intelbras

Manual do usuário

SF 2622 MR L2

intelbras

SF 2622 MR L2
Switch gerenciável 24 portas Fast Ethernet + 2 portas Mini-GBIC compartilhadas

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

O SF 2622 MR L2 é um switch de 24 portas Fast Ethernet com 2 portas Mini-GBIC compartilhadas com 2 portas Gigabit Ethernet. Proporciona altas taxas de transferência de dados, permitindo a integração de computadores, impressoras e dispositivos VoIP como ATA e telefone IP, além de compartilhamento de internet com 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.

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.

LGPD - Lei Geral de Proteção de Dados Pessoais

A Intelbras não acessa, transfere, capta, nem realiza qualquer outro tipo de 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.

Índice

1. Introdução

Este manual contém informações para instalação e gerenciamento do switch SF 2622 MR L2. Por favor, leia este manual com atenção antes de operar o produto.

Este manual é destinado a gerentes de redes familiarizados com conceitos de TI.

1.1. Especificações técnicas

Hardware	
Chipset	BCM53604
Memória DDR	128 MB
Memória Flash	8 MB
Portas RJ45 Fast Ethernet (10/100 Mbps)	24
Portas RJ45 Gigabit Ethernet (10/100/1000 Mbps)	2 portas combinadas
Slots Mini-GBIC/SFP (100/1000 Mbps)	2 portas combinadas
Portas console	1
LEDs indicativos	Alimentação
	Sys
	Link/atividade por porta
	Indicação de velocidade de conexão
Alimentação	
Entrada	100-240 Vac, 50/60 Hz
Disposição da fonte	Fonte de alimentação interna
Potência de consumo (sem link)	6 W
Potência máxima de consumo	12,3 W
Condições ambientais	
Temperatura de operação	0 °C a 45 °C
Temperatura de armazenamento	-20 °C a 70 °C
Umidade de operação	10% a 90% (sem condensação)
Umidade de armazenamento	5% a 90% (sem condensação)
Certificações	
Anatel	Equipamento homologado
Aparência	
Material	Aço
Dimensões (L × A × P)	310 × 44 × 163 mm
Instalação em rack-padrão EIA 19"	1 U de altura (acompanha suporte)
Cabeamento suportado	
10BASE-T	Cabo UTP categoria 3, 4, 5 (máximo 100 m)
	EIA/TIA-568 100Ω STP (máximo 100 m)
100BASE-TX	Cabo UTP categoria 5, 5e (máximo 100 m)
	EIA/TIA-568 100Ω STP (máximo 100 m)
1000BASE-T	Cabo UTP categoria 5e, 6 (máximo 100 m)
	EIA/TIA-568 100Ω STP (máximo 100 m)
1000BASE-FX	Fibra monomodo (SMF) e multimodo (MMF)

Principais padrões e protocolos	
Padrões IEEE	IEEE802.3, 802.3u, 802.3ab, 802.3z, 802.3x, 802.1p, 802.1q , 802.1x , 802.1d, 802.1w, 802.1s, 802.1v, 802.3ac
Padrões IETF	RFC1541, RFC1112, RFC2236, RFC2618, RFC1757, RFC1157, RFC2571, RFC2030
Outros padrões e protocolos	CSMA/CD, TCP/IP, SNMPv1/v2c, HTTP, HTTPS, SSHv1/v2
Características básicas	
Método de transmissão	Armazena e envia (Store-and-Forward)
Backplane (capacidade do switch)	8 Gbps
Tamanho da tabela de endereços MAC	8 kB
Jumbo frame	9 kB
Buffer de memória	384 kB
MTBF	100.000 horas
Taxa de encaminhamento de pacotes	6.6 Mbps
Taxa de latência	2.3 µs
Características avançadas	
Configuração de portas	Autonegociação
	MDI/MDI-X
	Controle de fluxo
	Espelhamento de portas
	Estatística de tráfego
Agregação de link	Agregação de link estática
	Agregação de link dinâmica (LACP)
	8 grupos
	8 portas por grupo
Tabela MAC	Endereço MAC estático
	Endereço MAC dinâmico
VLAN	VLAN baseada em endereço MAC
	VLAN baseada em protocolo
	VLAN baseada em tag (802.1q)
	VLAN baseada em porta
	4k VLANs ativas
	GARP/GVRP
	Voice VLAN
STP	802.1d Spanning Tree Protocol (STP)
	802.1w Rapid Spanning Tree Protocol (RSTP)
	802.1s Multiple Spanning Tree Protocol (MSTP)
	Loop Guard
	Root Guard
	BPDU Guard
	BPDU Filter

Multicast		IGMP v1/v2/v3
		Fast Leave
		Multicast VLAN
		Multicast estático
		Filtro Multicast
		Estatística IGMP
QoS		8 filas de prioridade
		8 filas de prioridade
		CoS baseado em portas
		CoS baseado em 802.1p
		CoS baseado em DSCP
		Algoritmos de escalonamento SP, WRR, WFQ, FCFS
		Storm control (Broadcast, Multicast e Unicast desconhecido)
		Controle de banda por porta
ACL (Lista de controle de acesso)		ACL nas camadas 2,3 e 4 (L2, L3 e L4)
		ACL baseada em tempo
Segurança	Segurança nas portas	Sim
	Filtro de endereço MAC	Sim
	Associação ARP	Manual e ARP Scanning
	Proteção ARP	Sim
	DoS (negação de serviço)	Sim
	Autenticação	802.1x baseado em porta
		802.1x baseado em MAC
		RADIUS
	Guest VLAN	Sim
	SSH	SSHv1/v2
	Restrição de acesso web	Baseada em IP e porta
	Isolação de porta	Sim
	Acesso de usuário	Sim
	Filtro DHCP	Sim
	Detecção de Loopback	Sim
	Criptografia de dados	Disponível para SSH, SNMPv3, SSL e senha
Gerenciamento	SNMP	SNMP v1/v2c/v3
	RMON	4 grupos
	Tipos de acesso	Web (HTTP/HTTPS)
		Telnet (CLI)
		Console (CLI)
		SSHv1/v2 (CLI)
	Atualização de firmware	Via console, web e TFTP

Manutenção	DHCP	Snooping
		Cliente DHCP
		DHCP Option 82
	SNTP	SNTP Cliente
	Monitoramento e diagnóstico	Teste virtual de cabo (VCT)
		Diagnóstico por ping
		Diagnóstico por tracer
		Sistema de log (local e remoto)
		Monitoramento de CPU
Criptografia de Dados		Não disponível
Garantia		3 anos

1.2. Visão geral do switch

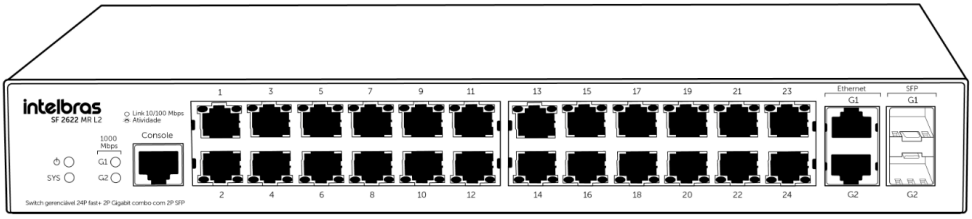
Projetado para grupos de trabalho e departamentos, o switch SF 2622 MR L2 da Intelbras possui um alto desempenho e um conjunto completo de recursos de gerenciamento de camada 2. Ele fornece uma variedade de características com elevado nível de segurança. A capacidade de configuração inteligente fornece soluções flexíveis para uma escala variável de redes.

ACL, 802.1x e Inspeção ARP fornecem uma robusta estratégia de segurança. QoS e IGMP Snooping/Filtro otimizam as aplicações de voz e vídeo. O LACP aumenta a largura de banda agregada, otimizando o transporte de dados, evitando gargalos na rede. SNMP, RMON, web/CLI/Telnet/SSH trazem uma grande variedade de políticas de gerenciamento. O SF 2622 MR L2 traz múltiplas funções com excelente desempenho e facilidade de gerenciamento, o que corresponde a total necessidade dos usuários que exigem um grande desempenho da rede.

1.3. Descrição do produto

Painel frontal

O painel frontal do SF 2622 MR L2 possui 24 portas Fast Ethernet 10/100 Mbps, 2 portas Gigabit Ethernet 10/100/1000 Mbps combinada com 2 portas Mini-GBIC/SFP 100/1000 Mbps, 1 porta console e LEDs de monitoramento.



Painel frontal

- » **Portas 10/100:** 24 portas 10/100 Mbps para conectar dispositivos com velocidade de 10 Mbps, 100 Mbps.
- » **Portas SFP:** 2 portas Mini-Gbic para conectar módulos SFP 1000 Mbps. Cada porta possui 1 LED correspondente.
- » **Porta Console:** 1 porta RJ45 para conectar com a porta serial de um computador para o gerenciamento e monitoramento do switch.

LEDs

No painel frontal são apresentados 12 LEDs de monitoramento, que seguem o comportamento a seguir:

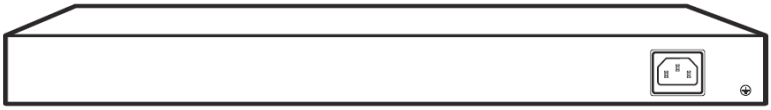
LED	Status	Indicação
Power	Aceso	Switch conectado na fonte de alimentação
	Apagado	Switch desligado ou com problema na fonte de alimentação
SYS	Aceso	Switch funcionando normalmente
	Apagado	Switch está funcionando de forma anormal

Ethernet Link/Act	Aceso amarelo	Conexão 1000 Mbps válida estabelecida, sem recepção/transmissão de dados
	Piscando amarelo	Conexão 1000 Mbps válida estabelecida, com recepção/transmissão de dados
	Aceso laranja	Conexão 10/100 Mbps válida estabelecida, sem recepção/transmissão de dados
	Piscando laranja	Conexão 10/100 Mbps válida estabelecida, com recepção/transmissão de dados
	Apagado	Nenhuma conexão válida nesta porta ou a porta está desativada
SFP Lin/ACT	Aceso amarelo	Conexão SFP 1000 Mbps válida estabelecida, sem recepção/transmissão de dados
	Piscando amarelo	Conexão SFP 1000 Mbps válida estabelecida, com recepção/transmissão de dados
	Aceso laranja	Conexão SFP 100 Mbps válida estabelecida, sem recepção/transmissão de dados
	Piscando laranja	Conexão SFP 100 Mbps válida estabelecida, com recepção/transmissão de dados
	Apagado	A porta está conectada em um dispositivo com velocidade diferente. Não há nenhuma conexão nesta porta ou a porta está desativada

Obs.: *utilizar o slot Mini-GBIC (SFP) apenas com módulos 1000 Mbps.*

Painel posterior

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



Painel posterior

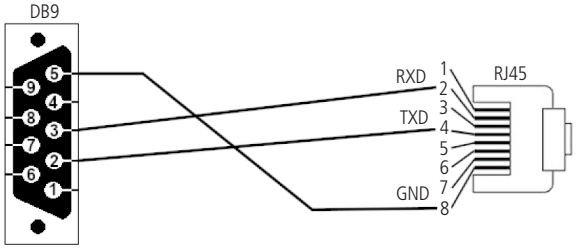
» **Terminal de aterramento:** além do mecanismo de proteção a surto elétrico que o switch possui, você pode utilizar o terminal de aterramento a fim de garantir uma maior proteção. Para informações mais detalhadas, consulte o *Guia de instalação*.

» **Conector do cabo de energia:** para ligar o switch, conecte o cabo de energia (fornecido com o switch) no conector do switch e a outra ponta em uma tomada elétrica no padrão brasileiro de 3 pinos. Após energizá-lo, verifique se o LED *PWR* está aceso, indicando que o switch está conectado à rede elétrica e pronto para ser utilizado. Para compatibilidade com os padrões elétricos mundiais, este switch é projetado para trabalhar com uma fonte de alimentação automática com variação de tensão de 100 a 240 Vac, 50/60 Hz. Certifique-se que sua rede elétrica esteja dentro desta faixa.

1.4. Porta console

O Switch possui uma porta console. A taxa de comunicação da porta varia entre 1200 bps até 115200 bps. Ela possui conexão padrão RJ45. Após conectar a porta console na porta serial do PC através do cabo console, você pode configurar e monitorar o switch rodando um software de emulação terminal, como o Putty ou o super terminal do windows. Os parâmetros de comunicação da porta serial do terminal podem ser configurados para uma taxa de 9600 bps, oito bits de dados, um bit de parada, nenhum bit de verificação de soma e controle de tráfego.

A pinagem do cabo serial segue o padrão demostrado abaixo:



Cabo console

Obs.: *a porta console não suporta controle de tráfego. Portanto, você deve definir o controle de tráfego de dados da opção como nenhum quando configurar o software terminal. Caso contrário, o problema de single-pass surgirá no terminal.*

2. Interface de configuração web (GUI)

1. Para acessar a interface de configuração, abra o navegador e na barra de endereços digite o endereço IP do switch: *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 192.168.0.x (x sendo qualquer número de 2 à 254), e máscara de rede igual a 255.255.255.0.*

2. Após digitado o endereço IP do switch no navegador, será exibido a tela de login, conforme imagem a seguir. Digite admin para o nome de usuário e senha, ambos em letras minúsculas. Leia os *TERMOS DE USO e a POLITICA DE PRIVACIDADE*, clicando nos seus respectivos links, caso concorde marque a caixa de *CONCORDO* e em seguida, clique no botão *Login* ou pressione a tecla *Enter.*

Tela de login

2.1. Ambientação

As telas apresentadas por este produto possuem algumas interações que serão explicadas a seguir:

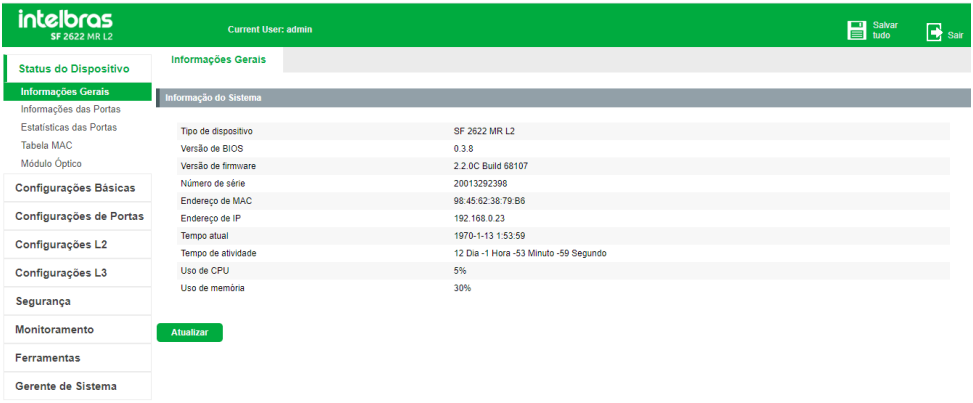
Atualizar	Atualizar: atualiza as informações da tela
Limpar	Limpar: limpa informações da tela como por exemplo as estatísticas das portas
Cancelar	Cancelar: cancela a configuração realizada na tela, funcionará caso as configurações novas ainda não tenham sido aplicadas
Aplicar	Aplicar: aplica as configurações realizadas na tela e salva no arquivo *running-config.* Essa funcionalidade não salva permanentemente as configurações, para isso deverão ser salvas as configurações
Salvar tudo	Salvar tudo: salva as configurações do *running-config* para o *startup-config.* É aconselhável realizar esse procedimento antes de colocar o switch em ambiente de produção
Novo	Novo: cria novas configurações e parâmetros nas telas disponíveis
Deletar	Deletar: deleta configurações e parâmetros criados anteriormente pelo usuário
Voltar	Voltar: volta para a tela anterior a atual
Sair	Sair: faz o logon do usuário corrente no navegador. Para isso é necessário fechar todas as guias do navegador

3. Status do dispositivo

Este menu é apenas para obter as informações básicas do dispositivo, como informações de hardware e de acesso ao gerenciamento, estado e estatísticas das portas e tabela MAC do switch.

3.1. Informações gerais

Nesta tela são exibidas as principais informações de hardware e de gerenciamento do dispositivo.



Informações gerais

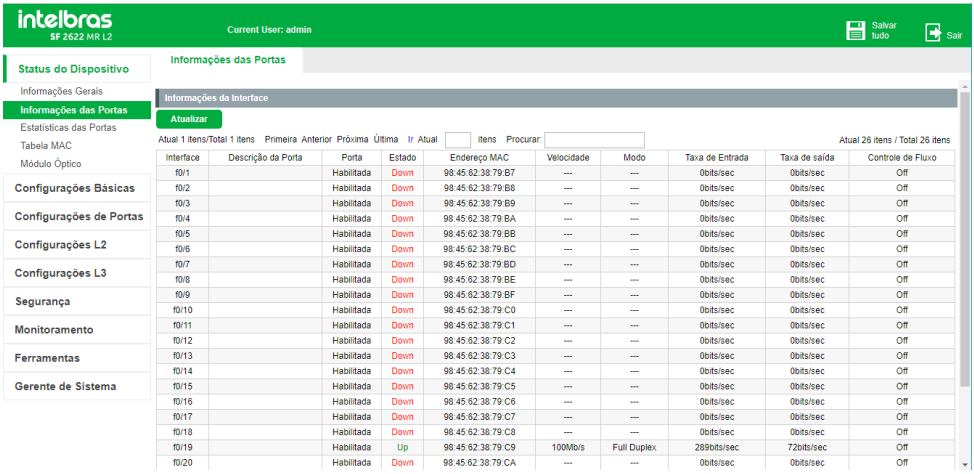
3.1.1. Informações gerais

Informações do sistema

- **Tipo do dispositivo:** exibe o modelo do switch.
- **Versão de BIOS:** exibe a versão de BIOS.
- **Versão de firmware:** exibe a versão de firmware.
- **Número de série:** exibe o número de série do produto.
- **Endereço MAC:** exibe o endereço MAC do switch.
- **Endereço IP:** exibe o endereço IP da interface VLAN acessada.
- **Tempo atual:** exibe a data e hora atual de acordo com a configuração realizada.
- **Tempo de atividade:** exibe o em que o switch esteve em atividade.
- **Uso de CPU:** exibe a quantidade de processamento.
- **Uso de memória:** exibe a quantidade de memória em uso.

3.2. Informações das portas

Nesta tela são exibidas as informações das interfaces físicas (portas) do dispositivo.



Informações das portas

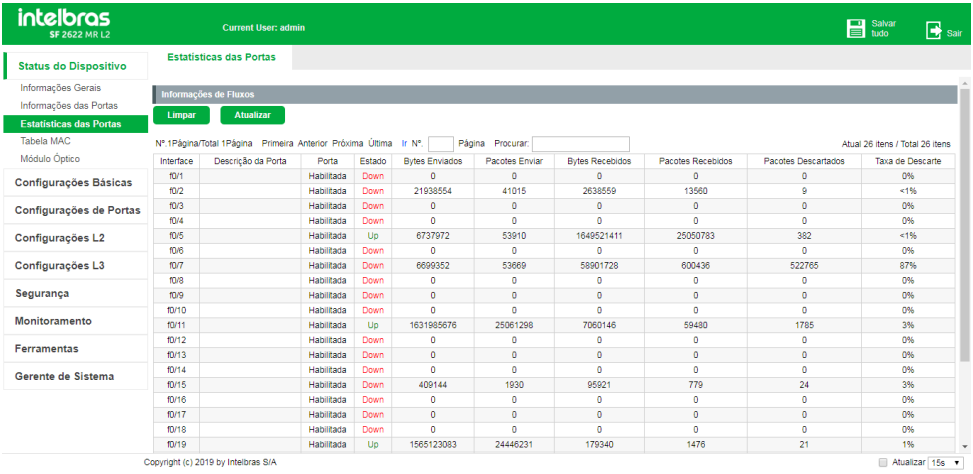
3.2.1. Informações das portas

Informações das interfaces

- **Interface:** indica a porta de referência.
- **Descrição da porta:** exibe a descrição configurada para a porta.
- **Porta:** exibe o estado configurado da porta.
- **Estado:** exibe o estado operacional da porta.
- **Endereço MAC:** exibe o endereço MAC vinculado a porta.
- **Velocidade:** exibe a velocidade operacional da porta.
- **Modo:** exibe o modo *Duplex* operacional da porta.
- **Taxa de entrada:** exibe o tráfego de ingresso da porta em bits por segundo (bps).
- **Taxa de saída:** exibe o tráfego de egresso da porta em bits por segundo (bps).
- **Controle de fluxo:** exibe a configuração de controle de fluxo da porta.

3.3. Estatísticas das portas

Nesta tela são exibidas as estatísticas de tráfego das portas do switch.



Estatísticas das portas

3.3.1. Estatísticas das portas

Informações de fluxos

- **Interface:** porta de referência.
- **Descrição da porta:** descrição configurada para a porta.
- **Porta:** estado configurado da porta.
- **Estado:** estado operacional da porta.
- **Bytes enviados:** exibe a quantidade de bytes enviados pela porta.
- **Pacotes enviados:** exibe a quantidade de pacotes enviados.
- **Bytes recebidos:** exibe a quantidade de bytes recebidos pela porta.
- **Pacotes recebidos:** exibe a quantidade de pacotes recebidos.
- **Pacotes descartados:** exibe a quantidade de pacotes descartados.
- **Taxa de destarte:** exibe o percentual de pacotes descartados em relação ao total de pacotes recebidos.

3.4. Tabela MAC

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, número da porta e VLAN, 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 endereço de origem e destino, diminuindo o tráfego em broadcast. Os endereços MAC podem ser adicionados na tabela de forma manual ou aprendidos automaticamente.

Existem recursos de filtragem de endereços MAC, permitindo que o switch filtre pacotes indesejados, proibindo seu encaminhamento e melhorando a segurança da rede.

Os tipos de endereços MAC são mostrados na tabela a seguir.

Tipo	Modo de configuração	Possui tempo de envelhecimento	Mantém-se após desligar o switch	Restrições de aprendizado
Estático	Manual	Não	Sim	Não é possível aprender o endereço na mesma VLAN em diferentes portas.
Dinâmico	Automático	Sim	Não	
Filtrado	Manual	Não	Sim	O aprendizado é apenas por VLAN, ou seja, possui efeito em todas as interfaces.

Tipos de endereço MAC

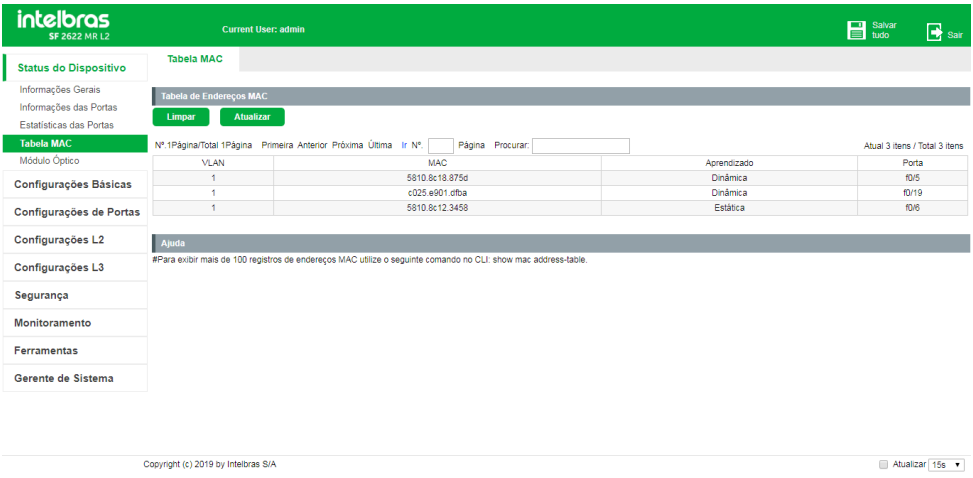


Tabela MAC

3.4.1. Tabela MAC

Tabela de endereços MAC

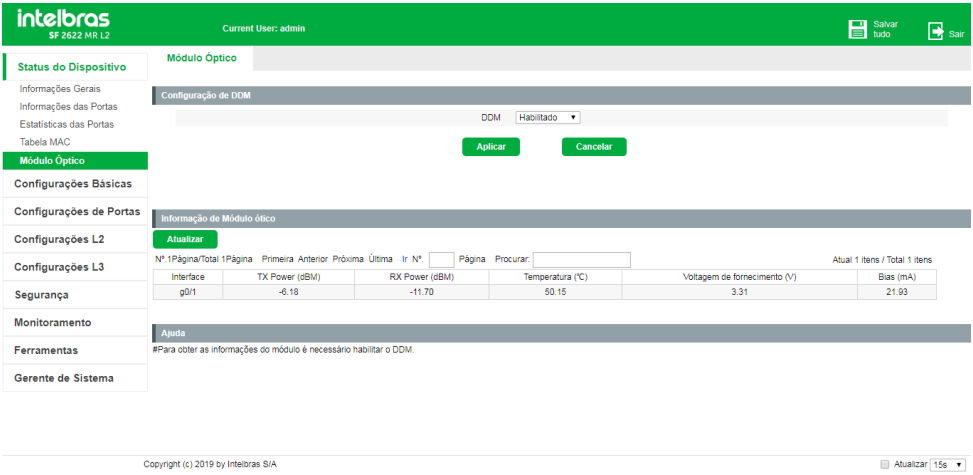
- **VLAN:** VLAN em que se encontra o endereço MAC.
- **MAC:** endereço MAC de referência no formato hexadecimal *H.H.H.*
- **Aprendizado:** tipo do endereço MAC.
- **Porta:** porta em que se encontra o endereço MAC.

3.5. Módulo óptico

O módulo óptico, ou módulo Gbic (*Gigabit interface converter*), é um transceiver óptico utilizado em switches que tem como função transformar o sinal elétrico em sinal óptico, e vice-versa, possibilitando a tecnologia de transmissão em fibra ótica.

3.5.1. Módulo óptico

Nesta tela são exibidas as informações dos módulos ópticos conectados no switch.



Módulo óptico

Configuração de DDM

O Monitoramento de Diagnóstico Digital (DDM) provê informações referentes ao módulo óptico conectado ao switch.

» **DDM:** para habilitar e desabilitar a obtenção de informações dos módulos óticos selecione *Habilitar/Desabilitar,* respectivamente.

Informação de módulo óptico

Esta seção é uma tabela que contém as informações de todos os módulos ópticos que suportam o DDM.

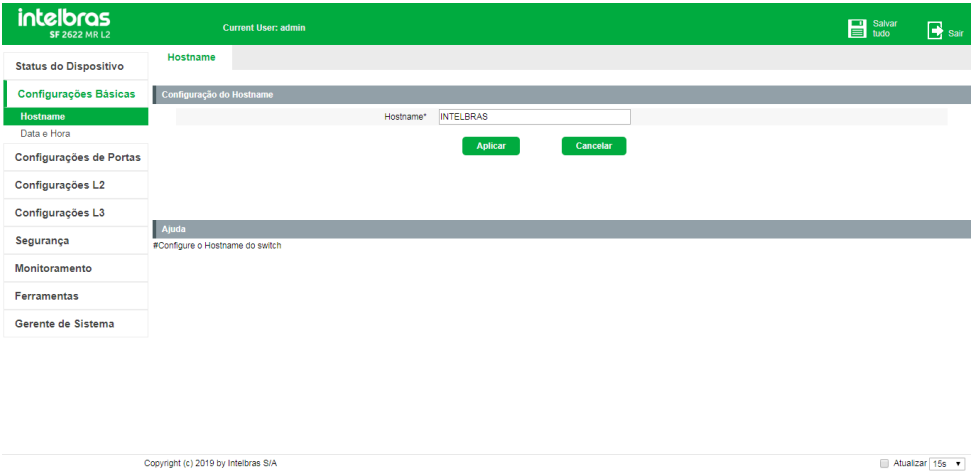
» **Interface:** porta em que o módulo óptico esta conectado.
» **TX Power (dbm):** potência de transmissão do módulo.
» **RX Power (dbm):** potência recebida no módulo.
» **Temperatura (°C):** temperatura no módulo.
» **Voltagem de fornecimento (V):** tensão de entrada no módulo.
» **Bias (mA):** corrente de entrada no módulo.

4. Configurações básicas

As configurações básicas do switch são configurações que não influenciam a operação do switch, apenas ajustam certos parâmetros à preferência do usuário.

4.1. Hostname

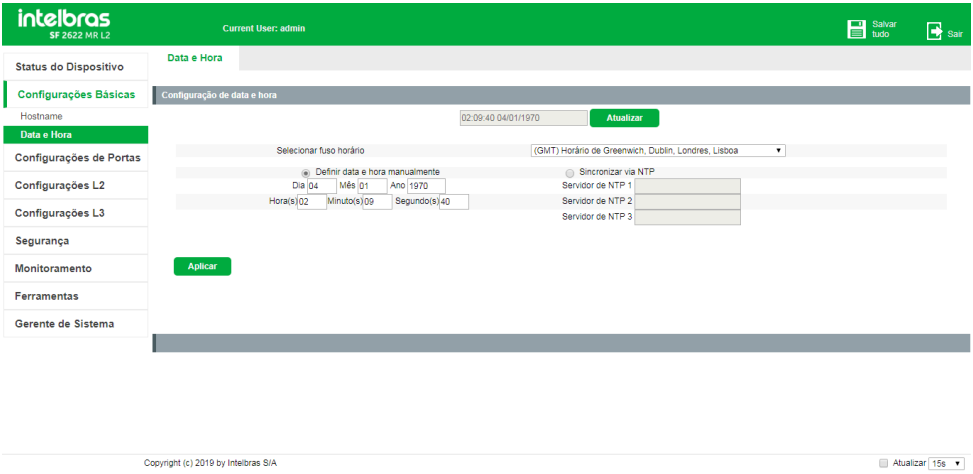
Nessa página você pode configurar o nome do switch (hostname).



Hostname

4.2. Data e hora

Nessa página você pode configurar a data e hora do sistema, pode ser feito manualmente ou através do protocolo NTP.



Data e hora

4.2.1. Data e hora

Configuração de data e hora

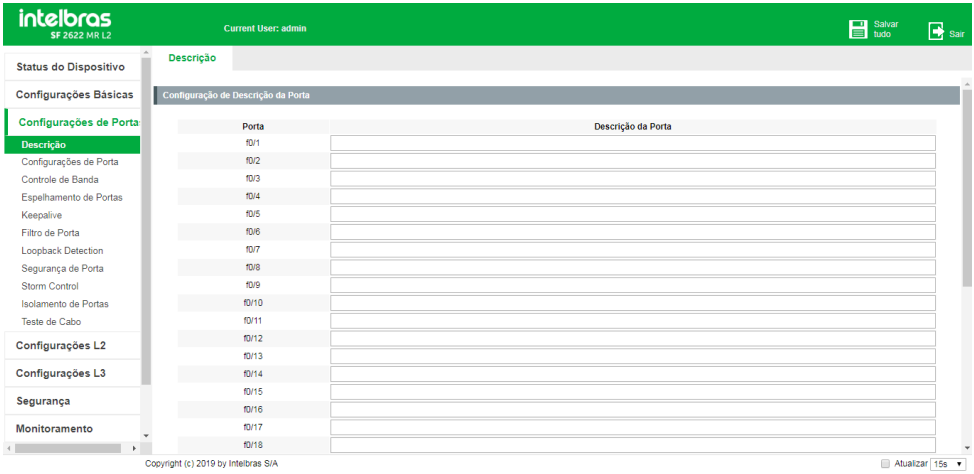
- **Definir data e hora manualmente:** selecione a opção *Definir data e hora manualmente*, selecione o fuso horário local, especifique a data e hora e clique em *Aplicar.*
- **Definir data e hora através de um servidor NTP:** selecione a opção *Sincronizar via NTP* e especifique o endereço IP de até três servidores NTP nos campos *Servidor NTP*.

5. Configurações de portas

Neste menu são realizadas as configurações respectivas as interfaces L2 (portas) do switch. As configurações realizadas são controle de banda, espelhamento de portas, detecção de loop, isolamentos de portas entre outros.

5.1. Descrição

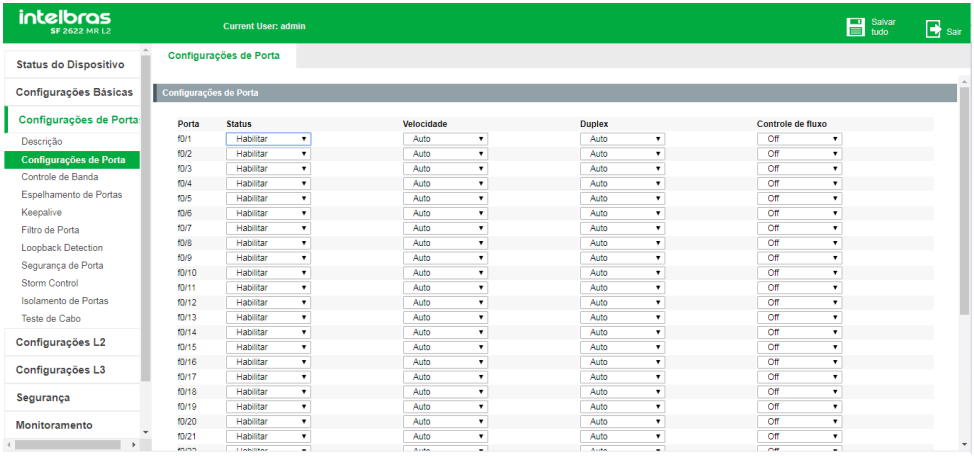
Nesta tela são configuradas as informações de descrição para as portas.



Descrição

5.2. Configurações de porta

Nesta página são configurados os parâmetros básicos para as portas, quando a porta está desativada todos os pacotes serão descartados. Defina os parâmetros conforme sua necessidade.



Configurações de porta

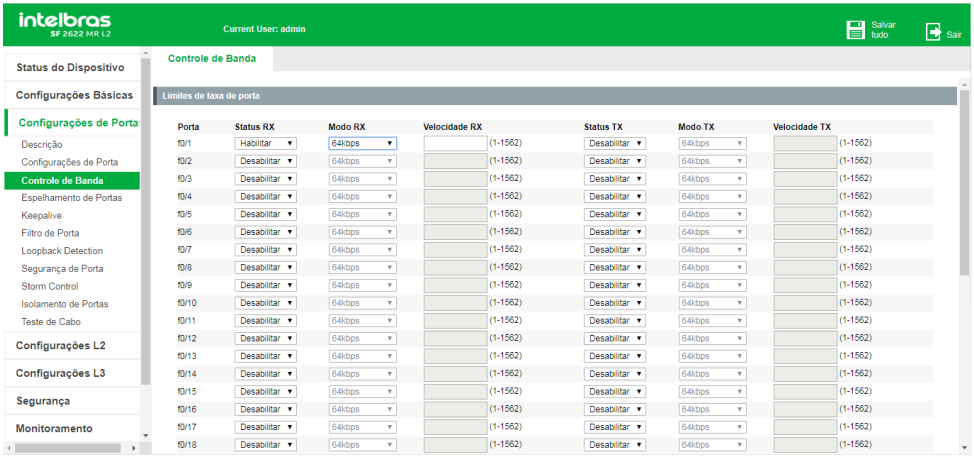
5.2.1. Configurações de porta

Configuração de porta

- » **Status:** quando a porta estiver habilitada o switch poderá encaminhar os pacotes normalmente.
- » **Velocidade/Duplex:** o dispositivo conectado ao switch deve estar na mesma velocidade e modo *Duplex*. Quando o modo *Auto* for selecionado o modo *Duplex* será determinado pela autonegociação.
- » **Controle de fluxo:** quando o controle de fluxo é ativado, o switch pode sincronizar a transmissão de dados, evitando a perda de pacotes causada por congestionamentos na rede.

5.3. Controle de banda

A tela de Controle de banda permite que seja configurado a largura de banda e o fluxo de transmissão de cada porta.



Controle de banda

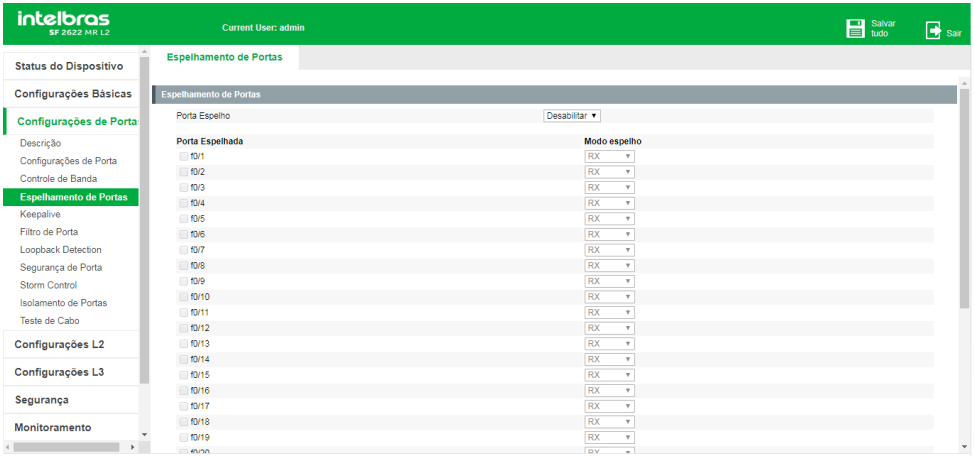
5.3.1. Controle de banda

Limites de taxa de porta

- » **Status RX:** quando o status da porta estiver desabilitado o switch irá receber os pacotes até a velocidade em que a porta foi negociada.
- » **Modo *RX*:** pode ser configurado em unidades de 64 kbps ou em porcentagem. Se for escolhido *64 kbps* a configuração de controle de banda deve ser realizada de forma granular, com valores múltiplos 64 kpbs. Se for escolhido *Porcentagem* o valor configurado deve ser um entre 1 e 100% da rede.
- » **Velocidade RX:** selecione a largura de banda para recebimento de pacotes na porta.
- » **Status TX:** quando o status da porta estiver desabilitado o switch irá transmitir os pacotes na velocidade que a porta foi negociada.
- » **Modo *TX*:** pode ser configurado como *64 kbps* ou *Porcentagem*. Se for escolhido *64 kbps* a configuração de controle de banda deve ser realizada de forma granular, com valores múltiplos 64 kpbs. Se for escolhido *Porcentagem* o valor configurado deve ser um entre 1 e 100% da rede.
- » **Velocidade TX:** selecione a largura de banda para envio de pacotes na porta.

5.4. Espelhamento de 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.



Espelhamento de portas

5.4.1. Espelhamento de portas

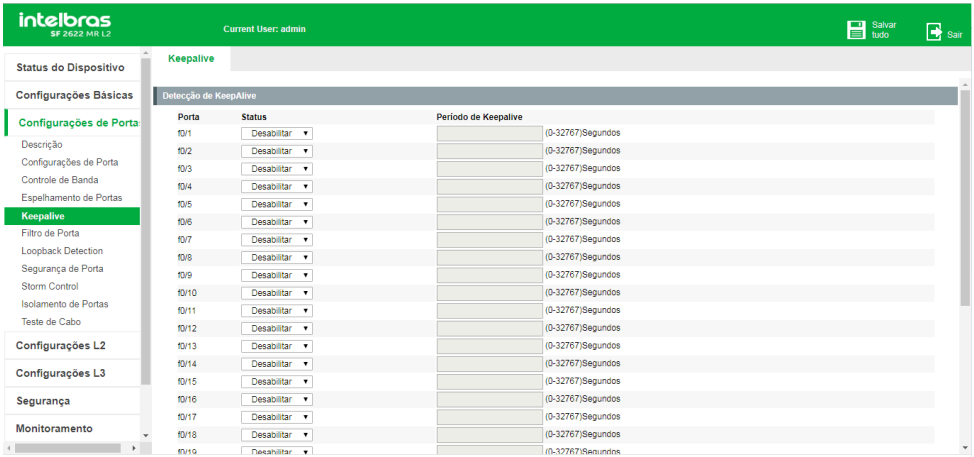
Espelhamento de portas

É possível configurar uma porta espelho de cada vez.

- » **Porta Espelho:** porta que irá receber o fluxo de pacotes das portas espelhadas.
- » **Porta Espelhada:** devem ser selecionadas as portas que terão o fluxo de dados encaminhados para a porta espelho.
- » **Modo *Espelho*:** modo de configuração para a função *Espelho*. A função pode ser configurada como espelhamento do tráfego de *RX, TX* ou *RX & TX*.

5.5. Keepalive

Nesta tela é possível configurar, habilitar/desabilitar o intervalo de tempo para a verificação do link entre as portas e o equipamento conectado.



Keepalive

5.5.1. Keepalive

Detecção de keepalive

» **Porta:** indicação da porta para configuração.

» **Status:** selecione *Habilitar/Desabilitar* para habilitar ou desabilitar a verificação *Keepalive* na porta selecionada.

» **Período de Keepalive:** configuração do período de tempo em segundos para a verificação *Keepalive*. O valor padrão é *12 segundos*.

5.6. Filtro de porta

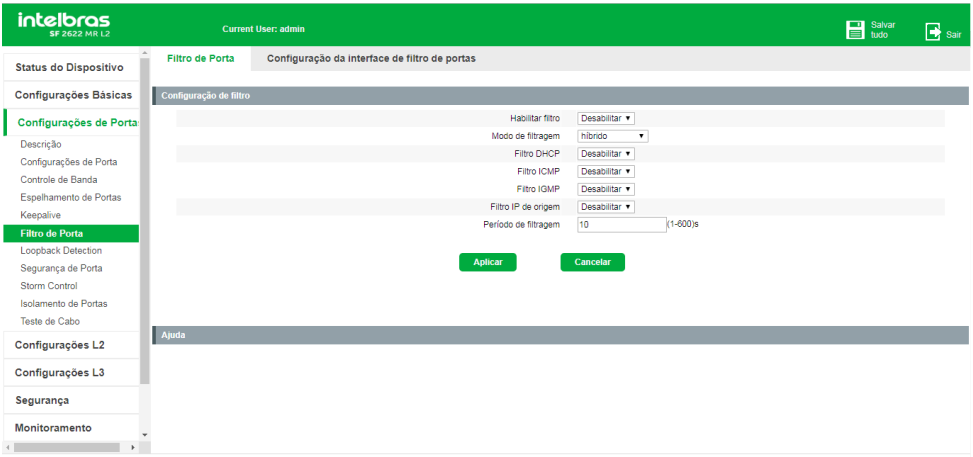
O filtro de porta analisa fluxos de dados e contabiliza a quantidade de pacotes recebidos com origem e tipo iguais, se a quantidade exceder o limite configurado o switch irá tomar o fluxo por um ataque e irá realizar uma ação de bloqueio de acordo com o modo do filtro configurado. Existem dois modos de configuração do filtro de porta:

» **Modo *Simples*:** no modo *Simples*, após um fluxo ser considerado como ataque o switch irá bloquear todos os fluxos com a mesma origem até que o tempo de bloqueio acabe e então comece uma nova contagem.

» **Modo *Avançado* (híbrido):** no modo *Avançado*, após um fluxo ser considerado como ataque o switch irá bloquear este único fluxo durante o tempo de bloqueio do modo *Avançado* e iniciará uma nova contagem de pacotes, se a contagem exceder o limite novamente o fluxo continuará bloqueado, caso contrário o bloqueio será retirado.

Para os fluxos de camada 2 como o ARP a origem é a combinação do endereço MAC de origem e a porta de ingresso de fluxo, já para fluxos de camada 3 como o IGMP e IP a origem é a combinação do endereço IP de origem e da porta de ingresso.

Nesta tela serão configurados quais os tipos de fluxos de pacotes serão analisados pela função e filtrados ou não pelo equipamento.



Filtro de porta

5.6.1. Filtro de porta

Configuração de filtro

Nesta seção são feitas as configurações globais do filtro de porta.

» **Habilitar filtro:** selecione *Habilitar/Desabilitar* para habilitar ou desabilitar o filtro de portas globalmente. Após esta configuração é necessário aplicar o filtro correspondente na porta desejada.

» **Modo de filtragem:** selecione *Sem alteração/Híbrido* para um modo de filtragem simples (*Sem alteração*) ou avançado (*Híbrido*).

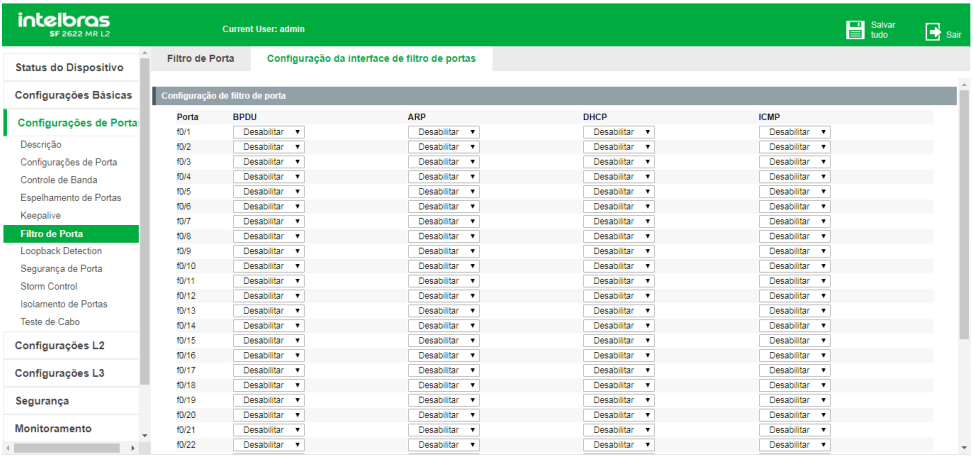
» **Filtro DHCP:** selecione *Habilitar/Desabilitar* para habilitar ou desabilitar a verificação de pacotes DHCP. Após esta configuração é necessário aplicar o filtro correspondente na porta desejada.

» **Filtro ICMP:** selecione *Habilitar/Desabilitar* para habilitar ou desabilitar a verificação de pacotes ICMP. Após esta configuração é necessário aplicar o filtro correspondente na porta desejada.

» **Filtro ICMPv6:** selecione *Habilitar/Desabilitar* para habilitar ou desabilitar a verificação de pacotes ICMPv6. Após esta configuração é necessário aplicar o filtro correspondente na porta desejada.

» **Filtro IGMP:** selecione *Habilitar/Desabilitar* para habilitar ou desabilitar a verificação de pacotes IGMP.
» **Filtro IP de origem:** selecione *Habilitar/Desabilitar* para habilitar ou desabilitar a verificação do IP de origem. Após esta configuração é necessário aplicar o filtro correspondente na porta desejada.
» **Período de filtragem:** configure o período de contagem de pacotes.

5.6.2. Configuração da interface de filtro de portas



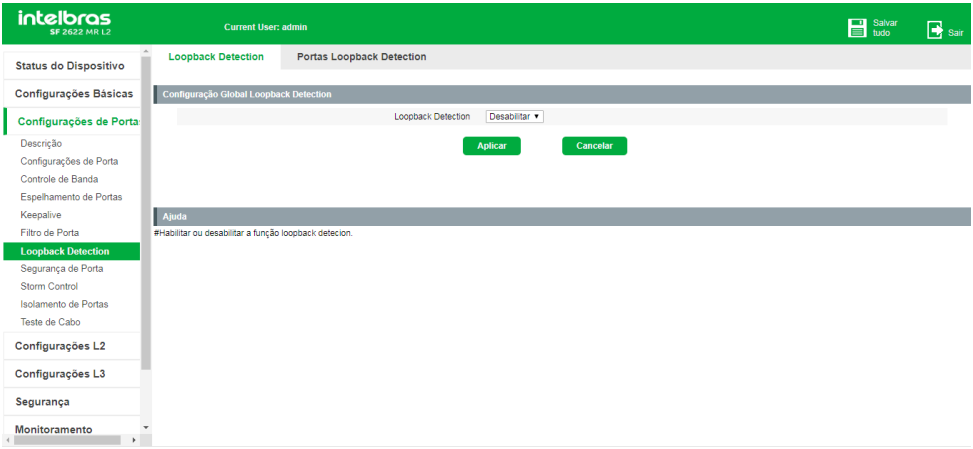
Configuração da interface de filtro de portas

Configuração de filtro de porta

» **Porta:** indicação da porta para configuração.
» **BPDU:** selecione *Habilitar/Desabilitar* para habilitar ou desabilitar o filtro de pacotes BPDU na porta selecionada.
» **ARP:** selecione *Habilitar/Desabilitar* para habilitar ou desabilitar o filtro de pacotes ARP na porta selecionada.
» **DHCP:** selecione *Habilitar/Desabilitar* para habilitar ou desabilitar o filtro de pacotes DHCP na porta selecionada.
» **ICMP:** selecione *Habilitar/Desabilitar* para habilitar ou desabilitar o filtro de pacotes ICMP na porta selecionada.

5.7. Loopback detection

Com o recurso *Loopback detection* habilitado, o switch pode detectar a ocorrência de looping em suas portas enviando pacotes de detecção e verificando se o pacote enviado foi recebido na mesma porta. Esta função auxilia na prevenção de problemas de loop na rede.



Loopback detection

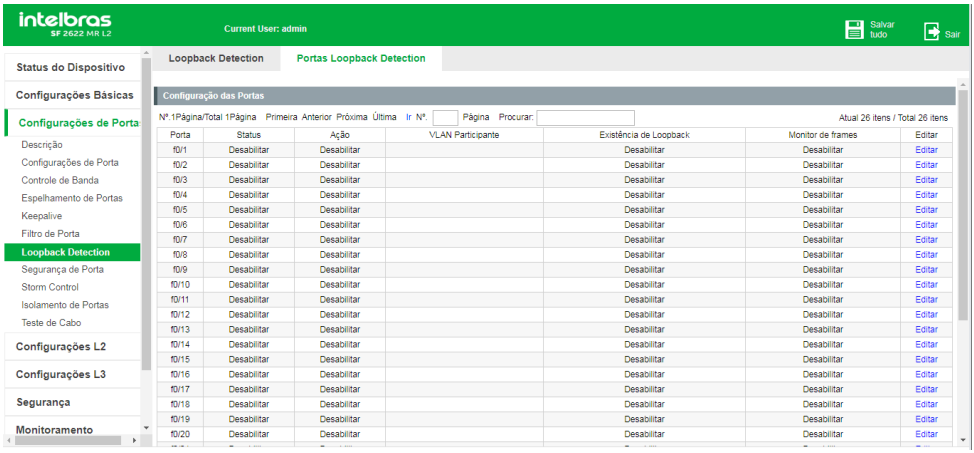
5.7.1. Loopback detection

Configuração global loopback detection

» **Loopback Detection:** selecione *Habilitar/Desabilitar* para habilitar ou desabilitar o Loopback Detection globalmente. Após este passo é necessário configurar na porta desejada a ação para a função de detecção de loop.

5.7.2. Portas loopback detection

Nesta tela são feitas as configurações loopback detection das interfaces.



Portas loopback detection

Configuração das portas

» **Porta:** indicação da porta para configuração.

» **Status:** indica o status da configuração do Loopback Detection na porta correspondente.

» **Ação:** indica o tipo de ação que será realizada na porta caso seja detectada a presença de loop.

» **VLAN participante:** indica a VLAN que será ativada a detecção de loopback.

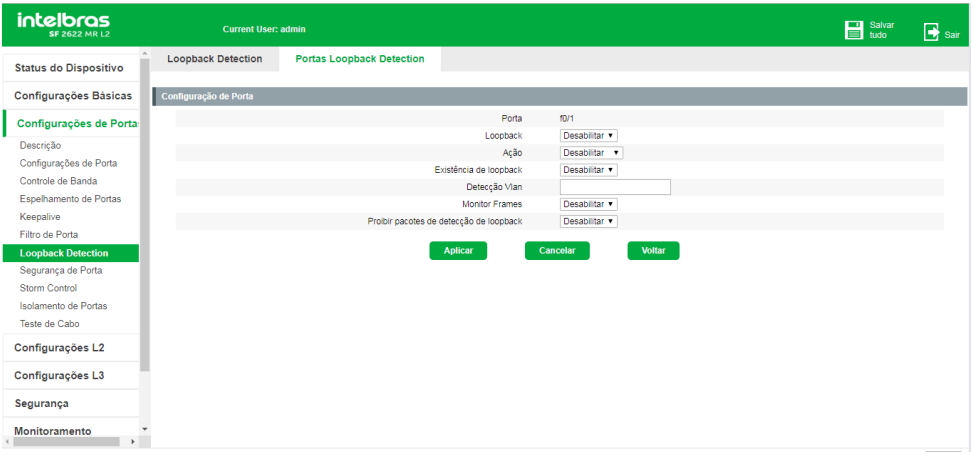
Obs.: *para configurar mais de uma VLAN na porta faça a configuração da seguinte maneira* 1,3,5,7 *ou* 1,3-5,7 *ou ainda* 1-7.

» **Existência de loopback:** indica se a porta foi configurada manualmente com a presença de loop ou não.

» **Monitor de frames:** indica se o switch realizará a contagem do número de pacotes de loop antes de considerar que a porta está em loop ou não.

» **Editar:** botão que irá abrir a tela de *Configuração de porta* onde devem ser realizadas as configurações de *Loopback Detection* na porta correspondente.

A tela a seguir mostra os parâmetros para configuração de *Loopback detection* na porta *Gigabit Ethernet 1*. Para configurar em outra porta clique em *Editar* na porta correspondente.



Portas loopback detection - configuração de porta

Configuração de porta

- **Porta:** indicação da porta para configuração.
- **Loopback:** selecione *Habilitar/Desabilitar* para habilitar ou desabilitar a função *Loopback Detection* na porta selecionada.
- **Ação:** selecione B*loquear/Aprendendo/Desligar* para configurar uma ação na porta depois de detectar o loop.
  - Para que a porta seja bloqueada, selecione *Bloquear.*
  - Para que a porta não aprenda os endereços MAC, selecione *Aprendendo.*
  - Para desligar a porta, selecione *Desligar.*
- **Existência de loopback:** selecione *Habilitar/Desabilitar* para habilitar ou desabilitar manualmente a existência de loop na porta. Ao habilitar a existência de loop na porta, a mesma será considerada com loop, independente se houver ou não loop estabelecido.
- **VLAN participante:** configure quais VLANs participarão da detecção de loop.
- **Monitor frames:** selecione *Habilitar/Desabilitar* para habilitar ou desabilitar o contador de pacotes de Loopback detection.
- **Proibir pacotes de detecção de loopback:** selecione *Habilitar/Desabilitar* para habilitar ou desabilitar a porta a enviar ou encaminhar pacotes para detecção de loop. Esta função e a função *Loopback* não podem estar habilitadas ao mesmo tempo na mesma porta. Por padrão, se uma estiver habilitada a outra necessariamente deverá estar desabilitada.

5.8. Segurança de portas

Neste menu são configuradas limitações de entradas de MAC possibilitando uma segurança em nível de enlace. O switch realiza a segurança de portas através vínculos IP-MAC, entradas estáticas de MAC, limitação de MACs dinâmicos e configuração de MAC Sticky.

Obs.: *o MAC Sticky é configurável apenas na Interface de linha de comando (CLI).*

5.8.1. Vinculação de IP MAC

Com a configuração de vínculos IP-MAC o switch filtra pacotes que não correspondem a lista de vínculos configurados da porta, ou seja, o switch irá descartar pacotes com IP e MAC de origem que não combinem com nenhum dos vínculos criados na porta.

Tela de vinculação de IP MAC

Vinculação de porta de IP MAC

- **Nome da interface:** identificação da porta.
- **Detalhe:** clique em *Detalhe* para abrir a seção *Informações sobre a regra de vinculação de IP MAC* e criar, visualizar ou modificar as configurações da porta.

Vínculo de IP MAC - informação sobre as regras de vinculação

Informações sobre a regra de vinculação de IP MAC

- **Novo|Editar:** abre a seção *Criar|Modificar Endereço IP MAC* para configuração de um vínculo IP-MAC.
- **Número de série:** identifica a regra de vinculação.
- **Endereço de IP:** informa o endereço IP vinculado.
- **Endereço de MAC:** informa o endereço MAC vinculado.

Vinculação de IP MAC - modificar endereço IP MAC

Modificar endereço IP MAC

- **Insira um novo endereço IP:** insira um endereço IP que será vinculado.
- **Insira um novo MAC:** insira um endereço MAC que será vinculado. Formato hexadecimal *HHHH.HHHH.HHHH* ou *HHHHHHHHHHHH*.

5.8.2. Modo de segurança estática

Com o modo de segurança estática o switch irá filtrar pacotes que com endereço MAC de origem de acordo com lista configurada de entradas estáticas de MAC, ou seja, o switch irá permitir ou descartar pacotes que combinem com a lista configurada de acordo com o modo de filtragem.

Modo de segurança estática

Configurações de modo Estático

- **Nome da interface:** especifica a interface.
- **Modo de porta:** informa o modo da porta. Apenas portas em modo *Acesso* podem participar de configurações de segurança estática.
- **Modo de filtragem:**
  - **Desabilitar:** desabilita a função.
  - **Aceitar:** permite o tráfego de pacotes com endereço MAC que combinem com a lista da porta de ingresso.
  - **Rejeitar:** bloqueia o tráfego de pacotes com endereço MAC que combinem com a lista da porta de ingresso.

Obs.: *na tela* Entrada estática de MAC *é possível configurar as regras estáticas.*

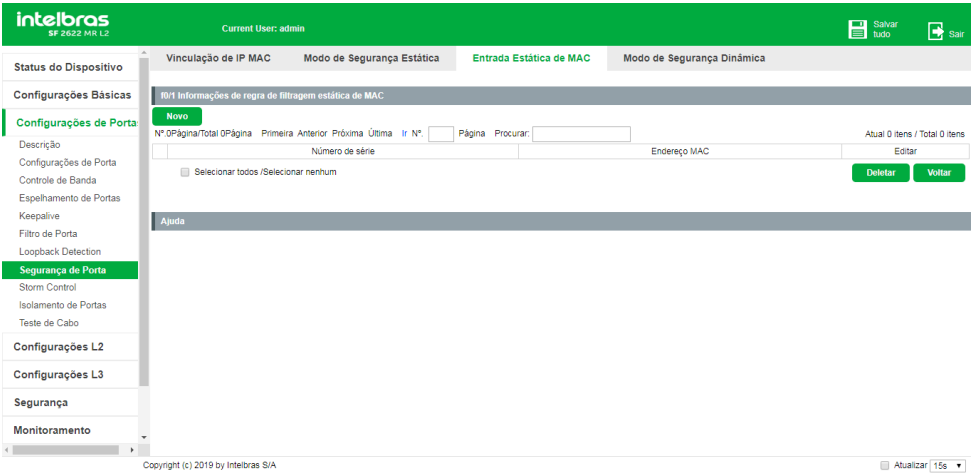
5.8.3. Entrada estática de MAC

Nesta tela é configurada a lista de MACs de cada porta do switch.

Entrada estática de MAC

Configurar filtragem estática de MAC

- » **Nome da interface:** identificação da porta.
- » **Detalhe:** abre a seção *Filtragem estática de MAC* para criar, visualizar ou modificar as configurações da porta.



Entrada estática de MAC - filtragem estática de MAC

Informações de regra de filtragem

- » **Nome de série:** identificação da regra estática.
- » **Endereço MAC:** informa o endereço MAC da configurado.
- » **Novo|Editar:** abre a seção *Endereço MAC* para configuração de uma entrada estática de MAC.

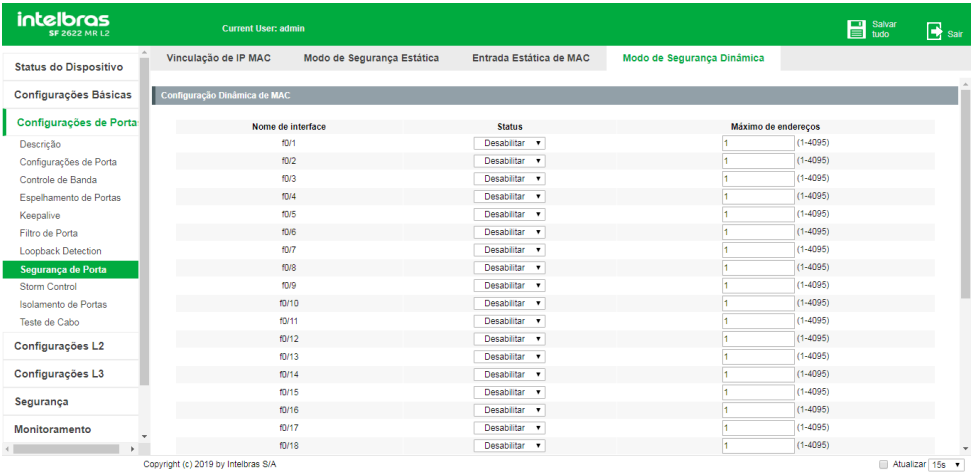
Entrada estática de MAC - endereço MAC

Endereço MAC

» **Endereço MAC estático:** insira um endereço MAC. Formato hexadecimal *HHHH.HHHH.HHHH* ou *HHHHHHHHHHHH*.

5.8.4. Modo de segurança dinâmica

Com o modo de segurança dinâmica o switch irá limitar a quantidade máxima de endereços MAC aprendidos por porta limitando a quantidade de dispositivos que trafegam por porta.



Modo de segurança dinâmica

Configuração dinâmica de MAC

» **Nome da Interface:** indica a interface.

» **Status:** clique em *Habilitar/Desabilitar* para habilitar ou desabilitar a limitação do aprendizado de endereços MAC.

» **Máximo de endereços:** digite o número máximo de endereços MAC que podem ser aprendidos.

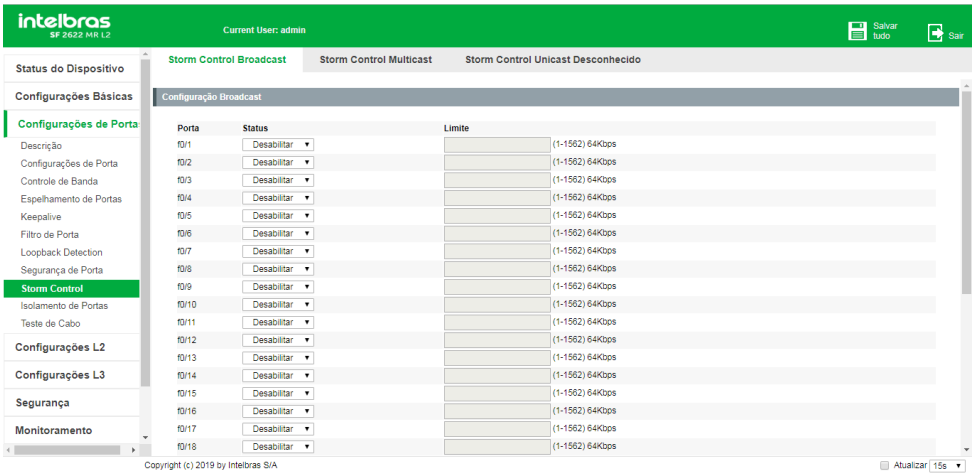
5.9. Storm control

A função *Storm control* permite que o switch filtre por porta os pacotes do tipo *Broadcast, Multicast* e *Unicast* desconhecido. 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.

A função *Storm control* permite que o switch filtre por porta os pacotes do tipo *Broadcast, Multicast* e *Unicast* desconhecido. Se a taxa de transmissão de algum dos três tipos de pacotes excederem a largura de banda configurada, os pacotes serão rejeitados automaticamente.

5.9.1. Storm control broadcast

Nesta tela é feita a configuração para limitação de banda de tráfego broadcast.



Storm control broadcast

Configuração broadcast

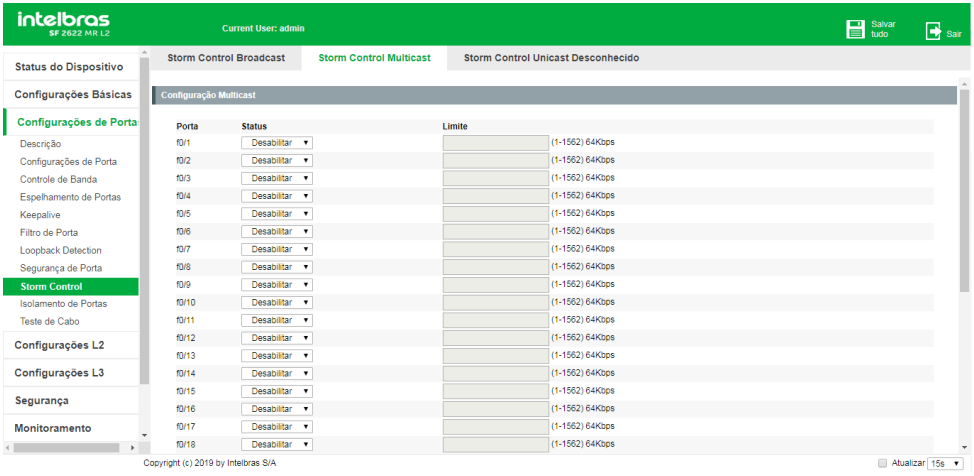
» **Porta:** exibe o número da porta do switch.

» **Status:** selecione *Habilitar/Desabilitar* para habilitar ou desabilitar o *Storm control broadcast* na porta correspondente.

» **Limite:** informe o limite permitido em unidades de 64 Kbps (1-16384).

5.9.2. Storm control multicast

Nesta tela é feita a configuração para limitação de banda de tráfego multicast.



Storm control multicast

Configuração multicast

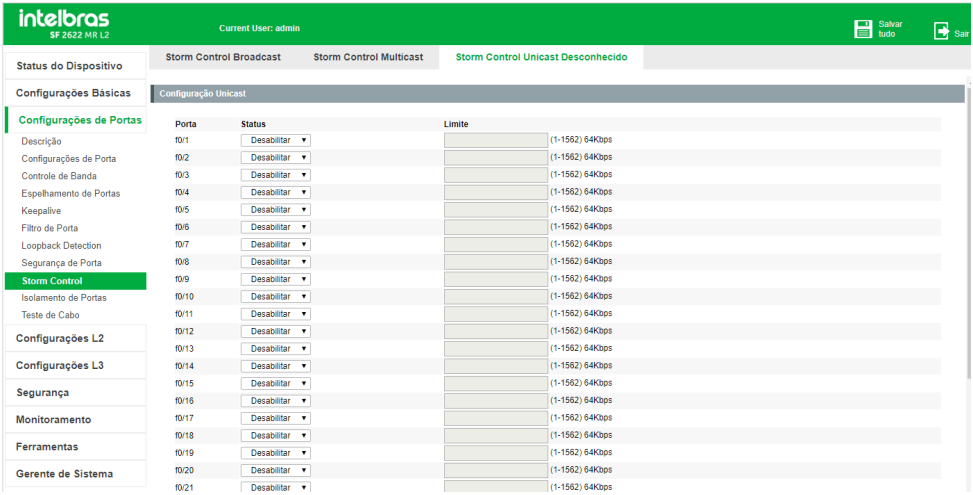
» **Porta:** exibe o número da porta do switch.

» **Status:** selecione *Habilitar/Desabilitar* para habilitar ou desabilitar o *Storm control multicast* na porta correspondente.

» **Limite:** informe o limite permitido em unidades de 64 Kbps (1-16384).

5.9.3. Storm control unicast desconhecido

Nesta tela é feita a configuração para limitação de banda de tráfego multicast.



Tela Storm control unicast desconhecido

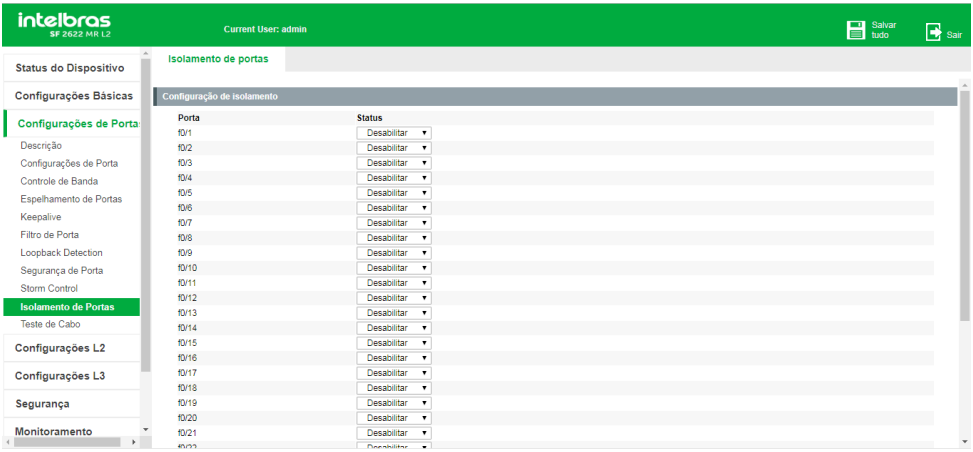
Configuração unicast

- » **Porta:** exibe o número da porta do switch.
- » **Status:** selecione *Habilitar/Desabilitar* para habilitar ou desabilitar o Storm control de unicast desconhecido na porta correspondente.
- » **Limite:** informe o limite permitido em Kbps (1-16384).

5.10. Isolamento de portas

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

Se a porta estiver com o status de configuração do isolamento de portas habilitado, ela não poderá se comunicar com outra porta que também esteja configurada com o isolamento de portas habilitado. Mas poderá se comunicar com todas as portas que estiverem com o isolamento de portas desabilitado.



Grupos de isolamento

5.10.1. Isolamento de portas

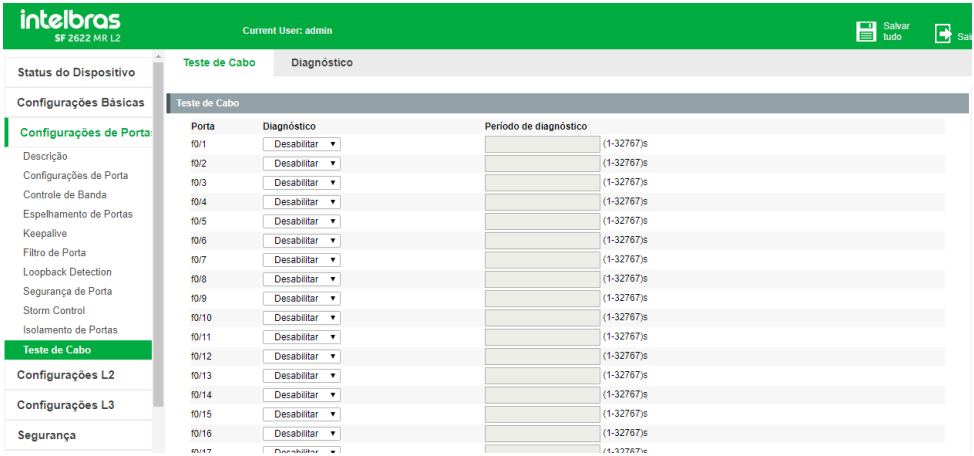
Lista de grupos de isolamento

» **Porta:** indicação da porta para configuração.

» **Status:** selecione *Habilitar/Desabilitar* para habilitar ou desabilitar a função *Isolamento de portas* na porta selecionada.

5.11. Teste de cabo

Este switch oferece as funções teste de cabo para averiguação de problemas físicos nos links.



Teste de cabo

5.11.1. Teste de cabo

Teste de cabo

» **Porta:** identifica a interface.

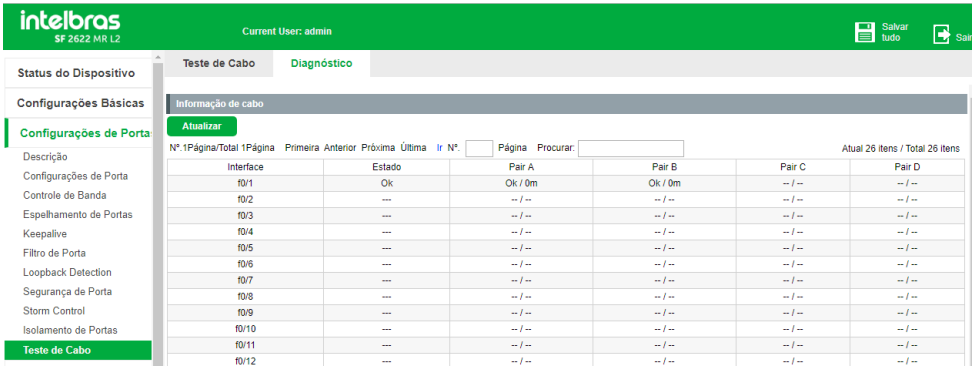
» **Diagnóstico:** clique em *Habilitar/Desabilitar* para habilitar ou desabilitar o diagnóstico da porta.

» **Período de diagnóstico:** escolha o período que o diagnóstico irá diagnosticar a porta. A porta pode ficar indisponível durante o diagnóstico.

Obs.: *o campo* Diagnóstico *não exibe o status da configuração e sim apenas seleciona uma ação a ser aplicada. Após habilitar o diagnóstico e aplicar as configurações, o diagnóstico voltará para a opção* Desabilitar. *É necessário ir para tela* Diagnóstico *para verificar o resultado obtido no teste.*

5.11.2. Diagnóstico

Na seguinte tela é possível conferir o resultado do diagnóstico.



Diagnóstico

Informação de cabo

- **Interface:** identifica a interface.
- **Estado:** informa o estado obtido no diagnóstico.
  - **Open:** cabo não conectado ou avariado (circuito aberto).
  - **Ok:** porta conectada e funcional.
- **Pair X:** informa o status e comprimento do par X.
- **Open/comprimento:** informa que o par está desconectado ou partido e a distância do par.
  - **Ok/comprimento:** informa que o par está funcional e a distância do par.

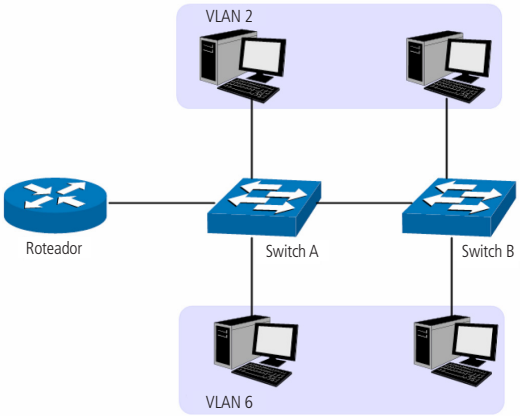
6. Configurações L2

Este menu é para as configurações das funções relativas aos padrões que operam na camada 2 do modelo OSI, como o STP e VLAN, e também algumas funções de controle de padrões de camadas mais elevadas como as funções de snooping do ICMP e MLD.

6.1. VLAN

VLAN (*Virtual Local Area Network*) é uma técnica 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 e otimizando a performance do switch, além facilitar o gerenciamento e segurança da rede. Para haver comunicação entre computadores em VLANs diferentes é necessária a utilização de roteadores ou switch L3 para o encaminhamento dos pacotes. A figura a seguir ilustra uma implementação de VLAN.



Implementação de VLAN

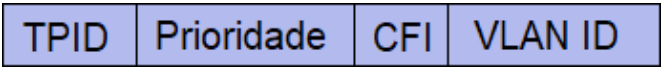
Principais vantagens na utilização de VLAN:

1. As transmissões em broadcast estão restritas a cada VLAN. Isso diminui a utilização de banda e melhora o desempenho da rede;
2. 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.

6.1.1. 802.1q VLAN

O padrão 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 os quatro campos que o padrão adiciona ao frame Ethernet: *TPID (Identificador do Protocolo)*, *Prioridade, CFI (Indicador do Formato Canônico)* e *VLAN ID*.



Tag de VLAN

- **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*.
- **Prioridade:** 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*. Esta informação é utilizada no método de acesso ao meio roteado por FDDI/Token-Ring sinalizando a ordem do endereço encapsulado no quadro.
- **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. Quando o switch recebe um pacote que não possui tag de VLAN, o switch irá encapsular o quadro com a tag de VLAN da porta de ingresso.

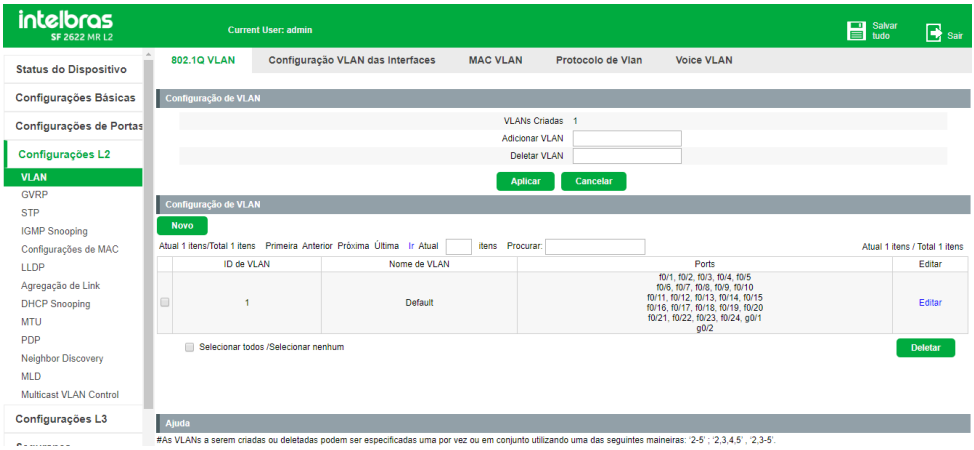
A configuração do 802.1q VLAN pode ser feita de duas maneiras:

- **Configuração em massa:**

1. Defina as VLANs conhecidas pelo switch na seção C*riação de VLAN da* tela a seguir;
2. Vá para a tela adjacente *Configuração VLAN das interfaces* e realize as configurações 802.1q VLAN das interfaces.

- **Configuração individual:**

1. Vá para a seção *Configuração de VLAN* e crie ou edite uma VLAN definindo seu nome e modo de egresso nas interfaces;
2. Vá para a tela adjacente *Configuração VLAN das interfaces* e realize as configurações restantes de 802.1q VLAN das interfaces.



802.1q VLAN

Criação de VLAN

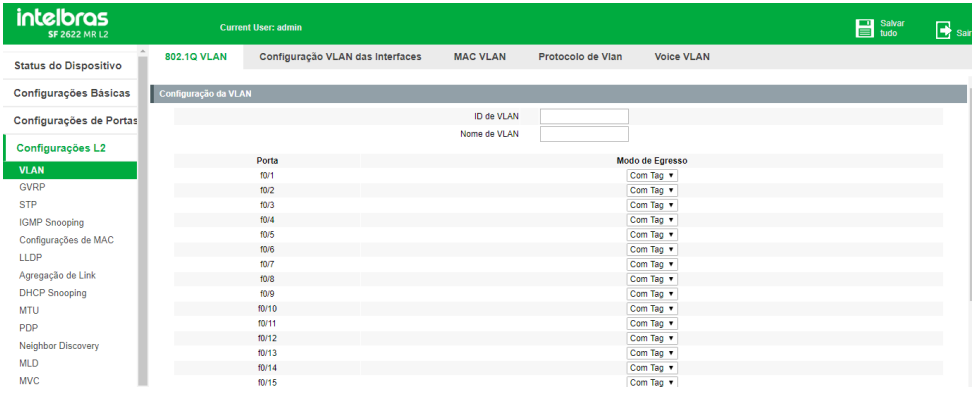
Esta seção é para adicionar e remover um intervalo de VLANs da lista de VLANs conhecidas do switch. Os campos dessa seção são explicados a seguir:

- » **VLANs criadas:** exibe as VLANs conhecidas pelo switch, estas podem ser criadas manualmente ou automaticamente pelo GVRP.
- » **Adicionar VLAN:** especifica VLANs a serem adicionadas na lista de VLANs conhecidas.
- » **Deletar VLAN:** especifica VLANs a serem removidas da lista de VLANs conhecidas.

Configuração de VLAN

Nesta seção é mostrada uma lista com as VLANs conhecidas pelo switch e suas informações de identificador e de nome.

- » **Novo|Editar:** abre a tela de *Configuração da VLAN* para configuração de uma única VLAN.



Configuração da VLAN

Configuração da VLAN

- » **ID de VLAN:** identificador da VLAN que está sendo configurada.
- » **Nome de VLAN:** nome descritivo que será atribuído à VLAN.
- » **Modo de egresso:** configura o modo de egresso de uma porta para a VLAN atual em específico. Esta configuração possui efeito apenas para portas no modo *Tronco*, para portas no modo acesso o modo de egresso é sempre sem a marcação VLAN.

6.1.2. Configuração VLAN das interfaces

As portas do switch podem operar em dois modos VLAN diferentes, a seguir a descrição de cada um dos modos:

» **Acesso:** a porta em modo *Acesso* permite apenas uma única VLAN e o tráfego de egresso da porta é sem a marcação VLAN.

» **Tronco:** a porta em modo *Tronco* pode permitir várias VLANs e ter um modo de egresso diferente configurado para cada VLAN. A regra de saída padrão é com a marcação VLAN.

Obs.: *quando a porta estiver em modo tronco e forem adicionados VLAN IDs ao campo VLANs Desmarcadas, veja na figura a baixo, a porta se comportará em modo híbrido, ou seja, as VLANs permitidas irão ser taggeadas normalmente, e as VLANs Desmarcadas passaram sem Tag.*

Quando o switch recebe um pacote sem marcação VLAN, ele irá adicionar uma tag de VLAN no pacote de acordo com o identificador VLAN da porta (PVID). O PVID possui a seguinte finalidade:

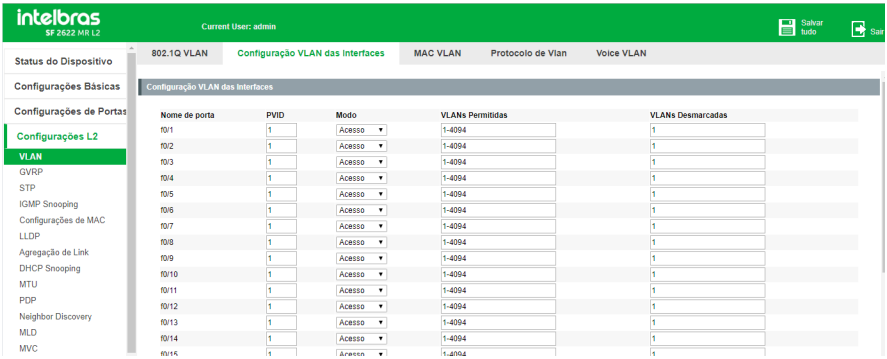
» Manipular os quadros sem marcação VLAN.

» Determinar o domínio de broadcast de portas no modo *Acesso*, ou seja, quando o switch recebe um pacote broadcast ele encaminhará apenas para as portas com o PVID igual ao VLAN ID do pacote.

Para configurar 802.1q VLAN nas interfaces siga os seguintes passos:

1. Especifique o modo *VLAN* da interface;
2. Especifique o PVID da porta;
3. Especifique as VLANs permitidas. Esta configuração define quais são as VLANs permitidas pela interface, ou a quais VLANs essa interface pertence, fazendo com que a porta receba ou não tráfego de determinadas VLANs;
4. Especifique as VLANs que terão seu trafego de egresso desmarcado.

Obs.: *os itens 3 e 4 tem efeito apenas para portas no modo* Tronco.



Configuração VLAN das interfaces

6.1.3. MAC VLAN

MAC VLAN é a maneira de classificar as VLANs de acordo com o endereço MAC dos dispositivos, ou seja, com esta função é possível adicionar um dispositivo a uma VLAN através do seu endereço MAC.

Os pacotes do MAC VLAN são processados da seguinte maneira:

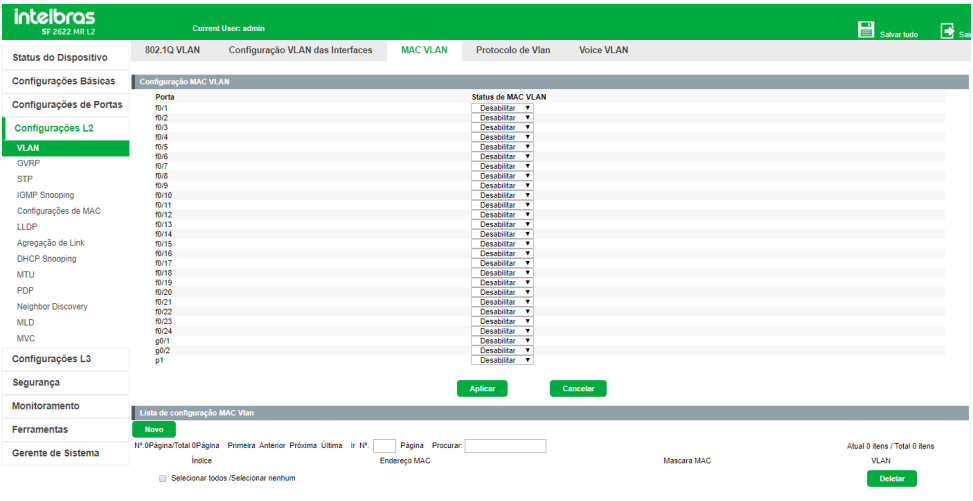
» Ao receber um pacote sem tag, o switch verifica se o endereço MAC do pacote possui uma entrada correspondente nas configurações de MAC VLAN. Se o endereço MAC corresponder, o switch adicionará a tag de VLAN no pacote de acordo com o VLAN ID do MAC VLAN configurado. Se o endereço MAC não corresponder, o switch adicionará a tag de VLAN no pacote de acordo com o PVID configurado para a porta. Assim o pacote será atribuído automaticamente para a VLAN correspondente.

» Ao receber um pacote com tag, o switch irá processá-lo de acordo com as configurações 802.1q VLAN.

» Ao criar um MAC VLAN é necessário habilitar a porta para ser membro da VLAN 802.1q correspondente, de modo a garantir que os pacotes sejam encaminhados normalmente.

Para configurar o MAC VLAN siga os seguintes passos:

1. Configure o 802.1q VLAN;
2. Habilite a função na porta desejada na seção *Configuração MAC VLAN* da tela a seguir;
3. Crie as entradas de mapeamento MAC-VLAN na seção *Lista de MAC VLAN* da tela a seguir.



MAC VLAN

Configuração MAC VLAN

» **Status de MAC VLAN:** habilita ou desabilita o MAC VLAN na porta.

Lista de MAC VLAN

Nesta seção é mostrada uma lista com as entradas de mapeamento MAC-VLAN configuradas.

» **Novo:** abre a tela *Lista MAC VLAN* para configuração de um novo mapeamento MAC-VLAN.

Lista MAC VLAN

Lista MAC VLAN

Nesta seção são feitas as entradas de mapeamento MAC-VLAN.

» **Endereço MAC:** endereço MAC de 48 bits no formato hexadecimal *H.H.H*.

» **Máscara MAC:** a máscara MAC define qual porção do endereço MAC será fixa e qual porção poderá variar. Esta é definida no mesmo formato do endereço MAC.

» **VLAN:** VLAN que será atribuída ao endereço MAC especificado.

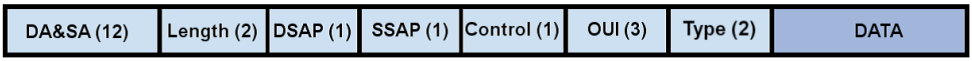
6.1.4. Protocolo VLAN

VLAN baseada em protocolo é a maneira de classificar as VLANs de acordo com o protocolo de rede utilizado, entre eles o IP, ARP, IPX 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.

Existem três formatos de encapsulamento dos dados Ethernet que carregam o identificador do protocolo de rede (Tipo Ethernet), o encapsulamento Ethernet II, o encapsulamento 802.3 LLC e o encapsulamento 802.3 LLC SNAP.

Encapsulamento Ethernet II

Encapsulamento 802.3 LLC



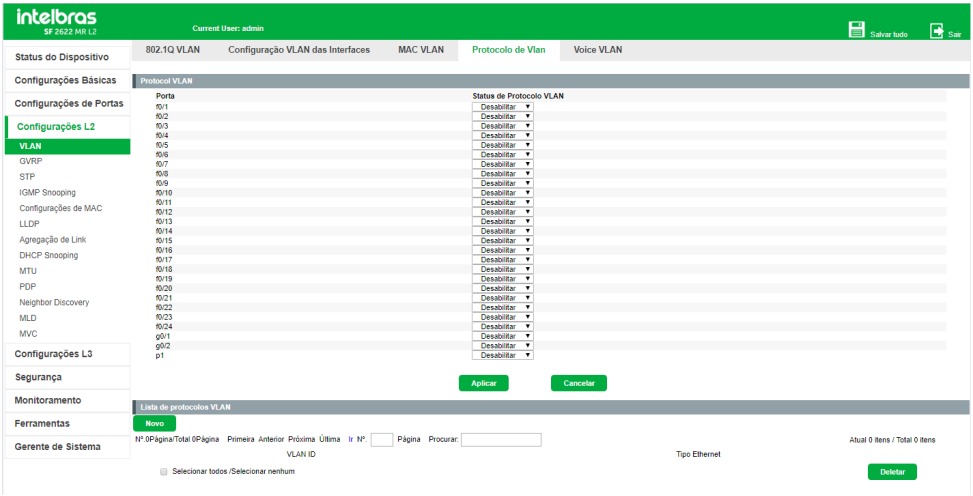
Encapsulamento 802.3 LLC SNAP

No encapsulamento Ethernet II e no 802.3 SNAP o campo *Type* permite valores entre 0x0600 e 0xFFF (1536 a 4095) e identifica o protocolo de rede utilizado, já no encapsulamento 802.3 LLC os campos utilizados são o *DSAP* e o *SSAP*.

Obs.: *o switch verifica apenas o campo* Type *presente nos encapsulamentos Ethernet II e 802.3 SNAP.*

Para configurar o protocolo VLAN siga os seguintes passos:

1. Configure o 802.1q VLAN;
2. Defina os fluxos que serão mapeados para determinadas VLAN em *Lista de protocolos VLAN*;
3. Configure o vínculo entre os tipos criados no item *2* e as portas e VLANs desejadas na seção *Status de protocolo VLAN*.



Protocolo VLAN

Lista de protocolos VLAN

Nesta seção é mostrada uma lista com as entradas de tipos de fluxos.

» **Novo:** abre a tela *Protocolo VLAN* para configuração de um novo tipo de fluxo.

Protocolo VLAN – adicionar protocolo VLAN

Adicionar protocolo VLAN

Nesta tela são feitas as entradas de tipos de fluxo Ethernet.

» **VLAN ID:** VLAN que será usada para pacotes que tenham esse vínculo.

» **Tipo Ethernet:** identificador do protocolo de rede no formato hexadecimal *0xH*.

6.1.5. Voice VLAN

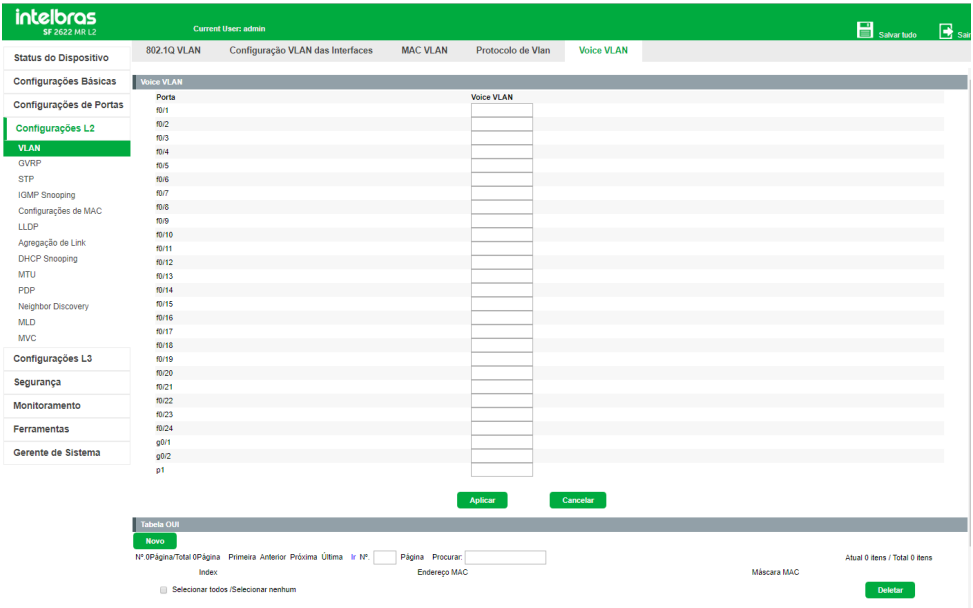
Voice VLANs são configuradas especialmente para o fluxo de voz. Ao configurar uma Voice VLAN e adicionar as portas a dispositivos de voz, você pode executar QoS garantindo a prioridade de transmissão dos fluxos de voz.

O switch pode determinar se um pacote é ou não de voz, marcando seu endereço MAC de origem. Se a origem do endereço MAC corresponde a algum Identificador Único Organizacional (OUI) configurado no sistema, os pacotes serão determinados como pacotes de voz e serão transmitidos na VLAN de voz.

Obs.: *é preciso que a porta esteja no modo* Tronco *para a Voice VLAN poder operar.*

Para configurar a Voice VLAN siga os seguintes passos:

1. Crie entradas na tabela OUI na seção *Tabela OUI;*
2. Configure a Voice VLAN da interface na seção *Voice VLAN*.



Voice VLAN

Voice VLAN

Nesta seção é configurada a Voice VLAN das interfaces.

» **Voice VLAN:** identificador da Voice VLAN.

Tabela OUI

Nesta seção esta uma lista com todas as entradas configuradas da *Tabela OUI*.

» **Novo:** abre a seção *Adicionar tabela OUI* para configuração de uma nova entrada.

Voice VLAN – adicionar tabela OUI

Adicionar tabela OUI

» **Endereço MAC:** endereço MAC de origem do dispositivo de voz.

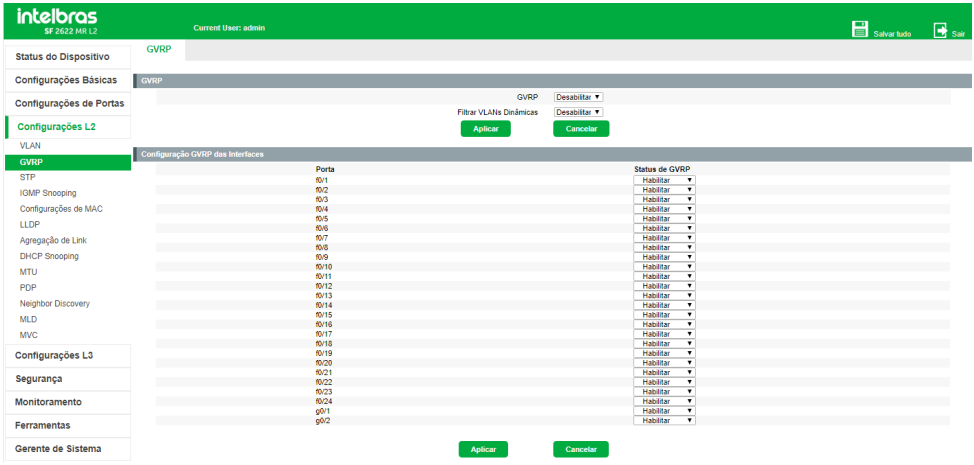
» **Máscara MAC:** especifica qual parte do endereço MAC será fixa e qual parte poderá variar.

6.2. GVRP

GVRP (*GARP VLAN Registration Protocol*) é uma implementação GARP (*Generic Attribute Registration Protocol*). O protocolo GVRP permite que o switch adicione ou remova VLANs automaticamente através de informações dinâmicas de registro de VLANs, propagando as informações de registro da VLAN local para outros switches, sem a necessidade de configurar individualmente as VLANs em cada switch.

Para configurar o GVRP no switch siga os seguintes passos:

1. Habilite o GRVP globalmente na seção *GVRP* da tela a seguir;
2. (Opcional) - na seção *GVRP* da tela a seguir habilite a filtragem de VLANs dinâmicas para que as mesmas tenham efeito apenas para as interfaces com o GRVP ativo;
3. Na seção *Configuração GVRP das interfaces* da tela a seguir habilite o GVRP nas interfaces desejadas para que as mesmas possam enviar e receber pacotes GVRP.



GVRP

6.2.1. GVRP

GPRV

Nesta seção são feitas as configurações globais de GVRP.

- **GVRP:** habilita ou desabilita o GVRP globalmente.
- **Filtra VLANs dinâmicas:** habilita ou desabilita o filtro de VLANs dinâmicas.

Configuração GVRP das interfaces

Nesta seção é feita a configuração GVRP das interfaces.

- **Status de GVRP:** habilita ou desabilita o GVRP na interface.

6.3. STP

O switch suporta os três principais padrões de *Spanning Tree*, os mesmos são apresentados a seguir junto com uma breve revisão dos principais parâmetros.

STP

STP (*Spanning Tree Protocol*), pertence ao padrão IEEE802.1d 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. BPDU (*Bridge Protocol Data Unit*) é o quadro de mensagem trocado entre os switches que utilizam a função *STP.*

- **Elementos STP**
  - **Bridge ID:** indica valor da prioridade e endereço MAC do switch. O switch que possuir o menor Bridge ID terá maior prioridade.
  - **Bridge root (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 bridge possui maior prioridade. O switch com a maior prioridade possui maior chance de ser escolhido como Bridge Root.
  - **Porta 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.
- **Temporizadores STP**
  - **Hello time:** especifica o intervalo de envio de pacotes BPDU. O valor pode variar de 1 à 10 segundos.
  - **Max age:** especifica o tempo máximo que o switch aguarda para remover sua configuração e iniciar uma nova eleição da Bridge Root. O valor pode variar de 6 à 40 segundos.
  - **Forward delay:** especifica o tempo para a porta alterar seu estado após uma alteração na topologia da rede. O valor pode variar de 4 à 30 segundos.

RSTP

O RSTP (IEEE802.1w) é uma evolução do 802.1d padrão. A terminologia de STP do 802.1w permanece essencialmente igual à terminologia de STP do IEEE802.1d. 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.

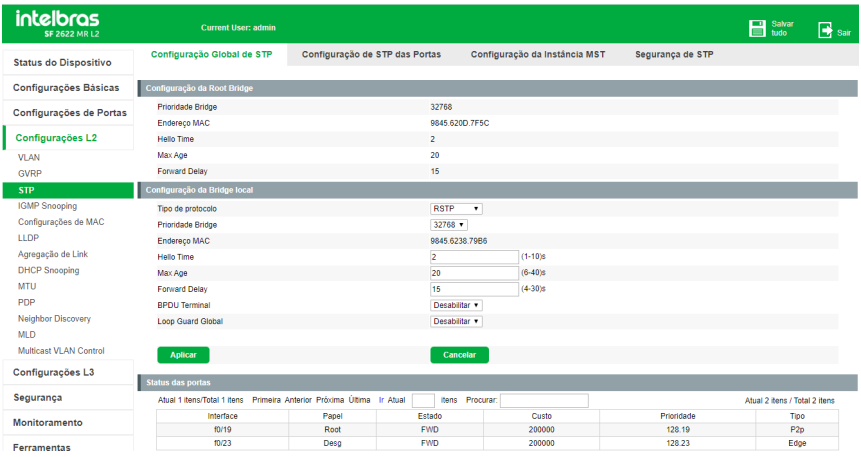
- **Elementos RSTP**
  - **Porta edge:** indica que a porta do switch está conectada diretamente aos terminais.
  - **Link P2P:** indica que a porta do switch está conectada diretamente a outro switch.
  - **Loop Fast:** com o RSTP habilitado, a função *Loop fast* faz com que as portas passem diretamente para o estado *Encaminhando* aumentando a velocidade de convergência da Spanning Tree.

MSTP

MSTP (*Multiple Spanning Tree Protocol*), referente à norma IEEE802.1s, 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.

- **Funcionamento 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.
- **Estado das portas**
  - **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**
  - **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.

6.3.1. Configuração global de STP



Configuração global de STP

Configuração de root bridge

exibe as informações do root switch da rede.

Configuração de bridge local

configure os parâmetros globais do STP do switch.

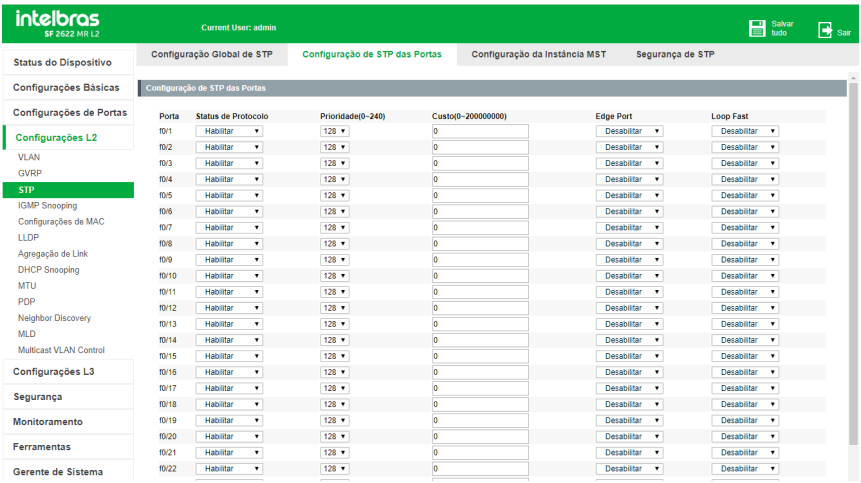
- » **BPDU Terminal:** a função *BPDU terminal* fará com que o switch não encaminhe BPDUS se o STP não estiver ativo.
- » **Loop Guard Global:** a função de *Loop guard* será ativada em todas as interfaces.
- » **Saltos máximo:** é a quantidade de saltos que um pacote BPDU pode realizar.
- » **Mst-compátivel:** habilita ou desabilita compatibilidade com versões mais antigas (RSTP e STP).

Obs.: *quando MSTP é habilitado, o campo* Prioridade *não é mais exibido e os campos* Saltos máximo *e* mst-compatível *são habilitados para configuração.*

Status das portas

Exibe as informações e status do STP das portas que estão ativas.

6.3.2. Configuração de STP das portas

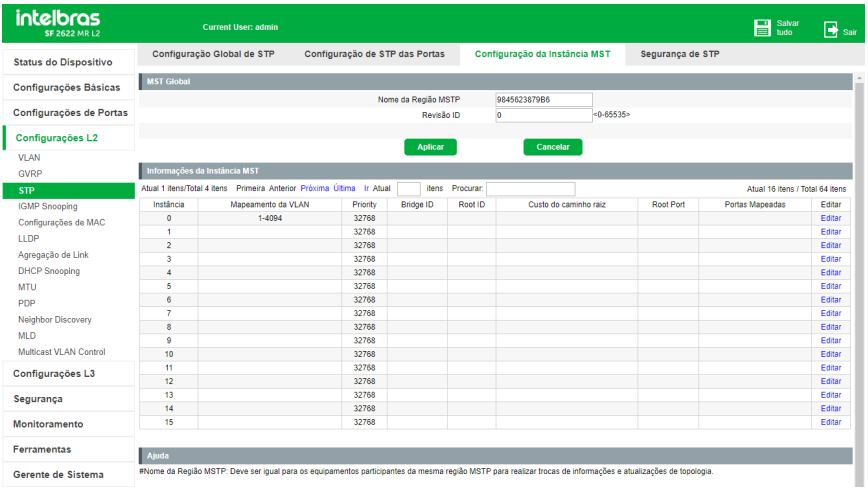


Configuração de STP das portas

Configuração de STP das portas

Configure os parâmetros STP por porta.

6.3.3. Configuração da instância MSTP



Configuração da instância MST

MSTP global

Configure os parâmetros globais do MST. Quando o switch tem o mesmo nível de revisão e conjunto de atributos, então pertence a mesma região, do contrário, estarão em regiões diferentes.

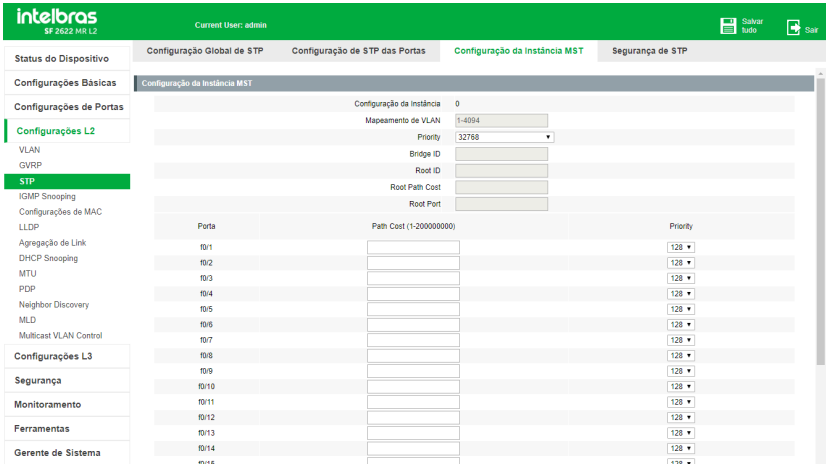
A BPDU do MST contém atributos de configuração de tal maneira que os switches que recebem essas BPDU podem compará-las contra a configuração MST local. Se os atributos coincidem a instancia MST será compartilhada como parte de uma mesma região, do contrário o switch é visto como parte de outra região.

Informações da instância MST

Exibe e permite a edição dos parâmetros MSTP por instância.

A instância 0 é a CIST. Quando uma VLAN é associada a uma outra instância, automaticamente ela será removida da CIST.

» **Editar:** abre a seção *Configuração da instância MST* que permite configurar os parâmetros da instância.

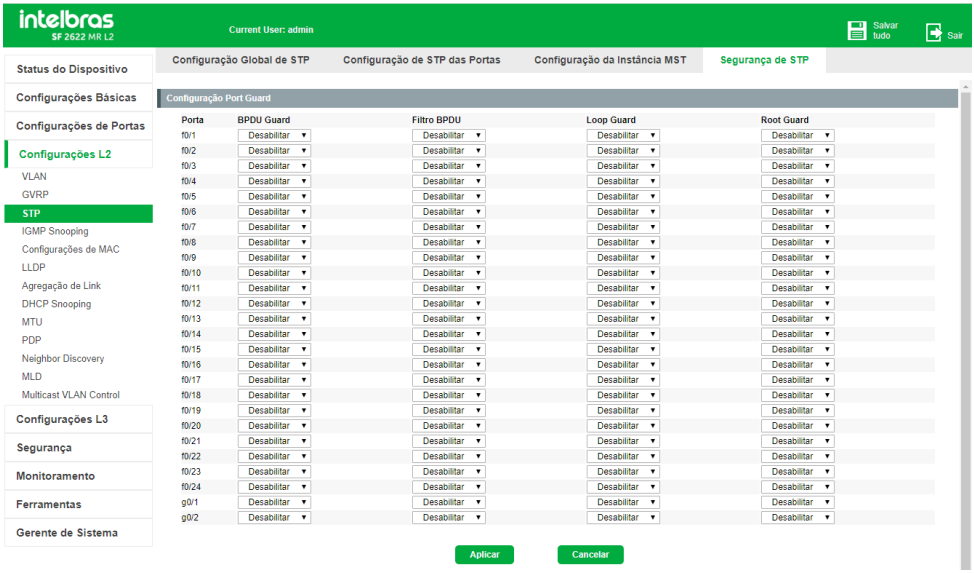


Configuração da instância MST - configuração da instância MST

6.3.4. Segurança STP

As funções de segurança STP fornecem segurança e estabilidade para a Spanning Tree. A seguir são descritas as funções suportadas pelo switch.

- **BPDU Guard:** as portas do switch conectadas diretamente em computadores ou servidores podem ser configuradas como Porta Edge, para que o estado da porta seja alterado rapidamente, otimizando o processo de convergência STP. As portas configuradas como Porta Edge não podem receber quadros BPDUs. Quando essas portas recebem BPDUs, o sistema automaticamente configura essas portas como Non-Edge e regenera o Spanning Tree, podendo causar atrasos na convergência do STP. Um usuário mal-intencionado pode atacar o switch enviando quadros BPDUs, que resultaria em atrasos na convergência do STP. Para evitar esse tipo de ataque, o MSTP fornece a função de *BPDU protect*. Com essa função habilitada, o switch desabilita as portas configuradas como Porta Edge ao receberem quadros BPDUs.
- **Root protect:** um CIST e suas Bridges Root secundárias estão geralmente localizados no core da rede. Configurações erradas ou ataques maliciosos podem resultar com que quadros BPDUs com maior prioridade sejam recebidas pela Bridge Root, o que faz com que a Bridge Root atual perca a sua posição, podendo ocasionar atrasos na rede. Para evitar isso, o MSTP fornece a função *Root protect*. As portas que estiverem com esta função habilitada só podem ser definidas como Portas Designadas em todas as instâncias do Spanning Tree. Quando este recurso está habilitado na porta e esta porta receber quadros BPDU com maior prioridade, a porta transitará seu estado para bloqueado *Blocked* negando o encaminhamento de pacotes (como se o link estivesse desconectado). A porta retorna seu estado normal se não receber quadros de configuração BPDUs com prioridades maiores em um período igual a duas vezes o tempo do Forward Delay.
- **Loop protect:** em uma rede estável, o switch mantém o estado das portas recebendo e processando quadros BPDU. No entanto, quando ocorre congestionamento no link, falhas na conexão ou alteração indevida na topologia da rede, o switch pode não receber quadros BPDU por um determinado período, resultando em uma nova execução do algoritmo Spanning Tree, podendo ocorrer a alteração do estado das portas antes da convergência STP da rede, isto é, as portas passariam do estado bloqueado (Blocked) para o estado de encaminhamento (Forwarding) precocemente, podendo ocasionar loops na rede.



Segurança de STP

Configuração port guard

É possível habilitar dois métodos de proteção simultaneamente, não tendo dependência entre eles.

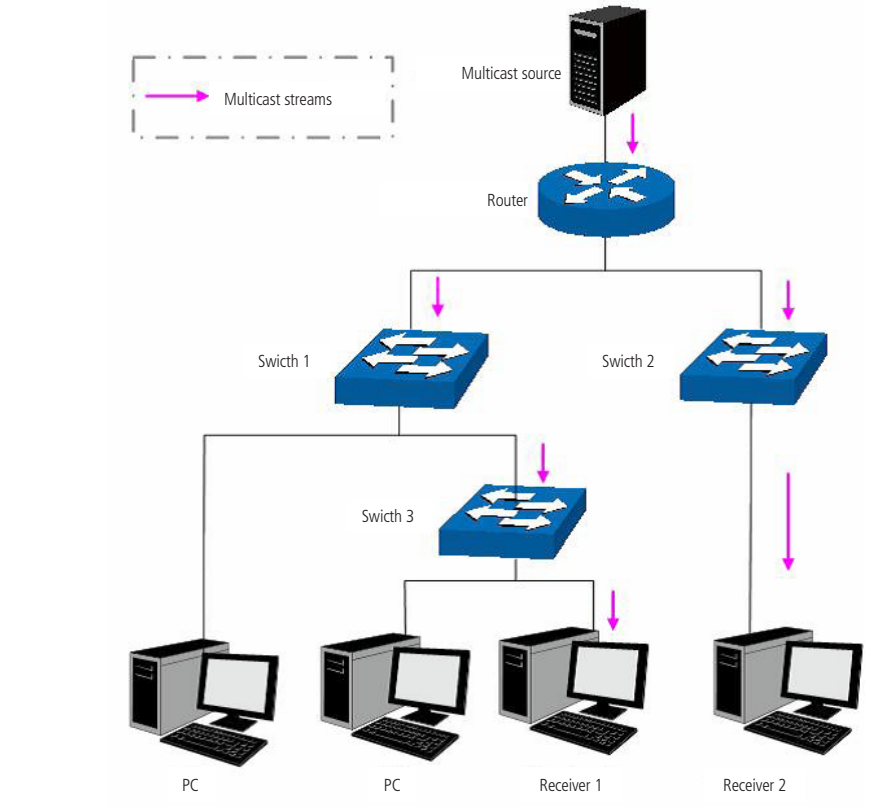
- **BPDU Guard:** configura o BPDU Guard.
- **Filtro BPDU:** configura o Filtro BPDU.
- **Loop Guard:** configura o Loop Guard.
- **Root Guard:** configura o root protect.

6.4. IGMP snooping

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 mostra como o tráfego Multicast é transmitido.



Tráfego Multicast

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 especifico 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.

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*.

6.4.1. Espionar IGMP

Nesta página é possível habilitar a função *IGMP snooping* no switch.

Se o endereço Multicast dos dados recebidos não estiverem na tabela de endereços Multicast, o switch irá enviar um broadcast na VLAN.

Quando a função *Multicast desconhecido* está selecionada em *Descartar*, o switch descartará os pacotes de Multicast desconhecidos que são recebidos, evitando assim o uso desnecessário de largura de banda e melhorando a performance do sistema. Configure esse recurso de acordo com suas necessidades.

IGMP Snooping

Configuração geral de IGMP

- **Multicast desconhecido:** selecione a operação que o switch irá fazer ao receber Multicast desconhecido.
  - **Transferir:** o switch encaminhará o pacote Multicast em forma de broadcast à todas as portas pertencentes à VLAN.
  - **Descartar:** o switch descartará os pacotes Multicast desconhecido que são recebidos, evitando assim o uso desnecessário de largura de banda e melhorando a performance do sistema.
- **IGMP Snooping:** selecione *Habilitar/Desabilitar* para habilitar ou desabilitar a função *IGMP snooping* no switch.
- **Auto Query:** selecione *Habilitar/Desabilitar* para habilitar ou desabilitar o IGMP Querier.

6.4.2. Lista de VLAN

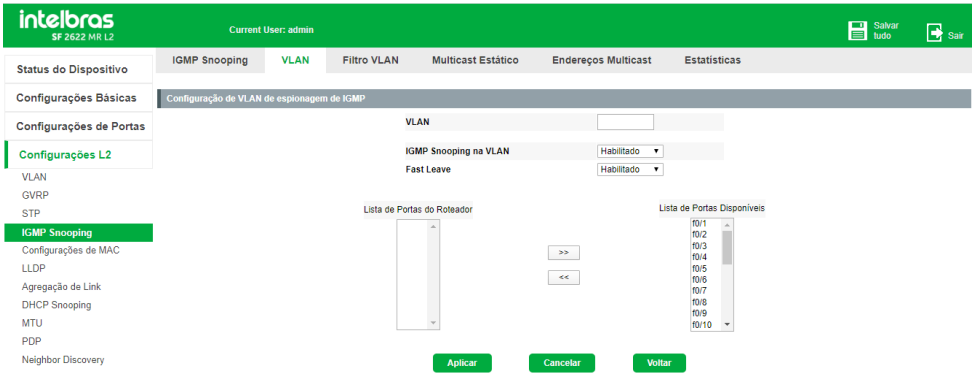
Nesta tela é possível verificar as VLANs com IGMP Snooping e Fast Leave habilitados e definir a porta roteador da VLAN.

VLAN

Configuração de VLAN para grupos Multicast

- **VLAN:** identifica a VLAN.
- **Status da VLAN do IGMP:** informa que a VLAN está com o IGMP Snooping em execução.
- **Fast Leave:** informa o status do Fast leave.
  - **Desabilitar:** *Fast leave* desabilitado.
  - **Habilitar:** *Fast leave* habilitado.
- **Porta do Roteador Multicast:** informa a porta definida como porta roteador da VLAN.
- **Editar:** clique em *Editar* para modificar as configurações da VLAN.

Após clicar em *Novo,* a tela seguinte permite realizar as configurações de Fast leave e porta roteador na VLAN selecionada.



VLAN - configuração da VLAN IGMP

Configuração da VLAN IGMP

- **VLAN:** identifica a VLAN a ser configurada.
- **IGMP Snooping na VLAN:** selecione *Habilitar/Desabilitar* para habilitar ou desabilitar a função *IGMP snooping* na VLAN.
- **Fast Leave:** selecione *Habilitar/Desabilitar* para habilitar ou desabilitar a função *Fast leave* na VLAN desejada. A função *Fast leave* faz com o switch remova imediatamente a porta da Tabela de endereços Multicast, assim que receber uma mensagem IGMP Leave.
- **Lista de portas disponíveis:** informa as portas disponíveis para ingressarem como porta roteador.
- **Lista de portas do roteador:** informa as portas habilitas como portas roteador. É possível configurar até 8 portas para o roteador multicast.

Obs.: *Fast Leave somente é suportado na porta do switch quando o cliente utiliza o IGMP v2 ou v3.*

6.4.3. Filtro de VLAN

Na página a seguir é possível vincular os endereços multicast com um determinada VLAN. Somente os endereços multicast vinculados serão encaminhados para membros multicast, filtrando endereços multicast não vinculados na VLAN.

Filtro de VLAN – configurações de filtro multicast

Configurações de filtro multicast

- **VLAN ID:** informa a VLAN.
- **Endereço IP permitido:** informa o endereço multicast permitido na VLAN informada.
- **Novo:** abre a seção *Configuração de filtro* para configuração de um novo filtro.

Filtro VLAN – configuração de filtro

Configuração de filtro

Nesta seção é possível realizar o vínculo da VLAN com o endereço multicast. Ao vincular um endereço Multicast em uma VLAN, somente pacotes com esse endereço multicast serão encaminhados para os membros.

6.4.4. Multicast estático

Nesta página é possível configurar a tabela de endereços Multicast manualmente. Esta tabela funciona de modo isolado em relação ao grupo Multicast dinâmico e do filtro Multicast. Estes endereços não são aprendidos pelo IGMP Snooping, desta forma é possível melhorar a qualidade e segurança dos dados Multicast transmitidos na rede.

Multicast estático

Configuração de multicast estático

- **Porta designada (destino):** digite a porta na qual os fluxos multicast serão encaminhados.

6.4.5. Endereços Multicast

Nesta página o equipamento lista todos os endereços multicast recebidos e encaminhados, informando a VLAN, porta e o método de aprendizado.

Endereços multicast

Informações da lista

- » **Tipo:** informa como o endereço multicast foi aprendido.
- » **IGMP:** endereço descoberto através do protocolo IGMP.
- » **User:** endereço configurado de forma estática pelo usuário.

6.4.6. Estatísticas IGMP

Nesta página você pode visualizar o tráfego de dados Multicast em cada VLAN do switch, o que facilita o monitoramento de mensagens IGMP na rede.

Estatísticas IGMP

Estatísticas IGMP snooping

- » **Versão x:** informa todos os pacotes trafegados nas respectivas versões do IGMP: *Versão 1*, *2* e *3*.

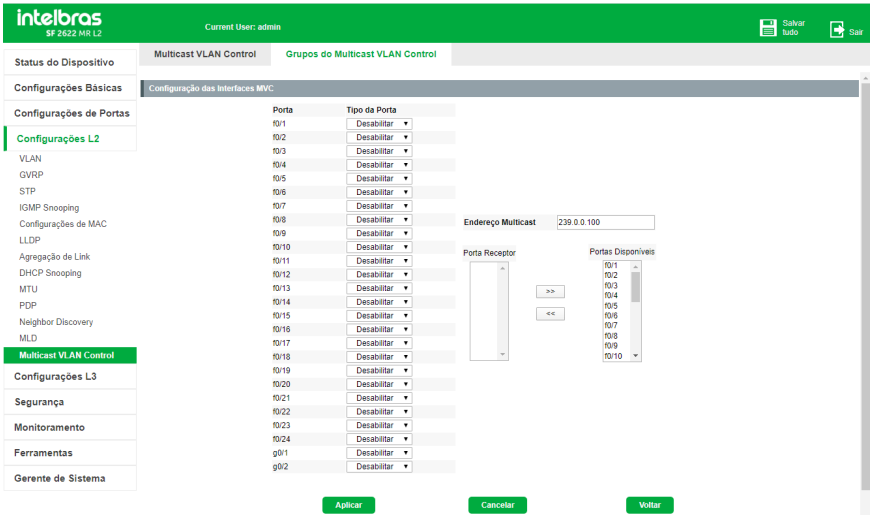
6.5. Configurações de MAC

Neste menu é possível configurar as entradas estáticas e dinâmicas na tabela MAC.

6.5.1. MACs estáticos

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.



MACs estáticos

Lista de endereços MAC estáticos

Lista das entradas estáticas a tabela MAC.

» **Novo|Editar:** abre a seção *Configuração de endereço de MAC estático.*

Configuração de endereço de MAC estático

Configuração de endereço de MAC estático

Apenas uma porta pode ser configurada para um Endereço de MAC unicast, enquanto que múltiplas portas podem ser configuradas para um Endereço de MAC multicast ou broadcast.

» **Endereço de MAC estático:** endereço MAC no formato *XXXX.XXXX.XXXX*.

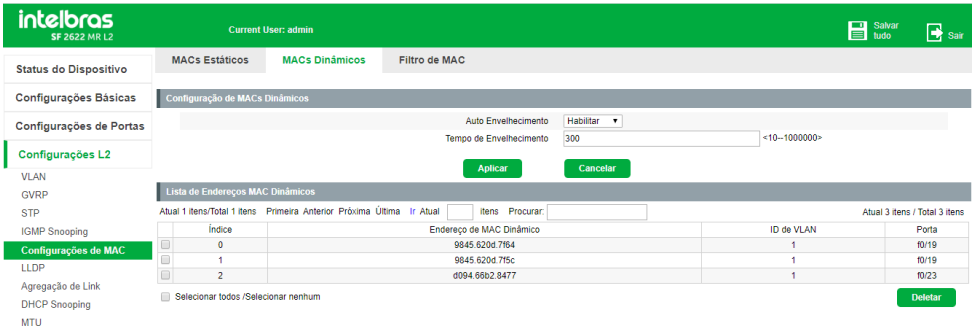
» **ID de VLAN:** identificador da VLAN.

6.5.2. MACs dinâmicos

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 torna possível a manutenção da tabela de endereços MAC.

O tempo de envelhecimento define o tempo em que o switch irá manter o registro do endereço MAC após o mesmo estar ocioso.

Nesta página você pode configurar os endereços MAC dinâmicos.



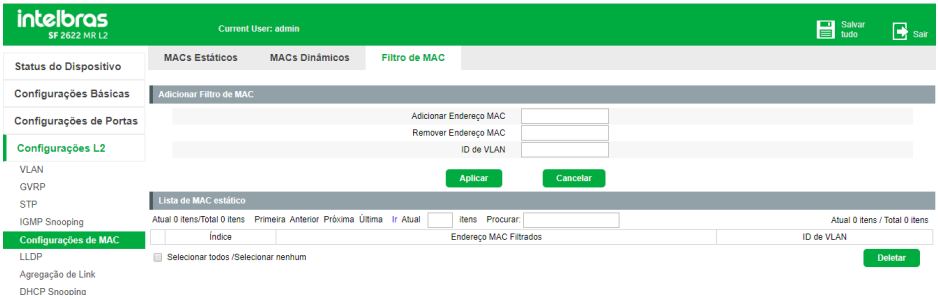
MACs dinâmicos

Configuração de MACs dinâmicos

Quando o *Autoenvelhecimento* está desabilitado, significa que um MAC aprendido dinamicamente nunca será removido a mesmo que a porta do endereço seja desconectada ou o switch reinicie.

6.5.3. Filtro MAC

Nesta página é possível configurar entradas de filtro na tabela de endereços MAC. Você pode adicionar ou remover endereços MAC da tabela.



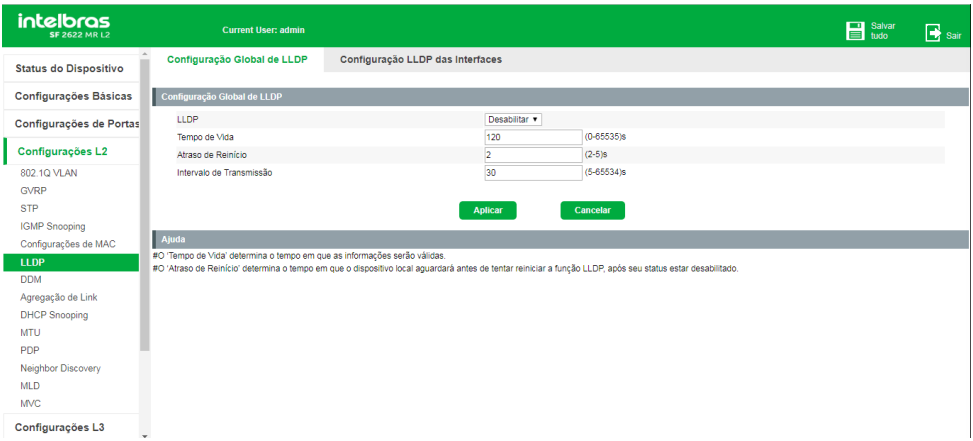
Filtro MAC

- **Adicionar endereço de MAC:** aponde um endereço MAC para ser filtrado na tabela MAC.
- **Remover endereço de MAC:** aponde um endereço MAC para ser removido do filtro na tabela MAC.
- **ID de VLAN:** identificador da VLAN.

6.6. LLDP

O protocolo LLDP (*Link Layer Discovery Protocol*) é usado para permitir o switch conheça e seja reconhecido por outros equipamentos de rede conectados nele.

6.6.1. Configuração global de LLDP

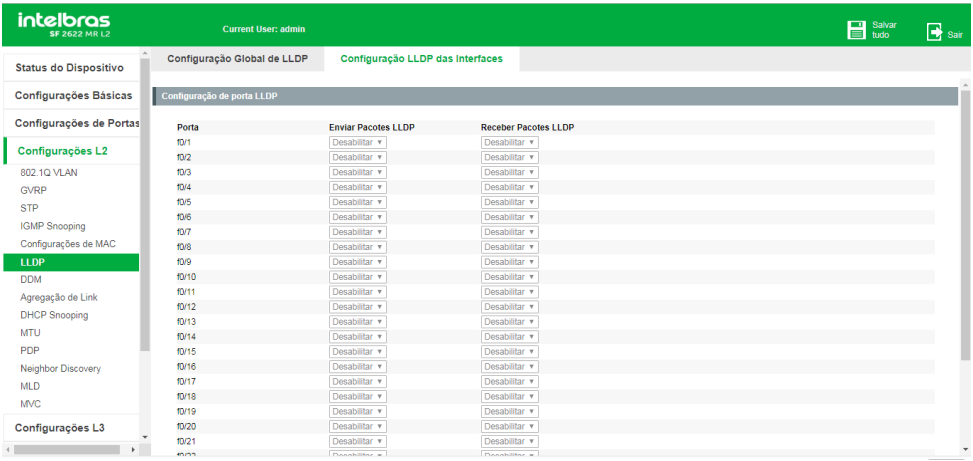


Configuração global de LLDP

Configuração global de LLDP

- » **LLDP:** selecione *Habilitar/Desabilitar* para habilitar ou desabilitar o protocolo LLDP globalmente no equipamento. Após esta configuração será necessário configurar o envio ou recebimento de pacotes nas portas na tela *Configuração LLDP das interfaces*.
- » **Tempo de vida:** indica o intervalo de tempo que as informações do pacote LLDP a ser enviado serão válidos.
- » **Atraso de reinício:** indica o intervalo de tempo que o equipamento aguardará antes de tentar reiniciar a função *LLDP*, após seu status estar desabilitado.
- » **Intervalo de transmissão:** indica o intervalo de transmissão entre pacotes LLDP.

6.6.2. Configuração LLDP das interfaces



Configuração LLDP das interfaces

Configuração de porta LLDP

- **Porta:** indicação da porta para configuração.
- **Enviar pacotes LLDP:** selecione *Habilitar/Desabilitar* para habilitar ou desabilitar o envio de pacotes LLDP na porta selecionada.
- **Receber Pacotes LLDP:** selecione *Habilitar/Desabilitar* para habilitar ou desabilitar o recebimento de pacotes LLDP na porta selecionada.

6.7. Agregação de link

LAG (*Link Aggregation Group*) é a função de agregação de links. Esta função permite a utilização de múltiplas portas para o aumento da velocidade do link além dos limites nominais de uma única porta, introduz controle de falhas e redundância para a conexão a outro dispositivo que disponha do mesmo recurso. As portas pertencentes a um grupo LAG devem possuir os mesmos parâmetros de configuração, caso utilizadas com as seguintes funções: *VLAN* e *Configuração das portas* (velocidade, modo *Duplex* e controle de fluxo) e que participam de um mesmo grupo LAG, deverão obrigatoriamente possuir as mesmas configurações.

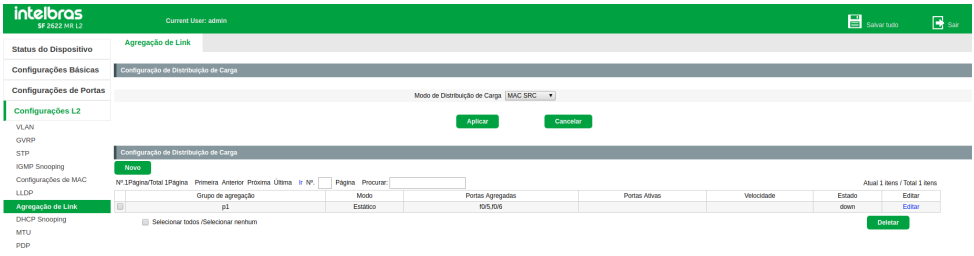
O balanceamento de carga entre as portas pertencentes a um grupo LAG será de acordo com o algoritmo de Hash configurado. Se a conexão de uma porta estiver com perdas de pacotes, o tráfego será transmitido pelas portas que estejam normais. De modo a garantir a confiabilidade da conexão.

Algoritmos de distribuição de carga

- **MAC DST:** este algoritmo utiliza o endereço de MAC de destino para realizar o balanceamento de carga.
- **MAC SRC:** este algoritmo utiliza o endereço de MAC de origem para realizar o balanceamento de carga.
- **AMBOS MAC:** este algoritmo utiliza o endereço de MAC de origem e de destino para realizar o balanceamento de carga.
- **IP DST:** este algoritmo utiliza o endereço IP de destino para realizar o balanceamento de carga.
- **IP SRC:** este algoritmo utiliza o endereço IP de origem para realizar o balanceamento de carga.
- **AMBOS IP:** este algoritmo utiliza o endereço IP de origem e de destino para realizar o balanceamento de carga.

LACP (*Link Aggregation Control Protocol*) é definida pela norma IEEE802.3ad, e permite a agregação e desagregação de link de forma dinâmica, realizado através de trocas de pacotes LACP. Com o recurso LACP ativado, o switch enviará pacotes contendo a identificação da agregação de link (ID) para o seu parceiro e outras informações como Prioridade, endereço MAC do switch e Chave Administrativa. Uma agregação de link dinâmica somente será realizada entre portas de switches com o mesmo ID de agregação de link.

Existem dois modos de portas: *Ativo* e *Passivo*. No modo *Ativo*, a porta pode enviar pacotes LACP ativamente enquanto no modo *Passivo*, a porta só pode enviar pacotes LACP depois de ter recebido um pacote LACP. Sugere-se que defina um lado como modo *Ativo* e o outro lado como modo *Passivo*.



Agregação de link

6.7.1. Agregação de link

Configuração de distribuição de carga

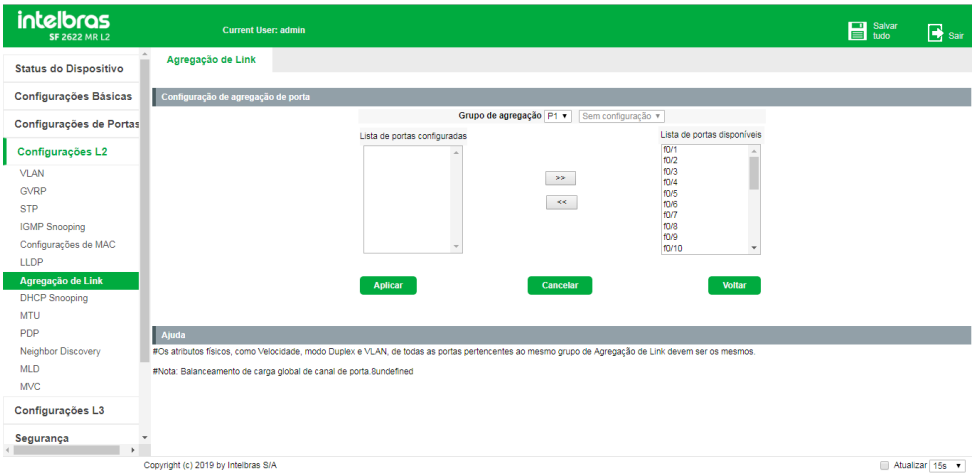
Configure o modo de distribuição de carga (algoritmo de hash) dos grupos (suporta até 8).

Lista de LAG

A tabela informa as configurações e status dos grupos.

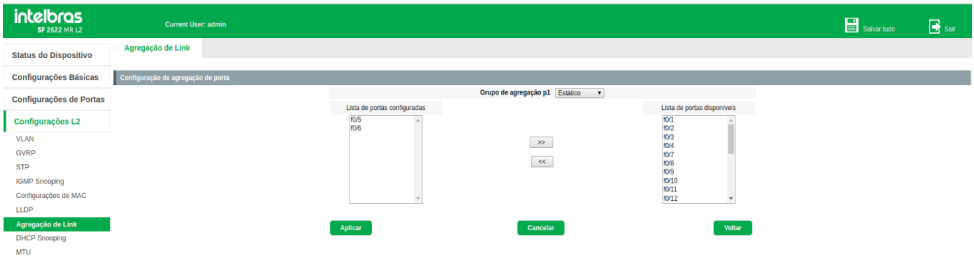
» **Novo|Editar:** abre a seção *Configuração de agregação de porta* para configuração de um LAG.

» **Tela novo grupo:** seleciona as portas e o modo do grupo (estático, passivo e ativo).



Agragação de link - configuração de agregação de porta

» **Tela edição de grupo:** permite editar as configurações do grupo.

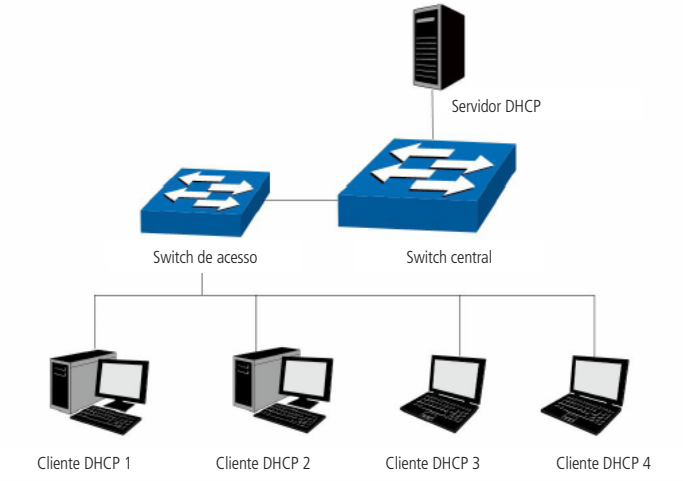


Tela edição de grupo

6.8. DHCP snooping

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, permitindo o perfeito funcionamento dos computadores e recursos da rede. O protocolo DHCP (*Dynamic Host Configuration Protocol*) foi desenvolvido baseando-se no protocolo BOOTP e é utilizado para otimizar e resolver os problemas mencionados acima.

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:

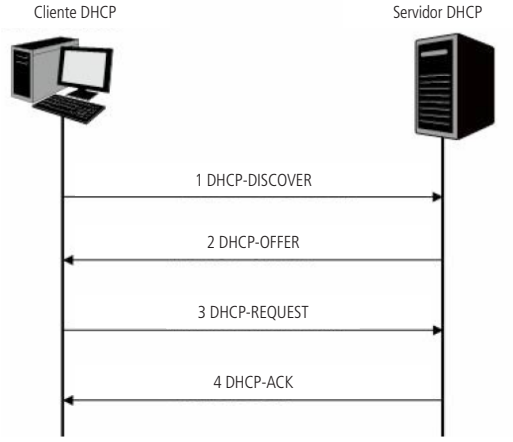


Funcionamento do DHCP

O servidor DHCP fornece três métodos de atribuição de endereços IPs.

- **Manual:** permite o 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 os endereços IPs dinamicamente, como ilustrado na figura a seguir:



Negociação DHCP

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 a vários servidores DHCP enviando pacotes DHCP-OFFER, o cliente só irá responder ao primeiro pacote recebido e transmitir 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.

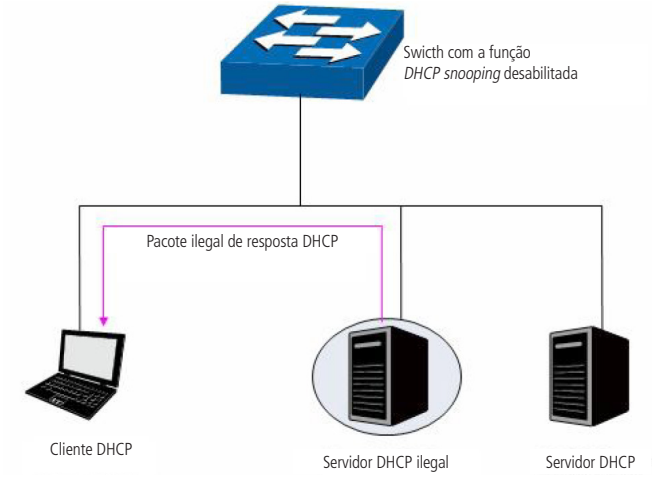
O campo *Option 82* pode conter no máximo 255 subopções. Uma vez que o campo *Option 82* é definido, pelo menos uma das subopções deve ser configurada. O switch suporta duas subopções: *Circuit-ID* e *Remote-ID*. Como não existe um padrão universal para o campo *Option 82*, diferentes implementações de diferentes fabricantes podem existir. Para esse switch, as subopções 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, acontecerá certa confusão e insegurança na rede. Os casos mais comuns que podem ocorrer estão listados a seguir.

1. O servidor DHCP ilegal é configurado manualmente pelo usuário por engano.
2. Hacker esgotam os endereços IPs do servidor DHCP e fingem ser um servidor DHCP para atribuir os endereços IPs e demais informações de rede para os clientes. Por exemplo, um hacker usou o servidor DHCP para atribuir uma modificação no servidor DNS, de modo que os usuários irão acessar sites de comércio eletrônico e digitarão suas senhas achando que é o site real. A figura a seguir ilustra a DHCP Cheating Attack.



DHCP cheating attack

A função *DHCP snooping* permite que apenas a porta conectada a um servidor DHCP possa transmitir pacotes DHCP, isso garante que os usuários receberam de forma correta os endereços IPs e parâmetros da rede. O DHCP snooping monitora o processo de obtenção do endereço IP entre o cliente e o servidor DHCP, registrando o endereço IP, endereço MAC, VLAN e porta do switch que o cliente está conectado, criando assim uma tabela de vínculos, que poderá ser utilizada por outras funções, como por exemplo, Inspeção ARP e outros recursos de proteção e segurança. A função de *DHCP snooping* impede o DHCP Cheating Attack descartando os pacotes DHCP de portas não confiáveis.

6.8.1. Configuração global

Nesta página é possível habilitar o DHCP snooping e escolher parâmetros do campo *Option 82*.

Configuração global

Configuração global DHCP snooping

- **Options 82:** define o formato da *Option 82*.
  - **format snmp-ifindex:** preenche no campo *Option 82* o *SNMP ifindex* (opcional)
  - **format manual:** usa a configuração manual para preencher a *opção82* (opcional).
  - **format cm-type:** usa o *cm-type* para preencher o campo *Option 82* (opcional)
  - **format hn-type [host]:** usa o formato utilizado na cisco para preencher o campo *Option 82*.

Configuração de VLAN

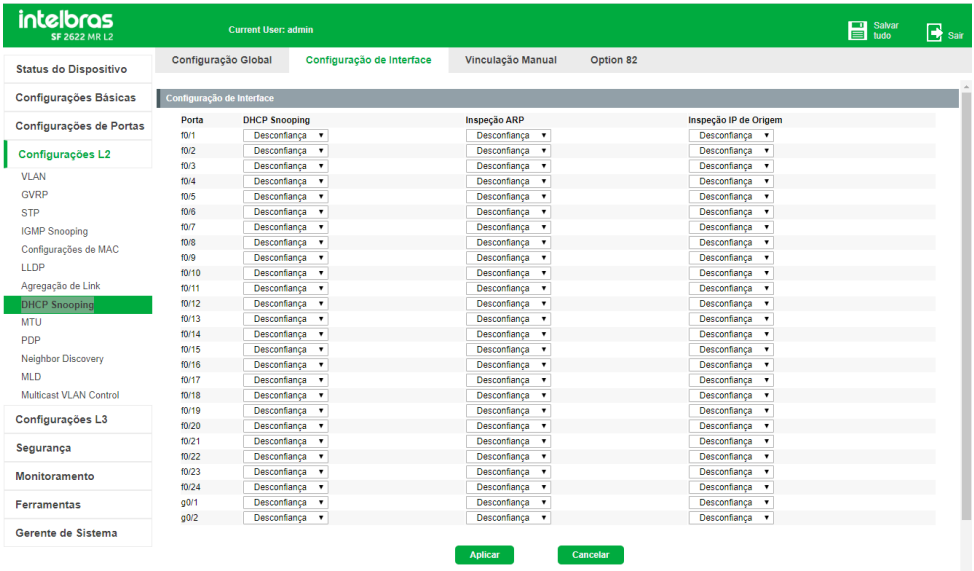
Nessa página é possível escolher quais VLANs serão inspecionadas pelo DHCP snooping, habilitar a inspeção ARP e inspeção do IP de origem.

» **Configuração global DHCP snooping**
  » **VLAN DHCP snooping:** selecione quais VLANs irão participar do DHCP snooping para monitorar os pacotes DHCP.
  » **VLAN inspeção ARP:** selecione quais VLANs irão participar do monitoramento dos pacotes ARP. É possível obter ajuda sobre a função na guia de configuração de interface.
  » **VLAN IP de origem:** selecione quais VLANs irão participar do monitoramento de IP de origem. É possível obter ajuda sobre a função na guia de configuração de interface.

Obs.: *para usar mais de uma VLAN use as expressões: Expressão 1:* 1-10 *(para incluir da VLAN 1 até a VLAN 10). Expressão 2:* 1,3,5 *(para incluir da VLAN 1, 3 e 5). Expressão 3:* 1,3-5 *(para incluir da VLAN 1, 3, 4 e 5). Outras combinações podem ser usadas.*

6.8.2. Configuração de interface

Nesta página é possível determinar quais funções do DHCP snooping serão habilitadas em cada porta. Somente as portas no modo *Desconfiança* terão os pacotes inspecionados.



Configuração da interface – DHCP snooping

Configuração da interface

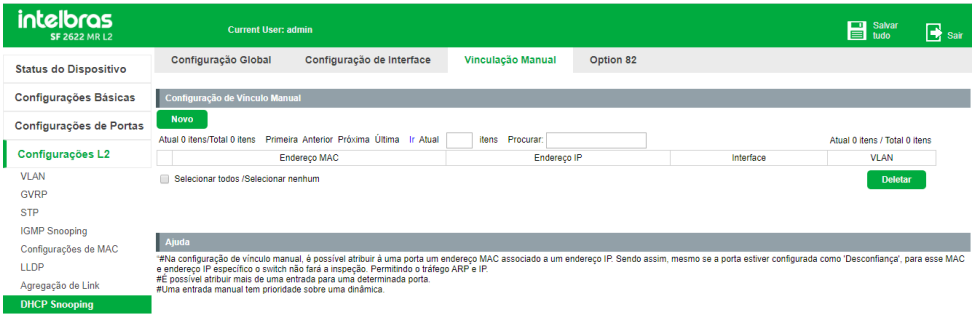
» **DHCP snooping:** faz o monitoramento dos pacotes do protocolo DHCP. Use a configuração *Confiança* em uma porta que contenha um servidor DHCP.
  » **Confiança:** permitirá que os pacotes *DHCP offer* sejam respondidos para os hosts solicitantes na interface selecionada.
  » **Desconfiança:** não permitirá que os pacotes *DHCP offer* sejam retornados pela interface selecionada.
» **Inspeção ARP:** faz o monitoramento do protocolo ARP.
  » **Confiança:** permite que os pacotes ARPs possam trafegar livremente pela interface selecionada.
  » **Desconfiança:** os pacotes ARPs só poderão trafegar se o host que está nesta porta passar pelo processo de alocação de IP dinâmico (receber um IP de um servidor DHCP). Nesse caso o switch fará um vínculo entre o IP + MAC + porta dinamicamente. Outra maneira de permitir é configurando um vínculo do IP + MAC + porta manual no menu *Vinculação Manual*.
» **Inspeção IP de origem:** faz o monitoramento dos pacotes do protocolo IP. Mesmo que um host tenha aprendido a tabela ARP, ela pode ter o tráfego do protocolo IP bloqueado, até que um vínculo dinâmico ou manual seja realizado, ou altere a porta para o modo *Confiança*.

» **Confiança:** permite os pacotes com protocolo IP na interface selecionada.

» **Desconfiança:** realiza o monitoramento dos pacotes com protocolo IP, neste caso, só permitirá pacote com o protocolo IP, caso algum vínculo tenha sido estabelecido de forma dinâmica ou manual (a vinculação manual pode ser realizada no menu *Vinculação Manual*).

6.8.3. Vinculação manual

Nesta página é possível vincular o IP, MAC, VLAN e Porta. E os pacotes vinculados manualmente não serão monitorados.



Vinculação manual

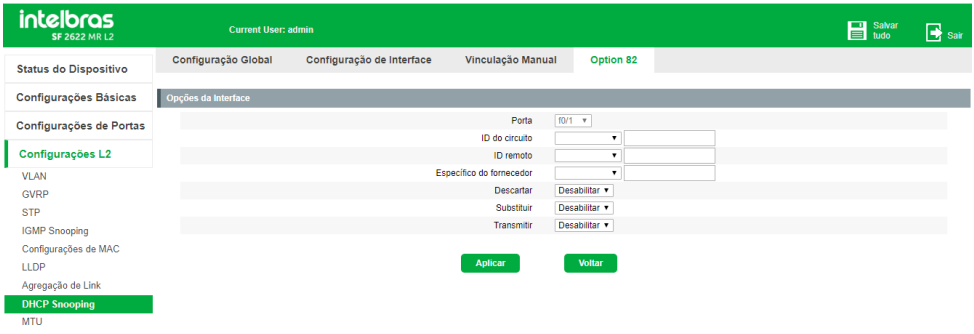
Lista de vinculação manual

No exemplo acima os pacotes provenientes que corresponderem as regras criadas (IP, MAC, VLAN e porta) serão permitidos em portas no modo desconfiança em *Inspeção IP de origem*.

6.8.4. Option 82

Nessa página é possível customizar os parâmetros do option 82. O Option 82 altera os pacotes *DHCP Discover* do protocolo DHCP e insere um novo rótulo *option* (Option 82) nos pacotes com informações adicionais.

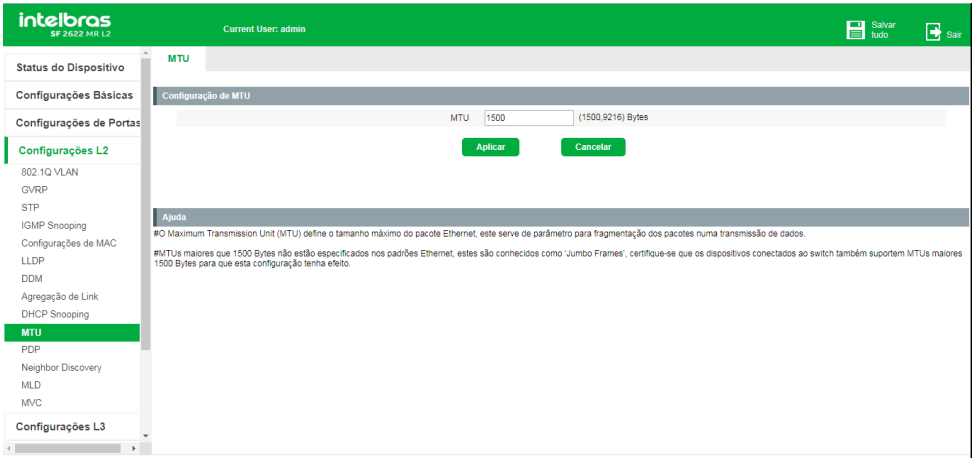
Com a edição das ações do Option 82, também é possível alterar o conteúdo dos pacotes que o switch recebe de outros switches, descartar os pacotes ou simplesmente deixar passar sem alterações.



Option 82

6.9. MTU

O Maximum Transmission Unit (MTU) define o tamanho máximo do pacote Ethernet, este serve de parâmetro para fragmentação dos pacotes numa transmissão de dados.



MTU

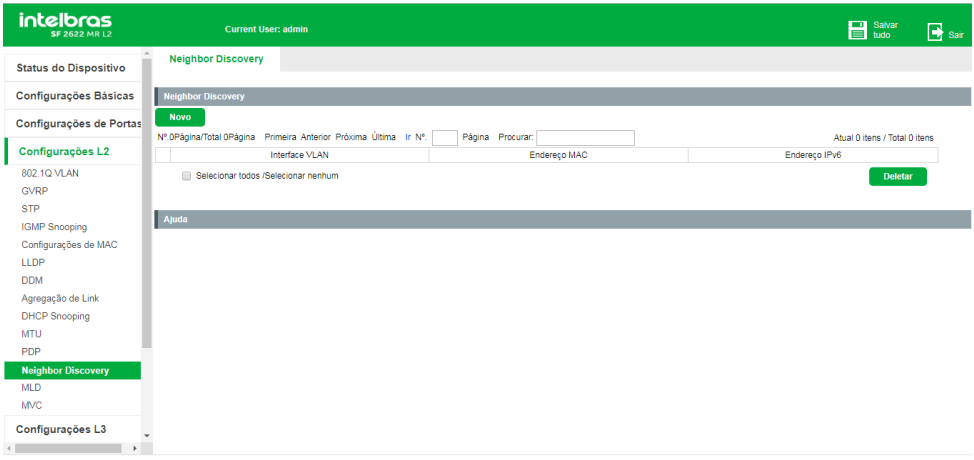
6.9.1. MTU

Configuração de MTU

» **MTU:** indica o valor para o MTU.

6.10. Neighbor Discovery

O protocolo Neighbor Discovery (ND) é responsável por identificar e conhecer as características da vizinhança de onde o switch está inserido. O objetivo do ND é resolver questões relacionadas a conexão de nós vizinhos em uma rede IPv6.

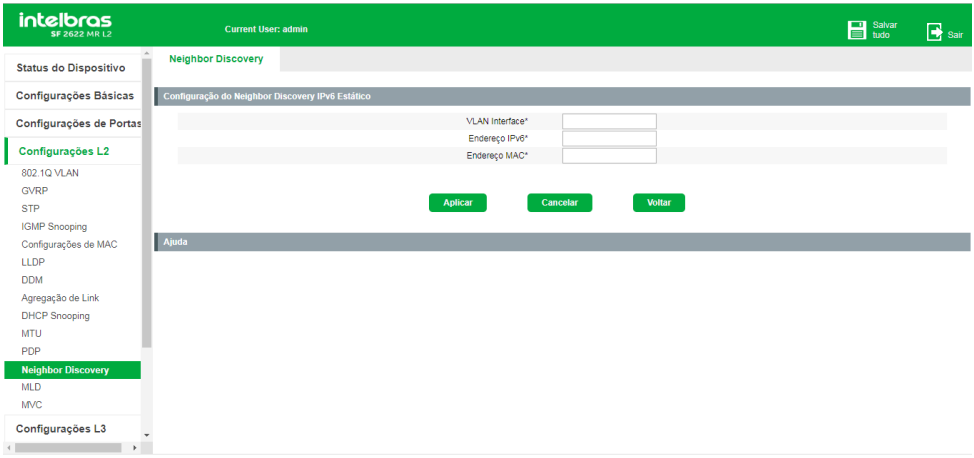


Neighbor Discovery

6.10.1. Neighbor Discovery

Neighbor Discovery

- » **Novo:** para uma nova configuração global estática de descoberta de vizinhos, clique no botão *Novo*. Será aberta a tela para configuração do Neighbor Discovery IPv6 estático.
- » **Interface VLAN:** indica a interface VLAN ondo o equipamento cadastrado manualmente no switch está conectado.
- » **Endereço MAC:** indica o endereço MAC do equipamento cadastrado.
- » **Endereço IPv6:** indica o endereço IPv6 do equipamento cadastrado.
- » **Deletar:** para deletar uma ou mais entradas IPv6 manuais de vizinhos, primeiro selecione as portas correspondentes e então clique em *Deletar.*



Neighbor Discovery - configuração do Neighbor Discovery IPv6 estático

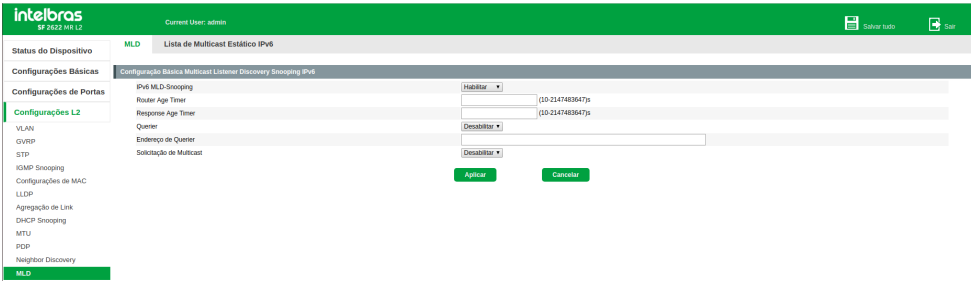
Configuração do Neighbor Discovery IPv6 estático

- » **VLAN Interface:** configure a interface VLAN do equipamento para ser cadastrado manualmente no switch.
- » **Endereço IPv6:** configure o endereço IPv6 do equipamento para ser cadastrado manualmente no switch.
- » **Endereço MAC:** configure o endereço MAC do equipamento para ser cadastrado manualmente no switch.

6.11. MLD

MLD (*Multicast Listener Discovery*) faz parte do protocolo IPv6, usando para suportar e gerenciar o multicast IP entre o host e o roteador multicast. O multicast IP permite que os datagramas sejam transmitidos para um conjunto de hosts que compõem um grupo multicast. As relações entre os membros do grupo multicast são dinâmicas, ou seja, os hosts podem entrar ou sair deles para minimizar a carga da rede, de modo a obter a efetiva transmissão de dados. O snooping MLD é usado para monitorar os pacotes MLD entre o host e o roteador. Ele dinamicamente cria, mantém e exclui a tabela de endereços multicast com base na entrada e saída dos membros do grupo multicast. Nesse caso, os quadros multicast são encaminhados de acordo com a tabela de endereço multicast.

Em uma rede multicast executando o protocolo MLD, um roteador multicast é responsável pelo envio de consultas MLD. Mas você pode configurar o MLD-Snooping querier para que o switch possa enviar ativamente uma mensagem de consulta de grupo geral para estabelecer e manter uma entrada de encaminhamento multicast. Os usuários também podem configurar o MLD-Snooping querier para encaminhar em um endereço de origem especifico (*Endereço de Querier*), o tempo de resposta máximo (*Response Age timer*) e o intervalo de consulta (*Router Age Timer*) para o envio de mensagens de consulta geral.



MLD

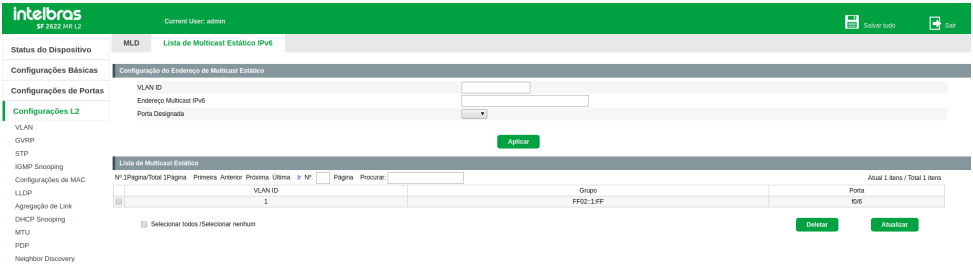
6.11.1. MLD

Configuração básica Multicast Listener Discovery Snooping IPv6

Habilite o MLD e configure o Querier.

» **Solicitação multicast:** habilita a solicitação de encaminhamento de hardware para o grupo multicast.

6.11.2. Lista de multicast estático IPv6



Lista de multicast estático IPv6

Configuração do endereço de multicast estático

Adicione um grupo estático na tabela.

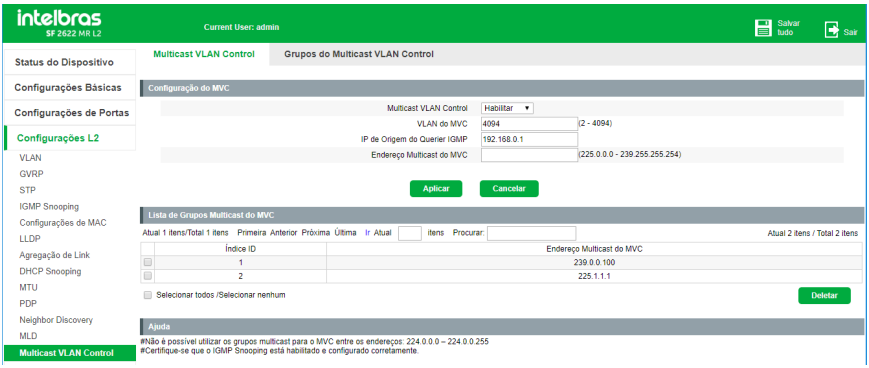
Lista de multicast estático

Mostra os grupos estáticos da tabela.

6.12. MVC

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 Control (MVC) roteia pacotes recebidos em uma VLAN de origem de multicast para uma ou mais VLANs de recebimento. Os clientes estão nas VLAN de recepção e o servidor de multicast está na VLAN de origem.

Para que o MVC libere o fluxo multicast para a porta receptora, é necessário que receba uma solicitação para o grupo em questão (em qualquer VLAN).



MVC

6.12.1. MVC

Configuração de multicast VLAN

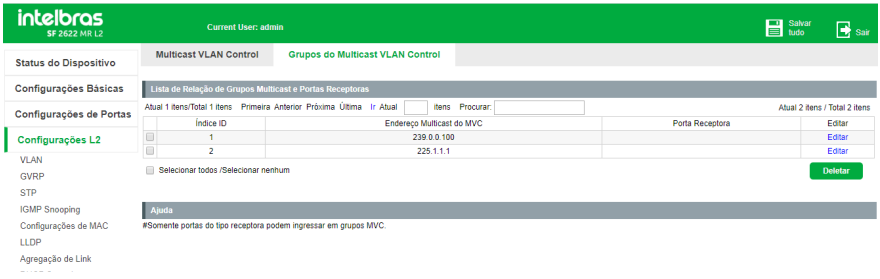
Para que o MVC funcione corretamente é necessário habilitar o IGMP e negar o encaminhamento de multicast desconhecidos.

- **MVC Multicast VLAN:** VLAN onde os pacotes multicast serão recebidos da fonte, necessário configurar apenas uma vez.
- **IP de origem do querier IGMP:** IP do Querier que o MVC irá gerar para verificar se o receptor quer continuar recebendo o fluxo multicast, necessário configurar apenas uma vez (necessário habilitar o IGMP Querier nas configurações de IGMP Snooping).
- **Endereço Multicast do MVC:** IP do grupo MVC que será criado.

Lista de grupo MVC Multicast

Lista todos os grupos criados.

MVC configuração de endereço multicast



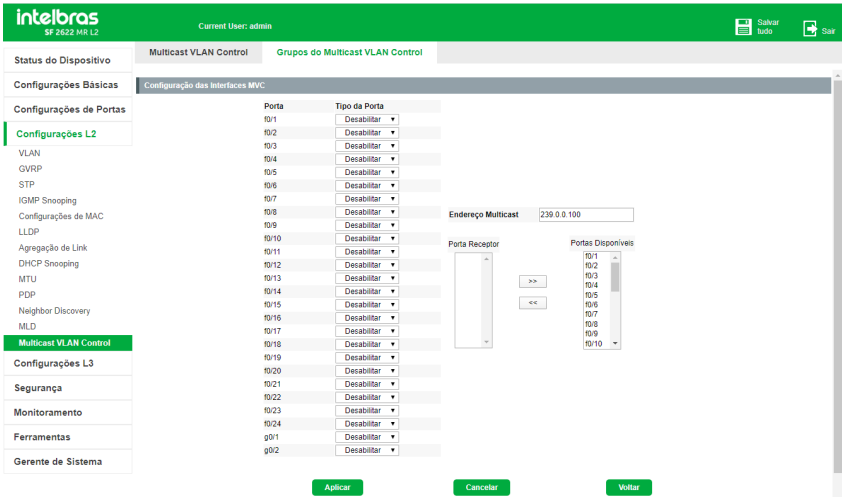
MVC configuração de endereço multicast

Informações do grupo Multicast MVC

Mostra os grupos criados e quais portas estão associadas.

» **Editar:** abre a seção *Configurar o Modificador MVC Multicast* para adicionar portas a um grupo recém-criado, ou alterar de um que já estava criado.

Obs.: *para adicionar uma porta em um grupo é necessário que ela seja receptora.*



MVC configuração de porta e de endereço Multicast - configurar o modificador MVC Multicast

Configuração da interface MVC

Configure o modo *MVC* da porta, podendo ser receptora, fonte ou estar desabilitada.

» **Fonte:** porta usada para conectar com o roteador.

» **Receptor:** porta usada para conectar os hosts.

7. Configurações L3

Com exceção do gerenciamento do switch, este geralmente opera até a camada 2 do modelo OSI, realizando funções de controle e priorização através de padrões como VLAN e STP. Neste menu são realizadas as configurações de L3 do switch que incluem as configurações de interface VLAN.

7.1. Interface VLAN

Interfaces são utilizadas para trocar dados e interagir com interfaces de outros dispositivos de rede. Existem dois tipos de interface:

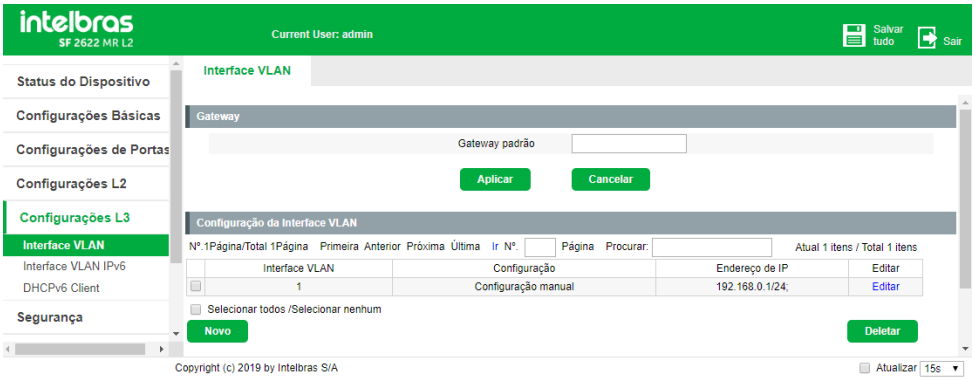
» **Interface L2:** são as portas físicas do switch. Estas encaminham pacotes baseando-se na tabela MAC do switch.

» **Interface L3:** são as interfaces VLAN configuradas. Estas encaminham pacotes baseando-se na tabela ARP do switch (endereços IP) e servem como gateway padrão de todos os dispositivos na VLAN correspondente. As interfaces VLAN também são utilizadas roteamento inter-VLAN, roteamento IP e gerenciamento do dispositivo.

Obs.: *este modelo não possui a função de roteamento.*

7.1.1. Interface VLAN

Na tela a seguir é feita a configuração das interfaces VLAN.



Interface VLAN

Gateway

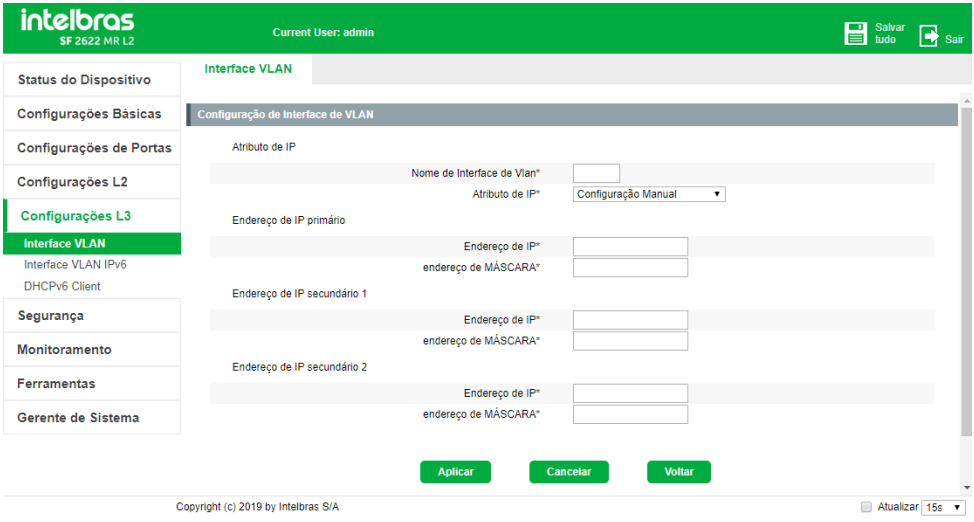
Nesta seção é configurado o gateway padrão do switch. O gateway padrão corresponde ao próximo salto da rota padrão do switch, ou seja, será encaminhado a este dispositivo todo o tráfego de roteamento.

» **Gateway padrão:** endereço IP do gateway padrão.

Configuração da interface VLAN

Nesta seção é exibida uma lista com todas as interfaces VLAN configuradas.

» **Novo|Editar:** abre a seção *Configuração de interface de VLAN* para a configuração de uma interface VLAN.



Interface VLAN - configuração de interface de VLAN

Configuração de interface de VLAN

» **Nome de Interface de VLAN:** identificador da interface VLAN.

» **Atributo de IP:** seleciona o modo de configuração do endereço IP da VLAN. O endereço IP pode ser configurado manualmente ou obtido via DHCP.

» **Endereço de IP:** configura um endereço IP manualmente.

» **Endereço de máscara:** máscara do endereço IP especificado.

7.2. Interface VLAN IPv6

Os endereços IPv6 Unicast identificam em nível de rede um dispositivo único. Os dois principais tipos são:

- **Global:** como os endereços públicos do IPv4, este é um endereço válido na internet. Normalmente são utilizados os 64 bits mais a esquerda para identificação da rede e os 64 bits mais a direita para identificação do dispositivo (enlace e Host). O endereço é constituído de três partes:
  - **Prefixo global:** identifica a rede.
  - **Sub-rede:** identifica um enlace em uma rede.
  - **Host:** identifica o dispositivo dentro de um enlace.
- **Link Local:** como os endereços privados do IPv4, este não é um endereço válido na internet e por isso pode apenas ser usado no enlace do dispositivo. Este utiliza o prefixo *FE80::/64*.

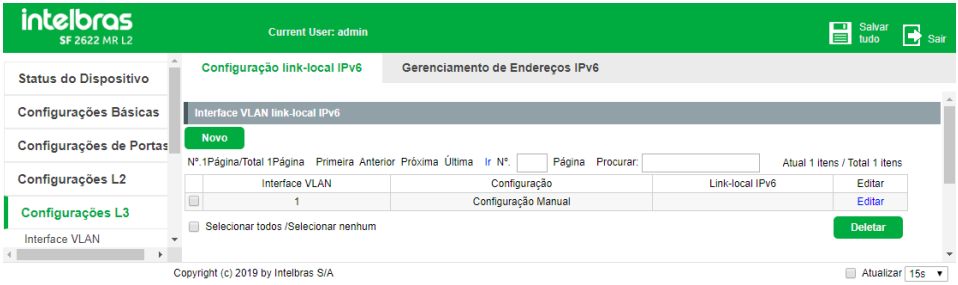
As interfaces VLANs com IPv6 configurado encaminham pacotes baseando-se na tabela de vizinhos IPv6 e servem como gateway padrão de todos os dispositivos IPv6 na VLAN correspondente.

Para configurar os endereços IPv6 da interface VLAN siga os seguintes passos:

1. Configure o endereço link-local na tela *Configuração link-local*;
2. Configure manualmente o endereço global na tela *Gerenciamento de endereços IPv6* ou vá para o menu *Cliente DHCPv6* e configure a obtenção automática do endereço global IPv6.

7.2.1. Configuração link-local IPv6

Na tela a seguir é feita a configuração do endereço IPv6 de link-local da interface VLAN.

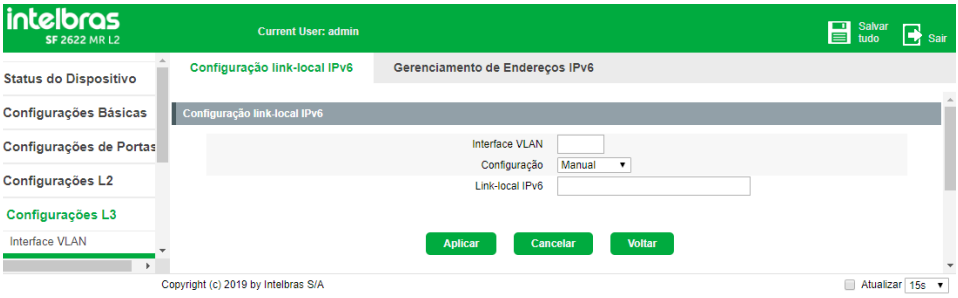


Configuração link-local IPv6

Interface VLAN link-local IPv6

Nesta seção é exibida uma lista com todas as interfaces VLAN configuradas.

- **Novo|Editar:** abre a seção *Configuração link-local IPv6* para a configuração de uma interface VLAN e seu endereço link-local IPv6.



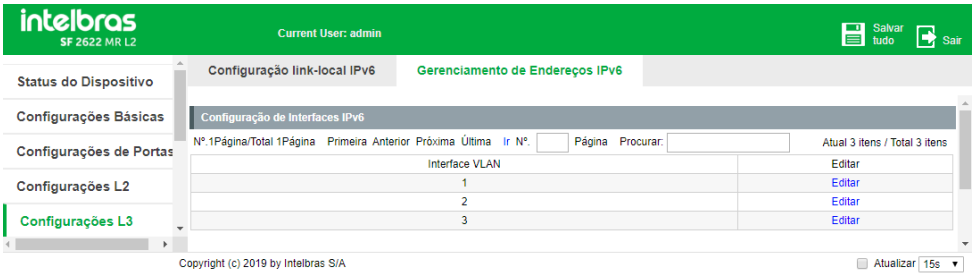
Configuração link-local IPv6 - configuração link-local IPv6

Configuração link-local IPv6

- **Interface VLAN:** identificador da interface VLAN.
- **Configuração:** modo de configuração do endereço IPv6 link-local. A configuração pode ser feita manualmente ou através do método EUI-64.
- **Link-local IPv6:** configuração manual do endereço IPv6 link-local.

7.2.2. Gerenciamento de endereços IPv6

Na tela a seguir é feita a configuração do endereço global IPv6 da interface VLAN.



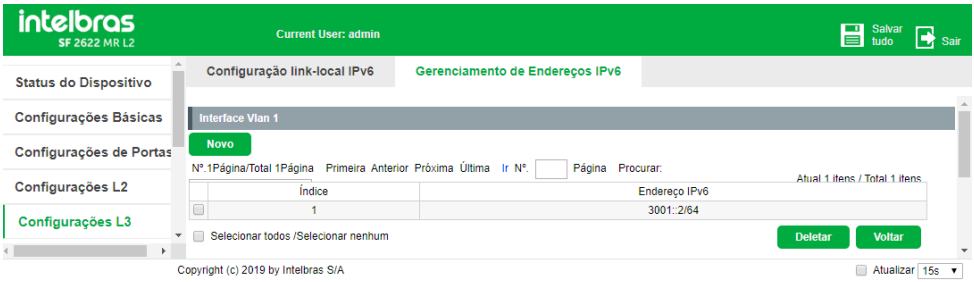
Gerenciamento de endereços IPv6

Configuração de interfaces IPv6

Nesta seção é exibida uma lista com as interfaces VLAN criadas para a configuração dos endereços globais IPv6.

» **Interface VLAN:** identificador da interface VLAN.

» **Editar:** abre a seção *Interface VLAN* para configuração do endereço IPv6 global da interface VLAN respectiva.



Gerenciamento de endereços IPv6 - interface VLAN

Interface VLAN

Nesta seção é exibida uma lista com os endereços globais IPv6 de uma interface VLAN.

» **Novo:** abre a seção *Novo endereço global* para configuração de um novo endereço IPv6 global.

Gerenciamento de endereços IPv6 - novo endereço global

Novo endereço global

» **Endereço IPv6:** especifica o novo endereço IPv6 global a ser configurado.

8. Segurança

Além das funções de segurança presentes no menu *Configurações de porta* o switch ainda possui funções de DoS, ACL e controle de acesso através do 802.1x e RADIUS.

A ACL (*Lista de Controle de Acesso*) é utilizada para a configuração de uma lista de regras para a recepção de pacotes, controlando o acesso ilegal a rede. Além disso, a função de *ACL* pode controlar os fluxos dos dados, economizando recursos da rede de forma flexível, facilitando o controle da rede.

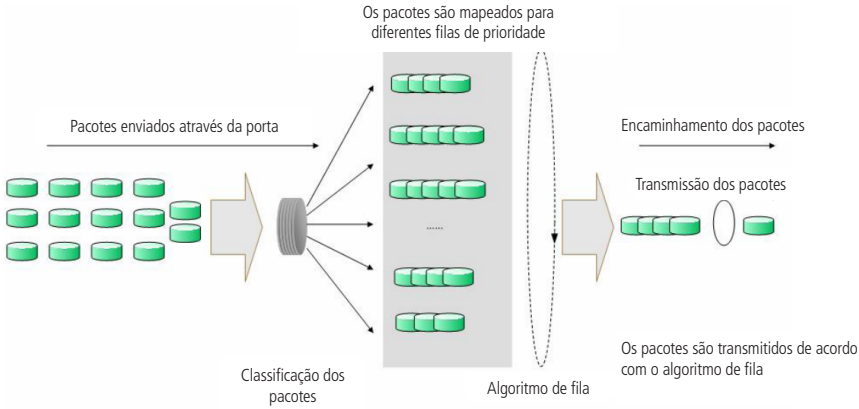
Neste switch, as ACLs classificam os pacotes com base em uma série de condições que podem ser encontrados em protocolos utilizados entre as camadas 2 a 4 do modelo de referência OSI.

Também é possível controlar as ACLs baseando-se em intervalos de tempo, flexibilizando ainda mais o uso das ACLs.

8.1. 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 prioridade, em seguida encaminha os pacotes de acordo com o algoritmo de fila selecionado, implementando a função de *QoS*.

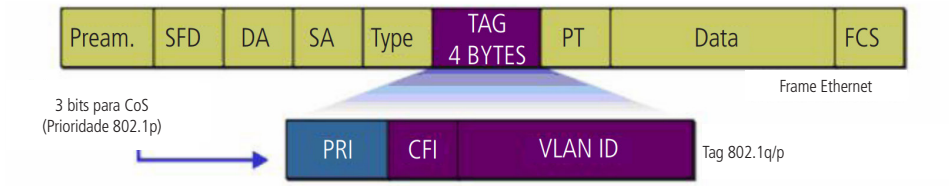


QoS

Classificação dos pacotes

O switch implementa três modelos de prioridades, *Prioridade por Porta*, *por 802.1p* e *DSCP*.

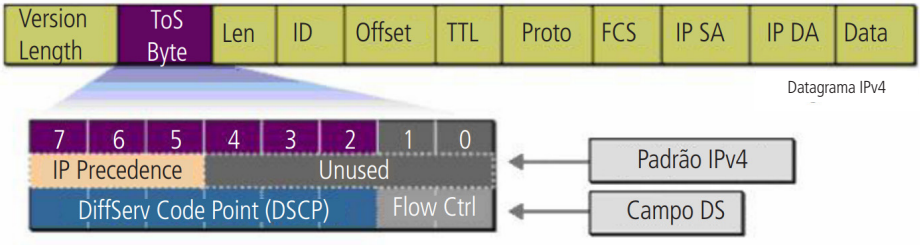
- **Prioridade por porta:** neste modo de prioridade o fluxo de dados será mapeado para as filas de prioridade conforme o valor CoS definido para cada porta.
- **Prioridade 802.1p:**



Tag 802.1q

De acordo com a figura anterior, 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).

» **Prioridade DSCP:**



ToS

De acordo com a figura anterior, 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.

Algoritmos de fila

O switch suporta 8 filas de prioridade que podem ser priorizadas em quatro de algoritmos:

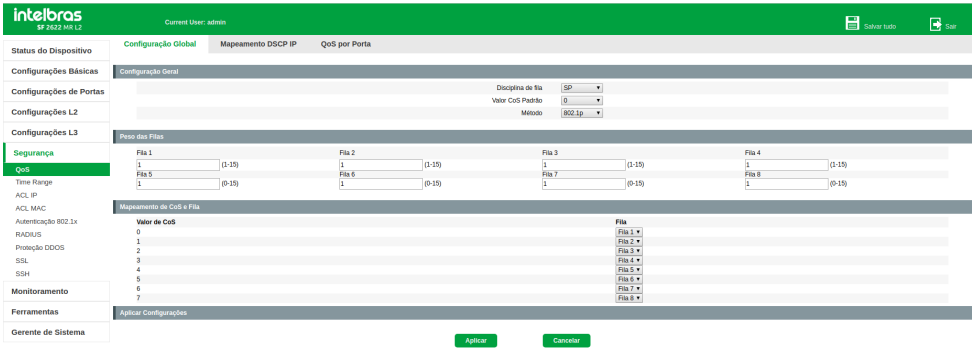
» **SP:** algoritmo SP (*Strict Priority*). Neste modo, a fila com maior prioridade ocupará totalmente a largura de banda. Os pacotes em fila de menor prioridade somente serão enviados após todos os pacotes de filas com maior prioridade serem enviados.

» **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.

» **WFQ:** o Weighted Fair Queuing (WFQ) classifica o pacote de acordo com a prioridade do tráfego. Define a largura de banda de saída com base no peso de cada tráfego. Quanto maior o peso, maior a largura de banda. Assim, garante a justiça dos serviços prioritários e incorpora o peso dos diferentes serviços prioritários

» **FCFS:** o algoritmo de fila First-Come-First-Served (FCFS), fornece serviço a esses pacotes de acordo com sua sequência de chegada a um switch, e o pacote que chega primeiro ao switch será encaminhado primeiro.

8.1.1. Configuração global



Configuração global

Configuração geral

» **Disciplina de fila:** selecione o algoritmo de fila que será implementado, o switch suporta SP, WRR, WFQ e FCFS.

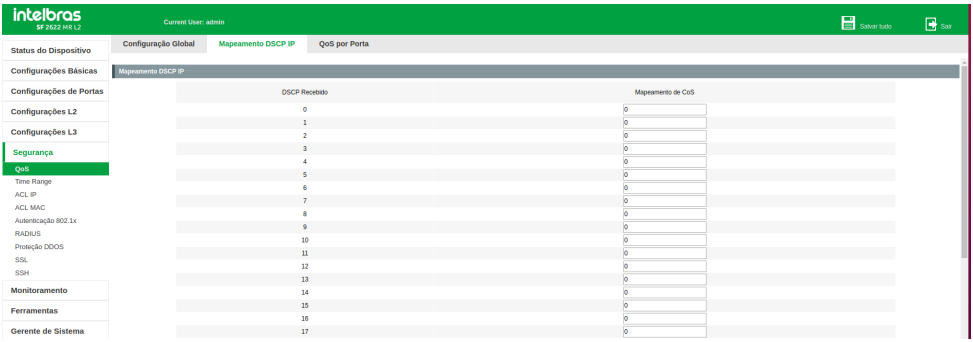
» **Valor CoS padrão:** selecione o valor do CoS que será aplicado nos pacotes entrantes em todas as interfaces (configuração válida somente para QoS por porta).

» **Método:** selecione o método de priorização. Se selecionado o método *802.1p*, o sistema irá tratar o campo *priority* (3 bits 0 - 7) do cabeçalho VLAN. Se selecionado o método *DSCP*, o sistema irá tratar o campo *ToS* do cabeçalho IP, respeitado os 6 primeiros bits mais significativos, que sãos os bits mapeados para o DSCP. Se selecionado *Desabilitar*, somente será possível utilizar o QoS por portas.

» **Peso das filas:** o switch suporta até 8 filas de prioridade, onde você pode selecionar pesos entre 1 até 15.

» **Mapeamento de CoS e fila:** selecione a fila em que cada CoS irá pertencer.

8.1.2. Mapeamento DSCP IP



Mapeamento DSCP IP

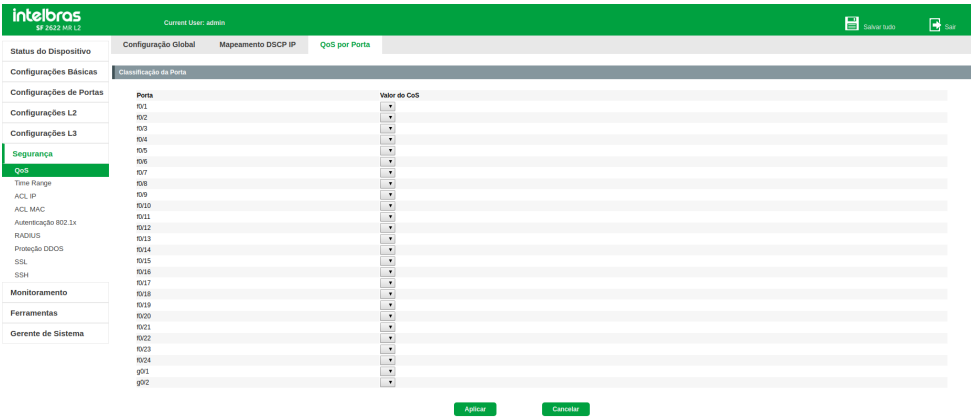
Mapeamento DSCP IP

» **DSCP recebido:** é o campo *DSCP* do cabeçalho IP dos pacotes que o switch recebe. Os pacotes podem conter o valor 0 ou até 63.

» **Mapeamento de CoS:** informa qual classificação estamos atribuindo para um determinado DSCP. O valor pode variar de 0 até 7.

» Por exemplo, ao informar que o campo *Mapeamento de CoS* tem o valor 3 para o *DSCP Recebido 1*, todo pacote que constar o valor 1 no campo *DSCP* será classificado com o CoS 3. Para saber em qual fila esse pacote irá pertencer, é necessário verificar a configuração de *Mapeamento de CoS e Fila* na página *Configuração global*.

8.1.3. QoS por porta



QoS por porta

Classificação da porta

» **Valor de CoS:** informe no campo *Valor de CoS* qual classificação você deseja atribuir à porta.

» Por exemplo, Ao selecionar o valor de CoS 0 para a porta 1 e valor de CoS 1 para a porta 2, elas serão classificadas como tal, mas depende de como foi configurado cada fila em *Configuração global*. Por padrão o CoS 0 está vinculado à fila 1, CoS 1 à fila 2 até CoS 7 à fila 8. Mas isso pode ser alterado.

8.2. Time Range

Neste menu são configurados intervalos de tempo (time range) utilizados por algumas funções do switch como a ACL.

Time range

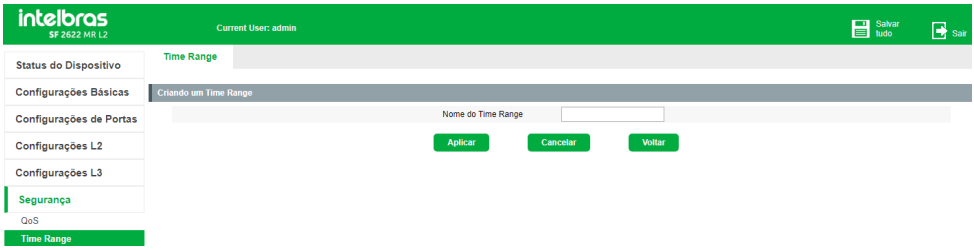
8.2.1. Time Range

Lista time range

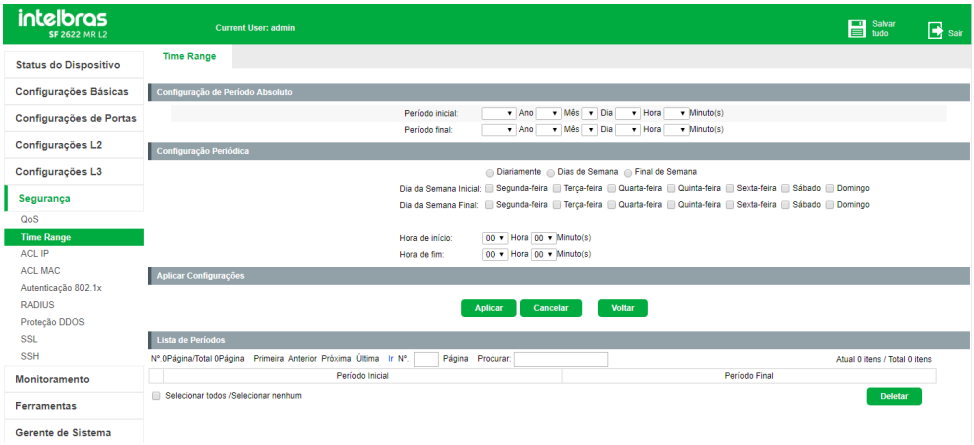
Exibe uma lista com todos os Time Ranges configurados.

» **Novo:** abre a seção *Criando um Time Range* para criação de um novo Time Range.

» **Editar:** abre as seções de edição de uma Time Range.



Time range – criando um time range



Configuração do time range

Configuração do time range

Um *Time range* pode ter um período absoluto e vários periódicos.

- **Configuração de período absoluto:** em *Configuração de período absoluto* é possível definir um período macro, que pode compreender um dia específico ou até um ano. Quando for configurado um período absoluto todas as demais regras periódicas só irão operar nesse intervalo de tempo.
- **Configuração periódica:** é possível ter mais de uma *Configuração periódica*. A configuração pode ser diariamente, somente nos dias de semana, somente nos finais de semana ou de forma mesclada. Toda regra deve ter pelo menos um período inicial com uma hora de início e fim.
- **Lista de períodos:** exibe todos os períodos configurados do Time range.

8.3. ACL IP

A ACL IP configurada nesta seção cria regras baseadas em condições do protocolo IP e possui dois principais tipos:

- **ACL standart:** esta é a ACL IP padrão e permite a configuração de regras baseadas no endereço IP de origem ou destino.
- **ACL extended:** esta é a ACL IP estendida e permite a configuração de regras mais complexas incluindo a possibilidade da verificação de outros campos do cabeçalho IP e do cabeçalho TCP/UDP.

Para configurar a ACL IP siga os seguintes passos:

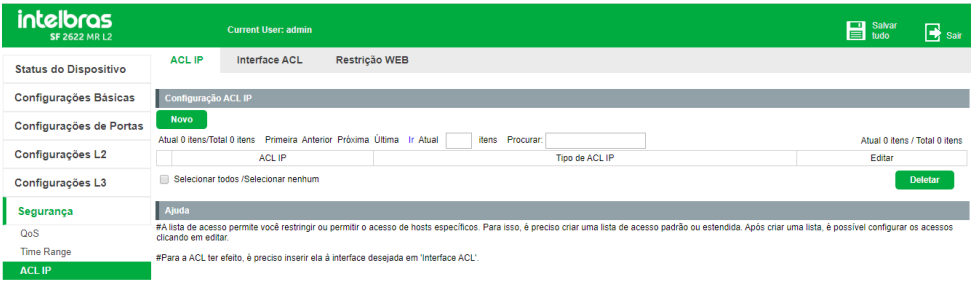
1. Crie ACL IP standart ou extended na seção *Criando um IP ACL* da tela *Configuração de lista de acesso IP*,
2. Configure as regras da ACL criada na seção *Criar regra* da tela *Configuração de lista de acesso IP*;
3. Aplique a ACL configurada na porta desejada na tela *Aplicação de lista de acesso IP*.

Para configurar a restrição de acesso web siga os seguintes passos:

1. Configure uma ACL IP;
2. Vá para a tela *Restrição web* e aplique uma *ACL IP*.

8.3.1. Configuração de lista de acesso IP

Nesta tela é criada e configurada a ACL IP.

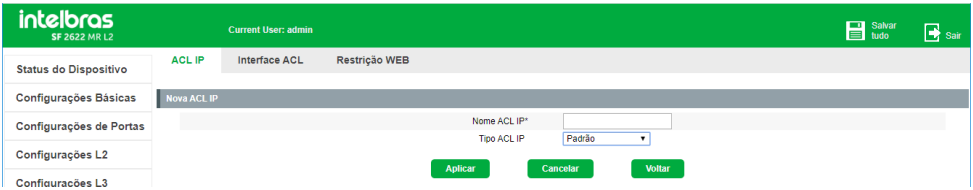


Configuração de lista de acesso IP

Configuração de IP ACL

Nesta seção é exibida uma lista com todas as ACLs IP criadas.

- **Novo:** abre a seção *Criando um IP ACL* para criação de uma nova ACL IP.
- **Editar:** abre a seção *ACL IP* com as regras existentes.

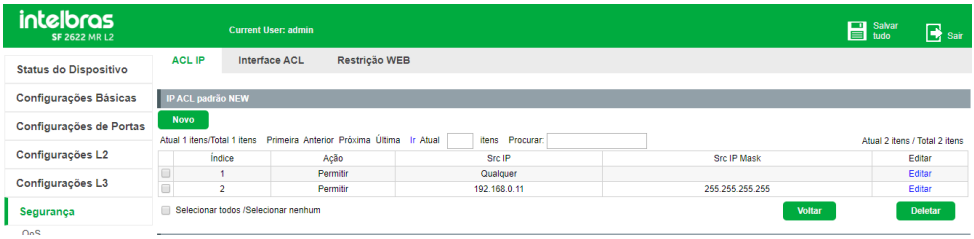


Configuração de lista de acesso IP – criando um IP ACL

Criando um IP ACL

Nesta seção é criado uma nova ACL IP.

- » **Nome de IP ACL:** nome descritivo da ACL.
- » **Atributo:** tipo da ACL.

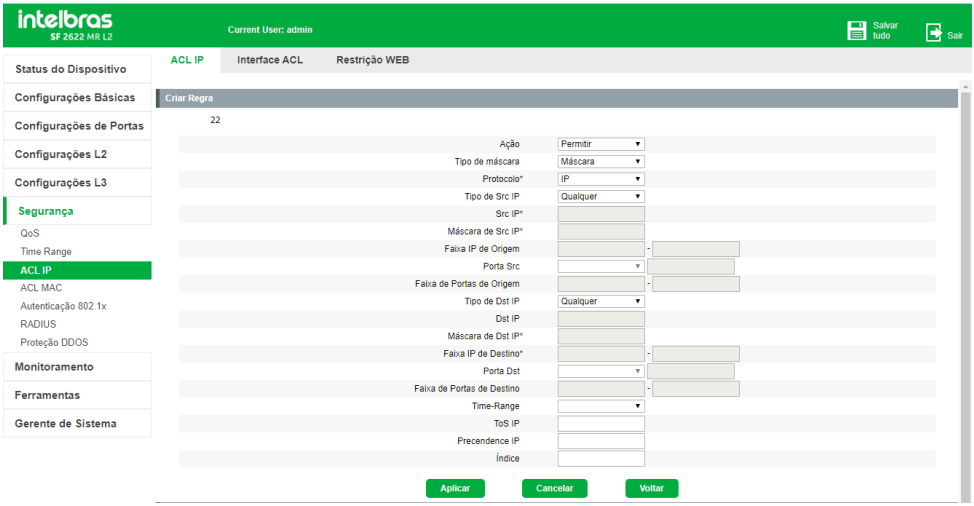


Configuração de lista de acesso IP - ACL IP

ACL IP

Nesta seção é exibida uma lista com todas as regras criadas.

- » **Novo:** abre a seção *Criar regra* para configuração de uma nova regra.
- » **Editar:** abre a seção *Alterar regra* para editar uma regra existente.



Configuração de lista de acesso IP - criar regra

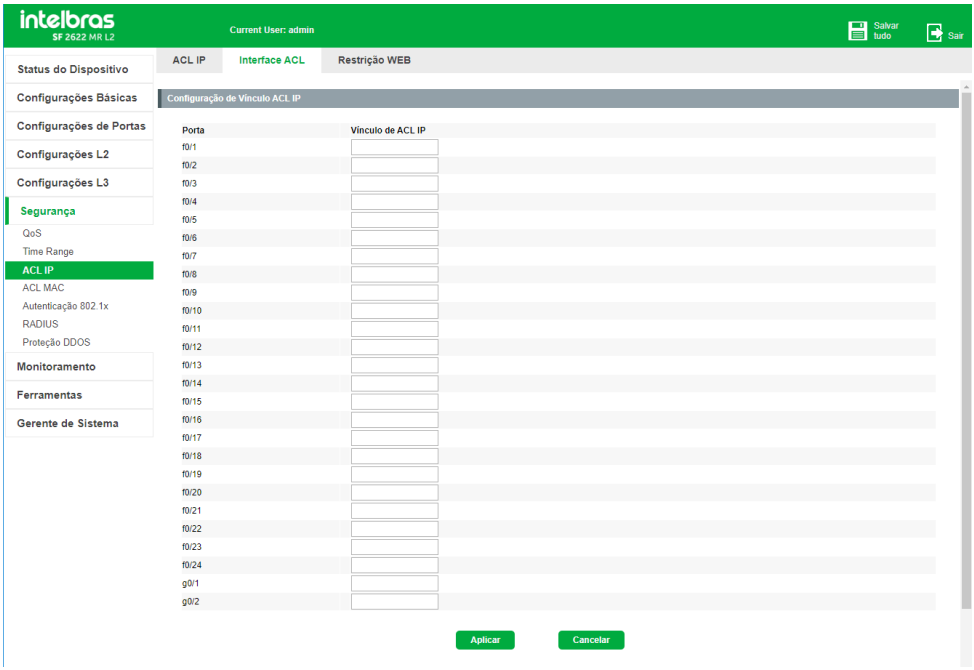
Criar regra/alterar regra

- » **Ação:** configura se os pacotes que combinarem com a regra serão permitidos ou rejeitados.
- » **Tipo de Src IP:** configura a verificação da origem do pacote. Esta pode ser feita de 3 maneiras:
  - » **any:** qualquer IP de origem irá combinar.
  - » **reverse-mask:** será especificado um IP de origem com máscara reversa para combinar.
  - » **Especificar IP:** será especificado um IP de origem com máscara direta para combinar.
- » **IP de Src:** IP de origem.
- » **Máscara de Src IP:** a entrada deste campo depende da opção escolhida em *Tipo de Src IP*.
  - » Máscara reversa para a opção *reverse-mask*.
  - » Máscara direta para as demais opções.
- » **Localização:** índice da regra na lista.
- » **Porta Src:** configura o modo de verificação da porta TCP/UDP de origem. A verificação pode ser feita especificando um comparador e uma porta de origem ou especificando um intervalo de portas de origem com modo *src-port-range*.

» **Porta Dest:** configura o modo de verificação da porta TCP/UDP de destino. A verificação pode ser feita especificando um comparador e uma porta de origem ou especificando um intervalo de portas de origem com modo *dst-port-range*.
» **Alcance da porta Dst:** intervalo de portas de destino.
» **ToS:** valor do campo *ToS* do cabeçalho do protocolo IP.
» **Procedence IP:** bits de precedência no campo *ToS* do cabeçalho IP.

8.3.2. Aplicação da ACL à interface

Nesta tela a ACL IP é aplicada em uma porta do switch.



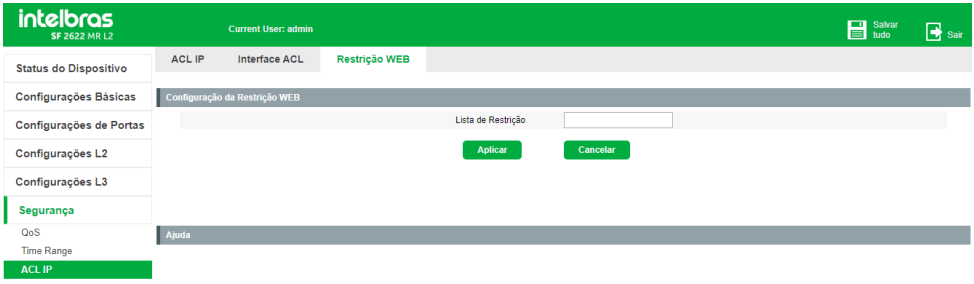
Aplicação de lista de acesso IP

Aplicação do IP ACL

» **Vínculo de ACL IP:** nome da ACL que será aplicada na respectiva porta.

8.3.3. Restrição web

Nesta tela é configurada a restrição de acesso web através da aplicação de uma ACL configurada.



Restrição web

Configuração da restrição web

» **Lista de restrição:** nome da ACL IP que será aplicada.

8.4. ACL MAC

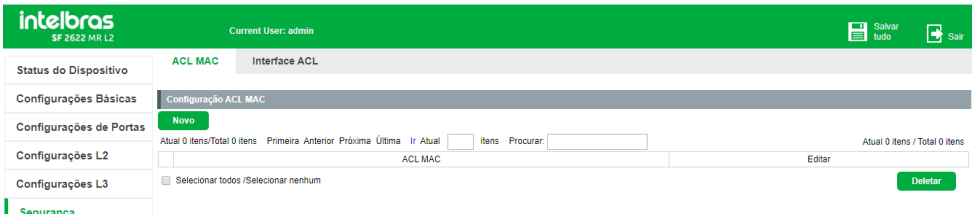
ACLs MAC podem analisar e processar os pacotes com base no endereço MAC de origem e de destino.

Para configurar a ACL MAC siga os seguintes passos:

1. Crie ACL MAC na seção *Criando um ACL MAC* da tela *Configuração de lista de acesso MAC*;
2. Crie as regras da ACL criada na seção *Novo regulamento de MAC ACL* da tela *Configuração de lista de acesso MAC;*
3. Aplique a ACL configurada na porta desejada na tela *Aplicação de lista de acesso MAC.*

8.4.1. Configuração ACL MAC

Nesta tela você pode criar, editar ou deletar as listas de ACL disponíveis.



Configuração de lista de acesso MAC – configuração de MAC ACL

Configuração de MAC ACL

Exibe uma lista com todas as MAC ACLs criadas.

» **Editar:** abre a seção *MAC ACL* para configuração das regras.

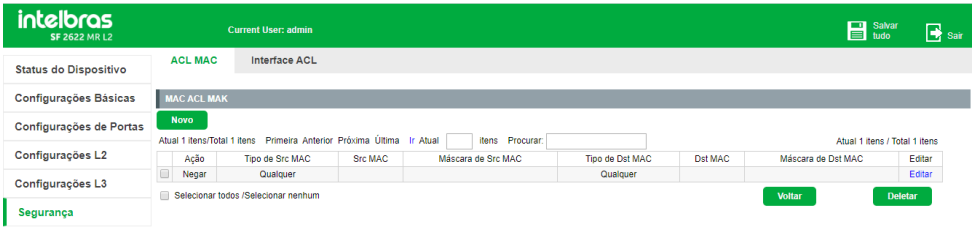
» **Novo:** abre a seção de *Criando um MAC ACL* para criação de uma nova ACL.

Configuração de Lista de acesso MAC – Criando um MAC ACL

Criando um MAC ACL

Esta seção possibilita a configuração de uma nova ACL.

» **Nome do MAC ACL:** nome descritivo da ACL MAC.



Configuração de lista de acesso MAC – MAC ACL

MAC ACL

Exibe uma lista com todas as regras da MAC ACL acessada.

» **Novo:** abre a seção *Novo regulamento de MAC ACL* para criação de uma nova regra.

Novo regulamento de MAC ACL

Na tela de *Configuração de lista de acesso MAC* selecione o nome da ACL criada na seção *Criando um MAC* ACL e clique em *Editar* e depois clique em *Novo*.

Configuração de lista de acesso MAC – novo regulamento de MAC ACL

Novo regulamento de MAC ACL

» **Autoridade:** selecione a ação a ser realizado com o pacote quando o mesmo combinar com a regra.

» **Tipo de Scr MAC:** configura a verificação da origem MAC do pacote. Esta pode ser feita de 3 maneiras:

  » **Any:** qualquer endereço MAC irá combinar.

  » **Host:** será especificado um MAC de origem para corresponder.

  » **Especificar MAC:** será especificado um MAC de origem com máscara para combinar.

» **Scr MAC:** MAC de origem.

» **Máscara de Src MAC:** a entrada deste campo depende da opção escolhida em *Tipo de Src MAC*.

» **Tipo de Dst MAC:** configura a verificação do destino do pacote. Esta pode ser feita de 3 maneiras:

  » **Any:** qualquer endereço MAC irá corresponder.

  » **Host:** será especificado um IP de origem com máscara direta para corresponder.

  » **Especificar MAC:** será especificado um MAC de origem com máscara para corresponder.

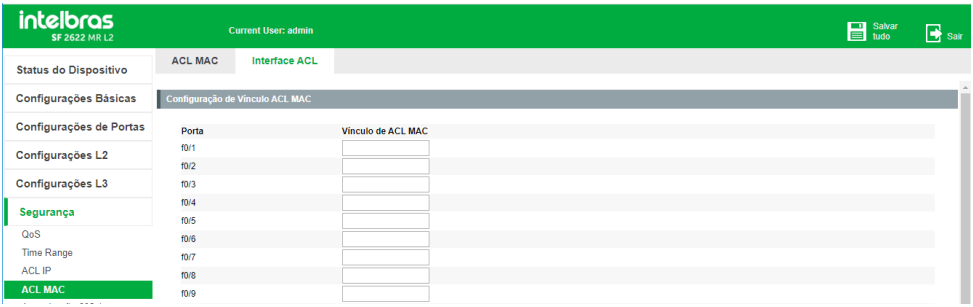
» **Dst MAC:** MAC de destino.

» **Máscara de Dst MAC:** a entrada deste campo depende da opção escolhida em *Tipo de Dst MAC*.

Obs.: *o endereço de MAC válido pode ter um dos seguintes formatos:* XXXXXXXXXXXX, XXXX.XXXX.XXXX, XX:XX:XX:XX:XX:XX, *e* XX-XX-XX-XX-XX-XX, *no qual X é um número Hex.*

8.4.2. Aplicação da ACL MAC à interface

Nesta tela é possível associar uma ACL de ingresso a uma porta especifica.



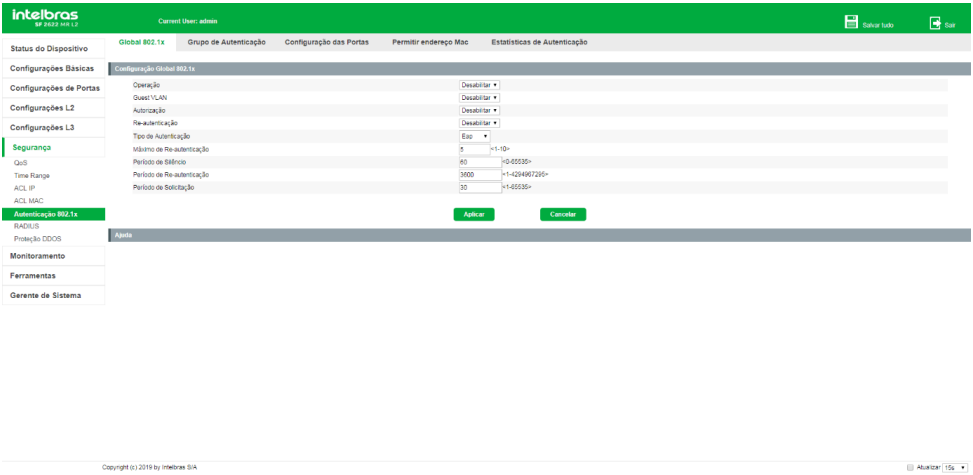
Aplicação de lista de acesso MAC – aplicação de MAC ACL

Aplicação de MAC ACL

» **ACL de ingresso:** nome da ACL a ser vinculada na porta.

8.5. Autenticação 802.1x

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.



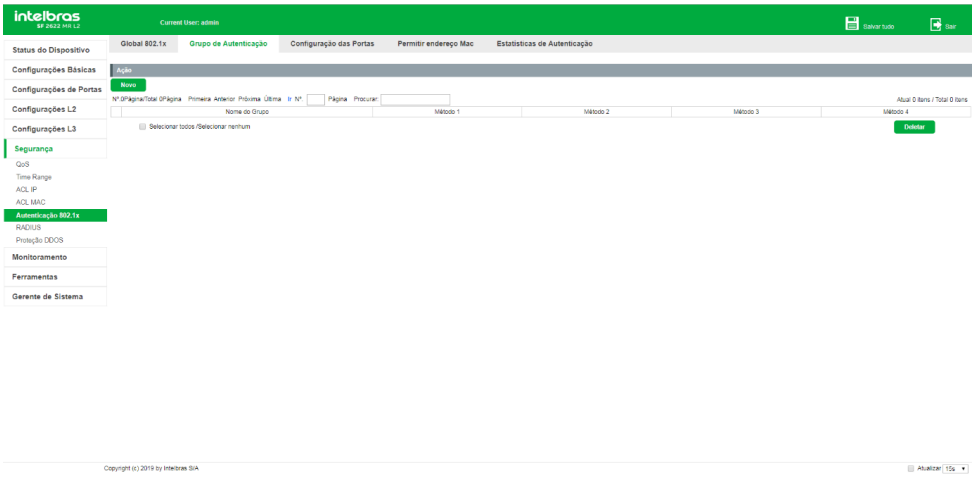
Global 802.1x

8.5.1. Configuração de autenticação por porta

Nesta página pode ser configurado o protocolo 802.1x de maneira global permitindo o acesso às portas por meio de autenticação. Para isso é necessário habilitar o protocolo no campo *Operação*.

Também pode ser habilitada a necessidade de configurar uma VLAN de autenticação com o servidor, se o suplicante terá seu pedido de autorização aceite ou não, as configurações relacionadas a reautenticação além do tipo de autenticação (CHAP ou EAP) trocadas entre o suplicante e o servidor.

8.5.2. Grupos de autenticação

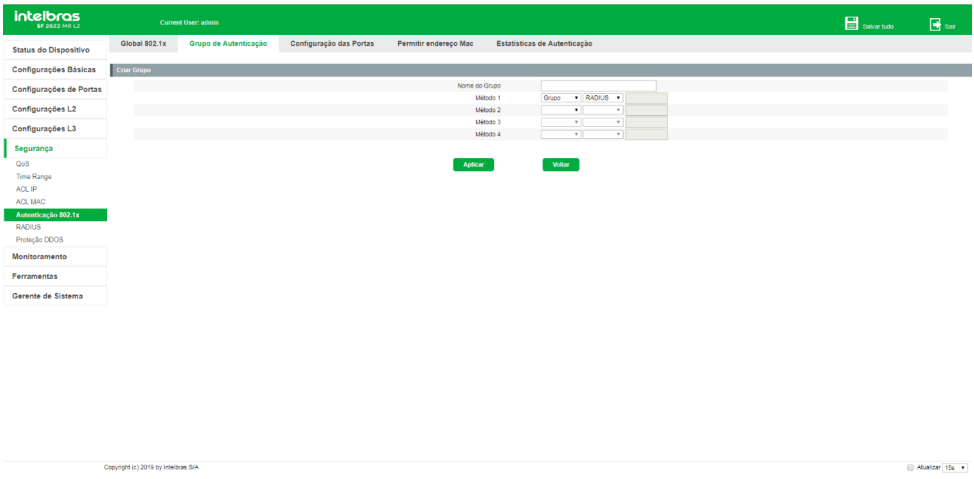


Grupos de autenticação

Ação

Nesta página são informadas as configurações dos métodos de autenticação dentro dos grupos de autenticação.

Para realizar estas configurações clique no botão *Novo*. Para editar uma configuração já realizada clique em *Editar*. A tela a seguir será exibida.



Grupos de autenticação – criar grupo

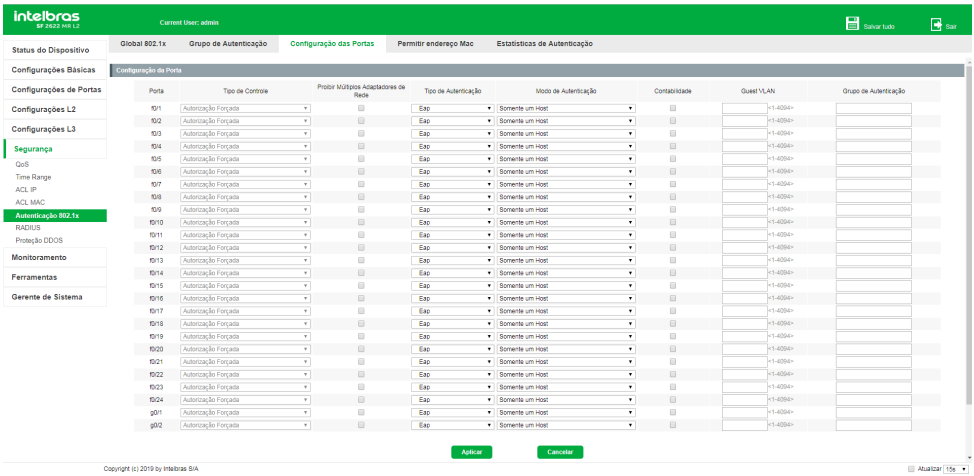
Criar grupo

Nesta tela são criados os grupos de autenticação. Para isso é preciso informar o nome para o grupo e o método de autenticação.

Caso o método de um grupo seja do tipo RADIUS, será necessário efetuar as configurações do servidor RADIUS no meu RADIUS que está localizando no menu principal *Segurança*.

Caso o grupo tenha somente um método, mas não seja informando que o método seguinte contenha o valor *Nenhum*, o grupo permitirá todos os métodos, mas será utilizado como preferência o primeiro método adotado. Se existir somente um método, deve ser configurado o valor *Nenhum*.

8.5.3. Configuração das portas



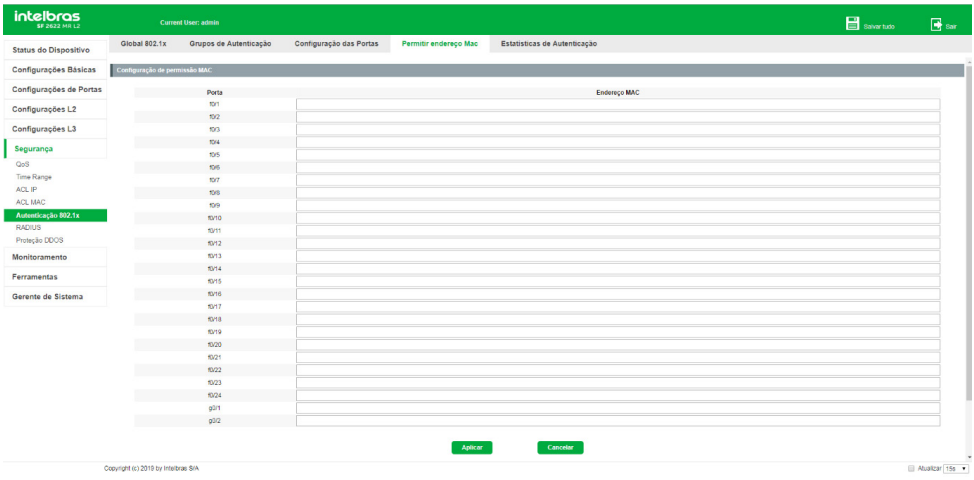
Configuração das portas

Configuração da porta

Nesta tela são configurados os parâmetros de autenticação para cada porta do switch.

- **Porta:** indicação da porta para configuração.
- **Tipo de controle:** seleciono a autenticação 802.1x nas portas.
  - **Auto:** a porta deve passar pelo processo de autenticação. Neste modo é possível configurar a função *Guest VLAN.*
  - **Autorização forçada:** a porta sempre estará autenticada. Mesmo que não tenha outro equipamento conectado na porta ela estará autenticada. A porta não precisa que o suplicante se autentique para liberar o acesso.
  - **Autorização não forçada:** neste modo a porta não permitirá autenticação. Ela negará toda e qualquer solicitação de autorização.
- **Proibir múltiplos adaptadores de rede:** configura a interface a proibir múltiplos adaptadores de rede.
- **Tipo de autenticação:** pode ser escolhido entre:
  - **EAP:** protocolo de autenticação.
  - **CHAP:** protocolo de autenticação.
- **Modo de autenticação:** configura como a porta irá realizar a autenticação.
  - **Somente um host:** apenas um host será autenticado na porta.
  - **Múltiplos hosts:** com apenas um usuário autenticado a porta será liberada para acesso sem necessidade de autenticação de outros usuários.
  - **Autenticação Múltipla:** todos os usuários devem se autenticar para liberar o acesso.
- **Contabilidade:** habilita as estatísticas de autenticação 802.1x na interface.
- **Guest VLAN:** é possível configurar uma Guest VLAN. Se a autenticação for autorizada, a porta pertencerá na VLAN da própria porta. Após uma desconexão da porta, a mesma volta para a Guest VLAN. A porta deve estar no modo *TRUNK*.
- **Grupo de autenticação:** configuração do grupo de autenticação.

8.5.4. Permitir endereço MAC

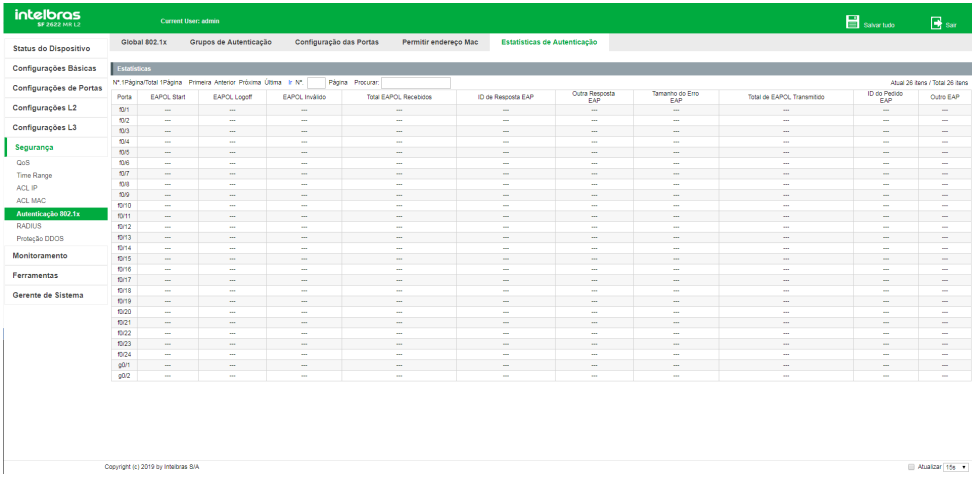


Permitir endereço MAC

Configuração de permissão MAC

Nesta tela são configurados os endereços MAC em uma porta, somente esse endereço poderá se autenticar na porta.

8.5.5. Estatísticas de autenticação



Estatísticas de autenticação

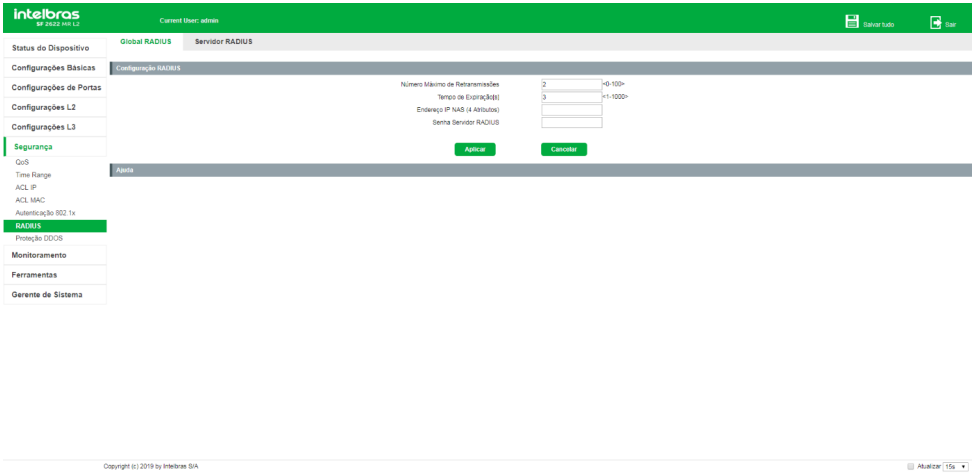
Estatísticas

Nesta tela são informadas as estatísticas de pacotes de autenticação das interfaces.

8.6. RADIUS

Configuração do servidor RADIUS e seus parâmetros de autenticação.

8.6.1. Global RADIUS

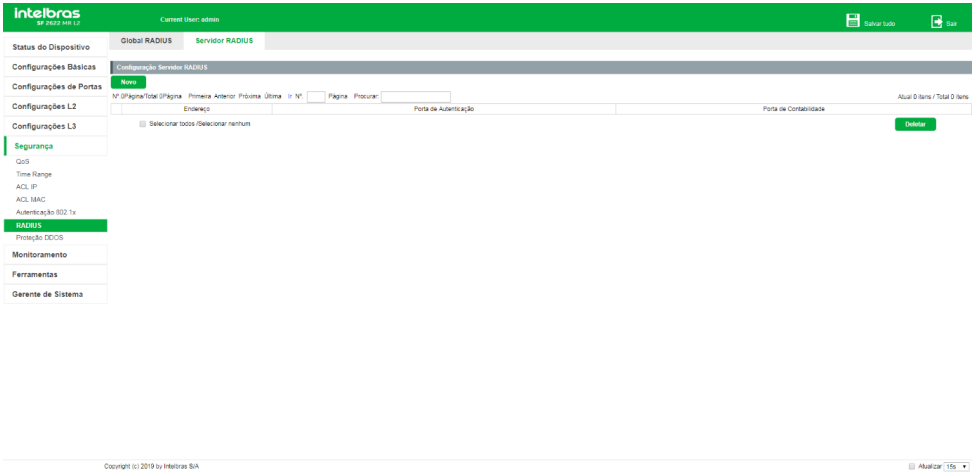


Global RADIUS

Configuração RADIUS

Nesta tela são configurados o número máximo de retransmissões, o tempo de expiração, o endereço IP NAS dos pacotes *Access-Request* e também a senha de acesso ao servidor RADIUS.

8.6.2. Servidor RADIUS



Servidor RADIUS

Configuração servidor RADIUS

Nesta tela são informadas as configurações do servidor RADIUS e as portas de autenticação e contabilidade.

Para realizar estas configurações clique no botão *Novo*. A tela a seguir será exibida.

Servidor RADIUS – novo servidor RADIUS

Novo servidor RADIUS

Nesta tela são configurados o endereço IP do servidor RADIUS e as portas de autenticação e contabilidade.

8.7. Proteção DoS

Ataques DoS (*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 (DoS).

Proteção DoS – configuração DoS

8.7.1. Proteção DoS

Configuração DoS

- **ICMP:** descarta pacotes ICMP IPv4/IPv6 com tamanho maior que o valor máximo.
- **IPv4/IPv6:** descarta pacotes com endereços IP de origem e destino iguais.
- **L4 Port:** descarta pacotes com portas de origem e destino iguais.
- **TCP flags:** descarta pacotes TCP com flags inválidas.
- **TCP frags:** descarta pacotes com cabeçalho TCP menores que 20 bytes.

9. Monitoramento

9.1. SNMPv1 | v2

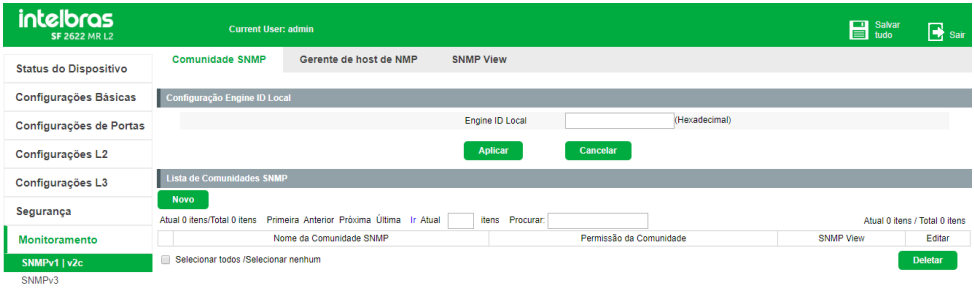
As versões do SNMP adotadas pela Estação de Gerenciamento e o Agente SNMP devem ser a mesma. Caso contrário, a Estação de Gerenciamento SNMP e o Agente SNMP podem não se comunicar corretamente. Você pode selecionar o modo de gerenciamento com níveis de segurança adequado as suas exigências de aplicação.

O SNMPv1 adota autenticação utilizando o nome da comunidade. O nome da comunidade é usado para definir a relação entre a estação de gerenciamento SNMP e o agente SNMP. Os pacotes SNMP que não conseguirem aprovação de autenticação serão descartados.

O SNMPv2c também adota a autenticação utilizando o nome da comunidade. É compatível com SNMP v1, com algumas funcionalidades a mais, como implementação de comunicação Gerente-Gerente e aumento no nível de segurança.

Com a função *SNMP* configurada, os administradores de rede podem monitorar o desempenho da rede, detectar as falhas e configurar os dispositivos de rede.

9.1.1. Comunidade SNMP



SNMP de configuração global

Configuração engine ID local

Nesta página pode ser configurado o EngineID local do switch. Este parâmetro é utilizado pelos clientes remotos. O EngineID é uma sequência de caracteres hexadecimal únicos, usados para identificar o switch.

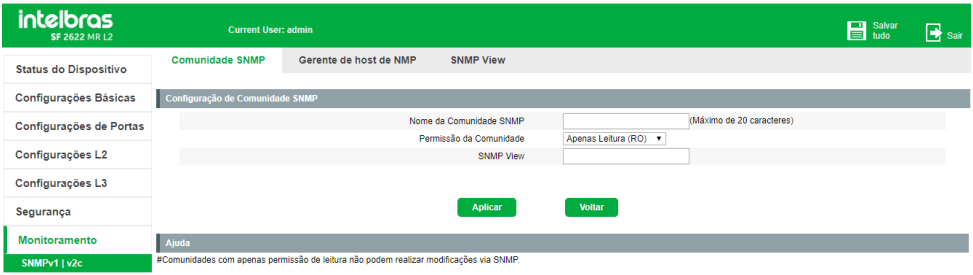
Lista de comunidades SNMP

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.

Nesta tela são informadas as configurações realizadas para comunidade SNMP:

- **Nome de comunidade de SNMP:** exibe o nome da comunidade.
- **Permissão da comunidade:** define o tipo de permissão para a comunidade.
- **Apenas para leitura:** neste modo, a comunidade terá permissão somente de leitura, nenhuma alteração poderá ser feita.
- **Apenas para modificação:** neste modo, a comunidade terá permissão de configuração, podendo realizar alterações.

Para realizar estas configurações clique no botão *Novo*. Para editar uma configuração já realizada clique em *Editar*. A tela a seguir será exibida.

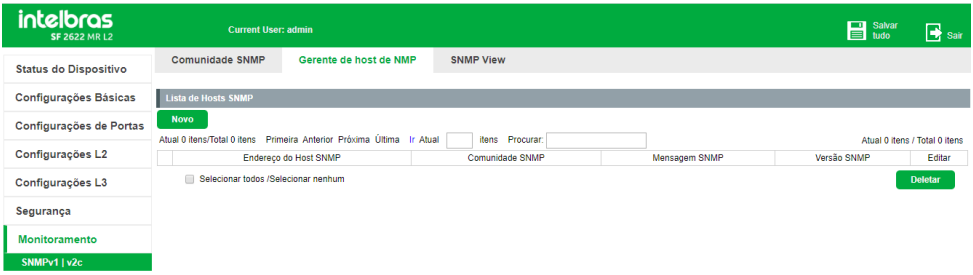


Configuração de comunidade de SNMP – gestão de comunidade de SNMP

Configuração de comunidade de SNMP

Nesta página pode ser configurado o nome para a comunidade e o atributo da mesma. Se a comunidade criada será para leitura ou configuração.

9.1.2. Gerente de host de SNMP



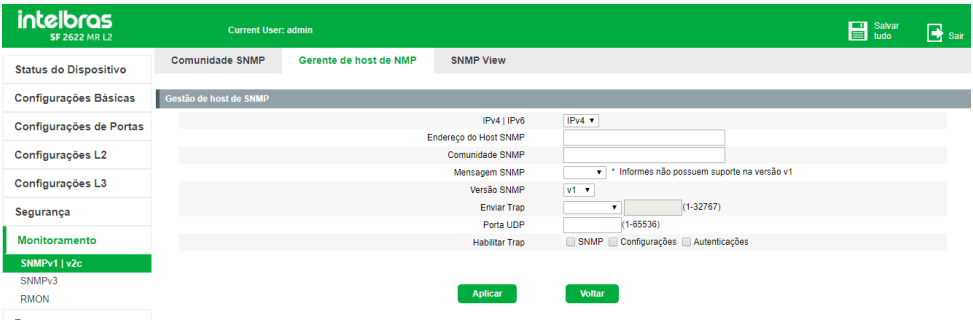
Gerente de host de SNMP

Gerente de comunidade de SNMP

Permite configurar hosts para receber traps ou informações SNMP.

Nesta tela são informadas as configurações realizadas para hosts SNMP. Como IP do host, string da comunidade, tipo da comunidade (informe ou traps) e versão do SNMP (v1, v2c ou v3).

Para realizar estas configurações clique no botão *Novo*. Para editar uma configuração já realizada clique em *Editar*. A tela a seguir será exibida.



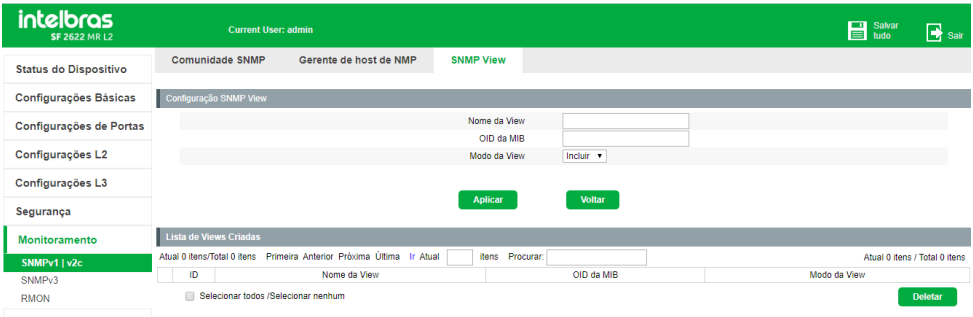
SNMPv1 | v2 - gerente de host de SNMP

Gerente de host de SNMP

Nesta página é possível configurar o host que receberá as informações SNMP configuradas.

- **IPv4 | IPv6:** escolha entre IPv4 e IPv6.
- **Endereço do host SNMP:** endereço IP do host que vai receber as informações SNMP.
- **Comunidade SNMP:** pode limitar o acesso ao agente SNMP da estação de gerenciamento SNMP, funcionando como uma senha.
- **Tipo de mensagem SNMP:**
  - **Informes:** apenas informação. Não possui suporte para versão de SNMP v1.
  - **Armadilhas:** envia traps.
- **Versão SNMP:** SNMP v1, v2c ou v3.
- **Enviar trap:** informe um índice para o envio de trap.
- **Deny:** nega o envio de trap.
- **Permit:** permite o envio de trap.
- **Porta UDP:** número da porta UTP para o envio das mensagens SNMP.
- **Habilitar Traps:** selecione quais informações de traps serão enviadas, como SNMP, configure e authentication.

9.1.3. SNMP view



SNMP View

Configuração SNMP view

Permite configurar as MIBs que serão permitidas ou excluídas do gerenciamento SNMP.

Para realizar estas configurações clique no botão *Novo*. Para editar uma configuração já realizada clique em *Editar*. A tela a seguir será exibida.

SNMP view config

Nesta página é possível configurar o host que receberá as informações SNMP configuradas.

- **Nome da view:** digite o nome de identificação da view. Cada view pode incluir mais de uma entrada com o mesmo nome.
- **MIB OID:** digite o OID utilizado pela view.
- **Modo da view:** selecione o tipo de entrada da view.
- **Include:** inclui para o gerenciamento da view o OID especificado.
- **Excluded:** exclui do gerenciamento da view o OID especificado.

9.2. SNMPv3

Baseado em SNMPv1 e v2c, o SNMPv3 aumenta em muito a segurança e capacidade de gerenciamento. Adota autenticação VACM (*View-based Access Control Model*) e USM (*User-Based Security Model*). O usuário pode configurar a autenticação e as funções de criptografia. A função de autenticação é utilizada para limitar o acesso de usuários ilegais, autenticando o remetente do pacote. Enquanto isso, a função de criptografia é usada para criptografar os pacotes transmitidos entre a estação de gerenciamento SNMP e o agente SNMP, de modo a evitar que qualquer informação seja capturada. As múltiplas combinações da função de autenticação e criptografia garantem uma comunicação mais confiável entre a estação de gerenciamento SNMP e o agente SNMP.

9.2.1. Configuração do grupo SNMPv3

Configuração do grupo SNMPv3

Configuração do grupo SNMPv3

Nesta página é informado os grupos SNMPv3 criados para controlar o acesso à rede, fornecendo aos usuários de vários grupos diferentes, permissões de leitura, escrita e notificação.

Para realizar estas configurações clique no botão *Novo*. Para editar uma configuração já realizada clique em *Editar*. A tela a seguir será exibida.

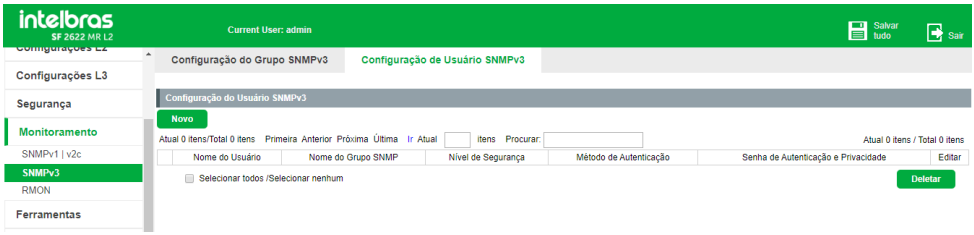
SNMPv3 - configuração do grupo SNMPv3

Configuração do grupo SNMPv3

Nesta página são configurados os grupos SNMPv3 para controlar o acesso à rede.

- **Nome do grupo SNMP:** nome para o grupo SNMPv3.
- **Nível de segurança:** selecione o nível de segurança para grupos SNMPv3.
  - **NoAuthNoPriv:** não realiza autenticação e criptografia.
  - **AuthNoPriv:** realiza autenticação porém não realiza criptografia.
  - **AuthPriv:** realiza autenticação e criptografia.
- **View de notificação:** insira o nome da view para notificação. A View de Notificação poderá enviar notificações a estação de gerenciamento SNMP.
- **View de leitura:** insira o nome da view para acesso de leitura. A View de Leitura somente poderá ser lida, não é possível modificá-la.
- **View de escrita:** insira o nome da view para acesso de escrita. A View de Escrita poderá ser lida e alterada.

9.2.2. Configuração do usuário SNMPv3



Configuração de usuário SNMPv3

Configuração de usuário SNMPv3

Nesta página é informado o usuário que será o gerente do grupo SNMPv3.

Para realizar estas configurações clique no botão *Novo*. Para editar uma configuração já realizada clique em *Editar*. A tela a seguir será exibida.

SNMPv3 - configuração de usuário SNMPv3

Configuração de usuário SNMPv3

Nesta página são configurados os usuários para gerenciar os grupos SNMPv3.

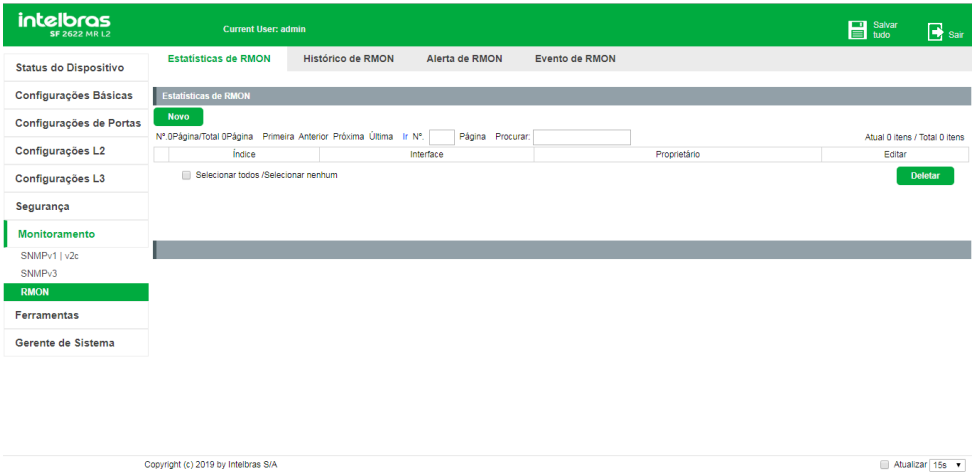
- **Nome do usuário:** nome do usuário.
- **Nome do grupo SNMP:** nome para o grupo SNMPv3.
- **Nível de segurança:** selecione o modo de autenticação para o usuário SNMPv3.
  - **NoAuthNoPriv:** não realiza autenticação e criptografia.
  - **AuthNoPriv:** realiza autenticação porém não realiza criptografia.
  - **AuthPriv:** realiza autenticação e criptografia.
- **Método de autenticação:** selecione o modo de autenticação para o usuário SNMPv3.
  - **sha:** a autenticação da porta é realizada através de SHA (*Secure Hash Algorithm*). Esse modo de autenticação é mais seguro que o modo *MD5*.
  - **md5:** a autenticação da porta usa o algoritmo HMAC-MD5.
- **Método de privacidade:** utiliza o método de encriptação DES.
- **Senha de autenticação e privacidade:** digite a senha configurada utilizada na criptografia. Ao utilizar o nível de privacidade *AuthPriv* a senha utilizada na autenticação e privacidade será a mesma.

9.3. 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.

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

Estatísticas de RMON

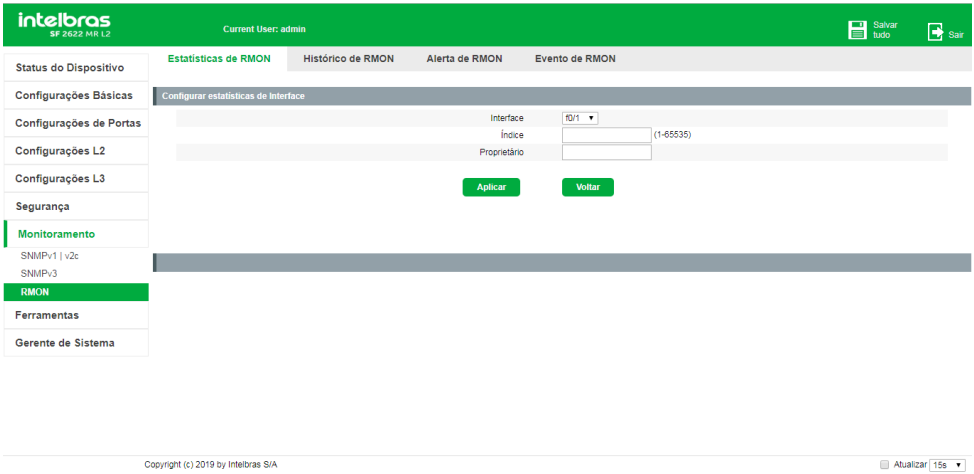


Estatísticas de RMON

Estatísticas de RMON

Nesta página pode ser configurada a interface para registro das estatísticas da porta para a função *RMON*. As estatísticas para a porta estão disponíveis via interface CLI através do comando *Show rmon*.

Para habilitar uma interface a coletar informações, faça a configuração clicando no botão *Novo*. A tela a seguir será exibida.



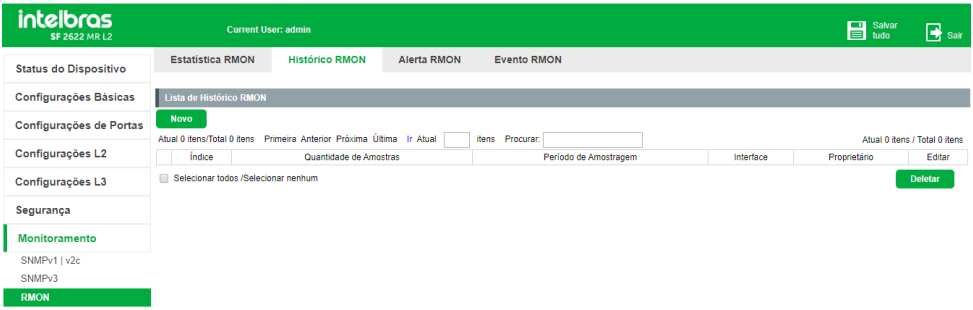
Estatísticas de RMON – configurar estatísticas de Interface

Configurar estatísticas de interface

Nesta tela são realizadas as configurações das interfaces para monitoramento da função *RMON.*

No campo *Proprietário* pode ser inserido texto com o máximo de 31 caracteres.

9.3.1. Histórico de RMON



Histórico de RMON

Histórico de RMON

Nesta página são informados os históricos para a função *RMON.*

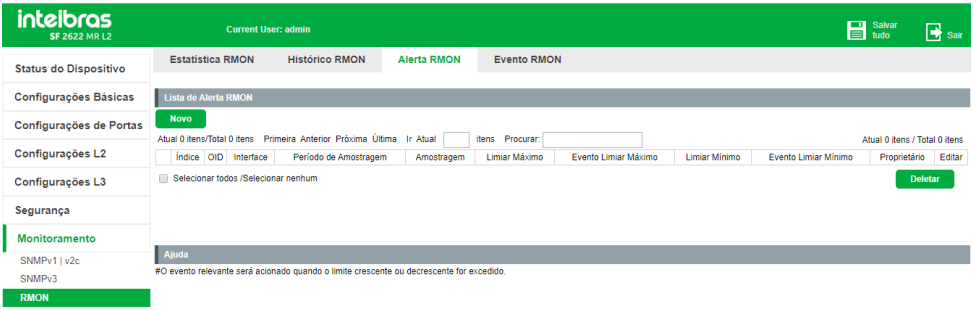
Para habilitar uma interface a monitorar as informações, faça a configuração clicando no botão *Novo.* A tela a seguir será exibida.

Histórico de RMON – configuração de histórico de Interface

Configuração de histórico de interface

Nesta tela são realizadas as configurações da interface para monitoramento, o número de amostras e o intervalo de tempo em segundos para salvar as informações da amostra e o nome do usuário para a função *RMON.*

9.3.2. Alerta de RMON



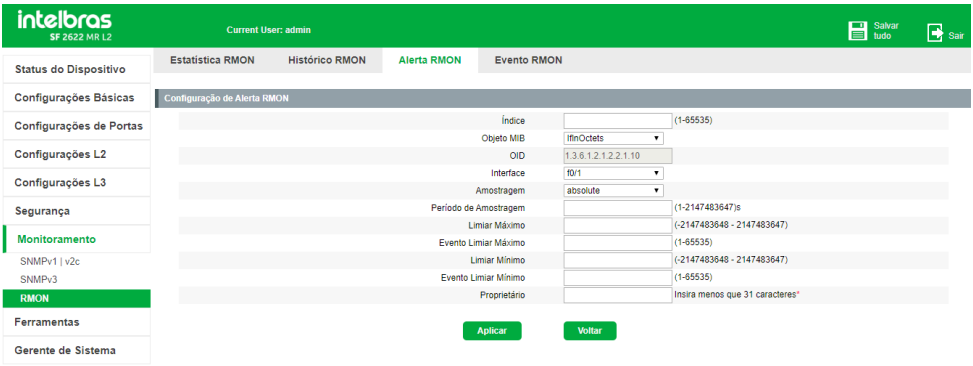
Alerta de RMON

Alerta de RMON

Nesta página são informados os alarmes para a função *RMON*.

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.

Para configurar uma interface a monitorar os limites para o disparo de um alarme, faça a configuração clicando no botão *Novo*. A tela a seguir será exibida.



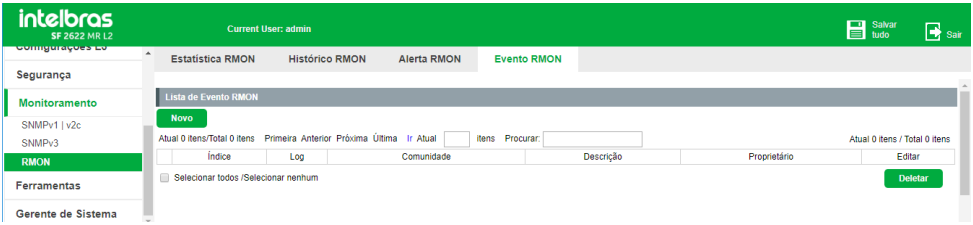
Alerta de RMON – configuração de alerta de RMON

Configuração de alerta de RMON

Nesta tela são realizadas as configurações das estatísticas e alarmes para a função *RMON*. A seguir estão descritos os parâmetros de configuração:

- **Índice:** exibe o índice da entrada.
- **Objeto MIB:** informação do objeto que deve ser monitorado.
- **Interface:** indicação da porta para configuração.
- **Amostragem:** especifique o método de amostragem da variável selecionada para comparar os valores entre os limites.
  - **Absolute:** 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.
- **Período de amostragem:** intervalo de amostragem em segundos.
- **Limiar máximo:** digite o valor para o contador disparar o alarme caso o valor máximo seja excedido.
- **Evento limiar máximo:** selecione o índice para o evento do *Limite crescente*.
- **Limiar mínimo:** digite o valor para o contador disparar o alarme caso o valor mínimo seja excedido.
- **Evento limiar mínimo:** selecione o índice para o evento do *Evento decrescente*.
- **Proprietário:** informe o nome do dispositivo ou usuário que definiu regra.

9.3.3. Evento de RMON

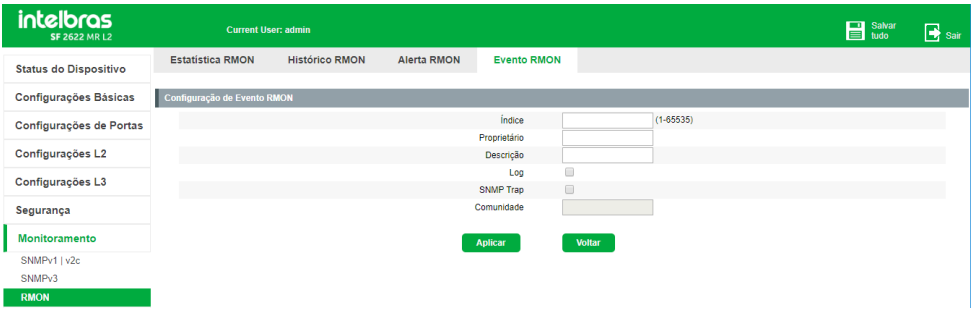


Evento de RMON

Evento de RMON

Nesta página são informados os eventos para a função *RMON.*

Para configurar uma interface a monitorar os limites para o disparo de um alarme, faça a configuração clicando no botão *Novo*. A tela a seguir será exibida.



Evento de RMON – Configuração de evento de RMON

Configuração de evento de RMON

Nesta tela são realizadas as configurações dos eventos para a função *RMON.*

A seguir estão descritos os parâmetros de configuração:

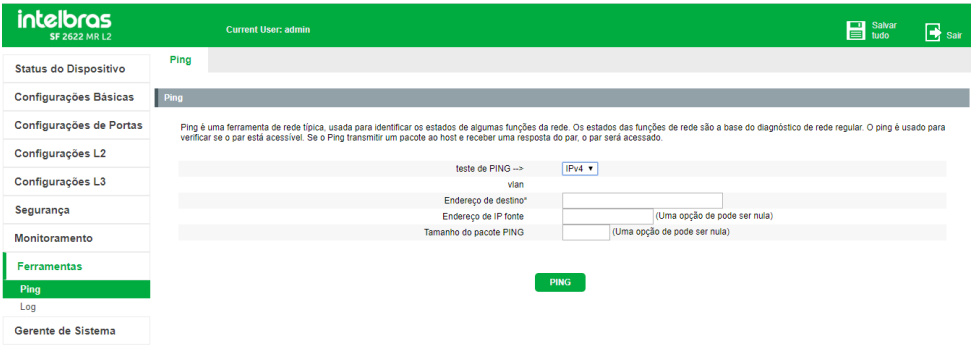
- **Índice:** exibe o índice da entrada.
- **Proprietário:** informe o nome do dispositivo ou usuário que definiu regra. Pode ter no máximo 31 caracteres.
- **Descrição:** texto com descrição do evento. Pode ter no máximo 127 caracteres.
- **Log:** se o log está habilitado, os itens serão inseridos na tabela de log quando o evento for acionado.
- **SNMP trap:** se a trap estiver habilitada, ela será gerada com o nome da comunidade do evento.
- **Comunidade:** informa o nome da comunidade SNMP. Pode ter no máximo 31 caracteres.

10. Ferramenta

Este switch oferece funções de teste de Ping e Log para um melhor diagnostico da rede.

10.1. Ping

A função *Ping* testa a conectividade entre o switch e um dispositivo específico da rede, facilitando a localização de falhas.



Ping

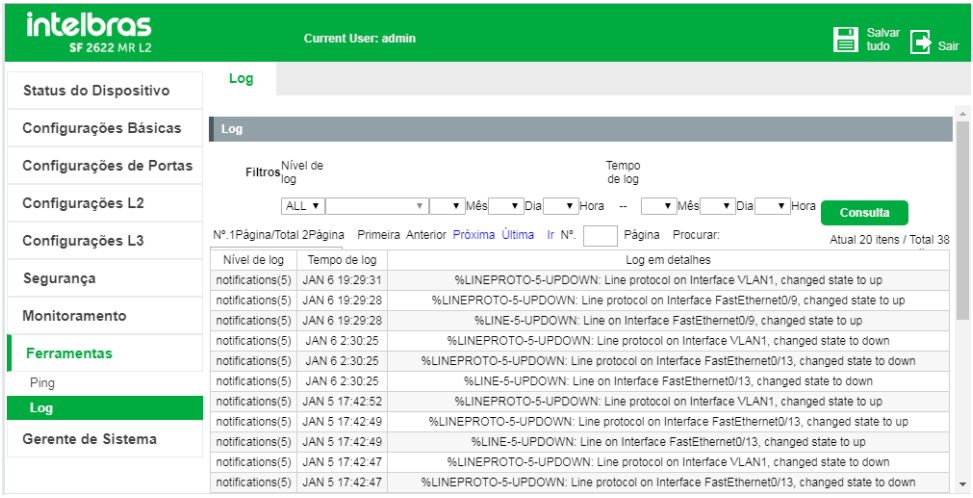
10.1.1. Ping

Ping

- **Protocolo:** selecione entre IPv4 e IPv6.
- **VLAN:** quando em IPv6, aponte a VLAN na qual a solicitação ping ocorrerá.
- **Endereço de destino:** digite o endereço IP do dispositivo de destino para o teste de Ping.
- **Endereço de IP fonte:** digite o endereço de IP de origem do Ping (opcional).
- **Tamanho:** digite o tamanho dos pacotes enviados durante o Ping (opcional).

10.2. Log

O sistema de Log do switch pode registrar, classificar 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.



Log

Os logs do switch são classificados nos seguintes níveis.

Criticidade	Nível	Descrição
Emergências	0	O sistema está inutilizável
Alertas	1	Devem ser tomadas medidas imediatamente
Crítico	2	Condições críticas
Erros	3	Condições de erro
Avisos	4	Condições de alerta
Notificações	5	Condições normais, mas significativas
Informações	6	Informações de mensagens
Depuração	7	Nível de depuração de mensagens
Dump	8	Demais eventos

É possível filtrar os resultados de forma personalizada especificando um intervalo de tempo, nível de Log, e criticidade.

As seguintes informações são exibidas na tela:

- **Nível de Log:** selecione entre as opções:
  - **All:** todos os níveis de criticidade.
  - **<:** menor que a criticidade selecionada.

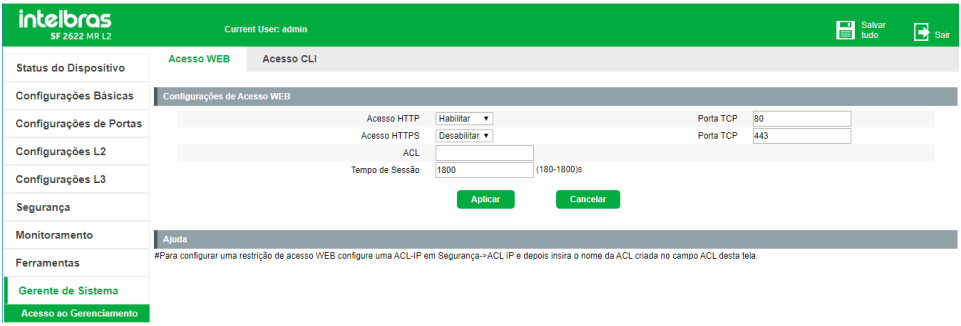
» **=:** igual a criticidade selecionada.
» **>:** maior que a criticidade selecionada.
» **Criticidade:** selecione a criticidade de 0 a 8 conforme a tabela anterior.
» **Tempo de log:** digite o início e fim do intervalo desejado.
» **Log em detalhes:** exibe as informações sobre o evento.

11. Gerente de sistema

Nesse menu você pode configurar os usuários, o gerente de log, fazer backup das configurações/firmware, atualizar o firmware e também reiniciar manualmente o switch.

11.1. Acesso ao gerenciamento

11.1.1. Acesso Web



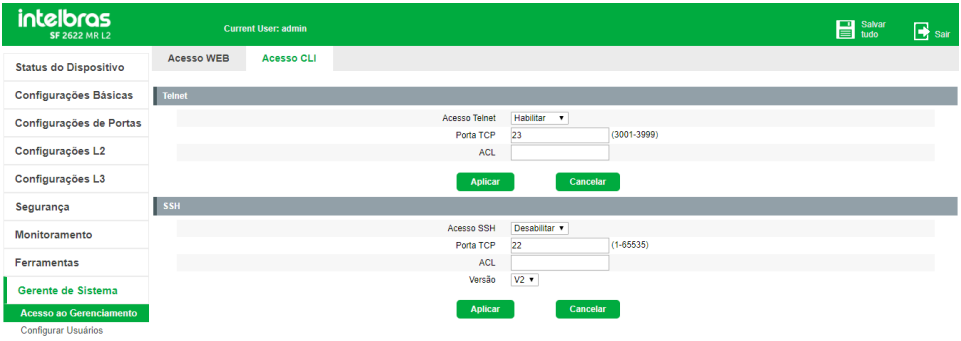
Acesso Web

Nesta tela são realizadas as configurações de acesso ao switch através da interface web.

A seguir estão descritos os parâmetros de configuração:

» **Acesso HTTP:** habilita ou desabilita o acesso web através do protocolo HTTP.
» **Acesso HTTPs:** habilita ou desabilita o acesso web através do protocolo HTTPs.
» **ACL:** Entre com a ID de uma regra ACL para controlar o acesso web.
» **Porta TCP:** entre com o número de porta TCP que será utilizado para o respectivo acesso web.
» **Tempo de sessão:** entre com o número em segundos que a sessão de acesso web ficará ativa em caso de inatividade do usuário.

11.1.2. Acesso CLI



Acesso CLI

Telnet

Nesta tela você pode habilitar ou desabilitar o acesso via Telnet, escolher a porta de acesso e até apontar uma regra ACL para Gerenciar o acesso via Telnet.

Configuração de Telnet

- » **Acesso Telnet:** habilita/desabilita a função Telnet.
- » **Porta TCP:** indica a porta através da qual o Telnet realizará a conexão.
- » **ACL:** Indique uma regra ACL para gerir o acesso Telnet.

SSH

O SSH é composto por um servidor e um cliente, possui duas versões, V1 e V2 que não são compatíveis entre si. Na comunicação entre o servidor e o cliente, o SSH pode negociar em qual versão irá operar e qual algoritmo de criptografia irá utilizar. Após realizar com sucesso a autonegociação, o cliente envia a solicitação de autenticação ao servidor para realização do login. Somente após autenticado, a comunicação entre o cliente e o servidor será estabelecida.

Nesta tela você pode habilitar ou desabilitar o acesso via SSH, escolher a porta de acesso e até apontar uma regra ACL para Gerenciar o acesso via Telnet.

Configuração de SSH

- » **Acesso SSH:** habilita/desabilita a função *SSH.*
- » **Porta TCP:** indica a porta através da qual o SSH realizará a conexão.
- » **ACL:** Indique uma regra ACL para gerir o acesso SSH.
- » **Versão:** configura a versão SSH.

11.2. Configurar usuários

O submenu *Configurar usuários* é utilizado para realizar configurações de usuários e senhas com níveis de acessos diferentes ao logar na página de gerenciamento web. Este submenu possui os seguintes itens: *Configurar usuários, Gerente de grupo, Grupo de senha* e *Grupo de autenticação.*

11.2.1. Configurar usuários

Nesta tela você pode criar usuários e configurar seus níveis de acesso que serão utilizados ao acessar a página de gerenciamento web. O switch possui dois níveis de acesso: *Usuário limitado* e *Administrador de sistema.* No nível de acesso Usuário limitado, somente é possível visualizar as configurações do switch, já no nível de acesso Administrador de sistema, é possível realizar a configuração de qualquer função presente no switch.

Obs.: *quando existir apenas um usuário Administrador de sistema, este não poderá ser excluído.*

Gestão de usuário

Gestão de usuário

- » **Nome de usuário:** nome do usuário criado.
- » **Permissão de usuário:** nível de permissão do usuário.
- » **Status do usuário:** situação do usuário criado.
- » **Editar:** possibilita editar as informações do usuário.
- » **Deletar:** exclui um usuário.
- » **Novo:** abre a seção de *Gestão de usuário.*

Configurar usuários – gestão de usuário

Gestão de usuário

Esta seção possibilita a configuração de um novo usuário e a criação de sua senha de acesso.

- » **Nome de usuário:** digite o nome de usuário que será criado.
- » **Senha:** digite uma senha acesso para o usuário.
- » **Confirmação de senha:** digite novamente a senha de acesso do usuário.
- » **Grupo senha:** digite o grupo de senha ao qual o usuário pertence (não obrigatório).
- » **Grupo de autenticação:** digite o grupo de autenticação ao qual o usuário pertence (não obrigatório).

11.2.2. Grupo de senha

Nesta página é possível criar um grupo de senha, personalizando as regras de composição de senhas e validade de uso.

Grupo de senha

Grupo senha

- **Número de série:** identifica o grupo de senha.
- **Nome de Pass-Group:** nome do grupo senha
- **O mesmo que o nome de usuário:** mostra se a regra foi criada.
- **Min. Comprimento:** mostra o valor definido.
- **Validade:** mostra o valor definido.
- **Letra minúscula:** mostra se a regra foi criada.
- **Letra maiúscula:** mostra se a regra foi criada.
- **Caractere especial:** mostra se a regra foi criada.
- **Editar:** possibilita editar as definições do grupo senha.
- **Novo:** abre a seção *Grupo senha* para a configuração de um novo grupo.

Grupo senha

Grupo senha

- **Nome do grupo senha:** digite um nome para o grupo.
- **Usuário e senha iguais:**
  - **Permitir:** permite a criação de senha com os mesmos caracteres nos campos *Usuário* e *Senha* (Ex.: Usuário *admin*/ Senha *admin*).
  - **Não permitir:** não permite a criação de usuário e senha iguais.
- **Números:**
  - **Deve conter:** obriga o uso de caractere numérico.
  - **Nenhum comando:** não estabelece a regra.
- **Letras minúsculas:**
  - **Deve conter:** obriga o uso de letras minúsculas.
  - **Nenhum comando:** não estabelece a regra.
- **Letras maiúsculas:**
  - **Deve conter:** obriga o uso de letras maiúsculas.
  - **Nenhum comando:** não estabelece a regra.
- **Caracteres especiais:**
  - **Deve conter:** obriga o uso de caractere especial.
  - **Nenhum comando:** não estabelece a regra.
- **Comprimento mínimo:** defina o número mínimo de caracteres (não obrigatório).
- **Validade do usuário:** define o tempo de validade do usuário (não obrigatório).

11.2.3. Grupo de autenticação

Nesta tela é possível criar ou deletar grupos de autenticação e configurá-los como *Administrador do sistema* ou *Usuário limitado*.

Grupo de autenticação

Grupo de autenticação

- » **Número de série:** identifica o grupo de autenticação.
- » **Nome do grupo de autenticação:** nome do grupo de autenticação.
- » **Privilégio:** administrador do sistema ou usuário limitado.
- » **Editar:** abre a seção *Grupo de autenticação* para a alteração de nível de acesso
- » **Novo:** abre a seção *Grupo de autenticação* para a configuração de um grupo e nível de acesso.

Grupo de autenticação

Grupo de autenticação

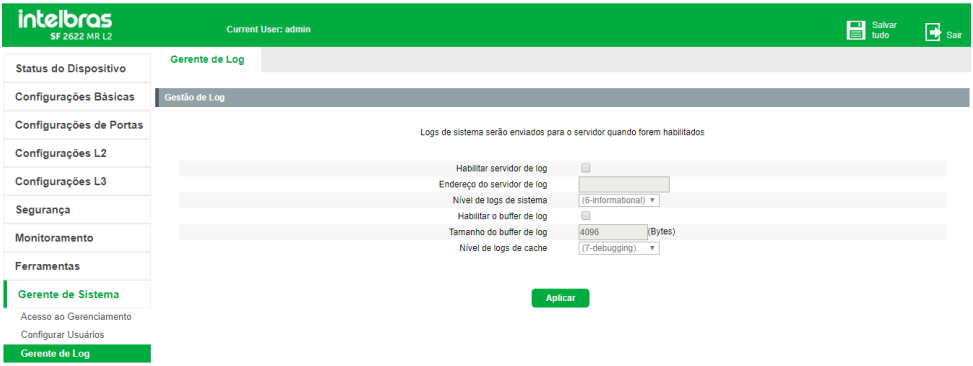
- » **Nome do grupo de autenticação:** digite o nome de usuário que será criado.
- » **Privilégio:** escolha o nível de permissão do grupo.

***Obs.:** não é permitido o uso de caractere especial.*

11.3. Gerente de log

Na tela a seguir é possível determinar um servidor para armazenamento externo desses logs, assim como o tamanho da memória de buffer e especificar um nível de criticidade a ser armazenada.

Por padrão os logs são salvos e armazenados na memória cache do switch.



Gerente de log - gestão de log

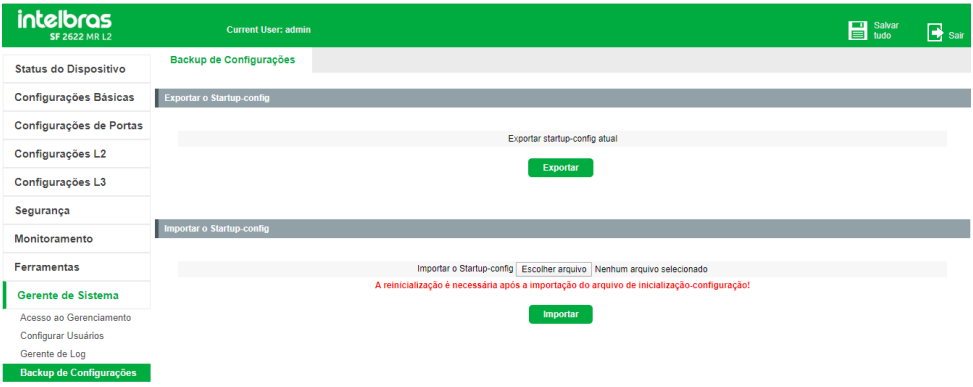
11.3.1. Gerente de log

Gestão de log

- **Habilitar servidor de log:** os logs de sistema serão enviados ao endereço de servidor de log.
- **Endereço do servidor de log:** determina o endereço IP do servidor onde os logs serão enviados.
- **Nível de logs de sistema:** filtra o nível de criticidade a ser armazenado no servidor (0 a 8).
- **Habilitar o buffer de log:** possibilita personalizar o tamanho alocado para o armazenamento de logs do sistema.
- **Tamanho do buffer de log:** determina o tamanho da memória de buffer de logs.
- **Nível de logs de cache:** determina o nível de criticidade a ser armazenado na memória cache.

11.4. Backup de configurações

Na tela a seguir é possível realizar o backup das configurações atuais do equipamento além de importar as configurações salvas.



Backup de configurações

11.4.1. Backup de configurações

Exportar o startup-config

Ao clicar no botão *Exportar,* será realizado o download do arquivo atual de configuração do equipamento. Será salvo arquivo com o nome *startup-config.*

Importar o startup-config

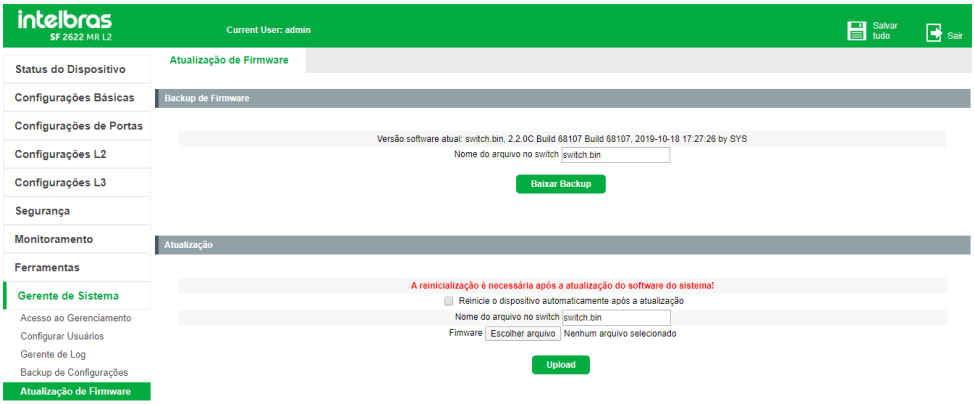
2. Clique no botão *Escolher arquivo;*
3. Selecionar o arquivo com as configurações deste equipamento;
4. Clique em *Importar.*

Importante: para que a importação das configurações seja feita corretamente é necessário reiniciar o equipamento após o carregamento do arquivo.

Obs.: *se o arquivo de configuração estiver incorreto, todas as configurações atuais serão perdidas.*

11.5. Atualização de firmware

Nesta página é possível atualizar e salvar um backup do atual firmware.



Atualização de firmware

11.5.1. Atualização de firmware

Backup de firmware

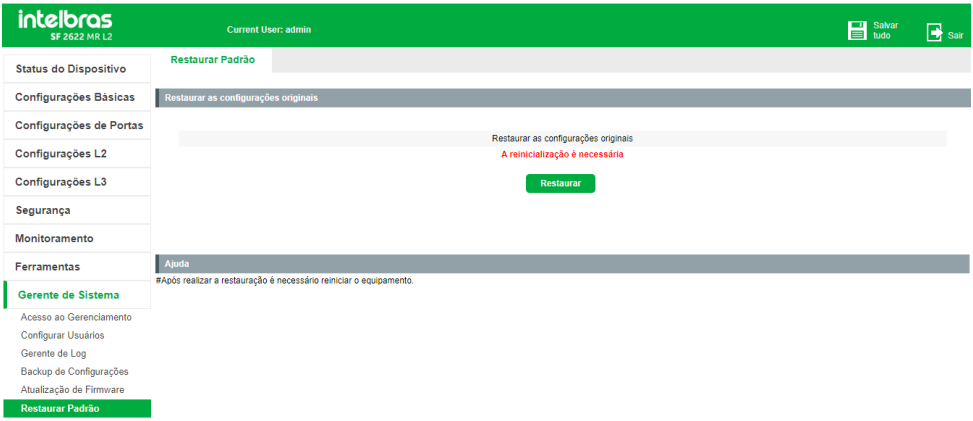
Para gerar uma cópia do firmware que está rodando no sistema, clique no botão *Baixar o backup*. O arquivo será baixado com o nome *switch.bin*.

Atualização de firmware

Selecione o arquivo com a nova versão, sendo que esse possua o nome *switch.bin*, para que assim o sistema possa reconhecê-lo, após o upload do arquivo será necessária a reinicialização. Caso a opção *Reinicie o dispositivo automaticamente após a atualização* não seja marcada, será necessário reiniciar manualmente.

11.6. Restaurar padrão

Nesta página é possível restaurar as configurações para o padrão de fábrica.



Restaurar padrão

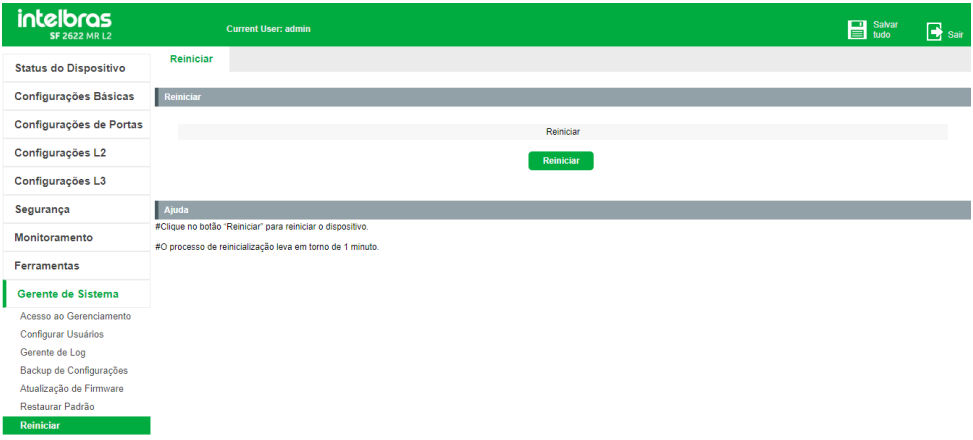
11.6.1. Restaurar padrão

Restaurar

Clique no botão *Restaurar,* após restauração é necessário reiniciar o switch.

11.7. Reiniciar

Nesta página é possível reiniciar o dispositivo.



Reiniciar

11.7.1. Reiniciar

Reiniciar

Clique no botão para reinicializar o sistema, o processo dura em torno de 1 min.

12. Interface de linha de comando (CLI)

É possível realizar acessar a CLI através de duas maneiras:

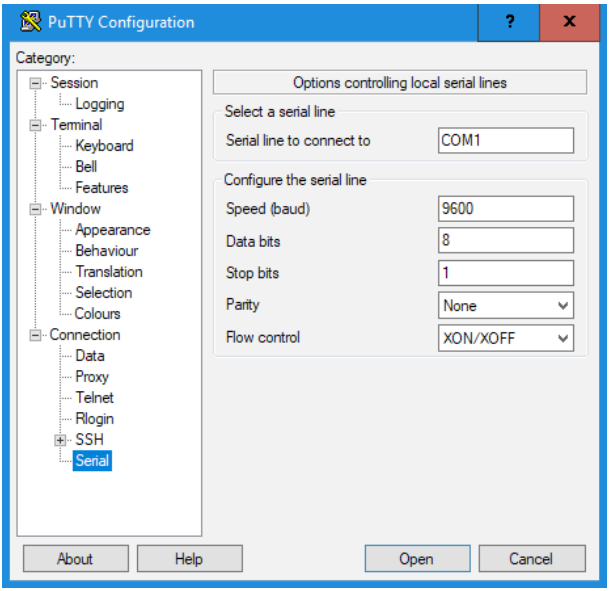
- Utilizando a porta console do switch.
- Remotamente utilizando uma conexão SSH ou Telnet.

12.1. 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 (recomendamos o Putty®).

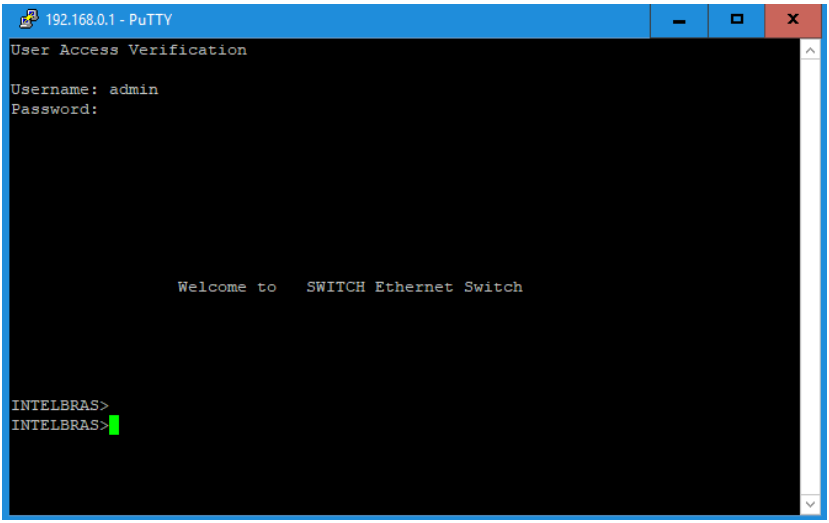
O software de emulação de terminal deve ser iniciado com a seguinte configuração:



Configuração do Putty®

- **Tamanho da palavra:** 8 bits.
- **Velocidade:** 9600 bps.
- **Bits de parada:** 1 bit.
- **Bits de paridade:** nenhum.
- **Controle de fluxo:** desligado.

Após pressionar o botão *Open*, será solicitado o nome de usuário e senha na tela inicial da CLI. O usuário e senha padrão de fábrica é *admin*.

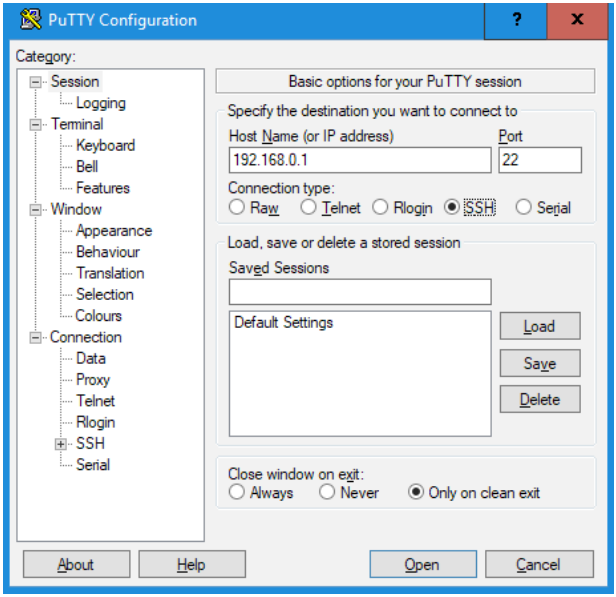


Tela inicial CLI

12.2. Login via SSH

Siga os seguintes passos para realizar o acesso via SSH:

1. Abra o software Putty®;
2. Digite o endereço IP do switch no campo *Host name*. O endereço IP de fábrica do switch é *192.168.0.1;*
3. Mantenha o valor padrão de *22* no campo *Port*;
4. Selecione *SSH* como o tipo de conexão;
5. Clique no botão *Open* para acessar a CLI do switch.



Configuração da conexão SSH

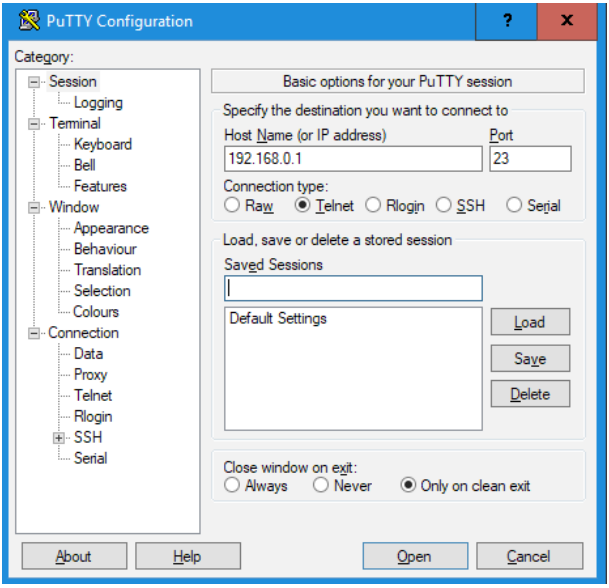
Após pressionar o botão *Open*, será solicitado o nome de usuário e senha na tela do Putty®. O usuário e senha padrão de fábrica é *admin*.

Obs.: *o acesso via SSH não vem habilitado de fábrica.*

12.3. Login via Telnet

Siga os seguintes passos para realizar o acesso via Telnet:

1. Abra o software Putty®;
2. Digite o endereço IP do switch no campo *Host name*. O endereço IP de fábrica do switch é *192.168.0.1;*
3. Mantenha o valor padrão de *23* no campo *Port*;
4. Selecione *Telnet* como o tipo de conexão;
5. Clique no botão *Open* para acessar a CLI do switch.



Configuração da conexão Telnet

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

12.4. Restaurar padrão de fábrica

A restauração do padrão de fábrica via CLI pode ser feita nos modos padrão de acesso ao switch explicados nas sessões *12.1. Login pela porta console* e *12.3. Login via Telnet* ou no modo *Monitor* em caso de perda da senha de acesso do switch.

12.4.1. Acesso padrão

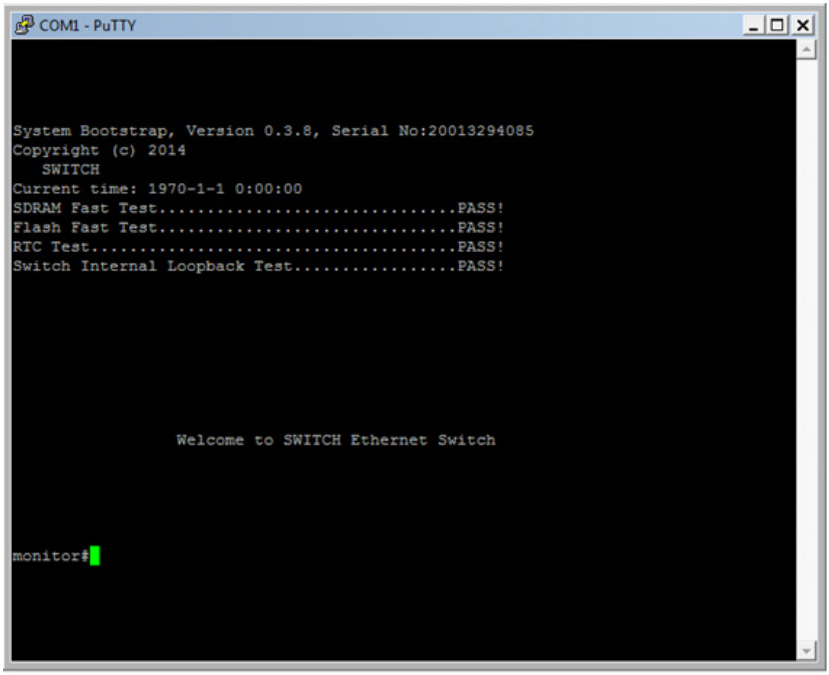
Siga o passo a passo a seguir para restaurar o padrão de fábrica do switch.

1. Acesse o switch via Telnet, SSH ou porta console;
2. Acesse o modo *Privilegiado* através do comando *enable*;
3. Delete o arquivo de configurações do switch através do comando *delete startup-config*;
4. Reinicie o switch através do comando *reboot*.

12.4.2. Modo *Monitor*

Siga o passo a passo a seguir para restaurar o padrão de fábrica do switch se não tiver os dados de login.

1. Desligue o equipamento da alimentação;
2. Conecte na porta console do switch com as configurações de comunicação serial descritas na sessão *12.1. Login pela porta console*;
3. Ligue o equipamento na alimentação;
4. Fique pressionando *Ctrl+P* durante a inicialização para entrar no modo monitor;
5. Delete o arquivo de configurações do switch através do comando *delete startup-config*;
6. De o comando *yes* para confirmar a exclusão do startup-config;
7. Reinicie o switch através do comando *reboot*.



Acessando o modo Monitor

12.5. Modos de comando CLI

A CLI agrupa todos os comandos em modos apropriados pela natureza dos comandos, cada modo de comando suporta comandos específicos de configuração ou visualização das funcionalidades do switch. Inserindo " *?* " (ponto de interrogação sem aspas) no prompt de comando da CLI, será mostrado uma lista dos comandos disponíveis e sua descrição.

Os principais modos de comando da CLI são mostrados na figura a seguir:

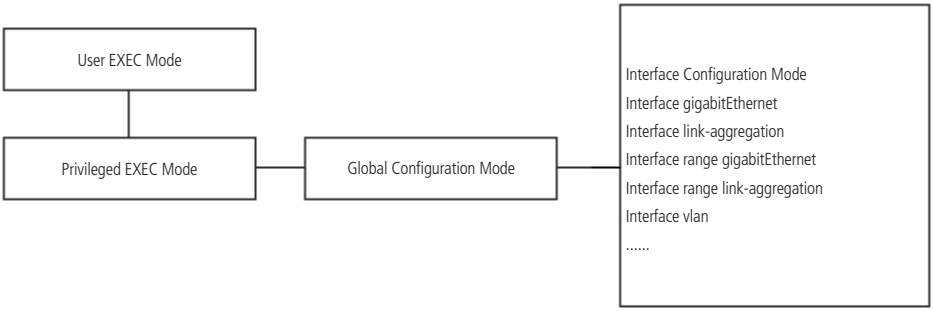


Diagrama de modos de comando

A tabela a seguir fornece informações sobre os modos de comando, o prompt utilizado e como sair do modo atual e acessar o modo seguinte.

Modo	Descrição	Prompt	Modo seguinte
User EXEC	Este é o primeiro nível de acesso após inserir o usuário (user) e senha (password). Executa tarefas básicas e lista informações do sistema.	**INTELBRAS>**	Use o comando **enable** para acessar o modo EXEC privilegiado.
Privileged EXEC	Neste modo é permitido ao usuário visualizar todas as informações do sistema.	**INTELBRAS#**	Use o comando **config** para acessar o modo Global Configuration.
Global Configuration	Neste modo são realizadas configurações referentes ao switch, como criação de VLANs e controle de acesso.	**INTELBRAS_config#**	Use o comando **interface *tipo ID*** para acessar o modo *Interface Configuration.*
Interface Configuration	Neste modo são realizadas as configurações referentes a uma interface, como velocidade e modo *Duplex*.	**INTELBRAS_config_if#**	

Modos de comando

12.6. Convenções

As seguintes convenções são utilizadas neste manual:

- **Comando principal:** o comando principal é destacado em negrito.
- **Parâmetros fixos:** os parâmetros fixos são escritos sem nenhuma formatação especial.
- **Descritivos:** os descritivos são formatados em itálico. Descritivos são nomes atribuídos a comandos que não são fixos.
- **Valores:** os valores são descritos na seguinte forma: (valor inicial permitido- valor máximo permitido).
- **Múltiplas opções:** quando há mais de uma opção de parâmetro para um comando as opções são separadas por um '|'.

Exemplo de descrição de comando:

interface FastEthernet | Vlan | Loopback | Port-aggregator | Null *interface_id*

Exemplo de utilização de comando:

interface FastEthernet 0/1

13. Configuração do terminal

13.1. Porta Telnet

Descrição: o comando **attach-port** é utilizado para vincular uma porta Telnet ao número da linha vty e ativar a conexão Telnet na porta.

Sintaxe: **attach-port** (*3001-3999*)
no attach-port

Parâmetros:

» **(3001-3999):** número da porta (3001-3999).

Modo de comando: Line Configuration Mode.

Exemplo: ativar a escuta na porta 3001 para line vty 2 3.

INTELBRAS_config#line vty 2 3

INTELBRAS_config_line#attach-port 3001

13.2. Autocommand

Descrição: o comando **autocommand** é usado para definir a execução automática quando o usuário efetuar login no terminal. A conexão será perdida após o comando ser executado.

Sintaxe: **autocommand** *line*
no autocommand

Parâmetros:

» **line:** comando a ser executado.

Modo de comando: Line Configuration Mode.

Exemplo:

INTELBRAS_config#line vty 1

INTELBRAS_conf_line#autocommand pad 123456

13.3. Clear line

Descrição: o comando **clear line** é usado para limpar a linha informada.

Sintaxe: **clear line** console | vty *number*

Parâmetros:

» **console:** número da linha a ser limpa (0).
» **vty:** número da linha a ser limpa (0-31).
» **number:** número 0 para console e de 0 a 31 para vty.

Modo de comando: Privileged EXEC.

Exemplo: limpe a line vty 0.

INTELBRAS#clear line vty 0

13.4. Servidor Telnet

Descrição: o comando **connect** é utilizado para conectar a um servidor Telnet.

Sintaxe: **connect** *server-ip-addr / server-host-name (0-65535)* | source-interface | local script

Parâmetros:

» **server-ip-addr:** endereço IP do servidor.
» **server-host-name:** host servidor.
» **(0-65535):** número da porta.
» **source-interface:** interface onde a conexão Telnet é originada Null (0) ou Vlan (1).
» **local:** endereço de IP local onde a conexão Telnet é originada.
» **script:** nome do script.

Modo de comando: todos os modos de configuração.

Exemplo: conecte a um servidor Telnet com IP 192.168.0.10.

INTELBRAS#connect 192.168.0.10 /port 3000 /source-interface vlan 1 /script TELNET

13.5. Disconnect

Descrição: o comando **disconnect** é usado para desconectar de um servidor Telnet.

Sintaxe: **disconnect** *N*

Parâmetros:

» **N:** número do diálogo Telnet que será desconectado.

Modo de comando: todos os modos de configuração.

Exemplo: desconecte de um servidor Telnet com IP 192.168.0.10.

INTELBRAS#disconnect 192.168.0.10

13.6. Tempo de ociosidade do terminal

Descrição: o comando **exec-timeout** é usado para configurar o tempo de ociosidade de um terminal.

Sintaxe: **exec-timeout** *(0-86400)*
no exec-timeout

Parâmetros:

» **(0-86400):** tempo em segundos que o terminal permanece ocioso. Por padrão o valor é *0*, sem limite de tempo.

Modo de comando: Line Configuration Mode.

Exemplo: configure o tempo de ociosidade do terminal para 1 hora.

INTELBRAS_config_line#exec-timeout 3600

13.7. Length

Descrição: o comando **length** é usado para configurar o número de linhas na tela do terminal.

Sintaxe: **length** *(0-512)*
no length

Parâmetros:

» **(0-512):** número de linhas exibida na tela após a execução de um comando. Para mostrar todas as linhas sem pausa escolha 0. Por padrão a quantidade de linhas é *24*.

Modo de comando: Line Configuration Mode.

Exemplo: configure 10 linhas para saída de um comando.

INTELBRAS_config_line#length 10

13.8. Line

Descrição: o comando **line** é usado para entrar no modo de configuração de linha.

Sintaxe: **line** console | vty *number*

Parâmetros:

» **number:** número para a console [0] ou line vty [0 a 31].

Modo de comando: Global Configuration.

Exemplo: acessar no modo de configuração de linha de VTY 0 a 10.

INTELBRAS_config#line vty 0 10

13.9. Location

Descrição: o comando **location** é usado para atribuir um nome para line vty.

Sintaxe: **location** *line*
no location

Parâmetros:

» **line:** nome da line vty.

Modo de comando: Line Configuration Mode.

Exemplo: atribuir o nome TESTE para a line vty 1.

INTELBRAS_config#line vty 1

INTELBRAS_config_line#location TESTE

13.10. Login authentication

Descrição: o comando **login authentication** é usado para definir a autenticação de login de linha.

Sintaxe: **login authentication** *default* | *word*
no login authentication

Parâmetros:

» **default:** modo de autenticação padrão.

» **word:** nome da lista de autenticação.

Modo de comando: Line Configuration Mode.

Exemplo: atribuir o nome TESTE para autenticação da linha line vty 0 15.

INTELBRAS_config#line vty 1 15

INTELBRAS_config_line#login authentication TESTE

13.11. Monitor

Descrição: o comando **monitor** é usado para exportar as informações de log e depuração para a linha.

Sintaxe: **monitor**
no monitor

Modo de comando: Line Configuration Mode.

Exemplo:

INTELBRAS_config_line#monitor

13.12. No debug all

Descrição: o comando **no debug all** é usado para desligar todas as saídas de depuração do line vty atual.

Sintaxe: **no debug all**

Modo de comando: Privileged EXEC.

Exemplo:

INTELBRAS#no debug all

13.13. Senha de acesso ao terminal

Descrição: o comando **password** é usado para configurar uma senha para o terminal.

Sintaxe: **password** *line* | *(0/7) encrypted-password*
no password

Parâmetros:

» **line:** senha configurada para a linha com tamanho máximo é de 30 caracteres.

» **(0/7):** com ou sem criptografia. Escolha 0 para senha sem criptografia e 7 para senha com criptografia.

» **encrypted-password:** se na opção anterior for escolhido 7, a senha inserida já deve estar criptografada.

Modo de comando: Line Configuration Mode.

Para criptografia de senha, consulte a explicação dos comandos **service password-encryption** e **enable password**.

Exemplo: atribuir a senha teste sem criptografia para line vty 1.

INTELBRAS_config#line vty 1

INTELBRAS_config_line#password teste ou INTELBRAS_config_line#password 0 teste

13.14. Resume

Descrição: o comando **resume** é usado para retomar a sessão de Telnet iniciada.

Sintaxe: **resume** *N*

Parâmetros:

» **N:** senha número do terminal Telnet para ser suspendido.

Modo de comando: todos os modos de configuração.

Exemplo:

INTELBRAS#resume 1

13.15. Show debug

Descrição: o comando **show debug** é usado para informar o que está em processo de debugging no momento.

Sintaxe: **show debug**

Modo de comando: Privileged EXEC ou Global Configuration.

Exemplo:

INTELBRAS#show debug

13.16. Show line

Descrição: o comando **show line** é usado para informar o status das sessões iniciadas.

Sintaxe: **show line** console | vty *(0-31)*

Parâmetros:

» **(0-31):** número para a console [0] ou line vty [0 a 31].

Modo de comando: Privileged EXEC ou Global Configuration.

Exemplo:

INTELBRAS#show line

INTELBRAS#show line vty 5

13.17. Terminal length

Descrição: o comando **terminal length** é usado para alterar a quantidade de linhas que são exibidas na sessão corrente.

Sintaxe: **terminal length** *num*
no terminal length

Parâmetros:

» **num:** linhas que serão exibidas na sessão. Por padrão o valor é *24 linhas*. O valor pode ser entre 0 e 512.

Modo de comando: Global Configuration.

Exemplo:

» INTELBRAS#terminal length 30

13.18. Terminal monitor

Descrição: o comando **terminal monitor** é usado para exibir a depuração de saída e as informações de erro do sistema.

Sintaxe: **terminal monitor**
no terminal monitor

Modo de comando: Global Configuration.

Exemplo:

INTELBRAS#terminal monitor

13.19. Terminal width

Descrição: o comando **terminal width** é usado para alterar a quantidade de caracteres em uma linha da sessão.

Sintaxe: **terminal width** *(0-256)*
no terminal width

Parâmetros:

» **number:** número de caracteres em cada linha. Por padrão o valor é *80 caracteres*.

Modo de comando: Global Configuration.

Exemplo:

INTELBRAS#terminal width 40

13.20. Terminal-type

Descrição: o comando **terminal-type** é usado para definir o tipo do terminal.

Sintaxe: **terminal-type** *name*
no terminal-type

Parâmetros:

» **name:** nome do terminal. Os tipos de terminais atualmente suportados são *VT100*, *ANSI* e *VT100J*.

Modo de comando: Line Configuration Mode.

Exemplo:

INTELBRAS#terminal-type ANSI

13.21. Where

Descrição: o comando **where** é usado para mostrar na tela as conexões Telnet atuais.

Sintaxe: **where**

Modo de comando: todos os modos de configuração.

Exemplo:

INTELBRAS#where

13.22. Width

Descrição: o comando **width** é usado para definir a largura de caracteres em uma linha do terminal.

Sintaxe: **width** *value*
no width

Parâmetros:

» **value:** quantidade de caracteres que são impressos em uma linha. Por padrão o valor é *80 caracteres*.

Modo de comando: Line Configuration Mode.

Exemplo:

INTELBRAS_config_line#width 80

14. Ferramentas

14.1. Ping

Descrição: o comando **ping** é utilizado para verificar a conectividade entre o switch e outro dispositivo de rede.

Sintaxe: **ping** *ip*

Parâmetros:

» **ip:** endereço IP do dispositivo de rede de destino.

Modo de comando: Privileged EXEC e Global Configuration.

Exemplo: teste a conectividade entre o switch e o computador que possui o endereço IP 192.168.0.100.

INTELBRAS_config#ping 192.168.0.100

14.2. 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** *ip*

Parâmetros:

» **ip:** endereço IP do dispositivo de rede de destino.

Modo de comando: Privileged EXEC e Global Configuration.

Exemplo: teste a conectividade entre o switch e o computador que possui o endereço IP 192.168.0.10.

INTELBRAS_config#traceroute 192.168.0.10

14.3. Ping6

Descrição: o comando **ping6** é utilizado para a ferramenta de diagnóstico Ping6.

Sintaxe: **ping6** *destino* –a | -l *tamanho* | -n *quantidade* | -w *tempo* | -b *intervalo*

Parâmetros:

» **destino:** destino IPv6.
» **-a:** executa o Ping6 até a interrupção do programa.
» **-l *tamanho*:** configura o tamanho dos pacotes ICMPv6 Request.
» **-n *quantidade*:** configura a quantidade de pacotes ICMPv6 Request.
» **-w *tempo*:** configura o tempo de espera dos pacotes ICMPv6 Reply.
» **-b *intervalo*:** configura a o intervalo de trasnmissão de pacotes ICMPv6 Request.

Modo de comando: Privileged EXEC.

Exemplo: execute o ping6 no host de destino 3001::5.

INTELBRAS#ping6 3001::5

14.4. Traceroute6

Descrição: o comando **traceroute6** é utilizado para a ferramenta de diagnóstico Traceroute6.

Sintaxe: **traceroute6** *destino* -i *endereço_ip* | -p *porta* | -q *quantidade* | -t *ttl* | -x *icmp* | -w *tempo*

Parâmetros:

» **destino:** destino IPv6.
» **-i *endereço_ip*:** configura um endereço IPv6 de origem.
» **-p *porta*:** configura a porta UDP de destino.
» **-q *quantidade*:** configura a quantidade de pacotes que o sistema envia cada vez.
» **-t *ttl*:** configura o TTL.
» **-x *icmp*:** configura a utilização do ICMPv6 em vez do UDP.
» **-w *tempo*:** configura o tempo de espera dos pacotes.

Modo de comando: privileged EXEC.

Exemplo: execute o traceroute6 no host de destino 3001::5.

INTELBRAS#traceroute6 3001::5

15. Diagnósticos de falha

15.1. Logging

Descrição: o comando **logging** é utilizado para exibir o estado do log (syslog).

Sintaxe: **logging** *ip level*

Parâmetros:

» **ip:** endereço IP do dispositivo do servidor de syslog.
» **level:** nível da informação do log.

Modo de comando: Global Configuration.

Exemplo:

INTELBRAS_config#logging 192.168.0.10 critical

15.2. Logging buffered

Descrição: o comando **logging buffered** é utilizado para gravar o log na memória do equipamento.

Sintaxe: **logging buffered** *(4096-2147483647)* | *level*
no logging buffered

Parâmetros:

» **size:** tamanho do cache de memória em bytes.
» **level:** nível da informação do log.

Prompt	Nível	Descrição	Definição do syslog
emergencies	0	Sistema inutilizável	LOG_EMERG
alerts	1	Necessita ação imediata	LOG_ALERT
critical	2	Críticas	LOG_CRIT
erros	3	Erro	LOG_ERR
warnings	4	Aviso	LOG_WARNING
notifications	5	Notificação relevante	LOG_NOTICE
informational	6	Informação	LOG_INFO
debugging	7	Mensagem de debugging	LOG_DEBUG

Modo de comando: Global configuration.

Exemplo:

INTELBRAS_config#logging buffered critical

15.3. Logging console

Descrição: o comando **logging console** é utilizado para controlar o volume de informações exibido no console.

Sintaxe: **logging console** *level*
no logging console

Parâmetros:

» **level:** nível da informação do log.

Prompt	Nível	Descrição	Definição do syslog
emergencies	0	Sistema inutilizável	LOG_EMERG
alerts	1	Necessita ação imediata	LOG_ALERT
critical	2	Críticas	LOG_CRIT
erros	3	Erro	LOG_ERR
warnings	4	Aviso	LOG_WARNING
notifications	5	Notificação relevante	LOG_NOTICE
informational	6	Informação	LOG_INFO
debugging	7	Mensagem de debugging	LOG_DEBUG

Modo de comando: Global configuration.

Exemplo:

INTELBRAS_config#logging console alerts

15.4. Logging facility

Descrição: o comando logging facility é utilizado para gravar a informação de um erro específico.

Sintaxe: **logging facility** *facility-type*
no logging facility

Parâmetros:

» **logging facility:** podem ser escolhidos de acordo com a planilha a seguir:

Tipo	Descrição
auth	Sistema de autorização
cron	Instalação Cron
daemon	Daemon do sistema
kern	Kernel
local0-7	Reservado para mensagens definidas localmente
lpr	Sistema de impressora de linha
mail	Sistema de correio
news	Notícias da USENET
sys9	Uso do sistema
sys10	Uso do sistema
sys11	Uso do sistema
sys12	Uso do sistema
sys13	Uso do sistema
sys14	Uso do sistema
syslog	Registro do sistema
user	Processo do usuário
uucp	Sistema de cópia UNIX®-para-UNIX®

Modo de comando: Global Configuration.

Exemplo:

INTELBRAS_config#logging facility

15.5. Logging monitor

Descrição: o comando **logging monitor** é utilizado para controlar o volume de informações exibido na linha do terminal.

Sintaxe: **logging monitor** *level*
no logging monitor

Parâmetros:

» **level:** nível da gravação do log.

Prompt	Nível	Descrição	Definição do syslog
emergencies	0	Sistema inutilizável	LOG_EMERG
alerts	1	Necessita ação imediata	LOG_ALERT
critical	2	Críticas	LOG_CRIT
erros	3	Erro	LOG_ERR
warnings	4	Aviso	LOG_WARNING
notifications	5	Notificação relevante	LOG_NOTICE
informational	6	Informação	LOG_INFO
debugging	7	Mensagem de debugging	LOG_DEBUG

Modo de comando: Global Configuration.

Exemplo:

INTELBRAS_config#logging monitor emergencies

15.6. Logging on

Descrição: o comando **logging on** é utilizado para controlar a gravação de informações de erro.

Sintaxe: **logging on**
no logging on

Modo de comando: Global Configuration.

Exemplo:

INTELBRAS_config#logging on

15.7. Logging trap

Descrição: o comando **logging trap** é utilizado para controlar o volume de informações registradas no servidor syslog.

Sintaxe: **logging trap** *level*
no logging trap

Parâmetros:

» **level:** nível de informação dos registros exibidos na linha do terminal.

Prompt	Nível	Descrição	Definição do syslog
emergencies	0	Sistema inutilizável	LOG_EMERG
alerts	1	Necessita ação imediata	LOG_ALERT
critical	2	Críticas	LOG_CRIT
erros	3	Erro	LOG_ERR
warnings	4	Aviso	LOG_WARNING
notifications	5	Notificação relevante	LOG_NOTICE
informational	6	Informação	LOG_INFO
debugging	7	Mensagem de debugging	LOG_DEBUG

Modo de comando: Global Configuration.

Exemplo:

INTELBRAS_config#logging trap warnings

15.8. Logging command

Descrição: o comando **logging command** é utilizado para ativar a gravação da execução do comando.

Sintaxe: **logging command**
no logging command

Modo de comando: Global Configuration.

Exemplo:

INTELBRAS_config#logging command

15.9. Logging source-interface

Descrição: o comando **logging source-interface** é utilizado para definir a porta de origem da troca de log.

Sintaxe: **logging source-interface** vlan | null *(1-99)*
no logging source-interface

Parâmetros:

» **(1-99):** número da interface VLAN.

Modo de comando: Global Configuration.

Exemplo:

INTELBRAS_config#logging source-interface vlan 1

15.10. Logging history

Descrição: o comando **logging history** é utilizado para definir o nível da tabela de log histórico para os níveis das mensagens configuradas.

Sintaxe: **logging history** *level*
no logging history *level*

Parâmetros:

» **level:** nível da gravação do log.

Prompt	Nível	Descrição	Definição do syslog
emergencies	0	Sistema inutilizável	LOG_EMERG
alerts	1	Necessita ação imediata	LOG_ALERT
critical	2	Críticas	LOG_CRIT
erros	3	Erro	LOG_ERR
warnings	4	Aviso	LOG_WARNING
notifications	5	Notificação relevante	LOG_NOTICE
informational	6	Informação	LOG_INFO
debugging	7	Mensagem de debugging	LOG_DEBUG

Modo de comando: Global Configuration.

Exemplo:

INTELBRAS_config#logging history critical

15.11. Logging history rate-limit

Descrição: o comando **logging history rate-limit** é utilizado para definir a taxa de saída do log.

Sintaxe: **logging history rate-limit** *(1-512)*
no logging history rate-limit

Parâmetros:

» **(1-512):** número de logs que são exportados a cada segundo.

Modo de comando: Global Configuration.

Exemplo:

INTELBRAS_config#logging history rate-limit 256

15.12. Logging history size

Descrição: o comando **logging history size** é utilizado para definir o número de entradas na tabela de log histórico.

Sintaxe: **logging history size** *(0-500)*

Parâmetros:

» **(0-500):** representa o número de entradas de log históricas. Por padrão o valor é *0*.

Modo de comando: Global configuration.

Exemplo:

INTELBRAS_config#logging history size 256

15.13. Service timestamps

Descrição: o comando **service timestamps** é utilizado para definir a configuração do registro de data e hora que é adicionado quando o sistema é depurado ou é gravado as informações de registro.

Sintaxe: **service timestamps** debug | log | microsecond *date* | *uptime*
no service timestamps *log* | *debug*

Parâmetros:

- **debug:** adiciona o registro de data e hora antes das informações de depuração.
- **log:** adiciona o registro de data e hora antes das informações de log.
- **microsecond:** tempo decorrido entre a inicialização do switch e a hora atual.
- **data:** informação de data e hora.
- **uptime:** informação de data e hora, tempo de atividade do sistema.

Modo de comando: Global Configuration.

Exemplo:

INTELBRAS_config#service timestamps debug uptime

15.14. Clear logging

Descrição: o comando **clear logging** é utilizado para limpar as informações de log registradas na memória cache.

Sintaxe: **clear logging**

Modo de comando: Privileged EXEC.

Exemplo:

INTELBRAS#clear logging

15.15. Show break

Descrição: o comando **show break** é utilizado para exibir as informações sobre a falha anormal do switch.

Sintaxe: **show break**

Modo de comando: Privileged EXEC.

Exemplo:

INTELBRAS#show break

15.16. Show debug

Descrição: o comando **show debug** é utilizado para exibir as opções de depuração ativas do switch.

Sintaxe: **show debug**

Modo de comando: Privileged EXEC.

Exemplo:

INTELBRAS#show debug

15.17. Show logging

Descrição: o comando **show logging** é utilizado para exibir o estado atual do log de informações.

Sintaxe: **show logging**

Modo de comando: Privileged EXEC.

Exemplo:

INTELBRAS#show logging

16. Accounting Authentication Authorization (AAA)

16.1. Autenticação

Notificação de login

Descrição: o comando **aaa authentication banner** é usado para mostrar uma mensagem de entrada quando o usuário efetuar o login.

Sintaxe: **aaa authentication banner** delimiter *string* delimiter
no aaa authentication banner

Parâmetros:

» **delimiter:** a mensagem deve ser inserida entre os delimitadores " " para ser aceita como banner.
» **string:** mensagem para usar ao iniciar login/autenticação. O tamanho máximo do texto é 31 caracteres.

Modo de comando: Global Configuration.

Exemplo: insira a mensagem "Acesso restrito" como alerta de entrada.

INTELBRAS_config#aaa authentication banner "Acesso restrito"

Notificação de falha de login

Descrição: o comando **aaa authentication fail-message** é usado para mostrar uma mensagem quando o login falhar.

Sintaxe: **aaa authentication fail-message** delimiter *string* delimiter
no aaa authentication fail-message

Parâmetros:

» **delimiter:** a mensagem deve ser inserida entre os delimitadores " " para ser aceito como banner.
» **string:** mensagem para usar ao iniciar login/autenticação. O tamanho máximo do texto é 31 caracteres.

Modo de comando: Global Configuration.

Exemplo: insira a mensagem "Acesso para pessoas autorizadas" como alerta de erro de login.

INTELBRAS_config#aaa authentication fail-message "Acesso para pessoas autorizadas"

Solicitação de usuário

Descrição: o comando **aaa authentication username-prompt** é usado para alterar o texto de solicitação do usuário no login.

Sintaxe: **aaa authentication username-prompt** *text_string*
no aaa authentication username-prompt

Parâmetros:

» **text_string:** texto solicitando o login do usuário para login/autenticação. O texto não pode ter espaços e o tamanho máximo é 31 caracteres.

Modo de comando: Global Configuration.

Exemplo: insira o texto "Nome_de_usuário:" como solicitação para login de usuários.

INTELBRAS_config#aaa authentication username-prompt Nome_de_usuário:

Solicitação de senha

Descrição: o comando **aaa authentication password-prompt** é usado para alterar o texto de solicitação da senha do usuário no login.

Sintaxe: **aaa authentication password-prompt** *text_string*
no aaa authentication password-prompt

» **Parâmetros:**
» **text_string:** texto solicitando a senha do usuário para login/autenticação. O texto não pode ter espaços e o tamanho máximo é 31 caracteres.

Modo de comando: Global Configuration.

Exemplo: insira o texto "Senha_de_acesso:" como solicitação para o usuário digitar a senha.

INTELBRAS_config#aaa authentication password-prompt Senha_de_acesso:

Verficiação de login

Descrição: o comando **aaa authentication dot1x** é usado para configurar uma sequência de verificação para o login de acesso.

Sintaxe: **aaa authentication dot1x** *word* | *default method1* | *method2…*
no aaa authentication dot1x

Parâmetros:

» **word:** lista de autenticação nomeada.

» **default:** lista de autenticação padrão.

» **metlhod:** lista do método de autenticação. No final da lista insira a opção *none*. Ela será aplicada caso nenhuma outra esteja válida.

group name	Usa o grupo de servidores para autenticação
group radius	Usa autenticação RADIUS
group tacacs +	Usa autenticação de grupo TACACS+
local	Usa o banco de dados de nome de usuário para autenticação
local-case	Usa autenticação separando letras maiúsculas e minúsculas
none	Não usa autenticação

Modo de comando: Global Configuration.

Exemplo: o exemplo cria uma lista de autenticação AAA chamada TESTE. Essa autenticação primeiro tenta entrar em contato com um servidor TACACS+. Se nenhum servidor for encontrado, o TACACS+ retornará um erro. O AAA tentará usar a senha de ativação. Se essa tentativa também retornar um erro, o usuário terá permissão para acessar sem autenticação.

INTELBRAS_config#aaa authentication dot1x TESE group tacacs+ local none

Verificação de privilégio

Descrição: o comando **aaa authentication enable default** é usado para criar uma série de métodos de autenticação para validar se o usuário pode acessar o modo de comandos privilegiado.

Sintaxe: **aaa authentication enable default** *method1* | *method2…*
no aaa authentication enable default

Parâmetros:

» **metlhod:** lista do método de autenticação. No final da lista insira a opção *none*. Ela será aplicada caso nenhuma outra esteja válida.

group name	Usa o grupo de servidores para autenticação
group radius	Usa autenticação RADIUS
group tacacs +	Usa autenticação de grupo TACACS+
local	Usa o banco de dados de nome de usuário para autenticação
local-case	Usa autenticação separando letras maiúsculas e minúsculas
none	Não usa autenticação.

Modo de comando: Global Configuration.

Exemplo: o exemplo a seguir solicita cria uma lista de autenticação que primeiro tenta verificar em um servidor TACACS+ para realizar a autenticação ao nível de comandos privilegiado. Se a autenticação não puder ser realizada, o usuário terá permissão para acessar sem autenticação.

INTELBRAS_config#aaa authentication enable default group tacacs+ none

Autenticação no login

Descrição: o comando **aaa authentication login** é usado para definir autenticação no login.

Sintaxe: **aaa authentication login** *word* | *default method1* | *method2…*
no aaa authentication login *word* | *default*

Parâmetros:

» **word:** lista de autenticação nomeada.
» **default:** lista de autenticação padrão.
» **metlhod:** lista do método de autenticação. No final da lista insira a opção *none*. Ela será aplicada caso nenhuma outra esteja válida.

Enable	Usa a senha de ativação para autenticação
group name	Usa o grupo de servidores para autenticação
group radius	Usa autenticação RADIUS
group tacacs +	Usa autenticação de grupo TACACS+
line	Usa a senha da linha para autenticação
Local	Usa o banco de dados de nome de usuário para autenticação
local-group	Usa o banco de dados de nome de usuário do grupo de estratégia local para autenticação
local-case	Usa autenticação separando letras maiúsculas e minúsculas
none	Não usa autenticação

Modo de comando: Global Configuration.

Exemplo: o exemplo a seguir solicita cria uma lista de autenticação de login onde primeiro tenta verificar em um servidor TACACS+ está acessível para realizar a autenticação ao nível de comandos privilegiado. Se a autenticação não puder ser realizada, o AAA vai buscar autenticação em um serviço RADIUS. Se a autenticação também não puder ser realizada o usuário terá permissão para acessar sem autenticação.

INTELBRAS_config#aaa authentication login default group tacacs+ group radius none

Grupo de servidores

Descrição: o comando **aaa group server** é usado para agrupar diferentes servidores RADIUS e TACACS+ em listas e métodos distintos.

Sintaxe: **aaa group server radius** | tacacs+ *group-name*
no aaa group server radius | tacacs+ *group-name*

Parâmetros:

» **group-name:** nome usado para nomear o grupo de servidores.

Modo de comando: Global Configuration.

Exemplo: adicione um grupo de servidores RADIUS chamado Grupo_Radius.

INTELBRAS_config#aaa group server radius Grupo_Radius

Servidor

Descrição: o comando **server** é usado para adicionar o grupo de servidores descritos no comando anterior.

Sintaxe:

» Para adicionar um servidor RADIUS:
server *A.B.C.D* | *X: X:X:X::X* key *password* | *encryption-type* | *encrypted-password* auth-port *num* acct-port *num* retransmit *value* timeout *value* privilege *pri*

» Para adicionar um servidor TACACS+:
server *A.B.C.D* | *X:X:X:X::X* key *password* | *encryption-type* | *encrypted-password*
no server *A.B.C.D*

Parâmetros:

- **A.B.C.D:** endereço IP do servidor.
- **X: X:X:X::X:** endereço IPv6 do servidor.
- **password:** senha configurada para a linha com tamanho máximo é de 30 caracteres.
- **encryption-type:** com ou sem criptografia. Escolha 0 para senha sem criptografia e 7 para senha com criptografia.
- **encrypted-password:** se na opção anterior for escolhido 7, a senha inserida já deve estar criptografada.
- **num:** representa o ID de porta.
- **retransmit value:** tempo de retransmissão. O valor pode variar de 0 a 100 segundos. Por padrão o valor é *2 segundos*.
- **timeout value:** timeout da retransmissão. O valor pode variar de 0 a 1000 segundos. Por padrão o valor é *3 segundos*.
- **pri:** prioridade do servidor RADIUS.

Modo de comando: modo de configuração do grupo de servidores.

Exemplo: adicione um servidor no grupo de servidores TACACS+ de nome testes e endereço IP 192.168.0.1 e senha user.

INTELBRAS_config#aaa group server tacacs+ teste

INTELBRAS_config_sg_tacacs+_teste#server 192.168.0.1 key 0 user

Depuração

Descrição: o comando **debug aaa authentication** é usado para rastrear o processo de autenticação de cada usuário para detectar a causa da falha de autenticação.

Sintaxe: **debug aaa authentication**
no debug aaa authentication

Modo de comando: privileged EXEC.

Exemplo: habilite a função *debug* para autenticação AAA.

INTELBRAS#debug aaa authentication

Senha para privilégios

Descrição: o comando **enable password** é usado para definir uma senha local para controle de acesso aos vários níveis de privilégios de configuração.

Sintaxe: **enable password** *password* | *encryption-type* | *encrypted-password* level *number*
no enable password level *number*

Parâmetros:

- **password:** senha configurada para a linha com tamanho máximo é de 30 caracteres.
- **encryption-type:** com ou sem criptografia. Escolha 0 para senha sem criptografia e 7 para senha com criptografia.
- **encrypted-password:** se na opção anterior for escolhido 7, a senha inserida já deve estar criptografada.
- **number:** valor para o nível de privilégio de acesso. Quanto maior o level maior o privilégio para executar os comandos. Pode variar de 1 a 15.

Modo de comando: Global Configuration.

Exemplo: habilite o acesso pela senha teste_123 sem criptografia com nível de acesso 15.

INTELBRAS_config#enable password 0 teste_123 level 15

Criptografia das senhas

Descrição: o comando **service password-encryption** é usado para criptografar as senhas exibidas no show running-config.

Sintaxe: **service password-encryption**
no service password-encryption

Modo de comando: Global Configuration.

Exemplo: habilite a configuração da senha para todos os níveis e usuários.

INTELBRAS_config#service password-encryption

16.2. Autorização

Descrição: o comando **aaa authorization** é usado para configurar os parâmetros para limitar o acesso do usuário à rede.

Sintaxe: **aaa authorization commands** (*0-15*) network | exec *default* | *list-name method1 [method2*
no authorization commands (0-15) network | exec *default* | *list-name*
aaa authorization config-commands
no aaa authorization config-commands

Parâmetros:

- **(0-15):** valor para o nível de privilégio de acesso. Quanto maior o level maior o privilégio para executar os comandos. Pode variar de 1 a 15.
- **default:** lista de autenticação padrão.
- **list-name:** lista de autenticação nomeada.
- **metlhod:** lista do método de autenticação. No final da lista insira a opção *none*. Ela será aplicada caso nenhuma outra esteja válida.

Enable	Usa a senha de ativação para autenticação
group name	Usa o grupo de servidores para autenticação
group radius	Usa autenticação RADIUS
group tacacs+	Usa autenticação de grupo TACACS+
If-authenticated	Necessita autorização do usuário
local	Usa o banco de dados de nome de usuário para autenticação
none	Não usa autenticação

Modo de comando: Global Configuration.

Exemplo: o exemplo mostra como configurar uma lista de métodos de autorização de rede chamada teste. A lista de métodos designa o método de autorização RADIUS. Se o servidor RADIUS não responder, a autorização da rede local será executada.

INTELBRAS_config#aaa authorization exec teste group radius local

Depuração

Descrição: o comando **debug aaa authorization** é usado para rastrear o processo de autenticação de cada usuário para detectar a causa da falha de autorização.

Sintaxe: **debug aaa authorization**
no debug aaa authorization

Modo de comando: Privileged EXEC.

Exemplo: habilite a função *debug* para autorização para AAA.

INTELBRAS#debug aaa authorization

16.3. Contas locais

Descrição: o comando **aaa accounting** é usado para configurar os parâmetros de coleta de dados dos acessos do usuário à rede através dos métodos RADIUS ou TACACS+.

Sintaxe: **aaa accounting commands** *(0-15)* network | exec | connection *default* | *list-name* start-stop | stop-only group *groupname* radius | tacacs+ none
no aaa accounting network | exec | connection *default* | *list-name*

Parâmetros:

- **(0-15):** valor para o nível de privilégio de acesso. Quanto maior o level maior o privilégio para executar os comandos. Pode variar de 1 a 15.
- **default:** lista de accounting padrão.
- **list-name:** lista de accounting nomeada.

start-stop	Inicio e fim da coleta de dados
stop-only	Coleta de dados somente no final
none	Não usa a função
group name	Usa o grupo de servidores para coleta de dados
group radius	Usa coleta de dados através do RADIUS
group tacacs+	Usa coleta de dados através do Tacacs+

Modo de comando: Global Configuration.

Exemplo: o exemplo mostra como configurar uma lista de métodos de coleta de estatísticas do grupo chamada teste.

INTELBRAS_config#aaa accounting commands 15 default stop-only group teste

Upload das estatísticas

Descrição: o comando **aaa accounting update** é usado para transmitir periodicamente as estatisticas coletadas para o servidor.

Sintaxe: **aaa accounting update** newinfo | periodic *number*
no aaa accounting update newinfo | periodic

Parâmetros:

- **update:** ativa o dispositivo para transmitir.
- **newinfo:** transmite ao servidor quando há uma nova informação de estatística.
- **periodic:** transmite as estatísticas ao servidor por um período de tempo preestabelecido.
- **number:** define o período da coleta dos dados.

Modo de comando: Global Configuration.

Exemplo: o exemplo mostra como configurar o envio das estatísticas ao servidor durante um determinado período de tempo (30 minutos).

INTELBRAS_config#aaa accounting update periodic 30

Estatística de desconhecidos

Descrição: o comando **aaa accounting suppress null-username** é usado para encerrar a coleta de estatísticas dos desconhecidos.

Sintaxe: **aaa accounting suppress null-username**
no aaa accounting suppress null-username

Modo de comando: Global Configuration.

Depuração

Descrição: o comando **debug aaa accouting** é usado para rastrear o processo de coleta das estatísticas coletadas para o servidor.

Sintaxe: **debug aaa accounting**
no debug aaa accounting

Modo de comando: Privileged EXEC.

Exemplo: habilite a função *debug* para coletas de informações para AAA.

INTELBRAS#debug aaa accouting

17. Usuários

Para criar ou editar um usuário pela CLI é necessário utilizar os comandos a seguir.

17.1. Políticas de privilégio

Descrição: o comando **localauthor** é usado para criar um grupo de privilégios de acesso. Este comando configura o nível de privilégios do usuário, convidado ou administrador.

Sintaxe: **localauthor** *word*
no localauthor *word*

Modo de comando: Global Configuration.

Parâmetros:

» **word:** nome do configurador de usuários.

Exemplo: crie um grupo de privilégios com o nome usuario_local.

INTELBRAS_config#localauthor usuario_local

Nível de privilégio

Descrição: o comando **exec privilege** é usado para configurar o nível de prioridade do usuário.

Sintaxe: **exec privilege** *default* | console | *ssh* | *telnet autho*
no exec privilege *default* | *console* | *ssh* | *telnet*

Modo de comando: modo de configuração do grupo de políticas locais.

Parâmetros:

» **default:** para definir o nível de privilégio padrão para o usuário local.
» **console:** para definir o nível de privilégio padrão para o acesso console.
» **ssh:** para definir o nível de privilégio padrão para o acesso SSH.
» **telnet:** para definir o nível de privilégio padrão para o acesso Telnet.
» **autho:** define o privilégio para o configurador de usuários. Podendo variar de 1 a 15. Para configurações onde o nível escolhido estiver entre 1 e 8 o usuário será do tipo *user*, com acessos limitados de visualização. Para configurações onde o nível escolhido estiver entre 9 e 15 o usuário será do tipo *admin*. Para um usuário com acesso total, atribua o valor 15 para o configurador de usuários.

Exemplo 1: crie um configurador de usuários com o nome admin_local e nível de acesso admin total.

INTELBRAS_config#localauthor admin_local

INTELBRAS_config_localauthor_admin_local#exec privilege default 15

Exemplo 2: crie um configurador de usuários com o nome usuario_local e nível de acesso user.

INTELBRAS_config#localauthor usuario_local

INTELBRAS_config_localauthor_usuario_local#exec privilege default 8

17.2. Políticas de senha

Descrição: o comando **localpass** é usado para configurar um grupo onde será definido os parâmetros de senha. Esta senha pode ser customizada de acordo com a necessidade do usuário.

Sintaxe: **localpass** *word*
no localpass *word*

Modo de comando: Global Configuration.

Parâmetros:

» **word:** nome para o configurador de senhas.

Exemplo: crie um grupo de senha com o nome senha_admin_local.

INTELBRAS_config#localpass senha_admin_local

Relação usuário-senha

Descrição: o comando **non-user** é usado para configurar se a senha configurada pode ser a mesma do nome do usuário criado.

Sintaxe: **non-user**
no non-user

Modo de comando: modo de configuração do grupo de políticas locais.

Exemplo: permita que a senha de usuário possa ser igual ao nome do usuário. Por exemplo, o usuário e a senha serão user.

INTELBRAS_config#localpass senha_admin_local

INTELBRAS_config_localpass_senha_local#no non-user

Formato

Descrição: o comando **element** é usado para configurar se a senha configurada pode ter números, letras maiúsculas ou minúsculas e caractere especial.

Sintaxe: **element** *number* | *lower-letter* | *upper-letter* | *special-character*
no non-user

Modo de comando: modo de configuração do grupo de políticas locais.

Parâmetros:

- **number:** faz com que a senha necessite ser criada com números.
- **lower-letter:** faz com que a senha necessite ser criada com letras minúsculas.
- **upper-letter:** faz com que a senha necessite ser criada com letras maiúsculas.
- **special-character:** faz com que a senha necessite ser criada com caracteres especiais.

Exemplo: configure que a senha de usuário deve ser configurada com números e letras maiúsculas.

INTELBRAS_config#localpass senha_admin_local

INTELBRAS_config_localpass_senha_admin_local#element number

INTELBRAS_config_localpass_senha_admin_local#element upper-letter

Tamanho

Descrição: o comando **min-length** é usado para configurar o tamanho mínimo da senha.

Sintaxe: **min-length** *(1-127)*
no min-length

Modo de comando: modo de configuração do grupo de políticas locais.

Parâmetros:

- **(1-127):** indica a quantidade de caracteres que a senha deve ter.

Exemplo: configure a senha de usuário com o mínimo de 10 caracteres.

INTELBRAS_config_localpass_senha_local#min-length 10

Validade

Descrição: o comando **validity** é usado para configurar o tempo que o usuário ficará válido para acessar o equipamento.

Sintaxe: **validity** *1d2h3m4s*
no validity

Modo de comando: modo de configuração do grupo de políticas locais.

Parâmetros:

- **1d2h3m4s:** formato do tempo de validade do usuário. Para obter uma senha que não tenha validade, este parâmetro não deve ser configurado.

Exemplo: configure a senha de usuário com validade de 1 dia.

INTELBRAS_config_localpass_senha_local#validity 1d0h0m0s

17.3. Usuário

Descrição: o comando **username** é usado para adicionar usuários ao equipamento e configurar a senha de acesso. Os níveis de permissão e a estrutura da senha devem ser configuradas nos comandos **localauthor, exec privilegie, localpass, non-user, element, min-length** e **validity**.

Sintaxe: **username** *username* password *password* | *pass* | *string* author-group *word_author* pass-group *word_pass*
no username *username*

Modo de comando: Global Configuration.

Parâmetros:

- **password:** com ou sem criptografia. Escolha 0 para senha sem criptografia e 7 para senha com criptografia.
- **pass:** se escolhido 0 na opção *password* anterior a senha pode ter até 127 caracteres, mas, se for escolhido 7, a senha de acesso inserida já deve estar criptografada.
- **string:** senha de acesso sem criptografia. Tamanho máximo de 130 caracteres.
- **word_author:** informe o nome do grupo de privilégios de usuários criado. Este será o configurador que definirá o nível de acesso permitido ao usuário. Veja o comando *localauthor*.
- **word_pass:** informe o nome do grupo criado onde foram definidos os parâmetros da senha. Veja o comando *localpass*.

Exemplo: configure um usuário user com a senha A1234@ com nível de acesso administrador.

INTELBRAS_config#localauthor user_admin

INTELBRAS_config_localauthor_user_admin#exec privilege default 15

INTELBRAS_config_localauthor_user_admin#exit

INTELBRAS_config#localpass user_admin_pass

INTELBRAS_config_localpass_user_admin_pass#element upper-letter

INTELBRAS_config_localpass_user_admin_pass#element special-character

INTELBRAS_config_localpass_user_admin_pass#min-length 6

INTELBRAS_config_localpass_user_admin_pass#exit

INTELBRAS_config#username user password A1234@ author-group user_admin pass-group user_admin_pass

17.4. Informações

Descrição: o comando **show local-users** é usado para mostrar os usuários que estão configurados no equipamento, usuário ativo e informações sobre problemas de acesso.

Sintaxe: **show local-users**

Modo de comando: todos os modos de configuração.

18. RADIUS

18.1. Depuração

Descrição: o comando **debug radius** é usado para depurar o sistema de rede e encontrar o motivo da falha de autenticação do usuário.

Sintaxe: **debug radius** *event* | *packet*
no debug radius *event* | *packet*

Modo de comando: Privileged EXEC.

Parâmetros:

- **event:** rastreando o evento RADIUS.
- **packet:** rastreando pacotes RADIUS.

Exemplo: habilite o debug radius para a opção de verificação dos eventos.

INTELBRAS#debug radius event

18.2. Interface de origem

Descrição: o comando **ip radius source-interface** é usado para configurar um endereço IP em uma subinterface como origem para todos os pacotes RADIUS.

Sintaxe: **ip radius source-interface** *subinterface_name*
no ip radius source-interface

Modo de comando: Global Configuration.

Parâmetros:

» **subinterface_name:** interface que o RADIUS usará para todos os pacotes de saída.

Exemplo: habilite a subinterface VLAN 1 como sendo a origem de todos os pacotes RADIUS.

INTELBRAS_config#ip radius source-interface VLAN 1

18.3. Atributos

Descrição: o comando **radius-server attribute** é usado para designar um atributo específico a ser transmitido durante a autenticação ou requisição RADIUS.

Sintaxe: **radius-server attribute** *4 | 32 | 95*
no ip radius source-interface *4 | 32 | 95*

Modo de comando: Global Configuration.

Parâmetros:

» **4:** transmite o endereço IP como atributo 4 (endereço IP do NAS) durante a operação do RADIUS.
» **32:** transmite o atributo 32 (identificador NAS) durante a autenticação ou solicitação de RADIUS.
» **95:** transmite o endereço IPv6 como atributo 95 (NAS ipv6).

Exemplo: habilite o switch a enviar o endereço IP 192.168.0.50 como atributo para o RADIUS.

INTELBRAS_config#radius-server attribute 4 192.168.0.50

18.4. Access-challenge

Descrição: o comando **radius-server challenge-noecho** é usado para ocultar os dados do usuário durante o processo de Access-challenge com o servidor RADIUS.

Sintaxe: **radius-server challenge-noecho**
no radius-server challenge-noecho

Modo de comando: Global Configuration.

Exemplo: habilite o switch a proteger os dados do usuário durante a autenticação em um servidor RADIUS.

INTELBRAS_config#radius-server challenge-noecho

18.5. Tempo de espera

Descrição: o comando **radius-server deadtime** é usado para informar quais servidores RADIUS não estão acessíveis, evitando esperar por muito tempo antes de tentar acesso a outros servidores.

Sintaxe: **radius-server deadtime** *(0-1440)*
no radius-server deadtime

Modo de comando: Global Configuration.

Parâmetros:

» **(0-1440):** a duração do tempo de espera até considerar o servidor como inacessível.

Exemplo: habilite o switch a esperar até 5 minutos para considerar como inacessível um servidos RADIUS.

INTELBRAS_config#radius-server deadtime 5

18.6. Requisição direta

Descrição: o comando **radius-server directed-request** é usado para permitir que o usuário possa estabelecer o servidor RADIUS com o formato *@server*.

Sintaxe: **radius-server directed-request** *restricted*
no radius-server directed-request *restricted*

Modo de comando: Global Configuration.

Parâmetros:

» **restricted:** restringe consultas somente a servidores informados.

Exemplo:

INTELBRAS_config#radius-server directed-request restricted

18.7. Host

Descrição: o comando **radius-server host** é usado para informar o endereço IP do servidor RADIUS.

Sintaxe: **radius-server host** *A.B.C.D | X:X:X:X::X acct-port | auth-port port*
no radius-server host *A.B.C.D | X:X:X:X::X*

Modo de comando: Global Configuration.

Parâmetros:

» **A.B.C.D:** endereço IP do servidor RADIUS.
» **X:X:X:X::X:** endereço IPv6 do servidor RADIUS.
» **acct-port:** porta UDP para o servido de contabilidade RADIUS. Por padrão a porta usada é a *1813*.
» **auth-port:** porta UDP para o servido de autenticação RADIUS. Por padrão a porta usada é a *1812*.
» **port:** porta UDP a ser configurada. Pode variar da porta 1 até 65535.

Exemplo: configure um servidor RADIUS com o IP 192.168.10.2, a porta UDP 12 como autenticação e a porta UDP 16 como contabilidade RADIUS.

INTELBRAS_config#radius-server host 192.168.10.2 acct-port 16 auth-port 12

18.8. Senha de acesso

Descrição: o comando **radius-server key** é usado para configurar uma senha de acesso ao servidor RADIUS.

Sintaxe: **radius-server key** *password | pass | string*
no radius-server key

Modo de comando: Global Configuration.

Parâmetros:

» **password:** com ou sem criptografia. Escolha 0 para senha sem criptografia e 7 para senha com criptografia.
» **pass:** se escolhido 0 na opção password anterior a senha pode ter até 127 caracteres, mas, se for escolhido 7, a senha de acesso inserida já deve estar criptografada.
» **string:** senha de acesso sem criptografia. Tamanho máximo de 130 caracteres.

Exemplo: configure a senha *primeiro-acesso* para acessar a um servidor RADIUS.

INTELBRAS_config#radius-server key primeiro-acesso

18.9. Senha opcional

Descrição: o comando **radius-server optional-passwords** é usado para configurar que no primeiro acesso a um servidor RADIUS a senha não seja enviada. O servidor deve suportar este tipo de configuração.

Sintaxe: **radius-server optional-passwords**
no radius-server optional-passwords

Modo de comando: Global Configuration.

Exemplo:

INTELBRAS_config#radius-server optional-passwords

18.10. Tentativas de acesso

Descrição: o comando **radius-server retransmit** é usado para especificar o número de vezes que o será realizado uma pesquisa na lista de hosts do servidor RADIUS antes de desistir. Normalmente usado com o comando **radius-server timeout**.

Sintaxe: **radius-server retransmit** *retries*
no radius-server retransmit

Modo de comando: global Configuration.

Parâmetros:

» **retries:** número máximo de tentativas de retransmissão. Por padrão são *2 tentativas*. Podem ser configuradas entre 0 e 100 tentativas.

Exemplo:

INTELBRAS_config#radius-server retransmit 5

18.11. Tempo de espera

Descrição: o comando **radius-server timeout** é usado para definir o intervalo durante o qual o equipamento aguarda a resposta de um servidor RADIUS.

Sintaxe: **radius-server timeout** *(0-1000)*
no radius-server timeout

Modo de comando: Global Configuration.

Parâmetros:

» **(0-1000):** tempo limite de espera para resposta do servidor RADIUS.

Exemplo:

INTELBRAS_config#radius-server timeout 15

18.12. VSA Send

Descrição: o comando **radius-server vsa send** é usado para comunicar atributos específicos do cliente com o servidos RADIUS.

Sintaxe: **radius-server vsa send** *authentication*
no radius-server vsa send *authentication*

Modo de comando: Global Configuration.

Parâmetros:

» **authentication:** configura apenas atributos relativos a autenticação

Exemplo:

INTELBRAS_config#radius-server vsa send authentication

18.13. Acct-on

Descrição: o comando **radius-server acct-on** é usado para iniciar a função de contabilização de dados e retransmissão de pacotes para o servidor RADIUS.

Sintaxe: **radius-server acct-on** *enable* | *retransmit*
no radius-server acct-on enable | retransmit

Modo de comando: Global Configuration.

Parâmetros:

» **enable:** ativa a contabilização de pacotes para servidor RADIUS.

» **retransmit:** configura o tempo de retransmissão dos pacotes de contabilização RADIUS. O tempo de retransmissão é de 3 segundos.

Exemplo:

INTELBRAS_config#no radius-server acct-on enable

INTELBRAS_config#no radius-server acct-on retransmit

19. TACACS

19.1. Depuração

Descrição: o comando **debug tacacs** é usado para rastrear o protocolo TACACS ou verificar os pacotes recebidos e enviados.

Sintaxe: **debug tacacs** *event* | *packet*
no debug tacacs *event* | *packet*

Modo de comando: Privileged EXEC.

Parâmetros:

- **event:** rastreando o evento TACACS.
- **packet:** rastreando pacotes TACACS.

Exemplo: habilite o debug TACACS para a opção de verificação dos eventos.

INTELBRAS#debug tacacs event

19.2. Interface de origem

Descrição: o comando **ip tacacs source-interface** é usado para configurar um endereço IP em uma subinterface como origem para todos os pacotes TACACS.

Sintaxe: **ip tacacs source-interface** *subinterface_name*
no ip tacacs source-interface

Modo de comando: Global Configuration.

Parâmetros:

- **subinterface_name:** interface que o TACACS usará para todos os pacotes de saída.

Exemplo: habilite a subinterface VLAN 1 como sendo a origem de todos os pacotes TACACS.

INTELBRAS_config#ip tacacs source-interface VLAN 1

19.3. Host

Descrição: o comando **tacacs-server host** é usado para informar o endereço IP do servidor TACACS além de configurações extras como timeout de resposta do servidor, senha para autenticação e portas de conexão.

Sintaxe: **tacacs-server host** *A.B.C.D* | *X:X:X:X::X key* | *port* | *timeout* | *single-connect* | *multi-connect*
no tacacs-server host *A.B.C.D* | *X:X:X:X::X*

Modo de comando: Global Configuration.

Parâmetros:

- **A.B.C.D:** endereço IP do servidor TACACS.
- **X: X:X:X::X:** endereço IPv6 do servidor TACACS.
- **key:** senha criptografada ou não para acessar o servidor. Deve ser a mesma configurada no servidor TACACS.
- **port:** porta a ser configurada. Pode variar da porta 1 até 65535. Por padrão a porta usada é a *49*.
- **timeout:** tempo limite de espera pela resposta do servidor.
- **single-connect:** uma única conexão TCP.
- **multi-connect:** múltiplas conexões TCP.

Exemplo: configure um servidor TACACS com o IP 192.168.10.2, porta 12, com a senha 12345, e timeout de 1 segundo.
INTELBRAS_config#tacacs-server host 192.168.10.2 key 12345 port 12 timeout 1

19.4. Senha de acesso

Descrição: o comando **tacacs-server key** é usado para configurar uma senha de acesso ao servidor TACACS.

Sintaxe: **tacacs-server key** *password* | *pass* | *string*
no tacacs-server key

Modo de comando: Global Configuration.

Parâmetros:

- **password:** com ou sem criptografia. Escolha 0 para senha sem criptografia e 7 para senha com criptografia.
- **pass:** se escolhido 0 na opção password anterior a senha pode ter até 127 caracteres, mas, se for escolhido 7, a senha de acesso inserida já deve estar criptografada.
- **string:** senha de acesso sem criptografia. Tamanho máximo de 130 caracteres.

Exemplo: configure a senha "primeiro-acesso" para acessar a um servidor TACACS.

INTELBRAS_config#tacacs-server key primeiro-acesso

19.5. Tempo de espera

Descrição: o comando **tacacs-server timeout** é usado para definir o intervalo durante o qual o equipamento aguarda a resposta de um servidor TACACS. Este comando terá prioridade sobre a configuração realizada no comando *tacacs-server host* em relação ao timeout.

Sintaxe: **tacacs-server timeout** *(0-600)*
no radius-server timeout

Modo de comando: Global Configuration.

Parâmetros:

- **(0-600):** tempo limite de espera para resposta do servidor TACACS.

Exemplo:

INTELBRAS_config#tacacs-server timeout 10

20. 802.1x (Dot1x)

Descrição: o comando **dot1x enable** é usado para habilitar a autenticação 802.1x (dot1x) de forma global no switch.

Sintaxe: **dot1x enable**
no dot1x enable

Modo de comando: Global Configuration.

Exemplo:

INTELBRAS_config#dot1x enable

INTELBRAS_config#no dot1x enable

20.1. Habilitar na interface

Descrição: o comando **dot1x port-control** é usado para configurar a autenticação 802.1x (dot1x) nas interfaces Ethernet do switch.

Sintaxe: **dot1x port-control** auto | force-authorized | force-unauthorized | misc-mab
no dot1x enable

Modo de comando: interface de configuração Ethernet.

Parâmetros:

- **auto:** autenticar automaticamente.
- **force-authorized:** força a porta para o estado autorizado.
- **force-unauthorized:** força a porta para o estado não autorizado.
- **misc-mab:** modo promíscuo de multiautenticação.

Exemplo: habilite a autenticação automática na interface GigaEthernet 1.

INTELBRAS_config#interface GigaEthernet 0/1

INTELBRAS_config_g0/1#dot1x port-control auto

20.2. Autenticação única

Descrição: o comando **dot1x authentication multiple-hosts** é usado para autenticar usuários nas interfaces Ethernet do switch. Se apenas um usuário for autenticado a porta será liberada para acessos sem necessidade de autenticação.

Sintaxe: **dot1x authentication multiple-hosts**
no dot1x authentication multiple-hosts

Modo de comando: interface de configuração Ethernet.

Exemplo: habilite a autenticação de usuários na interface GigaEthernet 1.

INTELBRAS_config#interface GigaEthernet 0/1

INTELBRAS_config_g0/1#dot1x authentication multiple-hosts

20.3. Multiplas autenticações

Descrição: o comando **dot1x authentication multiple-auth** é usado para autenticar usuários que desejam acesso pela interface Ethernet do switch. Será necessário a autenticação de todos os usuários.

Sintaxe: **dot1x authentication multiple-auth**
no dot1x authentication multiple-auth

Modo de comando: interface de configuração Ethernet.

Exemplo: habilite a autenticação para todos os usuários na interface GigaEthernet 1.

INTELBRAS_config#interface GigaEthernet 0/1

INTELBRAS_config_g0/1#dot1x authentication multiple-auth

20.4. Configuração padrão

Descrição: o comando **dot1x default** é usado para voltar as configurações de 802.1x (dot1x) para as configurações padrão.

Sintaxe: **dot1x default**

Modo de comando: Global Configuration.

Exemplo:

INTELBRAS_config#dot1x default

20.5. Número máximo de tentativas

Descrição: o comando **dot1x reauth-max** é usado para configurar o número máximo de tentativas de autenticação.

Sintaxe: **dot1x reauth-max** *(1-10)*
no dot1x reauth-max

Parâmetros:

» **(1-10):** número de tentativas de autenticação.

Modo de comando: Global Configuration.

Exemplo:

INTELBRAS_config#dot1x reauth-max 4

20.6. Reautenticação

Descrição: o comando **dot1x re-authentication** é usado para configurar se o usuário deve ser reautenticado depois de um intervalo de tempo. O tempo pode ser configurado no comando **dot1x timeout re-authperiod**.

Sintaxe: **dot1x re-authenticatiom**
no dot1x re-authenticatiom

Modo de comando: Global Configuration.

Exemplo:

INTELBRAS_config#no dot1x re-authentication

20.7. Período de silêncio

Descrição: o comando **dot1x timeout quiet-period** é usado para configurar o período de silêncio após uma tentativa de autenticação com falha.

Sintaxe: **dot1x timeout quiet-period** *(0-65535)*
no dot1x timeout quiet-period

Parâmetros:

» **(0-65535):** intervalo de tempo em segundos.

Modo de comando: Global Configuration.

Exemplo:

INTELBRAS_config#dot1x timeout quiet-period 180

20.8. Intervalo entre autenticações

Descrição: o comando **dot1x timeout re-authperiod** é usado para definir o período de tempo entre tentativas de nova autenticação.

Sintaxe: **dot1x timeout re-authperiod** *(1-4294967295)*
no dot1x timeout re-authperiod

Parâmetros:

» **(1-4294967295):** intervalo de tempo em segundos.

Modo de comando: Global Configuration.

Exemplo:

INTELBRAS_config#dot1x timeout re-authperiod 300

20.9. Solicitar nova autenticação

Descrição: o comando **dot1x timeout tx-period** é usado para definir o intervalo de resposta da solicitação de autenticação do cliente. Se o intervalo for excedido, o switch retransmitirá a solicitação de autenticação.

Sintaxe: **dot1x timeout tx-period** *(1-65535)*
no dot1x timeout tx-period

Parâmetros:

» **(1-65535):** intervalo de tempo em segundos.

Modo de comando: Global Configuration.

Exemplo:

INTELBRAS_config#dot1x timeout tx-period 600

20.10. Autenticação MAB

Descrição: o comando **dot1x mab** é usado para autenticar um host que não suporta autenticação 802.1x (dot1x). Com isso o host envio o seu endereço MAC como usuário e senha de autenticação.

Sintaxe: **dot1x mab**
no dot1x mab

Modo de comando: interface de configuração Ethernet.

Exemplo:

INTELBRAS_config_f0/5#dot1x mab

Formato do endereço MAC

Descrição: o comando **dot1x mabformat** é usado para definir como será o formato do endereço MAC.

Sintaxe: **dot1x mabformat** *1* | *2* | *3* | *4* | *5* | *6*
no dot1x mabformat

Parâmetros:

- **1:** formato do endereço MAC: *aa:bb:cc:dd:ee:ff*.
- **2:** formato do endereço MAC: *AA:BB:CC:DD:EE:FF*.
- **3:** formato do endereço MAC: *aabbccddeeff*.
- **4:** formato do endereço MAC: *AABBCCDDEEFF*.
- **5:** formato do endereço MAC: *aa-bb-cc-dd-ee-ff*.
- **6:** formato do endereço MAC: *AA-BB-CC-DD-EE-FF*.

Modo de comando: Global Configuration.

Exemplo:

INTELBRAS_config#no dot1x mabformat 2

20.11. Configuração de usuário

Descrição: o comando **dot1x user-permit** é usado para vincular usuários a uma interface Ethernet para permissão de autenticação 802.1x (dot1x). Cada interface aceita a até 8 usuários configurados.

Sintaxe: **dot1x user-permit** *word*
no dot1x user-permit

Modo de comando: interface de configuração Ethernet.

Exemplo:

INTELBRAS_config#interface FastEthernet 0/5

INTELBRAS_config_f0/5#dot1x user-permit acesso

20.12. Método de autenticação

Descrição: o comando **dot1x authentication method** é usado para configurar um método de autenticação na interface do switch. Uma interface utiliza apenas um método de autenticação fornecido pelo AAA.

Sintaxe: **dot1x authentication method** *word*
no dot1x authentication method

Modo de comando: interface de configuração Ethernet.

Exemplo:

- INTELBRAS_config#interface FastEthernet 0/5
- INTELBRAS_config_f0/5#dot1x authentication method teste

20.13. Estatísticas de autenticação

Descrição: o comando **dot1x accounting enable** é usado para habilitar as estatísticas de autenticação 802.1x na interface.

Sintaxe: **dot1x accounting enable**
no dot1x accounting enable

Modo de comando: interface de configuração Ethernet.

Exemplo:

INTELBRAS_config#interface GigaEthernet 0/1

INTELBRAS_config_g0/1#dot1x accounting enable

20.14. Método de contas

Descrição: o comando **dot1x accounting method** é usado para configurar um método para contabilizar as estatísticas de autenticação 802.1x (dot1x) na interface. Deve ser um método conhecido pelo AAA, e estará ativo quando a estatística 801.x (dot1x) estiver habilitada.

Sintaxe: **dot1x accounting method** *word*
no dot1x accounting method

Parâmetros:

» **word:** nome do método de autenticação AAA.

Modo de comando: interface de configuração Ethernet.

Exemplo:

INTELBRAS_config#aaa accounting network acesso start-stop group radius

INTELBRAS_config#radius-server host 192.168.20.100

INTELBRAS_config#interface GigaEthernet 0/1

INTELBRAS_config_g0/1#dot1x accounting method acesso

20.15. Protocolo de autenticação global

Descrição: o comando **dot1x authen-type** é usado para configurar o tipo de protocolo de autenticação será utilizado globalmente no switch, podendo ser CHAP ou EAP.

Sintaxe: **dot1x authen-type** *CHAP | EAP*
no dot1x authen-type

Parâmetros:

» **CHAP:** seleciona o protocolo CHAP para autenticação.

» **EAP:** seleciona o protocolo EAP para autenticação.

Modo de comando: Global Configuration.

Exemplo:

INTELBRAS_config#dot1x authen-type CHAP

20.16. Protocolo de autenticação nas interfaces

Descrição: o comando **dot1x authentication type** é usado para configurar o tipo de protocolo de autenticação será utilizado localmente na interface Ethernet, podendo ser CHAP ou EAP.

Sintaxe: **dot1x authentication type** *CHAP | EAP*
no dot1x authentication type

Parâmetros:

» **CHAP:** seleciona o protocolo CHAP para autenticação.

» **EAP:** seleciona o protocolo EAP para autenticação.

Modo de comando: interface de configuração Ethernet.

Exemplo:

INTELBRAS_config#interface GigaEthernet 0/1

INTELBRAS_config_g0/1#dot1x authentication type EAP

20.17. Guest-VLAN

Descrição: o comando **dot1x guest-vlan** é usado para habilitar a função *guest-vlan* globalmente. Depois que a função *guest-vlan* for ativada, a interface GigaEthernet poderá ser agrupada na VLAN de visitante (guest).

Sintaxe: **dot1x guest-vlan**
no dot1x guest-vlan

Modo de comando: Global Configuration.

Exemplo:

INTELBRAS_config#dot1x guest-vlan

20.18. Guest-VLAN nas interfaces

Descrição: o comando **dot1x guest-vlan** é usado para configurar o ID do guest-vlan na interface Ethernet.

Sintaxe: **dot1x guest-vlan** *(1-4094)*
no dot1x guest-vlan

Parâmetros:

» **(1-4094):** configuração da VLAN para usuários guest.

Modo de comando: interface de configuração Ethernet.

Exemplo: configure a interface GigaEthernet 1 na VLAN de visitantes com o ID 20.

INTELBRAS_config#interface gigaEthernet 0/1

INTELBRAS_config_g0/1#dot1x guest-vlan 20

20.19. Proibir múltiplos adaptadores de rede

Descrição: o comando **dot1x forbid multi-network-adapter** é usado para configurar a interface Ethernet a proibir múltiplos adaptadores de rede.

Sintaxe: **dot1x forbid multi-network-adapter**
no dot1x forbid multi-network-adapter

Modo de comando: interface de configuração Ethernet.

Exemplo: configure a interface GigaEthernet 1 para proibir o uso de múltiplos adaptadores de rede nesta interface.

INTELBRAS_config#interface GigaEthernet 0/1

INTELBRAS_config_g0/1#dot1x forbid multi-network-adapter

20.20. Detecção de atividade

Descrição: o comando **dot1x keepalive** é usado para habilitar ou desabilitar a detecção de atividade no switch de maneira global.

Sintaxe: **dot1x keepalive**
no dot1x keepalive

Modo de comando: global Configuration.

Exemplo:

INTELBRAS_config#dot1x keepalive

20.21. Autenticação de senha 802.1x (dot1x)

Descrição: o comando **aaa authentication dot1x** é usado para configurar o método de autenticação da senha 802.1x (dot1x).

Sintaxe: **aaa authentication dot1x** *WORD* | default group | local | local-case | none *server_name* | radius | tacacs+
no aaa authentication dot1x *WORD* | default

Parâmetros:

» **WORD:** cria uma lista de autenticação nomeada.
» **default:** utiliza uma lista de autenticação padrão.
» **group:** utiliza o grupo de servidores.
» **local:** utiliza autenticação de nome de usuário local.
» **local-case:** utiliza a autenticação de usuário local, diferencia letras maiúsculas e minúsculas.
» **none:** não utiliza a autenticação AAA.
» **server_name:** nome do grupo de servidores.
» **radius:** utiliza a lista do host RADIUS.
» **tacacs+:** utiliza a lista do host TACACS+.

Modo de comando: Global Configuration.

Exemplo:

INTELBRAS_config#aaa authentication dot1x ACCESS group radius

20.22. Depuração

Descrição: o comando **debug dot1x** é usado para depuração do 802.1x.

Sintaxe: **debug dot1x** errors | state | packet
no debug dot1x errors | state | packet

Parâmetros:

» **errors:** depuração de erros.
» **state:** depuração do status.
» **packet:** depuração dos pacotes.

Modo de comando: privileged EXEC.

Exemplo:

INTELBRAS#debug dot1x errors

20.23. Informações

Descrição: o comando **show dot1x** é usado para informar os parâmetros de configuração de 802.1x (dot1x).

Sintaxe: **show dot1x** interface GigaEthernet *interface_id* | statistics | misc-mab-db
no debug dot1x packet

Parâmetros:

» **interface_id:** exibe informações da interface FastEthernet de 1 a 24.
» **statistics:** exibe informações de estatísticas 802.1x (dot1x).
» **misc-mab-db:** exibe informações do banco de dados 802.1x (dot1x).

Modo de comando: Privileged EXEC ou Global Configuration.

Exemplo:

INTELBRAS#show dot1x misc-mab-db interface gigaEthernet 0/5

21. Configuração SSH

21.1. Criptografia RSA

Descrição: o comando **ip sshd enable** é utilizado para gerar a chave de criptografia rsa e, em seguida, monitorar a conexão com o servidor SSH. O processo de geração da chave de criptografia é um processo que consome um tempo de processamento e pode levar um ou dois minutos.

Sintaxe: **ip sshd enable**
no ip sshd enable

Modo de comando: Global Configuration.

Exemplo:

INTELBRAS_config#ip sshd enable

21.2. Usuários não autorizados

Descrição: o comando **ip sshd timeout** é utilizado para evitar que usuários não autorizados ocupem recursos de conexão. As conexões que não forem aprovadas serão encerradas de acordo com as configurações realizadas.

Sintaxe: **ip sshd timeout** *(60-65535)*
no ip sshd timeout

Parâmetros:

» **(60-65535):** tempo máximo decorrido do estabelecimento da conexão até a aprovação da autenticação. Por padrão o valor é *180 segundos*.

Modo de comando: Global Configuration.

Exemplo:

INTELBRAS_config#ip sshd timeout 360

21.3. Autenticação SSH

Descrição: o comando **ip sshd auth-method** é utilizado para configurar o método de autenticação SSH.

Sintaxe: **ip sshd auth-method** *method*
no ip sshd auth-method

Parâmetros:

» **method:** define a lista de métodos de autenticação.

Modo de comando: Global Configuration.

Exemplo: configure uma lista de métodos de autenticação auth-ssh e aplique ao servidor SSH.

INTELBRAS_config#aaa authentication login auth-ssh local

INTELBRAS_config#ip sshd auth-method auth-ssh

21.4. Lista de acesso

Descrição: o comando **ip sshd access-class** é utilizado para configurar a lista de controle de acesso para o servidor SSH. Somente as conexões que estão de acordo com os regulamentos da lista de controle de acesso podem ser aprovadas.

Sintaxe: **ip sshd access-class** *access-list*
no ip sshd access-class

Parâmetros:

» **access-list:** nome para a lista de acesso configurada. O comprimento do nome da lista de acesso não ultrapassa 20 caracteres.

Modo de comando: Global Configuration.

Exemplo: configure uma negativa de acesso ao endereço de IP 192.168.20.40 com o nome ssh-accesslist.

INTELBRAS_config#ip access-list standard ssh-accesslist

INTELBRAS_config_std#deny 192.168.20.40

INTELBRAS_config#ip sshd access-class ssh-accesslist

21.5. Acesso SSH

Descrição: o comando **ip sshd auth-retries** é utilizado para encerrar a conexão quando os tempos da nova autenticação excederem os horários definidos.

Sintaxe: **ip sshd auth-retries** *(0-65535)*
no ip sshd auth-retries

Parâmetros:

» **(0-65535):** tempo máximo para a nova autenticação. Por padrão o valor é *6 segundos.*

Modo de comando: Global Configuration.

Exemplo: configure o tempo de acesso para 5 segundos.

INTELBRAS_config#ip sshd auth-retries 5

21.6. Desativar conexão SSH

Descrição: o comando **ip sshd clear** é utilizado para desativar uma conexão SSH específica. Você pode executar o comando show ssh para verificar o número atual da conexão.

Sintaxe: **ip sshd clear** *(0-15)*

Parâmetros:

» **(0-15):** número da conexão ssh com o dispositivo local.

Modo de comando: Global Configuration.

Exemplo:

INTELBRAS_config#ip sshd clear 5

21.7. Período de silêncio de login

Descrição: o comando **ip sshd silence-period** é utilizado para definir o período de silêncio de login. Depois que as falhas de login acumuladas excedem um determinado limite, o sistema considera que existem ataques e desativa o serviço SSH em um período de tempo, ou seja, o sistema entra no período de silêncio de login. As falhas de login permitidas são configuradas pelo comando **ip sshd auth-retries**, cujo valor padrão é *6*.

Sintaxe: **ip sshd silence-period** *(0-3600)*
no ip sshd silence-period

Parâmetros:

» **(0-3600):** configura o tempo de silêncio. O período de silêncio padrão é de *60 segundos*.

Modo de comando: Global Configuration.

Exemplo: configure o período de silencio para 200 segundos.

INTELBRAS_config#ip sshd silence-period 200

21.8. Sistema SFTP

Descrição: o comando **ip sshd sfpd** é usado para ativar a função *SFTP.* A função *SFTP* refere-se ao sistema seguro de transmissão de arquivos baseado em SSH, do qual o procedimento de autenticação e a transmissão de dados são criptografados.

Sintaxe: **ip sshd sfpd**
no ip sshd sfpd

Modo de comando: Global Configuration.

Exemplo: habilite o SFTP no switch.

INTELBRAS_config#ip sshd sftp

21.9. Salva a chave de acesso SSH

Descrição: o comando **ip sshd save** é usado para salvar a chave inicial. Quando o servidor SSH for reiniciado, a chave será lida primeiro da memória flash.

Sintaxe: **ip sshd save**
no ip sshd save

Modo de comando: Global Configuration.

Exemplo: ative a proteção de chave no switch.

INTELBRAS_config#ip sshd save

21.10. Ip sshd disable-aes

Descrição: o comando **ip sshd disable-aes** é usado para configuração do uso do algoritmo AES durante a negociação do algoritmo de criptografia ou não. Por padrão o algoritmo de criptografia AES é proibido.

Sintaxe: **ip sshd disable-aes**
no ip sshd disable-aes

Modo de comando: Global Configuration.

Exemplo: desative o algoritmo de criptografia AES.

INTELBRAS_config#no ip sshd disable-aes

21.11. Conexão SSH

Descrição: o comando **ssh** é usado para criar uma conexão remota com o servidor SSH.

Sintaxe: **ssh** –l *userid* –d *destIP* -c -o -p -v -s

Parâmetros:

- **-l:** conta de usuário no servidor.
- **-d:** endereço IP do servidor SSH.
- **-c:** algoritmo de criptografia usado durante a comunicação (des, 3des ou blowfish).
- **-o:** intervalo de tempo para nova autenticação após a primeira tentativa falhar. O range pode ser de 0 a 65535.
- **-p:** número da porta. O range pode ser de 0 a 65535.
- **-v:** versão SSH cliente, 1 ou 2.
- **-s:** senha de acesso.

Modo de comando: modo Privilegiado.

Exemplo: realize uma conexão com o servidor SSH 192.168.20.41, conta int com algoritmo de criptografia blowfish.

INTELBRAS#ssh -l int -d 192.168.20.41 -c blowfish

21.12. Informações

Descrição: o comando **show ssh** é usado para exibir as sessões no servidor SSH.

Sintaxe: **show ssh**

Modo de comando: modo Privilegiado.

Exemplo:

INTELBRAS#show ssh

22. Configuração web

22.1. Porta HTTP

Descrição: o comando **ip http port** é usado para configurar a porta HTTP.

Sintaxe: **ip http port** *port_number*
no ip http port

Modo de comando: Global Configuration.

Parâmetros:

- **port_number:** porta HTTP a ser configurada. Pode variar da porta 1 até 65535. Por padrão a porta usada é a *80*.

Exemplo:

INTELBRAS_config#ip http port 8080

22.2. Porta HTTPS

Descrição: o comando **ip http secure-port** é usado para configurar a porta HTTPS.

Sintaxe: **ip http secure-port** *port_number*
no ip http secure-port

Modo de comando: Global Configuration.

Parâmetros:

- **port_number:** porta HTTPS a ser configurada. Pode variar da porta 1 até 65535. Por padrão a porta usada é a *443*.

Exemplo:

INTELBRAS_config#ip http secure-port 1234

22.3. Servidor HTTP

Descrição: o comando **ip http server** é usado para habilitar/desabilitar o servidor HTTP do switch para gerenciamento do equipamento via interface web.

Sintaxe: **ip http server**
no ip http server

Modo de comando: Global Configuration.

Exemplo: desabilite o servidor web do switch para o gerenciamento web.

INTELBRAS_config#no ip http server

22.4. Acesso HTTP

Descrição: o comando **ip http http-access enable** é usado para habilitar/desabilitar o gerenciamento do switch via interface web.

Sintaxe: **ip http http-access enable**
no ip http http-access enable

Modo de comando: Global Configuration.

Exemplo: desabilite o gerenciamento web para o switch.

INTELBRAS_config#no ip http http-access enable

22.5. Acesso HTTPS

Descrição: o comando **ip http ssl-access enable** é usado para habilitar/desabilitar o gerenciamento do switch via interface web.

Sintaxe: **ip http http-access enable**
no ip http http-access enable

Modo de comando: Global Configuration.

Exemplo: desabilite o gerenciamento web para o switch.

INTELBRAS_config#no ip http http-access enable

22.6. Use-Footer

Descrição: o comando **ip http web use-footer** é usado para configurar a opção sob a página web do gerenciamento do switch.

Sintaxe: **ip http web use-footer**
no ip http web use-footer

Modo de comando: Global Configuration.

Exemplo:

INTELBRAS_config#ip http web use-footer

22.7. Exibição VLAN

Descrição: o comando **ip http web max-vlan** é usado para definir o número máximo de entradas de VLAN exibidas na página da web.

Sintaxe: **ip http web max-vlan**
no ip http web max-vlan *max_vlan*

Modo de comando: Global Configuration.

Parâmetros:

» **max_vlan:** número de entradas VLAN visíveis na interface web.

Exemplo:

INTELBRAS_config#ip http web max-vlan 100

22.8. Exibição tabela MAC

Descrição: o comando **ip http web max-macaddr-table** é usado para definir o número máximo de endereços MAC exibidas na página da web.

Sintaxe: **ip http web max-macaddr-table max_mac**
no ip http web max-macaddr-table

Modo de comando: Global Configuration.

Parâmetros:

» **max_mac:** número de entradas MAC visíveis na interface web.

Exemplo:

INTELBRAS_config#ip http web max-macaddr-table 100

22.9. Exibição grupos IGMP

Descrição: o comando **ip http web igmp-groups** é usado para definir o número máximo de entradas multicast exibidas na página da web.

Sintaxe: **ip http web igmp-groups** *igmp_groups*
no ip http web igmp-groups

Modo de comando: Global Configuration.

Parâmetros:

» **igmp_groups:** número de grupos IGMP visíveis na interface web.

Exemplo:

INTELBRAS_config#ip http web igmp-groups 100

22.10. Intervalo de atualização

Descrição: o comando **ip http web portpanel update-interval** é usado para definir o intervalo de tempo de atualização do painel de portas.

Sintaxe: **ip http web portpanel update-interval** *update_interval*
no ip http web portpanel update-interval

Modo de comando: Global Configuration.

Parâmetros:

» **update_interval:** intervalo de atualização do painel de portas.

Exemplo:

INTELBRAS_config#ip http web portpanel update-interval 1

22.11. Exibição log

Descrição: o comando **ip http web max-syslog** é usado para configurar o número máximo de logs mostrado na página de gerenciamento web do switch.

Sintaxe: **ip http web max-syslog** *max_syslog*
no ip http web portpanel visible

Modo de comando: Global Configuration.

Parâmetros:

» **max_syslog:** número de entradas no log do sistema.

Exemplo:

INTELBRAS_config#ip http web max-syslogs 300

22.12. Informações

Descrição: o comando **show ip http** é usado para verificar se o servidor HTTP está em execução no switch.

Sintaxe: **show ip http**

Modo de comando: Global Configuration e Mode EXEC.

Exemplo:

INTELBRAS_config#show ip http

23. Configuração da interface

23.1. Interface

Descrição: o comando **interface** é usado para acessar as configurações das portas físicas e lógicas do switch.

Sintaxe: **interface** range GigaEthernet | Vlan | Null *intervalo_interfaces*
interface GigaEthernet | Vlan | Loopback | Port-aggregator | Null *interface_id*
no interface GigaEthernet | Vlan | Null *interface_id*

Parâmetros:

- **GigaEthernet:** especifica que a configuração a ser acessada será a da interface GigaEthernet que é correspondente a uma porta física do switch.
- **VLAN:** especifica que a configuração a ser acessada será a de uma interface VLAN.
- **Port-agreggator:** especifica que a configuração a ser acessada será a da interface de grupo de links agregados (LAG).
- **Null:** especifica que a configuração a ser acessada será a da interface Null.
- **Loopback:** especifica que a configuração a ser acessada será a da interface de Loopback.
- **range:** comando para configuração de um intervalo de interfaces.
- **intervalo_interfaces:** para especificar um intervalo de interfaces utiliza-se "," para adicionar uma interface ao intervalo ou "-" para especificar o limite do intervalo.
- **interface_id:** identificador da interface a ser acessada. O parâmetro *interface_id* possui diferentes valores para cada tipo de interface:
  - **VLAN:** (1-4094).
  - **GigaEthernet:** 0/(1-10).
  - **Port-areggator:** (1-8).
  - **Null:** 0.
  - **Loopback:** (0-32767).

Modo de comando: Global Configuration.

Exemplo: acesse a configuração da interface VLAN 1.

INTELBRAS_config#interface vlan 1

INTELBRAS_config_v1#

Exemplo: acesse a configuração das interfaces GigaEthernet 1,3 a 10.

INTELBRAS_config#interface range GigaEthernet 0/1,3-10

INTELBRAS_config_if_range#

23.2. Description

Descrição: o comando **description** é usado para configurar uma descrição para uma porta.

Sintaxe: **description** *line*
no description line

Parâmetros:

- **line:** texto com a informação referente a porta.

Modo de comando: interface de configuração Ethernet.

Exemplo: acesse a interface de configuração da porta 8 e configure o nome UPLINK para a porta.

INTELBRAS_config#interface FastEthernet 0/8

INTELBRAS_config_f0/8#description UPLINK

23.3. Bandwidth

Descrição: o comando **bandwidth** é usado para limitar a largura de banda por porta.

Sintaxe: **bandwidth** *kilobps*
no bandwidth

Parâmetros:

» **kilobps:** largura de banda por porta. O valor pode variar de 1 a 10000000 kpbs.

Modo de comando: interface de configuração Ethernet.

Exemplo: acesse a interface de configuração da porta 1 e configure a largura de banda para 100 Mbps.

INTELBRAS_config#interface GigaEthernet 0/1

INTELBRAS_config_g0/1#bandwidth 100000

23.4. Delay

Descrição: o comando **delay** é usado para configurar um delay na interface.

Sintaxe: **delay** *tens_of_microseconds*
no delay

Parâmetros:

» **tens_of_microseconds:** delay em microssegundos inserido na interface. O valor pode variar de 1 a 10000000 microssegundos. Por padrão o valor é *1*.

Modo de comando: interface de configuração Ethernet.

Exemplo: acesse a interface de configuração da porta 5 e configure um delay de 1 segundo.

INTELBRAS_config#interface FastEthernet 0/5

INTELBRAS_config_f0/5#delay 1000000

23.5. Shutdown

Descrição: o comando **shutdown** é usado para habilitar ou desabilitar uma interface.

Sintaxe: **shutdown**
no shutdown

Modo de comando: interface de configuração Ethernet.

Exemplo: acesse a interface de configuração da porta 4 e configure a porta como desabilitada.

INTELBRAS_config#interface FastEthernet 0/4

INTELBRAS_config_f0/4#shutdown

23.6. Show interface

Descrição: o comando **show interface** é usado para mostrar as informações referentes a porta escolhida como estatísticas da porta, estado e protocolos.

Sintaxe: **show interface** *interface_id*

Parâmetros:

» **port:** porta escolhida para mostrar as informações. Se nenhuma porta for informada será retornada as informações de todas as portas.

Modo de comando: modo Privilegiado, Global Configuration e de configuração de interface.

Exemplo: acesse a interface de configuração da porta 1 e mostre as suas informações.

INTELBRAS_config#show interface GigaEthernet 0/1

GigaEthernet0/1 is down, line protocol is down

Ifindex is 1, unique port number is 1

Hardware is Giga-TX, address is 9845.620d.7f5d (bia 9845.620d.7f5d)

MTU 1500 bytes, BW 1000000 kbit, DLY 10 usec

Encapsulation ARPA

Auto-duplex, Auto-speed, Flow-Control Off

5 minutes input rate 0 bits/sec, 0 packets/sec
5 minutes output rate 0 bits/sec, 0 packets/sec
Real time input rate 0 bits/sec, 0 packets/sec
Real time output rate 0 bits/sec, 0 packets/sec
Received 0 packets, 0 bytes
0 broadcasts, 0 multicasts 0 ucasts
0 discard, 0 error, 0 PAUSE
0 align, 0 FCS, 0 symbol
0 jabber, 0 oversize, 0 undersize
0 carriersense, 0 collision, 0 fragment
0 L3 packets, 0 discards, 0 Header errors
Transmitted 0 packets, 0 bytes
0 broadcasts, 0 multicasts 0 ucasts
0 discard, 0 error, 0 PAUSE
0 sqettest, 0 deferred, 0 oversize
0 single, 0 multiple, 0 excessive, 0 late
0 L3 forwards

23.7. Show running-config interface

Descrição: o comando **show running-config** interface é usado para mostrar as configurações da porta selecionada.

Sintaxe: **show running-config interface** *interface_id*

Parâmetros:

» **interface_id:** porta escolhida para mostrar as informações configuradas.

Modo de comando: modo Privilegiado, Global Configuration e de configuração de interface.

Exemplo: acesse a interface de configuração da porta 4 e configure a porta como desabilitada.

INTELBRAS_config#interface FastEthernet 0/4

INTELBRAS_config_f0/4#shutdown

24. Configurações de porta

24.1. Velocidade

Descrição: o comando **speed** é usado para configurar a velocidade de uma porta.

Sintaxe: **speed** 10 | 100 | 1000 | auto
no speed

Parâmetros:

» **10:** velocidade 10 Mbit/s. Padrão *Ethernet*.
» **100:** velocidade 100 Mbit/s. Padrão *Fast Ethernet*.
» **1000:** velocidade 1000 Mbit/s. Padrão *Giga Ethernet*. Esta configuração é válida apenas para as portas uplink G1 e G2.
» **auto:** velocidade configurada automaticamente de acordo com a capacidade do link.
» **no:** mesmo efeito que o parâmetro *auto*.

Modo de comando: interface de configuração Ethernet.

Exemplo: configure a velocidade da interface FastEthernet 1 para o modo *Automático*.

INTELBRAS_config_f0/1#speed auto

24.2. Duplex

Descrição: o comando **duplex** é usado para configurar o modo *Duplex* de uma porta.

Sintaxe: **duplex** half | full | auto
no duplex

Parâmetros:

- **half:** modo *Half-duplex*. Neste modo o tráfego de dados é feito em um único sentido por vez.
- **full:** modo *Full-duplex*. Neste modo o tráfego de dados é feito em ambos sentidos ao mesmo tempo.
- **auto:** modo *Duplex automático*. Nesta configuração o modo *Duplex* da interface é definido automaticamente de acordo com a capacidade do link.
- **no:** mesmo efeito que o parâmetro "auto".

Modo de comando: interface de configuração Ethernet.

Exemplo: configure o modo *Duplex* da interface GigaEthernet 1 para automático.

INTELBRAS_config_f0/1#duplex auto

24.3. Controle de fluxo

Descrição: o comando **flow-control** é usado para configurar o controle de fluxo de uma porta.

Sintaxe: **flow-control** on | off | auto
no flow-control

Parâmetros:

- **on:** habilita o controle de fluxo.
- **off:** desabilita o controle de fluxo.
- **auto:** configura o controle de fluxo no modo *Automático*. Com esta configuração o switch apenas irá enviar pacotes de controle de fluxo se o dispositivo conectado ao mesmo tiver habilitado seu próprio controle de fluxo.

Modo de comando: interface de configuração Ethernet.

Exemplo: configure o controle de fluxo na interface GigaEthernet 1 para o modo *Automático*.

INTELBRAS_config_f0/1#flow-control auto

25. Espelhamento de porta

Quando configurado no equipamento uma porta como destino de uma sessão de espelhamento de portas, a porta espelho (porta destino) perde acesso a gerência do switch, ou seja, caso a porta espelho esteja sendo usada para acessar o switch o acesso será perdido.

25.1. Sessão de espelhamento

Descrição: o comando **mirror session** é utilizado para configurar uma sessão de espelhamento de portas. Em uma sessão de espelhamento de portas define-se porta(s) de origem que terão seu tráfego espelhado para a porta de destino.

Obs.: *ao configurar uma porta como destino de uma sessão de espelhamento perde-se o acesso ao gerenciamento do switch por esta porta.*

Sintaxe: **mirror session** (1-1) destination interface *interface_id*
mirror session (1-1) source interface *interface_range* both | tx | rx
no mirror session (1-1) source interface *interface_range* both | tx | rx
no mirror session (1-1)

Parâmetros:

- **(1-1):** número que identifica a sessão de espelhamento. Apenas uma sessão pode ser configurada.
- **destination:** especifica a porta de destino.
  Obs.: *a porta destino perderá acesso ao gerenciamento do switch.*
- **source:** especifica a porta de origem.
- **interface_id:** especifica qual interface GigaEthernet está sendo configurada.

» **interface_range:** especifica quais interfaces GigaEthernet estão sendo configuradas. Este parâmetro deve ser definido com a especificação de uma interface por vez, estas devem ser separadas por "," para adicionar uma única interface ou "-" para adicionar um intervalo de interfaces.
» **both:** especifica que o tráfego espelhado será de ambos TX e RX.
» **rx:** especifica que o tráfego espelhado será de apenas o tráfego recebido pela porta.
» **tx:** especifica que o tráfego espelhado será de apenas o tráfego transmitido pela porta.

Modo de comando: Global Configuration.

Exemplo: configure uma sessão de espelhamento para que o tráfego de TX e RX das portas FastEthernet 1 a FastEthernet 4 seja espelhado na porta uplink GigaEthernet 1.

INTELBRAS_config#mirror session 1 source interface fastEthernet 0/1 - 4 both

INTELBRAS_config#mirror session 1 destination interface gigaEthernet 0/1

25.2. Informações

Descrição: o comando **show mirror** é utilizado para exibir as configurações de isolamento de porta do sistema.

Sintaxe: **show mirror**
show mirror session (1-1)

Parâmetros:

» **session (1-1):** especifica a sessão de espelhamento.

Modo de comando: Privileged EXEC.

Exemplo: exiba as informações de espelhamento da sessão 1.

INTELBRAS_config#show mirror session 1

Session 1

Destination Ports: g0/2

Source Ports:

RX Only: None

TX Only: None

Both: f0/1 f0/2 f0/3 f0/4

26. Link Agreggation (LAG)

Descrição: o comando **aggregator-group** permite a utilização de múltiplas portas para 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.

Sintaxe: **aggregator-group** *id* mode static
aggregator-group *id* mode lacp active | passive static
no aggregator-group

Parâmetros:

» **id (1-8):** identificação do grupo de portas.
» **lacp active:** modo *LACP ativo.*
» **lacp passive:** modo *LACP passivo.*
» **static:** modo *Estático.*

Modo de comando: interface de configuração Ethernet.

Exemplo: configure as interfaces GigaEthernet 1 e GigaEthernet 2 no LAG 1 no modo Estático.

INTELBRAS_config_f0/1#aggregator-group 1 mode static

INTELBRAS_config_f0/1#interface g0/2

INTELBRAS_config_f0/2#aggregator-group 1 mode static

26.1. Informações

Descrição: o comando **show aggregator-group** é usado para visualizar as configurações correntes do grupo de portas agregadas.

Sintaxe: show aggregator-group *id* detail | brief | summary

Parâmetros:

- **id:** identificação do grupo de portas agregadas.
- **brief:** exibe informações resumidas.
- **detail:** exibe informações detail.
- **summary:** exibe informações de sumário.

Modo de comando: Global Configuration.

Exemplo: exibir os detalhes de agregação.

INTELBRAS_config#show aggregator-group 1 detail

26.2. Informações da interface

Descrição: o comando **show interface port-aggregator** é usado para visualizar as configurações correntes da interface do grupo de portas agregadas.

Sintaxe: show interface aggregator-group *id*

Parâmetros:

- **id:** identificação do grupo de portas agregadas.

Modo de comando: Privileged EXEC.

Exemplo: exibir os detalhes da interface das portas agregadas.

INTELBRAS#show interface port-aggregator 1

26.3. Depuração

Descrição: o comando **debug lacp** é usado para habilitar a depuração lacp.

Sintaxe: **debug lacp** errors|state|packet
no debug lacp errors|state|packet

Parâmetros:

- **errors:** depuração de erros.
- **state:** depuração do status.
- **packet:** depuração dos pacotes.

Modo de comando: Privileged EXEC.

Exemplo: iniciar o debug de erros da função *LACP.*

Switch# debug lacp errors

27. Isolamento de portas

Descrição: o comando **switchport protected** é utilizado para habilitar o isolamento de portas na interface. As interfaces configuradas com isolamento de portas não poderão trocar pacotes entre si.

Sintaxe: **switchport protected**
no switchport protected

Exemplo: adicione a porta FastEthernet 1 e 5 com isolamento entre si.

INTELBRAS_config#interface fastEthernet 0/1

INTELBRAS_config_f0/1#switchport protected

INTELBRAS_config_f0/1#interface fastEthernet 0/5

INTELBRAS_config_f0/5#switchport protected

28. Storm control

Descrição: o comando **storm-control** é utilizado para configurar um controle banda para tráfegos broadcast, multicast e unknow unicast.

Sintaxe: **storm-control** broadcast | multicast | unicast threshold (1-65535)
no storm-control broadcast | multicast | unicast threshold

Parâmetros:

- **broadcast:** especifica o tipo de tráfego como broadcast.
- **unicast:** especifica o tipo de tráfego como unicast desconhecido.
- **multicast:** especifica o tipo de tráfego como multicast.
- **threshold (1-65535):** define o limite de banda em unidades de 64 Kbps.

Modo de comando: interface de configuração Ethernet.

Exemplo: configure um controle de banda de 128 Kbps para tráfegos unicast desconhecido.

INTELBRAS_config_f0/1#storm-control unicast threshold 2

29. Controle de banda

Descrição: o comando **switchport rate-limit** é utilizado para configurar o controle de banda de uma porta.

Sintaxe: **switchport rate-limit** bandwidth (1-100) ingress|egress
switchport rate-limit (1-16383) ingress | egress
no switchport rate-limit ingress | egress

Parâmetros:

- **bandwidth (1-100):** especifica a porcentagem de tráfego a ser permitida em relação a capacidade total da porta.
- **(1-16383):** especifica a quantidade de tráfego a ser permitida em unidades de 64 Kbps.
- **ingress:** especifica o sentido do tráfego que esta a ser limitado como de ingresso.
- **egress:** especifica o sentido do tráfego que esta a ser limitado como de egresso.
- **Modo de comando:** interface de configuração Ethernet.

Exemplo: configure um controle de banda de 1024 Kbps para o tráfego de ingresso da interface GigaEthernet 1.

INTELBRAS_config_f0/1#switchport rate-limit 16 ingress

Exemplo: configure um controle de banda de 10% da capacidade total da porta para o tráfego de egresso da mesma.

INTELBRAS_config_f0/1#switchport rate-limit bandwidth 10 egress

30. Keepalive

Descrição: o comando **keepalive** é utilizado para habilitar e configurar a verificação do estado operacional do link entre os dispositivos conectados na porta através do envio de pacotes de verificação keepalive.

Sintaxe: **keepalive** (0-32767)
no keepalive

Parâmetros:

- **(0-32767):** especifica o intervalo de transmissão em segundos de pacotes keepalive. Se não for especificado o intervalo de transmissão será de 12 segundos.

Modo de comando: interface de configuração Ethernet.

Exemplo: habilite e configure a transmissão de pacotes keepalive em intervalos de 30 segundos na interface GigaEthernet 1.

INTELBRAS_config_f0/1#keepalive 30

31. Aprendizado de MAC

Descrição: o comando **switchport disable-learning** é utilizado para desabilitar o aprendizado de endereços MAC de uma interface GigaEthernet.

Sintaxe: **switchport disable-learning**
no switchport disable-learning

Modo de comando: interface de configuração Ethernet.

Exemplo: desabilite o aprendizado de endereços MAC na interface GigaEthernet 1.

INTELBRAS_config_f0/1#switchport disable-learning

32. Segurança de porta

32.1. Modo de segurança

Descrição: o comando **switchport port-security mode** é utilizado para definir o modo de segurança de porta numa interface GigaEthernet.

Sintaxe: **switchport port-security mode** dynamic | sticky
switchport port-security mode static accept | reject
no switchport port-security mode

Parâmetros:

- **dynamic:** especifica o modo de segurança de porta da interface para *Dinâmico*.
- **sticky:** especifica o modo de segurança de porta da interface para *Sticky*.
- **accept:** especifica o modo de segurança de porta da interface para *Permitir estático*.
- **reject:** especifica o modo de segurança de porta da interface para *Rejeitar estático*.

Modo de comando: interface de configuração Ethernet.

Exemplo: configure o modo de segurança da porta GigaEthernet 1 para Permitir Estático.

INTELBRAS_config_f0/1#switchport port-security mode static accept

32.2. Modo *Dinâmico*

Descrição: o comando **switchport port-security dynamic** é utilizado para configurar o modo de segurança *Dinâmico* numa interface GigaEthernet.

Sintaxe: **switchport port-security dynamic** maximum (1-2048)

Parâmetros:

- **maximum (1-2048):** especifica a quantidade máxima de endereços que serão aprendidos pela porta.

Modo de comando: interface de configuração Ethernet.

Exemplo: configure a porta GigaEthernet 1 no modo de segurança *Dinâmico* para que aprenda no máximo 1000 endereços MAC.

INTELBRAS_config_f0/1#switchport port-security mode dynamic

INTELBRAS_config_f0/1#switchport port-security dynamic maximum 1000

32.3. Modo *Estático*

Descrição: o comando **switchport port-security static** é utilizado para configurar o modo de segurança *Estático* numa interface GigaEthernet.

Sintaxe: **switchport port-security stati**c mac-adress *endereço_mac*

Parâmetros:

- **endereço_mac:** especifica o endereço MAC de 48 bits que será filtrado ou permitido pela porta dependendo do modo de segurança estático configurado.

Modo de comando: interface de configuração Ethernet.

Exemplo: configure a porta GigaEthernet 1 no modo de segurança *Rejeitar estático* para que permita o tráfego de pacotes com todos os endereços MAC exceto o 1234.1234.1234.

INTELBRAS_config_f0/1#switchport port-security mode static reject

INTELBRAS_config_f0/1#switchport port-security static mac-adress 1234.1234.1234

32.4. Modo *Sticky*

Descrição: o comando **switchport port-security sticky** é utilizado para configurar o modo de segurança *Sticky* numa interface GigaEthernet.

Sintaxe: **switchport port-security sticky** aging-time (0-100)
switchport port-security sticky maximum (1-2048)
switchport port-security sticky mac-adress *endereço_mac*

Parâmetros:

- **maximum (1-2048):** especifica a quantidade máxima de endereços MAC Sticky que serão aprendidos pela porta.
- **aging-time (1-100):** especifica o tempo de envelhecimento dos endereços MAC Sticky.
- **mac-adress endereço_mac:** adiciona um endereço MAC Sticky manualmente.

Modo de comando: interface de configuração Ethernet.

Exemplo: configure a porta GigaEthernet 1 no modo de segurança *Sticky* para que aprenda no máximo 100 endereços MAC Sticky.

INTELBRAS_config_f0/1#switchport port-security mode sticky

INTELBRAS_config_f0/1#switchport port-security sticky maximum 100

32.5. Vínculos IMPB

Descrição: o comando **switchport port-security bind|block** é utilizado para definir um vínculo entre a interface GigaEthernet e um IP ou MAC em específico para que pacotes IP ou ARP sejam filtrados de acordo com os dados de vínculo da porta.

Sintaxe: **switchport port-security bind|block** ip | arp | both-arp-ip *endereço_ip*
switchport port-security bind|block ip | arp | both-arp-ip *endereço_ip* mac *endereço_mac*
switchport port-security bind|block mac *endereço_mac*

Obs.: *o parâmetro* no *pode ser utilizado antes dos comandos acima para excluir um vínculo ao invés de criá-lo.*

Parâmetros:

- **bind:** especifica que a porta deverá permitir o tráfego de pacotes que combinem com o vínculo que esta sendo criado.
- **block:** especifica que a porta deverá bloquear o tráfego de pacotes que combinem com o vínculo que esta sendo criado.
- **ip endereço_ip:** especifica que a ação relativa ao vínculo que está configurado terá efeito para pacotes IP com o endereço IP *endereço_ip*.
- **arp endereço_ip:** especifica que a ação relativa ao vínculo que está configurado terá efeito para pacotes ARP com o endereço IP *endereço_ip*.
- **both-arp-ip endereço_ip:** especifica que a ação relativa ao vínculo que está configurado terá efeito para pacotes ARP e IP com o endereço IP *endereço_ip*.
- **mac endereço_mac:** especifica que a ação relativa ao vínculo que está configurado terá efeito para pacotes com o endereço MAC *endereço_ip*.

Modo de comando: interface de configuração Ethernet.

Exemplo: configure um vínculo para que a porta GigaEthernet 1 permita o tráfego de todos os pacotes IP ou ARP que possuam o endereço IP 192.168.0.1 e o endereço MAC 1234.1234.1234

INTELBRAS_config_f0/1#switchport block both-arp-ip 192.168.0.1 mac 1234.1234.1234

33. SLV e IVL

Descrição: o comando **vlan shared-learning** é utilizado para definir o modo de aprendizado VLAN das portas como compartilhado ou independente.

Sintaxe: **vlan shared-learning**
no vlan shared-learning

Modo de comando: Global Configuration.

Exemplo: configura o modo de aprendizado VLAN das portas como independente.

INTELBRAS_config#no vlan shared-learning

34. Link scan

Descrição: o comando **link-scan** é utilizado para definir o modo e período de verificação de estado operacional das interfaces.

Sintaxe: **link scan** normal | fast (10-100)
no link scan normal | fast

Parâmetros:

» **normal (10-100):** configura a verificação de estado das interfaces para o modo *Normal* com período (10-100).
» **fast (10-100):** configura a verificação de estado das interfaces para o modo *Rápido* com período (10-100).

Modo de comando: Global Configuration.

Exemplo: configure o a verificação do estado operacional das interfaces para o modo *Normal* com um período de 20 segundos.

INTELBRAS_config#link scan 20

35. Enhanced-link

Descrição: o comando **switchport enhanced-link** é utilizado para habilitar o modo de verificação de estado da interface para enhanced-link fazendo com que a verificação seja mais rápida.

Sintaxe: **switchport enhanced-link**
no switchport enhanced-link

Modo de comando: interface de configuração Ethernet.

Exemplo: configure o modo de verificação de estado da interface GigaEthernet 1 para enhanced-link.

INTELBRAS_config_f0/1#switchpor enhanced-link

36. MTU

Descrição: o comando **system mtu** é utilizado para definir o MTU do sistema.

Sintaxe: **system mtu** (1500-9216)
no system mtu

Parâmetros:

» **(1500-9216):** especifica em bytes o tamanho MTU do sistema.

Modo de comando: Global Configuration.

Exemplo: configure o MTU do sistema para 9216 bytes.

INTELBRAS_config#system mtu 9216

37. Spanning Tree Protocol (STP)

Descrição: o comando **spanning-tree** é utilizado para habilitar/desabilitar a função de *STP* que desativa a porta do switch que apresente loop. Por padrão o RSTP é habilitado no equipamento.

Sintaxe: **spanning-tree**
no spanning-tree

Modo de comando: Global Configuration.

Exemplo: desabilite o Spanning Tree.

INTELBRAS_config#no spanning-tree

37.1. Modo *STP*

Descrição: o comando **spanning-tree mode** é utilizado para definir o modo do Spanning Tree.

Sintaxe: **spanning-tree mode** mstp | pvst | rstp | sstp
no spanning-tree

Parâmetros:

- **mstp:** Multiple Spanning Tree Protocol.
- **pvst:** Per VLAN Spanning-Tree.
- **rstp:** Rapid Spanning Tree Protocol.
- **sstp:** Spanning Tree Protocol.

Modo de comando: Global Configuration.

Exemplo: desabilite o Spanning Tree.

INTELBRAS_config#no spanning-tree

37.2. VLAN para PVST

Descrição: o comando **spanning-tree vlan** é utilizado para configurar o envio de dados STP por determinadas VLANs.

Sintaxe: **spanning-tree vlan** *vlan-list*
no spanning-tree *vlan-list*

Parâmetros:

- **vlan-list:** informa a VLAN para o protocolo PVST (Per VLAN Spanning-Tree).

Modo de comando: Global Configuration.

Exemplo: habilite o switch a trafegar dados STP pela VLAN 100.

INTELBRAS_config#spanning-tree vlan 100

37.3. Nome para MSTP

Descrição: o comando **spanning-tree mstp name** é utilizado para configurar o nome para mstp.

Sintaxe: **spanning-tree mstp name** *text*
no spanning-tree mstp name

Parâmetros:

- **name:** configure o nome para o mstp. Por padrão se nenhum nome for informado o endereço MAC do switch será utilizado. Tamanho máximo de 32 caracteres.
- **no:** configura o endereço MAC do switch como o nome do MSTP.

Modo de comando: Global Configuration.

Exemplo: configure o nome do mstp para teste_1

INTELBRAS_config#spanning-tree mstp name teste_1

37.4. Revisão MSTP

Descrição: o comando **spanning-tree mstp revision** é utilizado para configurar o nível de revisão para MSTP.

Sintaxe: **spanning-tree mstp name** *(0-65535)*
no spanning-tree mstp name

Parâmetros:

» **(0-65535):** valor do nível de revisão MSTP. Por padrão o valor da revisão é *0*.
» **no:** retorna a revisão para o valor padrão.

Modo de comando: Global Configuration.

Exemplo: configure o nível da revisão MSTP para 10.

INTELBRAS_config#spanning-tree mstp revision 10

37.5. Instância MSTP

Descrição: o comando **spanning-tree mstp instance** é utilizado para configurar a instância MSTP e atribuir uma VLAN para esta instância.

Sintaxe: **spanning-tree mstp instance** *(1-15)* vlan *(1-4094)*
no spanning-tree mstp instance *(1-15)*

Parâmetros:

» **(1-15):** identificador da instância MSTP.
» **(1-4094):** identificador da VLAN.
» **no:** apaga a instância criada.

Modo de comando: Global Configuration.

Exemplo: configure a instância 2 para a VLAN 50.

INTELBRAS_config#spanning-tree mstp instance 2 vlan 50

37.6. MSTP Root

Descrição: o comando **spanning-tree mstp root** é utilizado para configurar a prioridade MSTP para as instâncias configuradas como primária ou secundária.

Sintaxe: **spanning-tree mstp** *(1-15)* root *primary* | *secondary* diameter (2-7) hello-time *(0-10)*
no spanning-tree mstp *instance-id* root

Parâmetros:

» **(1-15):** identificador da instância MSTP.
» **primary:** configura a instância como principal, o valor da prioridade é *24576*.
» **secondary:** configura a instância como secundária, o valor da prioridade é *28672*.
» **(2-7):** número de Bridges entre dois nós finais.
» **(0-10):** define o valor intervalo de tempo em segundos para o envio da mensagem BPDU. Por padrão o tempo de envio é de *2 segundos*.
» **no:** apaga a configuração da instância principal/secundária. Prioridade igual a *32768*.

Modo de comando: Global Configuration.

Exemplo: configure a instância 2 para primário com saltos de bridge 5 e hello time para 5.

INTELBRAS_config#panning-tree mstp 2 root primary diameter 5 hello-time 5

37.7. Prioridade STP

Descrição: o comando **spanning-tree priority** é o comando que define a prioridade para o protocolo Spanning Tree.

Sintaxe: **spanning-tree sstp priority** *(0-61440)*
spanning-tree vlan *vlan-list* **priority** *(0-61440)*
spanning-tree rstp priority *(0-61440)*
spanning-tree mstp *(0-15)* **priority** *(0-61440)*

no spanning-tree sstp priority
no spanning-tree vlan *vlan-list* **priority**
no spanning-tree rstp priority
no spanning-tree mstp *(0-15)* **priority**

Parâmetros:

- **(0-61440):** define o valor da variável *Prioridade Bridge*. O switch com o menor valor será o root bridge. Valor padrão é *32768*.
- **vlan-list:** informa a VLAN para o protocolo PVST (*Per VLAN Spanning-Tree*).
- **(0-15):** número da instância MSTP.
- **no:** define o valor da prioridade para *32768*, que é o valor padrão.

Modo de comando: Global Configuration.

Exemplo: configure a prioridade RSTP para 4096.

INTELBRAS_config#spanning-tree sstp priority 4096

Exemplo: retorne a configuração do STP para RSTP com prioridade 32768.

INTELBRAS_config#no spanning-tree rstp priority

37.8. Hello time

Descrição: o comando **spanning-tree hello-time** é o comando utilizado para definir o intervalo de envio de quadros BPDU para os dispositivos vizinhos.

Sintaxe: **spanning-tree sstp hello-time** *(0-10)*
spanning-tree vlan *vlan-list* **hello-time** *(0-10)*
spanning-tree rstp hello-time *(0-10)*
spanning-tree mstp hello-time *(0-10)*
no spanning-tree sstp hello-time
no spanning-tree vlan *vlan-list* **hello-time**
no spanning-tree rstp hello-time
no spanning-tree mstp hello-time

Parâmetros:

- **(0-10):** define o valor intervalo de tempo em segundos para o envio da mensagem BPDU. Por padrão o tempo de envio é de *2 segundos*.
- **vlan-list:** informa a VLAN para o protocolo PVST (*Per VLAN Spanning-Tree*).
- **no:** define o valor do tempo para *2 segundos*, que é o valor padrão.

Modo de comando: Global Configuration.

Exemplo: configure o tempo de envio do BPDU para 5 segundos.

INTELBRAS_config#spanning-tree rstp hello-time 5

Exemplo: retorne o tempo ao valor inicial, 2 segundos.

INTELBRAS_config#no spanning-tree rstp hello-time

37.9. Max age

Descrição: o comando **spanning-tree hello-time** é o comando utilizado para definir o tempo de envelhecimento caso o quadro BPDU não retorne. O tempo padrão é *20 segundos*.

Sintaxe: **spanning-tree sstp max-age** *(6-40)*
spanning-tree vlan *vlan-list* **max-age** *(6-40)*
spanning-tree rstp max-age *(6-40)*
spanning-tree mstp max-age *(6-40)*
no spanning-tree sstp max-age

no spanning-tree vlan *vlan-list* **max-age**
no spanning-tree rstp max-age
no spanning-tree mstp max-age

Parâmetros:

» **(6-40):** define o valor intervalo de tempo em segundos para a validade da mensagem BPDU enviada. Por padrão o tempo de envio é de *20 segundos*.
» **vlan-list:** informa a VLAN para o protocolo PVST (*Per VLAN Spanning-Tree*).
» **no:** define o valor do tempo para *20 segundos*, que é o valor padrão.

Modo de comando: Global Configuration.

Exemplo: configure o tempo de vida hello-time para 10 segundos.

INTELBRAS_config#spanning-tree mstp hello-time 10

Exemplo: retorne o tempo ao valor inicial, 20 segundos.

INTELBRAS_config#no spanning-tree mstp hello-time

37.10. Forward time

Descrição: o comando **spanning-tree forward-time** é o comando utilizado para configurar o intervalo que a porta muda de estado. Depois de encerrado o loop a porta voltará a operação no intervalo de tempo configurado neste comando, por padrão o intervalo é de *15 segundos***.**

Sintaxe: **spanning-tree sstp forward-time** *(4-30)*
spanning-tree vlan *vlan-list* **forward-time** *(4-30)*
spanning-tree rstp forward-time *(4-30)*
spanning-tree mstp forward-time *(4-30)*
no spanning-tree sstp forward-time
no spanning-tree vlan *vlan-list* **forward-time**
no spanning-tree rstp forward-time
no spanning-tree mstp forward-time

Parâmetros:

» **(4-30):** define o intervalo de tempo para a porta mudar de estado.
» **vlan-list:** informa a VLAN para o protocolo PVST (*Per VLAN Spanning-Tree*).
» **no:** define o valor do tempo para *15 segundos*, que é o valor padrão.

Modo de comando: Global Configuration.

Exemplo: configure o intervalo de tempo de 17 segundos para porta voltar a operação normal.

INTELBRAS_config#spanning-tree rstp forward-time 17

Exemplo: retorne o tempo ao valor inicial, 15 segundos.

INTELBRAS_config#no spanning-tree rstp forward-time

37.11. Custo SSTP/RSTP/MSTP

Descrição: o comando **spanning-tree xxx cost** é o comando utilizado para definir o custo do caminho a ser computado pelo switch para SSTP/RSTP/MSTP.

Sintaxe: **spanning-tree sstp cost** *(1-200000000)*
spanning-tree vlan vlan-list cost *(1-200000000)*
spanning-tree rstp cost *(1-200000000)*
spanning-tree mstp *(0-15)* **cost** *(1-200000000)*
no spanning-tree sstp cost
no spanning-tree vlan *vlan-list* **cost**
no spanning-tree rstp cost
no spanning-tree mstp *(0-15)* **cost**

Parâmetros:

- **(1-200000000):** custo do caminho da porta na instância STP.
- **vlan-list:** informa a VLAN para o protocolo PVST (*Per VLAN Spanning-Tree*).
- **(0-15):** número da instância STP, pode variar de 0 a 15.
- **no:** deleta o custo da configuração STP.

Modo de comando: interface de configuração Ethernet.

Exemplo: configure o Path Cost da instância 1 para 100 na porta GigaEthernet 1.

INTELBRAS_config_f0/1#spanning-tree mstp 1 cost 100

37.12. Custo do caminho

Descrição: o comando **spanning-tree cost** é o comando utilizado para definir o custo do caminho a ser computado pelo switch.

Sintaxe: **spanning-tree cost** *(1-200000000)*
no spanning-tree cost

Parâmetros:

- **(1-200000000):** custo do caminho da porta no protocolo STP.
- **no:** deleta o custo da configuração STP.

Modo de comando: interface de configuração Ethernet.

Exemplo: configure o custo do caminho para 500 na porta GigaEthernet 1.

INTELBRAS_config#interface GigaEthernet 0/1

INTELBRAS_config_g0/1#spanning-tree cost 500

37.13. Prioridade SSTP/RSTP/MSTP

Descrição: o comando **spanning-tree xxx port-priority** é o comando utilizado para configurar a prioridade da porta STP para SSTP/RSTP/MSTP.

Sintaxe: **spanning-tree sstp port-priority** *(0-240)*
spanning-tree vlan *vlan-list* **port-priority** *(0-240)*
spanning-tree rstp port-priority *(0-240)*
spanning-tree mstp *(0-15)* **port-priority** *(0-240)*
no spanning-tree sstp port-priority
no spanning-tree vlan *vlan-list* **port-priority**
no spanning-tree rstp port-priority
no spanning-tree mstp *(0-15)* **port-priority**

Parâmetros:

- **(0-240):** valor da prioridade da porta.
- **vlan-list:** informa a VLAN para o protocolo PVST (*Per VLAN Spanning-Tree*).
- **(0-15):** número da instância STP, pode variar de 0 a 15.
- **no:** deleta o custo da configuração STP.

Modo de comando: interface de configuração Ethernet.

Exemplo: configure a prioridade da instância 1 para 96 na porta GigaEthernet 1.

INTELBRAS_config#interface GigaEthernet 0/1

INTELBRAS_config_g0/1#spanning-tree mstp 1 port-priority 96

37.14. Prioridade da porta

Descrição: o comando **spanning-tree port-priority** é o comando utilizado para definir a prioridade do caminho a ser configurado no switch.

Sintaxe: **spanning-tree port-priority** *(0-240)*
no spanning-tree port-priority

Parâmetros:

» **(0-240):** prioridade da porta para o protocolo STP.

» **no:** deleta a prioridade da porta STP.

Modo de comando: interface de configuração Ethernet.

Exemplo: configure o custo da porta GigaEthernet 1 para 96.

INTELBRAS_config#interface GigaEthernet 0/1

INTELBRAS_config_g0/1#spanning-tree cost 96

37.15. Porta edge

Descrição: o comando **spanning-tree xxx edge** é o comando utilizado para configurar uma porta como EDGE PORT.

Sintaxe: **spanning-tree** rstp | mstp edge
no spanning-tree rstp | mstp edge

Modo de comando: interface de configuração Ethernet.

Exemplo: configure a interface GigaEthernet 1 como uma porta Edge com protocolo RSTP.

INTELBRAS_config#interface GigaEthernet 0/1

INTELBRAS_config_g0/1#spanning-tree rstp edge

37.16. Porta auto

Descrição: o comando **spanning-tree xxx auto** é o comando utilizado para definir o status de uma conexão ponto a ponto em uma interface do switch.

Sintaxe: **spanning-tree** rstp | mstp point-to-point force-true | force-false | auto
no spanning-tree rstp | mstp point-to-point

Modo de comando: interface de configuração Ethernet.

Exemplo: configure a interface GigaEthernet 1 com status auto de uma conexão ponto a ponto.

INTELBRAS_config#interface GigaEthernet 0/1

INTELBRAS_config_g0/1#spanning-tree rstp point-to-point auto

37.17. Migration-check

Descrição: o comando **spanning-tree xxx migration-check** é o comando utilizado para reiniciar a verificação de transferência de protocolo em uma porta.

Sintaxe: **spanning-tree** rstp | mstp migration-check

Modo de comando: interface de configuração Ethernet.

Exemplo:

INTELBRAS_config#spanning-tree rstp migration-check

INTELBRAS_config_f0/1#spanning-tree mstp migration-check

37.18. Distância administrativa

Descrição: o comando **spanning-tree mstp diameter** é o comando utilizado para configurar o número máximo de bridges entre os hosts.

Sintaxe: **spanning-tree** mstp diameter (2-7)
no spanning-tree mstp diameter

Modo de comando: Global Configuration.

» **Parâmetros:**

» **(2-7):** número de Bridges entre dois nós finais.

Exemplo: configure o número máximo de bridges entre dois hosts como 4.

INTELBRAS_config#spanning-tree mstp diameter 4

37.19. Saltos MSTP

Descrição: o comando **spanning-tree mstp max-hops** é o comando utilizado para configurar o número máximo de saltos no protocolo MSTP.

Sintaxe: **spanning-tree mstp max-hops** *(6-40)*
no spanning-tree mstp max-hops

Modo de comando: Global Configuration.

Parâmetros:

» **(6-40):** número máximo de saltos que um BPDU é válido.
» **no:** retorna o valor a configuração padrão (*20*).

Exemplo: configure o número máximo de bridges entre dois hosts como 4.

INTELBRAS_config#spanning-tree mstp diameter 4

37.20. MST-compatível

Descrição: o comando **spanning-tree mstp mst-compatible** é o comando utilizado para habilitar ou desabilitar o MST-compatível.

Sintaxe: **spanning-tree mstp mst-compatible**
no spanning-tree mstp mst-compatible

Modo de comando: Global Configuration.

Exemplo: habilite o comando MST-compatível no switch.

INTELBRAS_config#spanning-tree mstp mst-compatible

37.21. Restrição de porta

Descrição: o comando **spanning-tree mstp restricted-role** é o comando utilizado para restringir uma porta de ser uma porta root.

Sintaxe: **spanning-tree mstp restricted-role**
no spanning-tree mstp restricted-role

Modo de comando: interface de configuração Ethernet.

Exemplo: configure a interface FastEthernet 10 como uma porta não root.

INTELBRAS_config#interface FastEthernet 0/10

INTELBRAS_config_f0/10#spanning-tree mstp restricted-role

37.22. Mudança de topologia de porta

Descrição: o comando **spanning-tree mstp restricted-tcn** é o comando utilizado para restringir a divulgação da mudança de topologia em uma porta.

Sintaxe: **spanning-tree mstp restricted-tcn**
no spanning-tree mstp restricted-tcn

Modo de comando: interface de configuração Ethernet.

Exemplo: configure a interface FastEthernet 2 como uma porta que não divulga a alteração de topologia para outras portas.

INTELBRAS_config#interface FastEthernet 0/2

INTELBRAS_config_f0/2#spanning-tree mstp restricted-rtcn

37.23. Informações STP

Descrição: o comando **show spanning-tree** é o comando utilizado para informar o estado das configurações de STP.

Sintaxe: **show spanning-tree** detail | interface *interface_id*

Parâmetros:

» **interface_id:** identificador da interface.

Modo de comando: Global Configuration.

Exemplo: mostre os detalhes das informações de STP da porta GigaEthernet 1.

INTELBRAS_config#show spanning-tree interface gigaEthernet 0/1

37.24. Informações STP VLAN

Descrição: o comando **show spanning-tree vlan** é o comando utilizado para informar o estado das configurações de STP de uma VLAN específica.

Sintaxe: **show spanning-tree vlan** *vlan-list* detail

Parâmetros:

- **interface_id:** identificador da interface.
- **vlan-list:** informa a VLAN para o protocolo PVST (*Per VLAN Spanning-Tree*).

Modo de comando: Global Configuration.

Exemplo: mostre os detalhes das informações das VLANs 1 e 2.

INTELBRAS_config#show spanning-tree vlan 1-2

37.25. Informações MSTP

Descrição: o comando **show spanning-tree mstp** é o comando utilizado para informar o estado das configurações MSTP do switch.

Sintaxe: **show spanning-tree mstp** region | instance *(0-15)* | detail | interface *interface_id* | protocol-migration

Parâmetros:

- **region:** exibe as configurações e o status da região MSTP.
- **(0-15):** número da instância MSTP.
- **detail:** exibe as configurações detalhadas do protocolo MSTP.
- **interface_id:** identificador da interface.
- **protocol-migration:** exibir as informações de migração do protocolo de porta MSTP.

Modo de comando: Global Configuration.

Exemplo: mostre os detalhes das informações da configuração MSTP.

INTELBRAS_config#show spanning-tree mstp

37.26. Gerenciamento SNMP para STP

Descrição: o comando **spanning-tree management trap** é o comando utilizado para configurar o gerenciamento SNMP para STP.

Sintaxe: **spanning-tree management trap** newroot | topologychange
no spanning-tree management trap newroot | topologychange

Parâmetros:

- **newroot:** habilita o envio de trap newroot.
- **topologychange:** habilita o envio de trap topologychange.

Modo de comando: Global Configuration.

Exemplo:

INTELBRAS_config#spanning-tree management trap topologychange

37.27. Portfast

Descrição: o comando **spanning-tree portfast** permite a configuração das portas do switch como interface para conexão de hosts (edge) para os protocolos SSTP e PVST. Esta opção faz com que a interface configurada como portfast não passe pelas fazes de configurações anteriores para a porta.

Sintaxe: **spanning-tree portfast** bpdufilter | bpduguard | default
no spanning-tree portfast bpdufilter | bpduguard | default

Parâmetros:

» **bpdufilter:** inicia o filtro BPDU.
» **bpduguard:** inicia a proteção BPDU.
» **default:** habilita o portfast globalmente.

Modo de comando: Global Configuration.

Exemplo: habilite o portfast globalmente no switch.

INTELBRAS_config#spanning-tree portfast default

37.28. Portfast na interface

Descrição: o comando **spanning-tree portfast** quando executado no modo de configuração de interface, configura a interface como uma porta para conexão de host (edge). Não passando pelas fazes de configurações anteriores para a porta.

Sintaxe: **spanning-tree portfast** disable
no spanning-tree portfast

Parâmetros:

» **disable:** desabilita a função *Portfast.*

Modo de comando: interface de configuração Ethernet.

Exemplo: habilite o portfast na interface FastEthernet 1.

INTELBRAS_config#interface FastEthernet 0/1

INTELBRAS_config _f0/1#spanning-tree portfast

37.29. BPDU Guard

Descrição: se uma porta configurada como porta edge, com a função **Spanning-tree bpduguard** habilitada, receber um pacote BPDU a porta será desativada e precisará ser ativada novamente para configuração no protocolo SSTP e PVST.

Para o protocolo RSTP e MSTP a porta será bloqueada por um período de tempo.

Sintaxe: **spanning-tree bpduguard** disable | enable
no spanning-tree bpduguard

Parâmetros:

» **disable:** desabilita a função *Bpduguard.*
» **enable:** habilita a função *Bpduguard.*

Modo de comando: interface de configuração Ethernet.

Exemplo: habilite a interface FastEthernet 1 a receber pacotes de proteção BPDU.

INTELBRAS_config#interface FastEthernet 0/1

INTELBRAS_config_f0/1#spanning-tree bpduguard enable

37.30. Uplinkfast

Descrição: o comando **spanning-tree uplinkfast** é utilizado para configurar uma rota alternativa mais rápida quando há a necessidade de uso, quando o link principal cai por exemplo. Possível configurar este comendo apenas em SSTP e PVST.

Sintaxe: **spanning-tree uplinkfast**
no spanning-tree uplinkfast

Modo de comando: Global Configuration.

Exemplo: habilite a configuração uplinkfast no switch.

INTELBRAS_config_f0/1#spanning-tree uplinkfast

37.31. Backbonefast

» **Descrição:** o comando **spanning-tree backbonefast** é utilizado para habilitar a mudança de rotas na comunicação entre switches quando existem mudança de topologia. Esta mudança acontece de uma maneira mais rápida com o backbonefast configurado.

Sintaxe: **spanning-tree backbonefast**
no spanning-tree backbonefast

Modo de comando: Global Configuration.

Exemplo: habilite a configuração backbonefast no switch.

INTELBRAS_config#spanning-tree backbonefast

37.32. STP Guard

Descrição: o comando **spanning-tree guard** é utilizado para configurar o tipo de segurança do protocolo Spanning Tree.

Sintaxe: **spanning-tree guard** loop | none | root
no spanning-tree guard

Modo de comando: interface de configuração Ethernet.

Parâmetros:

- **loop:** evita que a interface seja a origem de loop no switch.
- **none:** desativa a função *Guard*.
- **root:** a porta não seleciona novamente a root bridge após receber um BPDU prioritário.

Exemplo: configure a interface FastEthernet 1 para não ser uma porta raiz.

INTELBRAS_config#interface FastEthernet 0/1

INTELBRAS_config_f0/1#spanning-tree guard root

37.33. Loopguard

Descrição: o comando **spanning-tree loopguard** é utilizado para configurar as interfaces do switch a não gerar loop na rede quando não receberem pacotes BPDU da interface root.

Sintaxe: **spanning-tree loopguard default**
no spanning-tree loopguard default

Modo de comando: Global Configuration.

Exemplo: configure as interfaces do switch com a função *Loopguard*.

INTELBRAS_config#spanning-tree loopguard default

37.34. Loopfast

Descrição: o comando **spanning-tree loopfast** é utilizado para configurar uma melhoria na convergência das redes. Esta configuração evita o loop na rede em um cenário de anel com outros switches.

Sintaxe: **spanning-tree loopfast**
no spanning-tree loopfast

Modo de comando: Global Configuration.

Exemplo: configure as interfaces do switch com a função *Loopfast*.

INTELBRAS_config#spanning-tree loopfast

37.35. Loopfast na interface

Descrição: o comando **spanning-tree loopfast** quando executado no modo de configuração de interface, configura a interface para uma melhoria na convergência da rede.

Sintaxe: **spanning-tree loopfast**
no spanning-tree loopfast

Modo de comando: interface de configuração Ethernet.

Exemplo: habilite o loopfast na interface FastEthernet 1.

INTELBRAS_config#interface FastEthernet 0/1

INTELBRAS_config _f0/1#spanning-tree loopfast

37.36. Envelhecimento rápido

Descrição: o comando **spanning-tree fast-aging** é utilizado para habilitar, configurar e proteger a tabela de endereçamento MAC para STP.

Sintaxe: **spanning-tree fast-aging** protection time (10-60) | flush-fdb
no spanning-tree fast-aging protection time | flush-fdb

Modo de comando: Global Configuration.

Parâmetros:

- **protection:** configuração do aging time para STP.
- **(10-60):** tempo do aging time para a tabela MAC STP. Por padrão o tempo é *15 segundos.*
- **flush-fdb:** funciona de maneira independente da configuração fast-aging. Encaminha solicitação para atualização das tabelas ARP e MAC.

Exemplo: desabilite o fast-aging e habilite o FDB-Flush.

INTELBRAS_config#no spanning-tree fast-aging

INTELBRAS_config#spanning-tree fast-aging flush-fdb

37.37. BPDU-Terminal

Descrição: o comando **spanning-tree bpdu-terminal** é utilizado para configurar o switch a não encaminhar pacotes BPDUS se o STP não estiver ativo.

Sintaxe: **spanning-tree bpdu-terminal**
no spanning-tree bpdu-terminal

Modo de comando: Global Configuration.

Exemplo: desabilite o envio de pacotes BPDU se o STP não estiver habilitado.

INTELBRAS_config#spanning-tree bpdu-terminal

38. 802.1q VLAN

38.1. Criação de VLAN

Descrição: o comando **vlan** é utilizado para criar uma VLAN, se a mesma já não estiver sido criada, e acessar a configuração da mesma.

Sintaxe: **vlan** (1-4094)
no vlan (1-4094)

Parâmetros:

- **(1-4094):** identificador da VLAN.

Modo de comando: Global Configuration.

Exemplo: crie a VLAN 10.

INTELBRAS_config#vlan 10

INTELBRAS_config_vlan10#

38.2. Atribuição de nome à VLAN

Descrição: o comando **name** é utilizado para definir um nome para uma VLAN já criada.

Sintaxe: **name** *nome_da_vlan*
no name

Parâmetros:

- **nome_da_vlan:** frase que será atribuída ao nome da VLAN. Para a especificação de nomes com mais de uma palavra é necessário inclui-lo dentro de aspas.
- **no:** o nome da VLAN será o nome padrão fornecido pelo sistema.

Modo de comando: VLAN Configuration.

Exemplo: configure o nome "VLAN de Teste" para a VLAN 10.

INTELBRAS_config_vlan10#name *VLAN de Teste*

38.3. PVID

Descrição: o comando **switchport pvid** é utilizado para definir o identificador VLAN de uma porta ou grupo de portas.

Sintaxe: **switchport pvid** (1-4094)
no switchport pvid

Parâmetros:

» **(1-4094):** identificador VLAN.

Modo de comando: interface de configuração Ethernet.

Exemplo: configure o pvid 10 para a interface GigaEthernet 1.

INTELBRAS_config_f0/1#switchport pvid 10

38.4. Modo *VLAN*

Descrição: o comando **switchport mode** é utilizado para definir o modo *VLAN* de uma porta ou grupo de portas.

Sintaxe: **switchport mode** access | trunk | dot1q-tunnel-uplink | dot1q-translating-tunnel
no switchport mode

Parâmetros:

» **access:** modo *VLAN acesso*.
» **trunk:** modo *VLAN tronco*.
» **dot1q-tunnel-uplink:** modo *Dot1Q Uplink Tunnel*.
» **dot1q-translating-tunnel:** modo *Dot1Q Translating Tunnel*.
» **no:** mesmo efeito que o parâmetro access.

Modo de comando: interface de configuração Ethernet.

Exemplo: configure o modo *VLAN tronco* na interface GigaEthernet 1.

INTELBRAS_config_f0/1#switchport mode trunk

38.5. VLANs permitidas

Descrição: o comando **switchport trunk vlan-allowed** é utilizado para definir as VLANs permitidas de uma porta ou grupo de portas no modo *VLAN tronco*.

Sintaxe: switchport trunk vlan-allowed *intervalo_vlan_id*
switchport trunk vlan-allowed add *intervalo_vlan_id*
switchport trunk vlan-allowed except *intervalo_vlan_id*
switchport trunk vlan-allowed remove *intervalo_vlan_id*
switchport trunk vlan-allowed all
switchport trunk vlan-allowed none
no switchport trunk vlan-allowed

Parâmetros:

» **intervalo_vlan_id:** intervalo de IDs VLAN que será permitido pela porta.
» **add:** o intervalo VLAN especificado será adicionado aos já permitidos pela interface.
» **remove:** o intervalo VLAN especificado será removido dos já permitidos pela interface.
» **except:** a interface irá permitir todas as VLANs, exceto as especificadas no intervalo.
» **all:** a interface irá permitir todas as VLANs.
» **none:** a interface não irá permitir pacotes de nenhuma VLAN.
» **no:** mesmo efeito que o parâmetro all.

Modo de comando: interface de configuração Ethernet.

Exemplo: configure a interface GigaEthernet 1 para que ela permita as VLANs 10,20 a 30.

INTELBRAS_config_f0/1#switchport trunk vlan-allowed 10,20-30

38.6. VLANs desmarcadas

Descrição: o comando **switchport trunk vlan-untagged** é utilizado para configurar o modo de egresso como *Sem tag* de uma VLAN de uma porta ou grupo de portas no modo *Tronco*.

Sintaxe: **switchport trunk vlan-untagged** *intervalo_vlan_id*
switchport trunk vlan-untagged add *intervalo_vlan_id*
switchport trunk vlan-untagged except *intervalo_vlan_id*
switchport trunk vlan-untagged remove *intervalo_vlan_id*
switchport trunk vlan-untagged all
switchport trunk vlan-untagged none
no switchport trunk vlan-untagged

Parâmetros:

- **intervalo_vlan_id:** intervalo de IDs de VLAN que serão desmarcados pela porta.
- **add:** o intervalo VLAN especificado será adicionado aos já desmarcados pela interface.
- **remove:** o intervalo VLAN especificado será removido dos já desmarcados pela interface.
- **except:** a interface irá desmarcar todas as VLANs, exceto as especificadas no intervalo.
- **all:** a interface irá desmarcar todas as VLANs.
- **none:** a interface não irá desmarcar nenhuma VLAN.
- **no:** a interface irá desmarcar os pacotes da VLAN correspondente ao seu PVID.

Modo de comando: interface de configuração Ethernet.

Exemplo: configure a interface GigaEthernet 1 para que ela retire a marcação VLAN dos pacotes pertencentes as VLANs 10,20 a 30.

INTELBRAS_config_f0/1#switchport trunk vlan-untagged 10,20-30

38.7. Informações VLAN

Descrição: o comando **show vlan** é utilizado para visualizar as informações de VLAN do sistema.

Sintaxe: **show vlan** id (1-4094)
show vlan interface GigaEthernet|Port-Agreggator *interface_id*
show vlan mac-vlan
show vlan protocol-vlan
show vlan dot1q-tunnel|dot1q-translating-tunnel
show vlan dot1q-tunnel|dot1q-translating-tunnel interface GigaEthernet|Port-Agreggator *interface_id*
show vlan subnet

Parâmetros:

- **id (1-4094):** as informações exibidas serão da VLAN (1-4094).
- **interface:** serão exibidas informações VLAN de uma porta ou grupo de portas.
- **interface_id:** identificador da interface.
- **mac-vlan:** as informações exibidas serão referentes a função de *MAC VLAN*.
- **protocol-vlan:** as informações exibidas serão referentes a função de *Protocolo VLAN*.
- **dot1q-tunnel:** as informações exibidas serão referentes a função de *Dot1Q Uplink Tunnel*.
- **dot1q-translating-tunnel:** as informações exibidas serão referentes a função de *Dot1Q Translating Tunnel*.
- **subnet:** as informações exibidas serão referentes a sub-redes baseadas em VLAN.

Modo de comando: Privileged EXEC.

Exemplo: exiba as informações da VLAN 1.

INTELBRAS#show vlan id 1

Exemplo: exiba as informações VLAN da interface GigaEthernet 1.

INTELBRAS#show vlan interface GigaEthernet 0/1

38.8. MAC VLAN

Descrição: o comando mac-vlan é utilizado para configurar manualmente uma entrada MAC com uma VLAN.

Sintaxe: **mac-vlan mac-address** *mac_add mask mac_mask* | vlan (1-4094)
no mac-vlan mac-address *mac_add mask mac_mask*

Parâmetros:

- **mac_add:** MAC address a ser inserido na tabela.
- **mac_mask:** máscara do MAC de origem.
- **(1-4094):** identificador da VLAN.

Modo de comando: Global Configuration.

Exemplo: configure o MAC 00:11:22:33:44:55 na VLAN 20.

INTELBRAS_config#mac-vlan mac-address 0001.1222.3334 mask ffff.ffff.ff00 vlan 20

Habilitar MAC VLAN na interface

Descrição: o comando **switchport mac-vlan** é utilizado para habilitar ou desabilitar o MAC VLAN na interface.

Sintaxe: **switchport mac-vlan**
no switchport mac-vlan

Modo de comando: interface de configuração Ethernet.

Exemplo: configure o MAC VLAN na interface GigaEthernet 1.

INTELBRAS_config_f0/1#switchport mac-vlan

38.9. Protocolo VLAN

Descrição: o comando **protocol-vlan** é utilizado para configurar manualmente uma entrada MAC com um tipo de protocolo.

Sintaxe: **protocol-vlan** ether-type *(0x0600-0xFFFF)* vlan (1-4094)
no protocol-vlan ether-type *(0x0600-0xFFFF)*

Parâmetros:

- **(0x0600 – 0xFFFF):** valor ether-type do pacote.
- **(1-4094):** identificador da VLAN.

Modo de comando: Global Configuration.

Exemplo: configure uma entrada para o protocolo VLAN, tipo Ethernet 0x0800 para a VLAN 20.

INTELBRAS_config#protocol-vlan ether-type 0x0800 vlan 20

Habilitar protocolo VLAN na interface

Descrição: o comando **switchport protocol-vlan** é utilizado para habilitar ou desabilitar o protocolo VLAN na interface.

Sintaxe: **switchport protocol-vlan**
no switchport protocol-vlan

Modo de comando: interface FastEthernet Configuration.

Exemplo: configure uma entrada para o protocolo VLAN na interface FastEthernet 1.

INTELBRAS_config#interface fastEthernet 0/1

INTELBRAS_config_f0/1#switchport protocol-vlan

38.10. Voice VLAN

Descrição: o comando **switchport voice-vlan** é utilizado para configurar uma VLAN especialmente para o fluxo de voz. Inicialmente deve-se criar uma VLAN para depois atribuí-la à VLAN de voz em uma porta específica.

Sintaxe: **switchport voice-vlan** vlan *(1-4094)*
no switchport voice-vlan

Parâmetro:

» **(1-4094):** identificador da VLAN.

Modo de comando: interface de configuração Ethernet.

Exemplo: configurar a VLAN 2 como VLAN de voz para porta FastEthernet 1.

INTELBRAS_config#interface FastEthernet 0/1

INTELBRAS_config_f0/1# switchport voice-vlan 2

Voice VLAN OUI

Descrição: o comando **voice-vlan** 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.

Sintaxe: **voice-vlan mac-address** *mac_add* mask *mac_mask*
no voice-vlan mac-address *mac_add* mask *mac_mask*

Parâmetro:

» **mac_add:** MAC address a ser inserido na tabela.

» **mac_mask:** máscara do MAC address.

Modo de comando: Global Configuration.

Exemplo: insira na tabela a faixa de MAC de 0200.1232.5600 até 0200.1232.56FF.

INTELBRAS_config#voice-vlan mac-address 0200.1232.5600 mask ffff.ffff.ff00

39. GVRP

Descrição: o comando **gvrp** é utilizado para habilitar o aprendizado de VLANs dinâmicas através do protocolo GVRP.

Sintaxe: **gvrp**
no gvrp

Modo de comando: Global Configuration.

Exemplo: habilite o protocolo GVRP.

INTELBRAS_config#gvrp

39.1. Filtro de VLANs dinâmicas

Descrição: o comando **gvrp dynamic-vlan-pruning** é utilizado para filtrar as VLANs dinâmicas para que as mesmas tenham efeito apenas para as interfaces com o GVRP ativo.

Sintaxe: **gvrp dynamic-vlan-pruning**
no gvrp dynamic-vlan-pruning

Modo de comando: Global Configuration.

Exemplo: habilite o filtro de VLANs dinâmicas.

INTELBRAS_config#gvrp dynamic-vlan-pruning

INTELBRAS_config#

39.2. Depuração GVRP

Descrição: o comando **debug gvrp** é utilizado para habilitar a depuração de GVRP do sistema.

Sintaxe: **debug gvrp** event | packet
no debug gvrp event | packet

Parâmetros:

» **event:** serão depurados eventos GVRP.

» **packet:** serão depurados pacotes GVRP.

Modo de comando: Privileged EXEC.

Exemplo: habilite a depuração de eventos GVRP do sistema.

INTELBRAS#debug gvrp event

39.3. Informações GVRP

Descrição: o comando **show gvrp** é utilizado para exibir o status ou estatísticas GVRP do sistema.

Sintaxe: **show gvrp** status | statistics
show gvrp statistics interface GigaEthernet | Port-aggregator *interface_id*

Parâmetros:

- **status:** o status GVRP do sistema será exibido.
- **statistics:** serão exibidas estatísticas GVRP.
- **interface:** será exibida a estatística GVRP de uma única interface.
- **interface_id:** identificador da interface.

Modo de comando: Privileged EXEC.

Exemplo: exiba as estatísticas GVRP da interface GigaEthernet 1.

INTELBRAS#show gvrp statistics interface GigaEthernet 0/1

GVRP statistics on port g0/1

GVRP Status : Enabled

GVRP Frames Received : 0

GVRP Frames Transmitted : 20

GVRP Frames Discarded : 0

GVRP Last Pdu Origin : 0000.0000.0000

40. GARP

40.1. Tempo GARP global

Descrição: o comando **garp timer leaveall** é utilizado para especificar o tempo GARP de LeaveAll do sistema. Quando esgotado este tempo o sistema irá apagar seus registros de VLANs dinâmicas e enviará mensagens de cancelamento de registro para seus vizinhos.

Sintaxe: **garp timer leaveall** (10-32765)
no garp timer leaveall

Parâmetros:

- **(10-32765):** tempo em centésimos de segundos.

Modo de comando: Global Configuration.

Exemplo: configure o tempo GARP de LeaveAll para 100 centésimos de segundos.

INTELBRAS_config#garp timer leaveall 100

40.2. Tempos GARP de interface

Descrição: o comando **garp timer** é utilizado para especificar tempos GARP respectivos as interfaces do switch.

Sintaxe: **garp timer** hold | join | leave (10-32765)
no garp timer hold | join | leave

Parâmetros:

- **hold:** especifica a configuração do tempo GARP de Hold.
- **join:** especifica a configuração do tempo GARP de Join.
- **leave:** especifica a configuração do tempo GARP de Leave.

Modo de comando: interface de configuração Ethernet.

Exemplo: configure o tempo GARP de Leave da interface GigaEthernet 1 para 100 centésimos de segundos.

INTELBRAS_config_f0/1#garp timer leave 100

40.3. Informações GARP

Descrição: o comando **show garp** é utilizado para exibir o status ou tempos GARP do sistema.

Sintaxe: **show garp** status | timers
show garp timers interface GigaEthernet | Port-aggregator *interface_id*

Parâmetros:

- **status:** o status GVRP do sistema será exibido.
- **timers:** serão exibidos os tempos GARP do sistema.
- **interface:** será exibida o tempo GARP de uma única interface.
- **interface_id:** identificador da interface.

Modo de comando: Privileged EXEC.

Exemplo: exiba as estatísticas GVRP da interface GigaEthernet 1.

INTELBRAS#show garp timers interface GigaEthernet 0/1

GARP timers on port 1(G0/1)

Garp Join Time : 20 centiseconds

Garp Leave Time : 60 centiseconds

Garp LeaveAll Time : 1000 centiseconds

Garp Hold Time : 10 centisecondsGVRP Last Pdu Origin : 0000.0000.0000

41. SNMP

41.1. Comunidade SNMP

Descrição: o comando **snmp-server community** permite criar comunidades SNMP.

Sintaxe: **snmp-server community** (0-7) | *string* view/*view-name* ro | rw | *word*
no snmp-server community

Parâmetros:

- **0|7:** com ou sem criptografia. Escolha 0 para senha sem criptografia e 7 para senha com criptografia. Se for escolhido 7, o nome da comunidade inserida já deve estar criptografado.
- **string:** nome da comunidade SNMP. Tamanho máximo de 20 caracteres.
- **view/view-name:** configuração opcional. Representa o nome da view previamente definida. Nesta view, os objetos MIB são definidos.
- **ro:** somente leitura (read only).
- **rw:** leitura e escrita (read and write).
- **word:** nome da ACL IP do proxy SNMP.

Modo de comando: Global Configuration.

Exemplo: crie a comunidade teste com permissão de leitura e escrita.

INTELBRAS_config#snmp-server community teste rw

41.2. Agente SNMP

Descrição: o comando **snmp-server engineID local** permite configurar um agente SNMP.

Sintaxe: **snmp-server engineID local** *engineID*
no snmp-server engineID local *engineID*

Parâmetros:

- **engineID:** identificação do agente SNMP. Pode ser inserido um valor até 31 números como identificação do agente.

Modo de comando: Global Configuration.

Exemplo: crie um agente SNMP com identificação 852341599cfed.

INTELBRAS_config#snmp-server engineID local 852341599cfed

41.3. Grupos SNMP

Descrição: o comando **snmp-server group** permite criar grupos SNMP.

Sintaxe: **snmp-server group** *groupname* v3 *auth* | *noauth* | *priv* read *readview* write *writeview* notify *notifyview* access access-list *word*
no snmp-server group groupname

Parâmetros:

- **groupname:** nome do grupo SNMP.
- **auth:** especifica a autenticação de um pacote sem criptografia.
- **noauth:** especifica um pacote sem criptografia.
- **priv:** especifica a autenticação de um pacote com criptografia.
- **access-list:** permite que seja associado uma lista de acesso a este grupo.
- **notifyview:** permite especificar uma notificação para o grupo.
- **readview:** permite especificar uma leitura para o grupo.
- **writeview:** permite especificar uma escrita para o grupo.
- **word:** nome da view.

Modo de comando: Global Configuration.

Exemplo: crie um grupo SNMP.

INTELBRAS_config#snmp-server group TESTE v3 priv write TESTE_1

41.4. Hosts SNMP

Descrição: o comando **snmp-server host** permite criar hosts para receber as traps.

Sintaxe: **snmp-server host | hostv6** *host* udp | port *port-num* permit | deny *event-id* version v1 | v2c | v3 informs | traps | auth | noauth *community-string* | *user* authentication | configure | snmp
no snmp-server host host community-string

Parâmetros:

- **host:** nome ou endereço do host.
- **port-num:** especifica o ID de uma porta UDP.
- **event-id:** permite ou bloqueia a transmissão em uma porta específica.
- **community-string/user:** nome da comunidade SNMPv1/v2c ou nome de usuário SNMPv3.

Modo de comando: Global Configuration.

Exemplo: crie um host 10.20.30.40 para receber traps do tipo public.

INTELBRAS_config#no snmp-server host 10.20.30.40 public

41.5. Local

Descrição: o comando **snmp-server location** é usado para criar uma informação da localização do nó.

Sintaxe: **snmp-server location** *text*
no snmp-server location

Parâmetros:

- **text:** localização do nó.

Modo de comando: Global Configuration.

Exemplo: crie uma localização para o switch.

INTELBRAS_config#no snmp-server location Predio_central

41.6. Contato

Descrição: o comando **snmp-server contact** é usado para enviar o texto do objeto mib sysContact.

Sintaxe: **snmp-server contact** *line*
no snmp-server contact

Parâmetros:

» **line:** identificação da pessoa de contato.

Modo de comando: Global Configuration.

Exemplo: crie um contato para informações SNMP.

INTELBRAS_config#snmp-server contact RAMAL_111

41.7. Tamanho do pacote

Descrição: o comando **snmp-server location** é usado para definir o tamanho máximo do pacote SNMP quando o servidor faz uma requisição.

Sintaxe: **snmp-server packetsize** *(484-17940)*
no snmp-server packetsize

Parâmetros:

» **(484-17940):** tamanho do pacote, pode variar entre 484 e 17940. O valor padrão é *3000 bytes*.

Modo de comando: Global Configuration.

Exemplo: configure um filtro para pacotes com tamanho máximo de 1024 bytes.

INTELBRAS_config#snmp-server packetsize 1024

41.8. Queue-length

Descrição: o comando **snmp-server queue-length** é usado para definir o tamanho da fila para hosts.

Sintaxe: **snmp-server queue-length** *(0-1000)*
no snmp-server queue-length

Parâmetros:

» **(0-1000):** tamanho da fila de traps que podem ser salvas, pode variar de 1 até 1000. O valor padrão é *10 traps*.

Modo de comando: Global Configuration.

Exemplo:

INTELBRAS_config#snmp-server queue-length 200

41.9. Interface de origem

Descrição: o comando **snmp-server trap-source** é usado para definir a porta de origem de todas as conexões.

Sintaxe: **snmp-server trap-source** *interface*
no snmp-server trap-source

Parâmetros:

» **interface:** interface em que os traps SNMP são gerados.

Modo de comando: Global Configuration.

Exemplo:

INTELBRAS_config#snmp-server trap-source VLAN 1

41.10. Tempo de retransmissão

Descrição: o comando **snmp-server trap-timeout** é usado para definir o tempo de retransmissão das traps.

Sintaxe: **snmp-server trap-timeout** *(1-1000)*
no snmp-server trap-timeout

Parâmetros:

» **(1-1000):** intervalo de tempo para a retransmissão das traps. O valor padrão é *30 segundos*.

Modo de comando: Global Configuration.

Exemplo: configure um intervalo de tempo de 20 segundos para retransmissão das traps.

INTELBRAS_config#snmp-server trap-timeout 20

41.11. Usuário SNMP

Descrição: o comando **snmp-server user** é usado para configurar um usuário e senha para acessar os servidores SNMP.

Sintaxe: **snmp-server user** *username groupname* v3 auth | encrypted md5 | sha *auth-password*
no snmp-server user *username groupname* v3

Parâmetros:

» **username:** nome de usuário.
» **groupname:** grupo ao qual o usuário pertence.
» **auth-password:** senha para autenticação de usuário.

Modo de comando: Global Configuration.

Exemplo: configure um usuário com nome ACCESS pertencente ao grupo admin com autenticação e criptografia utilizando MD5 como algoritmo harsh e senha 12345678.

INTELBRAS_config#snmp-server user ACCESS admin v3 encrypted auth md5 12345678

41.12. Verificação de MIB

Descrição: o comando **snmp-server view** é usado para configurar uma visualização para uma MIB específica.

Sintaxe: **snmp-server view** *view-name oid-tree* include | exclude
no snmp-server view *view-name*

Parâmetros:

» **view-name:** nome para a visualização da MIB.
» **oid-tree:** árvore da MIB.

Modo de comando: Global Configuration.

Exemplo: inclua a visualização da MIB 1.3.6.2.4.

INTELBRAS_config#snmp-server view teste 1.3.6.2.4 included

41.13. Endereço de origem

Descrição: o comando **snmp-server source-addr** é usado para especificar um endereço de origem para responder a todas as solicitações SNMP.

Sintaxe: **snmp-server source-addr** *A.B.C.D*
no snmp-server source-addr

Parâmetros:

» **A.B.C.D:** endereço IP de origem das respostas SNMP.

Modo de comando: Global Configuration.

Exemplo: configure o endereço de IP 192.168.10.1 como o endereço de origem de todos os pacotes SNMP.

INTELBRAS_config#snmp-server source-addr 192.168.10.1

41.14. Porta UDP

Descrição: o comando **snmp-server source-addr** é usado para especificar a porta para um agente SNMP receber os pacotes.

Sintaxe: **snmp-server udp-port** *portnum*
no snmp-server udp-port

Parâmetros:

» **udp-port:** porta UDP do Agente SNMP. É a porta de escuta do agente SNMP por padrão é a porta *162*.

Modo de comando: Global Configuration.

Exemplo: configure a porta 1234 como a porta de escuta do agente SNMP.

INTELBRAS_config#snmp-server udp-port 1234

41.15. Criptografia

Descrição: o comando **snmp-server encryption** é usado para criptografar a senha da comunidade SNMP.

Sintaxe: **snmp-server encryption**

Modo de comando: Global Configuration.

Exemplo: crie uma criptografia para senhas de acesso a servidores SNMP que não estejam criptografadas.

INTELBRAS_config#snmp-server encryption

41.16. Hostname

Descrição: o comando **snmp-server trap-add-hostname** é usado para adicionar o nome do host na variável vinculada quando ocorre o envio de traps SNMP.

Sintaxe: **snmp-server trap-add-hostname**
no snmp-server trap-add-hostname

Modo de comando: Global Configuration.

Exemplo: ative a função de enviar o nome do host quando ocorre o envio e traps SNMP.

INTELBRAS_config#snmp-server trap-add-hostname

41.17. Log

Descrição: o comando **snmp-server trap-logs** é usado para gravar os registros das transmissões de traps SNMP em logs.

Sintaxe: **snmp-server trap-logs**
no snmp-server trap-logs

Modo de comando: Global Configuration.

Exemplo: ative a função de enviar os logs de traps SNMP para um servidor.

INTELBRAS_config#snmp-server trap-logs

41.18. Controle de acesso

Descrição: o comando **snmp-server set-snmp-dos-max** é usado para configurar a quantidade de acessos com login errados ao servidor SNMP durante o intervalo de 5 minutos.

Sintaxe: **snmp-server set-snmp-dos-max** *retry times*
no snmp-server set-snmp-dos-max

Parâmetros:

» **retry times:** tentativa de solicitação máxima de SNMP em 5 minutos.

Modo de comando: Global Configuration.

Exemplo: configure a quantidade de 10 tentativas de acesso errado em 5 minutos a um servidor SNMP.

INTELBRAS_config#snmp-server set-snmp-dos-max 10

41.19. Keep-alive

Descrição: o comando **snmp-server keep-alive** é usado para configurar o tempo de envio das traps keepalive (mantenha vivo).

Sintaxe: **snmp-server keep-alive** *times*
no snmp-server keep-alive

Parâmetros:

» **times:** define o período de envio da trap keep-alive, pode variar de 1 até 100000 segundos.

Modo de comando: Global Configuration.

Exemplo: configure o tempo de envio da trap keep-alive para 3 segundos.

INTELBRAS_config#snmp-server keep-alive 3

41.20. Código de rede

Descrição: o comando **snmp-server necode** é usado para definir o código do elemento da rede SNMP.

Sintaxe: **snmp-server necode** *text*
no snmp-server necode

Parâmetros:

» **text:** código do elemento da rede.

Modo de comando: Global Configuration.

Exemplo: configure a informação sobre o nó de gerenciamento SNMP.

INTELBRAS_config#snmp-server necode Dial_System_Operator_at_beeper_#_27345

41.21. Eventos

Descrição: o comando **snmp-server event-id** é usado para configurar uma lista de eventos.

Sintaxe: **snmp-server event-id** *number* trap-oid *oid*
no snmp-server event-id *number* trap-oid *oid*

Parâmetros:

» **number:** identificado único para evento.

» **oid:** trap OID incluída no evento.

Modo de comando: Global Configuration.

Exemplo: configure o OID 1.2.3.4.5 para o ID do evento 1.

INTELBRAS_config#snmp-server event-id 1 trap-oid 1.2.3.4.5

41.22. Tempo de Getbulk

Descrição: o comando **snmp-server getbulk-timeout** é usado para configurar o tempo limite para a resposta do processamento do getbulk.

Sintaxe: **snmp-server getbulk-timeout** *(1-30)*
no snmp-server getbulk-timeout

Parâmetros:

» **(1-30):** tempo limite do processamento do pedido de atualização em massa.

Modo de comando: Global Configuration.

Exemplo: configure o tempo para atualização em massa para 5 segundos.

INTELBRAS_config#snmp-server getbulk-timeout 5

41.23. Atraso Getbulk

Descrição: o comando **snmp-server getbulk-delay** é usado para definir o tempo de atraso para evitar que o SNMP ocupe processamento de CPU excessivo quando o agente SNMP processa a solicitação getbulk.

Sintaxe: **snmp-server getbulk-delay** *ticks*
no snmp-server getbulk-delay

Parâmetros:

» **ticks:** define o tempo de intervalo de processamento da CPU para solicitação getbulk. Pode variar de 1 até 50 onde a unidade está em 0,01 segundos. Máximo de 0,5 segundos e mínimo de 0,01 segundo.

Modo de comando: Global Configuration.

Exemplo: configure o menor intervalo para o processamento da CPU quando o agente SNMP realizar atualização em massa.

INTELBRAS_config#snmp-server getbulk-timeout 5

41.24. Informações

Descrição: o comando **show snmp** é usado para mostrar as estatísticas SNMP.

Sintaxe: **show snmp** engineID | host | view | mibs | group | user

Parâmetros:

- **snmp:** mostra as estatísticas de entrada e saída SNMP.
- **engineID:** mostra as informações do agente SNMP.
- **host:** mostra as informações sobre os hosts.
- **view:** mostra as informações de visualização SNMP.
- **mibs:** mostra as informações de registro de mib.
- **group:** mostra as informações de grupos SNMP.
- **user:** mostra as informações de usuários SNMP.

Modo de comando: Privileged EXEC e Global Configuration.

Exemplo: mostre as informações SNMP.

INTELBRAS_config#show snmp

41.25. Depuração

Descrição: o comando **debug snmp** é usado para ativar a troca de informações de depuração SNMP, eventos SNMP de saída e informações de envio e recebimento de pacotes.

Sintaxe: **debug snmp** error | event | packet
no debug snmp

Parâmetros:

- **error:** habilita a depuração das informações de erro SNMP.
- **event:** habilita a depuração das informações dos eventos SNMP.
- **packet:** habilita a depuração das informações sobre entrada e saída de pacotes SNMP.

Modo de comando: Privileged EXEC.

Exemplo: configure o debug para os pacotes SNMP.

INTELBRAS#debug snmp packet

42. RMON

42.1. Alarme

Descrição: o comando **rmon alarm** é usado para criar ou modificar um alarme de evento RMON.

Sintaxe: **rmon alarm** *index variable interval absolute | delta* rising-threshold *value event_number_rising* falling-threshold *value event_number_falling repeat owner string*
no rmon alarm *index*

Parâmetros:

- **index:** configure um índice para a criação ou alteração do evento RMON. Pode variar de 1 à 65535.
- **variable:** informação do objeto que deve ser monitorado.
- **interval:** intervalo de amostragem. Pode variar de 1 à 2147483647 segundos.
- **absolute:** faz uma comparação direta com o valor estabelecido no final do intervalo da amostra.
- **delta:** subtrair o valor da última amostra com o valor corrente e comparar a diferença com o valor estipulado.
- **value:** valor máximo da variável para iniciar o alarme.
- **event_number_rising:** número do alarme caso o valor máximo seja atingido.
- **value:** valor mínimo da variável para iniciar o alarme.
- **event_number_falling:** número do alarme caso o valor mínimo seja atingido.
- **repeat:** informa a necessidade da repetição do alarme.
- **owner:** informa a necessidade da configuração do usuário que definiu o alarme.
- **string:** informe o nome do dispositivo ou usuário que definiu regra, o nome pode ter no máximo 31 caracteres.

Modo de comando: Global Configuration.

Exemplo: configure uma entrada de alarme para monitorar o objeto ifInOctets.2 (1.3.6.1.2.1.2.2.1.10) com intervalo de amostragem 10. Quando o intervalo de amostragem aumenta mais de 15, o evento 1 será acionado. Quando o intervalo de amostragem diminui mais de 25, o evento 2 será acionado.

INTELBRAS_config#rmon alarm 1 1.3.6.1.2.1.2.2.1.10 10 absolute rising-threshold 15 1 falling-threshold 25 2 repeat owner switch

42.2. Evento

Descrição: o comando **rmon event** é usado para criar ou modificar uma entrada de evento.

Sintaxe: **rmon event** *(1-65535)* description *des-string* log owner *owner-string* trap *community* ifctrl *interface*
no rmon event *index*

Parâmetros:

- **(1-65535):** configure um índice para a criação ou alteração do evento RMON.
- **des-string:** informe uma descrição para o evento
- **owner-string:** informe o nome do dispositivo ou usuário que definiu regra, o nome pode variar de 1 a 31 caracteres.
- **community:** informe o nome da comunidade SNMP, o nome pode variar de 1 a 31 caracteres.
- **ifctrl:** informe a interface para o monitoramento do evento.

Modo de comando: Global Configuration.

Exemplo: 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 description teste_1 trap public owner dono_1

42.3. Monitoramento

Descrição: o comando **rmon event** é usado para configurar monitoramento remoto em uma interface.

Sintaxe: **rmon collection stats** *(1-65535)* owner *(1-31)*
no rmon collection stats *index*

Parâmetros:

- **(1-65535):** configure um índice para o controle do monitoramento RMON.
- **(1-31):** informe o nome do dono para o monitoramento.

Modo de comando: interface de configuração Ethernet.

Exemplo: configure a interface GigaEthernet 1 para monitoramento das estatísticas RMON.

INTELBRAS_config#interface GigaEthernet 0/1

INTELBRAS_config_g0/1#rmon collection stats 10 owner dono_1

42.4. Histórico de eventos

Descrição: o comando **rmon collection history** é usado para criar ou modificar histórico dos eventos RMON.

Sintaxe: **rmon collection history** *(1-65535)* buckets *bucket-number* interval *second* owner *owner-name*
no rmon collection history *index*

Parâmetros:

- **(1-65535):** configure um índice para o controle do histórico RMON.
- **bucket-number:** configure o número da amostra. Pode variar de 1 à 65535.
- **second:** representa o intervalo em segundos para amostras em cada intervalo de tempo.
- **owner-name:** informe o nome do dispositivo ou usuário que definiu regra, o nome pode variar de 1 a 31 caracteres.

Modo de comando: interface de configuração Ethernet.

Exemplo: habilite a porta GigaEthernet 1 do grupo RMON history na porta 1, tamanho da amostragem 50 com intervalo de amostragem de 300 segundos e configure o proprietário como dono_1.

INTELBRAS_config#interface GigaEthernet 0/1

INTELBRAS_config_g0/1#ction history 1 buckets 50 interval 300 owner dono_1

42.5. Informações

Descrição: o comando **show rmon** é usado para mostrar as configurações de RMON. Pode ser exibida informações gerais ou de uma porta específica.

Sintaxe: **show rmon** alarm | event | statistics | history

Parâmetros:

- **alarm:** mostra as configurações de alarme para RMON.
- **event:** mostra as configurações dos eventos RMON.
- **statistics:** mostras as estatísticas de RMON.
- **history:** mostra as configurações de history RMON.

Modo de comando: todos os modos de configuração.

Exemplo: exiba as informações RMON da interface FastEthernet 5.

INTELBRAS_config#interface FastEthernet 0/5

INTELBRAS_config_f0/5#show rmon

43. LLDP

Descrição: o comando **lldp run** é utilizado para habilitar o LLDP.

Sintaxe: **lldp run**
no lldp run

Modo de comando: Global Configuration.

Exemplo: habilite o LLDP.

INTELBRAS_config#lldp run

43.1. Tempo de vida

Descrição: o comando **lldp holdtime** é utilizado para configurar o tempo de vida de um pacote LLDP. O tempo de vida LLDP corresponde ao tempo que as informações do pacote a ser enviado serão válidas.

Sintaxe: **lldp holdtime** (0-65535)
no lldp holdtime

Parâmetros:

- **(0-65535):** tempo de vida em unidades de segundo.

Modo de comando: Global Configuration.

Exemplo: configure o Tempo de Vida LLDP para 10 segundos.

INTELBRAS_config#lldp holdtime 10

43.2. Intervalo de transmissão

Descrição: o comando **lldp timer** é utilizado para configurar o intervalo de transmissão entre pacotes LLDP.

Sintaxe: **lldp timer** (5-65534)
no lldp timer

Parâmetros:

- **(5-65534):** intervalo de transmissão em unidades de segundo.

Modo de comando: Global Configuration.

Exemplo: configure o intervalo de transmissão de pacotes LLDP para 10 segundos.

INTELBRAS_config#lldp timer 10

43.3. Atraso de reinício

Descrição: o comando **lldp reinit** é utilizado para configurar o atraso de reinício LLDP.

Sintaxe: **lldp reinit** (2-5)
no lldp reinit

Parâmetros:

» **(2-5):** atraso de reinício em unidades de segundo.

Modo de comando: Global Configuration.

Exemplo: configure o Atraso de Reinício LLDP para 10 segundos.

INTELBRAS_config#lldp reinit 10

43.4. TLV

Descrição: o comando **lldp tlv-select** é utilizado para configurar quais TLVs serão adicionados ao pacote LLDP. Por padrão todos os TLVs são enviados.

Sintaxe: **lldp tlv-select** management-address | port-description | system-capabilities | system-description | system-name
no lldp tlv-select management-address | port-description | system-capabilities | system-description | system-name

Parâmetros:

» **management-address:** será adicionado um TLV com a informação do endereço IP de gerenciamento do sistema.
» **port-description:** será adicionado um TLV com as informações de descrição de porta do sistema.
» **system-capabilities:** será adicionado um TLV com informações relativas as capacidades do sistema.
» **system-description:** será adicionado um TLV com a informação de descrição do sistema.
» **system-name:** será adicionado um TLV com a informação do nome atribuído ao sistema.

Modo de comando: Global Configuration.

Exemplo: configure a função *LLDP* para que o sistema não envie pacotes LLDP com a informação do endereço IP de gerenciamento.

INTELBRAS_config#no lldp tlv-select magement-address

43.5. Envio de Trap SNMP

Descrição: o comando **lldp trap-send** é utilizado para configurar o envio de Trap SNMP respectivas ao protocolo LLDP.

Sintaxe: **lldp trap-send** lldp-mib | ptopo-mib
no lldp trap-send lldp-mib | ptopo-mib

Parâmetros:

» **lldp-mib:** para enviar Trap SNMP de notificação para o LLDP MIB.
» **ptopo-mib:** para enviar Trap SNMP de notificação para o PTOPO MIB.

Modo de comando: Global Configuration.

Exemplo: configure o envio de Trap SNMP para o LLDP MIB.

INTELBRAS_config#lldp trap-send lldp-mib

43.6. Configuração LLDP das interfaces

Descrição: o comando **lldp receive|transmit** é utilizado para habilitar no equipamento o recebimento e o envio respectivamente de pacotes LLDP na interface.

Sintaxe: **lldp** receive | transmit
no lldp receive | transmit

Parâmetros:

» **receive:** habilita o recebimento de pacotes LLDP.
» **transmit:** habilita a transmissão de pacotes LLDP.

Modo de comando: interface de configuração Ethernet.

Exemplo: habilite a transmissão de pacotes LLDP na interface GIgaEthernet 1.

INTELBRAS_config_f0/1#lldp trasnmit

43.7. Dot1 TLV

Descrição: o comando **lldp dot1-tlv-select** é utilizado para configurar os TLVs com informações respectivas ao padrão 802.1 que serão adicionados no pacote LLDP em cada interface.

Sintaxe: **lldp dot1-tlv-select** port-vlan-id | protocol-vlan-id | vlan-name | protocol-identity
no lldp dot1-tlv-select port-vlan-id | protocol-vlan-id | vlan-name | protocol-identity

Parâmetros:

- **port-vlan-id:** será adicionado um TLV com a informação de PVID da porta.
- **protocol-vlan-id:** será adicionado um TLV com informação indicando se a porta suporta VLAN baseada em porta ou protocolo, e o VLAN ID associado.
- **vlan-name:** será adicionado um TLV com a informação do nome da VLAN e PVID da porta.
- **protocol-identity:** será adicionado um TLV com informação de quais protocolos estão ativos na porta.

Modo de comando: interface de configuração Ethernet.

Exemplo: habilite a inclusão do TLV de nome de VLAN na transmissão dos pacotes LLDP enviados pela interface GigaEthernet 1.

INTELBRAS_config_f0/1#lldp dot1-tlv-select vlan-name

43.8. Dot3 TLV

Descrição: o comando l**ldp dot3-tlv-select** é utilizado para configurar os TLVs com informações respectivas ao padrão 802.3 que serão adicionados no pacote LLDP em cada interface.

Sintaxe: **lldp dot3-tlv-select** link-agreggation | macphy-confg | max-frame-size | power
no lldp dot3-tlv-select link-agreggation | macphy-confg | max-frame-size | power

Parâmetros:

- **link-agreggation:** será adicionado um TLV com informação de agregação de link da porta.
- **macphy-confg:** será adicionado um TLV com informações de Duplex, Velocidade, tipo MAU, e capacidades PMD.
- **max-frame-size:** será adicionado um TLV com a informação do tamanho de quadro máximo da porta.
- **power:** será adicionado um TLV com a informação de PoE da porta.

Modo de comando: interface de configuração Ethernet.

Exemplo: habilite a inclusão do TLV de agregação de link na transmissão dos pacotes LLDP enviados pela interface GigaEthernet 1.

INTELBRAS_config_f0/1#lldp dot3-tlv-select link-agreggation

43.9. TLV MED

Descrição: o comando **lldp med-tlv-select** é utilizado para configurar os TLVs incluídos ao pacote LLDP na versão LLDP-MED.

Sintaxe: **lldp med-tlv-select** *network-policy* | *inventory* | *location* | *power-management*
no lldp med-tlv-select *network-policy* | *inventory* | *location* | *power-management*

Parâmetros:

- **network-policy:** será incluído um TLV com as informações de políticas de rede, ou seja, Voice VLAN ID, prioridade VLAN e prioridade DSCP.
- **inventory:** será incluído um TLV com as informações de número de revisão de hardware, software e firmware, número de série do switch, nome do fabricante, nome do modelo e Asset ID.
- **location:** será incluído um TLV com a informações de localização, são estas: coordenadas, número de emergência (ELIN) e endereço.
- **power-management:** será incluído um TLV com informações de PoE.

Modo de comando: interface de configuração Ethernet.

Exemplo: habilite a inclusão do TLV MED de políticas de rede na transmissão dos pacotes LLDP enviados pela interface GigaEthernet 1.

INTELBRAS_config_f0/1#lldp med-tlv-select network-policy

43.10. Informações de LLDP

Descrição: o comando **show lldp** é utilizado para exibir as informações respectivas ao LLDP.

Sintaxe: **show lldp** errors | neighbors | traffic
show lldp neighbors detail
show lldp interface GigaEthernet *interface_id*

Parâmetros:

- **errors:** será exibido dados sobre erros relacionados ao LLDP.
- **neighbors:** será exibido uma tabela com dados básicos dos dispositivos vizinhos recebidos via LLDP.
- **traffic:** será exibido as estatísticas de tráfego de pacotes LLDP.
- **neighbors detail:** será exibido dados detalhados dos dispositivos vizinhos recebidos via LLDP.
- **interface GigaEthernet:** será exibido o status LLDP de uma interface GigaEthernet.
- **interface_id:** identificador da interface, formato: *0/(1-10)*.

Modo de comando: Privileged EXEC.

Exemplo: exiba as informações básicas dos dispositivos vizinhos.

INTELBRAS#show lldp neighbors

Capability Codes:

(R)Router,(B)Bridge,(C)DOCsIs Cable Device,(T)Telephone

(W)WLAN Access Point, (P)Repeater,(s)station,(O)Other

Device-ID Local-Intf Hldtme Port-ID Capability

switch Gig0/2 115 Gig0/32 B

switch Gig0/32 114 Gig0/2 B

Total entries dispalyed: 2

43.11. Limpar informações LLDP

Descrição: o comando **clear lldp** é utilizado limpar os dados LLDP.

Sintaxe: **clear lldp** counters | table

Parâmetros:

- **counters:** os contadores LLDP serão zerados.
- **table:** a tabela LLDP de informações de vizinhos será limpada.

Modo de comando: Privileged EXEC.

Exemplo: limpe a tabela LLDP de vizinhos.

INTELBRAS#clear lldp table

43.12. Localização

Número de emergência

Descrição: o comando **location elin identifier** é utilizado para configurar um número de emergência associado a um identificador ELIN.

Sintaxe: **location elin identifier** (1-65535) *número_de_emergência*
no location elin identifier (1-65535)

Parâmetros:

- **(1-65535):** identificador do número de emergência a ser configurado.
- **número_de_emergência:** número de emergência a ser configurado.

Modo de comando: Global Configuration.

Exemplo: configure o número de emergência 55 48 9 9123 4567 associado ao identificador ELIN 1.

INTELBRAS_config#location elin identifier 1 5548991234567

43.13. Endereço

Descrição: o comando **location civic identifier** é utilizado para criar um identificador que será associado a informações de endereço.

Sintaxe: **location civic identifier** (1-65535)
no location civic identifier (1-65535)

Parâmetros:

» **(1-65535):** identificador do endereço a ser configurado.

Modo de comando: Global Configuration.

Exemplo: crie o identificador de endereço 1.

INTELBRAS_config#location civic identifier 1

Os comandos a seguir são utilizados para definir as informações de um endereço.

Modo de comando: address configuration.

» Tabela 1 - Comandos de endereço

Comando	Parâmetro	Descrição
additional-code	*código_adicional*	Informação de código adicional
additional-location	*local_adicional*	Informação de local adicional
building	*edifício*	Informação do edifício
city	*cidade*	Nome da cidade
country	*código_país*	Código do país (ISO 3166)
county	*município*	Nome do município
division	*divisão*	Informação de divisão
floor	*andar*	Informação do andar
landmark	*referência*	Referência
language	*idioma*	Idioma
leading-street-dir	*direção_rua_principal*	Direção da rua principal
name	*nome*	Nome do local
neighborhood	*vizinhança*	Informação da vizinhança
number	*número_da_casa*	Número da casa
postal-code	*código_postal*	Código postal
postal-community	*unidade_postal*	Unidade postal
post-office-box	*caixa_postal*	Caixa postal
room	*sala*	Informação da sala
script	*script*	Informação de como chegar ao local
state	*estado*	Nome do estado
street	*rua*	Nome da rua
street-number-suffix	*sufixo_número_rua*	Sufixo do número da rua
street-suffix	*sufixo_rua*	Sufixo do nome da rua
trailing-street-suffix	*sufixo_rua_adjacente*	Sufixo da rua adjacente
type-of-place	*tipo_do_lugar*	Informação do tipo do lugar
unit	*unidade*	Informação da unidade local

Exemplo: configure o nome da cidade como Florianópolis para o endereço de identificador 5.

INTELBRAS_config#location civic identifier 5

INTELBRAS_config_civic#city Florianopolis

43.14. Atribuição de localização

Descrição: o comando **location** é utilizado para atribuir um endereço ou número de emergência a uma interface para que esta envie essas informações no pacote LLDP se a função estiver habilitada.

Sintaxe: **location** civic | elin (1-65535)
no location civic | elin (1-65535)

Parâmetros:

- **civic:** será atribuído um endereço.
- **elin:** será atribuído um número de emergência.
- **(1-65535):** identificador do número de emergência ou do endereço a ser atribuído.

Modo de comando: interface de configuração Ethernet.

Exemplo: atribua o número de emergência de identificador ELIN 2 para a interface GigaEthernet 1.

INTELBRAS_config_f0/1#location elin 1

44. IGMP Snooping

Descrição: a função **Igmp-snooping** permite o controle de multicast que funciona na camada 2 do switch. Multicast é o método de transmissão de um pacote de dados a múltiplos destinos ao mesmo tempo. Este comando pode efetivamente impedir que os grupos multicast sejam transmitidos na rede. É possível ativar o IGMP snooping em uma VLAN específica.

Sintaxe: **ip igmp-snooping** vlan *vlan_id*
no ip igmp-snooping vlan *vlan_id*

Parâmetros:

- **vlan id (1- 4094):** identificação da VLAN.

Modo de comando: Global Configuration.

Exemplo: ative a função *Ip igmp-snooping* para a VLAN 1.

INTELBRAS_config#ip igmp-snooping vlan 1

44.1. Endereços estáticos

Descrição: a função **Igmp-snooping static** permite configurar um endereço Multicast Estático. Os hosts que não suportam o IGMP podem receber mensagens multicast correspondentes configurando o endereço multicast estático.

Sintaxe: **ip igmp-snooping** vlan *vlan_id* **static** *A.B.C.D* interface *intf*
no ip igmp-snooping vlan *vlan_id* **static** *A.B.C.D* interface *intf*

Parâmetros:

- **vlan id (1- 4094):** identificação da VLAN.
- **A.B.C.D:** especifica o endereço de IP Multicast.
- **intfl:** especifica a porta da interface.

Modo de comando: Global Configuration.

Exemplo: configure o igmp-snooping static na porta 5 da interface FastEthernet, IP Multicast estático 234.5.6.7.

INTELBRAS_config#ip igmp-snooping vlan 2 static 234.5.6.7 interface GigaEthernet0/5

44.2. Saída imediata

Descrição: a função **Igmp-snooping immediate-leave** é usada para habilitar a função de saída imediata. Com a função de saída imediata configurada, o switch pode deletar a porta da lista de portas do grupo multicast depois que o switch recebe a mensagem de saída.

Sintaxe: **ip igmp-snooping** vlan *vlan_id* **immediate-leave**
no ip igmp-snooping vlan *vlan_id* **immediate-leave**

Parâmetros:

- **vlan id (1- 4094):** identificação da VLAN.

Modo de comando: Global Configuration.

Exemplo: atribua a permissão imediata para a VLAN 1.

INTELBRAS_config#ip igmp-snooping vlan 1 immediate-leave

44.3. Roteamento Multicast

Descrição: a função **Igmp-snooping mrouter** é usada para configurar uma porta de roteamento estático multicast da VLAN. O switch irá enviar os reports multicast para todas as portas configuradas da VLAN.

Sintaxe: **ip igmp-snooping** vlan *vlan_id* **mrouter** interface *intf*
no ip igmp-snooping vlan *vlan_id* **mrouter** interface *intf*

Parâmetros:

- **vlan id (1- 4094):** identificação da VLAN.
- **intfl:** especifica a porta da interface.

Modo de comando: Global Configuration.

Exemplo: defina a porta 5 para o roteamento estático da interface Gigabit Ethernet, VLAN 2.

INTELBRAS_config#ip igmp-snooping vlan 2 mrouter interface GigaEthernet0/5

44.4. Encaminhamento L3

Descrição: o comando **igmp-snooping forward-l3-to-mrouter** é usado para enviar os pacotes de dados para a porta de roteamento Multicast.

Sintaxe: **ip igmp-snooping forward-l3-to-mrouter**
no ip igmp-snooping forward-l3-to-mrouter

Modo de comando: Global Configuration.

Exemplo: enviar os pacotes de dados Multicast upstream para a porta de roteamento.

INTELBRAS_config#ip igmp-snooping forward-l3-to-mrouter

44.5. Política de encaminhamento

Descrição: o comando **igmp-snooping policy** é usado para definir a lista de IP ACL detectada pelo igmp-snooping, adicionando a tabela de encaminhamento dos endereços Multicast.

Sintaxe: **ip igmp-snooping policy** word
no ip igmp-snooping policy

Parâmetro:

- **word:** especifica o nome do IP ACL.

Modo de comando: Global Configuration.

Exemplo: detectar o IP ACL cujo o nome é 123, adicionando a tabela de IP Multicast.

INTELBRAS_config#ip igmp-snooping policy 123

44.6. Política DLF

Descrição: o comando **igmp-snooping dlf-drop** é usado para descartar os pacotes cujos os endereços Multicast de destino não estão mapeados tabela criada pelo IGMP Snooping.

Sintaxe: **ip igmp-snooping dlf-drop**
no ip igmp-snooping dlf-drop

Modo de comando: Global Configuration.

Exemplo: comando para descartar os pacotes que os endereços Multicast não estão registrados.

INTELBRAS_config#ip igmp-snooping dlf-drop

44.7. Tempo de vida do querier

Descrição: o comando **ip igmp-snooping timer router-age** é usado para configurar o tempo de vida do querier, indicando se o mesmo existe ou não para o IGMP. Por padrão, seu valor é de *260 segundos*.

Sintaxe: **ip igmp-snooping timer router-age** *time_value*
no ip igmp-snooping timer router-age

Parâmetro:

» **time_value:** especifica o tempo de vida da função.

Modo de comando: Global Configuration.

Exemplo: altere o tempo de vida da função para 300 segundos.

INTELBRAS_config#ip igmp-snooping timer router-age 300

44.8. Tempo de espera

Descrição: o comando **ip igmp-snooping timer response-time** é usado para configurar o tempo máximo de resposta do host a uma query multicast. Se não há resposta até o tempo de espera configurado o switch irá deletar o endereço da sua tabela IGMP. Por padrão este tempo é de *15 segundos*.

Sintaxe: **ip igmp-snooping timer response-time** *time_value*
no ip igmp-snooping timer response-time

Parâmetro:

» **time_value (1-2000000000):** estabelece o tempo máxima de resposta.

Modo de comando: Global Configuration.

Exemplo: altere o tempo máximo de resposta da função para 20 segundos.

INTELBRAS_config#ip igmp-snooping timer response-time 20

44.9. Querier

Descrição: o comando **igmp-snooping querier** envia mensagens de consulta, para descobrir quais dispositivos de rede são membros de um determinado grupo de multicast.

Sintaxe: **ip igmp-snooping querier** [address <*ip_addr*>]
no ip igmp-snooping querier [address]

Parâmetro:

» **ip_addr:** endereço de IP de origem do pacote.

Modo de comando: Global Configuration.

Exemplo: ative a função Igmp-snooping querier.

INTELBRAS_config#ip igmp-snooping querier

44.10. Transmissão de querys

Descrição: o comando **igmp-snooping querier querier-timer** configura o intervalo de encaminhamento de querys.Por padrão, este intervalo é de *200 segundos*.

Sintaxe: **ip igmp-snooping querier querier-timer** *time_value*
no ip igmp-snooping querier querier-timer

Parâmetro:

» **time_value:** estabelece o intervalo de tempo de encaminhamento de pacotes.

Modo de comando: Global Configuration.

Exemplo: altere o intervalo de tempo dos pacotes para 140 segundos.

INTELBRAS_config#ip igmp-snooping querier querier-timer 140

44.11. Modo *Sensitive*

Descrição: o comando **igmp-snooping sensitive** é usado para modificar a o tempo de vida dos pacotes da rota estabelecida na porta que está com o mrouter (porta de roteamento de endeço Multicast).

Sintaxe: **ip igmp-snooping sensitive [value** int**]**
no ip igmp-snooping sensitive [value]

Parâmetro:

» **int (3-30):** estabelece o tempo de vida da rota configurada na porta de roteamento de endereços Multicast.

Modo de comando: Global Configuration.

Exemplo: o exemplo a seguir mostra como ativar esta função e definir o tempo em que a rota ficará ativa, na porta de roteamento de endereços Multicast.

INTELBRAS_config#ip igmp-snooping sensitive

INTELBRAS_config#ip igmp-snooping sensitive value 10

44.12. V3 Leave check

Descrição: o comando **igmp-snooping v3-leave-check** é usado para enviar os pacotes de consulta especiais após o recebimento do pacote de saída v3.

Sintaxe: **ip igmp-snooping v3-leave-check**
no ip igmp-snooping v3-leave-check

Modo de comando: Global Configuration.

Exemplo: o exemplo a seguir mostra como ativar o IGMP v3-leave-check e enviar o pacote de consulta especial após o recebimento do pacote de licença v3.

INTELBRAS_config#ip igmp-snooping v3-leave-check

44.13. Encaminhamento para L2

Descrição: através do comando **igmp-snooping forward-wrongiif-within-vlan**, os pacotes multicast que foram recebidos na interface VLAN errada serão enviados para as portas físicas da VLAN.

Sintaxe: **ip igmp-snooping forward-wrongiif-within-vlan**
no ip igmp-snooping forward-wrongiif-within-vlan

Exemplo: o exemplo a seguir mostra como enviar os pacotes Multicast para as portas físicas vinculadas a VLAN.

Modo de comando: Global Configuration.

INTELBRAS_config#ip igmp-snooping forward-wrongiif-within-vlan

44.14. Endereços por porta

Descrição: o comando **igmp-snooping limit** é usado para configurar o número máximo de endereços IP multicast na porta do IGMP-snooping, estimando os grupos aplicados atingiram o número de configuração quando a IGMP-snooping gerar uma tabela de encaminhamento. Caso contrário, porta não será mais inserida nesta tabela.

Sintaxe: **ip igmp-snooping limit** *value*
no ip igmp-snooping limit

Parâmetro:

» **value (1-2048):** estabelece o número máximo de IPs Multicast.

Modo de comando: configuração de porta.

Exemplo: o exemplo a seguir mostra como definir o número máximo de Ips Multicast.

INTELBRAS_config_f0/1#ip igmp-snooping limit 1000

44.15. Informações

Descrição: o comando **show ip igmp-snooping** é usado para visualizar as configurações da função *Igmp-snooping*.

Sintaxe: **show ip igmp-snooping**
show ip igmp-snooping timer | groups | statistics

Parâmetros:

- **timer:** exibe as informações de tempo.
- **groups:** exibe as informações de grupos.
- **statistics:** exibes as informações de estatísticas.

Modo de comando: Global Configuration.

Exemplo: o exemplo a seguir mostra como exibir cada VLAN onde o snooping IGMP está sendo executado.

INTELBRAS_config#show ip igmp-snooping

44.16. Depuração

Descrição: o comando **debug ip igmp-snooping** é usado para habilitar e desabilitar a depuração da função *Igmp-snooping*.

Sintaxe: **debug ip igmp-snooping** packet | timer | event | error
no debug ip igmp-snooping packet | timer | event | error

Parâmetro:

- **packet:** depuração dos pacotes.
- **timer:** depuração dos cronômetros.
- **event:** depuração dos eventos.
- **error:** depuração de erros.

Modo de comando: Privileged EXEC.

Exemplo: habilitar a depuração dos pacotes da função *Igmp-snooping*.

INTELBRAS#debug ip igmp-snooping packet

45. DHCP snooping

Descrição: o comando **ip dhcp-relay snooping** é utilizado para habilitar a função de *DHCP snooping*. Com a função de *DHCP snooping* habilitada o switch irá analisar os pacotes DHCP recebidos e irá formar vínculos IP-MAC-Porta (IMPB) que serão utilizados pelas funções de Inspeção ARP e Inspeção IP de Origem.

Obs.: *se o DHCP snooping não estiver habilitado as configurações de Inspeção ARP, Inspeção IP de Origem e VLAN DHCP snooping não terão efeito.*

Sintaxe: **ip dhcp-relay snooping**
no ip dhcp-relay snooping

Modo de comando: Global Configuration.

Exemplo: habilite o DHCP snooping.

INTELBRAS_config#ip dhcp-relay snooping

45.1. Desabilitar DHCP snooping

Descrição: o comando **dhcp snooping deny** é utilizado para desabilitar o DHCP snooping em uma interface.

Sintaxe: **dhcp snooping deny**
no dhcp snooping deny

Modo de comando: interface de configuração Ethernet.

Exemplo: desabilite as funções de DHCP snooping na interface GigaEthernet 1.

INTELBRAS_config_f0/1#ip dhcp snooping deny

45.2. VLAN DHCP snooping

Descrição: o comando **ip dhcp-relay snooping vlan** é utilizado para definir quais VLANs serão monitoradas pelo DHCP snooping. Nas VLANs monitoradas pelo DHCP snooping os pacotes de oferta DHCP só serão recebidos por portas com o modo de confiança DHCP configurado como *Confiável*.

Sintaxe: **ip dhcp-relay snooping vlan** *intervalo_vlan*
ip dhcp-relay snooping vlan *intervalo_vlan* max-client (0-65535)

no ip dhcp-relay snooping vlan *intervalo_vlan*
no ip dhcp-relay snooping vlan *intervalo_vlan* max-client

Parâmetros:

» **intervalo_vlan:** intervalo de IDs das VLANs que serão monitoradas.
» **max-client (0-65535):** número máximo de clientes DHCP na VLAN.

Modo de comando: Global Configuration.

Exemplo: habilite o DHCP snooping nas VLANs 1 a 5 com um numero máximo de clientes de 50.

INTELBRAS_config#ip dhcp-relay snooping vlan 1-5 max-client 50

45.3. VLAN inspeção IP de origem

Descrição: o comando **ip verify source vlan** é utilizado para definir quais VLANs irão verificar o IP de origem dos pacotes. Se o endereço IP e o endereço MAC de origem não combinarem com o vínculo criado pelo DHCP snooping o pacote recebido pela porta será descartado.

Obs.: *as interfaces com o modo de confiança de IP de origem configurado como* Confiável *não terão seus pacotes IP inspecionados.*

Sintaxe: **ip verify source vlan** *intervalo_vlan*
no ip verify source vlan *intervalo_vlan*

Parâmetros:

» **intervalo_vlan:** intervalo de IDs das VLANs que serão monitoradas.

Modo de comando: Global Configuration.

Exemplo: habilite a verificação do IP de origem nas interfaces da VLAN 1 a 5.

INTELBRAS_config#ip verify source vlan 1-5

45.4. VLAN inspeção ARP

Descrição: o comando **ip arp inspection vlan** é utilizado para definir quais VLANs irão verificar o IP de origem dos pacotes ARP. Se o endereço IP e o endereço MAC de origem não combinarem com o vínculo criado pelo DHCP snooping o pacote ARP recebido pela porta será descartado.

Obs.: *as interfaces com o modo de confiança ARP configurado como* Confiável *não terão seus pacotes ARP inspecionados.*

Sintaxe: **ip arp inspection vlan** *intervalo_vlan*
no ip arp inspection vlan *intervalo_vlan*

Parâmetros:

» **intervalo_vlan:** intervalo de IDs das VLANs que serão monitoradas.

Modo de comando: Global Configuration.

Exemplo: habilite a verificação do IP de origem dos pacotes ARP recebidos por todas as interfaces da VLAN 1 a 5.

INTELBRAS_config#ip arp inspection vlan 1-5

45.5. Atualização rápida de vínculos

Descrição: o comando **ip dhcp-relay snooping rapid-refresh-bind** é utilizado para habilitar a atualização rápida de vínculos. Com esta função habilitada é possível mudar um cliente DHCP de porta sem ter que esperar o tempo de expiração do seu vínculo criado anteriormente, ou seja, quando a conexão for trocada o vínculo será atualizado e a solicitação DHCP não será tratada como ilegal.

Sintaxe: **ip dhcp-relay snooping rapid-refresh-bind**
no ip dhcp-relay snooping rapid-refresh-bind

Modo de comando: Global Configuration.

Exemplo: habilite a atualização rápida de vínculos IMPB.

INTELBRAS_config#ip dhcp-relay snooping rapid-refresh-bind

45.6. Vínculo manual

Descrição: o comando **ip source bindign** é utilizado para configurar um vínculo IMPB manualmente.

Sintaxe: **ip source bindign** *endereço_mac endereço_ip* interface GigaEthernet
ip source bindign *endereço_mac endereço_ip* interface GigaEthernet vlan (1-4094)
no ip source bindign *endereço_mac endereço_ip* vlan (1-4094)

Parâmetros:

» **endereço_mac:** endereço MAC do vínculo a ser criado no formato *XX.XX.XX.XX.XX.XX*.
» **endereço_ip:** endereço IPv4 do vínculo a ser criado.
» **interface GigaEthernet:** porta do vínculo a ser criado.
» **vlan 0/(1-4094):** VLAN do vínculo a ser criado.

Modo de comando: Global Configuration.

Exemplo: crie o vínculo IMPB do IP 192.168.0.1 com o MAC 01:02:03:04:05:06 e com a porta GigaEthernet 1 na VLAN 2.

INTELBRAS_config#ip source binding 01:02:03:04:05:06 192.168.0.1 interface GigaEthernet 0/1 vlan 2

45.7. Servidor de backup

Descrição: o comando **ip dhcp-relay snooping database-agent** é utilizado para configurar um servidor que receberá via TFTP o arquivo de backup do DHCP snooping.

Sintaxe: **ip dhcp-relay snooping database-agent** *endereço_ip*
no ip dhcp-relay snooping database-agent *endereço_ip*

Parâmetros:

» **endereço_ip:** endereço IPv4 do servidor TFTP.

Modo de comando: Global Configuration.

Exemplo: configure o cliente 192.168.0.100 para receber o arquivo de backup do DHCP snooping.

INTELBRAS_config#ip dhcp-relay snooping database-agent 192.168.0.100

45.8. Backup de dados

Descrição: o comando **ip dhcp-relay snooping db-file** é utilizado para configurar um arquivo de backup com os dados de vínculos IMPB criados através do DHCP snooping. Para que o arquivo backup seja criado é necessário ter configurado um servidor para o mesmo.

Sintaxe: **ip dhcp-relay snooping db-file** *nome_do_arquivo*
ip dhcp-relay snooping *nome_do_arquivo* timestamp
no ip dhcp-relay snooping
no ip dhcp-relay snooping timestamp

Parâmetros:

» **nome_do_arquivo:** nome do arquivo que será criado para guardar os dados.
» **timestamp:** configura a utilização de Timestamp para o arquivo.

Modo de comando: Global Configuration.

Exemplo: configure o arquivo "dhcp_snooping_db.txt" para servir como backup dos dados de DHCP snooping.

INTELBRAS_config#ip dhcp-relay snooping db-file dhcp_snooping_db.txt

Intervalo de atualização do backup

Descrição: o comando **ip dhcp-relay snooping write-time** é utilizado para configurar o intervalo de atualização do arquivo de backup do DHCP snooping.

Sintaxe: **ip dhcp-relay snooping write-time** (2-1440)
no ip dhcp-relay snooping write-time

Parâmetros:

» **(2-1440):** tempo de atualização em unidade de minuto.

Modo de comando: Global Configuration.

Exemplo: configure o tempo de atualização do arquivo de backup dos vínculos de DHCP snooping para 5 minutos.

INTELBRAS_config#ip dhcp-relay snooping write-time 5

Atualização imediata do backup

Descrição: o comando **ip dhcp-relay snooping write-immediately** é utilizado para definir a atualização imediata do arquivo de backup do DHCP snooping quando houver uma mudança nos vínculos criados.

Sintaxe: **ip dhcp-relay snooping write-immediately**
no ip dhcp-relay snooping write-immediately

Modo de comando: Global Configuration.

Exemplo: configure a atualização imediata do arquivo backup de DHCP snooping.

INTELBRAS_config#ip dhcp-relay snooping write-immediately

45.9. Log

Descrição: o comando **ip dhcp-relay snooping log** é utilizado para habilitar o registro de eventos de DHCP snooping. Quando habilitada esta função o Syslog irá reportar se pacotes de servidor DHCP estão sendo recebidos numa porta configurada como *Não confiável*, o que indicaria a existência de um servidor DHCP ilegal na porta.

Sintaxe: **ip dhcp-relay snooping log**
no ip dhcp-relay snooping log

Modo de comando: Global Configuration.

Exemplo: habilite o registro de eventos de DHCP snooping.

45.10. INTELBRAS_config#ip dhcp-relay snooping log Modo de confiança DHCP

Descrição: o comando **dhcp snooping trust** é utilizado para configurar o modo de confiança DHCP das interfaces. O comando descrito acima configura a interface no modo *Confiável* e o comando precedido do parâmetro no configura a interface no modo *Não confiável*.

Sintaxe: **dhcp snooping trust**
no dhcp snooping trust

Modo de comando: interface de configuração Ethernet.

Exemplo: configure o modo de confiança DHCP da interface GigaEthernet 1 como confiável.

INTELBRAS_config_f0/1#dhcp snooping trust

45.11. Modo de confiança ARP

Descrição: o comando **arp inspection trust** é utilizado para configurar o modo de confiança ARP das interfaces. O comando descrito acima configura a interface no modo *Confiável* e o comando precedido do parâmetro no configura a interface no modo *Não confiável*.

Sintaxe: **arp inspection trust**
no arp inspection trust

Modo de comando: interface de configuração Ethernet.

Exemplo: configure o modo de confiança ARP da interface GigaEthernet 1 como Confiável.

INTELBRAS_config_f0/1#arp inspection trust

45.12. Modo de confiança IP de origem

Descrição: o comando **ip-source trust** é utilizado para configurar o modo de confiança de IP de Origem das interfaces. O comando descrito acima configura a interface no modo *Confiável* e o comando precedido do parâmetro no configura a interface no modo *Não confiável*.

Sintaxe: **ip-source trust**
no ip-source trust

Modo de comando: interface de configuração Ethernet.

Exemplo: habilite o registro de eventos de DHCP snooping.

INTELBRAS_config#ip-source trust

45.13. Informações

Descrição: o comando **show ip dhcp-relay snooping** é utilizado para exibir informações de DHCP snooping.

Sintaxe: s**how ip dhcp-relay** snooping | binding

- » **snooping:** exibe informações de DHCP snooping.
- » **event:** exibe informações de vínculos.

Modo de comando: Privileged EXEC.

Exemplo: exiba as informações de DHCP snooping.

INTELBRAS#show ip dhcp-relay snooping

45.14. Depuração

Descrição: o comando **debug ip dhcp-relay** para habilitar a depuração das funções de DHCP Relay.

Sintaxe: **debug ip dhcp-relay** snooping | event | binding
no debug ip dhcp-relay snooping | event | binding

Parâmetros:

- » **snooping:** depuração de DHCP snooping.
- » **event:** depuração de eventos.
- » **binding:** depuração de vínculos.

Modo de comando: Privileged EXEC.

Exemplo: habilite a depuração de DHCP snooping.

INTELBRAS#debug ip dhcp-relay snooping

46. DHCP option 82

Descrição: o comando **ip dhcp-relay information option** é utilizado para habilitar a inclusão da Option 82 nos pacotes de requisição DHCP recebidos quando o switch estiver com o DHCP snooping ativado.

Sintaxe: **ip dhcp-relay snooping information option**
no ip dhcp-relay snooping information option

Modo de comando: Global Configuration.

Exemplo: habilite a inclusão da Option 82 nos pacotes DHCP recebidos.

INTELBRAS_config#ip dhcp-relay snooping information option

46.1. Formato option 82

Descrição: o comando **ip dhcp-relay snooping information option format** é utilizado para configurar o formato dos dados Option 82.

Sintaxe: **ip dhcp-relay snooping information option** format snmp-ifindex | hn-type | cm-type | hw-type | manual | snmp-ifindex
n**o ip dhcp-relay snooping information option** format snmp-ifindex | hn-type | cm-type | hw-type | manual | snmp-ifindex

Parâmetros:

- » **snmp-ifindex:** formato *ifindex SNMP*.
- » **hn-type:** formato *Cisco®*.
- » **cm-type:** formato *cm-type.*
- » **hw-type:** formato *hw-type.*
- » **manual:** formato *Manual*. O formato *Manual* é o especificado no comando *dhcp snooping information* de cada interface.

Modo de comando: Global Configuration.

Exemplo: configure a formatação dos dados Option 82 como manual.

INTELBRAS_config#ip dhcp-relay snooping information option format manual

46.2. Descartar

Descrição: o comando **dhcp snooping information drop** é utilizado para descartar os pacotes DHCP recebidos numa interface com a Options 82.

Sintaxe: **dhcp snooping information drop**
no dhcp snooping information drop

Modo de comando: Interface Configuration.

Exemplo: configura a interface GigaEthernet 1 para descartar os pacotes recebidos com a Option 82.

INTELBRAS_config#dhcp snooping information drop

46.3. Substituir

Descrição: o comando **dhcp snooping information replace** é utilizado para substituir a Options 82 e encaminhar o pacote DHCP.

Sintaxe: **dhcp snooping information drop**
no dhcp snooping information drop

Modo de comando: Interface Configuration.

Exemplo: configura a interface GigaEthernet 1 para descartar os pacotes recebidos com a Option 82.

INTELBRAS_config#dhcp snooping information drop

46.4. Encaminhar

Descrição: o comando **dhcp snooping information transmit** é utilizado para encaminhar o pacote DHCP sem alterações.

Sintaxe: **dhcp snooping information drop**
no dhcp snooping information drop

Modo de comando: Interface Configuration.

Exemplo: configura a interface GigaEthernet 1 para descartar os pacotes recebidos com a Option 82.

INTELBRAS_config#dhcp snooping information drop

46.5. Circuit-ID

Descrição: o comando **ip dhcp-relay snooping information type circuit_id** é utilizado para configurar o identificador de circuito da Option 82 representado pela subopção *Circuit-ID*.

Sintaxe: **ip dhcp-relay snooping information type circuit_id** hostname | port | vlan

Parâmetros:

- **hostname:** será incluído o nome do switch.
- **port:** será incluído a porta de ingresso da requisição DHCP.
- **vlan:** será incluído a VLAN de ingresso da requisição DHCP.

Modo de comando: Global Configuration.

Exemplo: inclua as informações de hostname, porta e VLAN na subopção *Circuit-ID*.

INTELBRAS_config#ip dhcp-relay snooping information type circuit-id hostname port vlan

46.6. Remote-ID

Descrição: o comando **ip dhcp-relay snooping information type remote-id** é utilizado para configurar o identificador remoto da Option 82 representado pela subopção *Remote-ID*.

Sintaxe: i**p dhcp-relay snooping snooping information type remote-id** cliente-mac | switch-mac | palavra

Parâmetros:

- **client_mac:** o endereço MAC do cliente será o identificador do dispositivo que originou a requisição DHCP.
- **switch-mac:** o endereço MAC do switch será o identificador do dispositivo que originou a requisição DHCP.
- **palavra:** identificador do dispositivo que originou a requisição DHCP.

Modo de comando: Global Configuration.

Exemplo: defina o identificador remoto da Option 82 como o endereço MAC do cliente DHCP.

INTELBRAS_config#ip dhcp-relay snooping snooping information type remote-id client-mac

46.7. Vendor-Specific

Descrição: o comando **dhcp snooping information append** é utilizado para configurar a subopção *vendor-specific* da Option 82.

Obs.: *o comando sem parâmetros apenas habilita a inclusão da subopção.*

Sintaxe: **dhcp snooping information append**
dhcp snooping information append first-subop9-param | second-subop9-param hex *palavra_hexadecimal*
dhcp snooping information append first-subop9-param | second-subop9-param hostname | vlanip

Parâmetros:

- **first-subop9-param:** configura o primeiro parâmetro da subopção *vendor-specific*.
- **second-subop9-param:** configura o segundo parâmetro da subopção *vendor-specific*.
- **hostname:** atribui o nome do switch a um parâmetro.
- **vlanip:** atribui a VLAN ID da porta a um parâmetro.
- **hex palavra_hexadecimal:** atribui uma palavra em hexadecimal a um parâmetro.

Modo de comando: Interface Configuration.

Exemplo: atribua o hostname ao primeiro parâmetro da subopção *vendor-specifc*.

INTELBRAS_config#dhcp snooping information append first-subop9-param hostname

46.8. Formato subopções Option 82

Descrição: o comando **dhcp snooping information** é utilizado para configurar a informações das subopções da Option 82 nos pacotes DHCP.

Sintaxe: **dhcp snooping information** circuit-id | remote-id | vendor-specific string palavra
dhcp snooping information circuit-id | remote-id | vendor-specific hex palavra_hexadecimal

Parâmetros:

- **circuit-id:** define o formato da subopção *Circuit-ID*.
- **remote-id:** define o formato da subopção *Remotet-ID*.
- **vendor-specific:** define o formato da subopção *vendor-specific*.
- **string *palavra*:** palavra carregada pela subopção.
- **hex *palavra_hexadecimal*:** palavra carregada no formato hexadecimal.

Modo de comando: interface de configuração Ethernet.

Exemplo: configure manualmente a subopção *Circuit-ID* como *SALA_A* para a interface GigaEthernet 1.

INTELBRAS_config#dhcp snooping information circuit-d string SALA_A

47. Encaminhamento forçado de MAC (MACFF)

Descrição: o comando **macff enable** é utilizado para habilitar o encaminhamento forçado de MAC.

Sintaxe: **macff enable**
no macff enable

Modo de comando: Global Configuration.

Exemplo: habilite o encaminhamento forçado de MAC.

INTELBRAS_config#macff enable

47.1. VLAN MACFF

Descrição: o comando **macff vlan** é utilizado para habilitar e configurar o encaminhamento forçado de MAC em uma determinada VLAN.

Sintaxe: **macff vlan** *vlan_range* enable
macff vlan default-ar | other-ar *endereço_ip*
no macff vlan *intervalo_vlan* enable
no macff vlan default-ar | other-ar *endereço_ip*

Parâmetros:

- **intervalo_vlan:** intervalo de IDs de VLAN.
- **enable:** habilita o encaminhamento forçado de MAC nas VLANs especificadas.
- **default-ar:** configura o gateway padrão para o intervalo VLAN especificado.
- **other-ar:** configura o outro gateway, além do padrão, para o intervalo VLAN especificado.

Modo de comando: Global Configuration.

Exemplo: habilite o encaminhamento forçado de MAC nas VLAN 1 a 5.

INTELBRAS_config#macff vlan 1-5 enable

Exemplo: configure o gateway padrão 192.168.0.254 para as VLANs 1 a 5.

INTELBRAS_config#macff vlan 1-5 default-ar 192.168.0.254

47.2. Desabilitar

Descrição: o comando **macff disable** é utilizado para desabilitar o aprendizado forçado de MAC em uma porta.

Sintaxe: **macff disable**
no macff disable

Modo de comando: interface de configuração Ethernet.

Exemplo: desabilite o encaminhamento forçado de MAC na porta 1.

INTELBRAS_config_f0/1#macff disable

47.3. Depuração

Descrição: o comando **macff debug** é utilizado para habilitar a depuração do MACFF.

Sintaxe: **macff debug**
no macff debug

Modo de comando: Global Configuration.

Exemplo: habilite a depuração MACFF.

INTELBRAS_config#macff debug

48. Protocolo de túnel L2

Descrição: o comando **l2protocol-tunnel** é utilizado para habilitar o protocolo de túnel L2 em uma porta do switch. Com o protocolo de túnel L2 habilitado na porta os pacotes referentes a protocolos de L2, como o STP, não serão processados pelo switch.

Obs.: *o único protocolo que o switch suporta o tunelamento é o STP.*

Sintaxe: **l2protocol-tunnel**
no l2protocol-tunnel

Modo de comando: interface de configuração Ethernet.

Exemplo: habilite o protocolo de túnel L2 na interface GigaEthernet 1.

INTELBRAS_config_f0/1#l2protocol-tunnel

49. Loopback detection

Descrição: o comando **loopback detection** é utilizado para habilitar globalmente a detecção de loop nas portas do switch.

Sintaxe: **loopback detection**
no loopback detection

Modo de comando: Global Configuration.

Exemplo: habilite globalmente o loopback detection.

INTELBRAS_config#loopback detection

49.1. Portas loopback detection

Descrição: o comando **loopback detection enable** é utilizado para habilitar a detecção de loop em uma porta específica do switch.

Sintaxe: **loopback detection enable**
no loopback detection enable

Modo de comando: interface de configuração Ethernet.

Exemplo: habilite o loopback detection na interface GigaEthernet 1.

INTELBRAS_config_f0/1#loopback detection enable

49.2. VLAN loopback detection

Descrição: o comando **loopback detection vlan-control** é utilizado para habilitar o Loopback Detection em VLANs específicas.

Sintaxe: **loopback detection vlan-control** *intervalo_vlan*
no loopback detection vlan-control *intervalo_vlan*

Modo de comando: Global Configuration.

Parâmetros:

» **intervalo_vlan:** intervalo de IDs de VLAN.

Exemplo: habilite o loopback detection nas VLANs 1 a 5.

INTELBRAS_config#loopback detection vlan-control 1-5

49.3. Período de transmissão

Descrição: o comando **loopback detection hello-time** é utilizado para configurar o intervalo de transmissão de pacotes de Loopback Detection.

Sintaxe: **loopback detection hello-time** (3-65535)
no loopback detection hello-time

Modo de comando: Interface Configuration.

Parâmetros:

» **(3-65535):** período de transmissão em unidade de segundo.

Exemplo: configure o período de transmissão de pacotes Loopback Detection para 5 segundos na interface GigaEthernet 1.

INTELBRAS_config_f0/1#loopback detection hello-time 5

49.4. Controle das portas

Descrição: o comando **loopback detection control** é utilizado para configurar a ação de controle realizada numa porta quando é detectado o estado de loop na mesma pelo Loopback Detection.

Sintaxe: **loopback detection control** block | learning | shutdown
no loopback detection control

Modo de comando: interface de configuração Ethernet.

Parâmetros:

» **block:** a porta será bloqueada.

» **learning:** a porta não aprenderá endereços MAC.

» **shutdown:** a porta será desativada.

Exemplo: configure a ação de controle da porta como desativar.

INTELBRAS_config_f0/1#loopback detection control shutdown

49.5. Tempo de recuperação

Descrição: o comando **loopback detection recovery-time** é utilizado para configurar o tempo de recuperação de uma porta após a mesma ter sido controlada pelo Loopback Detection.

Sintaxe: **loopback detection recovery-time** (3-65535)
no loopback detection recovery-time

Modo de comando: interface de configuração Ethernet.

Parâmetros:

» **(10-65535):** tempo de recuperação em unidades de segundo.

Exemplo: configure o período de transmissão de pacotes Loopback Detection para 5 segundos na interface GigaEthernet 1.

INTELBRAS_config_f0/1#loopback detection hello-time 5

49.6. MAC de destino

Descrição: o comando loopback **detection dest-mac** é utilizado para configurar o endereço MAC de destino dos pacotes de Loopback Detection de uma porta.

Sintaxe: **loopback detection dest-mac** *endereço_mac*
no loopback detection dest-mac

Modo de comando: interface de configuração Ethernet.

Parâmetros:

» **endereço_mac:** endereço MAC de 48 bits no formato *H.H.H.*

Exemplo: configure o endereço MAC de destino dos pacotes de Loopback Detection da interface GigaEthernet 1 para 1111. 1111. 1111.

INTELBRAS_config_f0/1#loopback detection dest-mac 1111. 1111. 1111.

49.7. Existência de loop

Descrição: o comando **loopback existence** é utilizado configurar manualmente a existência de loop na porta.

Sintaxe: **loopback existence**
no loopback existence

Modo de comando: interface de configuração Ethernet.

Exemplo: configure um loop na porta GigaEthernet 1.

INTELBRAS_config_f0/1#loopback detection existence

49.8. Threshold

Descrição: o comando **loopback detection frames-threshold** é utilizado configurar o threshold de pacotes de Loopback Detection recebidos pela porta em um minuto.

Sintaxe: **loopback detection frames-threshold** (10-200)
no loopback detection frames-threshold

Modo de comando: interface de configuração Ethernet.

Parâmetros:

» **(10-200):** valor configurado para o limite de pacotes antes de considerar como loop.

Exemplo: configure a porta GigaEthernet 1 com 200 pacotes como limite para loopback.

Switch_config_g0/1#loopback-detection frames-threshold 200

49.9. Contador de pacotes

Descrição: o comando **loopback detection frames-monitor** é utilizado habilitar o contador de pacotes de Loopback Detection.

Sintaxe: **loopback-detection frames-monitor**
no loopback-detection frames-monitor

Modo de comando: interface de configuração Ethernet.

Exemplo: habilite o contador de pacotes de Loopback Detection na porta GigaEthernet 1.

INTELBRAS_config_f0/1#loopback detection frames-monitor

49.10. Informações

Descrição: o comando **show loopback detection** é utilizado para exibir as configurações globais de Loopback Detection.

Sintaxe: **show loopback detection**

Modo de comando: Privileged EXEC mode.

Exemplo: exiba as configurações globais de Loopback Detection.

INTELBRAS#show loopback detection

49.11. Informações de portas

Descrição: o comando **show loopback detection interface** é utilizado para exibir as informações de porta de Loopback Detection.

Sintaxe: **show loopback detection interface** GigaEthernet

Modo de comando: Privileged EXEC mode.

Parâmetros:

» **GigaEthernet:** especificação da interface.

Exemplo: exiba as informações de Loopback Detection da porta GigaEthernet 1.

INTELBRAS#show loopback detection interface GigaEthernet 0/1

50. QoS

50.1. Priorização por porta

Descrição: o comando **cos default** é utilizado para configurar um valor CoS para um fluxo de dados baseado na sua porta de ingresso.

Obs.: *» Para que este comando tenha efeito é necessário que o modo de confiança QoS esteja configurado como* UNTRUSTED.
» Este comando pode ser executado globalmente ou em uma interface tendo seu efeito de acordo com o modo de comando.

Sintaxe: **cos default** (0-7)
no cos default

Parâmetros:

» **(0-7):** valor CoS.

Modo de comando: interface de configuração Ethernet. | GLOBAL configuration.

Exemplo: configure o valor de CoS 7 para fluxos recebidos na porta GigaEthernet 1.

INTELBRAS_config_f0/1#cos default 7

50.2. Mapeamento DSCP

Descrição: o comando dscp map é utilizado para mapear o valor DSCP para um valor CoS e também para substituir o campo DSCP de um fluxo de dados.

Obs.: *para que o mapeamento DSCP para CoS tenha efeito é necessário que o modo de confiança QoS esteja configurado como* TRUST DSCP.

Sintaxe: **dscp map** *intervalo_dscp* cos (0-7)
no dscp map *intervalo_dscp*

Parâmetros:

» **intervalo_dscp:** intervalo DSCP entre 0 e 63.
» **cos (0-7):** o valor DSCP será mapeado para um valor CoS.

Modo de comando: Global Configuration.

Exemplo: configure o valor de DSCP 50 para CoS 7 recebidos em todas as portas do switch.

INTELBRAS_config#dscp map 50 cos 7

50.3. Priorização CoS

Descrição: o comando **cos map** é utilizado para configurar a fila de prioridade de um tráfego baseado no seu valor de CoS.

Obs.: *o valor de CoS de um fluxo de dados pode ser obtido através do valor CoS no cabeçalho Ethernet do mesmo ou através do mapeamento DSCP para CoS e Porta para CoS, como explicado na sessão 50.4. Modo de confiança.*

Sintaxe: **cos map** (1-8) (0-7)
no cos map (1-8)
no cos map

Parâmetros:

» **(1-8):** fila de prioridade.
» **(0-7):** valor CoS.

Modo de comando: Global Configuration.

Exemplo: configure a fila de prioridade 8 para o valor de CoS 7 em todas as portas do switch.

INTELBRAS_config#cos map 8 7

50.4. Modo de confiança

Descrição: o comando **qos trust** é utilizado para configurar o modo de confiança QoS. O modo de confiança define como o valor de CoS de um tráfego será obtido.

Sintaxe: **qos trust** cos | dscp | untrust
no qos trust

Parâmetros:

» **cos:** através do seu próprio valor CoS contido no cabeçalho Ethernet.
» **dscp:** através do mapeamento do seu valor DSCP.
» **untrust:** através do mapeamento da sua porta de ingresso.

Modo de comando: Global Configuration.

Exemplo: configure o modo de confiança QoS para que os fluxos recebidos em todas as portas do switch sejam priorizados de acordo com o seu valor DSCP.

INTELBRAS_config#qos trust dscp

50.5. Fila de prioridade

Descrição: o comando **scheduler weight bandwidth** é utilizado para configurar o peso de uma fila de prioridade.

Obs.: *este comando pode ser executado globalmente ou em uma interface tendo seu efeito de acordo com o modo de comando.*

Sintaxe: **scheduler weight bandwidth** *peso_da_fila(1-8)*
no scheduler weight bandwidth

Parâmetros:

» **peso_da_fila(1-8):** valor entre 1 e 15 que determina o peso de uma determinada fila de prioridade. A especificação do peso das filas é feita sequencialmente e em ordem crescente.

Modo de comando: interface de configuração Ethernet. | Global Configuration.

Exemplo: configure o peso das filas de prioridade em todas as portas do switch de acordo com a tabela a seguir:

Fila	1	2	3	4	5	6	7	8
Peso	1	3	5	7	9	11	13	15

INTELBRAS_config#scheduler weight bandwidth 1 3 5 7 9 11 13 15

50.6. Algoritmo de balanceamento

Descrição: o comando **scheduler policy** é utilizado para configurar o algoritmo de balanceamento das filas de prioridade.

Obs.: *este comando pode ser executado globalmente ou em uma interface tendo seu efeito de acordo com o modo de comando.*

Sintaxe: **scheduler policy** sp | wrr | wfq | fcfs
no scheduler policy

Parâmetros:

- **sp:** configura o algoritmo Strict Priority.
- **wrr:** configura o algoritmo Weighted Round Robin.
- **wfq:** configura o algoritmo Weighted Fair Queuing.
- **fcfs:** configura o algoritmo First-Come-First-Served.

Modo de comando: interface de configuração Ethernet. | Global Configuration.

Exemplo: configure o algoritmo WRR para o balanceamento das filas de prioridade em todas as portas do switch.

INTELBRAS_config#scheduler policy wrr

50.7. Política de mapeamento

Descrição: o comando **policy map** é utilizado para criar uma política de mapeamento.

Sintaxe: **policy map** *nome*
no policy map *nome*

Parâmetros:

- **nome:** nome da política de mapeamento a ser configurada.

Modo de comando: Global Configuration.

Exemplo: crie a política "politicaQoS".

INTELBRAS_config#policy map politicaQoS

Aplicação

Descrição: o comando **qos policy** para aplicar uma política QoS globalmente ou em uma interface.

Obs.: *este comando pode ser executado globalmente ou em uma interface tendo seu efeito de acordo com o modo de comando.*

Sintaxe: **qos policy** *nome* ingress
no qos policy *nome*

Parâmetros:

- **nome:** nome da política de mapeamento.
- **ingress:** a política terá efeito no tráfego de ingresso.

Modo de comando: interface de configuração Ethernet. | Global Configuration.

Exemplo: aplique a política QoS *politicaQoS* globalmente.

INTELBRAS_config#qos policy politicaQoS

Descrição

Descrição: o comando **description** é utilizado para configurar a descrição da política criada.

Sintaxe: **description** *descrição*
no description *descrição*

Parâmetros:

» **descrição:** texto que descreve a política de mapeamento.

Modo de comando: QoS POLICY configuration.

Exemplo: atribua a descrição "Politica de QoS para o setor A" para uma política criada.

INTELBRAS-policy-map#description *Politica de QoS para o setor A*

Lista de comparação

Descrição: o comando **classify** é utilizado para configurar em quais fluxos a política criada será aplicada.

Sintaxe: **classify** *parâmetro valor*
no classify *parâmetro valor*

Parâmetros:

Na tabela a seguir são mostrados os parâmetros do comando *classify*, com estes é criado uma de uma lista com itens que são comparados com o fluxo recebido para que se o mesmo combinar com algum dos itens a política criada seja aplicada.

Parâmetro	Valor	Descrição
any	Não se aplica	Todos pacotes
cos	0 - 7	Valor CoS dos pacotes
icos	0 - 7	Valor CoS interno (QinQ)
vlan	1 - 4094	VLAN ID do pacote
ivlan	1 - 4094	VLAN ID interna (QinQ)
ether-type	0x0600 - 0xFFFF	Valor ether-type do pacote
precedence	0 - 7	Valor de precedência ToS do pacote
dscp	0 - 63	Valor DSCP do pacote
tos	0 - 15	Campos de latência, taxa de transferência, confiabilidade e custo no valor ToS do pacote
diffserv	0 - 255	Valor ToS do pacote
ip	*nome_acl_ip*	Nome da ALC-IP que o pacote combina
Ipv6	*nome_acl_ipv6*	Nome da ALC-IPv6 que o pacote combina
mac	*nome_acl_mac*	Nome da ALC-MAC que o pacote combina

Modo de comando: QoS POLICY Configuration.

Exemplo: configure a política criada para que a mesma seja aplicada a todos os pacotes com VLAN ID 10.

INTELBRAS-policy-map#classify vlan10

Lista de ações

Descrição: o comando **action** é utilizado para configurar uma lista de ações a serem tomadas para os fluxos em que a política criada for aplicada.

Sintaxe: **action** *parâmetro valor*
no action *parâmetro valor*

Parâmetros:

Parâmetro	Valor	Descrição
bandwidth	1 - 163840	Limita a banda em unidades de 64 kbps
cos	0 – 7	Substitui a prioridade VLAN
drop		Descarta os pacotes
dscp	0 – 63	Substitui o valor DSCP
Precedence	0 – 7	Substitui o valor de precedência ToS
forward		Encaminha os pacotes

Parâmetro	Valor	Descrição
icos	0 - 7	Substitui valor CoS interno (QinQ)
ivlan	1 – 4094	Substitui VLAN ID interna (QinQ)
monitor	1 – 4	Espelha o pacote para uma porta de destino configurada numa sessão de espelhamento
quequ	1 - 8	Mapeia para uma fila de prioridade
redirect	*interface_id*	Redireciona o pacote
stat-packet		Conta a quantidade de pacotes
stat-byte		Conta a quantidade de bytes
vlanID	*vlan_id*	Substitui a VLAN ID
copy-to-cpu		Encaminha para a CPU

Modo de comando: QoS POLICY configuration.

Exemplo: configure a política criada para que limite a banda dos fluxos para 640 kbps.

INTELBRAS-policy-map#action bandwidth 10

Exibir informações

Descrição: o comando **show policy map** é utilizado para exibir as informações das políticas de QoS.

Sintaxe: **show policy map**
show policy map n*ome_da_política*

Parâmetros:

» **nome_da_política:** especifica uma política de QoS.

Modo de comando: Privileged EXEC mode.

Exemplo: exiba as informações de Loopback Detection da porta GigaEthernet 1.

INTELBRAS#show policy-map

policy-map 1

classify any

action redirect g0/1

51. Denial of Service (DoS)

Descrição: o comando **dos enable** é utilizado para habilitar as funções de DoS.

Sintaxe: **dos enable parâmetro** *valor*
no dos enable *parâmetro*

Parâmetro	Valor	Descrição
all		Previne contra todos os tipos de ataques
icmp	0-1023	Descarta pacotes icmp com comprimento maior que o especificado em unidades de bytes
ip		Descarta pacotes com endereço IP de origem igual ao endereço IP de destino
l4port		Descarta pacotes com porta TCP/UDP de origem igual a porta TCP/UDP de destino
mac		Descarta pacotes com endereço MAC de origem igual ao endereço MAC de destino
tcpflags		Descarta pacotes com flags TCP ilegais
tcpfrag	0-31	Descarta pacotes TCP fragmentados com cabeçalho de comprimento menor que o especificado em unidades de bytes
tcpsmurf		Descarta pacotes TCP com endereços de destino broadcast

icmpsmurf	Descarta pacotes ICMP com endereços de destino broadcast
ipsmurf	Descarta pacotes IP com endereços de destino broadcast

Modo de comando: Global Configuration.

Exemplo: habilite todas as funções de DoS.

INTELBRAS_config#dos enable all

51.1. Informações

Descrição: o comando **show dos** é utilizado para exibir as configurações de DoS do sistema.

Sintaxe: **show dos**

Modo de comando: Privileged EXEC mode.

Exemplo: exiba as configurações de DoS do sistema.

INTELBRAS#show dos

dos enable tcpfrag

52. Prevenção de ataques

Descrição: o comando **filter enable** é utilizado para habilitar a função de prevenção de ataques.

Sintaxe: **filter enable**
no filter enable

Exemplo: habilite a prevenção de ataques.

INTELBRAS_config#filter enable

52.1. Fluxos analisados

Descrição: o comando filter é utilizado para configurar quais tipos de fluxos serão analisados pela função de prevenção de ataques.

Sintaxe: **filter** icmp | icmpv6 | ip | igmp | dhcp | bpdu | arp
no filter icmp | icmpv6 | ip | igmp | dhcp | bpdu | arp

Parâmetros:

- **icmp:** habilita prevenção de ataque ICMP. Para ter efeito esta função deve ser habilitada globalmente e na interface desejada.
- **icmpv6:** habilita prevenção de ataque ICMPv6. Para ter efeito esta função deve ser habilitada globalmente e na interface desejada.
- **ip:** habilita prevenção de ataque IP. Para ter efeito esta função deve ser habilitada globalmente e na interface desejada.
- **igmp:** habilita prevenção de ataque IGMP. Esta função é habilitada globalmente.
- **dhcp:** habilita prevenção de ataque DHCP. Para ter efeito esta função deve ser habilitada globalmente e na interface desejada.
- **bpdu:** habilita prevenção de ataque BPDU. Esta função é habilitada na interface desejada.
- **arp:** habilita prevenção de ataque ARP. Esta função é habilitada na interface desejada.
- **Modo de comando:** interface de configuração Ethernet. | Global Configuration.

Exemplo: habilite a prevenção de ataque icmp na interface FastEthernet 1.

INTELBRAS_config#filter icmp

INTELBRAS_config#interface FastEthernet 0/1

INTELBRAS_config_f0/1#filter icmp

52.2. Modo

Descrição: o comando **filter mode** é utilizado para configurar o modo de prevenção de ataques.

Sintaxe: filter mode raw | hybrid

Parâmetros:

- **raw:** modo *Simples*. No modo *Simples*, após um fluxo ser considerado como ataque o switch irá bloquear todos os fluxos com a mesma origem até que o tempo de bloqueio acabe e então comece uma nova contagem.
- **hybrid:** modo *Avançado*. No modo *Avançado*, após um fluxo ser considerado como ataque o switch irá bloquear este único fluxo durante o tempo de bloqueio do modo *Avançado* e iniciará uma nova contagem de pacotes, se a contagem exceder o limite novamente o fluxo continuará bloqueado, caso contrário o bloqueio será retirado.

Exemplo: configure a operação do filtro de prevenção de ataques para o Modo *Simples*.

INTELBRAS_config#filter mode raw

52.3. Modo *Simples*

Período de contagem

Descrição: o comando **filter period** é utilizado para configurar o período de contagem de pacotes.

Sintaxe: **filter period** *(1-600)*
no filter period

Parâmetros:

- **(1-600):** período de tempo em unidades de segundo.

Modo de comando: Global Configuration.

Exemplo: configure o período de verificação de ataques em 5 segundos.

INTELBRAS_config#filter period 5

Threshold

Descrição: o comando **filter threshold** é utilizado para configurar a quantidade limite de pacotes recebidos dentro do período de contagem para que o sistema considere um ataque e bloqueie o fluxo.

Sintaxe: **filter threshold** icmp | icmpv6 | ip | igmp | dhcp | bpdu | arp *(5-2000)*
no filter threshold icmp | icmpv6 | ip | igmp | dhcp | bpdu | arp

Parâmetros:

- **icmp:** configura prevenção de ataque ICMP.
- **icmpv6:** configura prevenção de ataque ICMPv6.
- **ip:** configura prevenção de ataque IP.
- **igmp:** configura prevenção de ataque IGMP.
- **dhcp:** configura prevenção de ataque DHCP.
- **bpdu:** configura prevenção de ataque BPDU.
- **arp:** configura prevenção de ataque ARP.
- **(5-2000):** quantidade de pacotes para o gatilho da função de prevenção de ataque.

Modo de comando: Global Configuration.

Exemplo: configure a prevenção de ataque para que se considere ataque um fluxo de pacotes ARP superior a 500 pacotes recebidos dentro do período de contagem.

INTELBRAS_config#filter threshold arp 500

Tempo de bloqueio

Descrição: o comando **filter block-time** é utilizado para configurar o tempo de bloqueio de um fluxo após o mesmo ter sido considerado um ataque.

Sintaxe: **filter block-time** *(1-86400)*
no filter block-time

Parâmetros:

» **(1-86400):** tempo de bloqueio em unidades de segundo.

Modo de comando: Global Configuration.

Exemplo: configure o tempo de bloqueio da prevenção de ataque para 500 segundos.

INTELBRAS_config#filter block-time 500

52.4. Modo *Avançado*

Período de verificação

Descrição: o comando **filter polling period** é utilizado para configurar o período de verificação do Modo *Avançado*. O período de verificação corresponde ao período de contagem e o tempo de bloqueio do modo *Avançado*.

Sintaxe: **filter polling period** *(1-600)*
no filter polling period

Parâmetros:

» **(1-600):** período de tempo em unidades de segundo.

Modo de comando: Global Configuration.

Exemplo: configure o período de verificação de ataques em 5 segundos.

INTELBRAS_config#filter polling period 5

Threshold

Descrição: o comando **filter polling threshold** é utilizado para configurar a quantidade limite de pacotes recebidos dentro do período de verificação para que o sistema considere um ataque e bloqueie o fluxo durante um intervalo de tempo igual ao período de verificação.

Sintaxe: **filter polling threshold** icmp | icmpv6 | ip | igmp | dhcp | bpdu | arp (5-2000)
no filter polling threshold icmp | icmpv6 | ip | igmp | dhcp | bpdu | arp

Parâmetros:

» **icmp:** configura prevenção de ataque ICMP.
» **icmpv6:** configura prevenção de ataque ICMPv6.
» **ip:** configura prevenção de ataque IP.
» **igmp:** configura prevenção de ataque IGMP.
» **dhcp:** configura prevenção de ataque DHCP.
» **bpdu:** configura prevenção de ataque BPDU.
» **arp:** configura prevenção de ataque ARP.
» **(5-2000):** quantidade de pacotes para o gatilho da função de prevenção de ataque.

Modo de comando: Global Configuration.

Exemplo: configure o filtro de prevenção de ataque para que se considere ataque um fluxo de pacotes ARP superior a 500 pacotes recebidos dentro do período de verificação.

INTELBRAS_config#filter polling threshold arp 500

Configuração automática

Descrição: o comando **filter polling auto-fit** é utilizado para configurar o período de verificação e quantidade gatilho de pacotes do modo *Avançado* baseado nas configurações de período de contagem e quantidade gatilho de pacotes do modo *Simples*. O período de verificação será igual ao período de contagem e a quantidade gatilho de pacotes será ¾ da quantidade gatilho de pacotes do modo *Simples*.

Sintaxe: **filter polling auto-fit**
no filter polling auto-fit

Exemplo: configure as configurações do Modo *Avançado* automaticamente baseadas nas configurações do Modo *Simples*.

INTELBRAS_config#filter polling auto-fit

52.5. Informações

Descrição: o comando **show filter** é utilizado para exibir as informações de prevenção de ataques do sistema.

Sintaxe: **show filter**

Exemplo: exiba as informações de prevenção de ataques do sistema.

INTELBRAS_config#show filter

53. Network Time Protocol (NTP)

53.1. Cliente NTP

Descrição: o comando **ntp server** é utilizado para configurar um servidor NTP para o dispositivo poder obter serviço de sincronização de data e hora.

Sintaxe: **ntp server** *endereço_ip*
ntp server *endereço_ip* key *(1-4294967295)*
ntp server *endereço_ip* version *(1-4)*
ntp server *endereço_ip* key *(1-4294967295*) version *(1-4)*
no ntp server *endereço_ip*

Parâmetros:

- **endereço_ip:** endereço IPv4 ou IPv6 do servidor NTP.
- **key (1-4294967295):** define a chave de autenticação utilizada.
- **version (1-4):** define a versão NTP.

Modo de comando: Global Configuration.

Exemplo: configure o servidor NTP 10.0.0.1

INTELBRAS_config#ntp server 10.0.0.1

53.2. Servidor NTP

Descrição: o comando **ntp master** é utilizado para configurar o dispositivo como servidor NTP Mestre (stratum=1).

Obs.: *se o dispositivo não tiver configurado como cliente NTP é necessário configurar o servidor NTP Mestre Primário ou o dispositivo não será capaz de oferecer o serviço de sincronização.*

Sintaxe: **ntp master** primary | secondary
no ntp master

Parâmetros:

- **primary:** configura o dispositivo como servidor NTP Mestre Primário.
- **secondary:** configura o dispositivo como servidor NTP Mestre Secundário.

Modo de comando: Global Configuration.

Exemplo: configure o dispositivo como servidor NTP primário.

INTELBRAS_config#ntp master primary

Autenticação

Descrição: o comando ntp authentication é utilizado para configurar o serviço de autenticação NTP.

Sintaxe: **ntp authentication** enable
ntp authentication key *(1-4294967295)* md5 *senha*
ntp authentication trusted key *(1-4294967295)*
no ntp authentication key *(1-4294967295)*
no ntp authentication trusted key *(1-4294967295)*

Parâmetros:

- **enable:** habilita o serviço de autenticação.
- **key *(1-4294967295)*:** configura a chave de autenticação.

» **md5 senha:** configura a senha de autenticação referente a chave que está sendo configurada.
» **trusted key *(1-4294967295)*:** configura uma chave de autenticação como confiável.

Modo de comando: Global Configuration.

Exemplo: habilite o serviço de autenticação NTP, crie a chave 4956841 com a senha abc1234 e configure a mesma como confiável.

INTELBRAS_config#ntp authentication enable

INTELBRAS_config#ntp authentication key 4956841 md5 abc1234

INTELBRAS_config#ntp authentication trusted key 4956841

53.3. Par NTP

Descrição: o comando **ntp peer** é utilizado para configurar um par NTP para que os dispositivos possam sincronizar entre si suas informações de data e hora.

Obs.: *podem ser configurados até 3 servidores NTP.*

Sintaxe: **ntp peer** *endereço_ip*
ntp peer *endereço_ip* key *(1-4294967295)*
ntp peer *endereço_ip* version *(1-4)*
ntp peer *endereço_ip* key *(1-4294967295)* version *(1-4)*
no ntp peer *endereço_ip*

Parâmetros:

» **endereço_ip:** endereço IPv4 ou IPv6 do par NTP.
» **key (1-4294967295):** define a chave de autenticação utilizada.
» **version (1-4):** define a versão NTP.

Modo de comando: Global Configuration.

Exemplo: configure o par NTP 192.168.0.2

INTELBRAS_config#ntp peer 192.168.0.2

53.4. Informações

Descrição: o comando **show ntp** é utilizado para exibir as informações de NTP do sistema.

Sintaxe: **show ntp**
show ntp associations detail
show ntp status | associations | timers

Parâmetros:

» **associations:** exibe o status das associações.
» **timers:** exibe os status dos relógios.
» **status:** exibe o status NTP do sistema.
» **associations detail:** exibe o status detalhado das associações.

Modo de comando: Privileged EXEC mode.

Exemplo: exiba o status NTP do sistema.

INTELBRAS#show ntp status

53.5. Depuração

Descrição: o comando **debug ntp** é utilizado para configura a depuração NTP.

Sintaxe: **debug ntp** packet | event | error | all
no debug ntp

Parâmetros:

» **packet:** habilita a depuração dos pacotes.
» **event:** habilita a depuração dos eventos.
» **error:** habilita a depuração de erros.
» **all:** habilita todos os tipos de depuração NTP disponíveis.

Modo de comando: Privileged EXEC mode.

Exemplo: habilite a depuração de eventos NTP.

INTELBRAS#debug ntp event

53.6. Fuso horário

Descrição: o comando **time-zone** é utilizado para configurar o fuso horário do sistema.

Sintaxe: **time-zone** *nome offset_horas offset_minutos*
time-zone *nome offset_horas*
no time-zone

Parâmetros:

- **nome:** configura o nome do fuso horário.
- **offset_horas:** configura o offset de horas em relação ao UTC.
- **offset_minutos:** configura o offset de minutos em relação ao UTC.

Modo de comando: Global Configuration.

Exemplo: configure o fuso horário fuso_horario com 5 horas de offset.

INTELBRAS_config#time-zone fuso_horario 5

54. Neighbor Discovery (ND)

54.1. Tabela de vizinhos

Descrição: o comando **show ipv6 neighbors** é utilizado para exibir a tabela de vizinhos IPv6.

Sintaxe: **show ipv6 neighbors**
show ipv6 neighbors vlan *(1-4096)*

Parâmetros:

- **vlan *(1-4096)*:** exibe a tabela de vizinhos de uma interface VLAN específica.

Modo de comando: Privileged EXEC mode.

Exemplo: exiba a tabela de vizinhos da interface VLAN 2.

INTELBRAS#show ipv6 neighbors vlan 2

54.2. Limpar tabela

Descrição: o comando **clear ipv6 neighbors** é utilizado para limpa a tabela de vizinhos IPv6.

Sintaxe: **clear ipv6 neighbors**

Modo de comando: Privileged EXEC mode.

Exemplo: limpe a tabela de vizinhos.

INTELBRAS#clear ipv6 neighbors

54.3. Entrada manual

Descrição: o comando **ipv6 neighbor** é utilizado para adicionar uma entrada global manualmente na tabela de vizinhos IPv6.

Sintaxe: **ipv6 neighbor** *endereço_ipv6* vlan *(1-4094) endereço_mac*

Parâmetros:

- **endereço_ipv6:** endereço IPv6.
- **vlan (1-4094):** interface VLAN.
- **endereço_mac:** endereço MAC no formato *H:H:H:H:H:H.*

Modo de comando: Global Configuration.

Exemplo: adicione manualmente na tabela de vizinhos da interface VLAN 2 o endereço 3001::1 com o MAC D5:97:66:A7:47:DD

INTELBRAS_config#ipv6 neighbor 3001::1 vlan 2 D5:97:66:A7:47:DD

54.4. Depuração

Descrição: o comando **debug ipv6 nd** é utilizado para configurar a depuração ND do sistema.

Sintaxe: **debug ipv6 nd**
debug ipv6 nd *endereço_ipv6* | entry | timer | adj-table
no debug ipv6 nd
no debug ipv6 nd *endereço_ipv6* | entry | timer | adj-table

Parâmetros:

- **endereço_ipv6:** endereço IPv6.
- **entry:** entrada na tabela de vizinhos.
- **timer:** cronômetro da tabela de vizinhos.
- **adj-table:** tabela adjacente de vizinhos.

Modo de comando: Privileged EXEC mode.

Exemplo: habilite a depuração de ND.

INTELBRAS#debug ipv6 nd

55. ACL IP

Descrição: o comando **ip access-list** é usado para criar e nomear uma lista de controle de acesso. Para a ACL ser criada é necessário sair da interface de configuração ACL com o comando exit.

Sintaxe: **ip access-list** standard | extended *name*
no ip access-list standard | extended *name*

Parâmetros:

- **standard:** criação de lista de controle de acesso padrão.
- **extended:** criação de lista de controle de acesso estendida.
- **name:** nome da lista de controle acesso. O nome pode ter no máximo 20 caracteres.

Modo de comando: Global Configuration.

Exemplo: crie uma regra de ACL padrão com o nome teste.

INTELBRAS_config#ip access-list standard teste

55.1. Regras de permissão

Descrição: o comando **permit** é usado para configurar as regras de permissão de acesso para uma ACL criada.

Para uma ACL de modo *Standard*:

Sintaxe: **permit any** | **A.B.C.D_src** *mask_src* | **reverse-mask** A.B.C.D_*src mask_reverse* | **src-range** *A.B.C.D_inicio A.B.C.D_final* log | location
no permit any | **A.B.C.D**_*src mask_src* | **reverse-mask** *mask* | **src-range** *A.B.C.D_inicio A.B.C.D_final* log

Para uma ACL de modo *Extended*:

Sintaxe: **permit protocol*** config** | *config_adicionais****
no permit protocol* config** | *config_adicionais****

Parâmetros:

- **any:** indica que a regra ACL é aceitar qualquer host de origem.
- **A.B.C.D_src:** configuração do endereço IP de acesso.

» **mask_src:** máscara de rede do endereço IP.
» **reverse-mask:** indica que a configuração de máscara de rede deve ser a máscara inversa.
» **mask_reverse:** mascará de rede inversa.
» **src-range:** indica que a regra ACL é válida para o intervalo de endereço IP configurado.
» **A.B.C.D_inicio:** endereço IP de início.
» **A.B.C.D_final:** endereço IP de final.
» **log:** pacote de dados de registro.
» **location:** informa a sequencia em que a regra ACL deve ser configurada.

Informações sobre **protocol** para uma ACL estendida:

» *** protocol:** representa um número ou o nome do protocolo IP.
» **reverse-mask:** informa que a mascará de rede será invertida.

Protocolo	Descrição
(0-250)	Número de protocolo IP
ICMP	Internet Control Message Protocol
IGMP	Internet Gateway Message Protocol
IP	Internet Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
GRE	Generic Routing Encapsulation Protocol
OSPF	OSPF routing protocol

Informações sobre **config** para uma ACL estendida:

» *** config:** configurações relacionadas aos hosts de acesso ou negação.

A.B.C.D_src	Endereço IP de acesso
Mask_src	Máscara do endereço IP
A.B.C.D_dst	Endereço IP de destino
Interface	Máscara do endereço IP
VLAN	Interface VLAN
NULL	Interface Null
Any	Todos os hosts
Src-range	Será configurado um range de acesso de origem
A.B.C.D_rng_src	Endereço de origem do range de acesso
A.B.C.D_rng_dst	Endereço final do range de acesso
Dsc-range	Será configurado um range de acesso de destino
A.B.C.D_rng_src	Endereço de origem do range de acesso
A.B.C.D_rng_dst	Endereço final do range de acesso

Informações sobre **config_adicionais** para uma ACL estendida:

Configurações adicionais	
log	Pacote de log
time-range	Intervalo de tempo
tos	Pacotes com o ToS informado
tos – (0-15)	Tipo do valor do serviço
precedence	Pacotes com valor de procedência informado

Configurações adicionais	
(0-7)	Valor da procedência
location	Informa o índice para a regra ACL criada
donotfragment-set	Não fragmentar conjunto de sinalizadores
donotfragment-notset	Não fragmentar conjunto de sinalizadores não configurado
is-fragment	Fragmentar pacote
not-fragment	Não fragmentar pacote
totallen	Combine pacotes com o comprimento total informado
totallen - eq	Apenas TTL
totallen – gt	Todo valor TTL maior que este TTL
totallen - lt	Todo valor TTL menor que este TTL
ttl	Combine pacotes com o tempo de vida informado
offset-not-zero	Campo de deslocamento do pacote não é zero
offset-zero	Campo de deslocamento do pacote é zero

Modo de comando: interface de configuração ACL.

Exemplo: crie uma regra de ACL chamada teste do tipo estendida e permita acesso do IP 192.168.0.15 ao IP 192.168.0.1.

INTELBRAS_config#ip access-list extended teste

INTELBRAS_config_ext#92.168.0.15 255.255.255.255 192.168.0.1 255.255.255.255

55.2. Regras de negação

Descrição: o comando **deny** é usado para configurar as regras de negação de acesso para uma ACL criada.

Para uma ACL de modo standard:

Sintaxe: **deny any** | **A.B.C.D_src** *mask_src* | **reverse-mask** A.B.C.D_*src mask_reverse* | **src-range** *A.B.C.D_inicio A.B.C.D_final* log | location
no deny any | **A.B.C.D_src** *mask_src* | **reverse-mask** *mask* | **src-range** *A.B.C.D_inicio A.B.C.D_final* log

Para uma ACL de modo extended:

Sintaxe: **deny protocol*** config** | *config_adicionais****
no deny protocol* config** | *config_adicionais****

Parâmetros:

- **any:** indica que a regra ACL é negar qualquer host de origem.
- **A.B.C.D_src:** configuração do endereço IP de acesso.
- **mask_src:** máscara de rede do endereço IP.
- **reverse-mask:** indica que a configuração de máscara de rede deve ser a máscara inversa.
- **mask_reverse:** mascará de rede inversa.
- **src-range:** indica que a regra ACL é válida para o intervalo de endereço IP configurado.
- **A.B.C.D_inicio:** endereço IP de início.
- **A.B.C.D_final:** endereço IP de final.
- **log:** pacote de dados de registro.
- **location:** informa a sequencia em que a regra ACL deve ser configurada.

Informações sobre **protocol** para uma ACL estendida:

- ***** **protocol:** representa um número ou o nome do protocolo IP.
- **reverse-mask:** informa que a mascará de rede será invertida.

Protocolo	Descrição
(0-250)	Número de protocolo IP
ICMP	Internet Control Message Protocol
IGMP	Internet Gateway Message Protocol
IP	Internet Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
GRE	Generic Routing Encapsulation Protocol
OSPF	OSPF routing protocol

Informações sobre **config** para uma ACL estendida:

» *** config:** configurações relacionadas aos hosts de acesso ou negação.

A.B.C.D_src	Endereço IP de acesso
Mask_src	Máscara do endereço IP
A.B.C.D_dst	Endereço IP de destino
Interface	Máscara do endereço IP
VLAN	Interface VLAN
NULL	Interface Null
Any	Todos os hosts
Src-range	Será configurado um range de acesso de origem
A.B.C.D_rng_src	Endereço de origem do range de acesso
A.B.C.D_rng_dst	Endereço final do range de acesso
Dsc-range	Será configurado um range de acesso de destino
A.B.C.D_rng_src	Endereço de origem do range de acesso
A.B.C.D_rng_dst	Endereço final do range de acesso

Informações sobre **config_adicionais** para uma ACL estendida:

Configurações adicionais	
log	Pacote de log
time-range	Intervalo de tempo
tos	Pacotes com o ToS informado
tos – (0-15)	Tipo do valor do serviço
precedence	Pacotes com valor de procedência informado
(0-7)	Valor da procedência
location	Informa o índice para a regra ACL criada
donotfragment-set	Não fragmentar conjunto de sinalizadores
donotfragment-notset	Não fragmentar conjunto de sinalizadores não configurado
is-fragment	Fragmentar pacote
not-fragment	Não fragmentar pacote
totallen	Combine pacotes com o comprimento total informado
totallen - eq	Apenas TTL
totallen – gt	Todo valor TTL maior que este TTL

Configurações adicionais	
totallen - lt	Todo valor TTL menor que este TTL
ttl	Combine pacotes com o tempo de vida informado
offset-not-zero	Campo de deslocamento do pacote não é zero
offset-zero	Campo de deslocamento do pacote é zero

Modo de comando: interface de configuração ACL.

Exemplo: crie uma regra de ACL chamada negação do tipo estendida e negue acesso ao IP 192.168.0.1 vindo do IP 192.168.0.100.

INTELBRAS_config#ip access-list extended negacao

INTELBRAS_config_ext#deny 0 192.168.0.100 255.255.255.255 192.168.0.1 255.255.255.255

55.3. Aplicar ACL-IP

Descrição: o comando **ip|ipv6 access-group** é utilizado para aplicar uma ACL-IP nas interfaces. Além de configurar a interface de aplicação da ACL também é possível configurar as VLANs em que a ACL terá efeito.

Sintaxe: **ip|ipv6 access-group** *nome_da_acl* vlan *intervalo_vlan*
ip|ipv6 access-group *nome_da_acl* vlan add | remove *intervalo_vlan*

Parâmetros:

- **ip:** ACL-IPv4.
- **ipv6:** ACL-IPv6.
- **nome_da_acl:** nome da ACL.
- **vlan intervalo_vlan:** configura o intervalo de VLAN de aplicação.
- **vlan add intervalo_vlan:** adiciona um intervalo de VLAN de aplicação.
- **vlan remove intervalo_vlan:** remove um intervalo de VLAN de aplicação.

Modo de comando: global configuration|INTERFACE configuration.

Exemplo: aplique globalmente a ACL testeACL nas VLANs 1 e 3 a 5.

INTELBRAS_config#ip access-group testeACL vlan 1,3-5

55.4. Informações

Descrição: o comando **show ip access-list** é usado para informar as informações correntes de ACLs ou de uma ACL específica.

Sintaxe: **show ip access-list** *name*

Parâmetros:

- **name:** nome para a ACL criada.

Modo de comando: privileged EXEC, GLOBAL configuration e interface de configuração FastEthernet.

Exemplo: verifique as informações de ACL configuradas no switch.

INTELBRAS_config#show ip access-list

56. MAC ACL

Descrição: o comando mac access-list é usado para configurar o nome de uma regra de acesso por endereço MAC.

Sintaxe: **mac access-list** *name*
no mac access-list *name*

Parâmetros:

- **name:** nome para a regra de acesso por MAC. Por padrão, quando criado uma regra de acesso, será automaticamente criado uma regra para negar o restante, e esta regra não será exibida.

Modo de comando: Global Configuration.

Exemplo: crie a regra para acesso via MAC address com o nome control_mac.

INTELBRAS_config#mac access-list control_mac

56.1. Regras de permissão

Descrição: o comando **permit** é usado para adicionar regras de permissão de acesso ao switch.

Sintaxe: **permit** any | host | *scr_mac_addr scr_mac_mask dst_mac_addr dst_mac_mask* ethertype arp any | *A.B.C.D* | *IP_mask* cos *value*
no permit any | host | *scr_mac_addr scr_mac_mask dst_mac_addr dst_mac_mask* ethertype arp any | *A.B.C.D* | *IP_mask* cos *value*

Parâmetros:

- **any:** permite qualquer acesso.
- **host:** especifica acesso de um único host de origem.
- **scr_mac_addr:** MAC address do host de origem.
- **scr_mac_mask:** máscara do MAC de origem.
- **dst_mac_addr:** MAC address do host de destino.
- **dst_mac_mask:** máscara do MAC de destino.
- **ethertype:** tipo do pacote Ethernet.
- **arp:** identifica um endereço IP.
- **A.B.C.D:** endereço IP.
- **IP-mask:** máscara de rede do endereço IP.
- **cos:** especifica a classe de serviço.
- **value:** valor da classe de serviço. Pode variar de 0 a 7.

Modo de comando: interface de configuração de acesso MAC.

Exemplo: crie a regra de acesso MAC address com o nome control_mac e permita o host com endereço MAC 1234.5678.abcd de acessar o equipamento.

INTELBRAS_config#mac access-list control_mac

INTELBRAS-config-macl#permit host 1234.5678.abcd

56.2. Regras de negação

Descrição: o comando **deny** é usado para adicionar regras de negação de acesso ao switch.

Sintaxe: deny any | host | *scr_mac_addr scr_mac_mask dst_mac_addr dst_mac_mask* ethertype arp any | *A.B.C.D* | *IP_mask* cos *value*
no deny any | host | *scr_mac_addr scr_mac_mask dst_mac_addr dst_mac_mask* ethertype arp any | *A.B.C.D* | *IP_mask* cos *value*

Parâmetros:

- **any:** permite qualquer acesso.
- **host:** especifica acesso de um único host de origem.
- **scr_mac_addr:** MAC address do host de origem.
- **scr_mac_mask:** máscara do MAC de origem.
- **dst_mac_addr:** MAC address do host de destino.
- **dst_mac_mask:** máscara do MAC de destino.
- **ethertype:** tipo do pacote Ethernet.
- **arp:** identifica um endereço IP.
- **A.B.C.D:** endereço IP.
- **IP-mask:** máscara de rede do endereço IP.
- **cos:** especifica a classe de serviço.
- **value:** valor da classe de serviço. Pode variar de 0 a 7.

Modo de comando: interface de configuração de acesso MAC.

Exemplo: crie a regra de acesso MAC address com o nome control_mac e negue o host com endereço MAC 1234.5678.abcd de acessar o equipamento.

INTELBRAS_config#mac access-list control_mac

INTELBRAS-config-macl#deny host 1234.5678.abcd

56.3. Aplicar ACL-MAC

Descrição: o comando **mac access-group** é usado para criar/adicionar grupos de acesso MAC nas portas Ethernet.

Sintaxe: **mac access-group** *name* vlan *ID* add | remove *ID*
no mac access-group *name* vlan

Parâmetros:

- **name:** nome para o grupo de acesso MAC.
- **ID:** identifica a VLAN.
- **add:** adiciona a VLAN.
- **remove:** remove a VLAN.

Modo de comando: Global Configuration.

Exemplo: crie a regra de acesso MAC address com o nome control_mac adicionando a VLAN 50 e atribua a interface FastEthernet 1.

INTELBRAS_config#mac access-group control_mac vlan add 50

INTELBRAS_config#interface FastEthernet 0/1

INTELBRAS_config_f0/1#mac access-group control_mac

57. ARP

57.1. Entrada na tabela ARP

Descrição: o comando **arp** é usado para inserir ou retirar o endereço IP da tabela ARP do switch.

Sintaxe: **arp** *A.B.C.D mac_add* vlan (1-X) alias
no arp *A.B.C.D* vlan (1-X)

Parâmetros:

- **A.B.C.D:** endereço IP a ser inserido na tabela.
- **mac_add:** MAC address a ser inserido na tabela.
- **(1-X):** interface VLAN.
- **alias:** o switch responde às solicitações ARP como se fosse a interface do endereço solicitado.

Modo de comando: Global Configuration.

Exemplo: insira o endereço de IP 192.168.10.1 00:11:22:33:44:55 na tabela ARP.

INTELBRAS_config#arp 192.168.10.1 00:11:22:33:44:55 vlan 1

57.2. Atualização do gateway

Descrição: o comando **arp max-gw-retries** é usado para configurar o número de tentativas de retransmissão dos pacotes de atualização da tabela ARP quando o gateway expirar.

Sintaxe: **arp max-gw-retries** (0-5)
no arp max-gw-retries

Parâmetros:

- **(0-5):** quantidade de retransmissão do pacote.

Modo de comando: Global Configuration.

Exemplo: configure para 5 o número de retransmissão do pacote para atualização da tabela ARP para o gateway do switch.

INTELBRAS_config#arp max-gw-retries 5

57.3. Atualização da tabela

Descrição: o comando **arp retry-allarp** é usado para configurar que o switch atualize todos os endereços da tabela ARP após o tempo limite expirar, não apenas a configuração para o gateway como no comando anterior.

Sintaxe: **arp retry-allarp**
no arp retry-allarp

Modo de comando: Global Configuration.

Exemplo: configure o switch para atualizar as entradas ARP após o tempo de cada uma expirar.

INTELBRAS_config#arp retry-allarp

57.4. Tempo de vida

Descrição: o comando **arp timeout** é usado para configurar o tempo de vida de uma entrada dinâmica na tabela ARP do switch.

Sintaxe: **arp timeout** (0-4294967)
no arp timeout
default arp timeout

Parâmetros:

- **(0-4294967):** intervalo de tempo em segundos de validade da tabela ARP do switch. Para que a tabela nunca expire utilize o valor 0.
- **default:** retorna o valor para o intervalo padrão, *04:00:00*.
- **no:** mesmo que o comando default.

Modo de comando: interface de configuração Ethernet.

Exemplo: configure o switch para manter as entradas da tabela ARP por um período de tempo de 900 segundos na interface vlan 1.

INTELBRAS_config#interface vlan 1

INTELBRAS_config_v1#arp timeout 900

57.5. Gratuitous ARP

Descrição: o comando **arp send-gratuitous** é usado para configurar o envio de pacotes gratuitous ARP pelo switch. Gratuitous ARP são pacotes de envio de requisição ou resposta mesmo quando não são solicitados e geralmente são utilizados para atualizar a tabela ARP.

Sintaxe: **arp send-gratuitous** interval *(15-600)*
no arp send-gratuitous interval

Parâmetros:

- **interval:** para configurar o intervalo de tempo entre o envio dos pacotes.
- **(15-600):** intervalo de tempo em segundos para o envio o pacote gratuitous pelo switch. Por padrão o intervalo de tempo é de *120 segundos*.

Modo de comando: interface de configuração Ethernet.

Exemplo: configure o switch para enviar pacotes gratuitous ARP no intervalo de 3 minutos. INTELBRAS_config#interface vlan 1

INTELBRAS_config_v1#arp send-gratuitous interval 180

57.6. Limpeza da tabela

Descrição: o comando **clear arp-cache** é usado para limpar todas as entradas dinâmicas da tabela ARP ou apenas uma entrada específica.

Sintaxe: **clear arp-cache** *A.B.C.D IP-mask* | vlan (1-X)

Parâmetros:

- **A.B.C.D:** endereço IP para ser retirado da tabela.
- **IP-mask:** máscara de rede do endereço IP.
- **(1-X):** interface VLAN.

Modo de comando: Privileged EXEC.

Exemplo: limpe as entradas dinâmicas da tabela ARP.

INTELBRAS#clear arp-cache

57.7. Informações

Descrição: o comando **show arp** é usado para exibir as informações da tabela ARP.

Sintaxe: **show arp**

Obs.: *a saída do comando show arp é uma tabela com as informações de Protocolo, endereço de IP, tempo de entrada na tabela, endereço MAC, tipo de encapsulamento utilizado e a interface onde a entrada está associada.*

Modo de comando: Privileged EXEC.

Exemplo:

INTELBRAS#show arp

58. Endereço IP

Descrição: o comando **ip address** é usado para configurar um endereço de IP como endereço principal. Pode ser usado para configurar mais dois endereços secundários em interfaces VLAN diferentes.

Sintaxe: **ip address** *A.B.C.D | dhcp IP-mask* secondary
no ip address *A.B.C.D IP-mask*
no ip address

Parâmetros:

- **A.B.C.D:** endereço IP para ser cadastrado na interface VLAN.
- **IP-mask:** máscara de rede do endereço IP.
- **dhcp:** endereço IP será configurado por um servidor DHCP.
- **secondary:** configura o endereço de IP como secundário na interface VLAN.
- **no:** apaga o endereço IP especificado ou todos os endereços da interface VLAN escolhida.

Modo de comando: interface de configuração Ethernet.

Exemplo: configure o endereço de IP 202.0.0.1 com a máscara de rede 255.255.255.0 como endereço principal e o endereço 204.0.01 com a máscara de rede 255.255.255.0 como secundário na interface VLAN 10.

INTELBRAS_config#interface vlan 10

INTELBRAS_config_v10#ip address 202.0.0.1 255.255.255.0

INTELBRAS_config_v10#ip address 204.0.0.1 255.255.255.0 secondary

58.1. MTU

Descrição: o comando **ip mtu** é usado para definir o MTU do pacote IP transmitido de uma interface.

Sintaxe: **ip mtu** (68-1500)
no ip mtu

Parâmetros:

- **(68-1500):** tamanho máximo do pacote MTU.

Modo de comando: interface de configuração Ethernet.

Exemplo: configure o MTU do switch na interface vlan 1 para 1200.

INTELBRAS_config#interface VLAN 1

INTELBRAS_config_v1#ip mtu 1200

58.2. Informações

Descrição: o comando **show ip interface** é usado para exibir as informações das configurações das interfaces do switch.

Sintaxe: **show ip interface** VLAN | Null | loopback | brief number

Parâmetros:

- **VLAN:** interface VLAN.
- **Null:** interface null.

» **loopback:** interface loopback.
» **brief:** informações reduzidas das configurações das interfaces.
» **number:** número da interface.

Modo de comando: Privileged EXEC.

Exemplo:

INTELBRAS#show ip interface

58.3. Mapeamento IP-Host

Descrição: o comando **ip host** é usado para mapear um endereço de IP com um nome. Após esta configuração quando for necessário utilizar o IP, pode ser utilizado o nome atribuído a ele.

Sintaxe: **ip host** *word A.B.C.D*
no ip host *word A.B.C.D*

Parâmetros:

» **word:** nome atribuído ao endereço de host.
» **A.B.C.D:** endereço IP para ser cadastrado como host.

Modo de comando: Global Configuration.

Exemplo: configure o endereço de IP 192.168.10.3 como o nome teste-ping e execute o teste de conexão até o host.

INTELBRAS_config#ip host teste-ping 192.168.10.3

INTELBRAS_config#ping teste-ping

Informações

Descrição: o comando **show host** é usado para exibir as informações das configurações de hosts do comando anterior, ip host.

Sintaxe: **show host**

Modo de comando: Privileged EXEC.

Exemplo:

INTELBRAS#show host

59. Cliente DHCP

Descrição: o comando **ip address dhcp** é usado para configurar um endereço de IP através de um servidor DHCP na interface VLAN selecionada.

Sintaxe: **ip address dhcp**
no ip address dhcp

Modo de comando: interface de configuração Ethernet.

Exemplo: configure um endereço de IP através de um servidor DHCP na interface VLAN 1.

INTELBRAS_config#interface vlan 1

INTELBRAS_config_v1#ip address dhcp

59.1. Configurações adicionais

Descrição: o comando **ip dhcp client** é usado para configurar os parâmetros de cliente DHCP do switch.

Sintaxe: **ip dhcp client** bootfileaddmac | class_identifier *word* | client_identifier *hrd_ether* | minlease *(60-86400)* | retransmit *(1-10)* | retry_interval *(1-1440)* | select *(5-30)* | tftpdownload | timeout_shut
no ip dhcp client bootfileaddmac | class_identifier | client_identifier | minlease | retransmit | retry_interval | select | tftpdownload | timeout_shut

Parâmetros:

» **bootfileaddmac:** habilitar DHCP *bootfile name* para adicionar endereço MAC do cliente.

» **class_identifier:** define o ID da classe pertence ao cliente.
» **word:** identificador de classe de fornecedor.
» **client_identifier:** identificador de cliente.
» **hrd_ether:** endereço de hardware Ethernet.
» **minlease:** tempo de locação mínimo aceitável.
» **(60-86400):** pode variar de 60 a 86400 segundos. O tempo padrão é *60 segundos*.
» **retransmit:** configuração da contagem de retransmissão de pacotes.
» **(1-10):** pode variar de 1 a 10 vezes. A quantidade padrão é *4 vezes*.
» **retry_interval:** define o intervalo de repetição.
» **(1-1440):** pode variar de 1 a 1440 minutos. O tempo padrão é *1 minuto*.
» **select:** configuração do intervalo SELECT.
» **(5-30):** pode variar de 5 a 30 segundos. O tempo padrão é *5 segundos*.
» **tftpdownload:** ativar a função de *download TFTP*.
» **timeout-shut:** desabilitar a interface quando o tempo atingir o tempo limite.

Modo de comando: Global Configuration.

Exemplo: o exemplo a seguir mostra como definir o tempo de concessão mínimo aceitável do cliente DHCP no switch para 100 segundos.

INTELBRAS_config#ip dhcp client minlease 100

O exemplo a seguir mostra como definir os tempos de retransmissão dos pacotes de protocolo no cliente DHCP do switch como 3.

INTELBRAS_config#ip dhcp client retransmit 3

60. Servidor DHCP

Descrição: o comando **ip dhcp-server** é usado para configurar um endereço de IP para o servidor DHCP.

Sintaxe: **ip dhcp-server** *A.B.C.D*
no ip dhcp-server *A.B.C.D*

Parâmetros:

» **A.B.C.D:** endereço IP do servidor DHCP.

Modo de comando: Global Configuration.

Exemplo: configure um endereço de IP 192.168.20.1 para o servidor DHCP.

INTELBRAS_config#ip dhcp-server 192.168.20.1

60.1. Endereços atribuídos

Descrição: o comando **show dhcp lease** é usado para exibir os endereços de IP atribuídos por um servidor DHCP.

Sintaxe: **show dhcp lease**

Modo de comando: Privileged EXEC ou Global Configuration.

Exemplo: mostre as informações de distribuição de IP via DHCP.

INTELBRAS_config#show dhcp lease

60.2. Informações

Descrição: o comando **show dhcp server** é usado para exibir as informações do servidor DHCP.

Sintaxe: **show dhcp server**

Modo de comando: Privileged EXEC ou Global Configuration.

Exemplo: mostre as informações do servidor DHCP.

INTELBRAS_config#show dhcp server

60.3. Depuração

Descrição: o comando **debug dhcp** é usado para exibir as informações do protocolo DHCP enquanto ele é executado no switch.

Sintaxe: **debug dhcp** detail

Parâmetros:

» **detail:** exibir o conteúdo do pacote DHCP.

Modo de comando: Privileged EXEC.

Exemplo: mostre as informações do protocolo DHCP.

INTELBRAS#debug dhcp detail

61. Endereço IPv6

Descrição: o comando **ipv6 enable** é utilizado para habilitar o IPv6 em interface VLAN.

Sintaxe: **ipv6 enable**
no ipv6 enable

Modo de comando: Interface VLAN Configuration.

Exemplo: habilite o ipv6 na interface VLAN 1.

INTELBRAS_config_v1# ipv6 enable

61.1. Prefixo geral IPv6

Descrição: o comando **ipv6 general-prefix** é utilizado para configurar um prefixo geral IPv6.

Sintaxe: **ipv6 adress general-prefix** *nome prefixo_ipv6*
no ipv6 adress general-prefix *nome prefixo_ipv6*

Parâmetros:

» **prefixo_ipv6:** prefixo IPv6.
» **nome:** nome do prefixo geral IPv6.

Modo de comando: Global Configuration.

Exemplo: configure o prefixo geral IPv6 3001::/48.

INTELBRAS_config#ipv6 general-prefix 3001::/48

61.2. Atribuição de endereço

Descrição: o comando **ipv6 address** é utilizado para configurar o endereço IPv6 de uma interface VLAN.

Sintaxe: **ipv6 adress** *endereço_ipv6* link-local
ipv6 adress *endereço_ipv6* | autoconfig
ipv6 adress *endereço_ipv6* anycast
ipv6 adress *prefixo_ipv6* eui-64
ipv6 adress general-prefix n*ome endereço_ipv6*
ipv6 adress general-prefix *nome endereço_ipv6* anycast
ipv6 adress general-prefix *nome prefixo_ipv6* eui-64
no ipv6 adress

Parâmetros:

» **link-local:** configura endereço local IPv6.
» ***endereço_ipv6*:** endereço global IPv6.
» **autoconfig:** configura automaticamente o endereço global IPv6 via mensagem RA (Router Advertisement).
» **anycast:** configura o endereço global IPv6 como anycast.
» ***prefixo_ipv6*:** prefixo IPv6.
» **eui-64:** configura o endereço global IPv6 com o método EUI-64.
» **general-prefix:** configura endereço global IPv6 com um prefixo geral.
» **nome:** configura o nome de um prefixo genérico IPv6.

» **Modo de comando:** Interface VLAN Configuration.

Exemplo: configure a obtenção automática do endereço global IPv6 na interface VLAN 1.

INTELBRAS_config_v1# ip address autoconfig

61.3. MTU

Descrição: o comando **ipv6 mtu** é utilizado para configurar o MTU do pacote IPv6 em uma interface VLAN.

Sintaxe: **ipv6 mtu** *tamanho*
no ipv6 mtu

Parâmetros:

» **tamanho:** tamanho em bytes do MTU.

Modo de comando: Interface VLAN Configuration.

Exemplo: configure o MTU na interface VLAN 1 para 1200 bytes.

INTELBRAS_config_v1# ipv6 mtu 1200

61.4. Informações IPv6

Descrição: o comando **show ipv6** é utilizado para exibir as informações IPv6 do sistema.

Sintaxe: **show ipv6** interface brief | vlan *interface_id*
show ipv6 traffic | general-prefix

Parâmetros:

» **brief:** exibe informações resumidas de todas as interfaces.
» **vlan interface_id:** exibe informações e estatísticas de uma determinada interface.
» **traffic:** exibe as estatísticas de trafego.
» **general-prefix:** exibe os prefixos gerais configurados.

Modo de comando: Privileged EXEC.

Exemplo: exiba as informações IPv6 resumidas de todas as interfaces.

INTELBRAS#show ipv6 interface brief

61.5. Limpar estatísticas

Descrição: o comando **clear ipv6 traffic** é utilizado para limpar as estatísticas de trafego IPv6 do sistema.

Sintaxe: **clear ipv6 traffic**

Modo de comando: Privileged EXEC.

Exemplo: limpe as estatísticas de trafego IPv6 do sistema.

INTELBRAS#clear ipv6 traffic

61.6. Depuração

Descrição: o comando **debug ipv6 packet** é utilizado para habilitar a depuração de pacotes IPv6.

Sintaxe: **debug ipv6 packet** detail | interface *interface_id* | access-list *nome_acl*
no debug ipv6 packet detail | interface *interface_id* | access-list *nome_acl*

Parâmetros:

» **detail:** configura a depuração detalhada.
» **interface interface_id:** configura a depuração em uma interface.
» **access-list nome_acl:** configura a depuração em pacotes que combinam com uma ACL.

Modo de comando: Privileged EXEC.

Exemplo: habilite a depuração de pacotes IPv6 na interface VLAN 1.

INTELBRAS#debug ipv6 packet interface vlan 1

62. ICMP

62.1. Redirecionamento

Descrição: o comando **ip redirects** é utilizado para habilitar a transmissão de pacotes ICMP de redirecionamento.

Sintaxe: **ip redirects**
no ip redirects

Modo de comando: Interface VLAN Configuration.

Exemplo: habilitar a transmissão de pacotes ICMP de redirecionamento.

INTELBRAS_config_v1# ip redirects

62.2. IP inacessível

Descrição: o comando **ip unreachables** é usado para configurar o switch a responder ao host de origem a informação que ele não conhece a rota. Assim ele pode detectar esta rota e corrigir o problema para uma futura transmissão.

Sintaxe: **ip unreachables**
no ip unreachables

Modo de comando: Interface VLAN Configuration.

Exemplo: configure o switch para retornar ao host de origem a informação de IP inacessível.

INTELBRAS_config#interface VLAN 1

INTELBRAS_config_v1#ip unreachables

63. ICMPv6

63.1. Redirecionamento

Descrição: o comando **ipv6 redirects** é utilizado para habilitar a transmissão de pacotes ICMPv6 de redirecionamento.

Sintaxe: **ipv6 redirects**
no ipv6 redirects

Modo de comando: Interface VLAN Configuration.

Exemplo: habilitar a transmissão de pacotes ICMPv6 de redirecionamento.

INTELBRAS_config_v1# ipv6 redirects

63.2. Inalcançável

Descrição: o comando **ipv6 unreachables** é utilizado para habilitar a transmissão de pacotes ICMPv6 de destino inalcançável.

Sintaxe: **ipv6 unreachables**
no ipv6 unreachables

Modo de comando: Interface VLAN Configuration.

Exemplo: habilitar a transmissão de pacotes ICMPv6 de destino inalcançável.

INTELBRAS_config_v1# ipv6 redirects

64. MLD snooping

Descrição: o comando **ipv6 mld snooping** é utilizado para habilitar o MDL Snooping.

Sintaxe: **ipv6 mld snooping**
no ipv6 mld snooping

Modo de comando: Global Configuration.

Exemplo: habilite o MLD Snooping.

 INTELBRAS_config#ipv6 mld snooping

64.1. Encaminhamento MLD

Descrição: o comando **ipv6 mld solicitation** é utilizado para habilitar o encaminhamento de pacotes MLD.

Sintaxe: **ipv6 mld solicitation**
no ipv6 mld solicitation

Modo de comando: Global Configuration.

Exemplo: habilite o encaminhamento de pacotes MLD.

INTELBRAS_config#ipv6 mld solicitation

64.2. Endereço multicast estático

Descrição: o comando **ipv6 mld vlan** é utilizado para configurar um endereço Multicast estático em uma interface físcia.

Sintaxe: **ipv6 mld-snooping vlan** *(1-4094)* static *endereço_ipv6* interface GigaEthernet
no ipv6 mld-snooping vlan *(1-4094)* static *endereço_ipv6* interface GigaEthernet

Parâmetros:

» **vlan *(1-4094)*:** identificador da VLAN.
» **static *endereço_ipv6*:** endereço Multicast estático.
» **interface GigaEthernet:** identificador da interface.

Modo de comando: Global Configuration.

Exemplo: configure o endereço multicast estático ff12::5 na vlan 1 da porta GigaEthernet 1.

INTELBRAS_config#ipv6 mld-snooping vlan 1 static ff12::5 interface GigaEthernet 0/1

64.3. Tempo de envelhecimento

Descrição: o comando **ipv6 mld-snooping timer router-age** é utilizado para configurar o tempo de envelhecimento do MLD Snooping. O tempo de envelhecimento determina o tempo em que o sistema considera um querier como existente.

Sintaxe: **ipv6 mld-snooping timer router-age** *(10-2147483647)*
no ipv6 mld-snooping timer router-age

Parâmetros:

» **(10-2147483647):** tempo de envelhecimento em unidades de segundo.

Modo de comando: Global Configuration.

Exemplo: configure o tempo de envelhecimento do MLD Snooping para 50 segundos.

INTELBRAS_config#ipv6 mld-snooping timer router-age 50

64.4. Tempo de espera

Descrição: o comando **ipv6 mld-snooping timer router-age** é utilizado para configurar o tempo de espera de uma resposta do host à query Multicast após a mesma ter sido enviada.

Sintaxe: **ipv6 mld-snooping timer response-time** *(10-2147483647)*
no ipv6 mld-snooping timer response-time

Parâmetros:

» **(10-2147483647):** tempo de espera em unidades de segundo.

Modo de comando: Global Configuration.

Exemplo: configure o tempo de espera do MLD Snooping para 50 segundos.

INTELBRAS_config#ipv6 mld-snooping timer response-time 50

64.5. Querier

Descrição: o comando **ipv6 mld-snooping querier** é utilizado para imitar um roteador multicast na ausência do mesmo na VLAN em que o MLD Snooping está ativado.

Obs.: *se existe um roteador multicast na VLAN a função é desabilitada na VLAN.*

Sintaxe: **ipv6 mld-snooping querier**
ipv6 mld-snooping querier address *endereço_ipv6*
no ipv6 mld-snooping querier
no ipv6 mld-snooping querier address

Parâmetros:

» **endereço_ipv6:** endereço IPv6 de origem da query.

Modo de comando: Global Configuration.

Exemplo: habilite a função de *Roteador multicast falso*.

INTELBRAS_config#ipv6 mld-snooping querier

64.6. Roteamento multicast

Descrição: o comando **ipv6 mld-snooping vlan** *(1-4094)* **mrouter** é utilizado para configurar a porta como uma porta conectada a um Roteador Multicast. Após feita esta configuração na porta a mesma irá encaminhar todos os pacotes de report e done do MLD-Snooping.

Sintaxe: **ipv6 mld-snooping vlan** *(1-4094)* **mrouter** interface GigaEthernet
no ipv6 mld-snooping querier address

Parâmetros:

» **(1-4094):** identificador da VLAN.
» **interface GigaEthernet:** identificador da interface.

Modo de comando: Global Configuration.

Exemplo: configure a porta GigaEthernet 1 como uma porta conectada a um Roteador Multicast.

INTELBRAS_config#ipv6 mld-snooping vlan 1 mrouter interface GigaEthernet 0/1

64.7. Saída imediata

Descrição: o comando **ipv6 mld-snooping vlan** *(1-4094)* **immediate-leave** é utilizado para habilitar a função de *Saída imediata* do MLD Snooping numa VLAN.

Sintaxe: **ipv6 mld-snooping vlan** *(1-4094)* **immediate-leave**
no ipv6 mld-snooping vlan *(1-4094)* **immediate-leave**

Parâmetros:

» **(1-4094):** identificador da VLAN.

Modo de comando: Global Configuration.

Exemplo: habilitar a função de *Saída imediata* do MLD-Snooping na VLAN 1.

INTELBRAS_config#ipv6 mld-snooping vlan 1 immediate-leave

64.8. Informações

Descrição: o comando **show ipv6 mld-snooping** é utilizado para exibir as informações de MLD Snooping do sistema.

Sintaxe: **show ipv6 mld-snooping**
show ipv6 mld-snooping timers | groups | statistics | vlan | mac

Parâmetros:

» **timers:** exibe os cronômetros.
» **groups:** exibe os grupos Multicast.
» **statistics:** exibe as estatísticas.
» **vlan:** exibe as configurações nas VLANs.
» **mac:** exibe os endereços Multicast MAC.

Modo de comando: Privileged EXEC.

Exemplo: exiba as informações de MLD Snooping do sistema.

INTELBRAS#show ipv6 mld-snooping

Termo de garantia

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

Nome do cliente:
Assinatura do cliente:
Nº da nota fiscal:
Data da compra:
Modelo: Nº de série:
Revendedor:

1. Todas as partes, peças e componentes do produto são garantidos contra eventuais vícios de fabricação, que porventura venham a apresentar, pelo prazo de 3 (três) anos – sendo este prazo de 3 (três) meses de garantia legal mais 33 (trinta e três) meses de garantia contratual –, contado a partir da data da compra do produto pelo 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 expressa de produtos que apresentarem vício de fabricação. Caso não seja constatado vício de fabricação, e sim vício(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. Constatado o vício, o Senhor Consumidor deverá imediatamente comunicar-se com o Serviço Autorizado mais próximo que conste na relação oferecida pelo fabricante – somente estes estão autorizados a examinar e sanar o defeito durante o prazo de garantia aqui previsto. Se isso não for respeitado, esta garantia perderá sua validade, pois estará caracterizada a violação do produto.
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.
8. Após sua vida útil, o produto deve ser entregue a uma assistência técnica autorizada da Intelbras ou realizar diretamente a destinação final ambientalmente adequada evitando impactos ambientais e a saúde. Caso prefira, a pilha/bateria assim como demais eletrônicos da marca Intelbras sem uso, pode ser descartado em qualquer ponto de coleta da Green Eletron (gestora de resíduos eletroeletrônicos a qual somos associados). Em caso de dúvida sobre o processo de logística reversa, entre em contato conosco pelos telefones (48) 2106-0006 ou 0800 704 2767 (de segunda a sexta-feira das 08 ás 20h e aos sábados das 08 ás 18h) ou através do e-mail suporte@intelbras.com.br.

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.

O processo de fabricação deste produto não é coberto pelos requisitos da ISO 14001.

Todas as imagens deste manual são ilustrativas.

intelbras

fale com a gente

Suporte a clientes: (48) 2106 0006
Fórum: forum.intelbras.com.br
Suporte via chat: intelbras.com.br/suporte-tecnico
Suporte via e-mail: suporte@intelbras.com.br
SAC: 0800 7042767
Onde comprar? Quem instala?: 0800 7245115

Importado no Brasil por: Intelbras S/A – Indústria de Telecomunicação Eletrônica Brasileira
Rodovia SC 281, km 4,5 – Sertão do Maruim – São José/SC – 88122-001
CNPJ 82.901.000/0014-41 – www.intelbras.com.br

03.20
Origem: China