	Fila8
10	Fila2	26	Fila4	42	Fila6	58	Fila8
11	Fila2	27	Fila4	43	Fila6	59	Fila8
12	Fila2	28	Fila4	44	Fila6	60	Fila8
13	Fila2	29	Fila4	45	Fila6	61	Fila8
14	Fila2	30	Fila4	46	Fila6	62	Fila8
15	Fila2	31	Fila4	47	Fila6	63	Fila8

Descrição do parâmetro

Nome	**Descrição**
DSCP	Especifica o nível de prioridade (intervalo: 0 a 63) definido pelo campo DS do pacote IP.
Porta Fila	Ele especifica a fila do agendador da prioridade DSCP correspondente.

Prioridade de porta

Clique em **Política de QoS > Prioridade de porta** para entrar na página. Nesta página, você pode configurar o modo de confiança e a prioridade CoS para as portas físicas do switch.

Descrição do parâmetro

Nome	Descrição
Porta	Ele especifica o ID da porta.
Prioridade CoS	Especifica a prioridade CoS das portas físicas. Quando o switch recebe mensagens que não estão de acordo com as regras do modo confiável ou a porta está no modo não confiável, as mensagens entram nas filas com base na prioridade do CoS.
Modo de confiança	Especifica o método que a porta usa para processar as mensagens recebidas. − Non-Trust : Todas as mensagens recebidas pela porta entram nas filas de acordo com a correspondência da prioridade CoS configurada. − Confiança 802.1P : Quando a porta recebe mensagens VLAN, as mensagens entram nas filas de acordo com a correspondência do 802.1P . Quando a porta recebe outras mensagens, as mensagens voltam a entrar nas filas de acordo com a correspondência da prioridade do CoS. − DSCP Trust : Quando a porta recebe mensagens IP, as mensagens entram em filas de acordo com a correspondência do DSCP . Quando a porta recebe outras mensagens, as mensagens voltam a entrar nas filas de acordo com a correspondência da prioridade do CoS.

Segurança de rede

ACL

Visão geral

ACL (Access Control List) é usado para filtrar mensagens configurando regras e operações correspondentes. Após a mensagem ser recebida pela porta do switch, ela é analisada de acordo com as regras ACL desta porta. E essas regras decidem quais pacotes podem passar e quais devem ser rejeitados, o que pode efetivamente impedir que

usuários ilegais acessem a rede e melhorar a segurança da rede. Este switch suporta ACL com base em duas regras correspondentes: endereço MAC e endereço IP. − MAC ACL: Combine as regras de filtragem de acordo com o endereço MAC de origem e o endereço MAC de destino do quadro de dados da camada 2. − IP ACL: Combine as regras de filtragem com base no endereço IP de origem e no endereço IP de destino do cabeçote IP do pacote da camada 3. Um ID de ACL pode ser configurado com várias regras de correspondência de ACL e a mensagem corresponde à regra de acordo com a prioridade da regra. Depois que uma mensagem corresponde a uma regra com prioridade mais alta, ela deixa de corresponder a outras regras.

Orientação de configuração

Flite com base no endereço M AC

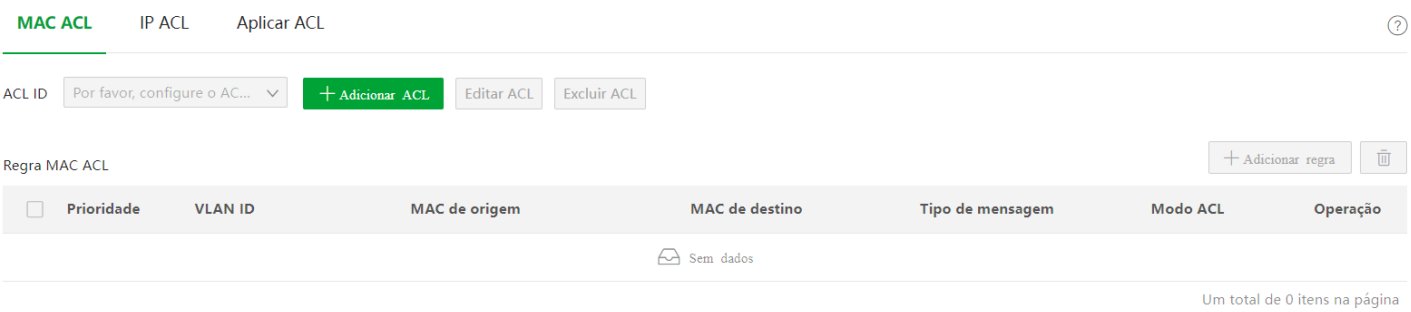
Etapa	Tarefa	Descrição
1	MAC ACL	Obrigatório. Você pode configurar a regra de filtragem que corresponde aos endereços MAC de origem e destino do quadro de dados da camada 2 . Várias regras MAC ACL podem ser configuradas com um ID ACL.
2	Aplicar ACL	Obrigatório. A regra MAC ACL entra em vigor quando é aplicada à porta correspondente do switch.

Flite com base no endereço IP

Etapa	Tarefa	Descrição
1	IP ACL	Obrigatório. Você pode configurar a regra de filtragem que corresponde aos endereços IP de origem e destino do pacote de dados da camada 3. Várias regras IP ACL podem ser configuradas com um ID ACL.
2	Aplicar ACL	Obrigatório. A regra IP ACL entra em vigor quando é aplicada à porta correspondente do switch.

MAC ACL

Clique em Segurança de rede > ACL > MAC ACL para entrar na página. Nesta página, você pode visualizar e configurar as regras MAC ACL.



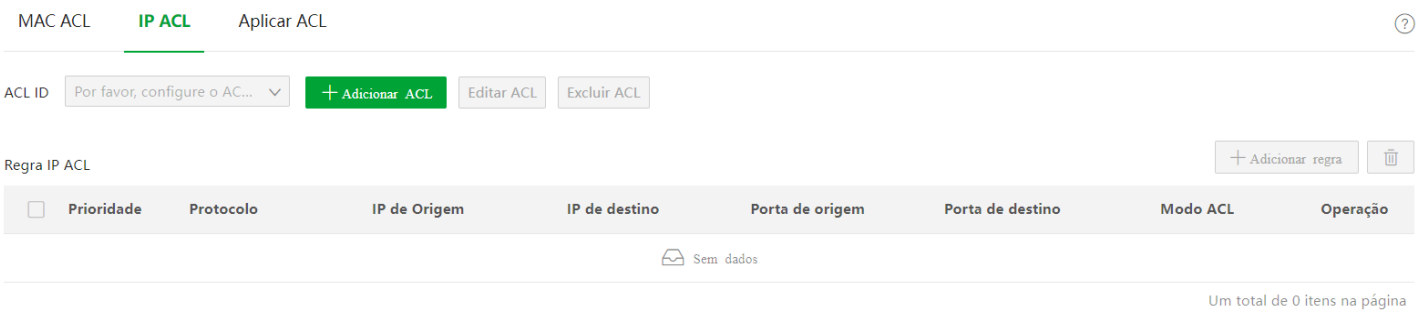
Descrição do parâmetro

Nome	Descrição
ID ACL	Ele especifica o ID ACL da regra MAC ACL. Você deve adicionar o ID ACL aqui antes de configurar as regras MAC ACL.
Prioridade	Este campo especifica a prioridade de uma regra. Um valor menor indica uma prioridade mais alta. A mensagem começa a corresponder à regra com a prioridade mais alta. Uma vez correspondido, a mensagem para de verificar as regras.
ID da VLAN	Especifica a VLAN à qual a mensagem pertence. Se este campo não estiver configurado, indica mensagens de todas as VLANs.
MAC de origem	Ele especifica o endereço MAC de origem da mensagem. • Qualquer MAC : Especifica todos os endereços MAC./li> • MAC especificado : Combinado com a máscara, é usado para especificar um determinado endereço MAC ou segmento de endereço MAC.
MAC de destino	Ele especifica o endereço MAC de destino da mensagem. • Qualquer MAC : Especifica todos os endereços MAC. • MAC especificado : Combinado com a máscara, é usado para especificar um determinado endereço MAC ou segmento de endereço MAC.

Nome	Descrição
Tipo de mensagem	Ele especifica o tipo de mensagem do quadro de dados da camada 2. Se este campo não estiver configurado, indica qualquer tipo de mensagem.
Modo ACL	Ele especifica o modo ACL no qual o switch processa as mensagens que correspondem à regra. • Permitir : Encaminhar as mensagens que correspondem à regra. • Proibir: Descarte as mensagens que correspondem à regra.

IP ACL

Clique em **Segurança de rede > ACL > IP ACL** para entrar na página. Nesta página, você pode visualizar e configurar as regras IP ACL.



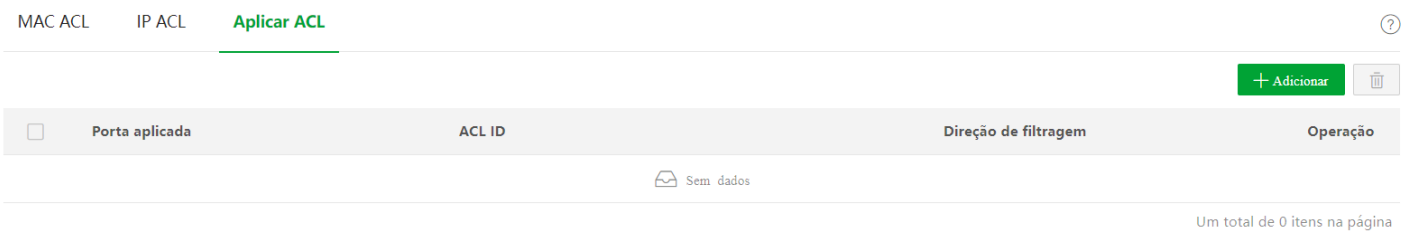
Descrição do parâmetro

Nome	Descrição
ID ACL	Ele especifica o ID ACL da regra IP ACL. Você deve adicionar o ID ACL aqui antes de configurar as regras IP ACL.
Prioridade	Especifica a prioridade da regra. Um valor menor indica uma prioridade mais alta. A mensagem começa a corresponder à regra com a prioridade mais alta. Uma vez correspondido, a mensagem para de verificar as regras.
Protocolo	Ele especifica o tipo de protocolo da mensagem, como IP, ICMP e assim por diante. Você também pode inserir o número do protocolo manualmente.
IP fonte	Ele especifica o endereço IP de origem da mensagem. • Qualquer IP : Indica todos os endereços IP. • IP especificado : Combinado com a máscara, indica um determinado endereço de rede.
IP de destino	Ele especifica o endereço IP de destino da mensagem. • Qualquer IP : Indica todos os endereços IP. • IP especificado : Combinado com a máscara, indica um determinado endereço de rede.
Porta de origem	Quando o tipo de protocolo for TCP ou UDP, digite o número da porta de origem da mensagem.
Porto de destino	Quando o tipo de protocolo for TCP ou UDP, digite configure o número da porta de destino da mensagem.
Modo ACL	Ele especifica o modo ACL no qual o switch processa as mensagens que correspondem à regra. • Permitir : Encaminhar as mensagens que correspondem à regra. • Proibir: Descarte as mensagens que correspondem à regra.

Aplicar ACL

As regras ACL entram em vigor quando aplicadas a portas físicas.

Clique em Segurança de rede > ACL > Aplicar ACL para entrar na página. Nesta página, você pode aplicar as regras ACL configuradas às portas físicas.



Descrição do parâmetro

Nome	Descrição
Porta Aplicada	Ele especifica o número da porta física à qual a regra ACL se aplica.
ID ACL	Ele especifica a regra ACL aplicada à porta.

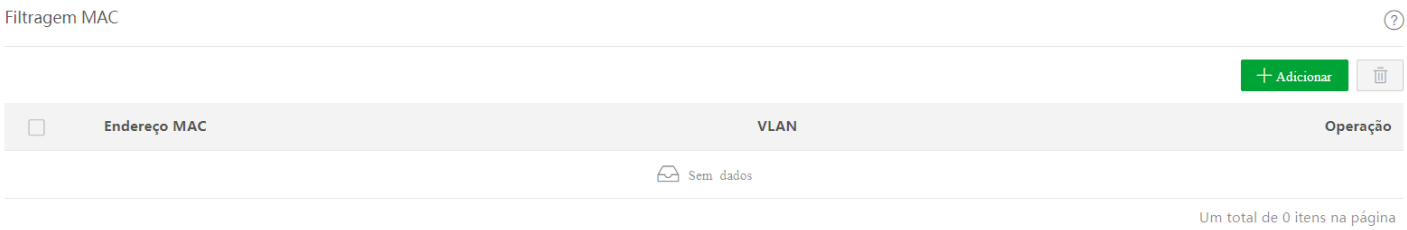
Direção de Filtragem	Ele especifica a direção de filtragem de mensagens da porta. Somente o Ingress é compatível com essa opção.

Filtragem MAC

Com esta função habilitada, o switch verifica o endereço MAC de origem e o endereço MAC de destino dos pacotes recebidos. Se o endereço MAC de origem ou o endereço MAC de destino de um pacote existir na lista de filtragem MAC, o pacote será descartado.

A filtragem MAC pode efetivamente impedir que usuários ilegais acessem a rede, melhorando assim a segurança da rede.

Clique em Network Security > MAC Filtering para entrar na página. Nesta página, você pode configurar as regras de filtragem MAC.



Descrição do parâmetro

Nome	Descrição
Endereço MAC	Ele especifica o endereço MAC a ser filtrado. Quando o endereço MAC de origem ou o endereço MAC de destino de um pacote for igual ao endereço MAC listado, o pacote será descartado.
VLAN	Ele especifica a VLAN na qual a regra de filtragem MAC entra em vigor.

802.1X

Visão geral

802.1X é uma tecnologia de controle de acesso à rede criada pelo IEEE. Ele é usado para autenticar e controlar os usuários da LAN. O sistema de autenticação envolve três partes: cliente, dispositivo e servidor de autenticação.

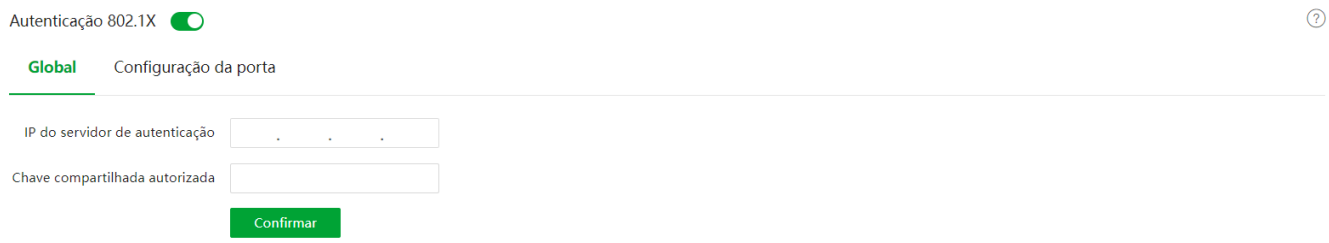
- Cliente de autenticação: Um dispositivo cliente envia uma solicitação de autenticação e o servidor de autenticação na LAN verifica sua validade. É necessário um software cliente compatível com autenticação 802.1X.
- Dispositivo de autenticação: Fornece interface para o cliente se conectar à LAN. Ele está localizado entre o cliente e o servidor de autenticação e decide se o cliente pode acessar a LAN ou não de acordo com a mensagem retornada pelo servidor de autenticação.

- Servidor de autenticação: Fornece serviço de autenticação para clientes. O comumente usado é o servidor RADIUS (Remote Authentication Dial-In User Service). O servidor de autenticação decide se o cliente passa a autenticação de acordo com a mensagem de autenticação do cliente enviada pelo dispositivo de autenticação e notifica o resultado ao dispositivo de autenticação. O dispositivo decide se o cliente pode acessar a LAN ou não. Essa chave serve como dispositivo de autenticação no sistema de autenticação. Ele se comunica com o servidor de autenticação por meio de terminação EAP. Depois de receber a mensagem EAP do cliente, o switch encapsula as informações de autenticação do cliente da mensagem na mensagem RADIUS padrão e, em seguida, encaminha a mensagem RADIUS para o servidor de autenticação. O diagrama básico do sistema de autenticação é mostrado a seguir.

Este switch suporta apenas autenticação com base no acesso à porta. Se um dos usuários passar na autenticação, a porta fica autorizada, e os seguintes usuários que utilizarem esta porta poderão acessar a rede sem autenticação. No entanto, quando esse usuário está offline, a porta se torna não autorizada e todos os outros usuários nessa porta não conseguem acessar a rede.

Global

Clique em **Segurança de rede > 802.1X > Global** para entrar na página. Nesta página, você pode configurar os parâmetros do servidor de autenticação 802.1X.

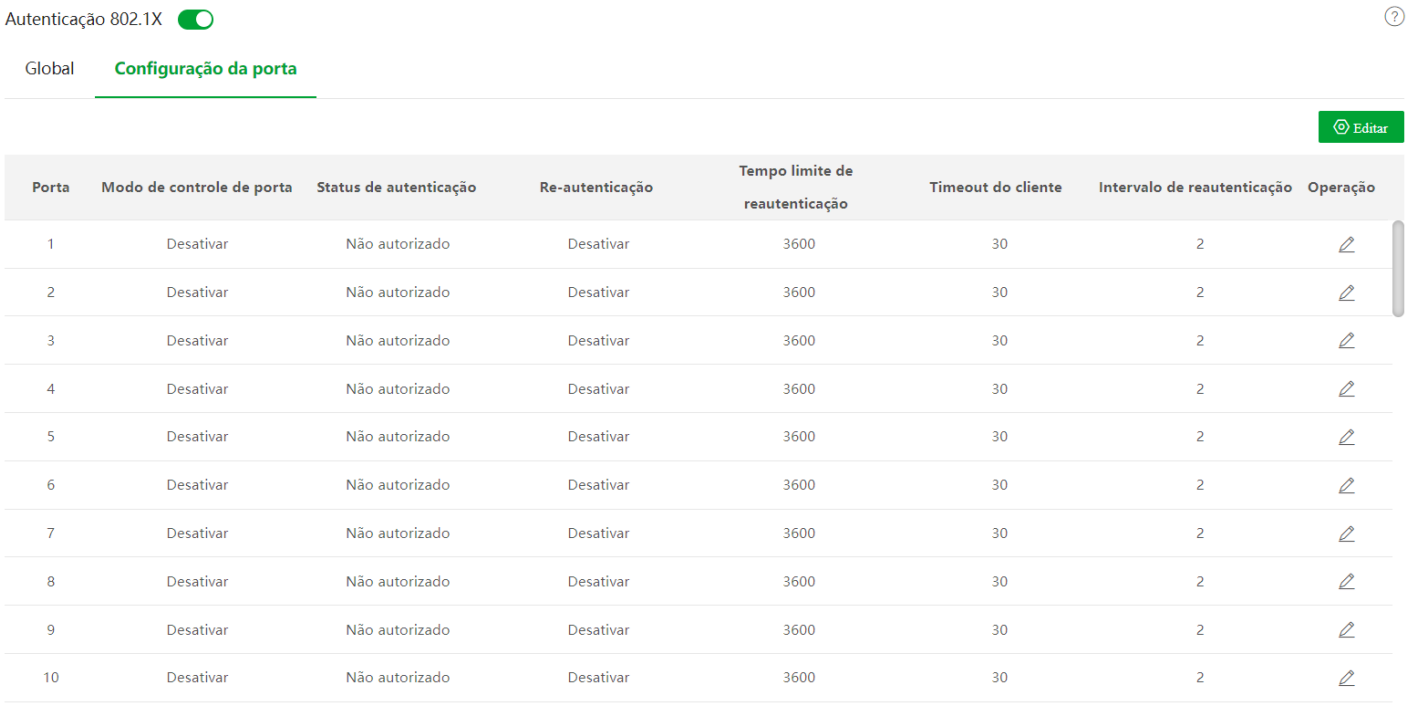


Descrição do parâmetro

Nome	Descrição
Autenticação 802.1X	É usado para ativar/desativar a função de autenticação 802.1X.
IP do servidor de autenticação	Ele especifica o endereço IP do servidor de autenticação RADIUS. Deve haver rotas alcançáveis entre o servidor de autenticação RADIUS e este switch.
Chave compartilhada autorizada	Ele especifica a chave compartilhada das mensagens de autenticação/autorização RADIUS. Deve ser igual à chave definida no lado do servidor de autenticação/autorização RADIUS.

Configuração da porta

Clique em **Network Security > 802.1X > Port Configuration** para entrar na página. Nesta página, você pode configurar os parâmetros de autenticação 802.1X para cada porta.



Descrição do parâmetro

Nome	Descrição
Porta	Ele especifica o ID da porta.
Modo de controle de porta	Especifica o modo de controle da porta para acessar a rede. • Auto: A autenticação 802.1X está habilitada na porta. O estado inicial é não autorizado e o usuário não pode acessar os recursos da rede. Se um usuário passar na autenticação, a porta é autorizada e o usuário pode acessar os recursos da rede. • Autorização Obrigatória: A porta está sempre no estado de autorização. Ele permite que os usuários acessem os recursos da rede. • Mandatory Non-authorization : A porta está sempre no estado de não-autorização. Ele proíbe os usuários de acessar os recursos da rede sem autenticação e autorização. • Desabilitar : A autenticação está desabilitada na porta. Ele permite que os usuários acessem os recursos da rede.
Status de Autenticação	Ele especifica o status de autenticação da porta. • Autorizado: O usuário tem permissão para acessar os recursos de rede pela porta. • Não autorizado: O usuário não tem permissão para acessar os recursos de rede pela porta.

Nome	Descrição
Reautenticação	Ele é usado para ativar/desativar a função de reautenticação 802.1X da porta. Com a função habilitada, o switch envia periodicamente uma solicitação de reautenticação ao cliente de autenticação para verificar o status da conexão e confirmar se o cliente de autenticação está online.

Tempo limite de reautenticação	Ele especifica o intervalo no qual o switch inicia a reautenticação para clientes de autenticação. Se a função de reautenticação estiver habilitada em uma porta, o switch lançará solicitações de reautenticação para os dispositivos online conectados à porta neste intervalo.
Tempo Limite do Cliente	Ele especifica o período de tempo limite no qual o cliente responde à solicitação de reautenticação. Após o switch enviar uma mensagem de solicitação de reautenticação para um cliente, se o switch não receber nenhuma resposta nesse período de tempo, o switch enviará a mensagem novamente.
Max Re- Horas de Autenticação	Ele especifica os tempos máximos de reautenticação com falha para um cliente. O switch força o cliente offline se os tempos de reautenticação com falha do cliente excederem esse valor.

Defesa de ataque

Visão geral

O switch suporta três métodos de defesa de ataque: Defesa de Ataque ARP, Defesa de Ataque DoS (Denial of Service) e Defesa de Ataque de Endereço MAC.

- Defesa de Ataque ARP

  A taxa recebida ARP é definida para evitar que as mensagens ARP na LAN sejam enviadas em massa para uma porta, resultando em sobrecarga da CPU e levando a falha de função ou até mesmo mau funcionamento do dispositivo.

  Se a taxa de recebimento de ARP do switch exceder o valor limite definido, o switch descartará aleatoriamente algumas mensagens ARP para garantir que a taxa recebida de ARP esteja dentro do valor limite definido.

- Defesa de Ataque DoS

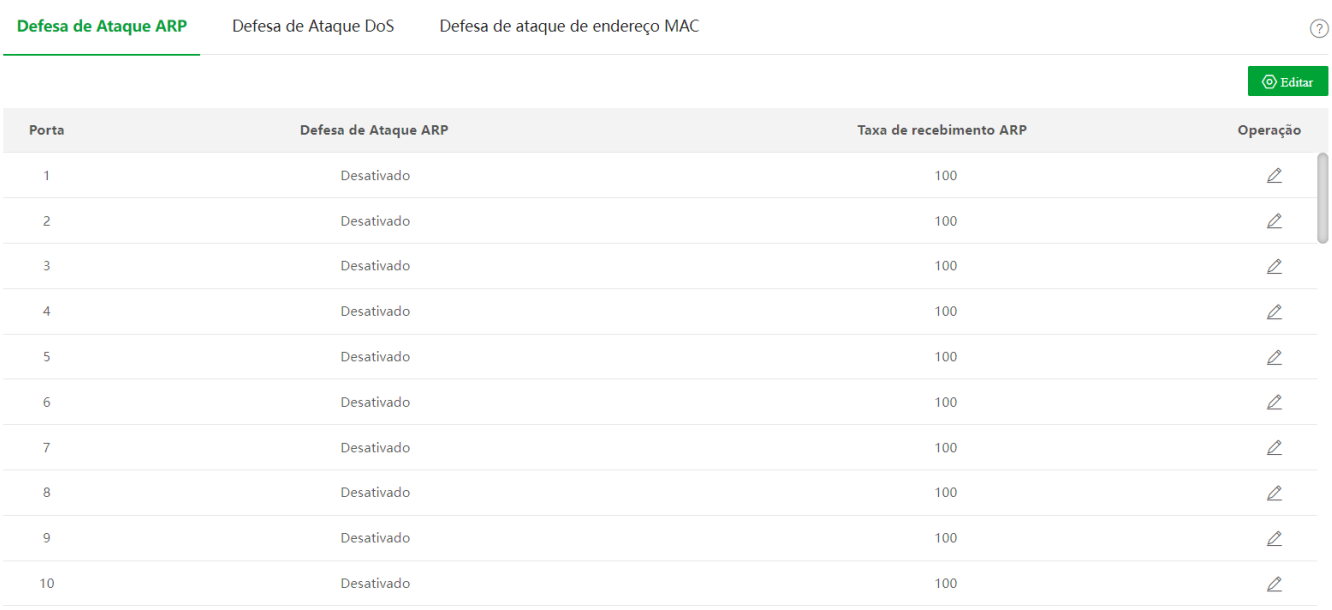
  A função DoS Attack Defense é usada para impedir que alguns hosts consumam recursos do servidor de forma maliciosa enviando um grande número de solicitações de serviço, deixando outros hosts incapazes de usar os serviços de rede adequadamente.

- Defesa de ataque de endereço MAC

  A defesa de ataque de endereço MAC limita o switch para aprender o endereço MAC, de modo a evitar que ele aprenda constantemente um grande número de endereços MAC de origem de mensagem inválida na LAN, o que pode aumentar a tabela de encaminhamento de endereço MAC e resultar na degradação do desempenho de encaminhamento.

Defesa de ataque ARP

Clique em Segurança de Rede > Defesa de Ataque > Defesa de Ataque ARP para entrar na página. Nesta página, você pode configurar o valor limite da taxa de recebimento de ARP do switch.

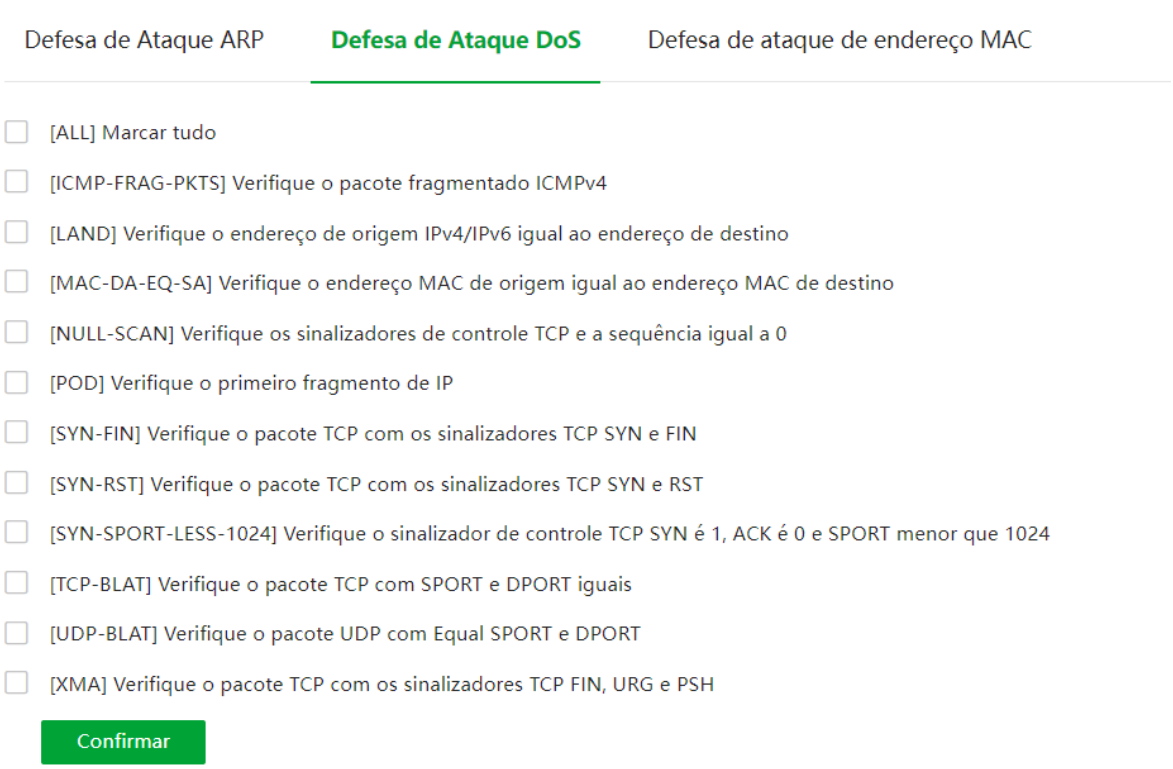


Descrição do parâmetro

Nome	Descrição
Porta	Ele especifica o número da porta do switch.
Defesa de Ataque ARP	É usado para habilitar ou desabilitar a função de defesa de ataque ARP.
Taxa Recebida ARP	Ele especifica a taxa máxima na qual o switch recebe as mensagens ARP. Se as mensagens ARP recebidas pelo switch dentro de 1 segundo excederem esse valor limite, o switch será considerado atacado pelo ARP e o switch descartará aleatoriamente algumas mensagens ARP.

Defesa de ataque DoS

Clique em Segurança de Rede > Defesa de Ataque > Defesa de Ataque DoS para entrar na página. Nesta página, você pode configurar as regras de defesa contra ataque DoS.



Descrição do parâmetro

Nome	**Descrição**
[TODOS] Marque tudo	Depois de marcado, o switch não encaminha todos os tipos de pacotes abaixo mencionados.
[ICMP-FRAG-PKTS] Verifique ICMPv4 fragmentado Pacote	Depois de marcado, o switch não encaminha pacotes fragmentados ICMPv4.
[TERRA] Verifique se o endereço de origem IPv4/IPv6 é igual Endereço de destino	Depois de marcado, o switch não encaminha pacotes IPv4/IPv6 com endereços IP de origem e destino correspondentes.
[MAC-DA-EQ-SA] Verifique o endereço MAC de origem Endereço MAC de destino igual	Depois de marcado, o switch não encaminha pacotes com endereços MAC de origem e destino correspondentes.
[NULL-SCAN] Verifique os sinalizadores de controle TCP e Sequência Igual a 0	Depois de marcado, o switch não encaminha pacotes TCP cujos sinalizadores de controle e números de sequência são definidos como 0.
[POD] Verifique o primeiro fragmento de IP	Depois de marcado, o switch não encaminha o primeiro fragmento de pacotes IP.
[SYN-FIN] Verifique o pacote TCP com os sinalizadores TCP SYN e FIN	Depois de marcado, o switch não encaminha pacotes TCP que contenham os sinalizadores SYN e FIN.
[SYN-RST] Verifique o pacote TCP com os sinalizadores TCP SYN e RST	Depois de marcado, o switch não encaminha pacotes TCP que contenham os sinalizadores SYN e RST.
[SYN-SPORT-LESS-1024] Verifique o sinalizador de controle TCP SYN é 1, ACK é 0 e SPORT menor que 1024	Depois de marcado, o switch não encaminha pacotes TCP cujo flag de controle SYN é 1, ACK é 0 e a porta de origem é menor que 1024.

[TCP-BLAT] Verifique o pacote TCP com SPORT e DPORT iguais	Depois de marcado, o switch não encaminha pacotes TCP com portas de origem e destino correspondentes.
[UDP-BLAT] Verifique o pacote UDP com igual ESPORTE e DPORT	Depois de marcado, o switch não encaminha pacotes UDP com portas de origem e destino correspondentes.
[XMA] Verifique o pacote TCP com os sinalizadores TCP FIN, URG e PSH	Depois de marcado, o switch não encaminha pacotes TCP que contenham sinalizadores TCP FIN, URG e PSH.

Defesa de ataque de endereço MAC

Clique em Segurança de rede > Defesa de ataque > Defesa de ataque de endereço MAC para entrar na página. Nesta página, você pode configurar se a porta pode encaminhar a mensagem unicast desconhecida.

Descrição do parâmetro

Nome	Descrição
Porta	Ele especifica o ID da porta.
Descarte MAC	Com esta função habilitada, a porta não aprende mais os endereços MAC e descarta as mensagens unicast desconhecidas recebidas.

Configurações do dispositivo

Gerenciamento de usuários

Atribuir diferentes permissões de acesso a diferentes tipos de usuários pode reduzir o risco de adulteração da configuração do switch.

Este switch suporta três tipos de usuários: administrador, usuário operacional e usuário comum.

- Administrador

  Há apenas um administrador criado pelo sistema por padrão. O administrador pode executar operações de todas as funções. O nome de usuário e a senha padrão são admin .

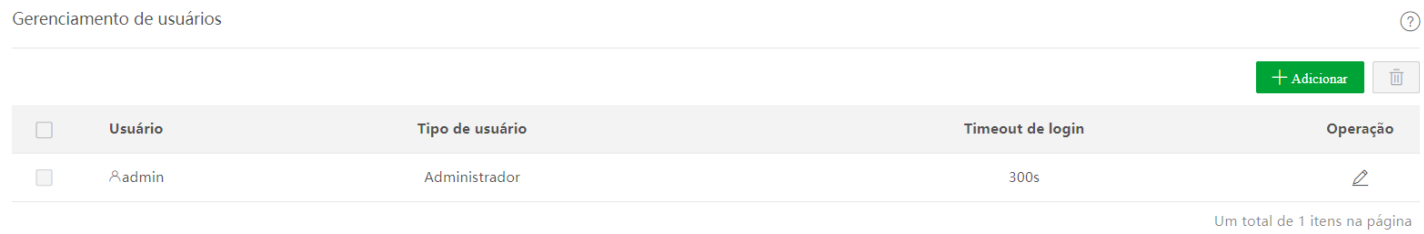
- usuário da operação

  Um usuário de operação pode executar todas as operações, exceto atualização de firmware, redefinição e gerenciamento de usuário.

- usuário comum

  Um usuário comum só pode verificar a configuração do switch.

  Clique em Configurações do dispositivo > Gerenciamento de usuários para entrar na página. Nesta página, você pode adicionar usuários para este switch (8 usuários no máximo).



Descrição do parâmetro

Nome	Descrição
Do utilizador	Ele especifica o nome do usuário.
Tipo de usuário	Ele especifica o tipo de um usuário. Este switch suporta três tipos de usuários: administrador, usuário operacional e usuário comum.
Tempo limite de login	Se um usuário não executar nenhuma operação no intervalo após o login no dispositivo, o sistema desconectará o usuário.

SNMP

Visão geral

O SNMP (Simple Network Management Protocol) permite que uma estação de gerenciamento gerencie remotamente os dispositivos de rede que suportam este protocolo, incluindo monitoramento do status da rede, modificação da configuração do dispositivo de rede, recebimento de alertas de eventos de rede e assim por diante.

O SNMP pode ignorar as diferenças físicas entre os dispositivos e realizar o gerenciamento automático para dispositivos de diferentes fornecedores.

estrutura de gerenciamento SNMP

A estrutura de gerenciamento SNMP consiste em três partes: gerenciador SNMP, agente SNMP e MIB (Management Information Base).

- Gerenciador SNMP: Um sistema usado para controlar e monitorar nós de rede por SNMP. O mais utilizado é o NMS (Network Management System), que pode ser um servidor especialmente utilizado para gerenciamento de rede ou um programa aplicativo para executar funções de gerenciamento de um dispositivo de rede.
- Agente SNMP: Software executado em dispositivos gerenciados para manter informações de gerenciamento e relatar dados de gerenciamento para um sistema de gerenciamento SNMP quando necessário.
- MIB: É uma coleção de objetos gerenciados. Quando o NMS gerencia os dispositivos, alguns parâmetros funcionais dos dispositivos gerenciados são necessários, como o estado da porta, a utilização da CPU e similares, que também são chamados de objetos gerenciados. A MIB define uma série de propriedades para esses objetos gerenciados: nome do objeto, direito de acesso, tipo de dados e assim por diante. Cada agente SNMP possui seu MIB correspondente e o gerenciador SNMP pode realizar operações de leitura/gravação de acordo com as permissões de gerenciamento.

O agente SNMP é gerenciado pelo gerenciador SNMP na rede SNMP e eles interagem entre si via SNMP.

Operações básicas do SNMP

As três operações básicas a seguir estão disponíveis para este switch obter intercomunicação entre o gerenciador SNMP e o agente SNMP:

- Obter: O gerenciador SNMP o utiliza para recuperar o(s) valor(es) de um ou mais objetos do agente SNMP.
- Set: O gerenciador SNMP o utiliza para reconfigurar o(s) valor(es) de um ou mais objetos no MIB.
- Trap: O agente SNMP o utiliza para enviar informações de alerta ao gerenciador SNMP.

Versões SNMP

Este switch é compatível com SNMPv1, SNMPv2c e SNMPv3.

- O SNMPv3 adota o método de autenticação com nome de usuário e senha.
- SNMPv1 e SNMPv2c adotam autenticação de nome de comunidade. Se o nome da comunidade da mensagem SNMP não passar na autenticação, a mensagem será descartada. O nome da comunidade SNMP define o relacionamento entre o gerenciador SNMP e o agente SNMP. Funciona como uma senha que limita o gerenciador SNMP para acessar o agente SNMP do switch.

Introdução MIB

O SNMP apresenta uma estrutura de árvore e cada nó de árvore representa um objeto gerenciado. Um objeto pode ser identificado com uma sequência de números que indicam um caminho a partir da raiz. A string numérica é o OID (identificador de objeto). Na figura a seguir, o OID do objeto A é (1.3.6.1.2.1.1); enquanto o objeto B é (1.3.6.1.2.1.2).

Visualizar

A exibição MIB é um subconjunto de todos os objetos gerenciados no MIB. Os objetos gerenciados são representados por OIDs, e a regra de visualização configurada (incluir / excluir) decide se o objeto é gerenciado ou não. OID de cada objeto gerenciado pode ser encontrado no software de gerenciamento SNMP.

Grupo

Depois de criar a exibição, você pode criar grupos SNMP. Você pode adicionar somente leitura / leitura e

de gravação/notificação para cada grupo SNMP para atribuir diferentes permissões de acesso a usuários em diferentes grupos.

Do utilizador

Depois de criar os grupos, você pode adicionar usuários a cada grupo. O gerenciador SNMP usa o nome de usuário e a senha de autenticação/criptografia criados aqui para efetuar login no agente SNMP.

Comunidade

Para SNMPv1 e SNMPv2c, após a criação da visualização, é necessário criar a comunidade. O nome do grupo funciona como uma senha para autenticação do gerenciador SNMP. As permissões de acesso de exibição de cada grupo podem ser adicionadas aqui para obter o gerenciamento de permissão de acesso.

Orientação de configuração

SNMPv3

Etapa	Operação	Descrição
1	básico	Obrigatório. Ative a função do agente SNMP.
2	Criar visualizações	Opcional. Crie exibições para os objetos gerenciados na página Exibir lista no controle de permissão . Uma exibição chamada Padrão é criada pelo sistema por padrão.
3	Criar grupos	Obrigatório. Crie grupos SNMP na página Group List on Permission Control e adicione exibições com diferentes permissões de acesso para os grupos.
4	Criar usuários	Obrigatório. Crie usuários SNMP na lista de usuários na página Controle de permissão e configure o modo de autenticação/criptografia, bem como a senha.
5	Configurar notificação	Opcional. Configure a notificação com a versão de segurança v3 na página Notificação .

SNMPv1/SNMPv2c

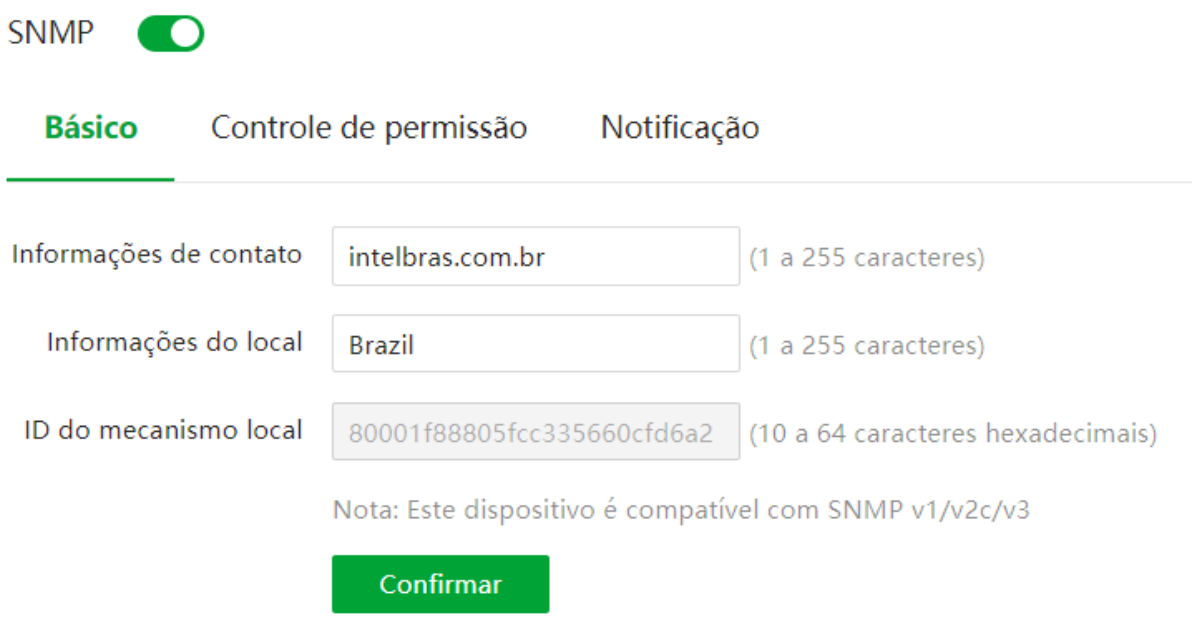
Etapa	Operação	Descrição
1	básico	Obrigatório. Ative a função do agente SNMP.
2	Criar visualizações	Opcional. Crie exibições para os objetos gerenciados na lista de exibição em Controle de permissão página. Uma exibição chamada Padrão é criada pelo sistema por padrão.

Etapa	Operação	Descrição

3	Criar comunidades	Obrigatório. Crie comunidades SNMP na lista de comunidades no controle de permissão página.
4	Configurar notificação	Opcional. Configure a notificação com a versão de segurança de v1/v2c em Notificação página.

Básico

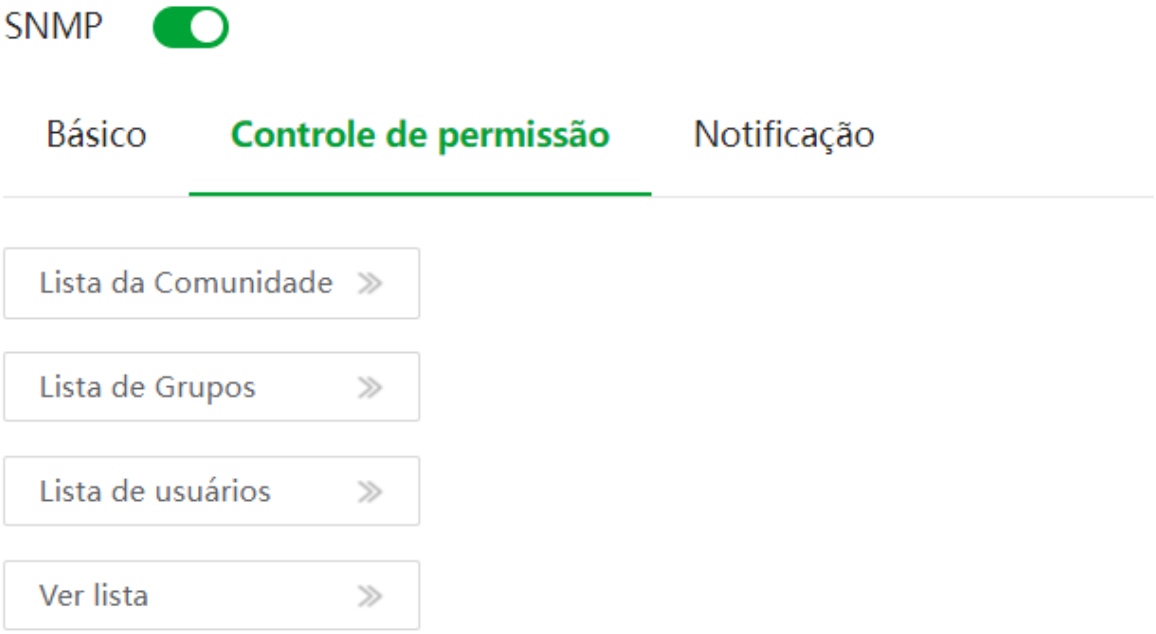
Clique em Configurações do dispositivo > SNMP > Básico para entrar na página. Nesta página, você pode configurar os parâmetros SNMP básicos.



Nome	Descrição
SNMP	É usado para habilitar/desabilitar a função SNMP.
Informações de contato	Ele é usado para configurar as informações de contato do switch para que o gerenciador SNMP localize rapidamente esse switch.
Informações de localização	Ele é usado para configurar as informações de localização do switch para que o gerenciador SNMP localize rapidamente esse switch.
ID do mecanismo local	Ele especificou o ID do mecanismo local do switch. Você precisa inserir esse ID no lado do gerenciador SNMP para gerenciar o switch.

Controle de permissão

Clique em **Configurações do dispositivo > SNMP > Controle de permissão** para entrar na página. Nesta página, você pode configurar as permissões SNMP.



Descrição do parâmetro

Funcionamento da porta		
Lista da Comunidade	Nome da comunidade	Especifica o nome de uma comunidade.
	Regra de acesso	Ele especifica a permissão de acesso para a comunidade acessar as exibições, incluindo somente leitura e leitura e gravação.
	Visualização MIB	Ele especifica as exibições que a comunidade pode acessar. A exibição MIB deve ser configurada com antecedência na lista de exibição .

Lista de grupos	Nome do grupo	Especifica o nome de um grupo.
	Nível de segurança	Ele especifica o nível de segurança do grupo: No Security , Authentication , Authentication&Privacy .
	Somente leitura	Controle as permissões de acesso para usuários em um grupo através da visualização Read&Write. Pelo menos um dos três tipos deve ser configurado.
	Notificação	A exibição MIB deve ser configurada com antecedência na lista de exibição .

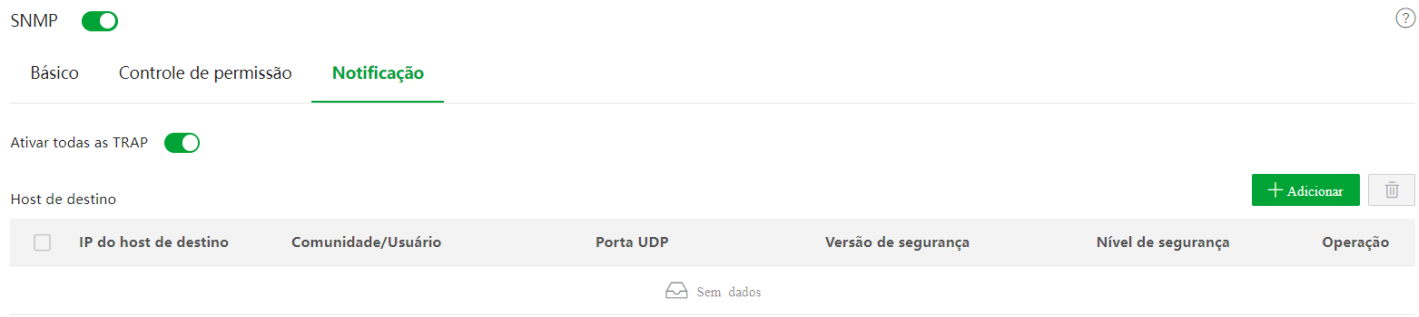
Lista de usuários	Nome de usuário	Ele especifica o nome do usuário.
	Grupo de usuários	Especifica o grupo do usuário. O grupo precisa ser configurado na Lista de grupos com antecedência.
	Nível de segurança	Especifica o nível de segurança do usuário. Após a seleção do grupo de usuários, o nível de segurança é preenchido automaticamente.
	Autenticação Modo	Ele especifica o modo de autenticação do usuário. Esta opção suporta apenas MD5 (MD5 Message Digest Algorithm). Este parâmetro pode ser definido apenas se o nível de segurança do grupo for Authentication ou Authentication&Privacy .
	Senha de Autenticação	Especifica a senha de autenticação do usuário. Este parâmetro pode ser definido apenas se o nível de segurança do grupo for Authentication ou Authentication&Privacy .
	modo de segurança	Ele especifica o modo de segurança do usuário. Este switch suporta dois modos de segurança: AES e DES. Este parâmetro pode ser definido apenas se o nível de segurança do grupo for Authentication&Privacy .
	Senha de segurança	Especifica a senha de segurança do usuário. Este parâmetro pode ser definido apenas se o nível de segurança do grupo for Authentication&Privacy .

	Exibir nome	Ele especifica o nome de uma visualização.
Ver lista	Regra	Ele especifica a regra OID. • include : Este OID pode ser gerenciado pelo SNMP. • exclude : Este OID não pode ser gerenciado pelo SNMP.
	MIB Subárvore OID	Especifica os objetos gerenciados (representados por OID) da visão.

Notificação

A função de notificação permite que o switch use o mecanismo Trap para relatar eventos importantes (como uma reinicialização do dispositivo) das visualizações, para que o gerente possa monitorar e lidar com os eventos específicos do switch com o software de gerenciamento SNMP.

Clique em Configurações do dispositivo > SNMP > Notificação para entrar na página. Nesta página, você pode configurar a função de notificação SNMP.



Descrição do parâmetro

Nome	Descrição
Ativar todas as armadilhas	É usado para habilitar/desabilitar a função Trap.
IP do host de destino	Ele especifica o endereço IP do host de destino da interceptação, que também é o endereço IP do host gerenciado. Certifique-se de que haja rotas alcançáveis entre o host de destino e este switch.

Comunidade/Usuário	Ele especifica o nome da comunidade, nome do usuário ou nome do grupo exigido pela autenticação. Você precisa inserir o nome do grupo correspondente, nome de usuário ou nome da comunidade. Se a Versão de segurança for definida como v3 , apenas um nome de usuário ou nome de grupo será permitido. Se a Versão de segurança for definida como v1 ou v2c , apenas um nome de comunidade será permitido.
Porta UDP	Ele especifica a porta UDP habilitada para Trap no host gerenciado.
Versão de segurança	É usado para selecionar uma versão de segurança usada pelo Trap, incluindo v1, v2c e v3, que deve ser consistente com a versão do gerenciador SNMP.
Nível de segurança	Quando a versão de segurança é definida como v3, você precisa selecionar um nível de segurança. O nível de segurança inclui Sem segurança , Autenticação e Autenticação e privacidade .

Hora do sistema

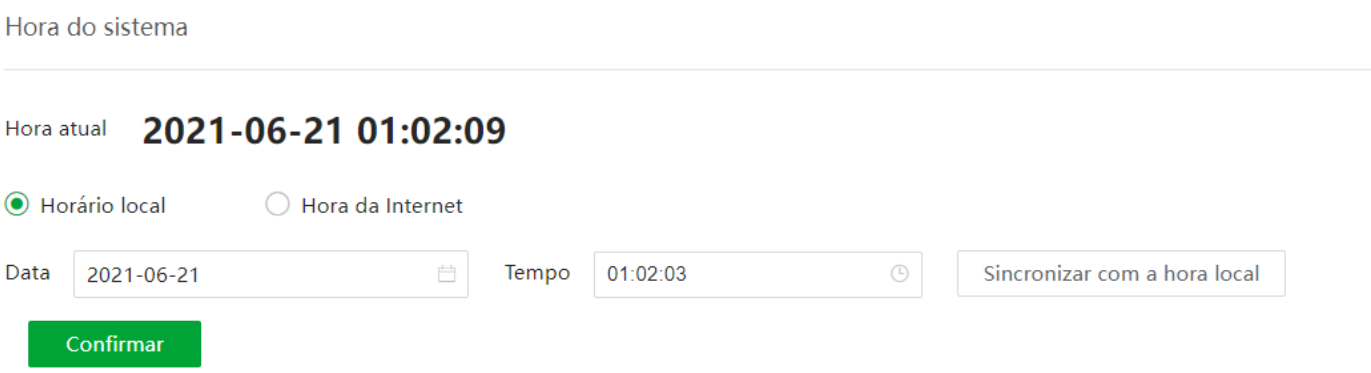
Para garantir que as funções baseadas em tempo do comutador funcionem corretamente, é necessário garantir que a hora do sistema do comutador seja precisa. Este switch suporta configuração manual e calibração de internet.

Para acessar a página, clique em Configurações do dispositivo > Hora do sistema .

Configuração manual

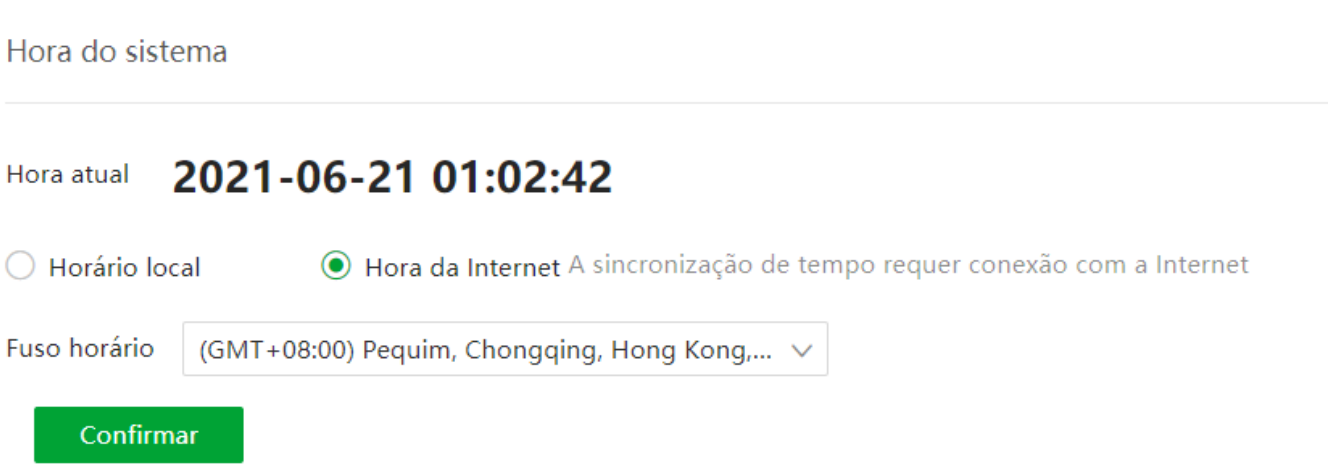
O administrador da rede precisa definir manualmente a hora do sistema do switch. Após a reinicialização do switch a cada vez, o administrador precisa redefini-lo.

Você pode modificar manualmente a data e a hora ou clicar em Sincronizar com a hora local para sincronizar a hora do switch com o dispositivo de gerenciamento.



Calibração Internet

O switch sincroniza automaticamente com o servidor de horário da Internet. Desde que o switch esteja conectado à Internet, ele pode calibrar automaticamente a hora do sistema. Depois que o interruptor é reiniciado, ele também pode calibrar o tempo automaticamente.



Gerenciamento de registros

Informações de registro

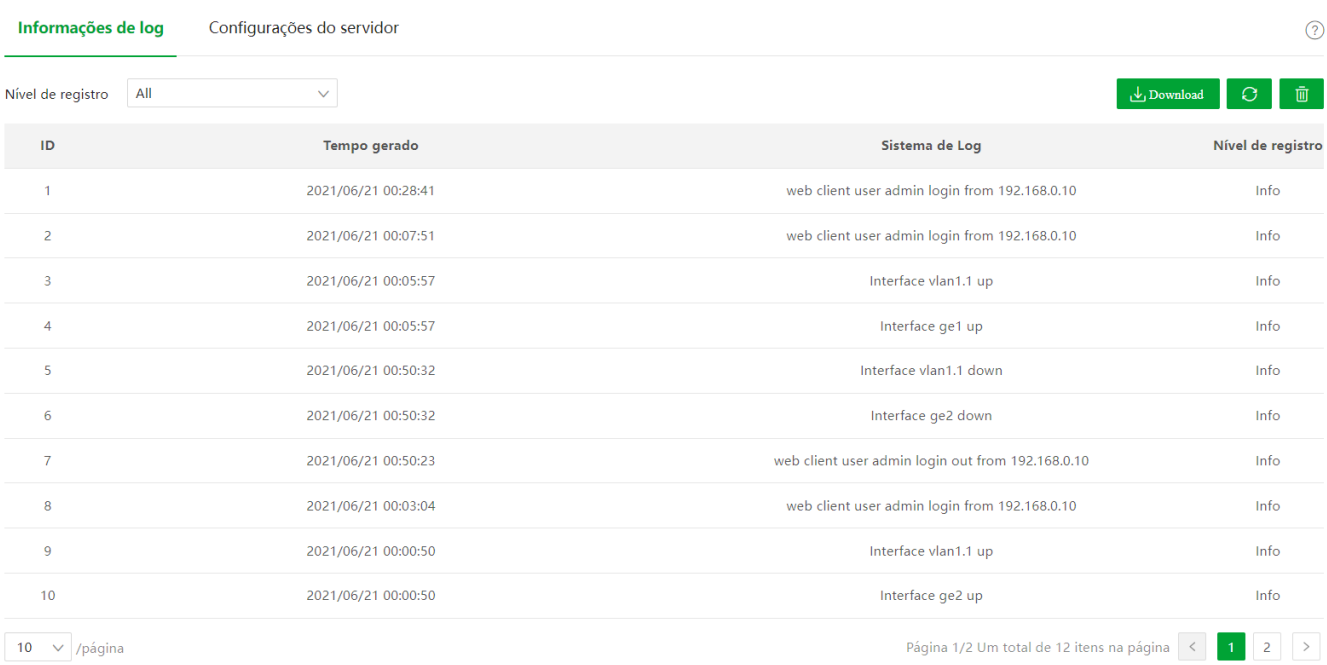
Os logs de um switch registram todos os eventos e as operações do usuário após o switch ser redefinido desde a última vez. Você pode verificar as informações de log do switch para solucionar problemas se houver alguma falha de rede.

Por padrão, o switch salva os últimos 1.000 logs. Se os logs excederem o limite, o switch limpará os logs anteriores.

Os logs são divididos em sete níveis com base na importância e podem ser filtrados de acordo com o nível do log. Quanto menor o valor, maior a emergência.

Nível de registro	Valor	Descrição
Emergência	1	Informações indisponíveis do sistema
Alerta	2	Mensagem que precisa ser respondida rapidamente
Crítico	3	Informacao critica
Erro	4	Informação de erro
Aviso	5	Informações de aviso
informação	6	Notificação que precisa ser registrada
depurar	7	Mensagem gerada no processo de depuração

Clique em **Dispositivo Settings > Log Management > Log Info** para entrar na página. Nesta página, você pode visualizar, baixar e excluir as informações de log do switch.

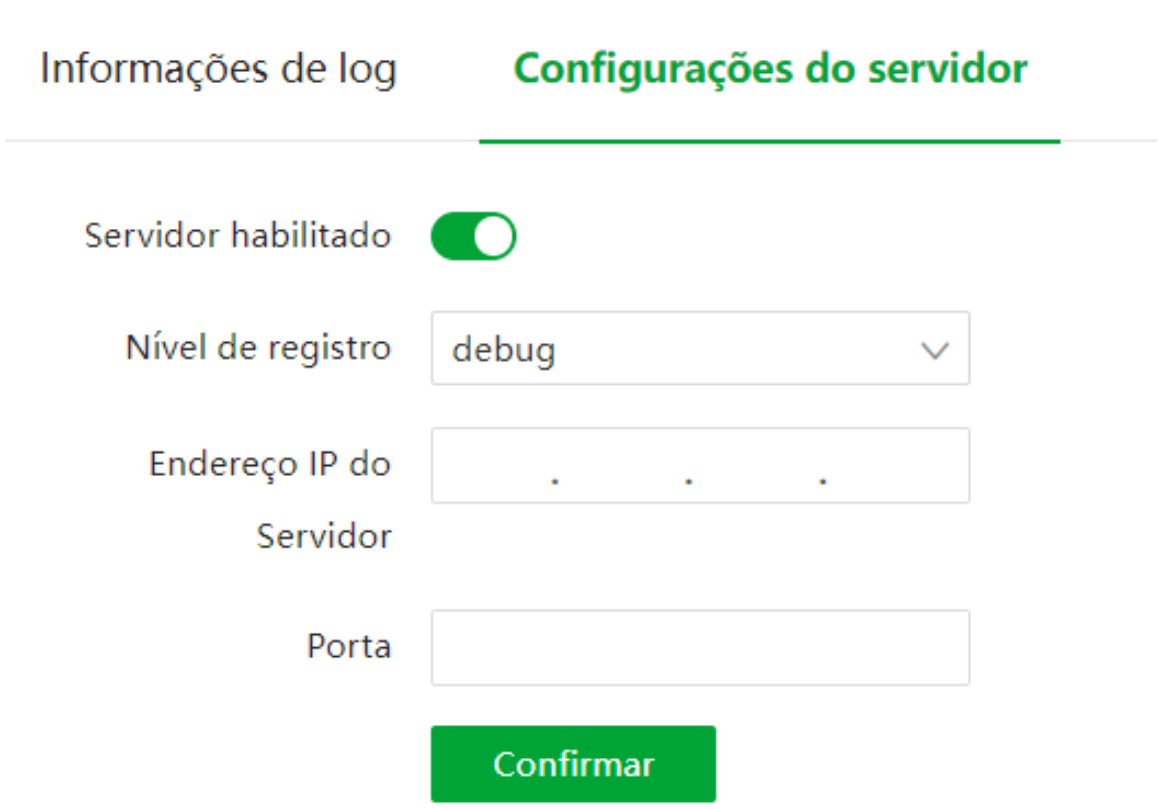


Descrição do parâmetro

Nome	Descrição
Nível de registro	Ele é usado para filtrar quais logs são exibidos por nível de log.
EU IA	Ele especifica o ID do log.
Tempo Gerado	Ele especifica o ponto no tempo quando o log é gerado.
Registro do sistema	Exibe o conteúdo do log.
Nível de registro	Ele especifica o nível do log.

Configurações do servidor

Clique em **Dispositivo Configurações > Log Management > Configurações do servidor** para entrar na página. Nesta página, você pode configurar o servidor de log e carregar as informações de log do switch para o servidor.



Descrição do parâmetro

Nome	Descrição
Servidor ativado	É usado para ativar/desativar o servidor de log.
Nível de registro	Logs deste nível e acima serão enviados para o servidor.
Endereço IP do servidor	Ele especifica o endereço IP do servidor de log. Certifique-se de que haja rotas alcançáveis entre o servidor de log e este switch.
Porta	Especifica a porta na camada de transporte usada pelo servidor de log.

RMON

Visão geral

RMON (Remote Network Monitoring), baseado em SNMP, é uma especificação de monitoramento padrão desenvolvida pela IETF (Internet Engineering Task Force) que permite aos administradores de rede detectar problemas de rede, como queda de pacotes, colisões de rede e congestionamento de tráfego. Por meio do RMON MIB, os administradores de rede podem monitorar dispositivos de rede remotos com eficiência, analisando os dados históricos. O RMON reduz o fluxo de tráfego entre o NMS e os dispositivos gerenciados, o que é conveniente para gerenciar grandes redes.

Mecanismo RMON

O RMON inclui duas partes: o NMS e os Agentes executados em cada dispositivo de rede. O switch é um Agente RMON.

Os Agentes coletam e salvam estatísticas de tráfego no RMON MIB. O switch é incorporado com a função de agentes para sondar.

Com base no protocolo SNMP, o NMS coleta dados da rede por meio da comunicação com os Agentes.

grupo RMON

O switch suporta RMONv1 que define vários grupos RMON. O switch implementa grupo de estatísticas, grupo de histórico, grupo de alarme e grupo de evento suportado pelo MIB público.

- Estatisticas

  O grupo de estatísticas define que o sistema coleta várias estatísticas de tráfego em uma interface Ethernet e salva as estatísticas na tabela de estatísticas Ethernet para recuperação futura. As estatísticas de tráfego da interface incluem colisões de rede, erros de alinhamento CRC, pacotes subdimensionados/superdimensionados, broadcasts, multicasts, bytes recebidos e pacotes recebidos.

  Depois de criar uma entrada de estatísticas para uma interface, o grupo de estatísticas começa a coletar estatísticas de tráfego na interface. As estatísticas na tabela de estatísticas Ethernet são somas cumulativas.

- História

  O grupo de histórico define que o sistema coleta periodicamente estatísticas de tráfego nas interfaces e salva as estatísticas na tabela de registro de histórico. As estatísticas incluem eventos perdidos, bytes recebidos, unicasts, broadcasts, multicasts, erros de alinhamento CRC, pacotes subdimensionados/superdimensionados e pacotes em conflito.

  A tabela de estatísticas de histórico registra as estatísticas de tráfego coletadas para cada intervalo de amostragem. O intervalo de amostragem é configurável pelo usuário.

- Alarme

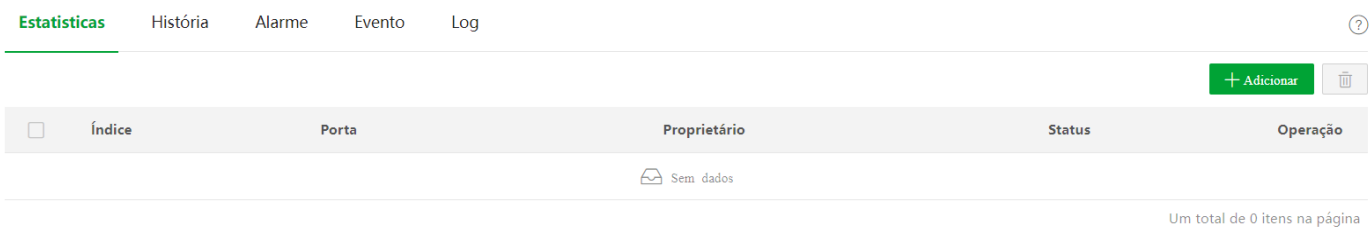
  O grupo de alarme monitora variáveis de alarme, como a contagem de pacotes recebidos em uma interface. Depois de definir uma entrada de alarme, o sistema obtém o valor da variável de alarme monitorada no intervalo especificado. Se o valor da variável monitorada for maior ou igual ao limite de aumento, um evento de aumento é acionado. Se o valor da variável monitorada for menor ou igual ao limite de queda, um evento de queda é acionado. O evento é tratado conforme definido no grupo de eventos.

- Evento

  O grupo de eventos define índices de eventos e controla a geração e notificações dos eventos acionados pelos alarmes definidos no grupo de alarmes. Os eventos podem ser tratados de duas formas: Log e Trap.

Estatisticas

Clique em **Dispositivo Configurações > RMON > Estatísticas** para entrar na página. Nesta página, você pode configurar o grupo de estatísticas RMON.

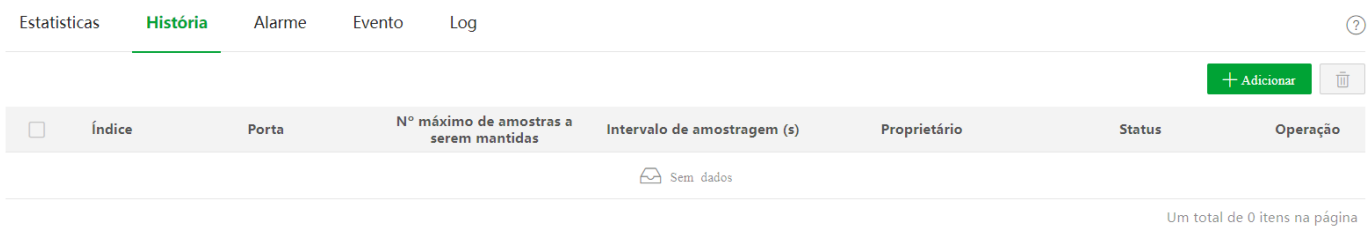


Descrição do parâmetro

Nome	Descrição
Índice	Ele especifica o número do índice de entrada de estatísticas.
Porta	É usado para escolher uma porta para a qual a entrada de estatísticas deve ser exibida. Cada porta corresponde a apenas uma entrada de estatísticas.
Proprietário	Ele especifica o proprietário da entrada.
Status	Especifica o status da entrada de estatísticas, ativo ou inativo.

Histórico

Clique em **Dispositivo Histórico** para entrar na página. Nesta página, você pode configurar o grupo de histórico RMON.



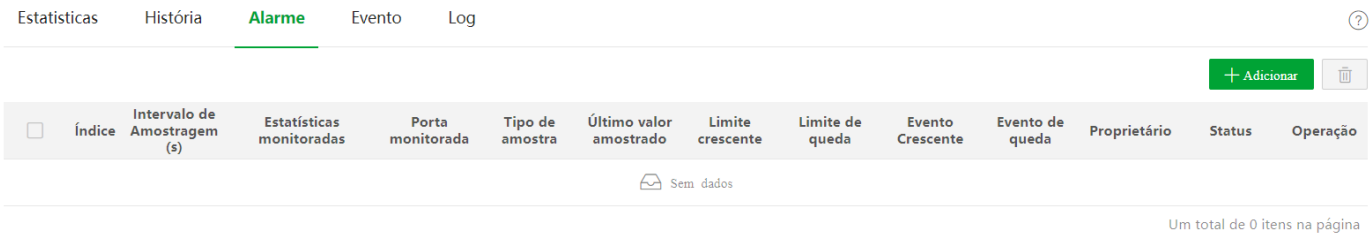
Descrição do parâmetro

Nome	Descrição
Índice	Ele especifica o número do índice da entrada do histórico.
Porta	É usado para escolher uma porta para a qual a entrada do histórico deve ser exibida.

Nº máximo de amostras a serem mantidas	É usado para definir a capacidade da tabela de histórico. Quando as amostras atingirem o máximo, o sistema excluirá os registros anteriores para salvar novas amostras.
Intervalo de amostragem (seg)	Especifica o tempo em segundos que as amostras são coletadas das portas.
Proprietário	Ele especifica o proprietário da entrada.
Status	Ele especifica o status da entrada do histórico, ativo ou inativo.

Alarme

Clique em **Dispositivo Alarme para entrar na página**. Nesta página, você pode configurar o grupo de alarme RMON.



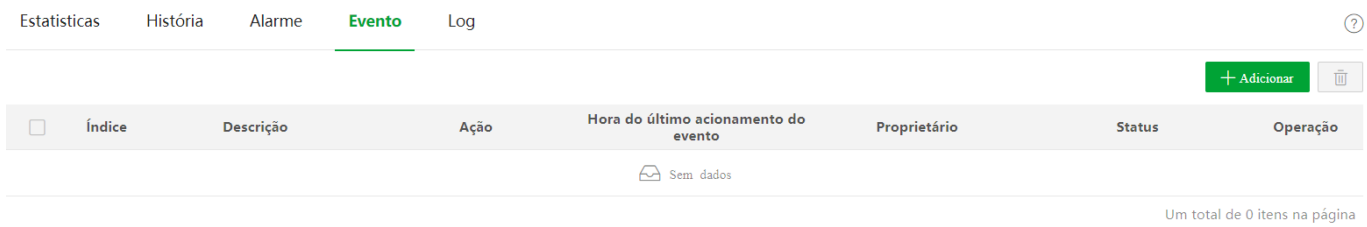
Descrição do parâmetro

Nome	**Descrição**
Índice	Especifica o número de índice da entrada de alarme.
Intervalo de amostragem (seg)	Especifica o tempo em segundos que as amostras são coletadas das portas.
Estatísticas monitoradas	Ele especifica as estatísticas de tráfego a serem coletadas e monitoradas.
Porta Monitorada	Ele especifica a porta cujas estatísticas de tráfego são coletadas e monitoradas.
Tipo de amostra	Especifica o método de amostragem para gerar um alarme - Absoluto ou Delta. • Absoluto : A chave compara o valor de amostragem com os limites de subida e descida predefinidos. • Delta : O switch obtém a diferença entre os valores de amostragem do intervalo atual e do intervalo anterior e, em seguida, compara a diferença com os limites de aumento e queda predefinidos.
Último valor amostrado	Ele especifica o valor amostrado mais recente.
Limiar crescente	Especifica o limite de aumento do alarme.
Limiar de queda	Especifica o limite de queda do alarme.
Evento Ascendente	É usado para definir a ação que o sistema executa quando o valor da variável de alarme é maior que o limite de aumento do alarme.

Evento de queda	É usado para definir a ação que o sistema toma quando o valor da variável de alarme é menor que o limite de queda do alarme.
Proprietário	Ele especifica o proprietário da entrada.
Status	Especifica o status da entrada de alarme, ativo ou inativo.

Evento

Clique em **Dispositivo Evento para entrar na página**. Nesta página, você pode configurar o grupo de eventos RMON.

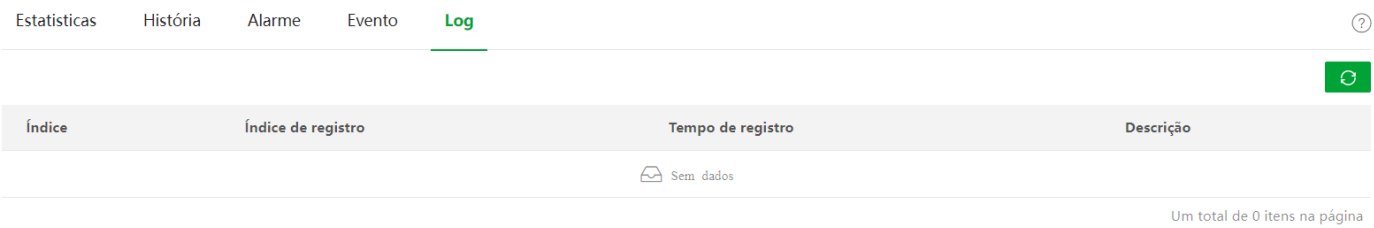


Descrição do parâmetro

Nome	Descrição
Índice	Ele especifica o número do índice da entrada do evento.
Descrição	Especifica a descrição do evento.
Ação	Especifica a ação a ser executada quando um evento é acionado. − Log : O switch registra as informações do evento (incluindo hora e descrição do evento) na tabela de log de eventos para que o dispositivo de gerenciamento possa obter os logs por meio do SNMP. − Trap : O switch envia uma notificação SNMP para o NMS.
Hora do último acionamento do evento	Ele especifica a hora mais recente de um evento acionado.
Proprietário	Ele especifica o proprietário da entrada.
Status	Ele especifica o status da entrada do evento, ativo ou inativo.

Registro

Clique em Dispositivo Log para entrar na página. Nesta página, você pode visualizar os logs gerados sobre os eventos disparados do RMON.



Descrição do parâmetro

Nome	Descrição
Índice	Ele especifica o número do índice da entrada do evento.
Índice de registro	Especifica o número de série do log.
Tempo de registro	Especifica o tempo de geração das informações de log.
Descrição	Especifica a descrição do evento.

Visualização

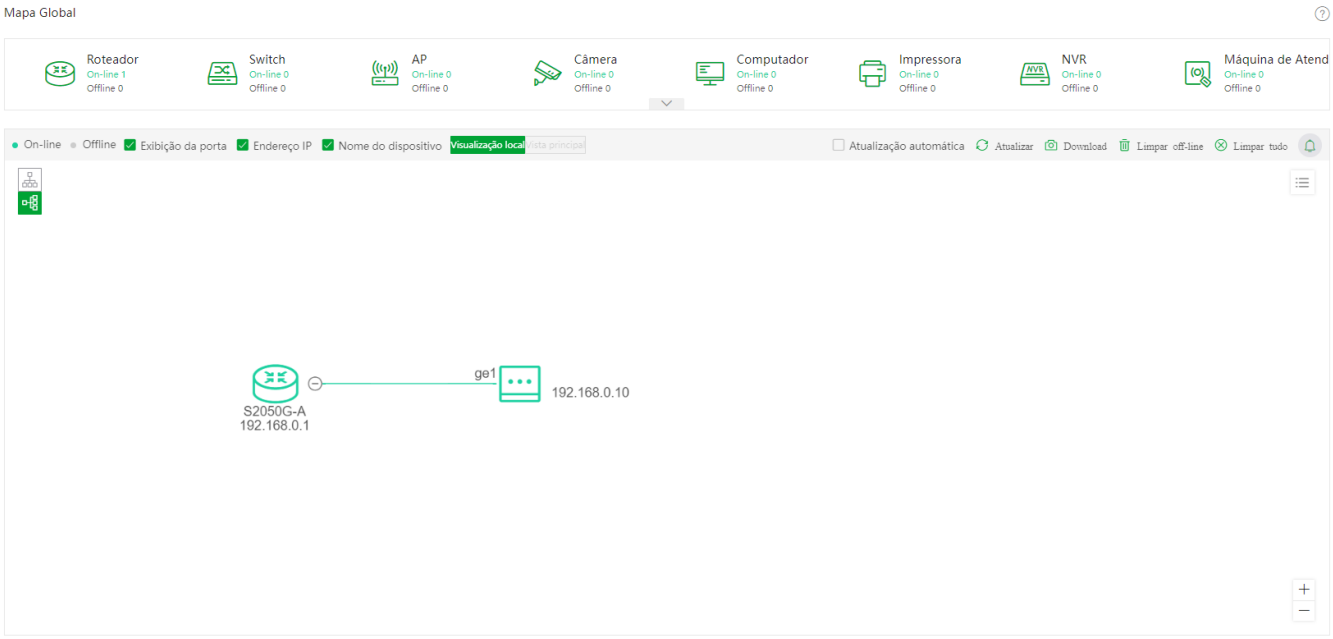
Para redes sem necessidade de acesso à internet (como redes de monitoramento de segurança de médio e grande porte), o gerenciamento em nuvem não está disponível. A função de visualização deste switch fornece gerenciamento central e manutenção para essas redes.

Com a função Visualização, o switch pode gerenciar localmente os dispositivos na rede. Com base em protocolos como LLDP, UPnP e ARP, o sistema pode descobrir automaticamente os dispositivos conectados a este switch (como roteador, switch, câmera IP, AP) e gerar uma topologia de rede, na qual você pode visualizar e configurar o parâmetros básicos desses dispositivos.

Mapa global

Clique em Visualização > Mapa Global para entrar na página. Nesta página, você pode visualizar e configurar os parâmetros básicos do switch e dos dispositivos conectados a este switch.

Descrição do parâmetro



,

Nome	Descrição
Mapa global	Ele exibe todos os tipos de dispositivos online e offline na rede LAN.

Online & Offline	Na topologia, os ícones de dispositivo verde representam dispositivos online, cinza para dispositivos offline.
Display Port	Com esta função habilitada, as portas do switch que estão conectadas aos dispositivos enquanto cinza para dispositivos offline.
Endereço de IP & Nome do dispositivo	Com as funções ativadas, os endereços IP e os nomes dos dispositivos são exibidos na topologia.

Ele especifica a visão topológica da rede atual.

- Local View: Especifica a topologia com este dispositivo como nó raiz.
- Main View: Especifica a topologia com o dispositivo principal como nó raiz.

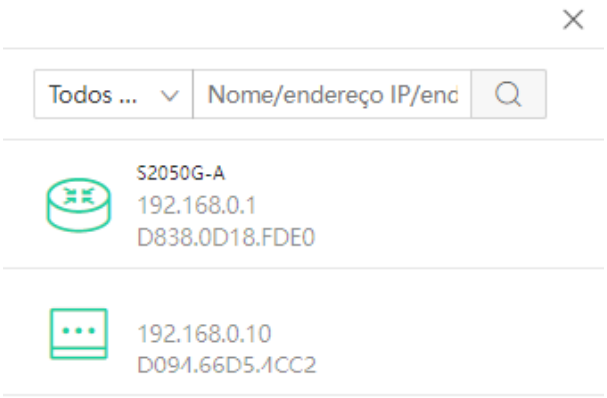
Visualização Local/Visualização Principal

Dica

- Quando houver apenas um dispositivo principal que não seja este dispositivo na topologia, você pode alternar para a exibição principal.
- O dispositivo principal é o principal dispositivo de comutação da rede. Você pode personalizá-lo.

- Pesquisar um dispositivo

  Se você deseja pesquisar um dispositivo, clique. Em seguida, você pode pesquisar o dispositivo filtrando o tipo de dispositivo ou inserindo diretamente o nome do dispositivo/endereço IP/endereço MAC na barra de pesquisa. Clique no ícone do dispositivo e você será direcionado para a localização deste dispositivo na topologia de rede.



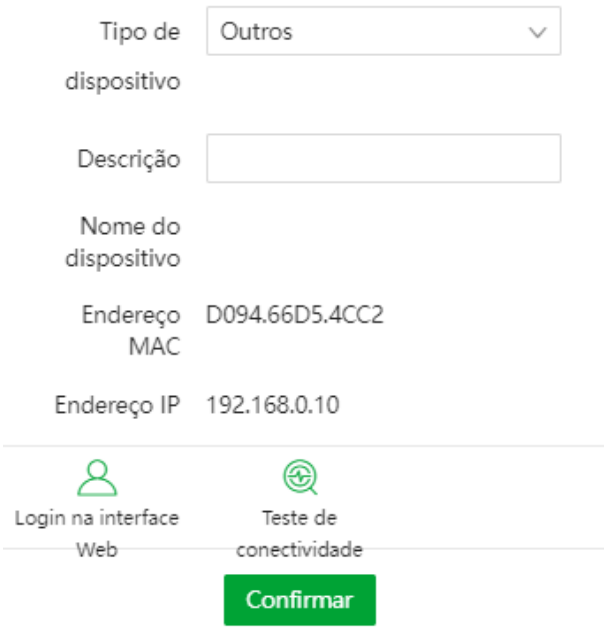
- Ver e modificar parâmetros

  Você pode visualizar e modificar os parâmetros deste switch clicando no ícone deste switch.

: É usado para atualizar a topologia da rede.

: É usado para habilitar/desabilitar cada porta.

Você pode visualizar e modificar os parâmetros de outros dispositivos clicando no ícone do dispositivo.

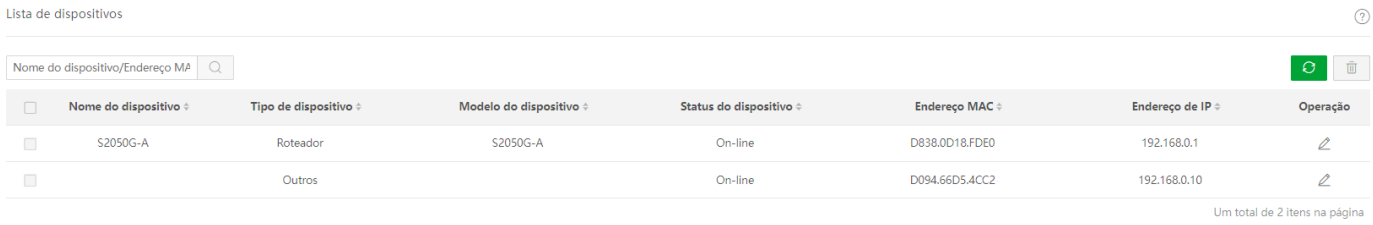


: Ele é usado para entrar na IU da web do dispositivo..

: É usado para testar a conectividade do dispositivo.

Lista de dispositivos

Clique em **Visualização > Lista de dispositivos** para entrar na página. Nesta página, você pode visualizar e modificar as informações básicas de todos os dispositivos.



Descrição do parâmetro

Nome	Descrição
Nome do dispositivo	Dica O nome do dispositivo modificado aqui é exibido apenas na seção Visualização, e o campo correspondente na mensagem do protocolo não será alterado.
Tipo de dispositivo	Especifica o tipo do dispositivo. Você pode clicar para modificar o tipo de dispositivo. Dica

Ele especifica o nome do dispositivo. Se estiver em branco, indica que não há campo correspondente na mensagem do protocolo. Você pode clicar para modificar o nome do dispositivo.

O tipo de dispositivo modificado aqui é exibido apenas na seção Visualização, e o campo correspondente na mensagem do protocolo não será alterado.

Modelo do dispositivo	Especifica o modelo do dispositivo. Se estiver em branco, indica que não há campo correspondente na mensagem do protocolo. Você pode clicar em modificar o modelo do dispositivo.
Status do dispositivo	Ele especifica o status online/offline do dispositivo.
Endereço MAC	Ele especifica o endereço MAC do dispositivo.
Endereço de IP	Ele especifica o endereço IP do dispositivo.

Apêndice

Siglas e abreviaturas A

Sigla ou Abreviatura	Ortografia completa
ACL	Lista de controle de acesso
ARP	Protocolo de Resolução de Endereço
BPDU	Unidade de dados do protocolo de ponte
CIST	Árvore abrangente comum e interna
CoS	Classe de serviço
CRC	Verificação de redundância Cíclica
CST	Árvore Abrangente Comum
DHCP	Protocolo de Configuração de Host Dinâmico
DoS	Negação de serviço
DS	Serviços Diferenciados
DSCP	Ponto de Código de Serviços Diferenciados
IEEE	Instituto de Engenheiros Elétricos e Eletrônicos
IETF	Força-Tarefa de Engenharia da Internet
IGMP	Protocolo de Gerenciamento de Grupo de Internet
IST	Árvore Abrangente Interna
LACP	Protocolo de controle de agregação de link
LLDP	Protocolo de Descoberta da Camada de Enlace
LLDP-MED	Protocolo de Descoberta da Camada de Link - Descoberta de Endpoint de Mídia
LLDPDU	Unidade de Dados do Protocolo de Descoberta da Camada de Enlace
MSTI	Múltiplas Instâncias Spanning Tree
MIB	Base de Informações Gerenciais
MSTP	Protocolo Multi Spanning Tree
NMS	Sistema de gerenciamento de rede
OID	Identificador de objeto
QoS	Qualidade de serviço
RAIO	Serviço de usuário de discagem de autenticação remota
RMON	Monitoramento remoto de rede

Sigla ou Abreviatura	Ortografia completa
RSTP	Protocolo Rapid Spanning Tree
SNMP	Protocolo de gerenciamento de rede simples
STP	Protocolo Spanning Tree
TCI	Informações de controle de etiqueta
TCN BPDU	Notificação de alteração de topologia BPDU
TLV	Tipo/Comprimento/Valor
Para% s	Tipo de serviço
TPID	Identificador de Protocolo de Tag
TTL	Tempo de Viver
VoD	Vídeo sob demanda
VoIP	Voz sobre Protocolo de Internet
VLAN	Rede local virtual

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

Produzido por: Intelbras S/A – Indústria de Telecomunicação Eletrônica Brasileira

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)

Indústria Brasileira