Manual do Usuário

SG 2404 PoE L2+

Versão deste manual: 1.1.1

SG 2404 PoE L2+

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

O SG 2404 PoE L2+ é um switch de 24 portas PoE Gigabit Ethernet com 4 portas Mini-GBIC independentes. Atende aos padrões IEEE802.3af e IEEE802.3at, podendo fornecer potência máxima de até 192 W, distribuídos conforme o padrão utilizado e a quantidade de portas disponíveis. Com a tecnologia PoE é possível transmitir energia elétrica e dados através do mesmo cabo de rede (cat5 ou superior) para dispositivos compatíveis com os padrões 802.3af ou 802.3at, eliminando a necessidade de tomadas para os produtos alimentados, minimizando os custos de instalação.

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

ÍNDICE

TERMO DE GARANTIA

FALE COM A GENTE

EXPORTAR PARA PDF

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

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

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

PROTEÇÃO E SEGURANÇA DE DADOS

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

Tratamento de dados pessoais

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

Diretrizes que se aplicam aos funcionários da Intelbras

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

Diretrizes que controlam o tratamento de dados

- Assegurar que apenas pessoas autorizadas tenham acesso aos dados de clientes.

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

Uso indevido e invasão de hackers

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

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

SOBRE O MANUAL

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

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

Este manual contém informações para instalação e gerenciamento do switch SG 2404 PoE L2+. Por favor, leia-o com atenção antes de operar o produto.

Público destinado para o manual

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

Convenções

Neste manual as seguintes convenções serão usadas:

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

Estrutura do manual

Capítulo	Introdução
1 – Sobre o manual	Introdução de como o manual está estruturado.
2 – Introdução	Especificações gerais do produto.
3 – Acessando o Switch	Introdução para acessar a interface de gerenciamento do produto.
4 – Sistema de Gestão	Este módulo é utilizado para configurações do sistema e propriedades do switch. - Informações: configuração da descrição, tempo do sistema e parâmetros de redes do switch. - Usuários: configuração de usuários e senhas, além de configurar o nível de acesso para cada usuário. - Ferramentas: manipulação dos arquivos de configuração do switch. - Gerenciamento: fornece diferentes medidas de segurança para acessar o gerenciamento web do switch. - Configuração PoE: configuração geral da função PoE. - Agendamentos: configuração de data e hora específicos para o funcionamento do PoE.
5 – Gerenciando as Interfaces Físicas	Este módulo é utilizado para configurar as funções de interfaces físicas do switch. - Configurações básicas: configuração de status, velocidade, tipo de conexão, controle de fluxo e configuração de MTU. - Isolamento de Portas: configurações para controle de dados que a porta pode encaminhar e sua lista de encaminhamento. - Loopback Detection: configurações para controle de Loop na rede.
6 – Configuração LAG	Este módulo é utilizado para configurar a função de grupos de Link Aggregation. Para unir múltiplas interfaces físicas em uma interface lógica para aumentar a banda e a confiabilidade.

7 – Gerenciamento a Tabela de endereço MAC	Este módulo é utilizado para configurar as funções da tabela MAC do switch. - Tabela de endereço MAC: contém as informações dos endereços físicos que o switch utiliza para encaminhar pacotes. - Configurações de Endereço MAC: configura as entradas de endereços na tabela, seu tempo de aging e entradas de filtro.
8 – VLAN 802.1Q	Este módulo é utilizado para configurar VLANs. - VLAN 802.1Q: configuração de VLANs baseadas em TAG de VLAN e portas.
9 – MAC VLAN	Este módulo é utilizado para configurar VLANs baseadas em MAC.
10 –VLAN de Protocolo	Este módulo é utilizado para configurar VLANs baseadas em Protocolo.
11 – GVRP	Este módulo é utilizado para configurar a função de GVRP do switch.
12 – Multicast de Camada 2	Este módulo é utilizado para configurar a função Multicast do switch. - IGMP Snooping: configuração global dos parâmetros IGMP Snooping, propriedade da porta, VLAN e Multicast VLAN. - Multicast estático: configuração da tabela de IP Multicast estático e visualização da tabela de endereços Multicast. - Filtro Multicast: configuração dos recursos de filtros de endereços Multicast. - Estatísticas IGMP: visualização das mensagens IGMP em cada porta do switch.
13 – STP	Este módulo é utilizado para configurar a função Spanning Tree no switch. - Spanning Tree: configuração e visualização das configurações globais da função Spanning Tree. - Portas STP: configuração dos parâmetros da função STP para cada porta. - Instâncias MSTP: configuração de instâncias MSTP. - Segurança STP: configuração de proteção contra invasões maliciosos à função STP.

14 – LLDP	Este módulo é utilizado para configurar a função LLDP, fornecendo informações para aplicações SNMP, simplificando a solução de problemas. - Configuração LLDP: configuração dos parâmetros de funcionamento da função LLDP. - Informações dos dispositivos: visualização das informações LLDP do dispositivo local e dispositivo vizinho. - Estatísticas LLDP: visualização das estatísticas LLDP do dispositivo local. - LLDP-MED: configuração dos parâmetros da função LLDP-MED do dispositivo local.
15 – Interfaces de Camada 3	Este módulo é utilizado para configurar a função
16 – Roteamento	Este módulo é utilizado para configurar a função
17 – DHCP	Este módulo é utilizado para configurar a função
18 – ARP	Este módulo é utilizado para configurar e visualizar a tabela ARP. - Tabela ARP:
19 – QoS	Este módulo é utilizado para configuração de QoS, provendo qualidade e priorizando serviços desejados. - DiffServ: configuração de prioridade por porta, 802.1P e DSCP, além de configuração do algoritmo de fila. - Controle de banda: configuração do limite de banda e Storm Control por porta.
20 – Segurança de Acesso	Este módulo é utilizado para configurar a função de Segurança de Acesso. - Controle de Acesso: Você pode controlar o acesso dos usuários ao switch filtrando endereços IP, endereços MAC ou porta nesta página. - Configuração HTTP: Você pode permitir ou negar o acesso de usuários ao switch por um navegador web nesta página. - Configuração HTTPs: Você pode permitir ou negar o acesso de usuários ao switch por um navegador web nesta página. - Configuração SSH: SSH (Shell de Segurança) fornece segurança e autenticação poderosa para um gerenciamento remoto não seguro, a fim de garantir que a informação de gerenciamento está protegida. - Configuração Telnet: Você pode configurar o login telnet nesta página.

21 – AAA	Este módulo é utilizado para configurar a função AAA (Autenticação, Autorização, Contabilidade), a autenticação pode ser processada localmente no switch ou em servidores. - Configuração Global: Você pode configurar múltiplos servidores e métodos de autenticação ao mesmo tempo, para garantir a estabilidade do sistema de autenticação. - Configuração de Método: Uma lista de método descreve os métodos de autenticação e sua sequência para autenticar os usuários. - Configuração Dot1x: Você pode configurar grupos de servidor RADIUS para autenticação e contabilidade 802.1X nesta página. - Grupo Servidor: Você pode editar grupos de servidor existentes, ou adicionar novos grupos de servidor. - Configuração RADIUS: Você pode adicionar um ou mais servidores RADIUS ao switch para autenticação. - Configuração TACACS+: Você pode adicionar um ou mais servidores TACACS+ ao switch para autenticação
22 – 802.1x	Este módulo é utilizado para configurar a função 802.1x. - Configuração Global: Você pode usar o protocolo 802.1x para autenticar e controlar o acesso de dispositivos conectados às portas. - Configuração de Porta: Você pode configurar a autenticação 802.1x na porta desejada. - Estado do Autenticador: Você pode visualizar o estado de autenticação nesta página. Selecione uma porta para a qual você deseja visualizar o estado de autenticação.
23 – Segurança de Porta	Este módulo é utilizado para configurar as funções de segurança de porta. Você pode limitar o número de endereços MAC que pode ser aprendido em cada porta nesta página, assim evitando que a tabela de endereços MAC seja exaurida pelos pacotes do ataque.

24 – ACL	Este módulo é utilizado para configurar a função ACL e criar listas de controle de acesso. - Configuração ACL: você pode criar diferentes tipos de ACL e definir as regras com base na fonte MAC ou IP, no destino MAC ou IP, tipo de protocolo, número da porta e assim por diante. Então, os registros ACL que você configurou serão exibidos na tabela ACL. - Vinculo ACL: Você pode vincular ACL a uma porta nesta página.
25 – IPv4 IMPB	Este módulo é utilizado para configurar a função IPv4 IMPB - Vinculo IPv4 para vincular um endereço IP e/ou endereço MAC à uma porta como um registro. - A função ND Detection usa os registros na tabela de vinculação IPv6-MAC para filtrar pacotes ND forjados e evitar ataques ND. - A função IPv4 Source Guard permite que o switch filtre os pacotes que não correspondem às regras na Tabela de Vinculação IPv6-MAC.
26 – IPv6 IMPB	Este módulo é utilizado para configurar a função IPv6 IMPB - Vinculo IvPv6 para vincular um endereço IP e/ou endereço MAC à uma porta como um registro. - A função ND Detection usa os registros na tabela de vinculação IPv6-MAC para filtrar pacotes ND forjados e evitar ataques ND. - A função IPv6 Source Guard permique que o switch filtre os pacotes que não correspondem às regras na Tabela de Vinculação IPv6-MAC.
27 – Filtro DHCP	Este módulo é utilizado para configurar a função de Filtro DHCP para filtrar pacotes ilegais.
28 – DoS	Este módulo é utilizado para configurar a função DOS. A função DoS (Negativa de Serviço) Defend fornece proteção contra ataques DoS.
29 – Monitoramento do Sistema	Este módulo é utilizado para visualizar o uso de memória e CPU
30 – Monitoramento Trafego	Este módulo é utilizado para configurar a função de monitoramento de trafego das interfaces físicas.
31 – Espelhamento de Trafego	Este módulo é utilizado para configurar a função de espelhamento de trafego para análise em uma porta de monitoramento.
32 – DLDP	Este módulo é utilizado para configurar a função

33 – SNMP & RMON	Este módulo é utilizado para configurar a função SNMP, provendo um monitoramento e gerenciamento do switch na rede. - SNMP: define as configurações globais da função SNMP. - Notificação: configuração das notificações (Trap e Inform) enviadas para a estação de gerenciamento. - RMON: configuração da função RMON para monitorar a rede de forma mais eficiente.
34 – Diagnóstico do Dispositivo e Rede	Este módulo é utilizado para monitorar o switch e diagnosticar possíveis problemas na rede. - Monitoramento: monitoramento da utilização da Memória e CPU do Switch. - Log: permite classificar, visualizar e gerenciar informações do sistema de forma eficaz. - Ferramentas: teste o estado do cabo de rede conectado ao switch e também a disponibilidade das portas do switch. - Diagnóstico: testa se o endereço IP de destino está ao alcance do switch, bem como a quantidade de saltos necessários até alcançá-lo.
35 – Logs do Sistema	Este módulo é utilizado para visualizar e configurar os logs locais e remotos e realizar o backup dos logs do sistema.

INTRODUÇÃO

Visão geral do Switch

Projetado para grupos de trabalho e departamentos, o switch SG 2404 PoE L2+ da Intelbras possui um alto desempenho e um conjunto completo de recursos de gerenciamento de camada 2 e 3. Ele fornece uma variedade de características com elevado nível de segurança. A capacidade de configuração inteligente fornece soluções flexíveis para uma escala variável de redes. Filtro de endereço MAC, isolamento e segurança das portas fornecem uma robusta estratégia de segurança. O QoS e IGMP Snooping/filtro otimizam as aplicações de voz e vídeo. A agregação de link permite o aumento da velocidade do link além dos limites nominais de uma única porta, evitando gargalos na rede. SNMP, RMON e web trazem uma grande variedade de políticas de gerenciamento. O SG 2404 PoE L2+ possui todas as suas 24 portas RJ45 com suporte à função PoE, podendo detectar automaticamente os dispositivos que são alimentados por PoE e que atendam as normas IEEE802.3af ou IEEE802.3at, além de trazer múltiplas funções com excelente desempenho e facilidade de gerenciamento, o que corresponde a total necessidade dos usuários que exigem um grande desempenho da rede.

Principais funções

Resiliência e disponibilidade

- Agregação de link, aumenta a largura de banda agregada, otimizando o transporte de dados críticos.
- IEEE802.1s Multiple Spanning Tree, oferece alta disponibilidade de link em ambientes com várias VLANs.
- Snooping Multicast previne automaticamente a inundação de tráfego IP Multicast.
- Root Guard, protege a bridge raiz de ataques maliciosos ou erros de configurações da função spanning Tree.

Protocolos da camada de enlace

- Suporte a 512 VLANs ativas e 4K VLAN ID.

Qualidade de serviço

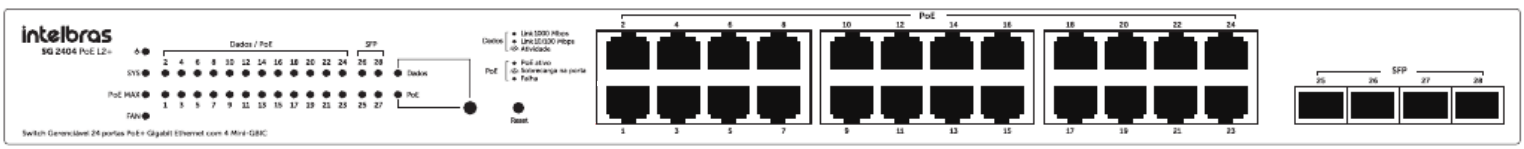
- Suporte a QoS nas camadas 2/3 com até 4 filas de prioridade por porta.
- Controle de banda por porta, limitando o tráfego de acordo com o valor determinado.

Gerenciamento

- Suporte a SNMP v1/v2c/v3, RMON e acesso web.

Descrição do produto

O painel frontal do SG 2404 PoE L2+ possui 24 portas Gigabit Ethernet 10/100/1000 Mbps e mais 4 portas Mini-GBIC independentes (100/1000 Mbps), 1 botão reset e 1 botão para o monitoramento da função PoE, além de LEDs para o monitoramento.



- Portas 10/100/1000 Mbps: 24 portas 10/100/1000 Mbps para conectar dispositivos com velocidade de 10 Mbps, 100 Mbps ou 1000 Mbps. Cada porta possui 1 LED correspondente.
- Portas Mini-GBIC (SFP): 4 portas Mini-GBIC independentes para conectar módulos SFP de 100 Mbps ou 1000 Mbps.
- Reset: botão utilizado para retornar as configurações do switch ao padrão de fábrica.

LEDs

No painel frontal são apresentados 34 LEDs de monitoramento, que seguem o comportamento a seguir:

Quando o LED Dados está aceso

LED	Status		Indicação
Power	Aceso		Switch conectado na fonte de alimentação.
	Piscando		Switch com problema na fonte de alimentação.
	Apagado		Switch desligado ou com problema na fonte de alimentação.
SYS	Aceso		Switch está funcionando de forma anormal.
	Piscando		Switch funcionando normalmente.
	Apagado		Switch está funcionando de forma anormal.
Link/Atividade	Aceso		Conexão válida estabelecida, sem recepção/transmissão de dados.
	Piscando		Conexão válida estabelecida, com recepção/transmissão de dados.
	Apagado		Nenhuma conexão válida nesta porta ou a porta está desativada.
10/100/1000 Mbps	Verde	Aceso	Conexão a 1000 Mbps estabelecida, sem transmissão/recepção de dados.
		Piscando	Conexão a 1000 Mbps estabelecida, com transmissão/recepção de dados.
	Laranja	Aceso	Conexão a 10/100 Mbps estabelecida, sem transmissão/recepção de dados.
		Piscando	Conexão a 10/100 Mbps estabelecida, com transmissão/recepção de dados.
	Apagado		Nenhuma conexão válida nesta porta, ou a porta está desativada.

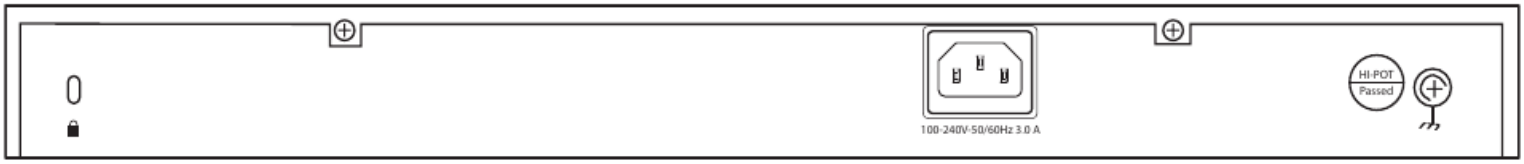
Quando o LED PoE está aceso

LED	Status	Indicação
Power	Aceso	Switch conectado a energia elétrica.
	Piscando	Switch com problema na fonte de alimentação.
	Apagado	Switch desligado ou com problema na fonte de alimentação.
SYS	Aceso	Switch está funcionando de forma anormal.
	Piscando	Switch funcionando normalmente.

	Apagado		Switch está funcionando de forma anormal.
PoE MAX	Aceso		A potência PoE remanescente é ≤ 7 W.
	Piscando		A potência PoE remanescente permanece ≤ 7W após 2 minutos acesa.
	Apagado		A potência PoE remanescente é ≥ 7W.
10/100/1000 Mbps	Verde	Aceso	A porta está fornecendo energia normalmente.
		Piscando	O fornecimento de energia excede a potência máxima da porta.
	Laranja	Aceso	Detecção de sobrecarga ou curto-circuito na porta correspondente.
		Piscando	Falha no auto teste da porta correspondente.
	Apagado		Nenhum dispositivo conectado à porta.
			Dispositivo (PD) conectado à porta não atende a norma IEEE802.3af ou IEEE802.3at

Painel posterior

O painel posterior possui um conector de alimentação de energia elétrica e um terminal de aterramento, representado pelo símbolo ⏚.



- **Terminal de aterramento:** além do mecanismo de proteção a surto elétrico que o switch possui, você deve utilizar o terminal de aterramento a fim de garantir uma maior proteção. Para informações mais detalhadas, consulte o Guia de instalação.
- **Conector do cabo de energia:** para ligar o switch, conecte o cabo de energia (fornecido com o equipamento) no conector do switch e a outra ponta em uma tomada elétrica no padrão brasileiro de 3 pinos. Após energizá-lo, verifique se o LED PWR está aceso, indicando que o switch está conectado à rede elétrica e pronto para ser utilizado. Para compatibilidade com os padrões elétricos mundiais, este switch é projetado para trabalhar com uma fonte de alimentação automática com variação de tensão de 100 a 240 VCA, 50/60 Hz. Certifique-se que sua rede elétrica esteja dentro desta faixa.

ACESSANDO O SWITCH

Visão geral

Você pode acessar e gerenciar o switch usando a interface gráfica GUI (graphical User interface) ou utilizando a interface CLI (Command Line Interface). Na interface web existem funções equivalentes às funções da interface de linha de comando, apresentadas de uma forma mais simples, visual e intuitiva que a configuração CLI. Você pode escolher o método de configuração de acordo com a disponibilidade de aplicação e sua preferência.

Acesso à Interface Web

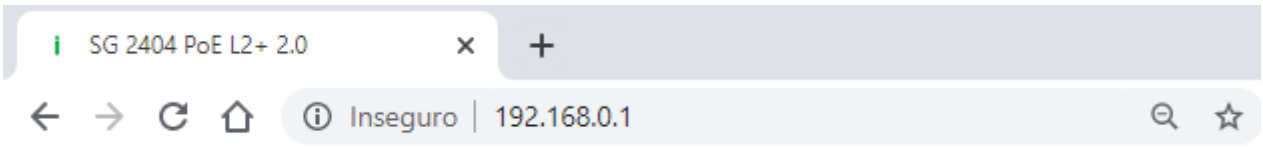
Você pode acessar a interface web do switch através de autenticação web. O switch utiliza dois servidores de acesso web, HTTP e HTTPS, para autenticação do usuário.

Os exemplos à baixo mostram como realizar o login através do servidor HTTP.

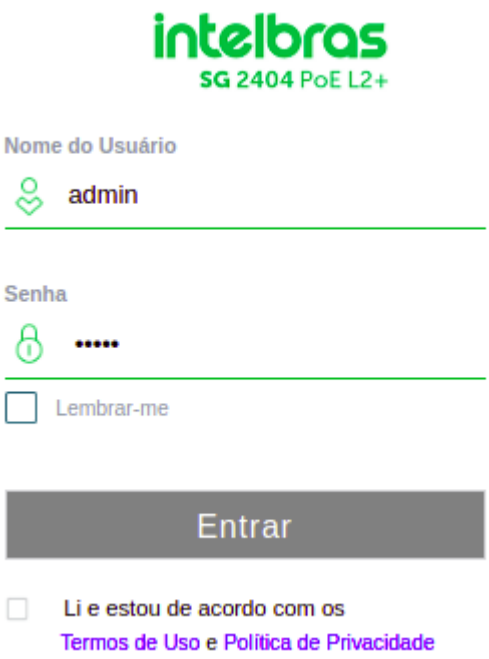
Login

Para gerenciar seu Switch através de um navegador de internet no seu computador:

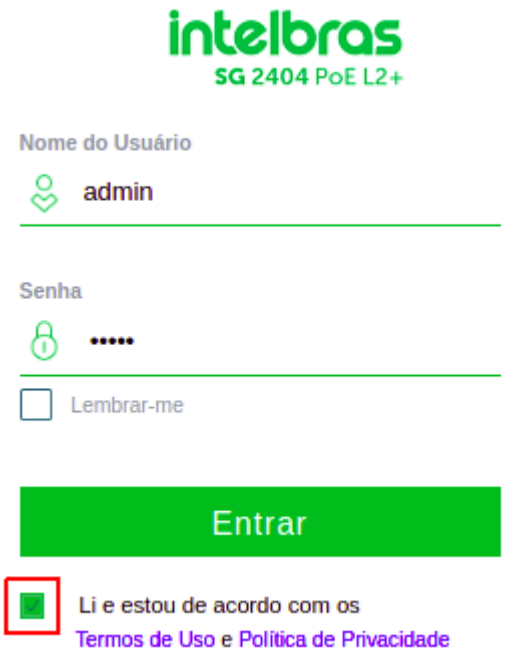
1. Garanta que a conexão entre o computador e o switch esteja ativa;
2. Abra seu navegador. Os navegadores com suporte à interface, não exclusivamente, são os seguintes:
   a. IE 8.0 ou superior;
   b. Firefox 26.0 ou superior;
   c. Chrome 32.0 ou superior.
3. Digite o endereço IP do Switch na barra de endereços do seu navegador. O endereço Padrão do switch é 192.168.0.1.



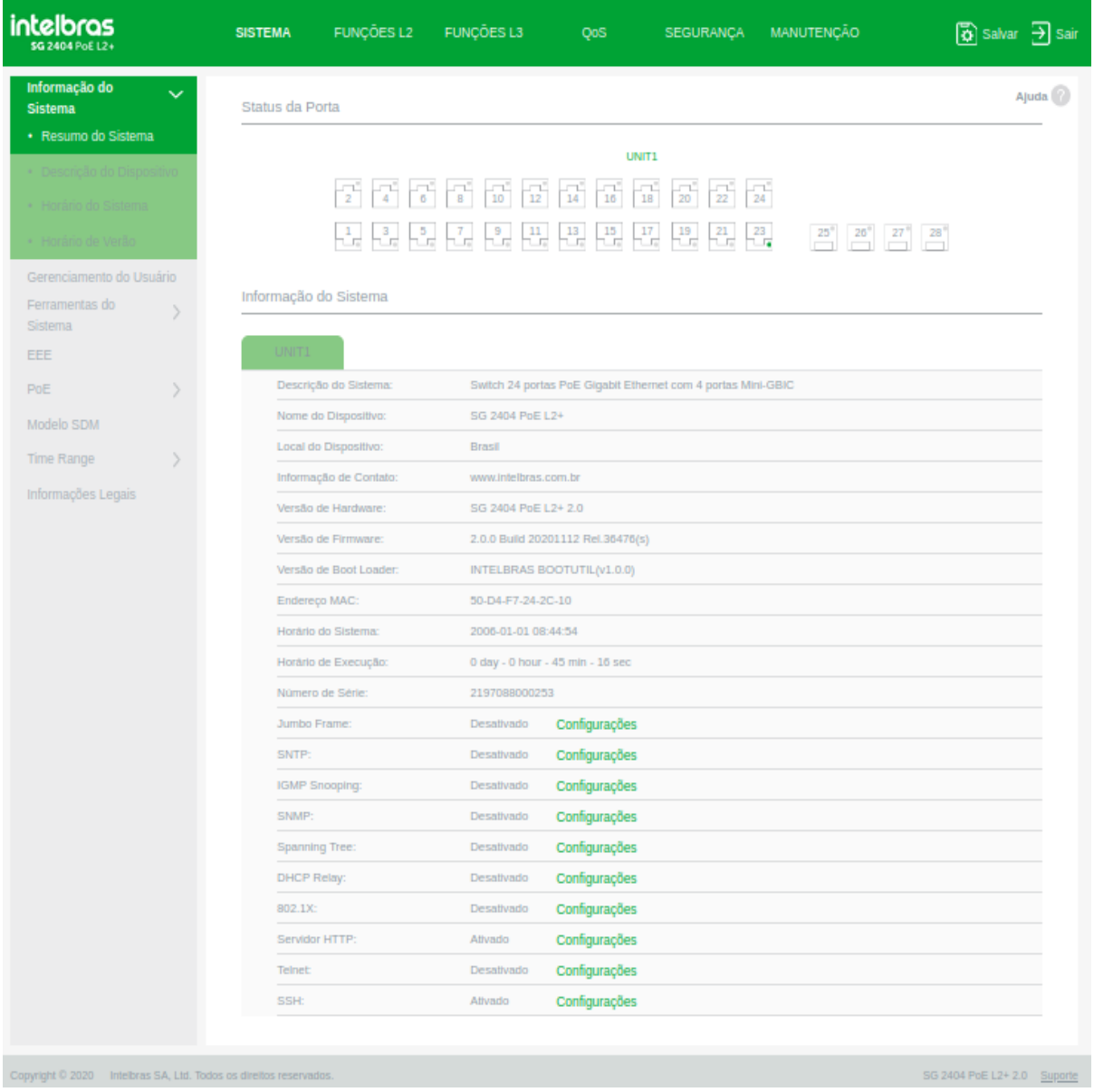
4. Digitando o nome de usuário e a senha na janela de login. O usuário padrão é **admin** e a senha padrão é **admin**.



5. Os Termos de Uso (https://backend.intelbras.com/sites/default/files/download/politicas-privacidade/termos-unificados/portugues-termo_unificado_sw_app_cloud/termos-de-uso-unico-portugues.html?prod=4780033) e a Política de Privacidade (https://backend.intelbras.com/sites/default/files/download/politicas-privacidade/termos-unificados/portugues-termo_unificado_sw_app_cloud/politica-de-privacidade-unica-portugues.html) devem ser aceitos assinalando o *Checkbox.* Assim, o *login* será liberado.



6. Na tela abaixo é possível ver a interface web típica. Você também pode ver o estado de operação do switch e configurar o switch nessa interface.

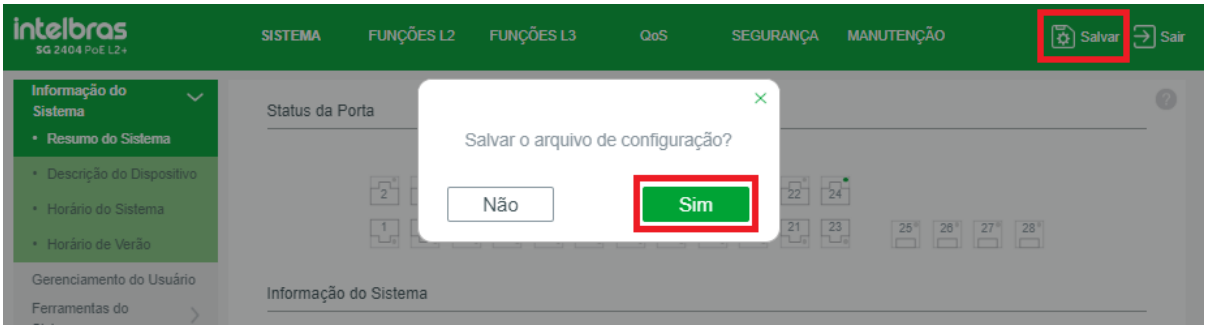


Função de salvar a configuração

O arquivo de configuração do switch é dividido em dois tipos: arquivo de configuração de operação e arquivo de configuração de inicialização.

Após você executar configuração nas subinterfaces e clicar em **Aplicar**, as modificações serão salvas no arquivo de configurações de operação. A configuração será perdida quando o switch reiniciar.

Se você precisa manter as configurações após o reinicio do switch utilize a função salvar na interface principal para **salvar** as configurações no arquivo de configuração de inicialização.

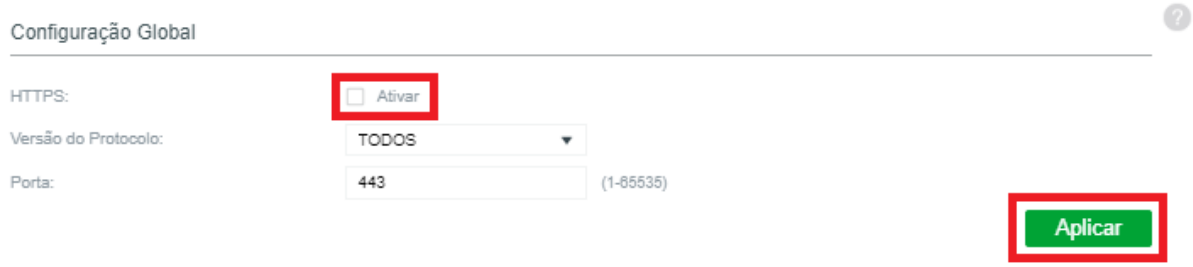


Desabilitando o Servidor Web

Você pode desabilitar o servidor HTTP ou HTTPs bloqueando qualquer acesso à interface web.

Vá para **Segurança > Segurança de Acesso > Configuração HTTP**, desabilite o servidor HTTP e clique em **Aplicar**.

Vá para **Segurança > Segurança de Acesso > Configuração HTTPS**, desabilite o servidor HTTPS e clique em **Aplicar**.



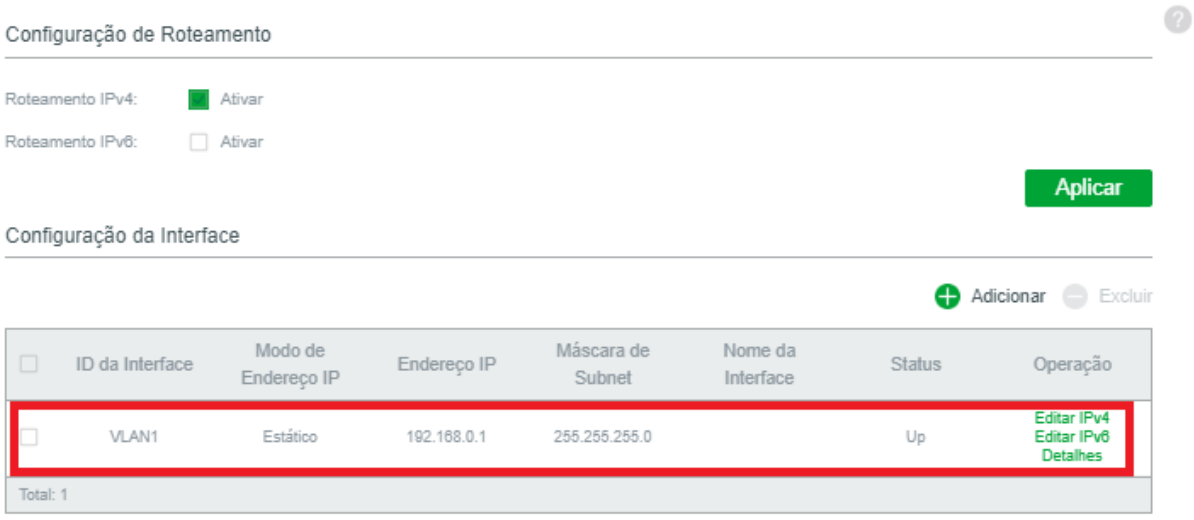
Configure o endereço IP e o Gateway padrão do Switch

Se você desejar acessar o switch através de uma porta específica (Será tratada como acesso à porta futuramente), você pode configurar a porta como porta roteada e especificar seu endereço IP, ou configurar o endereço IP da VLAN a qual a porta de acesso pertence.

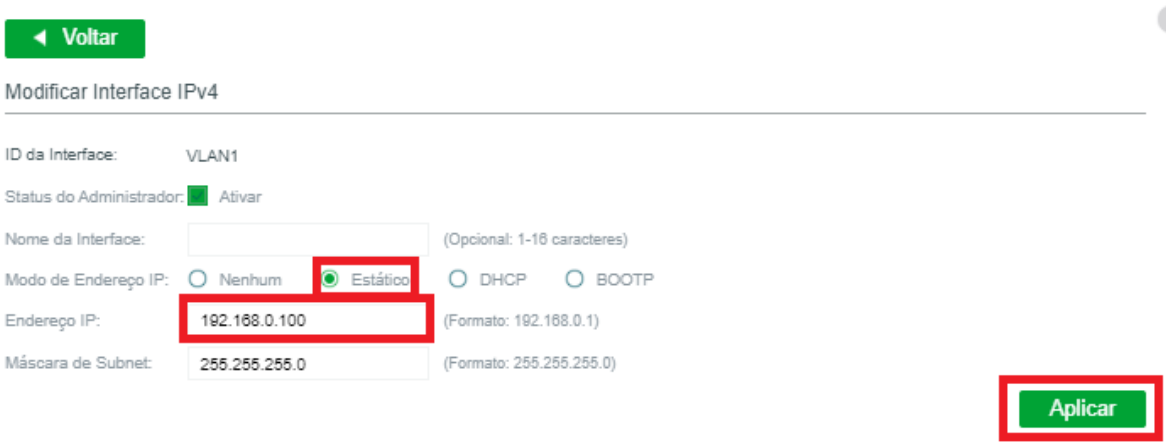
- **Alterando o endereço IP**

  Por padrão, todas as portas pertencem à VLAN 1 com a interface 192.168.0.1. Os próximos exemplos mostram como alterar o endereço padrão para acesso ao switch.

  1. Vá para **Funções L3 > Interface**. O endereço IP padrão de acesso à VLAN 1 na lista de interface. Clique em **Editar IPv4** para alterar o endereço IP da VLAN 1;



  2. Escolha o **Modo de Endereço IP** como **Estático**. Digite o novo endereço no campo **Endereço IP** e clique em **Aplicar**. Garanta que a rota entre o computador de acesso e o novo endereço IP do Switch seja válida.



3. Digite o novo endereço IP na barra de endereço do seu navegador para acessar o switch.
4. Clique no botão **Salvar** para guardar as configurações.

- **Configure o Gateway Padrão**

Os exemplos a seguir mostram como configurar o Gateway para o switch. Por padrão o switch não possui nenhum Gateway Padrão configurado.

1. Vá para **Funções L3 > Rota Estática > Rota Estática IPv4**. Clique no botão **Adicionar** para carregar a próxima página e configurar os parâmetros relacionados ao Gateway do switch. Então clique em **Criar**;

Destino	Especifique o destino como 0.0.0.0.
Máscara de SubRede	Especifique a máscara como 255.255.255.0.
Próximo Salto	Configure o seu Gateway desejado como Próximo Salto
Distância	Especifique a distância como 1

2. Clique no botão **Salvar** para guardar as configurações;
3. Verifique a tabela de roteamento para confirmar que o gateway padrão é o endereço que você configurou. A entrada marcada com o retângulo vermelho mostra o Gateway Padrão válido.

Acesso à interface CLI

Os usuários podem acessar a interface de linha de comando através do Telnet ou conexão SSH, e gerenciar o Switch com linhas de comando. As conexões Telnet e SSH suportam conexão remota e local.

A tabela a seguir demonstra as aplicações típicas utilizadas no acesso CLI:

Método	Porta Utilizada	Aplicações Típicas
Telnet	Porta RJ-45	CMD
SSH	Porta RJ-45	PuTTY

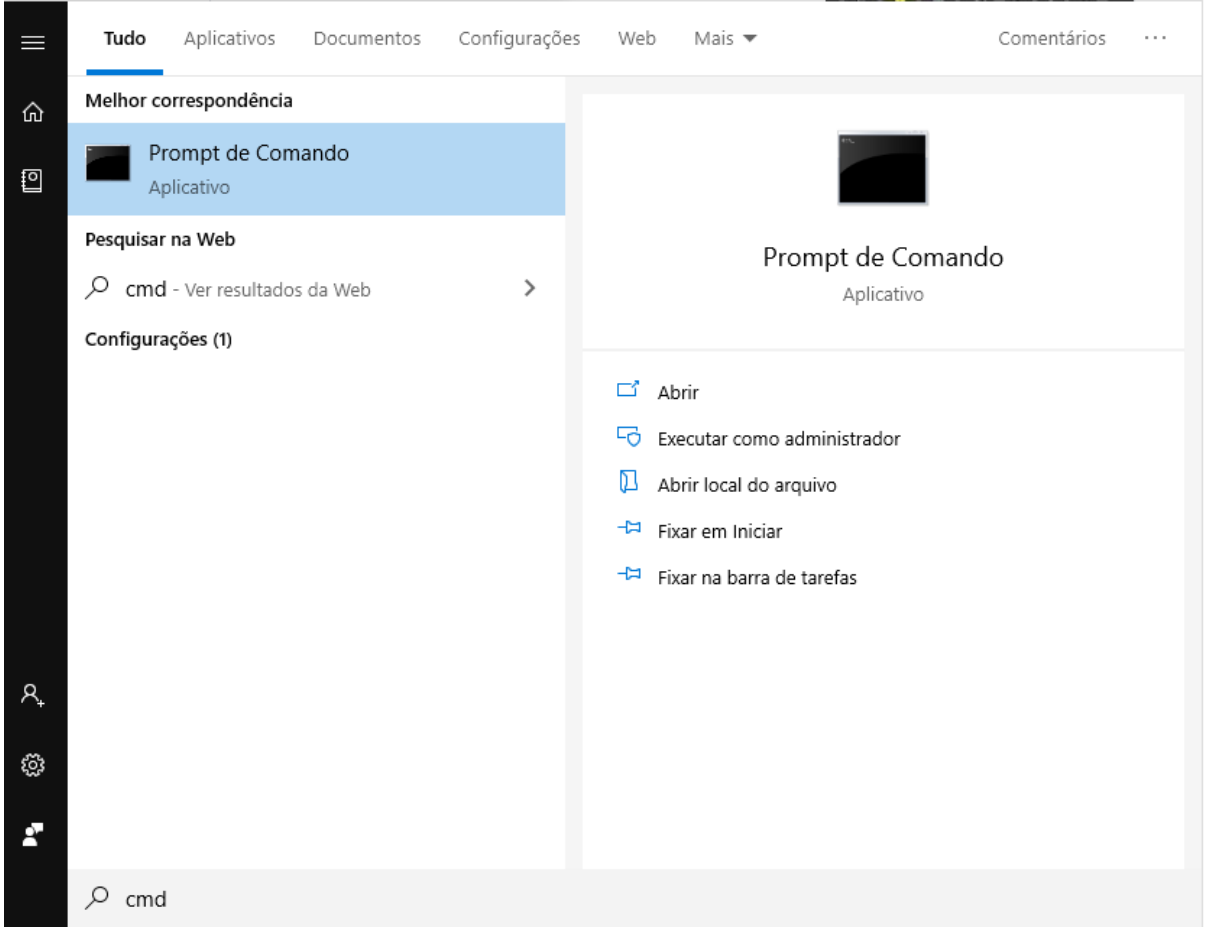
Telnet Login

O Switch suporta modo de login local para autenticação como padrão.

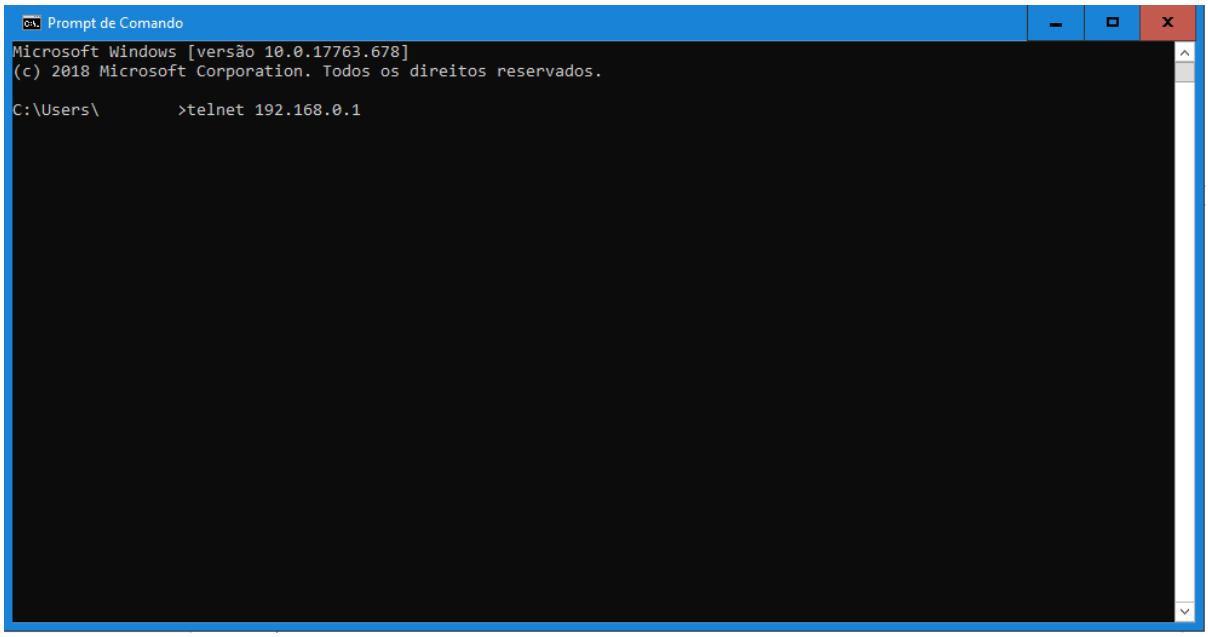
Modo de Login Local: Nome de usuário e senha são necessários, os quais são respectivamente **admin**, **admin** por padrão.

Os próximos passos mostram como acessar o switch através do modo de login local para gerenciamento do mesmo:

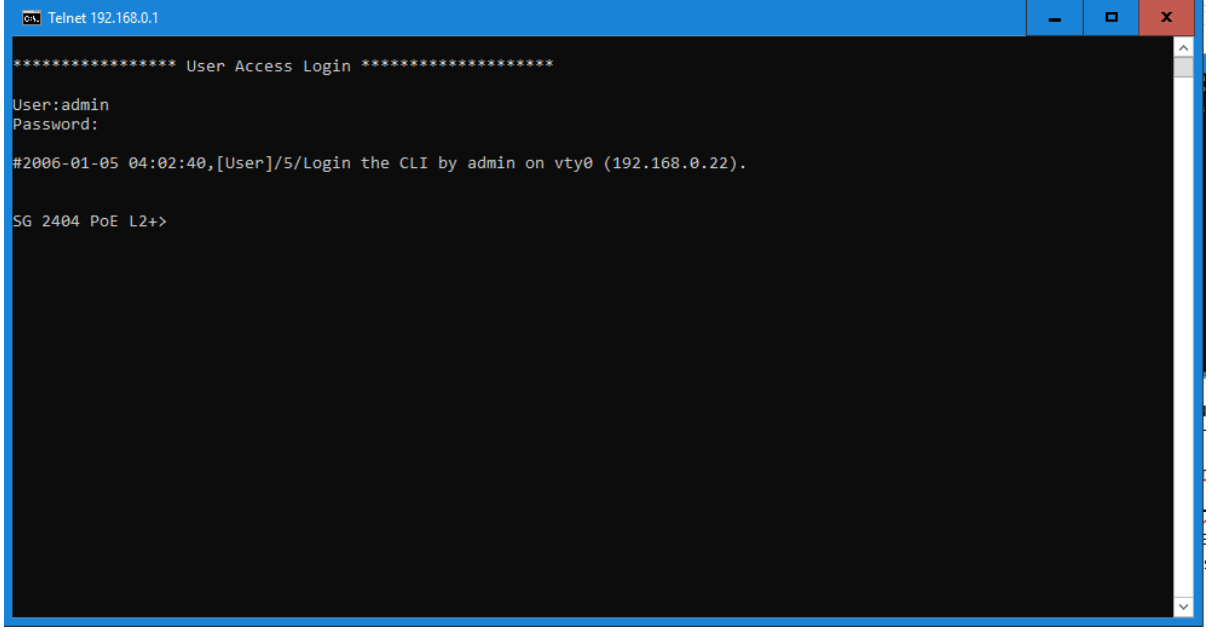
1. Verifique e garanta que o switch e o Computador estejam conectados à mesma Rede, clique em **iniciar** e digite **cmd** na barra de pesquisa, e então pressione **Enter**.



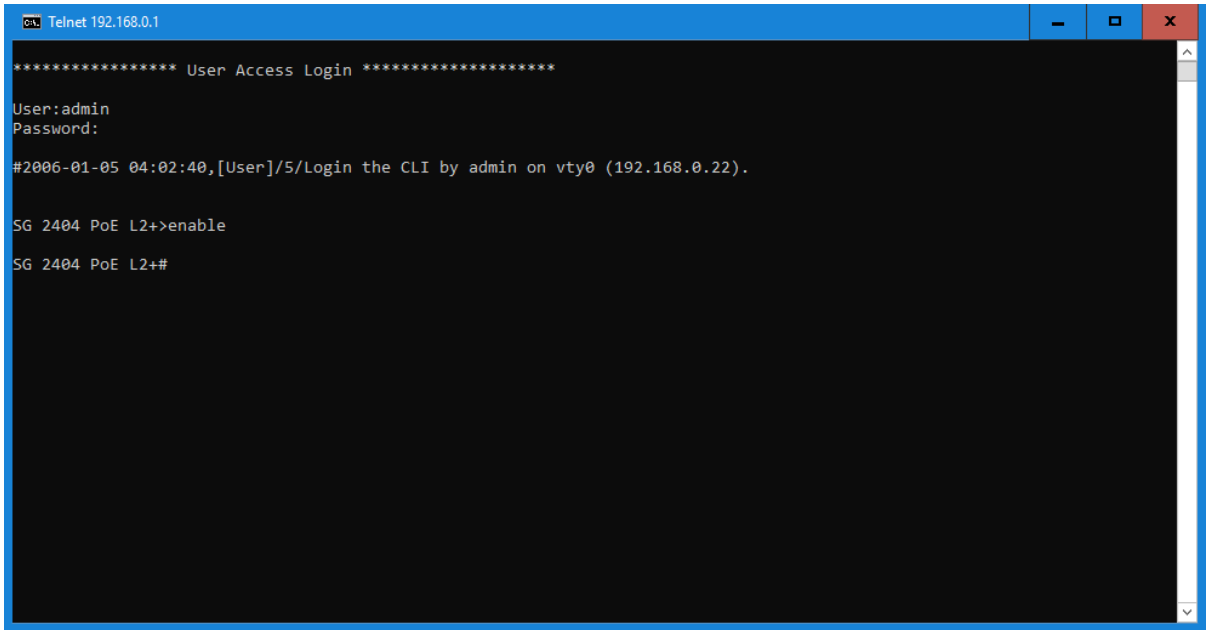
2. Digite **telnet 192.168.0.1** na janela CMD e então pressione **Enter**.



3. Digite o nome de usuário e a senha (ambos são **admin** por padrão). Pressione **Enter** e você irá entrar no modo User EXEC do switch. .



4. Digite o comando **enable** e você irá entrar no modo Privileged EXEC. Por padrão nenhuma senha é necessária para esse acesso. Depois é possível determinar uma senha para que os usuários que querem acessar o modo Privileged EXEC..

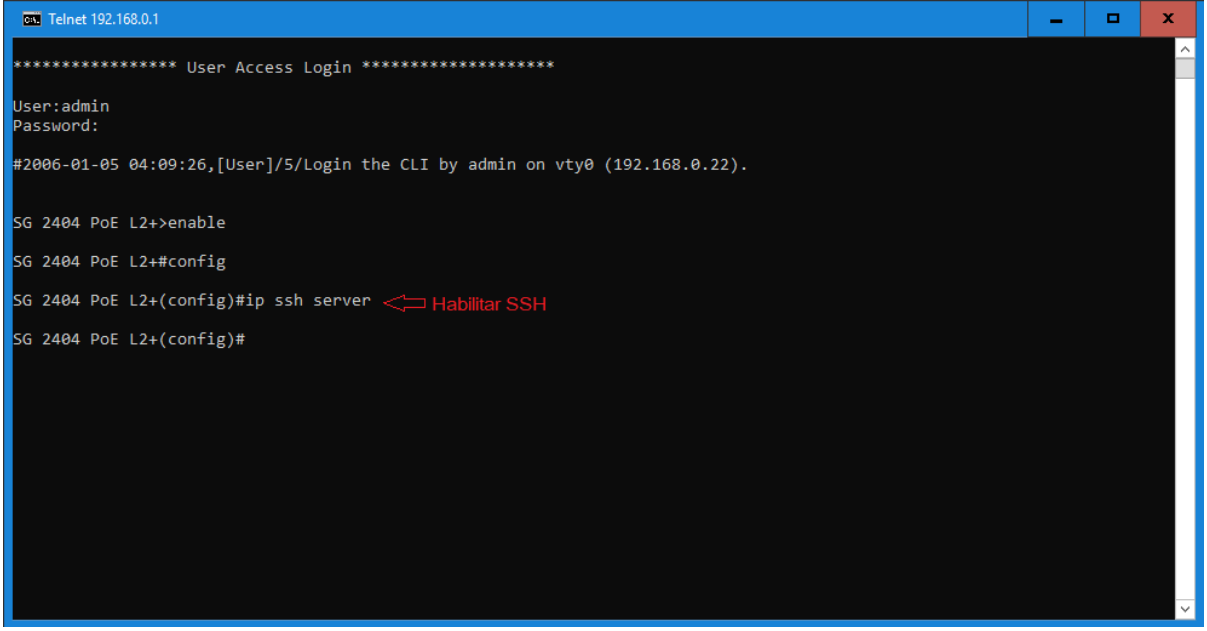


SSH Login

O login através da conexão SSH suporta dois modos: modo autenticação através de senha e modo autenticação através de chave. Você pode escolher conforme a sua necessidade:

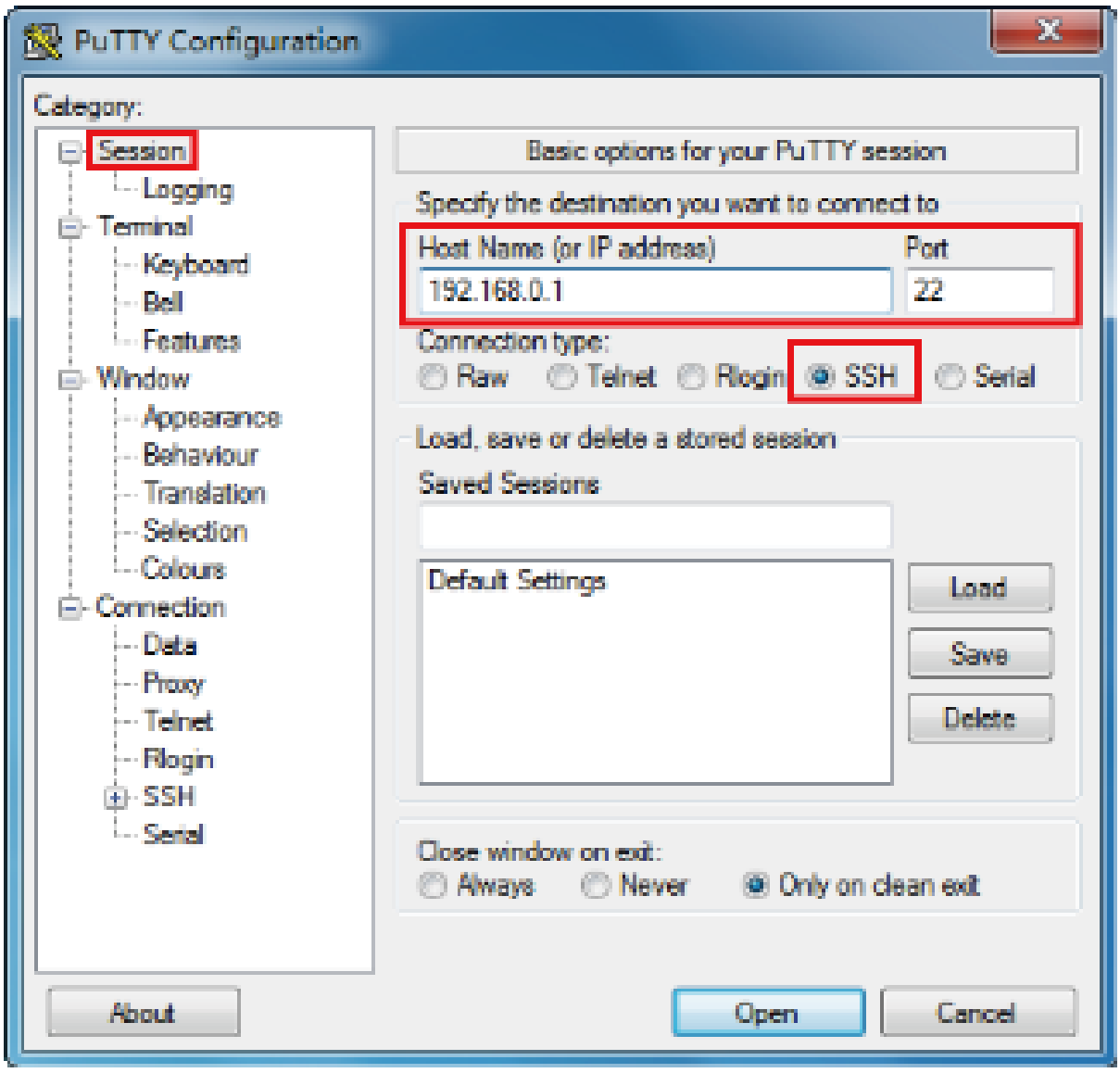
- Modo de autenticação através de Senha: necessário usuário e senha, os quais são ambos admin por padrão.
- Modo de autenticação por Chave (Recomendado): Uma chave pública para o switch e uma chave privada para o software cliente (PuTTY) são necessárias. Você pode gerar a chave pública e a chave privada através do gerador de chave do PuTTY.

Antes de acessar através da conexão SSH, siga os passos seguintes para habilitar a conexão SSH no programa emulador de terminal:

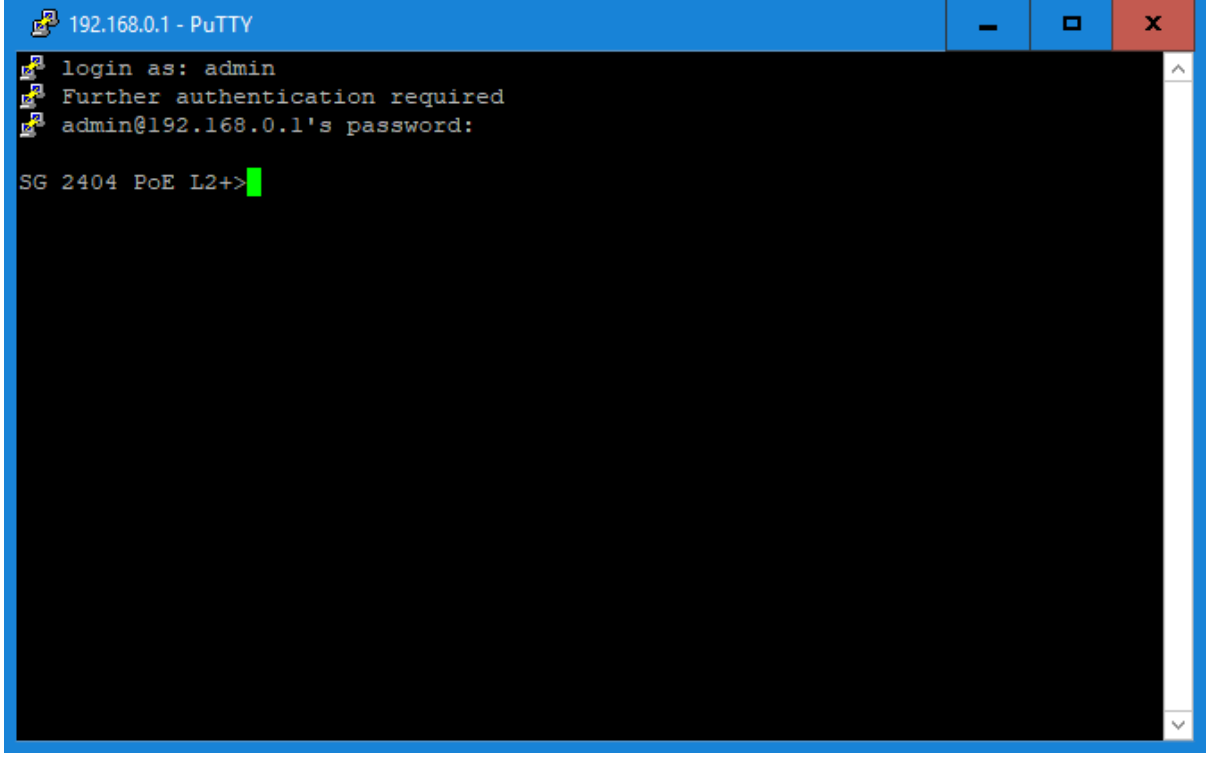


Modo de autenticação através de Senha

1. Abra o software PuTTY e vá até a página Sessão. Digite o endereço IP do switch no campo **Host Name** e mantenha o valor 22 para o campo **Port**. Clique em **Open**.

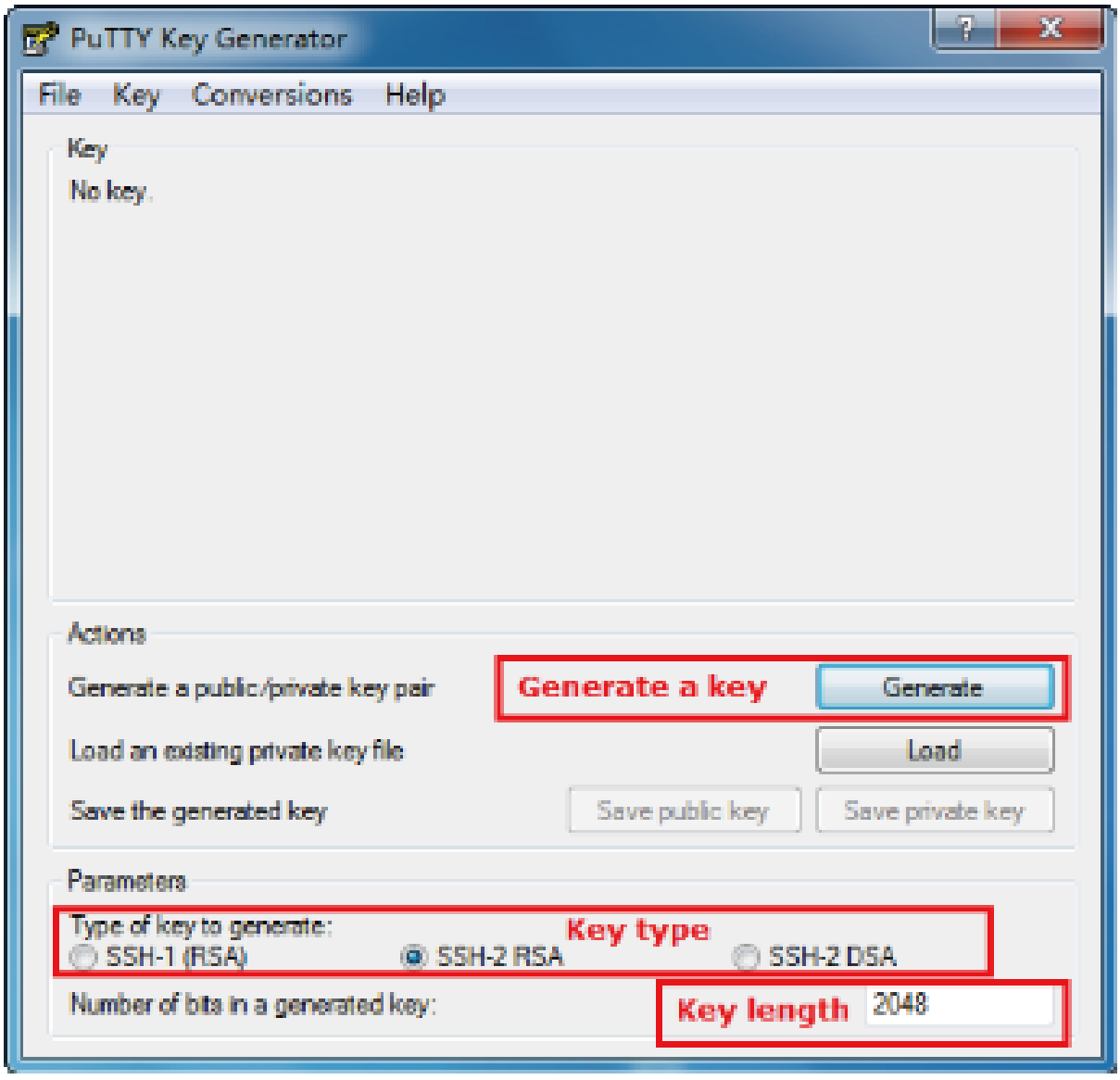


2. Digite o nome de usuário e a senha para logar no switch, e então você pode continuar para as configurações do mesmo.



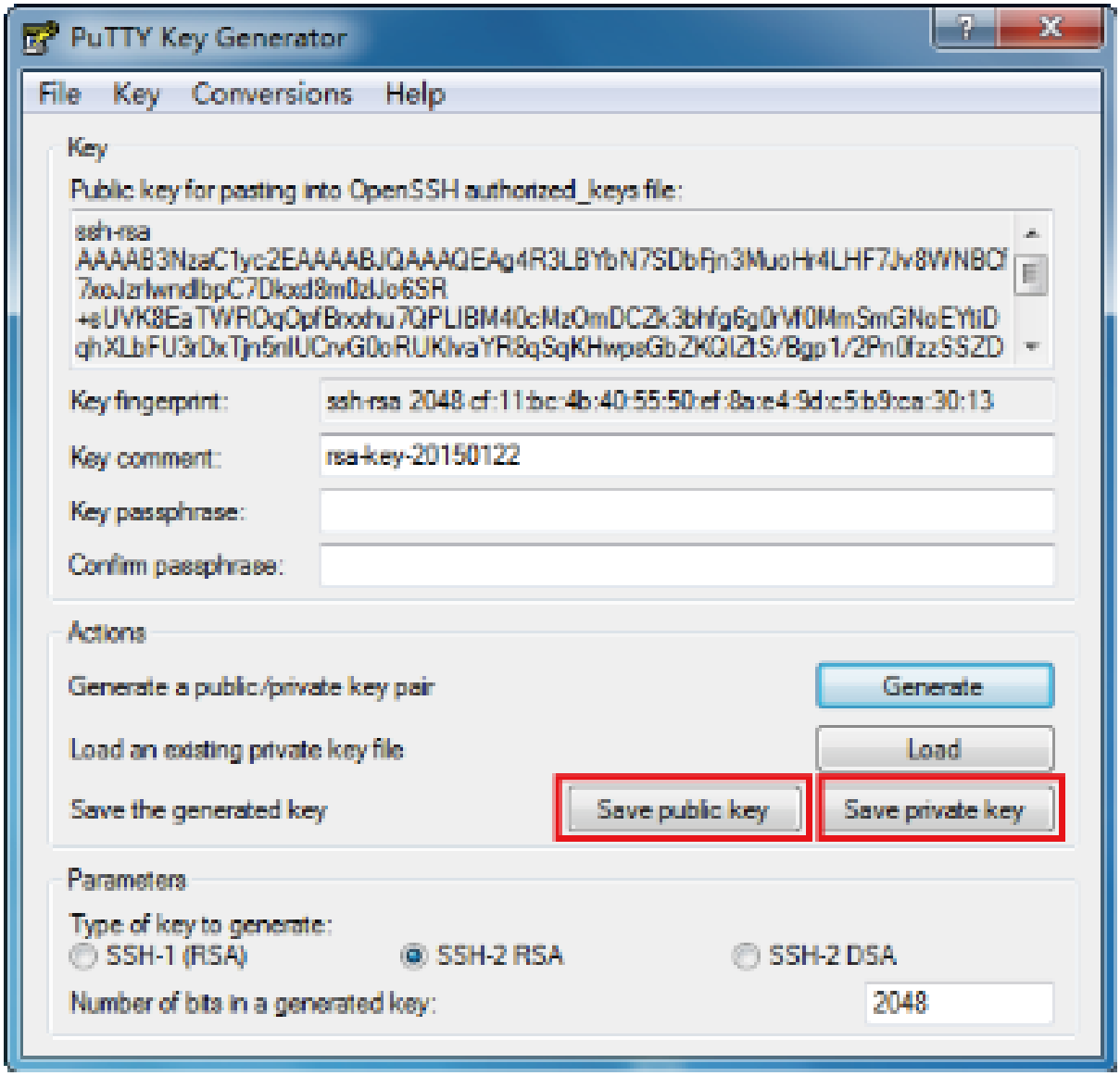
Modo de autenticação através de Chave

1. Abra o Gerador de Chave do PuTTY. Na seção de **Parâmetros** selecione o tipo de chave e entre o tamanho da mesma. Na seção **Actions**, clique em **Generate** para gerar um par de chaves pública/privada. E na figura seguinte um par de chaves SSH-2 RSA é gerada, e o comprimento de cada uma é 1024 bits..

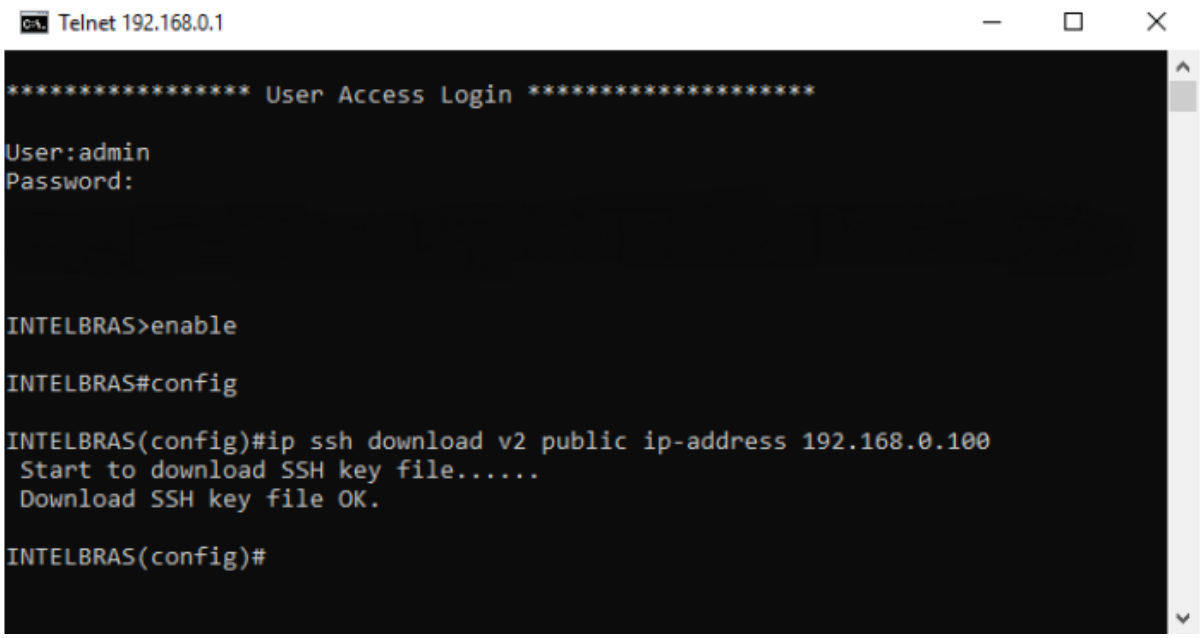


O comprimento da Chave deve estar entre 512 e 3072 bits;
Você pode acelerar o processo de geração de chave movendo aleatoriamente e rapidamente o cursor do mouse na seção Key.

2. Após as chaves serem geradas com sucesso, clique em **Save public Key** para salvar a chave pública em um servidor TFTP; Clique em **Save private Key** para salvar a chave privada no computador de acesso.

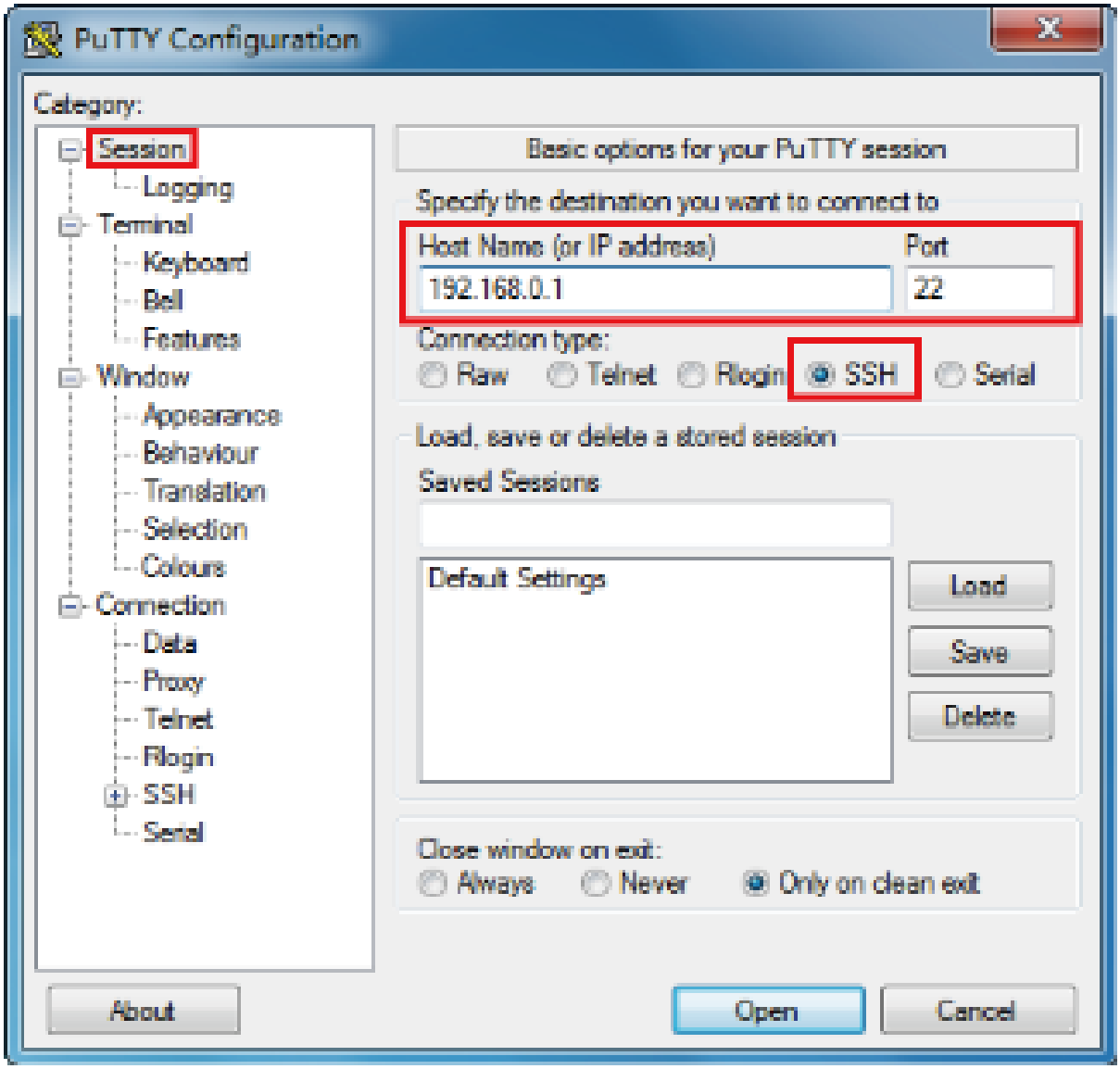


3. Dentro do Hyper Terminal, baixe a chave pública do servidor TFTP para o switch como mostrado na figura a baixo:

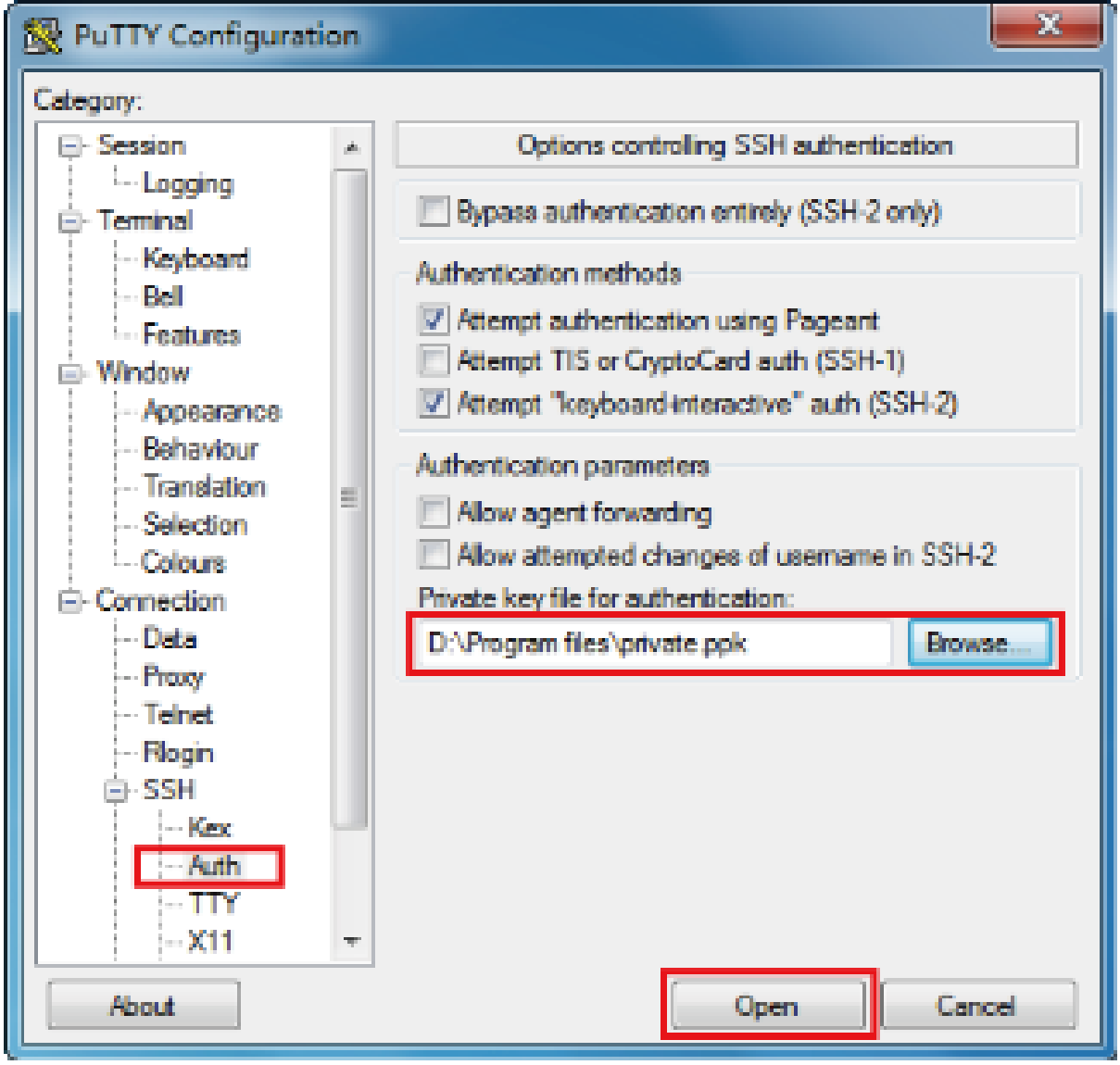


O tipo de chave deve estar de acordo com o tipo de arquivo de chave. No CLI à cima, v1 corresponde à SSH-1 (RSA) e v2 corresponde à SSH-2 RSA e SSH-2 DAS.
O processo de download da chave não pode ser interrompido.

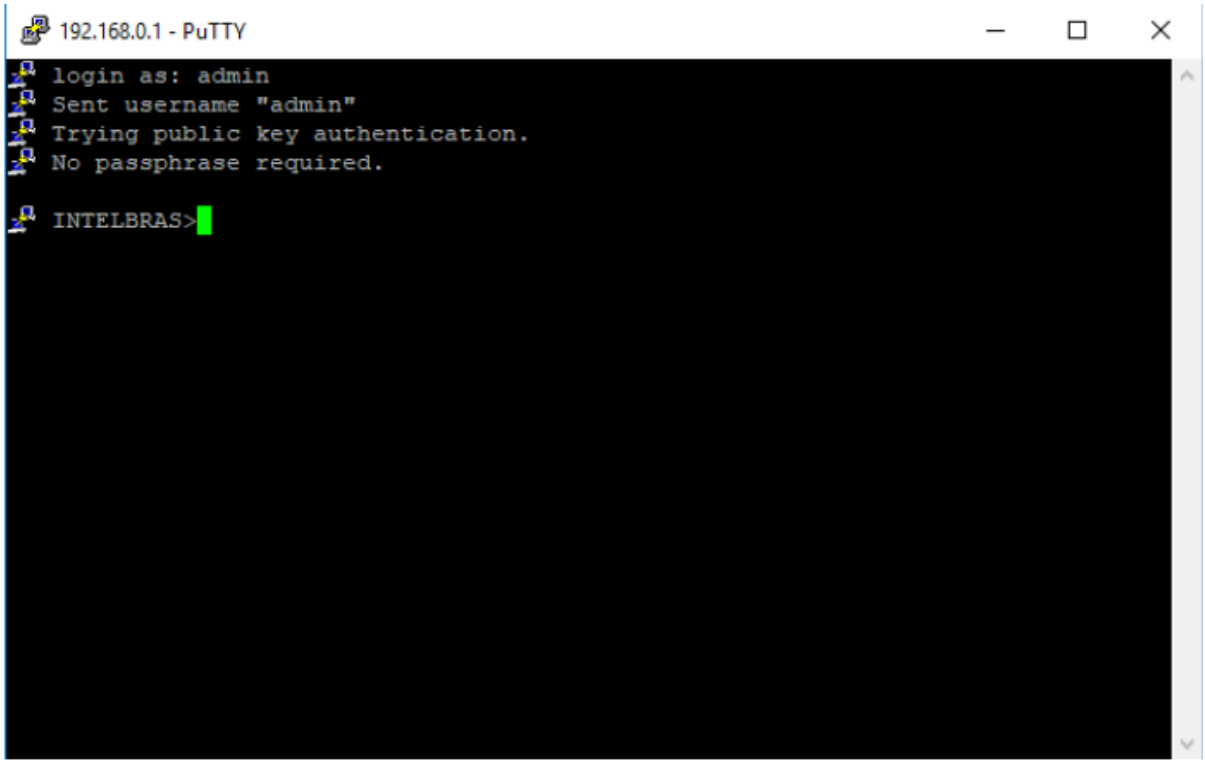
4. Após o download da chave pública abra o PuTTY e vá para a página **Session**. Digite o endereço de IP do switch e selecione SSH como sendo o tipo de conexão (mantenha o valor padrão que está no campo **Port**).



5. Vá para **Connection > SSH > Auth**. Clique **Browse** para baixar a chave privada para o PuTTY. Clique em **Open** para iniciar a negociação de conexão.



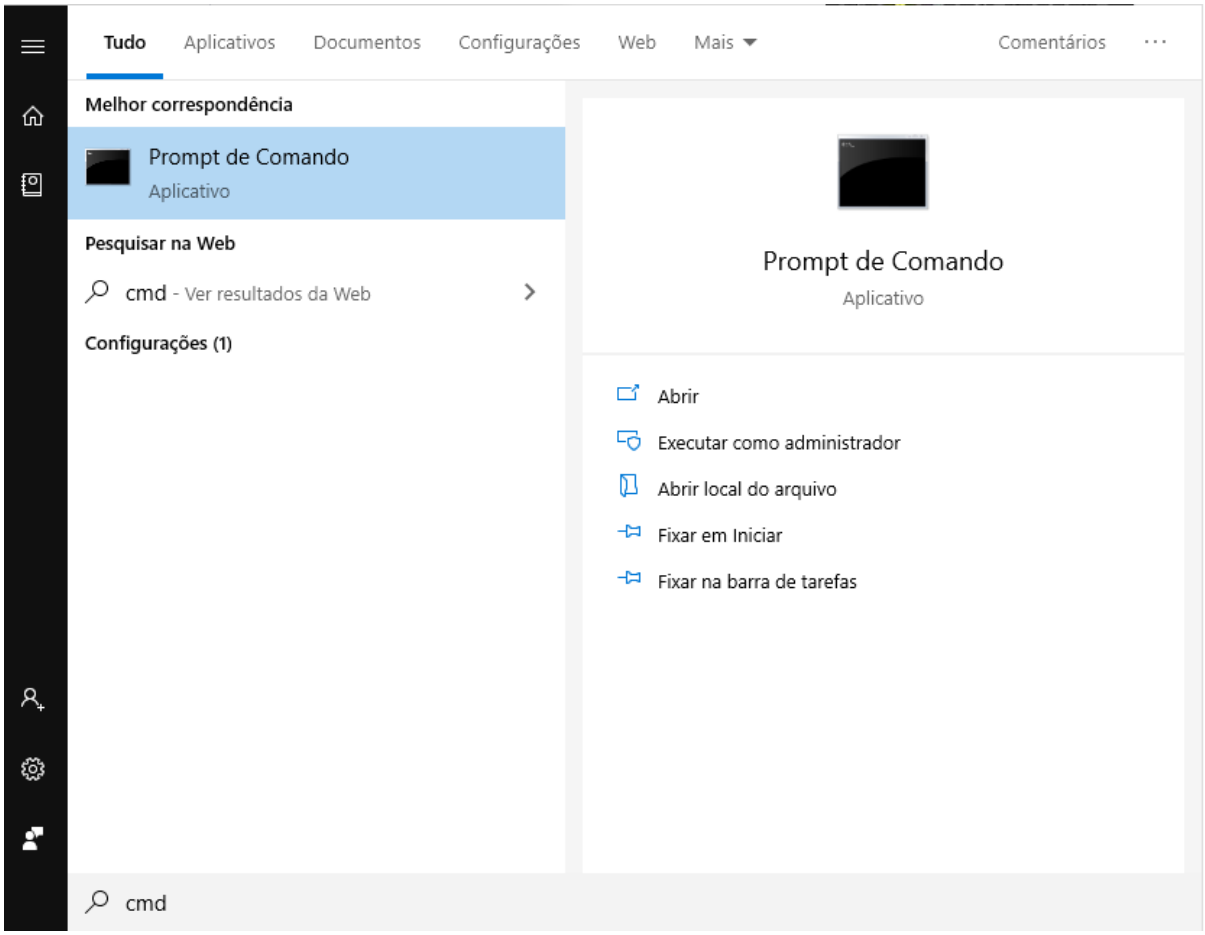
6. Assim que a negociação estiver completa, entre com o usuário e senha para autenticação. Se você conseguir autenticar o login sem a inserção da senha significa que a autenticação por chave foi completa com sucesso.



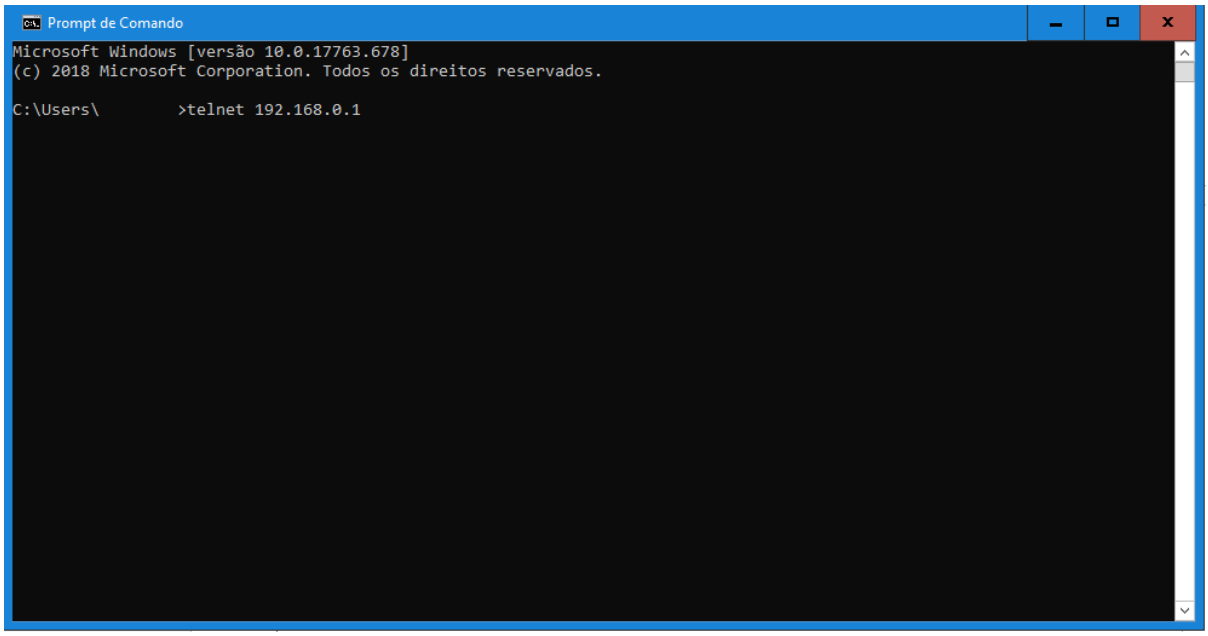
Modo de Login Local: Nome de usuário e senha são necessários, os quais são respectivamente **admin**, **admin** por padrão.

Os próximos passos mostram como acessar o switch através do modo de login local para gerenciamento do mesmo:

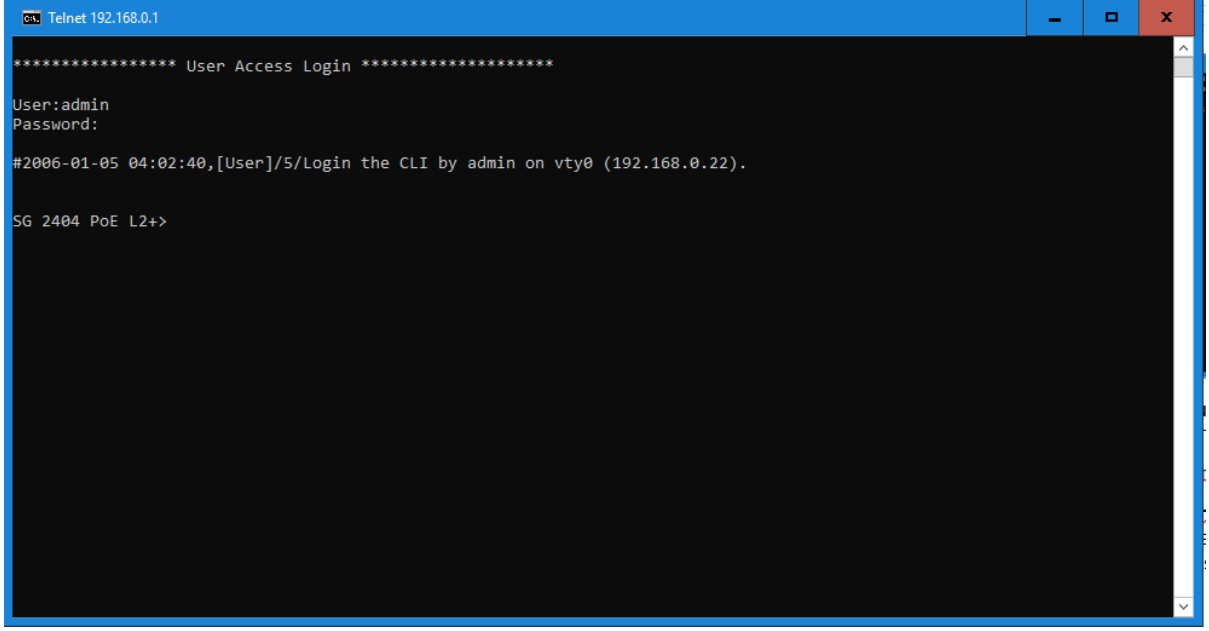
1. Verifique e garanta que o switch e o Computador estejam conectados à mesma Rede, clique em **iniciar** e digite **cmd** na barra de pesquisa, e então pressione **Enter**.



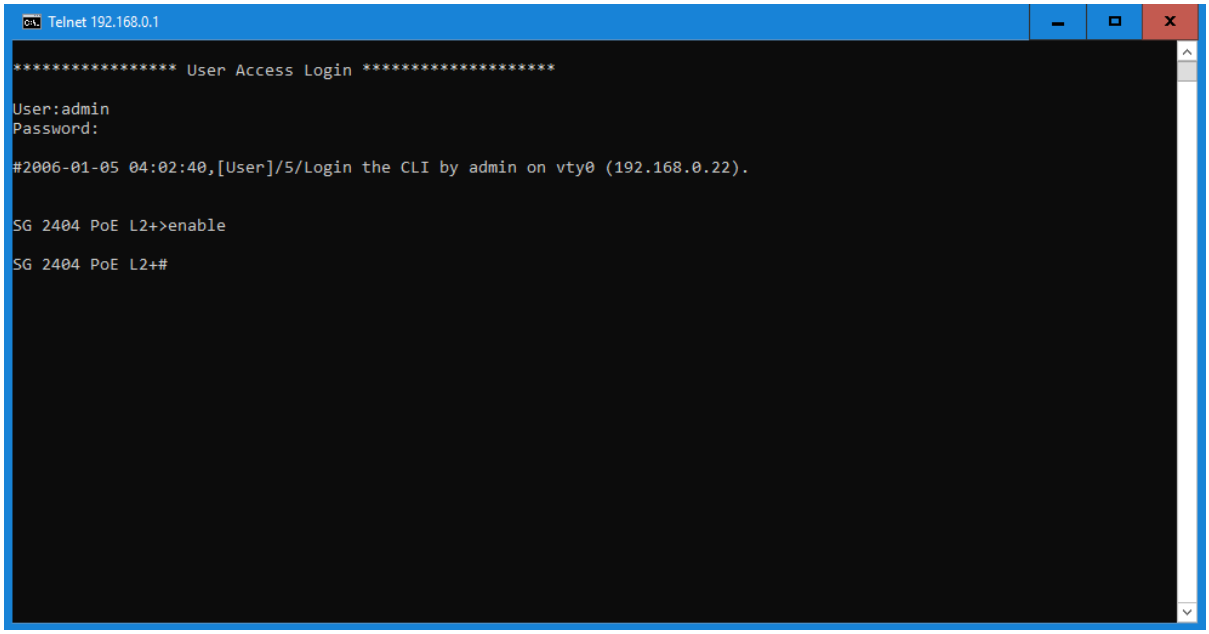
2. Digite **telnet 192.168.0.1** na janela CMD e então pressione **Enter**.



3. Digite o nome de usuário e a senha (ambos são **admin** por padrão). Pressione **Enter** e você irá entrar no modo User EXEC do switch. .



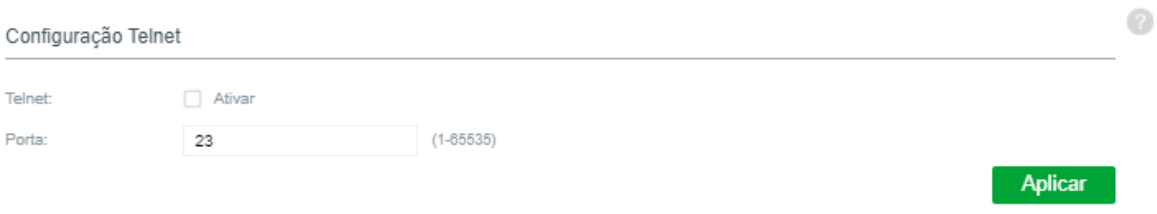
4. Digite o comando **enable** e você irá entrar no modo Privileged EXEC. Por padrão nenhuma senha é necessária para esse acesso. Depois é possível determinar uma senha para que os usuários que querem acessar o modo Privileged EXEC..



Desabilitando o Login Telnet

Você pode desabilitar a função de TELNET para bloquear qualquer acesso à interface CLI via Telnet.

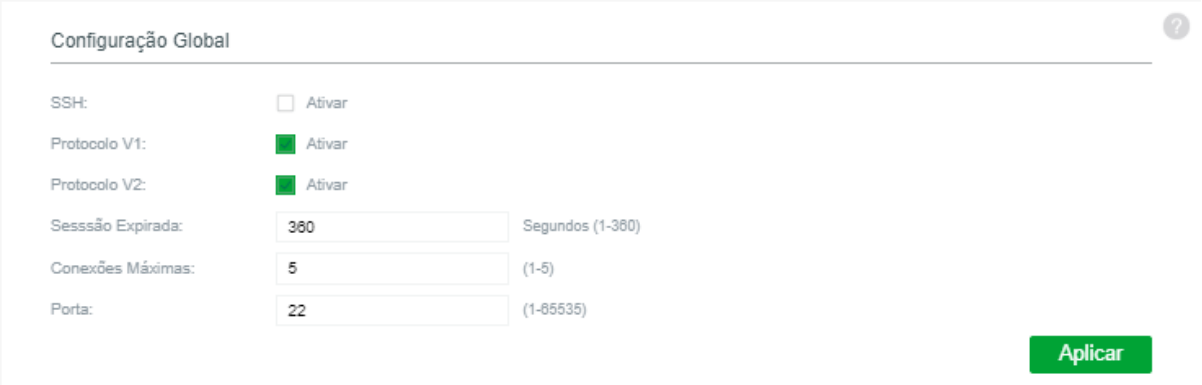
Vá até o menu **Segurança > Segurança de Acesso > Configuração Telnet**, desabilite a função de TELNET e clique em **Aplicar**.



Desabilitando o Login SSH

Você pode desabilitar o servidor SSH para bloquear qualquer acesso à interface CLI via SSH.

Vá até o menu **Segurança > Segurança de Acesso > Configuração SSH**, desabilite o servidor SSH e clique em **Aplicar**.



SISTEMA DE GESTÃO

Sistema

Visão Geral

No módulo sistema você pode visualizar as informações do sistema e configurar os parâmetros e características do sistema do switch.

Funções suportadas

Informação do Sistema

Você pode visualizar o estado das portas e as informações do sistema do switch, e configurar a descrição do dispositivo, horário do sistema e o tempo de horário de verão.

Gerenciamento de Usuário

Você pode gerenciar as contas de usuário para acesso ao switch. Existem vários tipos de usuários os quais possuem diferentes níveis de acesso e você pode criar diferentes contas de usuário conforme sua demanda.

Ferramentas do Sistema

Você pode configurar os arquivos de inicialização, backup e restauração do switch além de ter acesso à atualização de firmware, reset e reinicialização do switch.

EEE

Energy Efficient Ethernet (EEE) é utilizado para reduzir o consumo de energia do switch em períodos de baixa atividade de dados. Você pode simplesmente ativar essa função para as portas para permitir a redução do consumo de energia.

PoE

Power over Ethernet (PoE) é uma função de fornecimento de energia remota. Com essa função o switch pode fornecer energia à dispositivos conectados através do cabo de rede.

Alguns dispositivos como telefones IP, access points (APs) e câmeras podem sem instalados distantes de instalações de energia elétrica. PoE pode prover energia para esses dispositivos sem precisar de cabos de energia e instalação elétrica no local. Isso permite que um único cabo providencie conexão de dados e energia para os dispositivos.

Os padrões de PoE IEEE 802.3af e IEEE 802.2at possuem processos para descobrir dispositivos que precisam ser alimentados por PoE, administração de energia, detecção de desconexão e uma classificação do dispositivo energizado opcional.

- **PSE**

  Power sourcing equipment (PSE), é um dispositivo que disponibiliza energia para os dispositivos conectados à Ethernet, este switch por exemplo. Os PSE podem detectar os PDs e determinar os requisitos de alimentação do mesmo.

- **PD**

  Powered Device (PD) é um dispositivo que recebe alimentação do PSE, por exemplo, telefones IPs e Access Points. Os PDs em conformidade com os padrões IEEE podem ser classificados como PDs padrões e PDs não padronizados, somente os PDs dentro dos padrões IEEE serão alimentados por este switch.

Modelo SDM

Modelo SDM (Switch Database Management) é utilizado para priorizar os recursos do hardware para certas funções. O switch disponibiliza três Modelos os quais alocam diferentes recursos de hardware para diferentes usos, e você pode escolher de acordo com a sua necessidade.

Time Range

Com essa função você pode configurar um “time range” e vincular à uma porta PoE ou à uma regra ACL.

Configurações das informações do Sistema

Com as configurações das informações do sistema você pode:

- Visualizar o resumo do sistema
- Configurar a descrição do dispositivo
- Configurar o horário do sistema
- Configurar o horário de verão

Visualizando o resumo do sistema

Vá para **SISTEMA > Informação do Sistema > Resumo do Sistema** para carregar a página com o resumo do sistema. Você pode visualizar o estado das portas e as informações do sistema do switch.

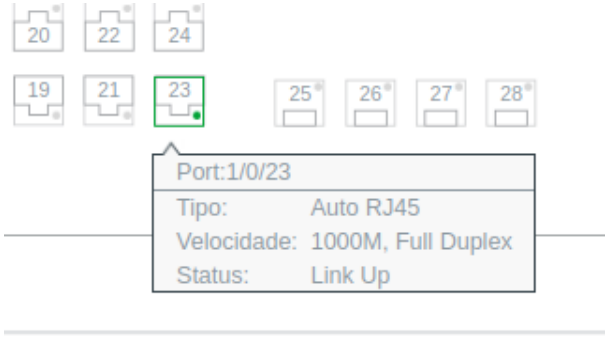
Visualizando o estado das portas

Na seção **Estado das Portas** você pode ver o estado das portas e a velocidade de banda utilizada por cada porta.

A Tabela a seguir mostra o significado de cada estado da porta:

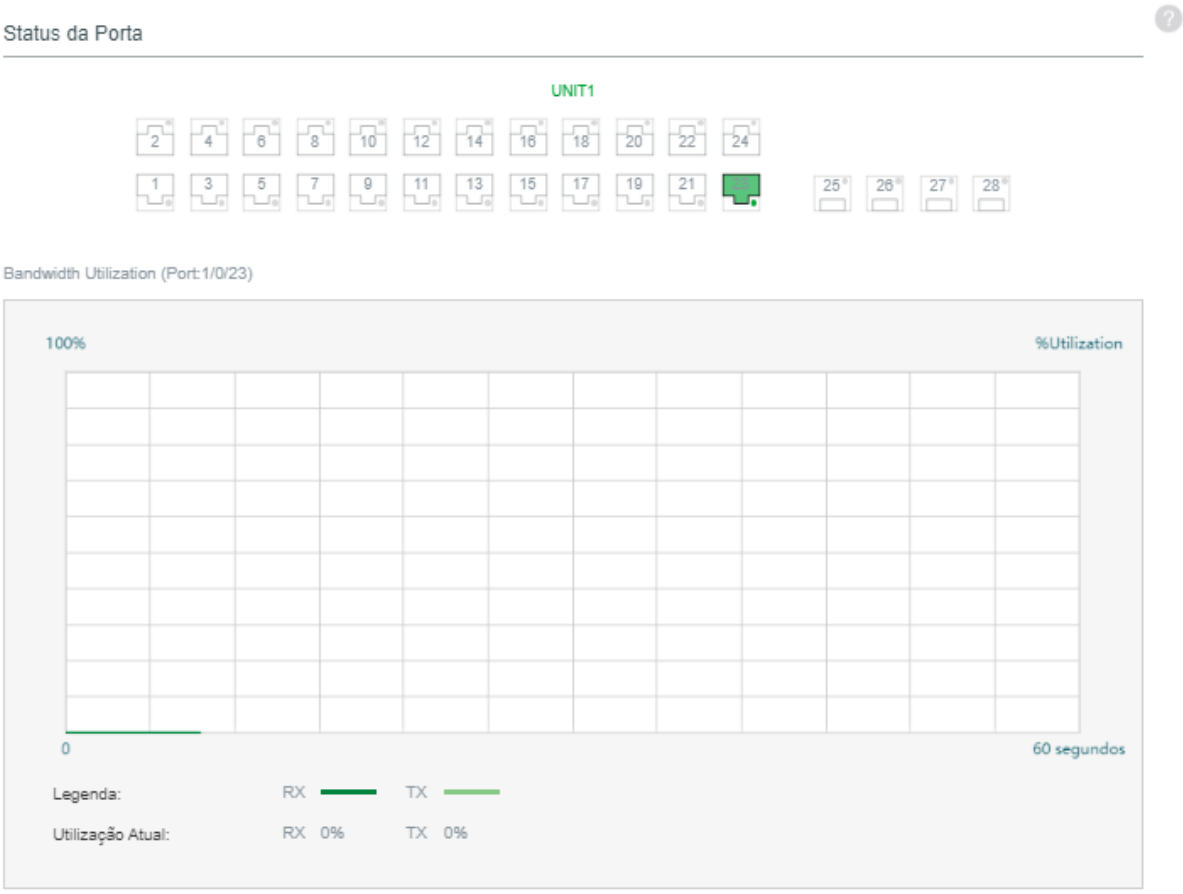
Estado da Porta	Indicação
	Indica que a porta Gigabit correspondente está desconectada
	Indica que a porta Gigabit correspondente está conectada à 1000Mbps
	Indica que a porta Gigabit correspondente está conectada à 10Mbps ou 100Mbps
	Indica que a porta SFP correspondente não está conectada
	Indica que a porta SFP correspondente está conectada à 1000Mbps
	Indica que a porta SFP correspondente está conectada à 100Mbps

Você pode mover o cursor sobre uma porta para visualizar as informações detalhadas da porta.



Informação da Porta	Indicação
Port	Mostra o número da porta
Tipo	Mostra o tipo de porta
Velocidade	Mostra a velocidade máxima de transmissão e seu modo duplex
Status	Mostra o estado de conexão da porta

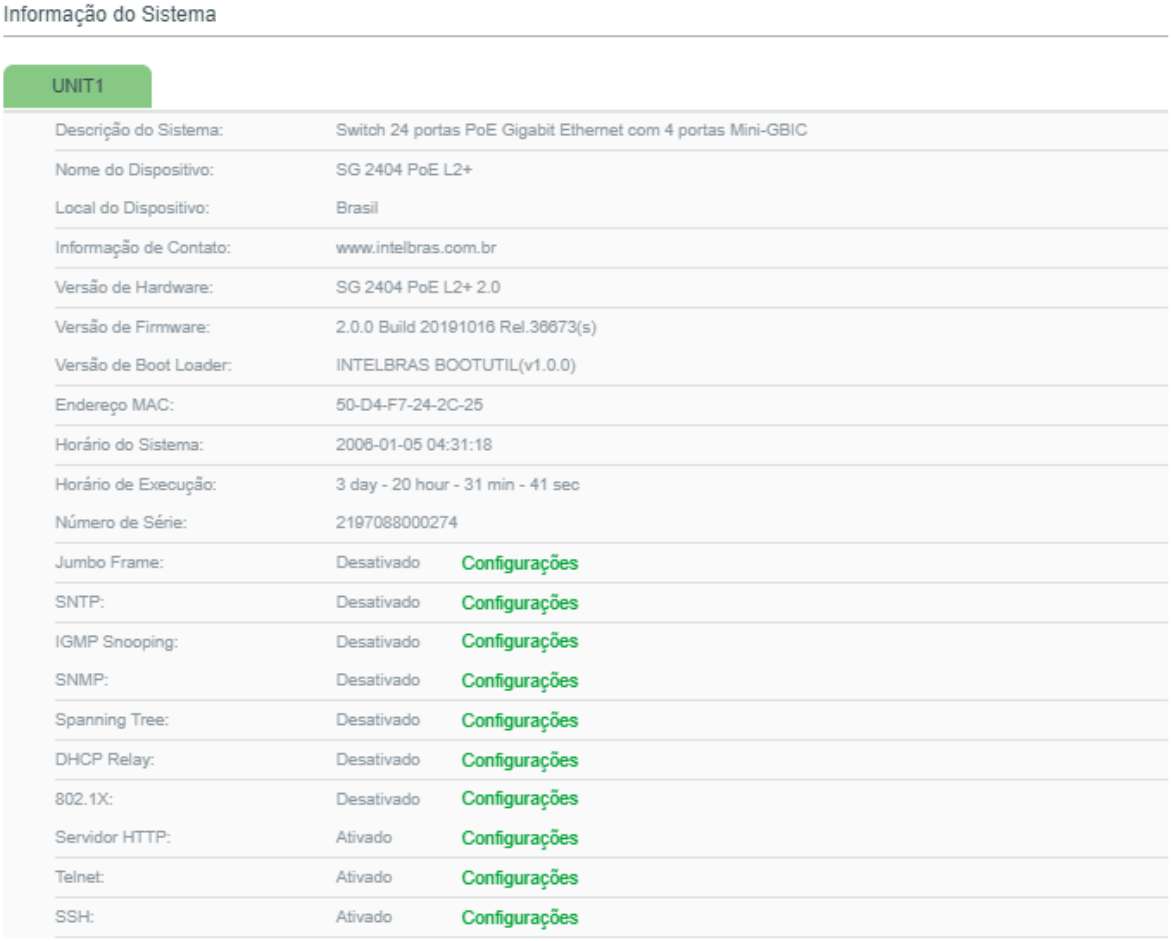
Você pode clicar em uma porta para visualizar a utilização de banda da mesma.



RX	Mostra a utilização de banda que a porta está utilizando para receber pacotes
TX	Mostra a utilização de banda que a porta está utilizando para enviar pacotes

Visualizando a informação do Sistema

Na seção **Informação do Sistema** você pode visualizar as informações do sistema do switch.

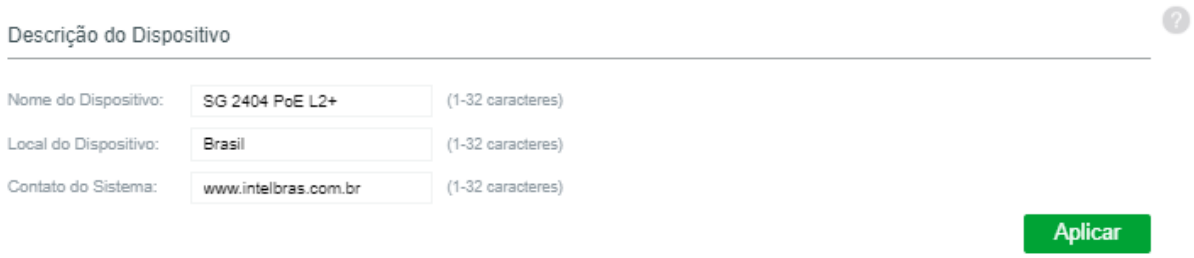


Descrição do sistema	Mostra a descrição do sistema do Switch.
Nome do dispositivo	Mostra o nome do Switch. Você pode editar na página de Descrição do Dispositivo.
Localização do dispositivo	Mostra a localização do Switch. Você pode editar na página de Descrição do Dispositivo.
Informação para contato	Mostra a informação para contato a respeito do Switch. Você pode editar na página de Descrição do Dispositivo.
Versão do Hardware	Mostra a versão do hardware do Switch.
Versão do Firmware	Mostra a versão do Firmware do Switch.
Versão do Boot Loader	Mostra a versão do Boot Loader do Switch.
Endereço MAC	Mostra o endereço MAC do Switch.
Horário do sistema	Mostra o Horário configurado no Switch.
Tempo em execução	Mostra o Tempo que o Switch está em operação.
Número de Série	Mostra o número de série do Switch.
Jumbo Frame	Mostra se o Jumbo Frame está habilitado. Você pode Clicar em Configurações para ir para a página de configurações do Jumbo Frame.

SNTP	Mostra se o Switch está sincronizando o horário através de um servidor NTP. Você pode clicar em Configurações para ir à página de Configuração de horário do sistema.
IGMP Snooping	Mostra se o IGMP Snooping está habilitado. Você pode clicar em Configurações para ir à página de configuração do IGMP Snooping.
SNMP	Mostra se o SNMP está habilitado. Você pode clicar em Configurações para ir à página de configuração do SNMP.
Spanning Tree	Mostra se o Spanning Tree está habilitado. Você pode clicar em Configurações para ir à página de configuração do Spanning Tree.
DHCP Relay	Mostra se o DHCP Relay está habilitado. Você pode clicar em Configurações para ir à página de configuração do DHCP Relay.
802.1x	Mostra se o padrão IEEE 802.1x está habilitado. Você pode clicar em Configurações para ir à página de configuração do 802.1x.
HTTP Server	Mostra se o servidor HTTP está habilitado. Você pode clicar em Configurações para ir à página de configuração do HTTP.
Telnet	Mostra se a conexão Telnet está habilitada. Você pode clicar em Configurações para ir à página de configuração do Telnet.
SSH	Mostra se a conexão SSH está habilitada. Você pode clicar em Configurações para ir à página de configuração do SSH.

Configurando a Descrição do Dispositivo

Vá para **SISTEMA > Informação do Sistema > Descrição do Dispositivo** para carregar a seguinte página:



1. Na seção **Descrição do Dispositivo** configure os seguintes parâmetros:

Nome do Dispositivo	Especifique o nome do Switch.
Local do Dispositivo	Digite a Localização do Switch.
Contato do Sistema	Digite a informação para contato.

2. Clique em **Aplicar**.

Configurando o Horário do Sistema

Vá para **SISTEMA > Informação do Sistema > Horário do Sistema** para carregar a seguinte página:

Na seção de **Informação de Horário** você pode ver a informação do horário atual do switch.

Horário atual do Sistema	Mostra o horário e data atuais do Switch.
Fonte do Horário atual	Mostra como foi configurado esse horário no Switch.

Na Seção **Configuração de Horário** siga os seguintes passos para configurar o horário do sistema:

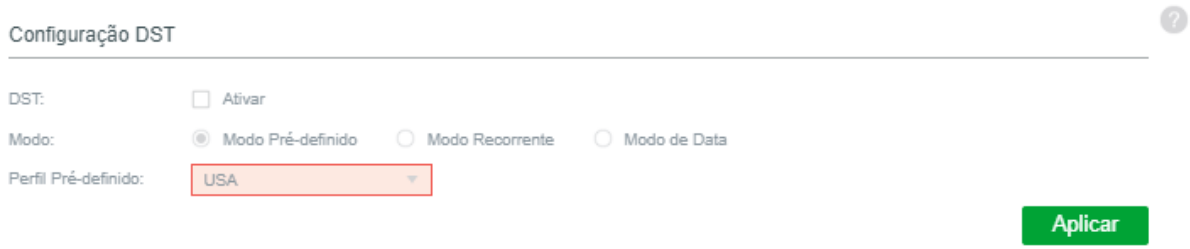
1. Escolha um método para apontar o horário e data do sistema e especifique os parâmetros relacionados.

Configurar Manualmente	Aponte a Data e Hora do sistema de forma manual. **Data:** Especifica a data do sistema. **Hora:** Especifica a hora do sistema.
Obter Horário do Servidor NTP	Sincroniza a Data e Hora do sistema com um servidor NTP. Primeiramente garanta que o servidor está acessível em sua rede. Se o servidor NTP estiver na WEB conecte seu Switch à internet primeiramente. **Fuso Horário:** Selecione o seu Fuso Horário local. **Servidor Primário:** Digite o Endereço IP do servidor NTP primário. **Servidor Secundário:** Digite o Endereço IP do servidor NTP secundário. Uma vez que o servidor primário estiver inalcançável o Switch conseguirá sincronizar o horário com o servidor secundário. **Taxa de Atualização:** Especifica o intervalo com o qual o Switch irá sincronizar com o servidor NTP o qual varia entre 1 e 24 horas.
Sincronizar com o Relógio do PC	Sincroniza o horário do sistema com o relógio do computador que Logado no sistema do Switch.

2. Clique em **Aplicar**.

Configurando o Horário de Verão

Vá para **SISTEMA > Informação do Sistema > Horário de Verão** para carregar a seguinte página:



Siga os seguintes passos para configurar o Horário de Verão:

1. Na seção **Configuração de Horário de Verão**, habilite a função de Horário de Verão.
2. Escolha um método para seleção do Horário de Verão e especifique seus parâmetros.

Modo Predefinido	Se você selecionar o **Modo Predefinido** escolhendo uma das seguintes opções para agendar no switch: **USA:** Seleciona o horário de verão dos Estados Unidos. O qual vai das 2:00 do segundo Domingo de Março Até às 2:00 do Primeiro Domingo de Novembro. **Austrália:** Seleciona o horário de verão da Austrália. O qual vai das 2:00 do primeiro Domingo de Outubro Até às 2:00 do primeiro Domingo de Abril. **Europa:** Seleciona o Horário de Verão da Europa. O qual vai da 1:00 do último domingo de março até às 1:00 do último domingo de outubro. **Nova Zelândia:** Seleciona o Horário de Verão da Nova Zelândia. O qual vai das 2:00 do último Domingo de Setembro Até às 3:00 do primeiro Domingo de Abril.
Modo Recorrente	Se você selecionar o **Modo Recorrente**, especifica um ciclo de Time Range para o Horário de Verão como Horário para o Switch. Essa configuração pode ser usada todos os anos. O intervalo entre a Data de Início e a Data de Término do Horário de verão deve ser maio que 1 dia e menor que 1 ano (365 dias). **Deslocamento:** Representa o quanto o relógio será adiantado; **Hora de início:** Especifica a data e hora de início para o Horário de Verão. **Hora de Término:** Especifica a data e hora de término para o Horário de Verão.

Modo de Data	Se você selecionar o **Modo de Data** você especificará um Time Range absoluto para o horário de verão do Switch. Essa configuração será utilizada somente uma vez. O intervalo entre a Data de Início e a Data de Término do Horário de verão deve ser maio que 1 dia e menor que 1 ano (365 dias). **Deslocamento:** Representa o quanto o relógio será adiantado; **Hora de início:** Especifica a data e hora de início para o Horário de Verão. **Hora de Término:** Especifica a data e hora de término para o Horário de Verão.

3. Clique em **Aplicar**.

Configurações de Gerenciamento do Usuário

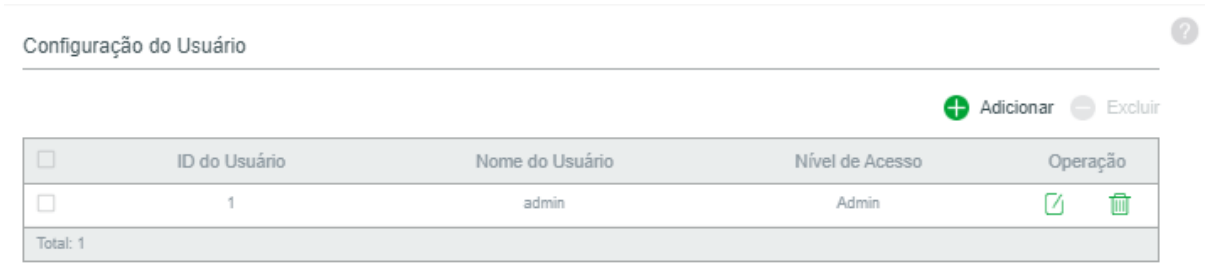
Com o gerenciamento de usuário você pode criar e gerenciar contas de usuário para acesso ao switch.

Existem quatro tipos de contas de usuário com diferentes níveis de acesso: Admin, Operador, Usuário Avançado e Usuário.

- Existe um usuário padrão administrador que não pode ser deletado, por padrão o usuário e senha desse usuário é **admin**. Você pode criar mais contas de Administrador.
- Se você criar contas de nível Operador, Usuário Avançado e Usuário você precisará ir até a sessão AAA para criar uma senha enable. Se necessário esses níveis de usuário podem usar essa senha para alterar os seus respectivos níveis de acesso para nível administrador.

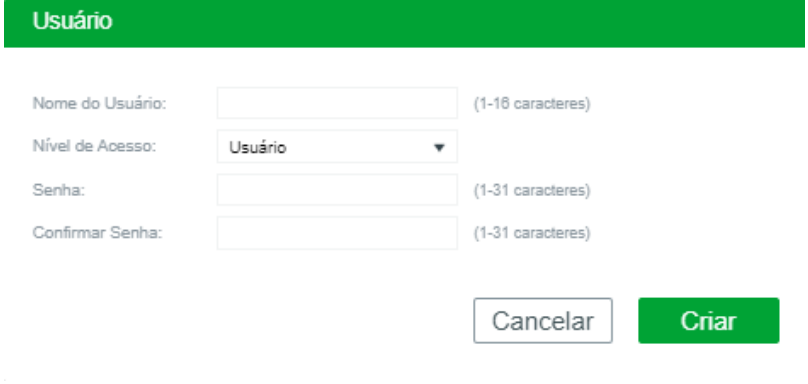
Criando Contas de Usuário

Vá até o menu **SISTEMA > Gerenciamento do Usuário**, para carregar a seguinte página:



Por padrão existe um usuário Admin padrão na tabela. Você pode clicar em para editar essa conta de administrador, porém você não poderá excluir a mesma.

Você pode criar novas contas de usuário. Clique em Adicionar e a seguinte janela irá aparecer:



Siga os seguintes passos para criar um novo usuário:

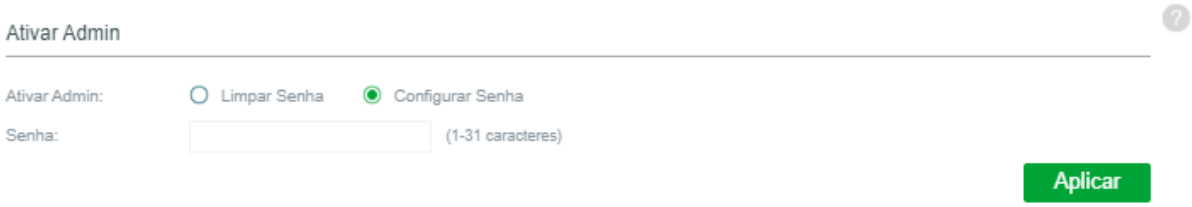
1. Configure os seguintes parâmetros:

Nome de Usuário	Especifique o nome de usuário para a conta. Ela pode conter até 16 caracteres, compostas por letras, números e underline (_).
Nível de Acesso	Aponte o nível de acesso que o usuário terá. Você tem 4 opções: **Admin:** administrador pode editar, modificar e ver todas as configurações e funções; **Operador:** operador pode editar, modificar e ver a maioria das configurações e funções; **Power User:** ou usuário avançado pode editar, modificar e ver algumas configurações e funções; **Usuário:** usuário pode ver as configurações sem o direito de editá-las ou modifica-las.
Senha	Especifica a senha da conta de usuário com até 31 caracteres alfanuméricos ou símbolos, este campo é *Case Sensitive*, diferencia letras maiúsculas e minúsculas.
Confirme a Senha	Repita a mesma senha do campo anterior.

2. Clique em **Criar**.

Configuração da Senha Enable

Vá até o menu **Segurança > AAA > Configuração Global**, para carregar a seguinte página:



Siga os seguintes passos para configurar a Senha de Enable:

1. Selecione **Configurar Senha** e especifique a senha de Enable no campo de **Senha**.

2. Clique em **Aplicar**.

   Dica: os usuários que estão ativos, logados, podem vir à essa página para elevar seu nível de privilégio para administrador utilizando a senha de Enable.

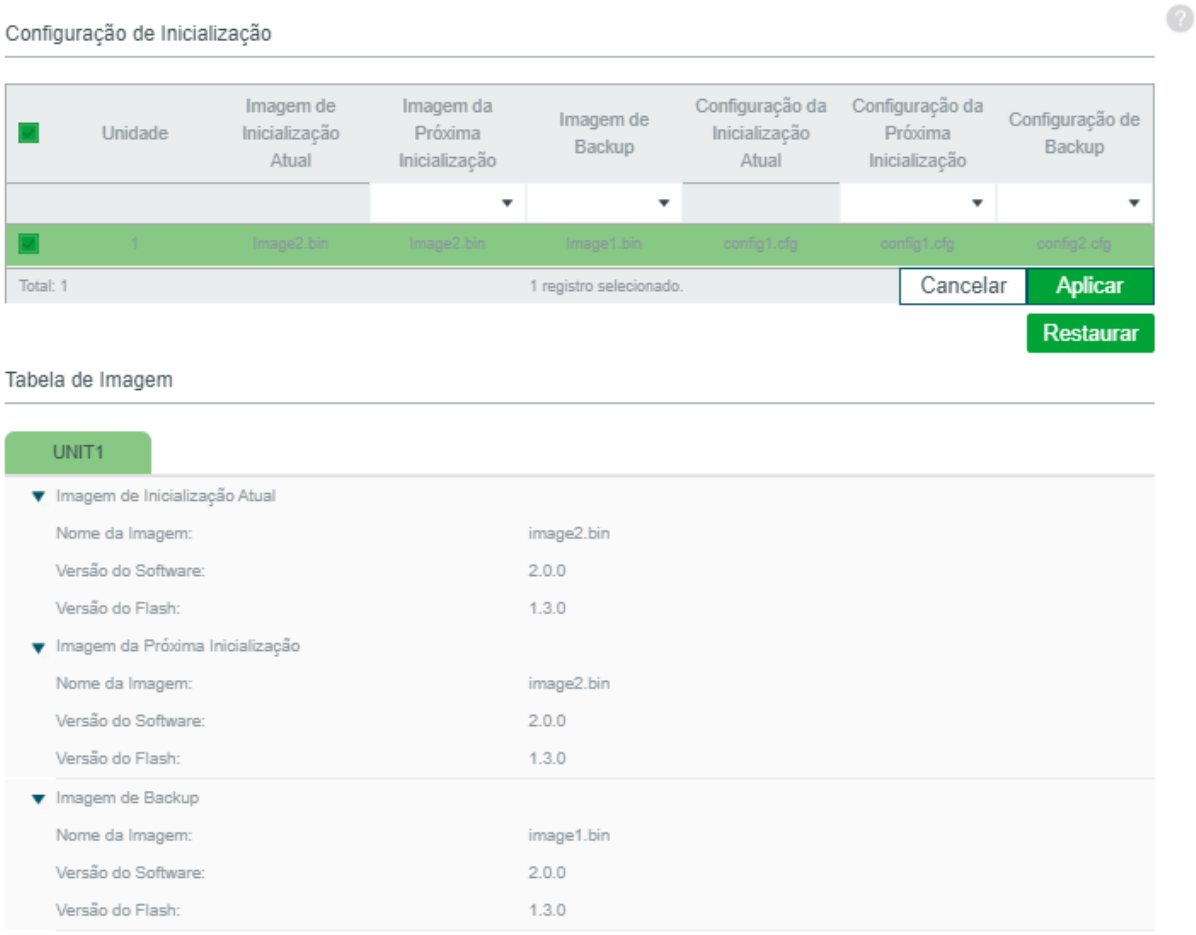
Configuração das Ferramentas do Sistema

Com as Ferramentas do Sistema você pode:

- Configurar o arquivo de inicialização;
- Restaurar as configurações do Switch;
- Criar um arquivo de Backup;
- Atualizar o Firmware do Switch;
- Reiniciar o Switch;
- Voltar às configurações de Fábrica, resetar o Switch.

Configurando o arquivo de inicialização

Vá até o menu **SISTEMA > Ferramentas do Sistema > Configuração de Boot** para carregar a seguinte página:



Siga os seguintes passos para configurar o arquivo:

1. Na seção **Configuração de inicialização** selecione uma ou mais unidades e configure os parâmetros relevantes.

Unidade	Mostra o número da unidade.

Imagem de inicialização atual	Mostra a imagem de inicialização atual.
Imagem da Próxima Inicialização	Seleciona uma próxima imagem para inicialização. Quando o switch ligar ele tentará inicializar com essa imagem. Não pode ser igual a **Imagem de Backup**.
Imagem de Backup	Seleciona uma imagem de backup. Quando o Switch falhar ao inicializar com a **Próxima Imagem de Inicialização**, ele tentará inicializar a **Imagem de Backup**. Não pode ser igual a **Próxima Imagem de Inicialização**.
Configuração da inicialização atual	Mostra a configuração de inicialização atual.
Configuração da Próxima inicialização	Especifica uma próxima configuração para inicialização. Quando o switch ligar ele tentará inicializar com essas configurações. Não pode ser igual a **Configuração de Backup**.
Configuração de Backup	Especifica uma configuração de backup. Quando o Switch falhar ao inicializar com a **Próxima Configuração de Inicialização**, ele tentará inicializar a **Configuração de Backup**. Não pode ser igual a **Próxima Configuração de Inicialização**.

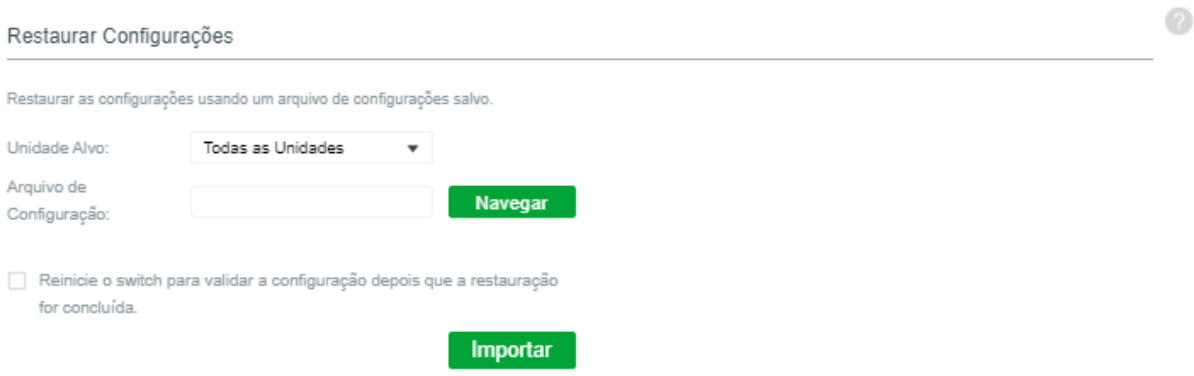
2. Clique em **Aplicar**

Na seção Tabela de Imagem você pode visualizar as informações de imagem de inicialização atual, próxima imagem de inicialização e imagem de backup. As informações exibidas são as seguintes:

Nome da Imagem	Mostra o nome da imagem.
Versão do Software	Mostra a versão do software da imagem.
Versão do Flash	Mostra a versão flash da imagem.

Restaurando as configurações do Switch

Vá até o menu **SISTEMA > Ferramentas do Sistema > Configuração de Restauração** para carregar a seguinte página:



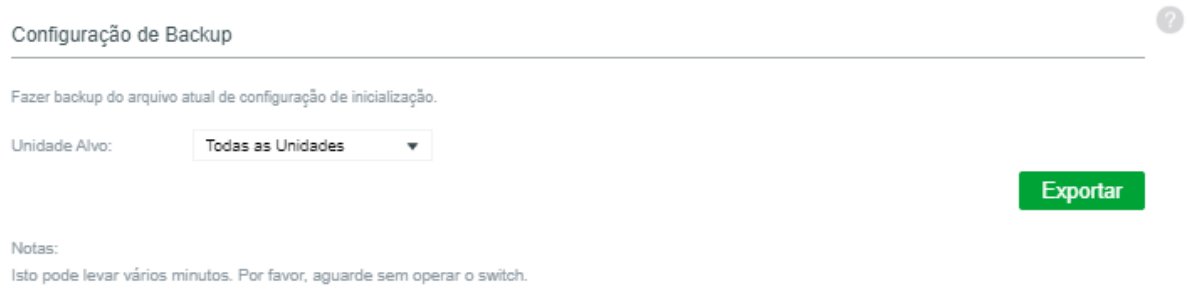
Siga os seguintes passos para restaurar as configurações do Switch:

1. Na seção **Restaurar Configurações** selecione a unidade que deseja restaurar;
2. Clique em **Navegar para selecionar** a configuração que você deseja importar;
3. Escolha se você marcará o campo “reiniciar o switch após a restauração estar completa”. A imagem importada só terá efeito no Switch após o reinicio do mesmo;
4. Clique no botão **Importar** para importar o arquivo de configuração.

> Levará algum tempo até o Switch restaurar as configurações, aguarde sem realizar nenhuma operação.

Backup do arquivo de Configuração

Vá até o menu **SISTEMA > Ferramentas do Sistema > Configuração de Backup** para carregar a seguinte página:

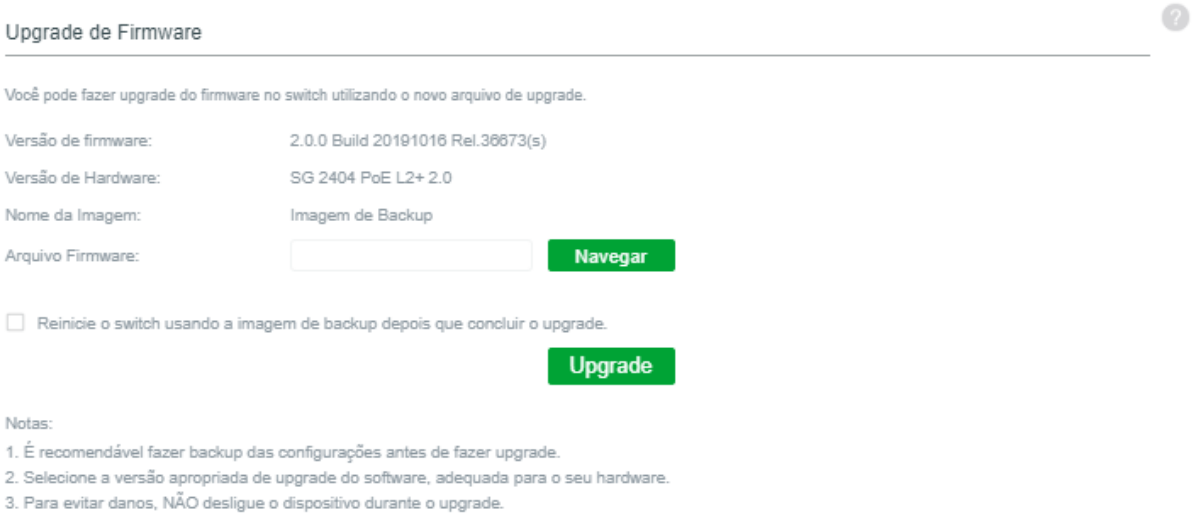


Na seção **Configuração de Backup** selecione uma unidade e clique em **Exportar** para exportar o arquivo de Configuração.

> Levará algum tempo até o Switch exportar as configurações, aguarde sem realizar nenhuma operação.

Upgrading de Firmware

Vá até o menu **SISTEMA > Ferramentas do Sistema > Upgrade de Firmware** para carregar a seguinte página:



Você pode visualizar as informações atuais do firmware nesta página:

Versão do Firmware	Mostra a versão atual do Firmware.
Versão de Hardware	Mostra a versão atual do Hardware.
Nome da Imagem	Mostra a imagem a ser atualizada. A operação só terá efeito na imagem mostrada aqui.

Siga os passos a seguir para realizar a atualização do Firmware do Switch:

1. Clique no botão **Navegar** e selecione o arquivo para atualização do firmware;
2. Escolha se você marcará o campo “reiniciar o switch após a atualização estar completa”. A nova versão do Firmware só estará ativa no Switch após o reinicio do mesmo;
3. Clique no botão **Upgrade** para atualizar o sistema.

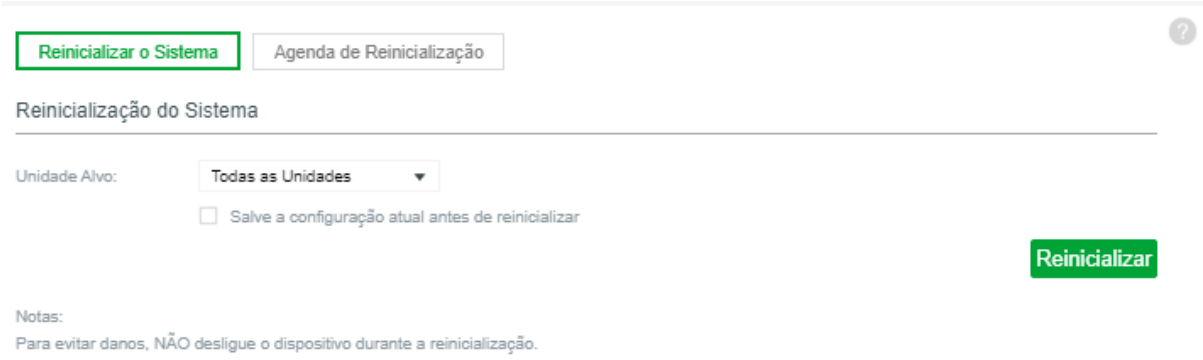
> Levará algum tempo até o Switch realizar o upgrade completo, aguarde sem realizar nenhuma operação.
> É recomendado realizar um backup das configurações antes de realizar a atualização do firmware.

Reiniciando o Switch

Existem dois métodos para realizar a reinicialização do Switch: reiniciar manualmente o switch e configurar um agendamento para realizar a reinicialização automática do Switch.

Reiniciando o Switch Manualmente

Vá até o menu **SISTEMA > Ferramentas do Sistema > Reinicializar o Sistema > Reinicializar o Sistema** para carregar a seguinte página:



Siga os seguintes passos para reiniciar o Switch:

1. Na seção **Reinicialização do Sistema** selecione a unidade desejada;
2. Escolha se você deseja salvar a configuração atual antes da reinicialização;
3. Clique em **Reinicializar**.

Configurando uma Reinicialização Agendada

Vá até o menu **SISTEMA > Ferramentas do Sistema > Reinicializar o Sistema > Agenda de Reinicialização** para carregar a seguinte página:

Siga os seguintes passos para configurar uma reinicialização agendada para o Switch:

1. Na seção **Configuração de Agendamento de Reinicialização** selecione um método e especifique os parâmetros relacionados;

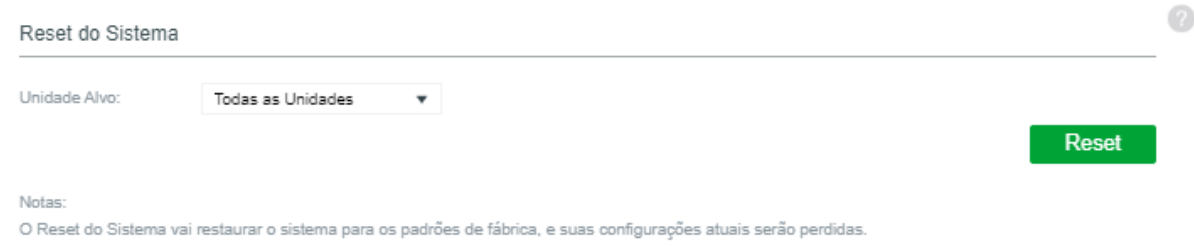
Intervalo de Tempo	Especifique um período de tempo. O Switch irá reiniciar após esse período. Os valores variam entre 1 e 43200 minutos. Clique no botão **Salvar** para tornar esse agendamento recorrente ou marque a opção “salve a configuração atual antes de reiniciar”.
Horário Especial	Especifique uma data e horário para que o Switch reinicie. **Mês/Dia/Ano:** Especifique a data para o Switch reiniciar. **Horário (HH:MM):** Especifique o horário que o Switch irá reiniciar, no formato HH:MM.

2. Escolha se você deseja salvar a configuração atual antes da reinicialização;
3. Clique em **Aplicar**

> Se após o agendamento da reinicialização o Switch for reiniciado por algum motivo, o agendamento será considerado como já efetuado.

Reset do Sistema

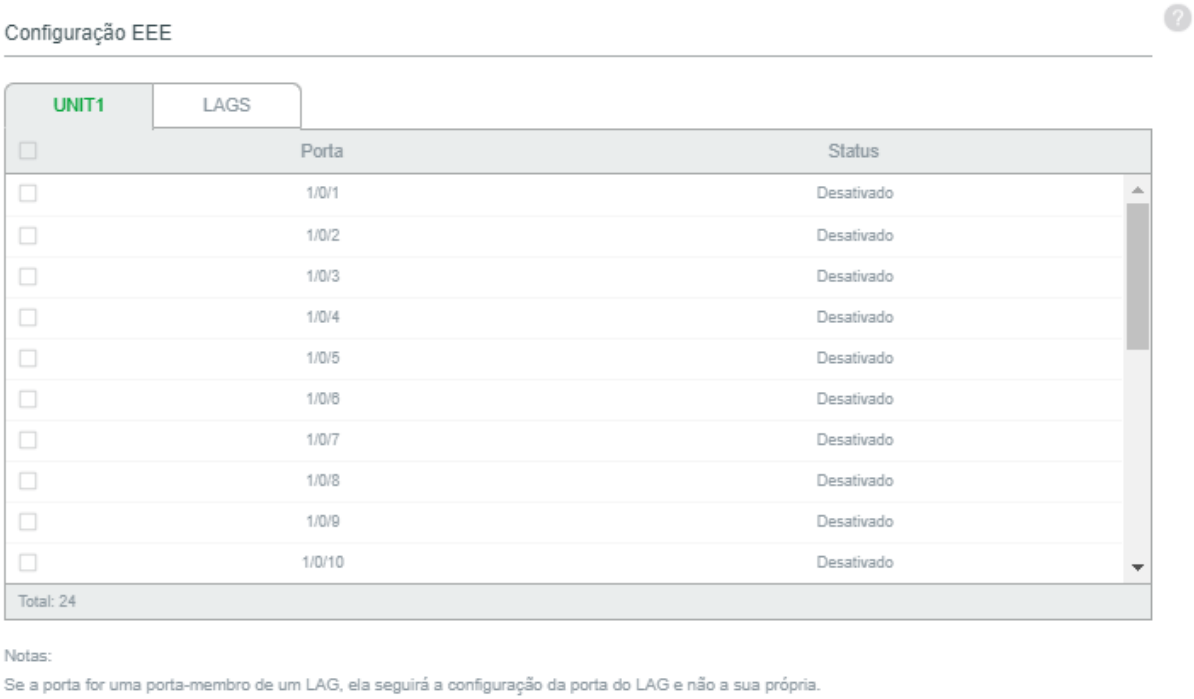
Vá até o menu **SISTEMA > Ferramentas do Sistema > Reinicializar o Sistema > Reset do Sistema** para carregar a seguinte página:



Na seção **Reset do Sistema** selecione a unidade que você deseja resetar e clique em **Reset**. Após o Reset acontecer todas as configurações do switch serão restauradas para o padrão de fábrica.

Configuração EEE

Vá até o menu **SISTEMA > EEE** para carregar a seguinte página:



Siga os seguintes passo para configurar o EEE:

1. Na seção **Configuração EEE** selecione uma ou mais portas para serem configuradas;
2. Habilite ou desabilite o EEE nas portas selecionadas;
3. Clique em **Aplicar**

Configuração PoE

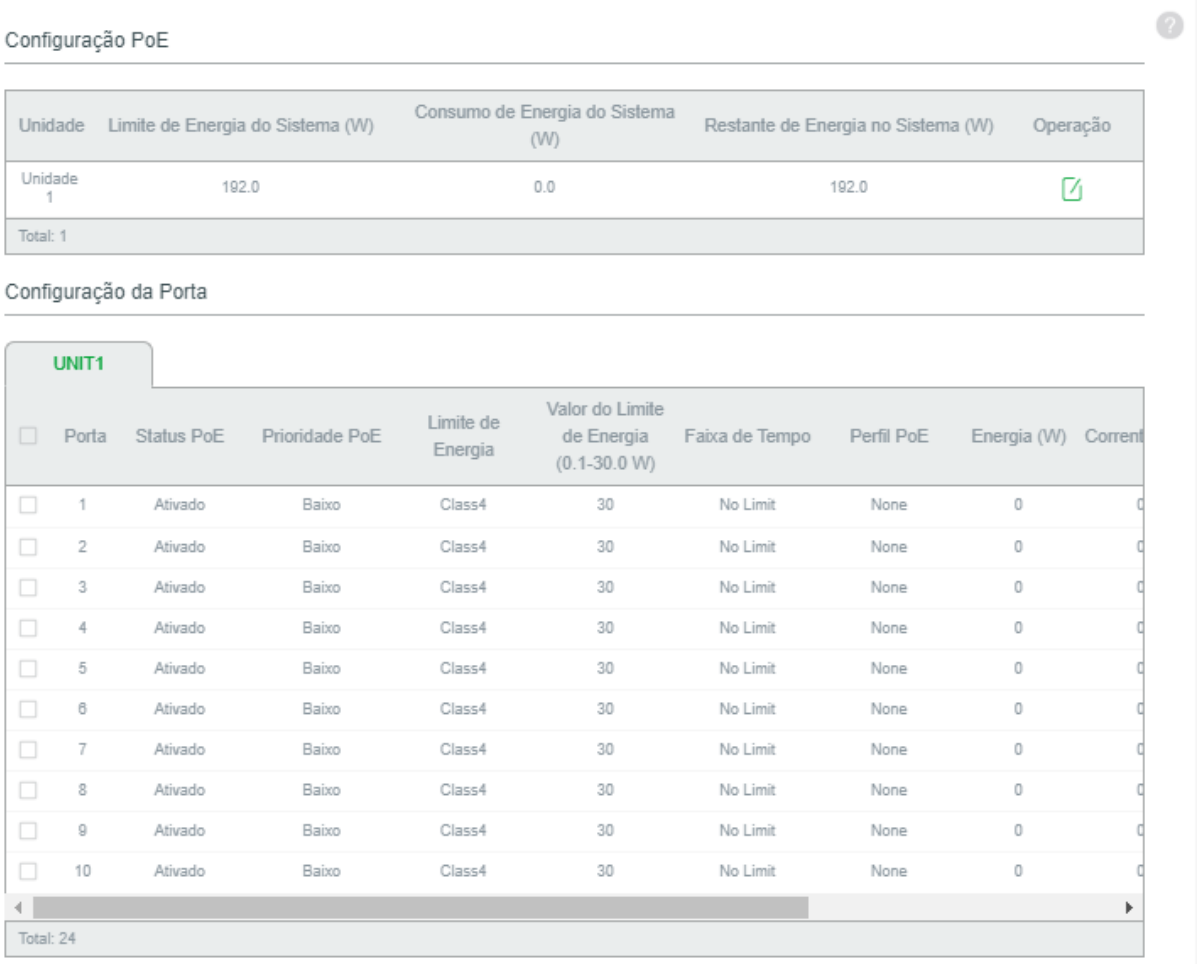
Com a função PoE você pode:

- Configurar os parâmetros PoE manualmente;
- Configurar os parâmetros PoE utilizando perfis.

Você pode configurar os parâmetros PoE um-a-um através da configuração de parâmetros PoE manualmente. Você também pode criar perfis com os parâmetros desejados e vincular o perfil à porta para obter agilidade na configuração.

Configurando os Parâmetros PoE Manualmente

Vá até o menu SISTEMA > PoE > Configuração PoE para carregar a seguinte página:

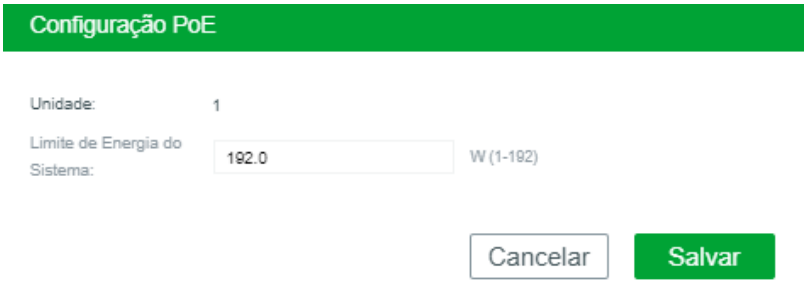


Siga os seguintes passos para configurar os parâmetros básicos do PoE:

1. Na seção **Configuração PoE** você pode visualizar os parâmetros atuais do PoE.

Limite de Energia do Sistema (w)	Mostra o máximo de potência que o Switch PoE pode fornecer.
Consumo de Energia do Sistema (w)	Mostra, em tempo real, o consumo de energia do Switch PoE.
Restante de Energia do Sistema (w)	Mostra, em tempo real, a quantidade de potência que o Switch tem disponível para fornecer.

Você ainda pode clicar no botão para configurar o Limite de Potência do Sistema. Clique em **Aplicar**.



Unidade	Mostra a unidade em números.

Limite de Energia do Sistema	Especifica o valor máximo de potência que o Switch poderá fornecer, variando em 1 e 192 Watts.

2. Na seção **Configuração da Porta** você pode selecionar a porta que você quer configurar, especificar os parâmetros e então clique em **Aplicar**.

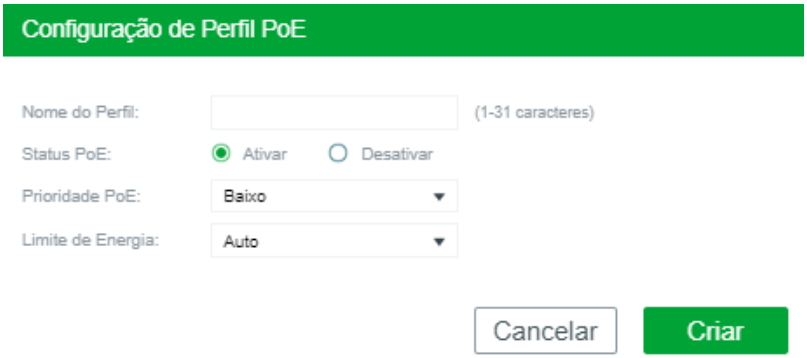
Status PoE	Habilita ou desabilita a função PoE para a porta correspondente. A porta só pode fornecer energia para o PD quando seu estado PoE estiver habilitado.
Prioridade PoE	Selecione o nível de prioridade correspondente para a porta. Quando o fornecimento de energia exceder o limite do sistema o Switch irá desativar a energia dos PDs em portas de baixa prioridade para garantir uma operação estável para os outros PDs.
Limite de Energia	Especifica o máximo de potência que a porta pode fornecer. As seguintes opções estarão disponíveis: **Auto:** o Switch irá alocar um valor máximo para a porta automaticamente; **Class1:** o limite de potência da porta será 4 Watts; **Class2:** o limite de potência da porta será 7 Watts; **Class3:** o limite de potência da porta será 15.4 Watts; **Class4:** o limite de potência da porta será 30 Watts; **Manual:** você poderá entrar com um valor manualmente.
Valor do Limite de Energia (0.1 – 30 W)	Se você selecionar o modo de limite de potência como **Manual** você deve especificar um valor neste campo. Se você selecionar um modo de limite de potência entre classe 1 e classe 4 você pode ver o valor da potência nesse campo.
Faixa de Tempo	Selecione um Time Range, a porta só fornecerá energia durante o período do time range. Para ver como criar um Time Range vá até **Configurações de Time Range**.
Perfil PoE	Um método de configuração ágil para as portas correspondentes. Se um perfil é selecionado você não será capaz de alterar o estado PoE, a prioridade PoE ou os limites de potência manualmente. Para ver como criar os perfis vá até **Configurando Parâmetros PoE usando um perfil.**.
Energia (W)	Mostra em tempo real a potência consumida pela porta.
Corrente (mA)	Mostra em tempo real a corrente consumida pela porta.

Tensão (V)	Mostra em tempo real a Tesão fornecida à porta.
Classe PD	Mostra a Classe à qual pertence o PD conectado à porta.
Status de Energia	Mostra em tempo real se a porta está fornecendo alimentação.

Configuração dos parâmetros PoE por perfil de usuário

Criando um perfil PoE

Vá até o menu **SISTEMA > PoE > Perfil PoE** e clique no botão **Adicionar** para carregar a seguinte página:



Siga os seguintes passos para criar um perfil PoE:

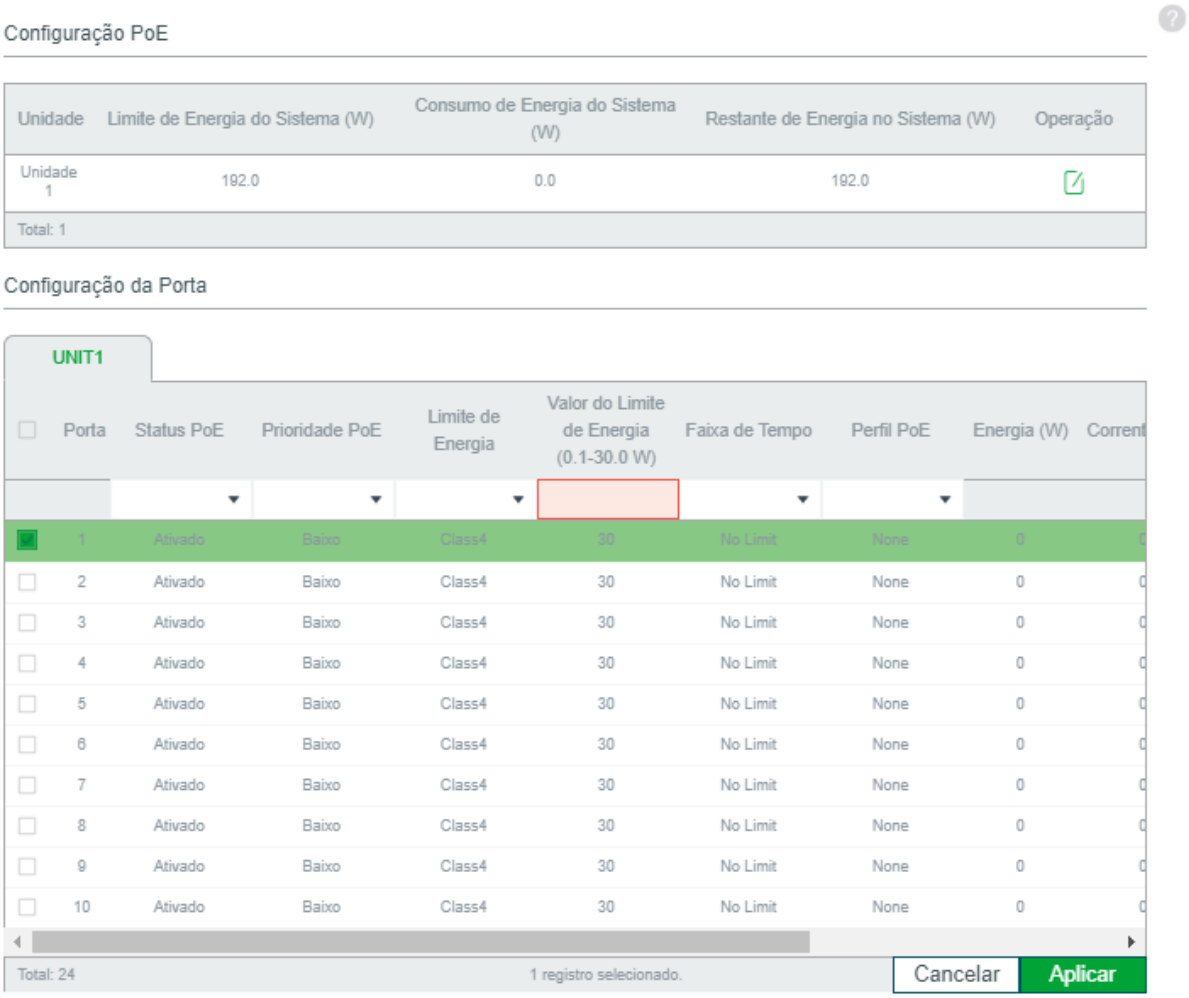
1. Na seção **Criar um Perfil PoE** especifique as configurações desejadas ao perfil.

Nome do Perfil	Especifique o nome do Perfil PoE.
Status PoE	Especifique o estado PoE para o Perfil PoE.
Prioridade PoE	Especifique o nível de prioridade do Perfil PoE. Pode ser **Alto**, **Médio** ou **Baixo**. Quando a energia fornecida exceder o limite de potência do sistema o switch irá desligar os PDs em portas de baixa prioridade para garantir funcionamento estável para os outros PDs.
Limite de Energia	Especifica o máximo de potência que a porta pode fornecer. As seguintes opções estarão disponíveis: **Auto:** o Switch irá alocar um valor máximo para a porta automaticamente; **Class1:** o limite de potência da porta será 4 Watts; **Class2:** o limite de potência da porta será 7 Watts; **Class3:** o limite de potência da porta será 15.4 Watts; **Class4:** o limite de potência da porta será 30 Watts; **Manual:** você poderá entrar com um valor manualmente.

2. Clique em **Criar**

Vinculando um perfil PoE à uma porta.

Vá até o menu **SISTEMA > PoE > Configuração PoE** e clique no botão **Adicionar** para carregar a seguinte página:

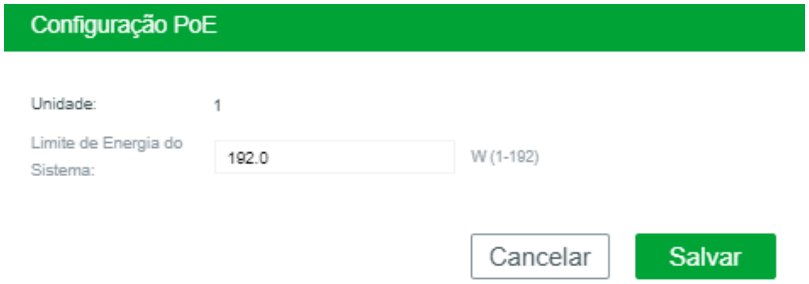


Siga os seguintes passos para vincular um perfil PoE à uma porta:

1. Na seção **Configuração PoE** você pode visualizar os parâmetros atuais do PoE.

Limite de Energia do Sistema (w)	Mostra o máximo de potência que o Switch PoE pode fornecer.
Consumo de energia do Sistema (w)	Mostra, em tempo real, o consumo de energia do Switch PoE.
Restante de Energia do Switch (w)	Mostra, em tempo real, a quantidade de potência que o Switch tem disponível para fornecer.

Você ainda pode clicar no botão para configurar o Limite de Potência do Sistema. Clique em **Aplicar**.



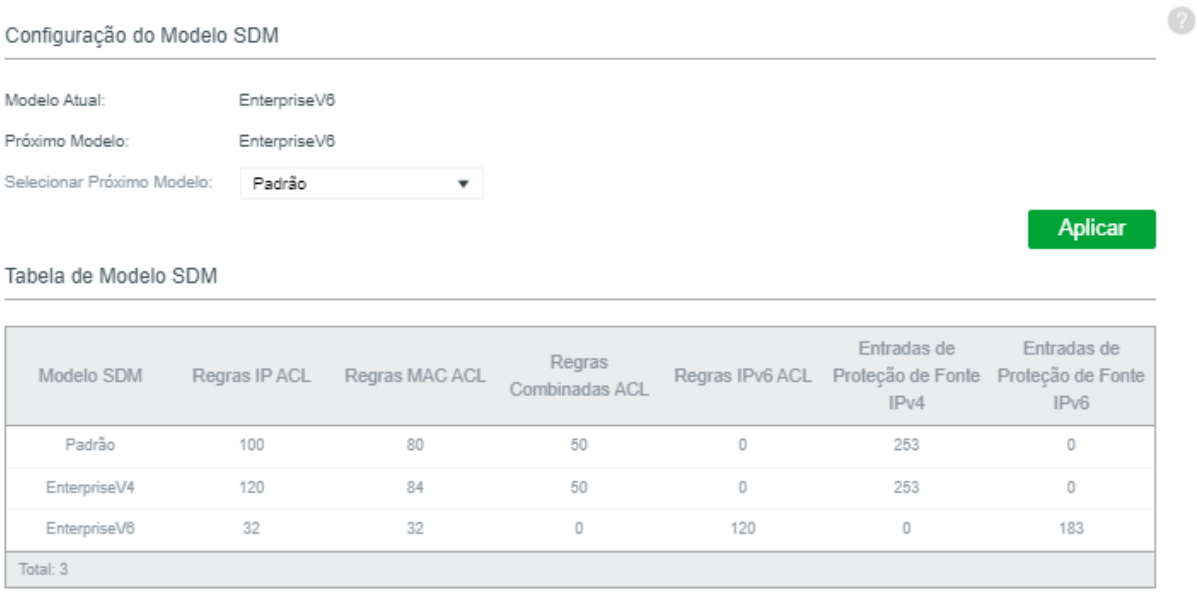
Unidade	Mostra a unidade em números.
Limite de Potência do Sistema	Especifica o valor máximo de potência que o Switch poderá fornecer, variando em 1 e 192 Watts.

2. Na seção **Configuração da Porta** você pode selecionar uma ou mais portas e configurar os seguintes parâmetros: **Faixa de Tempo** e **Perfil PoE**. Clique em **Aplicar** e os parâmetros do Perfil PoE selecionado serão exibidos na tabela.

Status PoE	Exibe o estado da função PoE para a porta correspondente. A porta só pode fornecer energia para o PD quando seu estado PoE estiver habilitado.
Prioridade PoE	Exibe o nível de prioridade correspondente para a porta. Quando o fornecimento de energia exceder o limite do sistema o Switch irá desativar a energia dos PDs em portas de baixa prioridade para garantir uma operação estável para os outros PDs.
Limite de Energia	Exibe o máximo de energia que a porta pode fornecer.
Valor do Limite de Energia (0.1 – 30 W)	Exibe o valor do limite de potência.
Time Range	Selecione um Time Range, a porta só fornecerá energia durante o período do time range. Para ver como criar um Time Range vá até **Configurações de Time Range**.
Perfil PoE	Selecione um perfil PoE que você deseja para a porta. Se um perfil é selecionado você não será capaz de alterar o estado PoE, a prioridade PoE ou os limites de potência manualmente.
Energia (W)	Mostra em tempo real a potência consumida pela porta.
Corrente (mA)	Mostra em tempo real a corrente consumida pela porta.
Tensão (V)	Mostra em tempo real a Tesão fornecida à porta.
Classe PD	Mostra a Classe à qual pertence o PD conectado à porta.
Status de Energia	Mostra em tempo real se a porta está fornecendo alimentação.

Configuração de Modelo SDM

Vá até o menu **SISTEMA > Modelo SDM** para carregar a seguinte página:



Na seção **Configuração do Modelo SDM** selecione um modelo e clique em **Aplicar**. As configurações ficarão ativas após o Switch reiniciar.

Modelo Atual	Mostra o Modelo que está em vigor.
Próximo Modelo	Mostra o Modelo que entrará em vigor após a reinicialização do sistema.
Selecionar Próximo Modelo	Seleciono o Modelo que entrará em vigor após a reinicialização do sistema. **Padrão:** Seleciona o Modelo padrão. O qual proporciona balanço em ter as regras IP ACL, MAC ACL e entradas de detecção ARP. **EnterpriseV4:**Selecionando o Modelo EnterpriseV4 você maximizará os recursos do sistema para regras IP ACL e MAC ACL. **EnterpriseV6:** Selecionando o Modelo enterpriseV6 você maximizará os recursos do sistema para regras IPv6 ACL.

A tabela de Modelos mostra a alocação de recursos para cada Modelo.

Modelo SDM	Mostra o nome dos Modelos.
Regras IP ACL	Mostra o número de regras IP ACL incluindo regras ACL de Camada 3 e Camada 4.
Regras MAC ACL	Mostra o número de regras ACL Camada 2.
Regras combinadas ACL	Mostra o úmero de regras ACL combinadas.
Regras IPv6 ACL	Mostra o número de regras IPv6 ACL.
Entradas de Proteção de Fonte IPv4	Mostra o número de entradas de Proteção de Fonte IPv4.
Entradas de Proteção de Fonte IPv6	Mostra o número de entradas de Proteção de Fonte IPv6.

Regra ACL contador de pacotes	Mostra o número de regras ACL de conteúdo de pacotes.

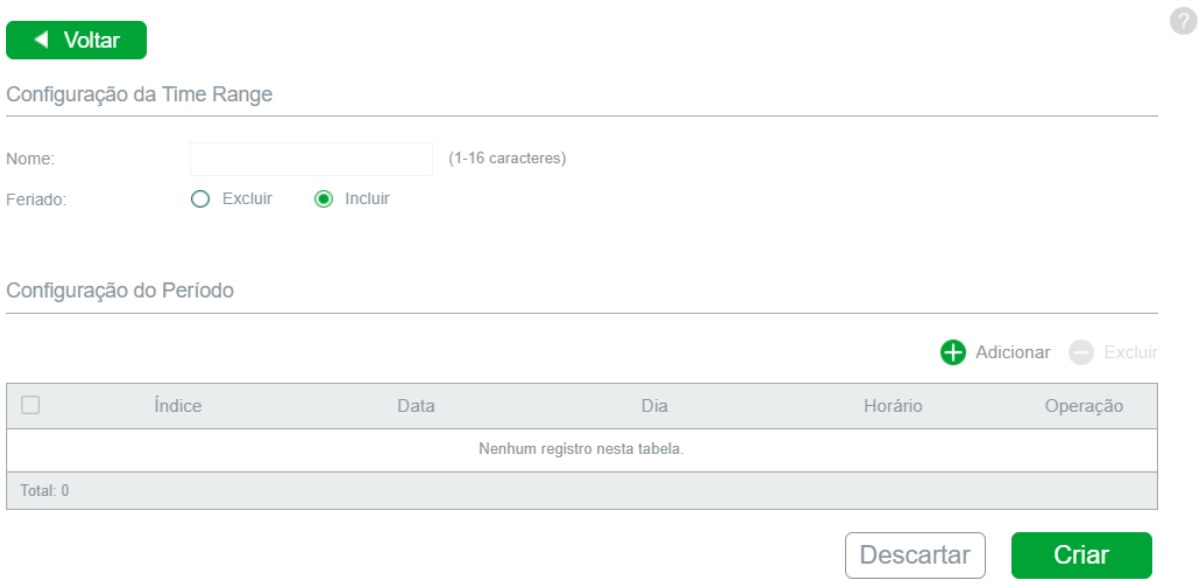
Configuração Time Range

Para completar a configuração Time Range siga os seguintes passos:

1. Adicione entradas Time Range;
2. Configure os Time Range para feriados.

Adicionando entradas Time Range

Vá até o menu **SISTEMA > Time Range > Configuração da Time Range** e clique no botão Adicionar para carregar a seguinte página:

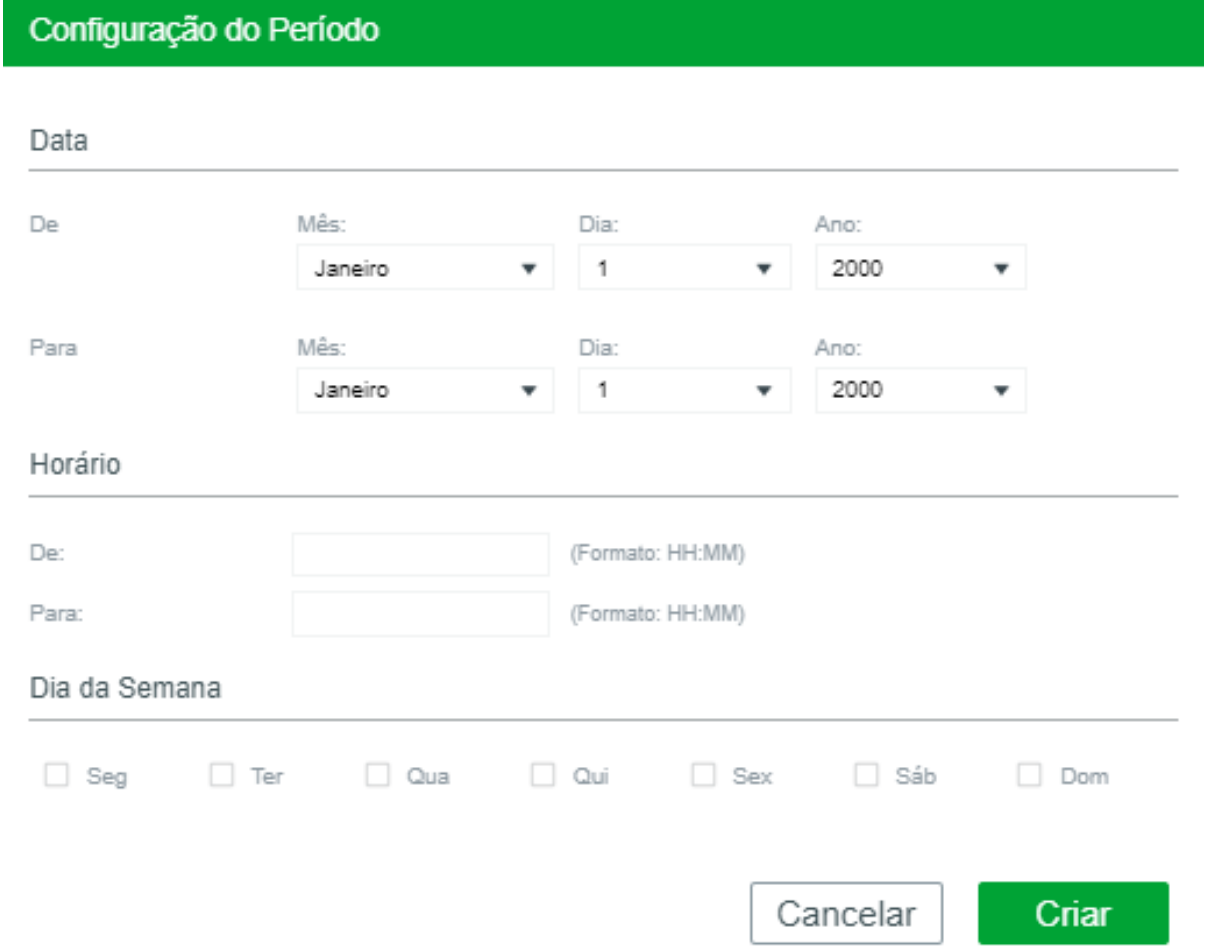


Siga os seguintes passos para adicionar entradas de Time Range:

1. Na seção **Configuração da Time Range**, especifique o nome para uma entrada e selecione o modo de Feriado.

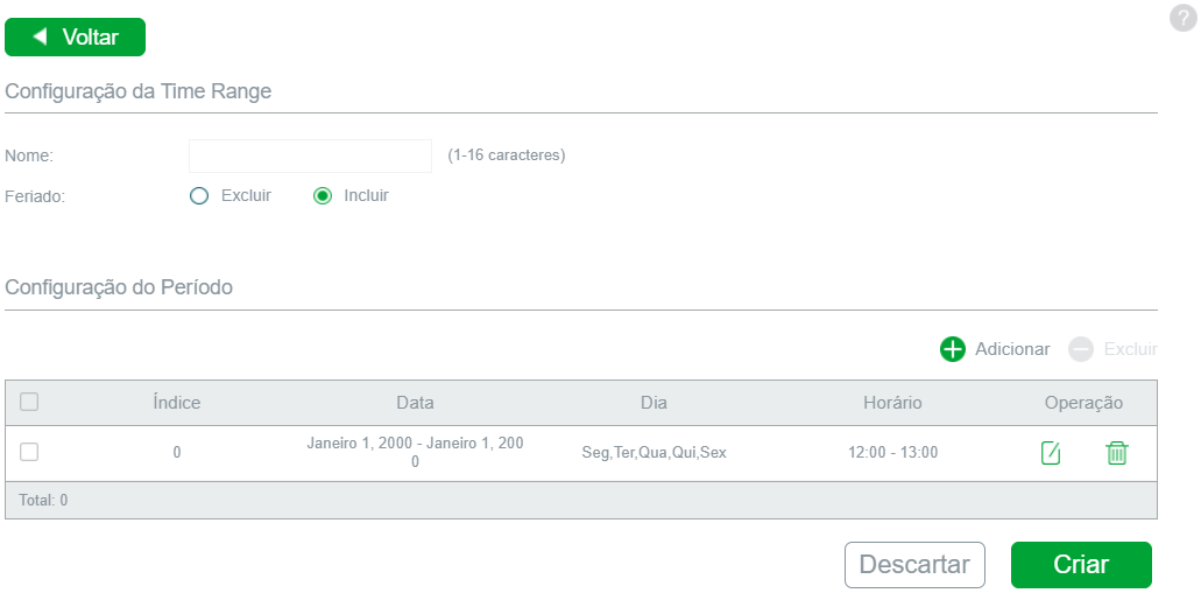
Nome	Especifique um nome para a entrada.
Feriado	Selecione para incluir ou excluir os feriados no Time Range. **Excluir:** O time range não terá efeito em feriados. **Incluir:**O time range terá efeito em feriados. **Para Configurar os Feriados vá para Configurando de Feriado**

2. Na seção Configuração do Período clique no botão Adicionar e a seguinte janela irá aparecer:



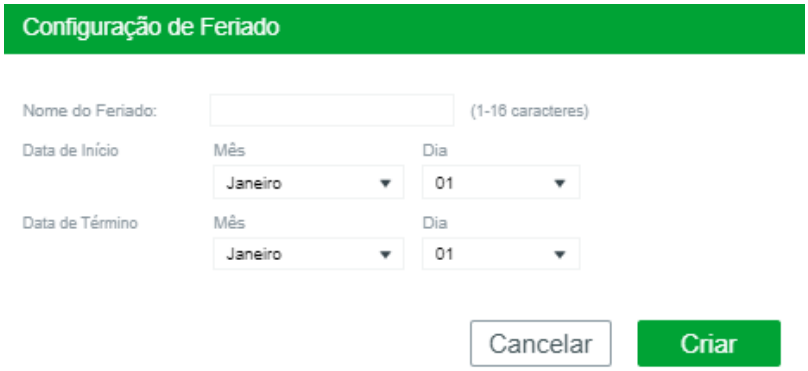
Data	Especifique uma data para início e uma para termino.
Horário	Especifique um horário para início e um horário para termino para o dia.
Dia da Semana	Selecione os dias da semana como períodos para o Time Range.

3. Da mesma forma você pode adicionar mais entradas de períodos de tempo de acordo com sua necessidade. O período de tempo final é a soma de todos os períodos de tempo da tabela. Clique em **Criar**.



Configuração de Feriado

Vá até o menu **SISTEMA > Time Range > Configuração de Feriado** e clique no botão Adicionar para carregar a seguinte página:



Configure os seguintes parâmetros e clique em **Criar** para adicionar um Feriado.

Nome do Feriado	Especifique o nome do feriado.
Data de início	Especifique a data de início do Time Range de feriado.
Data de Término	Especifique a data de término do Time Range de feriado.

Você pode adicionar mais feriados realizando o mesmo procedimento. O Time Range de Feriados é a soma de todos os feriados criados.

Informações Legais

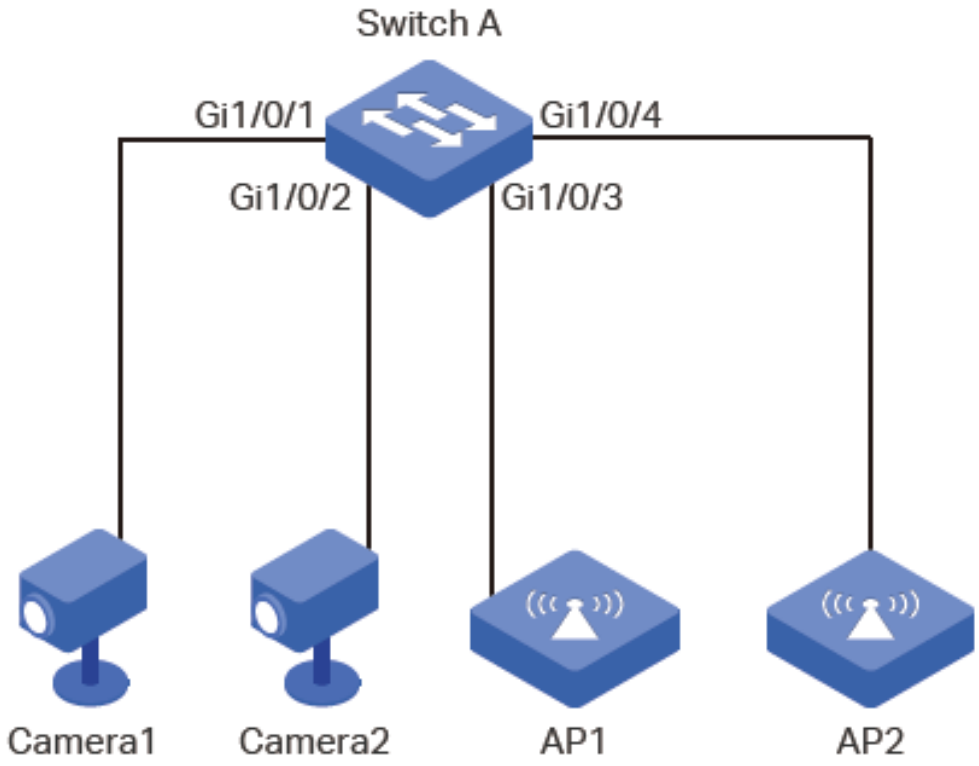
Permite o direcionamento aos Termos de Uso (https://backend.intelbras.com/sites/default/files/download/politicas-privacidade/termos-unificados/portugues-termo_unificado_sw_app_cloud/termos-de-uso-unico-portugues.html?prod=4780033) e a Política de Privacidade (https://backend.intelbras.com/sites/default/files/download/politicas-privacidade/termos-unificados/portugues-termo_unificado_sw_app_cloud/politica-de-privacidade-unica-portugues.html)

Para maiores informações, favor acesar os *links.*

Exemplo de configurações PoE

Requisitos de Rede

A topologia de rede de uma empresa é como mostrada a baixo. Camera1 e Camera2 trabalham para uma companhia de monitoramento e não podem ser desligadas. AP1 e AP2 disponibilizam conexão de internet e só são utilizados em horário comercial.

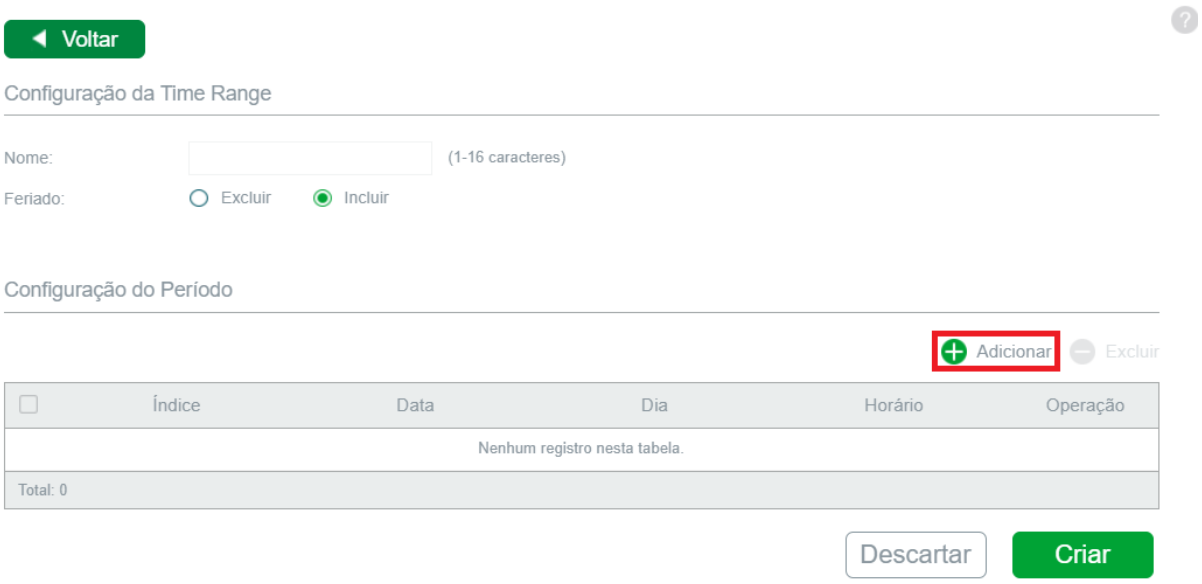


Configurando o Cenário

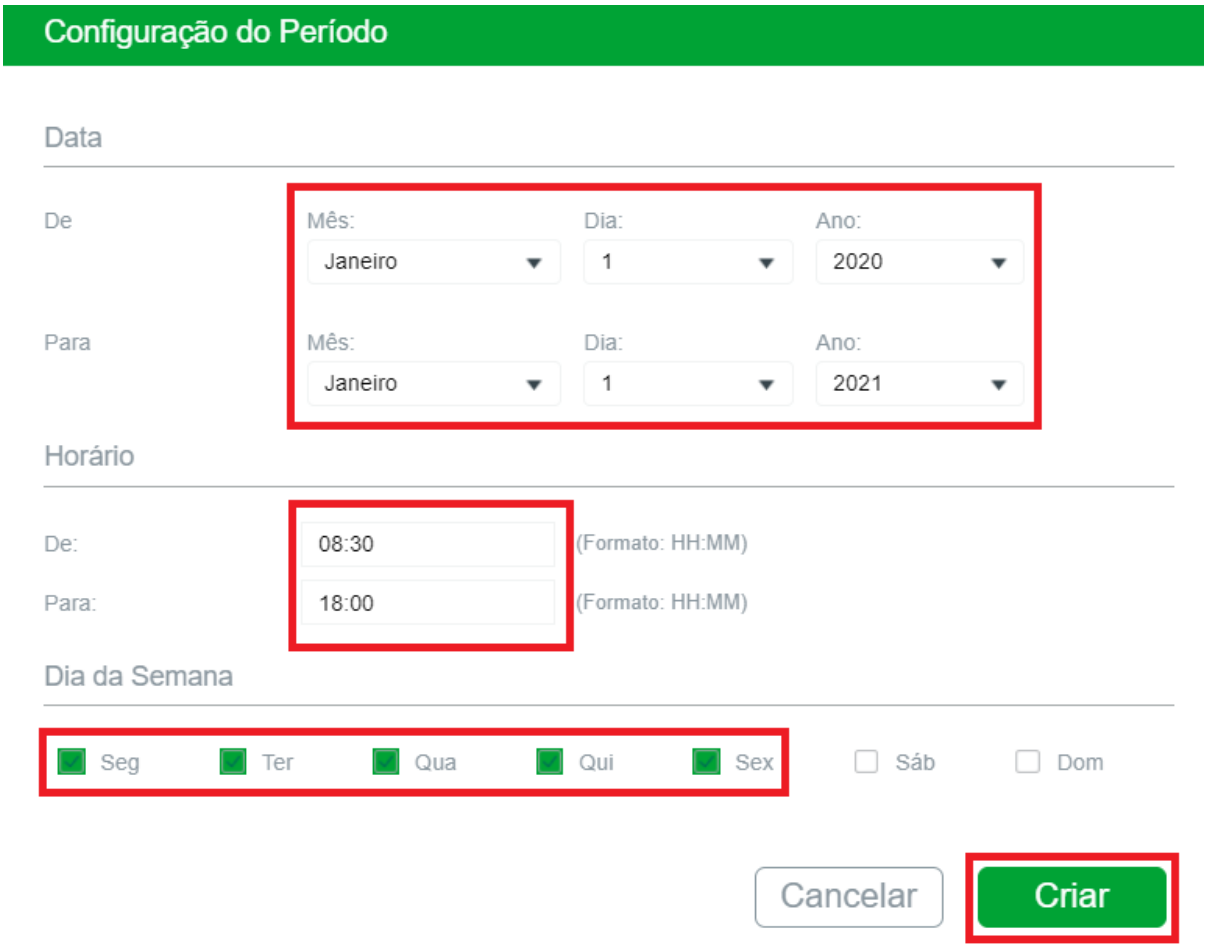
Para implementar os requisitos citados à cima você pode configurar um Time Range PoE horário comercial, por exemplo, das 08:30 às 18:00 para os dias de semana. E então aplicar as configurações para as portas 1/0/3 e 1/0/4. As portas 1/0/1 necessitam fornecer alimentação a todo momento, portanto elas podem ficar de fora de uma configuração de Time Range e podem permanecer com as configurações padrões.

Como a configuração da porta 1/0/3 e 1/04 são iguais iremos utilizar a porta 1/0/3 como exemplo.

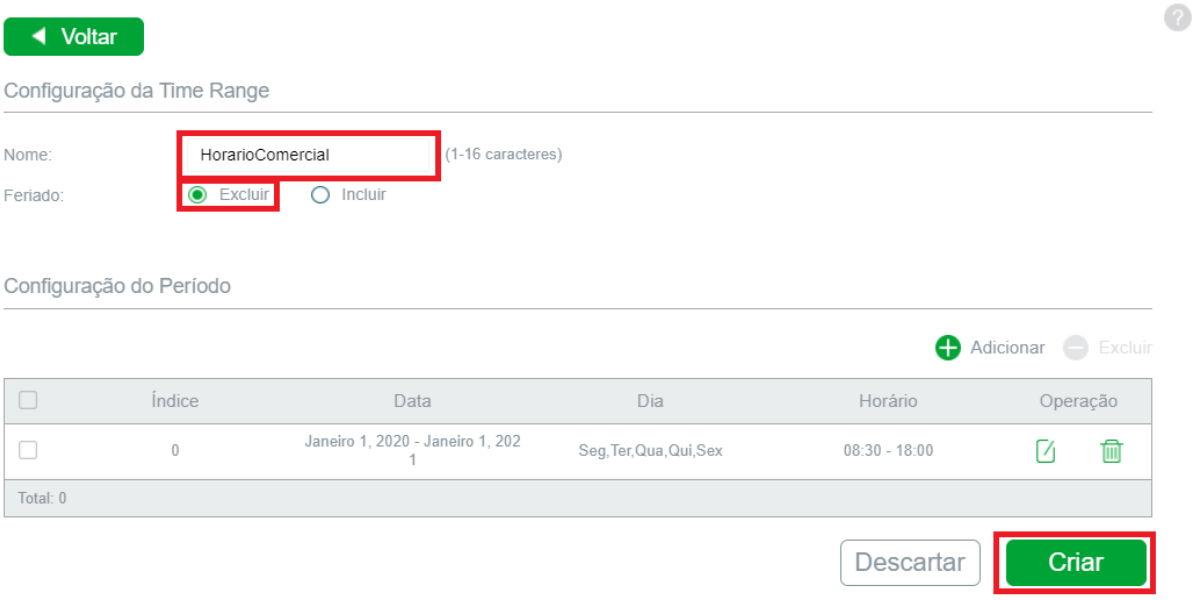
1. Vá até o menu **SISTEMA > Time Range > Configuração da Time Range** e clique no botão Adicionar para carregar a seguinte página:



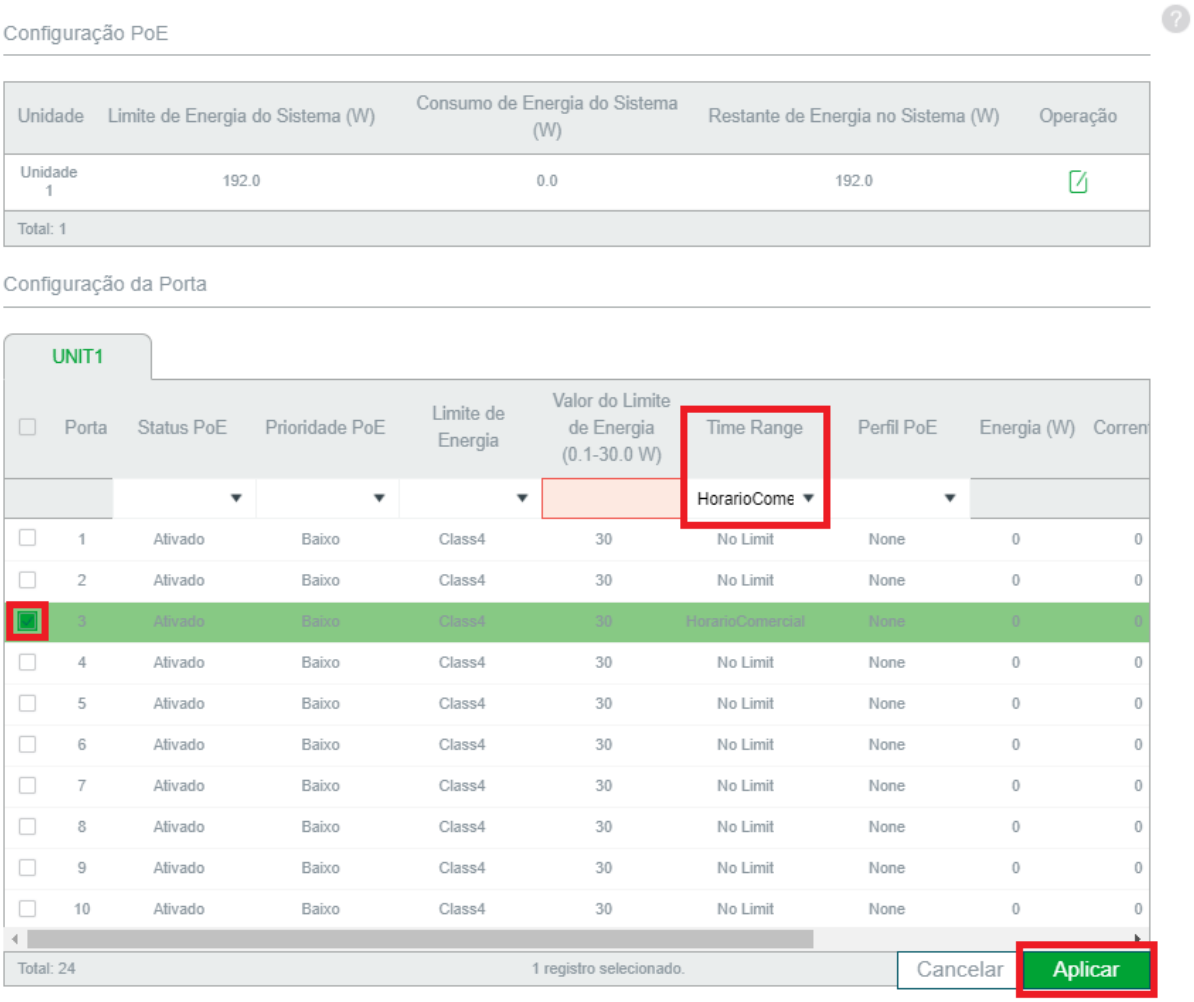
2. Clique no botão Adicionar e a seguinte janela aparecerá. Configure a **Data**, **Horário** e **Dia da Semana** como na figura a seguir. Clique em **Criar**.



3. Especifique um nome para o Time Range e selecione Excluir para fazer que as configurações do Time Range não afetem os feriados. Clique em **Criar**.



4. Vá até o menu **SISTEMA > PoE > Configurações PoE** para carregar a seguinte página. Selecione a porta 1/0/3 e aponte o Time Range como *HorarioComercial*. Clique em **Aplicar**.



5. Clique em Salvar para salvar as configurações.

Apêndice: Configuração Padrão

As configurações padrão de Informações do sistema estão listadas nas tabelas a seguir:

Configurações padrão da configuração de descrição do dispositivo

Parâmetros	Configurações Padrão
Nome do Dispositivo	SG 2404 PoE L2+
Localização do Dispositivo	Santa Catarina
Contato do Sistema	www.intelbras.com.br (http://www.intelbras.com.br/)

Configurações padrão da configuração de Horário do Sistema

Parâmetros	Configurações Padrão
Origem do Horário	Manual

Configurações padrão da configuração de Horário de Verão

Parâmetros	Configurações Padrão
Estado do Horário de Verão	Desabilitado

Configurações padrão de gerenciamento de usuário estão listadas na tabela a seguir:

Configurações padrão da configuração de Usuário

Parâmetros	Configurações Padrão
Nome de Usuário	admin
Senha	admin
Nível de Acesso	Administrador

Configurações padrão das ferramentas do sistema estão listadas na tabela a seguir:

Configurações padrão configuração de inicialização

Parâmetros	Configurações Padrão
Imagem de inicialização atual	image1.bin
Próxima imagem de inicialização	image1.bin
Imagem de Backup	Image2.bin

Configuração de inicialização atual	config1.cfg
Próxima Configuração de inicialização	config1.cfg
Configuração de Backup	config2.cfg

Configurações padrão do EEE está listada na tabela a seguir:

Configurações padrão da configuração EEE

Parâmetros	**Configurações Padrão**
Estado	Desabilitado

Configurações padrão do PoE estão listadas na tabela a seguir:

Configurações padrão da configuração PoE

Parâmetros	**Configurações Padrão**
Configuração PoE	
Limite de potência do sistema	192 Watts
Configuração de Portas	
Estado da Porta	Habilitado
Prioridade PoE	Baixa
Limite de Potência (0.1-30 watts)	Classe 4
Time Range	Sem limites
Perfil PoE	Nenhum
Configurações de Perfil	
Nome do Perfil	Nenhum
Estado PoE	Habilitado
Prioridade PoE	Alta
Limite de Potência	Automático

Configurações padrão do Modelo SDM estão listadas na tabela a seguir:

Configurações padrão da configuração do Modelo SDM

Parâmetros	**Configurações Padrão**
ID do Modelo atual	Padrão
Próxima ID de Modelo	Padrão

Configurações padrão de Time Range estão listadas na tabela a seguir:

Configurações padrão da configuração do Time Range

Parâmetros	Configurações Padrão
Feriado	Exclude

GERENCIANDO AS INTERFACES FÍSICAS

Interfaces Físicas

Visão Geral

Interfaces são utilizadas para trocar dados e interagir com interfaces de outros dispositivos de rede. Interfaces são classificadas em interfaces físicas e interfaces de camada 3.

- Interfaces físicas são as ports do Switch. Elas encaminham pacotes baseadas na tabela de endereços MAC.
- Interfaces de camada 3 são usadas para encaminhar pacotes IPv4 e IPv6 utilizando protocolos de rota estática ou dinâmica. Você pode usar interfaces de camada 3 para rotas IP e rotas entre VLANs.

Esse capítulo irá fazer uma introdução às configurações das interfaces físicas.

Funções Suportadas

O Switch suporta as seguintes função para as interfaces físicas:

Parâmetros Básicos:

Você pode configurar o estado da porta, velocidade, modo duplex, controle de fluxo e outros parâmetros básicos das portas.

Isolamento de Portas:

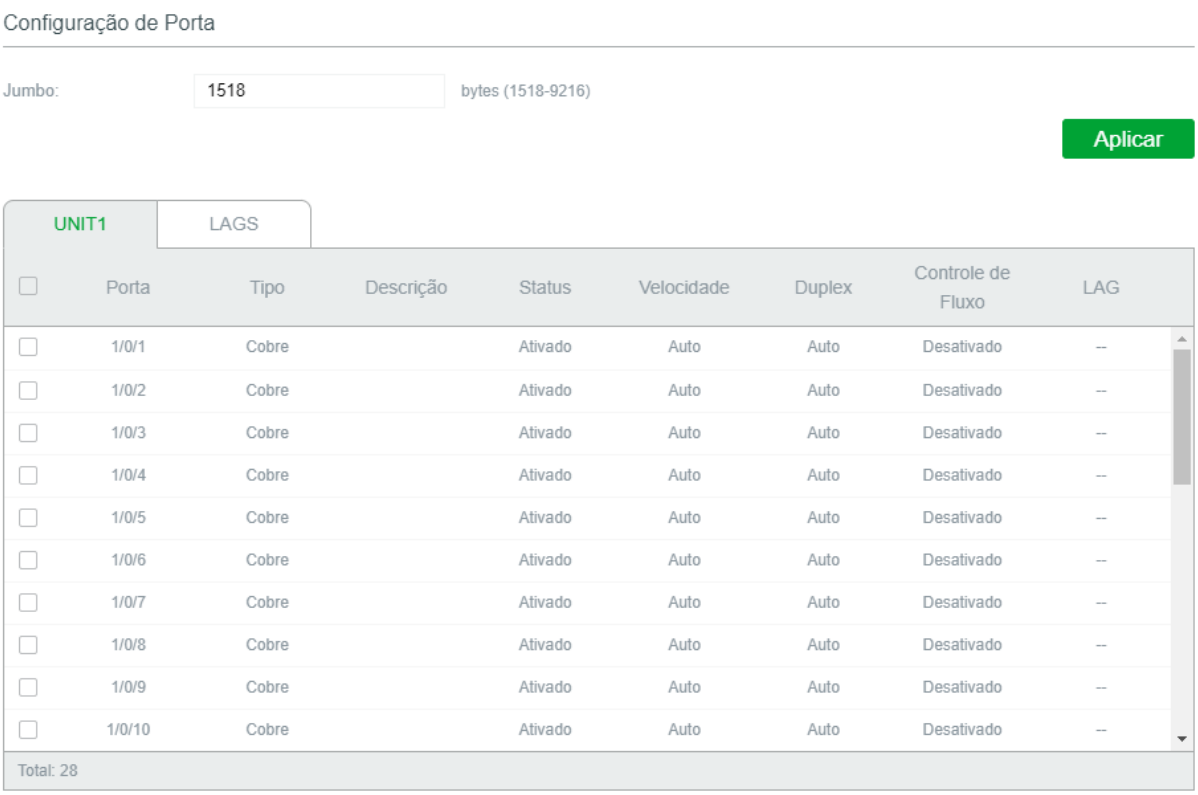
Você pode usar esta função para restringir o encaminhamento de pacotes de uma porta somente para as portas dentro da lista de encaminhamento.

Loopback Detection:

Essa função permite que o switch detecte loops na rede. Quando um loop é detectado em uma porta ou VLAN o switch irá exibir um alerta na interface de gerenciamento e bloqueará a interface correspondente ou VLAN, conforme as suas configurações.

Configurações de Parâmetros Básicos

Vá até o menu **FUNÇÕES L2 > Switching > Porta > Configuração de Porta**, para carregar a seguinte página.



Siga os passos a seguir para configurar os parâmetros básicos:

1. Configure o tamanho do MTU e do pacote Jumbo para todas as portas e então clique em **Aplicar**.

Jumbo	Configure o tamanho do pacote Jumbo, por padrão é 1518. Geralmente, o tamanho do MTU (Maximum Transmission Unit) é 1518 bytes. Se você quer que o switch dê suporte para transmitir pacotes maiores que 1518 você pode configurar o tamanho do MTU manualmente aqui. Varia entre 1518 e 9216 bytes.

2. Selecione uma ou mais portas para configurar os parâmetros básicos, e então clique em **Aplicar**.

UNIT/LAGS	Clique em **UNIT** para configurar a porta física. Clique em **LAGS** para configurar as LAGS.
Tipo	Mostra o tipo da porta. **Cobre** indica uma porta Ethernet e **Fibra** indica uma porta SFP.
Descrição	Especifique uma descrição para a porta (é opcional).
Status	Se essa opção estiver como habilitado, a porta encaminhará pacotes normalmente. Caso contrário a porta não funcionará. Por padrão vem habilitado.

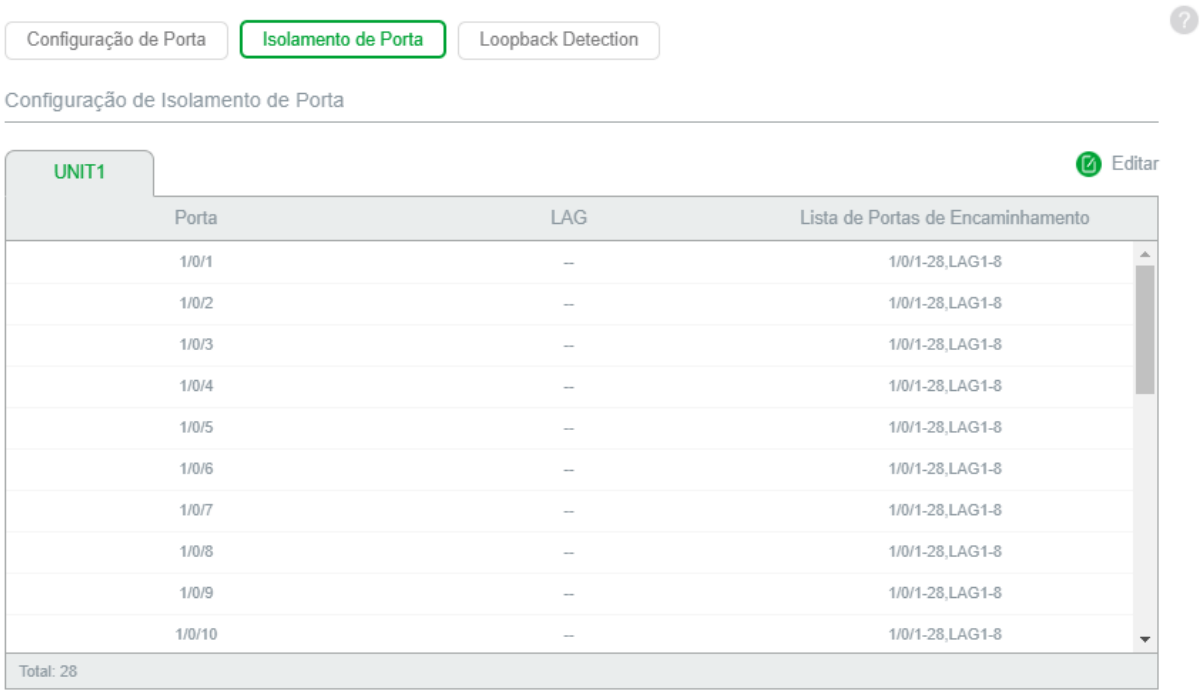
Velocidade	Selecione a velocidade de funcionamento apropriada para a porta. Vem configurado como **Auto** por padrão, o que indica que a porta irá negociar o modo de velocidade com os dispositivos vizinhos automaticamente. É recomendado a configuração automática quando as duas pontas do link negociam automaticamente
Duplex	Selecione o modo duplex apropriado para a porta. Existem as opções **Half**, **Full** e **Auto**. A configuração padrão é **Auto**. **Half:** A porta pode enviar e receber pacotes, porém em um sentido por vez. **Full:** A porta pode enviar e receber pacotes simultaneamente. **Auto:** A porta irá negociar automaticamente o modo Duplex.
Controle de Fluxo	Com essa opção habilitad0a, quando um dispositivo estiver sobrecarregado o switch enviará um pacote de pausa para o dispositivo de origem parar de enviar dados por um período específico para evitar perda de pacotes devido ao congestionamento de dados. Por padrão essa função vem desabilitada.

Recomendamos que você configure as portas em ambas as pontas do link com a mesma velocidade e modo duplex.

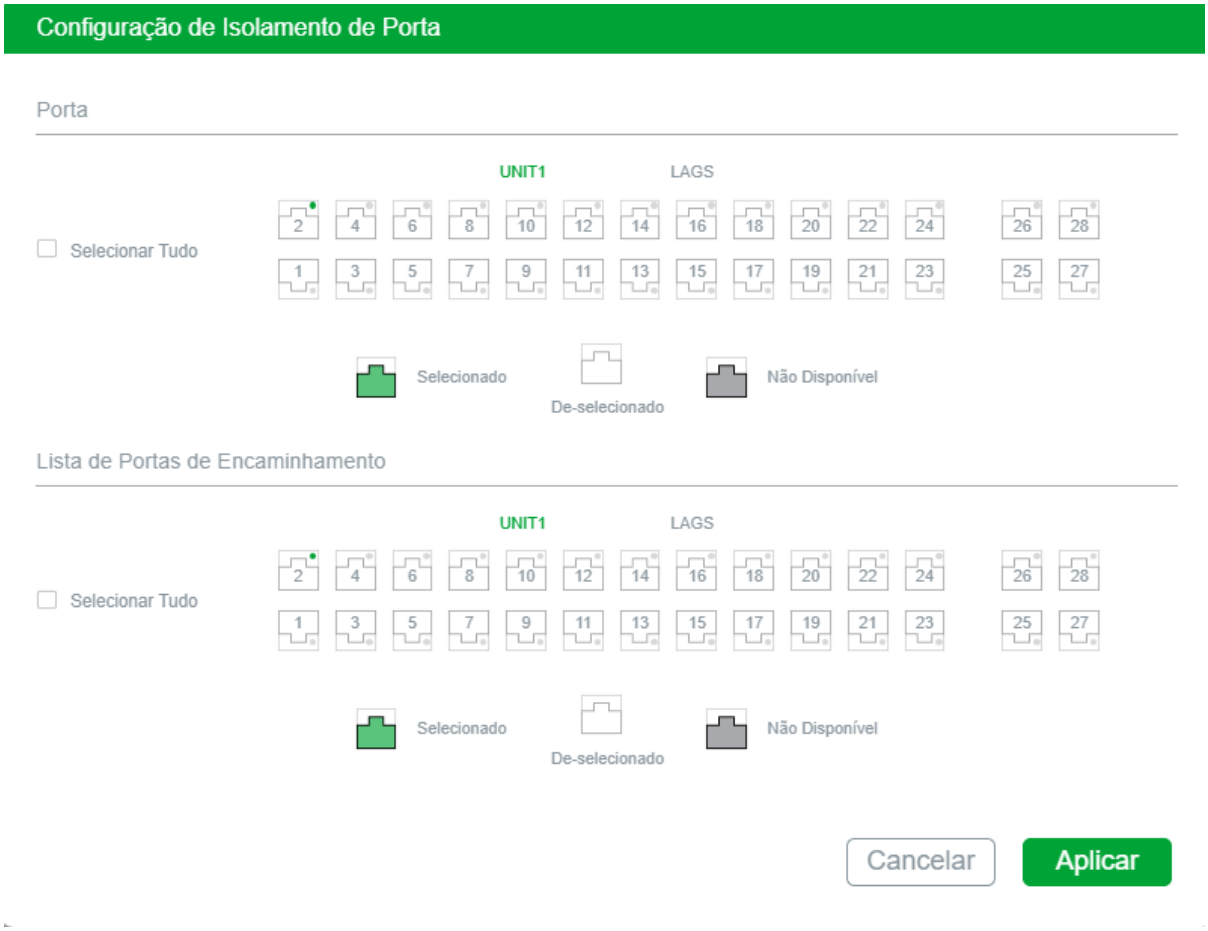
Configurações de Isolamento de Portas

Isolamento de portas é utilizado para limitar os dados transmitidos por uma determinada porta. A porta que estiver isolada só poderá enviar pacotes para portas especificadas na sua lista de Portas de Encaminhamento.

Vá até o menu **FUNÇÕES L2 > Switching > Porta > Isolamento de Porta**, para carregar a seguinte página.



A página à cima mostra a lista de portas isoladas. Clique no botão para configurar o isolamento de portas na próxima página.



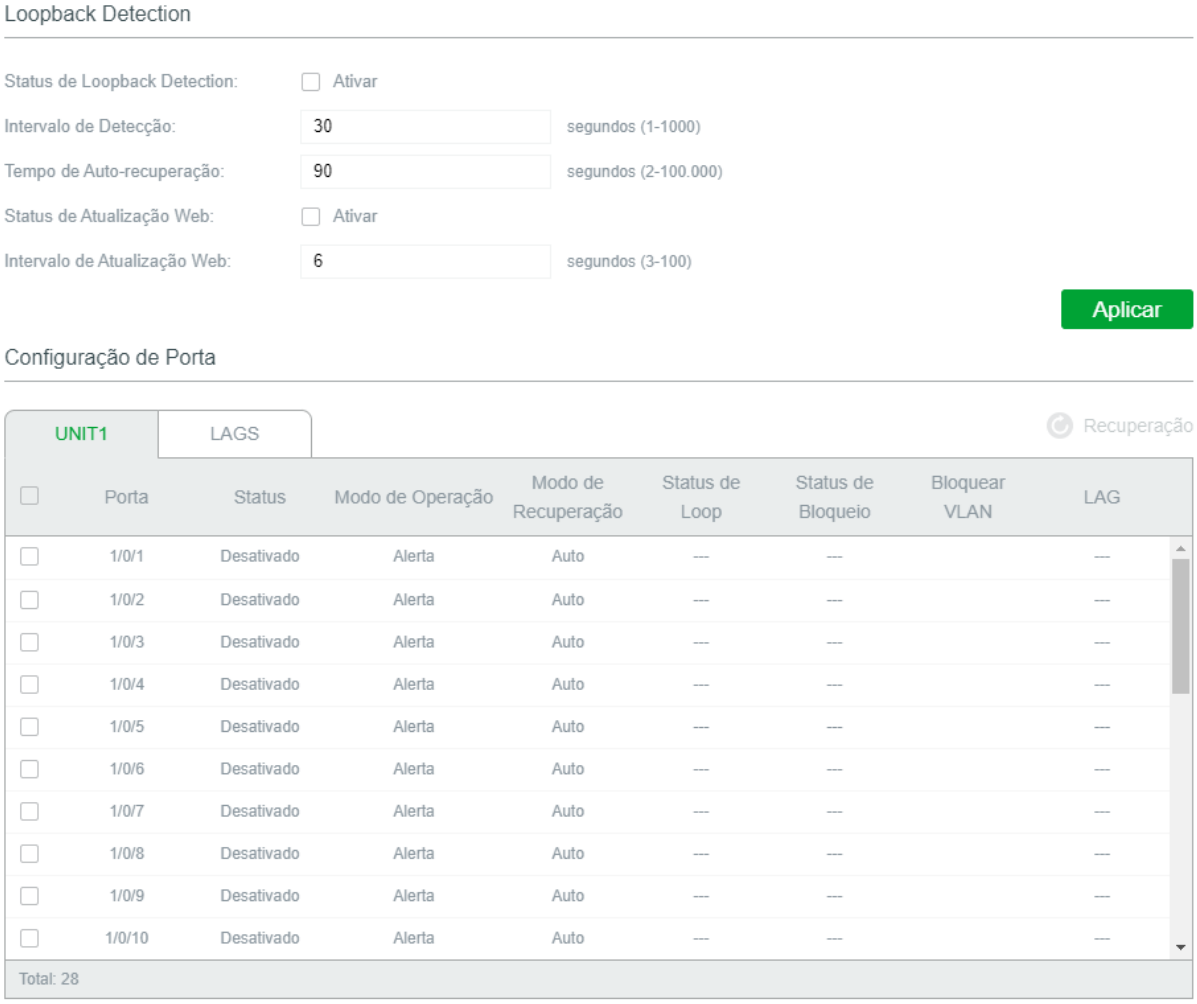
Siga os seguintes passos para configurar o Isolamento de Portas:

1. Na seção **Porta** selecione uma ou mais portas para serem isoladas.
2. Na seção **Lista de Portas de Encaminhamento** selecione as portas para encaminhamento ou LAGs com as quais as portas podem se comunicar. Você pode selecionar mais que uma opção.
3. Clique em **Aplicar**.

Configurações de Loopback Detection

Para evitar um Broadcast Storm recomendamos que você habilite o Storm Control antes de habilitar a Loopback Detection. Para instruções detalhadas sobre o Storm Control vá até **Configurado QoS**.

Vá até o menu **FUNÇÕES L2 > Switching > Porta > Loopback Detection**, para carregar a seguinte página.



Siga os seguintes passos para configurar o Loopback Detection:

1. Na seção **Loopback Detection** habilite a função de Loopback Detection e configure os parâmetros globais, e então clique em **Aplicar**.

Status de Loopback Detection	Habilita a Loopback Detection de forma global.
Intervalo de Detecção	Configura o intervalo do envio dos pacotes de Loopback Detection em segundos. Valores variam entre 1 e 1000 segundos, por padrão vem configurado como 30 segundos.
Tempo de auto recuperação	Configura o tempo de recuperação de forma global. Uma porta no modo de auto recuperação irá voltar ao estado normal automaticamente depois que o tempo de auto recuperação expirar. Varia entre 2 e 100000 segundos e por padrão é 90 segundos.
Status de atualização web	Com essa opção habilitada o Switch irá atualizar a página web periodicamente. Por padrão vem desabilitada.
Intervalo de atualização web	Se você habilitar o **Status de atualização web** configure o intervalo de tempo para a atualização entre 3 e 100 segundos, por padrão é 6.

2. Na seção **Configuração de Porta** selecione uma ou mais portas para configurar os parâmetros do Loopback Detection, e então clique em **Aplicar**.

Status	Habilita o Loopback Detection para as portas selecionadas.
Modo de operação	Selecione o modo de operação para quando um loopback é detectado: **Alerta:** O estado de Loop exibirá se há um loop detectado na porta correspondente. Essa é a configuração padrão. **Baseado em Porta:** Além de exibir alertas o switch irá bloquear a porta a qual o loop foi detectado. **Baseado em VLAN:** Se um loop for detectado em uma VLAN para aquela porta além de exibir alertas o Switch irá bloquear aquela VLAN. O tráfego para as outras VLAN ainda pode ser encaminhado pela porta.
Modo de Recuperação	Se você selecionar o modo de operação como Baseado em Porta ou VLAN você precisará configurar o tempo de recuperação para a porta bloqueada. **Auto:** A porta bloqueada irá se recuperar automaticamente para o estado normal depois que o tempo de recuperação expirar. É a configuração padrão. **Manual:** Você precisará liberar a porta bloqueada manualmente. Clique em **Recuperar** para liberar a porta selecionada.

3. Opcional – Visualizar as informações de Loopback Detection.

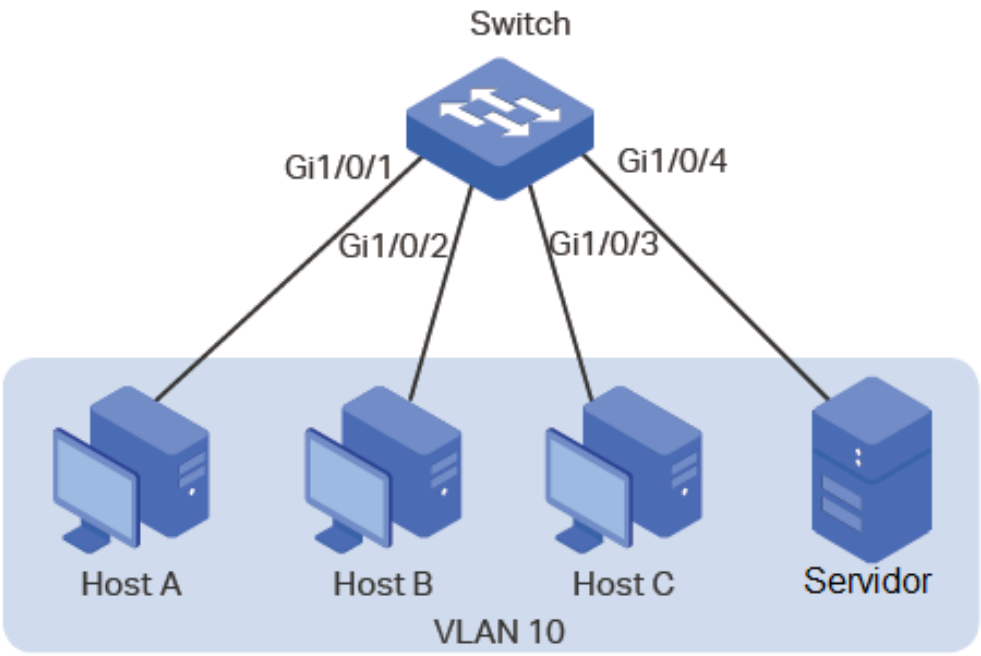
Status de Loop	Mostra se um loop é detectado na porta.
Status de Bloqueio	Mostra se a porta está bloqueada.
Bloquear VLAN	Mostra as VLANs bloqueadas.

Exemplos de Configuração

Exemplo de Isolamento de porta

Requisitos de Rede

Como mostrado a baixo, três hosts e um Servidor estão conectados ao Switch e todos pertencem à VLAN 10. Sem alterar as configurações de VLAN, o Host A não é permitido de se comunicar com outros equipamentos além do Servidor, mesmo se o endereço MAC ou endereço IP do Host A for alterado.



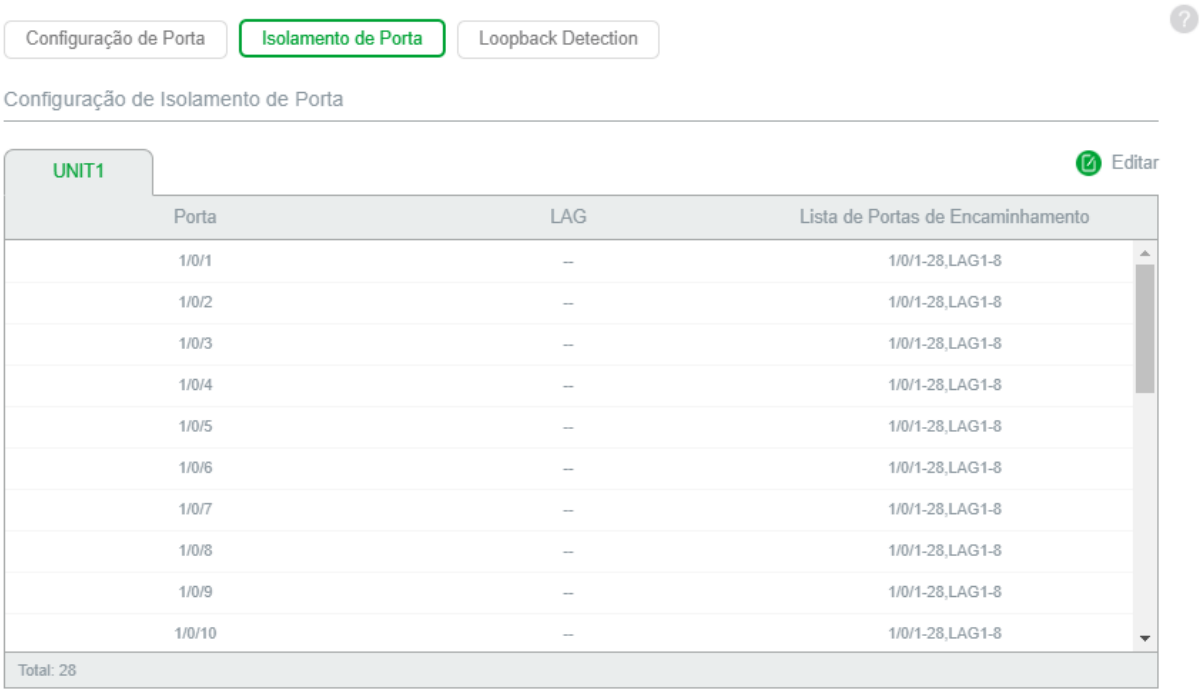
Configurando o Cenário

Você pode configurar um isolamento de portas para implementar o requisito. Configure a porta 1/0/4 como a única porta da lista de encaminhamento da porta 1/0/1, o que proibirá o Host A de encaminhar pacotes para os outros hosts.

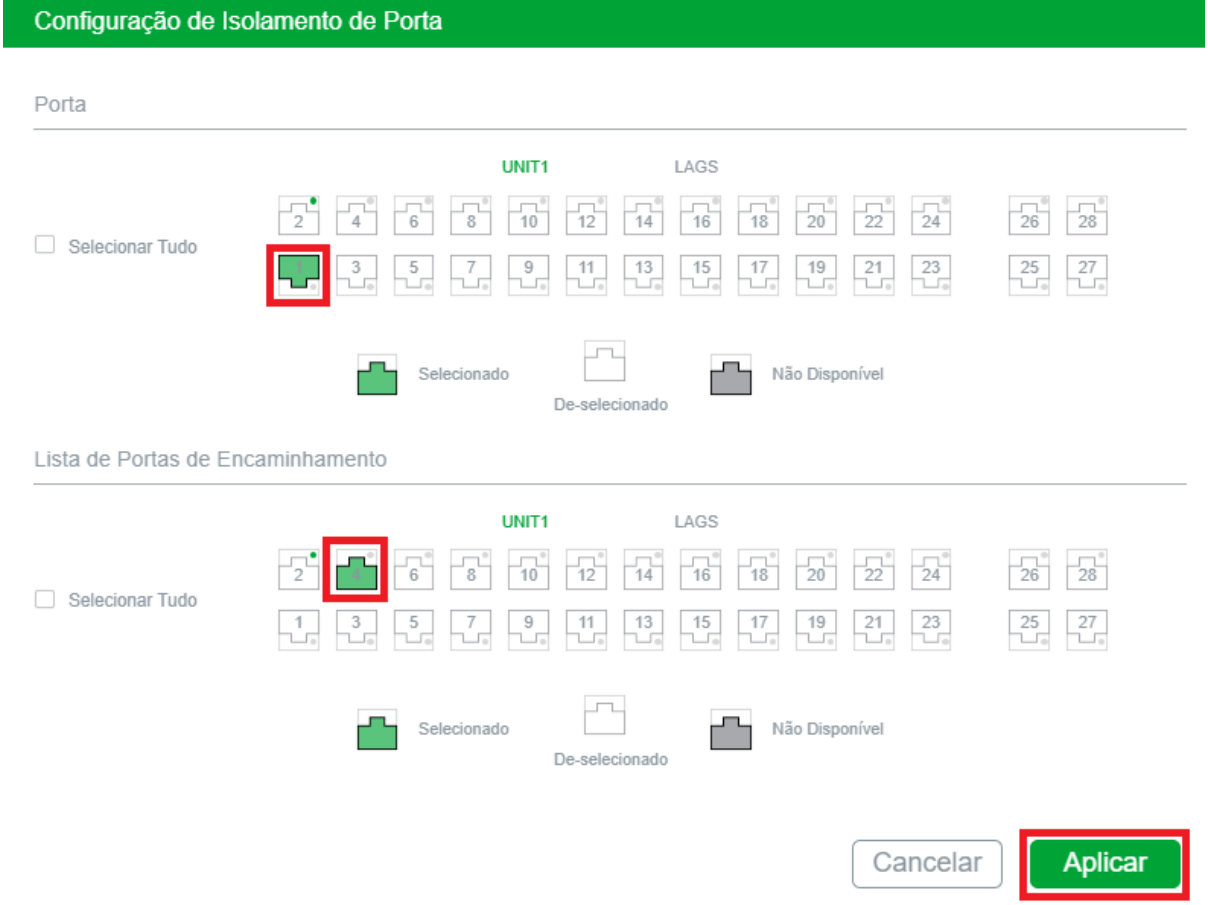
Uma vez que as comunicações são bidirecionais, se você quer que o Host A e o servidor se comuniquem normalmente, você também precisará adicionar a porta 1/0/1 como porta de encaminhamento para a porta 1/0/4.

Seguindo os passos à baixo você conseguirá realizar a configuração do requisito:

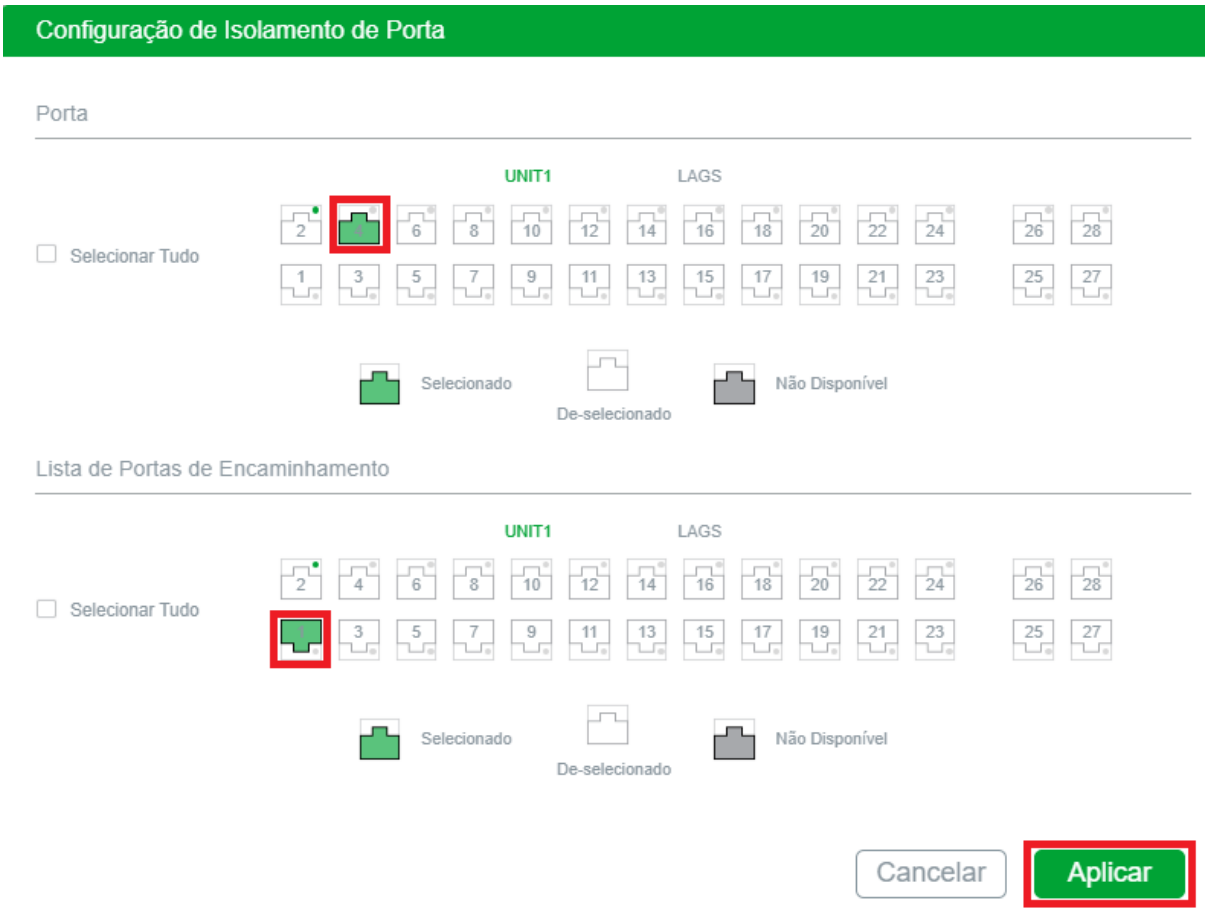
1. Vá até o menu **FUNÇÕES L2 > Switching > Porta > Isolamento de Porta**, para carregas a página a seguir, que exibirá a lista de portas isoladas.



2. Clique em **Editar** para carregar a próxima página. Selecione a porta 1/0/1 como porta a ser isolada e selecione a porta 1/0/4 como porta de encaminhamento. Clique em **Aplicar**.



3. Selecione a porta 1/0/4 como porta para ser isolada e seleciona a porta 1/0/1 como porta de encaminhamento para a porta. Clique em **Aplicar**.



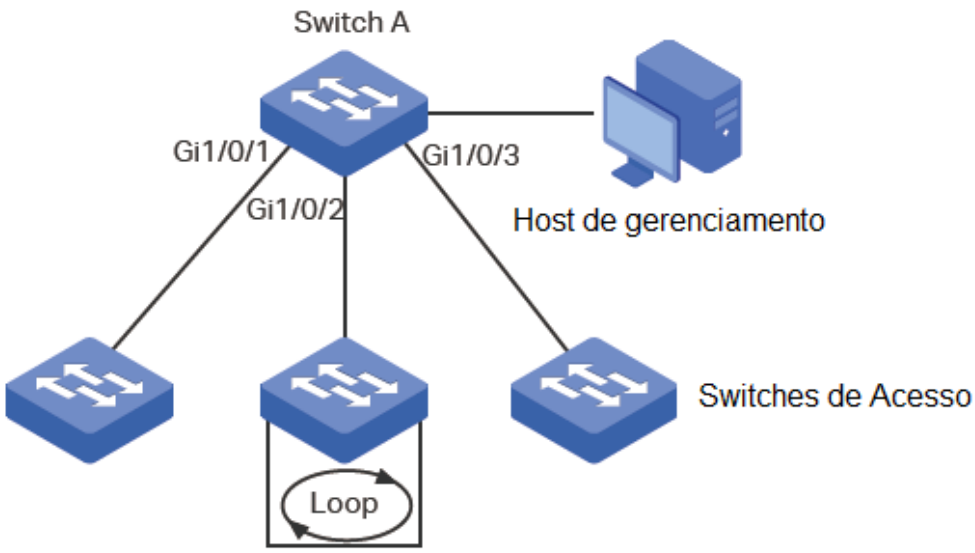
4. Clique em Salvar para salvar as configurações.

Exemplo de Detecção de Loopback

Requisitos de Rede

Como mostrado à baixo, o Switch A é um switch de convergência conectado à vários Switches de acesso. Loops podem facilmente ser causados por operações erradas nos switches de acesso, se houver um loop em um desses switches um Broadcast Storm irá ocorrer no Switch A ou até em toda a rede, criando trafego excessivo e degradando a performance da rede.

Para reduzir os impactos de um Broadcast Storm, os usuários precisam detectar loops na rede através do Switch A e bloquear temporariamente a porta na qual o loop foi detectado.



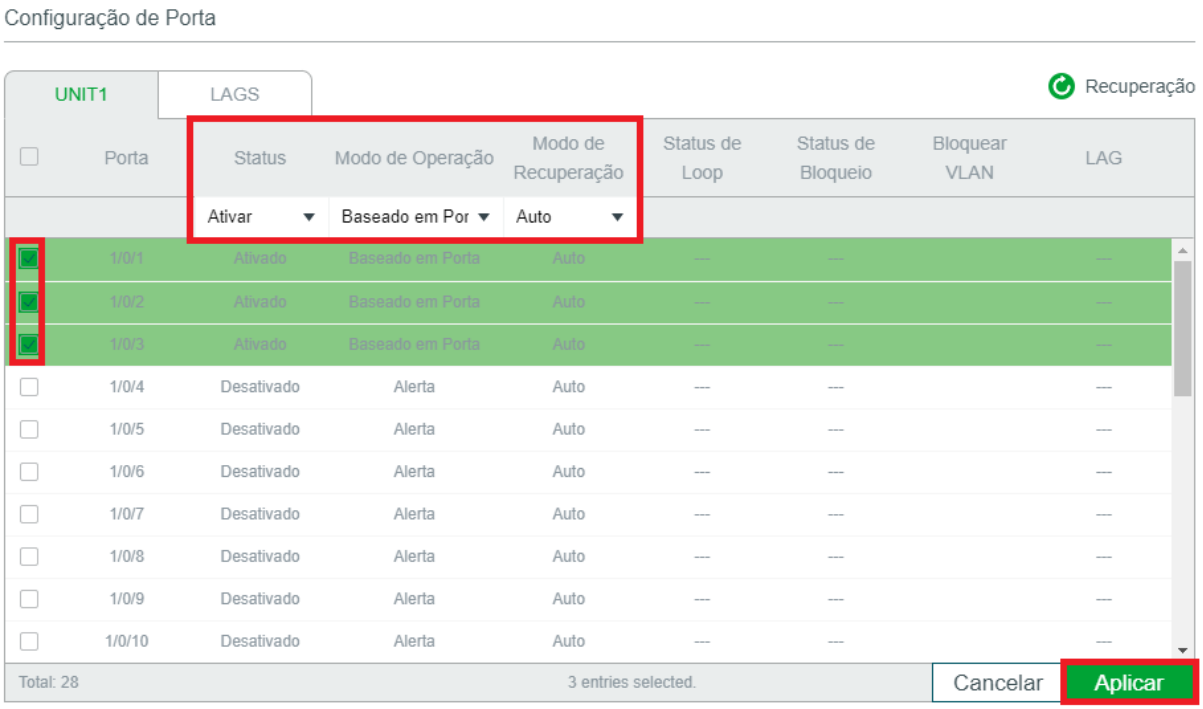
Configurando o Cenário

Habilite o Loopback Detection nas portas 1/0/1-3 e configure SNMP para receber notificação de Traps. Para instruções detalhadas sobre SNMP vá até **Configurando SNMP e RMON**. Aqui iremos mostrar como configurar a detecção Loopback e monitorar o resultado na interface de gerenciamento do Switch.

Siga os passos a seguir para configurar o cenário:

1. Vá para o menu **FUNÇÕES L2 > Switching > Portas > Loopback Detection** para carregar a página de configuração.
2. Na Seção **Loopback Detection** habilite a opção de Loopback Detection e o Status de Atualização Web globalmente. Mantenha os outros parâmetros com os valores padrões e clique em **Aplicar**.

3. Na seção **Configurações de Porta** habilite as portas 1/0/1-3, selecione o modo de operação como **Baseado em Porta** para que a porta seja bloqueada quando um loop for detectado, e mantenha o modo de recuperação como **Auto** para que a porta volte para o estado normal automaticamente após o tempo de recuperação. Clique em **Aplicar**.



4. Monitore o resultado da detecção na página à cima. O **Estado de Loop** e o **Estado de Bloqueio** são exibidos no lado direito das portas.

Apêndice: Configuração Padrão

As configurações padrões do Switch são listados nas tabelas abaixo.

Configurações das portas

Parâmetros	**Configurações Padrão**
Configurações das Portas	
Jumbo	1518 bytes
Tipo	Cobre (Para portas RJ45) Fibra (para portas SFP)
Estado	Habilitada
Velocidade	Auto (para portas RJ45) 1000M (para portas SFP)
Duplex	Auto (para portas RJ45) Full (para portas SFP)
Controle de Fluxo	Desabilitado

Loopback Detection	
Estado da Loopback Detection	Desabilitado
Intervalo de Detecção	30 segundos
Tempo de auto recuperação	90 segundos
Estado da atualização web	Desabilitado
Intervalo da atualização web	6 segundos
Estado da Porta	Desabilitado
Modo de operação	Alerta
Modo de recuperação	Auto

LAG

LAG

Visão Geral

Com a função LAG (Link Aggregation Group) você pode agregar múltiplas portas físicas em uma interface lógica aumentando a largura de banda disponível no link e providenciando portas de backup para aumentar a confiabilidade da conexão.

Funções Suportadas

Você pode configurar LAG de duas formas: LAG estático ou LACP (Link Aggregation Control Protocol).

LAG estático

As portas membro são adicionadas manualmente.

LACP

O Switch utiliza LACP para implementar dinamicamente a agregação e desagregação do Link através da troca de pacotes LACP com o dispositivo pareado. LACP aumenta e flexibiliza a configuração LAG.

Configuração LAG

Para completar a configuração LAG siga os passos a seguir:

1. Configure o Algoritmo global de Load-balance.
2. Configure um LAG estático ou um LACP.

Orientações para Configuração

- Garanta que as duas pontas do link estejam utilizando o mesmo modo LAG. Por exemplo, se a ponta local trabalha no modo LACP o seu par na outra ponta deve trabalhar em modo LACP também;
- Garanta que os dispositivos em ambas as pontas do Link agregado estejam utilizando o mesmo número de portas físicas com as mesmas configurações de velocidade, modo duplex, tamanho jumbo e mesmo modo de controle de fluxo;
- Uma porta não pode ser adicionada a mais que um LAG por vez;
- LACP não suporta links em modo Half-duplex;
- Um LAG estático suporta até oito portas. Todas as portas membro do LAG dividem a largura de banda de forma uniforme. Se um link ativo falhar os outros links ativos irão dividir a banda de forma uniforme;
- Uma LAG em modo LACP suporta múltiplas portas, porém no máximo oito delas podem trabalham simultaneamente, e as outras portas membro são portas de backup. Utilizando o protocolo LACP o Switch negocia os parâmetros e determina as portas funcionais. Quando uma porta funcional falha uma porta de backup com a maior prioridade toma o seu lugar;
- Para funções como IGMP Snooping, VLAN 802.1Q, MAC VLAN, protocolo VLAN, VLAN-VPN, GVRP, VLAN de voz, STP, QoS, DHCP Snooping e Controle de Fluxo as portas membro de um LAG seguem a configuração da LAG e não as suas próprias. As configurações da porta só terão efeitos quando essa deixar a LAG;
- Uma porta com Segurança de Porta, Espelhamento de Porta, filtro de endereço MAC ou 802.1X não podem ser adicionadas a um LAG, e as portas membro de uma LAG não podem ter essas funções adicionadas.

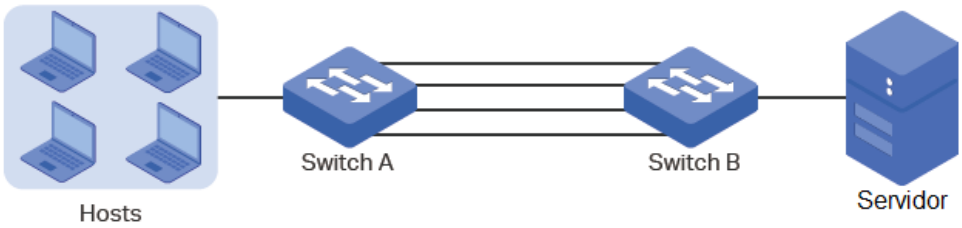
Configurando o Algoritmo de Balanceamento de carga

Vá até o menu **FUNÇÕES L2 > Switching > LAG > Tabela LAG**, para carregar a página a baixo.

Na seção **Configuração Global** selecione o modo do Algoritmo de balanceamento de carga (algoritmo Hash), e então clique em **Aplicar**.

Algoritmo Hash	Selecione o modo do Algoritmo Hash no qual o switch poderá escolher a porta para encaminhar os pacotes recebidos. Dessa forma diferentes fluxos de dados serão encaminhados em diferentes links físicos para implementar o balanceamento da carga. Existem seis opções: Geralmente, o tamanho do MTU (Maximum Transmission Unit) é 1518 bytes. Se você quer que o switch dê suporte para transmitir pacotes maiores que 1518 você pode configurar o tamanho do MTU manualmente aqui. Varia entre 1518 e 9216 bytes. **SRC MAC:** A computação dos pacotes será baseada no endereço MAC de origem dos pacotes; **DST MAC:** A computação dos pacotes será baseada no endereço MAC de destino dos pacotes; **SRC MAC+DST MAC:** A computação dos pacotes será baseada nos endereços MAC de origem e destino dos pacotes; **SRC IP:** A computação dos pacotes será baseada no endereço IP de origem dos pacotes; **DST IP:** A computação dos pacotes será baseada no endereço IP de destino dos pacotes; **SRC IP+DST IP:** A computação dos pacotes será baseada nos endereços IP de origem e destino dos pacotes;

O algoritmo de balanceamento de carga só é efetivo para trafego de saída. Se o stream de dados não é bem compartilhado com cada link, você pode alterar o algoritmo da interface de saída.
Escolha o algoritmo de balanceamento de carga adequado para evitar trafego de dados em um único link físico. Por exemplo, Switch A recebe pacotes de vários hosts a encaminha eles para o Servidor com endereço MAC fixo, você pode configurar o algoritmo como “SRC MAC” para permitir que Switch A determine a porta de encaminhamento baseado no endereço MAC de origem os pacotes recebidos.



Configurando LAG estático ou LACP

Para uma porta você pode escolher somente um modo LAG: estático ou LACP. Garanta que ambas as portas do LAG estejam no mesmo modo.

Configurando um LAG estático

Vá até o menu **FUNÇÕES L2 > Switching > LAG > LAG estático**, para carregar a página a baixo.

Siga os seguintes passo para configurar um LAG estático:

1. Selecione um LAG para configuração.

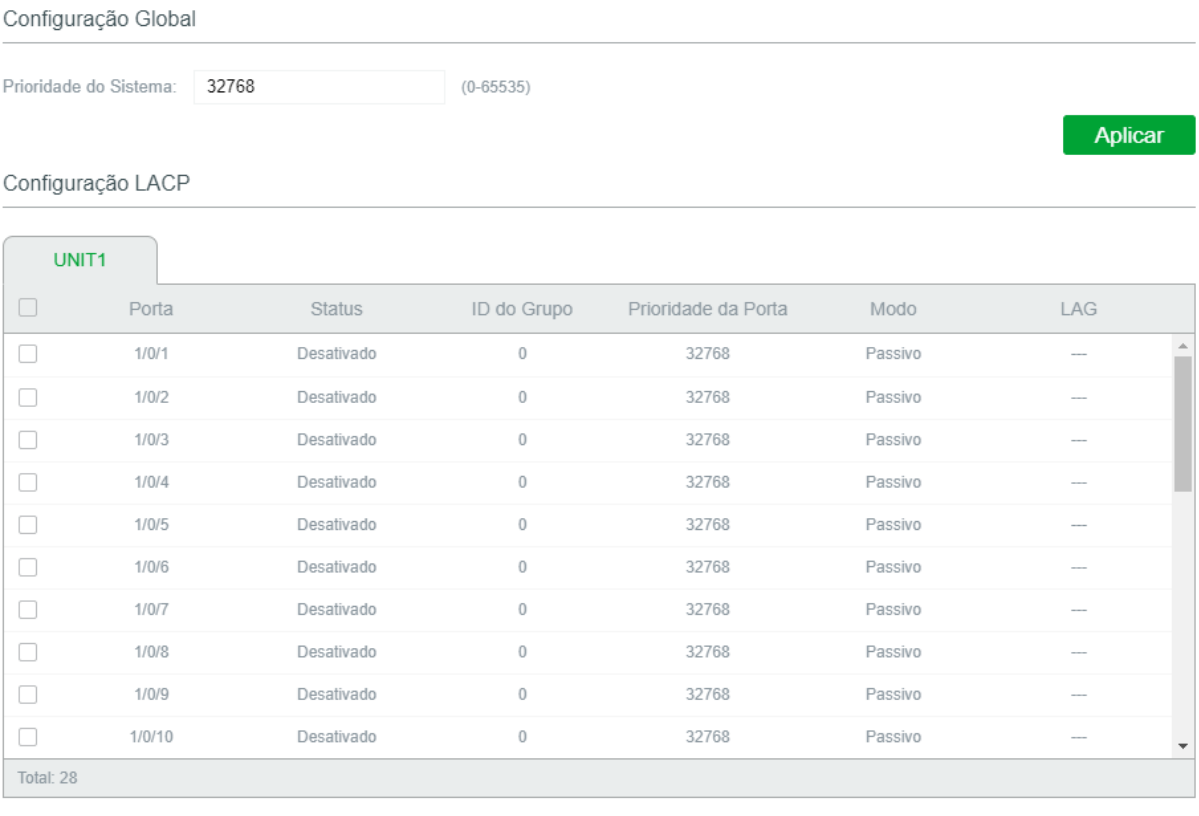
ID do grupo	Selecione um LAG estático para configuração.
Descrição	Mostra o modo do LAG.

2. Selecione as portas membro para a LAG. Você pode escolher até 8 portas.
3. Clique em **Aplicar**.

> Limpar todas as portas membro irá excluir a LAG.

Configurando LACP

Vá até o meu **FUNÇÕES L2 > Switching > LAG > Configuração LACP**, para carregar a próxima página.



Siga os seguintes passo para configurar o LACP:

1. Especifique a prioridade do sistema para o Switch e clique em **Aplicar**.

Prioridade do Sistema	Especifica a prioridade do sistema para o Switch. Valores menores significam maiores prioridades. Para manter ativa as portas em ambas as pontas você pode indicar a prioridade do sistema de um dispositivo maior que a do outro. O dispositivo com maior prioridade irá determinar suas portas ativas e o outro dispositivo poderá selecionar suas portas de acordo com o resultado da seleção do dispositivo com maior prioridade. E ambas as pontas do link tiverem a mesma prioridade do sistema o dispositivo com menor endereço MAC terá maior prioridade.

2. Selecione as portas membro para a LAG e configure os parâmetros relativos. Clique em **Aplicar**.

ID do grupo	Especifique uma ID para o grupo do LAG. Note que esse parâmetro não pode ser configurado em LAGs estáticos.
Prioridade da Porta (0-65535)	Especifica a prioridade da Porta. Um valor menor representa uma prioridade maior. As portas com as maiores prioridades no LAG serão selecionadas para serem as portas funcionais para encaminhamento de dados, podem ser no máximo 8 portas. Se duas portas tem o mesmo valor de prioridade a porta com o menor número físico terá maior prioridade.
Modo	Seleciona o modo LACP para a porta. Dentro do LACP, o Switch utiliza LACPDU (Link Aggregation Control Protocol Data Unit) para negociar os parâmetros com o seu par. Dessa forma as duas pontas selecionam suas portas ativas e formam o link agregado. O modo LACP determina qual porta terá iniciativa de enviar o LACPDU. Existem dois modos: **Passivo:** A porta não enviará o LACPDU antes de receber um LACPDU da outra ponta. **Ativo:** A porta terá a iniciativa de enviar o LACPDU.
Status	Habilita a função LACP para a porta. Por padrão vem desabilitada.

Limpar todas as portas membro irá excluir a LAG.

Exemplo de configuração

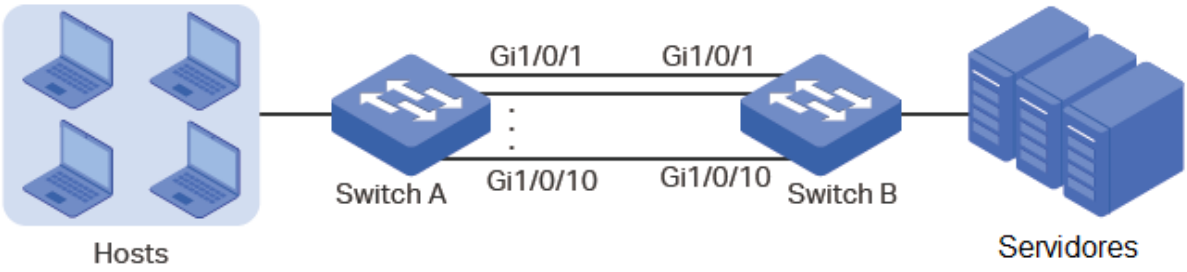
Requisitos de Rede

Como mostrado abaixo, os hosts e os servidores estão conectados através dos Switches A e B, e uma alta densidade de trafego é transmitida entre os dois Switches. Para alcançar altas velocidades e rentabilidade de transmissão de dados, os usuários precisam aumentar a largura de banda e a redundância do link entre os dois Switches.

Configurando o Cenário

A função LAG pode unir múltiplas portas físicas em uma interface lógica para aumentar a banda disponível e melhorar a rentabilidade do link. Nesse caso nós iremos utilizar o LACP como exemplo.

Como mostrado abaixo você pode agrupar até 8 portas físicas em uma agregação lógica para transmitir dados entre Switches, e respectivamente conectar as portas dos grupos. Em adição outros dois links podem ser adicionados como links de backup. Para evitar gargalo de tráfego entre o servidor e o switch B é possível configurar um LAG entre eles para aumentar a largura de banda. Aqui introduziremos a configuração LAG entre dois Switches.



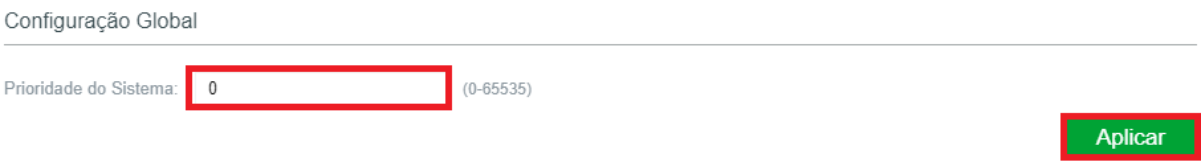
Uma visão geral da configuração será a seguinte:

1. Considerando que há múltiplos dispositivos nas duas pontas configure o algoritmo de balanceamento de carga como “SRC MAC+DST MAC”;
2. Especifique a prioridade do sistema para os Switches. Aqui nós escolheremos o Switch A como dispositivo dominante e especificaremos a maior prioridade nele;
3. Adicione as portas 1/0/1-10 no LAG e configure seu modo como LACP;
4. Especifique uma prioridade menor para as portas 1/0/9-10 para apontá-las como portas de backup. Quando qualquer porta entre 1/0/1-8 cair, uma das portas de backup automaticamente se habilitará para transmitir pacotes.

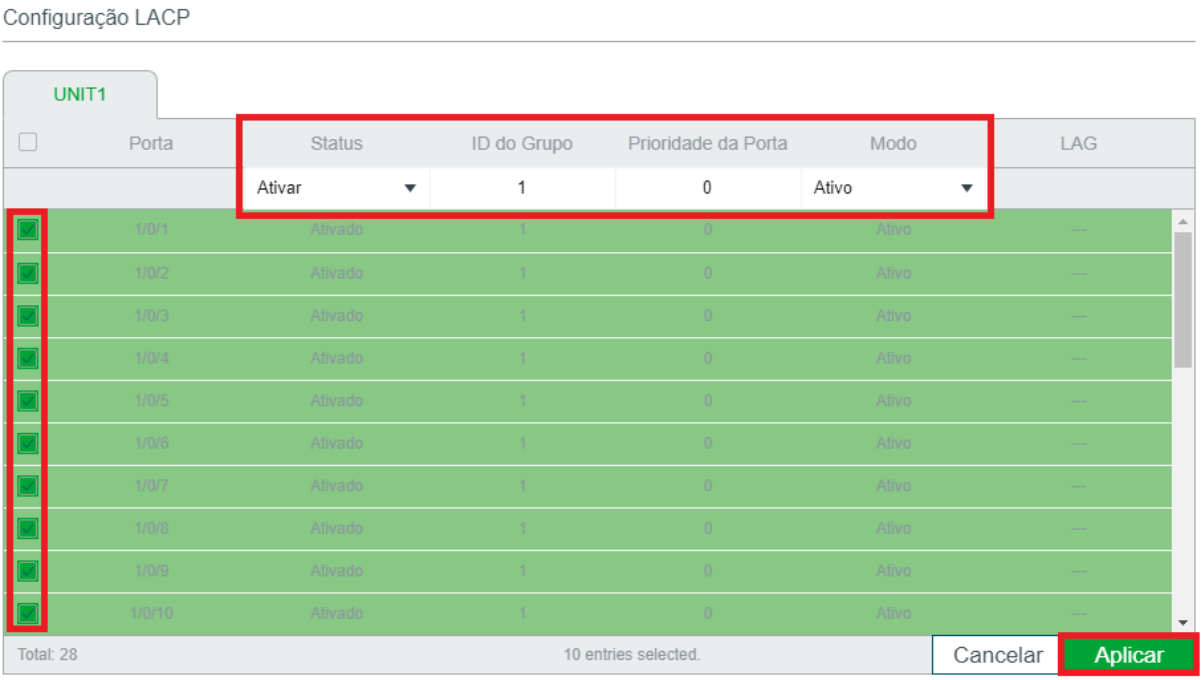
As configurações do Switch A e Switch B são similares. Para as instruções tomaremos o Switch A como exemplo. Para configuração do cenário descrito siga os passos a baixo:

1. Vá até o menu **FUNÇÕES L2 > Switching > LAG > Tabela LAG** para carregar a página a seguir. Selecione o Algoritmo Hash como “SRC MAC+DST MAC”.

2. Vá até o menu **FUNÇÕES L2 > Switching > LAG > Configurações LACP** para carregar a página abaixo. Na seção Configuração Global especifique a prioridade do Switch A como 0 e clique em **Aplicar**. Lembre-se de configurar a prioridade do sistema para o Switch B com um número maior que 0.



3. Na seção **Tabela LACP** selecione as portas 1/0/1-10 e configure respectivamente seus estados, ID de grupo, Prioridade de porta e modo para cada porta como segue na imagem.



4. Clique em Salvar para salvar as configurações.

Apêndice: Configuração Padrão

As configurações padrões estão listadas da tabela a seguir.

Configurações padrão do LAG

Parâmetros	Configurações Padrão
Tabela LAG	
Algoritmo Hash	SRC MAC+DST MAC
Configuração LACP	
Prioridade do Sistema	32768
Chave Administradora	0
Prioridade da Porta	32768
Modo	Passivo

Estado	Desabilitado

Tabela de endereço MAC

Tabela de endereço MAC

Visão Geral

A tabela de endereço MAC contém as informações de endereço que o switch utiliza para enviar os pacotes. Como mostrado abaixo, a tabela lista um mapa de entradas de endereços MAC, ID de VLANs e portas. Essas entradas podem ser adicionadas manualmente ou podem ser aprendidas automaticamente pelo switch. Baseada na tabela de mapeamento Endereço MAC para porta o switch pode encaminhar pacotes somente para as portas associadas.

Endereço MAC	ID VLAN	Port	Tipo	Estado de aging
00:00:00:00:00:01	1	1	Dinâmica	Aging
00:00:00:00:00:02	1	Prioridade do Sistema	Estática	No-aging

.....

Funções Suportadas

A tabela de endereços do switch contém endereços dinâmicos, endereços estáticos e endereços filtrados. Você pode adicionar ou remover essas entradas conforme a sua necessidade.

Configuração de Endereços

- Endereço dinâmico

  Endereços dinâmicos são endereços aprendidos automaticamente pelo switch, os quais o switch regularmente envelhece e descarta quando não estão em uso. Ou seja, o switch remove as entradas de endereços MAC relacionadas à um dispositivo de rede que não esteja recebendo pacotes de outros dispositivos dentro de um aging time. E você pode especificar este tempo caso necessário.

- Endereço estático

  Endereços estáticos são adicionados manualmente na tabela de endereços e não “envelhecem”. São utilizados para conexões fixas, por exemplo, para servidores frequentemente acessados, você pode adicionar o endereço MAC desse como uma entrada estática para aumentar a eficiência de encaminhamento do switch.

- Endereços filtrados

  Endereços filtrados são adicionados manualmente e determinam que pacotes com um endereço de origem ou destino específico serão descartados pelo Switch.

Configurações de endereço MAC

Com a tabela de endereços MAC você pode:

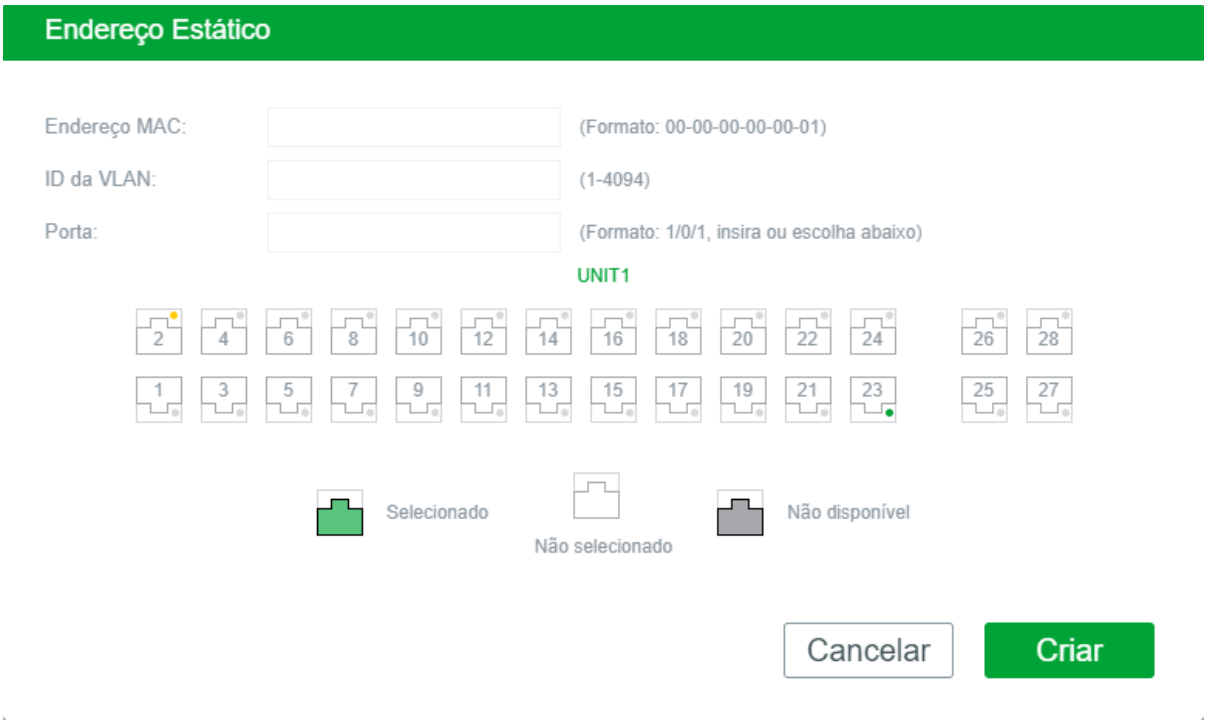
- Adicionar uma entrada de MAC estático;
- Alterar o aging time para os endereços MAC;
- Adicionar entradas de filtro para endereços MAC;
- Visualizar as entradas da tabela de endereços.

Adicionando uma entrada de endereço MAC estático

Você pode adicionar uma entrada de endereço MAC estático manualmente especificando o endereço MAC desejado ou vinculando uma entrada de endereço dinâmico.

- **Adicionando endereços MAC manualmente**

  Vá até o menu **FUNÇÕES L2 > Switching > endereço MAC > Endereço Estático** e clique em Adicionar para carregar a seguinte página:



  Siga os seguintes passos para adicionar uma entrada de endereço MAC estático:

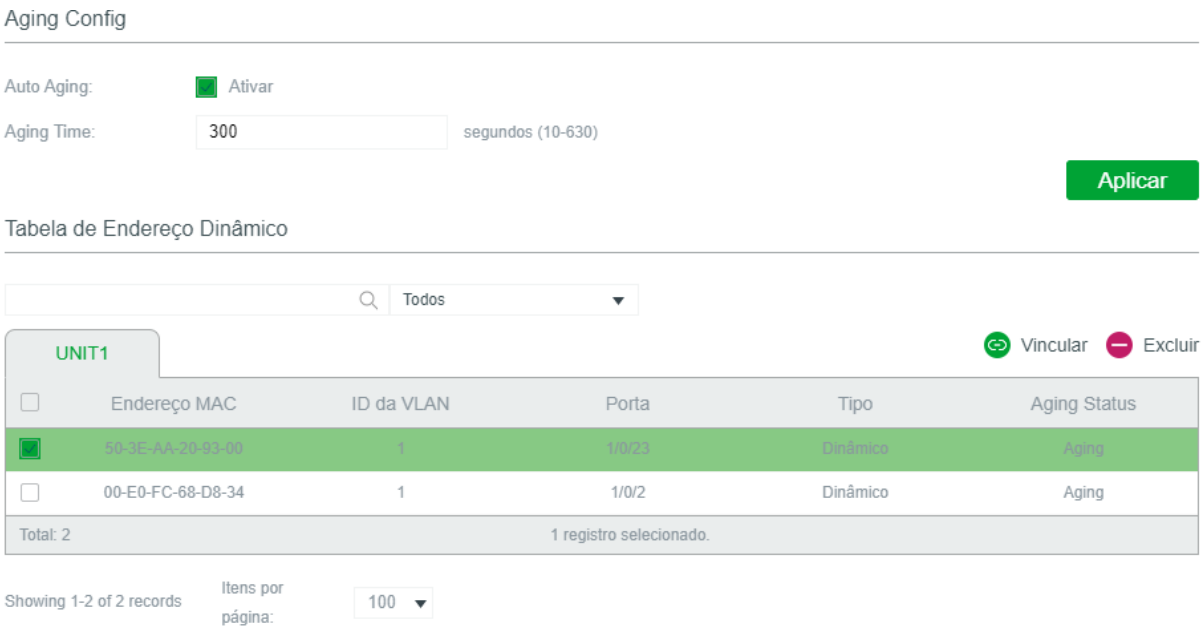
1. Aponte o endereço MAC e o ID da VLAN, depois selecione a porta que você quer vincular à entrada.

Endereço MAC	Entre com o endereço MAC estático para ser adicionado.
VLAN ID	Especifique uma VLAN existente na qual pacotes com o endereço MAC especificado serão recebidos.
Porta	Especifique uma porta na qual os pacotes com o endereço MAC especificado serão encaminhados. A porta deve pertencer à VLAN especificada. Depois que você criar uma entrada de endereço MAC estático, se o número da porta correspondente ao endereço MAC não estiver correto, ou se a porta ou dispositivo conectados forem alterados, o switch não será capaz de encaminhar os pacotes corretamente. Será necessário resetar a entrada de endereço estático de forma adequada.

2. Clique em **Criar**

- **Adicionando endereços MAC manualmente**

  Vá até o menu **FUNÇÕES L2 > Switching > endereço MAC > Endereço Dinâmico** para carregar a seguinte página:



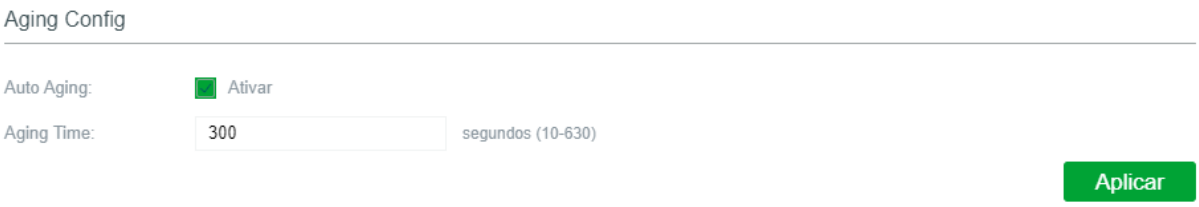
  Siga os seguintes passos para vincular uma entrada de endereço dinâmico:

1. Na seção Tabela de Endereço Dinâmico, selecione a entrada de endereço MAC desejada.
2. Clique em Vincular , e então a entrada selecionada se tornará uma entrada de endereço MAC estático.

> Na mesma VLAN, uma vez que um endereço é configurado como estático o mesmo não poderá ser configurando como endereço Filtrado e vice-versa.
> Endereços de Multicast ou Broadcast não podem ser adicionados como endereços estáticos.
> Portas pertencentes à LAGs (Link Aggregation Group) não são suportadas para configuração de endereços MAC estáticos.

Modificando o Aging Time de uma entrada de endereço Dinâmico

Vá até o menu **FUNÇÕES L2 > Switching > endereço MAC > Endereço Dinâmico** para carregar a seguinte página:



Siga os seguintes passos para modificar o Aging Time de uma entrada de endereço dinâmico:

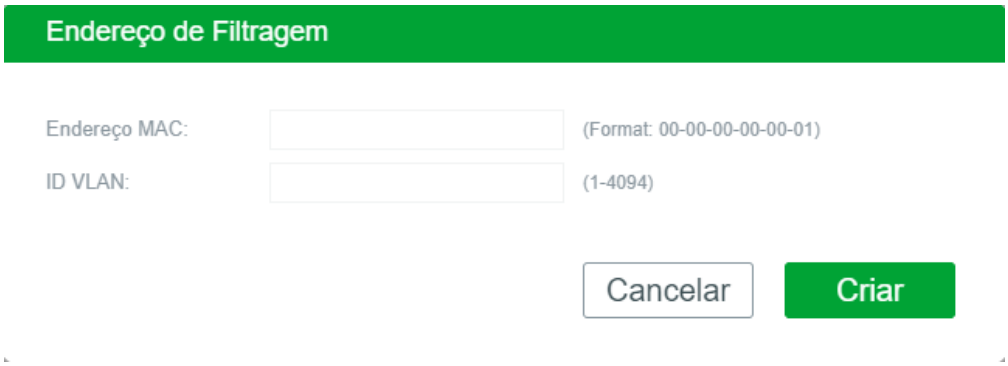
1. Na seção de **Aging Config** habilite o Auto Aging e entre com a duração de tempo desejado.

Auto Aging	Habilitando o Auto Aging o switch irá atualização automaticamente a tabela de endereços dinâmicos com o mecanismo de aging. Por padrão essa opção é habilitada.
Aging Time	Determina a duração do tempo que uma entrada dinâmica permanecerá na tabela de endereços MAC após ser utilizada ou atualizada. Os valores validos variam entre 10 e 630 segundos, por padrão vem configurada como 300. Um aging time curto é aplicável para redes com topologias que mudam frequentemente, e um aging time longo é aplicável às redes estáveis. Recomendamos que você mantenha o valor padrão caso não tenha certeza de quais configurações se adequem ao seu caso.

2. Clique em **Aplicar**.

Adicionando entrada de Filtro de endereço MAC

Vá até o menu **FUNÇÕES L2 > Switching > endereço MAC > Endereço de Filtragem** e clique em Adicionar para carregar a seguinte página:



Siga os seguintes passos para adicionar uma entrada de filtragem MAC:

1. Entre com o endereço MAC e a ID da VLAN

Endereço MAC	Especifique o endereço MAC que será usado pelo switch para filtrar os pacotes recebidos.
VLAN ID	Especifique uma VLAN existente na qual os pacotes com o endereço MAC especificado serão descartados.

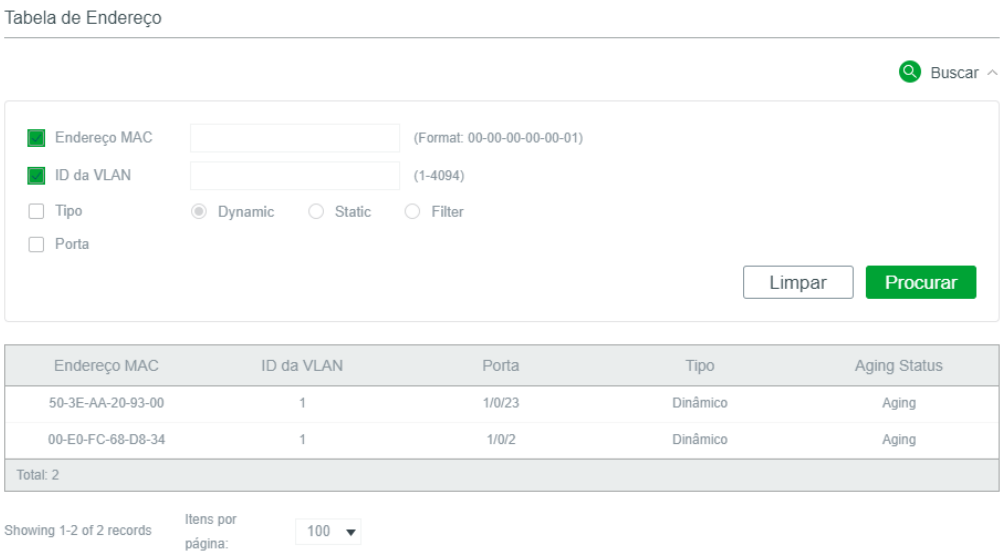
2. Clique em **Criar**

> Na mesma VLAN, uma vez que um endereço MAC é configurado como endereço de filtragem o mesmo não pode ser configurado como endereço estático e vice-versa.
> Endereços Multicast ou Broadcast não podem ser configurados como endereço de Filtragem.

Visualizando as Entradas na Tabela de Endereços

Você pode visualizar as entradas na tabela de endereço MAC para verificar suas operações e informação dos endereços.

Vá até o menu **FUNÇÕES L2 > Switching > endereço MAC > Tabela de Endereços** e clique em Buscar para carregar a seguinte página:



Apêndice: Configuração Padrão

As configurações padrões estão listadas da tabela a seguir.

Entradas na Tabela de Endereços MAC

Parâmetros	Configurações Padrão
Entradas de Endereço Estático	Nenhum
Entradas de Endereço Dinâmico	Autoaprendizagem
Entradas de Endereço de Filtragem	Nenhum

Configurações Padrões Tabela de Endereços Dinâmicos

Parâmetros	Configurações Padrão
Auto Aging	Habilitado
Aging Time	300 segundos

VLAN 802.1Q

Visão Geral

VLAN (Virtual Local Área Network) é uma técnica de rede que resolve os problemas de broadcast em redes locais. Ela é aplicada normalmente nas seguintes ocasiões:

- Para restringir o domínio de broadcast: A técnica de VLAN divide uma rede local grande em várias VLANs, e todo o tráfego de VLAN permanece dentro da sua VLAN. Ela reduz a tráfego de broadcast da rede de camada 2 para toda a rede.
- Para melhorar a segurança da rede: Dispositivos de diferentes VLANs não podem alcançar a camada 2 de comunicação, e assim, os membros e dispositivos do grupo podem se isolar para melhorar a segurança.
- Para facilitar o gerenciamento: Agrupa dispositivos VLANs de forma logica em vez de forma física, por isso os dispositivos na mesma VLAN não precisam estar localizados no mesmo lugar. Facilitando a gestão dos dispositivos no mesmo grupo de trabalho, mas localizados em lugares diferentes.

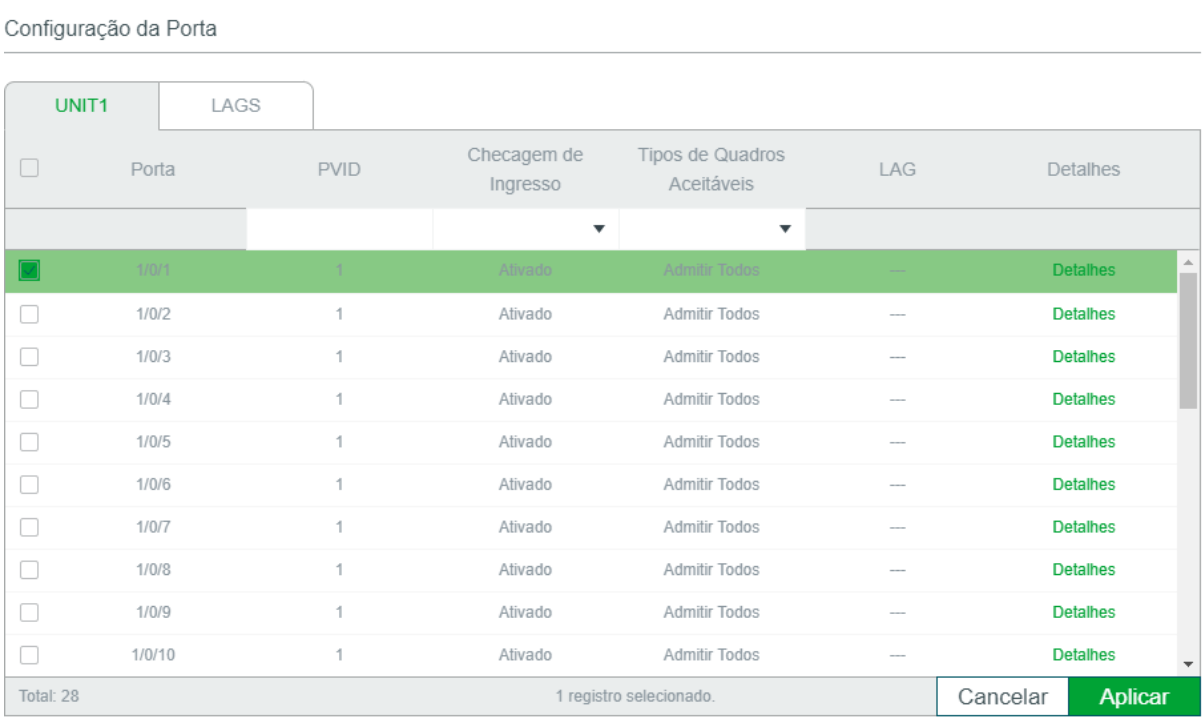
Configuração da VLAN 802.1Q

Para completar a configuração VLAN 802.1Q, siga estes passos:

1. Configure os parâmetros da porta;
2. Configure a VLAN, incluindo a criação de uma VLAN, e adicionando a porta configurada à VLAN.

Configurar o PVID da porta

Escolha o menu **FUNÇÕES L2> VLAN> VLAN 802.1Q> Configuração de porta** para carregar a próxima página.

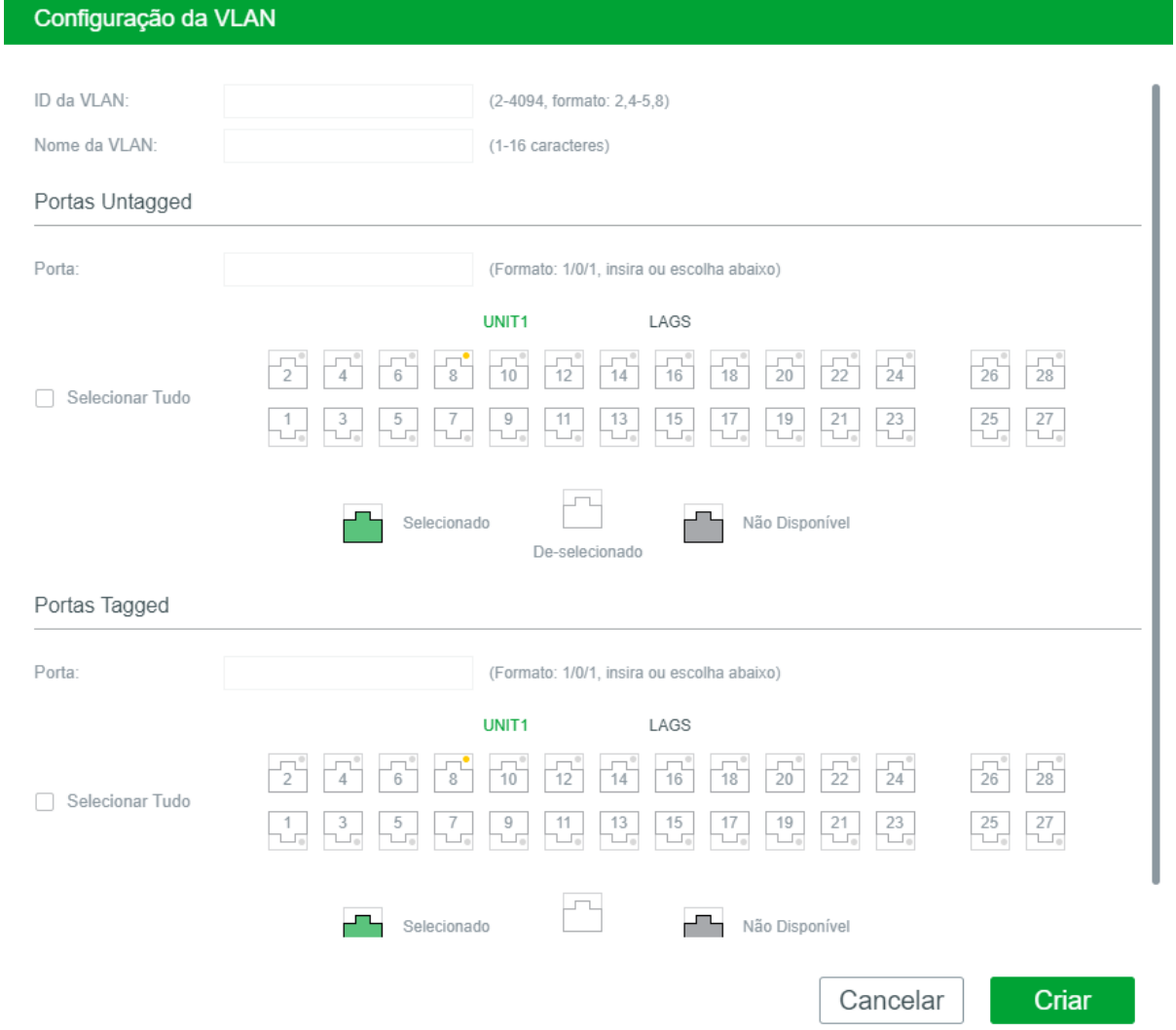


Selecione uma porta, e configure os parâmetros. Clique em **Aplicar**.

PVID	Define o ID VLAN padrão da porta. Os valores válidos são de 1 a 4094. É usada principalmente nas seguintes formas: Quando a porta recebe um pacote não identificado, o switch insere uma tag VLAN para o pacote baseado no PVID.
Checagem de Ingresso	Ativar ou desativar a verificação de Ingresso. Com esta função ativada, a porta aceitará o pacote do qual o VLAN ID está na lista de VLAN da porta e descarte as outras. Com esta função desabilitada, a porta irá encaminhar o pacote diretamente.
Tipos de quadros aceitáveis	Selecionar o tipo de quadro aceitável para a porta, e qual a porta vai executar esta operação antes da Verificação de ingresso. **Admita Todos:** A porta irá aceitar tanto os pacotes tagged quanto os untagged. **Tagged Only:** A porta irá aceitar apenas os pacotes tagged.
LAG	Exibe o LAG (Link Aggregation Group) do qual a porta pertence.
Detalhes	Clique no botão Detalhes para ver o VLANs ao qual a porta pertence.

Configurando a VLAN

Escolha o menu **FUNÇÕES L2> VLAN> VLAN 802.1Q> Configuração VLAN** e clique em Adicionar para carregar a próxima página.



Siga estes passos para configurar a VLAN:

1. Insira um ID de VLAN, e uma descrição para identificação da VLAN criada.

VLAN ID	Introduzir uma VLAN ID de identificação com os valores entre 2 e 4094.
Nome da VLAN	Dê uma descrição para identificar a VLAN com até 16 caracteres.

2. Selecione as respectivas portas untagged e as portas tagged para adicionar a VLAN a ser criada baseada na topologia da rede.

Portas Untagged	As portas selecionadas que vão encaminhar pacotes não marcados na VLAN alvo.
Portas Tagged	As portas selecionadas que vão encaminhar pacotes marcados na VLAN alvo.

3. Clique em **Aplicar**.

Exemplo de configuração

Requisitos de Rede

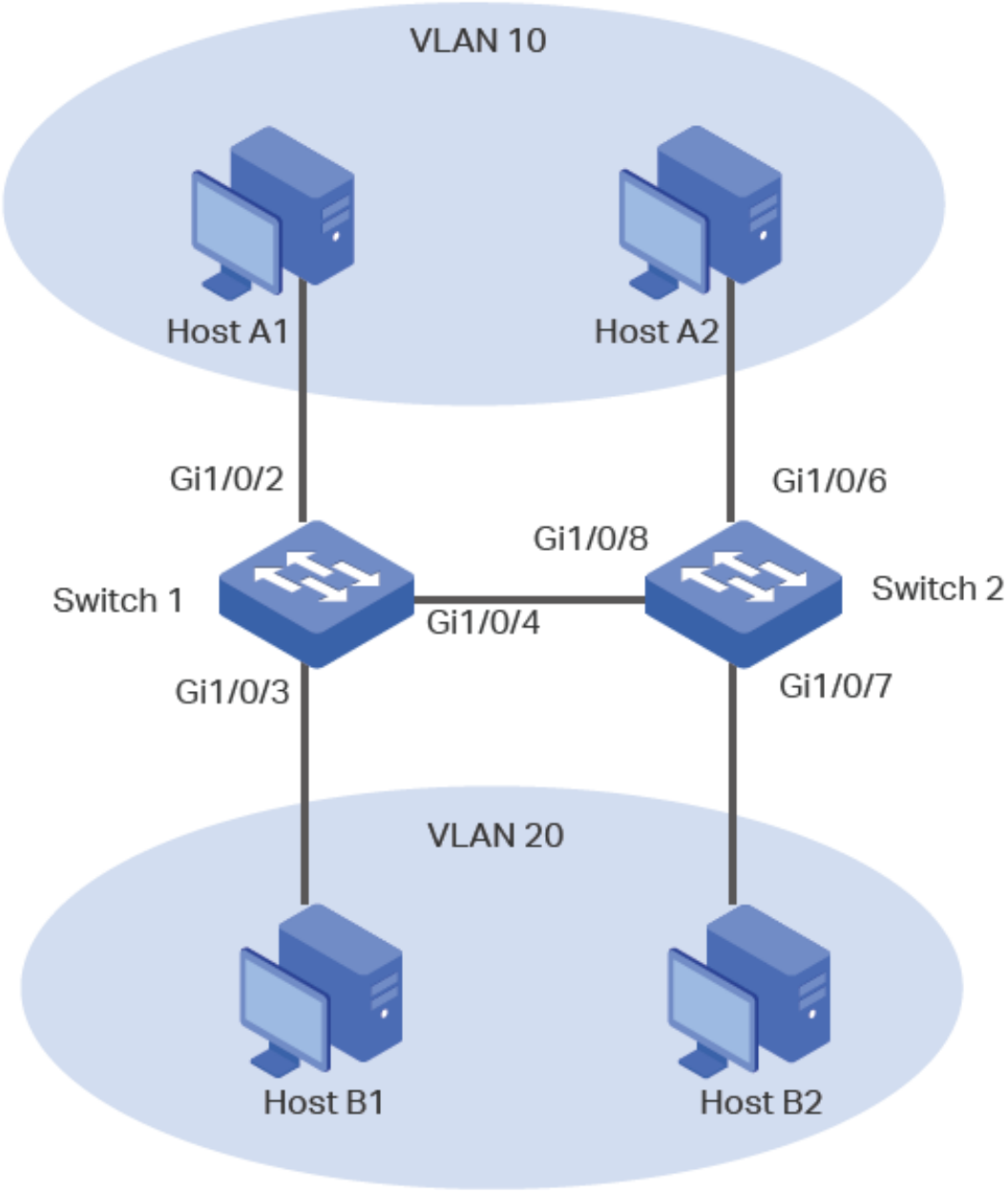
- Escritórios onde o departamento A, e departamento B da empresa estão localizados em lugares diferentes, e alguns computadores tambem em lugares diferentes para conectar ao mesmo switch.
- É necessário que os computadores possam se comunicar uns com os outros no mesmo departamento, mas não se comuniquem com computadores de outros departamentos.

Configurando o Cenário

- Dividir os computadores no Departamento A e Departamento B em duas VLANs, respectivamente de forma que os computadores possam se comunicar uns com os outros no mesmo departamento, mas não com computadores de outro departamento.
- Dispositivos finais como computadores geralmente não suportam marcações de VLAN. Adicionar portas untagged para as VLANs correspondentes e especificar a PVID.
- O elo intermediário entre dois switches carrega o tráfego de duas VLANs simultaneamente. Adicione as portas tagged para as duas VLANs.

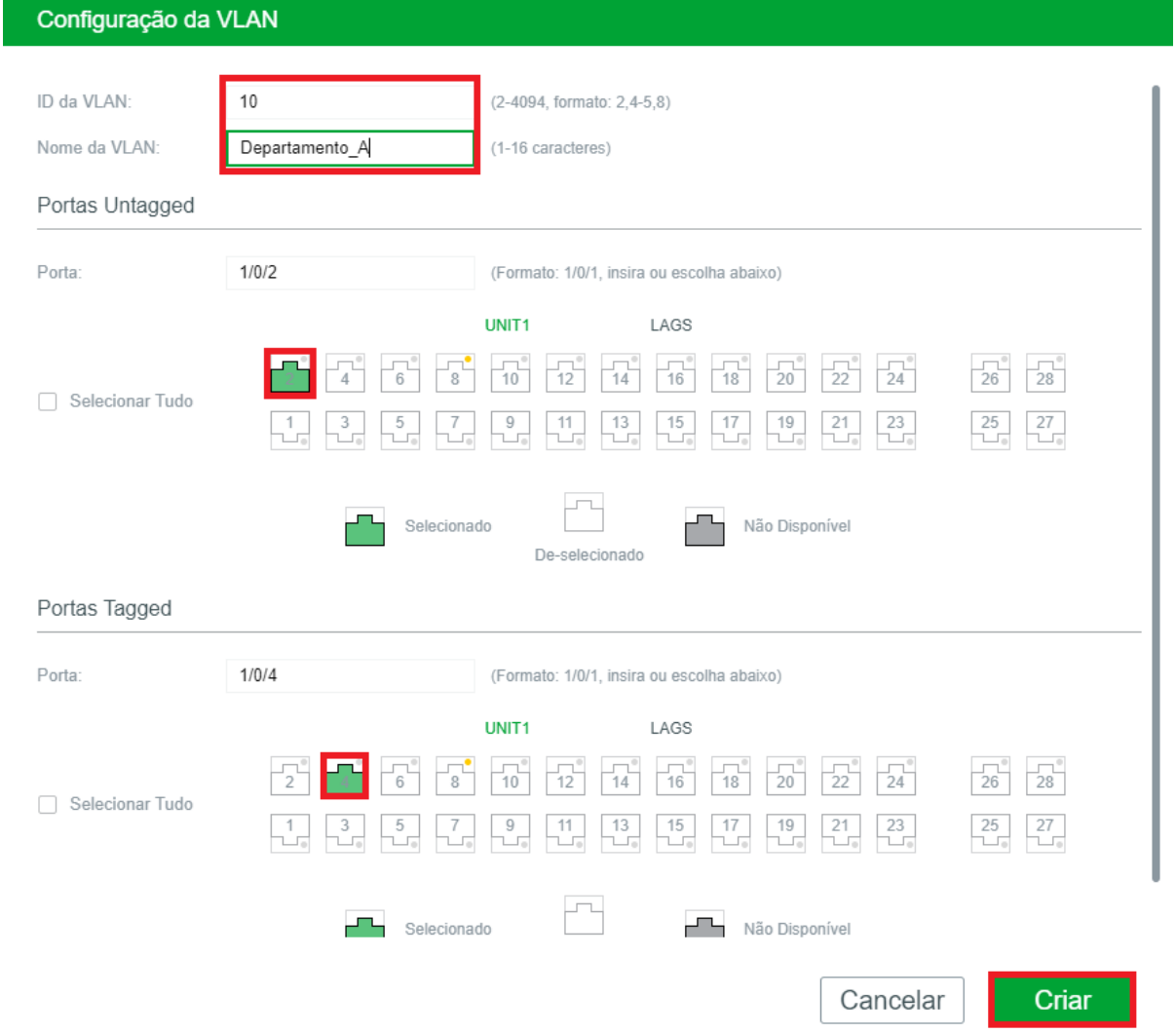
Topologia da Rede

A figura abaixo mostra uma topologia da rede. Os Hosts A1 e A2 estão no departamento A, enquanto os hots B1 e B2 estão no departamento B. Os Switches 1 e 2 estão localizados em lugares diferentes. O Hosts A1 e B1 estão ligados a portas 1/0/2 e 1/0/3 no switch 1, enquanto os A2 e B2 estão ligados à porta 1/0/6 e 1/0/7 do switch 2. A porta 1/0/4 do switch 1 está ligada à porta 1/0/8 do switch 2.

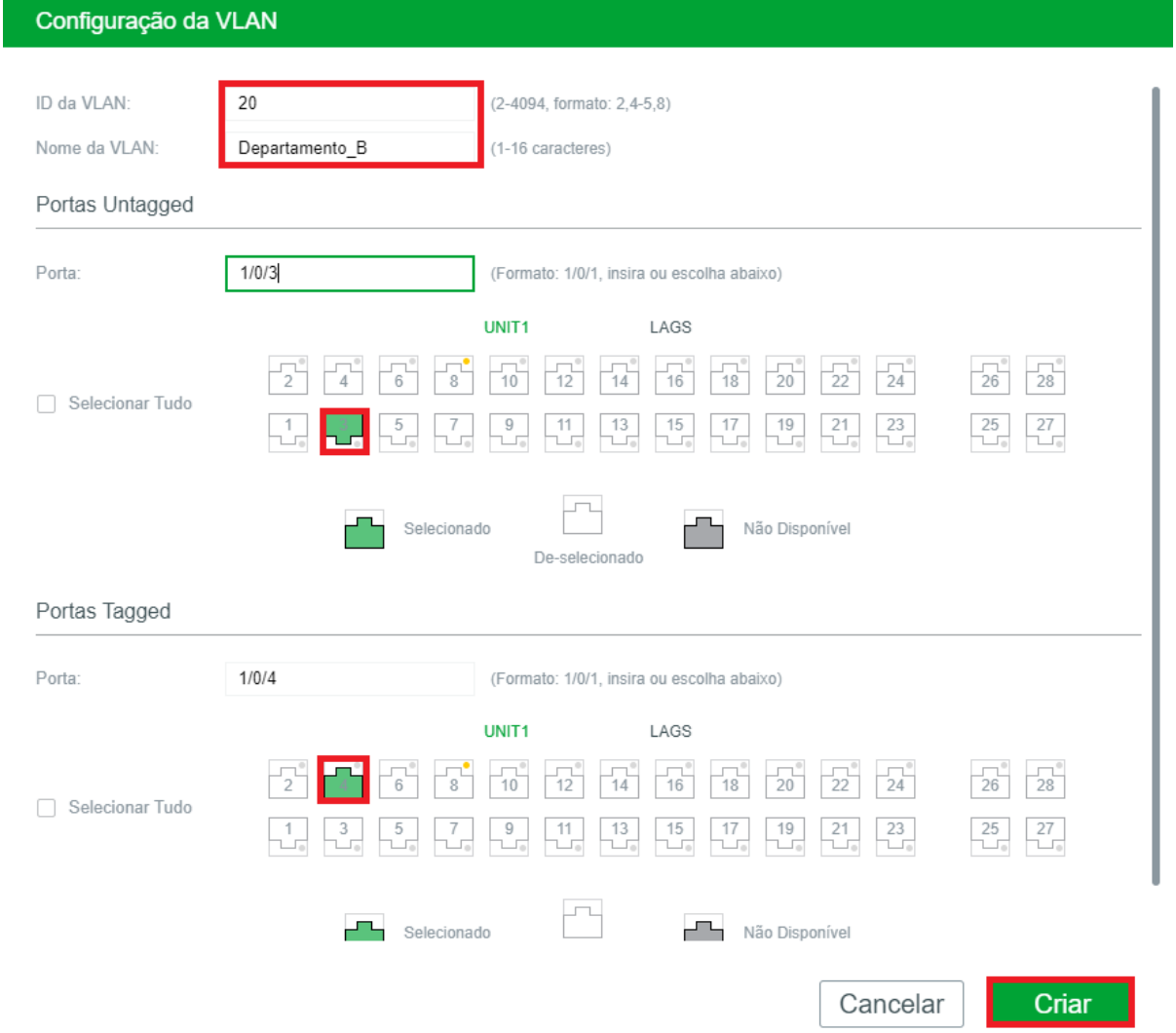


As configurações do switch 1 e switch 2 são semelhantes. A introdução a seguir usa o switch 1 como exemplo.

1. Selecione no menu **FUNÇÕES L2> VLAN> VLAN 802.1Q> Configuração VLAN** e clique em Adicionar para carregar a página a seguir. Criar VLAN 10 com a descrição Departamento_A. Adicione porta 1/0/2 como uma porta não marcado e porta 1/0/4 como uma tagged port VLAN 10. Clique em **Criar**.

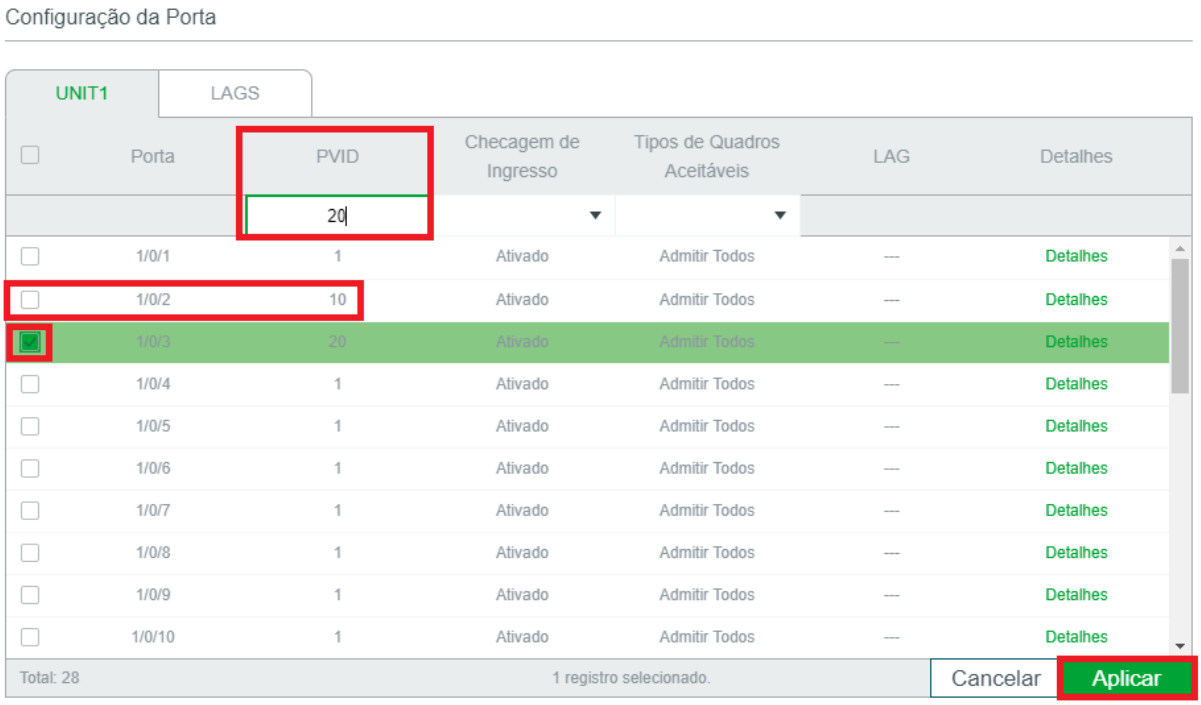


2. Escolha no menu **FUNÇÕES L2> VLAN> VLAN 802.1Q> Configuração VLAN** e clique em Adicionar para carregar a página a seguir. Criar VLAN 20 com a descrição Department_B. Adicionar porta 1/0/3 como uma porta não marcado e porta 1/0/4 como tagged para a VLAN 20. Clique em **Criar**.



3. Selecione no menu **FUNÇÕES L2> VLAN> VLAN 802.1Q> Confiugração de Porta** para carregar a página a seguir.

   Defina o PVID da porta 1/0/2 como 10 e clique em **Aplicar**. Defina a porta da PVID 1/0/3 como 20 e clique em **Aplicar**.



4. Clique em Salvar para salvar as configurações.

Apêndice: Configuração Padrão

As configurações padrão de VLAN 802.1Q estão listados na tabela a seguir.

Tabela Configurações padrão de VLAN 802.1Q

Parâmetros	Configurações Padrão
VLAN ID	1
PVID	1
Verificação de Ingresso	Habilitado
Tipos de quadro aceitáveis	Aceita todos

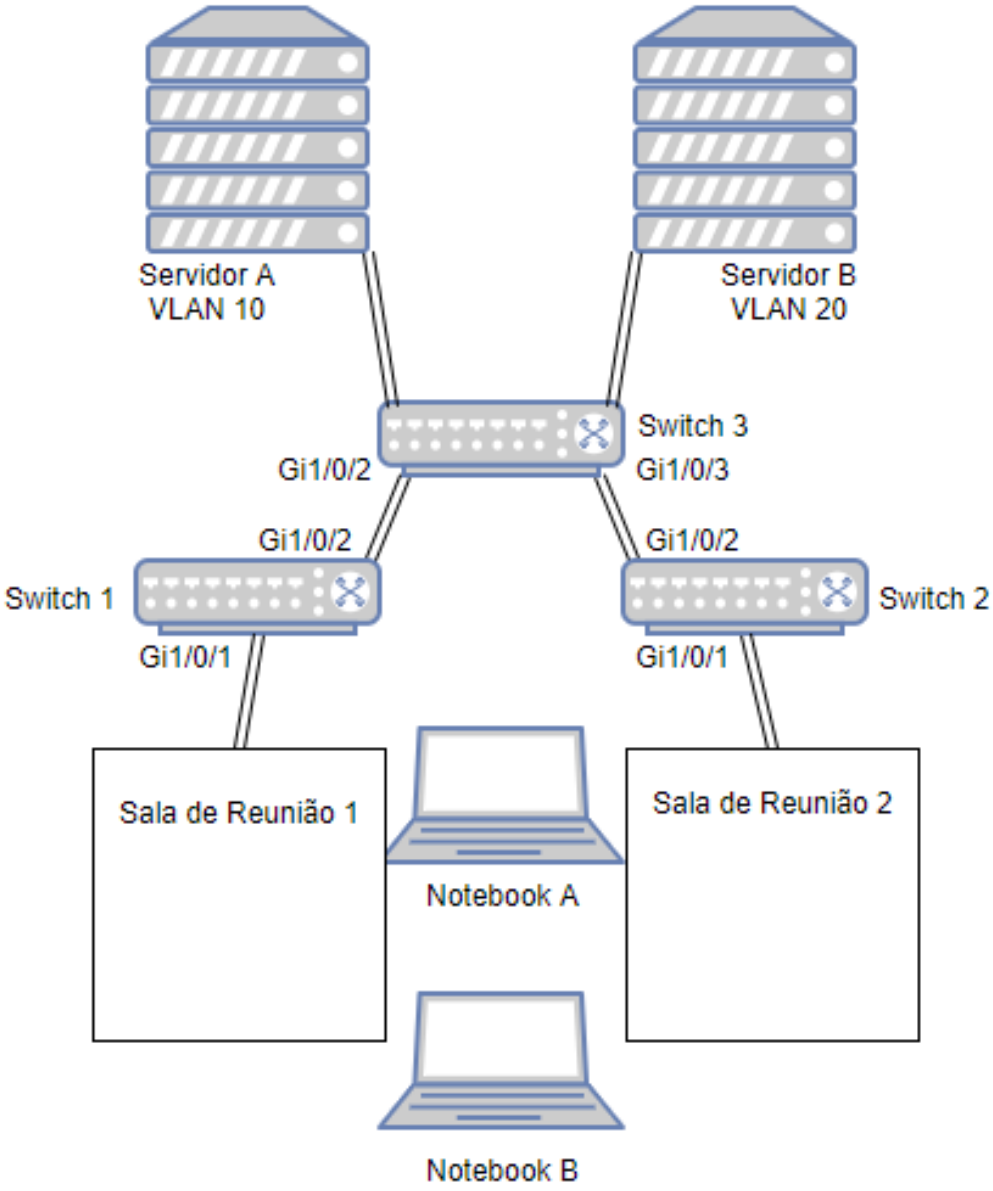
MAC VLAN

Visão Geral

Uma VLAN geralmente é dividida por portas. É uma maneira comum de divisão, mas não é adequado para essas redes que requerem mudanças na topologia frequentes. Com a popularidade do celular escritório, em momentos diferentes de um dispositivo final pode acessar a rede através de portas diferentes. Por exemplo, um dispositivo final que acessou um switch através da porta 1 da última vez, pode mudar para a porta 2 neste tempo. Se as portas 1 e 2 não pertencerem a mesma VLAN (s), o utilizador terá que configurar novamente a chave para acessar a VLAN original.

Usando o MAC VLAN pode poupar o utilizador desse tipo de problema. Essa função divide as VLANs com base nos endereços MAC dos dispositivos finais. Dessa forma, esses dispositivos finais sempre vão pertencer a suas MAC VLAN(s) correspondente(s), mesmo quando as portas de acesso forem alteradas.

A figura abaixo mostra um cenário de aplicação comum de MAC VLAN.



Dois departamentos compartilham todas as salas de reuniões da empresa, mas usam servidores e laptops diferentes. O departamento A usa o servidor A e o laptop A, enquanto o departamento B usa servidor B e laptop B. O servidor A está na VLAN 10, enquanto o servidor B está na VLAN 20. É necessário que o laptop A só possa acessar o servidor A, e o laptop B só pode acessar o servidor B, não importando qual sala de reunião os laptops estão sendo usados.

Para atender a essa exigência, é necessário apenas direcionar os endereços MAC dos laptops para as VLANs correspondentes ao servidor a ser acessado. Desta forma, o endereço MAC determina a qual VLAN o laptop pertence. Cada laptop pode acessar somente o servidor da mesma VLAN a qual ele pertence.

Configuração de MAC VLAN

Para completar a configuração MAC VLAN, siga estes passos:

1. Configurar a VLAN 802.1Q.
2. Ativar o endereço MAC para a VLAN desejada.
3. Habilitar o MAC VLAN na porta.

Orientações de configuração

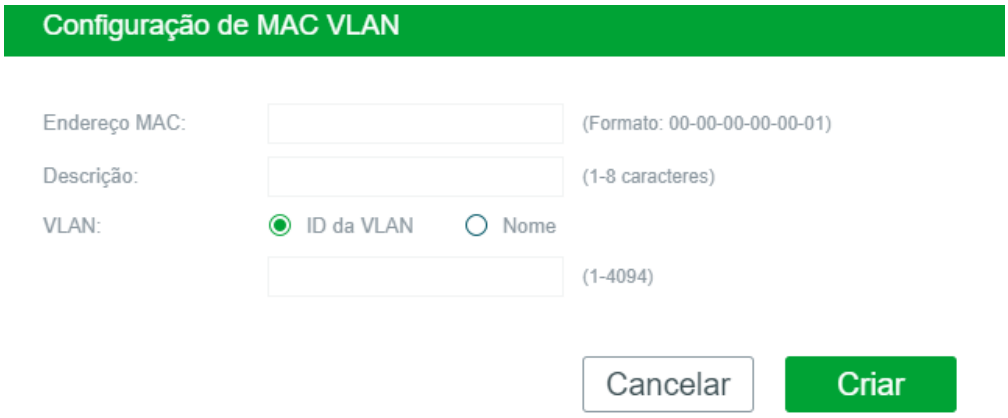
Quando uma porta MAC VLAN recebe um pacote de dados untagged, o switch irá verificar primeiro se o endereço MAC de origem está vinculado ao MAC VLAN. Se sim, o switch irá inserir a tag correspondente ao pacote de dados, e enviá-lo dentro da VLAN a qual ele pertence. Se não, o switch vai continuar verificando se o pacote de dados coincide com as regras de outras VLANs (tal como o protocolo de VLAN). Se houver uma correspondência, o switch vai encaminhar o pacote de dados. Caso contrário, o switch vai processar o pacote de dados de acordo com a regra de processamento do 802,1Q VLAN. Quando a porta recebe um pacote de dados identificado, o switch processará diretamente o pacote de dados de acordo com a regra de processamento da 802.1Q VLAN.

Configurando 802.1Q VLAN

Antes de Configurar a MAC VLAN, crie uma VLAN 802.1Q e configure o tipo de porta de acordo com o requisito da rede. Para mais detalhes vá Configuração da VLAN 802.1Q.

Vinculando o Endereço MAC à VLAN

Vá até o menu **FUNÇÕES L2> VLAN> MAC VLAN** clique em Adicionar para carregar a página a seguir.



Siga os seguintes passo para vincular um endereço MAC à uma VLAN:

1. Entre com o endereço MAC do dispositivo, determine uma descrição e entre com a ID da VLAN para vincular à VLAN.

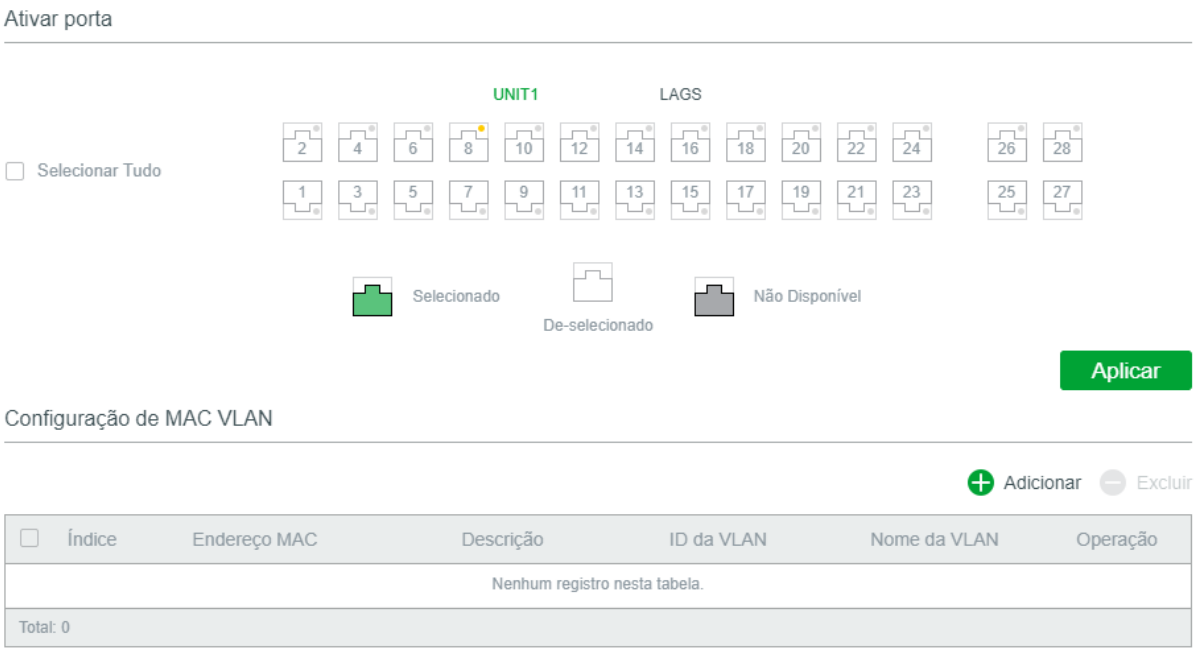
Endereço MAC	Entre com o endereço MAC do dispositivo no formato 00-00-00-00-00-01.
Descrição	Dê uma descrição ao endereço MAC para identificação com até 8 caracteres.
VLAN ID da VLAN/Nome	Entre com o ID ou nome da VLAN à qual será vinculada à MAC VLAN.

2. Clique em **Criar**.

Ativando a MAC VLAN para a porta

Por padrão, o MAC VLAN vem desabilitado em todas as portas. É necessário habilitar manualmente o MAC VLAN para as portas desejadas.

Escolha o menu **FUNÇÕES L2> VLAN> MAC VLAN** para carregar a página a seguir.



Na seção **Ativar a porta**, selecione as portas desejadas para permitir o MAC VLAN e clique em **Aplicar**.

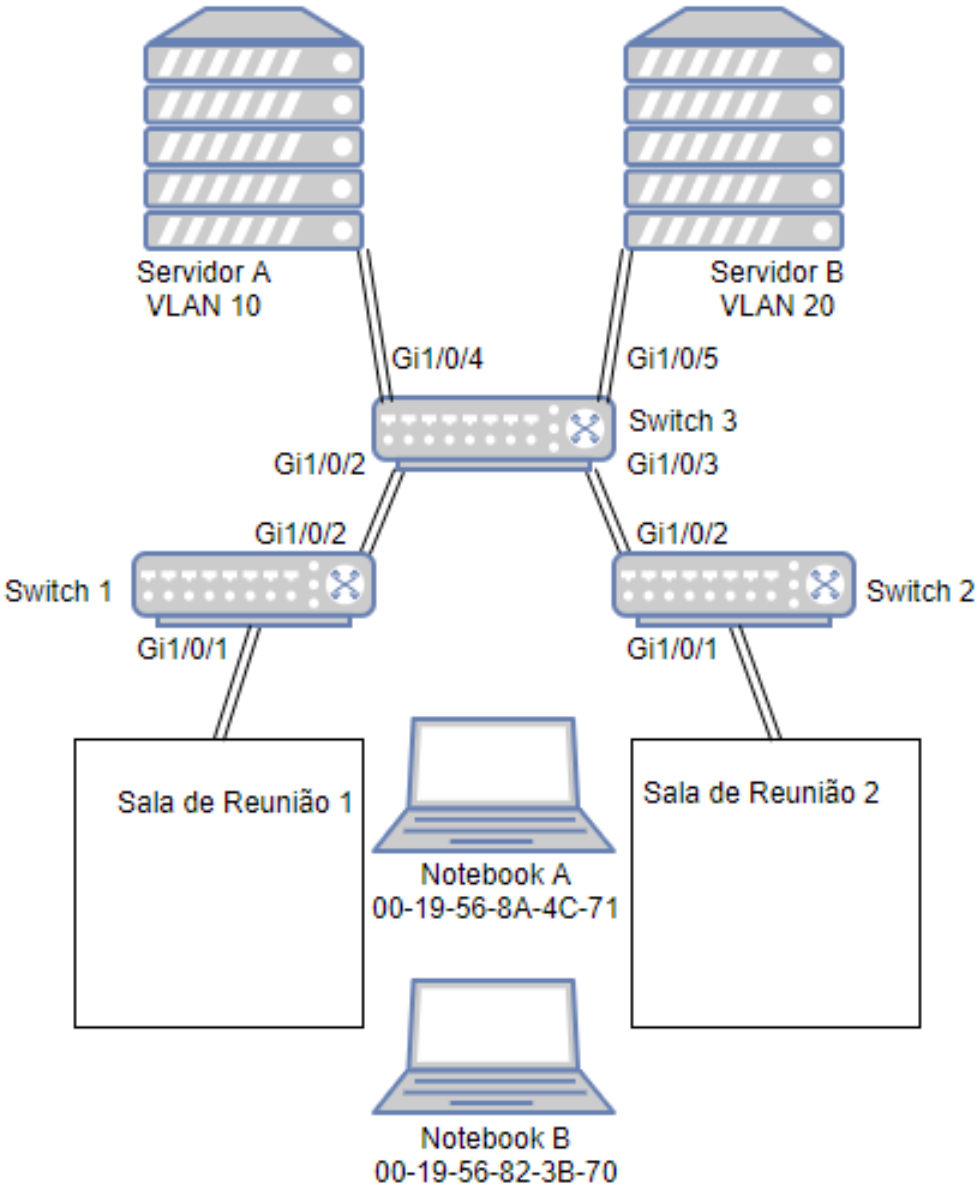
Obs: A porta membro de um LAG (Link Aggregation Group) segue a configuração do LAG, e não a sua própria configuração. As configurações da porta terão efeito somente depois que ele sair do LAG.

Exemplo de Configuração

Requisitos de Rede

Dois departamentos compartilham todas as salas de reuniões na empresa, mas usam servidores e laptops diferentes. O departamento A usa o servidor A e o laptop A, enquanto o departamento B usa o servidor B e o laptop B. O servidor A está na VLAN 10, enquanto o servidor B está na VLAN 20. É necessário que o laptop A só possa ter acesso ao servidor A, e o laptop B só pode acessar o servidor B, não importa qual a sala de reuniões os laptops estão sendo usados.

A figura abaixo mostra a topologia da rede.



Configurando o Cenário

Você pode configurar o MAC VLAN para atender essa exigência. Os switches 1 e 2, direcionam os laptops para as VLANs correspondentes analisando o seu MAC. Desta forma, cada laptop pode acessar somente o servidor da mesma VLAN a qual ele pertence, não importa qual a sala de reuniões os laptops estão sendo utilizados.

A visão geral da configuração é a seguinte:

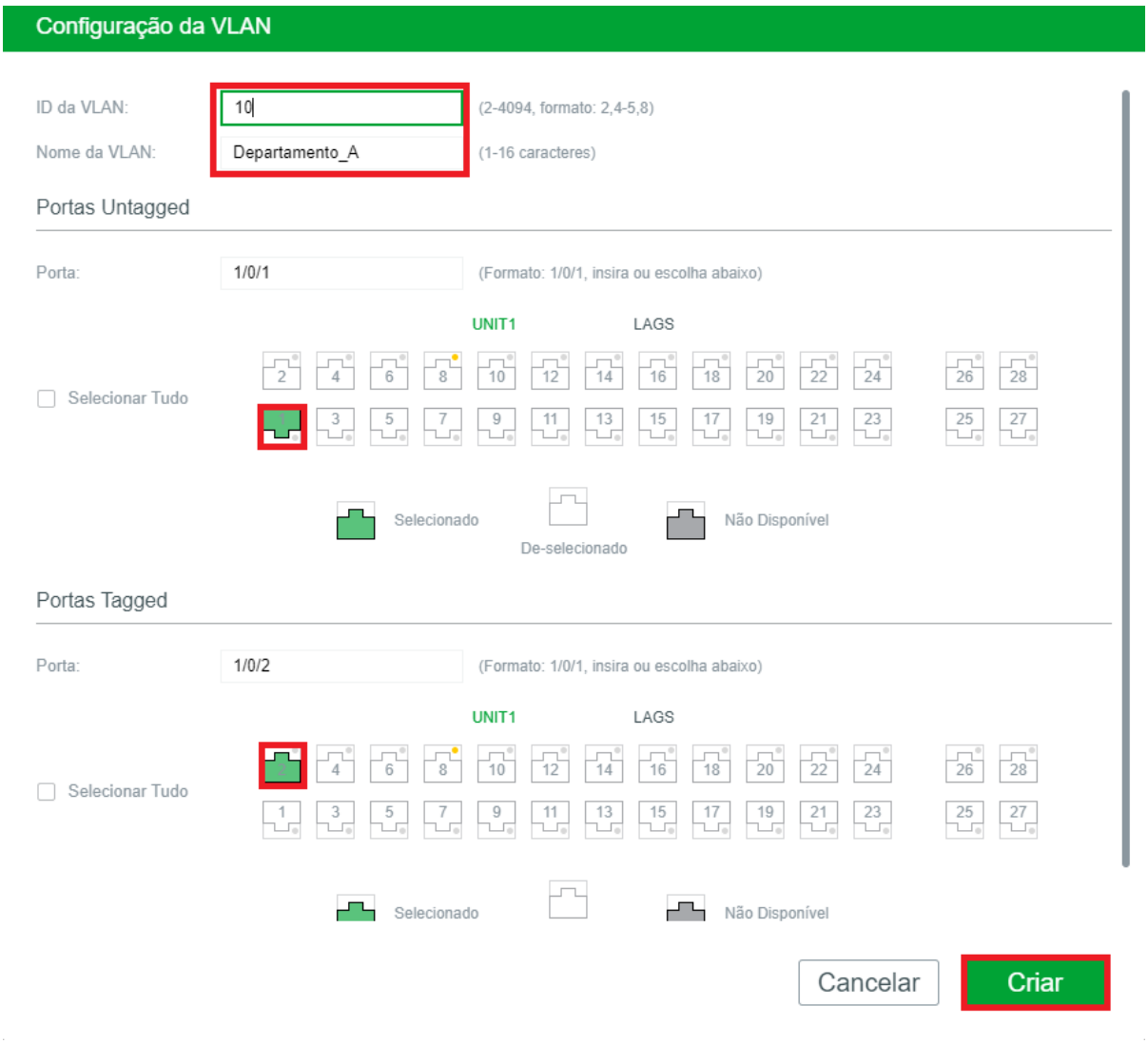
1. Criar a VLAN 10 e VLAN 20 em cada um dos três switches, e adicionar as portas para as VLANs baseado na topologia da rede. Para as portas que ligam os laptops, defina a regra de saída como Untagged; para as portas de conexão para outro switch, definir a regra de saída como Tagged.
2. Nos switches 1 e 2, vincule os endereços MAC dos laptops com a VLANs correspondentes, e habilite o MAC VLAN nas portas.

Como demonstrado a seguir com SG 2404 PoE L2+, o procedimento de configuração:

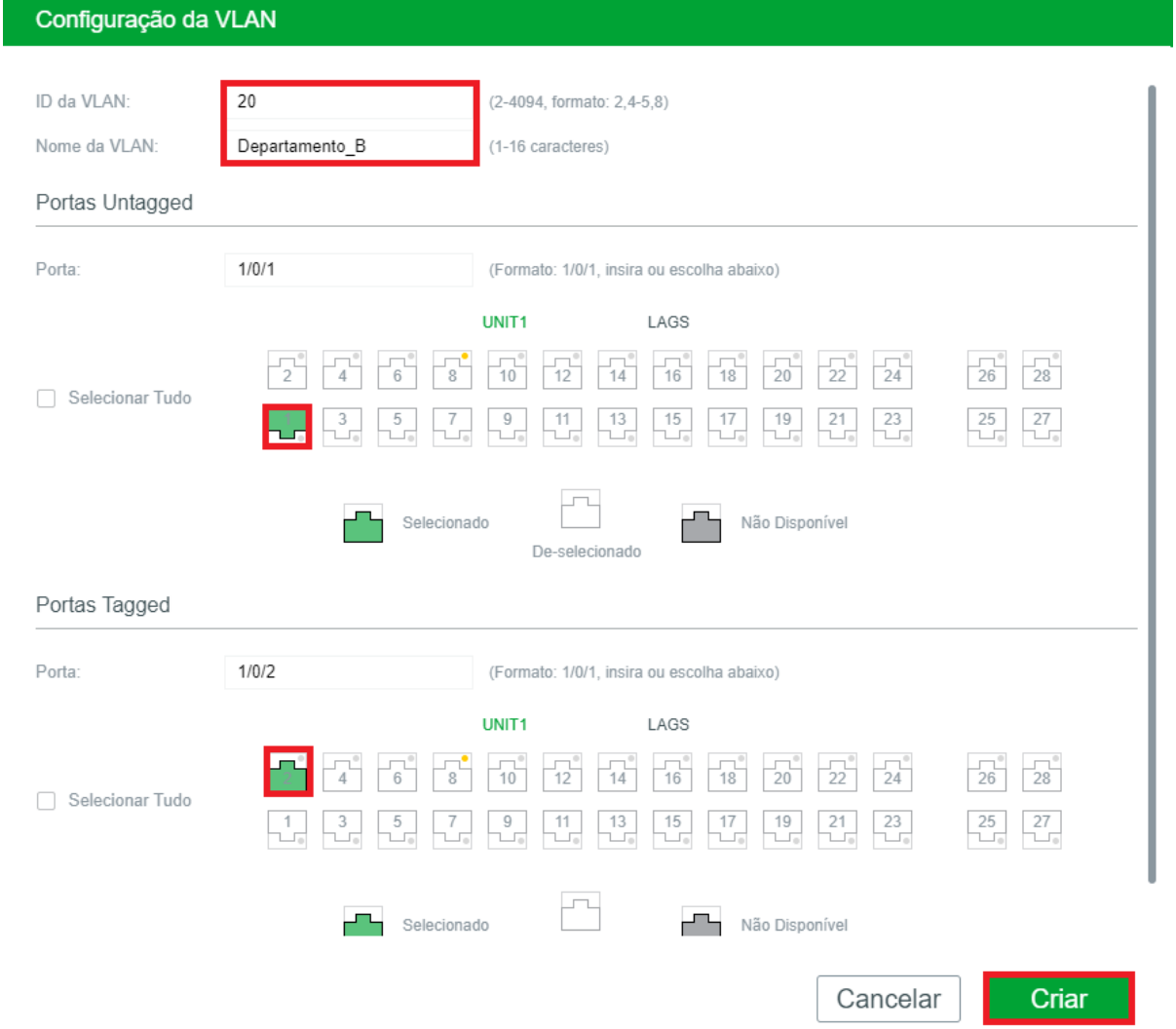
Configuração para os switches 1 e 2

As configurações dos switches 1 e 2 são semelhantes. A apresentação a seguir pode ser tomada como exemplo.

1. Selecione no menu **FUNÇÕES L2> VLAN> VLAN 802.1Q> Configuração VLAN** e clique em Adicionar para carregar a página a seguir. Crie a VLAN 10, e adicione a porta untagged 1/0/1 e porta 1/0/2 marcado tagged para VLAN 10. Clique em **Criar**.

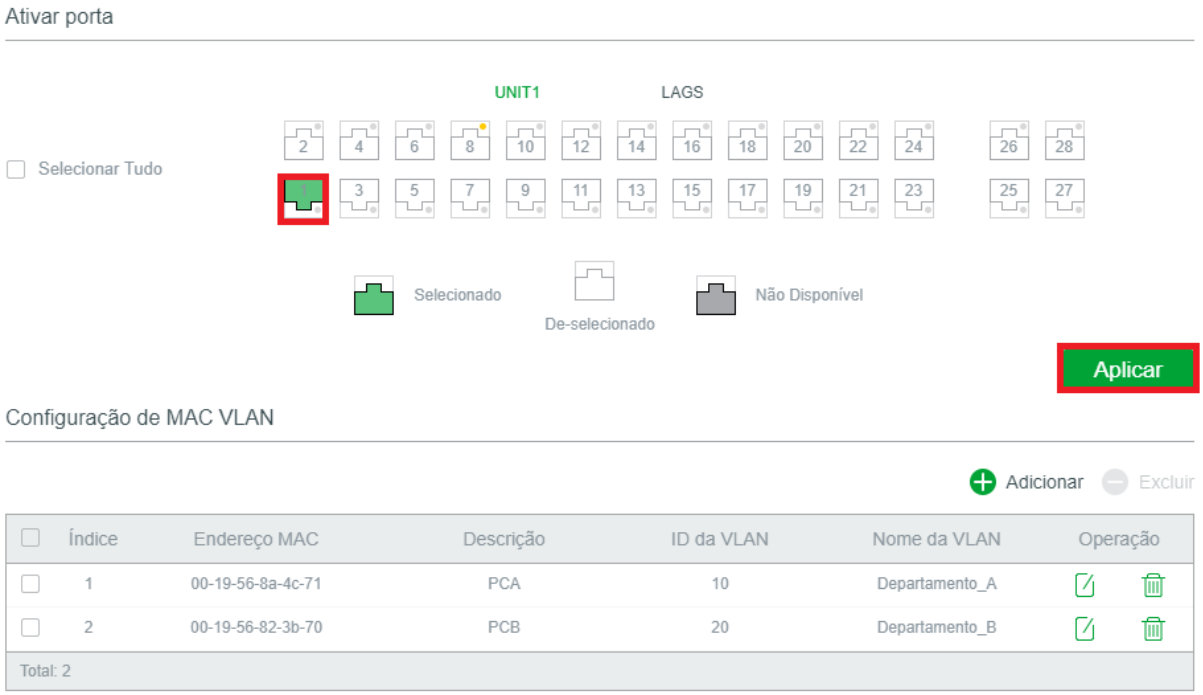


2. Escolha o menu **FUNÇÕES L2> VLAN> VLAN 802.1Q> Configuração VLAN** e clique em Adicionar para carregar a próxima página. Crie a VLAN 20, e adicione a porta untagged 1/0/1 e a porta 1/0/2 tagged para VLAN 20. Clique em **Criar**.



3. Escolha o menu **FUNÇÕES L2> VLAN> MAC VLAN** e clique em Adicionar para carregar a página a seguir. Especifique os parâmetros correspondentes e clique em **Criar** para vincular o endereço MAC do notebook A a VLAN 10 e vincular o endereço MAC do notebook B a VLAN 20.

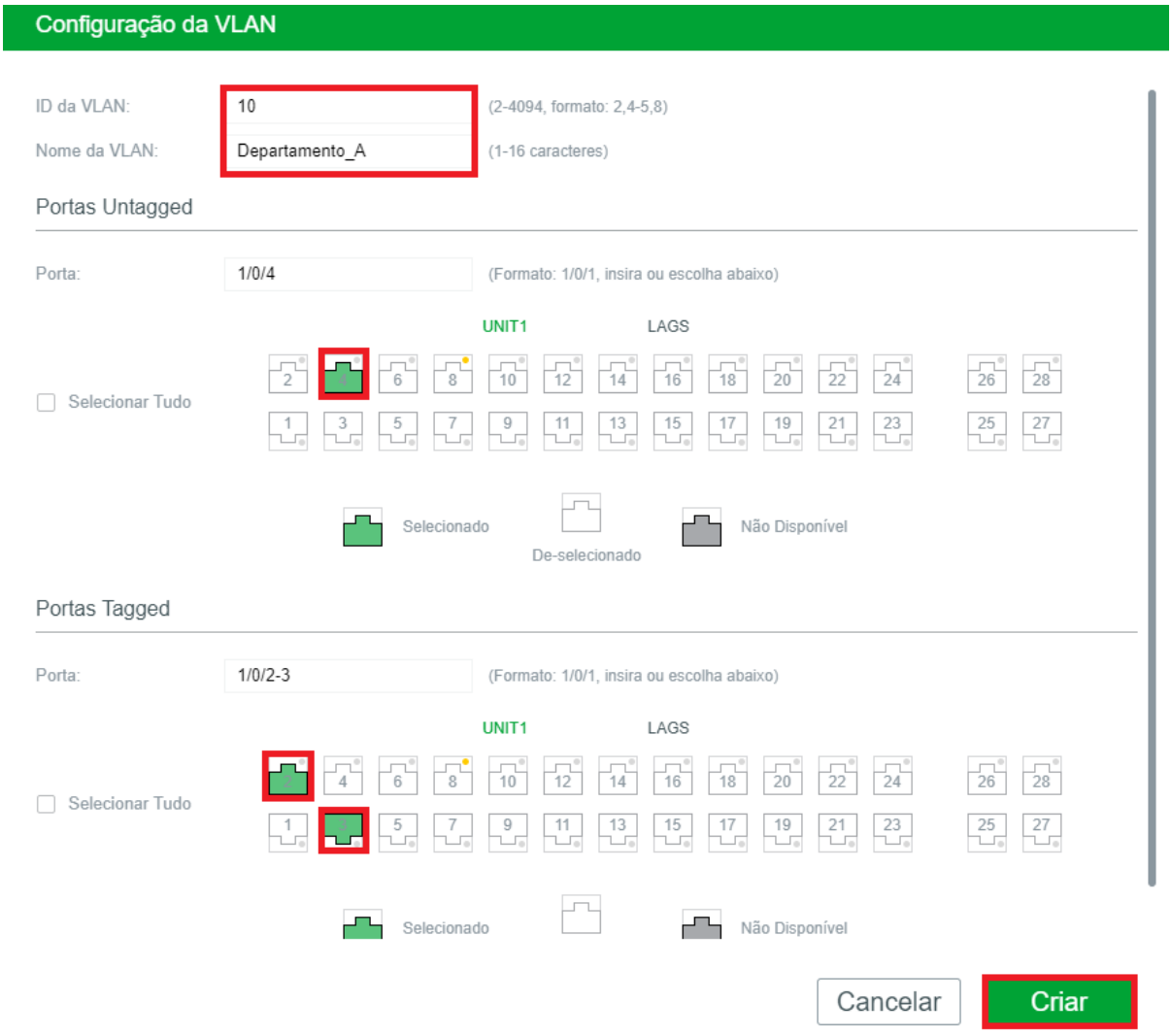
4. Escolha o menu **FUNÇÕES L2> VLAN> MAC VLAN** clique em Adicionar para carregar a página a seguir. Na seção **Ativar porta** selecione a porta 1/0/1 e clique em **Aplicar** para permitir MAC VLAN.



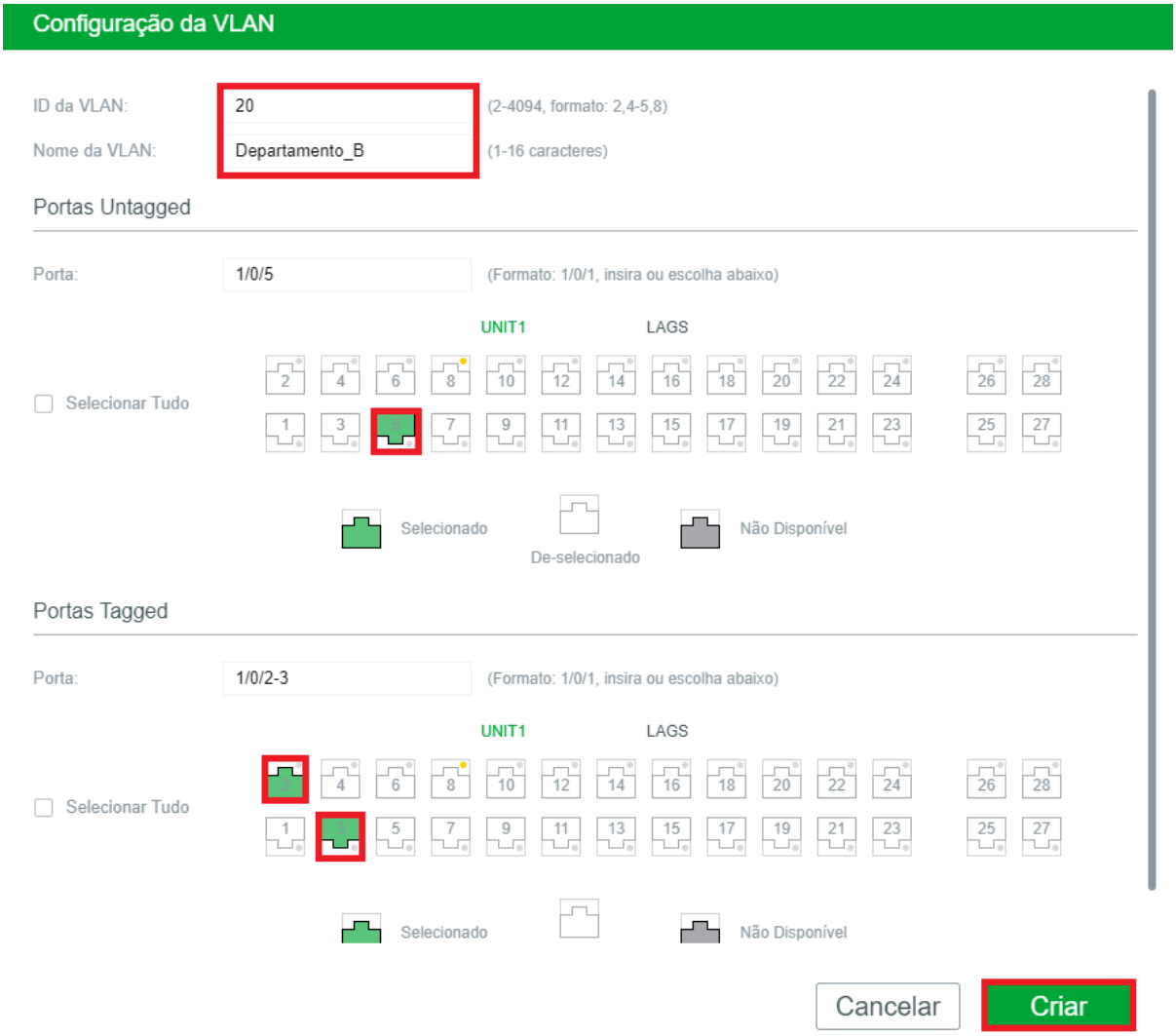
5. Clique em Salvar para salvar as configurações.

Configurações do Switch 3

1. Escolha o menu **FUNÇÕES L2> VLAN> VLAN 802.1Q> Configuração VLAN** e clique em Adicionar para carregar a página a seguir. Crie a VLAN 10 e adicione a porta untagged 1/0/4 e portas 1/0/2-3 tagged à VLAN 10. Clique em **Criar**.



2. Clique em **Criar** para carregar a próxima página. Crie a VLAN 20, e adicione a porta 1/0/5 untagged e as portas 1/0/2-3 tagged à VLAN 20. Clique em **Criar**.



3. Clique em Salvar para salvar as configurações.

Apêndice: Configuração Padrão

As configurações padrão do MAC VLAN estão listadas na tabela a seguir.

Tabela Configurações padrão de MAC VLAN

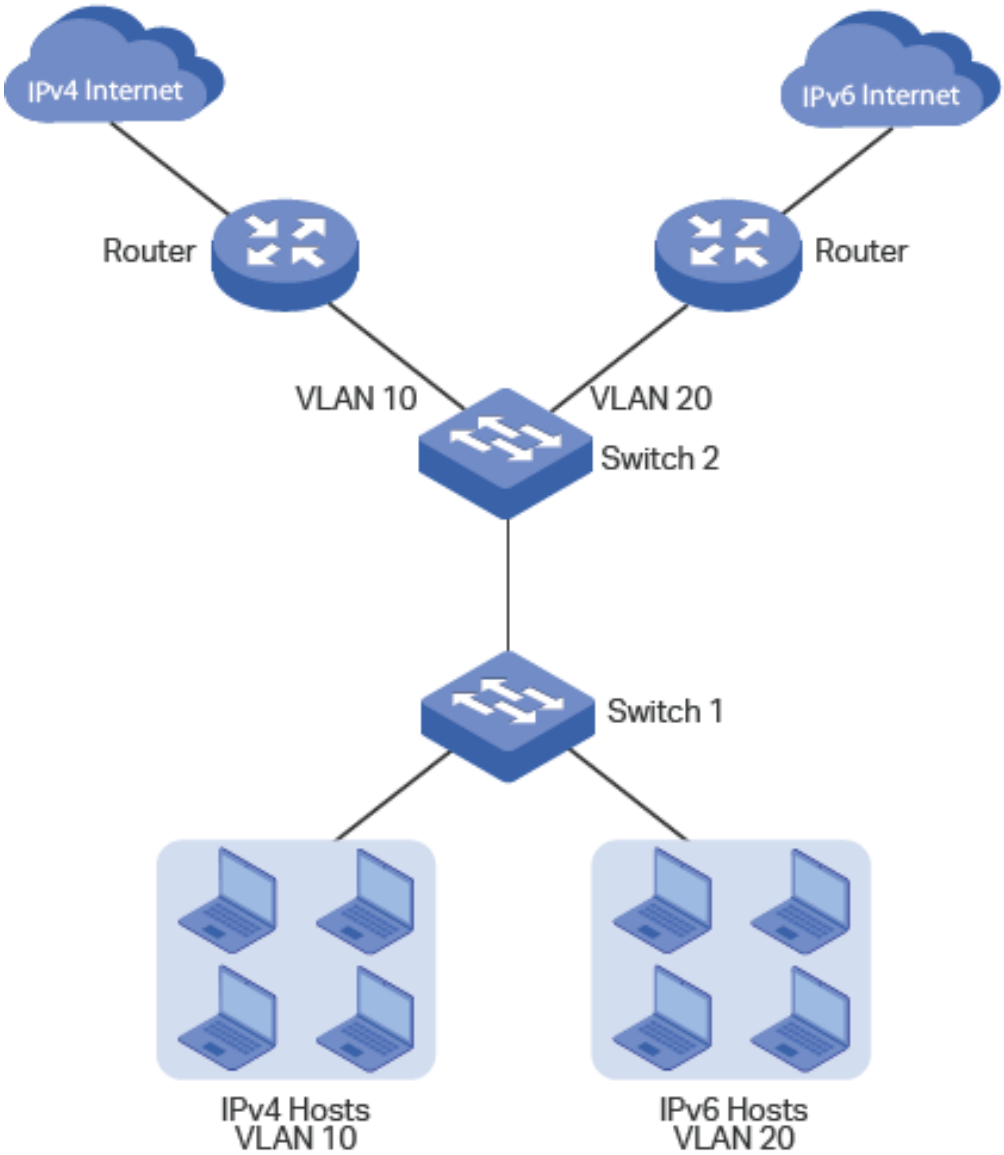
Parâmetros	Configurações Padrão
MAC Address	Nenhum
Descrição	Nenhum
VLAN ID	Nenhum
Ativar porta	Desabilitado

VLAN DE PROTOCOLO

Visão Geral

Protocolo VLAN é uma tecnologia que divide VLANs com base no protocolo da camada de rede. Com a regra de protocolo VLAN configurada com base na 802.1Q VLAN existente, o switch pode analisar campos específicos de pacotes recebidos, encapsular os pacotes em formatos específicos e encaminhar os pacotes com diferentes protocolos às VLANs correspondentes. Como aplicativos e serviços diferentes usam protocolos diferentes, os administradores de rede podem usar o protocolo VLAN para gerenciar a rede com base em aplicativos e serviços específicos.

A figura abaixo mostra um cenário de aplicação comum do protocolo VLAN. Com o protocolo VLAN configurado, o Switch 2 pode encaminhar pacotes IPv4 e IPv6 de diferentes VLANs para as redes IPv4 e IPv6, respectivamente.



Configuração de VLAN de Protocolo

A completa configuração do protocolo VLAN, segue os seguintes passos:

1. Configurar a VLAN 802.1Q.

2. Criar o modelo do protocolo.
3. Configurar o protocolo VLAN.

Configurando 802.1Q VLAN

Antes de Configurar a MAC VLAN, crie uma VLAN 802.1Q e configure o tipo de porta de acordo com o requisito da rede. Para mais detalhes vá Configuração da VLAN 802.1Q.

Criando Modelo de Protocolo

Escolha o menu **FUNÇÕES L2 > VLAN > VLAN Protocolo > Modelo de Protocolo** para carregar a seguinte página.

Siga os seguintes passos para criar o modelo de protocolo.

1. Verifique se o modelo desejado já existe na seção **Configuração do Modelo de Protocolo**. Caso contrário, clique em Adicionar para criar um novo modelo.

Nome do Modelo	Dê um nome de protocolo para identificar o modelo de protocolo.

Tipo de Frame	Selecione o tipo de quadro do novo modelo de protocolo. **Ethernet II:** Um formato de quadro Ethernet comum. Selecione para especificar o Tipo de quadro digitando o Ether Type. **SNAP:** Um formato de quadro Ethernet 802.3 baseado no SNAP IEEE 802.3 e IEEE 802.2. Selecione para especificar o Tipo de quadro digitando o Ether Type **LLC:** Um formato de quadro Ethernet 802.3 baseado no IEEE 802.3 e IEEE 802.2 LLC. Selecione para especificar o Tipo de quadro digitando o DSAP e o SSAP.
Ether Type	Digite o valor do tipo de protocolo Ethernet para o modelo de protocolo. Está disponível quando Ethernet II e SNAP está selecionado. O campo Ether Type do quadro e é usado para identificar o tipo de dados do quadro.
DSAP	Digite o valor DSAP para o modelo de protocolo. Está disponível quando LLC está selecionado. É o campo DSAP no quadro e é usado para identificar o tipo de dados do quadro.
SSAP	Digite o valor SSAP para o modelo de protocolo. Está disponível quando LLC está selecionado. É o campo SSAP no quadro e é usado para identificar o tipo de dados do quadro.

2. Clique em **Criar**.

> Um modelo de protocolo vinculado a uma VLAN não pode ser excluído.

Configurando a VLAN de Protocolo

Escolha o menu **FUNÇÕES L2 > VLAN > VLAN Protocolo > Grupo de VLAN Protocolo** e clique em Adicionar para carregar a seguinte página.

Siga os seguintes passos para efetuar a configuração do grupo de protocolo:

1. Na seção de **Configuração do Protocolo de Grupo VLAN**, especifique os seguintes parâmetros.

Nome do Modelo	Selecione o modelo de protocolo definido anteriormente.
ID da VLAN / Nome da VLAN	Digite o número de identificação ou o nome da VLAN 802.1Q que será vinculada à VLAN de protocolo.
Prioridade 802.1p	Especifique a prioridade 802.1p para os pacotes que pertencem ao protocolo VLAN. O switch determinará a sequência de encaminhamento de acordo com este valor. Os pacotes com maior valor de prioridade 802.1p têm a prioridade mais alta.

2. Selecione as portas desejadas. Clique em **Criar**.

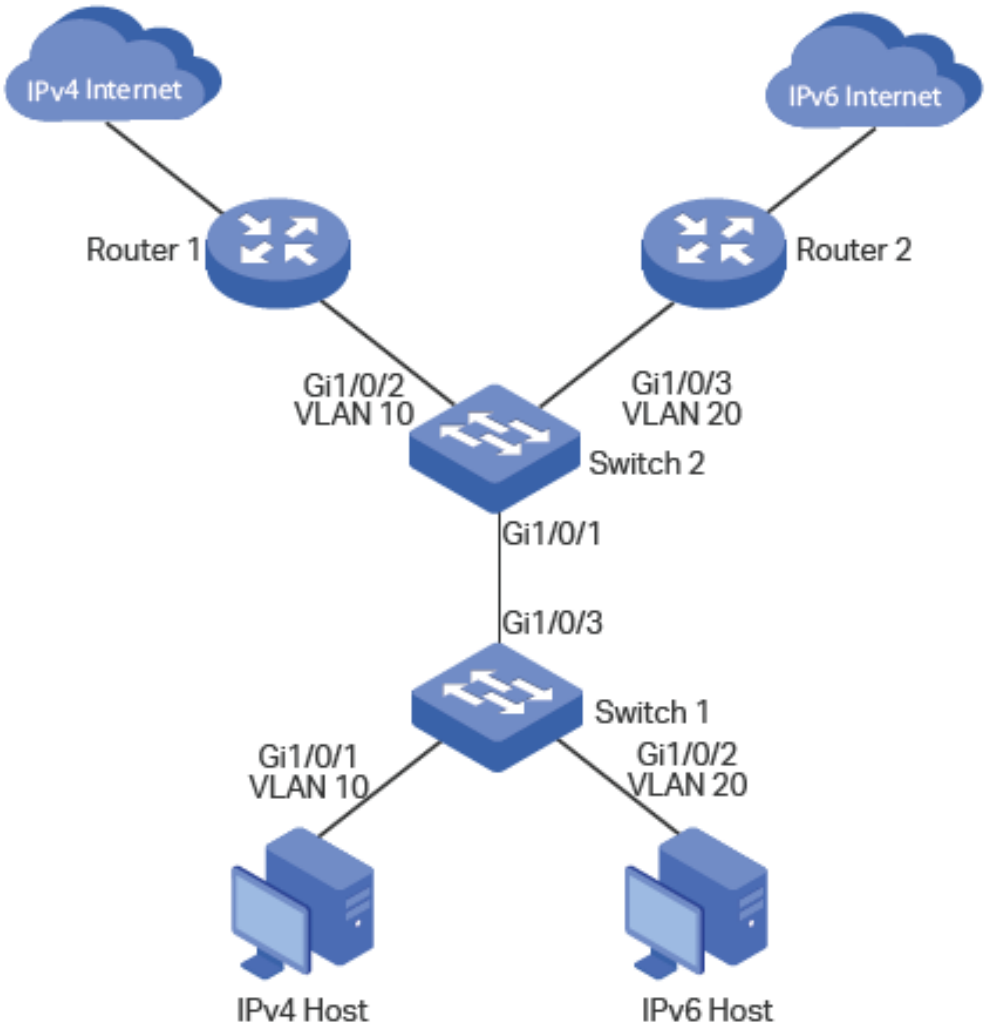
> A porta membro de um LAG (Link Aggregation Group) segue a configuração do LAG e não a sua. As configurações da porta podem entrar em vigor somente após a saída do LAG.

Exemplo de Configuração

Requisitos de Rede

Uma empresa usa hosts IPv4 e IPv6, e esses hosts acessam a rede IPv4 e a rede IPv6, respectivamente, por meio de roteadores diferentes. É necessário que os pacotes IPv4 sejam encaminhados para a rede IPv4, os pacotes IPv6 sejam encaminhados para a rede IPv6 e outros pacotes sejam descartados.

A figura abaixo mostra a topologia de rede. O host IPv4 pertence à VLAN 10, o host IPv6 pertence à VLAN 20 e esses hosts acessam a rede através do Switch 1. O Switch 2 é conectado a dois roteadores para acessar a rede IPv4 e a rede IPv6, respectivamente. Os roteadores pertencem à VLAN 10 e VLAN 20, respectivamente.



Configurando o Cenário

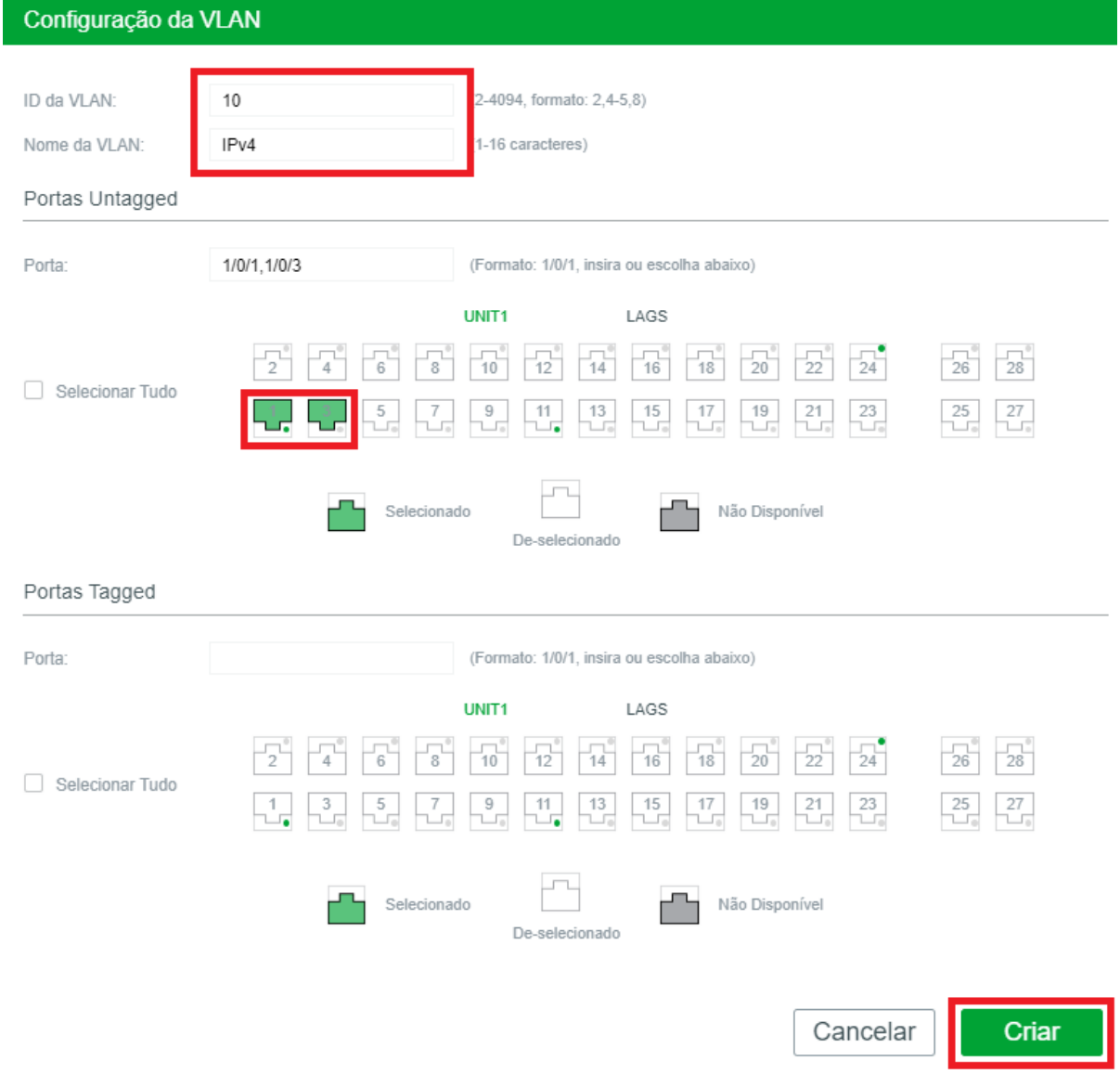
Você pode configurar o protocolo VLAN na porta 1/0/1 do Switch 2 para atender a esse requisito. Quando essa porta recebe pacotes, o Switch 2 os encaminha para as VLANs correspondentes, de acordo com seus tipos de protocolo. A visão geral da configuração no Switch 2 é a seguinte:

1. Crie VLAN 10 e VLAN 20 e adicione cada porta à VLAN correspondente.
2. Use o modelo de protocolo IPv4 fornecido pelo switch e crie o modelo de protocolo IPv6.
3. Ligue os modelos de protocolo às VLANs correspondentes para formar grupos de protocolos e adicione a porta 1/0/1 aos grupos.

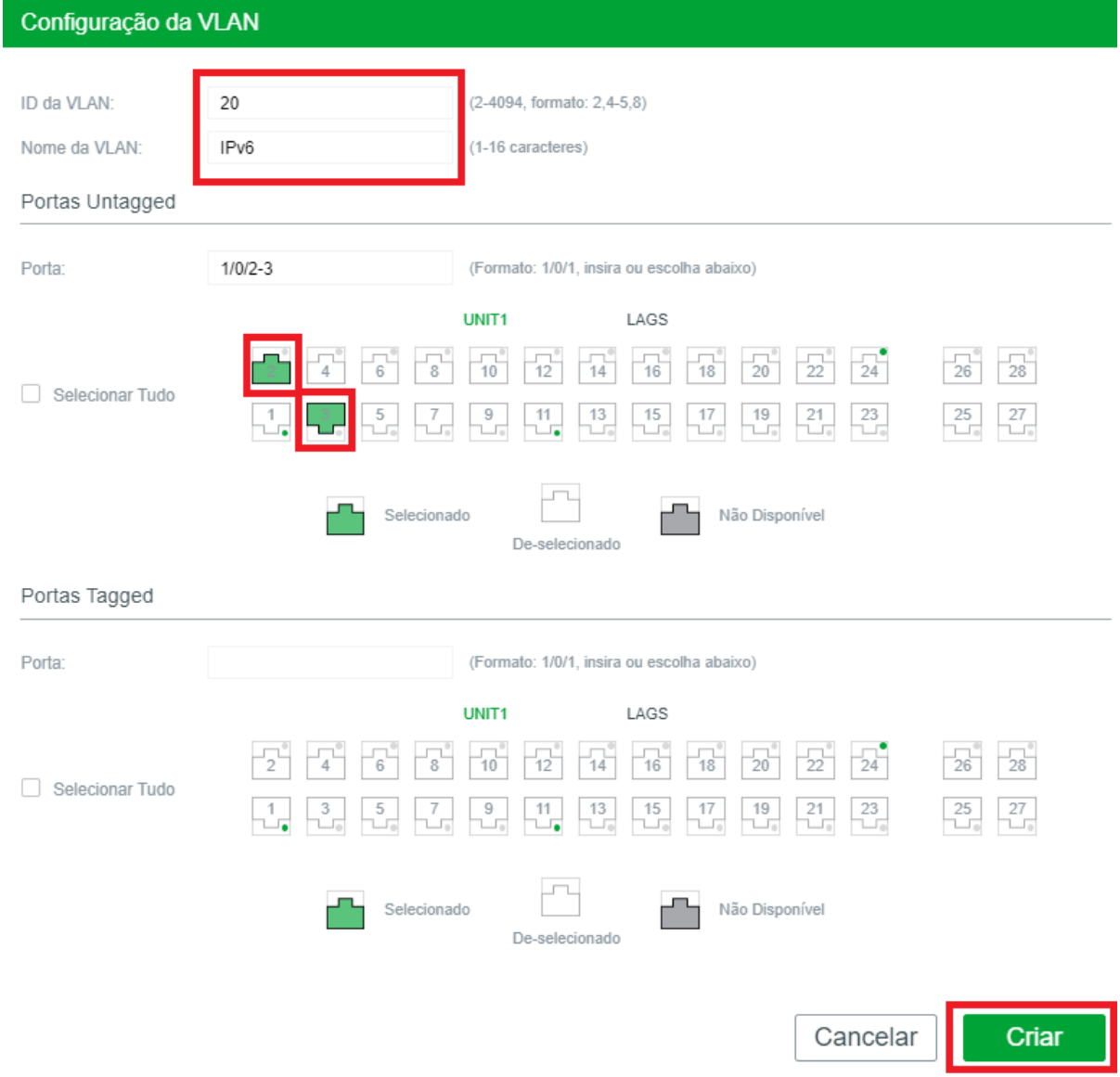
Para o Switch 1, configure a VLAN 802.1Q de acordo com a topologia de rede.

Configurações no Switch 1

1. Escolha o menu **FUNÇÕES L2 > VLAN > VLAN 802.1Q > Configuração de VLAN** e clique em Adicionar para carregar a página seguinte. Crie a VLAN 10 e adicione a porta untagged 1/0/1 e a porta untagged 1/0/3 à VLAN 10. Clique em **Criar**.



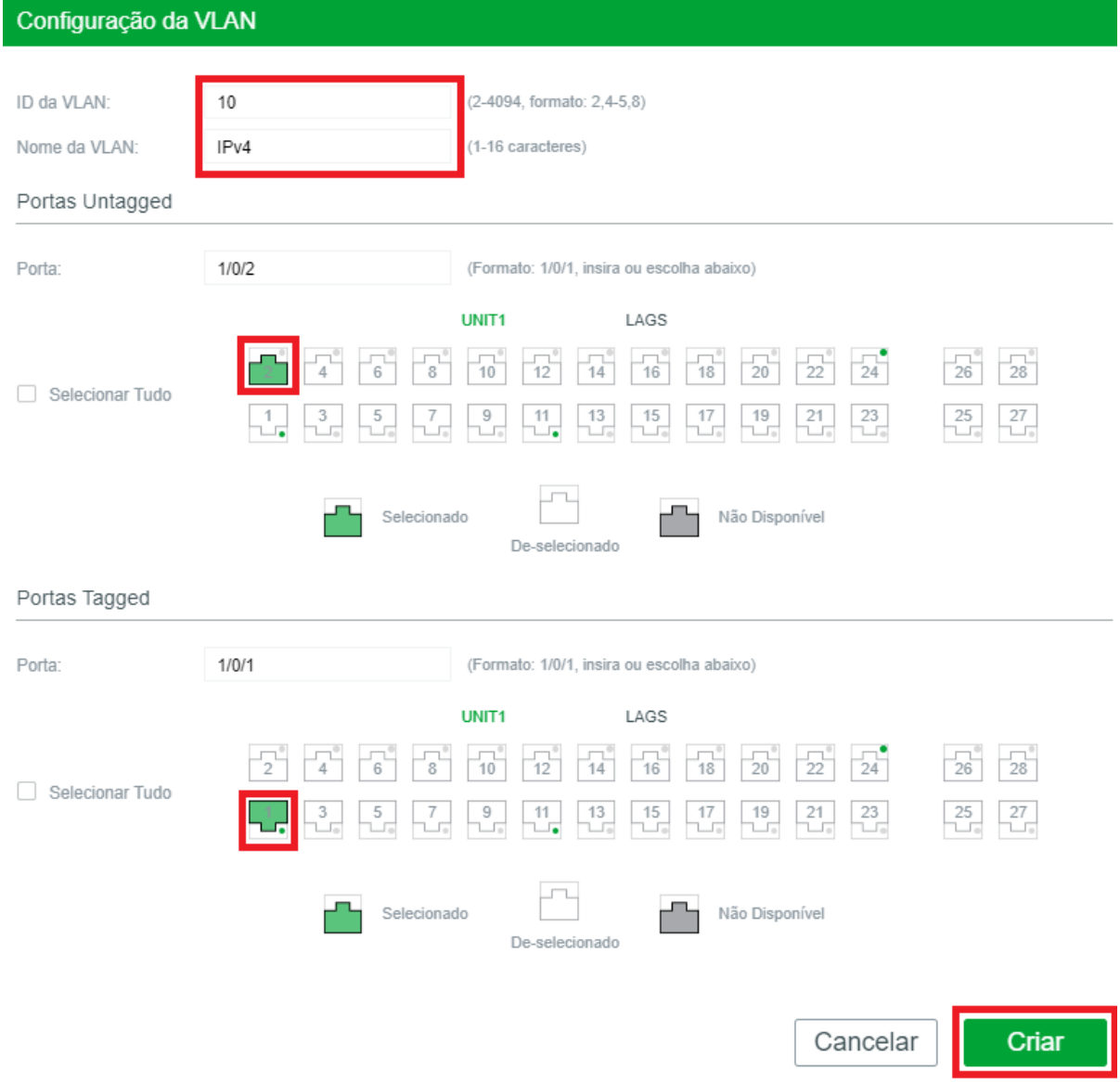
2. Clique em Adicionar para carregar a página seguinte. Crie a VLAN 20 e adicione portas untagged 1/0/2-3 à VLAN 20. Clique em **Criar**.



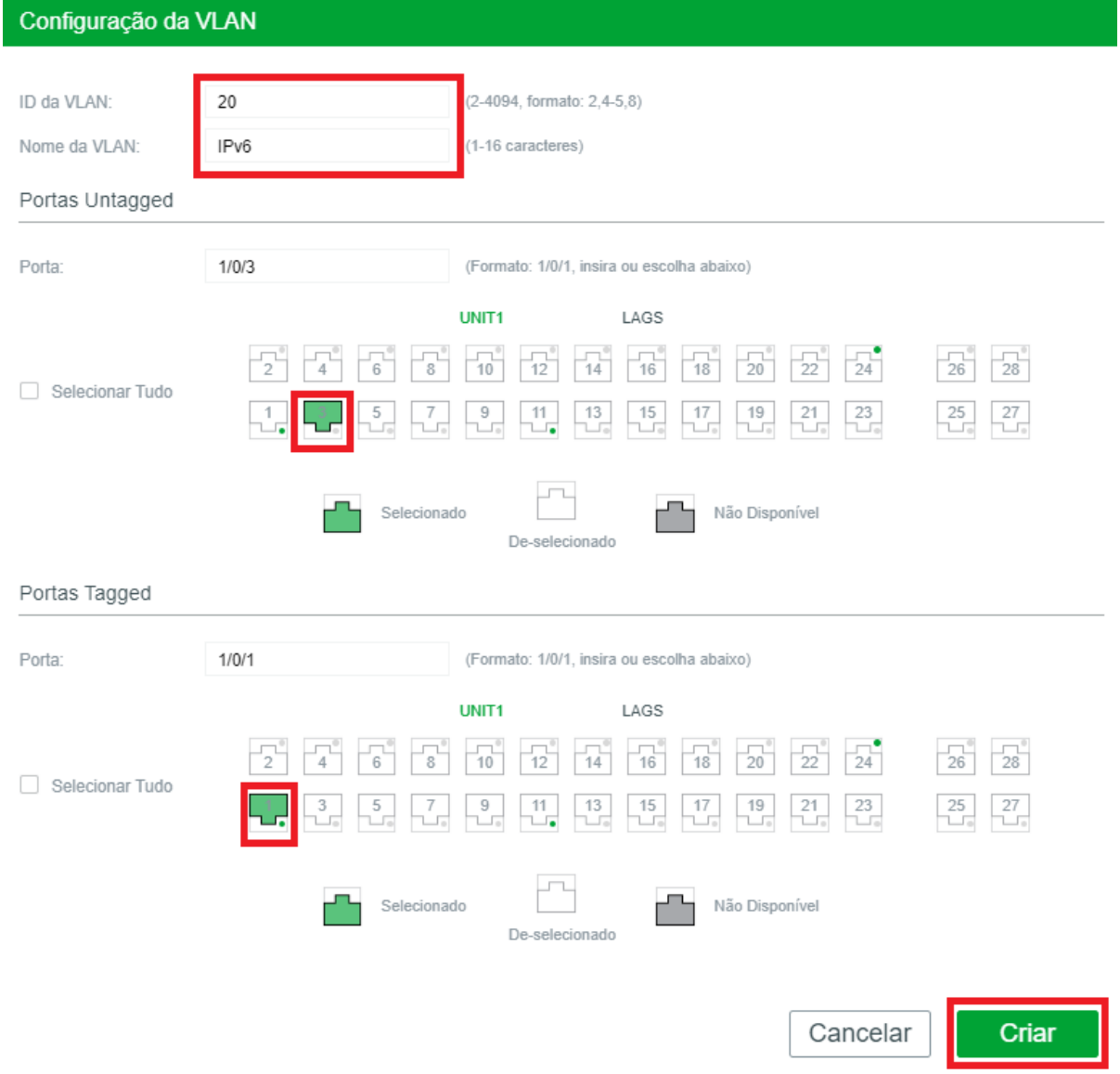
3. Clique em Salvar para salvar as configurações.

Configurações no Switch 2

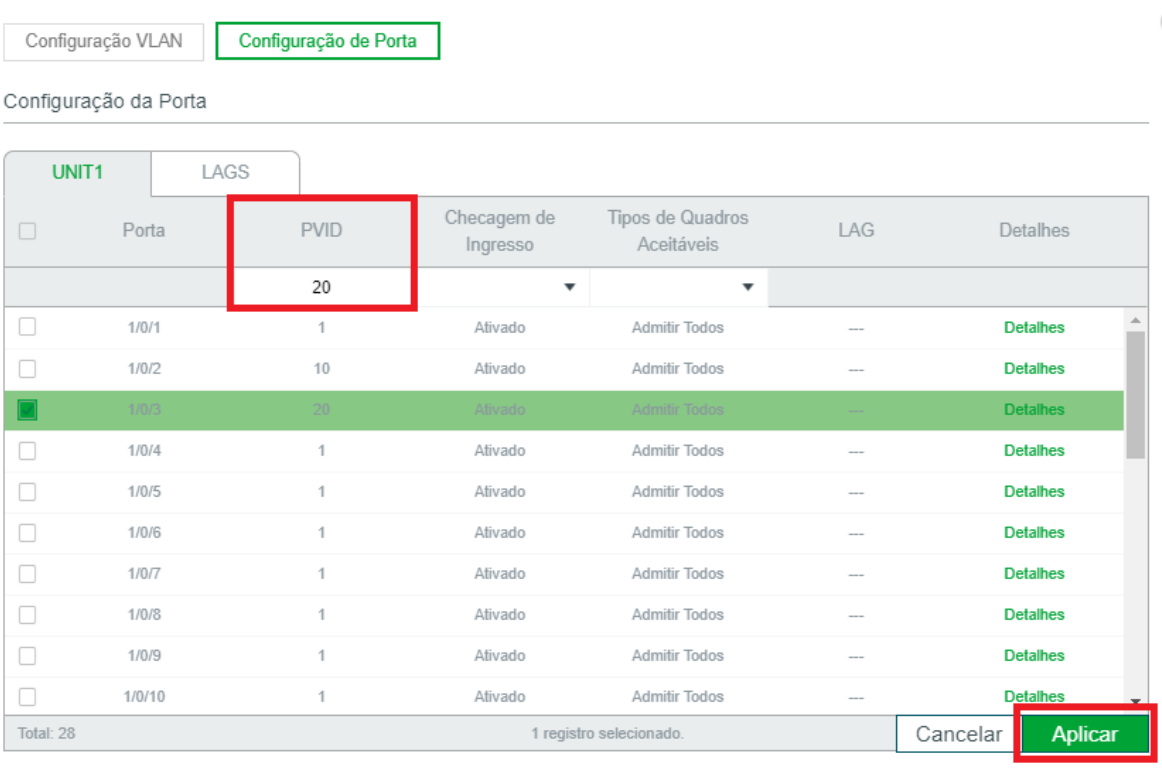
1. Escolha o menu **FUNÇÕES L2 > VLAN > VLAN 802.1Q > Configuração de VLAN** e clique em Adicionar para carregar a página seguinte. Crie a VLAN 10 e adicione a porta tagged 1/0/1 e a porta untagged 1/0/2 à VLAN 10. Clique em **Criar**.



2. Clique em ⊕ Adicionar para carregar a página seguinte. Crie a VLAN 20 e adicione portas tagged 1/0/1 e a porta untagged 1/0/3 à VLAN 20. Clique em **Criar**.



3. Escolha o menu **FUNÇÕES L2 > VLAN > VLAN 802.1Q > Configuração de Porta** para carregar a página seguinte. Defina o PVID da porta 1/0/2 e da porta 1/0/3 como 10 e 20, respectivamente. Clique em **Aplicar**.

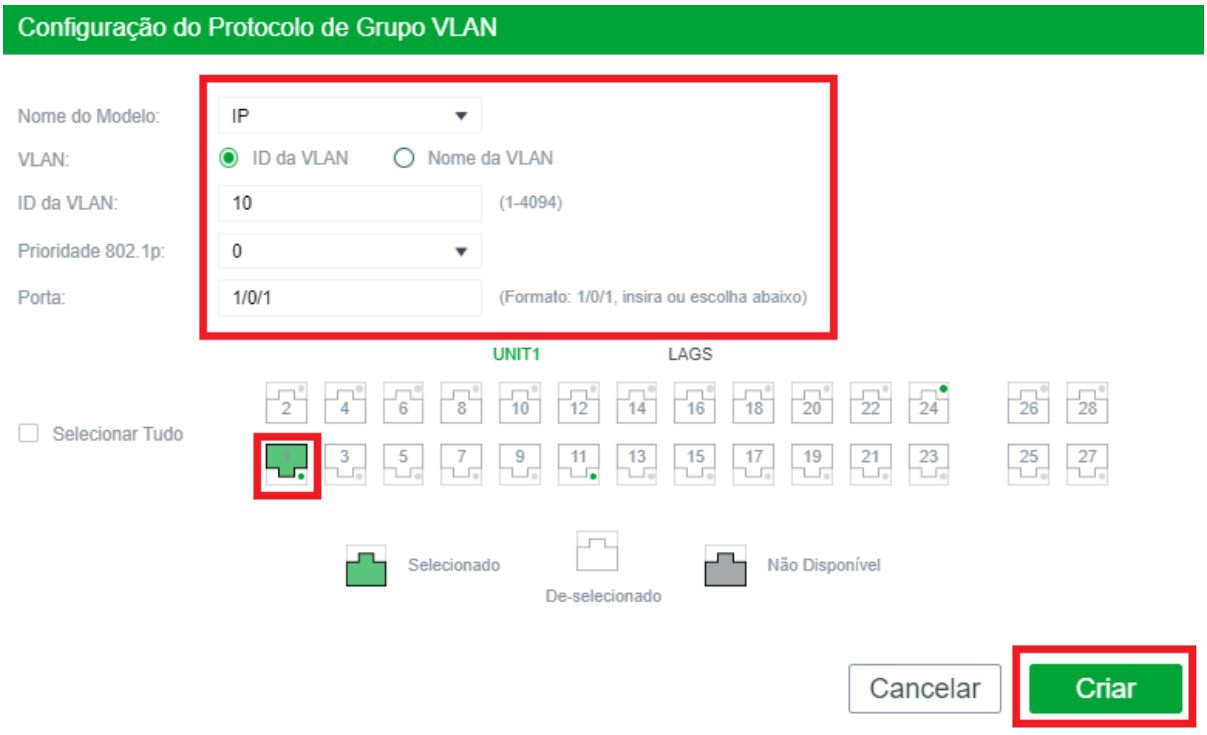


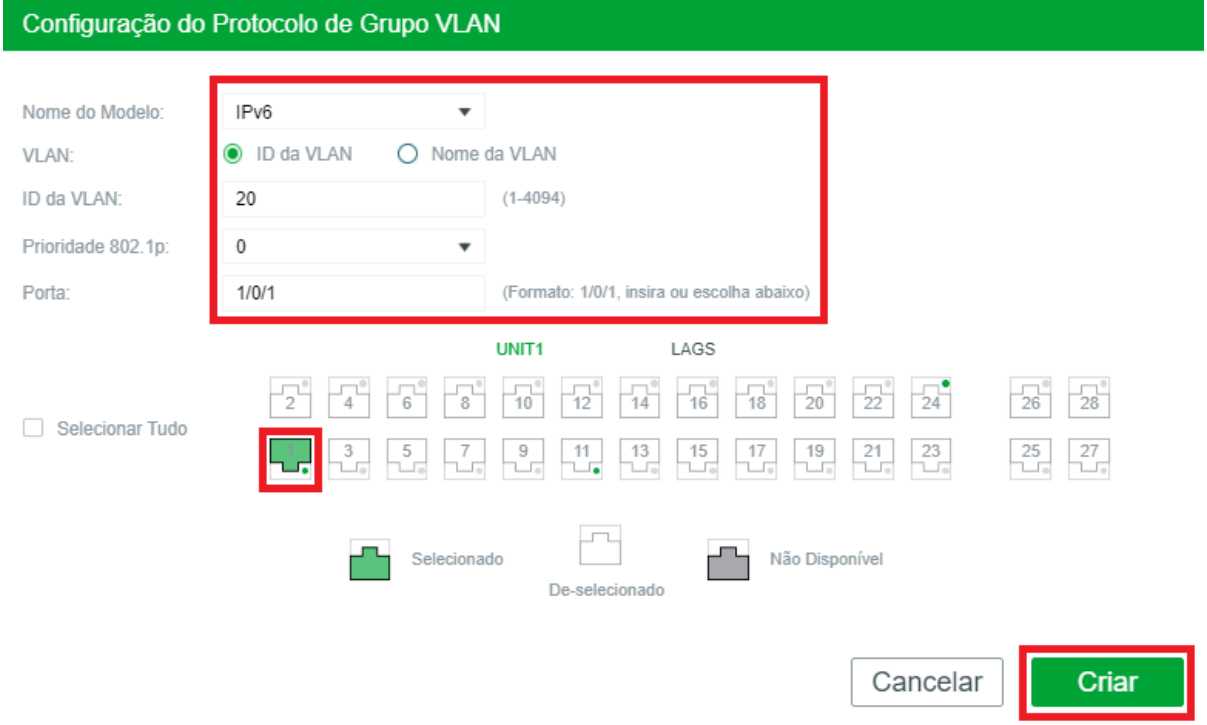
Notas:
As portas membro de um LAG seguem as configurações do LAG, e não suas próprias. As configurações individuais das portas só têm efeito depois que a porta deixa o LAG.

4. Escolha o menu **FUNÇÕES L2 > VLAN > VLAN Protocolo > Modelo de Protocolo** e clique em Adicionar para carregar a página seguinte. Digite IPv6 no nome do protocolo, selecione o tipo de quadro Ethernet II, digite 86DD no campo Ether Type e clique em **Criar** para criar o modelo de protocolo IPv6.

   Dicas: O modelo de protocolo IPv4 já é fornecido pelo switch. Você só precisa criar o modelo de protocolo IPv6.

5. Escolha o menu **FUNÇÕES L2 > VLAN > VLAN Protocolo > Grupo de VLAN Protocolo** e clique em Adicionar para carregar a página seguinte. Selecione o nome do protocolo IP (que é o modelo do protocolo IPv4), digite VLAN ID 10, selecione a porta 1 e clique em Criar. Selecione o nome do protocolo IPv6, digite VLAN ID 20, selecione a porta 1 e clique em **Criar**.





6. Clique em Salvar para salvar as configurações.

Apêndice: Configuração Padrão

Tabela de modelos de protocolo

Configuração Padrão		
1	IP	Ethernet II ether-type 0800
2	ARP	Ethernet II ether-type 0806
3	RARP	Ethernet II ether-type 8035
4	IPX	SNAP ether-type 8137
5	AT	SNAP ether-type 809B

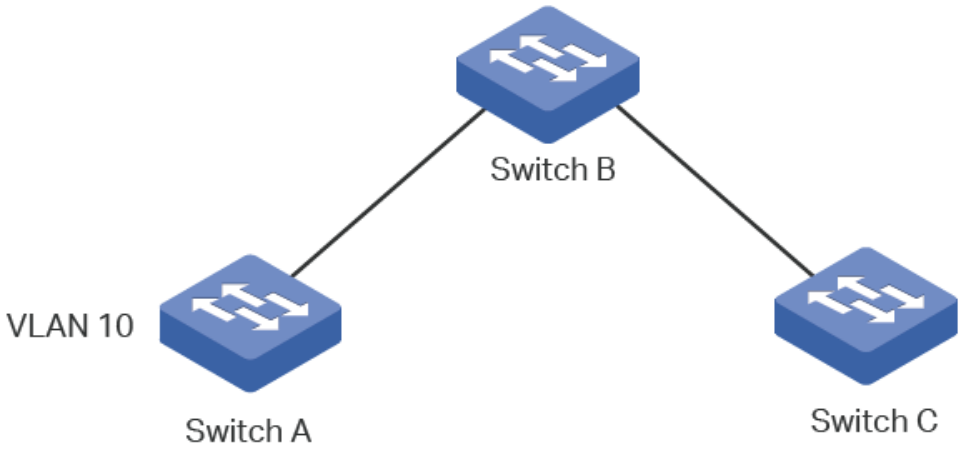
GVRP

Visão Geral

O GVRP (GARP VLAN Registration Protocol) é uma aplicação GARP (Registo atributo genérico Protocol) que permite o registo, e cancelamento do registro de valores de atributos a uma VLAN, e criação de VLAN dinâmica.

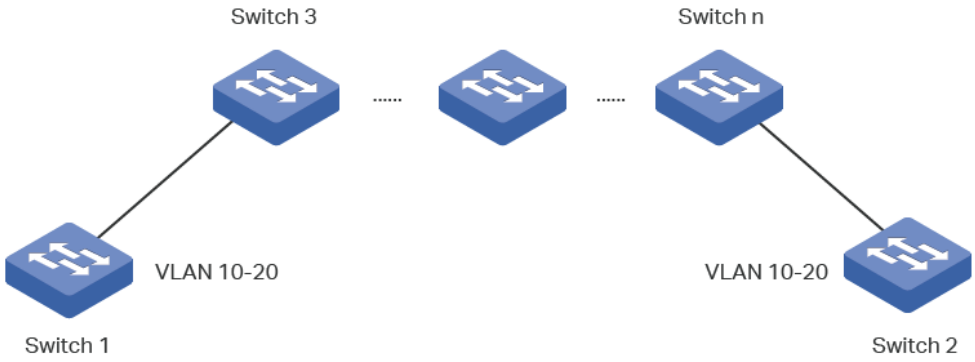
Sem o GVRP em funcionamento, configurando a mesma VLAN em uma rede, seria necessário a configuração manual em cada dispositivo. Conforme mostrado na Figura 1-1, os switches A, B e C estão conectados através de portas de tronco. A VLAN 10 é configurada no switch A, e uma VLAN é configurada no switch B e C.

O switch C pode receber mensagens enviadas do switch A na VLAN 10 única quando o administrador de rede criar manualmente a VLAN 10 no switch B e switch C.



A configuração pode parecer fácil nessa situação. No entanto, para uma rede maior ou mais complexa, com a configuração manual seria necessário muito tempo.

O GVRP pode ser usado para implementar uma configuração de VLAN dinâmica. Com GVRP, o switch pode trocar informações sobre a VLAN de configuração com o switch GVRP adjacente, criar dinamicamente e gerenciar as VLANs. Isto reduz a carga de trabalho na configuração de VLANs e assegura uma VLAN com configuração correta.



Configuração GVRP

Para a configuração completa do GVRP, siga estes passos:

1. Crie uma VLAN.
2. Ativar o GVRP globalmente.
3. Permitir o GVRP em cada porta e configurar os parâmetros correspondentes.

Diretrizes de configuração

Para criar uma VLAN dinamicamente em todas as portas em um link de rede, você deve configurar a mesma VLAN estática em ambas extremidades do link.

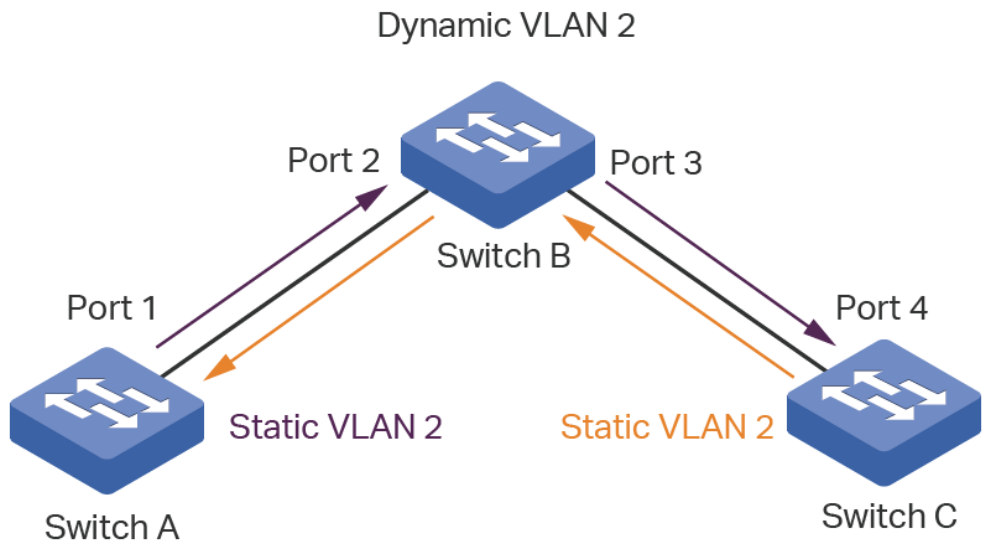
Chamamos de configuração manual quando o VLAN 802.1Q é definido como VLAN estática, e quando a VLAN é criada através do GVRP chamamos de VLAN dinâmica.

As portas em uma VLAN estática podem iniciar o envio de mensagens com registros GVRP para outras portas. E uma porta que registra VLANs somente quando ele recebe mensagens de GVRP.

Como as mensagens só podem ser enviadas a partir de um membro do GVRP para outro, duas vias de registro são necessárias para configurar uma VLAN em todas as portas em um link.

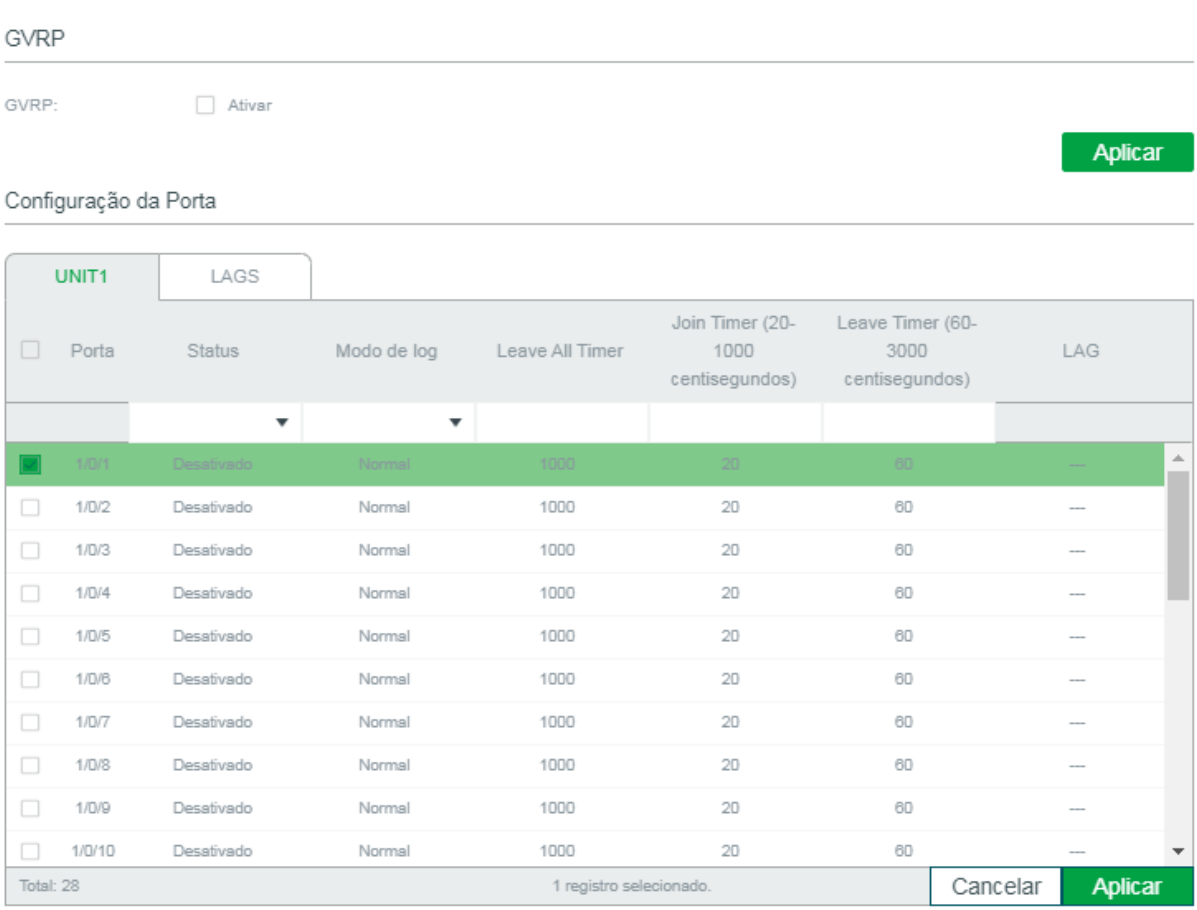
Para implementar o registro bidirecional é necessário configurar manualmente a mesma VLAN estática em ambas das extremidades do link.

Como mostrado na figura abaixo, o registro da VLAN do switch A para o switch C, adiciona a porta 2 para a VLAN 2. E os registros de VLAN do switch C para switch A adiciona a porta 3 para a VLAN 2.



Da mesma forma, se você quiser excluir uma VLAN a partir do link de duas vias, o cancelamento é necessário. E você precisa excluir manualmente a VLAN estática em ambas das extremidades do link.

Vá até o menu **Funções L2 > VLAN > GVRP** para carregar a página a seguir.



Siga esses passos para configurar o GVRP:

1. Na seção GVRP, você deve permitir o GVRP globalmente, e em seguida, clique em **Aplicar**.
2. Na seção **Configuração de Porta**, selecione uma ou mais portas, e defina o status como **Ativar** e configure os parâmetros relacionados de acordo com suas necessidades.

Nome do Modelo	Dê um nome de protocolo para identificar o modelo de protocolo.
Porta	Selecionar a porta desejada para a configuração GVRP.
Status	Ativar ou desativar o GVRP na porta. Por padrão, ele vem desativado.
Registration Mode	Selecione o modo de registro do GVRP para a porta. **Normal:** Neste modo, a porta pode registrar dinamicamente e remover o registro das VLANs, e transmitir as informações de registro da VLAN de ambos de forma dinâmica e estática. **Fixo:** Neste modo, a porta é incapaz de registrar e remover os registros de VLANs dinamicamente, e pode transmitir apenas as informações de registro da VLAN estática. **Proibido:** Neste modo, a porta é incapaz de registrar e remover os registros de VLANs dinamicamente, e pode transmitir apenas as informações da VLAN 1.

LeaveAll Timer (centésimo de segundo)	Quando um membro GARP está habilitado, o temporizador LeaveAll será iniciado. Quando o temporizador LeaveAll expirar, o participante GARP irá enviar mensagens LeaveAll para solicitar os outros membros GARP para registrar novamente todos os seus atributos. Depois disso, o participante reinicia o temporizador LeaveAll. O temporizador varia de 1000 a 30000 centésimo de segundo e deve ser um integrante múltiplo de 5. O valor padrão é 1000 centésimo de segundo.
Join Timer Centésimo de segundo	O Join timer controla o envio de mensagens Join. Um membro GVRP inicia o Join timer após o envio da primeira mensagem de Join. Caso o membro não receba qualquer resposta, ele irá enviar a segunda mensagem de Join quando o Join timer expirar para assegurar que a mensagem foi enviada elas podem ser enviadas para outros membros. O timer varia de 20 a 1000 centésimo de segundo e deve ser um membro múltiplo de 5. O valor padrão é de 20 centésimos de segundo.
Leave Timer (centésimo de segundo)	Os controles de Leave Timer podem atribuir um cancelamento. Um participante irá enviar uma Leave message se ele quer que outros participantes cancelem alguns de seus atributos. O membro que receber a mensagem inicia o temporizador da licença. Se o participante não receber quaisquer Join message do atributo correspondente antes da licença, o timer irá expirar, e o participante removerá o registro do atributo. O temporizador varia de 60 a 3000 centésimo de segundo e deve ser um membro múltiplo de 5. O valor padrão é de 60 centésimos de segundo.
LAG	Irá exibir LAG na porta de entrada.

3. Clique em **Aplicar**.

A porta membro de um LAG segue a configuração do LAG e não a sua própria. As configurações da porta podem ter efeito somente depois que ela deixa o LAG.
A regra de saída das portas adicionadas dinamicamente para a VLAN são tagged.
A regra de saída das portas fixas devem ser tagged.
Ao definir os valores do timer, certifique-se os valores estão dentro do intervalo necessário. O valor de configuração para o LeaveAll deve ser maior ou igual a dez vezes o valor da licença. O valor para a licença deve ser maior ou igual a duas vezes o valor Join.

Exemplo de configuração

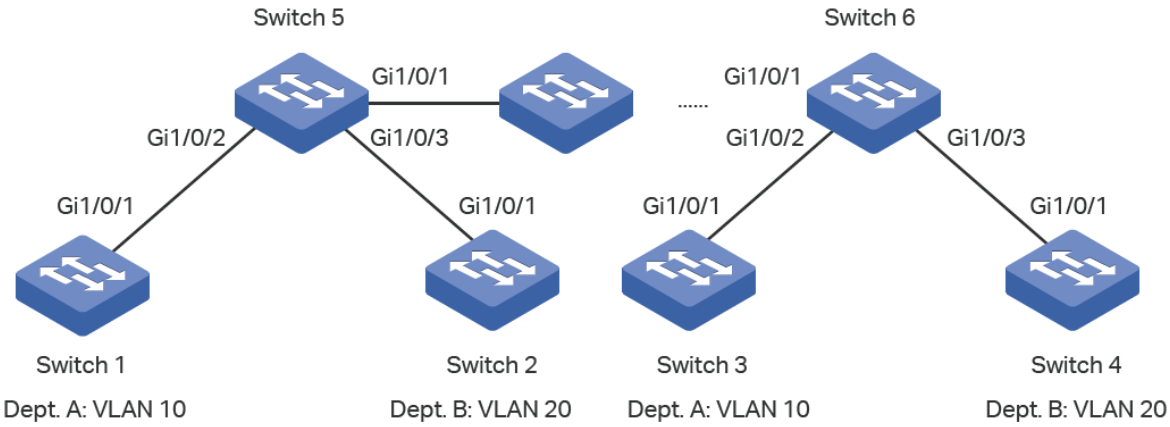
Requisitos de Rede

O departamento de A e o departamento B de uma empresa estão ligados através de switches.

Os escritórios de um departamento são distribuídos em diferentes andares.

Como mostrado na figura abaixo, a topologia da rede é complexa.

A configuração da mesma VLAN em diferentes switches é necessária de modo que os computadores no mesmo departamento possam se comunicar uns com os outros.



Configurando o Cenário

Para reduzir a carga de trabalho com a necessidade de configuração manual e manutenção, o GVRP pode ser habilitado para implementar o registro de VLAN dinâmica, e a atualização sobre os switches.

Ao configurar o GVRP, observe o seguinte:

- Os dois departamentos estão em VLANs separadas. Para garantir que os switches criem dinamicamente a VLAN apenas do seu próprio departamento, você precisa definir o modo de registro para as portas no Switch 1 para o Switch 4 como fixo para impedir o registro e cancelamento de registro dinâmicos.
- Para configurar a criação de VLAN dinâmica em outros switches, defina o modo de registro nas portas correspondentes como normal para permitir o registo dinâmico e de cancelamento VLANs.

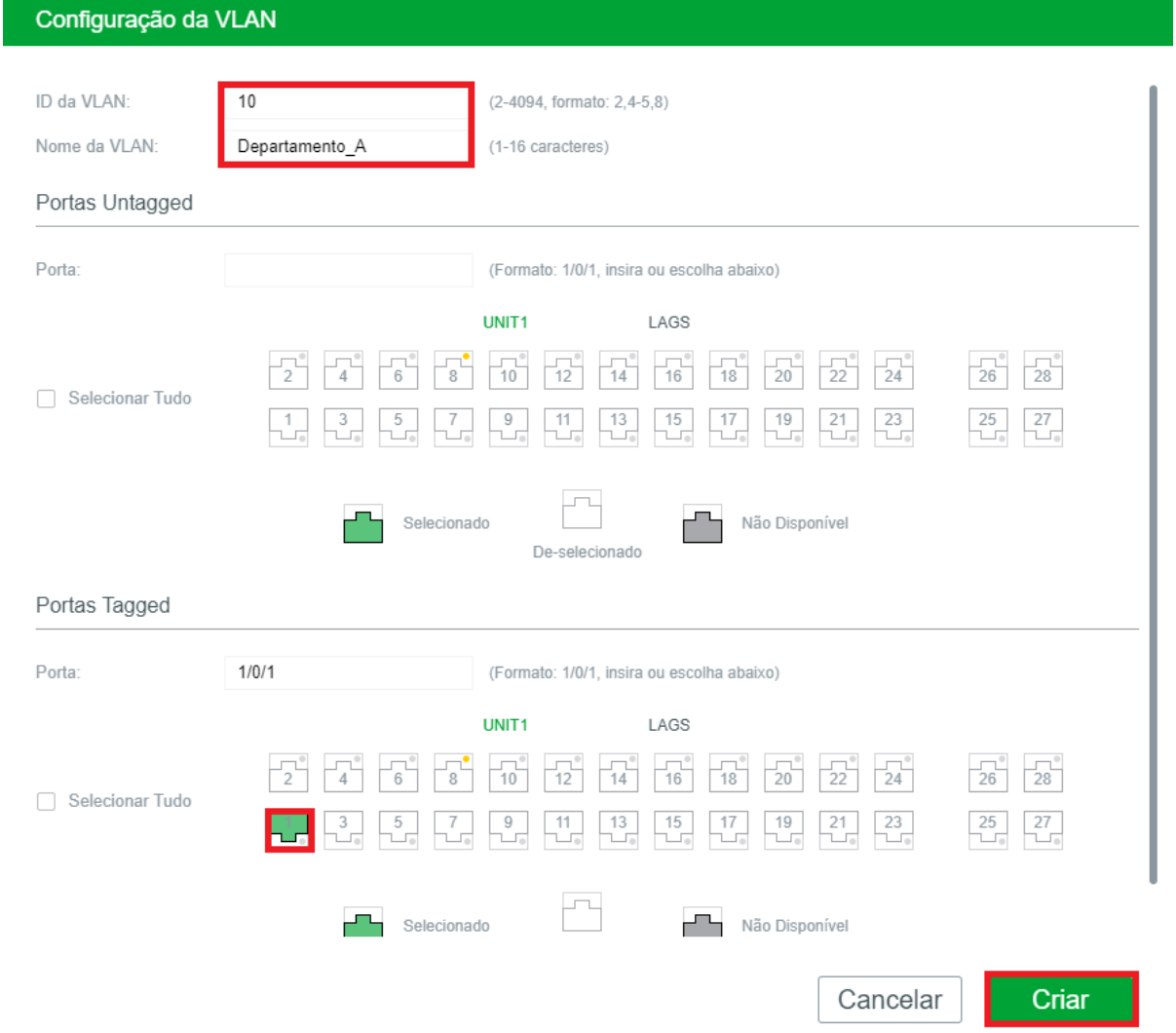
A configuração de GVRP para o switch 3 é a mesma do switch 1, e no switch 4 a mesma configuração do switch 2.

Outros switches podem compartilhar configurações similares.

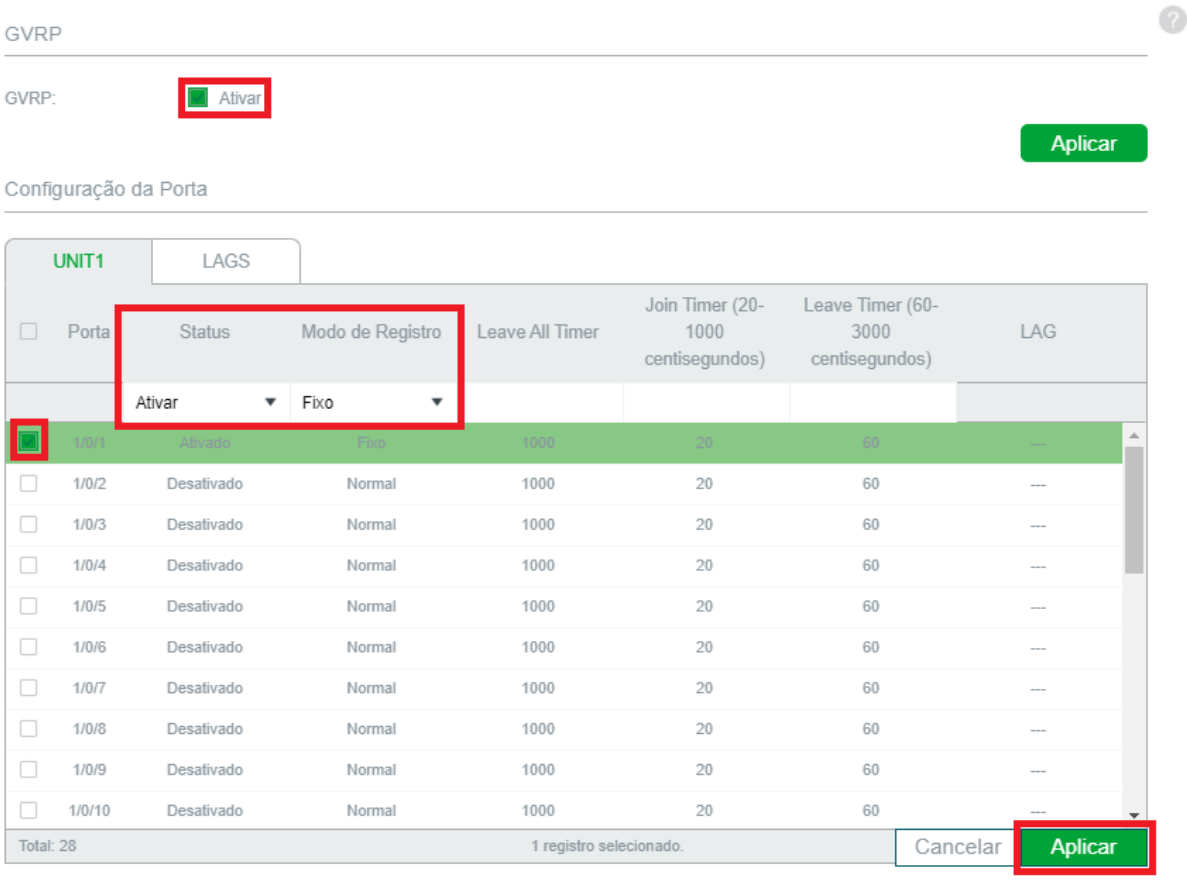
Os seguintes procedimentos de configuração vão ter o Switch 1, Switch 2 e Switch 5 como exemplo.

Configurações do Switch 1

1. Selecione no menu **FUNÇÕES L2 > VLAN > VLAN 802.1Q > Configuração de VLAN** e clique em Adicionar para carregar a página a seguir. Crie a VLAN 10 e marque a porta 1/0/1 como tagged. Clique em **Criar**.



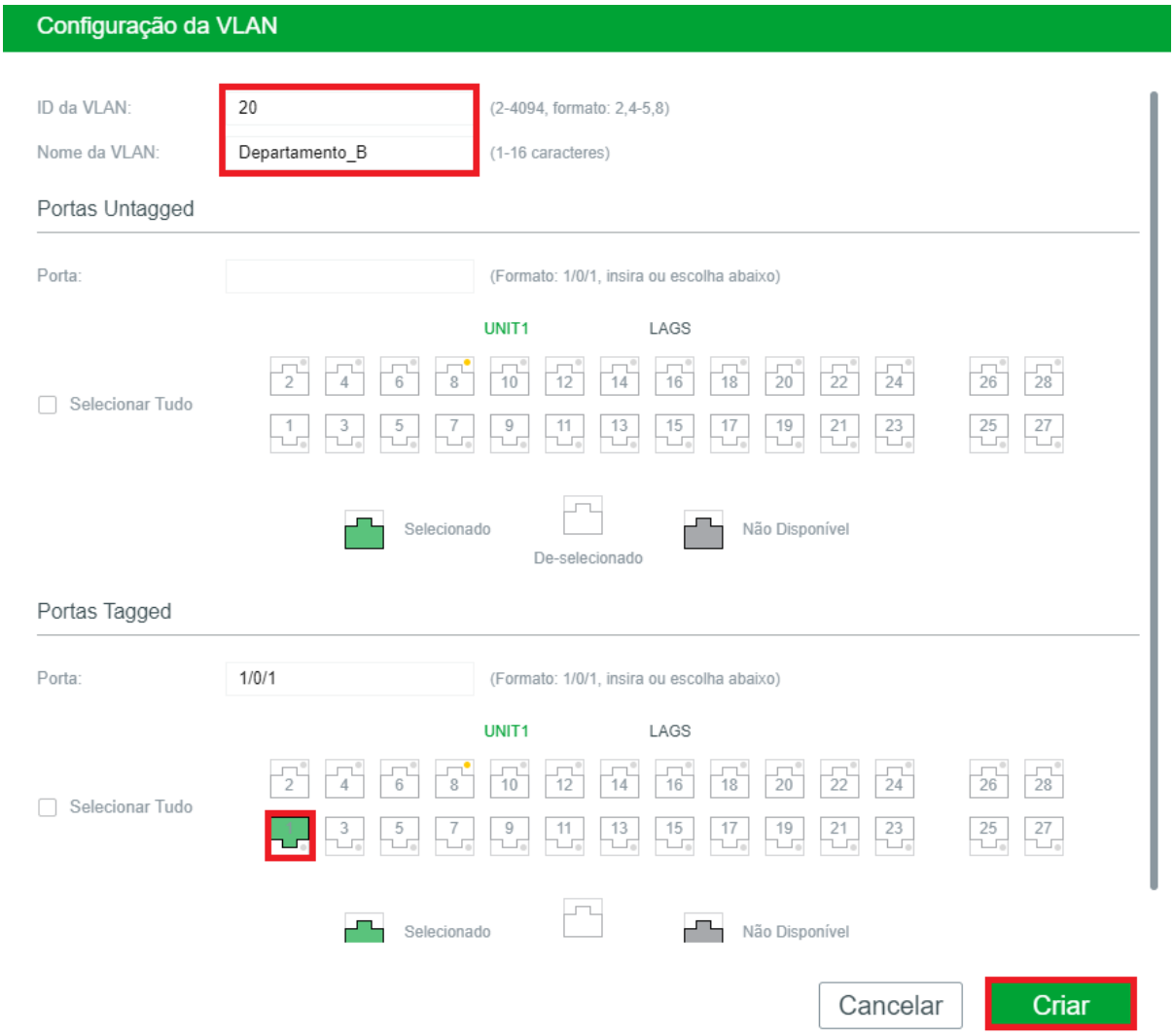
2. Escolha no menu **FUNÇÕES L2 > VLAN > GVRP** para carregar a seguinte página. Habilite o GVPR globalmente, e clique em **Aplicar**. Selecione a porta 1/0/1, e coloque o modo de registro como fixo. Mantenha os valores de tempo padrão. Clique em **Aplicar**.



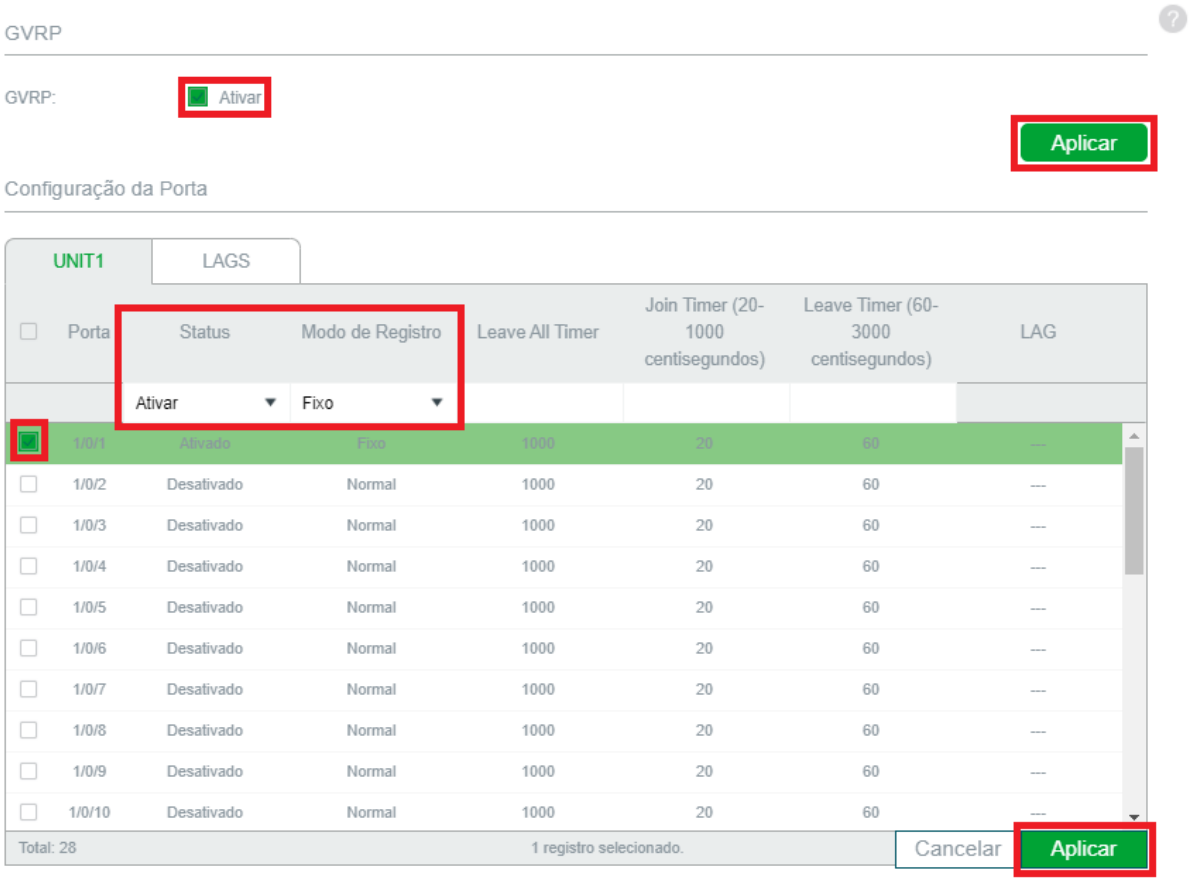
3. Clique em Salvar para salvar as configurações.

Configurações do Switch 2

1. Escolha no menu **FUNÇÕES L2 > VLAN > VLAN 802.1Q > Configuração de VLAN** e clique em Adicionar para carregar a página a seguir. Crie a VLAN 20 e defina a porta 1/0/1 como tagged e clique em **Criar**.



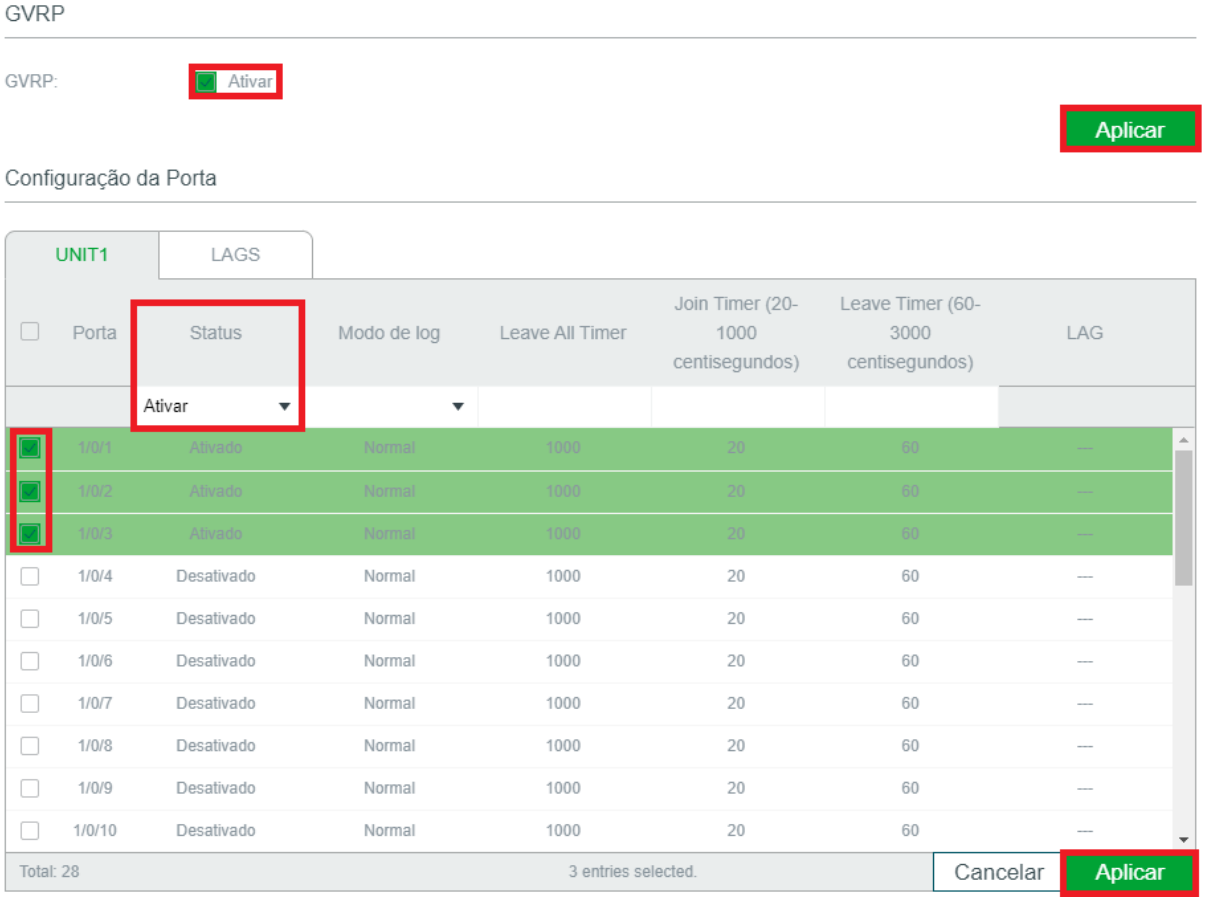
2. Escolha no menu **FUNÇÕES L2 > VLAN > GVRP** para habilitar a página a seguir. Habilite o GVRP globalmente, e clique em **Aplicar**. Selecione a porta 1/0/1, e altere seu estado para Ativo. Mantenha os valores de tempo padrão e clique em **Aplicar**.



3. Clique em Salvar para salvar as configurações

Configurações do Switch 5

1. Escolha no menu **FUNÇÕES L2 > VLAN > GVRP** para carregar a página a seguir. Habilite o GVRP globalmente e clique em **Aplicar**. Selecione a porta 1/0/1~3, e configure o estado dela como Ativo, e mantenha o Modo de Registro e os valores de tempo padrão. Clique em **Aplicar**.



2. Clique em Salvar para salvar as configurações

Apêndice: Configuração Padrão

As configurações padrão de GVRP estão listadas na tabela a seguir.

Tabela Configurações padrão de GVRP

Parâmetros	Configurações Padrão
Configuração Global	
GVRP	Desativar
Configuração da Porta	
Status	Desativar
Modo de log	Normal
Leave All Timer	1000 centésimos de segundo
Join Timer	20 centésimos de segundo
Leave Timer	60 centésimos de segundo

MULTICAST DE CAMADA 2

Visão Geral

Em uma rede ponto-a-multiponto pacotes podem ser enviados de três formas: Unicast, Broadcast e Multicast. No Unicast, muitas cópias da mesma informação serão enviadas para todos os receptores, ocupando uma grande quantidade de banda.

No Broadcast, a informação será enviada a todos os usuários da rede não importando se eles precisam ou não dela, consumindo recursos importantes da rede e impactando negativamente na segurança da informação.

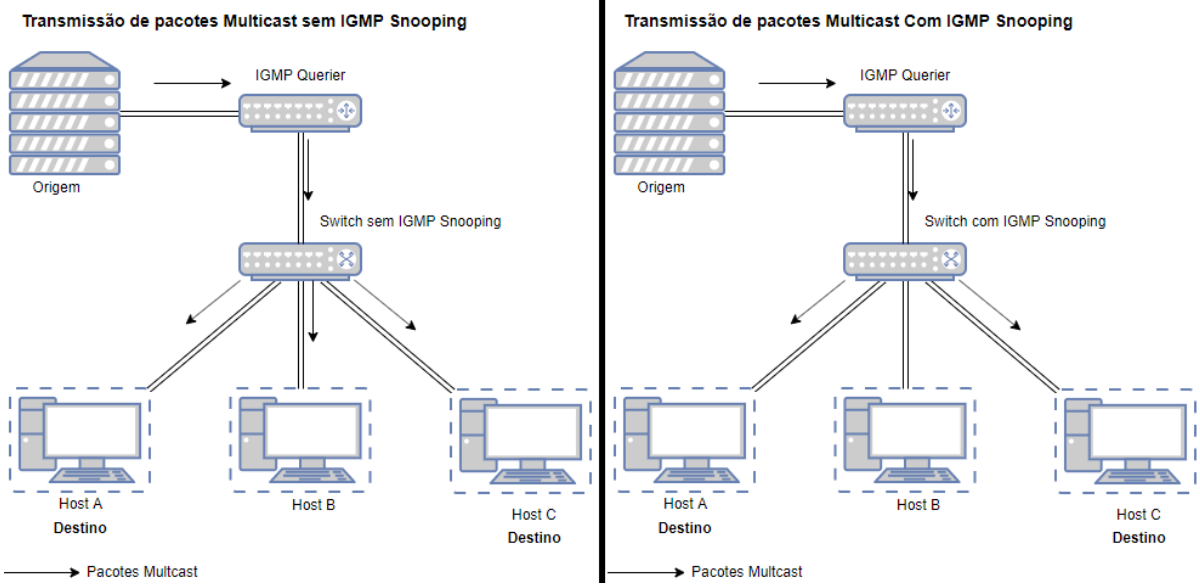
O Multicast resolve todos os problemas causados pelo envio Unicast e Broadcast. Com Multicast, a origem só necessita enviar uma parte da informação e então todos os usuários que necessitam da informação irão recebe-la, e somente eles. Em uma rede ponto-a-multiponto, a tecnologia Multicast não apenas transmite dados com alta eficiência como também economiza largura de banda e reduz a carga da rede.

Em aplicações práticas, provedores de informações da internet podem prover serviços de valor agregado como transmissões ao vivo, IPTV, educação à distância, telemedicina, rádio na internet e conferências de vídeo em tempo real de forma muito mais conveniente usando Multicast.

Multicast de camada 2 permite que switches de camada 2 “escutem” o IGMP (Internet Group Management Protocol) entre os IGMP Queriers e os hosts de usuário para estabelecer a tabela de encaminhamento Multicast e para gerenciar e controlar as transmissões de pacotes.

Tomando o IGMP Snooping como exemplo. Quando o mesmo é desabilitado em dispositivos de camada 2, pacotes Multicast serão transmitidos na forma de broadcast na rede de camada 2. Quando o IGMP Snooping está ativado nos dispositivos de camada 2, dados Multicast de um grupo conhecido serão transmitidos para os destinos designados ao invés de ser transmitido como Broadcast.

Como demonstrado abaixo:



Os conceitos básicos de IGMP Snooping como IGMP Querier, Snooping Switch, Porta roteada e Porta Membro serão introduzidos abaixo:

- **IGMP Querier**

  Um IGMP Querier é um roteador Multicast (um roteador ou switch de camada 3) o qual encaminha mensagens de consulta para manter uma lista de membros de um grupo Multicast para cada rede conectada e um timer para cada membro.

  Normalmente somente um dispositivo age como Querier para cada rede física. Se houver mais que um roteador Multicast na rede um processo de escolha de Querier será implementado para determinar qual agirá como Querier.

- **Snooping Switch**

  Um snooping switch indica um switch com IGMP Snooping habilitado. Os switches mantem uma tabela de encaminhamento Multicast através do Snooping das transmissões IGMP entre o Querier e o host. Com a tabela de encaminhamento Multicast, o switch pode encaminhar os dados Multicast somente para as portas as quais participam do grupo Multicast, de forma a restringir o Flooding para dados Multicast na rede de camada 2.

- **Porta roteadora**

  Uma porta roteadora é uma porta no snooping switch a qual é conectada ao IGMP Querier.

- **Porta Membro**

  Uma Porta Membro é uma porta no snooping switch que está conectada à um host.

Funções Suportadas

- **Protocolo Multicast de camada 2 para IPv4: IGMP Snooping**

Em dispositivos de camada 2, o IGMP Snooping transmite dados em demanda na camada de link, através da análise dos pacotes IGMP trocados entre o IGMP Querier e o usuário, o dispositivo consegue construir e manter uma tabela de encaminhamento de Multicast Camada 2.

- **Protocolo Multicast de camada 2 para IPv6: MLD Snooping**

  Em dispositivos de camada 2, o MLD (Multicast Listener Discovery Snooping) Snooping transmite dados em demanda na camada de link, através da análise dos pacotes MLD trocados entre o MLD Querier e o usuário, o dispositivo consegue construir e manter uma tabela de encaminhamento de Multicast de camada 2.

- **Multicast VLAN Registration (MVR)**

  MVR permite que uma única VLAN Multicast seja dividida entre portas membros do Multicast em diferentes VLANs nas redes IPv4. No IGMP Snooping, se uma porta membro estiver em uma VLAN diferente, uma cópia do stream de Multicast é encaminhada para cada VLAN que tenha portas membro. Já o MVR proporciona uma VLAN Multicast dedicada para encaminhar trafego Multicast através das redes de camada 2. Os clientes podem entrar ou sair de forma dinâmica dessa VLAN Multicast dedicada sem interferir com seu relacionamento com outras VLANs. Existem dois Modos MVR:

  - **Modo Compatibilidade:**
    No modo de compatibilidade, o switch MVR não encaminha mensagens de report ou leave dos hosts para o IGMP Querier. Então o IGMP Querier não consegue aprender as informações dos membros do grupo de Multicast do switch MVR. Você terá que configurar manualmente o IGMP Querier para transmitir todos os streams Multicast requisitados para o switch MVR através da VLAN de Multicast.

  - **Modo Dinâmico:**
    No modo dinâmico, depois de receber as mensagens de report ou leave dos hosts, o switch MVR as encaminhará para o IGMP Querier através da VLAN de Multicast (com a devida tradução da VLAN ID). Então o IGMP Querier poderá aprender as informações dos membros do grupo Multicast através das mensagens de report e leave, e transmitir os streams Multicast para o switch MVR através da VLAN de Multicast de acordo com a tabela de encaminhamento Multicast.

- **Filtragem Multicast**

  A Filtragem Multicast permite você controlar o conjunto de grupos Multicast aos quais um host pode pertencer. Você pode filtrar o ingresso à grupos Multicast baseado em portas configurando o IP dos perfis Multicast (IGMP ou MLD) associando eles a portas individuais do switch.

Configuração IGMP Snooping

Para completar a configuração do IGMP Snooping siga os seguintes passos:

1. Habilite globalmente o IGMP Snooping e configure os parâmetros globais;

2. Configure o IGMP Snooping para VLANs;
3. Configure o IGMP Snooping para portas;
4. (Opcional) Configure para participar de um grupo de forma estática.

IGMP Snooping só terá efeito nas portas e VLANs correspondentes quando habilitado de forma global.

Configurando IGMP Snooping Global

Vá até o menu **FUNÇÕES L2 > Multicast > IGMP Snooping > Configuração globais** para carregar a seguinte página:

Siga os seguintes passos para configurar o IGMP Snooping de forma global:

1. Na seção **Configuração Global**, habilite o IGMP Snooping globalmente e configure os parâmetros globais.

IGMP Snooping	Habilite ou desabilite o IGMP Snooping de forma global.
Versão IGMP	Especifique a versão IGMP: **v1:** O switch funcionará como um IGMPv1 Snooping switch. Ele só irá processar mensagens IGMPv1 dos hosts. Mensagens de outras versões serão ignoradas. **v2:** O switch funcionará como um IGMPv2 Snooping switch. Ele só irá processar mensagens IGMPv1 e IGMPv2 dos hosts. Mensagens de outras versões serão ignoradas. **v3:** O switch funcionará como um IGMPv3 Snooping switch. Ele só irá processar mensagens IGMPv1, IGMPv2 e IGMPv3 dos hosts.

Grupos Multicast Desconhecidos	Configure o caminho no qual o switch processará os dados que forem enviados para um grupo Multicast desconhecido como Encaminhar ou Descartar. Por padrão vem configurado como Encaminhar. Grupos Multicast desconhecidos são grupos que não possuem correspondência no anúncio de grupos previamente reportados pelo IGMP membership report, e, portanto, não podem ser encontrados na tabela de encaminhamento do Switch. **Nota:** GMP Snooping e MLD Snooping compartilham as configurações de grupos Multicast desconhecidos, então será necessário habilitar o MLD Snooping de forma global no menu **FUNÇÕES L2 > Multicast > MLD Snooping > Configurações Globais**.
Validação de Cabeçalho	Habilita ou desabilita a validação de cabeçalho. Por padrão vem desabilitado. Genericamente, para pacotes IGMP, o valor TTL deve ser 1, Campo ToS deve ser 0xC0 e a opção Router Alert deve ser 0x94040000. Os campos para serem validados dependem de qual versão o IGMP está usando. IGMPv1 verifica somente o campo de TTL. IGMPv2 verifica o campo de TTL e a opção de Router Alert. IGMPv3 verifica os três campos. Pacotes que falham na validação são descartados.

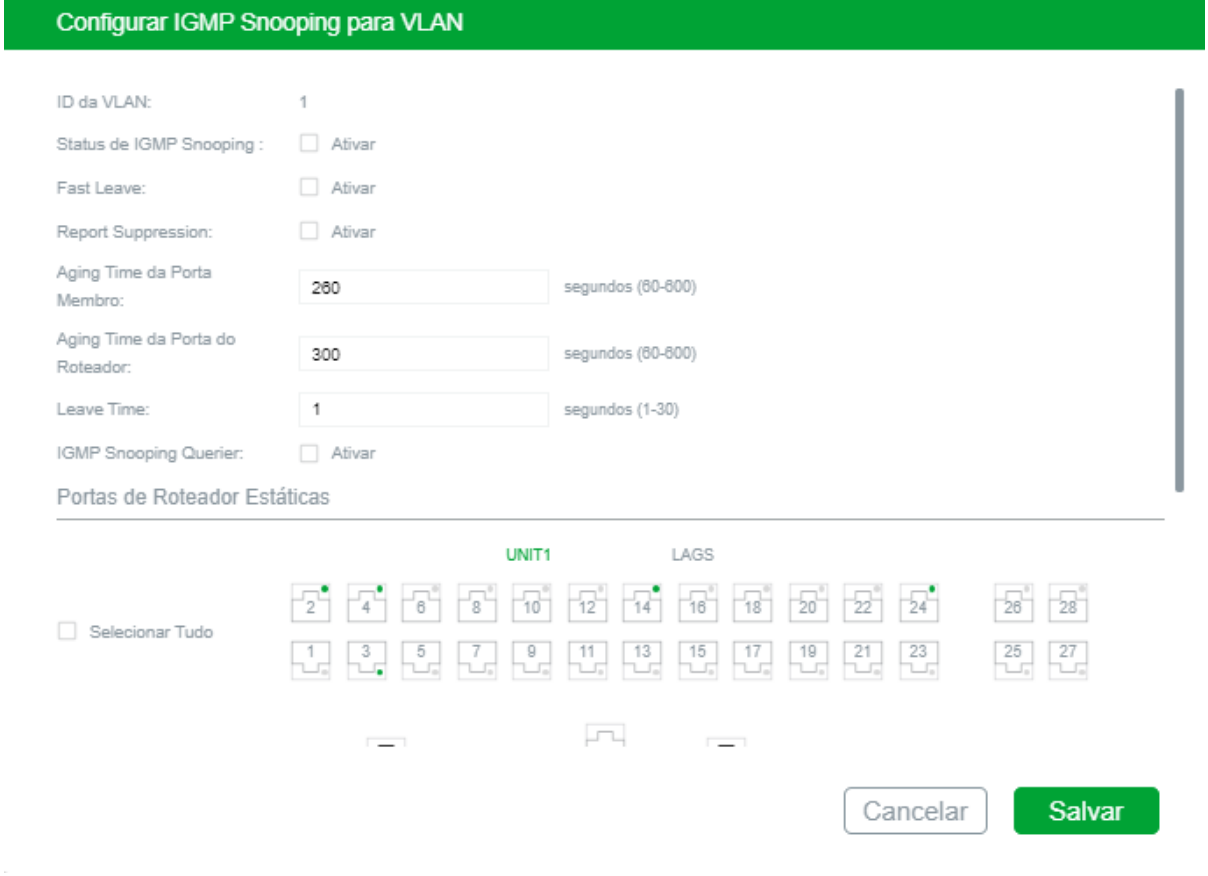
2. Clique em **Aplicar**.

IGMP Snooping para VLANs

Antes de configurar o IGMP Snooping para VLANs, configure as VLANs que as portas roteadoras e as portas membros estão. Para mais detalhes vá para Configuração da VLAN 802.1Q.

O switch suporta configurações IGMP Snooping baseadas em VLAN. Após habilitar o IGMP Snooping globalmente, você também precisará habilitar e configurar os parâmetros correspondentes do IGMP Snooping para as VLANs que a Porta roteadora e as Portas Membro estão.

Vá até o menu **FUNÇÕES L2 > Multicast > IGMP Snooping > Configuração global** clique em na entrada de VLAN desejada na seção **IGMP VLAN Config** para carregar a seguinte página.



Siga os seguintes passos para configurar o IGMP para uma VLAN específica:

1. Habilite o IGMP Snooping para a VLAN e configure os parâmetros correspondentes.

VLAN ID	Exibe a VLAN ID.
IGMP Snooping	Habilita ou desabilita o IGMP Snooping para a VLAN.

Fast Leave	Habilita ou desabilita o Fast Leave para a VLAN. IBMPv1 não suporta esta função. Sem Fast Leave, após o host enviar uma mensagem IGMP Leave para sair do grupo Multicast, o switch irá encaminhar esta mensagem para o dispositivo de Camada 3 (Querier). No ponto de vista do Querier, a porta conectada no switch é uma porta membro de um grupo Multicast correspondente. Após receber a mensagem de Leave do switch, o Querier irá enviar um número de configuração (Last Member Query Count) para pesquisas do grupo específico em qual a porta está com o intervalo configurado (Last Member Query Interval), e irá aguardar pelos membership reports para o grupo IGMP. Se existir outros hosts pertencentes ao grupo conectados ao switch eles irão responder à consulta antes que o Last Member Query Interval expire. Se não forem recebidos nenhum report após o tempo de resposta o Querier irá remover a porta da lista de encaminhamento do grupo Multicast correspondente. Ou seja, se houverem outros hosts pertencentes ao grupo conectados ao switch, aquele que enviou uma leave message precisará aguardar até que seu Aging time expire para sair da lista de encaminhamento do grupo Multicast correspondente (O tempo máximo de espera é decidido pelo Aging Time da Porta Membro). Com Fast Leave habilitado em uma VLAN, o switch irá remover a entrada (Grupo de Multicast, Porta, VLAN) da tabela de encaminhamento Multicast antes de encaminhar a mensagem de leave para o Querier. Isso ajuda a reduzir o desperdício de banda uma vez que o switch não precisará enviar streams de Multicast para aquela porta
Supressão de Report	Habilita ou desabilita a supressão de report para a VLAN. Quando habilitada, o switch somente encaminhará a primeira mensagem de report de cada grupo Multicast para o IGMP Querier e irá suprimir as mensagens de report subsequentes do mesmo grupo durante o período do query interval. Essa função previne que mensagens de report duplicadas sejam enviadas ao IGMP Querier.

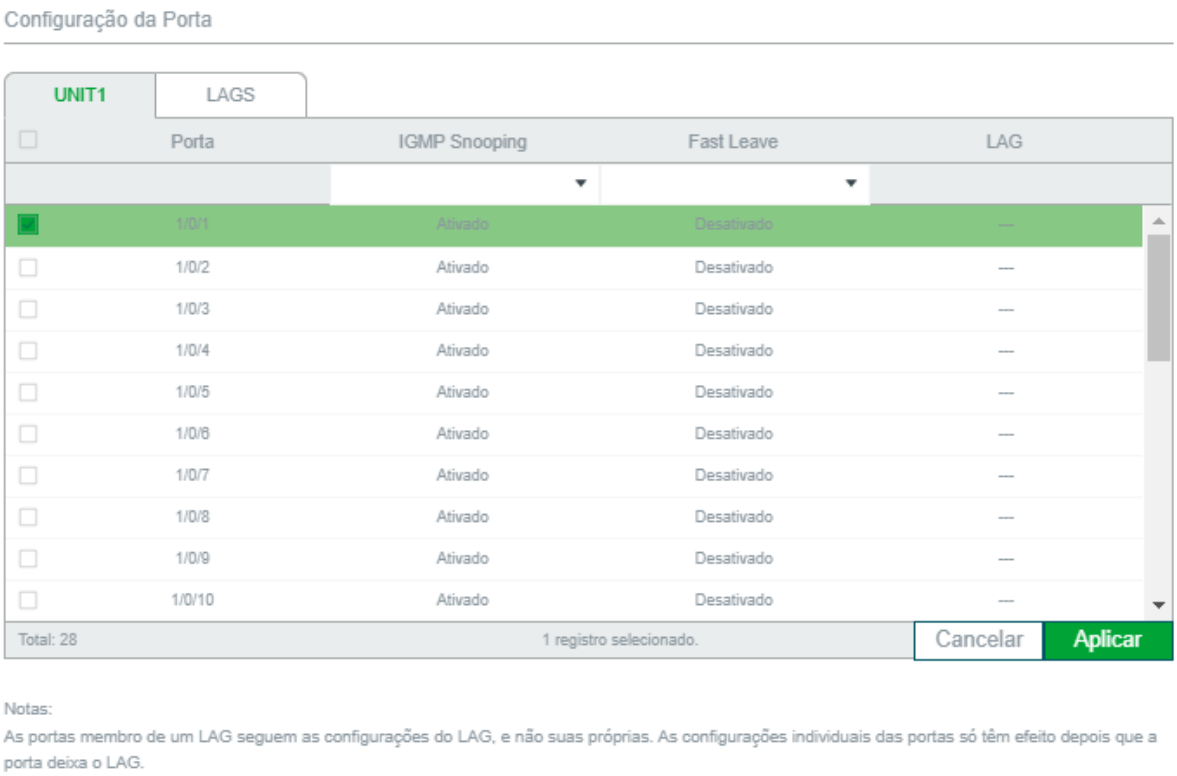
Aging Time da Porta Membro	Especifica o aging time para as portas membro na VLAN. Uma vez que o switch receba uma mensagem de IGMP membership report de uma porta, o switch adicionará essa porta à lista de portas membro do correspondente grupo Multicast. As portas membro que são aprendidas dessa forma são Portas membro dinâmicas. Se o switch não receber qualquer mensagem de IGMP Membership report de uma porta membro dinâmica de um grupo Multicast específico após o aging time expirar essa porta não será mais considerada como uma porta membro do grupo Multicast e será deletada de sua tabela de encaminhamento.
Aging Time da Porta roteadora	Especifica o aging time para as portas roteadoras na VLAN. Uma vez que o switch receba uma mensagem de IGMP general query de uma porta, o switch adicionará essa porta para a lista de portas roteadoras. Portas roteadoras que são aprendidas dessa forma são chamadas portas roteadoras dinâmicas. Se o switch não receber qualquer mensagem IGMP general query de uma porta roteadora dinâmica durante o período do aging time, após o aging time expirar o switch não considerará mais essa porta como uma porta roteadora e irá deletar ela da lista de portas roteadoras.
Leave Time	Especifica o leave time para a VLAN. Quando o switch recebe uma mensagem leave de uma porta para deixar o grupo de Multicast, ele irá esperar o tempo de leave time antes de remover a porta do grupo de Multicast. Durante o período, se o switch receber qualquer mensagem de report vinda dessa porta, ele não será removido da lista do grupo de Multicast. Exceções: 1 - Caso o aging time da porta expire antes do leave time e nenhum report for recebido a porta será removida do grupo Multicast uma vez que o Aging time de porta Membro expirar. 2 - O mecanismo de Leave Time não terá efeito quando o Fast Leave estiver habilitado. Um valor de leave time apropriado pode evitar que outros hosts que se conectem à mesma porta do switch sejam removidos por engano de um grupo Multicast quando somente alguns deles quiserem sair.

IGMP Snooping Querier	Habilita ou desabilita o IGMP Snooping Querier para a VLAN. Quando habilitado, o switch age como um IGMP Snooping Querier para os hosts nessa VLAN. O query irá enviar uma mensagem periodicamente para essa rede solicitando as informações dos membros do grupo Multicast, e enviará queries específicas quando receber mensagens de leave vindo dos hosts.
Intervalo de Query	Com o IGMP Snooping Querier habilitado, especifique o intervalo entre as mensagens de General Query que serão enviadas pelo switch.
Tempo de resposta máxima	Com o IGMP Snooping Querier habilitado, especifique o tempo máximo de resposta para as mensagens de general query.
Last Member Query Interval	Com o IGMP Snooping Querier habilitado, quando o switch receber uma mensagem de leave, ele obterá o endereço do grupo Multicast ao qual o host pretende deixar de participar. Então o switch enviará queries específicos de grupo para este grupo Multicast através dessa porta a qual ele recebeu a mensagem de leave. Este parâmetro determina o intervalo entre as consultas específicas de grupo.
Last Member Query Count	Com o IGMP Snooping Querier habilitado, especifique o número de queries especificas de grupo a serem enviados. Se o contador específico de grupo for enviado e não forem recebidas mensagens de reports, o switch irá deletar o endereço de Multicast da tabela de encaminhamento Multicast.
General Query Source IP	Com o IGMP Snooping Querier habilitado, especifique o endereço IP de origem para as mensagens de general query enviadas pelo switch. Deve ser um endereço Unicast.
Portas roteadoras estáticas	Selecione uma ou mais portas para serem portas roteadoras estáticas na VLAN. Portas roteadoras estáticas não sofre efeitos do aging time. Streams Multicast e pacotes IGMP para todos os grupos desta VLAN serão encaminhados através das portas roteadoras estáticas. Streams Multicast e pacotes IGMP pata grupos que tem portas roteadoras dinâmicas também serão encaminhadas através da correspondente porta roteadora dinâmica.
Portas roteadoras proibidas	Selecione as portas que serão proibidas de serem portas roteadoras na VLAN.

2. Clique em **Aplicar**.

IGMP Snooping para Portas

Vá até o menu **FUNÇÕES L2 > Multicast > IGMP Snooping > Configuração de Porta** para carregar a seguinte página.



Siga os seguintes passos para configurar o IGMP Snooping para portas:

1. Habilite o IGMP Snooping para as portas e habilite o Fast Leave se houver apenas um host Multicast conectado à porta.

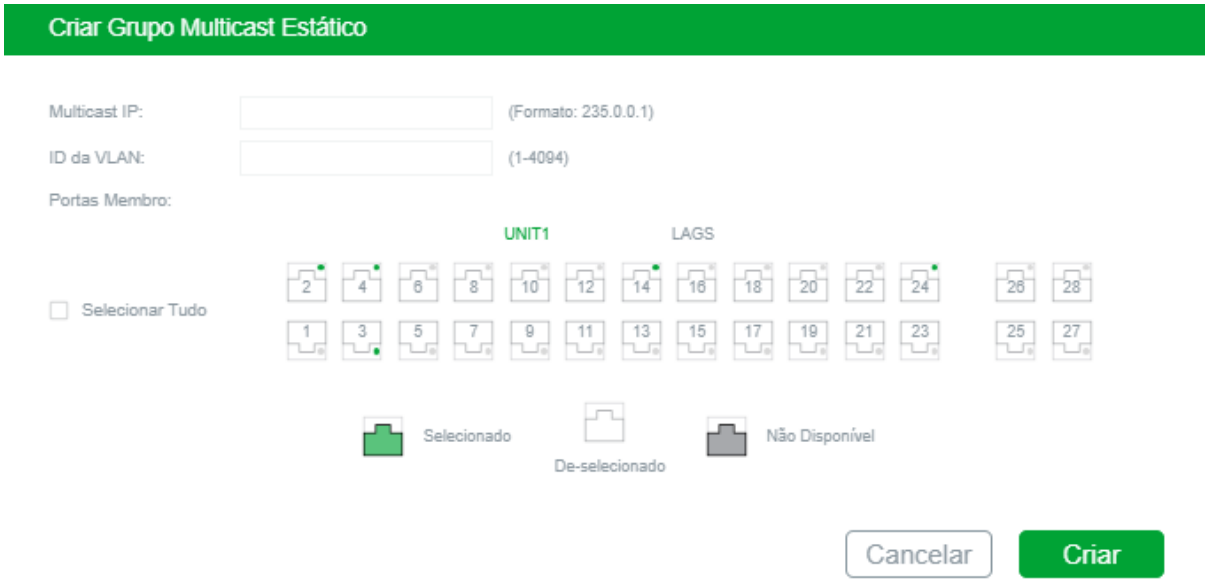
IGMP Snooping	Habilite ou desabilite o IGMP Snooping para a porta.
Fast Leave	Habilite ou desabilite o Fast Leave para a porta. IGMPv1 não suporta Fast Leave. Fast Leave pode ser habilitado tanto para porta como para VLAN. Quando habilitado no formato baseado em porta, o switch irá remover a porta do correspondente grupo Multicast de todas as VLANs antes de encaminhar a mensagem de leave para o Querier. Você somente deve utilizar Fast Leave baseado em portas quando existir um único host Multicast conectado à porta. Para mais detalhes sobre o Fast Leave veja Configurando IGMP Snooping para VLANs.
LAG	Mostra o LAG ao qual a porta pertence.

2. Clique em **Aplicar**.

Ingresso Estático de Hosts para os Grupos Multicast

Portas de camada 2 e hosts normalmente ingressam em grupos Multicast dinamicamente, mas você pode configurar hosts estáticos para os grupos.

Vá até o menu **FUNÇÕES L2 > Multicast > IGMP Snooping > Configuração estática de grupo** clique em Adicionar para carregar a seguinte página.



Siga os seguintes passos para configurar ingressos estáticos para grupos Multicast.

1. Especifique o endereço IP Multicast e o VLAN ID. Selecione as portas que serão membros estáticos do grupo Multicast.

IP Multicast	Especifique o endereço do grupo Multicast que os hosts irão ingressar.
VLAN ID	Especifique a VLAN a qual os hosts pertencem.
Portas Membro	Selecione as portas à quais os hosts estão conectados. Essas portas se tornaram membros estáticos do grupo Multicast e não sofrerão o efeito do aging time.

2. Clique em **Criar**.

MLD Snooping

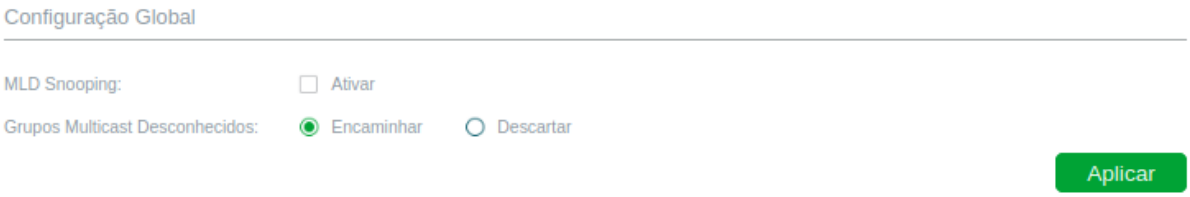
Para realizar a configuração do MLD Snooping siga os passos a seguir:

1. Habilite o MLD Snooping de forma global e configure os parâmetros globais;
2. Configure MLD Snooping para as VLANs;
3. Configure MLD Snooping para as portas;
4. (Opcional) Configure os hosts para ingressar o grupo de forma estática.

> MLD Snooping só toma efeito quando é habilitado de forma global correspondentemente para VLANs e portas.

Configurando MLD Snooping Global

Vá até o menu **FUNÇÕES L2 > Multicast > MLD Snooping > Configuração globais** para carregar a seguinte página:



Siga os seguintes passos para configurar o MLD Snooping de forma Global.

1. Na seção **Configuração Global** habilite o MLD Snooping e configure as funções globais dos grupos de Multicast desconhecido.

MLD Snooping	Habilite ou desabilite o MLD Snooping de forma global.
Grupos de Multicast desconhecido	Configure a forma com a qual o switch irá processar dados que são enviados por um grupo de Multicast desconhecido como Encaminhar ou Descartar. Por padrão é configurado como Encaminhar. Grupos de Multicast desconhecidos são grupos de Multicast que não tem correspondência de nenhum grupo anunciado previamente pelos report de membro de IGMP e, portanto, não podem ser encontrados na tabela de encaminhamento Multicast do switch. **Nota:** IGMP Snooping e MLD Snooping compartilham as mesmas configurações de grupos de Multicast desconhecidos, então você deve habilitar o IGMP Snooping globalmente em **FUNÇÕES L2 > Multicast > IGMP Snooping > Configuração global** concomitantemente com o MLD.

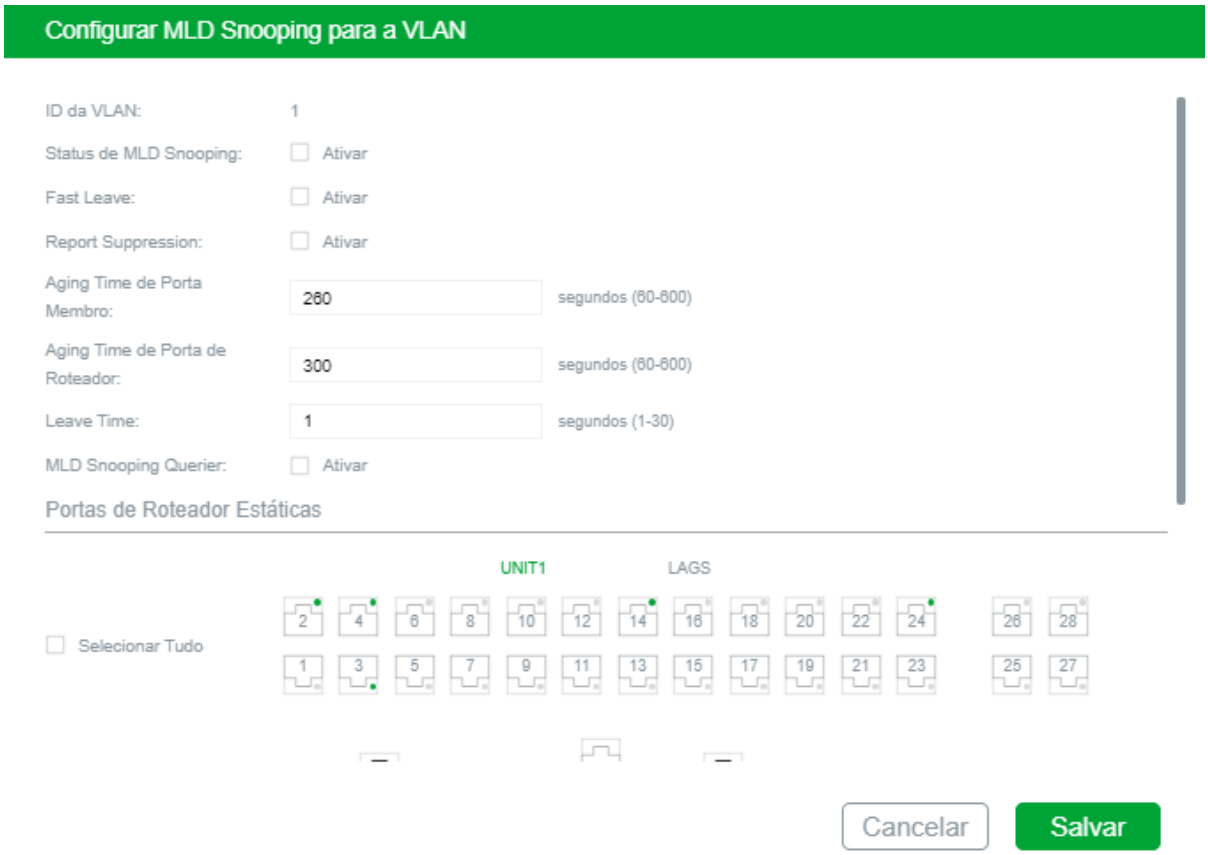
2. Clique em **Aplicar**.

MLD Snooping para VLANs

Antes de configurar o MLD Snooping para VLANs, configure as VLANs que as portas roteadoras e as portas membros estão. Para mais detalhes vá para Configuração da VLAN 802.1Q.

O switch suportas configurações MLD Snooping baseada em VLAN. Após habilitar o MLD Snooping globalmente, você também precisará habilitar e configurar os parâmetros correspondentes para as VLANs que as portas roteadoras e as portas membros estão conectadas.

Vá até o menu **FUNÇÕES L2 > Multicast > MLD Snooping > Configuração Global** clique em na entrada de VLAN desejada na seção **Configuração MLD VLAN** para carregar a seguinte página.



Siga os seguintes passos para configurar o MLD Snooping para uma VLAN específica.

1. Habilite o MLD Snooping para a VLAN e configure os correspondentes parâmetros.

VLAN ID	Exibe a VLAN ID.
IGMP Snooping	Habilita ou desabilita o IGMP Snooping para a VLAN.

Fast Leave	Habilita ou desabilita o Fast Leave para a VLAN. IBMPv1 não suporta esta função. Sem Fast Leave, após o host enviar uma mensagem MLD done (equivalente à mensagem de leave no IGMP) para sair do grupo Multicast, o switch irá encaminhar esta mensagem para o dispositivo de Camada 3 (Querier). No ponto de vista do Querier, a porta conectada no switch é uma porta membro de um grupo Multicast correspondente. Após receber a mensagem done do switch, o Querier irá enviar um número de configuração (Last Listener Query Count) para pesquisas de Endereço Multicast específico (MASQs Multicast-Add) em qual a porta está com o intervalo configurado (Last Listener Query Interval), e irá aguardar pelos membership reports para o grupo MLD. Se existir outros hosts pertencentes ao grupo conectados ao switch eles irão responder à consulta de endereço Multicast específico antes que o Last Listener Query Interval expire. Se não forem recebidos nenhum report após o tempo de resposta o Querier irá remover a porta da lista de encaminhamento do grupo Multicast correspondente. Ou seja, se houverem outros hosts pertencentes ao grupo conectados ao switch, aquele que enviou uma leave message precisará aguardar até que seu Aging time expire para sair da lista de encaminhamento do grupo Multicast correspondente (O tempo máximo de espera é decidido pelo Aging Time da Porta Membro). Com Fast Leave habilitado em uma VLAN, o switch irá remover a entrada (Grupo de Multicast, Porta, VLAN) da tabela de encaminhamento Multicast antes de encaminhar a mensagem de done para o Querier. Isso ajuda a reduzir o desperdício de banda uma vez que o switch não precisará enviar streams de Multicast para aquela porta da VLAN tão rapidamente quanto o switch recebe a mensagem de done.
Supressão de Report	Habilita ou desabilita a supressão de report para a VLAN. Quando habilitada, o switch somente encaminhará a primeira mensagem de MLD report de cada grupo Multicast para o MLD Querier e irá suprimir as mensagens de report subsequentes do mesmo grupo durante o período do query interval. Essa função previne que mensagens de report duplicadas sejam enviadas ao MLD Querier.

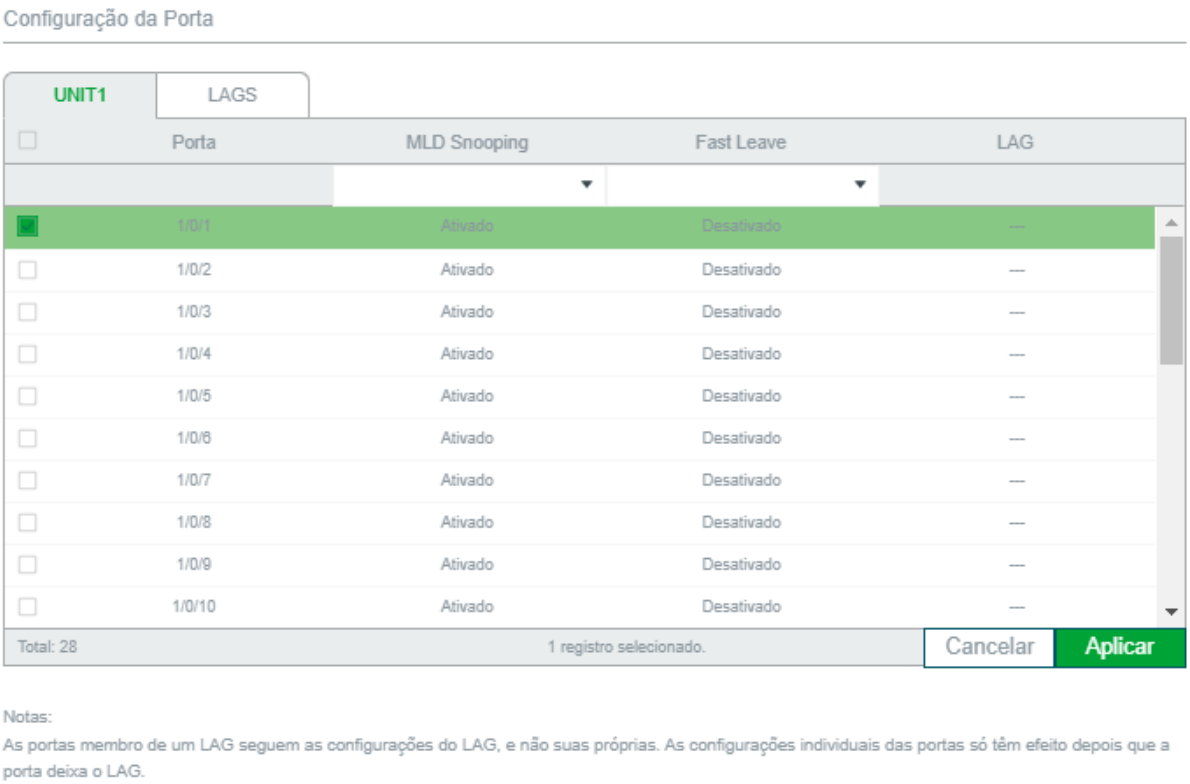
Aging Time da Porta Membro	Especifica o aging time para as portas membro na VLAN. Uma vez que o switch receba uma mensagem de MLD membership report de uma porta, o switch adicionará essa porta à lista de portas membro do correspondente grupo Multicast. As portas membro que são aprendidas dessa forma são Portas membro dinâmicas. Se o switch não receber qualquer mensagem de MLD report de uma porta membro dinâmica de um grupo Multicast específico após o aging time expirar essa porta não será mais considerada como uma porta membro do grupo Multicast e será deletada de sua tabela de encaminhamento.
Aging Time da Porta roteadora	Especifica o aging time para as portas roteadoras na VLAN. Uma vez que o switch receba uma mensagem de MLD general query de uma porta, o switch adicionará essa porta para a lista de portas roteadoras. Portas roteadoras que são aprendidas dessa forma são chamadas portas roteadoras dinâmicas. Se o switch não receber qualquer mensagem MLD general query de uma porta roteadora dinâmica durante o período do aging time, após o aging time expirar o switch não considerará mais essa porta como uma porta roteadora e irá deletar ela da lista de portas roteadoras.
Leave Time	Especifica o leave time para a VLAN. Quando o switch recebe uma mensagem leave de uma porta para deixar o grupo de Multicast, ele irá esperar o tempo de leave time antes de remover a porta do grupo de Multicast. Durante o período, se o switch receber qualquer mensagem de report vinda dessa porta, ele não será removido da lista do grupo de Multicast. Exceções: 1 - Caso o aging time da porta expire antes do leave time e nenhum report for recebido a porta será removida do grupo Multicast uma vez que o Aging time de porta Membro expirar. 2 - O mecanismo de Leave Time não terá efeito quando o Fast Leave estiver habilitado. Um valor de leave time apropriado pode evitar que outros hosts que se conectem à mesma porta do switch sejam removidos por engano de um grupo Multicast quando somente alguns deles quiserem sair.

MLD Snooping Querier	Habilita ou desabilita o MLD Snooping Querier para a VLAN. Quando habilitado, o switch age como um MLD Snooping Querier para os hosts nessa VLAN. O query irá enviar uma mensagem periodicamente para essa rede solicitando as informações dos membros do grupo Multicast, e enviará queries específicas quando receber mensagens de done vindo dos hosts.
Intervalo de Query	Com o MLD Snooping Querier habilitado, especifique o intervalo entre as mensagens de General Query que serão enviadas pelo switch.
Tempo de resposta máxima	Com o MLD Snooping Querier habilitado, especifique o tempo máximo de resposta para as mensagens de general query.
Last Listener Query Interval	Com o MLD Snooping Querier habilitado, quando o switch receber uma mensagem de done, ele obterá o endereço do grupo Multicast ao qual o host pretende deixar de participar. Então o switch enviará MASQs para este grupo Multicast através dessa porta a qual ele recebeu a mensagem de done. Este parâmetro determina o intervalo entre as consultas MASQs.
Last Listener Query Count	Com o MLD Snooping Querier habilitado, especifique o número MASQs a serem enviados. Se o contador específico de grupo for enviado e não forem recebidas mensagens de reports, o switch irá deletar o endereço de Multicast da tabela de encaminhamento Multicast.
General Query Source IP	Com o MLD Snooping Querier habilitado, especifique o endereço IPv6 de origem para as mensagens de general query enviadas pelo switch. Deve ser um endereço Unicast.
Portas roteadoras estáticas	Selecione uma ou mais portas para serem portas roteadoras estáticas na VLAN. Portas roteadoras estáticas não sofre efeitos do aging time. Streams Multicast e pacotes MLD para todos os grupos desta VLAN serão encaminhados através das portas roteadoras estáticas. Streams Multicast e pacotes MLD pata grupos que tem portas roteadoras dinâmicas também serão encaminhadas através da correspondente porta roteadora dinâmica.
Portas roteadoras proibidas	Selecione as portas que serão proibidas de serem portas roteadoras na VLAN.

2. Clique em **Aplicar**.

MLD Snooping para Portas

Vá até o menu **FUNÇÕES L2 > Multicast > MLD Snooping > Configuração de Porta** para carregar a seguinte página.



Siga os seguintes passos para configurar o MLD Snooping para portas:

1. Habilite o MLD Snooping para as portas e habilite o Fast Leave caso tenha apenas um participante do grupo Multicast conectado à porta.

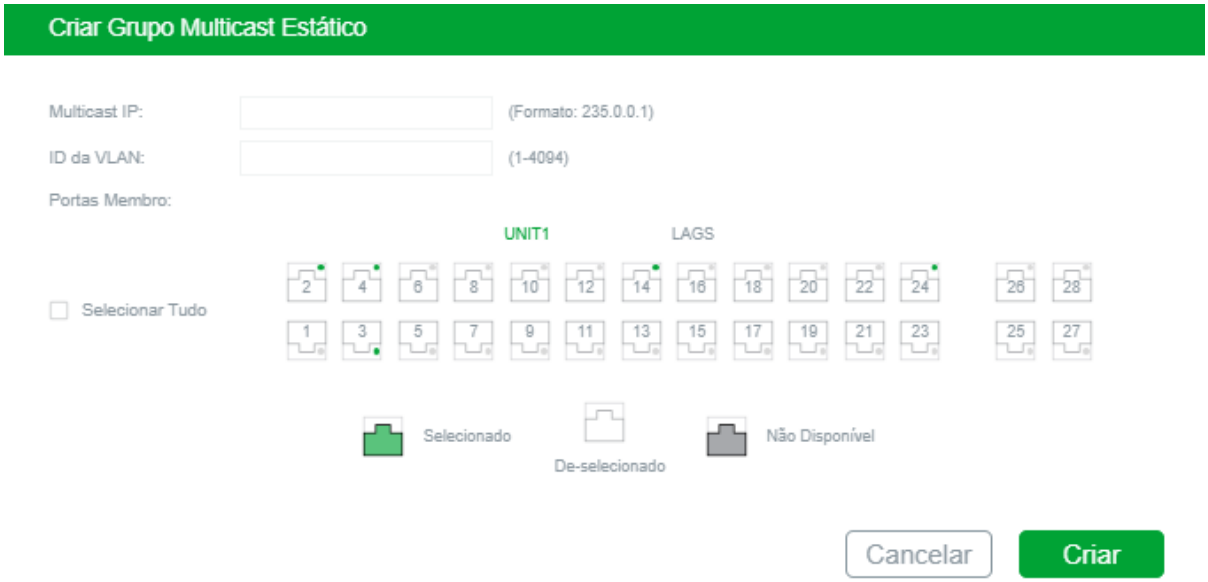
MLD Snooping	Habilite ou desabilite o MLD Snooping para a porta.
Fast Leave	Habilite ou desabilite o Fast Leave para a porta. Fast Leave pode ser habilitado tanto para porta como para VLAN. Quando habilitado no formato baseado em porta, o switch irá remover a porta do correspondente grupo Multicast de todas as VLANs antes de encaminhar a mensagem de leave para o Querier. Você somente deve utilizar Fast Leave baseado em portas quando existir um único host Multicast conectado à porta. Para mais detalhes sobre o Fast Leave veja Configurando MLD Snooping para VLANs.
LAG	Mostra o LAG ao qual a porta pertence.

2. Clique em **Aplicar**.

Ingresso Estático de Hosts para os Grupos Multicast

Portas de camada 2 e hosts normalmente ingressam em grupos Multicast dinamicamente, mas você pode configurar hosts estáticos para os grupos.

Vá até o menu **FUNÇÕES L2 > Multicast > MLD Snooping > Configuração estática de grupo** clique em Adicionar para carregar a seguinte página.



Siga os seguintes passos para configurar ingressos estáticos para grupos Multicast:

1. Especifique o endereço IP Multicast e o VLAN ID. Selecione as portas que serão membros estáticos do grupo Multicast.

IP Multicast	Especifique o endereço do grupo Multicast que os hosts irão ingressar.
VLAN ID	Especifique a VLAN a qual os hosts pertencem.
Portas Membro	Selecione as portas à quais os hosts estão conectados. Essas portas se tornaram membros estáticos do grupo Multicast e não sofrerão o efeito do aging time.

2. Clique em **Criar**.

MVR

Para completar as configurações de MVR siga os seguintes passos:

1. Configure VLANS 802.1Q;
2. Configure MVR globalmente;
3. Adicione grupos Multicast ao MVR;
4. Configure MVR para as portas;
5. (Opcional) Adicione portas estáticas ao grupo MVR.

Orientações para configuração

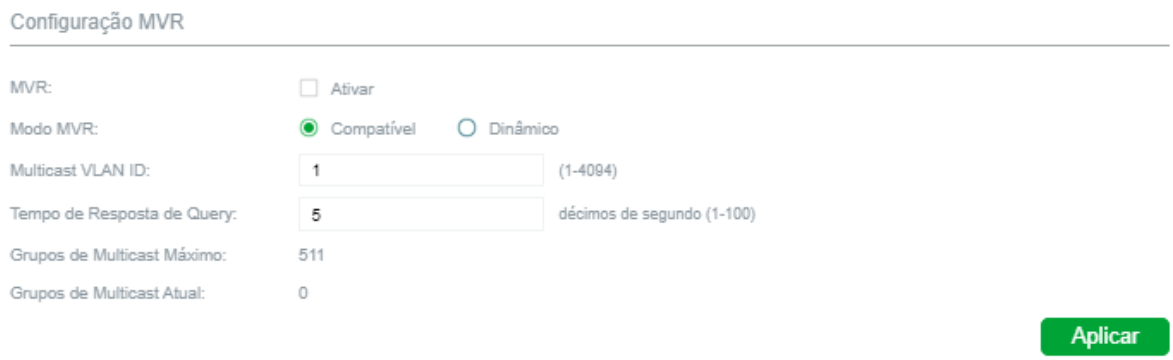
- MVR não suporta mensagens IGMPv3.
- Não configure MVR em portas privadas da VLAN, caso isso ocorra MVR não terá efeito.
- MVR opera com um mecanismo subjacente do IGMP Snooping, mas as duas funções operam independente uma da outra. Ambos protocolos podem ser habilitados em uma porta ao mesmo tempo. Quando ambas estão habilitadas, MVR escuta as mensagens de leave e report somente dos grupos Multicast configurados no MVR. Todos os outros grupos são gerenciados pelo IGMP Snooping.

Configurando VLAN 802.1Q

Antes de configurar o MVR, crie uma VLAN 802.1Q como VLAN Multicast. Adicione todas as portas de origem (portas uplink que receberão dados do roteador) para a VLAN como portas tagged. Configure a VLAN para as portas receptoras (portas que estarão conectadas aos hosts) de acordo com os requerimentos da rede. Note que portas receptoras só podem pertencer à uma VLAN e não podem ser adicionadas à VLAN de Multicast. Para mais detalhes vá até Configuração da VLAN 802.1Q.

Configurando MVR Globalmente

Vá até o menu **FUNÇÕES L2 > Multicast > MVR > Configuração MVR** para carregar a seguinte página.



Siga os seguintes passo para configurar MVR globalmente.

1. Habilite o MVR Globalmente e configure os parâmetros globais.

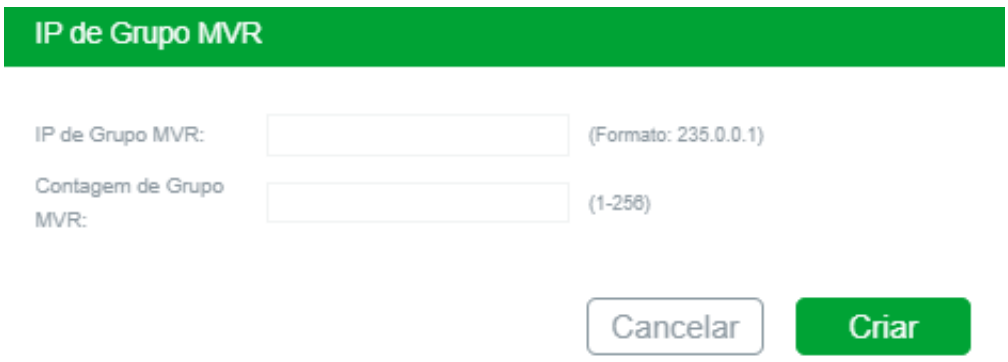
MVR	Habilita ou desabilita MVR Globalmente.

Modo MVR	Especifica o modo MVR como compatível ou dinâmico. **Compatível:** Nesse modo o switch não encaminha mensagens de report ou leave dos hosts para o IGMP Querier. Isso significa que o IGMP Querier não consegue aprender a informação dos membros dos grupos Multicast do switch. O IGMP Querier deve ser configurado estaticamente para transmitir todos os stream Multicast solicitados para o switch através da VLAN de Multicast. **Dinâmico:** Nesse modo após receber mensagens de report ou leave dos hosts o switch irá encaminhá-las para o IGMP Querier através da VLAN de Multicast (com a tradução apropriada para a VLAN ID). O IGMP Querier pode aprender as informações de membros de grupo Multicast através das mensagens de report e leave, e então transmitir os streams Multicast para o switch através da VLAN de Multicast de acordo com a tabela de encaminhamento Multicast.
Multicast VLAN ID	Especifique uma VLAN 802.1Q existente como a VLAN de Multicast.
Tempo de resposta de Query	Especifique o tempo máximo de espera para recebimento de IGMP report em uma porta receptora antes de remover a porta como membro de um grupo Multicast.
Máximo de grupos Multicast	Mostra o número máximo de grupos Multicast que podem ser configurados no switch.
Grupos Multicast corrente	Mostra o número de grupos Multicast que estão configurados no switch.

2. Clique em **Aplicar**.

Adicionando Grupos Multicast ao MVR

Você precisa adicionar manualmente grupos Multicast ao MVR. Vá até o menu **FUNÇÕES L2 > Multicast > MVR > Configuração Grupo MVR** clique em ⊕ Adicionar para carregar a seguinte página.



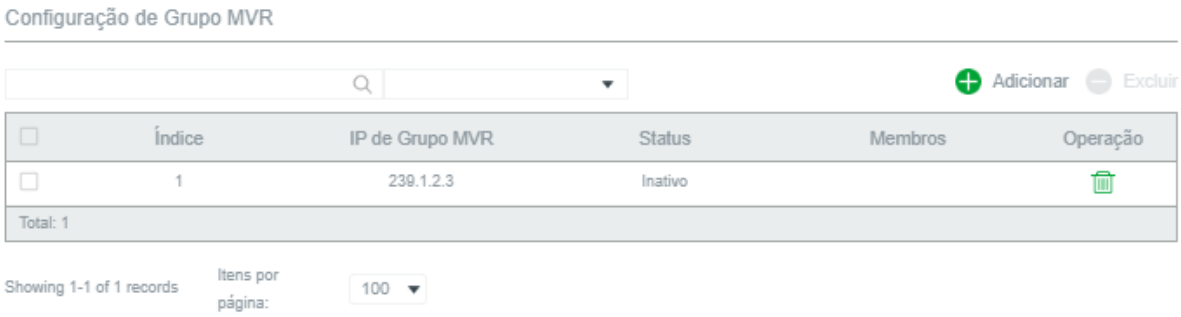
Siga os seguintes passos para adicionar grupos Multicast ao MVR:

1. Especifique o endereço IP do grupo Multicast.

IP Grupo MVR/Contador de grupo MVR	Especifique o endereço IP inicial e o número de endereços adjacentes dos grupos Multicast. Dados Multicast enviados apara endereços especificados aqui serão enviados a todas as portas de origem no switch e todos as portas receptoras que requisitarem receber dados dos endereços Multicast.

2. Clique em **Criar**.

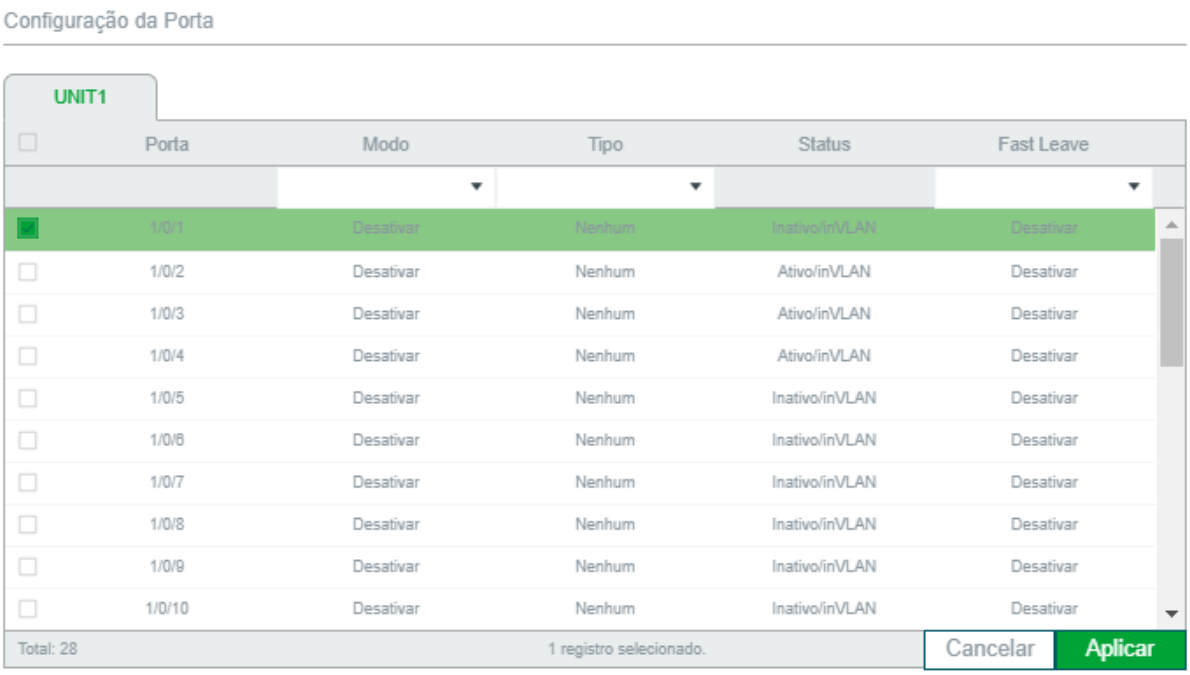
   Então os grupos Multicast irão aparecer na tabela de grupos MVR como mostrado na figura abaixo:



IP Grupo MVR	Mostra o endereço IP do grupo Multicast.
Estado	Mostra o estado do grupo MVR. No modo compatibilidade, todos os grupos MVR são adicionados manualmente, então o estado será sempre ativo. No modo dinâmico tem dois estados: **Inativo:** O grupo MVR foi adicionado com sucesso, porém a porta de origem não recebeu nenhuma mensagem de query deste grupo Multicast. **Ativo:** O grupo MVR foi adicionado com sucesso e a porta de origem já recebeu mensagem de query do grupo Multicast.
Membro	Mostra as portas membro do grupo MVR.

MVR para as Portas

Vá até o menu **FUNÇÕES L2 > Multicast > MVR > Configurações de Porta** para carregar a seguinte página.



Siga os seguintes passo para configurar grupos Multicast MVR para portas:

1. Selecione uma ou mais portas para configurar.
2. Habilite o MVR, e configure o tipo e a função de Fast Leave para a porta.

Modo	Habilita ou desabilite o MVR para as portas selecionadas.
Tipo	Configure o tipo da porta. **Nenhum:** A porta é uma porta não MVR. Se você está tentando configurar uma porta não MVR com características MVR a operação não será bem-sucedida. **Origem:** Configure portas uplink que receberão e enviarão dados Multicast na VLAN de Multicast como porta de origem. Portas de origem devem pertencer a VLAN de Multicast. No modo de dinâmico, portas de origem serão adicionadas automaticamente a todos os grupos Multicast, enquanto no modo compatibilidade você precisará adicionar manualmente elas para o grupo Multicast correspondente. **Receptora:** Configure as portas que estão conectadas aos hosts como portas receptoras. Uma porta receptora só pode pertencer à uma VLAN, e não pode pertencer à VLAN de Multicast. Em ambos os modos o switch irá adicionar ou remover as portas receptoras aos grupos Multicast correspondentes escutando as mensagens de report e leave dos hosts.

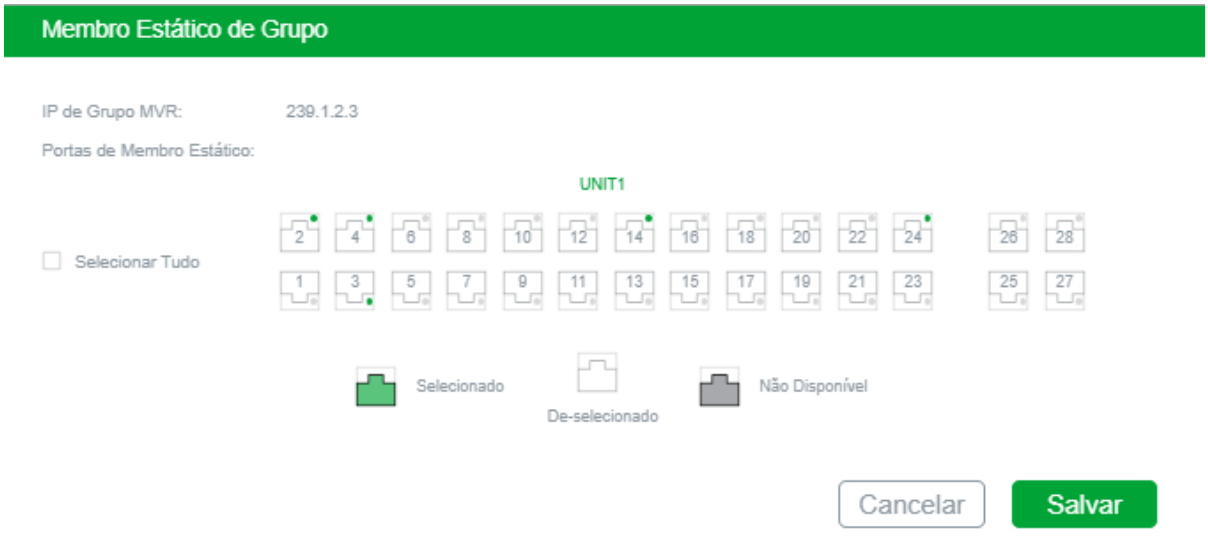
Estado	Mostra o estado da porta. **Ativa/na VLAN:** A porta está fisicamente conectada e em uma ou mais VLANs. **Ativa/não em uma VLAN:** A porta está fisicamente conectada e não está em nenhuma VLAN. **Inativa/na VLAN:** A porta está fisicamente desconectada e está em uma ou mais VLANs. **Inativa/não em uma VLAN:** A porta está fisicamente desconectada e não está em nenhuma VLAN.
Fast Leave	Habilite ou desabilite o Fast Leave para as portas selecionadas. Somente portas receptoras suportam o Fast Leave. Antes de habilitar o Fast Leave para uma porta, garanta que há somente um dispositivo receptor conectado à porta.

3. Clique em **Aplicar**.

(Opcional) Adicionando Portas ao grupo MVR estaticamente

Você pode adicionar somente portas receptoras estaticamente aos grupos MVR. O switch adiciona ou remove portas receptoras aos correspondentes grupos Multicast escutando as mensagens de report e leve dos hosts. Você também pode adicionar uma porta receptora estaticamente ao grupo MVR.

Vá até o menu **FUNÇÕES L2 > Multicast > MVR > Membros estáticos** clique em no grupo MVR desejado para carregar a página seguinte.



Siga os seguintes passos para adicionar portas estáticas ao grupo MVR:

1. Selecione as portas para adicioná-las ao grupo MVR.
2. Clique em **Salvar**.

Filtro Multicast

Para completar a configuração de filtragem Multicast siga os seguintes passos:

1. Crie um perfil IGMP ou MLD;
2. Configure os grupos Multicast aos quais uma porta pode ingressar e a ação de overflow.

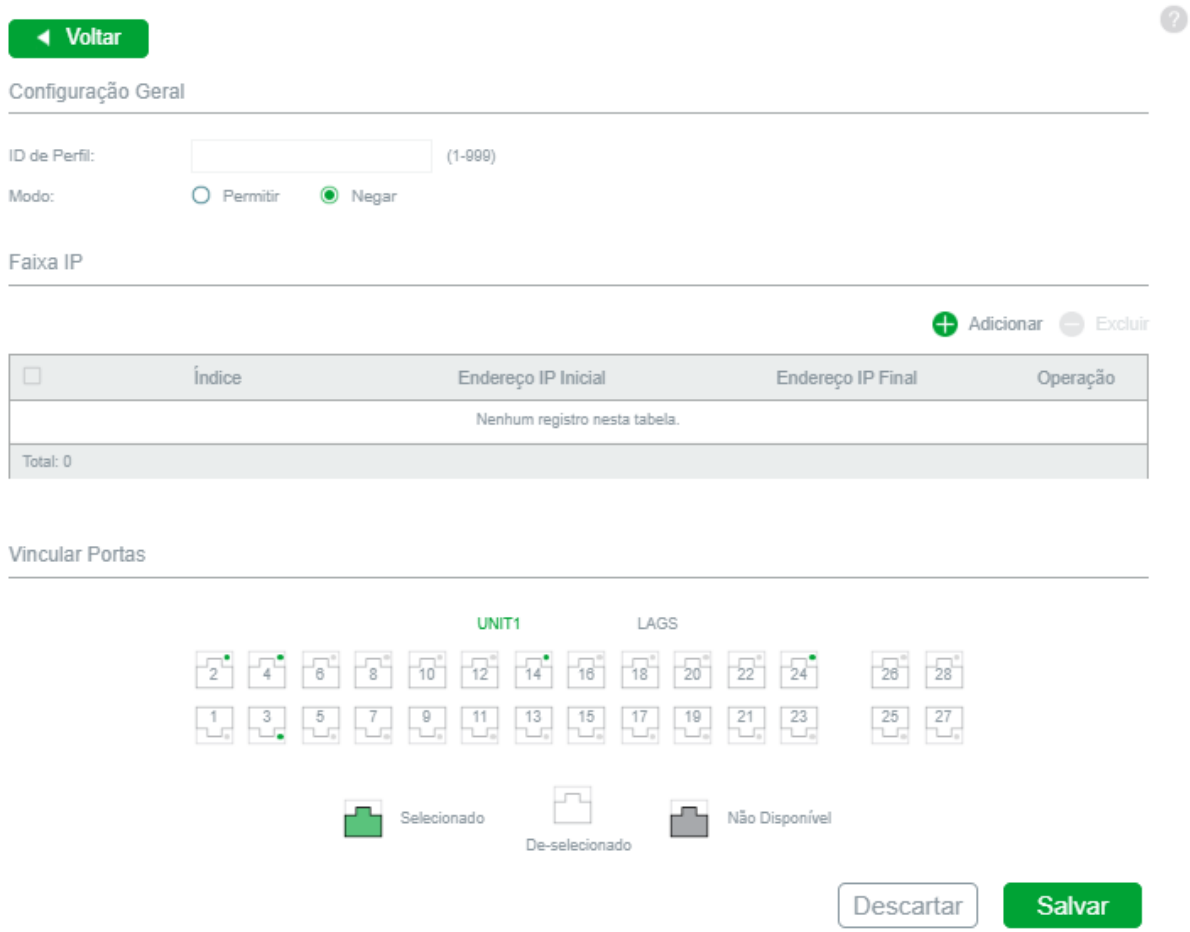
Criando Perfis Multicast

Você pode criar perfil Multicast para redes IPv4 e IPv6. Com perfis Multicast o switch pode definir uma blacklist ou uma whitelist dos grupos Multicast para que sirva como filtro das origens Multicast.

O processo para criar um perfil Multicast para IPv4 e IPv6 são similares. As seguintes instruções tomarão a criação de um perfil IPv4 como exemplo.

Vá até o menu **FUNÇÕES L2 > Multicast > Filtragem Multicast > Perfil IPv4** e clique em Adicionar para carregar a seguinte página.

> Para criar um perfil Multicast IPv6 vá até o menu **FUNÇÕES L2 > Multicast > Filtragem Multicast > Perfil IPv6**.

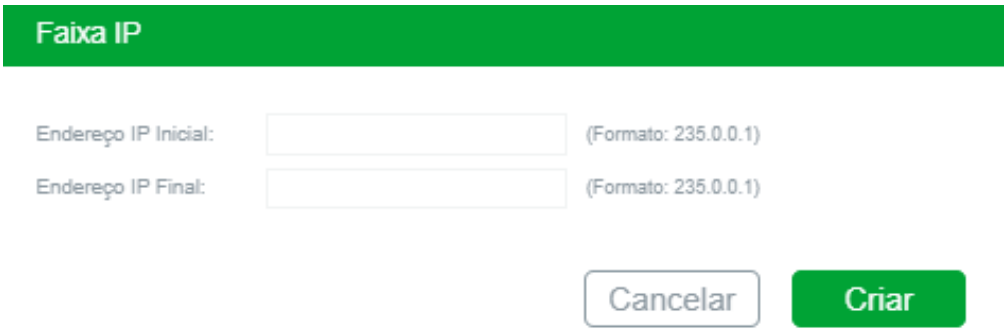


Siga os seguintes passos para criar um perfil.

1. Na seção **Configuração Geral**, especifique a ID do perfil e seu modo.

ID do Perfil	Entre com a ID do perfil valores válidos entre 1 e 999.
Modo	Selecione **Permitir** ou **Negar** como modo de filtro. **Permitir:** age como Whitelist e permite portas membros específicas a ingressar grupos Multicast específicos. **Negar:** age como Blacklist e impede portas membros específicas de ingressar grupos Multicast específicos.

2. Na seção **Faixa IP**, clique em Adicionar para carregar a seguinte página. Configure o endereço IP de início e fim para filtragem do grupo Multicast, e clique em **Criar**.



3. Na seção **Vincular portas**, selecione as portas desejadas à serem vinculadas ao perfil.
4. Clique em **Salvar**.

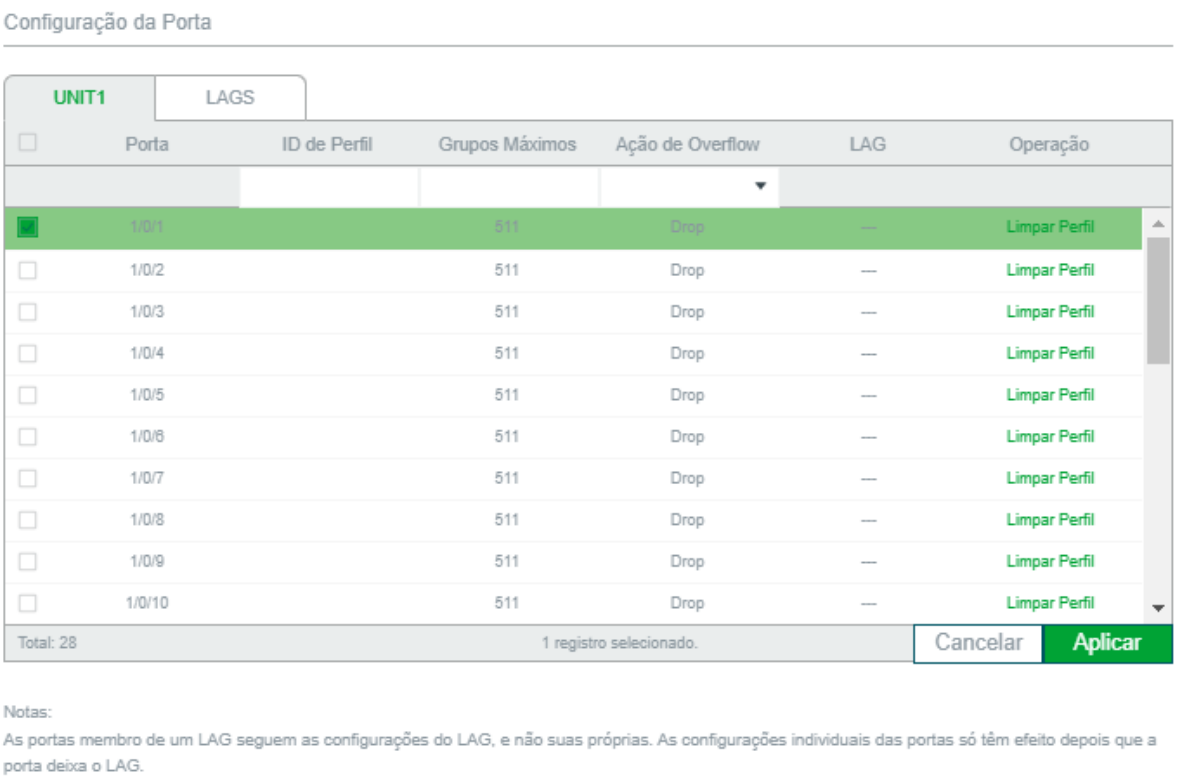
Filtro Multicast para Portas

Você pode modificar a relação de mapeamento entre portas e perfis em lotes e configurar o número de grupos Multicast aos quais uma porta pode ingressar e a ação de overflow.

O processo para configuração de filtro Multicast para portas em IPv4 e Ipv6 é similar. As seguintes instruções tomarão a configuração de filtragem Multicast para portas para IPv4 como exemplo.

Vá até o menu **FUNÇÕES L2 > Multicast > Filtro Multicast > Configuração de Porta IPv4** para carregar a seguinte página.

> Para criar um perfil Multicast IPv6 vá até o menu **FUNÇÕES L2 > Multicast > Filtragem Multicast > Perfil IPv6**.



Siga os seguintes passos para vincular um perfil a portas e configurar os parâmetros correspondentes:

1. Selecione uma ou mais portas para configurar.
2. Especifique o perfil para ser vinculado e configure o valor máximo de grupos que uma porta pode ingressar e sua ação e overflow.

ID do Perfil	Especifique o ID de um perfil existente para vincular o perfil às portas selecionadas. Uma porta pode ser vinculada somente à um perfil.
Grupos Máximos	Entre com o número máximo de grupos Multicast que uma porta pode ingressar. Valores validos variam entre 0 e 1000.
Ação de Overflow	Selecione a ação que o switch irá tomar com os novos grupos Multicast quando o número de grupos Multicast aos quais a porta ingressou exceder o máximo. **Descartar:** descarta todos as mensagens de report de membro para prevenir que a porta ingresse em novos grupos Multicast. **Repor:** Repõem um existente grupo Multicast mais antigo com o menor endereço MAC com o novo grupo Multicast.
LAG	Mostra a LAG a qual a porta pertence.
Operação	Clique em **Limpar Perfil** para limpar o vínculo entre o perfil e a porta.

3. Clique em **Aplicar**.

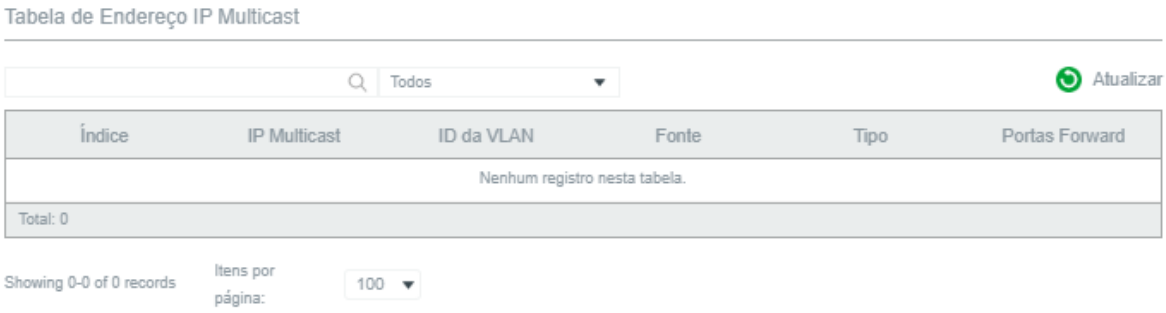
Visualizando informação de Multicast Snooping

Você pode visualizar as seguintes informações do Multicast Snooping:

- Visualizar a tabela de Multicast IPv4.
- Visualizar as estatísticas Multicast IPv4 para cada porta.
- Visualizar a tabela de Multicast IPv6.
- Visualizar as estatísticas Multicast IPv6 para cada porta.

Visualizando a Tabela Multicast IPv4

Vá até o menu **FUNÇÕES L2 > Multicast > Informação Multicast > Tabela de Multicast IPv4** para carregar a seguinte página:

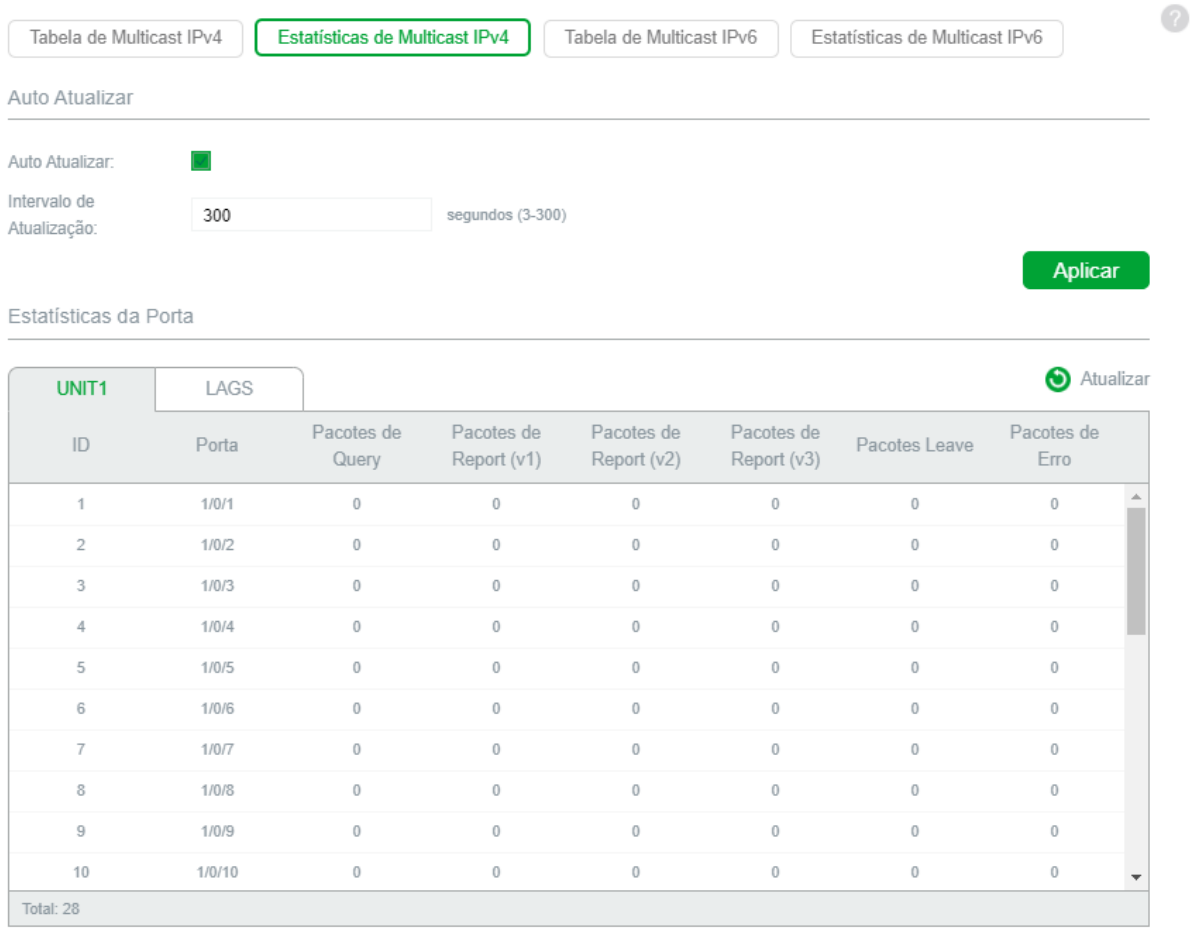


A tabela de endereço IP Multicast mostra todas as entradas Multicast IP-VLAN-Porta válidas.

IP Multicast	Mostra o endereço IP de origem de Multicast.
ID VLAN	Mostra a ID da VLAN à qual o grupo Multicast pertence.
Origem	Mostra se o grupo Multicast foi aprendido dinamicamente ou adicionado manualmente.
Tipo	Mostra se o grupo Multicast é gerenciado por IGMP Snooping ou MVR.
Portas de encaminhamento	Todas as portas do grupo Multicast, incluindo portas roteadoras e as portas membro.

Visualizando as estatísticas Multicast IPv4 para cada Porta

Vá até o menu **FUNÇÕES L2 > Multicast > Informação Multicast > Estatísticas de Multicast IPv4** para carregar a seguinte página:



Siga os seguintes passos para visualizar as estatísticas Multicast IPv4 para cada porta:

1. Para obter as estatísticas Multicast em tempo real, habilite a função **Auto Atualizar** ou clique em **Atualizar**.

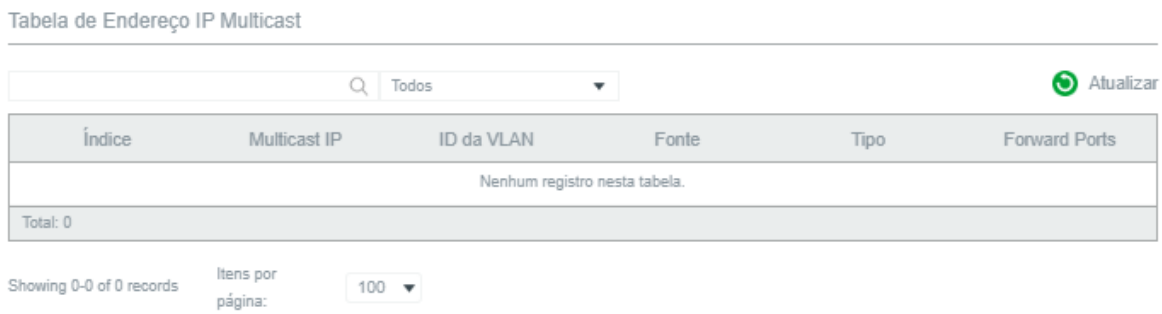
Auto Atualizar	Habilite ou desabilite a atualização automática. Quando habilitada o switch irá atualizar as estatísticas Multicast automaticamente.
Intervalo de Atualização	Após habilitar a função Auto Atualizar especifique o intervalo no qual o switch irá atualizar as estatísticas.

2. Na seção **Estatísticas de Porta**, visualize as estatísticas Multicast IPv4 para cada porta.

Pacotes Query	Mostra o número de pacotes query recebidos pela porta.
Pacotes de Report (v1)	Mostra o número de pacotes de report IGMPv1 recebidos pela porta.
Pacotes de Report (v2)	Mostra o número de pacotes de report IGMPv2 recebidos pela porta.
Pacotes de Report (v3)	Mostra o número de pacotes de report IGMPv3 recebidos pela porta.
Pacotes Leave	Mostra o número de pacotes leave recebidos pela porta.
Pacotes de erro	Mostra o número de pacotes de erro recebidos pela porta.

Visualizando a Tabela Multicast IPv6

Vá até o menu **FUNÇÕES L2 > Multicast > Informação Multicast > Tabela de Multicast IPv6** para carregar a seguinte página:

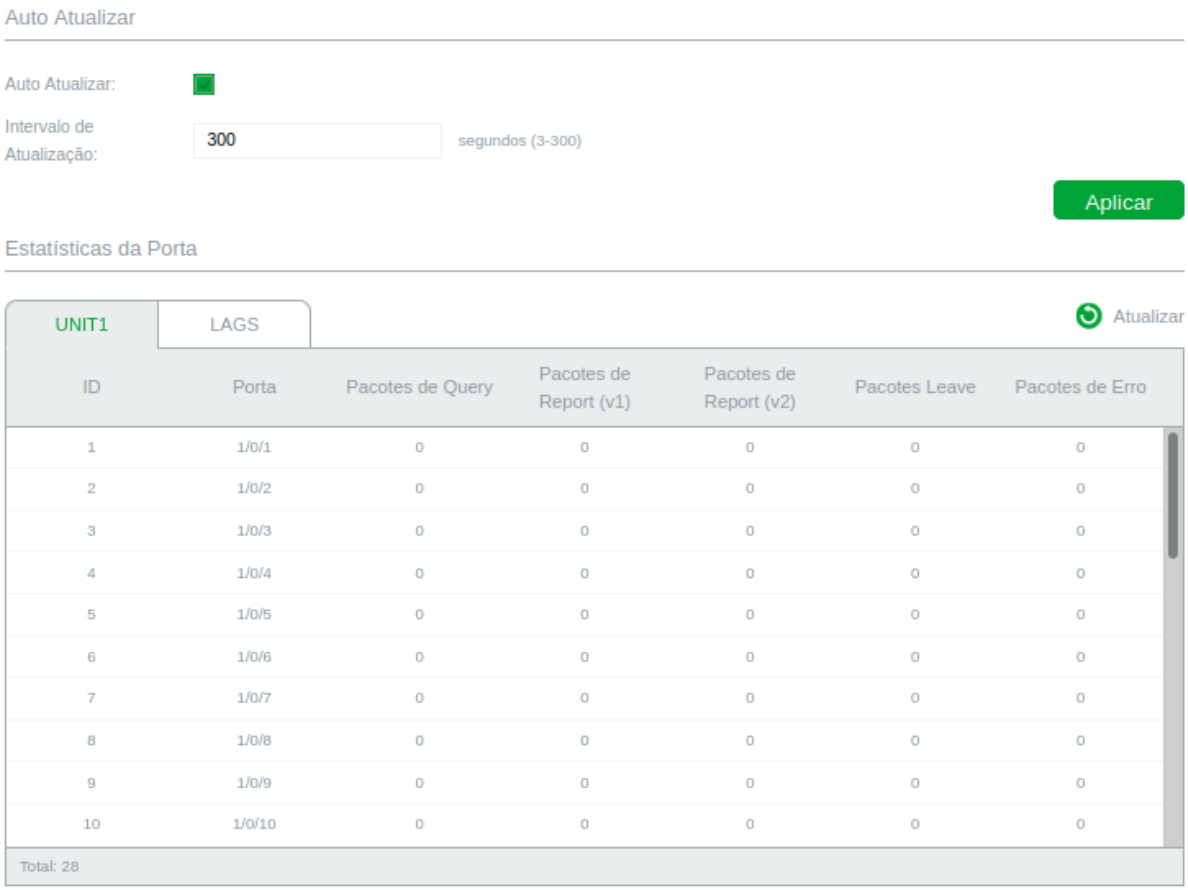


A tabela de endereço IP Multicast mostra todas as entradas Multicast IP-VLAN-Porta válidas.

IP Multicast	Mostra o endereço IP de origem de Multicast.
ID VLAN	Mostra a ID da VLAN à qual o grupo Multicast pertence.
Origem	Mostra se o grupo Multicast foi aprendido dinamicamente ou adicionado manualmente.
Tipo	Mostra se o grupo Multicast é gerenciado por IGMP Snooping ou MVR.
Portas de encaminhamento	Todas as portas do grupo Multicast, incluindo portas roteadoras e as portas membro.

Visualizando as estatísticas Multicast IPv6 para cada Porta

Vá até o menu **FUNÇÕES L2 > Multicast > Informação Multicast > Estatísticas de Multicast IPv6** para carregar a seguinte página:



Siga os seguintes passos para visualizar as estatísticas Multicast IPv6 para cada porta:

1. Para obter as estatísticas Multicast em tempo real, habilite a função **Auto Atualizar** ou clique em **Atualizar**.

Auto Atualizar	Habilite ou desabilite a atualização automática. Quando habilitada o switch irá atualizar as estatísticas Multicast automaticamente.
Intervalo de Atualização	Após habilitar a função Auto Atualizar especifique o intervalo no qual o switch irá atualizar as estatísticas.

2. Na seção **Estatísticas de Porta**, visualize as estatísticas Multicast IPv6 para cada porta.

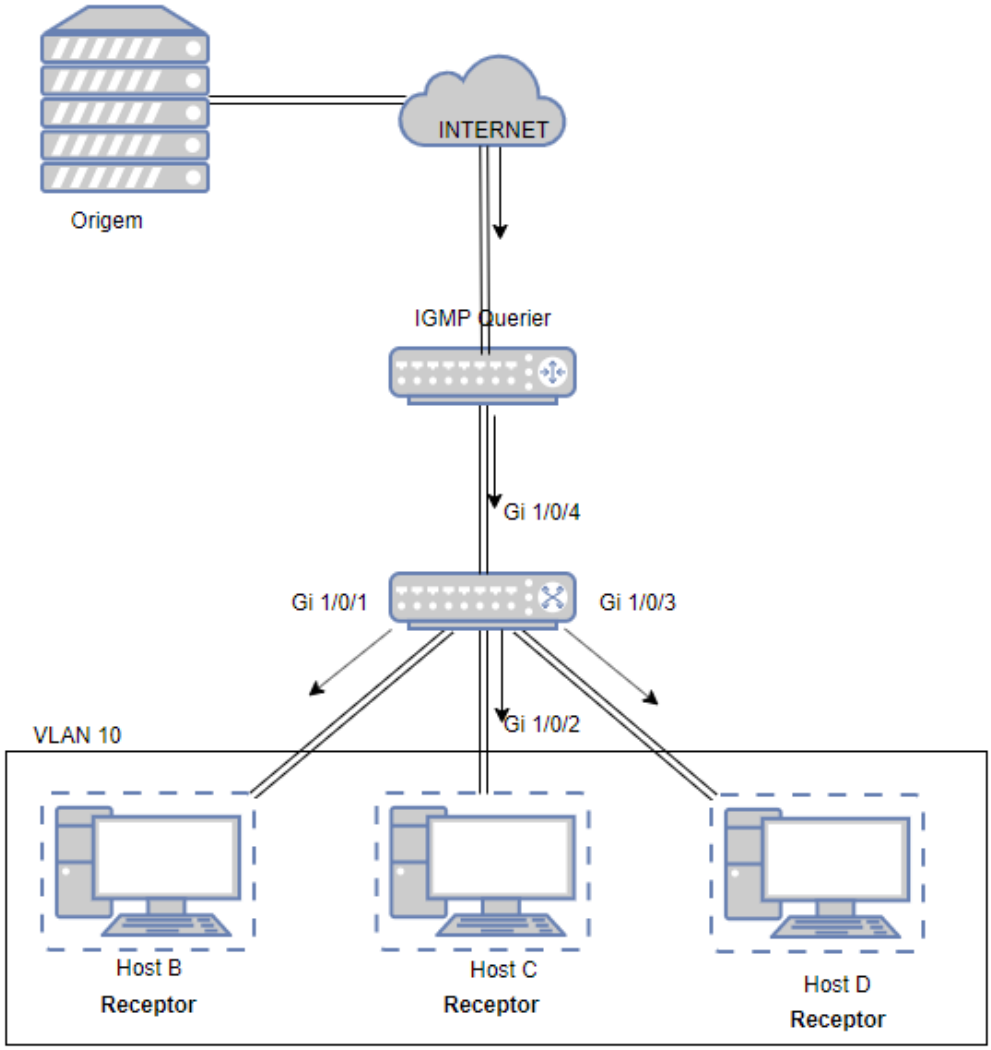
Pacotes Query	Mostra o número de pacotes query recebidos pela porta.
Pacotes de Report (v1)	Mostra o número de pacotes de MLDv1 recebidos pela porta.
Pacotes de Report (v2)	Mostra o número de pacotes de MLDv2 recebidos pela porta.
Pacotes Leave	Mostra o número de pacotes leave recebidos pela porta.
Pacotes de erro	Mostra o número de pacotes de erro recebidos pela porta.

Exemplo de Configuração Básica para IGMP Snooping

Requisitos da Rede

Hosts B, C e D estão na mesma VLAN do Switch. Todos desejam receber stream Multicast enviado do grupo Multicast 225.1.1.1.

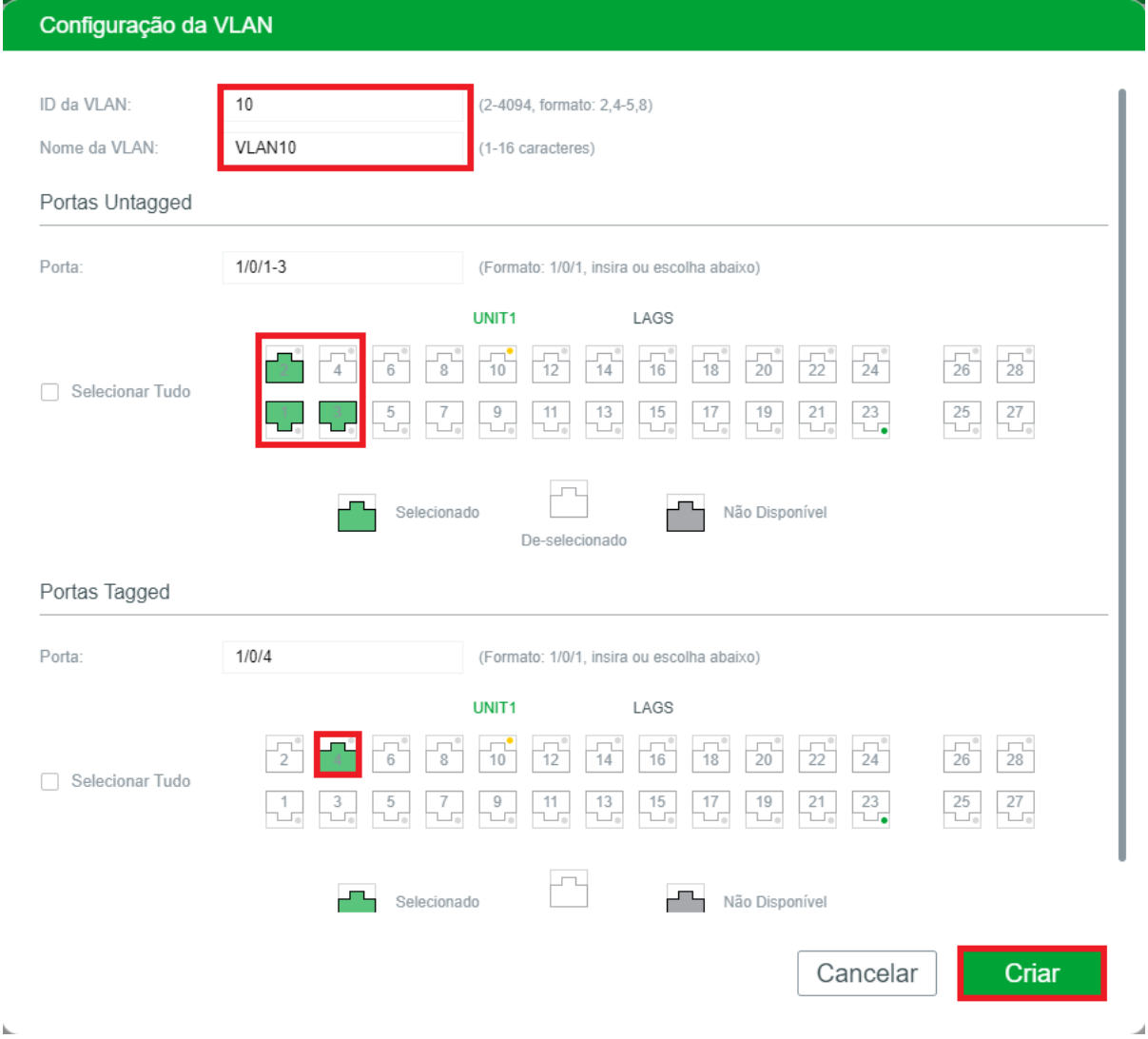
Como mostrado na topologia abaixo, Host B, Host C e Host D estão conectados respectivamente às portas 1/0/1, 1/0/2 e 1/0/3. Porta 1/0/4 é a porta roteadora conectada ao Multicast Querier.



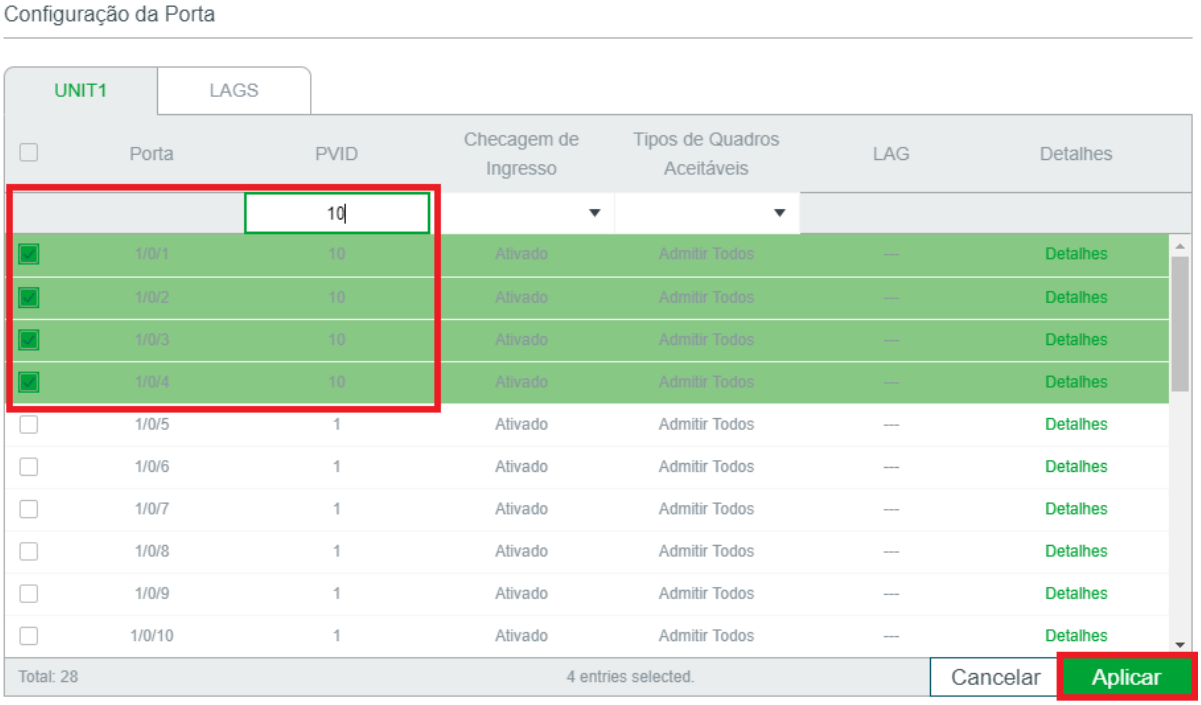
Configurando o Cenário

- Adicione as 3 portas membro e a porta roteadora à VLAN e configure suas PVIDs.
- Habilite o IGMP Snooping globalmente e na VLAN.
- Habilite o IGMP Snooping às portas.

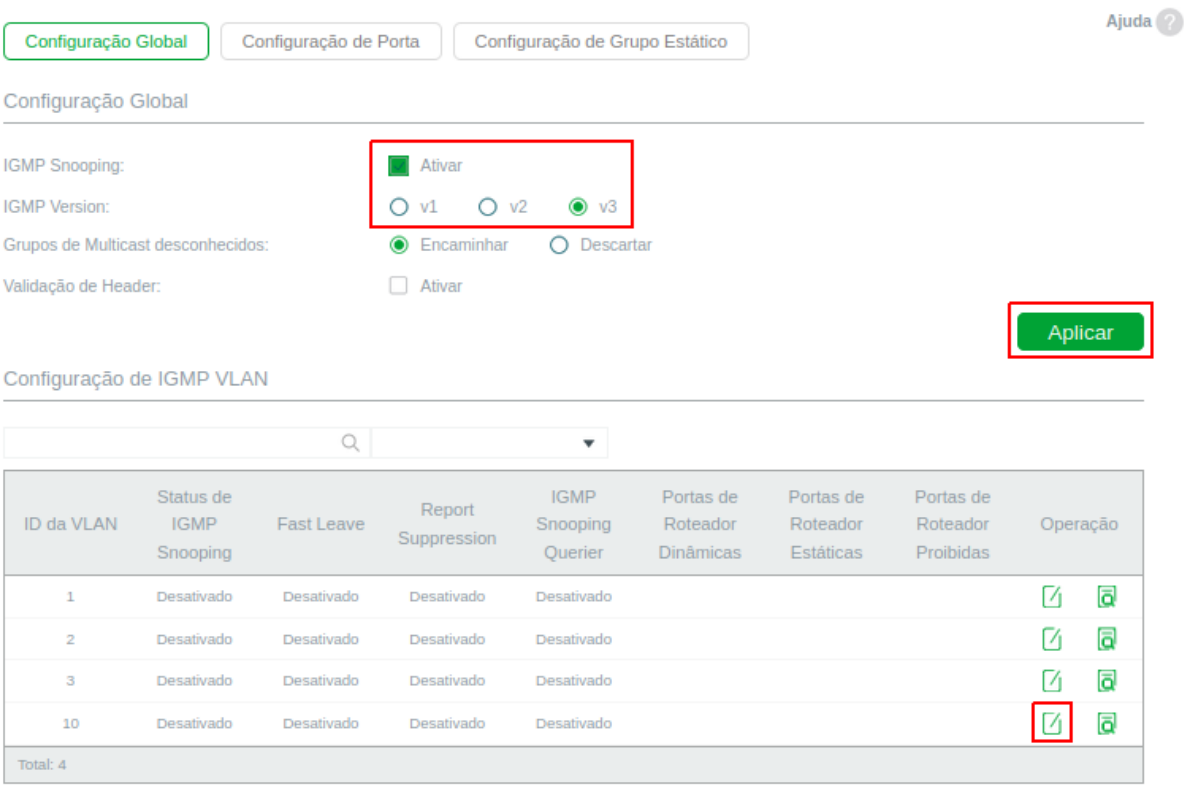
1. Vá até o menu **FUNÇÕES L2 > VLAN > VLAN 802.1Q > Configurações VLAN** clique em Adicionar para carregar a seguinte página. Crie a VLAN 10 e adicione as portas Untagged 1/0/1-3 e tagged 1/0/4 para a VLAN 10.



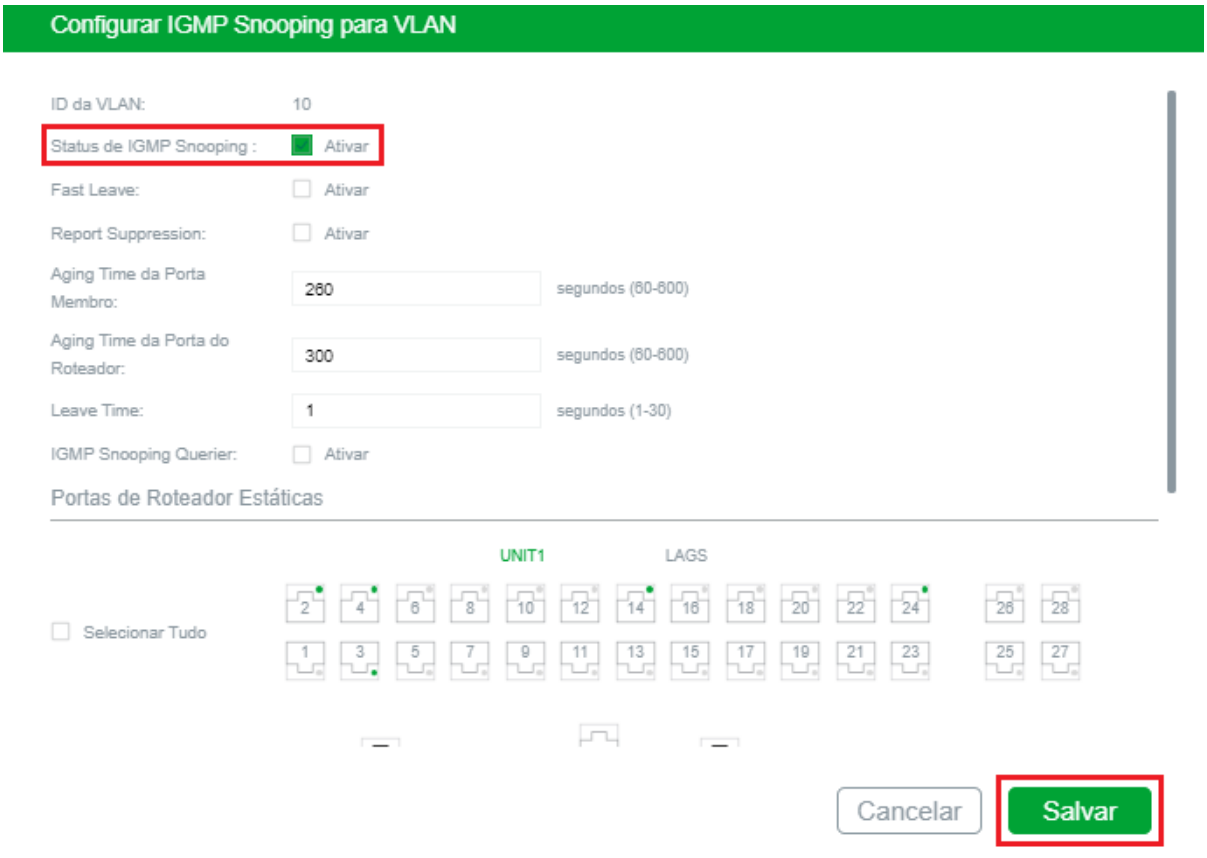
2. Vá até o menu **FUNÇÕES L2 > VLAN > VLAN 802.1Q > Configuração de Porta** para carregar a seguinte página. Configure o PVID das portas 1/0/1-4 como 10.



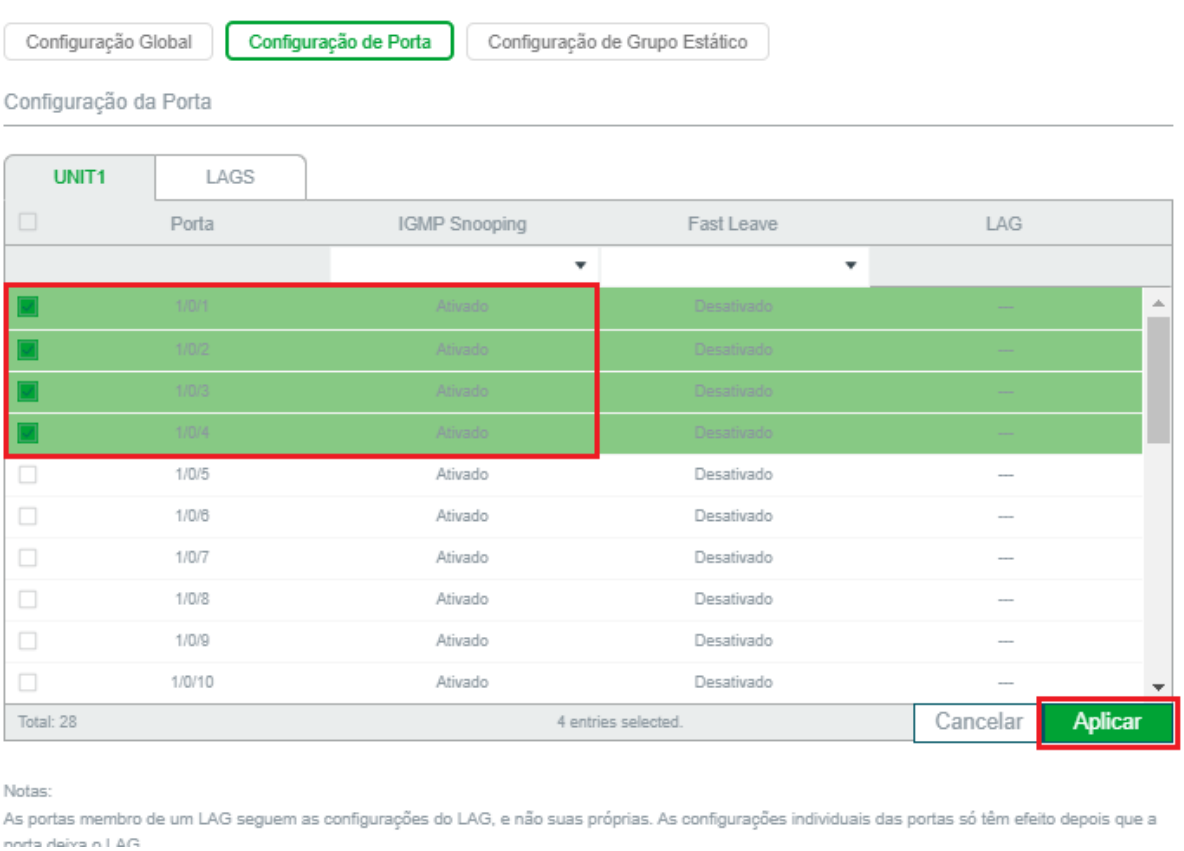
3. Vá até o menu **FUNÇÕES L2 > Multicast > IGMP Snooping > Configuração Global** para carregar a seguinte página. Na seção **Configuração Global**, habilite o IGMP Snooping globalmente. Configure a versão do IGMP para v3 para que o switch possa processar mensagens IGMP de todas as versões e então clique em **Aplicar**.



4. Na seção **Configuração IGMP VLAN**, na VLAN 10 clique em para carregar a seguinte página. Habilite o IGMP Snooping para VLAN 10.



5. Vá até o menu **FUNÇÕES L2 > Multicast > IGMP Snooping > Configuração de Porta** para carregar a seguinte página. Habilite IGMP Snooping para as portas 1/0/1-4.



6. Clique em Salvar para salvar as configurações.

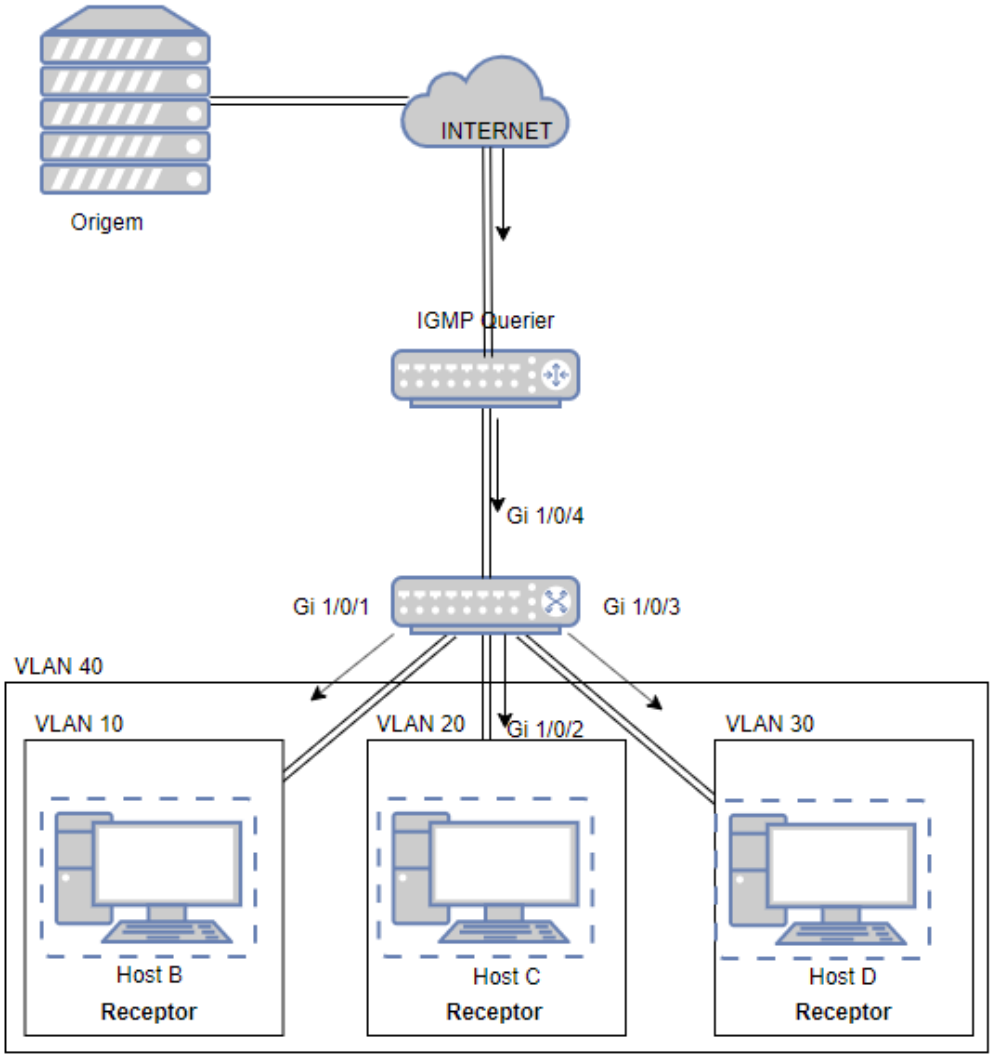
Exemplo de Configuração MVR

Requisitos da Rede

Host B, Host C e Host D estão em três VLANs diferentes do switch. Todos eles desejam receber stream Multicast enviados do grupo Multicast 225.1.1.1.

Topologia de Rede

Como mostrado na topologia de rede a seguir, HostB, Host C e Host D estão conectados às portas 1/0/1, porta 1/0/2 e porta 1/0/3 respectivamente. Porta 1/0/1, porta 1/0/2 e porta 1/0/3 pertencem às VLAN 10, VLAN 20 e VLAN 30 respectivamente. Porta 1/0/4 está conectada à rede Multicast de maior camada.

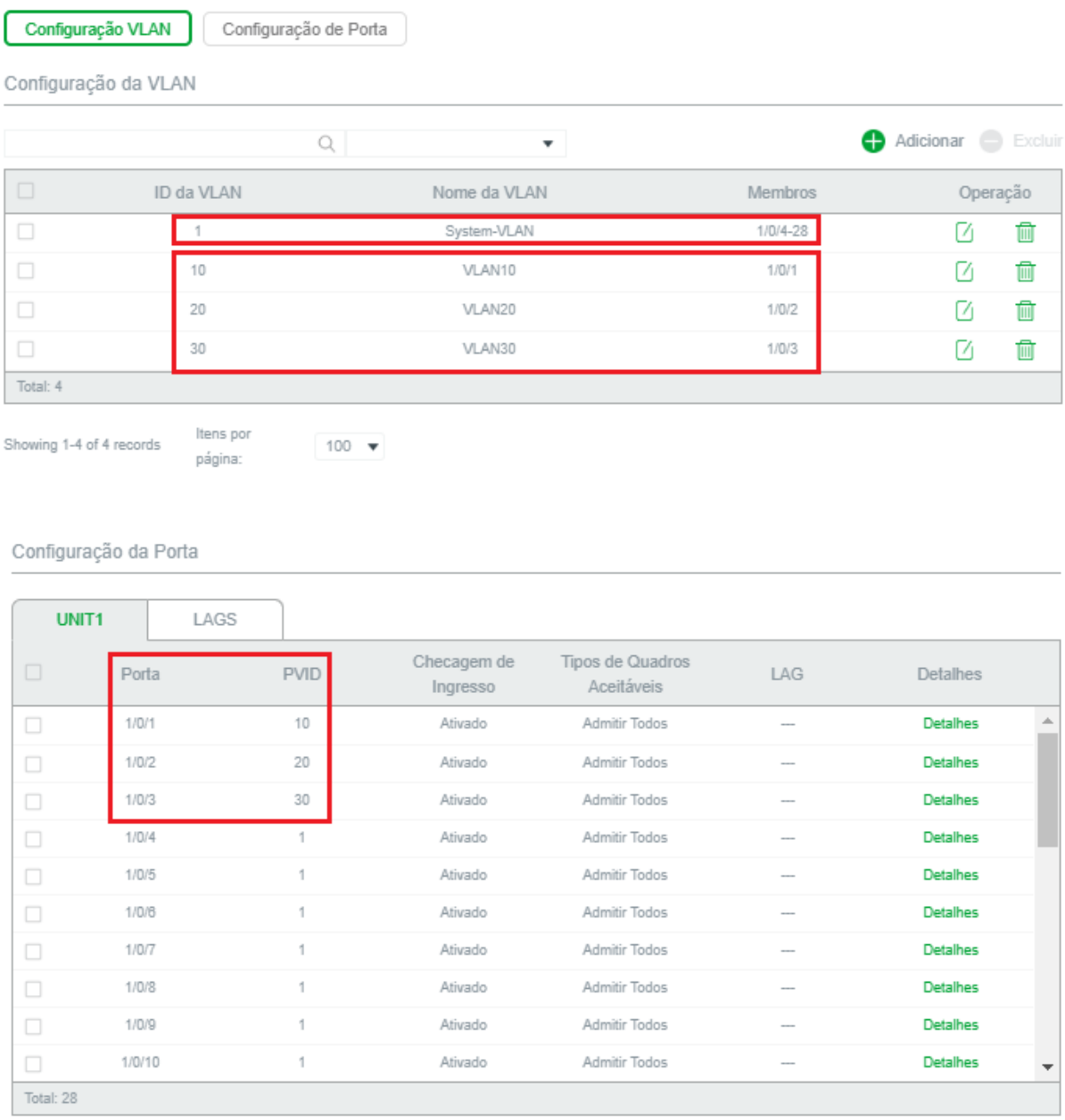


Configurando o Cenário

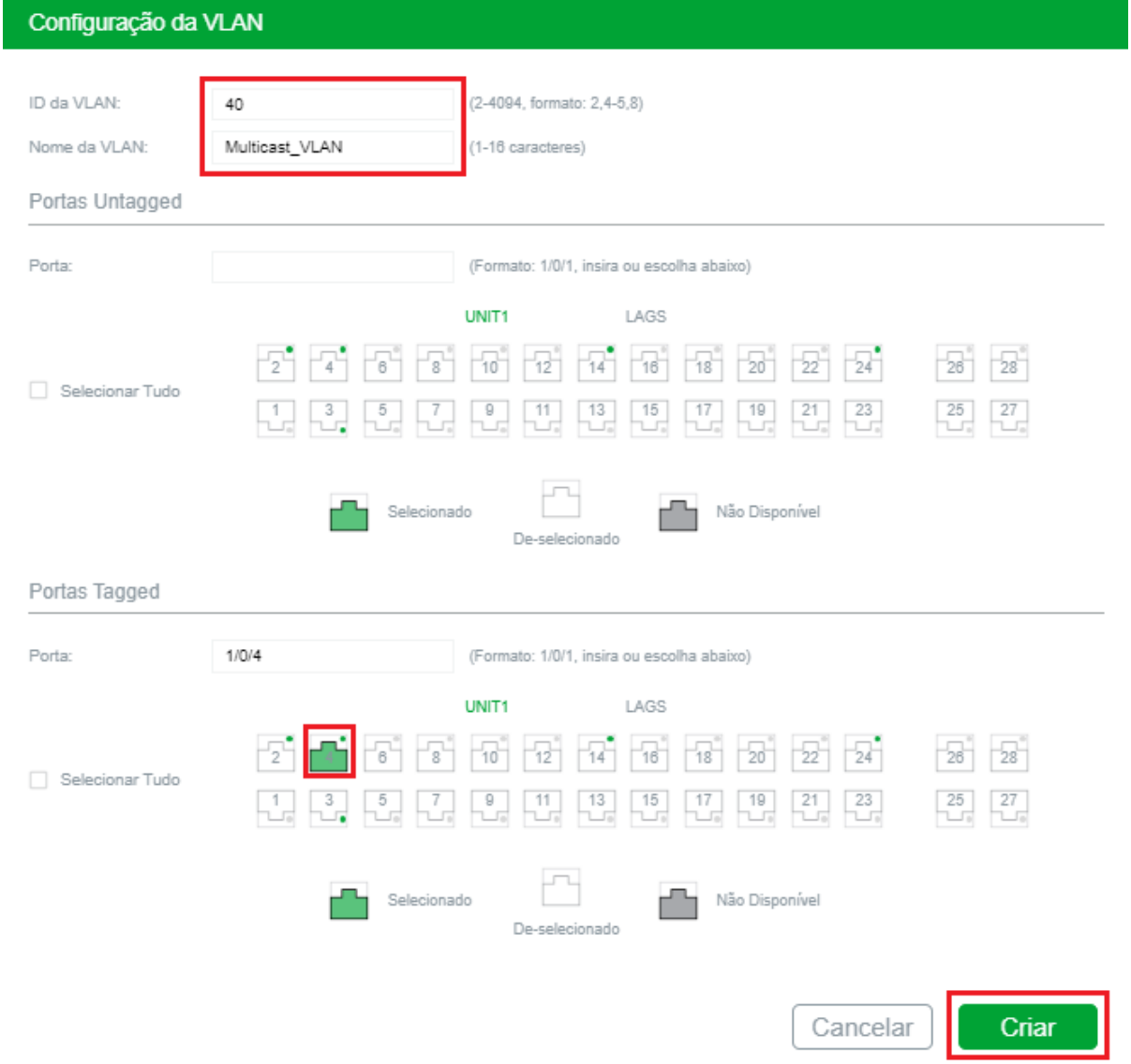
Como os hosts estão em VLANs diferentes, no IGMP Snooping, o Querier necessita duplicar os streams de Multicast para os hosts em cada VLAN. Para evitar duplicação de streams Multicast enviados entre o Querier e o switch, você pode configurar MVR no switch.

O switch consegue trabalhar tanto no modo **Compatibilidade** como no modo **Dinâmico** no MVR. Quando em modo compatibilidade lembre de configurar estaticamente para que o Querier consiga transmitir os streams de grupo Multicast 225.1.1.1 para o switch através da VLAN de Multicast. Aqui nós utilizaremos o MVR **Dinâmico** como exemplo.

1. Adicione as portas 1/0/1-3 às VLANs 10, 20 e 30 como portas Untagged, respectivamente. E configure o PVID da porta 1/0/1 como 10, da porta 1/0/2 como 20, da porta 1/0/3 como 30. Garanta que as portas 1/0/1-3 pertençam somente às VLAN 10, 20 e 30 respectivamente. Para mais detalhas vá para Configuração da VLAN 802.1Q.

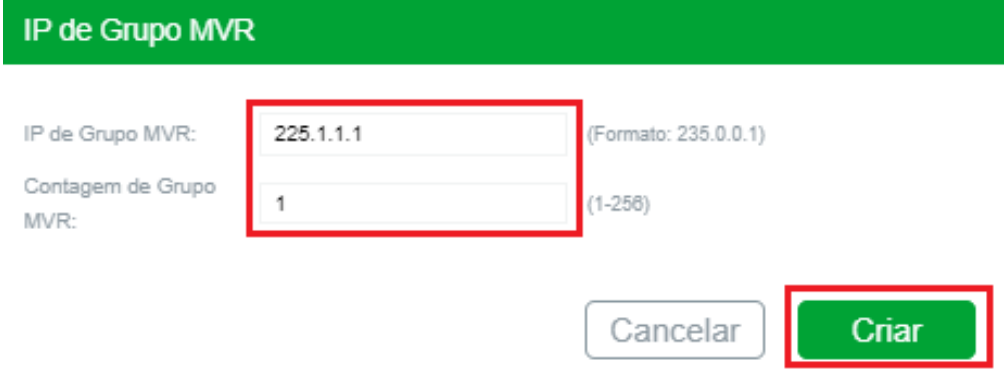


2. Vá até o menu **FUNÇÕES L2 > VLAN > VLAN 802.1Q** clique em Adicionar para carregar a seguinte página. Crie a VLAN 40 e adicione a porta 1/0/4 à VLAN como porta Tagged.

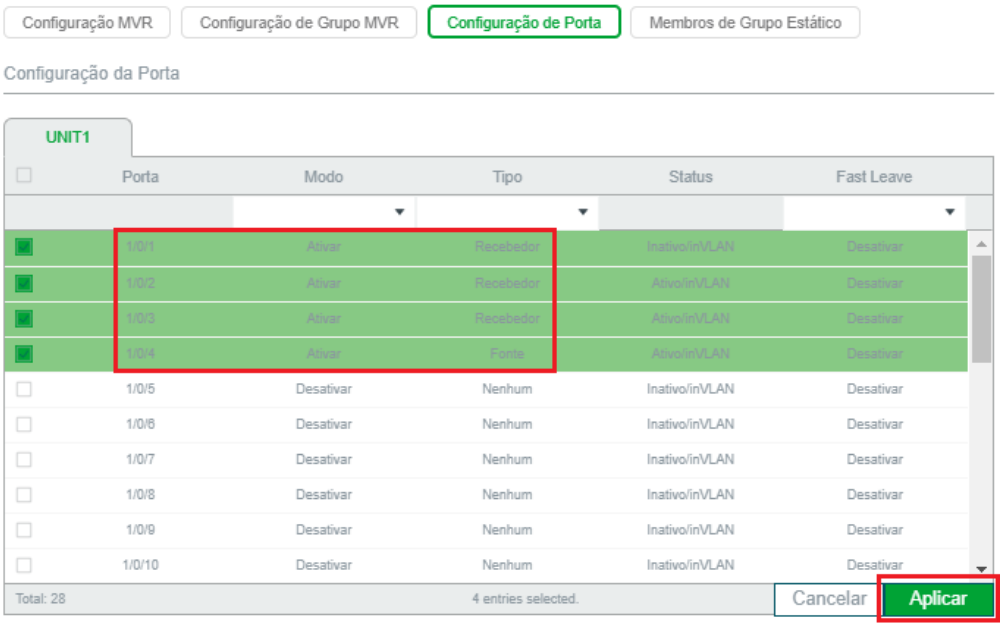


3. Vá até o menu **FUNÇÕES L2 > Multicast > MVR > Configuração MVR** para carregar a seguinte página. Habilite MVR globalmente e configure o modo do MVR como **Dinâmico**, Multicast VLAN ID como 40.

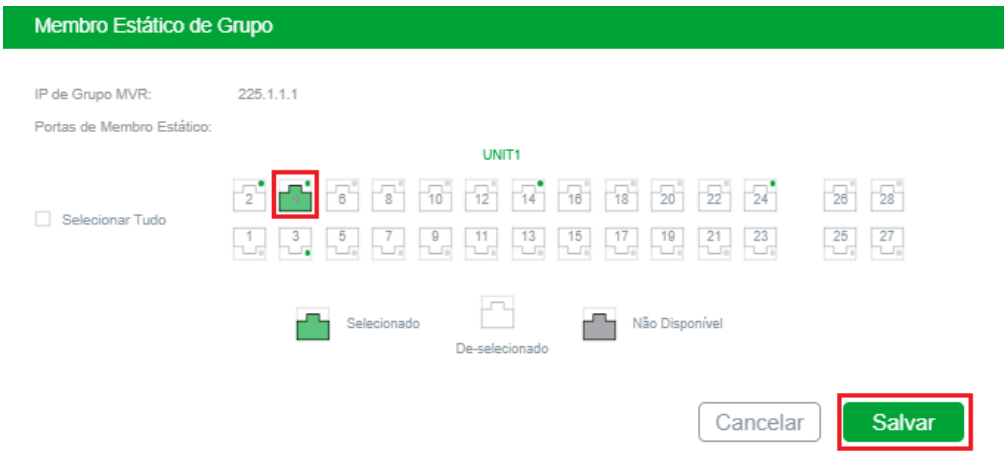
4. Vá até o menu **FUNÇÕES L2 > Multicast > MVR > Configuração de Grupo MVR** e clique em Adicionar para carregar a seguinte página. Adicione o grupo de Multicast 225.1.1.1 ao MVR.



5. Vá até o menu **FUNÇÕES L2 > Multicast > MVR > Configuração de Porta** para carregar a seguinte página. Habilite o MVR para as portas 1/0/1-4. Configure as portas 1/0/1-3 como **Recebedoras** e a porta 1/0/4 como porta de **Fonte**.



6. Vá até o menu **FUNÇÕES L2 > Multicast > MVR > Membros estáticos do Grupo** clique em na entrada do grupo 225.1.1.1 para carregar a seguinte página. Selecione porta 1/0/4 para ingressar estaticamente ao grupo e clique em **Salvar**.

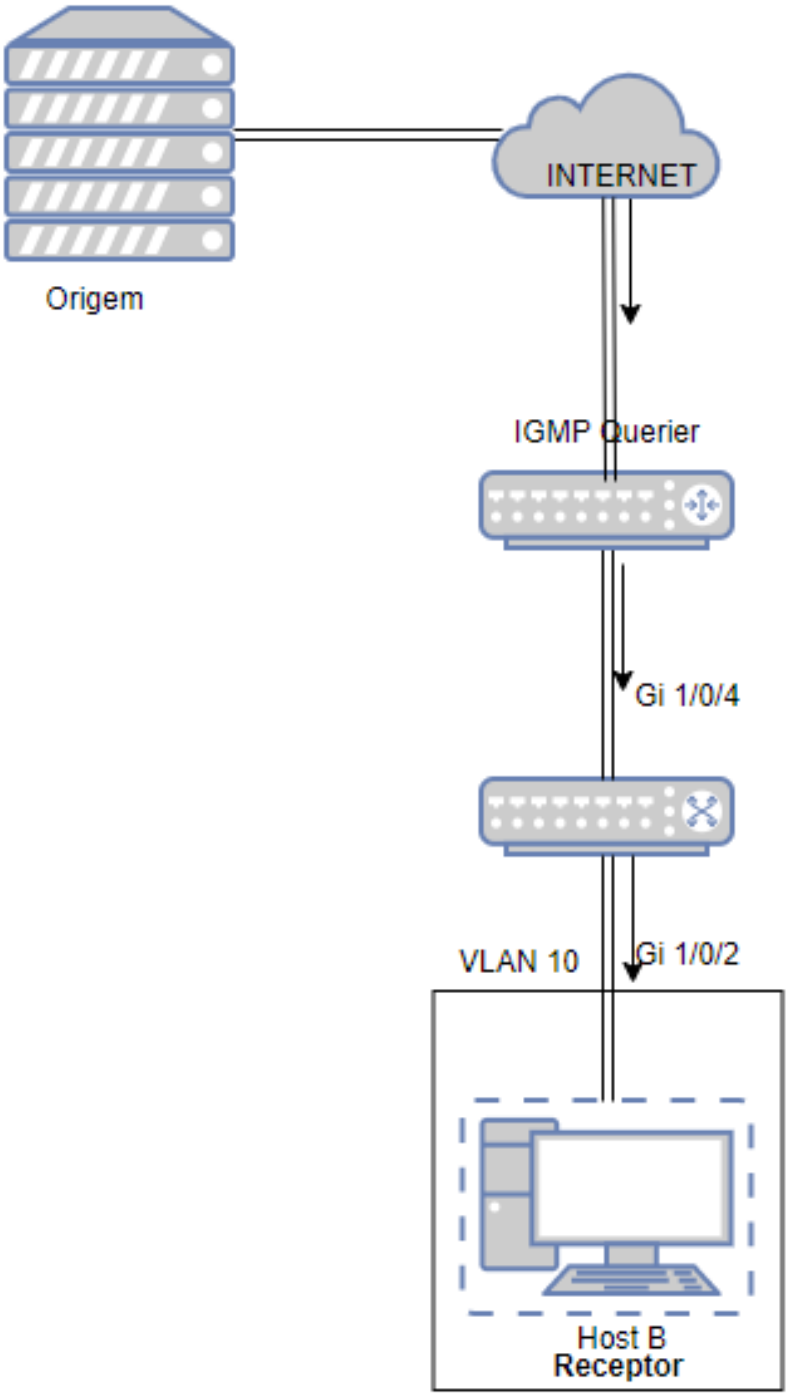


7. Clique em Salvar para salvar as configurações.

Exemplo de Configuração de Multicast Desconhecido e Fast Leave

Requisitos da Rede

Um usuário sofre um atraso quando está trocando de canal em sua IPTV. Ele deseja solucionar o seu problema. Como mostrado na topologia de rede à baixo, porta 1/0/4 do switch está conectado à rede de camada 3, e a porta 1/0/2 está conectada ao Host B.

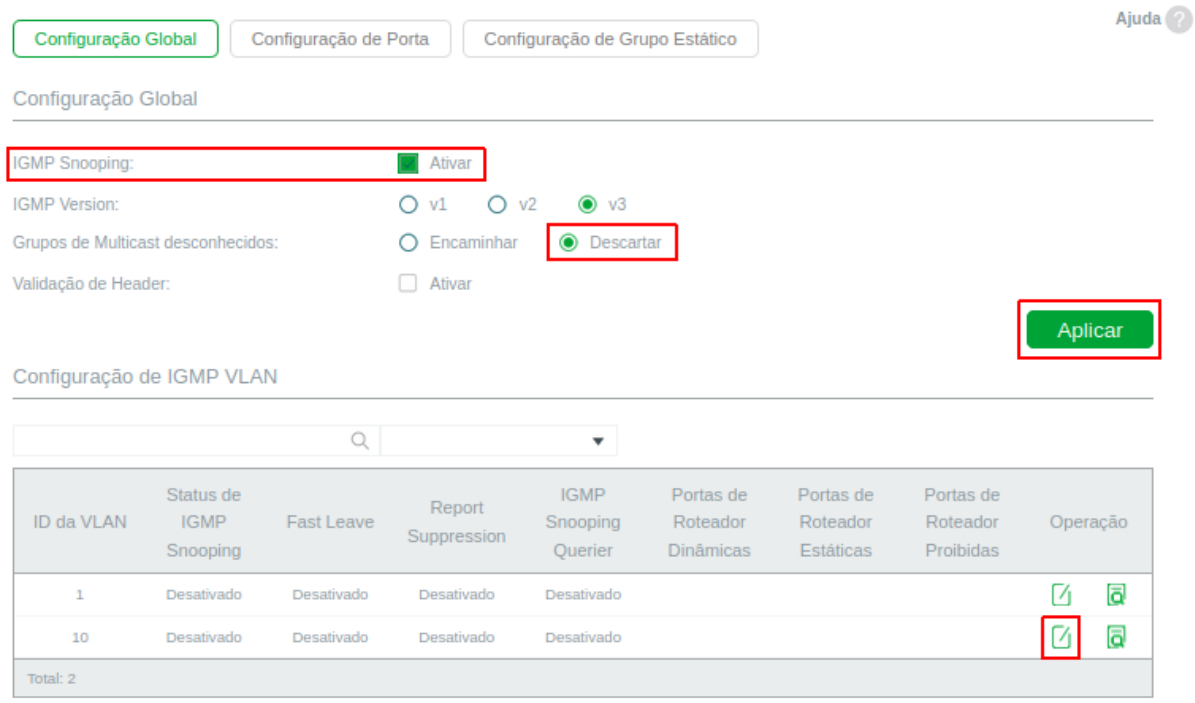


Configurando o Cenário

Após a troca de canal, o cliente (Host B) ainda está recebendo dado Multicast irrelevante, os dados do canal anterior e possivelmente outros dados de Multicast desconhecido, os quais aumentam a carga da rede e resultam em congestionamento da mesma.

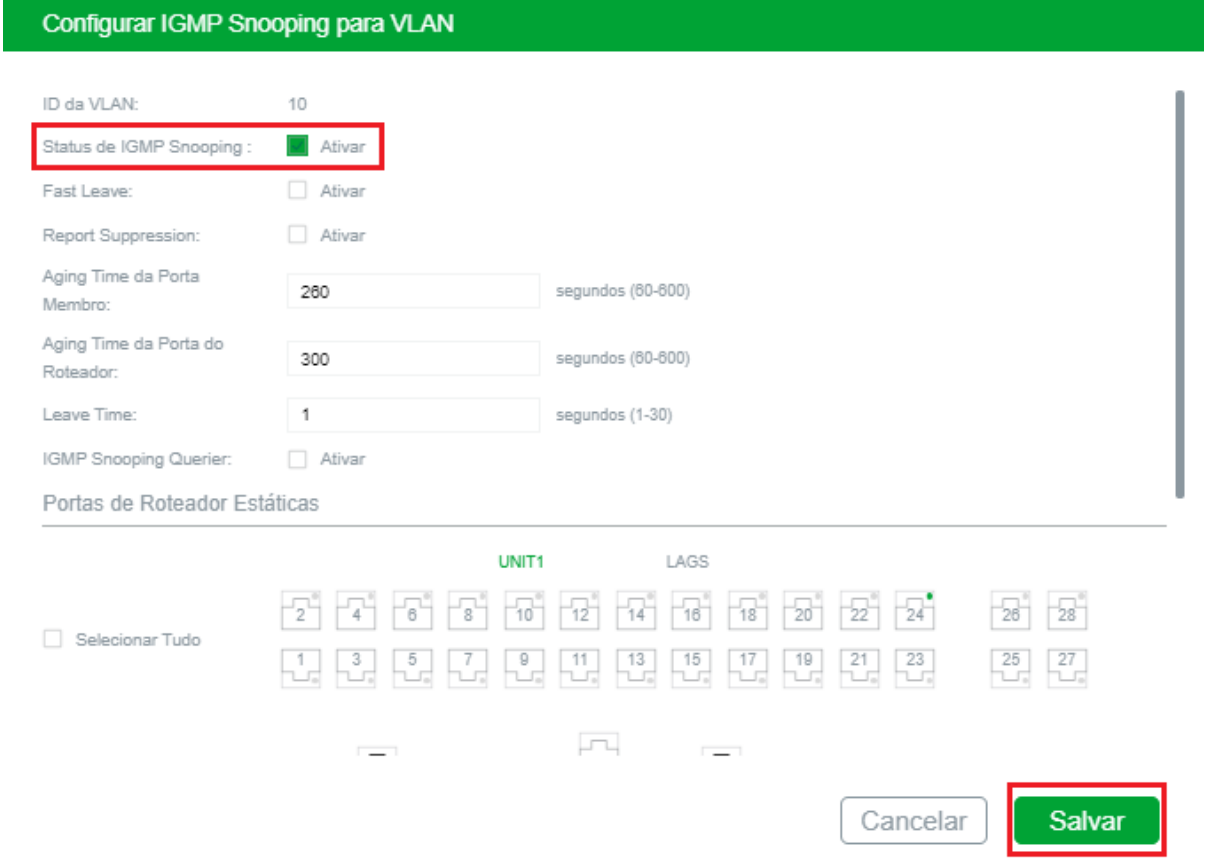
Para evitar que o Host B receba dados Multicast irrelevantes, você pode habilitar o Fast leave na porta 1/0/2 e configure para que o switch descarte dados de Multicast desconhecido. Para trocar de canal, o Host B envia uma mensagem de leave a respeito de deixar o canal anterior. Com o Fast Leave habilitado na porta 1/0/2, o switch irá então descartar dados Multicast do canal anterior, o que garante que o Host B somente receberá dados Multicast do novo canal e a rede Multicast ficará impedida.

1. Crie a VLAN 10. Adicione a porta 1/0/2 para a VLAN como porta untagged e a porta 1/0/4 como porta tagged. Configure o PVID das duas portas como 10. Para mais detalhes vá até Configuração da VLAN 802.1Q.
2. Vá até o menu **FUNÇÕES L2 > Multicast > IGMP Snooping > Configuração Global** para carregar à seguinte página. Na seção **Configuração Global** habilite o IGMP Snooping Globalmente e configure Grupos de Multicast Desconhecido como **Descartar**.

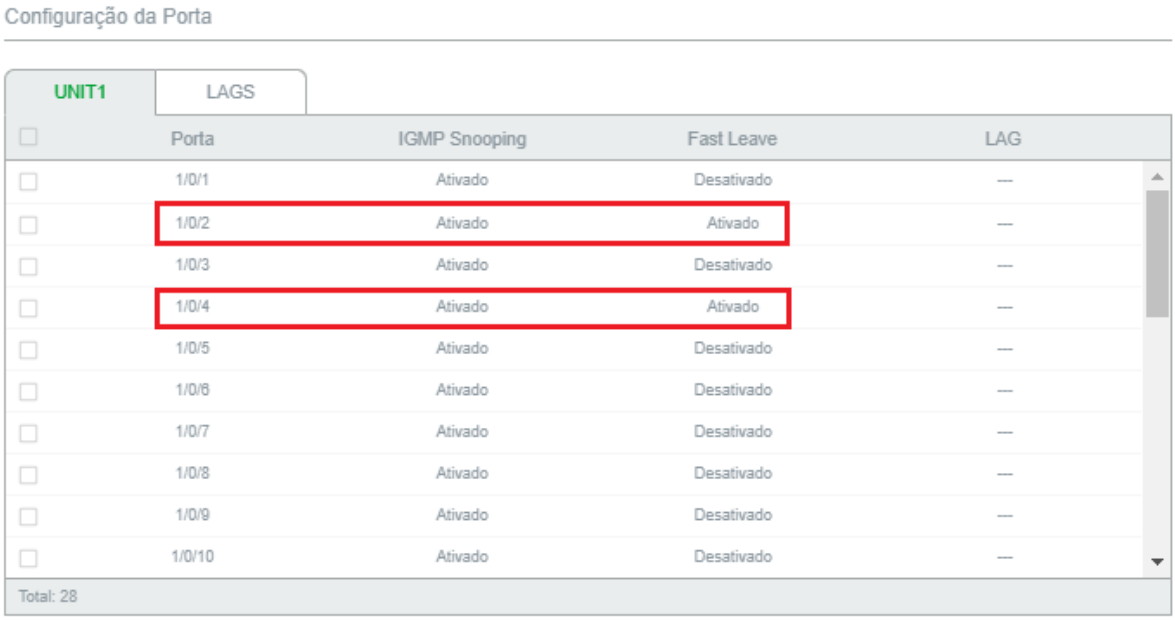


> IGMP Snooping e MLD Snooping compartilham as mesmas configurações de Multicast desconhecido, então você deve habilitar o MLD Snooping globalmente no menu **FUNÇÕES L2 > Multicast > MLD Snooping > Configuração Global** ao mesmo tempo.

3. Na seção **Configuração IGMP VLAN** clique em na VLAN 10 para carregar a seguinte página. Habilite o IGMP Snooping para a VLAN 10.



4. Vá até o menu **FUNÇÕES L2 > Multicast > IGMP Snooping > Configuração de Porta** para carregar a seguinte página. Habilite o IGMP Snooping na porta 1/0/2 e porta 1/0/4 e então habilite o Fast Leave na porta 1/0/2.



5. Clique em Salvar para salvar as configurações.

Exemplo de Configuração de Filtragem Multicast

Requisitos da Rede

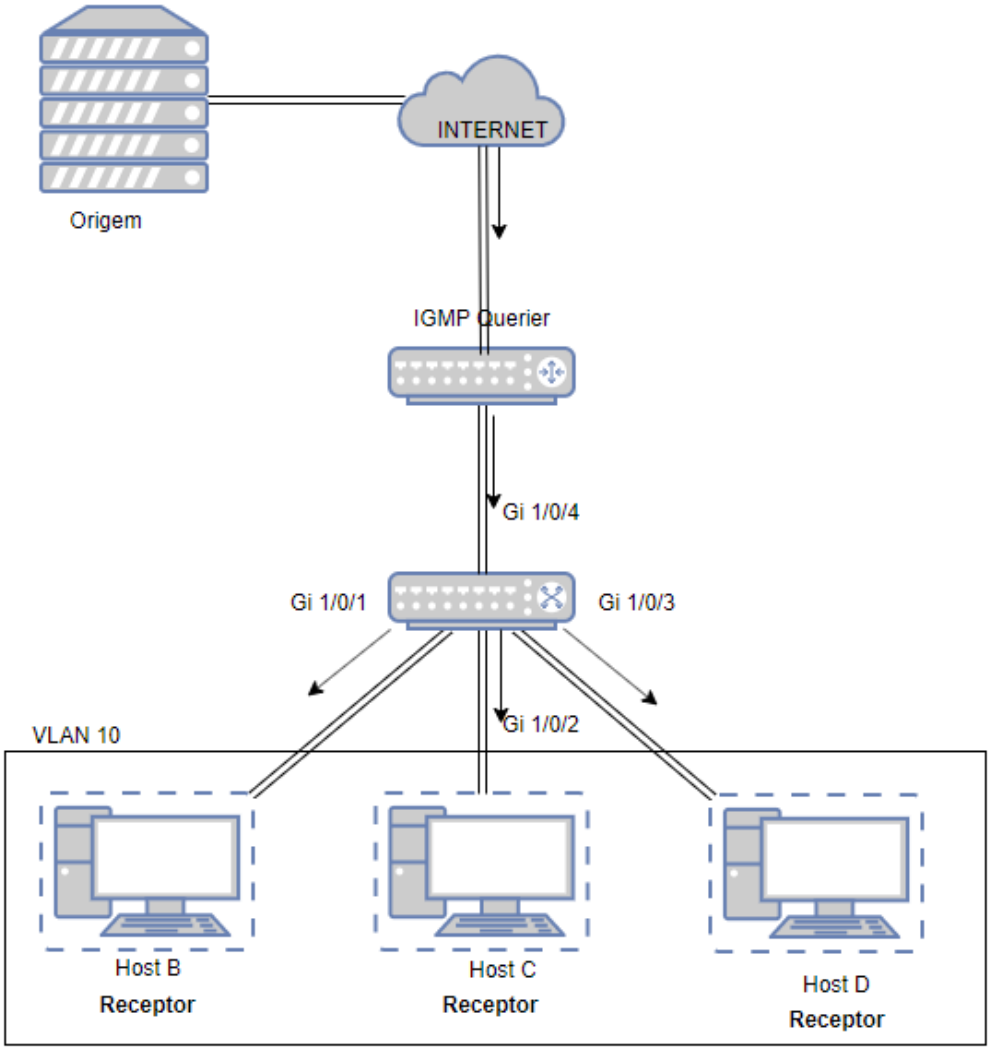
Host B, Host C e Host D estão na mesma SubRede. Host C e Host D recebem somente dados Multicast enviados pelo 225.0.0.1, enquanto o Host B recebe todos dos dados Multicast exceto o enviado por 225.0.0.2.

Configurando o Cenário

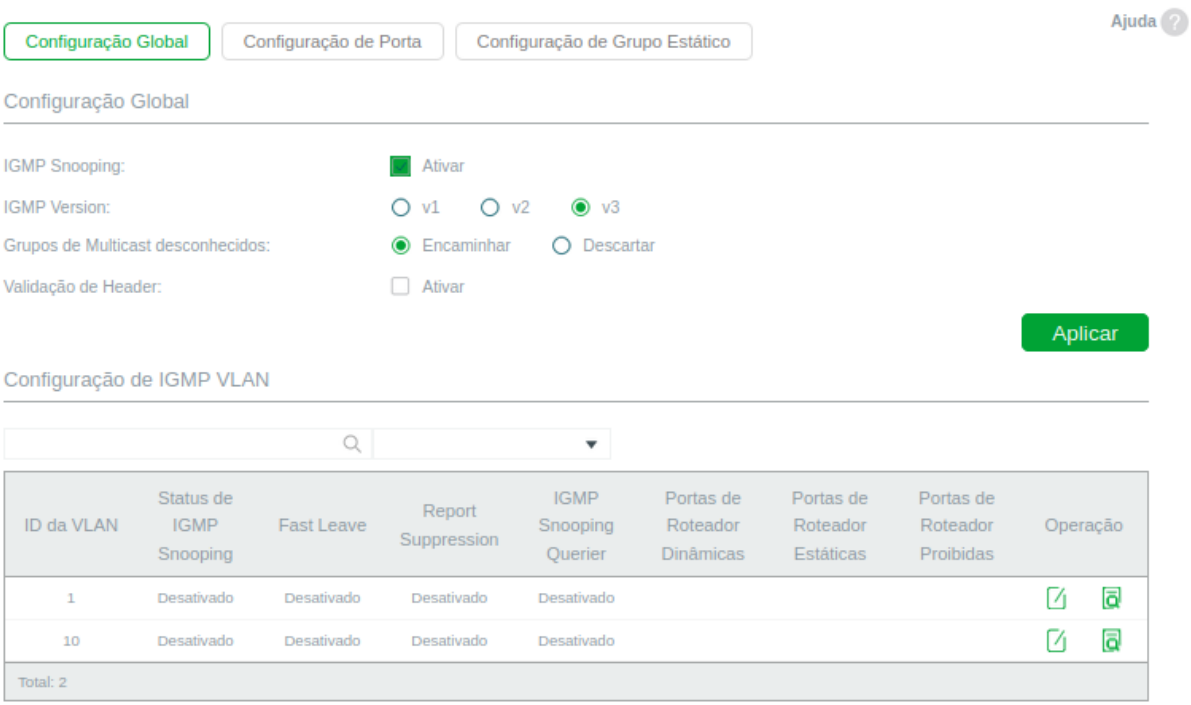
Com as funções para gerenciar os grupos Multicast, mecanismos de Blacklist e Whitelist (vinculo de perfis), o switch consegue permitir portas específicas para ingressar à grupos específicos ou impedir portas específicas de ingressar em grupos Multicast específicos. Você pode conseguir essa função de filtragem cirando um perfil e vinculando-o à porta correspondente.

Topologia de Rede

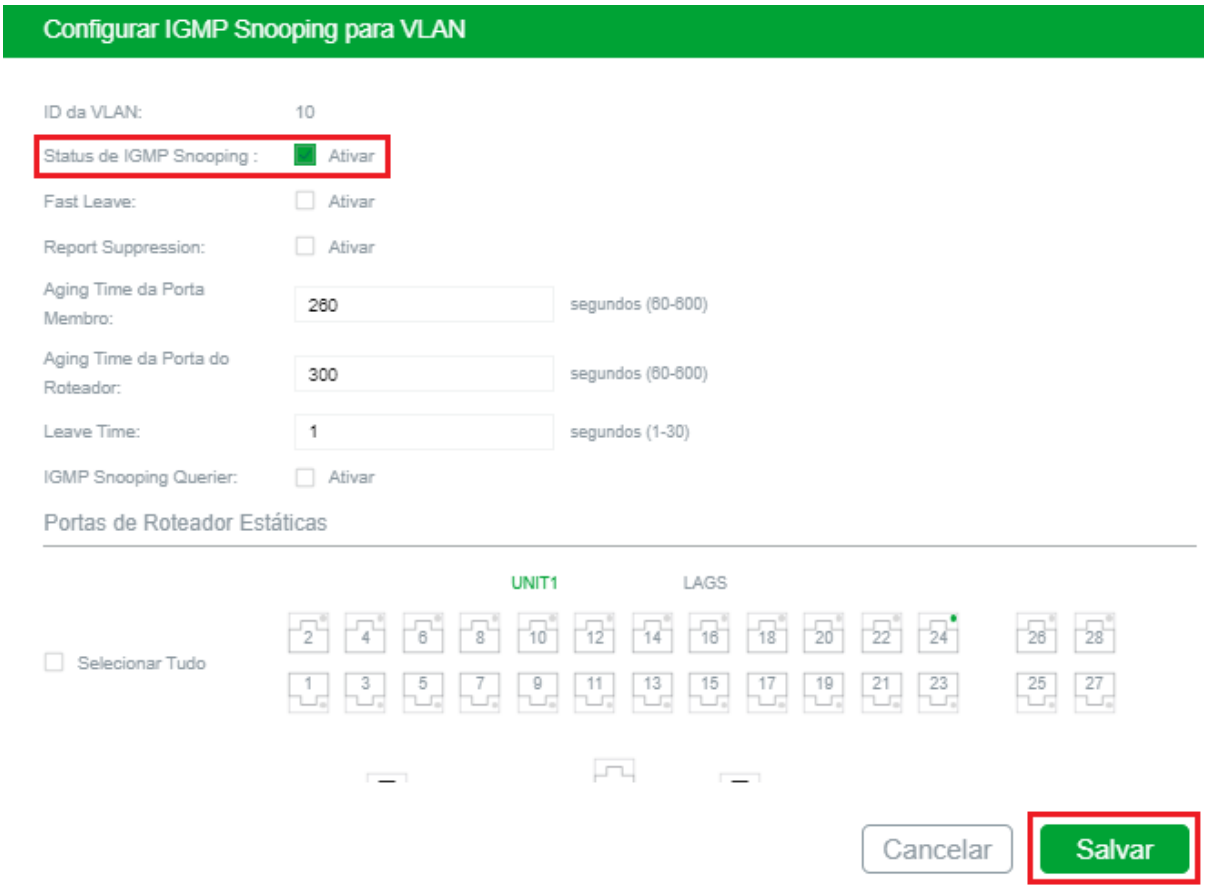
Como mostrado na topologia de rede a seguir, Host B está conectado à porta 1/0/1, Host C está conectado à porta 1/0/2 e host D está conectado à porta 1/0/3. Todos estão na VLAN 10.



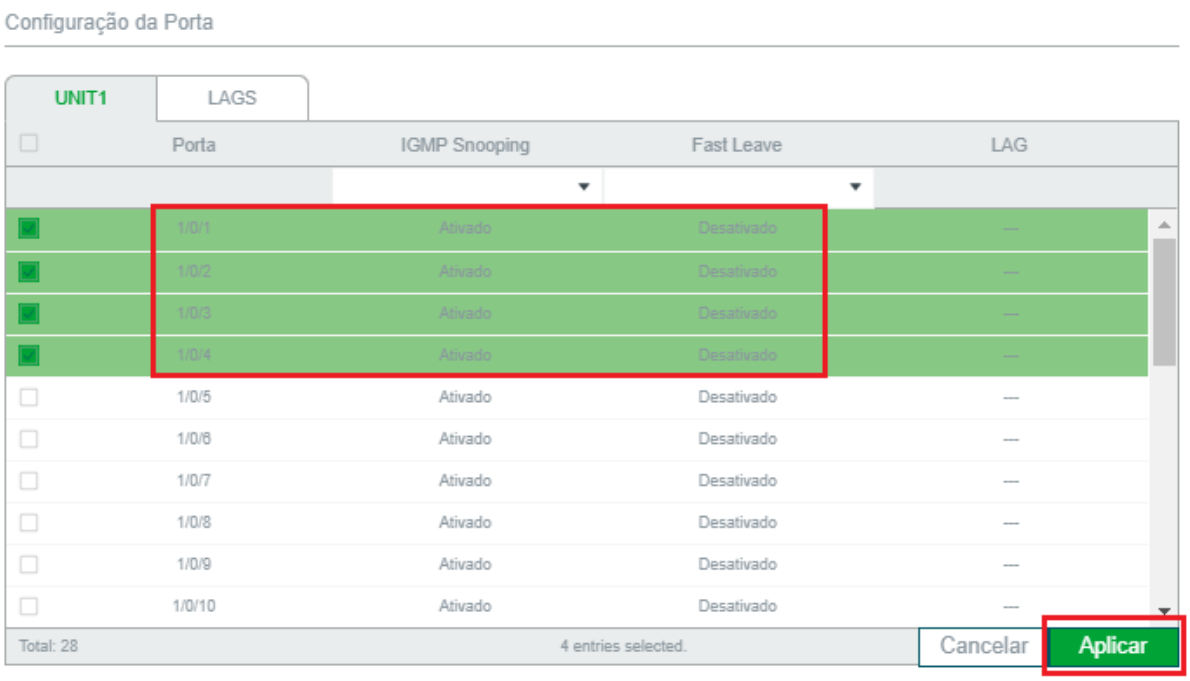
1. Crie a VLAN 10. Adicione as portas 1/0/1-3 à VLAN como portas untagged e a porta 1/0/4 como porta tagged. Configure o PVID das portas como 10. Para mais detalhes vá até Configuração da VLAN 802.1Q.
2. Vá até o menu **FUNÇÕES L2 > Multicast > IGMP Snooping > Configuração Global** para carregar a seguinte página. Na seção **Configuração Global** habilite o IGMP Snooping Globalmente.



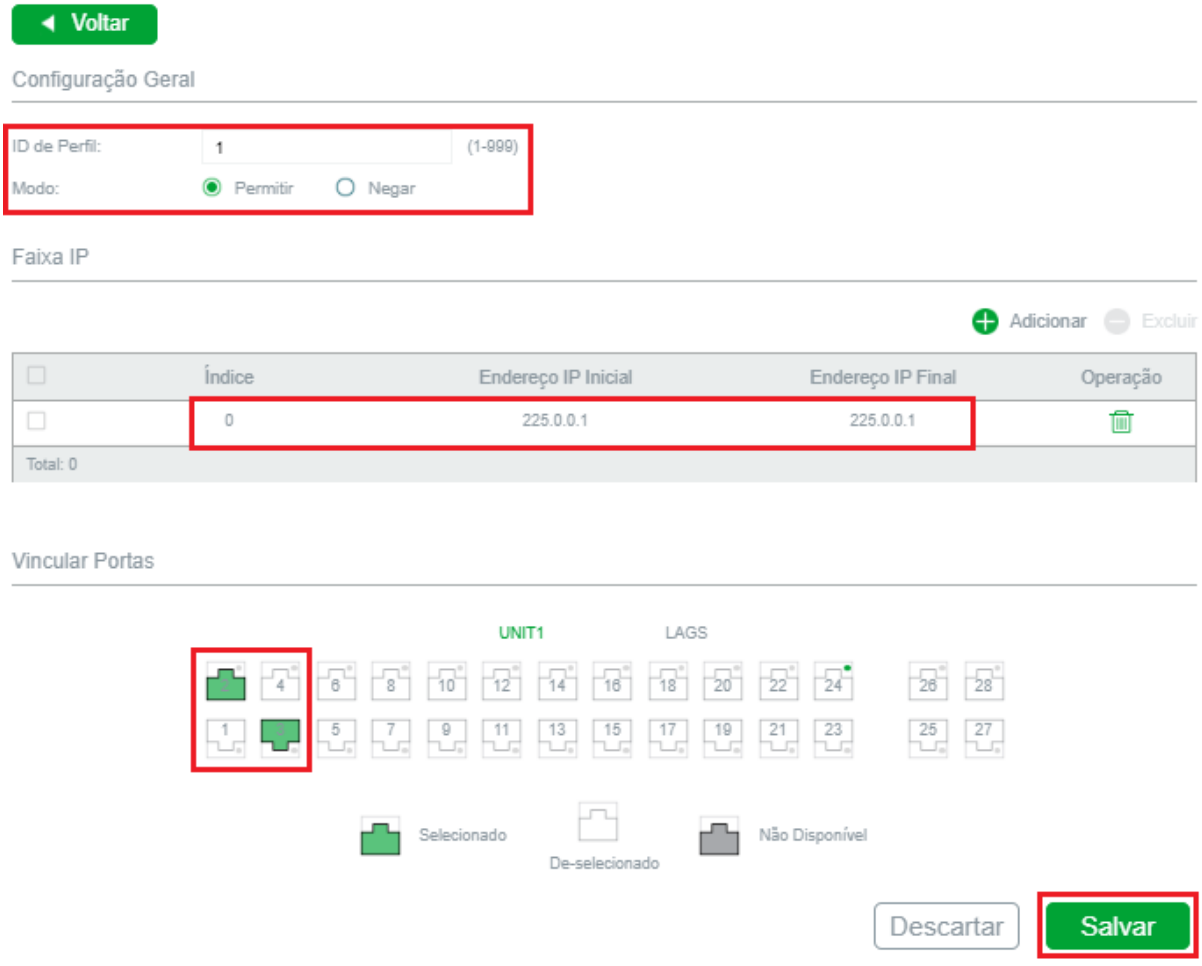
3. Na seção **Configuração IGMP VLAN**, clique em na VLAN 10 para carregar a página a seguir. Habilite IGMP Snooping para VLAN 10.



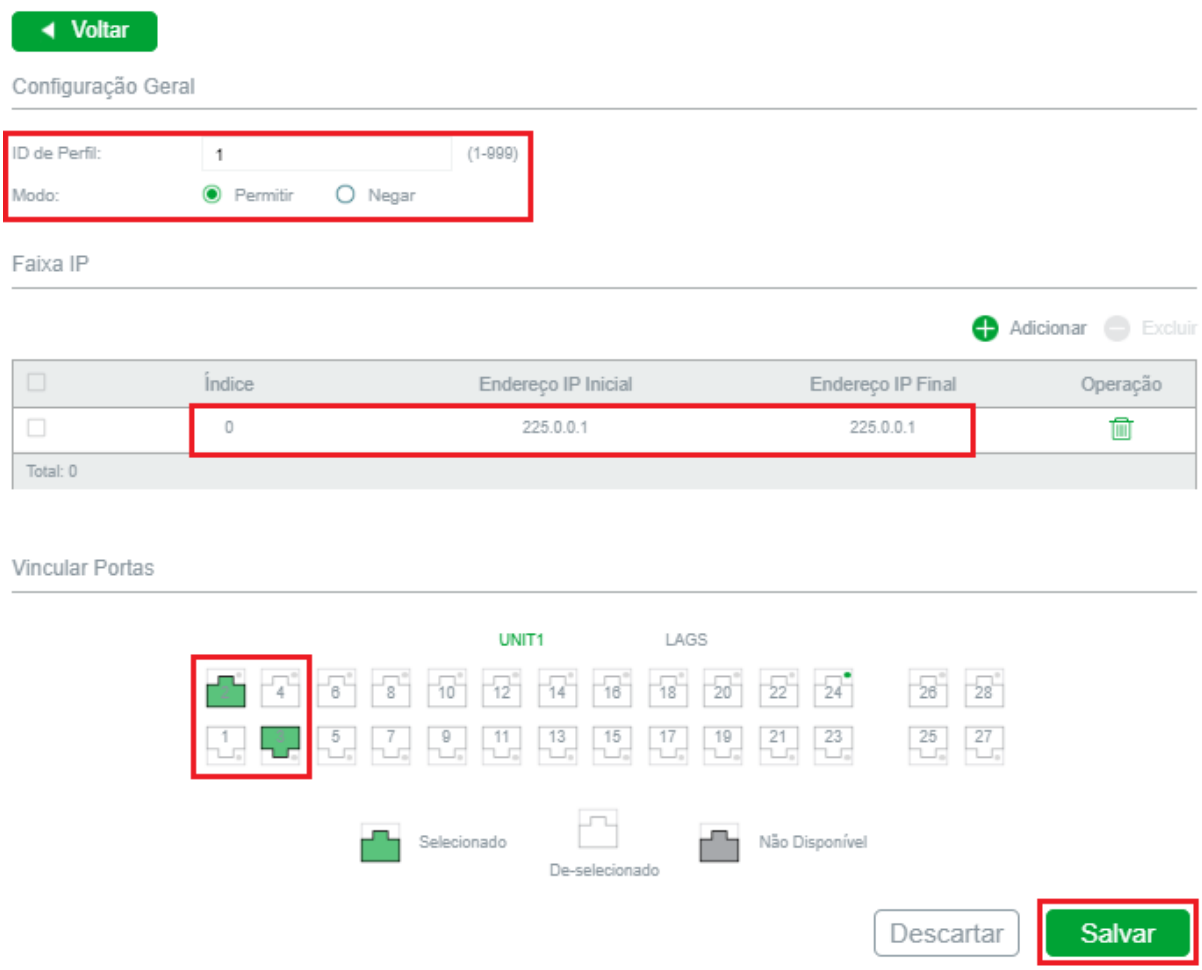
4. Vá até o menu **FUNÇÕES L2 > Multicast > IGMP Snooping > Configuração de Porta** para carregar a página a seguir.



5. Vá até o menu **FUNÇÕES L2 > Multicast > Filtragem Multicast > Perfil IPv4** e clique em Adicionar para carregar a seguinte página. Crie o Perfil 1, especifique o modo como **Permitir**, vincule o perfil às portas 1/0/2-3, e especifique o endereço IP de Multicast de filtragem como 225.0.0.1. Então clique em **Voltar** para retornar à página **Tabela de Perfil IPv4**.



6. Clique em Adicionar novamente para carregar a seguinte página. Crie o Perfil 2, especifique o modo como **Negar**, vincule o perfil à porta 1/0/1, e especifique o endereço IP de Multicast de filtragem como 225.0.0.2.



7. Clique em Salvar para salvar as configurações.

Apêndice: Configuração Padrão

Configuração Padrão do IGMP Snooping

Função	Parâmetro	Configuração Padrão
Configurações Globais para IGMP Snooping	IGMP Snooping	Desabilitado
	Versão IGMP	v3
	Grupos de Multicast Desconhecido	Encaminhar
	Validação de Cabeçalho	Desabilitado
Configurações IGMP Snooping para VLAN	IGMP Snooping	Desabilitado
	Fast Leave	Desabilitado
	Supressão de Report	Desabilitado
	Aging Time de Porta Membro	260 segundos
	Aging Time de Porta Roteadora	300 segundos
	Tempo de Leave	1 segundo
	IGMP Snooping Querier	Desabilitado
	Intervalo de Query	60 segundos

	Tempo Máximo de Resposta	10 segundos
	Intervalo de Last Member Query	1 segundo
	Last Member Query Count	2
	Origem IP de General Query	0.0.0.0
	Portas Roteadoras Estáticas	Nenhum
	Portas Roteadoras Proibidas	Nenhum
Configurações IGMP Snooping par Portas e LAGs	IGMP Snooping	Habilitado
	Fast Leave	Desabilitado
Configurações estáticas de grupo Multicast	Entradas estáticas de grupo Multicast	Nenhum

Configuração Padrão MLD Snooping

Função	**Parâmetro**	**Configuração Padrão**
Configurações Globais para MLD Snooping	MLD Snooping	Desabilitado
	Grupos de Multicast Desconhecido	Encaminhar
Configurações MLD Snooping para VLAN	MLD Snooping	Desabilitado
	Fast Leave	Desabilitado
	Supressão de Report	Desabilitado
	Aging Time de Porta Membro	260 segundos
	Aging Time de Porta Roteadora	300 segundos
	Tempo de Leave	1 segundo
	MLD Snooping Querier	Desabilitado
	Intervalo de Query	60 segundos
	Tempo Máximo de Resposta	10 segundos
	Intervalo Last Listener Query	1 segundo
	Last Listener Query Count	2
	Origem IP de General Query	::
	Portas Roteadoras Estáticas	Nenhum
	Portas Roteadoras Proibidas	Nenhum
Configurações MLD Snooping par Portas e LAGs	MLD Snooping	Habilitado
	Fast Leave	Desabilitado
Configurações estáticas de grupo Multicast	Entradas estáticas de grupo Multicast	Nenhum

Configuração Padrão do MVR

Função	Parâmetro	Configuração Padrão
Configurações Globais MVR	MVR	Desabilitado
	Modo MVR	Compatibilidade
	ID VLAN de Multicast	1
	Tempo de resposta de Query	0,5 segundos
	Grupos de Multicast Máximo	256
Configurações de Grupo MVR	Entradas de Grupo MVR	Nenhum
Configurações MVR para portas	Modo MVR	Desabilitado
	Tipo de porta MVR	Nenhum
	Fast leave	Desabilitado
Membros estáticos de Grupo MVR	Entradas de membros estáticos de grupo MVR	Nenhum

Configuração Padrão de Filtragem Multicast

Função	Parâmetro	Configuração Padrão
Configurações de Perfil	Entradas de Perfis IPv4 e IPv6	Nenhum
Configurações de filtragem Multicast em Portas e LAGs	Perfil de Vinculo	Nenhum
	Máximo de Grupos	1000
	Ação de Overflow	Descartar

SPANNING TREE

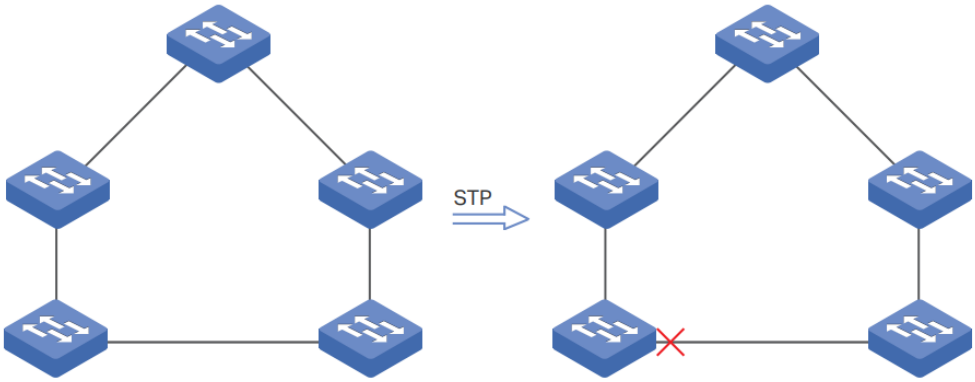
Spanning Tree

Overview

STP

STP (Spanning Tree Protocol) é um protocolo de camada 2 que evita loops na rede. Como é mostrado na Figura a baixo, o STP ajuda a:

- Bloquear portas específicas dos switches para criar uma topologia sem loop.
- Detectar alterações na topologia e gerar automaticamente uma nova topologia sem loop.



RSTP

O RSTP (Rapid Spanning Tree Protocol) fornece os mesmos recursos que o STP. Além disso, o RSTP pode fornecer uma convergência do spanning tree muito mais rápida.

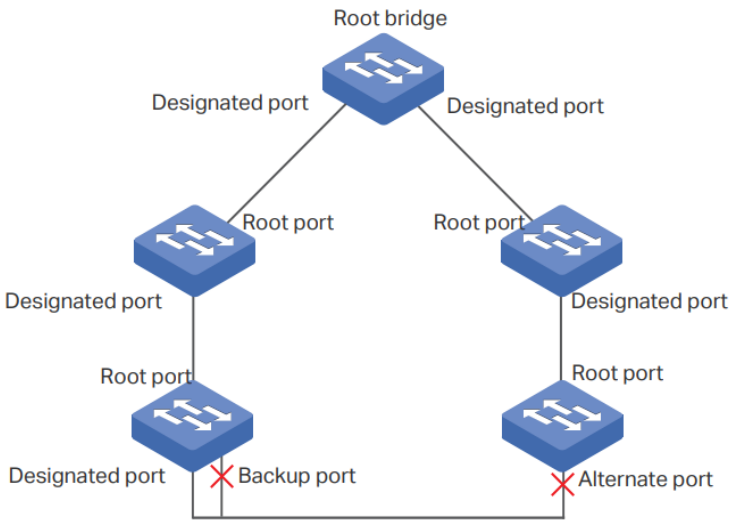
MSTP

O MSTP (Multiple Spanning Tree Protocol) também fornece a convergência rápida do spanning tree como RSTP. Além disso, o MSTP permite que as VLANs sejam mapeadas para diferentes spanning tree (instâncias MST) e o tráfego em diferentes VLANs serão transmitidos pelos respectivos caminhos e a implementação de balanceamento de carga.

Conceitos Básicos

Conceitos STP/RSTP

Com base na topologia de rede abaixo, esta seção apresentará alguns conceitos básicos em STP / RSTP.



Root Bridge

A Root raiz é a raiz de um spanning tree. O switch com o menor Bridge ID será o Bridge raiz e há apenas um bridge raiz em uma topologia spanning tree.

Bridge ID

O Bridge ID é usado para selecionar a bridge raiz. É composto de uma prioridade de 2 bytes e uma de 6 bytes do endereço MAC. A prioridade pode ser configurada manualmente no switch, o switch com o menor valor de prioridade será eleito como bridge raiz. Se a prioridade dos switches for igual, o switch com o menor endereço MAC será selecionado como o Bridge raiz.

Função da porta

- Porta raiz

  A porta raiz é selecionada na bridge não raiz (non-root) que pode fornecer o menor custo do caminho raiz. Há apenas uma porta raiz em cada bridge não raiz.

- Porta designada

  A porta designada é selecionada em cada segmento da LAN que pode fornecer o caminho para a bridge raiz de mais baixo custo desse segmento de LAN para a bridge raiz.

- Porta alternativa

  Se uma porta não for selecionada como a porta designada, ela receberá melhores BPDUs de outro switch, ele se tornará uma porta alternativa.

  No RSTP / MSTP, a porta alternativa é o backup da porta raiz. É bloqueado quando a porta raiz funciona normalmente. Quando a porta raiz falhar, a porta alternativa se tornará a nova Porta raiz.

  No STP, a porta alternativa é sempre bloqueada.

- Porta de backup

  Se uma porta não for selecionada como a porta designada, ela receberá melhores BPDUs do switch vizinho e se tornará uma porta de backup.

No RSTP / MSTP, a porta de backup é o backup da porta designada. É bloqueado quando a porta designada funciona normalmente. Depois que a porta raiz falhar, a porta de backup se tornará nova porta designada.

No STP, a porta de backup está sempre bloqueada.

- Porta desabilitada
  A porta desconectada com a função Spanning Tree ativada.

Status da porta

Geralmente, no STP, o status da porta inclui: Blocked, Listening, Learning, Forwarding e Disconnected.

- Blocked
  Nesse status, a porta recebe e envia BPDUs. Os outros pacotes são descartados.
- Listening
  Nesse status, a porta recebe e envia BPDUs. Os outros pacotes são descartados.
- Learning
  Nesse status, a porta recebe e envia BPDUs. Ele também recebe os outros pacotes de usuário para atualize sua tabela de endereços MAC, mas não os encaminha.
- Forwarding
  Nesse status, a porta recebe e envia BPDUs. Ele também recebe os outros pacotes de usuário para atualize sua tabela de endereços MAC e encaminha-os.
- Disconnected
  Nesse status, a porta não está participando do Spanning Tree e descarta todos os pacotes que recebe.

No RSTP / MSTP, o status da porta inclui: Discarding, Learning e Forwarding. O status que descarta outros pacotes são do agrupamento de blocked, disable do STP e o status de learning e forwarding corresponde exatamente ao status de learning e forwarding especificado em STP.

- Blocking
  Nesse status, a porta recebe e envia BPDUs. Os outros pacotes são descartados.
- Learning
  Nesse status, a porta recebe e envia BPDUs. Ele também recebe os outros pacotes de usuário para atualize sua tabela de endereços MAC, mas não os encaminha.
- Forwarding
  Nesse status, a porta recebe e envia BPDUs. Ele também recebe os outros pacotes de usuário para atualize sua tabela de endereços MAC e encaminha-os.
- Disconnected
  Nesse status, a porta é ativada com a função Spanning Tree, mas não está conectada a nenhum Dispositivo.

Custo do caminho (Path cost)

O custo do caminho reflete a velocidade do link da porta. Quanto menor o valor, maior a velocidade do link que a porta possui. O custo do caminho pode ser configurado manualmente em cada porta. Caso contrário, os valores de custo do caminho são calculados automaticamente de acordo com a velocidade do link, como mostrado abaixo:

Velocidade do Link	Valor do Custo do Caminho
10Mb/s	2000000
100Mb/s	200000
1Gb/ss	20000
10Gb/s	2000

Custo do caminho raiz

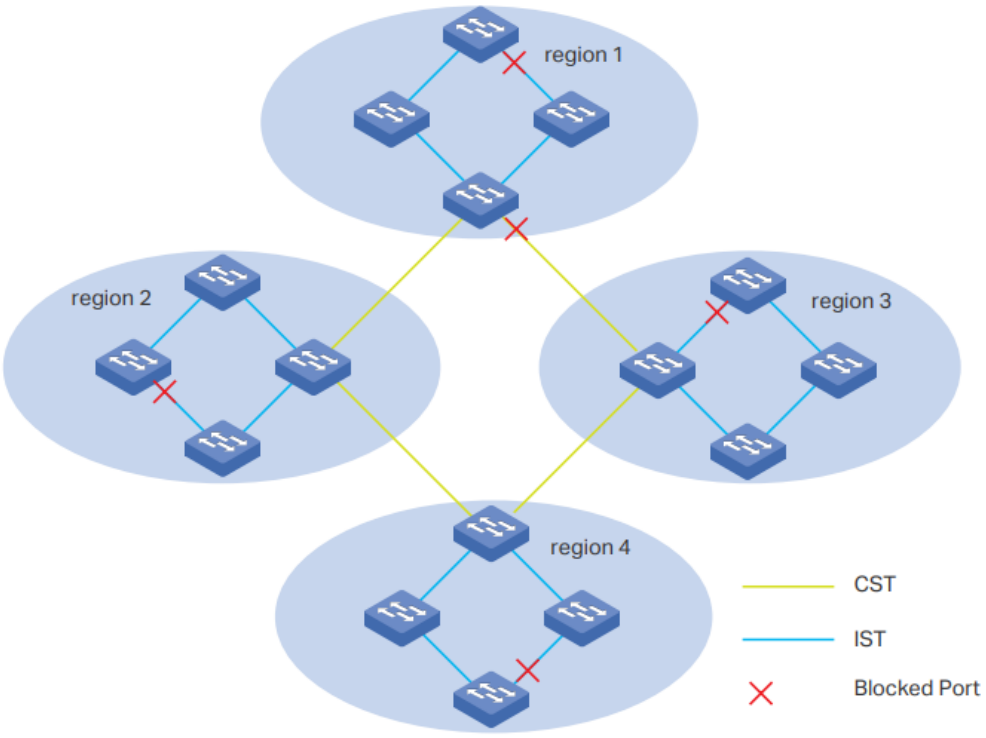
O custo do caminho raiz é o custo do caminho acumulado da bridge raiz para o outro switch. Quando a bridge raiz envia seu BPDU, o valor do custo do caminho raiz é 0. Quando um switch recebe esse BPDU, o custo do caminho raiz será aumentado de acordo com o custo do caminho da porta de recebimento. Em seguida, ele cria um novo BPDU com o novo custo do arquivo raiz e o encaminha para o próximo switch. O valor do custo acumulado do caminho raiz aumenta à medida que o BPDU se espalha ainda mais.

BPDU

BPDU é um tipo de pacote usado para gerar e manter o spanning tree, os BPDUs (Bridge Protocol Data Unit) contêm muitas informações, como ID da bridge, custo do caminho raiz, prioridade da porta e assim por diante. Os switches compartilham essas informações para ajudar a determinar o a topologia do spanning tree.

Conceitos MSTP

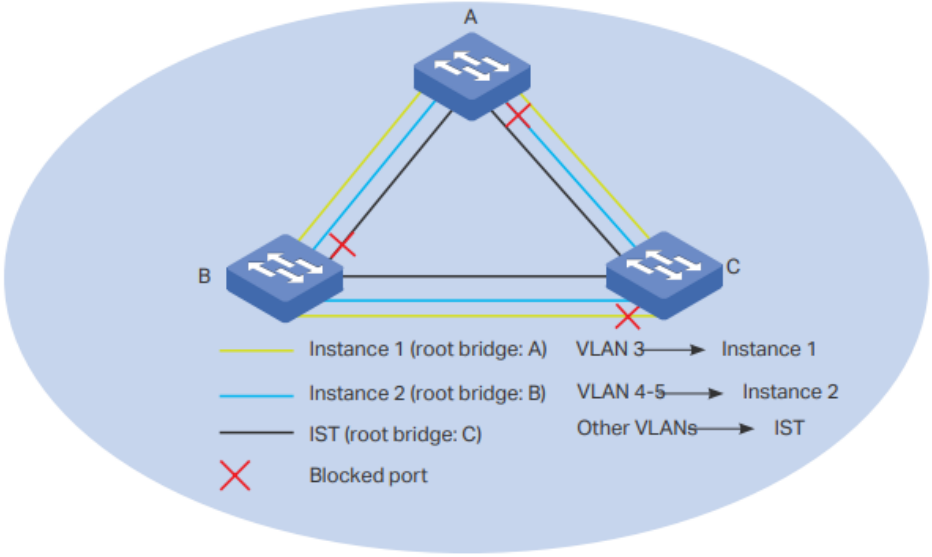
O MSTP, compatível com STP e RSTP, possui os mesmos elementos básicos usados no STP e no RSTP. Com base na topologia de rede, esta seção apresentará alguns conceitos usados apenas em MSTP.



Região MST

Uma região MST consiste em vários switches interconectados. Os switches são considerados na mesma região com as mesmas seguintes características:

- Mesmo nome de região;
- Mesmo nível de revisão;
- Mesmo mapeamento de instância de VLAN.



Mapeamento de instância de VLAN

O mapeamento de instância de VLAN descreve o relacionamento de mapeamento entre VLANs e instâncias. Várias VLANs podem ser mapeadas para uma mesma instância, mas uma VLAN pode ser mapeado para apenas uma instância. Como mostra a Figura 1-4, a VLAN 3 é mapeada para a instância 1, VLAN 4 e VLAN 5 são mapeados para a instância 2, as outras VLANs são mapeadas para o IST.

IST

O Spanning tree interna (IST), que é uma instância especial do MST com um ID de instância 0. Por padrão, todas as VLANs são mapeadas para o IST.

CST

O spanning tree comum (CST), que é o spanning tree que conecta todas as regiões do MST. Como é mostrado na Figura 1-3, a região 1-região 4 é conectada pelo CST.

CIST

Spanning tree Comum e Interna (CIST), compreendendo IST e CST. CIST é spanning tree que conecta todos os switches da rede.

Segurança STP

O STP Security evita os loops causados por configurações incorretas ou ataques de BPDU. Isto contém funções de proteção de loop, proteção de raiz, proteção de BPDU, filtro de BPDU e proteção de TC.

- Loop Protect

  A função Loop Protect é usada para evitar loops causados por congestionamentos ou falhas no link. É recomendável ativar esta função em portas raiz e portas alternativas. Se o switch não puder receber BPDUs devido a congestionamentos ou falhas de link, a porta raiz se tornará uma porta designada e a porta alternativa passará para o status de encaminhamento, então loops ocorrerão. Com a função Loop Protect ativada, a porta transitará temporariamente para o estado de bloqueio quando a porta não recebe BPDUs. Depois que o link retornar ao normal, a porta passará para o seu estado normal, para que loops possam ser evitados.

- Root Protect

  A função Root Protect é usada para garantir que a bridge raiz desejada não perca sua posição. É recomendável habilitar esta função nas portas designadas da bridge raiz. Geralmente, a bridge raiz perde sua posição depois de receber BPDUs de prioridade mais alta causada por configurações incorretas ou ataques maliciosos. Nesse caso, spanning tree deverá ser regenerado, e o tráfego necessário a ser encaminhado ao longo de links de alta velocidade pode levar a links de baixa velocidade. Com a função root protect ativada, quando a porta recebe BPDUs de maior prioridade, transita temporariamente para o estado de bloqueio. Após dois intervalos do Forward Delay, se a porta não receber quaisquer BPDUs de prioridade mais alta, ele passará para o estado normal.

- BPDU Protect

  A função BPDU Protect é usada para impedir que a porta receba BPDUs. Isto é recomendado para ativar esta função nas portas de borda. Normalmente, as portas de borda não recebem BPDUs, mas se um usuário atacar o switch maliciosamente enviando BPDUs, o sistema configura automaticamente essas portas como portas não externas e regenera a árvore de abrangência. Com a função de BPDU Protect ativada, a porta de borda será desligada quando receber BPDUs e relata esses casos ao administrador. Somente o administrador pode restaurá-la.

- BPDU Filter

A função BPDU Filter é para impedir a inundação de BPDU na rede. Recomenda-se ativar esta função nas portas de borda. Se um switch recebe BPDUs maliciosos, ele os encaminha para os outros switches participantes do spanning tree que terá continuamente regenerado. Nesse caso, o switch ocupa muita CPU ou o status do protocolo de BPDUs ficará incorreto. Com a função BPDU Filter ativada, a porta não encaminha BPDUs dos outros switches.

- TC Protect

  A função TC Protect é usada para impedir que o switch remova frequentemente as entradas de endereço MAC. É recomendável ativar essa função nas portas de switches não raiz. Um switch remove as entradas de endereço MAC ao receber TC-BPDUs (os pacotes usados para anunciar alterações na topologia da rede). Se um usuário envia maliciosamente um grande número de TC-BPDUs para um switch em um curto período, o switch estará ocupado com a remoção das entradas de endereço MAC, o que pode diminuir o desempenho e a estabilidade da rede. Com a função de TC Protect ativada, se o número de TC-BPDUs recebidos exceder o número máximo definido no limite do TC, o switch não removerá o endereço MAC entradas no ciclo de proteção do TC.

Configurações STP/RSTP

Para concluir a configuração STP / RSTP, siga estas etapas:

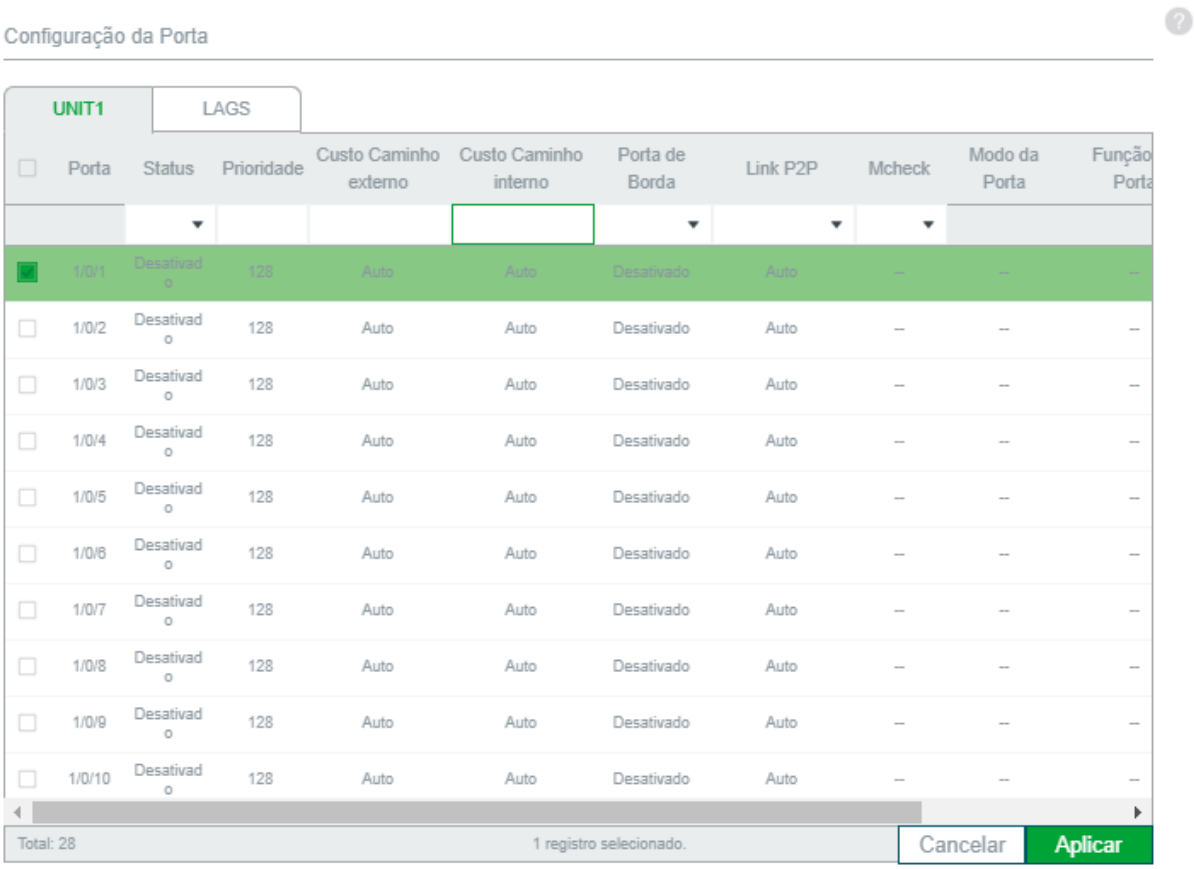
1. Configure os parâmetros STP / RSTP nas portas.
2. Configure o STP / RSTP globalmente.
3. Verifique as configurações STP / RSTP.

Diretrizes de configuração

- Antes de configurar o STP, é necessário deixar claro a função que cada o switch possuiu em uma spanning tree.
- Para evitar possíveis alterações de rede causadas por alterações nos parâmetros STP / RSTP, é recomendável ativar a função STP / RSTP globalmente após a configuração dos parâmetros.

Configurando os Parâmetros STP/RSTP nas Portas

Escolha o menu **FUNÇÕES L2 > Spanning Tree > Configurações de Porta** para carregar a seguinte página.



Siga estas etapas para configurar os parâmetros STP / RSTP nas portas:

1. Na seção **Configuração da Porta**, configure os parâmetros STP / RSTP nas portas.

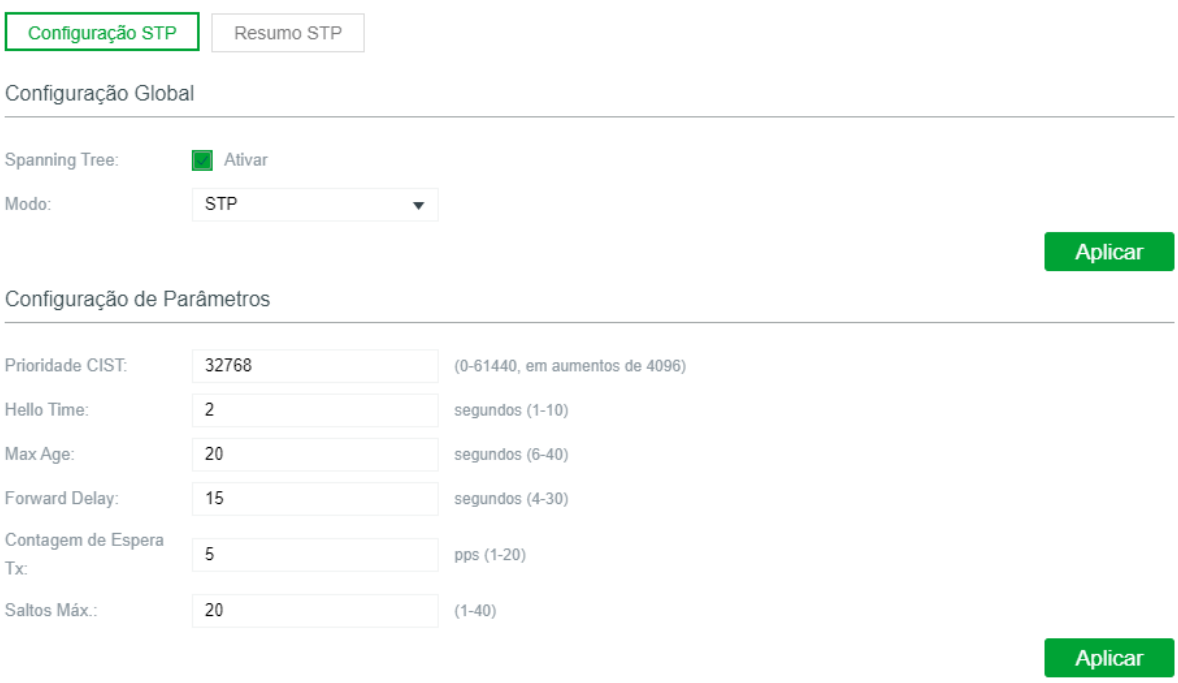
Unidade	Selecione a unidade ou LAGs desejados.
Status	Ative ou desative a função Spanning Tree na porta desejada
Prioridade	Especifique a prioridade para a porta desejada. O valor deve ser um inteiro múltiplo de 16, variando de 0 a 240. A porta com menor valor tem a maior prioridade. Quando o caminho raiz da porta é igual a outras portas, o switch comparará as prioridades da porta entre essas portas e selecionará uma porta raiz com a maior prioridade.
Custo Caminho externo	Digite o valor do custo do caminho externo. Os valores válidos são de 0 a 2000000. A configuração padrão é Automático, o que significa que a porta calcula o custo do caminho externo automaticamente de acordo com a velocidade do link da porta. Para STP / RSTP, o custo do caminho externo indica o custo do caminho da porta no STP. A porta com o menor custo do caminho raiz será eleita como a porta raiz do switch. Para MSTP, o custo do caminho externo indica o custo do caminho da porta no CST.

Custo Caminho interno	Digite o valor do custo do caminho interno. A configuração padrão é Automático, que significa que a porta calcula o custo do caminho interno automaticamente de acordo com a velocidade do link da porta. Este parâmetro é usado apenas no MSTP e você não precisa configurá-lo se o modo de spanning tree for STP / RSTP. Para o MSTP, o custo interno do caminho é usado para calcular o custo do caminho no IST. A porta com o menor custo do caminho raiz será eleita como a porta raiz no IST.
Edge Port	Selecione Ativar para definir a porta como uma porta de borda. Quando a topologia é alterada, a porta de borda pode transitar seu estado de blocking para forwarding diretamente. Para a geração rápida do spanning tree, é recomendável definir as portas que estão conectadas aos dispositivos finais como portas de borda.
Link P2P	Selecione o status do link P2P (ponto a ponto) ao qual as portas estão conectadas. Durante a regeneração do spanning tree, se a porta do P2P link é eleito como a porta raiz ou a porta designada, ele pode transitar seu estado para forwarding diretamente. Existem três opções suportadas: Auto, Open (Force) e Closed (Force). Por padrão, é Auto. **Auto:** O switch verifica automaticamente se a porta está conectada a um link P2P, depois define o status como Open ou Closed. **Abrir** (Forçar): Uma porta é definida como a que está conectada a um link P2P. Deverá ser verificado o link primeiro. **Fechar** (Forçar): Uma porta é definida como aquela que não está conectada a um link P2P. Deverá ser verificado o link primeiro.
MCheck	Selecione se deseja executar operações MCheck na porta. Se uma porta em um dispositivo habilitado para RSTP / MSTP está conectado a um dispositivo habilitado para STP, a porta mudará para o modo compatível com STP e enviará pacotes em formato do STP. MCheck é usado para alternar o modo da porta de volta para RSTP / MSTP depois que a porta for desconectada do dispositivo habilitado para STP. A configuração pode entrar em vigor apenas uma vez, depois que o status MCheck da porta mudará para desativado.
Modo da Porta	Exibe o modo da porta no spanning tree. **STP:** O modo do spanning tree da porta é STP. **RSTP:** O modo do spanning tree da porta é RSTP. **MSTP:** O modo do spanning tree da porta é MSTP.

Função da Porta	Exibe a função que a porta desempenha no spanning tree. **Porta Root:** indica que a porta é a porta raiz no spanning tree. Possui o menor custo de caminho da bridge raiz para esse switch e é usado para se comunicar com a bridge raiz. **Porta Designada:** indica que a porta é a porta designada no spanning tree. Tem o menor custo de caminho desde a bridge raiz até este segmento de rede física e é usado para encaminhar dados para o correspondente ao segmento de rede. **Porta alternativa:** indica que a porta é a porta alternativa no spanning tree. É o backup da porta raiz ou porta mestre. **Porta de backup:** indica que a porta é a porta de backup no spanning tree. É o backup da porta designada. **Desativado:** indica que a porta não está participando do spanning tree.
Status da Porta	Exibe o status da porta. **Forwarding:** a porta recebe e envia BPDUs e encaminha os dados do usuário. **Learning:** a porta recebe e envia BPDUs. Ele também recebe tráfego de usuários, mas não encaminha o tráfego **Bloqueando:** a porta recebe e envia apenas BPDUs. **Desconectada:** a porta tem a função do STP ativada, mas não é conectado a qualquer dispositivo.
LAG	Exibe a LAG a qual a porta pertence.

Configurando STP/RSTP Globalmente

Vá até o Menu **FUNÇÕES L2 > Spanning Tree > Configuração STP > Configuração STP** para carregar a página a seguir.



Siga estas etapas para configurar globalmente o STP / RSTP:

1. Na seção **Configuração de parâmetros**, configure os parâmetros globais de STP / RSTP e clique em **Aplicar**.

Prioridade do CIST	Especifique a prioridade do CIST para o switch. A prioridade CIST é um parâmetro usado para determinar a bridge raiz no STP. O switch com o valor mais baixo tem a maior prioridade. No STP / RSTP, a prioridade CIST é a prioridade do switch no STP. O switch com a prioridade mais alta será eleito como ponte raiz. No MSTP, a prioridade CISP é a prioridade do switch no CIST. O switch com a maior prioridade será eleito como a bridge raiz no CIST.
Hello Time	Especifique o intervalo entre o envio das BPDUs. O valor padrão é 2. A Bridge raiz envia BPDUs de configuração em no intervalo do Hello Time. Trabalha com o MAX Age para testar as falhas do link e manter a topologia.
Max Age	Especifique o tempo máximo que o switch pode esperar sem receber um BPDU antes de tentar regenerar a topologia spanning tree. O valor padrão é 2.
Forward Delay	Especifique o intervalo entre a transição do estado da porta de listening para learning. O valor padrão é 15. É usado para impedir que a rede cause loops temporários durante a cálculo da topologia. O intervalo entre a transição do estado da porta do learning para forwarding também é Atraso de encaminhamento (Forward Delay).
Contagem de Espera	Especifique o número máximo de BPDU que pode ser enviado em um segundo. O valor padrão é 5.

Edge Port	Selecione Ativar para definir a porta como uma porta de borda. Quando a topologia é alterada, a porta de borda pode transitar seu estado de blocking para forwarding diretamente. Para a geração rápida do spanning tree, é recomendável definir as portas que estão conectadas aos dispositivos finais como portas de borda.
Saltos Máx	Especifique as contagens máximas de BPDU que podem ser encaminhadas em uma região MST. O valor padrão é 20. Um switch recebe BPDU e depois diminui o contador de salto por um e gera BPDUs com o novo valor. Quando o salto atingir zero, o switch descartará o BPDU. Este valor pode controlar a escala do STP na região MST. Nota: Max Hops é um parâmetro configurado no MSTP. Você não precisa configurar se o modo Spanning Tree for STP / RSTP.

Para evitar trocas frequentes de rede, verifique se Hello Time, Forward Delay e Max Age conforme as seguintes fórmulas:
- 2*(Hello Time + 1) <= Max Age
- 2*(Forward Delay - 1) >= Max Age

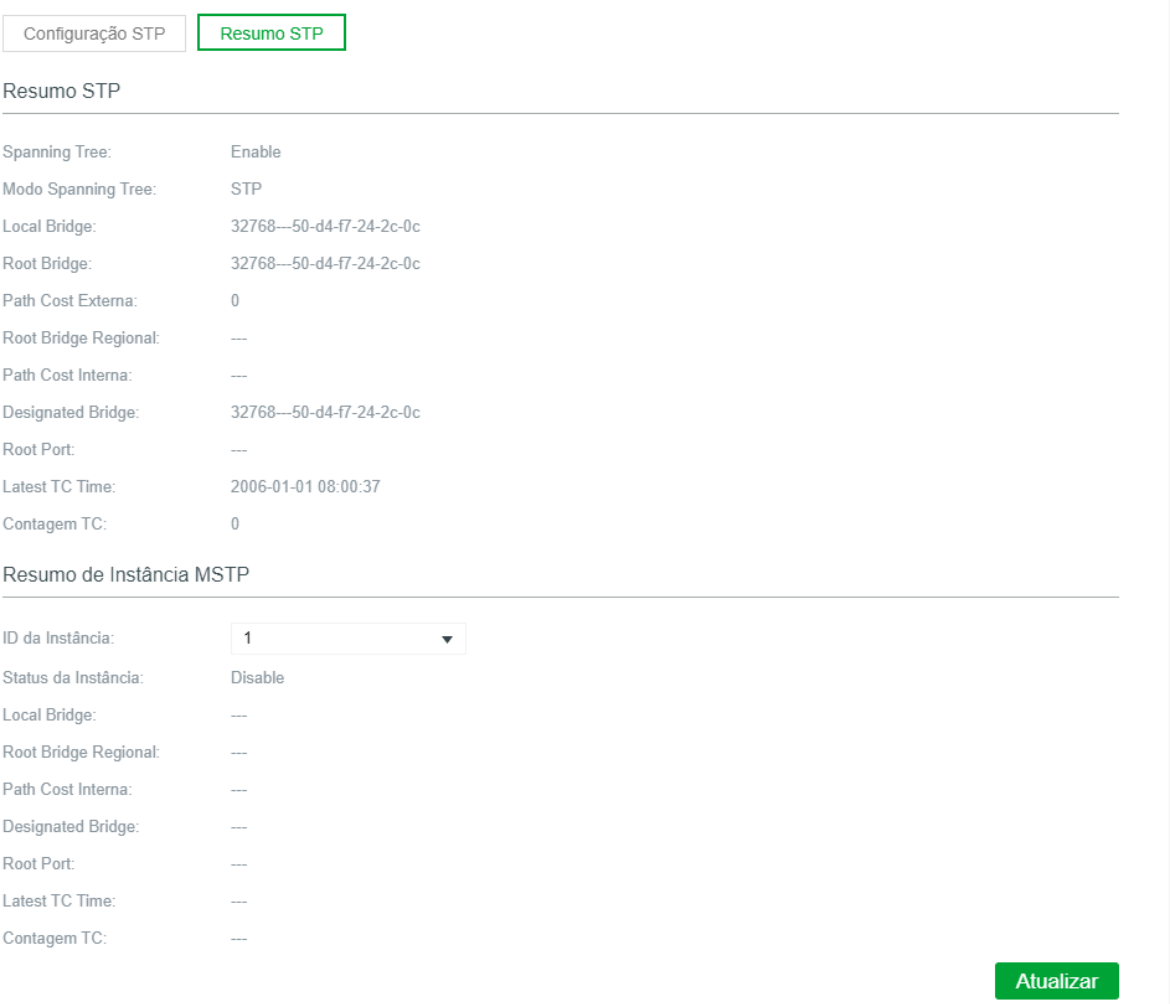
2. Na seção **Configuração Global**, ative a função Spanning Tree, escolha o modo STP como STP / RSTP e clique em **Aplicar**.

Spanning tree	Marque a caixa para ativar a função globalmente.
Modo	Selecione o modo do spanning tree desejado como STP / RSTP no switch. Por padrão, é STP. **STP:** especifique o modo do spanning tree como é STP. **RSTP:** especifique o modo do spanning tree como é RSTP. **MSTP:** especifique o modo do spanning tree como é MSTP.

Configurando STP/RSTP Globalmente

Verifique as informações STP / RSTP do seu switch depois que todas as configurações estiverem concluídas.

Escolha o menu **FUNÇÕES L2> Spanning Tree> Configuração de STP> Resumo do STP** para carregara página seguinte:



A seção **Resumo do STP** mostra as informações de resumo do spanning tree:

Spanning tree	Exibe o status da função Spanning Tree.
Modo Spanning Tree	Exibe o modo do Spanning Tree.
Local Bridge	Exibe o ID da bridge local. A bridge local é o próprio switch.
Root Bridge	Exibe o ID da bridge raiz.
Custo Caminho Externo	Exibe o custo do caminho raiz do switch para a bridge raiz.
Root Bridge Regional	É a ponte raiz do IST. Não é exibido quando você escolhe modo STP / RSTP.
Custo Caminho Interno	O custo do caminho interno é o custo do caminho raiz do switch para a bridge raiz do IST. Não é exibido quando você escolhe o modo STP / RSTP.
Designated Bridge	Exibe o ID da bridge designada. A bridge designada é o switch que possui portas designadas.
Root Port	Exibe a porta raiz do switch atual.
Latest TC time	Exibe a hora mais recente em que a topologia é alterada.
TC Count	Exibe quantas vezes a topologia foi alterada.

Configurações MSTP

Para concluir a configuração do MSTP, siga estas etapas:

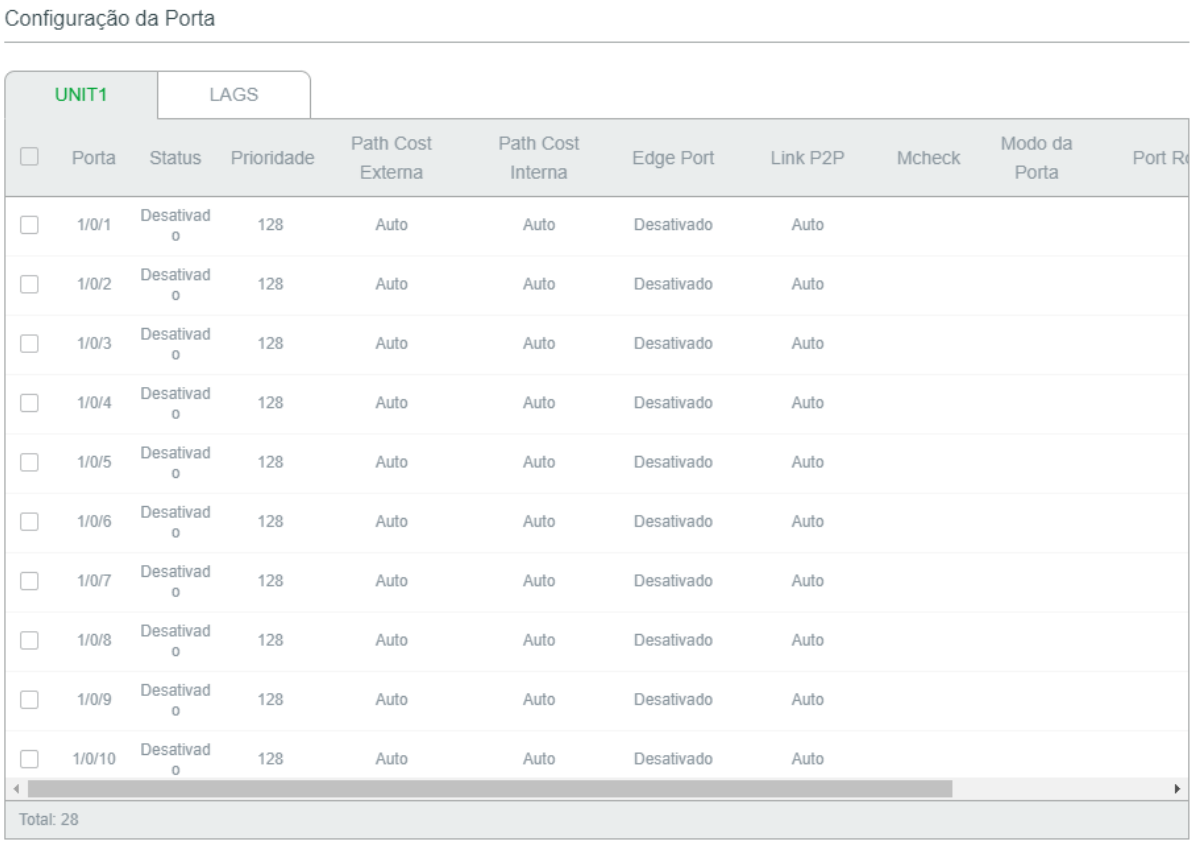
1. Configure os parâmetros nas portas no CIST.
2. Configure a região MSTP.
3. Configure o MSTP globalmente.
4. Verifique as configurações do MSTP.

Diretrizes de configuração

- Antes de configurar spanning tree, é necessário deixar claro a função que cada o switch exerce em uma topologia.
- Para evitar possíveis alterações de rede causadas por alterações nos parâmetros MSTP, é recomendável ativar a função MSTP globalmente depois de realizar as configurações e parâmetros relevantes.

Configurando Parâmetros CIST nas Portas

Escolha o menu **FUNÇÕES L2 > Spanning Tree > Configuração de Porta** para carregar a seguinte página.



Siga estas etapas para configurar parâmetros nas portas no CIST:

1. Na seção **Configuração da Porta**, configure os parâmetros nas portas.

Unidade	Selecione a unidade ou LAGs desejados.
Status	Ative ou desative a função Spanning Tree na porta desejada.
Prioridade	Especifique a prioridade para a porta desejada. O valor deve ser um inteiro múltiplo de 16, variando de 0 a 240. A porta com menor valor tem a maior prioridade. Quando o caminho raiz da porta é igual a outras portas, o switch comparará as prioridades da porta entre essas portas e selecionará uma porta raiz com a maior prioridade.
Custo Caminho externo	Digite o valor do custo do caminho externo. Os valores válidos são de 0 a 2000000. A configuração padrão é Automático, o que significa que a porta calcula o custo do caminho externo automaticamente de acordo com a velocidade do link da porta. Para STP / RSTP, o custo do caminho externo indica o custo do caminho da porta no STP. A porta com o menor custo do caminho raiz será eleita como a porta raiz do switch. Para MSTP, o custo do caminho externo indica o custo do caminho da porta no CST.
Custo Caminho interno	Digite o valor do custo do caminho interno. A configuração padrão é Automático, que significa que a porta calcula o custo do caminho interno automaticamente de acordo com a velocidade do link da porta. Este parâmetro é usado apenas no MSTP e você não precisa configurá-lo se o modo de spanning tree for STP / RSTP. Para o MSTP, o custo interno do caminho é usado para calcular o custo do caminho no IST. A porta com o menor custo do caminho raiz será eleita como a porta raiz no IST.
Edge Port	Selecione Ativar para definir a porta como uma porta de borda. Quando a topologia é alterada, a porta de borda pode transitar seu estado de blocking para forwarding diretamente. Para a geração rápida do spanning tree, é recomendável definir as portas que estão conectadas aos dispositivos finais como portas de borda.

Link P2P	Selecione o status do link P2P (ponto a ponto) ao qual as portas estão conectadas. Durante a regeneração do spanning tree, se a porta do P2P link é eleito como a porta raiz ou a porta designada, ele pode transitar seu estado para forwarding diretamente. Existem três opções suportadas: Auto, Open (Force) e Closed (Force). Por padrão, é Auto. **Auto:** O switch verifica automaticamente se a porta está conectada a um link P2P, depois define o status como Open ou Closed. **Abrir** (Forçar): Uma porta é definida como a que está conectada a um link P2P. Deverá ser verificado o link primeiro. **Fechar** (Forçar): Uma porta é definida como aquela que não está conectada a um link P2P. Deverá ser verificado o link primeiro.
MCheck	Selecione se deseja executar operações MCheck na porta. Se uma porta em um dispositivo habilitado para RSTP / MSTP está conectado a um dispositivo habilitado para STP, a porta mudará para o modo compatível com STP e enviará pacotes em formato do STP. MCheck é usado para alternar o modo da porta de volta para RSTP / MSTP depois que a porta for desconectada do dispositivo habilitado para STP. A configuração pode entrar em vigor apenas uma vez, depois que o status MCheck da porta mudará para desativado.
Modo da Porta	Exibe o modo da porta no spanning tree. **STP:** O modo do spanning tree da porta é STP. **RSTP:** O modo do spanning tree da porta é RSTP. **MSTP:** O modo do spanning tree da porta é MSTP.

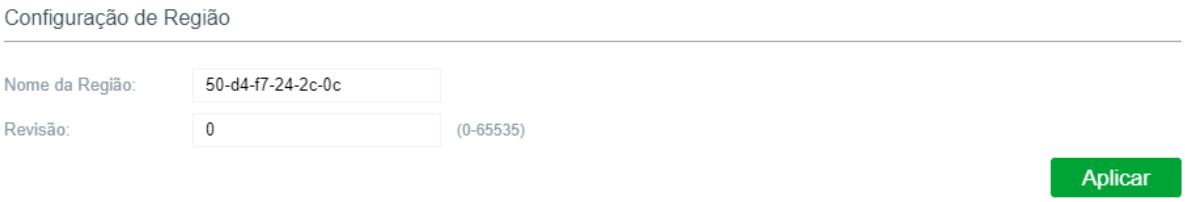
Função da Porta	Exibe a função que a porta desempenha no spanning tree. **Porta Root:** indica que a porta é a porta raiz no spanning tree. Possui o menor custo de caminho da bridge raiz para esse switch e é usado para se comunicar com a bridge raiz. **Porta Designada:** indica que a porta é a porta designada no spanning tree. Tem o menor custo de caminho desde a bridge raiz até este segmento de rede física e é usado para encaminhar dados para o correspondente ao segmento de rede. **Porta alternativa:** indica que a porta é a porta alternativa no spanning tree. É o backup da porta raiz ou porta mestre. **Porta de backup:** indica que a porta é a porta de backup no spanning tree. É o backup da porta designada. **Desativado:** indica que a porta não está participando do spanning tree.
Status da Porta	Exibe o status da porta. **Forwarding:** a porta recebe e envia BPDUs e encaminha os dados do usuário. **Learning:** a porta recebe e envia BPDUs. Ele também recebe tráfego de usuários, mas não encaminha o tráfego **Bloqueando:** a porta recebe e envia apenas BPDUs. **Desconectada:** a porta tem a função do STP ativada, mas não é conectado a qualquer dispositivo.
LAG	Exibe a LAG a qual a porta pertence.

Configurando Região MSTP

Configure o nome da região, o nível de revisão, o mapeamento da instância de VLAN do switch. Os switches com os mesmos nomes de região, o mesmo nível de revisão e a mesmo mapeamento de instância de VLAN serão considerados switches da mesma região. Além disso, configure a prioridade do switch, a prioridade e o custo do caminho das portas na instância desejada.

Configurando o nome da região e o nível de revisão

Escolha o menu **FUNÇÕES L2 > Spanning Tree> Instância MSTP> Configuração de Região** para carregar a página seguinte.



Siga estas etapas para criar uma região MST:

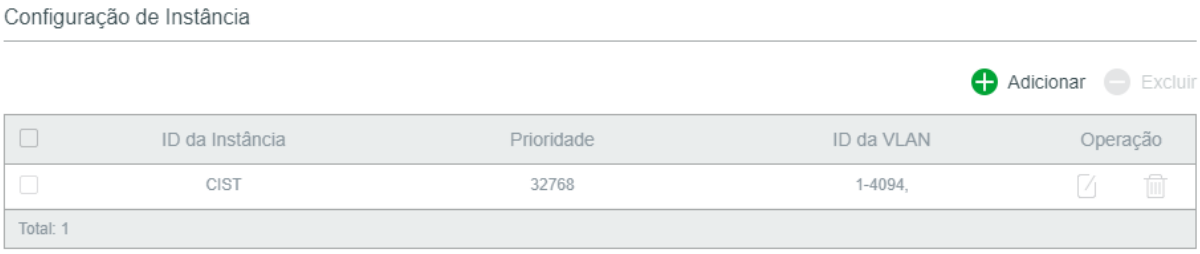
1. Na seção **Configuração de região**, defina o nome e o nível de revisão para especificar uma região MSTP.

Nome da Região	Configure o nome para uma região MST usando até 32 caracteres. Por padrão é o endereço MAC do Switch.
Revisão	Digite o nível de revisão. Por padrão é 0.

2. Clique em **Aplicar**.

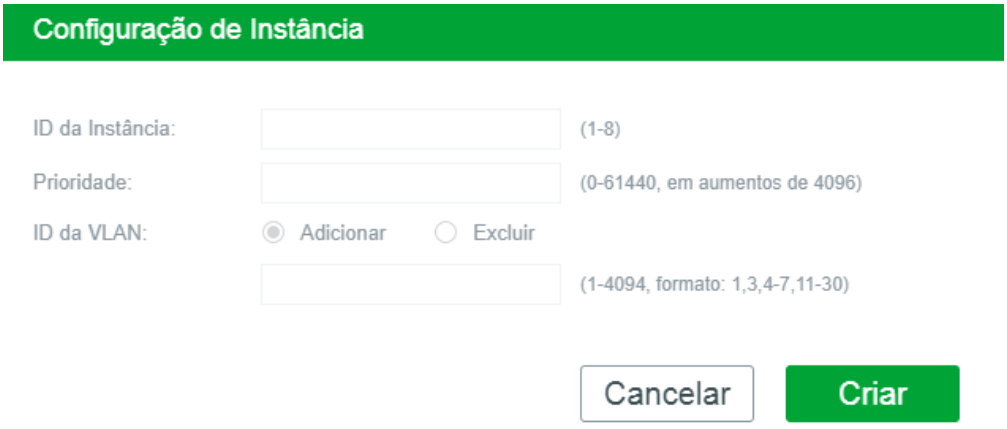
Configurando o mapeamento de instância da VLAN e a prioridade do Switch

Vá até o menu **FUNÇÕES L2 > Spanning Tree> Instância MSTP> Configuração de Instância** para carregar a página seguinte.



Siga os seguintes passo para mapear a correspondente instância da VLAN, e configure a prioridade do switch para as instâncias desejadas:

1. Na seção **Configuração de Instância** clique em Adicionar e entre com a ID da Instância, Prioridade e a ID da VLAN correspondente.

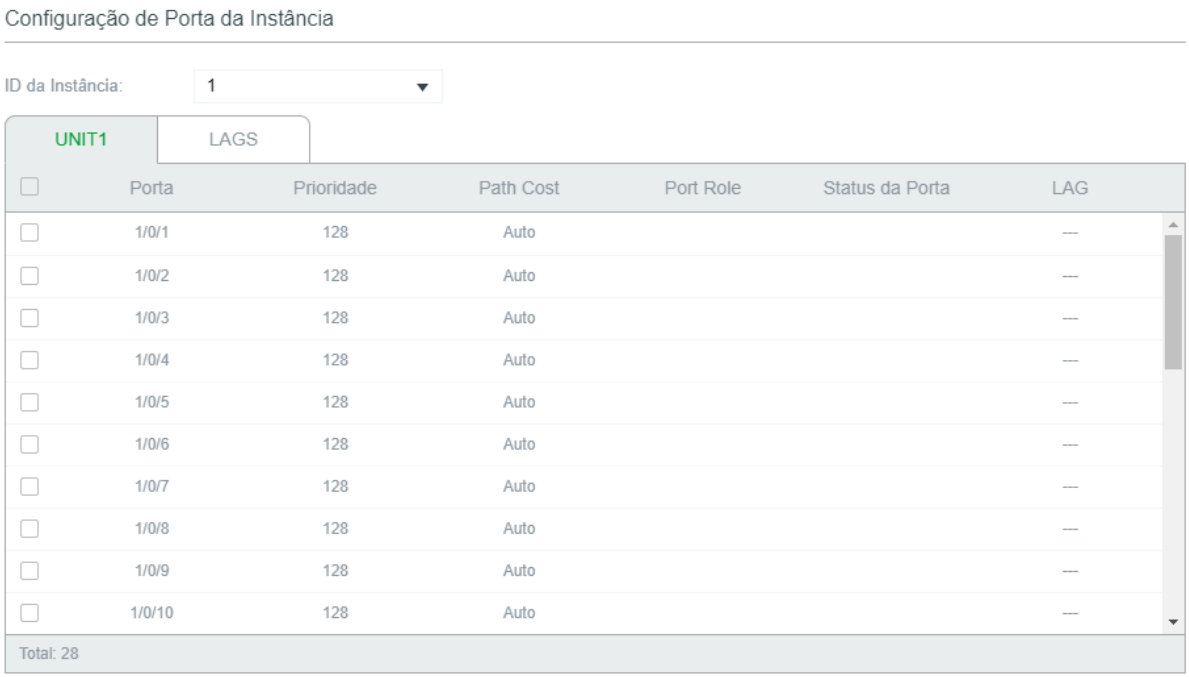


ID da Instância	Digite a ID da instância correspondente.
Prioridade	Especifique a prioridade do switch na instância correspondente. O valor que deve ser um múltiplo inteiro de 4096, variando de 0 a 61440. É usado para determinar a bridge raiz para a instância. Os switches com um valor mais baixo têm prioridade mais alta, e o switch com a prioridade mais alta será eleito a bridge raiz na instância correspondente.
ID da VLAN	Digite o ID da VLAN para mapear a VLAN para a instância desejada ou desvincular o Mapeamento de instância de VLAN.

2. Clique em **Criar**.

Configurando parâmetros na instância das portas.

Escolha o menu **FUNÇÕES L2 > Spanning Tree > Instância MSTP > Configuração de Porta de Instância** para carregar a página seguinte.



Siga estas etapas para configurar os parâmetros da instância na porta:

1. Na seção **Configuração de Porta da Instância**, selecione o ID da instância desejada.

ID da Instância	Selecione o número de ID da instância que você deseja configurar.

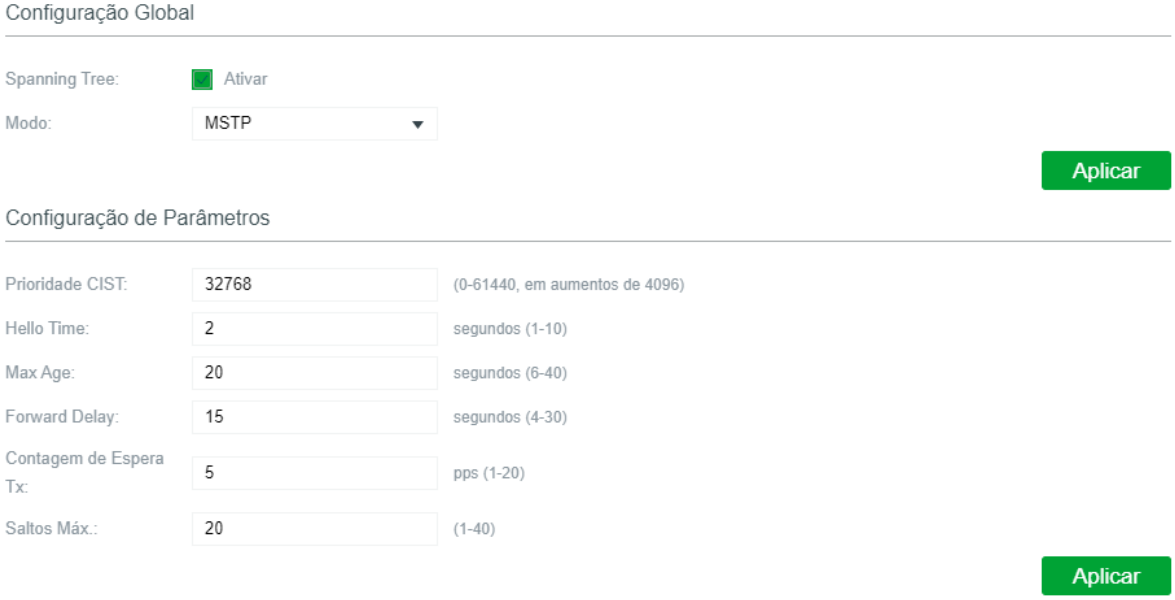
2. Configure os parâmetros da porta na instância desejada.

Unidade

Prioridade	Digite o valor do custo do caminho na instância correspondente. Os valores válidos são de 0 a 2000000. A configuração padrão é automático, o que significa que a porta calcula o custo do caminho externo automaticamente de acordo com as velocidades dos links. A porta com o menor custo do caminho raiz será eleita como a porta raiz do switch.
Função da Porta	Exibe a função que a porta desempenha no spanning tree. **Porta Root:** indica que a porta é a porta raiz no spanning tree. Possui o menor custo de caminho da bridge raiz para esse switch e é usado para se comunicar com a bridge raiz. **Porta Designada:** indica que a porta é a porta designada no spanning tree. Tem o menor custo de caminho desde a bridge raiz até este segmento de rede física e é usado para encaminhar dados para o correspondente ao segmento de rede. **Porta alternativa:** indica que a porta é a porta alternativa no spanning tree. É o backup da porta raiz ou porta mestre. **Porta de backup:** indica que a porta é a porta de backup no spanning tree. É o backup da porta designada. **Desativado:** indica que a porta não está participando do spanning tree.
Status da Porta	Exibe o status da porta. **Forwarding:** a porta recebe e envia BPDUs e encaminha os dados do usuário. **Learning:** a porta recebe e envia BPDUs. Ele também recebe tráfego de usuários, mas não encaminha o tráfego **Bloqueando:** a porta recebe e envia apenas BPDUs. **Desconectada:** a porta tem a função do STP ativada, mas não é conectado a qualquer dispositivo.
LAG	Exibe a LAG a qual a porta pertence.

Configurando MSTP Globalmente

Escolha o menu **FUNÇÕES L2 > Spanning Tree> STP Config> Configuração STP** para carregar a página seguinte.



Siga estas etapas para configurar o MSTP globalmente:

1. Na seção **Configuração de Parâmetros**, configure os parâmetros globais do MSTP e clique em **Aplicar**.

Prioridade do CIST	Especifique a prioridade do CIST para o switch. A prioridade CIST é um parâmetro usado para determinar a bridge raiz no STP. O switch com o valor mais baixo tem a maior prioridade. No STP / RSTP, a prioridade CIST é a prioridade do switch no STP. O switch com a prioridade mais alta será eleito como ponte raiz. No MSTP, a prioridade CISP é a prioridade do switch no CIST. O switch com a maior prioridade será eleito como a bridge raiz no CIST.
Hello Time	Especifique o intervalo entre o envio das BPDUs. O valor padrão é 2. A Bridge raiz envia BPDUs de configuração em no intervalo do Hello Time. Trabalha com o MAX Age para testar as falhas do link e manter a topologia.
Max Age	Especifique o tempo máximo que o switch pode esperar sem receber um BPDU antes de tentar regenerar a topologia spanning tree. O valor padrão é 2.
Forward Delay	Especifique o intervalo entre a transição do estado da porta de listening para learning. O valor padrão é 15. É usado para impedir que a rede cause loops temporários durante a cálculo da topologia. O intervalo entre a transição do estado da porta do learning para forwarding também é Atraso de encaminhamento (Forward Delay).
Contagem de Espera	Especifique o número máximo de BPDU que pode ser enviado em um segundo. O valor padrão é 5.

Saltos Máx	Especifique as contagens máximas de BPDU que podem ser encaminhadas em uma região MST. O valor padrão é 20. Um switch recebe BPDU e depois diminui o contador de salto por um e gera BPDUs com o novo valor. Quando o salto atingir zero, o switch descartará o BPDU. Este valor pode controlar a escala do STP na região MST. Nota: Max Hops é um parâmetro configurado no MSTP. Você não precisa configurar se o modo Spanning Tree for STP / RSTP.

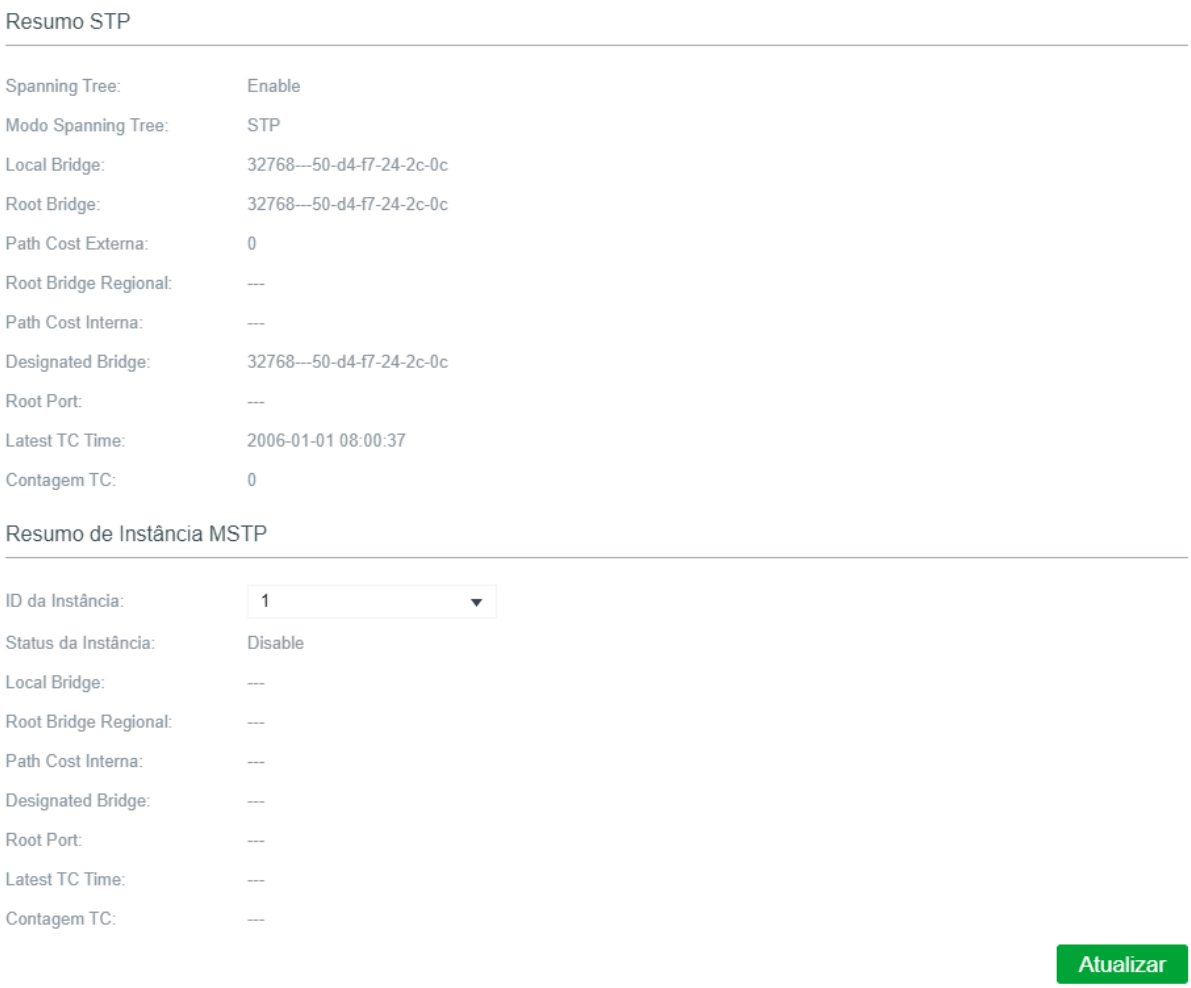
Para evitar trocas frequentes de rede, verifique se Hello Time, Forward Delay e Max Age conforme as seguintes fórmulas:
- 2*(Hello Time + 1) <= Max Age
- 2*(Forward Delay - 1) >= Max Age

2. Na seção **Configuração Global**, ative a função Spanning-Tree e escolha o STP como modo MSTP e clique em **Aplicar**.

Spanning tree	Marque a caixa para ativar a função globalmente.
Modo	Selecione o modo do spanning tree desejado como STP / RSTP no switch. Por padrão, é STP. **STP:** especifique o modo do spanning tree como é STP. **RSTP:** especifique o modo do spanning tree como é RSTP. **MSTP:** especifique o modo do spanning tree como é MSTP.

Verificando as Configurações MSTP

Escolha o menu **FUNÇÕES L2 > Spanning Tree> Configuração STP > Resumo STP** para carregar a seguinte página.



A seção **Resumo do STP** mostra as informações resumidas do CIST:

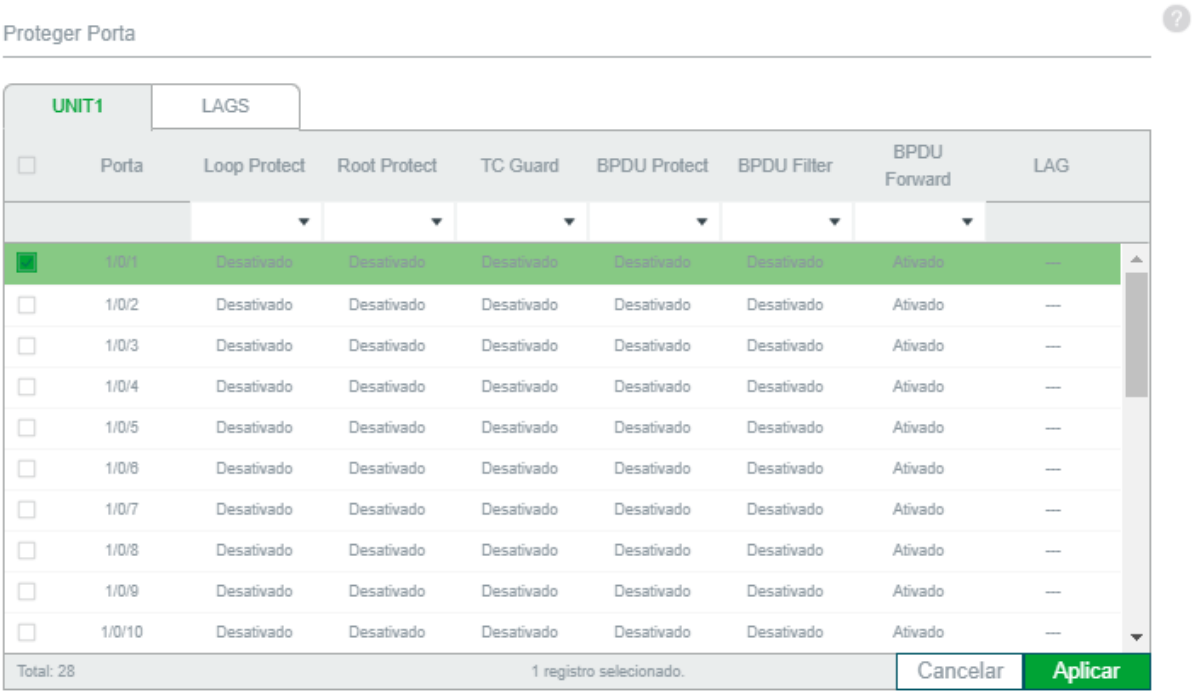
Spanning tree	Exibe o status da função Spanning Tree.
Modo Spanning Tree	Exibe o modo do Spanning Tree.
Local Bridge	Exibe o ID da bridge local. A bridge local é o próprio switch.
Root Bridge	Exibe o ID da bridge raiz.
Custo Caminho Externo	Exibe o custo do caminho raiz do switch para a bridge raiz.
Root Bridge Regional	É a ponte raiz do IST. Não é exibido quando você escolhe modo STP / RSTP.
Custo Caminho Interno	O custo do caminho interno é o custo do caminho raiz do switch para a bridge raiz do IST. Não é exibido quando você escolhe o modo STP / RSTP.
Designated Bridge	Exibe o ID da bridge designada. A bridge designada é o switch que possui portas designadas.
Root Port	Exibe a porta raiz do switch atual.
Latest TC time	Exibe a hora mais recente em que a topologia é alterada.
TC Count	Exibe quantas vezes a topologia foi alterada.

A seção **Resumo da instância do MSTP** mostra as informações nas instâncias do MST:

ID da instância	Selecione a instância desejada.
Status da Instância	Exibe o status da instância desejada.
Local Bridge	Exibe o ID da bridge local. A bridge local é o próprio switch.
Root Bridge Regional	Exibe o ID da bridge raiz na instância desejada.
Custo Caminho Interno	Exibe o custo do caminho interno. É o custo do caminho raiz do switch atual para a bridge raiz regional.
Designated Bridge	Exibe o ID da bridge designada na instância desejada.
Root Port	Exibe a porta raiz da instância desejada.
Latest TC time	Exibe a hora da última alteração de topologia.
TC Count	Exibe quantas vezes a topologia foi alterada.

Configurações de Segurança STP

Escolha o menu **FUNÇÕES L2 > Spanning Tree> Segurança STP** para carregar a seguinte página.



Configure os recursos de proteção de porta para as portas selecionadas e clique em **Aplicar**.

Unidade	Selecione a unidade ou LAGs desejados para configuração.

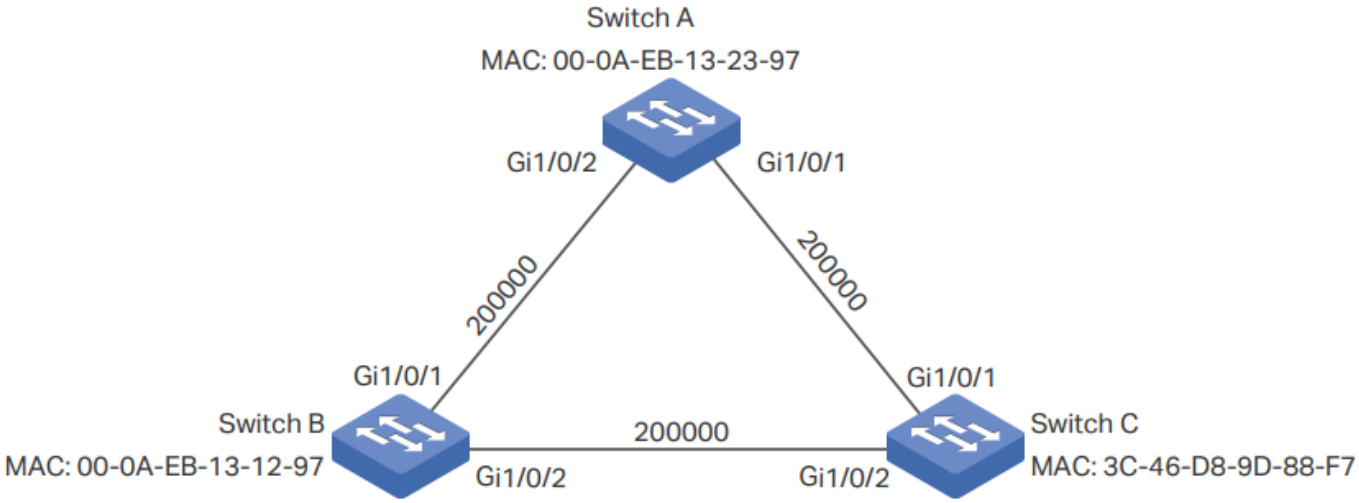
Loop Protect	Ative ou desative a proteção de loop. Recomenda-se ativar esta função em portas raiz e portas alternativas. Quando houver congestionamentos ou falhas de link na rede, e o switch não receber BPDUs do dispositivo upstream a tempo. O Loop Protect é usado para evitar loop causado pelo recálculo nessa situação. Com função de proteção de loop ativada, a porta transitará temporariamente para um estado de bloqueio após não receber BPDUs a tempo.
Root Protect	Ative ou desative o Root Protect. Recomenda-se habilitar esta função nas portas designadas da bridge raiz. Switches com configurações defeituosas podem produzir BPDU de prioridade mais alta do que da ponte raiz, e essa situação causará o recálculo do spanning tree. O Root Protect é usado para garantir que a bridge raiz desejada não perca sua posição no cenário acima. Com o root protect ativado, a porta transitará temporariamente para o estado de bloqueio quando recebe BPDUs de prioridade mais alta. Depois de dois atrasos de encaminhamento, se a porta não receber outros BPDUs de prioridade mais alta, ele vai passar para o seu estado normal.
TC Guard	Ative ou desative a função TC Guard. Recomenda-se ativar esta função nas portas de switches não raiz. A função TC Guard é usada para impedir que o switch altere frequentemente a tabela de endereços MAC. Com a função TC Guard ativada, quando o switch recebe TC-BPDUs, ele não processará os TC-BPDUs de uma só vez. O switch irá esperar por um tempo fixo e processará os TC-BPDU juntos após receber o primeiro TC-BPDU, então ele reiniciará o tempo de contagem.
BDPDU Protect	Ative ou desative a função BPDU Protect. Recomenda-se ativar esta função nas portas de borda. As portas de borda no spanning tree são usadas para conectar-se aos dispositivos finais e não receber BPDUs na situação normal. Se as portas de borda receberem BPDUs, pode ser um ataque. O BPDU Protect é usado para proteger o switch do ataque mencionado acima. Com a função de proteção BPDU ativada, as portas de borda serão desligadas quando elas receberem BPDUs e relatam esses casos ao administrador. Apenas o administrador pode restaurar o estado das portas.
BDPDU Filter	Ative ou desative o filtro BPDU. Recomenda-se ativar esta função nas portas de borda. Com a função Filtro BPDU ativada, a porta não encaminha BPDUs de outros switches.
BDPU Forward	Ative ou desative o BPDU Forward. Esta função só entra em vigor quando o spanning tree é desativado globalmente. Com o encaminhamento de BPDU ativado, a porta ainda pode encaminhar BPDUs do STP quando o spanning tree estiver desativado.

Exemplo de Configuração MSTP

O MSTP, compatível com o STP e o RSTP, pode mapear VLANs para instâncias para implementar balanceamento de carga, fornecendo um método mais flexível no gerenciamento de rede. Aqui tomamos a configuração do MSTP como um exemplo.

Requisitos de Rede

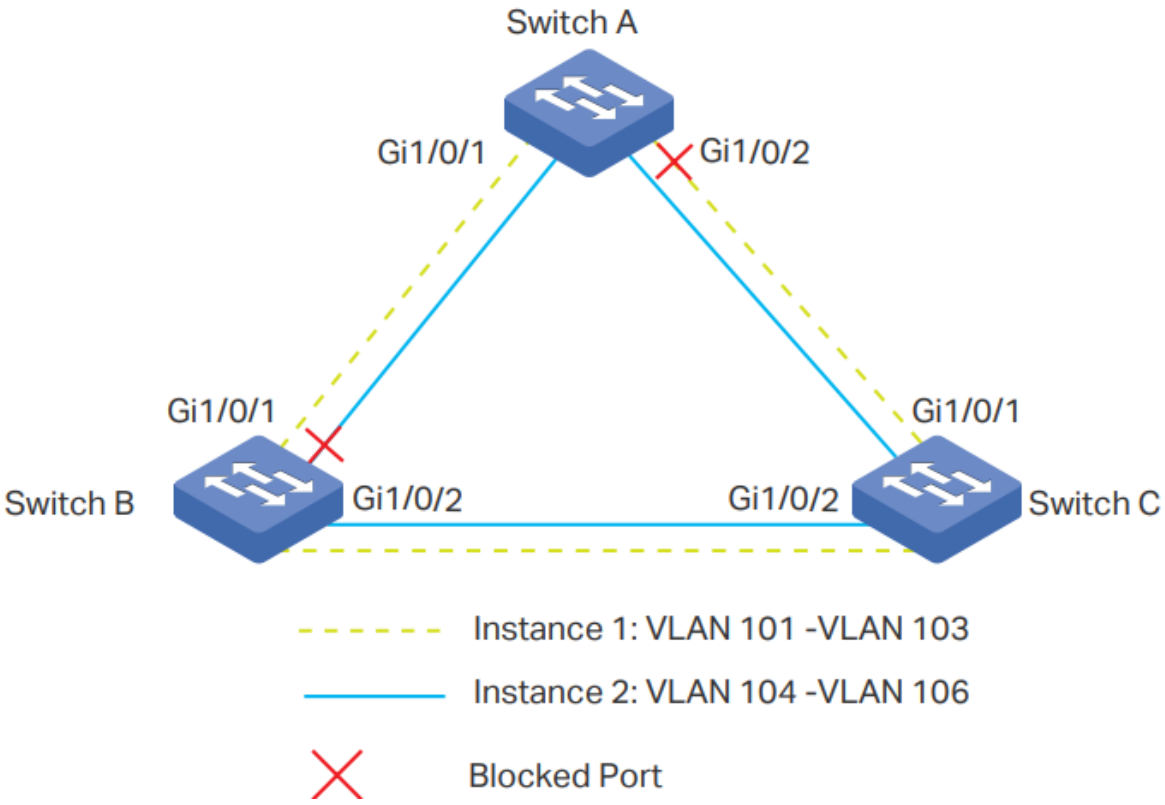
A figura abaixo exibe uma rede que consiste em três switches. Tráfego na VLAN 101-VLAN 106 é transmitido nesta rede. A velocidade do link entre os switches é de 100 Mb / s (o custo do caminho padrão da porta é 200000). É necessário que o tráfego na VLAN 101 - VLAN 103 e o tráfego na VLAN 104 - VLAN 106 ser transmitido por diferentes caminhos.



Configurando Cenário

Para atender a esse requisito, sugerimos que você configure a função MSTP nos switches. Mapeie as VLANs para diferentes instâncias para garantir que o tráfego possa ser transmitido ao longo das respectivas instâncias.

Aqui, configuramos duas instâncias para atender ao requisito, conforme mostrado abaixo:

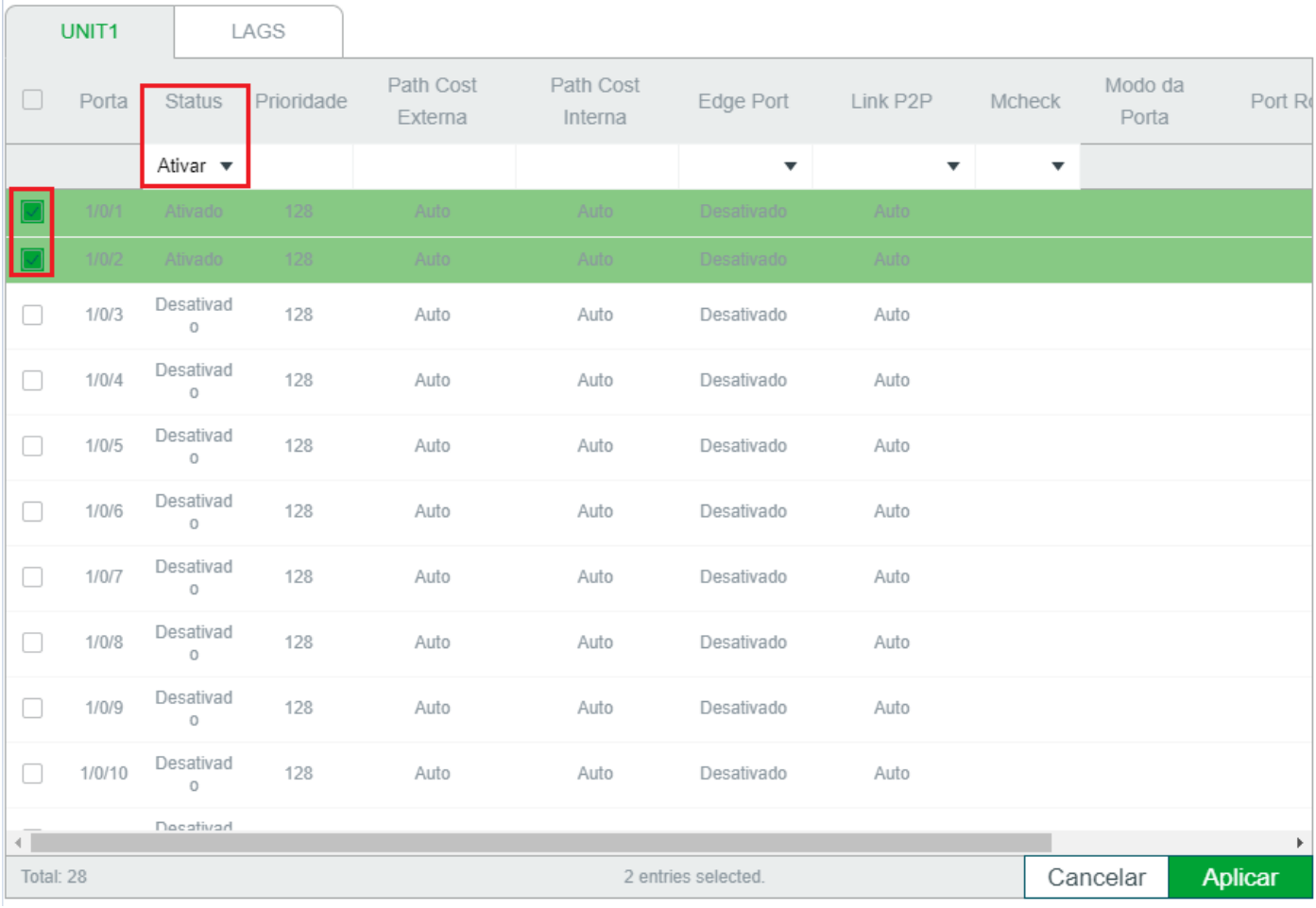


A visão geral da configuração é a seguinte:

1. Habilite a função MSTP globalmente em todos os switches.
2. Habilite a função Spanning Tree nas portas de cada switch.
3. Configure o Switch A, Switch B e Switch C na mesma região. Configure a região com o nome 1 e o nível de revisão como 100. Mapeie VLAN 101 - VLAN 103 para a instância 1 e VLAN 104 - VLAN 106 para a instância 2.
4. Configure a prioridade do Switch B como 0 para configurá-lo como a bridge raiz na instância 1; configure a prioridade do Switch C como 0 para defini-lo como a bridge raiz na instância 2.
5. Configure o custo do caminho para bloquear as portas especificadas. Por exemplo 1, defina o custo do caminho da porta 1/0/1 do switch A para que seja maior que o custo do caminho padrão (200000). Para instância 2, defina o custo do caminho da porta 1/0/2 do Switch B como maior que o custo do caminho padrão (200000). Após essa configuração, a porta 1/0/2 do Switch A na instância 1 e a porta 1/0/1 do Switch B na instância 2 serão bloqueados, pois não podem ser nem porta raiz nem porta designada.

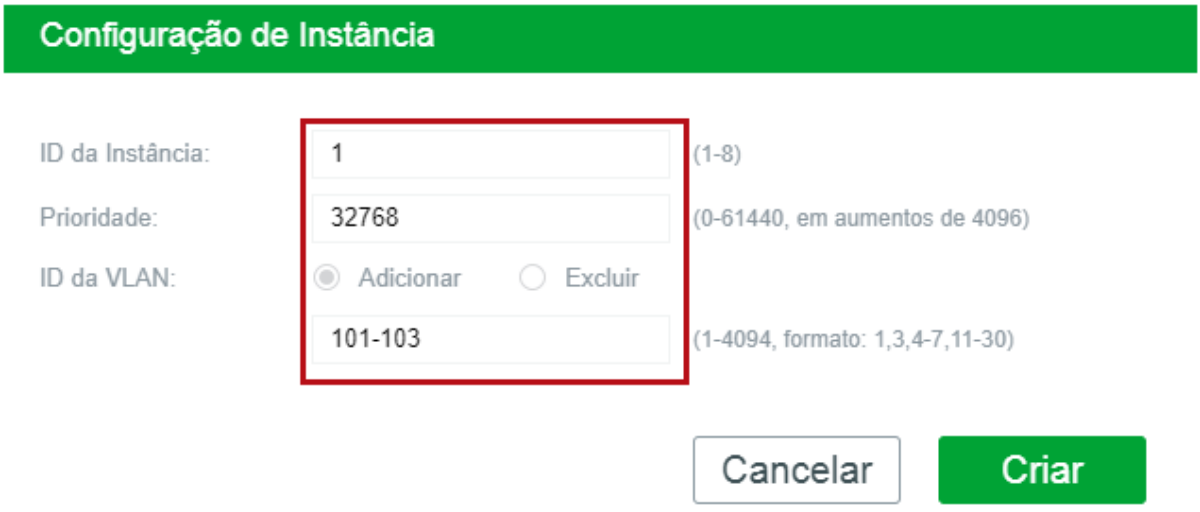
Configurações para o switch A

1. Vá ao menu **FUNÇÕES L2 > Spanning Tree > Configuração da Porta** para carregar a seguinte página. Habilite a função do STP na porta 1/0/1 e na porta 1/0/2. Aqui deixe os valores dos outros parâmetros como padrão. Clique em **Aplicar**.

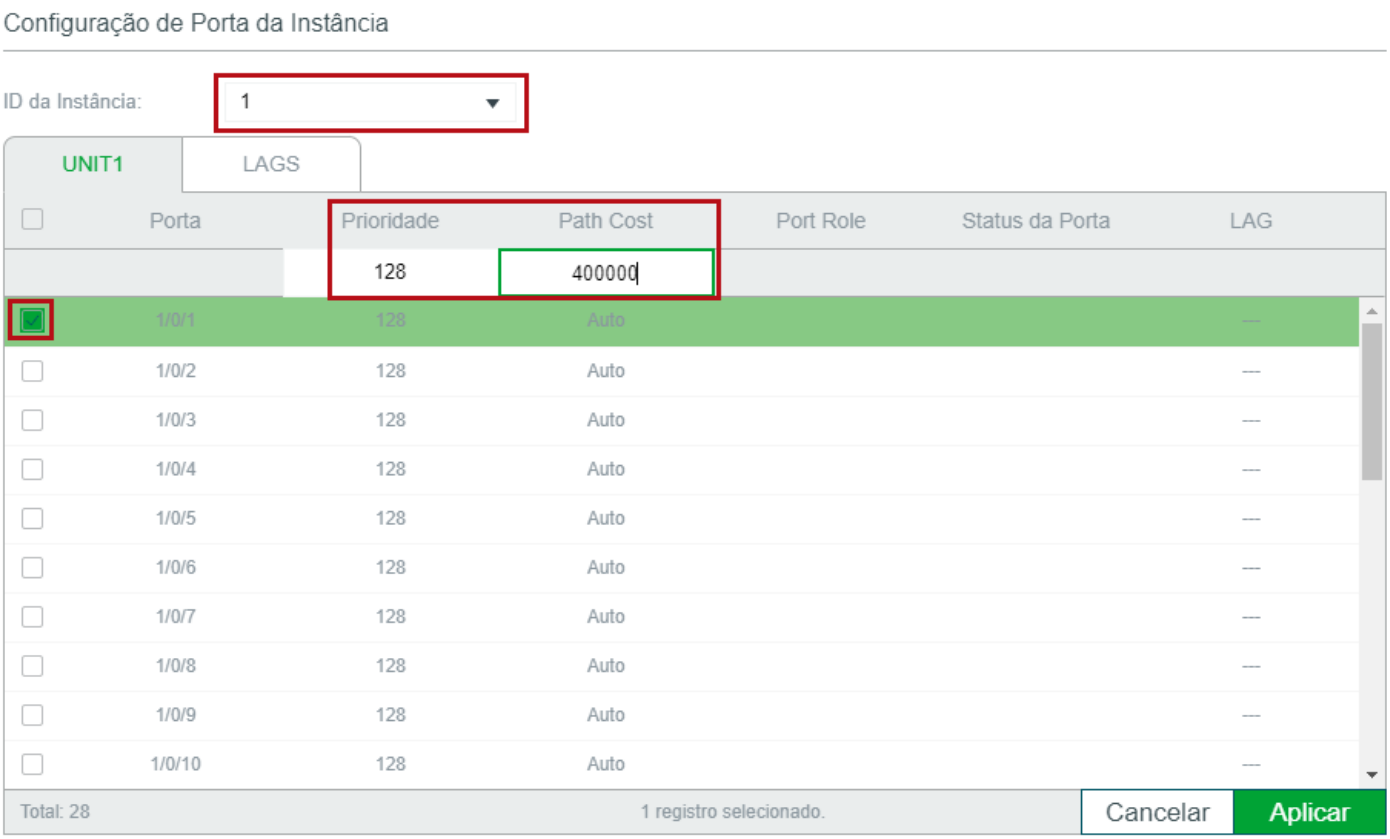


2. Vá até o menu **FUNÇÕES L2 > Spanning Tree > Instância MSTP > Configuração de Região** para carregar a página a seguir. Defina o nome da região como 1 e o nível de revisão como 100. Clique em **Aplicar**.

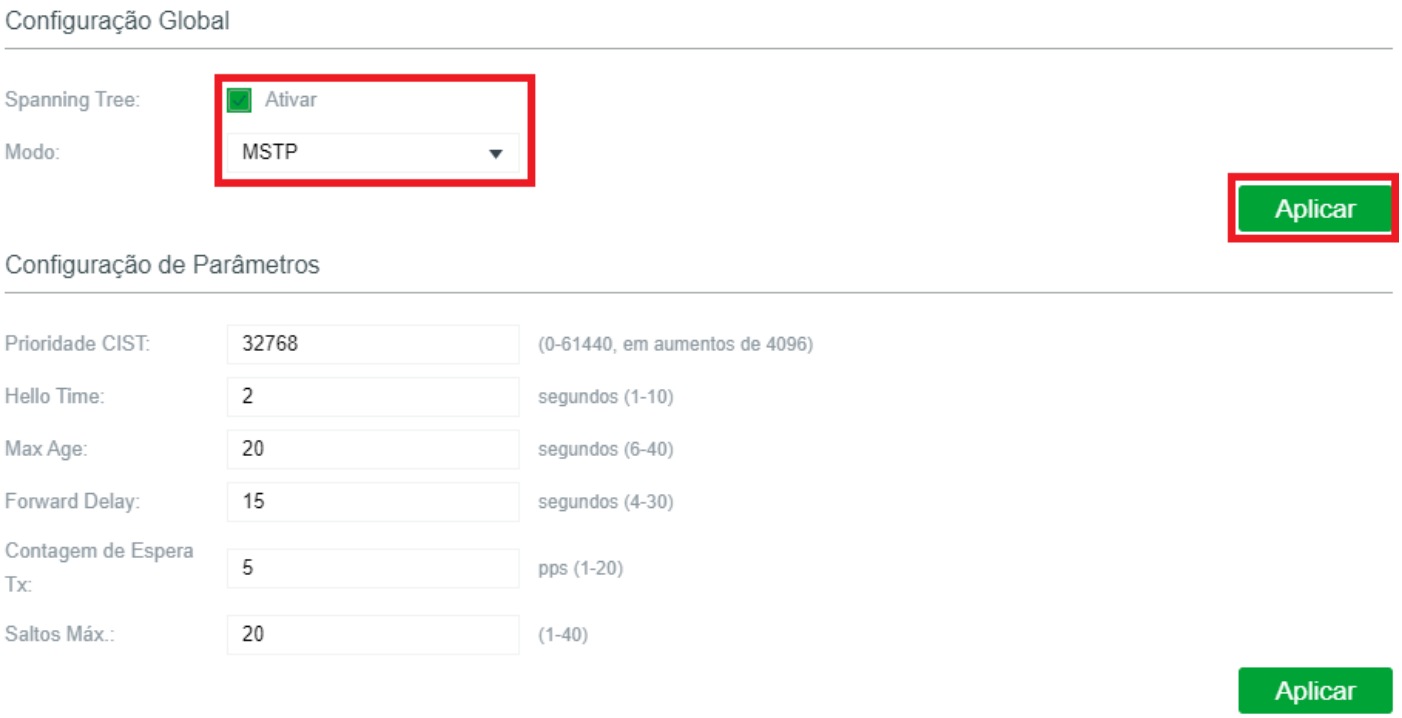
3. Vá até o menu **FUNÇÕES L2 > Spanning Tree > Instância MSTP > Configuração de Instância**. Clique em Adicionar e mapeie VLAN101-VLAN103 para a instância 1 e defina a prioridade como 32768; mapeie VLAN104-VLAN106 para a instância 2 e defina a prioridade como 32768. Clique em **Criar**.



4. Vá até o menu **FUNÇÕES L2 > Spanning Tree > Instância MSTP > Configuração de Porta da Instância** para carregar a página a seguir. Defina o custo do caminho da porta 1/0/1 na instância 1 como 400000. Clique em **Aplicar**.



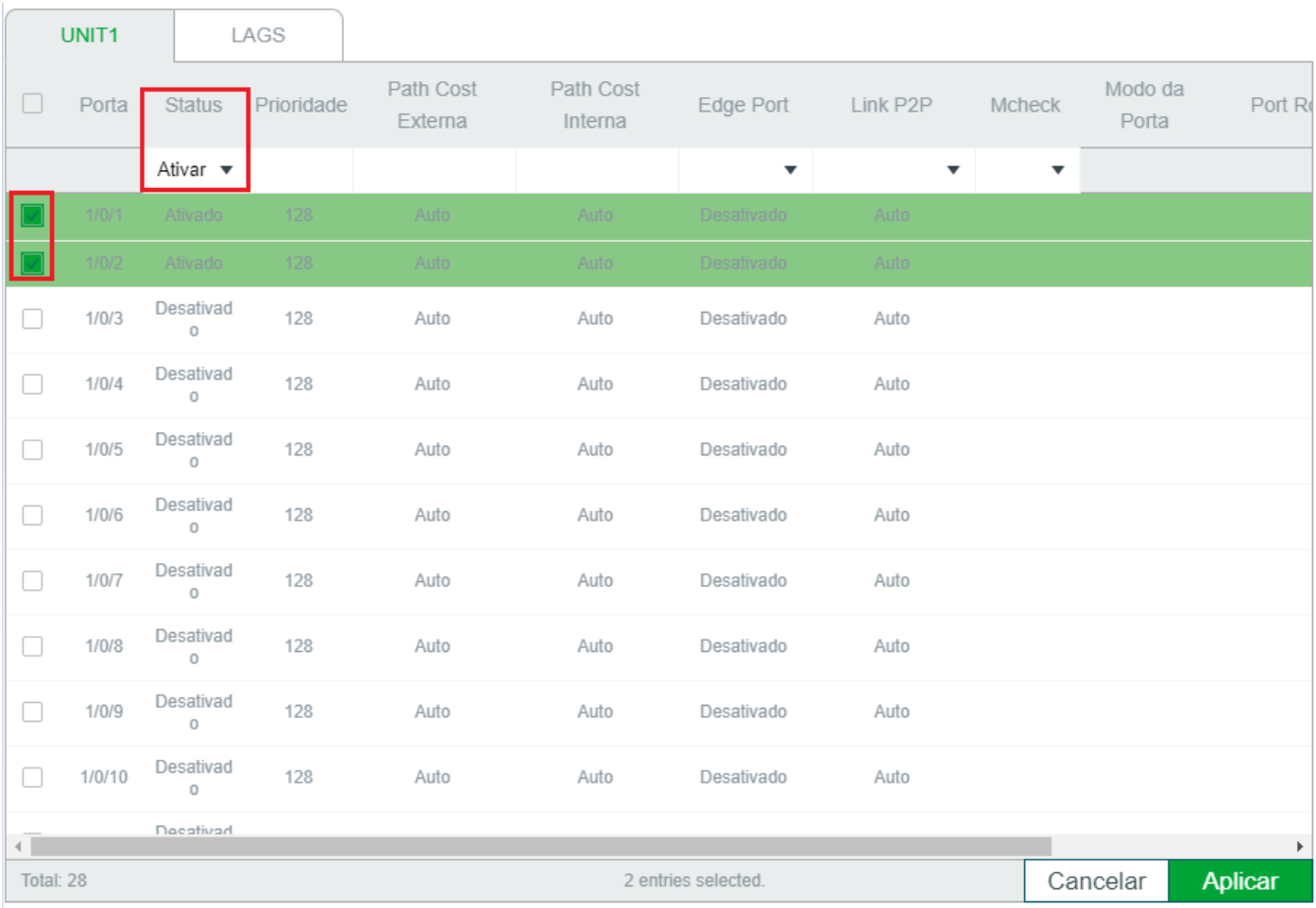
5. Vá até o menu **FUNÇÕES L2 > Spanning Tree > Configuração STP > Configuração STP** Habilite a função MSTP globalmente. Aqui deixamos os valores dos outros parâmetros globais como configurações padrão. Clique em **Aplicar**.



6. Clique Salvar para salvar as configurações.

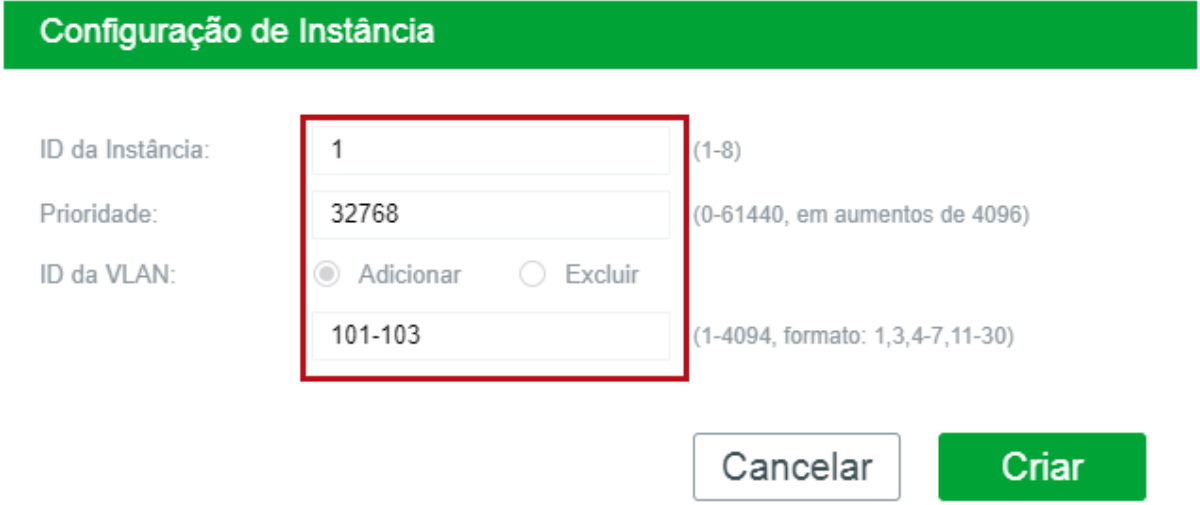
Configurações para o switch B

1. Vá ao menu **FUNÇÕES L2 > Spanning Tree > Configuração da Porta** para carregar a seguinte página. Habilite a função do STP na porta 1/0/1 e na porta 1/0/2. Aqui deixe os valores dos outros parâmetros como padrão. Clique em **Aplicar**.

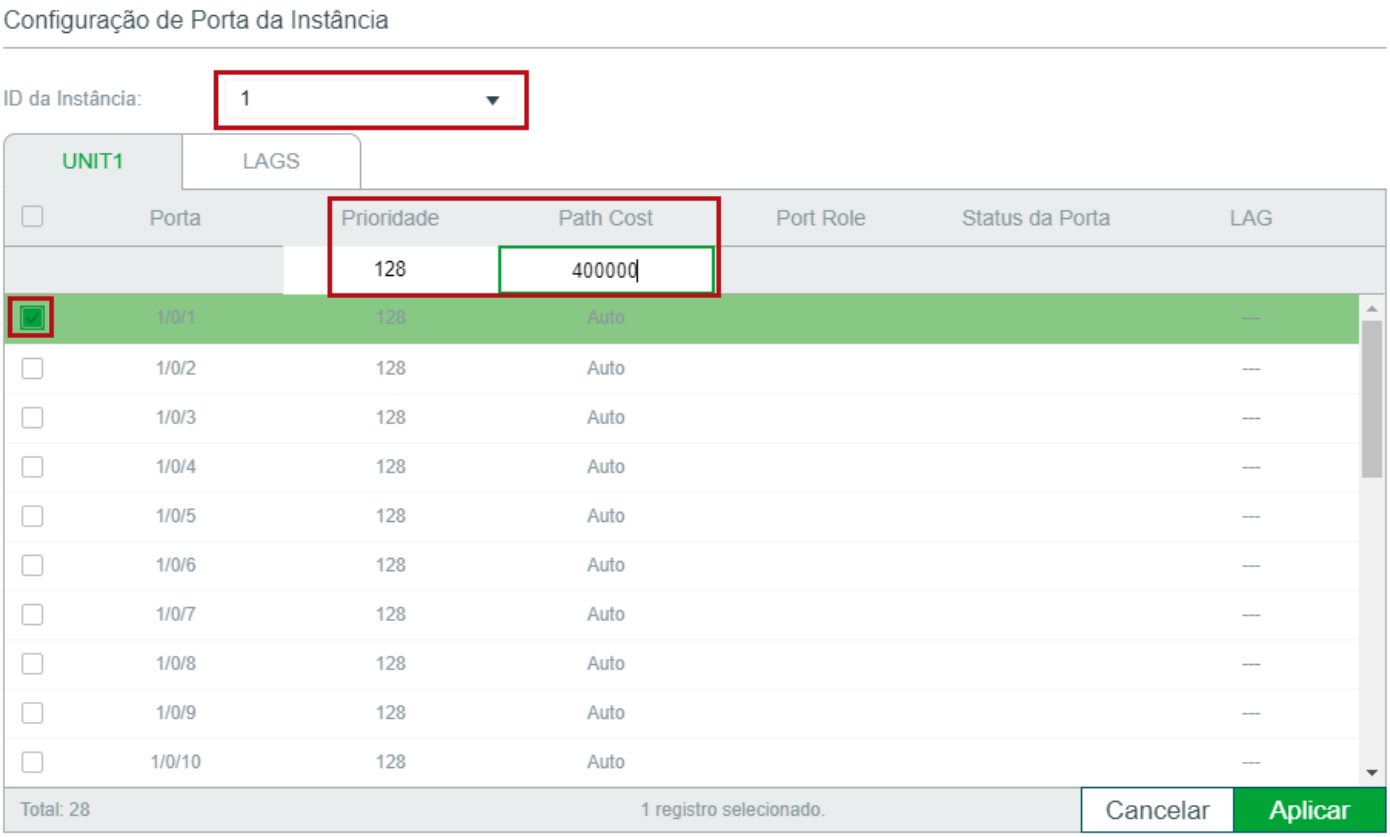


2. Vá até o menu **FUNÇÕES L2 > Spanning Tree > Instância MSTP > Configuração de Região** para carregar a página a seguir. Defina o nome da região como 1 e o nível de revisão como 100. Clique em **Aplicar**.

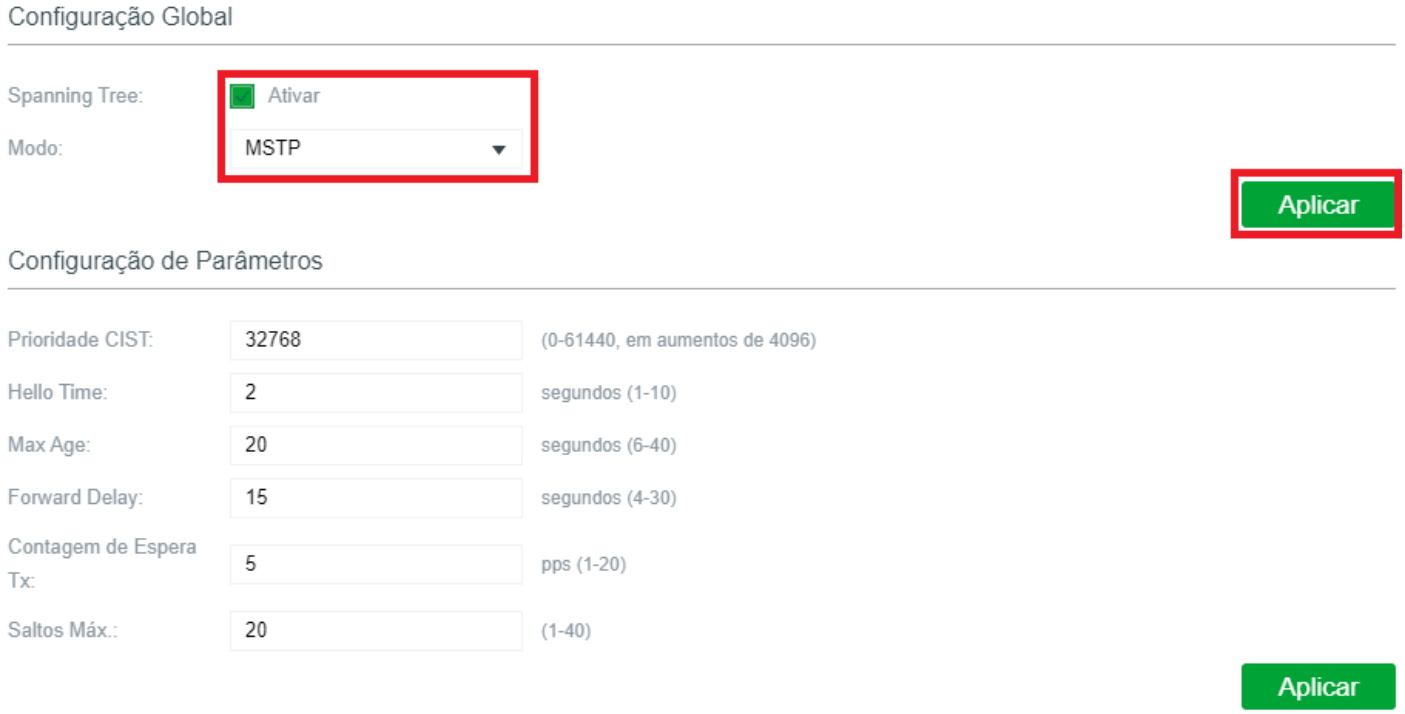
3. Vá até o menu **FUNÇÕES L2 > Spanning Tree > Instância MSTP > Configuração de Instância**. Clique em Adicionar e mapeie VLAN101-VLAN103 para a instância 1 e defina a prioridade como 0; mapeie VLAN104-VLAN106 para a instância 2 e defina a prioridade como 32768. Clique em **Criar**.



4. Vá até o menu **FUNÇÕES L2 > Spanning Tree > Instância MSTP > Configuração de Porta da Instância** para carregar a página a seguir. Defina o custo do caminho da porta 1/0/1 na instância 1 como 400000. Clique em **Aplicar**.



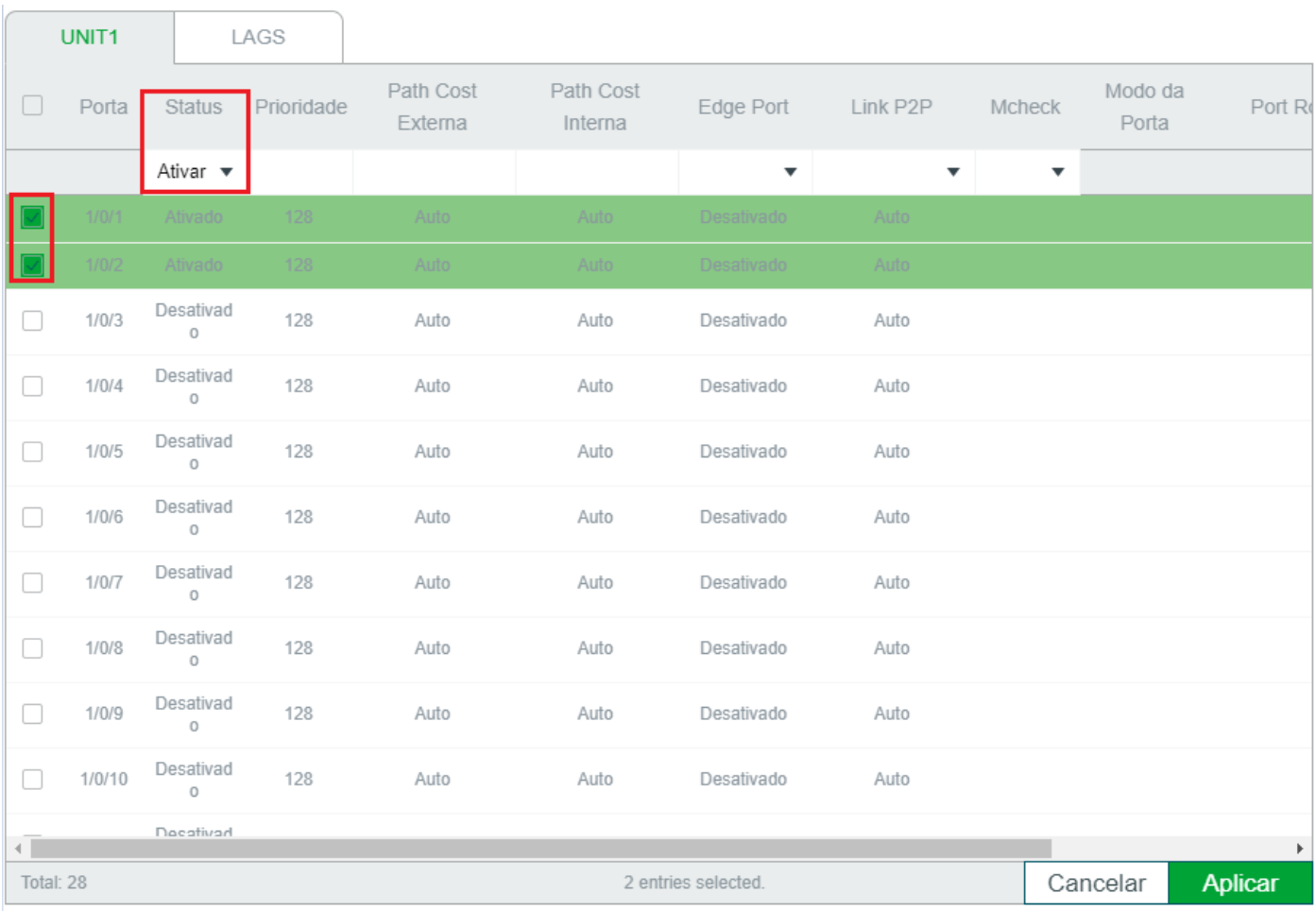
5. Vá até o menu **FUNÇÕES L2 > Spanning Tree > Configuração STP > Configuração STP** Habilite a função MSTP globalmente. Aqui deixamos os valores dos outros parâmetros globais como configurações padrão. Clique em **Aplicar**.



6. Clique Salvar para salvar as configurações.

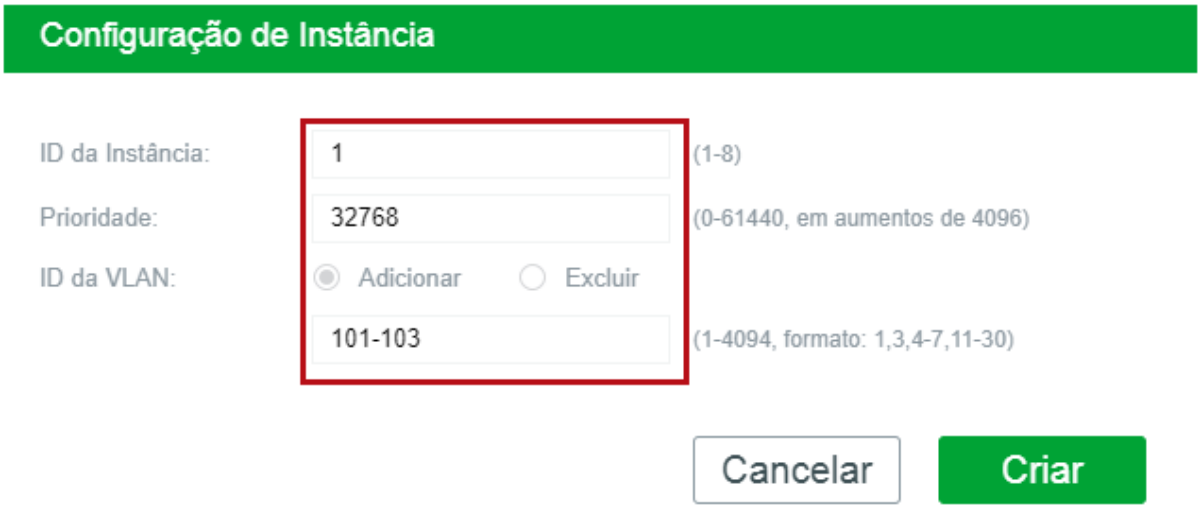
Configurações para o switch C

1. Vá ao menu **FUNÇÕES L2 > Spanning Tree > Configuração da Porta** para carregar a seguinte página. Habilite a função do STP na porta 1/0/1 e na porta 1/0/2. Aqui deixe os valores dos outros parâmetros como padrão. Clique em **Aplicar**.

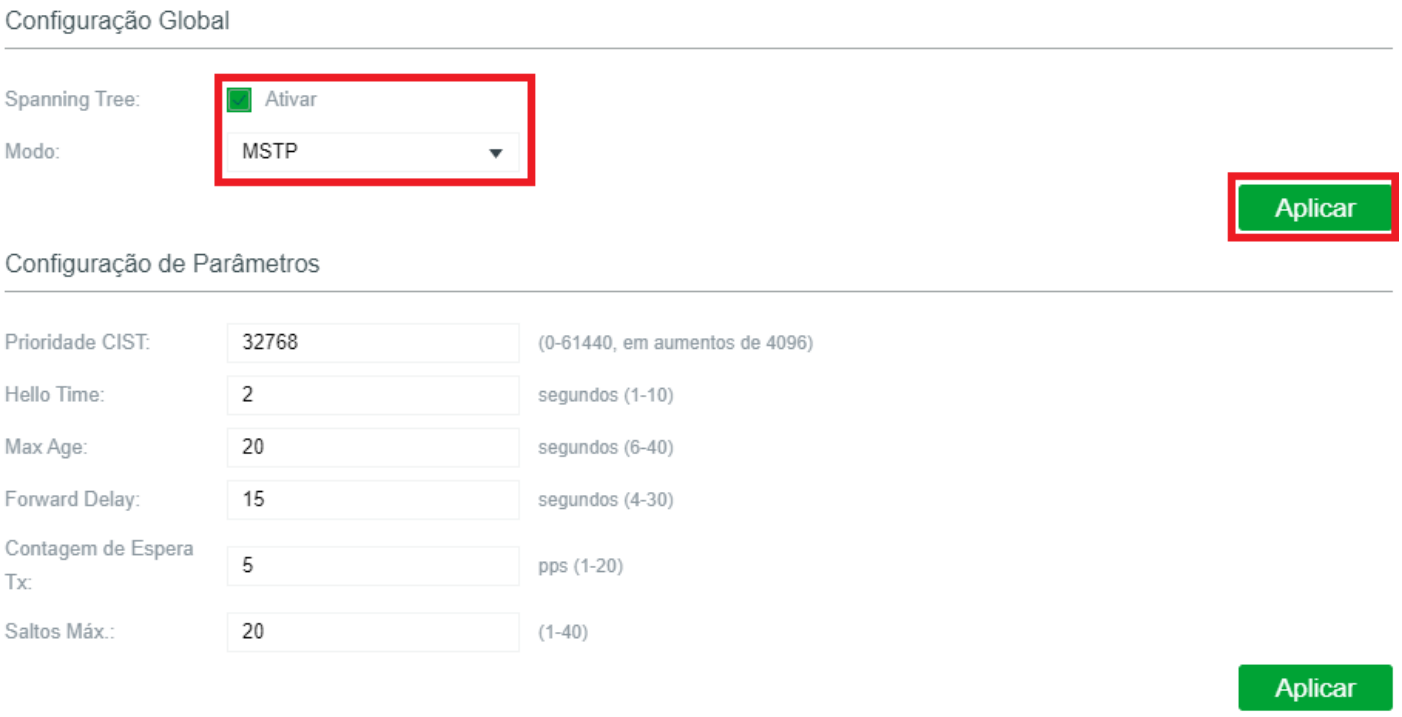


2. Vá até o menu **FUNÇÕES L2 > Spanning Tree > Instância MSTP > Configuração de Região** para carregar a página a seguir. Defina o nome da região como 1 e o nível de revisão como 100. Clique em **Aplicar**.

3. Vá até o menu **FUNÇÕES L2 > Spanning Tree > Instância MSTP > Configuração de Instância**. Clique em Adicionar e mapeie VLAN101-VLAN103 para a instância 1 e defina a prioridade como 32768; mapeie VLAN104-VLAN106 para a instância 2 e defina a prioridade como 0. Clique em **Criar**.



4. Vá até o menu **FUNÇÕES L2 > Spanning Tree > Configuração STP > Configuração STP** Habilite a função MSTP globalmente. Aqui deixamos os valores dos outros parâmetros globais como configurações padrão. Clique em **Aplicar**.



5. Clique Salvar para salvar as configurações.

Apêndice: Configuração Padrão

As configurações padrão do recurso Spanning Tree estão listadas na tabela a seguir.

Configurações padrão dos parâmetros globais

Parâmetros	Configurações Padrão
Spanning Tree	Desativado
Modo	STP
Prioridade CIST	32768
Hello Time	2 segundos
Max Age	20 segundos
Forward Delay	15 segundos
Contador TX Hold	5pps
Saltos Máx	20 saltos

Configurações padrão dos parâmetros de Porta

Parâmetros	Configurações Padrão
Status	Desativado
Prioridade	128
Ext-Path Cost	Auto
In-Path Cost	Auto
Edge Port	Desativado
P2P Link	Auto
MCheck	--

Configurações padrão da Instância MSTP

Parâmetros	Configurações Padrão
Status	Desativado
Nível de Revisão	0
Prioridade	32768
Prioridade de Porta	128
Path Cost	Auto

Configurações padrão segurança STP

Parâmetros	Configurações Padrão
Loop Protect	Desativado
Root Protect	Desativado
TC Guard	Desativado
BPDU Protect	Desativado
BPDU Filter	Desativado
BPDU Forward	Ativado

LLDP

LLDP

Visão Geral

O LLDP (Link Layer Discovery Protocol) é um protocolo de descoberta de vizinhos que é usado em dispositivos de rede para anunciar as suas próprias informações e informações a outros dispositivos na rede. Este protocolo é um 802.1AB norma IEEE definido protocolo e é executado através da camada 2 (camada de enlace de dados), que permite a interoperabilidade entre os dispositivos de rede de diferentes fornecedores.

Com o LLDP habilitado, o switch pode obter informações de seus vizinhos, e os administradores de rede podem usar os NMS (Network Management System) para reunir essas informações, ajudando-os a conhecer a topologia da rede, examinar a conectividade de rede, e solucionar as falhas da rede.

LLDP-MED (LLDP for Media Endpoint Discovery) é uma extensão do LLDP e é usado para fazer propagação de informações entre dispositivos de rede e endpoints de mídia. É especialmente utilizado em conjunto com Auto VoIP (Voice over Internet Protocol) para permitir o dispositivo VoIP para acessar a rede. Dispositivos VoIP pode usar LLDP-MED para autoconfiguração para minimizar o esforço de configuração.

Recursos Compatíveis

O switch suporta o LLDP e o LLDP-MED.

O LLDP permite que o dispositivo local possa encapsular o endereço gerenciamento, ID do dispositivo, ID de interface e outras informações em um LLDPDU (Link Layer Descoberta Protocol Data Unit) e anunciar periodicamente esta LLDPDU aos seus dispositivos vizinhos. Os vizinhos podem armazenar o LLDPDU recebido em um padrão MIB (Management Information Base), tornando possível para a informação ser acessado por um NMS (Network Management System) usando um protocolo de gerenciamento, como o SNMP (Simple Network Management Protocol).

LLDP-MED permite que o dispositivo de rede possa enviar suas informações, incluindo informações Auto VoIP, PoE capacidade (Power over Ethernet) e muito mais para os dispositivos endpoint mídia (por exemplo, telefones IP) para autoconfiguração. Os dispositivos endpoint media podem receber as informações Auto VoIP e terminar a autoconfiguração.

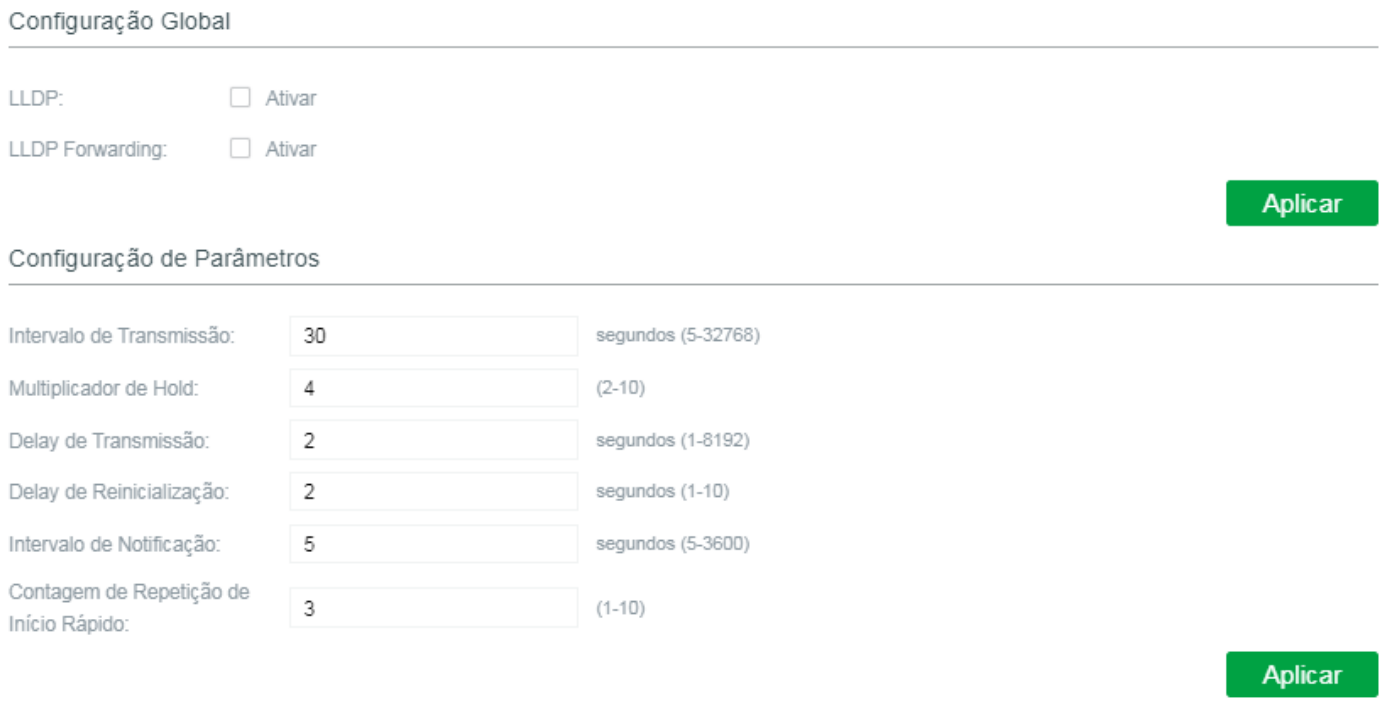
Configuração LLDP

Para configurar o LLDP, siga os passos:

1. Configurar o recurso LLDP globalmente.
2. Configurar o recurso LLDP para a porta.

Configurando o LLDP Globalmente

Escolha o **FUNÇÕES L2 > LLDP > Configuração LLDP > Configuração global** para carregar a página a seguir.



Siga estes passos para configurar o recurso de LLDP globalmente.

1. Na seção **Configuração Global**, permita o LLDP. Você também pode ativar o interruptor de transmitir mensagens LLDP quando a função LLDP está desativada. Clique em **Aplicar**.

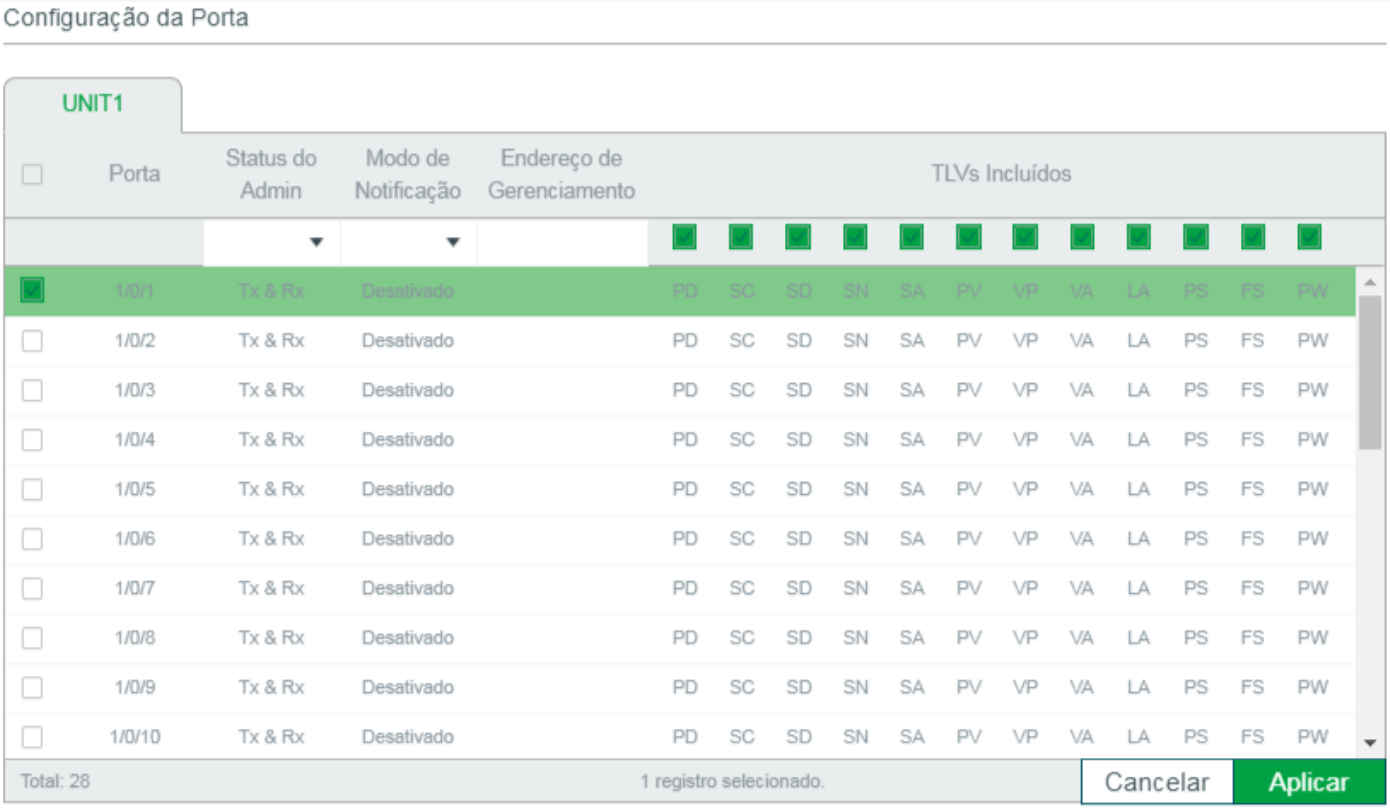
LLDP	Habilitar a função LLDP globalmente.
LLDP Forwarding	(Opcional) Habilite o switch para encaminhar mensagens LLDP para a frente quando a função LLDP é desativado.

2. Na seção **Configuração de parâmetros**, configure os parâmetros LLDP. Clique em **Aplicar**.

Intervalo de Transmissão	Digite o intervalo entre os pacotes LLDP sucessivos que são periodicamente enviados a partir do dispositivo local para os seus vizinhos. O padrão é de 30 segundos.
Multiplicador de Hold	Este parâmetro é um multiplicador no Intervalo de Transmissão que determina o valor real TTL (Time To Live) usado em um pacote LLDP. O TTL é a duração que o dispositivo vizinho deve segurar o pacote LLDP recebido antes de descartá-lo. O valor padrão é 4. TTL = Multiplicador de Hold * Intervalo de Transmissão.
Delay de Transmissão	Especifique a quantidade de Delay a partir de quando Admin Status de portas torna-se “Desativado” até que a reinicialização será tentada. O valor padrão é 2 segundos.
Delay de Reinicialização	Especifique a quantidade de atraso a partir de quando Admin Status de portas torna-se “Desativado' até que a tentativa de reinicialização ser feita. O valor padrão é 2 segundos.
Intervalo de Notificação	Digite o intervalo entre sucessivas em mensagens Trap que são periodicamente enviadas do dispositivo local para o NMS. O valor padrão é 5.
Contagem de Repetição de Início Rápido	Especifique o número de pacotes LLDP que o porto local envia quando suas mudanças de status de administrador de Disable (ou Rx_Only) a Tx e RX (ou Tx_Only). O valor padrão é 3. Neste caso, o dispositivo local vai encurtar o intervalo de transmissão de pacotes de LLDP a 1 segundo para torná-lo rapidamente descoberto por seus vizinhos. Após o número especificado de pacotes LLDP são enviados, o Intervalo de transmissão irá ser restaurada para o valor especificado.

Configurando o LLDP para a porta

Escolha no menu de **FUNÇÕES L2 > LLDP > Configuração de LLDP > Configuração de Porta** para carregar a página a seguir.



Siga estes passos para configurar o recurso de LLDP para a interface.

1. Selecione uma ou mais portas para configurar.
2. Configurar o Status do Admin e o Modo de Notificação para a porta.

Status do Admin	Conjunto de administração de status para a porta para lidar com pacotes LLDP. **Tx e Rx:** A porta transmite pacotes LLDP e recebe pacotes LLDP. **Rx_Only:** A porta só recebe pacotes LLDP. **Tx_Only:** A porta só transmite pacotes LLDP. **Desativado:** A porta não transmitirá pacotes LLDP ou descartar os pacotes LLDP recebidos.
Modo de Notificação	(Opcional) Habilite o switch para enviar mensagens de Trap aos NMS quando as informações do dispositivo vizinho ligado a estas mudanças de portas.
Endereço de Gerenciamento	Especifique o endereço IP de Gerenciamento da porta para o vizinho ser notificado. Valor 0.0.0.0 significa que a porta irá informar seu endereço de gerenciamento padrão para o vizinho.

3. Selecione os TLVs (Type / Comprimento / Valor) incluídos nos pacotes LLDP de acordo com suas necessidades.

TLVs incluídos	Configurar os TLVs incluídos nos pacotes LLDP saída. O switch suporta os seguintes TLVs: **PD:** Usado para anunciar a descrição porta definida pela estação LAN IEEE 802. SC: Usado para anunciar as funções suportadas e se estão ou não habilitadas. **SD:** Usado para anunciar a descrição do sistema, incluindo o nome completo e a identificação versão do tipo de hardware do sistema, sistema operacional de software e software de rede. **SN:** Usado para anunciar o nome do sistema. **SA:** Usado para anunciar endereço de gerenciamento do dispositivo local para tornar possível a ser gerida por SNMP. **PV:** Usado para anunciar o ID 802.1Q VLAN da porta. **VP:** Usado para anunciar o ID do protocolo VLAN da porta. **VA:** Usado para anunciar o nome da VLAN que a porta está IN. **LA:** Usado para anunciar se o link é capaz de ser agregado, se o link está atualmente em uma agregação, e o ID da porta quando ele está em uma agregação. **PS:** Usado para anunciar os atributos das portas, incluindo duplex e capacidade de taxa de bits do nó IEEE 802.3 LAN envio que está conectado ao meio físico, as configurações duplex e taxa de bits atuais do nó LAN envio IEEE 802.3 e se essas configurações são o resultado de auto negociação durante a ligação iniciação ou de ação conjunto de acionamento manual. **FS:** Usado para anunciar a capacidade máxima de tamanho de quadro do MAC implementado e PHY. **PW:** Usado para anunciar PoE da porta (Power over Ethernet) com capacidades de suportá-lo.

4. Clique em **Aplicar**.

Configurações LLDP-MED

Para configurar a função MED-LLDP, siga esses passos:

1. Ative o recurso LLDP globalmente e configure os parâmetros LLDP para as portas.
2. Configurando a contagem de repetição rápida LLDP-MED globalmente.
3. Habilite e configure o recurso MED-LLDP na porta.

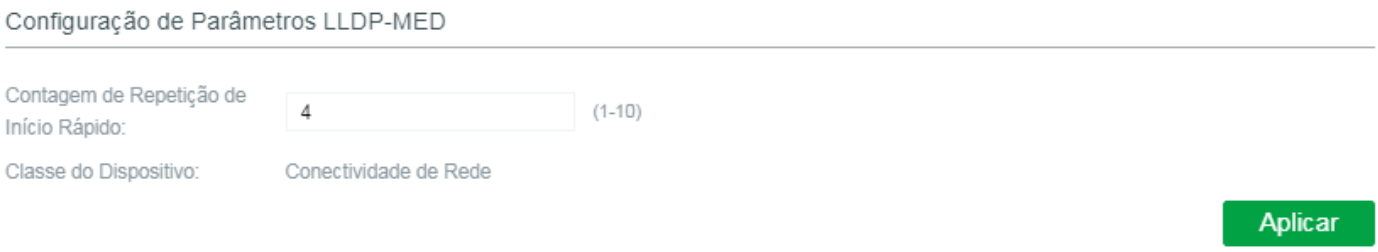
LLDP-MED é usado juntamente com Auto VoIP para implementar o acesso VoIP. Além da configuração do recurso LLDP-MED, você também precisa configurar o recurso Auto VoIP. Para obter instruções detalhadas consulte o capítulo Configurando QoS.

Configurando o LLDP Globalmente

Ativar LLDP globalmente e configurar os parâmetros LLDP para as portas. Para os detalhes da configuração LLDP, consulte Configuração LLDP.

Configurando o LLDP-MED Globalmente

Escolha o menu **FUNÇÕES L2 > LLDP > Configuração LLDP > Configuração LLDP-MED > Configuração global** para carregar a página a seguir.

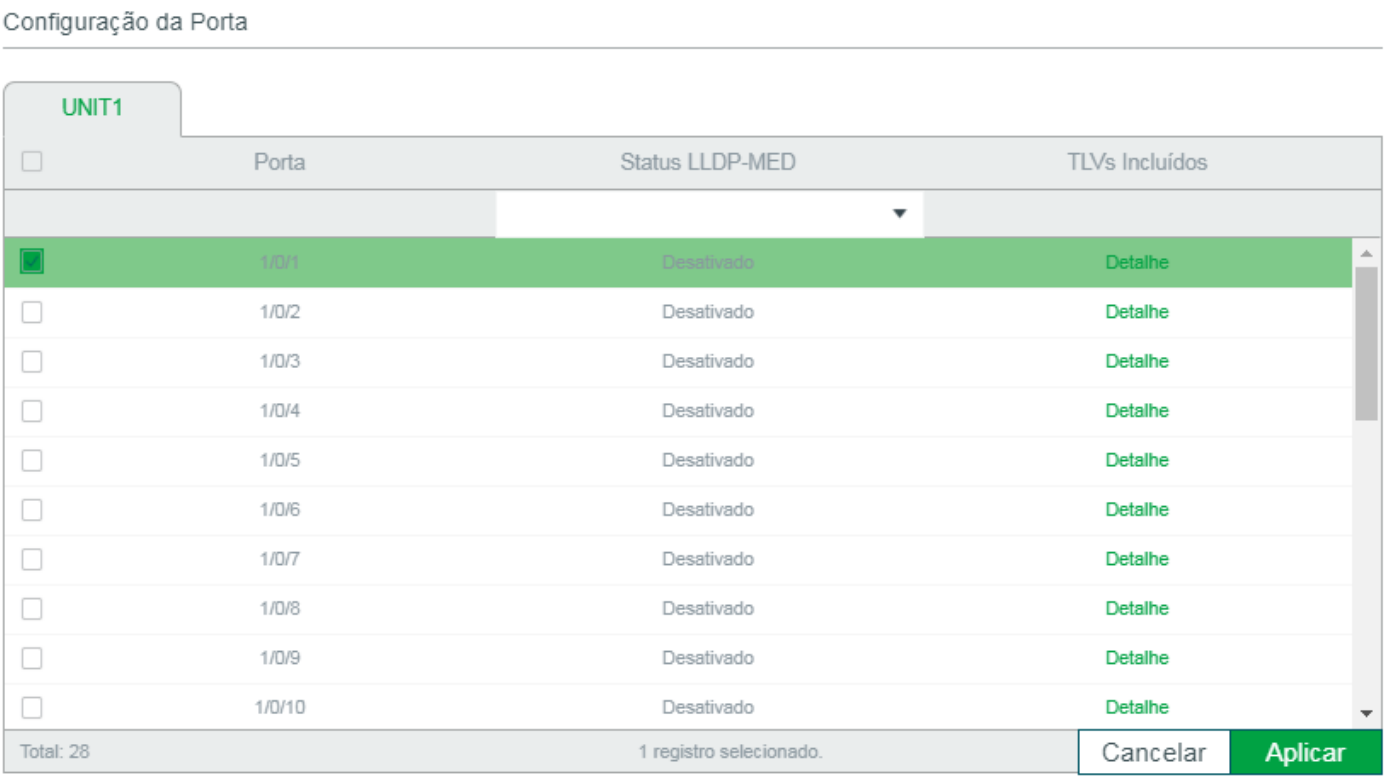


Configure a contagem de repetição de início rápido: e ver a classe de dispositivo atual. Clique em **Aplicar**.

Contagem de Repetição de Início Rápido	Especifique o número de pacotes MED-LLDP sucessivos que o switch envia quando recebe os pacotes MED-LLDP a partir dos parâmetros vizinho. O padrão é 4. Se o switch receber pacotes LLDP-MED a partir dos parâmetros do vizinho, pela primeira vez, ele irá enviar o número especificado de pacotes LLDP-MED transportando informações MED-LLDP. Depois disso, o intervalo de transmissão será restaurado para o valor especificado.
Classe do Dispositivo	Mostrar a classe de dispositivo atual. O LLDP-MED define duas classes de dispositivos, conectividade de rede do dispositivo e do dispositivo Endpoint. O switch é um dispositivo de conectividade de rede.

Configurando o LLDP-MED para as portas

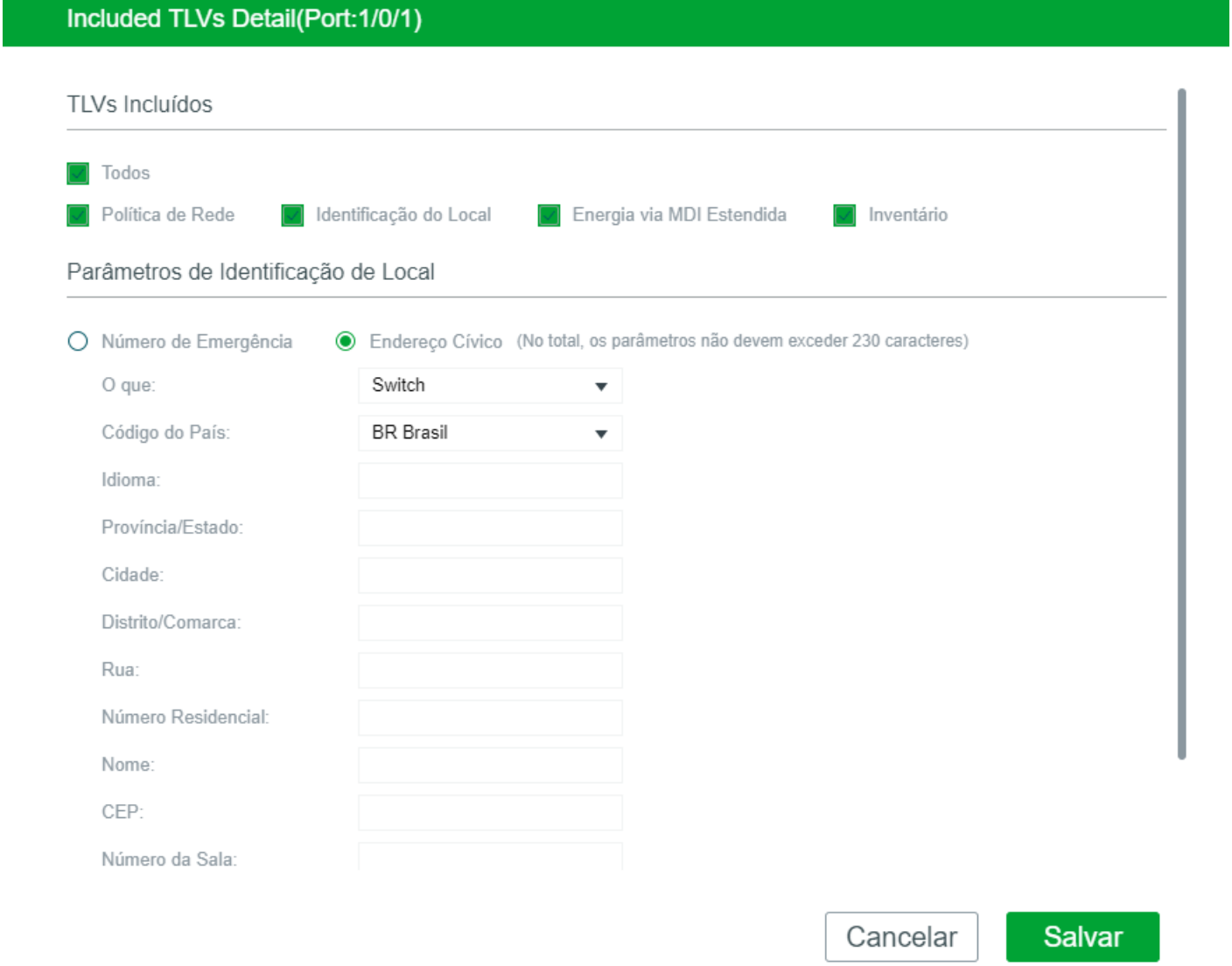
Escolha o menu **FUNÇÕES L2 > LLDP > Configuração LLDP-MED > Configuração de Porta** para carregar a página a seguir.



Siga estes passos para permitir o LLDP-MED:

1. Escolha a porta desejada e permita o LLDP-MED. Clique **Aplicar**.
2. Clique em Detalhe para entrar na página seguinte.

Configure os TLVs incluídas na saída LLDP pacotes. E se a Identificação do Local é selecionada, você precisa configurar o número de emergência ou selecione o Endereço Cívico para configurar os detalhes. Clique em **Aplicar**.



Política de Rede	Usado para anunciar a configuração da VLAN e os atributos de Camada 2 e Camada 3 associados da porta aos dispositivos finais.
Identificação do Local	Usado para atribuir o identificador informação local para os dispositivos endpoint. Se esta opção for selecionada, você pode configurar o número de emergência e o endereço detalhado do dispositivo endpoint na seção Localização Identificação Parâmetros.
Energia via MDI Estendida	Usado para anunciar a informação PoE detalhado incluindo prioridade de alimentação e status de alimentação entre os dispositivos LLDP-MED terminais e dispositivos de conectividade de rede.
Inventário	Usado para anunciar as informações de inventário. O conjunto Inventory TLV contém sete TLVs gestão de inventário básico, isto é, Hardware Revisão TLV, revisão de firmware TLV, Software Revisão TLV, número de série TLV, Fabricante Nome TLV, Modelo Nome TLV e identificação do recurso de TLV.

Número de Emergência	Configurar o número de emergência para CAMA chamada ou PSAP. O número deve conter 10-25 caracteres. Configure o endereço do dispositivo de áudio no formato de endereço IETF definido. O que: Especifique o tipo de função do dispositivo local, DHCP Server, switch ou LLDP-MED Endpoint.
Endereço Cívico	Código do país: Digite o código de país definido pela ISO 3166, por exemplo, CN, EUA. Idioma, Província /Estado etc. Digite os detalhes regulares.

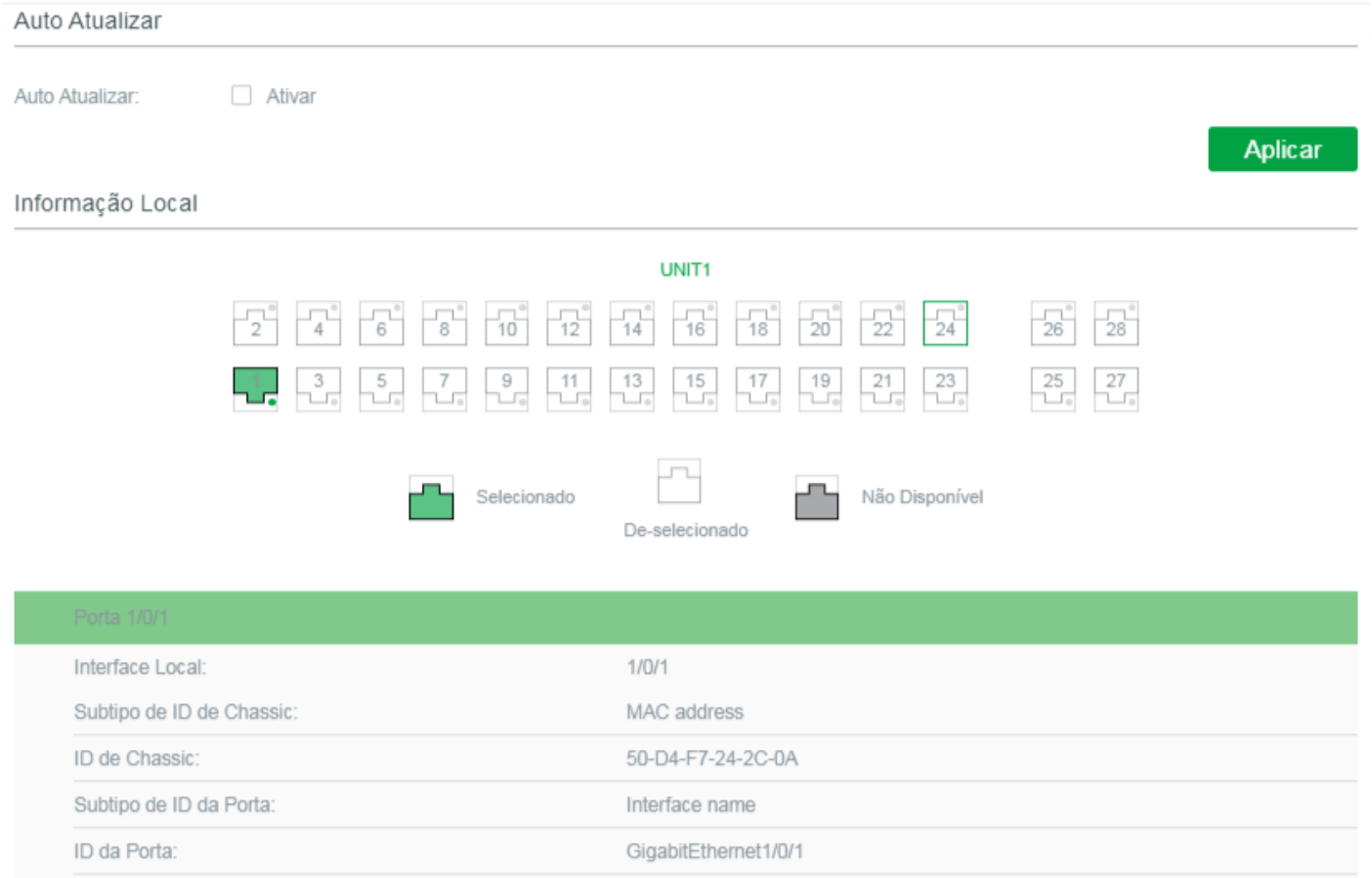
Visualizando as configurações de LLDP

Este capítulo mostra como visualizar as definições LLDP no dispositivo local.

Visualizando as informações LLDP do dispositivo

Visualizando o Informação local

Escolha o menu **FUNÇÕES L2 > LLDP > Configuração LLDP > Informação local** para carregar a página a seguir.



Siga os passos abaixo para visualizar as informações locais:

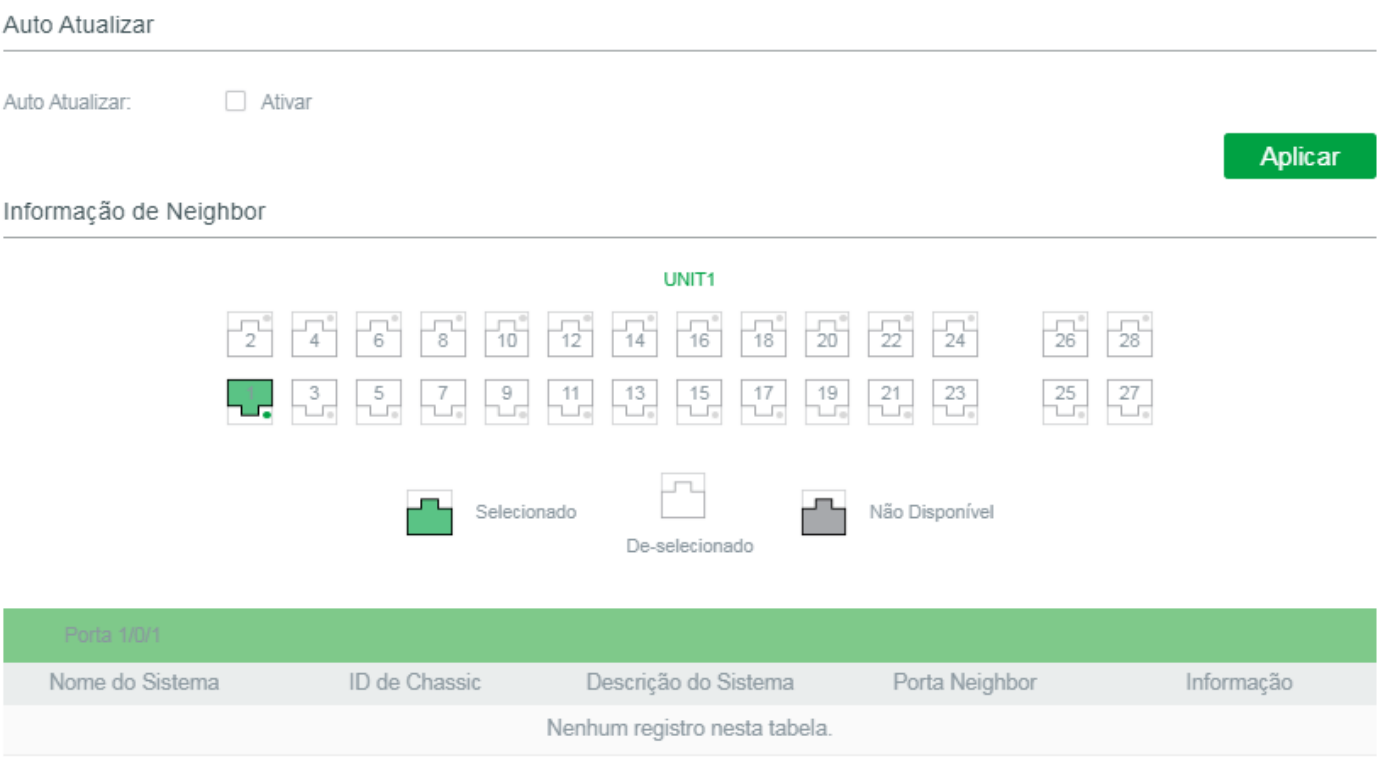
1. **Auto Atualizar**, ativar o recurso de auto atualizar e definir a taxa de atualização de acordo com suas necessidades. Clique em **Aplicar**.

2. Em **Informação local**, selecione a porta desejada para visualizar o seu dispositivo local associado em formação.

Interface local	Exibe o ID da porta local.
Subtipo de ID de Chassis	Exibe o tipo de Chassis ID.
ID de Chassis	Exibe o valor do Chassis ID.
Porto ID subtipo	Exibe o tipo de porta ID.
ID da Porta	Exibe o valor da porta ID.
TTL	Especificar a quantidade de tempo em segundos o dispositivo vizinho deve manter as informações recebidas antes de descartá-lo.
Descrição da Porta	Mostra a descrição do porto local.
Nome do Sistema	Exibe o nome do sistema do dispositivo local.
Descrição do Sistema	Exibe a descrição do sistema do dispositivo local.
Capacidades do Sistema Suportadas	Exibe as capacidades suportadas do sistema local.
Capacidades do Sistema Ativadas	Apresenta as funções primárias do dispositivo local.
Tipo de Endereço de Gerenciamento	Exibe o endereço IP de gerenciamento do dispositivo local.

Visualizando as Neighbor Info

Escolha o menu **FUNÇÕES L2 > LLDP > Configuração LLDP > Neighbor info** para carregar a página a seguir.



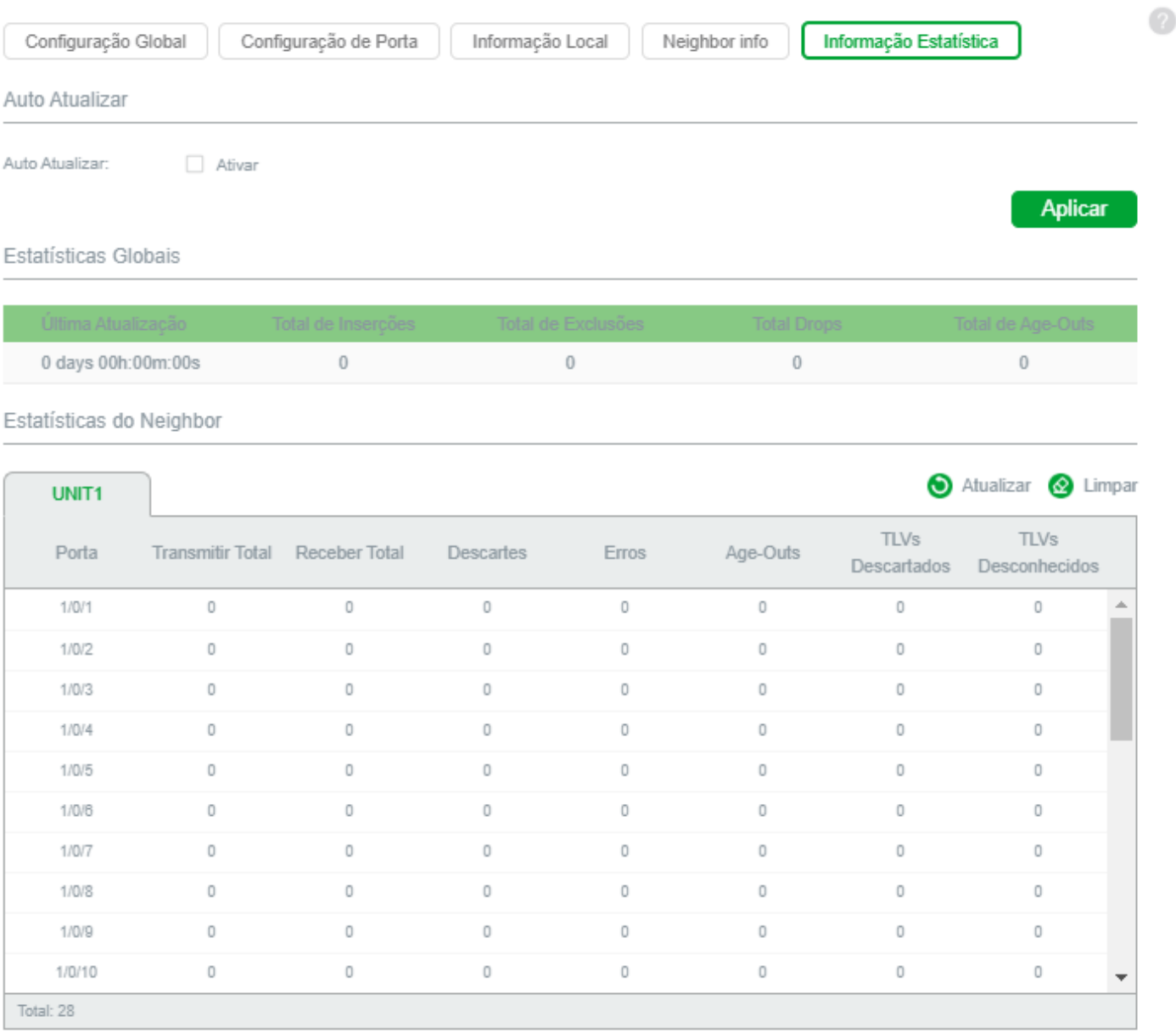
Siga estes passos para visualizar o Neighbor info:

1. Na seção **Atualização automática**, ative o recurso de Auto Atualizar e definir a taxa de atualização de acordo com suas necessidades. Clique em **Aplicar**.
2. Na secção **Neighbor info**, selecionar a porta desejada e visualizar o seu vizinho associado informação de dispositivo.

Nome do Sistema	Exibe o nome do sistema do dispositivo vizinho.
ID de Chassis	Exibe o ID do chassi do dispositivo vizinho.
Descrição do Sistema	Exibe a descrição do sistema do dispositivo vizinho.
Porta Neighbor	Exibe o ID da porta do dispositivo vizinho que é conectado à porta local.
Informação	Clique para ver os detalhes do dispositivo vizinho.

Visualizando as Estatísticas de LLDP

Escolha o menu **FUNÇÕES L2 > LLDP > Configuração LLDP > Informação Estatística** para carregar a página a seguir.



Siga os passos abaixo para visualizar estatísticas de LLDP:

1. Na seção Auto Atualizar, ative o recurso de atualização automática e defina a taxa de atualização de acordo com suas necessidades. Clique em **Aplicar**.
2. Na seção de Estatisticas Globais é possível visualizar as estatísticas globais do dispositivo local.

Última atualização	Exibe o tempo em que as estatísticas são atualizadas.
Total de inserções	Exibe o número total de vizinhos durante o tempo mais recente atualização.
Total de Exclusões	Exibe o número de vizinhos eliminados pelo dispositivo local. A porta será deletada quando a porta estiver desativada o TTL dos pacotes LLDP enviado pelo vizinho será 0.
Total Drops	Exibe o número de vizinhos recusados pelo dispositivo local. Cada porta pode aprender um máximo de 80 dispositivos vizinhos, e os vizinhos subsequentes serão descartados quando o limite for excedido.

Total de Age-Outs	Mostra os últimos números de vizinhos que envelheceram para fora no dispositivo local.

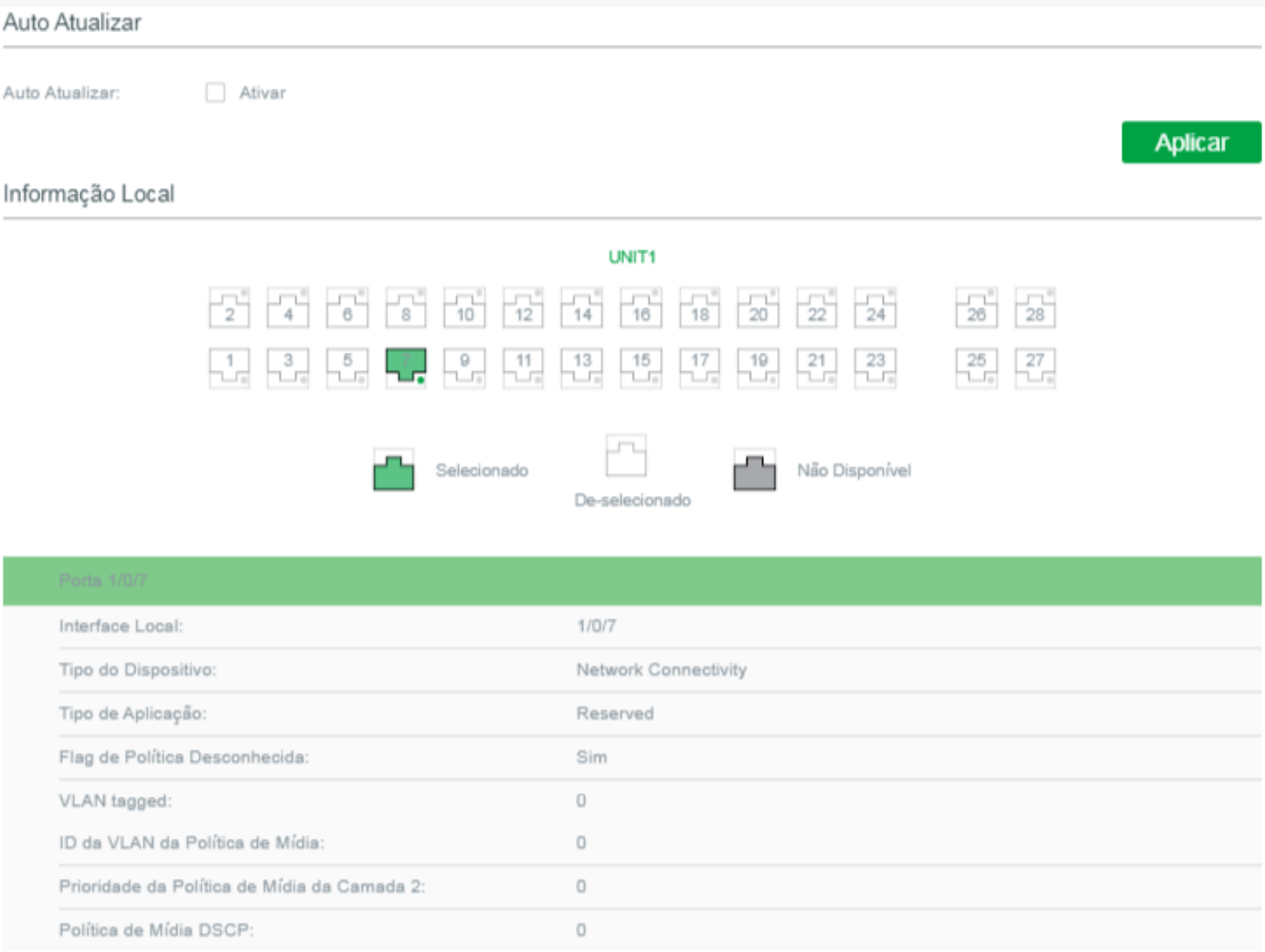
3. Na secção **Estatísticas do Neighbor**, ver as estatísticas da porta correspondente.

Transmitir total	Exibe o número total de pacotes LLDP enviados através da porta.
Receber total	Exibe o número total de pacotes recebidos LLDP através da porta.
Descartes	Exibe o número total de pacotes LLDP descartados através da porta.
Erros	Exibe o número total de pacotes LLDP com erro recebidos através da porta.
Age-Outs	Exibe o número de Neighbor conectados à porta em que ocorreu age-out.
TLVs Descartados	Exibe o número total dos TLVs descartados pela porta quando receber pacotes LLDP.
TLVs Desconhecidos	Exibe o número total dos TLVs desconhecidos incluídos nos pacotes LLDP recebidos.

Visualizando as configurações de LLDP-MED

Escolha o menu **FUNÇÕES L2 > LLDP > Configuração LLDP-MED > Informação local** para carregar a página a seguir.

Visualizando Informação local



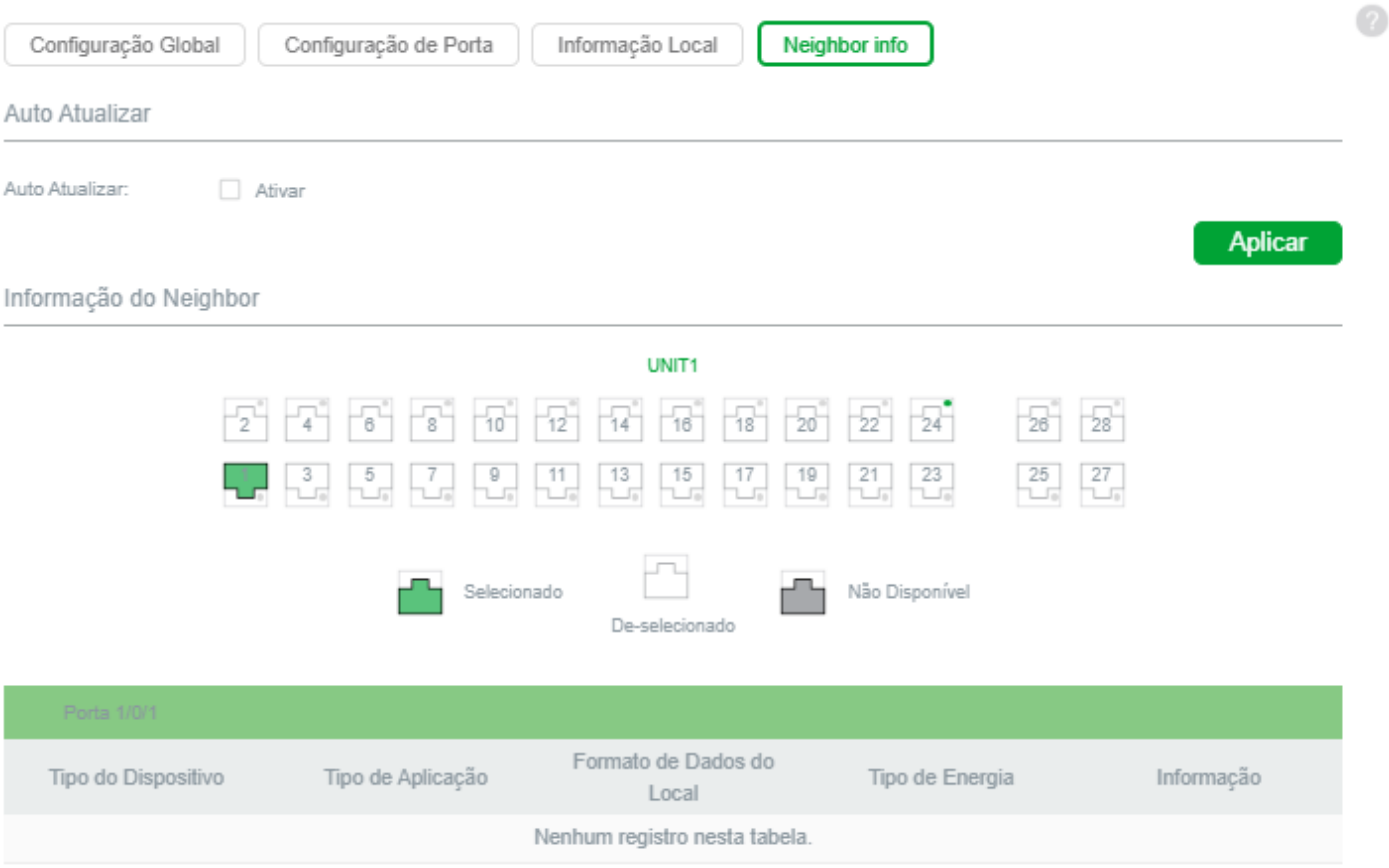
Siga os passos abaixo para visualizar as informações locais do LLDP-MED:

1. Na seção **Auto Atualizar**, ative o recurso de atualização automática e defina a taxa de atualização de acordo com suas necessidades. Clique em **Aplicar**.
2. Na seção **Informação local**, selecione a porta desejada e visualizar as configurações LLDP-MED.

Interface Local	Exibe o ID da porta local.
Tipo do Dispositivo	Exibe o tipo de dispositivo local definido pela LLDP-MED.
Tipo de Aplicação	Exibe os aplicativos suportados pelo dispositivo local.
Flag de Política Desconhecida	Exibe as configurações de localização desconhecidas incluídas na política de rede TLV.
VLAN tagged	Exibe o tipo de tag de VLAN das aplicações, marcadas ou não marcadas.
ID da VLAN da Política de Mídia	Exibe a ID 802.1Q VLAN da porta.
Prioridade da Política de Mídia da Camada 2	Exibe a prioridade de camada 2 usada na aplicação específica.
Política de Mídia DSCP	Exibe o valor DSCP usado na aplicação específica.

Visualizando o Neighbor Info

Escolha o menu **FUNÇÕES L2 > LLDP > Configuração LLDP-MED > Neighbor Info** para carregar a página a seguir.



Siga os passos abaixo para visualizar as Informações vizinho LLDP-MED:

1. Na seção **Auto Atualizar**, ative o recurso de atualização automática e defina a taxa de atualização de acordo com suas necessidades. Clique em **Aplicar**.
2. Na seção **Neighbor Info**, selecione a porta desejada e visualize as configurações MED-LLDP.

Tipo de dispositivo	Exibe o tipo de dispositivo MED-LLDP do dispositivo vizinho.
Tipo de Aplicação	Exibe o tipo de aplicação do dispositivo vizinho.
Formato de Dados do local	Exibe o tipo de localização do dispositivo vizinho.
Tipo de Energia	Exibe o tipo de alimentação do dispositivo vizinho.
Informação	Ver mais detalhes do MED-LLDP do dispositivo vizinho.

Exemplo de Configuração

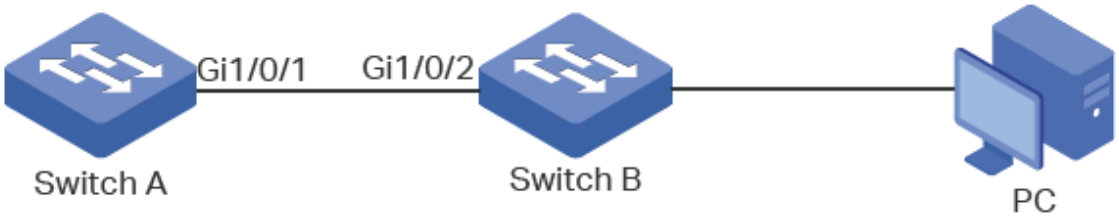
Requisitos de rede

A necessidade de o administrador de rede visualizar as informações dos dispositivos na rede da empresa para saber sobre a situação da ligação, e topologia de rede para que ele possa resolver as falhas de rede em potencial com antecedência.

Topologia da rede

Exemplificado com a seguinte situação:

Porta Gi1/0/1 no switch A é diretamente conectado à porta Gi1/0/2 do switch B. O switch B está diretamente conectado ao PC. O administrador pode visualizar as informações do dispositivo usando o NMS.



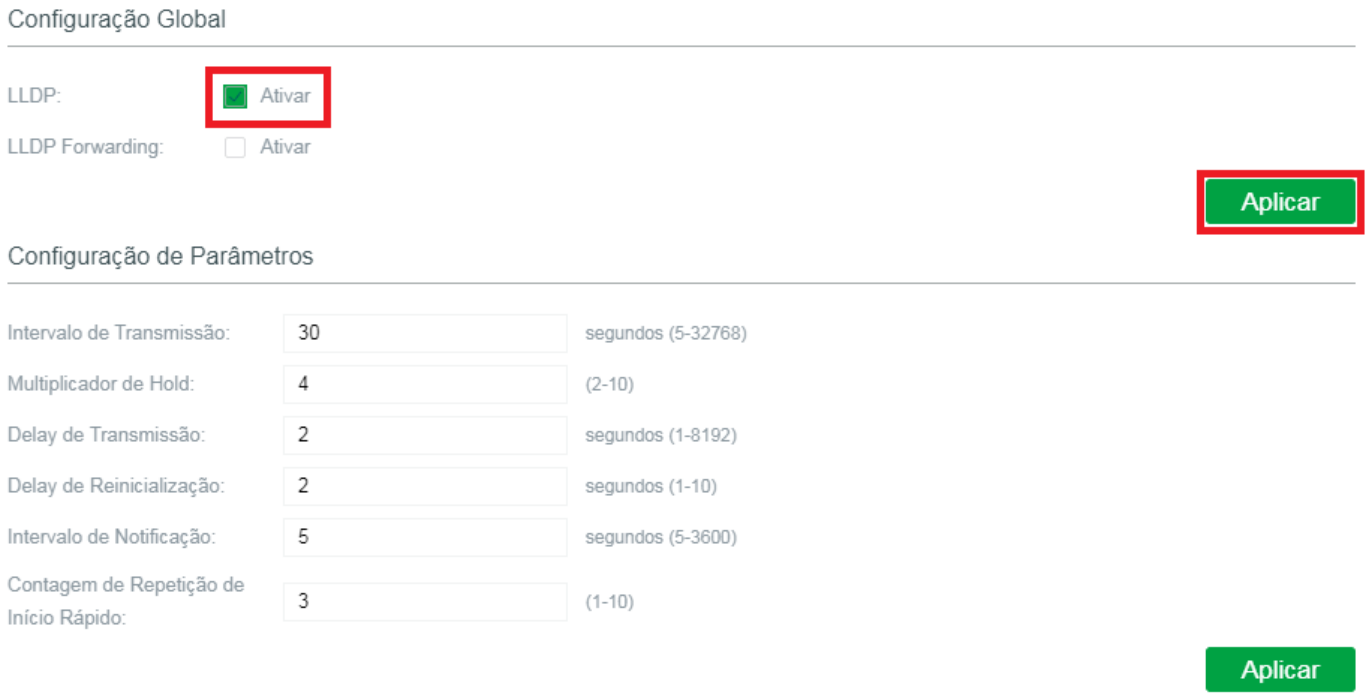
Configurando o Cenário

O LLDP pode atender os requisitos de rede. Habilite o recurso LLDP globalmente no switch A e no switch B. Configure os parâmetros LLDP relacionados nas portas correspondentes.

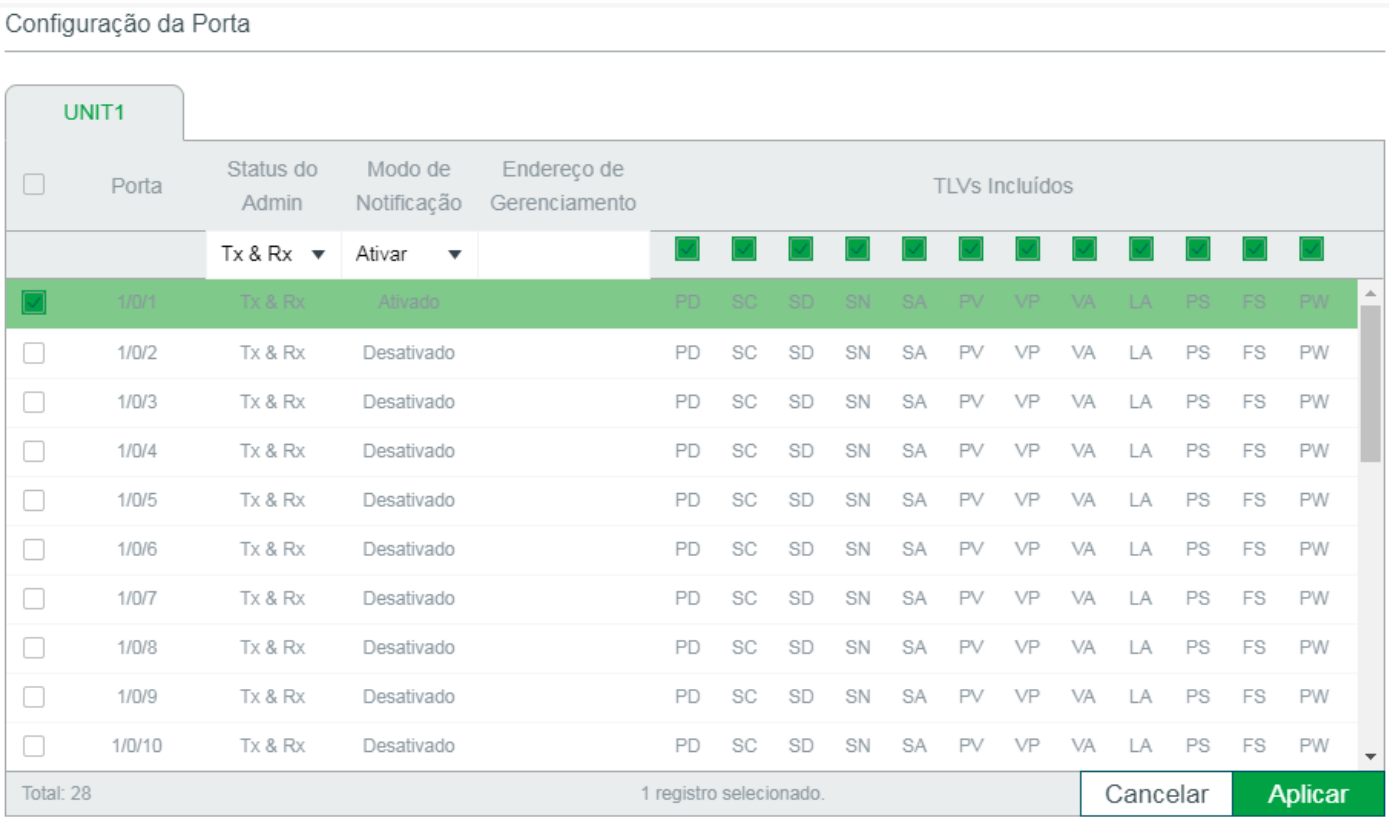
Configurando o switch A e o switch B:

As configurações dos switches A e B são semelhantes. As apresentações a seguir tomam o Switch A como exemplo. Demonstrada com o SG 2404 PoE L2+, este capítulo apresenta os procedimentos de configuração:

1. Escolha o menu **FUNÇÕES L2 > LLDP > Configuração LLDP > Configuração global** para carregar a página seguinte.
   Ative o LLDP globalmente e configurar os parâmetros relacionados. Aqui vamos dar as configurações padrão como exemplo.



2. Selecione no menu **FUNÇÕES L2 > LLDP > Configuração LLDP > Configuração de porta** para carregar a página seguinte. Defina o Status do Admin da porta Gi1/0/1 como Tx & Rx, e ative o Modo de notificação e configure todo o TLVs incluídos nos pacotes LLDP de saída.



Apêndice: Configuração Padrão

As configurações padrão de LLDP estão listados nas tabelas a seguir.

Configurações LLDP padrão

Configurações LLDP padrão

Parâmetros	Configurações Padrão
LLDP	Desativar
LLDP Forwarding:	Desativar
Intervalo de Transmissão	30 segundos
Multiplicador de Hold	4
Delay de Transmissão	2 segundos
Delay de Reinicialização	2 segundos
Intervalo de Notificação	5 segundos
Contagem de Repetição de Início Rápido	3

Configurações LLDP padrão na porta

Parâmetros	Configurações Padrão
Status do Admin	Tx & Rx
Modo de Notificação	Desativar
TLVs incluídos	Todos

Configurações LLDP-MED padrão

Configurações LLDP-MED padrão

Parâmetros	Configurações Padrão
Fast Start Conta de repetição	4
Status LLDP-MED	Desativar
TLVs incluídos	Todos

INTERFACES DE CAMADA 3

Visão Geral

As interfaces são usadas para trocar dados e interagir com interfaces de outros dispositivos de rede. As interfaces são classificadas em interfaces da camada 2 e de camada 3.

- **Interfaces da camada 2:** são as portas físicas no painel do switch. Elas encaminham pacotes com base na tabela de endereços MAC.
- **Interfaces da camada 3:** são usadas para encaminhar pacotes IPv4 e IPv6 usando protocolos de roteamento estático ou dinâmico. Você pode usar interfaces da camada 3 para roteamento IP e roteamento entre VLANs.

Este capítulo apresenta as configurações para as interfaces da camada 3. Os tipos de interfaces da camada 3 são mostrados abaixo:

Tipo	Descrição
Interface VLAN	Uma interface de camada 3 com a qual atua como o gateway padrão de todos os hosts na VLAN correspondente.
Interface Loopback	Uma interface com o status sempre ativo.
Porta Roteada	Uma porta física configurada como uma porta da Camada 3.
Interface Porta-canal	Várias portas roteadas são ligadas e configuradas como uma interface de Camada 3.

Configuração de Interface Camada 3

Para efetuar a configuração da interface IPv4, siga as seguintes etapas:

1. Crie uma interface de camada 3;
2. Configure os parâmetros IPv4 da interface criada;
3. Ver informações detalhadas da interface criada.

Criando uma Interface de Camada 3

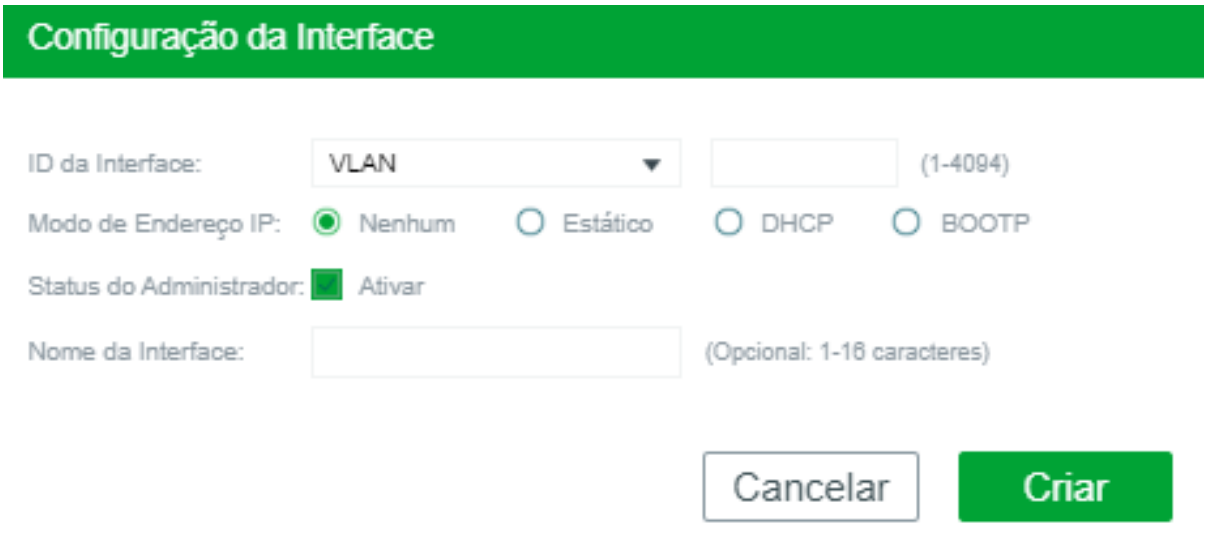
Escolha o menu **FUNÇÕES L3 > Interface VLAN** para carregar a seguinte página.

Siga os seguintes passos para criar uma interface de camada 3:

1. Na seção de **Configuração de Interface**, clique em Adicionar para carregar a seguinte página, configure os parâmetros correspondentes a interface de Camada 3. Depois clique em **Criar**.

Roteamento IPv4	Ative a função de roteamento IPv4 globalmente para todas as interfaces da camada 3. Está ativado por padrão.
Roteamento IPv6	(Opcional) Ative a função de roteamento IPv6 globalmente para todas as interfaces da camada 3. É desativado por padrão.

2. Na seção de **Configuração de Interface**, clique em para carregar a seguinte página, configure os parâmetros correspondentes a interface de Camada 3. Depois clique em **Criar**.

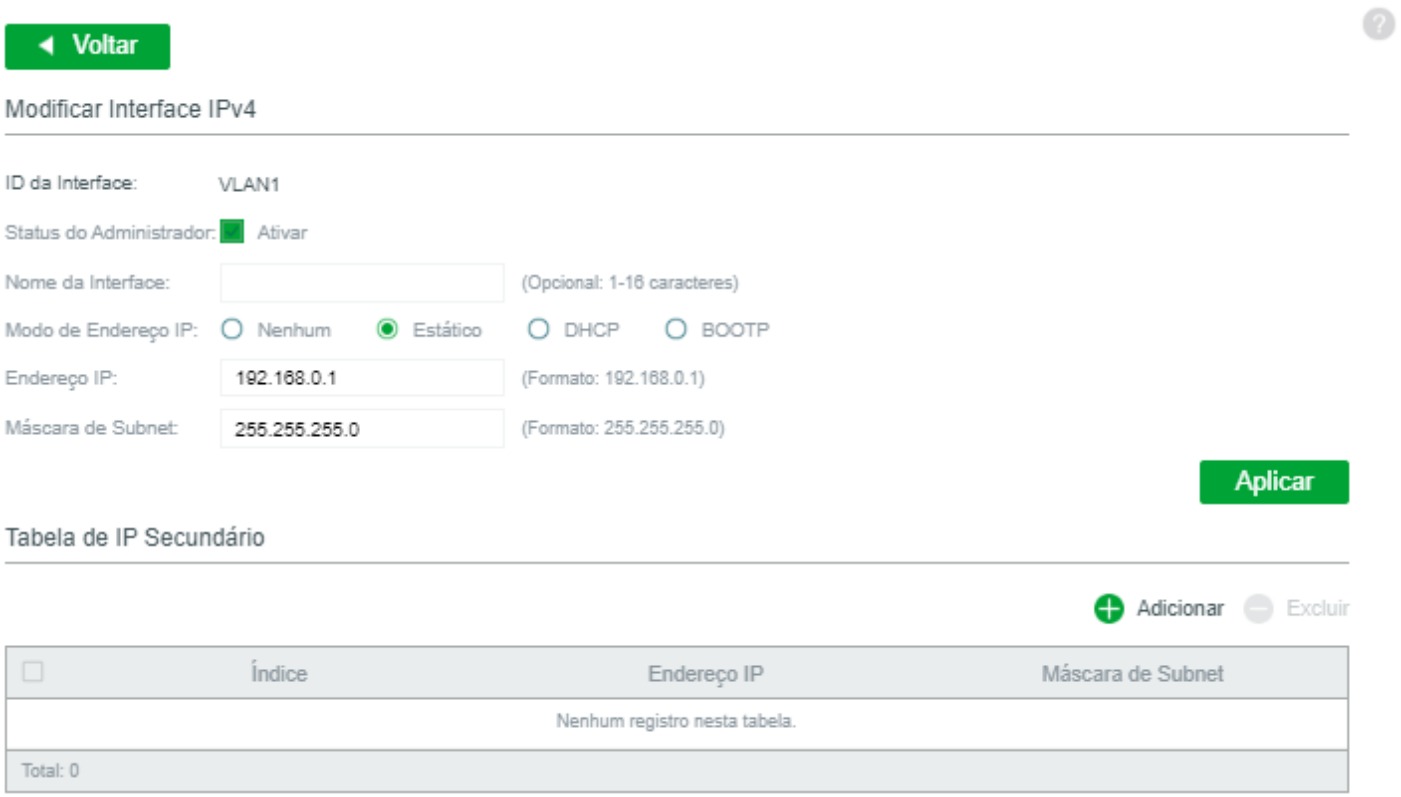


ID da interface	Selecione um tipo de interface e insira o ID da interface.
Modo de Endereço IP	Especifique o modo de atribuição de endereço IP da interface. **Nenhum:** nenhum endereço IP será atribuído à interface. **Estático:** atribua um endereço IP à interface manualmente. **DHCP:** atribua um endereço IP à interface através do servidor DHCP. **BOOTP:** atribua um endereço IP à interface através do servidor BOOTP.
DHCP Option 12	Se você selecionar DHCP como o modo de endereço IP, configure a opção 12 aqui. A opção 12 do DHCP é usada para especificar o nome do cliente.
Endereço IP	Especifique o endereço IP da interface se você escolher "Estático" como o modo de atribuição de endereço IP.
Máscara de sub-rede	Especifique a máscara de sub-rede do endereço IP da interface.
Status do Administrador	Ative ou desative os recursos da interface de camada 3.
Nome da Interface	(Opcional) Digite um nome para a interface.

A interface criada é uma interface IPv4. Para configurar os recursos do IPv6, clique em "Editar IPv6" depois que a interface for criada.

Configurando os Parâmetros IPv4 da Interface

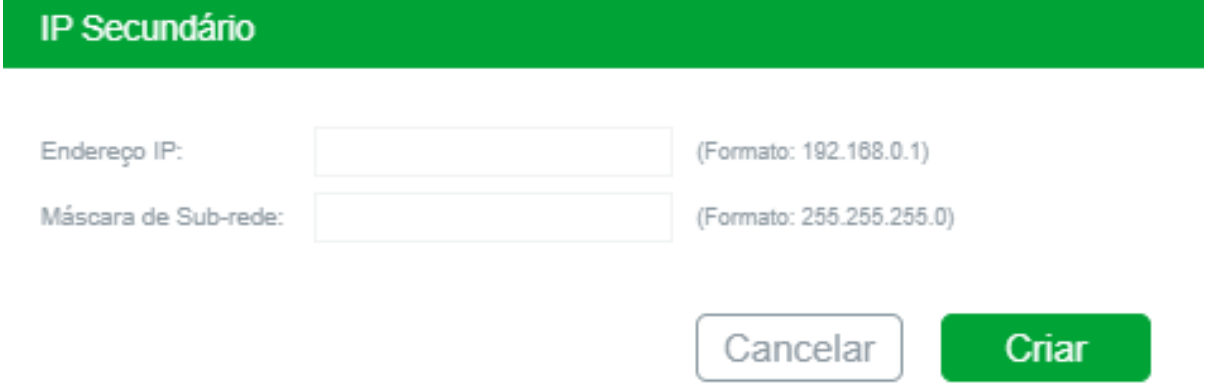
Vá ao menu **FUNÇÕES L3 > Interface VLAN** e clique em **Editar IPv4** para carregar a página a seguir e edite os parâmetros IPv4 da interface.



1. Na seção **Modificar Interface IPv4**, configure os parâmetros relevantes para a interface de acordo com suas necessidades reais. Depois clique em **Aplicar**.

ID da interface	Exibe o ID da interface.
Status do Administrador	Ativar os recursos da interface de camada 3.
Nome da Interface	(Opcional) Digite um nome para a interface.
Modo de Endereço IP	Especifique o modo de atribuição de endereço IP da interface. **Nenhum:** nenhum endereço IP será atribuído à interface. **Estático:** atribua um endereço IP à interface manualmente. **DHCP:** atribua um endereço IP à interface através do servidor DHCP. **BOOTP:** atribua um endereço IP à interface através do servidor BOOTP.
Endereço IP	Especifique o endereço IP da interface se você escolher "Estático" como o modo de atribuição de endereço IP.
Máscara de sub-rede	Especifique a máscara de sub-rede do endereço IP da interface.
DHCP Option 12	Se você selecionar DHCP como o modo de endereço IP, configure a opção 12 aqui. A opção 12 do DHCP é usada para especificar o nome do cliente.

2. Na seção **Tabela de IP Secundário**, clique em Adicionar para adicionar um IP secundário à interface especificada, o que permite que você tenha duas sub-redes lógicas. Então clique em **Criar**.

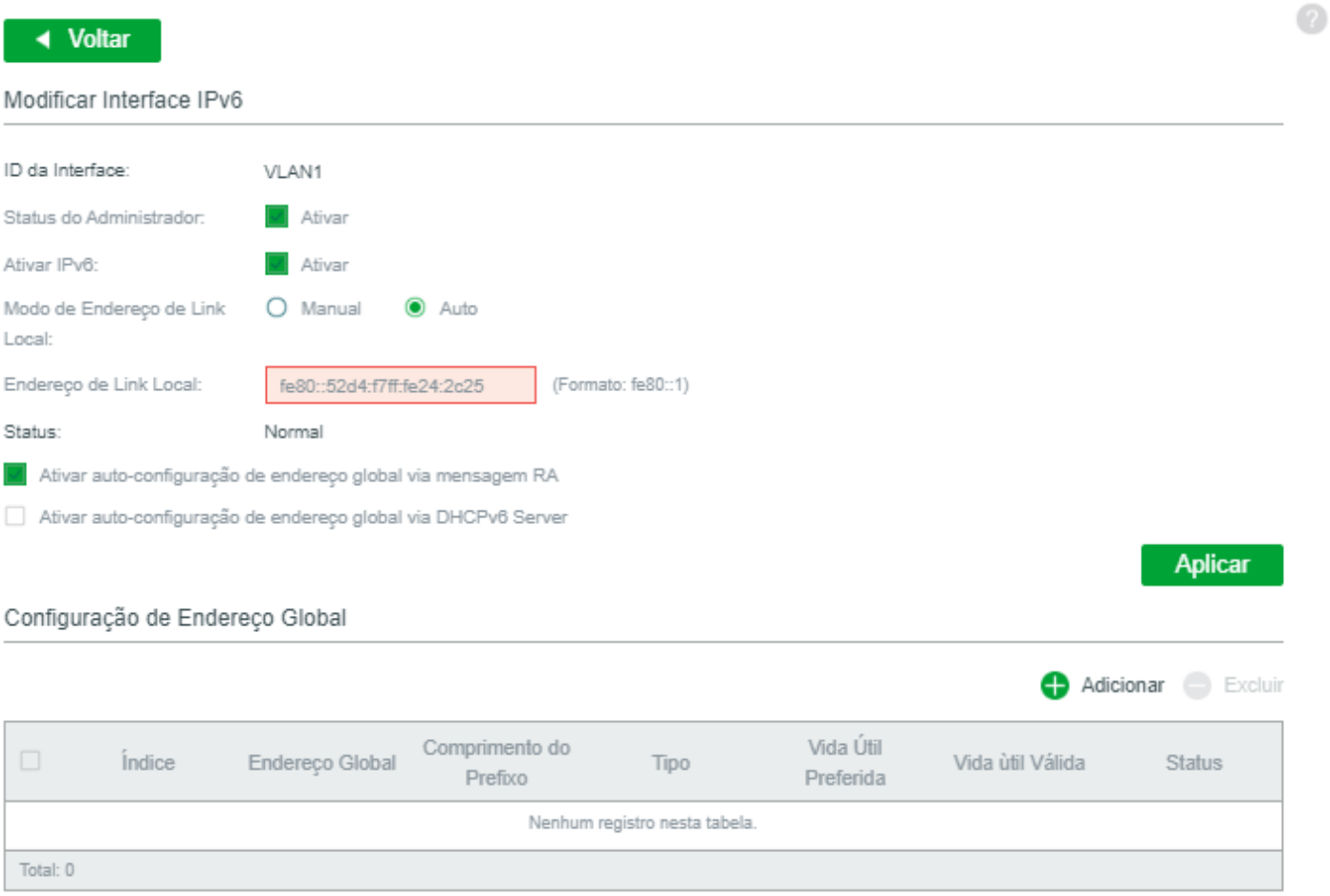


Endereço IP	Especifique o endereço IP secundário da interface.
Máscara de sub-rede	Especifique a máscara de sub-rede do endereço IP secundário.

3. (Opcional) Na seção Lista de IPs Secundários, você pode visualizar a entrada de IP secundária correspondente que você criou.

Configurando os Parâmetros IPv6 da Interface

Escolha o menu **FUNÇÕES L3 > Interface VLAN** e clique em **Editar IPv6** para carregar a página a seguir e edite os parâmetros IPv6 da interface.



1. Na seção **Modificar Interface IPv6**, ative o recurso IPv6 para a interface e configure os parâmetros correspondentes. Depois clique em **Aplicar**.

ID da interface	Exibe o ID da interface.
Status do Administrador	Ativar os recursos da interface de camada 3.
Ativar IPv6	Habilite o recurso IPv6 da interface.
Modo de Endereço de Link Local	Selecione o modo de configuração do endereço local do link. **Manual:** com esta opção selecionada, você pode atribuir um endereço de link local manualmente. **Automático:** com esta opção selecionada, o switch gera um endereço local de link automaticamente. **BOOTP:** atribua um endereço IP à interface através do servidor BOOTP.
Endereço de Link LocalIP	Digite um endereço de link local se você escolher “Manual” como o modo Endereço do link local.
Status	Exibe o status do endereço de link local. Um endereço IPv6 não pode ser usado antes de passar no DAD (Duplicate Address Detection), que é usado para detectar conflitos de endereço. No processo DAD, o endereço IPv6 pode ter três status diferentes: **Normal:** indica que o endereço de link local passou pelo DAD e pode ser usado normalmente. **Tente:** indica que o endereço de link local está em andamento no DAD e não pode ser usado no momento. **Repita:** indica que o endereço de link local está duplicado, esse endereço já está sendo usado por outro nó e não pode ser usado pela interface.

2. Configure o endereço IPv6 global da interface pode ser utilizada três maneiras:

- **Via mensagem RA:**

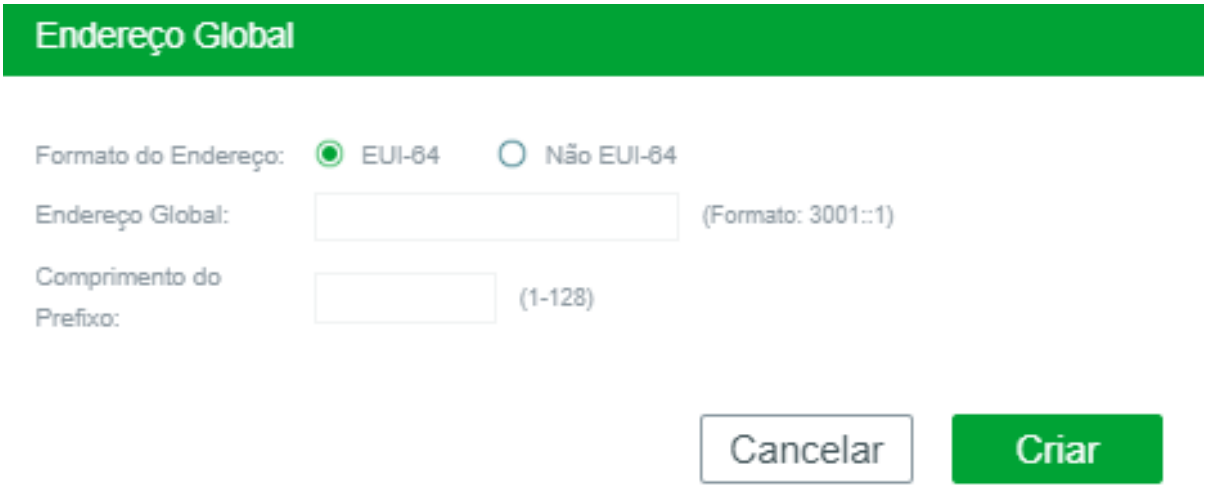
Ativar autoconfiguração de endereço global via mensagem RA	Com essa opção ativada, a interface gera automaticamente um endereço global e outras informações de acordo com o prefixo do endereço e outros parâmetros de configuração da mensagem RA (Anúncio do roteador) recebida.

- **Via Servidor DHCPv6:**

Ativar autoconfiguração de endereço global via DHCPv6 Server	Com essa opção ativada, o switch tentará obter o endereço global do servidor DHCPv6.

- **Manualmente:**

Na seção **Configuração de Endereço Global**, clique em Adicionar para atribuir manualmente um endereço global IPv6 à interface.



Formato do Endereço	Selecione o formato de endereço global de acordo com suas necessidades. **EUI-64:** indica que você só precisa especificar um prefixo de endereço; o sistema criará um endereço global automaticamente. **Não EUI-64:** indica que você precisa especificar um endereço global inteiro.
Endereço Global	Quando EUI-64 for selecionado, insira o prefixo do endereço; caso contrário, insira um endereço IPv6 inteiro.
Comprimento do Prefixo	Configure o comprimento do prefixo do endereço global.

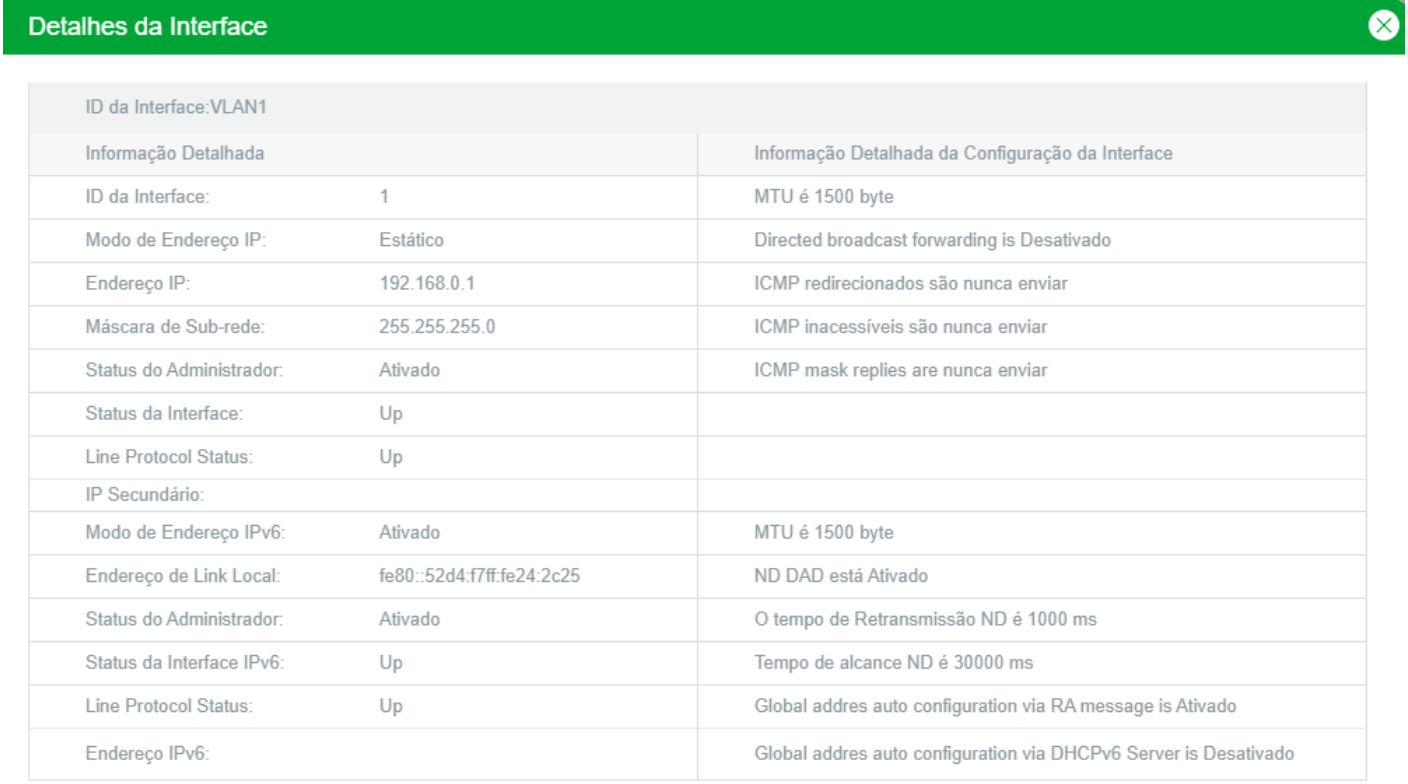
3. Veja a entrada de endereço global na tabela de endereços global.

Endereço global	Exiba ou modifique o endereço global.
Comprimento do Prefixo	Veja ou modifique o tamanho do prefixo do endereço global.

Tipo	Exibe o modo de configuração do endereço global. **Manual:** indica que o endereço correspondente está configurado manualmente. **Automático:** indica que o endereço correspondente é criado automaticamente usando a mensagem RA ou obtido do servidor DHCPv6.
Vida Útil Preferida	Exibe a vida útil preferida do endereço global. Vida útil preferida é o período em que um endereço IPv6 válido é preferido. Quando o horário preferido expira, o endereço fica obsoleto, mas ainda pode ser usado, e você precisa mudar para outro endereço.
Vida Útil Válida	Exibe a vida útil preferida do endereço global. Vida útil preferida é o período em que um endereço IPv6 é válido. Quando o tempo definido expira, o endereço fica obsoleto, mas ainda pode ser usado, e você precisa mudar para outro endereço.
Status	Exibe o status do endereço de link local. Um endereço IPv6 não pode ser usado antes de passar no DAD (Duplicate Address Detection), que é usado para detectar conflitos de endereço. No processo DAD, o endereço IPv6 pode ter três status diferentes: **Normal:** indica que o endereço de link local passou pelo DAD e pode ser usado normalmente. **Tente:** indica que o endereço de link local está em andamento no DAD e não pode ser usado no momento. **Repita:** indica que o endereço de link local está duplicado, esse endereço já está sendo usado por outro nó e não pode ser usado pela interface.

Visualizando Informações Detalhadas da Interface

Escolha o menu **FUNÇÕES L3 > Interface VLAN** para carregar a seguinte página. Clique em **Detalhes** para carregar a página a seguir e visualizar as informações detalhadas da interface.



Apêndice: Configuração Padrão

As configurações padrão para Interface de Camada 3 estão listadas nas tabelas a seguir.

Configurações padrão da interface de camada 3

Parâmetros	Configurações Padrão
Roteamento IPv4	Ativado
Roteamento IPv6	Desativado

Configurações dos parâmetros IPv4 da interface

Parâmetros	Configurações Padrão
ID da Interface	VLAN
Modo de Endereço IP	Nenhum
Status do Administrador	Ativado

Configurações dos parâmetros IPv6 da interface

Parâmetros	Configurações Padrão
Status do Administrador	Ativado
Ativar IPv6	Ativado
Modo de Endereço de Link Local	Automático

Ativar autoconfiguração de endereço global via mensagem RA	Ativado
Ativar autoconfiguração de endereço global via DHCPv6 Server	Desativado

ROTEAMENTO

Visão Geral

A tabela de roteamento é usada para um dispositivo da Camada 3 (neste manual de configuração, significa o switch) para encaminhar pacotes para o destino correto. Quando o switch recebe pacotes nos quais o endereço IP de origem e o endereço IP de destino estão em sub-redes diferentes, ele verifica a tabela de roteamento, encontra a interface de saída correta e encaminha os pacotes.

A tabela de roteamento contém principalmente dois tipos de entradas de roteamento: entradas de roteamento dinâmicas e entradas de roteamento estáticas.

As entradas de roteamento dinâmicas são geradas automaticamente pelo switch. O switch usa protocolos de roteamento dinâmico para calcular automaticamente a melhor rota para encaminhar pacotes.

Entradas de roteamento estático são adicionadas manualmente sem vencimento. Em uma rede simples com um pequeno número de dispositivos, você só precisa configurar rotas estáticas para garantir que os dispositivos de diferentes sub-redes possam se comunicar. Em uma rede complexa de larga escala, as rotas estáticas garantem conectividade estável para aplicativos importantes, porque as rotas estáticas permanecem inalteradas mesmo quando a topologia é alterada.

O switch suporta roteamento estático IPv4 e configuração de roteamento estático IPv6.

Configuração de Roteamento estático IPv4

Escolha o menu **FUNÇÕES L3> Roteamento Estático> Roteamento Estático IPv4** e clique em Adicionar para carregar a página a seguir.

Configure os parâmetros correspondentes para adicionar uma entrada de roteamento estático IPv4. Então clique em **Criar**.

Destino	Especifique o endereço IPv4 de destino dos pacotes.
Máscara de Sub-rede	Especifique a máscara de sub-rede do endereço IPv4 de destino.
Próximo Salto	Especifique o endereço do gateway IPv4 para o qual o pacote deve ser enviado a seguir.
Distância	Especifique a distância administrativa, que é a classificação de confiança de uma entrada de roteamento. Um valor mais alto significa uma classificação de confiança mais baixa. Entre as rotas para o mesmo destino, a rota com o menor valor de distância será registrada na tabela de roteamento IPv4. O valor válido varia de 1 a 255 e o valor padrão é 1.

Configuração de Roteamento estático IPv6

Escolha o menu **FUNÇÕES L3> Roteamento Estático> Roteamento Estático IPv6** e clique em Adicionar para carregar a página a seguir.

Configure os parâmetros correspondentes para adicionar uma entrada de roteamento estático IPv6. Então clique em **Criar**.

Endereço IPv6	Especifique o endereço IPv6 de destino dos pacotes.
Comprimento do Prefixo	Especifique o tamanho do prefixo do endereço IPv6.
Próximo Salto	Especifique o endereço do gateway IPv6 para o qual o pacote deve ser enviado a seguir.
Distância	Especifique a distância administrativa, que é a classificação de confiança de uma entrada de roteamento. Um valor mais alto significa uma classificação de confiança mais baixa. Entre as rotas para o mesmo destino, a rota com o menor valor de distância será registrada na tabela de roteamento IPv6. O valor válido varia de 1 a 255 e o valor padrão é 1.

Visualizando a Tabela de Roteamento

Você pode visualizar as tabelas de roteamento para aprender sobre a topologia de rede. O switch suporta a tabela de roteamento IPv4 e a tabela de roteamento IPv6.

Visualizando a Tabela de Roteamento IPv4

Escolha o menu **FUNÇÕES L3> Tabela de roteamento> Tabela de roteamento IPv4** para carregar a página a seguir.

Veja as entradas de roteamento IPv4.

Protocolo	Exibe o tipo da entrada de roteamento. **Conectado:** a rede de destino é direcionada conectada ao switch. **Estático:** a entrada de roteamento é uma entrada de roteamento estático adicionada manualmente.
Rede de Destino	Exibe o endereço IP de destino e a máscara de sub-rede.
Próximo Salto	Exibe o endereço do gateway IPv4 para o qual o pacote deve ser enviado a seguir.
Distância	Exibe a distância administrativa, que é a classificação de confiança de uma entrada de roteamento. Um valor mais alto significa uma classificação de confiança mais baixa. Entre as rotas para o mesmo destino, a rota com o menor valor de distância será registrada na tabela de roteamento IPv4. O valor válido varia de 1 a 255 e o valor padrão é 1.
Métrica	Exibe a métrica para alcançar o endereço IP de destino.
Nome da Interface	Exibe o nome da interface do gateway.

Visualizando a Tabela de Roteamento IPv6

Escolha o menu **FUNÇÕES L3> Tabela de roteamento> Tabela de roteamento IPv6** para carregar a página a seguir.

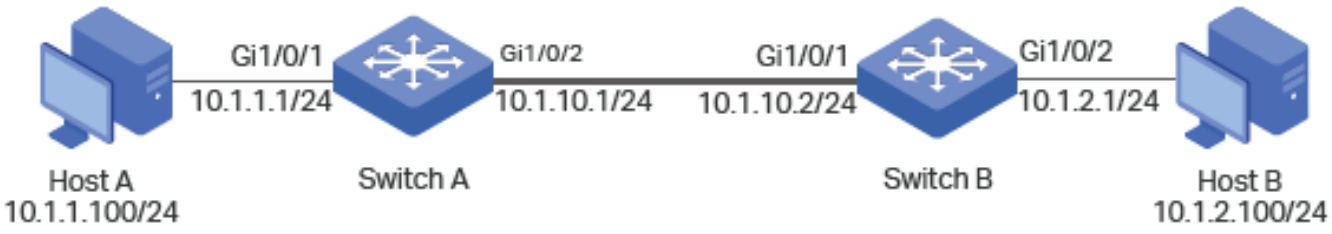
Veja as entradas de roteamento IPv6.

Protocolo	Exibe o tipo da entrada de roteamento. **Conectado:** a rede de destino é direcionada conectada ao switch. **Estático:** a entrada de roteamento é uma entrada de roteamento estático adicionada manualmente.
Rede de Destino	Exibe o endereço IP de destino e a máscara de sub-rede.
Próximo Salto	Exibe o endereço do gateway IPv6 para o qual o pacote deve ser enviado a seguir.
Distância	Exibe a distância administrativa, que é a classificação de confiança de uma entrada de roteamento. Um valor mais alto significa uma classificação de confiança mais baixa. Entre as rotas para o mesmo destino, a rota com o menor valor de distância será registrada na tabela de roteamento IPv6. O valor válido varia de 1 a 255 e o valor padrão é 1.
Métrica	Exibe a métrica para alcançar o endereço IP de destino.
Nome da Interface	Exibe o nome da interface do gateway.

Exemplos de Roteamento Estático

Requisitos de Rede

Como mostrado abaixo, o Host A e o Host B estão em diferentes segmentos de rede. Para atender às necessidades do negócio, o Host A e o Host B precisam estabelecer uma conexão sem usar protocolos de roteamento dinâmico para garantir conectividade estável.

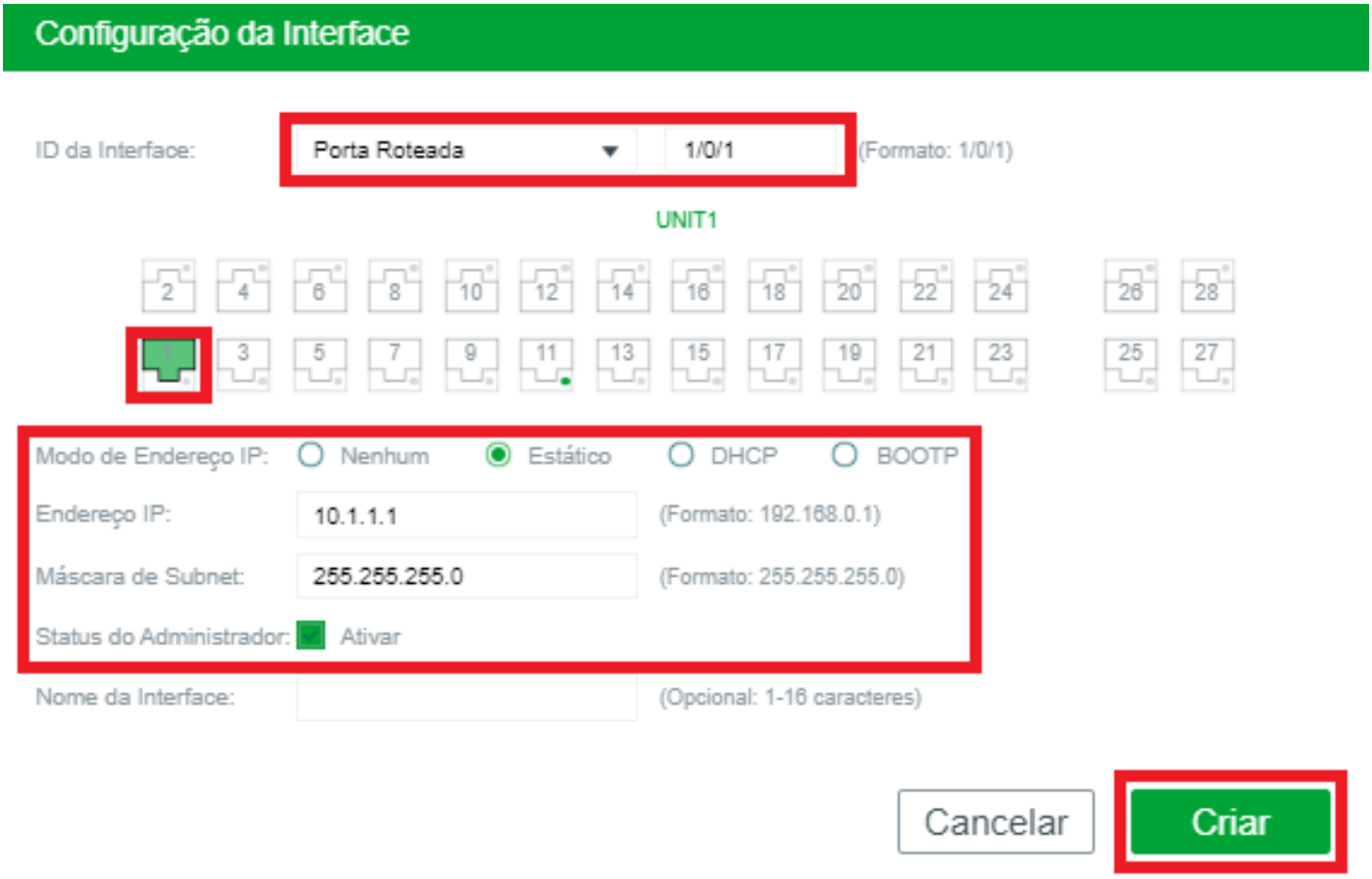


Configurando o Cenário

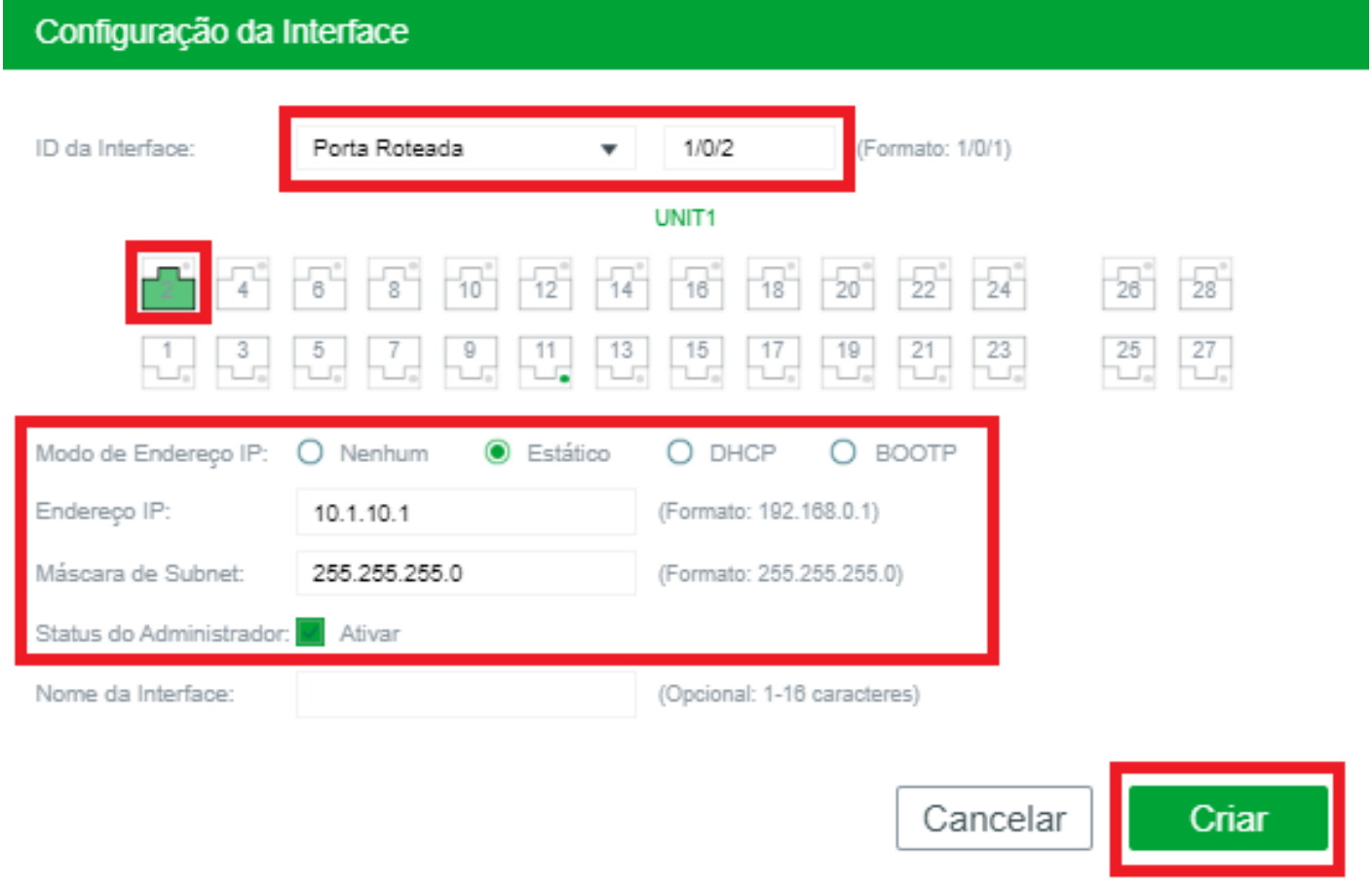
Para implementar esse requisito, você pode configurar o gateway padrão do host A como 10.1.1.1/24, o gateway padrão do host B como 10.1.2.1/24 e configurar as rotas estáticas IPv4 no Switch A e Switch B para que hosts em diferentes segmentos de rede possam se comunicar entre si.

As configurações do switch A e do switch B são semelhantes. As apresentações a seguir tomam o Switch A como exemplo.

1. Escolha o menu **FUNÇÕES L3> Interface** para criar uma porta roteada Gi1/0/1 no modo estático, com o endereço IP 10.1.1.1, a máscara 255.255.255.0 e o status de administrador **Ativar**, clique em **Criar**.



2. No mesmo menu, crie uma porta roteada Gi1/0/2 no modo estático, com o endereço IP 10.1.10.1, a máscara como 255.255.255.0 e o status de administrador Ativar, clique em **Criar**.



3. Escolha o menu **FUNÇÕES L3> Roteamento estático> Roteamento estático IPv4** clique em Adicionar para carregar a página a seguir. Adicione uma entrada de roteamento estático com o destino 10.1.2.0, a máscara de sub-rede 255.255.255.0 e o próximo salto 10.1.10.2, clique em Criar. Para o switch B, adicione uma entrada de rota estática com o destino 10.1.1.0, a máscara de sub-rede 255.255.255.0 e o próximo salto 10.1.10.1, clique em **Criar**.

SERVIÇOS DHCP

DHCP

Visão Geral

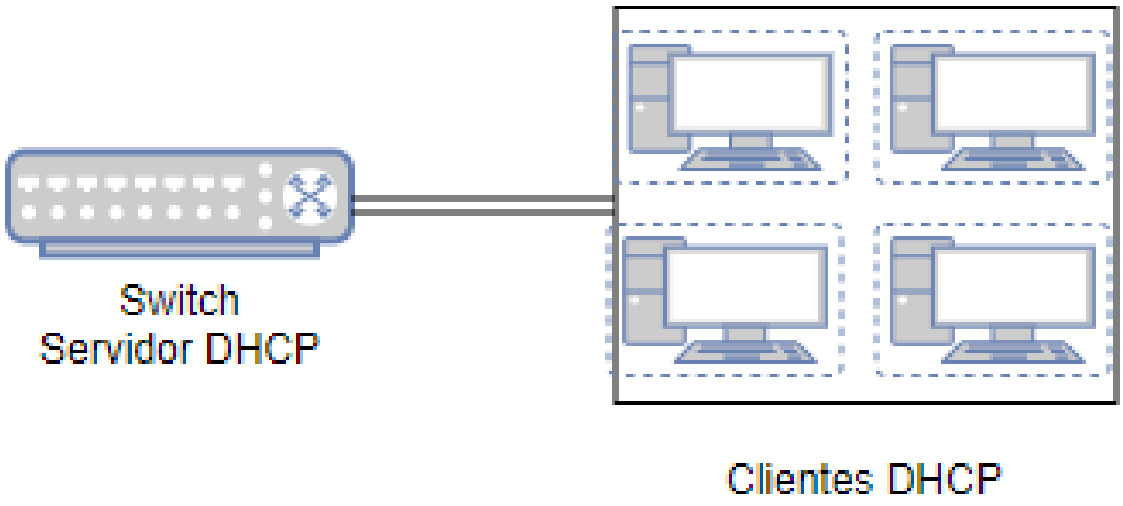
DHCP (Dynamic Host Configuration Protocol) é amplamente utilizado para atribuir automaticamente endereços IP e outros parâmetros de configuração à dispositivos na rede. Melhorando assim a utilização dos endereços IP.

Funções suportadas

As funções DHCP suportadas pelo switch incluem Servidor DHCP, DHCP Relay e DHCP L2 Relay.

DHCP Server

Servidor DHCP é utilizado para atribuir automaticamente endereço IP, gateway padrão e outros parâmetros aos clientes DHCP. Como mostrado na figura a baixo, o switch age como servidor DHCP e atribui endereços IP aos clientes.



DHCP Relay

DHCP Relay é utilizado para processar e encaminhar pacotes DHCP entre diferentes sub-rede ou VLANs.

O cliente DHCP encaminha a solicitação de um endereço IP através de uma requisição de DHCP utilizando pacotes broadcast. Uma vez que as transmissões de pacotes broadcast são sempre limitadas à rede local, então caso o servidor DHCP estiver em outra rede ou não estiver na mesma VLAN que o cliente, o cliente não conseguirá obter um endereço IP do servidor. Dessa forma, cada rede local deveria estar equipada com um servidor DHCP, aumentando o custo da construção da rede e criando dificuldades para a central de gerenciamento da mesma.

DHCP Relay resolve este problema. O dispositivo de DHCP Relay opera como um agente de retransmissão e encaminha os pacotes DHCP entre os clientes DHCP e o servidor DHCP em redes locais diferentes para que os clientes DHCP em diferentes redes locais possam compartilhar um servidor DHCP.

DHCP Relay inclui três funções: Option 82, Interface DHCP Relay e VLAN DHCP Relay.

- Option 82

  O switch pode gravar o local da informação do cliente DHCP utilizando a Option 82. O switch pode adicionar a Option 82 ao pacote de requisição DHCP e então transmitir o pacote para o servidor DHCP. O servidor DHCP com suporte à Option 82 pode configurar a política de distribuição de endereços IP e outros parâmetros de forma mais flexível para a

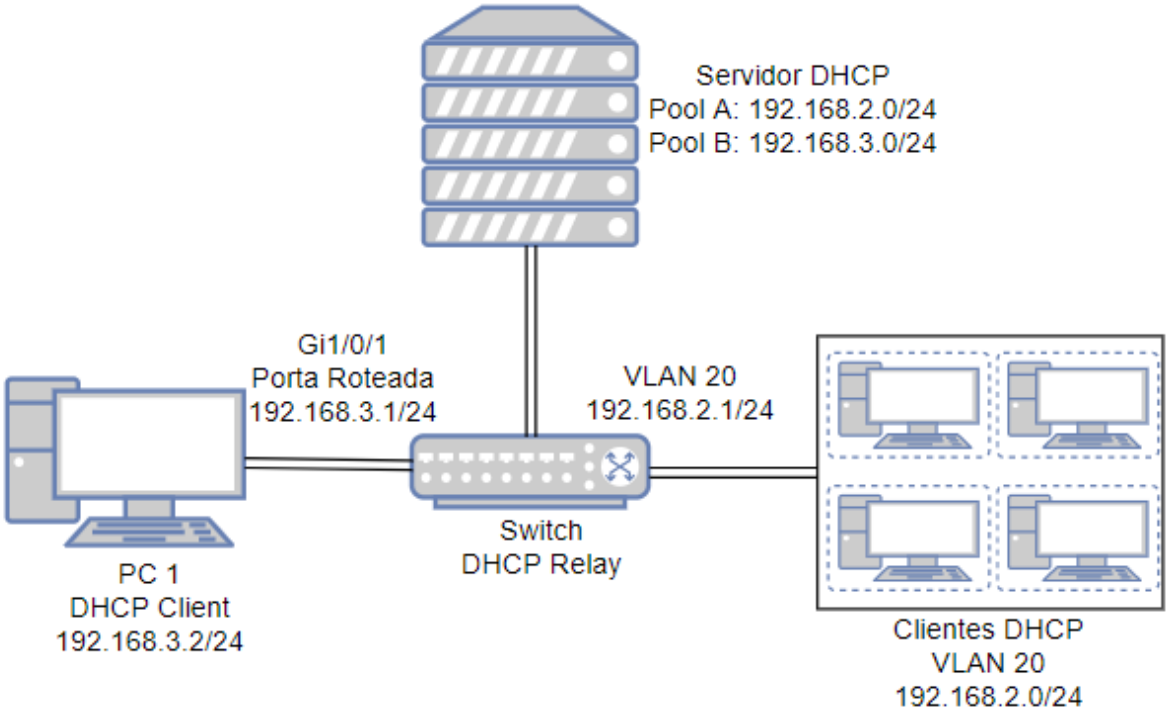
distribuição de endereços.

- Interface DHCP Relay

  O Interface DHCP Relay é utilizado para que clientes em diferentes sub-rede possam obter endereço IP do servidor DHCP que está ou não na mesma sub-rede que os clientes.

  No Interface DHCP Relay, você pode especificar um servidor DHCP para uma interface de camada 3 a qual os clientes estão conectados. Quando receber os pacotes DHCP dos clientes o switch irá preencher o endereço IP da interface correspondente no campo do agende de Relay do pacote DHCP e encaminhará os pacotes para o servidor DHCP. O servidor DHCP atribuirá os endereços IP para os clientes com base no campo de endereço do agende de Relay.

  Como mostrado na figura a seguir. O endereço IP para a VLAN 20 é 192.168.2.1/24 e para a porta roteada GI 1/0/1 é 192.68.3.1/24. Com a Interface de VLAN DHCP configurada. O switch utiliza os endereços de IP da VLAN 20 (192.168.2.1/24) quando atribuir endereços IP para clientes na VLAN 20 e utilizará os endereços da GI 1/0/1 (192.168.3.1/24) quando atribuir endereços IP para o PC 1. Como resultado o servidor DHCP irá atribuir endereços IP da Pool A (sub-rede dos endereços da VLAN 20) para clientes na VLAN 20, e atribuirá endereços da Pool B (sub-rede da GI 1/0/1) ao PC 1.



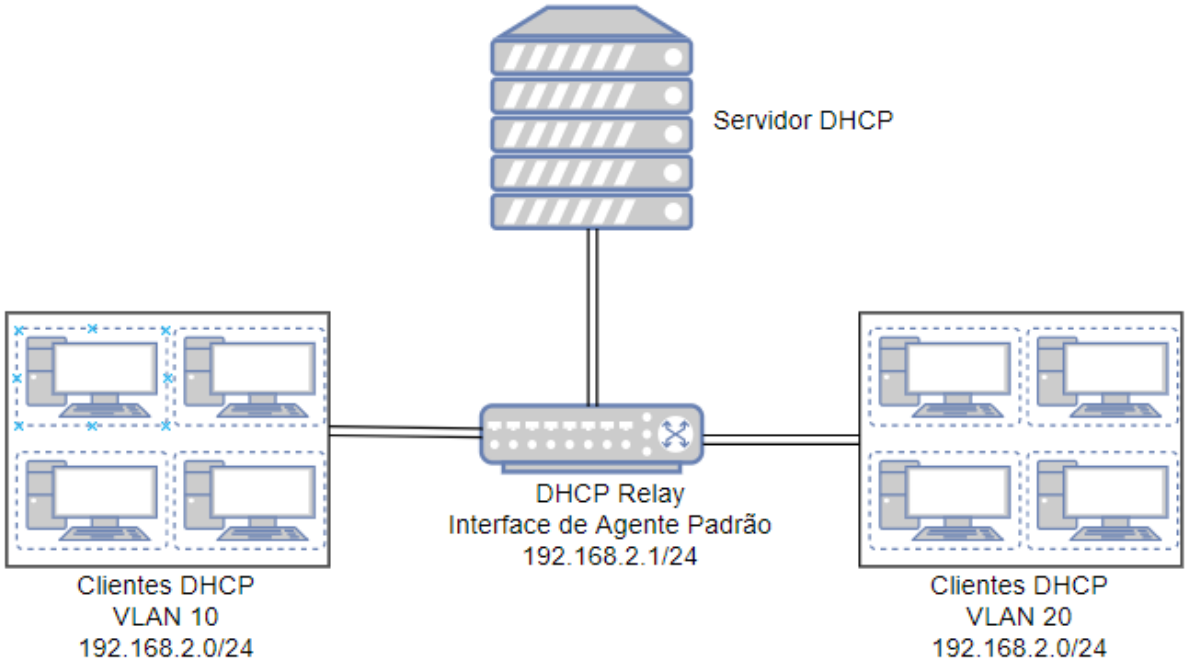
- VLAN DHCP Relay

  VLAN DHCP Relay permite clientes em diferentes VLAN obter endereços IP de um mesmo servidor DHCP usando um único endereço IP do agente de interface.

  No Interface DHCP Relay, para atribuir endereços IP para os clientes em diferentes VLANs você precisa criar uma interface de camada 3 para cada VLAN para garantir o alcance.

  No VLAN DHCP Relay, você pode simplesmente especificar uma interface de camada 3 como agente de interface padrão para todas as VLANs. O switch irá preencher o endereço IP da interface padrão do agente de Relay no campo do pacote DHCP de todas as VLANs.

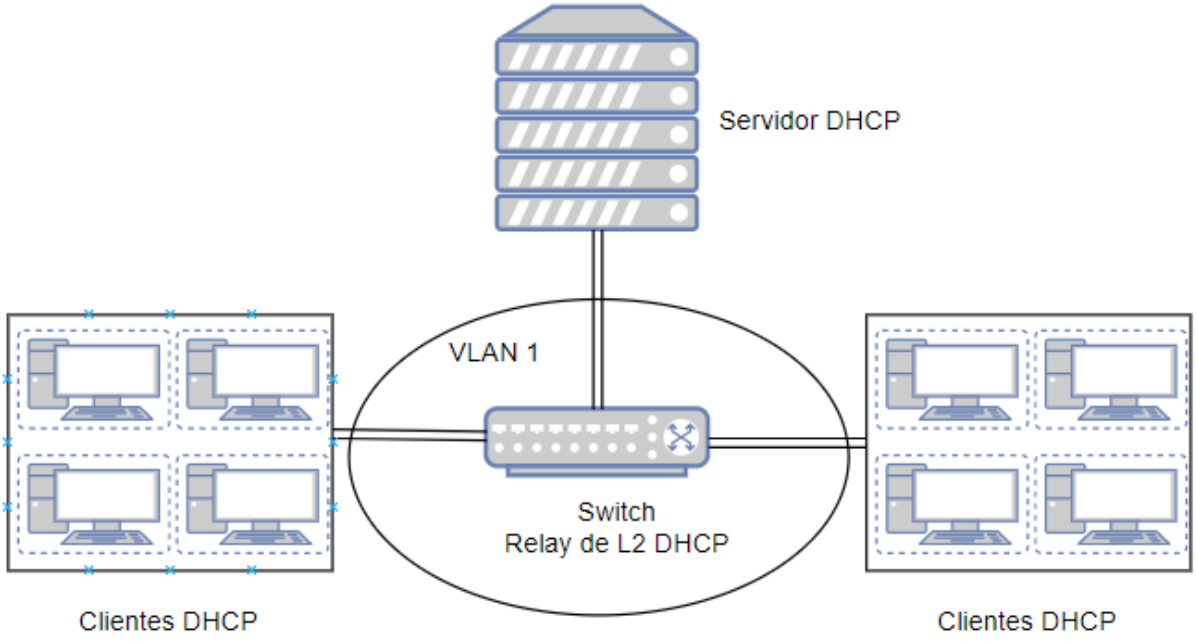
Como mostrado na figura a baixo, nenhum endereço IP está atribuído para as VLANs 10 e 20, porém a interface do agente padrão de relay está configurada com o endereço IP 192.168.2.1/24. O switch utilizará o endereço IP da interface do agente padrão de relay para solicitar endereços IP para os clientes em ambas as VLANs. Como resultado o servidor DHCP irá atribuir endereços IP da rede 192.168.2.0/24 (mesma sub-rede da interface do agente padrão) para os clientes na VLAN 10 e na VLAN 20.



> Se a VLAN já possuir um endereço IP, o switch utilizará o endereço IP da VLAN como endereço IP do agente de Relay. O endereço IP do agente padrão de Relay não terá efeito.
>
> Uma porta roteada ou uma interface de port channel não é associada à uma VLAN em particular. VLAN DHCP Relay não terá efeito em portas roteadas ou interfaces de port channel.

DHCP L2 Relay

Ao contrário do DHCP Relay, o DHCP L2 Relay é utilizado nas situações que o servidor DHCP e os clientes estão na mesma VLAN. No DHCP L2 Relay, em adição à atribuição normal de endereços aos clientes DHCP, o switch pode gravar a informação de localização do cliente DHCP usando a Option 82. O switch pode adicionar a Option 82 ao pacote de requisição DHCP e então transmitir o pacote ao servidor DHCP. O servidor DHCP com suporte à Option 82 pode configurar a política de distribuição de endereços IP e outros parâmetros disponibilizando maior flexibilidade.



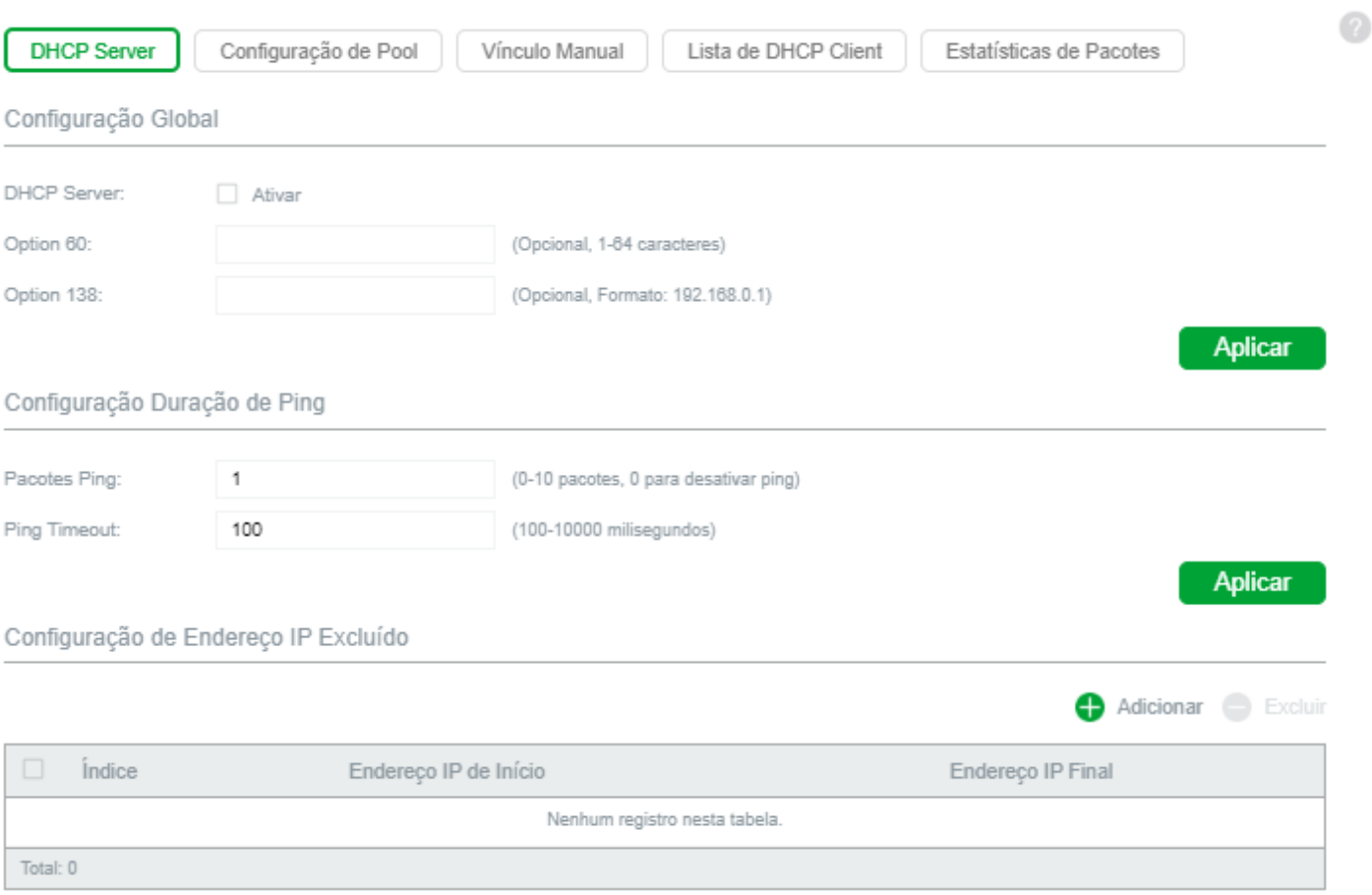
Configuração do Servidor DHCP

Para completar a configuração do servidor DHCP, siga os seguintes passos:

1. Habilite a função de Servidor DHCP no switch.
2. Configure a Pool do Servidor DHCP.
3. (Opcional) Atribua manualmente endereços IP estáticos a alguns clientes caso necessário.

Habilitando o Servidor DHCP

Vá até o menu **FUNÇÕES L3 > Serviço DHCP > DHCP Server > DHCP Server** para carregar a seguinte página.



Siga os seguintes passos para configurar o DHCP Server:

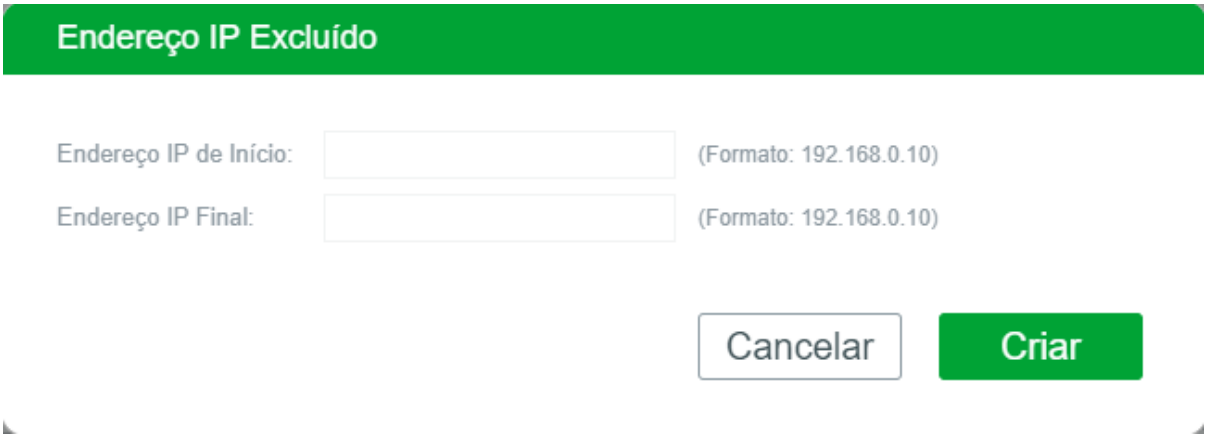
1. Na seção **Configuração Global**, habilite o DHCP Server. Clique em **Aplicar**.

DHCP Server	Habilita o servidor DHCP. Por padrão é desabilitado.
Option 60	(Opcional) Especifica a identificação da Option 60. Normalmente utilizada em cenários onde os APs (Access Points) solicitam endereços IP diferentes de diferentes servidores de acordo com a necessidade. Se um AP solicita a Option 60, o servidor irá responder com um pacote contendo a configuração da Option 60. E então o AP irá comparar a Option 60 recebida com a sua própria. Se forem a mesma o AP irá aceitar o endereço IP atribuído pelo servidor, caso contrário o endereço atribuído não será aceito.
Option 138	(Opcional) Especifique a Option 138, a qual pode ser configurada como de endereço IP de gerenciamento de um dispositivo AC (Access Control). Se os APs na rede local solicitarem essa opção, o servidor irá responder com um pacote contendo essa opção para informar aos APs o endereço IP do AC.

2. Na seção **Configuração Duração de Ping**, configure os pacotes de ping e o tempo de timeout para os testes de ping. Clique em **Aplicar**.

Pacotes Ping	Entre com o número de pacotes ping que o servidor poderá enviar em broadcast para testar se o endereço IP está ocupado. Valores válidos variam entre 1 e 10, por padrão é 1. Quando o switch é configurado como servidor DHCP para atribuir endereços IP dinamicamente aos clientes, o switch irá implementar teste de ping para evitar conflitos de endereço IP.
Timeout de Ping	Especifique o período para timeout do ping em milissegundos. Varia entre 100 até 10000 ms e por padrão é 100 ms. O servidor DHCP encaminhará um ICMP Echo Request (Ping) via broadcast para testar se um endereço IP está ocupado ou não. Se o número de pacotes ping alcançarem o limite especificado e não houver resposta o servidor irá atribuir o endereço IP. Caso contrário, o servidor irá gravar o endereço IP como endereço IP em conflito e irá atribuir outro endereço IP ao cliente.

3. Na seção **Configuração de Endereço IP Excluído**, clique em Adicionar para carregar a seguinte página para especificar um endereço IP que não deve ser atribuído aos clientes.



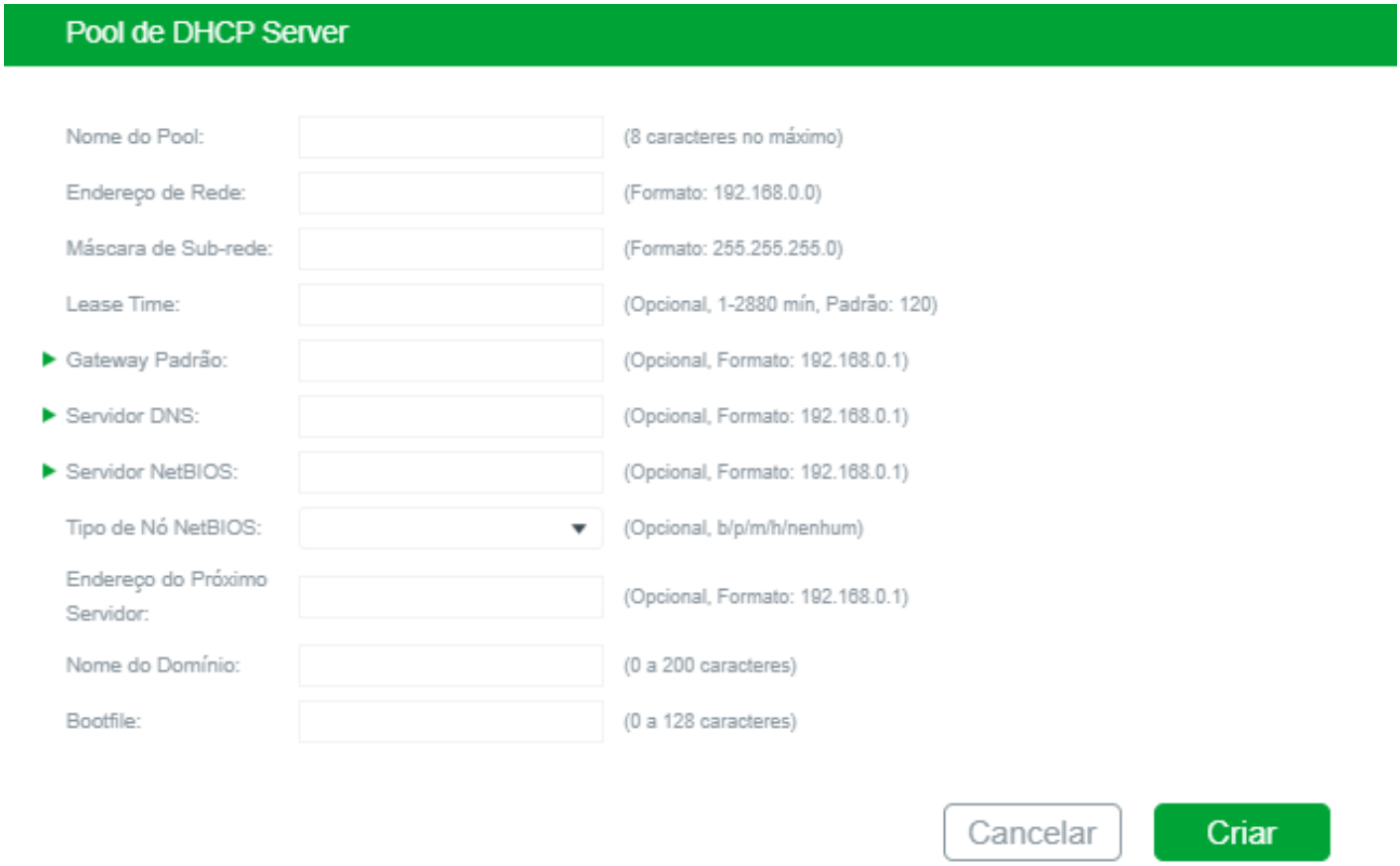
Entre com o endereço IP de início e endereço IP final para especificar o intervalo de endereços IP reservados. Clique em **Criar**.

Endereço IP de Início/Endereço IP Final	Especifique o endereço IP de início e o endereço IP final para excluir do intervalo de endereços IP excluídos. Se o endereço de início e o endereço final forem o mesmo o servidor irá excluir somente um endereço. Quando estiver configurando o servidor DHCP, você precisará reservar certos endereços IP para cada sub-rede, como endereço de gateway padrão, endereço de broadcast e endereço de servidor DNS.

Configurando o Pool do Servidor DHCP

O Pool do servidor DHCP define os parâmetros que serão atribuídos aos clientes DHCP.

Vá até o menu **FUNÇÕES L3 > Serviço DHCP > DHCP Server > Configuração de Pool** clique em ⊕ Adicionar para carregar página a seguir.



Configure os Parâmetros do Pool do servidor DHCP, e então clique em **Criar**.

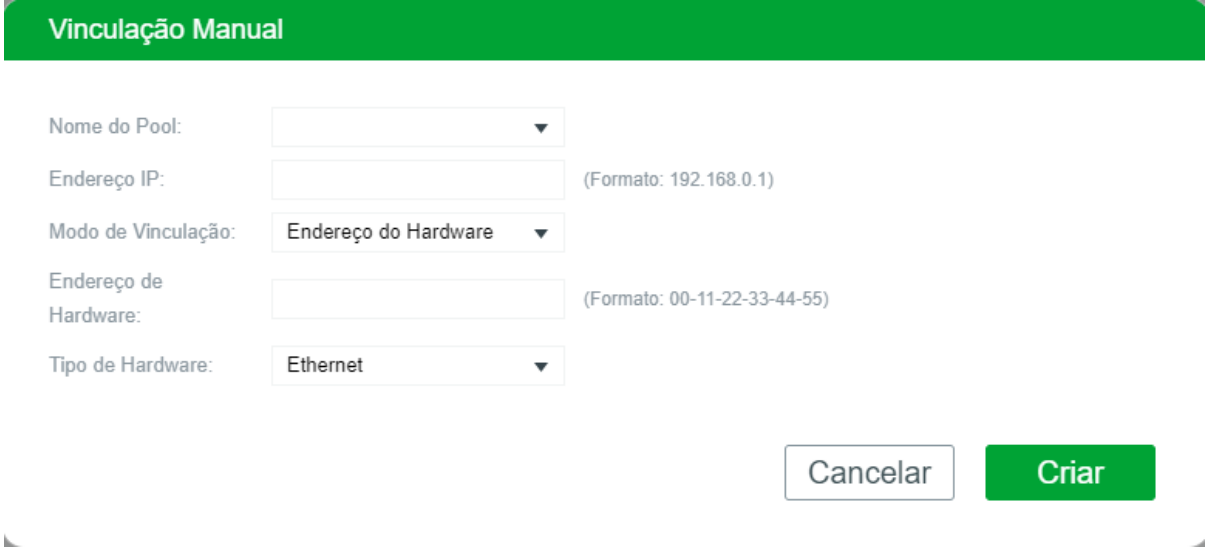
Nome do Pool	Especifique o nome para identificação do Pool.
Endereço de Rede/Máscara de Sub-rede	Configure o endereço de rede e a máscara de sub rede do Pool do servidor DHCP. O endereço de rede e a máscara de sub-rede decidem o intervalo do Pool do servidor DHCP. Na mesma sub-rede, todos os endereços podem ser atribuídos com exceção dos endereços excluídos e dos endereços especiais.
Lease Time	Especifique por quanto tempo um cliente pode utilizar um endereço IP atribuído por este Pool. Varia entre 1 e 2880 minutos e por padrão é configurado como 120 minutos.
Gateway Padrão	(Opcional) Configure o gateway padrão do Pool do Servidor DHCP. Você pode criar até 8 gateways padrão para cada Pool. Em geral você pode configurar o endereço IP da interface VLAN como endereço de gateway Padrão.

Servidor DNS	(Opcional) Especifique o endereço do servidor de DNS do Pool. Você pode especificar até 8 servidores de DNS para cada Pool.
Servidor NetBIOS	(Opcional) Especifique o nome do servidor NetBIOS do Pool. Você pode especificar até 8 servidores de NetBIOS para cada Pool. Quando cliente DHCP utiliza protocolo de rede NetBIOS (Basic Input Output System) para comunicação, o nome do host deve ser mapeado para o endereço IP. O nome do servidor NetBIOS consegue resolver os nomes dos hosts em endereços IP.
Tipo de Nó NetBIOS	(Opcional) Especifique o tipo de NetBIOS para os clientes, os quais são o modo de resolução de endereço IP. As seguintes opções são disponibilizadas: **b-node Broadcast:** os clientes enviam mensagens de query via Broadcast. **p-node Peer-to-Peer:** os clientes enviam mensagens de query via Unicast. **m-node Mixed:** os clientes enviam mensagens de query via Broadcast primeiramente. Se isso falhar os clientes irão tentar novamente via Unicast. **h-node Hybrid:** os clientes enviam mensagens de query via Unicast primeiramente. Se isso falhar os clientes irão tentar novamente via Broadcast.
Endereço do próximo Servidor	(Opcional) Especifique o endereço IP de um servidor TFTP para os clientes. Se necessário os clientes podem pegar o arquivo de configuração do servidor TFTP para auto instalação..
Nome do Domínio	(Opcional) Especifique o nome do domínio que os clientes devem usar quando forem resolver os nomes dos hosts via DNS.
Bootfile	(Opcional) Especifique o nome do bootfile. Se necessário os clientes podem pegar o arquivo d bootfile do servidor TFTP para auto instalação.

Configurando Vínculo Manual

Alguns dispositivos como servidores web necessitam de endereços IP estáticos. Para isso você pode vincular manualmente o endereço MAC ou a ID de cliente do dispositivo à um endereço IP, e o servidor DHCP irá reservar o endereço IP vinculado para este dispositivo sempre.

Vá até o menu **FUNÇÕES L3 > Serviço DHCP > DHCP Server > Vínculo Manual** clique em Adicionar para carregar a seguinte página.



Selecione o nome da Pool e entre com o endereço IP a ser vinculado. Seleciona o modo de vinculação então finalize a configuração adequadamente. Clique em **Criar**.

Nome do Pool	Selecione a Pool do Servidor DHCP na lista.
Endereço IP	Entre com o endereço IP à ser vinculado ao cliente.
Modo de Vinculação	Selecione o modo de vinculação: **ID do Cliente:** vincula o endereço IP à ID do cliente. **ID do Cliente em ASCII:** vincula o endereço IP à ID do cliente no formato ASCII. **Endereço de Hardware:** vincula o endereço IP ao endereço MAC do cliente.
ID do Cliente	Se você selecionar ID do cliente como modo de vinculação, entre com a ID do cliente neste campo.
Endereço de Hardware	Se você selecionar Endereço de Hardware como modo de vinculação, entre com o endereço MAC do cliente neste campo.
Tipo de Hardware	Se você selecionar Endereço de Hardware como modo de vinculação selecione o tipo de hardware. Os tipos de hardware podem ser Ethernet e IEEE802.

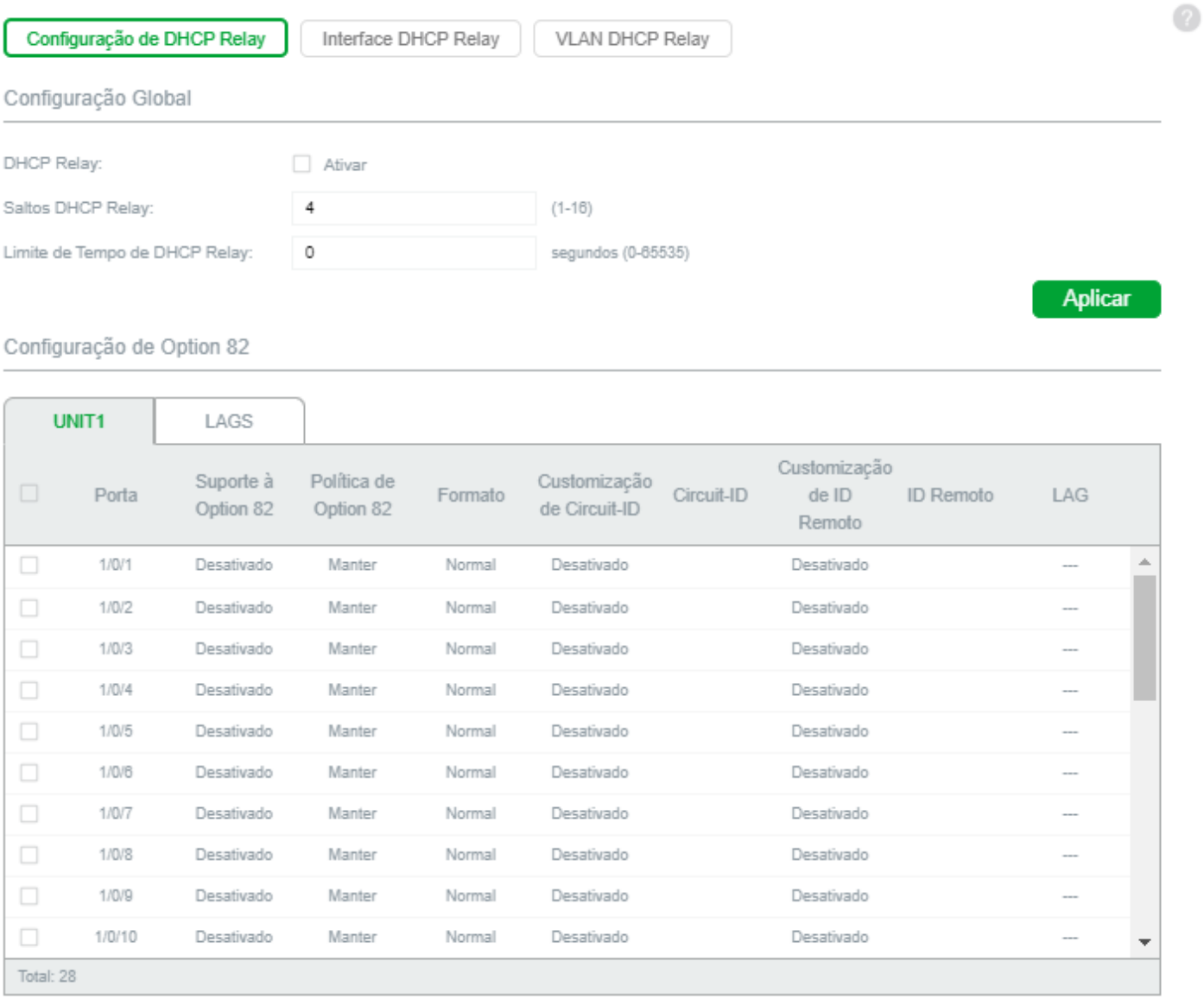
Configuração DHCP Relay

Para completar a configuração do DHCP Relay siga os seguintes passos:

1. Habilite o DHCP Relay. Configure a Option 82 se necessário.
2. Especifique o Servidor DHCP para a interface ou VLAN.

Habilitando o DHCP Relay e Configurando a Option 82

Vá até o menu **FUNÇÕES L3 > Serviço DHCP > DHCP Relay > Configuração de DHCP Relay** para carregar a seguinte página.



Siga os seguintes passos para habilitar o DHCP Relay e configurar a Option 82:

1. Na seção **Configuração Global**, habilite o DHCP Relay globalmente, configure os Saltos DHCP Relay e o Limite de Tempo de DHCP Relay. Clique em **Aplicar**.

DHCP Relay	Habilita o DHCP Relay globalmente.
Saltos DHCP Relay	Especifica o DHCP Relay Hops. DHCP Relay Hops define o número máximo de saltos (agente DHCP Relay) que os pacotes DHCP podem ser retransmitidos. Se um pacote precisar saltar mais vezes do que o número especificado aqui o mesmo será descartado.

	Especifique Threshold de Tempo de DHCP Relay. Valores válidos variam entre 0 e 65535 segundos.
Limite de Tempo de DHCP Relay	Threshold de Tempo de DHCP Relay é o tempo decorrido desde que o cliente iniciou a aquisição ou renovação de endereço IP. Quando o tempo for maior que o indicado aqui os pacotes DHCP serão descartados pelo switch. Valor 0 significa que o switch não irá examinar esse campo nos pacotes DHCP.

2. (Opcional) Na seção Configuração de Option 82, configure a Option 82.

Suporte à Option 82	Seleciona se a Option 82 será habilitada ou não. Por padrão é desabilitada. Option 92 é utilizada para gravar a localização do cliente DHCP, porta Ethernet, VLAN e etc. Se você precisa registrar a localização exata de um cliente, habilite a Option 82 do dispositivo com suporte à Relay mais próximo ao cliente.
Política de Option 82	Selecione a operação para o campo Option 82 nos pacotes DHCP de requisição. **Manter:** indica que será mantido o campo Option 82 nos pacotes. **Substituir:** indica que o campo Option 82 será substituído pelo do switch. Por padrão o Circuit-ID é definido para ser a VLAN e a porta a qual recebe os pacotes de requisição DHCP. Uma ID remota é definida para ser o endereço MAC do dispositivo de DHCP Relay o qual recebe os pacotes de requisição. **Drop:** indica que os pacotes com campo Option 82 serão descartados.
Formato	Seleciona o formato para a subopção da Option 82 dos pacotes de requisição DHCP. **Normal:** indica que o formato da subopção é TLV (Type-Lenght-Value), tipo, tamanho e valor.
Customização de Circuit-ID	Habilita ou desabilita a customização da Option 82. Se habilitado, você precisará configurar a informação da Option 82 manualmente; se desabilitado o switch configurará automaticamente a ID de VLAN e a ID da porta que está recebendo os pacotes DHCP como circuit-id.
Circuit-ID	Entre com o Circuit-ID customizado, o qual contém até 64 caracteres. A configuração de Circuit-ID do switch e do servidor DHCP devem ser compatíveis.
Customização de ID Remoto	Habilita ou desabilita o switch para definir o campo de subopção do ID remoto da Option 82. Se habilitado, você precisará configurar a informação do Id Remoto manualmente; se desabilitado o switch configurará automaticamente o seu próprio endereço de MAC como ID Remoto.

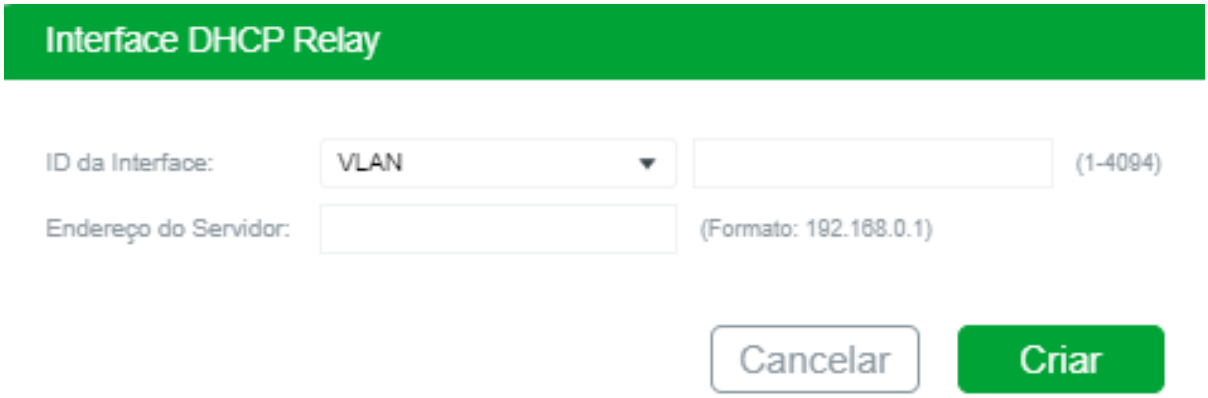
ID remoto	Entre com o ID Remoto customizado, o qual contém até 64 caracteres. A configuração de Circuit-ID do switch e do servidor DHCP devem ser compatíveis.

3. Clique em **Aplicar**.

Configurando Interface DHCP Relay

Interface DHCP Relay é utilizado para clientes que estão conectados à uma interface de camada 3 obter endereço IP de um servidor DHCP, o qual não está conectado na mesma sub-rede que os clientes.

Vá até o menu **FUNÇÕES L3 > Serviço DHCP > DHCP Relay > Interface DHCP Relay** clique em Adicionar para carregar a página a seguir.



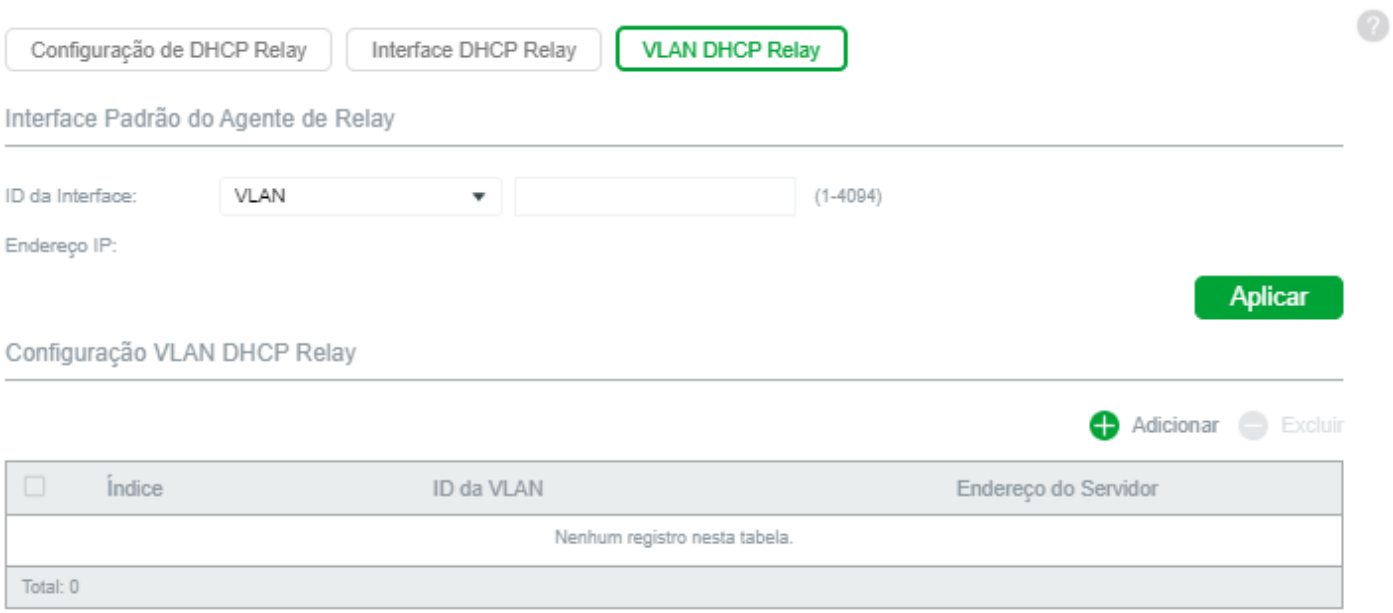
Selecione o tipo de interface e entre com a ID de interface, então entre com o endereço IP do servidor DHCP. Clique em **Criar**.

ID de interface	Especifique o tipo e a ID da interface. Essa é a interface de camada 3 conectada aos clientes DHCP. A interface deve ser uma interface de camada 3 existente.
Endereço do Servidor	Entre com o endereço IP do servidor DHCP.

Configurando VLAN DHCP Relay

VLAN DHCP Relay é usado para cliente em VLANs que não tem interfaces de camada 3 como gateway para obter endereço IP de um servidor DHCP, o qual não está conectado na mesma sub-rede que os clientes.

Vá até o menu **FUNÇÕES L3 > Serviço DHCP > DHCP Relay > VLAN DHCP Relay** para carregar a seguinte página.



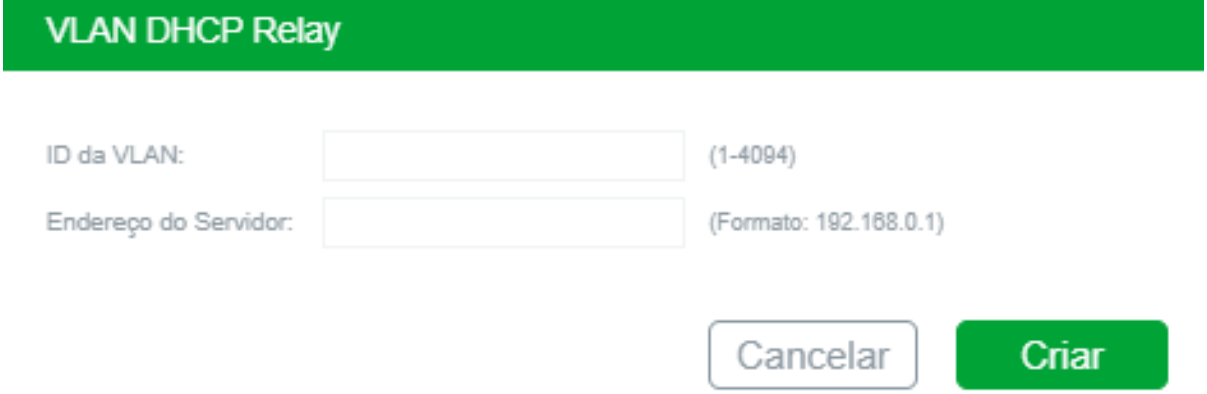
Siga os seguintes passos para especificar um servidor DHCP para uma VLAN específica:

1. Na seção **Interface Padrão do Agente de Relay**, especifique uma interface de camada 3 como agente de Relay padrão para a interface. Então clique em **Aplicar**.

ID de interface	Especifica o tipo e a ID da interface que precisa ser configurada como agente de Relay padrão. Você pode configurar uma interface de camada 3 existente como interface do Agente Padrão de Relay. O servidor DHCP irá fornecer endereços IP da mesma sub-rede que essa interface para os clientes que estão utilizando-a para solicitar endereços IP.
Endereço IP	Mostra o endereço IP da interface.

> Se em uma VLAN os clientes já possuírem um endereço IP, o switch usará a VLAN dos clientes como interface de agente de relay. E a interface do agente padrão de relay especificada manualmente não terá efeito.
>
> Uma porta roteada ou port channel não se associa particularmente à uma VLAN. VLAN DHCP Relay não terá efeito em portas roteadas ou port channels.

2. Na seção **Configuração VLAN do DHCP Relay**, clique em Adicionar para carregar a página de configuração.



Especifique a VLAN à qual os clientes pertencem e o endereço do Servidor. Clique em **Criar**.

ID da VLAN	Especifique a VLAN na qual os clientes podem conseguir endereços de IP do servidor DHCP.
Endereço do Servidor	Entre com o endereço IP do servidor.

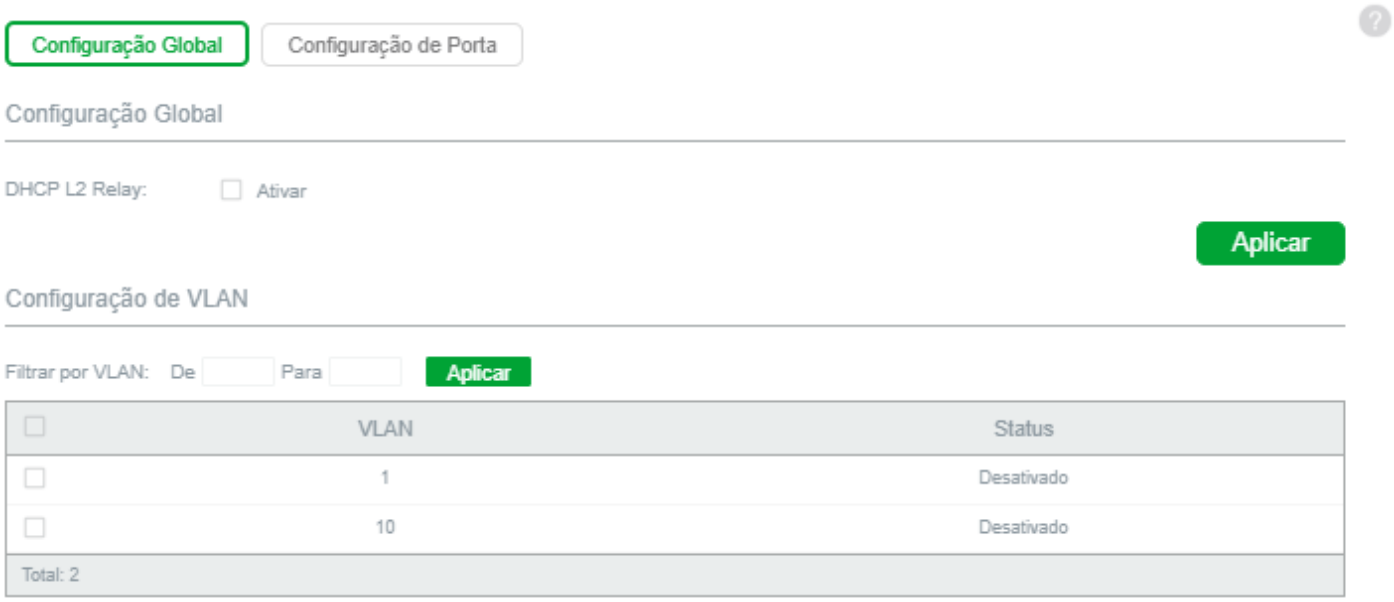
Configuração DHCP L2 Relay

Para completar a configuração do DHCP L2 Relay siga os passos a seguir:

1. Habilite o DHCP L2 Relay.
2. Configure a Option 82 para as portas.

Habilitando DHCP L2 Relay

Vá até o menu **FUNÇÕES L3 > Serviço DHCP > DHCP L2 Relay > Configuração Global** para carregar a seguinte página.



Siga os seguintes passos para habilitar o DHCP L2 Relay globalmente e para uma VLAN específica.

1. Na seção **Configuração Global**, habilite o DHCP L2 Relay globalmente e clique em **Aplicar**.

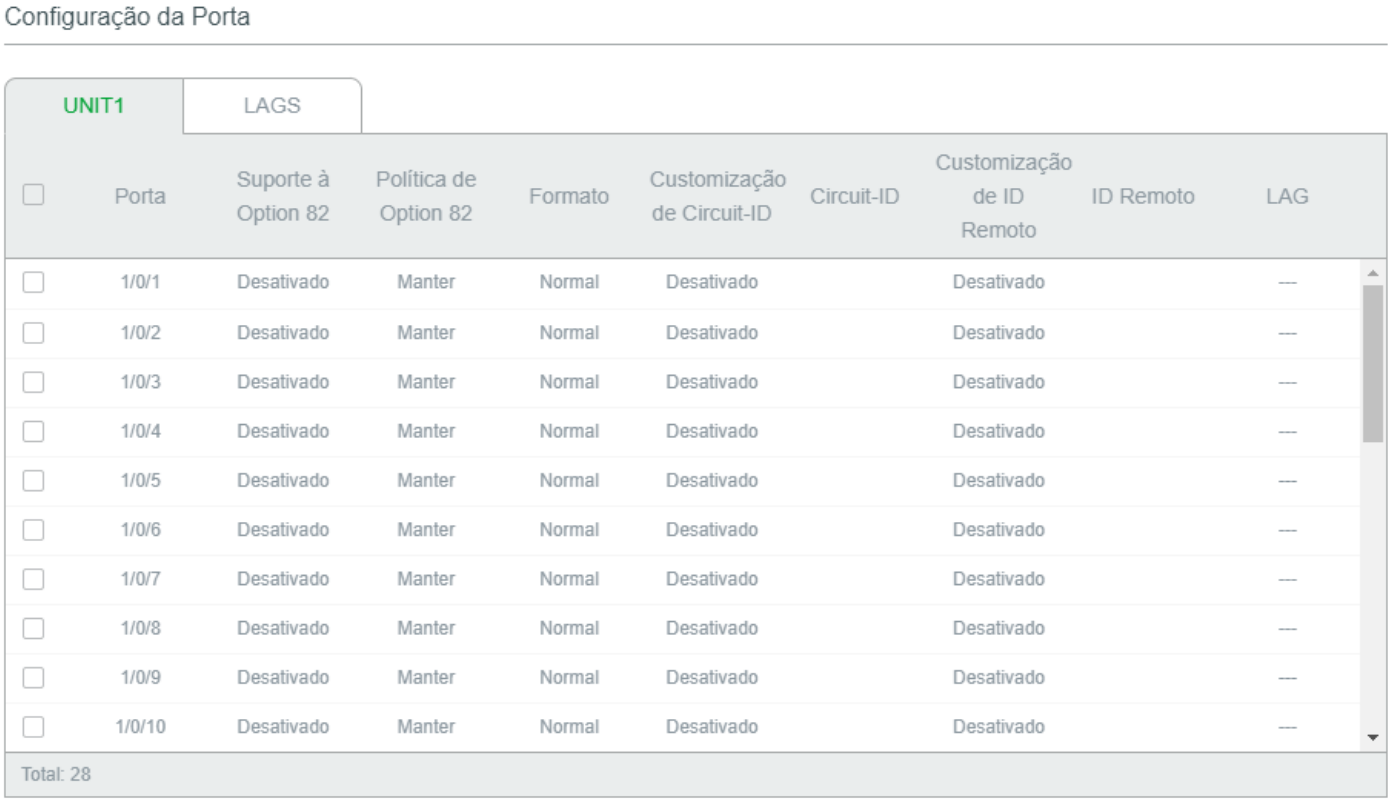
DHCP L2 Relay	Habilite o DHCP L2 Relay globalmente.

2. Na seção **Configuração de VLAN**, habilite o DHCP L2 Relay para uma VLAN específica. Clique em **Aplicar**.

VLAN	Mostra a ID da VLAN.
Status	Habilita o Relay de L2 para uma VLAN específica.

Configurando Option 82 para Portas

Vá até o menu **FUNÇÕES L3 > Serviço DHCP > DHCP L2 Relay > Configuração de Porta** para carregar a página a seguir.



Siga os seguintes passos para habilitar DHCP Relay e configurar a Option 82:

1. Selecione uma ou mais portas para configurar a Option 82.

Suporte à Option 82	Seleciona se a Option 82 será habilitada ou não. Por padrão é desabilitada. Option 92 é utilizada para gravar a localização do cliente DHCP, porta Ethernet, VLAN e etc. Se você precisa registrar a localização exata de um cliente, habilite a Option 82 do dispositivo com suporte à Relay mais próximo ao cliente.
Política de Option 82	Selecione a operação para o campo Option 82 nos pacotes DHCP de requisição. **Manter:** indica que será mantido o campo Option 82 nos pacotes. **Substituir:** indica que o campo Option 82 será substituído pelo do switch. Por padrão o Circuit-ID é definido para ser a VLAN e a porta a qual recebe os pacotes de requisição DHCP. Uma ID remota é definida para ser o endereço MAC do dispositivo de DHCP Relay o qual recebe os pacotes de requisição. **Drop:** indica que os pacotes com campo Option 82 serão descartados.
Formato	Seleciona o formato para a subopção da Option 82 dos pacotes de requisição DHCP. **Normal:** indica que o formato da subopção é TLV (Type-Lenght-Value), tipo, tamanho e valor. **Privado:** indica que o formato da subopção é somente valor.

Customização de Circuit-ID	Habilita ou desabilita a customização da Option 82. Se habilitado, você precisará configurar a informação da Option 82 manualmente; se desabilitado o switch configurará automaticamente a ID de VLAN e a ID da porta que está recebendo os pacotes DHCP como circuit-id.
Circuit-ID	Entre com o Circuit-ID customizado, o qual contém até 64 caracteres. A configuração de Circuit-ID do switch e do servidor DHCP devem ser compatíveis.
Customização de ID Remoto	Habilita ou desabilita o switch para definir o campo de subopção do ID remoto da Option 82. Se habilitado, você precisará configurar a informação do Id Remoto manualmente; se desabilitado o switch configurará automaticamente o seu próprio endereço de MAC como ID Remoto.
ID Remoto	Entre com o ID Remoto customizado, o qual contém até 64 caracteres. A configuração de Circuit-ID do switch e do servidor DHCP devem ser compatíveis.

2. Clique em **Aplicar**.

Exemplos de Configuração

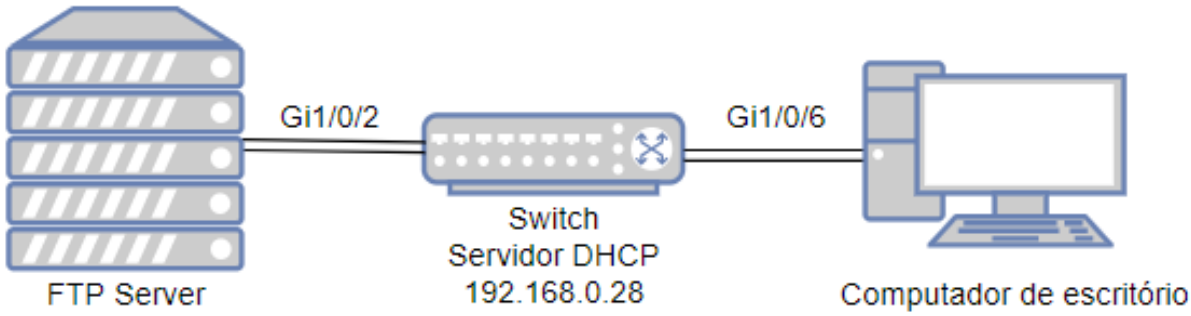
Requisitos de Rede

O administrador utiliza o switch como servidor DHCP para atribuir endereços IP para todos os dispositivos conectados. Os dispositivos conectados incluem um servidor FTP o qual necessita de endereço estático, e um computador que pode obter endereço IP automaticamente do servidor DHCP.

Configurando o Cenário

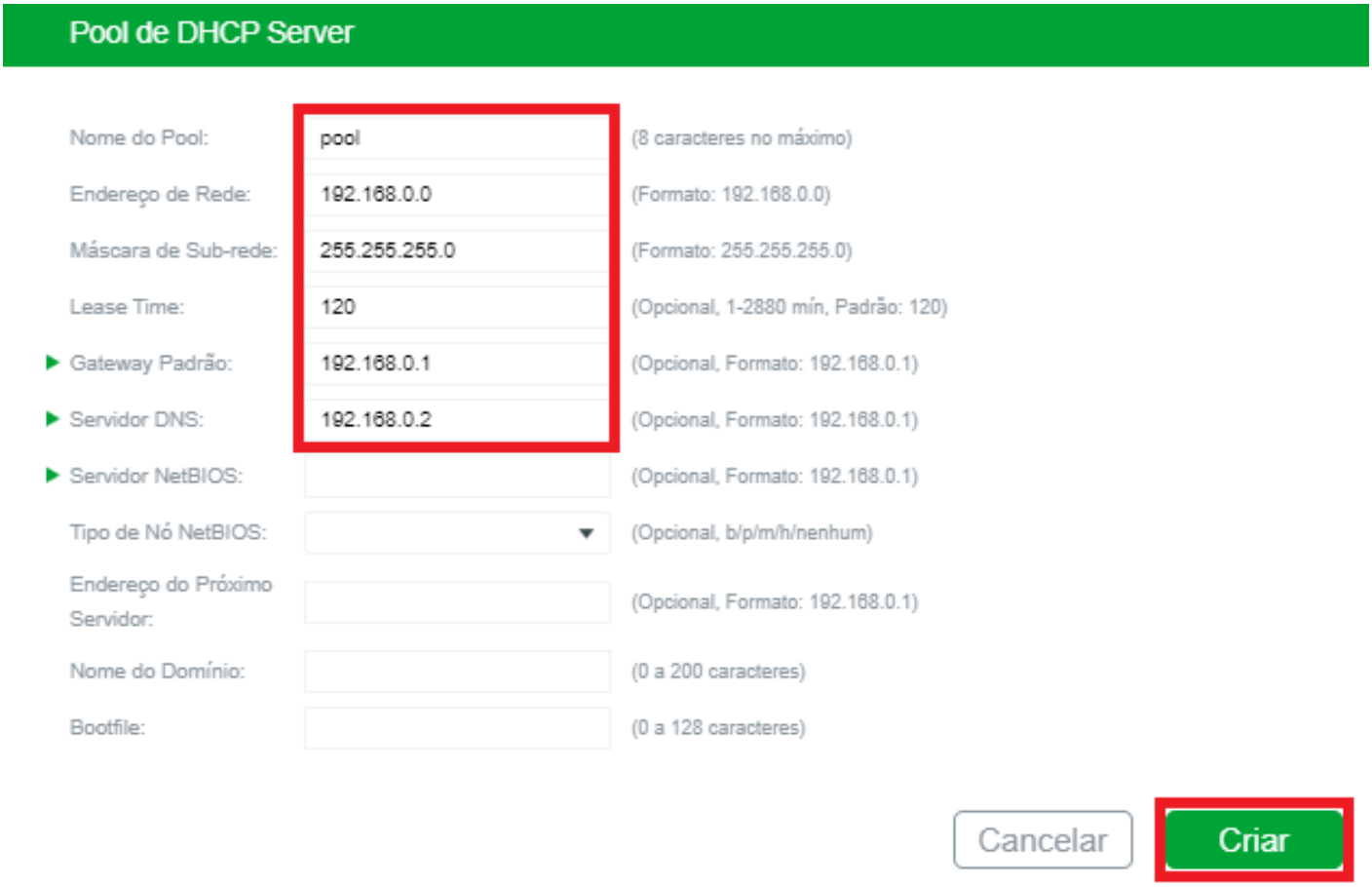
Para simplificar a topologia de rede, esse capitulo pega um servidor FTP e um computador de escritório como exemplo. O servidor FTP e o computador do escritório estão conectados ao switch. O switch atua como servidor DHCP, atribuindo endereço IP estático ao servidor FTP e endereço IP dinâmico ao computador do escritório.

Como mostrado na topologia a seguir. O endereço IP do switch é 192.168.0.28. A porta 1/0/2 está conectada ao servidor FTP e a porta 1/0/6 está conectada ao computador de escritório.



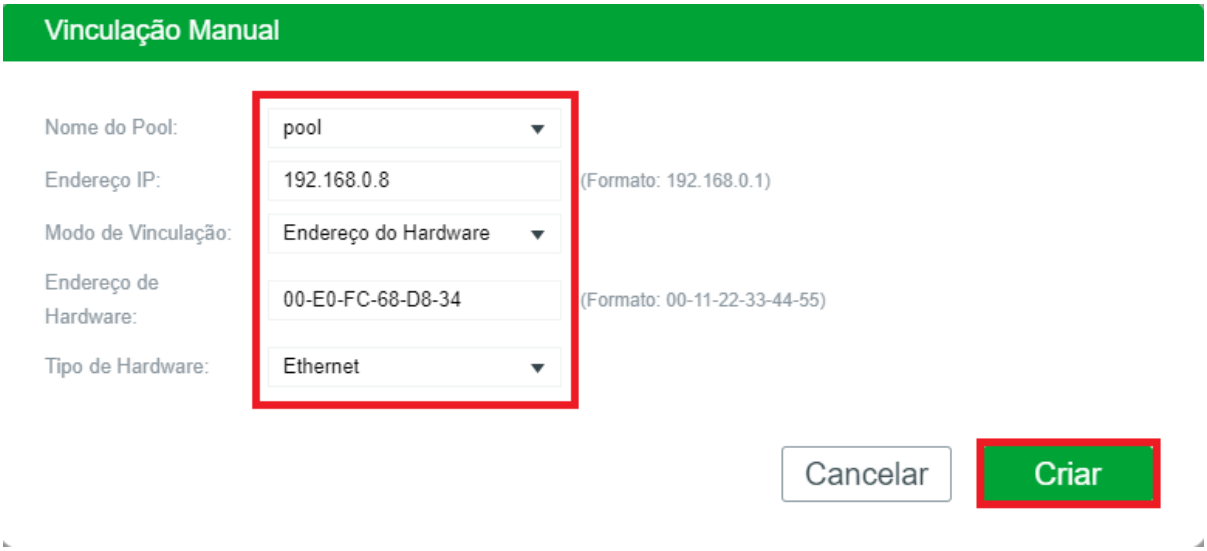
1. Vá até o menu **FUNÇÕES L3 > Serviço DHCP > DHCP Server > DHCP Server** para carregar a página a seguir. Na seção **Configuração Global**, habilite o Servidor DHCP.

2. Vá até o menu **FUNÇÕES L3 > Serviço DHCP > DHCP Server > Configuração de Pool** clique em Adicionar para carregar a página a seguir. Especifique o nome do pool, endereço de Rede, máscara de sub-rede, Lease Time, gateway padrão e servidor DNS como mostrado a baixo. Clique em **Criar**.



3. Vá até o menu **FUNÇÕES L3 > Serviço DHCP > DHCP Server > Vinculo Manual** clique em Adicionar para carregar a página a seguir. Selecione o nome do pool que você acabou de criar e entre com o endereço IP que o servidor FTP

terá no campo de endereço IP. Selecione Endereço de Hardware como modo de Vinculação, entre com o endereço MAC do servidor FTP no campo Endereço de Hardware. Selecione Ethernet como tipo de hardware. Clique em **Criar**.



4. Clique em Salvar para salvar as configurações.

Exemplo de Interface DHCP Relay

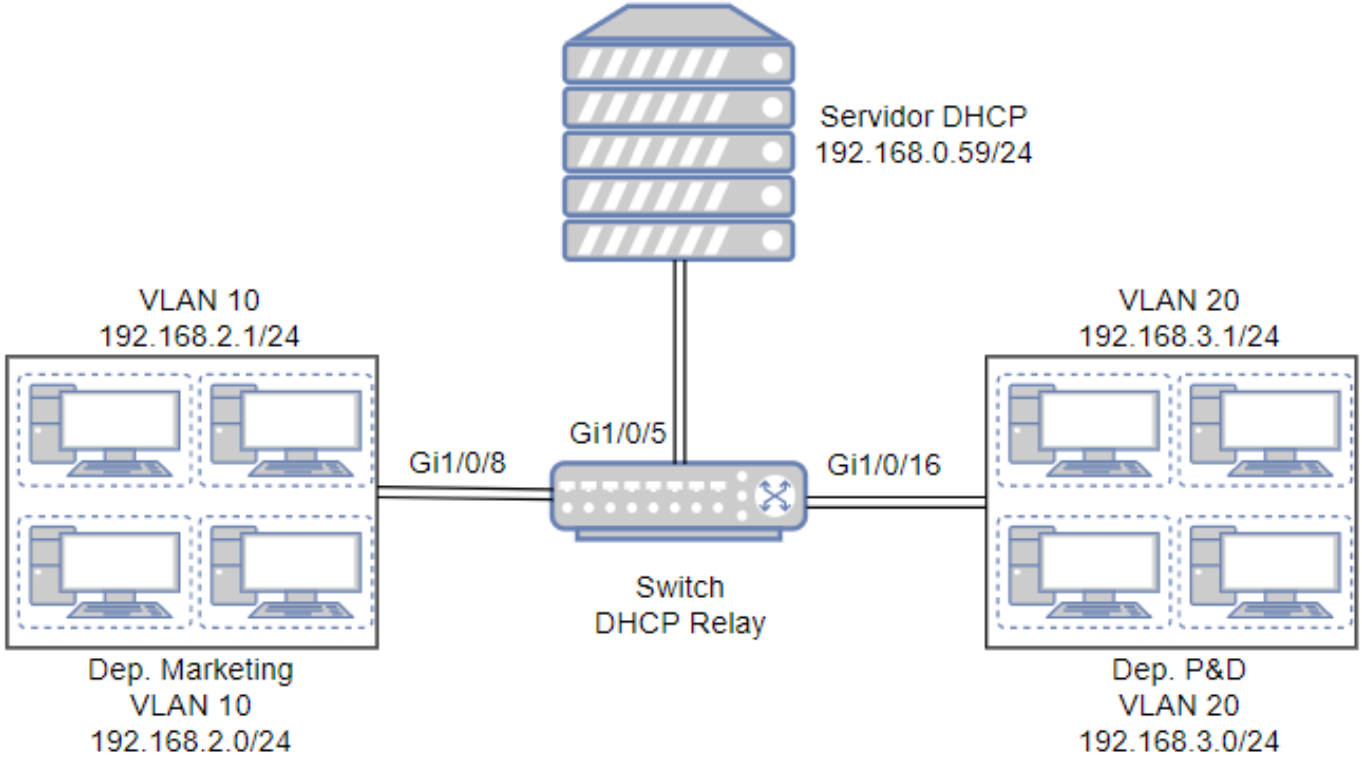
Requisitos de Rede

Uma companhia pretende atribuir endereços IP para todos os computadores em dois departamentos, e só há um servidor DHCP disponível. Por requisito os computadores do mesmo departamento devem estar na mesma sub-rede, enquanto computadores em diferentes departamentos devem estar em sub-rede diferentes.

Configurando o Cenário

Na situação proposta, a função de DHCP Relay pode satisfazer os requisitos porque DHCP Relay possibilita que clientes em diferentes sub-rede compartilhem o mesmo servidor. Garanta que o seu Servidor dê suporte à mais que uma Pool de endereços DHCP.

A topologia de rede é como mostrada na figura a baixo. Computadores no departamento de marketing pertencem à VLAN 10 a qual está conectada ao switch através da porta 1/0/8. O endereço da interface da VLAN 10 é 192.168.2.1/24. Computadores no departamento de P&D pertencem à VLAN 20 a qual está conectada no switch através da porta 1/0/16. O endereço da interface da VLAN 20 é 192.168.3.1/24. O servidor DHCP está conectado ao switch DHCP Relay através da port 1/0/5, e seu endereço de IP é 192.168.0.59/24.



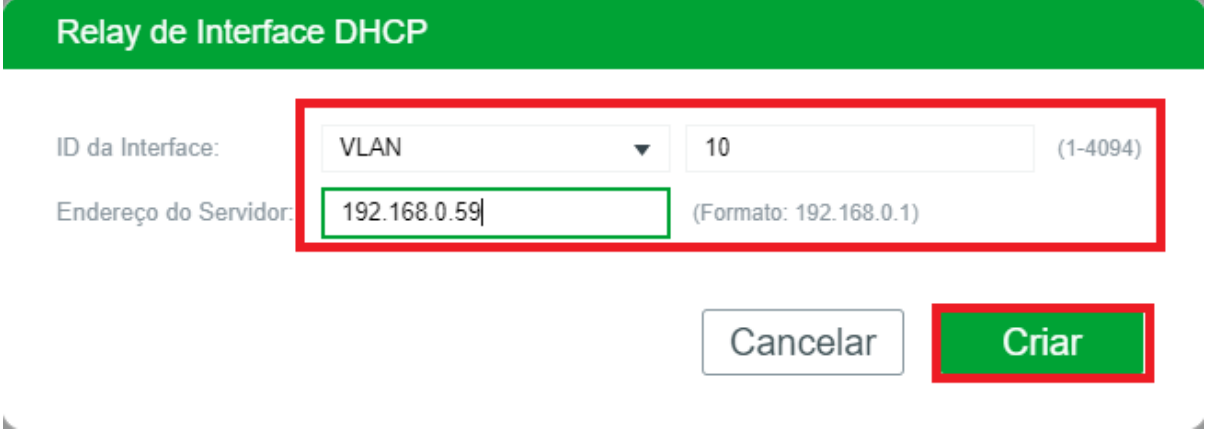
A visão geral das configurações são as seguintes:

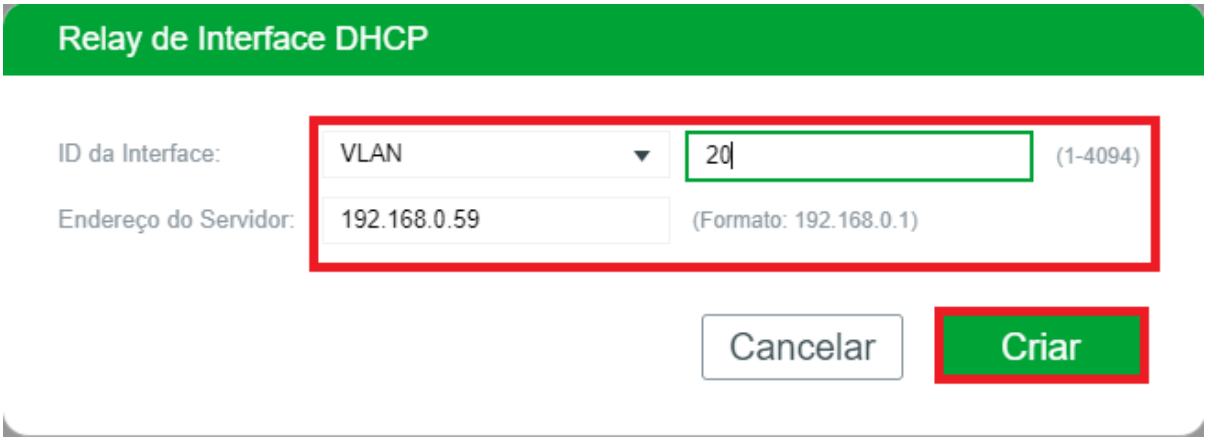
1. Antes de configurar o DHCP Relay, crie duas Pools de IP DHCP no servidor DHCP, uma para a rede 192.168.2.0/24 e a outra para a rede 192.168.3.0/24. Então crie rotas estáticas ou habilite um protocolo de roteamento dinâmico como o RIP no servidor DHCP para garantir que o servidor possa alcançar as duas redes.
2. Configure VLAN 802.1Q. Adicione todos os computadores do departamento do marketing à VLAN 10, e adicione todos os computadores do departamento de P&D à VLAN 20. Para mais detalhes vá até Configuração da VLAN 802.1Q.
3. Configure os endereços das interfaces das VLANs. Para mais detalhes vá até Configurando interfaces de camada 3.
4. Configure o DHCP Relay no switch. Habilite o DHCP Relay e adicione o endereço do servidor DHCP para cada VLAN. Após finalizar essas configurações o servidor DHCP conseguirá atribuir endereços IP para os computadores nos dois departamentos os quais estão em diferentes sub-rede.

Siga os seguintes passos para configurar DHCP Relay:

1. Vá até o menu **FUNÇÕES L3 > Serviço DHCP > DHCP Relay > Configuração de DHCP Relay** para carregar a página a seguir. Na seção **Configuração Global** habilite o DHCP Relay e então clique em **Aplicar**.

2. Vá até o menu **FUNÇÕES L3 > Serviço DHCP > DHCP Relay > Interface DHCP Relay** clique em Adicionar para carregar a página a seguir. Especifique o endereço IP do servidor DHCP para atribuir endereços IP para os clientes nas VLANs 10 e 20.





3. Clique em Salvar para salvar as configurações

Apêndice: Configuração Padrão

As Configurações Padrão do DHCP Server estão listadas na tabela a baixo.

Configuração Padrão do Servidor DHCP

Parâmetros	Configurações Padrão
Configuração Global	
DHCP Server	Ativado
Option 60	Nenhum
Option 138	Nenhum
Configuração de Tempo de ping	
Pacotes de Ping	1
Timeout de Ping	100 ms
Endereço de IP Excluído	
Endereço IP de Início	Nenhum
Endereço IP final	Nenhum
Configurações de Pool	
Nome de Pool	Nenhum

Endereço de Rede	Nenhum
Máscara de Sub-rede	Nenhum
Horário de Lease	120 min
Gateway padrão	Nenhum
Servidor DNS	Nenhum
Servidor NetBIOS	Nenhum
Tipo de nó NetBIOS	Nenhum
Endereço do Próximo Servidor	Nenhum
Nome de Domínio	Nenhum
Bootfile	Nenhum
Vinculo Manual	
Nome do Pool	Nenhum
Endereço IP	Nenhum
Modo de Vinculação	ID do cliente
ID do Cliente	Nenhum
Endereço de Hardware	Nenhum
Tipo de Hardware	Ethernet

As configurações Padrão do DHCP Relay estão listadas a tabela a baixo.

Configuração Padrão de DHCP Relay

Parâmetros	**Configurações Padrão**
DHCP Relay	
DHCP Relay	Desabilitado
DHCP Relay Hops	4
Threshold de Tempo de DHCP Relay	0
Configuração da Option 82	
Suporte a Option 82	Desabilitado
Política da Option 82	Manter
Formato	Normal
Customização de Circuit-ID	Desabilitado
Circuit-ID	Nenhum
Customização de ID Remoto	Desabilitado
ID Remoto	Nenhum
Interface DHCP Relay	
ID da Interface	Nenhum

Endereço do Servidor	Nenhum
VLAN DHCP Relay	
ID da interface	Nenhum
ID da VLAN	Nenhum
Endereço do Servidor	Nenhum

As configurações Padrão do DHCP L2 Relay estão listadas a tabela a baixo.

Configuração Padrão de DHCP L2 Relay

Parâmetros	**Configurações Padrão**
Configuração Global	
DHCP Relay	Desabilitado
Estado da VLAN	Desabilitado
Configuração de Porta	
Suporte a Option 82	Desabilitado
Política da Option 82	Manter
Formato	Normal
Customização de Circuit-ID	Desabilitado
Circuit-ID	Nenhum
Customização de ID Remoto	Desabilitado
ID Remoto	Nenhum

ARP

Visão Geral

O Protocolo de resolução de endereços (ARP) é usado para mapear endereços IP para endereços MAC. Tomando um endereço IP como entrada, o ARP aprende o endereço MAC associado e armazena o IP-MAC associação de endereço em uma entrada ARP para recuperação rápida.

Funções Suportadas

ARP Table

A tabela ARP exibe todas as entradas ARP, incluindo entradas dinâmicas e entradas estáticas.

Entrada dinâmica: aprendido automaticamente e será excluído após o tempo de envelhecimento.

Entrada estática: adicionado manualmente e será mantido a menos que modificado ou excluído manualmente.

Static ARP

Você pode adicionar manualmente entradas ARP especificando os endereços IP e endereços MAC.

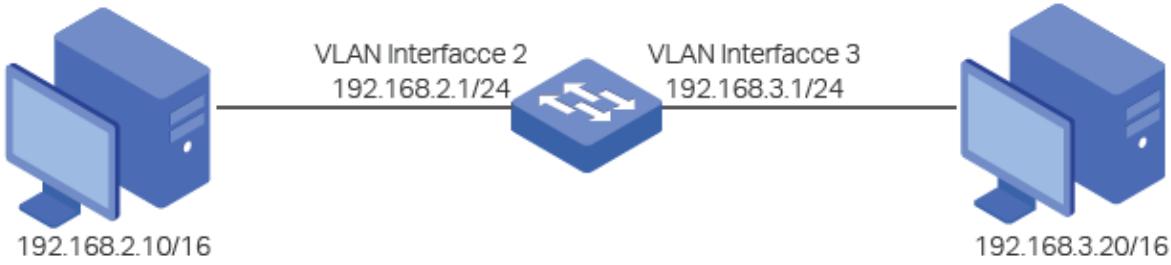
Gratuitous ARP

O Gratuitous ARP é um tipo especial de ARP. Tanto os endereços de origem quanto de destino do ARP em pacotes gratuitous ARP são o remetente seu próprio endereço IP. Ele é usado para detectar endereços IPs duplicados. Se uma interface enviar um pacote gratuitous ARP e nenhuma resposta for recebida, então o remetente sabe que seu endereço IP não é usado por outros dispositivos.

Proxy ARP

Normalmente, os pacotes ARP só podem ser transmitidos em um domínio broadcast, o que significa que se dois dispositivos no mesmo segmento de rede estiverem ligados a interfaces de Camada 3 diferentes, não podem comunicar uns com os outros porque não podem aprender o MAC um do outro usando pacotes ARP.

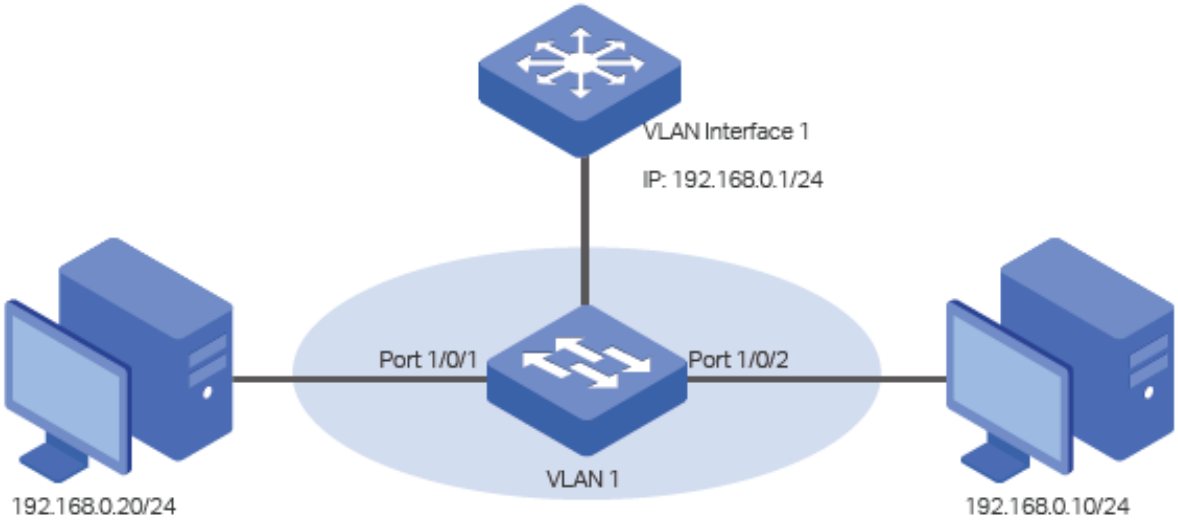
Proxy ARP resolve este problema. Como mostrado abaixo, quando uma máquina envia uma requisição ARP para outro dispositivo que não esteja no mesmo domínio broadcast, mas na mesma rede a interface da Camada 3 com o ARP Proxy habilitado responderá à solicitação de ARP com o seu próprio endereço MAC, se o IP de destino estiver acessível. Depois disso, o remetente da solicitação ARP envia pacotes para o switch, e o switch encaminha os pacotes para o dispositivo pretendido.



Local Proxy ARP

O Local Proxy ARP é semelhante ao Proxy ARP. Como mostrado abaixo, duas máquinas estão na mesma VLAN e ligadas à interface VLAN 1, mas a porta 1/0/1 e a porta 1/0/2 estão isoladas na camada 2. Neste caso, ambas as máquinas não podem receber o pedido ARP uma da outra. Portanto, eles não podem comunicam uns com os outros porque não conseguem aprender o endereço MAC uns dos outros usando Pacotes ARP.

Para resolver este problema, você pode habilitar o Local Proxy ARP na interface da Camada 3 e a interface responderá ao remetente do pedido ARP com seu próprio endereço MAC. Depois disso, o remetente da solicitação ARP envia pacotes para a interface da Camada 3, e a interface encaminha o pacote para o dispositivo pretendido.



Configurações ARP

Com as configurações ARP você pode:

- Visualizar as entradas dinâmicas na tabela ARP.
- Adicionar ou remover entradas estáticas na tabela ARP.

Para configurar o recurso Gratuitous ARP:

- Configure o Gratuitous ARP de forma global e defina o intervalo de envio do Gratuitous ARP.

Para configurar o recurso Proxy ARP:

- Habilite a função Proxy para as interfaces VLAN ou portas roteadas.

Visualizando entradas ARP

A tabela ARP consiste de dois tipos de entradas ARP: dinâmicas e estáticas.

- Entradas dinâmicas: Automaticamente aprendidas, sendo automaticamente excluídas após o tempo de envelhecimento.
- Entradas estáticas: Adicionada manualmente e permanecerá a menos que seja modificada ou excluída manualmente.

Escolha o menu FUNÇÕES L3 > ARP > Tabela ARP para carregar a seguinte página.

Atualizar

Interface	Endereço IP	Endereço MAC	Tipo
VLAN1	192.168.0.22	50-3e-aa-20-93-00	Dinâmico

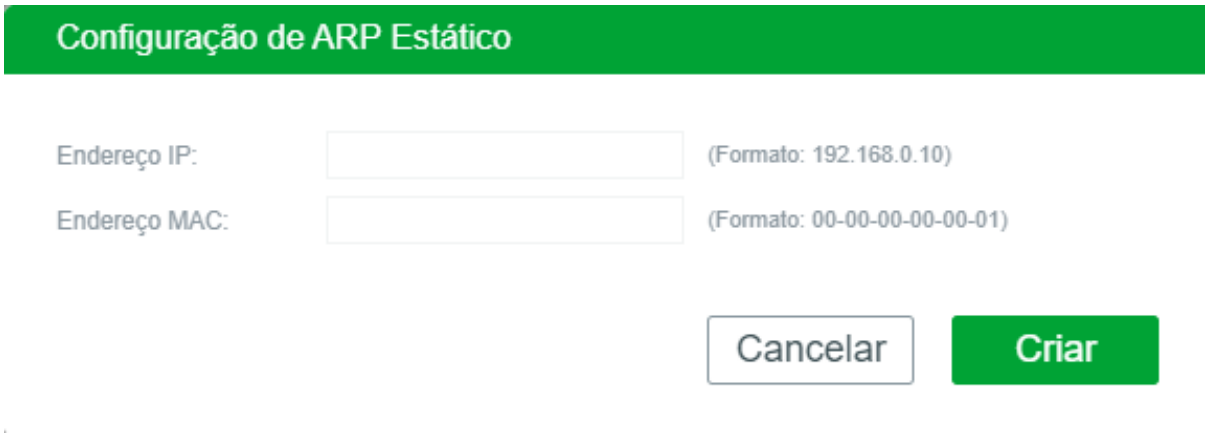
Total: 1

Interface	Exibe a interface de rede de uma entrada ARP.
Endereço IP	Exibe o endereço IP de uma entrada ARP.
Endereço MAC	Exibe o endereço MAC de uma entrada ARP.
Tipo	Exibe o tipo de uma entrada ARP. **Estática:** a entrada é adicionada manualmente e sempre permanecerá a mesma. **Dinâmica:** a entrada que será excluída após o tempo de validade concedido. O valor padrão do tempo de envelhecimento é 600 segundos. Se você deseja alterar o tempo de envelhecimento, pode usar a CLI para configurá-lo.

Adicionando Entradas ARP Estáticas Manualmente

Você pode adicionar entradas estáticas ARP desejadas especificando manualmente os endereços IP e endereços MAC.

Escolha o menu **FUNÇÕES L3 > ARP > ARP Estático** e clique em Adicionar para carregar a seguinte página.

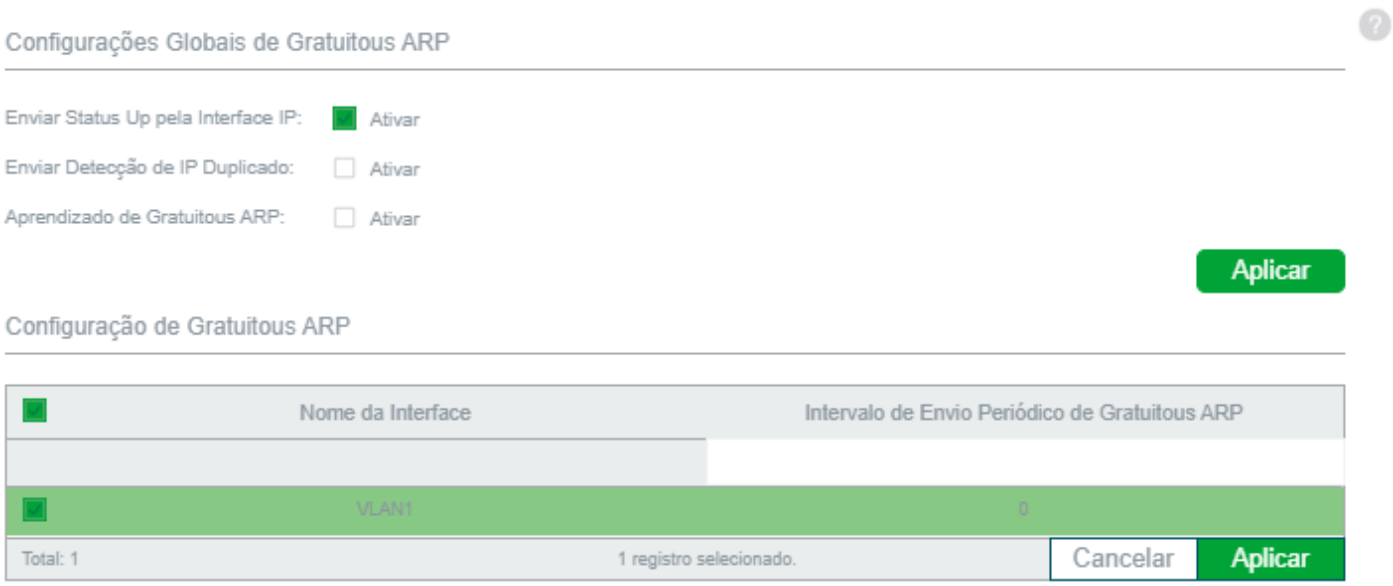


Digite o endereço IP e o endereço MAC, clique em **Criar**.

Endereço IP	Especifique o endereço IP da entrada ARP estática.
Endereço MAC	Especifique o endereço MAC da entrada ARP estática.

Gratuitous ARP

Escolha o menu **FUNÇÕES L3 > ARP > Gratuitous ARP** para carregar a seguinte página.



Siga os seguintes passos para configurar o Gratuitous ARP em uma interface.

1. Na seção **Configurações Globais do Gratuitous ARP**, configure os parâmetros globais para o Gratuitous ARP. Depois clique em **Aplicar**.

Enviar Status Up pela Interface IP	Com essa opção ativada, a interface enviará pacotes de solicitação gratuitous ARP quando seu status ficar ativo. Isso é usado para anunciar o endereço IP da interface para os outros hosts. Está ativado por padrão.
Enviar Detecção de IP Duplicado	Com esta opção ativada, a interface enviará pacotes de solicitação gratuitous ARP quando um pacote de solicitação gratuitous ARP for recebido para o qual o endereço IP é o mesmo que o da interface. Nesse caso, o switch sabe que outro host está usando o mesmo endereço IP que o seu. Para reivindicar o endereço IP para o proprietário correto, a interface envia pacotes gratuitous ARP. É desativado por padrão.
Aprendizado de Gratuitous ARP	Normalmente, o switch atualiza apenas a tabela de endereços MAC aprendidos com o pacote de resposta ARP ou o pacote de solicitação ARP normal. Com essa opção ativada, o switch também atualizará a tabela de endereços MAC aprendendo com os pacotes gratuitous ARP recebidos. É desativado por padrão

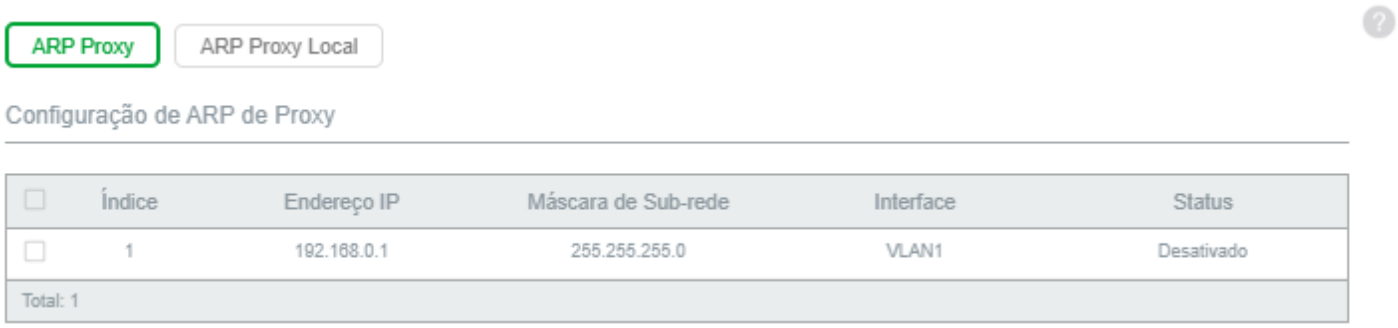
2. Na seção **Configuração de Gratuitous ARP**, configure os parâmetros globais para o gratuitous ARP. Depois clique em **Aplicar**.

Nome da Interface	Exibe o Identificador das interfaces de camada 3.
Intervalo de Envio Periódico de Gratuitous ARP	Especifique o intervalo de envio dos pacotes de requisição gratuitous ARP da interface. O valor 0 significa que a interface não enviará pacotes de solicitação gratuitous ARP periodicamente.

Configurando o ARP Proxy

O ARP Proxy é usado na situação em que dois dispositivos estão no mesmo segmento de rede, mas conectados a diferentes interfaces da camada 3.

Escolha o menu **FUNÇÕES L3 > ARP > ARP Proxy > ARP Proxy** para carregar a seguinte página.



Selecione a interface desejada e ative o ARP Proxy. Depois clique em **Aplicar**.

Endereço IP	Exibe o endereço IP da interface de camada 3.
Máscara de Sub-rede	Exibe a máscara da sub-rede do endereço IP.
Status	Habilite o recurso ARP Proxy na interface. A interface responderá ao remetente da solicitação ARP com seu próprio endereço MAC.

Configurando o ARP Proxy Local

O ARP Proxy Local é usado na situação em que dois dispositivos estão na mesma VLAN, mas isolados nas portas da camada 2.

Escolha o menu **FUNÇÕES L3 > ARP > ARP Proxy > ARP Proxy Local** para carregar a seguinte página.

Selecione a interface desejada e ative o ARP Proxy Local. Depois clique em **Aplicar**.

Endereço IP	Exibe o endereço IP da interface de camada 3.

Máscara de Sub-rede	Exibe a máscara da sub-rede do endereço IP.
Status	Habilite o recurso ARP Proxy na interface. A interface responderá ao remetente da solicitação ARP com seu próprio endereço MAC.

Apêndice: Configuração Padrão

As Configurações Padrão do ARP estão listadas na tabela a baixo.

Configuração Padrão ARP

Parâmetros	**Configurações Padrão**
Enviar Status Up pela Interface IP	Habilitado
Enviar Detecção de IP Duplicado	Desabilitado
Aprendizado de Gratuitous ARP	Desabilitado
Intervalo de Envio Periódico de Gratuitous ARP	0 segundos

QoS

Visão Geral

Com a expansão da escala da rede e o desenvolvimento de aplicativos, o tráfego da Internet aumenta drasticamente, resultando em congestionamento da rede, queda de pacotes e longo atraso na transmissão. Normalmente, as redes tratam todo o tráfego igualmente com base na entrega FIFO (primeiro a entrar, primeiro a sair), mas hoje em dia muitos aplicativos especiais, como VoD, videoconferências, VoIP, etc., exigem mais largura de banda ou menor atraso na transmissão para garantir o desempenho.

Com a tecnologia de QoS (Quality of Service), você pode classificar e priorizar o trafego da rede provendo serviços diferenciados para certos tipos de tráfego.

Funções Suportadas

Você pode configurar as funções de classe de servido, controle de largura de banda, VLAN de voz e Auto VoIP no switch para maximizar a performance da rede.

Classe de Serviço

O switch classifica os pacotes que estão chegando mapeando-os em diferentes filas de prioridade para então encaminha-los de acordo com as configurações específicas do agendados para implementar a função de QoS.

- Modo Prioridade: três modos são suportados são eles: Prioridade de Porta, Prioridade 802.1p e prioridade DSCP.
- Modo Agendador: dois tipos de agendador são suportados, Strict e Weighted.

Controle de Largura de Banda

Controle de largura de banda funciona para controlar a taxa e o limite de tráfego para cada porta para garantir a performance da rede.

- A Função de limite de taxa serve para limitar a taxa de tráfego de entrada e saída de cada porta. Dessa forma, a largura de banda da rede pode ser razoavelmente distribuída e utilizada.
- A função de Storm control permite que o switch monitore pacotes broadcast, Multicast e Quadros UL (Unknow Unicast Frames) na rede. Se a taxa de transmissão exceder o limite configurado, os pacotes serão automaticamente descartados para evitar uma Broadcast Storm na rede.

VLAN Voz e Auto VoIP

As funções de VLAN de Voz e Auto VoIP são utilizadas para priorizar a transmissão de tráfego de voz. Tráfego de voz é tipicamente mais sensível ao tempo que os outros dados em tráfego, e a qualidade da voz pode se deteriorar muito devida à perda de pacotes e o atraso da transmissão. Para garantir uma alta qualidade de voz você pode configurar VLAN de Voz ou Auto VoIP.

Essas duas funções podem ser habilitadas em portas que transmitem somente dados de voz ou que transmitem tráfego de voz e dados. VLAN de Voz pode alterar a prioridade 802.1p do pacote de voz e transmitir o pacote em uma VLAN desejada. Auto VoIP pode informar os dispositivos de voz para encaminharem pacotes com configuração especifica para trabalhar com a função LLDP-MED.

Configuração de Classe de Serviço

Com as configurações de classe de servido você pode:

- Configurar a prioridade da porta.
- Configurar a prioridade 802.1p.
- Configurar a prioridade DSCP.
- Especificar as configurações do agendador.

Diretrizes de configuração

Selecione o modo de prioridade que se encarregará das portas de acordo com os requisitos da sua rede.

Uma porta pode utilizar somente uma classificação de prioridade para os pacotes recebidos. Três modos de prioridade são suportados pelo switch: Prioridade de Porta, Prioridade 802.1p e Prioridade DSCP.

- Prioridade de Porta

  Nesse modo, o switch prioriza os pacotes de acordo com o recebimento nas portas, independentemente dos campos do pacote ou tipo.

- Prioridade 802.1p

  802.1p define os três primeiros bits do Tag 802.1Q como campo de prioridade (PRI Field). Os valores de PRI variam entre 0 e 7. Prioridade 802.1P determina a prioridade baseada nos valores PRI.

  Nesse modo o switch priorizará somente pacotes com tag de VLAN, independentemente do cabeçalho IP dos pacotes.

- Prioridade DSCP

  Prioridade DSCP determina a prioridade dos pacotes baseada no campo ToS (Type of Service) no cabeçalho IP. RFC2474 redefine o campo ToS nos cabeçalhos IP dos pacotes como campos DS. Os primeiros seis bits (bit 0 ao bit 5) do campo DS são utilizados para representar a prioridade DSCP. Os valores DSCP variam entre 0 e 63.

  Nesse modo o switch prioriza somente pacotes IP.

Especifique o mapeamento das filas 802.1p de acordo com a sua necessidade.

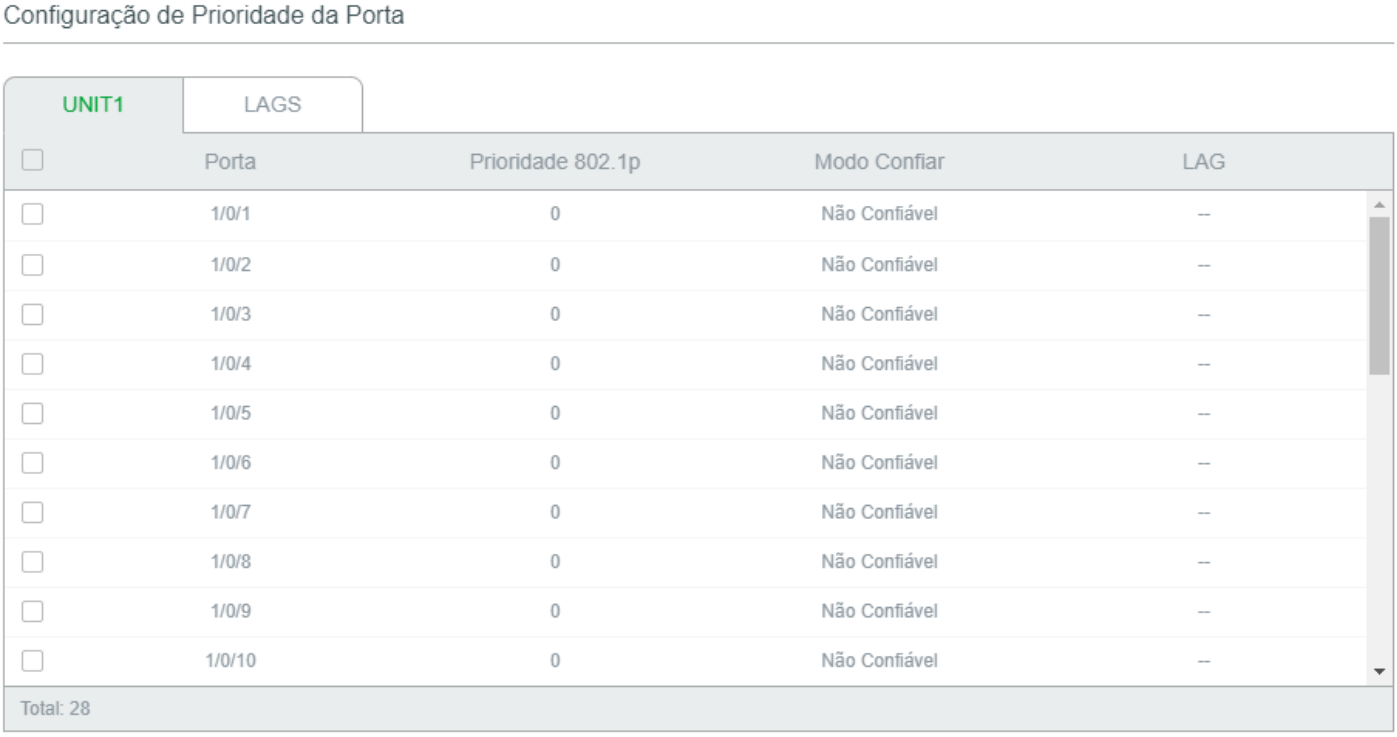
Para a prioridade 802.1p os pacotes serão encaminhados conforme o mapeamento das filas 802.1p.

Para Prioridade de Porta e Prioridade DSCP elas serão primeiramente mapeadas na prioridade 802.1p e então mapeadas de acordo com o mapeamento das filas 802.1p.

Configurando Prioridade de Porta

Configurando o Modo Confiar e o Mapeamento das Portas 802.1p

Vá até o menu **QoS > Classe de Servido > Prioridade da Porta** para carregar a página a seguir.



Siga os seguintes passos para configurar os parâmetros para a prioridade de portas.

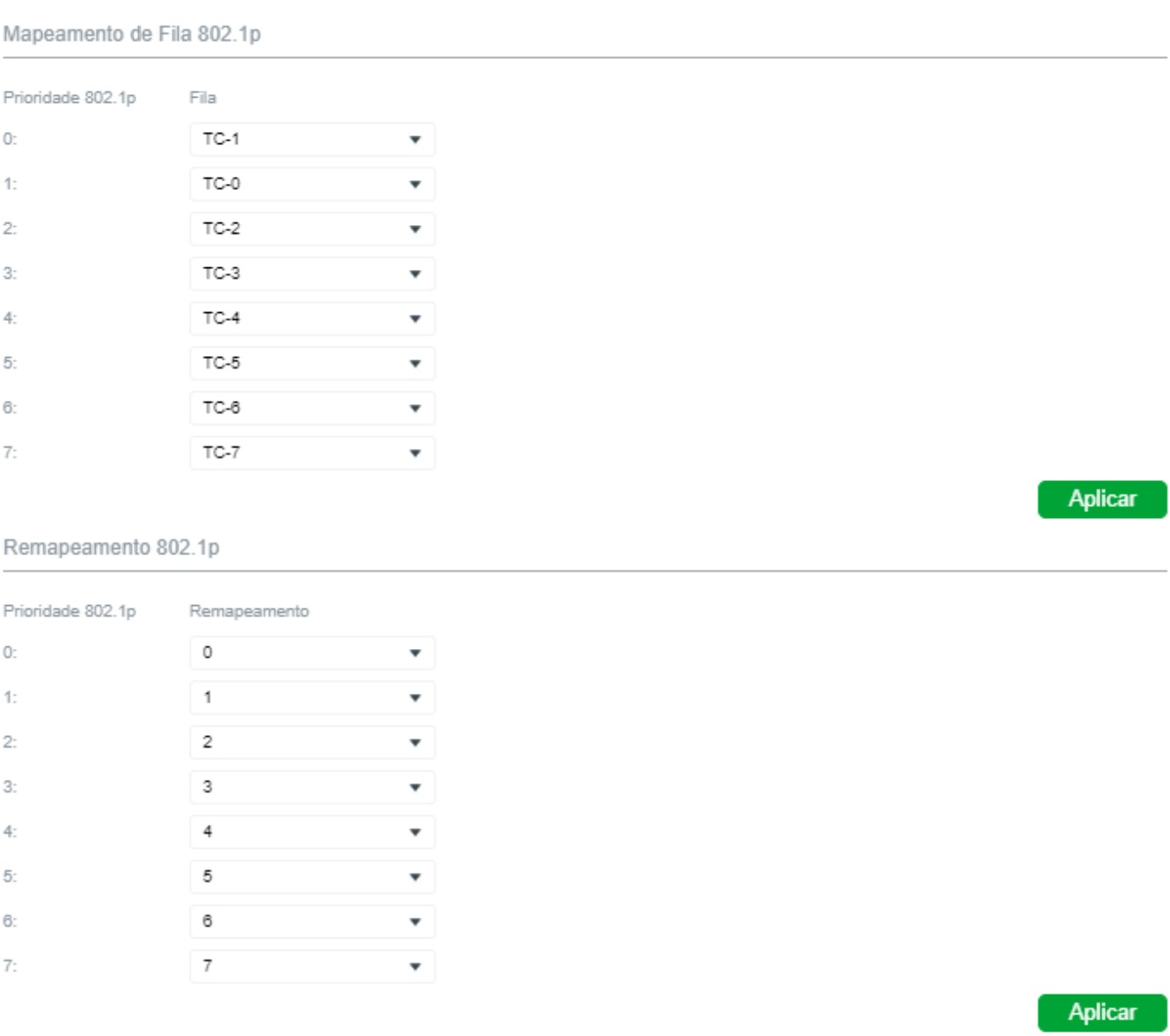
1. Selecione as portas desejadas, especifique a prioridade 802.1p e o Modo Confiar como Não Confiável.

Prioridade 802.1p	Especifique o mapeamento 802.1p para a porta desejada. Os pacotes recebidos por uma porta são primeiramente mapeados na prioridade 802.1p baseada no mapeamento 802.1p para portas, então para as filas TC baseadas no mapeamento de filas configurados pelo 802.1p. Os pacotes untagged de uma porta serão adicionados em um valor de prioridade 802.1p de acordo com o mapeamento de portas da prioridade 802.1p.
Modo Confiar	Selecione o Modo Confiar como Não confiável. Nesse modo os pacotes serão processados de acordo com a configuração de prioridade de porta.

2. Clique em **Aplicar**.

Configurando o 802.1p para mapeamento de fila

Vá até o menu **QoS > Classe de Serviço > Prioridade 802.1p** para carregar a página a seguir.



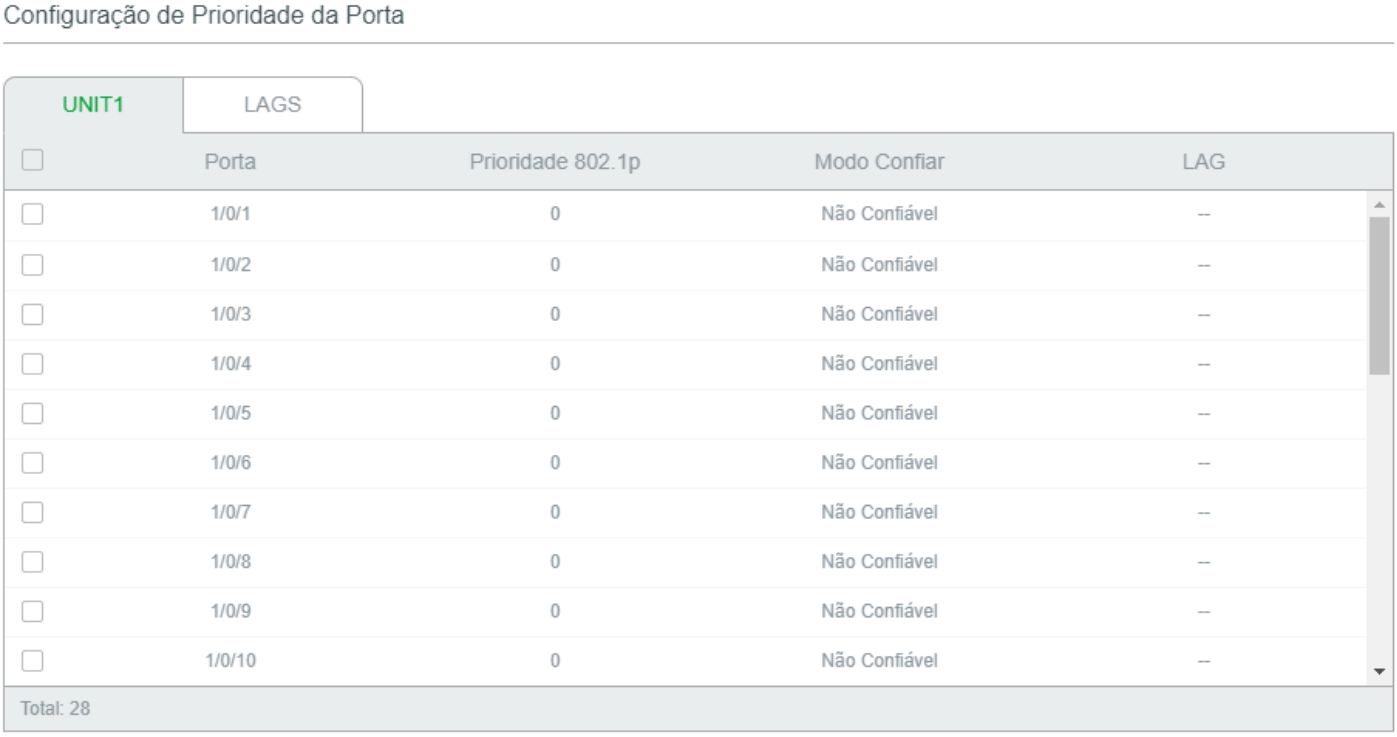
Na seção **Mapeamento de fila 802.1p** configure o mapeamento e clique em **Aplicar**.

Prioridade 802.1p	Mostra o número da prioridade 802.1p. No QoS a prioridade 802.1p é utilizada para representar a classe de serviço.
Fila	Selecione a fila TC para a prioridade 802.1p desejada. Os pacotes com a prioridade 802.1p desejada serão colocados nas filas correspondentes.

Configurando Prioridade 802.1p

Configurando o Modo Confiar

Vá até o menu **QoS > Classe de Serviço > Prioridade da Porta** para carregar a página a seguir.



Siga os seguintes passos para configurar o Modo Confiar:

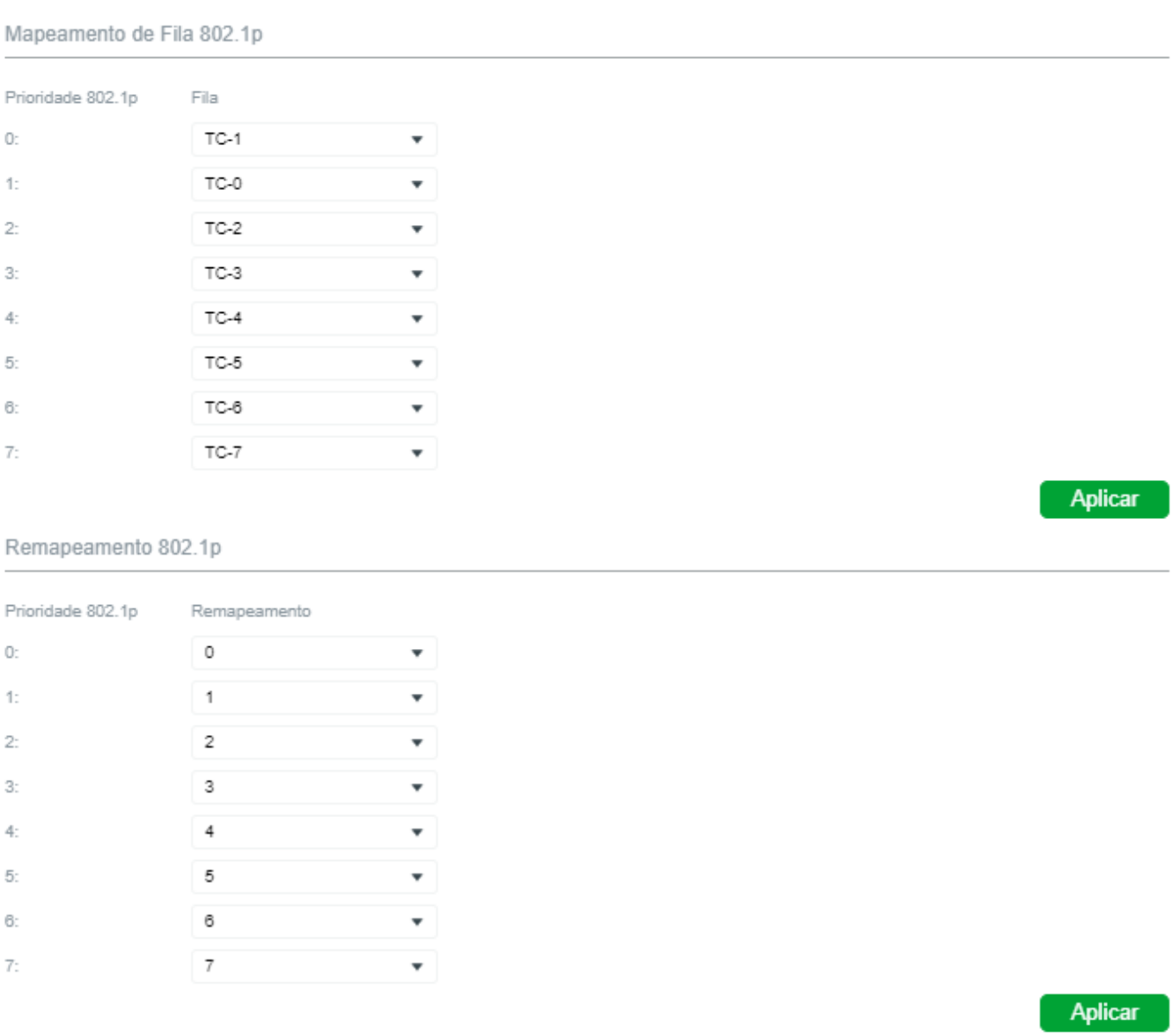
1. Selecione as portas desejadas e determine o modo confiar como Confiar 802.1p.

Modo Confiar	Selecione o modo confiar como confiar 802.1p. Nesse modo os pacotes tagged serão processados de acordo com a configuração da prioridade 802.1p e os pacotes untagged serão processados de acordo com a configuração de prioridade de porta.

2. Clique em **Aplicar**.

Configurando Mapeamento de Fila 802.1p e Remapeamento 802.1p

Vá até o menu **QoS > Classe de Serviço > Prioridade 802.1p** para carregar a página a seguir.



Siga os seguintes passos para configurar os parâmetros da prioridade 802.1p:

1. Na seção **802.1p Aguardar Mapeamento** configure o mapeamento e clique em **Aplicar**.

Prioridade 802.1p	Mostra o número da prioridade 802.1p. No QoS a prioridade 802.1p é utilizada para representar a classe de serviço. O padrão IEEE 802.1p define os três bits na tag 802.1Q como campo PRI. Os valores PRI são chamados prioridade 802.1p e são usados para representar a prioridade dos pacotes de camada 2. Essa função requer pacotes com tag VLAN.
Fila	Selecione a fila TC para a prioridade 802.1p desejada. Os pacotes com a prioridade 802.1p desejada serão colocados nas filas correspondentes.

2. (Opcional) Na seção **Remapemanto 802.1p** configure o mapeamento de 802.1p para 802.1p e clique em **Aplicar**.

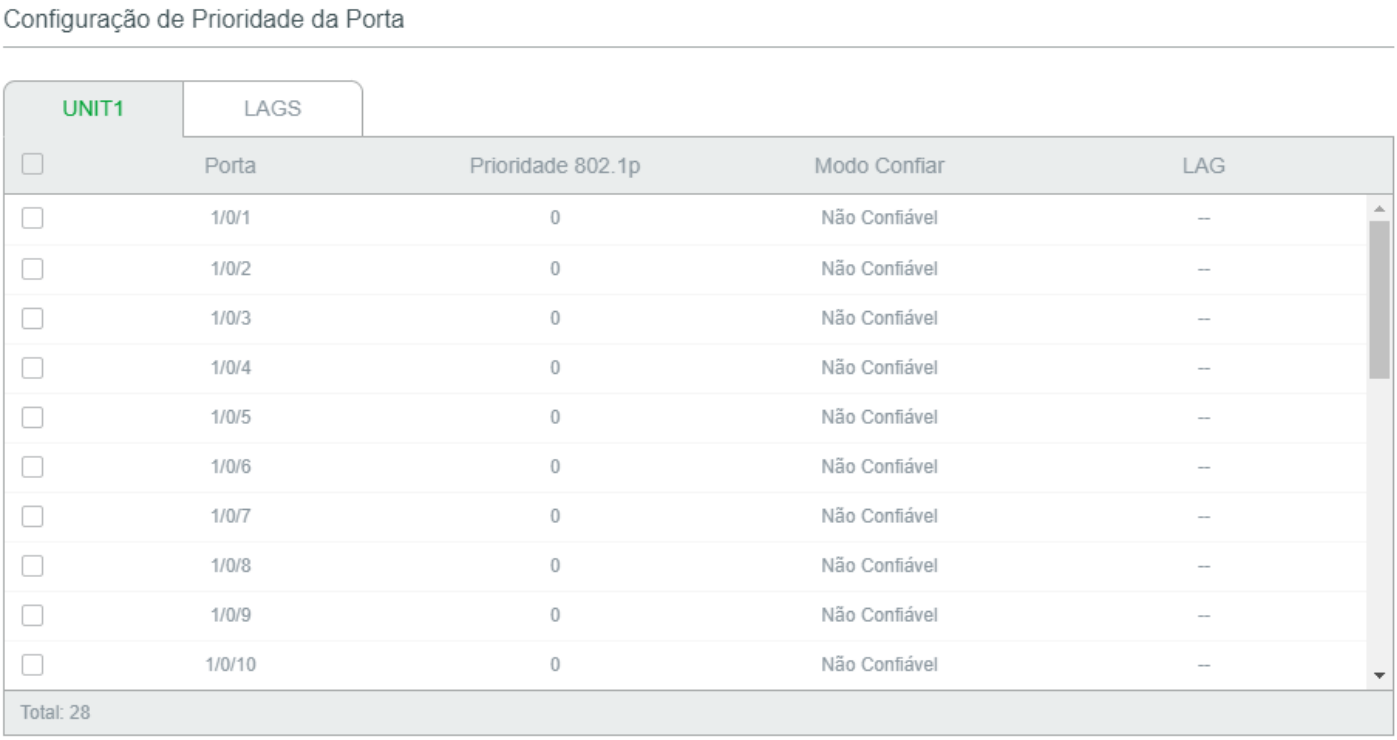
Prioridade 802.1p	Mostra o número da prioridade 802.1p. No QoS a prioridade 802.1p é utilizada para representar a classe de serviço. O padrão IEEE 802.1p define os três bits na tag 802.1Q como campo PRI. Os valores PRI são chamados prioridade 802.1p e são usados para representar a prioridade dos pacotes de camada 2. Essa função requer pacotes com tag VLAN.
Remap	Selecione um número de prioridade 802.1p a qual a prioridade original 802.1p será remapeada. 802.1p Remap é utilizado para modificar a prioridade 802.1p dos pacotes recebidos. Quando o switch detecta os pacotes com a prioridade 802.1p desejada ele irá modificar o valor da prioridade 802.1p de acordo com o mapa.

No modo Confiar 802.1p pacotes untagged serão adicionados a uma prioridade 802.1p baseada em porta para um mapeamento 802.1p e será encaminhada de acordo com o mapeamento das filas 802.1p.

Configurando Prioridade DSCP

Configurando Modo Confiar

Vá até o menu **QoS > Classe de Serviço > Prioridade de Porta** para carregar a página a seguir.



Siga os seguintes passos para configurar o Modo Confiar:

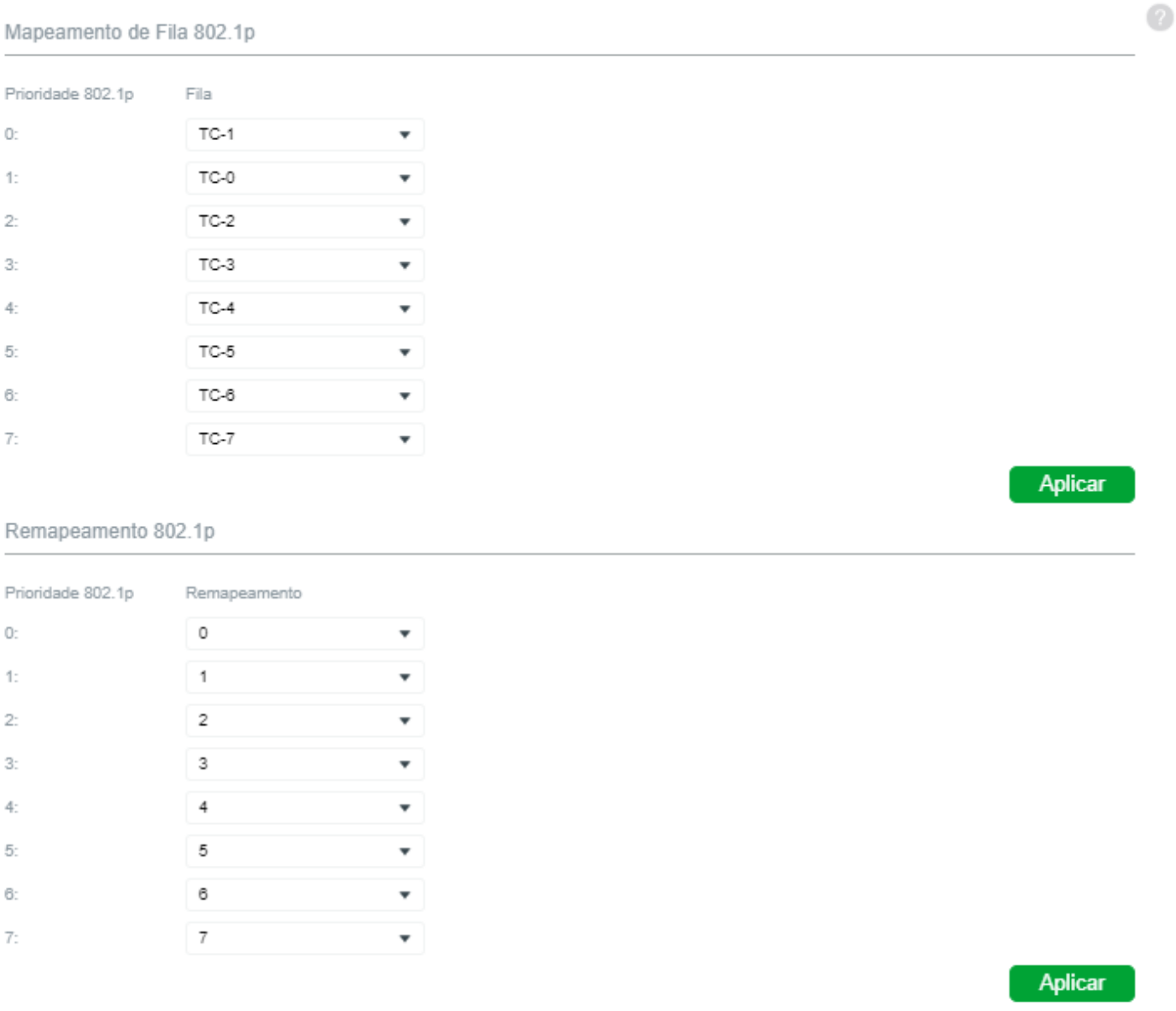
1. Selecione as portas desejadas e configure o Modo Confiar como Confiar DSCP.

Modo Confiar	Selecione o Modo Confiar como Confiar DSCP. Nesse modo os pacotes IP serão processados de acordo com a configuração da prioridade DSCP e os pacotes não IP serão processados de acordo com a configuração de prioridade de porta.

2. Clique em **Aplicar**.

Configurando Mapeamento de Fila 802.1p

Vá até o menu **QoS > Classe de Serviço > Prioridade 802.1p** para carregar a página a seguir.

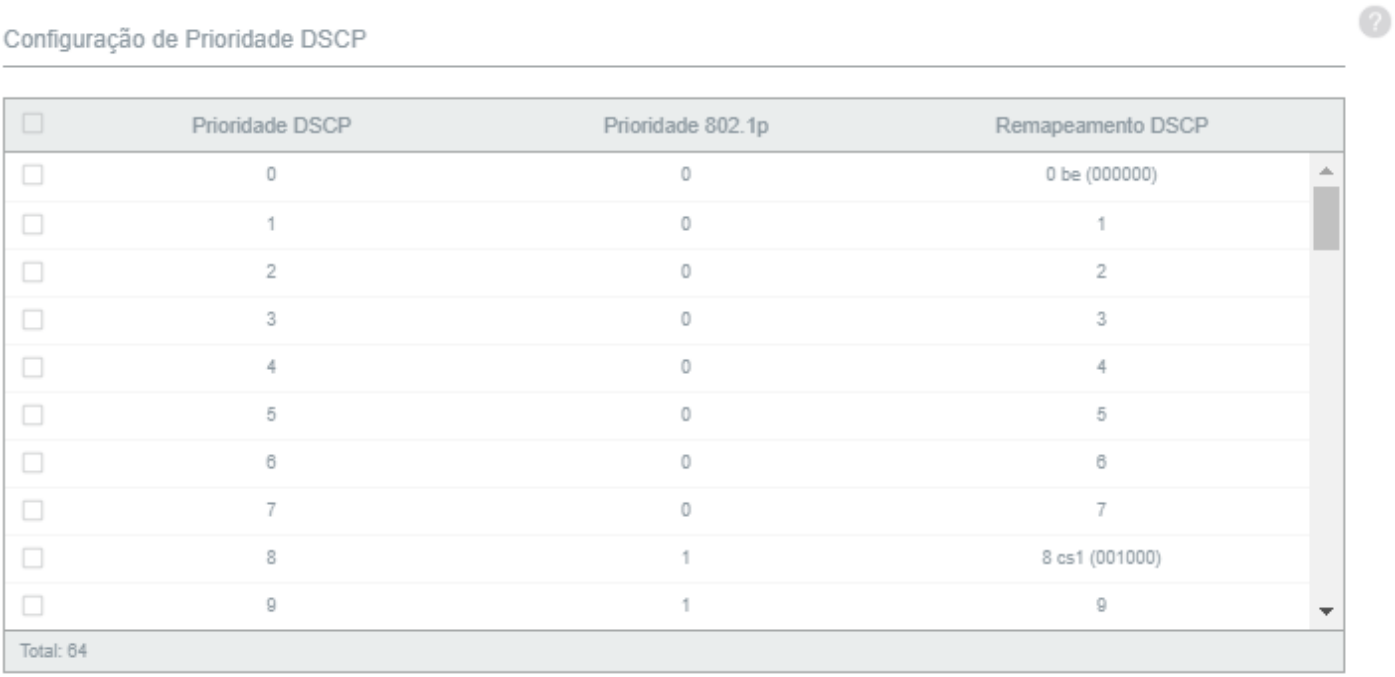


Na seção **Mapeamento de Fila 802.1p** configure os mapeamentos e clique em **Aplicar**.

Prioridade 802.1p	Mostra o número da prioridade 802.1p. No QoS a prioridade 802.1p é utilizada para representar a classe de serviço.
Fila	Selecione a fila TC par aa prioridade 802.1p desejada. Os pacotes com a prioridade 802.1p desejada serão colocados na fila correspondente.

Configurando Mapeamento DSCP para 802.1p e o Remapeamento DSCP

Vá até o menu **QoS > Classe de Serviço > Prioridade DSCP** para carregar a página a seguir.



Siga os seguintes passos para configurar a Prioridade DSCP:

1. Na seção **Configuração de Prioridade DSCP** configure o mapeamento DSCP para 802.1p e o DSCP Remap.

Prioridade DSCP	Mostra o número da prioridade DSCP. A prioridade DSCP é utilizada para classificar os pacotes baseados no valor DSCP, e mapeá-los em diferentes filas. ToS (Type of Service) é uma parte do cabeçalho IP do qual DSCP utiliza os primeiros 6 bits para representar a prioridade dos pacotes IP. Os valores DSCP variam entre 0 e 63.
Prioridade 802.1p	Especifique o mapeamento DSCP para 802.1p. Os pacotes recebidos serão primeiramente mapeados na prioridade 802.1p baseados no mapeamento DSCP para 802.1p, e então para as filas TC de acordo com o mapeamento das filas 802.1p. os pacotes IP untagged com os valores DSCP desejados serão adicionados aos valores de prioridade 802.1p de acordo com o mapeamento DSCP para 802.1p.
DSCP Remap	(Opcional) Selecione a prioridade DSCP a qual a prioridade DSCP original será remapeada. Quando o switch detectar pacotes com o valor DSCP desejado irá modificar o valor DSCP dos pacotes de acordo com o mapeamento.

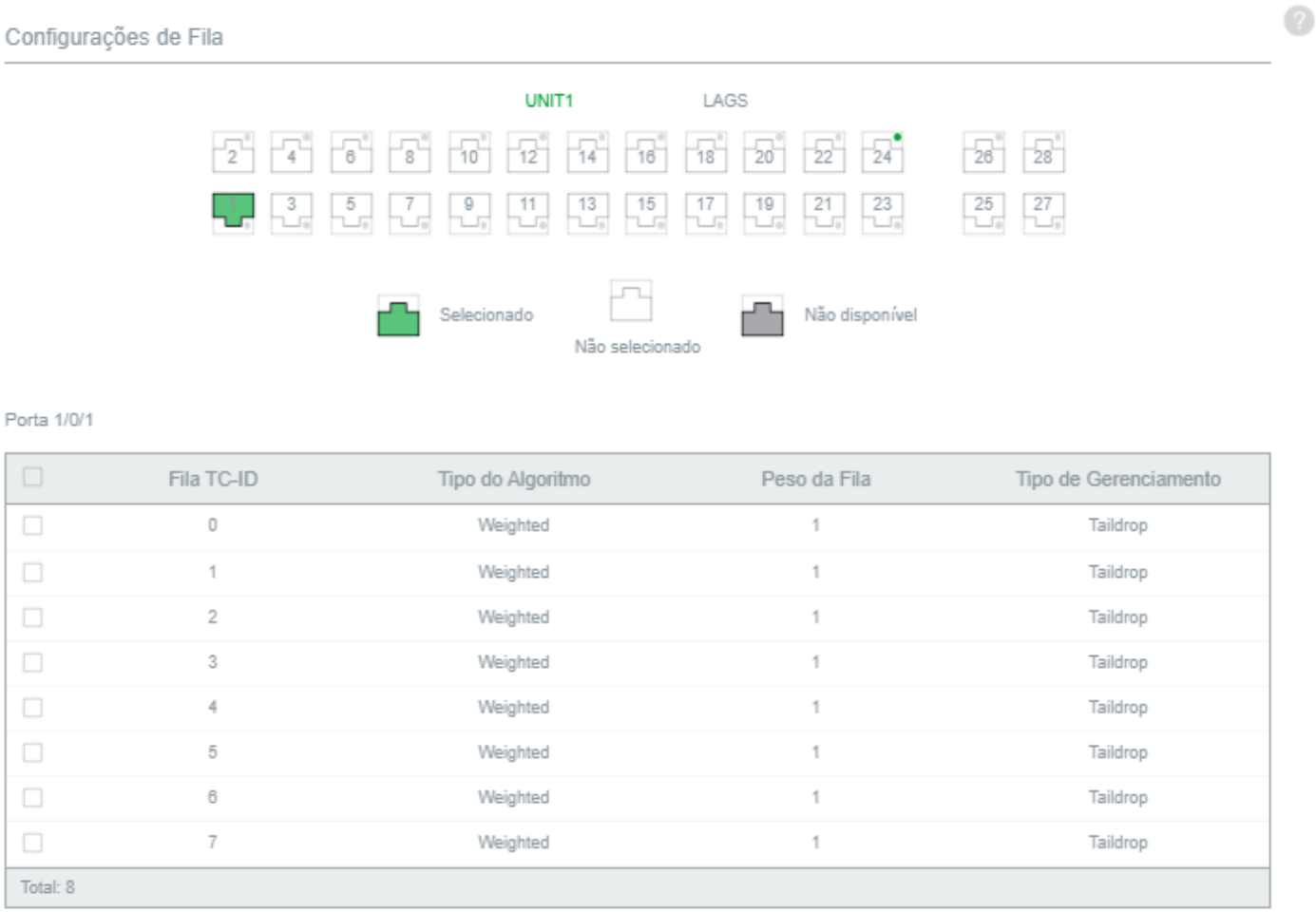
2. Clique em **Aplicar**.

No modo confiar DSP os pacotes não IP serão adicionados à prioridade 802.1p baseada em portas e serão encaminhadas de acordo com o mapeamento das filas 802.1p.

Especificando as configurações do Agendador

Especifique as configurações do Agendador para controlar o encaminhamento dos pacotes de diferentes filas TC quando ocorre congestionamento.

Vá até o menu **QoS > Classe de Serviço > Alg. de Enfileiramento** para carregar a seguinte página.



Siga os seguintes passos para configurar o Tipo de Agendador:

1. Na seção **Configuração do Agendador** selecione as portas desejadas.
2. Selecione a fila desejada e configure os parâmetros.

Fila TC-ID	Mostra o número do ID da prioridade da fila.

Tipo do Algoritmo	Selecione o tipo de Agendador usado para a fila correspondente. Quando ocorre um congestionamento a fila de envio terão a sequência de encaminhamento dos pacotes de acordo com o tipo. **Strict:** nesse modo a fila de envio irá utilizar SP (Strict Priority) para processar o trafego em filas diferentes. Quando ocorrer congestionamento o tráfego será transmitido estritamente de acordo com a prioridade de fila. Fila com prioridade maior ocupará toda a banda. Pacotes em filas com prioridades menores serão encaminhados somente quando a fila de maior prioridade estiver vazia. **Weighted:** nesse modo a fila de envio irá utilizar WRR (Weighted Round Robin) para processar o tráfego em filas diferentes. Quando ocorrer um congestionamento todo o trafego será transmitido, porém a banda que cada tráfego utilizará será alocada de acordo com o peso da fila.
Peso da Fila	Especifique o peso de fila para a fila desejada. Esse valor pode ser definido somente no modo Ponderado. Valores válidos variam entre 1 e 127.
Tipo de Gerenciamento	Mostra o tipo de gerenciamento para a fila. O switch suporta o modo Taildrop. Quando o tráfego exceder o limite o tráfego adicional será descartado.

3. Clique em **Aplicar**.

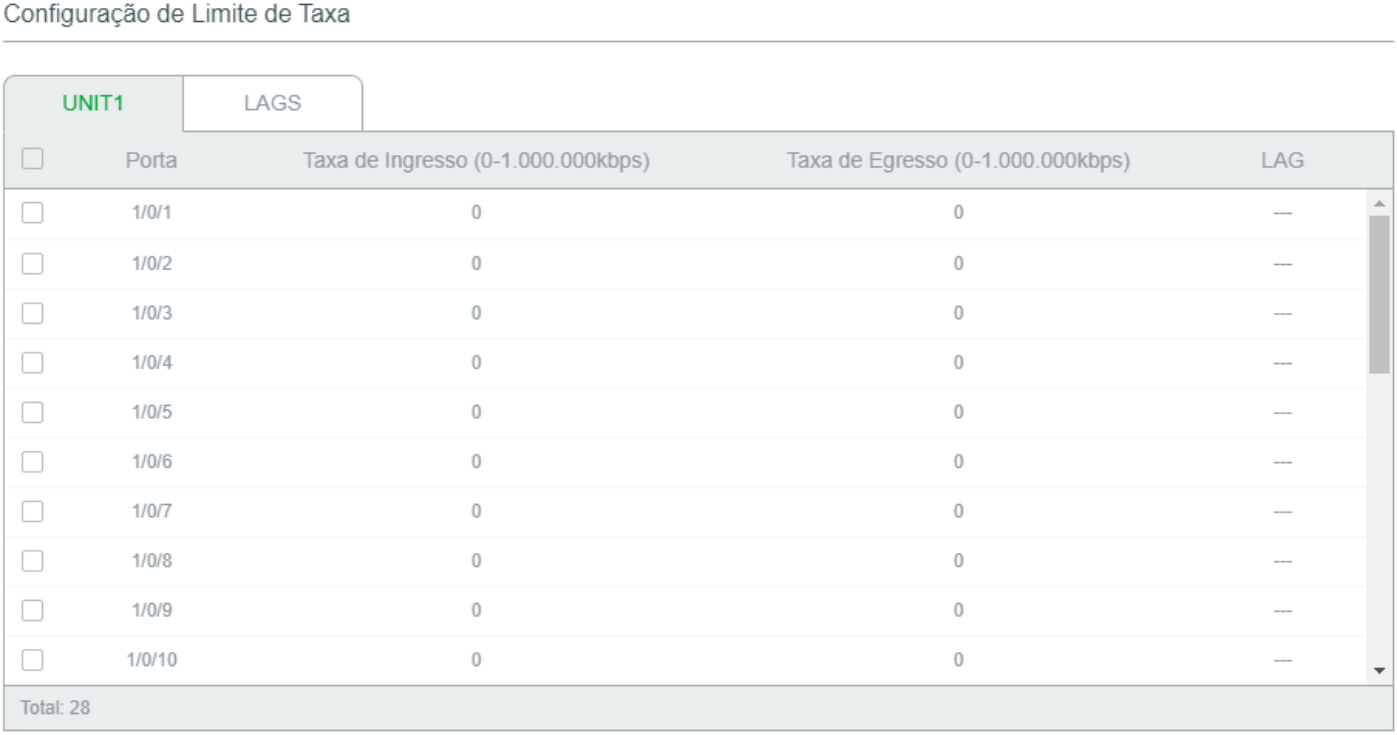
Configuração de Controle de Banda

Com as configurações de Controle de Banda você pode:

- Configurar o Limite de taxa
- Configurar o Storm Control

Configurando o Limite de Taxa

Vá até o menu **QoS > Controle de Largura de Banda > Limite de Taxa** para carregar a seguinte página.



Siga os seguintes passos para configurar a função de limite de taxa:

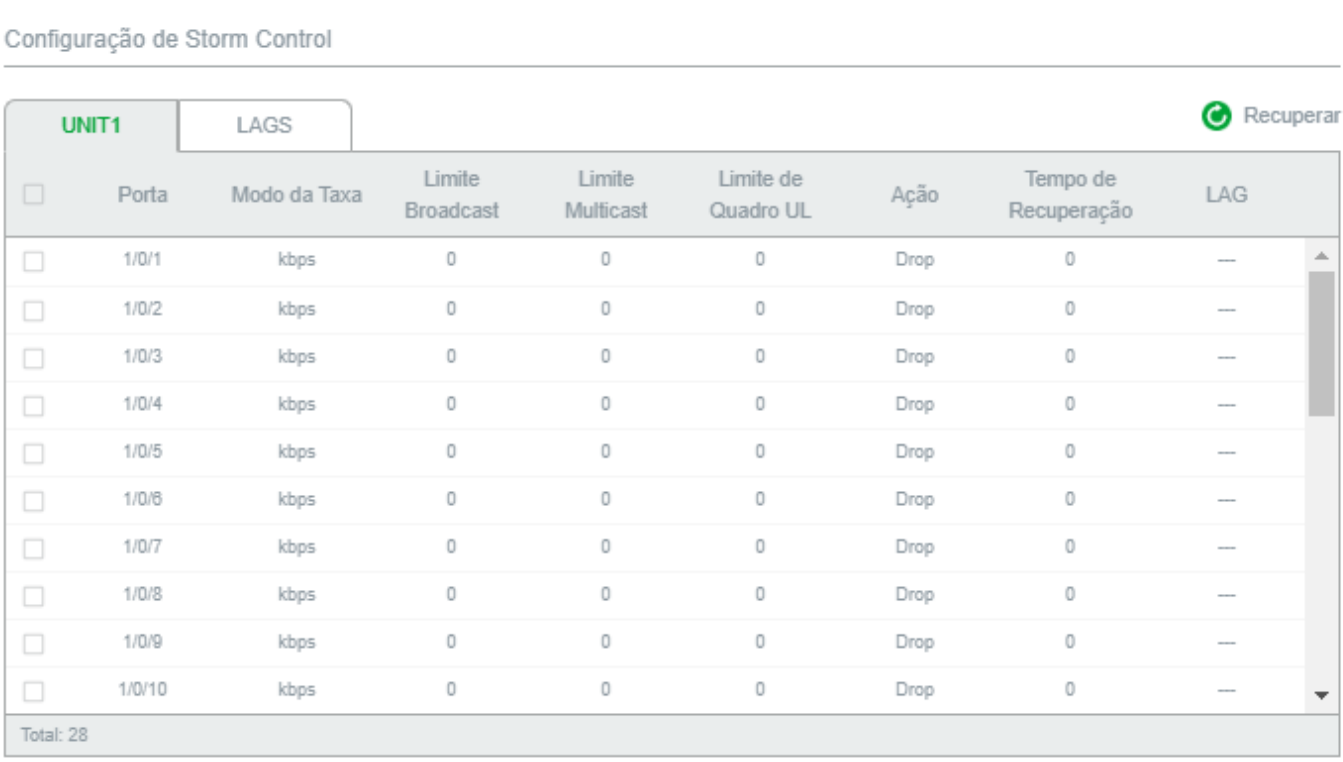
1. Selecione as portas desejadas e configura o limite máximo para recebimento e envio de pacotes.

Taxa de Ingresso (0-1.000.000kbps)	Configure o limite superior para a taxa de recebimento de pacotes para a porta. Os valores válidos variam entre 0 e 1000000 Kbps onde 0 significa que o limite de taxa está desabilitado.
Taxa de Egresso (0-1.000.000kbps)	Configure o limite superior para a taxa de envio de pacotes para a porta. Os valores válidos variam entre 0 e 1000000 Kbps onde 0 significa que o limite de taxa está desabilitado.

2. Clique em **Aplicar**.

Configurando o Storm Control

Vá até o menu **QoS > Controle de Largura de banda > Storm Control** para carregar a página a seguir.



Siga os seguintes passo para configurar a função de Storm Control:

1. Selecione as portas desejadas e configure o limite superior para o encaminhamento de pacotes broadcast, multicast e Threshold de Quadro UL (quadros de unicast desconhecido).

Modo da Taxa	Especifica o modo de taxa para limites de Broadcast, multicast e quadros-UL para as portas desejadas. **Kbps:** o switch irá limitar a velocidade máxima dos tipos de tráfegos especificados em quilo bits por segundo. **Taxa:** o switch irá limitar percentualmente a utilização de banda para o tipo de trafego especificado.
Limite Broadcast	Especifica o limite superior para o recebimento de pacotes broadcast. Os valores válidos diferenciam entre os tipos de modo de taxa escolhido. O valor 0 significa que o limite está desabilitado. O trafego broadcast excedente ao limite será processado de acordo com a configuração de Ação.
Limite Multicast	Especifica o limite superior para o recebimento de pacotes multicast. Os valores válidos diferenciam entre os tipos de modo de taxa escolhido. O valor 0 significa que o limite está desabilitado. O trafego excedente ao limite será processado de acordo com a configuração de Ação.

Limite de Quadro UL	Especifica o limite superior para o recebimento de quadros unicast desconhecidos. Os valores válidos diferenciam entre os tipos de modo de taxa escolhido. O valor 0 significa que o limite está desabilitado. O trafego unicast desconhecido excedente ao limite será processado de acordo com a configuração de Ação.
Ação	Selecione a ação a qual o switch irá tomar quando o trafego exceder o limite correspondente. **Drop:** configura a ação como drop. A porta irá descartar os pacotes subsequentes quando o trafego exceder o limite. **Desligar:** configura a ação como desligar. A porta será desativada quando o trafego exceder o limite.
Tempo de Recuperação	Especifica o recover time para a porta. Essa função só terá efeito quando a ação estiver configurada como desligar. Os valores válidos variam entre 0 e 3600 segundos. Quando uma porta é desativada ela pode se recuperar ao estado normal após o recover time passar. Se o recover time estiver especificado como 0 significa que a porta não se recuperará para o estado normal automaticamente e você poderá recuperar a porta manualmente.

2. Clique em **Aplicar**.

> Para portas em uma mesma LAG, o limite de taxa e storm control devem ser configurados com o mesmo valor para garantir o funcionamento correto do Link Aggregation.

Configuração VLAN Voz

Para completar a configuração de VLAN de voz siga os seguintes passos:

1. Crie uma VLAN 802.1Q
2. Configure o endereço OUI
3. Configure a VLAN Voz Globalmente
4. Adicione portas à VLAN Voz

Guia para configuração

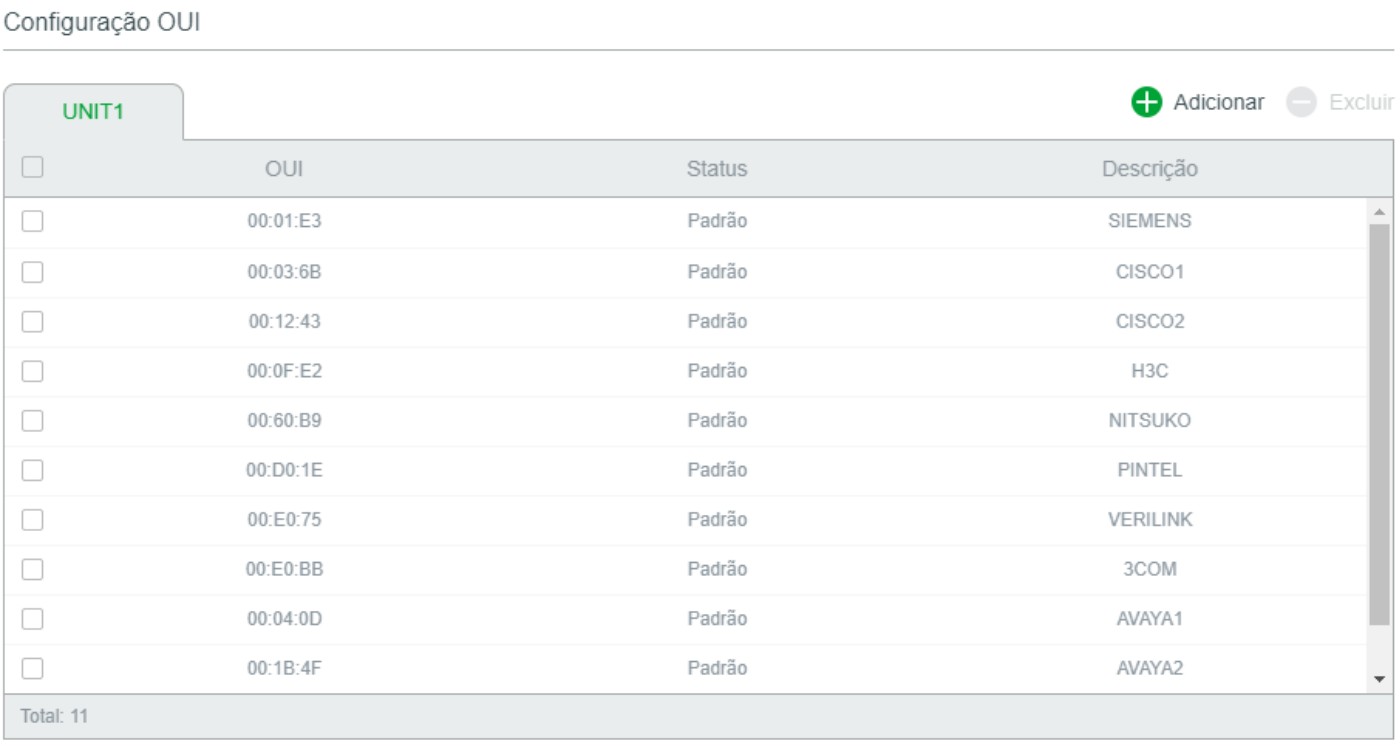
- Antes de configurar a VLAN Voz, você precisa criar uma VLAN 802.1Q para trafego de voz. Para mais detalhes sobre a configuração de VLAN 802.1Q vá até Configurando VLAN 802.1Q.
- A VLAN 1 é a VLAN padrão e não pode ser configurada como VLAN Voz.
- Somente uma VLAN pode ser apontada como VLAN Voz no switch.

Configurando endereço OUI

O endereço OUI é atribuído pelo IEEE como um identificador exclusivo à um fornecedor de dispositivos. É utilizado pelo switch para determinar se um pacote é um pacote de voz.

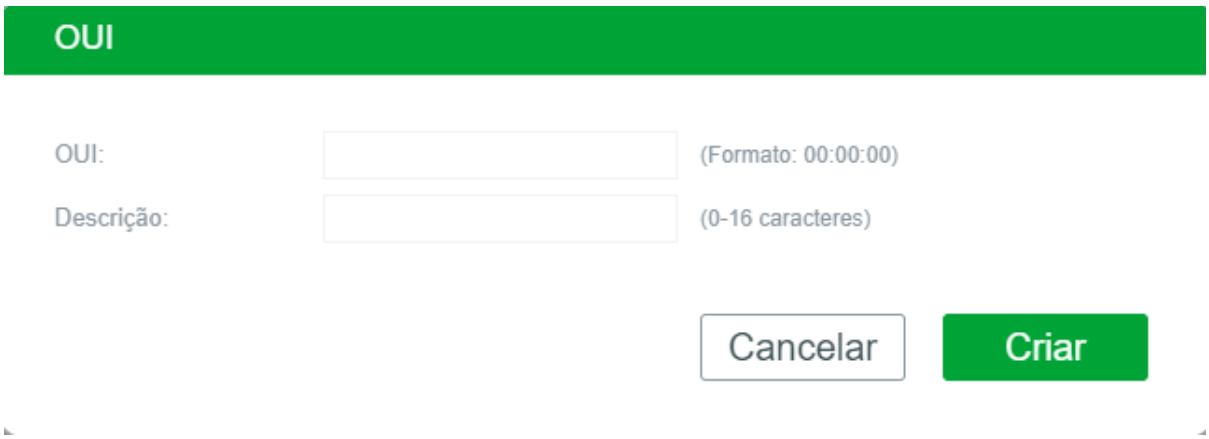
Se o endereço OUI do seu dispositivo de voz não estiver na tabela OUI você deverá adicioná-lo à tabela de endereços OUI.

Vá até o menu **QoS > VLAN Voz > Configuração OUI** para carregar a seguinte página.



Siga os seguintes passos para configurar endereços OUI:

1. Clique em Adicionar para carregar a seguinte página.



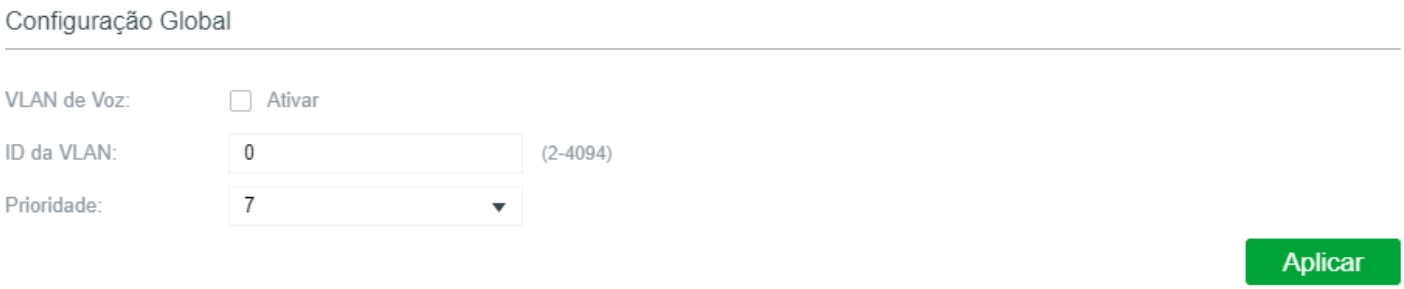
2. Especifique o OUI e a descrição.

OUI	Entre com o endereço OUI do seu dispositivo de voz. O endereço OUI é utilizado pelo switch para determinar se um pacote é um pacote de voz ou não. Um endereço OUI é composto pelos primeiros 24 bits do endereço MAC e é atribuído pelo IEEE como um identificador único à um vendedor de dispositivos. Se o Endereço MAC de origem for correspondente à um endereço OUI na lista o switch identificará o pacote como pacote de voz e priorizará a sua transmissão.
Descrição	Dê uma descrição para identificação do endereço OUI.

3. Clique em **Criar**.

Configurando VLAN Voz Globalmente

Vá até o menu **QoS > VLAN de Voz > Configuração Global** para carregar a seguinte página.



Siga os seguintes passos para configurar a VLAN Voz Globalmente:

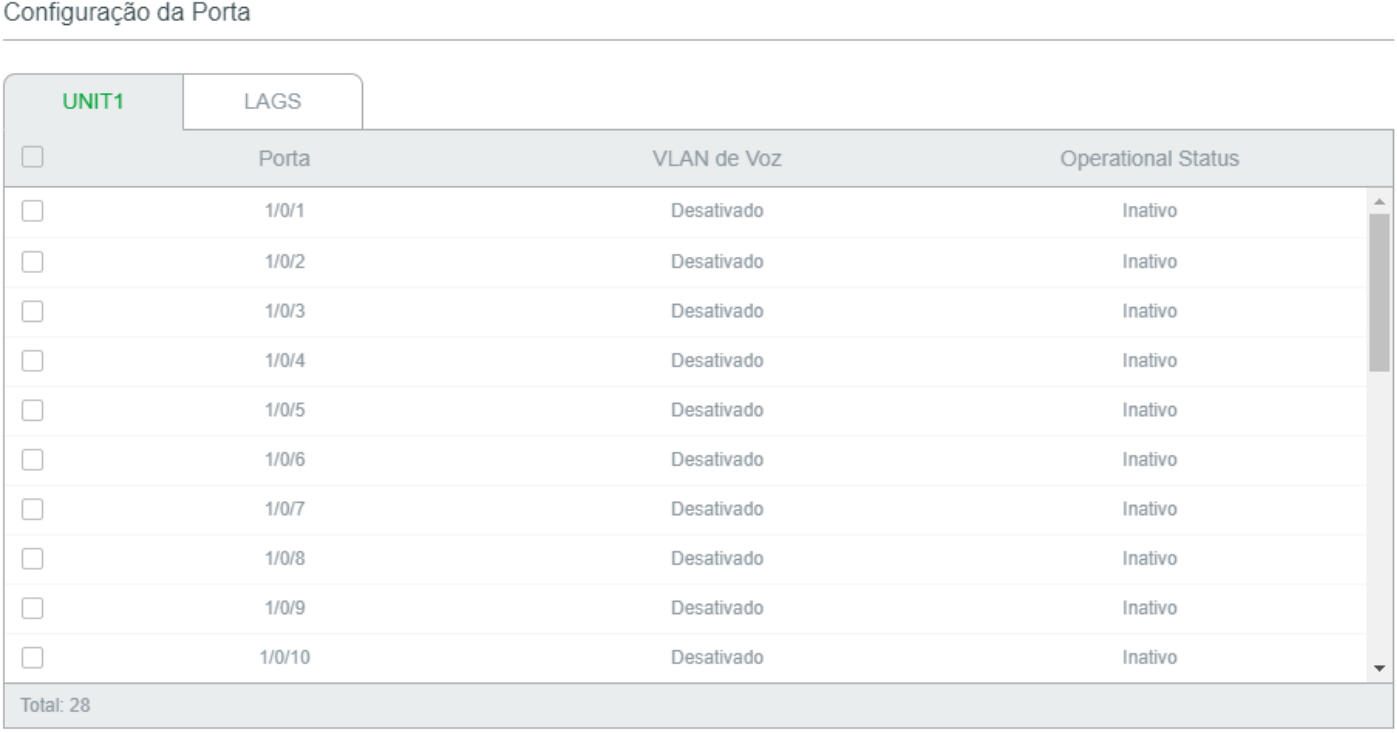
1. Habilite a função de VLAN Voz e especifique os parâmetros.

ID da VLAN	Especifique a ID da VLAN 802.1Q que será definida como VLAN Voz.
Prioridade	Selecione a prioridade que será atribuída aos pacotes de voz. Um valor maior representa uma prioridade maior. Esta é uma prioridade IEEE 802.1p e você pode configurar também seu modo Agendador na Classe de Serviço se necessário.

2. Clique em **Aplicar**.

Adicionando Portas à VLAN de Voz

Vá até o menu **QoS > VLAN de Voz > Configuração de Porta** para carregar a página a seguir.



Siga os seguintes passo para configurar a VLAN Voz para portas:

1. Selecione as portas desejadas e escolha Habilitar no campo VLAN de Voz.

VLAN de Voz	Selecione habilitar para habilitar a função de VLAN de Voz nas portas e adicioná-las à VLAN de Voz.
Status	Mostra o estado da VLAN de Voz para a porta correspondente. **Ativo:** indica que a função de VLAN de Voz está habilitada para a porta. **Inativo:** indica que a função VLAN de Voz está desabilitada para a porta.

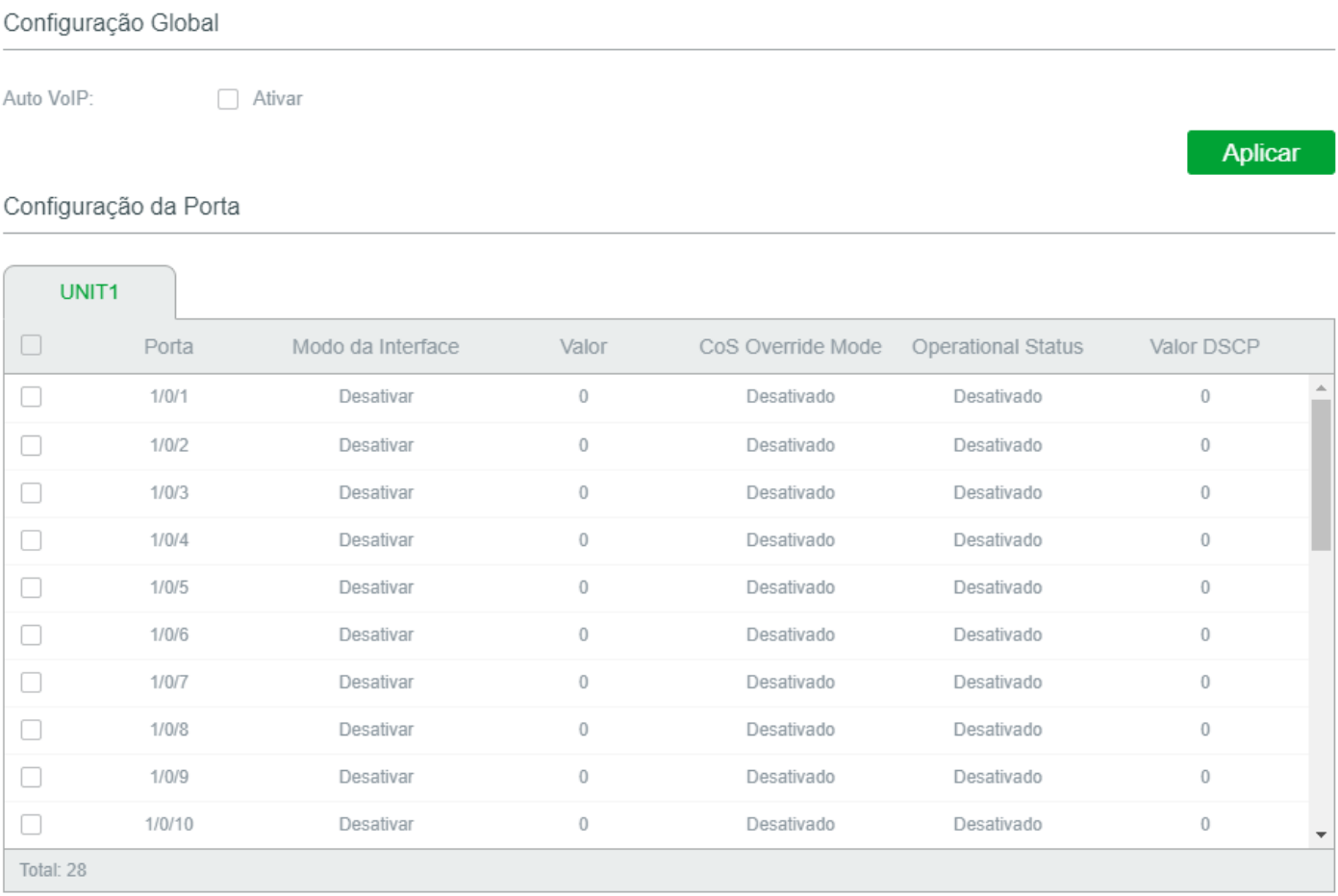
2. Clique em **Aplicar**.

Configuração Auto VoIP

Guia de Configuração

- Antes de configurar o Auto VoIP, você precisa habilitar o LLDP-MED nas portas e configurar os parâmetros relevantes. Para mais detalhes a respeito da configuração LLDP-MED vá até o Configurando LLDP.
- Auto VoIP provê uma solução flexível para otimização do trafego de voz. Ele pode funcionar com outras funções como VLAN e Classe de Serviço para processar pacotes de voz com campos específicos. Você pode escolher e configurar Auto VoIP e outras funções de acordo com a sua necessidade.

Vá até o menu **QoS > Auto VoIP** para carregar a página a seguir.



Siga os seguintes passos para configurar o Auto VoIP:

1. Na seção **Configuração Global** habilite o Autor VoIP globalmente.
2. Na seção **Configuração da Porta** selecione as portas desejadas e configure os parâmetros.

Modo da Interface

Selecione o modo de interface para a porta.

Desativar: desabilita a função de Auto VoIP para a porta correspondente.

Nenhum: permite que o dispositivo de voz utilize a sua própria configuração para encaminhar o trafego de voz.

ID da VLAN: o dispositivo de voz irá enviar pacotes de voz com a tag da VLAN desejada. Se esse modo estiver selecionado será necessário especificar o ID da VLAN no campo valor.

Você também necessitará configurar a VLAN 802.1Q para garantir que as portas correspondentes possam encaminhar pacotes normalmente.

Dot1p: os dispositivos de voz enviarão pacotes de voz com a prioridade 802.1p desejada. Se esse modo estiver selecionado será necessário especificar a prioridade 802.1p no campo Valor.

Você também necessitará configurar a Classe de Serviço para fazer que o switch processe os pacotes de acordo com a prioridade 802.1p.

Untagged: os dispositivos de voz enviarão pacotes de voz sem tag.

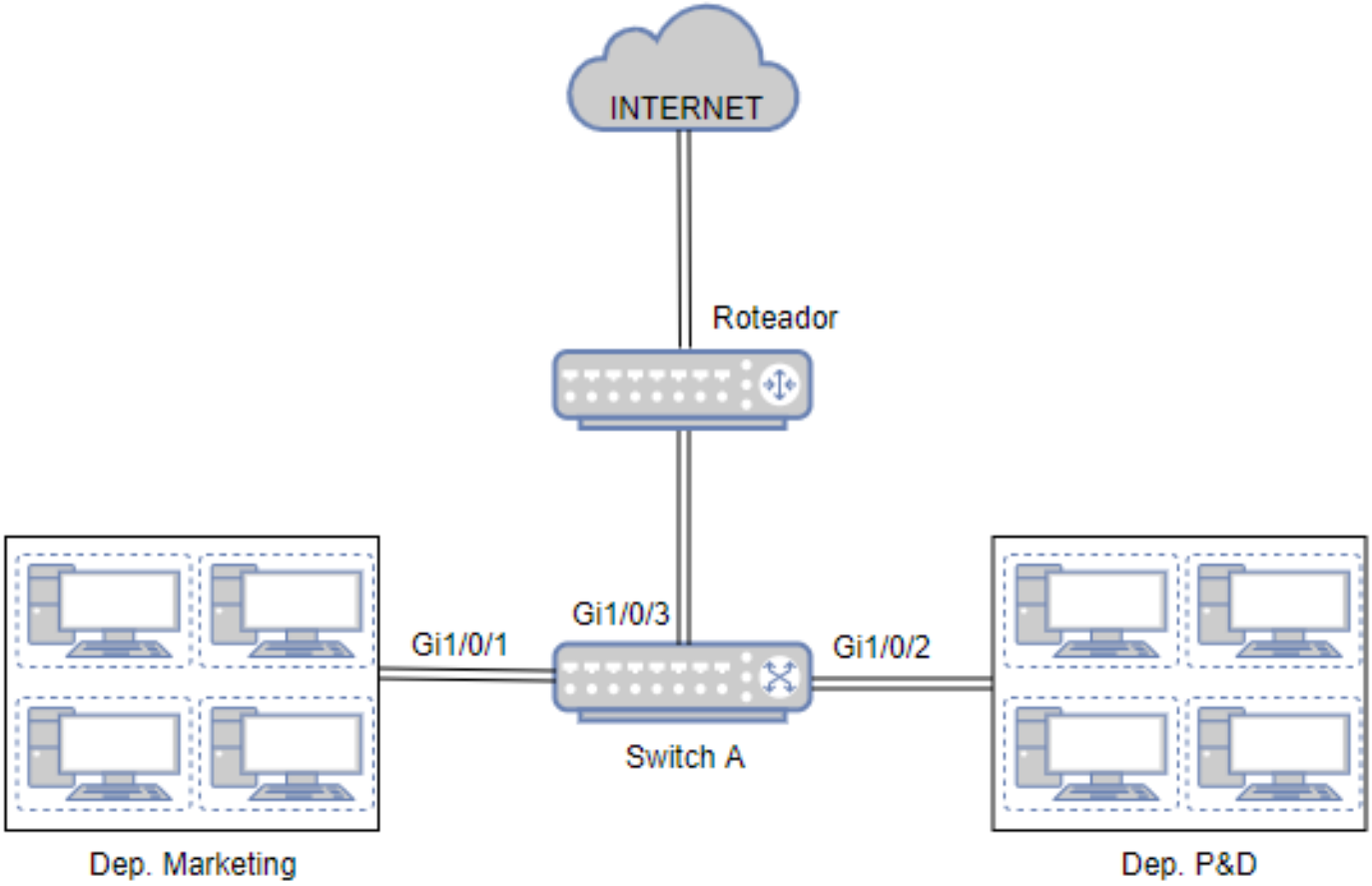
Valor	Entre com o ID da VLAN ou com o valor da prioridade 802.1p para a porta de acordo com a configuração do Modo da Interface.
CoS Override Mode	Habilita ou desabilita o modo CoS Override Mode. **Ativar:** habilita o CoS Override. O switch irá ignorar a prioridade 802.1p nos pacotes de voz e colocará os pacotes diretamente na fila TC-5. **Desativar:** desabilita o CoS Override. O switch irá então colocar os pacotes de voz na fila TC correspondente de acordo com a prioridade 802.1p dos pacotes.
Valor	Mostra o estado operacional da função VLAN de Voz para a interface. Para habilitar você deve habilitar a VLAN Voz tanto globalmente quanto para a interface.
Valor DSCP	Entre com o valor da prioridade DSCP. O dispositivo de voz irá encaminhar pacotes com o correspondente valor DSCP. Você também precisará configurar Classe de Serviço para fazer com que o switch processe os pacotes de acordo com a prioridade DSCP.

3. Clique em **Aplicar**.

Exemplo de Classe de Serviço

Requisitos de Rede

Como mostrado a baixo, os departamentos de Marketing e P&D pode acessar a internet. Quando ocorre um congestionamento o trafego de ambos os departamentos podem ser encaminhados e o trafego do departamento de Marketing deve preferência.



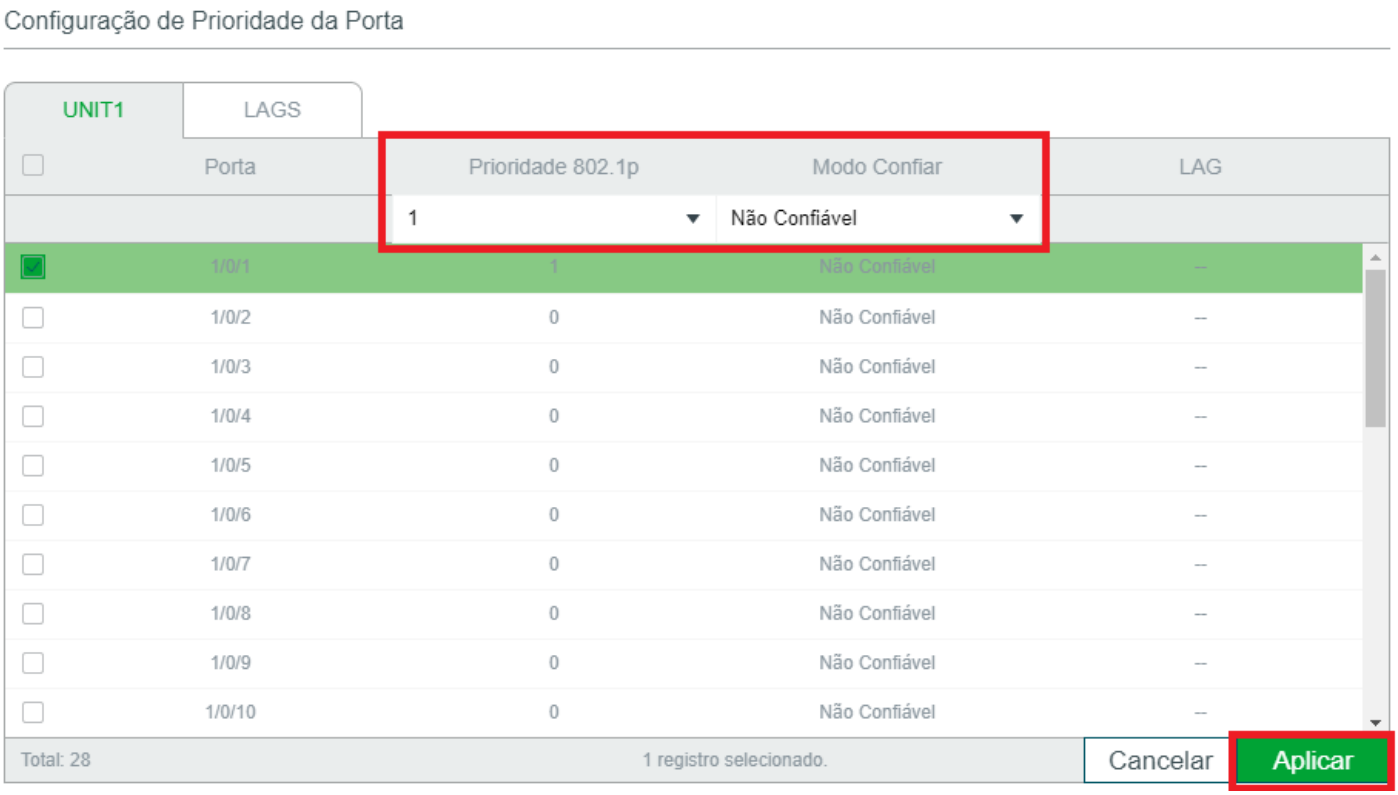
Configurando o Cenário

Para implementar esse requisito você pode configurar a prioridade de porta para colocar os pacotes do departamento de marketing em uma fila com prioridade mais alta que os pacotes do departamento de P&D.

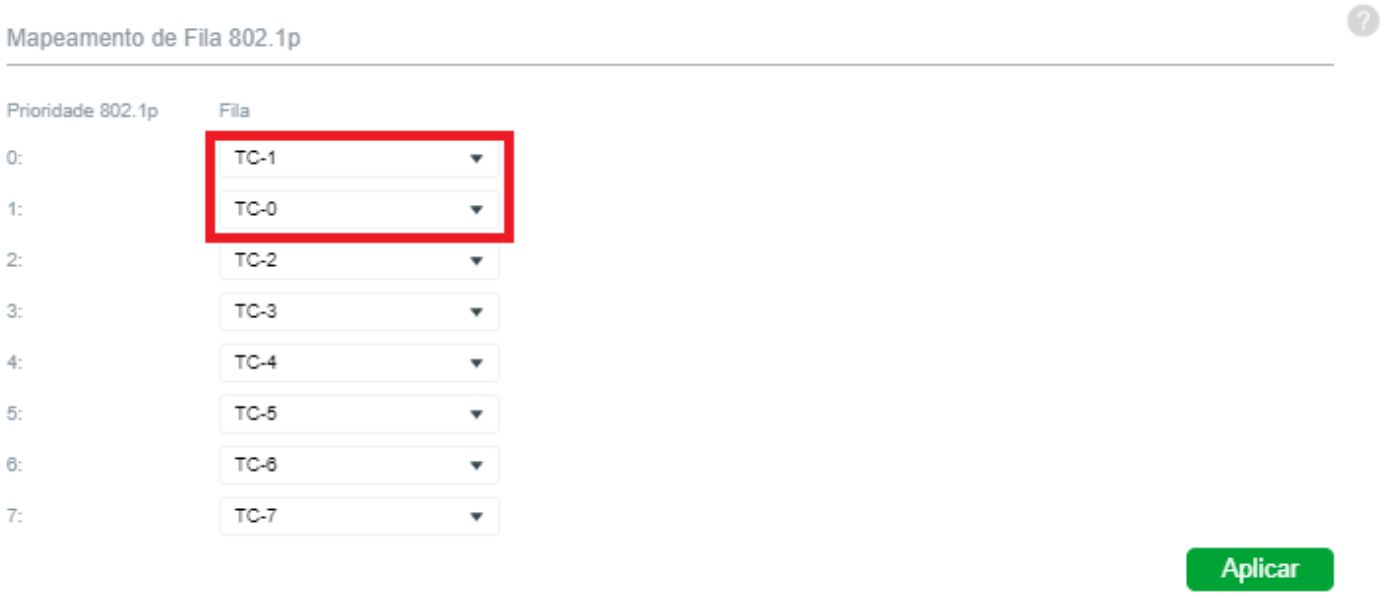
- Configure o Modo Confiar para a porta 1/01 e porta 1/0/2 como Não Confiável e mapeie as portas em diferentes filas.
- Configure o tipo do agendador como Weighted para porta 1/0/3 e especifique o Peso da Fila para fazer com que o trafego do departamento de marketing tenha preferência.

Como demonstrado a baixo:

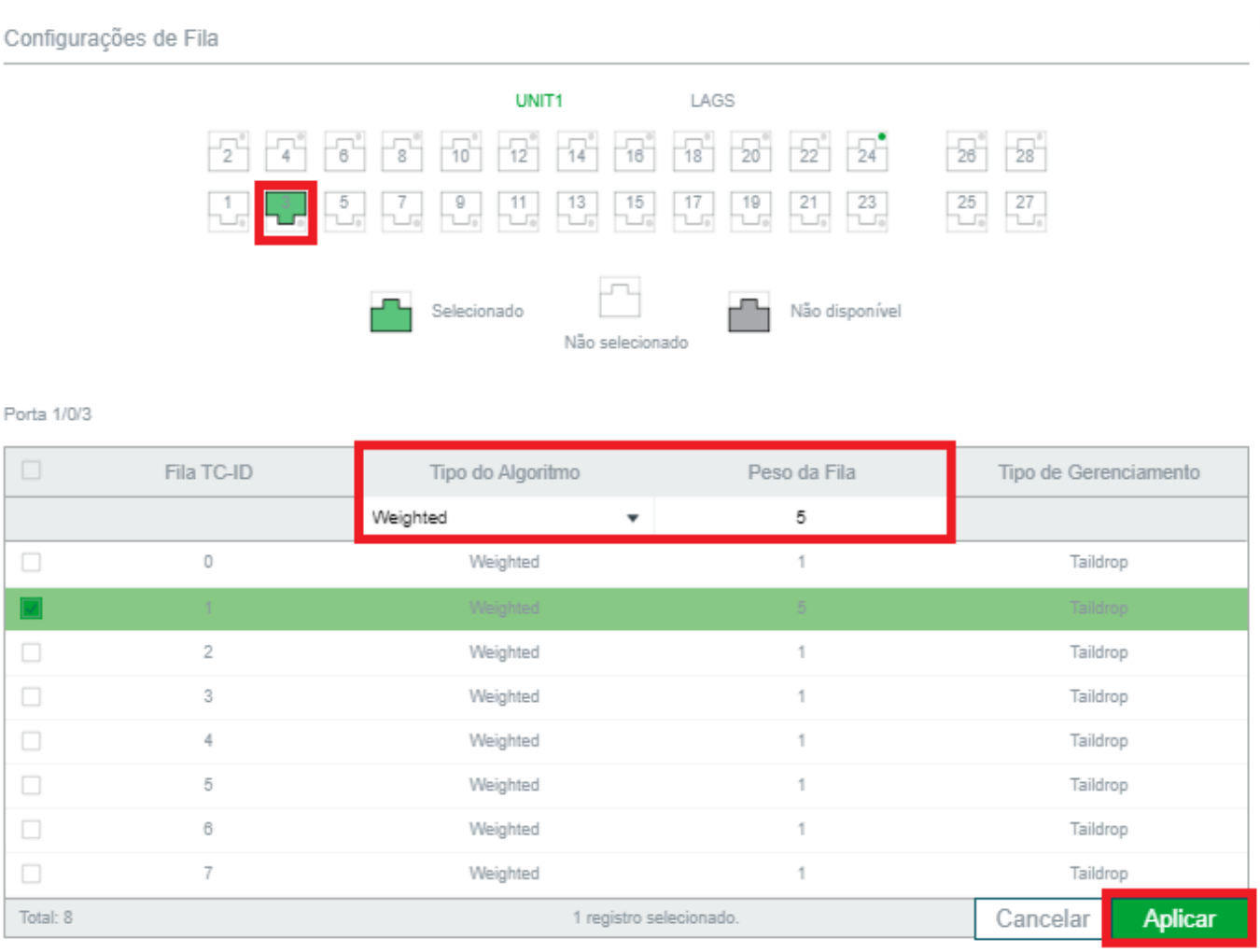
1. Vá até o menu **QoS > Classe de Serviço > Prioridade de Porta** para carregar a página a seguir. Configure o modo confiar da porta 1/01 e porta 1/0/2 como não confiável. Especifique a prioridade 802.1p para aporta 1/0/1 como 1 e especifique a prioridade 802.1p para a porta 1/0/2 como 0. Clique em **Aplicar**.



2. Vá até o menu **QoS > Classe de Serviço > Prioridade 802.1p** para carregar a página a seguir. Mapeie a prioridade 0 do 802.1p para TC-1 e mapeie a prioridade 1 do 802.1p para o TC-0. Clique em **Aplicar**.



3. Vá até o menu **QoS > Classe de Serviço > Configurações do Agendador** para carregar a página a baixo. Selecione a porta 1/0/3 e configure o tipo do agendador das filas TC-0 e TC-1 como ponderado. Especifique o Peso da Fila da TC-1 como 5. Clique em **Aplicar**.

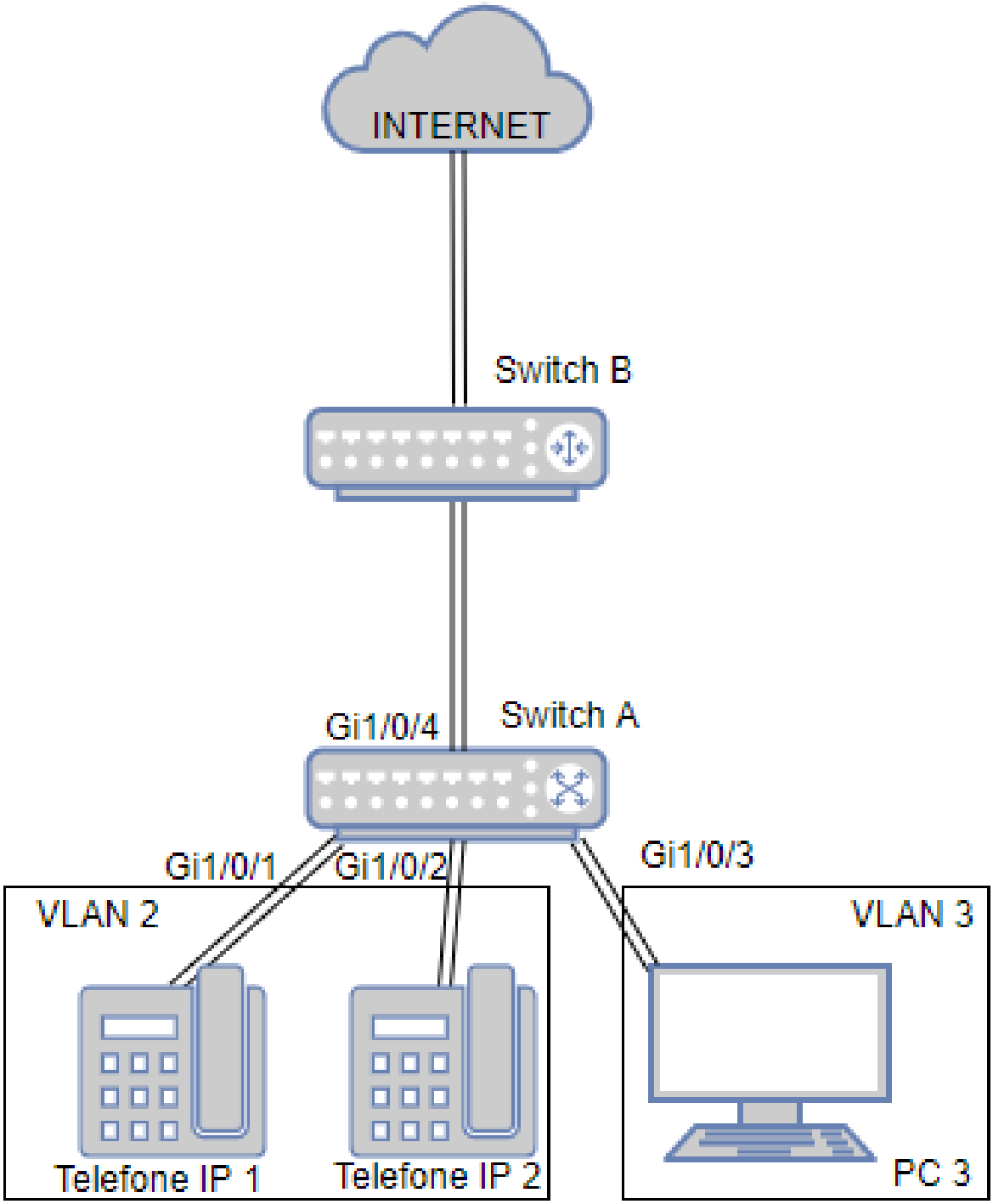


4. Clique em Salvar para salvar as configurações.

Exemplo para VLAN Voz

Requisitos de Rede

Como mostrado abaixo, uma companhia pretende instalar telefones IP na área de escritório. Para garantir uma boa qualidade de voz, os telefones IP e os computadores serão conectados em diferentes portas do switch, o tráfego de voz necessita de uma maior prioridade que o trafego de dados.



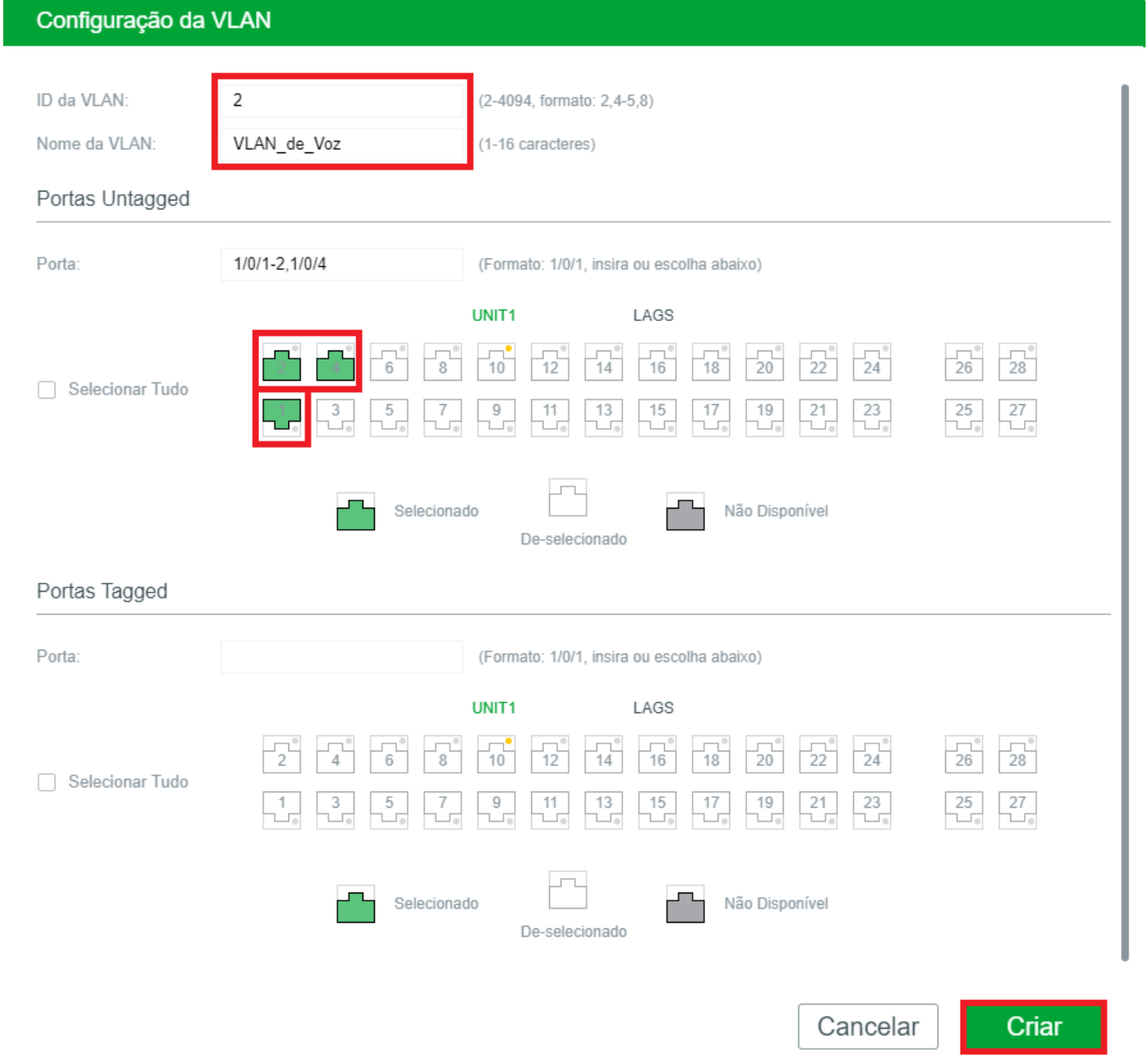
Configurando o Cenário

Para implementar o requisite você pode configurar a VLAN Voz para garantir que o trafego de voz possa ser transmitido na mesma VLAN e o tráfego de dados seja transmitido em outra VLAN. Você ainda pode especificar a prioridade para que o tráfego de voz tenha preferência quando ocorrer congestionamento.

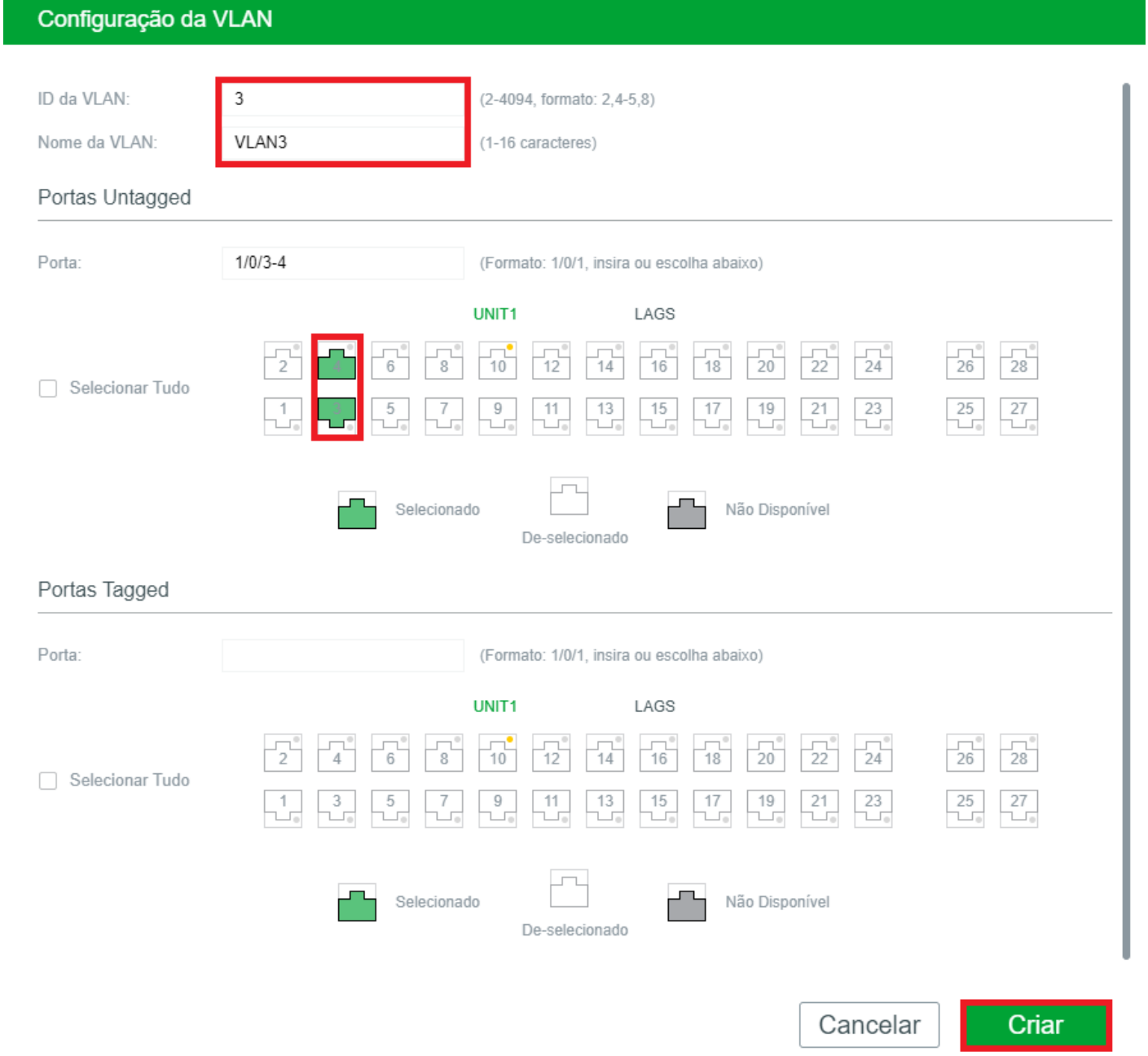
- Configure VLAN 802.1Q para as portas 1/01-2, para a porta 1/0/3 e porta 1/0/4.
- Configure a função de VLAN Voz para a porta 1/0/1 e porta 1/0/2.

Como demostrado à baixo:

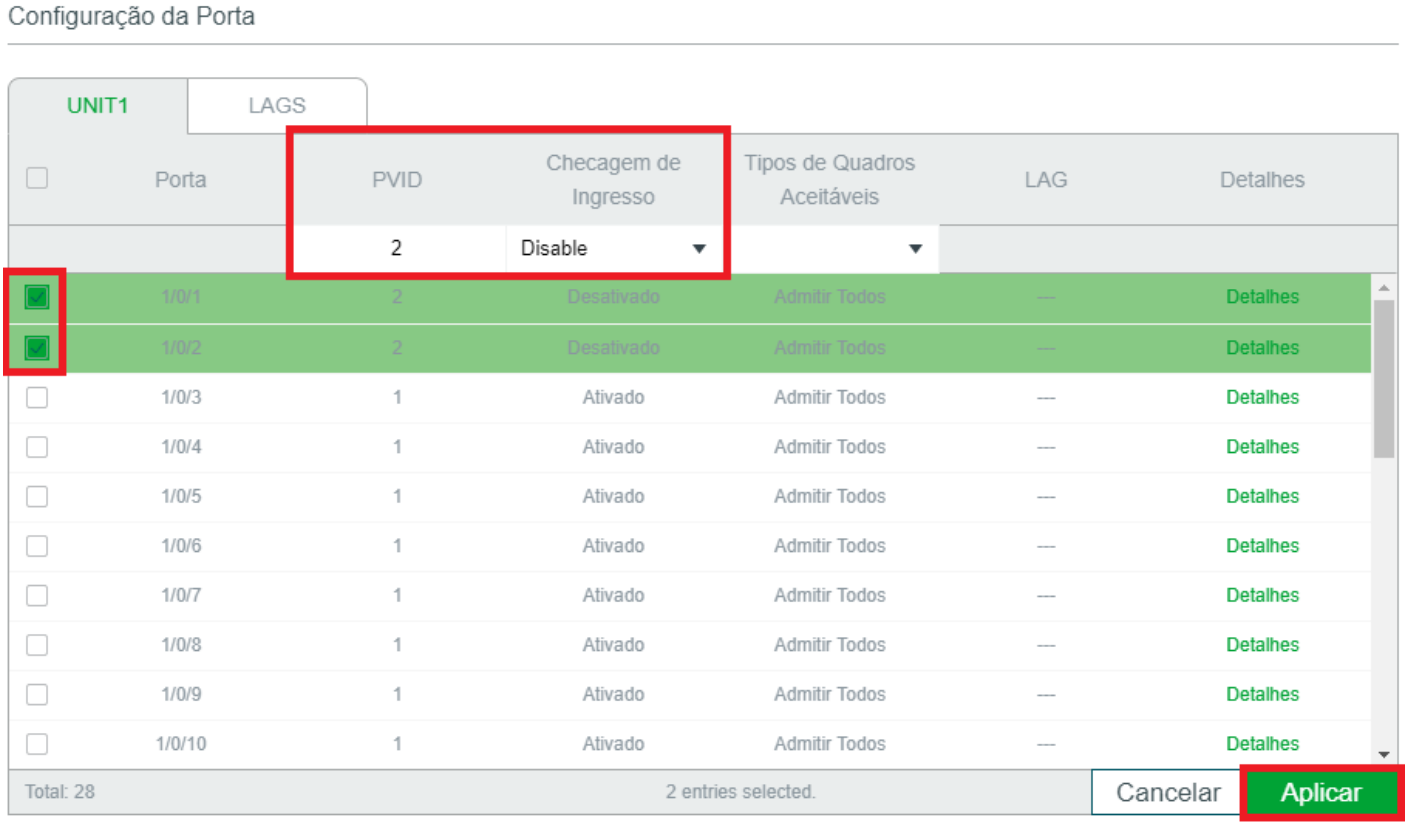
1. Vá até o menu **FUNÇÕES L2 > VLAN > VLAN 802.1Q > Configuração VLAN** e clique em Adicionar para carregar a página abaixo. Crie a VLAN 2 e adicione a porta 1/0/1, 1/0/2 e 1/0/4 como untagged. Clique em **Criar**.



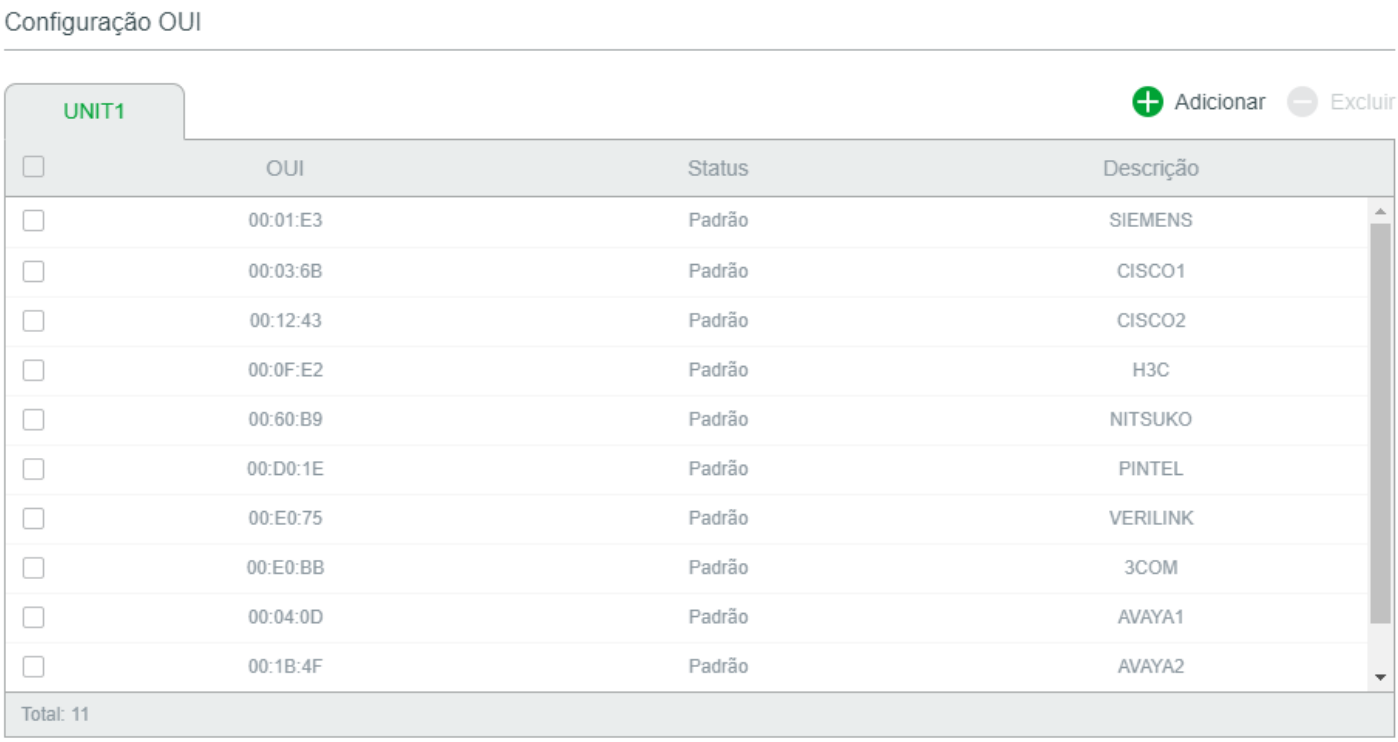
2. Clique em ⊕ Adicionar para carregar a página a baixo. Crie a VLAN3 e adicione as ports 1/0/3 e 1/0/4 como untagged. Clique em **Criar**.



3. Vá até o menu **FUNÇÕES L2 > VLAN > VLAN 802.1Q > Configuração de Porta** para carregar a página a seguir. Desabilite a função Checagem de Ingresso para a porta 1/0/1 e porta 1/0/2 e especifique o PVID como 2. Clique em **Aplicar**.

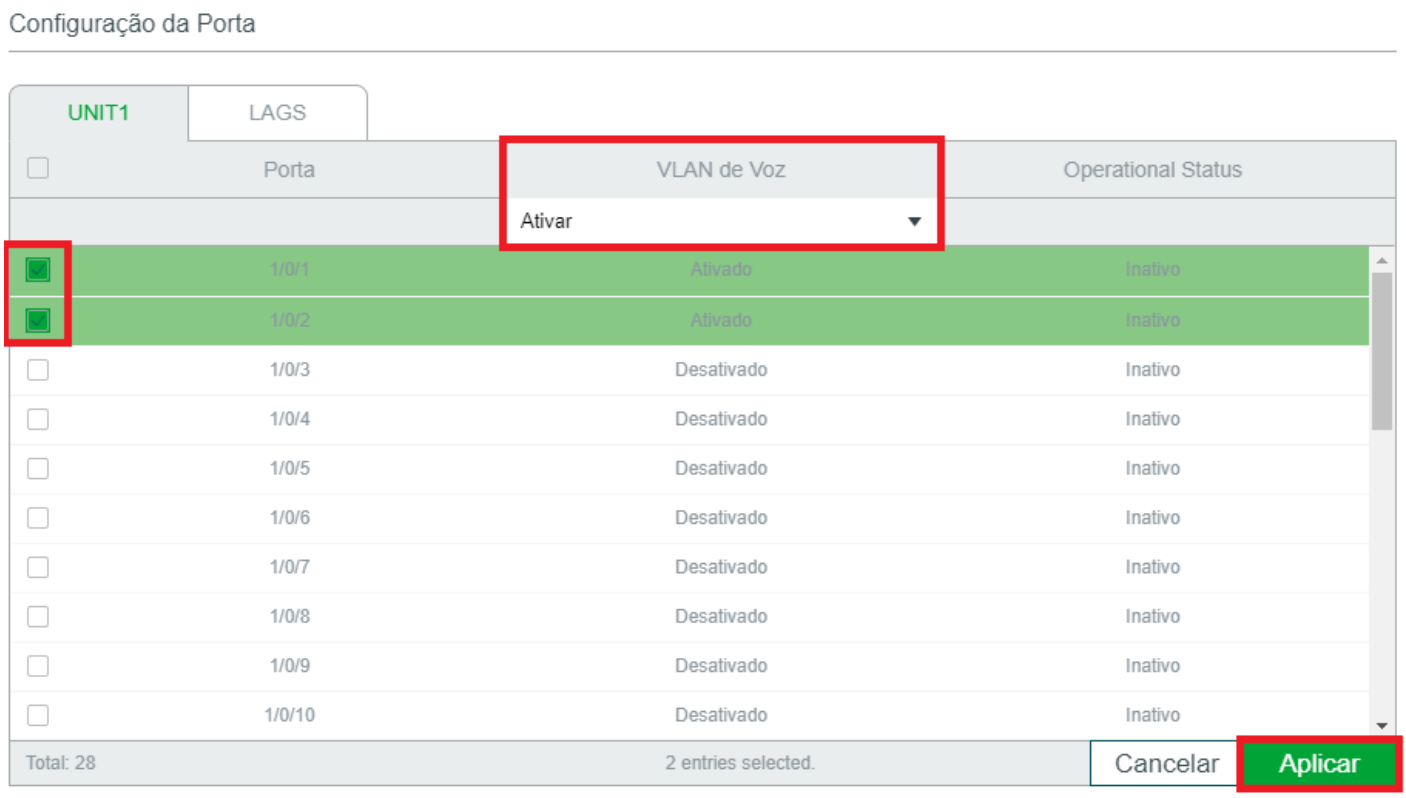


4. Vá até o menu **QoS > VLAN Voz > Configuração OUI** para carregar a página a seguir. Cheque a tabela OUI.



5. Vá até o menu **QoS > VLAN Voz > Configuração Global** para carregar a página a seguir. Habilite a VLAN Voz globalmente. Especifique a ID da VLAN como 2 e configure a sua prioridade como 7. Clique em **Aplicar**.

6. Vá até o menu **QoS > VLAN Voz > Configuração de Porta** para carregar a página a seguir. Habilite a VLAN Voz na porta 1/0/1 e porta 1/0/2. Clique em **Aplicar**.

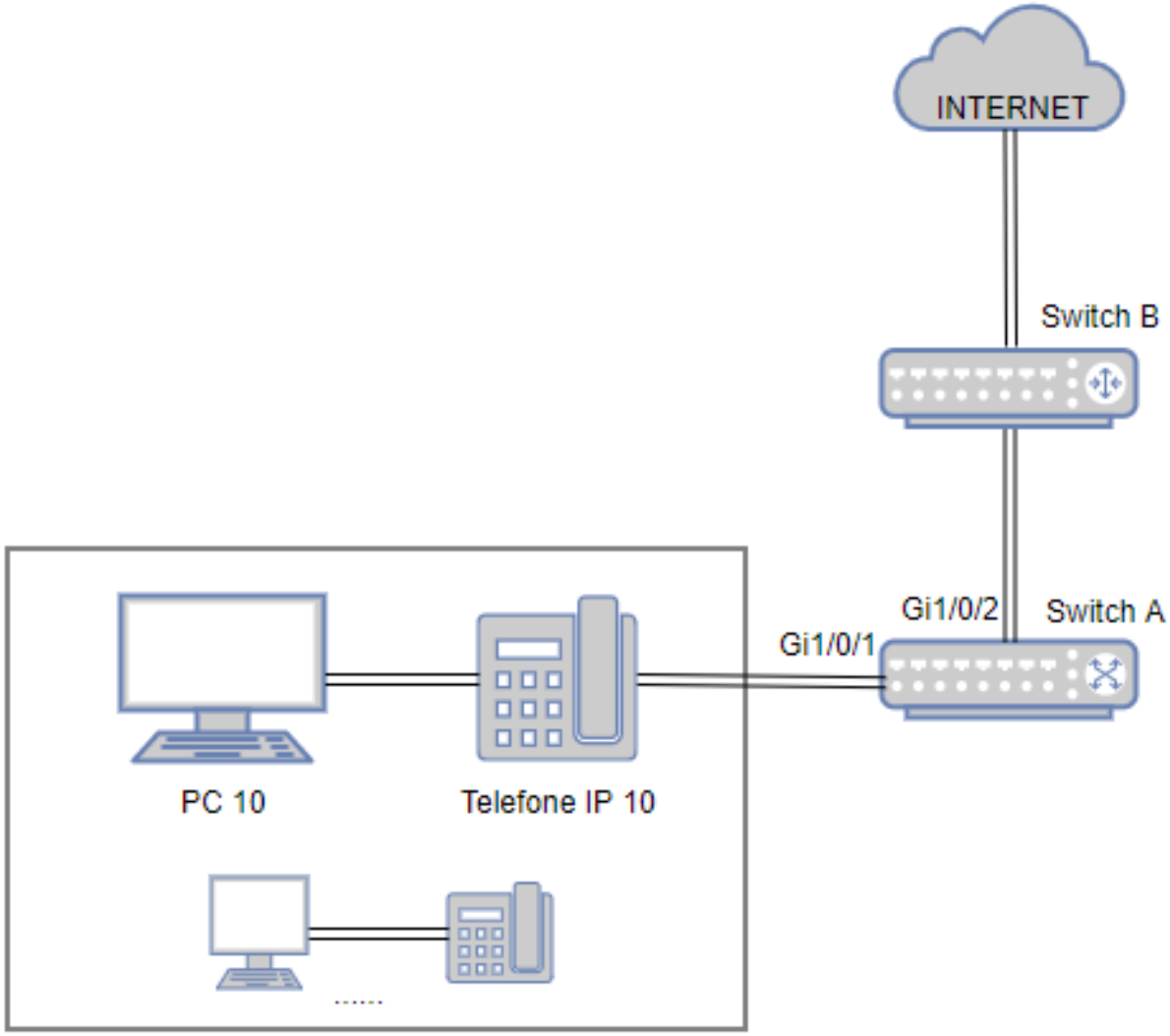


7. Clique em Salvar para salvar as configurações.

Exemplo para Auto VoIP

Requisitos de Rede

Como mostrado abaixo, a companhia planeja instalar telefones IP na área de escritório. Os telefones IP compartilham as portas do switch utilizadas pelos computadores porque não há portas sobrando para os telefones IP. Para garantir uma boa qualidade de voz o trafego de voz necessita de uma prioridade maior que o trafego de dados.



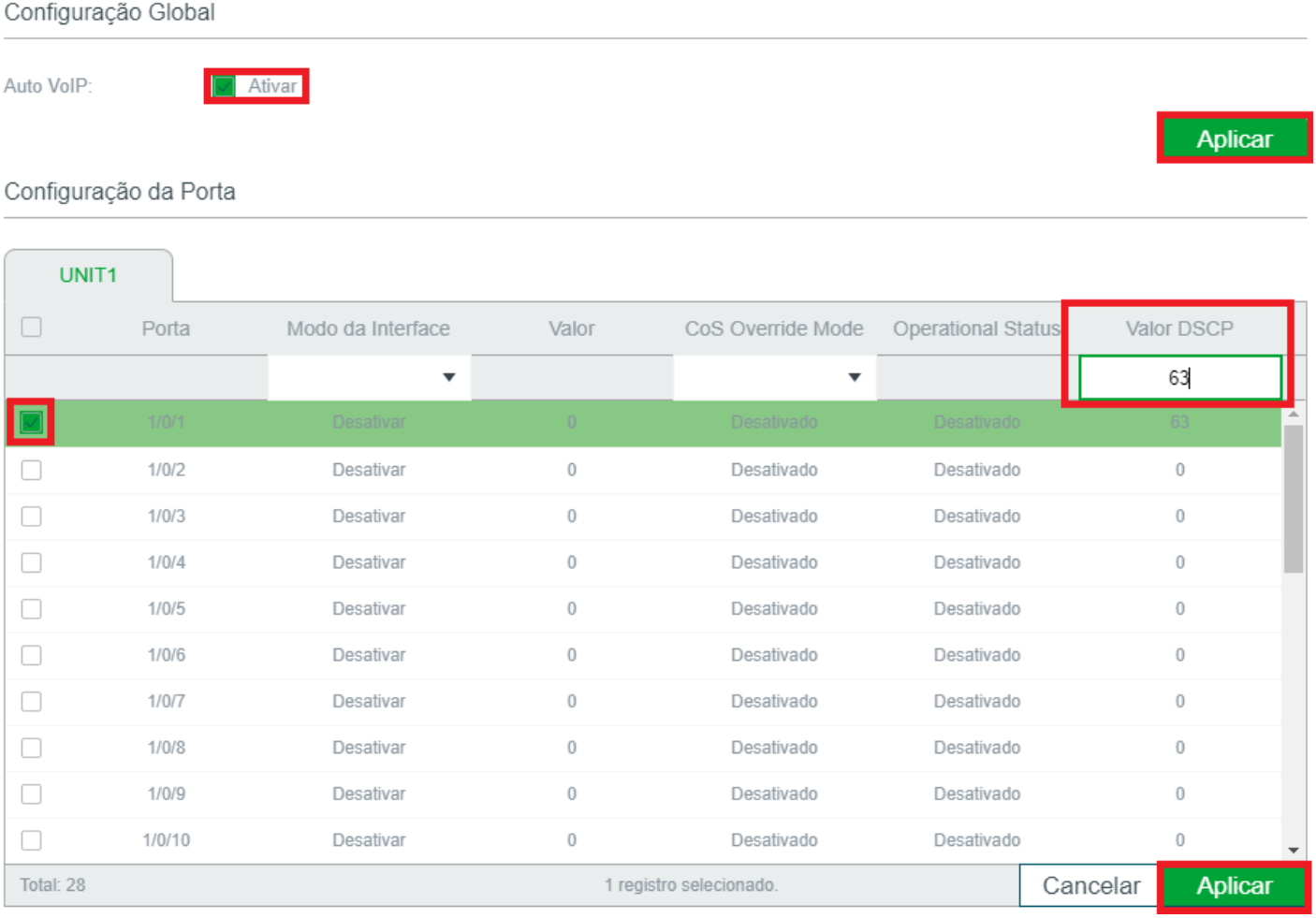
Configurando o Cenário

Para otimizar o trafego de voz configure o Auto VoIP e LLDP-MED para instruir os telefones IP a enviar trafego com a prioridade DSCP desejada. Trafego de voz é colocado em uma fila desejada e o trafego de dados é colocado em outra fila de acordo com a configuração da Classe de Serviço. Garantindo que o trafego de voz tenha preferência quando ocorrer congestionamento.

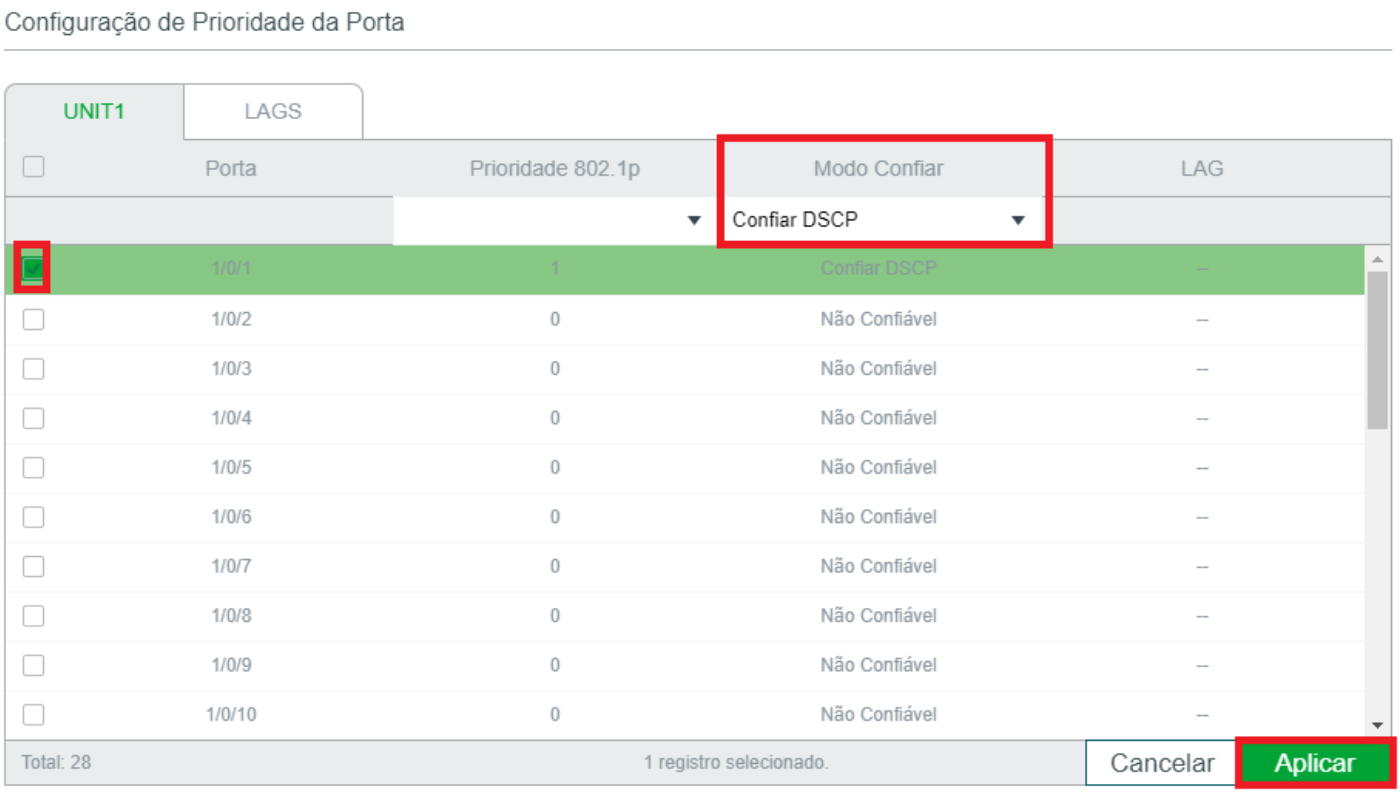
- Habilite a função Auto VoIP e configure o valor DSCP para as portas.
- Configure a Classe de Serviço.
- Habilite LLDP-MED e configure os parâmetros correspondentes.

A configuração Auto VoIP para a porta 1/0/1 e as outras portas conectadas à telefones IP são as mesmas, as configurações a seguir tomarão a porta 1/0/1 como exemplo:

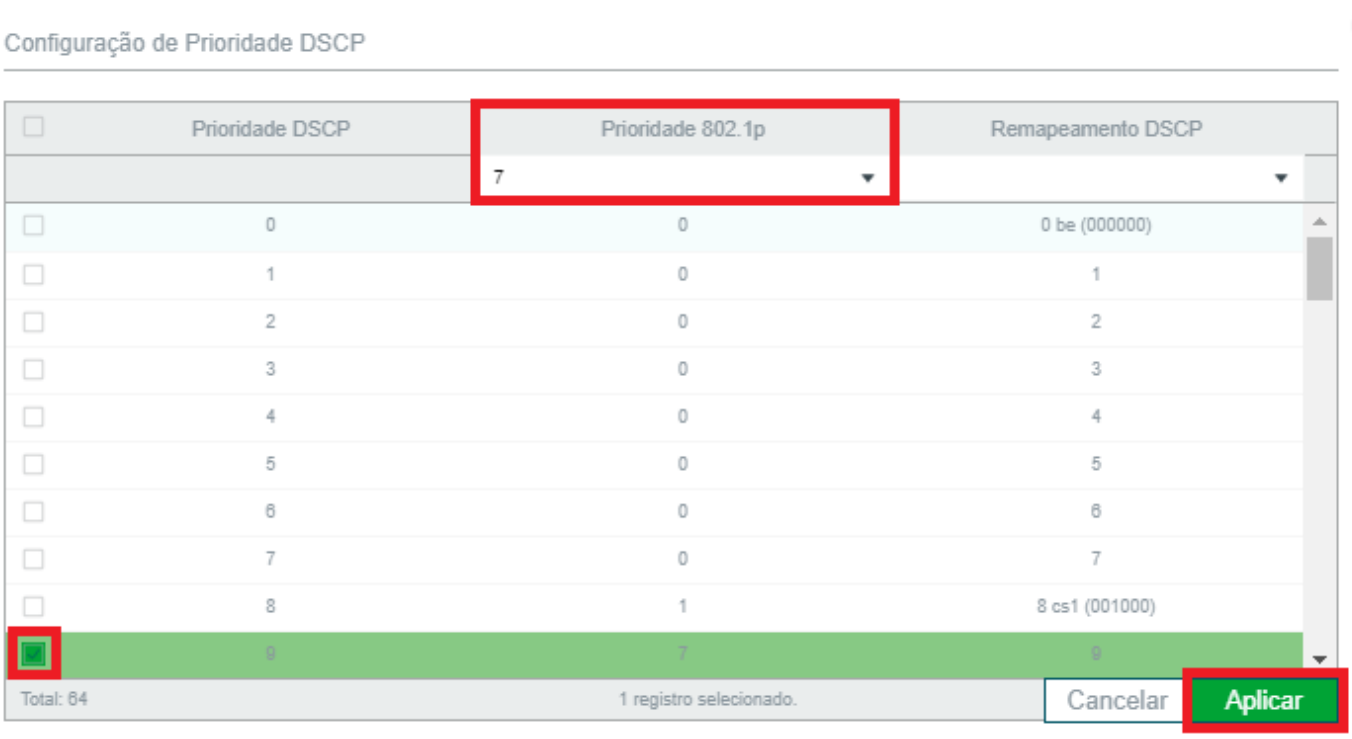
1. Vá até o menu **QoS > Auto VoIP** para carregar a página a seguir. Habilite o Auto VoIP globalmente e especifique o valor DSCP para porta 1/0/1 como 63. Clique em **Aplicar**.



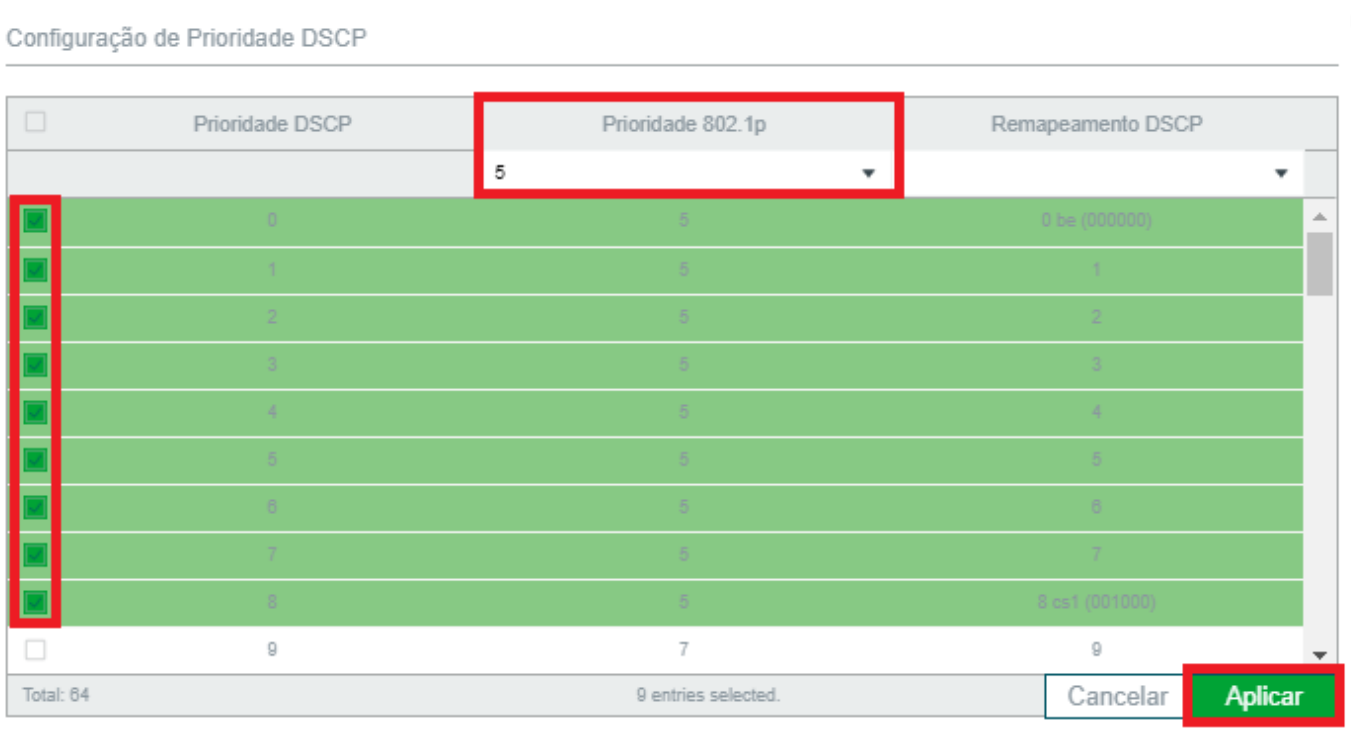
2. Vá até o menu **QoS > Classe de Serviço > Prioridade da Porta** para carregar a página a seguir. Configure o Modo Confiar para a porta 1/0/1 como Confiar DSCP. Clique em **Aplicar**.



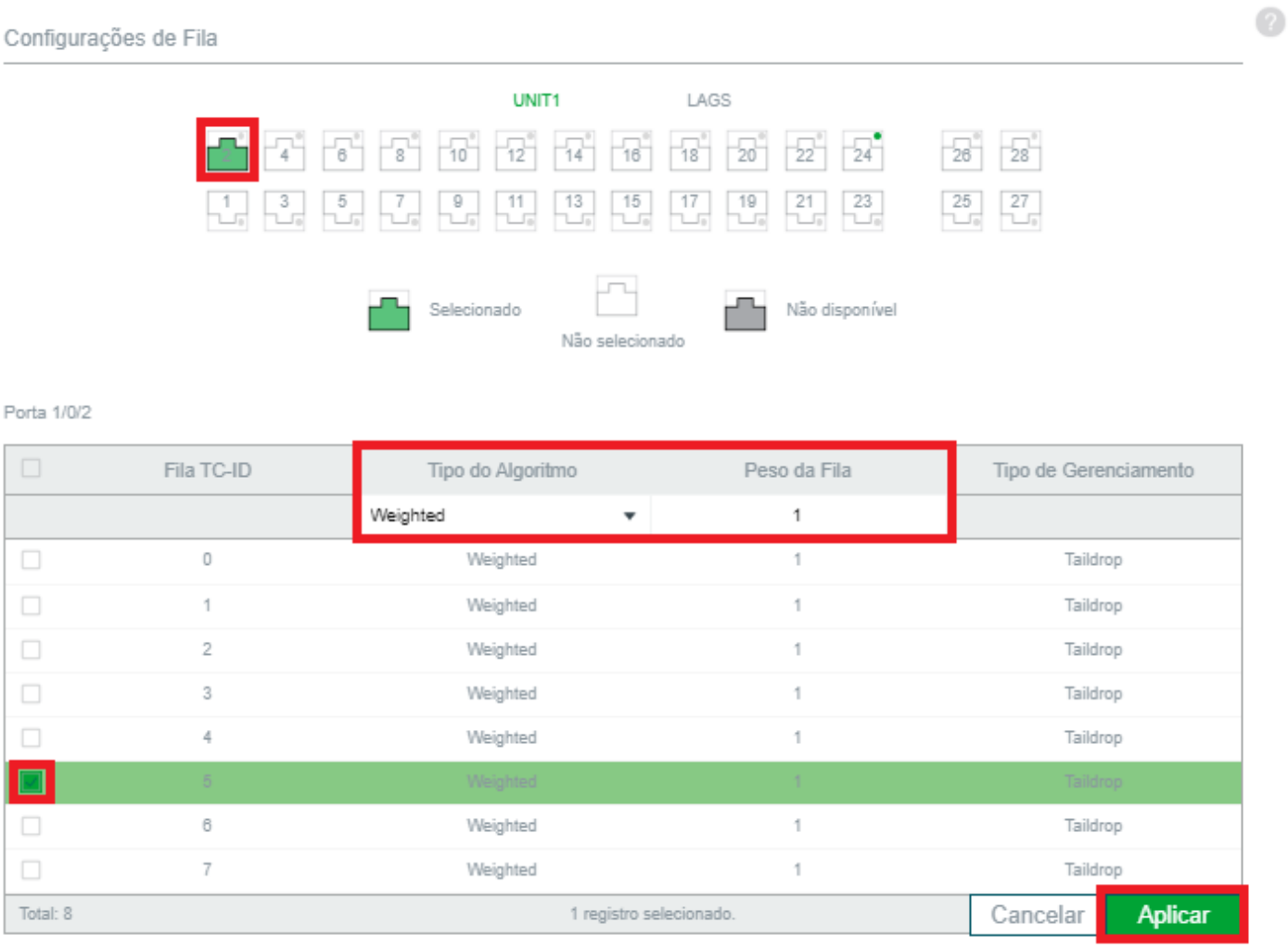
3. Vá até o menu **QoS > Classe de Serviço > Prioridade DSCP** para carregar a página a seguir. Especifique a prioridade 802.1p como 7 para prioridade 63 do DSCP. Clique em **Aplicar**.



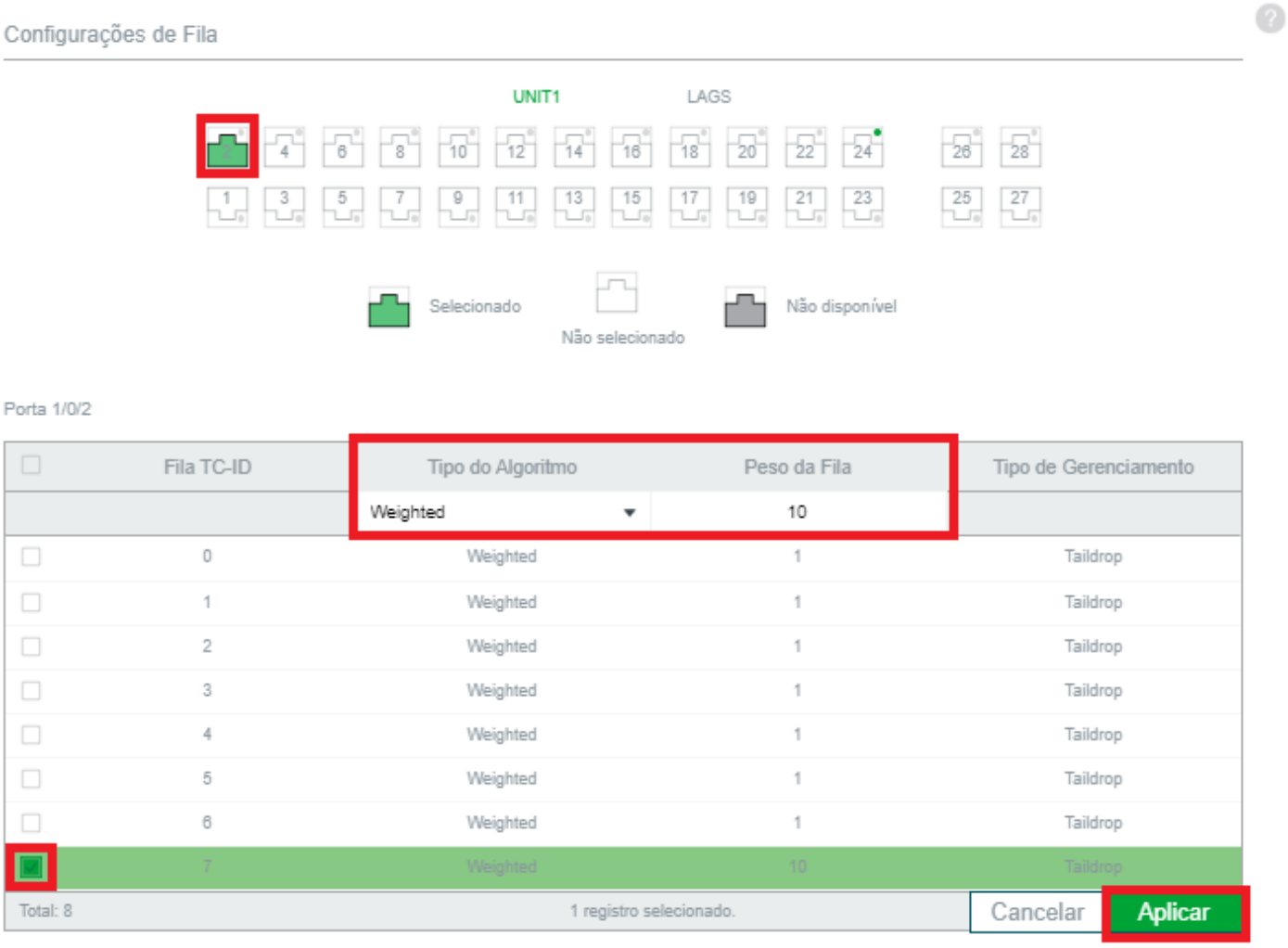
4. Especifique a prioridade 802.1p como 5 para as outras prioridades do DSCP.



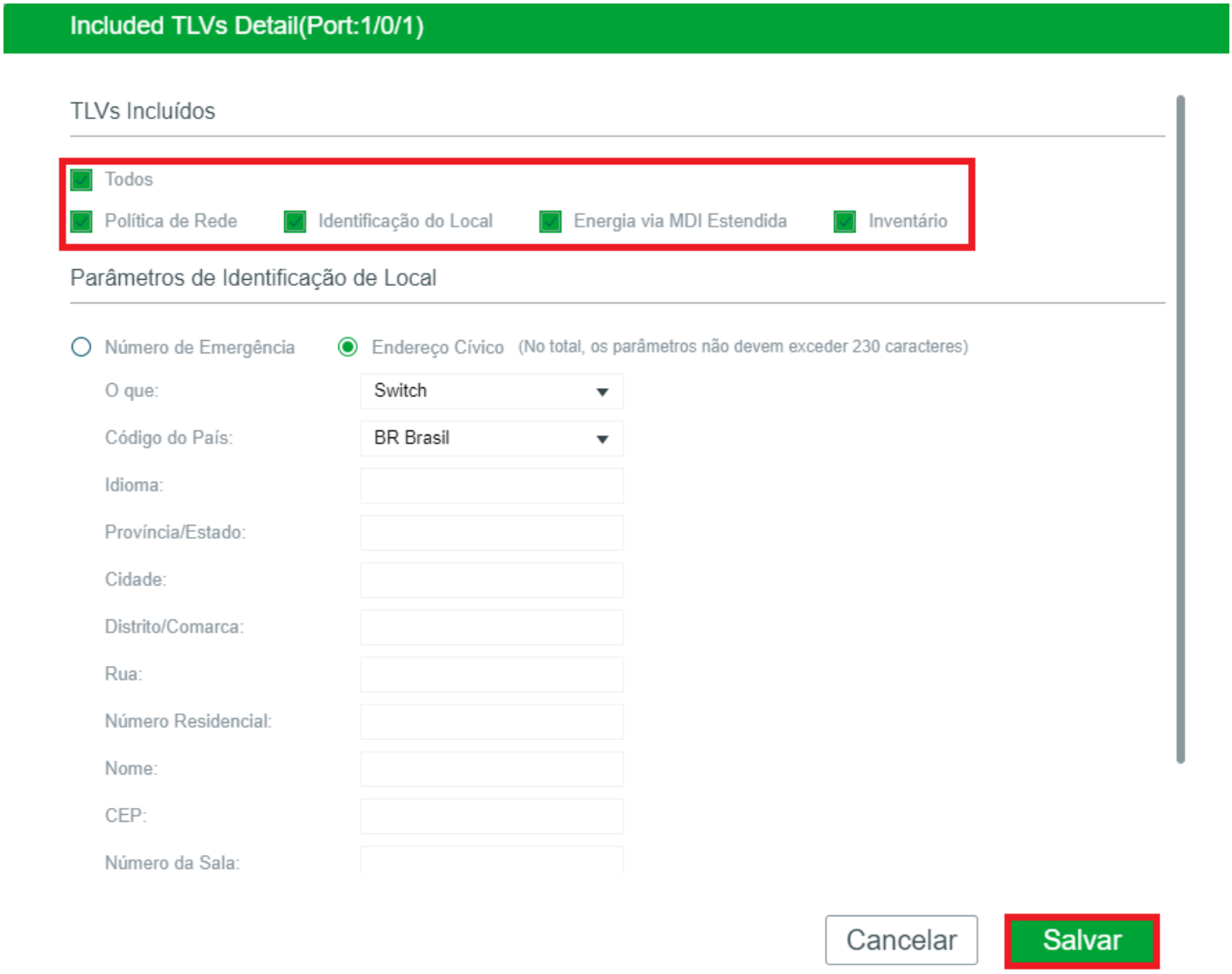
5. Vá até o menu **QoS > Classe de Serviço > Alg. Enfileiramento** para carregar a página a seguir. Selecione a porta 1/0/2. Configure o Tipo do Algorítimo como Weighted e especifique o Peso da Fila como 1 para a TC-5. Clique em **Aplicar**.



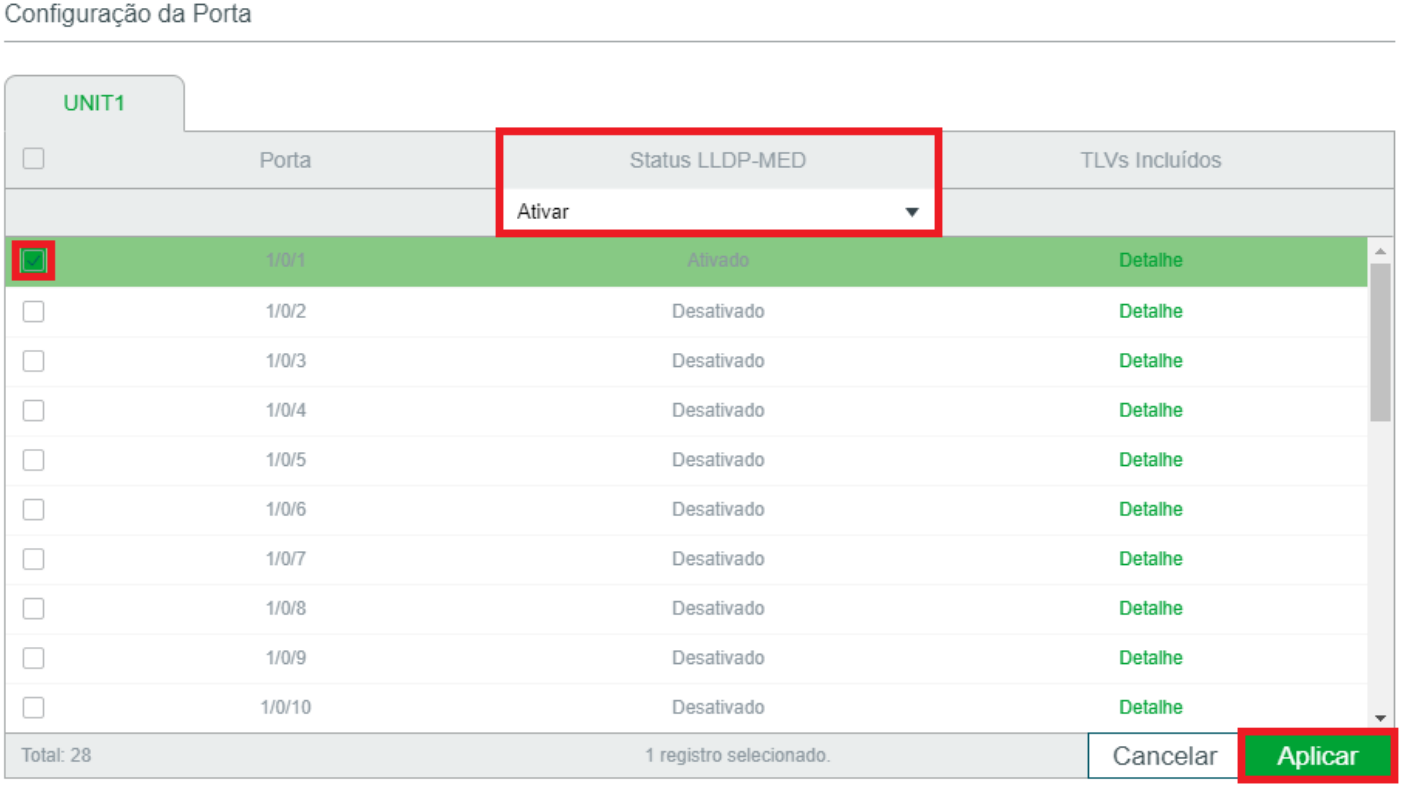
6. Selecione a porta 1/0/2. Configure o Tipo do Algorítimo como Weighted e especifique o Peso da fila como 10 para a TC-7. Clique em **Aplicar**.



7. Vá até o menu **FUNÇÕES L2 > LLDP > Configuração LLDP-MED > Configuração de Porta** clique em **Detalhe** da porta 1/0/1 para carregar a página a seguir. Cheque todos os TLVs Incluídos. Clique em **Salvar**.



8. Vá até o menu **FUNÇÕES L2 > LLDP > Configuração LLDP-MED > Configuração de Porta** para carregar a página a seguir. Habilite o LLDP-MED para a porta 1/0/1. Clique em **Aplicar**.



9. Clique em Salvar para salvar as configurações.

Apêndice: Configuração Padrão

As configurações padrão para Classe de serviço estão listadas nas tabelas a seguir.

Configuração Padrão da configuração de Prioridade de Porta.

Parâmetros	Configurações Padrão
Prioridade 802.1p	0
Modo Confiar	Não confiável

Configuração Padrão da configuração do 802.1p Aguardar Mapeamento.

Prioridade 802.1p	Fila
0	TC1
1	TC0
2	TC2
3	TC3
4	TC4
5	TC5
6	TC6

7	TC7

Configuração Padrão da configuração do 802.1p Remap.

Prioridade 802.1p Original	Nova Prioridade 802.1p
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

Configuração Padrão da configuração do mapeamento 802.1p para DSCP.

DSCP	Prioridade 802.1p
0 ao 7	0
8 ao 15	1
16 ao 23	2
24 ao 31	3
32 ao 39	4
40 ao 47	5
48 ao 55	6
56 ao 63	7

Configuração Padrão da configuração do remapeamento DSCP.

DSCP Original	Novo DSCP	DSCP Original	Novo DSCP	DSCP Original	Novo DSCP
0	0 be (000000)	22	22 af23(010110)	44	44
1	1	23	23	45	45
2	2	24	24 cs3 (011000)	46	46 ef (101110)
3	3	25	25	47	47
4	4	26	26 af31(011010)	48	48 cs6 (110000)
5	5	27	27	49	49

6	6	28	28 af32 (011100)	50	50
7	7	29	29	51	51
8	8 cs1 (001000)	30	30 af33 (011110)	52	52
9	9	31	31	53	53
10	10 af11 (001010)	32	32 cs4 (100000)	54	54
11	11	33	33	55	55
12	12 af12 (001100)	34	34 af41 (100010)	56	56 cs7 (111000)
13	13	35	35	57	57
14	14 af13 (001110)	36	36 af42 (100100)	58	58
15	15	37	37	59	59
16	16 cs2 (010000)	38	38 af43 (100110)	60	60
17	17	39	39	61	61
18	18 af21 (010010)	40	40 cs5 (101000)	62	62
19	19	41	41	63	63
20	20 af22 (010100)	42	42		
21	21	43	43		

Configuração Padrão das configurações do Agendador.

Parâmetros	**Configurações Padrão**
Tipo do Agendador	Ponderado
Aguardar Peso	1
Tipo de gerenciamento	Taildrop

Configuração Padrão das configurações de Controle de Largura de Banda.

Parâmetros	**Configurações Padrão**
Taxa de Ingresso (0-1.000.000kbps)	0
Taxa de Egresso (0-1.000.000kbps)	0

Configuração Padrão das configurações de Storm Control.

Parâmetros	**Configurações Padrão**
Modo de taxa	Kbps
Broadcast Threshold	0

Multicast Threshold	0
Threshold de Quadro UL	0
Ação	Drop
Recover time	0

As configurações padrão para VLAN Voz estão listadas nas tabelas a seguir.

Configuração Padrão das configurações globais.

Parâmetros	Configurações Padrão
VLAN Voz	Desabilitada
ID da VLAN	Nenhum
Prioridade	7

Configuração Padrão das configurações de porta.

Parâmetros	Configurações Padrão
VLAN Voz	Desabilitada

Configuração Padrão das configurações da tabela OUI.

OUI	Estado	Descrição
00:01:E3	Padrão	SIEMENS
00:03:6B	Padrão	CISCO1
00:12:43	Padrão	CISCO2
00:0F:E2	Padrão	H3C
00:60:B9	Padrão	NITSUKO
00:D0:1E	Padrão	PINTEL
00:E0:75	Padrão	VERILINK
00:E0:BB	Padrão	3COM
00:04:0D	Padrão	AVAYA1
00:1B:4F	Padrão	AVAYA2
00:04:13	Padrão	SNOM

As configurações padrão para Auto VoIP estão listadas na tabela a seguir

Configuração Padrão das configurações do Auto VoIP.

Parâmetros	Configurações Padrão

Modo da Interface	Desabilitada
Valor	Nenhum
CoS Override mode	Desativado
Operational Status	Desativado

SEGURANÇA DE ACESSO

Visão Geral

A segurança de acesso fornece diferentes medidas de segurança para acessar o switch remotamente, a fim de aprimorar a segurança do gerenciamento de configuração.

Funções Suportadas

Controle de acesso

Esta função é usada para controlar o acesso dos usuários ao switch com base no endereço IP, endereço MAC ou porta.

HTTP

Esta função é baseada no protocolo HTTP. Ele pode permitir ou negar aos usuários o acesso ao switch através de um navegador da web.

HTTPS

Esta função é baseada no protocolo SSL ou TLS da camada de transporte. Ele suporta um acesso de segurança através de um navegador da web.

SSH

Essa função é baseada no protocolo SSH, um protocolo de segurança estabelecido nas camadas de aplicação e transporte. A função SSH é semelhante a uma conexão telnet, mas o SSH pode fornecer maior segurança da informação e autenticação.

Telnet

Esta função é baseada no protocolo Telnet através do protocolo TCP / IP. Com o Telnet, os usuários podem fazer logon no switch remotamente.

Configurações de Segurança de Acesso

Com as configurações de segurança de acesso, você pode:

- Configurar o recurso de controle de acesso
- Configurar o recurso HTTP
- Configurar o recurso HTTPS
- Configurar o recurso SSH
- Configurar a função Telnet

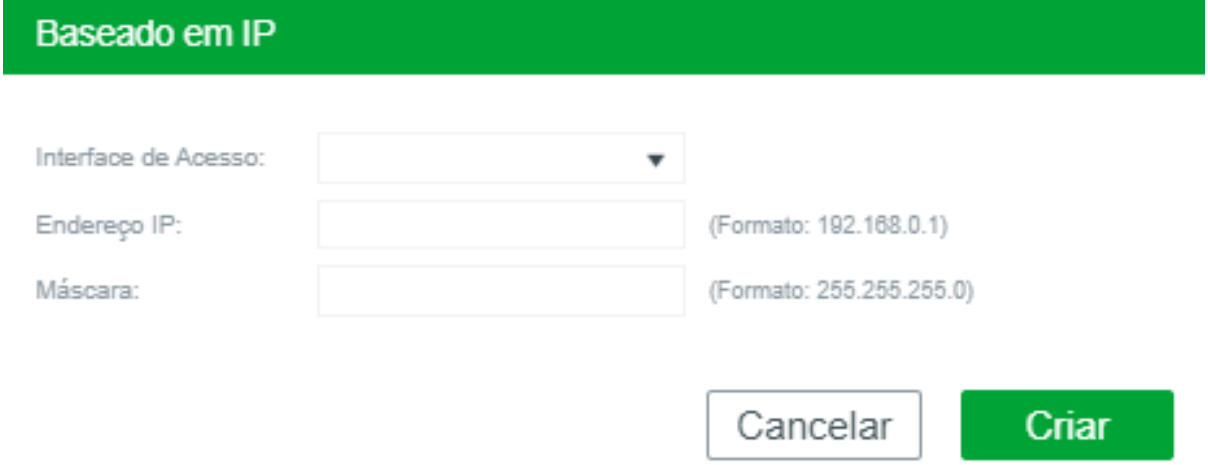
Configurando a função de Controle de Acesso

Escolha o menu **SEGURANÇA > Segurança de Acesso > Controle de Acesso** para carregar a seguinte página.

1. Na seção **Configuração Global**, ative o Controle de Acesso, selecione um modo de controle e clique em **Aplicar**.

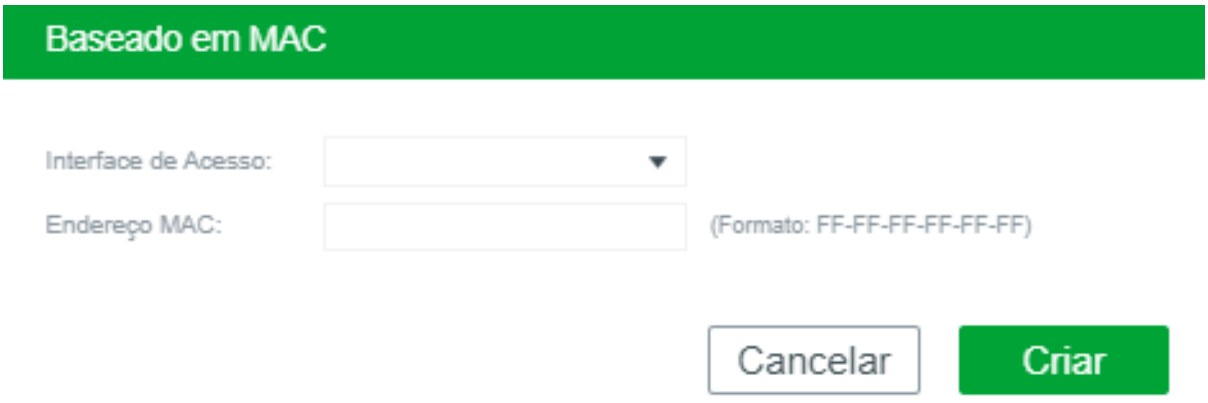
Modo de Controle	Selecione o modo de controle para que os usuários efetuem login na página de gerenciamento da web. **Baseado em IP:** somente os usuários dentro do intervalo de IP que você definir aqui têm permissão para acessar o switch. **Baseado em MAC:** somente os usuários com o endereço MAC definido aqui têm permissão para acessar o switch. **Baseado em porta:** somente os usuários que se conectam às portas definidas aqui têm permissão para acessar o switch.

2. Na seção **Configuração de Entrada**, clique em Adicionar para adicionar uma entrada de Controle de Acesso. Quando o modo baseado em IP é selecionado, a seguinte janela será exibida.



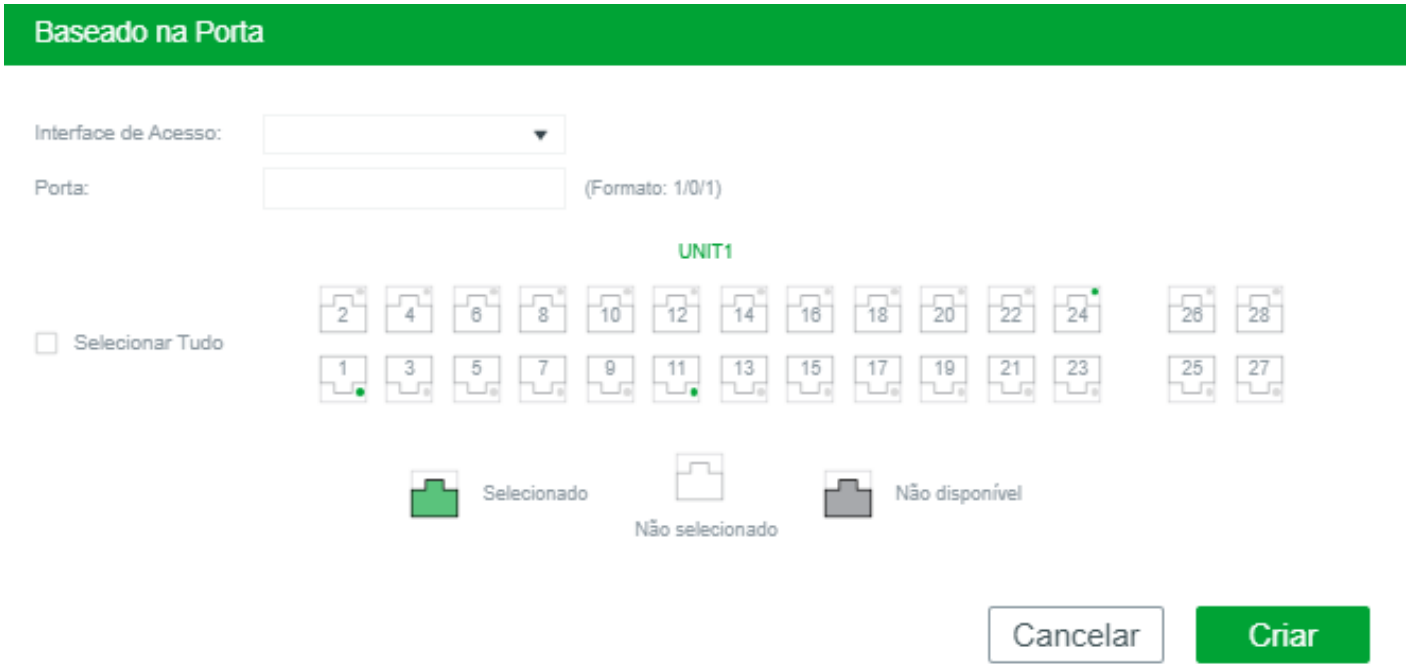
Interface de Acesso	Selecione a interface para controlar os métodos de acesso dos usuários. **SNMP:** uma função para gerenciar os dispositivos de rede via NMS. **Telnet:** um tipo de conexão para os usuários fazerem login remoto. **SSH:** um tipo de conexão baseado no protocolo SSH. **HTTP:** um tipo de conexão baseado no protocolo HTTP. **HTTPS:** um tipo de conexão baseado no protocolo SSL. **Ping:** um protocolo de comunicação para testar a conexão da rede.
Endereço IP / Máscara	Digite o endereço IP e a máscara para especificar um intervalo de IP. Somente os usuários dentro desse intervalo de IP podem acessar o switch.

Quando o modo baseado em MAC é selecionado, a seguinte janela será exibida.



Interface de Acesso	Selecione a interface para controlar os métodos de acesso dos usuários. **SNMP:** uma função para gerenciar os dispositivos de rede via NMS. **Telnet:** um tipo de conexão para os usuários fazerem login remoto. **SSH:** um tipo de conexão baseado no protocolo SSH. **HTTP:** um tipo de conexão baseado no protocolo HTTP. **HTTPS:** um tipo de conexão baseado no protocolo SSL. **Ping:** um protocolo de comunicação para testar a conexão da rede.
Endereço MAC	Especifique o endereço MAC. Somente os usuários com o endereço MAC correto podem acessar o switch.

Quando o modo baseado na Porta é selecionado, a seguinte janela será exibida.



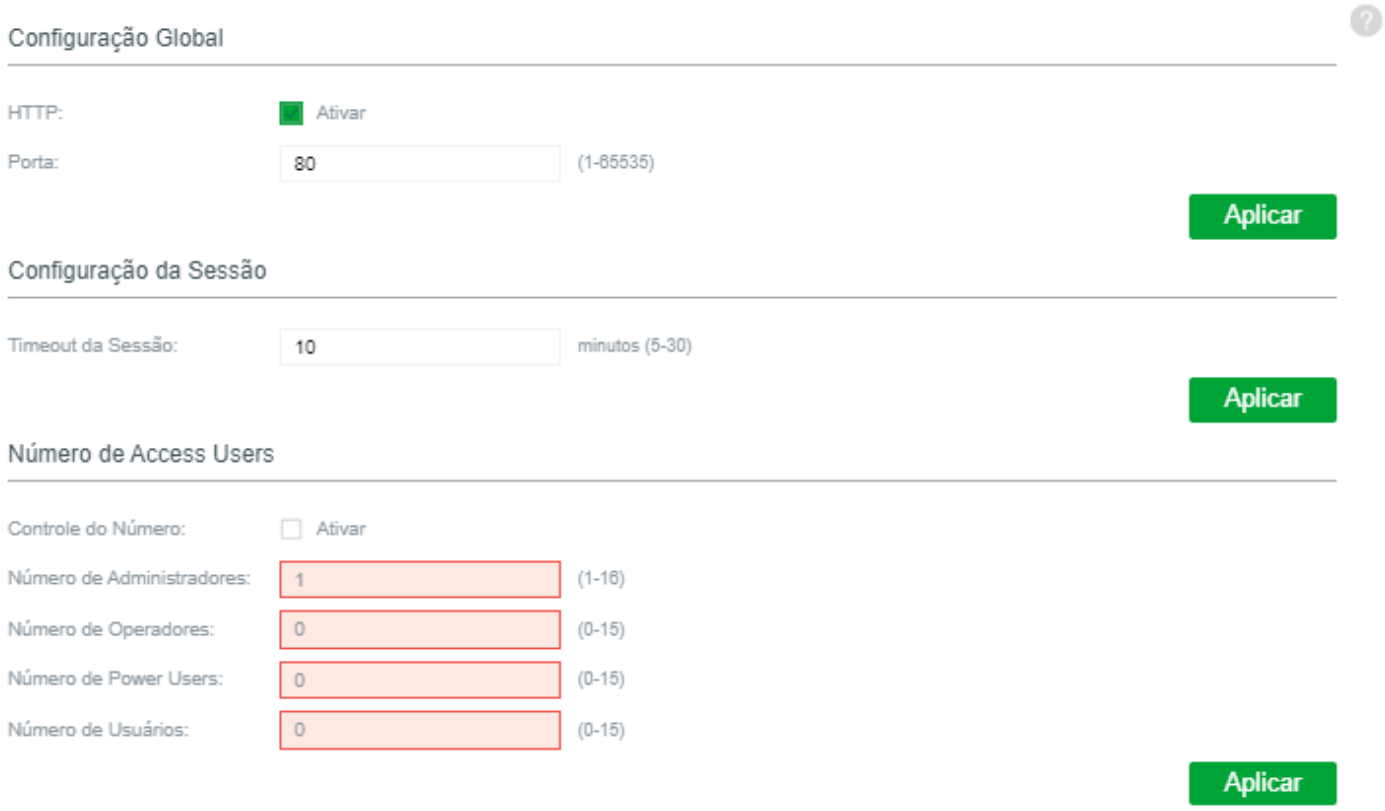
Interface de Acesso	Selecione a interface para controlar os métodos de acesso dos usuários. **SNMP:** uma função para gerenciar os dispositivos de rede via NMS. **Telnet:** um tipo de conexão para os usuários fazerem login remoto. **SSH:** um tipo de conexão baseado no protocolo SSH. **HTTP:** um tipo de conexão baseado no protocolo HTTP. **HTTPS:** um tipo de conexão baseado no protocolo SSL. **Ping:** um protocolo de comunicação para testar a conexão da rede.

Porta	Selecione uma ou mais portas para configurar. Somente os usuários conectados a essas portas têm permissão para acessar o switch.

3. Clique em **Criar**. Em seguida, você pode visualizar as entradas criadas na tabela de Configuração de Entrada.

Configurando a Função HTTP

Escolha o menu **SEGURANÇA > Segurança do Acesso > Configuração HTTP** para carregar a seguinte página.



1. Na seção **Configuração Global**, ative a função HTTP, especifique a porta usada para HTTP e clique em **Aplicar** para ativar a função HTTP.

HTTP	A função HTTP é baseada no protocolo HTTP. Ele permite que os usuários gerenciem o switch através de um navegador da web.
Porta	Especifique o número da porta para o serviço HTTP.

2. Na seção **Configuração da sessão**, especifique o timeout da sessão e clique em **Aplicar**.

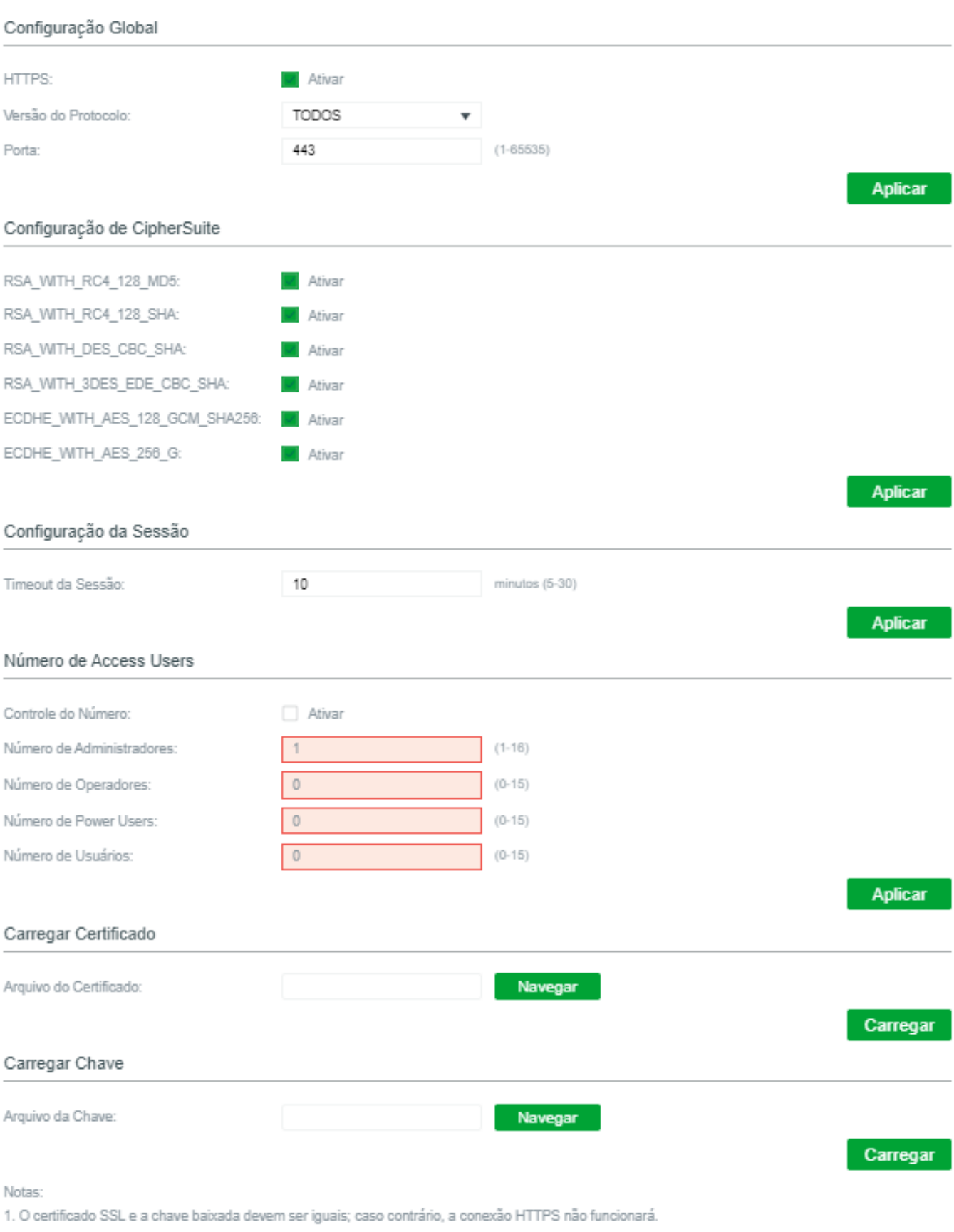
Timeout da Sessão	O sistema efetuará logout automaticamente se os usuários não fizerem nada dentro do tempo limite da sessão.

3. Na seção **Número de Access Users**, ative a função Controle de número, especifique os seguintes parâmetros e clique em **Aplicar**.

Controle do Número	Ativar ou desativar o controle de número. Com esta opção ativada, você pode controlar o número de usuários que efetuam logon na página de gerenciamento da web ao mesmo tempo. O número total de usuários não deve ser superior a 16.
Número de Administradores	Especifique o número máximo de usuários cujo nível de acesso é Administrador.
Número de Operadores	Especifique o número máximo de usuários cujo nível de acesso é Operador.
Número de Power Users	Especifique o número máximo de usuários cujo nível de acesso é Usuário avançado.
Número de Usuários	Especifique o número máximo de usuários cujo nível de acesso é Usuário.

Configurando a Função HTTPS

Escolha o menu **SEGURANÇA > Segurança do Acesso > Configuração HTTPS** para carregar a seguinte página.



1. Na seção **Configuração Global**, ative a função HTTPS, selecione o protocolo que o switch suporta e especifique a porta usada pelo HTTPS. Clique em **Aplicar**.

HTTPS	Ative ou desative a função HTTPS. A função HTTPS é baseada no protocolo SSL ou TLS. Ela fornece uma conexão segura entre o cliente e o switch.

SSL Versão 3.0	Habilite ou desabilite o protocolo SSL Versão 3 no switch. SSL é um protocolo de transporte. Ele pode fornecer autenticação, criptografia e integridade de mensagens do servidor para permitir conexão HTTP segura.
TLS Versão 1.0	Habilite ou desabilite o protocolo TLS Versão 1 no switch. TLS é um protocolo de transporte atualizado de SSL. Ele suporta um algoritmo de criptografia diferente do SSL, portanto, TLS e SSL não são compatíveis. O TLS pode suportar uma conexão mais segura.

2. Na seção **Configuração de CipherSuite**, selecione o algoritmo a ser ativado e clique em **Aplicar**.

RSA_WITH_RC4_128_MD5	Troca de chaves com criptografia RC4 de 128 bits e MD5.
RSA_WITH_RC4_128_SHA	Troca de chaves com criptografia RC4 de 128 bits e SH4.
RSA_WITH_DES_CBC_SHA	Troca de chaves com DES-CBC para criptografia de mensagens e SHA.
RSA_WITH_3DES_EDE_CBC_SHA	Troca de chaves com 3DES e DES-EDE3-CBC para criptografia de mensagens e SHA.

3. Na seção **Configuração da sessão**, especifique o timeout da sessão e clique em **Aplicar**.

Timeout da Sessão	O sistema efetuará logout automaticamente se os usuários não fizerem nada dentro do tempo limite da sessão.

4. Na seção Número de Access Users, ative a função Controle de número, especifique os seguintes parâmetros e clique em **Aplicar**.

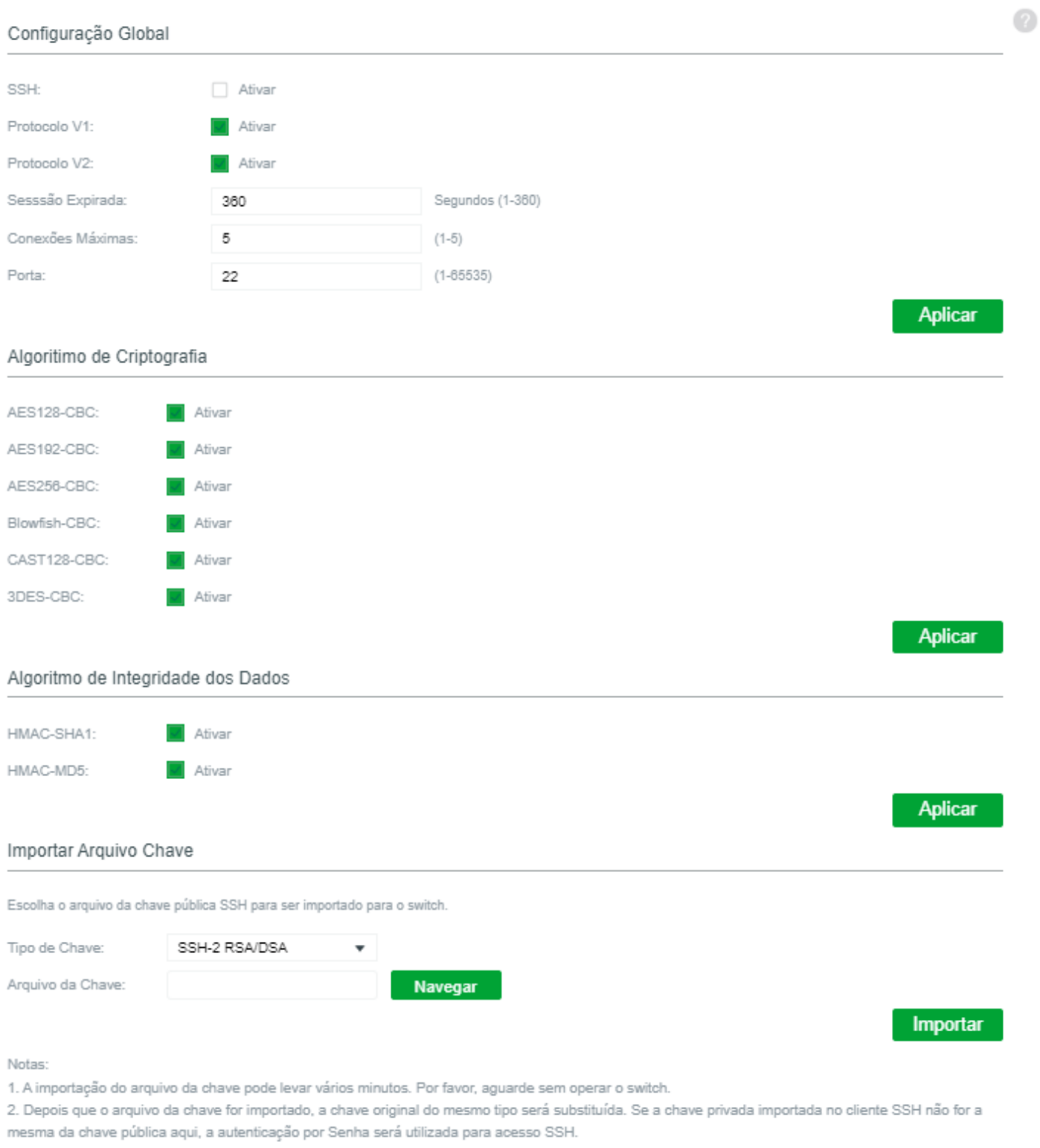
Controle do Número	Ativar ou desativar o controle de número. Com esta opção ativada, você pode controlar o número de usuários que efetuam logon na página de gerenciamento da web ao mesmo tempo. O número total de usuários não deve ser superior a 16.
Número de Administradores	Especifique o número máximo de usuários cujo nível de acesso é Administrador.
Número de Operadores	Especifique o número máximo de usuários cujo nível de acesso é Operador.
Número de Power Users	Especifique o número máximo de usuários cujo nível de acesso é Usuário avançado.
Número de Usuários	Especifique o número máximo de usuários cujo nível de acesso é Usuário.

5. Na seção **Carregar Certificado e Carregar Chave**, faça o download do certificado e da chave.

Arquivo do Certificado	Selecione o certificado desejado para fazer o download para o switch. O certificado deve ser codificado em BASE64. O certificado SSL e a chave baixados devem corresponder um ao outro, caso contrário, a conexão HTTPS não funcionará.
Arquivo da Chave	Selecione a chave desejada para fazer o download para o switch. A chave deve ser codificada em BASE64. O certificado SSL e a chave baixados devem corresponder um ao outro, caso contrário, a conexão HTTPS não funcionará.

Configurando a Função SSH

Escolha o menu **SEGURANÇA > Segurança do Acesso > Configuração SSH** para carregar a seguinte página.



1. Na seção **Configuração Global**, selecione **Ativar** para ativar a função SSH e especifique os seguintes parâmetros.

SSH	Selecione Ativar para ativar a função SSH. SSH é um protocolo que trabalha na camada de aplicação e na camada de transporte. Pode fornecer uma conexão remota segura com um dispositivo. É mais seguro que o protocolo Telnet, pois fornece criptografia.
Protocolo V1	Selecione Ativar para ativar a versão 1 do SSH.
Protocolo V2	Selecione Ativar para ativar a versão 2 do SSH.

Sessão Expirada	Especifique o tempo limite de inatividade. O sistema libera automaticamente a conexão quando o tempo acabar.
Sessão Expirada	Especifique o tempo limite de inatividade. O sistema libera automaticamente a conexão quando o tempo acabar.
Conexões Máximas	Especifique o número máximo de conexões com o servidor SSH. A nova conexão não será estabelecida quando o número de conexões atingir o número máximo definido.
Porta	Especifique a porta usada para SSH.

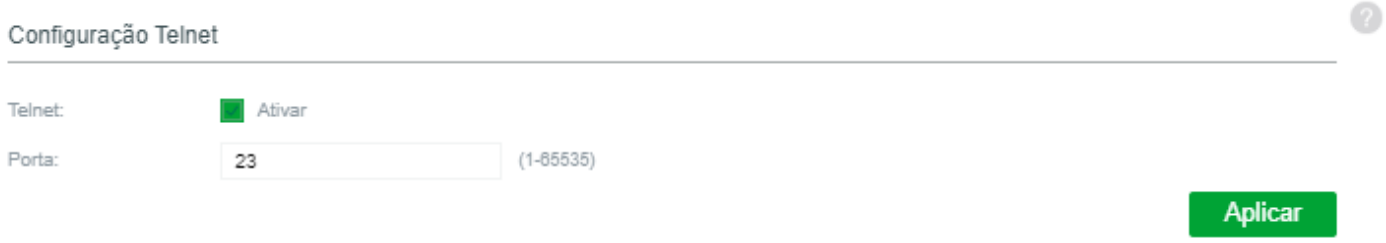
2. Na seção **Algoritmo de Criptografia**, ative o algoritmo de criptografia que você deseja que o switch suporte e clique em **Aplicar**.
3. Na seção **Algoritmo de Integridade dos Dados**, ative o algoritmo de integridade que você deseja que o switch suporte e clique em **Aplicar**.
4. Na seção **Importar Arquivo Chave**, selecione o tipo de chave na lista suspensa e clique em **Navegar** para baixar o arquivo de chave desejado.

Tipo de Chave	Selecione o tipo de chave. O algoritmo do tipo correspondente é usado para geração de chave e autenticação.
Arquivo da Chave	Selecione a chave pública desejada para fazer o download para o switch. O tamanho da chave do arquivo baixado varia de 512 a 3072 bits.

Pode demorar um tempo considerável para baixar o arquivo da chave. Aguarde sem qualquer operação.

Configurando a Função Telnet

Escolha o menu **SEGURANÇA > Segurança do Acesso > Configuração Telnet** para carregar a seguinte página.



Ative a função Telnet e clique em **Aplicar**.

Telnet	Selecione Ativar para efetivar a função Telnet. A função Telnet é baseada no protocolo Telnet através do protocolo TCP / IP. Ele permite que os usuários façam logon no switch remotamente.
Porta	Especifique a porta usada para o Telnet.

Apêndice: Configuração Padrão

As configurações padrão da Segurança de Acesso estão listadas nas tabelas a seguir.

Parâmetros	**Configurações Padrão**
Controle de Acesso	Desativado

HTTP

Parâmetros	**Configurações Padrão**
HTTP	Ativado
Porta	80
Timeout da Sessão	10 minutos
Controle do Número	Desativado

HTTPS

Parâmetros	**Configurações Padrão**
HTTPS	Ativado
SSL Versão 3	Ativado
TLS Versão 1	Ativado
Porta	443
RSA_WITH_RC4_128_MD5	Ativado
RSA_WITH_RC4_128_SHA	Ativado
RSA_WITH_DES_CBC_SHA	Ativado
RSA_WITH_3DES_EDE_CBC_SHA	Ativado
Timeout da Sessão	10 minutos
Controle do Número	Desativado

SSH

Parâmetros	Configurações Padrão
SSH	Desativado
Protocolo V1	Ativado
Protocolo V2	Ativado
Timeout	120 segundos
Conexões Máximas	5
Porta	22
AES128-CBC	Ativado
AES192-CBC	Ativado
AES256-CBC	Ativado
Blowfish-CBC	Ativado
CAST128-CBC	Ativado
3DES-CBC	Ativado
HMAC-SHA1	Ativado
HMAC-MD5	Ativado
Tipo de Chave	SSH-2 RSA/DSA

Telnet

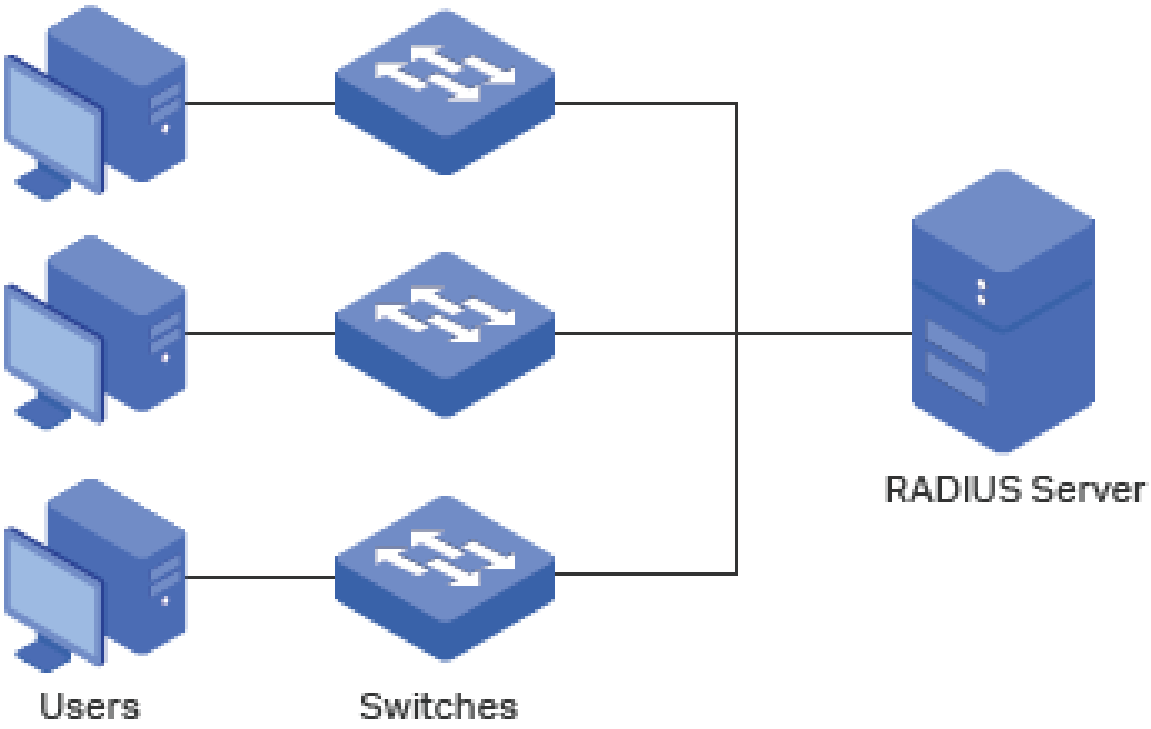
Parâmetros	Configurações Padrão
Telnet	Ativado
Porta	23

AAA

Visão Geral

AAA significa autenticação, autorização e contabilidade. No switch Intelbras, esse recurso é usado principalmente para autenticar os usuários que tentam efetuar login no switch ou obter privilégios administrativos. O administrador pode criar contas de convidado e uma senha de ativação para outros usuários. Os convidados não têm privilégios administrativos sem o fornecimento da senha de ativação.

AAA fornece um método de autenticação seguro e eficiente. A autenticação pode ser processada localmente no switch ou centralmente nos servidores RADIUS/TACACS +. Como mostra a figura a seguir, o administrador da rede pode configurar centralmente as contas de gerenciamento dos switches no servidor RADIUS e usar esse servidor para autenticar os usuários que tentam acessar o switch ou obter privilégios administrativos.



Configurações AAA

No recurso AAA, a autenticação pode ser processada localmente no switch ou centralmente nos servidores RADIUS / TACACS +. Para garantir a estabilidade do sistema de autenticação, você pode configurar vários servidores e métodos de autenticação ao mesmo tempo. Este capítulo apresenta como configurar esse tipo de autenticação abrangente no AAA.

Para concluir a configuração, siga estas etapas:

1. Adicione os servidores.
2. Configure os grupos de servidores.
3. Configure a lista de métodos.
4. Configure a lista de aplicativos AAA.
5. Configure a conta para login e a habilite a senha.

Diretrizes de configuração

Os conceitos básicos e o mecanismo de trabalho da AAA são os seguintes:

- Configuração padrão AAA

  Por padrão, o recurso AAA está ativado e não pode ser desativado.

- Grupo de Servidores

  Vários servidores executando o mesmo protocolo podem ser adicionados a um grupo de servidores, e os servidores no grupo autenticarão os usuários na ordem em que forem adicionados. O servidor adicionado primeiro ao grupo tem a maior prioridade e é responsável pela autenticação em circunstâncias normais. Se o primeiro falhar ou não

responder à solicitação de autenticação por algum motivo, o segundo servidor começará a funcionar para autenticação e assim por diante.

- Lista de Métodos

  Um grupo de servidores é considerado como um método, e a autenticação local é outro método. Vários métodos podem ser configurados para formar uma lista de métodos. A opção usa o primeiro método na lista de métodos para autenticar o usuário e, se esse método falhar em responder, a opção seleciona o próximo método. Esse processo continua até que o usuário tenha uma comunicação bem-sucedida com um método ou até que todos os métodos definidos estejam esgotados. Se a autenticação for bem-sucedida ou o servidor seguro ou o switch local negar o acesso do usuário, o processo de autenticação será interrompido e nenhum outro método será tentado.

  São fornecidos dois tipos de lista de métodos: a lista de métodos de autenticação do login para usuários de todos os tipos acessarem a opção e a lista de métodos para habilitar convidados a obterem privilégios administrativos.

- Lista de aplicações AAA

  O switch suporta as seguintes aplicações de acesso: Telnet, SSH e HTTP. Você pode selecionar as listas de métodos de autenticação configuradas para cada aplicativo.

Adicionando Servidores

Você pode adicionar um ou mais servidores RADIUS / TACACS + no switch para autenticação. Se vários servidores forem adicionados, o servidor adicionado primeiro ao grupo terá a maior prioridade e autentica os usuários que estão tentando acessar o switch. Os outros atuam como servidores de backup, caso o primeiro falhe.

Adicionando servidor RADIUS

Escolha o menu **SEGURANÇA > AAA > Configuração RADIUS** e clique em ⊕ Adicionar para carregar a seguinte página.

Siga os seguintes passos para adicionar o servidor RADIUS:

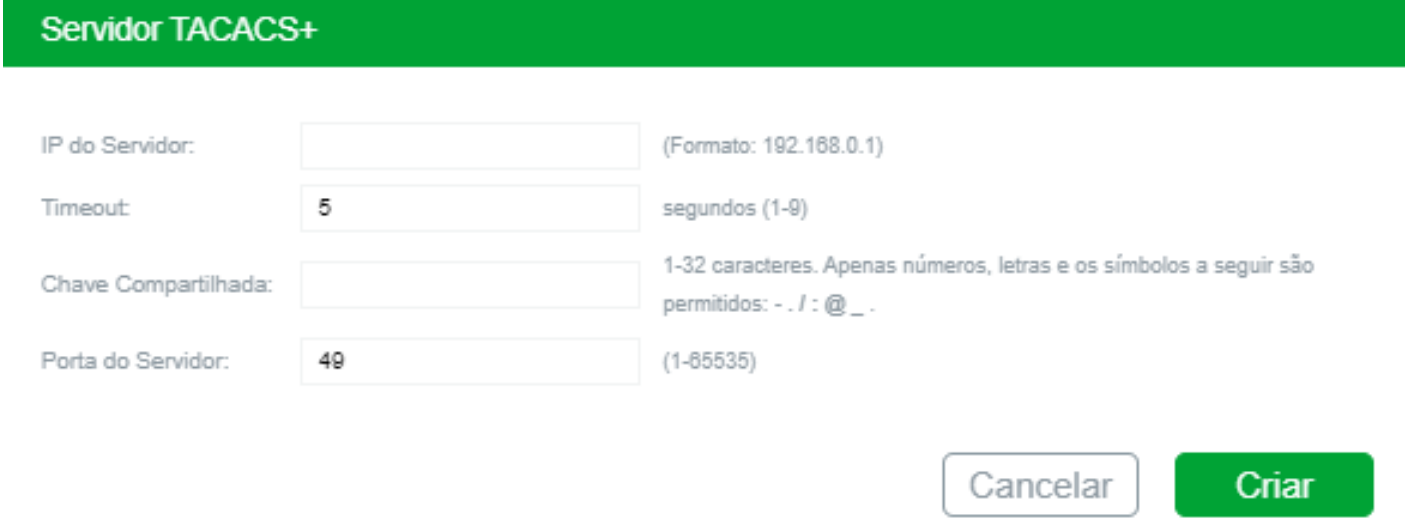
1. Configure os seguintes parâmetros.

IP do Servidor	Digite o endereço IP do servidor que está executando o protocolo seguro RADIUS.
Chave Compartilhada	Digite a chave compartilhada entre o servidor RADIUS e o switch. O servidor RADIUS e o switch usam a cadeia de chaves para criptografar senhas e trocar respostas.
Porta de Autenticação	Especifique a porta de destino UDP no servidor RADIUS para solicitações de autenticação. A configuração padrão é 1812.
Porta de Contabilidade	Especifique a porta de destino UDP no servidor RADIUS para solicitações de contabilidade. A configuração padrão é 1813. Geralmente, é usada no recurso 802.1x.
Retransmitir	Especifique o número de vezes que uma solicitação é reenviada para o servidor se o servidor não responder. A configuração padrão é 2.
Timeout	Especifique o intervalo de tempo que o switch espera que o servidor responda antes de reenviar. A configuração padrão é 5 segundos.
Identificador NAS	Especifique o nome do NAS (servidor de acesso à rede) a ser contido nos pacotes RADIUS para identificação. Varia de 1 a 31 caracteres. O valor padrão é o endereço MAC do switch. Geralmente, o NAS indica o próprio switch.

2. Chique em **Criar** para adicionar o servidor RADIUS no switch.

Adicionando servidor TACACS+

Escolha o menu **SEGURANÇA > AAA > Configuração TACACS+** e clique em Adicionar para carregar a seguinte página.



Siga os seguintes passos para adicionar o servidor TACACS+:

1. Configure os seguintes parâmetros.

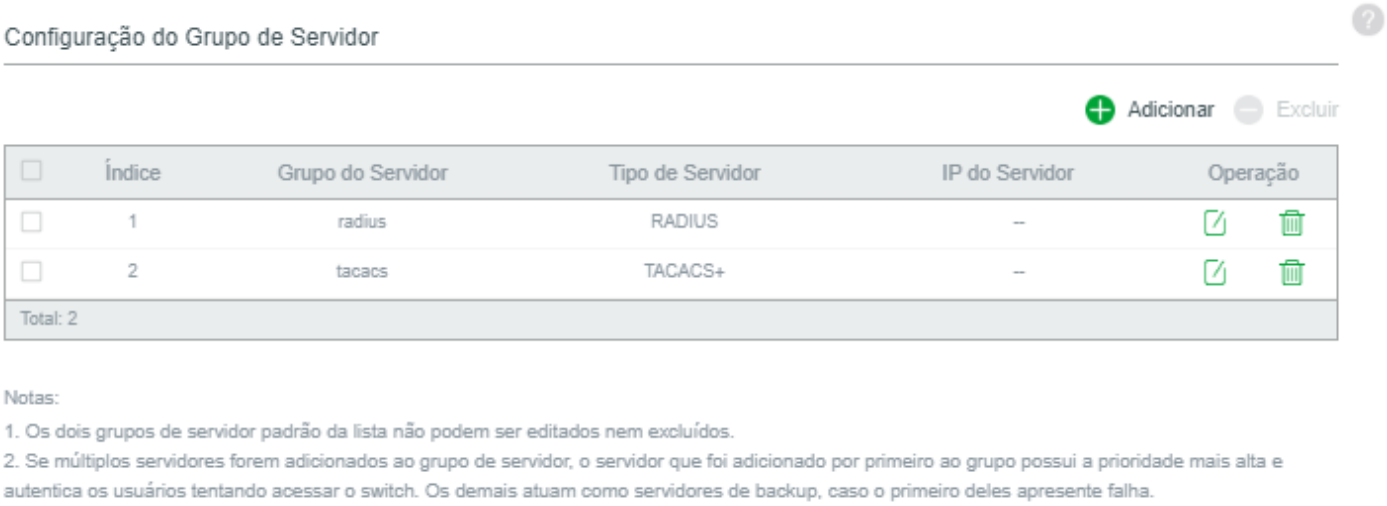
IP do Servidor	Digite o endereço IP do servidor que está executando o protocolo seguro TACACS+.
Timeout	Especifique o intervalo de tempo que o switch espera que o servidor responda antes de reenviar. A configuração padrão é 5 segundos.
Chave Compartilhada	Digite a chave compartilhada entre o servidor TACACS + e o switch. O servidor TACACS + e o switch usam a cadeia de chaves para criptografar senhas e trocar respostas.
Porta do Servidor	Especifique a porta TCP usada no servidor TACACS + para AAA. A configuração padrão é 49.

2. Clique em **Criar** para adicionar o servidor TACACS+ no switch.

Configurando Grupos de Servidor

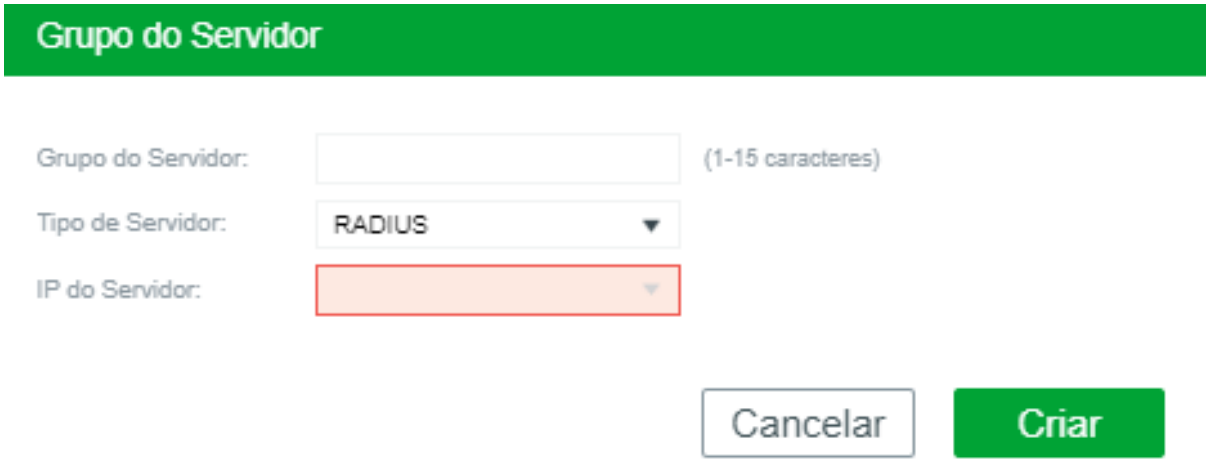
O switch possui dois grupos de servidores internos, um para servidores RADIUS e outro para servidores TACACS +. Os servidores que executam o mesmo protocolo são adicionados automaticamente ao grupo de servidores padrão. Você pode adicionar novos grupos de servidores, conforme necessário.

Escolha o menu **SEGURANÇA > AAA > Grupo Servidor** para carregar a seguinte página.



Existem dois grupos de servidores padrão na lista. Você pode editar os grupos de servidores padrão ou siga estas etapas para configurar um novo grupo de servidores:

1. Clique em Adicionar e a seguinte janela será exibida.



Configure os seguintes parâmetros:

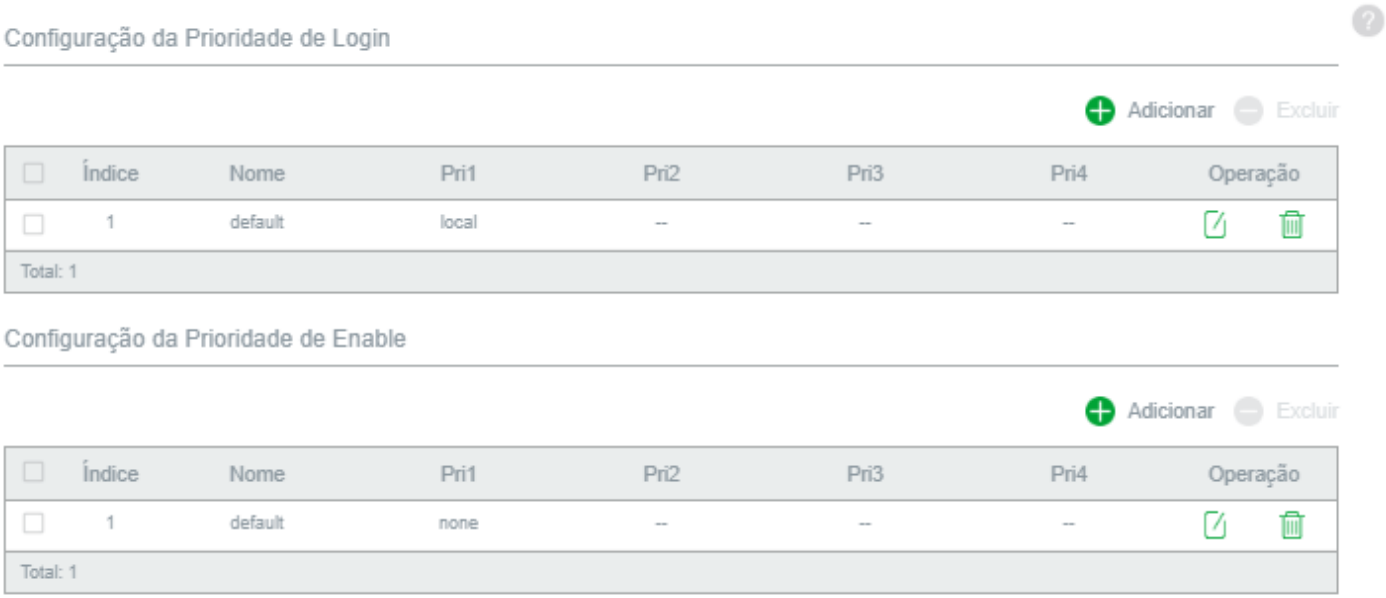
Grupo do Servidor	Especifique o nome do grupo servidor.
Tipo do Servidor	Selecione o tipo de servidor para o grupo. As seguintes opções são fornecidas: RADIUS e TACACS +.
IP do Servidor	Selecione o endereço IP do servidor que será adicionado ao grupo de servidores.

2. Clique em **Criar**.

Configurando a Lista de Métodos

Uma lista de métodos descreve os métodos de autenticação e sua sequência para autenticar os usuários. O switch suporta a Lista de Método de Autenticação do Login para usuários de todos os tipos para obter acesso ao switch, e a lista de Método de Ativar Autenticação para que os convidados obtenham privilégios administrativos.

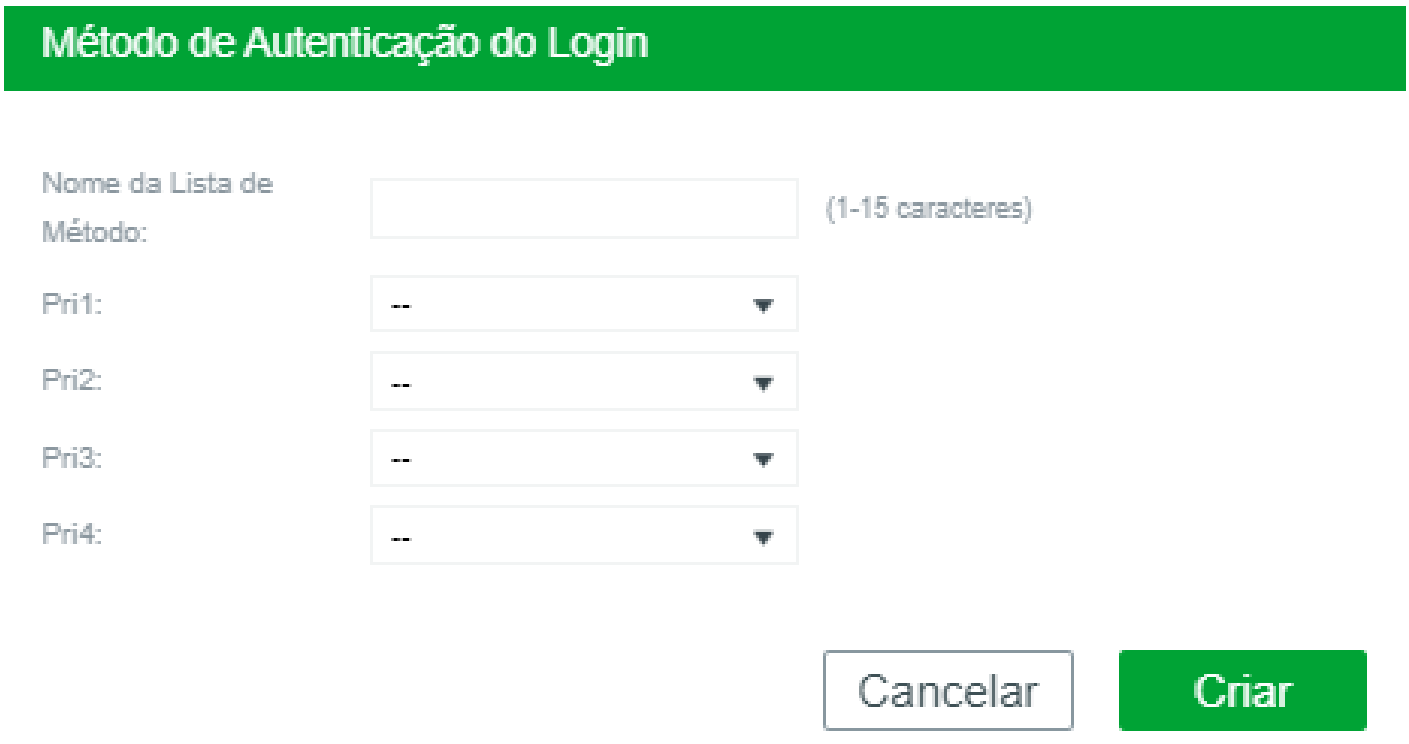
Escolha o menu **SEGURANÇA > AAA > Configuração de Método** para carregar a seguinte página.



Existem dois métodos padrão, para a autenticação de logon e a autenticação de ativação.

Você pode editar os métodos padrão ou siga estas etapas para adicionar um novo método:

1. Clique em Adicionar na seção Configuração do Método de Autenticação do Login ou na seção Configuração do Método de Ativar Autenticação para adicionar o tipo correspondente de lista de métodos. A janela a seguir será exibida.



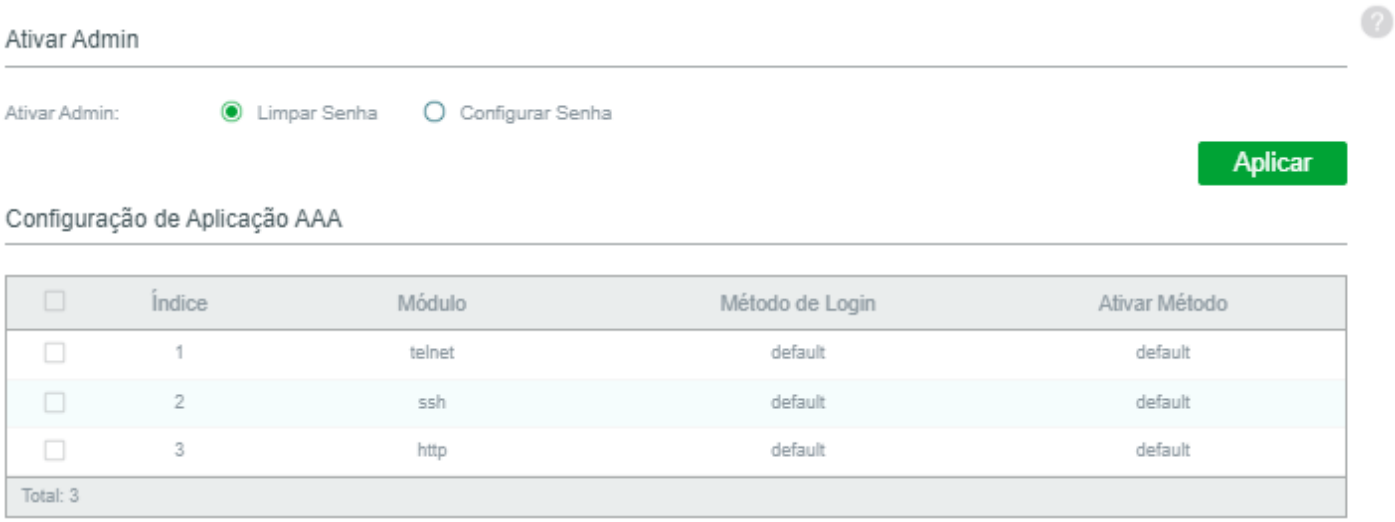
Configure os parâmetros para o método a ser adicionado.

Nome da Lista de Método	Especifique um nome do método.
Pri1 – Pri4	Especifique os métodos de autenticação em ordem. O método com prioridade 1 autentica um usuário primeiro, o método com prioridade 2 é tentado se o método anterior não responder e assim por diante. **local:** use o banco de dados local no switch para autenticação. **nenhum:** nenhuma autenticação é usada. **radius:** use o servidor/grupos de servidores RADIUS remotos para autenticação. **tacacs:** use os servidores/grupos de servidores TACACS + remotos para autenticação. **Outros grupos de servidores definidos pelo usuário:** use os grupos de servidores definidos pelo usuário para autenticação.

2. Clique em **Criar** para adicionar o novo método.

Configurando Lista de Aplicação AAA

Escolha o menu **SEGURANÇA > AAA > Configuração Global** para carregar a seguinte página.



Siga os seguintes passos para configurar a aplicação AAA.

1. Na seção **Configuração de Aplicação AAA**, selecione um método de acesso e configure o método de Login e o método Ativar.

Módulo	Exibe os aplicativos configuráveis no switch: telnet, SSH e HTTP.
Método de Login	Selecione uma lista de métodos de Login configurada anteriormente. Essa lista de métodos autentica os usuários que tentam efetuar login no switch.

Ativar Método	Selecione uma lista de métodos Ativar configurada anteriormente. Essa lista de métodos autentica os usuários que tentam obter privilégios administrativos.

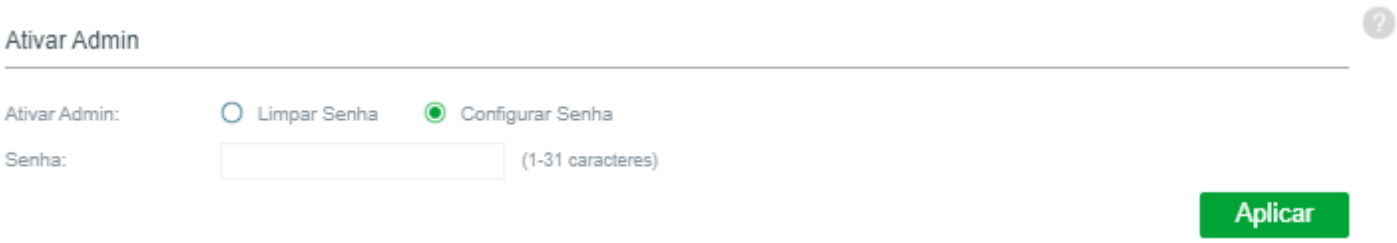
2. Clique em **Aplicar**.

Configurando Conta de Login e Senha de Enable

A conta de login e a senha de Enable podem ser configuradas localmente no switch ou centralmente nos servidores RADIUS/TACACS+.

- **No switch**

  O nome de usuário e a senha locais para login podem ser configurados no recurso Gerenciamento de usuários. Para detalhes, consulte Sistema de Gestão. Para configurar a senha local para obter privilégios administrativos, escolha o menu **SEGURANÇA> AAA> Configuração Global** para carregar a página a seguir.



  Existem duas opções: Limpar Senha e Configurar Senha. Você pode escolher se a senha Ativar Admin é necessária quando os convidados tentam obter privilégios administrativos. Clique em **Aplicar**.

  Dicas: Os convidados logados podem digitar a senha Ativar Admin nesta página para obter privilégios administrativos.

- **No servidor**

  As contas criadas pelo servidor RADIUS/TACACS+ podem exibir apenas as configurações e algumas informações de rede sem a senha Ativar Admin.

  Alguns princípios de configuração no servidor são os seguintes:

  1 - Para a configuração da autenticação de login, mais de uma conta de login pode ser criada no servidor. Além disso, o nome de usuário e a senha podem ser personalizados.

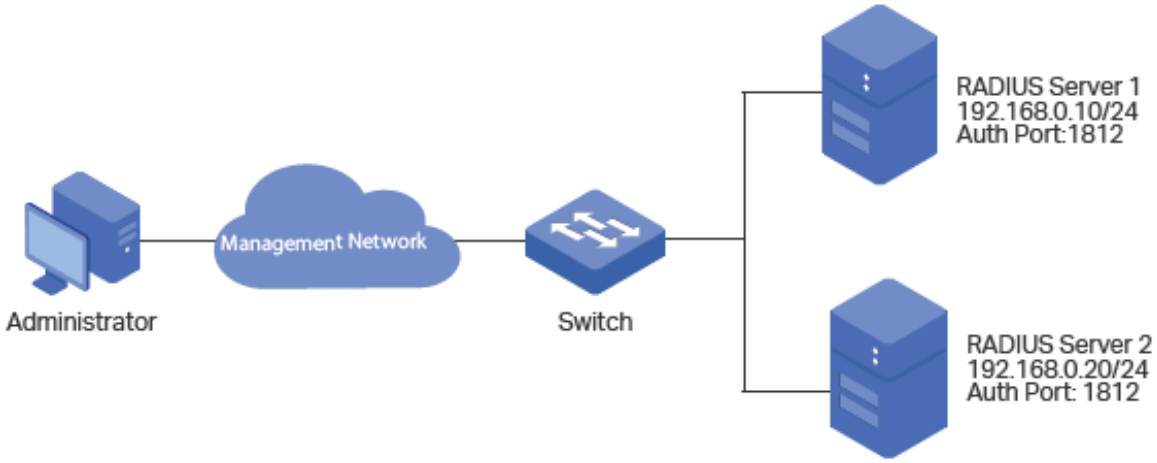
  2 - Para ativar configuração de senha:
  No servidor RADIUS, o nome de usuário deve ser definido como **$enable$** e a senha de ativação é personalizável. Todos os usuários que tentam obter privilégios administrativos compartilham essa senha de ativação.
  No servidor TACACS +, configure o valor de "enable 15" como a senha de ativação no arquivo de configuração. Todos os usuários que tentam obter privilégios administrativos compartilham essa senha de ativação.

Exemplo de Configuração

Requisitos de Rede

A Figura abaixo exemplifica um cenário possível, onde o switch precisa ser gerenciado remotamente via Telnet. Além disso, o administrador sênior da empresa deseja criar uma conta para os administradores com menor privilégio, que podem apenas visualizar as configurações e algumas informações de rede sem a senha de ativação fornecida.

Dois servidores RADIUS são implantados na rede para fornecer um método de autenticação mais seguro para os administradores que tentam efetuar login ou obter privilégios administrativos. Se o Servidor RADIUS 1 falhar e não responder à solicitação de autenticação, o Servidor RADIUS 2 funcionará, de modo a garantir a estabilidade do sistema de autenticação.



Configurando Cenário

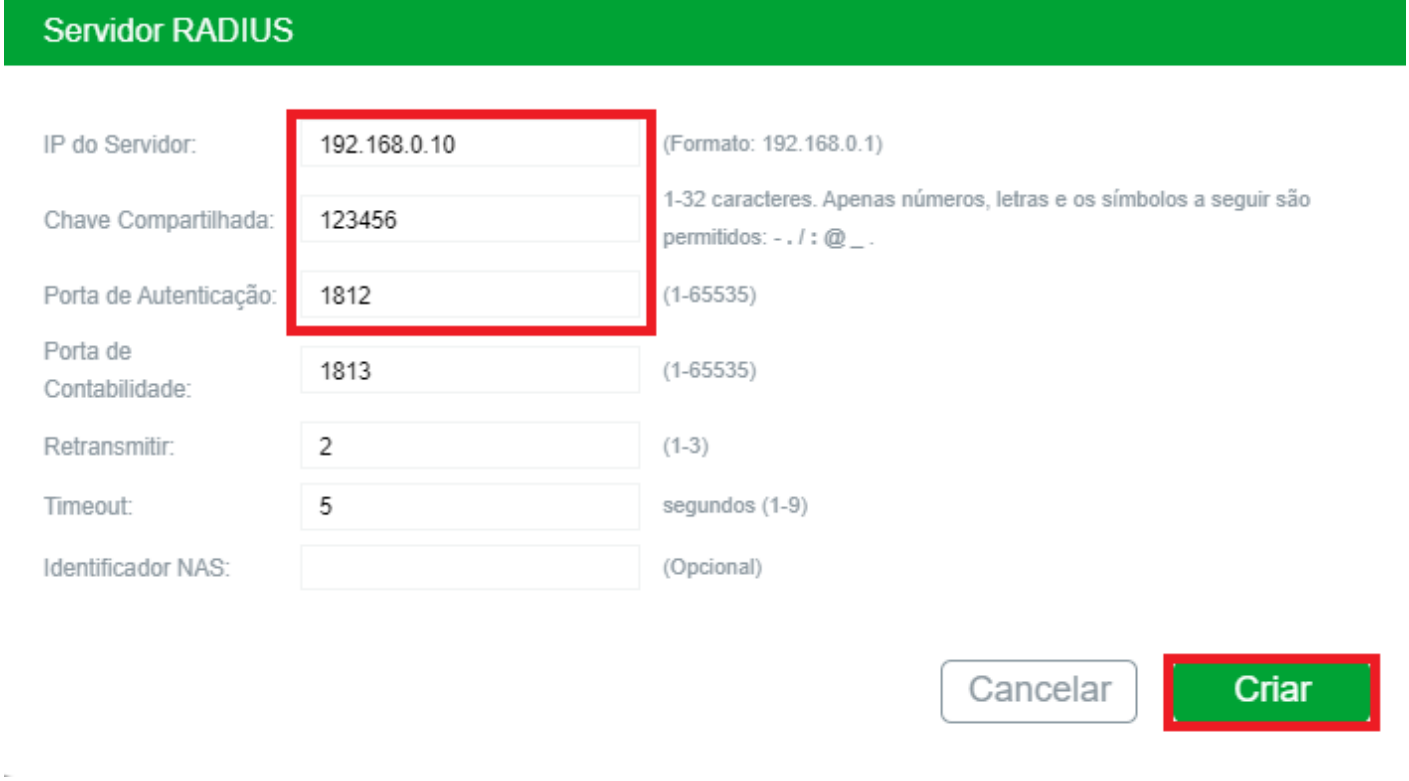
Para implementar esse requisito, o administrador sênior pode criar a conta de logon e a senha de ativação nos dois servidores RADIUS e configurar o recurso AAA no switch. Os endereços IP dos dois servidores RADIUS são 192.168.0.10/24 e 192.168.0.20/24; o número da porta de autenticação é 1812; a chave compartilhada é 123456.

A visão geral da configuração no switch é a seguinte:

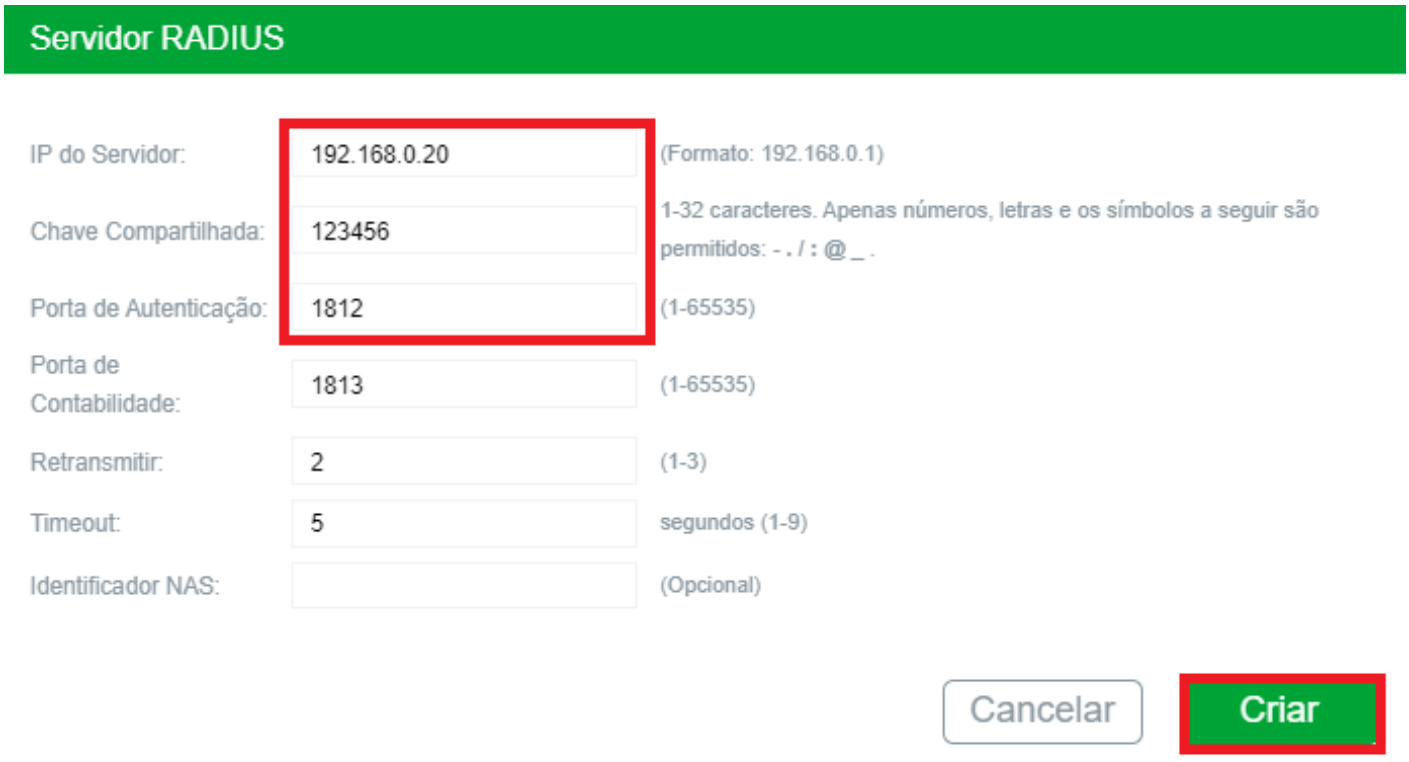
1. Adicione os dois servidores RADIUS no switch.
2. Crie um novo grupo de servidores RADIUS e adicione os dois servidores ao grupo. Verifique se o servidor RADIUS 1 é o primeiro servidor para autenticação.
3. Configure a lista de métodos.
4. Configure a lista de aplicativos AAA.

A seguir estão os passos necessários para efetuar a configuração:

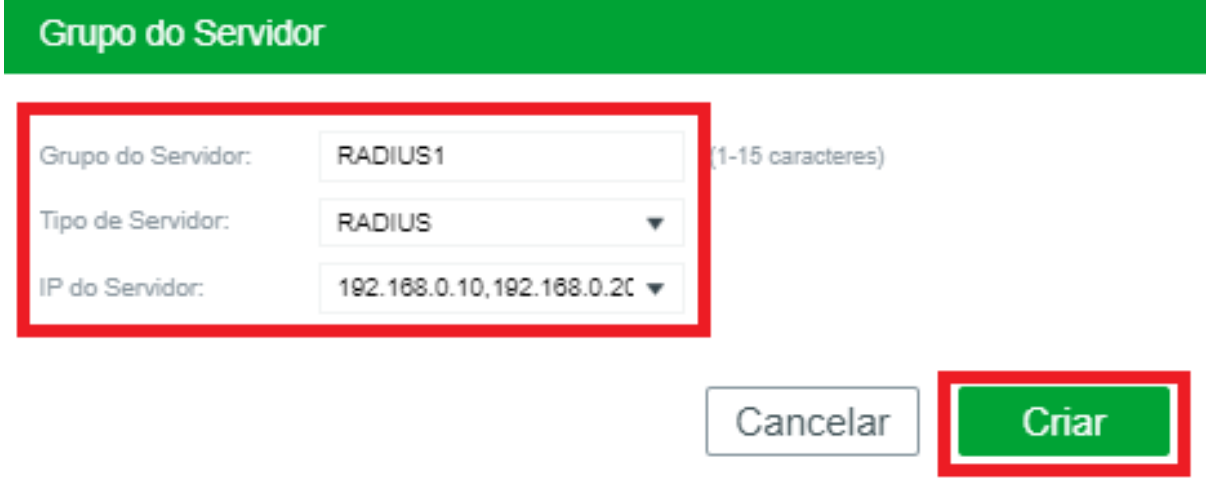
1. Escolha o menu **SEGURANÇA> AAA> Configuração RADIUS** e clique em Adicionar para carregar a seguinte página. Configure o IP do servidor como 192.168.0.10, a chave compartilhada como 123456, a porta de autenticação como 1812 e mantenha os outros parâmetros como padrão. Clique em **Criar** para adicionar o Servidor RADIUS 1 no switch.



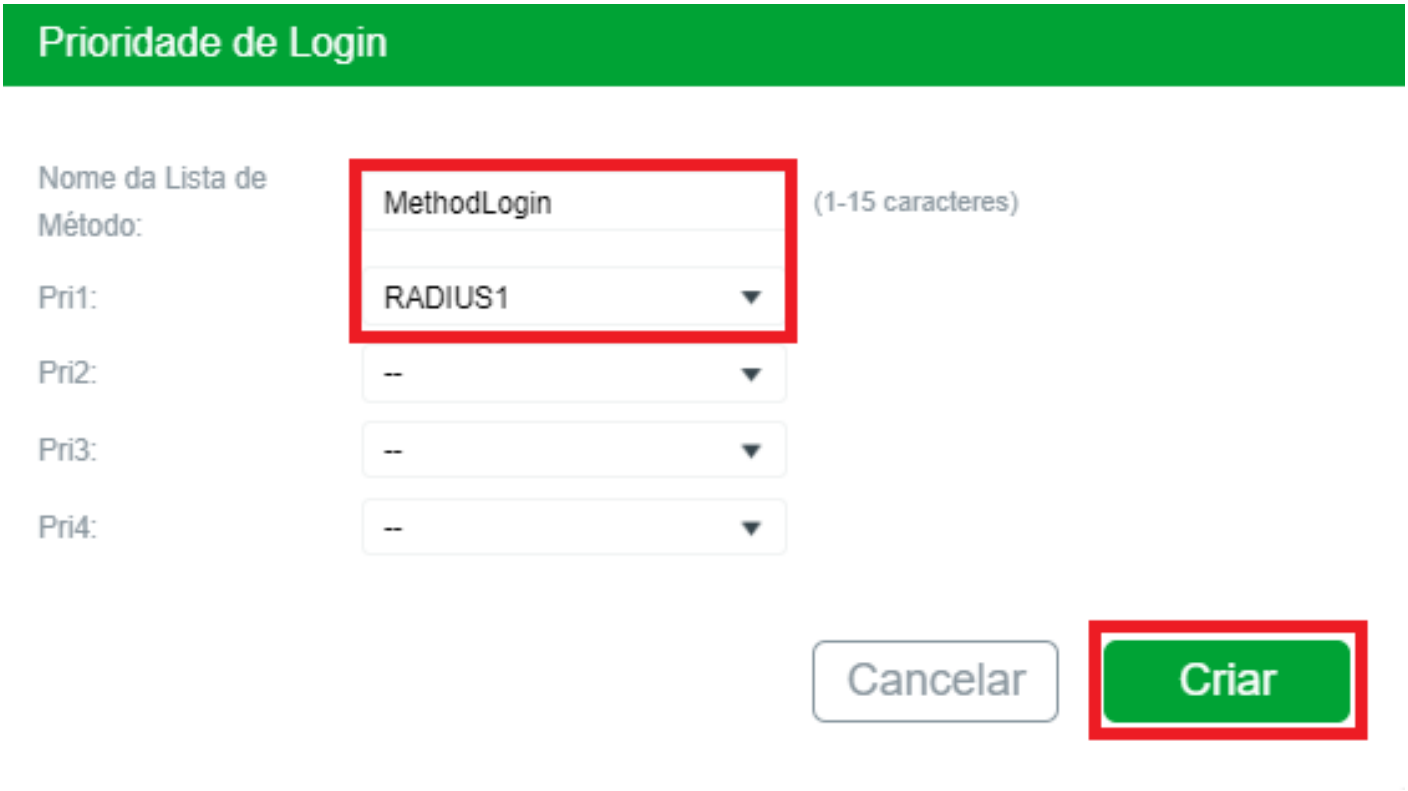
2. Na mesma página, clique em Adicionar para carregar a seguinte página. Configure o IP do servidor como 192.168.0.20, a chave compartilhada como 123456, a porta de autenticação como 1812 e mantenha os outros parâmetros como padrão. Clique em **Criar** para adicionar o servidor RADIUS 2 no switch.



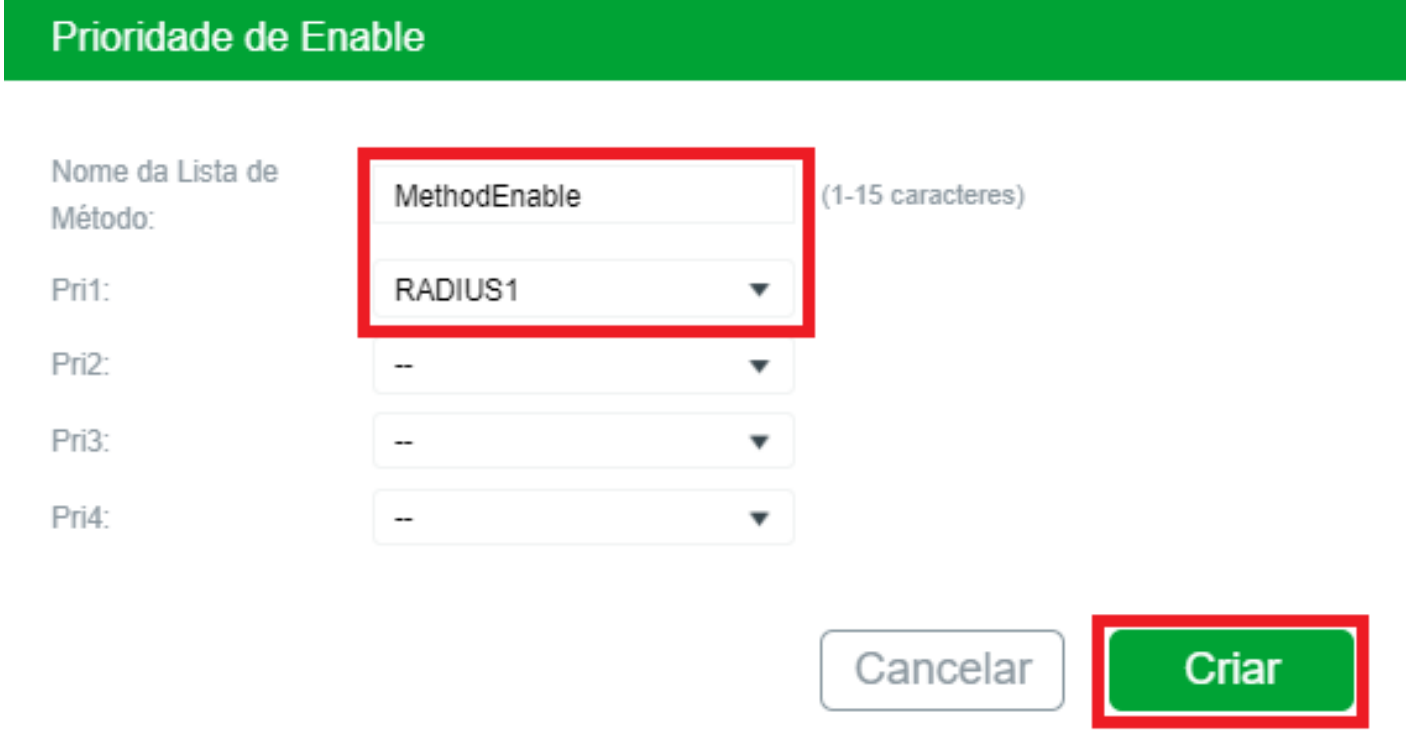
3. Escolha o menu **SEGURANÇA> AAA> Grupo Servidor** clique em Adicionar para carregar a seguinte página. Especifique o nome do grupo como RADIUS1 e o tipo de servidor como RADIUS. Selecione 192.168.0.10 e 192.168.0.20 na lista suspensa. Clique em **Criar** para criar o grupo de servidores.



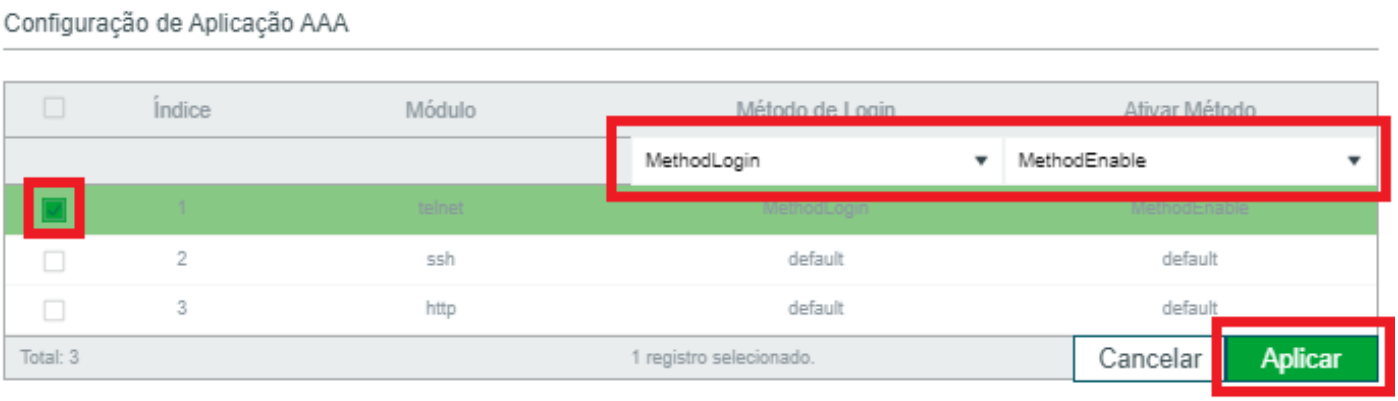
4. Escolha o menu **SEGURANÇA> AAA> Configuração de Método** e clique em Adicionar na seção Configuração da Prioridade de Login. Especifique o Nome da lista de métodos como MethodLogin e selecione Pri1 como RADIUS1. Clique em **Criar** para definir a configuração de métodos para a autenticação de login.



5. Na mesma página, clique em Adicionar na seção Configuração da Prioridade de Enable. Especifique o Nome da lista de métodos como MethodEnable e selecione Pri1 como RADIUS1. Clique em **Criar** para definir a opção para o método de ativar a autenticação por senha.



6. Escolha o menu **SEGURANÇA> AAA> Configuração Global** para carregar a página a seguir. Na seção Configuração de Aplicação AAA, selecione telnet e configure o Método de Login como MethodLogin e Ativar Método como MethodEnable. Depois clique em **Aplicar**.



7. Clique em Salvar para salvar as configurações.

Apêndice: Configuração Padrão

As configurações padrão do AAA estão listadas nas tabelas a seguir.

Parâmetros	Configurações Padrão
Configuração Global	
Recurso AAA	Ativado
Configuração RADIUS	
IP Servidor	Nenhum

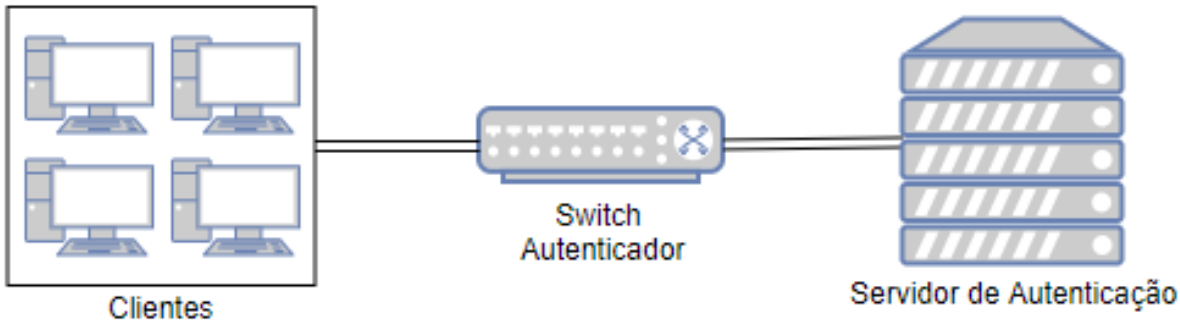
Shared Key	Nenhum
Porta de Autenticação	1812
Porta de Contabilidade/p>	1813
Retransmitir	2
Timeout	5 segundos
Identificador NAS	O endereço MAC do switch
Configuração TACACS+	
IP Servidor	Nenhum
Shared Key	Nenhum
Timeout	5 segundos
Porta do Servidor	49
Grupo de servidores	Existem dois grupos de servidores padrão: RADIUS e TACACS.
Configuração do Método	
Configuração do Método de Autenticação do Login	Nome: padrão Pri1: local
Configuração do Método de Ativar Autenticação	Nome: padrão Pri1: local
Configuração de Aplicação AAA	
Telnet	Método de Login: padrão Ativar Método: padrão
SSH	Método de Login: padrão Ativar Método: padrão
HTTP	Método de Login: padrão Ativar Método: padrão

802.1X

Visão Geral

O protocolo 802.1x é um protocolo de controle de acesso para redes baseado em porta. Ele é utilizado para autenticar e controlar o acesso de dispositivos conectados às portas. Se o dispositivo conectado à porta é devidamente autenticado por um servidor a sua solicitação de acesso à rede local será aceito, caso contrário sua solicitação será rejeitada.

A autenticação 802.1x utiliza o modelo cliente-servidor que contem três funções: cliente ou solicitante, autenticador e servidor de autenticação. Como descrito na figura a baixo.



- **Cliente**

  Um cliente ou suplicante é conectado ao autenticador através de uma porta física.

- **Autenticador**

  Um autenticador é usualmente um dispositivo de rede que suporta o protocolo 802.1x. Como mostrado na figura acima o switch é o autenticador.

  O autenticador funciona como um proxy intermediário entre o cliente e o servidor de autenticação. O autenticador solicita a informação de usuário do cliente e envia para o servidor de autenticador; o autenticador também obtém a resposta do servidor de autenticador e envia ao cliente. O autenticador permite que clientes autenticados acessem a LAN através das portas conectadas, porém nega acesso à clientes não autenticados.

- **Servidor autenticador**

  O servidor de autenticação normalmente é um host rodando um programa de servidor RADIUS. Esse servidor guarda informação de clientes, confirmando se um cliente é legal e informando o autenticador no qual o cliente está autenticado.

Configuração 802.1x

Para completar a configuração 802.1x siga os seguintes passos:

1. Configure um servidor de RADIUS.
2. Configure o 802.1x globalmente.
3. Configure o 802.1x nas portas.

Você também pode visualizar o Status do autenticador.

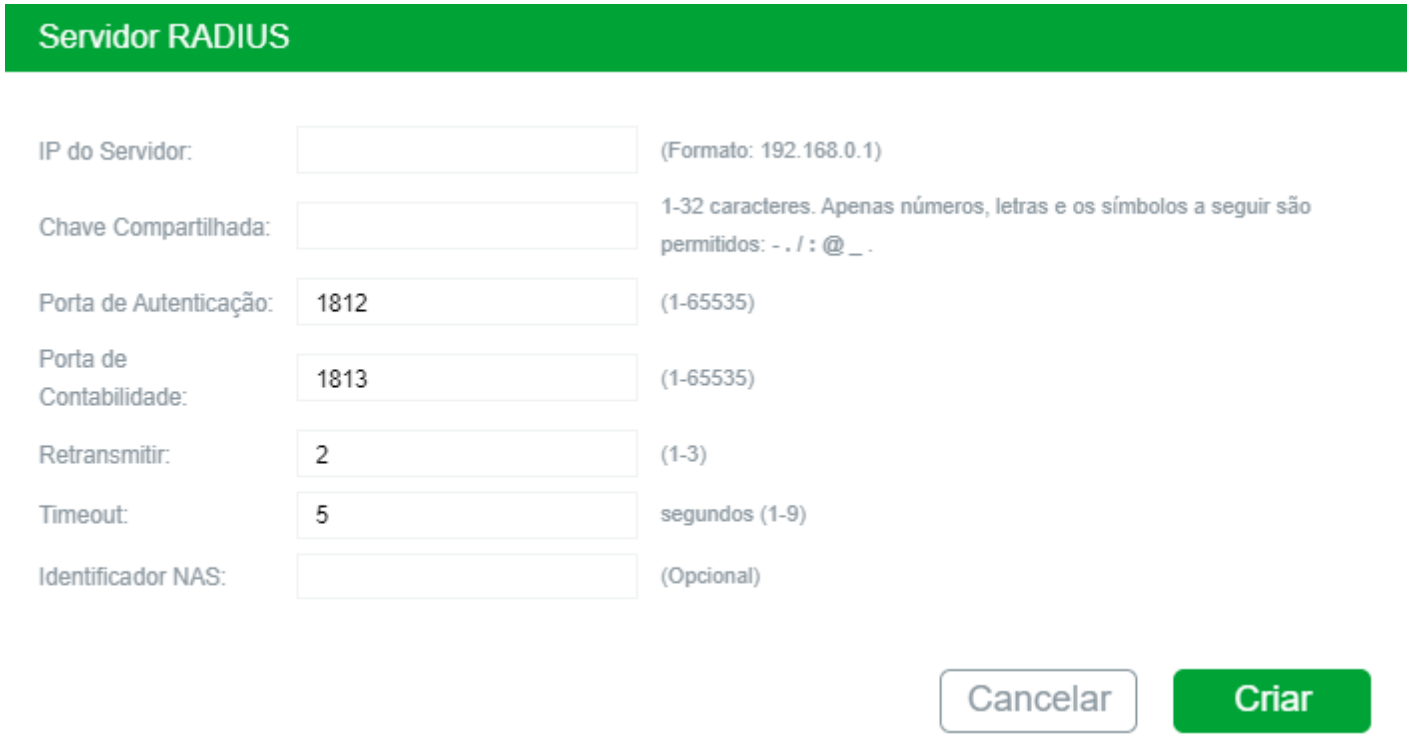
> A autenticação 802.1x e segurança de porta não podem ser habilitados ao mesmo tempo. Antes de habilitar a autenticação 802.1x verifique se a Segurança de Porta está desabilitada.

Configurando o Servidor RADIUS

Configure os parâmetros do servidor RADIUS e configure o Grupo Servidor.

Adicionando um Servidor RADIUS

Vá até o menu **Segurança > AAA > Configuração RADIUS** clique em Adicionar para carregar a página a seguir.



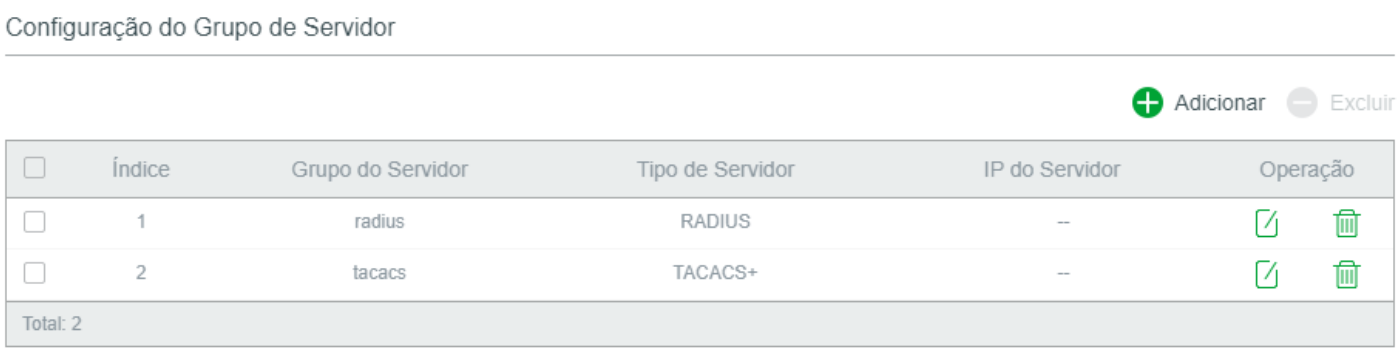
1. Configure os parâmetros do servidor RADIUS.

IP do Servidor	Digite o endereço IP do servidor que está executando o protocolo seguro RADIUS.
Chave Compartilhada	Digite a chave compartilhada entre o servidor RADIUS e o switch. O servidor RADIUS e o switch usam a cadeia de chaves para criptografar senhas e trocar respostas.
Porta de Autenticação	Especifique a porta de destino UDP no servidor RADIUS para solicitações de autenticação. A configuração padrão é 1812.
Porta de Contabilidade	Especifique a porta de destino UDP no servidor RADIUS para solicitações de contabilidade. A configuração padrão é 1813. Geralmente, é usada no recurso 802.1x.
Retransmitir	Especifique o número de vezes que uma solicitação é reenviada para o servidor se o servidor não responder. A configuração padrão é 2.
Timeout	Especifique o intervalo de tempo que o switch espera que o servidor responda antes de reenviar. A configuração padrão é 5 segundos.
Identificador NAS	Especifique o nome do NAS (servidor de acesso à rede) a ser contido nos pacotes RADIUS para identificação. Varia de 1 a 31 caracteres. O valor padrão é o endereço MAC do switch. Geralmente, o NAS indica o próprio switch.

2. Clique em **Aplicar**.

Configurando Grupo do Servidor RADIUS

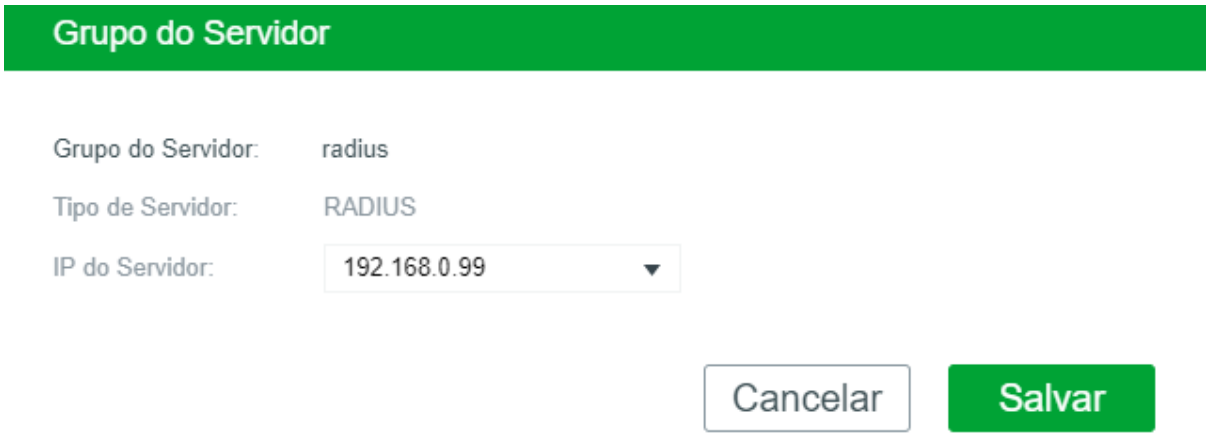
Vá até o menu **SEGURANÇA > AAA > Grupo Servidor** para carregar a página a seguir.



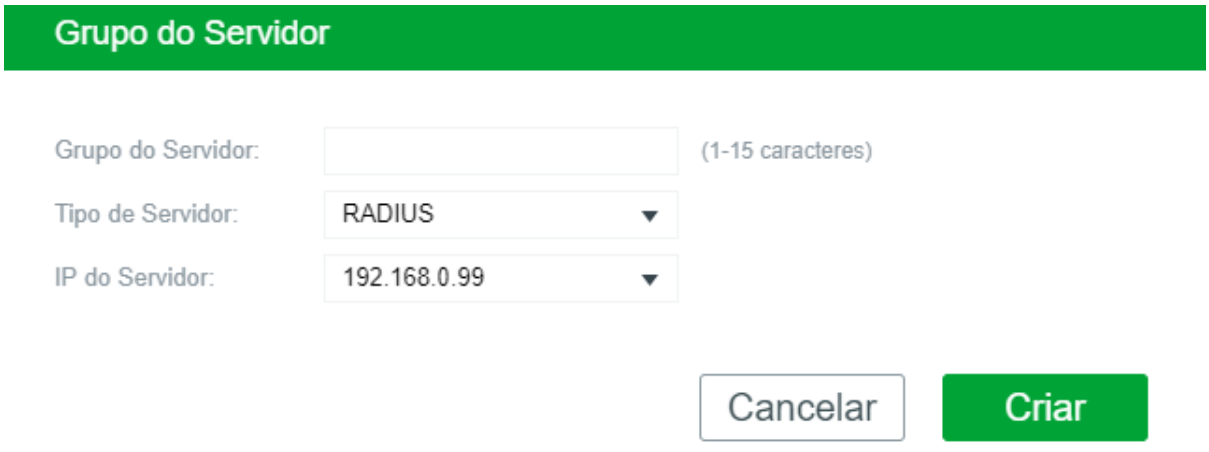
Siga os seguintes passos para adicionar um servidor RADIUS a um Grupo Servidor:

1. Clique em para editar o grupo do servidor RADIUS padrão ou clique em Adicionar para adicionar um novo grupo servidor.

   Se você clicar em , a seguinte janela irá aparecer. Selecione um servidor RADIUS e clique em **Salvar**.

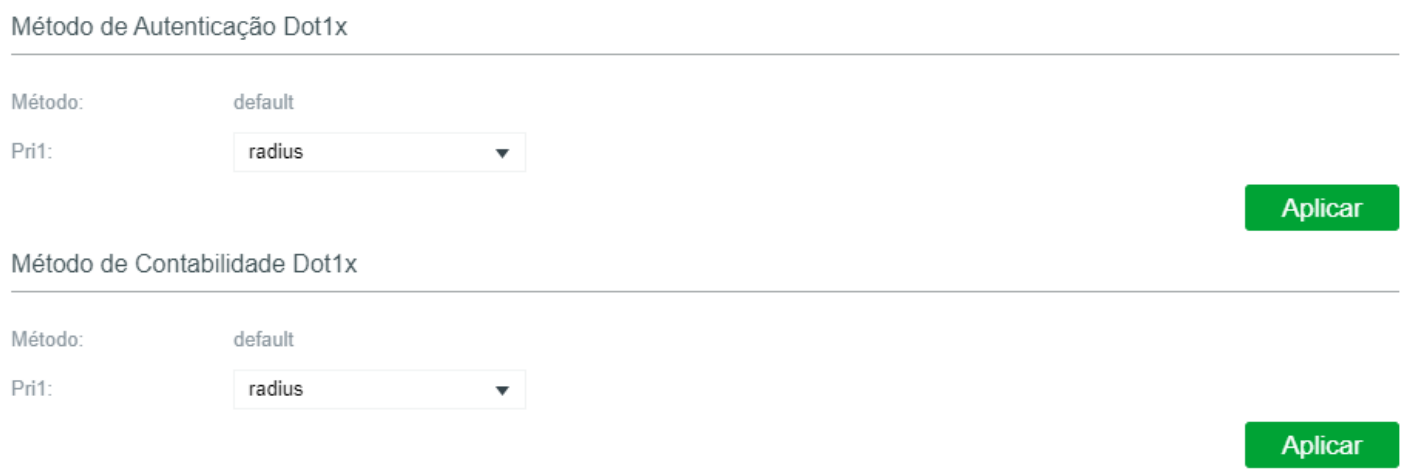


   Se você clicar em Adicionar , a seguinte janela irá aparecer. Especifique um nome para o grupo servidor, selecione o tipo do servidor como RADIUS e selecione o Endereço IP do servidor RADIUS. Clique em **Salvar**.



Configurando o Dot1x

Vá até o menu **SEGURANÇA > AAA > Configuração Dot1x** para carregar a página a seguir.

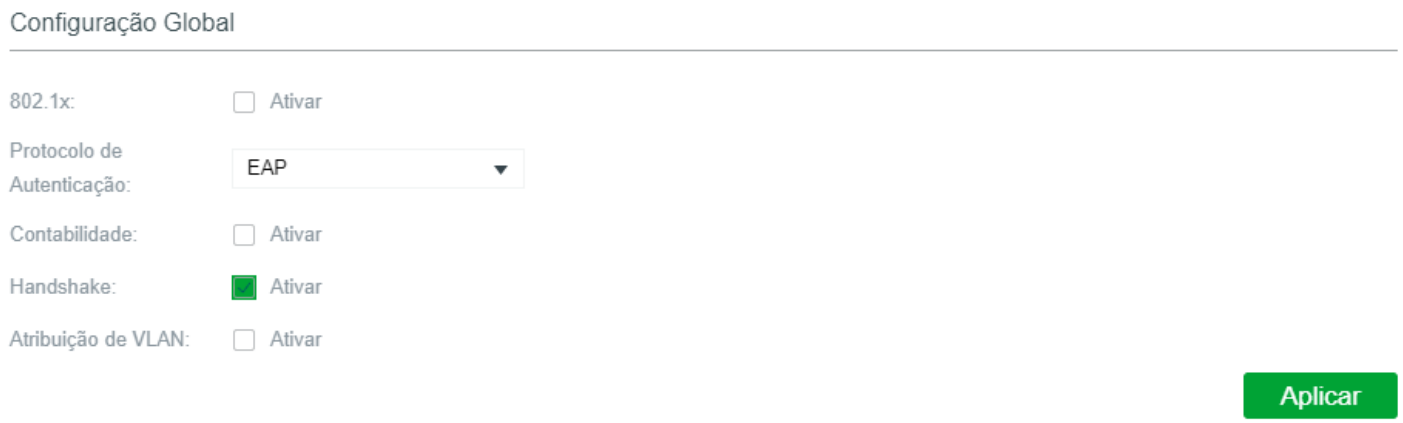


Siga os seguintes passo para configurar o grupo do servidor RADIUS para autenticação 802.1x e configurações de conta:

1. Na seção **Método de Autenticação Dot1x** selecione um grupo servidor RADIUS existente para autenticação na lista Pri1 e clique em **Aplicar**.
2. Na seção **Método de Contabilidade Dot1x** selecione um grupo servidor RADIUS existente para as configurações de conta na lista de Pri1 e clique em **Aplicar**.

Configurando 802.1x Globalmente

Vá até o menu **SEGURANÇA > 802.1x > Configuração Global** para carregar a página a seguir.



Siga os seguintes passo para configurar os parâmetros globais do 802.1x:

1. Na seção **Configuração Global** configure os seguintes parâmetros.

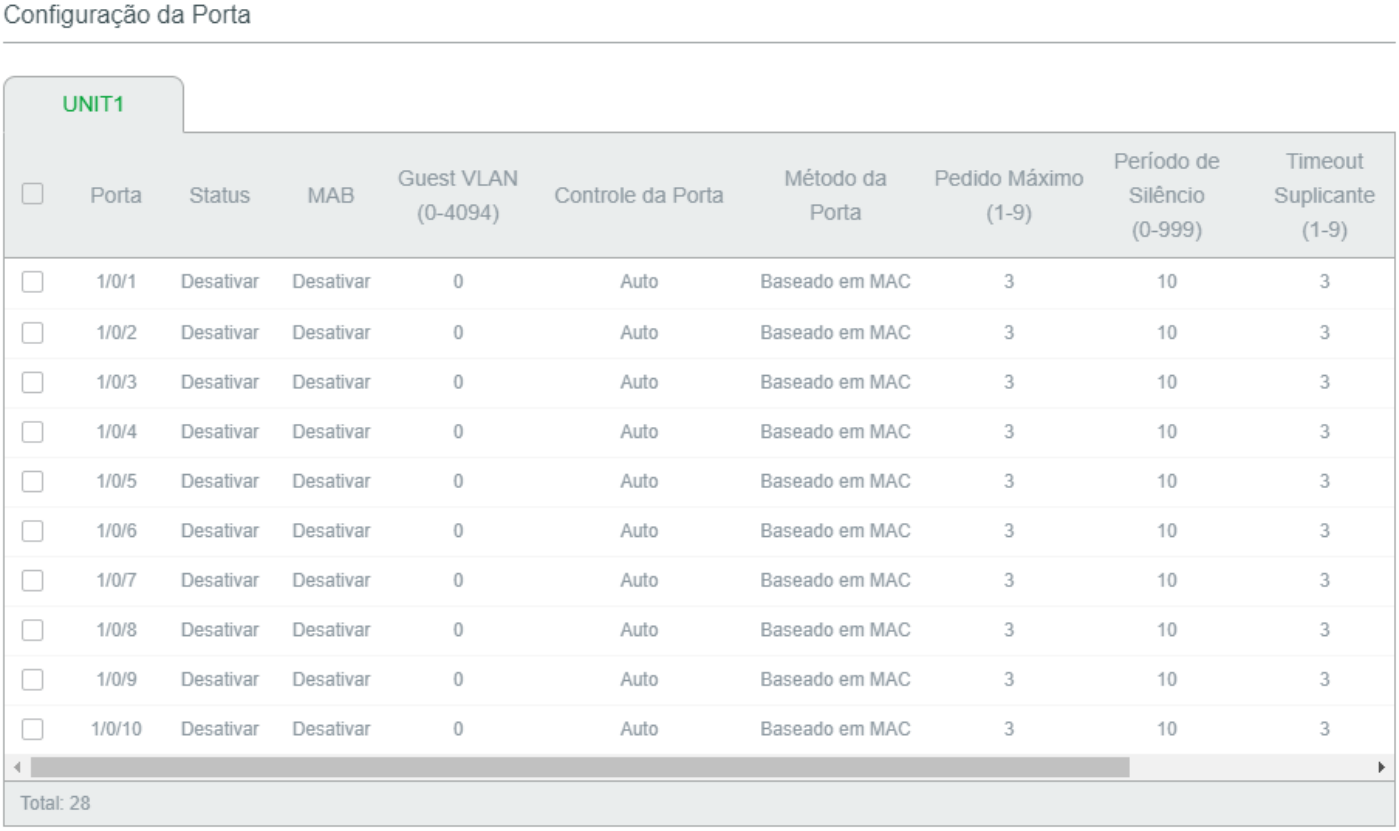
802.1x	Habilita ou desabilita o 802.1x globalmente.

Protocolo de Autenticação	Selecione o protocolo de autenticação para o 802.1x **PAP:** o sistema de autenticação 802.1x utiliza pacotes EAP para trocar informações entre o switch e o cliente. As transmissões dos pacotes EAP (Extensible Authentication Protocol) é finalizada no switch os pacotes EAP são convertidos em pacotes de protocolo (como o RADIUS), e depois são transmitidos par ao servidor de autenticação. **EAP:** o sistema de autenticação 802.1x utiliza pacotes EAP para trocar informação entre o switch e o cliente. Os pacotes EAP com os dados de autenticação são encapsulados em pacotes de um protocolo avançado (como o RADIUS) e transmitidos para o servidor de autenticador.
Contabilidade	Habilita a função de 802.1x accounting.
Handshake	Habilita ou desabilita a função de Handshake. A função de handshake é usada para detectar o status de conexão entre o cliente 802.1x (WPA suplicante) e o switch. Desabilite essa função se você estiver utilizando outros softwares.
Atribuição de VLAN	Habilita ou desabilita a função de atribuição de VLAN 802.1x. A atribuição de VLAN 802.1x é uma tecnologia que permite que o servidor RADIUS envie atribuição de VLAN para a porta quando essa é autenticada. Se VLAN atribuída não existir no switch, o switch irá criar uma VLAN automaticamente, adicionando a porta autenticada à VLAN e irá mudar o PVID baseado na VLAN atribuída. Se VLAN atribuída existir no switch, o switch irá adicionar diretamente a porta autenticada à VLAN e irá alterar o PVID ao invés de criar uma nova VLAN. Se nenhuma VLAN é fornecida pelo servidor RADIUS ou se a autenticação 802.1x estiver desabilitada, a porta permanecerá na sua VLAN original após a autenticação.

2. Clique em **Aplicar**.

Configurando 802.1x nas Portas

Vá até o menu **SEGURANÇA > 802.1x > Configuração de Porta** para carregar a página a seguir.



Siga os seguintes passo para configurar a autenticação 802.1x para a porta desejada:

1. Selecione uma ou mais portas e configure os seguintes parâmetros.

Status	Habilita a autenticação 802.1x para a porta.
MAB	Selecione para habilitar a função MAB (MAC-Based Authentication Bypass) para a porta. Com a função MAB habilitada, o switch automaticamente enviará o quadro de requisição de acesso com o endereço MAC do cliente juntamente com o nome de usuário e a senha ao servidor RADIUS de autenticação. Isso é necessário para configurar o servidor RADIUS com a informação do cliente para autenticação. Você pode habilitar essa função para portas IEEE 802.1x conectadas à dispositivos incompatíveis com o 802.1x. Por exemplo, a maioria das impressoras, telefones IP e máquinas de FAX.
Guest VLAN (0-4094)	Especifique a ID da Guest VLAN. 0 significa que a Guest VLAN está desabilitada. A VLAN configurada aqui deve ser uma VLAN 802.1Q existente. Com a Guest VLAN habilitado, a porta pode acessar recursos na guest VLAN mesmo através da porta que ainda não está autenticada; se a guest VLAN estiver desabilitada e a porta não está autenticada, a porta não pode visitar nenhum recurso da LAN.

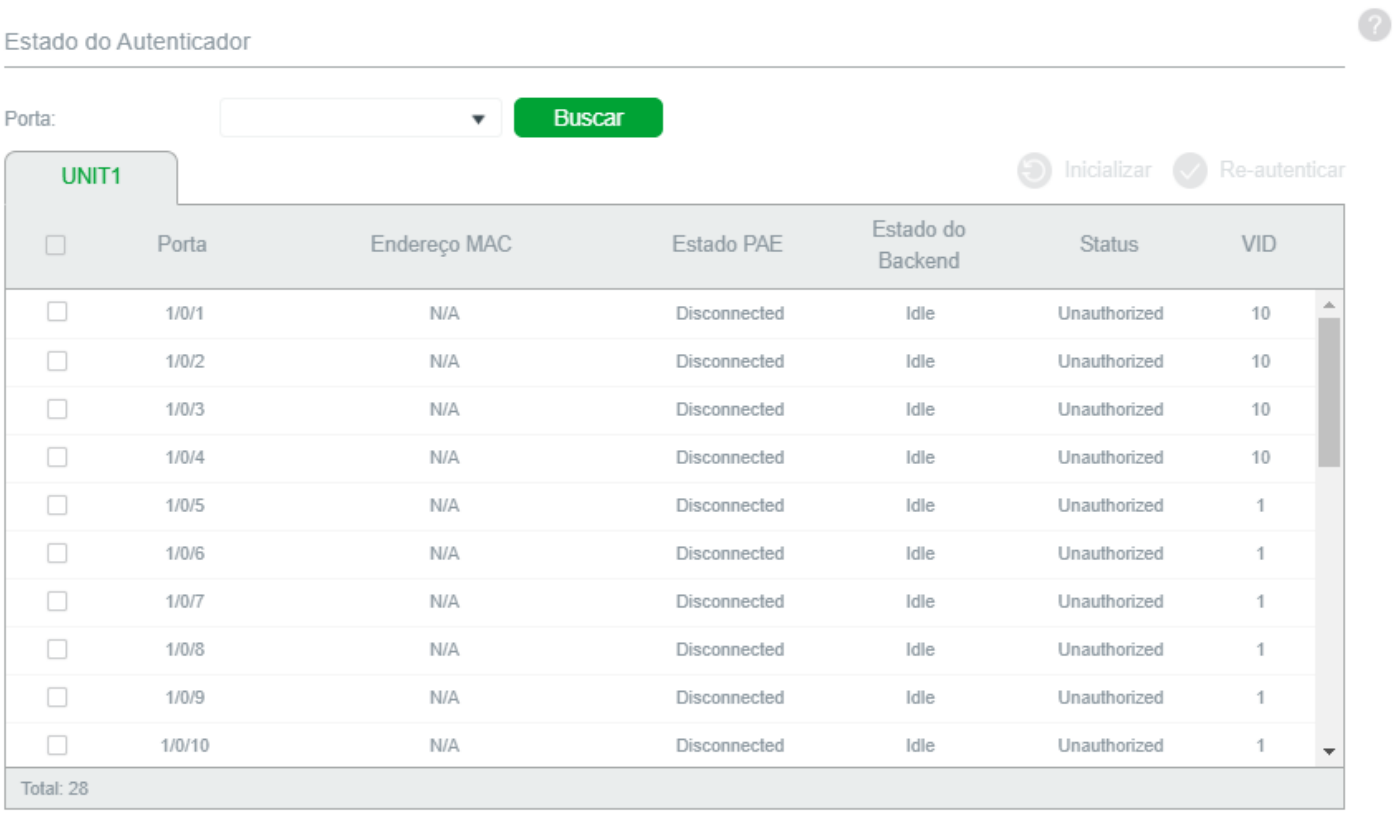
Controle da Porta	Selecione o modo de Controle da Porta. Por padrão é automático. **Auto:** se essa opção for selecionada, a porta pode acessar a rede somente quando estiver autenticada. **Autorizado a Força:** se essa opção for selecionada, a porta pode acessar a rede sem autenticação. **Desautorizado a Força:** se essa opção for selecionada, a porta nunca poderá ser autenticada.
Método da Porta	Selecione o Método da Porta. Por padrão é baseada em MAC. **Baseado em MAC:** todos os clientes conectados na porta precisar ser autenticados. **Baseado em Porta:** se um cliente conectado à porta estiver autenticado outros clientes pode acessar a LAN sem autenticação.
Pedido Máximo (1-9)	Especifica o número máximo de tentativas para enviar o pacote de autenticação. Varia entre 1 e 9 vezes e por padrão é 3 vezes.
Período de Silêncio (0-999)	Especifica o período de silencio. Varia entre 1 e 999 segundos e por padrão é 10 segundos. O período de silêncio inicia após uma autenticação falhar. Durante o período e silêncio o switch não processará solicitações de autenticação do mesmo cliente.
Timeout Suplicante (1-9)	Especifica o tempo máximo o switch aguardará pela resposta do cliente. Isso varia entre 1 e 9 segundos e por padrão é 3 segundos. Se o switch não receber nenhuma resposta do cliente dentro do tempo especificado ele reenviará a solicitação.
Autorizado	Mostra se a porta está autorizada ou não.
LAG	Mostra a LAG a qual a porta pertence.

2. Clique em **Aplicar**.

> Se a porta estiver em uma LAG, a função de autenticação 802.1x não poderá ser habilitada. Da mesma forma uma porta com a autenticação 802.1x não poderá ser adicionada à uma LAG.

Visualizando o Estado do Autenticador

Vá até o menu **SEGURANÇA > 802.1x > Estado do Autenticador** para carregar a página a seguir.



Nessa página você pode visualizar o estado do autenticador para cada porta:

Porta	Mostra o número da porta.
Endereço MAC	Mostra o endereço MAC do dispositivo autenticado. Quando o método da porta é baseado em porta, o endereço MAC do primeiro dispositivo autenticado irá ser exibido com um sufixo “p”.
Estado PAE	Exibe o estado atual da máquina de estado do autenticador PAE (Extensão de Endereço Físico). Possíveis valores: Inicializar, Desconectado, Conectando, Autenticando, Autenticado, Abortando, Mantido, Autorizado à Força e Não Autorizado à Força.
Estado do Backend	Exibe o estado atual da máquina de estado de autenticação backend. Valores possíveis: Solicitar, Resposta, Sucesso, Falha, Timeout, Inicializar e Ocioso.
Status	Mostra se a porta está autorizada ou não.
VID	Mostra a ID da VLAN atribuída pelo autenticado ao dispositivo do cliente quando a porta estiver autorizada. Se a porta não estiver autorizada e a Guest VLAN existir, a ID da Guest VLAN será exibido aqui.

Exemplo de Configuração

Requisitos de Rede

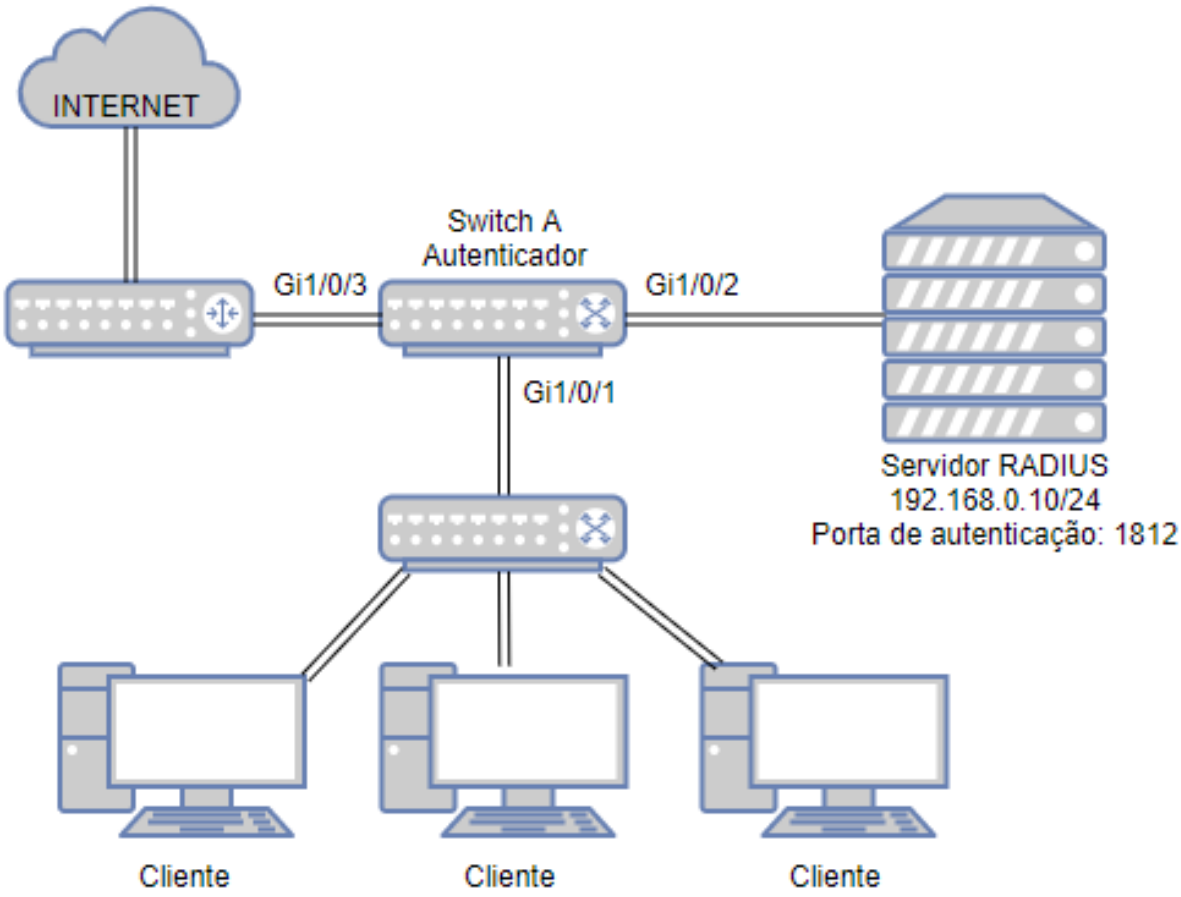
O administrado de rede quer controlar o acesso dos usuários finais (clientes) na sua companhia. É requerido que todos os clientes precisam ser autenticados separadamente e somente clientes autenticados podem acessar a internet.

Configurando o Cenário

- Para autenticar clientes separadamente habilite a autenticação 802.1x, configure o modo de controle como automática, e determine o tipo de controle como baseado em MAC.
- Habilite a autenticação 802.1x nas portas conectadas aos clientes.
- Mantenha a autenticação 802.1x desabilitada nas portas conectadas ao servidor de autenticação e à internet, o que garantirá conexão irrestrita entre o switch e o servidor de autenticação e à internet.

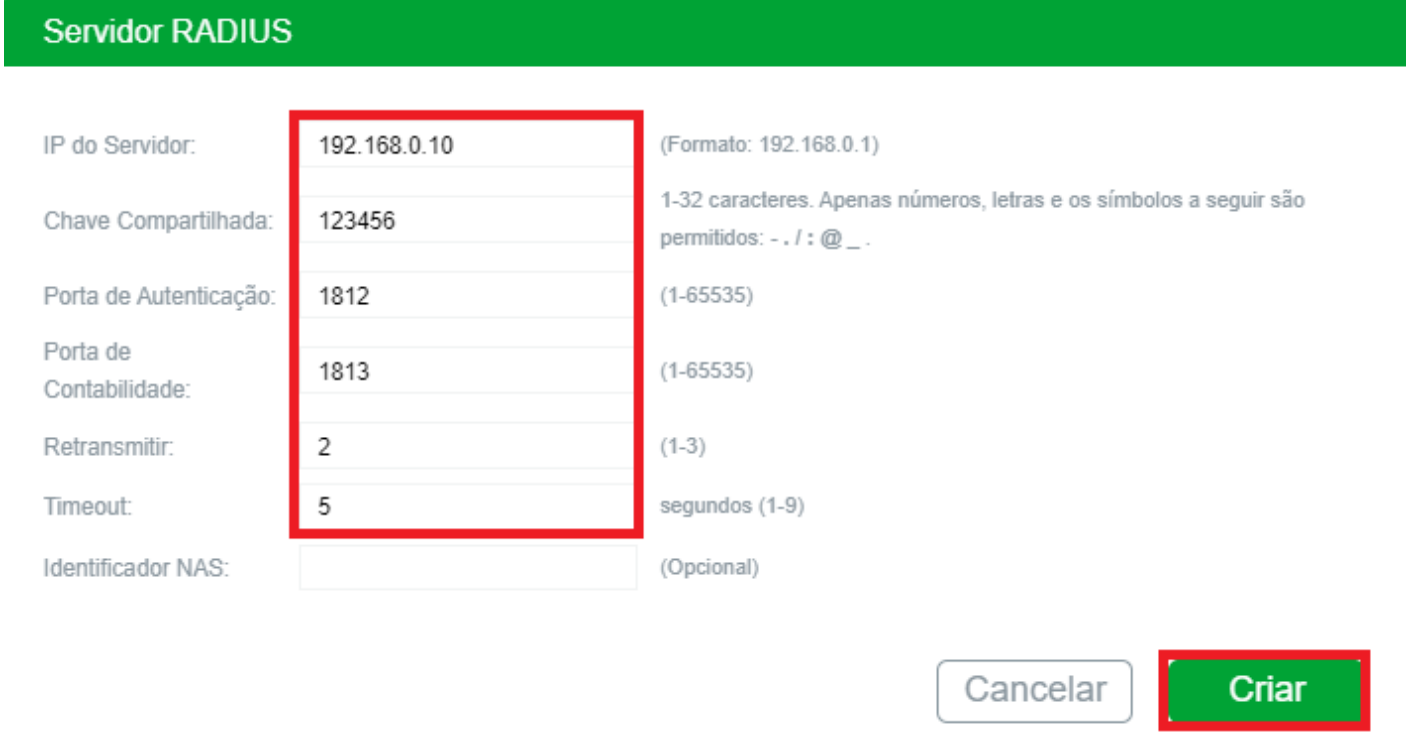
Topologia de rede

Como mostrado na figura a baixo, o switch A atua como autenticador. A porta 1/0/1 está conectada ao cliente, a porta 1/0/2 está conectada ao servidor RADIUS e a porta 1/0/3 está conectada à internet.

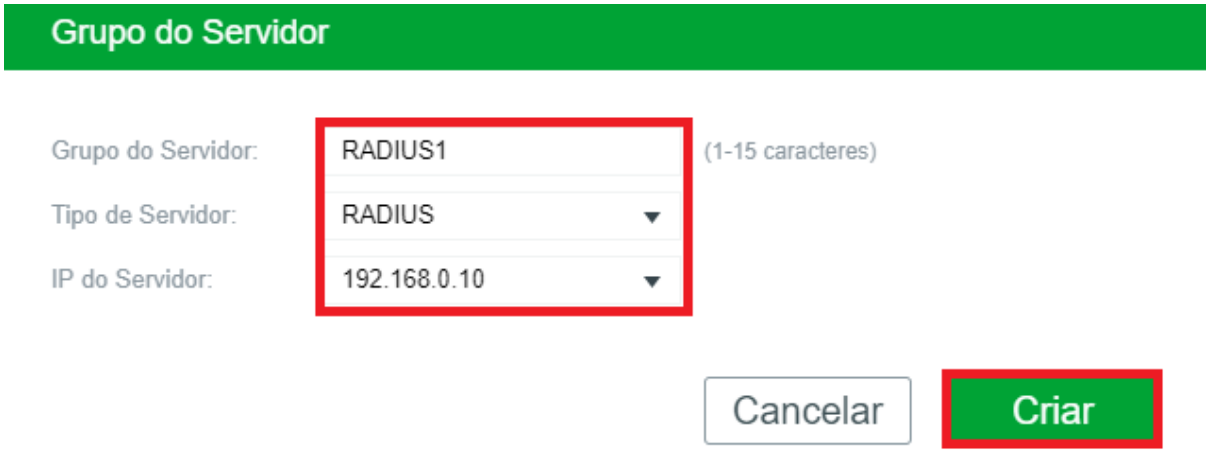


Para completar a configuração requerida siga os seguintes passos:

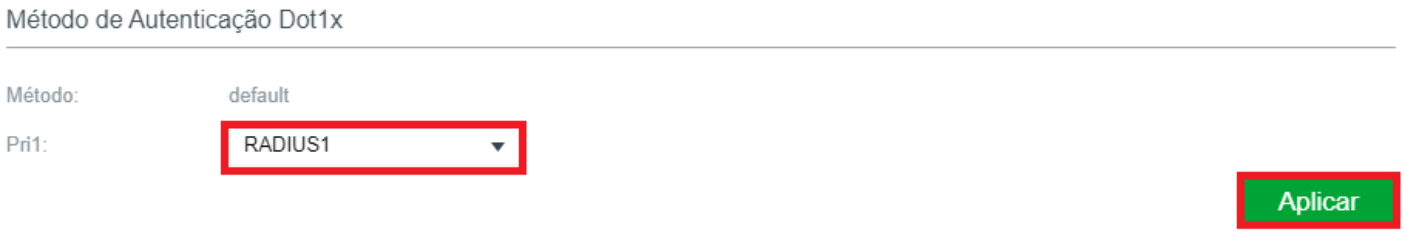
1. Vá até o menu **SEGURANÇA > AAA > Configuração RADIUS** clique em Adicionar para carregar a página a seguir. Configure os parâmetros do servidor RADIUS e clique em **Criar**.



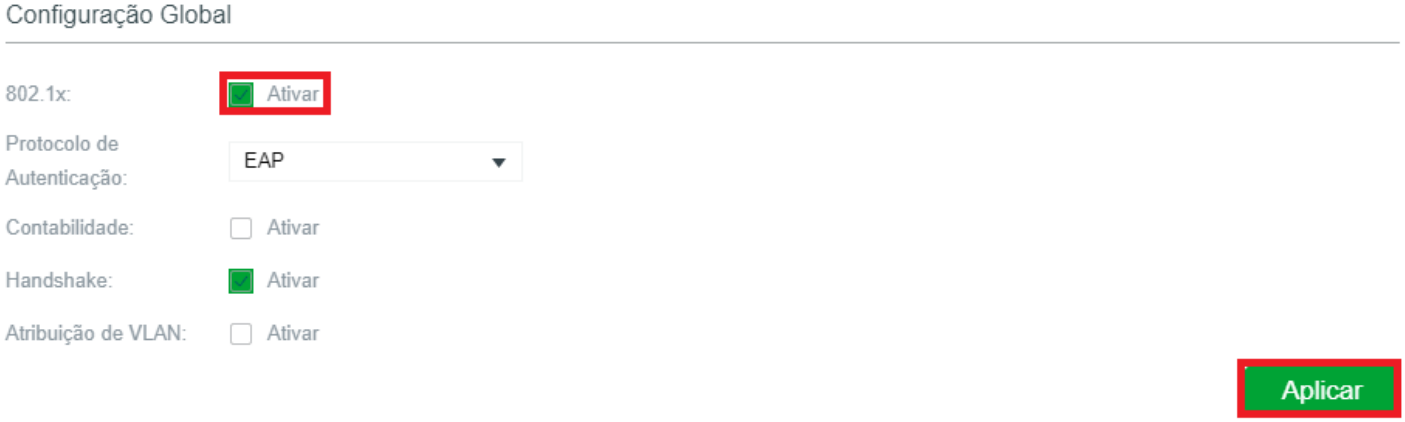
2. Vá até o menu **SEGURANÇA > AAA > Grupo Servidor** clique em Adicionar para carregar a página a seguir. Especifique o nome do grupo como RADIUS1, selecione o tipo de servidor como RADIUS e o endereço do servidor como 192.168.0.10. Clique em **Criar**.



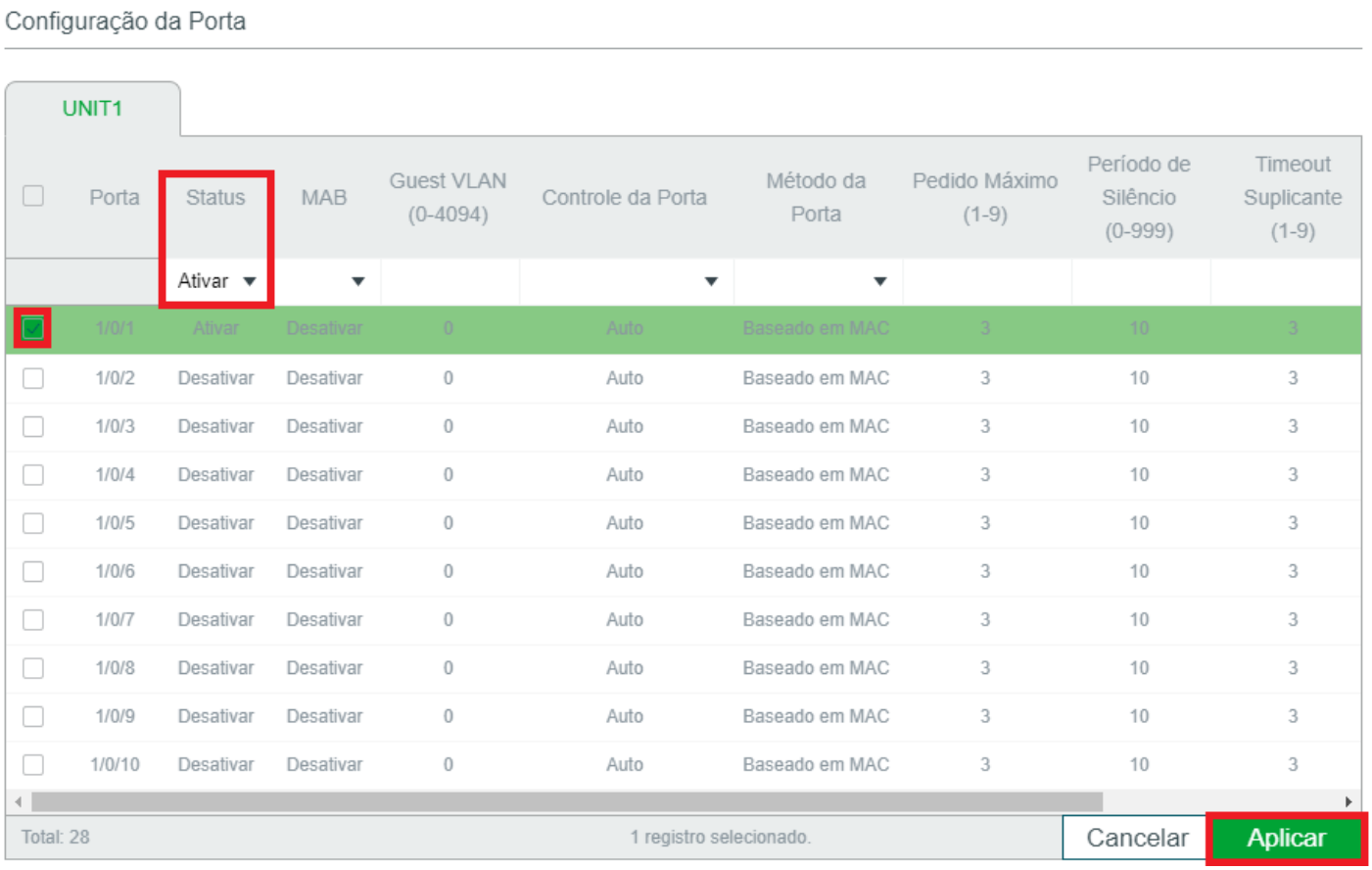
3. Vá até o menu **SEGURANÇA > AAA > Configuração Dot1x** para carregar a página a seguir. Na seção **Método de Autenticação Dot1x**, selecione RADIUS1 como grupo servidor para autenticação e clique em **Aplicar**.



4. Vá até o menu **SEGURANÇA > 802.1x > Configuração Global** para carregar a página a seguir. Habilite a autenticação 802.1x e configure o método de autenticação como EAP. Mantenha as configurações padrão para a autenticação. Clique em **Aplicar**.



5. Vá até o menu **SEGURANÇA > 802.1x > Configuração de Porta** para carregar a página a seguir. Para a porta 1/0/1 habilite a autenticação 802.1x, configure o modo de controle como auto e o tipo de controle como baseado em MAC; Para a porta 1/0/2 e porta 1/0/3 desabilite a autenticação 802.1x.



6. Clique em Salvar para salvar as configurações.

Apêndice: Configuração Padrão

As configurações Padrão do 802.1x estão listadas na tabela a seguir.

Parâmetros	Configurações Padrão
Configuração Global	
Autenticação 802.1x	Desativado

Método de Autenticação	EAP
Handshake	Ativado
Accounting	Desativado
Atribuição de VLAN	Desativado
Configuração de Porta	
Status 802.1x	Desativado
MAB	Desativado
Guest VLAN	0
Tipo de Controle	Auto
Pedido Máximo	3
Período de Silêncio	10 segundos
Timeout Suplicante	3 segundos
Método de Porta	Baseado em MAC
Configuração Dot1x	
Método de Autenticação Dot1x	Método: padrão Pri1: RADIUS
Método de Accounting Dot1x	Método: padrão Pri1: RADIUS

SEGURANÇA DA PORTA

Visão Geral

Você pode utilizar a função de Segurança da Porta para limitar o número de endereços MAC que podem ser aprendidos em cada porta, prevenindo assim que a tabela de endereços MAC esgote seu espaço através de pacotes de ataque. Além disso o switch pode enviar notificações caso o número de endereços MACs exceda o limite da porta.

Configuração de Segurança da Porta

Vá até o menu **SEGURANÇA > Segurança da Porta** para carregar a página a seguir.

Siga os seguintes passos para configurar a Segurança da Porta:

1. Selecione uma ou mais portas e configure os seguintes parâmetros.

Porta	Selecione uma ou mais portas para configurar.
Número Máximo de MAC aprendidos	Especifique o número máximo de endereços MAC que pode ser aprendido na porta. Quando o número de endereços MAC aprendidos atinge o limite, a porta parará a aprendizagem.
Número Atual Aprendido	Exibe o número de endereços MAC que foi aprendido na porta.
Trap de Excesso de Aprendizagem	Ative a Trap de Exceed Max Learned, e quando o número máximo de endereços MAC aprendido na porta especificada for excedido, uma notificação será gerada e enviada ao host de gerenciamento.
Modo de Aprendizagem de Endereço	Selecione o modo de aprendizado dos endereços MAC na porta. Há três modos: **Excluir no Timeout:** o switch excluirá os endereços MAC que não são usados ou atualizados dentro do aging time. É o padrão. **Excluir no Reboot:** os endereços MAC aprendidos estão fora da influência do aging time, e só podem ser excluídos manualmente. Os registros aprendidos serão limpos depois que o switch for reinicializado. **Permanente:** os endereços MAC aprendidos estão fora da influência do aging time, e só podem ser excluídos manualmente. Os registros aprendidos serão salvos mesmo que o switch seja reinicializado.

Status	Selecione o status da Segurança da Porta. Três tipos de status podem ser selecionados: **Forward:** quando o número de endereços MAC aprendidos atinge o limite, a porta parará de aprender, mas enviará os pacotes com os endereços MAC que não tenham sido aprendidos. **Drop:** quando o número de endereços MAC aprendidos atinge o limite, a porta parará de aprender e descartará os pacotes com os endereços MAC que não tenham sido aprendidos. **Desativar:** o limite do número na porta não é efetivo, e o switch segue as regras originais de encaminhamento. Esta é a configuração padrão.

2. Clique em **Aplicar**.

> A função de Segurança da Porta não pode ser habilitada em portas membro de LAGs, e portas com Segurança da Porta habilitadas não podem ser adicionadas a uma LAG.
>
> Em uma mesma porta as funções de Segurança da Porta e 802.1x não podem ser habilitadas ao mesmo tempo.

Apêndice: Configuração Padrão

As configurações Padrão da Segurança de Porta estão listadas na tabela a seguir.

Parâmetros	Configurações Padrão
Número Máximo de MAC aprendidos	64
Número Atual de MAC	0
Trap de Excesso de Aprendizagem	Desativado
Modo de Aprender Endereço	Excluir no timeout
Status	Desativado

ACL

Visão Geral

A ACL (lista de controle de acesso) filtra o tráfego à medida que ele passa por um switch e permite ou nega pacotes que cruzam interfaces ou VLANs especificadas. Identifica e processa com precisão os pacotes com base nas regras da ACL. Dessa maneira, a ACL ajuda a limitar o tráfego de rede, gerenciar comportamentos de acesso à rede, encaminhar pacotes para portas especificadas e muito mais.

Para configurar a ACL, siga estas etapas:

1. Configure um intervalo de tempo durante o qual a ACL está em vigor.
2. Crie uma ACL e configure as regras para filtrar diferentes pacotes.
3. Vincule a ACL a uma porta ou VLAN para torná-la eficaz.

Diretrizes de configuração

- Um pacote é "corresponde" a uma regra da ACL quando atende aos critérios de correspondência da regra. A ação resultante será "permitir" ou "negar" o pacote que corresponde à regra.
- Se nenhuma regra da ACL estiver configurada, os pacotes serão encaminhados sem serem processados pela ACL. Se houver regras de ACL configuradas e nenhuma regra correspondente for encontrada, os pacotes serão descartados.

Configuração ACL

Configurando Time Range

Alguns serviços ou recursos baseados em ACL podem precisar ser limitados para entrar em vigor apenas durante um período especificado. Nesse caso, você pode configurar um intervalo de tempo para a ACL. Para detalhes sobre a configuração do intervalo de tempo, consulte o capítulo Sistema de Gestão (g_sistema).

Criando uma ACL

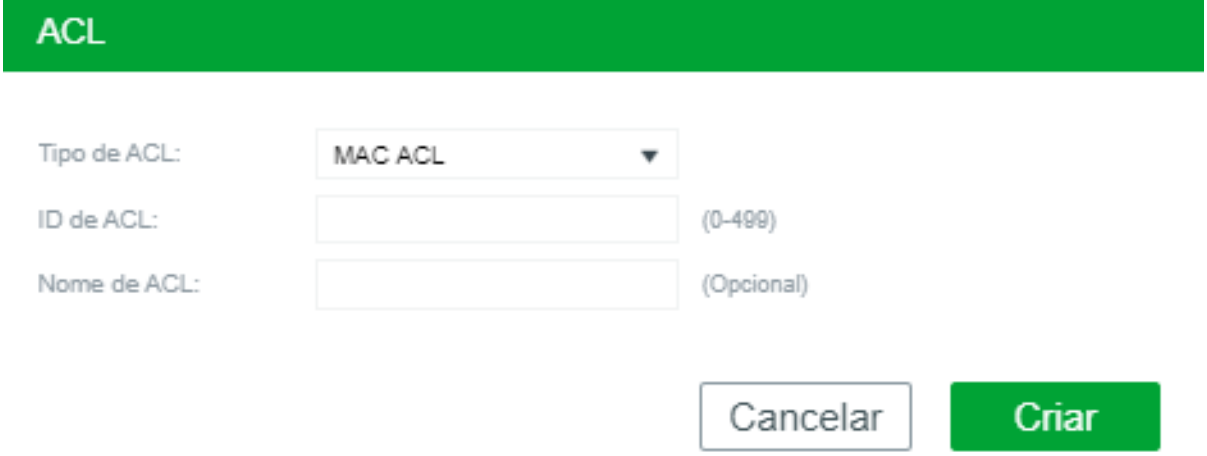
Você pode criar diferentes tipos de ACL e definir as regras com base no endereço IP ou MAC de origem, endereço IP ou MAC de destino, tipo de protocolo, número da porta e assim por diante.

ACL MAC:a ACL MAC usa o endereço MAC de origem e destino para operações correspondentes.

ACL IP: a ACL IP usa o endereço IP de origem e destino, os protocolos IP e assim por diante para operações correspondentes.

ACL IPv6: a ACL IPv6 usa o endereço IPv6 de origem e destino para operações correspondentes.

Escolha o menu **SEGURANÇA > ACL > Configuração ACL** e clique em Adicionar para carregar a seguinte página.



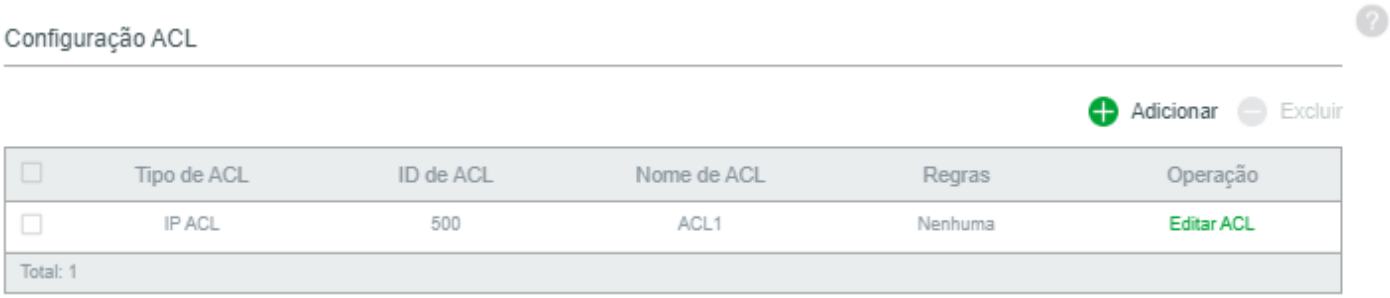
Siga os seguintes passos para criar a ACL:

1. Escolha o tipo da ACL e seu identificador.
2. (Opcional) Adicione um nome para a ACL.
3. Clique em **Criar**.

> O tipo de ACL e a faixa de ID suportados variam em diferentes modelos de switch. Por favor, consulte as informações na tela.

Configurando Regras ACL

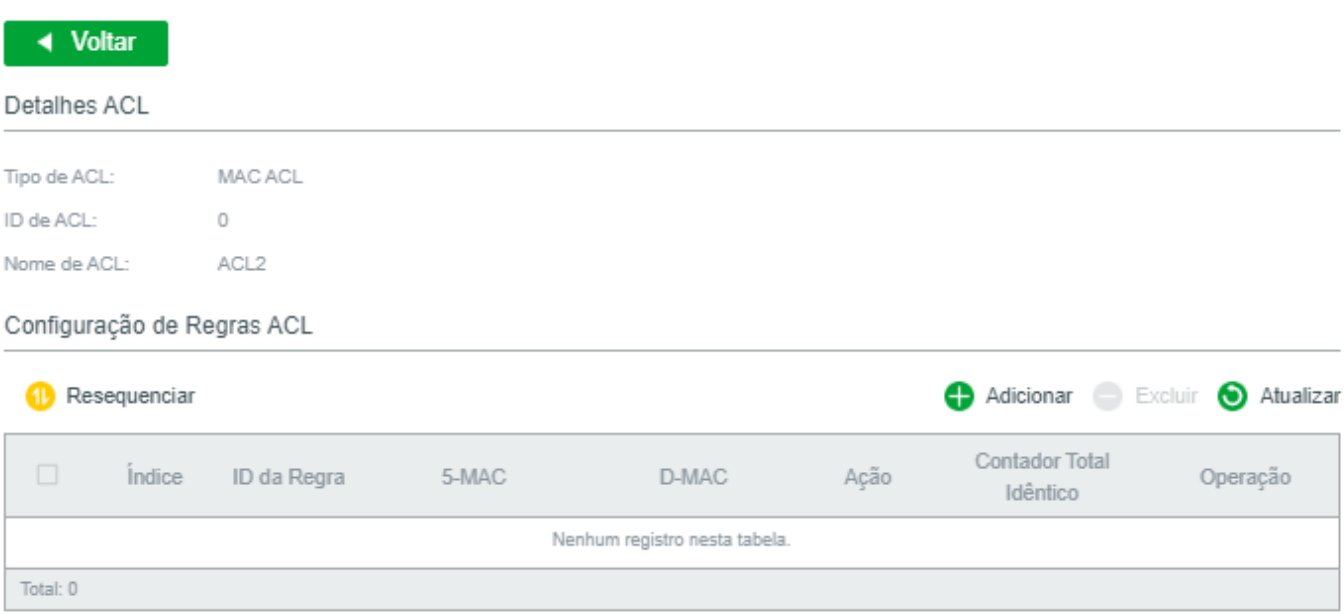
A ACL criada será exibida na página SEGURANÇA> ACL> Configuração ACL.



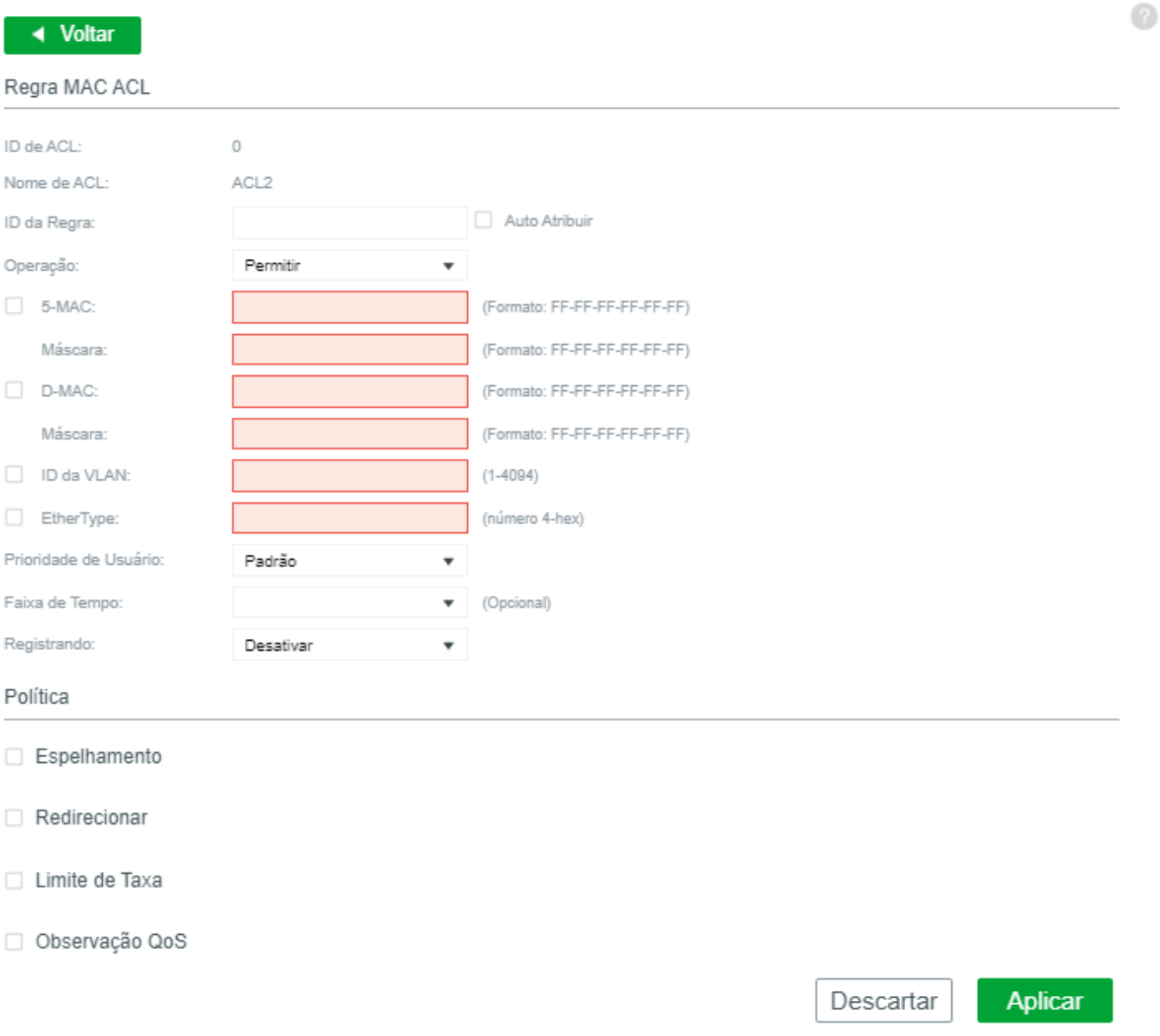
Clique em **Editar ACL** na coluna Operação. Em seguida, você pode configurar regras para esta ACL. As seções a seguir apresentam como configurar o MAC ACL, IP ACL e IPv6 ACL.

Configurando uma Regra MAC ACL

Clique em **Editar ACL** em uma ACL do tipo MAC ACL para carregar a página a seguir:



Na seção Configuração de Regras ACL, clique em Adicionar e a página a seguir será exibida.

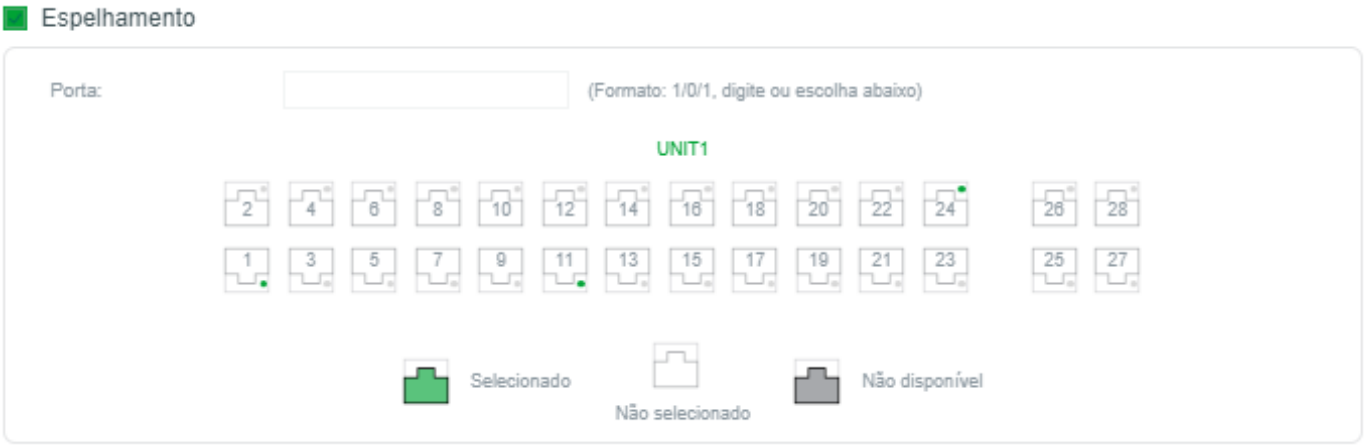


Siga os seguintes passos para configurar a regra ACL MAC:

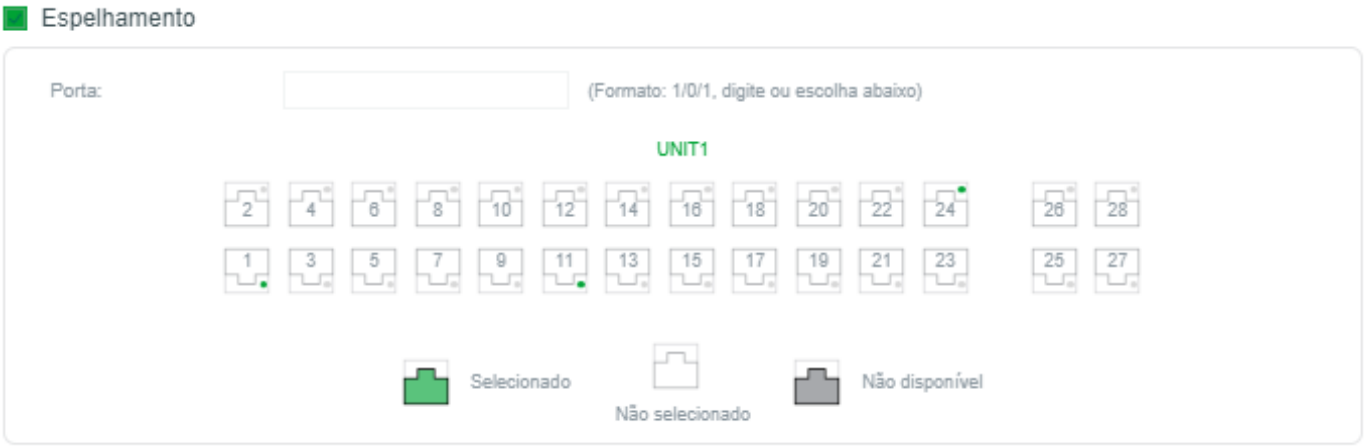
1. Na seção Regra MAC ACL, configure os seguintes parâmetros:

ID da Regra	Digite um número de identificação para identificar a regra. Não deve ser o mesmo que qualquer ID de regra atual na mesma ACL. Se você selecionar Atribuição automática, o ID da regra será atribuído automaticamente e o intervalo entre os IDs da regra será 5.
Operação	Selecione uma ação a ser tomada quando um pacote corresponder à regra. **Permitir:** encaminhar os pacotes correspondentes. **Negar:** para descartar os pacotes correspondentes.
S-MAC / Máscara	Digite o endereço MAC de origem com uma máscara. Um valor F na máscara indica que o bit correspondente no endereço deverá ser correspondido.
D-MAC / Máscara/b>	Digite o endereço MAC de destino com uma máscara. Um valor F na máscara indica que o bit correspondente no endereço deverá ser correspondido.
ID da VLAN	Digite o número de identificação da VLAN à qual a ACL se aplicará.
EtherType	Especifique o EtherType a ser correspondido usando 4 números hexadecimais.
Prioridade de Usuário	Especifique a prioridade do usuário a ser correspondida.
Faixa de Tempo	Selecione um intervalo de tempo durante o qual a regra entrará em vigor. O valor padrão é sem limite, o que significa que a regra está sempre em vigor. O intervalo de tempo mencionado aqui pode ser criado na página **SISTEMA> Faixa de Horário**.
Registrando	Habilite a função Log para a regra da ACL. Em seguida, os horários em que a regra é correspondida serão registrados a cada 5 minutos e uma interceptação relacionada será gerada. Você pode consultar o Contador total de correspondências na Configuração de Regras ACL para visualizar os horários correspondentes.

2. Na seção Política, ative ou desative o recurso Espelhamento para os pacotes correspondentes. Com esta opção ativada, escolha uma porta de destino para a qual os pacotes serão espelhados.



3. Na seção Política, ative ou desative o recurso Redirecionar para os pacotes correspondentes. Com esta opção ativada, escolha uma porta de destino para a qual os pacotes serão redirecionados.



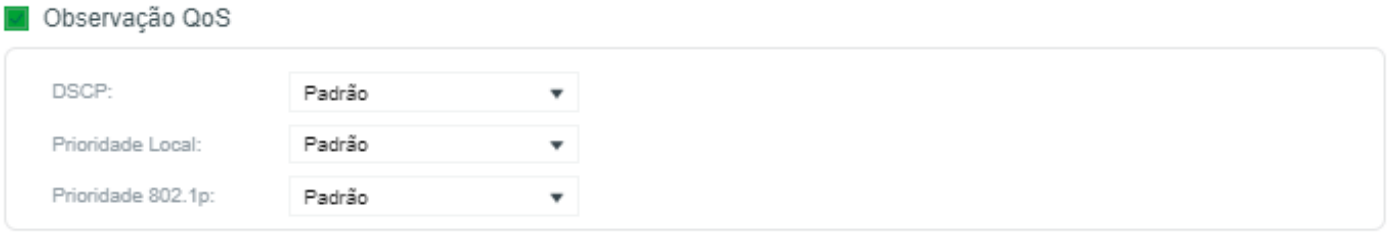
> No recurso Espelhamento, os pacotes correspondentes serão copiados para a porta de destino e o encaminhamento original não será afetado. Enquanto estiver no recurso Redirecionar, os pacotes correspondentes serão encaminhados apenas na porta de destino.

4. Na seção Política, ative ou desative o recurso Limite de taxa para os pacotes correspondentes. Com esta opção ativada, configure os parâmetros relacionados.

Taxa	Especifique a taxa de transmissão para os pacotes correspondentes.
Burst Size	Especifique o número máximo de bytes permitido em um segundo.

	Selecione a ação para os pacotes cuja taxa está além da taxa especificada.
Fora de Banda	**None:** os pacotes serão encaminhados normalmente. **Drop:** os pacotes serão descartados.

5. Na seção Política, ative ou desative o recurso Observação QoS para os pacotes correspondentes. Com essa opção ativada, configure os parâmetros relacionados e os valores observados entrarão em vigor no processamento de QoS no switch.



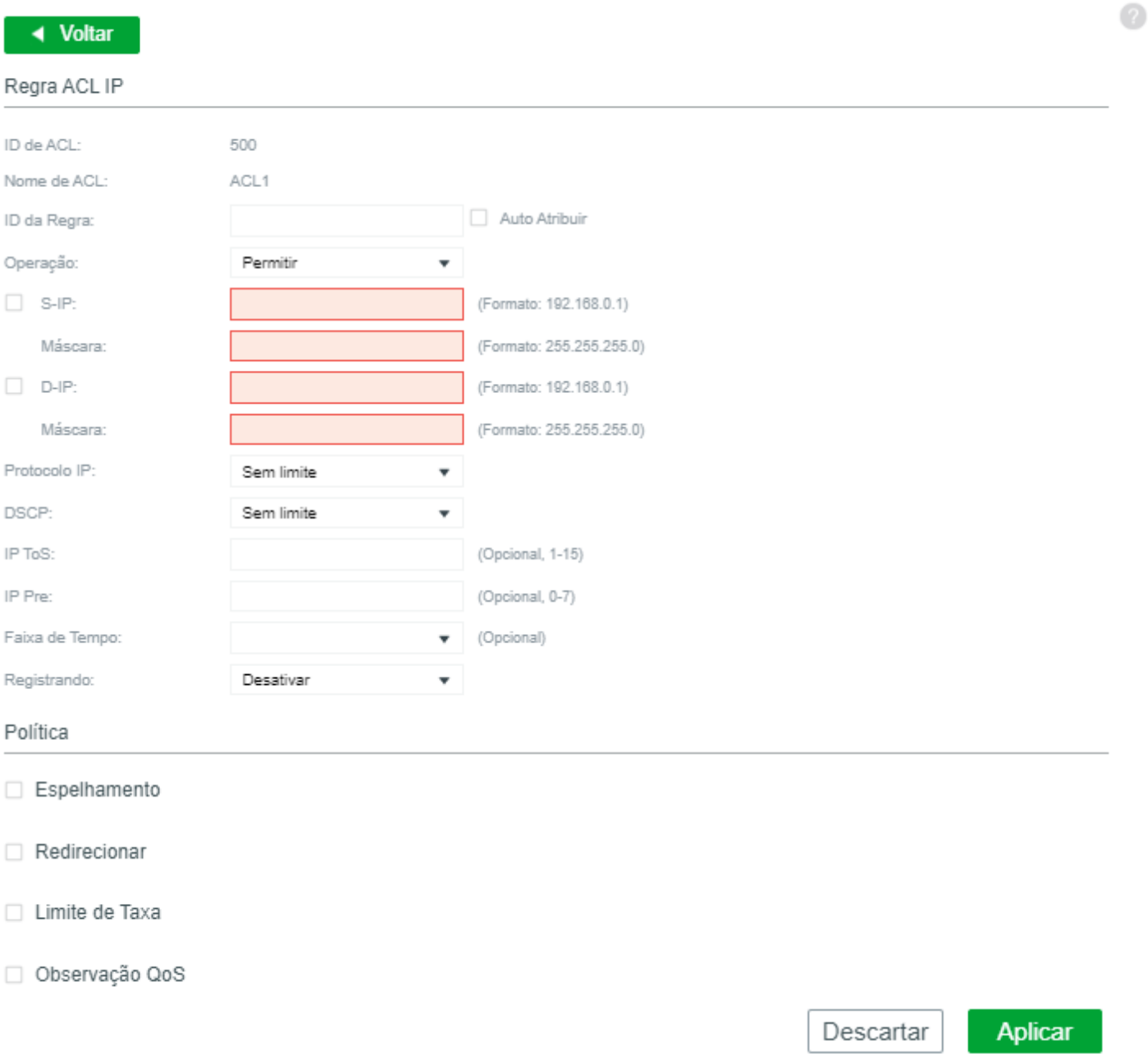
DSCP	Especifique o campo DSCP para os pacotes correspondentes. O campo DSCP dos pacotes será alterado para o especificado.
Prioridade Local	Especifique a prioridade local para os pacotes correspondentes. A prioridade local dos pacotes será alterada para a especificada.
Prioridade 802.1p	Especifique a prioridade 802.1p para os pacotes correspondentes. A prioridade 802.1p dos pacotes será alterada para a prioridade especificada.

6. Clique em **Aplicar**.

Configurando uma Regra IP ACL

Clique em **Editar ACL** em uma ACL do tipo IP ACL para carregar a página a seguir:

Na seção Configuração de Regras ACL, clique em Adicionar e a página a seguir será exibida.



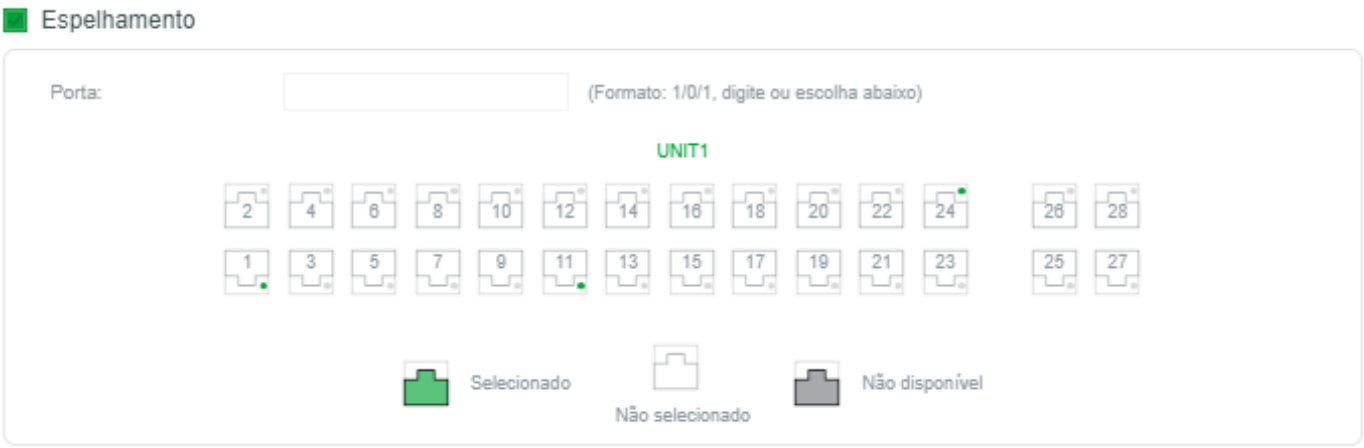
Siga os seguintes passos para configurar a regra ACL IP:

1. Na seção Regra ACL IP, configure os seguintes parâmetros:

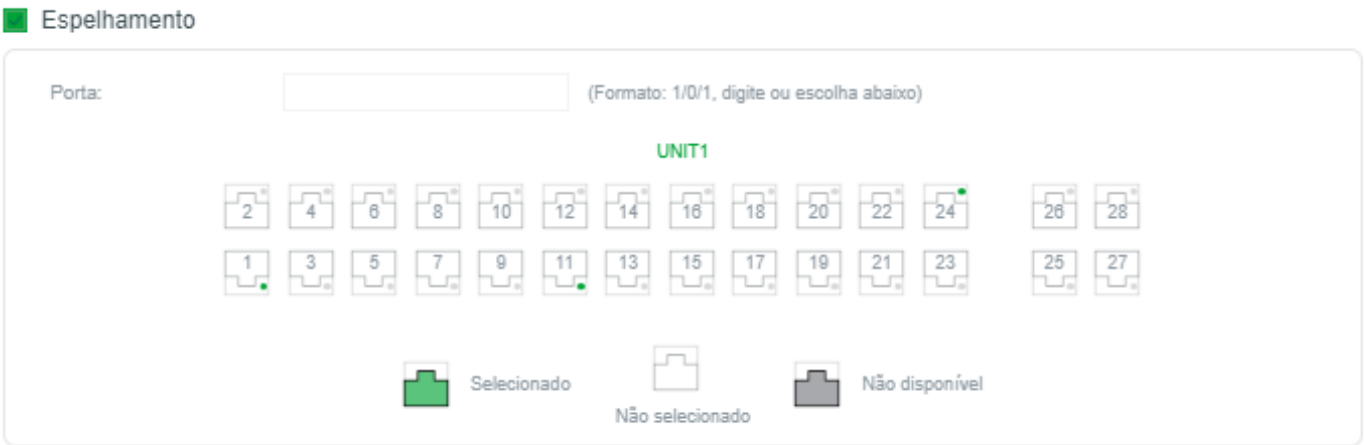
ID da Regra	Digite um número de identificação para identificar a regra. Não deve ser o mesmo que qualquer ID de regra atual na mesma ACL. Se você selecionar Atribuição automática, o ID da regra será atribuído automaticamente e o intervalo entre os IDs da regra será 5.
Operação	Selecione uma ação a ser tomada quando um pacote corresponder à regra. **Permitir:** encaminhar os pacotes correspondentes. **Negar:** para descartar os pacotes correspondentes.
S-IP / Máscara	Digite o endereço IP de origem com uma máscara. Um valor 1 na máscara indica que o bit correspondente no endereço será correspondido.
D-IP / Máscara	Digite o endereço IP de destino com uma máscara. Um valor 1 na máscara indica que o bit correspondente no endereço será correspondido.
Protocolo IP	Selecione um tipo de protocolo na lista suspensa. O padrão é Sem Limite, que indica que os pacotes de todos os protocolos serão correspondidos. Você também pode selecionar Definido pelo Usuário para personalizar o protocolo IP.
Flag TCP	Se o protocolo TCP estiver selecionado, você poderá configurar a Flag TCP para ser usada nas operações de correspondência da regra. Existem seis Flags e cada um tem três opções, que são *, 0 e 1. O padrão é *, que indica que o sinalizador não é usado para operações correspondentes. **URG:** bandeira urgente. **ACK:** Reconheça o sinalizador. **PSH:** Pressione a bandeira. **RST:** Redefinir sinalizador. **SYN:** Sincronizar sinalizador. **FIN:** Concluir sinalizador.
S-Port / D-Port	Se TCP / UDP estiver selecionado como protocolo IP, especifique o número da porta de origem e destino com uma máscara. **Valor:** especifique o número da porta. **Máscara:** especifique a máscara da porta com 4 números hexadecimais.
DSCP	Especifique um valor DSCP a ser correspondido entre 0 e 63. O padrão é Sem Limite.

IP ToS	Especifique um valor de IP ToS a ser correspondido entre 0 e 15.
IP Pre	Especifique um valor de Precedência de IP a ser correspondido entre 0 e 7.
Faixa de Tempo	Selecione um intervalo de tempo durante o qual a regra entrará em vigor. O valor padrão é sem limite, o que significa que a regra está sempre em vigor. O intervalo de tempo mencionado aqui pode ser criado na página **SISTEMA > Faixa de Horário**.
Registrando	Habilite a função Log para a regra da ACL. Em seguida, os horários em que a regra é correspondida serão registrados a cada 5 minutos e uma interceptação relacionada será gerada. Você pode consultar o Contador total de correspondências na Configuração de Regras ACL para visualizar os horários correspondentes.

2. Na seção Política, ative ou desative o recurso Espelhamento para os pacotes correspondentes. Com esta opção ativada, escolha uma porta de destino para a qual os pacotes serão espelhados.

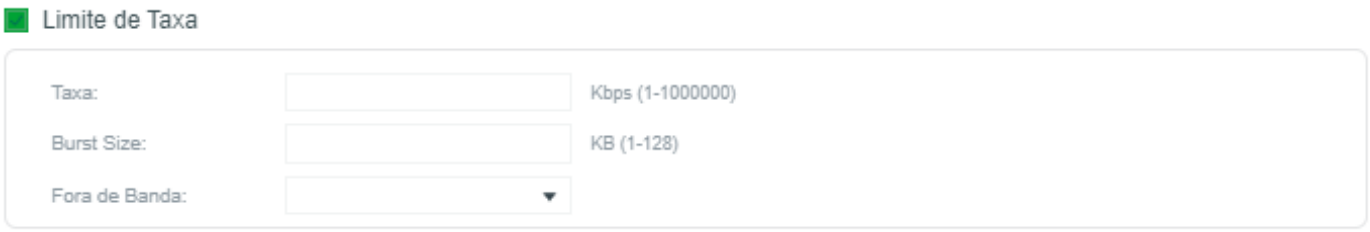


3. Na seção Política, ative ou desative o recurso Redirecionar para os pacotes correspondentes. Com esta opção ativada, escolha uma porta de destino para a qual os pacotes serão redirecionados.



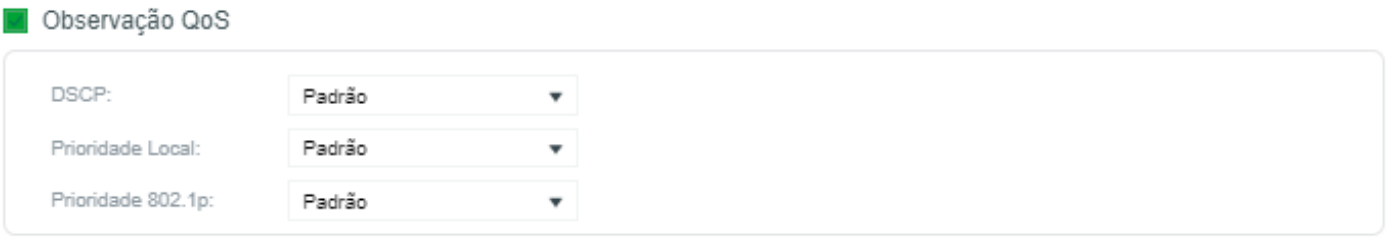
No recurso Espelhamento, os pacotes correspondentes serão copiados para a porta de destino e o encaminhamento original não será afetado. Enquanto estiver no recurso Redirecionar, os pacotes correspondentes serão encaminhados apenas na porta de destino.

4. Na seção Política, ative ou desative o recurso Limite de taxa para os pacotes correspondentes. Com esta opção ativada, configure os parâmetros relacionados.



Taxa	Especifique a taxa de transmissão para os pacotes correspondentes.
Burst Size	Especifique o número máximo de bytes permitido em um segundo.
Fora de Banda	Selecione a ação para os pacotes cuja taxa está além da taxa especificada. **None:** os pacotes serão encaminhados normalmente. **Drop:** os pacotes serão descartados.

5. Na seção Política, ative ou desative o recurso Observação QoS para os pacotes correspondentes. Com essa opção ativada, configure os parâmetros relacionados e os valores observados entrarão em vigor no processamento de QoS no switch.



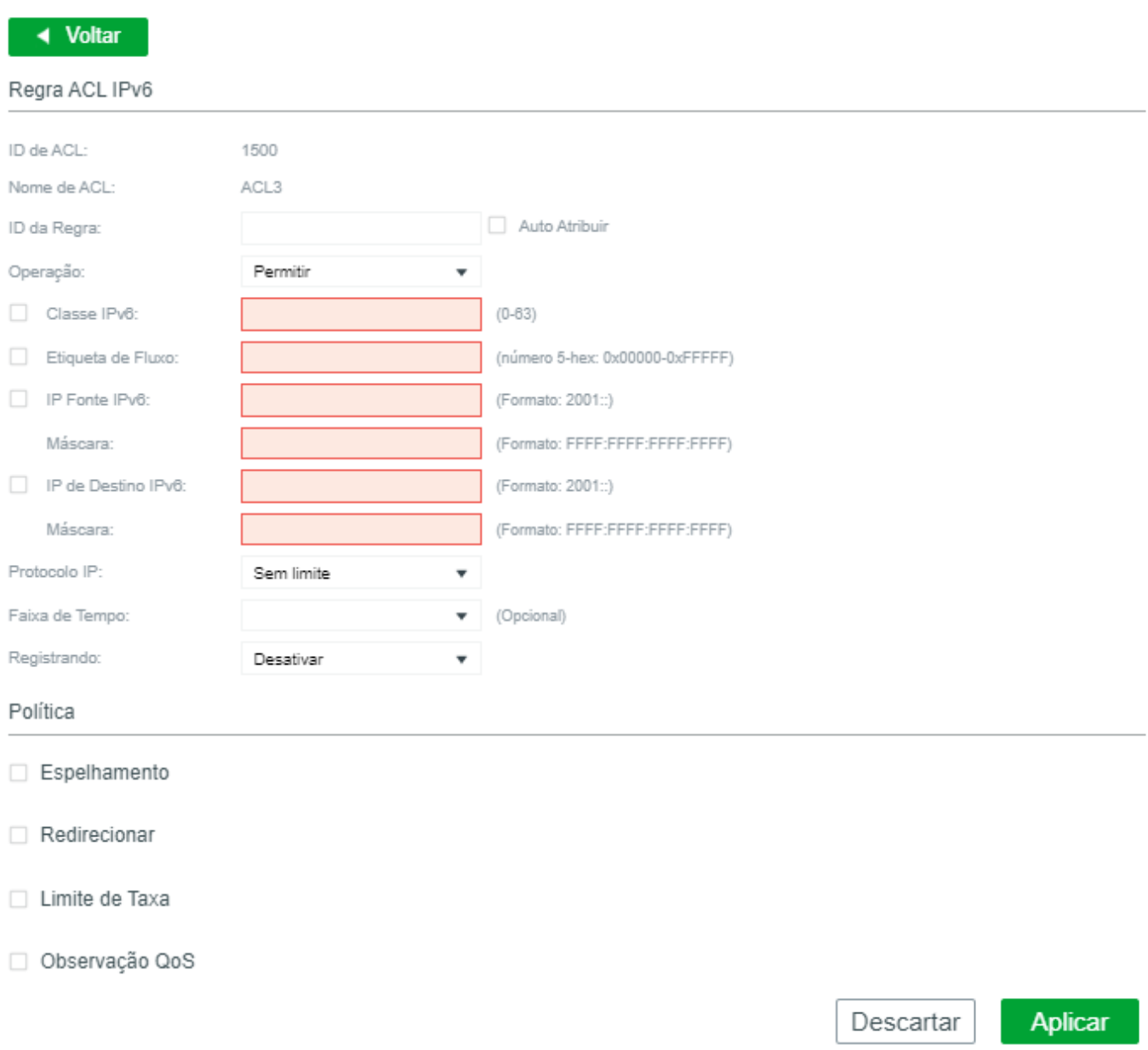
DSCP	Especifique o campo DSCP para os pacotes correspondentes. O campo DSCP dos pacotes será alterado para o especificado.
Prioridade Local	Especifique a prioridade local para os pacotes correspondentes. A prioridade local dos pacotes será alterada para a especificada.
Prioridade 802.1p	Especifique a prioridade 802.1p para os pacotes correspondentes. A prioridade 802.1p dos pacotes será alterada para a prioridade especificada.

6. Clique em **Aplicar**.

Configurando uma Regra ACL IPv6

Clique em **Editar ACL** em uma ACL do tipo ACL IPv6 para carregar a página a seguir:

Na seção Configuração de Regras ACL, clique em Adicionar e a página a seguir será exibida.



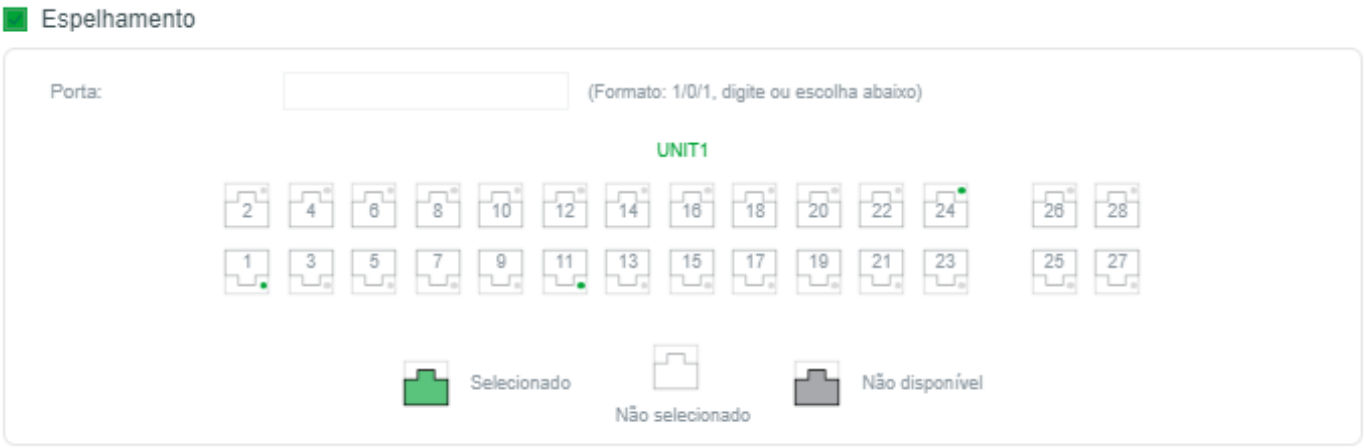
Siga os seguintes passos para configurar a regra ACL IPv6:

1. Na seção Regra ACL IP, configure os seguintes parâmetros:

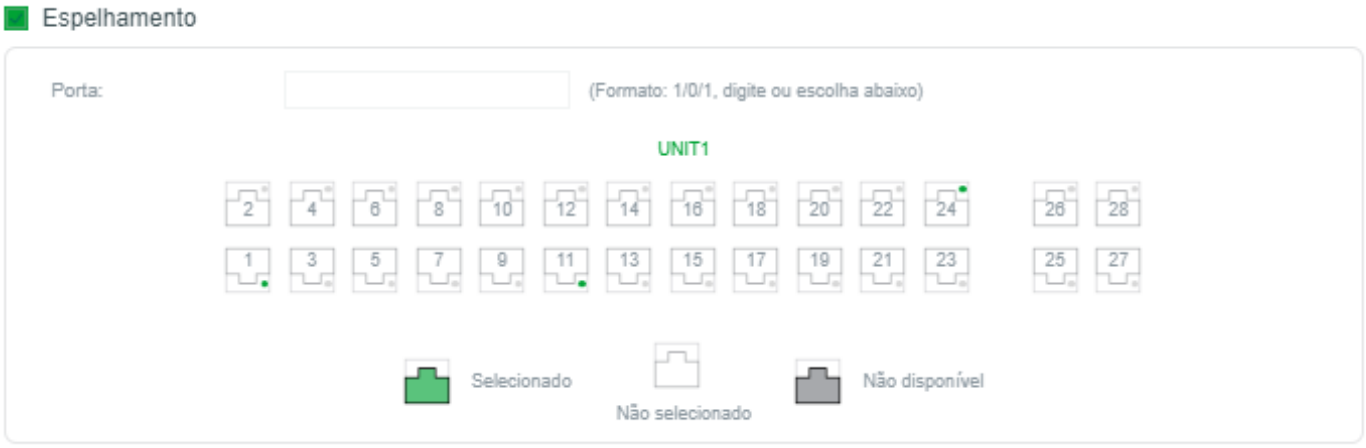
ID da Regra	Digite um número de identificação para identificar a regra. Não deve ser o mesmo que qualquer ID de regra atual na mesma ACL. Se você selecionar Atribuição automática, o ID da regra será atribuído automaticamente e o intervalo entre os IDs da regra será 5.
Operação	Selecione uma ação a ser tomada quando um pacote corresponder à regra. **Permitir:** encaminhar os pacotes correspondentes. **Negar:** para descartar os pacotes correspondentes.
Classe IPv6	Especifique um valor de classe IPv6 a ser correspondido. O switch verificará o campo de classe do cabeçalho IPv6.
Etiqueta de Fluxo	Especifique um valor de Etiqueta de Fluxo a ser correspondido.
IP Fonte IPv6	Digite o endereço IPv6 de origem a ser correspondido. Todos os tipos de endereço IPv6 serão verificados. Você pode inserir um endereço IPv6 completo de 128 bits, mas apenas os primeiros 64 bits serão válidos.
Máscara	A máscara é necessária se o endereço IPv6 de origem for inserido. Digite a máscara no formato completo (por exemplo, FFFF: FFFF: 0000: FFFF). A máscara de endereço IP especifica quais bits no endereço IPv6 de origem devem corresponder à regra. Um valor F na máscara indica que o bit correspondente no endereço será correspondido.
IP de Destino IPv6	Digite o endereço IPv6 de destino a ser correspondido. Todos os tipos de endereço IPv6 serão verificados. Você pode inserir um endereço IPv6 completo de 128 bits, mas apenas os primeiros 64 bits serão válidos.
Máscara	A máscara é necessária se o endereço IPv6 de origem for inserido. Digite a máscara no formato completo (por exemplo, FFFF: FFFF: 0000: FFFF). A máscara de endereço IP especifica quais bits no endereço IPv6 de origem devem corresponder à regra. Um valor F na máscara indica que o bit correspondente no endereço será correspondido.

Protocolo IP	Selecione um tipo de protocolo na lista suspensa. **Sem limite:** pacotes de todos os protocolos serão correspondidos. **UDP:** especifique a porta de origem e a porta de destino para o pacote UDP a ser correspondido. **TCP:** especifique a porta de origem e a porta de destino para o pacote TCP corresponder. **Definido pelo usuário:** você pode personalizar um protocolo IP.
S-Port / D-Port	Se TCP / UDP estiver selecionado como protocolo IP, especifique os números das portas de origem e de destino.
Faixa de Tempo	Selecione um intervalo de tempo durante o qual a regra entrará em vigor. O valor padrão é sem limite, o que significa que a regra está sempre em vigor. O intervalo de tempo mencionado aqui pode ser criado na página **SISTEMA > Faixa de Horário**.
Registrando	Habilite a função Log para a regra da ACL. Em seguida, os horários em que a regra é correspondida serão registrados a cada 5 minutos e uma interceptação relacionada será gerada. Você pode consultar o Contador total de correspondências na Configuração de Regras ACL para visualizar os horários correspondentes.

2. Na seção Política, ative ou desative o recurso Espelhamento para os pacotes correspondentes. Com esta opção ativada, escolha uma porta de destino para a qual os pacotes serão espelhados.

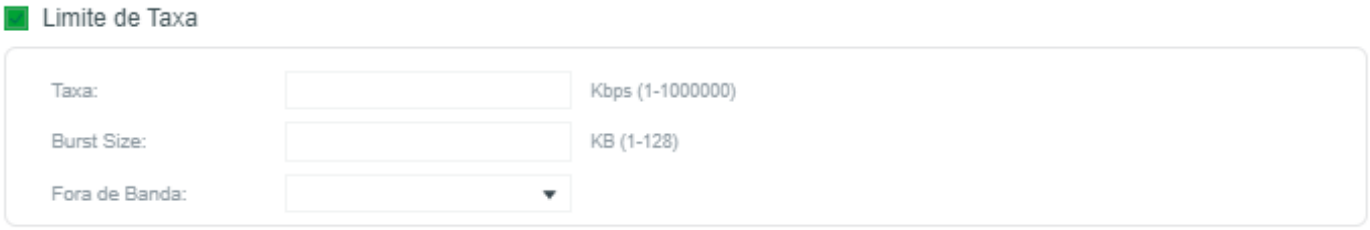


3. Na seção Política, ative ou desative o recurso Redirecionar para os pacotes correspondentes. Com esta opção ativada, escolha uma porta de destino para a qual os pacotes serão redirecionados.



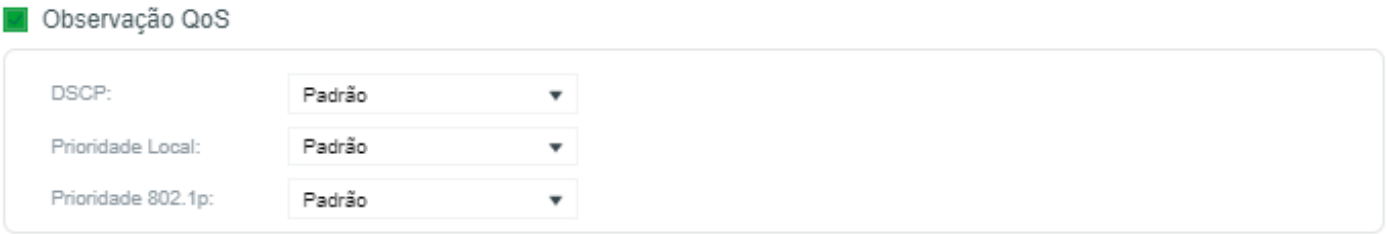
No recurso Espelhamento, os pacotes correspondentes serão copiados para a porta de destino e o encaminhamento original não será afetado. Enquanto estiver no recurso Redirecionar, os pacotes correspondentes serão encaminhados apenas na porta de destino.

4. Na seção Política, ative ou desative o recurso Limite de taxa para os pacotes correspondentes. Com esta opção ativada, configure os parâmetros relacionados.



Taxa	Especifique a taxa de transmissão para os pacotes correspondentes.
Burst Size	Especifique o número máximo de bytes permitido em um segundo.
Fora de Banda	Selecione a ação para os pacotes cuja taxa está além da taxa especificada. **None:** os pacotes serão encaminhados normalmente. **Drop:** os pacotes serão descartados.

5. Na seção Política, ative ou desative o recurso Observação QoS para os pacotes correspondentes. Com essa opção ativada, configure os parâmetros relacionados e os valores observados entrarão em vigor no processamento de QoS no switch.



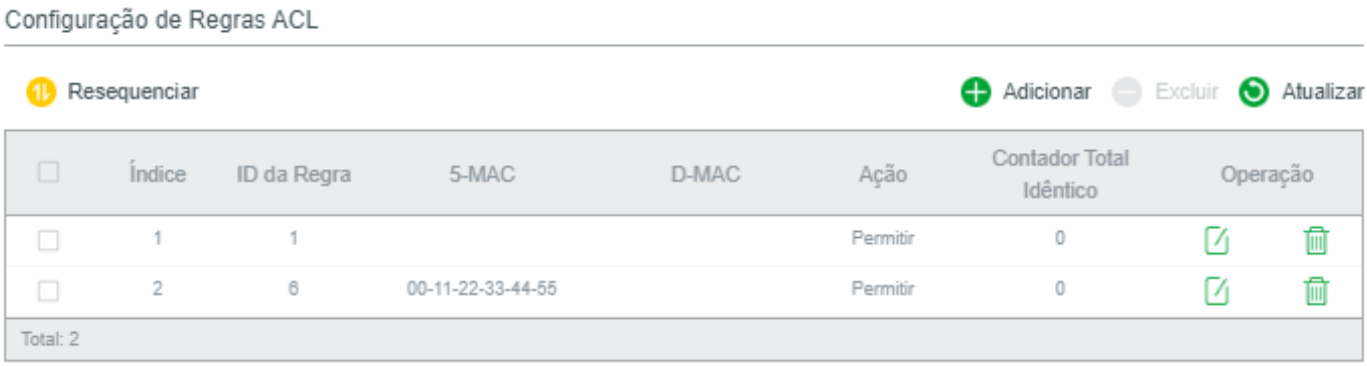
DSCP	Especifique o campo DSCP para os pacotes correspondentes. O campo DSCP dos pacotes será alterado para o especificado.
Prioridade Local	Especifique a prioridade local para os pacotes correspondentes. A prioridade local dos pacotes será alterada para a especificada.
Prioridade 802.1p	Especifique a prioridade 802.1p para os pacotes correspondentes. A prioridade 802.1p dos pacotes será alterada para a prioridade especificada.

6. Clique em **Aplicar**.

Visualizando Regras ACL

As regras em uma ACL são listadas em ordem crescente de seus ID da Regra. O switch combina um pacote recebido com as regras em ordem. Quando um pacote corresponde a uma regra, o switch interrompe o processo de correspondência e executa a ação definida na regra.

Clique em , para editar uma entrada que você criou, será possível visualizar a tabela de regras. Tomamos a tabela de regras de IP ACL, por exemplo.



Aqui você pode visualizar e editar as regras da ACL. Você também pode clicar em Resequenciar para ressequênciar as regras, fornecendo o ID de início e um valor de Passo.

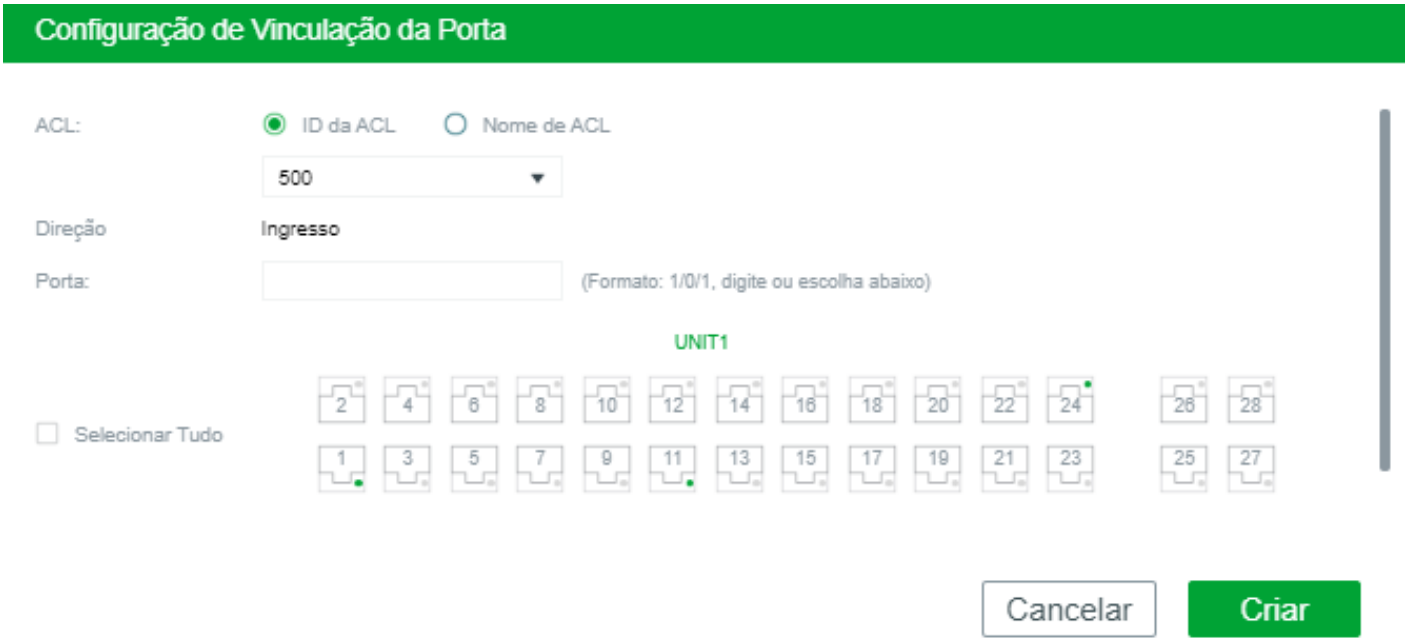
Configurando Vínculo ACL

Você pode vincular a ACL a uma porta ou uma VLAN. Os pacotes recebidos na porta ou na VLAN serão correspondidos e processados de acordo com as regras da ACL. Uma ACL entra em vigor somente após ser vinculada a uma porta ou VLAN.

> Diferentes tipos de ACLs não podem ser vinculados à mesma porta ou VLAN.
>
> Várias ACLs do mesmo tipo podem ser ligadas à mesma porta ou VLAN. O switch corresponde aos pacotes recebidos usando as ACLs em ordem. A ACL de menor ID da Regra tem uma prioridade mais alta.

Vinculando a ACL a uma porta

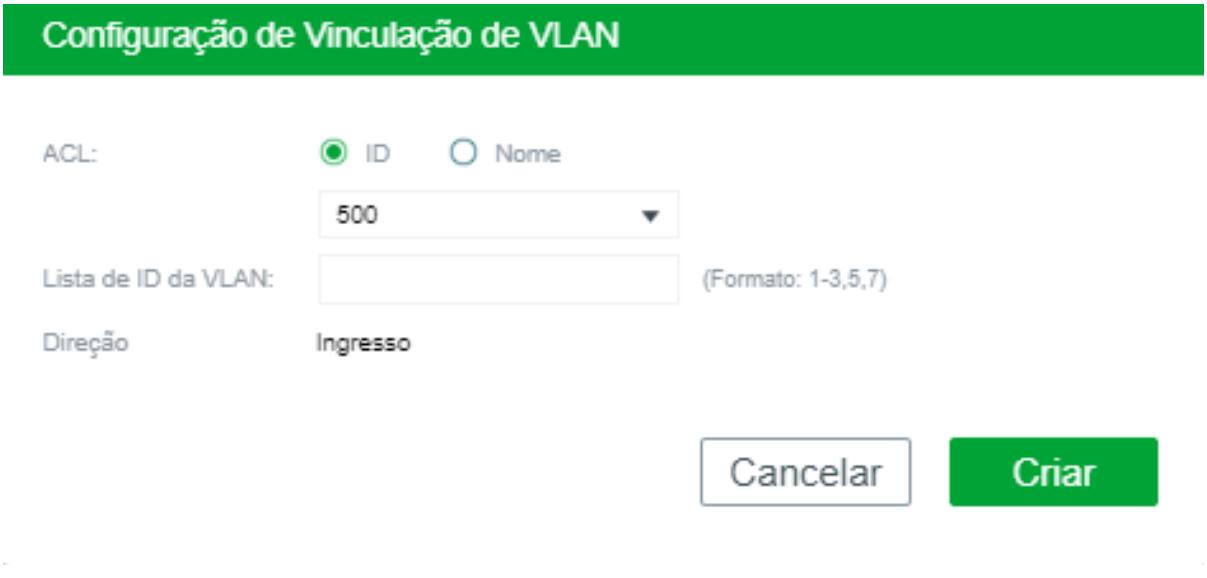
Escolha o menu **SEGURANÇA > ACL > Vínculo ACL > Vínculo de Porta** e clique em Adicionar para carregar a seguinte página.



Siga estas etapas para ligar a ACL a uma porta:

1. Escolha ID da ACL ou Nome de ACL a ser usado para corresponder à ACL. Em seguida, selecione uma ACL na lista suspensa.
2. Especifique a porta a ser vinculada.
3. Clique em **Criar**.

Escolha o menu **SEGURANÇA > ACL > Vínculo ACL > Vínculo VLAN** e clique em Adicionar para carregar a seguinte página.



Siga estas etapas para ligar a ACL a uma VLAN:

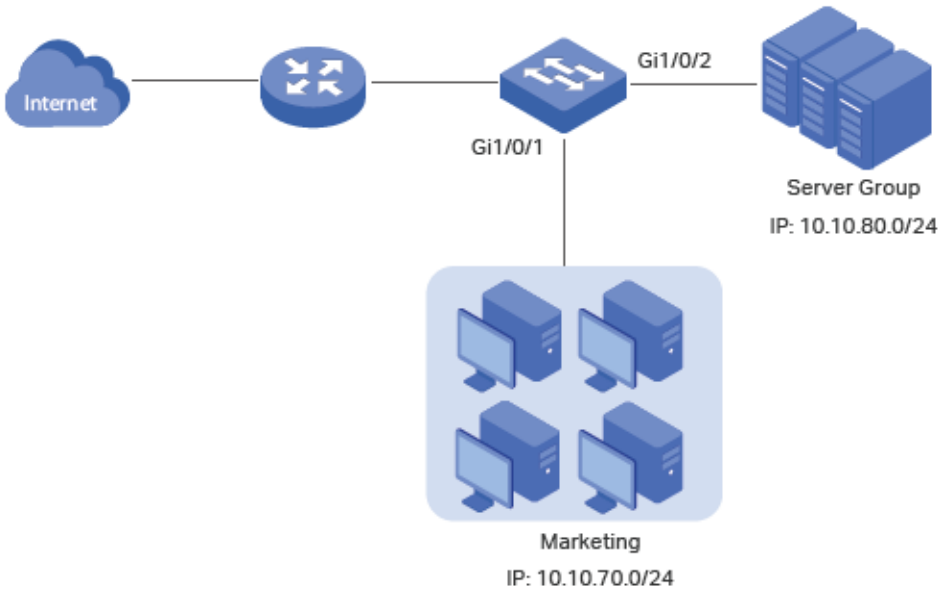
1. Escolha ID ou Nome a ser usado para corresponder à ACL. Em seguida, selecione uma ACL na lista suspensa.
2. Digite o ID da VLAN a ser vinculada.
3. Clique em **Criar**.

Exemplo de Configuração

Requisitos de Rede

Como mostrado abaixo, o grupo de servidores internos de uma empresa pode fornecer diferentes tipos de serviços.

Os computadores no departamento de Marketing estão conectados ao switch pela porta 1/0/1 e o grupo de servidores interno está conectado ao switch pela porta 1/0/2.



É necessário que:

- O departamento de Marketing pode acessar apenas o grupo de servidores internos na intranet.
- O departamento de marketing pode visitar apenas sites HTTP e HTTPS na internet.

Configurando o Cenário

Para atender aos requisitos acima, você pode configurar a filtragem de pacotes criando uma ACL IP e configurando regras para ela.

Configuração ACL

Crie uma ACL IP e configure as seguintes regras para ela:

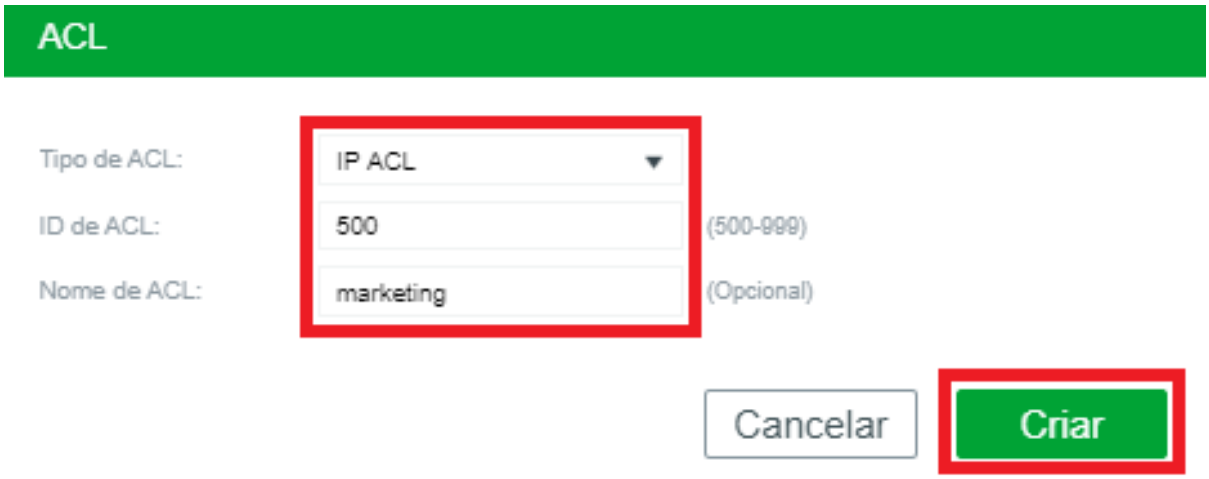
- Configure uma regra de permissão para corresponder aos pacotes com o endereço IP de origem 10.10.70.0/24 e o endereço IP de destino 10.10.80.0/24. Esta regra permite que o departamento de Marketing acesse servidores de rede internos da intranet.
- Configure quatro regras de permissão para combinar os pacotes com o endereço IP de origem 10.10.70.0/24 e as portas de destino TCP 80, TCP 443 e TCP / UDP 53. Isso permite que o departamento de Marketing visite sites HTTP e HTTPS na Internet.
- Configure uma regra de negação para combinar os pacotes com o endereço IP de origem 10.10.70.0/24. Esta regra bloqueia outros serviços de rede.

O switch combina os pacotes com as regras em ordem, começando com a Regra 1. Se um pacote corresponde a uma regra, o switch interrompe o processo de correspondência e inicia a ação definida na regra.

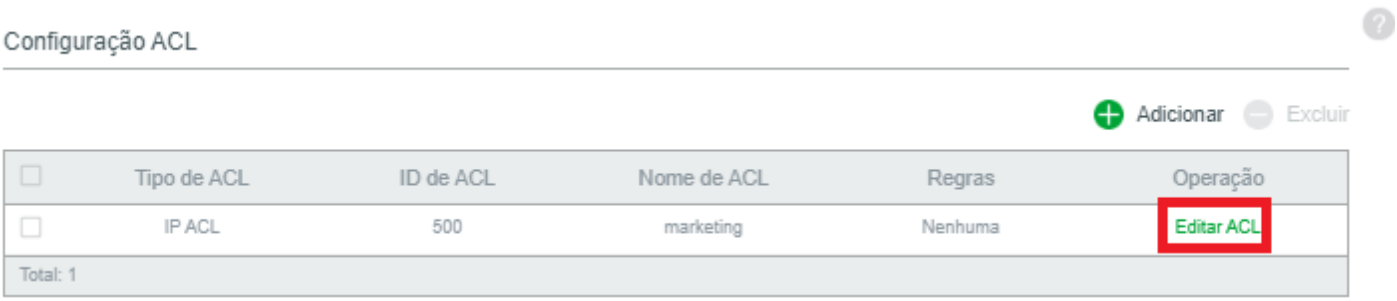
Configuração de Vínculo

Vincule a ACL IP à porta 1/0/1 para que as regras da ACL se apliquem apenas ao departamento de Marketing.

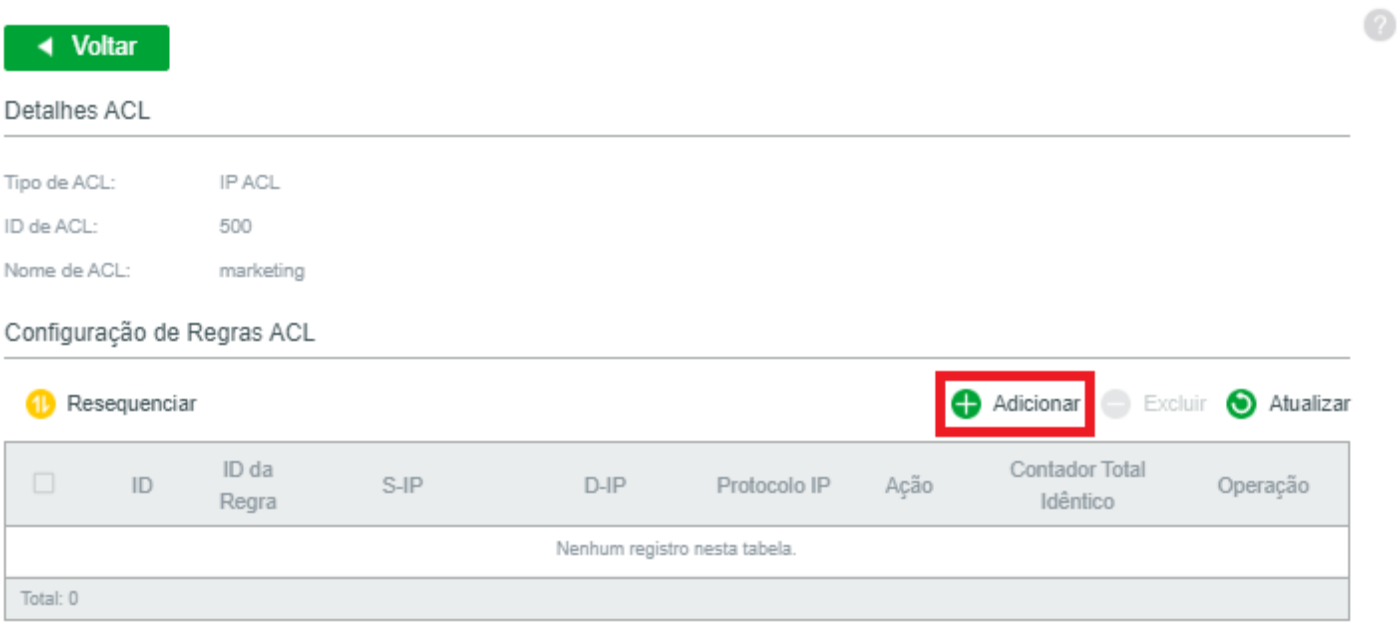
1. Escolha o menu SEGURANÇA > ACL > Configuração ACL e clique em para carregar a seguinte página. Em seguida, crie uma ACL IP para o departamento de marketing.



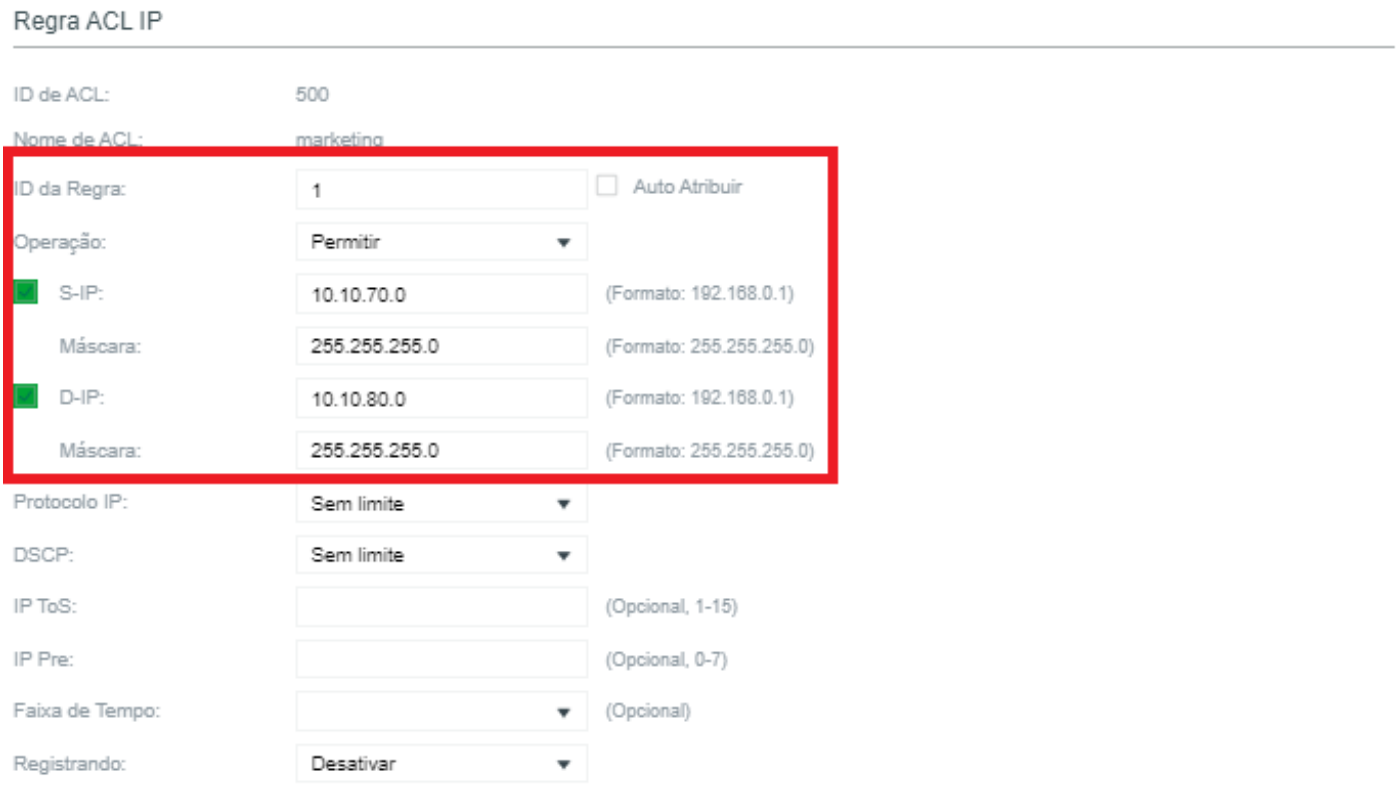
2. Clique em Editar ACL na coluna de Operação.



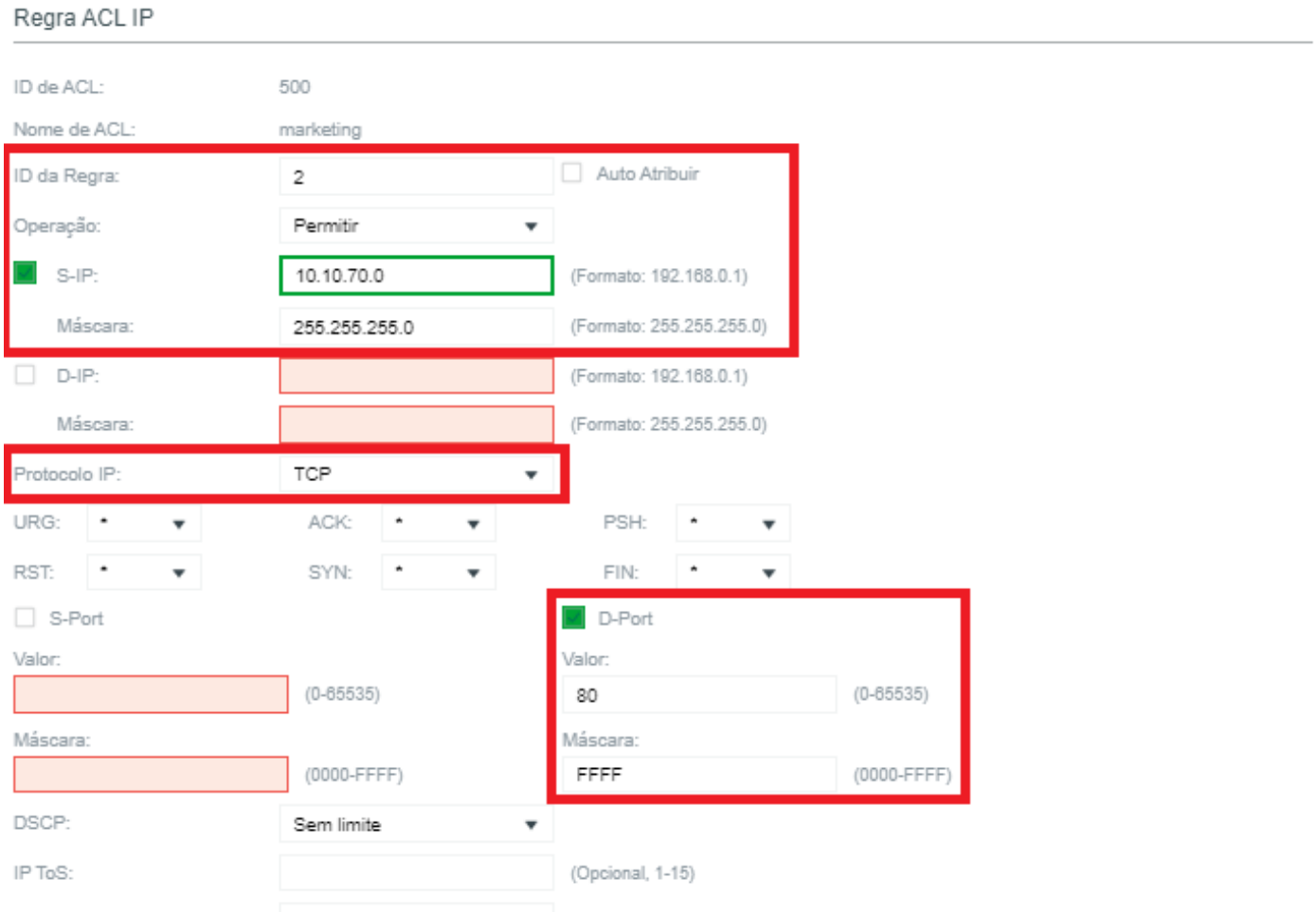
3. Na página de configuração da ACL, clique em Adicionar .



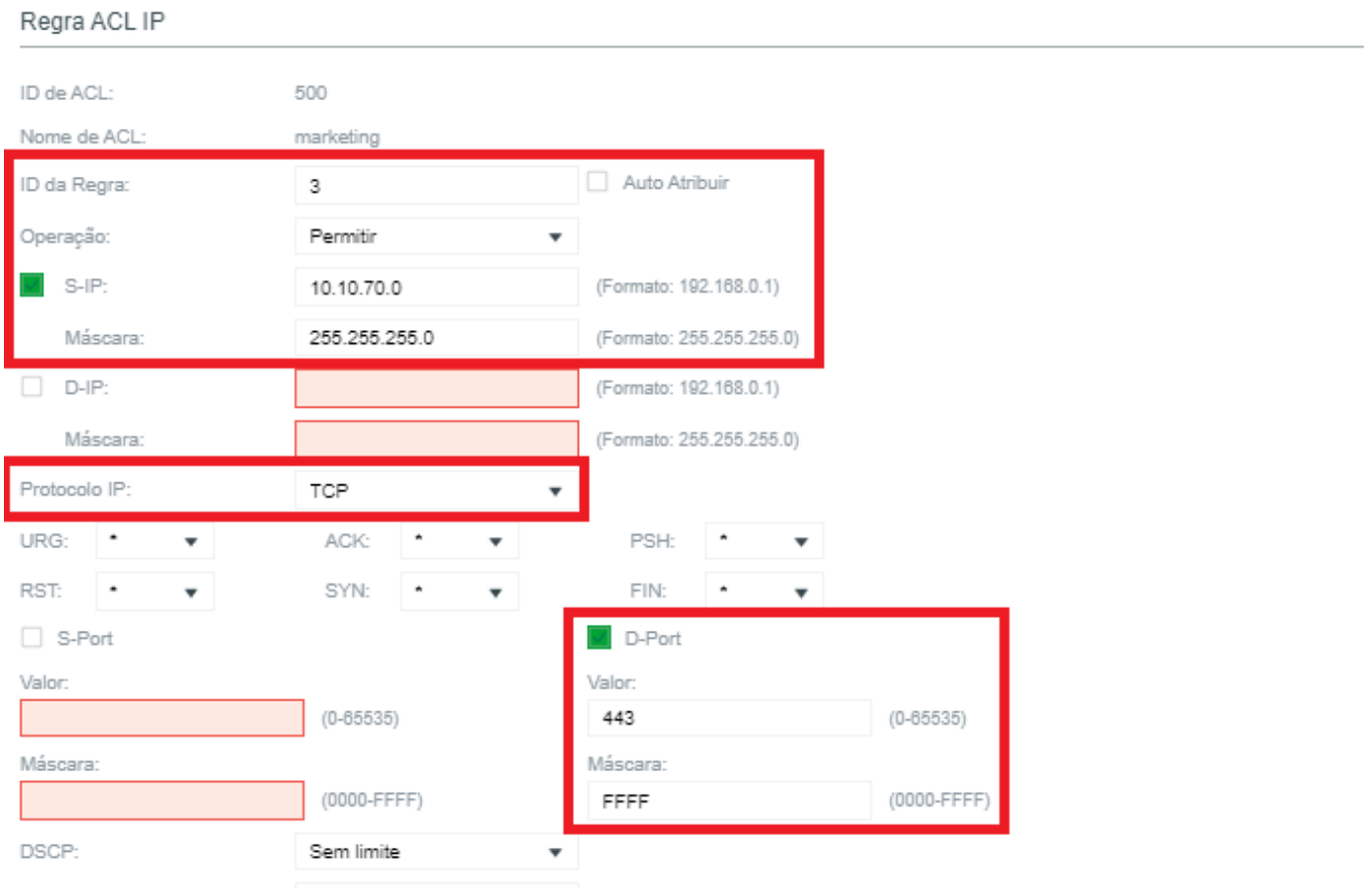
4. Configure a regra 1 para permitir pacotes com o endereço IP de origem 10.10.70.0/24 e o endereço IP de destino 10.10.80.0/24.



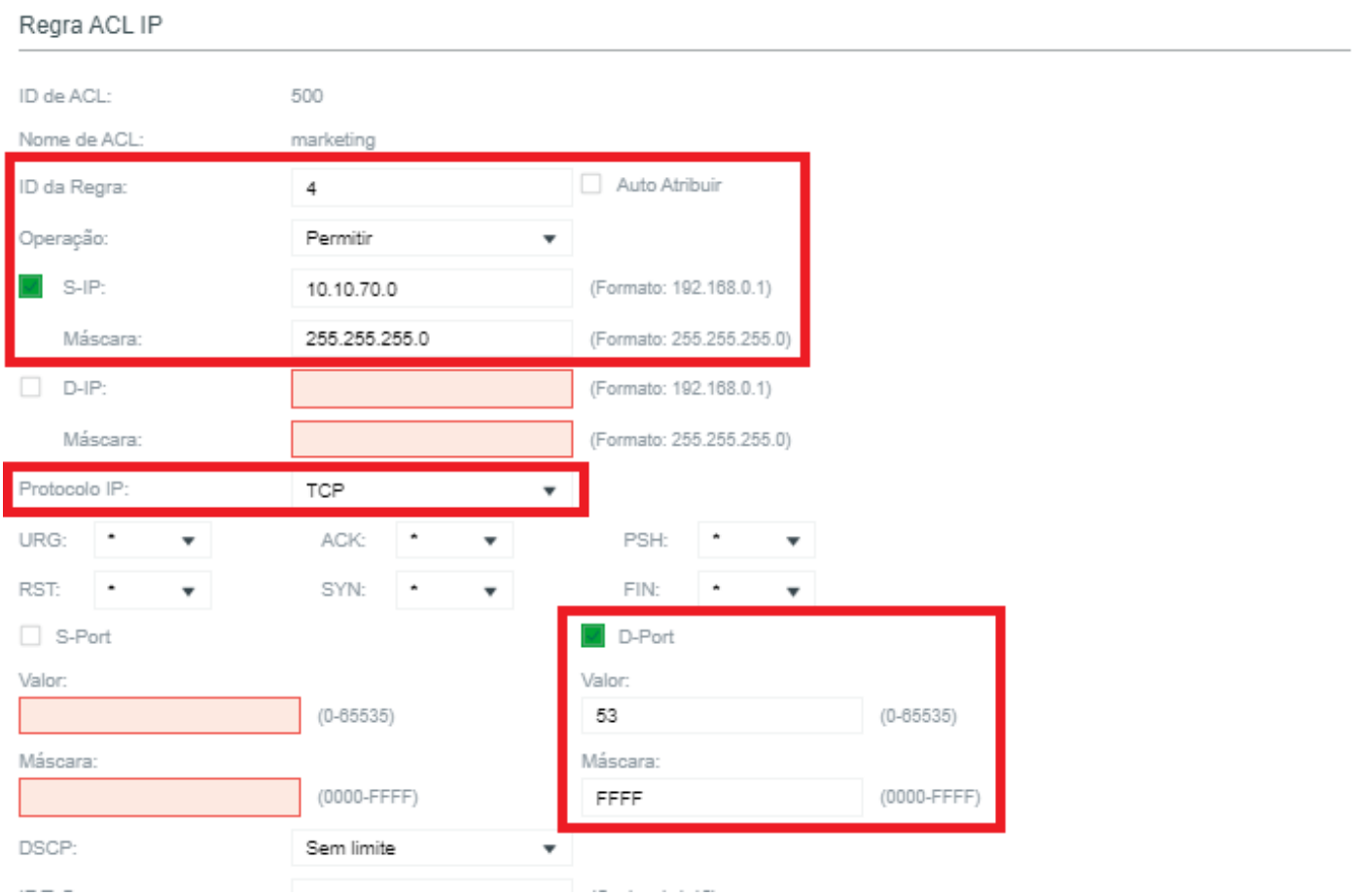
5. Da mesma forma, configure a regra 2 para permitir pacotes com IP de origem 10.10.70.0 e porta de destino TCP 80 (porta de serviço HTTP).



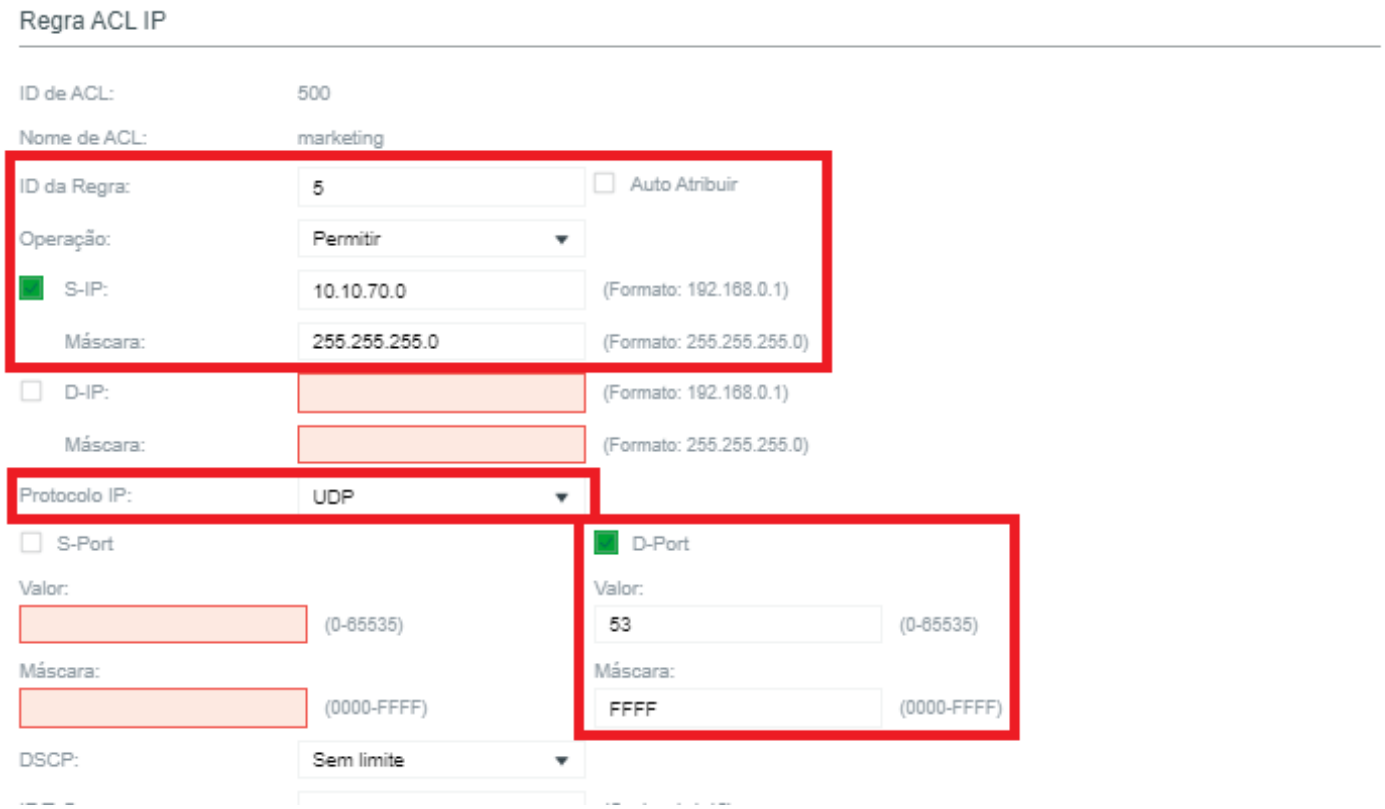
6. Configure também a regra 3 para permitir pacotes com IP de origem 10.10.70.0 e porta de destino TCP 443 (porta de serviço HTTPS).



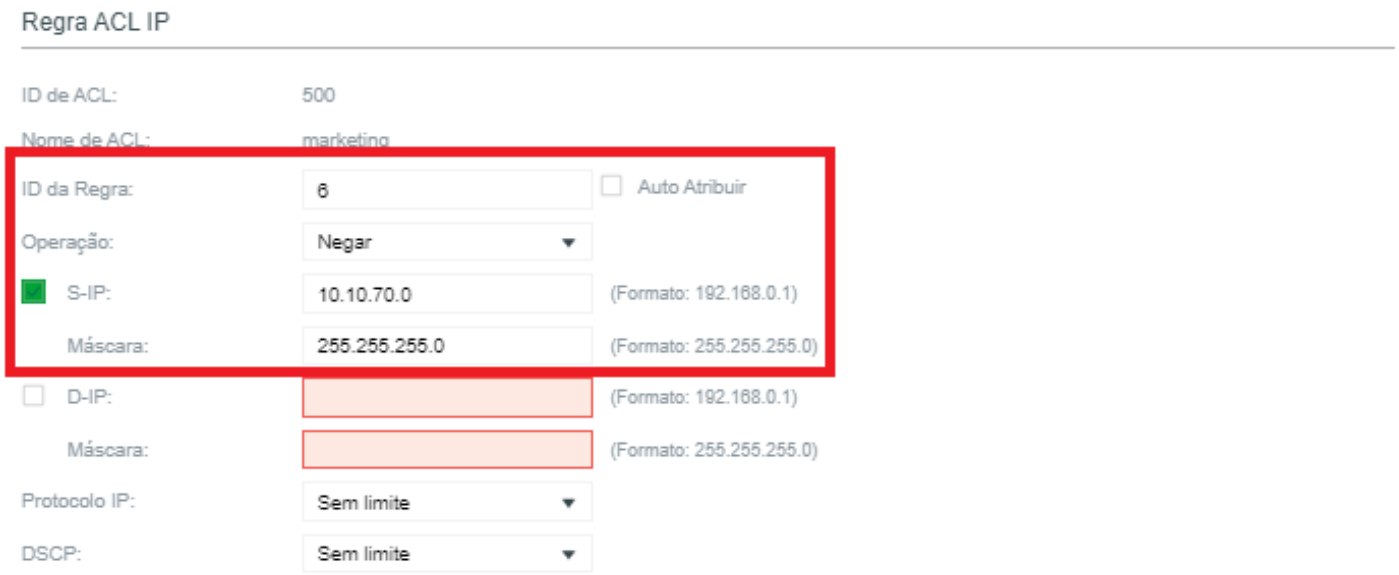
7. Configure a regra 4 para permitir pacotes com o IP de origem 10.10.70.0 e com a porta de destino TCP 53.



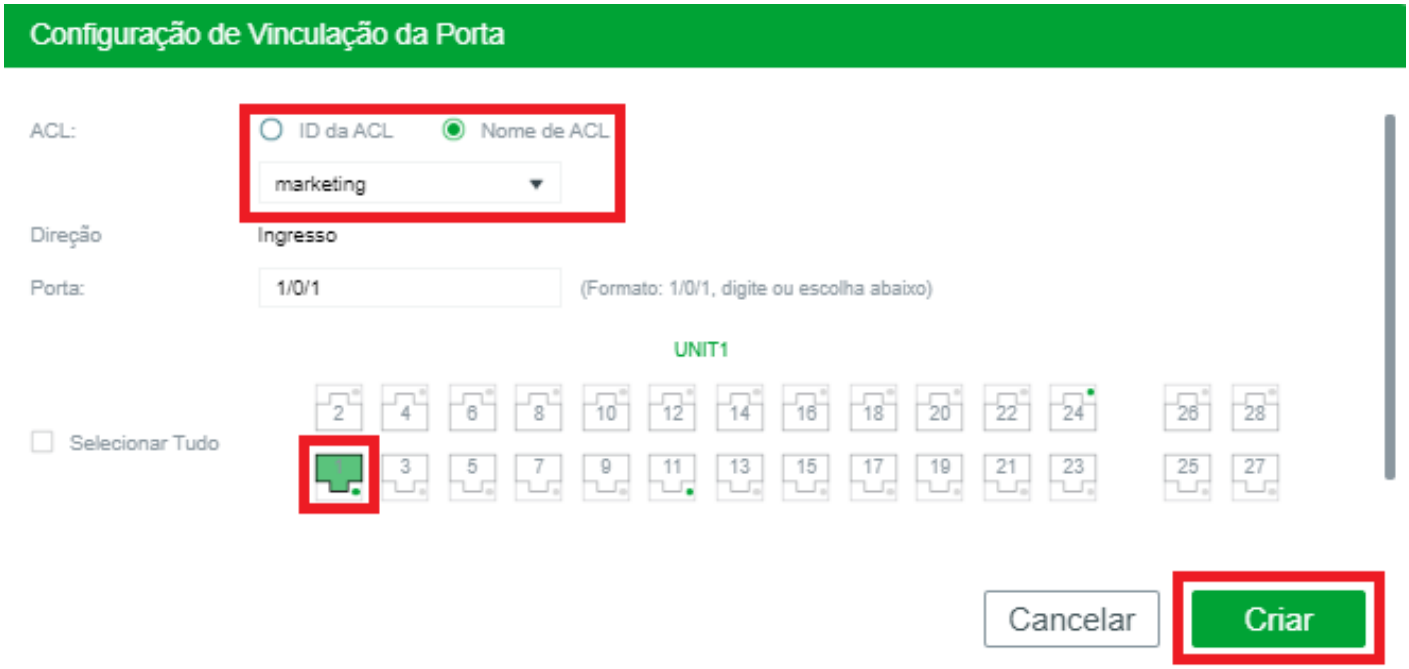
8. Da mesma maneira, configure a regra 5 para permitir pacotes com o IP de origem 10.10.70.0 e com a porta de destino UDP 53 (porta de serviço DNS).



9. Configure a regra 6 para negar pacotes com o IP de origem 10.10.70.0.



10. Escolha o menu **SEGURANÇA > ACL > Vínculo ACL > Vínculo de Porta** e clique em Adicionar para carregar a seguinte página. Vincule a ACL marketing à porta 1/0/1 para que ela entre em vigor.



11. Clique em Salvar para salvar as configurações.

Apêndice: Configuração Padrão

As configurações padrão da ACL estão listadas nas seguintes tabelas:

Configurações ACL MAC

Parâmetros	Configurações Padrão
Operação	Permitido
Prioridade de usuário	Sem Limite
Intervalo de tempo	Sem Limite

Configurações ACL IP

Parâmetros	Configurações Padrão
Operação	Permitido
Protocolo IP	Todos
DSCP	Sem Limite
IP ToS	Sem Limite
IP Pre	Sem Limite
Intervalo de tempo	Sem Limite

Configurações ACL IPv6

Parâmetros	Configurações Padrão
Operação	Permitido
Intervalo de tempo	Sem Limite

Configurações Política

Parâmetros	Configurações Padrão
Espelhamento	Desativado
Redirecionamento	Desativado
Limite de Taxa	Desativado
Observação QoS	Desativado

IPv4 IMPB

Visão Geral

O IPv4 IMPB (IP-MAC-Port Binding) é utilizado para ligar o endereço de IP, o endereço MAC, a VLAN ID e o número da porta ligado do host especificado. Baseando-se na tabela de ligação, o switch pode impedir os ataques cheating ARP com o recurso de ARP Detection, e filtrar os pacotes que não correspondem as entradas de ligação com o recurso IP Source Guard.

Funções Suportadas

IP-MAC Binding

Este recurso é usado para adicionar entradas binding. As entradas binding podem ser configuradas manualmente, ou serem aprendidas por ARP scanning, ou DHCP snooping. As funções ARP Detection and IPv4 Source Guard são baseadas nas entradas de ligação IP-MAC.

ARP Detection

Em uma rede real e complexa, existem altos riscos de segurança durante o procedimento de implementação do ARP. Os ataques cheating against ARP, faz com que a porta de entrada imite o gateway, enganando hosts e inundando a rede com pacotes ARP.

O ARP Detection pode evitar que a rede receba esses ataques.

- Prevenir os ataques ARP Cheating
  Com base nas entradas de IP-MAC Binding, o ARP Detection pode ser configurado para detectar os pacotes ARP, e filtrar os ilegais, de modo a evitar que a rede receba os ARP cheating attacks.
- Prevenir os ataques ARP Flooding
  Você pode limitar a velocidade de recebimento dos pacotes ARP legais na porta para evitar o ARP Flooding Attack.

IPv4 Source Guard

O IPv4 Source Guard é usado para filtrar os pacotes IPv4 com base na tabela de ligação IP-MAC. Apenas os pacotes que combinam com as regras de ligação são encaminhados.

Configuração do Vínculo IP-MAC

Você pode adicionar o IP-MAC Binding de três formas:

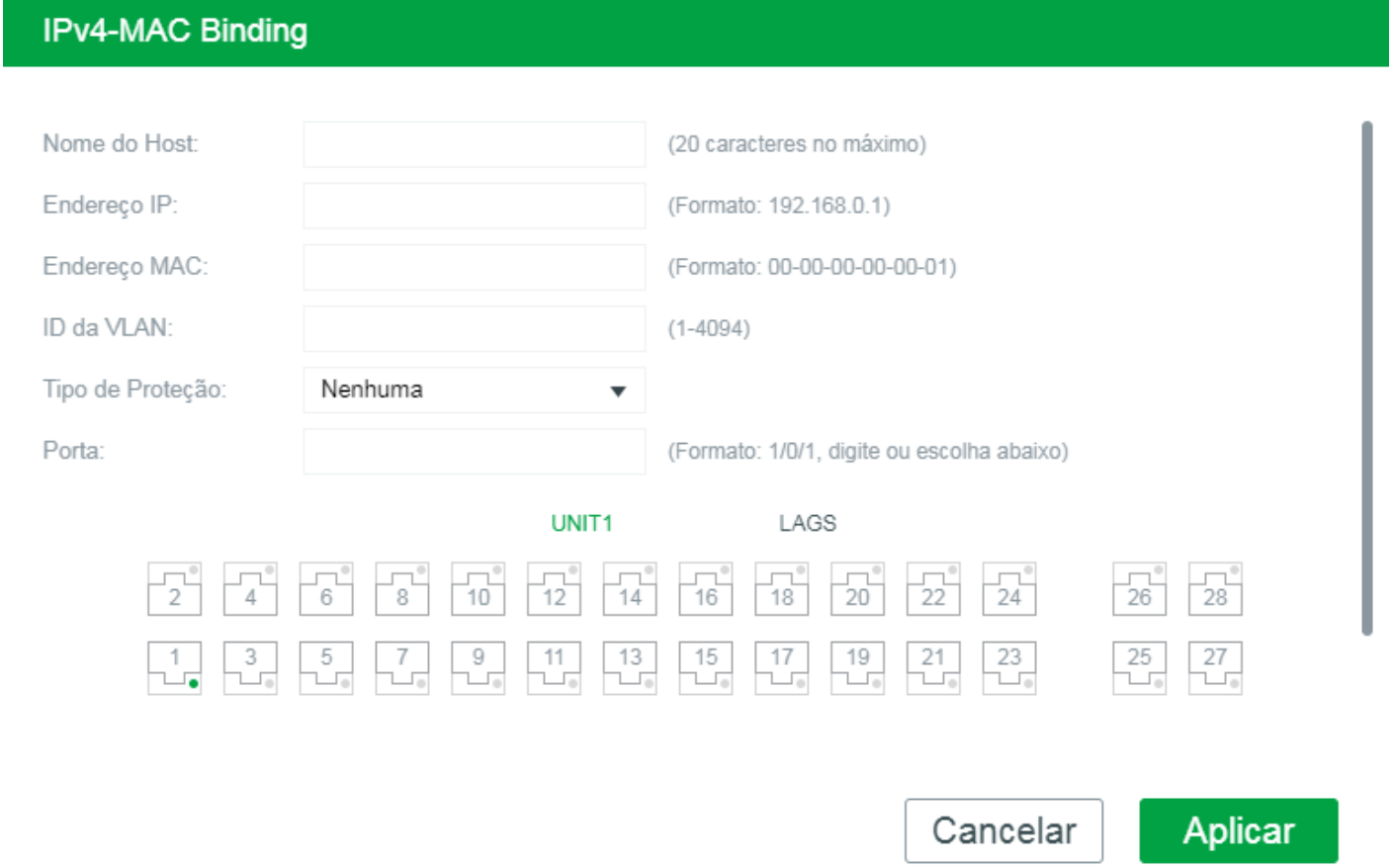
- Via Manual Binding
- Via ARP Scanning
- Via DHCP Snooping

Além disso, você pode visualizar, pesquisar e editar as entradas na tabela de ligação.

Entradas de Vínculo manual

Você pode vincular manualmente o endereço IP, endereço MAC, VLAN ID e o número da porta em conjunto com a condição e a informação detalhada que você tem dos hosts.

Selecione no menu **SEGURANÇA > IPv4 IMPB > IP-MAC Binding > Vinculo Manual** e clique em Adicionar para carregar a página a seguir.



Siga os passos abaixo para criar manualmente uma entrada IP-MAC Binding:

1. Preencha as seguintes informações para especificar um host.

Nome do Host	Digite o nome do host para identificação.
Endereço IP	Digite o endereço IP.
Endereço MAC	Digite o endereço MAC.
ID da VLAN	Digite o VLAN ID.

2. Selecione o tipo de proteção para a entrada.

Tipo de Proteção	Selecione o tipo de proteção para a entrada. A entrada será aplicada à para o recurso específico. As seguintes opções disponíveis são: **Nenhuma:** esta entrada não será aplicada a qualquer recurso. **ARP Detection:** esta entrada será aplicada ao recurso de ARP Detection. **IP Source Guard:** esta entrada será aplicada ao recurso IPv4 Source Guard. **Ambos:** esta entrada será aplicada a ambos dos recursos.

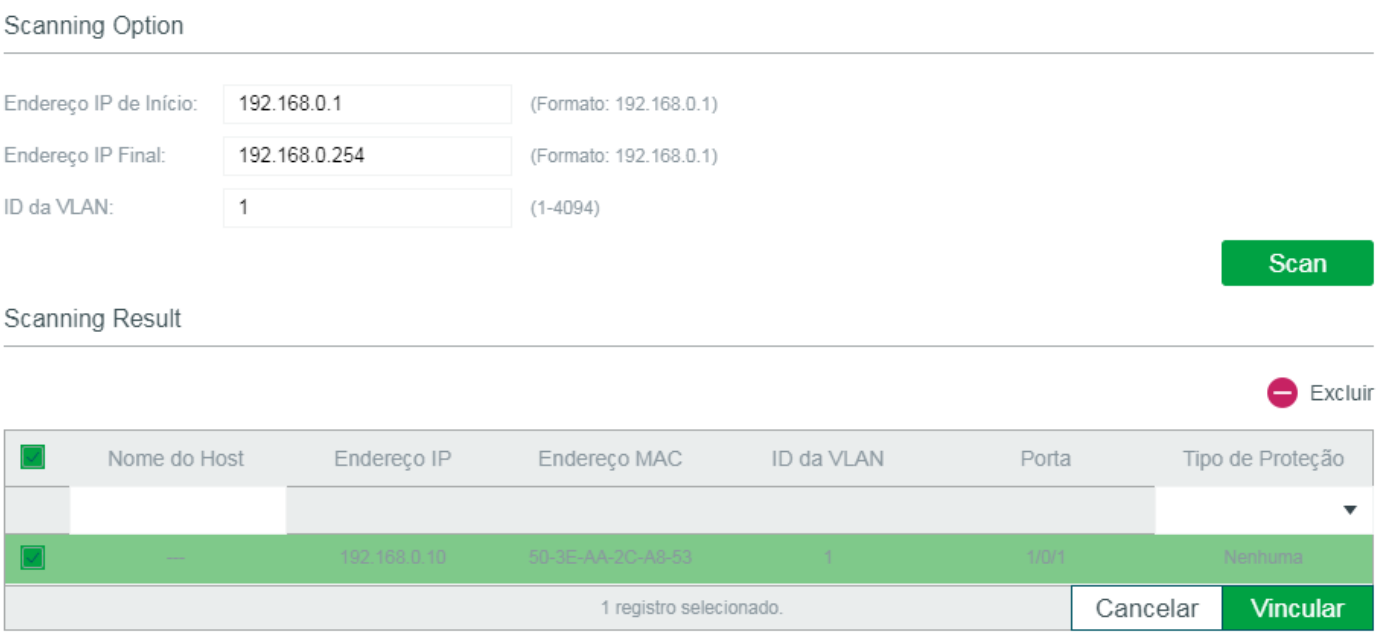
3. Selecione a porta que está ligada a este host.
4. Clique em **Aplicar**.

Entradas de Vínculo via ARP Scanning

Com o ARP Scanning, o switch envia os pacotes de solicitação ARP do campo IP especificado para os hosts. Ao receber o pacote de resposta ARP, o switch pode obter o endereço IP, endereço MAC, VLAN ID e o número da porta conectada do host. Você pode vincular essas entradas da forma que fora mais conveniente.

> Antes de usar esse recurso, certifique-se de que sua rede é segura, e que os hosts não estão sofrendo de ataques ARP no presente momento; caso contrário, você pode receber entradas de ligação IP-MAC falsas. Se a sua rede está sendo atacada, é recomendado ligar as entradas manualmente.

Selecione no menu **SEGURANÇA > IPv4 IMPB > IP-MAC Binding > ARP Scanning** para carregar a página a seguir.



Siga estes passos para configurar IP-MAC Binding via ARP scanning:

1. Na seção **Scanning Option**, especifique um intervalo de endereços IP, e um VLAN ID. Então clique em Scan para escanear as entradas no intervalo de endereços IP especificado e VLAN.

Endereço IP de início e Endereço IP de Final	Especifique uma faixa de IP, digitando um endereço IP inicial e final.
ID da VLAN	Especifique um VLAN ID.

2. Na seção **Scanning Result**, selecione uma ou mais entradas, e configure os parâmetros relevantes. Então clique em **Vincular**.

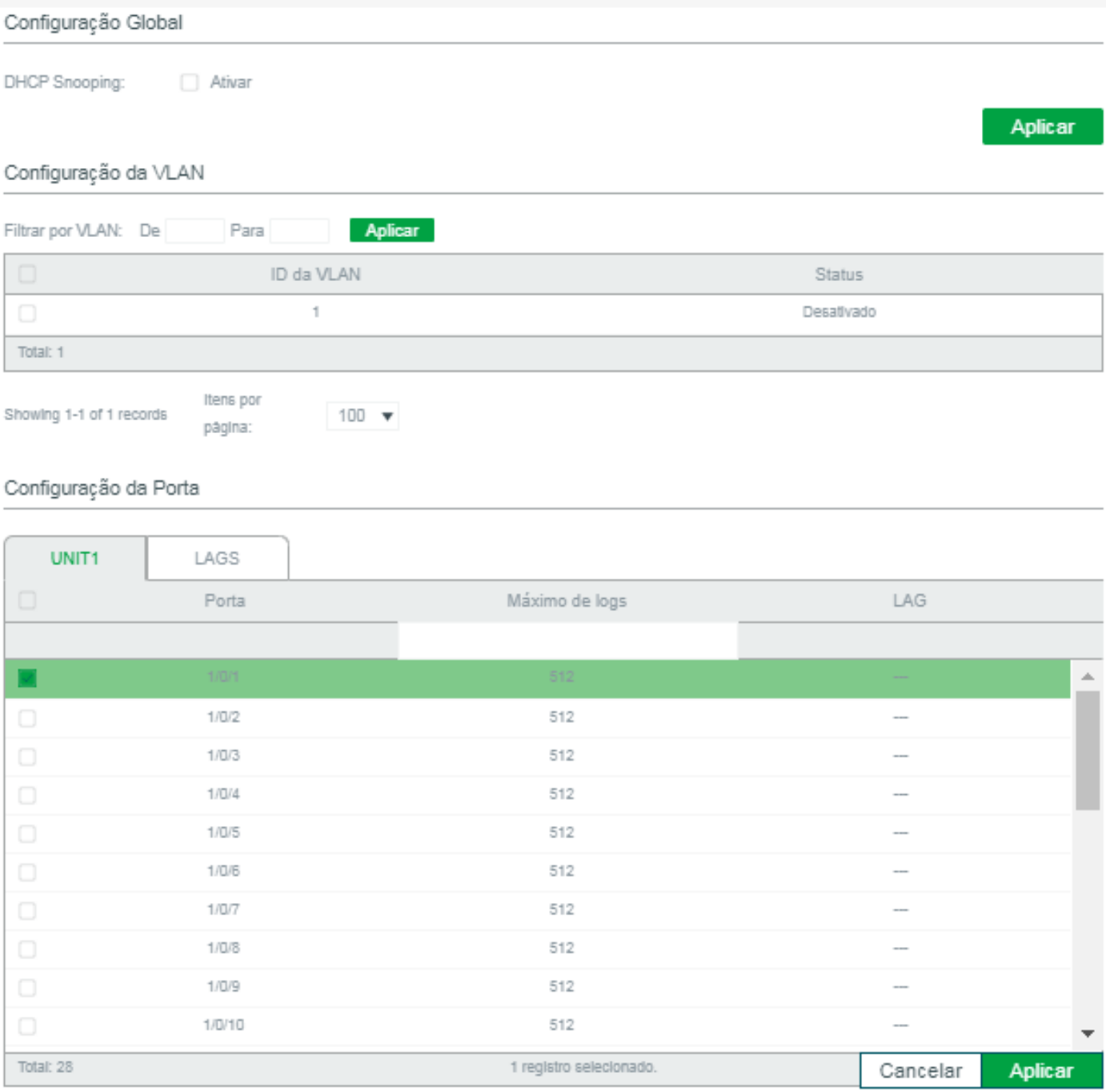
Nome do Host	Digite um nome de host para identificação.
Endereço IP	Exibe o endereço IP.

Endereço MAC	Exibe o endereço MAC.
ID da VLAN	Exibe o VLAN ID.
Porta	Mostra o número de porta.
Tipo de Proteção	Selecione o tipo de proteção para a entrada. A entrada será aplicada à para o recurso específico. As seguintes opções estão disponíveis: **Nenhuma:** esta entrada não será aplicada a nenhum recurso. **ARP Detection:** esta entrada será aplicada ao recurso de detecção de ARP. **IP Source Guard:** esta entrada será aplicada ao recurso Source Guard IP. **Ambos:** esta entrada será aplicada a ambos os recursos.

Entradas Vínculo via DHCP Snooping

Com o DHCP Snooping habilitado, o switch pode monitorar o endereço IP obtendo o processo do host obter e registrar o endereço IP, endereço MAC, VLAN ID e o número da porta conectada ao host.

Selecione no menu **SEGURANÇA > IPv4 IMPB > IP-MAC Binding > DHCP Snooping** para carregar a página a seguir.



Siga os passos para configurar o Binding IP-MAC via DHCP Snooping:

1. Na seção de Configuração global, ative o DHCP Snooping. Clique em **Aplicar**.
2. Na secção de Configuração VLAN, permita o DHCP Snooping em uma VLAN ou range de VLANs. Clique em **Aplicar**.

ID da VLAN	Exibe o ID da VLAN.
Status	Ativar ou desativar Snooping DHCP na VLAN.

3. Na seção **Configuração da Porta**, configure o número máximo de entradas binding que uma porta deve aprender via DHCP Snooping. Clique em **Aplicar**.

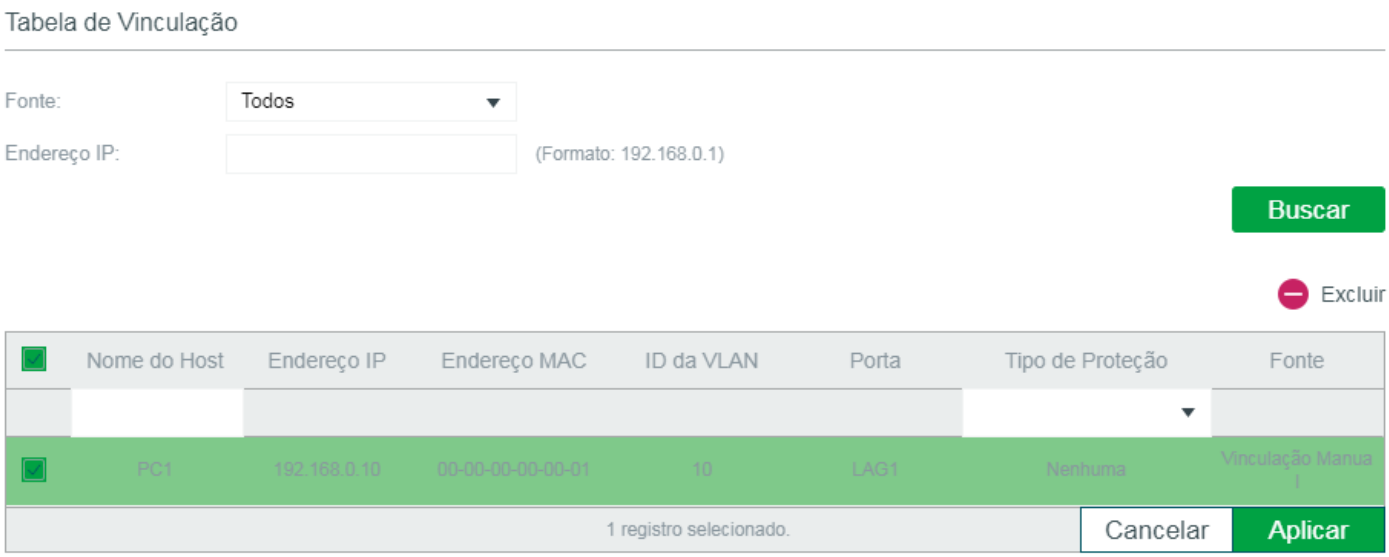
Porta	Mostra o número de porta.

Máximo de logs	Configurar o número máximo de entradas de ligação de uma porta pode aprender via DHCP Snooping.
LAG	Exibe o delay da porta.

4. As entradas aprendidas serão exibidas na tabela de ligação. Você pode ir para **SEGURANÇA > IPv4 IMPB > IP-MAC Binding > Tabela de Vinculo** para ver ou editar as entradas.

Visualizando as entradas de Vínculo

Na tabela de Binding, você pode visualizar, pesquisar e editar as entradas de Binding especificadas. Selecione no menu **SEGURANÇA > IPv4 IMPB > IP-MAC Binding > Tabela de Vinculo** para carregar a página a seguir.



Você pode especificar os critérios de pesquisa para as entradas desejadas.

Fonte	Selecione a fonte de entrada e clique em Procurar. **Todos:** exibe as entradas de todas as fontes. **Vinculação Manual:** exibe as entradas ligadas manualmente. **ARP Scanning:** exibe as entradas de ligação aprendidas com ARP Scanning. **DHCP Snooping:** exibe as entradas de ligação aprendidas com DHCP Snooping.
Endereço IP	Insira um endereço IP e clique em **Buscar** para procurar a entrada específica.

Além disso, você selecionar uma ou mais entradas para editar o nome do host e tipo de proteção e clique em **Aplicar**.

Nome do Host	Digite um nome de Host para identificação.
Endereço IP	Exibe o endereço IP.

Endereço MAC	Exibe o endereço MAC.
ID da VLAN	Exibe a VLAN ID.
Porta	Mostra o número de porta.
Tipo de Proteção	Selecione o tipo de proteção para a entrada. A entrada será aplicada para o recurso específico. As seguintes opções estão disponíveis: **Nenhuma:** esta entrada não será aplicada a qualquer recurso. **ARP Detection:** esta entrada será aplicada ao recurso de detecção de ARP. **IP Source Guard:** esta entrada será aplicada ao recurso IP Source Guard.
Fonte	Apresenta a fonte da entrada.

Configuração do ARP Detection

Para configuração completa do ARP Detection, siga os passos abaixo:

1. Adicionar as entradas de Vínculo IP-MAC.
2. Ativar o ARP Detection.
3. Configurar o ARP Detection nas portas.
4. Verifique as estatísticas ARP.

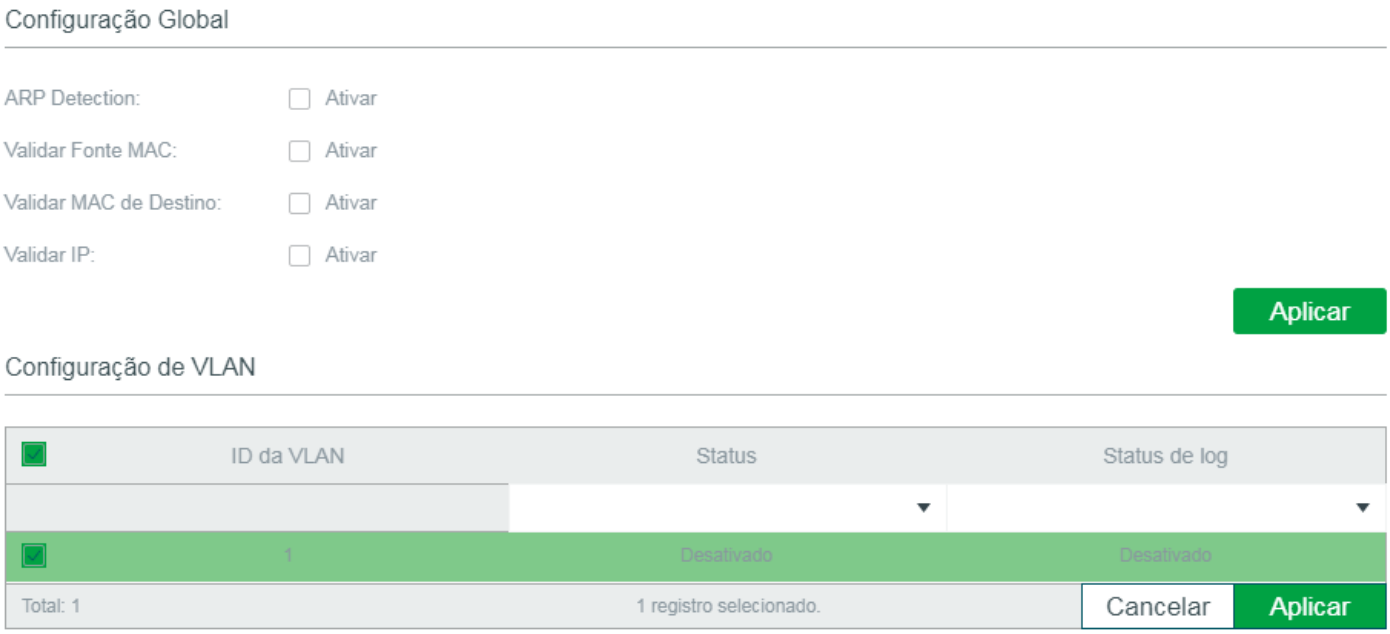
Adicionando entradas Vínculo IP-MAC

No ARP Detection, o switch detecta os pacotes ARP com base nas entradas Binding na tabela de ligação de IP-MAC.

Então, antes de configurar o ARP Detection, você precisa completar a configuração de ligação. Para mais detalhes, consulte Configuração de Vínculo IP-MAC.

Habilitando o ARP Detection

Selecione no menu **SEGURANÇA > IPv4 IMPB > ARP Detection > Configuração Global** para carregar a página a seguir:



Siga estes passos para ativar o ARP Detection:

1. Na seção de **Configuração global**, ative o ARP Detection e configure os parâmetros. Clique em **Aplicar**.

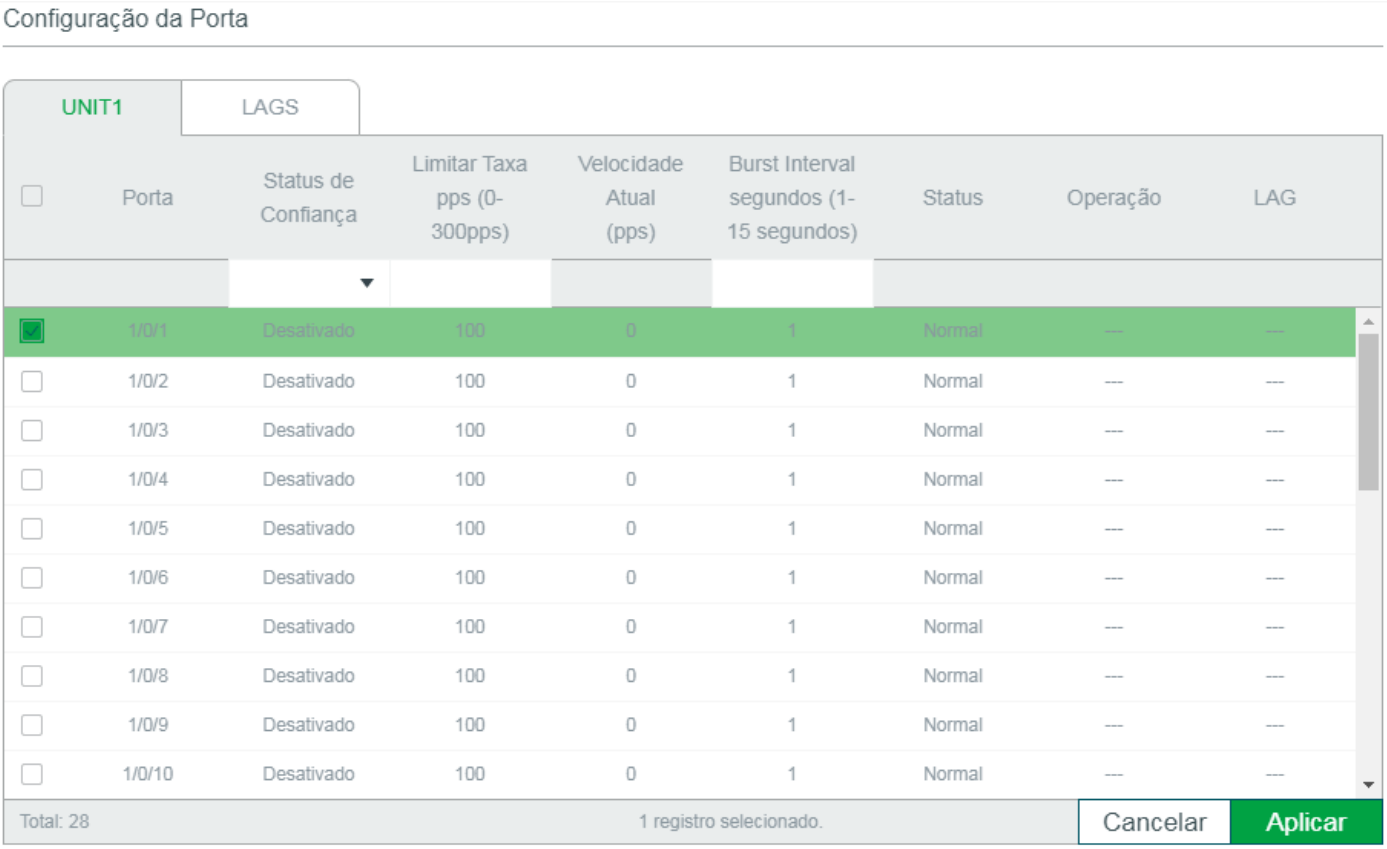
ARP Detection	Ativar ou desativar o ARP Detection globalmente.
Validar fonte MAC	Ativar ou desativar o switch para verificar se o endereço MAC de origem e o endereço MAC do remetente são os mesmos quando receber um pacote ARP. Se não, o pacote ARP serão descartadas.
Validar MAC de Destino	Ativar ou desativar o switch para verificar se o endereço MAC de destino e o endereço MAC de destino são os mesmos quando receber um pacote de resposta ARP. Se não, o pacote ARP serão descartadas.
Validar IP	Ativar ou desativar o switch para verificar se o endereço IP do remetente de todos os pacotes ARP e o endereço IP de destino dos pacotes de resposta ARP são legais. Os pacotes ARP ilegais serão devolvidos, incluindo endereços de broadcast, multicast endereços, endereços de Classe E, endereços de auto retorno (127.0.0.0/8) e o seguinte endereço: 0.0.0.0.

2. Na seção **Configuração VLAN**, permitir a detecção do ARP nas VLANs selecionadas. Clique em **Aplicar**.

ID da VLAN	Exibe o ID da VLAN.
Status	Ativar ou desativar a detecção de ARP na VLAN.
Status de log	Ativar ou recurso Log disable na VLAN. Com esse recurso ativado, o switch gera um log quando um pacote ARP ilegal é descartado.

Configurando o ARP Detection nas portas

Selecione no menu **SEGURANÇA > IPv4 IMPB > ARP Detection > Configuração da Porta** para carregar a página a seguir.



Siga estes passos para configurar o ARP Detection nas portas:

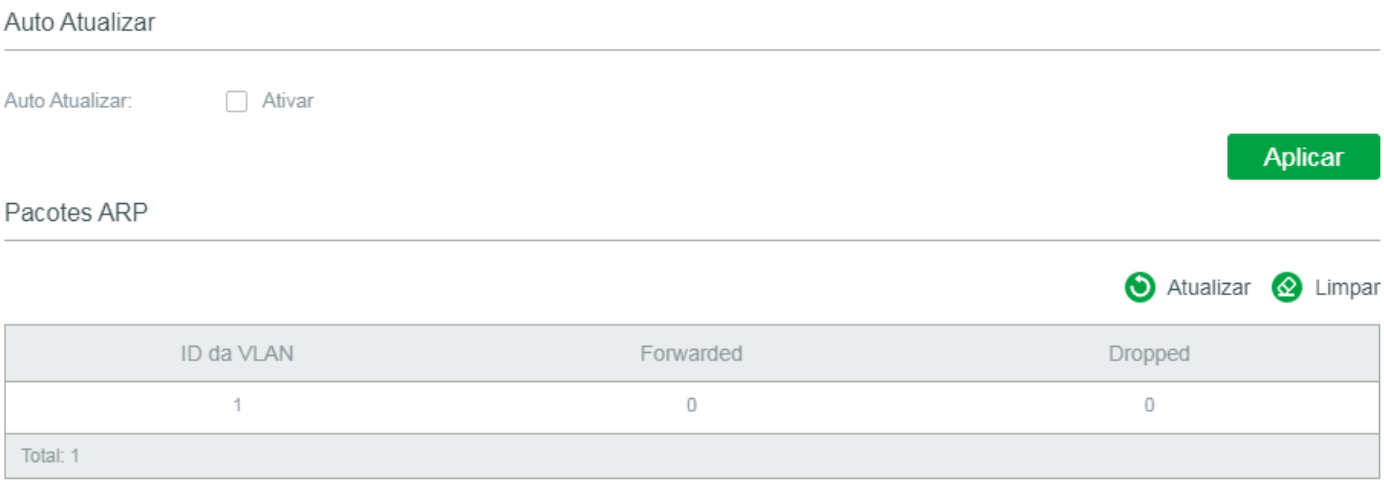
1. Selecione uma ou mais portas e configure os parâmetros.

Status de Confiança	Ativar ou desativar essa porta para ser uma porta de confiança. Em uma porta de confiança, os pacotes ARP são encaminhadas diretamente sem marcação. As portas específicas, como portas uplinks e portas de roteamento são sugeridas para serem definidas como portas confiáveis.
Limitar Taxa pps	Especificar o número máximo dos pacotes ARP que podem ser recebidos na porta por segundo.
Velocidade Atual	Mostra a velocidade atual de recebimento dos pacotes ARP na porta.
Burst Interval segundos	Especifique um intervalo de tempo. Se a velocidade de pacotes ARP recebido atinge o limite para este intervalo de tempo, a porta vai ser desligada.

Status	Exibe o status do ARP attack: **Normal:** o encaminhamento de pacotes ARP na porta é normal. **Baixa:** a velocidade de transmissão do pacote legais de ARP excede o valor definido. A porta será desligada durante 300 segundos. Você também pode clicar no botão Recover para recuperar.
Operação	Se o Status é alterado para Desativado, haverá um botão Recuperar. Você pode clicar no botão para restaurar a porta para o estado normal.
LAG	Exibe o atraso da porta.

Visualizando as estatísticas ARP

Você pode ver o número de pacotes ARP ilegais recebidos em cada porta, o que facilita para localizar um mau funcionamento na rede, e tomar as medidas de proteção apropriadas. Selecione no menu **SEGURANÇA > IPv4 IMPB > ARP Detection > Estatísticas ARP** para carregar a página a seguir.



Na seção **Auto Atualizar**, você pode habilitar o recurso de atualização automática, e especificar o intervalo de atualização, assim a página web será automaticamente atualizada. Na seção Pacotes ARP, você pode ver o número de pacotes ARP ilegais em cada VLAN.

ID da VLAN	Exibe a VLAN ID.
Forwarded	Exibe o número de pacotes ARP encaminhados nesta VLAN.
Dropped	Exibe o número de pacotes ARP descartados nesta VLAN.

Configuração do Source Guard IPv4

Para completar a configuração Source Guard IPv4, siga estes passos:

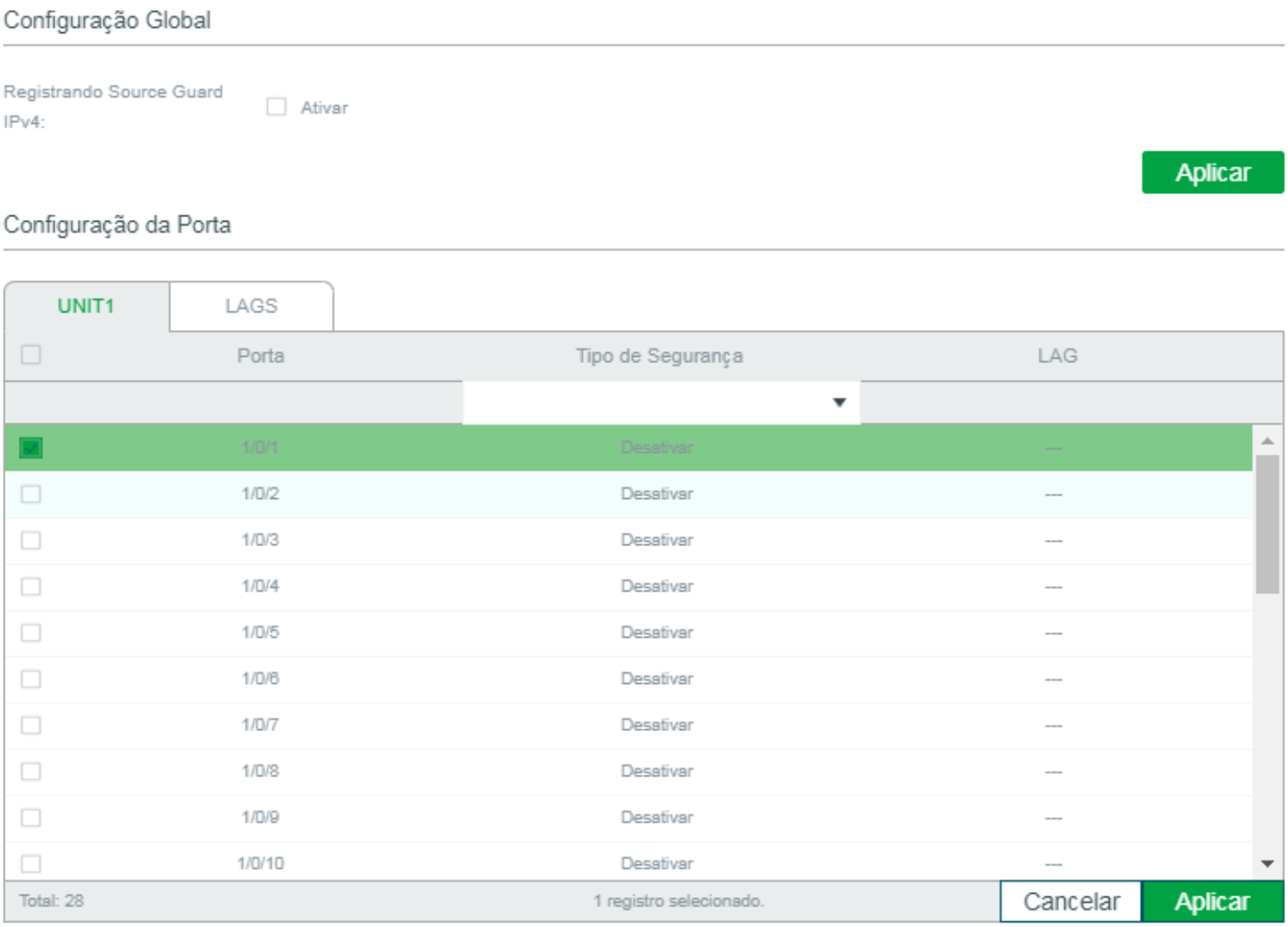
1. Adicionar as entradas IP-MAC Binding.
2. Configurar o IPv4 Source Guard.

Adicionando entradas IP-MAC Binding

No Source Guard IPv4, o switch filtra os pacotes que não correspondem às regras da tabela Binding IPv4 MAC. Então, antes de configurar o ARP Detection, você precisa configurar o IP-MAC Binding. Para mais detalhes, consulte a Configuração IP-MAC Binding.

Configurando o IPv4 Source Guard

Selecione no menu **SEGURANÇA > IPv4 IMPB > Protetor da Fonte IPv4** para carregar a página a seguir.



Siga os passos abaixo para configurar o IPv4 Source Guard:

1. Na seção de **Configuração Global**, escolha se deseja ativar o recurso Registrando Source Guard IPv4. Clique em **Aplicar**.

Registrando Source Guard IPv4	Exibe a VLAN ID.Ativar ou desativar o recurso log IPv4 Fonte Guarda. Com esse recurso ativado, o botão gera um log quando os pacotes ilegais são recebidos.

2. Na seção Configuração da Porta, configure o tipo de proteção da porta e clique em **Aplicar**.

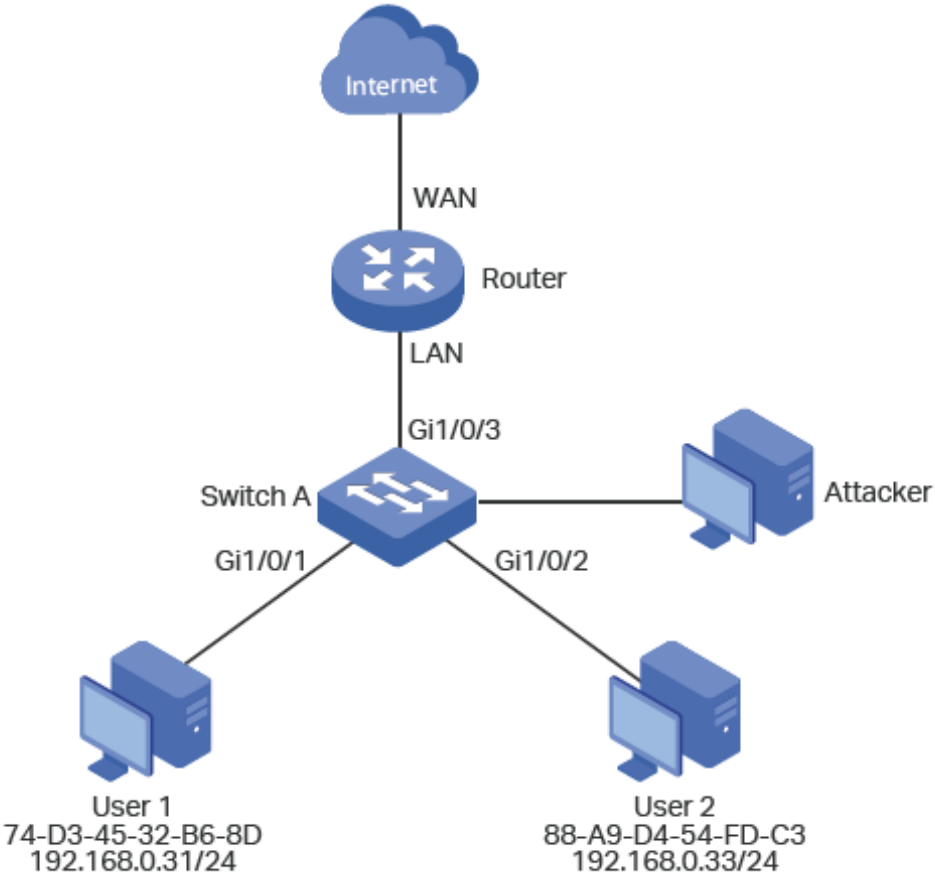
Porta	Mostra o número de porta.
Tipo de segurança	Selecione Tipo de segurança na porta para pacotes IPv4. As seguintes opções estão disponíveis: **Disable:** o recurso IP Source Guard é desativado na porta. **SIP + MAC:** apenas o pacote com seu endereço IP de origem, endereço MAC de origem e o número da porta combinando as regras IPv4-MAC binding pode ser processado, caso contrário, o pacote será descartado. **SIP:** apenas o pacote com seu endereço IP de origem e o número da porta combinando as regras IPv4-MAC binding podem ser processados, caso contrário, o pacote será descartado.
LAG	Exibe o atraso que a porta está em.

Exemplo de ARP Detection

Requisitos de rede

Como mostrado no exemplo abaixo, o usuário 1 e o usuário 2 são clientes legais na rede local, e estão conectados às portas 1/0/1 e 1/0/2. Ambos estão na VLAN 1 padrão.

O roteador foi configurado com recurso de segurança para evitar ataques na WAN. Agora, o administrador de rede quer configurar o switch A para evitar ataques ARP da LAN.



Configurando o Cenário

Para atender essa exigência, você pode configurar o ARP Detection para evitar que a rede sofra ataques ARP na LAN.

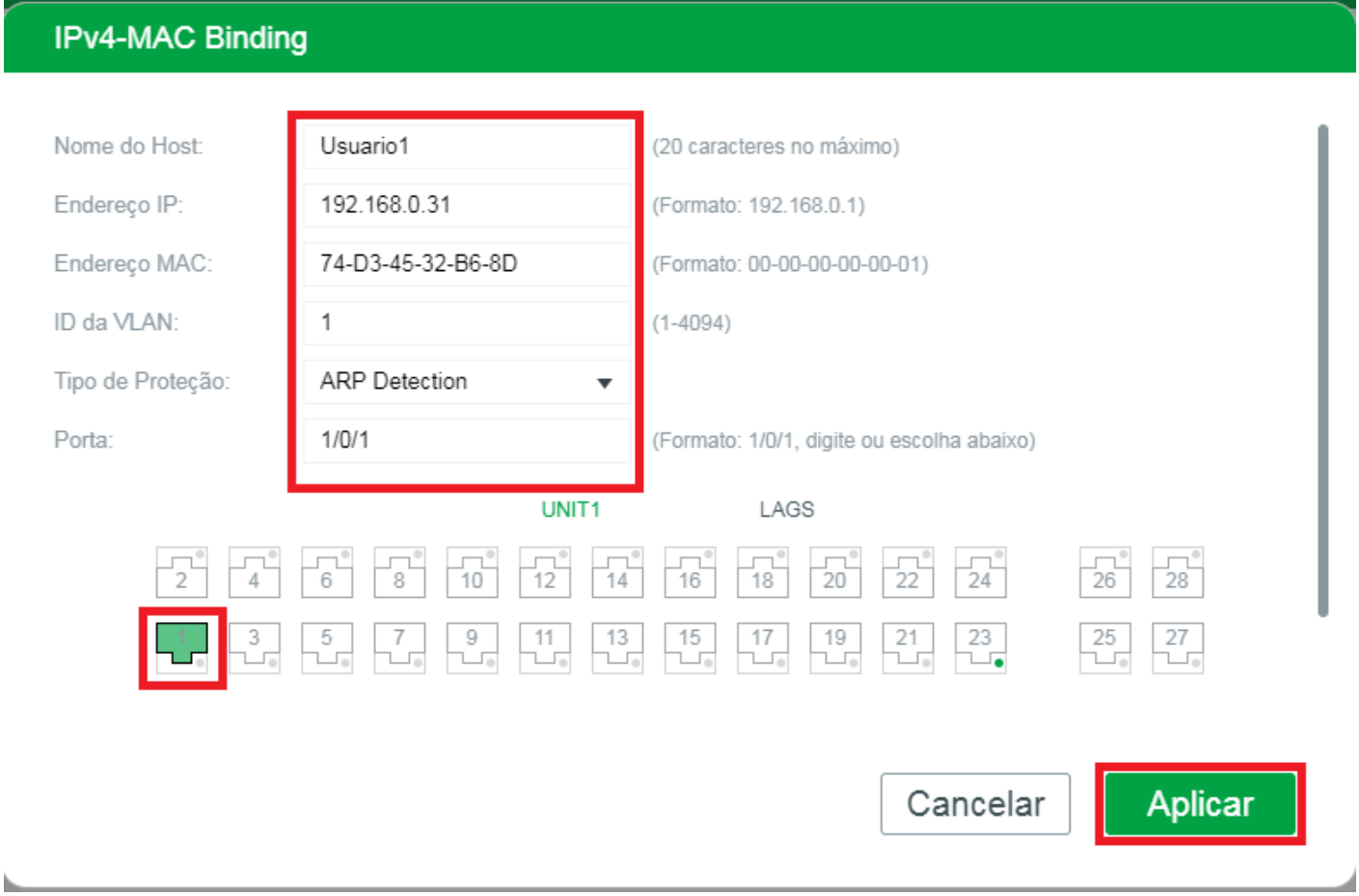
A visão geral de configurações no switch é a seguinte:

1. Configurar o IP-MAC Binding. As entradas de ligação para o usuário 1 e 2 devem ser ligadas manualmente.
2. Configurar o ARP Detection globalmente.
3. Configurar o ARP Detection nas portas. Uma vez que a porta 1/0/3 está conectada ao gateway (router), definido na porta 1/0/3 como porta de confiança. Para evitar ataques de ARP Flooding, limitar a velocidade de recebimento dos pacotes ARP legais em todas as portas.

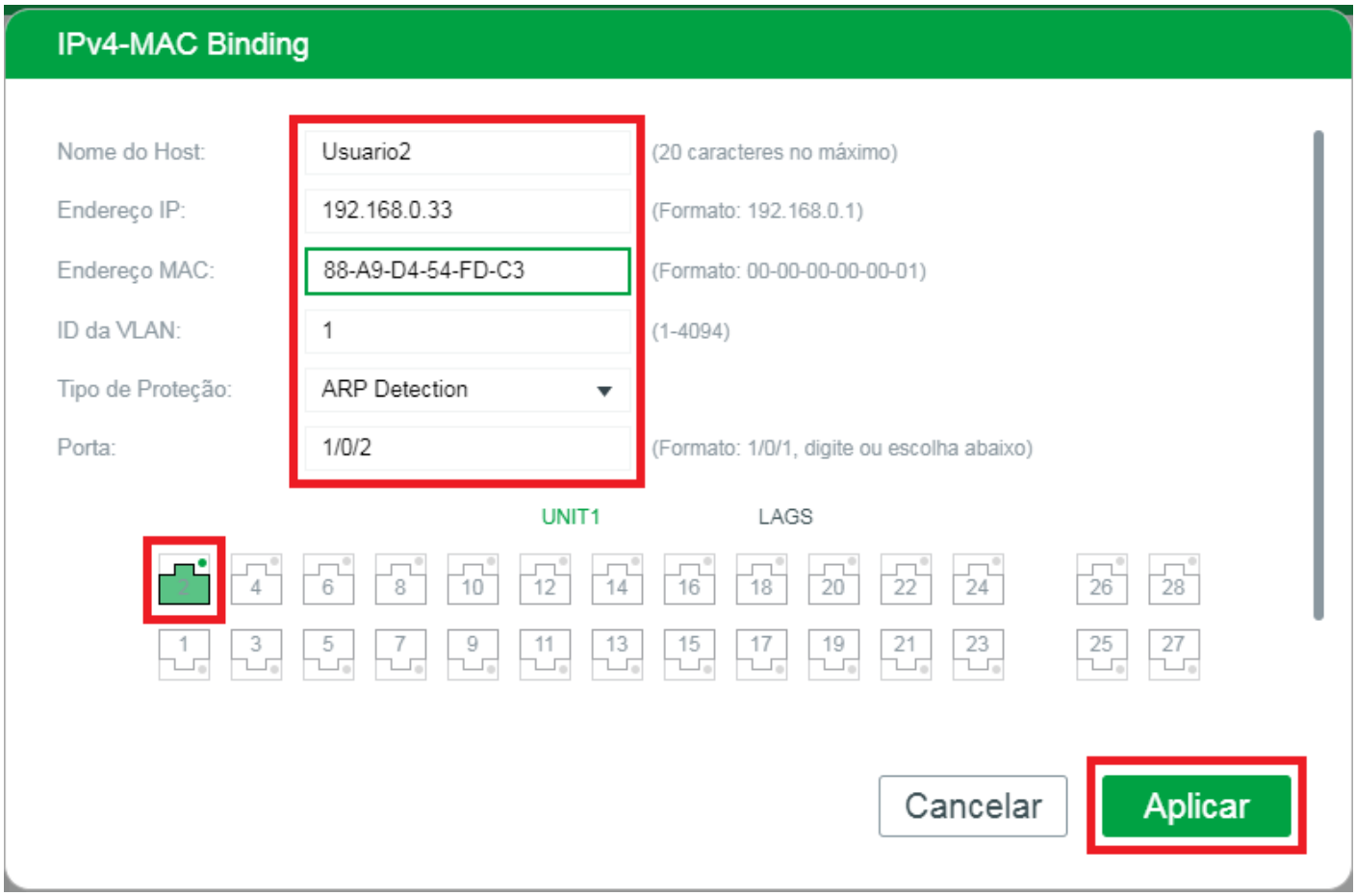
Demonstrado com SG 2404 PoE L2+, a seguir mostra o procedimento de configuração usando a Interface web:

1. Selecione no menu **SEGURANÇA > IPv4 IMBP > IP-MAC Binding > Vínculo Manual** e clique em Adicionar para carregar a página a seguir.

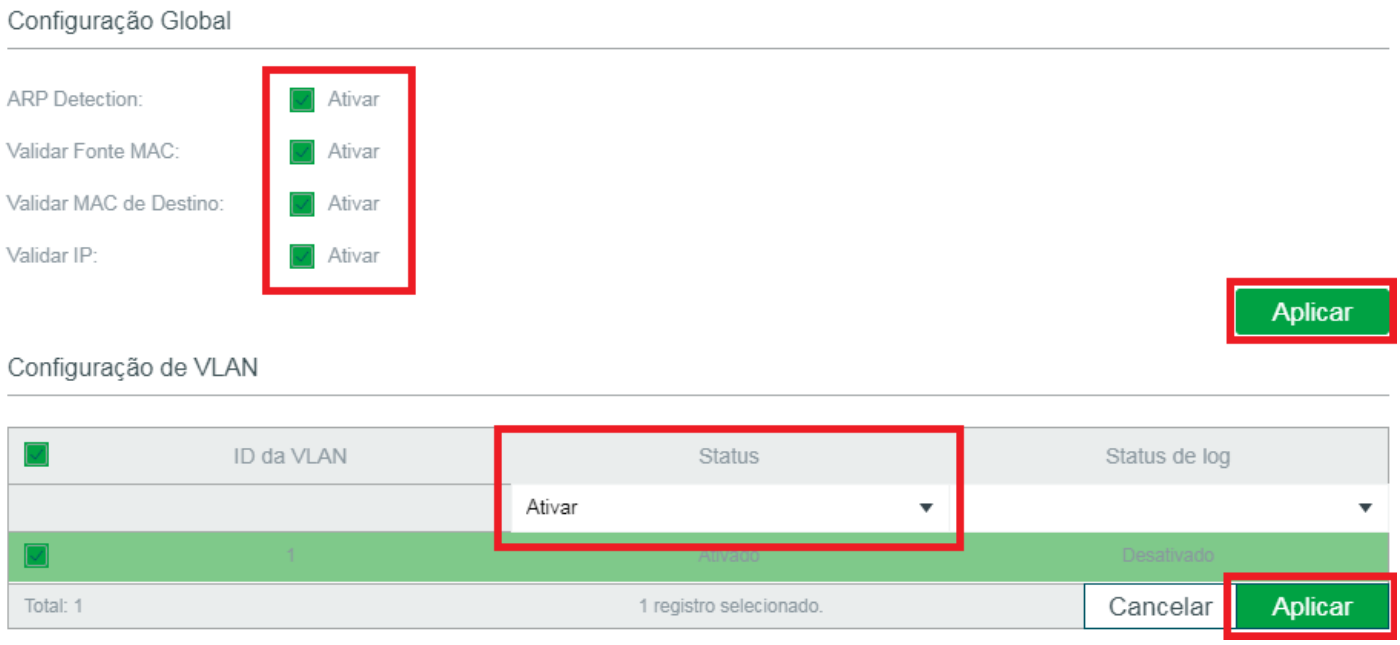
   Selecione no menu SEGURANÇA> IPv4 IMBP> IP-MAC Binding> Vínculo Manual e clique em para carregar a página a seguir. Digite o nome do host, endereço IP, endereço MAC e VLAN ID do usuário 1, selecione o tipo de proteção como ARP Detection, e selecione a porta 1/0/1 na tela. Clique em **Aplicar**.



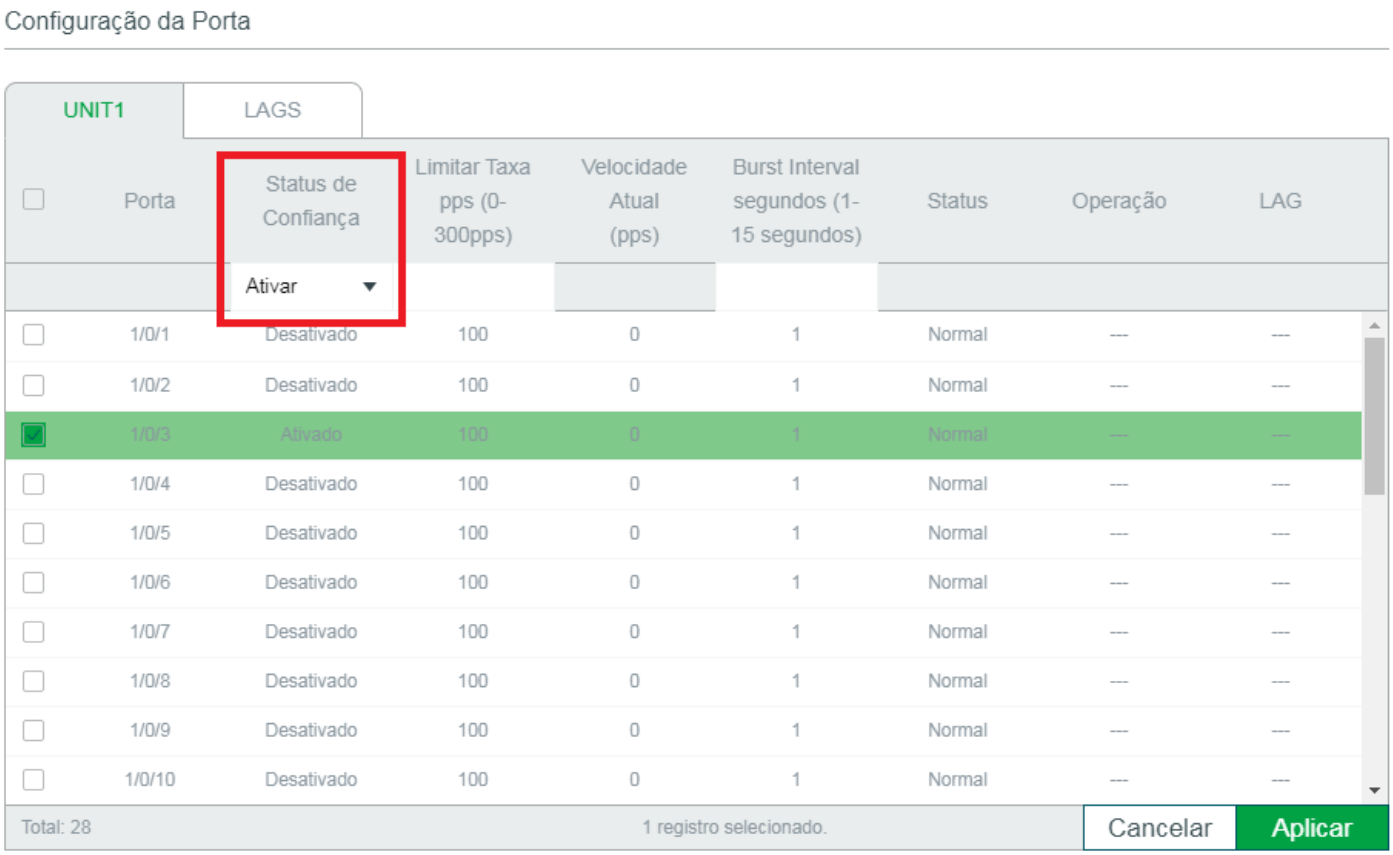
2. Na mesma página, adicione uma entrada de ligação para o usuário 2. Digite o nome do host, endereço IP, endereço MAC e VLAN ID de usuário 2, selecione o tipo de proteção como Detecção de ARP, e selecione a porta 1/0/2 no painel. Clique em **Aplicar**.



3. Selecione no menu **SEGURANÇA > IPv4 IMPB > ARP Detection > Configuração Global** para carregar a página seguinte. Ativar o ARP Detection, Validar Fonte MAC, Validar MAC de Destino e Validar IP, e clique em **Aplicar**. Selecione VLAN 1, mude o status para Ativar e clique em **Aplicar**.



4. Selecione no menu **SEGURANÇA > IPV4 IMPB > ARP Detection > Configuração de Porta** para carregar a página seguinte. Por padrão, todas as portas estão com o ARP Detection e ARP Flooding Defend ativos. Configurar a porta 1/0/3 como porta de confiança, e manter as outras no parâmetro padrão. Clique em **Aplicar**.

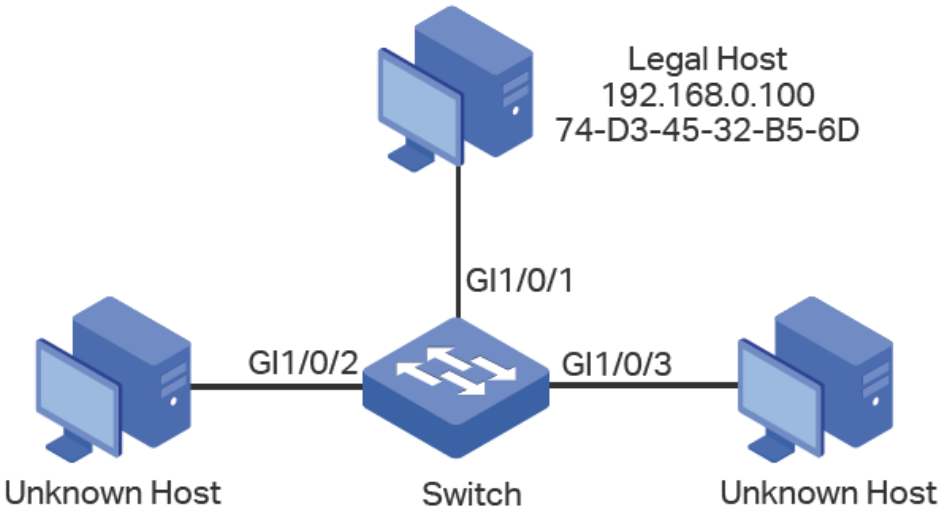


5. Clique em Salvar para salvar as configurações.

Exemplo do Source Guard IP

Requisitos de rede

Como mostrado abaixo, as ligações de hosts legais para o switch via porta 1/0/1 pertence à VLAN 1 (padrão). É necessário que apenas o host legal pode acessar a rede através da porta 1/0/1, e outros hosts desconhecidos serão bloqueados ao tentar acessar a rede através das portas 1/0/1-3.

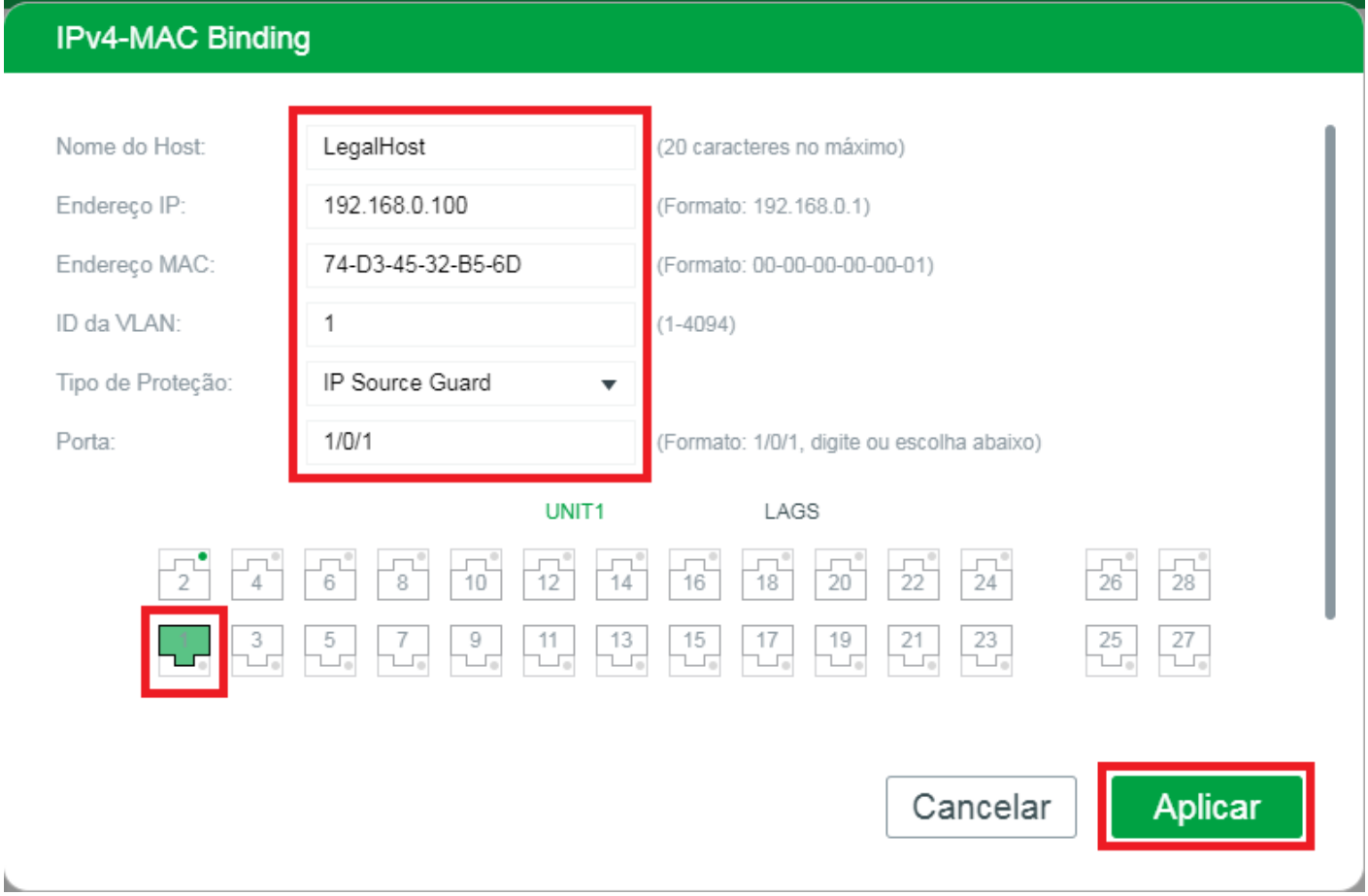


Configurando o Cenário

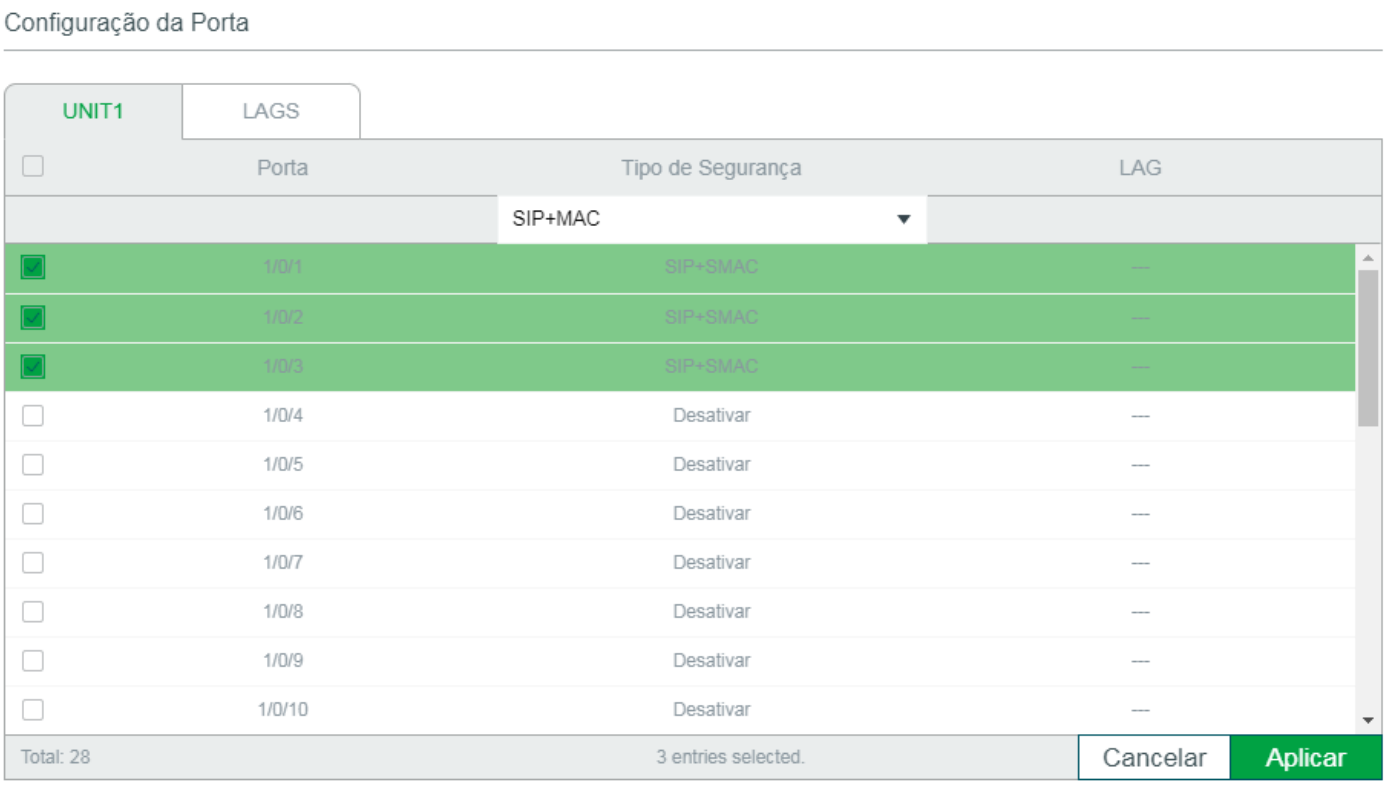
Para implementar este requisito, você pode usar o IP-MAC Binding e o IP Source Guard para filtrar os pacotes recebidos dos hosts desconhecidos. A visão geral de configuração no switch é a seguinte:

1. Ligar o endereço MAC, endereços IP, número da porta e da VLAN ID do host legal com o IP-MAC Binding.
2. Ativar o IP Source Guard nas portas 1/0/1, 1/0/2 e 1/0/3.

1. Selecione no menu **SEGURANÇA > IPv4 IMPB > IP-MAC Binding > Vinculo Manual** e Clique em Adicionar para carregar a página a seguir. Digite o nome do host, endereço IP, endereço MAC e VLAN ID do host legal, selecione o tipo de proteção como, e selecione porta 1/0/1 no painel. Clique em **Aplicar**.



2. Selecione no menu **SEGURANÇA > IPv4 IMPB > Protetor da Fonte IPv4** para carregar a seguinte página. Habilite o Registrando Source Guard IPv4 para fazer a troca e gerar logs quando receber pacotes ilegais e clique em Aplicar. Selecione as portas 1/0/1, 1/0/2 e 1/0/3, e configure o tipo de segurança como SIP + MAC, e clique em **Aplicar**.



3. Clique em Salvar para salvar as configurações.

Apêndice: Configuração Padrão

As configurações padrão de DHCP Snooping estão listadas na tabela a seguir:

Configurações DHCP Snooping

Parâmetros	Configurações Padrão
Configuração Global	
DHCP Snooping	Desativar
Configuração da VLAN	
Status	Desativar
Configuração da Porta	
Máximo de logs	512

As configurações padrão de Detecção ARP estão listadas na tabela a seguir:

Configurações Detecção ARP

Parâmetros	Configurações Padrão
Configuração Global	
ARP Detection	Desativar
Validar Fonte MAC	Desativar
Validar MAC de Destino	Desativar
Validar IP	Desativar
Configuração da VLAN	
Status	Desativar
Status de Log	Desativar
Configuração da Porta	
Status de Confiança	Desativar
Limitar Taxa pps	100 pps
BURST	1 segundo
ARP Estatísticas	

Desativar	Desativar
Intervalo de atualização	5 segundos

As configurações padrão de Protetor da Fonte IPv4 estão listados na tabela a seguir:

Configurações Protetor da Fonte IPv4

Parâmetros	**Configurações Padrão**
Configuração de Porta	
Registrando Source Guard IPv4:	Desativar
Tipo de Segurança	Desativar

IPv6 IMPB

IPv6 IMPB

Visão Geral

IPv6 IMPB (IP-MAC-Port Binding) é utilizado para vincular um endereço IPv6, endereço MAC, ID de VLAN, e um número de porta conectada à um host específico. Baseado na tabela de vinculo o switch pode prevenir ataques ND com a função de ND Detection e filtrar pacotes que não correspondem com as entradas de vínculo com a IPv6 Source Guard.

Funções Suportadas

Vínculo IPv6-MAC

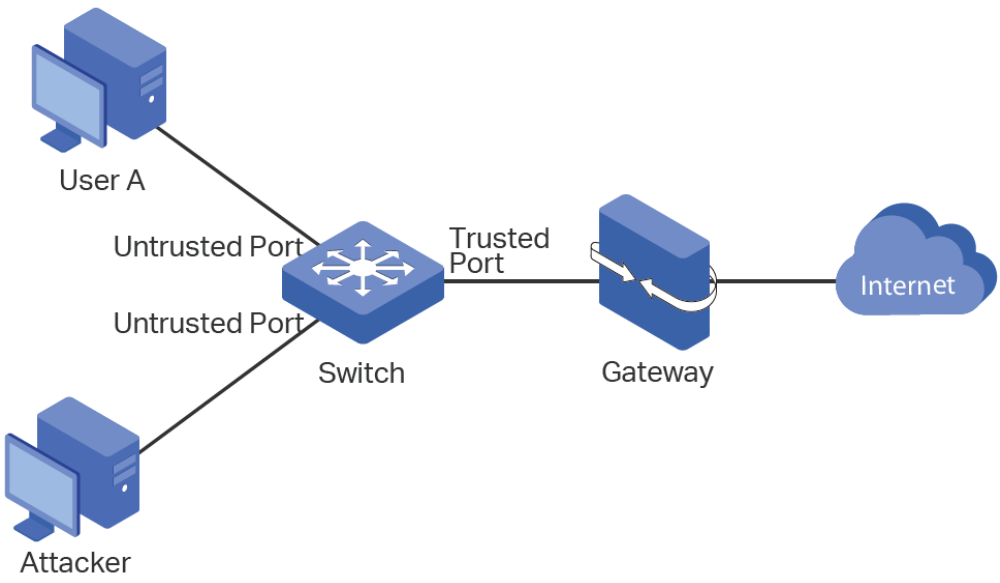
Essa função é utilizada para vincular entradas. As entradas de vínculo podem ser configuradas manualmente ou aprendidas através do ND Snooping ou DHCPv6 Snooping. As funções ND Detection e Protetor da Fonte IPv6 são baseadas nas entradas de vínculo IPv6-MAC.

ND Detection

Devido à falta de um mecanismo de segurança, o protocolo IPv6 ND (Neighbor Discovery) é facilmente explorado por hackers. A função ND Detection utiliza as entradas na tabela de vínculo IPv6-MAC para filtrar pacotes ND forjados e prevenir ataques ND.

A topologia de aplicação do ND Detection é mostrada na figura a baixo. A porta que está conectada ao gateway deve ser configurada como porta confiável e as outras portas devem ser configuradas como portas não confiáveis. Os princípios do encaminhamento de pacotes ND são os seguintes:

- Todos os pacotes ND recebidos em uma porta confiável serão encaminhados sem verificação.
- Pacotes RS (Router Solicitation) e NS (Neighbor Solicition) sem especificação de origem de endereço IPv6, tais como pacotes RS para requisição de endereços IPv6 e pacotes NS para detecção de endereços duplicados, não serão checados em ambos os tipos de porta.
- Pacotes RA (Router Adversiment) e RR (Router Redirect) recebidos em portas não confiáveis serão descartados diretamente, e outros pacotes ND serão verificados: O switch irá usar a tabela de vínculo IPv6-MAC para comparar endereços IPv6, endereços MAC, ID da VLAN e a porta receptora entre a entrada de vínculo e o pacote ND. Se uma correspondência for encontrada o pacote ND é considerado legal e será encaminhado. Caso nenhuma correspondência for encontrada o pacote ND será considerado ilegal e será descartado.



Guardião de Origem IPv6

O Guardião de Origem IPv6 é utilizado para filtrar pacotes IPv6 baseando-se na tabela de vínculo IPv6-MAC. Somente pacotes com correspondência nas regras de vínculo serão encaminhados.

Configurando Vínculo IPv6-MAC

Você pode adicionar entradas de vínculo IPv6-MAC de três formas;

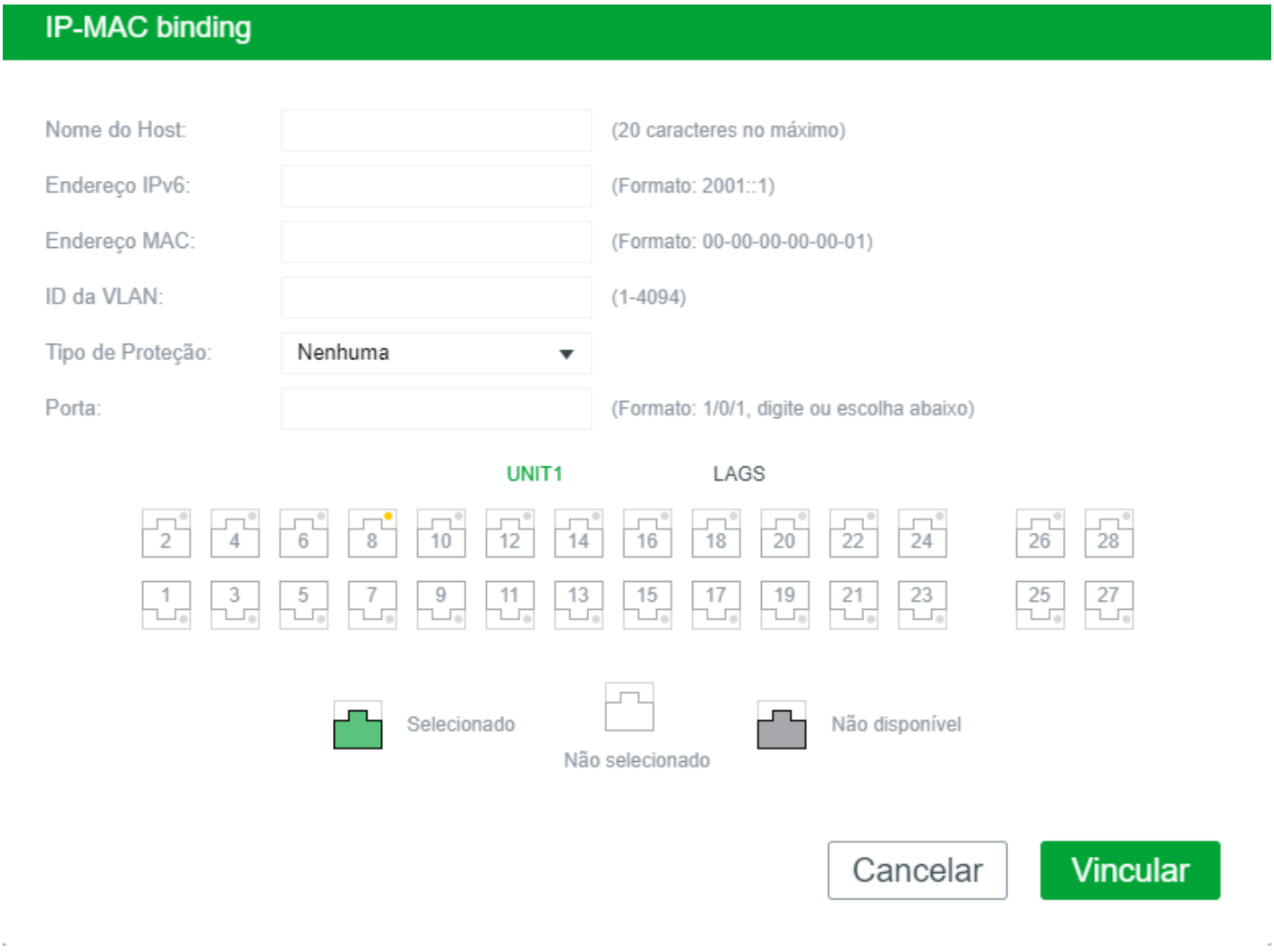
- Vínculo Manual.
- Através do ND Snooping.
- Através do DHCPv6 Snooping

Você também pode visualizar, pesquisar e editar entradas na tabela de Vínculo.

Vinculando entradas manualmente

Você pode vincular endereços IPv6, endereços MAC, ID de VLAN e número de portas manualmente na condição que você detenha as informações detalhadas dos hosts.

Vá até o menu **SEGURANÇA > IPv6 IMPB > Vínculo IPv6-MAC > Vínculo Manual** clique em Adicionar para carregar a página a seguir.



Siga os seguintes passos para criar uma entrada de vínculo IPv6-MAC manualmente:

1. Preencha as seguintes informações para especificar um host.

Nome do Host	Digite o nome do host para identificação.
Endereço IPv6	Digite o endereço IPv6.
Endereço MAC	Digite o endereço MAC.
ID da VLAN	Digite o VLAN ID.

2. Selecione o tipo de proteção para a entrada.

Tipo de Proteção	Selecione o tipo de proteção para a entrada. A entrada será aplicada à para o recurso específico. As seguintes opções disponíveis são: **Nenhuma:** esta entrada não será aplicada a qualquer recurso. **ND Detection:** esta entrada irá aplicar a função de ND Detection. **IPv6 Source Guard:** esta entrada será aplicada ao recurso IPv6 Source Guard. **Ambos:** esta entrada será aplicada a ambos dos recursos.

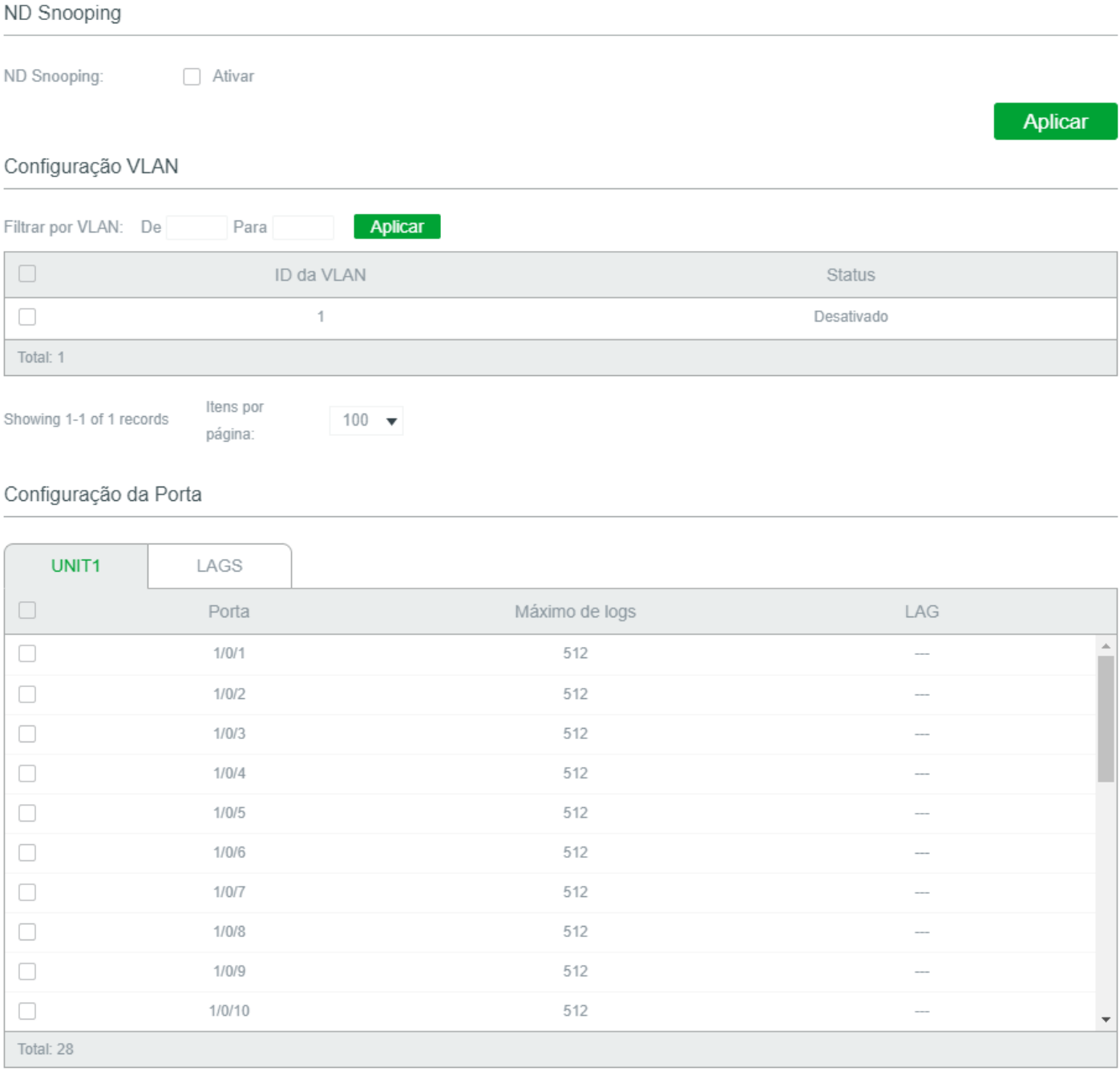
3. Entre ou selecione as portas que estarão conectadas a este host.
4. Clique em **Aplicar**.

Vinculando Entradas via ND Snooping

Com o ND Snooping o switch monitora os pacotes ND e grava os endereços IPv6, MAC, a ID da VLAN e o número da porta a qual o host IPv6 está conectado. Você pode vincular essas entradas de forma conveniente.

> Antes de utilizar esta função, garanta que sua rede está segura e que os hosts não estão sofrendo ataques ND; caso contrário você pode obter entradas de vínculo IPv6-MAC incorretas. Se sua rede estiver sobre ataque é recomendado vincular as entradas manualmente.

Vá até o menu **SEGURANÇA > IPv6 IMPB > Vínculo IPv6-MAC > ND Snooping** para carregar a página a seguir.



Siga os seguintes passos para configurar o vínculo IPv6-MAC através do ND Snooping:

1. Na seção **ND Snooping** habilite o ND Snooping e clique em **Aplicar**.
2. Na seção **Configuração de VLAN** selecione uma ou mais VLANs e habilite o ND Snooping para elas. Clique em **Aplicar**.

ID da VLAN	Mostra a ID da VLAN.
Status	Habilita ou desabilita o ND Snooping para a VLAN.

3. Na seção **Configuração de Porta** configure o número máximo de entradas que uma porta pode aprender através do ND Snooping. Clique em **Aplicar**.

Porta	Mostra o número da porta.

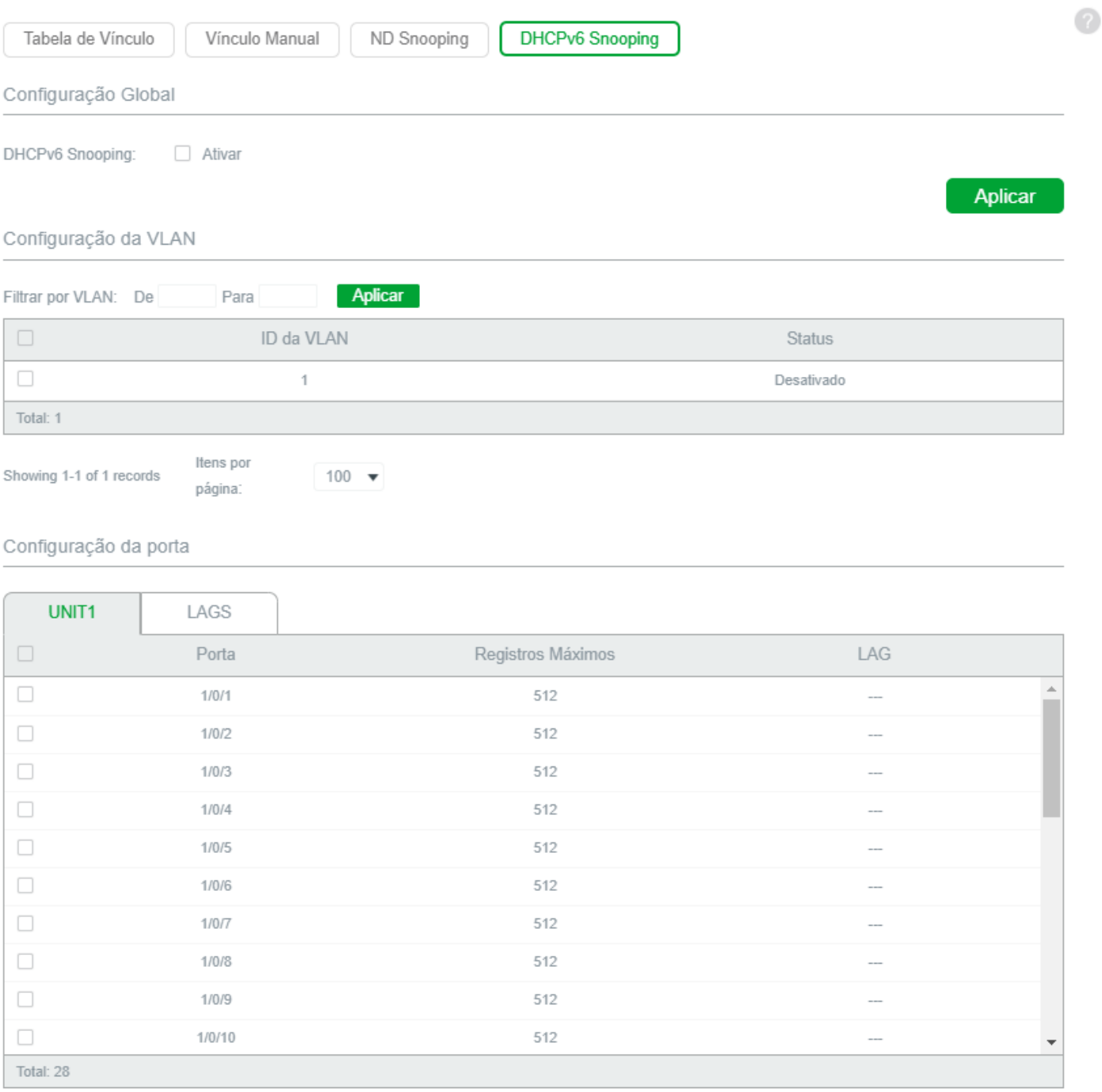
Máximo de Logs	Configure o número máximo de entradas de vínculo que a porta pode aprender através do ND Snooping.
LAG	Mostra a LAG a qual a porta pertence.

4. As entradas aprendidas serão mostradas na tabela de vínculo. Você pode ir até o menu **SEGURANÇA > IPv6 IMPB > Vínculo IPv6-MAC > Tabela de Vínculo** para visualizar e editar as entradas.

Vinculando Entradas via DHCPv6 Snooping

Com o DHCPv6 Snooping habilitado o switch pode monitorar o processo de obtenção de endereço IP do host e gravar o endereço IPv6, endereço MAC, ID da VLAN e o número da porta que o host está conectado.

Vá até o menu **SEGURANÇA > IPv6 IMPB > Vínculo IPv6-MAC > DHCPv6 Snooping** para carregar a página a seguir.



Siga os seguintes passos para configurar o vínculo IPv6-MAC utilizando o DHCPv6 Snooping:

1. Na seção **Configuração Global** habilite o DHCPv6 globalmente. Clique em **Aplicar**.
2. Na seção **Configuração VLAN** habilite o DHCPv6 para uma VLAN ou conjunto de VLANs. Clique em **Aplicar**.

ID da VLAN	Mostra a ID da VLAN.
Status	Habilita ou desabilita o ND Snooping para a VLAN.

3. Na seção **Configuração de Porta** configure o número máximo de entradas de vínculo que uma porta pode aprender através do DHCPv6 Snooping. Clique em **Aplicar**.

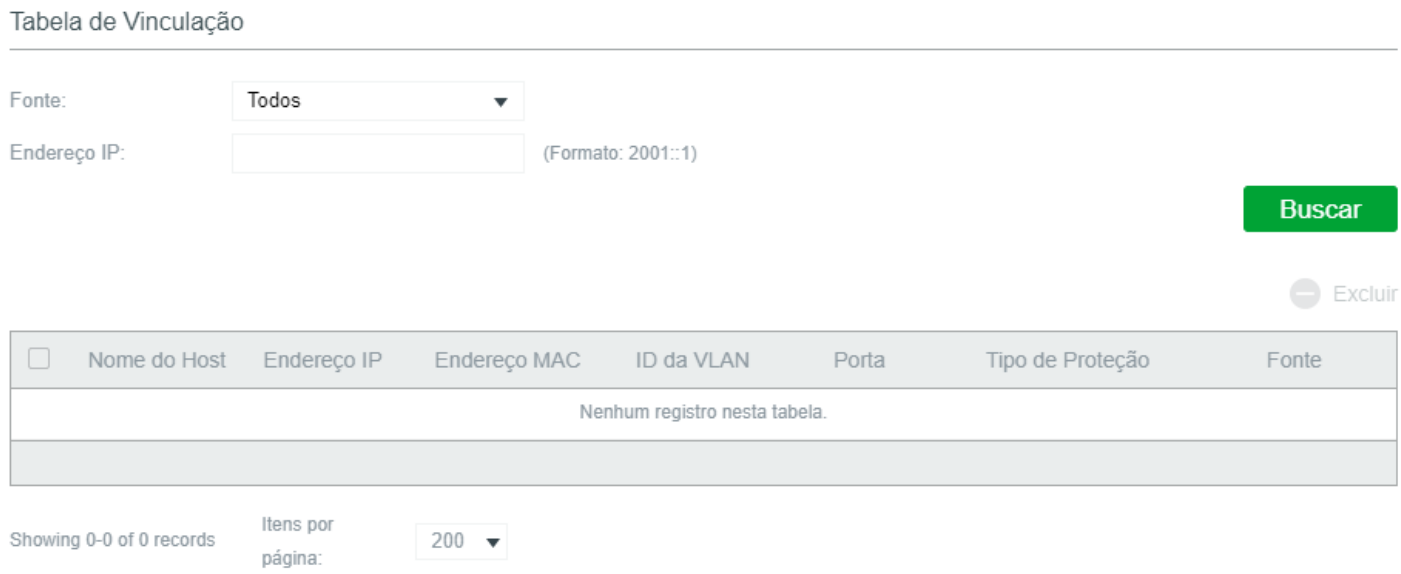
Porta	Mostra o número da porta.

Máximo de Logs	Configure o número máximo de entradas de vínculo que a porta pode aprender através do ND Snooping.
LAG	Mostra a LAG a qual a porta pertence.

4. As entradas aprendidas serão mostradas na tabela de vínculo. Você pode ir até o menu **SEGURANÇA > IPv6 IMPB > Vínculo IPv6-MAC > Tabela de Vínculo** para visualizar e editar as entradas.

Visualizando as entradas de Vínculo

Na tabela de Binding, você pode visualizar, pesquisar e editar as entradas de Binding especificadas. Selecione no menu **SEGURANÇA > IPv6 IMPB > Vínculo IPv6-MAC > Tabela de Vinculo** para carregar a página a seguir.



Você pode especificar os critérios de pesquisa para as entradas desejadas.

Fonte	Selecione a fonte de entrada e clique em **Buscar**. **Todos:** exibe as entradas de todas as fontes. **Vinculação Manual:** exibe as entradas ligadas manualmente. **ND Snooping:** exibe as entradas de vínculo aprendidas através do ND Snooping **DHCPv6 Snooping:** exibe as entradas de vínculo aprendidas através do DHCPv6 Snooping
Endereço IP	Insira um endereço IP e clique em **Buscar** para procurar a entrada específica.

Além disso, você selecionar uma ou mais entradas para editar o nome do host e tipo de proteção e clique em **Aplicar**.

Nome do Host	Digite um nome de Host para identificação.

Endereço IP	Exibe o endereço IPv6.
Endereço MAC	Exibe o endereço MAC.
ID da VLAN	Exibe a VLAN ID.
Porta	Mostra o número de porta.
Tipo de Proteção	Selecione o tipo de proteção para a entrada. A entrada será aplicada para o recurso específico. As seguintes opções estão disponíveis: **Nenhuma:** esta entrada não será aplicada a qualquer recurso. **ND Detection:** esta entrada irá aplicar a função de ND Detection. **IPv6 Source Guard:** esta entrada será aplicada ao recurso IPv6 Source Guard.
Fonte	Apresenta a fonte da entrada.

Configuração ND Detection

Para completar a configuração do ND Detection siga os seguintes passos:

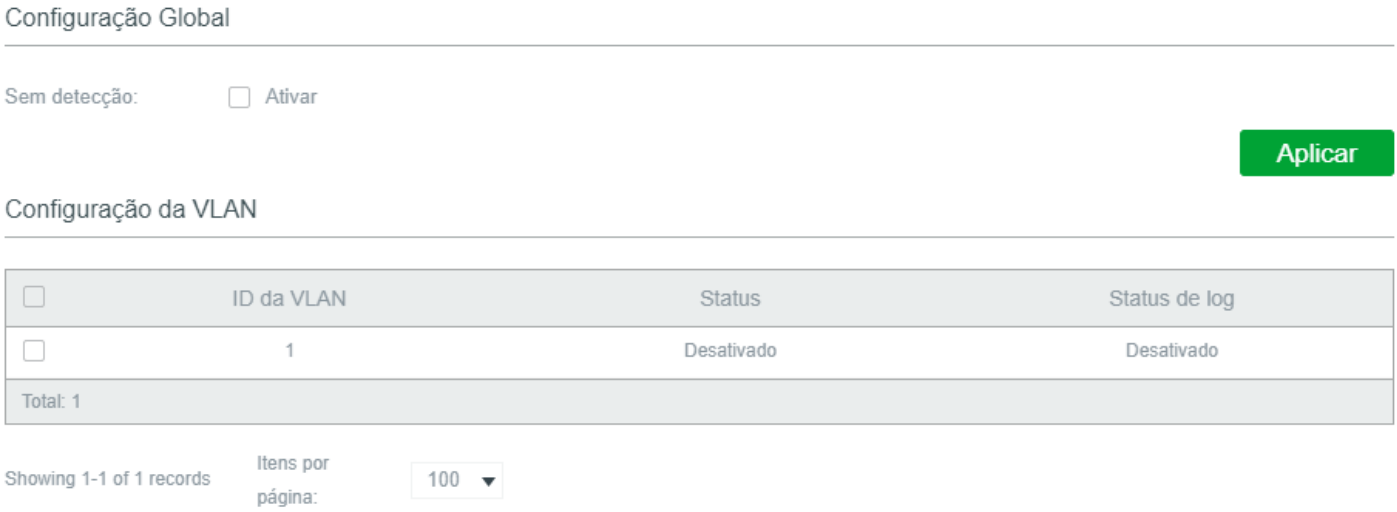
1. Adicione entradas de vínculo IPv6-MAC.
2. Habilite o ND Detection.
3. Configure o ND Detection nas portas.
4. Visualize as estatísticas ND.

Adicionando Entradas de Vínculo IPv6-MAC

A função de ND Detection permite que o switch detecte os pacotes ND baseado nas entradas de vínculo na tabela de vínculo IPv6-MAC e filtre os pacotes ND ilegais. Antes de configurar o ND Detection termine a configuração de vínculo IPv6-MAC. Para mais detalhes vá até Configuração de Vínculo IPv6-MAC.

Habilitando o ND Detection

Vá até o menu **SEGURANÇA > IPv6 IMPB > ND Detection > Configuração Global** para carregar a página a seguir.



Siga os seguintes passos para habilitar o ND Detection:

1. Na seção **Configuração Global** habilite o ND Detection e configure os parâmetros relacionados. Clique em **Aplicar**.

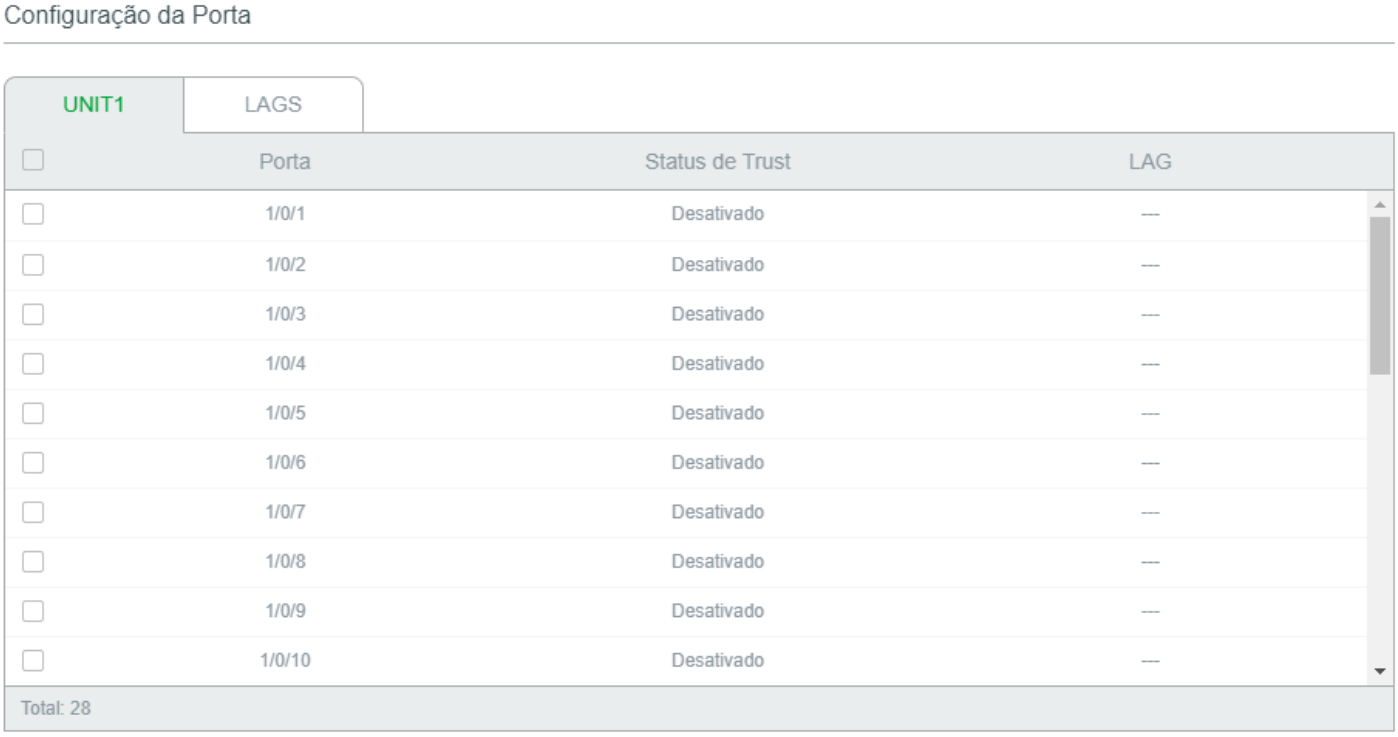
ND Detection	Habilita ou desabilita o ND Detection globalmente.

2. Na seção **Configuração de VLAN** habilite o ND Detection para as VLANs selecionadas. Clique em **Aplicar**.

ID da VLAN	Mostra o ID da VLAN.
Status	Habilita ou desabilita ND Detection para a VLAN.
Status de log	Habilita ou desabilita a função de Log na VLAN. Com essa função habilitada o switch gera log quando um pacote ND ilegal é descartado.

Configurando ND Detection nas Portas

Vá até o menu **SEGURANÇA > IPv6 IMPB > ND Detection > Configuração de Porta** para carregar a página a seguir.



Siga os seguintes passos para configurar o ND Detection nas portas:

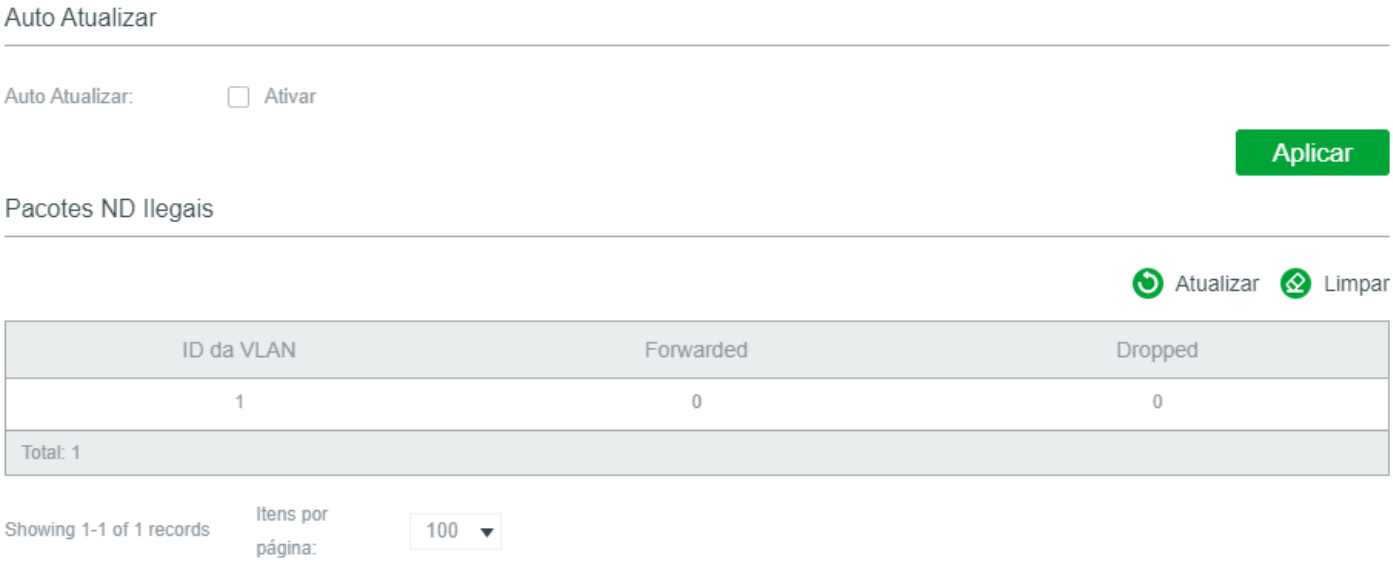
1. Selecione uma ou mais portas e configure os parâmetros.

Porta	Mostra o número da porta.
Status de Trust	Habilita ou desabilita a porta como porta confiável. Em uma porta confiável os pacotes ND são encaminhados sem verificação. Portas específicas, como portas de uplink e portas roteadoras, é sugerido que você as configure como portas confiáveis.
LAG	Mostra a LAG a qual a porta pertence.

2. Clique em **Aplicar**.

Visualizando as Estatísticas ND

Vá até o menu **SEGURANÇA > IPv6 IMPB > ND Detection > Estatísticas ND** para carregar a página a seguir.



Na seção **Auto Atualizar** você pode habilitar a função de atualização automática e especificar o intervalo de atualização, então a página web será atualizada automaticamente.

Na seção **Pacotes ND Ilegais** você pode visualizar o número de pacotes ND ilegais em cada VLAN.

ID da VLAN	Mostra o ID da VLAN.
Forwarded	Mostra o número de pacotes ND que foram encaminhados para essa VLAN.
Dropped	Mostra o número de pacotes ND que foram descartados para essa VLAN.

Configuração do IPv6 Source Guard

Para completar a configuração do Protetor da Fonte IPv6 siga os seguintes passos:

1. Adicione entradas de vínculo IP-MAC.
2. Configure o Protetor de Fonte IPv6.

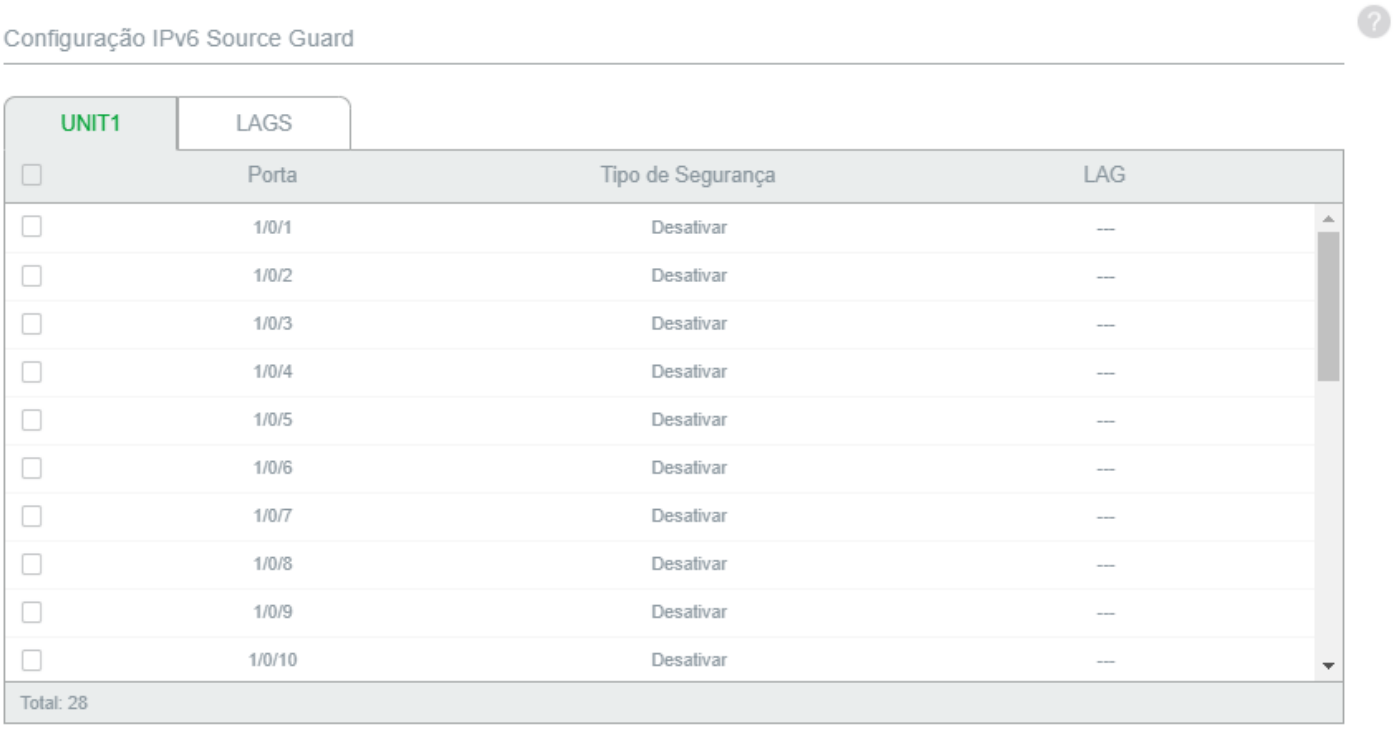
Adicionando Entradas de Vínculo IPv6-MAC

A função de IPv6 Source Guard permite que o switch detecte trafego ilegal baseado nas entradas de vínculo na tabela de vínculo IPv6-MAC e o bloqueie quando for originado de um endereço que não está configurado na tabela de vínculo IPv6-MAC. Antes de configurar o IPv6 Source Guard termine a configuração de vínculo IPv6-MAC. Para mais detalhes vá até Configuração de Vínculo IPv6-MAC.

Configurando o Protetor de Fonte IPv6

Antes de configurar o protetor de fonte IPv6, você precisa configurar o Modelo SDM como EnterpriseV6.

Vá até o menu **SEGURANÇA > IPv6 IMPB > IPv6 Source Guard** para carregar a página a seguir.



Siga os seguintes passos para configurar o Protetor de Fonte IPv6:

1. Selecione uma ou mais portas e configure o tipo de proteção para as portas.

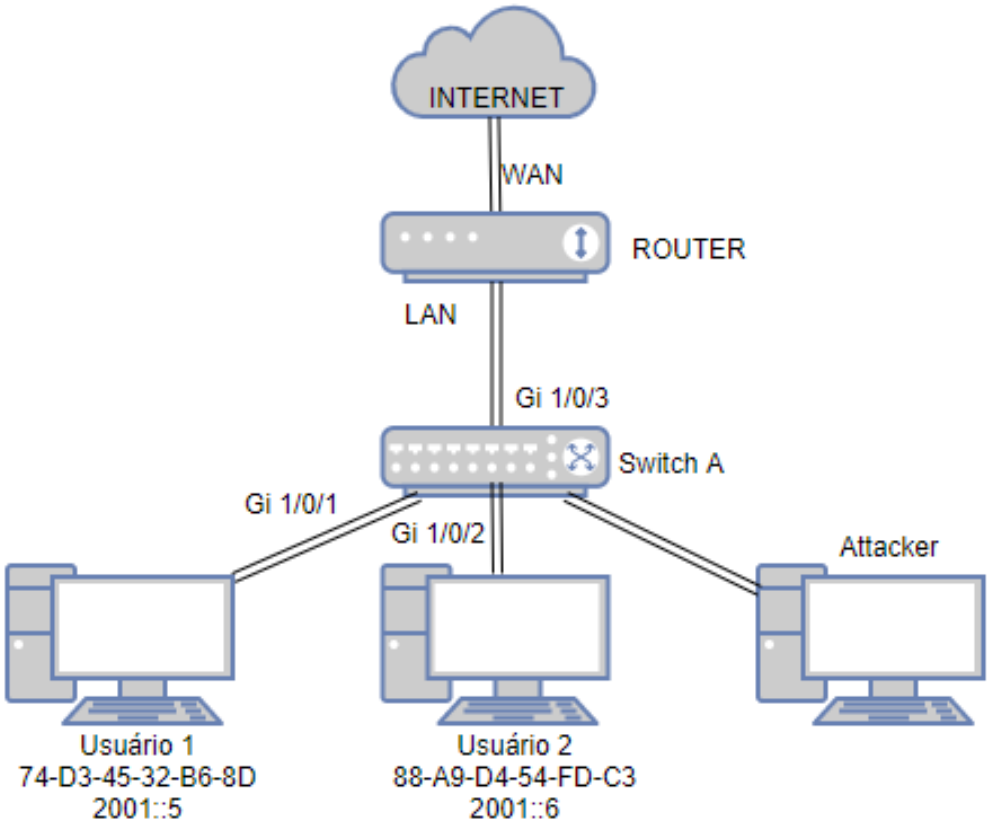
Porta	Mostra o número da Porta.
Tipo de Segurança	Selecione o tipo de segurança para os pacotes IPv6. As seguintes opções são suportadas: **Desabilitado:** a função de IPv6 Source Guard estará desabilitado para a porta. **SIP+MAC:** somente pacotes com seu endereço IPv6, endereço MAC e número de porta com correspondência nas regras de vínculo IPv6-MAC podem ser processados, caso contrário os pacotes serão descartados. **SIP:** somente pacotes com endereço IPv6 e número de porta com correspondência nas regras de vínculo IPv6-MAC podem ser processados, caso contrário os pacotes serão descartados.
LAG	Mostra a LAG a qual a porta pertence.

2. Clique em **Aplicar**.

Exemplo para ND Detection

Requisitos de Rede

Como mostrado a baixo, o Usuário 1 e Usuário 2 são usuários IPv6 legais na rede local conectados respectivamente às portas 1/0/1 e 1/0/2. Ambos estão na VLAN 1 padrão. O roteador está configurado com função de segurança para prevenir ataques a partir da WAN. Agora o administrador quer configurar o Switch A para prevenir ataques ND originados na LAN.



Configurando o Cenário

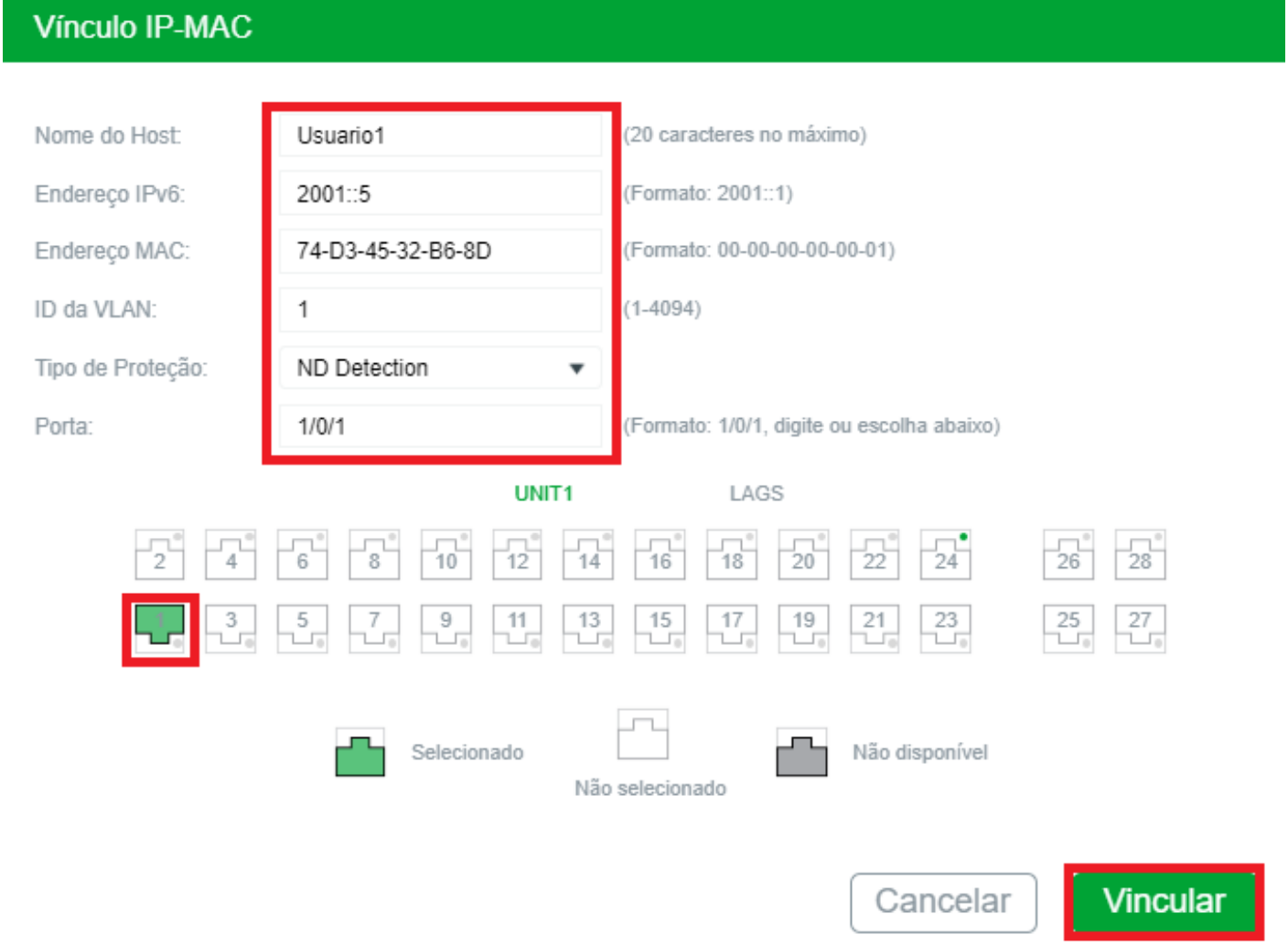
Para atender aos requisitos você pode configurar o ND Detection para impedir que a rede sofra ataques originados na LAN.

A visão geral da configuração do switch é mostrada a baixo:

1. Configure vínculo IPv6-MAC. As entradas de vínculo do Usuário 1 e Usuário 2 devem ser adicionadas manualmente.
2. Configure o ND Detection globalmente.
3. Configure o ND Detection nas portas. Uma vez que a porta 1/0/3 está conectada ao roteador de gateway é necessário configurar a porta 1/0/3 como porta confiável.

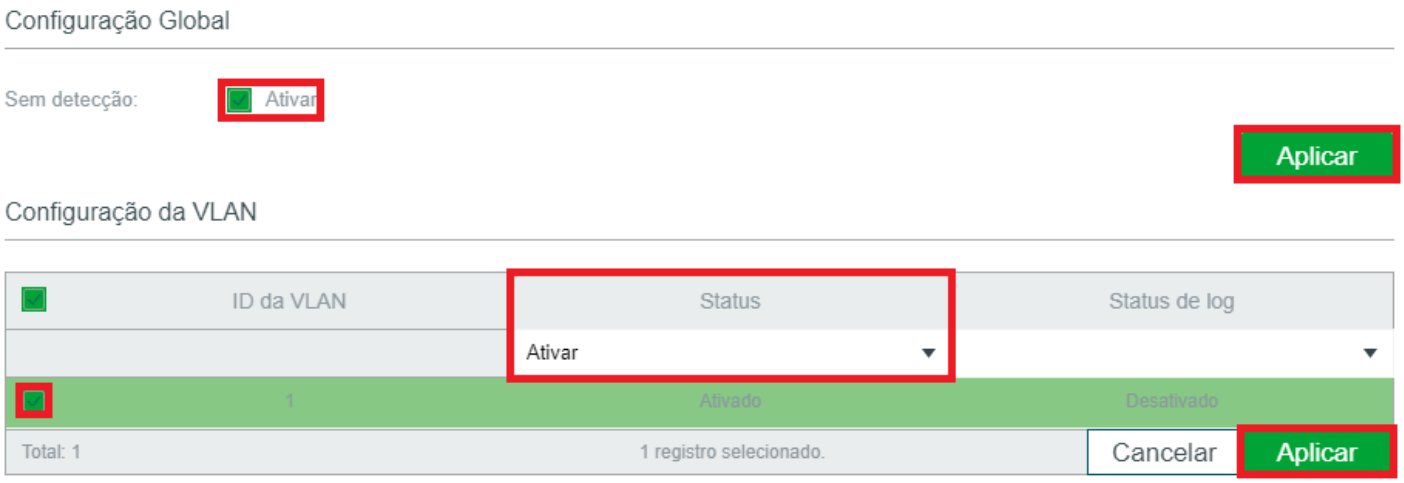
Para atender as configurações você deve seguir os seguintes passos:

1. Vá até o menu **SEGURANÇA > IPv6 IMPB > Vínculo IPv6-MAC > Vínculo Manual** clique em Adicionar para carregar a página a seguir. Entre com o nome do host, endereço IPv6, endereço MAC e ID da VLAN para o Usuário 1, selecione o tipo de proteção como ND Detection, e selecione a porta 1/0/1 no painel. Clique em **Aplicar**.

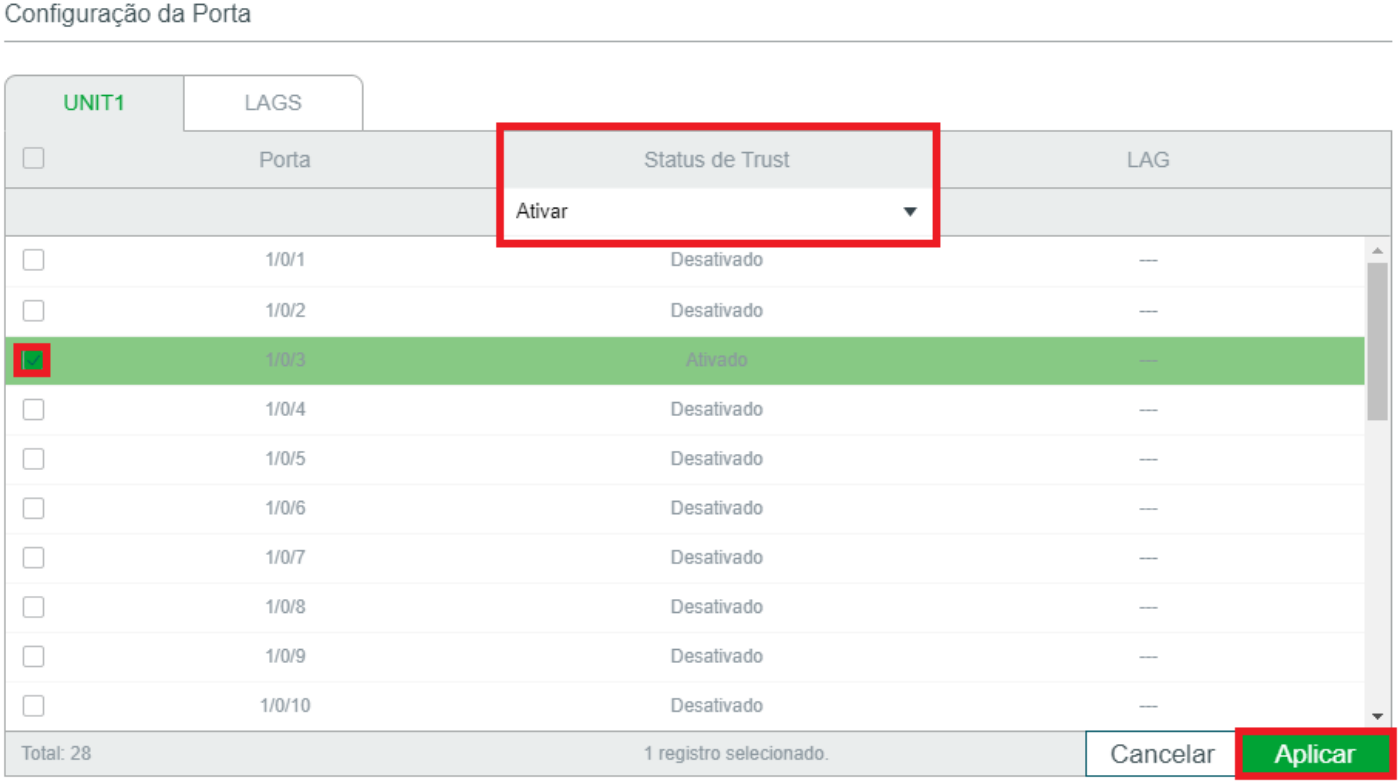


2. Da mesma forma adicione uma entrada de vínculo para o Usuário 2. Entre com o nome de Host, endereço IPv6, endereço MAC e ID da VLAN do Usuário 2, selecione o tipo de proteção como ND Detection e selecione a porta 1/0/2. Clique em **Aplicar**.

3. Vá até o menu **SEGURANÇA > IPv6 IMPB > ND Detection > Configuração Global** para carregar a página a seguir. Habilite o ND Detection e clique em **Aplicar**. Selecione a VLAN 1, mude seu status como Ativar e clique em **Aplicar**.



4. Vá até o menu **SEGURANÇA > IPv6 IMPB > ND Detection > Configuração de Porta** para carregar a página a seguir. Por padrão todas as ports estão habilitadas no ND Detection. Uma vez que a porta 1/0/3 está conectada ao roteador de gateway, configure a porta 1/0/3 como porta confiável. Clique em **Aplicar**.

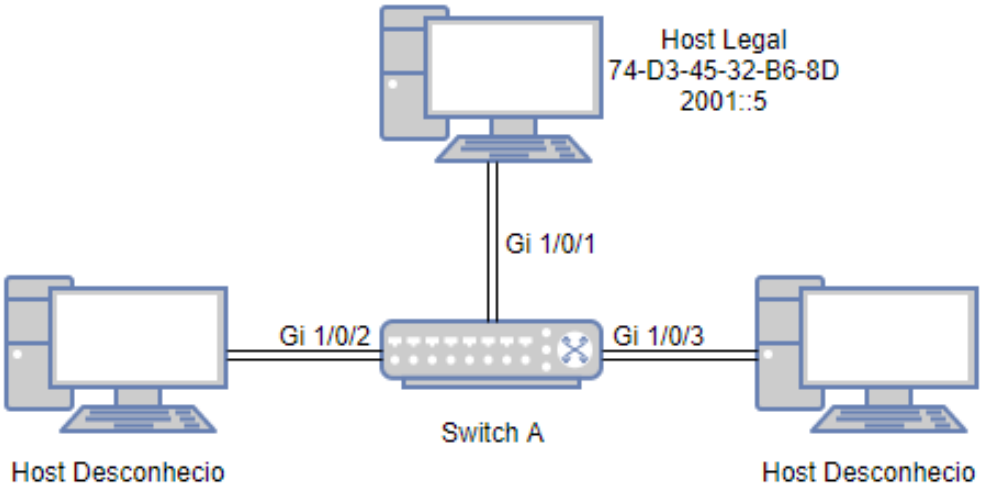


5. Clique em Salvar para salvar as configurações

Exemplo para IPv6 Source Guard

Requisitos de Rede

Como mostrado a baixo, o host IPv6 legal está conectado ao switch através da porta 1/0/1 e pertence à VLAN padrão VLAN 1. Como requisito que somente esse host legal possa acessar a rede através da porta 1/0/1 e os outros hosts desconhecidos serão bloqueados quando tentarem acessar a rede através das portas 1/0/1-3.



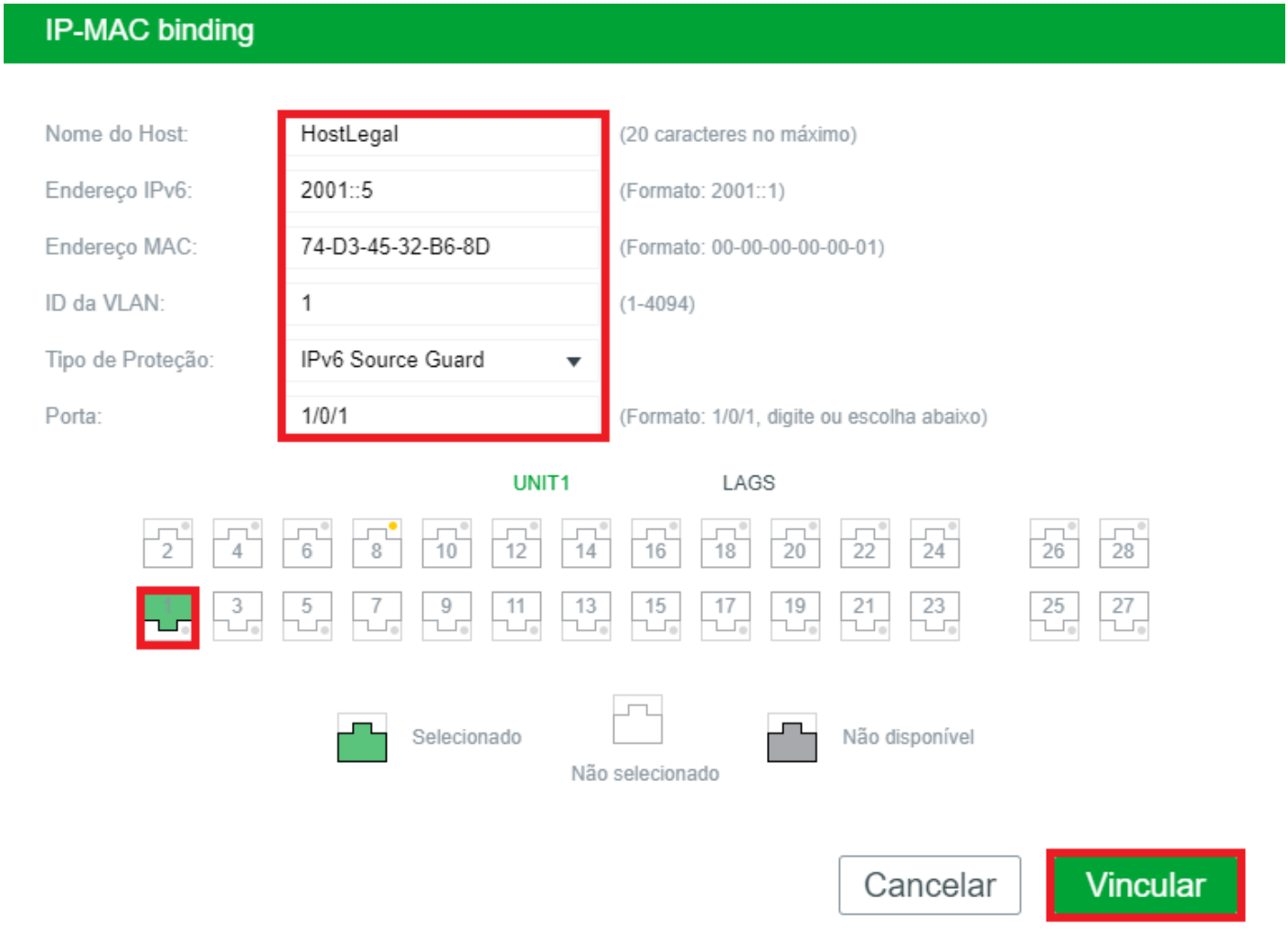
Configurando o Cenário

Para implementar esse requisito você pode usar o vínculo IPv6-MAC e o IPv6 Source Guard para filtrar os pacotes recebidos de hosts desconhecidos. A configuração geral é como mostrada a baixo:

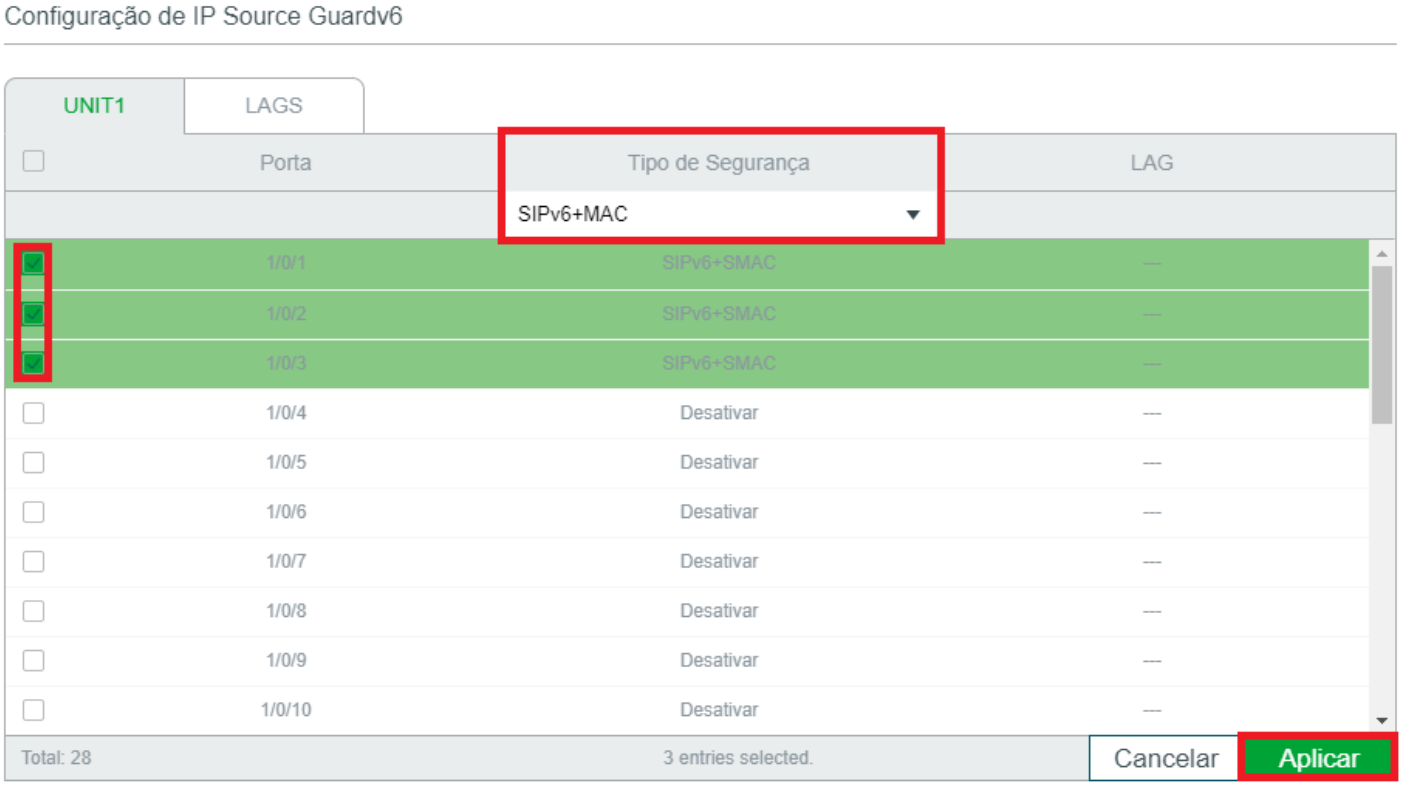
1. Vincule o endereço MAC, endereço IPv6, o número da porta conectada e a ID da VLAN dos Host Legal com o Vínculo IPv6-MAC.
2. Habilite o IPv6 Source Guard nas portas 1/0/1-3.

Para completar essas configurações siga os passos a baixo:

1. Vá até o menu **SEGURANÇA > IPv6 IMPB > Vínculo IPv6-MAC > Vínculo Manual** clique em Adicionar para carregar a página a seguir. Entre com o nome do host, endereço IPv6, endereço MAC e ID da VLAN para o host legal, selecione o tipo de proteção como IPv6 Source Guard, e selecione a porta 1/0/1 no painel. Clique em **Aplicar**.



2. Vá até o menu **SEGURANÇA > IPv6 IMPB > Protetor de Fonte IPv6** para carregar a página a seguir. Selecione as portas 1/0/1-3, configure o tipo de segurança como SIP+MAC, e então clique em **Aplicar**.



3. Clique em Salvar para salvar as configurações.

Apêndice: Configuração Padrão

As configurações padrão de DHCP Snooping estão listadas na tabela a seguir:

Configurações DHCP Snooping

Parâmetros	Configurações Padrão
Configuração Global	
DHCPv6 Snooping	Desativado
Configuração da VLAN	
Status	Desativado
Configuração da Porta	
Máximo de logs	512

As configurações Padrão do ND Detection estão listadas na tabela abaixo:

Configurações ND Detection

Parâmetros	Configurações Padrão
Configuração Global	
ND Detection	Desativado
Configuração da VLAN	

Status	Desativado
Status de Log	Desativado
Configuração da Porta	
Status de Trust	Desativado
Estatística ND	
Auto Atualizar	Desativado
Intervalo de Atualização	5 segundos

As configurações Padrão do Protetor de Fonte IPv6 estão listadas na tabela abaixo:

Configurações Protetor da Fonte IPv6

Parâmetros	**Configurações Padrão**
Configuração de Porta	
Tipo de Segurança	Desativado

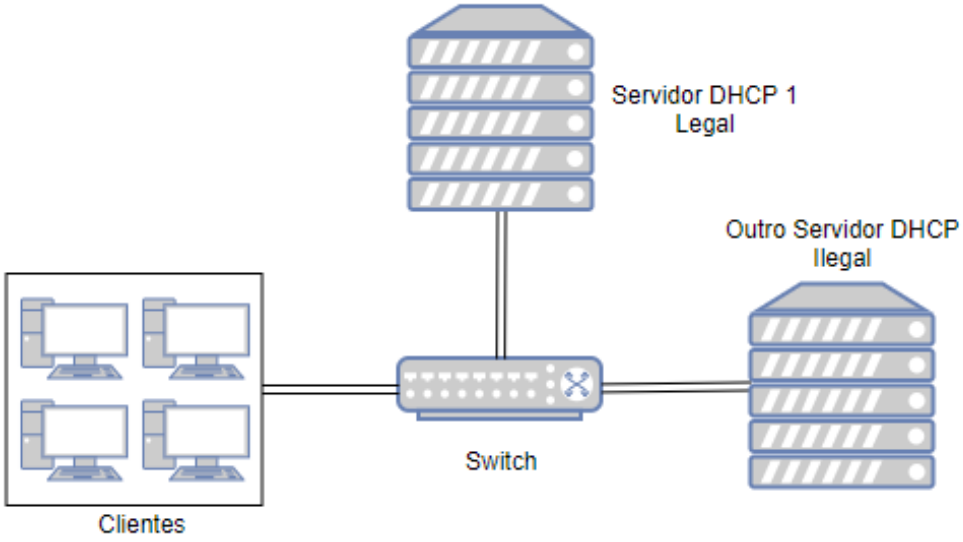
DHCP FILTER

Visão Geral

Durante o processo de funcionamento do DHCP geralmente não há mecanismo de autenticação entre o servidor DHCP e os clientes. Se existirem vários servidores DHCP na rede problemas de segurança e interferência de rede ocorrerão. O DHCP Filter resolve esse problema.

Com o filtro DHCP configurado o switch pode verificar se os pacotes DHCP são válidos e descartar os pacotes ilegais. Dessa forma o filtro DHCP garante que o usuário obtenha endereço IP de um servidor DHCP legal aumentando a segurança da rede.

Como mostrado na imagem a baixo, há ambos os Servidores DHCP na rede, um legal e um ilegal. Você pode confirmar o servidor DHCP 1 como um servidor legal provendo o endereço IP e número de porta do Servidor DHCP 1. Quando receber os pacotes de resposta DHCP o switch irá encaminhar os pacotes do servidor legal.



Você também pode limitar a taxa de encaminhamento de pacotes DHCP para cada porta.

Funções Suportadas

O Switch suporta filtro DHCPv4 e filtro DHCPv6.

DHCPv4 Filter

DHCPv4 Filter é utilizado para servidores e clientes IPv4.

DHCPv6 Filter

DHCPv6 Filter é utilizado para servidores e clientes IPv6.

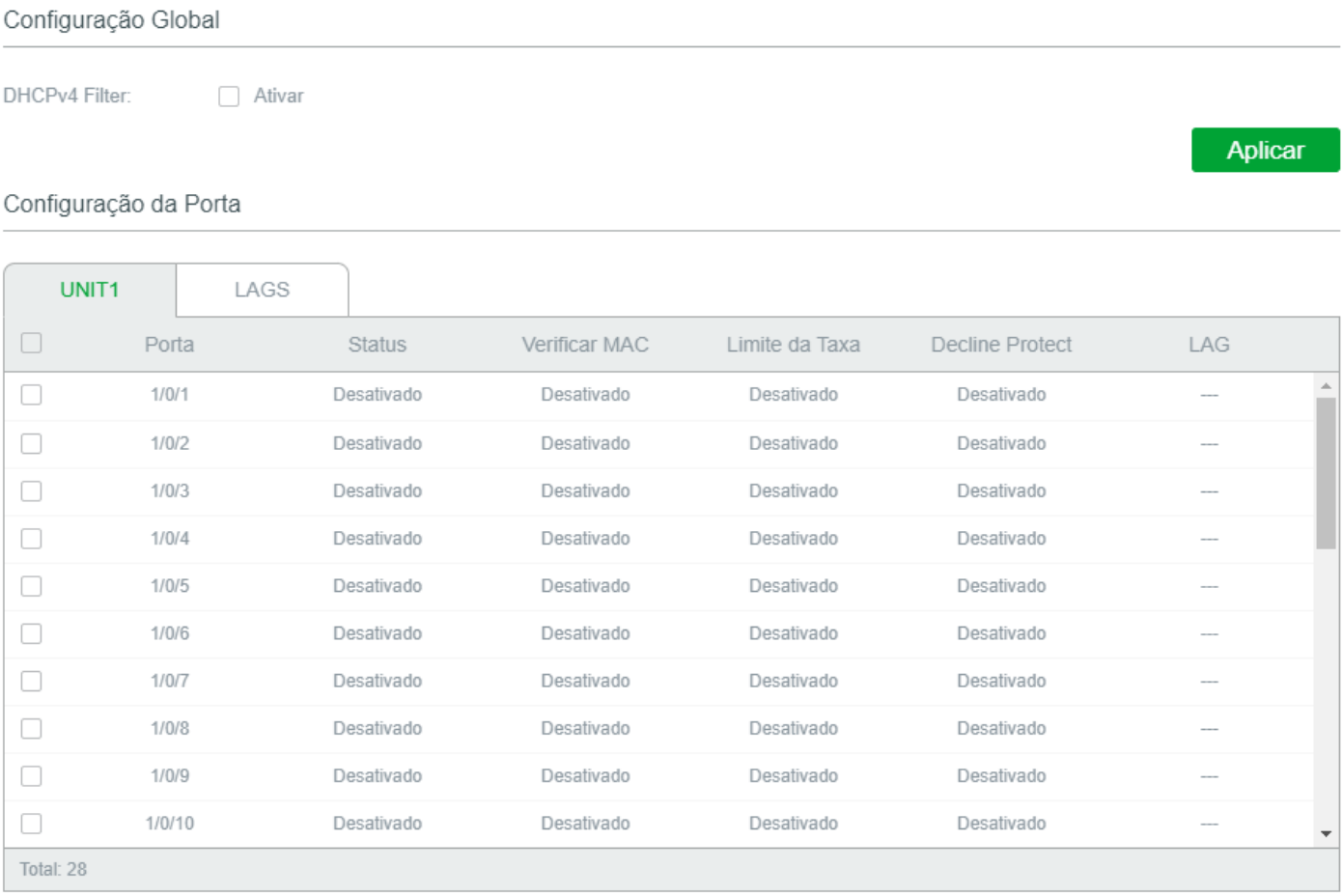
Configuração DHCPv4 Filter

Para completar a configuração do DHCPv4 Filter siga os seguintes passos:

1. Configure os parâmetros básicos para o DHCPv4 filter.
2. Configure o servidor DHCPv4 legal.

Configuração os Parâmetros Básicos do DHCPv4 Filter

Vá até o menu **SEGURANÇA > DHCP Filter > DHCPv4 Filter > Configuração Básica** para carregar a página a seguir.



Siga os seguintes passos para completar a configuração básica do DHCPv4:

1. Na seção **Configuração Global** habilite o DHCPv4 Filter globalmente.
2. Na seção **Configuração de Porta** selecione uma ou mais portas e configure os parâmetros correspondentes.

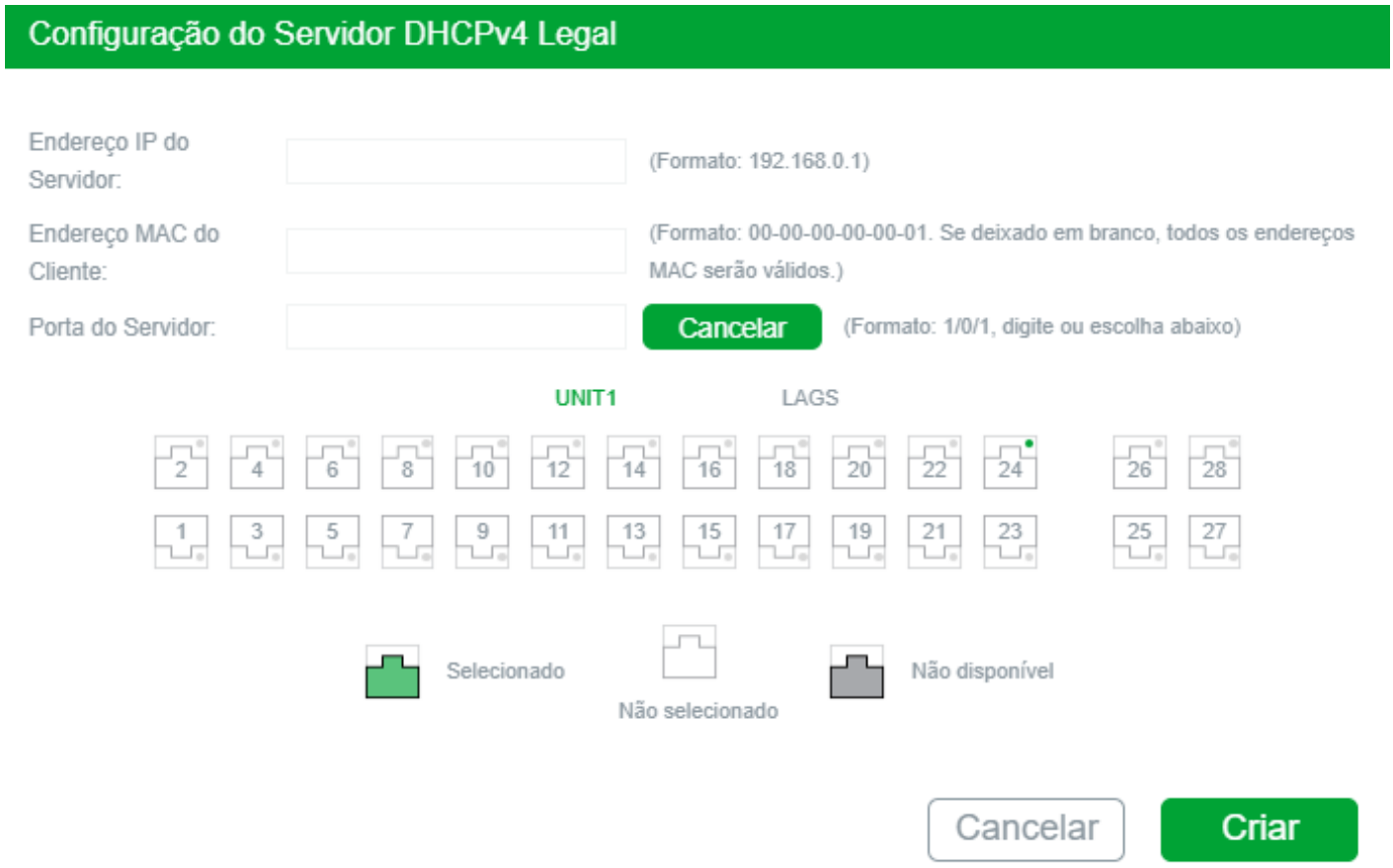
Porta	Mostra o número da Porta.
Status	Habilita ou desabilita a função de DHCPv4 Filter na porta.
Verificar MAC	Habilita ou desabilita a função de verificação de MAC. Há dois campos nos pacotes DHCPv4 que contém o endereço MAC do host. A função de verificar MAC compara os dois campos do pacote DHCPv4 e descarta os pacotes onde existem diferenças entre os campos. Isso evita que o recurso de endereços IP no servidor DHCPv4 acabem devido à endereços MAC forjados.
Limite da Taxa	Selecione para habilitar a função de limite de taxa especificando o número máximo de pacotes DHCPv4 que podem ser encaminhados pela porta por segundo. O excesso de pacotes será descartado.
Decline Protect	Selecione para habilitar a função de Decline Protect e especifique o número máximo de pacotes rejeitos que podem ser encaminhados na porta por segundo. O excesso de pacotes será descartado.
LAG	Mostra a LAG a qual a porta pertence.

3. Clique em Aplicar.

> Uma porta pertencente à um LAG (Link Aggregation Group) segue as configurações do LAG e não a sua própria. As configurações da porta só terão efeito quando a porta sair do LAG.

Configurando os Servidores Legais DHCPv4.

Vá até o menu **SEGURANÇA > DHCP Filter > DHCPv4 Filter > DHCPv4 Servers Legais** clique em Adicionar para carregar a página a seguir.



Siga os seguintes passos para adicionar um servidor DHCPv4:

1. Configure os seguintes parâmetros:

Endereço IP do Servidor	Especifique o endereço IP do Servidor DHCPv4 legal.
Endereço MAC do Cliente	(Opcional). Especifica o endereço MAC do cliente DHCP. Você também pode manter esse campo vazio, o que representa todos os clientes DHCP.
Porta do Servidor	Selecione o número da porta a qual o Servidor DHCPv4 legal está conectado.

2. Clique em **Criar**.

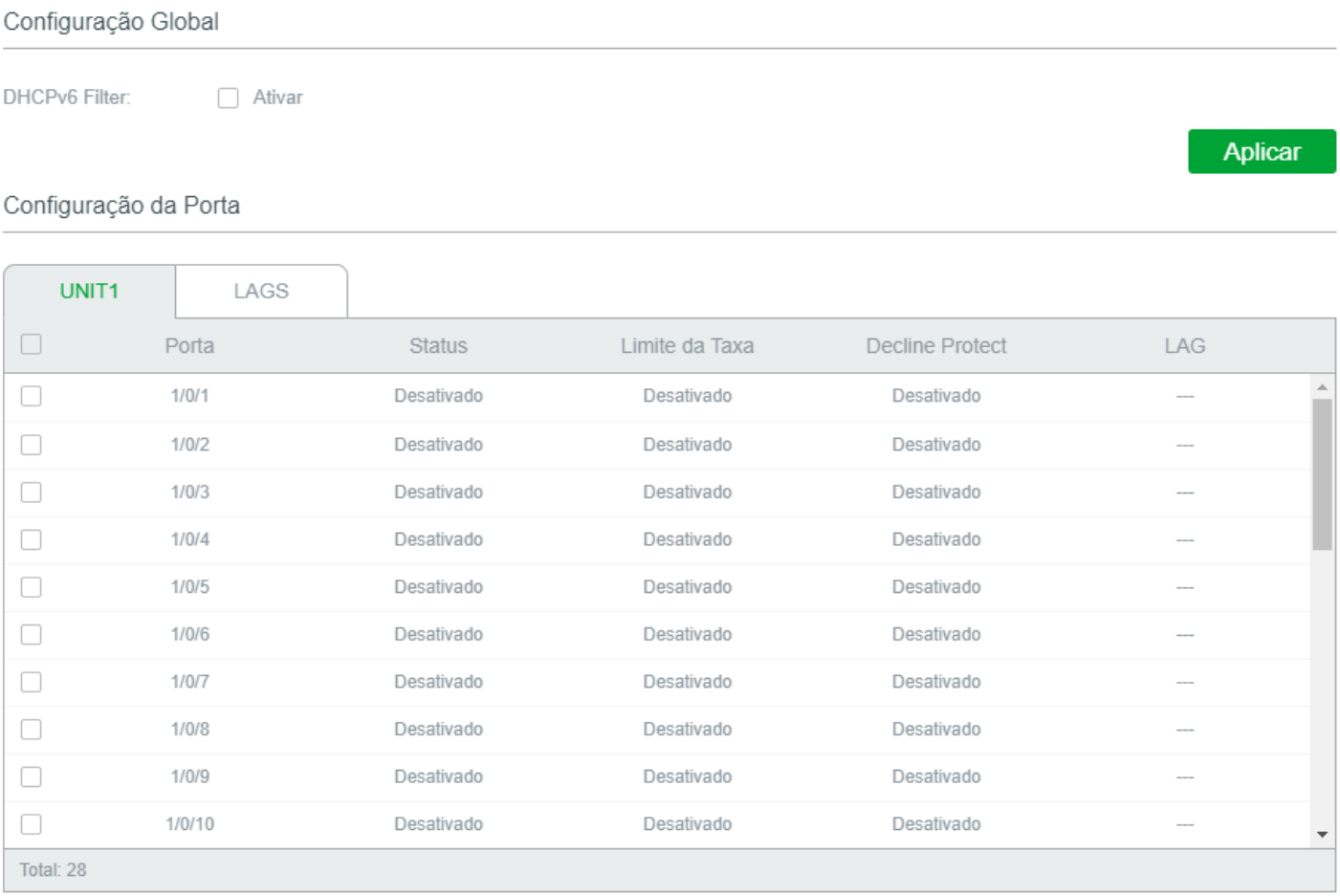
Configuração DHCPv6 Filter

Para completar a configuração do DHCPv6 Filter siga os seguintes passos:

1. Configure os parâmetros básicos para o DHCPv6 filter.
2. Configure o servidor DHCPv6 legal.

Configuração os Parâmetros Básicos do DHCPv6 Filter

Vá até o menu **SEGURANÇA > DHCP Filter > DHCPv6 Filter > Configuração Básica** para carregar a página a seguir.



Siga os seguintes passos para completar a configuração básica do DHCPv6:

1. Na seção **Configuração Global** habilite o DHCPv6 Filter globalmente.
2. Na seção **Configuração de Porta** selecione uma ou mais portas e configure os parâmetros correspondentes.

Porta	Mostra o número da Porta.
Status	Habilita ou desabilita a função de DHCPv4 Filter na porta.
Verificar MAC	Habilita ou desabilita a função de verificação de MAC. Há dois campos nos pacotes DHCPv6 que contém o endereço MAC do host. A função de verificar MAC compara os dois campos do pacote DHCPv6 e descarta os pacotes onde existem diferenças entre os campos. Isso evita que o recurso de endereços IP no servidor DHCPv6 acabem devido à endereços MAC forjados.
Limite da Taxa	Selecione para habilitar a função de limite de taxa especificando o número máximo de pacotes DHCPv6 que podem ser encaminhados pela porta por segundo. O excesso de pacotes será descartado.
Decline Protect	Selecione para habilitar a função de Decline Protect e especifique o número máximo de pacotes rejeitos que podem ser encaminhados na porta por segundo. O excesso de pacotes será descartado.
LAG	Mostra a LAG a qual a porta pertence.

3. Clique em Aplicar.

> Uma porta pertencente à um LAG (Link Aggregation Group) segue as configurações do LAG e não a sua própria. As configurações da porta só terão efeito quando a porta sair do LAG.

Configurando os Servidores Legais DHCPv6.

Vá até o menu **SEGURANÇA > DHCP Filter > DHCPv6 Filter > Servidor DHCPv6 Legal** clique em Adicionar para carregar a página a seguir.

Siga os seguintes passos para adicionar um servidor DHCPv6:

1. Configure os seguintes parâmetros:

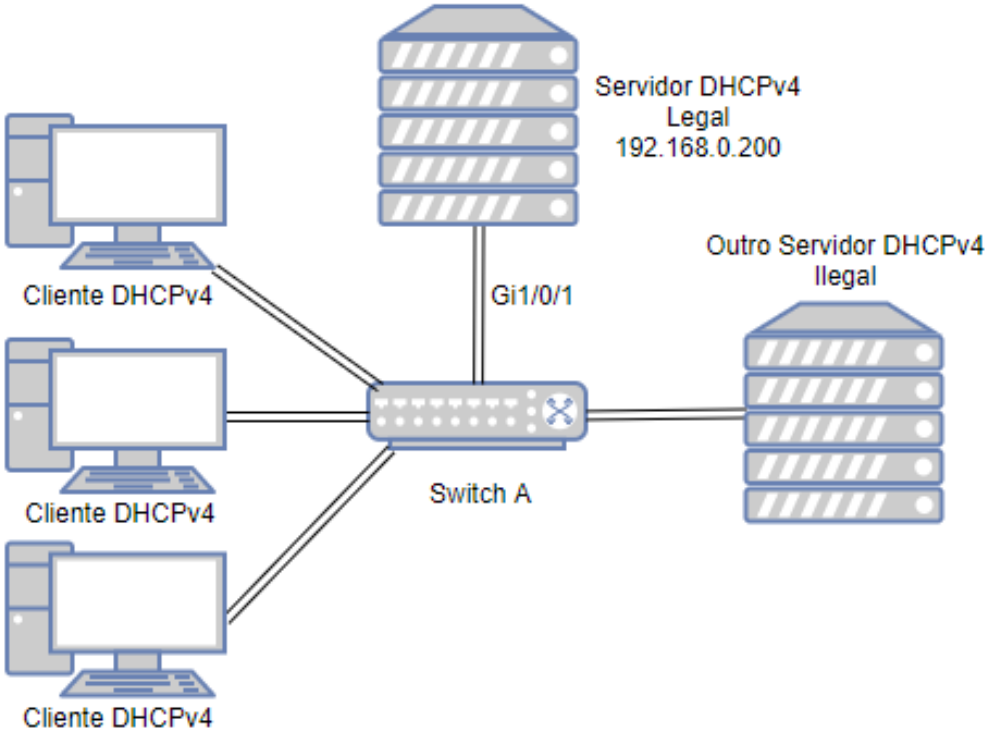
Endereço IP do Servidor	Especifique o endereço IP do Servidor DHCPv6 legal.
Porta do Servidor	Selecione o número da porta a qual o Servidor DHCPv6 legal está conectado.

2. Clique em **Criar**.

Exemplo para DHCPv4 Filter

Requisitos de Rede

Como mostrado a baixo os clientes DHCPv4 obtém endereço IP de um Servidor DHCPv4 legal, e qualquer outro servidor DHCPv4 na rede é tratado como ilegal. Agora o requisito é que somente o servidor legal seja permitido de atribuir endereços IP aos Clientes.



Configurando o Cenário

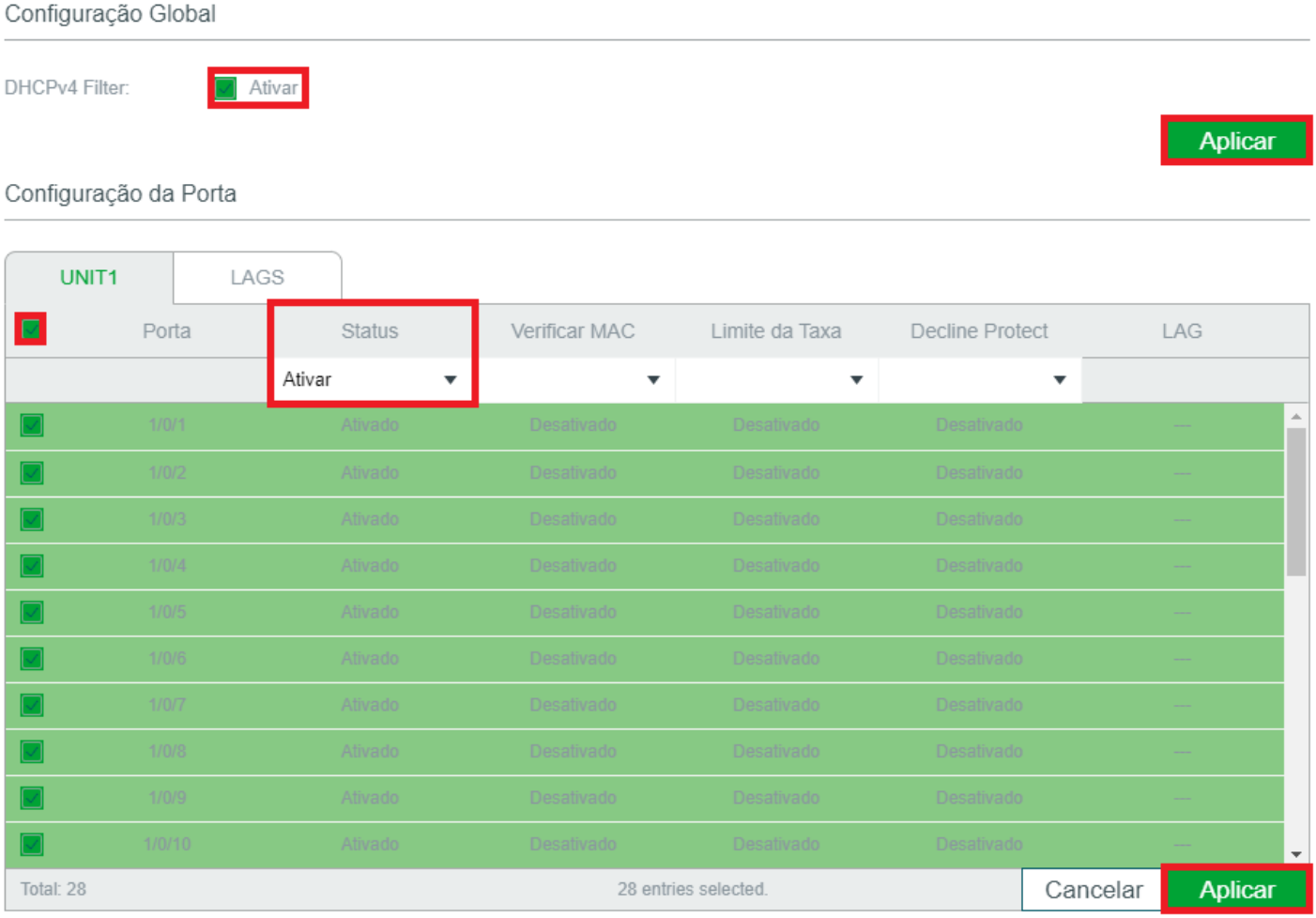
Para atingir os requisitos você pode configurar o DHCPv4 Filter para filtrar os pacotes DHCPv4 do servidor ilegal.

De modo geral a configuração é como segue:

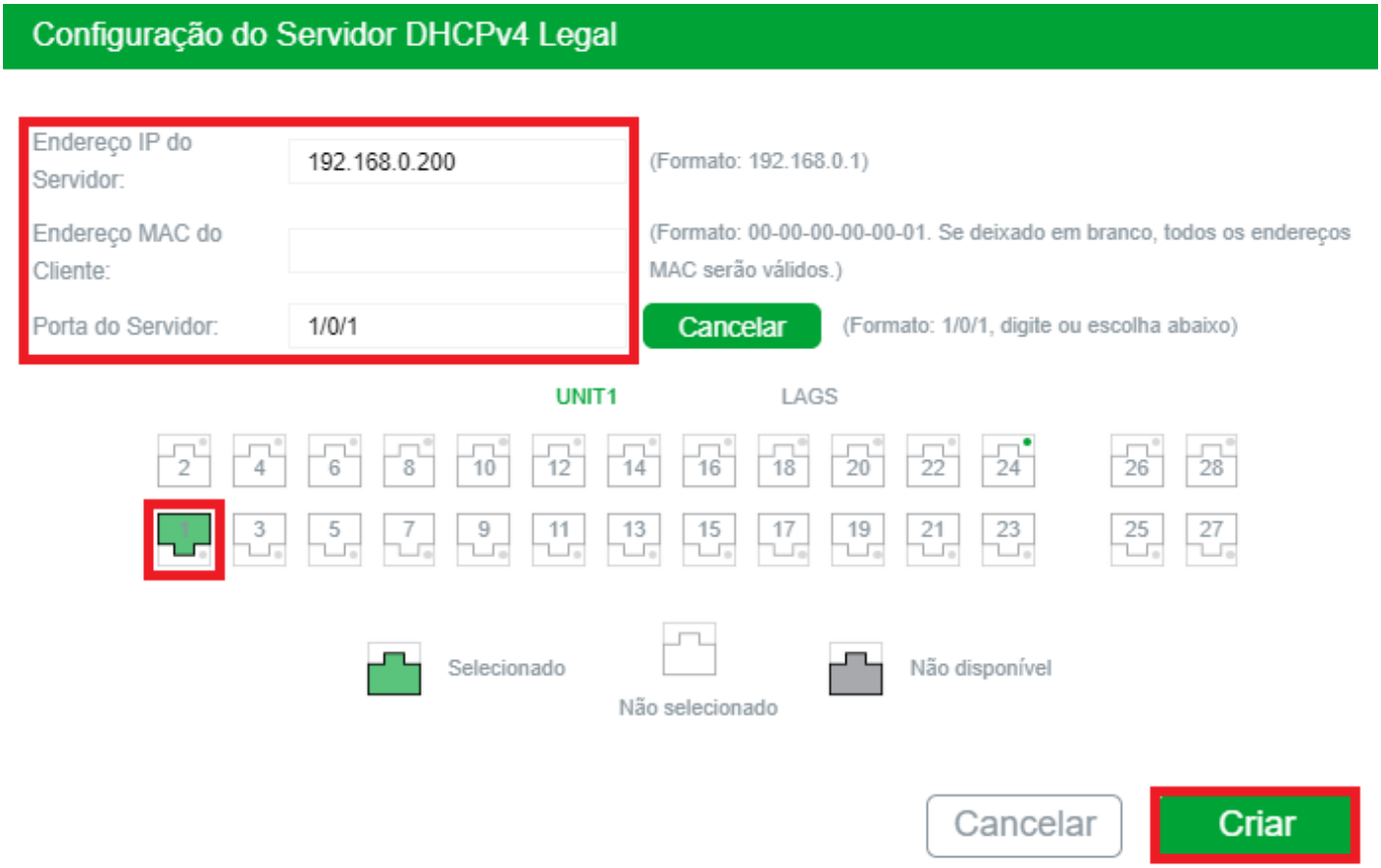
1. Habilite o DHCPv4 de forma global e para todas as portas.
2. Crie uma entrada para adicionar o DHCPv4 Server Legal.

Como será demonstrado a seguir:

1. Vá até o menu **SEGURANÇA > DHCP Filter > DHCPv4 Filter > Configuração Básica** para carregar a página a seguir. Habilite o DHCPv4 Filter globalmente e clique em **Aplicar**. Selecione todas as portas e mude o Status como Ativar, então clique em **Aplicar**.



2. Vá até o menu **SEGURANÇA > DHCP Filter > DHCPv4 Filter > DHCPv4 Servers Legais** clique em Adicionar para carregar a página a seguir. Especifique o endereço IP e o número da porta a qual o servidor DHCPv4 legal está conectado. Clique em **Criar**.

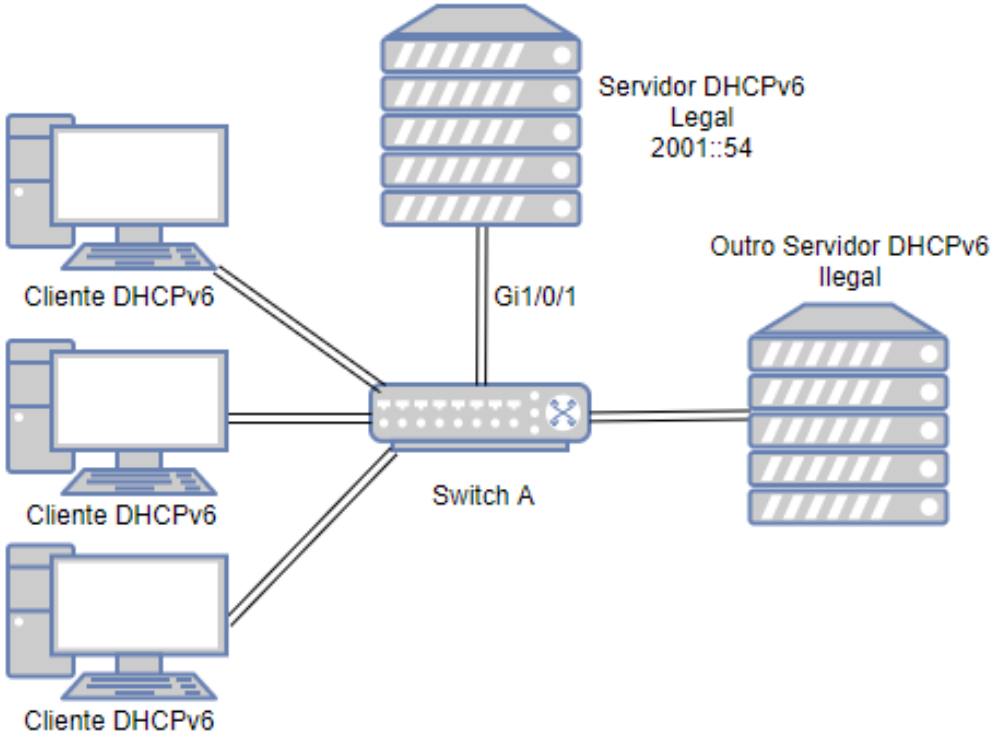


3. Clique em Salvar para salvar as configurações.

Exemplo para DHCPv6 Filter

Requisitos de Rede

Como mostrado a baixo os clientes DHCPv6 obtém endereço IP de um Servidor DHCPv6 legal, e qualquer outro servidor DHCPv6 na rede é tratado como ilegal. Agora o requisito é que somente o servidor legal seja permitido de atribuir endereços IP aos Clientes.



Configurando o Cenário

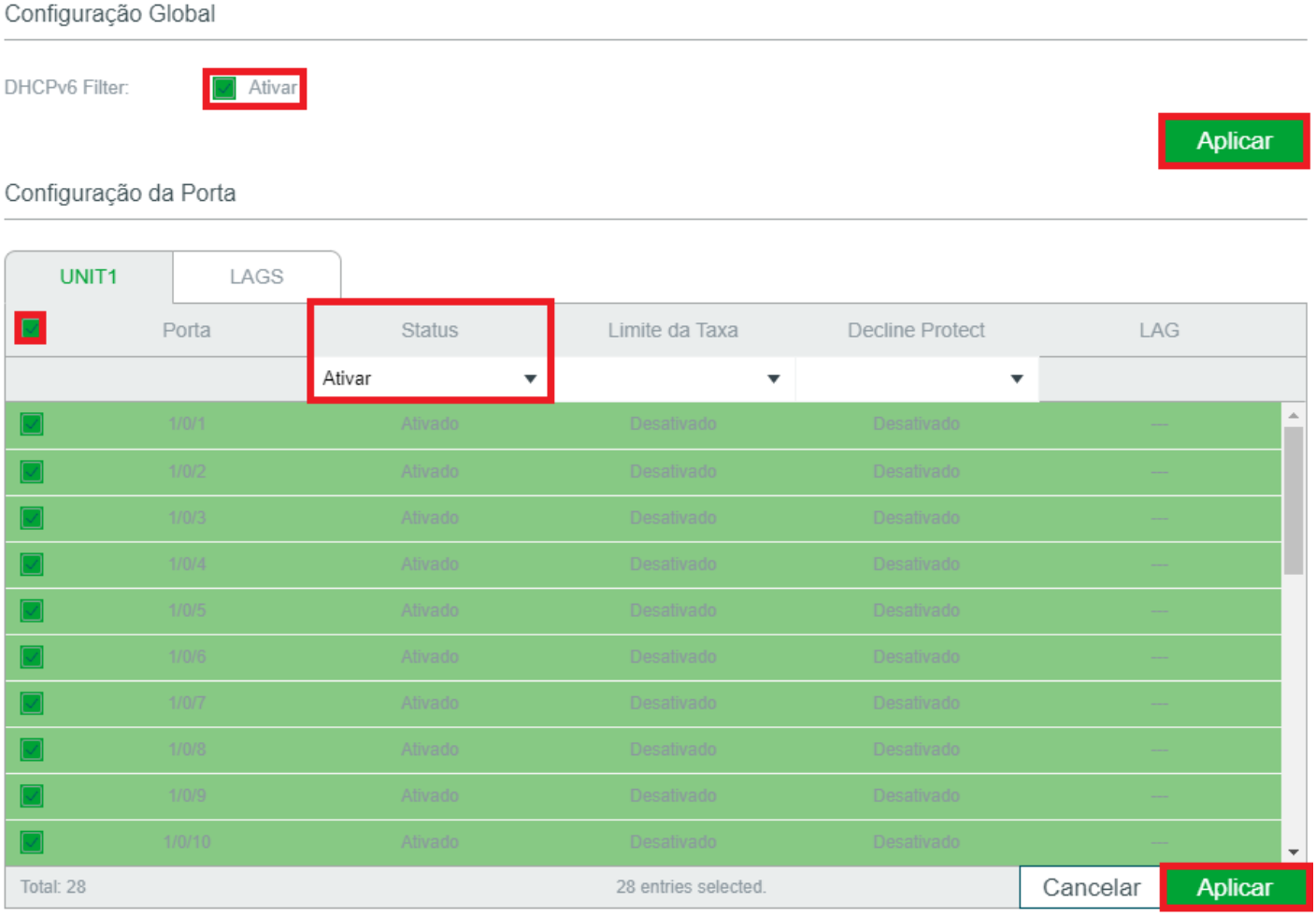
Para atingir os requisitos você pode configurar o DHCPv6 Filter para filtrar os pacotes DHCPv6 do servidor ilegal.

De modo geral a configuração é como segue:

1. Habilite o DHCPv6 de forma global e para todas as portas.
2. Crie uma entrada para adicionar o DHCPv6 Server Legal.

Como será demonstrado a seguir:

1. Vá até o menu **SEGURANÇA > DHCP Filter > DHCPv6 Filter > Configuração Básica** para carregar a página a seguir. Habilite o DHCPv6 Filter globalmente e clique em **Aplicar**. Selecione todas as portas e mude o Status como Ativar, então clique em **Aplicar**.



2. Vá até o menu **SEGURANÇA > DHCP Filter > DHCPv6 Filter > DHCPv6 Servers Legais** clique em Adicionar para carregar a página a seguir. Especifique o endereço IP e o número da porta a qual o servidor DHCPv6 legal está conectado. Clique em **Criar**.

3. Clique em Salvar para salvar as configurações.

Apêndice: Configuração Padrão

Configurações padrão do DHCP Filter estão listadas nas tabelas abaixo:

Configurações DHCPv4 Filter

Parâmetros	Configurações Padrão
Configuração Global	
DHCPv4 Filter	Desativado
Configuração de Porta	
Status	Desativado
Verificação MAC	Desativado
Limite de Taxa	Desativado
Decline Protect	Desativado

Configurações DHCPv6 Filter

Parâmetros	Configurações Padrão
Configuração Global	
DHCPv6 Filter	Desativado
Configuração de Porta	
Status	Desativado
Verificação MAC	Desativado
Limite de Taxa	Desativado
Decline Protect	Desativado

DOS

Visão Geral

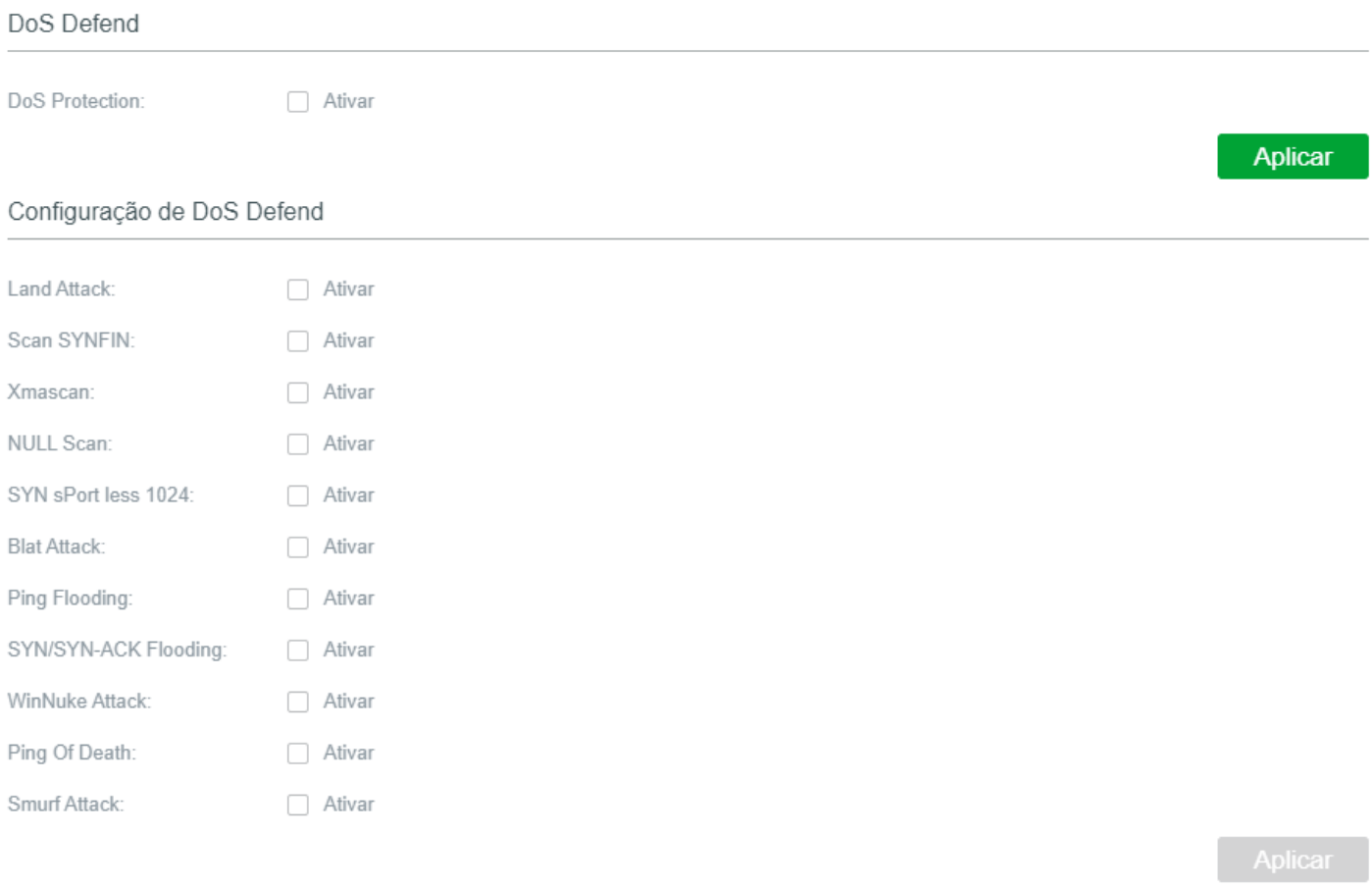
A função DoS (Denial of Service) provê proteção contra ataques DoS. Ataques DoS ocupam a largura de banda maliciosamente enviando inúmeras requisições de serviço aos hosts. Isso resulta em um serviço anormal ou quebra da rede.

Com a função DoS Defend o switch consegue analisar campos específicos dos pacotes IP distinguindo os pacotes maliciosos do ataque DoS e descartando-os diretamente. A função DoS Defend também pode limitar a taxa de transmissão dos pacotes legais. Quando o número de pacotes legais exceder o valor do limite e puder causar uma

quebra na rede o switch irá descartar os pacotes.

Configuração DoS

Vá até o menu **SEGURANÇA > DoS Defend** para carregar a página a seguir.



Siga os seguintes passo para configurar DoS Defend:

1. Na seção **DoS Defend** habilite o DoS Protection e clique em **Aplicar**.
2. Na seção **Configuração DoS Defend** selecione um ou mais tipos de defesa de acordo com a sua necessidade e clique em **Aplicar**. A tabela a seguir introduz cada tipo de ataque DoS.

Land Attack	Os invasores enviam pacotes específico com SYN (synchronous) falso para determinado host. Devido ao fato que ambos os endereços IP do pacote SYN, origem e destino, são do host, o host ficará preso em um ciclo infinito de tentativa de construir a conexão inicial.
Scan SYNFIN	Os invasores enviam pacotes com os campos SYN e FIN como 1. O campo SYN é usado para a requisição inicial da conexão onde o campo FIN é usado para solicitação de desconexão. Portanto pacotes desse tipo são ilegais.
Xmascan	Os invasores enviam pacotes ilegais com os campos index TCP, FIN, URG e PSH como 1.

NULL Scan	Os invasores enviam pacotes ilegais com a index TCP e todos os campo de controle como 0. Durante a conexão TCP e a transmissão de dados os pacotes com campos de controle como 0 são considerados ilegais.
SYN sPort less 1024	Os atacantes enviam pacotes ilegais com campo TCP SYN apontado como 1 e a porta de origem menor que 1024.
Blat Attack	Os atacantes enviam pacotes ilegais na camada 4 com o campo URG apontado como 1 e com a porta de origem e destino iguais. Similarmente ao Land Attack a performance do sistema do host atacado é reduzida devido ao comportamento cíclico do host tentando formar uma conexão com o invasor.
Ping Flooding	O invasor inunda o sistema de destino com pacotes de Ping, criando um Broadcast Storm que torna impossível para o sistema responder à comunicação legal.
SYN/SYN-ACK Flooding	Os atacantes utilizam endereços IP falsos para enviar pacotes de requisição TCP ao servidor. Uma vez recebido o pacote de requisição o servidor irá responder com pacotes de SYN-ACK. Desde que o endereço IP é falso nenhuma resposta retornará. O servidor continuará a enviar pacotes SYN-ACK. Se o invasor enviar uma grande quantidade de pacotes de requisição os recursos de rede serão ocupados maliciosamente e as requisições de clientes legais serão negadas.
WinNuke Attack	Devido a sistemas operacionais com Bug não conseguirem processar corretamente URG (urgente Pointer) dos pacotes TCP, o invasor envia esses tipos de pacotes para a porta TCP 139 (NetBIOS) dos hosts com bugs no sistema operacional, o qual irá causar com o que o host tenha tela azul.
Ping Of Death	A invasão Ping of Death significa que o invasor está enviando pacotes ping anormais com comprimento maior que 65535 bytes para causar crash no sistema do computador alvo.
Smurf Attack	Smurf attack é uma invasão distribuída de DoS (denial of service) na qual um grande número de pacotes ICMP com o endereço IP falsificado da vítima pretendida o qual será enviado via Broadcast para um computador da rede usando um endereço broadcast. A maioria dos dispositivos na rede, por padrão, irá responder a isso enviando uma resposta ao endereço de IP de origem. Se o número de maquinas na rede que responderem esse pacote for grande o computador da vítima será inundado com tráfego.

3. Clique em **Aplicar**.

Apêndice: Configuração Padrão

Configurações padrão de segurança da rede estão listadas na tabela a baixo:

Configurações DoS

Parâmetros	Configurações Padrão
DoS Defend	Desabilitado

MONITOR DO SISTEMA

Visão Geral

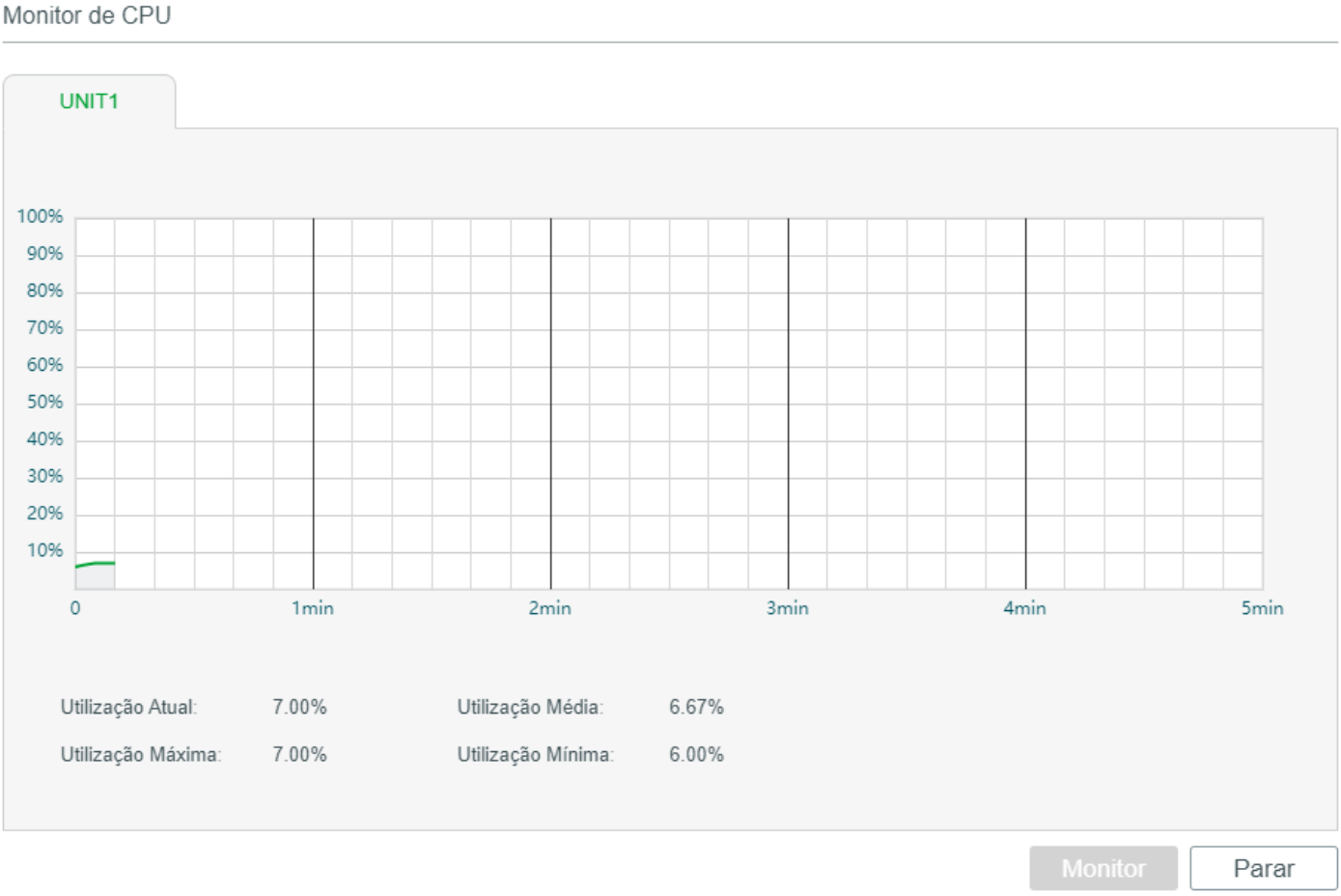
Com a função de Monitor do Sistema você pode:

- Monitorar a utilização da CPU do switch.
- Monitorar a utilização de memória do switch.

A utilização da CPU deve sempre estar abaixo de 80%, um uso excessivo pode resultar em um mal funcionamento do switch. Por exemplo, o switch falhou em responder às requisições de gerenciamento (ICMP ping, SNMP Timeouts, sessões Telnet e SSH lentas). Você pode monitorar o sistema para verificar o problema de utilização de CPU.

Monitoramento da CPU

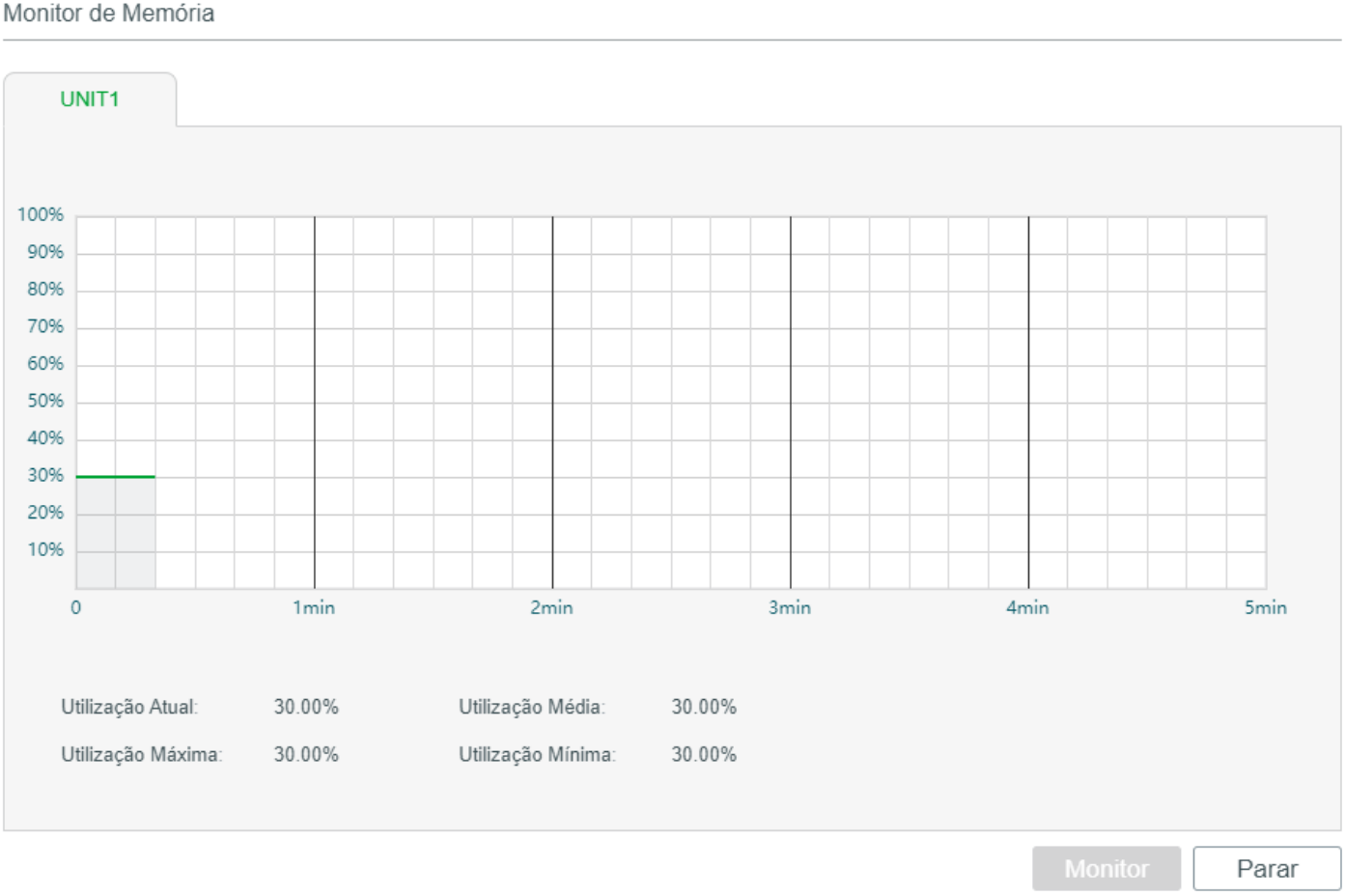
Vá até o menu **MANUTENÇÃO > Monitor do Sistema > Monitor de CPU** para carregar a seguinte página.



Clique em **Monitor** para habilitar o monitor e mostrar a visualização da taxa de utilização de CPU atualizando a cada 5 segundos.

Monitoramento da Memória

Vá até o menu **MANUTENÇÃO > Monitor do Sistema > Monitor de Memória** para carregar a seguinte página.



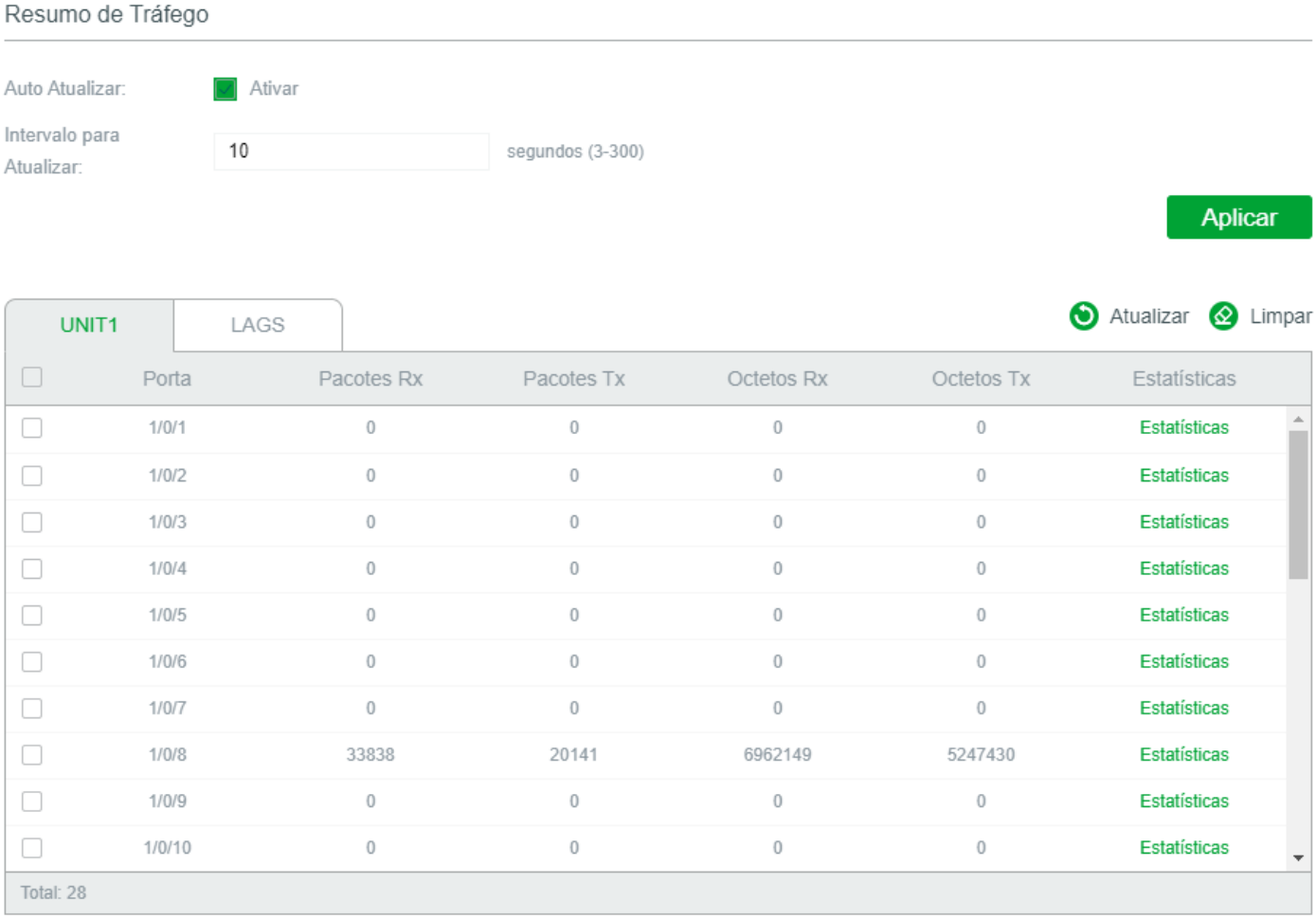
Clique em **Monitor** para habilitar o monitor e mostrar a visualização da taxa de utilização de memória atualizando a cada 5 segundos.

MONITORANDO TRÁFEGO

Monitor de Tráfego

Com a função Monitor de tráfego, você pode monitorar as informações de tráfego de cada porta, incluindo o resumo e as estatísticas de tráfego em detalhes.

Escolha o menu **MANUTENÇÃO > Monitor de Tráfego** para carregar a página a seguir.



Siga estas etapas para visualizar o resumo do tráfego de cada porta:

1. Para obter o resumo do tráfego em tempo real, ative a função Auto Atualizar ou clique em Atualizar.

Auto Atualizar	Com essa opção ativada, o switch atualizará automaticamente o resumo do tráfego.
Intervalo para Atualizar	Especifique o intervalo de tempo para o switch atualizar o resumo do tráfego.

2. Na seção **Resumo de Tráfego**, clique em UNIT1 para mostrar as informações das portas físicas e clique em LAGS para mostrar as informações dos LAGs.

Pacotes Rx	Exibe o número de pacotes recebidos na porta. Pacotes com erro não são contados.
Pacotes Tx	Exibe o número de pacotes transmitidos na porta. Pacotes com erro não são contados.
Octetos Rx	Exibe o número de octetos recebidos na porta. Octetos com erro são contados.
Octetos Tx	Exibe o número de octetos transmitidos na porta. Octetos com erro são contados.

Para visualizar as estatísticas de tráfego de uma porta em detalhes, clique em **Estatísticas** no lado direito da entrada.

Recebidos	Exibe as informações detalhadas dos pacotes recebidos. **Transmissão:** exibe o número de pacotes de transmissão válidos recebidos na porta. Os quadros com erro não são contados. **Multicast:** exibe o número de pacotes multicast válidos recebidos na porta. Os quadros com erro não são contados. **Unicast:** exibe o número de pacotes unicast válidos recebidos na porta. Os quadros com erro não são contados **Jumbo:** exibe o número de pacotes jumbo válidos recebidos na porta. Os quadros com erro não são contados. **Erros de alinhamento:** exibe o número de pacotes recebidos que possuem uma FCS (Frame Check Sequence) com um octeto não integral (erro de alinhamento). O tamanho do pacote está entre 64 bytes e 1518 bytes. **Pacotes de tamanho menor:** exibe o número de pacotes recebidos (excluindo pacotes com erro) com menos de 64 bytes. **Pacotes de 64 octetos:** exibe o número de pacotes recebidos (incluindo pacotes com erro) com 64 bytes de comprimento. **Pacotes de 65 a 127 Octetos:** exibe o número de pacotes recebidos (incluindo pacotes com erro) com comprimento entre 65 e 127 bytes. **Pacotes de 128 a 255 octetos:** exibe o número de pacotes recebidos (incluindo pacotes com erro) com comprimento entre 128 e 255 bytes. **Pacotes de 256 a 511 Octetos:** exibe o número de pacotes recebidos (incluindo pacotes com erro) com comprimento entre 256 e 511 bytes. **Pacotes de 512 a 1023 Octetos:** exibe o número de pacotes recebidos (incluindo pacotes com erro) com comprimento entre 512 e 1023 bytes. **Pacotes de 1023 a 1518 Octetos:** exibe o número de pacotes recebidos (incluindo pacotes com erro) com comprimento entre 512 e 1023 bytes. **Pacotes:** exibe o número de pacotes recebidos na porta. Pacotes de com erro não são contados. **Bytes:** exibe o número de bytes recebidos na porta. Pacotes com erro não são contados.

	Exibe as informações detalhadas dos pacotes enviados. **Broadcast:** exibe o número de pacotes de broadcast válidos transmitidos na porta. Os quadros com erro não são contados. **Multicast:** exibe o número de pacotes multicast válidos transmitidos na porta. Os quadros com erro não são contados. **Unicast:** exibe o número de pacotes unicast válidos transmitidos na porta. Os quadros com erro não são contados. **Pacotes:** exibe o número de pacotes transmitidos na porta. Pacotes com erro não são contados. **Bytes:** exibe o número de bytes transmitidos na porta. Pacotes com erro não são contados. **Colisões:** exibe o número de colisões experimentadas por uma porta half-duplex durante transmissões de pacotes.
Enviados	

Apêndice: Configuração Padrão

Configurações padrão do monitoramento de tráfego estão listadas na tabela a baixo:

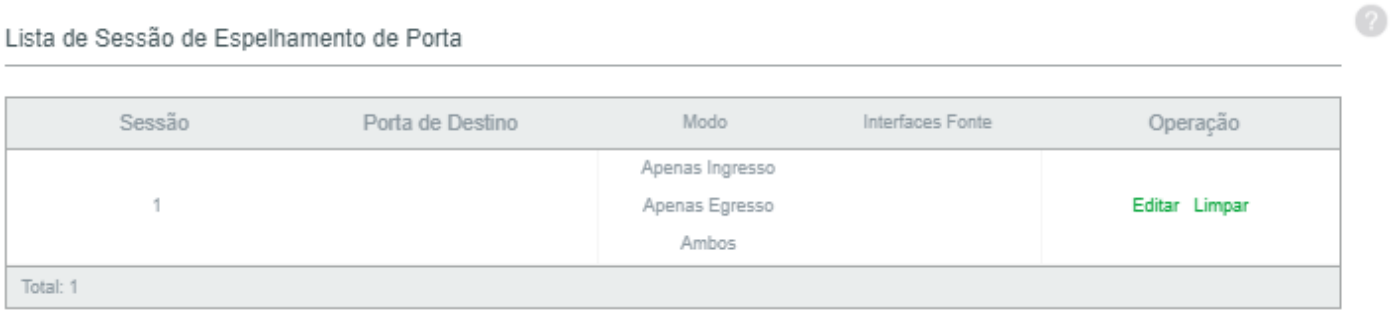
Parâmetros	**Configurações Padrão**
Resumo de Tráfego	
Auto Atualizar	Desativado
Intervalo para Atualizar	10 segundos

ESPELHAMENTO DE TRÁFEGO

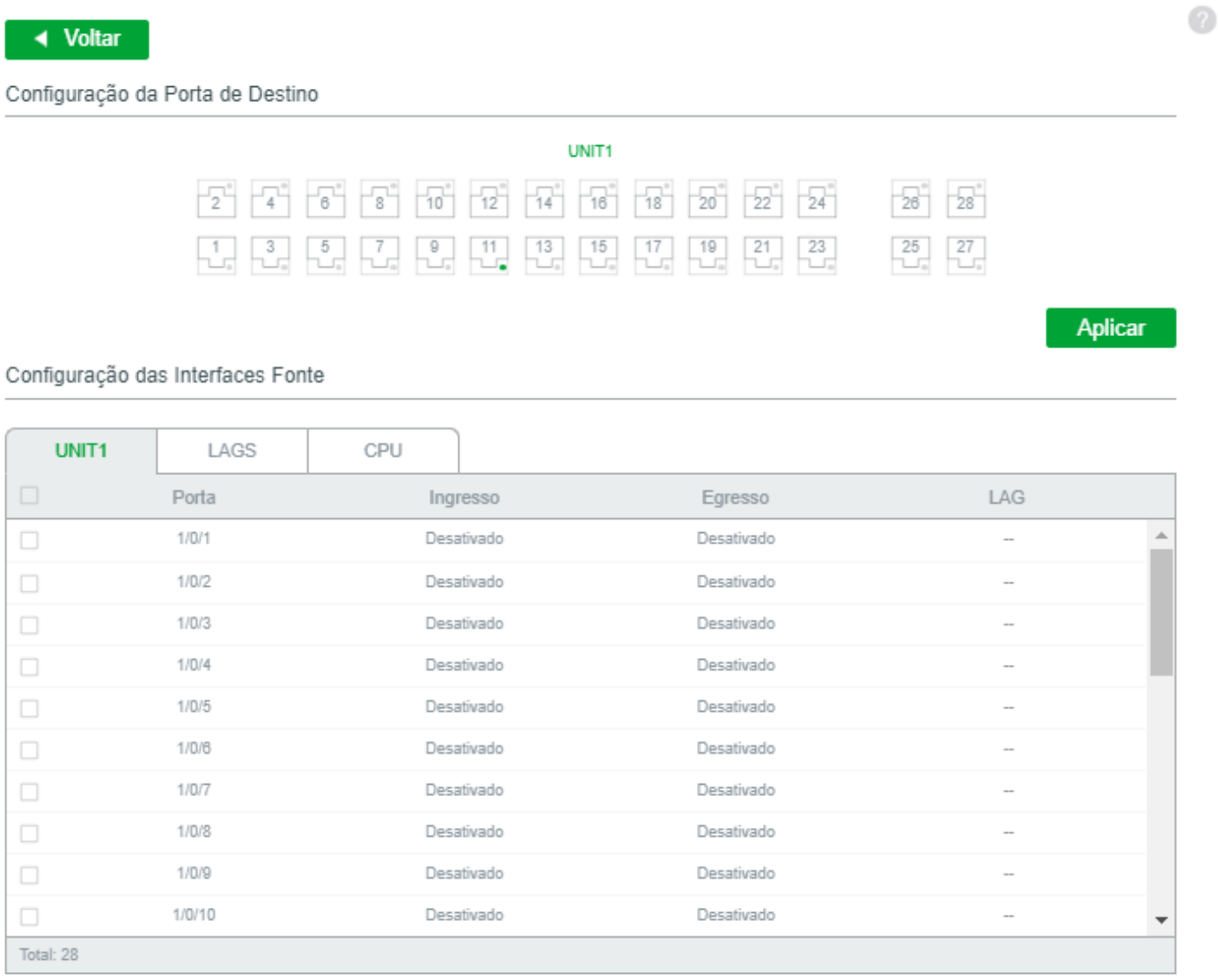
Espelhamento

Você pode analisar o tráfego de rede e solucionar problemas de rede usando o espelhamento. O espelhamento permite que o switch envie uma cópia do tráfego que passa pelas fontes especificadas (portas, LAGs ou CPU) para uma porta de destino. Não afeta a comutação do tráfego de rede nas portas de origem, nos LAGs ou na CPU.

Escolha o menu **MANUTENÇÃO > Espelhamento** para carregar a página seguinte.



A página acima exibe uma sessão de espelhamento e nenhuma outra sessão pode ser criada. Clique em **Editar** para configurar esta sessão de espelhamento na página a seguir.



Siga estas etapas para configurar a sessão de espelhamento:

1. Na seção **Configuração da Porta de Destino**, especifique uma porta de destino para a sessão de espelhamento e clique em **Aplicar**.
2. Na seção **Configuração das Interfaces Fonte**, especifique as interfaces de origem e clique em **Aplicar**. O tráfego que passa pelas interfaces de origem será espelhado na porta de destino. Existem três tipos de interface de origem: porta, LAG e CPU. Escolha um ou mais tipos de acordo com sua necessidade.

UNIT1	Selecione as portas desejadas como as interfaces de origem. O switch enviará uma cópia do tráfego que passa pela porta para a porta de destino.
LAGS	Selecione os LAGs desejados como interfaces de origem. O switch enviará uma cópia do tráfego passando pelos membros do LAG para a porta de destino.
CPU	Quando selecionado, o switch envia uma cópia do tráfego que passa pela CPU para a porta de destino.
Ingresso	Com esta opção ativada, os pacotes recebidos pela interface correspondente (porta, LAG ou CPU) serão copiados para a porta de destino. Por padrão, está desativado.
Egresso	Com esta opção ativada, os pacotes enviados pela interface correspondente (porta, LAG ou CPU) serão copiados para a porta de destino. Por padrão, está desativado.

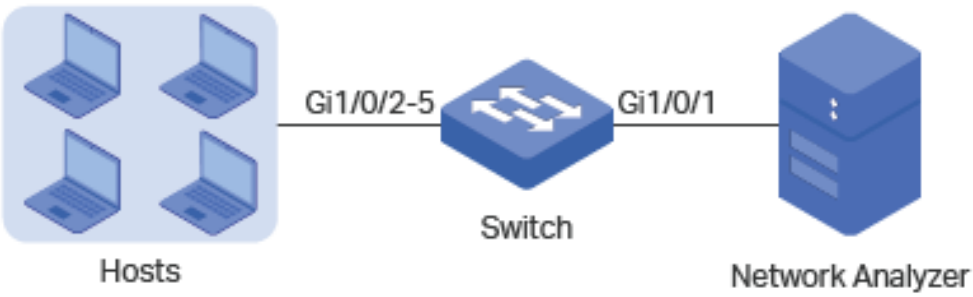
As portas membro de um LAG não podem ser definidas como porta de destino ou porta de origem.

Uma porta não pode ser definida como a porta de destino e a porta de origem ao mesmo tempo.

Exemplo de Configuração

Requisitos de Rede

Como mostrado abaixo, vários hosts e um analisador de rede estão diretamente conectados ao switch. Para segurança e solução de problemas de rede, o gerente de rede precisa usar o analisador de rede para monitorar os pacotes de dados dos hosts finais.



Configurando o Cenário

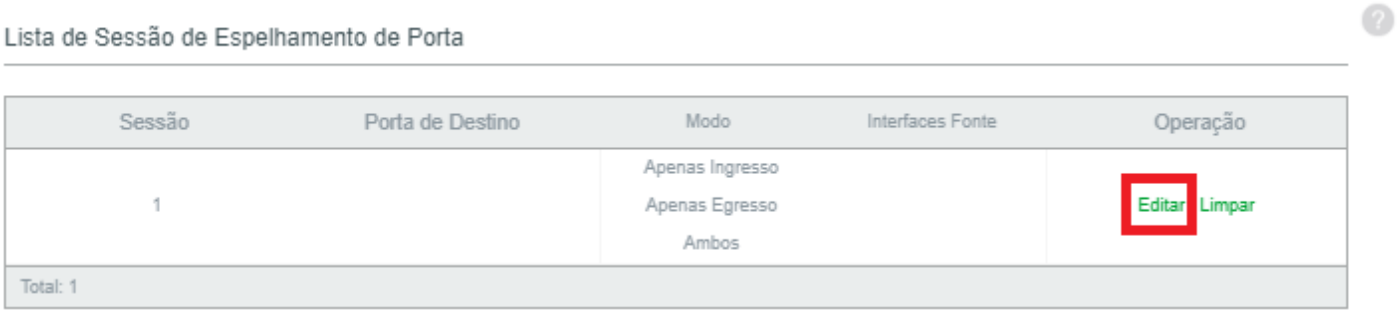
Para implementar esse requisito, você pode usar o recurso Espelhamento para copiar os pacotes das portas 1/0/2-5 para a porta 1/0/1. A visão geral da configuração é a seguinte:

1. Especifique as portas 1/0/2-5 como as portas de origem, permitindo que o switch copie os pacotes dos hosts.

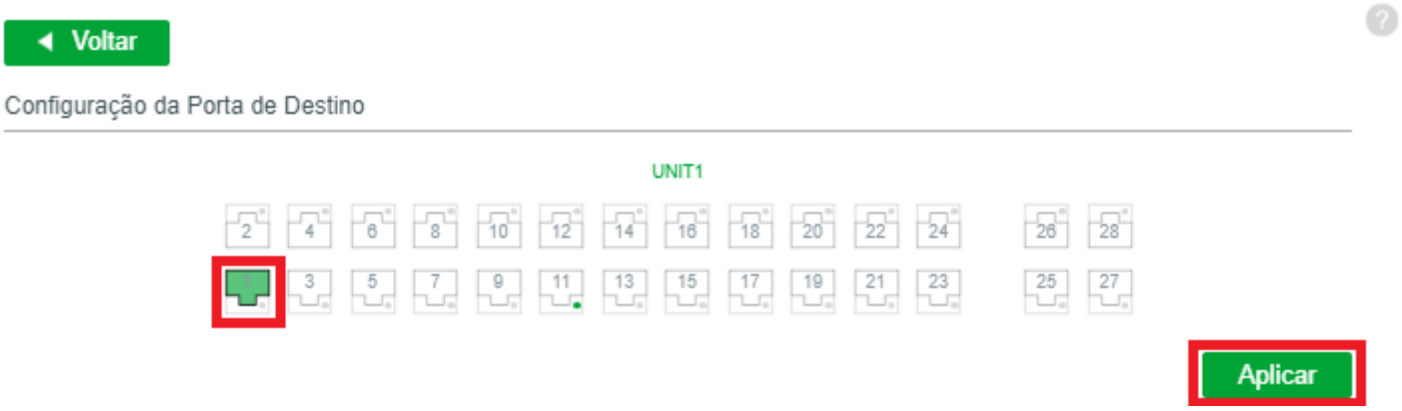
2. Especifique a porta 1/0/1 como a porta de destino para que o analisador de rede possa receber pacotes espelhados dos hosts.

A seção a seguir descreve o procedimento para configuração:

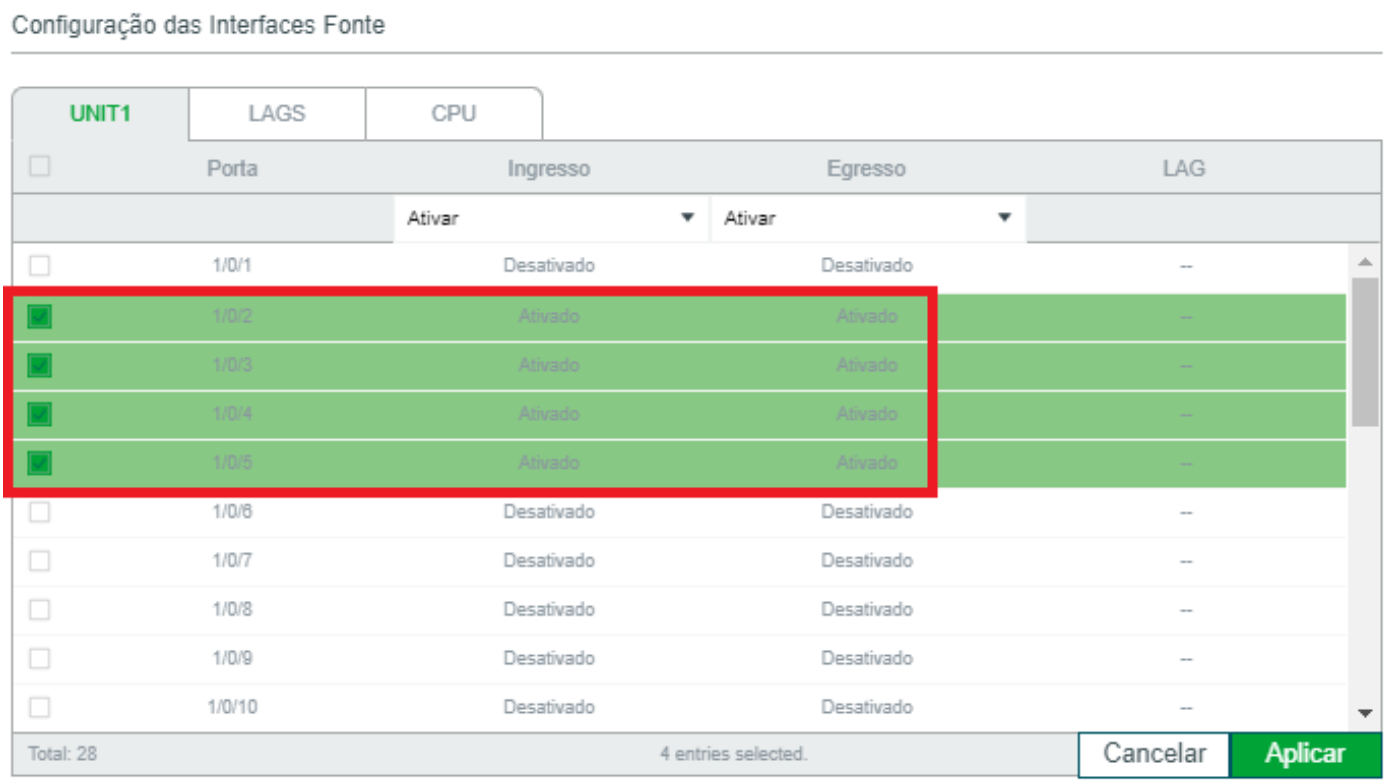
1. Escolha o menu **MANUTENÇÃO > Espelhamento** para carregar a página seguinte. Ele exibe as informações da sessão de espelhamento.



2. Clique em **Editar** na página acima para carregar a página seguinte. Na seção Configuração da Porta de Destino, selecione a porta 1/0/1 como a porta de destino e clique em **Aplicar**.



3. Na seção **Configuração das Interfaces Fonte**, selecione as portas 1/0/2-5 como portas de origem e ative o Ingresso e o Egresso para permitir que os pacotes recebidos e enviados sejam copiados para a porta de destino. Depois clique em **Aplicar**.



4. Clique em Salvar para salvar as configurações.

Apêndice: Configuração Padrão

As configurações padrão do Switch estão listadas na tabela a seguir.

Parâmetros	Configurações Padrão
Ingresso	Desativado
Egresso	Desativado

DLDP

Visão Geral

O DLDP (Protocolo de detecção de link de dispositivo) é um protocolo de camada 2 que permite que os dispositivos conectados através de cabos Ethernet de fibra ou par trançado detectem se existe um link unidirecional.

Um link unidirecional ocorre sempre que o tráfego enviado por um dispositivo local é recebido pelo dispositivo de mesmo nível, mas o tráfego do dispositivo de mesmo nível não é recebido pelo dispositivo local.

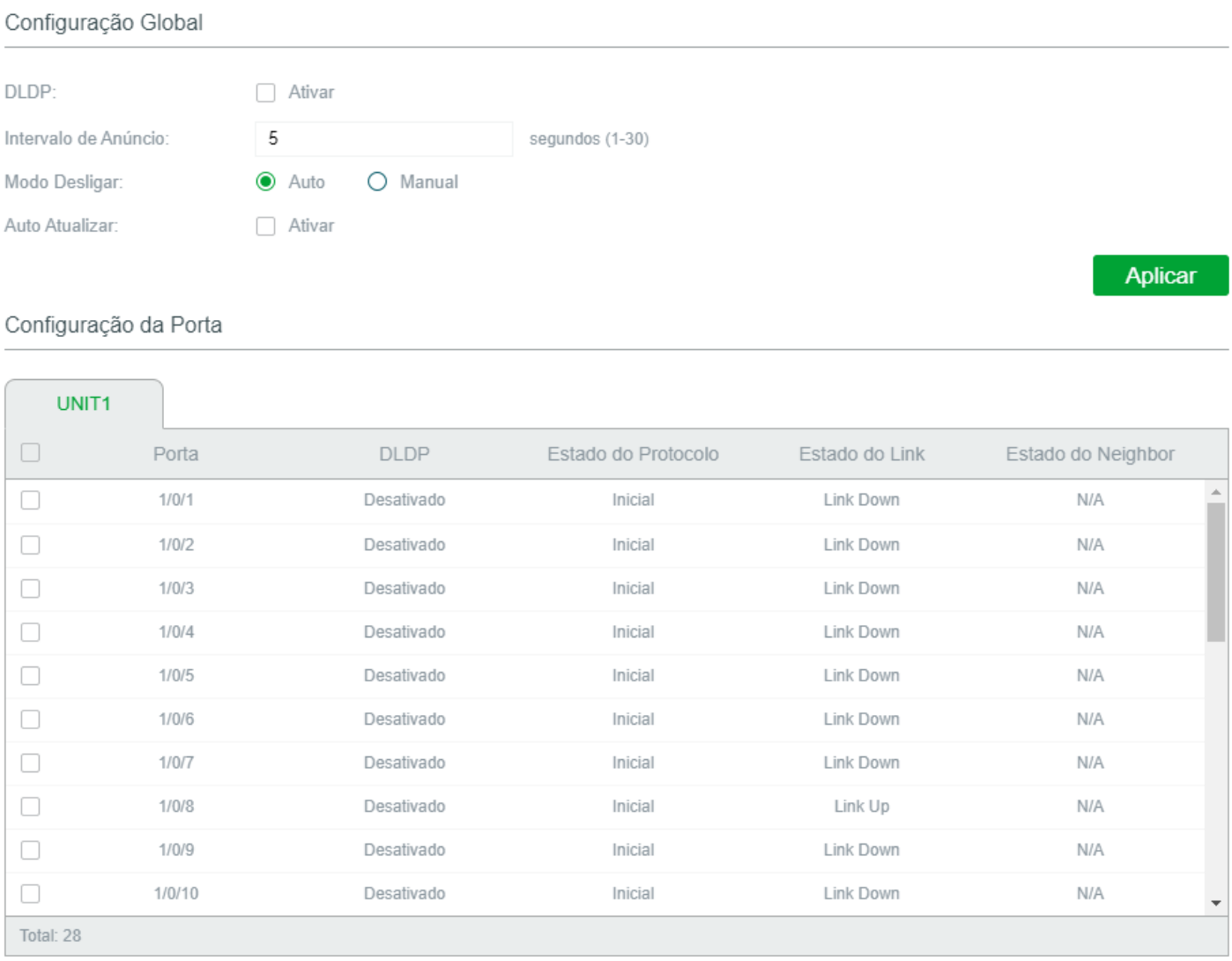
Links unidirecionais podem causar uma variedade de problemas, como loops de topologia de spanning-tree. Depois de detectar um link unidirecional, o DLDP pode desligar a porta relacionada automaticamente ou informar os usuários.

Configuração DLDP

Diretrizes de configuração

- Uma porta compatível com DLDP não pode detectar um link unidirecional se estiver conectada a uma porta não compatível com DLDP de outro switch.
- Para detectar links unidirecionais, verifique se o DLDP está ativado nos dois lados dos links.

Escolha o menu **MANUTENÇÃO> DLDP** para carregar a seguinte página.



Siga estas etapas para configurar o DLDP:

1. Na seção **Configuração Global**, ative o DLDP e configure os parâmetros relevantes. Clique em **Aplicar**.

DLDP	Ative ou desative o DLDP globalmente.
Intervalo de Anúncio	Configure o intervalo para enviar pacotes de anúncios. Os valores válidos são de 1 a 30 segundos e o valor padrão é 5 segundos.

Modo Desligar	Escolha como desligar a porta quando um link unidirecional for detectado: **Automático:** quando um link unidirecional é detectado em uma porta, o DLDP gera logs e traps e, em seguida, encerra a porta, e o DLDP nessa porta muda para Desativado. **Manual:** quando um link unidirecional é detectado em uma porta, o DLDP gera logs e traps e, em seguida, os usuários podem desligar manualmente as portas do link unidirecional
Auto Atualizar	Com essa opção ativada, o switch atualiza automaticamente as informações do DLDP.
Intervalo de Atualização	Especifique o intervalo de tempo em que o switch atualizará as informações do DLDP. Os valores válidos são de 1 a 100 segundos e o valor padrão é 3 segundos.

2. Na seção **Configuração da Porta**, selecione uma ou mais portas, ative o DLDP e clique em Aplicar. Em seguida, você pode visualizar as informações DLDP relevantes na tabela.

DLDP	Ative ou desative o DLDP na porta.
Estado do Protocolo	Exibe o estado do protocolo DLDP. **Inicial:** DLDP está desativado. **Inativo:** o DLDP está ativado, mas o link está inoperante. **Ativo:** o DLDP está ativado e o link está ativo, ou as entradas vizinhas neste dispositivo estão vazias. **Anúncio:** nenhum link unidirecional é detectado (o dispositivo estabeleceu links bidirecionais com todos os seus vizinhos) ou o DLDP permaneceu no status Ativo por mais de 5 segundos. **Teste:** nesse estado, o dispositivo enviará pacotes de teste para detectar se o link é unidirecional. A porta entra nesse estado no estado Ativo se receber um pacote de um vizinho desconhecido. **Desativar:**um link unidirecional é detectado.
Estado do Link	Exibe o estado do link. **Link-Down:** o link está inoperante. **Link-Up:** o link está ativo.

Estado do Neighbor	Exibe o estado vizinho. **Desconhecido:**a detecção de link está em andamento. **Unidirecional:** o link entre a porta e o vizinho é unidirecional. **Bidirecional:** o link entre a porta e o vizinho é bidirecional.

Apêndice: Configuração Padrão

As configurações padrão do DLDP estão listadas na tabela a seguir.

Parâmetros	Configurações Padrão
Configuração Global	
DLDP	Desativado
Intervalo de Anúncio	5 segundos
Modo Desligar	Auto
Auto Atualizar	Desativado
Intervalo de Atualização	3 segundos
Configuração da Porta	
DLDP	Desativado

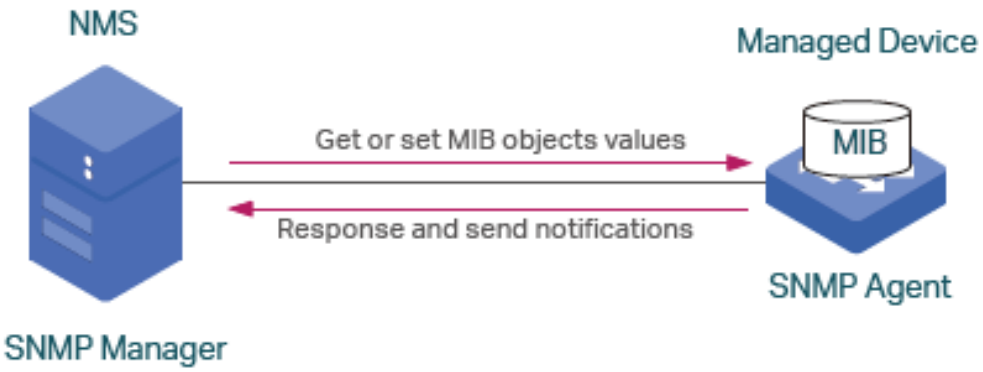
SNMP & RMON

SNMP

Visão Geral

O SNMP (Protocolo Simples de Gerenciamento de Rede) é um protocolo padrão de gerenciamento de rede, amplamente utilizado em redes TCP/IP. Facilita o gerenciamento de dispositivos usando o software NMS (Network Management System). Com o SNMP, os gerentes de rede podem visualizar ou modificar as informações do dispositivo de rede e solucionar problemas de acordo com as notificações enviadas por esses dispositivos em tempo hábil.

Como mostra a figura a seguir, o sistema SNMP consiste em um gerente SNMP, um agente SNMP e uma MIB (Management Information Base). O gerenciador de SNMP pode fazer parte de um NMS. O agente e o MIB residem no dispositivo gerenciado, como switch, roteador, host ou impressora. Para configurar o SNMP no switch, defina o relacionamento entre o gerente e o agente.



Conceitos Básico

Os seguintes conceitos básicos do SNMP serão introduzidos: Gerenciador SNMP, agente SNMP, MIB (Management Information Base), entidade SNMP, mecanismo SNMP e versão SNMP.

Gerenciador SNMP

O gerenciador SNMP usa o SNMP para monitorar e controlar agentes SNMP, fornecendo uma interface de gerenciamento amigável para o administrador gerenciar dispositivos de rede convenientemente. Ele pode obter valores de objetos MIB de um agente ou armazenar um valor de objeto MIB no agente. Além disso, ele recebe notificações dos agentes para conhecer as condições da rede.

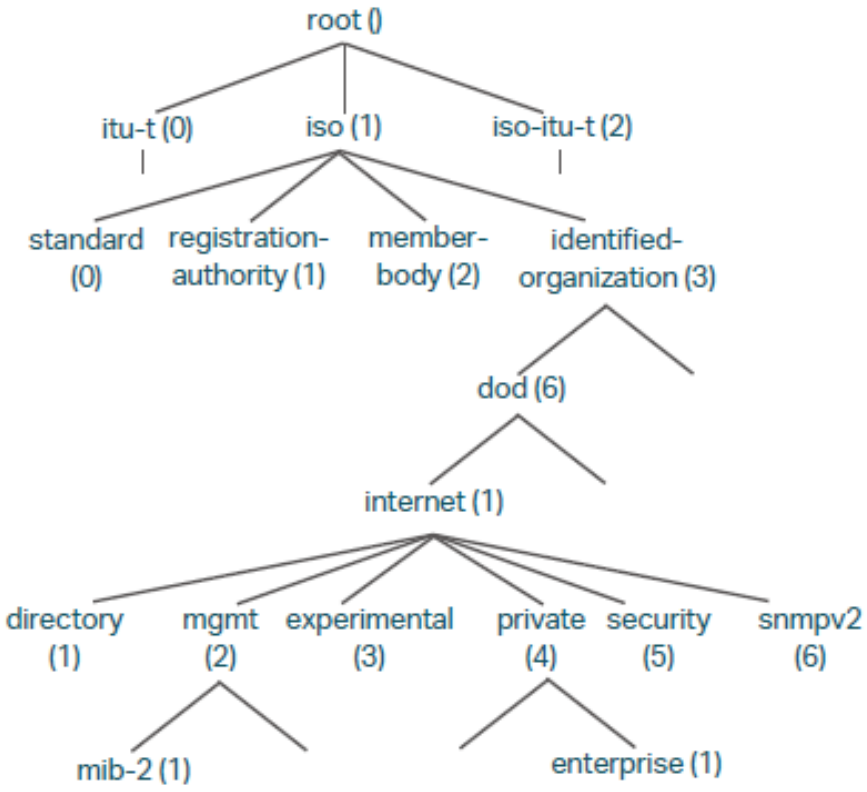
Agente SNMP

Um agente SNMP é um processo em execução no dispositivo gerenciado. Ele contém objetos MIB cujos valores podem ser solicitados ou alterados pelo gerenciador SNMP. Um agente pode enviar mensagens de interceptação não solicitadas para notificar o gerente SNMP de que ocorreu um evento significativo no agente.

MIB

Um MIB é uma coleção de objetos gerenciados organizados hierarquicamente. Os objetos definem os atributos do dispositivo gerenciado, incluindo os nomes, status, direitos de acesso e tipos de dados. Cada objeto pode ser endereçado através de um identificador de objeto (OID).

Como mostra a figura a seguir, a hierarquia do MIB pode ser descrita como uma árvore com uma raiz sem nome, cujos níveis são atribuídos por diferentes organizações. Os IDs de objeto MIB de nível superior pertencem a organizações de padrões diferentes, enquanto os IDs de objeto de nível inferior são alocados por organizações associadas. Os fornecedores podem definir ramificações particulares que incluem objetos gerenciados para seus próprios produtos.



O switch Intelbras suportam os seguintes MIBs públicos:

- LLDP.mib
- LLDP-Ext-Dot1.mib
- LLDP-Ext-MED.mib
- RFC1213.mib
- RFC1493-Bridge.mib
- RFC1757-RMON.mib
- RFC2618-RADIUS-Auth-Client.mib
- RFC2620-RADIUS-Acc-Client.mib
- RFC2674-pBridge.mib
- RFC2674-qBridge.mib
- RFC2863-pBridge.mib
- RFC2925-Disman-Ping.mib
- RFC2925-Disman-Traceroute.mib

Entidade SNMP

Uma entidade SNMP é um dispositivo executando o protocolo SNMP. O gerente e o agente SNMP são entidades SNMP.

Mecanismo SNMP

Um mecanismo SNMP faz parte da entidade SNMP. Toda entidade SNMP possui um e apenas um mecanismo. Um mecanismo SNMP fornece serviços para finalizar e receber mensagens, autenticar e criptografar mensagens e controlar o acesso a objetos gerenciados. Um mecanismo SNMP pode ser identificado exclusivamente por um ID de

mecanismo em um domínio administrativo. Como existe uma associação individual entre os mecanismos SNMP e as entidades SNMP, também podemos usar o ID do mecanismo para identificar de forma única e inequívoca a entidade SNMP nesse domínio administrativo.

Versão SNMP

O dispositivo suporta três versões SNMP: SNMPv1, SNMPv2c e SNMPv3. A Tabela a seguir lista os recursos suportados por diferentes versões SNMP.

Recurso	SNMPv1	SNMPv2c	SNMPv3
Controle de Acesso	Baseado na Comunidade SNMP e na MIB View	Baseado na Comunidade SNMP e na MIB View	Baseado no Usuário SNMP, Grupo e na MIB View
Autenticação e Privacidade	Baseado no nome da comunidade	Baseado no nome da comunidade	Os modos de autenticação e privacidade suportados são os seguintes: Autenticação: MD5/SHA Privacidade: DES
Trap	Suportado	Suportado	Suportado
Inform	Não suportado	Suportado	Suportado

Cenários de aplicação de diferentes versões.

Versão	Cenário de Aplicação
SNMPv1	Aplicável a redes de pequena escala ou redes simples, baixos requisitos de segurança ou boa estabilidade (como redes de campus e redes de pequenas empresas).
SNMPv2c	Aplicável a redes de média e grande escala com baixos requisitos de segurança e com boa segurança (como VPNs), mas com serviços ocupados nos quais o congestionamento do tráfego pode ocorrer. Você pode configurar o Inform para garantir que as notificações dos dispositivos gerenciados sejam recebidas pelos gerentes de rede.
SNMPv3	Aplicável a redes de várias escalas, principalmente aquelas que possuem altos requisitos de segurança e exigem que os dispositivos sejam gerenciados por administradores autenticados (como quando os dados precisam ser transferidos em redes públicas).

Configuração SNMP

Para concluir a configuração do SNMP, escolha uma versão do SNMP de acordo com os requisitos de rede e a capacidade de suporte do software NMS e siga estas etapas:

- **Escolha SNMPv1 ou SNMPv2c**

1. Habilite o SNMP.
2. Crie uma view SNMP para os objetos gerenciados.

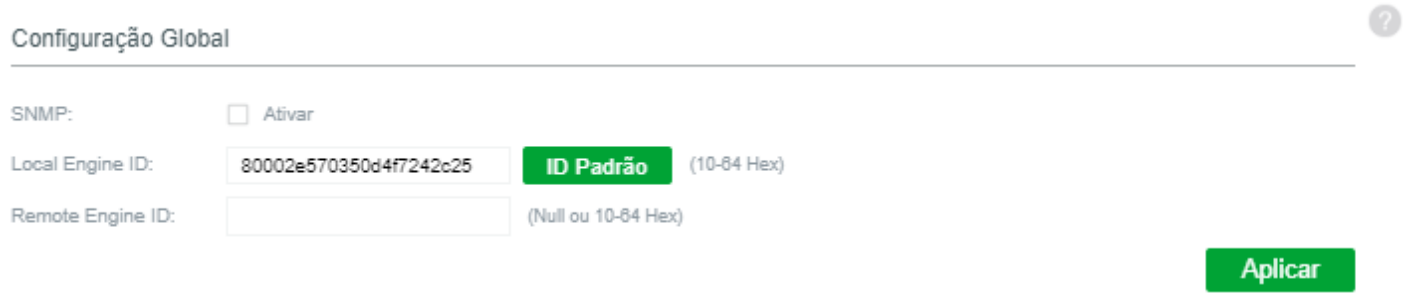
3. Crie uma comunidade, especifique a visualização acessível e os direitos de acesso correspondentes.

- **Escolha SNMPv3**

1. Habilite o SNMP.
2. Crie uma view SNMP para os objetos gerenciados.
3. Crie um grupo SNMP e especifique os direitos de acesso.
4. Crie usuários SNMP e configure o modo de autenticação, modo de privacidade e senhas correspondentes.

Habilitando o SNMP

Escolha **MANUTENÇÃO > SNMP > Configuração Global** para carregar a página a seguir.



Siga os seguintes passos para configurar o SNMP globalmente:

1. Na seção **Configuração Global**, ative o SNMP e configure Local Engine ID e Remote Engine ID. Criando assim uma Visualização SNMP.

SNMP	Ativa o desativa o SNMP globalmente.
Local Engine ID	Defina o ID do mecanismo do agente SNMP local (o switch) com 10 a 64 dígitos hexadecimais. Por padrão, o switch gera o ID do mecanismo usando seu próprio endereço MAC. O ID do mecanismo local é uma sequência alfanumérica exclusiva usada para identificar o mecanismo SNMP. Como um agente SNMP contém apenas um mecanismo SNMP, o ID do mecanismo local pode identificar exclusivamente o agente SNMP.
Remote Engine ID	Defina o ID do gerenciador SNMP remoto com 10 a 64 dígitos hexadecimais. Se nenhum gerenciador SNMP remoto for necessário, você poderá deixar esse campo em branco. O ID do mecanismo remoto é uma sequência alfanumérica exclusiva. É usado para identificar o mecanismo SNMP no dispositivo remoto que recebe mensagens de informações do Switch.

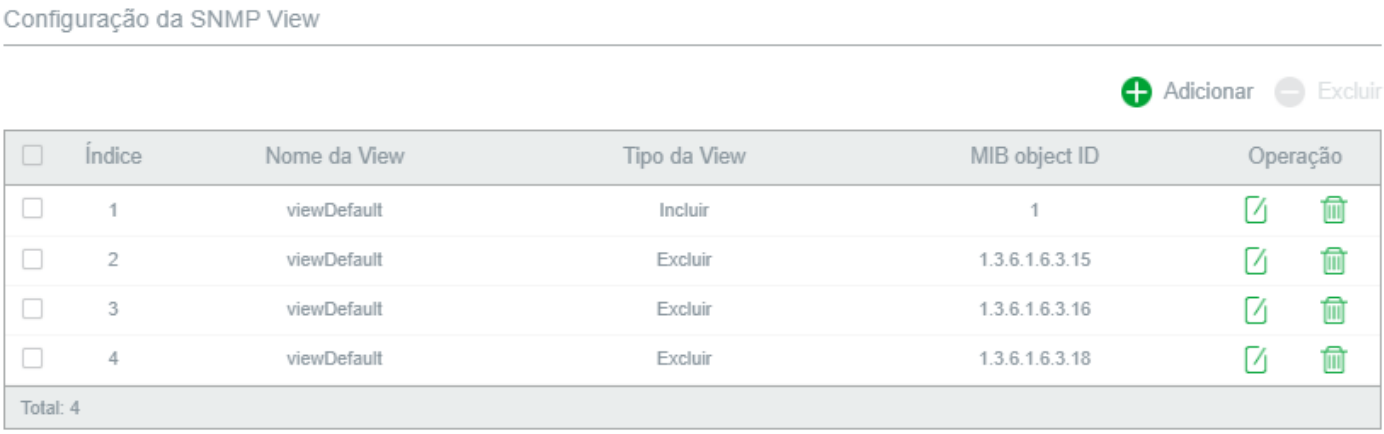
2. Clique em **Aplicar**.

O ID do mecanismo deve conter um número par de caracteres.

Alterar o valor do ID do mecanismo SNMP tem efeitos colaterais importantes. No SNMPv3, a senha de um usuário é convertida em um resumo de segurança MD5 ou SHA com base na senha e no ID do mecanismo. Se o valor do ID do mecanismo local for alterado, o switch excluirá automaticamente todos os usuários locais do SNMPv3 à medida que seus resumos de segurança se tornarem inválidos. Da mesma forma, todos os usuários remotos do SNMPv3 serão excluídos se o valor do ID do mecanismo remoto for alterado.

Criando uma SNMP View

Escolha **MANUTENÇÃO > SNMP > Configuração Global** para carregar a página a seguir.



O NMS gerencia objetos MIB com base na exibição SNMP. Uma SNMP View é um subconjunto de uma MIB. O sistema fornece uma visualização padrão chamada viewDefault, e você pode criar outras SNMP View de acordo com suas necessidades.

1. Clique em Adicionar para carregar a página seguinte. Digite o Nome da View, especifique o Tipo da View e um MIB object ID que esteja relacionado à exibição.

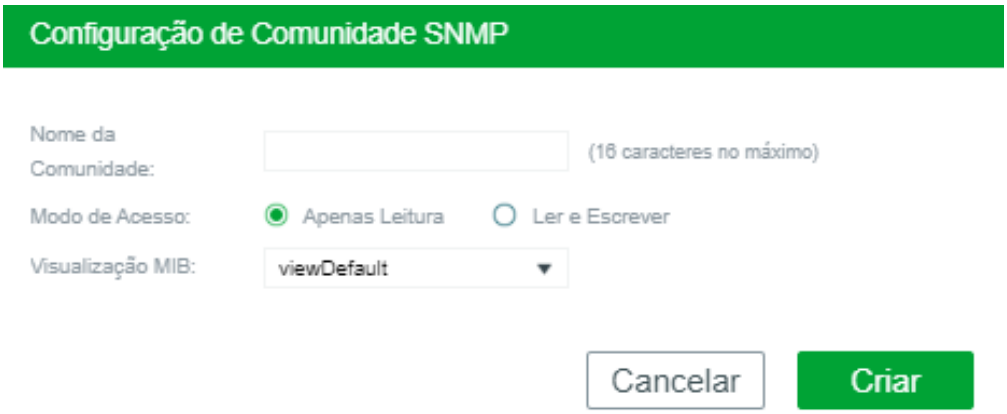
Nome da View	Defina o nome da exibição com 1 a 16 caracteres. Uma visualização completa consiste em todos os objetos MIB que possuem o mesmo nome de visualização.

Tipo da View	Defina a visualização para incluir ou excluir o objeto MIB relacionado. Por padrão, é incluir. **Incluir:** o NMS pode exibir ou gerenciar a função indicada pelo objeto. **Excluir:** o NMS não pode exibir ou gerenciar a função indicada pelo objeto.
MIB object ID	Digite um ID de objeto MIB para especificar uma função específica do dispositivo. Quando um ID de objeto MIB é especificado, todos os seus IDs de objeto filho são especificados. Para regras de identificação específicas, consulte as MIBs relacionadas ao dispositivo.

2. Clique em **Criar**.

Ciando Comunidades SNMP (SNMP v1/v2c)

Escolha **MANUTENÇÃO > SNMP > SNMP v1/v2c** e clique em Adicionar para carregar a página a seguir.



1. Defina o nome da comunidade, modo de acesso e visualização MIB.

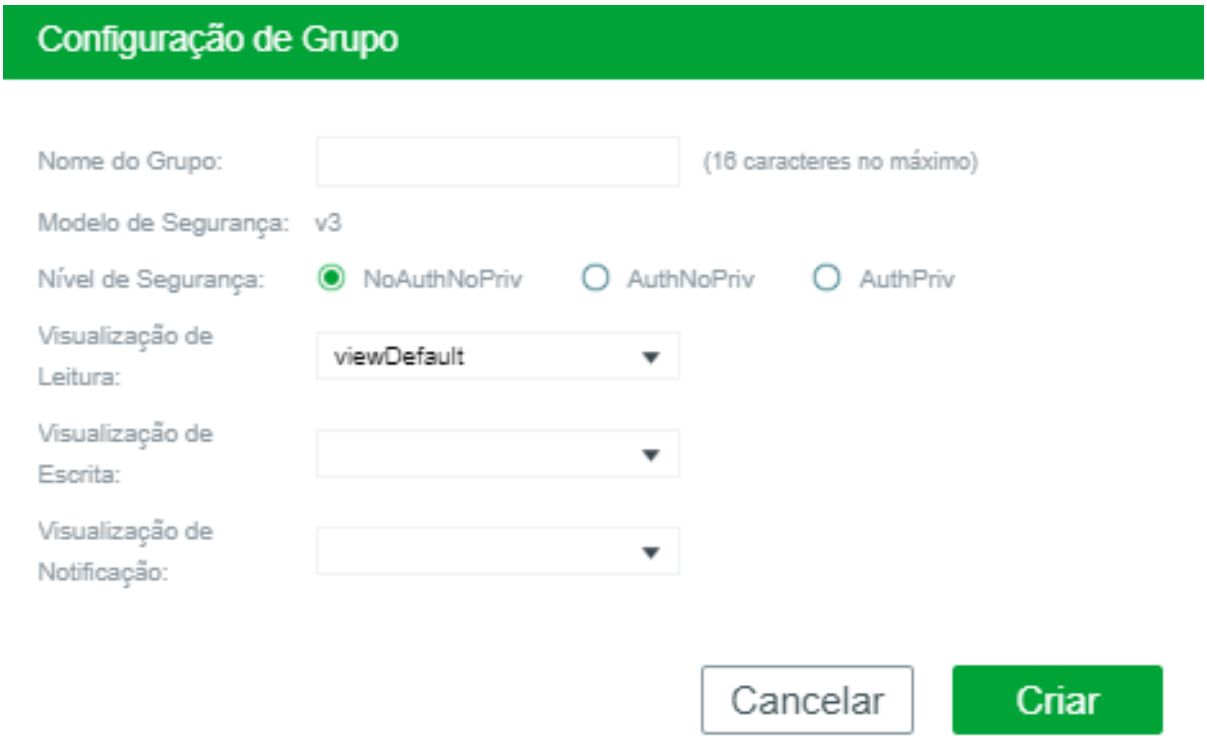
Nome da Comunidade	Configure o nome da comunidade. Esse nome de comunidade é usado como uma senha para conceder ao NMS acesso a objetos MIB no agente SNMP do switch.
Modo de Acesso	Especifique o direito de acesso à visualização relacionada. O padrão é Apenas Leitura. **Apenas Leitura:** o NMS pode visualizar, mas não pode modificar parâmetros da exibição especificada. **Ler e Escrever:** o NMS pode exibir e modificar parâmetros da exibição especificada.
Visualização MIB	Escolha uma visualização SNMP que permita o acesso da comunidade. A visualização padrão é viewDefault.

2. Clique em **Criar**.

Criando um Grupo SNMPv3

Crie um grupo SNMP e configure parâmetros relacionados.

Escolha **MANUTENÇÃO > SNMP > SNMP v3 > Grupo SNMP** e clique em Adicionar para carregar a página a seguir.



Siga estas etapas para criar um grupo SNMP:

1. Atribua um nome ao grupo, defina o nível de segurança e a visualização de leitura, gravação e notificação.

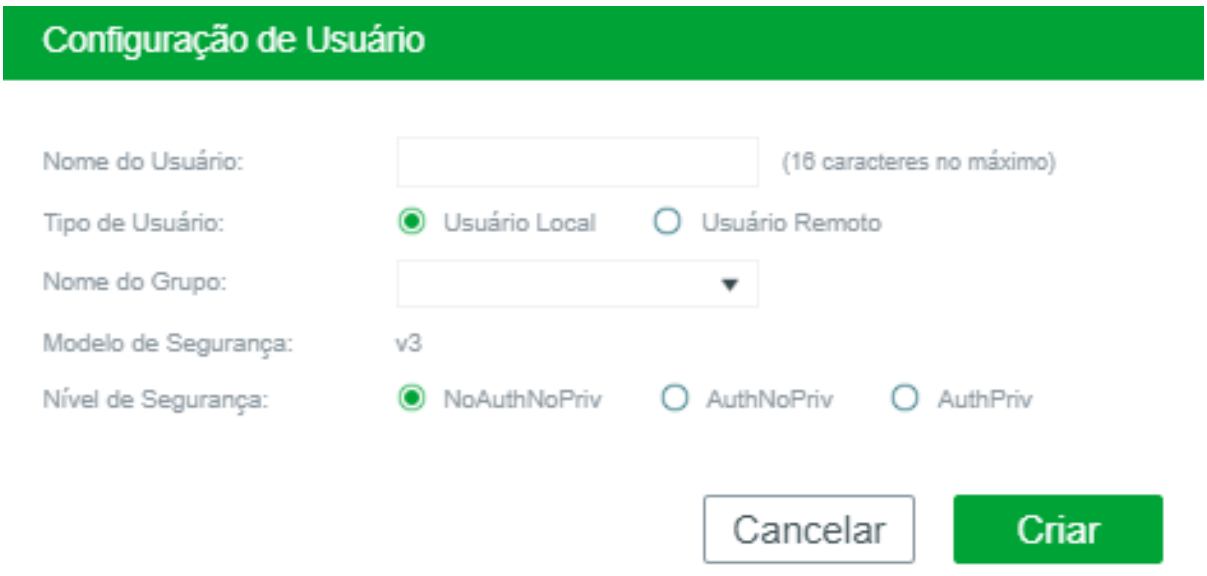
Nome do Grupo	Defina o nome do grupo SNMP. Você pode inserir 1 a 16 caracteres. O identificador de um grupo consiste em um nome de grupo, modelo de segurança e nível de segurança. Grupos do mesmo identificador são reconhecidos como estando no mesmo grupo.
Modelo de Segurança	Exibe o modelo de segurança. O SNMPv3 usa a v3, o modelo mais seguro.

Nível de Segurança	Defina o nível de segurança que para o grupo SNMPv3. O padrão é NoAuthNoPriv. **NoAuthNoPriv:** nenhum modo de autenticação ou privacidade é aplicado para verificar ou criptografar pacotes. **AuthNoPriv:** um modo de autenticação é aplicado para verificar pacotes, mas nenhum modo de privacidade é aplicado para criptografá-los. **AuthPriv:** um modo de autenticação e um modo de privacidade são aplicados para verificar e criptografar pacotes.
Visualização de Leitura	Escolha uma visualização para permitir que os parâmetros sejam visualizados, mas não modificados pelo NMS. A visualização é necessária para qualquer grupo. Por padrão, a visualização é viewDefault. Para modificar os parâmetros de uma exibição, você precisa adicioná-lo à Exibição de gravação.
Visualização de Escrita	Escolha uma visualização para permitir que os parâmetros sejam modificados, mas não visualizados pelo NMS. O padrão é nenhum. A exibição na Exibição de gravação também deve ser adicionada à Exibição de leitura.
Visualização de Notificação	Escolha uma exibição para permitir o envio de notificações ao NMS.

2. Clique em **Criar**.

Criando um Usuário SNMPv3

Escolha **MANUTENÇÃO > SNMP > SNMP v3 > Usuário SNMP** e clique em Adicionar para carregar a página a seguir.



Siga estas etapas para criar um usuário SNMP:

1. Especifique o nome do usuário, tipo de usuário e o grupo ao qual o usuário pertence. Em seguida, configure o nível de segurança.

Nome do Usuário	Defina o nome do usuário SNMP. Você pode usar de 1 a 16 caracteres. Para entradas diferentes, os nomes de usuário não podem ser os mesmos.
Tipo de Usuário	Escolha um tipo de usuário para indicar a localização do usuário. O padrão é Usuário Local. **Usuário Local:** o usuário reside no mecanismo local, que é o agente SNMP do switch. **Usuário Remoto:** o usuário reside no NMS. Como o ID do mecanismo remoto e a senha do usuário são usados para calcular os resumos de autenticação e privacidade, antes de configurar um usuário remoto, é necessário definir o ID do mecanismo remoto primeiro.
Nome do Grupo	Escolha o grupo ao qual o usuário pertence. Usuários com o mesmo nome de grupo, modelo de segurança e nível de segurança estarão no mesmo grupo.
Modelo de Segurança	Exibe o modelo de segurança. O SNMPv3 usa a v3, o modelo mais seguro.
Nível de Segurança	Defina o nível de segurança. O nível de segurança do mais alto para o mais baixo é: NoAuthNoPriv, AuthNoPriv, AuthPriv e o padrão é NoAuthNoPriv. O nível de segurança do usuário não deve ser inferior ao grupo ao qual ele pertence. **NoAuthNoPriv:** usa uma correspondência de nome de usuário para autenticação e nenhuma criptografia é implementada. **AuthNoPriv:** um modo de autenticação é aplicado para verificar pacotes, mas nenhum modo de privacidade é aplicado para criptografá-los. **AuthPriv:** um modo de autenticação e um modo de privacidade são aplicados para verificar e criptografar pacotes.

2. Se você escolheu **AuthNoPriv** ou **AuthPriv** como o nível de segurança, precisará definir o Modo de autenticação ou o Modo de privacidade correspondente. Caso contrário, pule a etapa.

Modo de Autenticação	Com AuthNoPriv ou AuthPriv selecionado, configure o modo de autenticação e a senha. São fornecidos dois modos de autenticação: **MD5:** ative o algoritmo HMAC-MD5 para autenticação. **SHA:** ative o algoritmo SHA (Secure Hash Algorithm) para autenticação. O algoritmo SHA é mais seguro que o MD5.

Senha de Autenticação	Defina a senha para autenticação.
Modo de Privacidade	Com AuthPriv selecionado, configure o modo de privacidade e a senha para criptografia. O switch usa o algoritmo DES (Data Encryption Standard) para criptografia.
Senha de Privacidade	Defina a senha para criptografia.

3. Clique em **Criar**.

Configuração de Notificações

Com a Notificação ativada, o switch pode enviar notificações ao NMS sobre eventos importantes relacionados à operação do dispositivo. Isso facilita o monitoramento e o gerenciamento do NMS.

Para configurar a notificação SNMP, siga estas etapas:

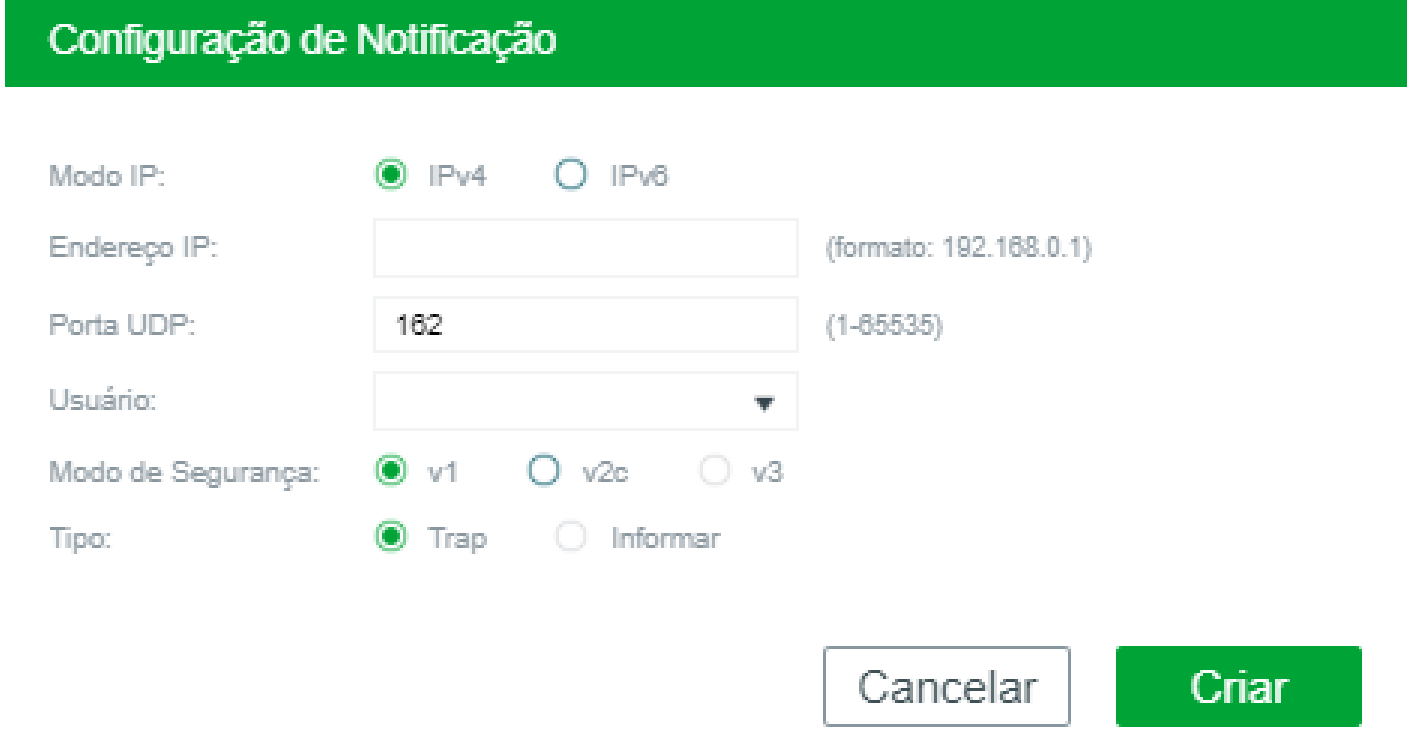
1. Configure as informações dos hosts NMS.
2. Habilite traps SNMP.

Diretrizes de configuração

Para garantir a comunicação entre o switch e o NMS, verifique se o switch e o NMS conseguem se conectar.

Configurando a Informação dos Hosts NMS

Escolha **MANUTENÇÃO > SNMP > Notificação > Configuração de Notificação** e clique em Adicionar para carregar a página a seguir.



Siga estas etapas para adicionar um host NMS:

1. Escolha o modo IP de acordo com o ambiente de rede e especifique o endereço IP do host NMS e a porta UDP que recebe notificações.

Modo IP	Escolha um modo IP para o host NMS.
Endereço IP	Se você definir o Modo IP como IPv4, especifique um endereço IPv4 para o host do NMS. Se você definir o Modo IP como IPv6, especifique um endereço IPv6 para o host do NMS.
Porta UDP	Especifique uma porta UDP no host NMS para receber notificações. O padrão é a porta 162. Para segurança da comunicação, recomendamos que você altere o número da porta sob a condição de que as comunicações em outras portas UDP não sejam afetadas.

2. Especifique o nome do usuário ou o nome da comunidade usado pelo host do NMS e configure o modelo e o nível de segurança com base nas configurações do usuário ou da comunidade.

Usuário	Escolha o nome de usuário ou o nome da comunidade usado pelo host do NMS.

Modo de Segurança	Se um nome de comunidade (criado para SNMPv1 / v2c) for inserido em Nome do Usuário, especifique o modo de segurança como v1 ou v2c. Se um nome de usuário (criado para SNMPv3) for inserido em Nome do Usuário, aqui será exibido o modo de segurança como v3. O host do NMS deve usar a versão SNMP correspondente.
Nível de Segurança	Se o Nível de segurança for v3, exibe o nível de segurança do usuário.

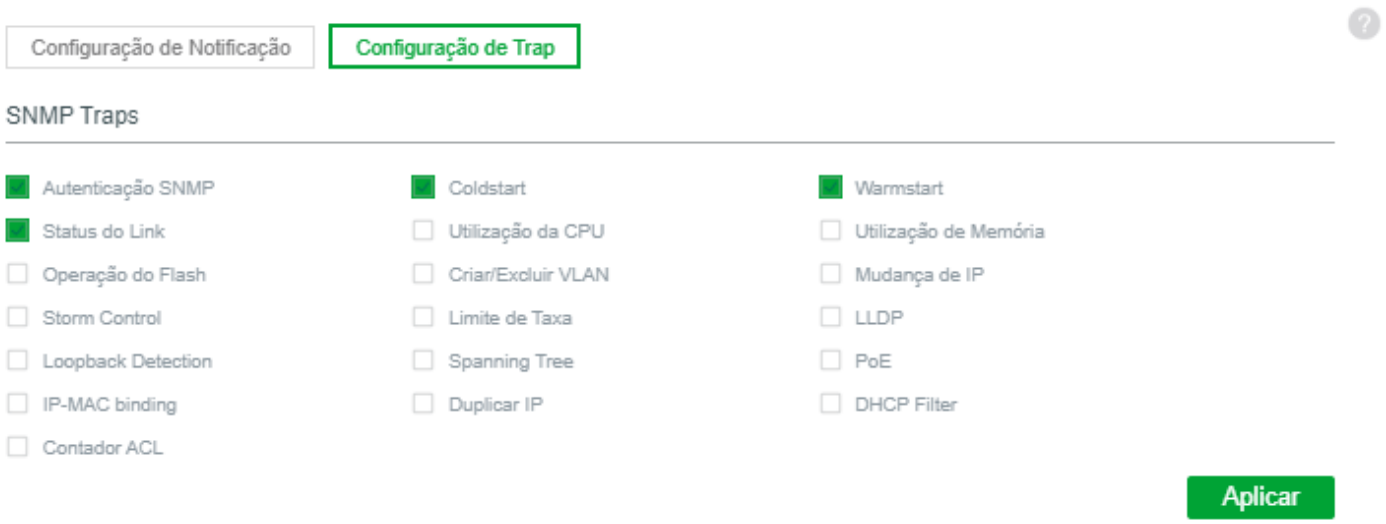
3. Escolha um tipo de notificação com base na versão SNMP. Se você escolher o tipo Informar, precisará definir o número de tentativas e o tempo limite.

Tipo	Escolha um tipo de notificação para o host do NMS. Para SNMPv1, o tipo suportado é trap. Para SNMPv2c e SNMPv3, você pode configurar o tipo como trap ou informar. **Trap:** o switch envia mensagens de trap ao host do NMS quando certos eventos ocorrem. Quando o host NMS recebe uma mensagem de trap, ele não envia uma resposta ao switch. Portanto, o switch não pode dizer se uma mensagem é recebida ou não, e as mensagens que não são recebidas não serão reenviadas. **Informar:** o switch enviará mensagens de Informar ao host do NMS quando certos eventos ocorrerem. Quando o host NMS recebe uma mensagem Inform, ele envia uma resposta ao switch. Se o switch não receber uma resposta dentro do intervalo de tempo limite, reenviará a mensagem Informar. Portanto, o Informar é mais confiável que os Traps.
Número de Tentativas	Defina os tempos de nova tentativa para o Informar. O switch reenviará a mensagem Informar se não receber resposta do host NMS dentro do intervalo de tempo limite. Ele irá parar de enviar mensagens de Informe quando o tempo de nova tentativa atingir o limite.
Timeout	Defina o tempo que o switch aguarda uma resposta do host NMS após o envio de uma mensagem informativa.

4. Clique em **Criar**.

Habilitando SNMP Traps

Escolha o menu **MANUTENÇÃO > SNMP > Notificação > Configuração de Trap** para carregar a página a seguir.



As traps suportadas estão listadas na página. Siga estas etapas para ativar um ou todos esses traps:

1. Selecione as traps para serem ativadas de acordo com suas necessidades.

Autenticação SNMPw	Disparado quando uma solicitação SNMP recebida falha na autenticação.
Coldstart	Indica uma inicialização SNMP causada pela reinicialização do sistema do switch. A trap pode ser disparada quando você reiniciar o switch.
Warmstart	Indica que o recurso SNMP no switch é reinicializado com a configuração física inalterada. A trap pode ser disparada se você desativar e ativar o SNMP depois que o SNMP estiver completamente configurado e ativado.
Status do Link	Disparado quando o switch detecta uma alteração no status do link.
Utilização da CPU	Disparado quando a taxa de utilização da CPU exceder o limite que você definiu. O limite da taxa de utilização da CPU para o switch é de 80% por padrão.
Utilização da Memória	Disparado quando a utilização da memória exceder 80%.
Operação do Flash	Disparado quando o flash é modificado durante operações como backup, redefinição, atualização de firmware, importação de configuração e assim por diante.
Criar/Excluir VLAN	Disparado quando VLANs são criadas ou excluídas com sucesso.
Mudança de IP	Monitora as alterações de endereço IP de cada interface. A trap pode ser disparada quando o endereço IP de qualquer interface for alterado.
Storm Control	Monitora se a taxa de Storm Control atingiu o limite que você definiu. A trap pode ser disparada quando o recurso está ativado e os quadros de broadcast/multicast/unicast desconhecido são enviados para a porta com uma taxa maior que a que você definiu.

Limite de Taxa	Monitora se a largura de banda atingiu o limite que você definiu. A trap pode ser disparada quando o recurso Limite de taxa estiver ativado e os pacotes forem enviados para a porta com uma taxa maior que a que você definiu.
LLDP	Indica alterações na topologia do LLDP. A trap pode ser disparada quando um novo dispositivo remoto conectado a uma porta local ou um dispositivo remoto desconectado ou movido de uma porta para outra.
Loopback Detection	Disparado quando o switch detecta um loopback com o recurso de Loopback Detection, ou quando um loopback é desfeito.
Spanning Tree	Indica mudanças no spanning tree. A trap pode ser disparada nas seguintes situações: uma porta muda do estado de não encaminhamento para o estado de encaminhamento ou vice-versa; uma porta recebe um pacote com sinalizador TC ou um pacote TCN.
PoE	Somente para produtos compatíveis com o recurso PoE. Permita todos os traps relacionados ao PoE, incluindo: **Over-max-pwr-budget:** disparado quando a energia total exigida pelos PDs conectados excede a energia máxima que o switch PoE pode fornecer. **Port-pwr-change:** disparado quando uma porta começa a fornecer energia ou para de fornecer energia. **Port-pwr-deny:** disparado quando o switch desliga PDs em portas PoE de baixa prioridade. Quando a energia total exigida pelos PDs conectados exceder o limite de energia do sistema, o switch desligará os PDs nas portas PoE de baixa prioridade para garantir o funcionamento estável dos outros PDs. **Port-pwr-over-30w:** disparado quando a energia requerida pelo PD conectado excede 30 watts. **Port-pwr-overload:** disparado quando a energia requerida pelo PD conectado excede a energia máxima que a porta pode fornecer. **Port-short-circuit:** acionado quando um curto-circuito é detectado em uma porta. **Thermal-shutdown:** disparado quando o chip PSE superaquece. O switch irá parar de fornecer energia neste caso.
IP-MAC binding	Disparado nas duas situações a seguir: o recurso ARP Inspection está ativado e o switch recebe um pacote ARP ilegal; ou o recurso IPv4 Source Guard está ativado e o switch recebe um pacote IP ilegal.
Duplicar IP	Disparado quando o switch detecta um evento de conflito de IP.

DHCP Filter	Disparado quando o recurso de filtro DHCPv4 está ativado e o switch recebe pacotes DHCP de um servidor DHCP ilegal.
Contador ACL	Monitora as informações da ACL correspondentes, incluindo o ID da ACL correspondente, o ID da regra e o número dos pacotes correspondentes. Com esse trap e o recurso Logging nas configurações de regra da ACL ativados, o switch verifica as informações correspondentes da ACL a cada cinco minutos e envia traps SNMP se houver alguma informação atualizada.

2. Clique em **Aplicar**.

RMON

O RMON (Monitoramento Remoto de Rede), juntamente com o sistema SNMP, permite ao gerente da rede monitorar dispositivos de rede remota com eficiência. O RMON reduz o fluxo de tráfego entre o NMS e os dispositivos gerenciados, o que é conveniente para o gerenciamento em grandes redes.

O RMON inclui duas partes: o NMS e os agentes em execução em todos os dispositivos de rede. O NMS geralmente é um host que executa o software de gerenciamento para gerenciar agentes de dispositivos de rede. E o agente geralmente é um switch ou roteador que coleta estatísticas de tráfego (como o total de pacotes em um segmento de rede durante um determinado período de tempo ou o total de pacotes corretos enviados a um host). Com base no protocolo SNMP, o NMS coleta dados de rede através da comunicação com agentes. No entanto, o NMS não pode obter todos os dados do RMON MIB devido aos recursos limitados do dispositivo. Geralmente, o NMS pode obter apenas informações dos quatro grupos a seguir: Estatísticas, Histórico, Evento e Alarme.

- **Estatísticas:** coleta estatísticas de Ethernet (como o total de bytes recebidos, o total de pacotes de transmissão e o total de pacotes do tamanho especificado) em uma interface.
- **Histórico:** coleta um grupo de estatísticas das portas Ethernet para um intervalo de pesquisa especificado.
- **Evento:** especifica a ação a ser tomada quando um evento é acionado por um alarme. A ação pode ser para gerar uma entrada de log ou uma interceptação SNMP.
- **Alarme:** monitora um objeto MIB específico por um intervalo especificado, dispara um evento em um valor especificado (limite crescente ou limite decrescente).

Configuração RMON

Com as configurações do RMON, você pode:

- Configurando o grupo Estatísticas.
- Configurando o grupo Histórico.
- Configurando o grupo Evento.

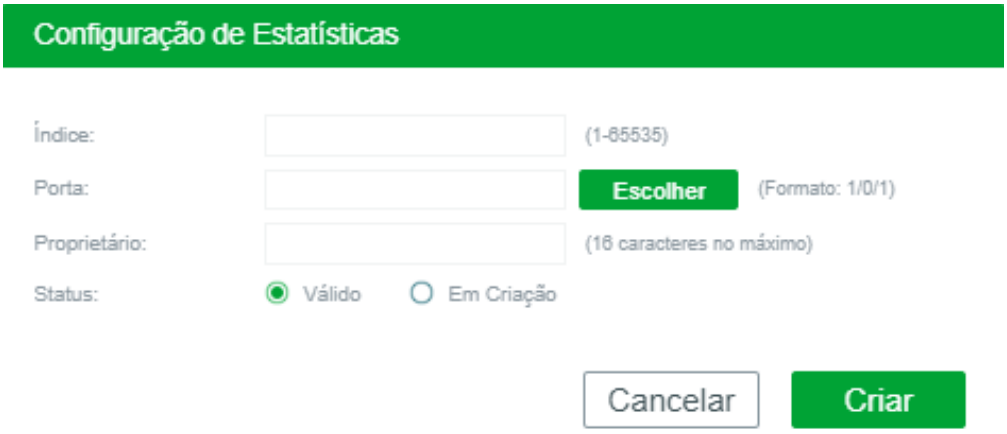
- Configurando o grupo Alarme.

Diretrizes de configuração

Para garantir que o NMS receba notificações normalmente, conclua as configurações do SNMP e do SNMP Notification antes das configurações do RMON.

Configurando Grupo de Estatísticas

Escolha o menu **MANUTENÇÃO > SNMP > RMON > Estatísticas** e clique em Adicionar para carregar a seguinte página.



Siga estas etapas para configurar o grupo Estatísticas:

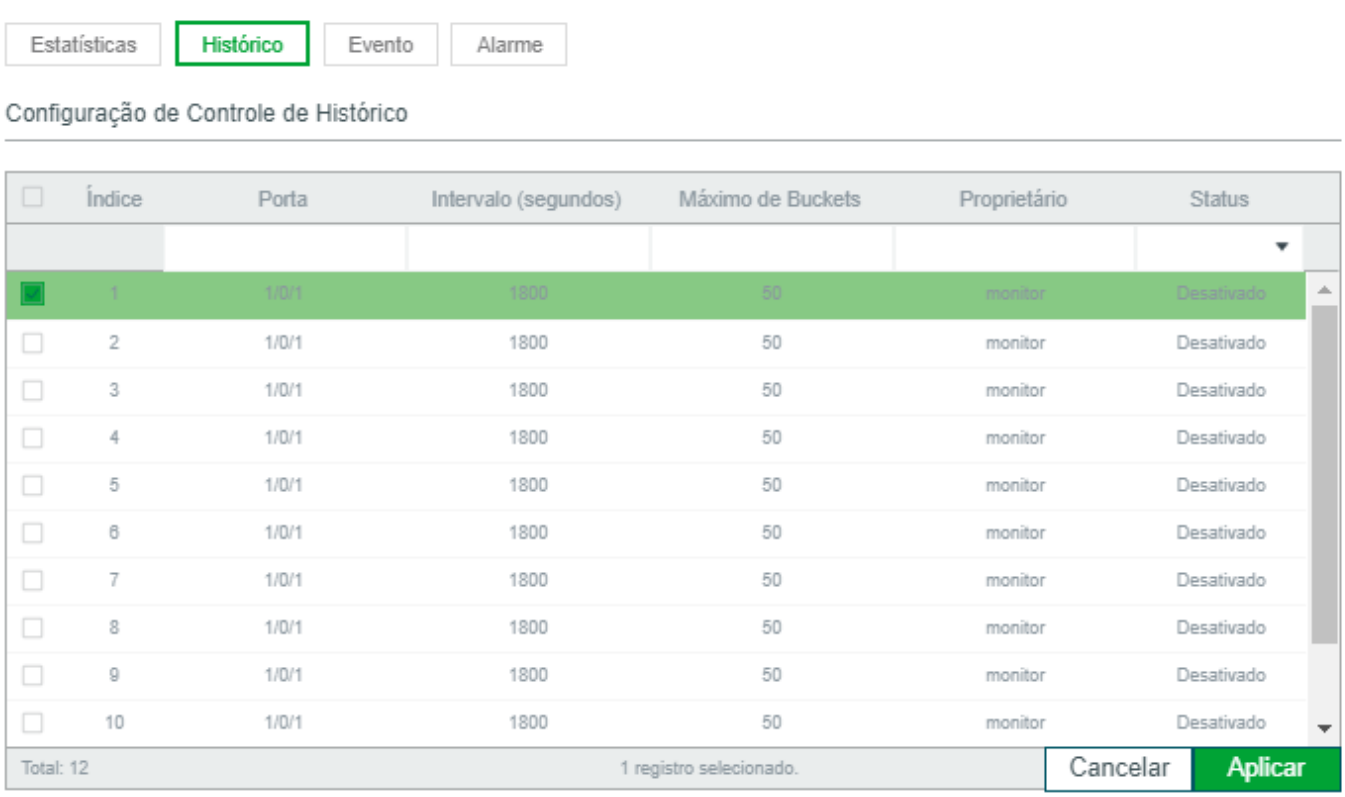
1. Especifique o índice da entrada, a porta a ser monitorada e o nome do proprietário da entrada.

Índice	Digite o índice da entrada.
Porta	Clique em Escolher para especificar uma porta Ethernet a ser monitorada na entrada ou digite o número da porta no formato 1/0/1.
Proprietário	Digite o nome do proprietário da entrada com 1 a 16 caracteres.
Status	Defina a entrada como Válida ou Em criação. Por padrão, é válido. O switch começa a coletar estatísticas de Ethernet para uma entrada Estatísticas, pois o status da entrada é configurado como válido. **Válido:** a entrada é criada e válida. **Em criação:** a entrada é criada, mas inválida.

2. Clique em **Criar**.

Configurando Grupo Histórico

Escolha o menu **MANUTENÇÃO > SNMP > RMON > Histórico** para carregar a seguinte página.



Siga estas etapas para configurar o grupo Histórico:

1. Selecione uma entrada Histórico e especifique uma porta a ser monitorada.

Índice	Exibe o índice de entradas do histórico. O switch suporta até 12 entradas de histórico.
Porta	Especifique uma porta no formato 1/0/1 a ser monitorada.

2. Defina o intervalo de amostra e os intervalos máximos de entradas do histórico.

Intervalo (segundos)	Especifique o número de segundos em cada ciclo de pesquisa. Os valores válidos são de 10 a 3600 segundos e o padrão é 1800 segundos. Cada entrada no histórico possui seu próprio cronômetro. Para a porta monitorada, o switch coleta informações de pacotes e gera um registro a cada intervalo.
Máximo de Buckets	Defina o número máximo de registros para a entrada Histórico. Quando o número de registros exceder o limite, o primeiro registro será substituído. Os valores válidos são de 10 a 130 e o padrão é 50.

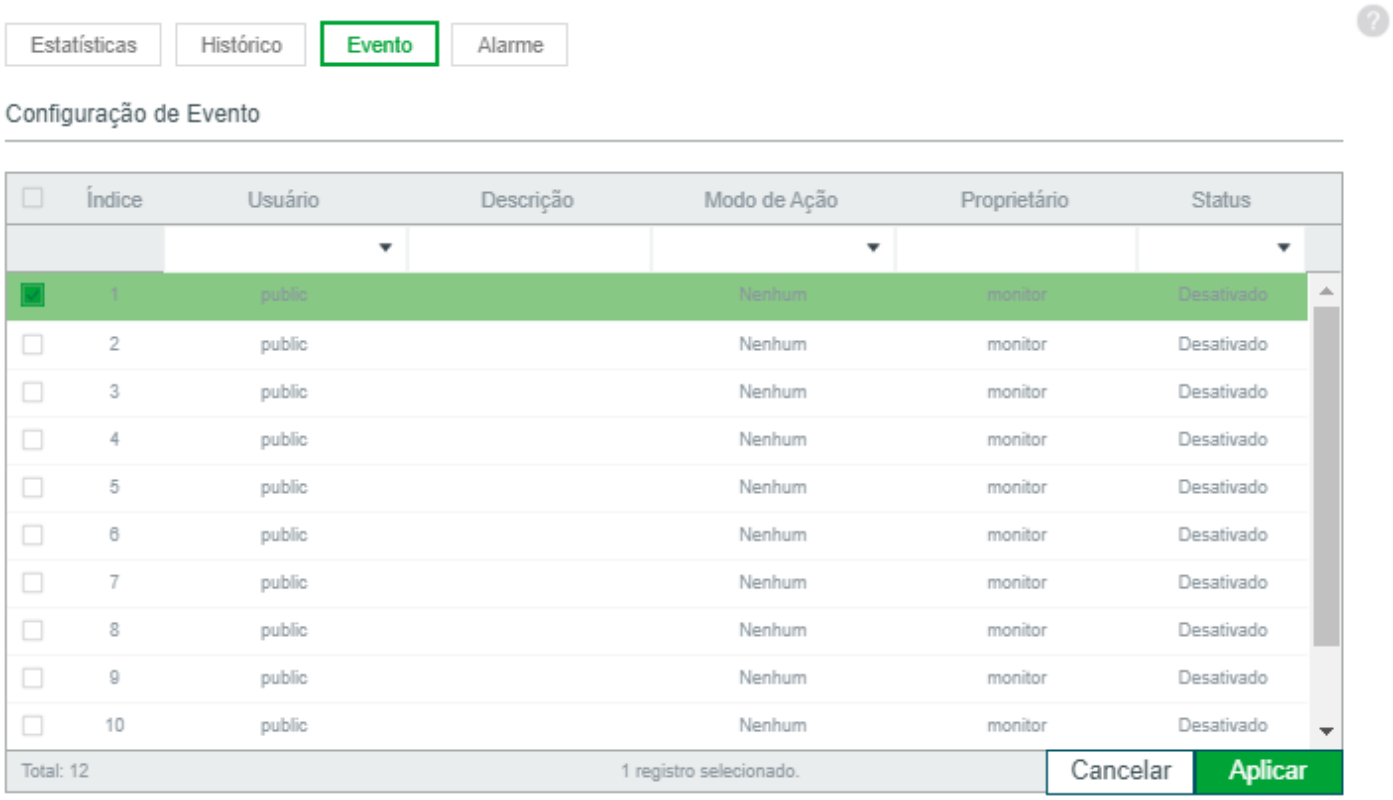
3. Digite o nome do proprietário e defina o status da entrada. Clique em **Aplicar**.

Proprietário	Digite o nome do proprietário da entrada com 1 a 16 caracteres. Por padrão, é monitor.
Status	Ative ou desative a entrada. Por padrão, está desativado. **Ativar:** a entrada está ativada. **Desativar:** a entrada está desativada.

Para alterar os parâmetros de uma entrada do histórico, ative a entrada ao mesmo tempo, caso contrário, a alteração não poderá entrar em vigor.

Configurando Grupo de Evento

Escolha o menu **MANUTENÇÃO > SNMP > RMON > Evento** para carregar a seguinte página.



Siga estas etapas para configurar o grupo Evento:

1. Escolha uma entrada de evento e defina o usuário SNMP da entrada.

Índice	Exibe o índice de entradas do histórico. O switch suporta até 12 entradas de histórico.
Usuário	Escolha um nome de usuário SNMP ou nome de comunidade para a entrada. O nome deve ser o mesmo que você definiu no SNMP anteriormente.

2. Defina a descrição e a ação a ser tomada quando o evento for acionado.

Descrição	Digite uma breve descrição desse evento para facilitar a identificação.
Modo de Ação	Especifique a ação a ser executada pela central quando o evento for acionado. **Nenhum:** nenhuma ação. É a configuração padrão. **Registrar:** o switch registra o evento no log e o NMS deve iniciar solicitações para obter notificações. **Notificar:** o switch inicia notificações para o NMS. **Registrar e Notificar:** o switch registra o evento no log e envia notificações para o NMS.

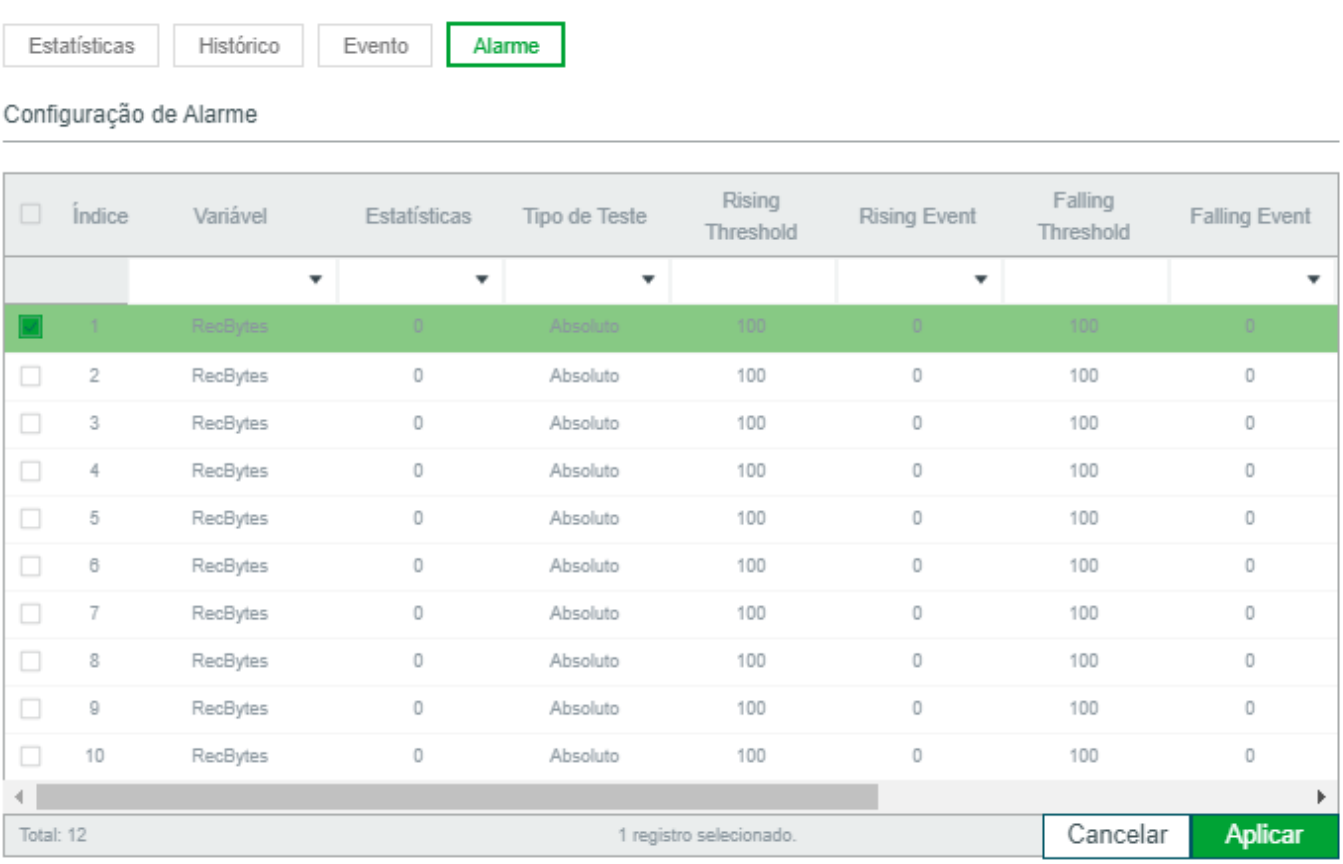
3. Digite o nome do proprietário e defina o status da entrada. Clique em **Aplicar**.

Proprietário	Digite o nome do proprietário da entrada com 1 a 16 caracteres. Por padrão, é monitor.
Status	Ative ou desative a entrada. Por padrão, está desativado. **Ativar:** a entrada está ativada. **Desativar:** a entrada está desativada.

Configurando Grupo de Alarme

Antes de começar, conclua as configurações das entradas Estatísticas e entradas de Eventos, porque as entradas de Alarme devem estar associadas às entradas de Estatísticas e Eventos.

Escolha o menu **MANUTENÇÃO > SNMP > RMON > Alarme** para carregar a seguinte página.



Siga estas etapas para configurar o grupo Alarme:

1. Selecione uma entrada de alarme, escolha uma variável a ser monitorada e associe a entrada a uma entrada de estatísticas.

Índice	Exibe o índice de entradas de Alarme. O switch suporta até 12 entradas de Alarme.

Variável	Defina a variável de alarme a ser monitorada. O switch monitorará a variável especificada em intervalos de amostra e atuará da maneira definida quando o alarme for acionado. A variável padrão é RecBytes. **RecBytes:** total de bytes recebidos. **RecPackets:** total de pacotes recebidos. **BPackets:** total de pacotes broadcast. **MPackets:** total de pacotes multicast. **CRC & Align ERR:** pacotes que variam de 64 a 1518 bytes e contêm Erro FCS ou erro de alinhamento. **Menores:** pacotes menores que 64 bytes. **Maiores:** pacotes maiores que 1518 bytes. **Jabbers:** pacotes enviados quando ocorrem colisões de portas. **Colisões:** tempos de colisão no segmento de rede. **64, 65-127, 128-255, 256-511, 512-1023, 1024-10240:** total de pacotes do tamanho especificado.
Estatísticas	Associe a entrada Alarme a uma entrada Estatísticas. Em seguida, o switch monitora a variável especificada da entrada Estatísticas.

2. Defina o tipo de amostra, o limite crescente e decrescente, o modo de ação do evento correspondente e o tipo de alarme da entrada.

Tipo de Teste	Defina o método de amostragem da variável especificada; o padrão é absoluto. **Absoluto:** compare o valor da amostra com o limite predefinido. **Delta:** o switch obtém a diferença entre os valores de amostragem do intervalo atual e o intervalo anterior e compara a diferença com o limite predefinido.
Rising Threshold	Defina o limite crescente da variável. Quando o valor amostrado excede o limite, o sistema aciona o Rising Event correspondente. Os valores válidos são de 1 a 2147483647 e o padrão é 100..
Rising Event	Especifique o índice da entrada de Evento que será acionada quando o valor amostrado exceder o limite threshold. A entrada de evento especificada aqui deve ser ativada primeiro.

Falling Threshold	Defina o limite de queda da variável. Quando o valor amostrado estiver abaixo do limite, o sistema acionará o Falling Event correspondente. Os valores válidos são de 1 a 2147483647 e o padrão é 100.
Falling Event	Especifique o índice da entrada de Evento que será acionada quando o valor amostrado estiver abaixo do limite Threshold. A entrada de evento especificada aqui deve ser ativada primeiro.
Tipo do Alarme	Especifique o tipo de alarme para a entrada. Por padrão, o tipo de alarme é All. **Rising:**o alarme é acionado apenas quando o valor amostrado excede o limite crescente. **Falling:** o alarme é acionado apenas quando o valor amostrado estiver abaixo do limite de queda. **All:** o alarme é acionado quando o valor amostrado excede o limite crescente ou está abaixo do limite decrescente.

3. Digite o nome do proprietário e defina o status da entrada. Clique em **Aplicar**.

Proprietário	Digite o nome do proprietário da entrada com 1 a 16 caracteres. Por padrão, é monitor.
Status	Ative ou desative a entrada. Por padrão, está desativado. **Ativar:** a entrada está ativada. **Desativar:** a entrada está desativada.

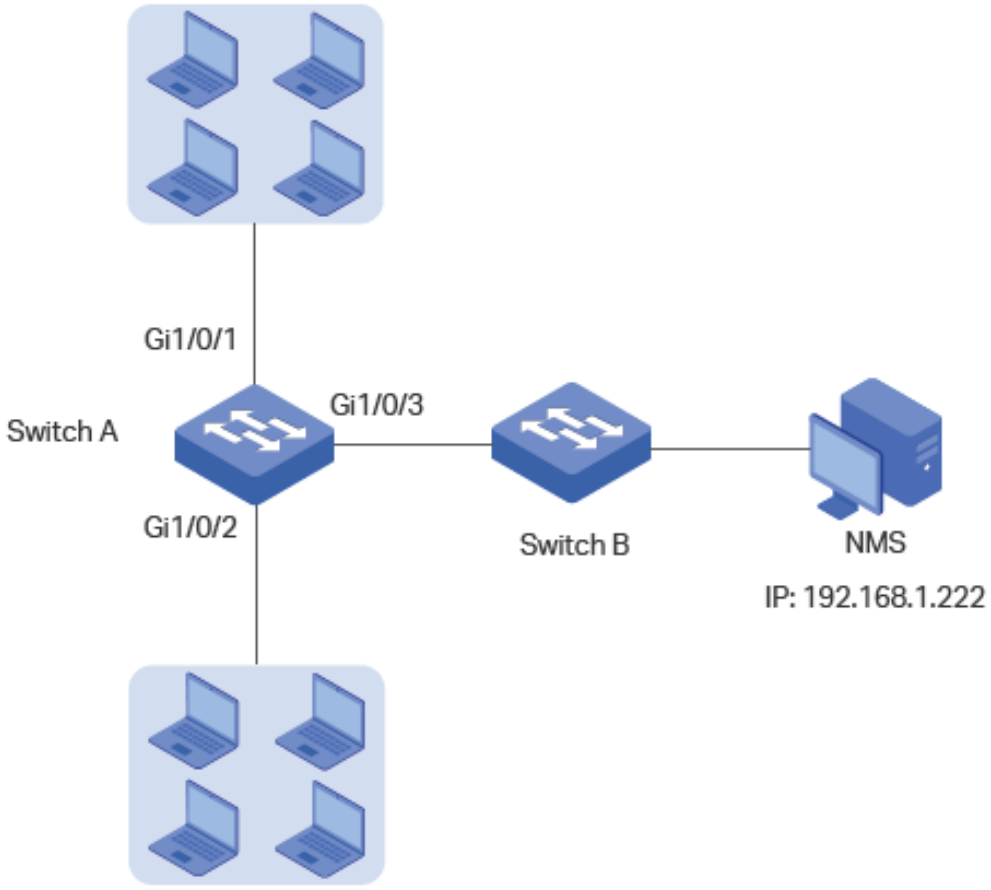
Exemplo de Configuração

Requisitos de Rede

A figura a seguir mostra a topologia de rede de uma empresa. A empresa possui os seguintes requisitos:

1. Monitore o fluxo de tráfego das portas 1/0/1 e 1/0/2 no Switch A e envie notificações ao NMS quando a taxa real de transmissão e recebimento de pacotes exceder o limite predefinido.
2. Monitore o status de envio das portas 1/0/1 e 1/0/2 no Switch A e colete e salve regularmente dados para verificações posteriores. Especificamente, durante o intervalo de amostra, o switch A deve notificar o NMS quando o número de pacotes transmitidos e recebidos na porta exceder o limite predefinido; O switch A deve registrar, mas não notificar o NMS, quando o número de pacotes transmitidos e recebidos estiver abaixo do limite.

O host NMS com endereço IP 192.168.1.222 está conectado ao switch principal, o Switch B. O switch A está conectado ao switch B pela porta 1/0/3. E a porta 1/0/3 e o NMS podem se conectar.



Configurando o Cenário

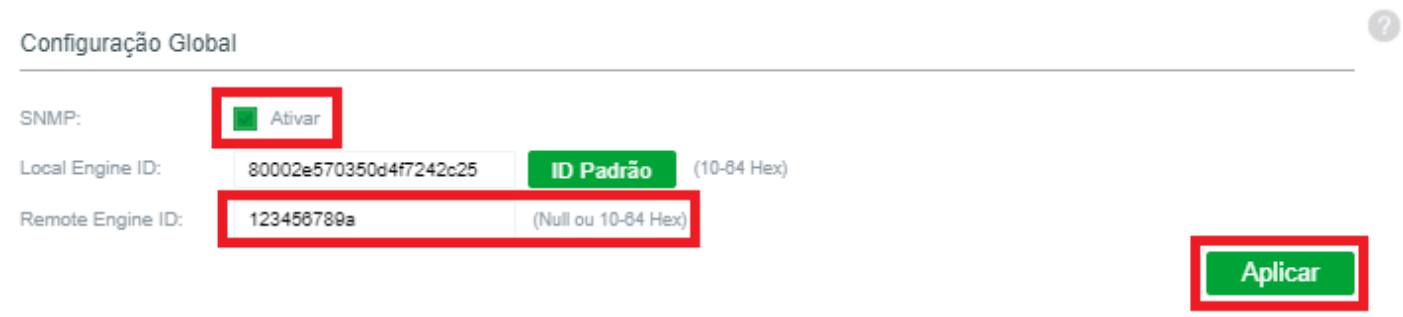
1. Defina um limite para a taxa das portas especificadas e ative o SNMP no Switch A. Configure SNMP e Notification e ative as notificações de trap nas portas. O Switch A pode enviar notificações ao NMS quando a taxa real exceder o limite predefinido.
2. Após as configurações SNMP e Notification, é necessário criar entradas estatísticas nas portas para monitorar a transmissão e o recebimento em tempo real de pacotes e criar entradas no Histórico para coletar e salvar dados relacionados regularmente. Crie duas entradas de evento: uma é o tipo de notificação usado para notificar o NMS, o outro é o tipo de log usado para registrar eventos relacionados. Além disso, crie uma entrada de alarme para monitorar BPackets (pacotes broadcast), defina o limite crescente e o limite decrescente e vincule o evento crescente à entrada do evento de notificação e o evento decrescente à entrada do evento de log.

Configurando o limite de taxa nas portas

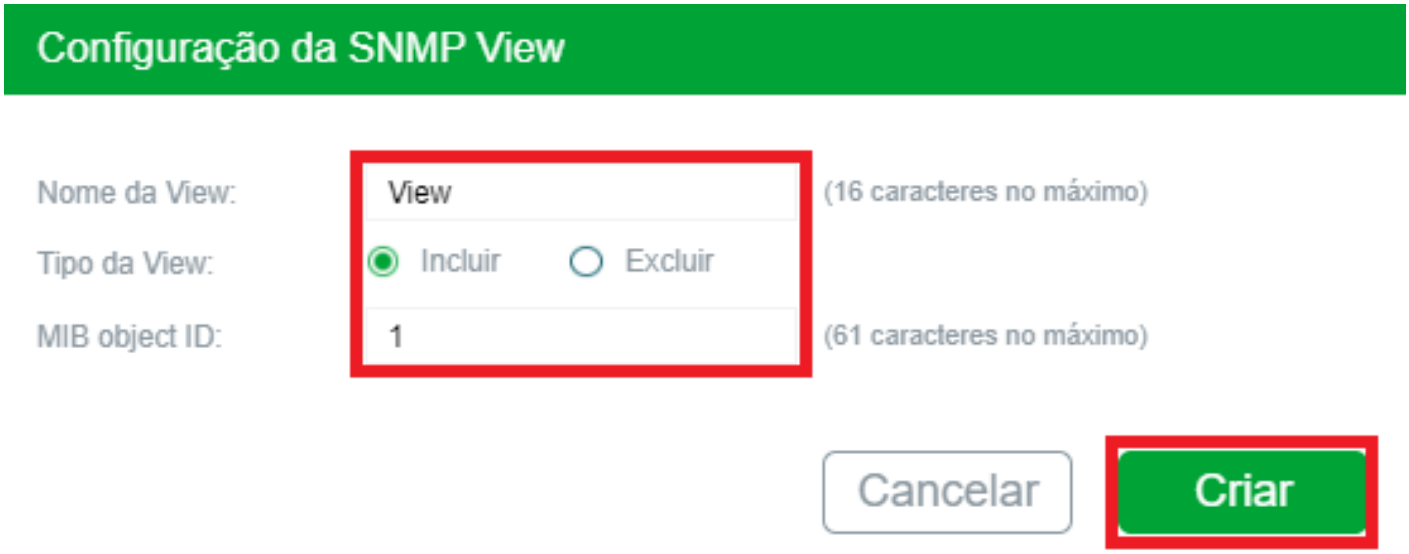
Configure o limite de taxa nas portas necessárias. Para configuração detalhada, consulte Configuração de QoS.

Configurando o SNMP

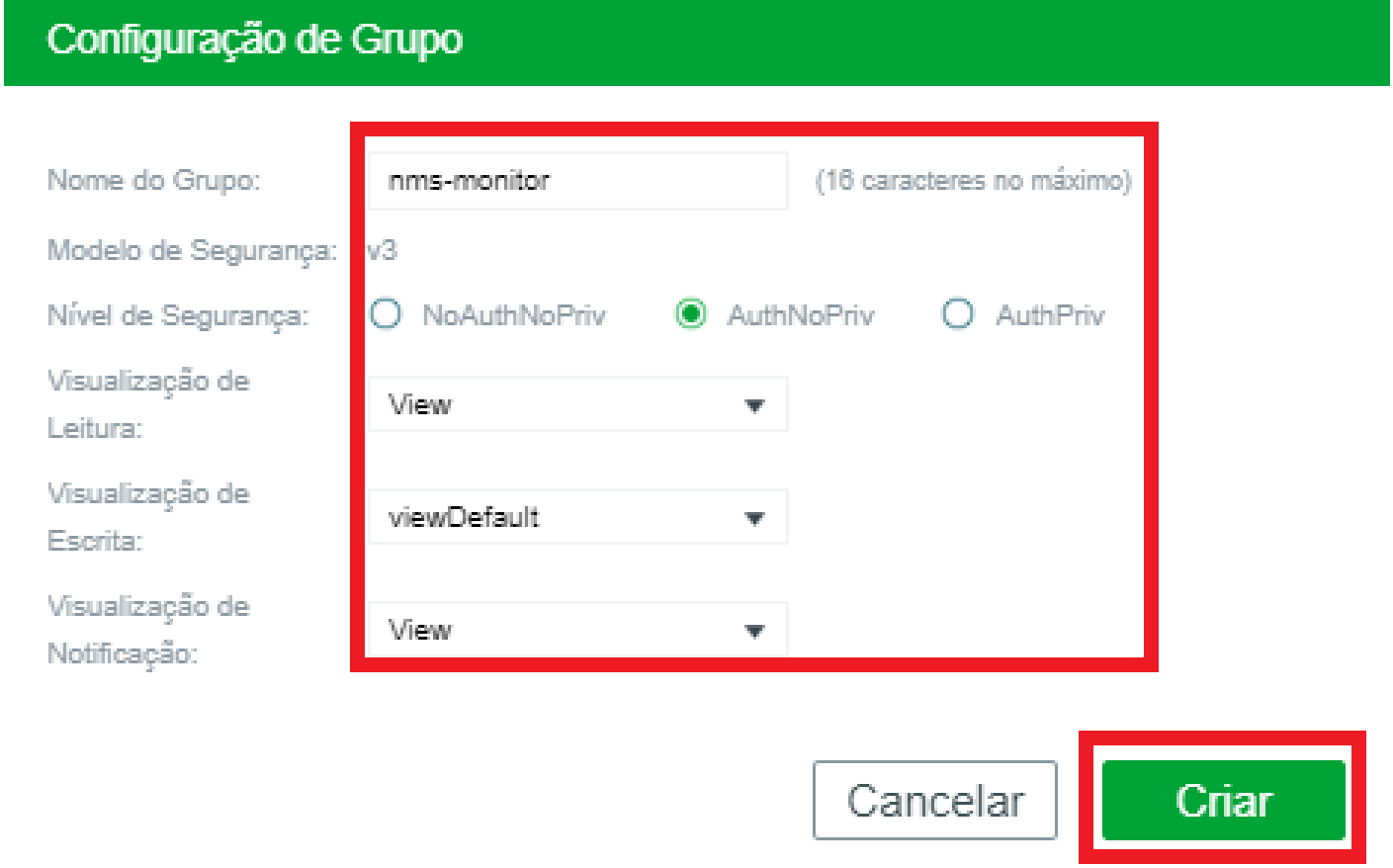
1. Escolha **MANUTENÇÃO > SNMP > Configuração Global** para carregar a página a seguir. Na seção Configuração Global, ative o SNMP e defina o ID do Mecanismo Remoto como 123456789a. Clique em **Aplicar**.



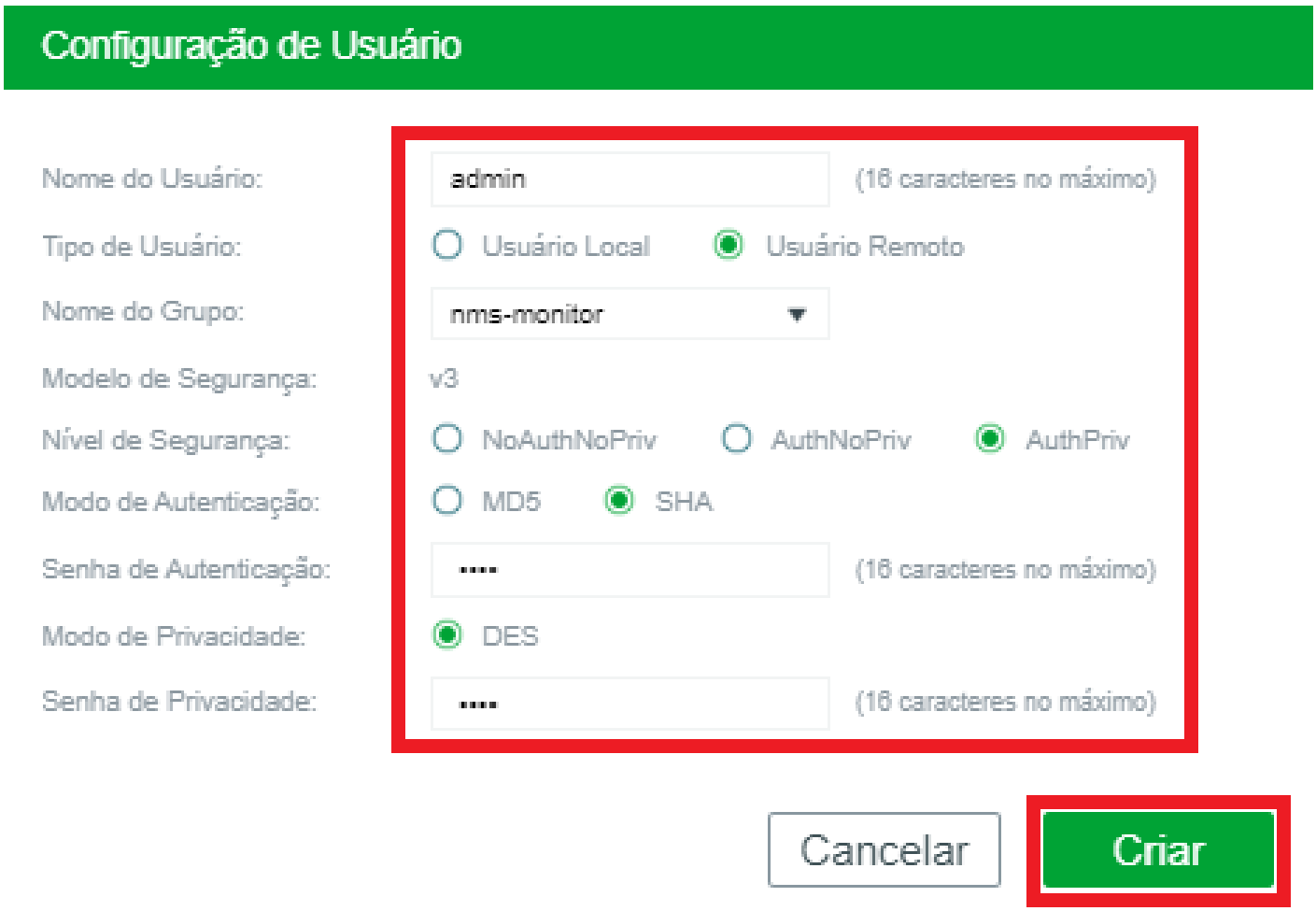
2. Na seção **Configuração de Visualização SNMP**, clique em Adicionar para carregar a página a seguir. Nomeie a visualização SNMP como View, defina o tipo de visualização como Incluir e defina o ID do Objeto MIB como 1 (o que significa todas as funções). Clique em **Criar**.



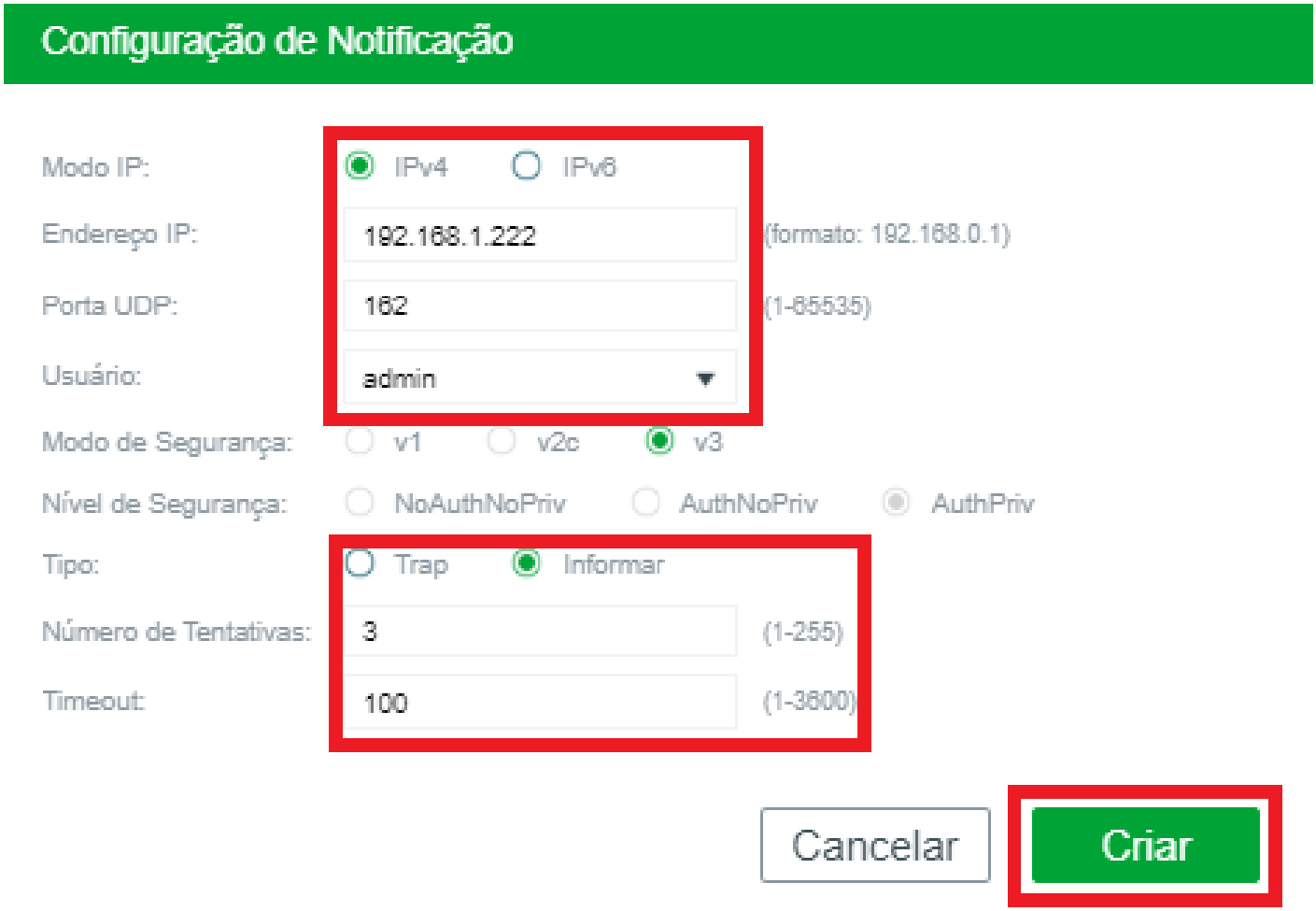
3. Escolha **MANUTENÇÃO > SNMP > SNMP v3 > Grupo SNMP** e clique em Adicionar para carregar a página a seguir. Crie um grupo com o nome de nms-monitor, ative o nível AuthNoPriv e inclua View em Visualização de Leitura e Visualização de Notificação. Clique em **Criar**.



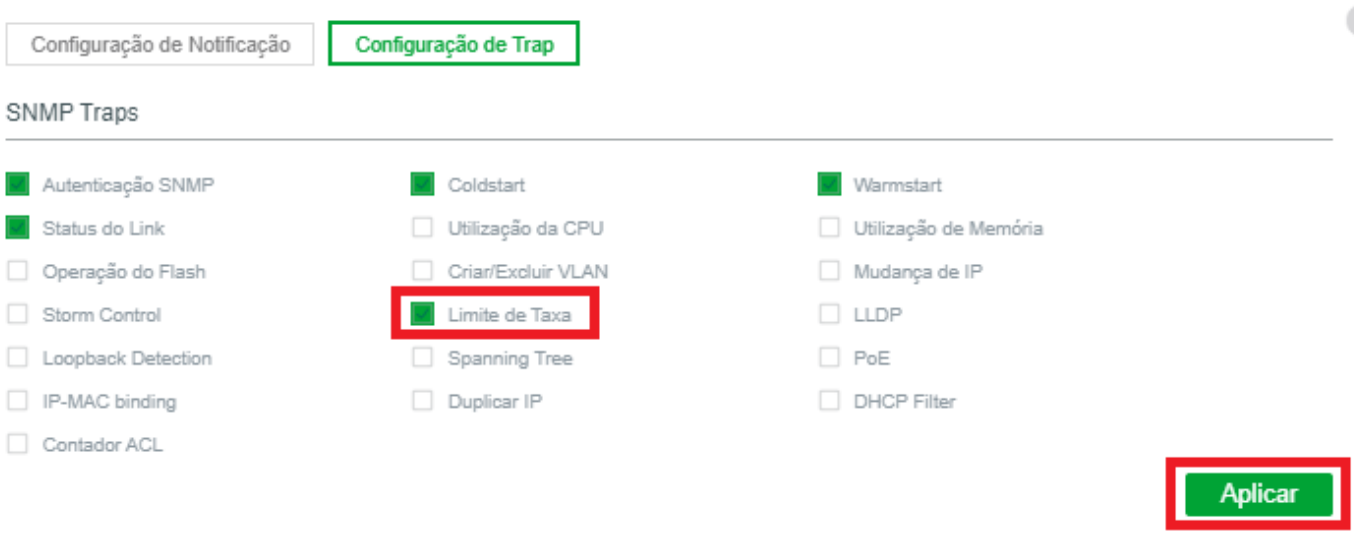
4. Escolha **MANUTENÇÃO > SNMP > SNMP v3 > Usuário SNMP** e clique em Adicionar para carregar a página a seguir. Crie um usuário chamado admin para o NMS, defina o tipo de usuário como Usuário Remoto e especifique o nome do grupo. Defina o nível de segurança de acordo com o do grupo nms-monitor. Escolha o algoritmo de autenticação SHA e o algoritmo de privacidade DES e defina as senhas correspondentes. Clique em **Criar**.



5. Escolha **MANUTENÇÃO > SNMP > Notificação > Configuração de Notificação** e clique em Adicionar para carregar a página a seguir. Escolha o Modo IP como IPv4 e especifique o endereço IP do host NMS e a porta do host para transmitir notificações. Especifique o usuário como admin e escolha o tipo como Informar. Defina o número de tentativas como 3, com o período de tempo limite como 100 segundos. Clique em **Criar**.



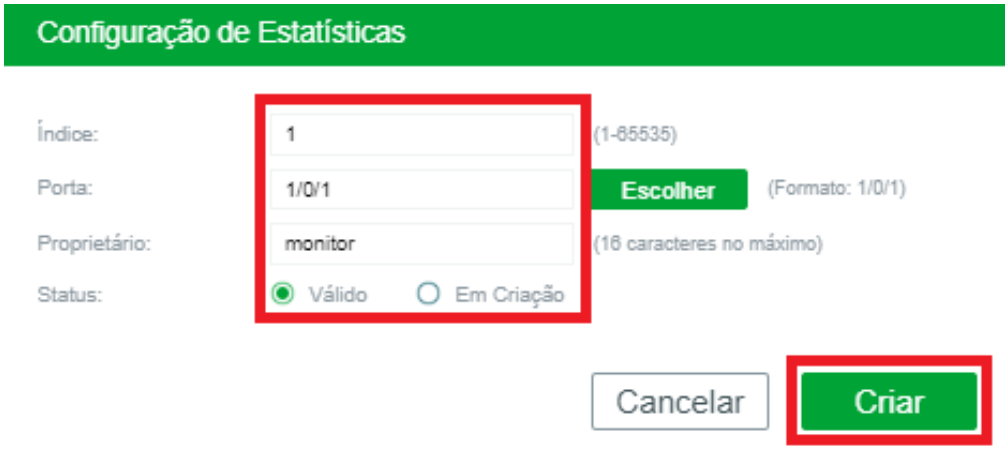
6. Escolha **MANUTENÇÃO > SNMP > Notificação > Configuração de Trap** para carregar a página a seguir. Ative a trap de limite de taxa e clique em **Aplicar**.

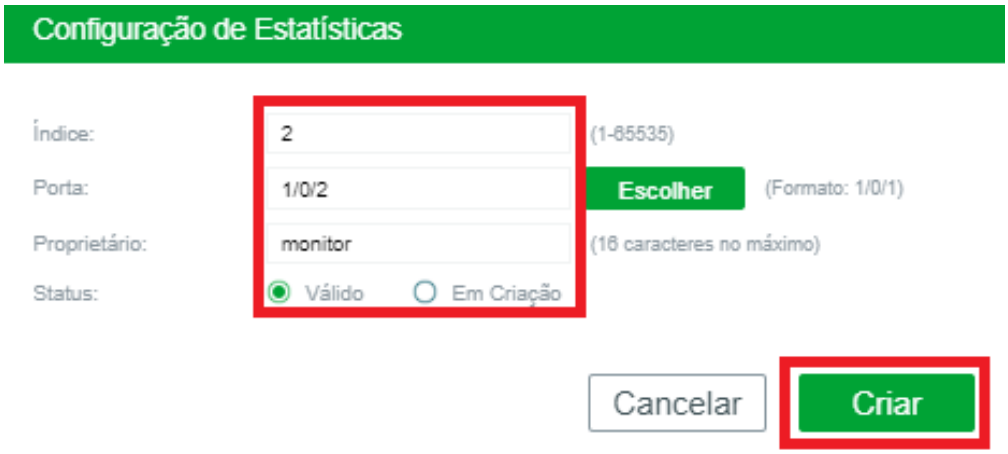


7. Clique em Salvar para salvar as configurações.

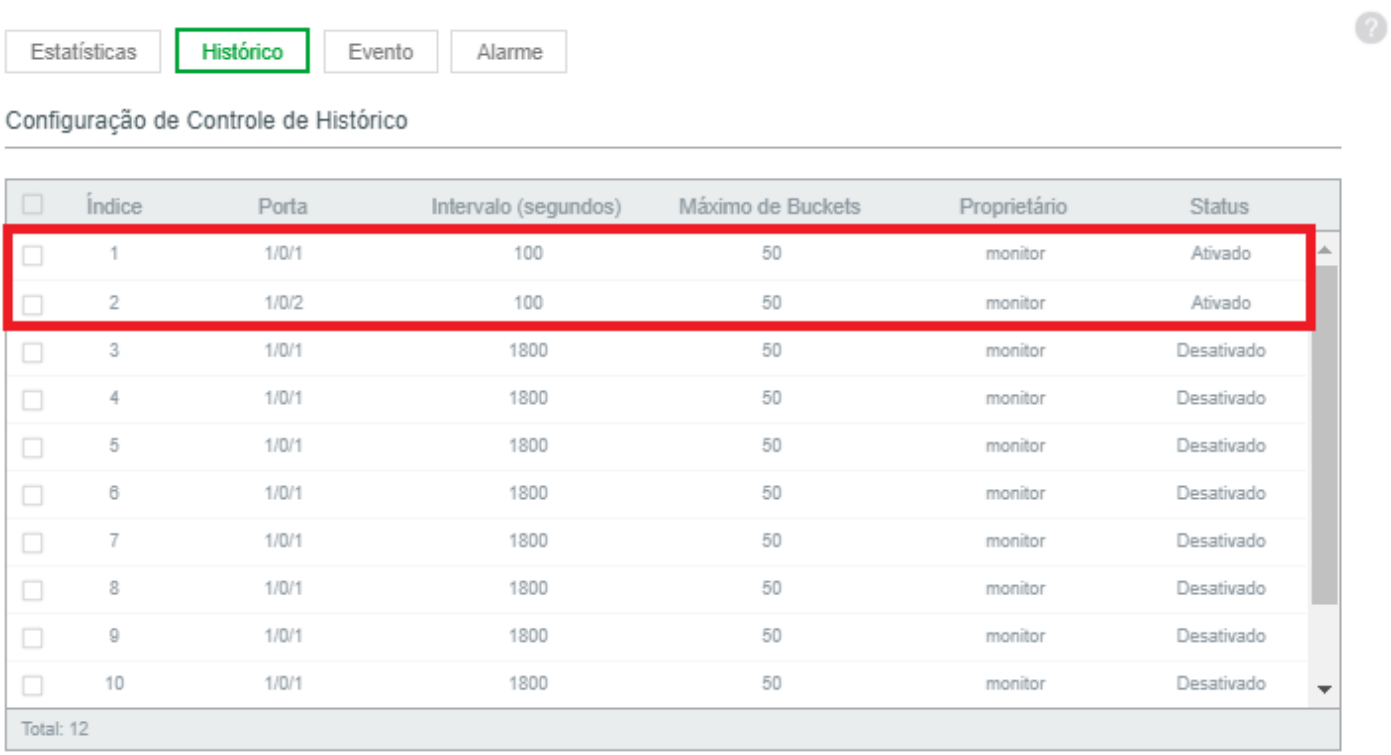
Configurando o RMON

1. Escolha **MANUTENÇÃO > SNMP > RMON > Estatísticas** e clique em Adicionar para carregar a página seguinte. Crie duas entradas e ligue-as às portas 1/0/1 e 1/0/2, respectivamente. Defina o proprietário das entradas como monitor e o status como válido.

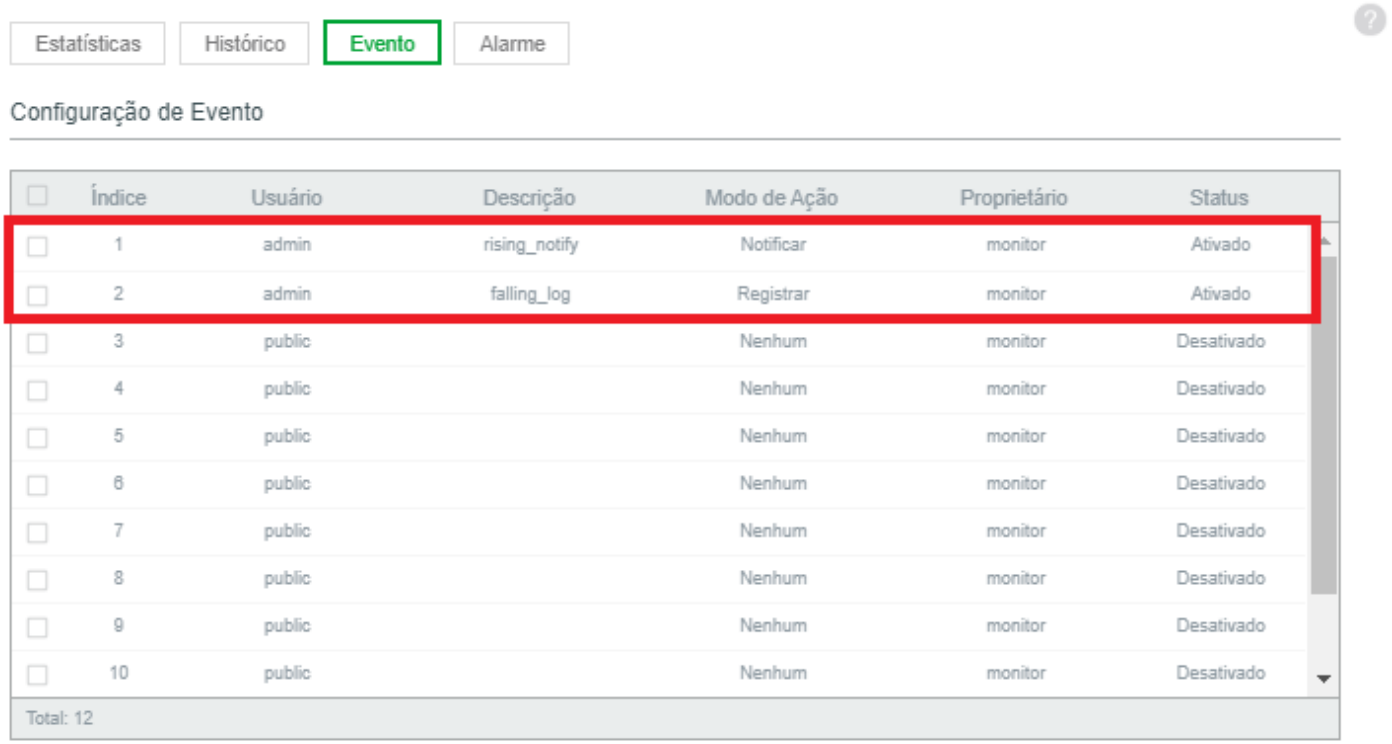




2. Escolha o menu **MANUTENÇÃO > SNMP > RMON > Histórico** para carregar a página seguinte. Configure as entradas 1 e 2. Vincule as entradas 1 e 2 às portas 1/0/1 e 1/0/2, respectivamente, e defina o intervalo como 100 segundos, Máximo de Buckets como 50, o proprietário das entradas como monitor e o status como Ativar.

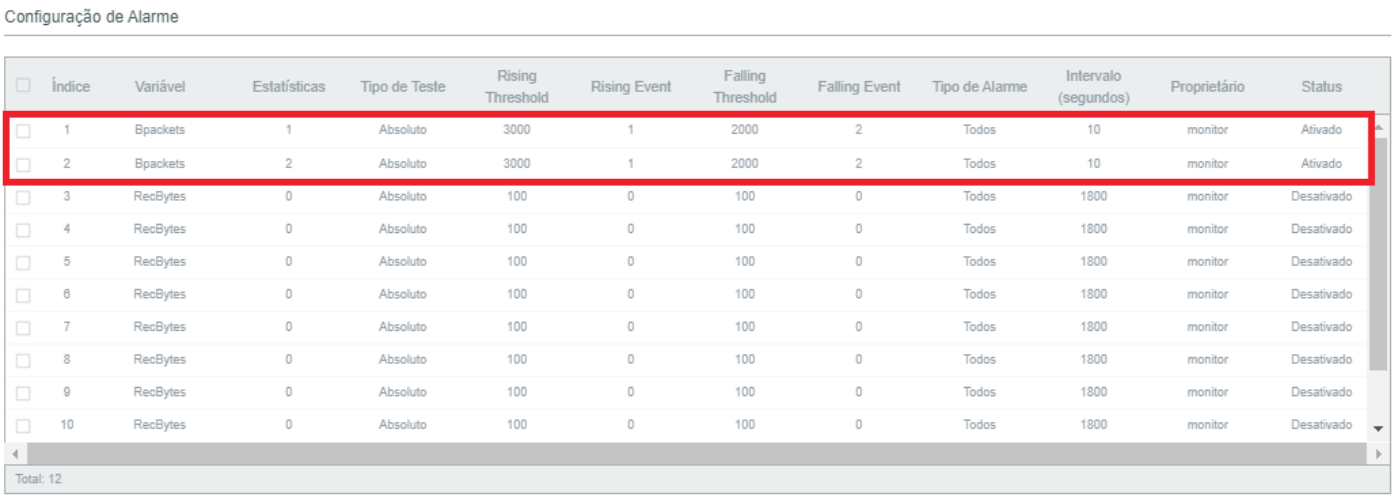


3. Escolha o menu **MANUTENÇÃO > SNMP > RMON > Evento** para carregar a página seguinte. Configure as entradas 1 e 2. Para a entrada 1, defina o nome do usuário SNMP como admin, digite como Notificar, a descrição como "rising_notify", o proprietário como monitor e o status como Ativar. Para a entrada 2, defina o nome de usuário SNMP como admin, digite como Registrar, a descrição como "falling_log", o proprietário como monitor e o status como Ativar.



4. Escolha **MANUTENÇÃO > SNMP > RMON > Alarme** para carregar a página a seguir. Configure as entradas 1 e 2. Para a entrada 1, defina a variável de alarme como BPackets, o ID da entrada de estatísticas relacionadas como 1 (ligado à porta 1/0/1), o tipo de amostra como Absoluto, o limite crescente como 3000, a entrada crescente de eventos associada ID como 1 (que é o tipo de notificação), o limite de queda como 2000, o ID de entrada de evento de queda associado como 2 (que é o tipo de log), o tipo de alarme como Todos, o intervalo como 10 segundos, o

nome do proprietário como monitor. Para a entrada 2, defina o ID da entrada de estatísticas associada como 2 (ligado à porta 1/0/2). Outras configurações são as mesmas da entrada 1.



5. Clique em Salvar para salvar as configurações.

Apêndice: Configuração Padrão

As configurações padrão do SNMP estão listadas nas tabelas a seguir.

Configrações SNMP

Parâmetros	Configurações Padrão
SNMP	Desativado
Local Engine ID	Automático
Remote Engine ID	Nenhum

Configurações da tabela de exibição SNMP padrão

Nome da Visualização	Tipo da Visualização	MIB object ID
ViewDefault	Incluir	1
ViewDefault	Excluir	1.3.6.1.6.3.15
ViewDefault	Excluir	1.3.6.1.6.3.16
ViewDefault	Excluir	1.3.6.1.6.3.18

Configurações padrão do SNMP v1/v2c

Parâmetros	Configurações Padrão
Entrada na Comunidade	Sem entradas
Nome da Comunidade	Nenhum
Modo de Acesso	Somente leitura
Visualização MIB	viewDefault

Configurações padrão do SNMP v3

Parâmetros	Configurações Padrão
Grupo SNMP	
Entrada no Grupo	Sem entradas
Nome do grupo	Nenhum
Modelo de Segurança	v1
Nível de Segurança	NoAuthNoPriv
Visualização de Leitura	ViewDefault
Visualização de Escrita	Nenhum
Visualização de Notificação	Nenhum
Usuário SNMP	
Entrada de Usuário	Sem entradas
Nome do Usuário	Nenhum
Tipo de Usuário	Usuário Local
Nome do Grupo	Nenhum
Modelo de Segurança	v1
Nível de Segurança	noAuthNoPriv
Modo de Autenticação	MD5 (quando o nível de segurança está configurado como AuthNoPriv ou AuthPriv)
Senha de Autenticação	Nenhum
Modo de Privacidade	DES (quando o nível de segurança está configurado como AuthPriv)
Senha de Privacidade	Nenhum

As configurações padrão da notificação estão listadas na tabela a seguir.

Configrações Notificação

Parâmetros	Configurações Padrão
Configuração da notificação	
Entrada de notificação	Sem entradas

Modo IP	IPv4
Endereço IP	Nenhum
Porta UDP	162
Usuário	Nenhum
Modo de Segurança	v1
Nível de Segurança	noAuthNoPriv
Tipo	Trap
Número de Tentativas	Nenhum no modo trap; 3 vezes no modo Informar.
Timeout	Nenhum no modo trap; 100 segundos no modo Informar.
Configuração Trap	
SNMP Traps ativados	Autenticação SNMP, Coldstart, Warmstart e Status do Link

As configurações padrão do RMON estão listadas nas tabelas a seguir.

Configrações RMON

Parâmetros	**Configurações Padrão**
Entrada de Estatísticas	Sem entradas
ID	Nenhum
Porta	Nenhum
Proprietário	Nenhum
Modo IP	Válido

Configurações padrão para entradas do histórico.

Parâmetros	**Configurações Padrão**
Porta	1/0/1
Intervalo	1800 segundos
Máximo de Buckets	50
Proprietário	Monitor
Status	Desabilitado

Configurações padrão para entradas de eventos.

Parâmetros	**Configurações Padrão**
Usuário	public
Descrição	Nenhum

Tipo	Nenhum
Proprietário	Monitor
Status	Desabilitado

Configurações padrão para entradas de alarme.

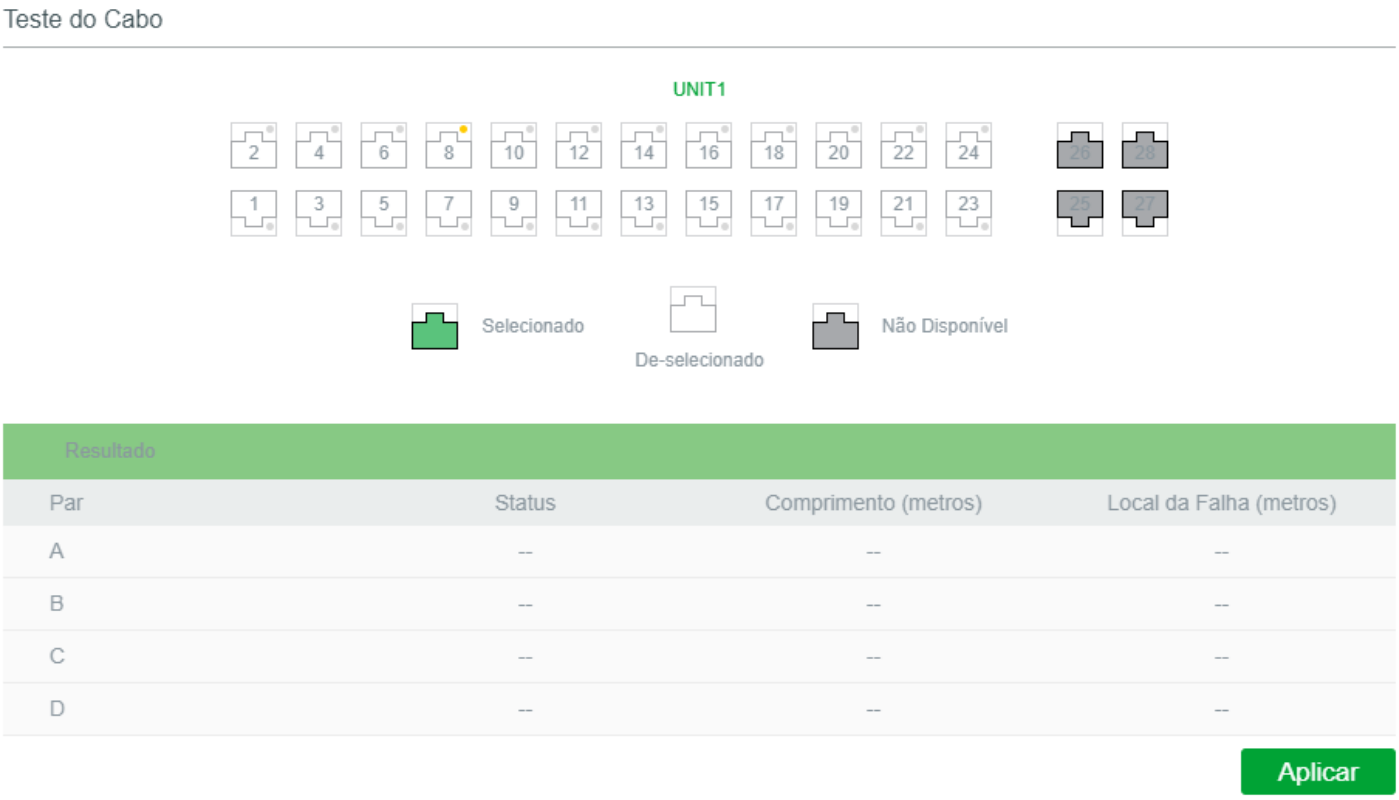
Parâmetros	**Configurações Padrão**
Variável	RecBytes
Estatísticas	0, significa que nenhuma entrada de Estatística está selecionada.
Tipo de Teste	Absoluto
Rising Threshold	100
Rising Event	Nenhum
Falling Threshold	100
Falling Event	Nenhum
Tipo de Alarme	Todos
Intervalo	1800 segundos
Proprietário	monitor
Status	Desabilitado

DIAGNÓSTICO DE DISPOSITIVO E REDE

Diagnóstico de Dispositivo

A função de diagnóstico de dispositivo disponibiliza teste de cabo, o qual permite a verificação de problemas baseado no estado da conexão, comprimento do cabo e local da falha.

Vá até o menu **MANUTENÇÃO > Diagnóstico de Dispositivo** para carregar a página a seguir.



Siga os seguintes passos para diagnosticar o cabo:

1. Selecione a porta desejada para o teste e clique em **Aplicar**.
2. Verifique os resultados dos testes na seção **Resultado**.

Par	Mostra o número do Par.
Status	Mostra o status do cabo. Os resultados incluem normal, curto, aberto e crosstalk. **Normal:** o cabo está conectado normalmente. **Curto:** um curto circuito está sendo causado por contato anormal entre os fios de um cabo **Aberto:** nenhum dispositivo está conectado na outra ponta, ou a conexão está interrompida. **Crosstalk:** incompatibilidade de impedância devido à qualidade do cabo.
Comprimento	Se a conexão estiver normal o comprimento do cabo será mostrado.
Local da Falha	Se o status da conexão for curto, aberto ou crosstalk, aqui será exibido o comprimento desde a porta até o ponto com problemas.

Diagnóstico de Rede

A função de diagnóstico de rede disponibiliza testes de Ping e Tracert. Você pode testar a conectividade de hosts remotos ou de gateways através do switch para o destino.

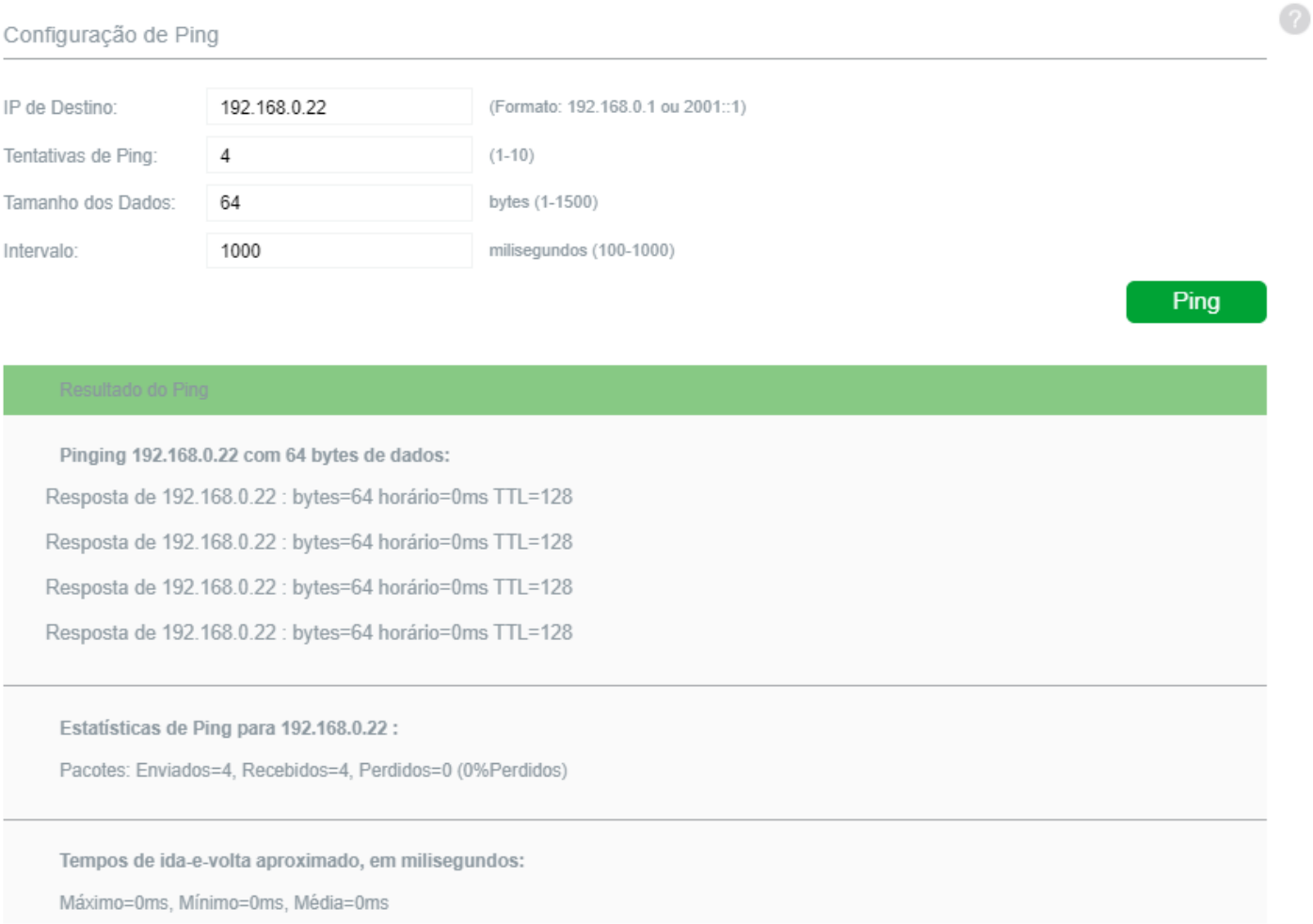
Com o Diagnóstico de Rede você pode:

- Verificar erros com o teste de Ping.
- Verificar erros com o teste de Tracert.

Verificar erros com o teste de Ping

Você pode utilizar a ferramenta de Ping par testar a conectividade de hosts remotos.

Vá até o menu **MANUTENÇÃO > Diagnóstico de Rede > Ping** para carregar a página a seguir.



Siga os seguintes passos para testar a conectividade entre o switch e um dispositivo na rede:

1. Na seção **Configuração de Ping** entre com o endereço IP do dispositivo de destino para o teste de Ping, configure as Tentativas de Ping, o tamanho dos dados e o intervalo de acordo com sua necessidade e clique em **Ping** para começar o teste.

IP de Destino	Entre com o endereço IP do destino para o teste de Ping. Tanto IPv4 e IPv6 são suportados.

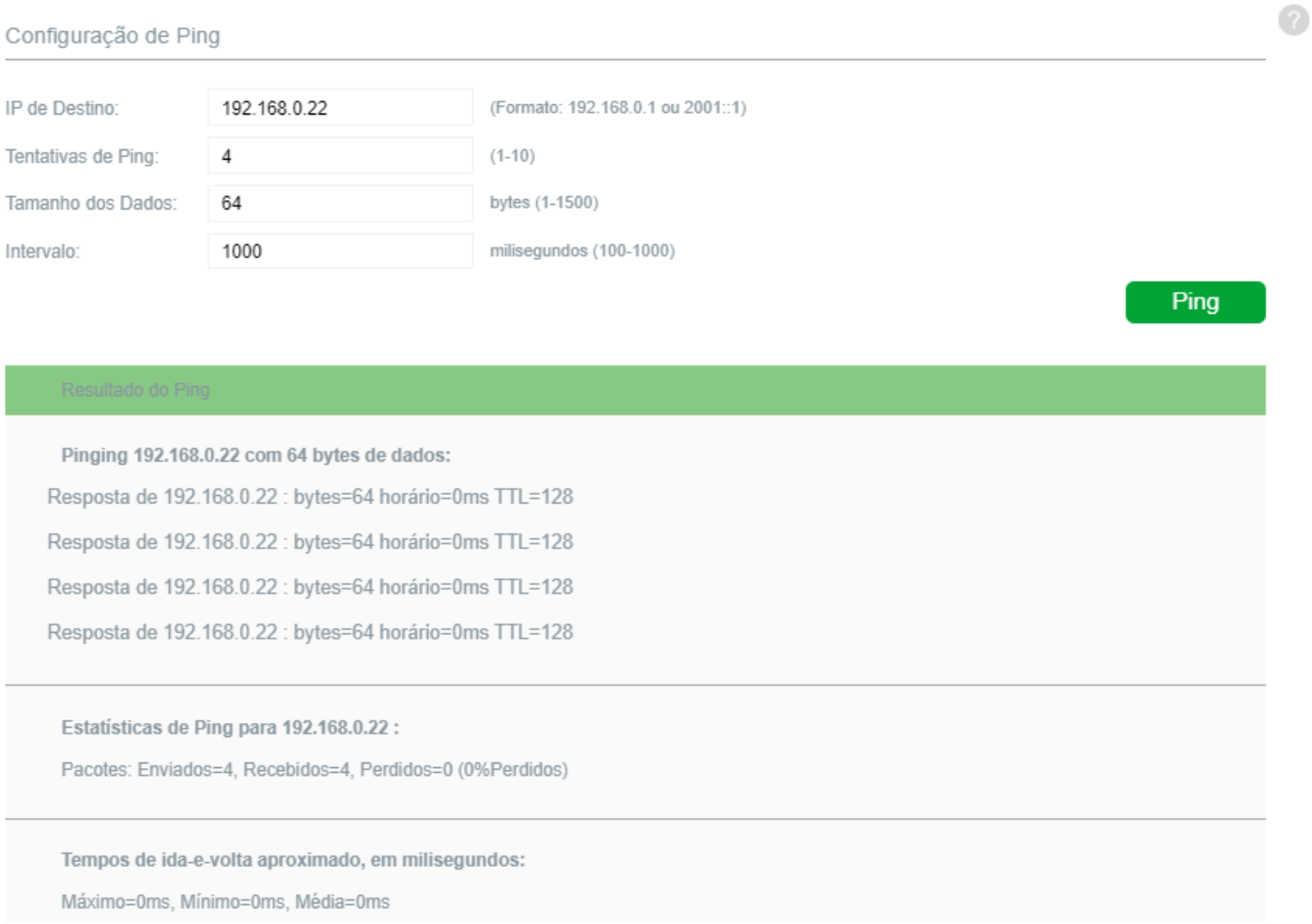
Horários de Ping	Entre com o número de vezes que os dados de teste serão enviados pelo teste de Ping. É recomendado que se utilize o valor padrão de 4 vezes.
Tamanho dos Dados	Entre com o tamanho dos dados que serão enviados pelo teste de Ping. É recomendado utilizar o valor padrão de 64 bytes.
Intervalo	Especifique o intervalo no qual os pacotes de requisições ICMP são enviados. É recomendado manter o valor padrão de 1000 milissegundos.

2. Na seção **Resultado do Ping** verifique os resultados do teste.

Verificar erros com o teste de Tracert

Você pode utilizar a ferramenta de Tracert para encontrar o caminho do switch até o destino e testar a conectividade entre o switch e os roteadores ao longo do caminho.

Vá até o menu **MANUTENÇÃO > Diagnóstico de Rede > Tracert** para carregar a página a seguir.



Siga os seguintes passo para testar a conectividade entre o switch e os roteadores ao longo do caminho entre a origem e o destino:

1. Na seção **Configuração Tracert** entre com o endereço IP do destino configure os saltos máximos e então clique em **Tracert** para iniciar o teste.

IP de Destino	Insira o endereço IP do dispositivo de destino. Tanto IPv4 quanto IPv6 são suportados.
Saltos Máximos	Especifique o número máximo de saltos da rota pelos quais os dados de teste podem passar.

2. Na seção **Resultado Tracert** verifique os resultados do teste.

Apêndice: Configuração Padrão

As configurações padrão para o Diagnóstico de Rede estão listados nas tabelas a seguir.

Configurações Padrão de Ping.

Parâmetros	**Configurações Padrão**
IP de Destino	192.168.0.1
Horários de Ping	4
Tamanho dos Dados	64 bytes
Intervalo	1000 milissegundos

Configurações Padrão de tracert.

Parâmetros	**Configurações Padrão**
IP de Destino	192.168.0.1
Saltos Máximos	4 saltos

CONFIGURANDO LOGS DO SISTEMA

Visão Geral

O switch gera mensagens em resposta a eventos, falhas ou erros ocorridos, bem como mudanças em configurações ou outras ocorrências. Você pode verificar mensagens do sistema para debugging e gerenciamento de rede.

Os logs do sistema podem ser salvos em vários destinos, como buffer de log, arquivo de log ou servidores de log remotos, dependendo da sua configuração. Logs salvos como buffer e arquivo de log são chamados logs locais, e logs salvos em servidores remotos são chamados logs remotos. Logs remotos facilitam você monitorar remotamente o estado corrente da rede.

Você pode configurar vários níveis de mensagens de log para controlar o tipo de mensagens de logs que serão salvos em cada destino.

Configurações dos Logs do Sistema

As configurações dos logs do sistema incluem:

- Configuração dos Logs locais;
- Configuração dos Logs remotos;
- Realizar backup dos Logs;
- Visualizar a tabela de Logs.

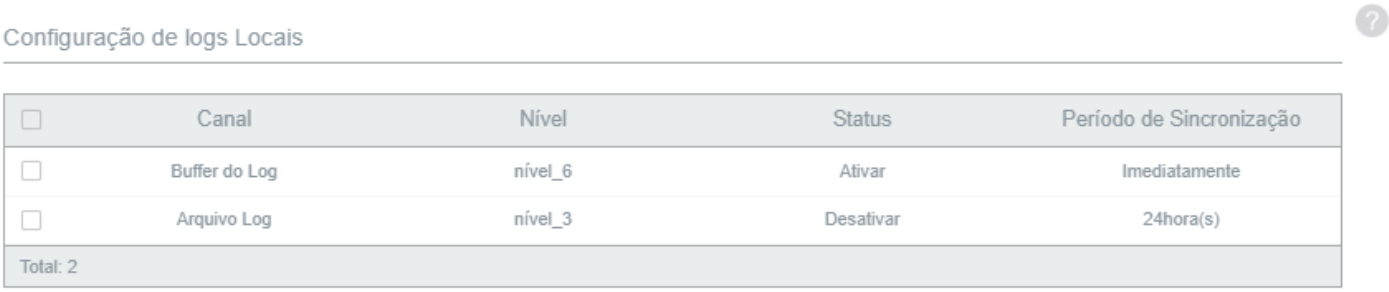
Os Logs são classificados nos 8 níveis seguintes. Mensagens de níveis entre 0 e 4 representam que a funcionalidade do switch foi afetada. Tome ações de acordo com as mensagens de log.

Gravidade	**Nível**	**Descrição**	**Exemplo**
Emergências	0	O sistema está fora de uso e você deverá reiniciar o switch.	Mal funcionamento de software afeta a funcionalidade do switch.
Alertas	1	Ações devem ser tomadas imediatamente.	A utilização de memória alcançou o limite.
Crítico	2	Análise de causas ou tomada de ações devem ser tomadas imediatamente.	A utilização de memória alcançou o limite de aviso.
Erros	3	Operações de erro ou processamento não usual que não afetará as operações subsequentes mas devem ser notadas e analisadas.	Comandos errados ou entrada de senha errada.

Avisos	4	Condições que podem causar falha no processamento e que devem ser notadas.	Detecção de pacotes de protocolos com erro.
Notificações	5	Normal, porém, condições significantes.	Comando de **Shutdown** aplicado em uma porta.
Informação	6	Mensagens normais para sua informação.	Uso do comando **display**.
Debugging	7	Mensagens de nível de debug que você pode ignorar.	Informação de operação geral.

Configurando Logs Locais

Vá até o menu **MANUTENÇÃO > Logs > Logs Locais** para carregar a página a seguir.



Siga os seguintes passos para configurar os logs locais:

1. Selecione o canal desejado e configure a severidade correspondente e status.

Canal	Exibe o local das mensagens de log. **Log Buffer:** Log Buffer indica a RAM para salvar logs do sistema. Esse canal é o habilitado por padrão. Informações que estão no buffer são mostradas na página **MANUTENÇÃO > Logs > Tabela de Logs**. Informações no log buffer serão perdidas quando o switch for reinicializado. **Arquivo Log:** Arquivo Log indica o setor flash para salvar os logs de sistema. Informações no arquivo log não serão perdidas quando o switch for reinicializado, e podem ser exportados na página **MANUTENÇÃO > Logs > Backup Logs**.
Nível	Especifique o nível das mensagens de log que são salvas no canal selecionado. Apenas mensagens log com valor de nível igual a este ou menores serão salvos. Há oito níveis disponíveis, marcados de 0 a 7. Um valor menor indica uma prioridade maior.
Status	Ativa ou desativa o canal.

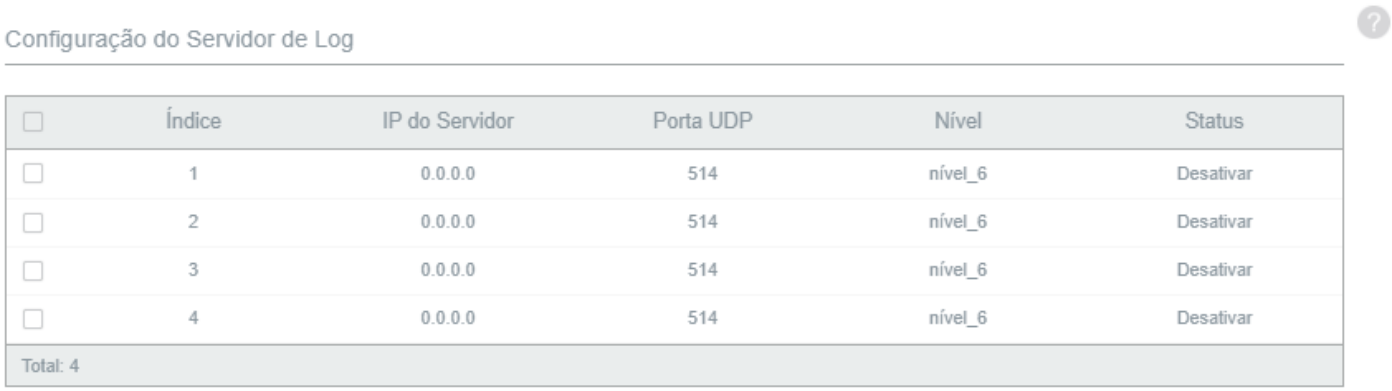
Período de Sincronização	Pelo padrão, as informações do log são salvas no buffer de log imediatamente, e sincronizadas para o arquivo log a cada 24 horas. Se necessário, você pode mudar a frequência de sincronização do log usando CLI.

2. Clique em **Aplicar**.

Configurando Logs Remotos

Você pode configurar até quatro hosts para recebem os logs do sistema do switch. Esses hosts são chamados Servidores de Log. O switch irá encaminhar mensagens de Log para os servidores uma vez que uma mensagem de log é gerada. Para mostrar os logs, os servidores devem rodar softwares de servidor de log para compilar os padrões de log do sistema.

Vá até o menu **MANUTENÇÃO > Logs > Logs Remotos** para carregar a página a seguir.



Siga os seguintes passo para configurar as informações dos servidores de log remoto:

1. Selecione uma entrada para habilitar o servidor, e então configure o endereço IP do servidor e o nível.

IP do Servidor	Insira o endereço IP do servidor de Log.
Porta UDP	Exibe a porta UDP usada pelo servidor para receber as mensagens de log. O switch usa a porta 514 como padrão para enviar mensagens de Log.
Nível	Especifique o nível de severidade das mensagens de log enviadas ao servidor de log selecionado. Apenas mensagens de log com um nível de severidade que seja igual ou menor que serão salvas.
Status	Ativa ou desativa o servidor de log.

2. Clique em **Aplicar**.

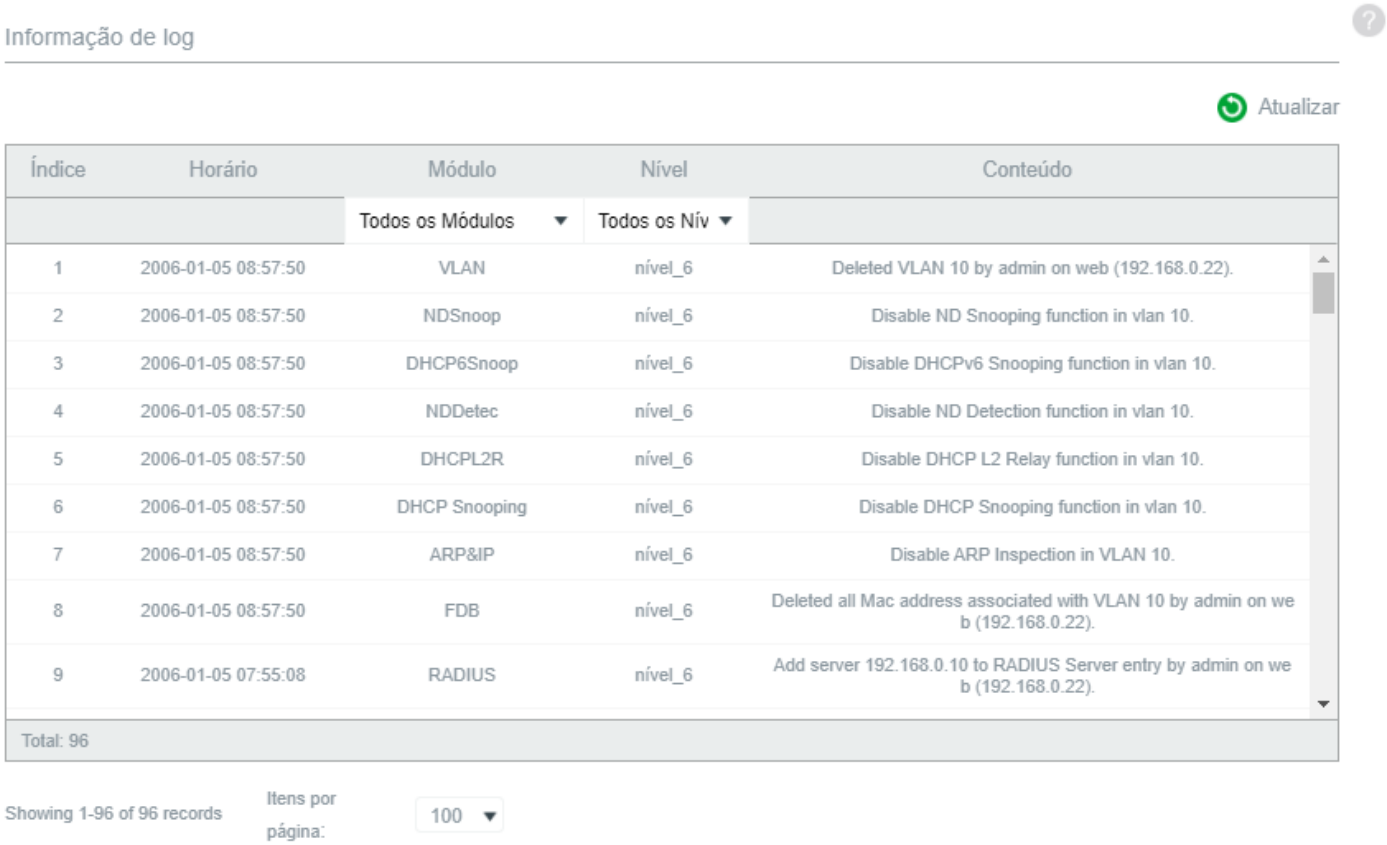
Backup dos Logs

Vá até o menu **MANUTENÇÃO > Logs > Backup dos Logs** para carregar a seguinte página.

Clique em **Backup Logs** para salvar os logs do sistema como arquivo em seu computador. Se o switch apresentar falhas, você poderá usar este arquivo para solucionar problemas.

Visualizando a Tabela de Logs

Vá até o menu **MANUTENÇÃO > Logs > Tabela de Log** para carregar a seguinte página.



Selecione o Módulo e o Nível para visualizar a informação de log correspondente.

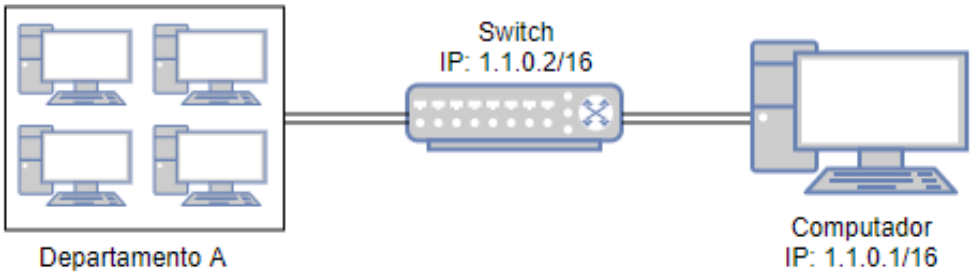
Horário	Exibe o horário que o evento registrado ocorreu. Para obter o horário exato em que ocorreu o evento registrado, você deve configurar o horário do sistema na página **SISTEMA > Info do Sistema > Horário do Sistema**.
Módulo	Selecione um módulo a partir da lista drop-down para exibir a informação do log correspondente.

Nível	Selecione um nível de Severity para exibir logs que tenham o nível de Severity que seja o mesmo valor ou menor.
Conteúdo	Exibe as informações detalhadas do evento registrado.

Exemplo de Configuração

Requisitos de Rede

O gerente de rede de uma companhia necessita monitorar a rede do departamento A para correção de problemas.



Configurando o Cenário

O gerente de rede pode configurar o PC como servidor de log para receber os logs do sistema do switch. Garanta que o computador e o switch estejam visíveis um para o outro; configure um servidor de log que compile o padrão do log do sistema no computador e configure o computador como servidor de Log.

1. Vá até o menu **MANUTENÇÃO > Logs > Logs Remotos** para carregar a página a seguir. Habilite o host 1, e configure o endereço IP do computador 1.1.0.1 como endereço IP do servidor, e o Nível com o nível_5; clique em **Aplicar**.

2. Clique em Salvar para salvar as configurações.

Apêndice: Configuração Padrão

As configurações padrão para manutenção estão listados nas tabelas a seguir.

Configurações Padrão Log local.

Parâmetros	**Configurações Padrão**
Status Buffer Log	Ativado
Severity Buffer Log	Nível_6
Sincronismo Periódico do Buffer Log	Imediatamente
Status do Arquivo de Log	Desabilitado
Severity do Arquivo de Log	Nível_3
Sincronismo Periódico do Arquivo de Log	24 horas

Configurações Padrão Log Remoto.

Parâmetros	**Configurações Padrão**
IP do Servidor	0.0.0.0
Porta UDP	514
Severity	Nível_6
Status	Desativado

Termo de garantia

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

Nome do cliente:

Assinatura do cliente:

Nº da nota fiscal:

Data da compra:

Modelo:

Nº de série:

Revendedor:

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

1. Todas as partes, peças e componentes do produto são garantidos contra eventuais defeitos de fabricação, que porventura venham a apresentar, pelo prazo de 1 (um) ano – sendo 3 (três) meses de garantia legal e 9 (nove) meses de garantia contratual –, contado a partir da data de entrega do produto ao Senhor Consumidor, conforme consta na nota fiscal de compra do produto, que é parte integrante deste Termo em todo o território nacional. Esta garantia contratual compreende a troca gratuita de partes, peças e componentes que apresentarem defeito de fabricação, incluindo a mão de obra utilizada nesse reparo. Caso não seja constatado defeito de fabricação, e sim defeito(s) proveniente(s) de uso inadequado, o Senhor Consumidor arcará com essas despesas.

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

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

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

5. A garantia perderá totalmente sua validade na ocorrência de quaisquer das hipóteses a seguir: a) se o vício não for de fabricação, mas sim causado pelo Senhor Consumidor ou por terceiros estranhos ao fabricante; b) se os danos ao produto forem oriundos de acidentes, sinistros, agentes da natureza (raios, inundações, desabamentos, etc.), umidade, tensão na rede elétrica (sobretensão provocada por acidentes ou flutuações excessivas na rede), instalação/uso em

desacordo com o manual do usuário ou decorrentes do desgaste natural das partes, peças e componentes; c) se o produto tiver sofrido influência de natureza química, eletromagnética, elétrica ou animal (insetos, etc.); d) se o número de série do produto tiver sido adulterado ou rasurado; e) se o aparelho tiver sido violado.

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

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

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

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

Todas as imagens deste manual são ilustrativas.

Suporte a clientes: (48) 2106 0006

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

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

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

SAC: 0800 7042767

Onde comprar? Quem instala?: 0800 7245115

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

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

www.intelbras.com.br (http://www.intelbras.com.br)

Indústria Brasileira