intelbras

Manual do Usuário

SG 2404D PoE Max

Versão deste manual: 1.0.1

SG 2404D PoE Max

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

O switch **SG 2404D PoE Max** possui 28 portas Gigabit Ethernet, sendo 24 portas RJ45 com a funcionalidade PoE e 4 portas RJ45 compartilhadas com 4 slots Mini-GBIC.

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

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

ÍNDICE

EXPORTAR PARA PDF

PROTEÇÃO E SEGURANÇA DE DADOS

- Tratamento de dados pessoais
- Diretrizes que se aplicam aos funcionários da Intelbras
- Diretrizes que controlam o tratamento de dados
- Uso indevido e invasão de hackers
- Informação

ACESSO A INTERFACE DE GERENCIAMENTO

- Login

INÍCIO

- Informações das portas
- Port
- VLAN
- Maintenance

SWITCHING

- DHCP Relay
- DHCP Snooping
- Spanning Tree
- LLDP Configuration
- IGMP Snooping
- MAC Settings

ROUTING

- Static Routing
- ARP
- DHCP Server

QoS POLICY

- QoS Scheduler
- 802.1P
- DSCP
- Port Priority

NETWORK SECURITY

- ACL
- MAC Filtering
- 802.1X
- Attack Defense

DEVICE SETTINGS

- User Management
- SNMP
- System Time
- Log Management
- Diagnostics
- Time Period

VISUALIZATION

- Global Map
- Device List

PoE MANAGEMENT

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.

> Esse produto vem com uma senha-padrão de fábrica. Para sua segurança, é IMPRESCINDÍVEL que você a troque assim que instalar o produto e questione o seu técnico quanto as senhas configuradas, quais os usuários que possuem acesso e os métodos de recuperação.

ACESSO A INTERFACE DE GERENCIAMENTO

Login

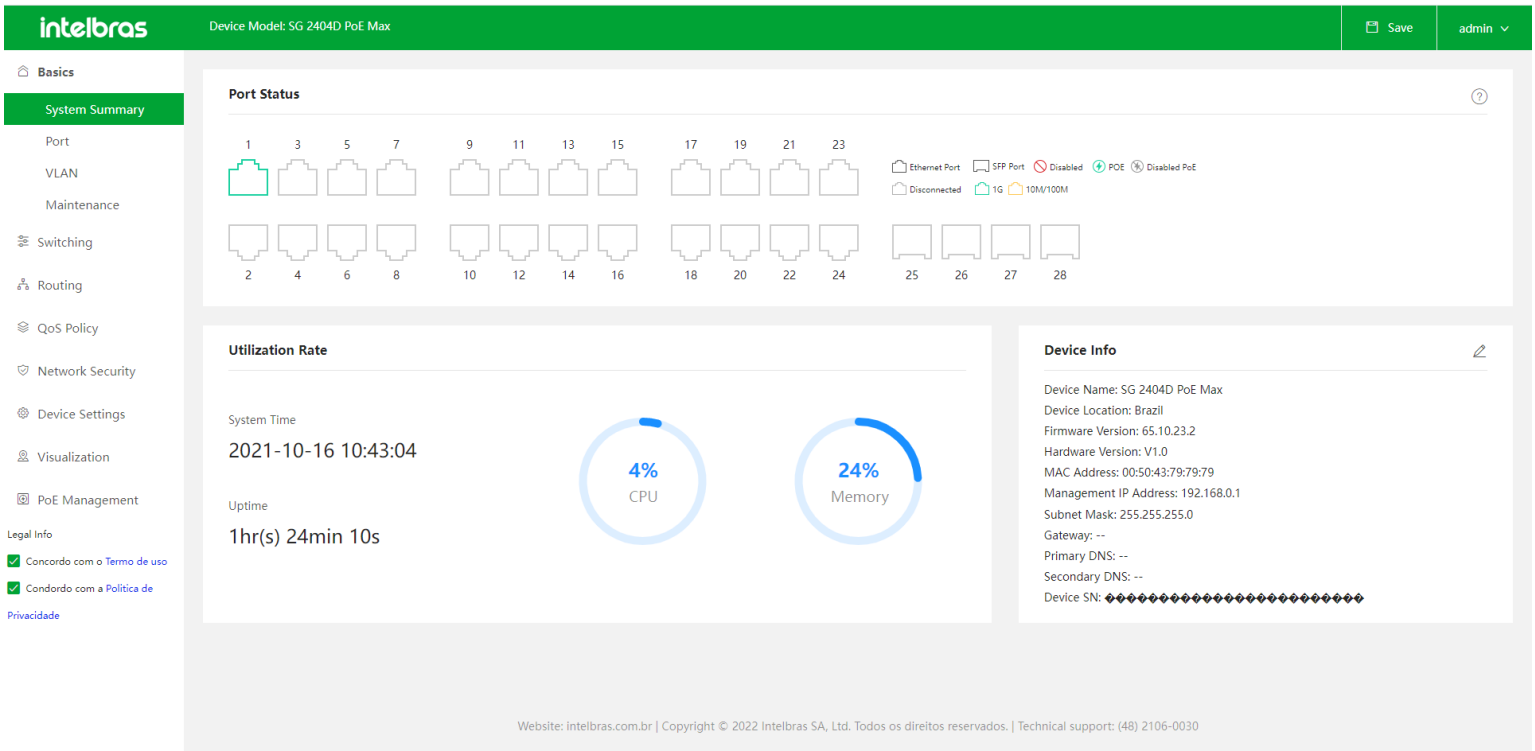
Para acessar a interface de gerenciamento do switch, abra o navegador e na barra de endereços digite o endereço IP de gerência do switch. http://192.168.0.1 (http://192.168.0.1), pressione a tecla Enter.

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

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

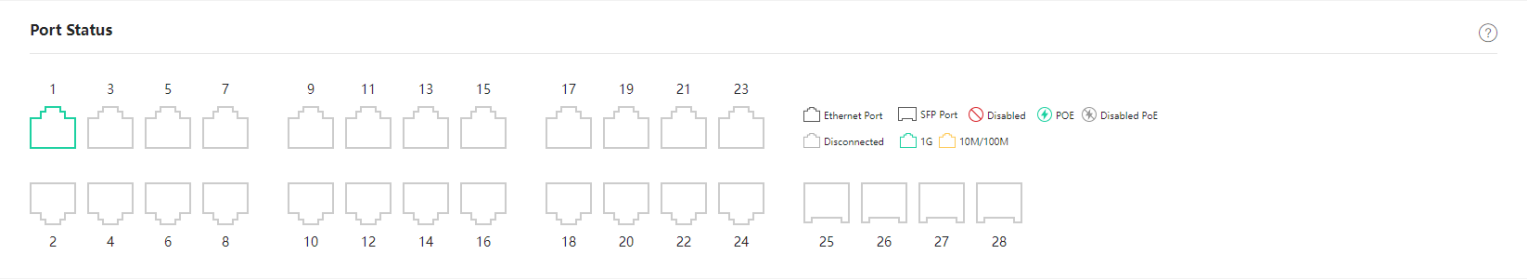
Basics

System Summary

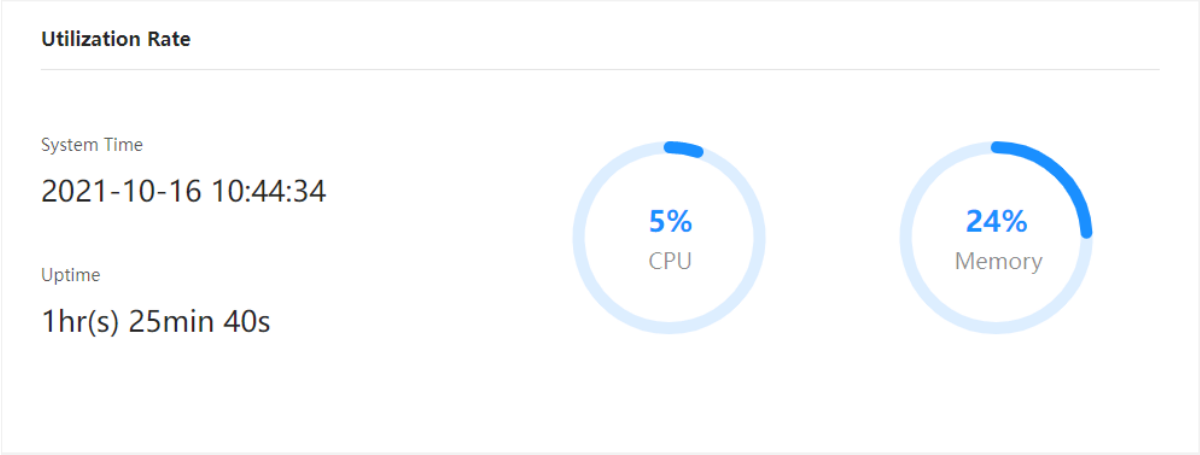


Após o login no equipamento será exibida o "Port Status", com uma ilustração das portas do switch e seus respectivos status. Ao lado da ilustração temos uma legenda, que mostra como ficará a representação da porta quando ela estiver com o respectivo status. Ainda nesta tela podemos ver mais inforamações sobre o status de cada porta, ao colocar o

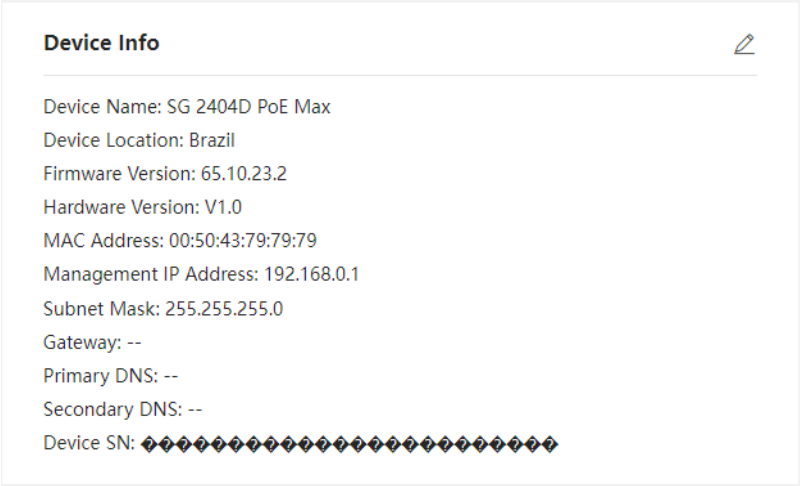
cursor do mouse sobre a porta serão exibidas informações sobre status, modo e velocidade da porta.



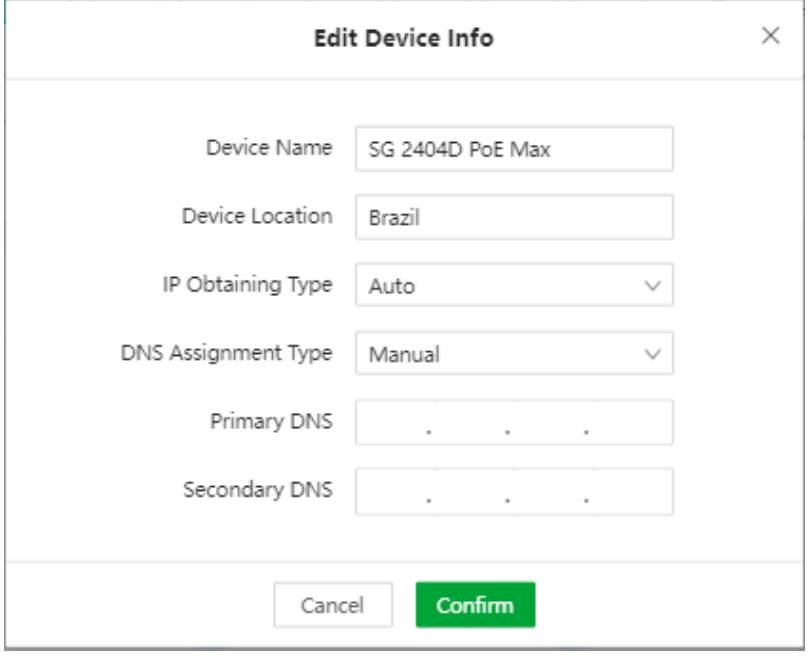
Na parte inferior esqueda da tela temos o "Utilization Rate", que trás informações do atual horário do Switch, do Uptime e dois indicadores com o percentual de CPU e memória RAM utilizados atualmente.



Na parte inferior direita da tela temos o "Device Info", que trás diversas informações do produto. Podemos observar as seguintes Informações sobre o Device: Nome, localização, versão de firmware, versão de harware, endereço MAC, endereço IP de gerência, máscara de rede, gateway, DNS primário, DNS secundário e número de série.



Em "Device Info" temos a presença de um botão de edição, ao clicar neste botão será aberta a tela "Edit Device Info".



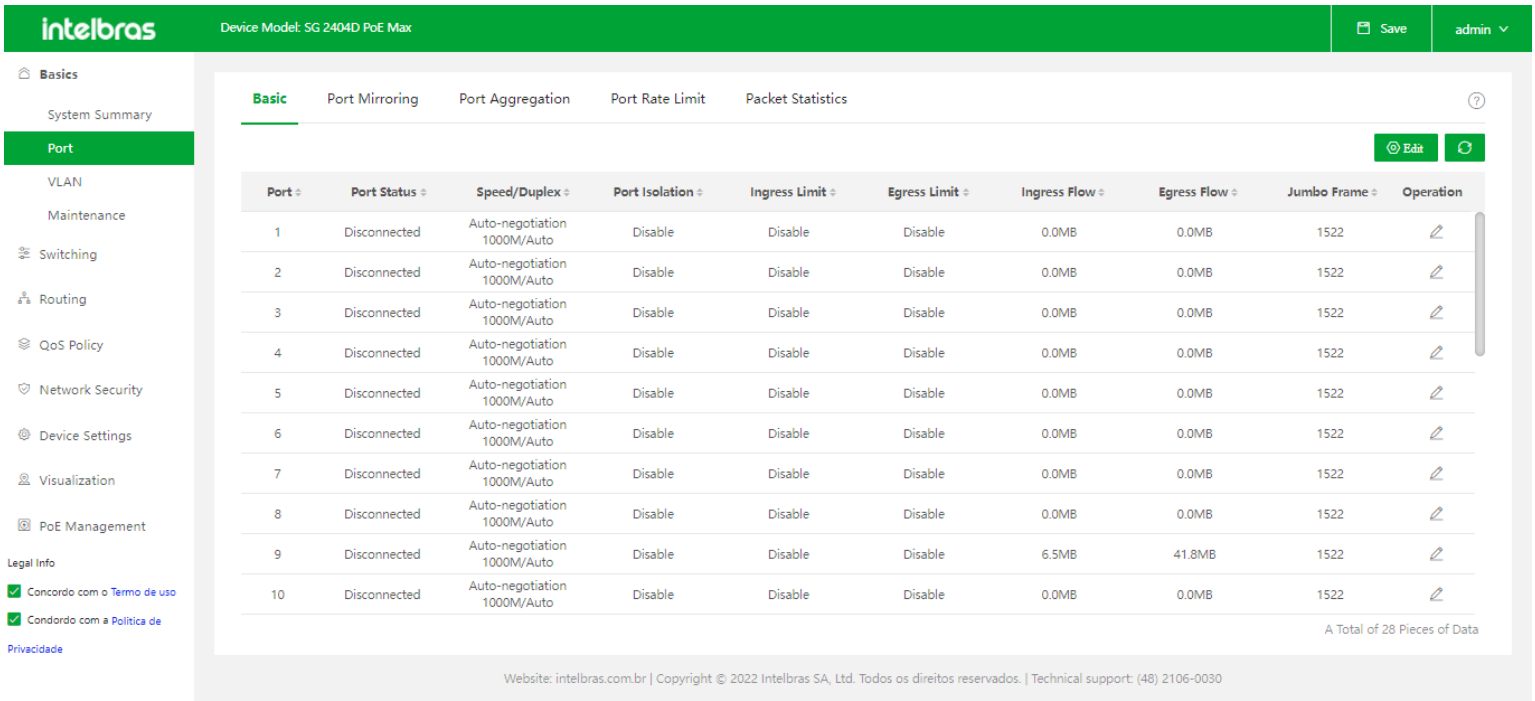
Nesta tela temos a possibilidade de alterar as seguintes informações:

Nome do dispositivo, localização, tipo de obtenção de IP (Manual ou automático/DHCP), endereço de IP e máscara, tipo de atibuição de DNS (só será possível deixar em automático quando a forma de obter IP também estiver em automática), DNS primário e secundário.

Port

Neste tópico temos acesso a configurações e status referente as portas físicas do Switch.

Basic



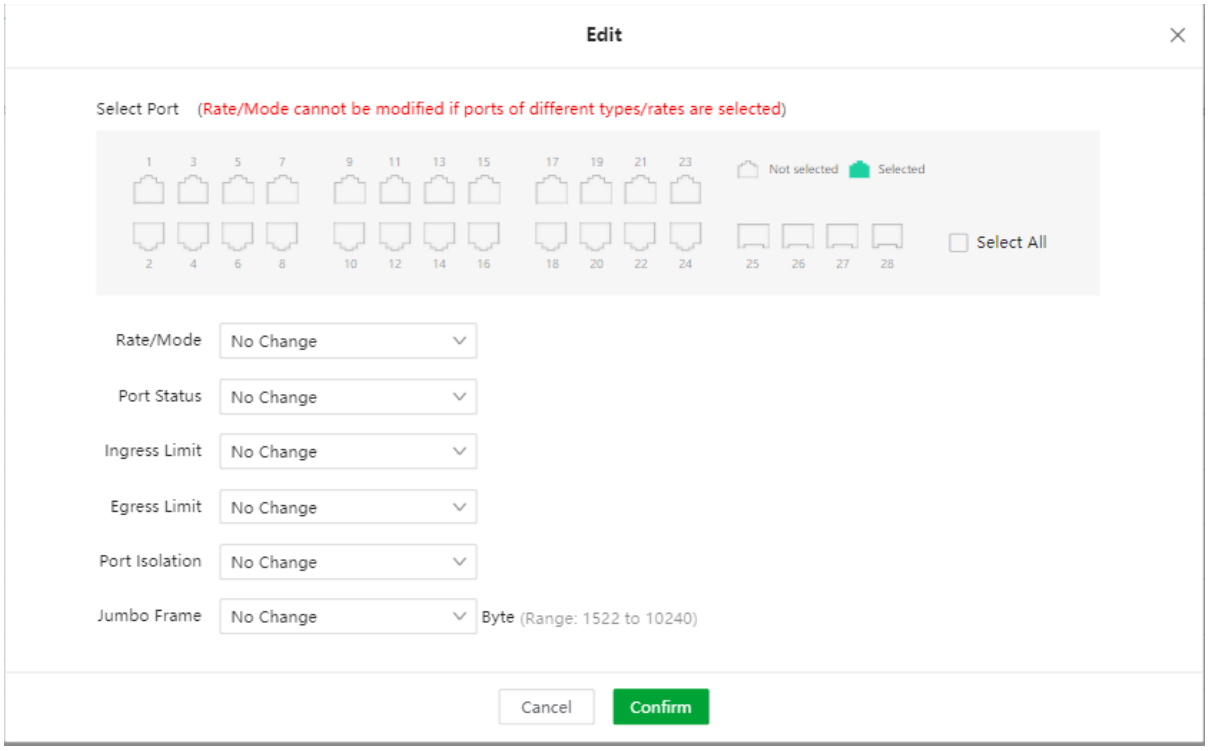
Ao abrir a página Basic, temos acesso a informações de status das interfaces físicas do Switch. São apresentadas as seguintes informações:

- **Port:** trás o número da interface fisica.

- **Port Status:** informa o status da respectiva interface física, informando se ela está conectada ou desconectada.
- **Speed/Duplex:** especifica a velocidade de negociação e o modo duplex de uma porta. HDX: Half duplex, FDX: Full duplex.
- **Port Isolation:** especifica o grupo de isolamento ao qual a porta pertence. As portas pertencentes a diferentes grupos de isolamento poderão se comunicar umas com as outras, enquanto as portas pertencentes ao mesmo grupo não poderão. As portas que não estão atribuídas a nenhum grupo de isolamento serão exibidas no estado "Disable", dessa forma poderão se comunicar com todas as portas.
- **Ingress Limit:** com a função em Enable, o fluxo de entrada da porta será monitorado. Quando um congestionamento ocorrer no fluxo de entrada da porta, o sistema irá enviar um Pause Frame para notificar que o dispositivo deve interromper ou diminuir a sua velocidade de transmissão por um determinado periodo de tempo.
- **Egress Limit:** com a função habilitada, quando o sistema receber um PAUSE frame do dispositivo conectado a porta, o sistema para ou diminui a velocidade da transmissão de dados por um período de tempo determinado para evitar a perda de pacotes e retransmissões.
- **Ingress Flow:** especifica as estatísticas de tráfego de dados recebidos pela porta.
- **Egress Flow:** especifica as estatísticas de tráfego de dados transmitidos pela porta.
- **Jumbo Frame:** especifica o tamanho do pacote que pode ser recebido ou transmitido pela porta. Os pacotes que excederem esse tamanho serão descartados. O valor padrão é 1522.
- **Botão Edit:** no canto superior direito da tela "Basic", conforme imagem anterior, temos a presença do botão Edit.

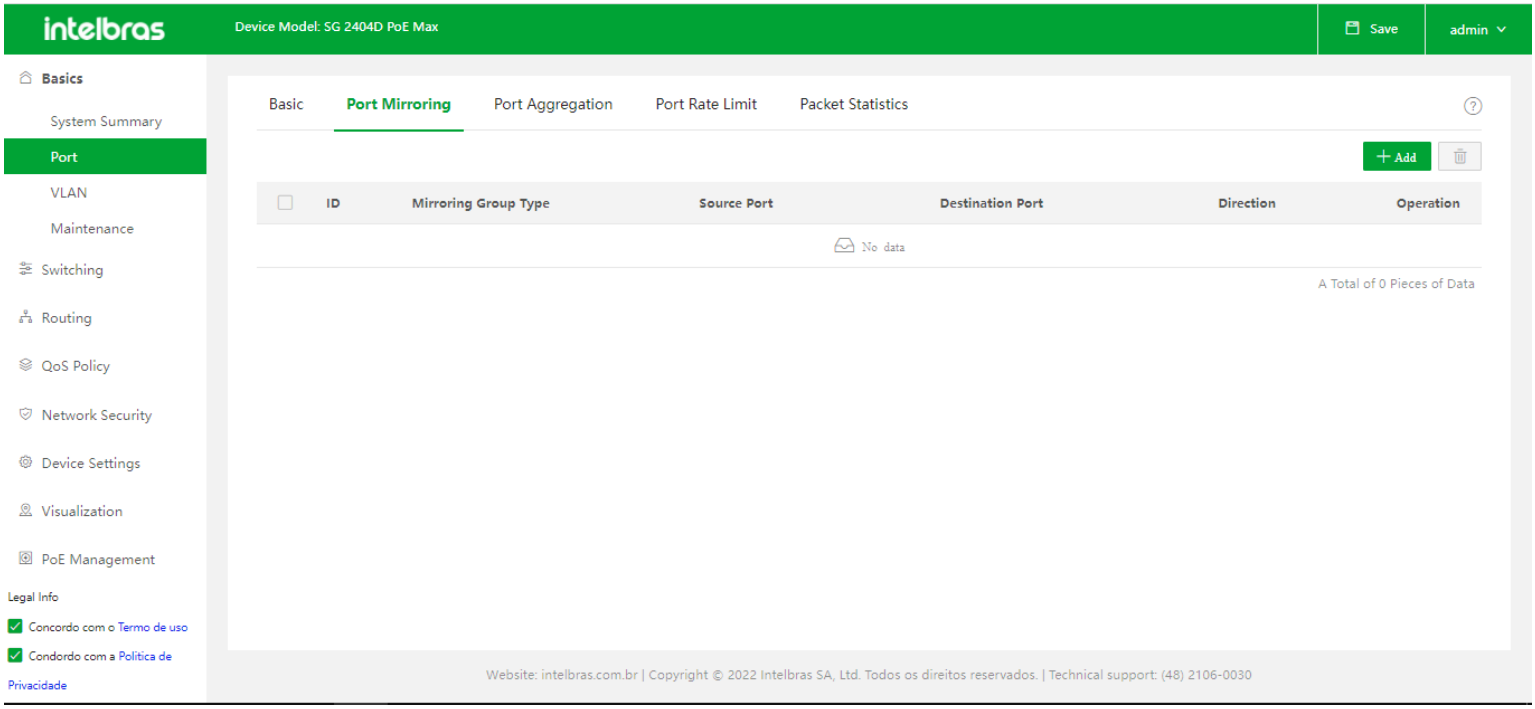
Ao clicar no botão, temos acesso a configurações das interfaces. Para alterar as configurações basta selecionar uma ou mais interfaces, clicando na(s) interface(s) desejada(s), e alterar a configuração.

OBS: O campo Rate/Mode não pode ser modificado se portas de diferentes types/rates forem selecionadas.



Port Mirroring

O Port Mirroring (espelhamento de porta) é um método de copiar e enviar pacotes de rede de uma porta ou portas múltiplas (Source Port) para uma porta especificada (Destination Port) do switch. A porta de destino é normalmente conectada a um dispositivo de monitoramento de dados, permitindo que você monitore o tráfego de dados, analise o desempenho e faça o diagnostico de falhas.



Na tela de Port Mirroring temos as seguintes informações:

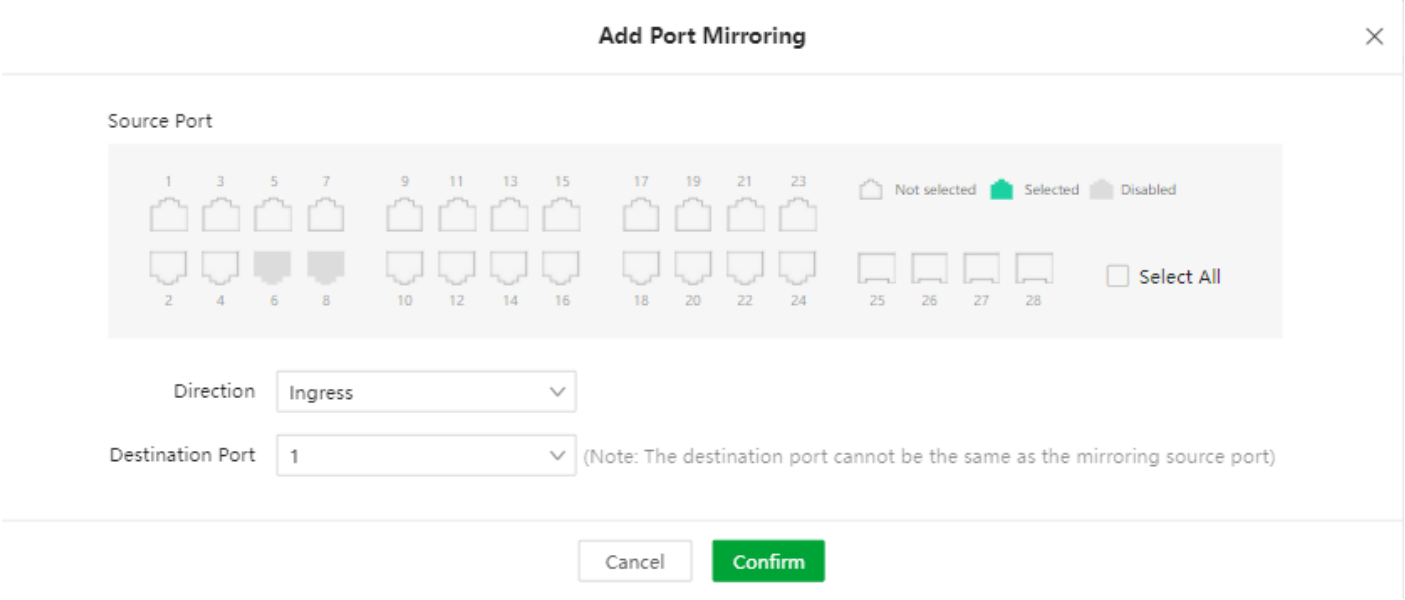
- **Source Port:** especifica as portas cujos pacotes serão copiados. Várias portas podem ser selecionadas.
- **Destination Port:**Os pacotes da Source Port serão copiados para esta porta. Um grupo de espelhamento poderá contra com apenas um porta de destino.
- **Direction:** especifica os pacotes que serão encaminhados da Source Port para a Destination Port:

  Ingress: somente os pacotes recebidos pelas Source Port's serão copiados para a porta de destino;

  Egress: somente os pacotes transmitidos pelas Source Port's serão copiados para a porta de destino;

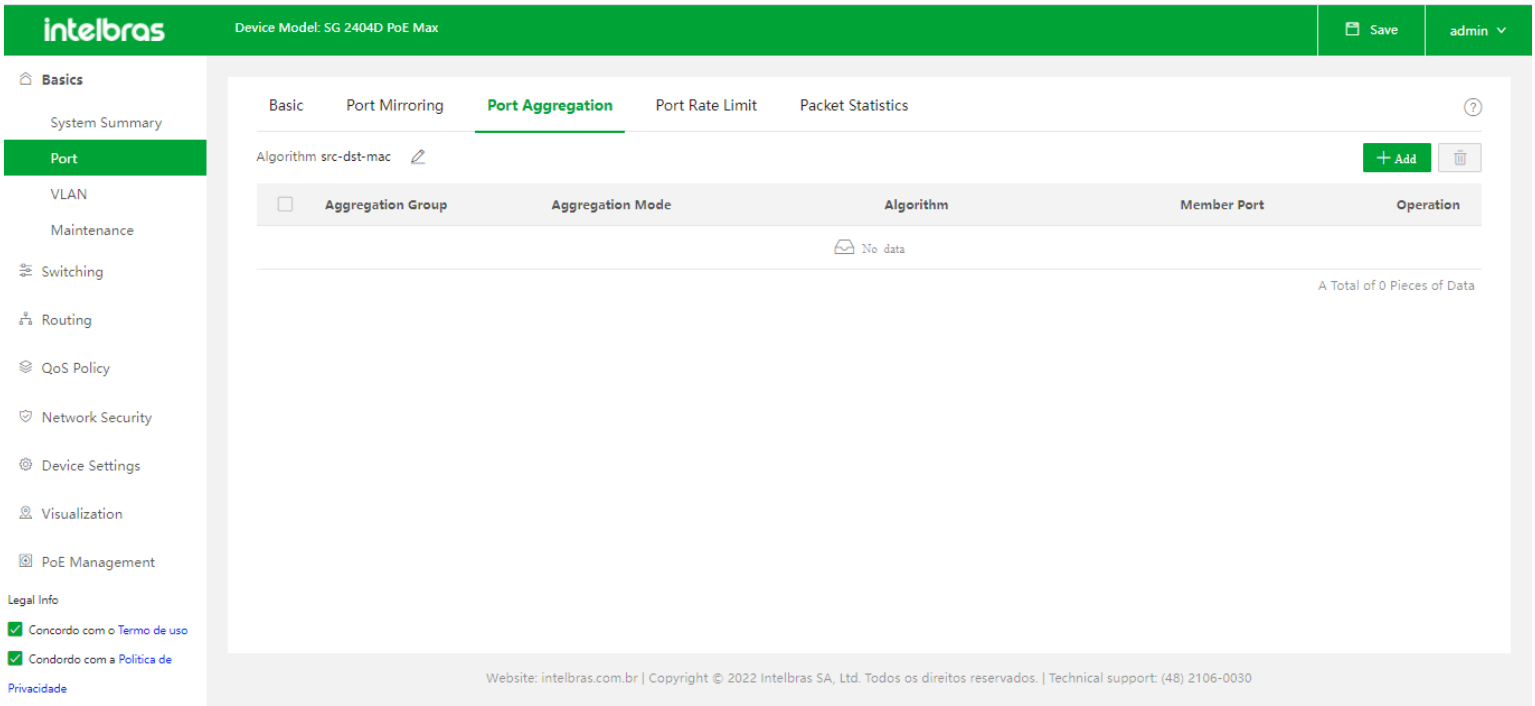
  Both: os pacotes transmitidos e recebidos pelas Source Port's serão copiados para a porta de destino.

- **Operation:** é usado para modificar e excluir o grupo de espelhamento desejado.
- **+ Add:** Para configurar um novo grupo de espelhamento deve-se clicar no botão "+ Add". Será aberta a tela "Add Port Mirroring", nela deve-se selecionar a(s) Source Port, a Direction (Ingress, Egress ou Both) e a Destination Port. O trafego das interfaces configuradas como Source Port será encaminhado para a a Destination port, respeitando a configuração de Direction.



Port Aggregation

O Port Aggregation é utilizado para convergir várias portas físicas em um grupo de agregação lógica. Vários links físicos em um grupo de agregação são considerados como um link lógico. A agregação de portas possibilita o compartilhamento de dados entre as interfaces de um grupo de agregação, aumentando a largura de banda. Por exemplo, se agregarmos 2 portas de 1Gbps teremos um link lógico com capacidade de 2Gbps. Todas as interface presente em um grupo de agregação farão backup dos dados uns dos outros dinamicamente, melhorando a confiabilidade da conexão.



Na tela de Port Aggregation temos as seguintes informações:

- **ID:** Especifica o número de ID dos grupos de agregação. Quando o Aggregation Mode é definido como Estático, o ID do Grupo de Agregação poderá ter valor de 1 a 32. Quando o Modo de Agregação é definido como Dinâmico, o ID do Grupo de Agregação varia de 33 a 64.
- **Aggregation Mode:** temos dois modos de agregação, static e dynamic:

  Static: todas as portas membro em um grupo de agregação convergem para uma porta lógica.

Dynamic: todas as portas membro em um grupo de agregação são habilitadas no protocolo LACP. A porta de agregação (onde converge o trafego) deve ser determinada pelo protocolo LACP do dispositivo de mesmo nível.

OBS: O Aggregation Mode do grupo de agregação deve ser igual ao do dispositivo que está conectado ao link lógico. Caso contrário, os dados podem ser encaminhados incorretamente ou pode ocorrer um loop.

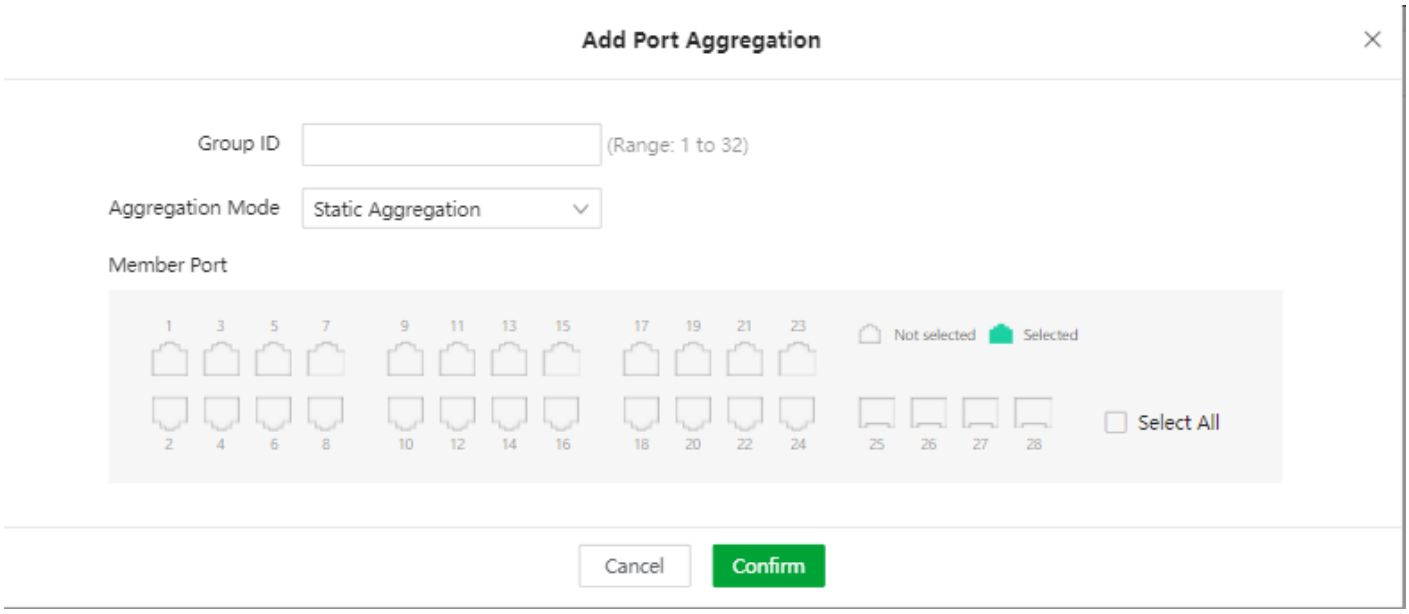
- **Algorithm:** informa o algoritmo que será utilizado para balancear o trafego do link lógico. É possível alterar o algoritmo clicando no lápis, que fica ao lado da informação de Algorithm. O algoritmo será o mesmo para todos os grupos de agregação. O Switch as seguintes opções de algoritmos:

  Src-dst-mac: o switch utilizará o endereço MAC de origem e de destino para fazer o balanceamento do trafego.

  Scr-dst-ip: o Switch utilizará o endereço IP de origem e de destino para fazer o balanceamento do trafego.

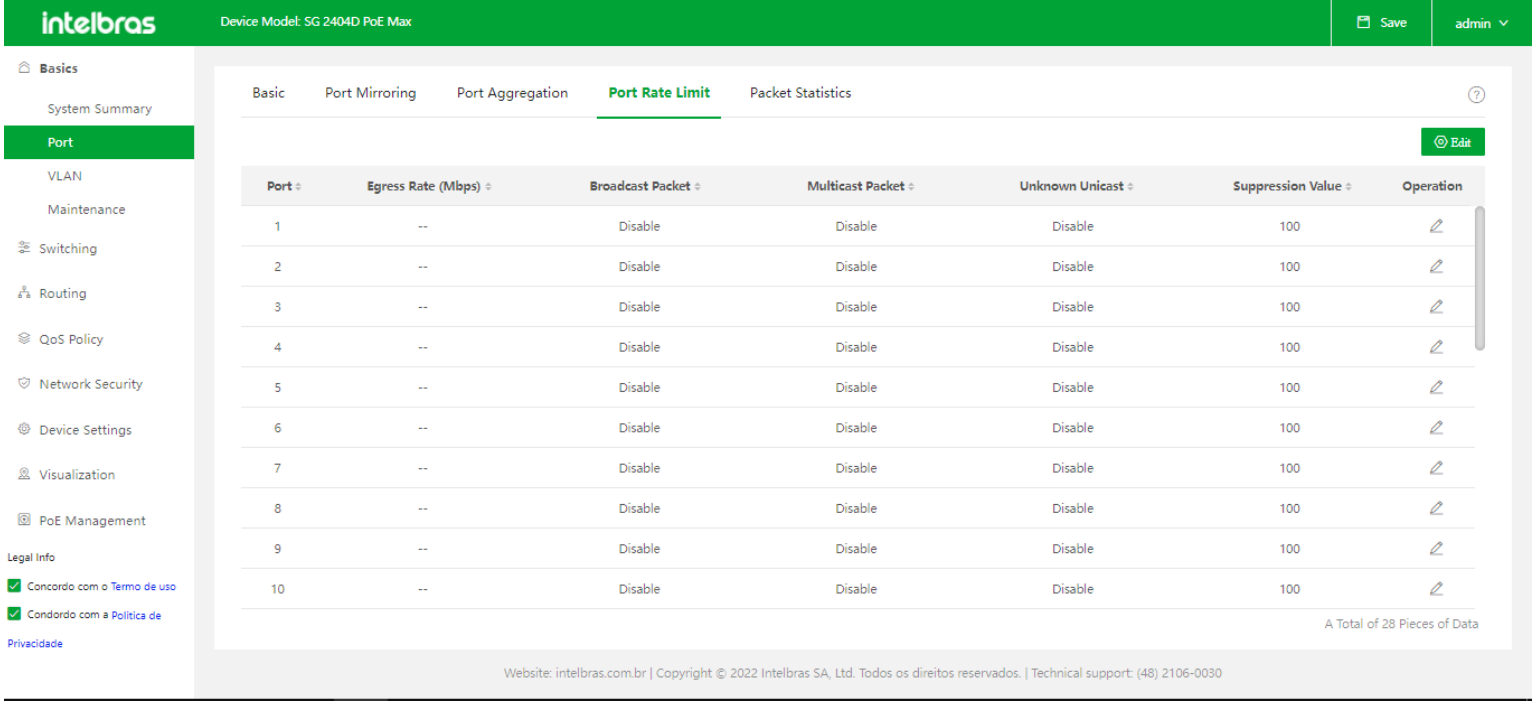
  Scr-dst-mac-ip-port: o Switch utilizirá os endeços de IP, MAC e porta de origem e de destino para fazer o balanceamento do trafego.

- **Member Port:** especifica os membros de um grupo de agregação. No modo de agregação **estática**, as portas membro são os membros de um grupo de agregação. No modo de agregação **dinâmica**, as portas membro são as portas habilitadas para o protocolo LACP. A porta de agregação (onde converge o trafego) deve ser determinada pelo protocolo LACP do dispositivo de mesmo nível.
- **Operation:** ele é usado para modificar ou excluir o grupo de agregação correspondente.
- **+ Add:** para configurar um novo grupo de agregação deve-se clicar no botão "+ Add". Será aberta a tela "Add Port Aggregation", nela deve-se configurar o Group ID, o Aggregation mode (Static ou Dynamic) e selecionar as portas que farão parte do grupo de agregação.



Port Rate Limit

Com a função Port Rate Limit você pode limitar a taxa de saída de uma porta e controlar a taxa na qual uma porta recebe mensagens de Broadcast, multicast e unicast desconhecidas.

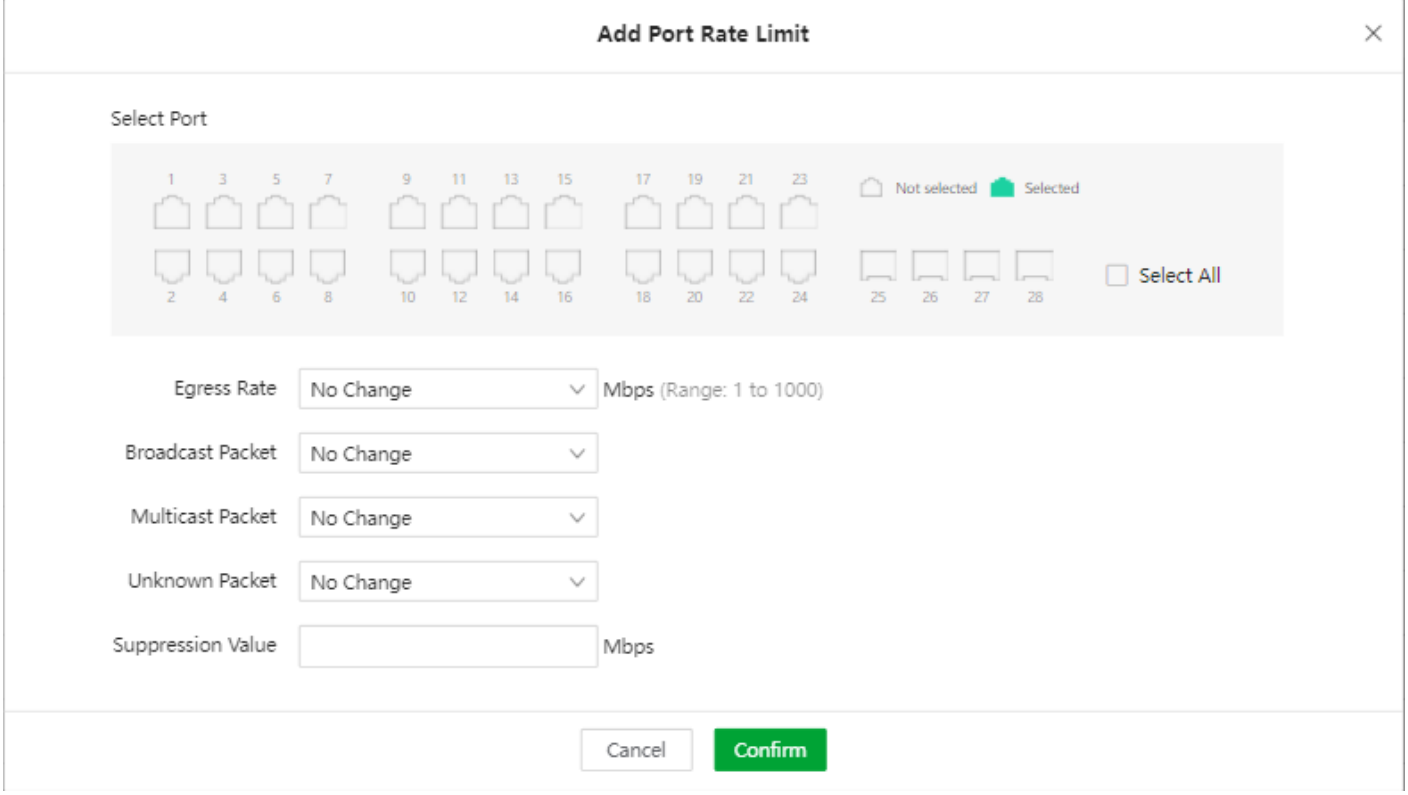


Na tela de Port Rate Limit temos as seguintes informações:

- **Port:** informa o número da porta.
- **Egress rate:** especifica a banda máxima de saída de uma porta. O simbolo "**--**" indica que não há limite configurado para esta porta.
- **Broadcast Packets:** é usado para habilitar ou desabilitar a função de supressão de pacotes broadcast, que por padrão é definida como desativada.
- **Multicast Packets:** é usado para habilitar ou desabilitar a função de supressão de pacotes multicast, que por padrão é definida como desativada.
- **Unknown Unicast:** é usado para habilitar ou desabilitar a função de supressão de pacotes unicast desconhecidos, que por padrão é definida como desativada.
- **Suppression Value:** especifica a taxa total na qual as mensagens de broadcast, multicast e unicast desconhecidas podem passar pela porta quando a função de supressão está habilitada. Não haverá descarte de pacotes quando a função de supressão estiver desabilitada na porta ou o Suppression Value configurado for maior que a taxa de entrada ou saída na porta.
- **Operation:** é usado para modificar a configuração de limite de taxa da porta correspondente.

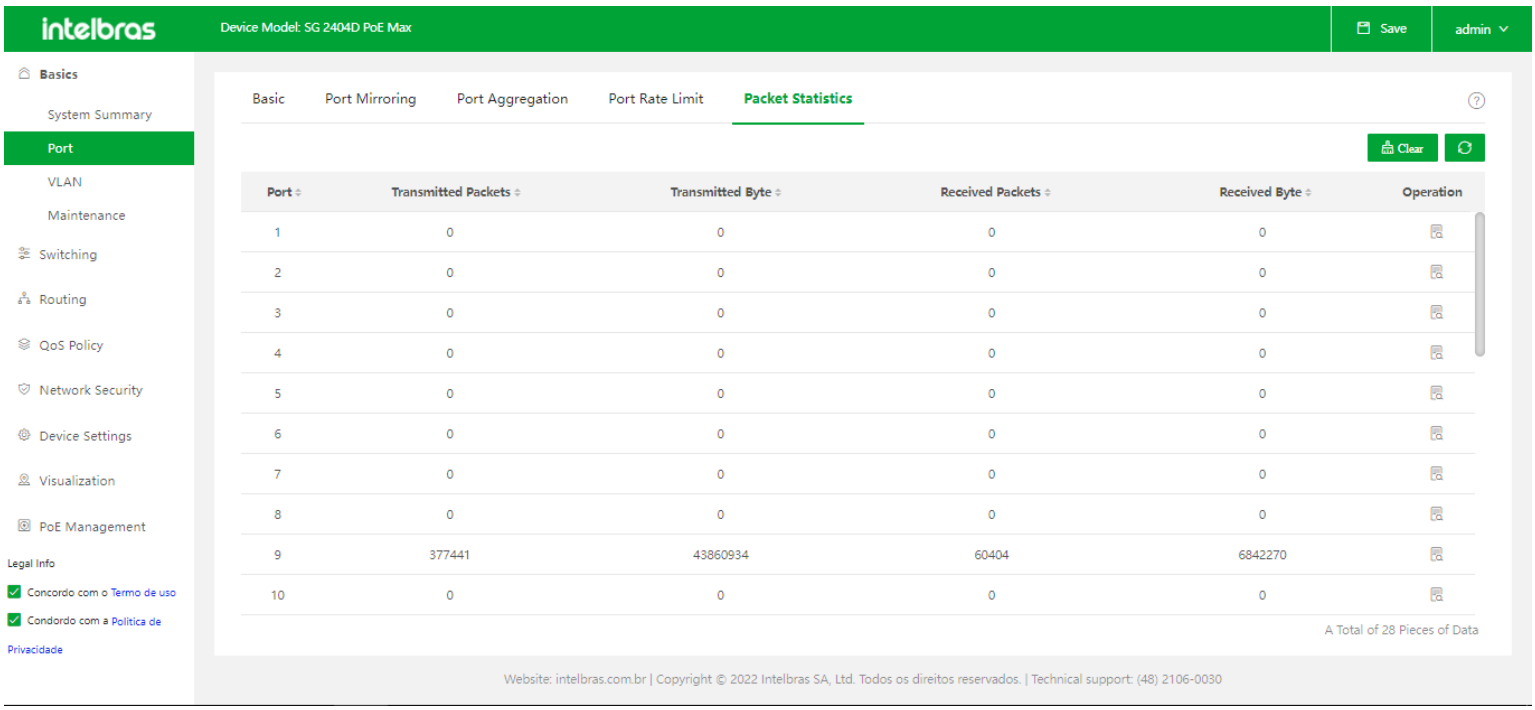
Exemplo de uso: configuramos o Suppresion Value em 10Mbps e ativamos na porta 1 os campos Broadcast Packet e Multicast Packet. Neste caso a porta 1 permitirá trafego de broadcast e multicast desconhecidos até 10Mbps, todo trafego que exceder este limite será descartado.

- **Edit:** para alterarmos as configurações de Port Rate Limit, basta clicarmos no botão de "Edit" no canto direito da tela. Será aberta a tela "Add Port Rate Limit", nela pode-se selecionar uma ou mais portas e realizar a mudança conforme necessário.



Packet Statistics

É usado para contabilizar os pacotes transmitidos ou recebidos por uma porta.



Na tela de Packet Statistics temos as seguintes informações:

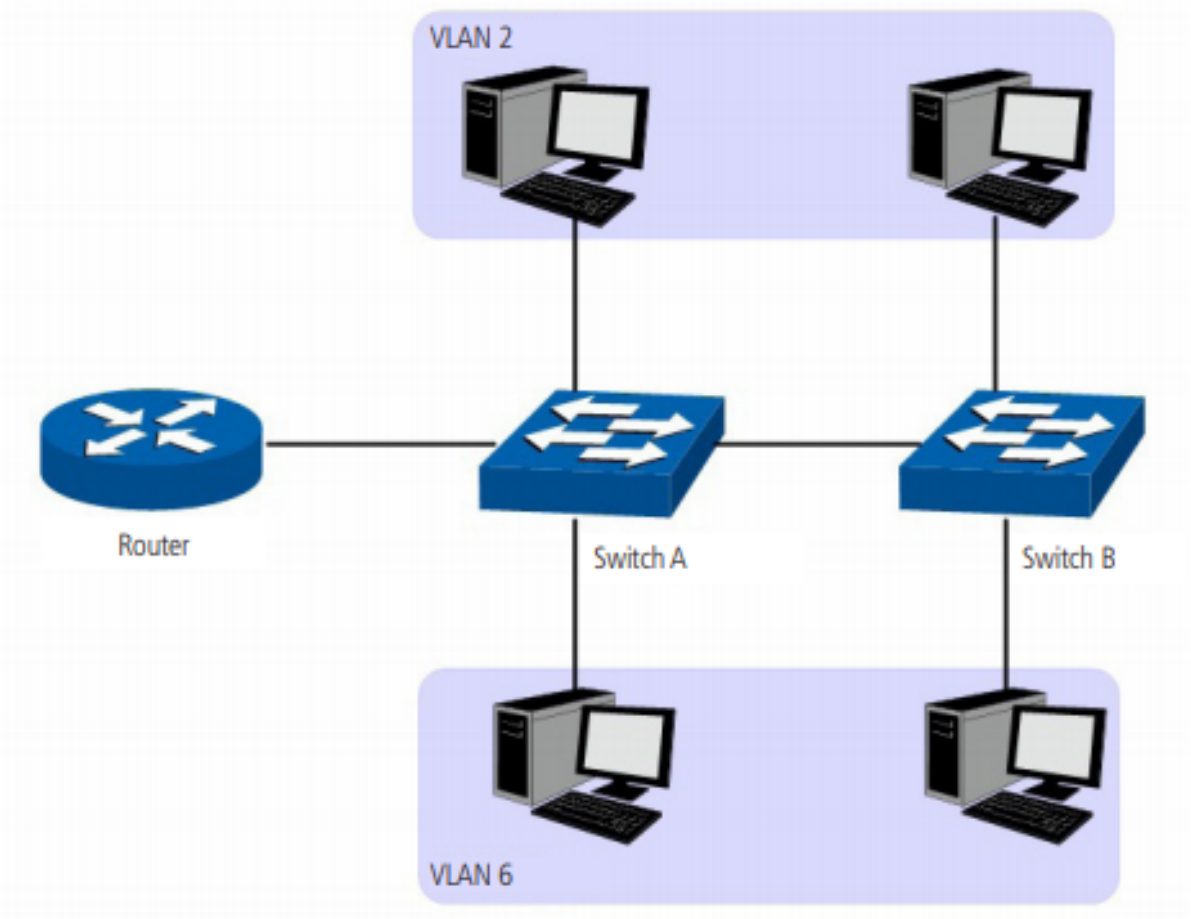
- **Port:** informa o número da porta.
- **Transmitted Packets:** informa o total de pacotes transmitido pela porta.
- **Transmited Byte:** informa o total de bytes transmitidos pela porta.
- **Received Packets:** informa o total de pacotes recebido pela porta.
- **Received Byte:** informa o total de bytes recebidos pela porta.
- **Operation:** trás informações mais detalhadas sobre as estatísticas de pacotes de uma porta, como número de pacotes de broadcast, unicast, pacotes de erro e pacotes de descarte.

- **Clear:** é usado para limpar todas as informações de estatísticas das portas.

VLAN

VLAN (*Virtual Local Area Network*) é o modo que torna possível dividir um único segmento de rede LAN em vários segmentos lógicos VLAN.

Cada VLAN se torna um domínio de broadcast, evitando assim a inundação de pacotes broadcast, otimizando a performance do switch, além de facilitar o gerenciamento e a segurança da rede. Para haver comunicação entre computadores em VLANs diferentes é necessária a utilização de roteadores ou switch layer 3 para o encaminhamento dos pacotes. A figura a seguir ilustra uma implementação de VLAN.



Principais vantagens na utilização de VLAN:

- As transmissões em broadcast estão restritas a cada VLAN. Isso diminui a utilização de banda e melhora o desempenho da rede.
- Melhoria na segurança da rede. VLANs não podem se comunicar umas com as outras diretamente, ou seja, um computador em uma VLAN não pode acessar os recursos contidos em outra VLAN, a menos que seja utilizado um roteador ou switch camada 3 para realizar esta comunicação.
- Flexibilidade na alteração de layout: é possível ter computadores separados geograficamente (por exemplo, computadores em andares diferentes) e pertencerem à mesma VLAN sem a necessidade de alteração física da topologia da rede.

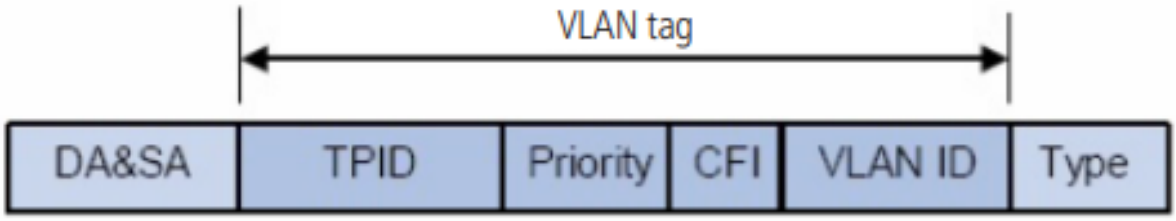
Este switch suporta os seguintes modos de classificação de VLAN: *802.1q VLAN.*.

VLAN TAG

As tags de VLANs são necessárias para o switch identificar os pacotes de diferentes VLANs. O switch trabalha nas camadas de enlace e rede do modelo OSI, podendo desta forma, analisar e gerenciar os quadros que possuam a tag de VLAN.

Em 1999, o IEEE padronizou a aplicação 802.1q VLAN, definindo uma estrutura de tags de VLAN nos quadros Ethernet. O protocolo IEEE 802.1q define que 4 bytes são adicionados ao quadro Ethernet (esta inserção ocorre logo após os campos de endereço MAC de destino e origem do frame Ethernet) para tornar possível a utilização de VLANs em redes Ethernet.

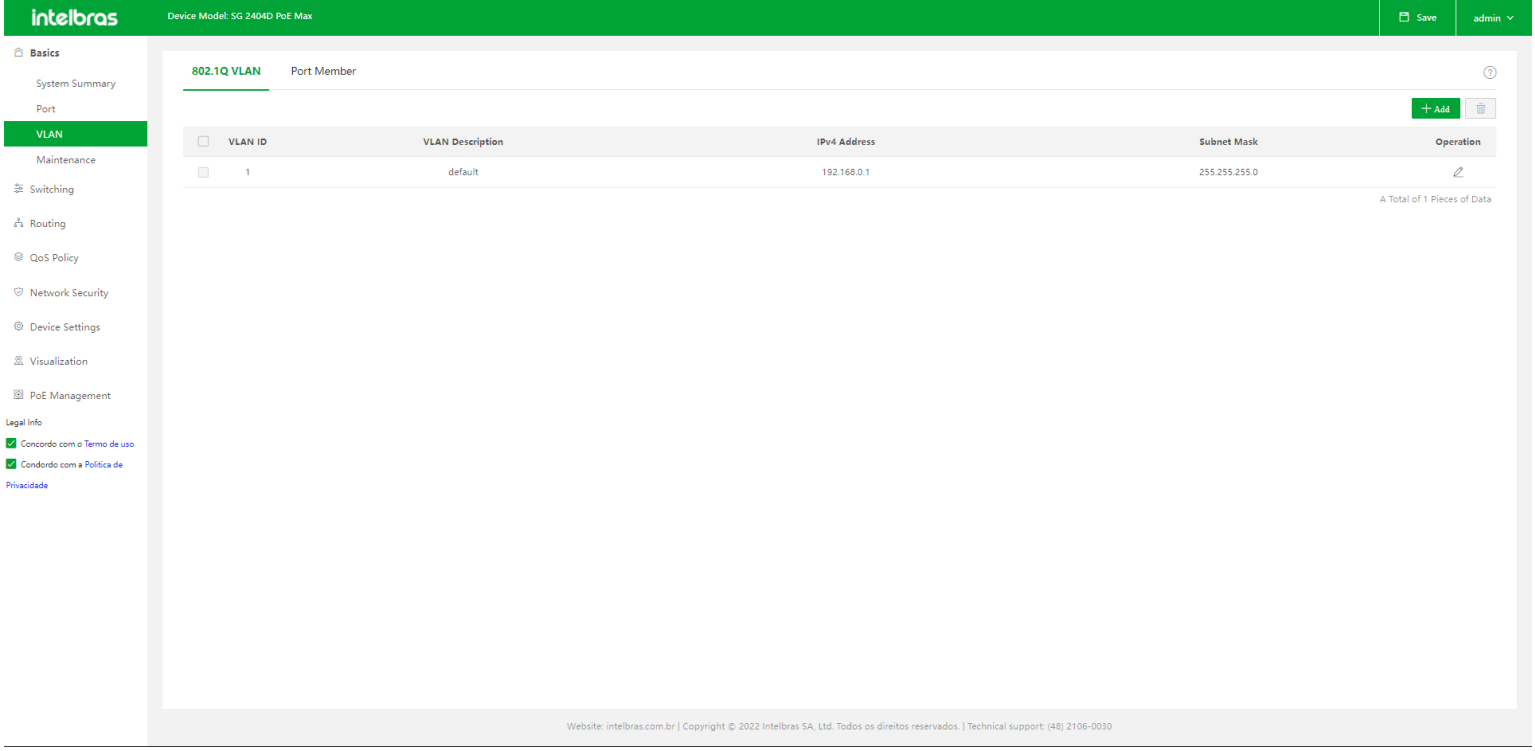
A figura a seguir exibe quatro novos campos que o protocolo 802.1q (tag de VLAN) adiciona ao frame Ethernet: TPID (*Tag Protocol Identifier*), Priority, CFI (*Canonical Format Indicator*) e VLAN ID.



- **TPID:** campo de 16 bits, indicando que a estrutura do frame é baseada em tag de VLAN, por padrão este valor é igual a 0x8100.
- **Priority:** campo de 3 bits, referindo-se à prioridade 802.1p.
- **CFI:** campo de 1 bit, indicando que o endereço MAC é encapsulado na forma canônica 0 ou não-canônica 1. Isso é utilizado no método de acesso ao meio roteado por FDDI/Token-Ring para sinalizar a ordem da informação de endereço encapsulado no quadro. Esse campo não é descrito em detalhes nesse manual.
- **VLAN ID:** campo de 12 bits, que identifica o VLAN ID (Identificação da VLAN) a qual o quadro pertence. Este intervalo varia entre 1 a 4094, normalmente os valores 0 e 4095 não são utilizados.

VLAN ID identifica a VLAN a qual o quadro pertence. Quando o switch recebe um pacote que não possui uma tag de VLAN (*untagged*), o switch irá encapsular o quadro com a tag de VLAN padrão da porta correspondente (VLAN nativa).

802.1Q VLAN



Na tela 802.1Q temos as seguintes informações:

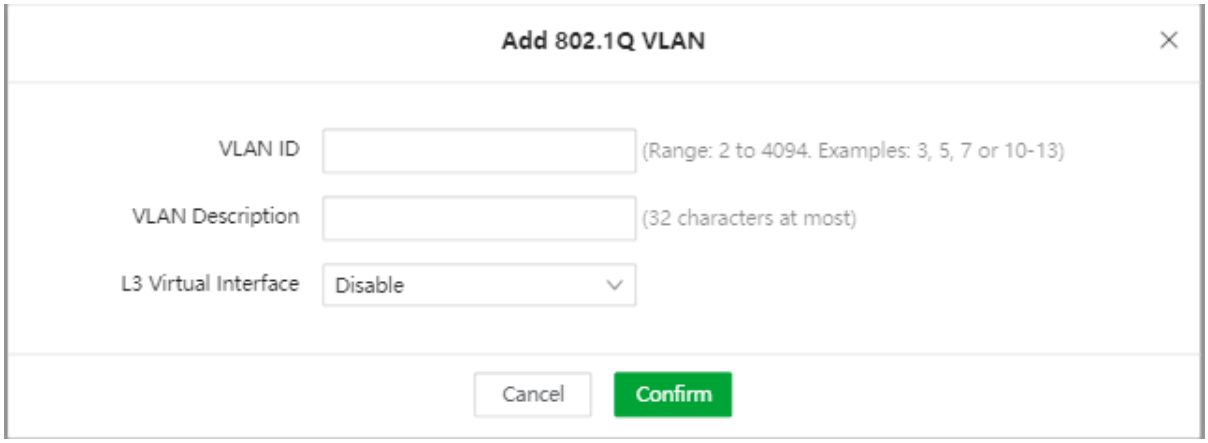
- **VLAN ID:** campo disponível para configuração do ID da VLAN. Podem ser utilizados valores de 2 a 4094.

Exemplo de configuração: colocando apenas um número, será criada uma única VLAN. Pode-se também adicionar um range de VLANs, para criar diversas VLANs ao mesmo tempo. Para configurar em range podemos usar os dois metodos a seguir: **1°**: 2,3,4,5,6; **2°**: 2-6.

Nos dois exemplos serão criadas as VLANs 2,3,4,5 e 6.

- **VLAN Description:** é usado para identificar grupos de VLAN. Se não for configurado, uma descrição padrão será automaticamente configurada no formato "VLAN + 4 digitos, sendo eles o ID da VLAN e o restante são 0". Por exemplo, quando o ID da VLAN é 3 e nenhuma descrição for adicionada, automaticamente será preenchida com VLAN0003.
- **IPv4 Address:** exibe o endereço de IP de uma interface VLAN, podendo ser configurado somente quando a intervace virtual L3 estiver habilitada. O endereço exibido neste campo será um endereço de gerencia, dispositivos presentes na VLAN podem acessar a interface WEB.
- **Subnet Mask:** exibe a máscara de sub-rede da interface VLAN.
- **Operation:** ao clicar no botão será aberta a tela "Edit 802.Q VLAN", o usuário poderá editar um VLAN já criada.
- **+ Add:** para adicionar uma nova VLAN basta clicar no botão "+ Add", no canto superior direito da tela de 802.1Q VLAN.

Ao clicar nele temos acesso a tela de "Add 802.1Q VLAN", onde pode-se configurar VLAN ID, VLAN Description, L3 virtual interface e IP Obtain Type:



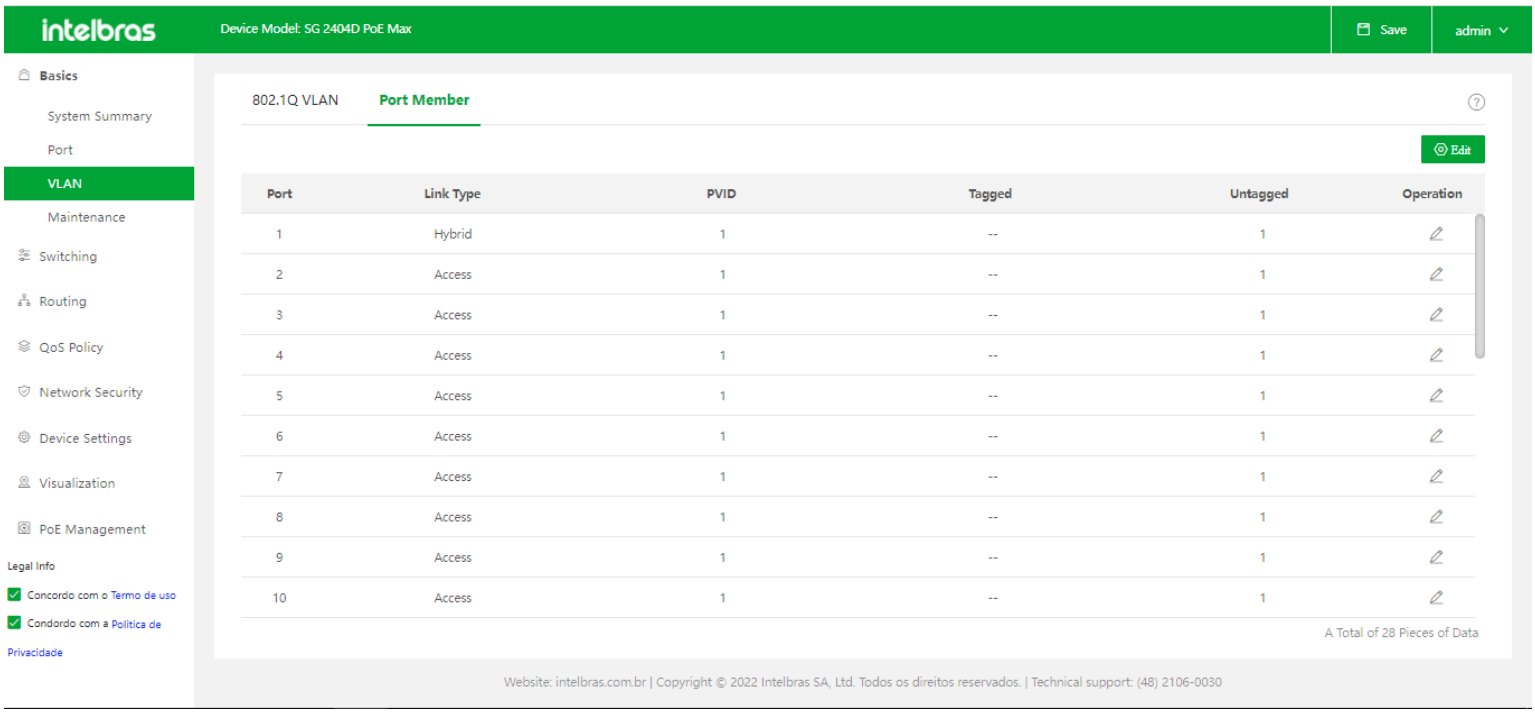
- **L3 Virtual Interface:** com este campo configurado como Enable, você poderá configurar um endereço IP e uma máscara de rede para a interface VLAN em questão.
- **IP Obtaining Type:** especifica o tipo que a interface VLAN emprega para obter um endereço IP. Há duas possíveis configurações para este campo:

Manual: configure manualmente o endereço IP e a máscara de sub-rede para a interface VLAN.

DHCP: obtém automaticamente as informações do endereço IP e mácara de sub-rede do servidor DHCP.

OBS: quando o tipo de obtenção do endereço IP estiver configurado para DHCP, certifique-se de que haja um servidor DHCP pertencente à VLAN.

Port Member



Nesta tela podemos configurar a qual VLAN as portas pertencem, qual o modo da porta e a política de processamento e transmissão de dados da porta.

Na tela principal temos algumas informações referente a configuração das portas. Podemos ver informações de:

- **Port:** informa o número da porta.
- **Link Type:** informa o modo que a porta está configurada. Temos 3 opções de modo de porta:

  Trunk: a porta em modo Trunk pode ser adicionada em várias VLANs, e a regra de saída da porta é TAG, ou seja, somente serão transmitidos pacotes com marcação de TAG. No caso de receber pacotes UNTAG, será transmitido com a VLAN nativa.

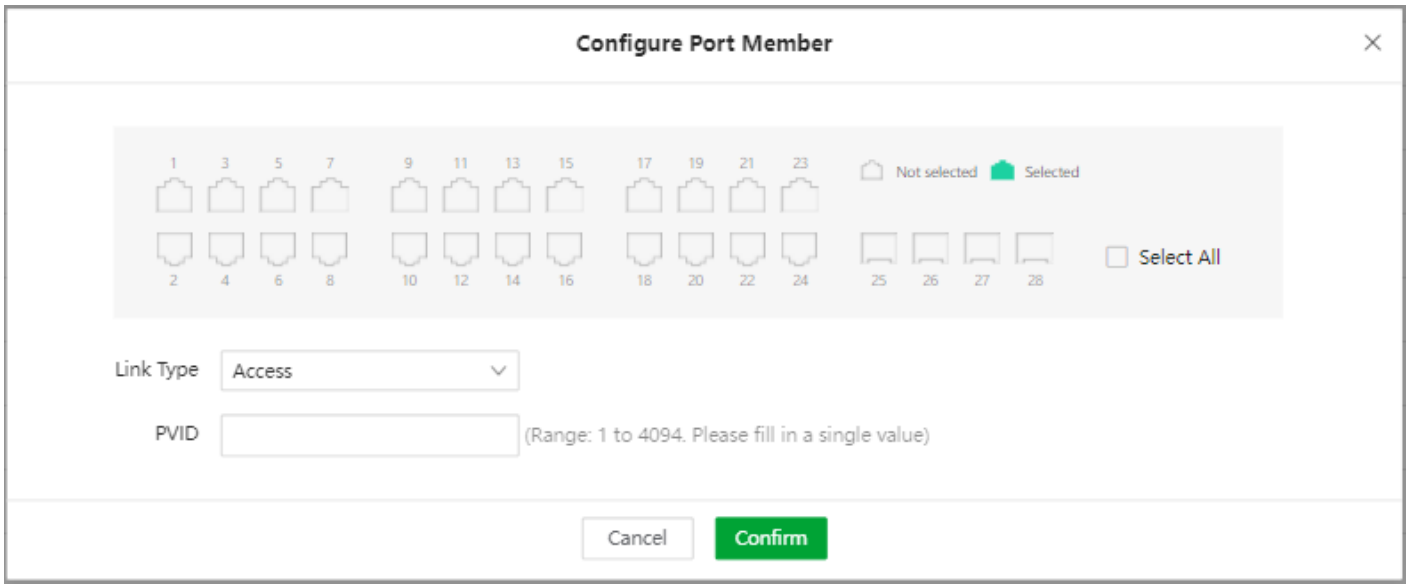
  Access: a porta em modo Access só pode ser adicionada em uma única VLAN, e a regra de saída da porta é UNTAG, ou seja, os pacotes encaminhados não possuirão marcação de TAG.

  Hybrid: pode receber e transmitir mensagens pertencentes a várias VLANs. Pode ser usado como uma porta conectada em cascata entre switches ou para conectar a terminais.

- **PVID:** especifica o ID de VLAN padrão da porta. Ao receber pacotes não marcados, a porta os encaminha para a VLAN correspondente com base no PVID da própria porta.
- **Tagged:** exibe a(s) tag(s) de VLAN de cada porta, ou seja, os pacotes transmitidos nestas portas sairão marcados com a tag de VLAN (pacotes contendo informações de VLAN).
- **Untagged:** exibe a(s) VLAN(s) untagged da porta, ou seja, quando uma porta receber um pacote com VID (Vlan ID) igual a VLAN untagged configurada, ele irá retirar a TAG e encaminhar o pacote.
- **Operation:** é utilizado para editar as configurações de VLAN de determinada porta.

Observação: por padrão todas as portas do Switch são untagged e tem a VLAN 1 como nativa.

- **Edit:** no lado superior direito da tela de port member, temos o botão de Edit. Ao clicar neste botão é aberta a seguinte tela:



É possível configurar uma porta ou mais portas (todas as portas selecionadas terão a mesma configuração). Para selecionar a(s) porta(s) basta clicar com o mouse naquela(s) que deseja configurar.

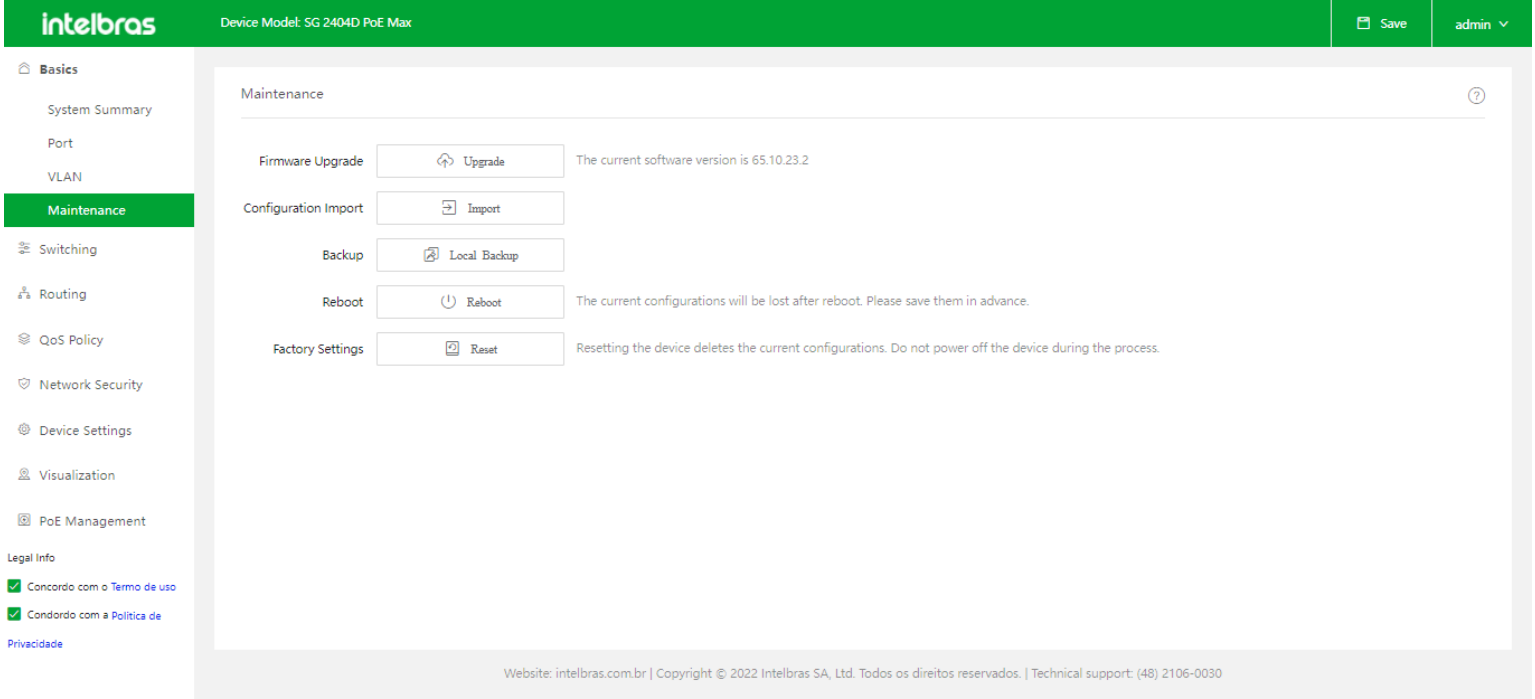
* Ao clicar em Select All, todas as portas serão selecionadas.

Após selecionar a(s) porta(s) desejada(s), deve-se selecionar qual será o Link Type (Access, hybrid ou trunk) e qual o PVID padrão da porta.

Ao escolher como Link Type trunk ou hybrid, também deve-se configurar as VLANs que serão Tagged e as que serão Untagged.

Maintenance

Está é a tela de manutenção do Switch, nela podemos realizar operações como atualização de firmware e fazer backup do produto.



Podemos fazer as seguintes operações no Switch:

- **Firmware Upgrade:** este botão tem a finalidade de atualizar o firmware do switch de forma local, buscando o arquivo na memória do dispositivo que está acessando a interface Web.

OBS: o arquivo de firmware utilizado deve ter o formato .bin. Caso seu arquivo esteja em .zip deve-se descompactar o arquivo.

- **Configuration import:** tem a finalidade de importar um arquivo de configuração para o Switch. Toda a configuração do Switch será alterada para a configuração presente no arquivo utilizado.

OBS: o switch não faz a verificação do arquivo de configuração. Certifique-se de que o arquivo que está importando esteja correto.

- **Local Backup:** é utilizado para baixar a configuração do switch para o dispositivo local.

OBS: clique no botão Salvar, no canto superior direito da página, antes de fazer o download.

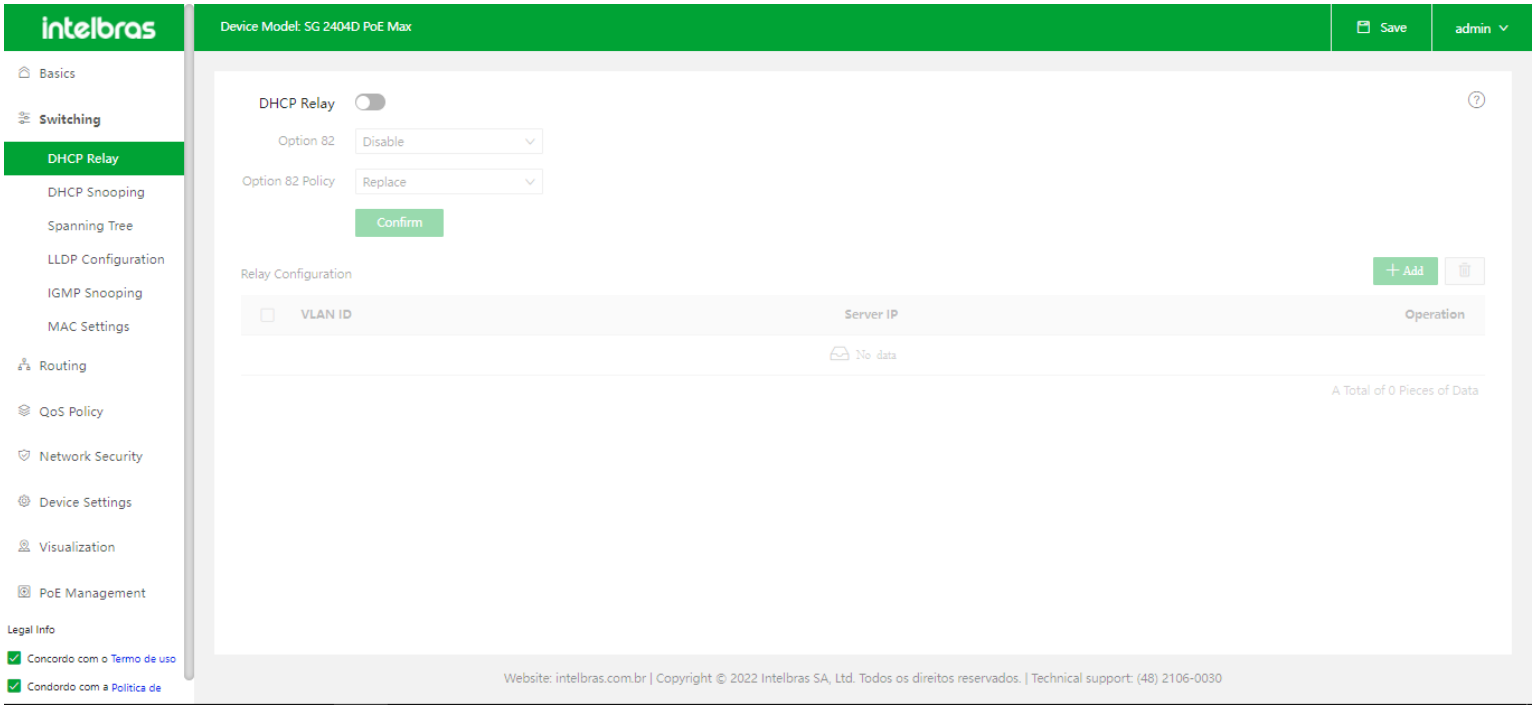
- **Reboot:** ao apertar este botão o switch será reiniciado, o tempo para reinicialição pode variar de 2 a 4 minutos. Para evitar que configurações sejam perdidas, antes de reiniciar o produto clique no botão de Salvar no canto direito superior da tela.
- **Factory settings (reset):** após clicar no botão Reset, as configurações do switch serão apagadas e ele será restaurado para as configurações de fábrica.

SWITCHING

Neste menu temos as configurações de Switching. Temos opções de configuração de diversas funções, como STP, DHCP snooping, IGMP Snooping entre outras.

DHCP Relay

Com esta função habilitada o switch pode fornecer serviço de retransmissão do DHCP para o servidor DHCP que está em um segmentos de rede diferente. Está função permite que clientes DHCP em várias redes compartilhem um mesmo servidor DHCP. O agente DHCP Relay irá receber os pacotes broadcast de solicitação DHCP do cliente e irá encaminhar em pacotes unicast para o servidor, que está em outra rede.



Podemos fazer as seguintes configurações no DHCP Relay do Switch:

- **DHCP Relay:** é usado para habilitar ou desabilitar a função de DHCP Relay.
- **Option 82:** é usado para habilitar ou desabilitar a politica do Option 82. A Option 82 registra informações de localização dos clientes DHCP. A Option 82 Policy só entrará em vigor quando o Option 82 estiver habilitado.
- **Option 82 Policy:** quando o agente DHCP Relay recebe mensagens de solicitação de DHCP ele as processa com base na política do Option 82 configurado pelo usuário e encaminha as mensagens processadas para o servidor DHCP. O switch suporta três políticas:

  Replace: quando o agente DHCP Relay recebe mensagens de solicitação de DHCP, ele substitui as informações originais da Option 82 pelo conteúdo padrão do switch e encaminha as mensagens.

  Retain: quando o agente DHCP Relay recebe mensagens de solicitação DHCP, ele mantem o estado original da Option 82 e encaminha as mensagens.

  Discard: o agente DHCP Relay descarta a mensagem de solicitação DHCP com a opção 82 e encaminha a mensagem de solicitação DHCP sem a opção 82.

- **Relay Configuration:** ele é usado para exibir opções relevantes do DHCP Relay.

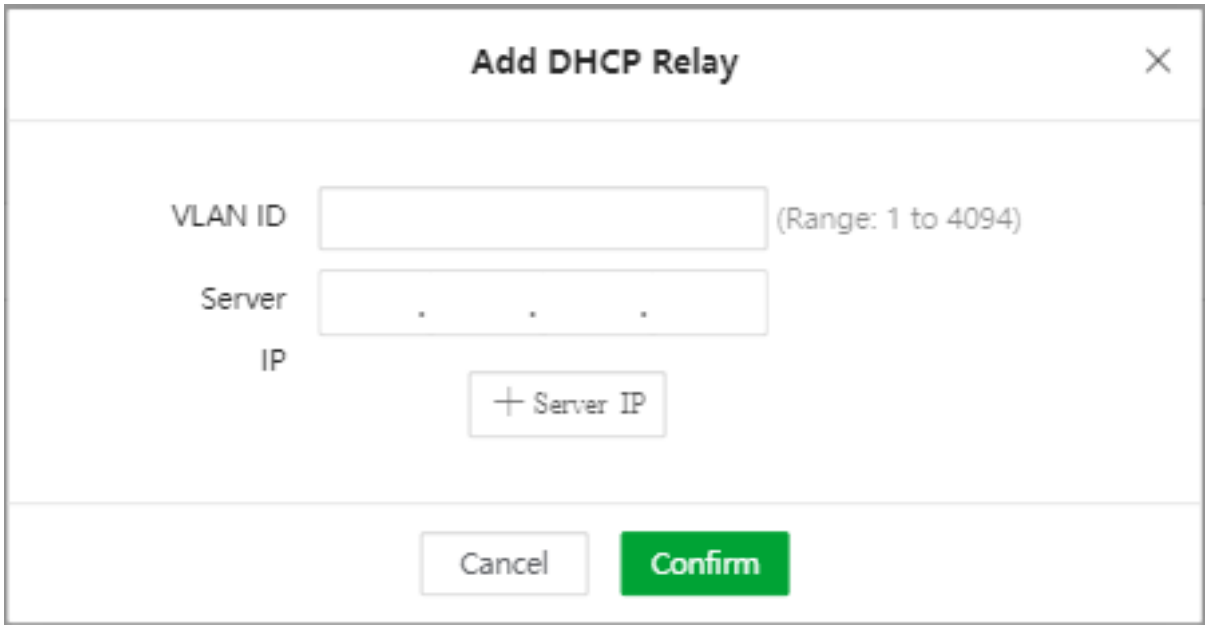
Na tela de Relay Configuration temos as seguintes opções:

VLAN ID: especifica a VLAN a qual os clientes pertencem. A VLAN já deve existir no Switch e sua L3 Virtual Interface deve estar configurada.

Server IP: especifica o endereço IP do servidor DHCP remoto. O endereço IP do servidor DHCP remoto não pode pertencer ao mesmo segmento de rede da VLAN à qual os clientes pertencem.

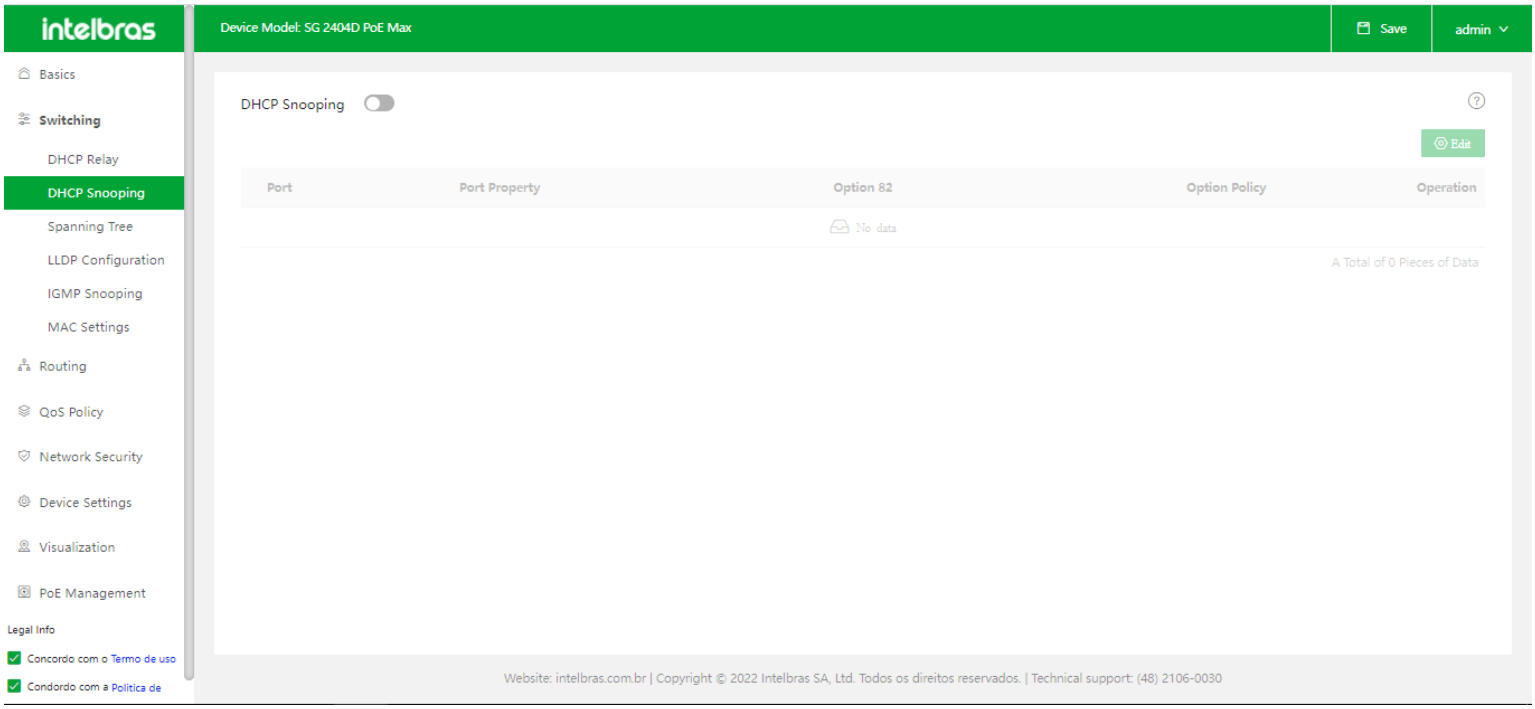
OBS: certifique-se de que o servidor DHCP remoto possa se comunicar com o switch corretamente. Caso contrário, o DHCP Relay falhará.

- **Operation:** É usado para modificar ou excluir a configuração de DHCP Relay da VLAN correspondente.
- **+ Add:** É usado para adicionar a configuração de DHCP Relay de uma VLAN. Ao clicar neste botão temos acesso a tela de Add DHCP Relay, nela deve-se configurar a VLAN ID desejada e os servidores DHCP que deseja redirecionar as requisições DHCP. Podem ser configurados até 4 servidores DHCP.



DHCP Snooping

O DHCP Snooping funciona como um firewall entre hosts não confiáveis e servidores DHCP confiáveis. Valida as mensagens DHCP recebidas de fontes não confiáveis e filtra mensagens de resposta inválidas de servidores DHCP. Também constrói e mantém o banco de dados de vinculação de DHCP snooping, que contém informações sobre hosts não confiáveis com endereços IP alugados.



Na tela de DHCP Snooping temos as seguintes informações:

Port: informa a porta física em questão.

Port Property: ele é usado para configurar a propriedade do DHCP Snooping da porta atual, incluindo a configuração de porta confiável ou porta não confiável.

Porta confiável: está conectado a um servidor DHCP confiável e encaminha as mensagens DHCP recebidas normalmente.

Porta não confiável: depois de receber as mensagens DHCP-ACK e DHCP-OFFER respondidas pelo servidor DHCP, a porta descarta as mensagens, desativando servidores DHCP não confiáveis e impedindo que ele atribua endereços IP aos clientes.

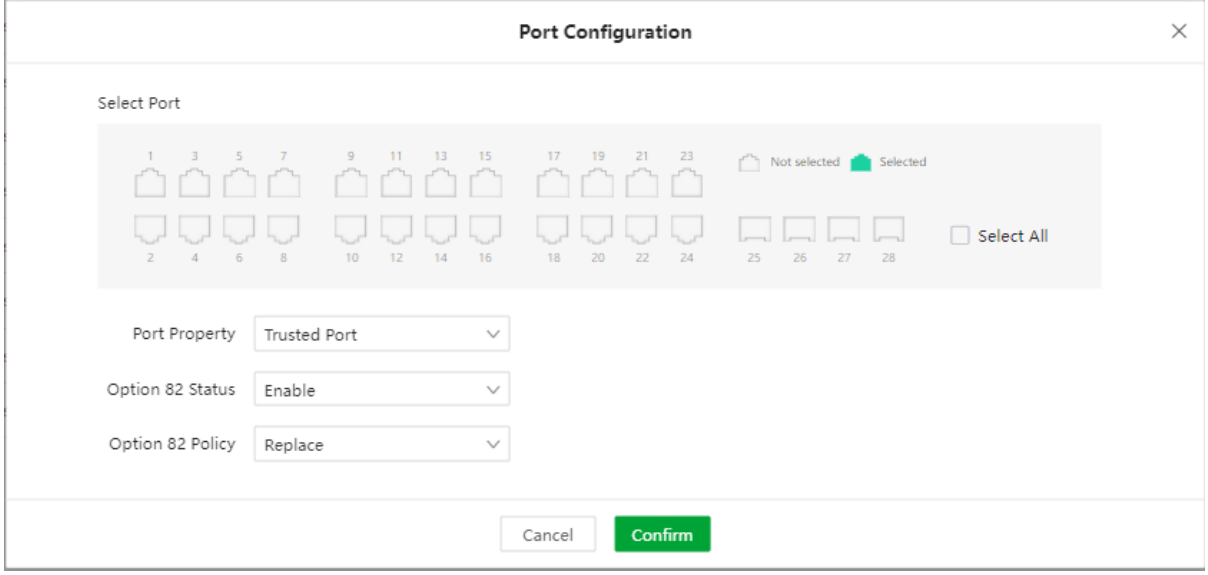
- **Option 82:** é usado para habilitar ou desabilitar a politica do Option 82. A Option 82 registra informações de localização dos clientes DHCP. A Option 82 Policy só entrará em vigor quando o Option 82 estiver habilitado.
- **Option 82 policy:** quando o switch recebe mensagens de solicitação de DHCP ele as processa com base na política da Opção 82 configurada pelo usuário e encaminha as mensagens processadas para o servidor DHCP. O switch suporta três políticas:

Replace: quando o agente DHCP Relay recebe mensagens de solicitação de DHCP, ele substitui as informações originais da Option 82 pelo conteúdo padrão do switch e encaminha as mensagens.

Retain: quando o agente DHCP Relay recebe mensagens de solicitação DHCP, ele mantem o estado original da Option 82 e encaminha as mensagens.

Discard: o agente DHCP Relay descarta a mensagem de solicitação DHCP com a opção 82 e encaminha a mensagem de solicitação DHCP sem a opção 82.

- **Operation:** é utilizado para editar as configurações da porta em questão.
- **Edit:** ao clicar abrimos a tela de Port Configuration. Nela podemos selecionar uma ou mais portas e configurar o Port property e o Option 82 status e policy. Clicando no botão Select All todas as portas serão selecionadas.



Spanning Tree

Spanning Tree é um protocolo que impede tempestades de broadcast em uma rede. O protocolo permite resolver problemas de loop em redes comutadas cuja topologia introduza anéis nas ligações, trazendo mais confiabilidade para a rede e auxiliando na melhor performance.

Global

Na tela Global temos as principais configurações de parametros do Spanning Tree, são elas:

Status: é utilizado para habilitar ou desabilitar a função Spanning Tree.

Mode: o Switch tem suporte a 3 modos de spanning tree, incluindo STP, RSTP e MSTP.

STP (Spanning Tree Protocol): é um protocolo usado para proteger a rede contra tempestades de broadcast (loops) e fornecer backup de redundância de link.

RSTP (Rapid Spanning Tree Protocol): é compatível com o protocolo 802.1d STP, fornece uma maior velocidade de convergência do Spanning Tree, que permite uma rápida geração da árvore de topologia quando alguma alteração acontece na rede.

MSTP: MSTP (Multi Spanning Tree) é um protocolo compatível com os protocolos STP e RSTP, que não apenas fornece velocidade de convergência do spanning tree, mas também permite que o tráfego de diferentes VLANs seja distribuído ao longo das respectivas rotas, proporcionando assim um melhor mecanismo de compartilhamento de carga para links redundantes.

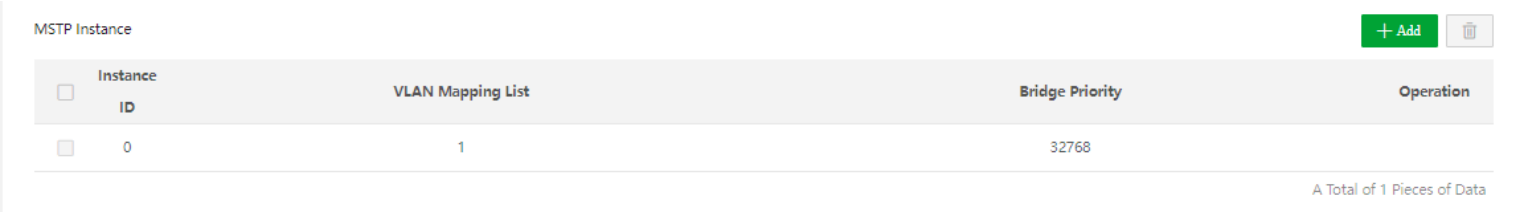
Bridge Configuration

- **Maximum Aging Time:** especifica a duração máxima durante a qual as mensagens de protocolo podem ser mantidas no switch. O limite máximo de configuração do Aging time deve ser configurado como mostrado abaixo: Maximum Aging Time: ≥ 2 x (Hello Time + 1) Maximum Aging Time: ≤ 2 x (atraso de encaminhamento - 1).
- **Hello Time:** é o intervalo no qual o Switch irá transmitir os pacotes BPDU (Bridge Protocol Data Unit).
- **Fowarding Delay:** especifica o atraso que a migração do estado da porta leva após uma mudança na topologia da rede.
- **Maximum Hops:** especifica o número máximo de saltos que as mensagens de protocolo podem ser encaminhadas. É usado para limitar a escala do Spanning Tree.
- **Bridge Priority:** especifica a prioridade que um switch terá na participação do cálculo da spanning tree. A prioridade é um critério importante pelo qual a bridge raiz é determinada. O switch com a prioridade mais alta será escolhido como root bridge.

MSTP Domain Setting

- **Region name:** Especifica o identificador de uma região MST (Multiple Spanning Tree Regions). O valor padrão é o endereço MAC do switch.
- **Revision:** Especifica o nível de revisão do MSTP do switch. O parâmetro é necessário quando o modo de spanning tree é MSTP. O valor padrão é 0.
- **Digest:** Especifica o valor calculado com base no interior do mapeamento da VLAN.

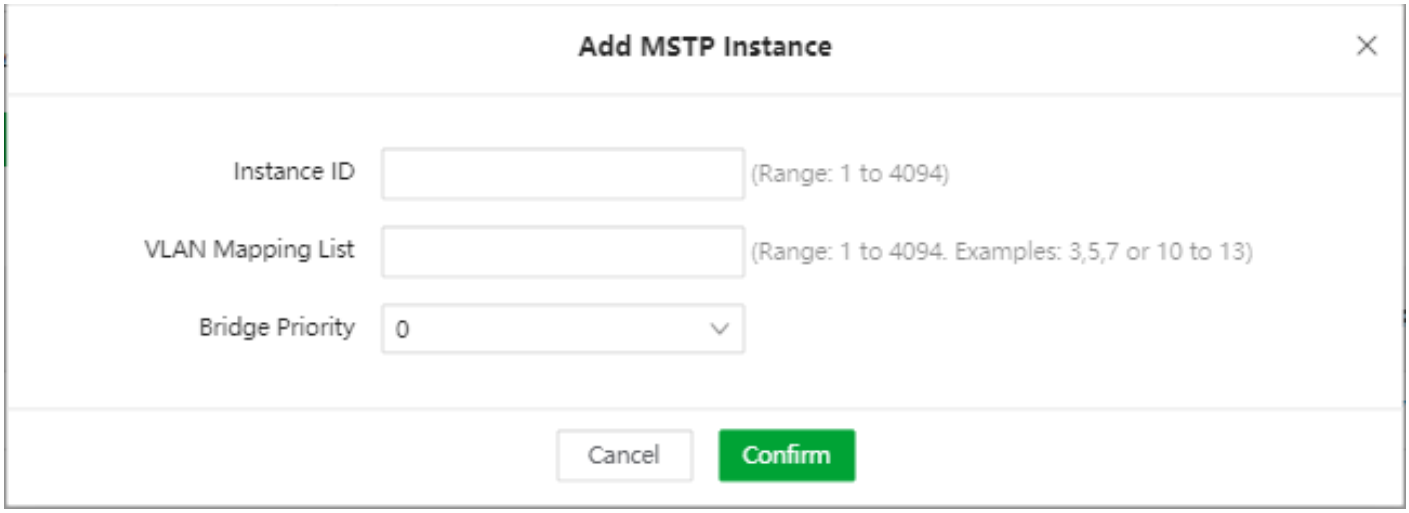
MSTP instance



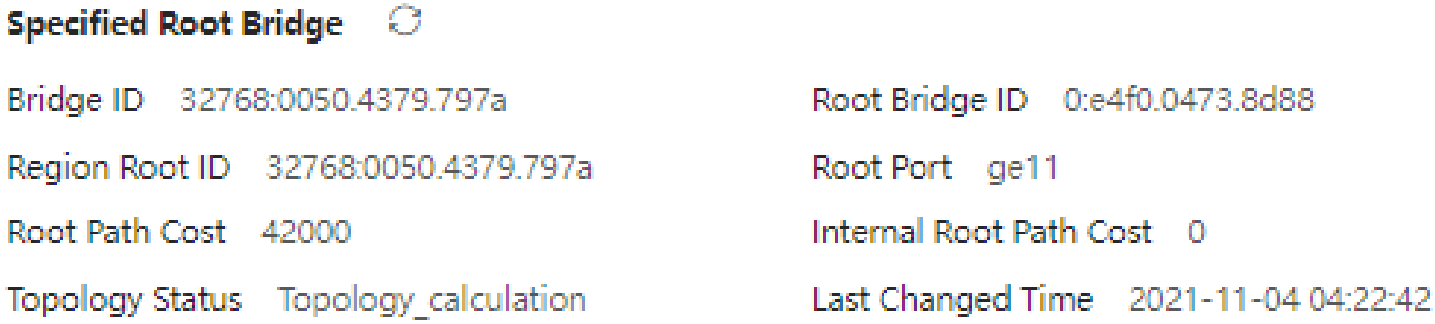
- **Instance ID:** são permitidos um total de 64 instâncias. O 0 indica Spanning Tree interno. O Spanning Tree será calculado em cada instância de forma separada.
- **VLAN Mapping List:** especifica a lista de VLANs mapeadas na instância.

- **Bridge Priority:** especifica o o valor de prioridade do sistema, usada para a eleição do root bridge de instâncias em regiões internas.

- **+ Add:** ao clicar no botão +Add é aberta a tela de ADD MSTP Instance. Deve-se configurar o Instance ID, o VLAN Mapping list e o valor de bridge priority para a instancia que está sendo criada



Especified Root Bridge



- **Bridge ID:** especifica a prioridade da bridge e o endereço MAC da bridge do switch.
- **Root bridge ID:** especifica o dispositivo Root bridge do CIST (Common and internal Spanning Tree).
- **Region Root ID:** especifica a prioridade do Root ID da região e o MAC Addres da bridge da região em que o Switch está localizado.
- **Root port:** especifica a porta mais próxima do Root Bridge no Switch que não é root bridge
- **Root Path Cost:** especifica a soma do custo do caminho da root port e o custo do caminho do root para todos os pacotes que passam pelo Switch. O custo de caminho do root para a root bridge é 0.
- **Internal Root Path Cost:** especifica o valor de referência usado para escolher o caminho e calcular o custo do caminho até a região MST. É também o critério usado para determinar se a porta é escolhida como a root port. Quanto menor o valor, maior será a prioridade.
- **Topology Status:** trará o status da porta que participa do Spanning Tree. Podemos ter dois valores:

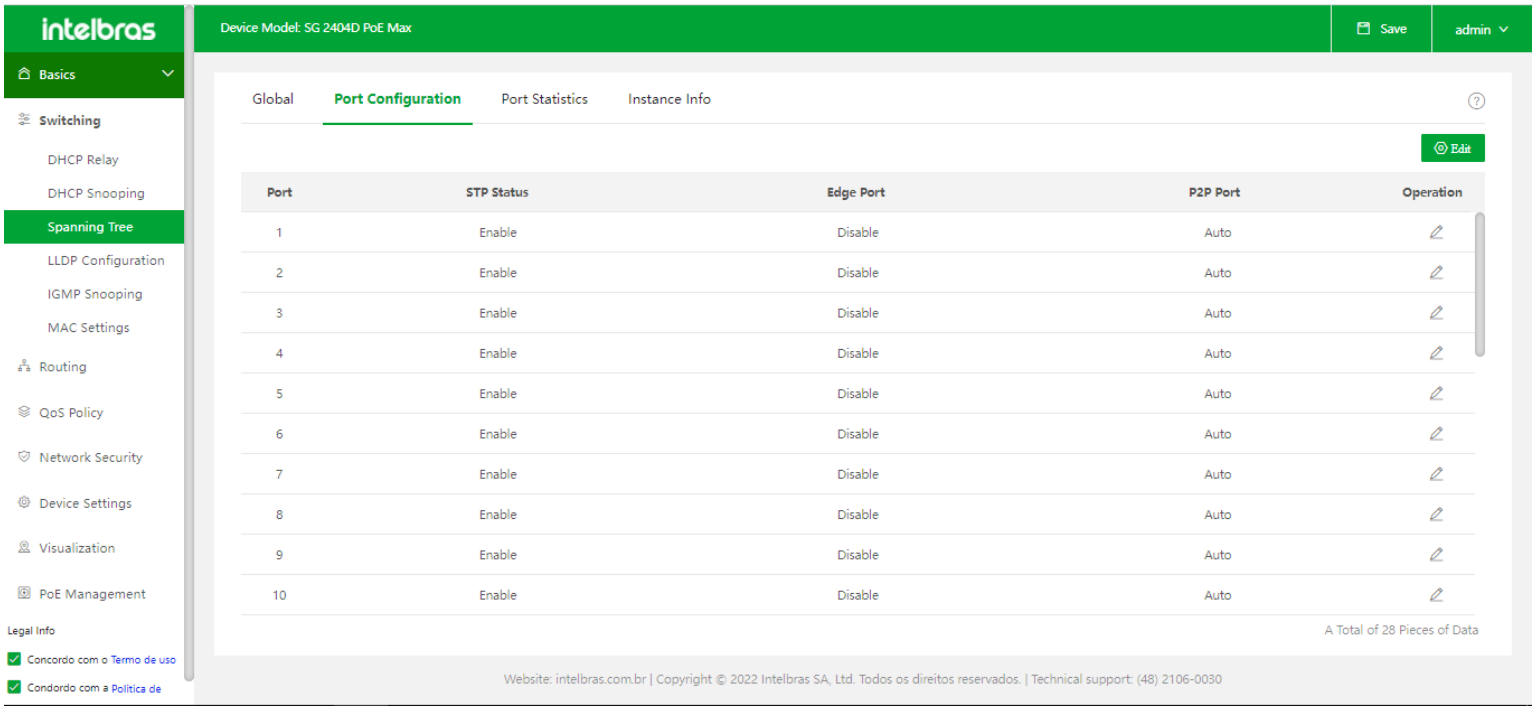
  Topology_Calculation: indica que a porta está instável durante o cálculo da spanning tree e os pacotes não podem ser encaminhados. Normalmente, com os parâmetros de tempo padrão, o status do cálculo_topologia pode durar até 50 segundos quando o modo é STP, enquanto para RSTP e MSTP, a duração do tempo é inferior a 3 segundos.

  Topological_stability: indica que a porta está estável e a rede está normal.

- **Last Changed Time:** especifica a hora em que as ultimas alterações na topologia foram feitas.

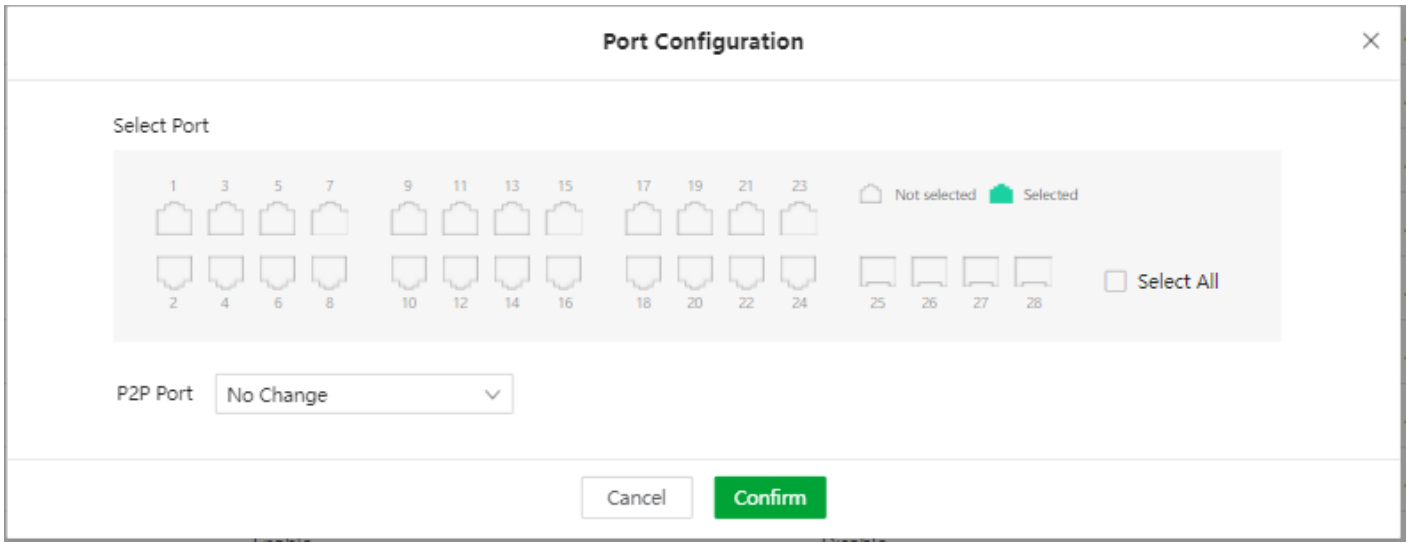
Port Configuration

A tela de Port Configuration é usada para configurar e exibir os parâmetros STP de cada porta.



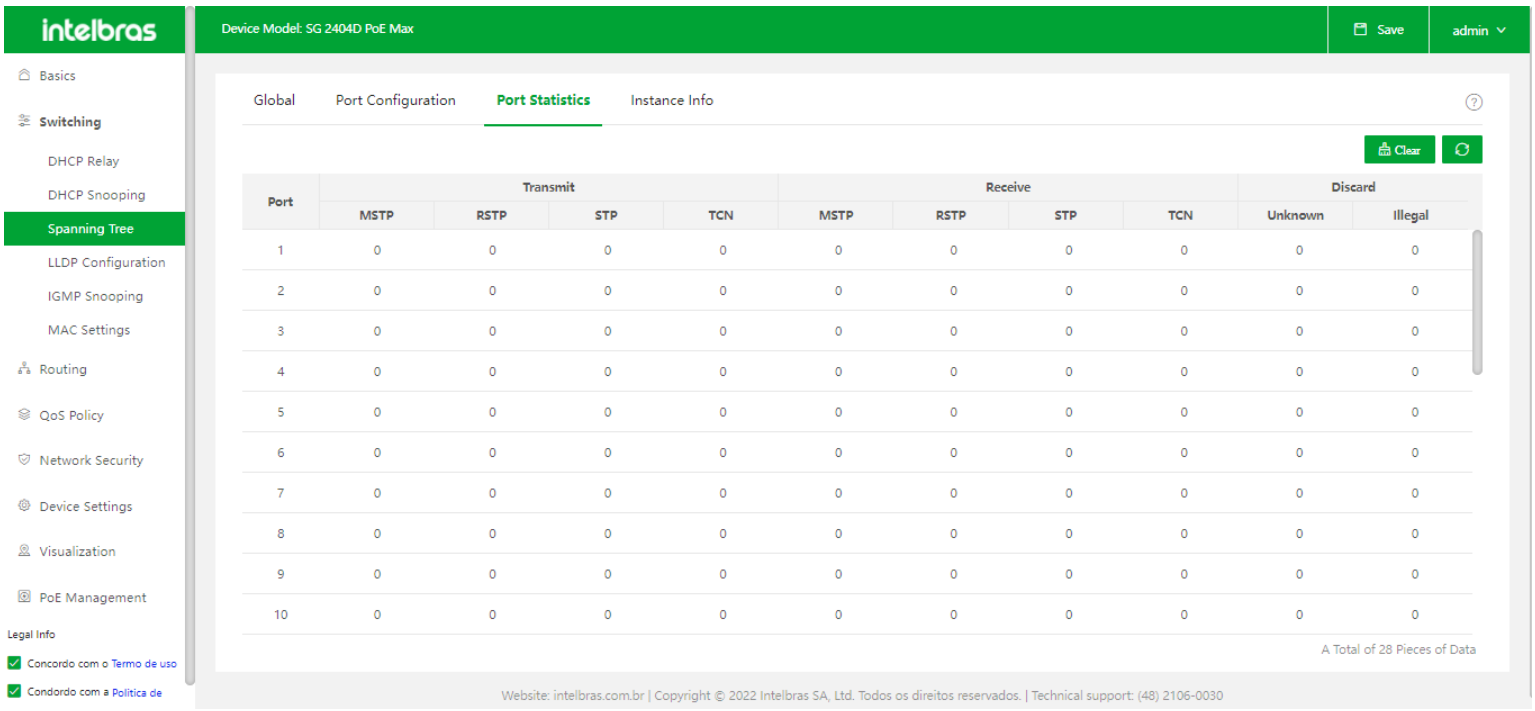
Na tela de port configuration temos as informações:

- **STP Satus:** exibe se a função está habilitada na porta.
- **Edge port:** a edge port pode migrar rapidamente do estado de congestionamento para o estado de encaminhamento. Não há necessidade de esperar o tempo de atraso. A edge port é comumente conectada aos terminais. Ao receber mensagens BPDU, a edge port é alterada para uma port-non-edge. Todas as portas são edge port por padrão
- **P2P Port:** a porta P2P (Ponto a ponto) pode realizar uma migração rápida. No modo RSTP/MSTP, todas as portas no modo full duplex são consideradas portas P2P. A porta padrão identifica links automaticamente.
- **Operation:** é utilizado para modificar os parametros STP da respectiva porta.
- **Edit:** é utilizado para modificar os parametros do STP correspondente a porta. Ao clicar no botão Edit temos a tela Port Configuration, onde podemos configurar uma ou mais portas como P2P port.



Port Statistics

Na tela de port statistics temos acesso a informações de número de mensagens de spanning tree transmitidas, recebidas e descartadas por cada porta.



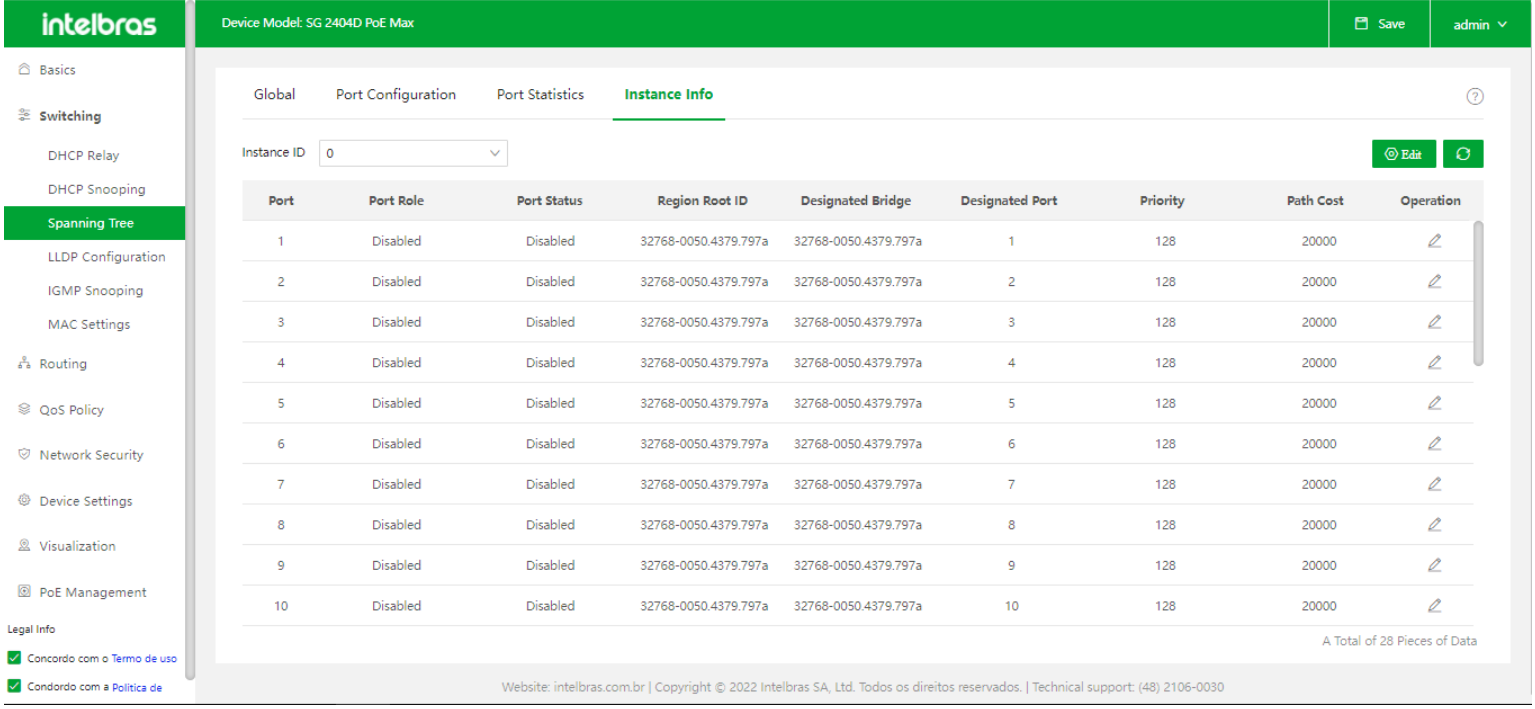
São contabilizados os pacotes BPDU transmitidos, recebidos e descartados em cada porta. Temos a quantidade de pacotes MSTP, RSTP, STP e TCN (topology change notification). Nos pacotes descartados temos unknown (especifica os pacotes desconhecidos que foram descartados) e illegal (especifica o número de pacotes STP de erro que foram descartados).

Ainda na tela de port configuration temos a presença de dois botões, clear e refresh.

- **Clear:** Quando utilizado ele limpa todas as informações de estatísticas das portas.
- **Refresh:** Quando utilizado ele renova(atualiza) as informações de estatísticas das portas.

Instance info

Esta tela é utilizada para exibir e configurar as informações da instância MSTP.



- **Instance ID:** é utilizado para selecionar o ID de uma instância e verificar as informações de estado do STP de cada porta da instância
- **Port Role:** especifica a função que a porta desempenha na instância de spanning tree. Temos as funções:

  Disable:a função spanning tree da porta está desabilitada ou a porta não está conectada a nenhum dispositivo.

  Designated: indica que a porta é a porta designada no spanning tree, que encaminha dados para segmentos ou dispositivos de rede de downlink.

  Master: indica que a porta fornece o menor custo de caminho raiz da região para a root bridge no MSTP.

  Alternate: indica que a porta é a porta alternativa no spanning tree, que é o backup da porta raiz e da porta master.

  Backup: indica que a porta é a porta de backup no spanning tree, que é o backup da porta designada.

- **Port Status:** Especifica o status operacional da porta. Podemos ter os status:

  Disabled: a porta não está conectada a nenhum dispositivo ou a função de spanning tree da porta está desativada.

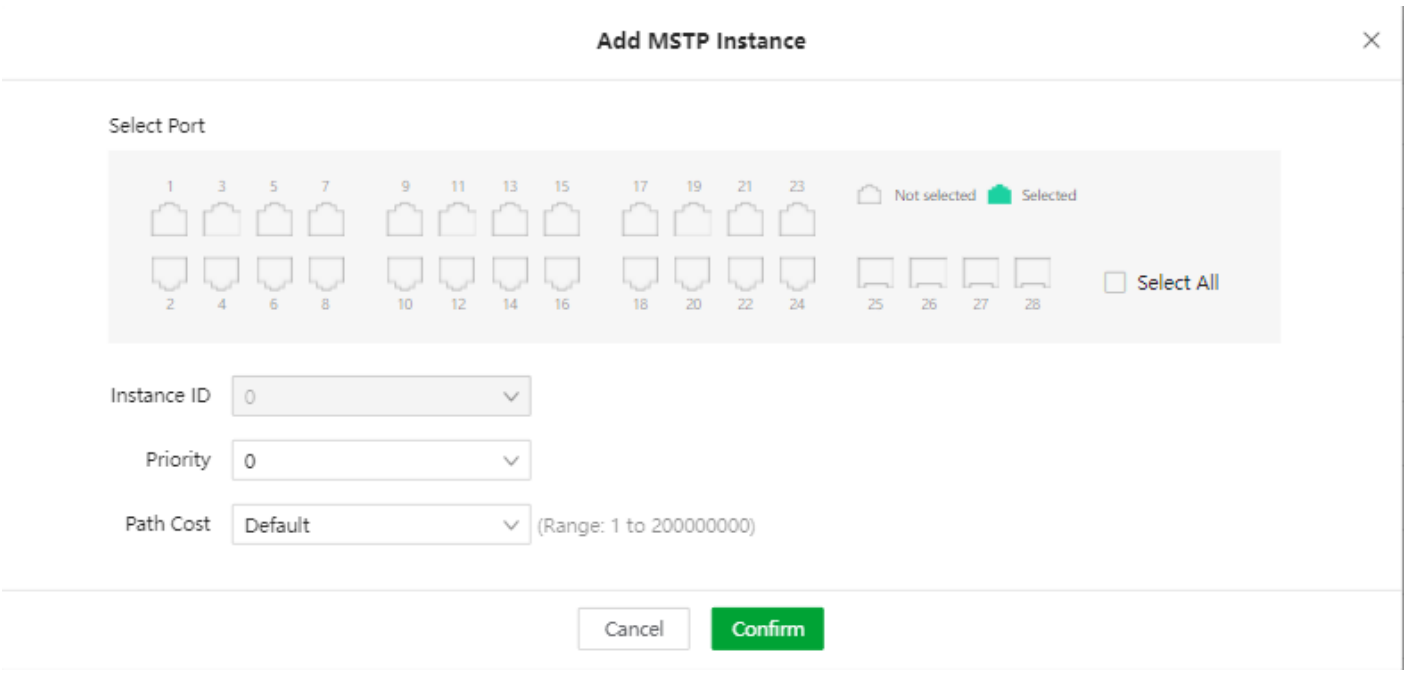
  Forwarding: a porta pode receber e transmitir mensagens BPDU e também encaminhar mensagens de dados. Depois que a topologia estiver estável, as portas Master, Designated e Root estarão todas no status Forwarding.

  Learning: a porta pode receber e transmitir mensagens BPDU, mas não encaminha mensagens de dados. As portas Master, Designated e Root estão em um status de transição antes que a topologia seja estável.

  Discarding: portas neste estado podem receber e transmitir mensagens BPDU, mas não encaminha mensagens de dados. Depois que a topologia estiver estável, as portas Alternate e Backup estarão no status Descartando.

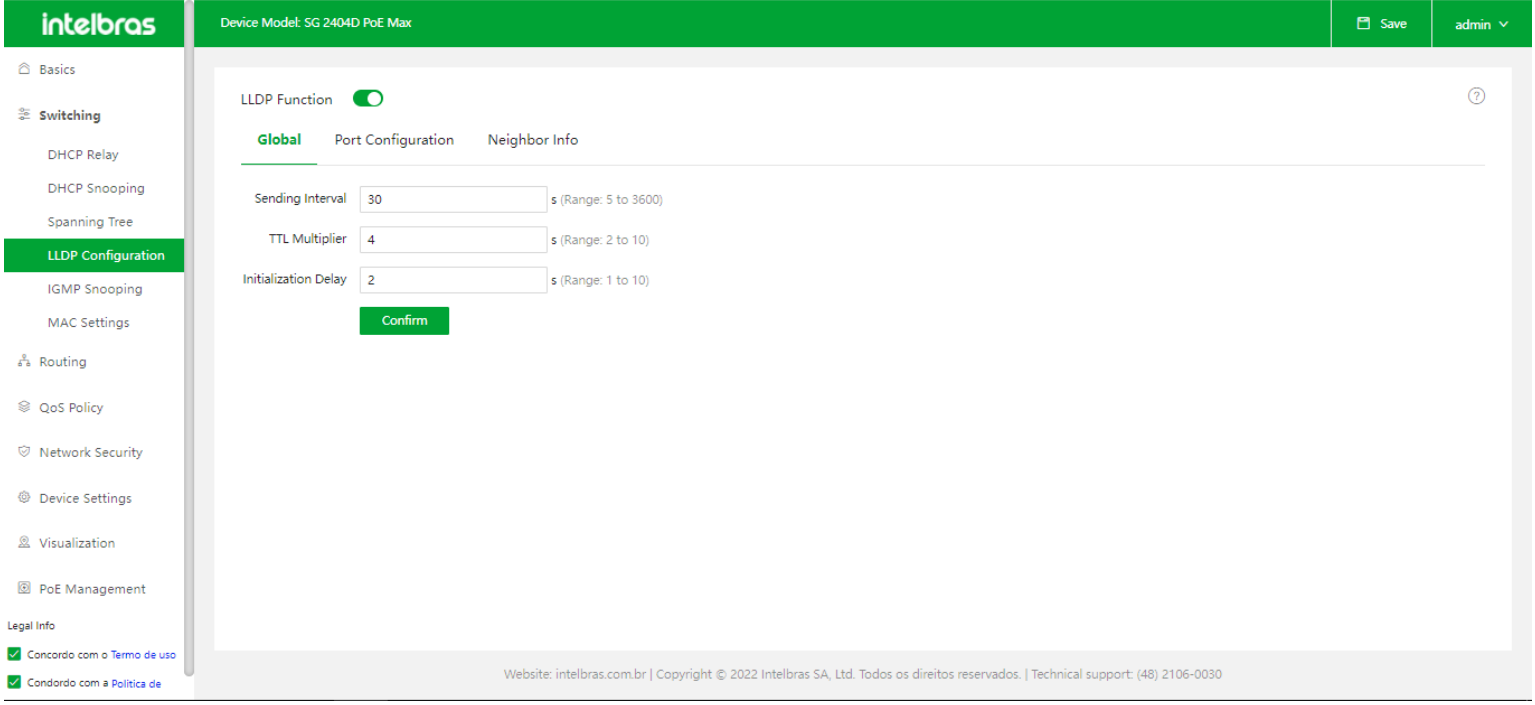
- **Region Root ID:** especifica o dispositivo com o menor bridge ID nas instâncias MSTI e IST.
- **Designated bridge:** especifica o bridge ID do dispositivo que está conectado ao switch e é usado para encaminhar mensagens BPDU ao switch. A bridge ID designada da root port e da porta de backup é a bridge ID do dispositivo usado para transmitir mensagens BPDU. A bridge ID designada da porta designada é a bridge ID do próprio dispositivo.
- **Designated port:** especifica a porta para a qual a bridge designada encaminha mensagens BPDU.

- **Priority:** quando a root brige, o root path cost e a bridge de rede são todos iguais, a prioridade da porta é um critério importante usado para determinar se a porta é escolhida como a root port. Quanto menor for o valor da prioridade da porta, maior será a prioridade.
- **Path cost:** especifica o valor de referência usado para escolher os caminhos e calcular os custos dos caminhos na instância MST. Também é um critério usado para determinar se a porta é escolhida como a root port. Quanto menor o valor, maior será a prioridade.
- **Operation:** ao clicar é aberta a tela de Edit MSTP Instance, onde se pode modificar a prioridade e o custo do caminho da porta correspondente.
- **Edit:** ao clicar é aberta a tela de Add MSTP Instance, É usado para configurar a prioridade da porta e o custo do caminho em uma ou mais portas.



LLDP Configuration

O LLDP (Link Layer Discovery Protocol) fornece um método de descoberta de camada de link padrão que organiza os principais recursos, endereço de gerenciamento, identificador de dispositivo e informações de identificador de interface de dispositivos. Estas informações são dispostas em diferentes TLVs (Type/Lenght/Value) e os encapsula em LLDPDUs (Link Layer Discovery Protocol Data Unit) para liberar para os vizinhos aos quais estão diretamente conectados. Após receber essas informações, os vizinhos irão salvá-las como o padrão MIB (Management Information Base) para permitir que o sistema de gerenciamento de rede verifique e julgue as condições de comunicação do link.



- **LLDP Function:** Este botão tem a finalinadade de ativar ou desativar a função LLDP no Switch.

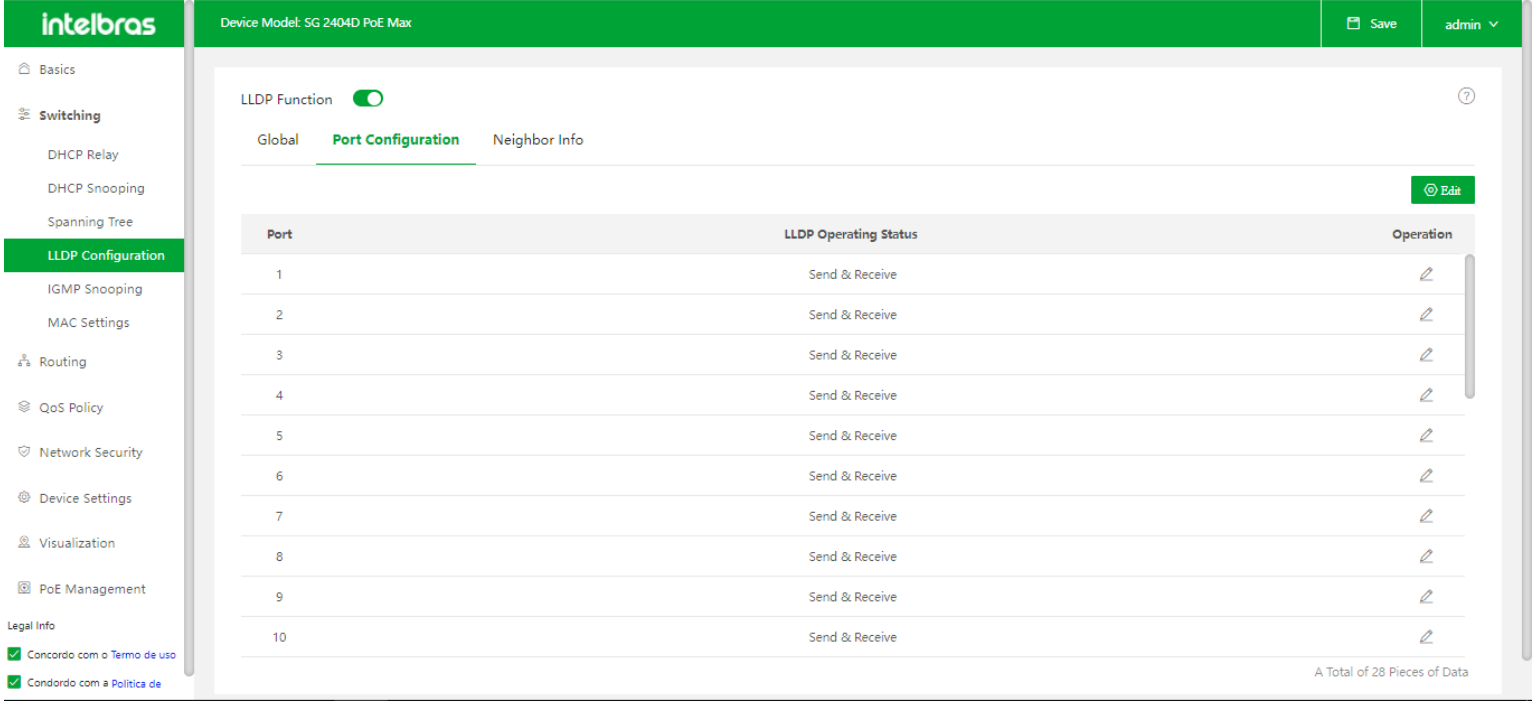
Global

Nesta tela temos as configurações dos parametros globais do LLDP. Temos os parâmetros:

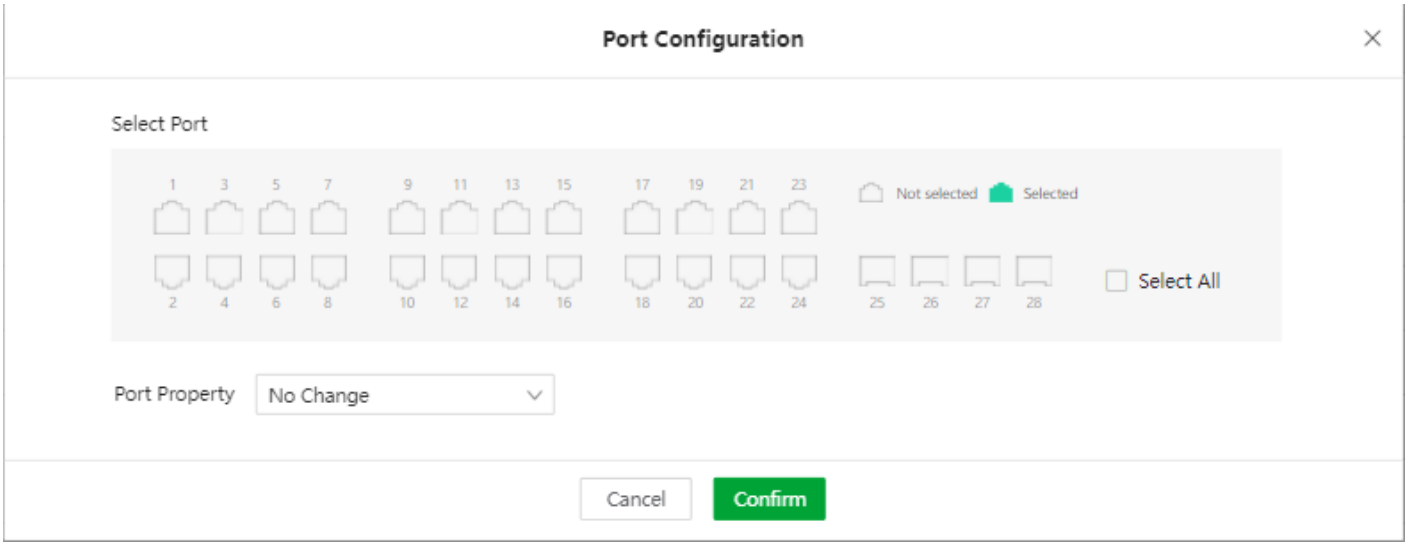
- **Sending interval:** especifica o intervalo no qual o switch transmite LLDPDUs aos vizinhos. O valor padrão é 30 segundos.
- **TTL multiplier:** o TTL multiplier é usado para controlar o valor do campo TTL dos LLDPDUs transmitidos pelo switch. O TTL é a duração em que as informações locais podem sobreviver nos dispositivos vizinhos. Podemos calcular o TTL da seguinte maneira: TTL = TTL Multiplier x sending interval. O valor padrão do TTL multiplier é 4.
- **Initialization delay:** para evitar que a porta execute a inicialização continuamente como resultado de alterações frequentes do modo de operação, você pode configurar um tempo de atraso de inicialização para a porta que permite que a inicialização seja feita algum tempo após a alteração do modo de operação. O valor padrão é 2.

Port Configuration

Neste menu pode-se configurar a propriedade das portas.



- **Edit:** ao clicar no botão Edit, será aberta a tela de Port Configuration.



Nesta tela pode-se alterar a configuração de status de uma ou mais portas. Temos os seguintes status disponíveis:

Disabled: desabilita o LLDP na porta, que não irá processar nem enviar quadros LLDPDU.

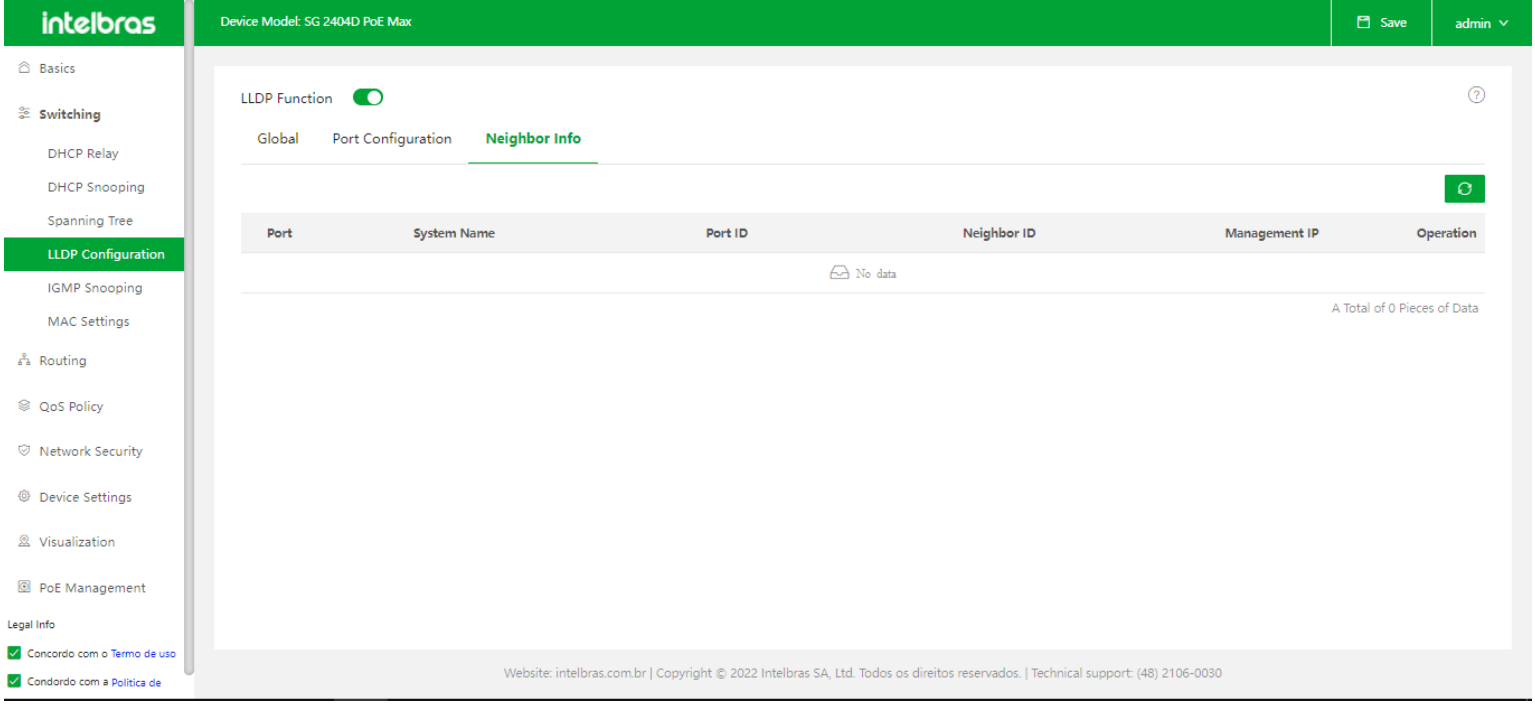
Send olny: a porta irá apenas enviar quadros LLDPDU.

Receive only: a porta irá apenas receber quadros LLDPDU.

Send & receive: a porta irá receber e enviar quadros LLDPDU.

Neighbor Info

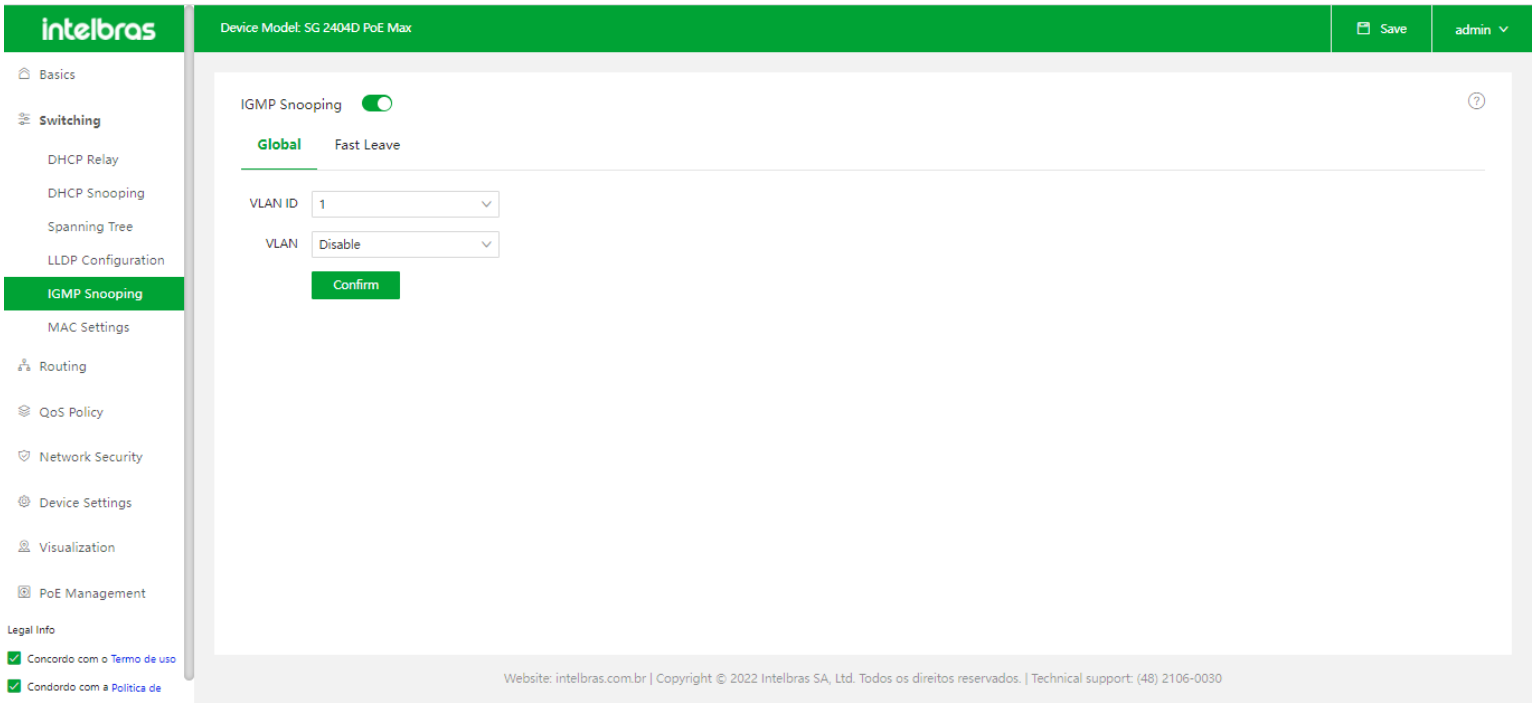
Neste menu temos as informações sobre os dispositivos vizinhos ao Switch.



- **Port:** especifica a porta que recebeu as mensagens LLDP.
- **System name:** exibe o system name do dispositivo vizinho.
- **Port ID:** informa a porta do dispositivo vizinho.
- **Neighbor ID:** enforma o MAC Address do dispositivo vizinho.
- **Management IP:** exibe o endereço IP de gerência do dispositivo vizinho.
- **Operation:** ao clicar é aberta a tela de "Edit Port", onde pode-se configurar o Port Property da respectiva interface física.

IGMP Snooping

IGMP Snooping (Internet Group Management Protocol Snooping) é um mecanismo de controle multicast que funciona na camada 2 do switch. Ele pode efetivamente impedir que os grupos multicast sejam transmitidos em rede.



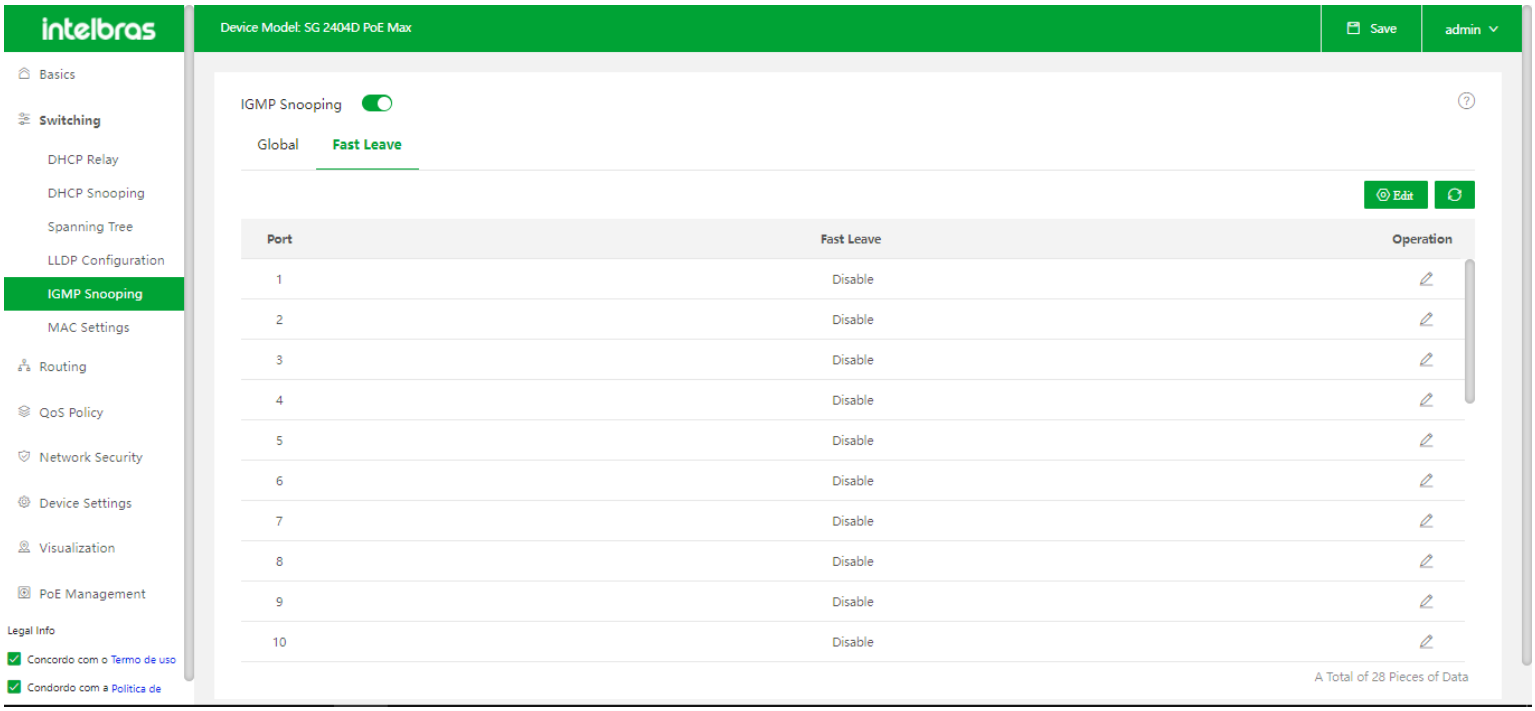
IGMP Snooping: temos o botão de IGMP Snooping, que habilita ou desabilita a função de forma global.

Global

Ele é usado para configurar os parâmetros globais do IGMP snooping.

- **VLAN ID:** especifica a VLAN que deseja-se configurar o IGMP.
- **VLAN:** habilita ou desabilita o IGMP Snooping na VLAN selecionada em VLAN ID.
- **Multicast VLAN status:** especifica a VLAN que deseja-se configurar o IGMP.
- **Protocol Version:** é possível escolher a versão do IGMP Snooping que deseja utilizar. Podendo ser a V1, V2 ou V3.
- **Routing time aging time:** tempo de envelhecimento do roteamento multicast.
- **General query response time:** intervalo de tempo entre respostas das consultas IGMP.
- **Specific query response time:**intervalo de tempo entre respostas das consultas especificas IGMP.
- **Aging Time of host port:** tempo em que o grupo multicast ficará salvo na porta.
- **Multicast discard:** discarta pacotes multicast.

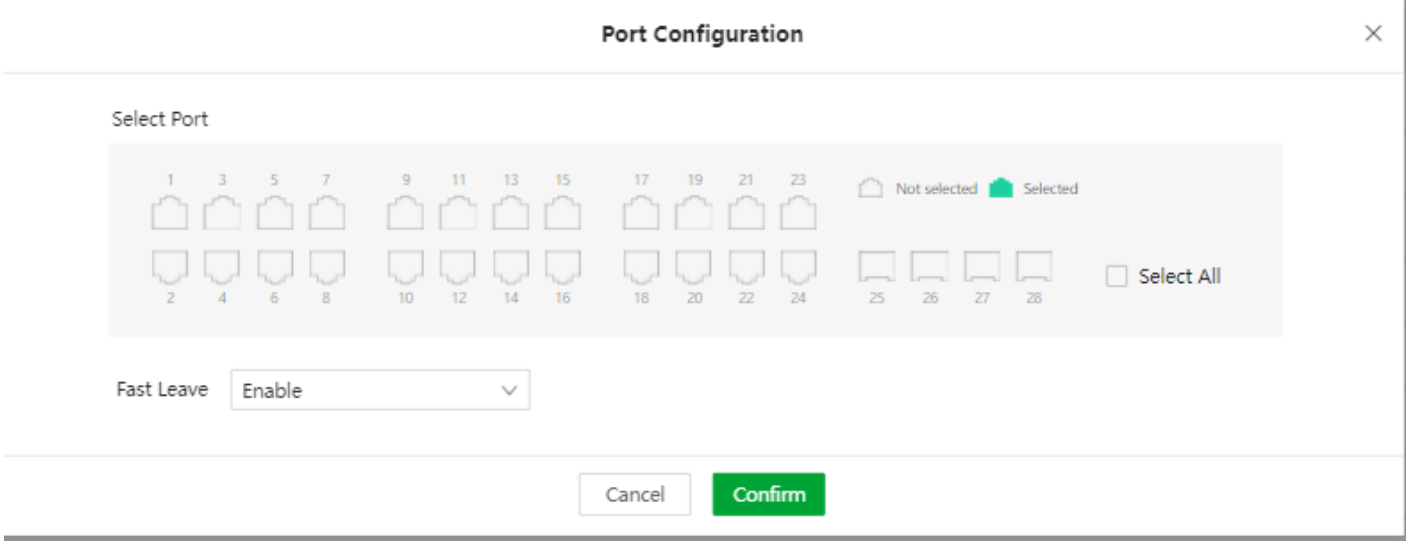
Fast Leave



Com a função habilitada, ao receber as mensagens IGMP leave group desta porta, o switch remove a porta da lista de encaminhamento multicast de IGMP Snooping correspondente e não espera até que o tempo de envelhecimento da porta do host expire.

- **Edit**

>Ao clicar no botão Edit, no canto direito superior da página, é aberta a tela de Port Configuration, onde é possível habilitar/desabilitar o fast leave em uma ou mais portas.



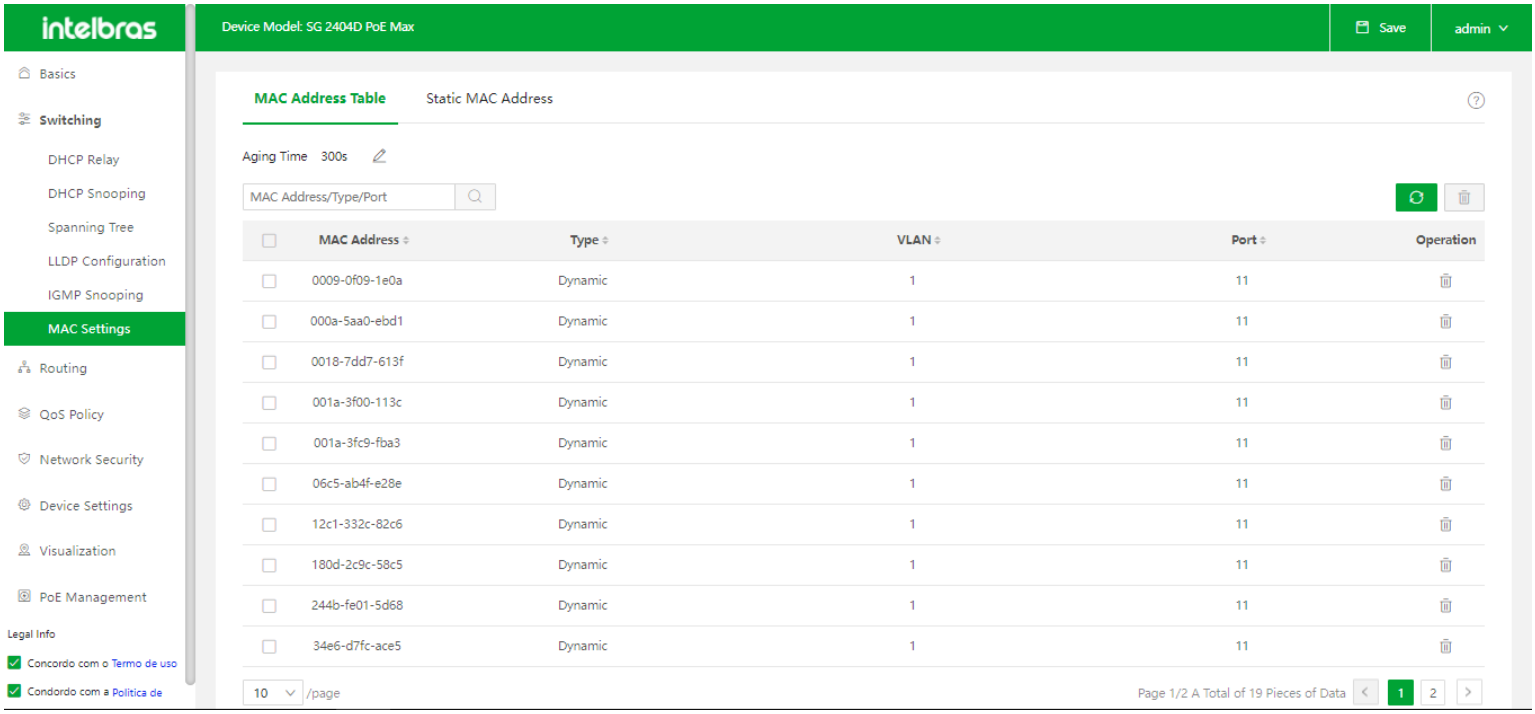
- **Refresh**

Temos também o botão de Refresh, que fica ao lado do botão de Edit, que ao ser clicado atualiza as informações da página.

Mac Settings

Nesta página temos informações sobre a tabela MAC do Switch. O Switch SG 2404D PoE Max tem capacidade de aprender até 16K de endereços MAC

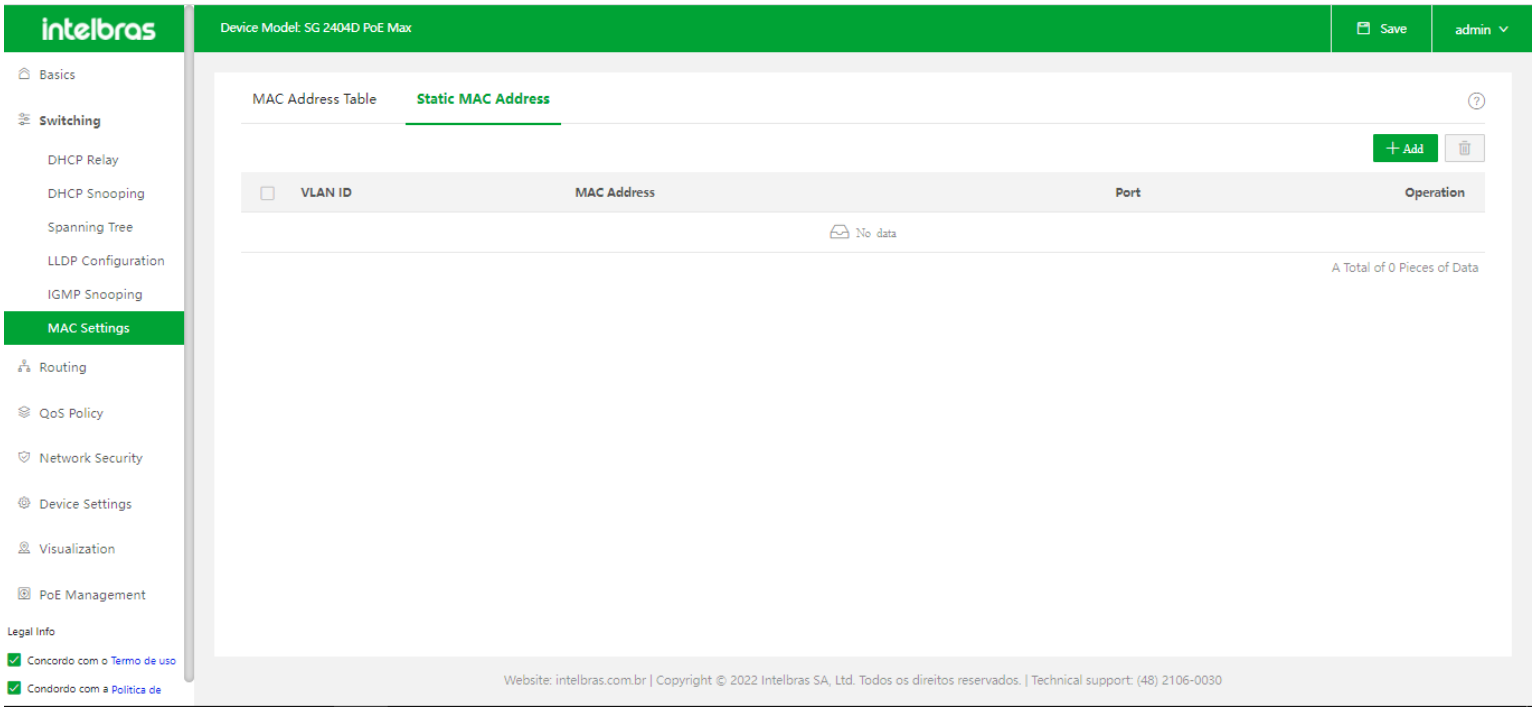
MAC Address Table



- **Aging Time:** especifica o tempo de envelhecimento da tabela de endereços MAC, que é funcional apenas para tabelas dinâmicas. O Switch monitora o ultimo envio de quadros para o MAC, se o tempo de envelhecimento terminar e nenhum outro quadro for enviado o endereço MAC será excluído automaticamente da tabela.
- **Type:** especifica o tipo do endereço MAC.
- **Estático:** especifica que o endereço MAC pertence a tabela configurada manualmente pelo administrador.
- **Dynamic:** especifica que o endereços MAC pertence a tabela gerada automaticamente pelo switch.
- **VLAN:** informa a qual VLAN pertence o respectivo MAC Address.

- **Port:** especifica a porta física que registrou a presença do MAC Address.
- **Operation:** clicando no botão de operation o endereço MAC em questão será retirado da tabela.

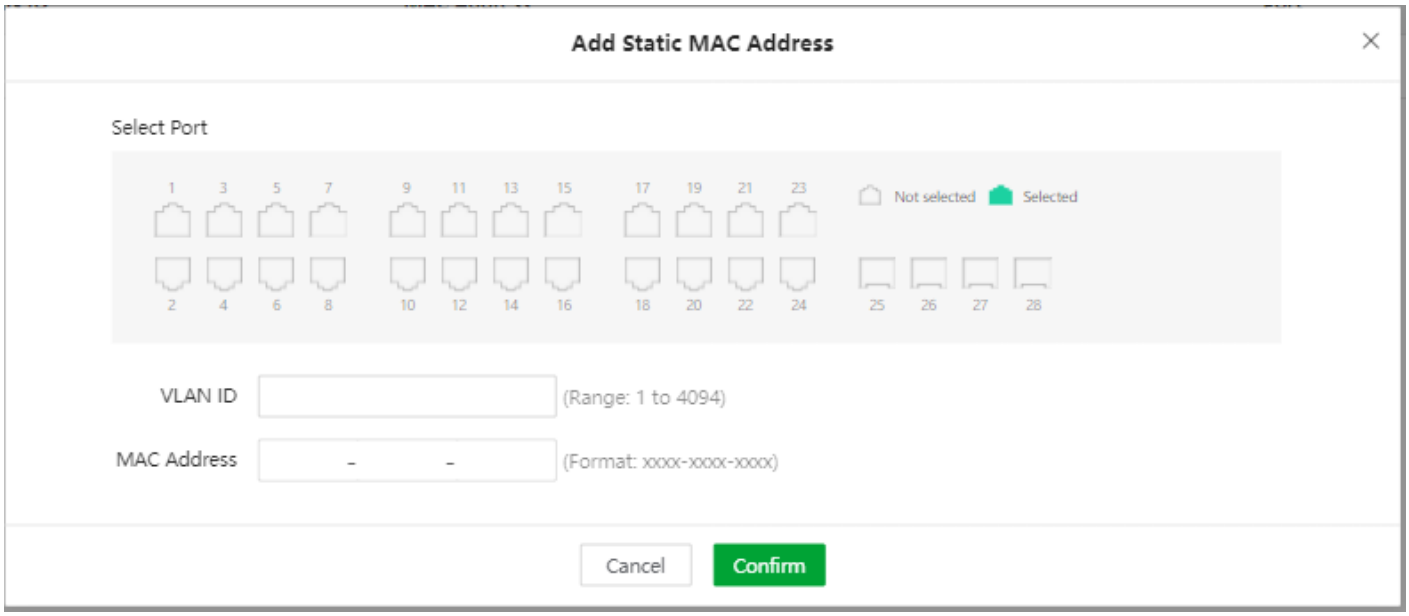
Static MAC Address



Na tela de Static MAC Address temos a opção de configurar manualmente endereços MAC que desejamos adicionar a tabela MAC.

- **+ Add:** Ao clicar no botão de +ADD temos a tela de ADD Static Mac Address. Nesta tela podemos configurar um MAC Address, a porta e a VLAN ao qual o MAC ficará apreendido.

OBS: O formato do MAC Address deve ser XXXX-XXXX-XXXX

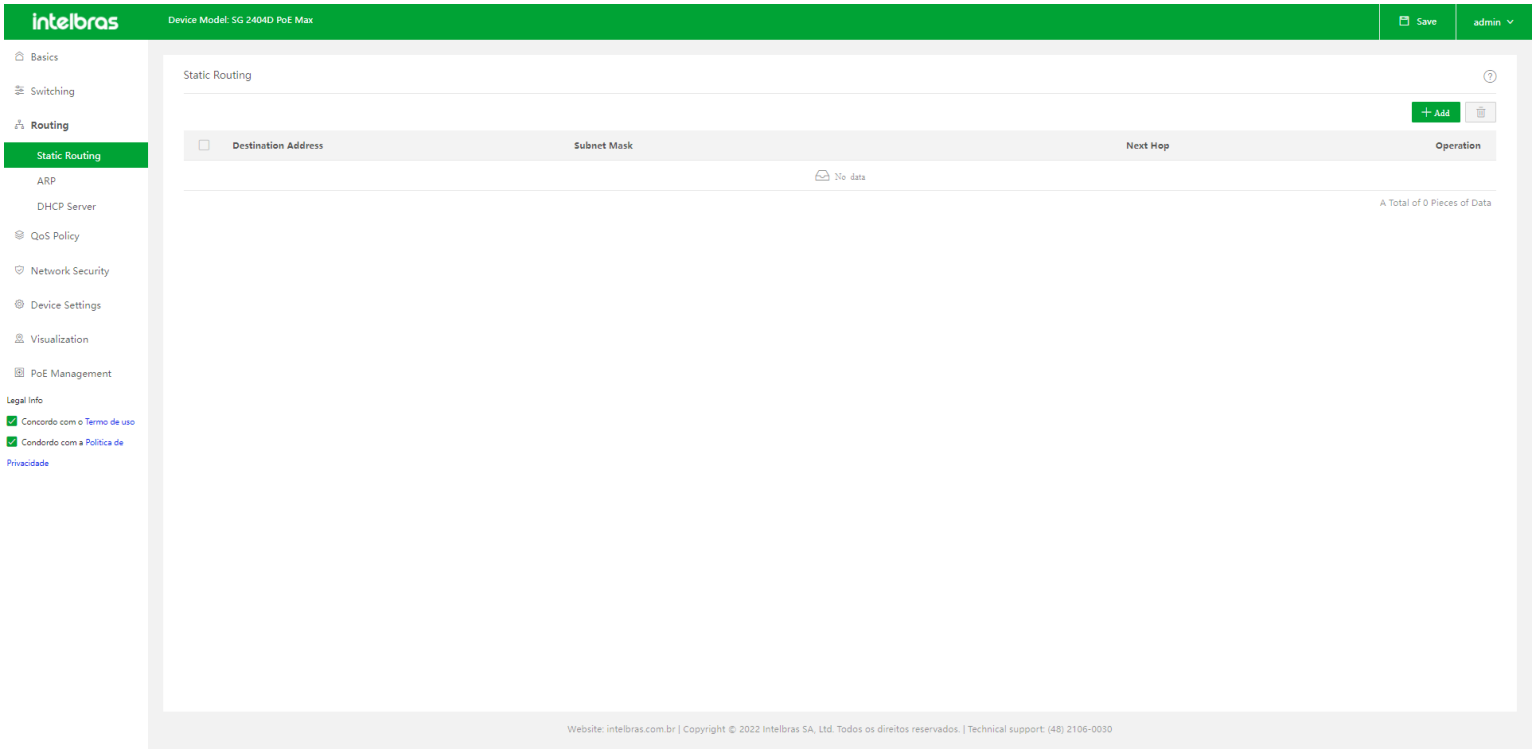


ROUTING

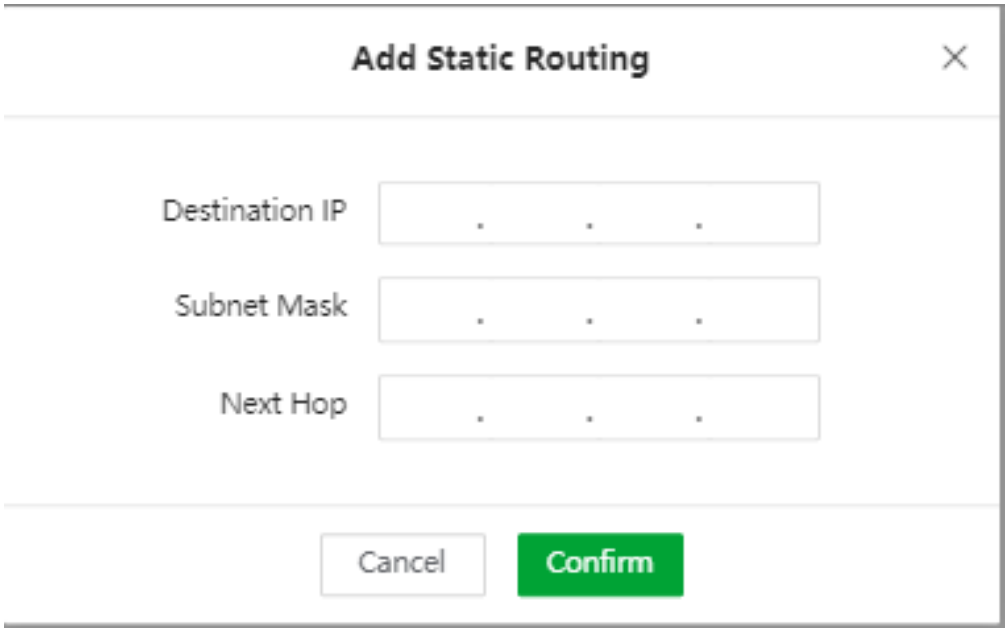
No menu de Routing temos algumas funções voltadas a camada de rede, temos as funções de rota estática, servidor DHCP e controle da tabela ARP do Switch.

Static Routing

É usado para verificar e configurar as regras de rota estática. Se os pacotes precisarem ser encaminhados para segmentos de rede de conexão não direta, serão necessárias rotas estáticas.



- **+ Add:** Para adicionar uma nova rota estática basta clicar no botão + Add, será aberta a tela de Add Static Routing.

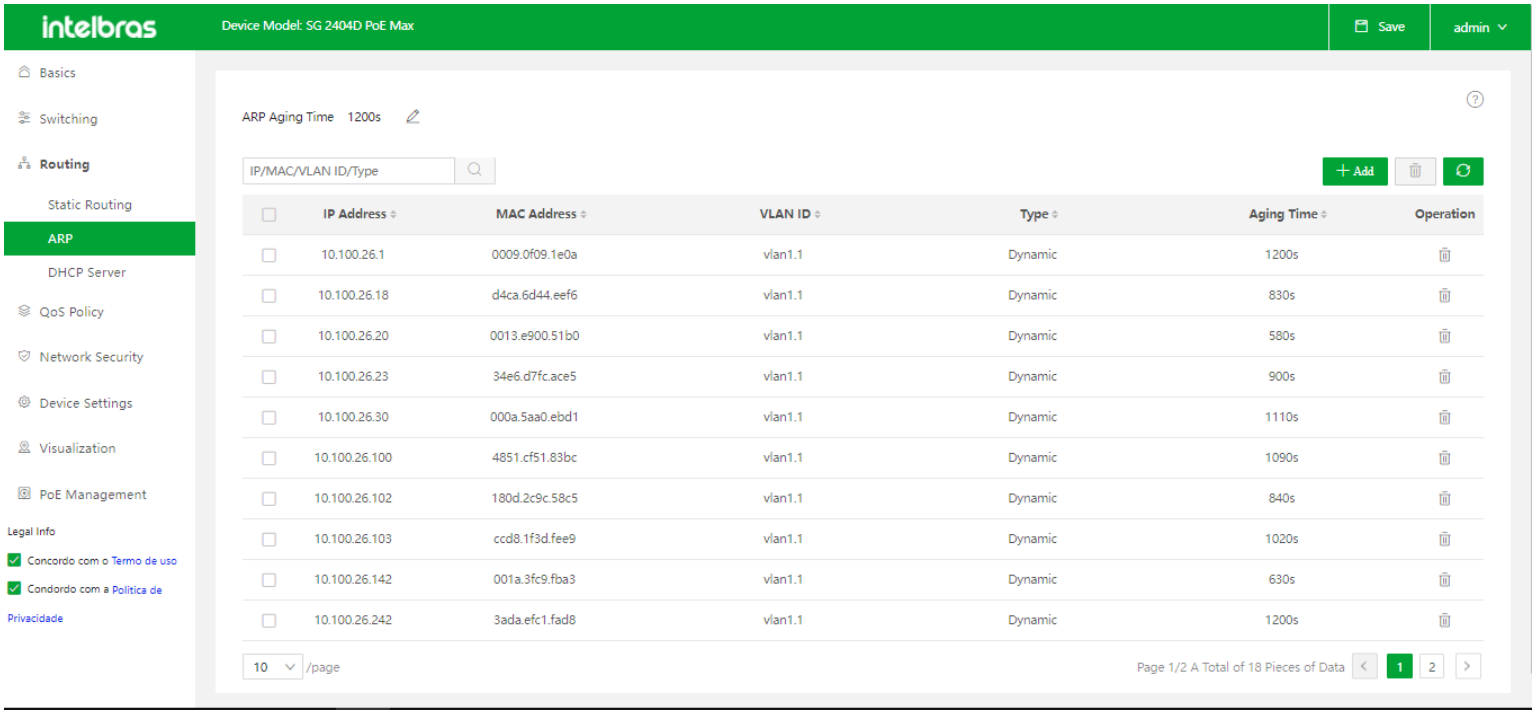


Para configurar uma rota estática é necessário configurar os três campos a seguir:

- **Destination IP:** especifica o segmento de rede da rede de destino.
- **Subnet Mask:** especifica a máscara de sub-rede da rede de destino.
- **Next Hop:** especifica o endereço IP de entrada da rota do próximo salto após a saída dos pacotes do switch, será o Gateway.

ARP

Nesta tela temos a tabela ARP do Switch, que pode conter endereços apreendidos de forma automática e também adicionados manualmente.

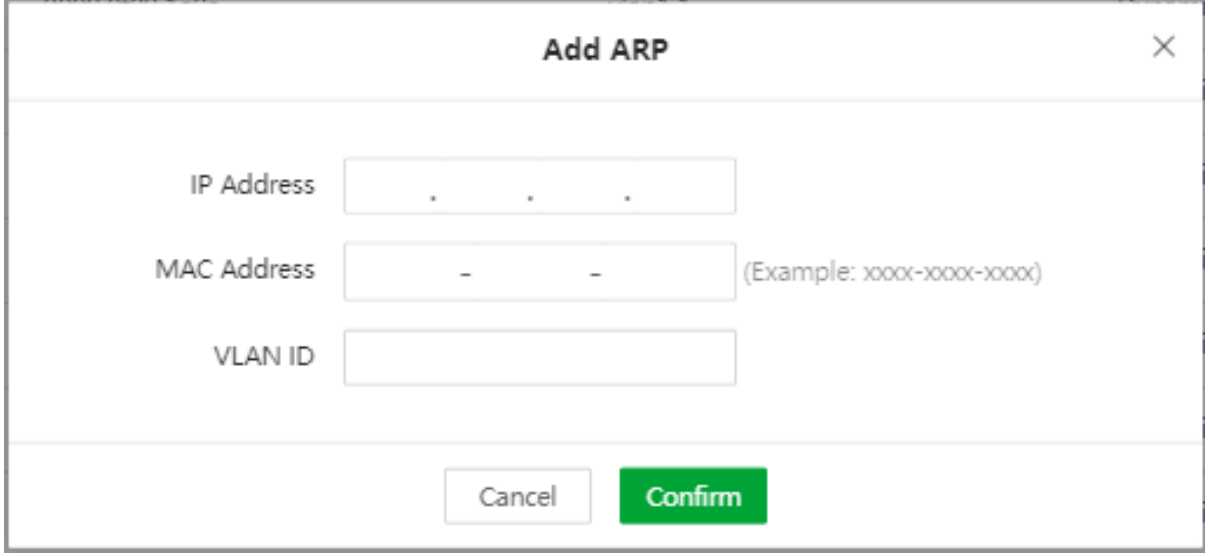


- **ARP Aging time:** especifica o tempo de envelhecimento do ARP. Se a duração desde a última vez que o switch recebeu as mensagens ARP de um determinado endereço exceder o aging time, o endereço será excluido da tabela.
- **IP Address:** especifica o IP do host em questão
- **MAC Address:** especifica o endereço MAC do host em questão.
- **VLAN ID :** especifica a VLAN ao qual pertence o host.
- **Type:** especifica o modo pelo qual o registro foi adicionado a tabela ARP.

  Dynamic: especifica que o endereço foi identificado automaticamente pelo switch. O ciclo de vida é o aging time configurado no ARP.

  Static: especifica o host configurado manualmente. Neste caso o registro está livre das limitações do tempo de envelhecimento ARP, ficará por tempo indeterminado.

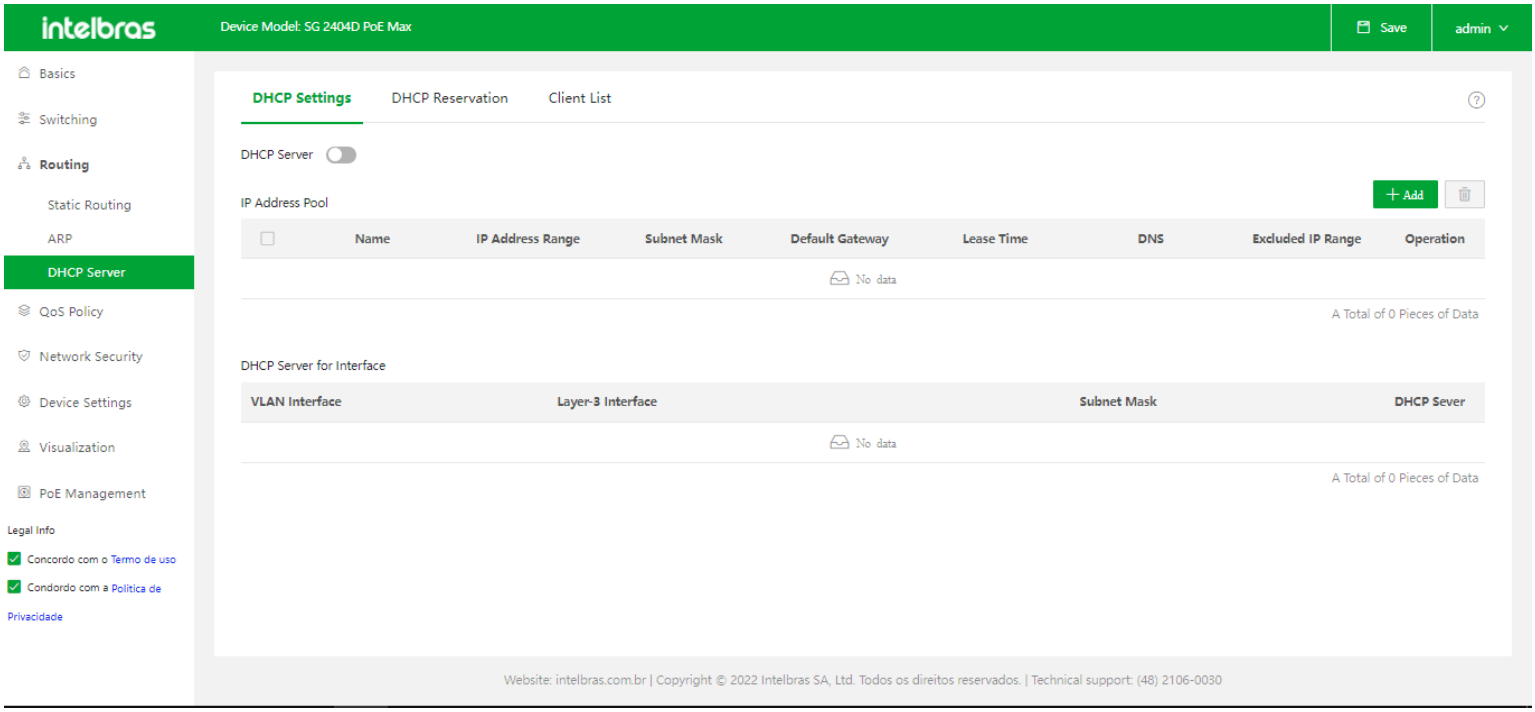
- **Aging time:** especifica o tempo de aging time que ainda resta para o registro do host, se o tempo chegar a 0 o registro será excluido automaticamente.
- **Operation:** permite que seja excluido o resgistro de um host na tabela ARP.
- **+ Add:** permite a inclusão de um host de forma manual. Neste caso não haverá aging time, o endereço só sairá da tabela caso o usuário o exclua.



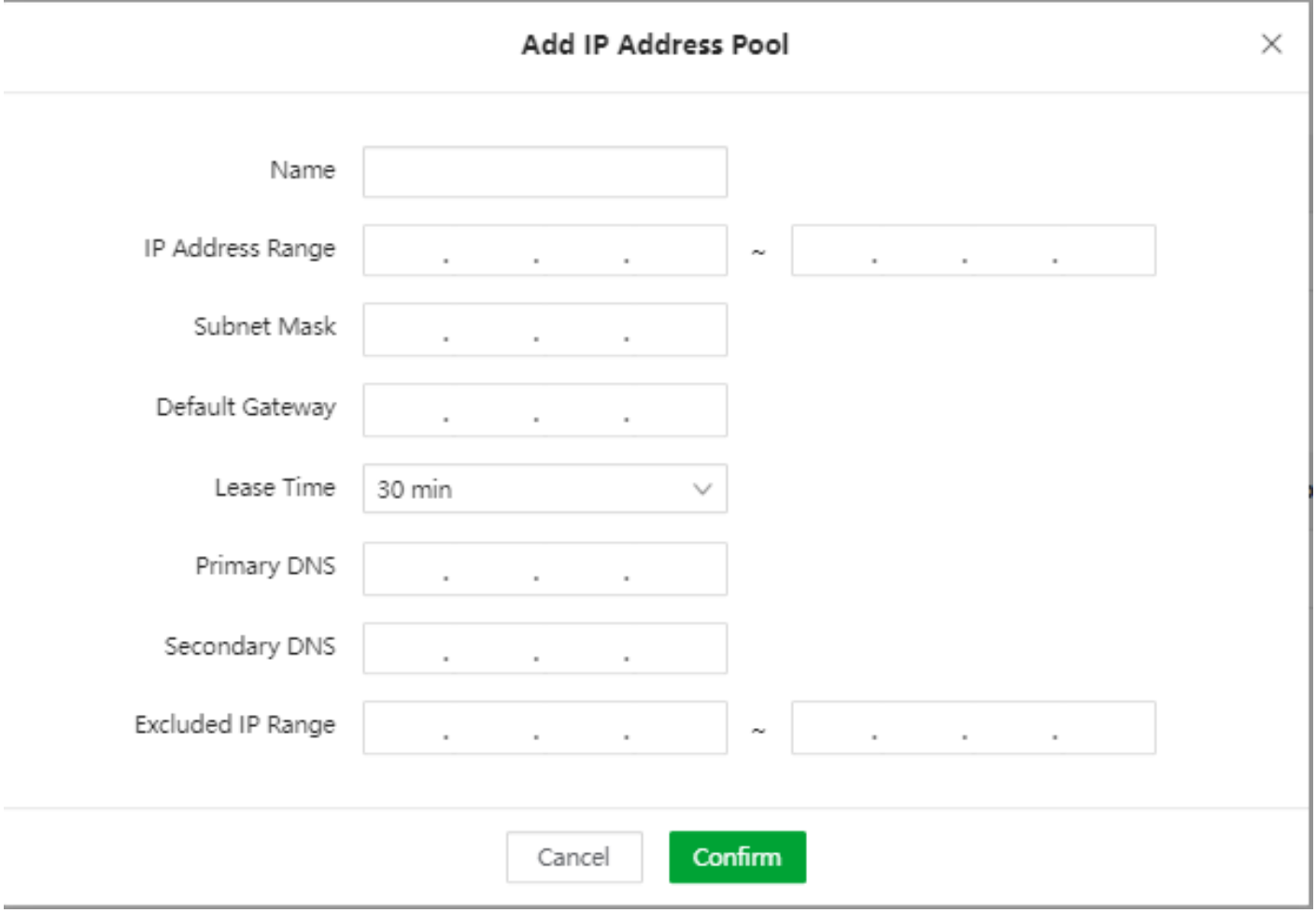
DHCP Server

O switch atribui automaticamente endereços IP, máscaras de sub-rede, gateways, endereços DNS, entre outras informações aos clientes na LAN.

DHCP Settings



- **DHCP Server:** Este botão serve para ativar ou desativar o servidor DHCP do Switch.
- **+ Add:** Para adicionar um novo servidor DHCP, deve-se clicar no botão +Add e será aberta a tela de Add IP Address Pool.



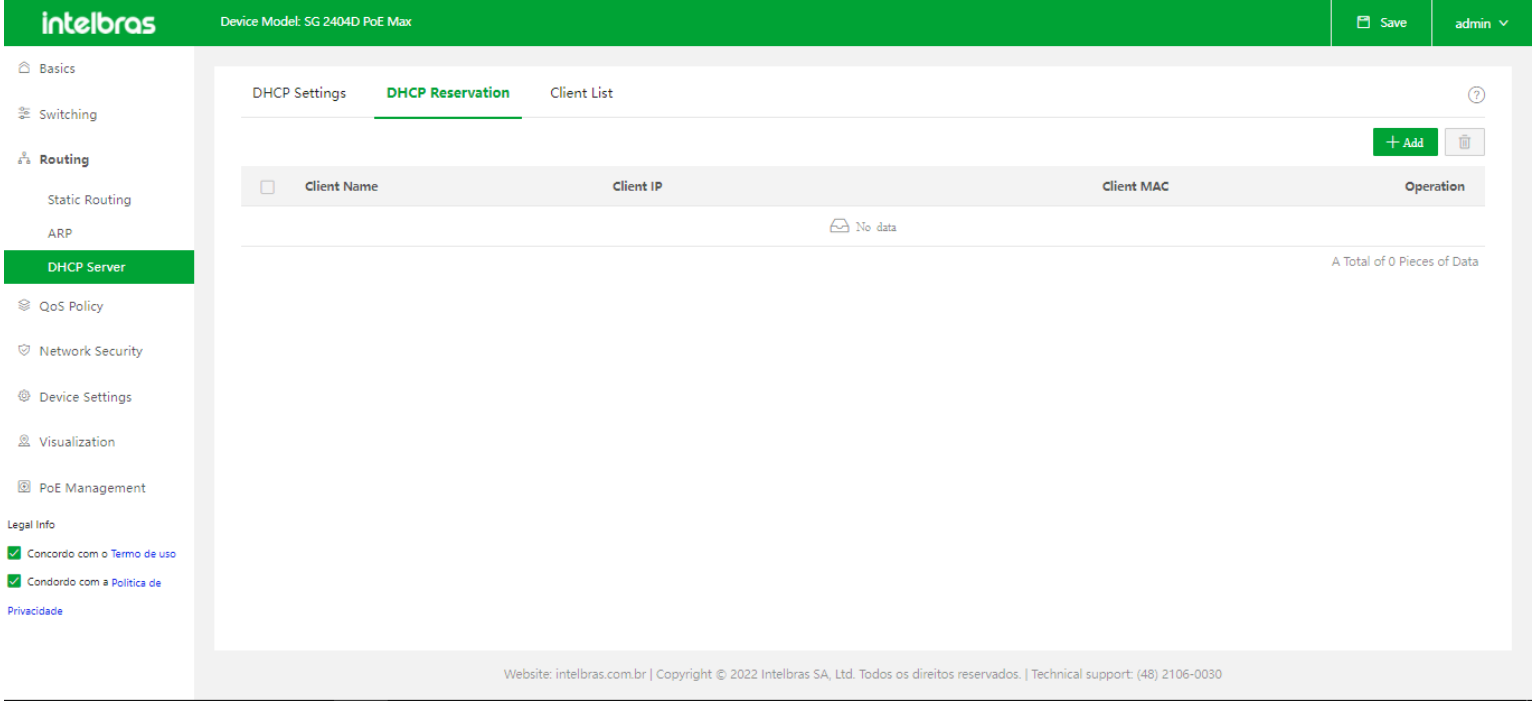
- **Name:** especifica o nome do servidor DHCP
- **IP Address Range:** especifica o intervalo de endereços IP que o servidor DHCP pode entregar aos Hosts.
- **Subnet Mask:** especifica a máscara de sub-rede que será entregue pelo servidor DHCP a um Host.
- **Default Gateway:** especifica o endereço de gateway que será entregue pelo servidor DHCP aos Hosts.
- **Lease Time:** especifica o período de validade de um endereço IP entregue pelo servidor DHCP a um host. Quando o lease time expira, se o host ainda estiver conectado ao switch, o lease time é estendido e o cliente continua ocupando o mesmo endereço IP. Se um host for desconectado do switch (desligamento ou remoção do cabo Ethernet), o switch liberará o endereço IP. Se outro cliente solicitar as informações de endereço IP posteriormente, o switch poderá atribuir esse endereço IP ao novo host.
- **DNS:** especifica os endereços do servidor DNS atribuído pelo servidor DHCP aos hosts.
- **Excluded IP Range:** ele especifica os endereços IP no pool de endereços que o servidor DHCP não irá atribuir.

DHCP Server for interface

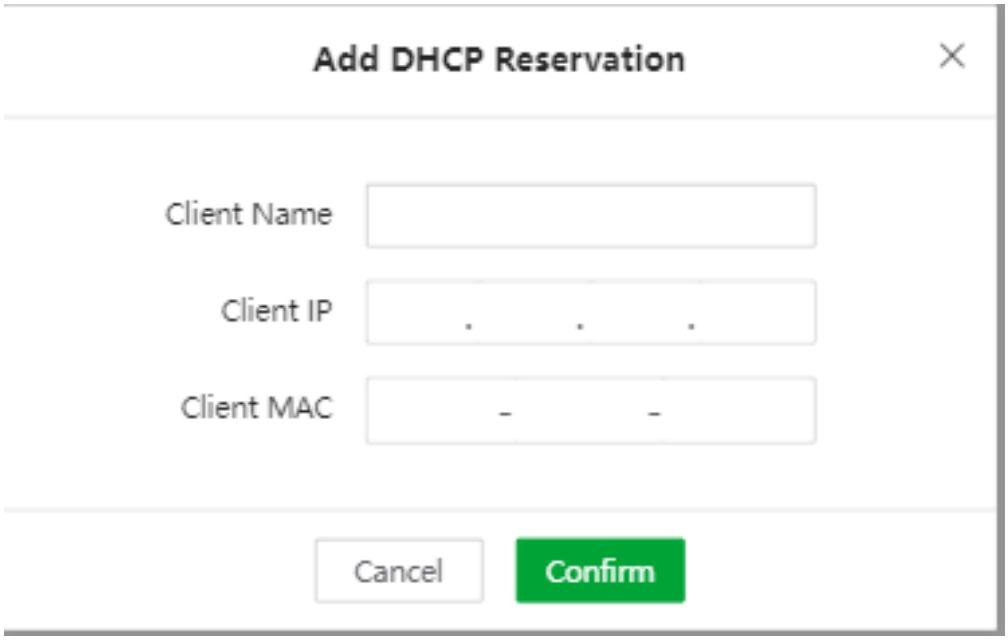
Com ele habilitado, o servidor DHCP de determinada interface VLAN entra em vigor. Para o pleno funcionamento o Range de DHCP e o IP da VLAN (Layer-3 interface) devem estar dentro do mesmo segmento de rede.

DHCP Reservation

Com esta função, o switch pode atribuir o endereço IP reservado a um cliente especificado, não correndo risco de outro dispositivo receber o mesmo endereço.



- **+ Add:** para adicionar uma nova reserva de IP, deve-se clicar no botão de +Add, será aberta a tela de Add DHCP Reservation.

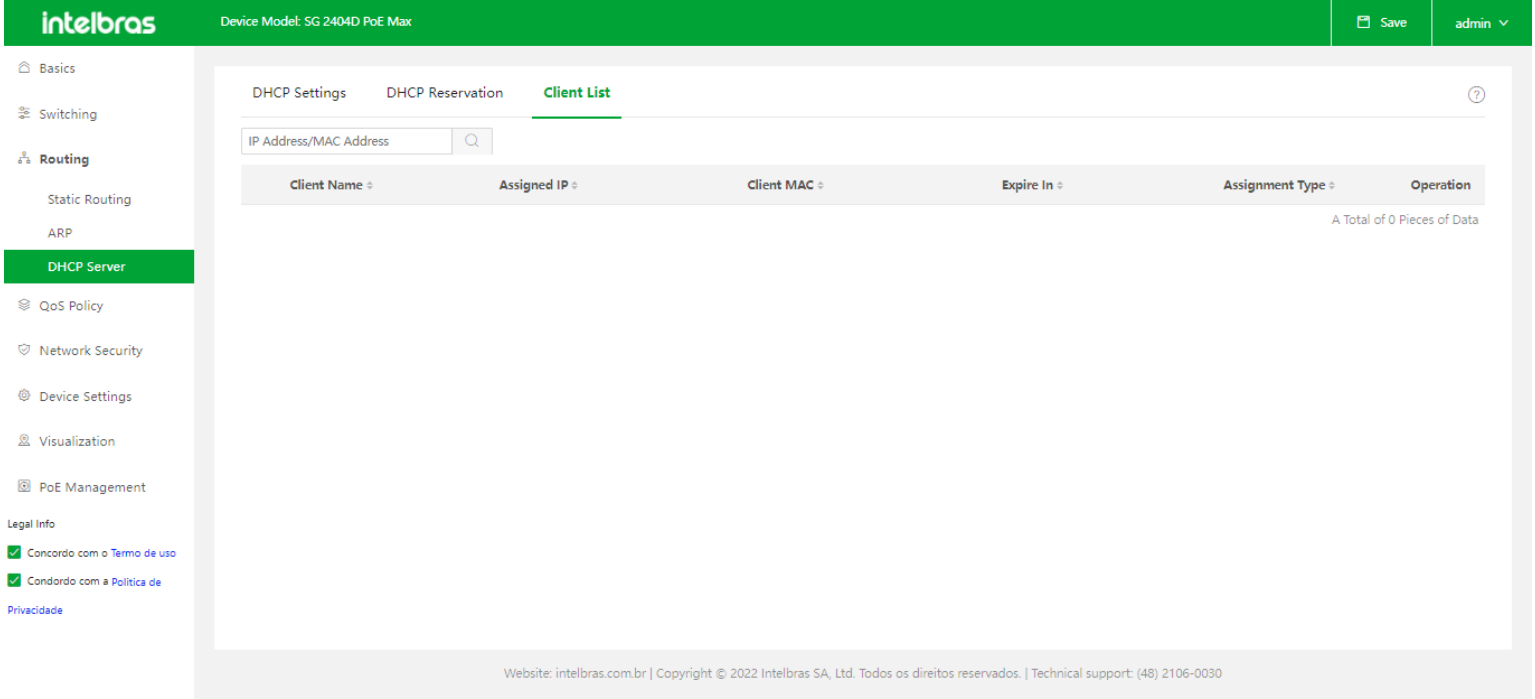


Para definir uma reserva deve-se configurar:

- **Client Name:** especifica o nome do cliente.
- **Client IP:** especifica o endereço IP reservado para o cliente.
- **Client MAC:** especifica o MAC do cliente que será atribuido ao IP.

Client List

Nesta tela são exibidas as informações dos clientes que obtêm endereço IP do servidor DHCP. Você também pode adicionar rapidamente regras de reserva DHCP aqui.

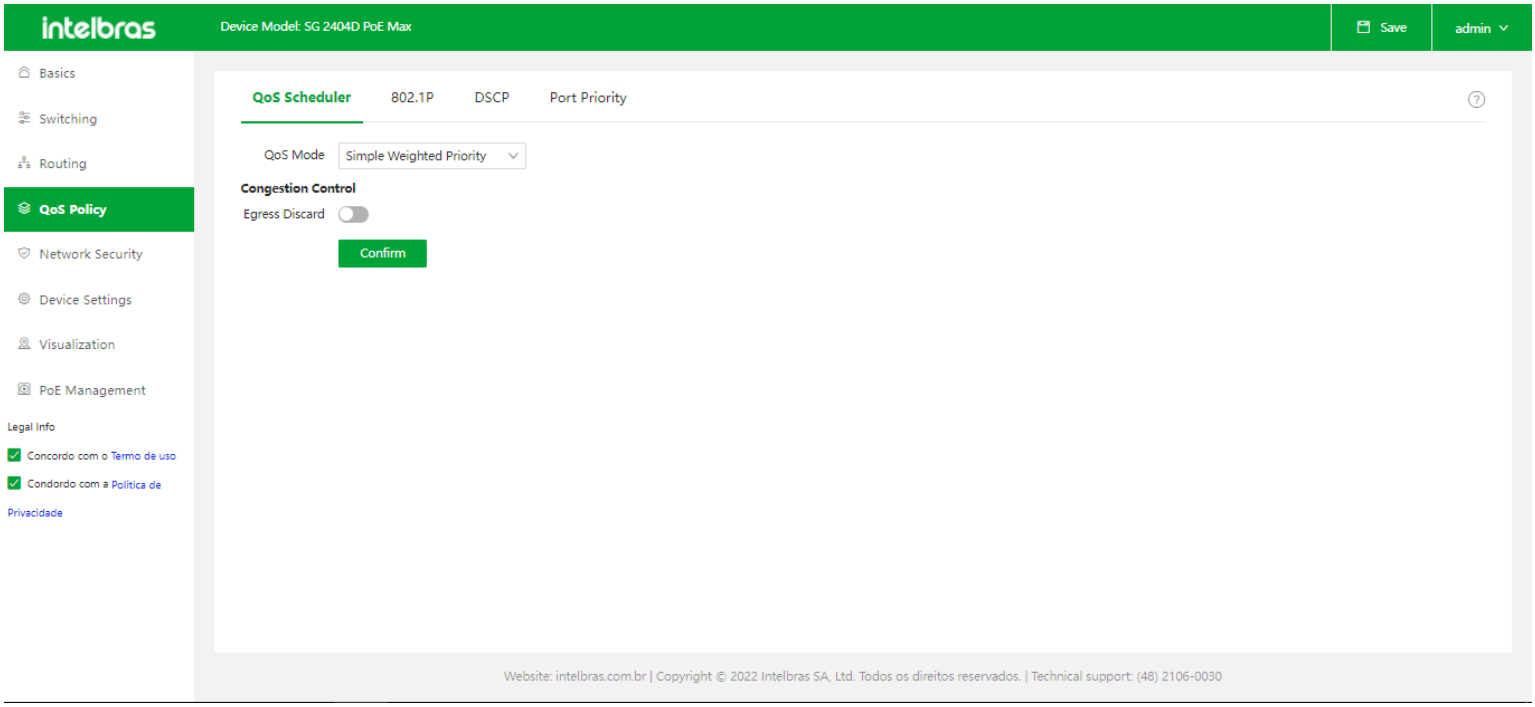


QoS POLICY

A função QoS (*Quality of Service*) é utilizada para fornecer qualidade de serviço a vários requisitos e aplicações utilizados na rede, otimizando e distribuindo a largura de banda. Este switch classifica e mapeia os pacotes entrantes e coloca-os em diferentes filas de prioridades, em seguida encaminha os pacotes de acordo com o algoritmo de fila selecionado, implementando a função de QoS

QoS Scheduler

Nesta tela há opção de configurar o modo de agendador do tráfego de porta do switch.



- **QoS Mode:** especifica o modo do planejador do tráfego da porta. Há 3 possíveis configurações de QoS Mode, são elas:

Strict Priority: o switch encaminha o tráfego da porta estritamente com base nas prioridades das mensagens. As mensagens de fila com prioridade mais baixa são encaminhadas somente quando a fila com prioridade mais alta está vazia.

Simple Weighted: 8 filas compartilham igualmente a largura de banda.

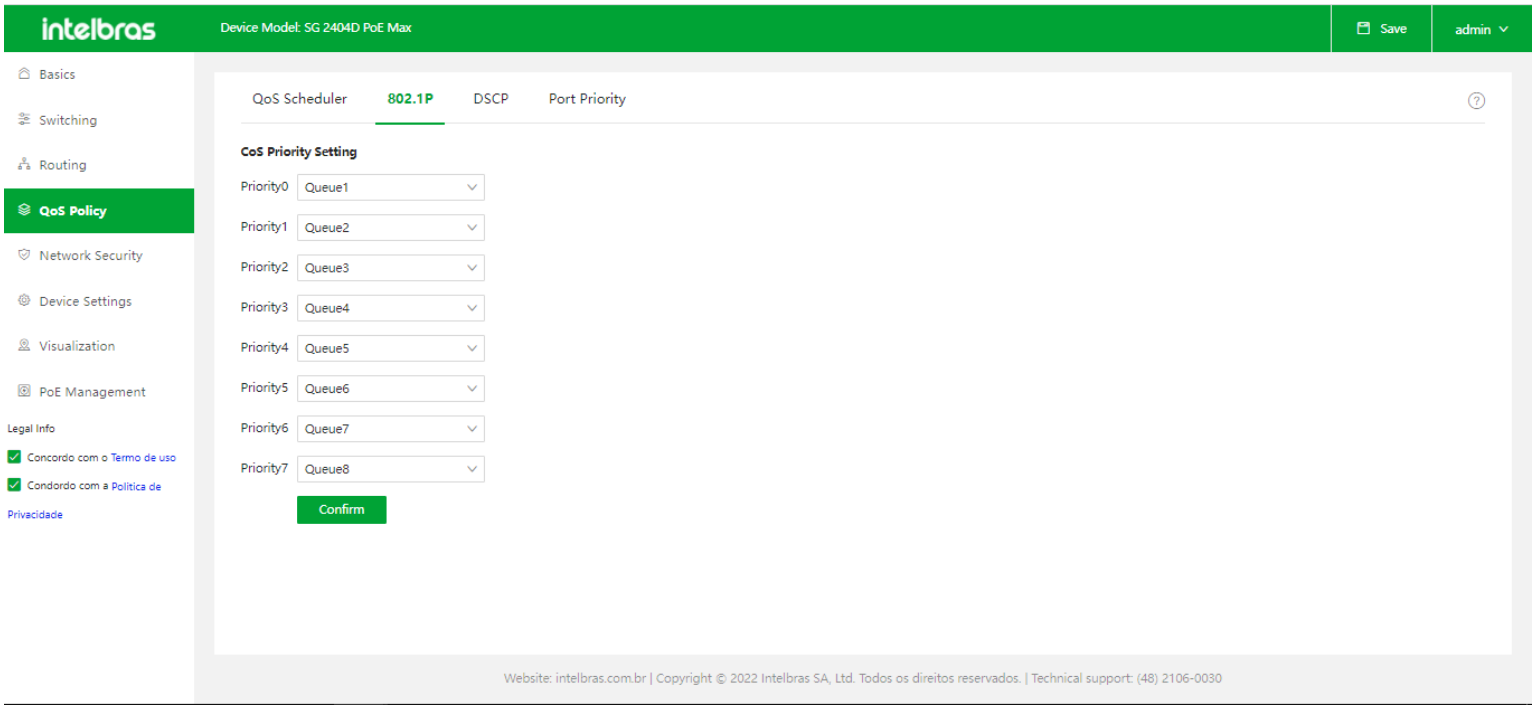
Weighted Priority: você precisa configurar um valor ponderado para cada fila. O valor ponderado indica o peso da obtenção de recursos. Se ocorrer congestionamento na porta, as larguras de banda são atribuídas com base no peso de cada fila.

- **Queue Settings:** se o Qos Mode estiver definido como Wighted Priority, você precisará configurar o valor ponderado para cada fila aqui.
- **Egress Discard:** as mensagens são descartadas na porta de saída quando ocorre congestionamento para reduzir o carregamento da porta de entrada. Vários cenários aplicáveis especiais: Existem portas de 100 Mbps e portas de 1000 Mbps quando os pacotes multicast são transmitidos.

OBS: esta função não é recomendada em cenários comuns.

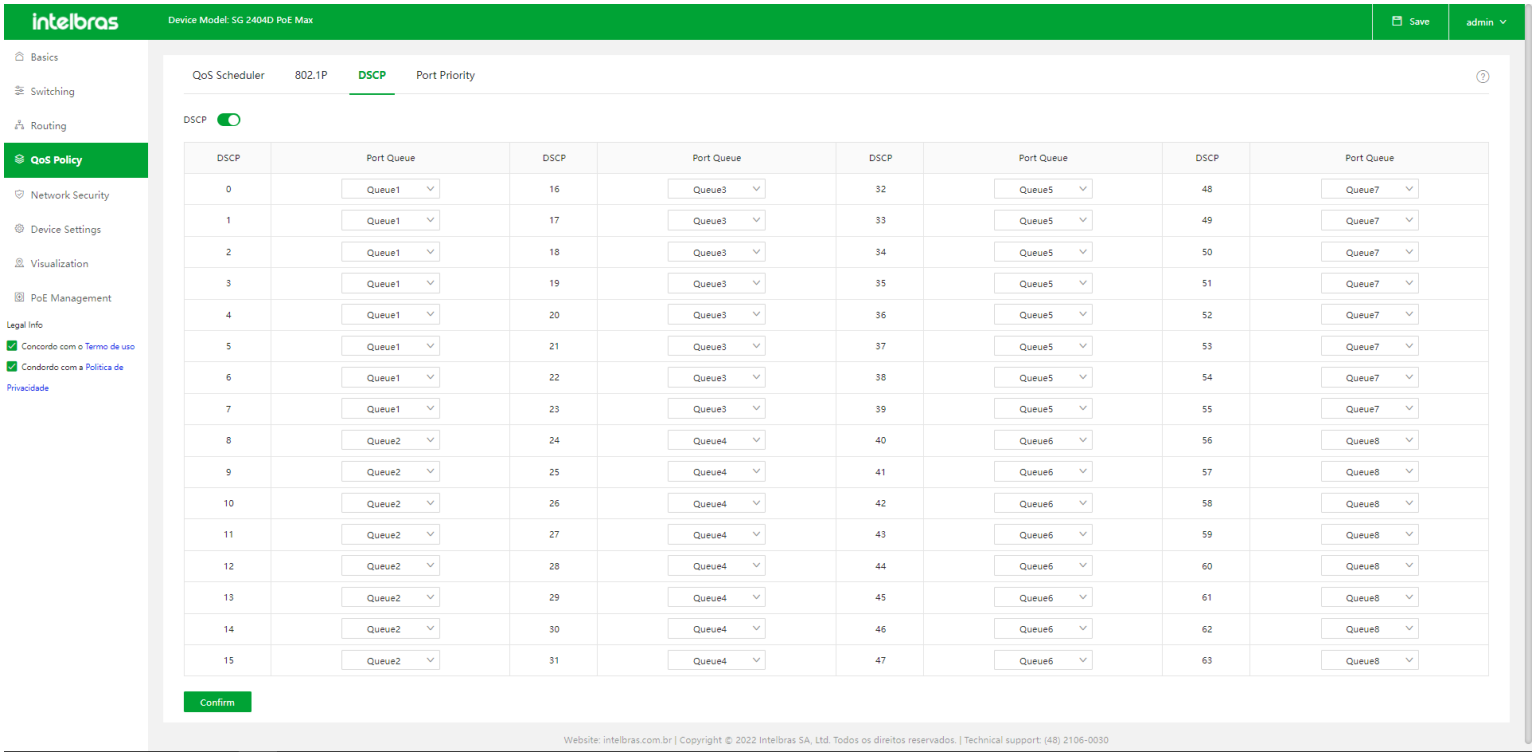
802.1P

É usado para configurar a fila interna correspondente de acordo com o valor de prioridade das mensagens VLAN. As filas 1 a 8 correspondem a 8 filas internas de portas de saída. Quando o switch transmite mensagens de VLAN, as mensagens retornam às filas com base em seus valores de prioridade.



DSCP

É usado para configurar as filas internas correspondentes de acordo com o valor DSCP das mensagens IP. Quando o switch encaminha mensagens IP, as mensagens se juntam novamente às filas com base em seus valores DSCP. Por padrão, as mensagens com valor DSCP de 0 a 7 reingressam na fila1. mensagens com valor DSCP de 8 a 15 reingressam na fila2 e assim por diante.

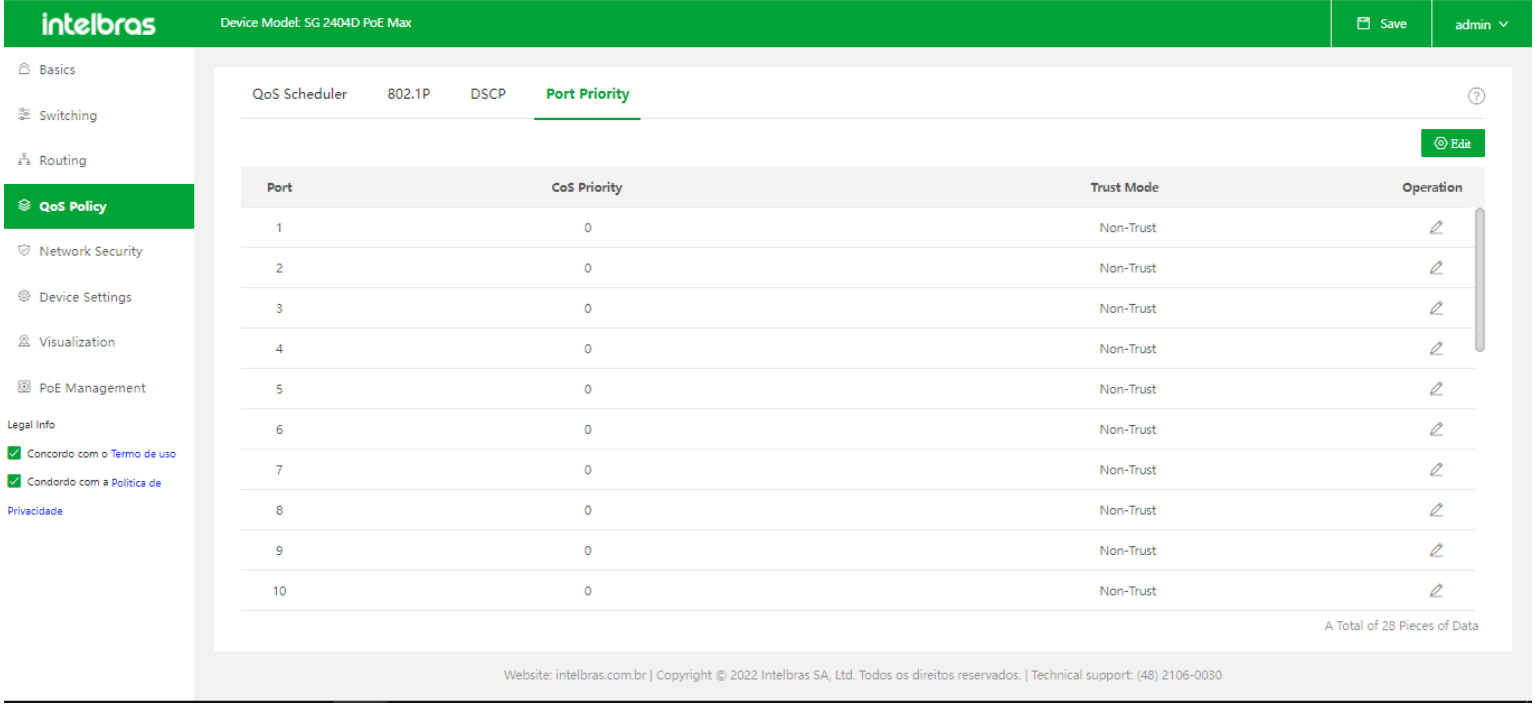


DSCP	Port Queue	DSCP	Port Queue	DSCP	Port Queue	DSCP	Port Queue
0	Queue1	16	Queue3	32	Queue5	48	Queue7
1	Queue1	17	Queue3	33	Queue5	49	Queue7
2	Queue1	18	Queue3	34	Queue5	50	Queue7
3	Queue1	19	Queue3	35	Queue5	51	Queue7
4	Queue1	20	Queue3	36	Queue5	52	Queue7
5	Queue1	21	Queue3	37	Queue5	53	Queue7
6	Queue1	22	Queue3	38	Queue5	54	Queue7
7	Queue1	23	Queue3	39	Queue5	55	Queue7
8	Queue2	24	Queue4	40	Queue6	56	Queue8
9	Queue2	25	Queue4	41	Queue6	57	Queue8
10	Queue2	26	Queue4	42	Queue6	58	Queue8
11	Queue2	27	Queue4	43	Queue6	59	Queue8
12	Queue2	28	Queue4	44	Queue6	60	Queue8
13	Queue2	29	Queue4	45	Queue6	61	Queue8
14	Queue2	30	Queue4	46	Queue6	62	Queue8
15	Queue2	31	Queue4	47	Queue6	63	Queue8

- **DSCP:** especifica o valor DSCP (intervalo: 0 a 63) dos cabeçalhos das mensagens IP.
- **Port Queue:** especifica a fila do planejador (fila 1 a 8) da porta de saída.

Port Priority

Ele é usado para configurar o modo de prioridade do aplicativo para as portas físicas do switch.



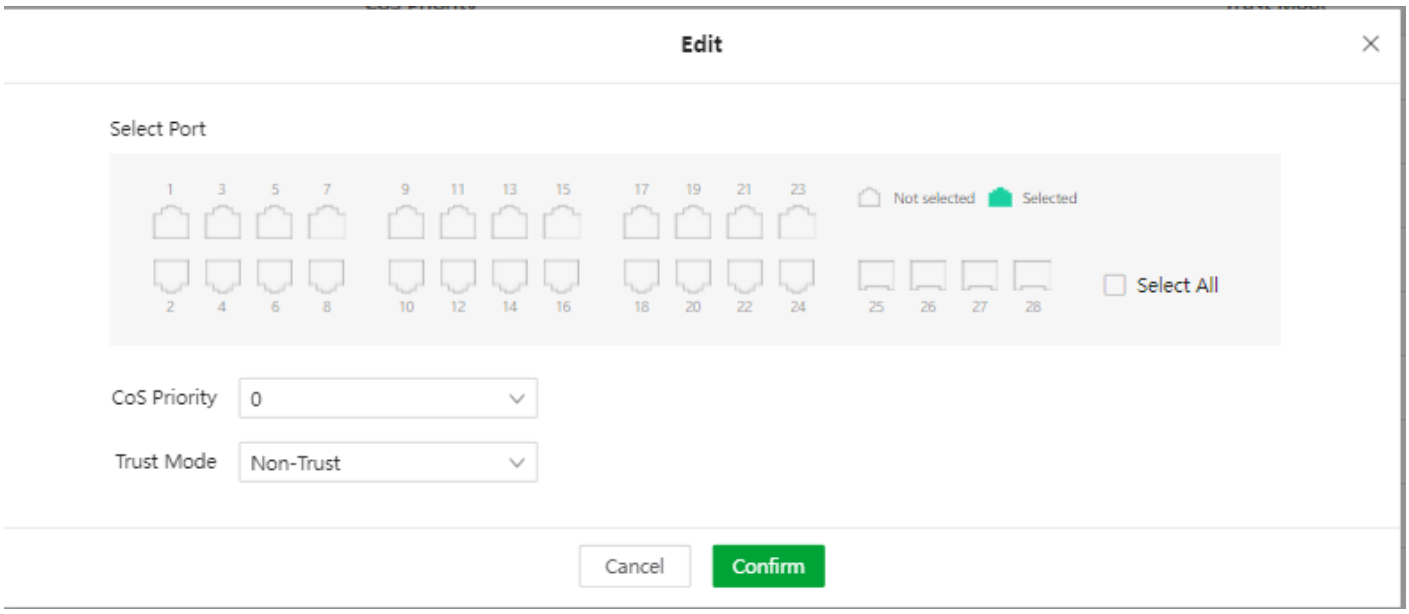
- **Port:** exibe o ID da porta. O Cos Priority especifica a correspondência entre as portas físicas do switch e as filas internas. Quando as mensagens recebidas pelo switch não cumprem as regras do trust mode, as mensagens voltam a se juntar às filas com base na correspondência.
- **Trust Mode:** especifica o método que a porta usa para processar as mensagens recebidas. Temos os modos:

  Non-Trust: todas as mensagens recebidas pela porta voltam a entrar nas filas de acordo com a correspondência do Cos Priority configurado.

  802.1P Trust: quando a porta recebe mensagens VLAN, as mensagens voltam a se juntar às filas de acordo com a relação de correspondência do 802.1P. Quando a porta recebe outras mensagens, as mensagens reingressam nas filas de acordo com a relação de correspondência do Cos Priority.

  DSCP Trust: quando a porta recebe mensagens IP, as mensagens voltam às filas de acordo com a relação de correspondência do DSCP. Quando a porta recebe outras mensagens, as mensagens reingressam nas filas de acordo com a relação de correspondência do Cos Priority.

- **Edit:** clicando no botão Edit é aberta a tela de Edit, onde podemos configurar o CoS Priority e o Trust Mode de uma ou mais portas



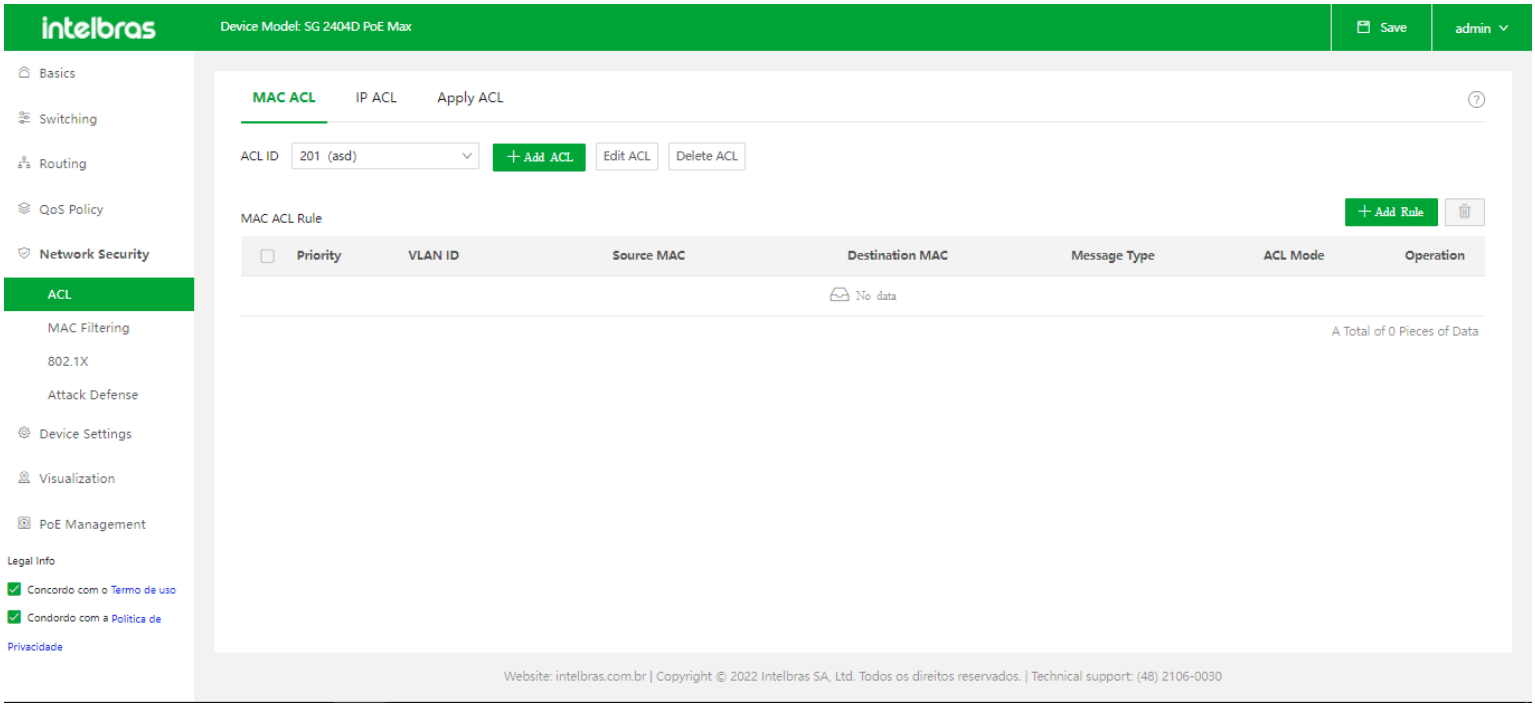
NETWORK SECURITY

No menu de Network Security temos disponíveis funções que irão auxiliar na segurança do seu produto e da sua rede.

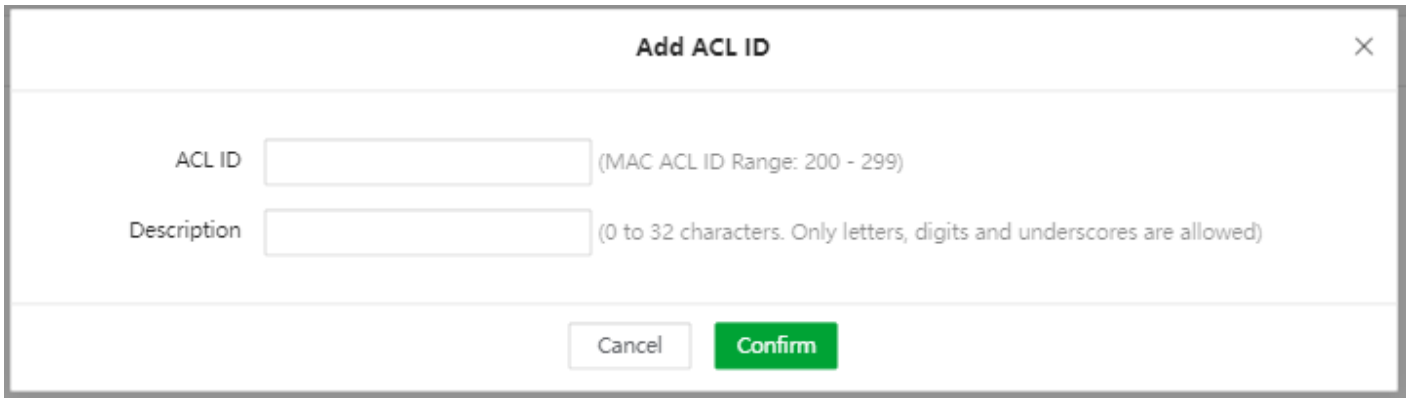
ACL

MAC ACL

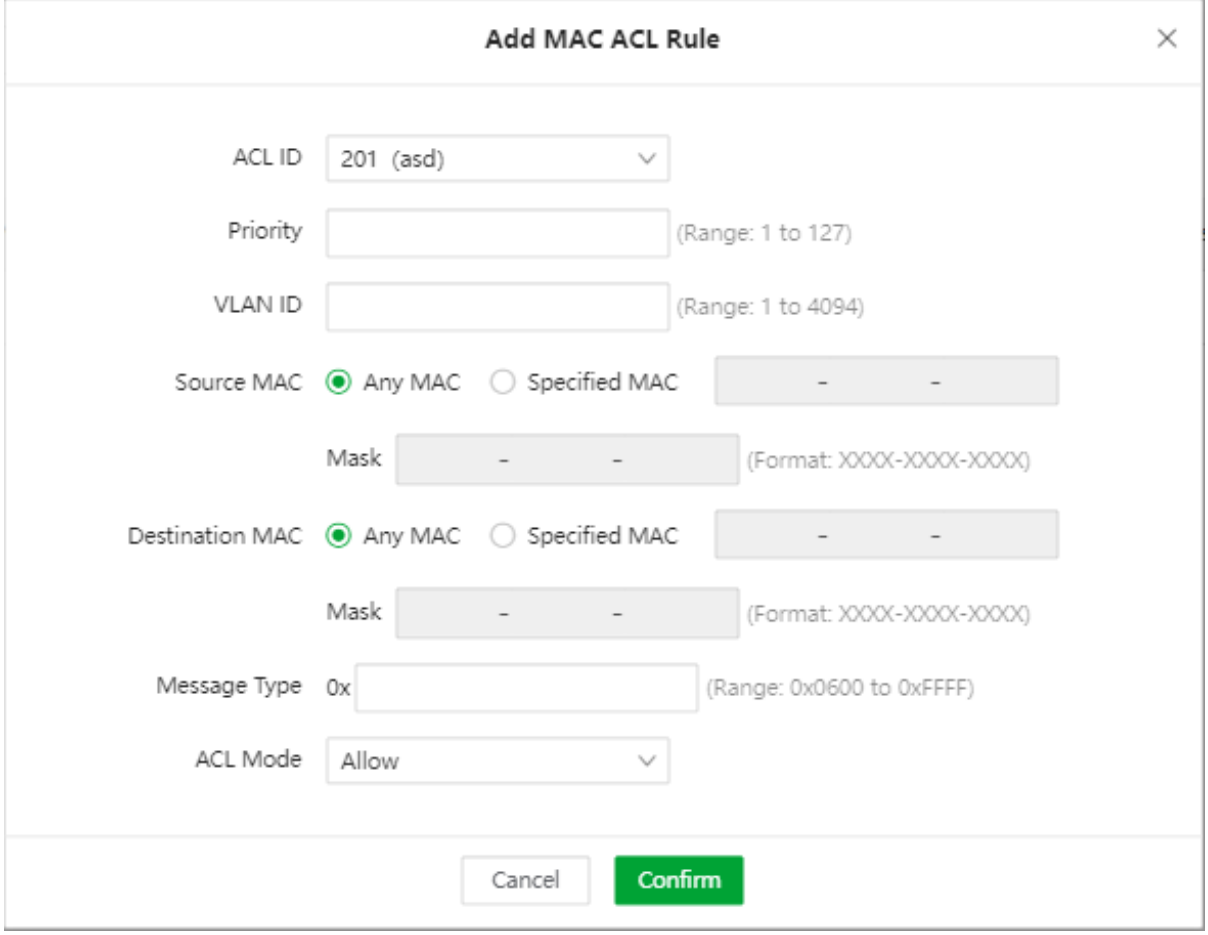
As regras da MAC ACL são usadas para filtrar mensagens com base no conteúdo do cabeçalho do quadro da camada 2.



- **ACL ID:** Neste campo podemos selecionar o ACL ID que desejamos editar ou visualisar. Cada ACL ID será um conjunto de regras MAC ACL, podem ser criadas até 99 ACL ID. Para adicionar uma nova ACL basta clicar no botão de +Add ACL. Para editar a ACL ID em questão pode-se utilizar o botão Edit ACL e para excluir/deletar temos o botão Delete ACL.



- **+ Add Rule:** Clicando neste botão é aberta a tela de ADD MAC ACL Rule. Nesta tela podemos configurar uma nova regra de MAC ACL.



- **Priority:** este campo é usado para configurar a prioridade de uma regra. Um valor menor indica uma prioridade mais alta. A mensagem começa a ser verificada começando a partir da regra com a prioridade mais alta. Uma vez que a mensagem se enquadra em uma regra, a mensagem para de verificar as regras. A prioridade das regras não é exigida por padrão, nas se forem adicionadas 127 regras, a prioridade será necessária.
- **VLAN ID:** especifica o ID de VLAN ao qual se aplicará a regra de ACL.
- **Source MAC:** especifica o endereço MAC de origem no quadro da camada 2 de uma mensagem. Temos duas opções de configuração:

  Any MAC: especifica todos os endereços MAC.

  Specified MAC: combinado com a máscara de rede, é usado para especificar um determinado endereço MAC ou segmento de endereço MAC.

- **Destination MAC:** especifica o endereço MAC de destino no quadro da camada 2 de uma mensagem. Temos duas opções de configuração:

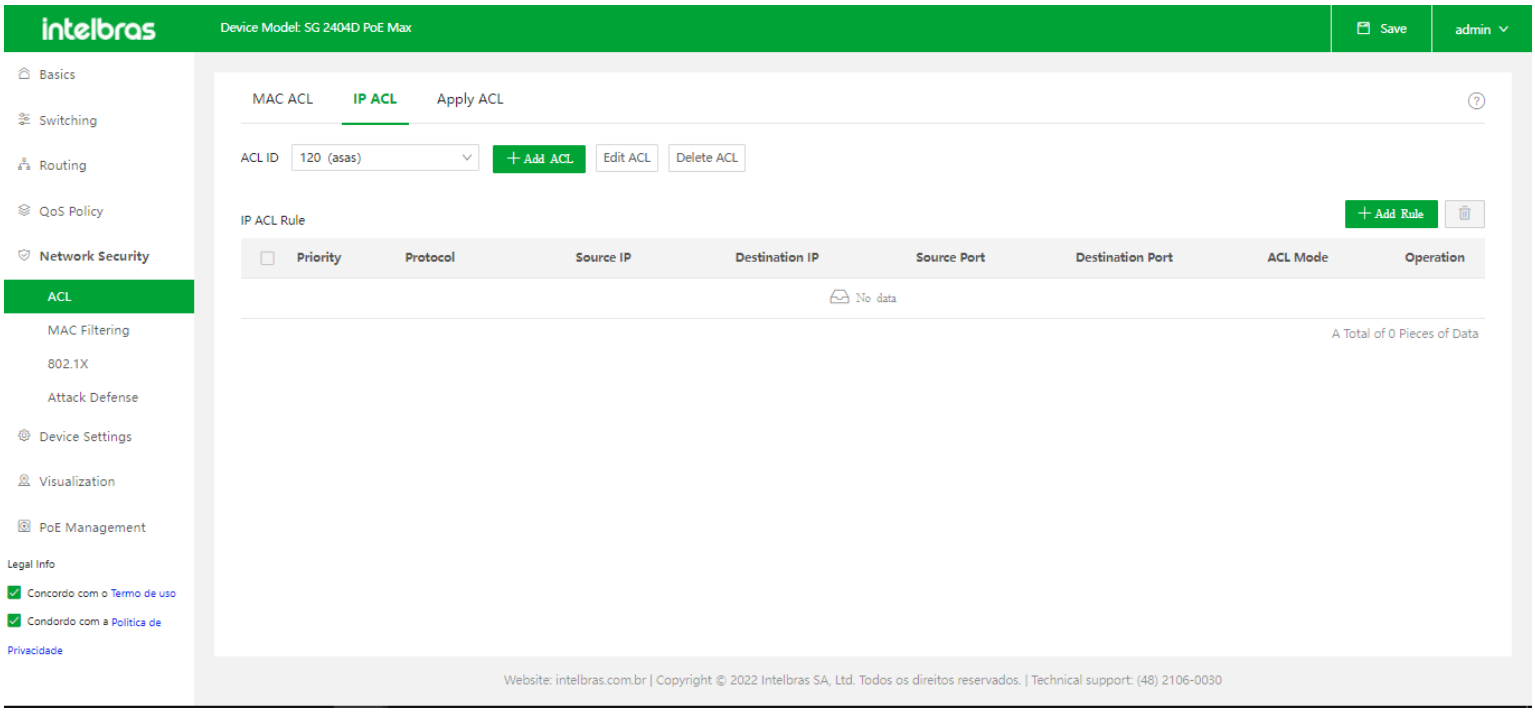
  Any MAC: especifica todos os endereços MAC.

  Specified MAC: combinado com a máscara de rede, é usado para especificar um determinado endereço MAC ou segmento de endereço MAC.

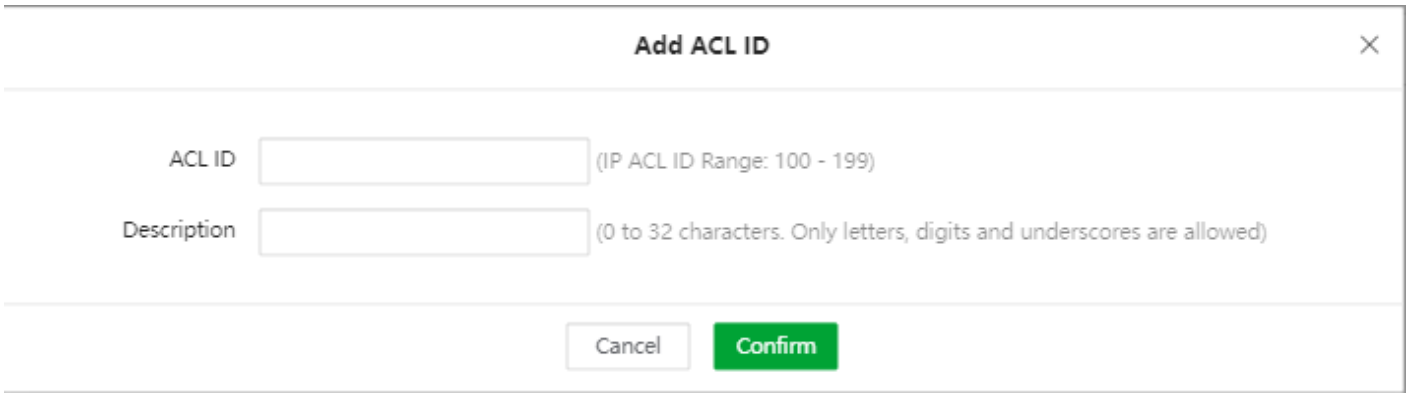
- **Message Type:** especifica o campo do tipo de mensagem no quadro da camada 2 de uma mensagem, que está no formato hexadecimal. Por exemplo, 0x0806 representa os pacotes ARP.
- **ACL Mode:** ele especifica o modo ACL no qual o switch processa as mensagens que correspondem à regra, podendo ser Allow(Permitir, ou seja, encaminhar) ou Block (Bloquear, ou seja, descartar).

IP ACL

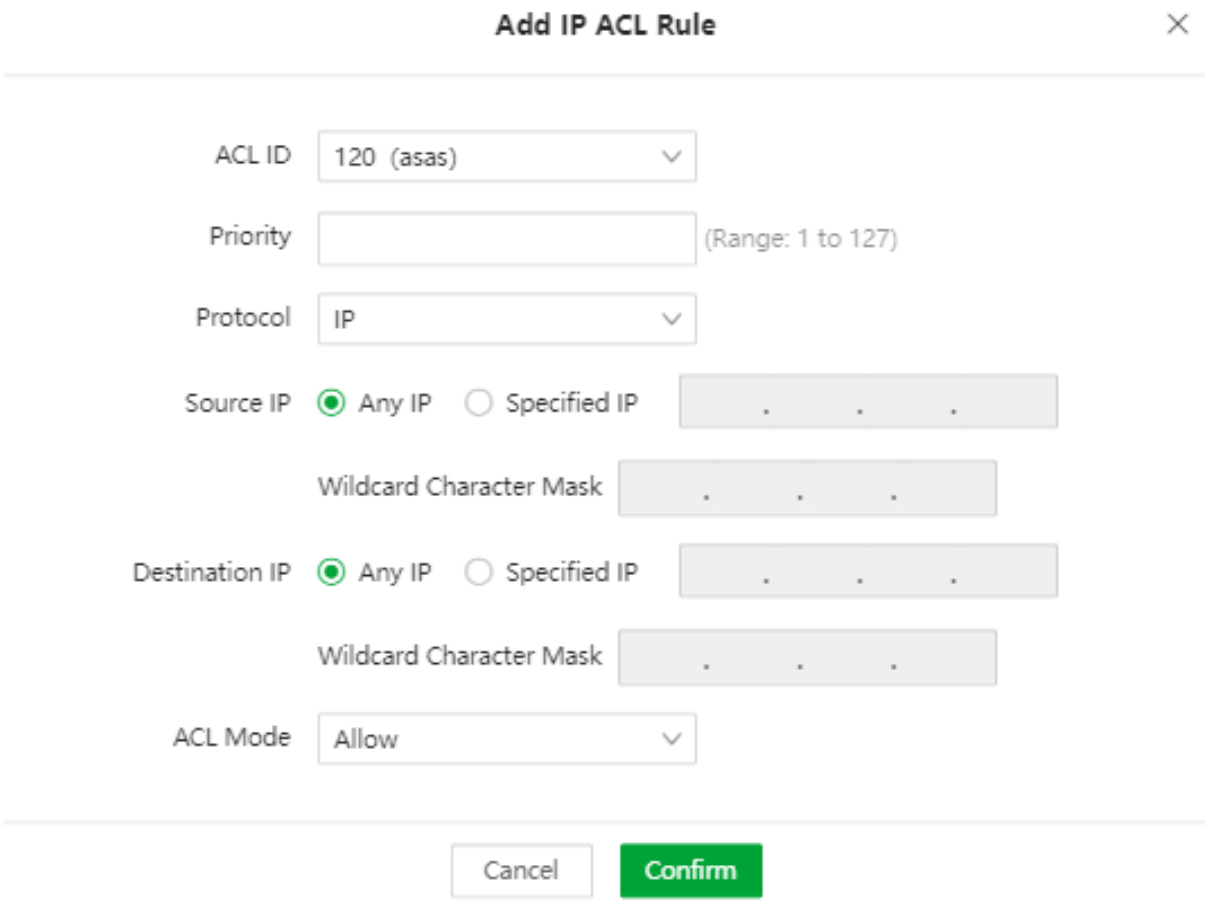
O IP ACL é usado para filtrar mensagens com base no conteúdo do cabeçalho do pacote IP e no número da porta TCP/UDP.



- **ACL ID:** neste campo podemos selecionar o ACL ID que desejamos editar ou visualisar. Cada ACL ID será um conjunto de regras IP ACL, podem ser criadas até 99 ACL ID. Para adicionar uma nova ACL basta clicar no botão de +Add ACL. Para editar a ACL ID em questão pode-se utilizar o botão Edit ACL e para excluir/deletar temos o botão Delete ACL.



- **+ Add Rule:** clicando neste botão é aberta a tela de ADD IP ACL Rule. Nesta tela podemos configurar uma nova regra de IP ACL.



- **Priority:** este campo é usado para configurar a prioridade de uma regra. Um valor menor indica uma prioridade mais alta. A mensagem começa a ser verificada começando a partir da regra com a prioridade mais alta. Uma vez que a mensagem se enquadra em uma regra, a mensagem para de verificar as regras. A prioridade das regras não é exigida por padrão, nas se forem adicionadas 127 regras, a prioridade será necessária.
- **VLAN ID:** especifica o ID de VLAN ao qual se aplicará a regra de ACL.
- **Protocol:** ele especifica o campo do tipo de protocolo do cabeçalho do pacote IP da camada 3 de uma mensagem, como IP, ICMP e assim por diante. Você também pode inserir o número do protocolo.
- **Source IP:** especifica o endereço IP de origem no cabeçalho do pacote IP de camada 3 de uma mensagem. Temos duas opções de configuração:

Any IP: especifica todos os endereços IP.

Specified IP: combinado com a máscara de rede, é usado para especificar um determinado endereço IP ou segmento de endereço MAC.

- **Destination IP:** especifica o endereço IP de destino no cabeçalho do pacote IP de camada 3 de uma mensagem. Temos duas opções de configuração:

Any IP: especifica todos os endereços MAC.

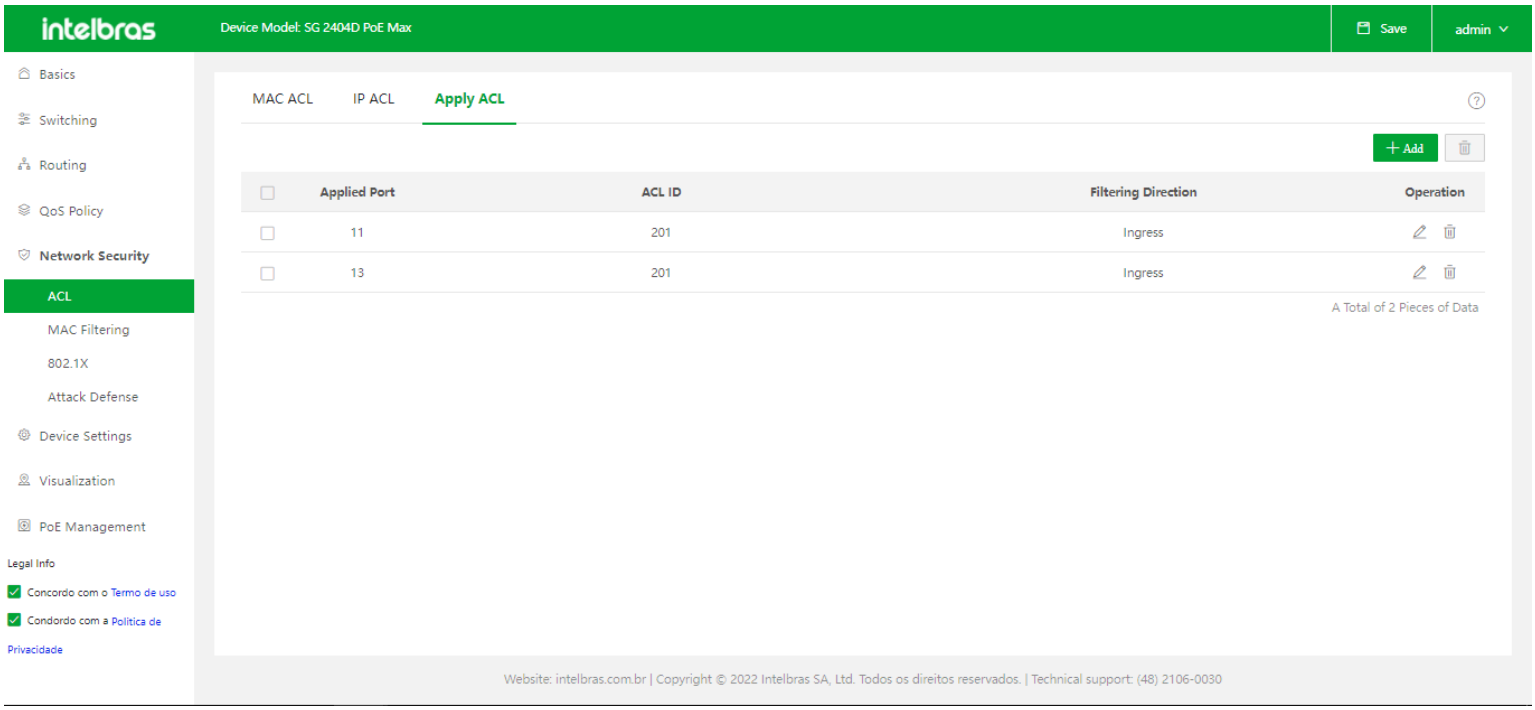
Specified IP: combinado com a máscara de rede, é usado para especificar um determinado endereço IP .

OBS: se no campo Protocol forem escolhidos os valores TCP ou UDP, teremos a opção de configurar a porta de origem e destino.

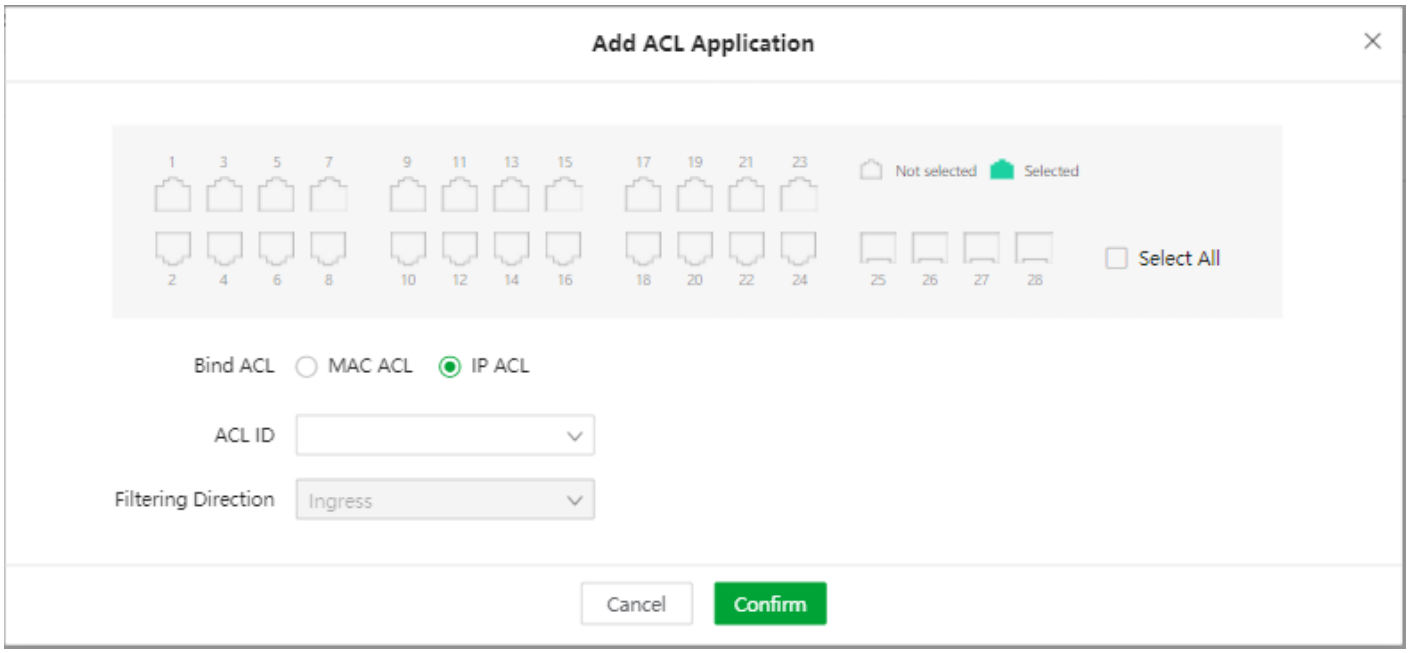
- **ACL Mode:** Ele especifica o modo ACL no qual o switch processa as mensagens que correspondem à regra, podendo ser Allow(Permitir, ou seja, encaminhar) ou Block (Bloquear, ou seja, descartar).

Apply ACL

Esta página é usada para aplicar as regras ACL às portas físicas.

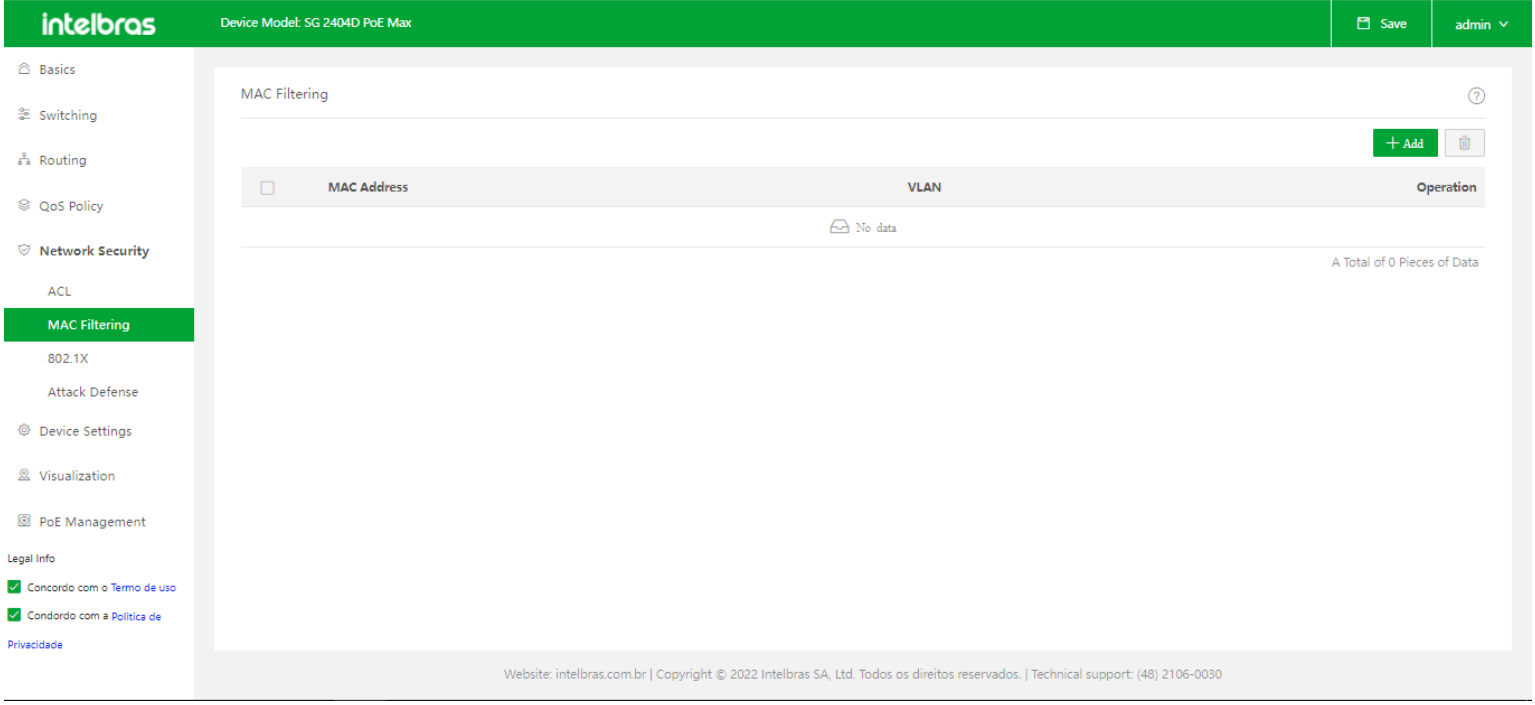


- **Applied Port:** especifica o número da porta fisica do Switch à qual a regra ACL se aplica.
- **ACL ID:** especifica a ACL ID que se aplica à porta física do Switch.
- **Filtering Direction** especifica a direção em que o filtro de mensagens se aplica na porta. Somente a entrada é compatível.
- **+ Add:** ao clicar no botão de + Add temos a tela de Add ACL Application. Nesta pela pode-se atrelar as regras de ACL as portas físicas.

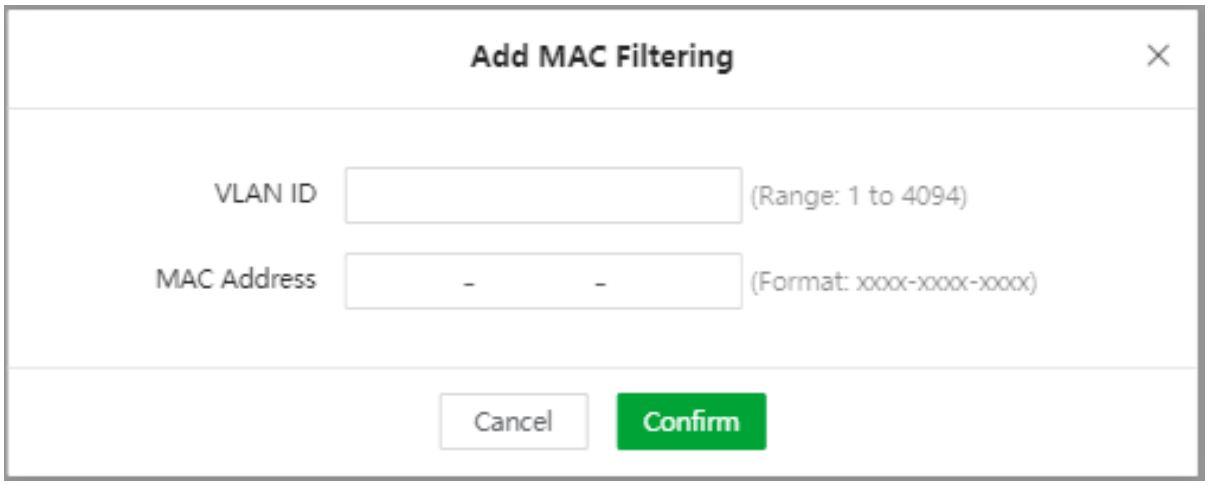


Mac Filtering

Esta função é usada para filtrar pacotes com endereços MAC especificados. Com a função habilitada, o switch verificará o endereço MAC de origem e o endereço MAC de destino dos pacotes recebidos. Se o endereço MAC de origem ou o endereço MAC de destino de um pacote existir na lista de filtragem MAC, o pacote será descartado.



- **MAC Address:** Especifica o endereço MAC a ser filtrado. Quando o endereço MAC de origem ou o endereço MAC de destino de um pacote for o mesmo que este endereço MAC, o pacote será descartado.
- **VLAN:** Especifica a VLAN na qual a regra de filtragem MAC entrará em vigor.
- **+ Add:** Ao clicar neste botão temos a tela de ADD Mac Filtering, onde pode-se criar novas regras de filtro de MAC.



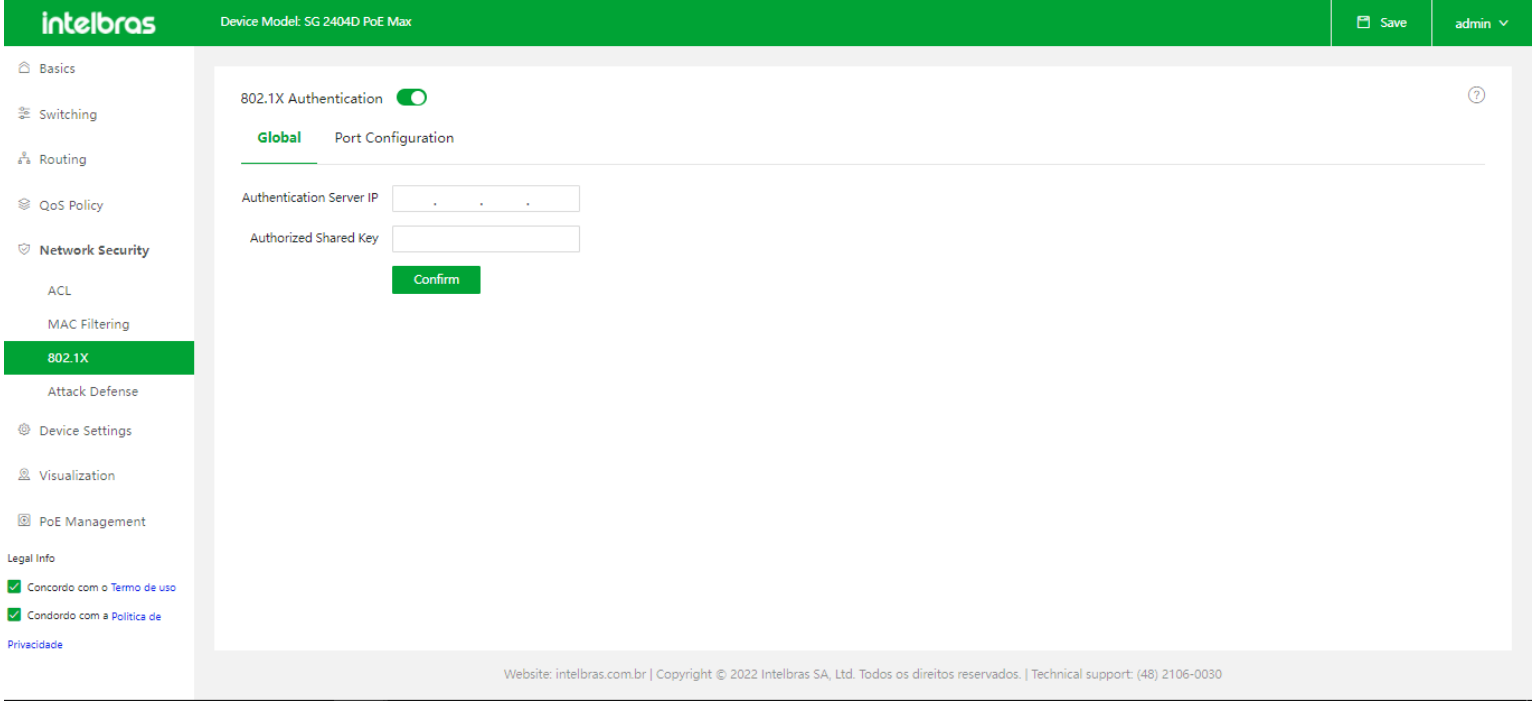
802.1X

802.1X é uma tecnologia de controle de acesso à rede criada pelo IEEE. É usado para autenticar e controlar usuários de LAN.

Se o dispositivo do usuário conectado ao switch puder passar pela autenticação, o switch encaminhará os pacotes de dados do usuário. Caso contrário, o switch não encaminha os pacotes de dados do usuário.

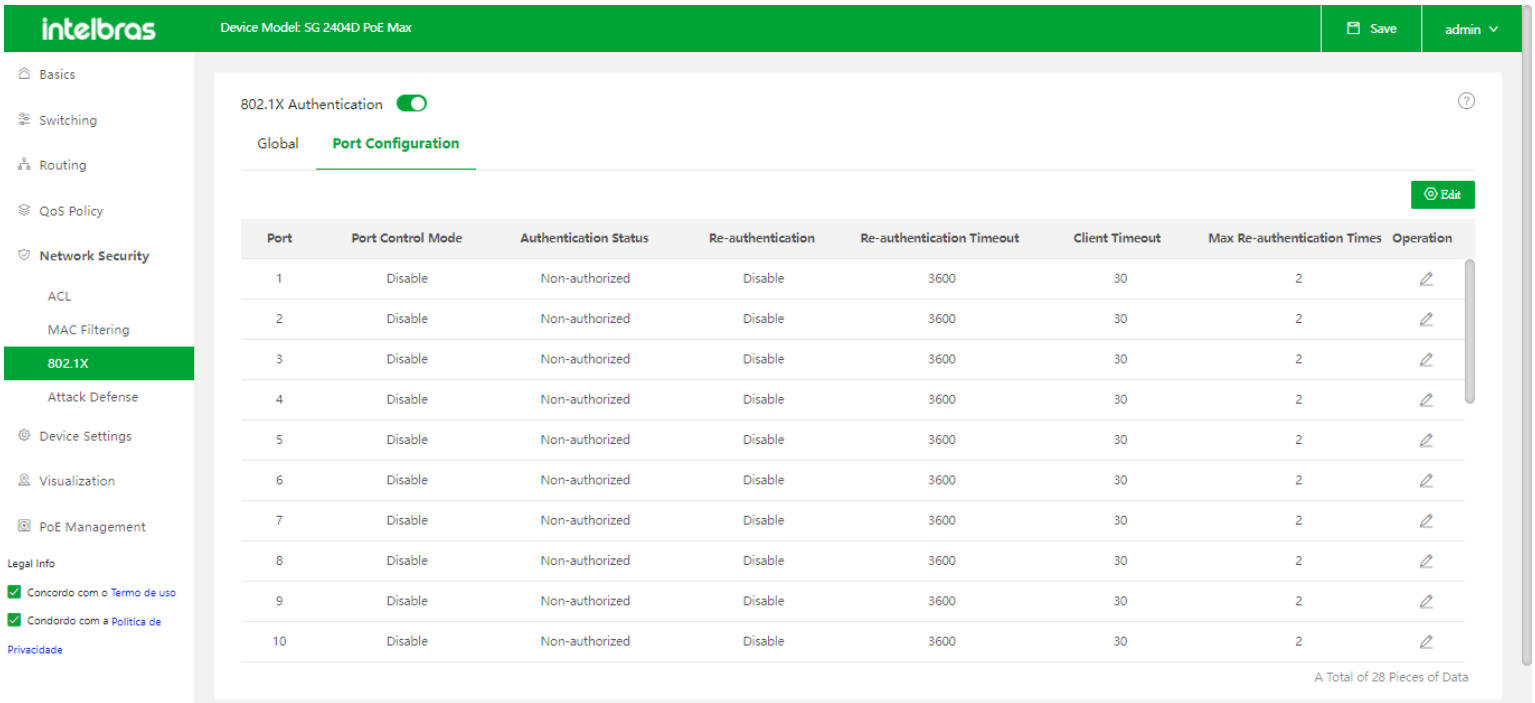
OBS: o switch não pode servir como servidor de autenticação, portanto, ele precisa se conectar ao servidor de autenticação na rede.

Global



- **Authentication Server IP:** especifica o endereço IP do servidor de autenticação Radius, que deve estar no mesmo segmento de rede com o endereço IP de gerenciamento do switch.
- **Authorized Shared Key:** especifica a chave compartilhada de uma mensagem de autenticação/autorização Radius. Deve ser igual à chave definida no servidor de autenticação/autorização Radius interconectado.

Port Configuration



- **Port Control Mode:** especifica o tipo de autenticação 802.1X da porta fisica. Temos 4 possibilidades de configuração, são elas:

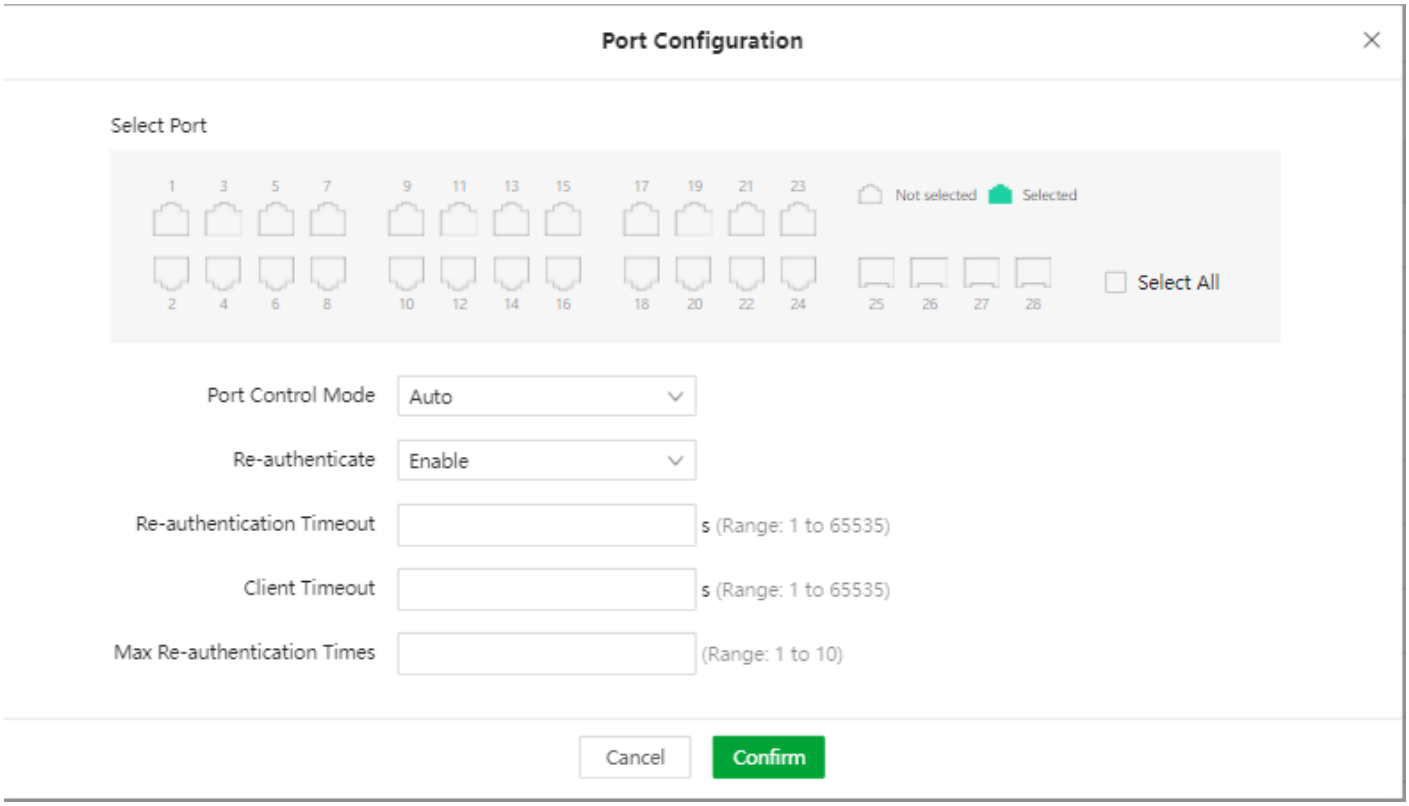
  Auto: a autenticação está habilitada na porta. Se um usuário passar na autenticação, ele terá permissão para acessar os recursos da rede. Caso contrário, o usuário não poderá acessar os recursos da rede.

  Mandatory Authorization: a porta está sempre no estado de autorização. Ele permite que os usuários acessem os recursos da rede sem autenticação e autorização.

Mandatory Non-authorization: a porta está sempre no estado de não-autorização. Ele proíbe os usuários de acessar os recursos da rede sem autenticação e autorização.

Disable: a autenticação está desabilitada na porta. Ele permite que os usuários acessem os recursos da rede.

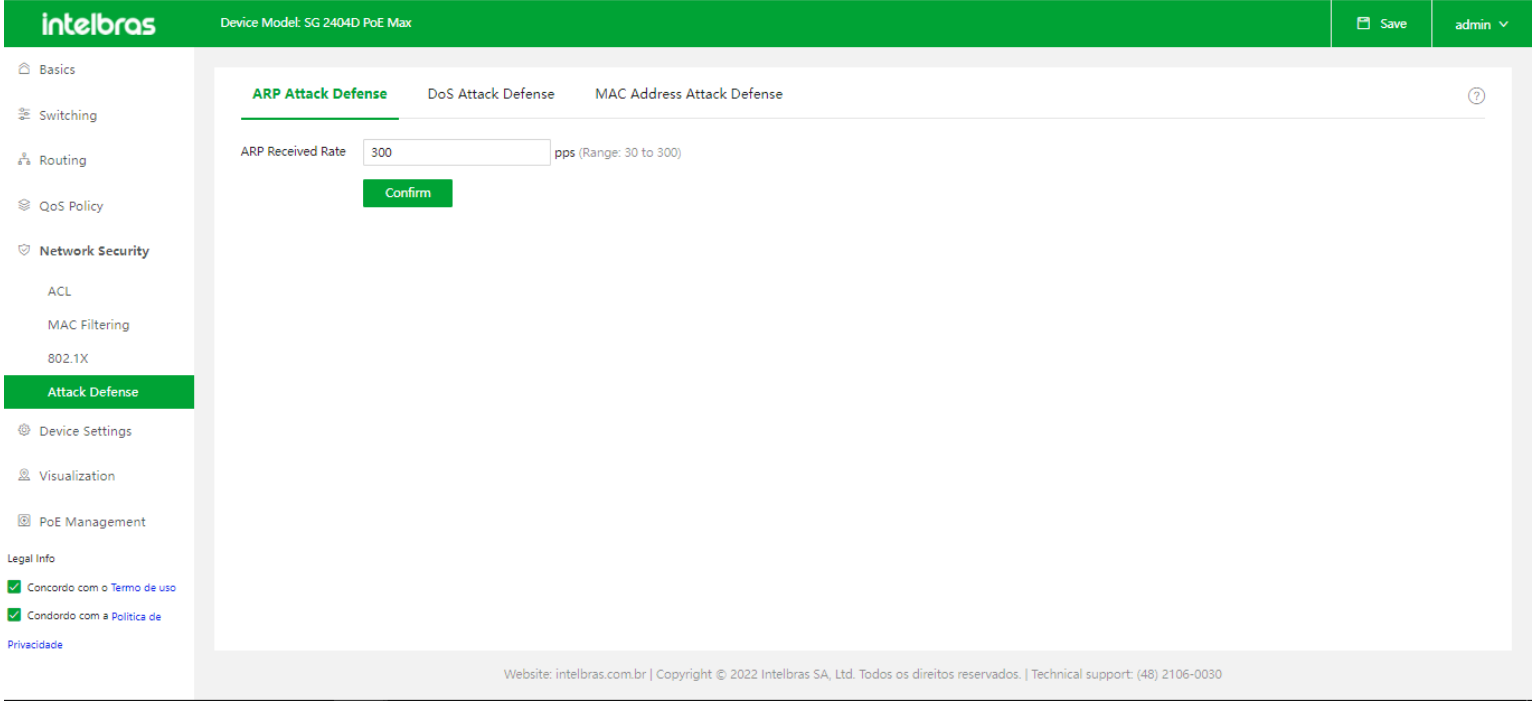
- **Authentication Status:** especifica o status de autenticação da porta.
- **Re-Authentication:** com a função habilitada, o switch requer periodicamente que os usuários se reautentiquem, para evitar que os usuários autenticados sejam mascarados.
- **Re-Authentication Timeout:** especifica o intervalo no qual o switch inicia a reautenticação para os clientes. Se a reautenticação estiver habilitada em uma porta, o switch lança solicitações de reautenticação para os dispositivos online conectados à porta nesse intervalo.
- **Client Timeout:** especifica o período de tempo em que o cliente deve responde à solicitação de reautenticação. Se o switch enviar uma mensagem de solicitação de reautenticação para um cliente e não receber nenhuma resposta nesse período de tempo, ele enviará a mensagem novamente.
- **Max Re-Authentication Times:** especifica o tempo máximo para um cliente se autenticar novamente. O switch força o cliente offline se o tempo de autenticação do cliente exceder esse valor.
- **Edit:** ao clicar neste botão temos a tela de Port Configuration. Pode-se alterar as configurações de 802.1X das portas físicas do Switch.



Attack Defense

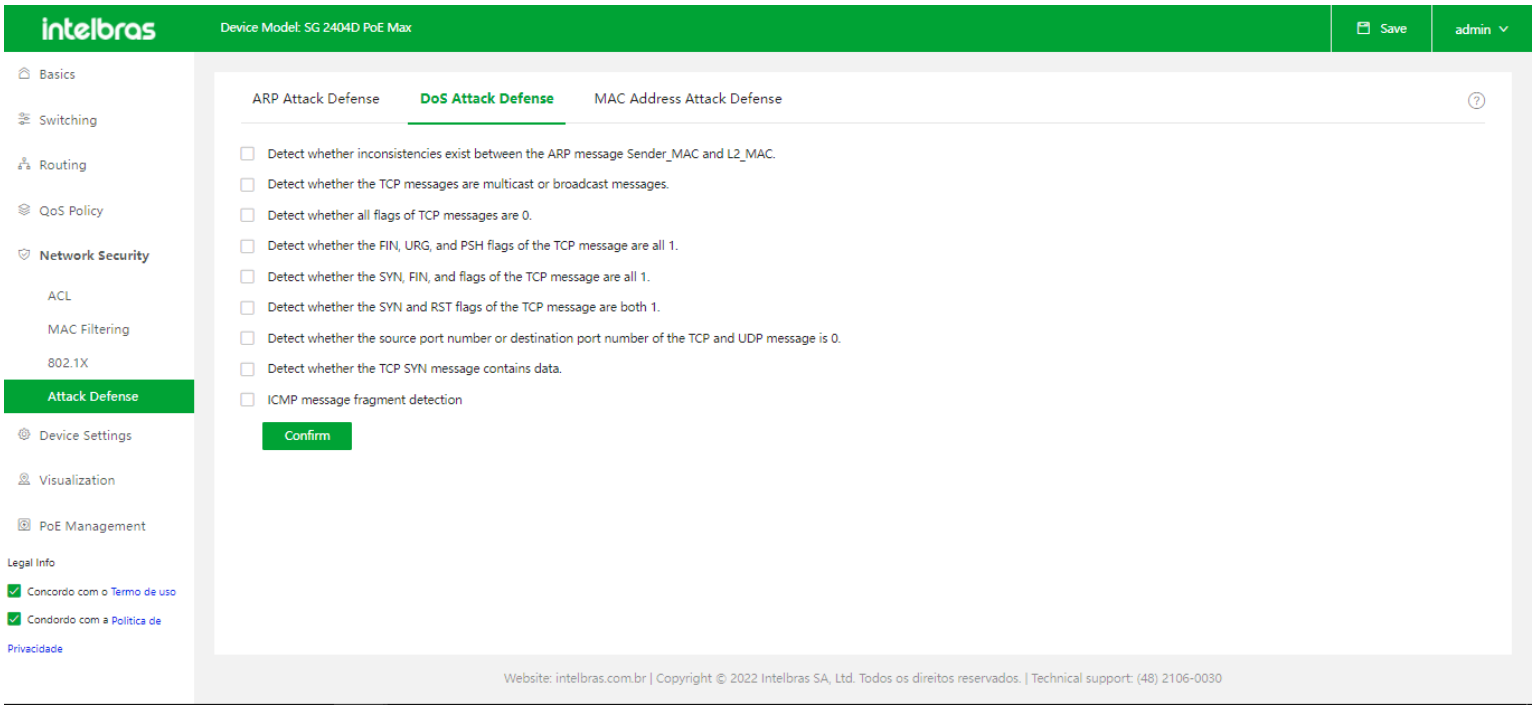
Neste menu temos algumas funções que previnem alguns tipos de ataque, como ARP Attack, DoS Attack e Mac Address Attack.

ARP Attack Defense



- **ARP Received Rate:** especifica a taxa na qual o switch recebe as mensagens ARP. Dentro de 1 segundo, se as mensagens ARP recebidas pelo switch excederem esse valor limite, o switch estará sendo atacado por protocolo ARP.

DoS Attack Defense



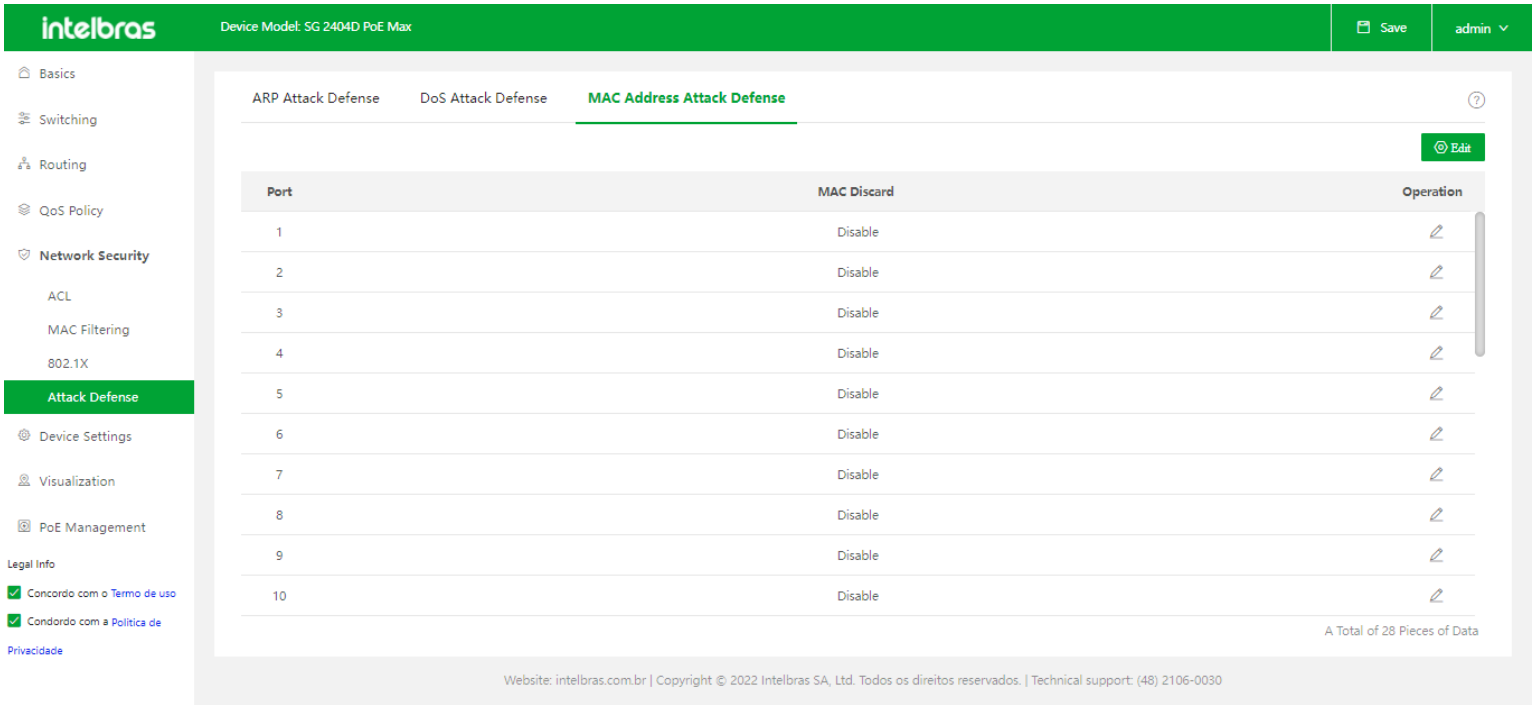
A função DoS Attack Defense é usada para evitar que alguns hosts consumam recursos do servidor de forma maliciosa, enviando um grande número de solicitações de serviço e deixando outros hosts incapazes de usar os serviços de rede corretamente (DoS- Denial of Service).

- **Detect whether inconsistencies exist between the ARP message Sender_MAC and L2_MAC:** proibi o encaminhamento das mensagens ARP cujo Sender_MAC (Mac de origem) e L2_MAC sejam inconsistentes.
- **Detect whether the TCP messages are multicast or broadcast messages:** proibir o encaminhamento das mensagens TCP cujos endereços de destino são endereços multicast ou broadcast

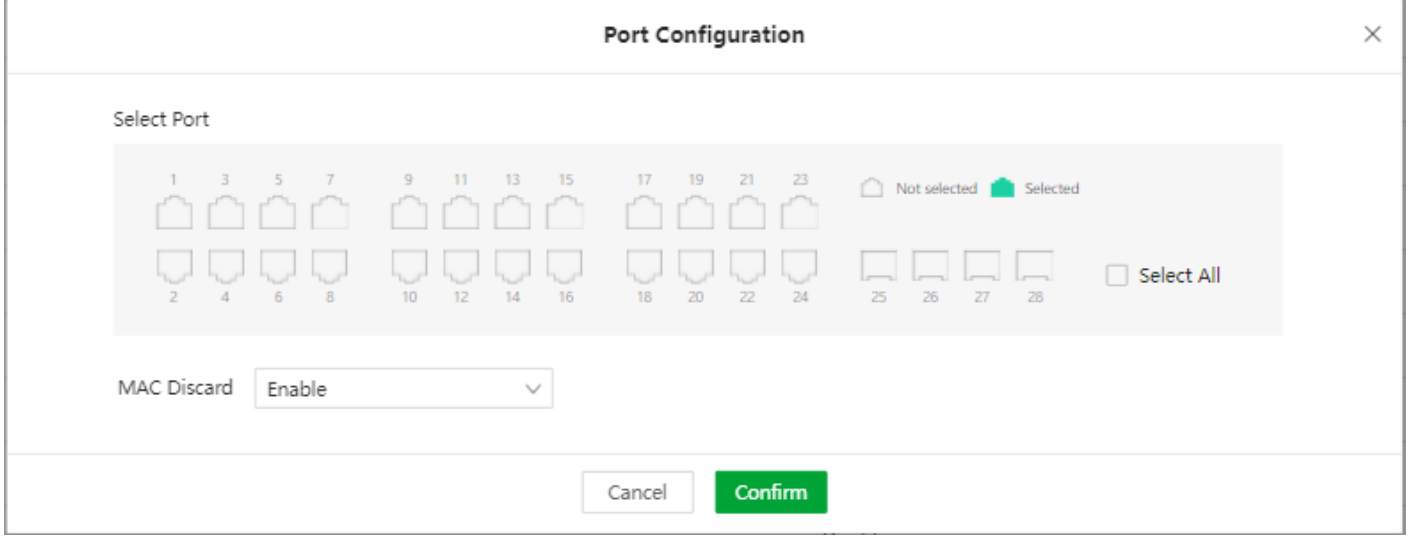
- **Detect whether all flags of TCP messages are 0:** proibir o encaminhamento das sequências TCP e das mensagens de ataque cujos sinalizadores são todos 0.
- **Detect whether the FIN, URG, and PSH flags of the TCP message are all 1:** proibir o encaminhamento das mensagens TCP em que sinalizadores FIN, URG e PSH são todos 1.
- **Detect whether the SYN, FIN, and flags of the TCP message are all 1:** proibir o encaminhamento das mensagens TCP cujos SYN, FIN e sinalizadores são todos 1.
- **Detect whether the SYN and RST flags of the TCP message are both 1:** proibir o encaminhamento das mensagens TCP quando os sinalizadores SYN e RST forem 1.
- **Detect whether the source port number or destination port number of the TCP and UDP message is 0:** proibir o encaminhamento de mensagens TCP e UDP cujo número de porta de origem ou número de porta de destino seja 0.
- **Detect whether the TCP SYN message contains data:** proibir o encaminhamento das mensagens TCP cujas mensagens SYN contenham dados.
- **ICMP message fragment detection:** o switch não responde às mensagens ICMP fragmentadas.

Mac Address Attack Defense

Com esta função habilitada, a porta não realiza o aprendizado de endereço MAC e descarta as mensagens desconhecidas recebidas.



- **Port:** ele exibe o ID da porta.
- **MAC Discard:** com esta função habilitada, a porta descarta as mensagens desconhecidas recebidas.
- **Edit:**ao clicar no botão de Edit temos a tela de Port Configuration, onde pode-se editar a configuração de MAC Discard das portas físicas do Switch.

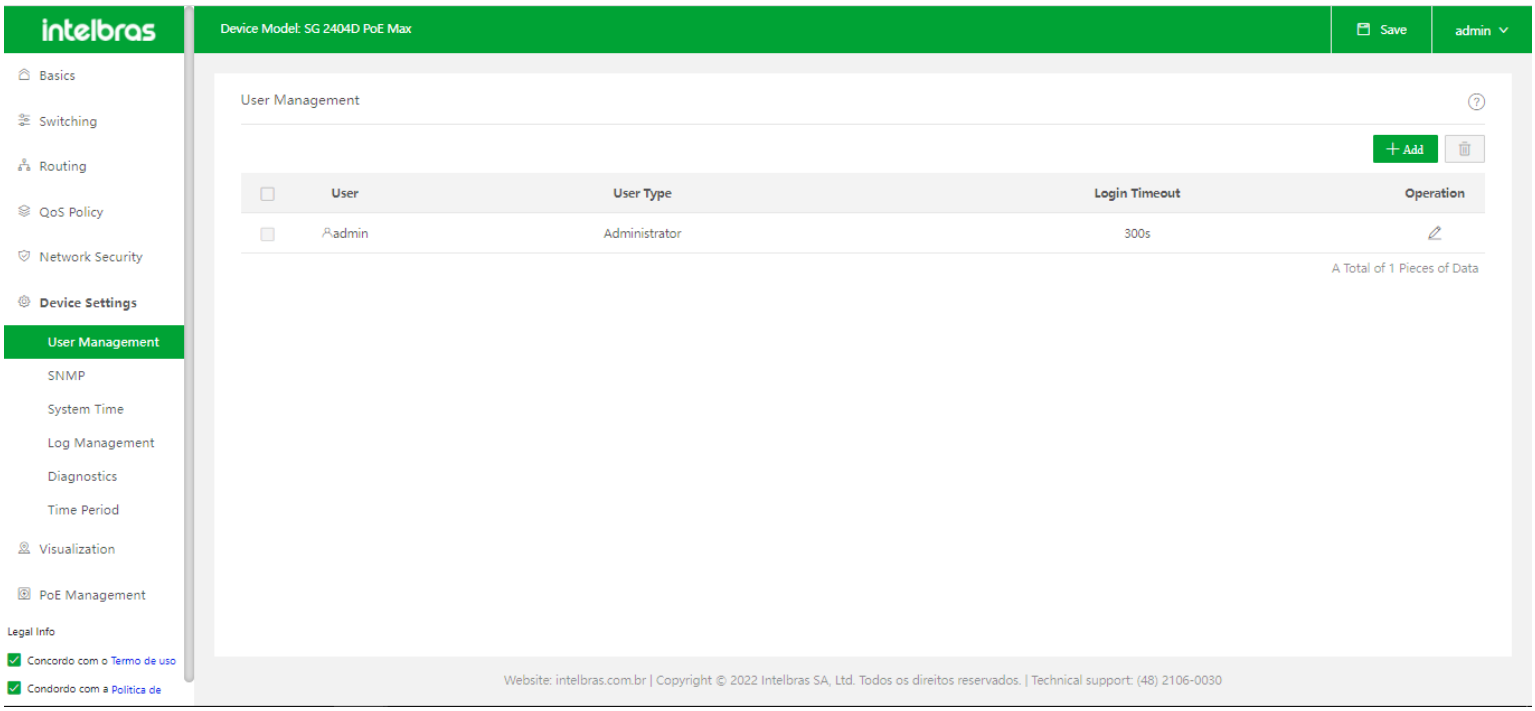


DEVICE SETTINGS

Neste menu temos as configurações de sistema do Switch, como configuração de usuários, Log, horário entre outras.

User Management

Ele é usado para gerenciar os usuários do switch. Admin é o usuário de gerenciamento padrão, ele não pode ser excluído e tem a permissão mais alta.



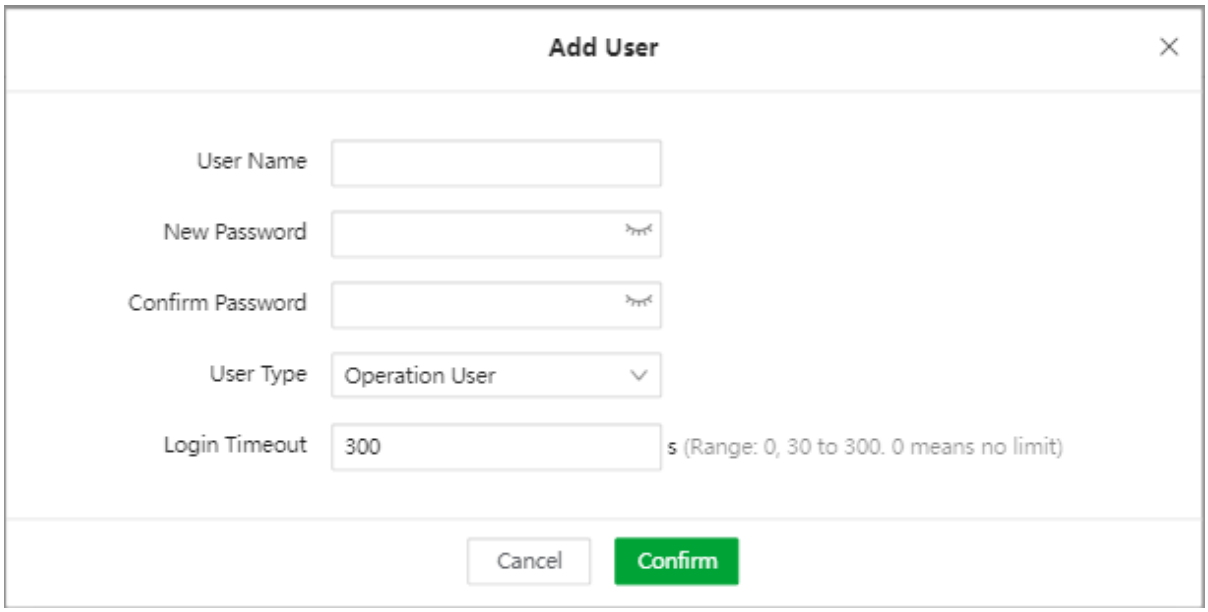
- **User:** especifica o nome do usuário.
- **User Type:** especifica o tipo de permissão que o usuário possui. Temos duas opções:

  Operation User: pode ser utilizado para adicionar e deletar configurações. Mas não pode atualizar, redefinir ou adicionar usuários.

  Common User: pode ser usado apenas para verificar configurações.

- **Login Timeout:** se um usuário não realizar nenhuma operação dentro do intervalo de timeout após fazer login no dispositivo, o sistema fará o logout do usuário.

- **+ Add:** ao clicar no botão + Add temos a tela de Add User, onde pode-se criar novos usuários para acesso ao Switch.

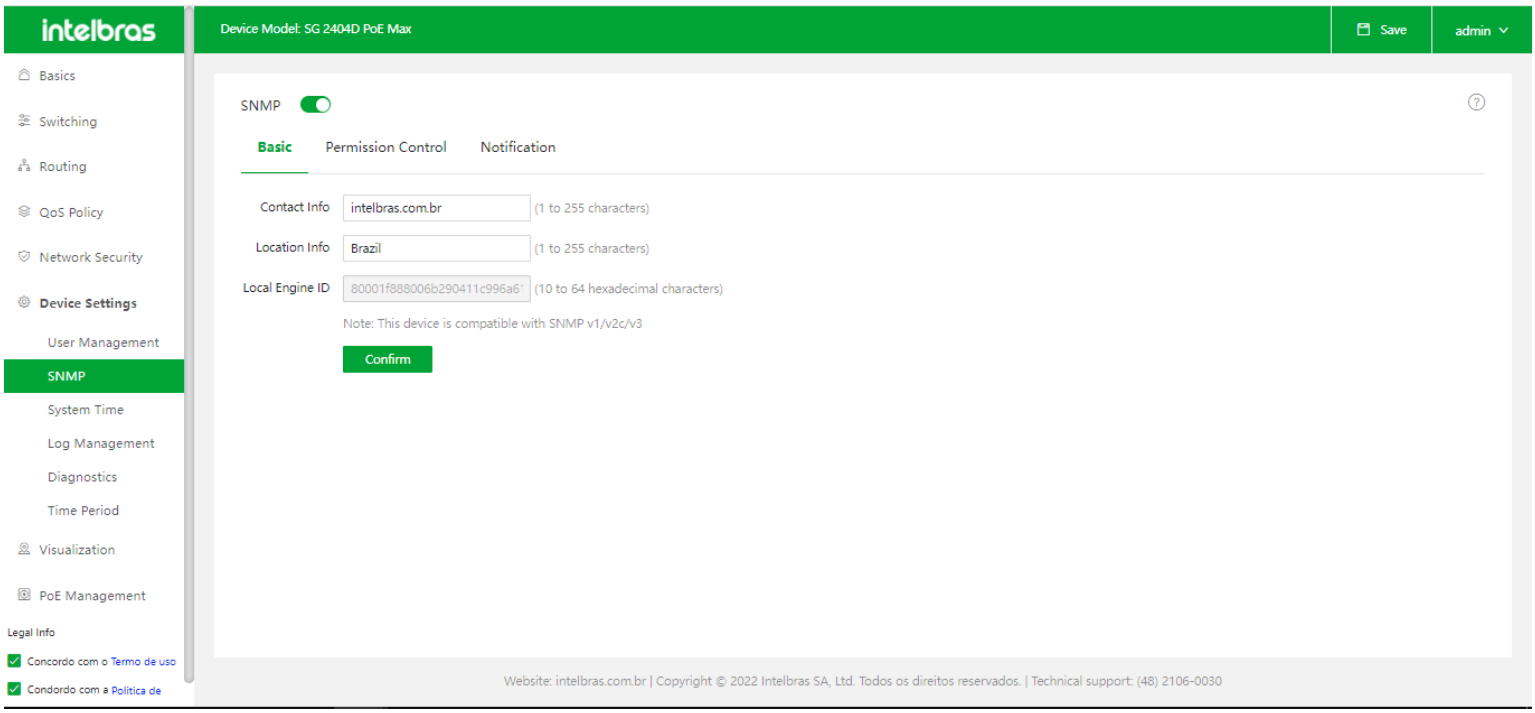


SNMP

SNMP (Simple Network Management Protocol): com o SNMP, uma estação de trabalho de gerenciamento pode gerenciar remotamente todos os dispositivos de rede que suportam este protocolo, incluindo monitoramento do status da rede, modificação da configuração do dispositivo de rede, recebimento de alarmes de eventos de rede e assim por diante.

OBS: o switch é compatível com SNMPv1, SNMPv2c e SNMPv3.

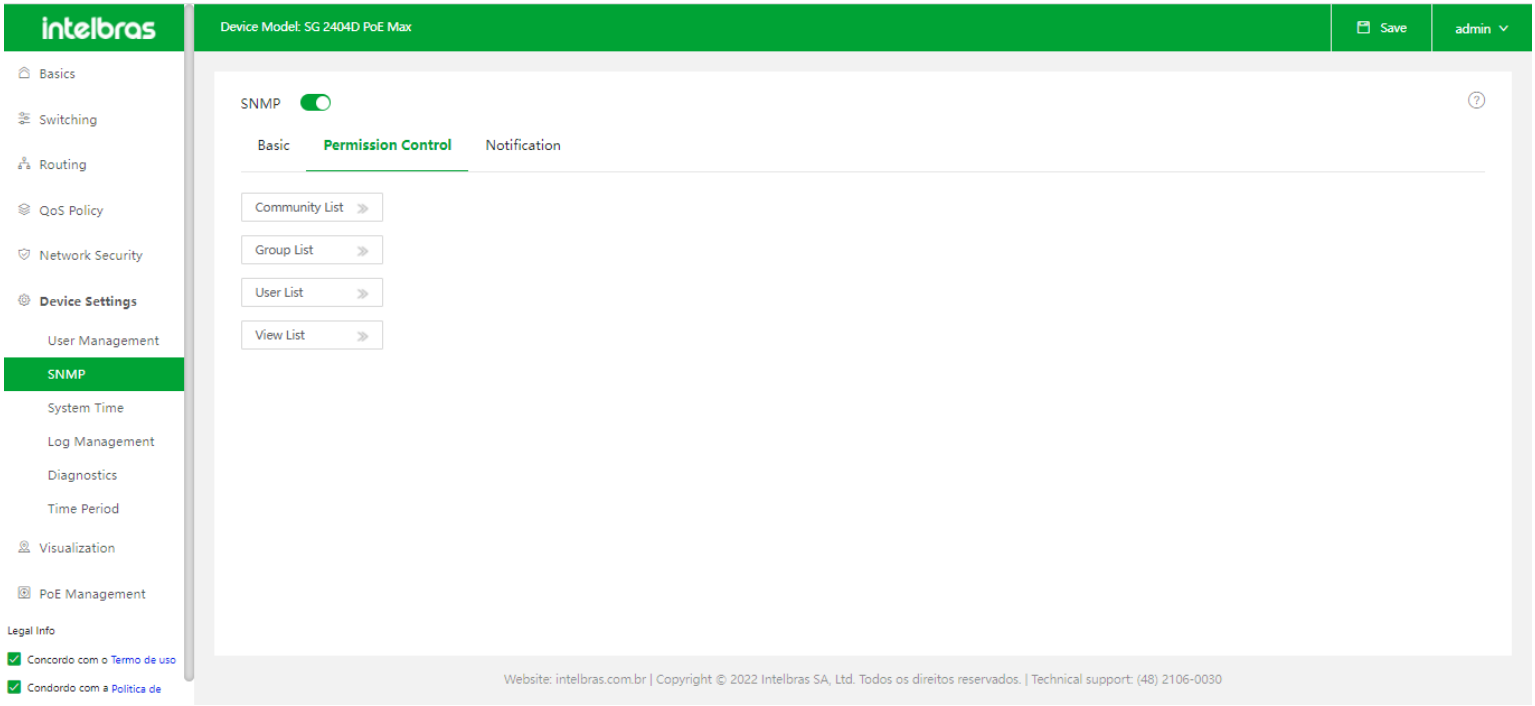
Basic



- **Contact Info:** é usado para configurar as informações de contato do switch para que o gerenciador SNMP localize rapidamente esse switch. Geralmente é definido como o nome de domínio ou endereço IP do switch.
- **Location Info:** é usado para configurar as informações de localização do switch para que o gerenciador SNMP localize rapidamente este switch.

- **Local Engine:** com a função SNMP habilitada, o Local Engine exibe o Engine ID. Você precisa inserir esse ID no servidor SNMP para gerenciar o Switch.

Permission Control



- **Community List**

Os usuários podem acessar o switch por meio do NMS somente após serem adicionados às comunidades. Não há nome de comunidade por padrão, será definido pelo Usuário.

Community Name: especifica o nome de uma comunidade.

Access Mode: especifica o modo usado para as comunidades acessarem informações, incluindo "Somente leitura" e "Leitura e gravação".

MIB View: especifica a visualização que as comunidades podem acessar.

- **Group List**

É usado para adicionar grupos SNMP. Os usuários do grupo podem acessar e controlar a exibição por meio de somente leitura, leitura e gravação e notificação, conforme definido pelo administrador.

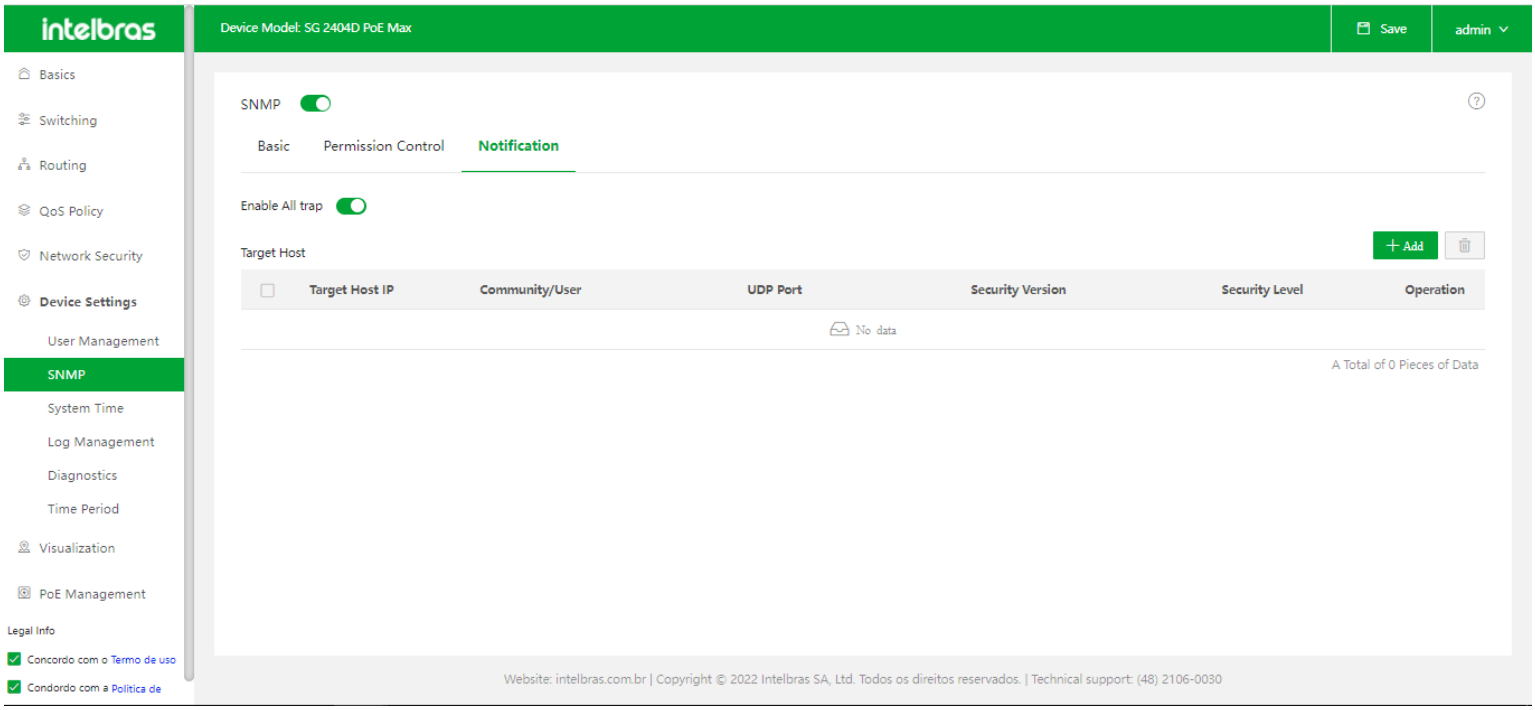
- **User List**

É usado para adicionar usuários. O gerenciador SNMP pode gerenciar o switch adicionando um usuário. Os usuários de um grupo têm o mesmo nível de segurança e a mesma permissão de controle de acesso do restante grupo.

- **View List**

É usado para adicionar visualizações. O OID é usado para descrever os objetos gerenciados do switch nas mensagens SNMP. MIB (Management Information Base) é um conjunto OID dos dispositivos de rede monitorados. A visualização é usada para controlar como gerenciar o OID.

Notification

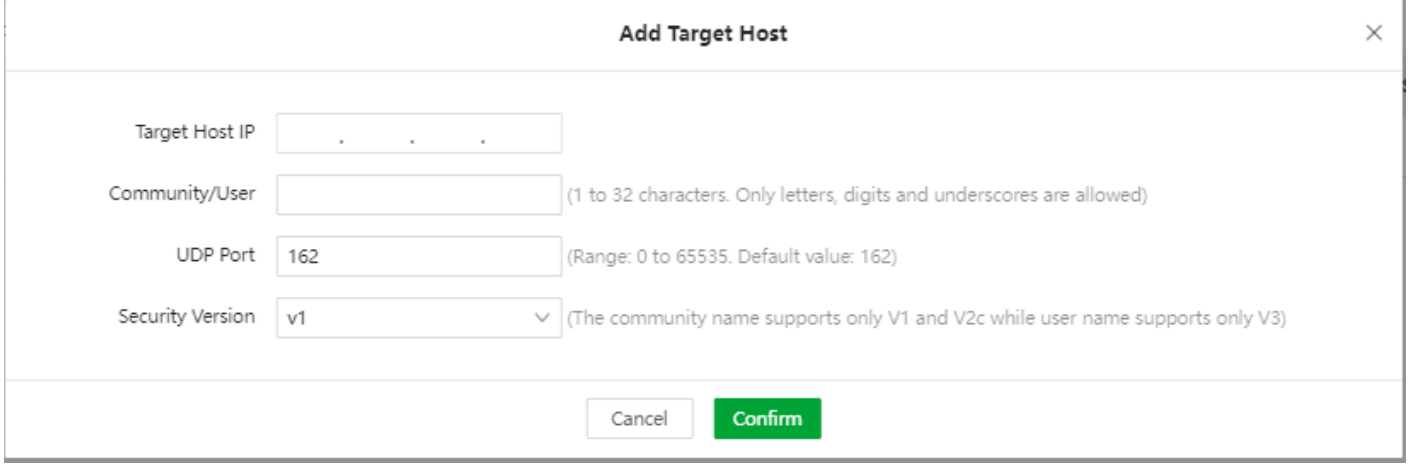


A função Trap permite que o switch envie mensagens ao gerenciador SNMP e notifique alguns eventos urgentes e importantes.

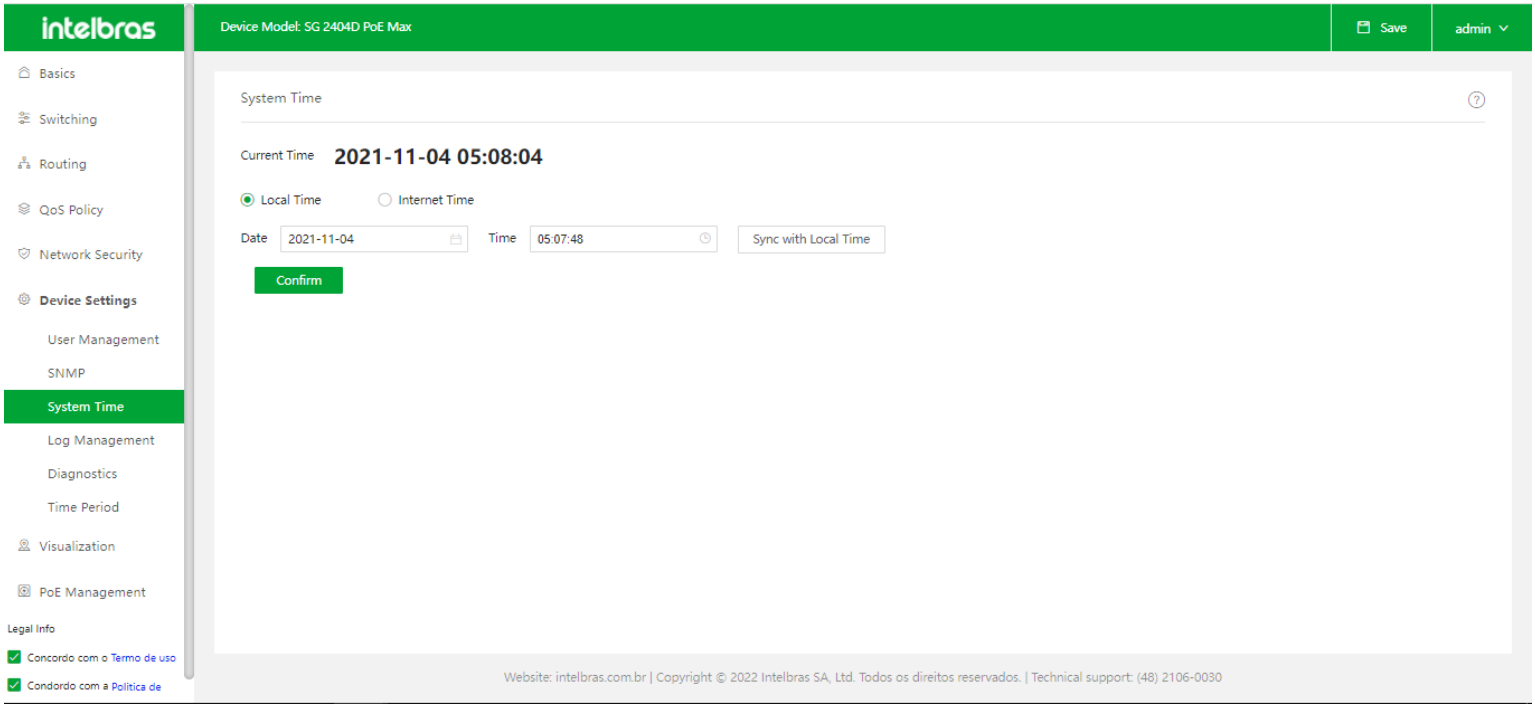
- **Enable All Trap:** este botão serve para habilitar todas as traps SNMP configuradas.
- **Target Host IP:** especifica o endereço IP do host de destino Trap, ou seja, o endereço IP do host de destino para o qual as informações de SNMP serão transmitidas.
- **Community/User:** especifica a Comunidade ou o nome de usuário exigido para autenticação. Você precisa inserir o nome de comunidade ou nome de usuário correspondente, é possível verificá-los no módulo SNMP>Permission Control. Se a Versão de segurança estiver definida como v3, apenas um nome de usuário será permitido. Quando a versão de segurança é definida como v1 ou v2c, apenas um nome de comunidade é permitido.
- **UDP Port:** especifica a porta UDP habilitada para as Traps no host gerenciado.
- **Security Version:** é usado para selecionar uma versão de segurança usada pelas Traps, incluindo v1, v2c e v3.
- **Security Level:** quando a versão de segurança é definida como v3, você precisa selecionar um nível de segurança. Os Níveis de Segurança incluem No Security (Sem segurança), Authentication (Autenticação), e Authentication and Privacy (Autenticação e privacidade).

OBS: quando a Comunidade/Usuário é definido com um nome de usuário, a Versão de segurança suporta apenas v3 e o Security Level só pode ser configurado igual ao security level do grupo ao qual o usuário pertence.

- **+ Add:** ao clicar no botão de + Add temos a tela de ADD Target Host, onde podemos configurar o host para qual as Traps SNMP serão enviadas.



System Time

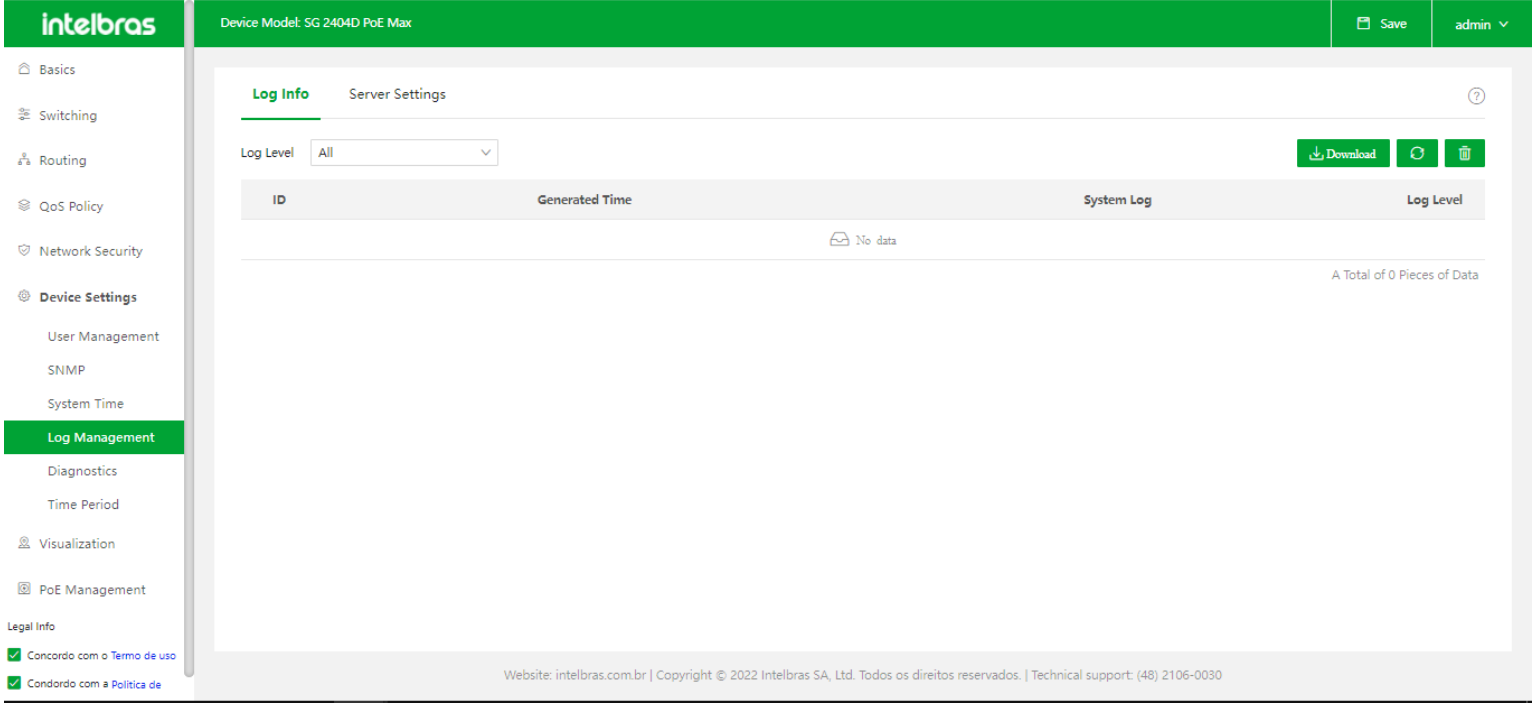


- **Local Time:**é usado para configurar a hora do sistema do switch localmente.
- **Sync with Local Time:** clique neste botão para sincronizar a hora do sistema do switch com o computador que está gerenciando o Switch
- **Internet Time:** depois de se conectar à Internet, o switch sincroniza o horário do sistema com o servidor de horário da Internet.
- **Time Zone:** ele especifica o fuso horário padrão do país ou região em que o switch está localizado.

Log Management

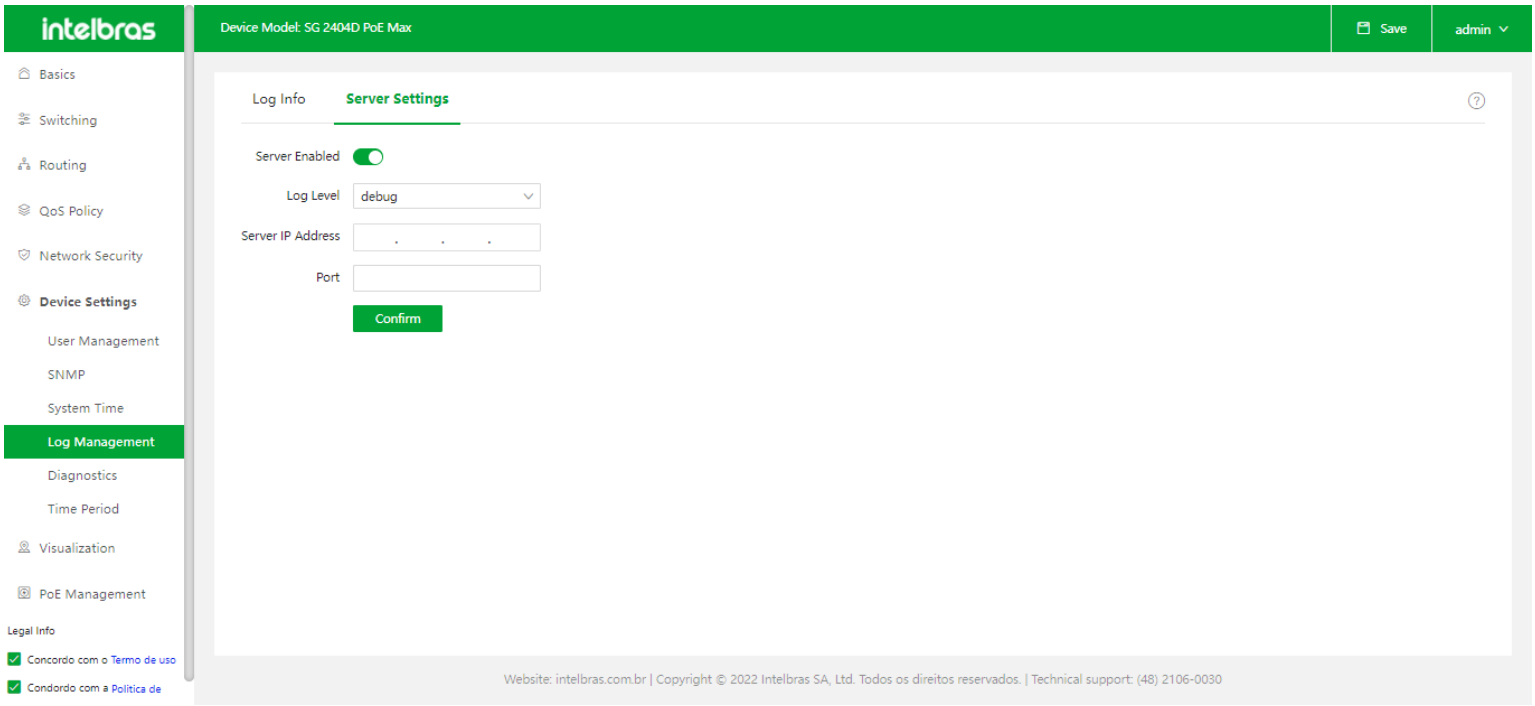
Exibe alarmes e outros logs gerados durante o processo de operação do switch.

Log Info



- **Log Level:** é usado para filtrar quais tipos de logs são exibidos.
- **Generated Time:** informa o horário em que o Log foi gerado.
- **Log Level:** informa qual o nível da respectiva mensagem de Log.
- **System log:** exibe o conteúdo da mensagem de log. Por exemplo, as informações UP/DOWN das portas.

Server Settings

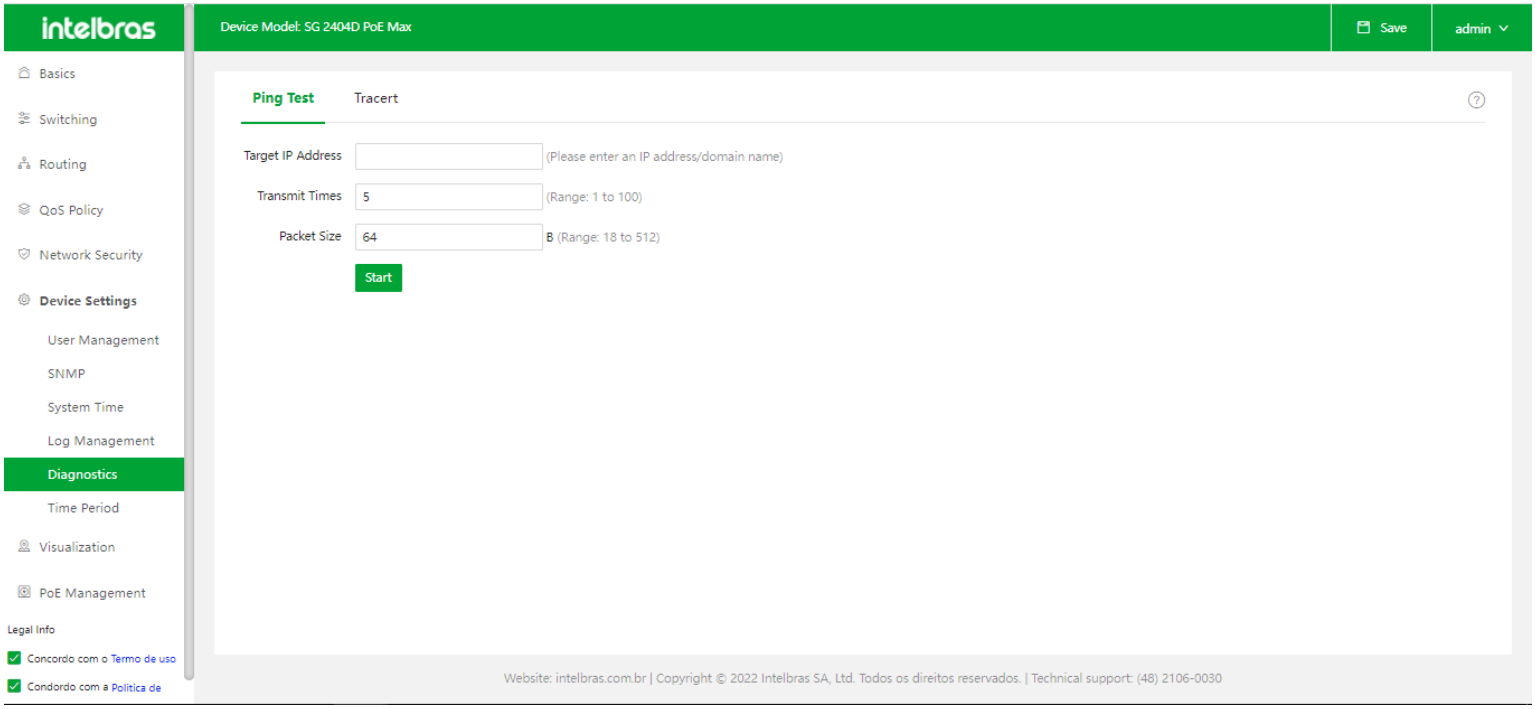


- **Log Level:** serão enviados ao servidor os Logs com o nível igual e maior do que o configurado.
- **Server IP Address:** especifica o endereço IP de um servidor de log.
- **Port:** especifica o número da porta usada pelo servidor de log.

Diagnostics

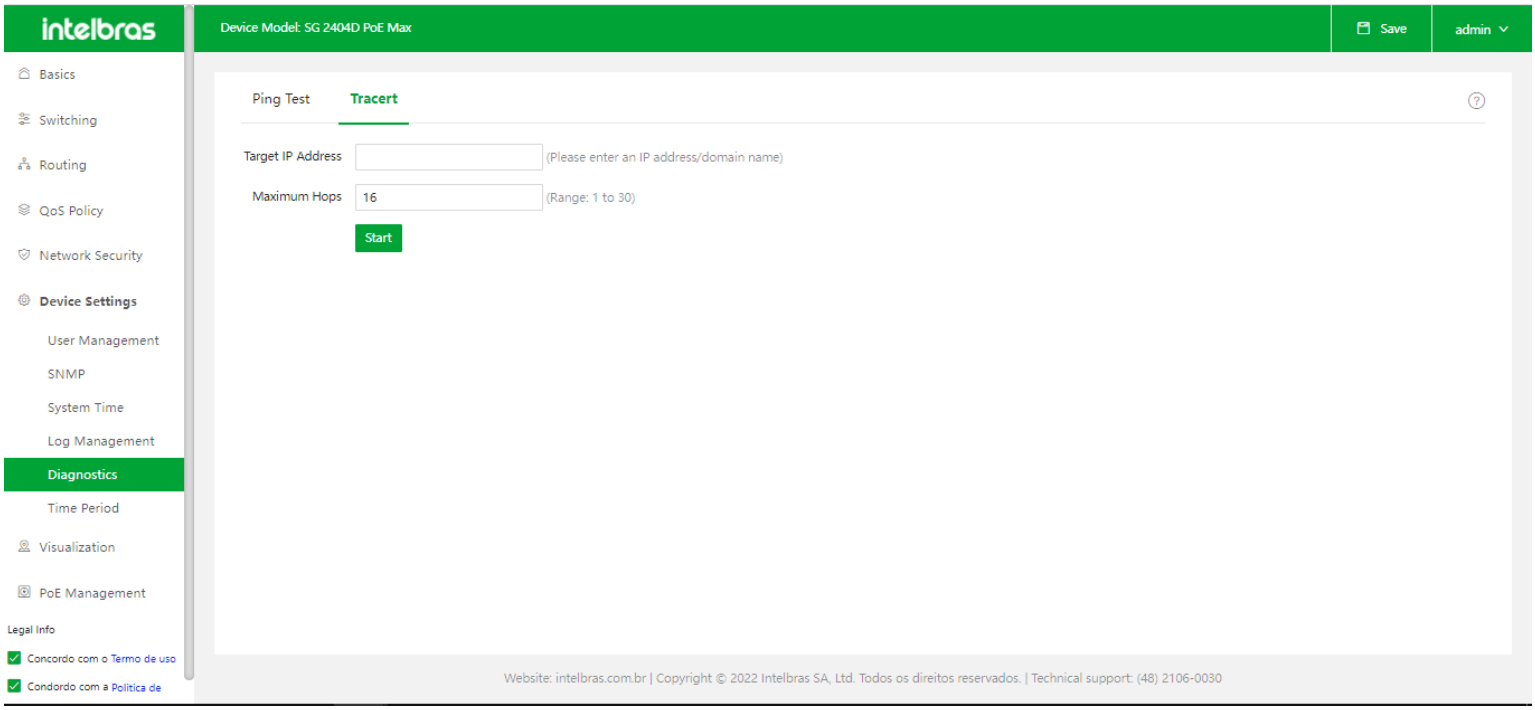
Neste menu temos disponíveis duas ferramentas para diagnostico de rede, ferramenta de ping e de traceroute.

Ping Test



- **Target IP Address:** especifica o endereço IP do dispositivo a ser pingado.
- **Transmit Times:** especifica o número de pacotes de dados enviados pelo Ping.
- **Packet Size:** especifica o tamanho dos pacotes de dados enviados pelo Ping.

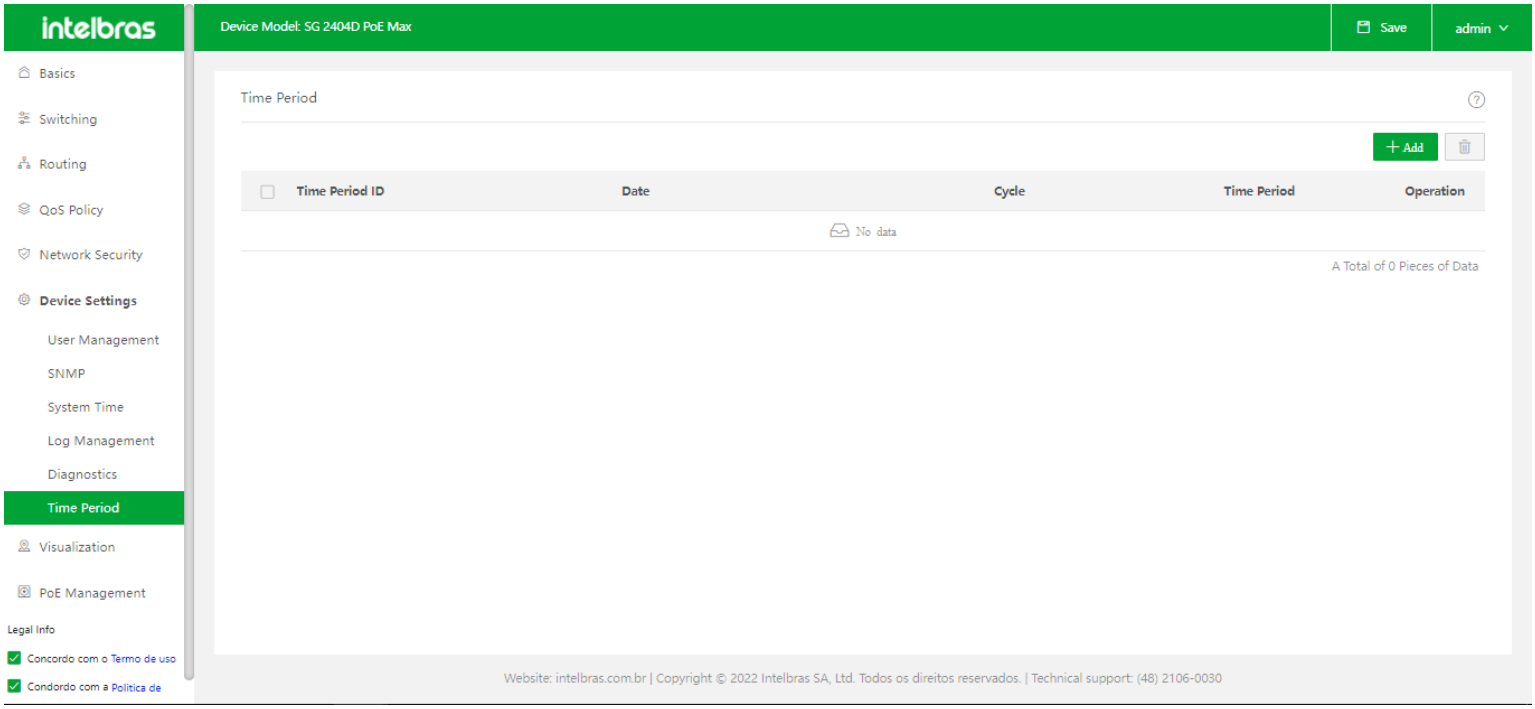
Tracert



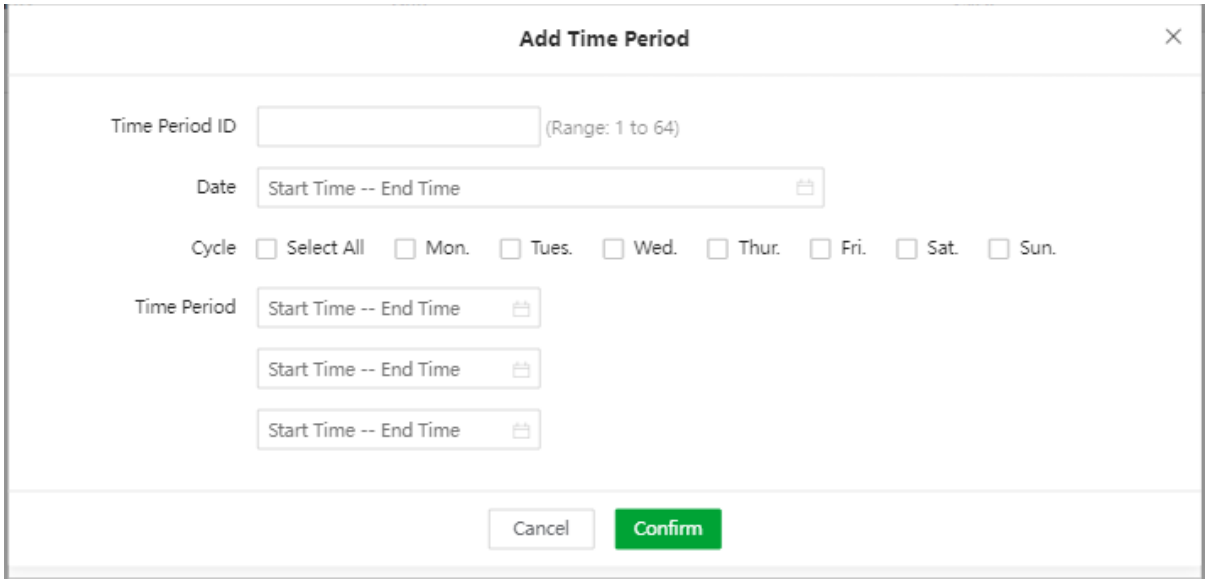
- **Target IP Address:** especifica o endereço IP do dispositivo para o qual o Teste Tracert deve ser realizado.
- **Maximum Hops:** especifica os saltos máximos para o teste Tracert.

Time Period

É usado para configurar a data, ciclo e período de tempo especificados para controlar os períodos no qual a função PoE tem efeito. Funciona como um agendamento do PoE.



- **Time Period ID:** especifica o ID do período de tempo.
- **Date:** usado para especificar as datas de início e término.
- **Cycle:** usado para especificar os dias do ciclo, variando de Segunda a Domingo.
- **Time Period:** usado para especificar o período de tempo, variando de 0 a 24 horas. A hora de início deve ser anterior à hora de término. São permitidos no máximo 3 períodos de tempo.
- **+ Add:** ao clicar no botão + Add temos a tela de Add Time Period. Nesta tela podemos configurar o agendamento do PoE.



Notas:

Se você configurou apenas um dentre Date, Cycle e Period, somente o parâmetro configurado é efetivo. Se você configurou dois ou três dos parâmetros, o tempo de sobreposição é efetivo.

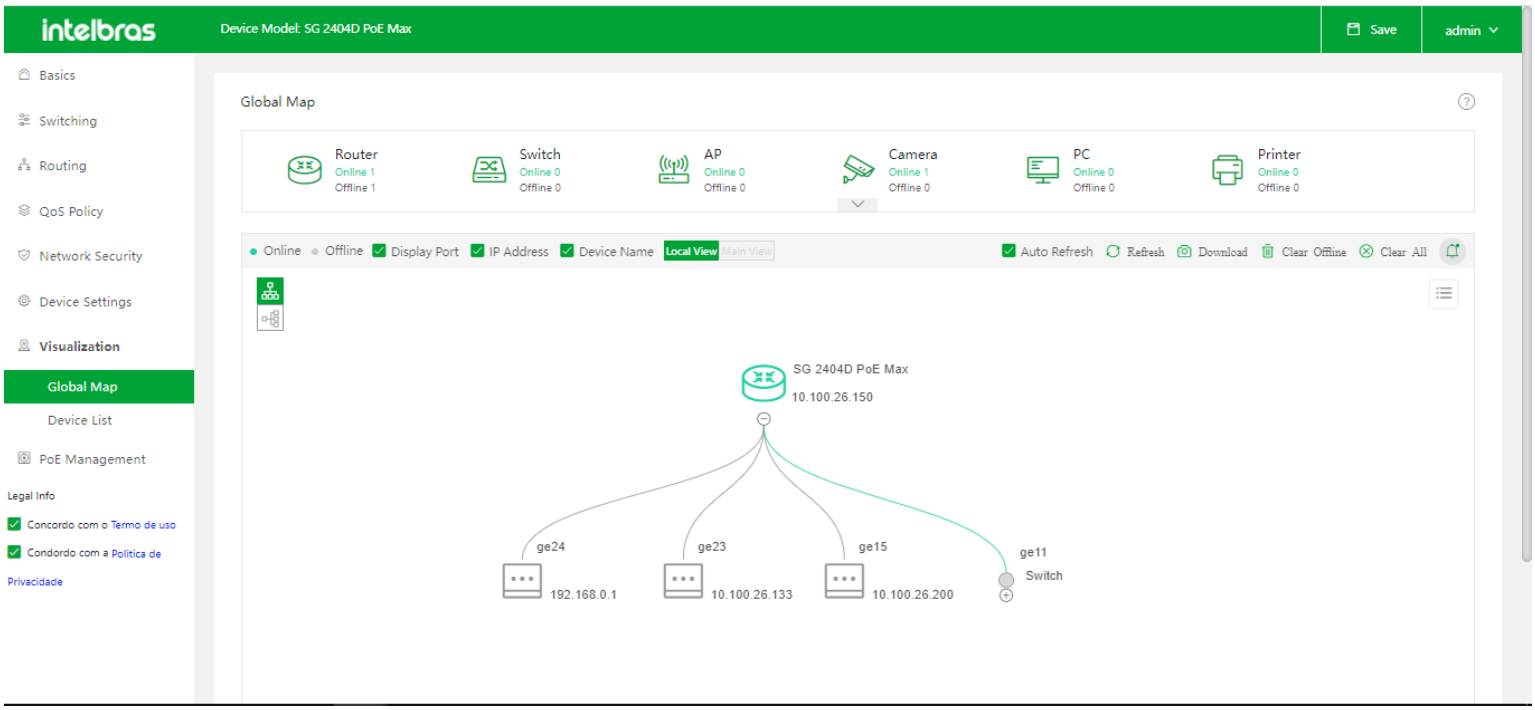
Se você configurou apenas o Período de Tempo, o período de tempo configurado é efetivo todos os dias por padrão.

Se você configurou apenas o Ciclo, como Domingo, mas não configurou o Período de Tempo, todas as 24 horas de domingo serão eficazes.

VISUALIZATION

Neste menu temos disponíveis informações sobre a vizinhança do Switch.

Global Map



- **Device Statistics:** mostra o número de dispositivos online/offline e cada tipo de dispositivo na rede.
- **Refresh/Auto Refresh:** para atualizar a topologia de rede, clique no botão Refresh ou ative a função Auto Refresh. Ciclo de atualização automática: 600 segundos.
- **Topology Download:** é usado para salvar a topologia no formato PNG localmente. A topologia com um máximo de 1000 dispositivos pode ser salva dependendo da configuração do processador do computador
- **Search Device:** é usado para pesquisar o dispositivo por nome do dispositivo/endereço IP/endereço MAC.
- **Online/Offline Status:** no mapa, os ícones de dispositivo cinza representam dispositivos off-line e verdes para dispositivos on-line.
- **Local View/Main View**

  Local View: especifica a topologia com o Switch como nó raiz.

  Main View: especifica a topologia com o dispositivo principal como nó raiz.

  Main Device: especifica o dispositivo central de comutação na rede. Você pode personalizá-lo.

  OBS: quando houver apenas um dispositivo principal que não seja este dispositivo na topologia, você poderá alternar para a visualização principal.

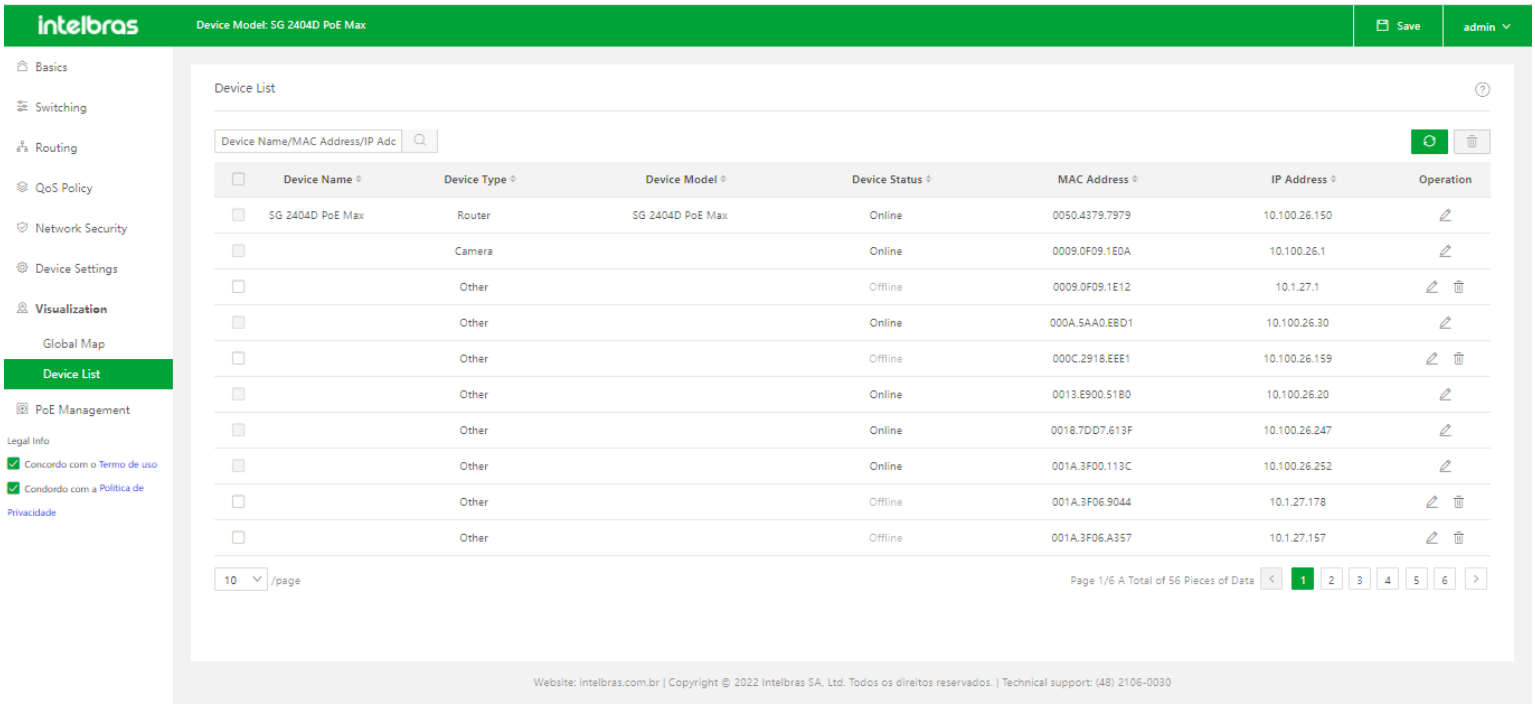
- **Vertical Expansion/Horizontal Expansion:** altera o modo exibição da topologia. Temos duas opções de visualização: Vertical e Horizontal
- **Alert Messages:** clique no icone de sino para visualizar as mensagens de alerta de loop da topologia. As mensagens de alerta são atualizadas automaticamente a cada 30 s.

- **Clear Offline:** limpa os dispositivos offline na topologia.
- **Clear All:** limpa todos os dispositivos da topologia.
- **Save:** é usado para salvar as descrições e tipos de dispositivos definidos pelo usuário, bem como a topologia atual (que é adotada após a reinicialização do dispositivo).

OBS: somente câmeras IP no mesmo segmento de rede com este switch podem ser identificadas como câmeras.

Device List

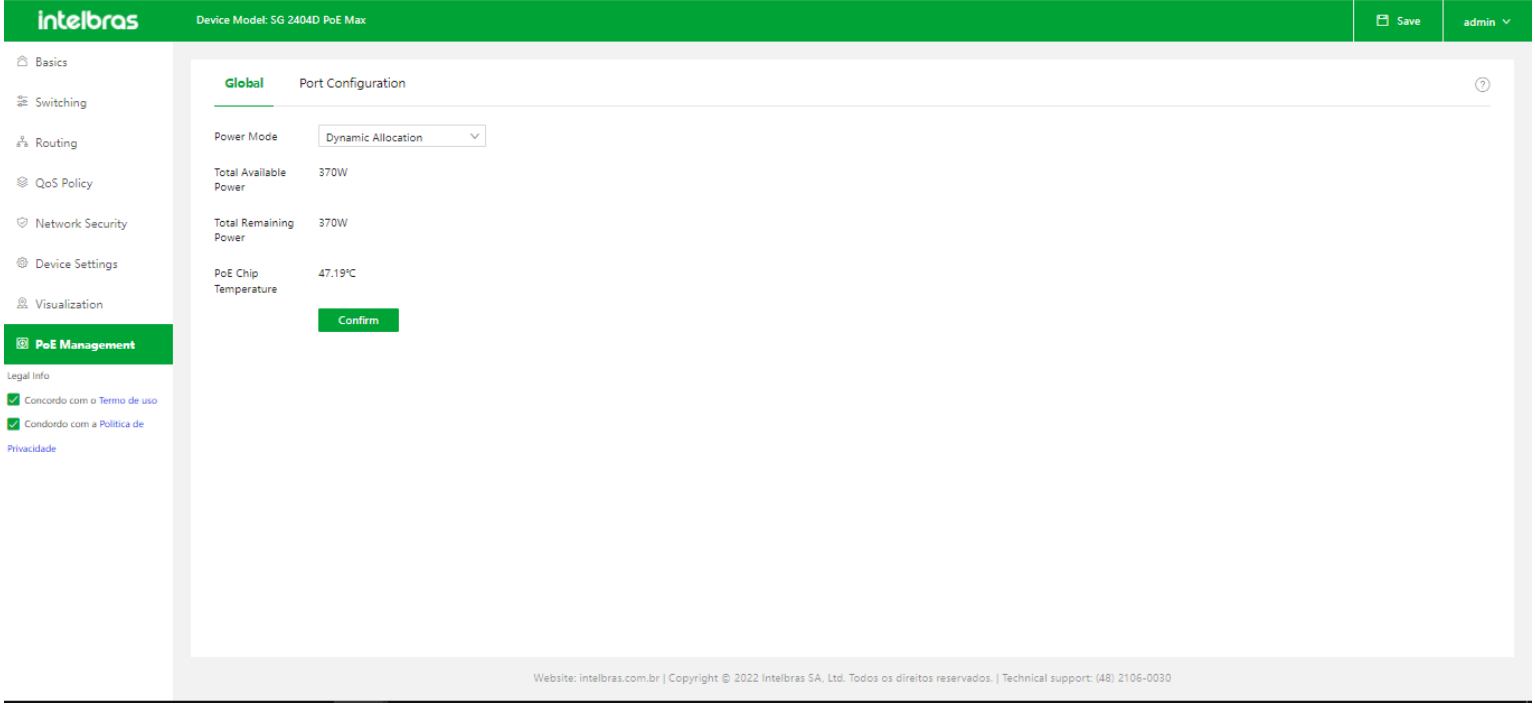
Ele exibe todos os dispositivos online e offline no mapa. Você pode excluir dispositivos offline em quantidade, mas não pode excluir dispositivos online. Os dispositivos excluídos da lista também serão excluídos do mapa.



POE MANAGEMENT

Neste menu teremos as configurações voltadas as propriedades do PoE do Switch.

Global



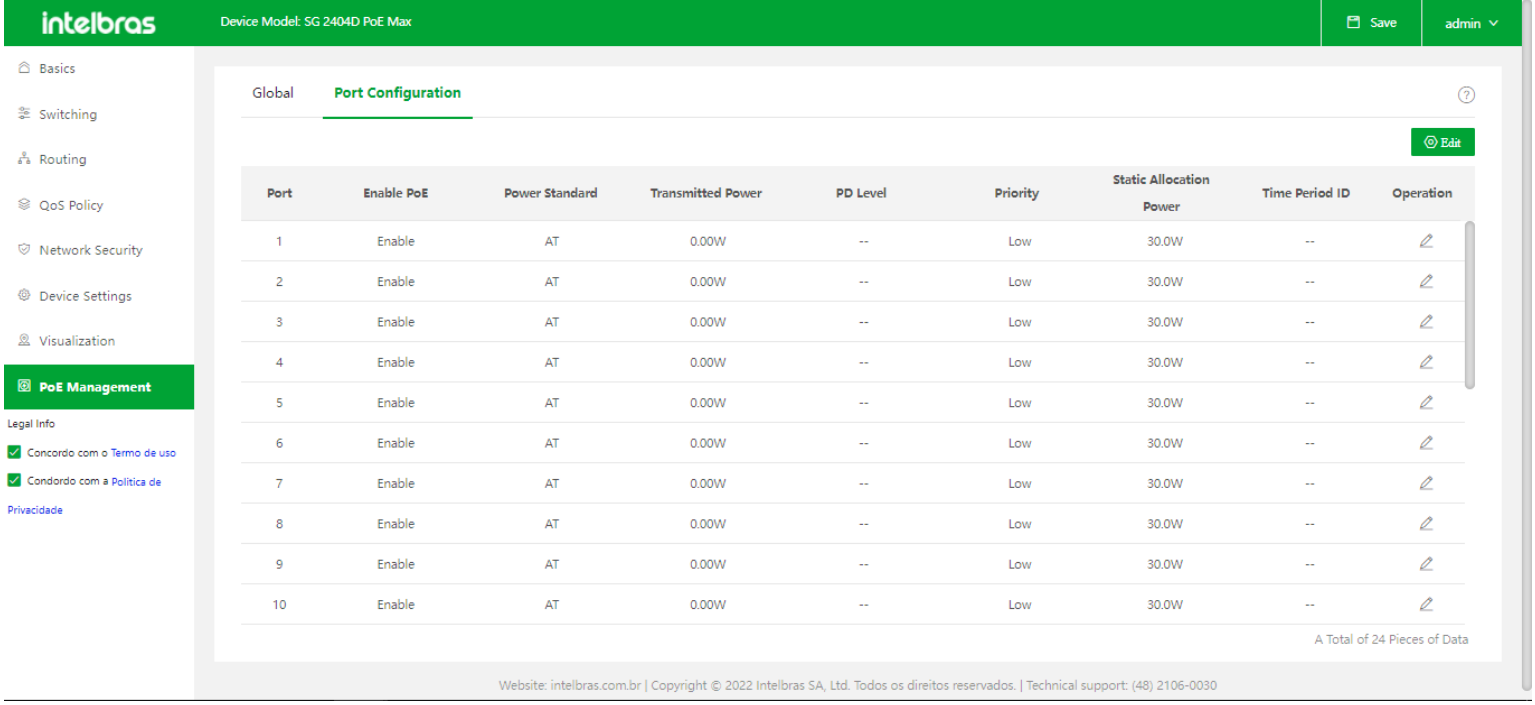
- **Power Mode:** É usado para selecionar um modo de energia para a fonte de alimentação PoE do switch. Temos duas opções de configuração:

  Static Allocation: permite configurar uma alimentação para cada porta do switch. Quando o switch fornecer energia PoE, a energia configurada será obrigatoriamente reservada para esta porta, não podendo ser utilizada por outras portas.

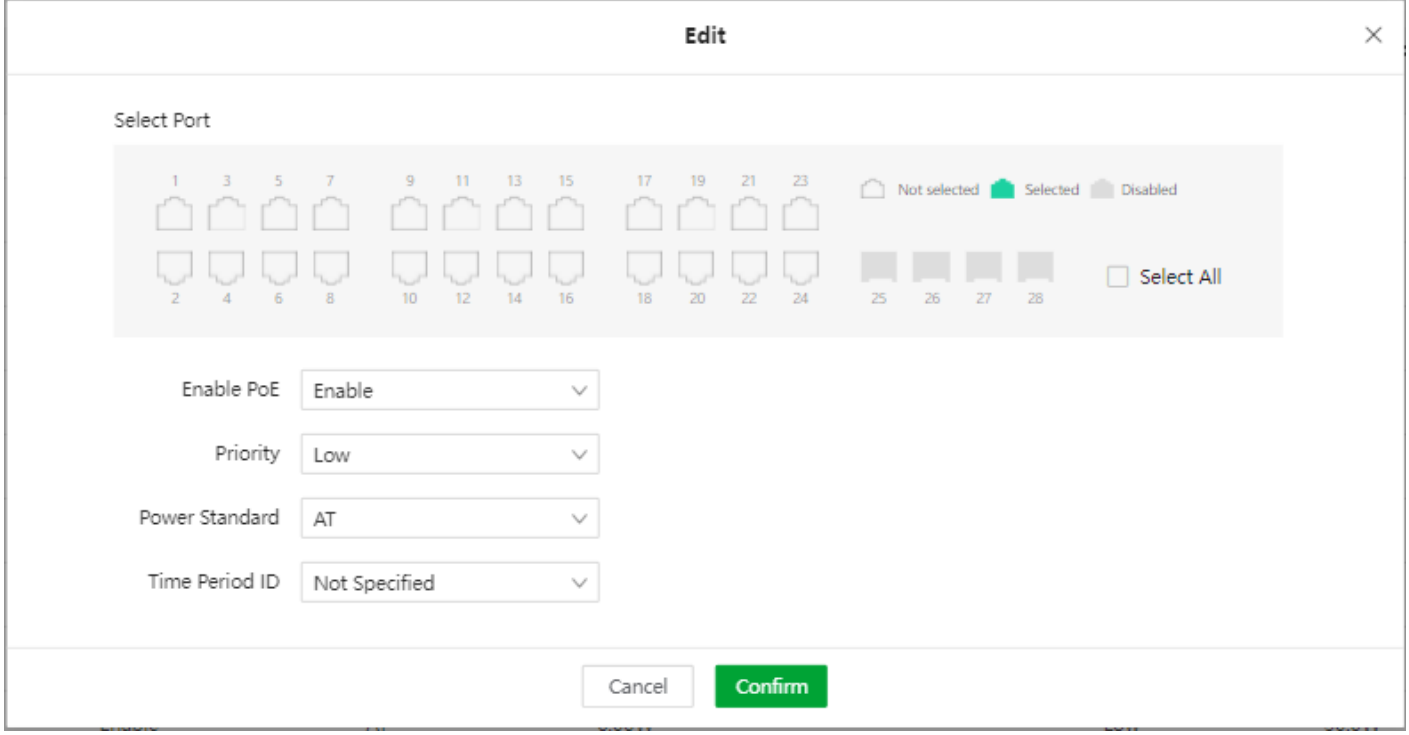
  Dynamic Allocation: o switch aloca energia com base na energia consumida por cada porta. Ao atingir a carga total, o switch aloca energia com base na prioridade da porta configurada (prioridade + número da porta). Se as prioridades forem as mesmas, a porta com o menor número de porta terá uma prioridade mais alta.

- **Total Available Power:** especifica a potência máxima suportada pelo switch.
- **Total Remaining Power:** especifica a potência restante do switch.
- **PoE Chip Temperature:** especifica a temperatura do chip PoE.

Port Configuration



- **Port:** especifica o número da porta física do switch.
- **PoE Status:** especifica o status do PoE da porta atual. Somente a porta com a função PoE habilitada pode fornecer energia a um dispositivo conectado e que tenha suporte a alimentação PoE.
- **Power Standard:** padrão de alimentação das portas: AT (IEEE 802.3at) ou AF(IEEE 802.3af) A potência máxima de cada porta no padrão AT é 30 W, enquanto que no padrão AF é 15,4 W.
- **Transmitted Power:** especifica a potência PoE em tempo real.
- **PD Level:** especifica o nível do dispositivo alimentado por PoE conectado à porta atual quando a fonte de alimentação está normal. O switch obtém automaticamente o nível do dispositivo.
- **Priority:** especifica a prioridade da porta, que entra em vigor somente quando o Power Mode é definido como Dynamic Allocation. Uma prioridade de porta razoável garante que as portas especificadas ainda possam fornecer energia adequadamente sob o estado de carga total. Entre as portas com prioridades diferentes, aquelas com prioridades mais altas deverão garantir a potência necessária. Entre as portas com a mesma prioridade, as portas com menores IDs devem ter prioridade para garantir a energia necessária.
- **Static Allocation Power:** especifica a potência de alocação estática da porta, que entra em vigor somente quando o Power Mode é definido como Static Allocation
- **Time Period ID:** especifica o período de tempo em que a função de alimentação PoE da porta está desabilitada. Você precisa configurar a regra de período de tempo no menu "Device Management" > " Time Period Management". Se nenhum período de tempo for especificado, a função de alimentação PoE de uma porta entrará em vigor normalmente e não terá limite de tempo.
- **Edit:** ao clicar no botão de Edit temos a tela para editar as configurações de PoE de uma ou mais portas.


Edit
Select Port
1 3 5 7 9 11 13 15 17 19 21 23
2 4 6 8 10 12 14 16 18 20 22 24
25 26 27 28
Not selected
Selected
Disabled
Select All
Enable PoE
Enable
Priority
Low
Power Standard
AT
Time Period ID
Not Specified
Cancel
Confirm

TERMO DE GARANTIA

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

Nome do cliente:

Assinatura do cliente:

Nº da nota fiscal:

Data da compra:

Modelo:

Nº de série:

Revendedor:

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

1. Todas as partes, peças e componentes do produto são garantidos contra eventuais defeitos de fabricação, que porventura venham a apresentar, pelo prazo de 3 (três) anos da data de compra – sendo 90 (noventa) dias de garantia legal e 33 (trinta e três) meses de garantia contratual –, contado a partir da data de entrega do produto ao Senhor Consumidor, conforme consta na nota fiscal de compra do produto, que é parte integrante deste Termo em todo o território nacional. Esta garantia contratual compreende a troca gratuita de partes, peças e componentes que apresentarem defeito de fabricação, incluindo a mão de obra utilizada nesse reparo. Caso não seja constatado defeito de fabricação, e sim defeito(s) proveniente(s) de uso inadequado, o Senhor Consumidor arcará com essas despesas.

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

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

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

5. A garantia perderá totalmente sua validade na ocorrência de quaisquer das hipóteses a seguir: a) se o vício não for de fabricação, mas sim causado pelo Senhor Consumidor ou por terceiros estranhos ao fabricante; b) se os danos ao produto forem oriundos de acidentes, sinistros, agentes da natureza (raios, inundações, desabamentos, etc.), umidade, tensão na rede elétrica (sobretensão provocada por acidentes ou flutuações excessivas na rede), instalação/uso em desacordo com

o manual do usuário ou decorrentes do desgaste natural das partes, peças e componentes; c) se o produto tiver sofrido influência de natureza química, eletromagnética, elétrica ou animal (insetos, etc.); d) se o número de série do produto tiver sido adulterado ou rasurado; e) se o aparelho tiver sido violado.

6. Esta garantia não cobre perda de dados, portanto, recomenda-se, se for o caso do produto, que o Consumidor faça uma cópia de segurança regularmente dos dados que constam no produto.

7. A Intelbras não se responsabiliza pela instalação deste produto, e também por eventuais tentativas de fraudes e/ou sabotagens em seus produtos. Mantenha as atualizações do software e aplicativos utilizados em dia, se for o caso, assim como as proteções de rede necessárias para proteção contra invasões (hackers). O equipamento é garantido contra vícios dentro das suas condições normais de uso, sendo importante que se tenha ciência de que, por ser um equipamento eletrônico, não está livre de fraudes e burlas que possam interferir no seu correto funcionamento.

A garantia contratual deste termo é complementar à legal, portanto, a Intelbras S/A reserva-se o direito de alterar as características gerais, técnicas e estéticas de seus produtos sem aviso prévio.

Sendo estas as condições deste Termo de Garantia complementar, a Intelbras S/A se reserva o direito de alterar as características gerais, técnicas e estéticas de seus produtos sem aviso prévio.

Todas as imagens deste manual são ilustrativas.

---

intelbras

fale com a gente

Suporte a clientes: (48) 2106 0006

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

Suporte via chat: intelbras.com/suporte-tecnico (http://www.intelbras.com/suporte-tecnico)

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

SAC: 0800 7042767

Onde comprar? Quem instala?: 0800 7245115

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

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

CNPJ 82.901.000/0014-41 - www.intelbras.com.br (http://www.intelbras.com.br)

Indústria Brasileira