Manual do usuário

Linha Smart

MANUAL DO USUÁRIO

Linha Smart | Manual do usuário

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

Este manual contempla os seguintes modelos da linha Smart :

- SMART SI2106G-HPA

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

Exportar para PDF

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

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

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

Proteção e Segurança de Dados

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

Tratamento de dados pessoais

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

Diretrizes que se aplicam aos funcionários da Intelbras

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

Diretrizes que controlam o tratamento de dados

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

Uso indevido e invasão de hackers

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

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

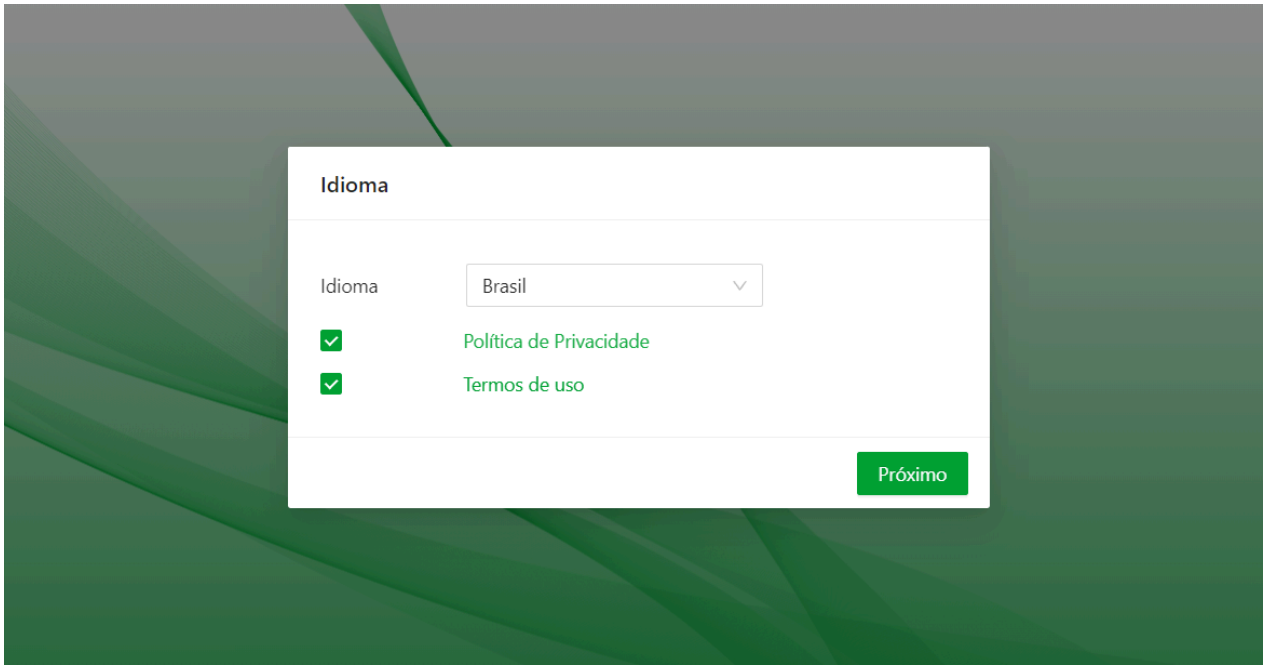
Acesso ao Switch

Certifique-se de que the switch e o dispositivo de configuração estão conectados na mesma faixa de rede e ligados.

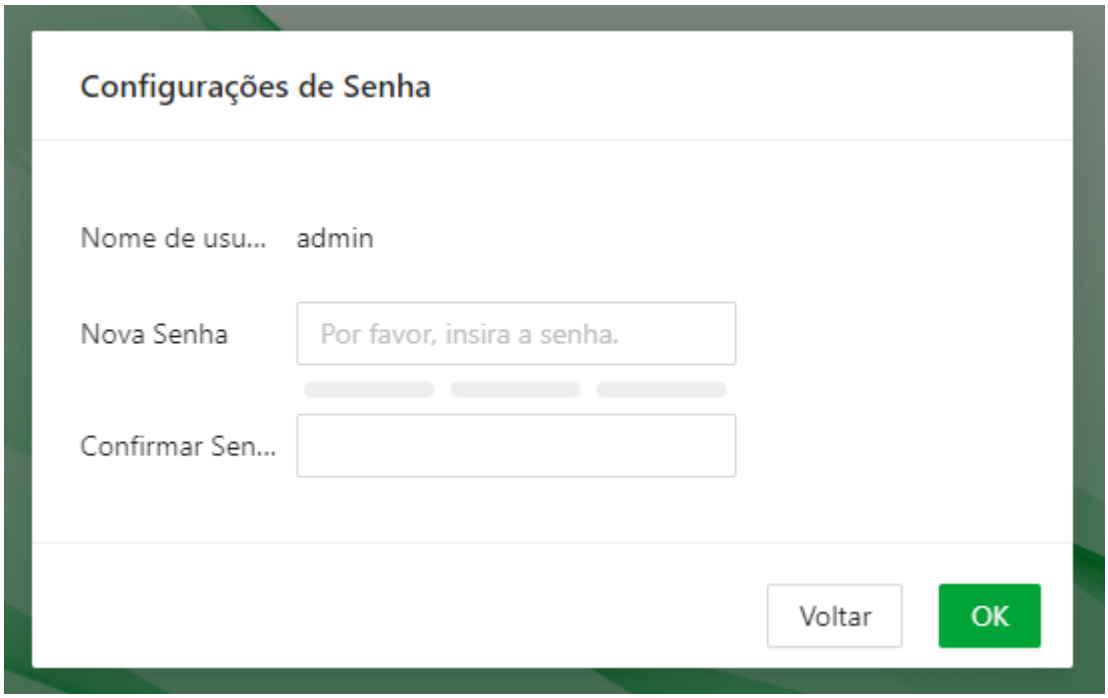
Procedimento

Passo 1 - Abra o seu navegador, insira o endereço IP (192.168.0.1 para primeiro acesso) do switch na barra de endereços do navegador e pressione a tecla Enter.

Passo 2 - Leia o Acordo de Licença de Software e a Política de Privacidade, clique em Eu li e concordo com os termos do Acordo de Licença de Software e da Política de Privacidade e, em seguida, clique em OK.



Passo 3 - Defina a senha do usuário admin.



Passo 4 - Clique em OK.

> O switch não possui senha padrão, a senha será definida no primeiro acesso ao dispositivo

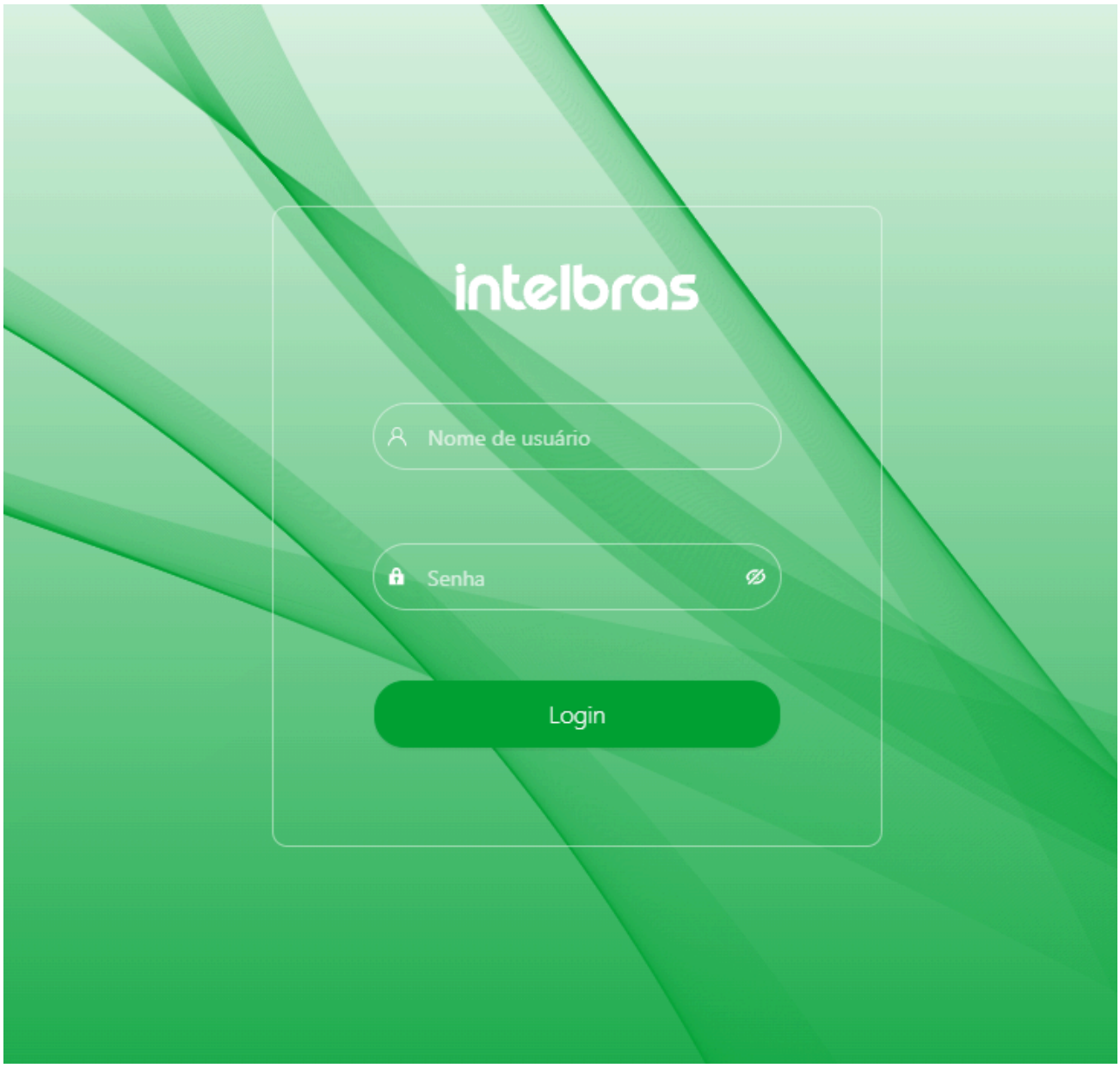
Fazendo Login

Antes de fazer login, certifique-se de:

Passo 1 - Insira o endereço IP (192.168.0.1 por padrão) do switch na barra de endereços do navegador e pressione a tecla Enter.

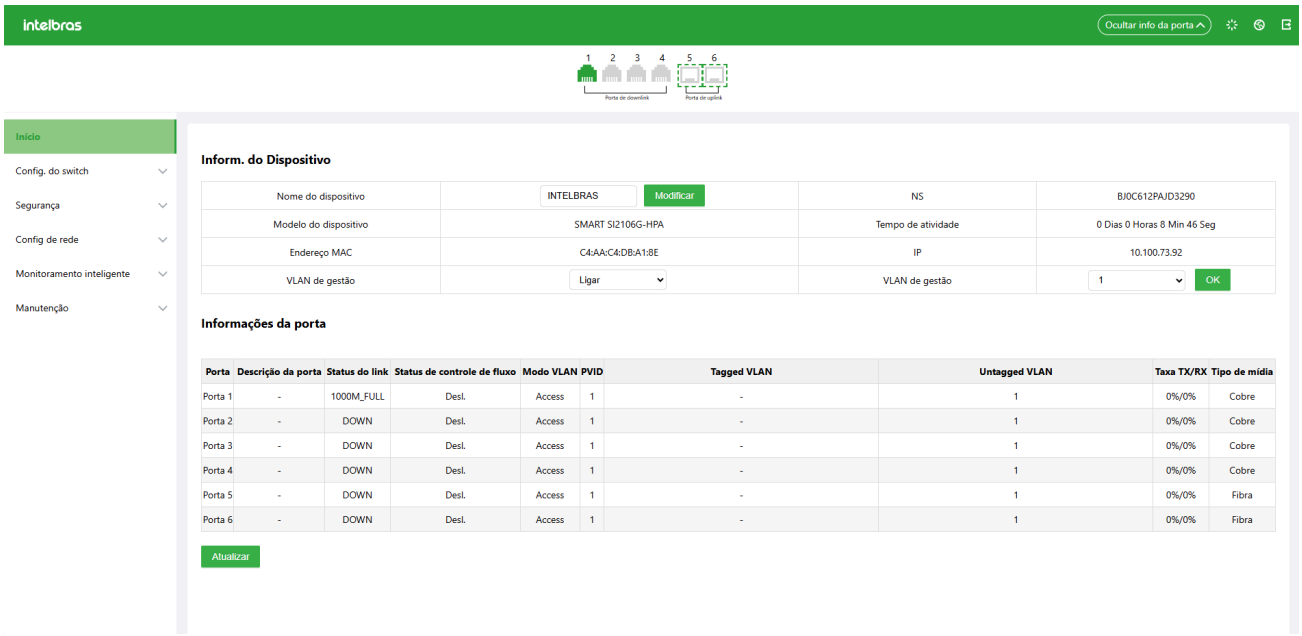
Passo 2 - Insira o nome de usuário e a senha.

Passo 3 - Clique em Login.



Dashboard

Após o login, você será redirecionado para a tela inicial do dispositivo. Nesta tela você poderá visualizar informações sobre o status do dispositivo, portas, especificações de sistema, software e hardware.



Configuração do Switch

Configuração das portas

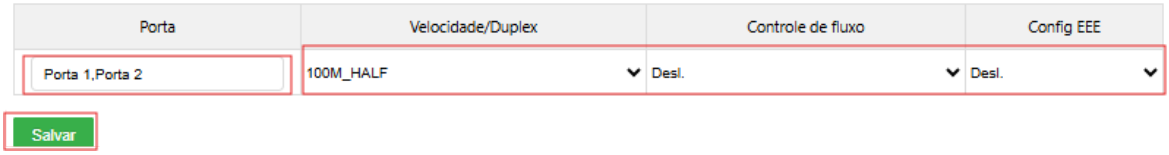
Você pode configurar os parâmetros da porta, incluindo velocidade/duplex, controle de fluxo e outros parâmetros. Os parâmetros da porta afetarão diretamente o modo de operação da mesma. Realize as configurações de acordo com os requisitos práticos.

Procedimento

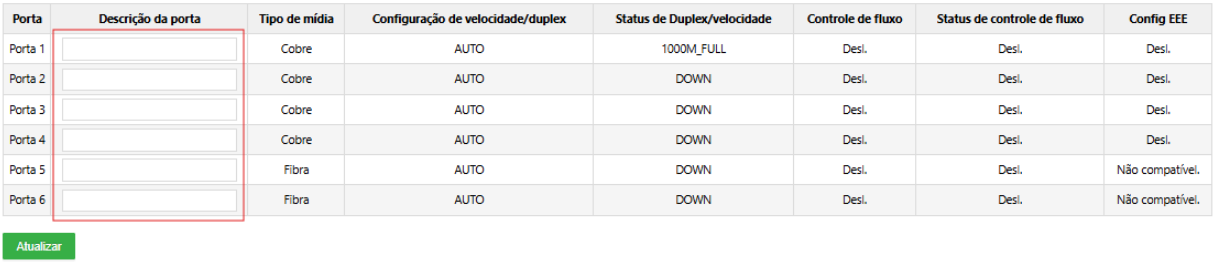
Passo 1 - Selecione **Configuração do Switch** > **Porta**.

Passo 2 - Selecione o número da porta, configure os parâmetros e clique em **Salvar**

- **Speed/Duplexing (Velocidade/Duplex):** Configura a velocidade e o modo duplex. A velocidade/duplex é definida como **Auto** para portas combinadas (combo ports).
- **Flow Control (Controle de Fluxo):** Ativar a função de controle de fluxo pode aliviar efetivamente o congestionamento da rede, reduzir a perda de dados e melhorar a estabilidade da rede e a confiabilidade dos dados.
- **EEE Config (Configuração EEE):** Ativar a função EEE (Energy-Efficient Ethernet) pode reduzir o consumo de energia quando a rede estiver ociosa e alcançar um efeito de economia de energia.



- **Passo 3** - No campo Descrição da Porta, você pode nomear sua porta.
  - A descrição deve seguir estas regras: Não pode exceder 16 caracteres. Deve conter apenas números, letras e o caractere especial underline (_).



Porta	Descrição da porta	Tipo de mídia	Configuração de velocidade/duplex	Status de Duplex/velocidade	Controle de fluxo	Status de controle de fluxo	Config EEE
Porta 1		Cobre	AUTO	1000M_FULL	Desl.	Desl.	Desl.
Porta 2		Cobre	AUTO	DOWN	Desl.	Desl.	Desl.
Porta 3		Cobre	AUTO	DOWN	Desl.	Desl.	Desl.
Porta 4		Cobre	AUTO	DOWN	Desl.	Desl.	Desl.
Porta 5		Fibra	AUTO	DOWN	Desl.	Desl.	Não compatível.
Porta 6		Fibra	AUTO	DOWN	Desl.	Desl.	Não compatível.

Atualizar

Parâmetro	Descrição
Status de Velocidade/Duplex	◦ **Online:** Exibe a taxa da porta e o modo duplex . ◦ **Offline:** Exibe **DOWN**.
Controle de Fluxo Status do Controle de Fluxo	Exibe se a função de controle de fluxo está ativada e o status atual do controle de fluxo.
Configuração EEE	Exibe se a função EEE (Eficiência Energética Ethernet) está ativada.

Configurando VLAN

Você pode adicionar a porta à VLAN. Por padrão, a VLAN é a VLAN1.

Logicamente, uma LAN (Rede Local) pode ser dividida em muitos subconjuntos. Cada subconjunto possui sua própria área de transmissão (broadcast): VLAN (LAN virtual). Uma VLAN é dividida de uma LAN em uma base lógica, em vez de uma física, para realizar a área de transmissão isolada na VLAN.

Os tipos de porta incluem **Acesso** e **Tronco**.

Acesso: A porta pertence a uma única VLAN e é usada para conectar à porta do computador.

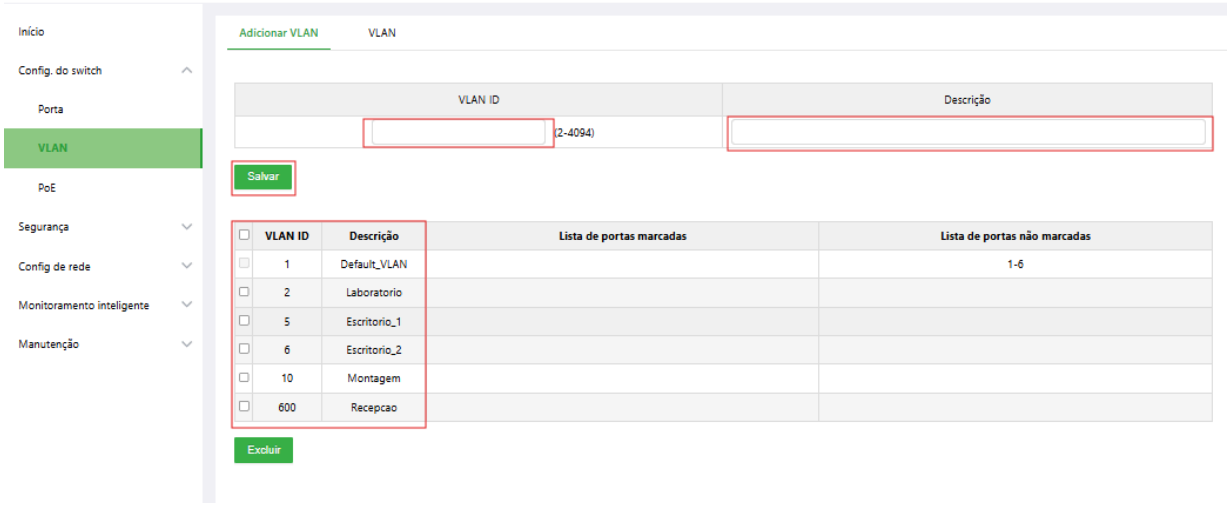
Trunk: A porta permite a passagem de múltiplas VLANs, para receber e enviar mensagens de várias VLANs, e é usada para a conexão entre os switches.

Procedimento

Passo 1: Selecione Config. do Switch > VLAN > Adicionar VLAN.

Passo 2: Insira o ID da VLAN e a descrição, e então clique em Salvar.

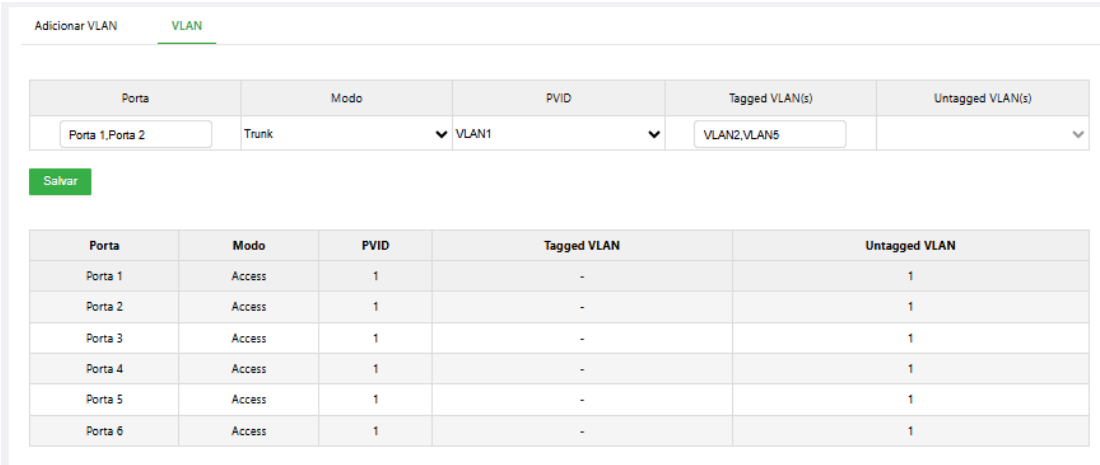
Selecione a VLAN e clique em Excluir para excluir a VLAN. A VLAN1 não pode ser excluída.



Passo 3: Clique na aba VLAN para configurar os parâmetros de VLAN da porta.

1 - Selecione uma ou mais portas.

2 - Selecione o modo da VLAN, incluindo **Access** (Acesso) e **Trunk** (tronco)



3 - Configure PVID, VLAN com tag (tagged) e VLAN sem tag (untagged).

Access (Acesso): você deve configurar a VLAN sem tag (untagged VLAN). A VLAN sem tag indica o ID da VLAN para a porta que tem permissão para ser enviada sem etiqueta ao transmitir pacotes.

Trunk (Tronco): você deve configurar o PVID e a VLAN com tag (tagged VLAN). O PVID indica que a porta foi adicionada a uma VLAN. Por padrão, a porta pertence à VLAN 1. Trata-se do ID da VLAN para a porta que tem permissão para ser etiquetada (com tag) ao enviar pacotes.

Tipo de Porta	**Processamento de quadros sem etiqueta (untagged)**	**Processamento de quadros com etiqueta (tagged)**	**Transmissão de quadros**
Access (Acesso)	Recebe um quadro sem etiqueta e adiciona uma etiqueta com o ID da VLAN padrão ao quadro.	▪ Aceita o quadro com etiqueta se o ID da VLAN do quadro coincidir com o ID da VLAN padrão ▪ Descarta o quadro com etiqueta se o ID da VLAN do quadro for diferente do ID da VLAN padrão.	Após a etiqueta PVID ser removida, o quadro é transmitido.

Tipo de Porta	Processamento de quadros sem etiqueta (untagged)	Processamento de quadros com etiqueta (tagged)	Transmissão de quadros
Trunk (Tronco)	▪ Adiciona uma tag com o ID da VLAN padrão a um quadro sem tag e aceita o quadro se a interface permitir o ID da VLAN padrão. ▪ Adiciona uma tag com o ID da VLAN padrão a um quadro sem tag e descarta o quadro se a interface negar o ID da VLAN padrão.	▪ Aceita um quadro com tag se o ID da VLAN contido no quadro for permitido pela interface . ▪ Descarta um quadro com tag se o ID da VLAN contido no quadro for negado pela interface.	▪ Se o ID da VLAN do quadro coincidir com o ID da VLAN padrão e for permitido pela interface, o dispositivo remove a tag e transmite o quadro ▪ Se o ID da VLAN do quadro for diferente da VLAN padrão, mas ainda permitido pela interface, o dispositivo transmitirá o quadro diretamente

PoE Management

O PoE (Power over Ethernet) permite que o switch utilize cabos de rede comuns para alimentar dispositivos externos (chamados de PD - Powered Devices) através de suas portas Ethernet. Essa tecnologia centraliza a distribuição de energia, o que facilita o uso de backups e elimina a necessidade de fontes de alimentação externas para cada terminal de rede; basta um único cabo para dados e energia.

Configuração Global

Você pode configurar o PoE perpétuo, a potência disponível e a potência de alerta.

Procedimento

Passo 1: Selecione **Config do Swich** > **PoE** > **Config Global**.

Passo 2: Selecione **PoE Perpétuo** e clique em **Salvar**.

Habilite o PoE perpétuo para permitir que os dispositivos conectados continuem recebendo energia mesmo após o switch ser reiniciado.

Passo 3: Configure a potência disponível e a potência de alerta.

No final da página, são exibidos: a potência total, potência disponível, potência de alerta, consumo de energia, potência reservada, potência restante e o status do PoE perpétuo. Potência reservada = Potência total – Potência de alerta.

- A potência de alerta deve ser maior que a potência disponível.
- Refere-se à potência máxima que pode ser fornecida aos dispositivos conectados. Quando o consumo atual é menor que a potência disponível, novos dispositivos podem ser ligados.
- Durante o funcionamento, o uso real de energia pode flutuar. Quando o consumo excede a potência de alerta, as portas terão o fornecimento de energia cortado da menor para a maior prioridade (quanto maior o número da porta, menor a prioridade), até que o consumo de energia seja inferior à potência de alerta.

Passo 4: Clique em **Salvar**.

Configuração da Porta

Ajuste as funcionalidades PoE para cada porta individualmente.

Procedimento

Passo 1: Selecione Switch Config > PoE > Port Config (Configuração do Switch > PoE > Configuração de Porta).

Passo 2: Selecione o número da porta e habilite as funções PoE, Long Distance PoE, PD alive e Force PoE, conforme necessário.

PoE: O dispositivo utiliza cabos de rede para conectar-se externamente a um PD (Powered Device) para fornecimento de energia remota através das portas elétricas Ethernet.

Long Distance PoE (PoE de Longa Distância): Após ativar esta função, a distância máxima de transmissão mudará de 100 m para 250 m, e a velocidade de transmissão será reduzida para 10 Mbps.

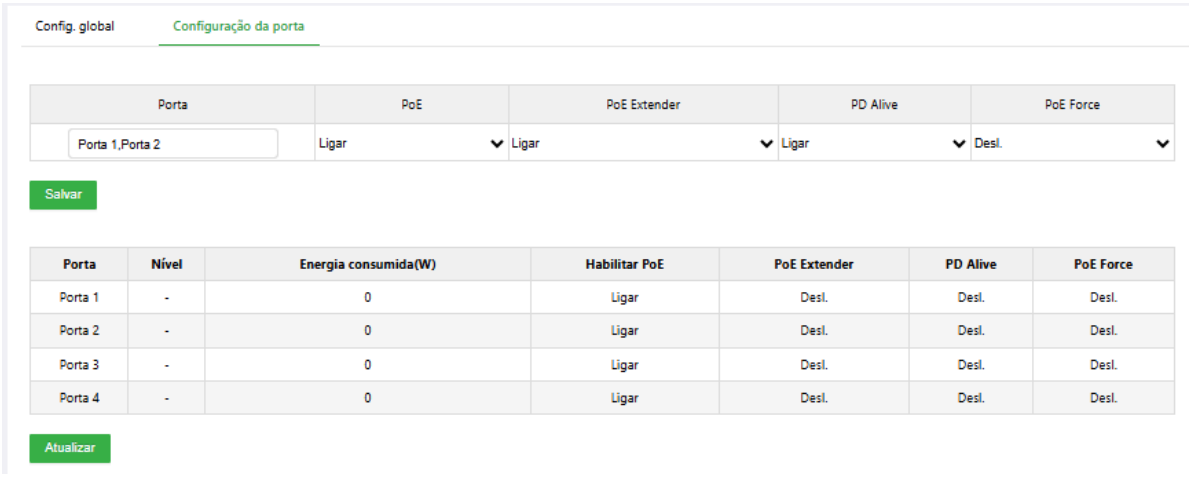
> A distância real de transmissão pode variar dependendo do consumo de energia dos dispositivos conectados ou do tipo e estado do cabo.

PD Alive Com esta função ativada, você pode monitorar o PD para mantê-lo online e verificar seu status com base em intervalos de tempo. Se não houver transmissão de dados, a porta PoE será automaticamente desligada e reiniciada. Os intervalos de tempo para as verificações aumentam progressivamente, começando em 1 minuto e dobrando a cada vez (1, 2, 4, 8, 16, etc.), até o intervalo máximo de 1024 minutos.

Force PoE (PoE Forçado): Quando o dispositivo alimentado conectado à porta é um modelo não padrão, utilize esta função para forçar o fornecimento de energia PoE.

> Após habilitar o Force PoE, a porta forçará a alimentação do dispositivo, independentemente de ele atender ou não aos requisitos padrão.

> As funções **Force PoE** e **PD Alive** não podem ser ativadas simultaneamente na mesma porta.



Passo 3: Clique em **salvar**.

Parâmetro	**Descrição**
Nível	Exibe o nível de fornecimento de energia dos dispositivos terminais. O nível de fornecimento varia de 0 a 8, e o nível padrão de alimentação Hi-PoE é exibido como 5+.
Power Consumption(W) (Consumo de Energia)	Exibe a potência PoE atual consumida pela respectiva porta individual.

Parâmetro	Descrição
PoE Enable (Habilitar PoE) Long Distance PoE (PoE de Longa Distância) PD Alive Force PoE (PoE Forçado)	Exibe se a função PoE está habilitada para a porta.

Segurança

Configurando o Isolamento de Portas

O isolamento de portas serve para alcançar o isolamento de mensagens na Camada 2. A função de isolamento de portas oferece aos usuários uma solução de rede mais segura e flexível.

Procedimento

Passo 1: Selecione Security > Port Isolation (Segurança > Isolamento de Portas).

Passo 2: Ative a separação de portas.

> Após o isolamento de portas ser ativado, as portas de download (downlink) serão isoladas entre si, enquanto as portas de upload (uplink) não serão isoladas. (Os dados só podem ser transferidos entre portas uplink and downlink) .

Passo 3: Clique em **Salvar.**

Configurando Storm Control

Os quadros de transmissão (broadcast) na rede são encaminhados continuamente, o que afeta as comunicações adequadas e reduz drasticamente o desempenho da rede. O controle de tempestade pode limitar os fluxos de transmissão da porta e descartar os quadros de transmissão assim que o fluxo exceder o limite especificado. Isso pode reduzir o risco de uma

tempestade de transmissão e garantir a operação correta da rede.

Procedimento

Passo 1: Selecione Security > Storm Control (Segurança > Controle de Tempestade).

Passo 2: Selecione o **tipo** e a **porta**, habilite o controle de tempestade e insira a **velocidade**.

Passo 3: Clique em **Salvar.**

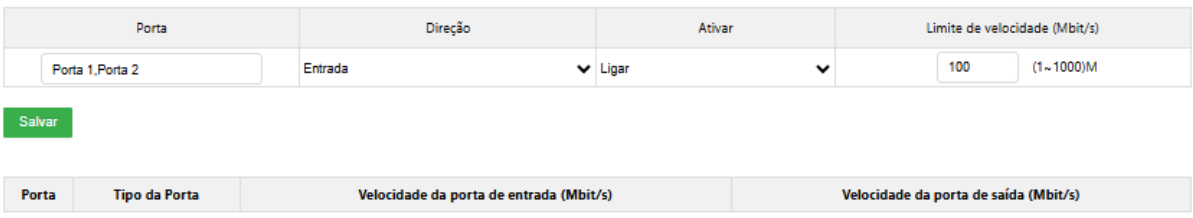
Configurando o limite de Velocidade da porta

Configure a política de limitação de taxa das portas para controlar o fluxo de pacotes de dados que entram e saem da porta em uma taxa desejada.

Procedimento

Passo 1: Selecione Security > Port Speed Limit (Segurança > Limite de Velocidade da Porta).

Passo 2: Selecione a porta e a direção, ative o limite de velocidade da porta e, em seguida, insira a velocidade.



Passo 3: Clique em **Salvar.**

Configurações de Rede

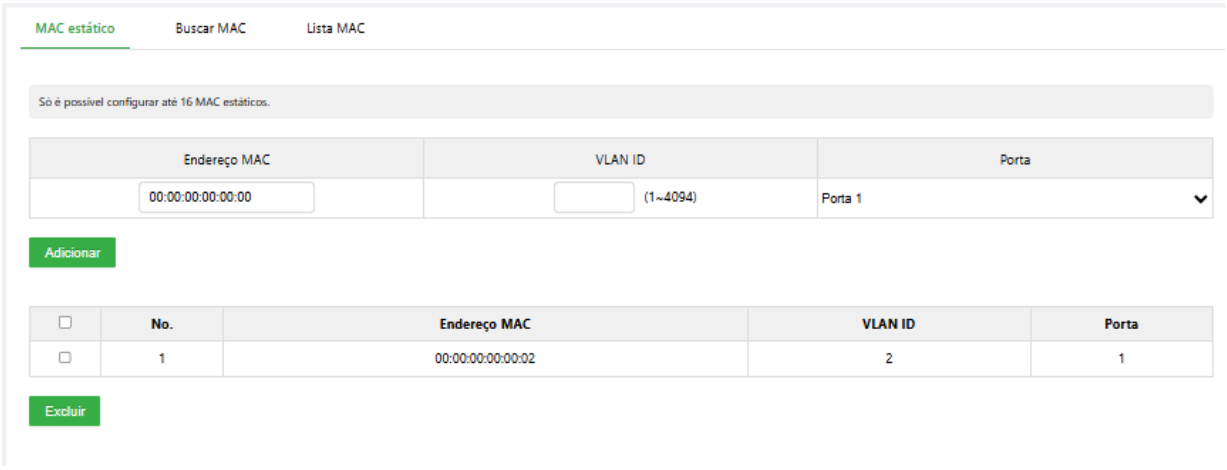
Configurando tabela MAC

A Tabela MAC (Media Access Control) registra a relação entre o endereço MAC e a porta, incluindo informações como a VLAN à qual a porta pertence. Quando o dispositivo está encaminhando um pacote, ele consulta na tabela de endereços MAC o endereço MAC de destino do pacote. Se o endereço MAC de destino estiver contido na tabela, o pacote é encaminhado diretamente através da porta indicada. Caso o endereço MAC de destino não conste na tabela, o dispositivo adota o modo de transmissão (broadcasting) para encaminhar o pacote para todas as portas da VLAN, exceto para a porta receptora.

Passo 1: Selecione Network Settings > MAC Management > Static MAC para visualizar as informações da tabela MAC.

Passo 2: Configure o endereço MAC, o ID da VLAN e a porta; em seguida, clique em Add (Adicionar).

- Você pode configurar apenas até 16 MACs estáticos.
- Para excluir um MAC estático, selecione-o e clique em Excluir.



Passo 3: Clique na aba MAC Search (Busca de MAC), insira o endereço MAC ou selecione a porta e, em seguida, clique em Search (Buscar) para pesquisar rapidamente o endereço MAC.

Passo 4: Clique na aba MAC List (Lista de MAC) e visualize os endereços MAC.

Podem ser exibidos até 100 itens.

Para pesquisar mais informações, utilize a função MAC Search.

Clique em Clear (Limpar) e depois em OK para apagar as informações.

Configuração de Proteção contra Loop

Selecione Network Settings > Loop Protection (Configurações de Rede > Proteção contra Loop), habilite a proteção contra loop e clique em Save (Salvar). Após a ativação, se um loop for detectado, a porta que causou o problema será desativada e, em seguida, restaurada automaticamente assim que o loop for eliminado.

Configuração de STP

O Protocolo de Árvore de Abrangência (Spanning Tree Protocol - STP) cria uma topologia lógica livre de loops para redes locais (LANs). Ele bloqueia links redundantes entre quaisquer dois dispositivos de rede, mantendo apenas um único link ativo entre eles para eliminar os loops.

Os protocolos STP, RSTP e MSTP oferecem as seguintes capacidades:

STP: É um protocolo de gerenciamento na camada de enlace de dados, utilizado para detectar e prevenir loops em uma rede de Camada 2. No entanto, sua convergência da topologia de rede é lenta.

RSTP: Uma melhoria do STP que permite uma convergência rápida da topologia de rede. Contudo, tanto o RSTP quanto o STP possuem a limitação de que todas as VLANs na mesma rede compartilham a mesma instância de spanning tree.

MSTP: Utiliza uma tabela de mapeamento de VLAN virtual onde os IDs das VLANs são associados a instâncias de spanning tree. Além disso, o MSTP divide uma rede de comutação em múltiplas regiões, cada uma com várias instâncias de spanning tree independentes entre si. Diferente do STP e RSTP, le MSTP oferece múltiplos caminhos redundantes para o encaminhamento de dados e implementa o balanceamento de carga entre as VLANs.

STP

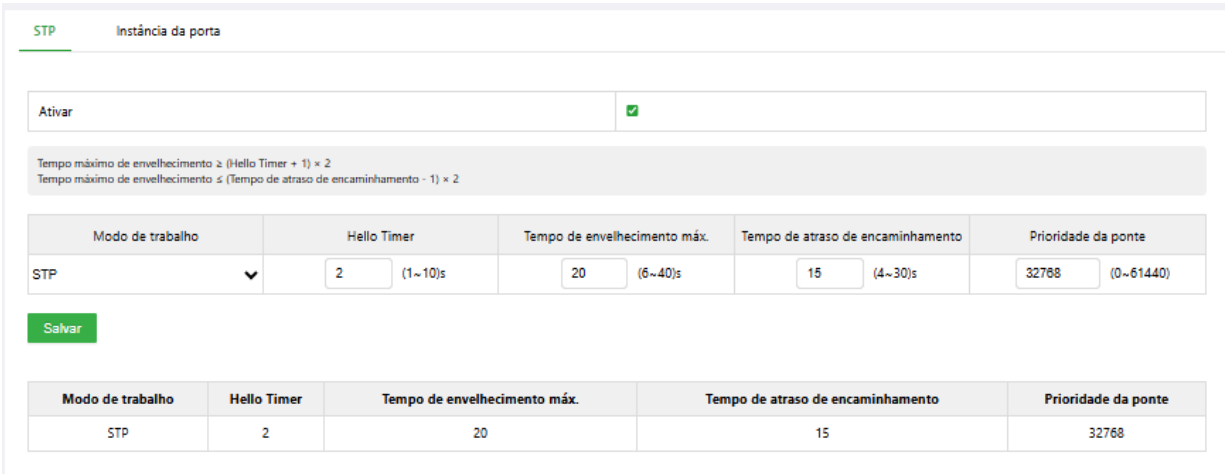
Procedimento

Passo 1: Selecione **Configurações de rede** > **STP** > **STP**.

Passo 2: Habilite o **STP**.

Passo 3: Selecione o modo de operação, incluindo **STP** e **RSTP**.

Passo 4: Configure os parâmetros.

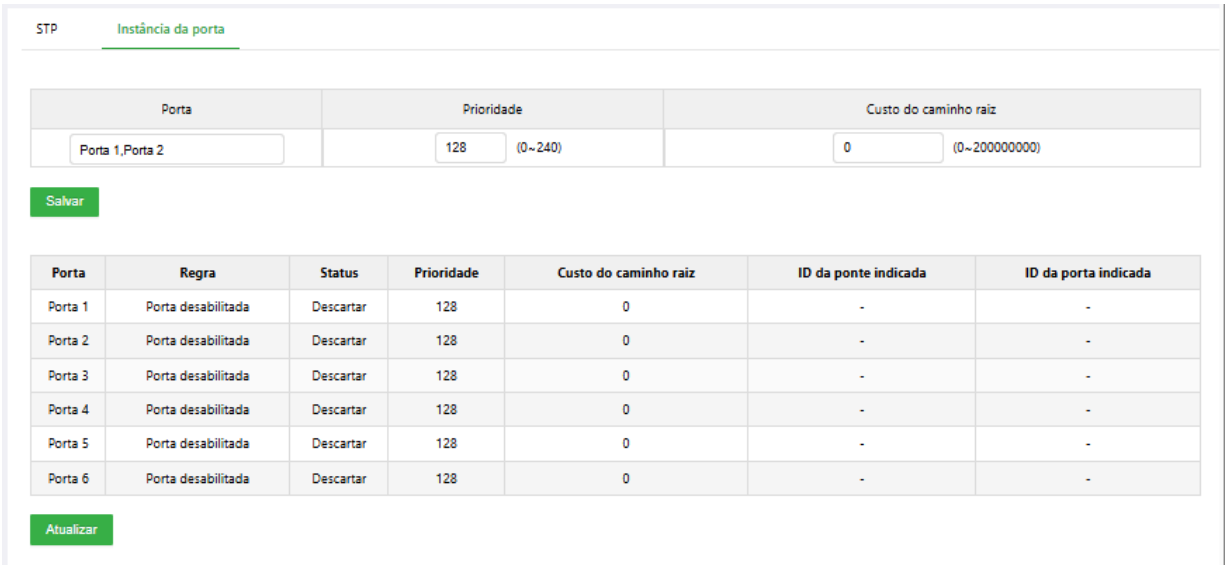


Passo 5: Clique em **Salvar**.

Instância de Porta

Selecione **Configurações de rede** > **STP** > Instância de porta, escolha a porta, insira a prioridade e o custo do caminho raiz e, em seguida, clique em Salvar.

- O valor da Prioridade varia de 0 a 240 e deve ser um múltiplo integral de 16.
- O valor padrão da Prioridade é 128.



Configuração de Agregação de Link

A agregação de link consiste em agrupar múltiplas portas físicas do switch para formar uma única porta lógica. Os múltiplos links no mesmo grupo podem ser considerados como um link lógico om uma clargura de banda maior. Através da agregação, as portas do mesmo grupo podem compartilhar o fluxo de comunicação para gerar uma banda maior. Além disso, as portas no mesmo grupo podem realizar backup recíproco e dinâmico para aumentar a confiabilidade do link.

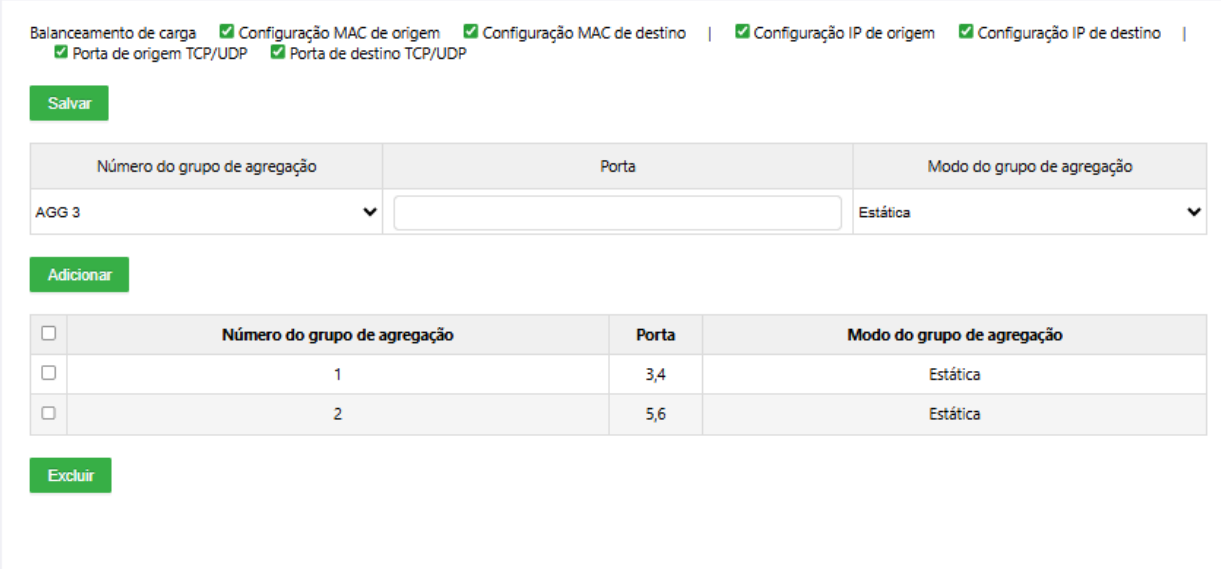
- Para estabelecer a agregação de link com sucesso, as configurações no dispositivo parceiro (peer) devem ser as mesmas deste dispositivo.
- A agregação de link está disponível apenas em modelos selecionados.

Procedimento:

Passo 1: Selecione Network Settings > Link Aggregation.

Passo 2: Na área Load Balancing (Equilíbrio de Carga), selecione o tipo e clique em Save.

Os tipos incluem: Configuração de MAC de Origem, Configuração de MAC de Destino, Configuração de IP de Origem, Configuração de IP de Destino, Porta de Origem TCP/UDP e Porta de Destino TCP/UDP.



Passo 3: Selecione o Número do Grupo de Agregação (Aggregation Group No.) e o número da porta.

O modo do grupo de agregação é Estático (Static) por padrão.

> Atenção: Portas com Controle de Tempestade (Storm Control) ou Limite de Velocidade (Port Speed Limit) habilitados não podem ser adicionadas a grupos de agregação.

Passo 4: Clique em Add (Adicionar).

Para remover, selecione o grupo de agregação e clique em Delete (Excluir).

Monitoramento Inteligente

Estatísticas da porta

Procedimento

Passo 1: Acesse Monitoramento Inteligente > Estatísticas da porta.

Passo 2: Visualize o tipo da porta e o uso de recebimento e envio.

Porta	Tipo da Porta	Uso de RX	Uso de TX	Bytes (KB) RX/TX	Pacote RX/TX bem-sucedido	Pacote RX/TX com falha
Porta 1	Porta física	0.01%	0.01%	1.07MB/826.02KB	6752/5539	0/0
Porta 2	Porta física	0%	0%	0.00B/0.00B	0/0	0/0
Porta 3	Porta física	0%	0%	0.00B/0.00B	0/0	0/0
Porta 4	Porta física	0%	0%	0.00B/0.00B	0/0	0/0
Porta 5	Porta física	0%	0%	0.00B/0.00B	0/0	0/0
Porta 6	Porta física	0%	0%	0.00B/0.00B	0/0	0/0

Reiniciar

Lista de Dispositivos (LLDP)

O LLDP (Link Layer Discovery Protocol) é um método padrão de descoberta na camada de enlace. Ele organiza suas principais capacidades, endereço de gerenciamento, número do dispositivo e número da porta no formato TLV (Type Length Value), encapsula essas informações em uma LLDPDU (Link Layer Discovery Protocol Data Unit) e as envia para seus vizinhos. O dispositivo vizinho armazena as informações recebidas em uma MIB (Management Information Base) padrão, permitindo que o gerenciamento de rede consulte e avalie o estado de comunicação do link.

Procedimento

Passo 1: Selecione Network Monitoring > Device List (Monitoramento de Rede > Lista de Dispositivos).

Passo 2: Habilite o LLDP e clique em Salvar.

Passo 3: Visualize as informações do dispositivo remoto descoberto via LLDP.

LLDP ☑

Salvar

Porta	Nome da porta remota	Nome do dispositivo	Endereço MAC	IP
Porta 1	[redacted]		[redacted]	

Manutenção

Configurando o Espelhamento de Porta (Port Mirroring)

O espelhamento consiste em copiar o tráfego recebido, enviado (ou ambos) de uma origem específica para uma porta de destino para fins de análise. A origem especificada é chamada de origem espelhada (mirrored source), a porta de destino é chamada de porta de observação (observing port), e o tráfego copiado é conhecido como tráfego espelhado.

O espelhamento envia uma cópia dos dados através da porta de observação do switch para um dispositivo de monitoramento, permitir a análise de serviços e tráfego.

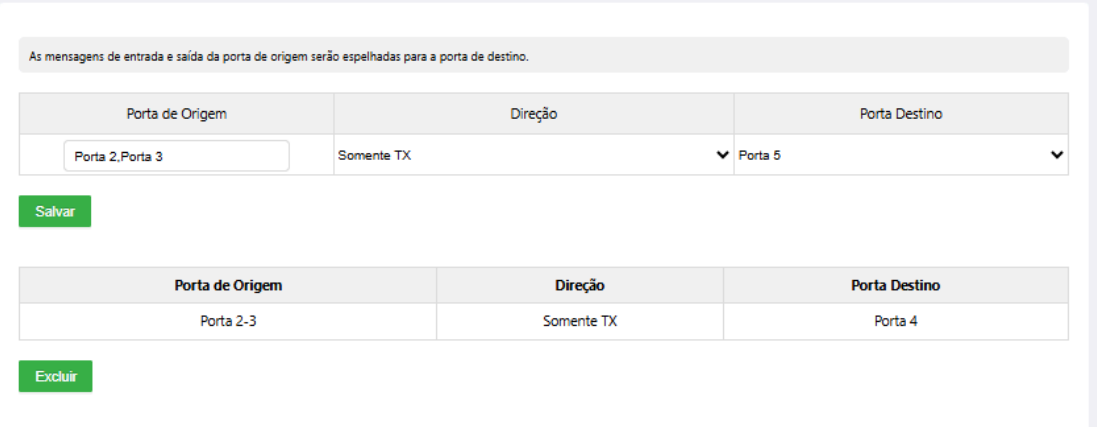
Procedimento

Passo 1: Selecione Maintenance > Port Mirroring (Manutenção > Espelhamento de Porta).

Passo 2: Selecione a porta de origem, a direção e a porta de destino.

As direções incluem Tx Only, Rx Only e Both:

- Tx Only: Suporta apenas o envio de tráfego.
- Rx Only: Suporta apenas o recebimento de tráfego.
- Both: Suporta tanto o envio quanto o recebimento de tráfego.



Passo 3: Clique em Salvar

Configuração de Firmware

Restaurar Padrão de Fábrica

Passo 1: Selecione Maintenance > Firmware Config (Manutenção > Configuração de Firmware).

Passo 2: Clique em Default (Padrão), digite a senha e clique em OK.

- **Todos os parâmetros retornam às configurações de fábrica, exceto o endereço IP, máscara de sub-rede, gateway e DNS.**
- **Você pode restaurar todos os parâmetros (incluindo as configurações de rede) através do botão físico de reset.**

Atualização de Software

Procedimento

Passo 1: Selecione Manutenção > **Configuração de Firmware**.

Passo 2: Clique em **Procurar** para importar o arquivo de atualização e, em seguida, clique em Update **Atualizar**.

Passo 3: Clique em **OK**.

> A atualização do software pode levar cerca de 3 minutos. Após a atualização, o sistema será reiniciado automaticamente.

Reiniciar Dispositivo

- Selecione **Manutenção** > **Configuração de Firmware**, clique em **Reiniciar** e, em seguida, clique em **OK**.

Alterando a Senha

Procedimento

Passo 1: Selecione **Manutenção** > **Alterar Senha**.

Passo 2: Insira a senha antiga, a nova senha e confirme a nova senha.

> A senha deve ser composta por 8 a 32 caracteres (sem espaços) e conter pelo menos dois tipos de caracteres entre: letras maiúsculas, letras minúsculas, números e caracteres

especiais (exceto os símbolos ' " ; : &).

Passo 3: Clique em **Salvar**

Configurando a Rede

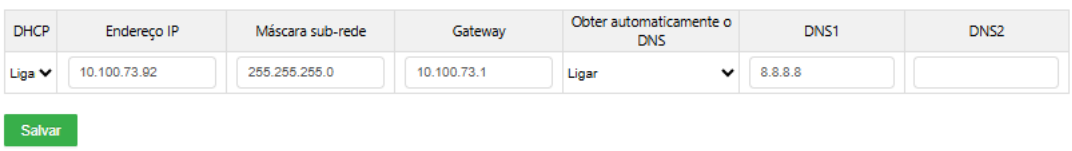
Configure o endereço IP e o servidor DNS.

Procedimento

Passo 1: Selecione Manutenção > Rede.

Passo 2: Configure os parâmetros.

- **Habilitar DHCP:** Ao ativar o DHCP, um novo endereço IP será adquirido e atribuído automaticamente ao dispositivo.
- **Desabilitar DHCP:** Insira manualmente o endereço IP, a máscara de sub-rede e o gateway para configurar um endereço IP estático.
- **Habilitar Obtenção Automática de DNS:** O dispositivo obtém automaticamente o endereço IP do servidor DNS disponível na rede.
- **Desabilitar Obtenção Automática de DNS:** Insira manualmente os endereços IP do DNS1 e DNS2.



Visualizando Informações do Dispositivo

Selecione **Manutenção** > **Informações do Dispositivo**; aqui você pode visualizar dados como o nome do dispositivo, versão do software, endereço MAC e tempo de atividade.

Visualizando Informações de Log

Selecione **Manutenção** > **Informações de registro** para visualizar os registros de eventos do sistema.

Visualizando Informações Legais

Manutenção > **Declaração Legal** e clique na aba correspondente para visualizar o contrato de licença de software, a política de privacidade e os avisos de software de código aberto.

Recomendações de Segurança

Gerenciamento de Contas

1. **Use senhas complexas Siga estas sugestões para configurar senhas:**

   Por favor, consulte as seguintes sugestões para configurar senhas:

   - O comprimento não deve ser inferior a 8 caracteres.
   - Inclua pelo menos dois tipos de caracteres: letras maiúsculas e minúsculas, números e símbolos.
   - Não utilize o nome da conta (nem na ordem inversa).
   - Não use sequências de caracteres (ex: 123, abc).
   - Não use caracteres repetidos (ex: 111, aaa).

2. **Altere as senhas periodicamente**

   Recomenda-se alterar a senha do dispositivo regularmente para reduzir o risco de

adivinhação ou quebra por força bruta.

3. **Atribua contas e permissões adequadamente**

   Adicione usuários conforme as necessidades de serviço e atribua apenas o conjunto mínimo de permissões necessário.

4. **Habilite a função de bloqueio de conta**

   Esta função vem ativada por padrão e deve ser mantida assim. Após várias tentativas falhas, o acesso da conta e do IP de origem será bloqueado.

5. **Atualize as informações de recuperação de senha**

   O dispositivo suporta o reset de senha. Mantenha as informações de segurança atualizadas e evite usar respostas óbvias em perguntas de segurança.

Configuração de Serviço

1. **Habilite o HTTPS**

   Recomenda-se o acesso via HTTPS para garantir canais de comunicação seguros.

2. **Criptografia de áudio e vídeo**

   Se os dados forem sensíveis, use a transmissão criptografada para evitar interceptações durante o envio.

3. **Desative serviços não essenciais e use o modo seguro**

   Se não forem necessários, recomenda-se desligar alguns serviços, tais como SSH, SNMP, SMTP, UPnP, hotspot AP, etc., para reduzir as superfícies de ataque.

   Se necessário, é altamente recomendável escolher modos seguros, incluindo, mas não se limitando aos seguintes serviços:

   - SNMP: Utilize SNMP v3 com criptografia e autenticação fortes.
   - SMTP: Utilize TLS para acessar servidores de e-mail.
   - FTP: Utilize SFTP com senhas complexas.
   - AP hotspot: Utilize criptografia WPA2-PSK.

4. **Altere as portas padrão**

   Mude as portas padrão do HTTP e outros serviços para qualquer valor entre 1024 e 65535 para dificultar a identificação por invasores.

Configuração de rede

1. **Habilite a Lista de Permissões (Allow List)**

   Permita que apenas IPs específicos acessem o dispositivo.

2. **Vinculação de endereço MAC**

   Vincule o IP do gateway ao endereço MAC do dispositivo para evitar ataques de ARP spoofing.

3. **Construir um ambiente de rede seguro**

   Para garantir melhor a segurança dos dispositivos e reduzir potenciais riscos cibernéticos, recomenda-se le seguinte:

   - Desative a função de mapeamento de portas (port mapping) do roteador para evitar o acesso direto aos dispositivos da intranet a partir da rede externa;
   - Segmente a rede de acordo com as necessidades reais: se não houver demanda de comunicação entre duas sub-redes, recomenda-se o uso de VLAN, gateway e outros métodos para particionar a rede e alcançar le isolamento de rede;
   - Estabeleça um sistema de autenticação de acesso 802.1x para reduzir o risco de acesso de terminais ilegais à rede privada.

Auditoria de Segurança

1. **Verificar usuários online**

   Recomenda-se verificar os usuários online regularmente para identificar acessos ilegais.

2. **Verificar o log do dispositivo**

   Ao visualizar os logs, você pode obter informações sobre os endereços IP que tentam

fazer login no dispositivo e as principais operações realizadas pelos usuários logados.

3. **Configurar log de rede**

   Devido à capacidade de armazenamento limitada dos dispositivos, o log armazenado é restrito. Se precisar salvar os logs por um longo período, recomenda-se habilitar a função de log de rede para garantir que os registros críticos sejam sincronizados com um servidor de log de rede para rastreamento.

Segurança de Software

1. **Atualizar o firmware em tempo hábil**

   De acordo com as normas operacionais padrão da indústria, o firmware deve ser atualizado para a versão mais recente para garantir que o dispositivo possua as funções e segurança mais atuais. Se o dispositivo estiver conectado à rede pública, recomenda-se habilitar a função de detecção automática de atualização online.

2. **Atualizar o software cliente**

   Recomenda-se baixar e utilizar a versão mais recente do software cliente.

Proteção Física

Recomenda-se realizar a proteção física dos dispositivos (especialmente dispositivos de armazenamento), como colocá-los em uma sala de máquinas e rack dedicados, com controle de acesso e gerenciamento de chaves adequados para evitar que pessoal não autorizado danifique o hardware ou outros equipamentos periféricos (como pen drives USB ou portas seriais).

Termo de garantia

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

Nome do cliente:

Assinatura do cliente:

Nº da nota fiscal:

Data da compra:

Modelo:

Nº de série:

Revendedor:

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

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

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

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

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

5. A garantia perderá totalmente sua validade na ocorrência de quaisquer das hipóteses a seguir: a) se le 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 le 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.

Descarte adequadamente seu produto após vida útil - entregue em pontos de coleta de produtos eletroeletrônicos, em alguma assistência técnica autorizada Intelbras ou consulte nosso site www.intelbras.com.br e suporte@intelbras.com.br ou (48) 2106-0006 ou 0800 7042767 para mais informações.

Produto beneficiado pela Legislação de Informática.

Este equipamento deve ser conectado obrigatoriamente em tomada de rede de energia elétrica que possua aterramento (três pinos), conforme a Norma NBR ABNT 5410, visando a segurança dos usuários contra choques elétricos

intelbras

fale com a gente

Suporte a clientes: (48) 2106 0006

Fórum: forum.intelbras.com.br

Suporte via chat: intelbras.com.br/suporte-tecnico

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

SAC: 0800 7042767

Intelbras S/A – Indústria de Telecomunicação Eletrônica Brasileira

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

CNPJ 82.901.000/0014-41 - www.intelbras.com.br

Indústria Brasileira

ultima atualização