



Manual do Usuário

S3028G-B LITE



Versão deste manual: 1.1.1

S3028G-B LITE

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

O switch S3028G-B LITE é um switch de 24 portas Gigabit Ethernet 10/100/1000 + 4 portas SFP +.

Proporciona altas taxas de transferência de dados, permitindo a integração de computadores, impressoras, dispositivos VoIP, telefones IP e câmeras de segurança, além do compartilhamento de internet para os demais dispositivos conectados a ele (dependendo do tipo de acesso e equipamento de banda larga disponível). Este switch integra múltiplas funções com excelente desempenho e fácil configuração.

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

ÍNDICE

EXPORTAR PARA PDF

PROTEÇÃO E SEGURANÇA DE DADOS

Tratamento de dados pessoais

Diretrizes que se aplicam aos funcionários da Intelbras

Diretrizes que controlam o tratamento de dados

Uso indevido e invasão de hackers

Informação

ACESSO A INTERFACE DE GERENCIAMENTO

Login

BÁSICO

Resumo do sistema

Porta

Espelhamento de porta

Agregação de porta

Limite de taxa de porta

Estatísticas de pacote

VLAN

Configuração VLAN 802_1Q

MAINTENANCE

Atualização de Firmware

Importação de configuração

Backup

Reiniciar

Configurações de fábrica

SWITCHING

DHCP relay

DHC Snooping

Global

Configuração LLDP

Configuração de porta

Informações do vizinho

SEGURANÇA DE REDE

ACL

Filtragem MAC

802.1X

Defesa de ataque

IMG SNOOPING

Global

Saida rapida

CONFIGURAÇÃO MAC

Endereço MAC

ROUTING

Roteamento estático

Roteamento dinamico

RIP Roteamento Dinâmico

ARP

Server DHCP

Configurações de DHCP

Reserva de DHCP

Lista de clientes

QoS POLICY

Orientação de configuração

Agendador de QoS

802.1P

DSCP

Prioridade de porta

SEGURANÇA DE REDE

MAC ACL

IP ACL

Aplicar ACL

Filtragem MAC

802.1X

Global

Configuração da porta

Defesa de ataque

Defesa de ataque ARP

Defesa de ataque DoS

Defesa de ataque MAC

CONFIGURAÇÕES DO DISPOSITIVO

SNMP

Hora do Sistema

Configuração manual

Calibração Internet

Gerenciamento

Configurações do servidor

Diagnóstico

Teste de ping

Teste de ping Tracert

TERMO DE GARANTIA

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.

ACESSO A INTERFACE DE GERENCIAMENTO

Login

Para acessar a interface de gerenciamento do switch, abra o navegador e na barra de endereços digite o endereço IP de gerência do switch(192.168.0.1). <http://192.168.0.1> (<http://192.168.0.1>), pressione a tecla Enter.



Obs: Para efetuar o login no switch, o endereço IP da interface de rede do seu computador conectada ao switch, deve estar fixado na sub-rede 192.168.0.0/24. O endereço IP da interface conectada ao Switch deve ser configurada como: 192.168.0.X, sendo que X pode ser qualquer valor de 2 a 254 e máscara de rede deve ser igual a 255.255.255.0.

Após digitado o endereço IP do switch no navegador, será exibida a tela de login, conforme imagem a seguir. No padrão de fábrica o usuário e a senha para login de acesso do Switch será admin, ambos em letras minúsculas. Para acessar a interface digite usuário e senha, marque o checkbox concordando com os Termos de Uso e com as Políticas de Privacidade. Em seguida, clique no botão Login ou pressione a tecla Enter.



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 no login tempo limite . Como alternativa, você pode clicar diretamente no nome do usuário no canto superior direito e, em seguida, clicar em Sair para sair da página da interface do usuário da Web.

Introdução à Interface de Usuário Web

layout da web

A página da interface do usuário da Web pode ser dividida em quatro partes: barra de navegação de nível 1, barra de navegação de nível 2, área da página da guia e área de configuração.

Status da porta



Taxa de utilização

Hora do sistema

2023-05-23 11:04:17

Uptime

14d 20hora 55min 23s



Informação do dispositivo

Nome do dispositivo: S3028G-B Lite
Localização do dispositivo: Brazil
Versão do firmware: 65.10.25.2
Versão do Hardware: V1.0
Endereço MAC: D8:38:0D:26:93:7C
Endereço IP de gerenciamento: 40.40.40.40
Máscara de sub-rede: 255.255.255.0
Gateway: 10.100.26.1
DNS primário: --
DNS secundário: --

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

Botões comuns

Botões comuns

Ícones 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 página 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.

Basico

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.

The screenshot displays the Intelbras S2050G-A switch management interface. The top navigation bar includes the Intelbras logo, the device model 'S2050G-A', and user controls for 'Salvar' and 'admin'. The left sidebar lists various configuration categories: Config. Básica, Resumo do sistema (highlighted), Porta, VLAN, Manutenção, Diagnóstico, Switching, Roteamento, Política de QoS, Segurança de rede, Config. do dispositivo, and Visualização. Below the sidebar, the 'Resumo do sistema' section is divided into three main areas: 1. 'Status da porta': A grid of 50 port status icons arranged in two rows of 25. A legend indicates: Green for 'Conexão de Rede', Yellow for 'Porta SFP', Red for 'Desativado', and Grey for 'Desconectado'. 2. 'Taxa de utilização': Two circular gauges showing '3% CPU' and '33% Memória'. It also displays 'Hora do sistema: 2021-06-21 00:28:47' and 'Uptime: 28min 49s'. 3. 'Informação do dispositivo': A list of device details including name, location, firmware version, hardware version, MAC address, management IP, subnet mask, gateway, and DNS settings.

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.
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

Porta	Status da porta	Velocidade/Duplex	Isolamento de Porta	Limite de entrada	Limite de saída	Fluxo de entrada	Fluxo de saída	Operação
1	Conectado	Auto-negociação 1000M/FDX	Desativar	Desativar	Desativar	0.3MB	3.0MB	
2	Desconectado	Auto-negociação 1000M/FDX	Desativar	Desativar	Desativar	0MB	0MB	
3	Desconectado	Auto-negociação 1000M/FDX	Desativar	Desativar	Desativar	0MB	0MB	
4	Desconectado	Auto-negociação 1000M/FDX	Desativar	Desativar	Desativar	0MB	0MB	
5	Desconectado	Auto-negociação 1000M/FDX	Desativar	Desativar	Desativar	0MB	0MB	
6	Desconectado	Auto-negociação 1000M/FDX	Desativar	Desativar	Desativar	0MB	0MB	
7	Desconectado	Auto-negociação 1000M/FDX	Desativar	Desativar	Desativar	0MB	0MB	
8	Desconectado	Auto-negociação 1000M/FDX	Desativar	Desativar	Desativar	0MB	0MB	
9	Desconectado	Auto-negociação 1000M/FDX	Desativar	Desativar	Desativar	0MB	0MB	
10	Desconectado	Auto-negociação 1000M/FDX	Desativar	Desativar	Desativar	0MB	0MB	

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)	<p>Especifica a velocidade de negociação e o modo duplex da porta.</p> <p>Auto-negociação : A porta negocia automaticamente a velocidade e o modo duplex com o dispositivo par.</p> <p>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.</p> <p>HDX : Modo meio duplex.</p> <p>FDX : Modo full duplex.</p> <p>Auto : A porta pode ajustar automaticamente o modo duplex.</p>
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.
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.

Nome	Descrição
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

Básico	Espelhamento de portas	Agregação de portas	Limite de taxa da porta	Estatísticas de pacote	?	
					+ Adicionar	
<input type="checkbox"/>	ID	Tipo de grupo de espelhamento	Porta de origem	Porta de destino	Direção	Operação
Sem dados						

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.

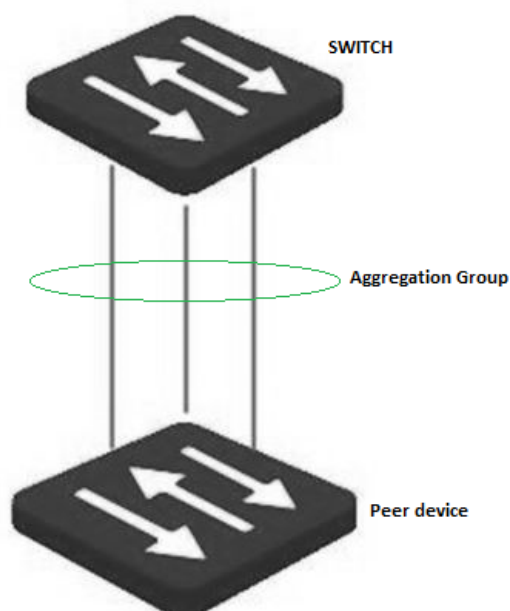
Nome	Descrição
	<ul style="list-style-type: none">• Ele especifica o tipo de pacote.• Ingress : Os pacotes recebidos pelas portas de origem serão copiados para a porta de destino.
Direção	<ul style="list-style-type: none">• Egress : Os pacotes transmitidos pelas portas de origem serão copiados para a porta de destino.• Bidirecional : Os pacotes transmitidos e recebidos pelas portas de origem serão copiados para a porta de destino.

Agregação de porta

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.

Algoritmo src-dst-mac [+ Adicionar](#)

de

Agregação

<input type="checkbox"/>	Grupo de agregação	Modo de agregação	Algoritmo de Agregação	Porta membro	Operação
--------------------------	--------------------	-------------------	------------------------	--------------	----------

Sem dados

Descrição do parâmetro

Nome	Descrição
Grupo de agregação	<p>Ele especifica o ID da porta.</p> <ul style="list-style-type: none"> 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	<p>Existem dois modos de agregação: Estático Agregação e Agregação Dinâmica.</p> <ul style="list-style-type: none"> Agregação estática : todas as portas membros no grupo de agregação convergem para uma porta lógica. Agregação Dinâmica : LACP (Link Aggregation Control Protocol) para todos
Porta Membro	<p>Ele especifica os membros de um grupo de agregação.</p> <ul style="list-style-type: none"> 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 <p>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.</p>
Algoritmo	<p>Ele especifica os algoritmos de roteamento para o grupo de agregação:</p> <ul style="list-style-type: none"> 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.

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.

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.

Básico	Espelhamento de portas	Agregação de portas	Limite de taxa da porta	Estatísticas de pacote	
--------	------------------------	---------------------	--------------------------------	------------------------	--

[?](#) [Editar](#)

Porta	Taxa de saída (Mbps)	Pacote de broadcast	Pacote Multicast	Unicast desconhecido	Valor de supressão	Operação
1	--	Desativar	Desativar	Desativar	100	✎
2	--	Desativar	Desativar	Desativar	100	✎
3	--	Desativar	Desativar	Desativar	100	✎
4	--	Desativar	Desativar	Desativar	100	✎
5	--	Desativar	Desativar	Desativar	100	✎
6	--	Desativar	Desativar	Desativar	100	✎
7	--	Desativar	Desativar	Desativar	100	✎
8	--	Desativar	Desativar	Desativar	100	✎
9	--	Desativar	Desativar	Desativar	100	✎
10	--	Desativar	Desativar	Desativar	100	✎

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.
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 pacote

Clique em **Basico > Porta > Estatísticas de pacote** para entrar na página. Nesta página, você pode visualizar e excluir as estatísticas de pacotes recebidos e enviados por cada porta.

Básico Espelhamento de portas Agregação de portas Limite de taxa da porta **Estatísticas de pacote** ?

[Limpar](#) [Atualizar](#)

Porta	Pacotes Transmitidos	Bytes transmitidos	Pacotes recebidos	Bytes Recebidos	Operação
1	4157	3437423	2967	414749	
2	0	0	0	0	
3	0	0	0	0	
4	0	0	0	0	
5	0	0	0	0	
6	0	0	0	0	
7	0	0	0	0	
8	0	0	0	0	
9	0	0	0	0	
10	0	0	0	0	

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.
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.

Porta	1
Estatísticas Recebidas	
Total de Bytes	414749
Pacotes de Broadcast	25
Pacotes Unicast	2755
Pacotes com erro	0
Pacotes Descartados	210
Estatísticas de Transmissão	
Total de Bytes	3437423
Pacotes de Broadcast	1
Pacotes Unicast	4156
Pacotes com erro	0
Pacotes Descartados	0

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.

Configuração de VLAN

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 e o endereço IP de 192.168.0.1. Esta regra não pode ser excluída.

Clique em **Basico > VLAN > 802.1Q VLAN** para entrar na página. sobre isso página , você pode configurar as regras da VLAN 802.1Q.

+ Adicionar



<input type="checkbox"/>	VLAN ID	Descrição da VLAN	Endereço IPv4	Máscara de sub-rede	Operação
<input type="checkbox"/>	1	default	40.40.40.40	255.255.255.0	
<input type="checkbox"/>	2	VLAN0002	--	--	
<input type="checkbox"/>	3	VLAN0003	--	--	
<input type="checkbox"/>	4	VLAN0004	--	--	
<input type="checkbox"/>	5	VLAN0005	--	--	
<input type="checkbox"/>	6	VLAN0006	--	--	
<input type="checkbox"/>	7	VLAN0007	--	--	
<input type="checkbox"/>	8	VLAN0008	--	--	
<input type="checkbox"/>	9	VLAN0009	--	--	
<input type="checkbox"/>	10	teste_MSTP_DUT1	--	--	

10 /página

Página 1/410 Um total de 4094 itens na página

Descrição do parâmetro

Nome	Descrição
ID da VLAN	Especifica o VLAN ID, utilizado para identificar a VLAN a qual o pacote pertence.
Especifica o VLAN ID, utilizado para identificar a VLAN a qual o pacote pertence.	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.
Interface Virtual L3	Após habilitar a interface virtual L3, você pode configurar o endereço IP e a máscara de sub-rede para a interface VLAN. Depois que as informações do endereço IP são configuradas, a comunicação entre as VLANs pode ser realizada por meio de rotas estáticas.
Tipo de obtenção de IP	Ele especifica o tipo que a interface VLAN emprega para obter um endereço IP. <ul style="list-style-type: none"> 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.
Endereço IPv4	O endereço IP da interface VLAN pode ser configurado somente quando a Interface Virtual L3 estiver habilitada. Os dispositivos conectados às portas no grupo VLAN podem usar esse endereço IP para fazer login na interface do usuário da Web do switch.
Máscara de sub-rede	Especifica a máscara de sub-rede da interface VLAN.

Configurar membros da porta

Clique em **Basico > VLAN > Membro da Porta** para entrar na página. sobre isso page , você pode configurar as políticas de tratamento PVID e Tag de cada porta para realizar o isolamento de VLAN.

802.1Q VLAN		Membro da Porta				?
Porta	Tipo de link	PVID	Tagged	Untagged	Operação	
1	Trunk	100	--	100		
2	Trunk	100	--	100		
3	Trunk	100	--	100		
4	Trunk	100	--	100		
5	Trunk	100	--	100		
6	Trunk	100	--	100		
7	Trunk	100	--	100		
8	Trunk	100	--	100		
9	Access	1	--	1		
10	Access	100	--	100		

Um total de 29 itens na página

Descrição do parâmetro

Nome	Descrição
Porta	Ele especifica o ID da porta.
Tipo de link	<p>Três tipos de link de VLAN são suportados: Access , Trunk e Hybrid.</p> <ul style="list-style-type: none">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.

Configuração de VLAN 802.1Q

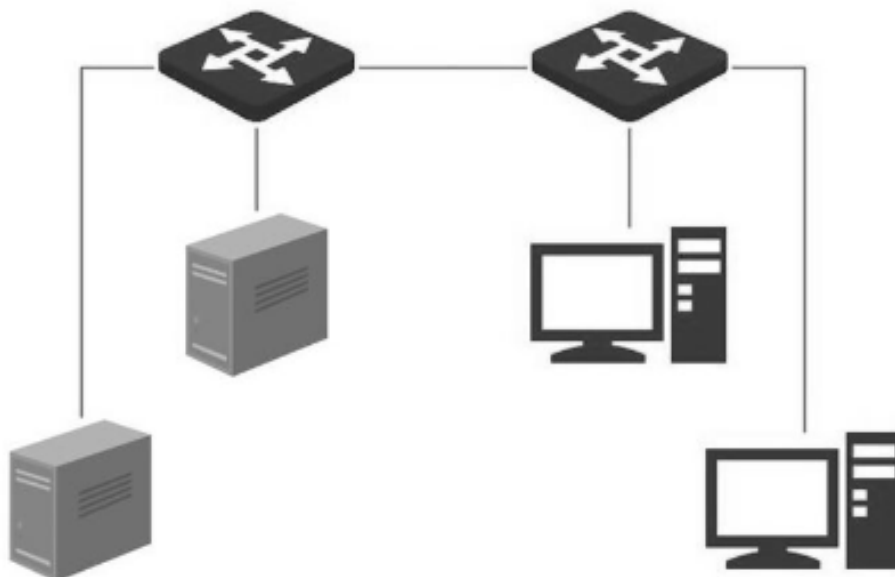
Requisito de rede

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 Interruptor A

1. Adicione VLANs

(1) Faça login na interface do usuário da Web do Switch A e clique em Basics > VLAN > 802.1Q VLAN

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

+ Adicionar



<input type="checkbox"/>	VLAN ID	Descrição da VLAN	Endereço IPv4	Máscara de sub-rede	Operação
<input type="checkbox"/>	1	default	40.40.40.40	255.255.255.0	
<input type="checkbox"/>	2	VLAN0002	--	--	
<input type="checkbox"/>	3	VLAN0003	--	--	
<input type="checkbox"/>	4	VLAN0004	--	--	
<input type="checkbox"/>	5	VLAN0005	--	--	
<input type="checkbox"/>	6	VLAN0006	--	--	
<input type="checkbox"/>	7	VLAN0007	--	--	
<input type="checkbox"/>	8	VLAN0008	--	--	
<input type="checkbox"/>	9	VLAN0009	--	--	
<input type="checkbox"/>	10	teste_MSTP_DUT1	--	--	

10 /página

Página 1/410 Um total de 4094 itens na página

2. Configurando atributo de porta

(1) Clique em Princípios Básicos > VLAN > Membro da porta.

(2) Clique no botão atrás da porta 5 e defina PVID como 5.

(3) Clique no botão atrás da porta 7 e defina PVID como 7.

(4) Clique no botão atrás da porta 1 para definir Link Type como Trunk e Tagged como 5, 7.

Porta	Tipo de link	PVID	Tagged	Untagged	Operação
1	Trunk	100	--	100	
2	Trunk	100	--	100	
3	Trunk	100	--	100	
4	Trunk	100	--	100	
5	Trunk	100	--	100	
6	Trunk	100	--	100	
7	Trunk	100	--	100	
8	Trunk	100	--	100	
9	Access	1	--	1	
10	Access	100	--	100	

Um total de 29 itens na página

II. Configurando o Interruptor 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.

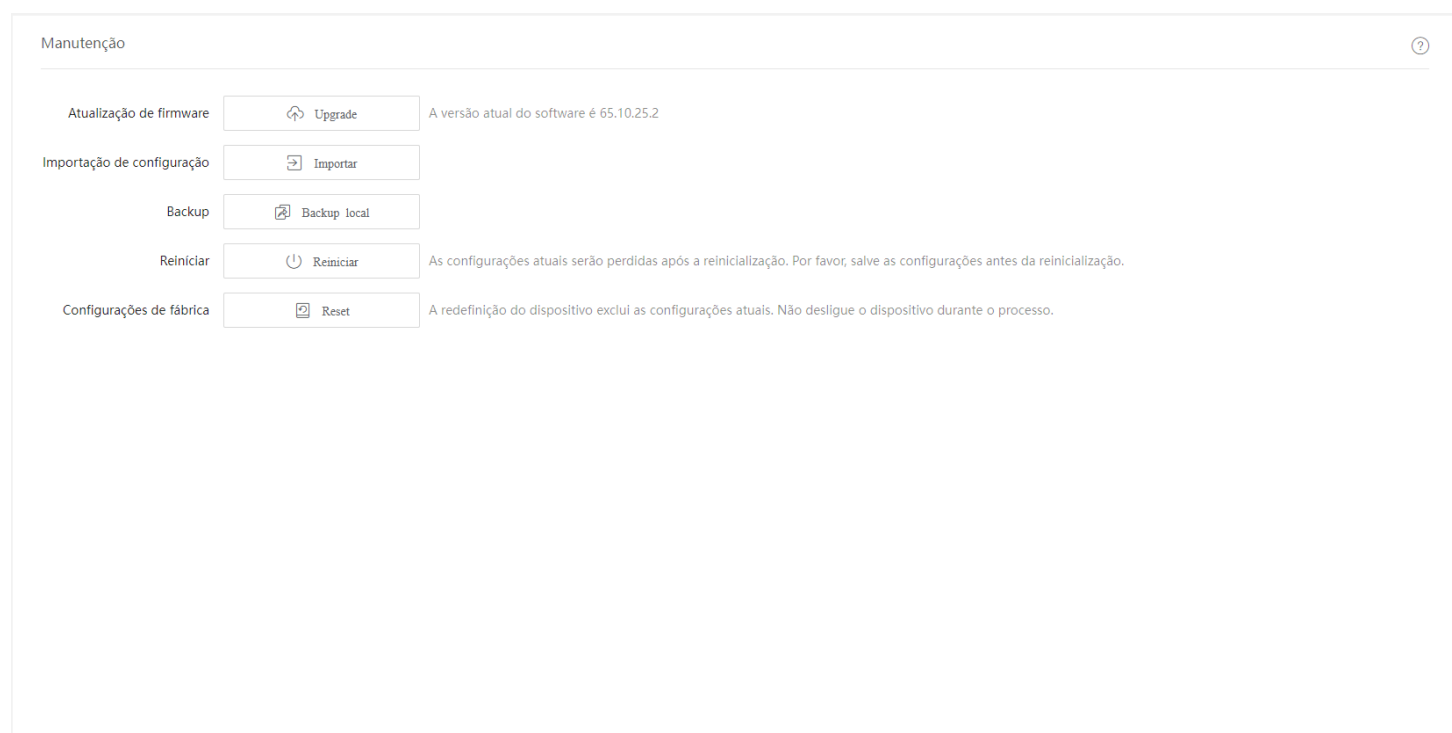
Manutenção

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.

- Antes de atualizar, baixe o firmware mais recente do switch no site oficial: www.intelbras.com.br. Geralmente, a extensão do arquivo de atualização é .bin.
- Durante o processo de atualização, garanta uma fonte de alimentação estável para o switch.



Manutenção

Atualização de firmware A versão atual do software é 65.10.25.2

Importação de configuração

Backup

Reiniciar As configurações atuais serão perdidas após a reinicialização. Por favor, salve as configurações antes da reinicialização.






Configurações de fábrica A redefinição do dispositivo exclui as configurações atuais. Não desligue o dispositivo durante o processo.

Importação de 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.

Manutenção

Atualização de firmware	 Upgrade	A versão atual do software é 65.10.25.2
Importação de configuração	 Importar	
Backup	 Backup local	
Reiniciar	 Reiniciar	As configurações atuais serão perdidas após a reinicialização. Por favor, salve as configurações antes da reinicialização.
Configurações de fábrica	 Reset	A redefinição do dispositivo exclui as configurações atuais. Não desligue o dispositivo durante o processo.

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 de nuvem IMS.

Para salvar as configurações do switch no computador local, clique em Local Backup ; para a plataforma de nuvem IMS, clique em Cloud Backup

- Clique em Salvar no canto superior direito de o página para salvar todas as configurações antes do backup.
- Somente quando o comutador é gerenciado pela plataforma de nuvem IMS é que as configurações podem ser copiadas para a plataforma de nuvem IMS.

Manutenção

Atualização de firmware	 Upgrade	A versão atual do software é 65.10.25.2
Importação de configuração	 Importar	
Backup	 Backup local	
Reiniciar	 Reiniciar	As configurações atuais serão perdidas após a reinicialização. Por favor, salve as configurações antes da reinicialização.
Configurações de fábrica	 Reset	A redefinição do dispositivo exclui as configurações atuais. Não desligue o dispositivo durante o processo.






Reiniciar

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.

Clique em Salvar no canto superior direito para salvar todas as configurações antes de reiniciar o switch.

Manutenção

Atualização de firmware	 Upgrade	A versão atual do software é 65.10.25.2
Importação de configuração	 Importar	
Backup	 Backup local	
Reiniciar	 Reiniciar	As configurações atuais serão perdidas após a reinicialização. Por favor, salve as configurações antes da reinicialização.
Configurações de fábrica	 Reset	A redefinição do dispositivo exclui as configurações atuais. Não desligue o dispositivo durante o processo.

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 . redefinir e hardware _ redefinir .

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.

Durante o processo de reinicialização, certifique-se de que a fonte de alimentação do switch esteja estável.

Manutenção

Atualização de firmware	 Upgrade	A versão atual do software é 65.10.25.2
Importação de configuração	 Importar	
Backup	 Backup local	
Reiniciar	 Reiniciar	As configurações atuais serão perdidas após a reinicialização. Por favor, salve as configurações antes da reinicialização.
Configurações de fábrica	 Reset	A redefinição do dispositivo exclui as configurações atuais. Não desligue o dispositivo durante o processo.

Redefinição de hardware

Quando o indicador LED SYS estiver piscando, mantenha pressionado o botão de reinicialização (Reset, Modo LED ou LED/RESET) por cerca de 10 segundos 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.

Switching

DHCP relay

O modelo básico de rede do DHCP requer o cliente e o servidor na mesma LAN. Em uma rede com múltiplas VLANs, é necessário configurar um servidor DHCP para cada VLAN, o que é de alto custo.

Com a função DHCP Relay ativada, o switch pode fornecer serviço de retransmissão para o servidor DHCP e clientes DHCP em diferentes segmentos de rede e encaminhar mensagens do protocolo DHCP em várias VLANs, permitindo que clientes DHCP em várias VLANs compartilhem um servidor DHCP.

- Quando o relé DHCP recebe as mensagens de descoberta DHCP ou solicitação DHCP enviadas por clientes DHCP em broadcast, ele preenche o endereço IP do relé DHCP com o campo giaddr na mensagem e encaminha a mensagem para o servidor DHCP especificado em unicast de acordo com a configuração.
- O servidor DHCP seleciona o endereço IP com o mesmo segmento de endereço no pool de endereços de acordo com o campo giaddr na mensagem e envia a mensagem de resposta com essas informações de endereço IP para a retransmissão DHCP.
- Quando a retransmissão DHCP recebe uma mensagem de resposta do servidor, a retransmissão DHCP remove o campo Option 82 no pacote e transmite a mensagem de resposta DHCP para a rede de interface do dispositivo de retransmissão.

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.

Mensagem de solicitação DHCP sem opção 82

Adicione o conteúdo padrão dessa opção às informações da Opção 82 da mensagem de solicitação DHCP e encaminhe a mensagem.

O conteúdo padrão deste switch inclui o ID da porta que recebe o pacote de solicitação do cliente DHCP, o endereço MAC do cliente DHCP e sua VLAN.

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.

Clique em Switching > DHCP Relay para entrar na página . sobre isso página , você pode configurar as regras de DHCP Relay.

DHCP Relay
?

Option 82 Desativar

Política da Option 82 Substituir

Confirmar

Configuração do Relay + Adicionar 🗑

	VLAN ID	IP do servidor	Operação
<input type="checkbox"/>			

Sem dados

✔ Configuração bem-sucedida

Um total de 0 itens na página

Nome	Descrição
Opção 82	Ele é usado para habilitar ou desabilitar a política da Opção 82. A opção 82 registra as informações de localização dos clientes DHCP. A política da Opção 82 entra em vigor somente quando a Opção 82 está habilitada.
Opção 82 Política	<p>O switch suporta três políticas:</p> <ul style="list-style-type: none"> • 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. • Reter : Quando o DHCP Relay recebe mensagens de solicitação DHCP, ele retém o estado original da Opção 82 e encaminha as mensagens. • 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.
ID da VLAN	<p>Especifica a VLAN à qual os clientes pertencem.</p> <p>A VLAN já deve existir e sua interface virtual L3 está configurada</p>
IP do servidor	<p>Ele especifica o endereço IP do servidor DHCP remoto.</p> <p>O endereço IP do servidor DHCP remoto não pode pertencer ao mesmo segmento de rede da VLAN à qual os clientes pertencem</p>

DHC Snooping

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 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

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

DHCP Snooping

[Editar](#)

Porta	Propriedade da porta	Option 82	Política de opções	Operação
1	Porta não confiável	Desativar	Substituir	✎
2	Porta não confiável	Desativar	Substituir	✎
3	Porta não confiável	Desativar	Substituir	✎
4	Porta não confiável	Desativar	Substituir	✎
5	Porta não confiável	Desativar	Substituir	✎
6	Porta não confiável	Desativar	Substituir	✎
7	Porta não confiável	Desativar	Substituir	✎
8	Porta não confiável	Desativar	Substituir	✎
9	Porta não confiável	Desativar	Substituir	✎
10	Porta não confiável	Desativar	Substituir	✎

Um total de 27 itens na página

Descrição do parâmetro

Nome	Descrição
Porta	Ele especifica o ID da porta. Ele é usado para configurar a propriedade de espionagem DHCP da porta atual, incluindo porta confiável ou não confiável. <ul style="list-style-type: none">Porta confiável : Está conectada a um servidor DHCP legal e encaminha as mensagens DHCP recebidas normalmente.Porta não confiável : Depois de receber as mensagens de resposta enviadas pelo servidor DHCP, a porta descarta as mensagens, desativando assim servidores DHCP falsos erguidos em particular para atribuir endereços IP aos clientes.
Propriedade Portuária	
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. Consulte a Opção 82 por seu mecanismo de trabalho.

Nome	Descrição
Política de opções	<p>Três políticas da Opção 82 são suportadas por este switch:</p> <ul style="list-style-type: none">• 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.

Spanning 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 a diminuição da capacidade de processamento de mensagens dos dispositivos devido à proliferação contínua e circulação infinita de mensagens na rede de loop.

Mensagem de 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 BPDUs entre os dispositivos. Existem dois tipos de BPDUs do protocolo STP:

- Configuração BPDUs: É usado para cálculo de spanning tree e manutenção da topologia de spanning tree.
- TCN BPDUs (Topology Change Notification BPDUs): 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 em árvore.

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.

BPDU no modo STP

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 iguais, 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 root bridge), a porta que recebe o BPDU ideal é escolhida como porta root do switch.
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. <ul style="list-style-type: none">• 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. <ul style="list-style-type: none">• O ID da ponte designada é substituído pelo do próprio switch.• O ID da porta designada é substituído pelo próprio ID da porta.

- 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 port 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 recalculer 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 full duplex 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.

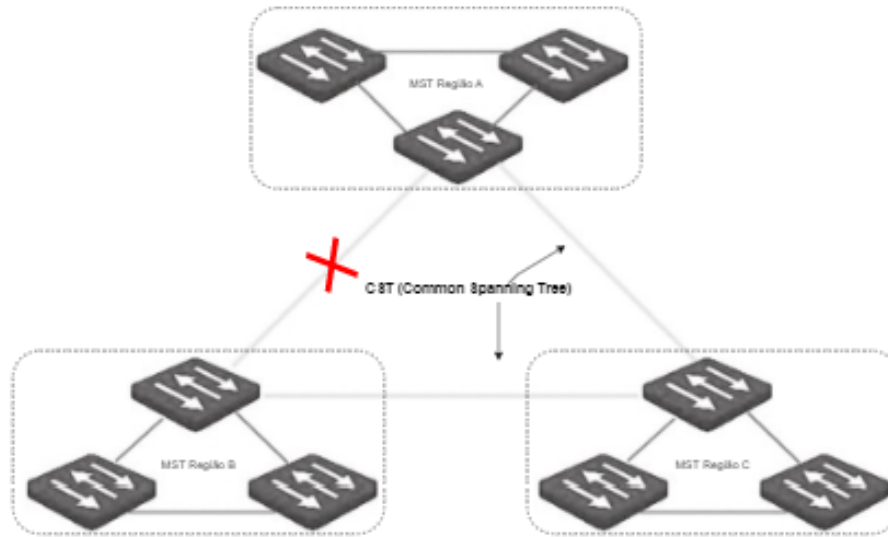
• **Regional Root**

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

• **Common Root Bridge**

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.

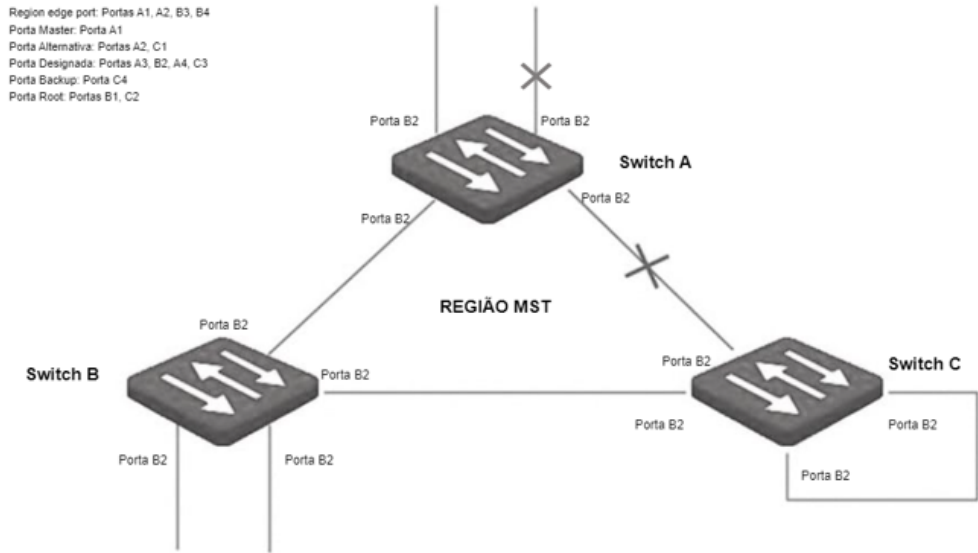
- Disabled: A porta não está conectada fisicamente.

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.

Global Configuração da porta Estatísticas da porta Informações da instância

Status

Modo

Nome	Descrição
Status	Ele é usado para habilitar ou desabilitar a função spanning tree.
Modo	<p>O switch suporta três modos spanning tree: STP, RSTP e MSTP.</p> <ul style="list-style-type: none"> • 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

Configuração da Bridge

Aging time máximo	<input type="text" value="20"/>	s (Intervalo: 6 a 40)
Hello Time	<input type="text" value="2"/>	s (Intervalo: 1 a 10)
Encaminhando Delay	<input type="text" value="15"/>	s (Intervalo: 4 a 30)
Máximo de saltos	<input type="text" value="20"/>	(Intervalo: 6 a 40)
Prioridade da Bridge	<input type="text" value="61440"/>	▼

Nota: Maximum aging time $\geq 2 \times$ (Hello Time + 1) Tempo máximo de envelhecimento $\leq 2 \times$ (Atraso de encaminhando - 1)

Descrição do parâmetro

Nome	Descrição
Tempo Máximo de Envelhecimento	<p>Especifica a duração máxima durante a qual o BPDU pode ser mantido no switch. A configuração deve atender às seguintes fórmulas:</p> <ul style="list-style-type: none">Tempo Máximo de Envelhecimento $\geq 2 \times$ (Hello Time + 1).Tempo Máximo de Envelhecimento $\leq 2 \times$ (Atraso de Encaminhamento - 1).
Alô hora	<p>Ele especifica o intervalo no qual o switch envia BPDU, que é definido como 2 segundos por padrão.</p>
Atraso de Encaminhamento	<p>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.</p>
Saltos Máximos	<p>Especifica o número máximo de BPDU que pode ser encaminhado, usado para limitar a escala da spanning tree.</p>
Ponte Prioridade	<p>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.</p>

Configuração da Região MSTP

Configuração da região MSTP

Nome da região (Intervalo: 1 a 32 caracteres)

Revisão (Intervalo: 0 a 65535)

Resumo da configuração (Digest) 0x9357EBB7A8D74DD5FEF4F2BAB50531AA

[Confirmar](#)

Nome	Descrição
Nome da região	Ele especifica a identidade da região MST. O valor padrão é o endereço MAC do switch.

Nome	Descrição
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.

MSTP Domain Setting

Instância MSTP

+ Adicionar



ID da instância	Lista de mapeamento de VLAN	Prioridade da Bridge	Operação
<input type="checkbox"/> 0	1-9,11-19,21-4094	61440	

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 designada

Root Bridge designada

ID da Bridge 61440:d838.0d26.937d

ID do Root Bridge 16384:e4f0.0473.8988

ID do root da região 61440:30c6.d73f.70c8

Porta Root po33

Custo do caminho para o root 20003

Custo do caminho do root interno 3000

Status da topologia Topological_stability

Hora da última alteração 2023-05-17 12:03:40

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.
Status da topologia	<p>Ele especifica o status da topologia da spanning tree deste switch.</p> <ul style="list-style-type: none"> 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.

Nome	Descrição
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 de porta

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	Status do STP	Porta Edge	Porta P2P	Operação
1	Habilitar	Desativar	Auto	
2	Habilitar	Desativar	Auto	
3	Habilitar	Desativar	Auto	
4	Habilitar	Desativar	Auto	
5	Habilitar	Desativar	Auto	
6	Habilitar	Desativar	Auto	
7	Habilitar	Desativar	Auto	
8	Habilitar	Desativar	Auto	
9	Habilitar	Desativar	Auto	
10	Habilitar	Desativar	Auto	

Um total de 27 itens na página

Descrição do parâmetro

Nome	Descrição
Porta	Especifica o ID da porta.
Status STP	Indica se a função STP está habilitada ou desabilitada.
Porta de Borda (Edge Port)	A porta de borda pode migrar rapidamente para o estado de encaminhamento a partir do estado de congestão. Não é necessário esperar pelo tempo de atraso. A porta de borda geralmente está conectada a terminais. Ao receber mensagens BPDU, a porta de borda é alterada para uma porta não de borda. Todas as portas são portas de borda por padrão.
Desabilitado	Esta porta não é uma porta de borda.
Habilitado	Esta porta é uma porta de borda.
Porta P2P	Uma porta ponto a ponto (P2P) pode realizar migração rápida. No modo RSTP/MSTP, todas as portas em modo full-duplex são consideradas portas P2P. A porta padrão identifica automaticamente links.

Nome	Descrição
Automático	A porta P2P pode ser identificada automaticamente.
Habilitado	Esta porta é uma porta P2P.
Desabilitado	Esta porta não é uma porta P2P.

Estatísticas de Porta

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

Porta	Transmitido				Recebido				Descartar	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Desconhecido	Illegal
1	0	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	23	0	0	2	4	0	0	3	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

Um total de 27 itens na página

Descrição do parâmetro

Nome	Descrição
Porta	Especifica o ID da porta.
MSTP	Especifica o número de BPDU de configuração com informações MSTP transmitidas ou recebidas pela porta.
RSTP	Especifica o número de BPDU de configuração com informações RSTP transmitidas ou recebidas pela porta.
STP	Especifica o número de BPDU de configuração com informações STP transmitidas ou recebidas pela porta.
TCN	Especifica o número de mensagens BPDU TCN transmitidas ou recebidas pela porta.
Desconhecido (Unknown)	Especifica o número de pacotes STP desconhecidos descartados.
Inválido (Illegal)	Especifica o número de pacotes STP inválidos 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.

ID da instância

[Editar](#) [Atualizar](#)

Porta	Função da porta	Status da porta	ID do root da região	Bridge Designada	Porta Designada	Prioridade	Custo do caminho	Operação
1	Desabilitada	Desabilitada	61440-30c6.d73f70c8	61440-d838.0d26.937d	1	128	20000	✎
2	Desabilitada	Desabilitada	61440-30c6.d73f70c8	61440-d838.0d26.937d	2	128	20000	✎
3	Desabilitada	Desabilitada	61440-30c6.d73f70c8	61440-d838.0d26.937d	3	128	20000	✎
4	Desabilitada	Desabilitada	61440-30c6.d73f70c8	61440-d838.0d26.937d	4	128	20000	✎
5	Desabilitada	Desabilitada	61440-30c6.d73f70c8	61440-d838.0d26.937d	5	128	20000	✎
6	Desabilitada	Desabilitada	61440-30c6.d73f70c8	61440-d838.0d26.937d	6	128	20000	✎
7	Desabilitada	Desabilitada	61440-30c6.d73f70c8	61440-d838.0d26.937d	7	128	20000	✎
8	Desabilitada	Desabilitada	61440-30c6.d73f70c8	61440-d838.0d26.937d	8	128	20000	✎
9	Desabilitada	Desabilitada	61440-30c6.d73f70c8	61440-d838.0d26.937d	9	128	20000	✎
10	Desabilitada	Desabilitada	61440-30c6.d73f70c8	61440-d838.0d26.937d	10	128	20000	✎

Um total de 27 itens na página

Descrição do parâmetro

Nome	Descrição
ID da Instância	É usado para selecionar o ID da instância para verificar as informações de estado STP da instância.
Porta	Especifica o ID da porta.
Função da Porta	Especifica o papel que a porta desempenha na instância da árvore de expansão. Para mais detalhes, consulte o papel da porta.
Status da Porta	Especifica o status operacional atual da porta. Para mais detalhes, consulte o status da porta.
ID da Raiz da Região	Especifica a prioridade da ponte e o endereço MAC da ponte da raiz regional.
Ponte Designada	Especifica o ID da ponte do switch que se conecta a este switch e é usado para encaminhar mensagens BPDU para o switch.
Ponta Designada	Especifica a porta para a qual a ponte designada encaminha mensagens BPDU.
Prioridade	Especifica a prioridade da porta no cálculo da árvore de expansão. Quando o ID da ponte raiz, o custo do caminho da raiz e o ID da ponte são os mesmos, a prioridade é um critério importante para determinar se a porta é 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 dos caminhos na instância dentro da região 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 encapsule-as 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 reiniciada. 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. sobre isso page, você pode configurar os parâmetros globais do LLDP.

Função LLDP

Global Configuração da porta Informações do vizinho

Intervalo de transmissão s (Faixa: 5 a 3600)

Multiplicador TTL s (Intervalo: 2 a 10)

Atraso de inicialização s (Intervalo: 1 a 10)

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. $TTL = \text{Min}(65535, \text{multiplicador TTL} \times \text{intervalo de envio LLDPDU})$, indicando o valor mínimo entre 65535 e o multiplicador TTL \times 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 de 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.

Porta	Status Operacional do LLDP	Operação
1	Enviar & recebido	
2	Enviar & recebido	
3	Enviar & recebido	
4	Enviar & recebido	
5	Enviar & recebido	
6	Enviar & recebido	
7	Enviar & recebido	
8	Enviar & recebido	
9	Enviar & recebido	
10	Enviar & recebido	

Um total de 28 itens na página

Descrição do parâmetro

Nome	Descrição
Porta	Ele especifica o ID da porta.
Operação LLDP Estado (Porta Propriedade)	<p>Indica o status operacional LLDP de cada porta.</p> <ul style="list-style-type: none">• 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.

Informações do vizinho

Clique em **Switching > Informações do vizinho** para entrar na página. Nesta página, você pode visualizar as informações do vizinho.

Função LLDP

Global Configuração da porta **Informações do vizinho**

Porta	Nome do sistema	ID da porta	ID do vizinho	IP de gerenciamento	Operação
28	HUAWEI	XGigabitEthernet0/0/2	14AB.020D.1580	15.15.15.15	

Um total de 1 itens na página

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.

IGMP snooping

Visao 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.

Global

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

IGMP Snooping

Global Fast Leave

VLAN ID: 1

VLAN: Habilitar

Status da VLAN Multicast: Desativar

Versão do protocolo: v3

Aging time da porta de roteamento: 260 s (Intervalo: 1 a 1000)

Tempo de resposta à Query: 10 s (Intervalo: 1 a 25)

Tempo de resposta de Query específica: 2 s (Intervalo: 1 a 5)

Aging time da porta do host: 260 s (Faixa: 200 a 1000)

Descartar Multicast: Desativar

Confirmar

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.
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: <ul style="list-style-type: none">v1 : Processa apenas mensagens de IGMPv1v2 : processa apenas mensagens de IGMPv1 e IGMPv2.v3 : processa mensagens de IGMPv1, IGMPv2 e IGMPv3.

Nome	Descrição
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 .
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.

Sáida rápida

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

The screenshot shows the IGMP Snooping configuration interface. At the top, 'IGMP Snooping' is enabled with a green toggle. Below it, 'Global' is selected, and 'Fast Leave' is highlighted in green. A table lists 10 ports, each with a 'Fast Leave' status set to 'Desativar' and an 'Operação' column containing an edit icon. In the top right corner, there are 'Editar' and 'Recarregar' buttons. At the bottom right, it says 'Um total de 27 itens na página'.

Porta	Fast Leave	Operação
1	Desativar	
2	Desativar	
3	Desativar	
4	Desativar	
5	Desativar	
6	Desativar	
7	Desativar	
8	Desativar	
9	Desativar	
10	Desativar	

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.



Configuração 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.
- **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. sobre isso page , você pode visualizar e excluir as entradas da tabela de endereços MAC.

Aging Time 300s Endereço MAC/Tipo/Porta 

<input type="checkbox"/>	Endereço MAC	Tipo	VLAN	Porta	Operação
<input type="checkbox"/>	f223-60ac-ce8e	Dinâmico	100	AGG33	
<input type="checkbox"/>	00e0-fc09-bcf9	Dinâmico	100	AGG33	
<input type="checkbox"/>	bcd0-ebfd-58fb	Dinâmico	100	AGG33	
<input type="checkbox"/>	ea12-c899-c081	Dinâmico	100	AGG33	
<input type="checkbox"/>	e2a7-42c8-c110	Dinâmico	100	AGG33	
<input type="checkbox"/>	00e0-4c68-0516	Dinâmico	100	AGG33	
<input type="checkbox"/>	0009-0f09-1e0a	Dinâmico	100	AGG33	
<input type="checkbox"/>	30c6-d73f-70f0	Dinâmico	30	AGG33	
<input type="checkbox"/>	30c6-d73f-70d6	Dinâmico	100	AGG33	
<input type="checkbox"/>	2601-8374-e6f7	Dinâmico	100	AGG33	

10 / página

Página 1/5 Um total de 43 itens na página 

Descrição do parâmetro

Nome	Descrição
Tempo de envelhecimento	<p>Ele especifica o tempo de vencimento das entradas na tabela de endereços MAC, que é efetivo apenas para entradas dinâmicas.</p> <p>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.</p>
Endereço MAC	Endereço MAC, formato: XXXX-XXXX-XXXX.
Tipo	<p>Ele especifica o tipo do endereço MAC.</p> <ul style="list-style-type: none"> 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. sobre isso page , você pode configurar a tabela de endereço MAC estático. A configuração existe como entradas estáticas na tabela de endereços MAC, além do controle do tempo de vencimento do MAC.

Tabela de endereços MAC **Endereço MAC estático** ?

[+ Adicionar](#)

<input type="checkbox"/>	VLAN ID	Endereço MAC	Porta	Operação
Sem dados				

Um total de 0 itens na página

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.

Roteamento

O roteamento refere-se a um processo em que um dispositivo de roteamento seleciona um caminho ideal para um pacote recebido de acordo com seu endereço de destino e o encaminha para o próximo nó da rede. O último nó de roteamento neste caminho encaminha o pacote para o host de destino.

O dispositivo de roteamento mantém uma tabela de roteamento que contém as informações do caminho da rede e seleciona um caminho ideal para encaminhar os dados de acordo com o protocolo de roteamento (como RIP e OSPF) suportado pelo dispositivo de roteamento .

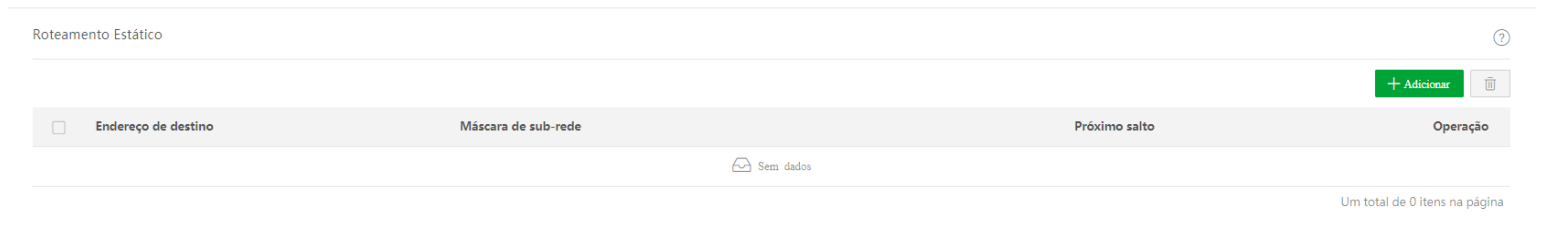
A tabela de roteamento inclui principalmente três tipos de rotas.

- **Rota direta:** Uma rota direta é descoberta pelo protocolo da camada de enlace de dados , geralmente uma rota entre o dispositivo de roteamento e sua rede conectada diretamente.
- **Rota estática:** Uma rota estática é configurada manualmente pelo administrador da rede e não mudará nem mesmo as mudanças na topologia da rede.
- **Rota dinâmica:** Uma rota dinâmica é calculada por um protocolo de roteamento depois que o dispositivo de roteamento troca informações de roteamento com seus dispositivos vizinhos. As rotas dinâmicas podem mudar automaticamente quando a topologia da rede muda.

Roteamento Estático

Rota estática é a rota fixa configurada manualmente pelo administrador, geralmente utilizada em uma rede de pequeno a médio porte com topologia estável. A rota estática é eficiente, confiável e fácil de configurar e pode melhorar a velocidade de encaminhamento dos pacotes. Mas a rota estática não pode mudar automaticamente com a topologia da rede. Portanto, quando a rede apresenta mau funcionamento ou a topologia da rede é alterada, o administrador precisa modificar manualmente a configuração de roteamento estático.

Clique em Roteamento > Roteamento Estático para entrar na página. sobre isso page , você pode visualizar e configurar as regras de roteamento estático.



Descrição do parâmetro

Nome	Descrição
Endereço de destino	Ele especifica o segmento de rede da rede de destino.
Máscara de sub-rede	Especifica a máscara de sub-rede da rede de destino.
Próximo salto	Ele especifica o endereço IP de entrada da rota do próximo salto após a saída dos pacotes do switch.

Roteamento dinâmico

Visão geral

O switch suporta RIP (Protocolo de Informação de Roteamento) e OSPF (Open Shortest Path First). O RIP é um IGP (Interior Gateway Protocol), geralmente usado para redes de pequeno a médio porte, como rede escolar. Comparado com o OSPF, o RIP é mais fácil de gerenciar e manter.

Operação RIP

R IP define dois tipos de mensagens:

- R equest message: Refere-se a mensagens que solicitam parte ou toda a informação da tabela de roteamento dos dispositivos de roteamento vizinhos.
- Mensagem de resposta: Refere-se a mensagens que respondem às solicitações dos dispositivos de roteamento vizinhos ou são enviadas periodicamente aos dispositivos de roteamento vizinhos com informações atualizadas.

No estágio de inicialização, a tabela de roteamento RIP contém apenas informações de rotas conectadas diretamente. O dispositivo de roteamento deve trocar e aprender tabelas de roteamento com seus dispositivos de roteamento vizinhos e, em seguida, atualizar sua tabela de roteamento RIP.

O procedimento é o seguinte:

1. No estágio de inicialização do RIP, o switch envia mensagens de solicitação de cada interface com a função RIP habilitada, que contém todas as informações da tabela de roteamento do switch.
2. Após receber esta mensagem de requisição, o dispositivo de roteamento vizinho envia uma mensagem de resposta com as informações de sua tabela de roteamento para a central .
3. Depois de receber esta mensagem de resposta, o switch atualiza sua tabela de roteamento e envia mensagens de atualização (resposta) para seus dispositivos vizinhos. Os dispositivos de roteamento vizinhos atualizarão suas informações da tabela de roteamento e enviarão mensagens de atualização para seus dispositivos de roteamento vizinhos.

Após a conclusão da troca de informações da tabela de roteamento, o switch gera sua tabela de roteamento RIP final. E todos os dispositivos de roteamento mantêm as informações de roteamento mais recentes. Depois disso, este switch enviará mensagens de atualização periodicamente e envelhecerá as rotas de acordo com o mecanismo de envelhecimento, garantindo a validade da tabela de roteamento.

Versão do IP R

RIP tem duas versões: RIPv1 e RIPv2.

RIPv1 é um protocolo de roteamento classful, que suporta apenas o envio de mensagens de protocolo por meio de broadcast. As mensagens de protocolo do RIPv1 não podem transportar informações de máscara e podem apenas identificar as rotas de redes naturais, como Classes A, B e C, portanto, o RIP v 1 não oferece suporte a sub-redes descontínuas.

Compatível com versões anteriores do RIPv1, o RIPv2 é um protocolo de roteamento sem classe. Comparado com o RIPv1, o RIPv2 tem as seguintes vantagens:

- Oferece suporte a tags de roteamento, que podem ser usadas para controlar rotas com flexibilidade em políticas de roteamento.
- Transporta informações de máscara e oferece suporte a resumo e CIDR (roteamento entre domínios sem classe).

- Oferece suporte ao próximo salto designado para selecionar o próximo salto ideal na rede de transmissão.
- Oferece suporte ao envio de mensagens de atualização multicast, o que pode reduzir o consumo de recursos.
- Suporta mensagens de protocolo de autenticação por Simple e MD5, que podem verificar a validade da origem da mensagem de atualização e aumentar a segurança.

RIP Roteamento Dinâmico

Clique em Roteamento > Roteamento Dinâmico para entrar na página. Nesta página, você pode visualizar e configurar as regras de roteamento dinâmico RIP.

RIP Roteamento Dinâmico ?

Importar Rotas Rota Direta Rota Estática OSPF

OK

Segmento de rede RIP + Adicionar 🗑️

<input type="checkbox"/>	Segmento de rede	Máscara de sub-rede	Operação
	Sem dados		

Um total de 0 itens na página

Configurações da interface + Adicionar 🗑️

<input type="checkbox"/>	Interface VLAN	Mensagem Tx	Mensagem Rx	Modo de autenticação	ID da chave	Senha	Status do RIP na Interface	Operação
<input type="checkbox"/>	105	RIPv2	RIPv1 & RIPv2	Não autenticar	--	--	Habilitado	✎ 🗑️

Um total de 1 itens na página

Descrição do parâmetro

Nome	Descrição
Importar Rotas	Ele é usado para importar informações de rota de outros processos ou protocolos para a tabela de roteamento RIP. O switch suporta a importação de rotas diretas, rotas estáticas e rotas OSPF.
RIP segmento de rede	
Segmento de rede e máscara de sub-rede	Ele especifica o segmento de endereço IP com RIP ativado. O RIP das interfaces do switch dentro do segmento de rede especificado está ativado.
Interface VLAN	Ele especifica a interface VLAN com RIP ativado.
Configurações da interface	

Mensagem Tx	<p>Ele especifica a versão RIP que a interface VLAN suporta ao transmitir mensagens RIP.</p> <ul style="list-style-type: none"> • Do Not Transmit: Esta interface não transmite mensagens RIP. • RIPv1: Esta interface transmite mensagens de requisição e resposta RIPv1. • RIPv2: Esta interface transmite mensagens de requisição e resposta RIPv2 através de multicast. • Broadcast RIPv2: Esta interface transmite mensagens de requisição e resposta RIPv2 através de broadcast.
Mensagem Rx	<p>Ele especifica a versão RIP suportada pela interface VLAN ao receber mensagens RIP.</p> <ul style="list-style-type: none"> • Do Not Receive: Esta interface não recebe mensagens RIP. • RIPv1: Esta interface recebe apenas mensagens de solicitação e resposta RIPv1. • RIPv2: Esta interface recebe apenas mensagens de solicitação e resposta RIPv2. • RIPv1 e RIPv2: Esta interface recebe mensagens de solicitação e resposta de RIPv1 e RIPv2.
Modo de autenticação	<p>Ele especifica o modo de autenticação usado pela interface VLAN para receber e transmitir mensagens RIP.</p> <ul style="list-style-type: none"> • Do Not Authenticate: A função de autenticação desta interface está desativada. • Simples: O modo de autenticação Simples é adotado. Quando a interface VLAN transmite mensagens RIP, a senha será adicionada ao cabeçalho da mensagem para autenticar o dispositivo de roteamento de mesmo nível. E a interface VLAN autenticará as mensagens RIP recebidas de acordo com a senha antes de responder. • MD5: O modo de autenticação MD5 é adotado. Quando a interface VLAN transmite mensagens RIP, a senha e o KeyID serão adicionados ao cabeçalho da mensagem para autenticar o dispositivo de roteamento de mesmo nível. E a interface VLAN autenticará as mensagens RIP recebidas de acordo com a senha e KeyID antes de responder.
Senha	Este campo é obrigatório quando a função de autenticação está habilitada para a interface.
Status RIP da interface	Ele especifica o status operacional RIP da interface VLAN.

Tabela de roteamento

Clique em Roteamento > Tabela de Roteamento para entrar na página. Nesta página, você pode configurar a tabela de roteamento do switch. Esta tabela de roteamento contém todas as informações de roteamento aprendidas pelo switch, incluindo rotas diretas, rotas estáticas e rotas dinâmicas.

Endereço de destino	Máscara de sub-rede	Tipo da Rota	Próximo salto
0.0.0.0	0.0.0.0	static	10.100.26.1
10.10.5.0	255.255.255.0	static	10.100.26.1
10.10.6.0	255.255.255.0	static	10.100.26.1
10.10.7.0	255.255.255.0	static	10.100.26.1
10.10.8.0	255.255.255.0	static	10.100.26.1
10.10.9.0	255.255.255.0	static	10.100.26.1
10.10.10.0	255.255.255.0	direct	vlan1.101
10.10.11.0	255.255.255.0	direct	vlan1.102
10.10.12.0	255.255.255.0	direct	vlan1.103
10.10.13.0	255.255.255.0	direct	vlan1.104

10 /página Página 1/6 Um total de 57 itens na página

Descrição do parâmetro

Nome	Descrição
Endereço de destino	Ele especifica o segmento de rede da rede de destino.
Máscara de sub-rede	Especifica a máscara de sub-rede da rede de destino.
Tipo de rota	It especifica o tipo da rota, incluindo: direct , static , RIP e OSPF .
Próximo salto	Ele especifica a interface de entrada da rota do próximo salto após a saída dos pacotes do switch.

ARP

No processo de transmissão de dados, o endereço IP é o endereço do host na camada de rede. Se você deseja enviar pacotes para o host de destino na camada de rede, é necessário o endereço da camada de enlace de dados do host de destino (como o endereço Ethernet MAC).

ARP (Address Resolution Protocol) pode converter um endereço IP em endereço MAC e mantém uma tabela ARP interna na base de dados do switch para registrar a relação correspondente entre endereços MAC e endereços IP de outros hosts que se comunicaram recentemente com este switch. Se o switch precisar se comunicar com o host de destino, ele executará primeiro a resolução de endereço com base no ARP. O processo de resolução é o seguinte:

1. O switch verifica se existe uma regra com o relacionamento correspondente entre o endereço IP e o endereço MAC do host de destino na tabela ARP do switch. Nesse caso, o switch envia dados para o host de destino de acordo com a regra consultada. Caso contrário, o switch transmite um quadro de dados de solicitação ARP na LAN, que contém o endereço IP e o endereço MAC do próprio switch, bem como o endereço IP do host de destino.

2. Todos os dispositivos na LAN podem receber esta solicitação. Quando o host de destino recebe essa solicitação, ele responde ao switch com um quadro de resposta ARP, que contém o endereço MAC do host de destino.
3. Depois que o switch recebe a resposta ARP, ele registra a relação correspondente do endereço IP e endereço MAC do host de destino em sua tabela ARP para uso posterior.

Clique em [Roteamento > ARP \(roteamento.html\)](#) para entrar na página. Sobre essa página, você pode visualizar e configurar a tabela ARP.

Aging time ARP 1200s

IP/MAC/VLAN ID/Tipo

[+ Adicionar](#)

<input type="checkbox"/>	Endereço de IP	Endereço MAC	VLAN ID	Tipo	Aging Time	Operação
<input type="checkbox"/>	10.100.26.147	d836.5f42.5ca8	vlan1.100	Dinâmico	1190s	
<input type="checkbox"/>	10.100.26.149	30c6.d73f.70d6	vlan1.100	Dinâmico	1180s	
<input type="checkbox"/>	10.100.26.157	9820.4453.744c	vlan1.100	Dinâmico	650s	
<input type="checkbox"/>	10.100.26.167	d094.66d5.4cc2	vlan1.100	Dinâmico	550s	
<input type="checkbox"/>	10.100.26.231	f223.60ac.ce8e	vlan1.100	Dinâmico	1100s	
<input type="checkbox"/>	30.30.30.1	30c6.d73f.70f0	vlan1.30	Dinâmico	1180s	
<input type="checkbox"/>	30.30.30.2	14ab.020d.1580	vlan1.30	Dinâmico	610s	
<input type="checkbox"/>	30.30.30.3	d836.5f42.5ca8	vlan1.30	Dinâmico	1190s	
<input type="checkbox"/>	105.105.105.3	d836.5f42.5ca8	vlan1.105	Dinâmico	1190s	

Um total de 9 itens na página

Nome	Descrição
Tempo de Envelhecimento ARP	Ele especifica o tempo de vencimento das entradas ARP. Se o switch não receber a mensagem ARP correspondente dentro desse período de tempo, a entrada ARP será removida da tabela ARP.
Endereço de IP	Ele especifica o endereço IP do host.
Endereço MAC	Ele especifica o endereço MAC do host correspondente ao endereço IP.
ID da VLAN	Ele especifica a interface da camada 3 da VLAN à qual a entrada ARP pertence.
Tipo	<p>Ele especifica o tipo da entrada ARP.</p> <ul style="list-style-type: none"> Dinâmico: Especifica a entrada ARP que é gerada automaticamente pelo switch de acordo com o ARP. Seu tempo de vida é definido pelo tempo de envelhecimento ARP. Estático: especifica as entradas ARP configuradas manualmente, que são válidas permanentemente e estão livres das limitações do tempo de envelhecimento ARP.
Tempo de Envelhecimento	Ele especifica o tempo restante de vencimento da entrada ARP.

Servidor DHCP

Com o aumento das demandas de rede, a rede se expande muito e se torna mais complexa, resultando em computadores superando os endereços IP alocáveis. Além disso, os locais dos dispositivos sem fio geralmente mudam, portanto, os endereços IP dos dispositivos precisam ser constantemente atualizados. DHCP (Dynamic Host Configuration Protocol) pode resolver os problemas acima pela estratégia de atribuição dinâmica de endereço IP.

O servidor DHCP deste switch não oferece suporte à alocação de endereços IP com base na opção 82.

De acordo com as diferentes necessidades dos clientes, o DHCP fornece dois tipos de estratégias de atribuição de endereços IP:

- Atribuição de endereço IP dinâmico: o DHCP atribui o endereço IP com um período válido ao cliente e o cliente precisa solicitar novamente o endereço IP após a expiração. Essa estratégia se aplica à maioria dos clientes.
- Atribuição de endereço IP estático: O administrador vincula os endereços IP fixos para alguns clientes específicos. A atribuição de um endereço IP fixo pode impedir a falha de algumas funções com base no endereço IP devido a alterações no endereço IP.

Configurações de DHCP

Clique em Roteamento > Servidor DHCP > Configurações DHCP para entrar na página. sobre isso página , você pode visualizar e configurar o servidor DHCP.

The screenshot shows a web interface for DHCP configuration. At the top, there are navigation tabs: "Configurações de DHCP" (active), "Reserva DHCP", and "Lista de clientes". A help icon is in the top right. Below the tabs, there is a "Servidor DHCP" toggle switch, currently turned off. Underneath, there is a section for "Conjunto de endereços IP" with a "+ Adicionar" button and a trash icon. A table with 9 columns (checkbox, Nome, Faixa de endereços IP, Máscara de sub-rede, Gateway padrão, Tempo de locação, DNS, Intervalo de IP excluído, Operação) is shown, but it is empty with "Sem dados" and "Um total de 0 itens na página" below it. The next section is "Servidor DHCP para Interface" with a table with 4 columns (Interface VLAN, Interface de Camada 3, Máscara de sub-rede, Servidor DHCP), also empty with "Sem dados" and "Um total de 0 itens na página" below it.

Descrição do parâmetro

Nome	Descrição	
Servidor DHCP	Ative ou desative a função do servidor DHCP.	
Conjunto de endereços IP	Nome	Especifica o nome do pool de endereços IP.
	Intervalo de endereços IP	Especifica o intervalo de endereços IP que podem ser atribuídos.
	Máscara de sub-rede	Especifica a máscara de sub-rede atribuída pelo servidor DHCP a um cliente.
	Gateway padrão	Especifica o endereço do gateway atribuído pelo servidor DHCP a um cliente.
	Tempo de Locação	Especifica o período de validade de um endereço IP atribuído pelo servidor DHCP a um cliente.
DNS	Especifica o endereço do servidor DNS atribuído aos clientes.	
Intervalo de IP excluído	Especifica os endereços IP no pool de endereços IP que não podem ser atribuídos pelo servidor DHCP pela estratégia de atribuição dinâmica.	

Servidor DHCP para Interface

Interface VLAN	Especifica a VLAN onde a política do pool de endereços entra em vigor.
Interface de camada 3	Especifica o endereço IP da interface VLAN.
Máscara de sub-rede	Especifica a máscara de sub-rede da interface VLAN.
Servidor DHCP	Com ele habilitado, a função Servidor DHCP da interface VLAN entra em vigor.

Reserva de DHCP

Clique em Roteamento > Servidor DHCP > DHCP Reserva para entrar na página. sobre isso página , você pode visualizar e configurar a política de reserva DHCP.

+ Adicionar



<input type="checkbox"/>	Nome do cliente	IP do cliente	Cliente MAC	Operação
--------------------------	-----------------	---------------	-------------	----------

Sem dados

Um total de 0 itens na página

Descrição do parâmetro**Nome****Descrição**

Nome do cliente	Especifica a observação da política de reserva DHCP. Se a política de reserva for adicionada da lista de clientes, ela exibirá o nome do cliente ou você poderá personalizá-la.
IP do cliente	Especifica um endereço fixo atribuído pelo servidor DHCP ao cliente.
MAC cliente	Especifica o endereço MAC de um cliente.

Lista de clientes

Clique em [Roteamento \(Roteamento.html\)](#) > [Servidor DHCP \(ServidorDHCP.html\)](#) > [Lista de clientes \(ListaDeClientes.html\)](#), para entrar na página. Na página, você pode realizar as seguintes operações para os dispositivos cujos endereços IP são obtidos a partir deste switch:

- Visualize o nome do cliente, o endereço IP atribuído e outras informações.
- Clique em **Reserve** em Operação e o endereço IP atribuído pode ser adicionado à lista de Reserva DHCP e o servidor DHCP atribui esse endereço IP ao cliente o tempo todo.

Endereço IP/endereço MAC



Nome do cliente ▾

IP atribuído ▾

Cliente MAC ▾

Expira em ▾

Tipo de atribuição ▾

Operação

Sem dados

Um total de 0 itens na página

Descrição do parâmetro**Nome****Descrição**

Nome do cliente

Especifica o nome de um cliente.

Um IP atribuído

Especifica um endereço IP atribuído pelo servidor DHCP ao cliente.

MAC cliente

Especifica o endereço MAC de um cliente.

Expira em

Especifica o tempo de descanso da concessão.

Tipo de Atribuição

Especifica a política de atribuição de endereço pelo servidor DHCP para o cliente.

Dinâmico

O servidor DHCP atribui endereço IP a este cliente usando a política de atribuição de endereço IP dinâmico.

Estático

O servidor DHCP atribui um endereço estático a este cliente usando a política de atribuição de endereço IP estático.

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, então as mapeia para diferentes filas no estágio de saída e, finalmente, encaminha essas mensagens por filas de acordo com o modo de agendamento, de forma 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 (filas de 0 a 7) 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 7 > Fila 6 > ... > Fila 0). 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 Prioridade, DSCP prioridade e porta Prioridade.

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. Como visto abaixo, a tag 802.1Q de 4 bytes contém um TPID (Tag Protocol Identifier, valor: 0x8100) de 2 bytes e um TCI de 2 bytes (Tag Control Information).

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

O RFC2474 redefine o campo ToS (Tipo de serviço) no cabeçalho da mensagem IP, que é chamado de campo DS (Serviços diferenciados). Os seis primeiros bits (bits 0 a 5) do campo DS indicam a prioridade DSCP (Differentiated Services Codepoint) 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
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 deste switch são mapeadas da seguinte forma:

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 (classe de serviço) 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 são mapeadas da seguinte forma:

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
1	QoS Agendador	Obrigatório. Selecione o modo de agendamento do switch com base nas demandas reais.
2	802.1P	Obrigatório. Configure a relação de mapeamento entre a prioridade 802.1P e as filas.
3	Porta Prioridade	Obrigatório. Defina o modo de prioridade das portas correspondentes para 802.1P Trust e configure a prioridade CoS para todas as portas.

Com base na prioridade DSCP

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

Agendador de QoS

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.

Modo QoS **Controle de congestão**Descarte de saída

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.
Descarte de saída	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. 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. sobre isso página , você pode configurar o relacionamento de mapeamento entre a prioridade 802.1P e as filas.

Configuração de prioridade de CoS

Prioridade0	<input type="text" value="Fila1"/>	▼
Prioridade1	<input type="text" value="Fila2"/>	▼
Prioridade2	<input type="text" value="Fila3"/>	▼
Prioridade3	<input type="text" value="Fila4"/>	▼
Prioridade4	<input type="text" value="Fila5"/>	▼
Prioridade5	<input type="text" value="Fila6"/>	▼
Prioridade6	<input type="text" value="Fila7"/>	▼
Prioridade7	<input type="text" value="Fila8"/>	▼

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. sobre isso page , você pode configurar o relacionamento de mapeamento entre a prioridade DSCP e as filas.

DSCP

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

Confirmar

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. sobre isso página , você pode configurar o modo de confiança e a prioridade CoS para as portas físicas do switch.

Editar

Porta	Prioridade CoS	Modo de confiança	Operação
1	0	Não confiável	
2	0	Não confiável	
3	0	Não confiável	
4	0	Não confiável	
5	0	Não confiável	
6	0	Não confiável	
7	0	Não confiável	
8	0	Não confiável	
9	0	Não confiável	
10	0	Não confiável	

Um total de 27 itens na página

Descrição do parâmetro

Nome **Descrição**

Porta	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 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.

Orientação de configuração

F baseadas no endereço MAC

Etapa	Tarefa	Descrição
-------	--------	-----------

1	MAC ACL	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	A regra MAC ACL entra em vigor quando é aplicada à porta correspondente do switch.

F com base no endereço IP

Etapa	Tarefa	Descrição
1	IP ACL	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	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	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 as mensagens de todas as VLANs.
MAC de origem	Especifica o endereço MAC de origem da mensagem. Opções: <ul style="list-style-type: none"> 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.
MAC de destino	Especifica o endereço MAC de destino da mensagem. Opções: <ul style="list-style-type: none"> 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.
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. <ul style="list-style-type: none"> Permitir : Encaminhar as mensagens que correspondem à regra. Bloquear: 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.

The screenshot shows the IP ACL configuration interface. At the top, there are three tabs: 'MAC ACL', 'IP ACL' (which is active and highlighted in green), and 'Aplicar ACL'. Below the tabs, there is a dropdown menu for 'ID da ACL' with the text 'Por favor, configure o AC...' and three buttons: '+ Adicionar ACL' (green), 'Editar ACL', and 'Excluir ACL'. Below this, there is a section for 'Regra IP ACL' with a '+ Adicionar regra' button and a trash icon. A table with the following columns is shown: 'Prioridade', 'Protocolo', 'IP de Origem', 'IP de destino', 'Porta de origem', 'Porta de destino', 'Modo ACL', and 'Operação'. The table is currently empty, with a message 'Sem dados' in the center and 'Um total de 0 itens na página' at the bottom right.

Descrição do parâmetro

Nome	Descrição
ID ACL	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	Especifica o campo do tipo de protocolo do cabeçalho do pacote IP da camada 3 de uma mensagem, como IP, ICMP e assim por diante. Você também pode inserir o número do protocolo manualmente.
IP fonte	Especifica o endereço IP de origem da mensagem. Opções: <ul style="list-style-type: none">• Qualquer IP: Indica todos os endereços IP.• IP especificado: Combinado com a máscara, indica um determinado endereço de rede.
IP de destino	Especifica o endereço IP de destino da mensagem. Opções: <ul style="list-style-type: none">• 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 é TCP ou UDP, você pode configurar o número da porta de origem do protocolo.
Porta de destino	Quando o tipo de protocolo é TCP ou UDP, você pode configurar o número da porta de destino do protocolo.
Modo ACL	Especifica o modo ACL no qual o switch processa as mensagens que correspondem à regra. Opções: <ul style="list-style-type: none">• Permitir: Encaminhar as mensagens que correspondem à regra.• Bloquear: Descartar 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 de ACL configuradas às portas físicas.

MAC ACL IP ACL **Aplicar ACL** + Adicionar

Porta aplicada	ID da ACL	Direção de filtragem	Operação
Sem dados			

Um total de 0 itens na página

Descrição do parâmetro

Nome	Descrição
Porta Aplicada	Especifica o número da porta física à qual a regra ACL se aplica.
ID ACL	Especifica a regra ACL aplicada à porta.
Direção de Filtragem	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 Segurança de rede > Filtragem MAC para entrar na página. Nesta página, você pode configurar as regras de filtragem MAC.

Filtragem MAC

+ Adicionar
🗑️

Endereço MAC	VLAN	Operação
📭 Sem dados		

Um total de 0 itens na página

Descrição do parâmetro

Nome	Descrição
Endereço MAC	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	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.

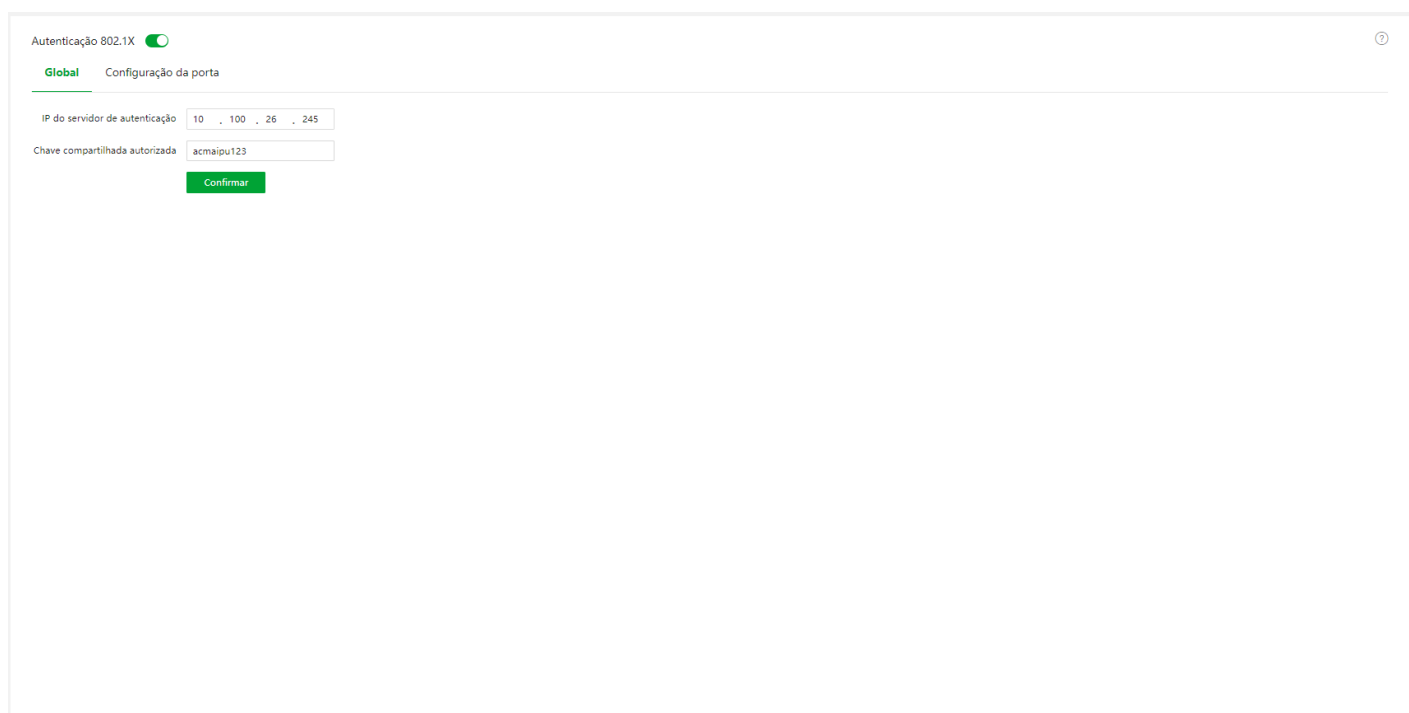
- **Cliente de autenticação:** Um dispositivo cliente envia uma solicitação de autenticação e o servidor de autenticação na LAN verifica sua validade. É necessário um software cliente compatível com autenticação 802.1X.
- **Dispositivo de autenticação:** Fornece interface para o cliente se conectar à 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 **Segurança de Rede > 802.1X > Configuração da porta** para entrar na página. Nesta página, você pode configurar os parâmetros de autenticação 802.1X para cada porta.

Porta	Modo de controle de porta	Status de autenticação	Re-autenticação	Tempo limite de reautenticação	Timeout do cliente	Intervalo de reautenticação	Operação
1	Desativar	Não autorizado	Desativar	3600	30	2	
2	Desativar	Não autorizado	Desativar	3600	30	2	
3	Desativar	Não autorizado	Desativar	3600	30	2	
4	Desativar	Não autorizado	Desativar	3600	30	2	
5	Desativar	Não autorizado	Desativar	3600	30	2	
6	Desativar	Não autorizado	Desativar	3600	30	2	
7	Desativar	Não autorizado	Desativar	3600	30	2	
8	Desativar	Não autorizado	Desativar	3600	30	2	
9	Desativar	Não autorizado	Desativar	3600	30	2	
10	Desativar	Não autorizado	Desativar	3600	30	2	

Descrição do parâmetro

Nome	Descrição
------	-----------

Porta	Ele especifica o ID da 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.

Modo de controle de porta	
---------------------------	--

- 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.

Nome	Descrição
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

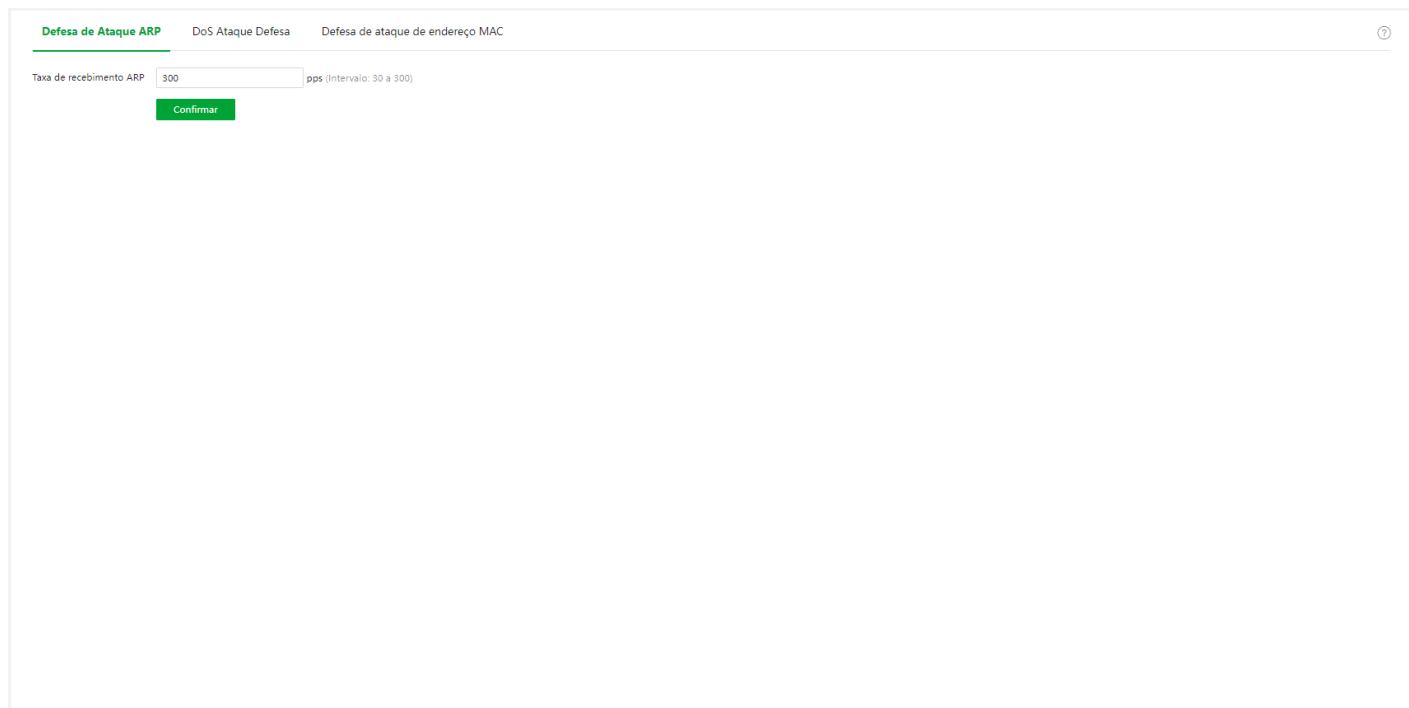
A função DoS Defesa de ataque é usada para impedir que alguns hosts consumam recursos do servidor de forma maliciosa enviando um grande número de solicitações de serviço, deixando outros hosts incapazes de usar os serviços de rede adequadamente.

- 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.



Defesa de Ataque ARP DoS Ataque Defesa Defesa de ataque de endereço MAC

Taxa de recebimento ARP pps (Intervalo: 30 a 300)

[Confirmar](#)

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.

- Detecta se existem inconsistências entre a mensagem do remetente ARP_MAC e L2_MAC.
- Detecta se as mensagens TCP são mensagens multicast ou broadcast.
- Detecta se todos os sinalizadores (flags) de mensagens TCP são 0.
- Detecta se os sinalizadores (flags) FIN, URG e PSH da mensagem TCP são todos 1.
- Detecta se o SYN, FIN e os sinalizadores (flags) da mensagem TCP são todos 1.
- Detecta se os sinalizadores SYN e RST da mensagem TCP são ambos 1.
- Detecta se o número da porta de origem ou o número da porta de destino da mensagem TCP e UDP é 0.
- Detecta se a mensagem TCP SYN contém dados.
- Detecta pacotes ICMP fragmentados

Confirmar

Descrição do parâmetro

Nome	Descrição
Detecte se existem inconsistências entre a mensagem ARP Sender_MAC e L2_MAC.	Depois de marcado, o switch não encaminha mensagens ARP com Sender_MAC e L2_MAC inconsistentes.
Detecta se as mensagens TCP são multicast ou broadcast.	Depois de marcado, o switch não encaminha mensagens multicast ou broadcast TCP.
Detecta se todos os sinalizadores de mensagens TCP são 0.	Depois de marcado, o switch não encaminha mensagens TCP cujos sinalizadores são todos 0.
Detecte se os sinalizadores FIN, URG e PSH da mensagem TCP são todos 1.	Depois de marcado, o switch não encaminha a mensagem TCP cujos sinalizadores FIN, URG e PSH são todos 1.
Detecte se os sinalizadores SYN, FIN e sinalizadores da mensagem TCP são todos 1.	Depois de marcado, o switch não encaminha a mensagem TCP cujos sinalizadores SYN e FIN são todos 1.
Detecte se os sinalizadores SYN e RST da mensagem TCP são ambos 1.	Depois de marcado, o switch não encaminha a mensagem TCP cujos sinalizadores SYN e RST são ambos 1.
Detecte se o número da porta de origem ou o número da porta de destino da mensagem TCP e UDP é 0.	Depois de marcado, o switch não encaminha a mensagem TCP e UDP cujo número de porta de origem ou número de porta de destino é 0.
Detecte se a mensagem TCP SYN contém dados.	Depois de marcado, o switch não encaminha a mensagem TCP SYN que contém dados.
Detecção de fragmento de mensagem ICMP.	Depois de marcado, o switch não responde à mensagem ICMP fragmentada.

Defesa de ataque de endereço MAC

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

Porta	Descartar MAC	Operação
1	Desativar	✎
2	Desativar	✎
3	Desativar	✎
4	Desativar	✎
5	Desativar	✎
6	Desativar	✎
7	Desativar	✎
8	Desativar	✎
9	Desativar	✎
10	Desativar	✎

Um total de 28 itens na página

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 .

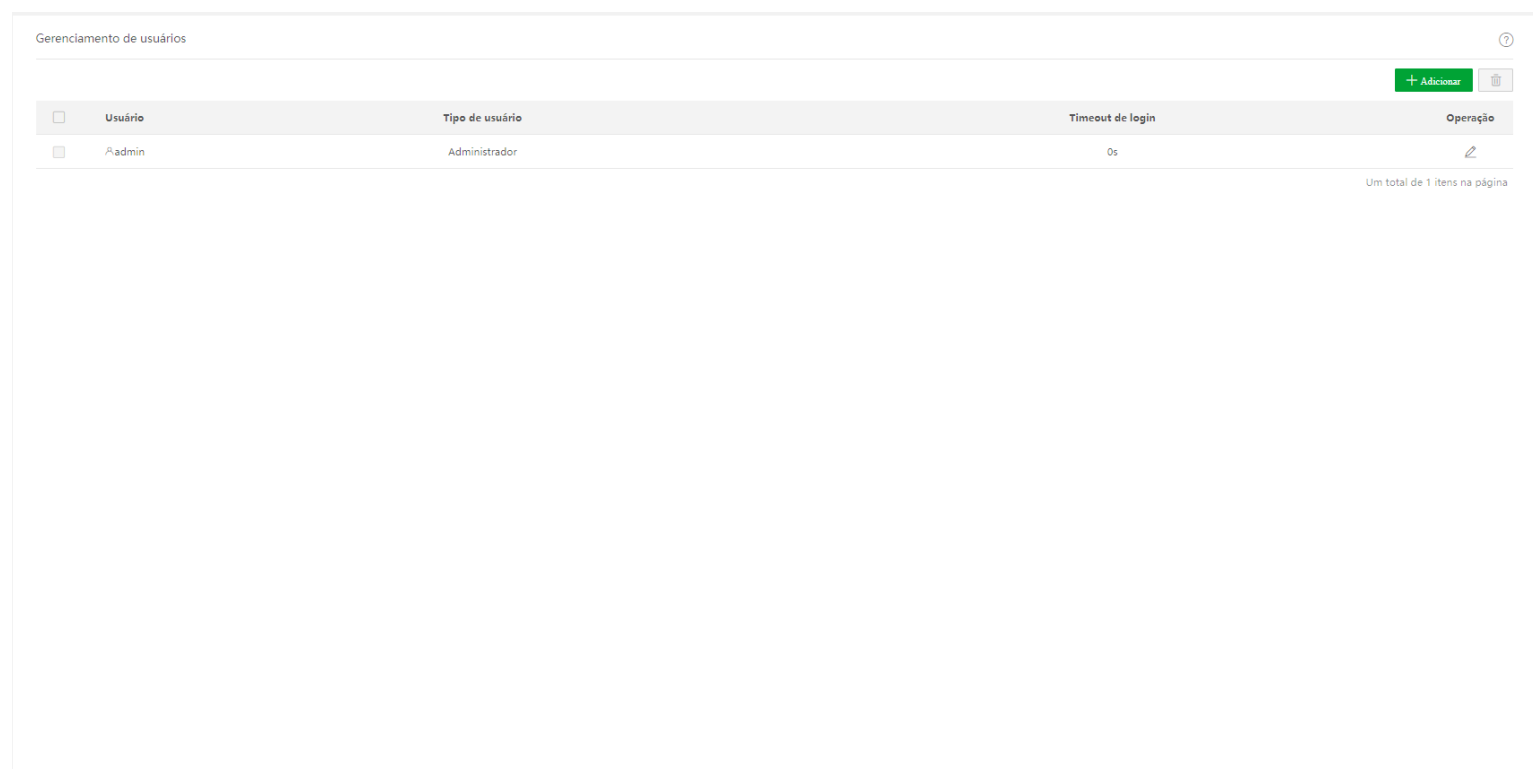
- usuário da operação

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).



Usuário	Tipo de usuário	Timeout de login	Operação
Admin	Administrador	0s	

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.

SNMP

Básico Controle de permissão Notificação

Informações de contato (1 a 255 caracteres)

Informações do local (1 a 255 caracteres)

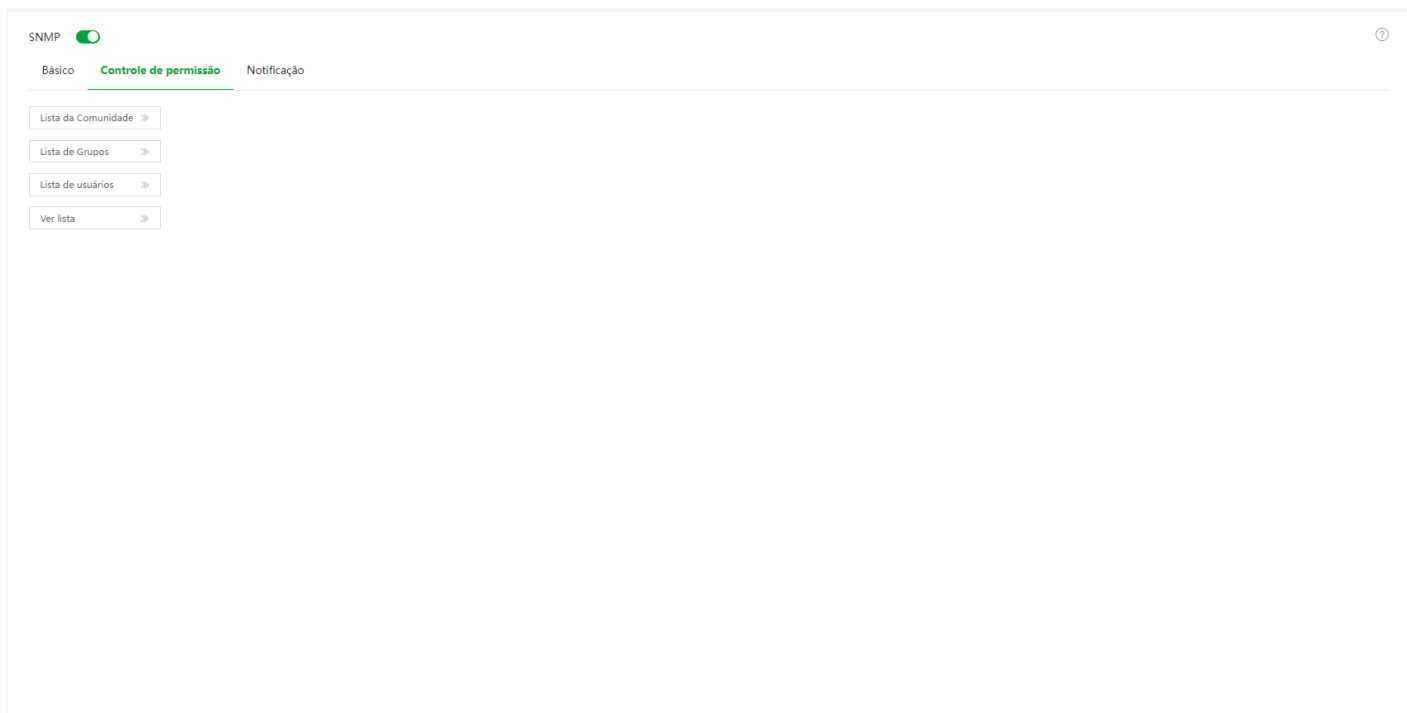
ID do mecanismo local (10 a 64 caracteres hexadecimais)

Nota: Este dispositivo é compatível com SNMP v1/v2c/v3

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**

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 .

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 .
Lista de usuários	
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	<p>Regra</p> <p>Ele especifica a regra OID.</p> <ul style="list-style-type: none"> • inclui : Este OID pode ser gerenciado pelo SNMP. • exclui : 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.

SNMP

Básico Controle de permissão **Notificação**

Ativar todas as TRAP

Host de destino + Adicionar

<input type="checkbox"/>	IP do host de destino	Comunidade/Usuário	Porta UDP	Versão de segurança	Nível de segurança	Operação
<input type="checkbox"/>	10.100.26.231	AuthPriv	162	v3	Autenticação e privacidade	
<input type="checkbox"/>	10.100.26.231	intelbras	162	v2c	--	

Um total de 2 itens na página

Descrição do parâmetro

Nome

Descrição

Ativar todas as armadilhas

É usado para habilitar/desabilitar a função Trap.

Nome	Descrição
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.

Hora do sistema

Hora atual **2023-05-23 11:55:55**

Horário local Hora da Internet

Data Tempo

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.

Hora do sistema

Hora atual **2023-05-23 11:56:16**

Horário local Hora da Internet A sincronização de tempo requer conexão com a Internet

Fuso horário

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 > Informações do log > Log Info** para entrar na página. Nesta página, você pode visualizar, baixar e excluir as informações de log do switch.

Informações de log Configurações do servidor

Nível de registro:

[Download](#) [Refresh](#) [Delete](#)

ID	Tempo gerado	Sistema de Log	Nível de registro
1	2023/05/23 11:02:46	web client user admin login from 10.100.26.167	Info
2	2023/05/17 18:39:27	web client user admin login from 10.100.26.150	Info
3	2023/05/17 18:12:23	Remote user login out. Ip:10.100.26.150	Info
4	2023/05/17 18:01:23	Remote user login. Ip:10.100.26.150	Info
5	2023/05/17 11:54:30	Interface ge5 down	Info
6	2023/05/17 11:53:48	Interface ge5 up	Info
7	2023/05/11 14:42:42	Interface ge16 down	Info
8	2023/05/10 17:02:13	Interface xe4 up	Info
9	2023/05/10 17:02:13	Interface xe4 down	Info
10	2023/05/10 17:02:13	Interface xe4 up	Info

/página

Página 1/181 Um total de 1809 itens na página [1](#) [2](#) [3](#) [4](#) [5](#) [...](#) [181](#)

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 > Informações do log > 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.

Informações de log **Configurações do servidor**

Servidor habilitado

Nível de registro debug

Endereço IP do servidor . . .

Porta

Confirmar

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.

Diagnóstico

Clique em **Configurações do dispositivo > Diagnósticos** para entrar na página. sobre isso page , você pode executar o teste Ping/Tracert.

- Ping test : É usado para testar a conexão de rede e a qualidade da conexão.
- Rastreador teste : É usado para testar as rotas dos pacotes do switch para o host de destino.

Teste de ping

Clique em Configurações do dispositivo > Diagnóstico > Teste de ping para entrar na página. sobre isso página , você pode testar a conexão de rede.

Teste de ping Tracert

Endereço IP de destino (Por favor, insira um endereço IP/nome de domínio)

Tempos de transmitido (Intervalo: 1 a 100)

Tamanho do pacote (Intervalo: 16 a 512)

Descrição do parâmetro

Nome	Descrição
Endereço IP de destino	Ele especifica o endereço IP do dispositivo a ser pingado.
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 Configurações do dispositivo > Diagnósticos > Tracert para entrar na página. sobre isso page , você pode testar as rotas do pacote desde o switch até o dispositivo de destino .

Descrição do parâmetro

Teste de ping **Tracert**

Endereço IP de destino (Por favor, insira um endereço IP/nome de domínio)

Máximo de saltos \$ (Intervalo: 1 a 30)

Começar

Nome	Descrição
Endereço IP de destino	Ele especifica o endereço IP do dispositivo de destino a ser testado.
Saltos Máximos	Ele especifica os saltos máximos para o teste tracert.

Visualização

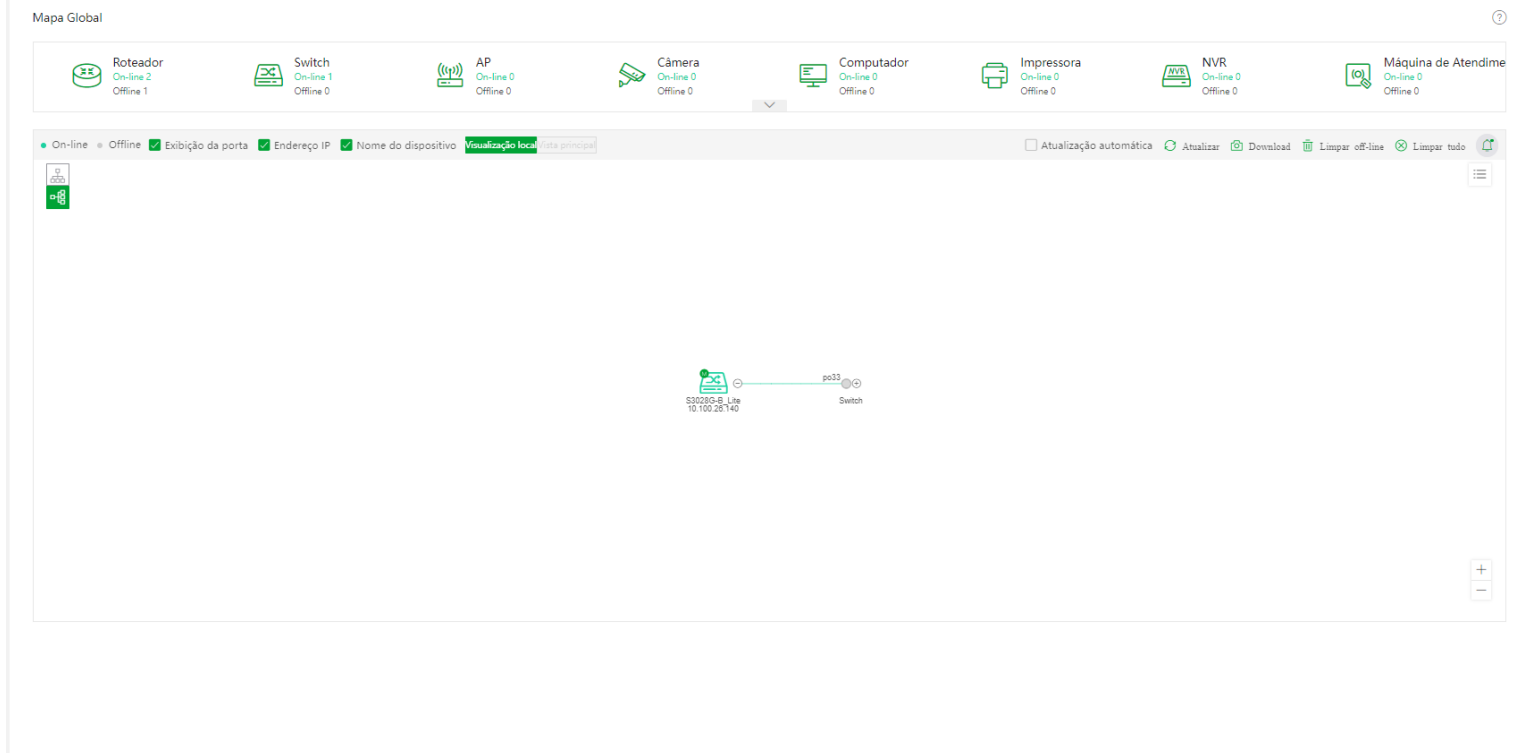
Para algumas redes que não precisam acessar a internet (como redes de monitoramento de segurança de médio e grande porte), o gerenciamento de nuvem IMS não está disponível. A função de visualização deste switch fornece gerenciamento central e manutenção para essas redes.

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.


Todos ...		Nome/endereço IP/enc	Q
	S3028G-B_Lite	10.100.26.140 D838.0D26.937C	
		10.100.26.1 0009.0F09.1E0A	
		10.100.26.30 000A.5AA0.EBD1	
		10.100.26.20 0013.E900.51B0	
		10.100.26.247 0018.7DD7.612F	

- Ver e modificar parâmetros

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

Tipo de dispositivo	Switch
Descrição	S3028G-B_Lite
Dispositivo principal	<input checked="" type="checkbox"/>
Nome do dispositivo	S3028G-B Lite
Endereço MAC	D838.0D26.937C
Endereço IP	10.100.26.140
 Dispositivo de Pesquisa	 Configuração da porta
Confirmar	

 : 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.



Tipo de dispositivo Outros

Descrição


Nome do dispositivo


Endereço MAC D094.66D5.4CC2

Endereço IP 192.168.0.10

 Login na interface Web
  Teste de conectividade


















Confirmar

 : 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.

Nome do dispositivo	Tipo de dispositivo	Modelo do dispositivo	Status do dispositivo	Endereço MAC	Endereço de IP	Operação
S3028G-8_Lite	Switch	S3028G-8 Lite	On-line	D838.0D26.937C	10.100.26.140	
	Outros		On-line	0009.0F09.1E0A	10.100.26.1	
	Outros		On-line	000A.5AA0.EBD1	10.100.26.30	
	Outros		Offline	0013.E900.51B0	10.100.26.20	 
	Outros		Offline	0018.7DD7.613F	10.100.26.247	 
	Outros		Offline	001A.3F00.113C	10.100.26.252	 
	Outros		Offline	0050.4376.7676	10.100.26.104	 
	Roteador		Offline	0050.4379.7979	10.100.26.104	 
	Outros		Offline	00D7.6D2E.082E	10.100.26.162	 
	Outros		Offline	00D7.6D7A.06CA	10.100.26.163	 

10 /página

Página 1/9 Um total de 81 itens na página

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.

Nome	Descrição
Tipo de dispositivo	Especifica o tipo do dispositivo. Você pode clicar para modificar o tipo de dispositivo. Dica
<hr/>	
<p>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.</p>	
<p>O tipo de dispositivo modificado aqui é exibido apenas na seção Visualização, e o campo correspondente na mensagem do protocolo não será alterado.</p>	
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.
<hr/>	
Status do dispositivo	Ele especifica o status online/offline do dispositivo.
<hr/>	
Endereço MAC	Ele especifica o endereço MAC do dispositivo.
<hr/>	
Endereço de IP	Ele especifica o endereço IP do dispositivo.
<hr/>	

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 da data de compra – sendo 90 (noventa) dias de garantia legal e 33 (três 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.

Produto beneficiado pela Legislação de Informática.

intelbras



fale com a gente

Suporte a clientes: (48) 2106 0006

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

Suporte via chat: [intelbras.com/suporte-tecnico](http://www.intelbras.com/suporte-tecnico) (<http://www.intelbras.com/suporte-tecnico>).

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

SAC: 0800 7042767

Onde comprar? Quem instala?: 0800 7245115

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

