Manual do Usuário

SG 2404 MR L2+ | SG 5204 MR L2+

Versão deste manual: 1.0.0

SG 2404 MR L2+ | SG 5204 MR L2+

Switch gerenciável 24 ou 52 portas Gigabit Ethernet com 4 portas Mini-GBIC

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

O switch SG 2404 MR L2 + possui 24 portas Gigabit Ethernet, sendo 24 portas RJ45 e 4 slots Mini-GBIC compartilhados.

O switch SG 5204 MR L2 + possui 52 portas Gigabit Ethernet, sendo 48 portas RJ45 e 4 slots Mini-GBIC independentes.

Ambos proporcionam altas taxas de transferência de dados, permitindo a integração de computadores, impressoras, dispositivos VoIP como ATA e telefone IP, além de 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.

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

ÍNDICE

VLAN

- VLAN
- VLAN de voz
- Surveillance VLAN
- MAC VLAN
- Guest VLAN
- VLAN por protocolo
- MVR - Multicast VLAN Registration
- GVRP

SEGURANÇA

- Prevenção de ataque
- Ferramentas
- Proteção DDoS
- Loopback
- STP
- Controle de acesso - ACL
- IGMP
- MLD - Multicast Listener Discovery

SISTEMA

- Sistema
- Atualizar firmware
- Informações
- Gerenciar configurações
- SNMP
- EEE
- RMON
- Roteamento estático - IPv4

QOS

- Agendar prioridade

UTILIZANDO O CLI

- Acessando a interface de Linha de Comando CLI
- Login pela porta console
- Login via SSH
- Logon via Telnet
- Modos de comandos CLI
- Mostrar usuários conectados
- Níveis de segurança
- Convenções

INTERFACE DO USUÁRIO

- Enable
- Disable
- Configure Terminal
- Exit
- End
- History

STORM CONTROL

- Storm control
- No storm-control
- Show storm control

CONTROLE DE FLUXO - FLOW CONTROL

- Ativando controle

AGREGAÇÃO DE LINK - LINK AGGREGATION

- Link-aggregation
- Interface link-aggregation

- Show link-aggregation

ESPELHAMENTO DE PORTAS - PORT MIRROR

- Monitor session
- Show monitor

COMANDOS DE ISOLAMENTO DE PORTAS - PORT ISOLATION

- Switchport protected
- Show protected

PORT SPEED LIMIT

- Rate-limit
- Show rate-limit

IEEE 802.1Q VLAN

- VLAN
- Description
- Show VLAN
- Switch mode
- Atribuir VLAN
- Vincular VLAN nativa

VLAN DE VOZ - VOICE VLAN

- Voice VLAN
- Modos Voice VLAN
- Voice VLAN OUI
- Voice VLAN aging-time and COS
- Show voice VLAN

VLAN DE VIGILÂNCIA - SURVEILANCE VLAN

- Surveilance VLAN
- Modos surveilance VLAN

- Surveilance Voice VLAN OUI
- Surveilance VLAN aging-time and COS
- Show surveilance VLAN

MAC VLAN

- TITULO
- TITULO
- TITULO

VLAN DE CONVIDADO - GUEST VLAN

- Configurações servidor RADIUS
- Modos de autenticação
- Guest VLAN
- Modo de controle da porta

VLAN POR PROTOCOLO

- Grupo protocolo VLAN
- Interface protocolo VLAN

MVR - MULTICAST VLAN REGISTRATION

- MVR
- Tipo de porta e MVR immediate
- Modo MVR
- Grupo MVR
- Tempo de consulta - query time

GVRP

- GVRP
- gvrp registration-mode
- gvrp vlan-creation-forbid

Proteção DDoS

- Configurando PROTEÇÃO DDOS
- Show DDoS

Inspeção ARP

- ARP inspection
- ARP inspection rate-limit
- ARP inspeciton trust
- ARP inspection validate
- Limopar estatística ARP inspection

COMANDOS DE SEGURANÇA DE PORTAS - PORT SECURITY

- Port-security
- Show port-security

DHCP-SNOOPING

- Ativando DHCP-snooping
- DHCP-snooping trust

SEGURANÇA DE ACESSO A INTERFACE WEB

- Habilitando segurança
- Vinculando interface e dispositivo confiável

FERRAMENTAS DE TESTE DE CONEXÃO

- Ping
- Traceroute
- Diagnóstico de cabo

DETECÇÃO DE LOOPBACK

- Loopback-detection

SPANNING TREE

- Habilitar spanning-tree
- Habilitar spanning-tree na interface

- Modo Spanning Tree
- Atraso progressive no Root
- Intervalo de envio BPDU
- Spanning-tree max-age
- Spanning-tree max-hops - saltos
- Spanning-tree pathcost method
- Spanning-tree priority - root bridge
- Spanning tree mst configure
- Modo BPDU
- Path Cost
- Spanning tree guard
- Tipo do link spanning-tree
- Spanning-tree portfast edgeport
- Spanning-tree BPDU - filterind | flooding
- Spanning-tree trap

ACL - CONTROLE DE ACESSO

- ACL padrão
- ACL estendida
- Configurando ACL padrão
- Configurando ACL estendida
- Vinculando ACL a uma interface - commit
- ACL padrão IPv6
- ACL IPv6 estendida
- Configurando ACL padrão IPv6
- Configurando ACL IPv6 estendida
- Vinculando ACL IPv6 a uma interface - commit
- ACL baseada no MAC
- Configurando ACL baseada em MAC
- Vinculando ACL baseada em MAC a uma interface - commit

- Show ACL

IGMP SNOOPING

- Ativar IGMP snooping
- Versão IGMP snooping
- IGMP snooping com VLAN
- IGMP snooping fast-leave
- IGMP snooping suppression
- IGMP snooping unknow-multicast action
- IGMP snooping VLAN mrouter learn
- IGMP snooping VLAN static
- IGMP snooping VLAN querier
- Snooping VLAN querier version
- IGMP snooping VLAN querier last-member-query-count
- IGMP snooping VLAN querier last-member-query-interval
- IGMP snooping VLAN querier max-response-time
- IGMP snooping VLAN querier query-interval
- IGMP snooping VLAN robustness-variable
- IGMP profile
- Clear statistics IGMP snooping
- IGMP snooping groups
- Lista de comandos show IGMP snooping

CONFIGURAÇÕES DE SISTEMA

- Show interfaces
- Gerenciamento IPv6
- Show IPv6
- Telnet
- Exportar Log
- Reiniciar - restart

- Criação e alteração de usuário web
- Criação ou alteração de usuário CLI
- Log do sistema
- Tabela ARP
- Informação de memória flash
- Informação do CPU
- Informação de memória
- Informação de versão
- informações de configurações
- Salvar configurações
- Restaurar padrão de fábrica
- Configuração de MAC estático
- Configuração de bloqueio de MAC - drop
- Tempo de envelhecimento da tabela MAC - aging time
- Contagem de endereços MAC
- Informações gerais de MAC address
- Uploading de configuração
- Firmware update
- Download de configuração
- MTU

SERVIDOR SNTP

- Sicronizar com servidor SNTP

CONFIGURAÇÃO SNMP

- Habilitar SNMP
- Habilitar SNMP Trap
- Comunidade SNMP
- SNMP host server
- SNMP trap auth

EXPORTAR PARA PDF

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

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

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

PROTEÇÃO E SEGURANÇA DE DADOS

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

Tratamento de dados pessoais

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

Diretrizes que se aplicam aos funcionários da Intelbras

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

Diretrizes que controlam o tratamento de dados

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

Uso indevido e invasão de hackers

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

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

ACESSO A INTERFACE DE GERENCIAMENTO

Login

Para acessar a interface de gerenciamento do switch, abra o navegador e na barra de endereços digite o endereço IP 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 do seu computador deve estar definido na mesma sub-rede utilizada pelo switch. O endereço IP de seu computador deve estar configurado como: 192.168.0.x, onde x é qualquer número de 2 a 254 e máscara de rede igual a 255.255.255.0.

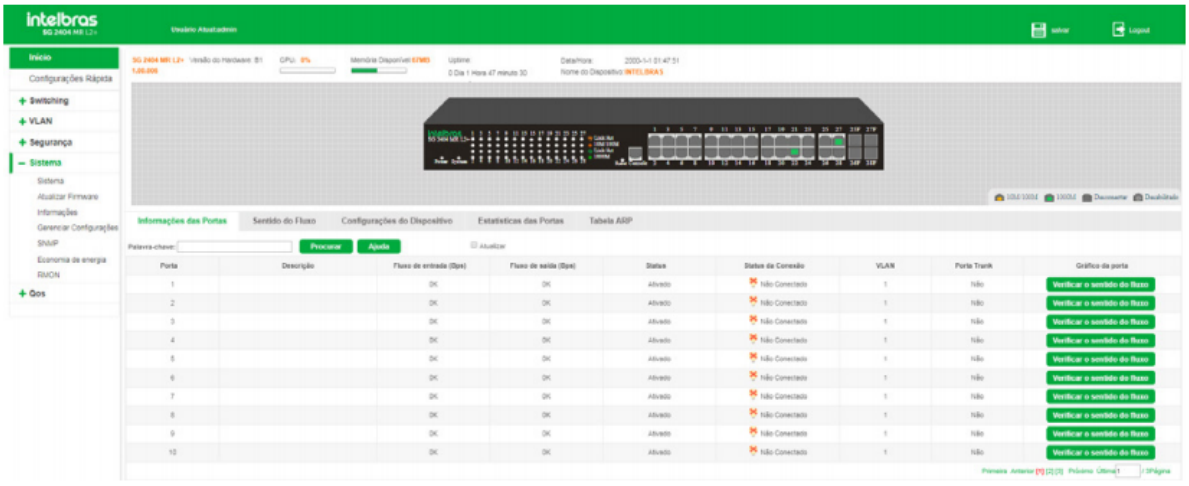
Após digitado o endereço IP do switch no navegador, será exibida a tela de login, conforme imagem a seguir. Digite admin para o nome de usuário e senha, ambos em letras minúsculas, em seguida, clique no botão Login ou pressione a tecla Enter.

INÍCIO

Após o login no equipamento, será exibida a tela a seguir, onde pode ser verificada a imagem do switch com a quantidade de portas disponíveis no produto, quais destas portas estão com link ativo, as portas que estão desabilitadas ou desconectadas.

Na parte superior da tela é possível verificar informações a respeito do nome do modelo e a versão do firmware e hardware do equipamento, informações sobre o uso da CPU, a memória RAM (total, usada e disponível), a quantidade de memória flash (total, usada e disponível), a data e a hora configurada no equipamento e a informação do nome do dispositivo.

Nesta tela também é possível ter acesso rápido ao tráfego de dados e o sentido do fluxo em cada porta, a descrição de cada porta, a VLAN configurada em cada porta e se a porta está configurada como Trunk.

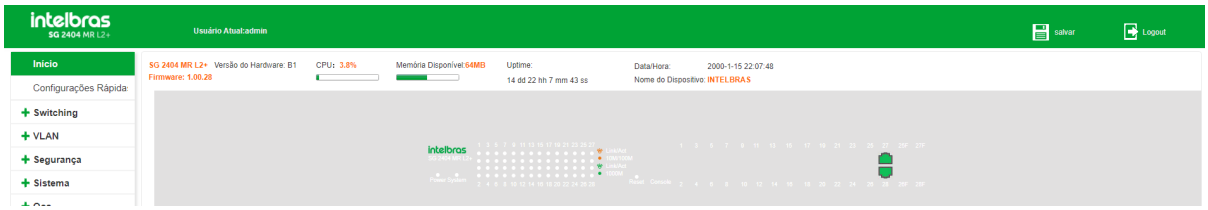


A imagem a seguir mostra o modelo do equipamento, a versão do firmware e hardware, uso de CPU, memórias, data e nome.

Para verificar os dados de uso da CPU, da memória RAM e memória flash deve-se posicionar o cursor do mouse sobre a informação desejada.

Pode-se verificar as informações básicas da porta posicionado o cursor do mouse sobre a porta desejada.

Abaixo segue imagem da tela com as informações que serão apresentadas relacionadas a porta 2, por exemplo.



Nesta tela é possível ter acesso ao caminho para verificar o fluxo de dados da porta, a descrição e os fluxos de entrada e saída além de habilitar ou desabilitar a porta.

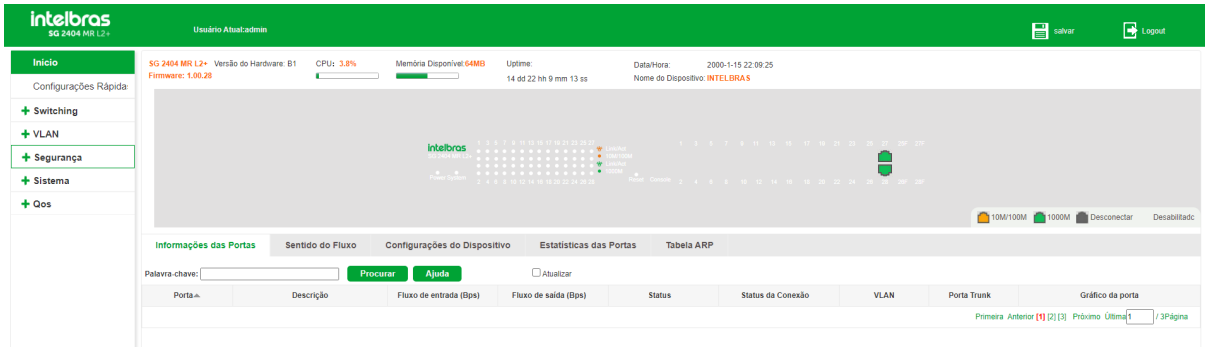
Para habilitar ou desabilitar a porta deve-se verificar a informação Status da porta. Se estiver marcada a opção Aberto a porta estará habilitada, se estiver marcada a opção Fechado a porta estará desabilitada.

Nesta mesma tela é apresentada a informação sobre a presença ou não de link em cada porta.

A legenda a seguir indica a situação de cada porta:

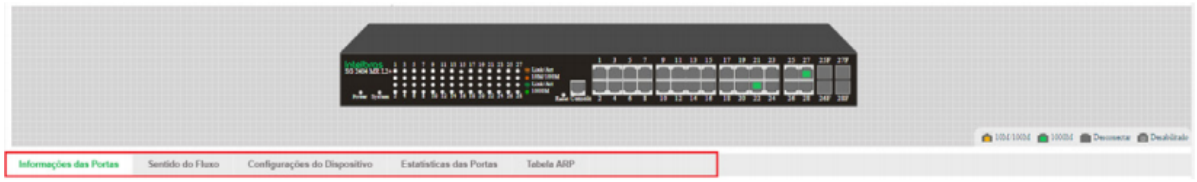
Informações das portas

Para informações sobre a situação de cada porta e suas configurações básicas escolha o menu Início > Informações das portas para mostrar tais informações:



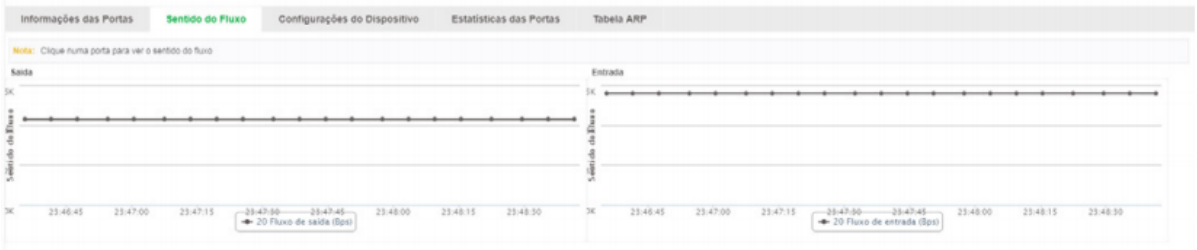
A seguir segue descritivo dos campos exibidos na tela Informações das portas:

- **Porta:** exibe o número da porta.
- **Descrição:** exibe a descrição da porta.
- **Fluxo de entrada (Bps):** exibe o fluxo de dados de entrada na porta em Bps.
- **Fluxo de saída (Bps):** exibe o fluxo de dados de saída na porta em Bps.
- **Status:** indica o status da porta (Ativado/Desativado).
- **VLAN:** exibe a configuração da VLAN nativa da porta.
- **Porta Trunk:** exibe a informação se a porta é Trunk ou não.
- **Editar:** clicando no botão Verificar o sentido do fluxo será aberta a tela com as informações em formato de gráfico do fluxo de dados da porta selecionada.



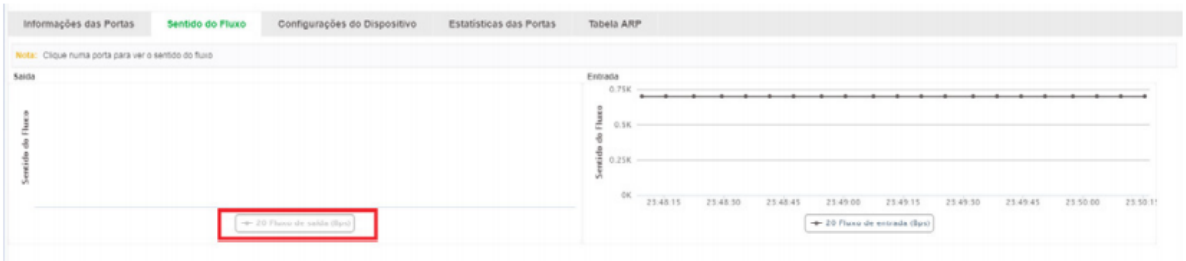
Sentido do fluxo

Acessando a tela Início > Sentido do fluxo é possível verificar o gráfico do fluxo de dados de entrada e saída de cada porta:



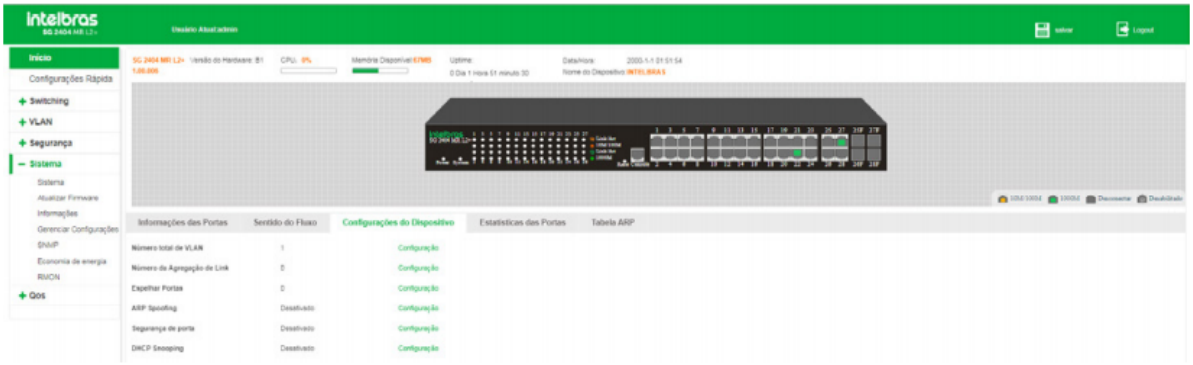
Clicando no botão Gi 0/5 Fluxo de saída (Bps) ou Gi 0/5 Fluxo de entrada (Bps) é possível desabilitar o gráfico nesta tela.

Para habilitar o gráfico, basta clicar no botão novamente.



Configurações do dispositivo

A tela Início > Configurações do dispositivo traz atalhos para diversas telas de configuração do equipamento e informações destas configurações.



Segue descritivo dos campos exibidos na tela Configurações da portas:

- **Número total de VLAN:** exibe o número de VLANs criadas.
- **Número de Agregação de Link:** exibe o número de configurações de agregação de link (ID de agregação).
- **Espelhar Portas:** exibe a quantidade de grupos de espelhamento de portas.
- **ARP Spoofing:** informa o status da função Inspeção ARP e oferece atalho para esta configuração em Segurança > Prevenção de ataque > Inspeção ARP.
- **Segurança de porta:** informa o status da função Segurança de porta e oferece atalho para esta configuração em Segurança > Prevenção de ataque > Segurança de porta.
- **DHCP Snooping:** informa o status da função DHCP snooping e oferece atalho para esta configuração em Segurança > Prevenção de ataque > DHCP snooping.

Estatísticas das portas

A tela Início > Estatísticas das portas mostra informações sobre as estatísticas para as portas.

Tabela ARP

Nesta página você pode visualizar as informações referentes a Tabela ARP. Escolha o menu Tabela ARP para carregar a seguinte página:

Protocolo ARP

O protocolo ARP (*Address Resolution Protocol*) é utilizado para analisar e mapear os endereços IP com seus respectivos endereços MAC, possibilitando assim a entrega dos pacotes aos seus destinos corretamente. Desta forma, o endereço IP de destino contido em um pacote precisa ser traduzido para o endereço MAC correspondente, formando assim a Tabela ARP. Quando um computador se comunica com outro, o protocolo ARP funciona conforme imagem e explicação a seguir:

- Suponha que há dois computadores pertencentes à mesma rede: computador A e o computador B. Para que o computador A possa enviar pacotes para o computador B, o computador A verifica se em sua tabela ARP há o relacionamento entre o endereço IP e o endereço MAC do computador B, caso possua, o pacote será transmitido diretamente ao computador B, caso não possua, o computador A transmitirá solicitações ARP em broadcast para a rede.
- Quando um pacote de solicitação ARP é transmitido em broadcast, todos os computadores pertencentes à mesma rede de visualização este pacote, no entanto, apenas o computador B responderá ao pedido, pois o endereço IP contido na solicitação ARP corresponderá com seu próprio endereço IP. Então o computador B enviará ao computador A um pacote de resposta contendo seu endereço MAC.
- Ao receber o pacote de resposta ARP, o computador A adiciona o endereço IP e o endereço MAC do computador B em sua tabela ARP, para que os próximos pacotes com destino ao computador B sejam encaminhados diretamente ao destino correto.

CONFIGURAÇÕES RÁPIDAS

A função Configurações rápidas permite configurar de forma rápida algumas das funcionalidades mais comuns do switch, como VLANs, modo das portas, SNMP, opções de gerenciamento, entre outros.

Configurar VLAN

A página Configurar VLAN permite adicionar novas VLANs, modificar VLANs existentes, apagar VLANs, etc. Configure de acordo com sua necessidade e clique em Próximo para continuar.

Escolha o menu Configurações rápidas > Configurar VLAN para carregar a seguinte página:

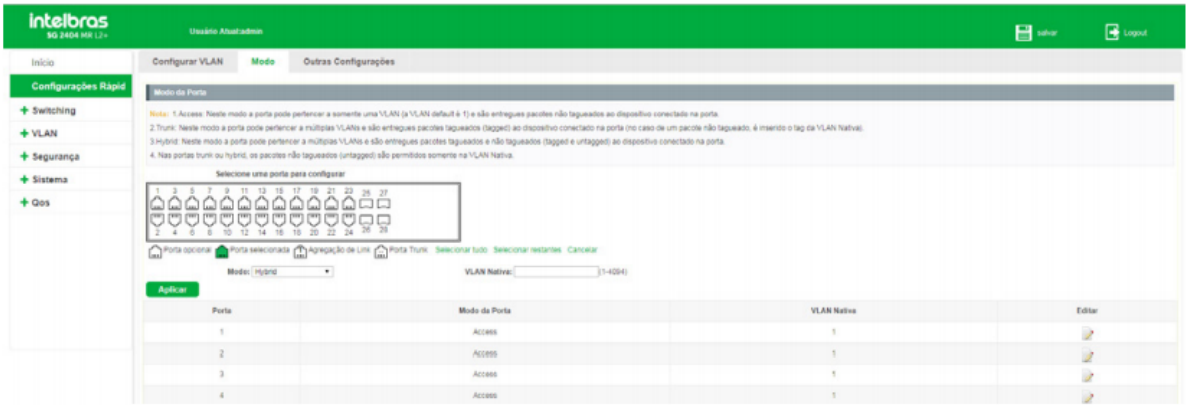
Obs: para mais informações sobre a configuração de VLAN no equipamento, verifique o item 5. VLAN deste manual.

Modo

A configuração de modo permite configurar o modo de operação das portas do switch como *Access, Trunk e Hybrid*. Observe a descrição de cada modo de porta:

- **Access:** neste modo a porta pode pertencer a somente uma VLAN (a VLAN padrão é 1) e são entregues pacotes não tagueados ao dispositivo conectado na porta.
- **Trunk:** neste modo a porta pode pertencer a múltiplas VLANs e são entregues pacotes tagueados (*tagged*) ao dispositivo conectado na porta (no caso de um pacote não tagueado, é inserido tag da VLAN nativa).
- **Hybrid:** neste modo a porta pode pertencer a múltiplas VLANs e são entregues pacotes tagueados e não tagueados (*tagged e untagged*) ao dispositivo conectado na porta.

Escolha o menu Configurações rápidas > Modo para carregar a seguinte página:



Após finalizar suas configurações, clique em Próximo para continuar ou Anterior para retornar

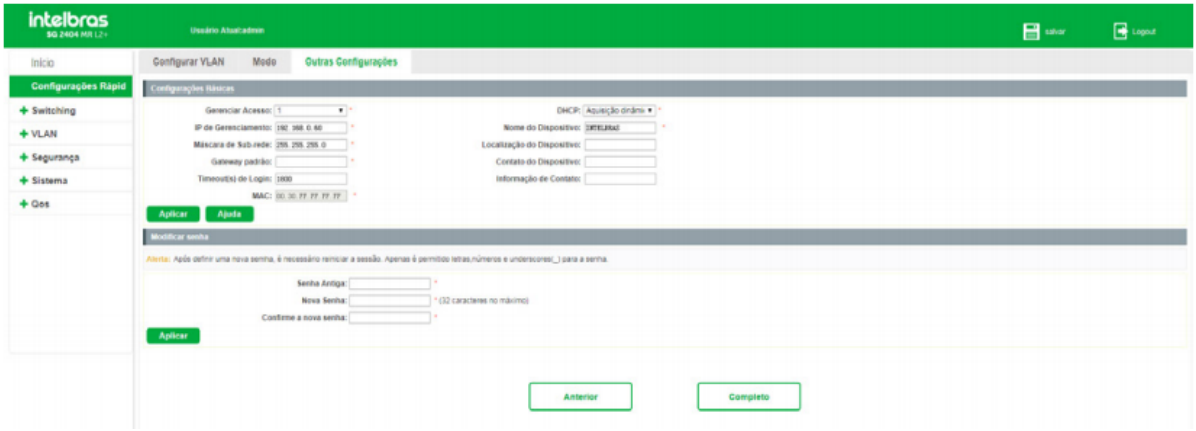
Observações:

- Nas portas Trunk ou Hybrid, os pacotes não tagueados (*untagged*) são permitidos somente na VLAN nativa.
- Para mais informações sobre o modo de operação das portas do equipamento, verifique o item Modo deste manual.

Outras configurações

Esta página permite alterar configurações como, VLAN de gerência, IP de gerenciamento, nome do dispositivo, localização, entre outros. Após fazer as configurações desejadas, clique em Completo para finalizar.

Escolha o menu Configurações rápidas > Outras configurações para carregar a seguinte página:



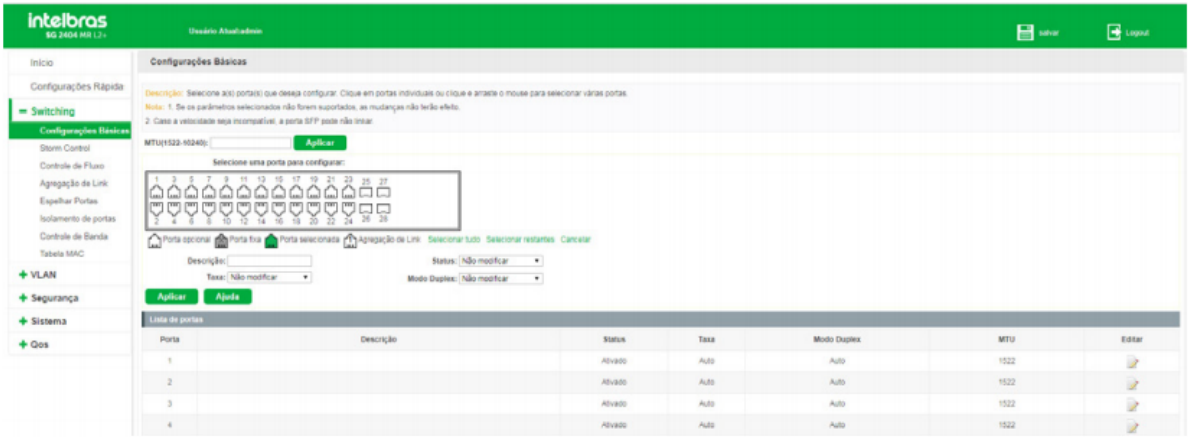
SWITCHING

O menu Switching permite ao administrador do sistema efetuar configurações nas portas do switch através dos seguintes menus: *Configurações básicas, Storm control, Controle de fluxo, Agregação de link, Espelhar portas, Isolamento de portas e Controle de banda*.

Configurações básicas

O submenu Configurações básicas dá acesso às configurações de status das portas, descrição, taxa de transmissão, MTU, entre outros.

Escolha o menu Switching >Configurações básicas para carregar a seguinte página:



A seguir apresentamos o descritivo dos campos exibidos na Lista de portas.

- **Porta:**exibe o número da porta.
- **Descrição:**exibe a descrição da porta.
- **Status:**indica o status da porta (Ativado/Desativado).
- **Taxa:**exibe a configuração de velocidade da porta (10/100/1000/Auto).
- **ModoDuplex:**exibe a configuração Duplex da porta (Full/Half/Auto).
- **MTU:**informa o tamanho máximo de pacote que a porta pode transferir (*MTU – Maximum Transmission Unit*).

Para alterar as configurações das portas siga as seguintes instruções:

1. Clique no ícone (EDITAR) da porta que deseja configurar ou selecione através do painel de portas (é possível selecionar mais de uma porta para configuração no painel);
2. Efetue as configurações desejadas;
3. Salve as configurações.

Para configurar o MTU das portas, entre com o valor desejado no campo MTU(1522-10240) e clique em Aplicar.

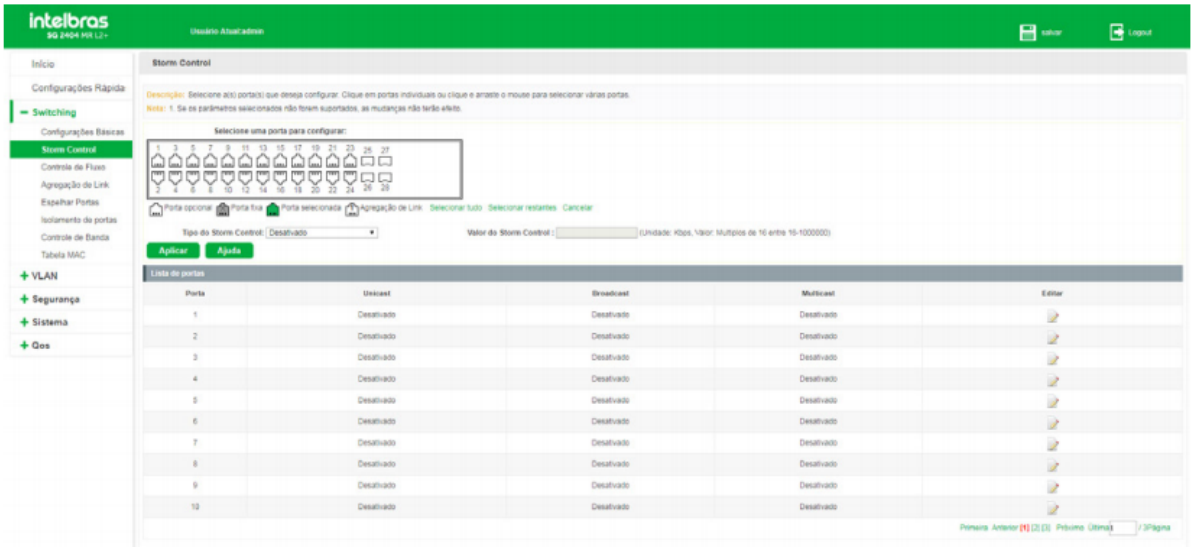
Observações

- A configuração de MTU é geral, ou seja, todas as portas receberão o valor de MTU configurado.
- É possível configurar mais de uma porta por vez. Neste caso selecione as portas diretamente no painel indicado na imagem acima.

Storm control

A função Storm control permite que o switch filtre por porta os pacotes do tipo unicast que não possuam um endereço IP definido, além de pacotes broadcast e multicast. Se a taxa de transmissão de algum destes três tipos de pacotes excederem a largura de banda configurada, os pacotes serão rejeitados automaticamente pelo switch, evitando assim uma tempestade de broadcast na rede.

Escolha o menu Switching > Storm control para carregar a seguinte página:



A seguir segue descritivo dos campos exibidos na Lista de portas:

- **Porta:**exibe o número da porta.

- **Unicast:**exibe a largura de banda configurada para receber pacotes unicast que não possuam um endereço IP definido na porta. O tráfego de pacotes superior a largura de banda configurada será descartado. Caso a função esteja desativada na porta, será exibido Desativado.
- **Broadcast:**exibe a largura de banda configurada para receber pacotes broadcast na porta. O tráfego de pacotes superior a largura de banda configurada será descartado. Caso a função esteja desativada na porta, será exibido Desativado.
- **Multicast:**exibe a largura de banda configurada para receber pacotes multicast na porta. O tráfego de pacotes superior a largura de banda configurada será descartado. Caso a função esteja desativada na porta, será exibido Desativado.

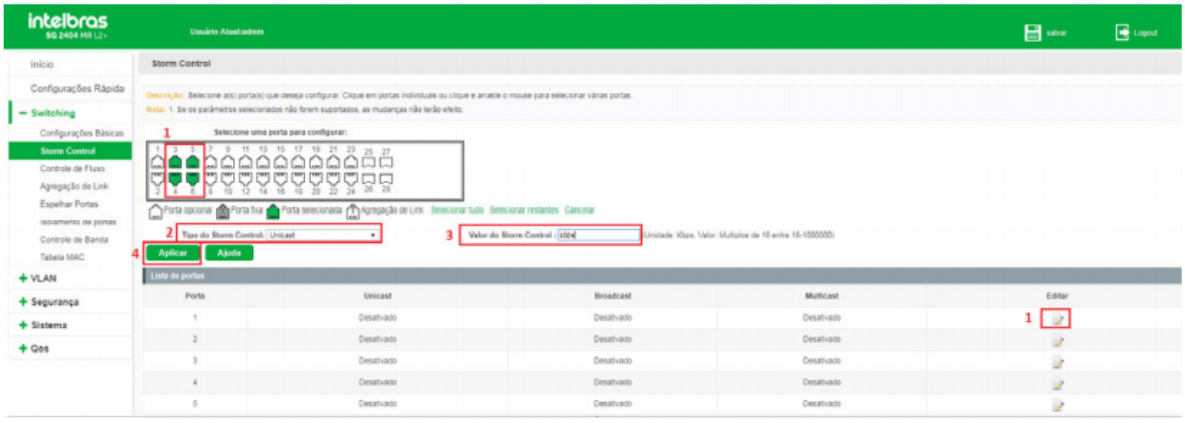
Observações

- Somente são permitidos valores múltiplos de 16 na configuração da largura de banda do Storm control. Caso utilize um valor não múltiplo de 16, o sistema irá arredondar automaticamente para valor múltiplo de 16 mais próximo.
- É permitido configurar somente um valor de largura de banda para unicast, broadcast e multicast em cada porta.

Para configurar o Storm control, siga o procedimento:

1. Clique no ícone (EDITAR) da porta que deseja configurar ou selecione através do painel de portas (é possível selecionar mais de uma porta para configuração no painel);
2. Selecione o tipo do Storm control;
3. Configure a largura de banda máxima;
4. Clique em Aplicar.

No exemplo a seguir iremos configurar as portas 3, 4, 5 e 6 com Storm control do tipo unicast e largura de banda de 1024 kbps.

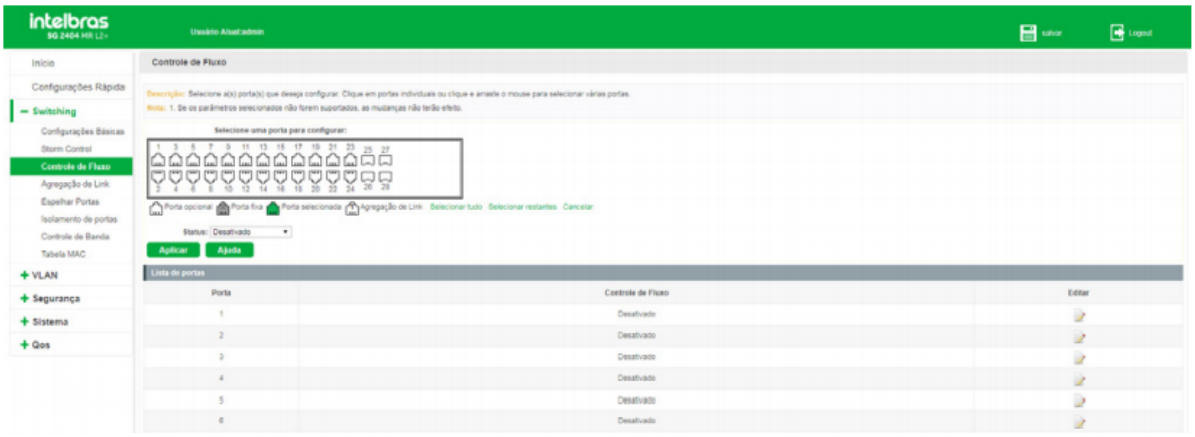


Após salvar as configurações, neste caso, a lista de portas aparecerá desta forma:

Controle de fluxo

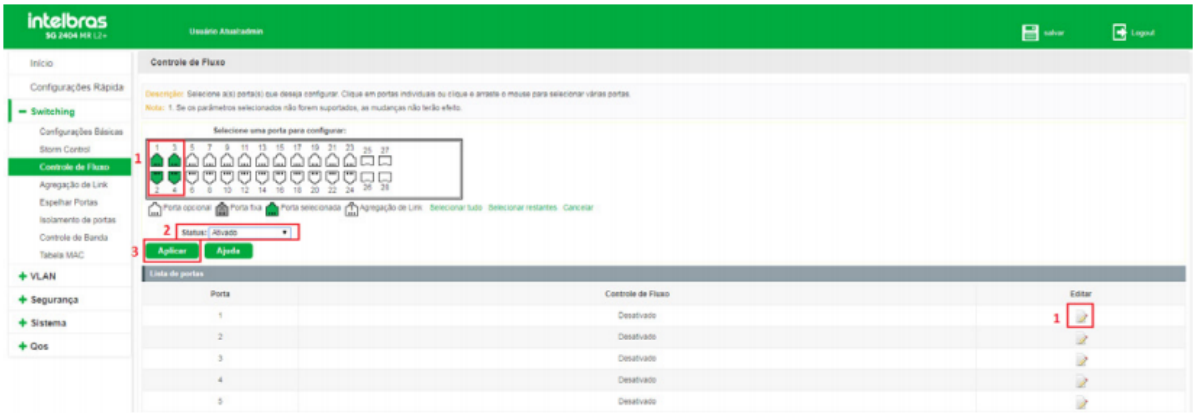
O controle de fluxo, quando ativado, permite ao switch sincronizar a transmissão de dados nas portas, evitando a perda de pacotes causada por congestionamentos na rede.

Escolha o menu Switching >Controle de fluxo para carregar a seguinte página:



Para habilitar/desabilitar a função Controle de fluxo nas portas do switch, siga as seguintes orientações:

1. Clique no ícone (EDITAR) da porta que deseja configurar ou selecione através do painel de portas (é possível selecionar mais de uma porta para configuração no painel);
2. Selecione o tipo do Controle de fluxo (Ativado/Desativado);
3. Clique em Aplicar.



Agregação de link

A função Agregação de link permite a utilização de múltiplas portas para permitir o aumento da velocidade do link para além dos limites nominais de uma única porta. Esta funcionalidade introduz controle de falhas e redundância para a conexão a outro dispositivo que disponha do mesmo recurso. As portas pertencentes a um grupo de agregação devem

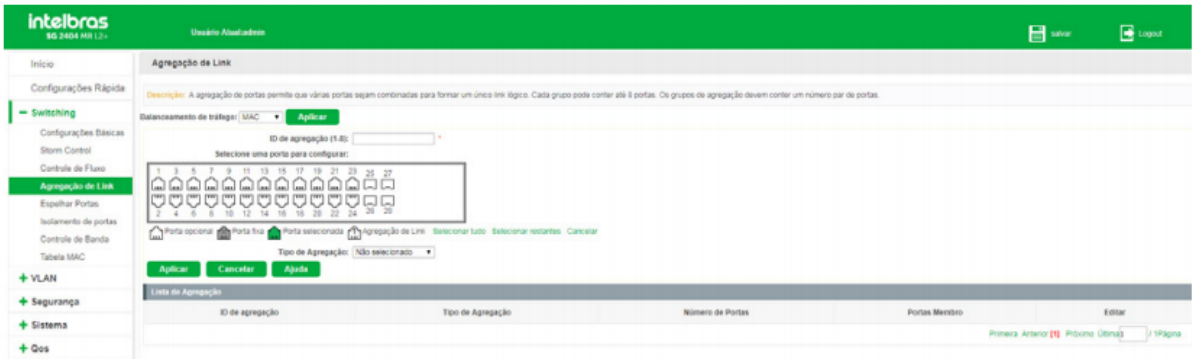
possuir os mesmos parâmetros de configuração, caso utilizadas as seguintes funções: *STP, QoS, VLAN, MAC Address Learning*. Seguem as explicações.

- Portas que estiverem habilitadas as funções 802.1q VLAN, Voice VLAN, STP, QoS, DHCP Snooping e Port Configuration (Speed e Duplex, Flow control) e que participam de um mesmo grupo LAG, deverão obrigatoriamente possuir as mesmas configurações.
- Portas que estiverem configuradas com as funções *Port security, Port mirror, MAC address filtering, Static MAC address binding e 802.1x*, não poderão ser adicionadas a um grupo LAG.
- Não é recomendado adicionar portas a um grupo LAG que esteja habilitado com as funções ARP inspection e DoS defend.
- É recomendável configurar primeiramente os grupos de agregação antes de configurar as demais funções.

Observações:

- Como calcular a largura de banda em uma agregação de link: suponhamos que um grupo LAG possua quatro portas com velocidade de 1000 Mbps full duplex, a largura de banda total do grupo LAG é de 8000 Mbps (2000 Mbps × 4) isto porque a largura de banda de cada porta é de 2000 Mbps, sendo 1000 Mbps de uplink e 1000 Mbps de downlink.
- O balanceamento de carga entre as portas pertencentes a um grupo LAG será de acordo com o algoritmo de balanceamento configurado. Se a conexão de uma porta estiver com perdas de pacotes, o tráfego será transmitido pelas portas que estejam normais. De modo a garantir a confiabilidade da conexão.

Escolha o menu Switching > Agregação de link para carregar a seguinte página:



A seguir segue descritivo das informações contidas na página de agregação de link:

- **ID de agregação:**exibe o ID da agregação de link.
- **Balanceamento de tráfego:**exibe a política utilizada para balanceamento do tráfego nos links da agregação.
- **Tipo de agregação:**informa o tipo de agregação (Dinâmico/Estático).
- **Número de portas:**informa a quantidade de portas que a agregação possui.
- **Porta membro:**informa as portas que pertencem a agregação.

Observações:

- Cada grupo de agregação pode conter até 8 portas associadas.
- As configurações de velocidade da porta, modo Duplex ou estado da porta não poderão ser alterados após a configuração da agregação de link.

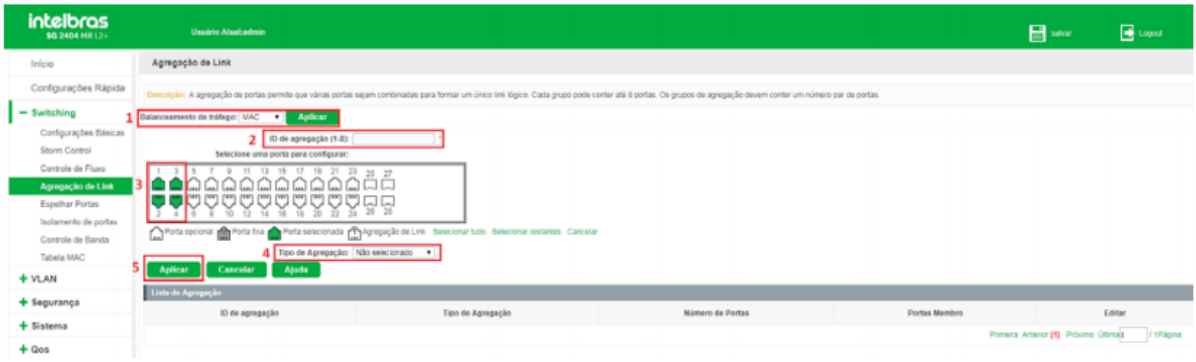
Adicionando agregação de link

Observe as instruções a seguir para adicionar uma agregação de link:

1. Escolha o tipo do balanceamento de tráfego e clique em Aplicar;

   Obs:essa configuração é geral e todas as agregações de link irão utilizar a mesma política.

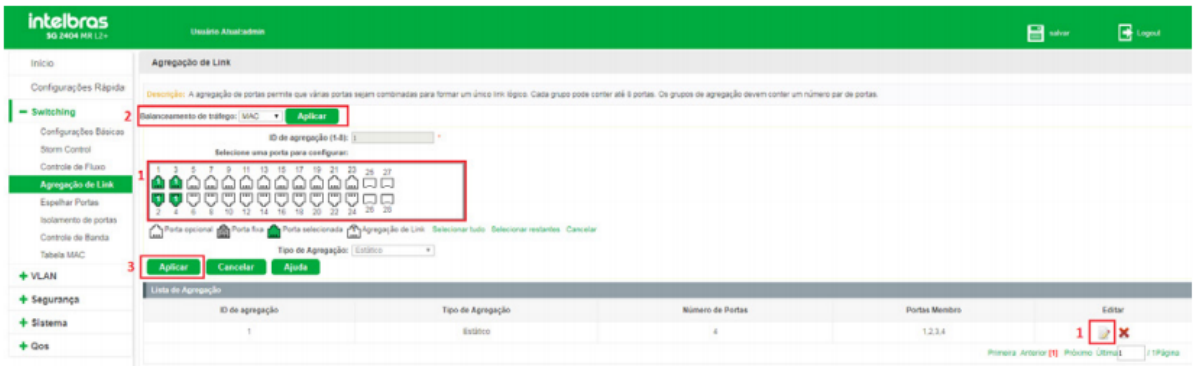
2. Insira o ID da agregação de link;
3. Selecione as portas que irão pertencer a agregação no painel de portas;
4. Selecione o tipo de agregação (Dinâmica/Estática);
5. Clique em Aplicar.



Modificando agregação de link

Caso queira modificar uma agregação de link, siga as instruções a seguir:

1. Clique no ícone (EDITAR) da agregação que deseja editar;
2. Observe que as portas pertencentes à agregação serão selecionadas no painel de portas;
3. Efetue as alterações desejadas;
4. Clique em Salvar.

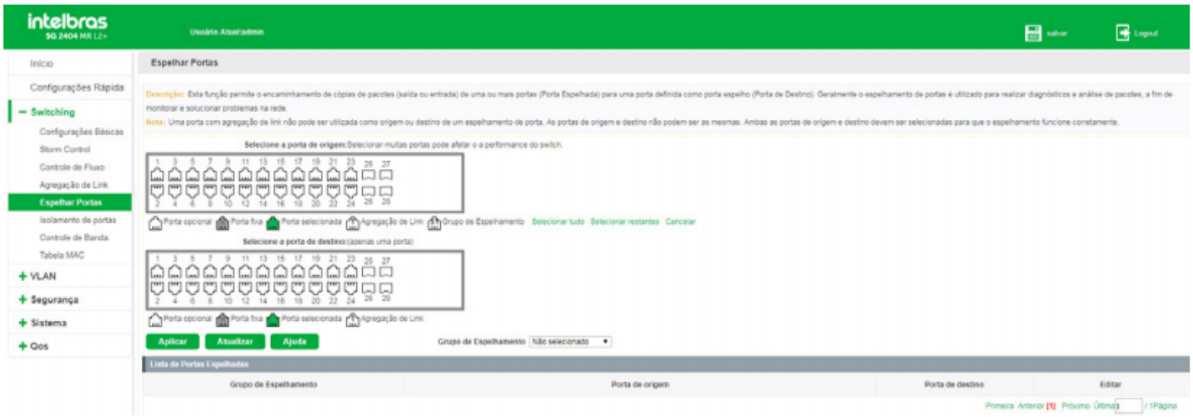


Espelhar portas

Nesta página é possível configurar o espelhamento de portas. Esta função permite o encaminhamento de cópias de pacotes de uma ou mais portas (portas origem) para uma porta definida como porta espelho (porta destino). Geralmente o espelhamento de portas é utilizado para realizar diagnósticos e análise de pacotes, a fim de monitorar e solucionar

problemas na rede.

Escolha o menu Switching > Espelhar portas para carregar a seguinte página:



A seguir segue descritivo das informações contidas na página de espelhamento de portas:

- **Grupo de espelhamento:**exibe o ID do grupo de espelhamento. São permitidos até 4 grupos.
- **Porta de origem:**exibe a(s) porta(s) de origem do grupo de espelhamento. As portas de origem terão seus pacotes espelhados para a porta de destino.
- **Porta de destino:**exibe a porta de destino do grupo de espelhamento. A porta de destino irá receber os pacotes espelhados das portas de origem.

Observações:

- Não é possível utilizar uma agregação de link como porta origem ou porta destino.
- Porta origem e porta destino não podem ser a mesma.
- Só é permitida uma porta destino por grupo de espelhamento.

'

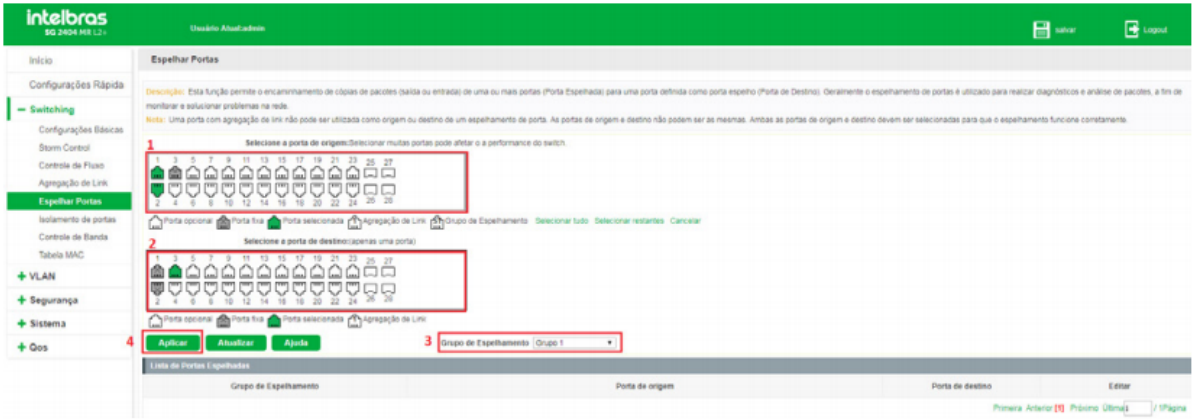
'

Adicionando grupo de espelhamento

Observe as instruções a seguir para adicionar um grupo de espelhamento de portas.

1. Selecione a(s) porta(s) de origem no painel de portas;
2. Selecione a porta de destino no painel de portas;
3. Selecione o grupo de espelhamento;
4. Clique em Aplicar.

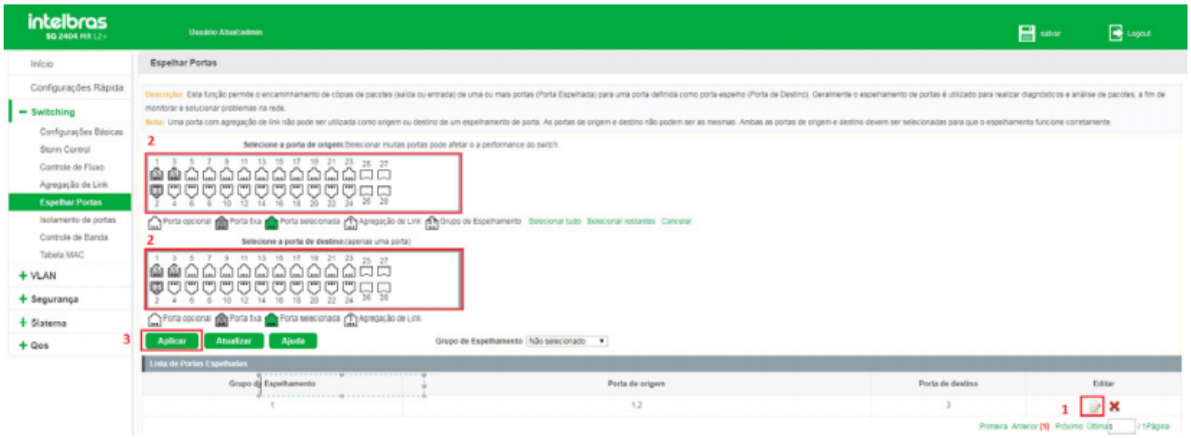
Na imagem a seguir estão sendo configuradas as portas 1 e 2 como origem, e porta 3 como destino, no grupo de espelhamento 1.



Modificando grupo de espelhamento

Para modificar um grupo de espelhamento siga as instruções a seguir:

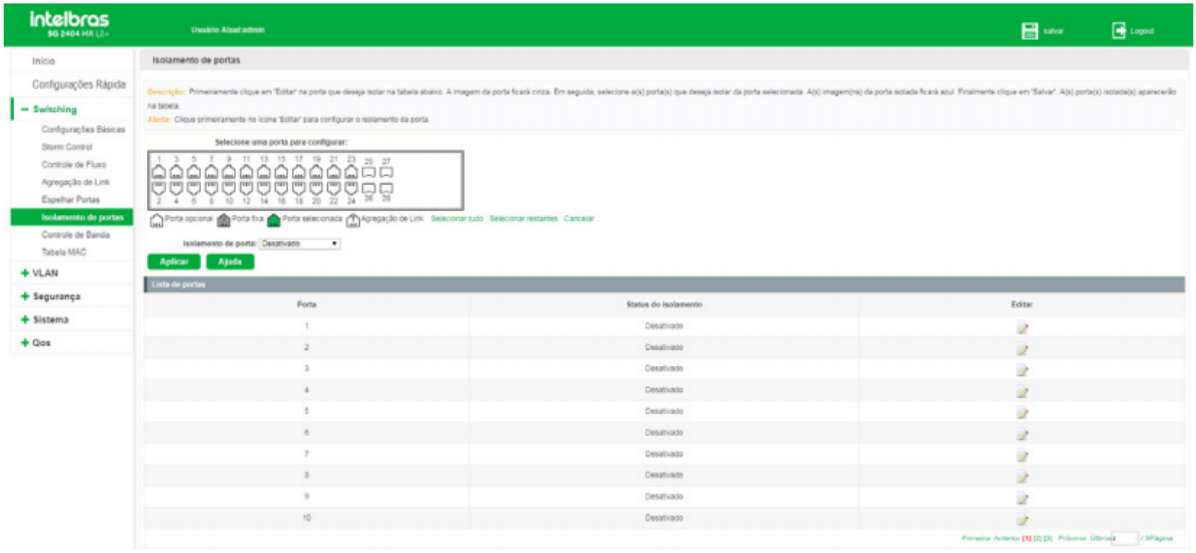
1. Clique no ícone (EDITAR) do espelhamento que deseja alterar;
2. Adicione ou remova as portas nos painéis de portas;
3. Para remover uma porta, basta clicar sobre a mesma no painel de portas;
4. Salve as alterações através do botão Aplicar.



Isolamento de portas

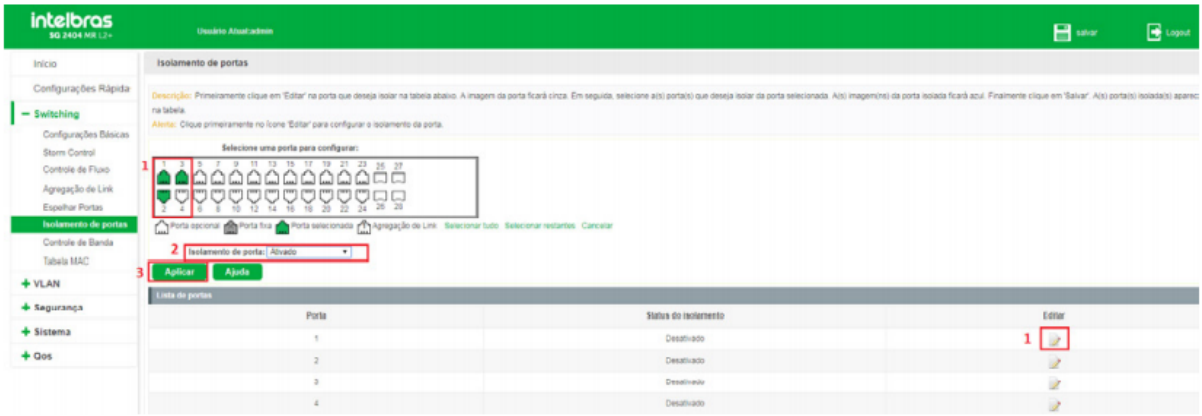
O Isolamento de portas fornece um método para restringir o fluxo do tráfego para melhorar a segurança da rede. Esta função permite o isolamento do tráfego entre as portas que estiverem com o isolamento ativado.

Escolha o menu Switching > Isolamento de portas para carregar a seguinte página:



A função Isolamento de portas restringe o tráfego entre as portas que estiverem com esta função ativada, ou seja, as portas que estiverem com status Ativado não se comunicarão entre si. Por outro lado, poderão se comunicar com todas as demais portas que estiverem com status Desativado. Para ativar o isolamento de portas, siga as orientações a seguir:

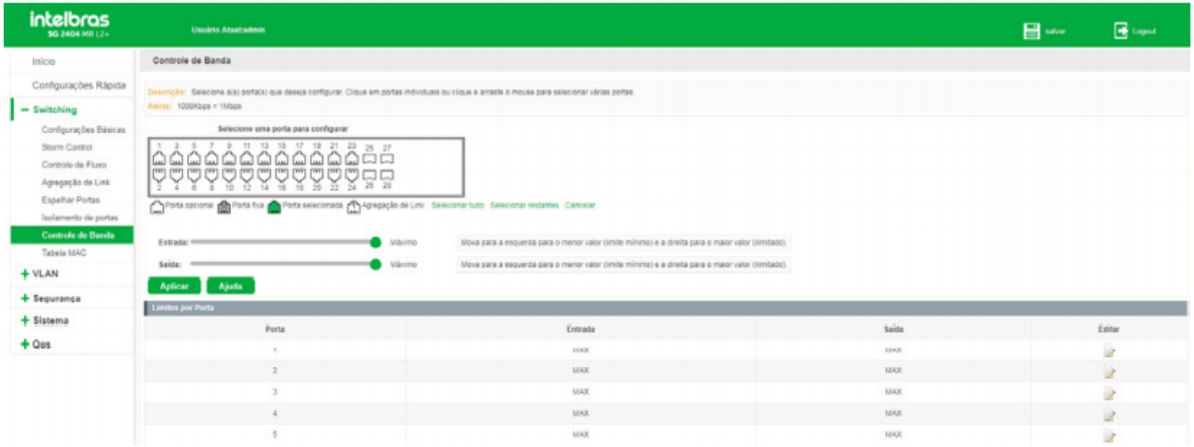
1. Clique no ícone (EDITAR) da porta que deseja configurar ou selecione através do painel de portas (é possível selecionar mais de uma porta para configuração no painel);
2. Selecione o tipo de isolamento de porta (Ativado/Desativado);
3. Clique em Aplicar.



Controle de banda

A função Controle de banda permite ao administrador do sistema controlar a largura de banda e o fluxo de transmissão de cada porta. Através desta funcionalidade é possível restringir o uso de recursos da rede, visando otimizar a transferência e encaminhamento de dados.

Escolha o menu Switching > Controle de banda para carregar a seguinte página:



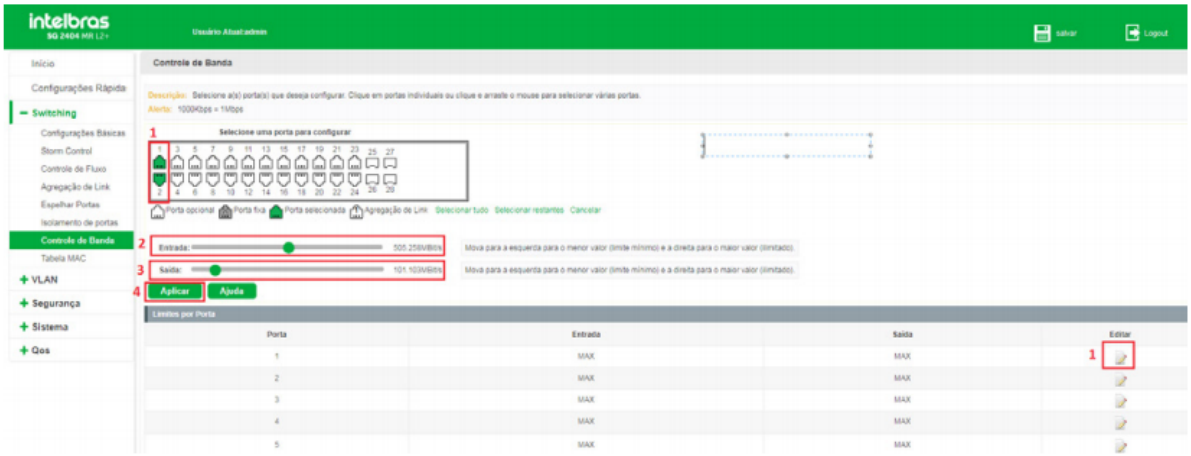
A seguir apresentamos o descritivo dos campos exibidos na Lista de portas.

- **Porta:**exibe o número da porta.
- **Entrada:**exibe o limite de largura de banda para o tráfego de entrada da porta.
- **Saída:**exibe o limite de largura de banda para o tráfego de saída da porta.

Configurando controle de banda

Observe as instruções a seguir para configurar o controle de banda:

1. Clique no ícone (EDITAR) da porta que deseja configurar ou selecione através do painel de portas (é possível selecionar mais de uma porta para configuração no painel);
2. Configure o limite da largura de banda do tráfego de entrada;
3. Configure o limite da largura de banda do tráfego de saída;
4. Clique em Aplicar.



Removendo controle de banda

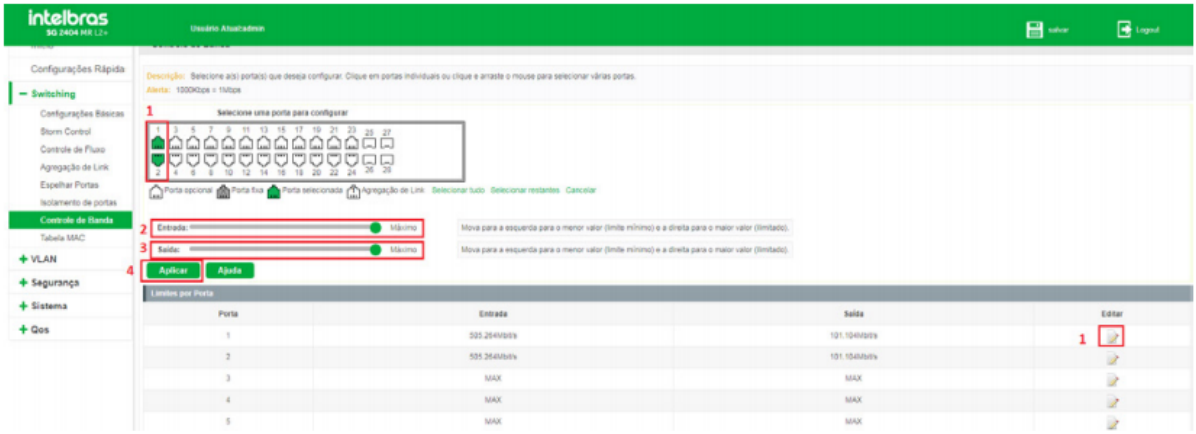
Para remover o controle de banda de uma ou mais portas, siga as orientações a seguir:

1. Clique no ícone (EDITAR) da porta que deseja configurar ou selecione através do painel de portas (é possível selecionar mais de uma porta para configuração no painel);
2. Configure o limite da largura de banda do tráfego de entrada para o valor máximo;
3. Configure o limite da largura de banda do tráfego de saída para o valor máximo;

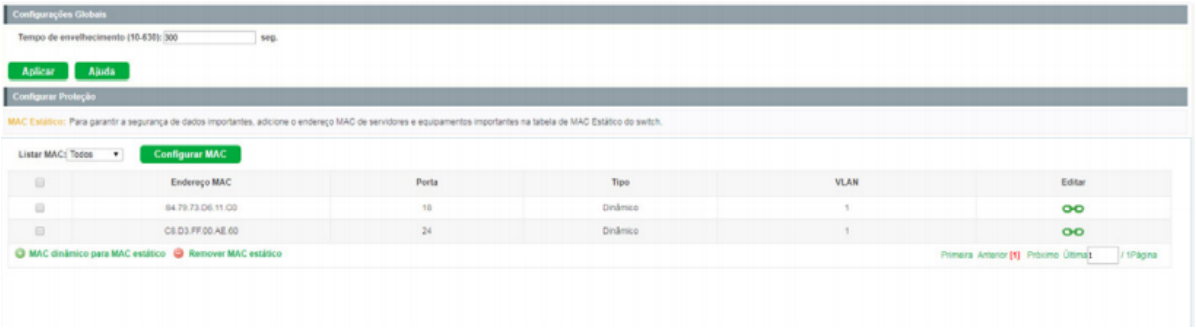
4. Clique em Aplicar.

Tabela MAC

A seguinte tela se encontra no menu Sistema > Sistema > Gerenciar MAC.



MAC dinâmico



As entradas de endereços MAC realizadas de forma dinâmica são geradas pelo mecanismo de autoaprendizagem do switch, através deste recurso e juntamente com o Aging Time (tempo de envelhecimento) é que se torna possível a manutenção da Tabela de endereços MAC. O Aging time faz com que o switch remova cada entrada da Tabela de endereços MAC dentro de um determinado período de tempo (tempo de envelhecimento) em que a entrada permanecer ociosa dentro da Tabela de endereços MAC. Nesta página você pode configurar os endereços MAC dinâmico.

Quando um equipamento de rede é conectado a uma das portas do switch, este aprende o endereço MAC do dispositivo e cria uma associação entre o endereço MAC e o número da porta, criando uma entrada na tabela de encaminhamento (Tabela de endereços MAC). Esta tabela é a base para que o switch possa encaminhar os pacotes rapidamente, entre o ende- reço de origem e destino, diminuindo o tráfego em broadcast. Os endereços MAC são adicionados na tabela de endereços de forma dinâmica (autoaprendizagem) ou configurados manualmente. Existem recursos de filtragem de endereços MAC, permitindo que o switch filtre pacotes indesejados, proibindo seu encaminhamento e melhorando a segurança da rede.

Características da tabela de endereços MAC

Modo de entrada dos endereços na Tabela de endereços MAC	Modo de configuração	As entradas da Tabela de endereço MAC possuem Aging Time	A Tabela de endereços MAC é mantida após reiniciar o switch (se a configuração for salva)	Relação entre o endereço MAC e a porta do switch
Endereços estáticos	Configuração manua	Não	Sim	O endereço MAC aprendido por uma porta não pode ser aprendido por outra porta em uma mesma VLAN.
Endereços dinâmicos	Aprendizado automático	Sim	Não	O endereço MAC aprendido por uma porta pode ser aprendido por outra porta em uma mesma VLAN.
Filtro MAC	Configuração manua	Não	Sim	-

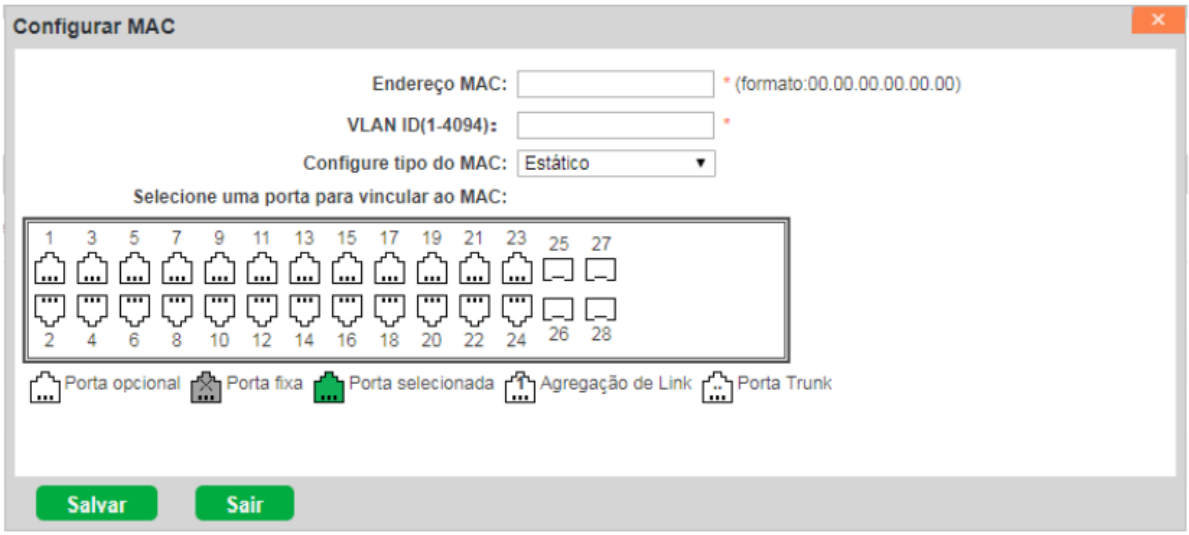
MAC estático

Nesta página é possível configurar entradas estáticas na Tabela de endereços MAC. As entradas estáticas somente podem ser adicionadas ou removidas manualmente, independentemente do Aging Time (tempo de envelhecimento). Em redes estáveis, as entradas de endereços MAC estático podem aumentar consideravelmente o desempenho de encaminhamento de pacotes do switch.

Configurando MAC estático

Para configurar MAC estático de um dispositivo que ainda não foi detectado pelo switch clique em Configurar MAC.

Será apresentada a seguinte tela:



- **Endereço MAC:**digite o MAC que você deseja vincular como MAC estático ou DROP**.**
- **VLAN ID (1-4094):**digite a VLAN.

- **Configure tipo do MAC:**
  - **Estático:** fixa o MAC na porta.
  - **DROP:** descarta os pacotes provenientes do MAC configurado.

Selecione a porta que será vinculada ao MAC estático.

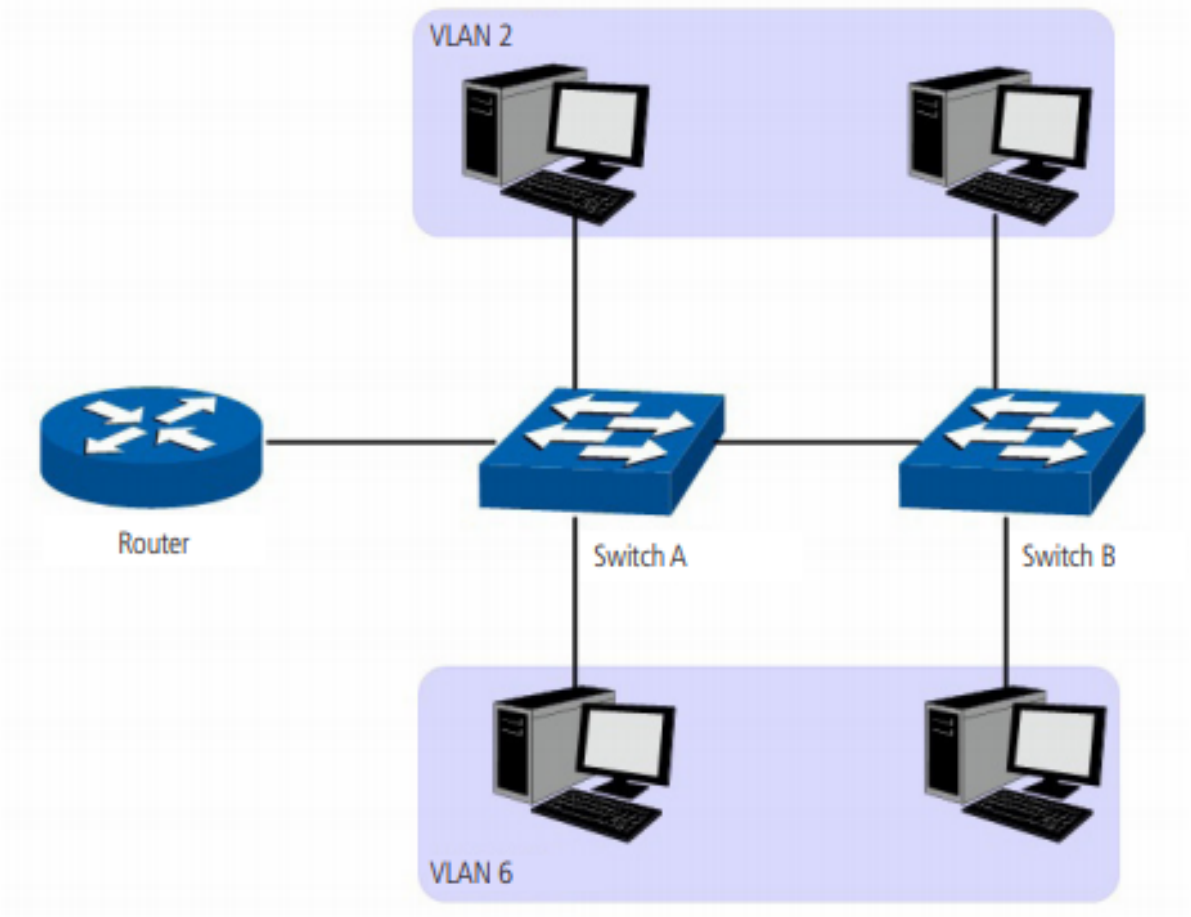
Obs: se configurada a regra em modo DROP o switch descartará os pacotes provenientes do MAC configurado em todas as portas.

Clique em Salvar para salvar as configurações.

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.

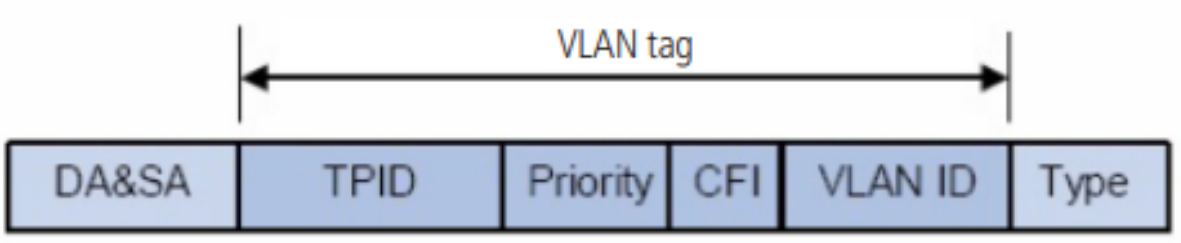
Este switch suporta os seguintes modos de classificação de VLAN: *802.1q VLAN, VLAN de voz, Surveillance VLAN, MAC VLAN, Guest VLAN e VLAN por protocolo*.

VLAN

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).

Configurar VLAN

O menu Configurar VLAN permite a criação, remoção e gerenciamento de VLANs no switch.

Escolha o menu VLAN > VLAN > Configurar VLAN para carregar a seguinte página:

A seguir apresentamos o descritivo das informações contidas nesta página:

- **VLAN ID:** exibe o VLAN ID da VLAN (identificação da VLAN).
- **Nome da VLAN:** exibe o nome da VLAN.
- **Porta tagged:** exibe a(s) porta(s) tagged da VLAN, ou seja, os pacotes transmitidos nestas portas serão marcados com a tag de VLAN (tagged – pacotes contendo informações de VLAN).
- **Porta untagged:** exibe a(s) porta(s) untagged da VLAN, ou seja, os pacotes transmitidos nestas portas não serão marcados com a tag de VLAN (untagged – pacotes que não contém informações de VLAN).

Obs: por padrão, todas as portas do switch são untagged e pertencem a VLAN 1.

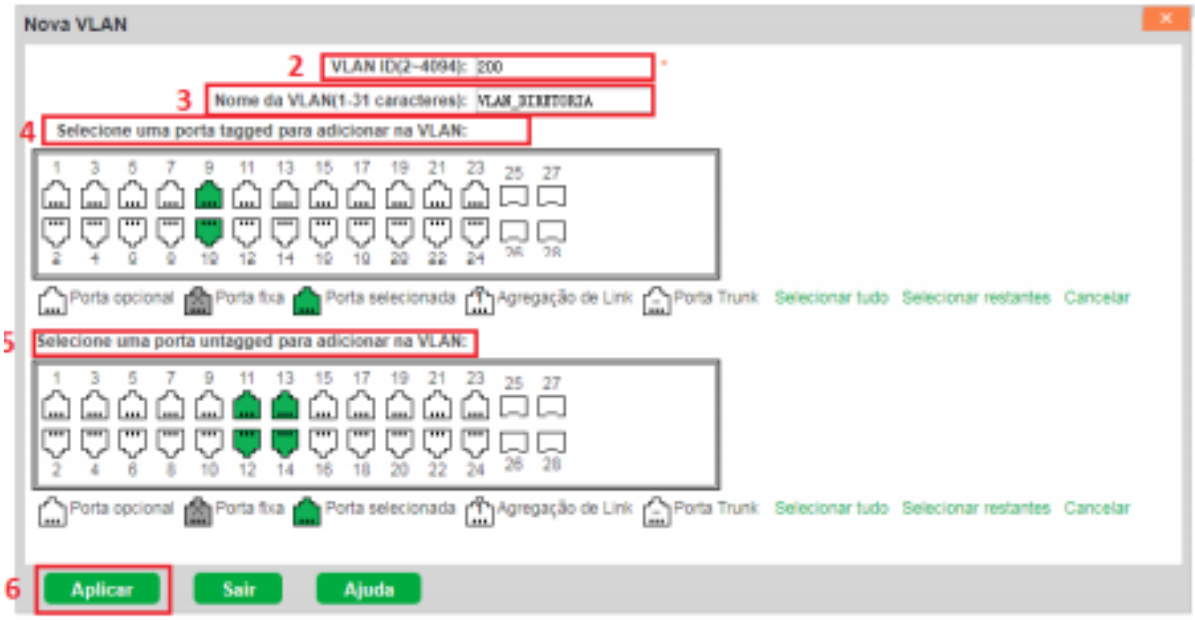
Adicionando VLAN

Para adicionar uma nova VLAN, siga o procedimento:

1. Clique no botão Nova VLAN;
2. Configure o VLAN ID desejado (1 – 4094);
3. Configure o nome da VLAN;
4. Selecione as portas tagged da VLAN (os pacotes transmitidos nas portas tagged serão marcados com a tag de VLAN);
5. Selecione as portas untagged da VLAN (os pacotes transmitidos nas portas untagged não serão marcados com a tag de VLAN);
6. Clique em Salvar.

No exemplo a seguir iremos configurar uma VLAN com as seguintes características:

- **VLAN ID:** 200.
- **Nome da VLAN:** VLAN_DIRETORIA.
- **Portas tagged:** 9 e 10.
- **Portas untagged:** 11, 12, 13 e 14.

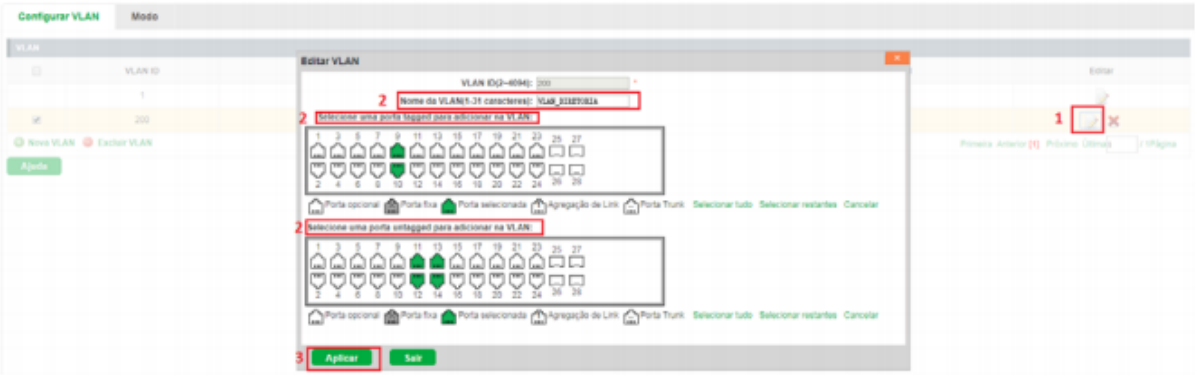


Obs: se não for especificado um nome para a VLAN, o sistema irá especificar automaticamente um nome seguindo o seguinte padrão: VLANXXXX, onde XXXX indica o ID da VLAN criada.

Editando VLAN

Para editar uma VLAN existente, acesse o menu VLAN > VLAN > Configurar VLAN e siga o procedimento:

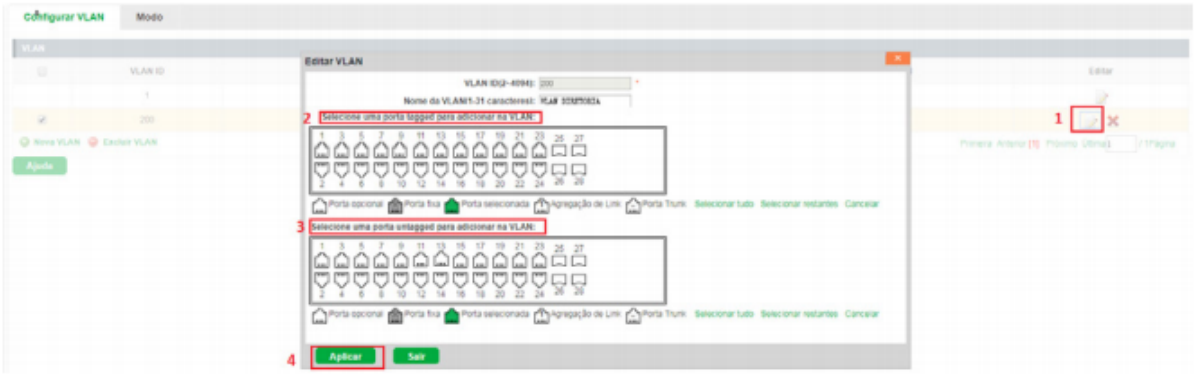
1. Clique no ícone (EDITAR) da VLAN que deseja editar;
2. Efetue as alterações desejadas;
3. Clique em Aplicar.



Removendo VLAN

Para remover uma VLAN é necessário primeiramente remover as portas que estão associadas àquela VLAN. Para isto, siga o procedimento:

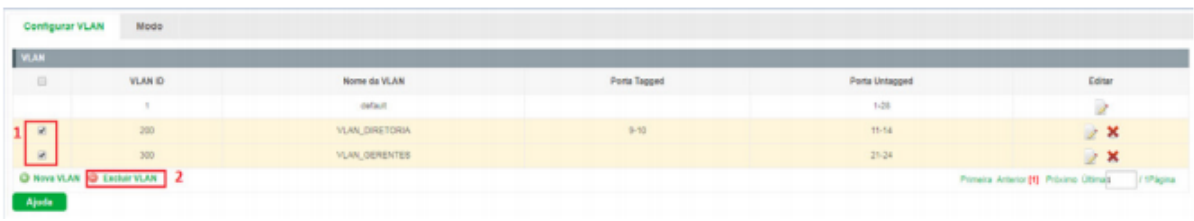
1. Clique no ícone (EDITAR) da VLAN que deseja excluir;
2. Remova as portas tagged da VLAN;
3. Remova as portas untagged da VLAN;
4. Clique em Aplicar.



Após remover as portas, clique no ícone (EXCLUIR) para remover a VLAN por completo.

Também é possível remover múltiplas VLANs, para isto siga o procedimento:

1. Selecione as VLANs a serem excluídas através da caixa de seleção;
2. Clique em Excluir VLAN.



Obs: somente poderão ser removidas VLANs que não possuam portas associadas.

Modo

O menu Modo determina o modo de funcionamento das portas. As portas do switch podem operar de três modos diferentes, a seguir apresentamos a descrição de cada um dos modos:

- **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.
- **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.
- **Hybrid:** a porta em modo Trunk pode ser adicionada em várias VLANs e transmitir pacotes TAG e UNTAG.

Observações:

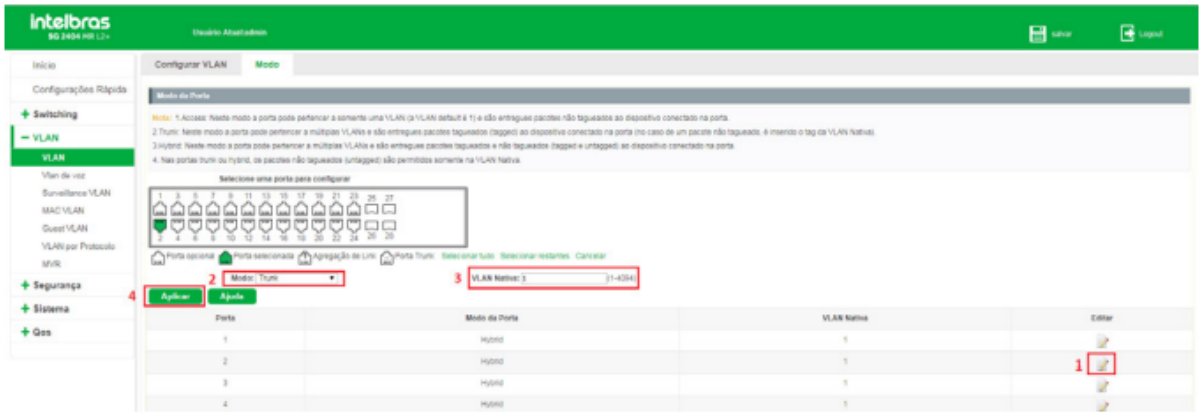
- Quando utilizado o modo Trunk ou Hybrid somente a VLAN nativa poderá ser transmitida por pacotes UNTAG.
- Por padrão, todas as portas são configuradas em modo Hybrid.
- Por padrão, a VLAN Nativa é 1.

Escolha o menu VLAN > VLAN > Modo para carregar a página de configuração de modo de porta.

Alterando o modo de uma porta

Observe as instruções a seguir para alterar o modo de funcionamento de uma determinada porta:

1. Clique no ícone (EDITAR) da porta que deseja configurar ou selecione através do painel de portas (é possível selecionar mais de uma porta para configuração no painel);
2. Altere o modo da porta;
3. Se o novo modo da porta for Trunk ou Hybrid, configure a VLAN nativa com a VLAN desejada;
4. Clique em Aplicar.

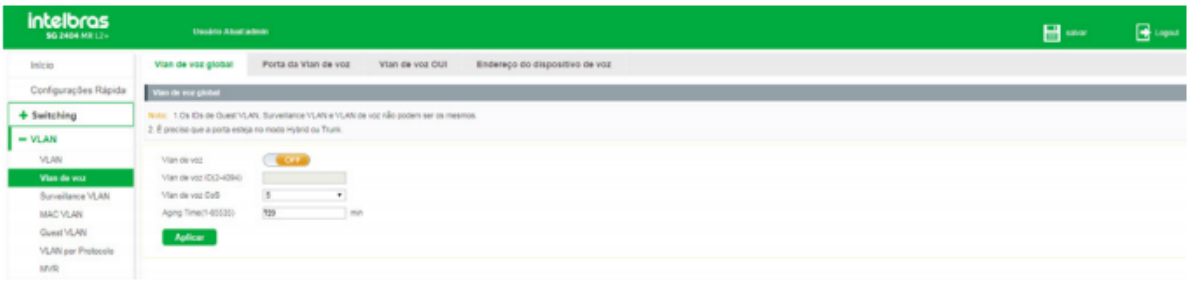


VLAN de voz

A VLAN de voz é configurada especialmente para o fluxo de dados de voz. Ao configurar uma VLAN de voz e adicionar as portas a dispositivos de voz, você pode executar QoS relacionando as configurações de dados e voz, garantindo a prioridade de transmissão dos fluxos de dados e a qualidade da voz.

VLAN de voz global

Escolha o menu VLAN > Vlan de voz > Vlan de voz global para carregar a seguinte página:



Habilitando VLAN de voz

Observe o procedimento a seguir para habilitar a VLAN de voz:

1. Clique no ícone para alterar o estado da VLAN de voz. O ícone deverá ficar com status ON: ;
2. Configure o ID da VLAN de voz;
3. Configure a classe de serviço (CoS) da VLAN de voz;
4. Este campo irá definir a prioridade (802.1p) que será inserida nos pacotes de voz;
5. Especifique o tempo de envelhecimento (*aging time*) para as portas membro da VLAN de voz;
6. Clique em Aplicar.

Obs: antes de habilitar a VLAN de voz é necessário criar a VLAN que será utilizada para voz em VLAN > VLAN > Configurar VLAN.

Portas da VLAN de voz

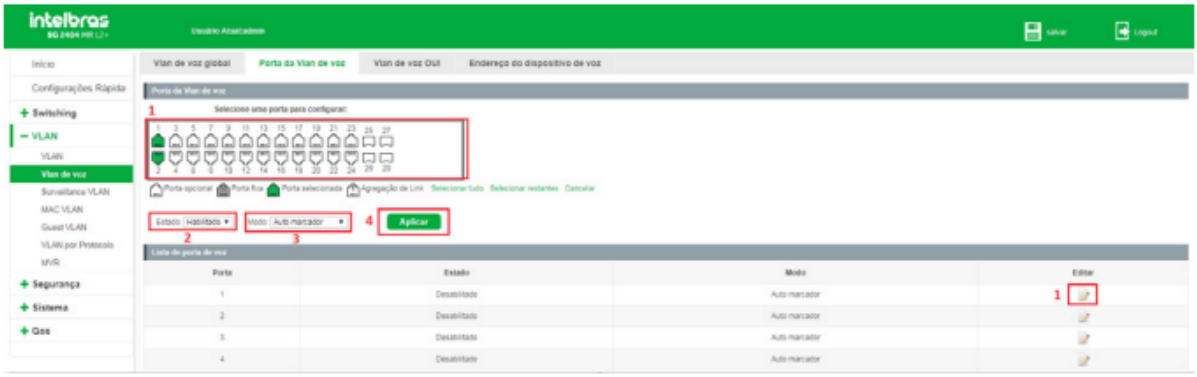
Nesse menu serão configuradas as portas que participarão da VLAN de voz, bem como seus parâmetros de configuração. Observe o procedimento a seguir para configurar as portas da VLAN de voz:

1. Selecione a(s) porta(s) que deseja configurar;
2. Escolha o estado de funcionamento da VLAN de voz na porta (Habilitado/Desabilitado);
3. Escolha o modo de funcionamento da porta. As opções são as seguintes:

- **Autodesmarcador:** neste modo o switch adiciona ou remove automaticamente a porta da VLAN de voz, verificando se o tráfego recebido pela porta é de voz ou não. O tráfego de voz transmitido pela porta será untagged (sem tag de VLAN).

- **Automarcador:** neste modo o switch adiciona ou remove automaticamente a porta da VLAN de voz, verificando se o tráfego recebido pela porta é de voz ou não. O tráfego de voz transmitido pela porta será tagged (com tag de VLAN).
- **Manual:** neste modo é possível adicionar ou remover manualmente uma porta da VLAN de voz.

4. Clique em Aplicar.



Obs: só é possível habilitar a porta na VLAN de voz, caso a porta esteja em modo Hybrid ou Trunk. Acesse o menu VLAN > VLAN > Modo para verificar o modo de funcionamento das portas.

VLAN de voz OUI

Tabela OUI (Organizationally Unique Identifier) para VLAN de voz

Nesta página é possível adicionar os endereços MAC dos dispositivos de voz, in- serindo o endereço OUI do fabricante. O switch determina se um pacote recebido é de voz ou não verificando se o endereço MAC de origem do pacote possui um endereço OUI correspondente, podendo então, adicionar automaticamente a porta para a VLAN de voz.

Observe as instruções a seguir para configurar um endereço OUI:

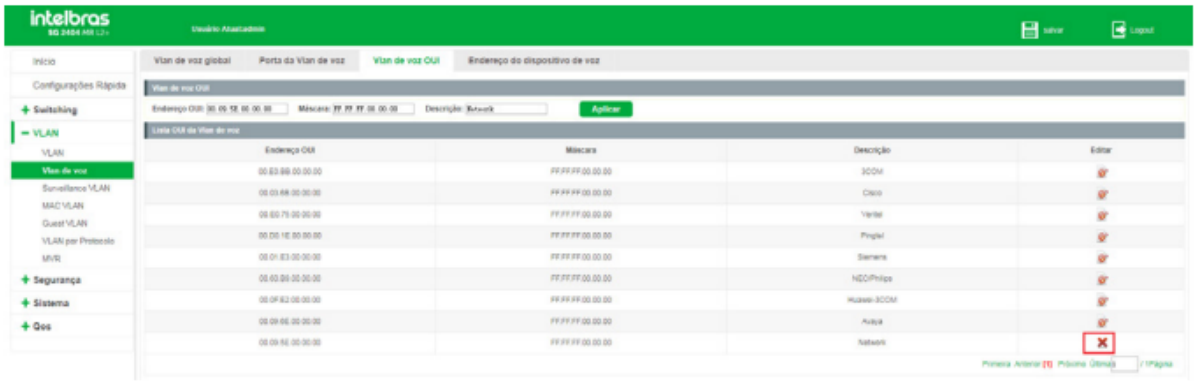
1. Configure o endereço de voz OUI do dispositivo de voz;
2. Configure a máscara utilizada pelo endereço OUI do dispositivo de voz;
3. Configure uma descrição para identificação do endereço OUI;
4. Clique em Aplicar.

Observações:

- O switch suporta até 16 endereços OUI configurados.
- O endereço OUI é válido somente para endereços unicast.
- Só são permitidos os caracteres F e 0 na configuração da máscara. O caractere F indica que o endereço MAC é fixo naquele ponto, já o caractere 0 indica que o valor pode variar.

- É permitido configurar máscaras com todos os caracteres F. Neste caso o endereço OUI não possui variações.
- Não é permitido utilizar o caractere 0 antes de um caractere F.

Para remover um endereço OUI clique no ícone (EXCLUIR), conforme imagem a seguir:



Endereço do dispositivo de voz

Quando o switch reconhece um endereço OUI em uma porta que esteja habilitada a VLAN de voz, este dispositivo é apresentado na lista de endereços de dispositivos de voz.

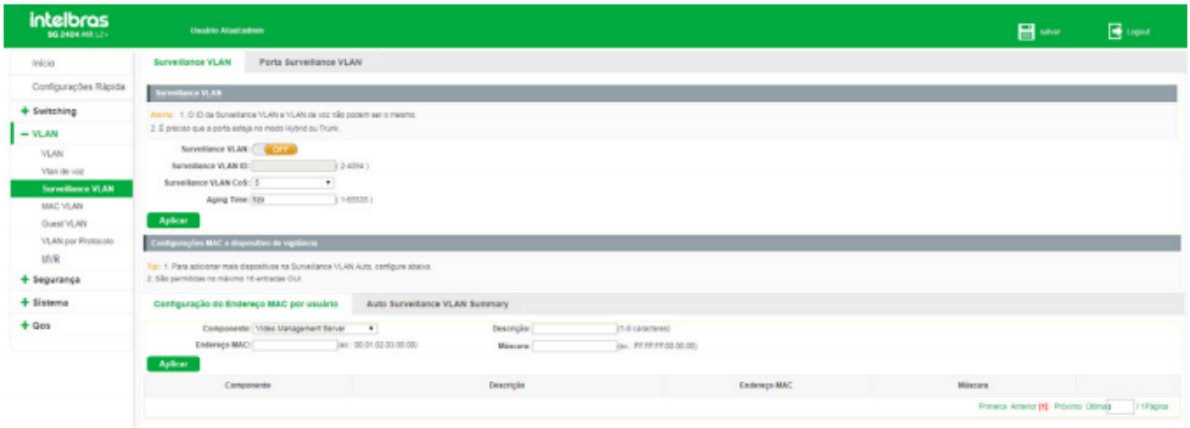
Escolha o menu VLAN > Vlan de voz > Endereço do dispositivo de voz para carregar a seguinte página:

Surveillance VLAN

Uma Surveillance VLAN, ou VLAN de vigilância, é configurada especialmente para o fluxo de dados de dispositivos de segurança, como câmeras e gravadores de vídeo. Ao configurar uma Surveillance VLAN e adicionar as portas aos dispositivos, é possível executar QoS, garantindo assim a prioridade de transmissão dos fluxos de dados dos dispositivos de segurança.

Surveillance VLAN

Escolha o menu VLAN > Surveillance VLAN > Surveillance VLAN para carregar a seguinte página:



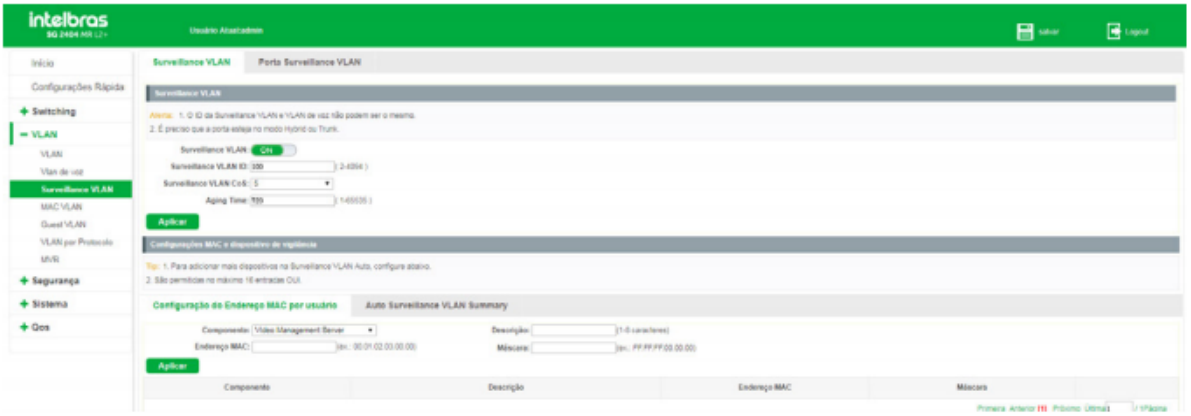
Habilitando Surveillance VLAN

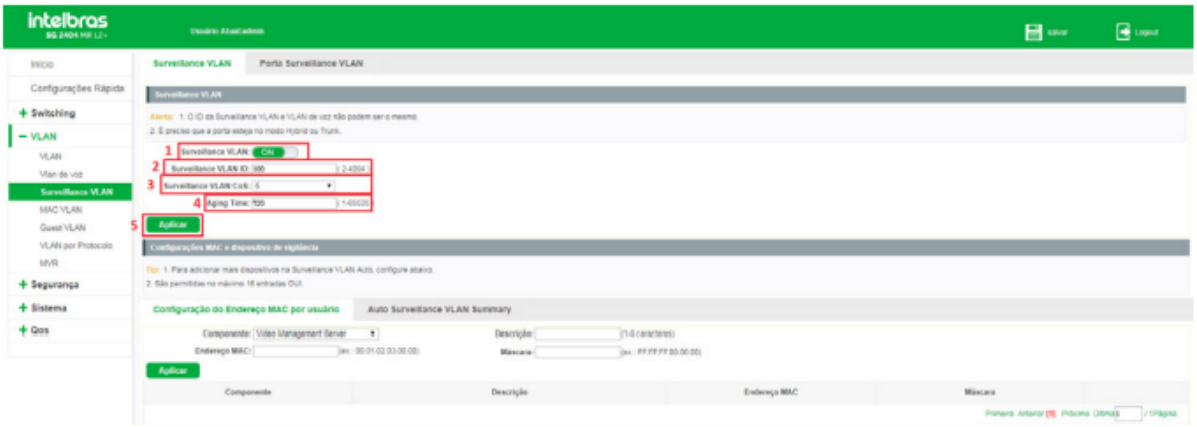
Observe o procedimento a seguir para habilitar a Surveillance VLAN:

1. Clique no ícone para alterar o estado da Surveillance VLAN. O ícone deverá ficar com status ON: ;
2. Configure o ID da Surveillance VLAN;
3. Configure a classe de serviço (CoS) da VLAN de voz;

   Este campo irá definir a prioridade (802.1p) que será inserida nos pacotes da Surveillance VLAN.

4. Especifique o tempo de envelhecimento (*aging time*) para as portas membro da Surveillance VLAN;
5. Clique em Aplicar.



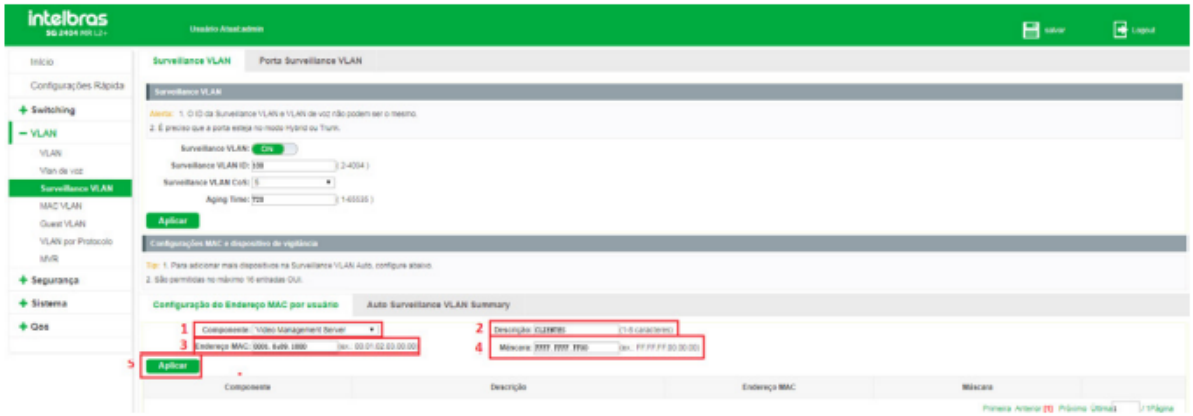


Obs: o ID da Surveillance VLAN e da VLAN de voz não pode ser o mesmo.

Configurando MAC dos Dispositivos da Surveillance VLAN

O switch permite configurar os dispositivos de segurança que irão utilizar a Surveillance VLAN. Para isto, acesse a página VLAN > Surveillance VLAN > Surveillance VLAN e observe as instruções a seguir:

1. Selecione o tipo de dispositivo;
2. Configure uma descrição para identificação do dispositivo;
3. Configure o endereço MAC;
4. Configure a máscara para o endereço MAC;
5. Clique em Aplicar.



Observações:

- O switch suporta até 16 endereços configurados.
- Só são permitidos os caracteres F e 0 na configuração da máscara. O caractere F indica que o endereço MAC é fixo naquele ponto, já o caractere 0 indica que o valor pode variar.
- É permitido configurar máscaras com todos os caracteres F. Neste caso o endereço OUI não possui variações.
- Não é permitido utilizar o caractere 0 antes de um caractere F.

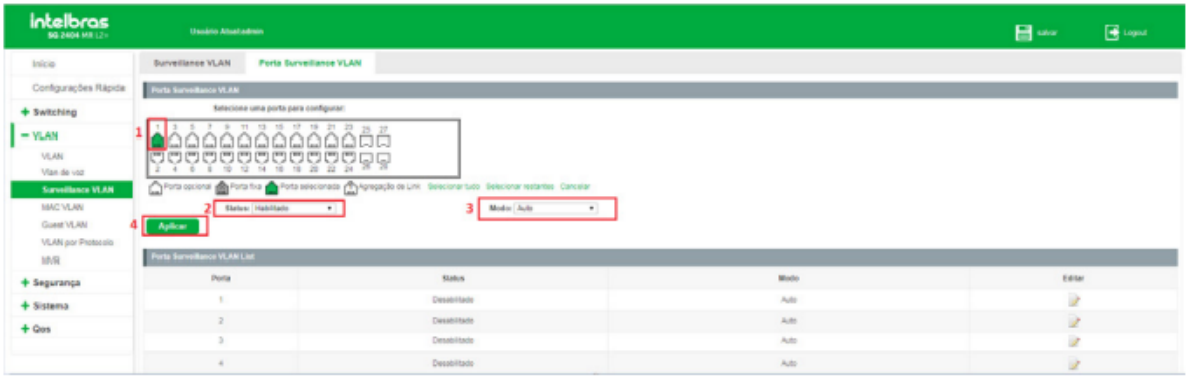
Porta Surveillance VLAN

Neste menu é possível configurar as portas que irão pertencer a Surveillance VLAN. Para isto, acesse a página VLAN > Surveillance VLAN > Porta Surveillance VLAN e observe as instruções a seguir:

1. Selecione a(s) porta(s) que deseja configurar;
2. Configure o status da porta (Habilitado/Desabilitado);
3. Configure o modo da porta (Auto/Manual);

- **Auto:** associa automaticamente a porta a VLAN.
- **Manual:** é necessário associar a porta a VLAN manualmente.

4. Clique em Salvar.

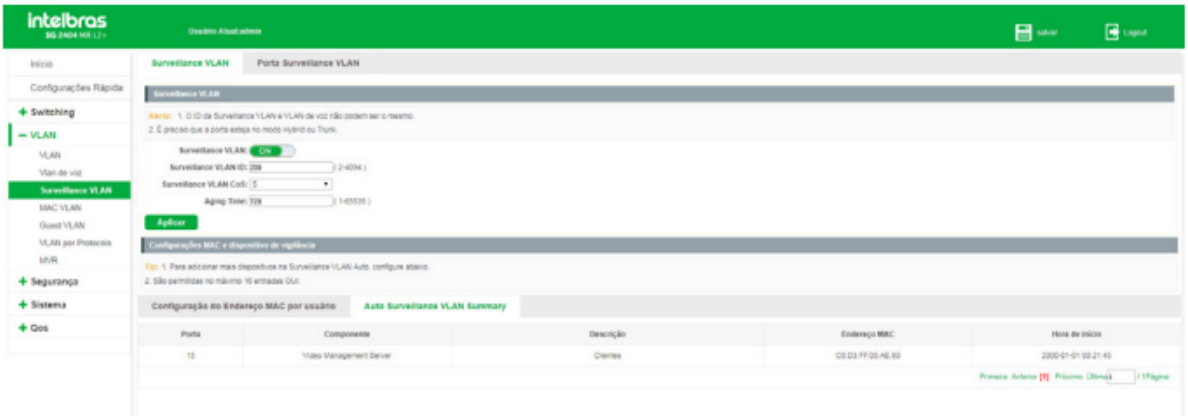


Obs: só é possível habilitar Surveillance VLAN na porta caso a porta esteja em modo Hybrid ou Trunk. Acesse o menu VLAN > VLAN > Modo para verificar o modo de funcionamento das portas.

Visualizar dispositivos pertencentes a Surveillance VLAN

Quando for detectado um dispositivo dentro da máscara de endereço MAC configurada numa porta onde a Surveillance VLAN está habilitada, o switch irá exibir este dispositivo em Auto Surveillance VLAN Summary.

Escolha o menu VLAN > Surveillance VLAN > Surveillance VLAN > Auto Surveillance VLAN Summary para carregar a seguinte página:



MAC VLAN

A função MAC VLAN faz um mapeamento entre endereços MAC de dispositivos conectados ao switch e VLANs cadastradas no equipamento. Este mapeamento permite que o switch, ao receber um pacote em uma porta que esteja habilitado o MAC VLAN, identifique o MAC de origem deste pacote e, de acordo com este MAC, encaminhe o pacote a determinada VLAN. Os pacotes de um MAC VLAN são processados da seguinte maneira:

- Ao receber um pacote untagged, o switch verifica se o endereço MAC do pacote possui uma entrada correspondente nas configurações de MAC VLAN. Se o endereço MAC corresponder, o switch adicionará a tag de VLAN no pacote, de acordo com o VLAN ID do MAC VLAN configurado. Se o endereço MAC não corresponder, o switch adicionará a tag de VLAN no pacote de acordo com a VLAN Nativa configurada para a porta. Assim o pacote será atribuído automaticamente para a VLAN correspondente.
- Ao receber um pacote tagged, o switch irá processá-lo de acordo com as configurações de VLAN. Se a porta que recebeu o pacote é membro da VLAN, o pacote será transmitido normalmente, caso contrário, o pacote será

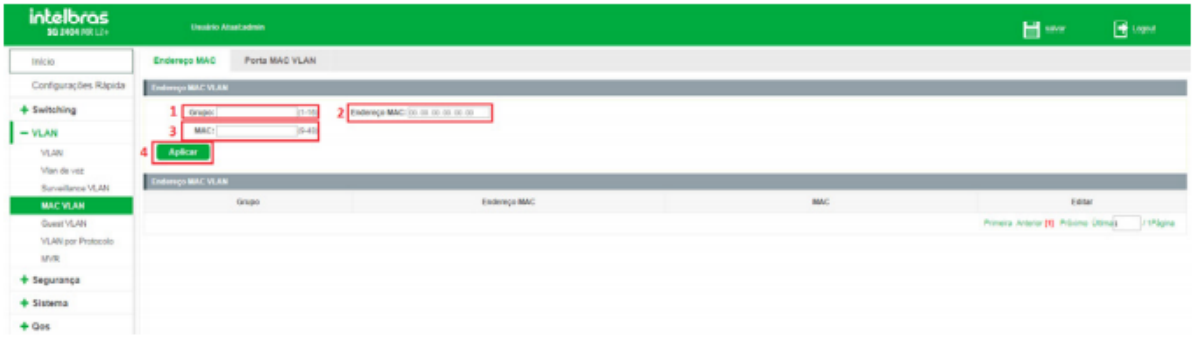
descartado.

- Ao criar um MAC VLAN é necessário habilitar a porta para ser membro da VLAN correspondente, de modo a garantir que os pacotes sejam encaminhados normalmente.

Endereço MAC

Para configurar a função MAC VLAN, acesse a página VLAN > MAC VLAN > Ende- reço MAC e observe as instruções a seguir:

1. Insira o número do grupo que deseja configurar. O switch aceita a configuração de no máximo 16 grupos;
2. Configure o endereço MAC que deseja associar a uma VLAN. Deve ser cadastrado um endereço MAC do tipo unicast;
3. Informe a máscara para coincidir com o número de bits do endereço MAC configurado;
4. Salve a configuração.

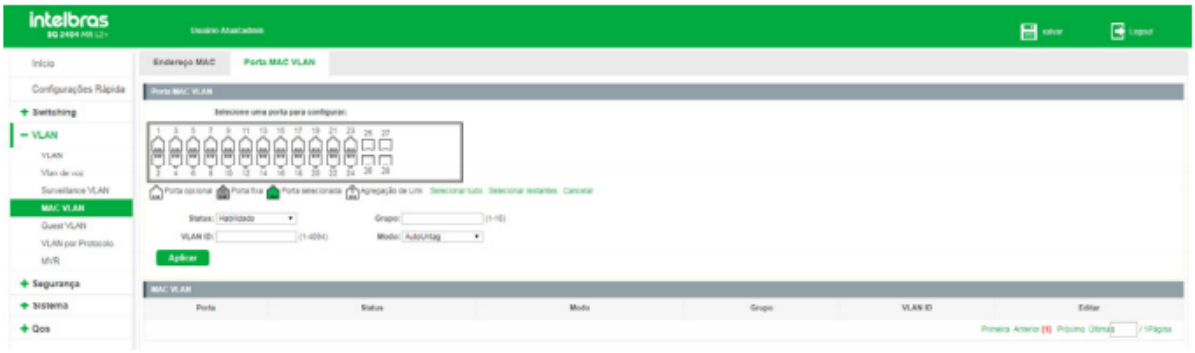


Porta MAC VLAN

Neste menu é possível configurar as portas que irão pertencer a um grupo de MAC VLAN. Para isto, acesse a página VLAN > MAC VLAN > Porta MAC VLAN e observe as instruções a seguir:

1. Selecione a(s) porta(s) que deseja configurar;
2. Configure o status da porta (Habilitado/Desabilitado);
3. Configure o grupo que esta porta deve pertencer. Este grupo deve ser o mesmo já criado antes na tela Endereço MAC. O switch aceita a configuração de no máximo 16 grupos;
4. Configure a VLAN para a porta. Esta VLAN deve ser criada antes na tela Menu VLAN > VLAN > Configurar VLAN;
5. Configure o modo da porta (Auto/Manual);

- **AutoUntag:** associa automaticamente a porta a VLAN.
- **Manual:** é necessário associar a porta a VLAN manualmente.



Guest VLAN

A função Guest VLAN, ou VLAN de convidado, permite que os dispositivos suplicantes que não passam na autenticação 802.1x possam acessar os recursos de uma rede específica. Por padrão, todas as portas conectadas aos suplicantes pertencem a uma VLAN, ou seja, a Guest VLAN. Usuários pertencentes à Guest VLAN podem acessar os recursos da Guest VLAN sem estarem autenticados. Ao realizar uma autenticação, as portas do switch irão ser removidas da Guest VLAN, permitindo acesso aos demais recursos da rede.

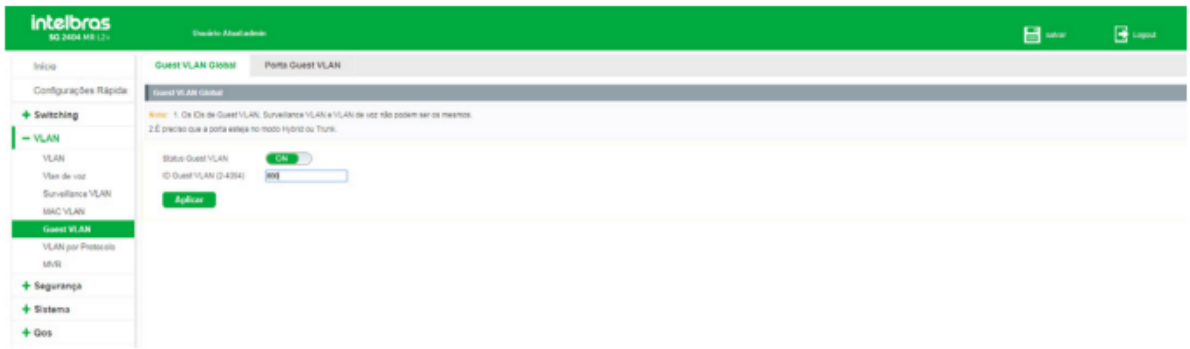
Com a função Guest VLAN habilitada, os usuários podem acessar a Guest VLAN para instalar o programa 802.1x cliente ou atualizar seus clientes 802.1x sem estar autenticado. Se não houver suplicantes na porta por certo período de tempo, o switch irá adicionar a porta para a Guest VLAN.

Com a função 802.1x habilitada e a Guest VLAN configurada, após o número máximo de tentativas terem sido feitas para enviar pacotes EAP-Request/Identify e ainda houver portas que não enviaram nenhuma resposta de volta, o switch irá adicionar essas portas para a Guest VLAN, de acordo com seus tipos de Links. Só quando o usuário correspondente realizar a autenticação 802.1x, a porta será removida da Guest VLAN e adicionada a VLAN especificada. Além disso, a porta voltará para a Guest VLAN quando seus usuários conectados fizerem logoff.

Guest VLAN globa

Para configurar a Guest VLAN, acesse a página VLAN > Guest VLAN > Guest VLAN global e observe as instruções a seguir:

1. Clique no ícone (OFF) para alterar o estado da Guest VLAN. O ícone deverá ficar com status (ON);
2. Configure o ID da Guest VLAN;
3. Clique em Aplicar.



Obs: para configurar a Guest VLAN é necessário primeiramente criar a VLAN em VLAN > VLAN > Configurar VLAN.

Porta Guest VLAN

Para configurar as portas que participarão da Guest VLAN, acesse a página VLAN > Guest VLAN > Porta Guest VLAN e observe as instruções a seguir:

1. Selecione a(s) porta(s) que deseja configurar;
2. Configure o estado da Guest VLAN (Habilitado/Desabilitado);
3. Configure o estado do dot1x (Habilitado/Desabilitado);

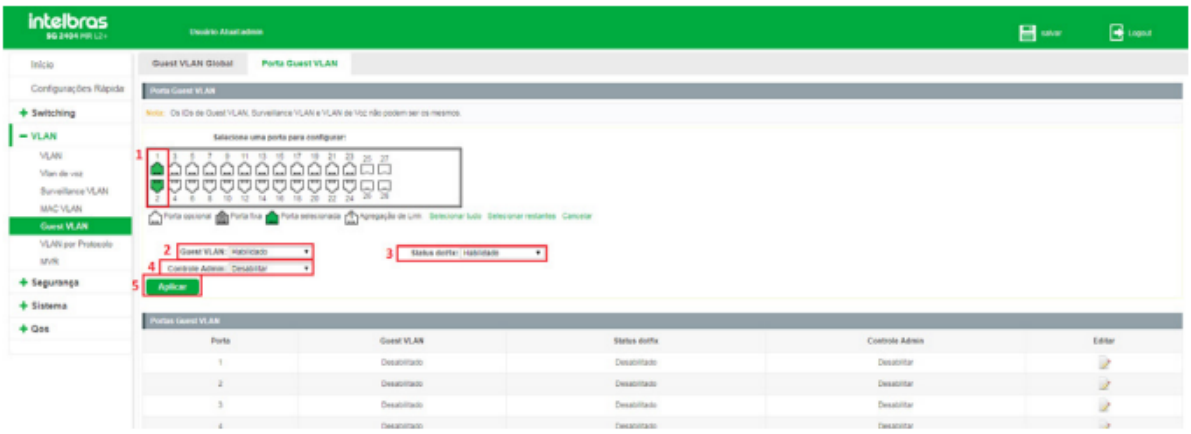
   O protocolo dot1x ou 802.1x foi desenvolvido pela IEEE 802 comissão LAN/ WAN, para lidar com as questões de segurança de redes sem fio. Em seguida foi utilizado como mecanismo de controle de acesso utilizado pelo Ethernet, resolvendo problemas de autenticação e segurança.

   802.1x é o padrão de autenticação para o controle de acesso a rede, onde cada dispositivo da LAN (suplicante) somente irá utilizar a rede se estiver autenticado em um servidor de modo seguro

4. Configure o status da autenticação de acordo com as opções a seguir:

   - **Auto:** a porta irá autenticar automaticamente quando houver acesso de um host.
   - **Forçar autenticação:** a porta é mantida autenticada independente se houver host ou não. Neste modo, o host não precisa solicitar autenticação.
   - **Forçar não autenticar:** a porta é mantida não autenticada independente se houver host ou não. Neste modo, não ocorre autenticação mesmo se houver solicitação do host.

5. Clique em Salvar.



VLAN por protocolo

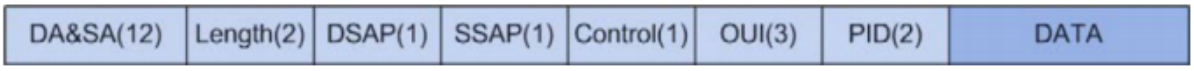
VLAN por protocolo é a maneira de classificar as VLANs de acordo com o protocolo de rede utilizado, entre eles o IP, IPX, DECnet, AppleTalk, Banyan e assim por diante. Com a criação de VLANs por protocolo, o administrador de rede pode gerenciar os clientes da rede baseando-se em suas aplicações e serviços de forma eficaz.

Formato de encapsulamento dos dados Ethernet

Esta seção introduz a forma de encapsulamento comum dos dados Ethernet. Estes formatos são utilizados para a identificação de cada protocolo presente nos pacotes recebidos pelo switch. Atualmente existem dois formatos de encapsulamento dos dados Ethernet. O encapsulamento Ethernet II e o encapsulamento 802.2/802.3, conforme mostrado a seguir:

Encapsulamento Ethernet II

Encapsulamento 802.2/802.3



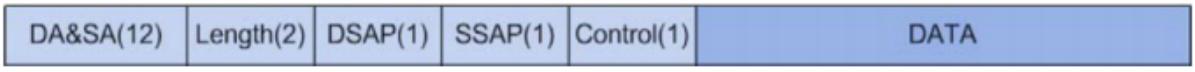
DA e SA referem-se respectivamente ao endereço MAC de destino e o endereço MAC de origem. O número informado entre parênteses indica o tamanho do campo em bytes.

O tamanho máximo de um frame Ethernet é de 1500 bytes, representado por 0x05DC em hexadecimal. O campo Length utilizado pelo encapsulamento 802.2/802.3 permite valores entre 0x0000 e 0x05DC (0 a 1500) e o campo Type utilizado pelo encapsulamento Ethernet II permite valores entre 0x0600 e 0xFFF (1536 a 4095), sendo através destes dois campos que o switch identifica o tipo de encapsulamento do frame Ethernet. Caso os campos Type e Length possuam valores entre 0x05DD a 0x05FF (1501 a 1535) o frame Ethernet é diretamente descartado, considerando o pacote como ilegal.

O encapsulamento 802.2/802.3 possui 3 possíveis formatos estendidos:

Encapsulamento 802.3 raw

Encapsulamento 802.2 LLC (Logic Link Control)



Apenas os campos Length, DSAP (*Destination Service Access Point*), SSAP (*Source Service Access Point*) e Control são encapsulados após o campo DA/SA (endereço MAC de destino e origem). O valor do campo Control é sempre 3. Os campos DSAP e SSAP do encapsulamento 802.2 LLC são utilizados para identificar o protocolo da camada superior, por exemplo, quando os dois campos possuem os valores 0xE0, indica que o protocolo da camada superior é o IPX.

Encapsulamento 802.2 SNAP (Sub-Network Access Protocol)

No encapsulamento 802.2 SNAP os valores dos campos DSAP e SSAP são sempre 0xAA e o valor do campo Control é 3. O switch diferencia os encapsulamentos 802.2 LLC e SNAP de acordo com os valores dos campos DSAP e SSAP

O dispositivo determina a forma de encapsulamento dos pacotes enviados. Um dispositivo pode enviar pacotes com os dois formatos de encapsulamento. O encapsulamento Ethernet II é o mais utilizado atualmente.

Procedimento de identificação do pacote pelo switch

Os pacotes em uma VLAN por protocolo são processados da seguinte maneira:

- Ao receber um pacote untagged, o switch verifica se o protocolo de rede do pacote possui uma entrada correspondente nas configurações de VLAN por protocolo. Se o protocolo de rede corresponder, o switch adicionará a tag de VLAN no pacote de acordo com o VLAN ID da VLAN por protocolo configurado. Se o protocolo de rede não corresponder, o switch adicionará a tag de VLAN no pacote de acordo com a VLAN Nativa configurada para a porta. Assim o pacote é atribuído automaticamente para a VLAN correspondente.
- Ao receber um pacote tagged, o switch irá processá-lo de acordo com as configurações de VLAN. Se a porta que recebeu o pacote é membro da VLAN, o pacote será transmitido normalmente, caso contrário, o pacote será descartado.

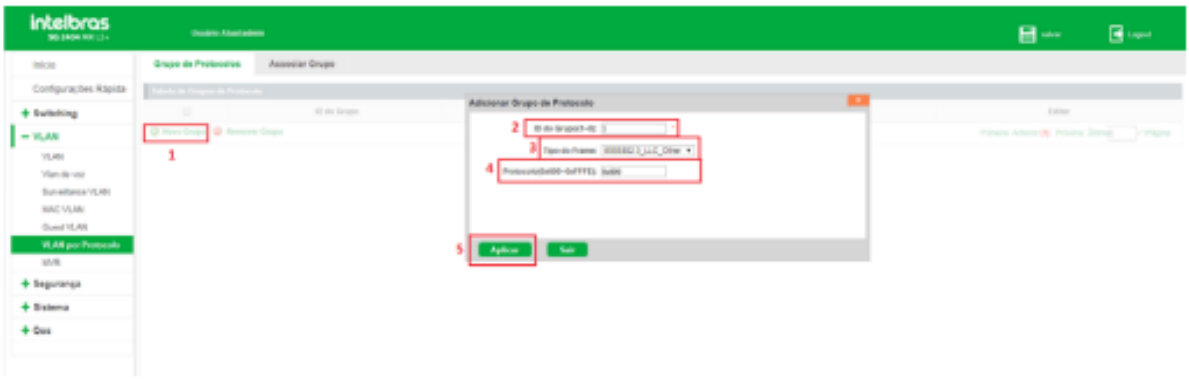
- Ao criar VLANs por Protocolo, é necessário habilitar a porta para ser membro da VLAN correspondente, de modo a garantir que os pacotes sejam encaminhados normalmente.

Grupo de protocolos

No switch é possível criar modelos de protocolos para transmitir os pacotes correspondentes nas VLANs desejadas. Modelos de protocolos compreendem a forma de encapsulamento e o tipo de protocolo, determinando desta forma, o protocolo de rede utilizado pelo pacote. A configuração de grupo de protocolos permite a criação destes modelos.

Para adicionar um grupo de protocolo, escolha o menu VLAN > VLAN por protocolo > Grupo de protocolos e observe as orientações a seguir:

1. Clique em Novo Grupo;
2. Insira o ID do grupo;
3. Selecione o tipo de encapsulamento utilizado pelo modelo de protocolo;
4. Digite o valor em hexadecimal referente ao tipo de protocolo de rede desejado;
5. Clique em Apply.



Obs: o switch permite a criação de até 8 grupos de protocolo.

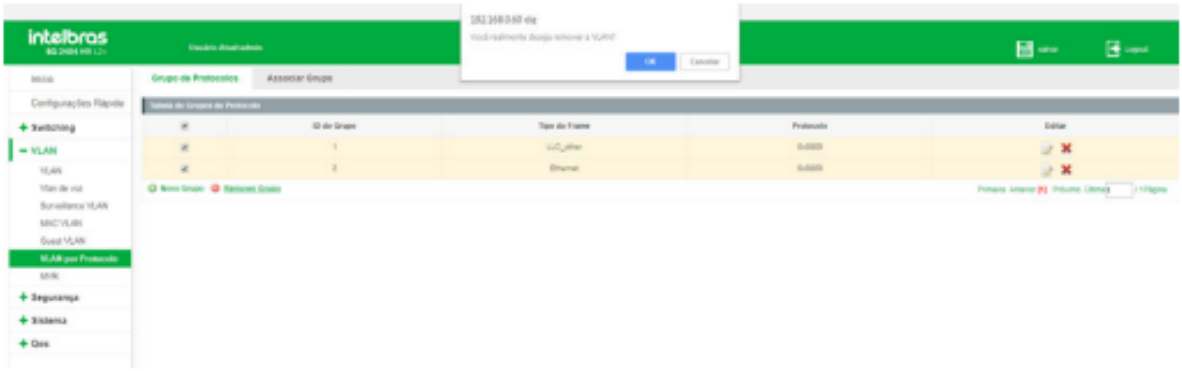
Alterando grupos de protocolo

Caso queira editar um grupo de protocolo já criado, siga as orientações a seguir:

1. Clique no ícone (EDITAR) do grupo que deseja alterar;
2. Edite o tipo do frame, se necessário;
3. Edite o protocolo, se necessário;
4. Clique em Apply.

Removendo grupos de protocolo

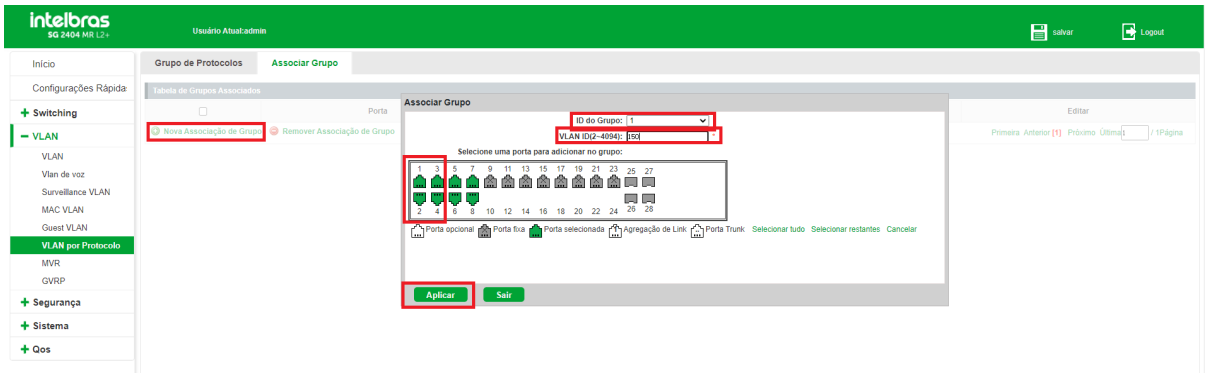
Para remover apenas um grupo de protocolo, basta clicar no ícone (EXCLUIR) e confirmar a exclusão. Caso queira remover mais de um grupo, selecione os grupos a serem excluídos nas caixas de seleção e clique em Remover grupo.



Associar grupo

A configuração de associação de grupos de protocolos permite vincular o grupo a uma determinada VLAN e as portas pertencentes ao grupo. Para configurar uma associação, escolha o menu VLAN > VLAN por protocolo > Associar grupo e siga as orientações a seguir:

1. Clique em Nova associação de grupo;
2. Selecione o ID do grupo que deseja configurar;
3. Digite a VLAN ID (identificação de VLAN) da VLAN por protocolo;
4. Selecione as portas participantes;
5. Clique em Salvar.



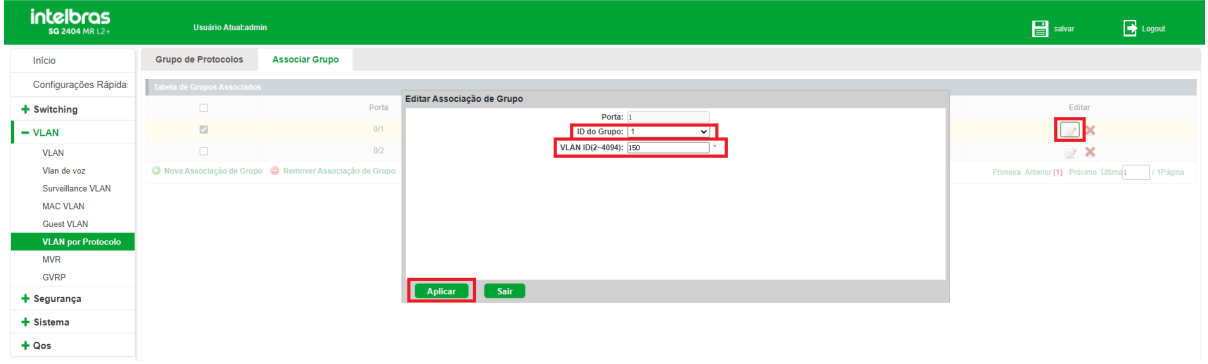
Obs: Antes de efetuar a associação, é necessário criar a VLAN no menu VLAN > VLAN > Configurar VLAN.

- As portas selecionadas deverão pertencer a VLAN configurada.
- As portas deverão estar em modo Trunk ou Hybrid.

Editando associação de grupos de protocolos

Caso deseje editar uma associação de grupos por protocolos, siga as instruções a seguir:

1. Clique no ícone (EDITAR) da porta que deseja editar;
2. Edite o ID do grupo ao qual a porta pertence, se necessário;
3. Edite a VLAN ID da VLAN por protocolo a qual a porta pertence, se necessário;
4. Clique em Aplicar.



Removendo associação de grupos de protocolos

Para remover uma associação de grupos de protocolos siga as instruções a seguir:

- Para remover apenas uma associação, basta clicar no ícone e confirmar a exclusão. Caso queira remover mais de uma associação de grupo, selecione as associações a serem excluídas nas caixas de seleção e clique em Remover associação de grupo.

MVR (*Multicast VLAN Registration*)

O MVR pode ser utilizado quando em uma rede existam hosts em VLANs diferentes que desejam receber o mesmo fluxo multicast. Neste cenário quando utilizado somente o IGMP snooping é preciso duplicar o fluxo multicast para hosts em cada VLAN. Para evitar o tráfego multicast duplicado entre o servidor e o switch surgiu o MVR.

O MVR pode ser configurado na seguinte tela: VLAN > MVR.

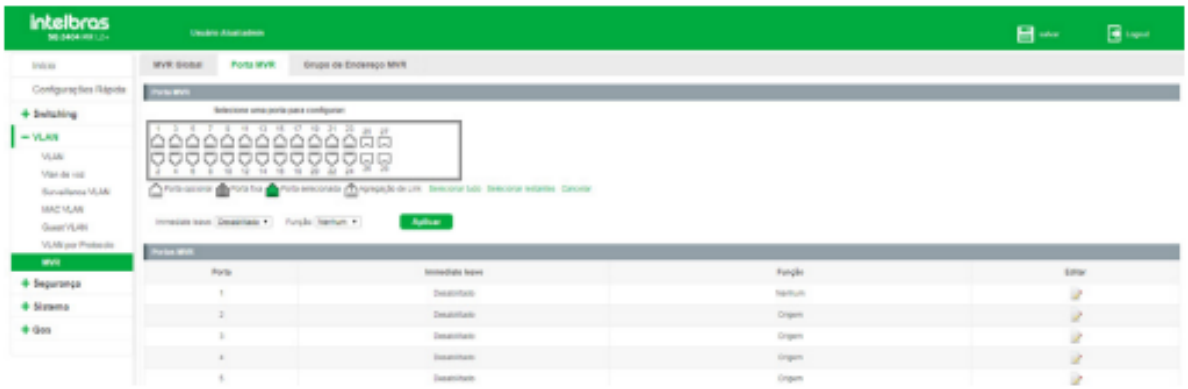
As seguintes opções são exibidas na tela:

- **MVR:** habilite ou desabilite o MVR.
- **Modo MVR:** selecione o modo do MVR.
  - **Compatível:** no modo Compatível o switch não encaminha mensagens de report e leave dos hosts para o roteador, isso significa que o roteador não consegue analisar os grupos multicast. Para que isso ocorra, é necessário adicionar um roteador estático para transmitir os fluxos multicast através do switch via MVR.
  - **Dinâmico:** no modo Dinâmico o switch pode encaminhar as mensagens report e leave para o roteador via MVR (através da mesma VLAN). Com isso, o roteador consegue analisar os grupos multicast e enviar o fluxo de acordo com a tabela multicast.
  - **Grupo inicial:** especifique o endereço do grupo. Os fluxos multicast enviados para o endereço especificado serão enviados para todas as portas de origem no switch e para todas as portas receptoras que solicitaram receber dados desse endereço multicast.

- **ID do grupo:** especifique um ID para o grupo multicast
- **Tempo de consulta:** especifique o intervalo de tempo que serão realizadas as consultas na tabela multicast.

Porta MVR

O Menu Porta MVR pode ser configurado na seguinte tela: VLAN > MVR > Porta MVR. Nesta página você pode configurar o modo das portas MVR.



As seguintes opções são exibidas na tela:

- **Immediate leave:** quando habilitada, a porta do receptor será removida do grupo multicast quando uma mensagem IGMP Leave for recebida nessa porta, sem verificar se há outros membros nesse grupo Multicast.
- **Função:** selecione uma opção:
  - **Origem:** os servidores multicast deverão ser conectados em portas em modo de Origem. No modo Compatível as portas de origem serão adicionadas automaticamente a todos os grupos multicast, no modo Dinâmico, é necessário adicionar os grupos multicast manualmente.
  - **Receptor:** os clientes deverão ser conectados em portas no modo Receptor. O switch pode remover ou adicionar as portas receptores do grupo multicast.

Grupo de endereço MVR

O Menu Grupo de endereço MVR pode ser configurado na seguinte tela: VLAN > MVR > Grupo de Endereço MVR.

Nesta página você pode configurar endereços estáticos.

As seguintes opções são exibidas na tela:

- **VLAN ID:** informa a VLAN configurada.

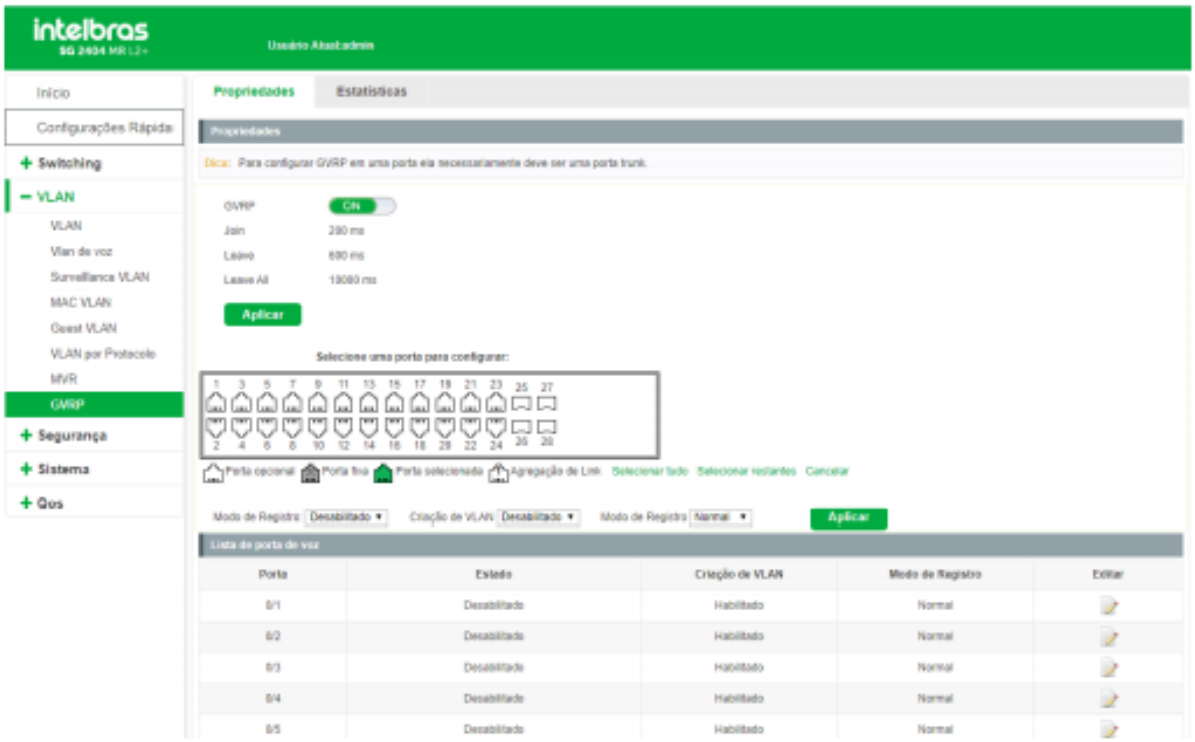
- **Grupo de endereço de grupo:** especifique o endereço estático do grupo multicast.

GVRP

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

Sem o GVRP em funcionamento, configurando a mesma VLAN em uma rede, seria necessário a configuração manual em cada dispositivo.

O GVRP pode ser configurado na seguinte tela: VLAN > GVRP.



As seguintes opções são exibidas na tela:

- **GVRP:** habilite ou desabilite o GVRP;
- **Porta GVRP:** selecione uma porta para configurar as informações do GVRP;
- **Modo de Registro:** habilite ou desabilite o GVRP na porta;
- **Criação de VLAN:** habilite ou desabilite a criação de VLAN na porta;
- **Modo de Registro:**
  - **Fixo:** neste modo, a porta é incapaz de registrar e remover os registros de VLANs dinamicamente, e pode transmitir apenas as informações de registro da VLAN estática.
  - **Normal:** neste modo, a porta pode registrar dinamicamente e remover o registro das VLANs, e transmitir as informações de registro da VLAN de ambos de forma dinâmica e estática.
  - **Proibido:** neste modo, a porta é incapaz de registrar e remover os registros de VLANs dinamicamente, e pode transmitir apenas as informações da VLAN 1.

SEGURANÇA

O menu Segurança é utilizado para fornecer e configurar diversas medidas de proteção para a segurança da rede. Este menu possui 8 submenus: *Prevenção de ataque, Ferramentas, Proteção DDoS, Loopback, STP, Controle de acesso, IGMP e MLD.*

Prevenção de ataque

O submenu Prevenção de ataque possui funcionalidades que visam prevenir ataques contra a rede, fornecendo maior segurança e confiabilidade aos dados trafegados. Este submenu possui outros 4 submenus: *Inspeção ARP, Segurança de porta, DHCP snooping e Proteção de CPU.*

O protocolo ARP (*Address Resolution Protocol*) é utilizado para analisar e mapear os endereços IP com seus respectivos endereços MAC, possibilitando assim a entrega dos pacotes aos seus destinos corretamente. Desta forma, o endereço IP de destino contido em um pacote precisa ser traduzido para o endereço MAC correspondente, formando assim a Tabela ARP. Quando um computador se comunica com outro, o protocolo ARP funciona conforme a explicação a seguir:

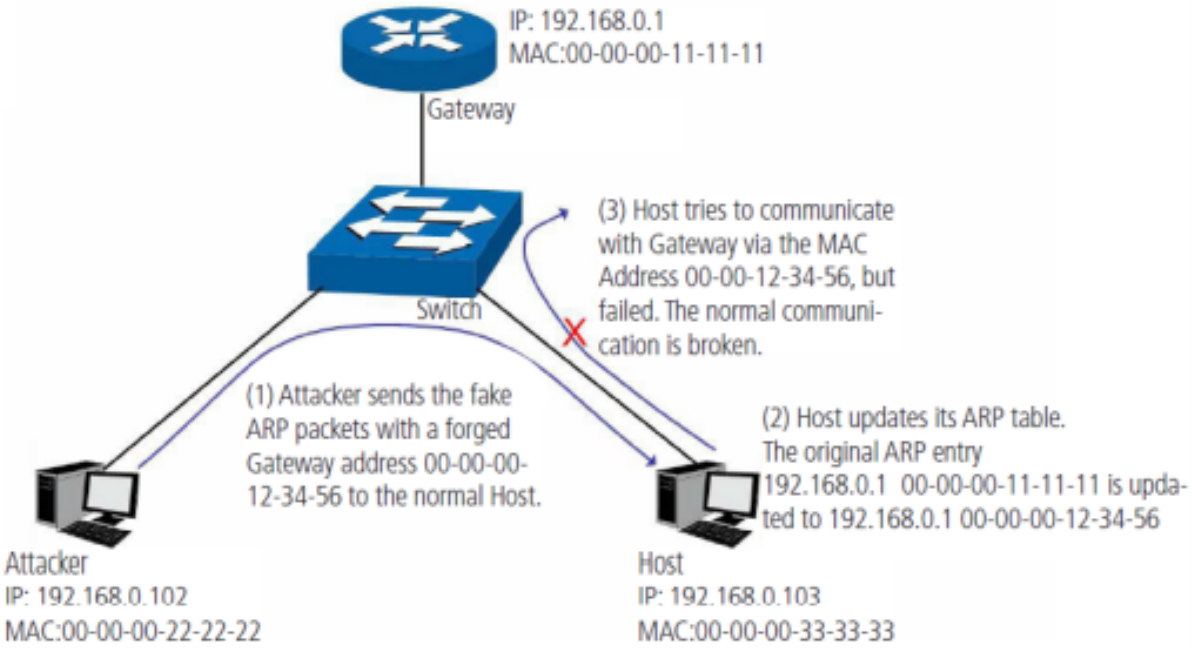
1. Suponha que há dois computadores pertencentes a mesma rede: computador A e o computador B. Para que o computador A possa enviar pacotes para o computador B, o computador A verifica se em sua tabela ARP há o relacionamento entre o endereço IP e o endereço MAC do computador B, caso possua, o pacote será transmitido diretamente ao computador B, caso não possua, o computador A transmitirá solicitações ARP em broadcast para a rede
2. Quando um pacote de solicitação ARP é transmitido em broadcast, todos os computadores pertencentes a mesma rede, visualizarão este pacote, no entanto apenas o computador B responderá ao pedido, pois o endereço IP contido na solicitação ARP corresponderá com seu próprio endereço IP. Então o computador B enviará ao computador A um pacote de resposta contendo seu endereço MAC.
3. Ao receber o pacote de resposta ARP, o computador A adiciona o endereço IP e o endereço MAC do computador B em sua tabela ARP, para que os próximos pacotes com destino ao computador B sejam encaminhados diretamente ao destino correto.

De acordo com essa explicação, o protocolo ARP auxilia na comunicação entre os computadores em uma mesma rede ou ainda no acesso a redes externas através do uso do gateway. Assim, ataques de falsificação ARP, tais como *Imitating gateway, Cheating gateway, Cheating terminal Hosts e ARP flooding attack*, ocorrem com frequência em redes de grandes dimensões.

Observe a seguir a explicação de alguns destes ataques:

- **Imitating gateway**

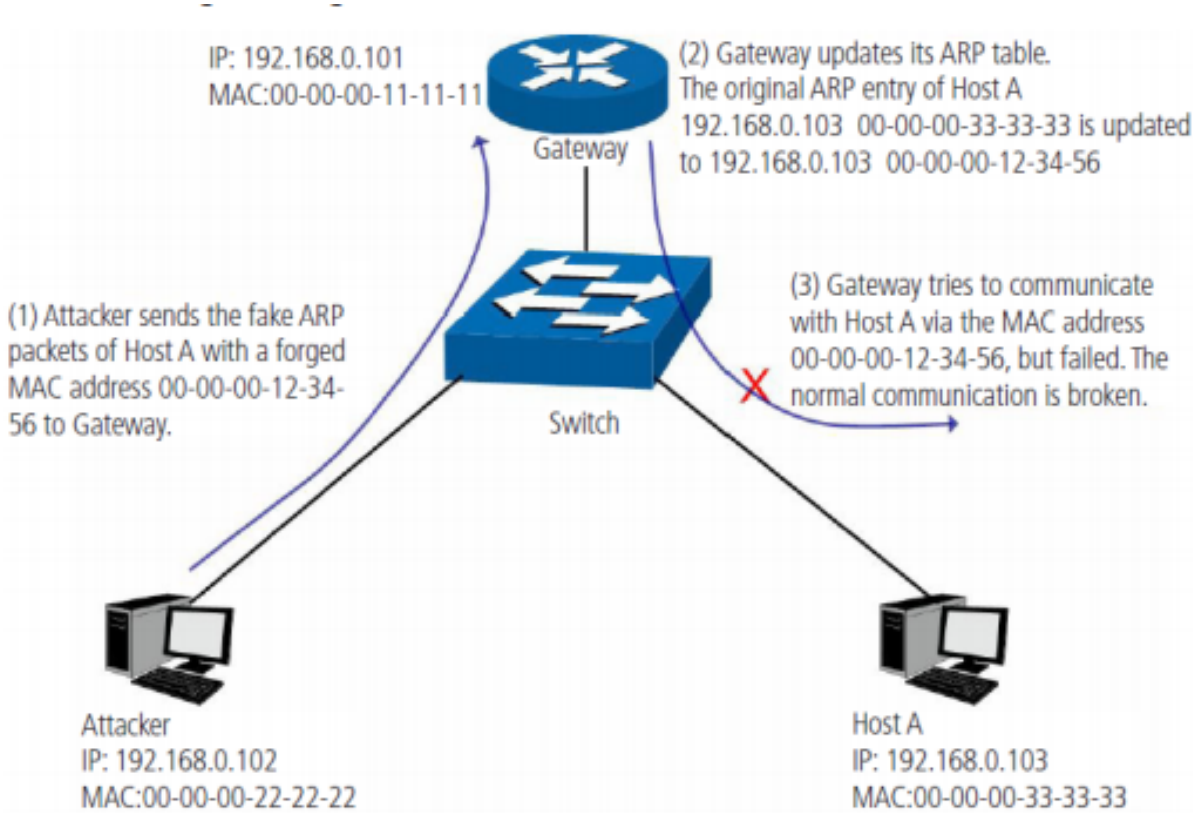
  O atacante envia um endereço MAC falso de um gateway para um determinado computador na rede, em seguida este computador atualizará automaticamente a sua tabela ARP, fazendo com que o computador não acesse a rede de forma normal. O Imitating gateway está sendo ilustrado na figura a seguir:



A figura anterior mostra o atacante enviando pacotes ARP falsificados com o endereço MAC do gateway forjado para um determinado computador na rede, em seguida, este computador atualizará sua tabela ARP automaticamente. Quando o computador tentar se comunicar com outro computador localizado em uma rede externa, ele irá enviar pacotes com o endereço MAC de destino errado, resultando na perda da comunicação.

- **Cheating gateway**

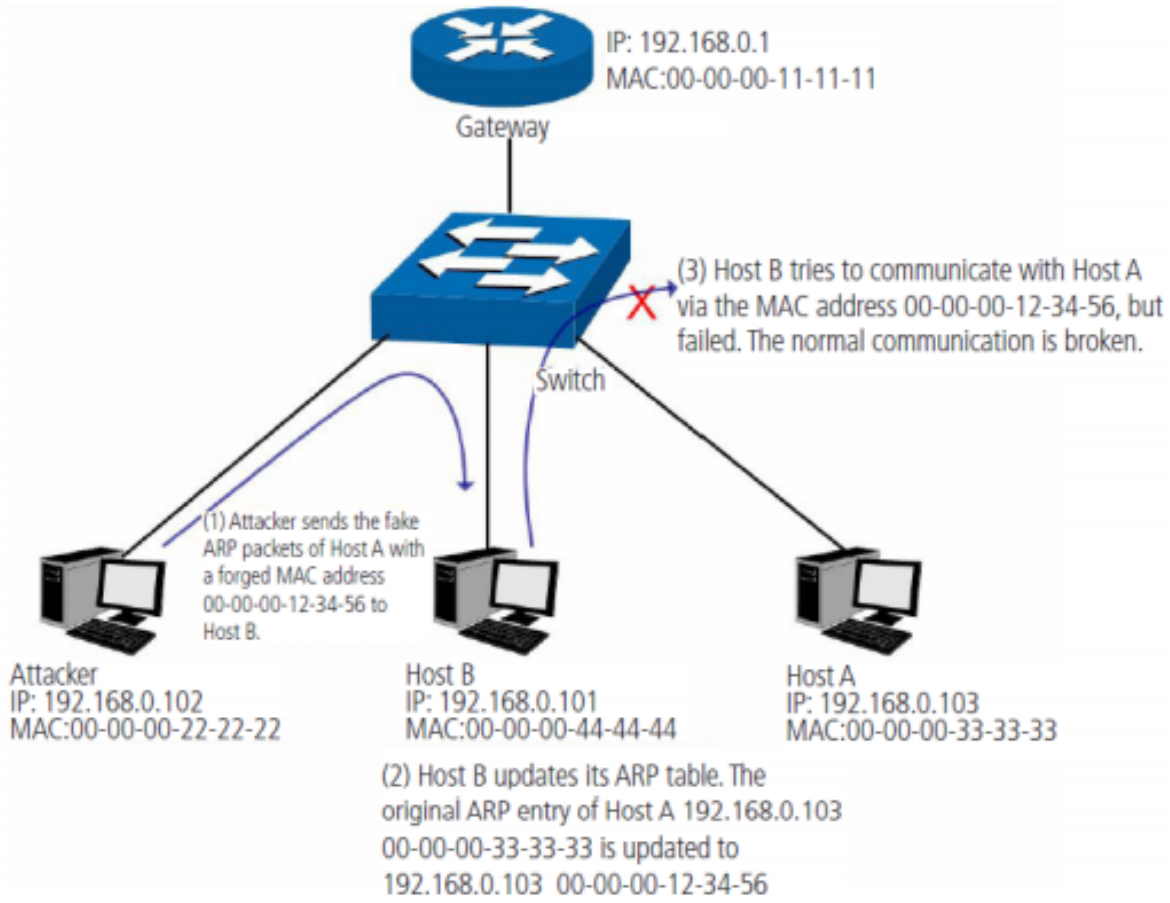
  O atacante envia um endereço MAC falso de um computador para o gateway da rede, em seguida, este gateway atualizará sua tabela ARP, fazendo com que o gateway não consiga responder as solicitações deste computador. O Cheating gateway é ilustrado na figura a seguir:



A figura anterior mostra o atacante enviando pacotes ARP falsificados para o gateway da rede, em seguida, este gateway atualizará sua tabela ARP automaticamente. Quando o gateway tentar responder a alguma solicitação do computador correto, o gateway irá enviar pacotes com o endereço MAC de destino errado, resultando na perda da comunicação.

- **Cheating terminal host**

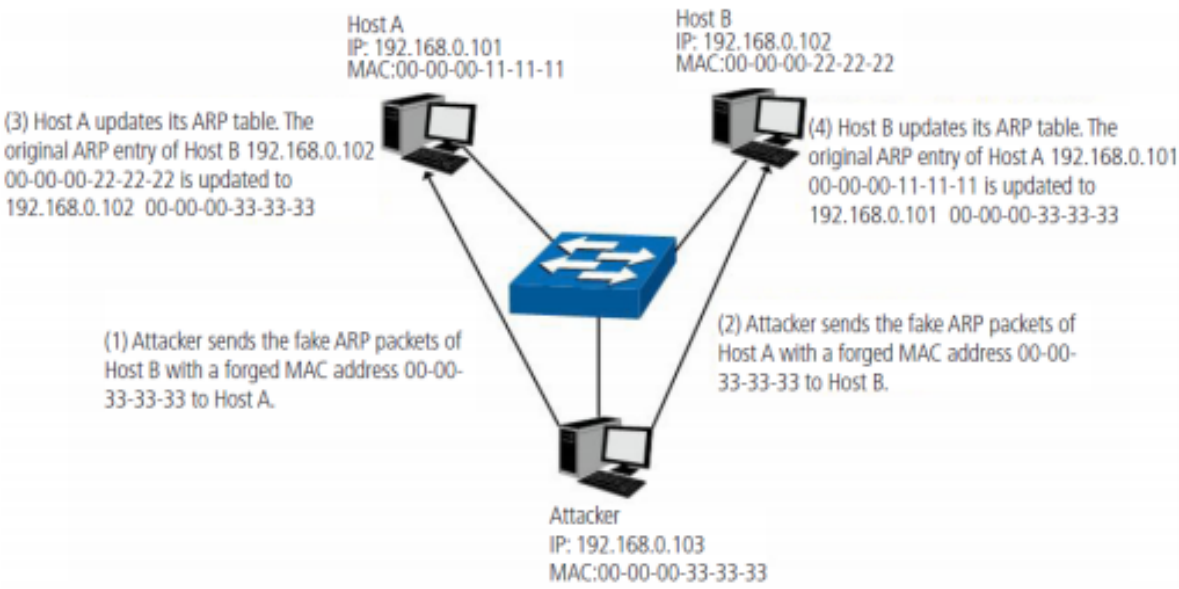
  O atacante envia um endereço MAC falso de um computador para outro computador da rede, fazendo com que estes computadores que estão na mesma rede não se comuniquem. O Cheating terminal hosts é ilustrado na figura a seguir:



A figura anterior mostra o atacante enviando pacotes ARP falsificados do computador A para o computador B, fazendo com que a tabela ARP do computador B seja atualizada automaticamente. Quando o computador B tentar se comunicar com o computador A, o computador B enviará pacotes com o endereço MAC de destino errado, resultando na falha da comunicação

- **Man-In-The-Middle attack**

  O atacante envia continuamente pacotes ARP falsificados para os computadores da rede. Quando estes computadores tentam se comunicar, eles enviarão pacotes para o atacante de acordo com a sua tabela ARP falsificada. Assim o atacante pode obter e processar os pacotes antes de encaminhá-los a seus destinos corretos. O Man-In-The-Middle attack é ilustrado na figura a seguir:



Suponha que existam 3 computadores conectados na rede através de um switch.

- **Computador A:** o seu endereço IP é 192.168.0.101 e o endereço MAC é 00-00-00-11-11-11.
- **Computador B:** o seu endereço IP é 192.168.0.102 e o endereço MAC é 00-00-00-22-22-22.
- **Atacante:** o seu endereço IP é 192.168.0.103 e o endereço MAC é 00-00-00-33-33-33.

1. Primeiramente, o atacante envia pacotes de respostas ARP falsificados;
2. Ao receber os pacotes de respostas ARP, os computadores A e B atualizam suas tabelas ARP;
3. Quando o computador A tentar se comunicar com o computador B, ele enviará os pacotes com o endereço MAC de destino falso, ou seja, o endereço MAC de destino do pacote está endereçado para o atacante;
4. Após receber e processar os pacotes dos computadores A e B, o atacante encaminha os pacotes para o endereço MAC correto, fazendo com que os computadores A e B não percebam que suas mensagens estão sendo interceptadas;
5. O atacante continua enviando pacotes ARP falsificados, mantendo a tabela ARP dos computadores A e B erradas.

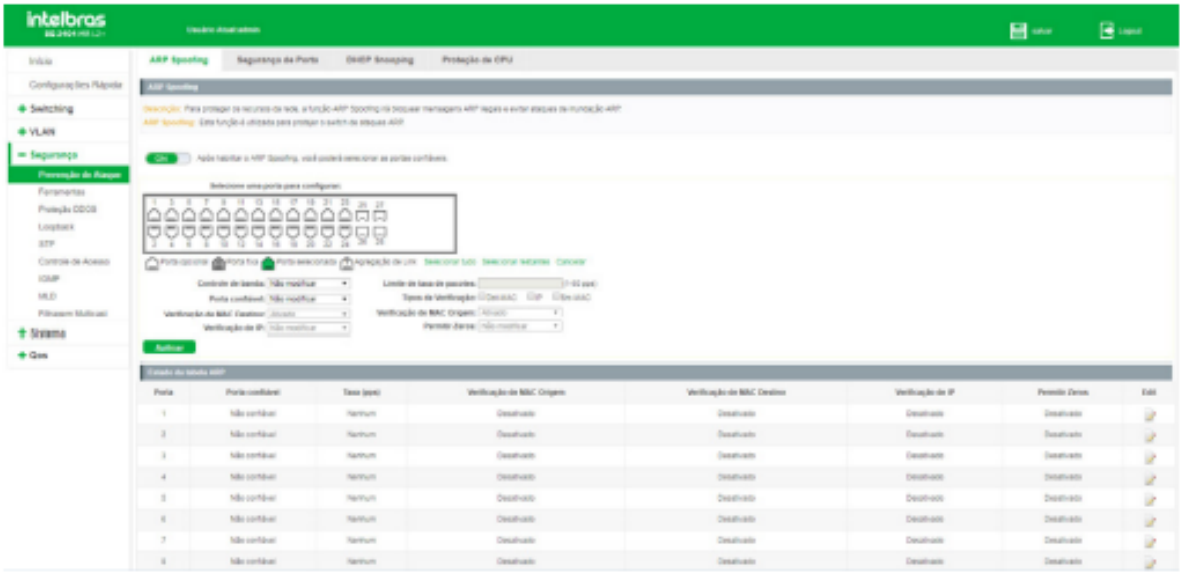
Na visão dos computadores A e B, os pacotes estão sendo enviados diretamente de um para o outro. Mas na verdade, há um outro computador roubando informações durante o processo de comunicação. Esse tipo de ataque ARP é chamado de Man-In-The-Middle.

- **ARP flooding attack**

  O atacante transmite uma quantidade muito grande de pacotes ARP falsificados em um segmento da rede, ocupando muita largura de banda, resultando em uma queda no desempenho da rede. O gateway aprende os endereços IPs/MAC falsificados e atualiza sua tabela ARP, como resultado, a tabela ARP do gateway é totalmente ocupada pelas entradas falsas, tornando-se incapaz de aprender os novos endereços dos computadores verdadeiros, fazendo com que estes não tenham acesso a rede externa.

Inspeção ARP

A função Inspeção ARP provê meios para detecção de pacotes ARP ilegais, podendo assim evitar ataques ARP na rede, conforme os exemplos mostrados acima. Para configurar a função Inspeção ARP é necessário primeiramente acessar o menu Segurança **>** Prevenção de ataque **>** Inspeção ARP e clicar sobre o ícone (OFF), alterando o status da funcionalidade para (ON) e habilitando o menu de configurações conforme imagem a seguir:



Após habilitar a função Inspeção ARP e carregar a imagem acima, selecione as portas a partir do painel de portas ou através do ícone (EDITAR) e configure-as de acordo com as seguintes opções:

- **Controle de banda:** configura a taxa limite de pacotes ARP.
- **Confiança:** configura a porta como sendo de confiança.
- **Verificação de MAC destino:** configura a verificação do MAC de destino do pacote. Se não for válido o pacote será descartado.
- **Verificação de IP:** configura a verificação do IP do pacote. A requisição será descartada se o IP for broadcast, multicast ou zerado e se o IP for inválido.
- **Limite de taxa de pacotes:** configure o limite de pacotes ARP.
- **Tipos de Verificação:** seleciona o tipo de verificação.
- **Verificação de MAC origem:** configura a verificação do MAC de origem do pacote. Se não for válido o pacote será descartado.
- **Permitir zeros:** faz com que requisições com IP zerado sejam aceitos ou não.

Segurança de porta

Ataques como o *ARP flooding attack*, por exemplo, podem encher por completo a tabela de endereços MAC do switch com endereços falsos. Este ataque poderia tornar o switch incapaz de aprender MACs de computadores verdadeiros, impedindo que estes computadores tenham acesso à rede. A função Segurança de porta impede que um ataque deste tipo encha por completo a tabela de endereços MAC do switch, limitando a quantidade de MACs aprendidos por porta.

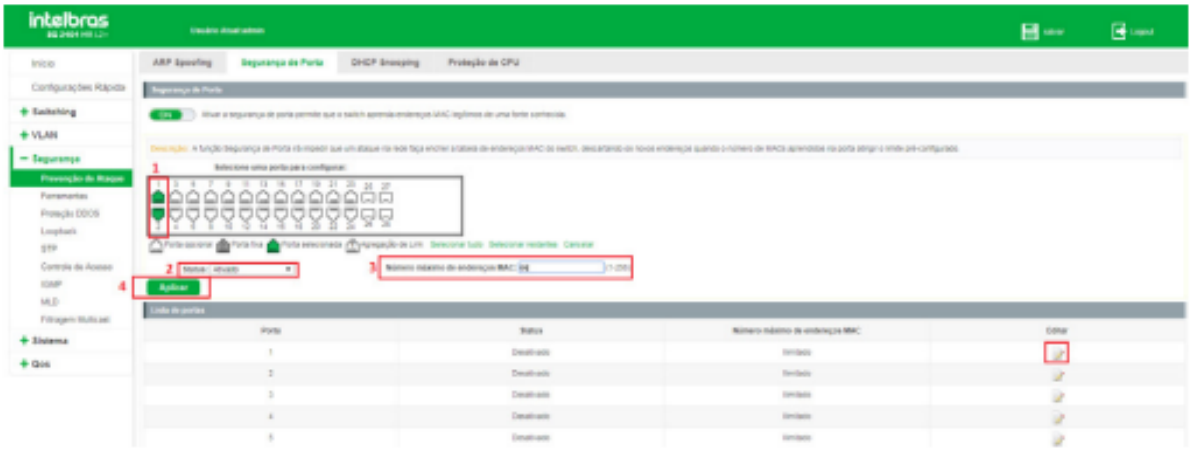
Configurando Segurança de porta

Para configurar a função Segurança de porta no switch, escolha o menu Segurança > Prevenção de ataque > Segurança de porta e siga as instruções a seguir:

1. Clique no ícone (EDITAR) da porta que deseja configurar ou selecione através do painel de portas;
2. Selecione o status administrativo:

   - **Ativado:** para ativar a função na porta.
   - **Desativado:** para desativar a função na porta.

3. Configure o número máximo de endereços MAC a serem aprendidos na porta (1 a 256);
4. Clique em Salvar.



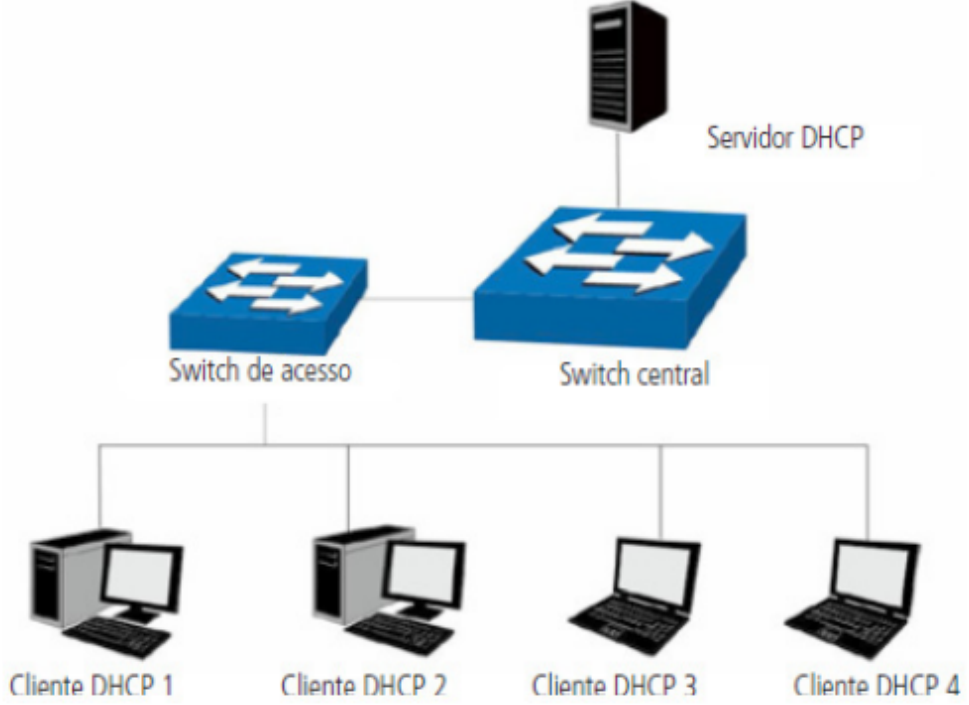
DHCP

Atualmente as redes estão ficando cada vez maiores e mais complexas. As configurações de endereços IP e parâmetros de redes utilizados devem ser analisados e atualizados com frequência para permitir o perfeito funcionamento dos computadores e recursos da rede. O protocolo DHCP (*Dynamic Host Configuration Protocol*) foi desenvolvido baseado no protocolo BOOTP e é utilizado para otimizar a situação mencionada acima.

No entanto, durante o processo de funcionamento do DHCP, não existe nenhum mecanismo de autenticação entre o cliente e o servidor e caso houver vários servidores DHCP na rede, poderão existir conflitos de endereços IP, gateways, etc., prejudicando a performance da rede, além de poder ocorrer falha na segurança, caso houver um usuário mal-intencionado.

Princípio de funcionamento do servidor DHCP

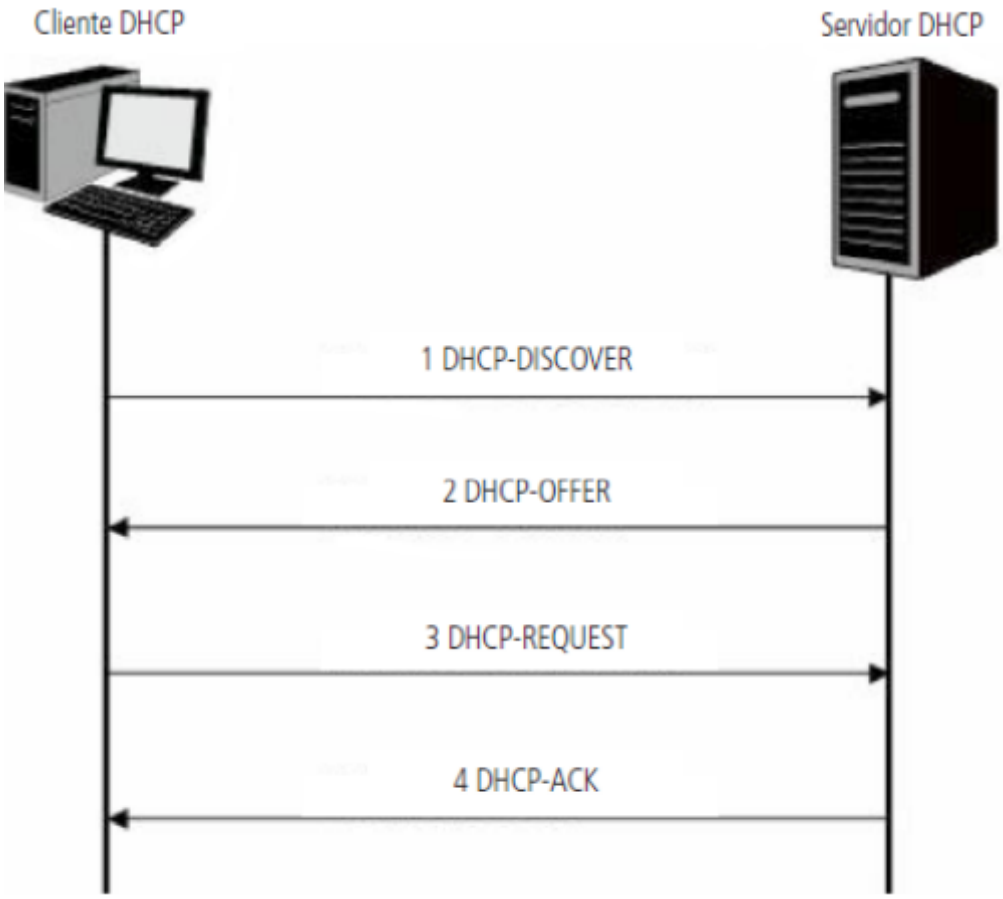
O DHCP funciona baseado na comunicação cliente/servidor. O cliente requisita informações para sua configuração e o servidor atribui as informações de configuração, como por exemplo, o endereço IP. Um servidor DHCP pode atribuir endereços IPs para vários clientes, como é ilustrado na figura a seguir:



O servidor DHCP fornece três métodos de atribuição de endereços IPs, são eles:

- **Manual:** permite ao administrador vincular o endereço IP estático para um cliente específico (ex. servidor WWW).
- **Automático:** o servidor DHCP atribui os endereços IPs para os clientes sem tempo de expiração.
- **Dinâmico:** o servidor DHCP atribui o endereço IP com um determinado tempo de expiração. Quando o tempo para o endereço IP expirar, o cliente terá que solicitar um novo endereço IP para o servidor DHCP.

A maioria dos clientes obtêm endereços IP dinamicamente, como ilustrado na figura a seguir:



1. **DHCP-DISCOVER:** o cliente transmite em broadcast o pacote DHCP-DISCOVER para descobrir o servidor DHCP.

2. **DHCP-OFFER:** ao receber pacotes DHCP-DISCOVER, o servidor DHCP, escolhe um endereço IP com base em uma faixa com prioridades e responde ao cliente com o pacote DHCP-OFFER contendo o endereço IP e algumas outras informações.
3. **DHCP-REQUEST:** em uma situação em que há vários servidores DHCP enviando pacotes DHCP-OFFER, o cliente só responderá ao primeiro pacote recebido e transmitirá o pacote DHCP-REQUEST, que inclui o endereço IP recebido do pacote DHCP-OFFER.
4. **DHCP-ACK:** uma vez que um pacote DHCP REQUEST é transmitido, todos os servidores DHCP na LAN podem recebê-lo. No entanto, apenas o servidor requisitado processará o pedido. Se o servidor DHCP confirmar a atribuição desse endereço IP para o cliente, ele enviará um pacote DHCP-ACK de volta para o cliente. Caso contrário, o servidor irá enviar pacotes DHCP-NAK, recusando atribuir esse endereço IP para o cliente.

Option 82

Os pacotes DHCP, são classificados de oito maneiras, com base no formato dos pacotes BOOTP. A diferença entre o DHCP e BOOTP é o campo Option. O campo Option do DHCP, é utilizado para expandir a função do DHCP, por exemplo, o DHCP pode transmitir informações de controle e parâmetros da configuração da rede através do campo Option.

Para maiores detalhes do campo Option do DHCP, consulte a **RFC 2132**.

A opção 82 do campo Option registra a localização dos clientes DHCP. Ao receber um pacote DHCP-REQUEST, o switch adiciona a opção 82 no campo Option no pacote DHCP e transmite o pacote para o servidor DHCP.

O administrador da rede pode ter o conhecimento da localização do cliente DHCP através do campo Option 82, obtendo maior controle e segurança no gerenciamento dos clientes DHCP. O servidor DHCP que suporta o campo Option 82, pode definir uma política de distribuições dos endereços IPs e outros parâmetros desejados, proporcionando uma distribuição mais flexível dos endereços.

O campo Option 82 pode conter no máximo 255 sub-opções. Uma vez que o campo Option 82 é definido, pelo menos uma das sub-opções deve ser configurada. O switch suporta duas sub-opções: Circuit-ID e Remote ID. Como não existe um padrão universal para o campo Option 82, diferentes implementações de diferentes fabricantes podem existir. Para esse switch, as sub-opções são definidas a seguir.

Circuit-ID é definido para ser o número da porta do switch que recebe os pacotes de solicitação DHCP juntamente com o VLAN ID.

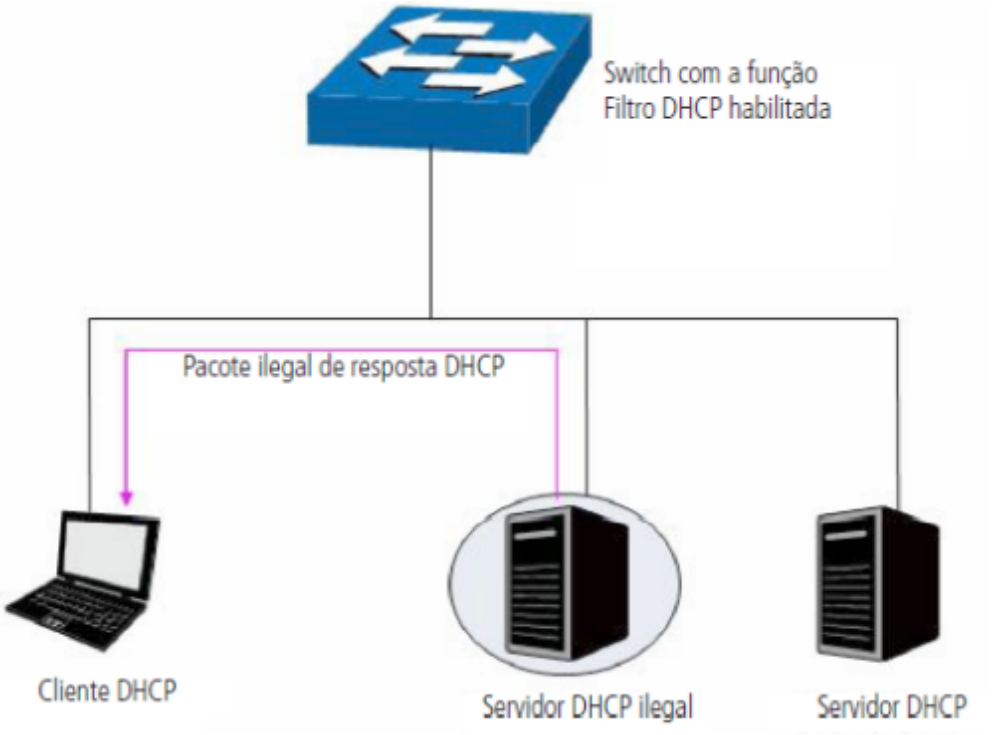
Remote ID é definido para ser o endereço MAC dos clientes DHCP que foram obtidos através dos pacotes DHCP Request.

DHCP cheating attack

Durante o processo de funcionamento do DHCP, geralmente não há nenhum mecanismo de autenticação entre o cliente e servidor. Se houver vários servidores DHCP na rede, poderá haver certa confusão e insegurança na rede. Um dos casos mais comuns que podem ocorrer está listado a seguir:

1. O servidor DHCP ilegal é configurado manualmente por um usuário comum por engano.

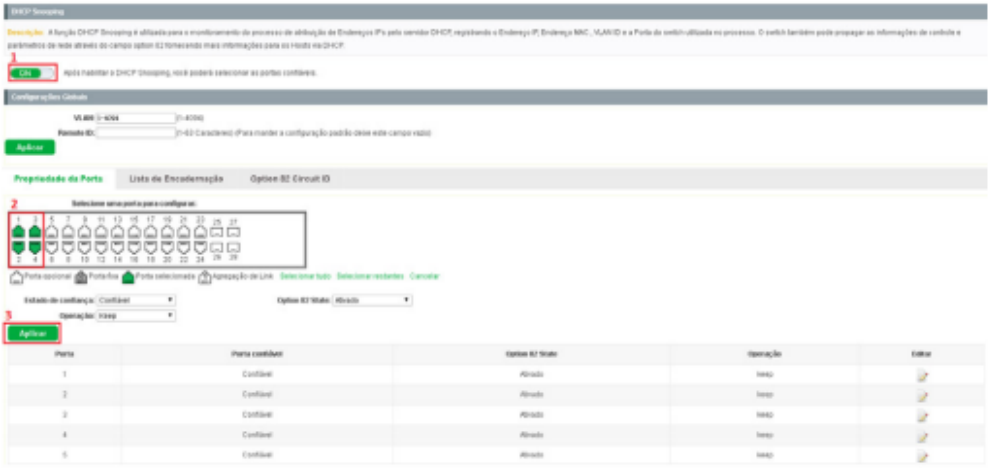
2. Usuários mal-intencionados podem esgotar os endereços IPs do servidor DHCP e fingirem ser um servidor DHCP para atribuir os endereços IPs e demais informações de rede para os clientes. Por exemplo: um usuário mal-intencionado utilizou o servidor DHCP para atribuir uma modificação no servidor DNS, de modo que os usuários que irão acessar sites de comércio eletrônico digitarão suas senhas achando que é o site real. A figura a seguir ilustra a DHCP cheating attack.



DHCP Snooping

A função DHCP snooping permite que apenas as portas configuradas como confiáveis possam receber pacotes de servidores DHCP, garantindo assim que os clientes DHCP recebam pacotes somente de servidores DHCP confiáveis, ou seja, serão descartados pelo switch todos os pacotes DHCP de servidores DHCP recebidos em portas que não estejam configuradas como portas confiáveis. Para configurar a função DHCP snooping, escolha o menu Segurança > Prevenção de ataque > DHCP snooping e siga as instruções a seguir:

1. Clique sobre o ícone (OFF) , alterando o status da funcionalidade para (ON) e habilitando o menu de configurações;
2. Selecione as portas confiáveis através do painel de portas; somente portas confiáveis poderão receber pacotes de servidores DHCP;
3. Clique em Aplicar



Configurações globais do DHCP Snooping

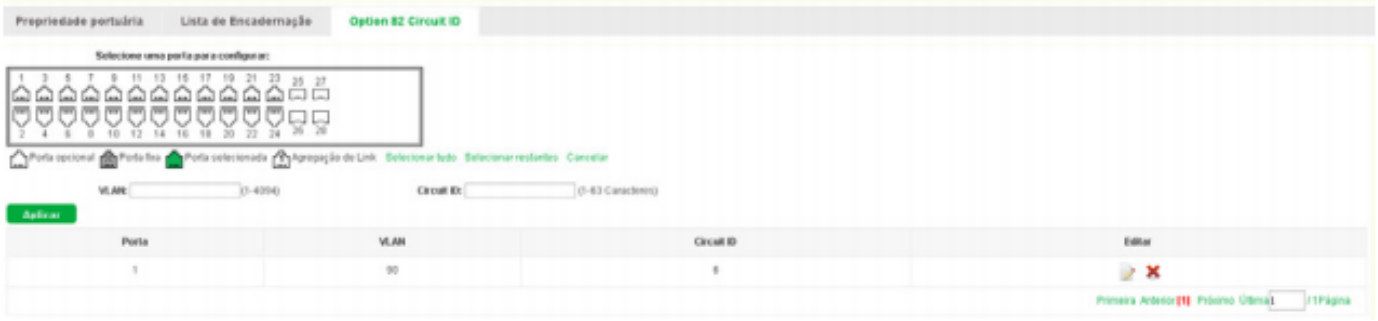
- **VLAN:** digite a VLAN que deseja aplicar as configurações.
- Remote ID: digite a sub-opção Remote ID para personalização do campo Option 82. Para manter a configuração padrão deixe este campo vazio.
- Estado de confiança: selecione o estado de confiança:
  - **Confiável:** permite que a porta tenha um servidor DHCP
  - **Não confiável:** permite ter apenas clientes DHCP conectados.
- **Option 82 State:** selecione Ativado/Desativado para habilitar ou desabilitar a função Option 82.
- **Operação:** selecione a operação para o campo Option 82 dos pacotes DHCP-REQUEST enviados dos clientes.
  - **Keep:** é utilizado para manter o campo Option 82 dos pacotes DHCP.
  - **Replace:** é utilizado para substituir o campo Option 82 dos pacotes DHCP com a informação que foi definida no switch.
  - **Drop:** é utilizado para descartar os pacotes DHCP incluindo o campo Option 82.

Lista de IPs atribuídos

Exibe as informações sobre a entrega dos IPs pelo servidor DHCP.

- **Porta:** exibe a porta que foi entregue o endereço IP.
- **VLAN ID:** exibe a VLAN que foi utilizada.
- **Endereço MAC:** exibe o endereço MAC do cliente.
- **Endereço IP:** exibe o endereço IP entregue ao cliente.
- **Máscara:** exibe a máscara.
- **Tipo:** exibe o método onde foi capturada a informação.
- **Tempo de alocação(ões):** exibe o tempo em segundos que o IP foi atribuído ao cliente.

Option 82 Circuit-ID



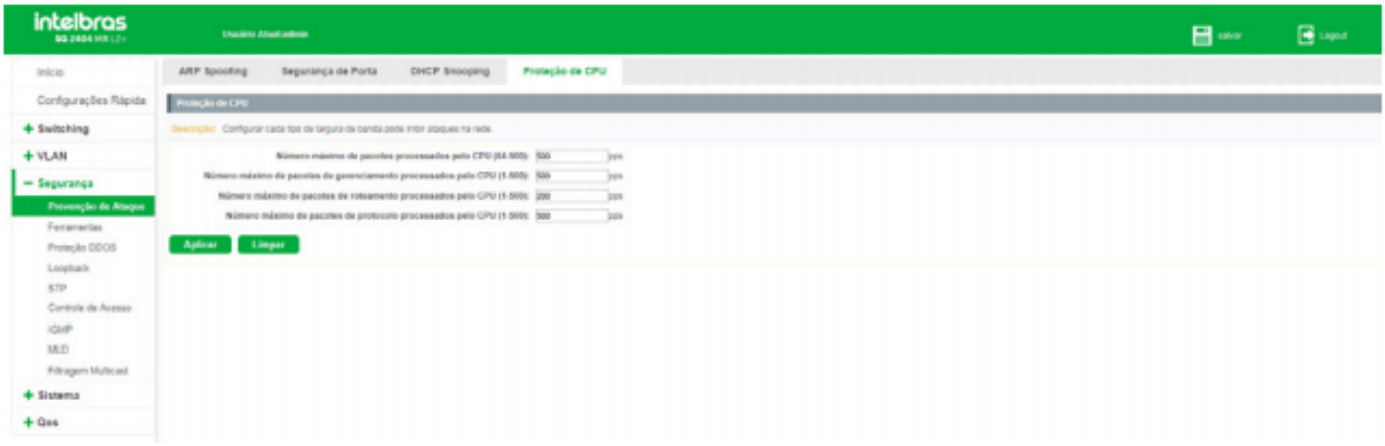
1. Selecione as portas que deseja configurar;
2. **VLAN:** indique a VLAN;
3. **Circuit-ID:** digite a informação desejada que o switch encaminhará no campo Option 82;
4. Clique em Aplicar.

Proteção de CPU

A função Proteção de CPU permite ao administrador do sistema limitar a taxa de pacotes transmitidos por determinados itens da CPU do switch.

Para configurar a Proteção de CPU, escolha o menu Segurança > Prevenção de ataque > Proteção de CPU e siga as instruções a seguir.

1. Número máximo de pacotes processados pelo CPU (64-500);
2. Número máximo de pacotes de gerenciamento processados pelo CPU (1-500);
3. Número máximo de pacotes de roteamento processados pelo CPU (1-500);
4. Número máximo de pacotes de protocolo processados pelo CPU (1-500);
5. Clique em Aplicar.



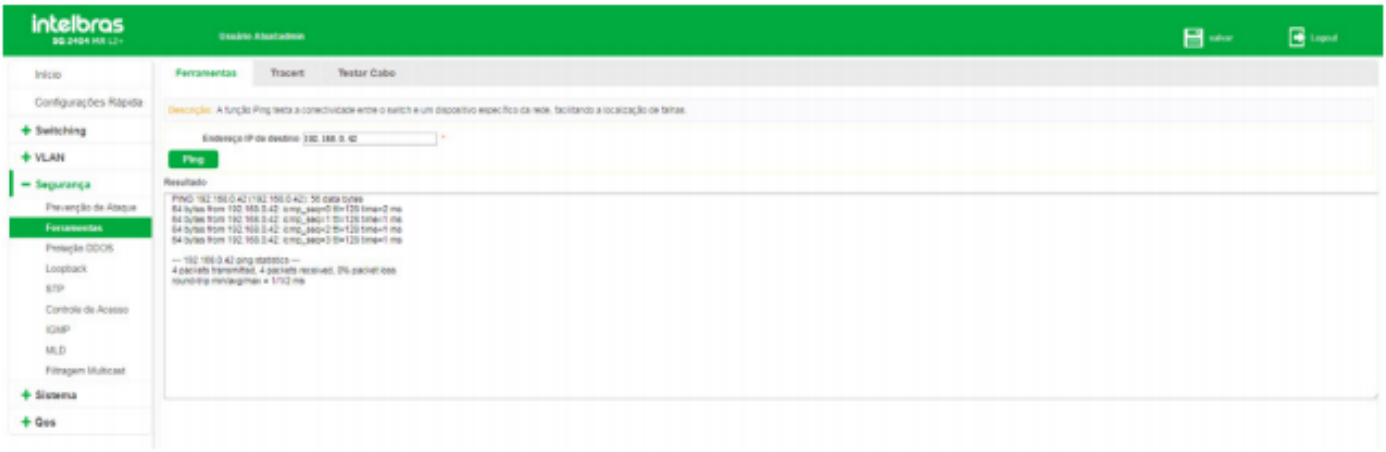
Ferramentas

O submenu Ferramentas possui ferramentas para diagnóstico de possíveis problemas na rede. Este submenu possui outros três submenus. São eles: *Ferramentas, Tracert e Testar cabo*.

Ferramentas

A guia Ferramentas realiza a função Ping. Ela testa a conectividade entre o switch e um dispositivo específico da rede, facilitando assim a localização de falhas e as intervenções em caso de problemas. Para executar um ping para um host na rede, escolha o menu Segurança > Ferramentas > Ferramentas e siga as instruções a seguir:

1. Digite o endereço IP do host de destino;
2. Clique em Ping;
3. Aguarde a execução e observe o resultado.

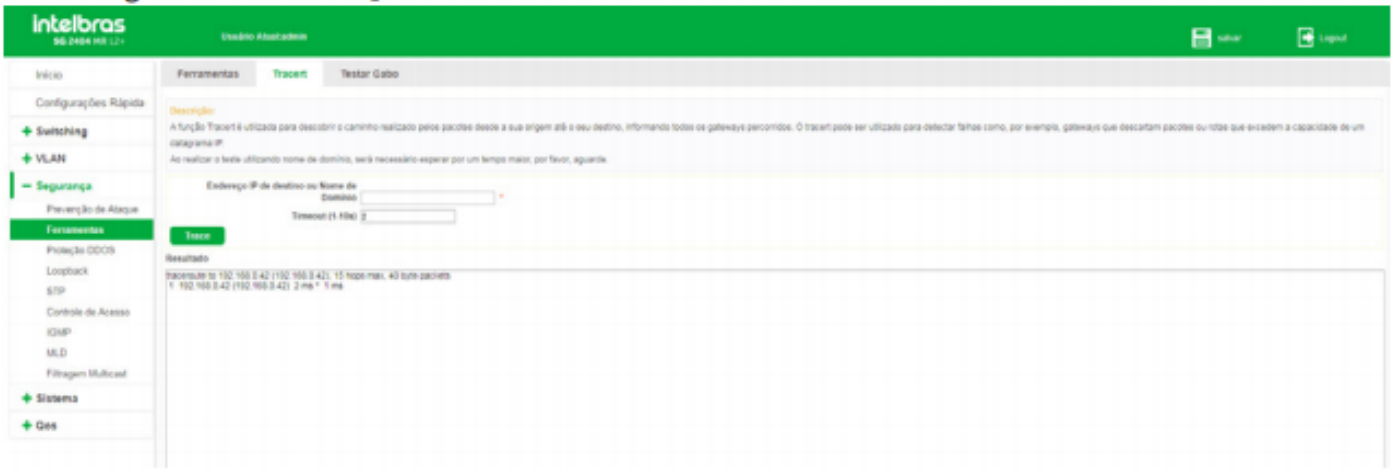


Tracert

A função Tracert é usada para descobrir o caminho feito pelos pacotes desde sua origem até o seu destino, informando todos os gateways percorridos. Ele é usado para testes, medidas e gerenciamento da rede. O Tracert pode ser utilizado para detectar falhas como, por exemplo, gateways que descartam pacotes ou rotas que excedem a capacidade de um datagrama IP.

Para executar um Tracert para determinado host, escolha o menu Segurança > Ferramentas > Tracert e siga as instruções a seguir:

1. Digite o endereço IP ou nome do host de destino;
2. Digite o timeout em segundos;
3. Clique em Ping;
4. Aguarde a execução e observe o resultado.

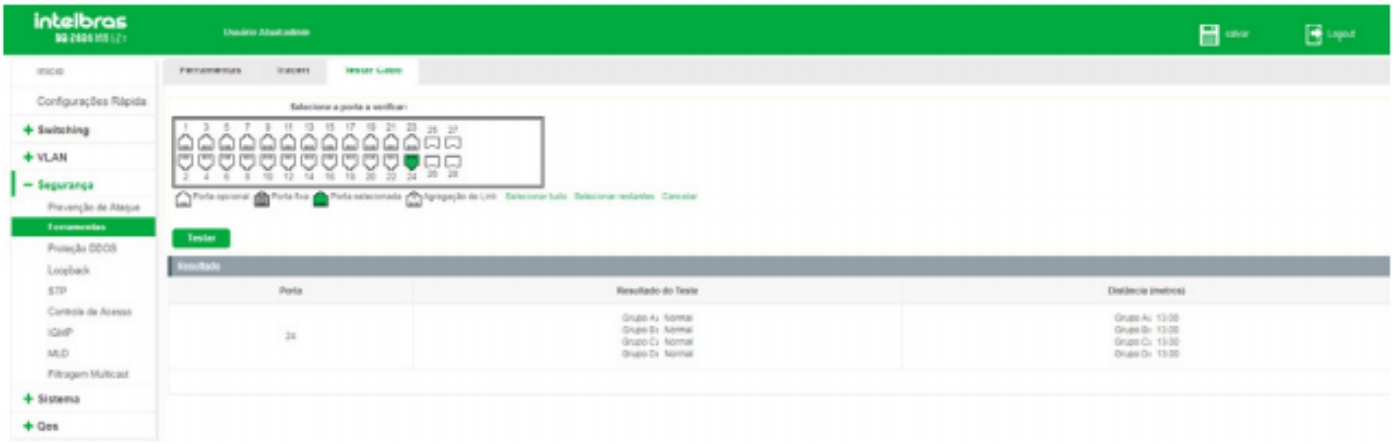


Testar cabo

A função Testar cabo é utilizada para testar o status da conexão do cabo conectado ao switch, o que facilita para localizar e diagnosticar os problemas da rede.

Para utilizar esta função, escolha o menu Segurança > Ferramentas > Testar cabo e siga as instruções a seguir:

1. Selecione a porta que deseja testar;
2. Clique em Testar;
3. Aguarde a execução e observe o resultado



Obs: O comprimento exibido é o comprimento dos pares internos do cabo, não do cabo físico em si. Sendo assim, o resultado é apenas para sua referência.

Proteção DDoS

Ataques DDoS (*Distributed Denial of Service*) ocasionam lentidão na rede, chegando muitas vezes a parar com o funcionamento do switch, devido a inúmeras requisições maliciosas enviadas pelo atacante. Com esta função habilitada, o switch analisa campos específicos dos pacotes recebidos, podendo permitir ou negar os serviços solicitados, evitando ataques de negação de serviço (DDoS).

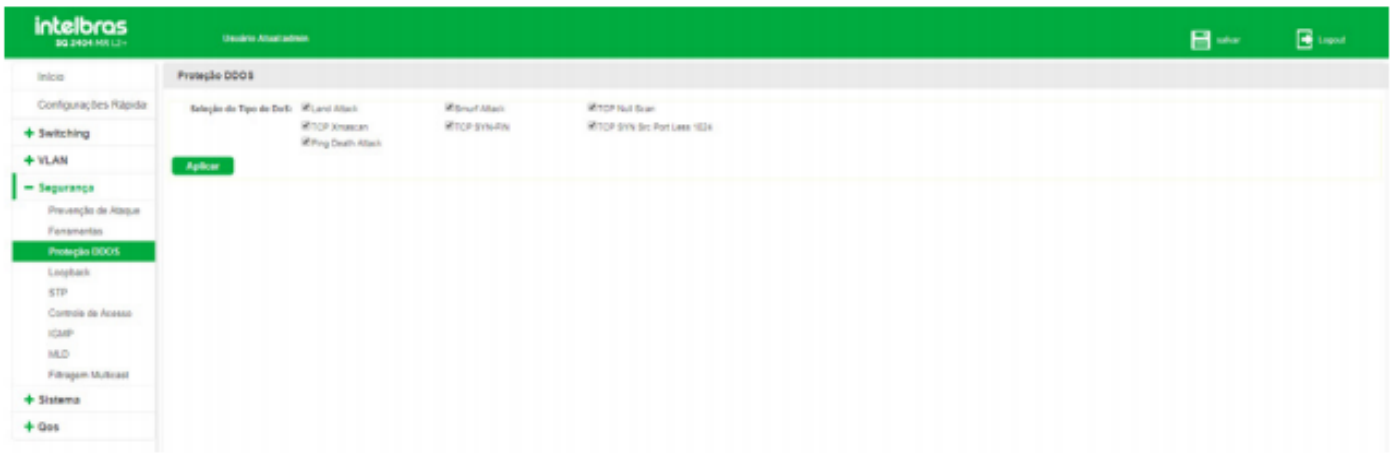
O switch pode detectar alguns tipos de ataques DDoS, conforme mostrado na tabela a seguir:

Tipo de ataque DDoS	Descrição

Tipo de ataque DDoS	Descrição
Land Attack	O atacante envia um pacote TCP falso com a flag SYN habilitada para um host de destino. Uma vez que este pacote possua os campos endereço IP de origem e destino configurado de acordo com o endereço IP do host atacado, este host ficará preso em um loop infinito, afetando drasticamente o desempenho da rede.
TCP SYN-FIN	O atacante envia um pacote TCP com as flags SYN e FIN habilitadas. A flag SYN é utilizada para iniciar uma nova conexão, enquanto a flag FIN é utilizada para solicitar uma desconexão. Portanto o pacote deste tipo é ilegal. O switch pode se defender desse tipo de pacote
TCP Xmascan	O atacante envia o pacote TCP com as seguintes flags habilitadas: FIN, URG e PSH.
TCP Null Scan	O atacante envia o pacote TCP com todas as flags de controle como 0. Durante a conexão e a transmissão de dados, os pacotes com todos os controles definidos como 0 serão considerados pacotes ilegais.
TCP SYN Src Port Less 1024	O atacante envia um pacote TCP com a flag SYN habilitada para uma porta de origem menor que 1024.
Ping Death Attack	O atacante faz uma inundação na rede com pings em broadcast, impedindo que o switch responda as verdadeiras comunicações.
Smurf Attack	O atacante envia uma série de solicitações de pacote ICMP (PING) com um endereço IP de origem falsificado em broadcast. A maioria dos dispositivos em uma rede, por padrão, responderá a essas solicitações enviando uma resposta para o IP de origem. Com isso, o computador da vítima poderá ser inundado com o tráfego, impedindo a utilização da rede.

Para utilizar a função de Proteção DDoS, escolha o menu Segurança > Proteção DDoS e siga as instruções a seguir:

1. Selecione os tipos de ataque que deseja prevenir;
2. Clique em Aplicar.

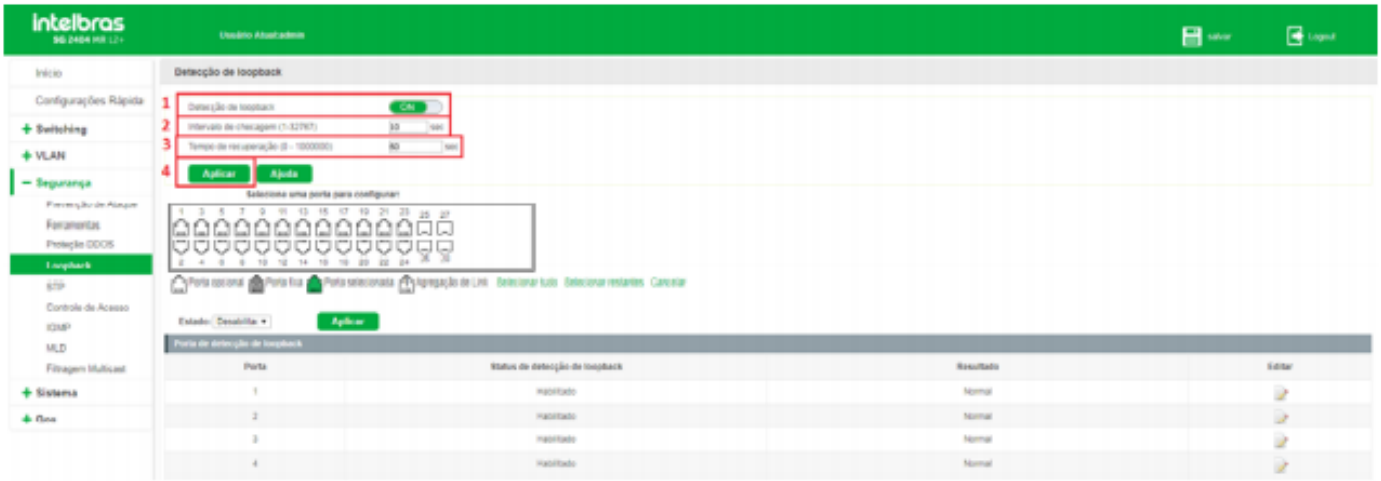


Loopback

Com o recurso Detecção de loopback habilitado, o switch pode detectar a ocorrência de looping em suas portas utilizando pacotes de detecção de autorretorno. Quando um loop é detectado, o switch poderá exibir um alerta ou bloquear a porta correspondente, conforme a configuração desejada na porta.

Para utilizar a função de Detecção de loopback, escolha o menu Segurança > Loopback e siga as instruções a seguir:

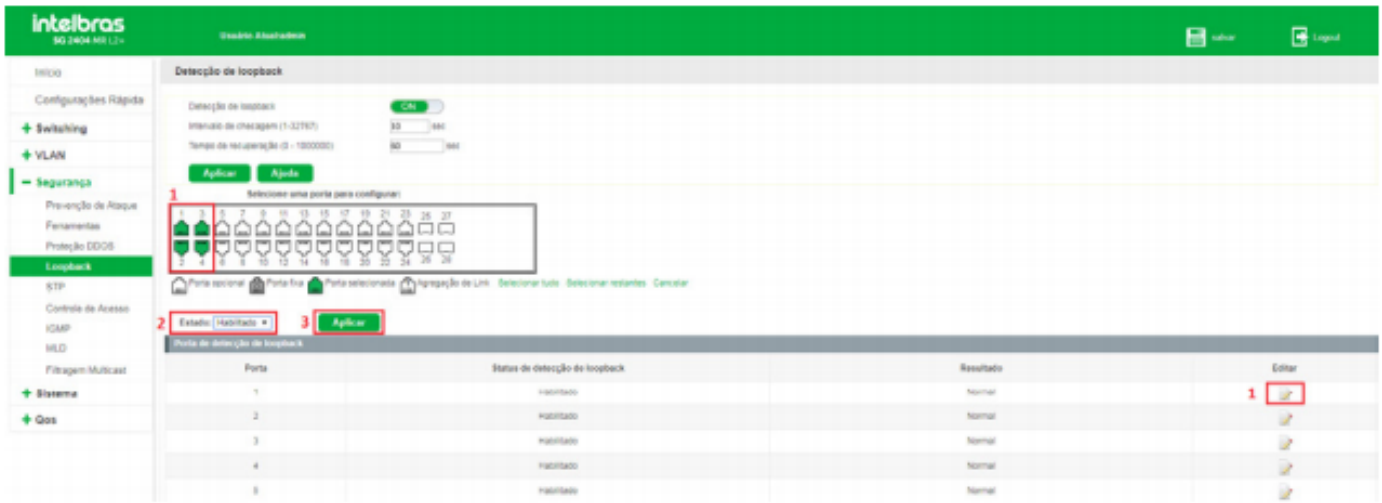
1. Clique no ícone para ativar a função, caso esteja desabilitada, ou no ícone caso queira desativar;
2. Digite o intervalo de tempo em que o switch tentará detectar loop em suas portas;
3. Digite o tempo para a tentativa de recuperação automática da porta quando um loop for detectado. O valor configurado é o intervalo de tempo, em segundos, que a porta faz a verificação da presença ou ausência de looping. Se for configurado o valor como 0 (zero) a porta é desativada na presença de loopback e não retorna ao funcionamento normal após a retirada do looping;
4. Clique em Aplicar.



Configurando portas com detecção de loopack

Para configurar a detecção de looping nas portas, escolha o menu Segurança > Loopback e siga as instruções a seguir:

1. Clique no ícone da porta que deseja configurar ou selecione através do painel de portas;
2. Selecione o estado da detecção de looping (Habilitado/Desabilitado);
3. Clique em Aplicar



A tabela exibida na página de detecção de loopback as seguintes informações:

1. **Porta:** exibe o número da porta do switch configurada.
2. **Status de detecção de loopback:** exibe o estado da configuração de detecção de loopback para a porta (Habilitado/Desabilitado).
3. **Resultado:** indica se foi detectado looping na porta ou não. Caso seja detectado looping, a porta será automaticamente desativada e será exibida a informação Loop-desligado no resultado da porta.

STP

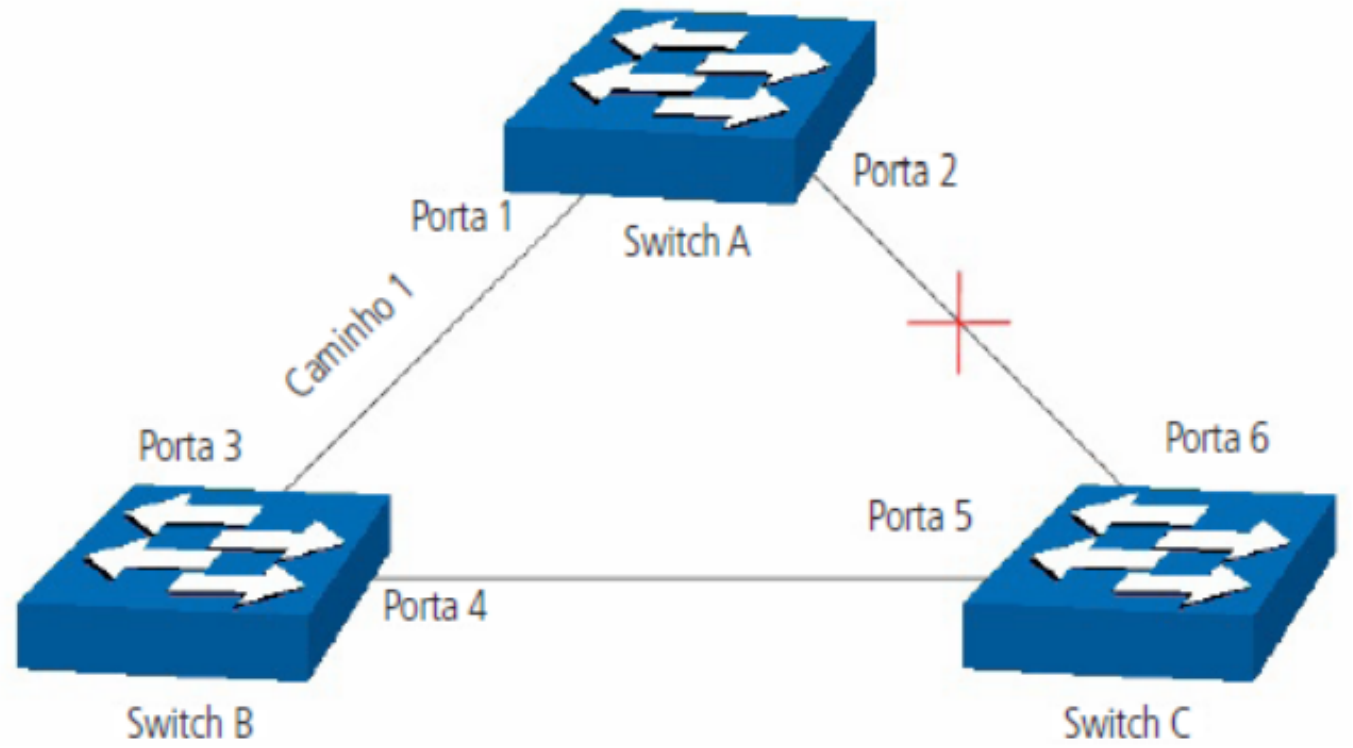
STP (*Spanning Tree Protocol*), pertence à norma IEEE 802.1d e assegura que haja somente um caminho lógico entre todos os destinos na camada de enlace em uma rede local, fazendo o bloqueio intencional dos caminhos redundantes que poderiam causar um loop. Uma porta é considerada bloqueada quando o tráfego da rede é impedido de entrar ou deixar aquela porta. Isto não inclui os quadros BPDU (*Bridge Protocol Data Unit*) que são utilizados pelo STP para impedir loops.

O BPDU é o quadro de mensagem trocada entre os switches que utilizam a função STP. Cada BPDU contém um campo chamado BID (*Bridge ID*) que identifica o switch que enviou o BPDU. O BID contém um valor de prioridade, o endereço MAC do switch de envio, e uma ID de Sistema Estendido opcional. Determina-se o valor o BID mais baixo através da combinação destes três campos.

Elementos STP

- **Bridge ID:** indica valor da prioridade e endereço MAC.
- **Root Bridge (switch referência):** indica o switch que possui o menor Bridge ID. O switch considerado Bridge Root serve como ponto de referência para todos os cálculos STP para garantir melhor desempenho e confiabilidade na rede.
- **Bridge designada:** indica o switch que possui o caminho com menor custo até a Bridge Root em cada segmento de rede. Os quadros BPDUs são encaminhados para o segmento de rede através dos switches definidos como Bridge Designada.
- **Custo do caminho root:** indica a soma de todos os custos de porta ao longo do caminho até a Bridge Root. O custo do caminho da Bridge Root é 0.
- **Prioridade da bridge:** a Prioridade da bridge pode ser ajustada para um valor no intervalo de 0 a 61440. O valor mais baixo da Prioridade da bridgepossui maior prioridade. O switch com a maior prioridade possui maior chance de ser escolhido como Bridge Root.
- **Porta do root (porta raiz):** indica a porta mais próxima (caminho com menor custo) para a Bridge Root. Por esta porta que os pacotes serão encaminhados para a Bridge Root.
- **Porta designada:** são todas as portas (não-raiz) que não são definidas como Portas root e que ainda podem encaminhar tráfego na rede.
- **Prioridade da porta:** a prioridade da porta pode ser ajustada em um intervalo de 0-255. O valor mais baixo para a Prioridade da porta possui maior prioridade. A porta com maior prioridade possui maior chance de ser escolhida como Porta root (porta raiz).
- **Custo do caminho:** indica o parâmetro para escolha do caminho do link STP. Ao calcular o custo do caminho, o STP escolhe os melhores caminhos entre as ligações redundantes.

O diagrama a seguir exibe o esboço de uma rede Spanning Tree. Os switches A, B e C estão conectados. Após a geração do STP, o switch A é escolhido como a Bridge Root, o caminho da porta 2 para porta 6 ficará bloqueado.



- **Switches:** switch A é a Bridge root da rede e o switch B é a bridge designada do switch C.
- **Portas:** a porta 3 é a Porta root (porta raiz) do switch B e a porta 5 é a Porta root (porta raiz) do switch C; a porta 1 é a porta designada do switch A e a porta 4 é a porta designada do switch B; a porta 6 do switch C está bloqueada.
- Temporizadores STP
  - **Hello time:** especifica o intervalo de envio de pacotes BPDU. O valor pode variar de 1 à 10 segundos.
  - **Maximum age:** especifica o tempo máximo que o switch aguarda para remover sua configuração e iniciar uma nova eleição da Bridge root.
  - **Forward delay:** especifica o tempo para a porta alterar seu estado após uma alteração na topologia da rede.

Quando a regeneração do STP é causada por um mau funcionamento da rede ou até mesmo por uma alteração na topologia da rede, a estrutura do STP começará a realizar as alterações necessárias. No entanto, como os BPDUs da nova configuração não podem ser enviados pela rede de uma só vez, um loop somente ocorreria se o estado da porta estivesse diretamente no estado de encaminhamento. Portanto, o STP adota um mecanismo de estados de portas STP, isto é, a nova porta root e a porta designada começam a transmitir dados (estado de encaminhamento) após duas vezes o tempo do forward delay, o que garante que os novos BPDUs já tenham sido enviados para toda a rede

Princípio de comparação de quadros BPDU

Supondo dois BPDUs: *BPDUx e BPDUy*.

Se o ID da Bridge root do x é menor que a do y, x terá prioridade ao y.

Se o ID da Bridge root do x é igual a do y, mas o custo do caminho da bridge de x é menor do que a de y, x terá prioridade ao y.

Se o ID da Bridge root e o custo do caminho de x é igual ao de y, mas o ID da Bridge de x é menor que a de y, x terá prioridade ao y.

Se o ID da Bridge root, custo do caminho e ID da Bridge de x for igual ao de y, mas o ID da porta de x for menor do que a de y, x terá prioridade.

Convergência STP

Iniciando

Ao iniciar, cada switch se considera a Bridge root e gera uma configuração BPDU para cada porta, com custo do caminho root sendo 0 e o ID da bridge designada e porta designada sendo do próprio switch.

Comparando BPDUs

Cada switch envia BPDUs com suas configurações e recebe BPDUs de outros switches através de suas portas. A tabela a seguir exibe a comparação de operações.

Passo	Operação
1	Se a prioridade da BPDU recebida na porta é menor que a BPDU da própria porta, o switch descarta a BPDU e não altera o BPDU da porta.
2	Se a prioridade da BPDU recebida é maior que a BPDU da porta, o switch substitui o BPDU da porta com a BPDU recebida e compara com as BPDUs das outras portas, afim de obter a BPDU com maior prioridade.

Selecionando a bridge root

A Bridge Root é selecionada pela comparação das BPDUs recebidas. O switch com o Root ID menor é escolhido como Bridge Root.

Selecionando a porta root e a porta designada

A operação é realizada da seguinte maneira:

Passo	Operação
1	Para cada switch da rede (exceto o escolhido como Bridge root), a porta que receber o BPDU com maior prioridade é escolhido como Porta root do switch.

Passo	Operação
2	Utilizando a Porta root BPDU e o Custo do caminho Root, o switch gera uma Porta designada BPDU para cada uma de suas portas. • Root ID é substituído com o da Porta root. • Caminho root é substituído com a soma do custo do caminho root da porta root e o custo do caminho da porta e a porta root. • O ID da Bridge Designada é substituído com o do switch. • O ID da Porta Designada é substituído com o da porta.
3	O switch compara o BPDU resultante com o BPDU da porta desejada. • Se o BPDU recebido tem prioridade sobre o BPDU da porta, a porta é escolhida como Porta Designada e o BPDU da porta é substituído pelo BDPU recebido. A porta então envia regularmente o BPDU com maior prioridade. • Se o BPDU da porta tem prioridade sobre o BPDU recebido, o BPDU da porta não será substituído, a porta entra em estado de bloqueio e somente pode receber BPDUs.

Obs: o STP em uma rede com topologia estável, somente a Porta root e Porta designada encaminham dados, as outras portas permanecem no estado de bloqueio. As portas bloqueadas somente podem receber BPDUs.

O RSTP (IEEE 802.1w) é uma evolução do 802.1d padrão. A terminologia de STP do 802.1w permanece essencialmente igual à terminologia de STP do IEEE 802.1d. A maioria dos parâmetros permaneceu inalterada, assim os usuários familiarizados com o STP podem configurar rapidamente o novo protocolo.

O RSTP adianta o novo cálculo do Spanning Tree quando a topologia de rede de Camada 2 é alterada. O RSTP pode obter uma convergência muito mais rápida em uma rede corretamente configurada.

Condição para a porta root alterar o estado da porta para encaminhamento

Quando a porta root do switch deixa de encaminhar dados a porta designada começa a transmitir dados imediatamente.

Condição para a porta designada alterar o estado da porta para encaminhamento

a porta designada pode operar de duas formas: Porta edge (Porta de acesso) e Link P2P (conexão direta com outro switch).

- **Se a porta designada é uma Porta edge:** a porta altera imediatamente seus estados para encaminhamento.
- **Se porta designada é um Link P2P:** a porta somente mudará o estado para encaminhamento após realização do handshake entre as portas do switch.

Elementos RSTP

- **Porta Network (Edge):** indica que a porta do switch está conectada diretamente aos terminais.

- **Porta Borda (Link P2P):** indica que a porta do switch está conectada diretamente a outro switch.

MSTP (*Multiple Spanning Tree Protocol*), referente à norma IEEE 802.1s, é compatível tanto com o STP quanto o RSTP, além de permitir a convergência do Spanning Tree, também permite que pacotes de diferentes VLANs sejam transmitidos ao longo de seus respectivos caminhos de modo a proporcionar ligações redundantes com um melhor mecanismo de balanceamento de carga.

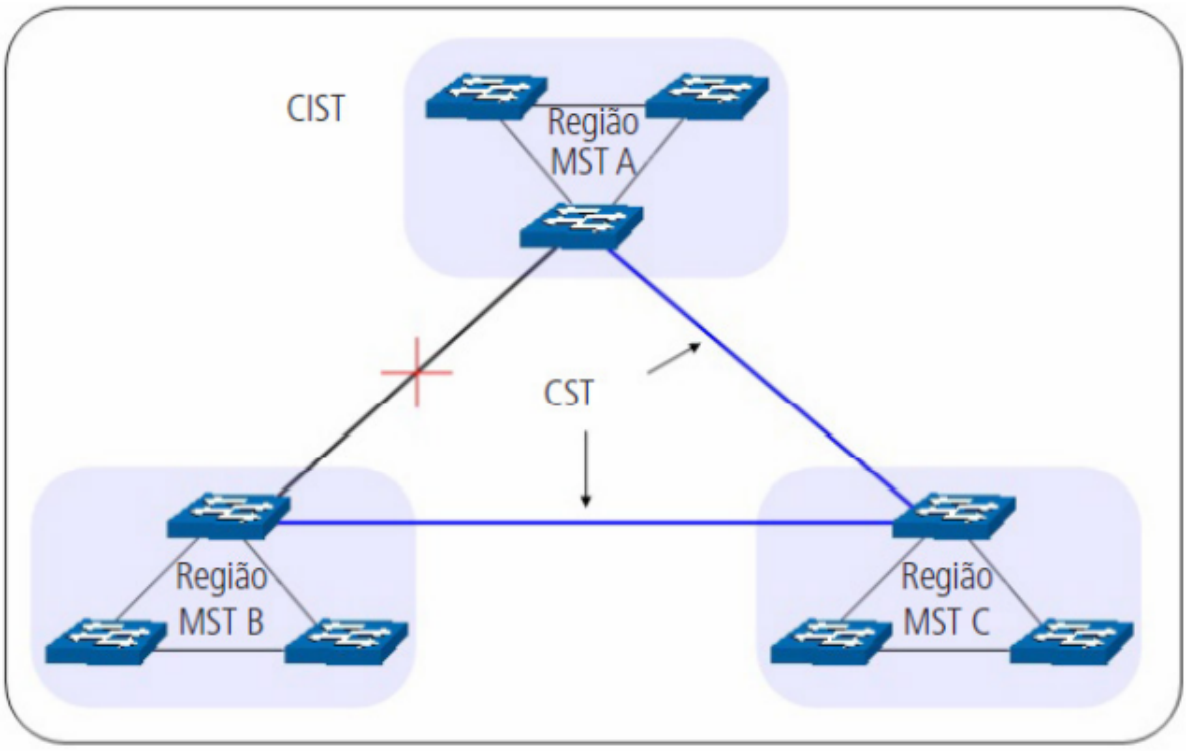
Funções do MSTP

- MSTP através das instâncias de VLAN faz com que o switch economize largura de banda durante a convergência e manutenção do STP, interligando várias VLANs a uma instância.
- MSTP divide uma rede com Spanning Tree em várias regiões. Cada região possui sua própria convergência STP que são independentes uma das outras.
- MSTP fornece um mecanismo de equilíbrio de carga para transmissões de pacotes na VLAN.
- MSTP é compatível com STP e RSTP.

Elementos MSTP

- Regiões MST (*Multiple Spanning Tree Region*): uma região MST corresponde aos switches que possuem a mesma configuração de região e instâncias de VLAN.
- **IST (*Internal Spanning Tree*):** uma IST é a execução interna do Spanning Tree dentro de uma região MST.
- **CST (*Common Spanning Tree*):** uma CST é a execução do Spanning Tree em uma rede que conecta todas as regiões MST na rede.
- **CIST (*Common and Internal Spanning Tree*):** um CIST compreende a IST e CST, é a execução do Spanning Tree que conecta todos os switches da rede.

A figura a seguir exibe o diagrama de uma rede com MSTP:



MSTP

O MSTP divide uma rede em várias regiões. O CST é gerado entre estas regiões do MST, cada região MST pode executar o Spanning Tree. Cada Spanning Tree é chamado de instância. Assim como o STP, o MSTP utiliza BPDUs para a execução do Spanning Tree. A única diferença é que o BPDU do MSTP transporta as informações de configuração MSTP dos switches

Estado das portas

No MSTP, as portas podem estar nos seguintes estados:

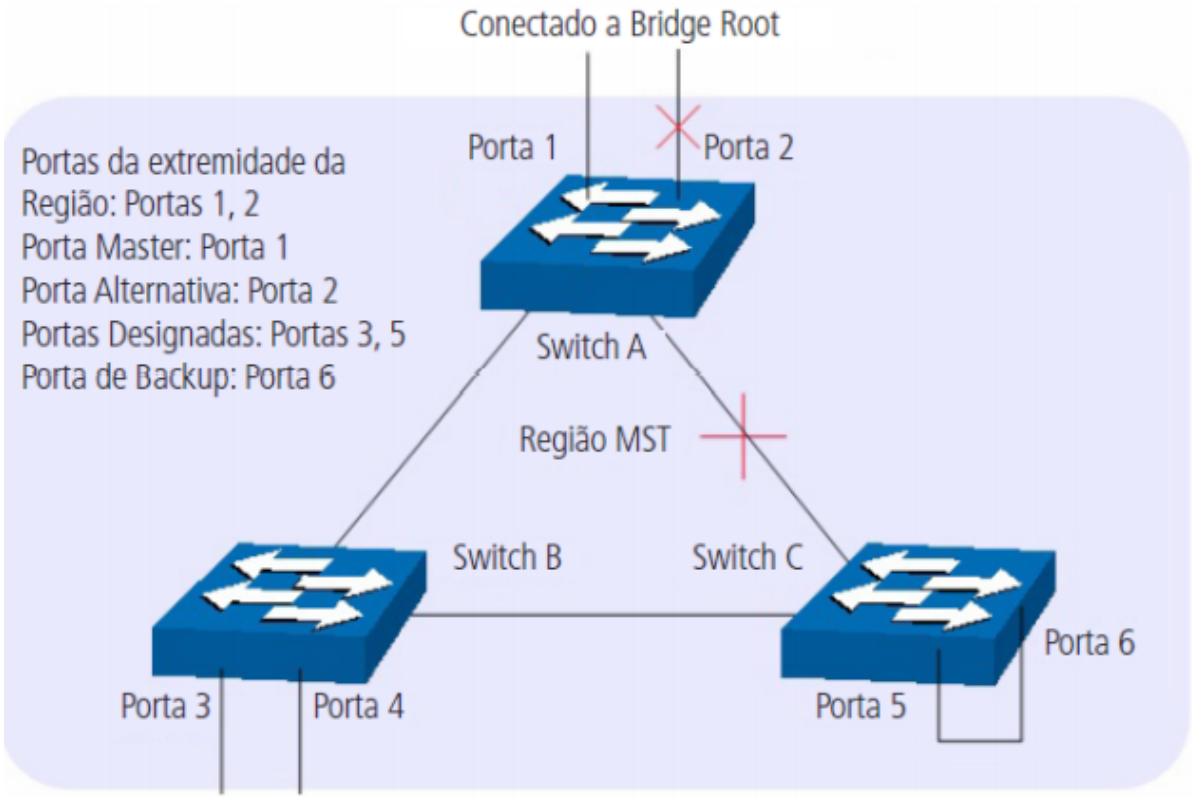
- **Encaminhamento:** neste estado a porta pode enviar e receber dados da rede além de enviar e receber quadros BPDUs e aprender endereços MAC.
- **Aprendizado:** neste estado a porta pode enviar e receber BPDUs e aprender endereços MAC.
- **Bloqueado:** neste estado a porta somente pode receber pacotes BPDUs.
- **Desconectado:** neste estado a porta não participa da execução do STP.

Funções das portas

Em um MSTP, existem as seguintes funções para as portas:

- **Porta root:** indica a porta que tem o caminho com menor custo (Path Cost) até o Bridge Root.
- **Porta designada:** indica a porta que encaminha pacotes para um segmento de rede do switch.
- **Porta master:** indica a porta que se conecta a região MST de outro switch.
- **Porta alternativa:** indica a porta que pode ser utilizada como backup da Porta Root ou Porta Master
- **Porta de backup:** indica a porta de backup da porta designada.
- **Desabilitada:** indica a porta que não participa do STP.

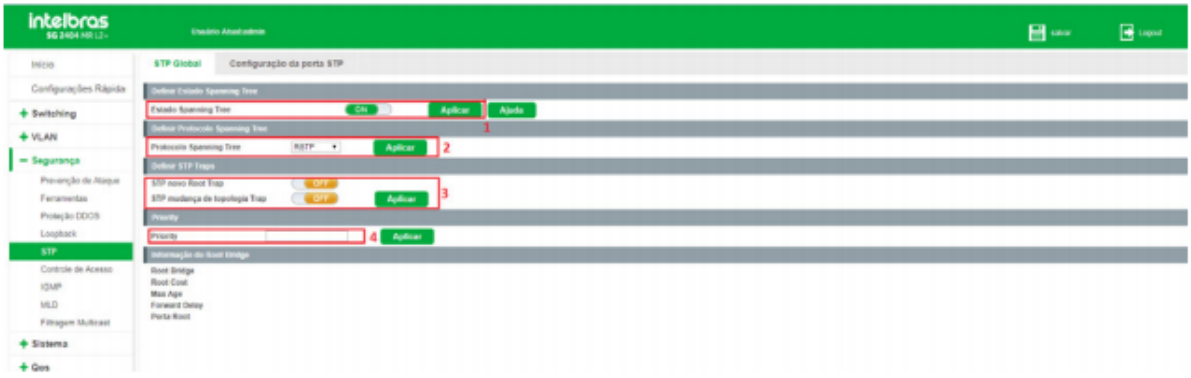
O diagrama a seguir exibe as diferentes funções das portas.



STP Global

Escolha o menu Segurança > STP > STP global e siga as instruções a seguir para efetuar a configuração global do Spanning Tree.

1. Defina o estado do Spanning Tree através do botão (OFF) e clique em Salvar; Clique no ícone (OFF) para ativar a função, caso esteja desabilitada, ou no ícone (ON) caso queira desativar;
2. Escolha o modo do Spanning Tree e clique em Aplicar;
    - **STP:** Spanning Tree Protocol
    - **RSTP:** Rapid Spannig Tree Protocol
    - **MSTP:** Multiple Spanning Tree Protocol.
3. Defina quando serão geradas traps do Spanning Tree e clique em Aplicar;
    - **STP Novo Root Trap:** caso esteja habilitado (ON), irá gerar trap SNMP quando for escolhido um novo Root Bridge.
    - **STP mudança da topologia TRAP:** caso esteja habilitado (ON), irá gerar trap SNMP quando for alterada a topologia do Spanning Tree.
4. Defina um valor múltiplo de 4096 para especificar a prioridade do switch durante a troca de quadros BPDUs.
    - **Prioridade:** a prioridade é um critério importante na determinação da Bridge Root. O switch com a maior prioridade será escolhido como Bridge Root.



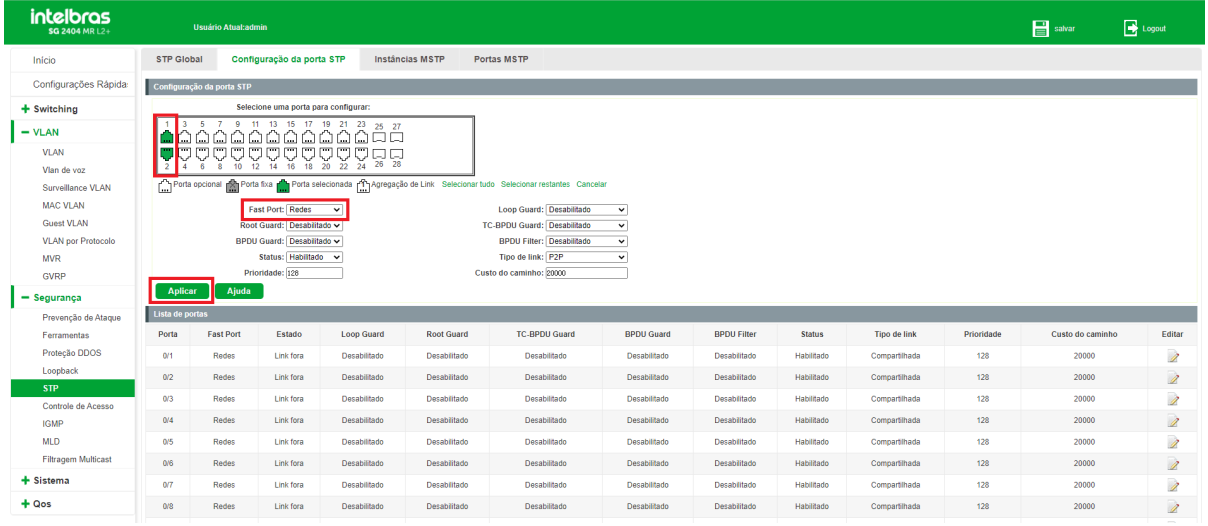
A seguir segue descrição das informações de Root Bridge exibidas na página:

- **Root Bridge:** indica o switch que possui o menor Bridge ID e seu MAC no seguinte formato: XXXXXAA:BB:CC:DD:EE:FF, onde XXXXX indica a prioridade da bridge do switch Root e AA:BB:CC:DD:EE:FF indica o MAC do switch root. O switch considerado Bridge Root serve como ponto de referência para todos os cálculos STP para garantir melhor desempenho e confiabilidade na rede. Por padrão, a prioridade do switch é 32768.
- **Root Cost:** indica a soma de todos os custos de porta ao longo do caminho até a Bridge Root. O custo do caminho da Bridge Root é 0.
- **Root Maximum Age:** indica o tempo máximo que o switch aguarda para remover sua configuração e iniciar uma nova eleição da Bridge Root. Por padrão, o Maximum Age do switch é de 20 segundos.
- **Atraso progressivo do Root:** indica o tempo para a porta alterar seu estado após uma alteração na topologia da rede. Por padrão, o atraso é de 15 segundos no switch.
- **Porta do Root:** indica a porta mais próxima (caminho com menor custo) para a Bridge Root. Por esta porta que os pacotes serão encaminhados para a Bridge Root.

Configuração da porta STP

Escolha o menu Segurança > STP > Configuração da porta STP e siga as instruções a seguir para configurar as portas STP.

1. Clique no ícone (EDITAR) da porta que deseja configurar ou selecione através do painel de portas;
2. Selecione o tipo de porta;
3. Clique em Aplicar.



A seguir apresentamos a descrição dos campos exibidos na tabela Lista de portas.

- **Porta:** indica o número da porta
- **Fast Port:** indica o tipo de porta.
  - **Porta redes:** indica que a porta do switch está conectada diretamente aos terminais
  - **Porta borda:** indica que a porta do switch está conectada diretamente a outro switch.
  - **Desativado:** indica que a porta não participa do Spanning Tree.
- **Estado:** indica o estado atual da porta.
  - **Encaminhamento:** neste estado a porta pode receber e enviar dados, receber e enviar quadros BPDUs bem como aprender endereços MAC.
  - **Conectando:** neste estado a porta pode receber e enviar quadros BPDUs e aprender o endereço MAC.
  - **Bloqueio:** neste estado a porta somente pode receber quadros BPDUs.
  - **Link fora:** neste estado a porta não apresenta a presença de link.

Controle de Acesso (ACL)

O Controle de acesso, ou ACL (*Access Control List*), é utilizado para a configuração de regras para o filtro e processamento dos pacotes, controlando o acesso ilegal a rede. Além disso, a função ACL pode controlar os fluxos dos dados, economizando recursos da rede de forma flexível, facilitando o controle da rede.

Neste switch, as ACLs classificam os pacotes com base em uma série de condições que podem ser encontradas em protocolos utilizados entre as camadas 2 a 4 do modelo de referência OSI.

O menu ACL permite configurar *ACL Padrão IPv4, ACL Estendida IPv4, MAC ACL, ACL Padrão IPv6* e *ACL Estendida IPv6*.

As regras ACL estão enumeradas no switch de acordo com a tabela a seguir:

Tipo de regra ACL	ID das listas	ID das regras
ACL Padrão IPv4	0 a 9	0 a 9
ACL Estendida IPv4	10 a 19	0 a 9
MAC ACL	20 a 25	0 a 9

Tipo de regra ACL	ID das listas	ID das regras
ACL Padrão IPv6	26 a 35	0 a 9
ACL Estendida IPv6	36 a 45	0 a 9

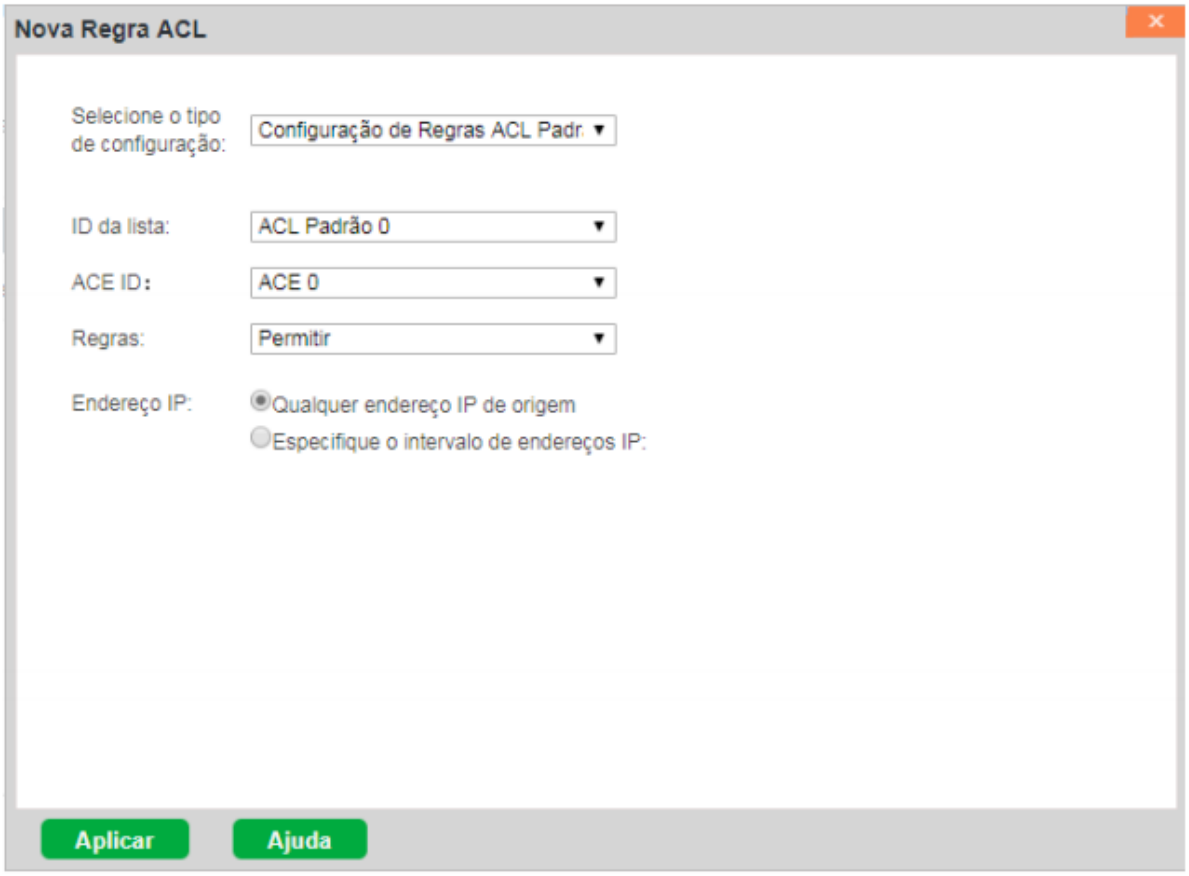
ACL

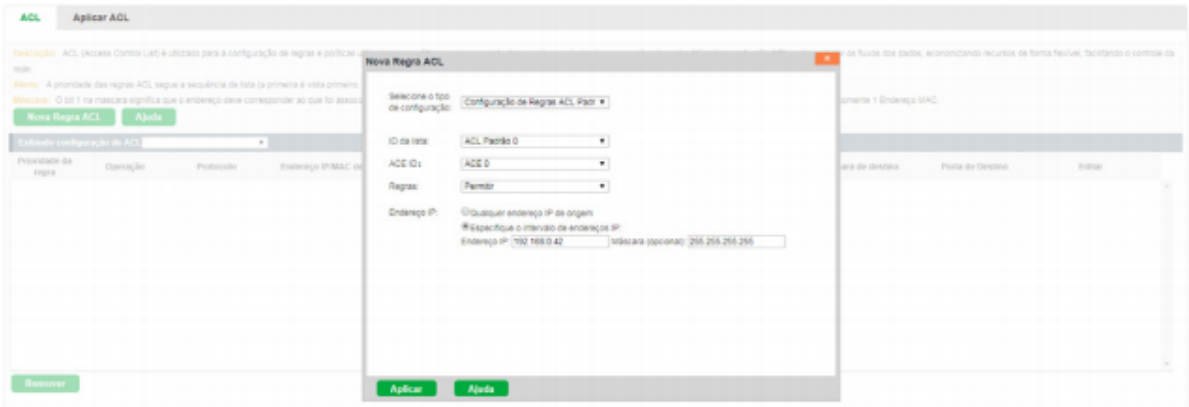
Para escolher uma das listas de ACL disponível, é necessário acessar o menu Segurança > Controle de acesso > ACL e clicar no botão Nova regra ACL.

Visualizando regras ACL

Conforme exibido na tabela anterior, as regras ACL estão divididas em listas.

Para escolher uma das listas de ACL disponível, é necessário acessar o menu Segurança > Controle de acesso > ACL e clicar no botão Nova regra ACL.





Obs: As regras para a configuração ACL são:

- Primeiramente deve-se incluir as regras condicionais. Os endereços IP que serão permitidos ou bloqueados na regra de acesso.
- A prioridade das regras ACL segue a sequência da lista configurada (a primeira é vista primeiro, depois a segunda, a terceira, e assim por diante).
- Por último deve ter uma regra geral para acesso ou bloqueio do restante dos IPs.

As ACLs padrão IPv4 ou IPv6 podem analisar e processar os pacotes com base nas seguintes informações: endereço IPv4 de origem e destino ou endereço IPv6 de origem e destino.

Escolha o menu Segurança > Controle de acesso > ACL e siga as instruções a seguir para configurar o ACL Padrão.

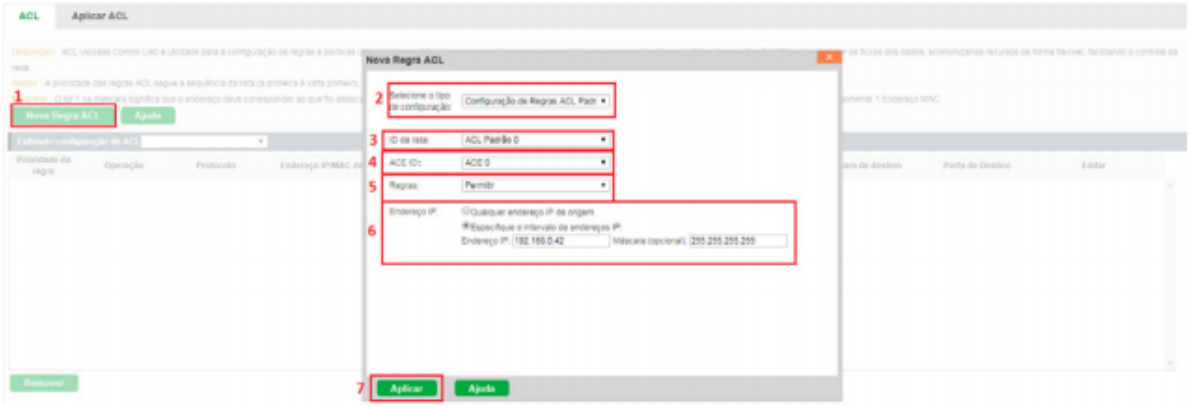
1. Clique no botão Nova regra ACL;
2. Selecione o tipo de configuração, Configuração de Regras ACL Padrão, para ACL Padrão IPv4 ou o tipo, Configuração de Regras ACL Padrão IPv6, para ACL Padrão IPv6;
3. Selecione o ID da lista na qual a regra será configurada;
4. Selecione o ID da regra;
5. Selecione o tipo de regra:

- **Permitir:** encaminha o pacote.
- **Negar:** descarta o pacote.

6. Escolha o endereço IP de acordo com as opções:

- **Qualquer endereço IP de origem:** indica que a regra será aplicada a todo pacote (com qualquer endereço IP de origem) que chegar numa porta em que esta regra esteja habilitada.
- **Especifique o intervalo de endereços IP:** indica que a regra será aplicada a todo pacote que possuir endereço IP de origem dentro do intervalo (máscara) configurado. Desde que a regra esteja habilitada na porta em que o pacote for recebido. Caso escolha esta opção, será necessário especificar o IP e a máscara desejados.

7. Clique em Aplicar.



É possível adicionar até 10 listas de regras ACL Padrão, que variam de 0 a 9 para IPv4 e 26 a 35 para IPv6. Cada lista pode conter até 10 regras, cujos IDs variam de 0 a 9. As regras dentro das listas são processadas de acordo com o número da regra, ou seja, caso o switch receba um pacote numa porta onde há regras ACL, elas serão processadas na

sequência de 0 a 9, de acordo com o número de regras que foram criadas. Por exemplo, caso a lista possua as regras ACL 0, 4 e 7, a ordem de processamento será 0 > 4 > 7.

Observações:

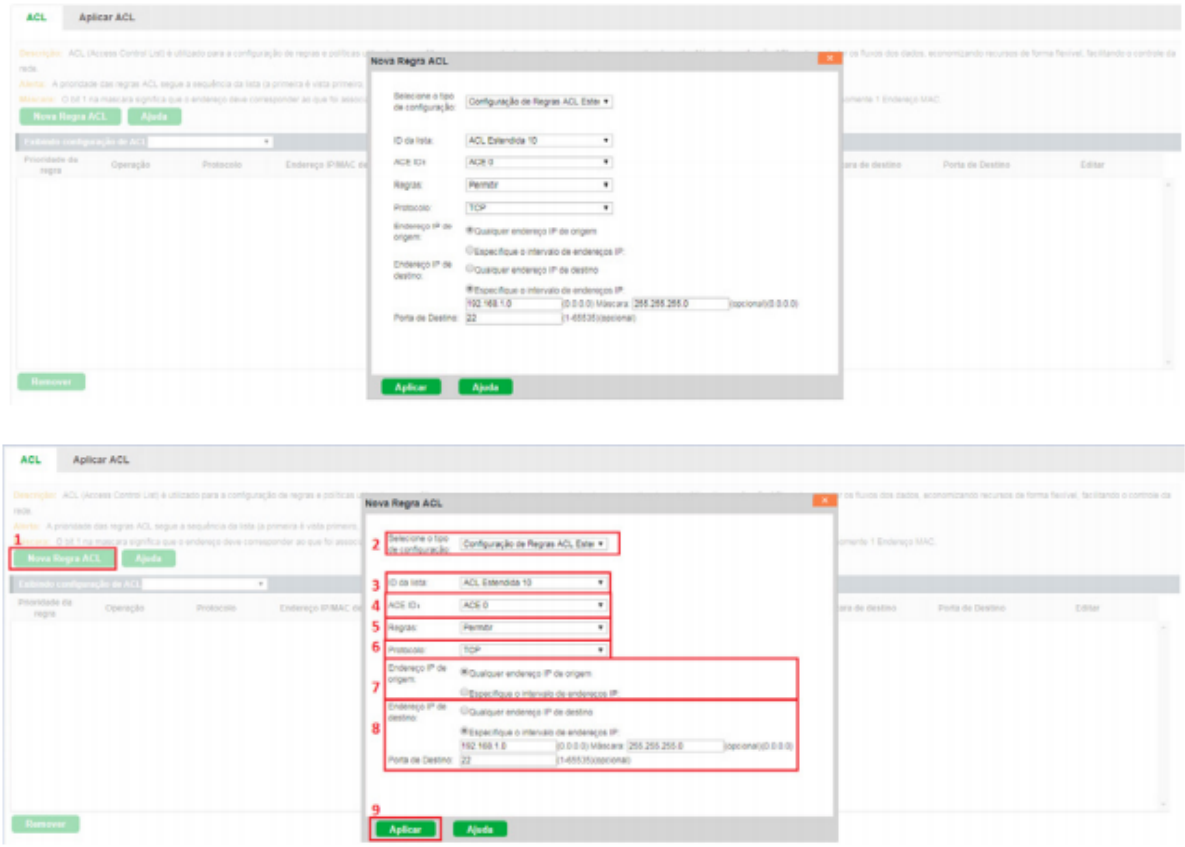
- Para a configuração de um range de IPs, a Máscara de Origem deve ser o Wildcad do endereço da rede. Por exemplo, o endereço de rede 10.90.90.0 tem o Wildcard como 0.0.0.3. É este o valor que deve ser configurado no campo Máscara (opcional). Neste exemplo os IPs que terão acesso ao equipamento são 10.90.90.1, 10.90.90.2 e 10.90.90.3.
- A máscara de rede utilizada para configuração de intervalo de endereço IPv6 deve variar de 0 a 128. Este número indica a quantidade de bits 1 contados da esquerda para a direita no endereço de máscara. Cada bit 1 indica que o endereço deve ser fixo naquele ponto. Por exemplo, uma máscara /64 indica que os primeiros 64 bits do endereço IPv6 serão 1 e, portanto, fixos. Os demais serão 0 e, portanto, variáveis.
- Caso não seja digitada uma máscara de rede para o intervalo, a máscara assumida será 0.0.0.0, ou seja, a regra será aplicada para qualquer endereço IP de origem.

ACL estendida

As ACLs Estendidas podem analisar e processar os pacotes com base em várias informações, como por exemplo: endereço IPv4 e IPv6 de origem e destino, portas de origem e destino.

Escolha o menu Segurança > Controle de Acesso > ACL e siga as instruções a seguir para configurar a ACL Estendida.

1. Clique no botão Nova regra ACL;
2. Selecione o tipo de configuração Configuração de Regras ACL Estendida para ACL Estendida IPv4 ou o tipo Configuração de Regras ACL Estendida IPv6 para ACL Estendida IPv6;
3. Selecione o ID da lista na qual a regra será configurada;
4. Selecione o ID da regra;
5. Selecione o tipo de regra;
   - **Permitir:** encaminha o pacote.
   - **Negar:** descarta o pacote
6. Escolha o protocolo (IP/UDP/TCP);
   Caso escolha TCP ou UDP, será permitida a opção de especificar as portas de origem e destino.
7. Escolha o endereço IP e a porta de origem, caso tenha selecionado protocolo TCP ou UDP;
   É possível escolher qualquer endereço IP ou especificar um intervalo de endereços IP de origem.
8. Escolha o endereço IP e a porta de destino, caso tenha selecionado protocolo TCP ou UDP;
   É possível escolher qualquer endereço IP ou especificar um intervalo de endereços IP de destino
9. Clique em Aplicar.



Cada regra é processada agregando os parâmetros que nela foram configurados. No caso da imagem acima, por exemplo, o switch irá permitir qualquer que endereço IP de origem com qualquer porta de origem tenha acesso aos IPs da rede 192.168.1.0/24 na porta TCP 22.

É possível adicionar até 10 listas de regras ACL Estendidas, que variam de 10 a 19 para IPv4 e 36 a 45 para IPv6. Cada lista pode conter até 10 regras, cujos IDs variam de 0 a 9. As regras dentro das listas são processadas de acordo com o número da regra, ou seja, caso o switch receba um pacote numa porta onde há regras ACL, elas serão processadas na sequência de 0 a 9, de acordo com o número de regras que foram criadas. Por exemplo, caso a lista possua as regras ACL 0, 4 e 7, a ordem de processamento será 0 > 4 > 7.

Observações:

- A máscara de rede utilizada para configuração de intervalo de endereço IPv4 deve ser escrita no seguinte formato extenso. Exemplo: 255.255.255.0, ou 255.255.255.240, ou 255.255.0.0, etc.
- A máscara de rede utilizada para configuração de intervalo de endereço IPv6 deve variar de 0 a 128. Este número indica a quantidade de bits 1 contados da esquerda para a direita no endereço de máscara. Cada bit 1 indica que o endereço deve ser fixo naquele ponto. Por exemplo, uma máscara /64 indica que os primeiros 64 bits do endereço IPv6 serão 1 e, portanto, fixos. Os demais serão 0 e, portanto, variáveis.
- Caso não seja especificada uma máscara de rede para o intervalo, a máscara assumida será 0.0.0.0, ou seja, a regra será aplicada para qualquer endereço IP de origem.
- Caso escolha protocolo TCP ou UDP e não especifique a porta, serão consideradas todas as portas no processamento da regra.

MAC ACL

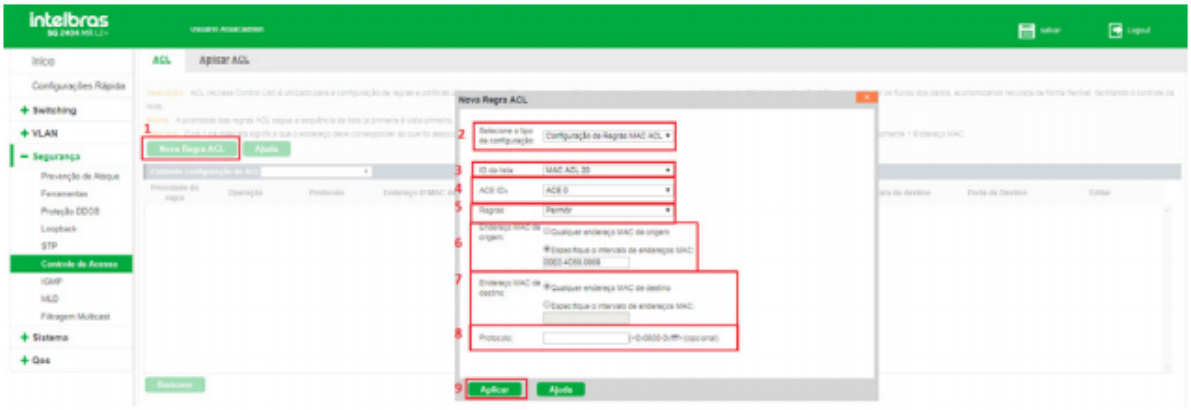
MAC ACLs podem analisar e processar os pacotes com base nas seguintes informações: endereço MAC de origem e endereço MAC de destino.

Escolha o menu Segurança > Controle de Acesso > ACL e siga as instruções a seguir para configurar o MAC ACL.

1. Clique no botão Nova regra ACL;
2. Selecione o tipo de configuração Configuração de Regras MAC ACL;
3. Selecione o ID da lista na qual a regra será configurada;
4. Selecione o ID da regra;
5. Selecione o tipo de regra;
   - Permitir: encaminha o pacote.
   - Negar: descarta o pacote.
6. Escolha o endereço MAC de origem;

   É possível escolher qualquer endereço MAC ou especificar um determinado endereço MAC de origem.
7. Escolha o endereço MAC de destino;

   É possível escolher qualquer endereço MAC ou especificar um determinado endereço MAC de destino.
8. Digite o EtherType do pacote no campo Protocolo. Ele será utilizado pela regra (opcional). Esta configuração se refere ao campo Type do cabeçalho Ethernet e os valores permitidos são 0x0600 a 0xffff;
9. Clique em Aplicar.



Cada regra é processada agregando os parâmetros que nela foram configurados. No caso da imagem acima, por exemplo, o switch irá permitir pacotes provenientes do MAC 00E0.4C68.0868 com destino a qualquer MAC.

É possível adicionar até 6 listas de regras MAC ACL, que variam de 20 a 25. Cada lista pode conter até 10 regras, cujos IDs variam de 0 a 9. As regras dentro das listas são processadas de acordo com o número da regra, ou seja, caso o switch receba um pacote numa porta onde há regras ACL, elas serão processadas na sequência de 0 a 9, de acordo com o número de regras que foram criadas. Por exemplo, caso a lista possua as regras ACL 0, 4 e 7, a ordem de processamento será 0 > 4 > 7.

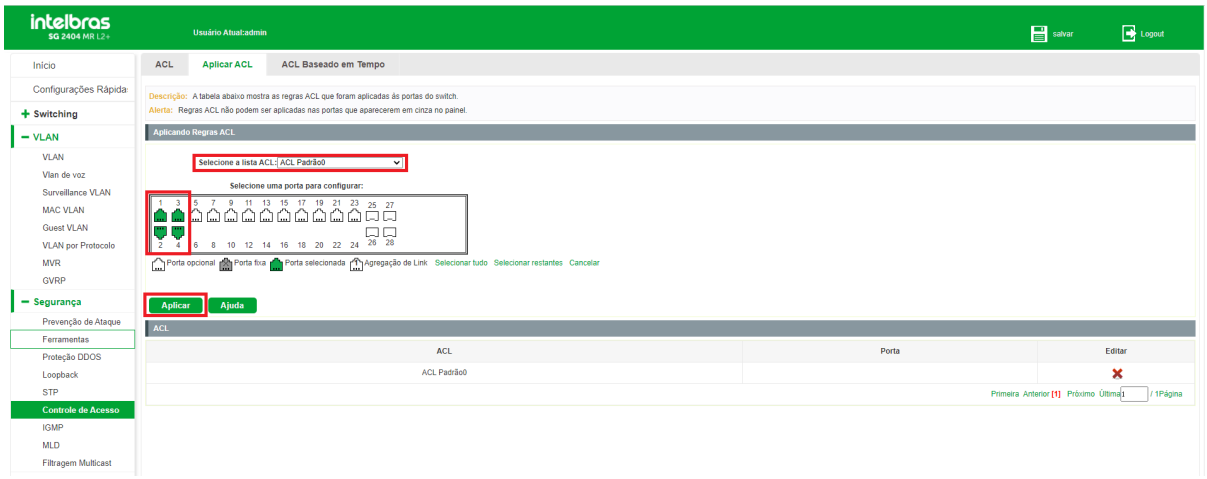
Obs: os endereços MAC deverão ser escritos no seguinte formato: XXXX.XXXX.XXXX. Por exemplo: 00E0.4C68.0868.

Aplicar ACL

Para que as regras ACL configuradas tenham efeito sobre os pacotes transmitidos através do switch, é necessário vinculá-las as portas do equipamento.

Escolha o menu Segurança > Controle de Acesso > Vincular ACL e siga as instruções a seguir para vincular as regras ACL criadas às portas do switch.

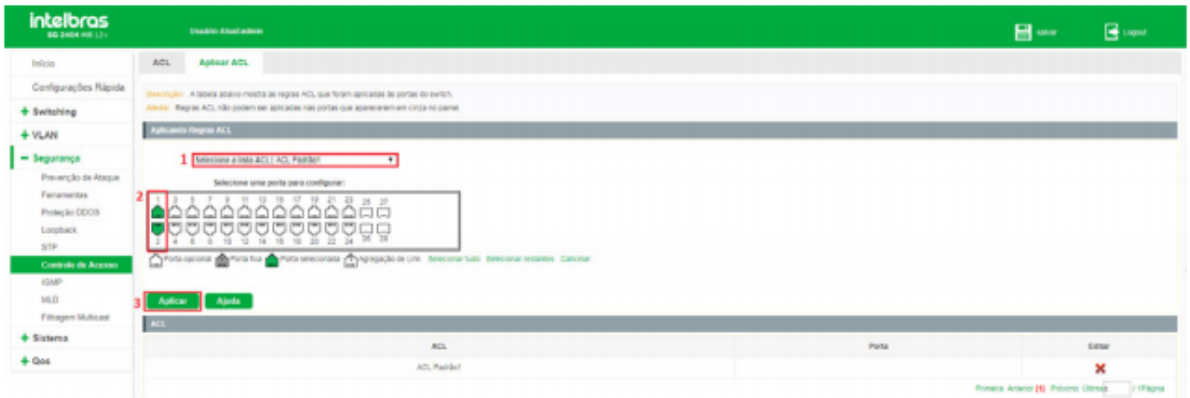
1. Selecione a Lista ACL que deseja vincular;
2. Selecione a(s) porta(s) que deseja vincular através do painel de portas;
3. Clique em Aplicar.



Removendo vínculo ACL

Escolha o menu Segurança > Controle de acesso > Vincular ACL e siga as instruções a seguir para remover o vínculo, ou desvincular, uma porta de uma regra ACL.

1. Selecione a lista ACL;
2. Desmarque as portas que deseja desvincular;
3. Clique em Salvar.

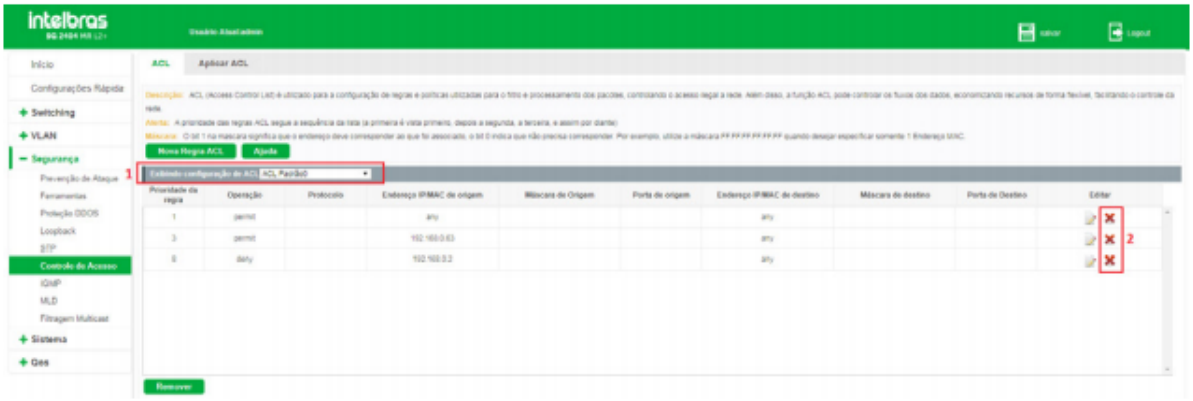


Também é possível desvincular diretamente uma regra ACL de todas as portas. Para isto, basta clicar no ícone (EXCLUIR) ao lado da regra que deseja desvincular.

Removendo regra ACL

Escolha o menu Segurança > Controle de acesso > ACL e siga as instruções a seguir para remover uma regra ACL de uma lista de regras.

1. Selecione a lista de regras a qual a regra pertence;
2. Clique no ícone da regra que deseja excluir.

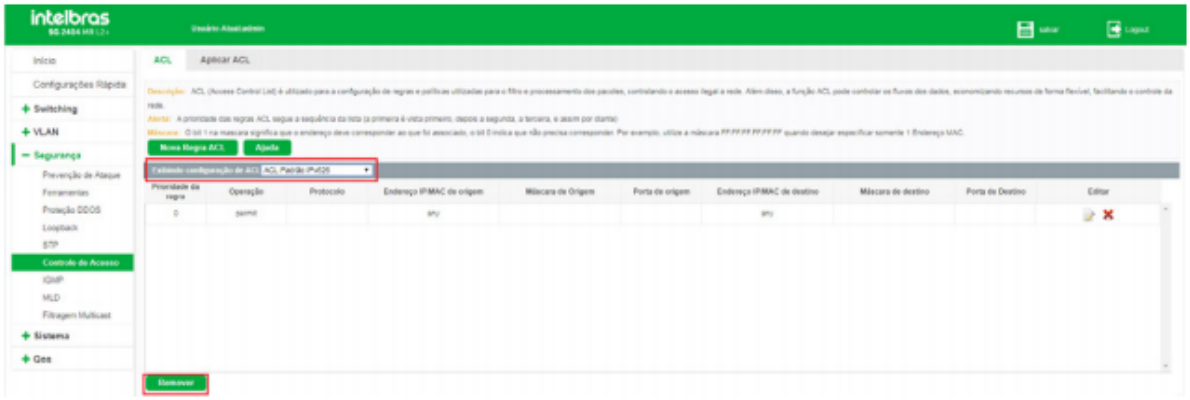


Obs: só é possível remover regras caso estas não estejam vinculadas a nenhuma porta. Se estiverem vinculadas, primeiramente remova o vínculo e depois remova a regra.

Removendo lista de regras ACL

Escolha o menu Segurança > Controle de acesso > ACL e siga as instruções a seguir para remover uma lista de regras ACL.

1. Selecione a lista que deseja remover;
2. Clique em Remover.



Obs: só é possível remover uma lista ACL caso esta não possua nenhuma porta vinculada. Se houver portas vinculadas, primeiramente remova os vínculos e depois remova a lista.

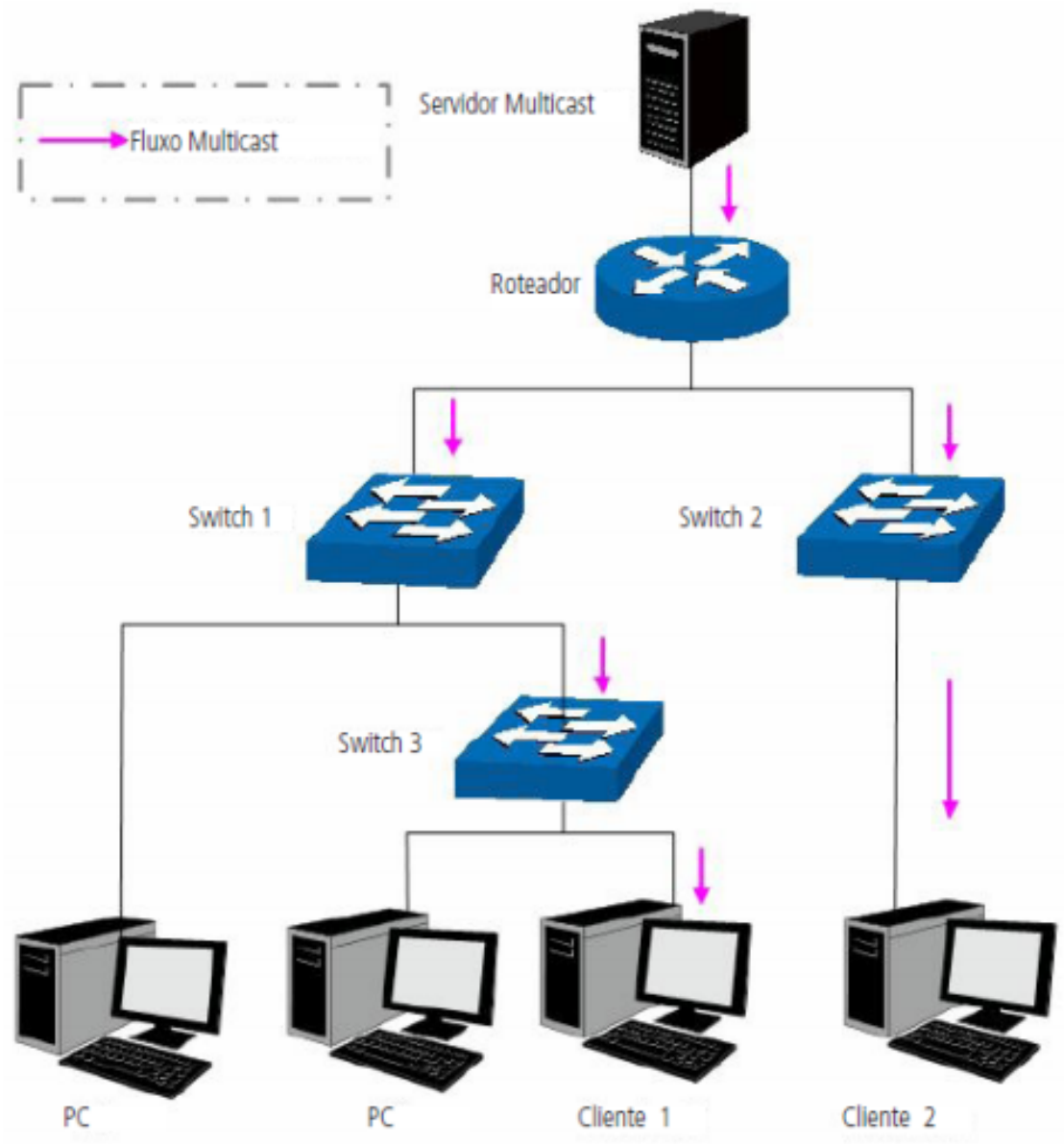
IGMP

Multicast

Multicast é o método de transmissão de um pacote de dados a múltiplos destinos ao mesmo tempo. O servidor Multicast envia os pacotes de dados somente uma vez, ficando a cargo dos clientes captarem esta transmissão e reproduzi-la, esta técnica diminui consideravelmente o tráfego da rede e é utilizado principalmente em aplicações de streaming de áudio e vídeo conferência. Este método possui uma alta eficiência na entrega dos pacotes a múltiplos clientes, reduzindo a carga da rede.

Este switch utiliza o protocolo IGMP (*Internet Group Management Protocol*) para consultar quais clientes desejam receber o serviço Multicast ofertado. Com a utilização deste procolo o switch consegue identificar em qual porta o cliente está conectado para receber a transmissão Multicast, a partir desta identificação, o switch encaminha o tráfego Multicast apenas para as portas onde houver solicitante.

A figura a seguir exibe como o tráfego Multicast é transmitido:



Funções do Multicast

1. Em uma rede ponto a multiponto, o número de clientes solicitando um serviço é desconhecido, neste caso, o Multicast otimiza os recursos da rede.
2. Os clientes que recebem a mesma informação do servidor Multicast, formam um Grupo Multicast. Deste modo o servidor Multicast necessita enviar a mensagem uma única vez.

3. Cada cliente pode entrar ou sair do Grupo Multicast a qualquer momento.
4. Em aplicações em tempo real, é aceitável ocorrer algumas perdas de pacotes (dentro de um limite que não prejudique o serviço).

Endereços Multicast

Conforme especificado pelo IANA (*Internet Assigned Numbers Authority*), os endereços Ips de classe D são usados como endereços Multicast. O intervalo de endereços Multicast vai de 224.0.0.0 a 239.255.255.255. A tabela a seguir exibe o intervalo e descrição de vários endereços Multicast especiais.

Faixa de endereços multicast	**Descrição**
224.0.0.0 – 224.0.0.255	Endereços Multicast reservados para protocolos de roteamento e outros protocolos de rede
224.0.1.0 – 224.0.1.255	Endereços para videoconferência
239.0.0.0 – 239.255.255.255	Endereços Multicast utilizados no gerenciamento da rede local

Endereços MAC Multicast

Quando um pacote Unicast é transmitido em uma rede Ethernet, o endereço MAC de destino é o endereço MAC do receptor. Quando um pacote Multicast é transmitido em uma rede Ethernet, o destino não é apenas um receptor, mas um grupo com um número indeterminado de membros. Para um determinado endereço MAC Multicast, é criado um endereço MAC lógico, utilizado como endereço de destino do pacote.

Conforme estipulado pela IANA, os 24 bits de maior ordem de um endereço MAC Multicast inicia-se com 01-00-5E enquanto os 23 bits de menor ordem do endereço IP Multicast substituem os 23 bits de menor ordem do endereço MAC, formando assim o endereço MAC Multicast, como exibe a figura a seguir:

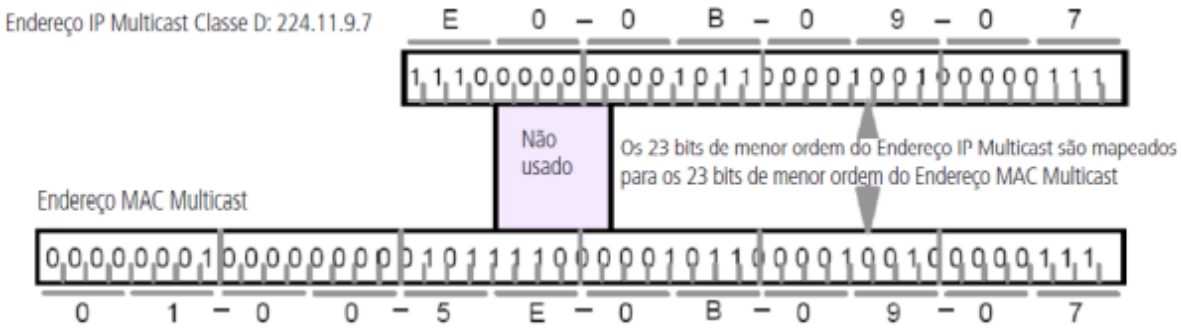


Tabela de endereços Multicast

O switch encaminha pacotes Multicast com base na Tabela de endereços Multicast. Como a transmissão de pacotes Multicast não pode se estender a VLANs, a primeira parte da Tabela de endereços Multicast é o VLAN ID, a partir do qual, os pacotes Multicast recebidos são transmitidos somente na VLAN que a porta pertence.

A Tabela de endereços Multicast não está mapeada para uma porta de saída, mas sim, para uma lista de portas pertencentes a um grupo. Ao encaminhar um pacote Multicast, o switch verifica sua Tabela de endereços Multicast, baseado no endereço de destino do pacote Multicast. Se a entrada correspondente não for encontrada na tabela, o switch irá transmitir via broadcast o pacote na VLAN. Se a entrada correspondente for encontrada na tabela, isso indica que o endereço MAC de destino deve estar na lista de grupos de portas, de modo que o switch irá duplicar estes dados de destino e entregará uma cópia para cada porta. O formato geral da tabela de endereços Multicast é descrito na figura a seguir:

VLAN ID	Multicast IP	Porta

IGMP Snooping

O IGMP Snooping é um mecanismo de controle Multicast, que pode ser usado no switch para registrar dinamicamente um grupo Multicast. O switch executando o IGMP snooping, gerencia e controla o grupo Multicast escutando e processando mensagens IGMP transmitidas entre os clientes e servidores Multicast, determinando os dispositivos conectados a ele e que pertencem ao mesmo grupo, evitando desta forma que os grupos Multicast transmitam pacotes via broadcast na rede.

Processo IGMP Snooping

O switch executando IGMP Snooping fica escutando as mensagens transmitidas entre os clientes e o servidor Multicast, controlando e registrando as mensagens IGMP que passam por suas portas. Ao receber mensagens IGMP Report, o switch adiciona a porta na Tabela de endereços MAC Multicast, quando o switch escuta mensagens IGMP Leave a partir de um cliente, ele aguarda o servidor Multicast enviar mensagens IGMP Query ao Grupo Multicast específico para verificar se os outros clientes do grupo ainda necessitam das mensagens Multicast: se sim, o servidor Multicast receberá mensagem IGMP Report, se não, o servidor Multicast não receberá mensagens IGMP Report, portanto o switch removerá a porta específica da Tabela de endereços Multicast. O servidor Multicast envia regularmente mensagens IGMP Query, após o envio destas mensagens, o switch irá remover a porta da Tabela de endereços Multicast, caso não escute nenhuma mensagem IGMP Report do cliente em um determinado período de tempo.

Mensagens IGMP

O switch, executando IGMP Snooping, processa as mensagens IGMP das seguintes formas:

1. **IGMP Query (Consulta IGMP):** as mensagens IGMP Query (Consulta IGMP) enviadas pelo servidor Multicast podem ser classificadas de duas formas: IGMP General Query (Consulta Geral) ou Group-Specific-Query (Consulta a Grupo Específico). O servidor envia regularmente mensagens de consulta geral, para verificar se os grupos Multicast possuem membros. Ao receber mensagens IGMP Leave, o switch encaminhará as mensagens de consulta ao grupo Multicast específico enviadas pelo servidor Multicast para as portas pertencentes ao grupo, para verificar se outros membros do grupo ainda necessitam do serviço Multicast.
2. **IGMP Report (Relatório IGMP):** as mensagens IGMP Report são enviadas pelos clientes quando desejam se associar (join) a um grupo Multicast ou responder as mensagens de consulta IGMP (IGMP Query) do servidor Multicast. Ao

receber uma mensagem IGMP Report, o switch encaminhará a mensagem de relatório através da porta denominada Porta do roteador para o servidor Multicast, além de analisar a mensagem para obter o endereço do grupo Multicast que o cliente irá se juntar. A porta de recepção do switch procederá da seguinte maneira: se a porta que o cliente está conectado no switch é um novo membro para um grupo Multicast, a porta será adicionada a Tabela de endereços Multicast, se a porta que o cliente está conectado já pertence ao grupo Multicast, o tempo de permanência da porta ao grupo Multicast é reiniciado.

3. **IGMP Leave (Remoção do Grupo Multicast):** clientes que executam o IGMP v1 não enviam mensagens IGMP Leave ao sair de um grupo Multicast, como resultado, o switch somente removerá a porta da Tabela de endereços Multicast após o término do tempo de vida da porta na tabela de endereços. Os clientes que executam IGMP v2 ou IGMP v3, enviam mensagens IGMP Leave ao sair de um grupo Multicast para informar ao servidor Multicast a sua saída.Ao receber mensagens IGMP Leave, o switch encaminha as mensagens de consulta ao grupo Multicast específico enviadas pelo servidor Multicast para as portas pertencentes ao grupo, para verificar se outros membros do grupo ainda necessitam do serviço Multicast e reiniciar o tempo de permanência da porta na Tabela de endereços Multicast.

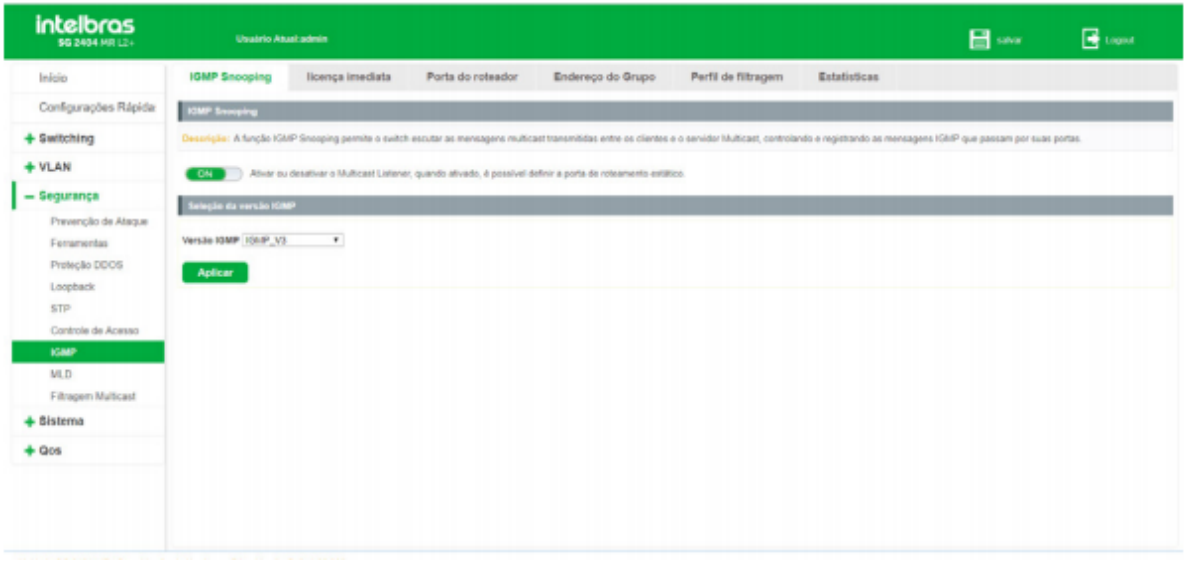
Fundamentos do IGMP Snooping

- **Portas**
  - **Porta do roteador:** indica a porta do switch conectada diretamente ao servidor Multicast.
  - **Portas membro:** indica a porta do switch conectado diretamente a um membro (cliente) do grupo Multicast
- **Temporizadores**
  - **Tempo limite da porta do roteador:** se o switch não receber mensagens IGMP Query da porta em que o servidor Multicast está conectado dentro de um intervalo de tempo, a porta não será mais considerada como Porta do Roteador. O valor padrão é 300 segundos.
  - **Tempo limite das portas membro:** se o switch não receber mensagens IGMP Report da porta em que os membros (cliente) de um grupo Multicast estão conectados dentro de um intervalo de tempo, a porta não será mais considerada como Portas Membro. O valor padrão é 260 segundos.
  - **Leave time:** indica o intervalo entre o switch receber uma mensagem Leave a partir de um cliente e o servidor Multicast remover o cliente do grupo Multicast. O valor padrão é 1 segundo.

Habilitando IGMP Snooping Dinâmico

Escolha o menu Segurança > IGMP > IGMP Snooping e siga as instruções a seguir para habilitar o IGMP Snooping no modo Dinâmico.

1. Clique no ícone (OFF) para ativar a função, caso esteja desabilitada, ou no ícone (ON) caso queira desativar;
2. Selecione a versão do IGMP Snooping;
3. Clique em Aplicar.



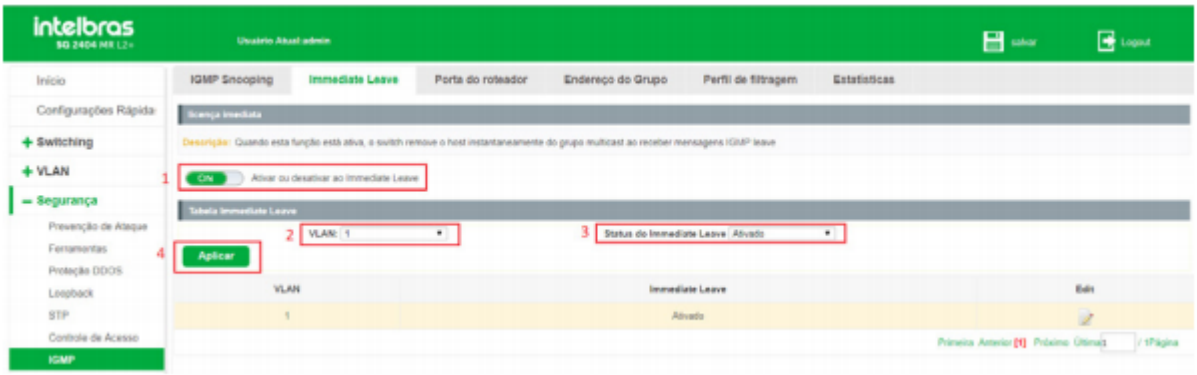
Ao habilitar a função IGMP Snooping no modo Dinâmico, o switch ficará escutando as portas e fará a detecção automática das portas roteador (que possuem um servidor multicast conectado) e das portas membro.

Observações:

- Por padrão, a função Fast-Leave é desabilitada. Para habilitá-la é necessário acessar a CLI (interface de linha de comando) do switch. Para isto, consulte o manual da CLI do switch
- Por padrão, o IGMP Snooping dinâmico é habilitado em forma global, ou seja, esta função escutará em todas as VLANs.
- A versão 3 do IGMP Snooping é a escolhida por padrão.

Immediate Leave

Quando habilitada essa função, os clientes que enviarem mensagens IGMP leave serão removidos do grupo Multicast imediatamente, sem esperar esgotar o tempo de vida da tabela.



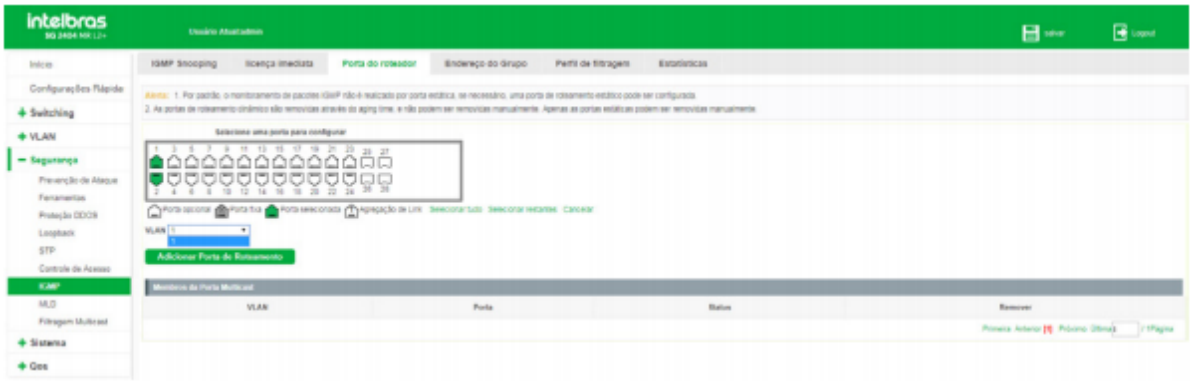
1. Habilite o Immediate Leave;
2. Selecione a VLAN que deseja habilitar/desabilitar o Immediate Leave;
3. Habilite ou desabilite o Immediate Leave;
4. Clique em Aplicar.

Porta do roteador

O switch também permite configurar Portas roteador de forma estática. Desta forma é possível fixar portas roteador e removê-las quando necessário.

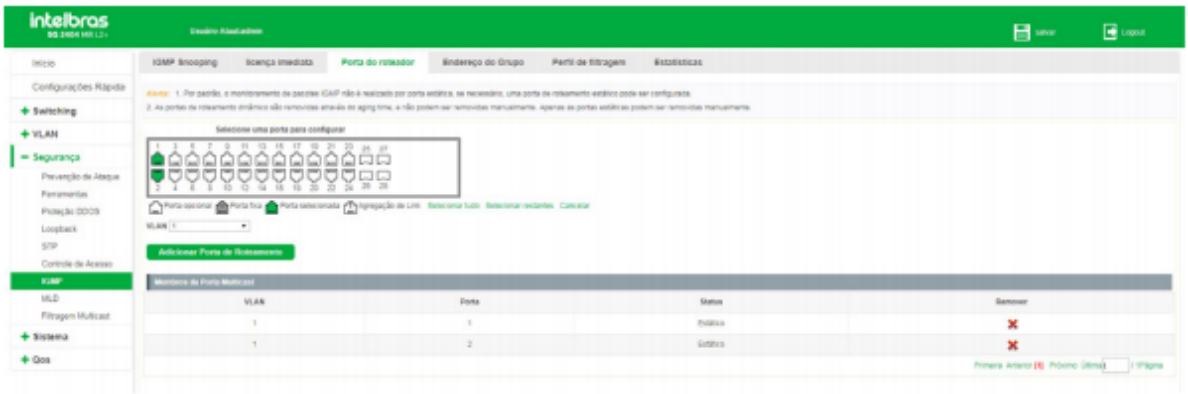
Escolha o menu Segurança > IGMP > Porta do roteador e siga as instruções a seguir para configurar uma porta roteador estática.

1. Selecione a(s) porta(s) desejada(s) no painel de portas;
2. Selecione a VLAN desejada;
3. Clique em Adicionar Porta de Roteamento.



Nesta página são exibidas também as portas que foram detectadas automaticamente pelo IGMP Snooping. A tabela Membros da Porta Multicast exibe as seguintes informações:

- **VLAN:** indica a VLAN onde foi detectado (ou configurado de forma estática) um tráfego multicast.
- **Porta:** exibe a porta onde foi detectado (ou configurado de forma estática) um tráfego multicast.
- **Status:** indica se a porta foi configurada de forma estática ou se foi detectado tráfego multicast de forma dinâmica.
- **Remover:** permite a remoção de uma porta roteador, seja ela dinâmica ou estática. Para isto, basta clicar sobre o ícone (EXCLUIR).



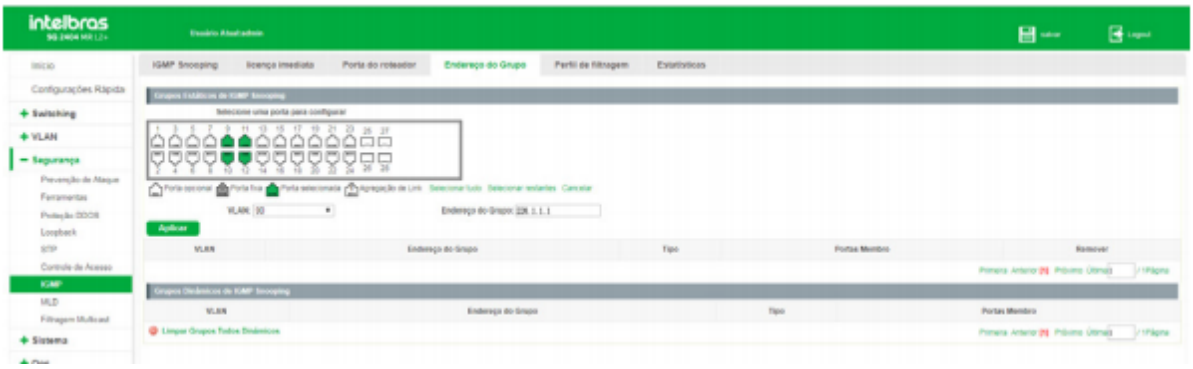
Observações:

- É necessário que a porta esteja configurada na VLAN desejada para que ela seja configurada como porta roteador naquela VLAN.
- Não é possível remover portas dinâmicas. Estas portas serão removidas automaticamente através do aging time.

Endereço do grupo

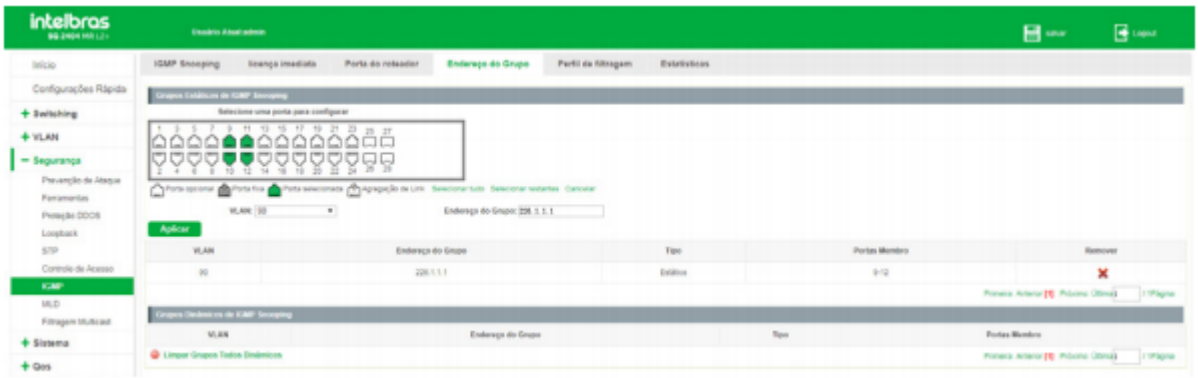
Além de portas estáticas, também é permitida a configuração de grupos multicast estáticos. Escolha o menu Segurança > IGMP > Endereço do grupo e siga as instruções a seguir para configurar um grupo estático:

1. Selecione a(s) porta(s) desejada(s) no painel de portas;
2. Selecione a VLAN desejada;
3. Digite o endereço multicast do grupo;
4. Clique em Aplicar.



Nesta página são exibidas informações a respeito dos grupos estáticos configurados e também dos grupos dinâmicos identificados automaticamente pela função IGMP Snooping. As informações a seguir são exibidas na página:

- **VLAN:** indica a VLAN onde foi detectado (ou configurado de forma estática) um grupo Multicast.
- **Endereço do Grupo:** exibe o endereço do grupo Multicast (configurado de forma estática ou detectado dinamicamente).
- **Tipo:** indica se o grupo foi configurado de forma estática ou se foi detectado de forma dinâmica.
- **Porta Membro:** exibe as portas membro do grupo Multicast.
- **Remover:** permite a remoção de um grupo estático. Para isto, basta clicar sobre o ícone (EXCLUIR).



Perfil de filtragem

Quando o IGMP Snooping é habilitado, é possível especificar uma faixa de endereços IP Multicast que serão permitidos ou negados de serem adicionados na tabela de endereços Multicast. Ao solicitar um grupo Multicast, o cliente envia uma mensagem IGMP Report, após receber a mensagem, o switch irá, em primeiro lugar, verificar as regras de filtragem de Multicast configuradas na porta de recebimento. Se a porta pode ser adicionada ao grupo Multicast, ela será adicionada a tabela de endereços Multicast, se a porta não pode ser adicionada ao grupo de Multicast, o switch irá bloquear a mensagem IGMP Report. Desta forma, impedindo a associação do cliente ao grupo Multicast

Para adicionar um filtro Multicast é necessário primeiramente especificar uma faixa de endereços Multicast e seu modo de operação, ou seja, permitir ou negar esta faixa de ser adicionada na tabela de endereços Multicast do switch. Após configurar a faixa, é necessário associá-la às portas desejadas.

Configurando faixa de endereços Multicast

Escolha o menu Segurança > IGMP > Perfil do filtragem e siga as instruções a seguir para configurar uma faixa de endereços Multicast:

1. Digite o ID da faixa (1 a 128);
2. Digite o endereço inicial da faixa;
3. Digite o endereço final da faixa;
4. Escolha o modo de operação (Permitir/Negar);
    - **Permitir:** permite a inclusão da faixa na tabela de endereços Multicast do switch.
    - **Negar:** não permite a inclusão da faixa na tabela de endereços Multicast do switch.
5. Clique em Aplicar.

Obs: são permitidas até 128 faixas de endereços Multicast

Editando faixa de endereços Multicast

Escolha o menu Segurança > IGMP > Perfil de filtragem e siga as instruções a seguir para editar uma faixa de endereços Multicast:

1. Clique no ícone (EDITAR) da faixa que deseja editar;
2. Edite as configurações desejadas;
3. Clique em Aplicar.

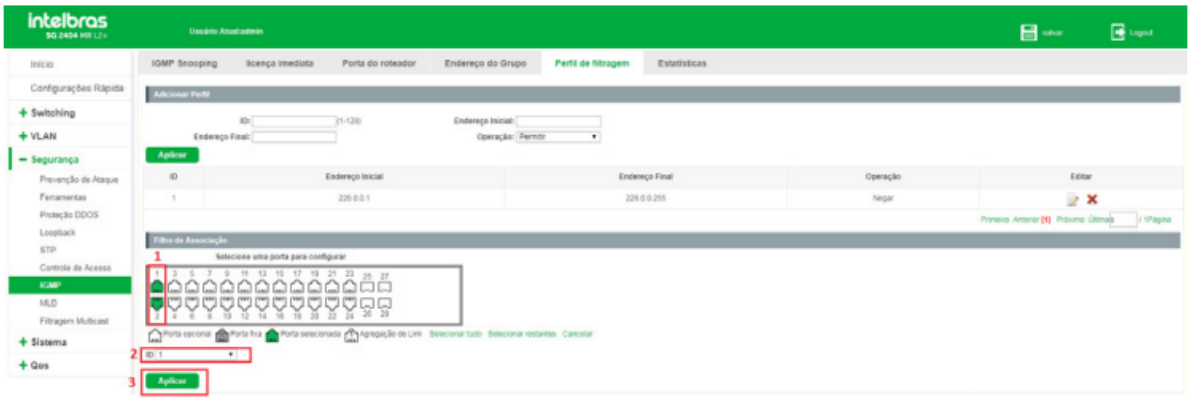
Para remover uma faixa de endereços Multicast, basta clicar sobre o ícone (EXCLUIR).

Obs: só é possível editar ou remover uma faixa de endereços Multicast caso esta faixa não esteja associada a nenhuma porta do switch.

Associando faixa de endereços Multicast

Após configurar uma faixa de endereços é possível associá-la a uma ou mais portas para aplicar o filtro Multicast. Para isto, escolha o menu Segurança > IGMP > Perfil de filtragem e siga as instruções a seguir:

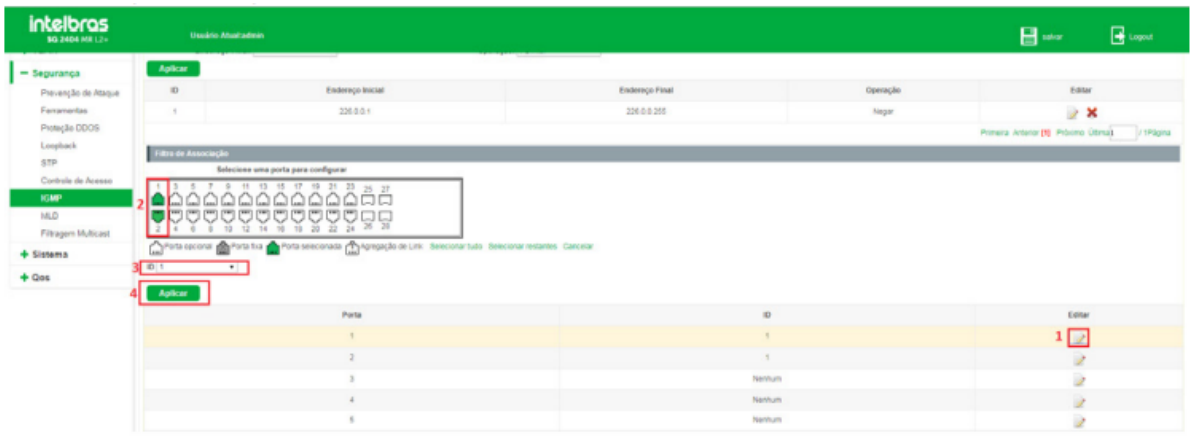
1. Selecione a(s) porta(s) que deseja associar no painel de portas;
2. Selecione o ID da faixa de endereços Multicast que deseja associar às portas selecionadas;
3. Clique em Aplicar.



Editando associação de faixa de endereços Multicast

Para editar uma associação de faixa de endereços Multicast, siga as instruções a seguir:

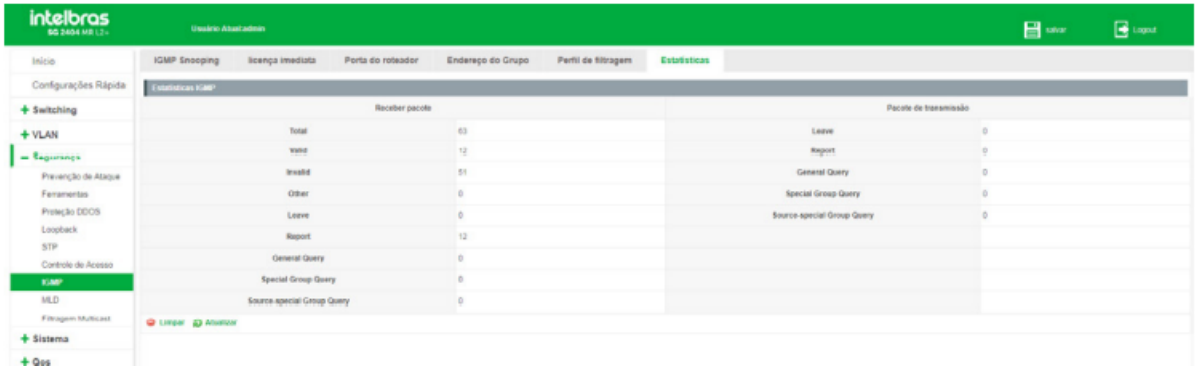
1. Clique no ícone ou selecione a(s) porta(s) que deseja editar no painel de portas;
2. Edite conforme desejar;
3. Clique em Aplicar.



Estatísticas IGMP

Este submenu permite a visualização das estatísticas geradas a partir do tráfego de pacotes Multicast transmitidos através do switch.

Escolha o menu Segurança > IGMP > Estatísticas para carregar a seguinte página:



As seguintes informações são exibidas na página:

- Receber pacote
  - **Total:** exibe o total de pacotes Multicast recebidos no switch
  - **Valid:** exibe o número de pacotes Multicast válidos recebidos no switch.
  - **Invalid:** exibe o número de pacotes Multicast inválidos recebidos no switch.
  - **Other:** exibe o número de outros tipos de pacotes recebidos pelo switch.
  - **Leave:** exibe o número de pacotes IGMP Leave que o switch recebeu.
  - **Report:** exibe o número de pacotes IGMP Report que o switch recebeu.
  - **General Query:** exibe o número de pacotes IGMP Query gerais que o switch recebeu
- Pacote de transmissão
  - **Leave:** exibe o número de pacotes IGMP Leave transmitidos pelo switch.
  - **Report:** exibe o número de pacotes IGMP Report que o switch transmitiu.
  - **General Query:** exibe o número de pacotes IGMP Query gerais que o switch transmitiu.

É possível limpar e atualizar as estatísticas exibidas na página, para isto basta clicar em Limpar e Atualizar, respectivamente.

MLD (*Multicast Listener Discovery*)

O MLD é um mecanismo de controle multicast semelhante ao protocolo IGMP Snooping, mas com a chegada do protocolo IPv6 o IGMP deu lugar ao MLD. Este protocolo permite o roteamento multicast no IPv6.

O MLD é utilizado por um roteador IPv6 para encontrar nós que desejam receber pacotes multicast e por hosts para anunciarem a necessidade em receber fluxos de pacotes multicast de um determinado endereço de grupo. Cada enlace pode possuir mais de um roteador, porém pode existir somente um (*Querier*). Todos os roteadores inicializam como Querier do enlace, caso o mesmo possua mais de um roteador, serão trocadas mensagens query entre os roteadores e o roteador com o endereço IPv6 numericamente menor se tornará o Querier, o outro será definido como Non-querier e terá a função de espelho do Querier, que se por algum problema parar de enviar mensagens query, será substituído pelo roteador Non-querier.

Mensagens MLD

O switch, executando o protocolo MLD, processa as mensagens MLD das seguintes formas:

- **Multicast Listener Query:** usada pelo roteador para buscar ouvintes multicast em um enlace, essa mensagem possuiu dois tipos:
  - **General Query:** aprende os endereços multicast que possuem ouvintes no enlace.
  - **Multicast-Address-Specific Query:** usada para verificar se algum endereço multicast em especifico possuiu ouvintes no enlace.
- **Multicast Listener Report:** esta mensagem é utilizada por ouvintes multicast para sinalizarem interesse em receber tráfegos multicast específicos e também para responderem a uma Query.
- **Multicast Listener Done:** esta mensagem é utilizada por ouvintes que desejam sair do grupo multicast.

MLD

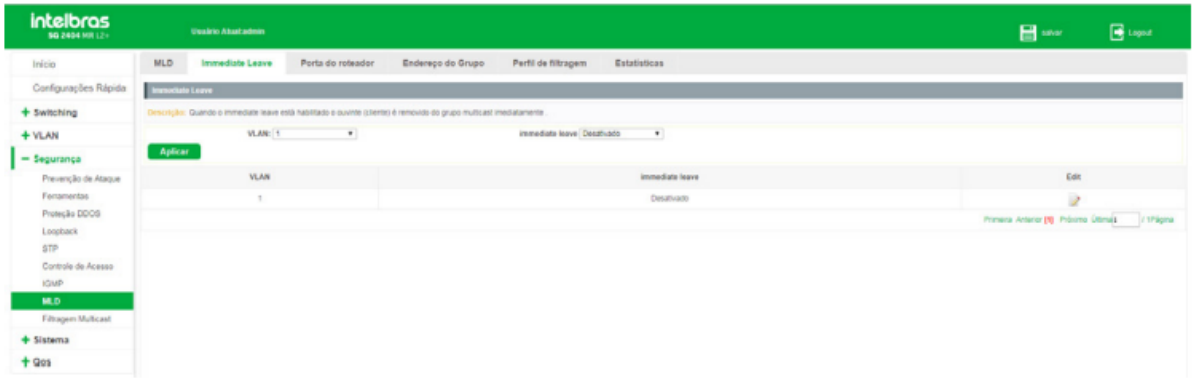
A função MLD pode ser configurada na seguinte tela: Segurança > MLD.

Ao ativar o MLD a seguinte página é apresentada:

- **Versão do MLD:** selecione a versão desejada.

Immediate Leave

Escolha o menu Segurança > MLD > Immediate Leave para ser exibida a seguinte tela:



As seguintes opções são exibidas na tela:

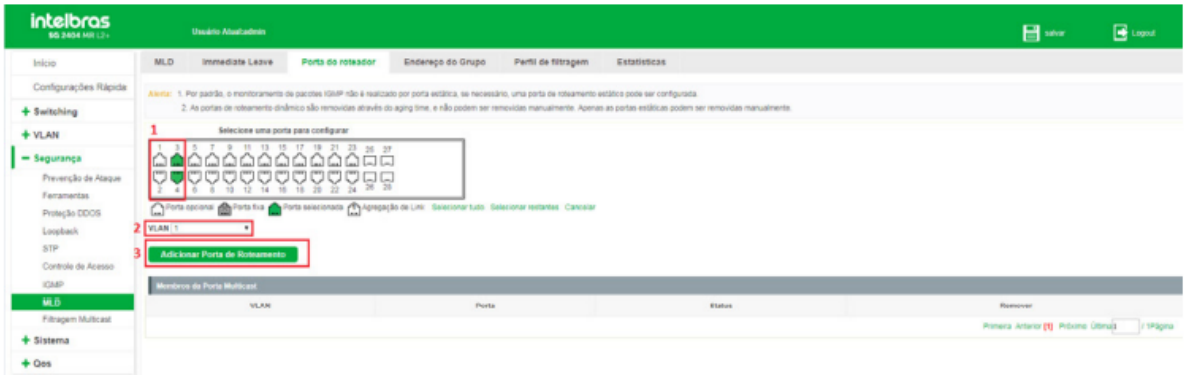
- **VLAN:** escolha a VLAN que deseja ser configurada.
- **Immediate Leave:** selecione ativar/desativar para habilitar ou desabilitar o Immediate Leave na VLAN selecionada.

Porta do roteador

O switch também permite configurar Portas roteador de forma estática. Desta forma é possível fixar portas roteador e removê-las quando necessário.

Escolha o menu Segurança > MLD > Porta roteador siga as instruções aseguir para configurar uma porta roteador estática.

1. Selecione a(s) porta(s) desejada(s) no painel de portas;
2. Selecione a VLAN desejada;
3. Clique em Adicionar porta de roteamento.



Nesta página são exibidas também as portas que foram detectadas automaticamente pelo MLD. A tabela Membros da Porta Multicast exibe as seguintes informações:

- **VLAN:** indica a VLAN onde foi detectado (ou configurado de forma estática) um tráfego multicast.
- **Porta:** exibe a porta onde foi detectado (ou configurado de forma estática) um tráfego multicast.
- **Status:** indica se a porta foi configurada de forma estática ou se foi detectado tráfego multicast de forma dinâmica.
- **Remover:** permite a remoção de uma porta roteador, seja ela dinâmica ou estática. Para isto, basta clicar sobre o ícone (EXCLUIR).

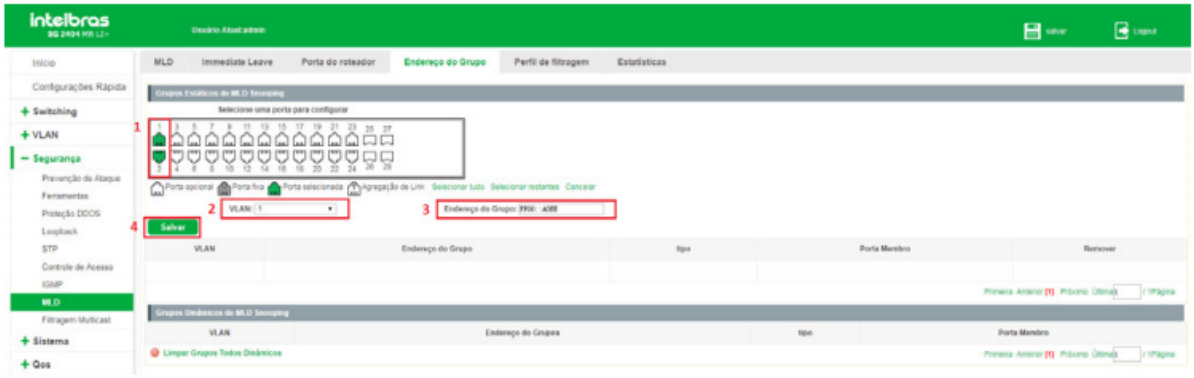
Observações:

- É necessário que a porta esteja configurada na VLAN desejada para que ela seja configurada como porta roteador naquela VLAN.
- Não é possível remover portas dinâmicas. Estas portas serão removidas automaticamente através do aging time.

Endereço de grupo

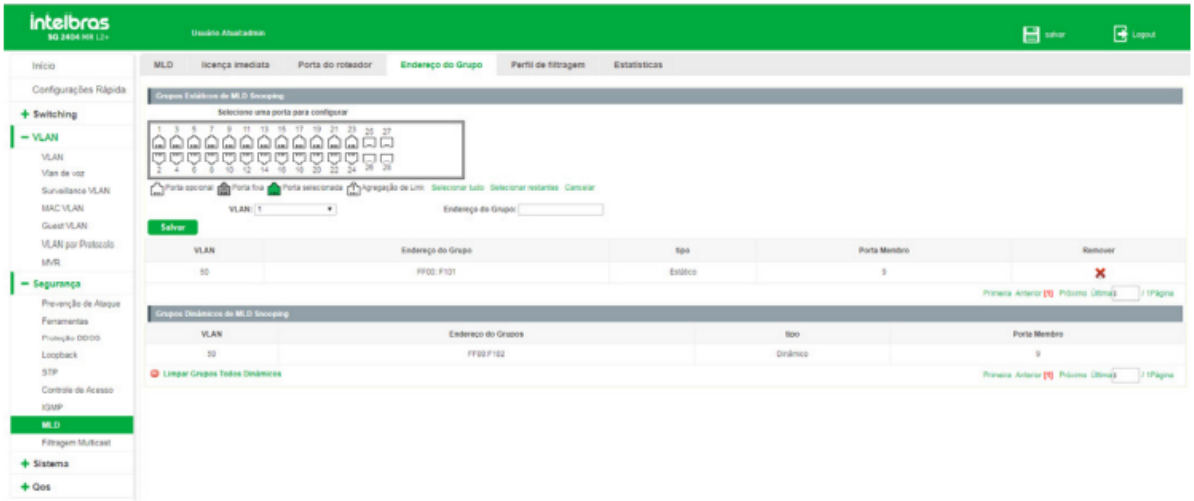
Além de portas estáticas, também é permitida a configuração de grupos multicast estáticos. Escolha o menu Segurança > MLD > Endereço do grupo e siga as instruções a seguir para configurar um grupo estático.

1. Selecione a(s) porta(s) desejada(s) no painel de portas;
2. Selecione a VLAN desejada;
3. Digite o endereço multicast do grupo;
4. Clique em Aplicar.



Nesta página são exibidas informações a respeito dos grupos estáticos configurados e também dos grupos dinâmicos identificados automaticamente pelo MLD. As informações a seguir são exibidas na página:

- **VLAN:** indica a VLAN onde foi detectado (ou configurado de forma estática) um grupo Multicast.
- **Endereço do grupo:** exibe o endereço do grupo Multicast (configurado de forma estática ou detectado dinamicamente).
- **Tipo:** indica se o grupo foi configurado de forma estática ou se foi detectado de forma dinâmica.
- **Porta membro:** exibe as portas membro do grupo Multicast.
- **Remover:** permite a remoção de um grupo estático. Para isto, basta clicar sobre o ícone (EXCLUIR).



Perfil de filtragem

Quando o MLD é habilitado, é possível especificar uma faixa de endereços IP Multicast que serão permitidos ou negados de serem adicionados na tabela de endereços Multicast. Ao solicitar um grupo Multicast, o cliente envia uma mensagem Multicast Listener Report, após receber a mensagem, o switch irá, em primeiro lugar, verificar as regras de filtragem de Multicast configuradas na porta de recebimento. Se a porta pode ser adicionada ao grupo Multicast, ela será adicionada a tabela de endereços Multicast, se a porta não pode ser adicionada ao grupo de Multicast, o switch irá bloquear a mensagem Multicast Listener Report. Desta forma, impedindo a associação do cliente ao grupo Multicast.

Para adicionar um filtro Multicast é necessário primeiramente especificar uma faixa de endereços Multicast e seu modo de operação, ou seja, permitir ou negar esta faixa de ser adicionada na tabela de endereços Multicast do switch. Após configurar a faixa, é necessário associá-la às portas desejadas.

Configurando faixa de endereços Multicast

Escolha o menu Segurança > MLD > Perfil de filtragem e siga as instruções a seguir para configurar uma faixa de endereços Multicast.

1. Digite o ID da faixa (1 a 128);
2. Digite o endereço inicial da faixa;
3. Digite o endereço final da faixa;
4. Escolha o modo de operação (Permitir/Negar);
   - **Permitir:** permite a inclusão da faixa na tabela de endereços Multicast do switch.
   - Negar: não permite a inclusão da faixa na tabela de endereços Multicast do switch.
5. Clique em Aplicar.

Obs: são permitidas até 128 faixas de endereços Multicast.

Editando faixa de endereços Multicast

Escolha o menu Segurança > MLD > Perfil de filtragem e siga as instruções a seguir para editar uma faixa de endereços Multicast.

1. Clique no ícone da faixa que deseja editar;
2. Edite as configurações desejadas;
3. Clique em Aplicar.

Para remover uma faixa de endereços Multicast, basta clicar sobre o ícone (EXCLUIR).

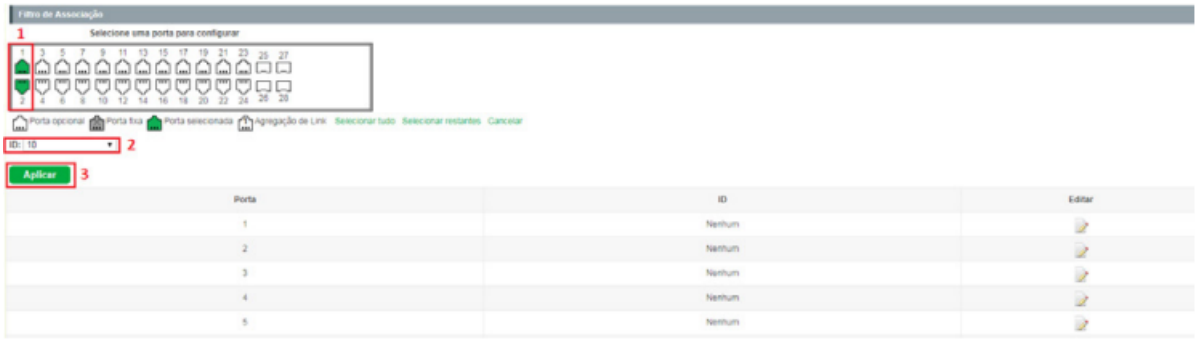
Obs: só é possível editar ou remover uma faixa de endereços Multicast caso esta faixa não esteja associada a nenhuma porta do switch.

Associando faixa de endereços Multicast

Após configurar uma faixa de endereços é possível associá-la a uma ou mais portas para aplicar o filtro Multicast. Para isto, escolha o menu Segurança > MLD > Perfil de filtragem e siga as instruções a seguir:

1. Selecione a(s) porta(s) que deseja associar no painel de portas;

2. Selecione o ID da faixa de endereços Multicast que deseja associar às portas selecionadas;
3. Clique em Aplicar.



Estatísticas IGMP

Este submenu permite a visualização das estatísticas geradas a partir do tráfego de pacotes Multicast transmitidos através do switch.

Escolha o menu Segurança > MLD > Estatísticas para carregar a seguinte página:

As seguintes informações são exibidas na página:

- **Receber pacote**
  - **Total:** exibe o total de pacotes Multicast recebidos no switch.
  - **Valid:** exibe o número de pacotes Multicast válidos recebidos no switch.
  - **Invalid:** exibe o número de pacotes Multicast inválidos recebidos no switch.
  - **Other:** exibe o número de outros tipos de pacotes recebidos pelo switch.
  - **Leave:** exibe o número de pacotes MLD Done que o switch recebeu.
  - **Report:** exibe o número de pacotes MLD Report que o switch recebeu
  - **General Query:** exibe o número de pacotes General Query gerais que o switch recebeu.
- **Pacote de transmissão**
  - **Leave:** exibe o número de pacotes MLD Done transmitidos pelo switch.
  - **Report:** exibe o número de pacotes MLD Report que o switch transmitiu.
  - **General Query:** exibe o número de pacotes General Query gerais que o switch transmitiu.

É possível limpar e atualizar as estatísticas exibidas na página, para isto basta clicar em Limpar e Atualizar, respectivamente.

SISTEMA

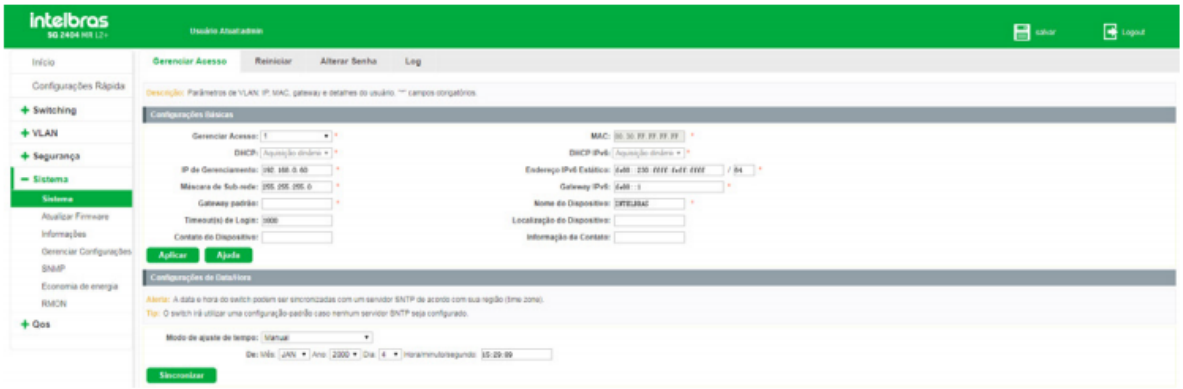
O menu Sistema é utilizado para configuração do switch. Nele podemos realizar configurações de acesso, boot, atualização do sistema, SNMP e RMON.

Sistema

Neste submenu é possível realizar ajustes de data e hora, reiniciar o equipamento, alterar senha e verificar o *log* do equipamento.

Gerenciar VLAN

Na página Sistema > Sistema > Gerenciar VLAN. É apresentado a seguinte tela.



As seguintes opções são exibidas na tela:

- **Configurações básicas**
  - **Gerenciar acesso:** por padrão, o gerenciamento do switch é feito via VLAN 1, que está atribuída a todas as portas, sendo assim, o switch pode ser gerenciado através de todas as portas. No entanto, essa configuração pode ser alterada atribuindo o gerenciamento VLAN a uma interface. Descrição: atribuir o gerenciamento VLAN a uma interface

    Na página Sistema > Sistema > Gerenciar Acesso.

    1. Clique no ícone (OFF) para atribuir o gerenciamento VLAN.
    2. Selecione a VLAN desejada.
    3. Selecione Alocação estática
    4. Adicione o IP desejado
    5. Adicione a máscara de sub-rede.
    6. Clique em Aplicar.

    Exemplo: atribuir o estado de gerenciamento a VLAN 10:

    Atenção: após essa configuração, o switch só poderá ser gerenciado pela(s) porta(s) atribuída(s) a VLAN.

- **DHCP**
  - **Alocação estática:** quando esta opção for selecionada, você deverá digitar o endereço IP, máscara de rede e gateway padrão manualmente.
  - **Alocação dinâmica:** quando esta opção for selecionada, o switch receberá o endereço IP e parâmetros de rede através de um servidor DHCP
- **IP de gerenciamento:** Defina o IP no qual o switch será acessado pelo navegador.
- **Máscara de sub-rede:** Digite a máscara de sub-rede do switch quando estiver selecionado o modo IP Estático.
- **Gateway Padrão / Gateway IPv6:** Digite o gateway padrão do switch quando estiver selecionado o modo IP Estático.

Observações:

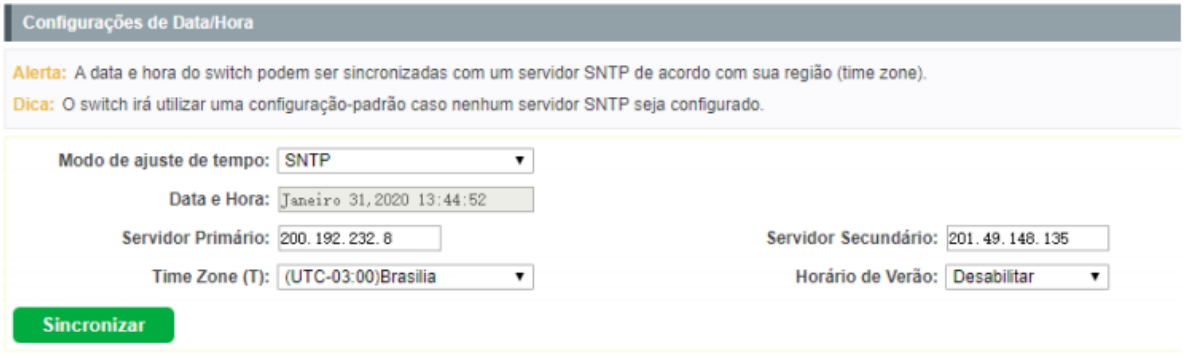
- Alterando o endereço IP, para um IP localizado em uma sub-rede diferente, ocorrerá perda na comunicação com o switch. Para isso não acontecer, mantenha o endereço IP do switch dentro da mesma sub-rede da rede local.
- O switch possui somente um endereço IP. O endereço IP é configurável substituindo o endereço IP original. Por padrão, o endereço IP do switch é 192.168.0.1.

- **Timeout(s) de login:** configura o tempo da sessão. Caso o usuário fique inativo num período de tempo maior que o configurado na interface web, o switch encerra a sessão e deverão ser inseridas as credenciais de acesso para restabelecer a conexão. Este campo é configurado em segundos
- **MAC:** mostra o MAC que está configurado no switch. Neste campo não é possível alterar o MAC.
- **DHCP Ipv6**
  - **Alocação estática:** quando esta opção for selecionada, você deverá digitar o endereço IP (IPV6), máscara de rede e gateway padrão manualmente
  - **Alocação dinâmica:** quando esta opção for selecionada, o switch receberá o endereço IP (IPV6) e parâmetros de rede através de um servidor DHCP.
- **Endereço IPV6 estático:** defina o IP no qual o switch será acessado pelo navegador utilizando o protocolo IPV6.
- **Nome do dispositivo:** este nome é visualizado na sessão de login
- **Localização do dispositivo:** informa aonde o equipamento está localizado fisicamente, exemplo: RACK – Sala 01.
- **Contato do dispositivo:** número para entrar em contato com o dono do dispositivo.

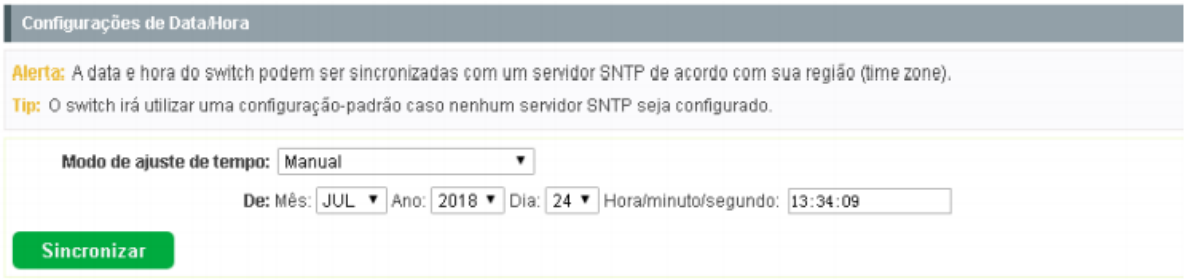
- **Informações do contato:** localização ou outras informações relevantes sobre o dono do dispositivo

- **Data e Hora**

Nesta página você pode configurar a data e hora do sistema que serão utilizadas por outras funções que necessitam deste tipo de informação. A configuração poderá ser realizada de forma automática, conectando-se a um servidor NTP, de forma manual ou ainda pela timezone. Escolha o menu Sistema > Sistema > Data/Hora para carregar a seguinte página:



- **Modo SNTP:** quando esta opção estiver selecionada, você pode configurar o fuso horário e o IP do servidor NTP. A mudança somente ocorrerá após o switch se conectar ao servidor NTP.
- **Servidor Primário:** indique o endereço IP do servidor NTP ao qual o switch se conectará para adquirir a informação de data e hora
- **Servidor Secundário:** indique o enderçeo IP de um servidor NTP ao qual o switch se conectará caso não seja possível se conectar ao servidor primário.
- **Fuso horário:** selecione o fuso horário desejado.
- **Horário de verão:** ative ou desative o horário de verão.
- **Manual:** quando esta opção estiver selecionada, você pode configurar o fuso horário manualmente. Preencha o mês, dia, ano e o horário desejado para sincronizar. Neste Modo quando reiniciar o switch as informações de data e hora irão retornar para o padrão de fábrica.



Reiniciar

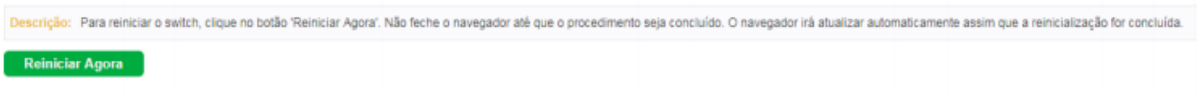
Nesta página é possível reiniciar o switch e retornar a página de login. Para evitar a perda das configurações realizadas ao reiniciar o switch, salve as modificações no menu > Sistema > Gerenciar configurações. Escolha o menu Sistema > Sistema > Reiniciar para carregar a seguinte página:

Clique em (REINICIAR AGORA) para reiniciar o equipamento.

Obs: para evitar danos, por favor, não desligue o switch durante a reinicialização.

Alterar senha

Tela destinada a alterar a senha de login de acesso do equipamento. Para encontrar a seguinte tela escolha o menu Sistema > Sistema > Altera senha:



Sistema - Reiniciar

Obs: a senha alterada nessa etapa não se aplica a senha de acesso via CLI.

Log

O sistema de Log do switch pode registrar, pesquisar e gerenciar as informações do sistema de forma eficaz, fornecendo um poderoso suporte para administração de redes, monitorando a operação da rede e diagnosticando avarias. Escolha o menu Sistema > Sistema > Log/Exportar log.

Digite o IP do servidor TFTP e o nome do arquivo que será enviado ao computador.

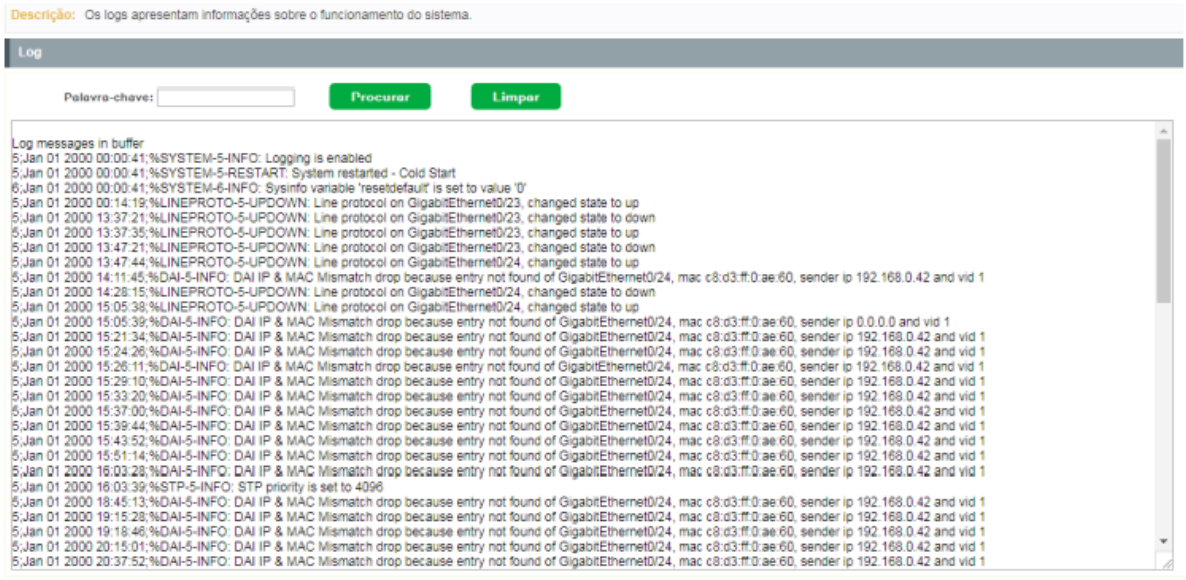
Obs: poderá levar alguns minutos para fazer o Export do arquivo de Log. Aguarde sem executar qualquer operação

Na tela de LOG é possível encontrar o tipo do LOG digitando na área de busca Palavra-Chave.

Por exemplo: ao digitar SSH são encontrados os logs referente ao protocolo SSH. Clique em (LIMPAR) para limpar a tela de LOG.

Exportar Log

A função Exportar Log permite que o sistema registre as informações de log do switch em arquivos, tornando possível sua análise posteriormente. Quando um erro crítico acontecer e o sistema entrar em colapso, você poderá exportar os logs após o switch ser reiniciado.



Atualizar firmware

O firmware do switch pode ser atualizado através da página de gerenciamento web. Para atualizar o sistema com a versão mais recente do firmware, faça o download através do site da Intelbras www.intelbras.com.br (http://www.intelbras.com.br). É recomendável que seja feito um backup das configurações do switch antes do procedimento, pois a atualização do firmware pode causar a perda de todas as configurações existentes. Escolha no menu Sistema > Sistema > Atualizar firmware para carregar a seguinte página:

Observações:

- Não interrompa a atualização do switch.
- Selecione a versão de software apropriada para seu hardware.
- Após a atualização do firmware, o switch reiniciará automaticamente. Esta atualização poderá levar alguns minutos.
- É sugerido que você faça um backup das configurações antes de atualizar.

Informações

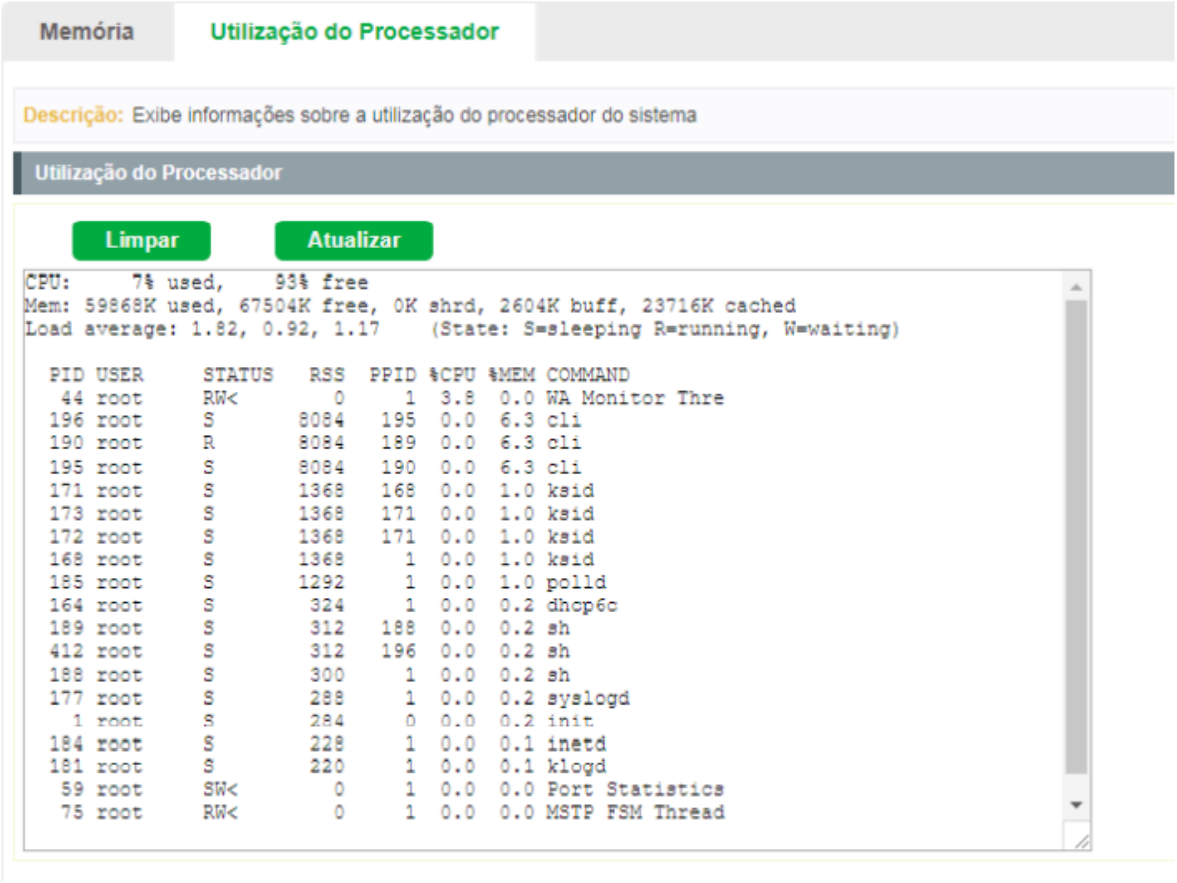
A função de informações exibe o status de utilização da memória e da CPU do switch. A taxa de utilização da CPU e a taxa de utilização da memória devem apresentar-se de forma estável em torno de um valor específico. Se a taxa de utilização da CPU ou a taxa de utilização da memória aumentar muito, por favor, verifique se a rede está sendo atacada. A função Monitoramento é visualizada nas páginas Memória e Utilização do processador.

Memória

Escolha o menu Sistema > Sistema > Informações para carregar a seguinte página:

Utilização do processador

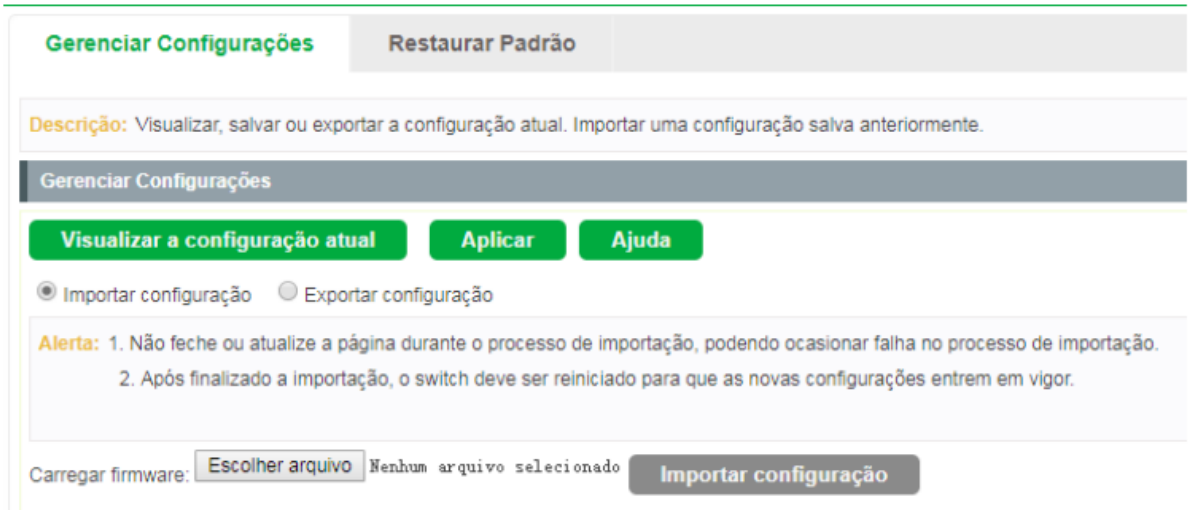
Escolha o menu Sistema > Sistema > Utilização do processador Informações para carregar a seguinte página:



Gerenciar configurações

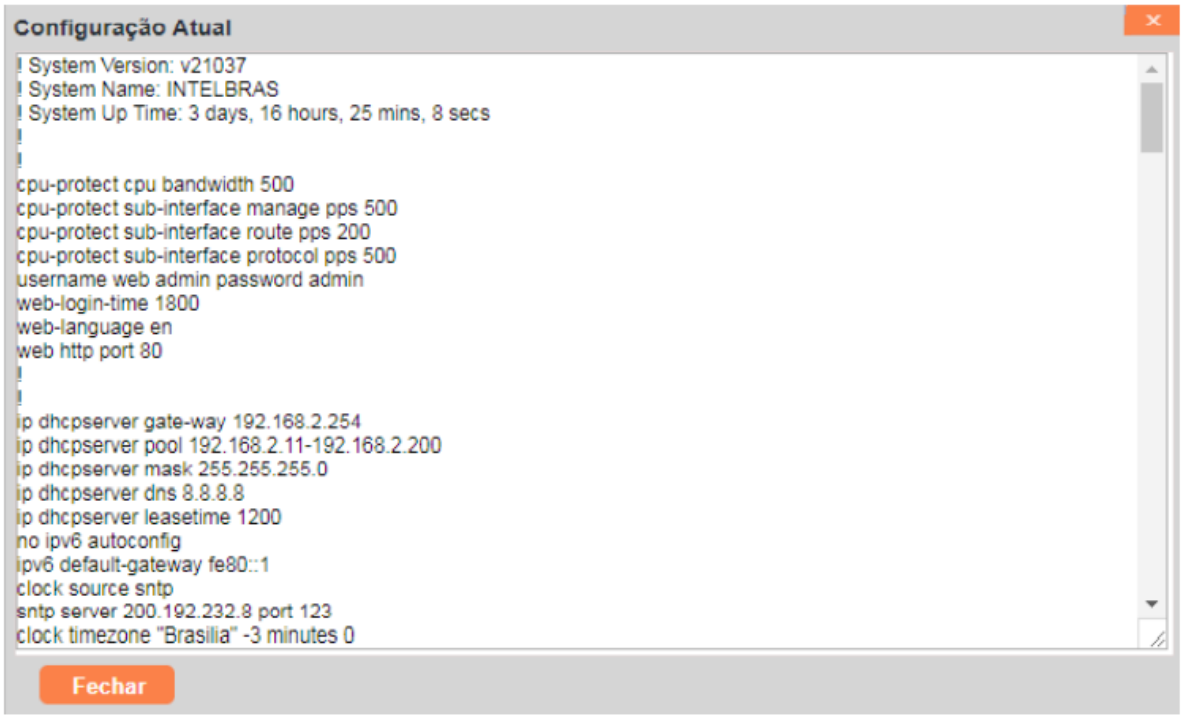
Em Gerenciar configurações você pode visualizar as configurações atuais do switch, restaurar o padrão de fábrica e importar e exportar configurações. Escolha o menu Sistema > Gerenciar configurações.

Gerenciar configurações



Clique em (VISUALIZAR CONFIGURAÇÃO ATUAL) para verificar as configurações atuais do equipamento.

Será exibida a seguinte página:



Clique em (APLICAR) para aplicar as configurações realizadas no switch.

Obs: é indicado que em cada configuração realizada no equipamento seja salvo as configurações. Caso o switch desligue e não sejam salvas as alterações, todas as configurações serão perdidas.

Importar e exportar configurações

Selecione o campo *Importar* para importar configurações ou *Exportar* para exportar as configurações do switch.

Observações:

- Não feche ou atualize a página durante o processo de importação, podendo ocasionar falha no processo de importação.
- Após finalizada a importação, o switch deve ser reiniciado para que as novas configurações entrem em vigor.

Restaurar padrão

Escolha o menu Sistema > Gerenciar configurações > Restaurar padrão e a seguinte página será exibida:

Clique em (RESTAURAR) para restaurar o switch para o padrão de fábrica.

Observações:

- A restauração das configurações levará alguns segundos. Por favor, espere sem realizar nenhuma outra operação.
- Enquanto as configurações estiverem sendo restauradas, não desligue o switch.
- Após serem restauradas, as configurações atuais serão perdidas. Fazer o upload de um arquivo de backup errado pode fazer com que o switch perca o gerenciamento.

SNMP

SNMP

As configurações SNMP se encontram no menu Sistema > SNMP > Configurar SNMP.

A seguinte página é exibida:

Configuração SNMP

SNMP: selecione On/Off para habilitar ou desabilitar a função SNMP.

Engine SNMP Local

Engine ID local: digite a identificação do SNMP Engine do switch Local, este parâmetro é utilizado pelos clientes remotos. O engine ID é uma sequência de caracteres alfanuméricos únicos, usado para identificar o switch.

Engine SNMP Remoto

Tipo de endereço: selecione o tipo do endereço do servidor:

- **Hostname:** selecione esta opção para entrar com endereços URL.
- **IPv4:** selecione esta opção para entrar com endereços IPv4.
- **IPv6:** selecione esta opção para entrar com endereços IPv6.

Endereço do servidor: digite o endereço do servidor para onde serão enviadas as mensagens SNMP.

Engine SNMP remoto: digite a identificação do SNMP Engine do switch remoto (o Engine Remoto é utilizado para o envio de snmp inform V3 para o switch ou dispositivo remoto SNMP v3). O Engine ID é uma sequência de caracteres alfanuméricos únicos, usado para identificar o switch.

Obs: a quantidade de caracteres para identificação dos Engines IDs devem ser o mesmo

View SNMP

O OID (*Object Identifier*) dos pacotes SNMP são usados para descrever os objetos gerenciados do switch, e as MIB (*Management Information Base*) são o conjunto dos OIDs. A View SNMP é criada para a estação de gerenciamento SNMP gerenciar os objetos MIB.

Configurar View

- **Nome da view:** digite o nome de identificação da view. Cada view pode incluir várias entradas com o mesmo nome.
- **MIB OID:** digite o OID utilizado pela view
- **Modo da view:** selecione o tipo de entrada da view.

- **Incluir:** inclui para o gerenciamento da view o OID especificado.
- **Excluir:** exclui do gerenciamento da view o OID especificado.

- **Modo da máscara:** selecione o modo da máscara.
  - **Manual:** desbloqueia o campo máscara OID e nele é possível configurar as OID que podem ser visualizadas.
  - **Todos:** libera a visualização de todas as OIDs.

- **Máscara OID:** filtra as OID que poderão ser visualizadas. Por exemplo: na OID 1.3.6.1.2. Se inserido a máscara 11110, será possível visualizar todas as da OID 1.3.6.1.x em diante.

Grupo SNMP

Nesta página você pode configurar grupos SNMP para controlar o acesso à rede, fornecendo aos usuários de vários grupos diferentes, permissões de leitura, escrita e notificação.

As configurações do Grupo SNMP se encontram no menu Sistema > SNMP > Grupo SNMP.

Configuração do grupo SNMP

- **Nome do grupo SNMP:** digite o nome do grupo SNMP.
- **Versão do SNMP:** selecione a versão do protocolo SNMP utilizado pelo grupo SNMP.
  - **v1:** nesta versão, o nome da comunidade é utilizado para a autenticação. O SNMP v1 pode ser configurado diretamente na página de configuração Comunidade SNMP
  - **v2C:** nesta versão, o nome da comunidade é utilizado para a autenticação. O SNMP v2c pode ser configurado diretamente na página de configuração Comunidade SNMP.
  - **v3:** nesta versão, o mecanismo USM é utilizado para realizar a autenticação. Ao habilitar o SNMP v3, o campo nível de segurança deverá ser configurado.

- **Nível de segurança:** selecione o nível de segurança para grupos SNMPv3.
  - **noAuthNoPriv:** este nível de segurança não realiza autenticação e criptografia.
  - **authNoPriv:** este nível de segurança realiza autenticação porém não realiza criptografia.
  - **authPriv:** este nível de segurança realiza autenticação e criptografia.

- **View de leitura:** selecione a view desejada com acesso somente de leitura. A view definida como leitura somente poderá ser lida, não é possível modificá-la
- **View de escrita:** selecione a view desejada com acesso de escrita. A view definida como escrita poderá ser lida e alterada.
- **View de notificação:** selecione a view desejada com permissão de notificação. A view definida como notificação poderá enviar notificações a estação de gerenciamento SNMP.

Obs: cada Grupo SNMP deve conter uma view de leitura. A view de leitura padrão é view Default.

Grupos SNMP configurados

- **Grupo SNMP:** exibe o nome do grupo SNMP.
- **Versão SNMP:** exibe a versão do protocolo SNMP utilizada pelo grupo SNMP.
- **Nível de segurança:** exibe o nível de segurança do grupo SNMP.
- **View de leitura:** exibe a view de leitura.
- **View de escrita:** exibe a view de escrita.
- **View de notificação:** exibe a view de notificação.
- **Excluir:** clique no ícone (EXCLUIR) para excluir.

Usuário SNMP

Nesta página é possível configurar o nome de usuário que gerenciará o grupo SNMP. O usuário e grupo SNMP devem possuir o mesmo nível de segurança e direito de acesso.

As configurações do Usuário SNMP se encontram no menu Sistema > SNMP > Usuário SNMP.

Configuração do usuário SNMP

- **Nome de usuário**: digite o nome de usuário.
- **Versão SNMP:** selecione a versão do protocolo SNMP utilizado pelo usuário criado.
- **Autenticação:** selecione o modo de autenticação para o usuário SNMP v3.
  - **Nenhum:** nenhum método de autenticação é usado.
  - **MD5:** a autenticação da porta usa o algoritmo HMAC-MD5.
  - **SHA:** a autenticação da porta é realizada através de SHA (Secure Hash Algorithm). Esse modo de autenticação tem uma segurança maior que o modo MD5.
- **Criptografia:** selecione o modo de criptografia para o usuário SNMP v3.
  - **Nenhum:** nenhum método de criptografia é utilizado.

    - **DES:** utiliza o método de encriptação DES.

- **Grupo SNMP:** selecione o grupo SNMP desejado. O usuário é classificado para o grupo correspondente de acordo com o Nome do Grupo, Versão e Nível de Segurança SNMP.
- **Nível de segurança:** selecione o nível de segurança para o usuário SNMP v3.
- **Senha de autenticação:** digite a senha configurada para autenticação.
- **Senha de criptografia:** digite a senha configurada utilizada na criptografia.

Configuração do usuário SNMP

- **Nome de usuário:** exibe o nome do usuário.
- **Grupo SNMP:** exibe o nome do grupo do usuário.
- **Versão SNMP:** exibe a versão do protocolo SNMP utilizado pelo usuário.
- **Nível de segurança:** exibe o modo de segurança do usuário SNMP.
- **Autenticação**: exibe o modo de autenticação do usuário.
- **Criptografia:** exibe o modo de criptografia do usuário.
- **Excluir:** clique no ícone (EXCLUIR) para excluir.

Obs: o usuário e grupo SNMP devem possuir o mesmo modo e nível de segurança.

Comunidade SNMP

O SNMP v1 e v2c utiliza o método de autenticação baseado no nome da comunidade. O nome da comunidade pode limitar o acesso ao agente SNMP da estação de gerenciamento SNMP, funcionando como uma senha. Caso a versão do protocolo utilizada for, SNMP v1 ou SNMP v2c, é possível configurar a função utilizando somente esta página sem a necessidade de configurar as páginas Grupos SNMP e Usuários SNMP

As configurações da Comunidade SNMP se encontram no menu Sistema > SNMP > Comunidade SNMP.

Configuração de comunidade SNMP

- **Nome da comunidade:** digite o nome da comunidade.
- **Modo de acesso:** defina o tipo de permissão para a comunidade.
    - **Leitura:** neste modo, a comunidade terá permissão somente de leitura, nenhuma alteração poderá ser feita.
    - **Leitura/escrita:** neste modo, a comunidade terá permissão de leitura e escrita, podendo realizar alterações.
- **MIB View:** selecione a view de acesso da comunidade.

Comunidades SNMP configuradas

- **Nome da comunidade:** exibe o nome da comunidade.
- **Modo de acesso:** exibe o tipo de permissão da comunidade para acessar a view.
- **MIB view:** exibe a view que a comunidade pode acessar.
- **Excluir:** clique no ícone (EXCLUIR) para excluir.

Notificação

Com a função de notificação habilitada, o switch pode intuitivamente reportar as estações de gerenciamento SNMP, eventos que ocorreram nas views (ex.. Dispositivos reiniciados) permitindo que as estações de gerenciamento monitorem e processem os eventos.

As informações de notificação incluem os seguintes tipos:

- **Trap:** é a informação que o dispositivo gerenciado envia para a estação de gerenciamento de rede sem nenhum tipo de solicitação.
- **Inform:** pacotes inform são enviados para informar a estação de gerenciamento sobre eventuais eventos e sempre aguardam uma resposta. A notificação Inform somente é utilizada com o SNMP v3 e possui uma maior segurança quando comparado ao Trap.

Nesta página, você pode configurar as notificações da função SNMP. As configurações de Notificação se encontram no menu Sistema > SNMP > Notificação

Configuração de notificação

- **Endereço IP:** digite o endereço da estação de gerenciamento SNMP.
- **Porta UDP:** digite o número da porta UDP usada para enviar notificações. Padrão é 162.
- **Usuário:** digite o nome de usuário da estação de gerenciamento.
- **Versão SNMP:** selecione a versão do protocolo SNMP.
- **Nível de segurança:** selecione o nível de segurança para grupos SNMPv3.
  - **noAuthNoPriv:** este nível de segurança não realiza autenticação e criptografia.
  - **authNoPriv:** este nível de segurança realiza autenticação porém não realiza criptografia.
  - **AuthPriv:** este nível de segurança realiza autenticação e criptografia.
- **Tipo de notificação:** selecione o tipo de notificação.
  - **Trap:** indica que o tipo de notificação utilizada é a Trap.

- **Inform:** indica que o tipo de notificação utilizada é a Inform. O tipo Inform tem maior segurança em relação ao tipo Trap.

- **Reenviar:** insira a quantidade de vezes que o switch reenvia uma solicitação inform.
- **Tempo máximo:** insira o tempo máximo para o switch esperar pela resposta da estação de gerenciamento SNMP antes de reenviar um pedido.

Notificações configuradas

- **Endereço IP:** exibe o endereço IP da estação de gerenciamento SNMP.
- **Porta UDP:** exibe a porta UDP usada para notificações.
- **Usuário:** exibe o nome de usuário da estação de gerenciamento.
- **Versão SNMP:** exibe a versão do protocolo SNMP.
- **Nível de segurança:** exibe o nível de segurança SNMPv3.
- **Tipo de notificação:** exibe o tipo de notificação.
- **Reenviar:** exibe a quantidade de vezes que o switch reenvia uma solicitação inform.
- **Tempo máximo:** exibe o tempo máximo para o switch esperar pela resposta da estação de gerenciamento SNMP antes de reenviar um pedido.
- **Excluir:** clique no ícone para excluir.

EEE

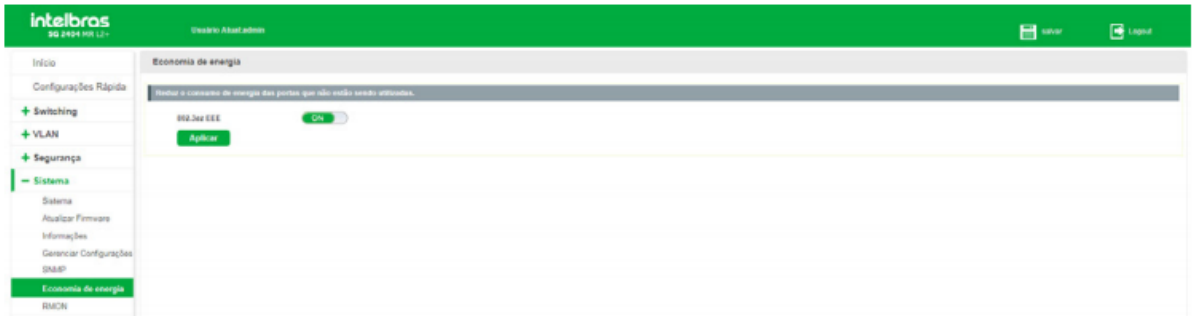
Ethernet com Eficiência Energética (EEE) é um padrão IEEE 802.3az projetado para reduzir o consumo de energia em redes Ethernet durante períodos inativos.

Ele regula a potência de transmissão para conexões menores de 100 metros e desativa o consumo das portas que não estão conectadas.

EEE

Configurações do EEE

No menu EEE a seguinte tela é exibida:



EEE - configuração

Clique em (ON) para ativar o modo EEE.

RMON

RMON (*Remote Monitoring*) é baseado na arquitetura SNMP (*Simple Network Management Protocol*). RMON é atualmente um padrão de gerenciamento de rede definido pelo *Internet Engineering Task Force* (IETF), é utilizado principalmente para monitorar o tráfego de dados através de um segmento de rede ou até mesmo de toda a rede, de modo a permitir que o administrador da rede possa tomar as medidas de proteção a tempo de evitar qualquer mau funcionamento da rede. Além disso, as MIB RMON registram informações estatísticas de desempenho da rede e mau funcionamento periodicamente, com base no que as estações de gerenciamento podem monitorar. RMON é útil para administradores de rede, para gerenciar a rede em grande escala, uma vez que reduz o tráfego de comunicação entre as estações de gerenciamento e os agentes de gerenciamento.

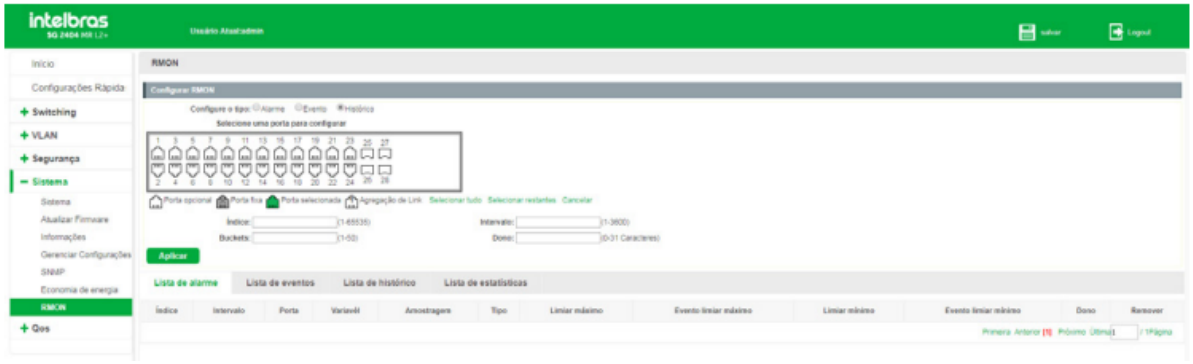
Grupos RMON

Este switch suporta os seguintes grupos RMON definidos no **padrão RFC1757**, *Históricos, Eventos, Estatísticas e Alarmes*.

Grupos RMON	**Descrição**
Grupo Histórico	Após configurado o grupo Histórico, o switch coleta e registra periodicamente informações de estatísticas de rede, baseado no que as estações de gerenciamento podem informar de forma eficaz.
Grupo Evento	O grupo Evento é utilizado para definir eventos RMON. Alarmes ocorrem quando um evento é detectado.
Grupo Estatística	O grupo Estatística é utilizado para monitorar as estatísticas variáveis de alarme nas portas especificadas.
Grupo Alarme	O grupo Alarme é utilizado para monitorar variáveis de alarme. Quando o valor de uma variável exceder o limite previamente estabelecido, um evento de alarme será gerado.

Histórico RMON

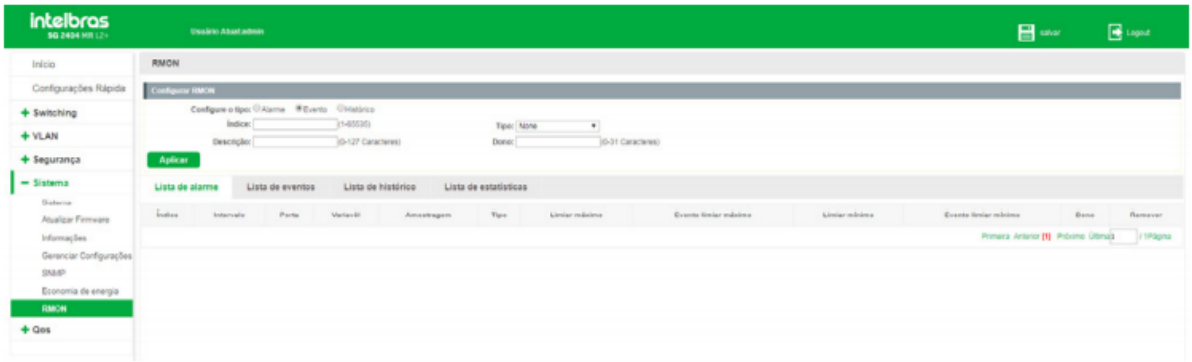
Nesta página você pode configurar o grupo Histórico da função RMON. Escolha o menu Sistema > RMON > Histórico para carregar a página seguinte:



- **Índice:** digite o índice da entrada.
- **Intervalo:** especifique o intervalo de coleta das amostras.
- **Bucket:** digite o número de históricos que poderão ser armazenados.
- **Dono:** digite o nome do dispositivo ou usuário que definiu a regra.
- **Porta:** selecione a(s) porta(s) desejada(s).

Evento RMON

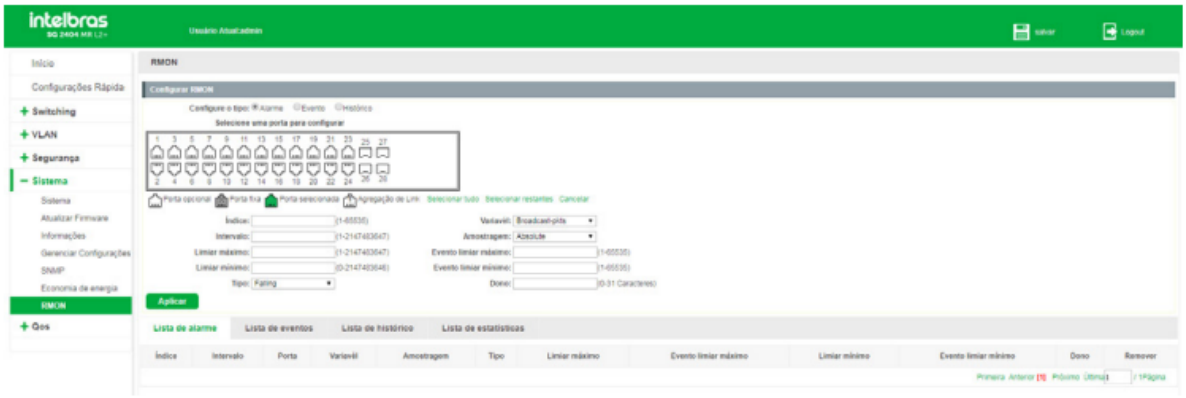
Nesta página você pode configurar o grupo Histórico da função RMON. Escolha o menu Sistema > RMON > Evento para carregar a página seguinte:



- **Índice:** digite o índice da entrada.
- **Descrição:** digite uma descrição para identificação.
- **Tipo:** escolha o tipo de notificação: Log, Trap ou Log e Trap.
- **Dono:** digite o nome do dispositivo ou usuário que definiu a regra.

Alarmes RMON

Nesta página você pode configurar os grupos Estatísticas e Alarmes da função RMON. Escolha o menu Sistema > RMON > Alarmes para carregar a seguinte página:



- **Porta:** selecione a(s) porta(s) desejada(s).
- **Índice:** exibe o índice da entrada.
- **Intervalo:** digite o intervalo de tempo do grupo Alarme em segundos.
- **Limiar máximo:** digite o valor para o contador disparar o alarme caso este valor seja excedido.
- **Limiar mínimo:** digite o valor para o contador disparar o alarme caso esse valor seja menor que o especificado.
- **Tipo:** Falling, Rising ou Falling e Rising
  - **Falling:** o alarme será gerado caso a variável identificada esteja abaixo do limite.
  - **Rising:** o alarme será gerado caso a variável identificada esteja acima do limite.
  - **Falling e Rising:** o alarme será gerado caso a variável identificada esteja abaixo ou acima do limite.
- **Variável:** selecione as variáveis desejadas presentes na lista.
- **Amostragem:**
  - **Absoluto:** compara os valores diretamente com os limiares configurados no final do intervalo de amostragem.
  - **Delta:** subtrai o último valor amostrado a partir do valor atual. A diferença nos valores é comparada com os limiares configurados.
  - **Índice do evento para limiar máximo:** digite o maior índice que deseja aplicar o alarme.
  - **Índice do evento para limiar mínimo:** digite o menor índice que deseja aplicar o alarme.

  Obs: o alarme será aplicado aos índices que estão entre o Evento de queda e de aumento.
  - **Proprietário:** digite o nome do dispositivo ou usuário que definiu a regra.

Lista de alarme

Nesta página você pode visualizar os alarmes que estão configurados.

Lista de eventos

Nesta página você pode visualizar os eventos que estão configurados.

Lista de histórico

Nesta página você pode visualizar o histórico.

Lista de estatísticas

Nesta página você pode visualizar todas as estatísticas das portas.

Roteamento estático (IPv4)

O roteamento estático IPv4 encaminha pacotes com redes IPv4 de origem e destino através de uma rota estática. Esta função é indicada para redes com poucos elementos de conexão onde não existam caminhos redundantes. Além disso, é necessário que o administrador da rede tenha conhecimento da topologia da rede para confeccionar as tabelas de roteamento e garantir a convergência da mesma.

Neste switch é possível criar 16 interfaces e 32 rotas estáticas.

Criar/excluir interface

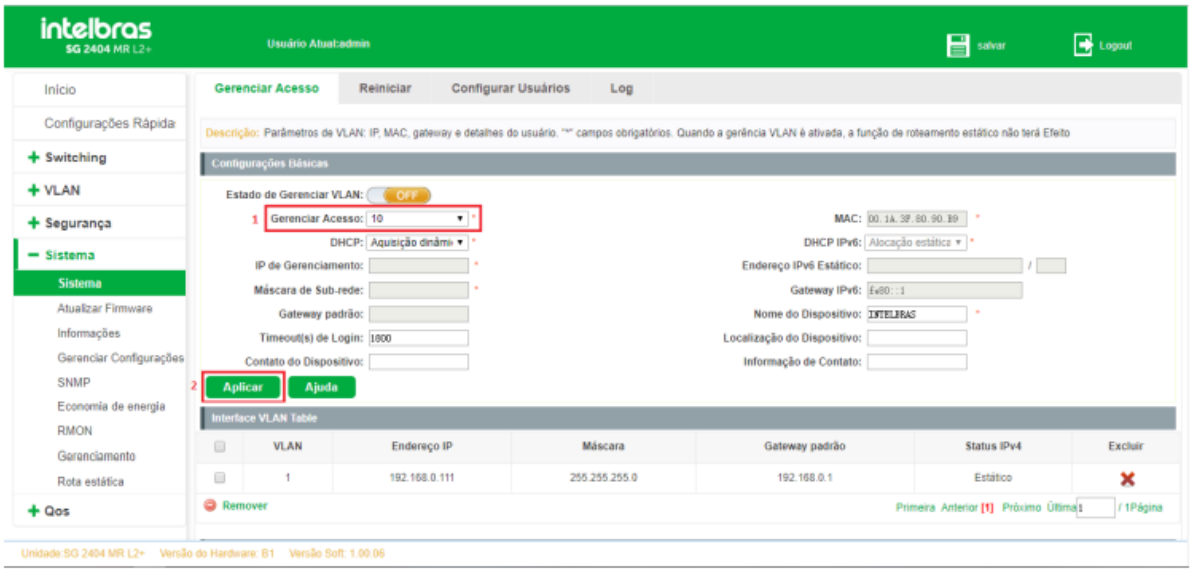
Descrição: criar uma interface.

Na página Sistema > Sistema > Gerenciar Acesso > Gerenciar Acesso

1. Selecione a VLAN desejada.
2. Clique em Aplicar.

Obs: a VLAN precisa estar criada.

Exemplo: criar interface na VLAN 10:

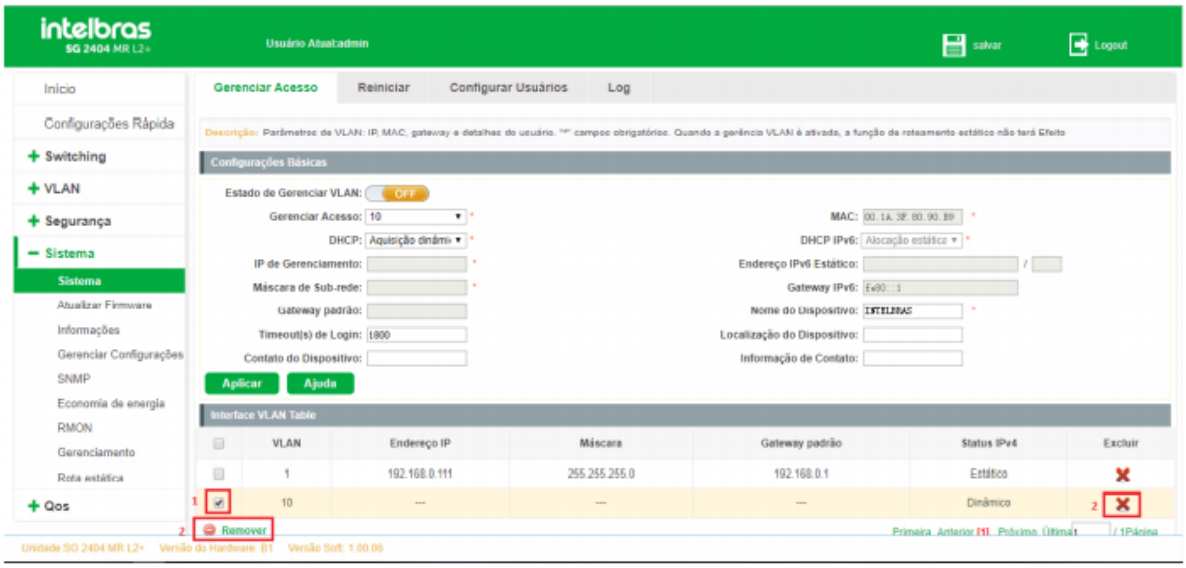


Descrição: excluir uma interface.

Na página Sistema > Sistema > Gerenciar Acesso.

1. Selecione a(s) VLAN(s) desejadas.
2. Clique em Remover ou Excluir.

Exemplo: Excluir interface na vlan 10:



Adicionar IP à interface

Descrição: adicionar um IP à interface.

Na página Sistema > Sistema > Gerenciar Acesso.

1. Selecione a VLAN desejada.
2. Selecione Alocação estática.
3. Adicione o IP desejado.
4. Adicione a máscara de sub-rede.
5. Clique em Aplicar.

Exemplo: adicionar o IP 192.168.10.100/24 na interface vlan 2:

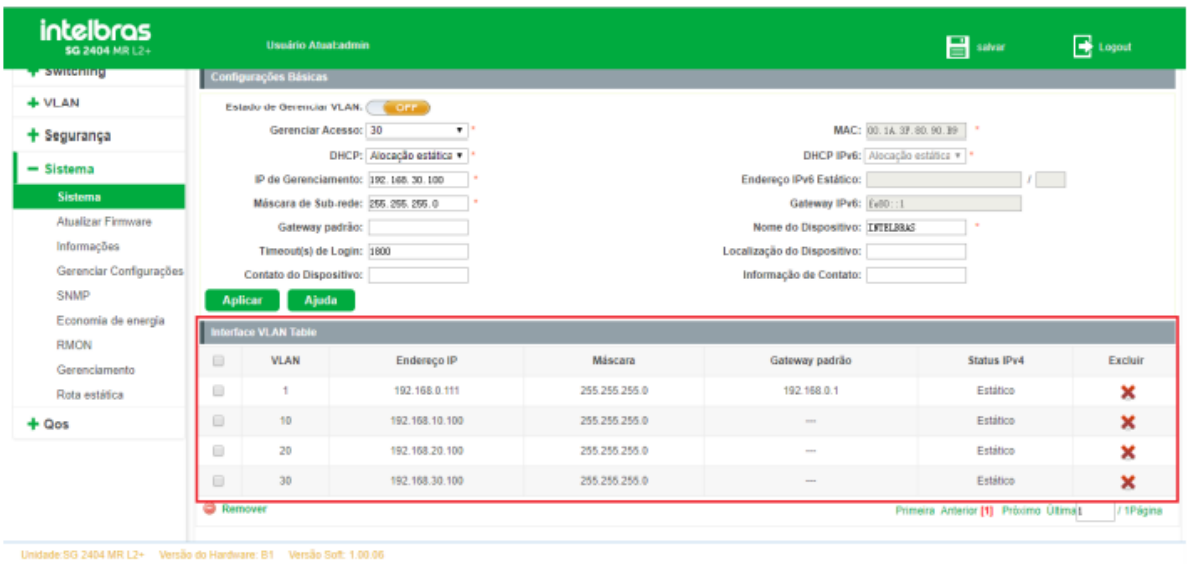
Obs: a VLAN precisa estar criada

Visualizar interfaces

Descrição: exibir os dados da interface.

Na página Sistema > Sistema > Gerenciar Acesso.

Exemplo: visualizar as interfaces criadas:



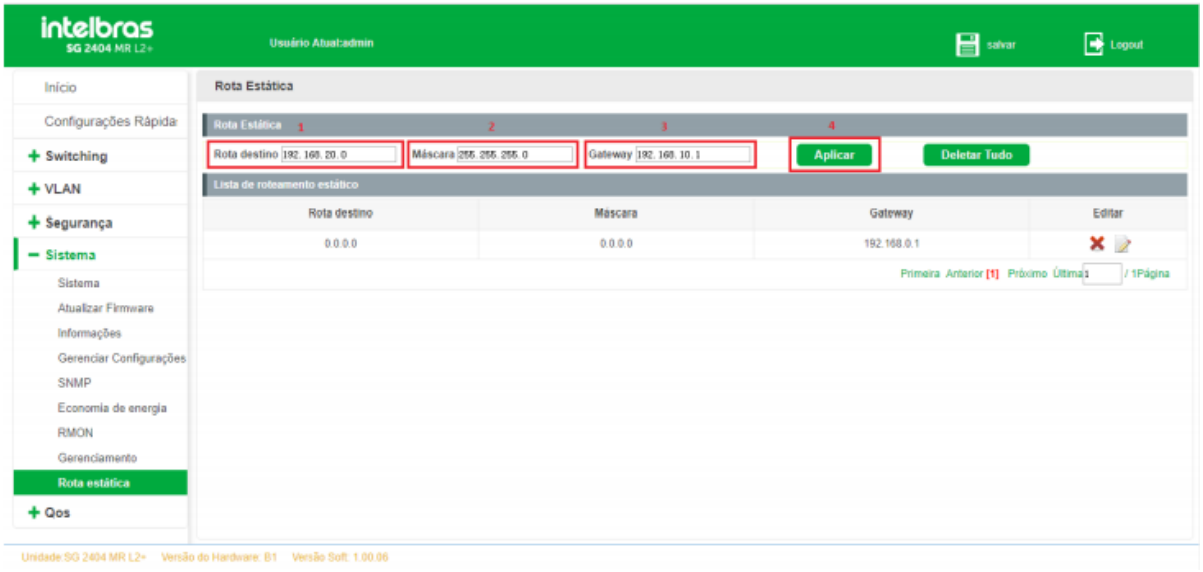
Criação de rotas estáticas

Descrição: criar rotas estáticas.

Na página Sistema > Rota estática.

1. Adicionar endereço IP da rede de destino (rede remota).
2. Adicionar a máscara de sub-rede.
3. Adicionar o endereço IP do gateway (next-hop).
4. Clique em Aplicar.

Exemplo: adicionar uma rota com destino de rede 192.168.20.0/24 e o roteador da rede sendo 192.168.10.1.

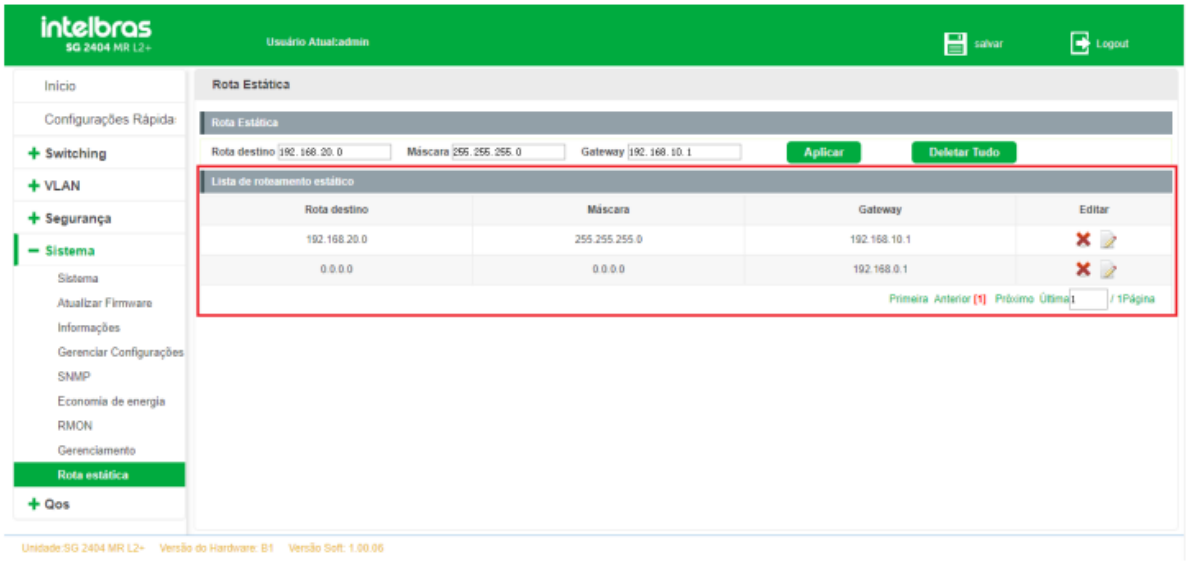


Visualizar rotas estáticas

Descrição: exibir as rotas criadas e suas configurações.

Na página Sistema > Rota estática.

Exemplo: visualizar as rotas estáticas e suas configurações:



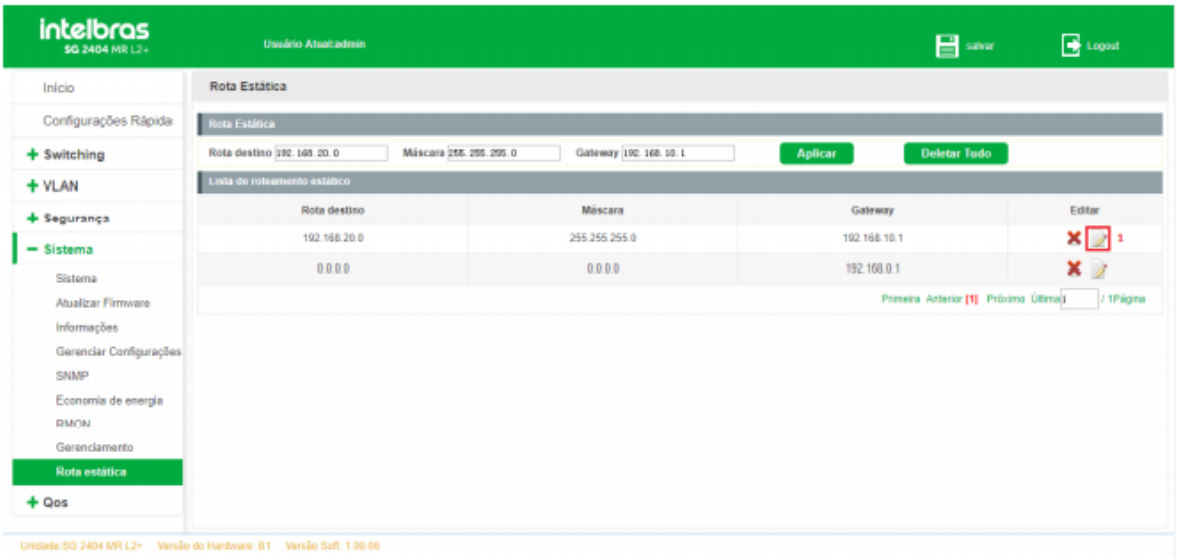
Editar rota estática

Descrição: editar rota estática.

Na página Sistema >Rota estática.

1. Clique no ícone (EDITAR) para editar a rota.
2. Seguir os passos da seção Criação de rotas estáticas.

Exemplo: editar a rota com destino de rede 192.168.20.0/24.



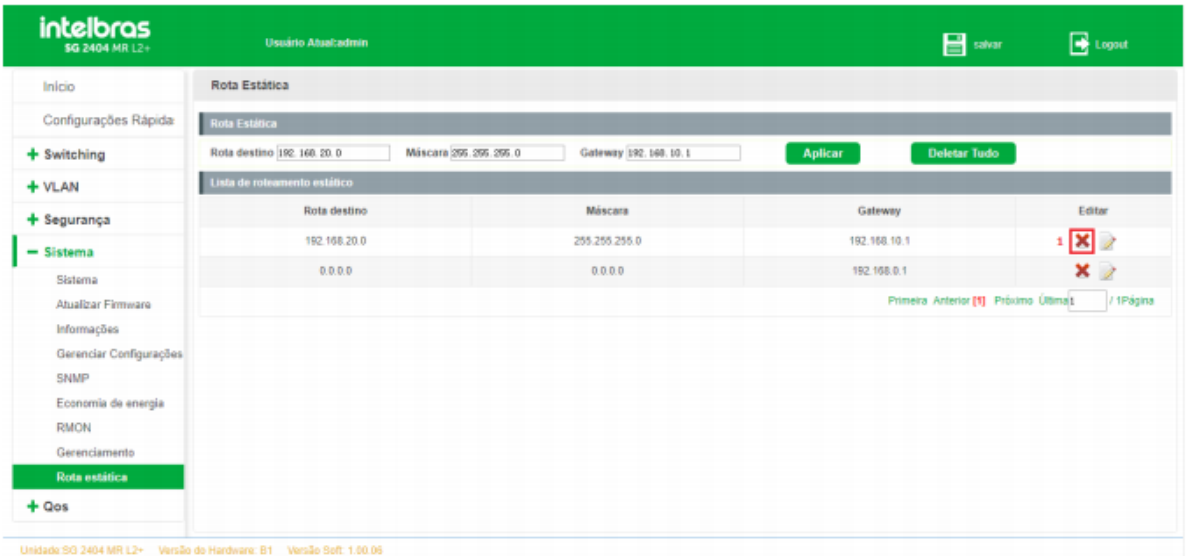
Deletar rota estática

Descrição: excluir rota estática.

Na página Sistema >Rota estática.

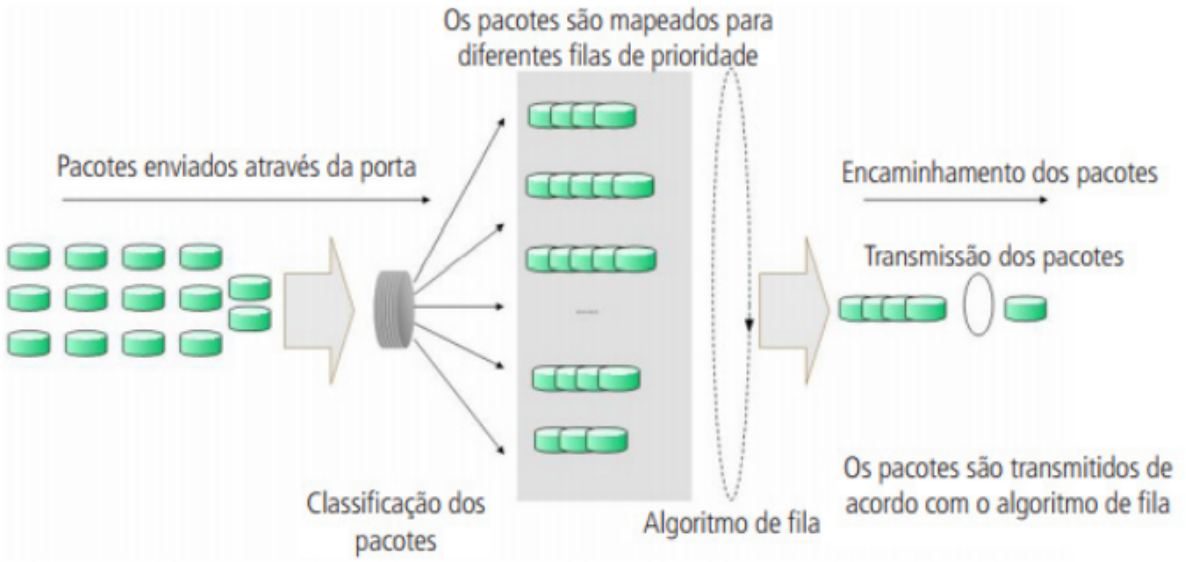
1. Clique no ícone (EXCLUIR) para remover a rota.

Exemplo: excluir a rota com destino de rede 192.168.20.0/24.



QOS

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



- **Classificação de tráfego:** identifica pacotes em conformidades com determinadas regras.
- **Mapeamento:** o usuário pode mapear os pacotes entrantes para filas de prioridades diferentes, com base nos modelos de prioridade. Este switch implementa dois modelos de prioridades: *802.1p e DSCP*.
- **Algoritmo de fila:** o switch suporta quatro modelos de algoritmos de fila: *SP, WRR, SP+WRR e Uniforme*.

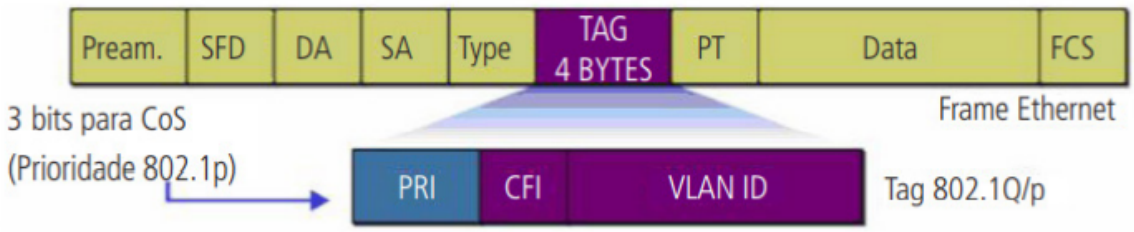
Agenda prioridade

Tipos de prioridades

O switch implementa dois modelos de prioridades, por 802.1p e DSCP.

Prioridade 802.1p

De acordo com a figura a seguir, cada TAG 802.1q inserida no quadro Ethernet possui um campo denominado PRI, este campo possui 3 bits que são utilizados para a classificação e priorização do pacote, sendo possível configurar até 8 níveis de priorização (0 a 7). Na página de gerenciamento web, é possível mapear diferentes níveis de priorização de acordo com a fila de prioridade desejada. O switch processa os pacotes não marcados (*untagged*) com base no modo de prioridade padrão.



Prioridade DSCP

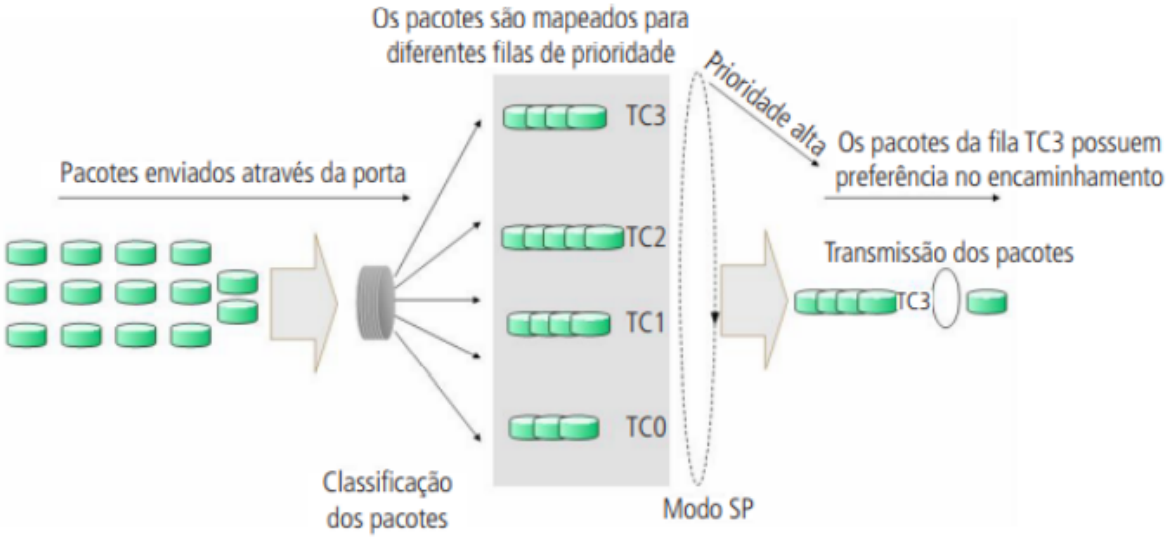
De acordo com a figura a seguir. O campo ToS (*Type Of Service*) do cabeçalho IP possui 1 byte, ou seja 8 bits. Os três primeiros bits indicam a Precedência IP e variam dentro do intervalo que vai de 0 a 7, os cinco bits restantes não são utilizados. A **RFC 2474** redefiniu o campo ToS do datagrama IP, chamando-o de campo DS (*Differentiated Service*), deste modo, os 6 primeiros bits mais significativos (bit 7 ao bit 2), diferenciam os pacotes recebidos em classes de tráfego,

conforme informações de atraso, processamento e confiabilidade, os dois últimos bits menos significativos (bit 1 e bit 0) são reservados. É possível configurar até 64 classes de tráfego DSCP, este intervalo é configurado dentro da faixa que vai de 0 a 63.

Algoritmo de fila

Quando a rede está congestionada, muitos pacotes podem ser perdidos ou chegarem com atrasos em seus destinos, ocasionando lentidão e prejudicando os serviços utilizados pela rede. Estes problemas podem ser resolvidos com a utilização de algoritmos de fila. O switch implementa 4 filas de prioridade: TC0, TC1, TC2 e TC3. TC0 tem a menor prioridade, enquanto TC3 tem a maior prioridade, que são implementados com os seguintes algoritmos de fila: SP, WRR, SP+WRR e Uniforme.

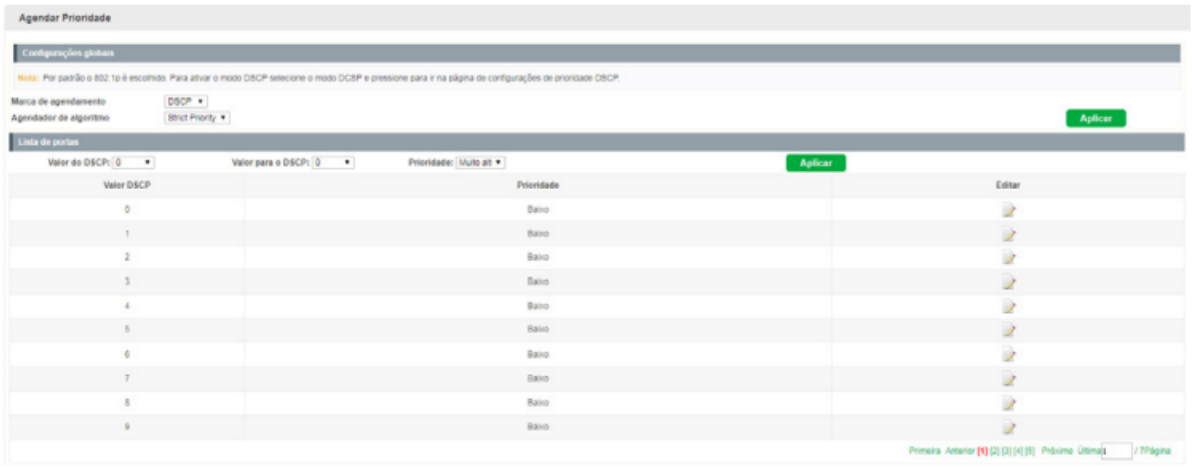
1. **SP:** algoritimo SP (*Strict Priority*). Neste modo, a fila com maior prioridade ocupará totalmente a largura de banda. Os pacotes em fila de menor prioridade somente serão enviados após todos os pacotes de filas com maior prioridade serem enviados. O switch possui 4 filas de prioridades definidos como: TC0, TC1, TC2 e TC3, quanto maior o valor da fila, maior a prioridade. A desvantagem de se utilizar o algoritmo de escalonamento de filas SP é que caso ocorra um congestionamento de pacotes em filas com maiores prioridades, os pacotes em filas de menores prioridades não serão atendidos.



2. **SP+WRR:** algoritmo SP+WRR. Neste modo, o switch faz a priorização das filas através do uso dos dois algoritmos de fila (SP e WRR). A fila TC3 pertence ao grupo SP, isto é, a fila ocupará toda a largura de banda até que não possua mais pacotes a serem enviados, enquanto os pacotes das filas TC0, TC1 e TC2 serão atendidos conforme o peso de cada fila utilizando o algoritmo WRR, a relação de prioridade das filas com o peso de cada fila, seguem a ordem: TC0, TC1 e TC2 = 1:2:4. 4.
3. **Uniforme:** neste modo, todas as filas ocupam igualmente a largura de banda. A relação de prioridade das filas com o peso de cada fila, seguem a ordem: TC0, TC1, TC2 e TC3 = 1:1:1:1.

Prioridade DSCP

Nesta página é possível configurar a Prioridade DSCP. O switch analisa o campo ToS (*Type of Service*) do cabeçalho IP. Este campo possui 1 byte (8 bits) de tamanho, os 6 primeiros bits mais significativos diferenciam os pacotes recebidos em classes de tráfego, conforme informações de atraso, processamento e confiabilidade, os dois últimos bits menos significativos são reservados. É possível configurar até 64 classes de tráfego DSCP, este intervalo é configurado dentro da faixa que vai de 0 a 63. Escolha o menu QoS > DiffeServ > Prioridade DSCP para carregar a seguinte página:



- **valor do DSCP:** informe o DSCP de início.
- **Valor para o DSCP:** informe o DSCP final.
- **Prioridade:**
  - **Baixo:** define o valor DSCP escolhido como baixo.
  - **Médio:** define o valor DSCP escolhido como médio.
  - **Alto:** define o valor DSCP escolhido como alto.
  - **Muito alto:** define o valor DSCP escolhido como muito alto.
- **Agendador de algoritmo:**
  - **SP:** algoritmo SP (*Strict Priority*). Neste modo, a fila com maior prioridade ocupará totalmente a largura de banda. Os pacotes em fila de menor prioridade somente serão enviados após todos os pacotes de filas com maior prioridade serem enviados. O switch possui 4 filas de prioridades definidos como: TC0, TC1, TC2 e TC3, quanto maior o valor da fila, maior a prioridade. A desvantagem de se utilizar o algoritmo de escalonamento de filas SP é que caso ocorra um congestionamento de pacotes em filas com maiores prioridades, os pacotes em filas de menores prioridades não serão atendidos.
  - **WRR:** algoritmo WRR (*Weight Round Robin*). Neste modo, os pacotes de todas as filas serão enviados de acordo com o peso de cada fila, este peso indica a proporção ocupada pelo recurso. As filas de prioridades são atendidas em ordem pelo algoritmo WRR, caso uma fila estiver vazia, o algoritmo passa para a próxima fila. A relação de prioridade das filas com o peso de cada fila, seguem a ordem: TC0, TC1, TC2 e TC3 = 1:2:4:8.
  - **SP+WRR:** algoritmo SP+WRR. Neste modo, o switch faz a priorização das filas através do uso dos dois algoritmos de escalonamento (SP e WRR). A fila TC3 pertence ao grupo SP, isto é, a fila ocupará toda a largura de banda até que não possua mais pacotes a serem enviados, enquanto os pacotes das filas TC0, TC1 e TC2 serão atendidos conforme o peso de cada fila utilizando o algoritmo WRR, a relação de prioridade das filas com o peso de cada fila, seguem a ordem: TC0, TC1 e TC2 = 1:2:4.
  - **Uniforme:** neste modo, todas as filas ocupam igualmente a largura de banda. A relação de prioridade das filas com o peso de cada fila, seguem a ordem: TC0, TC1, TC2 e TC3 = 1:1:1:1.

Prioridade 802.1p

Prioridade 802.1p Nesta página é possível configurar a prioridade 802.1p. O switch analisa a TAG de VLAN que foi inserido no quadro Ethernet do pacote enviado. Esta TAG possui um campo chamado PRI de 3 bits que são utilizados para a classificação e priorização do pacote, sendo possível configurar até 8 níveis de priorização (0 a 7).

- **Agendador de algoritmo:**
  - **SP:** algoritmo SP (*Strict Priority*). Neste modo, a fila com maior prioridade ocupará totalmente a largura de banda. Os pacotes em fila de menor prioridade somente serão enviados após todos os pacotes de filas com maior prioridade serem enviados. O switch possui 4 filas de prioridades definidas como: TC0, TC1, TC2 e TC3, quanto maior o valor da fila, maior a prioridade. A desvantagem de se utilizar o algoritmo de escalonamento de filas SP é que caso ocorra um congestionamento de pacotes em filas com maiores prioridades, os pacotes em filas de menores prioridades não serão atendidos.
  - **WRR:** algoritmo WRR (*Weight Round Robin*). Neste modo, os pacotes de todas as filas serão enviados de acordo com o peso de cada fila, este peso indica a proporção ocupada pelo recurso. As filas de prioridades são atendidas em ordem pelo algoritmo WRR, caso uma fila esteja vazia, o algoritmo passa para a próxima fila. A relação de prioridade das filas com o peso de cada fila, seguem a ordem: TC0, TC1, TC2 e TC3 = 1:2:4:8. Neste switch é possível também configurar o peso da fila conforme desejado.
  - **SP+WRR:** algoritmo SP+WRR. Neste modo, o switch faz a priorização das filas através do uso dos dois algoritmos de escalonamento (SP e WRR). A fila TC3 pertence ao grupo SP, isto é, a fila ocupará toda a largura de banda até que não possua mais pacotes a serem enviados, enquanto os pacotes das filas TC0, TC1 e TC2 serão atendidos conforme o peso de cada fila utilizando o algoritmo WRR, a relação de prioridade das filas com o peso de cada fila, segue a ordem: TC0, TC1 e TC2 = 1:2:4.
  - **Uniforme:** neste modo, todas as filas ocupam igualmente a largura de banda. A relação de prioridade das filas com o peso de cada fila, segue a ordem: TC0, TC1, TC2 e TC3 = 1:1:1:1.

UTILIZANDO O CLI

Acessando a interface de Linha de Comando CLI

É possível realizar o login no switch de duas formas, para acessar a Interface de Linha de Comando (CLI):

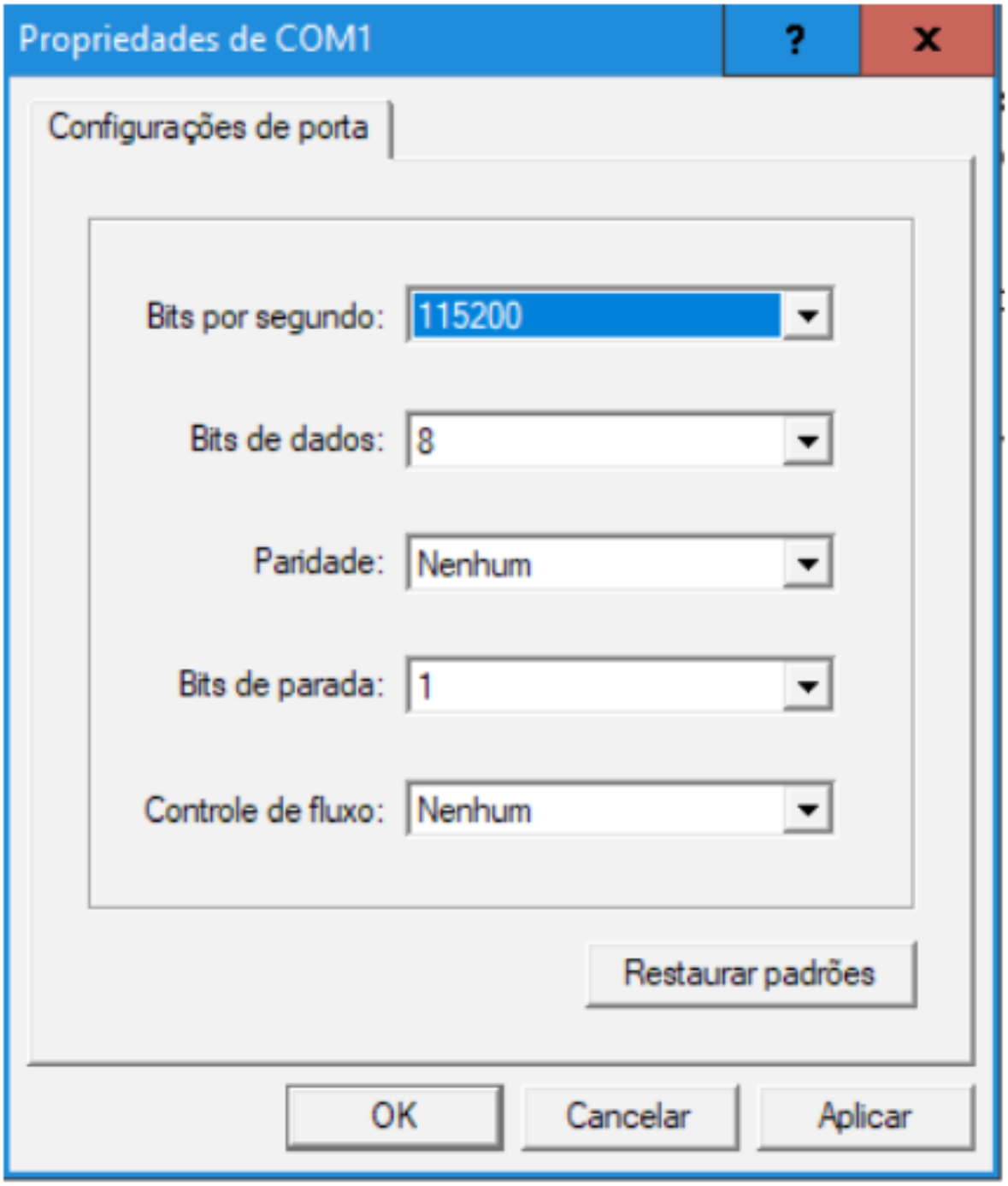
1. Realizar o Login utilizando a porta console do switch;
2. Realizar o Login remotamente utilizando uma conexão SSH ou Telnet.

Login pela porta console

Para exibir a interface de linha de comandos, conecte a extremidade (DB-9 fêmea) do cabo console na respectiva porta serial (COM) do computador e a outra extremidade (RJ45) na porta console (RJ45), localizada no painel frontal do switch.

Ative um software de emulação de terminal (por exemplo, *Hyper Terminal® no Windows® ou GtkTerm e Minicom em distribuições Linux® ou Unix®*).

O software de emulação de terminal deve ser iniciado com a seguinte configuração (veja exemplo para o *Hyper Terminal®* na figura a seguir).

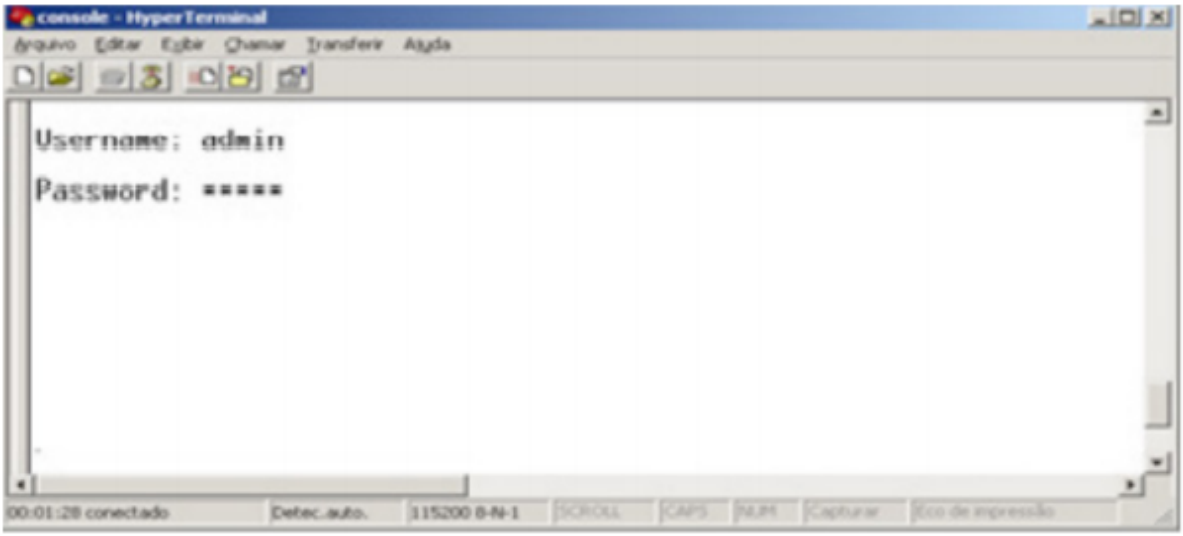


Taxa de dados: 115.200 bits por segundo.

Formato dos dados: 8 bits de dados, sem paridade e 1 bit de parada.

Controle de fluxo: nenhum.

Após pressionar o botão OK, será solicitado o nome de usuário e senha na tela do *Hyper Terminal*®. O usuário e senha padrão de fábrica é admin.



Username: admin

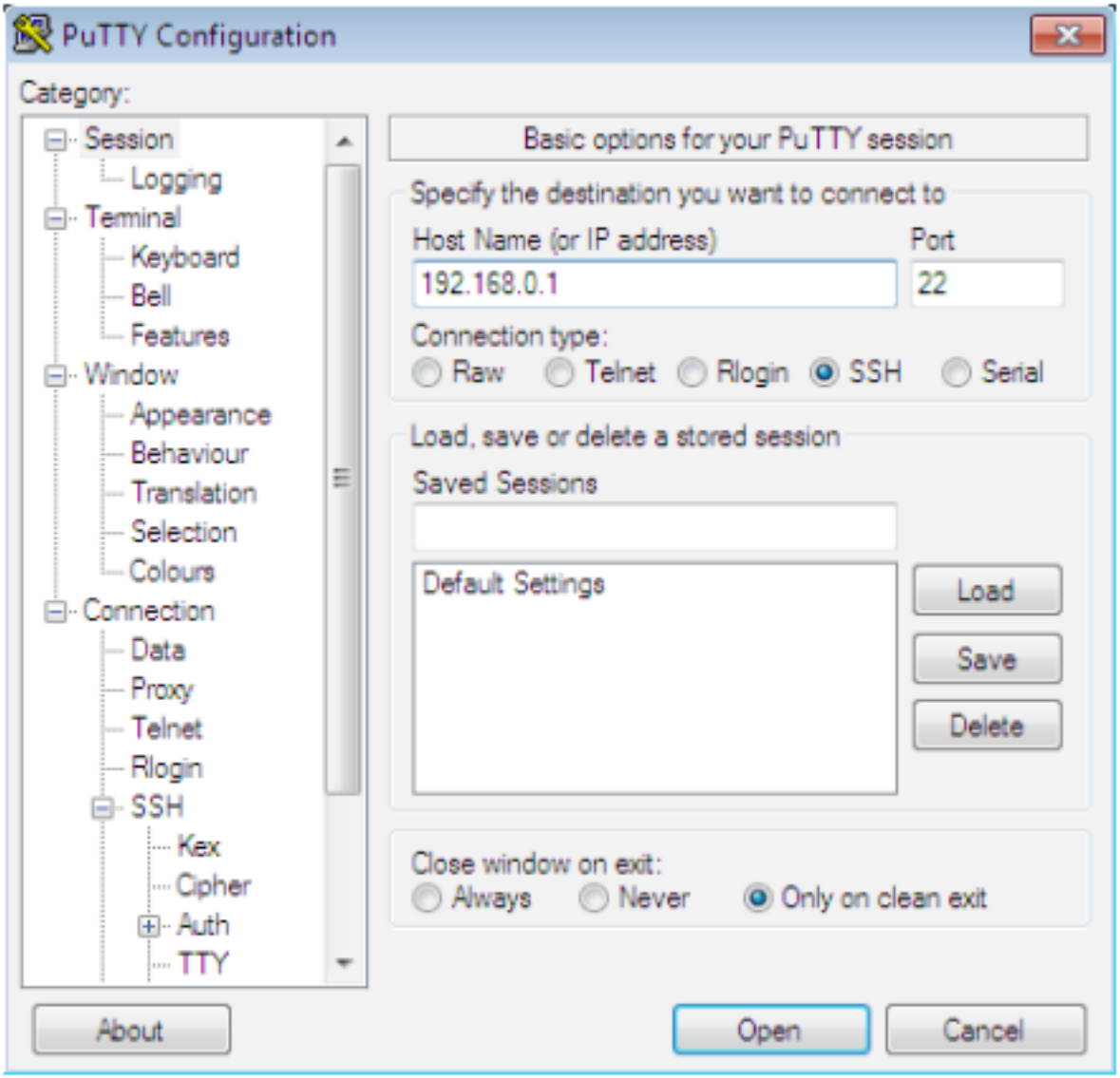
Password: admin

Logon via SSH

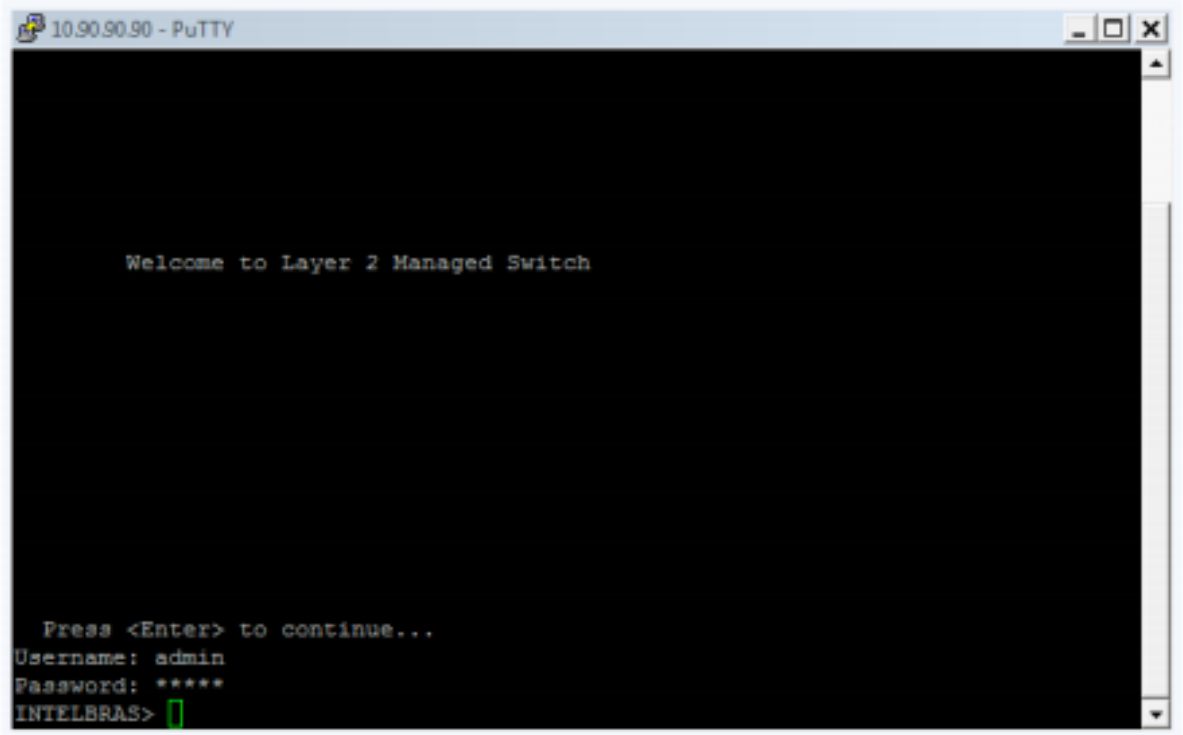
Para fazer logon via SSH, é recomendado usar o software *PuTTY*.

- **Modo de autenticação de senha**: exige nome de usuário e senha, que por padrão são *admin*.

1. Abra o software PuTTY para efetuar o login. Digite o endereço IP do switch no campo Host name; mantenha o valor padrão de 22 no campo Port; selecione SSH como o tipo de conexão;



2. Clique no botão Open para fazer logon no switch. Digite o nome de usuário e a senha para efetuar login no switch, em seguida, digite enable para entrar no modo Privileged EXEC, para que possa continuar a configurar o switch.



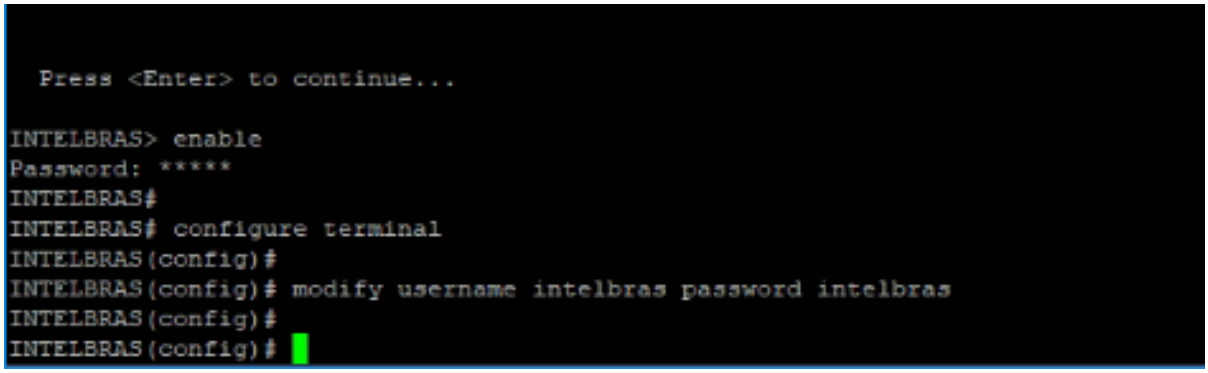
Alteração de login e/ou senha SSH

Para alteração do login e/ou senha SSH siga os procedimentos abaixo:

1. Acesse o equipamento via SSH, conforme procedimentos anteriores;
2. Utilize o comando **enable** para acessar o modo *Privileged EXEC*;
3. Informe a senha de acesso ao modo *Privileged EXEC* que por padrão é *admin*;
4. Utilize o comando ***configure terminal*** para acessar as configurações do sistema do switch;
5. Utilize o comando ***modify username USUÁRIO password SENHA*** e altere os campos "USUÁRIO" e "SENHA" para os valores de acesso desejados que por padrão é *admin*;

   Observações:

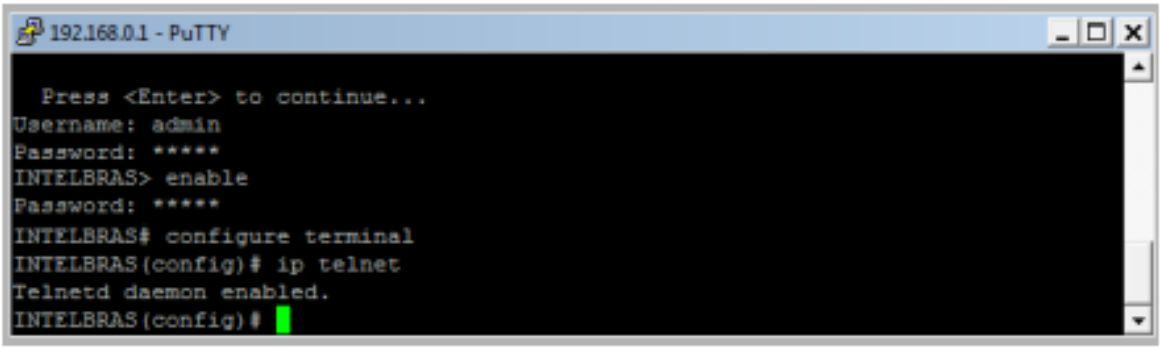
   - Para alteração apenas da senha de acesso SSH, basta informar no campo "USUÁRIO" o usuário utilizado atualmente para acesso, por padrão o valor é *admin*.
   - Para alteração apenas do usuário de acesso SSH, basta informar no campo "SENHA" a senha utilizada atualmente para acesso, por padrão o valor é *admin*.



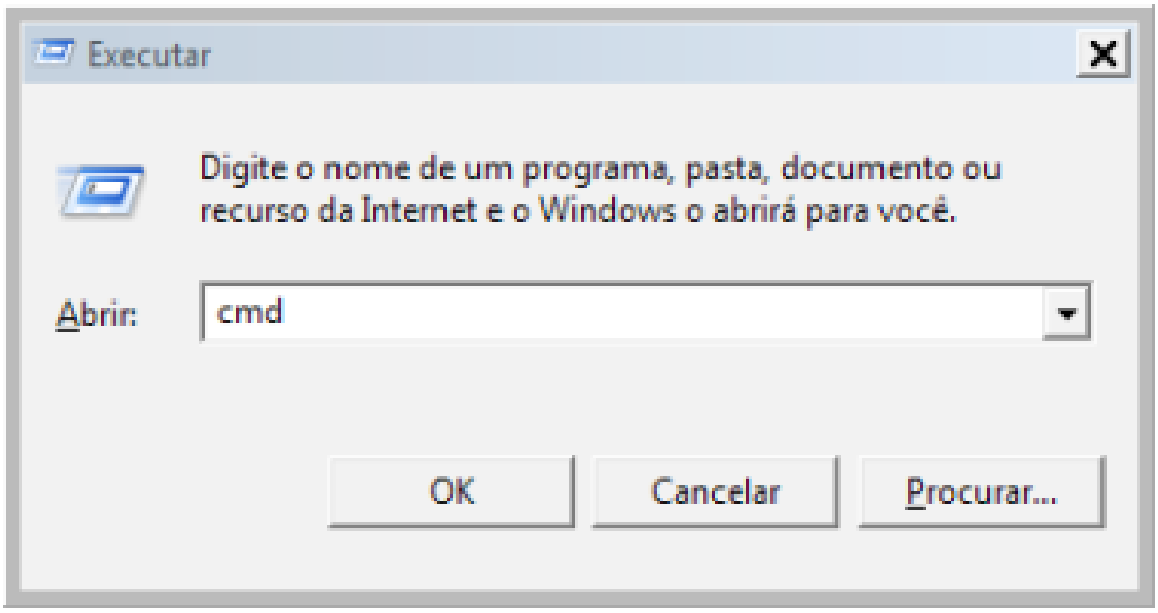
Logon via Telnet

Para fazer logon no switch por uma conexão Telnet, siga o procedimento:

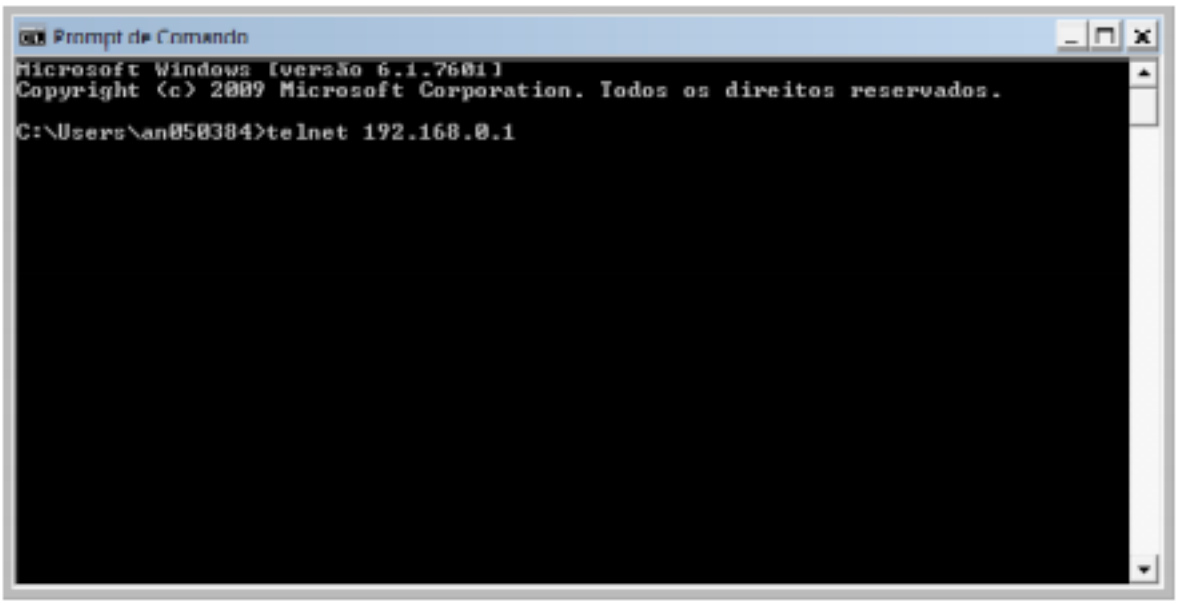
1. Verifique se o switch e o computador estão na mesma LAN;
2. Acesse o switch através do PUTTY e ative o modo de acesso via Telnet com os seguintes comandos:



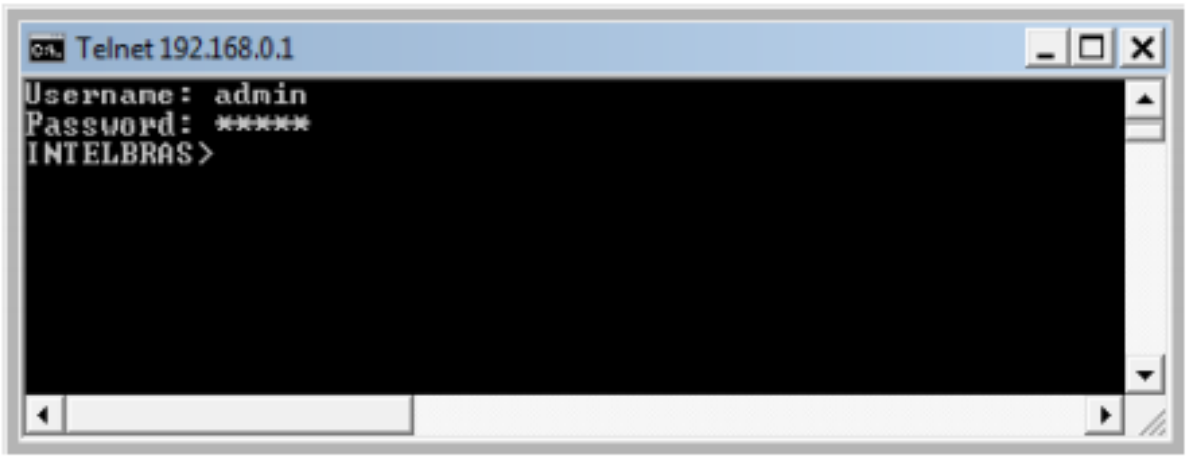
3. Aperte Windows + R para abrir a tela Executar.
4. Digite cmd na tela Executar, conforme a figura a seguir, e pressione o botão OK;



5. Digite telnet 192.168.0.1 no prompt de comando, conforme a figura a seguir, e pressione a tecla Enter;



6. Se a conexão for bem-sucedida, uma tela solicitando o nome de usuário e senha (*User e Password*) será apresentada;
7. Preencha ambos os campos com a palavra admin.



Alteração de login e/ou senha TELNET

Para alteração do login e/ou senha Telnet siga os procedimentos abaixo:

1. Acesse o equipamento via Telnet, conforme procedimentos anteriores;
2. Utilize o comando **enable** para acessar o modo *Privileged EXEC*;
3. Informe a senha de acesso ao modo *Privileged EXEC* que por padrão é *admin*;
4. Utilize o comando ***configure terminal*** para acessar as configurações do sistema do switch;
5. Utilize o comando ***modify username USUÁRIO password SENHA*** e altere os campos "USUÁRIO" e "SENHA" para os valores de acesso desejados que por padrão é *admin*;

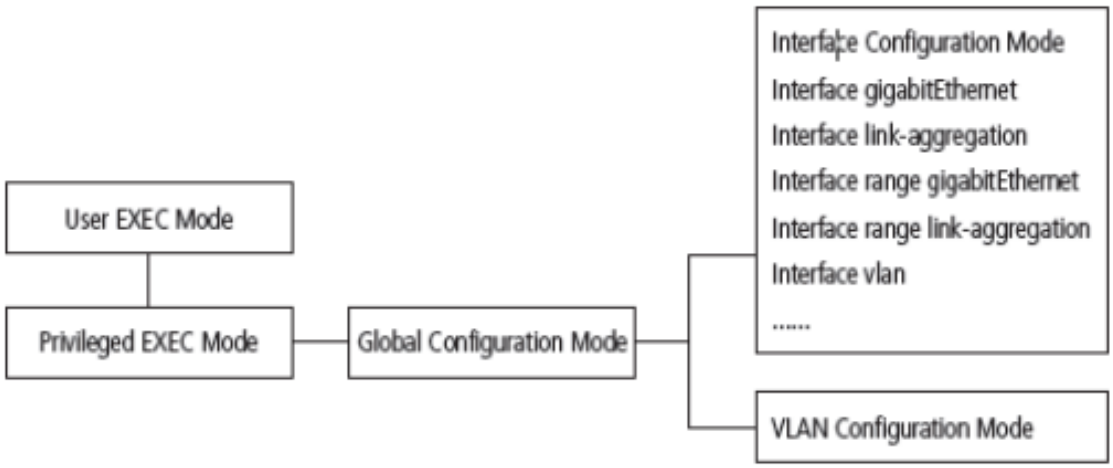
   Observações:

   - Para alteração apenas da senha de acesso telnet, basta informar no campo "USUÁRIO" o usuário utilizado atualmente para acesso, por padrão o valor é *admin*.
   - Para alteração apenas do usuário de acesso telnet, basta informar no campo "SENHA" a senha utilizada atualmente para acesso, por padrão o valor é *admin*.

```
Username: admin
Password: *****
INTELBRAS> enable
Password: *****
INTELBRAS# configure terminal
INTELBRAS(config)# modify username intelbras password intelbras
INTELBRAS(config)#
```

Modos de comandos CLI

O comando CLI é dividido em diferentes modos: *modo User EXEC, Privileged EXEC, Global Configuration, Interface Configuration e VLAN Configuration*. O modo de Interface Configuration também pode ser dividido em Interface Ethernet, Interface link-aggregation e alguns outros modos, o que é exibido no seguinte diagrama.



A tabela a seguir fornece informações detalhadas sobre o caminho acessado, o prompt de cada modo e como sair do modo atual e acessar o modo seguinte:

Modo	Método de acesso	Prompt
User EXEC	Modo Primário, uma vez que está conectado no switch	*INTELBRAS>*
Privileged EXEC	Use o comando **enable** para acessar este modo de configuração, a partir do modo UserExec	*INTELBRAS#*
Global Configuration	Use o comando configure para acessar este modo de configuração, a partir do modo Privileged Exec	*INTELBRAS(config)#*
Interface Configuration	Use o comando Interface gigabitEthernet port ou Interface range gigabitEthernet port-list para acessar este modo, a partir do modo Global configuration	*INTELBRAS(config-if)# or INTELBRAS(config-if-range)#*
VLAN Configuration	Use o comando vlan vlan-list para entrar neste modo, a partir do modo Global configuration	*INTELBRAS(config-vlan)#*

Obs: ao estabelecer uma conexão no switch via Telnet/SSH o modo padrão é o User EXEC.

Cada modo de comando tem seu próprio conjunto de comandos específicos. Para configurar alguns comandos, você deve acessar o modo de comando correspondente em primeiro lugar.

- **Modo de configuração global:** neste modo os comandos globais são fornecidos, tais deles como, Spanning Tree, Modo de programação e assim por diante.
- **Modo de configuração de interface:** neste modo os usuários podem configurar uma interface (porta) em particular. Os comandos de interface ativam ou modificam o modo de operação de uma ou mais portas.
  - **Interface gigabitEthernet:** configura parâmetros para uma porta Ethernet, como Duplex-mode, status de controle de fluxo.
  - **Interface range gigabitEthernet:** os comandos contidos são os mesmos que o da interface Ethernet. Configura parâmetros para várias portas Ethernet.
  - **Interface link-aggregation:** configura parâmetros para um link de agregação, congestionamento de transmissões.
  - **Interface range link-aggregation:** configura parâmetros para multi-trunks.
  - **Interface VLAN:** permite configurar os parâmetros de VLAN para uma porta.
- **Modo de configuração VLAN:** neste modo, os usuários podem criar uma VLAN e adicionar a mesma à uma porta específica.

Alguns comandos são globais, significa que eles podem ser realizados em todos os modos:

- **show:** exibe todas as informações da chave, por exemplo: informação estatística, as informações da porta, as informações da VLAN.
- **History:** mostra o histórico de comandos.

Mostrar usuários conectados

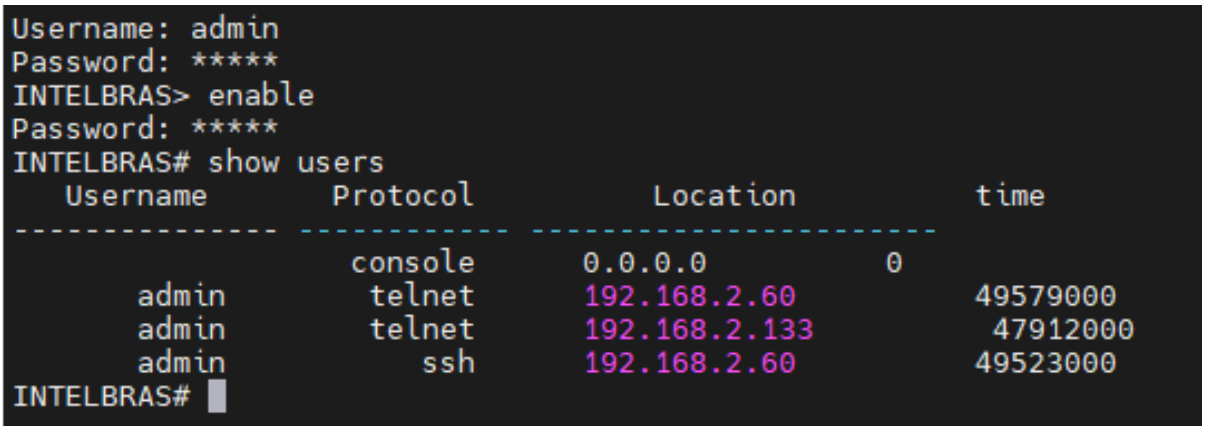
É possível visualizar em forma de tabela os usuários conectados atualmente ao switch utilizando o seguinte comando via terminal CLI:

INTELBRAS> enable

*Enter password: ******

INTELBRAS# show users

Abaixo é apresentada uma imagem que demonstra a aplicação dos comandos citados acima:



OBS: O modo Privileged EXEC é necessário para a entrada do comando *show users*.

Níveis de segurança

Existem dois níveis de segurança para o acesso ao CLI: *Nível de usuário* e *Nível de administrador*.

- **Nível de usuário:** ao acessar a Interface de Linha de Comando, o usuário entra automaticamente no nível de segurança de usuário (*User EXEC*). No entanto, usuários convidados são restritos para acessar o CLI.
- **Nível de administrador:** este nível (*Privileged EXEC*) é acessado após utilizar o comando enable dentro do modo User EXEC, permitindo o usuário monitorar, configurar e gerenciar o switch.

Convenções

Formato de convenções

As seguintes convenções são utilizadas neste manual:

- **Itens alternativos:** são agrupados em chaves e separados por uma barra vertical, por exemplo: speed {10 | 100 | 1000}.

Caracteres especiais

Você deve prestar atenção para a descrição a seguir, se a variável é uma cadeia de caracteres:

Estes seis caracteres “<>, \& não podem ser introduzidos.

Se um espaço em branco está contido dentro de uma cadeia de caracteres, aspas simples ou duplas devem ser usadas, por exemplo, *‘Olá mundo’*, *“Olá mundo”*, as palavras dentro das aspas serão identificadas como uma string. Caso contrário, as palavras serão identificadas como várias strings.

INTERFACE DO USUÁRIO

Enable

Descrição: o comando enable é utilizado para acessar o modo Privileged EXEC a partir do modo User EXEC.

Sintaxe: enable

Modo de comando: User EXEC.

Exemplo: se você definir a senha para acessar o modo Privileged EXEC a partir do modo User EXEC.

INTELBRAS > enable

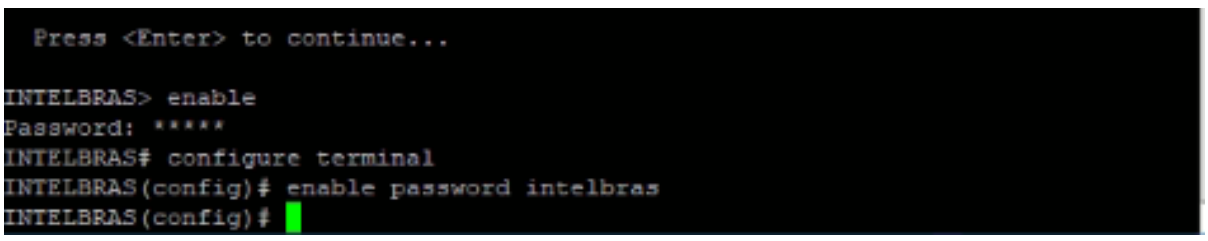
Enter password: *****

INTELBRAS#

Alterando senha de acesso ao modo Privileged EXEC (Enable)

Para alterar a senha de acesso ao modo *Privileged EXEC* siga os procedimentos a seguir:

1. Acesse o equipamento via SSH ou Telnet, conforme procedimentos anteriores;
2. Utilize o comando **enable** para acessar o modo *Privileged EXEC*;
3. Informe a senha de acesso ao modo *Privileged EXEC* que por padrão é *admin*;
4. Utilize o comando ***configure terminal*** para acessar as configurações do sistema do switch;
5. Utilize o comando ***enable password SENHA*** e altere o campo"SENHA" para o valor de acesso desejado que por padrão é *admin*;



Disable

Descrição: o comando disable é utilizado para retornar ao modo User EXEC a partir do modo Privileged EXEC.

Sintaxe: disable

Modo de comando: Privileged EXEC.

Exemplo: retornar ao modo User EXEC a partir do modo Privileged EXEC.

INTELBRAS# disable

INTELBRAS>

Configure terminal

Descrição: o comando Configure terminal é utilizado para acessar o modo Global Configuration a partir do modo Privileged EXEC.

Sintaxe: Configure terminal

Modo de comando: Privileged EXEC.

Exemplo: acessar o modo Global Configuration a partir do modo Privileged EXEC.

INTELBRAS# configure terminal

INTELBRAS(config)#

Exit

Descrição: o comando exit é utilizado para voltar ao modo de comando anterior a partir do modo de comando corrente.

Sintaxe: exit

Modo de comando: qualquer modo de comando.

Exemplo: retornar ao modo Global Configuration a partir do modo Interface Configuration, e depois voltar ao modo Privileged EXEC.

INTELBRAS(config)#

INTELBRAS(config)# exit

INTELBRAS# exit

End

Descrição: o comando end é utilizado para retornar ao modo Privileged EXEC.

Sintaxe: end

Modo de comando: qualquer modo de comando.

Exemplo: retornar ao modo Privileged EXEC a partir do modo Interface Configuration.

INTELBRAS(config-if)# end

INTELBRAS#

History

Descrição: o comando show history é utilizado para exibir os 20 últimos comandos digitados no modo atual, desde quando o switch estava ligado.

Sintaxe: show history

Modo de comando: qualquer modo de comando.

Exemplo: exibir os comandos que você digitou no modo atual.

INTELBRAS(config)# show history

COMANDOS STORM CONTROL

A função Storm control permite que o switch filtre por porta pacotes do tipo broadcast, multicast e unicast. Se a taxa de transmissão de algum dos três tipos de pacotes excederem a largura de banda configurada, os pacotes serão rejeitados automaticamente, evitando assim tempestade de broadcast na rede.

Storm control

O comando storm-control é utilizado para configurar a função Storm control. O valor deve ser múltiplo de 16. Caso o valor configurado não for múltiplo de 16, o switch irá configurar o valor mais próximo.

Sintaxe: storm-control broadcast/unknown-multicast/unknown-unicast kbps value

Parâmetros:

- **broadcast:** pacotes broadcast.
- **unknown-multicast:** pacotes multicast desconhecidos.
- **unknown-unicast:** pacotes unicast desconhecidos.
- **value:** configure o valor para o filtro.

Modo de comando: modo de configuração de interface.

Exemplo: habilite a função Storm control para a porta 5 e limite os tráfegos para 128 kbps.

INTELBRAS(config)# interface GigabitEthernet 0/5

INTELBRAS(config-if-GigabitEthernet0/5)# storm-control broadcast kbps 128

INTELBRAS(config-if-GigabitEthernet0/5)# storm-control unknown-multicast kbps 128

INTELBRAS(config-if-GigabitEthernet0/5)# storm-control unknown-unicast kbps 128

No storm-control

Para desabilitar a função, use o comando no storm-control.

Sintaxe: no storm-control broadcast/unknown-multicast/unknown-unicast > no storm-control

Parâmetros:

- **broadcast:** pacotes broadcast.
- **unknown-multicast:** pacotes multicast desconhecidos.
- **unknown-unicast:** pacotes unicast desconhecidos.

Modo de comando: modo de configuração de interface.

Exemplo 1: desabilite a função Storm control broadcast na porta 5.

INTELBRAS(config)# interface GigabitEthernet 0/5

INTELBRAS(config-if-GigabitEthernet0/5)# no storm-control broadcast

Exemplo 2: desabilite a função Storm control na porta 5.

INTELBRAS(config)# interface GigabitEthernet 0/5

INTELBRAS(config-if-GigabitEthernet0/5)# no storm-control

Show storm control

O comando show storm-control mostra as configurações de Storm control globalmente ou para a porta selecionada.

Sintaxe: show storm-control > show storm-control interfaces GigabitEthernet port_id

Parâmetros:

- **port_id:** informe a porta para visualizar as configurações.

Modo de comando: Privileged EXEC.

Exemplo 1: mostre as informações da configuração de Storm control para o switch.

INTELBRAS# show storm-control

Exemplo 2: mostre as informações da configuração de Storm control para a porta 5.

INTELBRAS# show storm-control interfaces GigabitEthernet 0/5

CONTROLE DE FLUXO (FLOW CONTROL)

Ativando controle

Descrição: comando flowcontrol on é utilizado para habilitar o controle de fluxo na porta desejada. Para desabilitar a função, utilize o comando flowcontrol off. Com esta função habilitada, a taxa de entrada e saída de pacotes pode ser sincronizada, evitando assim perdas na transmissão dos pacotes

Sintaxe: flowcontrol

Parâmetro:

- **on**
- **off**

Modo de comando: Interface configuration mode.

Exemplo: habilite a função de Controle de fluxo para a porta 1 do switch.

INTELBRAS(config-if-GigabitEthernet0/1)# flowcontrol on

COMANDOS DE AGREGAÇÃO DE LINK (LINK AGGREGATION)

LAG (*Link Aggregation Group*) é a função de agregação de links, permite a utilização de múltiplas portas para permitir o aumento da velocidade do link além dos limites nominais de uma única porta e introduz controle de falhas e redundância para a conexão a outro dispositivo que disponha do mesmo recurso.

link-aggregation

O comando link-aggregation cria um grupo de portas para a função de agregação de link.

O comando no link-aggregation executado no modo Global Configuration exclui o grupo de link-aggregation selecionado.

Sintaxe: link-aggregation group_number mode manual/lacp

link-aggregation load-balance hash-algorithm

no link-aggregation group_number

Parâmetros:

- **group_number:** o número do grupo para a configuração de link aggregation, variando de 1 a 8.
- **manual:** configure a agregação de link entre as portas de modo Estático.

- **lacp:** realiza a configuração com o protocolo LACP para agregação de link.
- **hash-algorithm:** configure o algoritmo de distribuição de carga.
  - **MAC:** o tráfego é alocado de acordo com o endereço MAC de origem e destino dos pacotes recebidos.
  - **IP+MAC:** o tráfego é alocado com base no MAC e IP de origem e destino.

Modo de comando: modo Global Configuration.

Exemplo: crie o grupo 1 de agregação de link manual com algoritmo IP+MAC.

INTELBRAS(config)# link-aggregation 1 mode manual

INTELBRAS(config)# link-aggregation load-balance mac-ip

Interface link-aggregation

A execução do comando link-aggregation na interface GigabitEthernet configura a porta como link-aggregation no grupo correspondente.

O comando no link-aggregation executado na interface exclui a porta do grupo de link-aggregation.

Sintaxe: interface GigabitEthernet port_id

interface range GigabitEthernet port_id_inicio-port_id_fim

link-aggregation group_number mode manual/lacp

no link-aggregation group_number

Parâmetros:

- **port_id:** configure a porta para configuração.
- **port_id_inicio-port_id_fim:** informe o range de portas para configurar.
- **active/passive/manual:**
  - **active:** habilita lacp na porta.
  - **passive:** ativa lacp somente se um dispositivo lacp for detectado.
  - **manual:** força a porta manualmente a ser uma porta agregada sem lacp.
- **group_number:** o número do grupo para a configuração de link aggregation, variando de 1 a 8.

Modo de comando: modo de configuração de interface.

Exemplo 1: crie o grupo 1 de agregação de link manual nas portas 1 a 4 com algoritmo MAC.

INTELBRAS(config)# link-aggregation 1 mode manual

INTELBRAS(config)# link-aggregation load-balance mac

INTELBRAS(config)# interface range GigabitEthernet 0/1-0/4

INTELBRAS(config-if-range)# link-aggregation 1 manual

Exemplo 2: exclua a porta 4 do link-aggregation grupo 1.

INTELBRAS(config)# interface GigabitEthernet 0/4

INTELBRAS(config-if-GigabitEthernet0/4)# no link-aggregation 1

Exemplo 3: exclua o grupo 1 de agregação de link das portas 1 a 3.

INTELBRAS(config)# interface range GigabitEthernet 0/1-0/3

INTELBRAS(config-if-range)# no link-aggregation 1

INTELBRAS(config-if-range)# exit

INTELBRAS(config)# no link-aggregation 1

Show link-aggregation

Descrição: o comando show link-aggregation group é utilizado para exibir as configurações dos grupos de agregação de link das portas.

Sintaxe: show link-aggregation group

show link-aggregation group group_number

Parâmetros:

- **group_number:** o número do grupo para a configuração de link aggregation, variando de 1 a 8.

Se não for especificado o número do grupo, por padrão serão mostradas as informações de todos os grupos.

Modo de comando: Privileged EXEC.

Exemplo 1: exibir as configurações de link-aggregation para todos os grupos criados.

INTELBRAS# show link-aggregation group.

Exemplo 2: exibir as configurações de link-aggregation para o grupo 1.

INTELBRAS# show link-aggregation group 1.

COMANDOS DE ESPELHAMENTO DE PORTAS (PORT MIRROR)

Espelhamento de portas é o processo de encaminhamento de cópias de pacotes de uma ou mais portas para uma porta definida como porta espelho. Geralmente o espelhamento de portas é utilizado para realizar diagnósticos e análise de pacotes, a fim de monitorar e solucionar problemas na rede.

Monitor session

Descrição: o comando monitor session source interface é utilizado para configurar a porta que será monitorada. O comando monitor session destination interface é utilizado para configurar a porta de monitoramento.

Cada sessão de monitoramento pode ter apenas uma porta.

O comando no monitor session é utilizado para excluir a sessão de monitoramento correspondente.

Sintaxe: monitor session session_number source interfaces GigabitEthernet

port-id port-list mode

monitor session session_number destination interface GigabitEthernet

port-id allow-ingress

no monitor session session_number

Parâmetros:

- **session_number:** o número da sessão de monitoramento, variando de 1 a 4.
- **port-id:** o número da porta Ethernet
- **port-list mode:** o modo de monitoramento possuiu três opções: rx, tx e both.
  - **rx (modo de monitoramento de entrada):** significa que os pacotes de entrada recebidos pela porta monitorada serão copiados para a porta de monitoramento.
  - **tx (modo de monitoramento de saída):** indica que os pacotes de saída enviados pela porta monitorada serão copiados para a porta de monitoramento
  - **both (entrada e saída):** apresenta os pacotes de entrada recebidos e os pacotes de saída enviados pela porta monitorada, ambos serão copiados para a porta de monitoramento.

Modo de comando: modo Global Configuration.

Exemplo 1: criar a sessão 1 e monitorar a entrada e saída de pacotes na porta 2, enviando para a porta 1.

INTELBRAS(config)# monitor session 1 source interfaces GigabitEthernet 0/2 both

INTELBRAS(config)# monitor session 1 destination interface GigabitEthernet 0/1

Exemplo 2: criar uma sessão 1, em seguida, configurar as portas 15, 16 e 17 como portas a serem monitoradas e permitir o monitoramento de entrada dos dados. Configurar a porta 20 como porta de monitoramento da sessão 1.

INTELBRAS(config)# monitor session 1 source interfaces GigabitEthernet 0/15-0/17

INTELBRAS(config)# monitor session 1 destination interface GigabitEthernet 0/20

Exemplo 3: excluir a sessão de monitoramento 1.

INTELBRAS(config)# no monitor session 1

Show monitor

Descrição: o comando show monitor session é utilizado para exibir a configuração de monitoramento das portas.

Sintaxe: show monitor session session_number

Parâmetros:

- session_number: o número da sessão de monitoramento. Por padrão a configuração de monitoramento de todas as sessões é exibida

Modo de comando: Privileged EXEC.

Exemplo 1: exibir a configuração de monitoramento de todas as sessões.

INTELBRAS# show monitor

Exemplo 2: exibir as configurações de monitoramento da sessão 1.

INTELBRAS# show monitor 1

COMANDO DE ISOLAMENTO DE PORTAS (PORT ISOLATION)

O isolamento de portas fornece um método para restringir o fluxo do tráfego para melhorar a segurança da rede. Esta função basicamente faz com que uma porta configurada com isolamento de portas não possa encaminhar pacotes para outras portas que estejam com essa função habilitada.

Switchport protected

O comando switchport protected deve ser executado no modo de configuração da interface, e realiza o isolamento do tráfego entre as portas com essa função habilitada.

O comando no switchport protected retira a porta do conjunto de portas isoladas.

Sintaxe: switchport protect

Modo de comando: modo de configuração de interface.

Exemplo: configure as portas 10 e 20 para não se comunicar entre si.

INTELBRAS(config)# interface GigabitEthernet 0/10

INTELBRAS(config-if-GigabitEthernet0/10)# switchport protected

INTELBRAS(config-if-GigabitEthernet0/10)# exit

INTELBRAS(config)# interface GigabitEthernet 0/20

INTELBRAS(config-if-GigabitEthernet0/20)# switchport protected

Show protected

O comando show interface port_id protected mostra as configurações de isolamento da porta selecionada.

Sintaxe: show interfaces port-id protected

Parâmetros:

port_id: configure a porta para configuração.

Modo de comando: Privileged EXEC.

Exemplo: mostre as configurações de isolamento da porta 10.

INTELBRAS# show interfaces GigabitEthernet 0/10 protected

COMANDOS PORT SPEED LIMIT

O comando rate-limit realiza a configuração da largura de banda na entrada e saída na porta.

Rate-limit

O comando rate-limit é utilizado para limitar a largura de banda por porta. O valor deve ser múltiplo de 16. Caso o valor configurado não for múltiplo de 16, o switch irá configurar o valor mais próximo. Para desabilitar a função, use o comando no rate-limit.

Sintaxe: rate-limit input/output value

Parâmetros:

- **input:** especifique a largura de banda para a recepção de pacotes.
- **output:** especifique a largura de banda para a transmissão dos pacotes.
- **value:** especifique a largura de banda da transmissão dos pacotes. Esta taxa varia de 1 a 102400 para as portas FAST e de 1 a 1024000 para portas GIGA.

Modo de comando: modo de configuração de interface.

Exemplo: configure taxa de entrada da porta 5 como 5120 kbps e a taxa de saída 1024 kbps.

INTELBRAS(config)# interface GigabitEthernet 0/5

INTELBRAS(config-if-GigabitEthernet0/5)# rate-limit input 5120

INTELBRAS(config-if-GigabitEthernet0/5)# rate-limit output 1024

Show rate-limit

O comando show rate-limit mostra as configurações de velocidade configurados para a porta selecionada.

Sintaxe: show rate-limit

show rate-limit interface port-id

Parâmetros:

- **port_id:** informe a porta para visualizar as configurações. Se não for informada porta, o comando terá como resposta as configurações das portas do switch.

Modo de comando: Privileged EXEC.

Exemplo 1: mostre as informações de configuração da porta 5 do switch.

INTELBRAS# show rate-limit interfaces GigabitEthernet 0/5

Exemplo 2: mostre as informações de configuração de todas as porta do switch.

INTELBRAS# show rate-limit

COMANDOS IEEE 802.1Q VLAN

VLAN (Virtual Local Area Network) é o modo que torna possível dividir um único segmento de rede LAN em vários segmentos lógicos VLAN. Os computadores de uma mesma VLAN podem se comunicar entre si, independentemente de seu local físico, além de melhorar o desempenho e a segurança da rede.

VLAN

Descrição: o comando vlan é utilizado para criar VLANs no padrão IEEE 802.1q. Para remover uma VLAN criada, utilize o comando no vlan.

Sintaxe: vlan vlan-list

no vlan vlan-list

Parâmetros:

- **vlan-list:** identificação da VLAN, no formato 2-5,7. Variando do ID 2 até 4094.

Modo de comando: modo Global Configuration.

Exemplo: criar VLAN 2-10 e a VLAN 100.

INTELBRAS(config)# vlan 2-10,100

Deletar a VLAN 2:

INTELBRAS(config)# no vlan 2

Description

Descrição: o comando description é utilizado para fornecer uma descrição para a VLAN. Para remover uma descrição criada, utilize o comando no description.

Sintaxe: description descript

no description

Parâmetros:

- **Descript:** nome para descrever a VLAN de no máximo 16 caracteres

Exemplo: especifique o nome da VLAN 2 como grupo1.

INTELBRAS(config)# vlan 2

INTELBRAS(config-vlan)# description grupo1

Show VLAN

Descrição: o comando show vlan é utilizado para exibir informações de VLANs específicas.

Sintaxe: show vlan [VLAN-ID]

Parâmetros:

- **vlan-id:** identificação da VLAN, variando do ID 1 até 4094.

Modo de comando: modo Privileged EXEC.

Exemplo: exibir as informações detalhadas de todas VLANs.

INTELBRAS# show vlan

Exibir detalhadamente as informações da VLAN 2.

INTELBRAS# show vlan 2

Exibir detalhadamente as informações da VLAN 3-10.

INTELBRAS# show vlan 3-10

Switch mode

Descrição: o uso deste comando permite a construção de redes lógicas na camada 2 (Enlace) que limitam os domínios broadcast. O comando especifica o modo de operação das portas do switch, que pode ser especificado como Access / Trunk / Hybrid.

- **Modo Access:** neste modo a porta configurada pode ser membro de apenas uma VLAN. A porta encaminhará os frames da VLAN como untagged.
- **Modo Trunk:** neste modo a porta configurada pode ser membro de uma ou mais VLANs utilizando 802.1q (os frames da VLAN trafegam como untagged por padrão).
- **Modo Hybrid:** neste modo a porta pode encaminhar o tráfego de inúmeras VLAN tagueadas ou não.

Sintaxe: switch mode [trunk, access, hybrid]

Modo de comando: modo Privileged EXEC.

Exemplo: definindo porta 1 como Trunk.

INTELBRAS(config)# interface GigabitEthernet 0/1

INTELBRAS(config-if-GigabitEthernet0/1)# switch mode trunk

Atribuir VLAN

Modo Access:

Sintaxe: switch mode access vlan-id

Parâmetro:

- **switch mode access vlan-id:** adiciona a porta em modo Access na VLAN indicada.

Modo de comando: Global Configuration.

Exemplo: inclua a porta 01 na VLAN 2 (a porta 01 está em modo Access).

INTELBRAS(config)# interface GigabitEthernet 0/1

INTELBRAS(config-if-GigabitEthernet0/1)# switch access vlan 2

Modo Trunk:

Sintaxe: switch mode trunk allowed vlan-id

Parâmetro:

- **switch mode trunk allowed vlan-id:** adiciona a porta em modo Trunk na VLAN indicada

- **no switch mode trunk allowed vlan-id:** remove a porta da VLAN.

Modo de comando: Global Configuration.

Exemplo: inclua a porta 01 na VLAN 3 (a porta 01 está em modo Trunk).

INTELBRAS(config)# interface GigabitEthernet 0/1

INTELBRAS(config-if-GigabitEthernet0/1)# switch trunk allowed vlan 3

Modo Hybrid:

Sintaxe: switch mode hybrid vlan-id [tagged / untagged]

Parâmetro:

- **switch mode hybrid vlan-id [tagged / untagged]:** adiciona a porta em modo Hybrid na VLAN indicada.
- **no switch mode hybrid vlan-id [tagged / untagged]:** para remover a porta da VLAN.

Modo de comando: Global Configuration.

Exemplo: inclua a porta 01 na VLAN 4 (a porta 01 está em modo Hybrid).

INTELBRAS(config)# interface GigabitEthernet 0/1

INTELBRAS(config-if-GigabitEthernet0/1)# switch hybrid vlan 4 untagged

INTELBRAS(config-if-GigabitEthernet0/1)# switch hybrid vlan 4 tagged

Vincular VLAN nativa

Modo Access: a VLAN nativa padrão é Access.

Modo Trunk:

Sintaxe: switch trunk native vlan-id

Parâmetro:

- **switch trunk native vlan-id:** adiciona a VLAN indicada como VLAN nativa na porta.
- **no switch trunk native vlan-id:** retorna a VLAN 1 como VLAN nativa da porta.

Modo de comando: Global Configuration.

Exemplo: inclua a VLAN 2 como VLAN nativa da porta 01.

INTELBRAS(config)# interface GigabitEthernet 0/1

INTELBRAS(config-if-GigabitEthernet0/1)# switch trunk native vlan 2

Modo Hybrid:

Sintaxe: switch trunk native vlan-id

Parâmetro:

- **switch trunk native vlan-id:** adiciona a VLAN indicada como VLAN nativa na porta.
- **no switch trunk native vlan-id:** retorna a VLAN 1 como VLAN nativa da porta.

Modo de comando: Global Configuration

Exemplo: inclua a VLAN 2 como VLAN nativa da porta 01.

INTELBRAS(config)# interface GigabitEthernet 0/1

INTELBRAS(config-if-GigabitEthernet0/1)# switch hybrid native vlan 2

COMANDOS VLAN DE VOZ (VOICE VLAN)

Voice VLANs são configuradas especialmente para o fluxo de voz. Ao configurar VLANs de voz e adicionar as portas a dispositivos de voz, você pode executar QoS relacionando as configurações de dados e voz, garantindo a prioridade de transmissão dos fluxos de dados e a qualidade da voz.

Voice VLAN

Descrição: primeiro deve-se criar uma VLAN para depois atribuir a VLAN para VLAN de voz.

Sintaxe: voice-vlan vlan [id]

voice-vlan

no voice vlan

Parâmetro:

id: ID da VLAN.

Modo de comando: Global mode.

Exemplo: especificar a VLAN 2 como VLAN de voz e habilitar serviço

INTELBRAS(config)# voice-vlan vlan 2

INTELBRAS(config)# voice-vlan

Modos Voice VLAN

Descrição: com o comando voice-vlan mode [autoTag | autounTag | manual]

Parâmetro:

- **autoTag:** se o modo de porta VLAN configurado na porta for autoTag, a porta é ingressada automaticamente com a VLAN de voz, com tag.
- **autounTag:** se o modo de porta VLAN configurado na porta for autoTag, a porta é ingressada automaticamente com a VLAN de voz, sem tag.
- **manual:** ao adicionar o modo VLAN de voz manual, você deve configurar a porta para a VLAN de voz com antecedência.

>Modo de comando: Interface configuration mode.

Exemplo: configure a porta 1 à VLAN de voz com autotag.

INTELBRAS(config)# interface GigabitEthernet 0/1

INTELBRAS(config-if-GigabitEthernet0/1)# voice-vlan mode autoTag

Voice VLAN OUI

Descrição: o comando voice-vlan oui-table é usado para preencher a tabela OUI. Quando o MAC de alguma porta corresponder a tabela OUI a porta será adicionada a VLAN de voz. É possível criar 8 regras na tabela.

Sintaxe: voice-vlan oui-table [endereço MAC] mask [Máscara do MAC]

Modo de comando: Global mode.

Exemplo: configure a tabela.

INTELBRAS(config)# voice-vlan oui-table 02:00:12:32:56:89 mask FF:FF:FF:FF:FF:00

Voice VLAN aging-time and COS

Descrição: o aging-time (tempo de envelhecimento) e o valor COS se referem ao tempo de gravação e à prioridade da mensagem de voz depois que a porta é adicionada à VLAN de voz.

Sintaxe: voice-vlan aging-time (1-65535)

voice-vlan cos (0-7) remark

Parâmetro:

- **aging-time:** (1-65535) o padrão é 720 minutos
- **cos:** valor padrão é 5.

Modo de comando: Global mode.

Exemplo: configure a voice VLAN para 30 minutos e com prioridade 7.

INTELBRAS(config)# voice-vlan aging-time 30

INTELBRAS(config)# voice-vlan cos 7 remark

Show voice VLAN

Descrição: os comandos Show vlan id e Show voice-vlan device são usados para exibir as configurações da VLAN de voz.

Sintaxe: Show vlan [id VLAN] - exibe as configurações globais.

Show voice-vlan device - exibe as portas na VLAN de voz.

Modo de comando: Global mode.

Exemplo:

INTELBRAS# show voice-vlan device

INTELBRAS# show vlan 2

VLAN DE VIGILÂNCIA (SURVEILLANCE VLAN)

Surveillance VLAN

Descrição: primeiro deve-se criar uma VLAN para depois atribuir a VLAN para Surveillance VLAN.

Sintaxe: surveillance-vlan vlan [id]

surveillance-vlan

no surveillance-vlan

Parâmetro:

- **id:** ID da VLAN.

Modo de comando: Global mode.

Exemplo: especificar a VLAN 3 como Surveillance VLAN e habilitar serviço.

IINTELBRAS(config)# surveillance-vlan vlan 3

INTELBRAS(config)# surveillance-vlan

Modos surveillance VLAN

Descrição: com o comando surveillance-vlan mode [auto | manual]

Parâmetro:

- **auto:** se o modo de porta VLAN for configurado na porta no modo Auto, a porta é ingressada automaticamente com a surveillance VLAN.
- **manual:** ao adicionar o modo Surveillance VLAN manual, você deve configurar a porta para a surveillance VLAN com antecedência.

Modo de comando: Interface configuration mode.

Exemplo: configure a porta 1 à surveillance VLAN no modo Auto

INTELBRAS(config)# interface GigabitEthernet 0/1

INTELBRAS(config-if-GigabitEthernet0/1)# surveillance-vlan mode auto

Surveillance Voice VLAN OUI

Descrição: o comando surveillance-vlan oui-table é usado para preencher a tabela OUI. Quando o MAC de alguma porta corresponder a tabela OUI a porta será adicionada a surveillance VLAN. É possível criar 8 regras na tabela.

Sintaxe: surveillance-vlan oui-table [endereço MAC] mask [Máscara do MAC] componentType [DLINK_DEV | network_storage | other | video_encoder | vms | vms_client]

Parâmetros:

- **DLINK_DEV** - dispositivo dlink
- **network_storage** - Network Storage
- **other** - Other IP Surveillance Device
- **video_encoder** - Video Encoder
- **vms** - Video Management Server
- **vms_client** - VMS Client/Remote Viewer

Modo de comando: Global mode

Exemplo: configure a tabela.

INTELBRAS(config)# surveillance-vlan oui-table 04:10:12:32:56:89 mask FF:FF:FF:FF:FF:00 componentType video_encoder

Surveillance VLAN aging-time and COS

Descrição: o aging-time (tempo de envelhecimento) e o valor COS se referem ao tempo de gravação e à prioridade da mensagem de voz depois que a porta é adicionada à Surveillance VLAN.

Sintaxe: surveillance-vlan aging-time (1-65535)

surveillance-vlan cos (0-7) remark

Parâmetro:

- **aging-time:** (1-65535) o padrão é 720 minutos
- **cos:** valor padrão é 5

Modo de comando: Global mode

Exemplo: configure a surveillance VLAN para 30 minutos e com prioridade 7.

INTELBRAS(config)# surveillance-vlan aging-time 30

INTELBRAS(config)# surveillance-vlan cos 7 remark

Show surveillance VLAN

Descrição: os comandos Show vlan id e Show surveillance-vlan device são usados para exibir as configurações de Surveillance VLAN.

Sintaxe: Show vlan [id vlan

Show surveillance-vlan device

Modo de comando: Global mode.

Exemplo:

INTELBRAS# show surveillance-vlan device

INTELBRAS# show vlan 2

MAC VLAN

MAC VLAN é a maneira de classificar as VLANs de acordo com o endereço MAC dos dispositivos. Um endereço MAC corresponde a uma identificação de VLAN. Para um dispositivo que possua seu endereço MAC vinculado a uma VLAN poderá ser conectada a outras portas membros desta VLAN, que mesmo assim, terá seu papel de membro efetivo sem alterar as configurações de outros membros da VLAN.

Grupo MAC VLAN

Descrição: primeiramente é necessário criar um grupo MAC VLAN (1 -16). O endereço MAC deve ser um endereço unicast, defina uma máscara para coincidir com o número de bits de endereço MAC.

Sintaxe: vlan mac-vlan group [vlan-id (1-16)] xx:xx:xx:xx:xx:xx mask (9-48)

no vlan mac-vlan group xx:xx:xx:xx:xx:xx mask (9-48)

show vlan mac-vlan groups

Parâmetro:

- **vlan ID:** varia de 1 à 16.
- **MAC:** endereço MAC.
- **mask:** varia de 9 à 48.

Modo de comando: Global mode.

Exemplo: crie o grupo 2 para o MAC 02:00:48:22:88:36 com máscara 48.

INTELBRAS(config)# vlan mac-vlan group 2 02:00:48:22:88:36 mask 48

Atribuir MAC VLAN

Descrição: primeiro crie uma VLAN e um grupo MAC VLAN para atribuir a VLAN à uma interface.

Sintaxe: vlan mac-vlan group grupo-id vlan vlan-id

mac-vlan

no mac-vlan

show vlan mac-vlan

Parâmetro:

- **grupo-id:** especifica a ID de grupo.
- **vlan-id:** especifica a ID da VLAN.

Modo de comando: Interface configuration mode.

Exemplo: adicione a porta 03 na VLAN 2 do grupo 2.

INTELBRAS(config-if-GigabitEthernet0/3)# vlan mac-vlan group 2 vlan 2

INTELBRAS(config-if-GigabitEthernet0/3)# mac-vlan

Modo MAC VLAN

Descrição: use a opção Auto Surveillance VLAN para reverter a interface ao padrão.

Sintaxe: mac-vlan mode [autountag | manual]

Parâmetro:

- **autountag:** se o modo MAC VLAN configurado na porta for autountag, a porta é automaticamente associada no MAC VLAN.
- **manual:** ao adicionar o modo MAC VLAN manualmente à porta você precisa encaminhar a porta para a MAC VLAN.

Modo de comando: Interface configuration mode

Exemplo: associe a porta 04 na MAC VLAN autountag.

INTELBRAS(config)# interface GigabitEthernet 0/4

INTELBRAS(config-if-GigabitEthernet0/4)# mac-vlan mode autoUntag

---

VLAN DE CONVIDADO (GUEST VLAN)

A função Guest VLAN permite que os suplicantes que não passam na autenticação possam acessar os recursos de uma rede específica. Por padrão, todas as portas conectadas aos suplicantes pertencem a uma VLAN, ou seja, a Guest VLAN. Usuários pertencentes à Guest VLAN podem acessar os recursos da Guest VLAN sem estarem autenticados. Ao realizar uma autenticação, as portas do switch irão ser removidas da Guest VLAN, permitindo o acesso aos recursos da rede.

Configurações servidor RADIUS

Descrição: no comando radius host é possível configurar um servidor radius.

Sintaxe: radius host (radius server ip) auth-port (The default billing port is 1812)

<0-65535> key (password) priority <0-65535> retransmit <1-10>

timeout <1-30> type 802.1x (login, 802.1x, all)

no radius host A.B.C.D(radius server ip)

Parâmetro:

- **Radius host:** IP do servidor radius
- **Auth-port:** porta de autenticação, por padrão a porta definida é 1812.
- **key Radius:** senha.
- **priority:** valor da prioridade do grupo de servidores.
- **retransmit:** número de retransmissão. O padrão são 3 tentativas
- **timeout:** tempo de espera da resposta do servidor RADIUS. O padrão são 3
- **type:** tipo de uso.

Modo de comando: Global mode.

Exemplo:

INTELBRAS(config)# radius host 192.168.0.10 priority 2 type login

Modos de autenticação

Descrição: o comando authentication host-mode permite configurar um modo de autenticação nas portas do switch.

Sintaxe: authentication host-mode [multi-auth | multi-host | single-host]

Parâmetros:

- **multi-auth:** cada endereço MAC precisa ser autenticado.
- **multi-host:** todos os hosts conectados na porta podem acessar o servidor RADIUS.
- **single-host:** somente um endereço MAC é autenticado.

Modo de comando: Interface configuration mode.

Exemplo: configure a porta 2 para o modo de autenticação multi-host.

INTELBRAS(config)# interface GigabitEthernet 0/2

INTELBRAS(config-if-GigabitEthernet0/2)# authentication host-mode multi-host

Guest VLAN

Descrição: primeiro deve-se criar uma VLAN para depois configurar uma GUEST VLAN.

Sintaxe: authentication guest-vlan [id]

no authentication guest-vlan

Show guest-vlan

Modo de comando: Global configuration mode.

Exemplo: configure a guest VLAN na VLAN 4.

INTELBRAS(config)# authentication guest-vlan 4

Modo de controle da porta

Descrição: o comando authentication port-control permite alterar o modo de controle da porta.

Sintaxe: authentication port-control [auto | force-auth| force-unauth]

Parâmetros:

- **auto:** neste modo a porta é autenticada automaticamente quando um host realiza o acesso.
- **force-auth:** neste modo a porta se mantém no estado de autenticada.
- **force-unauth:** neste modo a porta fica no estado não autenticado ignorando requisições do cliente.

Modo de comando: Interface configuration mode.

Exemplo: configure a porta 2 para auto.

INTELBRAS(config)# interface GigabitEthernet 0/2

INTELBRAS(config-if-GigabitEthernet0/2)# authentication port-control auto

---

VLAN POR PROTOCOLO

Ao receber um pacote o switch verifica se o protocolo de rede do pacote possui uma entrada correspondente nas configurações de VLAN por Protocolo.

Grupo protocolo VLAN

Descrição: primeiro deve-se criar uma VLAN para depois configurar uma VLAN por protocolo.

Sintaxe: Protocol-vlan group [vlan-id] frame-type [ethernet_ii | llc_other |

snap_1042] protocol-value [(0x0600-0xFFFE)]

no vlan protocol-vlan group [vlan-id]

Parâmetro:

- **ethernet_ii:** modo de encapsulamento Ethernet II.
-
- **llc_other:** modo de encapsulamento 802.3 LLC (logic link control).
- **snap_1042:** modo de encapsulamento 802.3 SNAP 1042.
- **protocol-value:** (0x0600-0xFFFE).

Modo de comando: Global mode.

Exemplo: configure o frame type para Ethernet II.

INTELBRAS(config)# vlan protocol-vlan group 2 frame-type ethernet_ii protoco -value 0x800

Interface protocolo VLAN

Descrição: é necessário que a porta esteja em modo Hybrid. O ID do protocolo VLAN não pode ser o mesmo que a ID Surveillance VLAN e a ID da VLAN de voz.

Sintaxe: vlan protocol-vlan group [group-id] vlan [vlan-id]

no vlan protocol-vlan group [group-id]

show vlan protocol-vlan interfaces GigabitEthernet 0/x

Modo de comando: Interface configuration mode.

Exemplo: insira a porta 01 na VLAN de protocolo 2.

INTELBRAS(config)# interface GigabitEthernet 0/2

INTELBRAS(config-if-GigabitEthernet0/2)# switch hybrid vlan 6 untagged

INTELBRAS(config-if-GigabitEthernet0/2)# vlan protocol-vlan group 2 vlan 6

MVR (MULTICAST VLAN REGISTRATION)

Em redes VLAN de multicast, os assinantes de um grupo Multicast podem existir em mais de uma VLAN. Se as restrições do limite da VLAN em uma rede consistem em switches de Camada 2, pode ser necessário replicar o stream multicast ao mesmo grupo em sub-redes diferentes, mesmo se estiverem na mesma rede física. O Multicast VLAN Registration (MVR) roteia pacotes recebidos em uma VLAN de origem de multicast para uma ou mais VLANs de recebimento. Os clientes estão nas VLANs de recepção e o servidor de multicast está na VLAN de origem.

MVR

Descrição: o comando mvr habilita o serviço no switch. Digite no mvr para desativar o serviço. É necessário criar uma VLAN para depois defini-la como VLAN MVR.

Sintaxe: mvr

mvr vlan [vlan-id]

no mvr

Modo de comando: Global mode.

Exemplo:

INTELBRAS(config)# no mvr

INTELBRAS(config)# mvr

INTELBRAS(config)# mvr vlan 4

Tipo de porta e MVR immediate

Descrição: o comando mvr type possibilita definir o tipo da porta

Sintaxe: mvr type [receiver| source]

Mvr immediate - Retira a porta da VLAN MVR

Parâmetros:

- **receiver:** define a porta como receptora.
- **source:** define a porta como origem.

Modo de comando: Interface configuration mode.

Exemplo: configure a porta 2 em modo Receiver

INTELBRAS(config)# interface GigabitEthernet 0/2

INTELBRAS(config-if-GigabitEthernet0/2)# mvr type receiver

Modo MVR

Descrição: o comando mvr mode configura o modo da VLAN MVR.

Sintaxe: Mvr mode [compatible | dynamic]

Parâmetros:

- **compatible:** neste modo é aplicado apenas a porta receiver. A porta de source deve ser configurada na VLAN e adicionada no grupo Multicast.
- **dynamic:** neste modo as portas receiver / source podem ser configuradas no grupo Multicast.

Modo de comando: Global mode

Exemplo: configure a MVR como modo Dynamic.

INTELBRAS(config)# mvr mode dynamic

Grupo MVR

Descrição: o comando mvr group adiciona uma faixa de endereços IPs ao grupo MVR.

Sintaxe: mvr group [endereço IP] [série contígua 1-128]

Parâmetro:

- **série contígua:** série contígua de endereço de multicast IPv4.

Modo de comando: Global mode.

Exemplo: adicione o IP 239.0.0.3 5.

INTELBRAS(config)# mvr group 239.0.0.3 5

INTELBRAS(config)# mvr query-time 2

Tempo de consulta (query time)

Descrição: o comando query-time define o tempo em segundos de consulta do grupo.

Sintaxe: query-time [1-10]

Modo de comando: Global mode.

Exemplo:

INTELBRAS(config)# query-time 5

GVRP

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

Sem o GVRP em funcionamento, configurando a mesma VLAN em uma rede, seria necessário a configuração manual em cada dispositivo.

Para criar uma VLAN dinamicamente em todas as portas em um link de rede, você deve configurar a mesma VLAN estática em ambas das extremidades do link. Chamamos de configuração manual quando o VLAN 802.1Q é definido como VLAN estática, e quando a VLAN é criada através do GVRP chamamos de VLAN dinâmica.

As portas em modo tronco em uma VLAN estática podem iniciar o envio de mensagens com registros GVRP para outras portas. E uma porta que registra VLANs somente quando ele recebe mensagens de GVRP. Como as mensagens só podem ser enviadas a partir de um membro do GVRP para outro, duas vias de registro são necessárias para configurar uma VLAN em todas as portas em um link.

Para implementar o registro bidirecional é necessário configurar manualmente a mesma VLAN estática em ambas das extremidades do link, configurar o modo de registro GVRP como fixo para evitar que o switch de acesso crie VLAN dinâmicas que não pertençam à sua rede prevenindo assim o registro dinâmico ou cancelamento do registro de VLAN em formação.

Para configurar a criação de VLAN dinâmica em outros switches, defina o modo de registro nas portas de conexão como normal para permitir o registo dinâmico e de cancelamento VLANs.

O GVRP somente funcionará em portas configuradas em modo trunk.

GVRP

Descrição: o comando gvrp habilita o serviço no switch. Digite no gvrp para desativar o serviço. No switch de acesso é necessário criar uma VLAN adicionar a porta de acesso e configurar esta porta como porta tronco.

Sintaxe: mvr

no mvr

Modo de comando: Global mode.

Exemplo:

INTELBRAS(config)# no gvrp

INTELBRAS(config)# gvrp

GVRP registration-mode

Descrição: o comando gvrp registration-mode permite configurar o modo do GVRP nas portas do switch. Use no gvrp para desabilitar o GVRP na interface.

Sintaxe: gvrp registration-mode [fixed | forbidden | normal]

- **fixed:** neste modo, a porta é incapaz de registrar e remover os registros de VLANs dinamicamente, e pode transmitir apenas as informações de registro da VLAN estática.
- **normal:** neste modo, a porta pode registrar dinamicamente e remover o registro das VLANs, e transmitir as informações de registro da VLAN de ambos de forma dinâmica e estática.
- **forbidden:** neste modo, a porta é incapaz de registrar e remover os registros de VLANs dinamicamente, e pode transmitir apenas as informações da VLAN 1.

Modo de comando: Interface configuration mode.

Exemplo: Configure a porta 18 como modo de gvrp fixo.

INTELBRAS(config)# interface GigabitEthernet 0/18

INTELBRAS(config-if-GigabitEthernet0/18)# gvrp registration-mode fixed

GVRP vlan-creation-forbid

Descrição: o comando vlan-gvrp registration-forbid no modo de configuração de interface, desabilita a criação ou modificação de VLANs dinâmicas. Utilize o comando no gvrp vlan-regsitration-forbid para habilitar o recurso.

Sintaxe: no gvrp vlan-registration-forbid

gvrp vlan-registration-forbid

Modo de comando: Interface configuration mode.

Exemplo: habilite a criação e modificação de VLANs dinâmicas para a porta 18.

INTELBRAS(config)# interface GigabitEthernet 0/18

INTELBRAS(config-if-GigabitEthernet0/18)# no gvrp vlan-registration-forbid

---

PROTEÇÃO DDOS

Em ataques DDoS baseados em volume (ou volumétricos), os invasores normalmente inundam a vítima com um alto volume de pacotes ou conexões, equipamentos de rede esmagadores, servidores ou recursos de largura de banda. O switch possuiu recursos para evitar esses tipos de ataques.

Configurando proteção DDoS

Descrição: com a proteção DDoS ativada o switch protege a rede contra possíveis ataques DDoS.

Sintaxe: Dos{[land-deny | smurf-deny | nullscan-deny | xma-deny | synfin-deny | syn-sportl1024-deny | pod-deny]}

Para desativar o DDoS use o comando no dos {[land-deny | smurf-deny | nullscandeny | xma-deny | synfin-deny | syn-sportl1024-deny | pod-deny]}

Parâmetro:

- **land-deny**
- **smurf-deny**
- **nullscan-deny**
- **xma-deny**
- **synfin-deny**
- **syn-sportl1024-deny**
- **pod-deny**

Modo de comando: Global mode.

Exemplo: ativar e desativar a proteção land-deny.

INTELBRAS(config)# dos land-deny

INTELBRAS(config)# no dos land-deny

Show DDoS

Descrição: veja as informações de configuração para proteção DDoS.

Sintaxe: show dos

Modo de comando: Privileged mode.

Exemplo:

INTELBRAS# show dos

INSPEÇÃO ARP

A inspeção ARP é um recurso de segurança que valida pacotes ARP em uma rede. Intercepta, logs, e rejeita pacotes ARP com as bindings do endereço IP-à-MAC inválidas. Esta capacidade protege a rede de determinados ataques que envolva pessoas.

Arp inspection

Descrição: use o comando arp-inspection para habilitar a função de Inspeção ARP.

Use no arp-inspection para desativar.

Sintaxe: arp-inspetion

no arp-inspection

Show arp-inspection

Modo de comando: Global mode.

Exemplo:

INTELBRAS(config)# arp-inspection

INTELBRAS(config)# arp-inspection

Arp inspection rate-limit

Descrição: o comando arp-inspection rate-limit limita os pacotes ARP recebidos. Quando o valor de pacotes recebidos ultrapassar o limite, os próximos pacotes ARP serão dropados.

Sintaxe: arp-inspection rate-limit [número de pacotes]

no arp-inspection rate-limit

Parâmetro:

- **número de pacotes:** varia de 1 à 50.
- show arp-inspection interfaces GigabitEthernet 0/x

Modo de comando: Interface configuration mode

Exemplo: configure o limite de rate-limite em 30 na porta 01.

INTELBRAS(config)# interface GigabitEthernet 0/1

INTELBRAS(config-if-GigabitEthernet0/1)# arp-inspection rate-limit 30

INTELBRAS(config-if-GigabitEthernet0/1)# end

Arp inspection trust

Descrição: o comando arp-inspection trust configura uma porta como confiável. Ao configurar uma porta confiável o switch não verifica os pacotes ARP na porta escolhida.

Sintaxe: arp-inspection trust

Parâmetro:

- show arp-inspection interfaces GigabitEthernet 0/x

Modo de comando: Interface configuration mode.

Exemplo: configure a porta 01 como confiável.

INTELBRAS(config)# interface GigabitEthernet 0/1

INTELBRAS(config-if-GigabitEthernet0/1)# arp-inspection trust

Arp inspection validate

Descrição: permite configurar o tipo de validação da inspeção ARP.

Sintaxe: arp-inspection validate {[src-mac|dst-mac|ip[allow-zeros]]}

no arp-inspection validate {[src-mac|dst-mac|ip[allow-zeros]]}

show arp-inspection interfaces GigabitEthernet 0/x

Parâmetro:

- **src-mac:** para o src-mac, ele verifica o endereço MAC da origem no cabeçalho Ethernet conjunto ao endereço MAC do remetente no corpo ARP. Esta verificação é realizada tanto em pedidos ARP quanto em respostas. Quando ativado, os pacotes com endereços MAC diferentes são classificados como inválidos e são descartados.
- **dst-mac:** para dst-mac, ele verifica o endereço MAC de destino no cabeçalho Ethernet conjunto ao endereço MAC alvo no ARP. Essa verificação é realizada para respostas ARP. Quando ativado, os pacotes com endereços MAC diferentes são classificados como inválidos e são descartados.
- **ip allow-zeros:** para ip, ele verifica o corpo ARP para endereços IP inválidos e inesperados. Os endereços incluem 0.0.0.0, 255.255.255.255 e todos os endereços de multicast IP. Os endereços IP do remetente são verificados em todos os pedidos e respostas ARP, e os endereços IP alvo são verificados apenas nas respostas ARP.

Modo de comando: interface configuration mode.

Exemplo:

INTELBRAS(config)# interface GigabitEthernet 0/1

INTELBRAS(config-if-GigabitEthernet0/1)# arp-inspection validate src-mac INTELBRAS(config-if-GigabitEthernet0/1)# arp-inspection validate dst-mac INTELBRAS(- config-if-GigabitEthernet0/1)# arp-inspection validate ip allow-zeros

Limpar estatística ARP inspection

Descrição: use o comando clear arp-inspection interface {port-id} para limpar as estatísticas que estão gravadas na interface.

Sintaxe: clear arp-inspection interface {port-id}

show arp-inspection interfaces GigabitEthernet 0/x statistics - Exibe estatísticas da interface

Parâmetro:

- **port-id:** indique a porta.

Modo de comando: Privileged mode.

Exemplo: limpando as estatísticas da porta 01.

INTELBRAS# clear arp-inspection interfaces GigabitEthernet 0/1 statistics

INTELBRAS# show arp-inspection interfaces GigabitEthernet 0/1 statistics

---

COMANDOS DE SEGURANÇA DE PORTAS (PORT SECURITY)

A função Port-Security impede que um ataque na rede faça encher a tabela de endereços MAC do switch, descartando os novos endereços quando o número de MACs aprendidos na porta atingir o limite pré-configurado.

Port-security

O comando port-security é utilizado para habilitar e configurar o limite de endereços MAC da porta. É necessário habilitar o funcionamento globalmente no switch. O comando no port-security desabilita a proteção na porta e globalmente no switch.

Sintaxe: port-security

port-security address-limit number_MAC action discard/forward/shutdown

no port-security

Parâmetros:

- **number_MAC:** limite do número de MAC
- **discard:** descartar os pacotes após atingir o limite máximo configurado.
- **forward:** encaminha os pacotes após atingir o limite máximo configurado.
- **shutdown:** desabilita a porta após atingir o limite máximo configurado. Para retornar, é necessário ativar a porta manualmente.

Modo de comando: modo de configuração de interface.

Exemplo 1: habilite na porta 1 a função de segurança nas portas, selecione modo Discard e especifique o número máximo de aprendizagem pela porta como 30.

INTELBRAS(config)# port-security

INTELBRAS(config)# interface GigabitEthernet 0/

INTELBRAS(config-if-GigabitEthernet0/1)# port-security

INTELBRAS(config-if-GigabitEthernet0/1)# port-security address-limit 30 action discard

Exemplo 2: desabilite a função Port-security na porta 1.

INTELBRAS(config)# interface GigabitEthernet 0/1

INTELBRAS(config-if-GigabitEthernet0/1)# no port-security

Exemplo 3: desabilite a função Port-security globalmente.

INTELBRAS(config)# no port-security

Show port-security

O comando show port-security mostra as configurações de limite de endereço MAC globalmente ou da porta selecionada.

Sintaxe: show port-security

show port-security interface GigabitEthernet port-lid

Parâmetros:

- **port_id:** informe a porta para visualizar as configurações.

Modo de comando: Privileged EXEC.

Exemplo 1: mostre o estado da configuração global da função Port-security

INTELBRAS# show port-security

Exemplo 2: mostre o estado da configuração port-security na porta 1.

INTELBRAS# show port-security interfaces GigabitEthernet 0/1

DHCP-SNOOPING

O snooping do DHCP 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.

Ativando DHCP-snooping

Descrição: se uma porta é uma porta não confiável, então a porta descarta a mensagem de serviço (DHCP_OFFER, DHCP_ACK, DHCP_NCK), se uma porta é uma porta confiável, a porta pode encaminhar mensagens normalmente. Depois ativar a função de DHCP-snooping você pode efetivamente impedir que servidores ilegais sejam estabelecidos na sua rede.

Sintaxe: dhcp-snooping

no dhcp-snooping

show dhcp-snooping

Modo de comando: Global mode./p>

Exemplo: ative a função DHCP-snooping.

INTELBRAS(config)# dhcp-snooping

DHCP-snooping trust

Descrição: configura portas como confiáveis. Por padrão todas as interfaces são não confiáveis. Portas não confiáveis terão os pacotes provenientes de servidores DHCP dropados.

Sintaxe: dhcp-snooping trust

no dhcp-snooping trust

show dhcp-snooping

Modo de comando: Global mode.

Exemplo: configurar a porta 02 como uma porta confiável.

INTELBRAS(config-if-GigabitEthernet0/2)# dhcp-snooping trust

SEGURANÇA DE ACESSO A INTERFACE WEB

Vincula uma interface à uma única máquina através do endereço MAC e endereço IP.

Habilitando segurança

Descrição: o comando web bind enable habilita a segurança de acesso a interface web.

Sintaxe: web bind enable

no web bind enable - Só é possível usar este comando quando nenhuma interface está vinculada a regra. É necessário desvincular a regra para depois desabilitar esta função.

show web bind table - Exibe a tabela de segurança

Modo de comando: Global mode

Exemplo: ative a segurança de acesso a interface WEB no switch.

INTELBRAS(config)# web bind enable

Vinculando interface e dispositivo confiável

Descrição: indique qual interface poderá acessar a interface web, o IP e endereço MAC confiáveis.

Sintaxe: web bind ip {ip-address} mac {mac-address} interface {port_id}

no web bind ip {ip-address} mac {mac-address} interface {port_id} - Para retirar o dispositivo da tabela de segurança. Após isso, é possível desabilitar a segurança web com o seguinte comando: no web bind enable

Parâmetro:

- **ip-address**
- **mac-address:** o formato do MAC deve ser xxxx.xxxx.xxxx
- **port_id**

Modo de comando: Configuration mode.

Exemplo: configure uma interface e um dispositivo como confiável.

INTELBRAS(config)# web bind ip 100.1.1.1 mac 0010.1234.abcd interface GigabitEthernet 0/1

FERRAMENTAS DE TESTE DE CONEXÃO

Através das ferramentas de conexão é possível realizar o diagnóstico básico da rede.

Ping

Descrição: o comando ping é utilizado para verificar a conectividade entre o switch e outro dispositivo de rede.

Sintaxe: ping {ip_addr}

Parâmetros:

- **ping {ip_addr}:** endereço IP do dispositivo de rede de destino.

Exemplo 1: teste a conectividade entre o switch e o computador que possui o endereço IP 192.168.0.100.

INTELBRAS# ping 192.168.0.100

Exemplo 2: teste a conectividade entre o switch e o computador que possui o endereço IPv6 fe80::1104:72ba:d80d:3c99.

INTELBRAS#ping fe80::1104:72ba:d80d:3c99

PING fe80::1104:72ba:d80d:3c99 (fe80::1104:72ba:d80d:3c99): 56 data bytes

64 bytes from fe80::1104:72ba:d80d:3c99: icmp6_seq=0 ttl=64 time=10.0 ms

64 bytes from fe80::1104:72ba:d80d:3c99: icmp6_seq=1 ttl=64 time=0.0 ms

64 bytes from fe80::1104:72ba:d80d:3c99: icmp6_seq=2 ttl=64 time=0.0 ms

64 bytes from fe80::1104:72ba:d80d:3c99: icmp6_seq=3 ttl=64 time=0.0 ms

Traceroute

Descrição: o comando traceroute é utilizado para descobrir o caminho percorrido pelos pacotes desde a sua origem até o seu destino, informando todos os gateways percorridos.

Sintaxe: traceroute endereço-ip [max_hop|time_out] valor

Parâmetros:

- **endereço-ip:** endereço IP de destino do dispositivo de rede.

- **max_hop (saltos):** número máximo de saltos (gateways) que o pacote poderá percorrer. Esta quantidade varia de 1 a 30 saltos, o valor padrão é 4 saltos.
- **time_out:** tempo de conexão entre os saltos em ms (milissegundos).

Modo de comando: User EXEC e Privileged EXEC.

Exemplo: teste a conectividade entre o switch e um dispositivo de rede com endereço IP 192.168.0.131 que possua no máximo 20 saltos.

INTELBRAS# traceroute 192.168.0.131 20 max_hop 20

Diagnóstico do cabo

Descrição: o comando show cable-diag é utilizado para exibir o diagnóstico do cabo conectado a uma porta Ethernet.

Sintaxe: show cable-diag interfaces [port]

Parâmetros:

- **port:** o número da porta para o teste de cabo.

Modo de comando: Privilege mode.

Exemplo: exibir o diagnóstico do cabo da porta 3:

INTELBRAS# show cable-diagnostics interface gigabitEthernet 0/3

DETECÇÃO DE LOOPBACK

Com o recurso de detecção de loopback habilitado, o switch pode detectar voltas usando pacotes de detecção de autorretorno. Quando um loop for detectado, vai aparecer um alerta ou bloquear ainda mais a porta correspondente, de acordo com a configuração.

Loopback-detection

Descrição: o comando loopback-detection é utilizado para ativar a função de detecção de autorretorno globalmente.

Sintaxe: loopback-detection

Parâmetros:

- **enable:** habilita a detecção de loopback.
- ctp-interval [valor 1 - 32767]: intervalo do envio de mensagens de verificação de loop.
- resume-interval [valor 0 ou 60 -1000000]: intervalo de tempo de recuperação automática da porta. O padrão é 60. Para 0 a recuperação da porta é instantânea

- **snmp-trap:** habilita o envio de uma mensagem de alarme, você precisa para iniciar a função SNMP e a SNMP trap primeiro.
- **show loopback-detection:** visualiza o status do loopback-detection nas interfaces.

Modo de comando: Global Configuration.

Exemplo 1: ative a função de detecção de autorretorno na função global:

INTELBRAS(config)# loopback-detection enable

INTELBRAS(config)# loopback-detection ctp-interval 1

INTELBRAS(config)# loopback-detection resume-interval 60

INTELBRAS(config)# loopback-detection snmp-trap

Exemplo 2: visualizar as configurações de loopback-detection.

INTELBRAS# show loopback-detection

Loopback detection configuration

Loopback detection : disabled

CTP tx interval : 1

Port resume interval : 2

Loopback detection trap: disabled

Interfaces	State	Result
gi0/1	*enabled*	*NORMAL*
gi0/2	*enabled*	*NORMAL*
gi0/3	*enabled*	*NORMAL*
gi0/4	*enabled*	*NORMAL*
gi0/5	*enabled*	*NORMAL*
gi0/6	*enabled*	*NORMAL*
gi0/7	*enabled*	*NORMAL*
gi0/8	*enabled*	*NORMAL*
gi0/9	*enabled*	*NORMAL*
gi0/10	*enabled*	*NORMAL*
gi0/11	*enabled*	*NORMAL*
gi0/12	*enabled*	*NORMAL*
gi0/13	*enabled*	*NORMAL*
gi0/14	*enabled*	*NORMAL*
gi0/15	*enabled*	*NORMAL*

gi0/16	*enabled*	*NORMAL*
gi0/17	*enabled*	*NORMAL*
gi0/18	*enabled*	*NORMAL*
gi0/19	*enabled*	*NORMAL*
gi0/20	*enabled*	*NORMAL*
gi0/21	*enabled*	*NORMAL*
gi0/22	*enabled*	*NORMAL*
gi0/23	*enabled*	*NORMAL*
gi0/24	*enabled*	*NORMAL*
gi0/25	*enabled*	*NORMAL*
gi0/26	*enabled*	*NORMAL*
gi0/27	*enabled*	*NORMAL*
gi0/28	*enabled*	*NORMAL*

SPANNING TREE

Spanning tree é a funcionalidade que desativa uma porta que está em LOOP

Habilitar spanning-tree

Descrição: o comando spanning-tree enable ativa o serviço Spanning Tree. Digite no spanning-tree enable para desativar o serviço.

Sintaxe: spanning-tree enable

Modo de comando: Global mode.

Exemplo: ative o Spanning Tree.

INTELBRAS(config)# spanning-tree enable

Habilitar spanning-tree na interface

Descrição: o comando spanning-tree enable ativa o serviço Spanning Tree na interface. Digite no spanning-tree enable para desativar o serviço na interface.

Sintaxe: spanning-tree enable

no spanning-tree enable

show spanning-tree interface gigabitEthernet0/1

Modo de comando: Interface configuration mode.

Exemplo: ative o Spanning Tree.

INTELBRAS(config-if-GigabitEthernet0/1)# spanning-tree enable

INTELBRAS(config-if-GigabitEthernet0/1)# no spanning-tree enable

Modo Spanning Tree

Descrição: o comando spanning-tree mode possibilita definir o modo do Spanning Tree.

Sintaxe: spanning-tree mode [rstp|stp|mstp

show spanning-tree

Parâmetros:

- **rstp:** Rapid Spanning Tree Protocol.
- **stp:** Spanning Tree Protocol, o valor padrão.
- **mstp:** Multiple Spanning Tree Protocol.

Modo de comando: Global mode.

Exemplo: configure o Spanning Tree no modo RSTP.

INTELBRAS(config)# spanning-tree mode rstp

Atraso progressive do Root

Descrição: o comando spanning-tree forward-time tempo de intervalo que a porta muda de estado. Depois de encerrado o loop a porta voltará a operação no intervalo de tempo configurado neste comando. Padrão é 15 segundos.

Sintaxe: spanning-tree forward-time [tempo 4-30s]

Modo de comando: Global mode.

Exemplo: configure o tempo de atraso para 17 segundos.

INTELBRAS(config)# spanning-tree forward-time 17

Intervalo de envio BPDU

Descrição: o comando spanning-tree hello-time spanning-tree hello-time define o intervalo de envio de quadros BPDU para os dispositivos vizinhos. O valor padrão é 2 segundos.

Sintaxe: spanning-tree hello-time [tempo 1-10s]

Modo de comando: Global mode.

Exemplo: configure o intervalo BPDU de 8 segundos.

INTELBRAS(config)# spanning-tree hello-time 8

Spanning-tree max-age

Descrição: o comando spanning-tree max-age [tempo 6-40s] define o tempo de envelhecimento caso o quadro BPDU não retorne, o switch irá recalcular a topologia após o tempo esgotar. O tempo padrão é 20 segundos.

Sintaxe: spanning-tree max-age [tempo 6-40s]

Modo de comando: Global mode.

Exemplo: configure o tempo de envelhecimento em 30 segundos.

INTELBRAS(config)# spanning-tree max-age 30

Spanning-tree max-hops (saltos)

Descrição: o comando spanning-tree max-hops define os hops (saltos) máximos que o quadro BDPU pode realizar. A cada salto é descontado o valor de 1 salto. Caso o valor chegue a 0 o quadro é descartado, com esse comando é possível definir o tamanho da sua topologia. Valor padrão é 20 saltos.

Sintaxe: spanning-tree max-hops [saltos 1-40]

Modo de comando: Global mode.

Exemplo: configure o máximo de 30 saltos para o quadro BPDU.

INTELBRAS(config)# spanning-tree max-hops 30

Spanning-tree pathcost method

Descrição: o comando spanning-tree pathcost method define o método no qual o switch irá calcular o custo de cada caminho. Podendo utilizar o método dot1D-1998 ou dot1T-2001. Por padrão o método dot1T-2001 vem ativado.

Sintaxe: spanning-tree pathcost method [dot1D-1998|dot1T-2001]

Parâmetros:

- **dot1T-2001:** utiliza os cálculos com base no método dot1T-2001.
- **dot1T-1998:** utiliza os cálculos com base no método dot1T-1998.

Modo de comando: Global mode.

Exemplo: configure o método de cálculo dot1T-1998.

INTELBRAS(config)# spanning-tree pathcost method dot1D-1998

Spanning-tree priority (root bridge)

Descrição: o comando spanning-tree priority define o valor de prioridade do ROOT BRIDGE. O switch com o menor valor será o root bridge. Valor padrão é 32768.

Sintaxe: spanning-tree priority [0-61440]

Modo de comando: Global mode.

Exemplo: configure a prioridade para 4096.

INTELBRAS(config)# spanning-tree priority 4096

Spanning tree mst configure

Descrição: o comando spanning-tree mst configuration permite definir alguns parâmetros no MST.

Sintaxe: spanning-tree mst configuration[instance|name|revision|no]}

spanning-tree mst instance (0-15) priority (0-61440)

show spanning-tree mst configuration

Parâmetros:

- **instance [1 -15] vlan [1-4096]:** configura o mapa de relação entre o MSTP e a VLAN.
- **name:** configura o nome da bridge, máximo de 32 caracteres.
- **no name b:** deleta o nome.
- **revision:** número de revisão da configuração MSTP
- **no revision:** deleta o número de revisão.

Modo de comando: spanning-tree mst configure.

Exemplo:

INTELBRAS(config)# spanning-tree mst configuration

INTELBRAS(config-mst)# instance 5 vlan 5

INTELBRAS(config-mst)# name nihao

INTELBRAS(config-mst)# revision 33

INTELBRAS(config)# spanning-tree mst instance 5 priority 4096

Modo BPDU

Descrição: o comando spanning-tree bpdu define o tipo do BPDU.

Sintaxe: spanning-tree bpdu [filter|guard]

no spanning-tree bpdu [filter|guard]

Parâmetros:

- **filter:** a porta não recebe e não envia mensagens BPDU.
- **guard:** a porta não recebe mensagens BPDU.

Modo de comando: Interface configuration mode.

Exemplo: configure a porta no modo BPDU guard.

INTELBRAS(config-if-GigabitEthernet0/1)# spanning-tree bpdu guard

Path Cost

Descrição: o comando spanning-tree cost define o custo do caminho a ser computado pelo switch. O valor padrão é 19.

Sintaxe: spanning-tree cost [1-200000000]

Modo de comando: Interface configuration mode.

Exemplo: defina o custo 2000 na porta 01.

INTELBRAS(config-if-GigabitEthernet0/1)# spanning-tree cost 2000

Spanning tree guard

Descrição: o comando spanning-tree guard configura o tipo de segurança do stp.

Sintaxe: spanning-tree guard [loop|none|root]

Parâmetros:

- **loop:** o BPDU continua bloqueado evitando o loop
- **root:** a porta não seleciona novamente a root bridge após receber um BPDU prioritário.
- **none:** desativa a função Guard.

Modo de comando: Global mode.

Exemplo:

INTELBRAS(config-if-GigabitEthernet0/1)# spanning-tree guard loop

Tipo do link spanning-tree

Descrição: o comando spanning-tree link-type define o tipo de link da porta. Por padrão, a opção seleciona automaticamente o tipo de link com base no modo Duplex da porta, a porta Full duplex é point-to-point e a porta Half duplex é compartilhada (shared).

Sintaxe: spanning-tree link-type [point-to-point|shared]

Modo de comando: Interface configuration mode.

Exemplo: configure a porta 01 para shared.

INTELBRAS(config-if-GigabitEthernet0/1)# spanning-tree link-type shared

Spanning-tree portfast edgeport

Descrição: algumas portas do switch estão conectadas diretamente a computadores, portanto essas portas não precisam participar do Spanning Tree, neste caso a porta pode ser configurada como edgeport.

Sintaxe: spanning-tree portfast [edgeport|network]

Modo de comando: Interface configuration mode.

Exemplo:

INTELBRAS(config-if-GigabitEthernet0/1)# spanning-tree portfast edgeport

Spanning-tree bpdu [filtering|flooding]

Descrição: os pacotes BPDU são filtrados ou sofrem flood quando o STP está desativado. O padrão é BPDU Flooding.

Sintaxe: spanning-tree bpdu [filtering |flooding]

Parâmetros:

- **filtering:** os pacotes BPDU serão filtrados quando o STP for desativado.
- **flooding:** os pacotes BPDU sofrerão flood quando o STP for desativado.

Modo de comando: Global mode.

Exemplo:

INTELBRAS(config)# spanning-tree bpdu filtering

Spanning-tree trap

Descrição: esta função permite ao switch mandar um TRAP caso a topologia mude ou seja definido um novo root.

Sintaxe: spanning-tree trap [new-root| toplogy-change

show spanning-tree trap new-root

Parâmetros:

- **new-root:** envia uma TRAP caso seja encontrado ou definido um novo root na topologia.
- **toplogy-change:** envia uma TRAP caso a topologia seja alterada.

Modo de comando: Global mode.

Exemplo:

INTELBRAS(config)# spanning-tree trap new-root

ACL - CONTROLE DE ACESSO

As regras ACL restringem a comunicação de clientes para clientes ou de clientes para servidores, sendo usada para restringir acessos ilegais na rede.

ACL padrão

Descrição: o comando ip access-list standard é utilizado para criar uma ACL padrão.

Sintaxe: ip access-list standard { número da ACL}

no ip access-list standard { número da ACL} - Para excluir uma regra ACL específica.

Parâmetro:

- **número da ACL:** varia de 0 à 9.

Modo de comando: Global mode.

Exemplo: crie a regra 0 na ACL padrão.

INTELBRAS(config) ip access-list standard 0

ACL estendida

Descrição: o comando ip access-list extended cria uma ACL estendida.

Sintaxe: ip access-list extended { número da ACL}

no ip access-list extended { número da ACL}

Parâmetro:

- **Número da ACL:** varia de 10 à 19.

Modo de comando: ACL configuration mode.

Exemplo: crie uma ACL estendida.

INTELBRAS(config)# ip access-list extended 10

Configurando ACL padrão

Descrição: uma sequência de comandos definem como a regra ACL padrão irá funcionar.

Sintaxe: [0-9] |deny| ou |permit| | any | ou |sip| ou |host|

Parâmetro:

- **número da regra (ACE ID):** varia de 0-9. É a prioridade na quais as regras serão interpretadas pelo switch.
- **no número da regra (ACE ID):** deleta ACE ID.
- **regra:** permite (permit) ou nega (deny).
- **any (qualquer endereço IP de origem) | host (endereço IP específico sem a atribuição de máscara) | sip (IP + máscara do tipo wildcard)**.

Modo de comando: ACL configuration mode.

Exemplo: crie uma regra com ACE ID 0 permitindo o IP 192.168.10.15/24.

INTELBRAS(config-ip-acl-std)# 0 permit sip 192.168.10.15 0.0.0.255

Configurando ACL estendida

Descrição: uma sequência de comandos define como a regra ACL estendida irá funcionar.

Sintaxe: [ace_id] {deny|permit} {ip|tcp|udp} {any|host|sip} [eq] {any|host|dip} [eq]

no {ace_id} - Deletar uma ACE ID.

Parâmetro:

- **ace_id:** varia de 0-9. É a prioridade na quais as regras serão interpretadas pelo switch.
- **deny|permit**
- **ip|tcp|udp**
- **any|host|sip**
- **eq:** porta de origem e/ou destino do protocolo.

Modo de comando: ACL configuration mode.

Exemplo: crie uma regra com ACE 01 estendida que permita pacotes TCP de qualquer host de origem e destino na porta 80.

INTELBRAS(config-ip-acl-ext)# 1 permit tcp any eq 80 any

Vinculando ACL a uma interface (commit)

Descrição: é necessário que as regras ACLs sejam vinculadas a uma interface para que funcionem.

Sintaxe: ip access-list [número da ACL] commit

Parâmetro:

- **Número da ACL:** varia de 0-19.

Modo de comando: interface configuration mode.

Exemplo: vincular ACL 2 na porta 15.

INTELBRAS(config)# interface GigabitEthernet 0/15

INTELBRAS(config-if-GigabitEthernet0/15)# ip access-list 2 commit

ACL padrão IPv6

Descrição: o comando ip access-list standard é utilizado para criar uma ACL padrão IPV6.

Sintaxe: ipv6 access-list standard { ACL-name }

no ipv6 access-list standard { ACL-name} - Para excluir uma regra ACL específica.

Parâmetro:

- **Número da ACL:** varia de 26-35.

Modo de comando: Global mode.

Exemplo: crie a regra 26 na ACL padrão IPV6.

INTELBRAS(config) ipv6 access-list standard 26

ACL IPv6 estendida

Descrição: o comando ip access-list extended cria uma ACL IPv6 estendida.

Sintaxe: ipv6 access-list extended { número da ACL}

no ipv6 access-list extended { número da ACL}

Parâmetro:

- **Número da ACL:** varia de 36 à 45.

Modo de comando: ACL configuration mode.

Exemplo: crie uma ACL estendida.

INTELBRAS(config)# ipv6 access-list extended 10

Configurando ACL padrão IPV6

Descrição: uma sequência de comandos definem como a regra ACL padrão IPv6 irá funcionar.

Sintaxe: [0-9] |deny| ou |permit| | any | ou |sip| ou |host|

Parâmetro:

- **Número da regra (ACE ID):** varia de 0-9. É a prioridade na quais as regras serão interpretadas pelo switch.
- **no número da regra (ACE ID):** deleta ACE ID.
- **regra:** permite (permit) ou nega (deny).
- **any (Qualquer endereço IP de origem) | host (endereço IP específico sem a atribuição de máscara) | sip (IP + prefixo)**.

Modo de comando: ACL configuration mode.

Exemplo: crie uma regra com ACE ID 0 permitindo o IP 2001::5 prefixo 64.

INTELBRAS(config-ipv6-acl-std)# 0 permit sip 2001::5/64

Configurando ACL IPv6 estendida

Descrição: uma sequência de comandos define como a regra ACL IPv6 estendida irá funcionar.

Sintaxe: [ace_id] {deny|permit} {ip|tcp|udp} {any|host|sip} [eq] {any|host|dip} [eq]

no {ace_id} - Deletar uma ACE ID.

Parâmetro:

- **ace_id:** varia de 0-9. É a prioridade na quais as regras serão interpretadas pelo switch.
- **deny|permit**
- **ip|tcp|udp**
- **any|host|sip**
- **eq:** porta de origem e/ou destino do protocolo.

Modo de comando: ACL configuration mode.

Exemplo: crie uma regra com ACE 01 estendida que permita pacotes TCP de qualquer host de origem e destino na porta 80.

INTELBRAS(config-ipv6-acl-ext)# 1 permit tcp any eq 80 any

Vinculando ACL IPV6 a uma interface (commit)

Descrição: é necessário que as regras ACLs sejam vinculadas a uma interface para que funcionem.

Sintaxe: ipv6 access-list [número da ACL] commit

Parâmetro:

- **Número da ACL:** varia de 26-35.

Modo de comando: interface configuration mode.

Exemplo: vincular ACL 2 na porta 15.

INTELBRAS(config)# interface GigabitEthernet 0/15

INTELBRAS(config-if-GigabitEthernet0/15)# ipv6 access-list 2 commit

ACL baseada no MAC

Descrição: uma sequência de comandos define como a regra ACL baseada em MAC irá funcionar.

Sintaxe: mac access-list extended { Número da ACL }

no mac access-list extended { Número da ACL }

Parâmetro:

- **Número da ACL:** varia de 20-25.

Modo de comando: Global mode.

Exemplo: crie uma regra ACL baseada no MAC.

INTELBRAS(config)# mac access-list extended 20

Configurando ACL baseada em MAC

Descrição: uma sequência de comandos define como a regra ACL baseada em MAC irá funcionar

Sintaxe: [0-9] |deny| ou |permit| | any | ou |host|

Parâmetro:

- **número da regra (ACE ID):** varia de 0-9. É a prioridade na quais as regras serão interpretadas pelo switch.
- **no número da regra (ACE ID):** deleta ACE ID.
- **regra:** permite (permit) ou nega (deny).
- **host:** endereço MAC.

Vinculando ACL baseada em MAC a uma interface (commit)

Descrição: é necessário que as regras ACLs sejam vinculadas a uma interface para que funcionem.

Sintaxe: imac access-list { número da ACL } commit

Parâmetro:

- **Número da ACL:** varia de 20-25.

Modo de comando: interface configuration mode.

Exemplo: vincular ACL 20 na porta 1.

INTELBRAS(config)# interface GigabitEthernet 0/1

INTELBRAS(config-if-GigabitEthernet0/15)# mac access-list 20 commit

Show ACL

Descrição: o comando show access-lists exibe as regras ACLs criadas.

Sintaxe: show access-lists

Modo de comando: Privileged mode.

INTELBRAS(config)#show access-lists

show access-list

mac access-list extended 20

0 permit any any

ip access-list standard 0

0 permit any

Example

ip access-list extended 10

0 permit ip any any

ipv6 access-list standard 26

0 permit any

ipv6 access-list extended 36

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.

Ativar IGMP snooping

Descrição: o comando ip igmp snooping ativa o serviço IGMP snooping. Desative o serviço usando o comando no ip igmp snooping.

Sintaxe: ip igmp snooping

no ip igmp snooping

show ip igmp snooping

Modo de comando: Global mode.

Exemplo:

INTELBRAS(config)# ip igmp snooping

INTELBRAS(config)# no ip igmp snooping

Versão IGMP snooping

Descrição: o comando ip igmp snooping version configura a versão do IGMP snooping.

Sintaxe: ip igmp snooping version (2|3)

Modo de comando: Global mode.

Exemplo:

INTELBRAS(config)# ip igmp snooping version 3

IGMP snooping com VLAN

Descrição: é possível ativar o IGMP snooping em uma VLAN específica.

Sintaxe: ip igmp snooping vlan [VLAN-LIST]

Modo de comando: Global mode.

Exemplo: configure o protocolo IGMP na VLAN 2.

INTELBRAS(config)# ip igmp snooping vlan 2

IGMP snooping fast-leave

Descrição: quando o membro sai do grupo o switch encerra a comunicação imediatamente.

Sintaxe: ip igmp snooping fast-leave

Modo de comando: Global mode.

Exemplo: ative o fast-leave.

INTELBRAS(config)# ip igmp snooping fast-leave

IGMP snooping suppression

Descrição: a porta roteador somente enviará pacotes caso ele primeiramente receba pacotes de algum grupo.

Sintaxe: ip igmp snooping suppression

Modo de comando: Global mode.

Exemplo: ative a função Suppression do IGMP

INTELBRAS(config)# ip igmp snooping suppression

IGMP snooping unknow-multicast action

Descrição: esta função permite a porta roteador floodar ou dropar pacotes provenientes de grupos multicast desconhecidos.

Sintaxe: ip igmp snooping unknown-multicast action (drop|flood|router-port)

Modo de comando: Global mode.

Exemplo:

INTELBRAS(config)# ip igmp snooping unknown-multicast action drop

IGMP snooping vlan mrouter learn

Descrição: para habilitar a função Learn use o comando ip igmp snooping vlan VLAN-LIST mrouter learn pim-dvmrp. Para desativar a função use o comando no ipv6 igmp snooping vlan VLAN-LIST mrouter learn pim-dvmrp

Sintaxe: ip igmp snooping vlan VLAN-LIST mrouter learn pim-dvmrp

Modo de comando: Global mode.

Exemplo: ative a função Learning router na VLAN 2.

INTELBRAS(config)# ip igmp snooping vlan 2 mrouter learn pim-dvmrp

IGMP snooping vlan static

Descrição: o grupo estático não aprenderá novas portas e irá sobrepor a configuração estática.

Para ativar a função, use o comando:

ip igmp snooping vlan [VLAN-LIST] static group-address interfaces [GigabitEthernet|Aggregateport] [porta].

Para desativar use o comando:

no ip igmp snooping vlan [VLAN-LIST] static group-address interfaces [GigabitEthernet|Aggregateport] [porta]

Sintaxe: ip igmp snooping vlan [VLAN-LIST] static group-address interfaces [GigabitEthernet|Aggregateport] [porta]

Modo de comando: Global mode.

Exemplo:

INTELBRAS(config)# ip igmp snooping vlan 2 static 239.1.1.1 interfaces GigabitEthernet 0/6

IGMP snooping vlan querier

Descrição: o comando ip igmp snooping vlan [VLAN-LIST] querier ativa a função Querier.

Sintaxe: ip igmp snooping vlan [VLAN-LIST] querier

no ip igmp snooping vlan [VLAN-LIST] querier

show ip igmp snooping querier

Modo de comando: Global mode.

Exemplo:

INTELBRAS(config)# ip igmp snooping vlan 2 querier

Snooping vlan querier version

Descrição: o comando ip igmp snooping vlan [VLAN-LIST] querier version (2|3) define a versão do querier. A versão 2 é configurada por padrão.

Sintaxe: ip igmp snooping vlan [VLAN-LIST] querier version (2|3)

show ip igmp snooping querier

Modo de comando: Global mode.

Exemplo:

INTELBRAS(config)# ip igmp snooping vlan 2 querier version 3

IGMP snooping vlan querier last-member-query-count

Descrição: limita o número de pacotes query que serão enviados. O padrão é 2.

Sintaxe: ip igmp snooping vlan [VLAN-LIST] querier last-member-query-count <1-7>

Modo de comando: Global mode.

Exemplo:

INTELBRAS(config)# ip igmp snooping vlan 2 querier last-member-query-count 5

IGMP snooping vlan querier last-member-query-interval

Descrição: use o comando para definir o intervalo de envio dos pacotes query. Padrão é 1.

Sintaxe: ip igmp snooping vlan [VLAN-LIST] querier last-member-queryinterval <1-25>

no ip igmp snooping vlan [VLAN-LIST] querier last-member-queryinterval

Modo de comando: Global mode.

Exemplo:

INTELBRAS(config)# ip igmp snooping vlan 2 querier last-member-query-interval 10

IGMP snooping vlan querier max-response-time

Descrição: configura o tempo máximo de resposta do pacote query. A unidade padrão é 10 segundos.

Sintaxe: ip igmp snooping vlan [VLAN-LIST] querier max-response-time <5-20>

no ip igmp snooping vlan [VLAN-LIST] querier max-response-time

Modo de comando: Global mode.

Exemplo:

INTELBRAS(config)# ip igmp snooping vlan 2 querier max-response-time 20

IGMP snooping vlan querier query-interval

Descrição: configura o intervalo de envio das mensagens query. Padrão é 125 segundos.

Sintaxe: ip igmp snooping vlan VLAN-LIST querier query-interval <30-18000>

no ip igmp snooping vlan VLAN-LIST querier query-interval

Modo de comando: Global mode.

Exemplo:

INTELBRAS(config)# ip igmp snooping vlan 2 querier query-interval 200

IGMP snooping vlan robustness-variable

Descrição: define o número de tentativas de envio dos pacotes query quando não são respondidos. Padrão são 2 tentativas.

Sintaxe: ip igmp snooping vlan VLAN-LIST robustness-variable <1-7>

no ip igmp snooping vlan VLAN-LIST robustness-variable

Modo de comando: Global mode.

Exemplo:

INTELBRAS(config)# ip igmp snooping vlan 1 robustness-variable 5

IGMP profile

Descrição: possibilita negar ou permitir grupos multicast.

Sintaxe: ip igmp profile <1-128>

no Ip igmp profile <1-128>

show ip igmp profile

Modo de comando: Global mode.

Exemplo: permita o perfil 1 e negue o perfil 5.

INTELBRAS(config)# ip igmp profile 1

INTELBRAS(config)# no ip igmp profile 5

Clear statistics IGMP snooping

Descrição: o comando clear ip igmp snooping statistics limpa as estatísticas do IGMP.

Sintaxe: clear ip igmp snooping statistics

Modo de comando: Privileged mode.

Exemplo:

INTELBRAS#clear ip igmp snooping statistics

IGMP snooping groups

Descrição: o comando clear ip igmp snooping groups limpa os grupos estáticos e dinâmicos salvos pelo switch, é possível limpar uma das opções ou as duas.

Sintaxe: clear ip igmp snooping groups [(dynamic|static)]

Modo de comando: Privileged mode.

Exemplo: limpe os grupo estáticos e dinâmicos.

INTELBRAS# clear ip igmp snooping groups

Lista de comandos show IGMP snooping

Sintaxe:

- **show ip igmp snooping**
- **show ip igmp snooping vlan**
- **show ip igmp snooping vlan** [VLAN-LIST]
- **show ip igmp snooping forward-all** [VLAN-LIST]
- **show ip igmp snooping groups** [counters|dynamic|static]
- **show ip igmp snooping mrouter** [counters|dynamic|static]
- **show ip igmp snooping querier**

Modo de comando: Privileged mode.

CONFIGURAÇÕES DE SISTEMA

Sistema de comando pode ser usado para configurar o sistema de informação e sistema de IP, reiniciar e repor o switch, atualizar o sistema e outras operações.

Show interfaces

Descrição: o comando show interfaces vlan ip permite visualizar as configurações de gerenciamento do switch (IP, gateway padrão e máscara).

Sintaxe: show interfaces vlan ip

Parâmetros:

- **show interfaces vlan ip**

Modo de comando: Privileged mode.

Exemplo: visualize as configurações de IP de gerenciamento.

INTELBRAS(config)# show interfaces vlan ip

Gerenciamento IPv6

Descrição: comando ipv6 define o IP de gerenciamento do switch.

Sintaxe: ipv6

Parâmetros:

- **address:** define o IP do switch.
- **gateway:** define o gateway padrão.
- **prefix:** define o prefixo do endereçamento IPv6.

Modo de comando: Global Configuration.

Exemplo: defina o IPV6 com o IP 2001::2 com gateway padrão 2001::1.

INTELBRAS(config)# ipv6 address 2001::2 prefix 64

INTELBRAS(config)# ipv6 default-gateway 2001::1

Show IPv6

Descrição: o comando show ipv6 permite visualizar as configurações de gerenciamento do switch no IPv6 (IP, gateway padrão e prefixo).

Sintaxe: show IPV6

Parâmetros:

- **show IPV6**

Modo de comando: Privileged mode.

Exemplo: visualize as configurações de IP de gerenciamento.

INTELBRAS(config)# show ipv6

Telnet

Descrição: comando ip telnet habilita o acesso do equipamento por meio do protocolo Telnet.

Sintaxe: ip telnet

Parâmetros:

- **ip telnet:** habilita acesso via Telnet.
- **no ip telnet:** desabilita acesso via Telnet.

Modo de comando: Global mode.

xemplo:E ativar e desativar o acesso via Telnet.

INTELBRAS(config)# ip telnet

INTELBRAS(config)# no telnet

Exportar Log

Descrição: comando copy flash:// e tftp:// permite exportar o log do sistema para um servidor tftp configurado.

Sintaxe: copy (flash://startup-config) (tftp://serverip/filename)

Parâmetros:

- **flash**
- **ftpt**

Modo de comando: Privileged mode.

Exemplo: copiar configurações do switch para o servidor TFTP

INTELBRAS(config)# copy flash://ram.log tftp://192.168.100.149/8

Reiniciar (restart)

Descrição: o comando reload reinicia o equipamento.

Sintaxe: reload

Modo de comando: Privileged mode.

Exemplo: reiniciando o switch.

INTELBRAS(config)# reload

Criação e alteração de usuário WEB

Descrição: o comando username web [usuário] password [senha] é utilizado para criar um novo usuário ou alterar a senha de usuário existente para o acesso web.

Sintaxe: username web [usuário] password [senha]

Parâmetro:

usuário

senha

Modo de comando: Global mode.

Exemplo: configure o nome e senha do usuário.

INTELBRAS(config)# username web gabriel password 123456

Criação ou alteração de usuário CLI

Descrição: o comando username [usuário] { nopassword | password | privilegie | secret } [senha] é utilizado para criar um novo usuário ou alterar um usuário existente somente disponível na CLI.

Sintaxe: username [usuário] nopassword, password, privilegie, secret [senha]

Parâmetro:

- **nopassword:** define um usuário sem senha.
- **password:** define uma senha em texto claro.
- **privilegie:** define os privilégios do usuário.
- **secret:** define uma senha com criptografia.

Modo de comando: Global mode.

Exemplo: configure o nome e senha do usuário CLI com a senha criptografada.

INTELBRAS(config)# username teste secret teste

Log do sistema

Descrição: o comando show logging buffered possibilita visualizar todos os logs do sistema.

Sintaxe: show logging buffered

Modo de comando: Privileged mode.

Exemplo: visualizar os logs do sistema.

INTELBRAS# show logging buffered

Tabela ARP

Descrição: o comando show arp informa os dados da tabela ARP.

Sintaxe: show arp

Modo de comando: Privileged mode.

Exemplo: visualizar a tabela arp.

INTELBRAS# show arp

Informação da memória flash

Descrição: o comando show flash mostra as informações que estão armazenadas na memória flash.

Sintaxe: show flash

Modo de comando: Privileged mode.

Exemplo: visualizar informações da flash.

INTELBRAS# show flash

Informação do CPU

Descrição: o comando show cpu mostra os processos e a porcentagem de uso do CPU.

Sintaxe: show cpu

Modo de comando: Privileged mode.

Exemplo: visualizar informações de CPU.

INTELBRAS# show cpu

Informação de memória

Descrição: o comando show memory mostra a utilização da memória pelo switch.

Sintaxe: show memory

Modo de comando: Privileged mode.

Exemplo: visualizar informações da memória.

INTELBRAS# show memory

Informação da versão

Descrição: o comando show version mostra as informações da versão de firmware corrente.

Sintaxe: show version

Modo de comando: Privileged mode.

Exemplo: visualizar a versão corrente.

INTELBRAS# show version

Informação de configurações

Descrição: o comando show running-config mostra as configurações correntes do switch.

Sintaxe: show running-config

Modo de comando: Privileged mode.

Exemplo: visualizar as configurações correntes do switch.

INTELBRAS# show running-config

Salvar configurações

Descrição: o comando write salva a configuração corrente do switch.

Sintaxe: write

Modo de comando: Privileged mode.

Exemplo: salve as configurações do switch.

INTELBRAS# write

Restaurar padrão de fábrica

Descrição: o comando restore-defaults restaura o switch aos padrões de fábrica.

Sintaxe: restore-defaults

Modo de comando: Privileged mode.

Exemplo: restaure o switch ao padrão de fábrica.

INTELBRAS# restore-defaults

Configuração de MAC estático

Descrição: o comando mac-address static adiciona endereços MAC de servidores e outros equipamentos importantes para a tabela de endereços MAC estática.

Sintaxe: mac-address static [endereço mac] vlan [vlan-id] interface gigabitEthernet [porta-id]

Parâmetro:

- **mac-address static [endereço mac] vlan [vlan-id] interface gigabitEthernet [porta-id]:** adiciona endereço MAC na tabela.
- **no mac-address static [endereço mac] vlan [vlan-id] interface gigabitEthernet [porta-id]:** remove endereço MAC da tabela.
- **show mac-address static:** visualiza tabela MAC.

Modo de comando: Privileged mode.

Exemplo: adicione e remova um endereço MAC estático:

INTELBRAS(config)#INTELBRAS(config)# mac-address static 0001.7A55.E7D2 vlan 1 interfaces GigabitEthernet 0/1

INTELBRAS(config)# no mac-address static 0001.7A55.E7D2 vlan 1

Configuração de bloqueio de MAC (drop)

Descrição: o comando mac-address static [endereço mac] vlan [vlan-id] drop permite bloquear um MAC específico, os pacotes provenientes deste MAC serão dropados.

Sintaxe: mac-address static mac-address vlan vlan-id drop

Parâmetros:

- **no mac-address static mac-address vlan vlan-id drop:** configurar bloqueio.
- **no mac-address static mac-address vlan vlan-id drop:** para desabilitar configuração.
- **show mac-address drop:** informa os MAC que estão sendo dropados.

Modo de comando: Global mode.

Exemplo: configure a tabela para que o MAC 0001.7A55.E7D5 seja dropado.

INTELBRAS(config)# mac-address static 0001.7A55.E7D5 vlan 1 drop

Tempo de envelhecimento da tabela MAC (aging time)

Descrição: o comando aging-time define o tempo de envelhecimento do MAC. Padrão 630s

Sintaxe: aging-time

Parâmetro:

- **show mac-address aging-time:** visualiza o aging time da tabela MAC.

Modo de comando: Global mode.

Exemplo: configure o aging time da tabela MAC para 500 segundos.

INTELBRAS(config)# mac-address aging-time 500

Contagem de endereços MAC

Descrição: o comando show mac-address count mostra os endereços MAC que estão interligados ao equipamento.

Sintaxe: show mac-address count

Modo de comando: Privileged mode.

Exemplo: visualizar endereços MAC aprendidos.

INTELBRAS(config)# show mac-address count

Informações gerais de MAC address

Descrição: o comando show mac-address all permite visualizar todas as informações sobre endereço MAC do switch. O comando engloba os seguintes comandos específicos:

show mac-address static

show mac-address drop

show mac-address dynamic

show mac-address interface

show mac-address vlan

Sintaxe: show mac-address all

Modo de comando: Privileged mode.

Exemplo: visualize todas as informações da tabela MAC.

INTELBRAS(config)# show mac-address all

Uploading da configuração

Descrição: é possível realizar o uploading das configurações para um servidor TFTP.

Sintaxe: copy flash://running-config tftp:// [IP] [porta]

Modo de comando: Privileged mode.

Exemplo: realizar o uploading das configurações para o servidor TFTP com IP 192.168.100.149.

INTELBRAS# copy flash://running-config tftp:///192.168.100.149/5002

Firmware update

Descrição: é possível realizar o update do firmware através de um servidor TFTP.

Sintaxe: copy tftp:// [IP] / [Arquivo].bix flash://image.bin

Modo de comando: Privileged mode.

Exemplo: realiza a atualização do firmware através do servidor tftp com IP 192.168.100.149.

INTELBRAS# copy tftp://192.168.100.149/vmlinux.bix flash:// image.bin

Download de configuração

Descrição: é possível importar as configuração de um servidor TFTP para o switch.

Sintaxe: copy tftp:// [IP] / [PORTA] running-config

Modo de comando: Privileged mode.

Exemplo: importe as configurações de um servidor TFTP:

INTELBRAS# copy tftp://192.168.100.149/5002 running-config

MTU

Descrição: o comando mtu define o tamanho máximo da unidade de transmissão. A MTU padrão é 1522. Unidade de medida: bytes.

O faixa de MTU disponível: 1522-10240.

Sintaxe: mtu [tamanho]

Parâmetro:

- **Show interfaces GigabitEthernet id mtu:** visualiza a MTU da interface configurada.

Modo de comando: Global mode.

Exemplo: defina a MTU em 10240:

INTELBRAS(config)# mtu 10240

SERVIDOR SNTP

Sincronizar com servidor SNTP

Descrição: use este comando para configurar o endereço IP do servidor NTP / SNTP.

Sintaxe: sntp server {server-ip}

show sntp

Parâmetro:

- **server-ip**

Modo de comando: Global mode.

Exemplo: configure o SNTP.

INTELBRAS(config)# sntp server 192.168.100.159

CONFIGURAÇÃO SNMP

Com a função SNMP habilitada, os administradores de rede podem facilmente monitorar o desempenho da rede, detectar as falhas e configurar os dispositivos

Habilitar SNMP

Descrição: use o comando snmp enable para habilitar o SNMP no switch.

Use no snmp enable para desativar o serviço.

Sintaxe: snmp enable

no snmp enable

Modo de comando: Global mode.

Exemplo: habilite o SNMP.

INTELBRAS(config)# snmp enable

Habilitar SNMP TRAP

Descrição: use o comando snmp-server enable traps para ativar o serviço.

Sintaxe: snmp-server enable traps

no snmp-server enable traps

Modo de comando: Global mode.

Exemplo: ative o serviço SNMP TRAP.

INTELBRAS(config)#nmp-server enable traps

Comunidade SNMP

Descrição: o comando snmp-server community permite criar comunidades SNMP.

Sintaxe: snmp-server community Community name [ro | rw|]

Parâmetro:

ro: somente leitura (*read only*).

rw: leitura e escrita (*read and write*).

Modo de comando: Global mode.

Exemplo: crie a comunidade teste com permissão de leitura e escrita.

INTELBRAS (config)# snmp-server community test rw

SNMP host server

Descrição: especificar um SNMP HOST (NMS) para enviar mensagens TRAP execute o comando snmp-server host. Para desativar a função use o comando no snmp-server host

Sintaxe: snmp-server host { endereço do host [traps] [version { 1 | 2c|2} nome da comunidade}

no snmp-server host community name

show snmp community

Parâmetro:

- **endereço do host:** endereço do host que o switch irá verificar a TRAP.
- **versão:** 1 | 2c | 2.
- **nome da comunidade.**

Modo de comando: Global mode.

Exemplo: configure a TRAP para o host com IP 192.168.100.149.

INTELBRAS(config)# snmp-server host 192.168.100.149 traps version 1 test

SNMP trap auth

Descrição: caso a autenticação do serviço SNMP TRAP falhar o SNMP emitirá um aviso auth trap.

Sintaxe: snmp trap auth

no snmp trap auth

show snmp host

Modo de comando: Global mode.

Exemplo: ativa e desative o serviço.

INTELBRAS(config)# snmp trap auth

INTELBRAS(config)# no snmp trap auth

Link Status SNMP TRAP

Descrição: o comando snmp trap linkUp faz com que qualquer mudança nos status de link do switch (*interface gigabitethernet*) seja enviado a um SNMP TRAP.

Sintaxe: snmp trap [linkUp|linkDown]

Parâmetro:

- **linkUp:** ativa o serviço.
- **linkDown:** desativa o serviço.

Modo de comando: Global mode.

Exemplo: ative o serviço SNMP TRAP link status.

INTELBRAS(config)# snmp trap linkup

SNMP TRAP restart

Descrição: caso seja realizado no switch um reboot será enviado uma SNMP TRAP de aviso.

Sintaxe: snmp trap [cold-start | warm-start]

Modo de comando: Global mode.

Exemplo:

INTELBRAS(config)# snmp trap cold-start

INTELBRAS(config)# snmp trap warm-start

SNMP TRAP STP

Descrição: caso a topologia STP mude ou um novo roteador seja criado, uma mensagem SNMP TRAP será enviada

Sintaxe: snmp trap stp

no snmp trap stp

Modo de comando: Global mode.

Exemplo:

INTELBRAS(config)# snmp trap stp

INTELBRAS(config)# no snmp trap stp

RMON

RMON (Monitoramento Remoto), é baseado na arquitetura SNMP. O grupo History é um dos 4 grupos RMON que o switch suporta. Após configurado o grupo History, o switch recolhe as informações de rede periodicamente, assim a estação de gerenciamento pode monitorar a rede de forma eficaz.

Criando evento RMON

Descrição: o comando rmon event é usado para criar ou modificar uma entrada de evento.

O comando rmon alarm é usado para criar ou modificar um alarme de evento RMON.

O comando rmon history é usado para criar ou modificar histórico dos eventos RMON.

O comando clear rmon interface é usado para limpar as estatísticas Ethernet RMON da porta selecionada.

Use o comando no rmon para deletar a configuração RMON.

Sintaxe: rmon event id_event event_type trap_COMMUNITY description_ DESCRIPTION owner_NAME.

Parâmetro:

- **id_event:** configure um índice para a criação ou alteração do evento RMON. Pode variar de 1 à 65535.
- **event_type:** informe o tipo do evento.
- **description:** informe o nome para o evento, variando de 1 a 127 caracteres.
- **log:** esta opção habilita log para o evento.
- **trap:** informe a comunidade trap para o evento. Esta comunidade deve ter sido criada anteriormente.
- **owner:** informe o nome do dispositivo ou usuário que definiu a regra, o nome pode variar de 1 a 31 caracteres.

Modo de comando: Interface configuration mode.

Exemplo 1: configure o nome da comunidade trap para a entrada 1 do grupo Evento como Public. Dê o nome de teste_1 e para o dono do evento chame de dono_1.

INTELBRAS(config)# rmon event 1 trap public description teste_1 owner dono_1

Exemplo 2: delete a entrada do evento 1.

INTELBRAS(config)# no rmon event 1

Criando alarme RMON

Descrição: o comando rmon alarm é usado para criar ou modificar um alarme de evento RMON.

Use o comando no rmon para deletar a configuração RMON.

Sintaxe: rmon alarm id_alarm interface port-id variable interval_sample sample_type rising sample_rising_max event_rising falling sample_falling_min event_ falling startup alarm_type owner name_owner.

Parâmetro:

- **id_alarm:** configure um índice para a criação ou alteração do alarme RMON. Pode variar de 1 à 65535.
- **port_id:** informe a porta para configuração.
- **variable:** selecione o tipo da variável de alarme.
- **interval_sample:** informe o valor para o alarme.
- **sample_type:** existem duas opções, absoluta e incremental:
  - **absolute:** indica uma comparação direta com o valor estabelecido no final do intervalo da amostra.
  - **delta:** indica subtrair o valor da última amostra com o valor corrente e comparar a diferença com o valor estipulado.
- **sample_rising_max:** valor máximo da variável para iniciar o alarme.
- **event_rising:** número do alarme caso o valor máximo seja atingido.
- **sample_falling_min:** valor mínimo da variável para iniciar o alarme.
- **event_falling:** número do alarme caso o valor mínimo seja atingido.
- **alarm_type:** selecione o tipo do alarme:
  - **rising:** indica que o evento de alarme será disparado quando o valor da amostra for maior que o limite superior estabelecido.
  - **falling:** indica que o evento de alarme será disparado quando o valor da amostra for menor que o limite inferior estabelecido.
  - **rising or falling:** indica que o evento de alarme será disparado se o valor da amostra ficar acima do valor do limite superior estabelecido ou abaixo do limite inferior estabelecido.
- **name_owner:** informe o nome do dispositivo ou usuário que definiu regra, o nome pode ter no máximo 31 caracteres.

Modo de comando: Interface configuration mode.

Exemplo 1: configure o alarme número 1 na interface 10, verificando a variável pkts, tendo como valor de referência 1000. O alarme deve verificar o valor absoluto da variável, tendo como valor máximo 5000 e mínimo 500. Monitorando o valor máximo e mínimo, caso atingir valor máximo chame o evento 1 se atingir o valor mínimo chame o evento 2. Definido como dono_1 o proprietário do alarme.

INTELBRAS(config)# rmon alarm 1 interface GigabitEthernet 0/10 pkts 1000 absolute rising 5000 1 falling 500 2 startup rising-falling owner dono_1

Exemplo 2: delete a entrada do alarme 1.

INTELBRAS(config)# no rmon alarm 1

Configurando history RMON

Descrição: o comando rmon history é usado para criar ou modificar estatísticas RMON.

Use o comando no rmon para deletar a configuração RMON.

Sintaxe: rmon history id_history interface port-id buckers num_buckers interval sample_interval owner name_owner

Parâmetro:

- **id_history:** configure um índice para a criação ou alteração do alarme RMON. Pode variar de 1 à 65535.
- **port_id:** informe a porta para configuração.
- **num_buckers:** informe o número de históricos que poderão ser armazenados. Máximo de 50.
- **sample_interval:** especifique o intervalo de coleta das amostras. O valor pode variar de 1 a 3600 segundos.
- **name_owner:** informe o nome do dispositivo ou usuário que definiu regra, o nome pode ter no máximo 31 caracteres.

Modo de comando: Interface configuration mode.

Exemplo 1: habilite a entrada 1 do grupo RMON history na porta 10, tamanho da amostragem 50 com intervalo de amostragem de 300 segundos e configure o proprietário como dono_1.

INTELBRAS(config)# rmon history 1 interface GigabitEthernet 0/10 buckets 50 interval 300 owner dono_1

Exemplo: delete a entrada de RMON history 1.

INTELBRAS(config)# no rmon history 1

Comando show rmon

Descrição: o comando show rmon mostra as configurações de rmon para a porta selecionada.

O comando show rmon interface mostras as estatísticas de rmon.

O comando show rmon event mostra as configurações dos eventos rmon.

O comando show rmon alarm mostra as configurações de alarm rmon.

O comando show rmon history mostra as configurações de history rmon.

Sintaxe: show rmon interfaces GigabitEthernet port_id statistics

show rmon event id_event

show rmon alarm id_alarm

show rmon history id_history

Parâmetro:

- **port_id:** informe a porta que deseja verificar as informações de configuração.
- **id_event:** informe o id do evento para mostrar as configurações de event.

- **id_alarm:** informe o id do alarme para mostrar as configurações de alarm.
- **id_history:** informe o id do history para mostrar as configurações de history.

Modo de comando: Privileged EXEC.

Comando clear rmon

Descrição: o comando clear rmon limpa as estatísticas de rmon da interface selecionada.

Sintaxe: clear rmon interfaces GigabitEthernet port_id statistics

Parâmetro:

- **port_id:** informe a porta para limpeza das estatísticas.

Modo de comando: Privileged EXEC.

Exemplo: delete as estatísticas de rmon da porta 20.

INTELBRAS# clear rmon interfaces GigabitEthernet 0/20 statistics

---

SSH

SSH (*Security Shell*) oferece uma conexão remota segura, garantindo a integridade das informações de gerenciamento do switch.

ip ssh server

Descrição: o comando ip ssh [all|v1|v2] é utilizado para habilitar a função SSH. Para desabilitar esta função, utilize o comando no ip ssh [all|v1|v2].

Sintaxe: ip ssh [all|v1|v2

no ip ssh [all|v1|v2]

Modo de comando: Global Configuration.

Exemplo: habilite a função SSH do switch:

INTELBRAS(config)# ip ssh v2

SSL

Gerar certificado SSL

Descrição: o comando ssl é utilizado para gerar o SSL no switch.

Sintaxe: ssl

Modo de comando: Privileged mode.

Exemplo: gerar SSL:

INTELBRAS(config)# ssl

Limpar certificado SSL

Descrição: o comando ssl replace é utilizado para limpar o SSL já existente no switch.

Sintaxe: ssl replace

Modo de comando: Privileged mode.

Exemplo: limpar configuração do SSL:

INTELBRAS(config)# ssl replace

IPV4 DHCP CLIENT

Ativar DHCP IPv4

Descrição: o comando ip dhcp permite ao switch obter o IP do servidor DHCP.

Sintaxe: ip dhcp

Parâmetros:

- **ip dhcp:** ativa a função DHCP client.
- **no ip dhcp:** desativa a função DHCP client.
- **show ip dhcp:** informa o status da função DHCP.

Modo de comando: Global mode.

Exemplo 1: ativar a função DHCP client.

INTELBRAS# ip dhcp

Exemplo 2: desativar a função DHCP client.

INTELBRAS# no ip dhcp

Exemplo 3: visualizar a função DHCP client e o IP disponibilizado ao switch.

INTELBRAS# show ip dhcp

INTELBRAS# show ip

IPV6 DHCP CLIENT

Ativar DHCP IPv6

Descrição: o comando ipv6 dhcp permite ao switch obter o IP do servidor DHCP

Sintaxe: ipv6 dhcp

Parâmetros:

- **ipv6 dhcp:** ativa a função DHCP client para IPv6.
- **no ipv6 dhcp:** desativa a função DHCP client para IPv6.
- **ipv6 autoconfig:** ativa a função DHCP automático.
- **no ipv6 autoconfig:** desativa a função DHCP automático.

Modo de comando:

Exemplo 1: ativar a função DHCP client.

INTELBRAS(config)# ipv6 dhcp

INTELBRAS(config)# ipv6 autoconfiguration

Exemplo 2: desativar a função DHCP client

INTELBRAS# no ipv6 dhcp

Exemplo 3: visualizar a função DHCP client e o IP disponibilizado ao switch.

INTELBRAS# show ip

Example IP Address: 192.168.0.143

Subnet Netmask: 255.255.255.0

Default Gateway: 192.168.0.177

INTELBRAS# show ip dhcp

DHCP Status : enabled

ROTEAMENTO ESTÁTICO (IPV4)

O termo roteamento refere-se ao processo de definir um caminho sobre o qual os pacotes serão encaminhados. Esta função é indicada para redes com poucos elementos de conexão onde não existam caminhos redundantes. Além disso, é necessário que o administrador da rede tenha conhecimento da topologia da rede para confeccionar as tabelas de roteamento e garantir a convergência da mesma.

Neste switch é possível criar 16 interfaces e 32 rotas estáticas.

Criar/deletar interface

Descrição: o comando interface vlan [vlan-id] cria uma interface.

Obs: a VLAN precisa estar criada.

Sintaxe: interface vlan [vlan-id]

no interface vlan [vlan-id]

Modo de comando: Global mode.

Exemplo: Criar interface na vlan 10:

INTELBRAS(config)# interface vlan 10

INTELBRAS(config-if-vlan)#

Adicionar IP à interface

Descrição: o comando ip address [ip] mask [máscara] adiciona um IP à interface.

Sintaxe: ip address [ip] mask [máscara]

Modo de comando: Global mode.

Exemplo: Adicionar o ip 192.168.10.100/24 na interface vlan 2.

INTELBRAS(config-if-vlan)# ip address 192.168.10.100 mask 255.255.255.0

INTELBRAS(config-if-vlan)#

Visualizar interfaces

Descrição: o comando show interfaces vlan exibe os dados da interface.

Sintaxe: show interface vlan

show interface vlan [vlan id]

show interface vlan ip

Modo de comando: modo Privileged EXEC.

Exemplo: exibir os status de todas as interfaces criadas e os IPs atribuídos.

INTELBRAS# show interfaces vlan

VID	***VLAN Name***	***L3 Interface Name***	***Status***
1	*default*	*eth0.1*	*up*
10	*rota*	*eth0.10*	*up*

INTELBRAS# show interfaces vlan ip

VID	***L3 Interface Name***	***IP Address***	***Subnet Netmask***	***gateway***
1	*eth0.1*	*192.168.0.60*	*255.255.255.0*	*192.168.0.1*
10	*eth0.10*	*192.168.10.200*	*255.255.255.0*	*...*

Criação de rotas estáticas

Descrição: o comando route-entry add ip cria rotas estáticas

Sintaxe: route-entry add ip [ip] netmask [máscara] gw [ip-gateway]

Modo de comando: Global mode.

Exemplo: Adicionar uma rota com destino de rede 192.168.20.0/24 e o roteador da rede sendo 192.168.10.1.

INTELBRAS(config)# route-entry add ip 192.168.20.0 netmask 255.255.255.0 gw 192.168.10.1

Visualizar rotas estáticas

Descrição: o comando show staticroute permite visualizar as rotas criadas e suas configurações.

Sintaxe: show staticrout

Modo de comando: Global mode.

Exemplo: INTELBRAS(config)# do show staticroute

Static Entry Number: 1

Dynamic Entry Number: 0

AclIndex	*Destination*	*Gateway*	*Netmask*	*Flags*	*VID*	*DstMAC*	*Port*
0	*192.168.20.0*	*192.168.10.1*	*255.255.255.0*	*static*	*...*	*...*	*...*

Deletar rota estática

Descrição: o comando route-entry delete index [AclIndex] deleta rotas estáticas.

Modo de comando: Global mode.

Exemplo: remover a rota estática ID 0 (AclIndex 0).

INTELBRAS(config)# route-entry delete index 0

COMANDO QOS

QoS (*Quality of Service*) esta função é utilizada para otimizar o desempenho da rede. Ele lhe proporciona experiência de uma melhor qualidade de serviço da rede.

Modo de prioridade

Descrição: o comando qos trust [prioridade] define o tipo de prioridade do QOS.

Parâmetro:

- **dscp:** prioridade DSCP.
- **cos:** prioridade 802.1p (COS).
- **no qos trust:** retorna as configurações de QOS para o padrão.

Sintaxe: qos trust [prioridade]

Modo de comando: Global mode.

Exemplo: defina a prioridade COS no switch.

INTELBRAS(config)# qos trust cos

Algoritmo de fila

Descrição: define tipo do algoritmo de fila.

Sintaxe: qos queue schedule [tipo da fila]

Parâmetro: qos queue schedule [tipo da fila]

- **wrr:** modo Round Robin Weight. Neste modo, os pacotes em todas as filas são enviados com base no valor de peso para cada fila. A relação valor do peso de TC0, TC1, TC2 e TC3 é de 1: 2: 4: 8.
- **sp:** modo Strict-Priority. Neste modo, a fila com maior prioridade vai ocupar toda a largura de banda. Pacotes na fila com prioridade mais baixa são enviados apenas quando a fila com maior prioridade está vazia.
- **hybrid:** Strict-Priority + modo Weight Round Robin. Neste modo, o switch fornece dois grupos de agendamento, grupo SP e WRR grupo. Filas nos grupos SP e WRR estão programadas estritamente com base no modo Strict-Priority enquanto as filas dentro do grupo WRR seguirem o modo de WRR. Em SP + modo WRR, TC3 é o grupo SP; TC0, TC1 e TC2 pertencem ao grupo WRR e a proporção de peso de valor TC0, TC1 e TC2 é de 1: 2: 4. Desta forma, durante a programação de filas, o interruptor permite TC3 para ocupar toda a largura de banda do seguinte modo SP e o TC0, TC1 e TC2 no grupo WRR vai ocupar a largura de banda de acordo com a sua relação de 1: 2: 4.
- **equ:** Equal-Mode. Neste modo, todas as filas ocupam a largura de banda de forma igual. A relação do valor do peso de todas as filas é 1: 1: 1: 1.
- **show qos queueing:** informa o tipo da fila configurada.

Modo de comando: Global mode.

Exemplo: defina fila wrr.

INTELBRAS(config)# qos queue schedule wrr

QoS map cos-queue

Descrição: o comando qos map cos-queue [valor cos] to [número queue] é utilizado para vincular a prioridade CoS a fila de saída (TC).

Sintaxe: qos map cos-queue [valor cos] to [prioridade da fila]

show qos map cos-queue: visualiza configuração de vínculo.

Parâmetros:

- **valor cos:** é possível utilizar os 8 níveis de prioridade definidos pela norma IEEE 802.1p.
- **número queue:** nível de prioridade da fila de saída (TC). Range de 1 a 4, representados da seguinte forma TC0, TC1, TC2 e TC3.

Modo de comando: Global Configuration.

Exemplo: vincular a prioridade CoS com a fila de saída TC.

INTELBRAS(config)# qos map cos-queue 5 to 2

QoS map dscp-queue

Descrição: o comando qos queue dscp-map é utilizado para configurar a relação entre DSCP e o CoS.

Sintaxe: qos map dscp-queue { dscp-list } to { cos-id }

Show qos map dscp-queue

Parâmetros:

- **dscp-list:** lista de valor DSCP. Um ou vários valores DSCP pode ser digitado usando vírgula para separar. Utilize um hífen para designar uma gama de valores, por exemplo, 1,4-7,11 indica escolher 1, 4, 5, 6, 7, 11. O valor DSCP varia de 0 a 63.
- **cos-id:** o nível de prioridade de pacotes com tag, varia de 0 CoS até COS 7.

Modo de comando: Global Configuration.

Exemplo: relacionar os valores 10-12 de DSCP com CoS 2

INTELBRAS(config)# qos map dscp-queue 10-12 to 2

Modo de comando: Global Configuration.

Exemplo: relacionar os valores 10-12 de DSCP com CoS 2.

INTELBRAS(config)# qos map dscp-queue 10-12 to 2

QoS queue weight

Descrição: quando você usa o modo WRR, você precisa configurar todos os valores de peso das filas. Você pode usar esse comando.

Sintaxe: qos queue weight [valor weight]

Show qos map queueing

Parâmetro:

- **valor weight:** varia de 1- 127.

Modo de comando: Global mode.

Exemplo: configure os pesos das filas 1:1:1:50.

INTELBRAS(config) qos queue weight 1 1 1 5

QoS queue strict-priority num

Descrição: quando você usa o modo Hybrid você precisa configurar as filas do algoritmo SP.

Sintaxe: qos queue strict-priority-num [número da fila]

Modo de comando: Global mode.

Exemplo: vincule o SP na fila 1.

INTELBRAS(config)# qos queue strict-priority-num 1

Show qos

Descrição: o comando show qos é usado para visualizar as configurações correntes e QOS.

Sintaxe: show qos

show qos queueing

show qos map dscp-queue

show qos map cos-queue

Modo de comando: Privileged mode

INTELBRAS(config) show qos

INTELBRAS(config) show qos queueing

INTELBRAS(config) show qos map dscp-queue

INTELBRAS(config) show qos map cos-queue

TERMO DE GARANTIA

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

Nome do cliente:

Assinatura do cliente:

Nº da nota fiscal:

Data da compra:

Modelo:

Nº de série:

Revendedor:

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

1. Todas as partes, peças e componentes do produto são garantidos contra eventuais defeitos de fabricação, que porventura venham a apresentar, pelo prazo de 1 (um) ano – sendo 3 (três) meses de garantia legal e 9 (nove) meses de garantia contratual –, contado a partir da data de entrega do produto ao Senhor Consumidor, conforme consta na nota fiscal de compra do produto, que é parte integrante deste Termo em todo o território nacional. Esta garantia contratual compreende a troca gratuita de partes, peças e componentes que apresentarem defeito de fabricação, incluindo a mão de obra utilizada nesse reparo. Caso não seja constatado defeito de fabricação, e sim defeito(s) proveniente(s) de uso inadequado, o Senhor Consumidor arcará com essas despesas.

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

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

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

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

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

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

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

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

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

Todas as imagens deste manual são ilustrativas.

Suporte a clientes: (48) 2106 0006

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

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

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

SAC: 0800 7042767

Onde comprar? Quem instala?: 0800 7245115

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

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

www.intelbras.com.br (http://www.intelbras.com.br)

Indústria Brasileira