

Manual do Usuário – SWITCH POSITIVO
10/100/1000MBPS, GERENCIÁVEL, 24 PORTAS POE + 4
PORTAS SFP, 250W CONSUMO MÁX
- PST-SWI-G224P

Prefácio

Obrigado por escolher a POSITIVO! Este guia do usuário ajuda você a configurar, gerenciar e manter o produto.

Convenções

Este guia do usuário é aplicável às seguintes opções. Para recursos do produto e capturas de tela de software, consulte o produto real. PST-SWI-G224P é usado para ilustração se não houver outra especificação.

Os elementos tipográficos que podem ser encontrados neste documento são definidos da seguinte forma.

Item	Apresentação	Exemplo
Menus cascata	em >	Escolha System > Live Users .
Parâmetro e valor	Negrito	Defina Nome de usuário como Tom .
Variável	Itálico	Formato: XX: XX: XX: XX: XX: XX: XX
Controle interface usuário	de Negrito do	Na página Política , clique no botão OK .

Os símbolos que podem ser encontrados neste documento são definidos da seguinte forma.

Item	Significado
 Nota	Este formato é usado para destacar informações de importância ou interesse especial. Ignorar esse tipo de nota pode resultar em configurações ineficazes, perda de dados ou danos ao dispositivo.
 Dica	Esse formato é usado para realçar um procedimento que economizará tempo ou recursos.

Para mais documentos

Acesse nosso site em <https://www.positivoseg.com.br/> e procure os documentos mais recentes para este produto.

Índice

1 Login na Web.....	1
1.1 Login.....	1
1.2 Logout.....	3
2 Introdução à interface do usuário da Web	4
2.1 Layout da Web	4
2.2 Botões mais usados	5
3 Resumo do sistema	6
4 Switching	8
4.1 Gestão de portas	8
4.1.1 Básico	8
4.1.2 Espelhamento de porta	9
4.1.3 Agregação de portas.....	10
4.1.4 Limite de taxa de porta.....	11
4.1.5 Estatísticas de pacotes.....	12
4.2 VLAN.....	15
4.2.1 Visão geral.....	15
4.2.2 Configuração de VLAN.....	16
4.2.3 Exemplo de configuração de VLAN 802.1Q.....	18
4.3 DHCP relay	21
4.4 DHCP snooping	24
4.5 STP.....	26
4.5.1 Visão geral.....	26
4.5.2 Global.....	33
4.5.3 Configuração de porta	37
4.5.4 Estatísticas de portas	38
4.5.5 Informações da instância	39
4.6 Configuração do LLDP	41
4.6.1 Visão geral.....	41
4.6.2 Global.....	42
4.6.3 Configuração de porta	43
4.6.4 Informações do vizinho	44
4.7 IGMP snooping.....	46
4.7.1 Princípio de IGMP snooping	46
4.7.2 Global.....	48
4.7.3 Saída rápida.....	49
5 Roteamento.....	50
5.1 Roteamento estático	50

5.2 ARP	51
5.3 Servidor DHCP	53
5.3.1 Visão geral	53
5.3.2 Configurações de DHCP	53
5.3.3 Reserva DHCP	55
5.3.4 Lista de clientes	55
6 Política de QoS	57
6.1 ACL	57
6.1.1 Visão geral	57
6.1.2 Diretrizes de configuração	57
6.1.3 Lista ACL	58
6.1.4 MAC ACL	58
6.1.5 IP ACL	59
6.1.6 Aplicar ACL	60
6.2 QoS	61
6.2.1 Visão geral	61
6.2.2 Diretrizes de configuração	65
6.2.3 Agendador de QoS	66
6.2.4 802.1P	67
6.2.5 DSCP	68
6.2.6 Prioridade de porta	68
7 Segurança de rede	70
7.1 Filtragem MAC	70
7.2 802.1X	71
7.2.1 Visão geral	71
7.2.2 Global	71
7.2.3 Configuração de porta	72
7.3 Defesa de ataque	74
7.3.1 Visão geral	74
7.3.2 Defesa de ataque ARP	74
7.3.3 Defesa de ataque DoS	75
7.3.4 Defesa de ataque de endereço MAC	76
8 Configurações do dispositivo	77
8.1 Gerenciamento de usuários	77
8.2 SNMP	78
8.2.1 Visão geral	78
8.2.2 Diretrizes de configuração	80
8.2.3 Básico	81
8.2.4 Controle de permissão	81
8.2.5 Notificação	83
8.3 Hora do sistema	85
8.4 Manutenção	86
8.4.1 Atualização de firmware	86

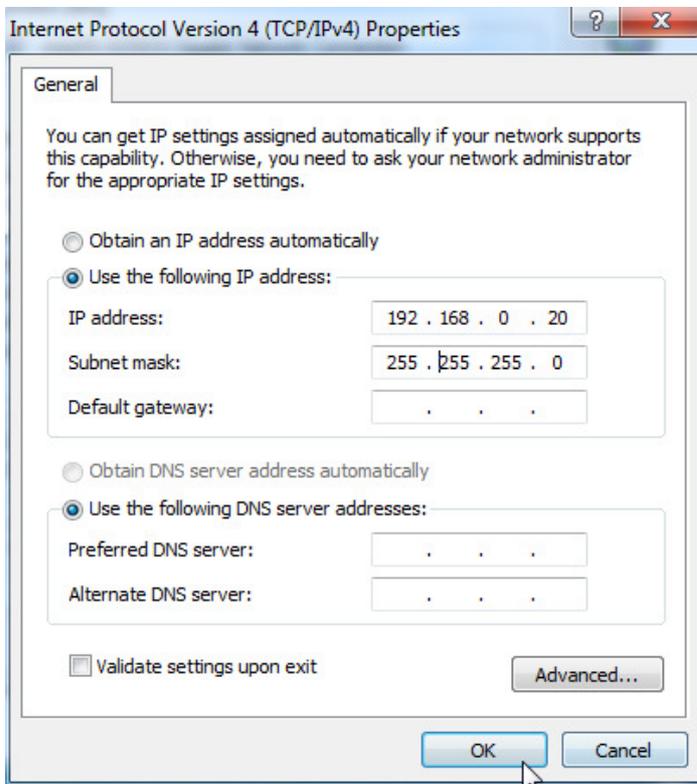
8.4.2	Importação de configuração	86
8.4.3	Backup	87
8.4.4	Reinicializar.....	87
8.4.5	Configurações de fábrica	88
8.5	Gerenciamento de logs	90
8.5.1	Informações de registro.....	90
8.5.2	Configurações do servidor.....	91
8.6	Diagnostics	92
8.6.1	Teste de ping.....	92
8.6.2	Teste Tracert	92
8.7	Configurações MAC.....	94
8.7.1	Tabela de endereços MAC.....	94
8.7.2	Endereço MAC estático	95
8.8	Período de tempo.....	96
9	Gerenciamento de PoE.....	97
9.1	Visão geral	97
9.2	Global.....	98
9.3	Configurações de porta	99
Apêndice	101

1 Login na Web

1.1 Login

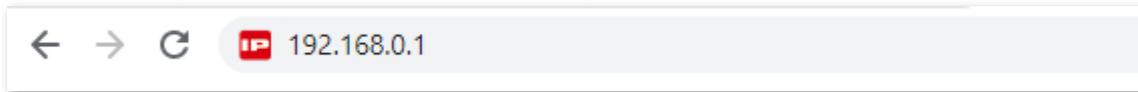
1. Conecte o computador a qualquer uma das portas de 1 a 24 do switch usando um cabo Ethernet.
2. Defina o endereço IP do computador como um não utilizado pertencente ao mesmo segmento de rede do endereço IP do switch.

O endereço IP padrão do switch é 192.168.0.1, **você pode definir o endereço IP do computador como 192.168.0.X** (X é um número não utilizado que varia de 2 a 254) e máscara de sub-rede para **255.255.255.0**.



3. Inicie um navegador (como o Internet Explorer) e digite o endereço IP do switch (padrão):

192.168.0.1) na barra de endereços para acessar a página de login.



4. Digite seu nome de usuário e senha (o nome de usuário e a senha padrão são **admin**) e clique em **Faça login**.

A screenshot of a web login page. It contains a 'User Name' input field with a magnifying glass icon, a 'Password' input field with a lock icon, a 'Forget password' link, a language dropdown menu set to 'English', and a prominent red 'Login' button.

----Fim



Dica

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

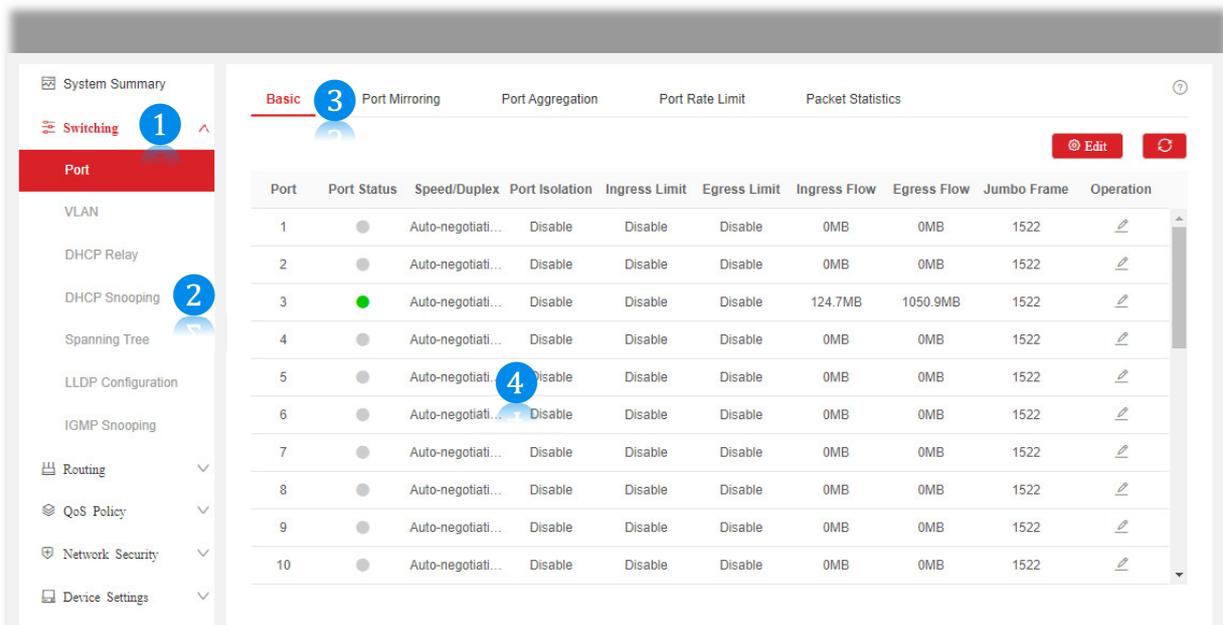
- Limpe o cache do navegador da Web ou tente outro navegador da Web.
- Verifique se existe outro dispositivo com o endereço IP 192.168.0.1 na rede local.
- Se o problema persistir, redefina a opção e tente novamente. Método de reinicialização: Quando o indicador LED SYS estiver piscando, mantenha pressionado o botão de reinicialização (Modo LED ou LED/Reset) por cerca de 10 segundos e, em seguida, solte-o quando todos os indicadores LED estiverem ligados. O interruptor é restaurado para as configurações de fábrica quando o indicador LED SYS pisca novamente.

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

2 Introdução à interface do usuário da Web

2.1 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 de página de guia e área de configuração.



No.	Name	Description
1	Barra de navegação de nível 1	As barras de navegação e as páginas de guias interruptor. Quando você seleciona uma função na barra de navegação, a configuração da função aparece na área de configuração.
2	Barra de navegação de nível 2	

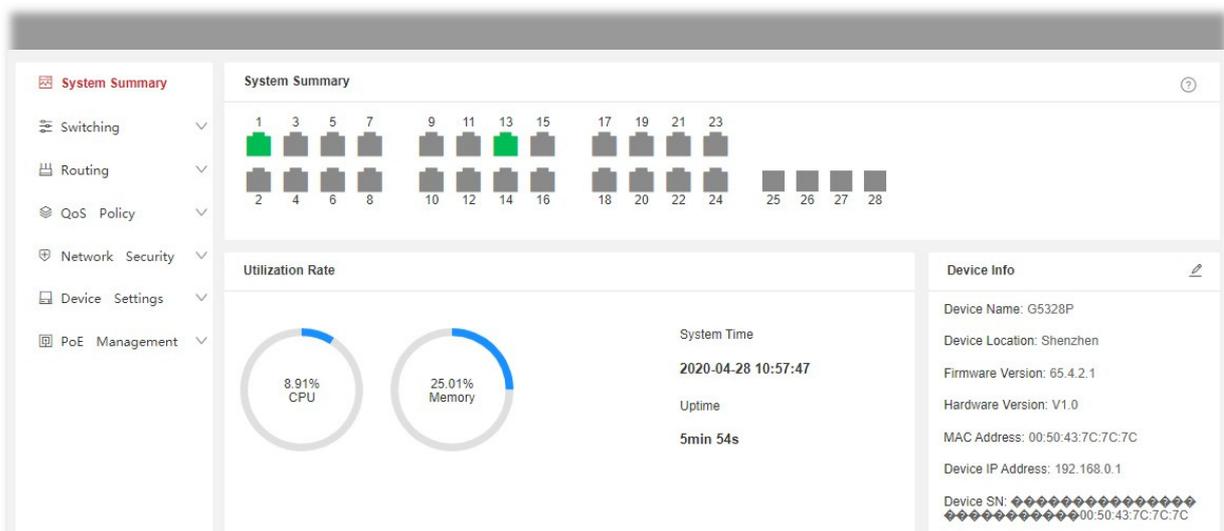
- 3 Area da página da guia
- 4 Área de configuração Esta área permite que você visualize e modifique a configuração.

Botões	Descrição
	Usado para atualizar o conteúdo exibido na página atual.
	Usado para definir as configurações na página atual em lotes.
	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, elas serão limpas após a reinicialização do switch.
Cancelar	Usado para restaurar a configuração original sem salvar a configuração na página atual.
	Usado para exibir informações de ajuda correspondentes às configurações na página atual.
	Usado para adicionar novas regras na página atual.
	Usado para excluir as regras na página atual.
	Usado para salvar todas as configurações atuais do switch. Se você clicar para Save salvar as configurações, elas ainda permanecerão após a reinicialização do switch.

2.1 Botões mais usados

3 Resumo do sistema

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



Descrição do parâmetro

Nome	Descrição
Resumo do sistema	Exibe o status de conexão de cada porta do switch: indica que a porta está conectada a um dispositivo e  indica que a porta não está conectada a um dispositivo. 
Taxa de Utilização	Exibe a utilização da CPU e memória do switch.
Tempo do Sistema	Exibe a hora do sistema do switch.
Uptime	Exibe o tempo durante o qual esse switch está operando desde a última reinicialização.

Informação do dispositivo	Nome do dispositivo	Exibe o nome do switch. Você pode clicar em  para modificá-lo. O nome padrão é G5328P.
	Localização do dispositivo	Exibe a localização do switch. Você pode clicar em  para modificá-lo. O padrão localização é Shenzhen.
	Firmware Version	Exibe a localização do switch. Você pode clicar em  para modificá-lo. O padrão localização é Shenzhen.
	Versão do hardware	Exibe a versão de hardware do switch.

Nome	Descrição
Endereço MAC	Exibe o endereço MAC do switch.
Endereço IP do dispositivo	Exibe o endereço IP da VLAN padrão do switch. O computador pertencente à VLAN padrão pode fazer logon na interface do usuário da Web do switch usando esse endereço IP.
Dispositivo SN	Exibe o número de série do switch..

4 Switching

4.1 Gestão de portas

4.1.1 Básico

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

Port	Port Status	Speed/Duplex	Port Isolation	Ingress Limit	Egress Limit	Ingress Flow	Egress Flow	Jumbo Frame	Operation
1	●	Auto-negotiati...	Disable	Disable	Disable	0MB	0MB	1522	✎
2	●	Auto-negotiati...	Disable	Disable	Disable	0MB	0MB	1522	✎
3	●	Auto-negotiati...	Disable	Disable	Disable	178.9MB	1197.0MB	1522	✎
4	●	Auto-negotiati...	Disable	Disable	Disable	0MB	0MB	1522	✎
5	●	Auto-negotiati...	Disable	Disable	Disable	0MB	0MB	1522	✎
6	●	Auto-negotiati...	Disable	Disable	Disable	0MB	0MB	1522	✎
7	●	Auto-negotiati...	Disable	Disable	Disable	0MB	0MB	1522	✎
8	●	Auto-negotiati...	Disable	Disable	Disable	0MB	0MB	1522	✎
9	●	Auto-negotiati...	Disable	Disable	Disable	0MB	0MB	1522	✎
10	●	Auto-negotiati...	Disable	Disable	Disable	0MB	0MB	1522	✎

Parameter description

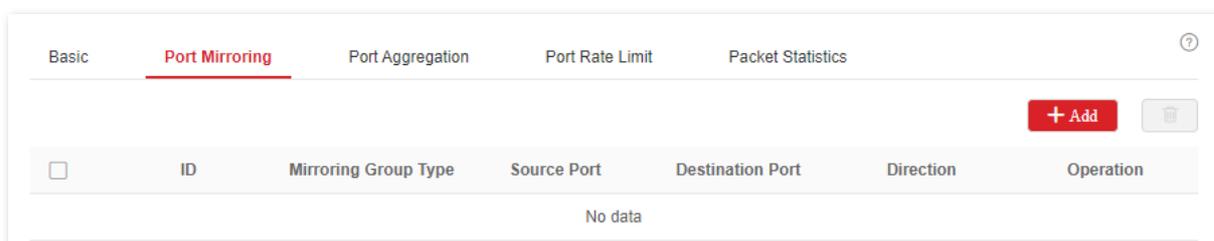
Nome	Descrição
Porta	Especifica a ID da porta.
Status da porta	<p>Especifica o status de conexão atual da porta.</p> <ul style="list-style-type: none"> : Porta Conectada. : Porta não conectada. : Porta desabilitada.

Velocidade/Duplex		Especifica a velocidade de transmissão e o modo duplex da porta. - HDX: Half duplex. - FDX: Full duplex.
Nome		Descrição
Isolamento de porta		Especifica o grupo de isolamento ao qual a porta pertence. As portas pertencentes a grupos de isolamento diferentes podem se comunicar entre si, enquanto as portas pertencentes ao mesmo grupo não podem. As portas que não são atribuídas a nenhum grupo de isolamento são exibidas no estado Desabilitado , indicando que elas podem se comunicar com todas as portas.
Limite de Entrada	de	Com a função ativada, 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 de mesmo nível para interromper ou desacelerar a transmissão de dados por um período de tempo específico, de modo a evitar a perda de mensagens incorridas.
Limite de Egresso	de	Com a função ativada, quando o switch recebe um quadro PAUSE do dispositivo peer, o switch pára ou diminui a velocidade de transmissão de dados da porta correspondente por um período de tempo específico para evitar a perda de mensagens incorridas.
Fluxo de Entrada	de	Especifica as estatísticas de tráfego de dados recebidos pela porta.
Fluxo de Egresso	de	Especifica as estatísticas do tráfego de dados transmitidos pela porta.
Moldura Jumbo		Especifica o tamanho do pacote que pode ser recebido ou transmitido pela porta. Os pacotes que excederem esse tamanho serão descartados.

4.1.2 Espelhamento de porta

O espelhamento de porta é um método de copiar e enviar pacotes de rede de uma porta ou várias portas (portas de origem) para uma porta especificada (porta de destino) do switch. A porta de destino é comumente conectada a um dispositivo de monitoramento de dados, permitindo que você monitore o tráfego de dados, analise o desempenho e diagnostique falhas.

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



Descrição do parâmetro

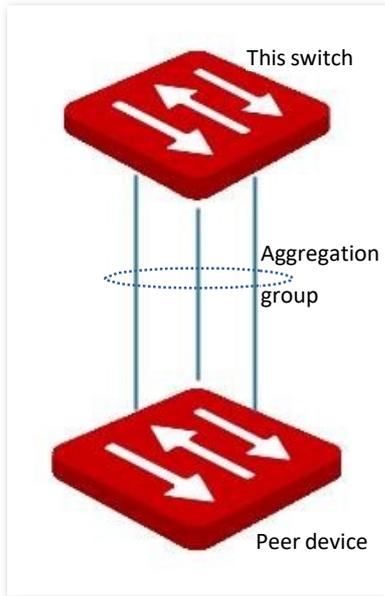
Nome	Descrição
ID	Especifica a ID do grupo de espelhamento.
Tipo de grupo de espelhamento	Essa opção oferece suporte apenas a tipos de grupo de espelhamento local.
Porta de origem	Especifica as portas cujos pacotes serão copiados. Várias portas podem ser selecionadas.
Porta de Destino	Os pacotes das portas de origem serão copiados para essa porta. Um grupo de espelhamento pode conter apenas uma porta de destino.

Nome	Descrição
	Especifica o tipo de pacote.
Direção	<ul style="list-style-type: none">- Ingresso: Os pacotes recebidos pelas portas de origem serão copiados para a porta de destino.- Egresso: 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.

4.1.3 Agregação de portas

A agregação de portas é usada para convergir várias portas físicas em um grupo de agregação lógica, e vários links físicos em um grupo de agregação são considerados como um link lógico. A função Agregação de Portas 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 peer. Enquanto isso, cada membro em um grupo de agregação faz backup dos dados um do outro dinamicamente, melhorando a confiabilidade da conexão.

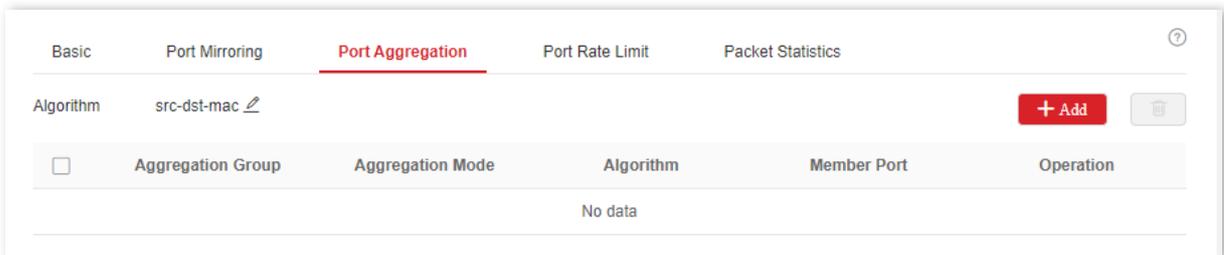
A topologia de rede da agregação de portas é mostrada a seguir.



 Nota

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

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



4 **Descrição do parâmetro**

5

Nome	Descrição
Grupo de Agregação	Especifica a ID dos grupos de agregação. Quando o Modo de Agregação é definido como Estático, a ID do Grupo de Agregação varia de 1 a 32. Quando o Modo de Agregação é definido como Dinâmico, a ID do Grupo de Agregação varia de 33 a 64.

Modo de agregação	de	<p>Há dois modos de agregação: Estático e Dinâmico.</p> <ul style="list-style-type: none">- Estática: Todas as portas membro no grupo de agregação convergem para uma porta lógica.- Agregação dinâmica: LACP (Link Aggregation Control Protocol) para todas as portas membro no grupo de agregação é habilitado, e as portas agregadas reais devem ser determinadas junto com o dispositivo peer através do protocolo LACP.
		<p> Nota</p> <p>O modo de agregação do switch precisa ser o mesmo do dispositivo peer. Caso contrário, os dados não poderão ser encaminhados corretamente ou os loops ocorrerão.</p>
Algoritmo		<p>Especifica os algoritmos de roteamento para o grupo de agregação:</p> <ul style="list-style-type: none">- src-dst-mac: As portas membro 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 membro 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 membro 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 número da porta de destino no pacote recebido.
Porto Membro		<p>Especifica os membros de um grupo de agregação.</p> <ul style="list-style-type: none">- No modo de agregação estática, as portas membro são membros de um grupo de agregação.- No modo de agregação dinâmica, as portas membro são as portas habilitadas pelo protocolo LACP, e as portas agregadas reais devem ser determinadas junto com o dispositivo peer através do protocolo LACP.

6

4.1.4 Limite de taxa de porta

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

Basic Port Mirroring Port Aggregation Port Rate Limit Packet Statistics						
Port	Egress Rate (Mbps)	Broadcast Packet	Multicast Packet	Unknown Unicast	Suppression Value	Operation
1	--	Disable	Disable	Disable	100	
2	--	Disable	Disable	Disable	100	
3	--	Disable	Disable	Disable	100	
4	--	Disable	Disable	Disable	100	
5	--	Disable	Disable	Disable	100	
6	--	Disable	Disable	Disable	100	
7	--	Disable	Disable	Disable	100	

Descrição do parâmetro

Nome	Descrição
Porta	Especifica a ID da porta.
Taxa de Egresso (Mbps)	Especifica a taxa máxima de saída da porta. "--" significa sem limite de taxa.
Pacote de Transmissão	Exibe se a função de supressão de pacotes de difusão está habilitada ou desabilitada.
Pacote Multicast	Exibe se a função de supressão de pacotes multicast está habilitada ou desabilitada.
Unicast desconhecido	Exibe se a função de supressão de pacotes unicast desconhecida está habilitada ou desabilitada.
Valor de supressão	Especifica a taxa total na qual as mensagens de difusão, multicast e unicast desconhecido podem passar quando a função de supressão está ativada. Não há supressão quando a função de supressão está desativada ou o valor de supressão é maior que a taxa de entrada ou saída.

4.1.1 Estatísticas de pacotes

Clique em **Alternar** > **Portas** > **Estatísticas de Pacotes** para entrar na página. Nesta página, você pode exibir e excluir as informações dos pacotes recebidos e enviados por cada porta.

Port	Transmitted Packets	Transmitted Byte	Received Packets	Received Byte	Operation
1	0	0	0	0	🔍
2	0	0	0	0	🔍
3	24862	16762963	17536	2650121	🔍
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	Especifica a 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 ver os detalhes dos pacotes recebidos e enviados por uma porta, clique no botão  atrás o porto.

Port	3		
Received Statistics		Transmission Statistics	
Total Bytes	2650121	Total Bytes	16762963
Broadcast Packets	499	Broadcast Packets	534
Unicast Packets	15143	Unicast Packets	0
Error Packets	0	Error Packets	0
Discard Packets	0	Discard Packets	0

Descrição do parâmetro

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

4.2 VLAN

4.2.1 Visão geral

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

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

VLAN 802.1Q

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

Este switch suporta três tipos de porta VLAN 802.1Q:

- Access: Uma porta de acesso pertence apenas a 1 VLAN, geralmente usada para conectar o computador.
- Trunk: uma porta trunk pode receber e enviar mensagens pertencentes a várias VLANs.
Normalmente, uma porta de tronco é usada para conexão de switches.

- Hybrid: uma porta híbrida pode receber e enviar mensagens pertencentes a várias VLANs. Normalmente, uma porta híbrida é usada para conexão de switches e pode ser conectada a um computador.

Os métodos de cada tipo de porta para processar pacotes são mostrados a seguir.

Tipo de link de porta	Recebendo dados marcados	Recebendo dados não marcados	Envio de dados
Porta de acesso			As mensagens são encaminhadas depois que as tags são removidas.
Porta tronco	Encaminhe para outras portas na VLAN correspondente de acordo com o VID na tag .	Encaminhe para outras portas na VLAN correspondente de acordo com o PVID nesta porta.	Se o valor VID da mensagem for o mesmo que seu valor PVID, a mensagem será encaminhada depois que as marcas forem removidas. Caso contrário <u>encaminhá-lo com suas etiquetas restantes.</u> Se o valor VID da mensagem pertence à VLAN marcada, a mensagem é encaminhada com suas tags restantes; se o valor VID da mensagem pertencer à VLAN não marcada, a mensagem será encaminhada depois que as tags forem removidas.
Porta híbrida			

4.1.1 Configuração de VLAN

Configurando regras de VLAN 802.1Q

Uma regra de VLAN é criada por padrão para garantir a comunicação entre switches nas configurações de fábrica. Todas as portas são definidas para serem membros dessa VLAN por padrão com a ID da VLAN de 1 e o endereço IP de 192.168.0.1. Esta regra não pode ser eliminada.

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

<input type="checkbox"/>	VLAN ID	VLAN Description	IPv4 Address	Subnet Mask	Operation
<input type="checkbox"/>	1	default	192.168.0.1	255.255.255.0	

Descrição do parâmetro

Nome	Descrição
VLAN ID	Especifica a ID da VLAN, usada para identificar a VLAN à qual o pacote pertence.
Descrição da VLAN	É usado para identificar grupos de VLAN. Se não estiver definido, a descrição padrão será "VLAN e ID de VLAN de quatro dígitos". Por exemplo, quando a ID da VLAN é 3, a descrição da VLAN é VLAN0003.
L3 Interface Virtual	Depois que a interface virtual L3 estiver habilitada, você poderá configurar o endereço IP e a máscara de sub-rede para a interface VLAN. Depois que as informações de endereço IP são configuradas, a comunicação entre VLANs pode ser realizada por meio de rotas estáticas.
Endereço IPv4	O endereço IP da interface VLAN pode ser configurado somente quando a Interface Virtual L3 está habilitada. Os dispositivos conectados às portas no grupo VLAN podem usar esse endereço IP para fazer logon na interface do usuário da Web do switch.
Máscara de sub-rede	Ele especifica a máscara de sub-rede da interface VLAN.

Configurando membros da porta

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

802.1Q VLAN		Port Member				?
Port	Link Type	PVID	Tagged	Untagged	Operation	⊞ Edit
1	Access	1	--	1		
2	Access	1	--	1		
3	Access	1	--	1		
4	Access	1	--	1		
5	Access	1	--	1		
6	Access	1	--	1		
7	Access	1	--	1		
8	Access	1	--	1		
9	Access	1	--	1		

Descrição do parâmetro

Nome	Descrição
Porta	Ele especifica a ID da porta.
Tipo de link	<p>Há suporte para três tipos de link de VLAN: 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 se conectar a terminais, como computadores. - Tronco: Uma porta tronco pode receber e transmitir mensagens pertencentes a várias VLANs, geralmente usada 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 se conectar a terminais.
Pvid	<p>Ele especifica a ID de VLAN padrão de uma porta.</p> <p>Ao receber pacotes não marcados, a porta os encaminha para a VLAN correspondente com base no PVID da própria porta.</p>
Etiquetado	Se o VID dos pacotes marcados recebidos pela porta for o mesmo com a VLAN marcada, a porta reterá as tags dos pacotes e as transmitirá.
Untagged	Se o VID dos pacotes marcados recebidos pela porta for o mesmo com a VLAN não marcada, a porta removerá as tags dos pacotes e as transmitirá.

4.2.2 Exemplo de configuração de VLAN 802.1Q

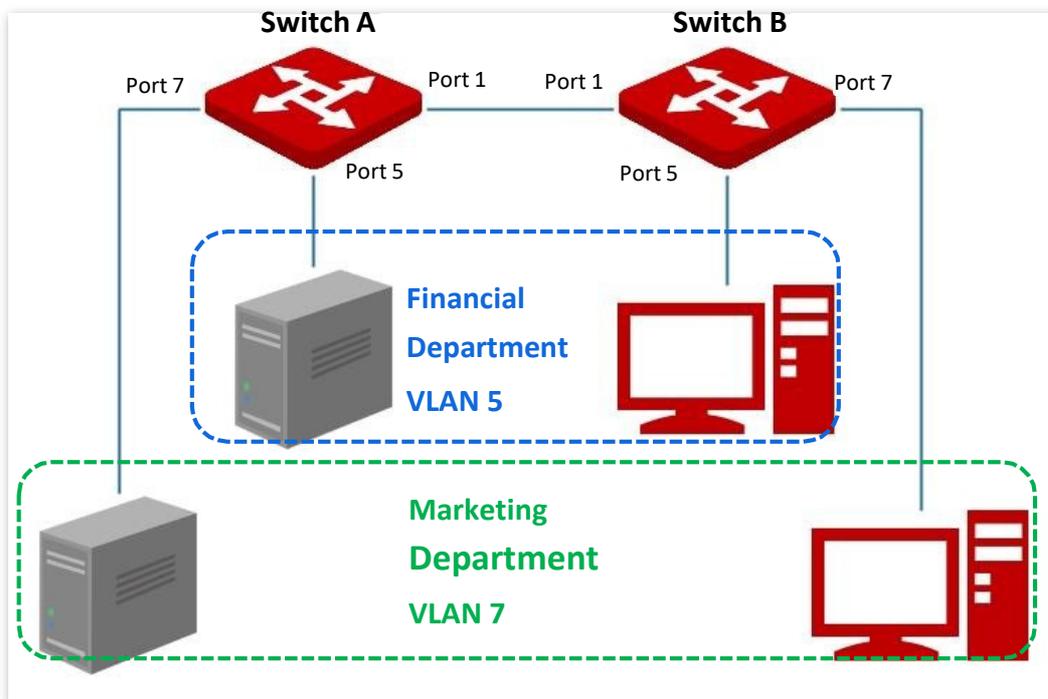
Requisitos de rede

Os funcionários do departamento financeiro e do departamento de marketing de uma empresa trabalham no segundo andar, enquanto os servidores desses dois departamentos estão 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 uma 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 VLAN 7.



Procedimento de configuração

I . Configurando o Switch A

1. Adicionar VLANs.

- (1) Faça login na interface do usuário da Web do Switch A e clique em **Switching > VLAN > 802.1Q VLAN**.
- (2) Clique em **+Adicionar** e insira as seguintes informações na janela pop-out e clique em **Confirmar**.
 - Defina a **ID da VLAN** como **5**.
 - Defina **Descrição da VLAN** como **Finanças**.
- (3) Repita a etapa (2) e adicione outra VLAN com o ID da VLAN de **7** e a **Descrição** da **VLAN** de **Marketing**.

802.1Q VLAN Port Member

+ Add

<input type="checkbox"/>	VLAN ID	VLAN Description	IPv4 Address	Subnet Mask	Operation
<input type="checkbox"/>	1	default	192.168.60.100	255.255.255.0	
<input type="checkbox"/>	5	Finance	--	--	
<input type="checkbox"/>	7	Marketing	--	--	

2. Configurando o atributo de porta.

- (1) Clique em **Alternar > membro da porta > da VLAN**.
- (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 **Tipo de link** como Tronco e Marcado como 5, 7.

802.1Q VLAN Port Member

Edit

Port	Link Type	PVID	Tagged	Untagged	Operation
1	Trunk	1	5,7	1	
2	Access	1	--	1	
3	Access	1	--	1	
4	Access	1	--	1	
5	Access	5	--	5	
6	Access	1	--	1	
7	Access	7	--	7	
8	Access	1	--	1	

II. Configurando o Switch B

Consulte as etapas de configuração do Switch A.

----Fim

Verificação

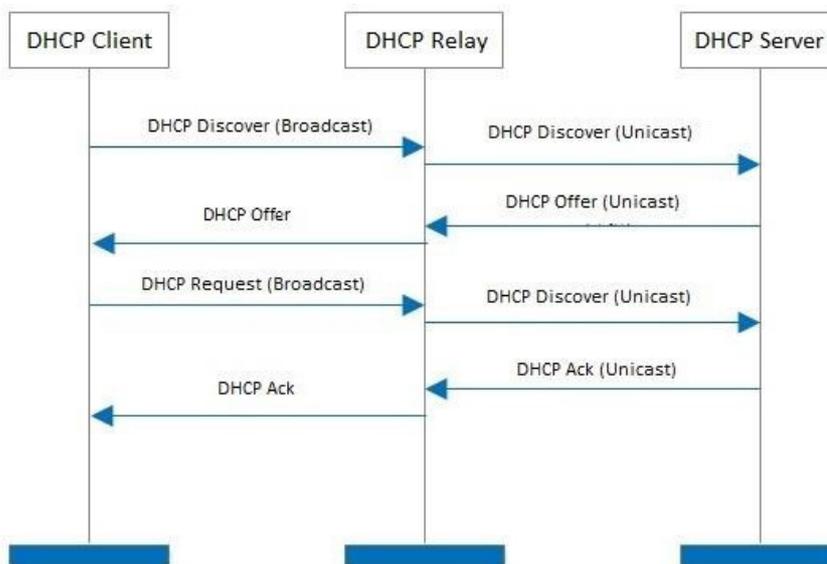
A equipe pode acessar o servidor de seu departamento, mas não pode acessar o servidor do outro departamento. O pessoal do mesmo departamento pode comunicar entre si, mas não pode comunicar com o pessoal de outros departamentos.

4.3 Retransmissão DHCP

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

Com a função de Retransmissão DHCP habilitada, 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 entre segmentos de rede, permitindo que clientes DHCP em várias redes compartilhem um mesmo servidor DHCP.

Os princípios de funcionamento do DHCP Relay são mostrados abaixo.



- Quando a retransmissão DHCP recebe as mensagens de descoberta ou solicitação DHCP enviadas pelo cliente DHCP em difusão, ela preenche o endereço IP da retransmissão 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 Opção 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 local dos clientes DHCP. Você pode usar essa opção para localizar o cliente DHCP, implementando assim a segurança e o controle de cobrança para os 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 desabilitada. Depois de ativado, o mecanismo de funcionamento da Opção 82 deste switch é mostrado a seguir.

4	Tipo de Política de processamento
Mensagem de solicitação DHCP sem a opção 82	Adicione o conteúdo padrão dessa opção às informações da Opção 82 da mensagem de solicitação DHCP e encaminhe a mensagem.  Dica O conteúdo padrão desse 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 a opção 82	As mensagens de solicitação DHCP são processadas de acordo com as seguintes diretivas de configuração. <ul style="list-style-type: none">- Substituir: Substitua as informações originais da Opção 82 na mensagem pelo conteúdo padrão do switch e encaminhe-o.- Reter: Manter o estado original da Opção 82 na mensagem e encaminhá-la.- Descarte: 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 **Alternar > Retransmissão DHCP** para entrar na página. Nesta página, você pode configurar as regras de Retransmissão DHCP.

Descrição do parâmetro

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.
Política da Opção 82	O switch oferece suporte a três políticas: <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.
	<ul style="list-style-type: none"> - Reter: Quando o DHCP Relay recebe mensagens de solicitação DHCP, ele mantém o estado original da Opção 82 e encaminha as mensagens. - Descarte: A Retransmissão DHCP descarta a mensagem de solicitação DHCP com a Opção 82 e encaminha a mensagem de solicitação DHCP sem a Opção 82.
VLAN ID	É a espécie da VLAN à qual os clientes pertencem. A VLAN já deve existir e sua interface virtual L3 está configurada.
IP do servidor	Ele especifica o endereço IP do servidor DHCP remoto. O endereço IP do servidor DHCP remoto não pode pertencer à mesma rede segmento como o da VLAN a que pertencem os clientes.....

4.3 DHCP snooping

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

- Garante que os clientes DHCP possam obter endereços IP dos servidores corretos.

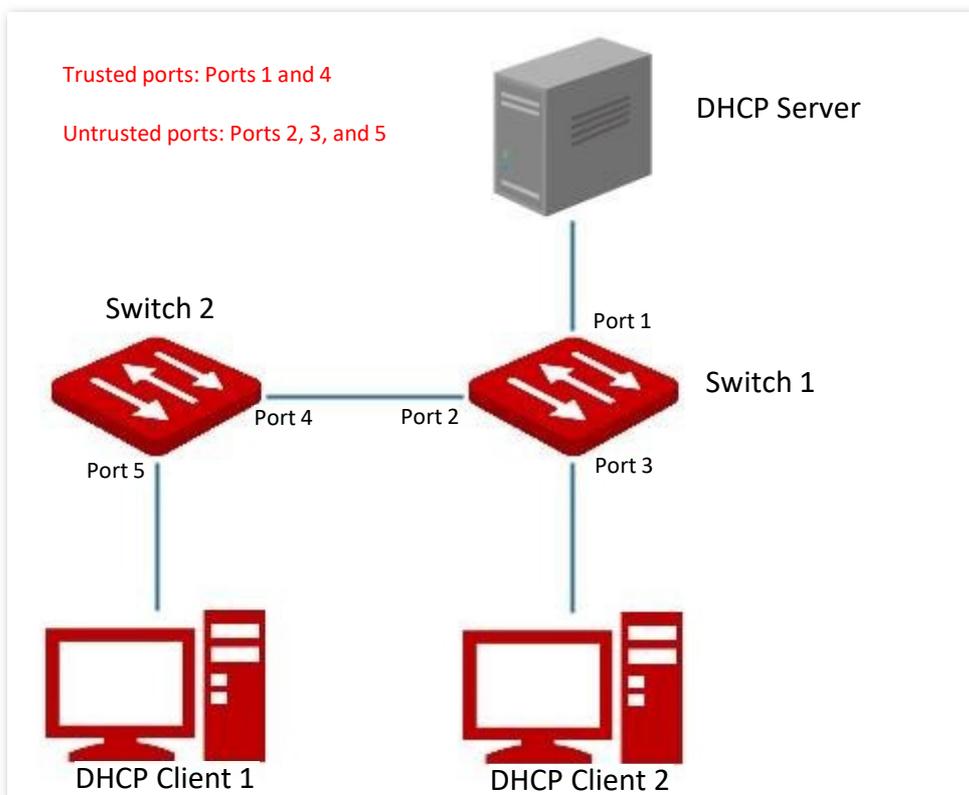
A porta que se conecta ao servidor DHCP autorizado é a porta confiável e outras portas são portas não confiáveis. O switch encaminha as mensagens DHCP recebidas pelas portas confiáveis e descarta as mensagens de resposta recebidas pelas portas não confiáveis do servidor DHCP, de modo a garantir que os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

- Registra as entradas da tabela DHCP Snooping.

Ao realizar verificar 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 um base importante para validação ARP.

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

5



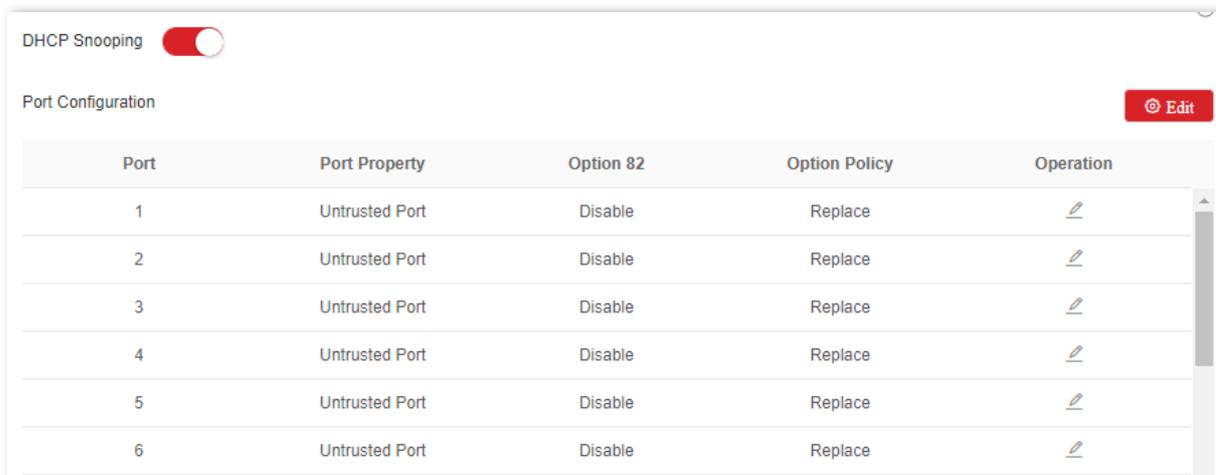
Nota

A função Snooping DHCP só está disponível quando essa função está

habilitada e o comutador está entre o cliente DHCP e o servidor DHCP (ou retransmissão DHCP) na rede de conexão. Quando a opção está entre o servidor DHCP e a retransmissão DHCP, a função de espionagem DHCP não está disponível.

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

7



8 Descrição do parâmetro

9

Nome	Descrição
Porta	Especifica a ID da porta.
Propriedade da porta	<p>É usado para configurar a propriedade de espionagem DHCP da porta atual, incluindo porta confiável ou porta não confiável.</p> <ul style="list-style-type: none"> - Porta confiável: Está conectado 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, desabilitando assim os falsos servidores DHCP erguidos de forma privada de atribuir endereços IP aos clientes.
Opção 82	<p>É usado para habilitar ou desabilitar a Opção 82. A opção 82 registra as informações de localização do cliente DHCP. A política de opção entra em vigor quando a Opção 82 está habilitada. Consulte a opção 82 para o seu mecanismo de funcionamento.</p>
Política de Opções	<p>Três políticas de opção 82 são suportadas por esta opção:</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 a Retransmissão DHCP recebe mensagens de solicitação DHCP, ela mantém o estado original da Opção 82 e encaminha a mensagem. - Descarte: A Retransmissão DHCP descarta a mensagem de solicitação DHCP com a Opção 82 e encaminha a mensagem de solicitação DHCP sem a Opção 82.

9.3 Spanning tree Protocolo (STP)

4.3.1 Visão geral

A STP 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 de STP: STP (Spanning Tree Protocol), RSTP (Rapid Spanning Tree Protocol) e MSTP (Multi Spanning Tree MST).

STP

STP é um protocolo de rede baseado no IEEE 802.1d. É um protocolo que garante um loop-free topologia para na rede local e fornecer links redundantes de backup. Os dispositivos sob este protocolo descobrem os loops na rede comunicando-se uns com os outros, e bloqueiam seletivamente algumas portas e, eventualmente, estabelecem uma estrutura de STP sem loops, de modo a impedir o declínio da capacidade de processamento de mensagens dos dispositivos devido à proliferação contínua e circulação interminável de mensagens na rede de loop.

Mensagem de protocolo STP

Para implementar a função de STP, os switches na rede transferem BPDUs (Bridge Protocol Data Unit) entre si para trocar informações. As BPDUs carregam as informações necessárias para que os switches calculem a STP.

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

- Configuração BPDUs: É usado para cálculo de STP e manutenção de topologia de STP.
- TCN BPDUs (Topology Change Notification BPDUs): É usado para notificar as alterações da estrutura da topologia de rede.

Conceitos básicos de STP

■ Bridge ID

O Bridge ID 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 raiz bridge é a ponte com o menor ID de ponte.

■ Root bridge

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

Inicialmente, todos os dispositivos se consideram como pontes raiz. Eles geram suas próprias BPDUs de configuração e as enviam periodicamente. Quando a topologia de rede se torna estável, somente o dispositivo de ponte raiz pode enviar BPDUs de configuração para fora e outros dispositivos só podem encaminhar esses BPDUs.

■ **Root port**

A root port é a porta em um dispositivo de ponte não raiz que tem o menor custo de caminho da ponte para a ponte raiz, responsável pela comunicação com a ponte raiz. Há apenas uma porta raiz no dispositivo de ponte não raiz e nenhuma porta raiz no dispositivo de ponte raiz.

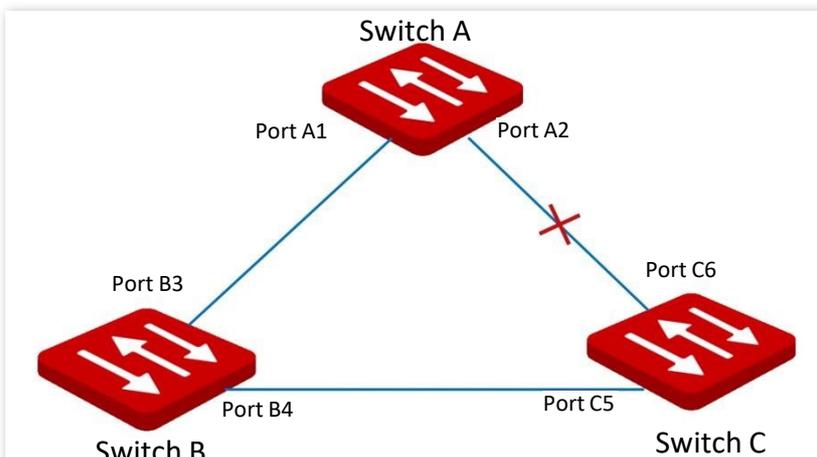
■ **Designated bridge e designated port**

- Designated bridge: 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.
- Designated port: Quanto a um dispositivo, é a porta que encaminha BPDUs para o host. Quanto a uma LAN, é a porta que encaminha BPDUs no mesmo segmento de rede.

■ **Custo do caminho**

É um parâmetro para escolher o caminho do link pelo STP. Ao calcular o custo do caminho, o STP escolhe os melhores links e bloqueia os links redundantes, de modo a desramificar a rede de loop para formar uma rede sem loop topológico de árvore.

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



Após o cálculo, a opção A é selecionada como a bridge raiz e o link entre as portas A2 e C6 é bloqueado.

- Bridges: O switch A é a bridge raiz da rede, enquanto o switch B é a bridge designada do switch C.
- Portas: A porta B3 e a porta C5 são as portas raiz do switch B e do switch C, respectivamente. A porta A1 e a porta B4 são as portas designadas do switch A e do switch B, respectivamente. A porta C6 é a porta de bloqueio do switch C.

Prioridade BPDU no modo STP

Quanto menor for o ID da bridge, maior será a prioridade da bridge. Se o ID da bridge raiz for o mesmo, os custos do caminho raiz serão comparados. O método de comparação é assumir o caminho raiz custo em BPDU e o custo de caminho correspondente a esta porta para ser S, então o BPDU com S menor tem maior prioridade. Se os custos do caminho raiz forem os mesmos, compare o ID da bridge designado, o ID da porta designada e o ID da porta que recebe a BPDU sucessivamente, uma com a menor ID tem prioridade mais alta.

Processo de computação STP

1. Status inicial

Inicialmente, cada porta do switch gera uma BPDU referente ao switch como a bridge raiz, com o custo do caminho raiz sendo 0, o ID da bridge designada sendo o ID do switch e o porto designado sendo ele mesmo.

2. Seleção ideal de BPDU

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

Pass	Conteúdo
0	
1	Recebendo BPDU com prioridade mais baixa: Se a prioridade da BPDU recebida por uma porta for menor que a da própria porta, o switch descarta a BPDU recebida e não lida com a BPDU dessa porta. Recebendo BPDU com prioridade mais alta: Se a prioridade da BPDU recebida for maior que a da própria porta, o switch substituirá a BPDU da porta pela recebida.
2	O switch seleciona o melhor BPDU comparando BPDUs em todas as portas.

3. Seleção de bridge raiz

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

4. Seleção de porta raiz e porta designada

O processo de seleção é apresentado no quadro seguinte:

Passo	Conteúdo
1	Para cada switch (exceto a bridge raiz), a porta que recebe a BPDU ideal é escolhida como a porta raiz do switch.
2	<p>O switch calcula uma porta designada BPDU para cada porta de acordo com o BPDU da porta raiz e o custo do caminho da porta raiz.</p> <ul style="list-style-type: none">- O ID da bridge raiz é substituído pelo da porta raiz.- O custo do caminho raiz é substituído pela soma do custo do caminho raiz da porta raiz BPDU e o custo do caminho correspondente à porta raiz.- O ID da bridge designada é substituído pelo do próprio switch.- A ID da porta designada é substituída pela própria ID da porta.
3	O switch compara a BPDU calculada com a BPDU da porta cuja função requer ser

Passo	Conteúdo
	determinou, e lidar com o porto de acordo com diferentes resultados de comparação.
	<ul style="list-style-type: none">- Se a BPDU calculada tiver precedência sobre a BPDU da porta, a porta é escolhida como a porta designada com a sua BPDU substituída pela BPDU calculada, e envia regularmente a BPDU.- Se a BPDU desta ort tiver precedência sobre a BPDU calculada, a BPDU desta porta não é alterada e a porta é bloqueada. A porta só recebe BPDUs, mas não pode encaminhar BPDU ou outros dados.



Dica

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

Temporizador STP

■ Olá Tempo

Especifica o intervalo para a bridge raiz enviar mensagens BPDU para outros switches, usado para testar se os links funcionam mal.

■ Tempo máximo de envelhecimento

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

■ Atraso de encaminhamento

Especifica o tempo de atraso que a migração do estado da porta leva depois que a topologia de rede é alterada.

O mau funcionamento do link leva ao recálculo do STP na rede, caso em que a estrutura do STP será alterada de acordo. No entanto, como as novas BPDUs não podem ser espalhadas 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 portas designadas começam a encaminhar dados após o atraso de encaminhamento duplo, o que garante que as novas BPDUs tenham sido espalhadas para toda a rede.

RSTP

O RSTP é definido pelo padrão IEEE 802.1w e compatível com o IEEE 802.1d STP. Além de uma rede livre de loop e links redundantes, ele apresenta convergência rápida. Se todas as bridges em uma LAN suportarem RSTP, ela habilitará uma geração rápida de árvore de topologia quando a topologia de rede for alterada (árvore de topologia STP tradicional: 50 segundos, árvore de topologia RSTP: 1 segundo).

O RSTP determina a topologia de rede trocando BPDUs entre switches. No entanto, o formato BPDUs do RSTP difere do formato do STP. Quando a topologia está mudando, RST-BPDU

As mensagens são espalhadas por inundações para notificar a mudança para toda a rede.

Condições para a migração rápida do estado das portas raiz e das 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 poderá 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 obtiver resposta do switch downstream por meio de handshake.

■ **Edge Port**

Uma edge port é uma porta designada na borda da rede de comutação. Ele está diretamente conectado a dispositivos terminais. Uma porta de borda pode transitar para o estado de encaminhamento imediatamente sem passar por estados de escuta e aprendizado. Se ele receber uma BPDU, ele imediatamente se transformará de uma porta de borda para uma porta de

STP comum e ingressará na geração de STP.

■ **Porta P2P**

Uma porta P2P usada para se conectar a outros switches. Em RSTP/MSTP, todas as portas que operam no modo full-duplex são consideradas portas P2P.

MSTP

Desvantagens do STP e RSTP em ambientes de trabalho comuns:

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

O MSTP é definido pelo padrão IEEE 802.1s e compatível com STP e RSTP. Não só apresenta convergência rápida, mas também permite que fluxos de dados de diferentes VLANs sejam encaminhados ao longo dos caminhos respectivamente, permitindo assim um melhor mecanismo de compartilhamento de carga para links redundantes, o que compensa as limitações de STP e RSTP.

Características do MSTP:

- O MSTP oferece suporte ao mapeamento de VLANs para as instâncias de STP por meio de VLAN-to-tabela de mapeamento de instância e realiza o balanceamento de carga mapeando várias VLANs para uma instância.
- O MSTP divide a rede de STP em várias regiões, cada uma das quais contém STP internas que são independentes umas das outras.
- O MSTP poda uma rede de loop em uma rede de árvore sem loop para evitar a proliferação contínua e a circulação infinita de mensagens, e também fornece várias caminhos redundantes para encaminhamento de dados, garantindo assim o balanceamento de carga no processo de encaminhamento de dados.

■ **Região MST**

A região MST (Multiple Spanning Tree Regions) é composta por vários dispositivos em uma rede de switch e seus segmentos de rede.

Esses dispositivos têm os seguintes recursos:

- Um protocolo de STP habilitado
 - Mesmo nome de região
 - Mesmo resumo de configuração (a configuração da relação de mapeamento entre VLAN e MSTI é a mesma)
 - Mesmo nível de revisão MSTP
 - Fisicamente ligados entre si

■ **MSTI**

O MSTP pode gerar várias STP independentes em uma região do MST, e cada STP é considerada como uma MSTI (Instância de STP Múltipla). Na região do MST, o MSTP

gera várias STP de acordo com a tabela de mapeamento de VLAN para instância e mapeia as VLANs para as árvores de abrangência. O método de cálculo de STP do MSTP é o mesmo do STP.

■ **IST**

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

■ **CST**

CST (Common Spanning Tree) é uma única STP que conecta todas as regiões do MST dentro da rede. O MSTP considera as regiões do MST como dispositivos separados e gera a conexão CST com todas as regiões.

■ **CIST**

CIST (Common and Internal Spanning Tree) é uma única STP que conecta todos os dispositivos dentro da rede. É composto pelos ISTs em todas as regiões do MST e pelo CST.

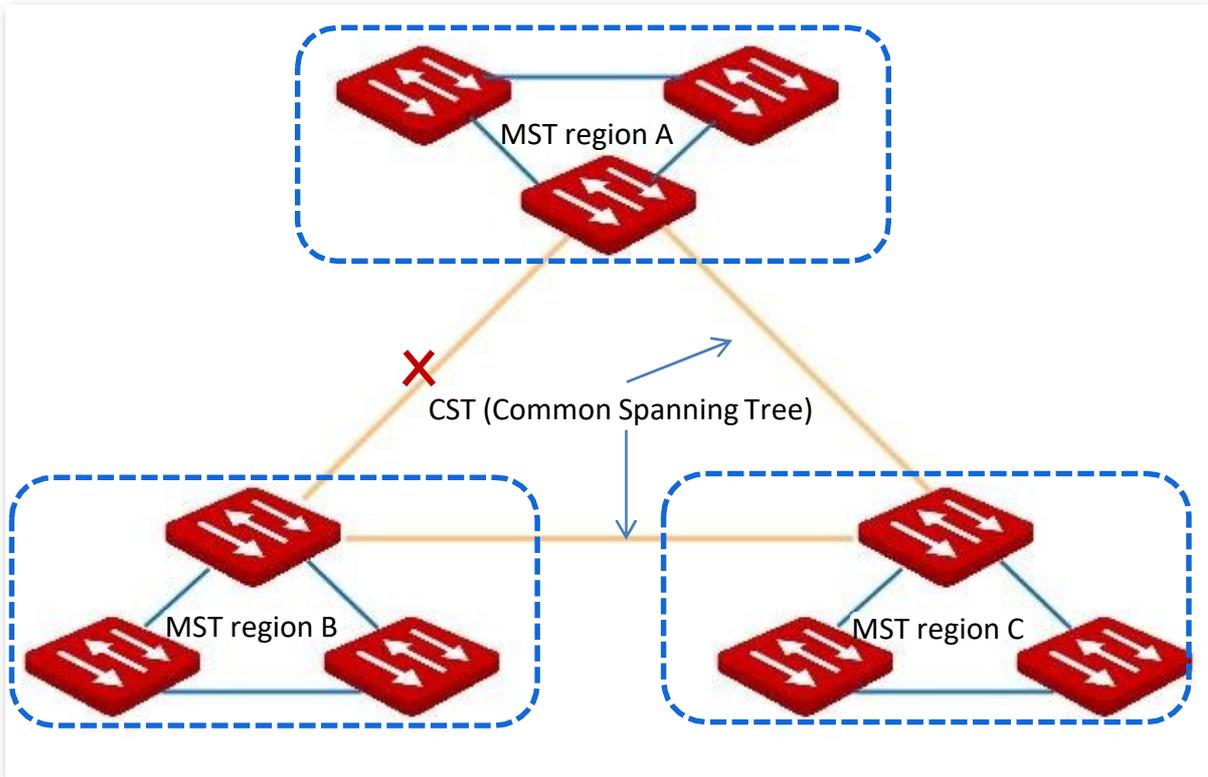
■ **Regional Root**

Regional Root é a bridge raiz do IST ou MSTI dentro da região MST. As raízes regionais variam de acordo com as diferentes topologias de árvores.

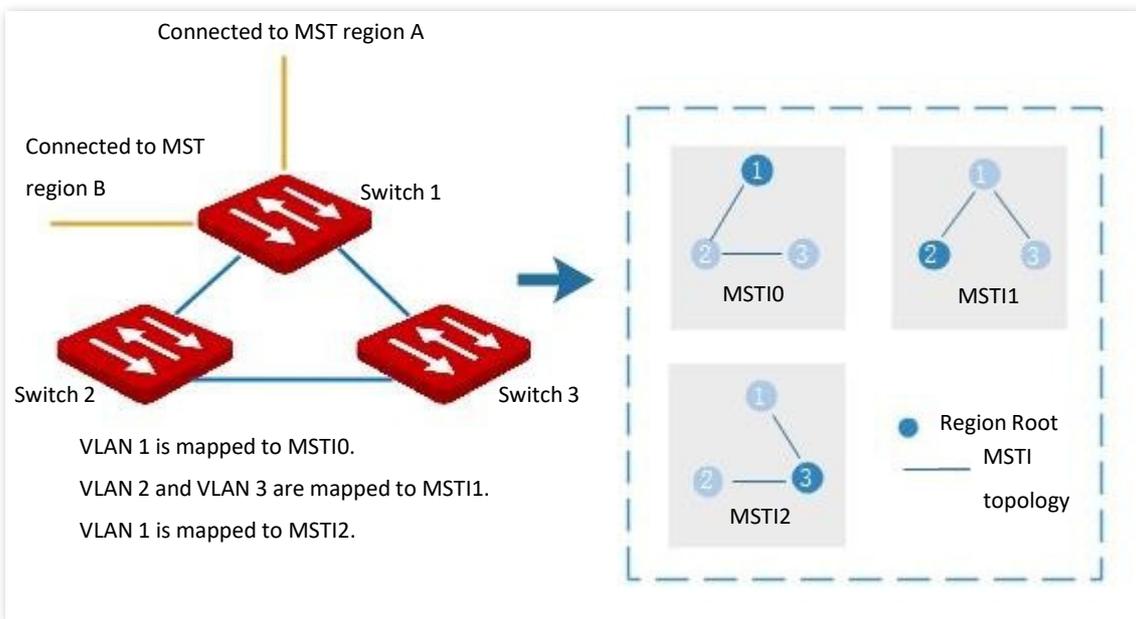
■ **Common Root Bridge**

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

Semelhante ao STP, o MSTP usa BPDUs para calcular árvores de abrangência, exceto que BPDUs carregam informações de configuração do MSTP. O diagrama de conceito básico do MSTP é mostrado a seguir.



A topologia de cada MSTI na região C do MST é a seguinte.



Status da porta

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

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

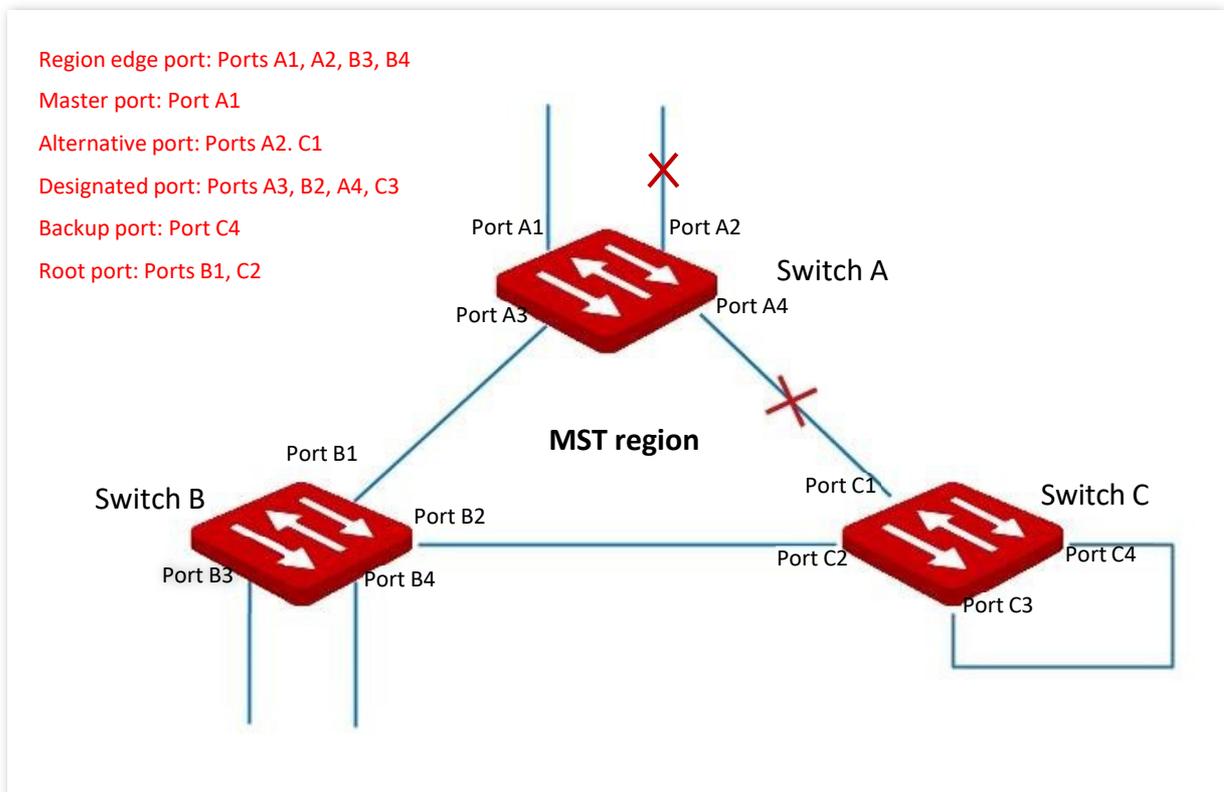
- Descarte: A porta não recebe ou encaminha dados, nem envia BPDUs ou aprende endereços, mas recebe BPDUs.
- Desabilitado: a porta não está fisicamente vinculada.

Função de porta

No MSTP, há diferentes funções das portas:

- Porta raiz: Ela tem o menor custo passado para a bridge raiz e é responsável por encaminhar dados de uma bridge não raiz para a bridge raiz.
- Porta designada: encaminha dados para o segmento ou dispositivo de rede downstream.
- Porta mestra: Está no caminho mais curto da região MST até a bridge raiz comum, conectando a região MST à bridge raiz comum.
- Porta alternativa: atua como a porta de backup para a porta raiz ou porta mestra.
- Porta de backup: atua como a porta de backup para a porta designada.
- Desativar porta: é uma porta que não está fisicamente vinculada.

As funções de porta são mostradas como o diagrama a seguir:



9.3.1 Global

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

Global	Port Configuration	Port Statistics	Instance Info
Status	<input checked="" type="checkbox"/>		
Mode	<input type="text" value="MSTP"/>		

Descrição do parâmetro

Nome	Descrição
Estado	É usado para habilitar ou desabilitar a função de STP.
Modo	O switch suporta três modos de STP: STP, RSTP e MSTP. STP: Protocolo de STP. RSTP: Rapid Spanning Tree Protocol, compatível com o protocolo STP, caracterizando-se com convergência rápida. MSTP: Multiple Spanning Tree Protocol, compatível com RSTP e STP, proporcionando melhor mecanismo de compartilhamento de carga para links redundantes.

Configuração de bridges

Bridge Configuration

Maximum Aging Time s (Range: 6 to 40)

Hello Time s (Range: 1 to 10)

Forwarding Delay s (Range: 4 to 30)

Maximum Hops (Range: 6 to 40)

Note: Maximum aging time $\geq 2 \times (\text{Hello Time} + 1)$ Maximum aging time $\leq 2 \times (\text{Forwarding Delay} - 1)$

Bridge Priority

Descrição do parâmetro

Nome	Descrição
Tempo máximo de envelhecimento	Especifica a duração máxima durante a qual a BPDU pode ser mantida no switch. A configuração deve atender às seguintes fórmulas: <ul style="list-style-type: none">- Tempo máximo de envelhecimento $\geq 2 \times (\text{Olá tempo} + 1)$- Tempo máximo de envelhecimento $\leq 2 \times (\text{atraso de encaminhamento} - 1)$
Olá Tempo	Especifica o intervalo no qual o switch envia BPDU, que é definido como 2 segundos

Nome	Descrição
	por padrão.
Atraso de encaminhamento	Especifica o atraso que a migração do estado da porta leva depois que a topologia de rede é alterada, que é definida como 15 segundos por padrão.
Lúpulo máximo	Especifica o número máximo da BPDU que pode ser encaminhado, usado para limitar a escala da STP.
Prioridade da bridge	Especifica a prioridade do sistema de um switch na participação no cálculo da STP. A prioridade é um critério importante pelo qual a bridge raiz é determinada. O switch com a prioridade mais alta será escolhido como a bridge raiz em condições iguais.

Configuração de domínio MSTP

MSTP Domain Setting

Region Name (Range: 1 to 32 characters)

Revision (Range: 0 to 65535)

Digest

[Confirm](#)

Descrição do parâmetro

Nome	Descrição
Nome da Região	Especifica a identidade da Região MST. O valor padrão é o endereço MAC de o interruptor.
Revisão	Especifica o nível de revisão MSTP, que é definido como 0 por padrão.
Digerir	Especifica o valor calculado com base no interior do mapeamento da VLAN.

Instância MSTP

MSTP Instance				
	Instance ID	VLAN Mapping List	Bridge Priority	Operation
<input type="checkbox"/>	0	1	32768	--

Descrição do parâmetro

Nome	Descrição
ID da instância	São permitidas no máximo 32 instâncias. 0 indica STP interna. A STP é calculada por cada instância separadamente.
Lista de mapeamento de VLAN	Especifica a VLAN de mapeamento de instância.
Prioridade da bridge	Especifica a prioridade do sistema de instâncias usada para a eleição de bridge raiz de instâncias em regiões MST.

Bridge raiz especificada

Specified Root Bridge			
Bridge ID	32768:0050.438a.8a8a	Root Bridge ID	32768:0050.438a.8a8a
Region Root ID	32768:0050.438a.8a8a	Root Port	none
Root Path Cost	0	Internal Root Path Cost	0
Topology Status	Topological_stability	Last Changed Time	2019-05-27-19:27

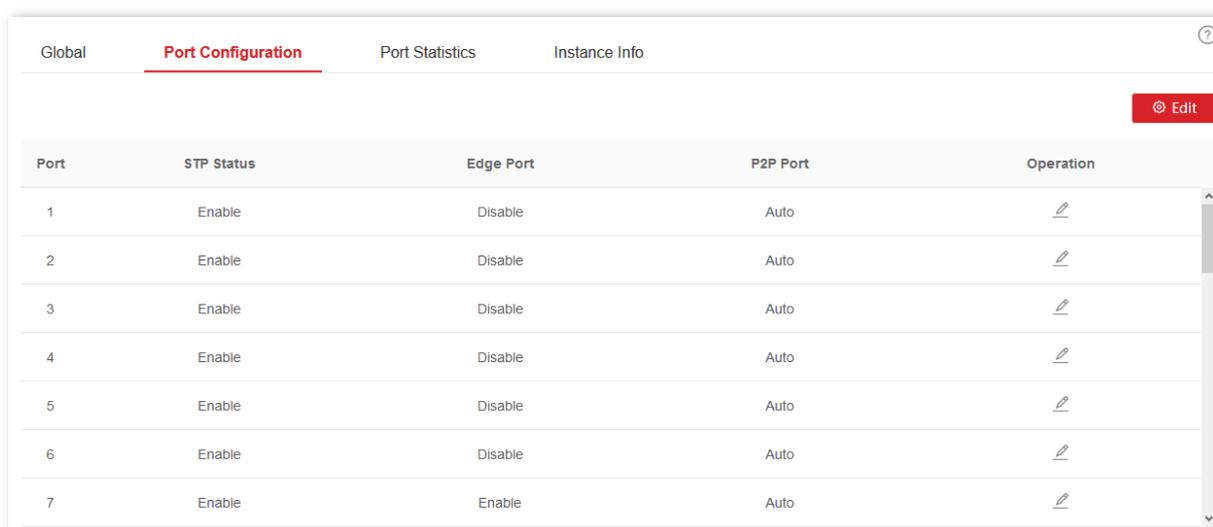
Descrição do parâmetro

Nome	Descrição
ID da bridge	Especifica a prioridade da bridge e o endereço MAC da bridge desse switch.
ID raiz da região	Especifica a prioridade da bridge e o endereço MAC da bridge raiz regional na região desse switch.
Custo do caminho raiz	Especifica a soma do custo do caminho da porta raiz e o custo do caminho raiz de todos os pacotes de switches passados. O custo do caminho raiz da bridge raiz é 0.
Status da topologia	Especifica o status da topologia da STP desse switch. <ul style="list-style-type: none"> - Topology_calculation: A porta é instável durante o cálculo da STP e os pacotes não podem ser encaminhados. Normalmente, com os parâmetros de tempo padrão, o status do 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 é estável e a rede é normal.
ID da bridge raiz	Para STP e RSTP, Especifica a prioridade da bridge e o endereço MAC da bridge raiz; enquanto para MSTP, Especifica a prioridade da bridge e o endereço MAC da bridge raiz comum.

Porta raiz		Especifica a porta mais próxima da bridge raiz em um switch que não seja de bridge raiz.
Custo do caminho interno	do raiz	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 porta raiz. Quanto menor for o valor, maior será a prioridade.
Última alteração de horário		Especifica a hora da última alteração de topologia.

4.3.2 Configuração de porta

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



Port	STP Status	Edge Port	P2P Port	Operation
1	Enable	Disable	Auto	
2	Enable	Disable	Auto	
3	Enable	Disable	Auto	
4	Enable	Disable	Auto	
5	Enable	Disable	Auto	
6	Enable	Disable	Auto	
7	Enable	Enable	Auto	

Descrição do parâmetro

Nome	Descrição
Porta	Especifica a ID da porta.
STP Status	Indica se a função STP está habilitada ou não. Somente quando a função STP na Configuração Global e na Configuração de Porta estiver habilitada, a porta poderá ingressar no cálculo da STP.
Edge Port	A porta de borda pode migrar rapidamente para o estado de encaminhamento do estado de congestionamento. Não há necessidade de esperar o tempo de atraso. A porta de borda é comumente conectada a terminais. Ao receber mensagens BPDU, a porta de borda é alterada para uma porta que não seja de borda. Todas as portas são portas de borda por padrão. <ul style="list-style-type: none"> - Desativar: Esta porta é uma porta sem borda. - Habilitar: Esta porta é uma porta de borda.
P2P Port	Uma porta P2P pode executar uma migração rápida. No modo RSTP/MSTP, todas as portas no modo full-duplex são consideradas como portas P2P. A porta padrão identifica automaticamente os links. <ul style="list-style-type: none"> - Auto: A porta P2P pode ser identificada automaticamente. - Desativar: Esta porta é uma porta P2P. - Ativar: Esta porta não é uma porta P2P.

4.3.3 Estatísticas de portas

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

Port	Transmit				Receive				Discard	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	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	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0

Descrição do parâmetro

Nome	Descrição
Porta	Especifica a ID da porta.
MSTP	Especifica o número de configuração BPDU 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 configuração BPDU com informações STP transmitidas ou recebidas pela porta.
TCN	Especifica o número de mensagens TCN BPDU transmitidas ou recebidas pela porta.
Desconhecido	Especifica o número de pacotes STP desconhecidos descartados.
Illegal	Especifica o número de pacotes STP de erro descartados.

4.3.4 Informações da instância

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

Port	Port Role	Port Status	Region Root ID	Designated Bridge	Designated Port	Priority	Path Cost	Operation
1	Disabled	Disabled	32768-0050.438a...	32768-0050.438a...	0	128	200000000	
2	Disabled	Disabled	32768-0050.438a...	32768-0050.438a...	0	128	200000000	
3	Disabled	Disabled	32768-0050.438a...	32768-0050.438a...	0	128	200000000	
4	Disabled	Disabled	32768-0050.438a...	32768-0050.438a...	0	128	200000000	
5	Disabled	Disabled	32768-0050.438a...	32768-0050.438a...	0	128	200000000	
6	Disabled	Disabled	32768-0050.438a...	32768-0050.438a...	0	128	200000000	

Descrição do parâmetro

Nome	Descrição
ID da instância	É usado para selecionar o ID da instância para verificar as informações de estado do STP da instância.
Porta	Especifica a ID da porta.
Função da porta	Especifica a função que a porta desempenha na instância da Spanning Tree. Para obter mais detalhes, consulte Função de porta .
Status da porta	Especifica o status operacional atual da porta. Para obter mais detalhes, consulte Status da porta .
ID raiz da região	Especifica a prioridade da bridge e o endereço MAC da bridge raiz regional.
Bridge designada	Especifica o ID da bridge do switch que se conecta a esse switch e é usado para encaminhar mensagens BPDU para o switch. O ID de bridge designado da porta raiz e da porta de backup é o ID de bridge do switch usado para enviar mensagens BPDU; enquanto o ID de bridge designado da porta designada é o ID de bridge do próprio switch.
Porto Designado	Especifica a porta para a qual a bridge designada encaminha mensagens BPDU.
Prioridade	Especifica a prioridade da porta no cálculo da Spanning Tree. Quando o ID da bridge raiz, o custo do caminho raiz e o ID da bridge são os mesmos, a prioridade é um critério importante para determinar se a porta está selecionada como a porta raiz. Quanto menor for 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 de caminho na instância dentro da região MST, também uma referência para a seleção de porta raiz. Quanto menor o valor, maior será a prioridade.

4.4 Configuração do LLDP

4.4.1 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 sistema e configuração informação.

O LLDP (Link Layer Discovery Protocol) fornece um método padrão de descoberta de camada de link que organiza os principais recursos, endereço de gerenciamento, identificador de dispositivo e informações de identificador de interface de dispositivos desse lado em diferentes TLVs (Tipo/Comprimento/Valor) e os encapsula em LLDPDUs (Link Layer Discovery Protocol Data Unit) para liberar para vizinhos aos quais eles estão diretamente conectado. Depois de receber essas informações, os vizinhos irão salvá-las como 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 em mensagem LLDP. Cada LLDPDU é uma sequência de estruturas de valor de comprimento tipo (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 TLV do endereço de gerenciamento da mensagem LLDP.

Mecanismo operacional

O LLDP é um protocolo unidirecional para notificação ou recuperação de

informações. Ele notifica um método operacional sem necessidade de confirmação e indisponível para consulta.

Principais trabalhos do LLDP:

- Inicialize e mantenha informações no MIB local.
- Obtenha as informações necessárias do MIB local e encapsula-as nos quadros LLDP. Há duas maneiras de acionar o envio de quadros LLDP: uma é acionada pela expiração do temporizador e a outra é acionada pela alteração de status do dispositivo.
- Identificar e processar os quadros LLDPDU recebidos.
- Mantenha os MIBs LLDP dos dispositivos remotos.
- Notifique as alterações de informações MIB dos dispositivos locais ou remotos.

■ **Status operacional do LLDP**

Existem quatro status operacionais do LLDP:

- Enviar & Receber: Nesse modo, o switch pode enviar e receber mensagens LLDP.
- Somente envio: nesse modo, o switch só pode enviar mensagens LLDP.
- Somente recebimento: nesse modo, o switch só pode receber mensagens LLDP.
- Desativar: nesse modo, o switch não pode enviar ou receber mensagens LLDP.

Quando o status operacional do LLDP muda, sua máquina de estado do protocolo LLDP é reinicializada. Você pode configurar o **Atraso de Inicialização** para evitar inicializações frequentes causadas por alterações frequentes do status operacional. Se você configurou o **Atraso de Inicialização**, o switch deverá aguardar o tempo especificado para inicializar o LLDP depois que o status operacional do LLDP for alterado.

■ **Mecanismo de transmissão de mensagens LLDP**

Quando o status operacional da porta é **Enviar e receber** ou **Enviar somente**, o switch envia mensagens LLDP para seus dispositivos vizinhos periodicamente.

Quando as informações do dispositivo local são alteradas, o switch notifica imediatamente as alterações para dispositivos vizinhos enviando mensagens LLDP. Mas para evitar que as mensagens LLDP

Enviada para a rede causada por alterações frequentes de informações do dispositivo local, cada mensagem LLDP precisa ser adiada por um tempo específico após o envio da última mensagem.

Quando o status operacional da porta muda de **Desabilitar** ou **Receber somente** para **Enviar e receber**

ou **Enviar somente**, o switch envia uma mensagem LLDP para seus dispositivos vizinhos imediatamente.

- **Mecanismo de recebimento de mensagens LLDP**

Quando o status operacional da porta é **Enviar e receber** ou **Receber somente**, o switch confirma a validade de cada mensagem LLDP recebida e seus TLVs. Após a verificação, ele salva o informações do dispositivo vizinho e inicia um temporizador de envelhecimento de acordo com o valor de TTL (Time to Live) em Time to Live TLV. Se o valor for zero, as informações do dispositivo vizinho serão eliminadas imediatamente.

9.3.2 Global

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

Descrição do parâmetro

Nome	Descrição
Função LLDP	Usado para habilitar ou desabilitar a função LLDP.
Intervalo de envio	Especifica o intervalo no qual o switch envia LLDPDUs para 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 na qual as informações locais podem sobreviver nos dispositivos vizinhos. = TTL Min (65535, multiplicador TTL x intervalo de transmissão LLDPDU), indicando o valor mínimo que varia de 65535 a multiplicador TTL x intervalo de transmissão LLDPDU

Atraso de inicialização

de

Para impedir que a porta execute a inicialização continuamente como resultado de alterações frequentes no status operacional, você pode configurar um tempo de atraso de inicialização para a porta que permite que a porta execute a inicialização para o tempo específico após a alteração do status operacional.

4.4.2 Configuração de porta

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

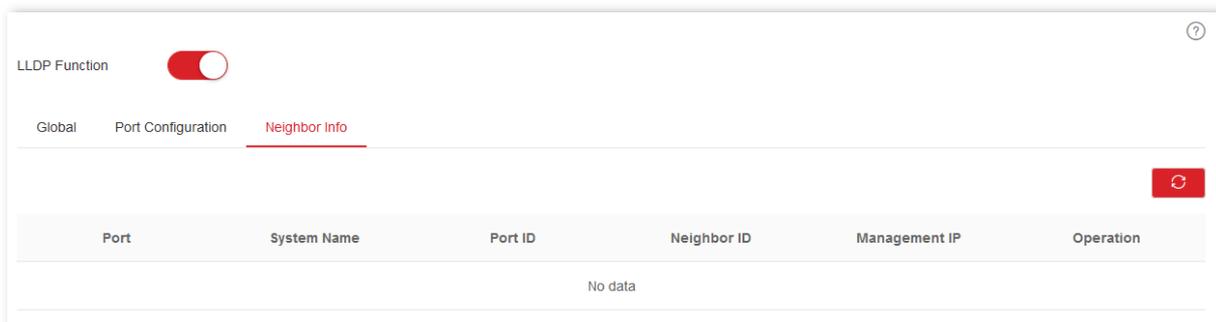
Port	LLDP Operating Status	Operation
1	Send & Receive	
2	Send & Receive	
3	Send & Receive	
4	Send & Receive	
5	Send & Receive	
6	Send & Receive	
7	Send & Receive	
8	Send & Receive	

Descrição do parâmetro

Nome	Descrição
Porta	Especifica a ID da porta.
Status operacional do LLDP	<p>Indica o status operacional LLDP de cada porta.</p> <ul style="list-style-type: none"> - Desativar: A função LLDP desta porta está desativada. - Somente envio: A porta só envia, mas não recebe mensagens LLDP. - Somente recebimento: A porta só recebe, mas não envia mensagens LLDP. - Send & Receive: A porta envia e recebe mensagens LLDP. - Sem alteração: Mantenha a configuração atual.

4.4.3 Informações do vizinho

Clique em **Switching > Configuração do LLDP > Informações do Vizinho** para entrar na página. Nesta página, você pode exibir as informações do vizinho.



Descrição do parâmetro

Nome	Descrição
Porta	Especifica a ID da porta.
Nome do sistema	Especifica o nome do sistema do dispositivo vizinho.
ID da porta	Especifica as informações de porta do dispositivo vizinho.
	 Dica As informações da porta podem ser um número de porta, endereço MAC ou outras informações, definidas pelas informações transportadas na mensagem LLDP do dispositivo vizinho.
ID do vizinho	Especifica o endereço MAC do dispositivo vizinho.
IP de gerenciamento	Especifica o endereço IP de gerenciamento do dispositivo vizinho.
Tempo de Sobrevivência	Especifica o restante do tempo em 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	Especifica a descrição detalhada do dispositivo vizinho.
Desempenho	Especifica os recursos suportados pelo dispositivo vizinho.

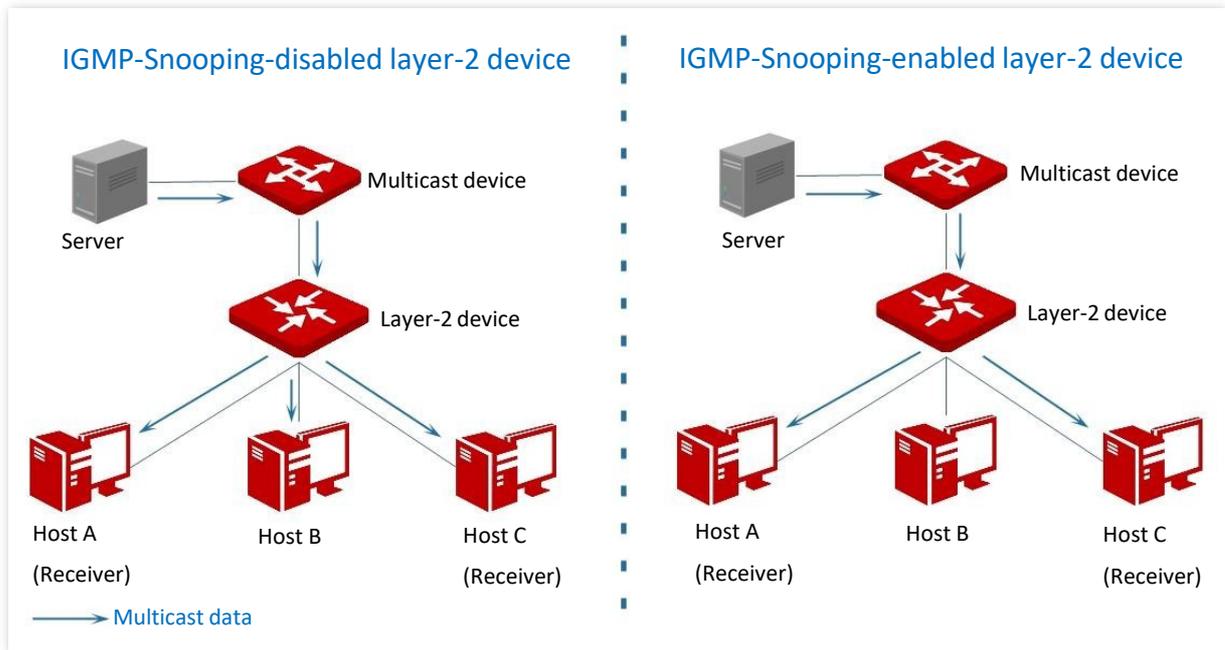
4.5 IGMP Snooping

IGMP Snooping (Internet Group Management Protocol Snooping) é um mecanismo de restrição de multicast executado nos switches Ethernet de camada 2, que é usado para gerenciar e controlar grupos de multicast.

4.5.1 Princípio de IGMP Snooping

Como mostrado na figura abaixo, os dados de multicast são transmitidos a partir do dispositivo de camada 2 desativado pelo IGMP-Snooping; Mas com o IGMP Snooping habilitado, o dispositivo de camada 2 estabelecerá uma tabela de mapeamento para portas e endereços MAC de multicast

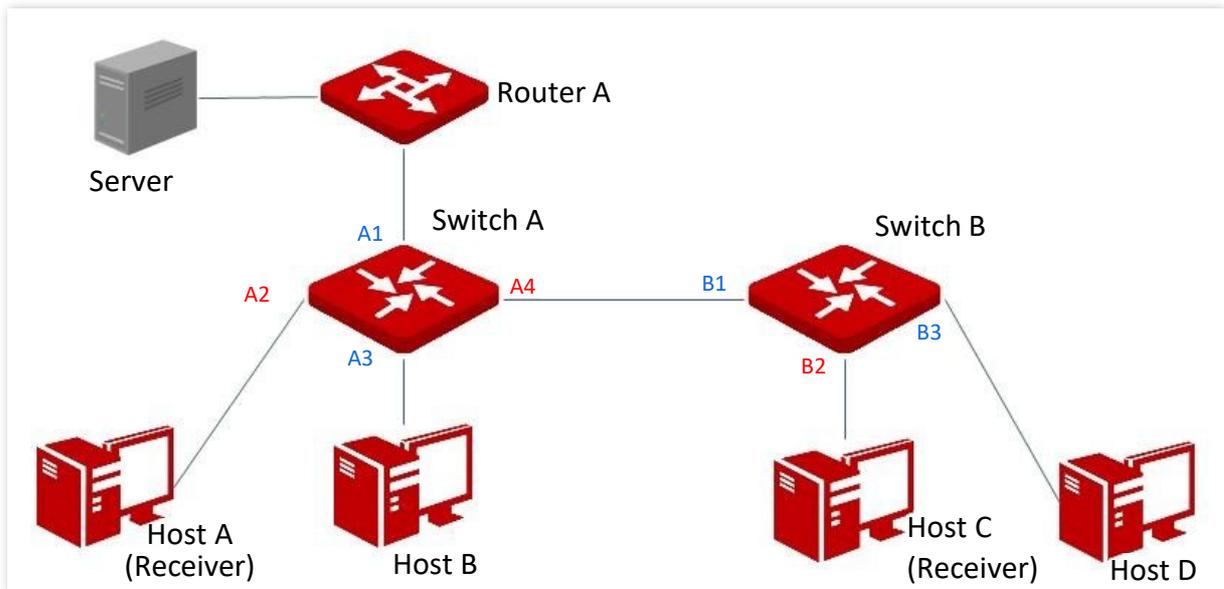
analisando mensagens IGMP e encaminhando dados de multicast para o receptor específico.



A snooping IGMP apenas encaminha dados para os receptores específicos através do multicast de camada 2, fornecendo as seguintes vantagens:

- Reduza a transmissão na rede de camada 2 e economize largura de banda de rede.
- Melhore a segurança dos dados de multicast.
- Proporcione conveniência para o gerenciamento de cobrança para cada host.

Como mostrado na figura a seguir, o roteador A está conectado à fonte de multicast, a snooping IGMP do switch A e do switch B está habilitada, enquanto o host A e o host C são os receptores dos dados de multicast.



■ **Porta do roteador**

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

■ **Porta do host**

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

■ **Consulta geral**

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

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

- Se a porta de recebimento estiver incluída na tabela de mapeamento, o dispositivo de camada 2 reiniciará o temporizador de envelhecimento da porta.
- Se a porta de recebimento for excluída na tabela de mapeamento, o dispositivo de camada 2 adicionará a porta à tabela de mapeamento e iniciará um temporizador de envelhecimento para a porta.

■ **Consulta específica**

Quando um host com IGMPv2 ou IGMPv3 habilitado deixa o grupo de multicast, ele envia mensagens de saída do grupo IGMP. Quando as portas dos dispositivos de camada 2 (switches A e B na figura acima) receberem a

mensagem IGMP leave group, as seguintes ações serão feitas de acordo com a tabela de mapeamento:

- Se nenhuma entrada de encaminhamento do grupo de multicast for encontrada ou a entrada de encaminhamento correspondente não contiver a porta de recebimento, o dispositivo de camada 2 descarta a mensagem de saída do grupo IGMP diretamente em vez de encaminhá-la para outras portas.
- Se a entrada de encaminhamento do grupo de multicast for encontrada e a entrada de encaminhamento correspondente contiver outras portas de host, o dispositivo de camada 2 descartará o grupo de saída IGMP diretamente em vez de encaminhá-lo para outras portas e envia uma mensagem de consulta específica do IGMP para o host de saída.
- Se a entrada de encaminhamento do grupo de multicast for encontrada e a entrada de encaminhamento correspondente não contiver outras portas de host, o dispositivo de camada 2 encaminhará a mensagem pela porta do roteador e também enviará uma mensagem de consulta específica do IGMP para o host.

4.5.2 Global

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

IGMP Snooping

Global Fast Leave

VLAN ID

VLAN

Confirm

Descrição do parâmetro

Nome	Descrição
Snooping IGMP	Usado para habilitar ou desabilitar a função de snooping IGMP.
VLAN ID	Especifica a VLAN cuja função IGMP Snooping é necessária.
VLAN	Usado para habilitar ou desabilitar a função IGMP Snooping da VLAN.

Versão do protocolo	<p>Versões de mensagens IGMP suportadas:</p> <ul style="list-style-type: none"> - v1: Somente processar mensagens do IGMPv1. - v2: Processe somente mensagens de consulta de IGMPv1 e IGMPv2. - v3: Processar mensagens de IGMPv1, IGMPv2 e IGMPv3.
Tempo de envelhecimento da porta de roteamento	Especifica a hora 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 geral da consulta	Especifica o tempo máximo de resposta para a consulta geral. Depois que a opção encaminhar a mensagem de consulta geral e durante esse período de tempo, 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	Especifica o tempo máximo de resposta para a consulta específica. Depois que o switch encaminha a mensagem de consulta específica do IGMP para as portas do host e durante o tempo ponto final, se a porta do host não receber a mensagem de associação IGMP que responde à consulta específica pelo host, o switch exclui a porta na tabela de mapeamento.
Tempo de envelhecimento da porta do host	Especifica a hora do temporizador de envelhecimento da porta do host. Quando a porta do host não recebe a mensagem de associação IGMP durante esse período de tempo, o switch exclui a porta da tabela de mapeamento.
Descarte Multicast	Com a função Multicast Discard ativada, o switch encaminha a mensagem de dados de multicast desconhecida apenas para a porta do roteador e não transmite na VLAN. Se o switch não tiver nenhuma porta de roteador, os dados de multicast desconhecidos serão descartados e não encaminhados.

4.5.3 Saída rápida

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

Global		Fast Leave	
Port	Fast Leave	Operation	
1	Disable		
2	Disable		
3	Disable		
4	Disable		
5	Disable		
6	Disable		
7	Disable		
8	Disable		

Descrição do parâmetro

Nome	Descrição
Porta	Especifica a ID da porta.
Saída Rápida	Com a função ativada, ao receber as mensagens de grupo de saída IGMP dessa porta, o switch remove a porta da lista de encaminhamento de multicast de snooping IGMP correspondente e não espera até que o tempo de envelhecimento da porta do host atinja o tempo limite.

5 Routing

5.1 Roteamento estático

Rota estática é a rota fixa configurada manualmente pelo administrador, geralmente usada na rede de topologia estável e de pequeno porte. A rota estática é eficiente, confiável e fácil de configurar, o que pode melhorar a velocidade de encaminhamento dos pacotes. Mas a rota estática não pode se adaptar automaticamente às alterações de topologia de rede. Assim, quando a rede não funciona ou a rede alterações de topologia, o administrador precisa modificar manualmente a configuração de roteamento estático.



A rota estática possui a prioridade mais alta entre todas as rotas.

Clique em **Roteamento > Roteamento Estático** para entrar na página. Nesta página, você pode exibir e configurar as regras de roteamento estático.

Descrição do parâmetro

Nome	Descrição
Endereço de Destino	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	Especifica o endereço IP de entrada da rota do próximo salto após a saída dos pacotes do switch.

5.2 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, o endereço da camada de link de dados do host de destino (como o endereço MAC Ethernet) é necessário.

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

1. O switch verifica se existe uma regra com a relação correspondente entre o endereço IP e o endereço MAC do host de destino na tabela ARP do switch. Em caso afirmativo, o switch envia os 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 camada de link de dados da 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 de endereço IP e endereço MAC do host de destino em sua tabela ARP para uso posterior.

Clique em **Roteamento > ARP**. Nesta página, você pode exibir e configurar o cabo ARP.

IP Address	MAC Address	VLAN ID	Type	Aging Time	Operation
192.168.60.163	00d8.61f6.a0f2	vlan1.1	Dynamic	1180s	

Descrição do parâmetro

Nome	Descrição
Tempo de envelhecimento	Especifica o tempo de envelhecimento do ARP. Se o switch não receber a mensagem ARP dentro desse período de tempo, a regra

o do ARP	de roteamento ARP será excluída da tabela ARP.
Endereço IP	Especifica o endereço IP do host de destino.
Endereço MAC	Especifica o endereço MAC do host de destino correspondente ao endereço IP.
VLAN ID	Especifica a interface de camada 3 da VLAN na qual a regra ARP se localiza.
Tipo	Especifica os tipos da tabela. <ul style="list-style-type: none">- Dinâmico: Especifica a tabela ARP que é identificada automaticamente pelo switch. O ciclo de vida é o tempo de envelhecimento do ARP.- Estático: Especifica a tabela ARP configurada manualmente. A regra é válida permanentemente e está livre das limitações do tempo de envelhecimento do ARP.
Tempo de envelhecimento	Especifica o tempo de envelhecimento restante da regra de roteamento ARP.

5.3 Servidor DHCP

5.3.1 Visão geral

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



- Dica

O servidor DHCP deste comutador não suporta a atribuição de endereços IP com base na Opção 82.

Estratégia de alocação de endereços IP

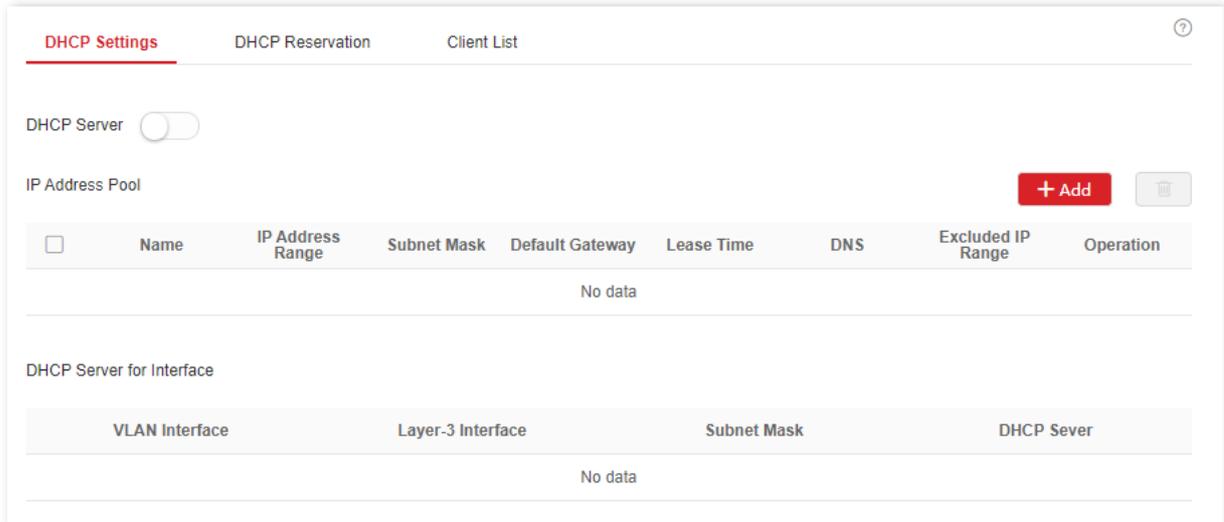
De acordo com diferentes necessidades dos clientes, o DHCP fornece dois tipos de estratégias de atribuição de endereços IP:

- 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 de alguns clientes específicos. A atribuição de um endereço IP fixo pode evitar a falha de algumas funções com base no endereço IP devido a alterações de endereço IP.

5.3.2 Configurações de DHCP

Clique em **Roteamento** > **Servidor DHCP** > **Configurações DHCP** para entrar na página. Nesta página, você pode exibir e configurar o servidor DHCP.



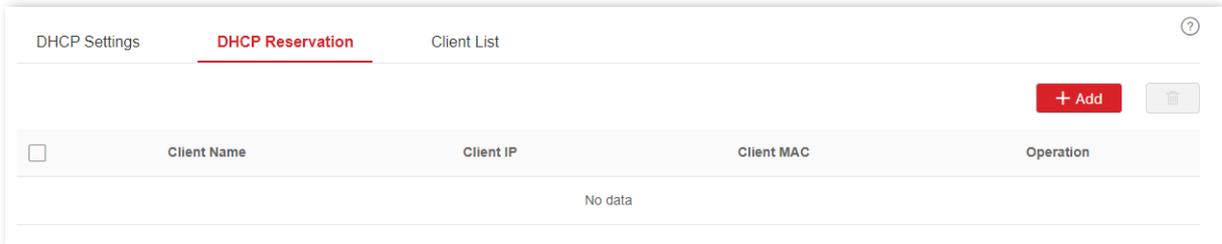
Descrição do parâmetro

Nome	Descrição
Servidor DHCP	Habilite ou desabilite a função do servidor DHCP.
Nome	Especifica o nome da diretiva de pool de endereços IP.
Intervalo de endereços IP	Especifica o intervalo de endereços IP que podem ser atribuídos por meio dessa regra.
Máscara 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. Na metade do tempo de concessão, o cliente envia uma solicitação DHCP para o DHCP servidor para renovar a concessão. Se a solicitação for bem-sucedida, a locação será renovada a partir do momento do envio da solicitação; Caso contrário, o processo de renovação reinicia em 7/8 do tempo de locação. Se a solicitação for bem-sucedida, a locação será renovada a partir do momento do envio da

solicitação; se a solicitação ainda falhar, o	c l i e n t e p	recisará solicitar novamente o endereço IP após a expiração da concessão. Para um menor consumo de recursos, defina o tempo de concessão de acordo com o ambiente de rede real e tente reduzir o número de mensagens enviadas. Recomenda-se definir para 1 dia se não houver outro requisito especial.
	DNS	Ela especifica o endereço do servidor DNS atribuído aos clientes.
	Intervalo de IP excluído	Especifica os endereços IP no pool de endereços IP que não são atribuídos pelo servidor DHCP por estratégia de atribuição dinâmica.
DHCP Servidor para Interface	VLAN Interface	Especifica a VLAN onde a diretiva de pool de endereços entra em vigor. Interface de camada 3 Ela especifica o endereço IP da interface VLAN.
	Máscara de sub-rede	Ela especifica a máscara de sub-rede da interface VLAN.
	Servidor DHCP VLAN é	Com ele habilitado, a função do servidor DHCP da interface é validado

5.3.3 Reserva DHCP

Clique em **Roteamento** > **Servidor DHCP** > **Reserva DHCP** para entrar na página. Nesta página, pode exibir e configurar a política de Reserva DHCP.



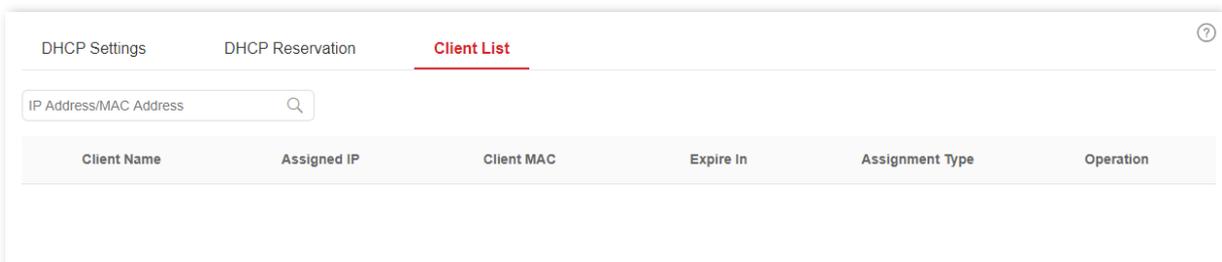
Descrição do parâmetro

Nome	Descrição
Nome do Cliente	Especifica a descrição 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.
Cliente MAC	Especifica o endereço MAC de um cliente.

5.3.4 Lista de clientes

Clique em **Roteamento** > **Servidor DHCP** > **Lista de Clientes** para entrar na página. Nesta página, pode executar as seguintes operações para os dispositivos cujos endereços IP são obtidos a partir deste switch.

- Exiba o nome do cliente, o endereço IP atribuído e outras informações.
- Clique **Reservar**, o endereço IP atribuído pode ser adicionado ao **Reserva DHCP** e o servidor DHCP atribui esse endereço IP ao cliente o tempo todo.



Descrição do parâmetro

Nome	Descrição
Nome do Cliente	Especifica o nome de um cliente.
IP do cliente	Especifica um endereço IP atribuído pelo servidor DHCP ao cliente.
Cliente MAC	Especifica o endereço MAC de um cliente.
Expirar em	Especifica o tempo de descanso da concessão.
Tipo de Atribuição	Especifica a diretiva 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 endereço estático a este cliente usando a política de atribuição de endereço IP estático .

6 Política de QoS

6.1 ACL

6.1.1 Visão geral

A ACL (Lista de Controle de Acesso) é usada para filtrar mensagens configurando regras correspondentes e Operações. Após a mensagem ser recebida pela porta do switch, ela é analisada de acordo com as regras de ACL dessa porta. E essas regras decidem quais pacotes podem passar e o que deve ser rejeitado, 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: Corresponde às regras de filtragem de acordo com o endereço MAC de origem e o endereço MAC de destino do quadro de dados de camada 2.
- ACL IP: corresponde às regras de filtragem com base no endereço IP de origem e no endereço IP de destino do cabeçalho IP do pacote de camada 3.

Uma ID de ACL pode ser configurada com várias regras de correspondência de ACL e a mensagem corresponde à regra de acordo com a prioridade da regra. Quando uma mensagem é correspondida a uma regra com prioridade mais alta, ela deixa de corresponder a outras regras.

6.1.2 Diretrizes de configuração

Regras de filtração baseadas no endereço MAC

Pass	Tarefa	Descrição
o		

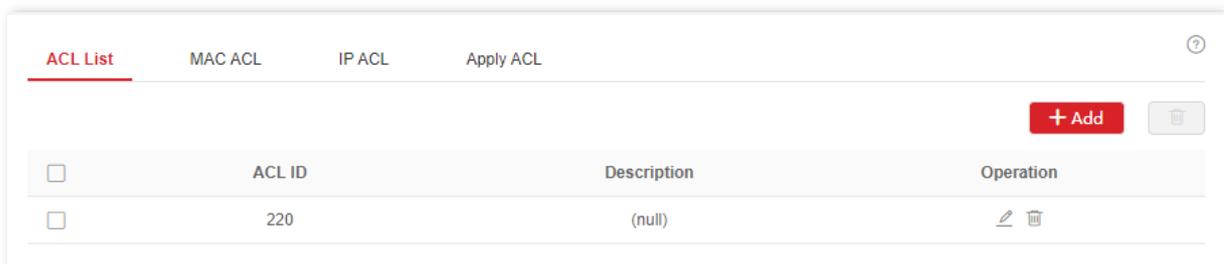
1	Lista ACL	Necessário. Você pode configurar uma ID de ACL que varia de 200 a 299.
2	MAC ACL	Necessário. Você pode configurar a regra de filtragem que corresponde aos endereços MAC de origem e destino do quadro de dados da camada 2. Várias regras de ACL MAC podem ser configuradas com uma ID de ACL.
3	Aplicar ACL	Necessário. A regra MAC ACL entra em vigor quando é aplicada à porta correspondente do switch.

Regras de filtração com base no endereço IP

Passo	Tarefa	Descrição
1	Lista ACL	Necessário. Você pode configurar uma ID de ACL que varia de 100 a 199.
2	IP ACL	Necessário. Você pode configurar a regra de filtragem que corresponde aos endereços IP de origem e de destino do pacote de dados de camada 3. Várias regras de ACL IP podem ser configuradas com uma ID de ACL.
3	Aplicar ACL	Necessário. A regra de ACL IP entra em vigor quando é aplicada à porta correspondente do switch.

6.1.3 Lista ACL

Clique em **Política de QoS** > ACL > Lista de ACL para entrar na página. Nesta página, você pode exibir e configurar a ID e a descrição da ACL.

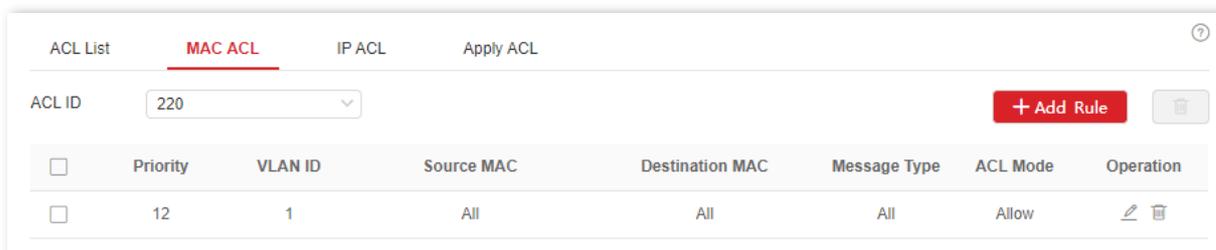


Descrição do parâmetro

Nome	Descrição
ACL ID	Especifica a ID da ACL, que é usada para identificar a ACL.
Descrição	Para um gerenciamento conveniente, você pode adicionar uma descrição para a ACL.

6.1.4 MAC ACL

Clique em **Política de QoS > ACL > ACL MAC** para entrar na página. Nesta página, você pode exibir e configurar as regras da ACL MAC.

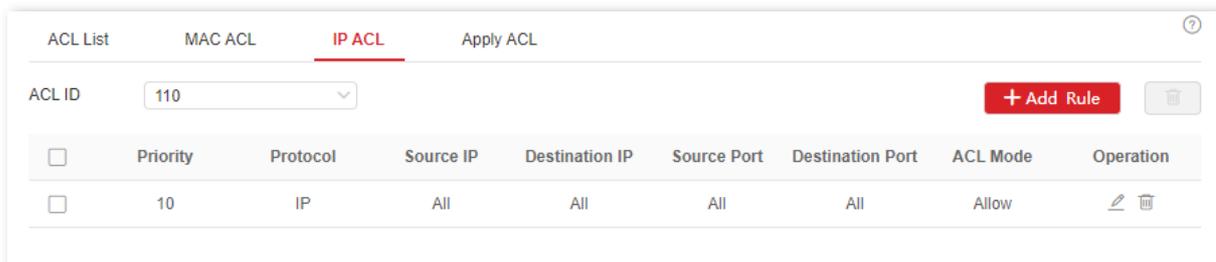


Descrição do parâmetro

Nome	Descrição
ACL ID	É usado para selecionar a ACL para configuração de regras de ACL MAC. A ID da ACL deve ser adicionado na Lista ACL com antecedência.
Prioridade	Este campo especifica a prioridade de uma regra. Um valor menor indica uma prioridade mais alta. A mensagem começa a corresponder da regra com a prioridade mais alta. Uma vez correspondida, a mensagem pára de verificar regras.
VLAN ID	Especifica a VLAN à qual a mensagem pertence. Se esse campo não estiver configurado, ele indicará mensagens de todas as VLANs.
MAC de origem	Especifica o endereço MAC de origem da mensagem. <ul style="list-style-type: none"> - Qualquer MAC: Especifica todos os endereços MAC. - MAC especificado: Combinado com 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. <ul style="list-style-type: none"> - Qualquer MAC: Especifica todos os endereços MAC. - MAC especificado: Combinado com máscara, é usado para especificar um determinado endereço MAC ou segmento de endereço MAC.
Tipo de mensagem	Especifica o tipo de mensagem do quadro de dados de camada 2. Se esse campo não estiver configurado, ele indicará qualquer tipo de mensagem.
Modo ACL	Especifica o modo ACL no qual o switch processa as mensagens correspondentes a regra, incluindo Permitir (ou seja, encaminhar) ou Bloquear (ou seja, descartar) .

6.1.5 IP ACL

Clique em **Política de QoS > ACL > ACL IP** para entrar na página. Nesta página, você pode exibir e configurar as regras de ACL IP.



Descrição do parâmetro

Nome	Descrição
ACL ID	É usado para selecionar a configuração de regras de ACL IP para ACL IP. A ID da ACL deve ser adicionada à Lista da ACL com antecedência.
Prioridade	Especifica a prioridade da regra. Um valor menor indica uma prioridade mais alta. A mensagem começa a corresponder da regra com a prioridade mais alta. Uma vez correspondida, a mensagem pára de verificar regras.
Protocolo	Especifica o campo de tipo de protocolo do cabeçalho de pacote IP de camada 3 de uma mensagem, como IP, ICMP e assim por diante. Você também pode inserir o número do protocolo manualmente.
IP de origem	Especifica o endereço IP de origem da mensagem. <ul style="list-style-type: none"> - Qualquer IP: Indica todos os endereços IP. - IP especificado: Combinado com máscara, indica um determinado endereço de rede.
IP de destino	Especifica o endereço IP de destino da mensagem. <ul style="list-style-type: none"> - Qualquer IP: Indica todos os endereços IP. - IP especificado: Combinado com 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, incluindo Permitir (ou seja, encaminhar) ou Bloquear (ou seja, descartar).

6.1.6 Aplicar ACL

As regras de ACL entram em vigor ao aplicá-las a portas físicas.

Clique em **Política de QoS** > ACL > **em Aplicar ACL** para entrar na página. Nesta página, você pode aplicar as regras de ACL configuradas a portas físicas.

<input type="checkbox"/>	Applied Port	ACL ID	Filtering Direction	Operation
<input type="checkbox"/>	1	220	Ingress	
<input type="checkbox"/>	18	110	Ingress	
<input type="checkbox"/>	20	110	Ingress	

Descrição do parâmetro

Nome	Descrição
Porta aplicada	Especifica o número da porta física à qual a regra de ACL se aplica.
ACL ID	Especifica a regra de ACL que se aplica à porta.
Direção da filtragem	Especifica a direção de filtragem de mensagens da porta. Somente a Entrada é suportada por essa opção.

6.2 QoS

6.2.1 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 ao seu destino com o melhor esforço, sem garantia de atraso de entrega, confiabilidade e assim por diante. Hoje em dia, além dos aplicativos tradicionais como www, FTP e E-mail, surgem novos serviços, como videoconferência, ensino remoto, Vídeo sob Demanda (VoD) e vídeo telefone, que precisam maiores requisitos de largura de banda, atraso e jitter. A política de QoS (Quality of Service) pode atender às demandas acima e melhorar a qualidade do serviço na rede.

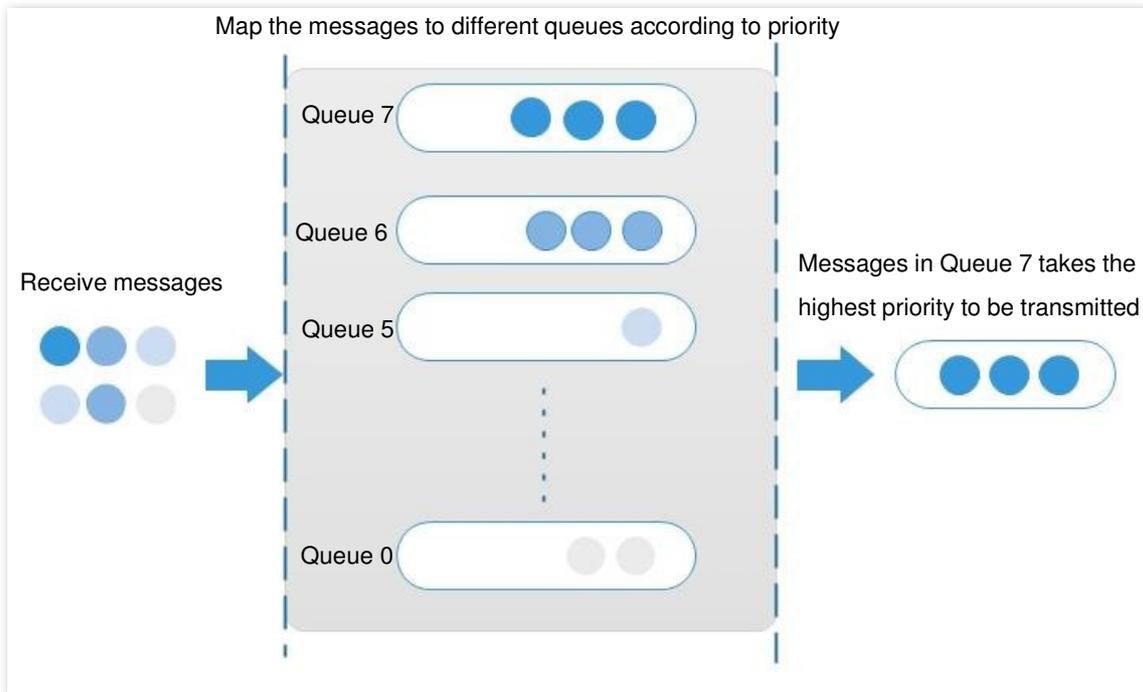
Esse switch classifica as mensagens de acordo com a prioridade no estágio de entrada, depois as mapeia para diferentes filas no estágio de saída e, finalmente, encaminha essas mensagens por filas de acordo com o modo de agendamento, de modo a garantir a qualidade do serviço de rede.

Modo de agendamento

O agendamento de fila é usado para resolver o problema de preempção de recursos por várias mensagens quando a rede está congestionada. Essa opção oferece suporte a três modos de agendamento: prioridade estrita, prioridade ponderada simples e prioridade ponderada. Cada modo de agendamento tem

oito filas (filas de 0 a 7) com prioridade de encaminhamento de dados diferente.

- **Prioridade estrita**



O algoritmo de agendamento de prioridade estrita é especialmente projetado para aplicativos de serviço críticos. Ano

Característica importante dos serviços críticos é que eles exigem serviço preferencial em congestionamento, a fim de reduzir o atraso de resposta.

No agendamento 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 está vazia, as mensagens na fila com prioridade mais baixa são enviadas. Você pode colocar mensagens de serviço críticas nas filas com prioridade mais alta e colocar mensagens de serviço não críticas (como email) nas filas com prioridade mais baixa. Dessa forma, as mensagens de serviço críticas são enviadas preferencialmente e as mensagens de serviço não críticas são enviadas quando as mensagens de serviço críticas não são enviadas.

Desvantagem da prioridade estrita: Se houver mensagens nas filas com prioridade mais alta por um longo tempo durante o congestionamento, as mensagens nas filas com prioridade mais baixa permanecerão presas porque não são atendidas.

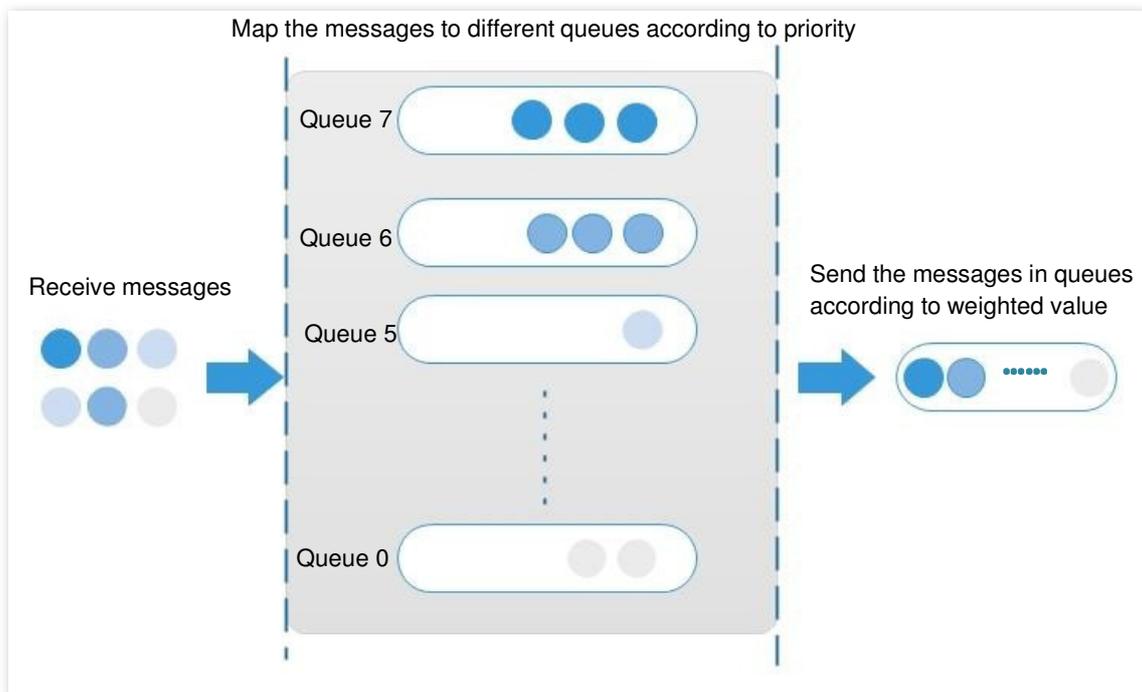
- **Prioridade ponderada simples**

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 por sua vez para garantir

que cada fila possa ser atribuída a um determinado tempo de serviço. O valor ponderado representa a proporção de atribuídos recurso. Supondo que haja oito filas de saída para uma porta e cada fila seja atribuída com 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. Dessa forma, a fila com a prioridade mais baixa pode ter a garantia de 5 Mbps de largura de banda pelo menos, evitando assim a desvantagem do algoritmo de agendamento de fila de prioridade simples de que as mensagens em filas de baixa prioridade possivelmente não devem ser atendidas por um longo tempo. Outra vantagem do algoritmo de agendamento de fila de Prioridade Ponderada é que, embora as filas sejam agendadas por sua vez, o tempo de serviço para cada fila não é fixo, o que significa que se uma fila estiver vazia, a próxima fila será agendada imediatamente. Dessa forma, os recursos de largura de banda podem ser totalmente utilizados.

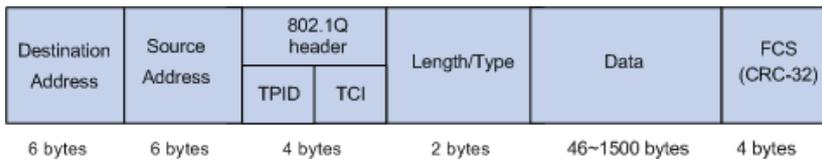


Prioridade

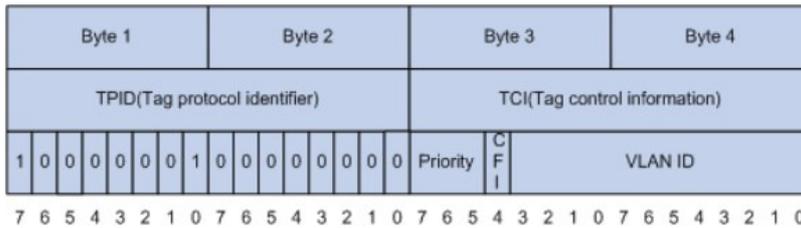
Esse switch oferece suporte a três modos de prioridade: [Prioridade 802.1P](#), [Prioridade DSCP](#) e [Prioridade de Porta](#).

■ Prioridade 802.1P

A prioridade 802.1P está nos cabeçalhos de pacote da Camada 2 e é aplicável a ocasiões em que o cabeçalho de 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 (Identificador de Protocolo de Tag, valor: 0x8100) de 2 bytes e um TCI (Informações de Controle de Tag) de 2 bytes.



A figura abaixo exibe uma visão detalhada de uma tag 802.1Q. O campo **Prioridade** em TCI é a prioridade 802.1P, que consiste em 3 bits que variam de 0 a 7.

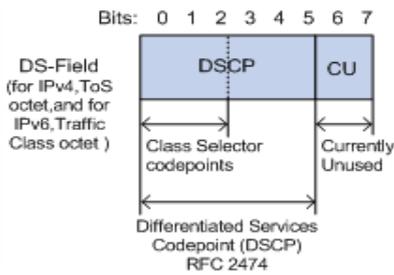


Por padrão, a prioridade 802.1P, as filas e as palavras-chave dessa opção são mapeadas da seguinte maneira.

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 redes

■ **Prioridade DSCP**

RFC2474 redefine o campo ToS (Tipo de Serviço) no cabeçalho da mensagem IP, que é chamado de campo DS (Serviços Diferenciados). Os primeiros seis 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 é a seguinte.

Prioridade (decimal)	DSCP	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	be (padrão)

Por padrão, a prioridade DSCP e as filas dessa opção são mapeadas da seguinte maneira.

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

■ **Prioridade de porta**

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

- As mensagens recebidas pela porta não carregam as marcas de prioridade confiáveis pela porta.
Exemplo: Para uma porta com o modo de prioridade 802.1P habilitado, as mensagens recebidas não carregam a marca 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 maneira.

Cos Prioridade	Fila
0	1
1	2
2	3
3	4
4	5
5	6
6	7
7	8

6.2.2 Diretrizes de configuração

Com base na prioridade 802.P

Passo	Tarefa	Descrição
1	Agendador de QoS	Necessário. Selecione o modo de agendador do switch com base nas demandas reais.
2	802.1P	Necessário. Configure a relação de mapeamento entre a prioridade 802.1P e as filas.
3	Prioridade de porta	Necessário. Defina o modo de prioridade das portas correspondentes como 802.1P Trust e configure a prioridade Cos para todas as portas.

Com base na prioridade DSCP

Passo	Tarefa	Descrição
1	Agendador de QoS	Necessário. Selecione o modo de agendador do switch com base nas demandas reais.
2	DSCP	Necessário. Configure a relação de mapeamento entre a prioridade DSCP e as filas.
3	Prioridade de porta	Necessário. Defina o modo de prioridade das portas correspondentes como DSCP Trust e configure a prioridade Cos para todas as portas.

6.2.3 Agendador de QoS

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

Descrição do parâmetro

Nome	Descrição
Modo QoS	<p>Especifica o modo do agendador para o tráfego de porta.</p> <ul style="list-style-type: none">- Prioridade estrita: O switch encaminha as mensagens estritamente com base na prioridade da mensagem de alta para baixa. As mensagens de fila com prioridade mais baixa são encaminhadas somente 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 serão atribuídas com base no peso de cada fila.
Configurações da fila	<p>Se o Modo QoS estiver definido como Prioridade Ponderada, você precisará configurar o valor ponderado para cada fila.</p>
Descarte de Egresso	<p>Quando essa função é habilitada, o switch desabilita a função de controle de fluxo para atender aos requisitos de clone de rede em vários ambientes.</p> <p> Dica</p> <p>Essa função se aplica ao cenário de clone de rede e não é recomendada em cenários comuns.</p>

6.2.4 802.1P

Clique em **Política de QoS > QoS > 802.1P** para entrar na página. Nesta página, você pode configurar a relação de mapeamento da prioridade e das filas do 802.1P.

QoS Scheduler
802.1P
DSCP
Port Priority
?

CoS Priority Setting

Priority0

Priority1

Priority2

Priority3

Priority4

Priority5

Priority6

Priority7

Confirm

Descrição do parâmetro

Nome	Descrição
Prioridade 0	Especifica a fila na qual a prioridade das mensagens é 0.
Prioridade 1	Especifica a fila na qual a prioridade das mensagens é 1.
Prioridade 2	Especifica a fila na qual a prioridade das mensagens é 2.
Prioridade 3	Especifica a fila na qual a prioridade das mensagens é 3.
Prioridade 4	Especifica a fila na qual a prioridade das mensagens é 4.
Prioridade 5	Especifica a fila na qual a prioridade das mensagens é 5.
Prioridade 6	Especifica a fila na qual a prioridade das mensagens é 6.
Prioridade 7	Especifica a fila na qual a prioridade das mensagens é 7.

6.2.5 DSCP

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

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

Descrição do parâmetro

Nome	Descrição
DSCP	Especifica o nível de prioridade (intervalo: 0 a 63) definido pelo campo DS dos cabeçalhos de mensagens IP.
Fila de portas	Especifica a fila do agendador da porta de saída.

6.2.6 Prioridade de porta

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

Port	CoS Priority	Trust Mode	Operation
1	0	Non-Trust	
2	0	Non-Trust	
3	0	Non-Trust	
4	0	Non-Trust	
5	0	Non-Trust	
6	0	Non-Trust	
7	0	Non-Trust	
8	0	Non-Trust	

Descrição do parâmetro

Nome	Descrição
Porta	Especifica a 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 de confiança ou a porta está no modo não confiável, as mensagens reingressam em filas com base na correspondência.
Modo de confiança	<p>Especifica o método que a porta usa para processar as mensagens recebidas.</p> <ul style="list-style-type: none"> - Não Confiável: Todas as mensagens recebidas pela porta reingressam nas filas de acordo com a correspondência da prioridade Cos configurada. - 802.1P Trust: Quando a porta recebe mensagens VLAN, as mensagens reingressam em filas de acordo com a correspondência do 802.1P. Quando a porta recebe outras mensagens, as mensagens reingressam em filas de acordo com a correspondência da prioridade Cos. - DSCP Trust: Quando a porta recebe mensagens IP, as mensagens reingressam em filas de acordo com a correspondência do DSCP. Quando a porta recebe outras mensagens, as mensagens reingressam em filas de acordo com a correspondência da prioridade Cos.

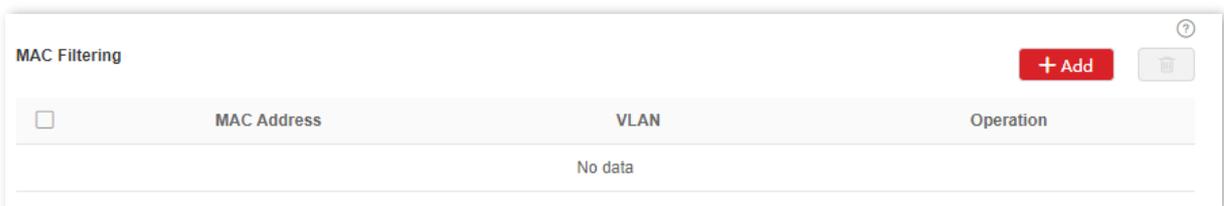
7 Segurança de rede

7.1 Filtragem MAC

Com esta função ativada, o switch pode verificar 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.



Descrição do parâmetro

Name	Description
Endereço MAC	Especifica o endereço MAC a ser filtrado. Quando o endereço MAC de origem ou endereço MAC de destino de um pacote é o mesmo que o endereço MAC listado, o pacote será descartado.
VLAN	Especifica a VLAN na qual a regra de filtragem MAC entra em vigor.

7,2 802,1X

7.2.1 Visão geral

802.1X é uma tecnologia de controle de acesso à rede trazida pelo IEEE. É usado para autenticar e controlar 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 que suporte a autenticação 802.1X.
- Dispositivo de autenticação: Fornece interface para o cliente se conectar à LAN. Pois é localizado entre o cliente e o servidor de autenticação e decide se o cliente pode acessar LAN ou não de acordo com a mensagem retornada pelo servidor de autenticação.
- Servidor de autenticação: fornece serviço de autenticação para clientes. O mais 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 para o dispositivo de autenticação. O dispositivo decide se o cliente pode acessar a LAN ou não.

Essa opção serve como o dispositivo de autenticação no sistema de autenticação. Ele se comunica com o servidor de autenticação por meio da terminação EAP. Depois de receber a mensagem EAP do cliente, o switch encapsula as informações de autenticação do cliente do para a 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.

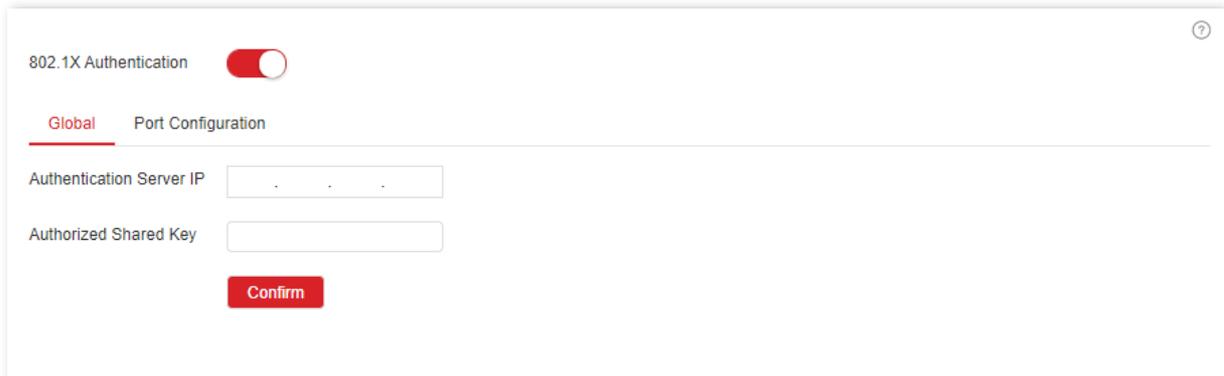


Essa opção oferece suporte apenas à autenticação com base no acesso à porta. Se um dos usuários passar a autenticação, a porta será autorizada e os seguintes usuários que usam essa porta poderão acessar a rede sem autenticação. No entanto, quando esse usuário está offline, a porta

torna-se não autorizado e todos os outros usuários sob essa porta não conseguem acessar a rede.

7.2.2 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
IP do Servidor de Autenticação	Especifica o endereço IP do servidor de autenticação RADIUS. Deve haver rotas acessíveis entre o servidor de autenticação RADIUS e esse switch.
Chave compartilhada autorizada	Especifica a chave compartilhada de uma mensagem de autenticação/autorização RADIUS. Ele deve ser o mesmo que a chave definida no lado do servidor de autenticação/autorização RADIUS.

7.2.3 Configuração de porta

Clique em **Segurança de Rede** > Configuração de Porta de > **802.1X** para entrar na página. Nesta página, você pode configurar os parâmetros de autenticação 802.1X para cada porta.

Port	Port Control Mode	Authentication Status	Re-authentication	Re-authentication Timeout	Client Timeout	Max Re-authentication Times	Operation
1	Disable	Non-authorized	Disable	3600	30	2	
2	Disable	Non-authorized	Disable	3600	30	2	
3	Disable	Non-authorized	Disable	3600	30	2	
4	Disable	Non-authorized	Disable	3600	30	2	
5	Disable	Non-authorized	Disable	3600	30	2	
6	Disable	Non-authorized	Disable	3600	30	2	
7	Disable	Non-authorized	Disable	3600	30	2	
8	Disable	Non-authorized	Disable	3600	30	2	

Descrição do parâmetro

Nome	Descrição
Porta	Especifica a ID da porta.
Modo de Controle de Porta	<p>Especifica o modo de controle da porta para acessar a rede.</p> <ul style="list-style-type: none"> - Auto: A autenticação 802.1X está ativada na porta. O estado inicial é não autorizado e o usuário não pode acessar os recursos de rede. Se um usuário passar a autenticação, a porta será autorizada e o usuário terá permissão para acessar os recursos de rede. - Autorização Obrigatória: A porta está sempre no estado de autorização. Ele permite que os usuários acessem os recursos de rede. - Não autorização obrigatória: O porto está sempre no estado de não autorização. Ele proíbe que os usuários acessem os recursos de rede sem autenticação e autorização. - Desativar: A autenticação está desativada na porta. Ele permite que os usuários acessem os recursos de rede.
Status da autenticação	<p>Especifica o status de autenticação da porta.</p> <ul style="list-style-type: none"> - Autorizado: O usuário tem permissão para acessar os recursos de rede através da porta. - Não autorizado: O usuário não tem permissão para acessar os recursos de rede através da porta.
Reautenticação	É usado para ativar/desativar a função de reautenticação 802.1X da porta. Com a função habilitada, o switch envia periodicamente uma solicitação de reautenticação ao cliente de autenticação para verificar o status da conexão e confirmar se o cliente de autenticação está online.

Tempo limite de reautenticação	<p>Especifica o intervalo no qual o switch inicia a reautenticação para clientes de autenticação.</p> <p>Se a função de reautenticação estiver habilitada em uma porta, o switch iniciará solicitações de reautenticação para os dispositivos online conectados à porta nesse intervalo.</p>
Tempo limite do cliente	<p>Especifica o período de tempo limite no qual o cliente responde à solicitação de reautenticação.</p> <p>Depois que o switch envia 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.</p>
Tempos máximos de reautenticação	<p>Especifica os tempos máximos de reautenticação com falha para um cliente. A opção força o cliente offline se os tempos de reautenticação com falha do cliente excederem esse valor.</p> <p> Dica</p> <p>O número de tempo limite de autenticação também é considerado como os tempos de reautenticação com falha. Se o número de tempo limite de autenticação do cliente exceder os tempos máximos de reautenticação, o switch forçará o cliente offline.</p>

7.3 Defesa de ataque

7.3.1 Visão geral

Esses switches suportam três métodos de defesa de ataque: ARP Attack Defense, DoS (Denial of Service) Attack Defense e MAC Address Attack Defense.

■ Defesa de ataque ARP

A taxa de recebimento ARP é definida para evitar que as mensagens ARP na LAN sejam enviadas esmagadoramente 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 descarta aleatoriamente algumas mensagens ARP para garantir que a taxa de recebimento de ARP esteja dentro do valor limite definido.

■ Defesa de ataque DoS

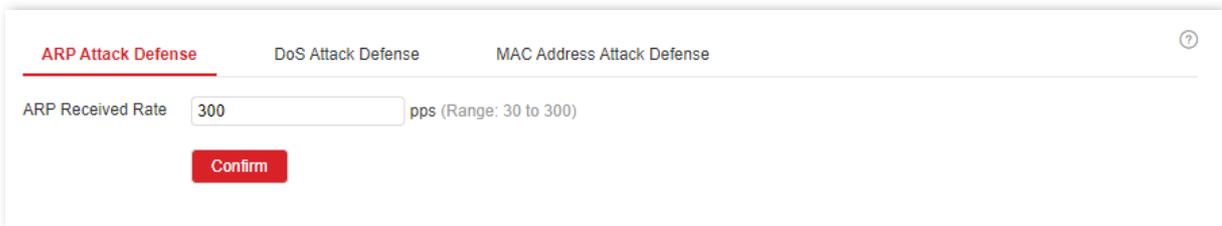
A função DoS Attack Defense é usada para impedir que alguns hosts consumam maliciosamente recursos do servidor enviando um grande número de solicitações de serviço, deixando outros hosts incapazes de usar os serviços de rede corretamente.

■ **Defesa de ataque de endereço MAC**

O MAC Address Attack Defense 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 mensagens inválidas na LAN, o que pode ampliar a tabela de encaminhamento de endereços MAC e resultar na degradação do desempenho de encaminhamento.

7.3.2 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 ARP do switch.

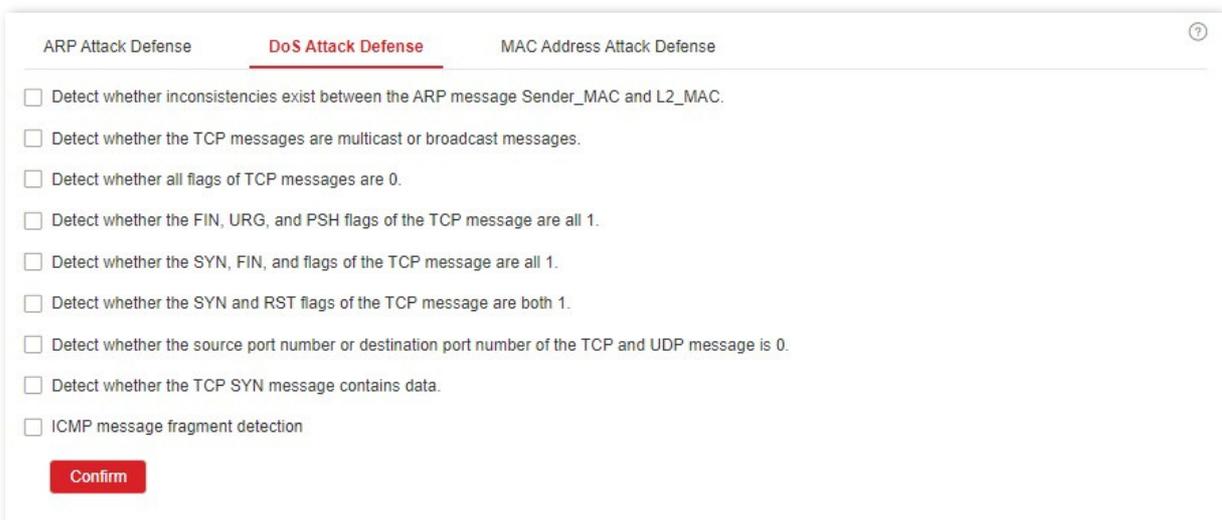


Descrição do parâmetro

Nome	Descrição
Taxa de Recebimento de ARP	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.

7.3.3 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 de Ataque DoS.



Descrição do parâmetro

Nome	Descrição
Detecte se existem inconsistências entre o Sender_MAC de mensagens ARP e L2_MAC.	Depois de marcado, o switch não encaminha mensagens ARP com Sender_MAC e L2_MAC inconsistentes.
Detecte se as mensagens TCP são mensagens de difusão ou multicast.	Depois de marcado, o switch não encaminha mensagens TCP de difusão ou multicast.
Detecte 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 da mensagem TCP são todos 1.	Depois de marcada, a opção 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 marcada, a opção não encaminha a mensagem TCP cujos sinalizadores SYN e RST são ambos 1.
Detecte se o número da porta de origem ou de destino da mensagem TCP e UDP é 0.	Depois de marcado, o switch não encaminha a mensagem TCP e UDP cujo número da porta de origem ou de destino é 0.
Detecte se a mensagem TCP SYN contém dados.	Depois de marcada, a opção não encaminha a mensagem TCP SYN que contém dados.
Detecção de fragmento de mensagem ICMP	Depois de assinalado, o comutador não responde ao fragmento de mensagem ICMP.

7.3.4 Defesa de ataque de endereço MAC

Clique em **Segurança de Rede** > Defesa de Ataque > Defesa de Ataque de Endereço MAC para entrar na página. Nesta página, você pode configurar se a porta pode encaminhar a mensagem de unicast desconhecida.

Port	MAC Discard	Operation
1	Disable	
2	Disable	
3	Disable	
4	Disable	
5	Disable	
6	Disable	
7	Disable	
8	Disable	
9	Disable	
10	Disable	

Descrição do parâmetro

Nome	Descrição
Porta	Especifica a ID da porta.
Descarte MAC	Com essa função ativada, a porta não aprende mais os endereços MAC e descarta as mensagens unicast desconhecidas recebidas.

8

Configurações do dispositivo

8.1 Gerenciamento de usuários

A atribuição de permissões de acesso diferentes a diferentes tipos de usuários pode reduzir o risco de violação da configuração do switch.

Essa opção oferece suporte a três tipos de usuários:

- **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 realizar todas as operações, além de atualização de software, redefinição ou gerenciamento de usuários.

- **Usuário comum**

Um usuário comum pode verificar a configuração do switch.

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

<input type="checkbox"/>	User	User Type	Login Timeout	Operation
<input type="checkbox"/>	admin	Administrator	300s	

Descrição do parâmetro

Nome	Descrição
Utilizador	Especifica o nome de usuário.
Tipo de usuário	Especifica os tipos de usuários. Essa opção oferece suporte a três tipos de usuários: Administrador, usuário da operação e usuário comum.....
Tempo limite de login	Se um usuário não executar nenhuma operação na interface do usuário da Web dentro do intervalo, o sistema fará logout do usuário.

8.2 SNMP

8.2.1 Visão geral

SNMP (Simple Network Management Protocol) permite que uma estação de gerenciamento de rede para

Gerencie remotamente os dispositivos de rede que oferecem suporte a esse protocolo, incluindo o monitoramento do status da rede, a modificação da configuração do dispositivo de rede, o recebimento de alarmes de eventos de rede e assim por diante.

O SNMP pode proteger as diferenças físicas entre dispositivos e realizar o gerenciamento automático de 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 comumente usado é o NMS (Network Management System), que pode ser um servidor especialmente usado para gerenciamento de rede ou um programa aplicativo para executar a função de gerenciamento em um determinado dispositivo de rede.
- Agente SNMP: Software que é executado em dispositivos gerenciados para manter informações gerenciais e relatar dados gerenciais 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, etc., que também são chamados de objetos gerenciados. O MIB define uma série de propriedades para esses objetos gerenciados: nome do objeto, direito de acesso, tipo de dados, etc. Cada agente SNMP tem seu MIB correspondente e o gerenciador SNMP pode executar

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 SNMP

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

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

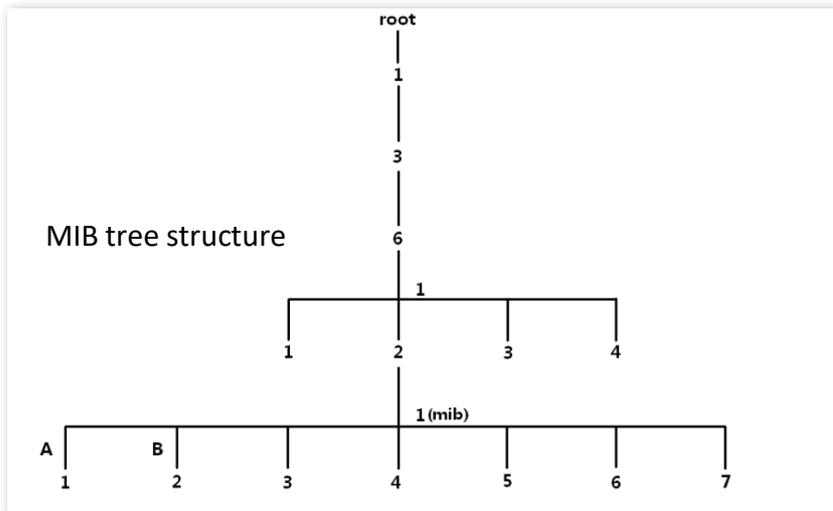
Versões SNMP

Este switch é compatível com SNMPv1, SNMPv2c e SNMPv3.

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

Introdução ao 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 cadeia de caracteres numérica é o OID (Object Identifier). 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).



Vista

O modo de exibição MIB é um subconjunto de todos os objetos gerenciados no MIB. Um objeto gerenciado é representado pelo OID, e a regra de exibição configurada (**incluir/excluir**) decide se o objeto é gerenciado ou não.

Grupo

Depois de criar o modo de exibição, você pode criar grupos SNMP. Você pode adicionar **o modo de exibição Somente Leitura/Leitura & Gravação/Notificação para cada grupo SNMP para atender à demanda de obter permissão de acesso diferente à função do switch para usuários de grupos diferentes.**

Utilizador

Depois de criar os grupos, você pode adicionar usuários para 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, depois que a exibição é criada, a comunidade é necessária para ser criada.

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 permissões de acesso.

8.2.2 Diretrizes de configuração

■ SNMPv3

Passo	Operação	Descrição
1	Básico	Necessário. Habilite a função de agente SNMP.
2	Criar modos de exibição	Opcional. Crie modos de exibição 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	Necessário. Crie grupos SNMP na página Lista de Grupos no Controle de Permissão e adicione modos de exibição com permissões de acesso diferentes para os grupos.
4	Criar usuários	Necessário. Crie usuários SNMP na página Lista de Usuários no Controle de Permissão e configure o modo de autenticação/criptografia, bem como a senha.
5	Configurar interceptação	Opcional. Configurar a notificação com a versão de segurança da v3 ativada Página de notificação .

■ SNMPv1/SNMPv2c

Passo	Operação	Descrição
1	Básico	Necessário. Habilite a função de agente SNMP.
2	Criar modos de exibição	Opcional. Crie modos de exibição para os objetos gerenciados na página Exibir Lista no Controle de Permissão . Uma exibição chamada Padrão é criada pelo sistema por padrão.
3	Criar comunidades	Necessário. Crie comunidades SNMP na página Lista de comunidades no controle de permissão .
5	Notificação	Opcional. Configurar a notificação com a versão de segurança da v1/v2c ativada

Pass	Operação	Descrição
o		Página de notificação.

8.2.3 Básico

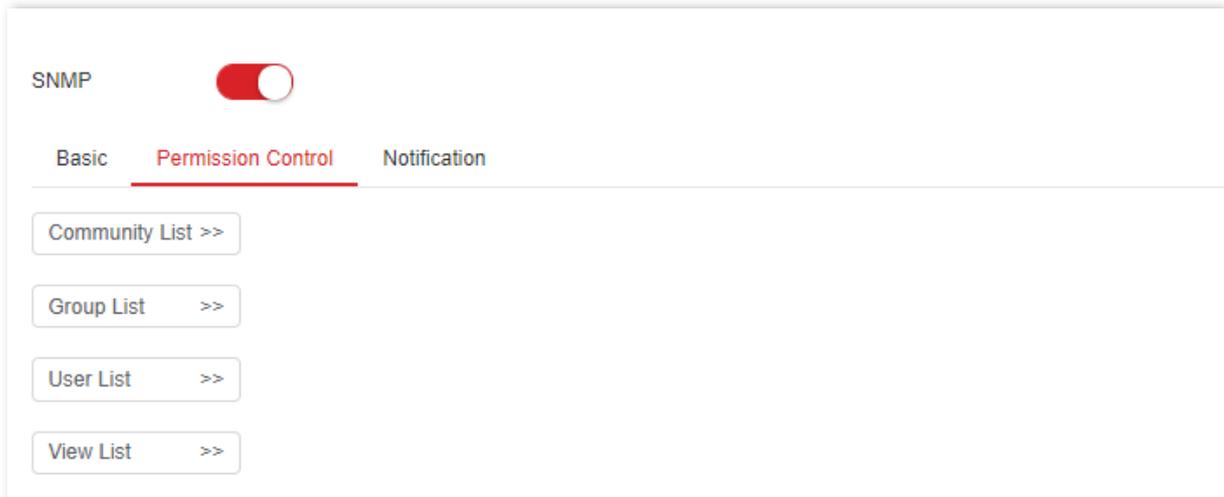
Clique em **Configurações do dispositivo** > **SNMP** > **Básico** para entrar na página. Nesta página, você pode configurar os parâmetros SNMP básicos.

Descrição do parâmetro

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

8.2.4 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

Name	Description
Nome da comunidade	Ela especifica o nome de uma comunidade.
Lista da Comunidade	Modo de Acesso Especifica a permissão de acesso para a comunidade acessar o visualizações, incluindo Somente leitura e leitura&gravação.
	Visualização MIB Especifica os modos de exibição que a comunidade pode acessar. A visualização MIB deve ser configurado em Ver lista Antecipadamente.
	Nome do Grupo Ela Especifica o nome de um grupo.
Lista de Grupos	Nível de Segurança Especifica o nível de segurança do grupo: Sem segurança, Autenticação, Autenticação&Privacidade.
	Somente leitura Controlar as permissões de acesso para usuários em um grupo por meio do
Notificação de leitura e gravação	vista. Pelo menos um dos três tipos deve ser configurado. O modo de exibição MIB deve ser configurado na Lista de Exibição com antecedência.
Nome de usuário	Ela Especifica o nome do usuário.
	Grupo de usuários Especifica o grupo do usuário. O grupo precisa ser configurado em Lista de Grupos Antecipadamente.
	Nível de Segurança Especifica o nível de segurança do usuário. Depois que o grupo do usuário é selecionado, o nível de segurança é preenchido automaticamente.
Lista de usuários	Modo de autenticação Especifica o modo de autenticação do usuário. Somente essa opção

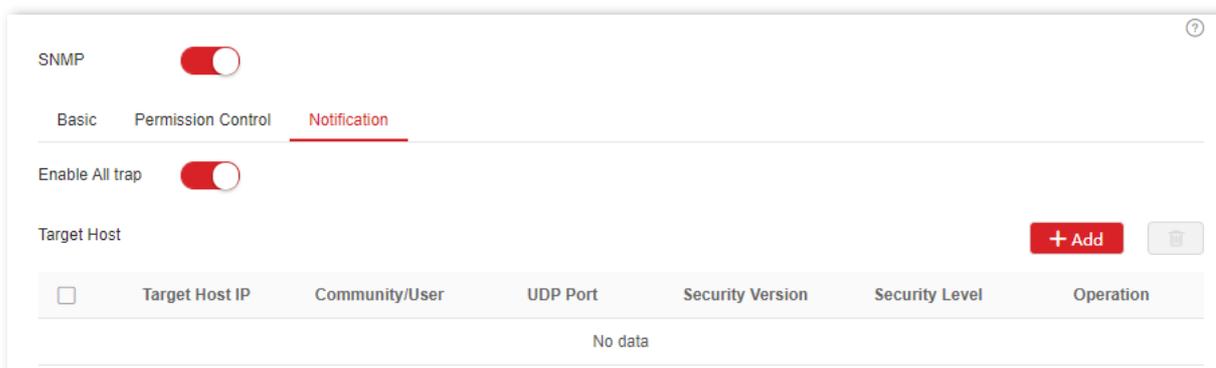
Senha de autenticação	suporta MD5 (MD5 Message Digest Algorithm). Esse parâmetro pode ser definido somente se o nível de segurança do grupo for Autenticação ou Autenticação& Privacidade .
Modo de Segurança	Especifica a senha de autenticação do usuário. Esse parâmetro pode ser definido somente se o nível de segurança do grupo for Autenticação ou Autenticação& Privacidade . Especifica o modo de segurança do usuário. Este switch suporta dois modos de segurança: AES e DES. Este parâmetro pode ser definido somente se o nível de segurança do grupo for

Nome	Descrição
	Autenticação&Privacidade.
Senha de segurança	Especifica a senha de segurança do usuário. de Esse parâmetro pode ser definido somente se o nível de segurança do grupo for Autenticação&Privacidade.
Ver Nome	Especifica o nome de um modo de exibição.
Ver lista	Regra Especifica a regra OID. - incluir: Este OID pode ser gerenciado pelo SNMP. - excluir: Este OID não pode ser gerenciado pelo SNMP.
	Subárvore MIB OID Especifica os objetos gerenciados (representados por OID) do modo de exibição.

8.2.5 Notificação

A função de notificação permite que o switch envie mensagens para o gerenciador SNMP e notifique alguns eventos importantes (como o dispositivo está reiniciando), 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 > Notificação de > SNMP** para entrar na página. Nesta página, você pode configurar a função de notificação SNMP.



Descrição do parâmetro

Nome	Descrição
Ativar todo o trap	É usado para ativar todas as traps.
IP do host de destino	Especifica o endereço IP do host de destino de interceptação, que também é o endereço IP do host gerenciado. Verifique se há rotas acessíveis entre o host de destino e esse switch.

Comunidade/Usuário		Especifica o nome da comunidade, nome de usuário ou nome de grupo exigido pela autenticação. Você precisa inserir o nome do grupo, nome de usuário ou nome da comunidade correspondente. Se a Versão de Segurança estiver definida como v3 , somente um nome de usuário ou nome de grupo será permitido. Se a Versão de Segurança estiver definida como v1 ou v2c , somente um nome de comunidade será permitido.
Porta UDP		Especifica a porta UDP habilitada para Trap no host gerenciado.
Versão de segurança	de	É usado para selecionar uma versão de segurança usada pelo Trap, incluindo v1, v2c e v3, que deve ser consistente com a versão de software do gerenciador SNMP.
Nível de Segurança	de	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 .

8.3 Hora do sistema

Para garantir que as funções baseadas no tempo do interruptor funcionem corretamente, é necessário garantir que a hora do sistema do interruptor seja precisa. Este switch suporta [configuração manual](#) e [calibração de rede](#) (padrão).

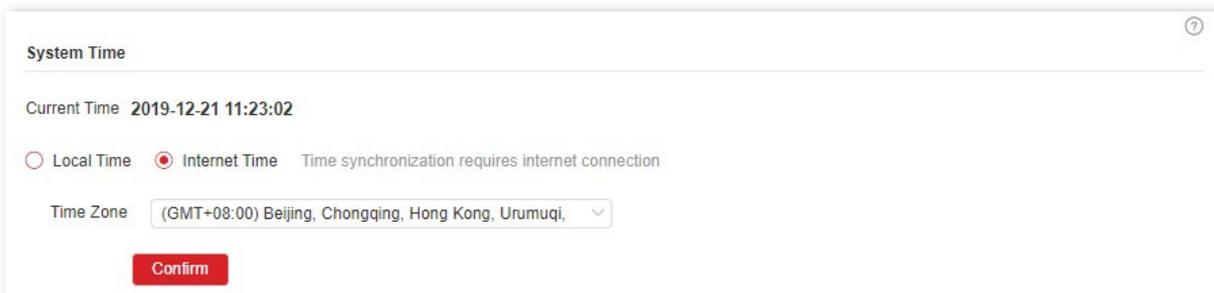
Configuração manual

O administrador de rede precisa definir manualmente a hora do sistema do switch. Depois que a opção for reiniciada para cada vez, o administrador precisará redefini-la.

Você pode modificar manualmente a data e a hora ou clicar em **Sincronizar com a Hora Local** para sincronizar a hora do comutador com o computador.

Calibração de rede

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



8.4 Manutenção

8.4.1 Atualização de firmware

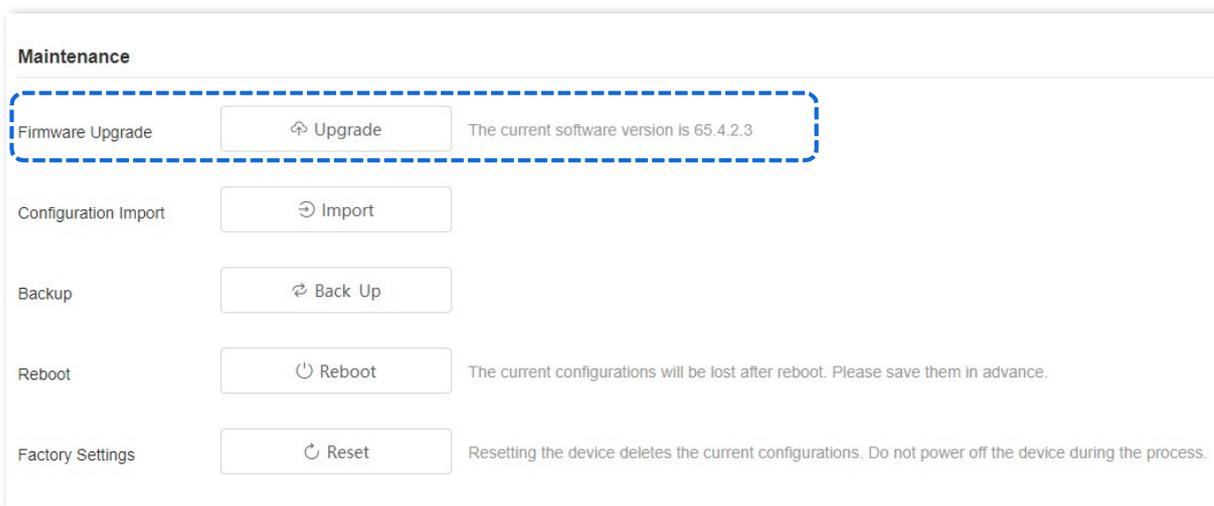
Clique em **Configurações do dispositivo** > Manutenção > Manutenção para entrar na página. Nesta página, você pode clicar em **Atualizar** para atualizar o software do switch, desfrutando de uma melhor experiência do usuário.



Nota

Para evitar danos ao switch, certifique-se de que o switch seja atualizado corretamente. Por favor, Nota que:

- Antes de atualizar, baixe o software mais recente do switch do site oficial: www.Positivo.com.cn. Geralmente, a extensão de nome de arquivo do arquivo de atualização é .bin.
- Durante o processo de atualização, assegure-se de uma fonte de alimentação estável para o interruptor.



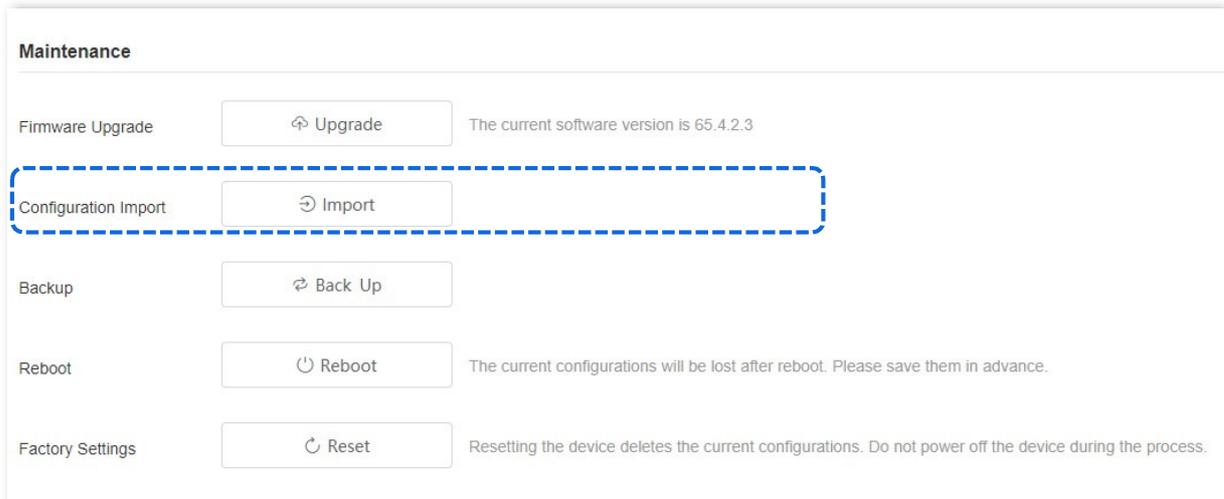
8.4.2 Importação de configuração

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



Nota

A opção não verifica o conteúdo de um arquivo, portanto, verifique se o arquivo está correto antes de importar.



8.4.3 Backup

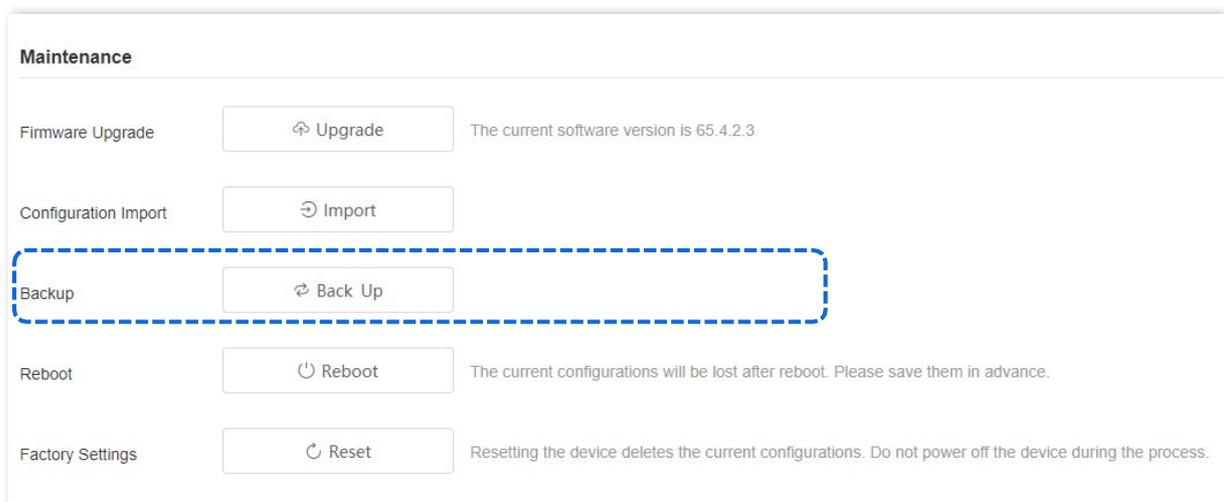
Clique em **Configurações do dispositivo** > Manutenção > Manutenção para entrar na página. Nesta página, você pode clicar em **Fazer backup** para salvar as informações de configuração do switch no computador local.

Por exemplo, se você tiver feito muita configuração no switch para melhor estado e

desempenho em um ambiente de operação específico, recomenda-se fazer backup da configuração do switch. Depois de atualizar o switch ou restaurar o switch para as configurações de fábrica, você pode importar esse arquivo de configuração de backup para restaurar o switch para o estado desejado.



Por favor,  em em o canto superior direito para salvar todas as configurações antes de fazer backup.



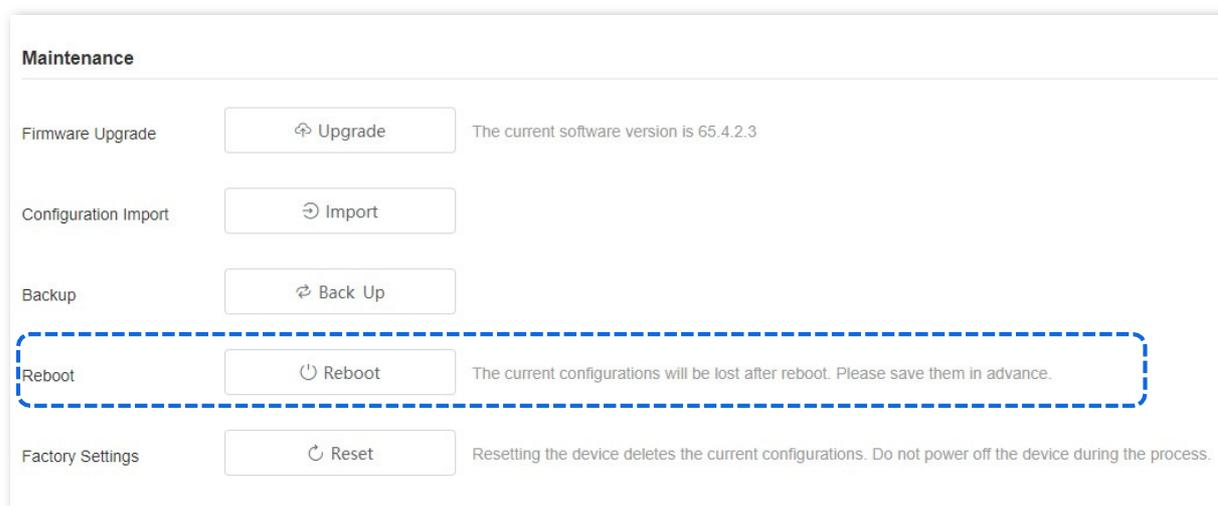
8.4.4 Reinicializar

Quando um parâmetro definido não funciona corretamente, você pode tentar reinicializar a opção para corrigir esse problema.

Clique em **Configurações do dispositivo** > Manutenção > Manutenção para entrar na página. Nesta página, você pode clicar em **Reinicializar** para reiniciar a opção.



Por favor, clique em  em o canto superior direito para salvar todas as configurações antes de reiniciar o switch.



8.4.5 Configurações de fábrica

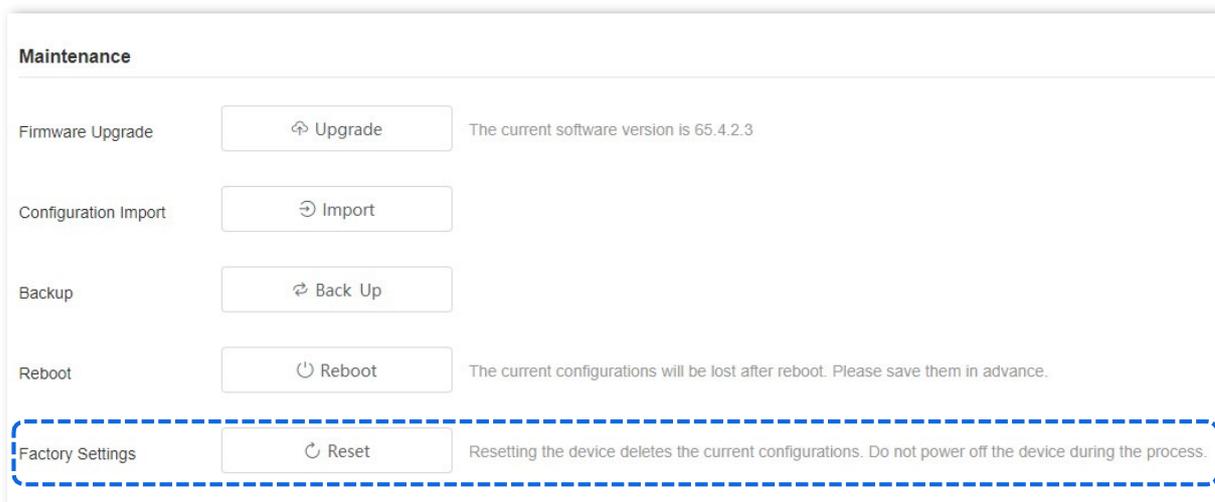
Se você esquecer seu nome de usuário ou senha ao efetuar login na interface do usuário da Web do switch, poderá restaurar as configurações de fábrica do switch e usar o nome de usuário e a senha padrão (ambos são **admin**) para fazer login. Este switch suporta [redefinição de software e redefinição de hardware](#).

Redefinição de software

Clique em **Configurações do dispositivo** > Manutenção > Manutenção para entrar na página. Nesta página, você pode clicar em **Redefinir para** restaurar a opção para as configurações de fábrica e todas as informações de configuração serão removidas.



Durante o processo de reinicialização, certifique-se de que a fonte de alimentação estável para o interruptor.



Redefinição de hardware

Quando o indicador LED de energia **estiver ligado e o indicador LED SYS** estiver piscando, pressione e segure o botão de reinicialização (**Modo LED ou LED/Reset**) por cerca de 10 segundos e solte-o quando tudo os indicadores são sólidos. Quando o indicador LED de **energia** estiver ligado e o indicador **LED SYS** piscar novamente, o interruptor será restaurado para as configurações de fábrica.

8.5 Gerenciamento de logs

8.5.1 Informações de registro

Os logs de um switch registram todas as situações e as operações do usuário depois que o switch é redefinido da última vez. Você pode verificar as informações de log do switch para solução de problemas se houver alguma falha de rede.

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

Nível de log	Valor	Descrição
Emergência	1	Informações indisponíveis do sistema
Alerta	2	Mensagem que precisa ser respondida rapidamente
Crítico	3	Informações críticas
Erro	4	Informações de erro
Aviso	5	Informações de aviso
informação	7	Notificação que precisa ser registrada
depurar	8	Mensagem gerada no processo de depuração

Clique em **Configurações do dispositivo** > Gerenciamento de Log > Informações de Log. Nesta página, você pode visualizar, baixar e excluir as informações de log do switch.

ID	Generated Time	Log Level	System Log
1	2019/12/21 11:17:18	Info	web client user admin login from 192.168.60.163
2	2019/12/21 09:23:25	Info	web client user admin login from 192.168.60.163
3	2019/12/21 09:21:27	Info	web client user admin login from 192.168.0.100
4	2019/12/21 09:17:25	Warning	Port up notification received for port ge1
5	2019/12/21 09:17:25	Warning	Port up notification received for port ge19
6	2019/12/22 09:46:33	Warning	Port down notification received for port ge1
7	2019/12/22 09:46:32	Warning	Port up notification received for port ge1

Descrição do parâmetro

Nome	Descrição
Nível de log	É usado para filtrar quais logs são exibidos por nível de log.
ID	Especifica a ID do log.
Tempo gerado	Especifica o ponto de tempo em que o log é gerado.
Nível de log	Especifica o nível do log.
Log do sistema	Ele exibe o conteúdo do log.

8.5.2 Configurações do servidor

Clique em Configurações do dispositivo > **Gerenciamento de logs** > **Configurações do servidor**. Nesta página, você pode configurar o servidor de log e carregar as informações de log do switch para o servidor.

Descrição do parâmetro

Nome	Descrição
Servidor habilitado	É usado para ativar/desativar o servidor de log.
Nível de log	Logs deste nível e acima serão carregados no servidor.
Endereço IP do servidor	Especifica o endereço IP do servidor de log. Verifique se há rotas acessíveis entre o servidor de log e esse switch.
Porta	Especifica o número da porta usado pelo servidor de log.

8.6 Diagnostics

Clique em **Configurações do dispositivo** > **Diagnóstico** para entrar na página. Nesta página, você pode executar o teste Ping/Traceroute.

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

8.6.1 Teste de ping

Clique em **Configurações do dispositivo** > Diagnóstico > Teste de Ping para entrar na página. Nesta página, você pode testar a conexão de rede.

Descrição do parâmetro

Nome	Descrição
Endereço IP de destino	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.

8.6.2 Teste Tracert

Clique em **Configurações do dispositivo** > **Diagnóstico** > **Tracert** para entrar na página. Nesta página, você pode testar as rotas do pacote do switch para o dispositivo de destino.

Descrição do parâmetro

Nome	Descrição
Endereço IP de destino	Especifica o endereço IP do dispositivo para o qual o teste Tracert deve ser executado.
Lúpulo máximo	Especifica os saltos máximos para o teste Tracert.

8.7 Configurações MAC

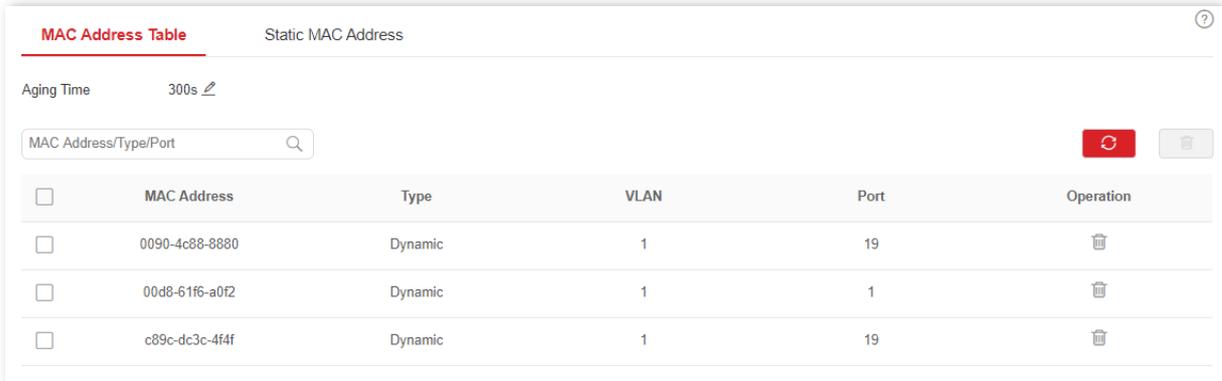
8.7.1 Tabela de endereços MAC

O switch cria a tabela de encaminhamento de endereços MAC por mecanismo de aprendizado de endereço. A tabela inclui endereço MAC, ID da VLAN e número da porta. Ao encaminhar uma mensagem, o switch adota os dois modos de encaminhamento a seguir com base na tabela de endereços MAC informação:

- 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 da tabela de endereços MAC.
- Modo de difusão: Se o switch receber uma mensagem com o endereço MAC de destino cujo bit mais baixo do segundo byte for 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 de recebimento no modo de difusão. As mensagens de transmissão, mensagens de multicast e mensagens unicast desconhecidas serão encaminhadas no modo de transmissão.

Clique em **Configurações do dispositivo** > **Configurações** MAC > **Tabela**

de **endereços MAC** para entrar na página. Nesta página, você pode exibir e excluir as entradas da tabela de endereços MAC.



Descrição do parâmetro

Nome	Descrição
Tempo de envelhecimento	<p>Especifica o tempo de envelhecimento da tabela de endereços MAC, que é eficaz apenas para entrada dinâmica.</p> <p>Quando a duração desde que o switch recebe a última mensagem cujo endereço de origem é consistente com o endereço MAC de origem na tabela excede o tempo de envelhecimento, a tabela de endereços MAC será excluída automaticamente.</p>
Endereço MAC	Endereço MAC, formato: XXXX-XXXX-XXXX
Tipo	<p>Especifica o tipo do endereço MAC.</p> <ul style="list-style-type: none"> - Estático: Especifica a entrada de endereço MAC configurada manualmente pelo administrador. - Dinâmico: Especifica a entrada de endereço MAC gerada automaticamente pelo switch.
VLAN	Especifica a VLAN à qual o endereço MAC pertence.
Porta	Especifica a porta física à qual o endereço MAC corresponde.

8.7.2 Endereço MAC estático

Clique em **Configurações do dispositivo > Configurações MAC > Endereço MAC estático** para entrar na página. Nesta página, você pode configurar a tabela de endereços MAC estáticos. A configuração existe como entradas de tabela estática na tabela de endereços MAC, além do controle do tempo de envelhecimento do MAC.

<input type="checkbox"/>	VLAN ID	MAC Address	Port	Operation
No data				

Descrição do parâmetro

Nome	Descrição
VLAN ID	Especifica a VLAN à qual o endereço MAC pertence.
Endereço MAC	Endereço MAC, formato: XXXX-XXXX-XXXX
Porta	Especifica a porta física à qual o endereço MAC corresponde.

8.8 Período de tempo



Dica

Esta seção só se aplica ao switch G5328P-24-410W.

Período de tempo é usado para configurar a data, o ciclo e o período de tempo especificados para controlar os períodos de tempo especificados durante os quais a função PoE entra em vigor.

Clique em **Configurações do dispositivo > Período** de tempo para entrar na página. Nesta página, você pode configurar o tempo de acordo com situações reais.

<input type="checkbox"/>	ID	Date	Cycle	Time Period	Operation
<input type="checkbox"/>	10	2019-11-13 00:00-2019-11-13 23:59	Mon. - Sun.	00:00-23:59	

Descrição do parâmetro

Name	Description
ID	Ela especifica a ID do período de tempo.
Data	Ela é usado para especificar as datas de início e término.
Ciclo	Ela é usado para especificar os dias do ciclo.
Período de tempo	É usado para especificar o período de tempo, e um máximo de 3 períodos de tempo são permitidos.



Nota

- Se você configurou apenas um dos **Data, Ciclo e Período de tempo**, somente o parâmetro configurado é efetivo. Se você configurou dois ou três dos parâmetros, o tempo de sobreposição será efetivo.
 - Se você configurou apenas o **Período de tempo**, o período de tempo configurado é efetivo todos os dias por padrão.
 - Se você configurou apenas o **Ciclo**, como Mon., mas fez **NÃO** configurar o **Período de tempo**, todas as 24 horas todas as segundas-feiras são eficazes.
-

9 Gestão de PoE



Esta seção só se aplica ao switch G5328P-24-410W.

9.1 Visão geral

PoE (Power over Ethernet, também conhecido como fonte de alimentação remota) refere-se à fonte de alimentação do dispositivo através da conexão externa do cabo Ethernet ao PD (Powered Device), como telefone IP, AP sem fio, câmera de rede, etc.

As vantagens da fonte de alimentação PoE são mostradas abaixo:

- Conexão conveniente: O terminal de rede só precisa de um cabo Ethernet em vez de fonte de alimentação externa.
- Estabilidade: PD suporta alimentação PoE e pode ser conectado a outra fonte de alimentação para realizar fonte de alimentação de redundância.
- Padrão: Está em conformidade com os padrões IEEE 802.3af e IEEE 802.3at, com interface de energia globalmente unificada.
- Ampla aplicação: Pode ser usado para telefone IP, AP sem fio (Access Point), carregador de dispositivo portátil, leitor de cartão, webcam, aquisição de dados, etc.
- Todas as portas 1-24 deste switch suportam a função PoE, podem detectar automaticamente PD e fornecer energia para PD em conformidade com os padrões IEEE 802.3af e IEEE 802.3at. Devido à potência limitada do sistema e de cada porta, algumas configurações devem ser feitas para o switch, a fim de garantir a potência adequada para cada PD e fazer pleno uso da energia do sistema.

9.2 Global

Clique em **Gerenciamento PoE > Global** para entrar na página. Nesta página, você pode verificar as informações da fonte de alimentação e configurar o modo de gerenciamento de energia.

The screenshot shows a configuration page titled "Global". It contains the following information:

- Power Mode:** A dropdown menu currently set to "Dynamic Allocation".
- Total Available Power:** 370W
- Total Remaining Power:** 0W
- PoE Chip Temperature:** 255.94°C
- Confirm:** A red button at the bottom of the configuration area.

Descrição do parâmetro

Nome	Descrição
Modo de alimentação	<p>É usado para selecionar um modo de energia para a fonte de alimentação PoE do switch.</p> <ul style="list-style-type: none"> - Alocação Estática: Permite configurar uma alimentação para cada porta do switch. Quando o switch fornece energia PoE, a energia configurada será obrigatoriamente reservada para essa porta e não poderá ser usada por outras portas. - Alocação dinâmica: O switch aloca energia com base na energia consumida por cada porta. Ao atingir a carga total, o switch aloca energia com base na prioridade da porta configurada (prioridade + número da porta). Se as prioridades forem as mesmas, a porta com o número de porta menor terá uma prioridade maior.
Potência Disponível Total	Especifica a potência máxima suportada pelo switch.
Potência Restante Total	Especifica a potência restante do switch.
Temperatura do chip PoE	Especifica a temperatura do chip PoE.

9.3 Configurações de porta

Clique em **Gerenciamento PoE > Configuração** da Porta para entrar na página. Nesta página, você pode configurar os parâmetros PoE das portas desse switch.

Port	PoE Status	Power Supply Standard	Transmitted Power	PD Level	Priority	Static Allocation Power	Time Period ID	操作
1	●	AT	0.00W	--	Low	30.0W	--	
2	●	AT	0.00W	--	Low	30.0W	--	
3	●	AT	0.00W	--	Low	30.0W	--	
4	●	AT	0.00W	--	Low	30.0W	--	
5	●	AT	0.00W	--	Low	30.0W	--	
6	●	AT	0.00W	--	Low	30.0W	--	
7	●	AT	0.00W	--	Low	30.0W	--	
8	●	AT	0.00W	--	Low	30.0W	--	

Descrição do parâmetro

Nome	Descrição
Porta	Especifica o número da porta.
PoE Status	Especifica o status da fonte de alimentação PoE da porta. ● : A função de fonte de alimentação PoE da porta está ativada e a alimentação é fornecida normalmente. ● : A função de fonte de alimentação PoE da porta está ativada, mas nenhuma energia é fornecida. ○ : A função de fonte de alimentação PoE da porta está desativada.
Padrão da fonte de alimentação	Especifica o padrão de fonte de alimentação das portas: AT (IEEE 802.3at) ou AF (IEEE 802.3af). A potência máxima de cada porta sob o padrão AT é de 30 W, enquanto que sob o padrão AF é de 15,4 W.
Potência transmitida	Especifica a potência PoE em tempo real da porta.
Nível PD	Especifica o nível do dispositivo alimentado por PoE conectado à porta atual quando a fonte de alimentação estiver normal. O switch obtém automaticamente o nível do dispositivo.

Prioridade	<p>As portas com prioridades só entram em vigor no modo dinâmico.</p> <p>Especifica a prioridade da porta atual, que entra em vigor somente quando o Modo de Energia é definido como Alocação Dinâmica. Uma prioridade de porta razoável garante que as portas especificadas ainda possam fornecer energia corretamente sob o estado de carga total. Entre os portos com prioridades diferentes, os portos com prioridades mais elevadas devem ter garantida a potência necessária primeiro. Entre as portas com uma mesma prioridade, as portas com IDs menores devem ter a energia necessária garantida primeiro.</p>
Potência de Alocação Estática	<p>Especifica o poder de alocação estática da porta atual, que leva efeito somente quando o Modo de Energia estiver definido como Alocação Estática.</p>
ID do período de tempo	<p>Especifica o período habilitado da função PoE para a porta, que precisa ser definido na seção Período de tempo. "--" indica que a porta não está atribuída com o período de tempo e a energia PoE está ativada em todos os Hora.</p>

Apêndice

A.1 Precauções de segurança

Antes de realizar uma operação, leia as instruções de operação e precauções a serem tomadas, e siga-as para evitar acidentes. Os itens de advertência e perigo em outros documentos não abrangem todas as precauções de segurança que devem ser seguidas. São apenas complementares informações, o pessoal de instalação e manutenção precisa entender as precauções básicas de segurança a serem tomadas.

1. Não utilize este aparelho perto da água.
2. Limpe apenas com pano seco.
3. Não bloqueie nenhuma abertura de ventilação, como jornais, toalhas de mesa, cortinas, etc.
4. Não instale perto de quaisquer fontes de calor, como radiadores, registradores de calor, fogões ou outros aparelhos que produzam calor.
5. Não danifique o condutor de terra nem opere o dispositivo na ausência de condutor de terra bem instalado. Realizar a inspeção elétrica adequada.
6. Proteja o cabo de alimentação de ser pisado ou beliscado, especialmente nas tomadas, recipientes de conveniência e no ponto em que eles saem do aparelho.
7. Utilize apenas acessórios/acessórios especificados pelo fabricante.
8. Desligue este aparelho da tomada durante tempestades de iluminação ou quando não for utilizado por longos períodos de tempo.
9. A ficha de alimentação é utilizada como dispositivo de desconexão, o dispositivo de desconexão deve permanecer prontamente operável.
10. Encaminhe todos os serviços para pessoal de serviço qualificado. A manutenção é necessária quando o aparelho tiver sido danificado de alguma forma, como o cabo de alimentação ou o plugue estiver danificado, o líquido tiver sido derramado ou objetos tiverem caído no aparelho, o aparelho tiver sido exposto à chuva ou umidade, não opera normalmente, ou foi derrubado.

11. Atenção: Para reduzir o risco de incêndio ou choque elétrico, não exponha este aparelho à chuva ou umidade. O aparelho não deve ser exposto a gotejamentos ou salpicos.

12. Aviso: Para reduzir o risco de choque elétrico, não remova a tampa, pois não há peças reparáveis no interior. Encaminhe a manutenção para pessoal qualificado.

A.2 Siglas e Abreviaturas

Sigla ou Abreviatura	Ortografia completa
ACL	Lista de Controle de Acesso
ARP	Protocolo de Resolução de Endereço
CIST	Spanning Tree comum e interna
DHCP	Protocolo de Configuração Dinâmica de Host
DoS	Negação de Serviço
IGMP	Protocolo de Gerenciamento de Grupo da Internet
LLDP	Protocolo de descoberta de camada de link
MSTP	Protocolo de Spanning Tree múltipla
OID	Identificador de objeto
Poe	Alimentação sobre Ethernet
QoS	Qualidade de Serviço
RSTP	Protocolo de Spanning Tree rápida
SNMP	Protocolo de Gerenciamento de Rede Simples
STP	Protocolo de Spanning Tree
TPID	Identificador de protocolo de tag
TCI	Informações de controle de tags
VLAN	Rede Local Virtual