intelbras

Manual do usuário

SG 5200 MR

intelbras

SG 5200 MR

Switch gerenciável 48 portas Gigabit Ethernet com 4 portas Mini-GBIC

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

O switch SG 5200 MR possui 52 portas Gigabit Ethernet, sendo 48 portas RJ45 e 4 slots Mini-GBIC independentes, proporcionando altas taxas de transferência de dados, permitindo a integração de computadores, impressoras, 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.

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

Proteção e segurança de dados

Observar as leis locais relativas à proteção e uso de tais dados e as regulamentacoes que prevalecem no pais.

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 de 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 a 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.

Índice

1. Sobre o manual 6
1.1. Público destinado para o manual .6
1.2. Convenções .6
1.3. Estrutura do manual .6
2. Introdução 7
2.1. Especificações técnicas .7
2.2. Visão geral do switch .9
2.3. Principais funções .9
2.4. Descrição do produto .9
3. Acesso à interface de gerenciamento 10
3.1. Login .10
3.2. Configuração .11
4. Sistema 11
4.1. Informações .11
4.2. Usuários .15
4.3. Ferramentas .17
4.4. Gerenciamento .19
5. Switching 27
5.1. Portas .27
5.2. Agregação de link .33
5.3. Tráfego .37
5.4. Endereço MAC .39
5.5. Filtro DHCP .44
6. VLAN 47
6.1. 802.1Q VLAN .47
6.2. Exemplos de aplicação para 802.1Q VLAN .50
7. Spanning tree 51
7.1. Spanning Tree .55
7.2. Portas STP .57
7.3. Instâncias MSTP .58
7.4. Segurança STP .61
7.5. Exemplos de aplicações STP .63
8. Multicast 66
8.1. IGMP Snooping .68
8.2. Multicast estático .74
8.3. Filtro multicast .76
8.4. Estatísticas IGMP .78

9. QoS 79
9.1. DiffServ .81
9.2. Controle de banda .85
9.3. Voice VLAN .87
10. ACL 91
10.1. Configurar ACL .91
10.2. Políticas ACL .95
10.3. Vínculos ACL .96
10.4. Exemplos de aplicação para ACL .98
11. SNMP 99
11.1. SNMP .101
11.2. Notificação .106
11.3. RMON .107
12. Manutenção 111
12.1. Monitoramento .111
12.2. Log .112
12.3. Ferramentas .115
12.4. Diagnóstico .117
13. Restaurando para o padrão de fábrica 118
Termo de garantia 119

1. Sobre o manual

Este manual contém informações para instalação e gerenciamento do switch SG 5200 MR. Por favor, leia-o com atenção antes de operar o produto.

1.1. Público destinado para o manual

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

1.2. Convenções

Neste manual as seguintes convenções serão usadas:

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

» *Itálico* indica um botão, um ícone na barra de ferramentas, menu ou um item de menu.

1.3. Estrutura do manual

Capítulo	Introdução
1 - Sobre o manual	Introdução de como o manual está estruturado.
2 - Introdução	Introdução das funções, aplicação e aparência do SG 5200 MR.
3 - Acesso à interface de gerenciamento	Introdução para logar na interface de gerenciamento web do produto.
4 - Sistema	Este módulo é utilizado para configurações do sistema e propriedades do switch. - Informações: configuração da descrição, tempo do sistema e parâmetros de redes do switch. - Usuários: configuração de usuários e senhas, além de configurar o nível de acesso para cada usuário. - Ferramentas: manipulação dos arquivos de configuração do switch. - Gerenciamento: fornece diferentes medidas de segurança para acessar o gerenciamento web do switch.
5 - Switching	Este módulo é utilizado para realizar as configurações básicas do switch. - Portas: configuração do modo de funcionamento das portas do switch. - Agregação de link: permite a utilização de múltiplas portas para o aumento da velocidade do link. - Tráfego: monitoramento do tráfego de dados nas portas do switch. - Endereço MAC: configuração da tabela de endereços MAC do switch. - Filtro DHCP: monitora o processo de atribuição do endereço IP através de um Servidor DHCP.
6 - VLAN	Este módulo é utilizado para configurar VLANs. - 802.1Q VLAN: configuração de VLANs baseadas em TAG de VLAN e portas.
7 - Spanning Tree	Este módulo é utilizado para configurar a função Spanning Tree no switch. - Spanning Tree: configuração e visualização das configurações globais da função Spanning Tree. - Portas STP: configuração dos parâmetros da função STP para cada porta. - Instâncias MSTP: configuração de instâncias MSTP. - Segurança STP: configuração de proteção contra ataques maliciosos à função STP.
8 - Multicast	Este módulo é utilizado para configurar a função Multicast do switch. - IGMP Snooping: configuração global dos parâmetros IGMP Snooping, propriedade da porta, VLAN e Multicast VLAN. - Multicast Estático: configuração da tabela de IP Multicast Estático e visualização da Tabela de Endereços Multicast. - Filtro Multicast: configuração dos recursos de filtros de endereços Multicast. - Estatísticas IGMP: visualização das mensagens IGMP em cada porta do switch.
9 - QoS	Este módulo é utilizado para configuração de QoS, provendo qualidade e priorizando serviços desejados. - DiffServ: configuração de prioridade por porta, 802.1P e DSCP, além de configuração do algoritmo de fila. - Controle de Banda: configuração do Limite de Banda e Storm Control por porta. - Voice VLAN: configuração da VLAN de voz, utilizada para garantir a prioridade e qualidade na transmissão do fluxo de voz dentro de uma VLAN específica.
10 - ACL	Este módulo é utilizado para bloquear/permitir pacotes através de regras e políticas ACL predeterminadas, afim de controlar o tráfego de dados na rede. A seguir as principais informações: - Configurar ACL: criação e configuração de regras para as ACLs. - Políticas ACL: configuração de políticas ACL. - Vínculos ACL: configuração de vínculos de políticas ACL a uma determinada VLAN ou porta do switch.
11 - SNMP	Este módulo é utilizado para configurar a função SNMP, provendo um monitoramento e gerenciamento do switch na rede. - SNMP: define as configurações globais da função SNMP. - Notificação: configuração das notificações (Trap e Inform) enviadas para a estação de gerenciamento. - RMON: configuração da função RMON para monitorar a rede de forma mais eficiente.

Capítulo	Introdução
12 - Manutenção	Este módulo é utilizado para monitorar o switch e diagnosticar possíveis problemas na rede. - Monitoramento: monitoramento da utilização da Memória e CPU do Switch. - Log: permite classificar, visualizar e gerenciar informações do sistema de forma eficaz. - Ferramentas: teste o estado do cabo de rede conectado ao switch e também a disponibilidade das portas do switch. - Diagnóstico: testa se o endereço IP de destino está ao alcance do switch, bem como a quantidade de saltos necessários até alcançá-lo.
13 - Restaurando para o padrão de fábrica	Restaurando o switch ao padrão de fábrica.

2. Introdução

2.1. Especificações técnicas

Chipset		Marvell 98DX3036 * 2
		Marvell 88E1545 * 12
Dimensões (L × A × P)		440 × 44 × 260 mm
		Acompanha suporte para rack padrão EIA 19" com 1 U de altura
Material		Aço
LED	Power	Verde
	SYS	Verde
	Link/Act	Verde
	10/100/1000 Mbps (RJ45)	Verde/Laranja (48)
	1000 Base-X (Mini-GBIC)	Verde (4)
Portas	10/100/1000M (RJ45)	48
	Mini GBIC (SFP)	4 (independentes)
Cabeamento suportado	10BASE-T	Cabo UTP/STP categoria 3, 4, 5 (máximo 100 m)
		EIA/TIA-568 100Ω STP (máximo 100 m)
	100BASE-TX	Cabo UTP/STP categoria 5, 5e (máximo 100 m)
		EIA/TIA-568 100Ω STP (máximo 100 m)
	1000BASE-T	Cabo UTP/STP categoria 5e, 6 (máximo 100 m)
		EIA/TIA-568 100Ω STP (máximo 100 m)
	1000BASE-X	Fibras Monomodo e Multimodo
Padrões e protocolos	Padrão IEEE	IEEE802.3, 802.3u, 802.3ab, 802.3z, 802.3x, 802.1p, 802.1Q, 802.1d, 802.1w, 802.1s, 802.3ad
	Padrão IETF	RFC1541, RFC1112, RFC2236, RFC1757, RFC1157, RFC2571
	Outros padrões e protocolos	CSMA/CD, TCP/IP, SNMPv1/v2c/v3, HTTP
Características básicas	Método de comutação	Armazena e envia (Store-and-Forward)
	Capacidade comutação	104 Gbps
	Tabela de endereço MAC	16 K
	Jumbo frame	10240 Bytes
	Taxa de encaminhamento de pacote	77,3 Mpps
	VLAN	512 VLANs ativas
		4K
	Agregação de link (LAG)	6 grupos
		4 portas por grupos
	Multicast	256 grupos
	QOS (Quality of Service)	4 filas de prioridade
	Número de ACL	32
Características	Configuração de portas	Auto negociação
		Controle de fluxo
		Espelhamento de portas
		Estatísticas de tráfego
	Agregação de link	Agregação de link manual
		Agregação de link dinâmica (LACP)
		Algoritmo baseado em endereço MAC de origem e destino
		Algoritmo baseado em endereço IP de origem e destino
	Tabela MAC	Aging Time configurável
		Endereço MAC estático
		Endereço MAC dinâmico

Características	VLAN	512 VLANs ativa e 4K VLANs IDs
		VLAN baseado em Tag 802.1Q
		VLAN de gerenciamento
		Voice VLAN
	Spanning tree	802.1d Spanning Tree Protocol (STP)
		802.1w Rapid Spanning Tree Protocol (RSTP)
		802.1s Multiple Spanning Tree Protocol (MSTP)
		Loop Guard
		Root Guard
		TC-BPDU Guard
		BPDU Guard
		BPDU Filter
	Gerenciamento Multicast	IGMP v1/v2/v3
		IGMP Snooping
		Fast Leave
		Multicast VLAN
		Multicast estático
		Filtro Multicast
		Estatísticas IGMP
	QOS	4 Filas de prioridade
		Algoritmos de fila: SP, WRR, SP+WRR
		CoS baseado em portas
		CoS baseado em 802.1p
		CoS baseado em DSCP
		Storm Control (Broadcast, Multicast, Unicast desconhecido)
		Controle de banda por porta
	Segurança	Segurança das portas
		Isolamento das portas
		Filtro de endereço MAC
		ACL (L2/L3/L4)
		Classificação de pacotes baseados em: End. MAC, End. IP, Portas TCP/UDP, Tipo de Protocolo
		Filtro DHCP
		Restrição do acesso WEB baseado em: Endereço IP, End. MAC e Porta
	Gerenciamento	SNMP v1/v2c/v3
		RMON (4 grupos)
		Gerenciamento web (HTTP/HTTPs)
		CLI (Telnet, SSHv1/v2)
		SSLv2/SSLv3/TLSv1
		Espelhamento de porta
		Atualização de firmware via TFTP/web
		Configuração backup/reload
	Manutenção	DHCP Cliente
		BOOTP Cliente
		SNTP Cliente
		Teste virtual do cabo e detecção de Loopback
		Testes de Ping e Tracert
		Sistema de Log (Local e Remoto)
		Monitoramento de CPU e Memória
Alimentação	Entrada	100-240 VAC, 50/60 Hz
Ambiente	Temperatura de operação	0° C a 40° C
	Temperatura de armazenamento	-40° C a 70° C
	Umidade de operação	10% a 90% sem condensação
	Umidade de armazenamento	5% a 90% sem condensação
Emissão de segurança e outros		Anatel
		FCC Part 15 B Class A
		CE: EN55022, EN61000-3-2, EN61000-3-3, EN55024, EN60950-1
		RoHS

2.2. Visão geral do switch

Projetado para grupos de trabalho e departamentos, o switch SG 5200 MR 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. Filtro de Endereço MAC, Isolamento e Segurança das Portas fornecem uma robusta estratégia de segurança. O QoS e IGMP Snooping/Filtro otimizam as aplicações de voz e vídeo. A Agregação de Link permite o aumento da velocidade do link além dos limites nominais de uma única porta, evitando gargalos na rede. SNMP, RMON e Web trazem uma grande variedade de políticas de gerenciamento. O SG 5200 MR 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.

2.3. Principais funções

Resiliência e disponibilidade

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

Protocolos da camada de enlace

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

Qualidade de serviço

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

Gerenciamento

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

2.4. Descrição do produto

Painel frontal

O painel frontal do SG 5200 MR possui 52 portas Gigabit Ethernet, sendo 48 portas RJ45 e 4 slots Mini-GBIC independentes, 1 botão de *Reset* e LEDs de monitoramento.

Painel frontal

» **Portas 10/100/1000 Mbps:** 48 portas 10/100/1000 Mbps para conectar dispositivos com velocidade de 10 Mbps, 100 Mbps ou 1000 Mbps. Cada porta possui 1 LED correspondente.
» **Portas Mini-GBIC (SFP):** 4 portas Mini-Gbic para conectar módulos SFP 1000 Mbps. Cada porta possui 1 LED correspondente.
» **Reset:** botão utilizado para retornar as configurações do switch ao padrão de fábrica.

LEDs

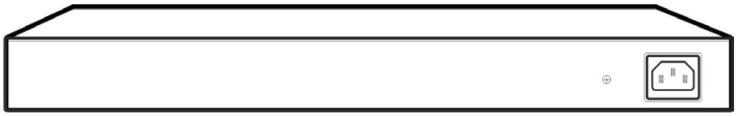
No painel frontal são apresentados 54 LEDs de monitoramento, que seguem o comportamento abaixo:

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

Obs.: *utilizar o slot Mini-GBIC (SFP) apenas com módulos 1000 Mbps. É necessário que a velocidade e o modo de transmissão correspondente ao módulo esteja configurado a 1000 MFD. Não é possível configurar o slot Mini-GBIC (SFP) com as opções (Auto, 10HD, 10FD, 100HD e 100FD).*

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.

3. Acesso à interface de gerenciamento

3.1. Login

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*.

Endereço IP

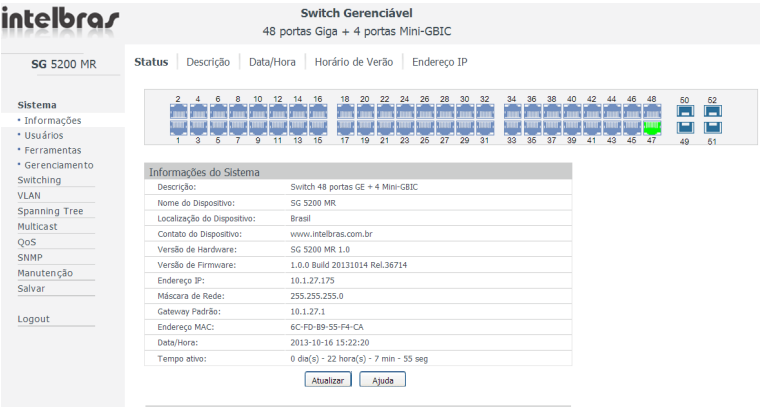
Obs.: *para efetuar o login no switch, o endereço IP do seu computador deve estar definido na mesma sub-rede utilizada pelo switch. O endereço IP de seu computador deve estar configurado como: 192.168.0.x (onde x é qualquer número de 2 à 254 com máscara de rede igual a 255.255.255.0).*

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 maiúsculas, em seguida, clique no botão *Login* ou pressione a tecla *Enter*.

Tela de login

3.2. Configuração

Após realizado o login, será possível configurar as funções do switch, clicando no menu de configuração localizado no lado esquerdo da tela, conforme imagem a seguir.



Tela de configuração

Obs.: *clicando em* Aplicar *as novas configurações ficarão ativas momentaneamente e serão perdidas ao reiniciar o switch. Para tornar as modificações permanentes no switch, por favor, clique em* Salvar.

4. Sistema

O menu *Sistema* é utilizado para configuração do switch e possui quatro submenus: *Informações, Usuários, Ferramentas e Gerenciamento.*

4.1. Informações

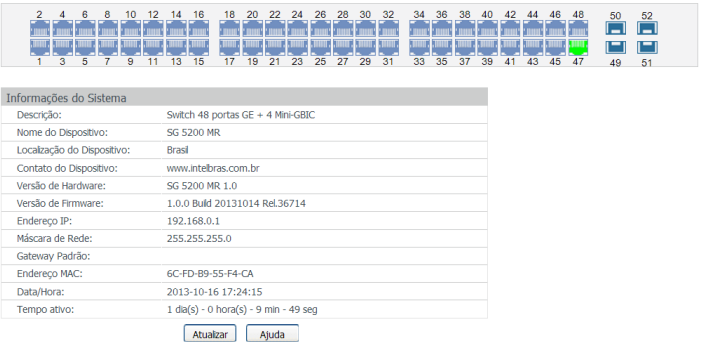
O submenu *Informações* é utilizado principalmente para as configurações básicas do switch. Este submenu possui os seguintes itens que podem ser configurados: *Status, Descrição, Data/Hora, Horário de Verão e Endereço IP.*

Status

Nesta página é possível visualizar o status das conexões das portas e as informações do sistema.

O diagrama de portas, exibe o status das 48 portas 10/100/1000 Mbps RJ45 e das 4 portas Mini-GBIC (SFP) do switch.

Escolha o menu *Sistema* → *Informações* → *Status* para carregar a seguinte página:



Status do sistema

» **Status das portas**


Indica que a porta 1000 Mbps não possui dispositivo conectado.

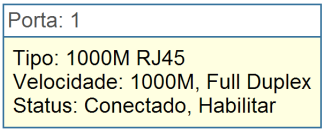

Indica que a porta 1000 Mbps possui um dispositivo 1000 Mbps conectado.


Indica que a porta 1000 Mbps possui um dispositivo 10 Mbps ou 100 Mbps conectado.


Indica que a porta Mini-Gbic (SFP) não possui dispositivo conectado.


Indica que a porta Mini-Gbic (SFP) possui um dispositivo 1000 Mbps conectado.

Ao passar o cursor do mouse por uma das portas, serão exibidas informações detalhadas referentes à porta desejada.



Detalhes da porta

» **Informações das portas**

Porta: exibe o número da porta do switch.

Tipo: exibe o tipo de porta do switch.

Velocidade: exibe a taxa de transmissão máxima da porta.

Status: exibe o status de conexão da porta.

Clique na porta desejada para visualizar a largura de banda utilizada. A figura a seguir, exibe a largura de banda utilizada pela porta. O monitoramento é realizado a cada quatro segundos, facilitando a análise de detecção de problemas.

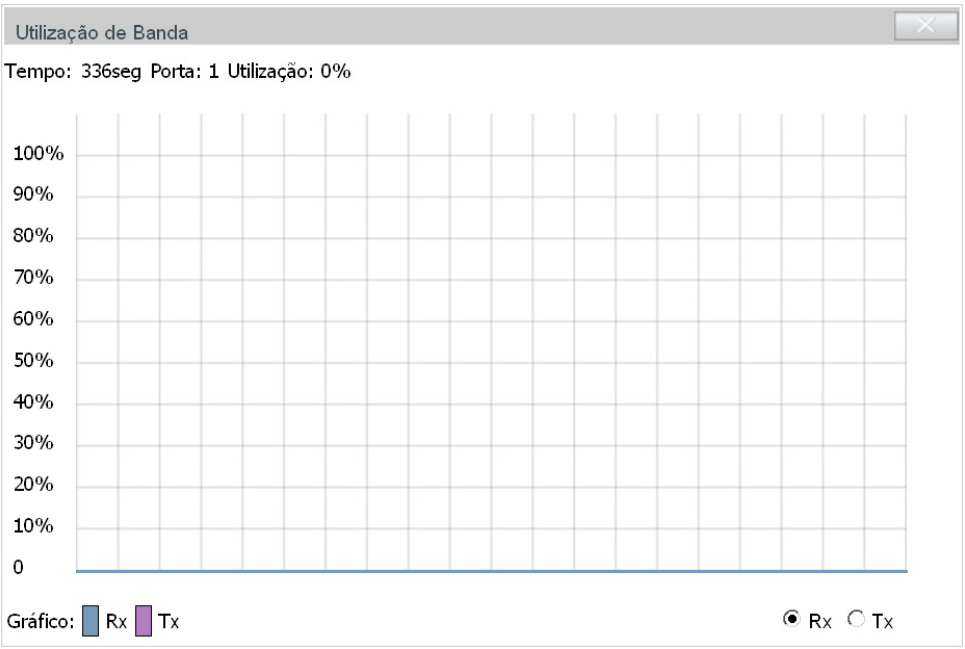


Gráfico de utilização da porta

» **Utilização de banda**

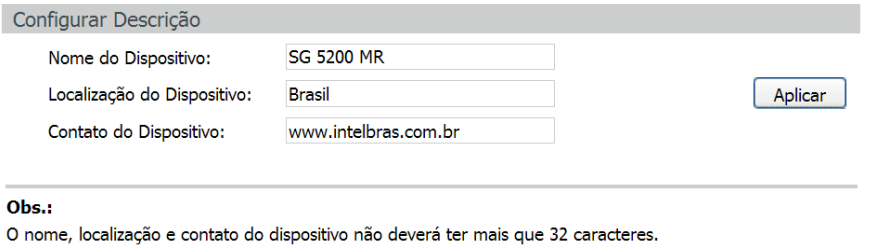
Rx: selecione *Rx* para exibir a banda utilizada durante a recepção de pacotes pela porta.

Tx: selecione *Tx* para exibir a banda utilizada durante a transmissão de pacotes pela porta.

Descrição

Nesta página você pode configurar a descrição do switch, incluindo o nome, localização e contato do dispositivo.

Escolha o menu *Sistema* → *Informações* → *Descrição* para carregar a seguinte página.



Descrição do switch

As seguintes opções são exibidas na tela:

» **Configurar descrição**

Nome do dispositivo: digite o nome de identificação do switch. Este campo permite no máximo 32 caracteres.

Localização do dispositivo: digite a localização do switch. Este campo permite no máximo 32 caracteres.

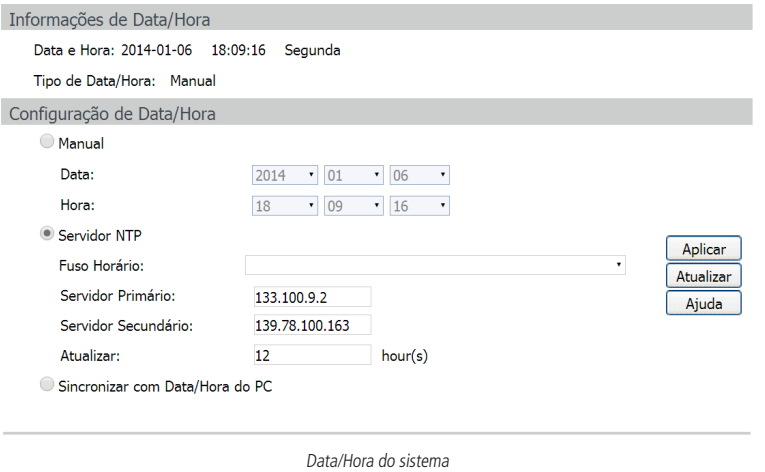
Contato do dispositivo: digite o contato do switch. Este campo permite no máximo 32 caracteres.

Data/Hora

Nesta página você pode configurar a data e hora do sistema que serão utilizadas por outras funções que necessitam deste tipo de informação, como por exemplo, *Registro de Log*.

A configuração poderá ser realizada de forma manual ou ainda sincronizando com a data e hora do computador.

Escolha o menu *Sistema* → *Informações* → *Data/Hora* para carregar a seguinte página:



Data/Hora do sistema

As seguintes opções são exibidas na tela:

» **Informações de data/hora**

Data e hora: informa a data e hora atual do sistema.

Tipo de data/hora: informa o modo de configuração da data e hora.

» **Configuração de data/hora**

Manual: quando esta opção estiver selecionada, você pode configurar a data e hora manualmente.

Servidor NTP: quando esta opção estiver selecionada, você pode configurar o fuso horário e o IP do servidor NTP. A mudança só ocorrerá após o switch se conectar ao servidor NTP.

Fuso horário: selecione o fuso horário desejado.

Servidor primário/secundário: digite o endereço IP primário e secundário do servidor NTP.

Atualizar: especifique o intervalo de tempo para consulta ao servidor NTP.

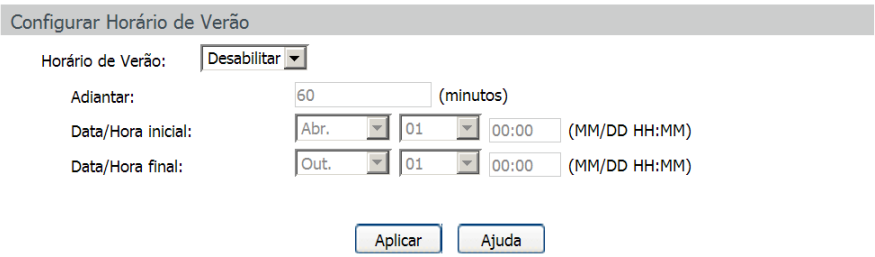
Sincronizar com data/hora do PC: ao selecionar esta opção, a data e hora do switch serão sincronizadas com a data e hora do computador que está administrando o switch.

Obs.: *a Data/Hora do switch será reiniciada para o padrão quando o switch for reiniciado.*

Horário de Verão

Nesta página você pode configurar a data e hora de início e término do horário de verão.

Escolha o menu: *Sistema* → *Informações* → *Horário de Verão* para carregar a seguinte página:



Horário de verão

As seguintes opções são exibidas na tela:

» **Configurar horário de verão**

Horário de Verão: habilita ou desabilita a função de horário de verão.

Adiantar: especifique o tempo em minutos que será adiantado ao horário atual do switch.

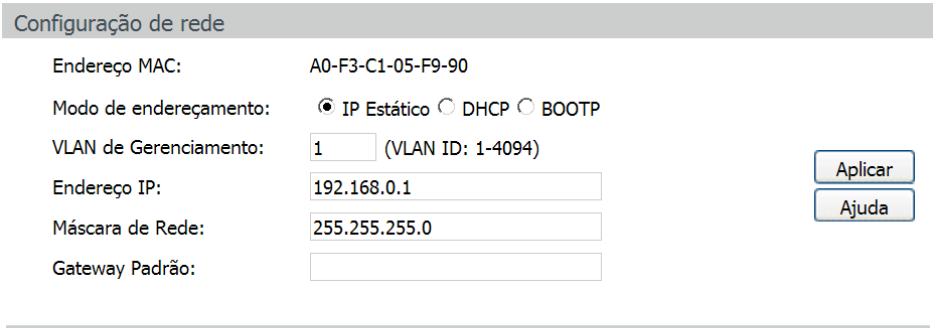
Data/Hora inicial: selecione o dia e hora de início do horário de verão.

Data/Hora final: selecione o dia e hora de término do horário de verão.

Endereço IP

Nesta página você pode configurar o endereço IP do swtich. Cada dispositivo na rede possui um endereço IP único. Você pode realizar o login na interface web de gerenciamento do switch através de seu endereço IP. O switch suporta três modos para obtenção do endereço IP: *Estático*, *DHCP* e *BOOTP*. Um endereço IP obtido utilizando um novo modo obtenção, substituirá o endereço IP corrente do switch.

Escolha o menu *Sistema* → *Informações* → *Endereço IP* para carregar a seguinte página:



Endereço IP

As seguintes opções são exibidas na tela:

» **Configuração de rede**

Endereço MAC: exibe o endereço MAC do switch.

Modo de endereçamento: selecione o modo como o switch obterá o endereço IP.

» **IP estático:** quando esta opção for selecionada, você deverá digitar o endereço IP, máscara de rede e gateway padrão manualmente.

» **DHCP:** quando esta opção for selecionada, o switch receberá o endereço IP e parâmetros de rede através de um servidor DHCP.

» **BOOTP:** quando esta opção for selecionada, o switch receberá o endereço IP e parâmetros de rede através de um servidor BOOTP.

» **VLAN de gerenciamento:** digite a VLAN de gerenciamento do switch. Somente através da VLAN de Gerenciamento é possível obter acesso à interface de gerenciamento web do switch. Por padrão, a VLAN de Gerenciamento e todas as portas do switch estão configuradas na VLAN 1. No entanto, se outra VLAN for criada e definida para ser a VLAN de Gerenciamento, será necessário reconectar o computador em uma porta que pertence a VLAN de Gerenciamento para poder ter acesso à interface web do switch.

» **Máscara de rede:** digite a máscara de sub-rede do switch quando estiver selecionado o modo IP Estático.

» **Gateway padrão:** digite o gateway padrão do switch quando estiver selecionado o modo IP Estático.

Obs.: » *Alterando o endereço IP, para um IP localizado em uma sub-rede diferente, ocorrerá perda na comunicação com o switch. Para isso não acontecer, mantenha o endereço IP do switch dentro da mesma sub-rede da rede local.*

» *O switch possui somente um endereço IP. O endereço IP é configurável substituindo o endereço IP original.*

» *Se for escolhida a opção DHCP ou BOOTP, o switch irá receber parâmetros de rede dinâmicamente, então o endereço IP, máscara de rede e gateway padrão não poderão ser configurados.*

» *Por padrão, o endereço IP do switch é* 192.168.0.1.

4.2. Usuários

O submenu *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: *Status dos Usuários e Configurar Usuários.*

Status dos usuários

Nesta página você pode visualizar informações sobre os usuários configurados no switch.

Escolha o menu *Sistema* → *Usuários* → *Status dos Usuários* para carregar a seguinte página:

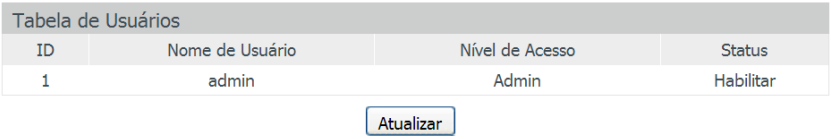
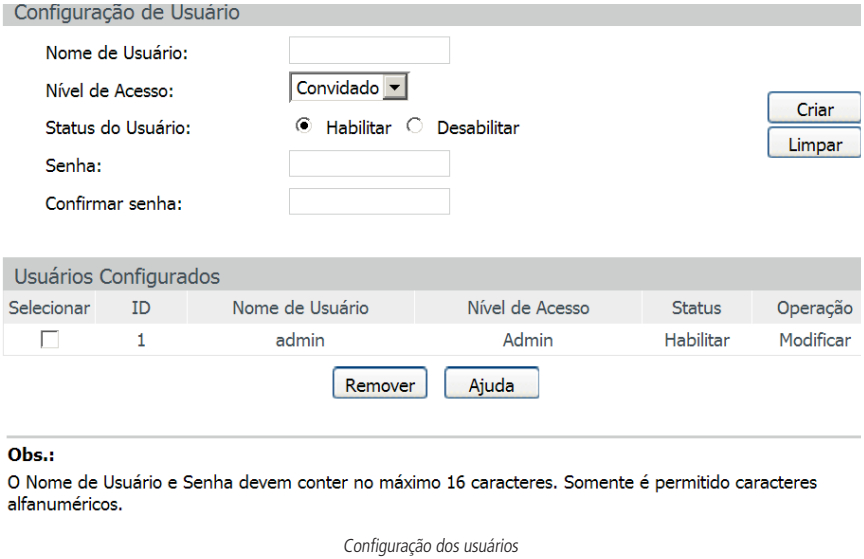


Tabela de usuários

Configurar usuários

Nesta página 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: *Convidado* e *Admin*. No nível de acesso convidado, somente é possível visualizar as configurações do switch, já no nível de acesso admin, é possível realizar a configuração de qualquer função presente no switch.

Escolha o menu *Sistema* → *Usuários* → *Configurar Usuários* para carregar a seguinte página:



Configuração dos usuários

» **Configuração de usuário**

Nome de usuário: digite o nome de usuário que será criado.

Nível de acesso: selecione o nível de acesso do usuário ao realizar login.

» **admin:** admin pode editar, modificar e visualizar todas as configurações.

» **convidado:** convidado somente pode visualizar as configurações sem poder configurá-las.

Status do usuário: selecione *Habilitar/Desabilitar* para habilitar ou desabilitar o usuário.

Senha: digite a senha desejada para o usuário realizar o login.

Confirmar senha: repita a senha para confirmá-la.

» **Usuários configurados**

Selecionar: selecione o usuário desejado e clique no botão *Remover* para excluir o usuário do sistema. O usuário corrente não poderá ser removido.

ID, nome de usuário, nível de acesso e status: exibe o ID, nome, nível de acesso e status do usuário.

Operação: clique em *Modificar* para editar as informações do usuário correspondente. Após modificar as configurações, clique no botão *Modificar* para validá-las. Não é possível modificar a configuração do usuário corrente.

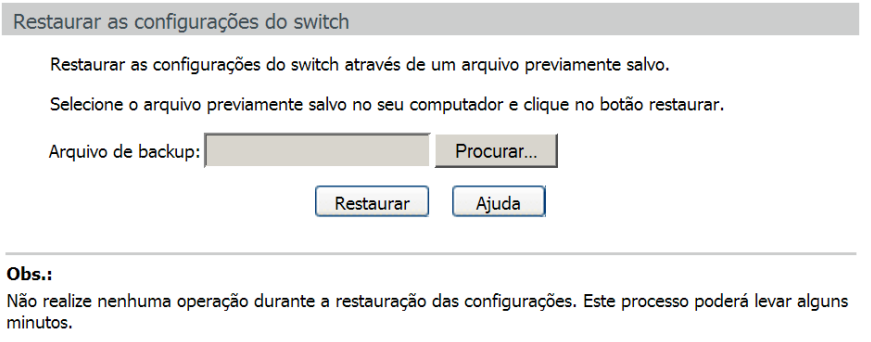
4.3. Ferramentas

No submenu *Ferramentas*, é possível gerenciar os arquivos de configuração do switch, atualizar o firmware, reiniciar e restaurar ao padrão de fábrica. Este submenu possui cinco itens de configuração: *Restaurar, Backup, Atualizar Firmware, Reiniciar e Restaurar Padrão.*

Restaurar

Nesta página você pode realizar o download de um arquivo de configuração previamente salvo, restaurando o switch para uma configuração anterior.

Escolha o menu *Sistema* ⟶ *Ferramentas* ⟶ *Restaurar* para carregar a seguinte página:



Restauração das configurações

As seguintes opções são exibidas na tela:

» **Restaurar as configurações do switch:**

Arquivo de backup: selecione o arquivo de configuração previamente salvo em seu computador e clique no botão *Restaurar* para restaurar as configurações.

Obs.: » *A restauração das configurações levará alguns segundos. Por favor, espere sem realizar nenhuma outra operação.*

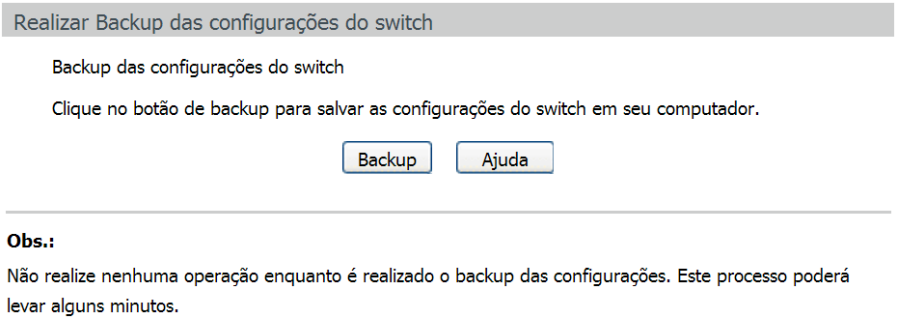
» *Enquanto as configurações estiverem sendo restauradas, não desligue o switch.*

» *Após serem restauradas, as configurações atuais serão perdidas, fazer o upload de um arquivo de backup errado pode fazer com que o switch perca o gerenciamento.*

Backup

Nesta página você poderá realizar o backup das configurações atuais do switch e salvá-los em um arquivo no seu computador, para uma restauração futura.

Escolha o menu *Sistema* ⟶ *Ferramentas* ⟶ *Backup* para carregar a página.



Backup das configurações

As seguintes opções são exibidas na tela:

» **Realizar backup das configurações do switch**

Backup: clique no botão *Backup* para salvar as configurações atuais em um arquivo no seu computador. Essa sugestão pode ser adotada antes de realizar uma atualização das configurações do switch.

Obs.: *o backup das configurações poderá levar alguns minutos.*

Atualizar firmware

O Firmware do switch pode ser atualizado através da página de gerenciamento web. Para atualizar o sistema com a versão mais recente do firmware, faça o download através do site da Intelbras *www.intelbras.com.br.* É recomendável que seja feito um backup das configurações do switch antes do procedimento, pois a atualização do firmware pode causar a perda de todas as configurações existentes.

Escolha no menu *Sistema* → *Ferramentas* → *Atualizar Firmware* para carregar a seguinte página:

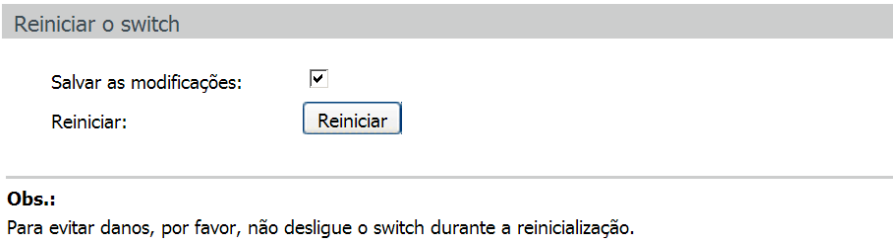
Atualização do firmware

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

Reiniciar

Nesta página é possível reiniciar o switch e retornar a página de login. Para evitar a perda das configurações realizadas ao reiniciar o switch, marque a opção *Salvar as modificações.*

Escolha o menu *Sistema* → *Ferramentas* → *Reiniciar* para carregar a seguinte página.



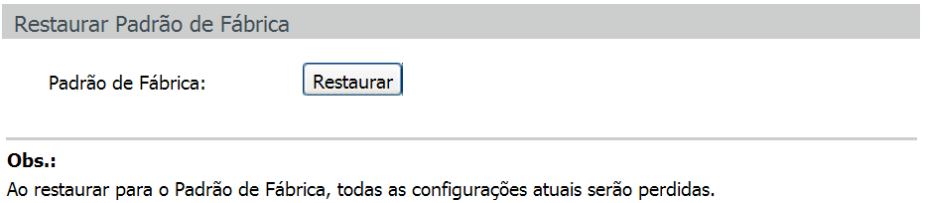
Reiniciando o sistema

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

Restaurar padrão

Nesta página você pode restaurar o switch para a configuração padrão de fábrica. Todas as configurações serão perdidas após o switch reiniciar.

Escolha no menu *Sistema* → *Ferramentas* → *Restaurar Padrão* para carregar a página.



Restaurando para o padrão de fábrica

Obs.: *após o sistema reiniciar, todas as configurações serão restauradas para o padrão de fábrica.*

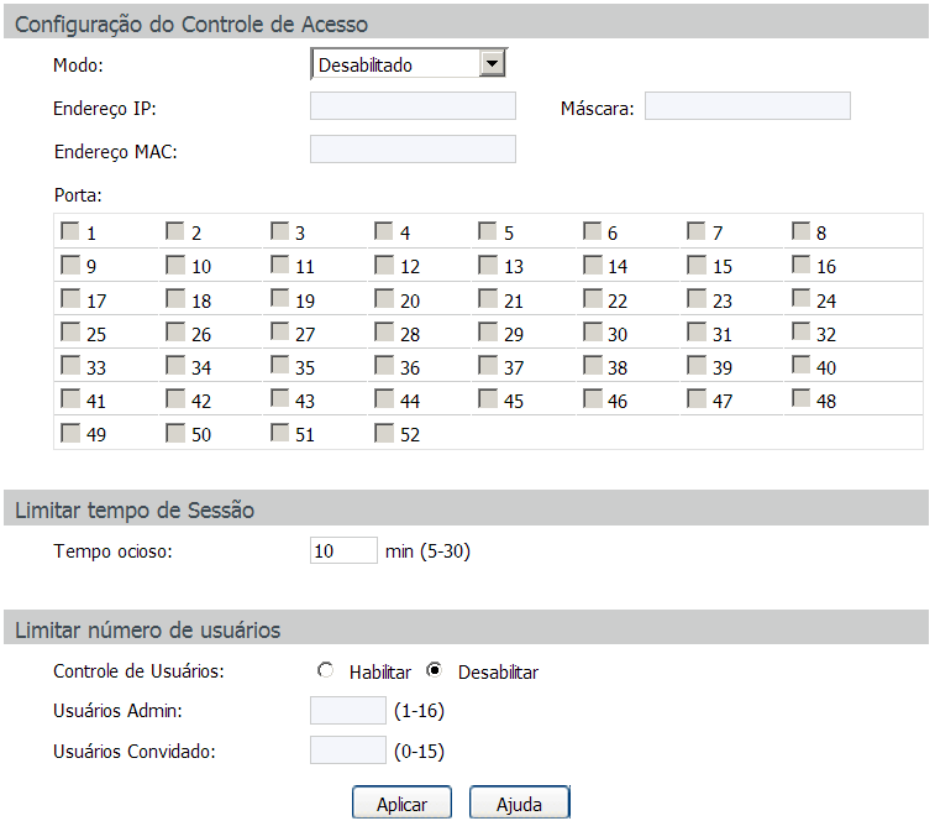
4.4. Gerenciamento

O submenu *Gerenciamento* possui diferentes tipos de segurança para login remoto, aumentando o nível de segurança no gerenciamento do switch. Você pode realizar essas configurações através de três itens de configuração: *Controle de Acesso*, *SSL* e *SSH*.

Controle de acesso

Nesta página você poderá controlar os usuários que acessarão a página de gerenciamento web. Para melhorar as configurações de segurança, utilize os níveis de acesso de usuário, explicado no capítulo *4.2.Usuários.*

Escolha o menu *Sistema* → *Gerenciamento* → *Controle de Acesso* para carregar a seguinte página.



Controle de acesso

As seguintes informações são exibidas na tela:

» **Configuração do controle de acesso**

Modo: selecione o modo de controle de login para a página de gerenciamento web do switch.

» **Baseado em IP:** selecione esta opção para especificar os endereços IPs dos computadores que poderão realizar login no switch.

» **Baseado em MAC:** selecione esta opção para especificar os endereços MACs dos computadores que poderão realizar login no switch.

» **Baseado em porta:** selecione esta opção para especificar em quais portas do switch os computadores deverão estar conectados para poder realizar login no switch.

Endereço IP e máscara: este campo somente estará disponível quando for selecionado o modo de controle *Baseado em IP*. Somente o os computadores que estiverem dentro da faixa de endereços IPs poderão realizar login no switch.

Endereço MAC: este campo somente estará disponível quando for selecionado o modo de controle *Baseado em MAC*. Somente os computadores que estiverem dentro da faixa de endereços MAC poderão realizar login no switch.

Porta: este campo somente estará disponível quando for selecionado o modo de controle *Baseado em Porta*. Somente os computadores que estiverem conectados as portas correspondentes poderão realizar login no switch.

» **Limitar tempo de sessão**

Tempo ocioso: tempo em minutos de ociosidade do switch para desconectar o usuário. O tempo varia entre 5 e 30 minutos, o padrão é de 10 minutos.

» **Limitar número de usuários**

Controle de usuários: selecione *Habilitar/Desabilitar* para habilitar ou desabilitar a função de controle do número de usuário.

Usuários admin: digite o número máximo de usuários que poderão logar simultaneamente no switch com nível de acesso admin. Este número varia de 1 a 16 usuários.

Usuários convidados: digite o número máximo de usuários que poderão logar simultaneamente no switch com nível de acesso convidado. Este número varia de 0 a 15 usuários.

SSL

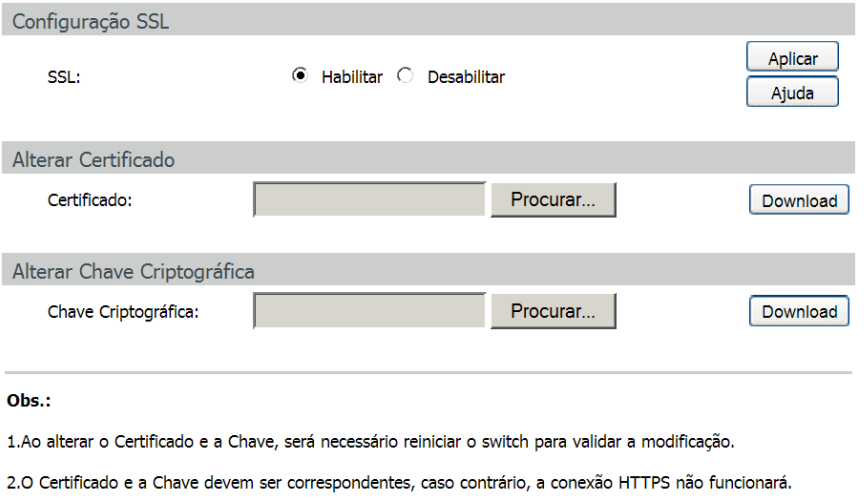
SSL (Secure Sockets Layer) é um protocolo de segurança que fornece uma conexão segura na camada de aplicação do modelo OSI (por exemplo, HTTP). Este protocolo é utilizado para proteger a transmissão de dados entre o navegador da web e o servidor de destino, sendo amplamente utilizado pelo comércio eletrônico e serviços bancários on-line. O SSL oferece os seguintes serviços:

1. Autenticar os usuários e os servidores com base em certificados, assegurando que os dados serão transmitidos para os servidores e usuários corretos.
2. Encriptação dos dados transmitidos, prevenindo uma interceptação ilegal dos pacotes.
3. Manter a integridade dos dados, garantindo que não serão alterados na transmissão.

Adotando a tecnologia de criptografia assimétrica, o SSL utiliza um par de chaves para criptografar e descriptografar as informações. Este par de chaves é referenciado como chave pública (contidas no certificado) e sua chave privada correspondente. Por padrão o switch possui um certificado autoassinado e uma chave privada correspondente. As opções *Alterar Certificado* e *Alterar Chave Criptográfica* permitem ao usuário substituir o par de chaves padrão do switch.

Após o SSL estar em funcionamento, você poderá realizar login na interface web de gerenciamento do switch de forma segura, digitando *https://192.168.0.1*. Na primeira vez que você logar no switch com o SSL ativado, será exibida uma mensagem de erro de certificado, como por exemplo, "O Certificado de Segurança apresentado pelo site não foi emitido por uma Autoridade de Certificação confiável" ou "Erros de certificado". Por favor, adicione este certificado para certificados confiáveis de seu navegador web ou clique em continuar no site.

Escolha no menu *Sistema* → *Gerenciamento* → *SSL* para carregar a seguinte página:



Configuração SSL

As seguintes opções são exibidas na tela:

» **Configuração SSL**

SSL: selecione *Habilitar/Desabilitar* para habilitar ou desabilitar a função SSL do switch.

» **Alterar certificado**

Certificado: selecione o certificado que deseja transferir para o switch, o certificado deverá ser codificado em BASE64.

» **Alterar chave criptográfica**

Chave criptográfica: selecione a chave que deseja transferir para o switch. A chave deve ser codificada em BASE64.

Obs.: » *O certificado SSL e a chave devem ser correspondentes, caso contrário a conexão SSL não irá funcionar.*

» *O certificado SSL e a chave somente estarão em funcionamento após o reinício do switch.*

» *Para estabelecer uma conexão segura durante a configuração do switch, digite na barra de endereço de seu navegador https://192.168.0.1.*

» *Uma conexão HTTPS pode demorar um pouco mais que uma conexão HTTP, isso porque em uma conexão HTTPS envolve autenticação, criptografia e descriptografia.*

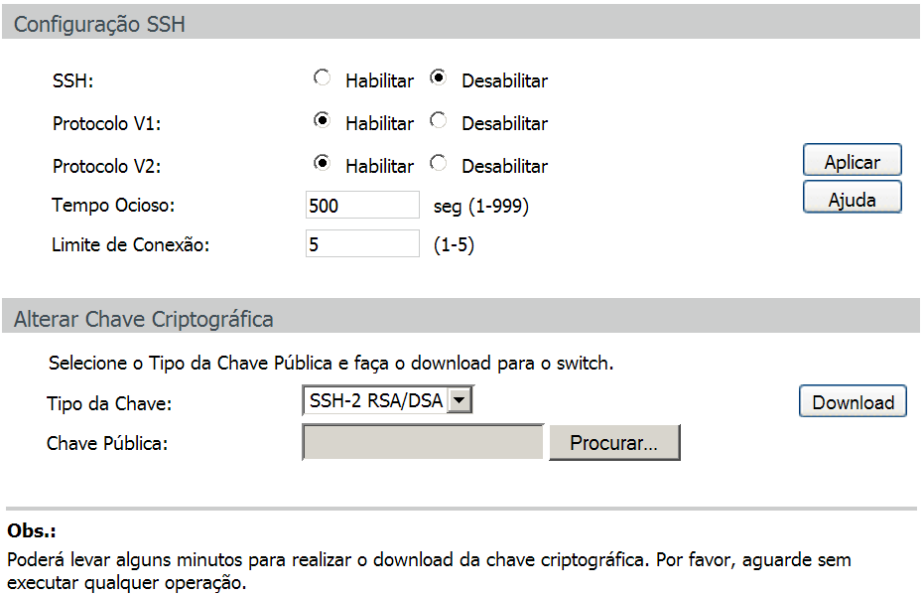
SSH

Conforme estipulado pela IETF (*Internet Engineering Task Force*), o SSH (*Secure Shell*) é um protocolo de segurança estabelecido nas camadas de transporte e aplicação. A conexão criptografada do SSH é semelhante a uma conexão telnet, porém as conexões remotas como o telnet não são seguras, pois as senhas e os dados são transmitidos em forma de texto claro, isto é, não possui criptografia, sendo facilmente captadas e interpretadas por pessoas não autorizadas. O SSH provê informações de autenticação segura mesmo que você se autentique no switch através de um ambiente de rede inseguro. Ele criptografa todos os dados envolvidos na transmissão e evita que as informações sejam interpretadas.

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 utilizará. 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.

O switch possui a função de servidor SSH, com isso, você pode instalar em seu computador um software SSH cliente para se conectar ao switch. Uma chave SSH pode ser salva no switch, se a chave for salva com êxito, a autenticação do certificado dará preferência a essa chave.

Escolha no menu *Sistema* → *Gerenciamento* → *SSH* para carregar a seguinte página:



Configuração SSH

As seguintes informações são exibidas na tela:

» **Configuração SSH**

SSH: selecione *Habilitar/Desabilitar* para habilitar ou desabilitar a função SSH.

Protocolo V1: selecione *Habilitar/Desabilitar* para habilitar ou desabilitar a versão v1 do SSH.

Protocolo V2: selecione *Habilitar/Desabilitar* para habilitar ou desabilitar a versão v2 do SSH.

Tempo ocioso: digite o tempo em segundos que o switch aguardará para desconectar a conexão SSH, caso esteja ociosa. Por padrão este tempo é de *500 segundos* e pode variar de 1 a 999 segundos.

Limite de conexão: digite o número máximo de conexões SSH que o switch suportará simultaneamente. O valor padrão é *5* e pode variar de 1 a 5.

» **Alterar chave criptográfica**

Tipo da chave: selecione o tipo da chave que será utilizado pelo SSH. O switch suporta três tipos: SSH-1 RSA, SSH-2 RSA e SSH2-DSA.

Chave pública: selecione a chave correspondente ao tipo de chave utilizado para download.

Download: clique no botão *Download* para salvar a nova Chave Criptográfica no switch.

Obs.: » *Por favor, tenha certeza que a chave SSH transferida possua tamanho entre 256 e 3072 bits.*

» *Após salvar a nova chave SSH, a chave original será substituída.*

» *Caso uma chave SSH seja salva erradamente, o acesso SSH será realizado através da senha de autenticação.*

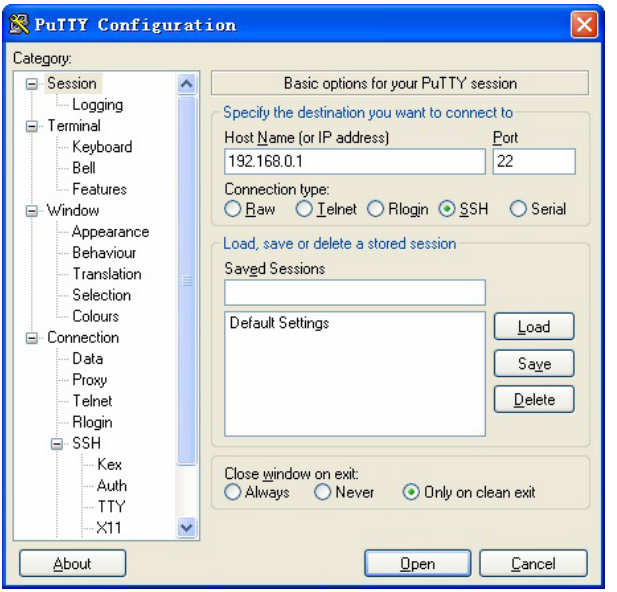
Primeiro exemplo de aplicação SSH

» **Requisitos de rede**

1. Faça login no switch utilizando um software cliente SSH. A função *SSH* do switch deverá estar habilitada.
2. Recomendamos o uso do programa PuTTY como software cliente SSH.

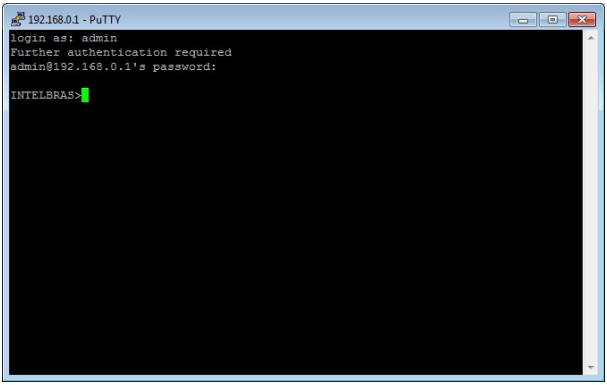
» **Procedimento de configuração**

1. Abra o programa PuTTY e digite o endereço IP do switch no campo Host Name (or IP address), mantenha o valor padrão do campo Port como 22, selecione *Connection type* como SSH, conforme imagem a seguir.



Configuração do PuTTY

2. Clique no botão *Open* para fazer o login no switch. Será exibido um terminal de linha de comandos, digite o nome de usuário e senha do switch (usuário e senha padrão do switch é *admin*), após realizar o login, será possível gerenciar o switch através do terminal de linha de comando, conforme imagem a seguir.



Terminal de linha de comandos

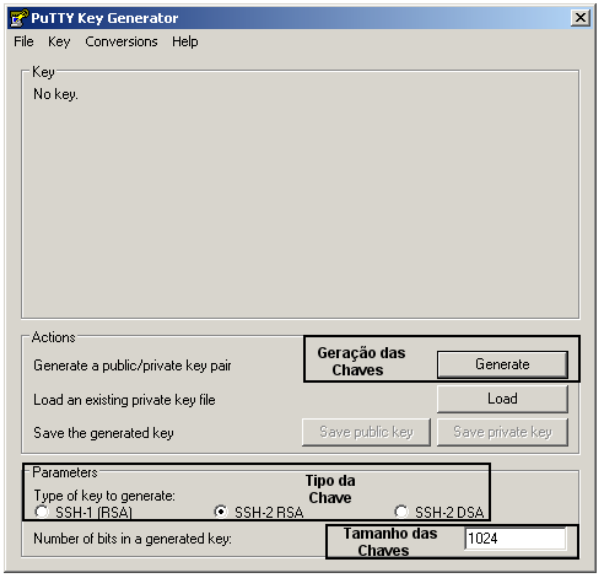
Segundo exemplo de aplicação SSH

» **Requisitos de rede**

1. Faça Login no switch utilizando um software cliente SSH, com chaves criptográficas geradas pelo usuário. A função SSH do switch deverá estar habilitada.
2. Recomendamos o uso do programa PuTTY como software cliente SSH, PuTTY Key Generator para a geração das novas chaves criptográficas e Pageant Key List para carregar a chave privada gerada. Todos estes programas estão disponíveis para download gratuitamente no site do fabricante do software PuTTY.

» **Procedimento de configuração**

1. Abra o programa PuTTY Key Generator, selecione o tipo e o comprimento da chave SSH e clique no botão *Generate*, conforme imagem a seguir:

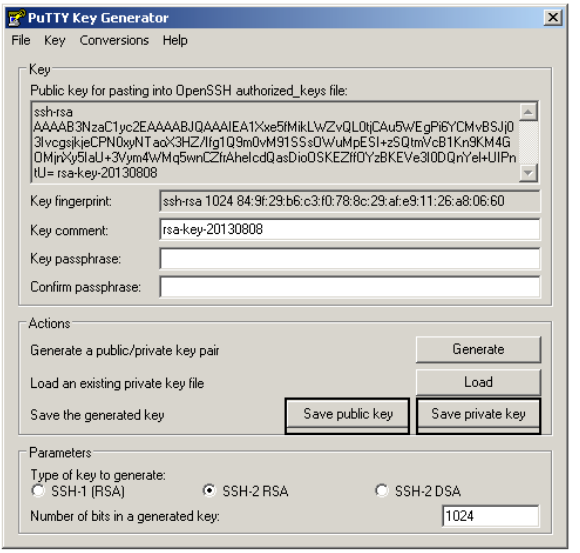


PuTTY key generator

Obs.: » *O comprimento da chave SSH deverá possuir tamanho entre 256 e 3072 bits.*

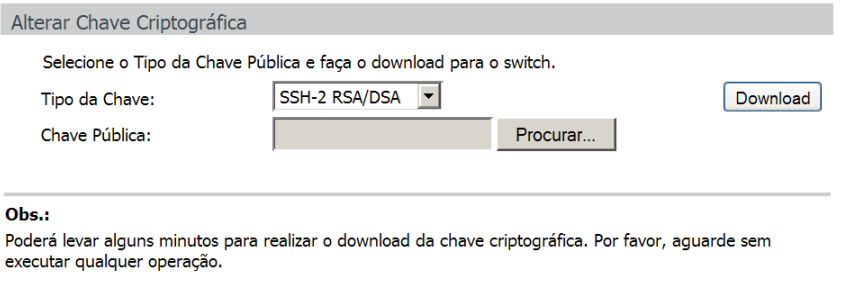
» *Durante a geração da chave SSH, mova o cursor do mouse aleatoriamente para auxiliar no processo de geração da chave.*

2. Após as chaves serem geradas com sucesso, por favor, salve-as em seu computador, utilizando os botões Save public key e Save private key, conforme imagem a seguir:



PuTTY key generator

3. Na página de gerenciamento web do switch, faça o download da chave pública gerada, que está salva em seu computador para o switch, conforme imagem a seguir:

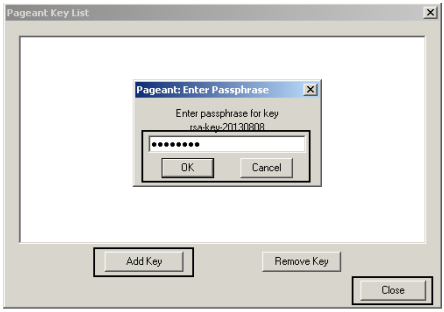


Download da chave SSH

Obs.: » *O tipo da chave selecionada no switch deverá estar de acordo com o tipo da chave criada pelo software PuTTY Key Generator.*

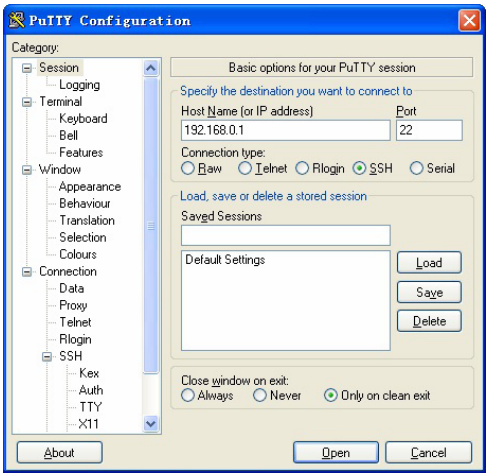
» *Não interrompa o download da chave SSH.*

4. Utilize o programa Pageant Key List para carregar a chave privada criada, que será utilizada pelo software cliente SSH, conforme imagem a seguir:



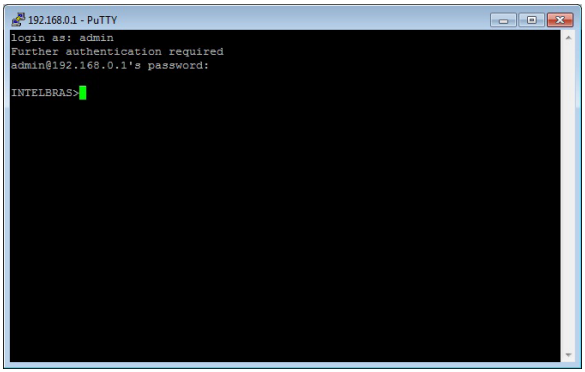
Carregando a chave privada

5. Após os procedimentos de criação e carregamento das chaves criptográficas, por favor acesse a interface do PuTTY e insira o endereço IP para login no switch, conforme imagem a seguir:



Conectando no switch via SSH

Após autenticação bem sucedida, digite o nome de usuário. Se você fizer login no switch sem precisar digitar a senha, significa que a chave foi salva com êxito, conforme imagem a seguir.



Autenticação bem sucedida

5. Switching

O menu *Switching* é utilizado para as configurações básicas do switch, incluindo cinco submenus: *Portas*, *Agregação de Link*, *Tráfego*, *Endereço MAC* e *Filtro DHCP*.

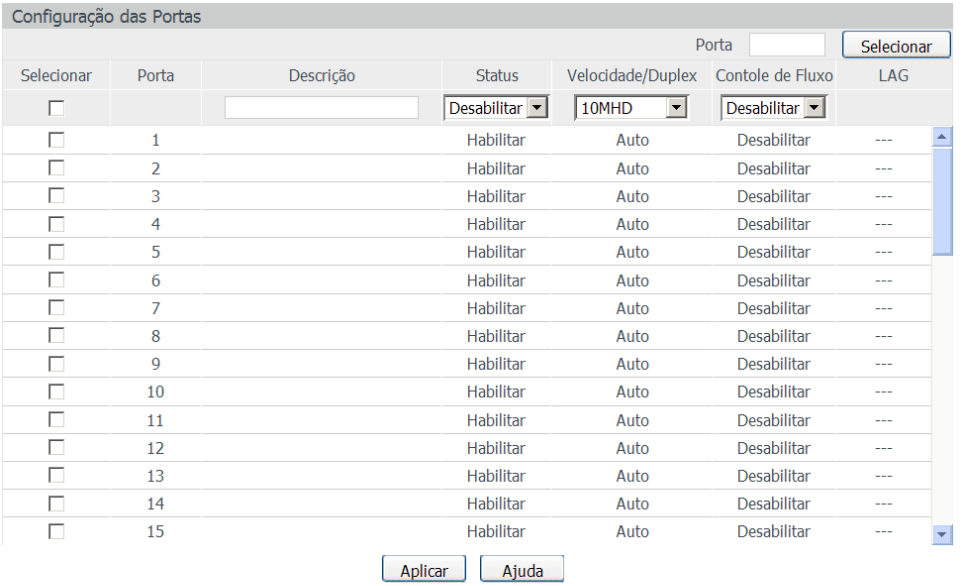
5.1. Portas

O submenu *Portas* permite configurar recursos básicos utilizados pelas portas do switch, a configuração pode ser realizada nas seguintes páginas: *Configurar Portas, Espelhar Portas, Segurança das Portas, Isolamento das Portas* e *Detecção de Loopback*.

Configurar portas

Nesta página são configurados os parâmetros básicos para as portas, quando a porta está desativada todos os pacotes serão descartados. Todos os parâmetros afetarão o modo de funcionamento das portas, por favor, defina os parâmetros conforme sua necessidade.

Escolha o menu *Switching* → *Portas* → *Configurar Portas* para carregar a seguinte página:



Obs.:
A Descrição da Porta deverá ter no máximo 16 caracteres.

Parâmetros das portas

As seguintes informações são exibidas na tela:

» **Configuração das portas**

Porta: digite o número da porta desejada dentro do campo correspondente e clique no botão *Selecionar* para selecionar a porta.

Selecionar: selecione a porta desejada para realizar a configuração. É possível selecionar mais de uma porta simultaneamente.

Porta: exibe o número da porta.

Descrição: digite uma descrição para a porta.

Status: selecione *Habilitar/Desabilitar* para habilitar ou desabilitar a porta correspondente. Quando a porta estiver habilitada o switch poderá encaminhar os pacotes normalmente.

Velocidade/Duplex: selecione a velocidade e o modo *Duplex* para porta. 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 auto negociação. As portas SFP não suportam auto negociação.

Controle de fluxo: selecione *Habilitar/Desabilitar* para habilitar ou desabilitar o 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.

LAG: exibe o número do grupo LAG a qual a porta pertence.

Obs.: » *Não desabilite a porta usada para o gerenciamento do switch.*

» *As portas membros de um grupo LAG devem possuir os mesmos parâmetros de configuração de porta.*

» *Os slots Mini-GBIC (SFP) apenas aceitam módulos 1000 Mbps. Por padrão as portas SFP vem configurado com velocidade e modo de operação 1000 MFD.*

Espelhar portas

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

Escolha o menu *Switching* → *Portas* → *Espelhar Portas* para carregar a seguinte página:

Espelhamento de Porta

Grupo	Porta Espelho	Modo	Porta Espelhada	Operação
1	0	Entrada	---	Modificar
		Saída	---	
2	0	Entrada	---	Modificar
		Saída	---	
3	0	Entrada	---	Modificar
		Saída	---	
4	0	Entrada	---	Modificar
		Saída	---	

Ajuda

Espelhamento de portas

As seguintes opções são exibidas na tela:

» **Espelhamento de porta**

Grupo: exibe o número do grupo de espelhamento de portas.

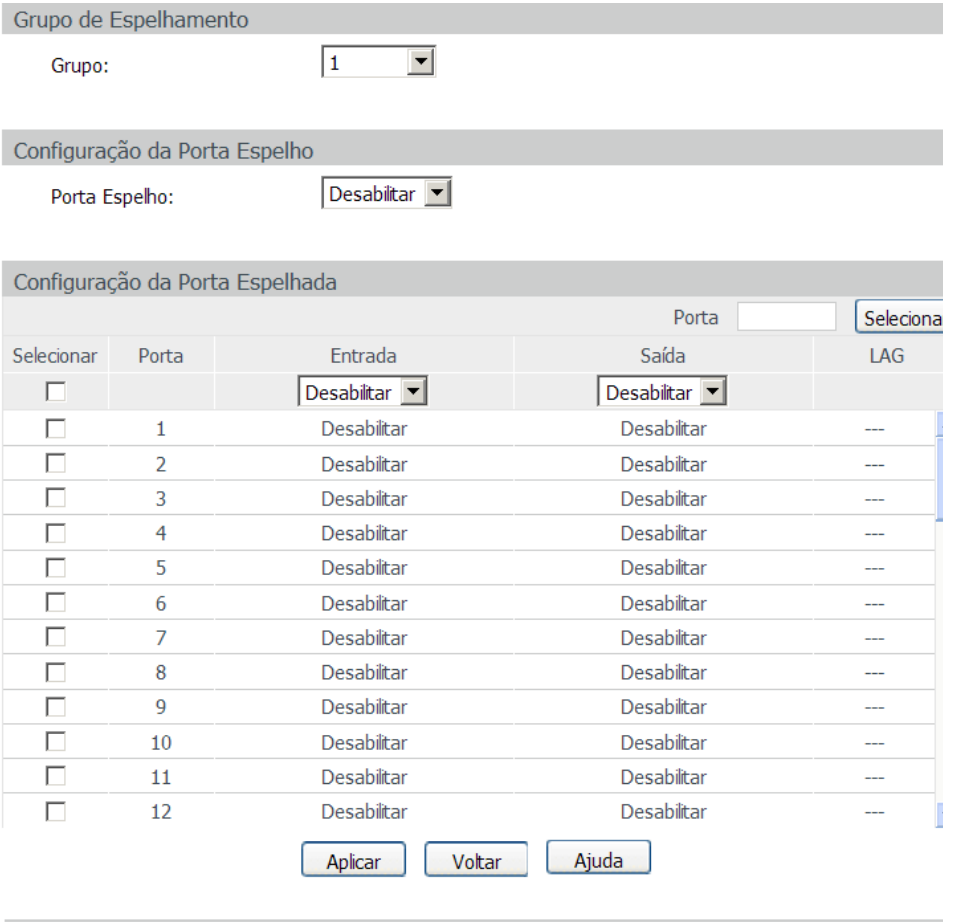
Porta espelho: exibe o número da porta espelho.

Modo: exibe a direção dos pacotes espelhados, "Entrada" pacotes recebidos, "Saída" pacotes enviados.

Porta espelhada: exibe as portas espelhadas.

Operação: clique em *Modificar* para configurar o grupo de espelhamento de portas.

Ao clicar em *Modificar*, será exibido a seguinte página:



Configuração do espelhamento de portas

As seguintes informações são exibidas na tela:

» **Grupo de espelhamento**

Grupo: selecione o grupo de espelhamento de portas que deseja configurar.

» **Configuração da porta espelho**

Porta espelho: selecione a porta espelho.

» **Configuração da porta espelhada**

Porta: digite o número da porta espelhada dentro do campo correspondente e clique no botão *Selecionar* para selecionar a porta.

Selecionar: selecione a porta espelhada desejada. É possível selecionar mais de uma porta simultaneamente.

Porta: exibe o número da porta.

Entrada: selecione *Habilitar/Desabilitar* para habilitar ou desabilitar o recurso de encaminhamento dos pacotes recebidos pela porta espelhada. Uma cópia desses pacotes será enviada para a porta espelho.

Saída: selecione *Habilitar/Desabilitar* para habilitar ou desabilitar o recurso de encaminhamento dos pacotes enviados pela porta espelhada. Uma cópia desses pacotes será enviada para a porta espelho.

LAG: exibe o número do grupo LAG que a porta pertence. Uma porta membro de um grupo LAG não pode ser selecionada como porta espelhada ou porta espelho.

Obs.: » *Portas membros de um grupo LAG não podem ser selecionadas como porta espelhada ou porta espelho.*

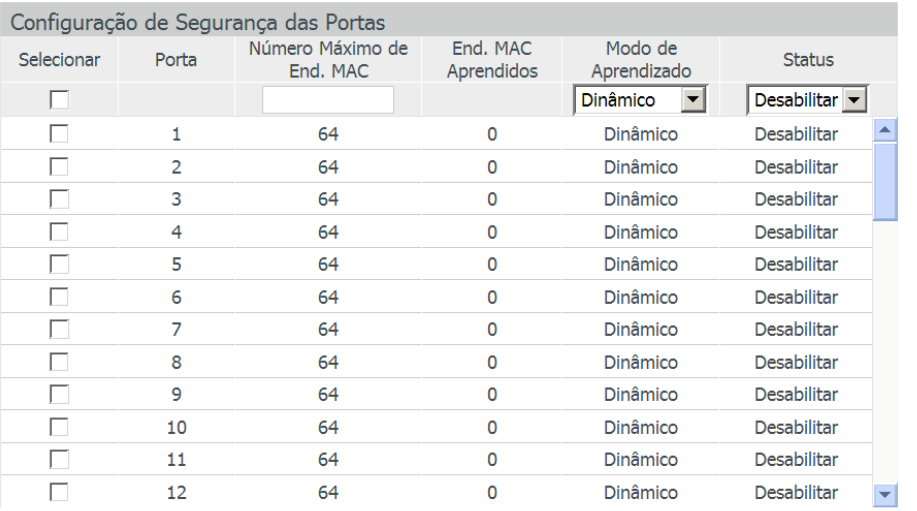
» *Uma porta não pode ser simultaneamente porta espelhada e porta espelho.*

» *A função de espelhamento abrange varias VLANs.*

Segurança das portas

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

Escolha no menu *Switching* → *Portas* → *Segurança das Portas* para carregar a seguinte página:



Segurança das portas

As seguintes informações são apresentadas na tela:

» **Configuração de segurança das portas**

Selecionar: selecione a porta que será configurada a segurança. É possível selecionar mais de uma porta simultaneamente.

Porta: exibe o número da porta.

Número máximo de end. MAC: especifique o número máximo de endereços MAC que poderão ser aprendidos pelo switch na porta desejada.

End. MAC aprendidos: exibe o número de endereços MAC que já foram aprendidos pela porta.

Modo de aprendizado: selecione o modo de aprendizagem da porta.

» **Dinâmico:** neste modo, o endereço MAC será aprendido de forma automática e excluído após o término do Aging Time (tempo de envelhecimento) da Tabela de Endereços MAC.

» **Estático:** neste modo, o endereço MAC deverá ser incluído ou removido manualmente, os endereços MAC estático não possuem Aging Time (tempo de envelhecimento).

» **Permanente:** neste modo, as entradas aprendidas somente poderão ser removidas manualmente, não possuem Aging Time (tempo de envelhecimento) e não serão removidas ao reiniciar o switch.

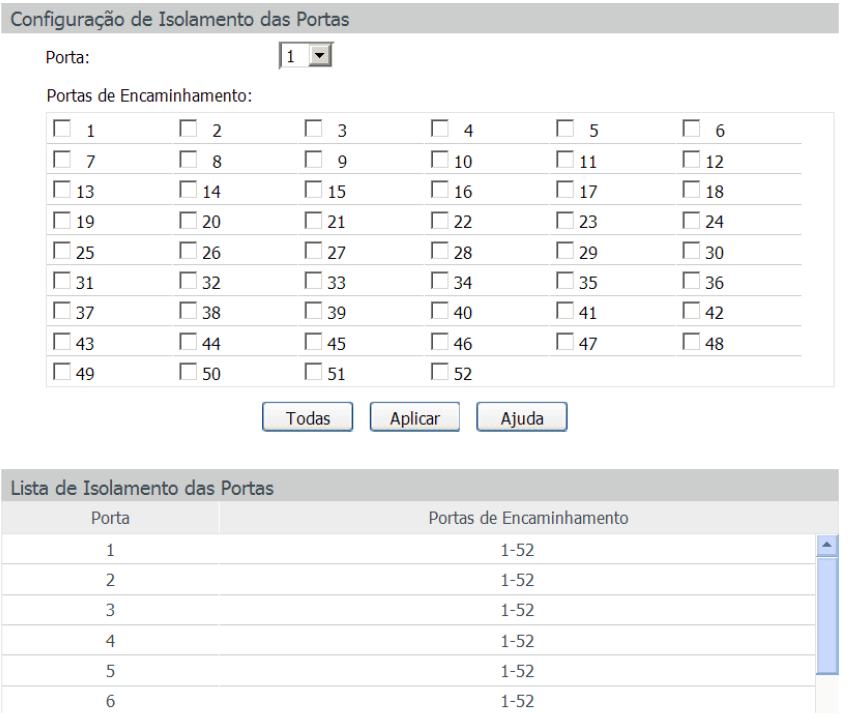
» **Status:** selecione *Habilitar/Desabilitar* para habilitar ou desabilitar a função *Segurança das Portas* para a porta desejada.

Obs.: *a função* Segurança das Portas *será desabilitada para as portas membros de grupos LAG.*

Isolamento das portas

O Isolamento das Portas fornece um método para restringir o fluxo do tráfego para melhorar a segurança da rede. Esta função basicamente permite que uma porta somente possa encaminhar pacotes para as portas que estão em sua lista de encaminhamento. Este método de segmentar o fluxo do tráfego é semelhante a utilização de VLANs, porém com mais restrições de configuração.

Escolha no menu *Switching* → *Portas* → *Isolamento das Portas* para carregar a seguinte página:



Isolamento das portas

As seguintes informações são apresentadas na tela:

» **Configuração de isolamentos das portas**

Porta: selecione a porta que será configurada como Porta Isolada.

Portas de encaminhamento: selecione as portas que poderão se comunicar com a porta configurada como Porta Isolada. É possível selecionar mais de uma porta simultaneamente.

» **Lista de isolamento das portas**

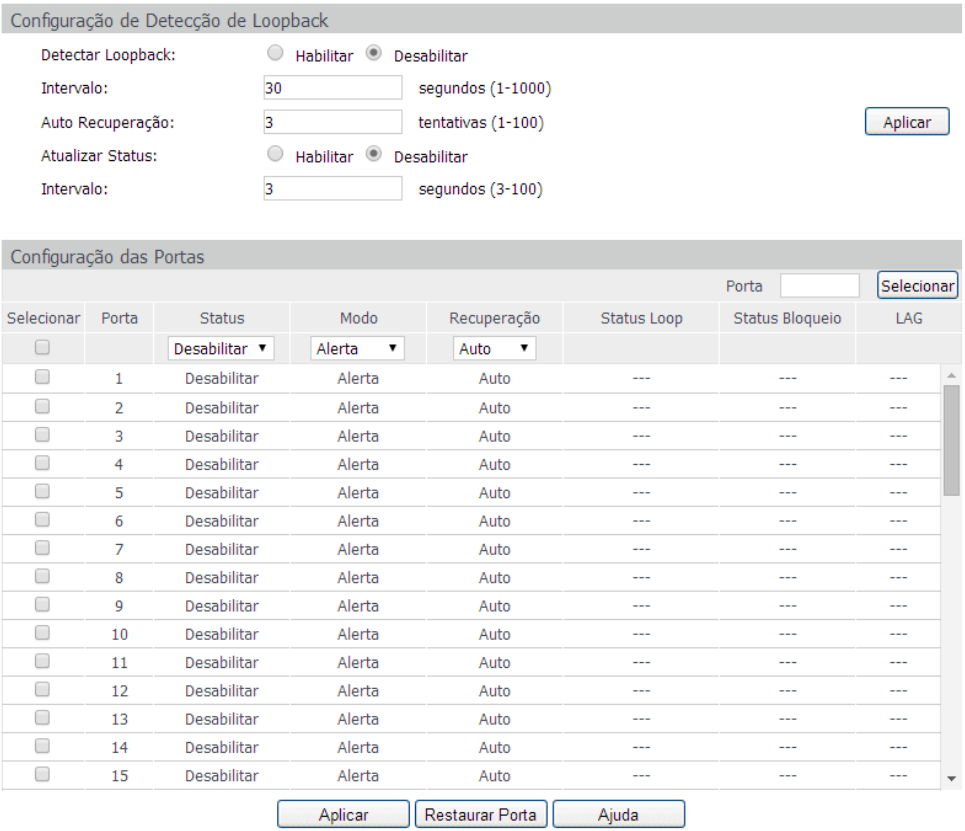
Porta: exibe o número da porta do switch.

Portas de encaminhamento: exibe a lista de portas que poderão se comunicar com a porta configurada como Porta Isolada.

Detecção de loopback

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

Escolha no menu *Switching* → *Portas* → *Detecção de Loopback* para carregar a seguinte página:



Detecção de loopback

As seguintes informações são apresentadas na tela:

» **Configuração de detecção de loopback**

Detectar loopback: selecione *Habilitar* ou *Desabilitar* a função de detecção de loopback.

Intervalo: digite o intervalo de tempo em que o switch tentará detectar loop em suas portas.

Auto recuperação: digite a quantidade de tentativas para a recuperação automática da porta quando um loop for detectado. A quantidade de tentativas X intervalo de detecção é igual ao tempo, em segundos, para a recuperação automática da porta.

Atualizar status: selecione *Habilitar* ou *Desabilitar* a atualização do status das portas pertencentes a função de detecção de loopback.

Intervalo: digite o intervalo de tempo em que o switch ficará atualizando o status das portas pertencentes a função de detecção de loopback.

» **Configuração das portas**

Porta selecionar: digite a porta desejada no campo correspondente e clique no botão *Selecionar* para escolher a porta.

Selecionar: selecione a porta desejada. Nesta opção você poderá selecionar mais de uma porta simultaneamente.

Porta: exibe o número da porta do switch.

Status: selecione *Habilitar* ou *Desabilitar* a função de detecção de loop na porta desejada.

Modo: selecione o modo de operação quando um loop é detectado.

» **Alerta:** quando um loop é detectado, é exibido um alerta.

» **Bloquear:** quando um loop é detectado, é exibido um alerta e a porta é bloqueada.

Recuperação: selecione o modo de recuperação da porta quando o estado da porta estiver bloqueado.

» **Auto:** neste modo, a porta será desbloqueada automaticamente após o término do prazo de auto recuperação.

» **Manual:** neste modo, a porta só poderá ser desbloqueada de forma manual, clicando no botão *Restaurar Porta*.

Status loop: exibe o estado da porta quando um loop é detectado.

Status bloqueio: exibe o estado da porta, bloqueada ou desbloqueada.

LAG: exibe o número do grupo LAG a qual a porta pertence.

Restaurar porta: após selecionar a porta bloqueada, clique no botão *Restaurar Porta* para a porta voltar ao seu estado normal de operação.

5.2. 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: *Spanning Tree, QoS* e *VLAN.* Seguem as explicações.

» Portas que estiverem habilitadas as funções *802.1Q VLAN, Spanning Tree, QoS 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.

» Portas que estiverem habilitadas as funções *Segurança das Portas, Espelhar Portas, Filtro de Endereços MAC,* não poderão ser adicionadas a um grupo LAG.

É recomendável configurar primeiramente os grupos LAG antes de configurar as demais funções.

Obs.: » *Como calcular a largura de banda em uma Agregação de Link? Suponhamos que um grupo LAG possua quatro portas com velocidade de 1000 Mbps Full Duplex, a largura de banda total do grupo LAG é de 8000 Mbps (2000 Mbps * 4) isto porque a largura de banda de cada porta é de 2000 Mbps, sendo 1000 Mbps de uplink e 1000 Mbps de downlink.*

» *O balanceamento de carga entre as portas pertencentes a um grupo LAG será de acordo com o algoritmo de 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.*

A função de *Agregação de Link* é configurada nas páginas *Grupos LAG, LAG Estático* e *LAG Dinâmico (LACP).*

Grupos LAG

Nesta página você pode visualizar e configurar as os Grupos LAG.

Escolha no menu *Switching* → *Agregação de Link* → *Grupos LAG* para carregar a seguinte página:

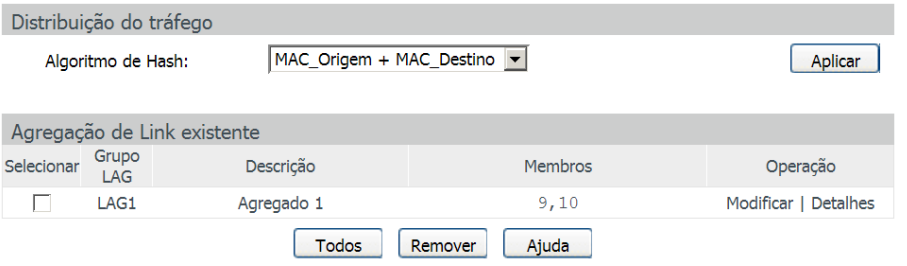


Tabela de agregação de link (LAG)

As seguintes informações são exibidas na tela:

» **Distribuição do tráfego**

Algoritmo de hash: selecione o algoritmo de hash utilizado para o balanceamento de carga utilizado pelas portas de um Grupo LAG.

» **MAC_origem + MAC_destino:** este algoritmo utiliza o endereço de MAC de origem e de destino para realizar o balanceamento de carga.

» **IP_origem + IP_destino:** este algoritmo utiliza o endereço IP de origem e de destino para realizar o balanceamento de carga.

» **Agregação de link existente**

Selecionar: selecione o grupo LAG desejado. É possível selecionar mais de um grupo simultaneamente.

Grupo LAG: exibe o número do grupo LAG.

Descrição: exibe a descrição do grupo LAG.

Membros: exibe as portas membros do grupo LAG.

Operação: permite visualizar informações detalhadas ou modificar as configurações de cada grupo LAG.

» **Modificar:** clique em *Modificar* para alterar as configurações do grupo LAG desejado.

» **Detalhes:** clique em *Detalhes* para exibir informações detalhadas do grupo LAG desejado.

Detalhes da Agregação de Link

Grupo LAG:	LAG1
Tipo do Grupo LAG:	Estático
Status da Porta:	Habilitar
Modo e Velocidade:	Auto
Espelhamento de porta:	Desabilitar
Limite de banda de entrada (bps):	--
Limite de banda de saída (bps):	--
Controle de Broadcast(bps):	--
Controle de Multicast (bps):	--
Controle de pacotes UL (bps):	--
Prioridade QoS:	CoS 0
VLAN:	1

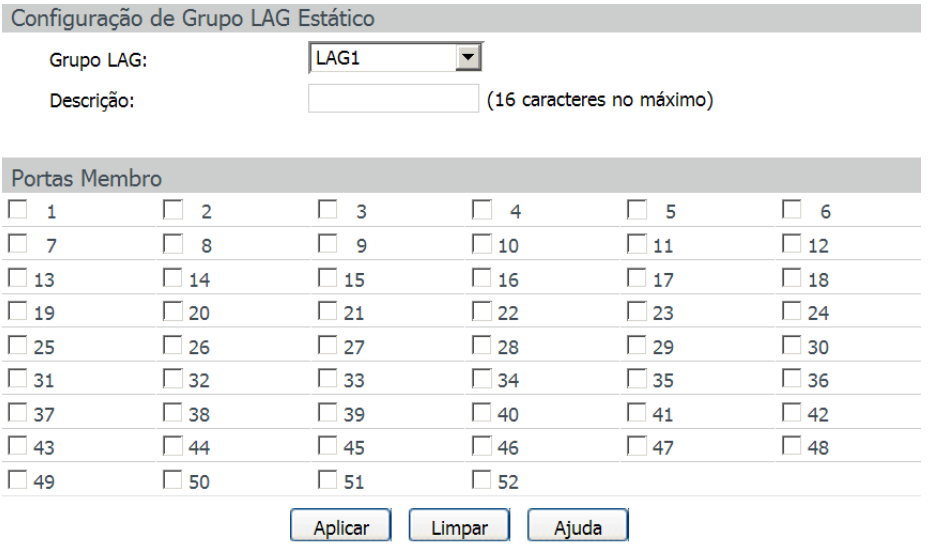
Voltar

Detalhes do grupo LAG

LAG estático

Nesta página é possível configurar grupos LAG Estáticos, selecionando as portas para cada grupo.

Escolha no menu *Switch* → *Agregação de Link* → *LAG Estático* para carregar a seguinte página:



Agregação de link estática

As seguintes informações são exibidas na tela:

» **Configuração de link estático**
Grupo LAG: selecione o número do grupo LAG.
Descrição: digite uma descrição para o grupo LAG.

» **Portas membro**
Portas: selecione as portas que participarão do grupo LAG. Para remover um grupo LAG, selecione todas as portas participantes do grupo e clique no botão *Limpar.*

Obs.: *uma porta somente poderá participar de um único grupo LAG.*

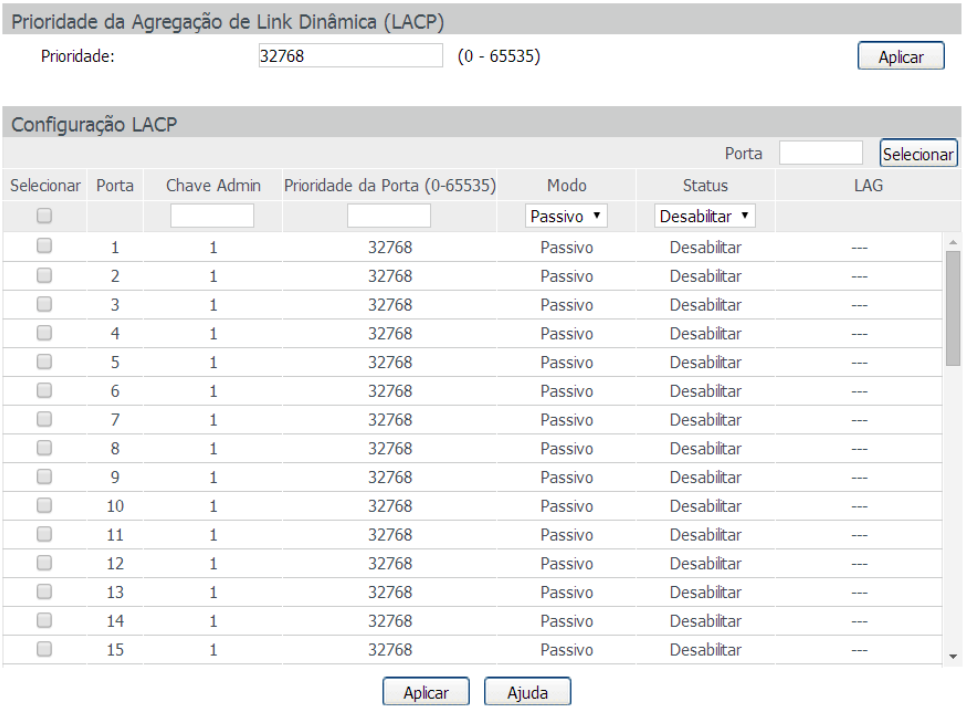
LAG dinâmico (LACP)

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 ativo, 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 só será realizada entre portas de switches com o mesmo ID de agregação de link.

É possível formar até seis grupos de agregação de link no switch. Se a quantidade configurada de grupos de agregação exceder o número máximo, o grupo que possuir o menor valor em Prioridade terá prioridade na realização da agregação de link.

Do mesmo modo, até quatro portas podem ser selecionadas para um grupo de agregação, portanto, a porta também possui uma prioridade para ser selecionada como membro de um grupo de agregação de link dinâmico. A porta com menor valor em Prioridade da Porta terá prioridade para realizar a agregação. Se duas portas possuírem prioridades iguais, a porta de número mais baixo terá a preferência.

Escolha o menu *Switching* → *Agregação de Link* → *LAG Dinâmico (LACP)* para carregar a seguinte página:



Obs.:

1. Para evitar tempestades de broadcast quando a função LACP estiver habilitada, ative a função Spanning Tree.
2. A função LACP não poderá ser habilitada em uma porta pertencente a um grupo de agregação de link estático.
3. O valor da chave administrativa não poderá ter o mesmo valor de qualquer grupo de agregação de link estático utilizado.

LACP (agregação de link dinâmico)

As seguintes informações são apresentadas na tela:

» **Prioridade de agregação de link dinâmica (LACP)**

Prioridade: digite o valor para a Prioridade do Sistema LACP. A prioridade do sistema combinado com o endereço MAC do switch constitui o ID de agregação. A agregação dinâmica somente será formada com grupos de agregação contendo o mesmo ID de agregação.

» **Configuração LACP**

Porta selecionar: digite o número da porta desejada dentro do campo correspondente e clique no botão *Selecionar* para selecionar a porta.

Selecionar: selecione a porta desejada para configuração LACP. É possível selecionar mais de uma porta simultaneamente.

Porta: exibe o número da porta.

Chave admin: especifique o valor da chave administrativa para a porta. Esta opção define a capacidade de agregação entre as portas. As portas membros da agregação dinâmica devem possuir a mesma chave admin.

Prioridade da porta: especifique o valor da Prioridade da Porta. É possível configurar a priorização de portas que pertencem ao mesmo grupo de agregação dinâmico. A porta com menor valor em Prioridade da Porta terá prioridade na realização da agregação. Se duas portas possuírem prioridades iguais, a porta de número mais baixo terá a preferência.

Modo: selecione o modo de funcionamento da função LACP na porta desejada.

Status: selecione *Habilitar* ou *Desabilitar* a função LACP na porta desejada.

LAG: exibe o número do grupo LAG a qual a porta pertence.

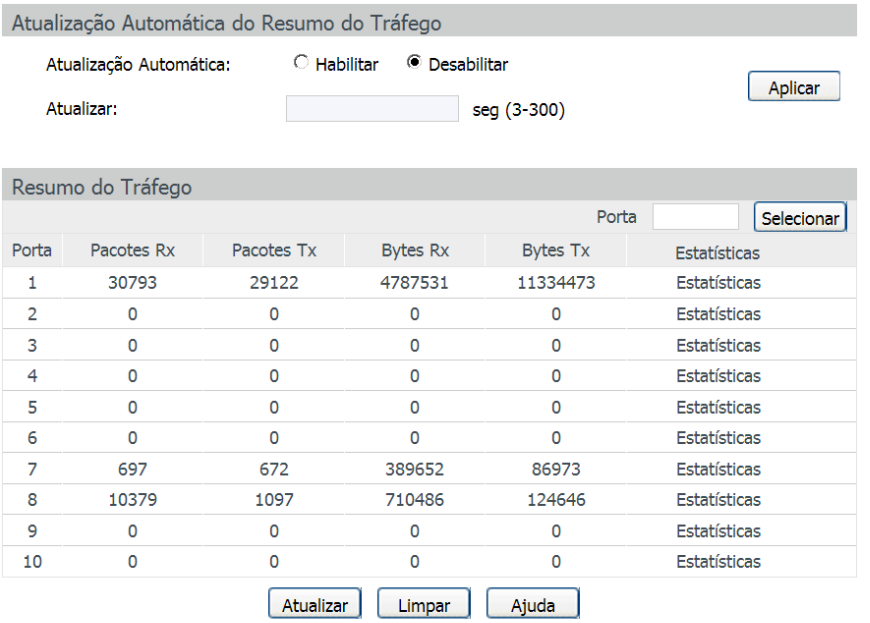
5.3. Tráfego

No submenu *Tráfego* é possível monitorar e visualizar informações detalhadas do tráfego em cada porta do switch através das páginas *Resumo do Tráfego* e *Estatísticas por Porta*.

Resumo do tráfego

A página *Resumo do Tráfego* exibe informações do tráfego em cada porta, o que facilita o monitoramento do tráfego da rede como um todo.

Escolha no menu *Switching* → *Tráfego* → *Resumo do Tráfego* para carregar a seguinte página:



Informações do tráfego

As seguintes informações são exibidas na tela:

» **Atualização automática do resumo do tráfego**

Atualização automática: selecione *Habilitar/Desabilitar* para habilitar ou desabilitar a atualização automática da página *Resumo do Tráfego*.

Atualizar: digite o valor do intervalo (em segundos) de atualização da página *Resumo do Tráfego*. O valor pode variar de 3 a 300 segundos.

» **Resumo do tráfego**

Porta selecionar: digite o número da porta desejada dentro do campo correspondente e clique no botão *Selecionar* para selecionar a porta.

Porta: exibe o número da porta.

Pacotes Rx: exibe o número de pacotes recebidos pela porta. Os pacotes com erro não participam desta estatística.

Pacotes Tx: exibe o número de pacotes transmitidos pela porta.

Bytes Rx: exibe o número de bytes recebidos pela porta.

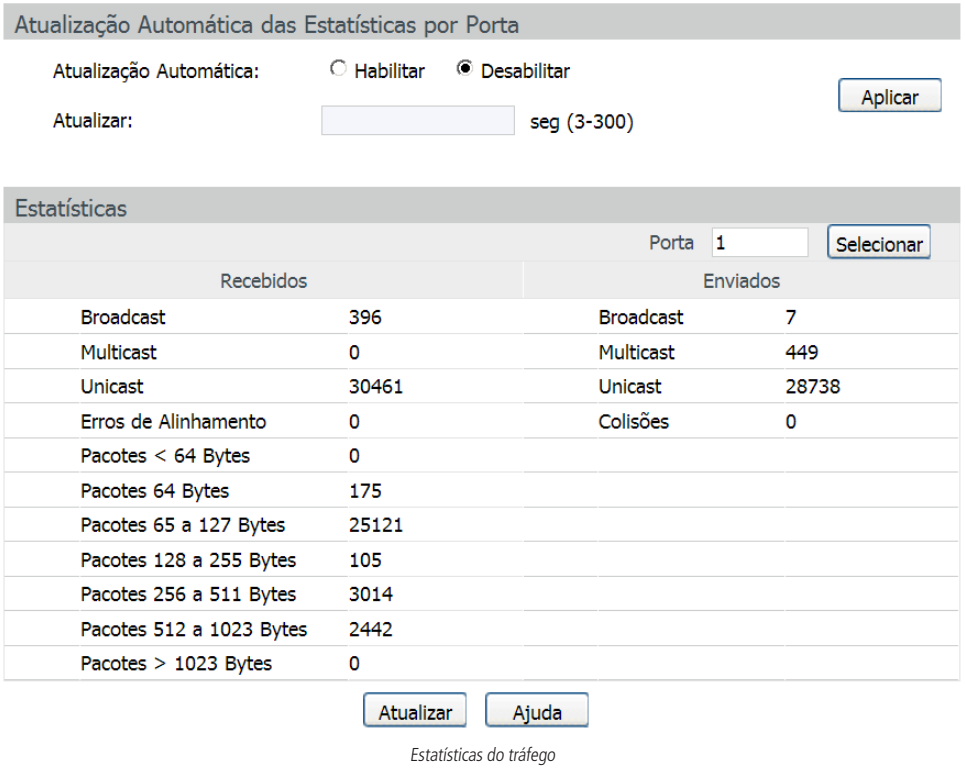
Bytes Tx: exibe o número de bytes transmitidos pela porta.

Estatísticas: clique em *Estatísticas* para visualizar as estatísticas detalhadas dos pacotes recebidos pela porta.

Estatísticas por porta

A página *Estatísticas por Porta* exibe as informações detalhadas do tráfego em cada porta, o que pode facilitar o monitoramento do tráfego da rede e localizar falhas rapidamente.

Escolha no menu *Switiching* → *Tráfego* → *Estatísticas por Porta* para carregar a seguinte página:



Estatísticas do tráfego

As seguintes informações serão exibidas:

» **Atualização automática do resumo do tráfego**

Atualização automática: selecione *Habilitar/Desabilitar* para habilitar ou desabilitar a atualização automática da página *Estatísticas por Porta*.

Atualizar: digite o valor do intervalo (em segundos) de atualização da página *Estatísticas por Porta*. O valor pode variar de 3 a 300 segundos.

» **Estatísticas**

Porta: digite o número da porta desejada dentro do campo correspondente e clique no botão *Selecionar* para selecionar a porta.

Recebidos: exibe os detalhes dos pacotes recebidos pela porta selecionada.

Enviados: exibe os detalhes dos pacotes enviados pela porta selecionada.

Broadcast: exibe o número de pacotes broadcast transmitidos ou recebidos na porta selecionada. Os pacotes com erros não são contabilizados nesta página.

Multicast: exibe o número de pacotes Multicast transmitidos ou recebidos na porta selecionada. Os pacotes com erros não são contabilizados nesta página.

Unicast: exibe o número de pacotes unicast transmitidos ou recebidos na porta selecionada. Os pacotes com erros não são contabilizados nesta página.

Erros de alinhamento: exibe o número dos pacotes recebidos que possuam erros de FCS (frame Check Sequence) ocasionados por erros nos bytes recebidos (Alignment Errors). O comprimento dos pacotes deverão possuir entre 64 e 1518 bytes de tamanho.

Pacotes < 64 bytes: exibe o número de pacotes recebidos menores que 64 bytes (pacotes com erros não são contabilizados).

Pacotes 64 bytes: exibe o número de pacotes recebidos iguais a 64 bytes (pacotes com erros não são contabilizados).

Pacotes 65 a 127 bytes: exibe o número de pacotes recebidos que possuem comprimento entre 65 e 127 bytes (pacotes com erros não são contabilizados).

Pacotes 128 a 255 bytes: exibe o número de pacotes recebidos que possuem comprimento entre 128 e 255 bytes (pacotes com erros não são contabilizados).

Pacotes 256 a 511 bytes: exibe o número de pacotes recebidos que possuem comprimento entre 256 e 511 bytes (pacotes com erros não são contabilizados).

Pacotes 512 a 1023 bytes: exibe o número de pacotes recebidos que possuem comprimento entre 512 e 1023 bytes (pacotes com erros não são contabilizados).

Pacotes > 1023 bytes: exibe o número de pacotes recebidos maiores que 1023 bytes (pacotes com erros não são contabilizados).

Colisões: exibe o número de colisões detectadas em uma porta durante a transmissão de pacotes.

5.4. Endereço 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 e o número da porta, criando uma entrada na tabela de encaminhamento (Tabela de endereços MAC). Esta tabela é a base para que o switch possa encaminhar os pacotes rapidamente, entre o endereço de origem e destino, diminuindo o tráfego em broadcast. Os endereços MAC são adicionados na tabela de endereços de forma dinâmica (autoaprendizagem) ou configurados manualmente.

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

Características da tabela de endereços MAC.

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

O submenu *Endereço MAC* possui as seguintes páginas de configuração: *Tabela MAC, MAC Estático, MAC Dinâmico e Filtro MAC.*

Tabela MAC

Nesta página, você poderá visualizar as informações da Tabela de endereços MAC.

Escolha no menu *Switching* → *Endereço MAC* → *Tabela MAC* para carregar a seguinte página:

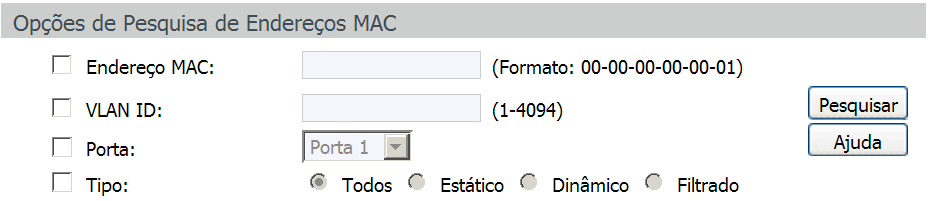


Tabela de Endereços MAC

Endereço MAC	VLAN ID	Porta	Tipo	Aging Time
6C-FD-B9-55-F1-84	1	1	Dinâmico	Aging Time
F8-1A-67-55-BF-5D	1	7	Dinâmico	Aging Time

Total de Endereços MAC: 2

Obs.:

A Tabela exibe os 100 últimos Endereços MAC. Para encontrar um Endereço MAC fora da lista, faça uma busca específica utilizando as opções de pesquisa.

Tabela de endereço MAC

As seguintes informações são exibidas na tela:

» **Opções de pesquisa de endereços MAC**

Endereço MAC: digite o endereço MAC desejada para visualizar as entradas correspondentes e clique no botão *Pesquisar*. Utilize o formato: *00-00-00-00-00-01*.

VLAN ID: digite a VLAN ID desejada para visualizar as entradas correspondentes e clique no botão *Pesquisar*.

Porta: selecione o número da porta desejada para visualizar as entradas correspondentes e clique no botão *Pesquisar*.

Tipo: selecione o tipo de entrada desejada para visualizar as entradas correspondentes e clique no botão *Pesquisar*.

- » **Todos:** esta opção exibe todas as entradas da Tabela de endereços MAC.
- » **Estático:** esta opção exibe todas as entradas estáticas da Tabela de endereços MAC.
- » **Dinâmico:** esta opção exibe todas as entradas dinâmicas da Tabela de endereços MAC.
- » **Filtrado:** esta opção exibe todos os endereços filtrados da Tabela de endereços MAC.

» **Tabela de endereços MAC**

Endereço MAC: exibe o endereço MAC aprendido pelo switch.

VLAN ID: exibe a VLAN ID que está vinculada ao endereço MAC.

Porta: exibe o número da porta que está vinculado ao endereço MAC.

Tipo: exibe o modo de aprendizagem dos endereços MAC.

Aging time: exibe se a entrada possui ou não Aging Time (tempo de envelhecimento).

MAC estático

Nesta página é possível configurar entradas estáticas na Tabela de endereços MAC. As entradas estáticas somente podem ser adicionadas ou removidas manualmente, independentemente do Aging Time (tempo de envelhecimento).

Em redes estáveis, as entradas de endereços MAC estático podem aumentar consideravelmente o desempenho de encaminhamento de pacotes do switch. O endereço MAC estático aprendido com a função *Segurança das Portas* habilitada, será exibido na Tabela de endereços MAC.

Escolha o menu *Switching* → *Endereço MAC* → *MAC Estático* para carregar a seguinte página:

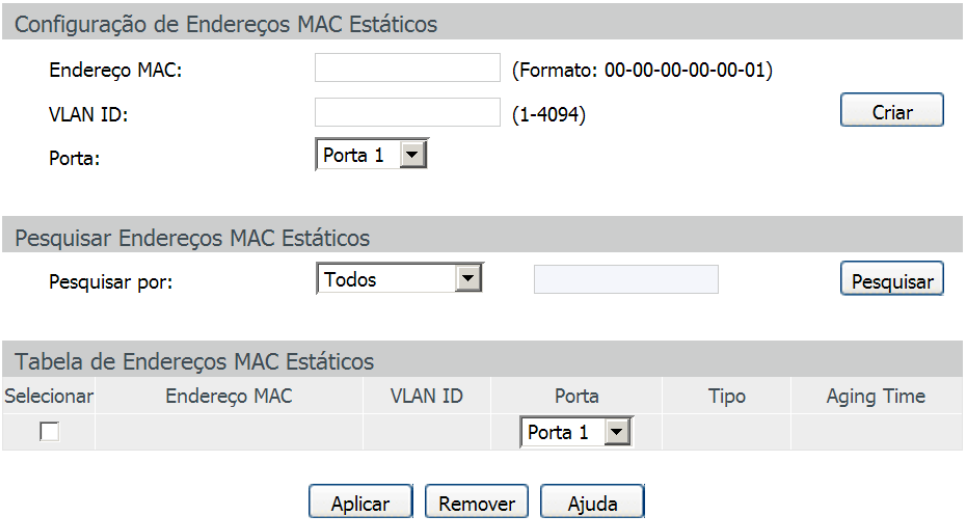


Tabela de endereços MAC estáticos

As seguintes mensagens são exibidas na tela:

» **Configuração de endereços MAC estáticos**

Endereço MAC: digite o endereço MAC que será adicionado a Tabela de endereços MAC, utilize o formato: *00-00-00-00-00-01* e clique no botão *Criar* (é necessário preencher os campos *VLAN ID* e *Porta* para validar a entrada).

VLAN ID: digite a VLAN ID que será associada ao endereço MAC que será adicionado a Tabela de endereços MAC.

Porta: selecione a porta que será vinculada ao endereço MAC que será adicionado a Tabela de endereço MAC.

» **Pesquisar endereços MAC estáticos**

Pesquisar por: selecione o modo de pesquisa e clique no botão *Pesquisar*, para encontrar a entrada estática na Tabela de endereços MAC.

- » **Endereço MAC:** digite o endereço MAC para sua pesquisa.
- » **VLAN ID:** digite o número da VLAN ID para sua pesquisa.
- » **Porta:** digite o número da porta para sua pesquisa.

» **Tabela de endereços MAC estáticos**

Selecionar: selecione a entrada desejada. Para excluir a entrada clique no botão *Remover*, para modificar a porta vinculada ao endereço MAC, selecione a nova porta e clique no botão *Aplicar*.

Endereço MAC: exibe o endereço MAC aprendido pelo switch.

VLAN ID: exibe a VLAN ID que está vinculada ao endereço MAC.

Porta: exibe o número da porta que está vinculado ao endereço MAC.

Tipo: exibe o modo de aprendizagem dos endereços MAC.

Aging time: exibe se a entrada possui ou não Aging Time (tempo de envelhecimento).

Obs.: » *Se o endereço MAC configurado para a porta correspondente estiver errado, ou o dispositivo conectado a porta for alterado, o switch não realizará o encaminhamento de pacotes. Por favor, redefina as entradas de endereço MAC de forma adequada.*

» *Se o endereço MAC de um dispositivo for configurado para uma porta e o dispositivo for conectado em outra porta, o switch não reconhecerá o endereço MAC dinamicamente. Portanto certifique-se que as entradas na Tabela de endereços MAC sejam válidas e corretas.*

» *Os endereços MAC configurados estaticamente não podem ser adicionados na tabela de endereços filtrados, ou vinculados a uma porta de forma dinâmica.*

MAC dinâmico

As entradas de endereços MAC realizadas de forma dinâmica são geradas pelo mecanismo de autoaprendizagem do switch, através deste recurso e juntamente com o Aging Time (tempo de envelhecimento) é que torna possível a manutenção da Tabela de endereços MAC.

O Aging Time faz com que o switch remova cada entrada da Tabela de endereços MAC dentro de um determinado período de tempo (tempo de envelhecimento) em que a entrada permanecer ociosa dentro da Tabela de endereços MAC.

Nesta página você pode configurar os endereços MAC dinâmico.

Escolha o menu *Switching → Endereço MAC → MAC Dinâmico* para carregar a seguinte página:

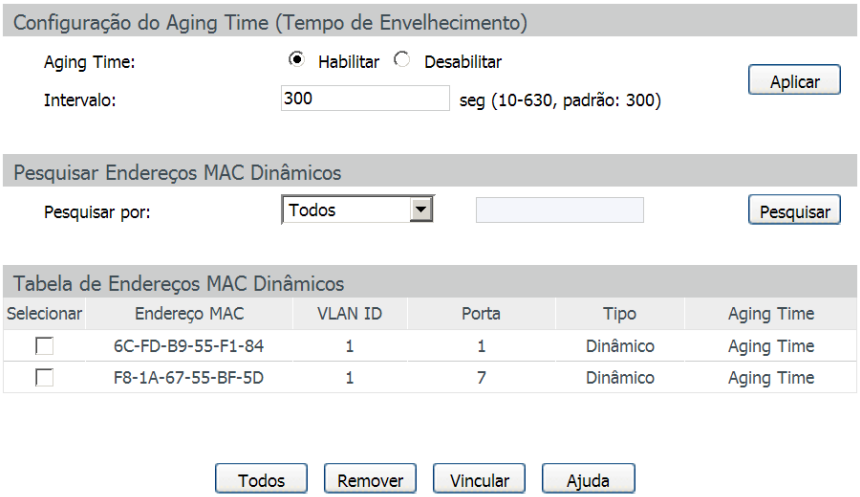


Tabela de endereços MAC dinâmica

As seguintes opções são exibidas na tela:

» **Configuração do aging time (tempo de envelhecimento)**

Aging time: selecione *Habilitar/Desabilitar* para habilitar ou desabilitar o Aging Time (tempo de envelhecimento) de uma entrada na Tabela de endereços MAC.

Intervalo: digite o valor do intervalo (em segundos) do Aging Time (tempo de envelhecimento) de uma entrada na Tabela de endereços MAC. O valor pode variar de 10 a 630 segundos, por padrão este valor é de *300 segundos*.

» **Pesquisar endereços MAC dinâmicos**

Pesquisar por: selecione o modo de pesquisa e clique no botão *Pesquisar*, para encontrar a entrada dinâmica na Tabela de endereços MAC.

» **Todos:** esta opção exibe todas as entradas dinâmicas da Tabela de endereços MAC.

» **Endereço MAC:** digite o endereço MAC para sua pesquisa.

» **VLAN ID:** digite o número da VLAN ID para sua pesquisa.

» **Porta:** digite o número da porta para sua pesquisa

» **Tabela de endereços MAC dinâmicos**

Selecionar: selecione a entrada desejada. Para excluir a entrada clique no botão *Remover*, para vincular a entrada de forma estática clique no botão *Vincular*.

Endereço MAC: exibe o endereço MAC aprendido pelo switch.

VLAN ID: exibe a VLAN ID que está vinculada ao endereço MAC.

Porta: exibe o número da porta que está vinculado ao endereço MAC.

Tipo: exibe o modo de aprendizagem dos endereços MAC.

Aging status: exibe se a entrada possui ou não Aging Time (tempo de envelhecimento).

Vincular: clique no botão *Vincular* para vincular o endereço MAC a uma porta de forma estática.

Obs.: *se o Aging Time (tempo de envelhecimento) do endereço MAC for muito longo ou muito curto poderá resultar em perda de desempenho do switch. Se o tempo for muito longo, poderá ocorrer o esgotamento da Tabela de endereços MAC, por estar com excesso de endereços MAC, o switch não aprenderá novos endereços, impedindo que as tabelas se atualizem com as mudanças ocorridas na rede. Se o tempo for muito curto, o switch poderá remover os endereços MAC válidos, isso fará com que o switch tenha que aprender várias vezes o mesmo endereço MAC, ocasionando uma perda de desempenho. Recomenda-se que mantenha o valor padrão.*

Filtro MAC

A filtragem de endereços MAC proíbe que pacotes indesejáveis sejam encaminhados pelo switch. Os endereços para filtragem podem ser adicionados ou removidos manualmente e não dependem do Aging Time (tempo de envelhecimento) do endereço MAC.

O Filtro MAC permite que o switch bloqueie os pacotes que possuam o endereço MAC especificado (tanto no endereço MAC de origem quanto no de destino do pacote), garantindo a segurança da rede. As regras de Filtro MAC atuarão na VLAN correspondente.

Escolha no menu *Switching* → *Endereço MAC* → *Filtro MAC* para carregar a seguinte página:

Filtro de endereço MAC

As seguintes informações são exibidas:

» **Configuração de filtro de endereços MAC**

Endereço MAC: digite o endereço MAC que será bloqueado, proibindo a sua inclusão na Tabela de endereços MAC e clique no botão *Criar* (é necessário preencher o campo VLAN ID para validar a entrada), utilize o formato: *00-00-00-00-00-01*.

VLAN ID: digite a VLAN ID que será vinculada ao endereço MAC que será filtrado na Tabela de endereços MAC.

» **Pesquisar endereços MAC filtrados**

Pesquisar por: selecione o modo de pesquisa e clique no botão *Pesquisar*, para encontrar a entrada filtrada na Tabela de endereços MAC.

» **Endereço MAC:** digite o endereço MAC para sua pesquisa.

» **VLAN ID:** digite o número da VLAN ID para sua pesquisa.

» **Tabela de filtro de endereços MAC**

Selecionar: selecione a entrada desejada. Para excluir a entrada clique no botão *Remover*.

Endereço MAC: exibe o endereço MAC que será bloqueado pelo switch.

VLAN ID: exibe a VLAN ID que está vinculada ao endereço MAC bloqueado.

Porta: exibe o número da porta que está vinculado ao endereço MAC bloqueado.

Tipo: exibe o modo de aprendizagem dos endereços MAC.

Aging time: exibe se a entrada possui ou não Aging Time (tempo de envelhecimento).

Obs.: *os endereços MAC filtrados não poderão ser inclusos na Tabela de endereços MAC, utilizando os métodos de aprendizagem Estático ou Dinâmico.*

5.5. Filtro DHCP

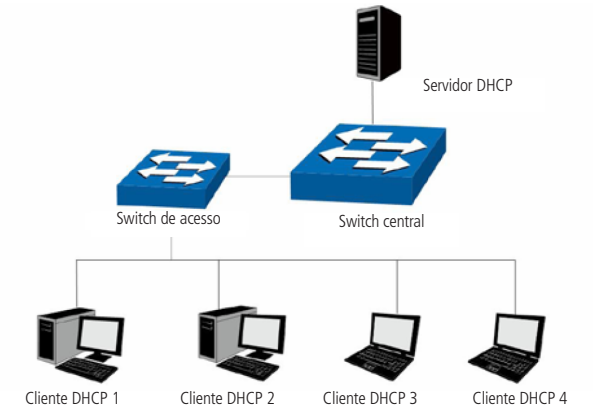
Atualmente as redes estão ficando cada vez maiores e mais complexas. As configurações de endereços IP e parâmetros de redes utilizados devem ser analisados e atualizados com frequência, para permitir o perfeito funcionamento dos computadores e recursos da rede. O protocolo DHCP (*Dynamic Host Configuration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

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

A função *Filtro DHCP* monitora o processo de obtenção de endereços IPs dos clientes através do servidor DHCP.

Princípio de funcionamento do servidor DHCP

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



Funcionamento do DHCP

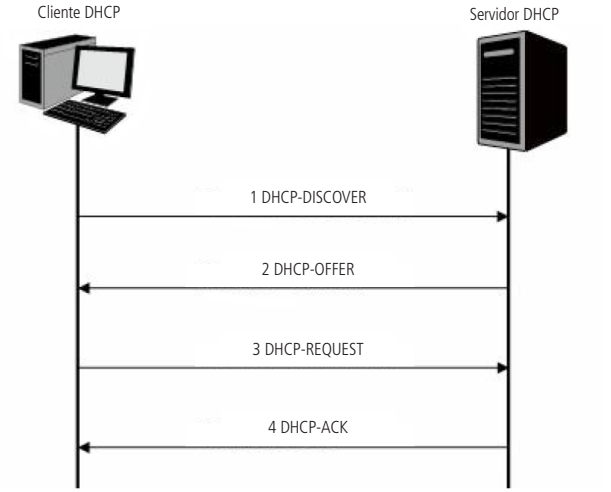
O servidor DHCP fornece três métodos de atribuição de endereços IPs.

» **Manual:** permite ao administrador vincular o endereço IP estático para um cliente específico (ex. servidor WWW).

» **Automático:** o servidor DHCP atribui os endereços IPs para os clientes sem tempo de expiração.

» **Dinâmico:** o servidor DHCP atribui o endereço IP com um determinado tempo de expiração. Quando o tempo para o endereço IP expirar, o cliente terá que solicitar um novo endereço IP para o servidor DHCP.

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



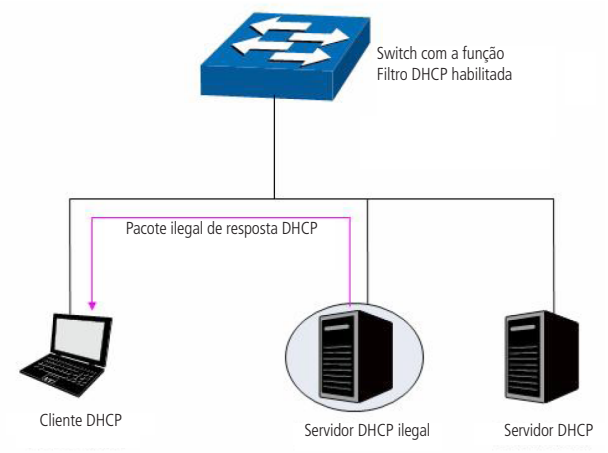
Negociação DHCP

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

DHCP cheating attack

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

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



DHCP cheating attack

A função de Filtro DHCP permite que apenas as portas configuradas como portas de confiança possam receber pacotes de servidores DHCP, garantindo assim que os clientes DHCP recebam somente pacotes de servidores DHCP confiáveis, ou seja, serão descartados pelo switch todos os pacotes DHCP de servidores DHCP recebidos em portas que não estejam configuradas como porta de confiança.

Escolha no menu *Switching* → *Filtro DHCP* → *Filtro DHCP* para carregar a seguinte página:

Configuração filtro DHCP

As seguintes informações são apresentadas na tela:

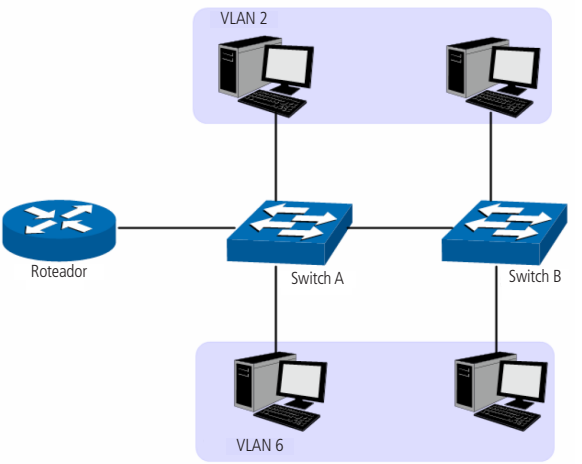
» **Configuração de filtro DHCP**
Filtro DHCP: selecione *Habilitar* ou *Desabilitar* a função de Filtro DHCP.

» **Portas de confiança**
Portas de confiança: selecione as portas consideradas como portas de confiança. Somente as portas marcadas como portas de confiança podem receber pacotes DHCP de servidores DHCP. Clique no botão *Todas* para selecionar todas as portas ou clique no botão *Limpar* para desmarcar as portas de confiança.

6. VLAN

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

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



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.
3. Flexibilidade na alteração de layout: é possível ter computadores separados geograficamente (por exemplo, computadores em andares diferentes) pertencerem à mesma VLAN sem a necessidade de alteração física da topologia da rede.

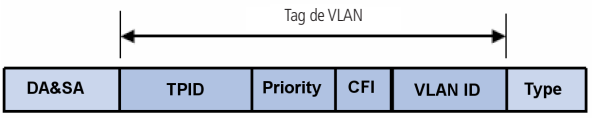
Este switch suporta o modo de classificação de VLAN baseado em TAG (802.1Q VLAN).

6.1. 802.1Q VLAN

As tags de VLANs são necessárias para o switch identificar os pacotes de diferentes VLANs. O switch trabalha na camada de enlace no modelo OSI, podendo desta forma, analisar e gerenciar os quadros que possuam a tag de VLAN.

Em 1999, o IEEE padronizou a aplicação 802.1Q VLAN, definindo uma estrutura de tags de VLAN nos quadros Ethernet. O protocolo IEEE802.1Q define que 4 bytes são adicionados ao quadro Ethernet (esta inserção ocorre logo após os campos de endereço MAC de destino e origem do frame Ethernet) para tornar possível a utilização de VLANs em redes Ethernet.

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



Tag de VLAN

1. **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.
2. **Priority:** campo de 3 bits, referindo-se a prioridade 802.1p. Consulte o capítulo 9. QoS, para mais detalhes.
3. **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. Esse campo não é descrito em detalhes nesse manual.
4. **VLAN ID:** campo de 12 bits, que identifica o VLAN ID (Identificação da VLAN) a qual o quadro pertence. Este intervalo varia entre 1 a 4094, normalmente os valores 0 e 4095 não são utilizados. VLAN ID identifica a VLAN a qual o quadro pertence. Quando o switch recebe um pacote que não possui tag de VLAN (untagged), o switch irá encapsular o quadro com a tag de VLAN padrão da porta correspondente (PVID).

» **Modo de funcionamento das portas**

As portas do switch podem operar de duas formas distintas, a seguir a descrição de cada uma delas:

Untagged: a porta untagged pode ser adicionada em várias VLANs. Se um pacote com TAG de VLAN chegar em uma porta e o VLAN ID deste pacote não corresponder com nenhuma VLAN pertencente a porta, este pacote será descartado. Os pacotes enviados por uma porta untagged são encaminhados sem marcação (untagged).

Tagged: a porta tagged pode ser adicionada em várias VLANs. Se um pacote com TAG de VLAN chegar em uma porta e o VLAN ID deste pacote não corresponder com nenhuma VLAN pertencente a porta, este pacote será descartado. Os pacotes com marcação de VLAN (TAG de VLAN) que corresponderem com alguma VLAN da porta de entrada, serão encaminhados sem alteração na TAG de VLAN.

» **PVID**

PVID (Port Vlan ID) é o VID (Identificação da VLAN) padrão da porta. Quando o switch recebe um pacote sem marcação (untagged), ele irá adicionar uma tag de VLAN no pacote de acordo com o PVID de sua porta. Ao criar VLANs, o PVID de cada porta indica a VLAN padrão a qual porta pertence. É um parâmetro importante com a seguinte finalidade:

- » Quando o switch recebe um pacote sem marcação (untagged), ele irá adicionar uma tag de VLAN no pacote de acordo com o PVID configurado em sua porta.
- » O PVID determina o domínio de broadcast padrão da porta, ou seja, quando a porta recebe pacotes de broadcast, a porta transmitirá os pacotes apenas para as portas do seu domínio de broadcast.

Pacotes marcados (tagged) ou não marcados (untagged) serão processados de maneiras diferentes, se recebidos por portas com diferentes modos de funcionamento. A tabela a seguir exibe como são tratados os pacotes.

	Recebendo pacotes		**Enviando pacotes**	
Modo da porta	**Pacotes untagged (sem marcação)**	**Pacotes tagged (com marcação)**	**Pacotes untagged (sem marcação)**	**Pacotes tagged (com marcação)**
Untagged	Ao receber pacotes não marcados, a porta adicionará a tag de VLAN padrão no pacote recebido, ou seja, o valor do PVID da porta receptora do pacote.	Se o VID do pacote for permitido pela porta, o pacote será recebido.	O pacote será encaminhado sem alteração.	O pacote será encaminhado após remover sua Tag de VLAN.
Tagged		Se o VID do pacote for proibido pela porta, o pacote será descartado.	O pacote será encaminhado com Tag de VLAN com o valor correspondente ao PVID da porta de saída.	O pacote será encaminhado com sua atual Tag de VLAN.

Relação entre os modos da porta e o processamento dos pacotes

A função 802.1Q VLAN pode ser configurada na página *Configurar VLAN*.

Configurar VLAN

Nesta página você poderá configurar e visualizar as VLANs.

Para garantir uma comunicação normal, o switch vem configurado de fábrica com todas as portas pertencentes a VLAN 1.

Escolha o menu *VLAN* → *802.1Q VLAN* → *Configurar VLAN* para carregar a seguinte página:

VLANs Configuradas

VLAN ID [ ] Selecionar

Selecionar	VLAN ID	Descrição:	Portas Untagged	Portas Tagged	Operação
☐	1	Default VLAN	1-52		Remover

Membros da VLAN

VLAN ID --- Nome da VLAN [ ]

Porta	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Untagged	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Tagged	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Não Membro	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉
PVID	1	1	1	1	1	1	1	1	1	1	1	1	1	1
LAG	---	---	---	---	---	---	---	---	---	---	---	---	---	---
Porta	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Untagged	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Tagged	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Não Membro	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉
PVID	1	1	1	1	1	1	1	1	1	1	1	1	1	1
LAG	---	---	---	---	---	---	---	---	---	---	---	---	---	---
Porta	29	30	31	32	33	34	35	36	37	38	39	40	41	42
Untagged	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Tagged	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Não Membro	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉
PVID	1	1	1	1	1	1	1	1	1	1	1	1	1	1
LAG	---	---	---	---	---	---	---	---	---	---	---	---	---	---
Porta	43	44	45	46	47	48	49	50	51	52				
Untagged	○	○	○	○	○	○	○	○	○	○				
Tagged	○	○	○	○	○	○	○	○	○	○				
Não Membro	◉	◉	◉	◉	◉	◉	◉	◉	◉	◉				
PVID	1	1	1	1	1	1	1	1	1	1				
LAG	---	---	---	---	---	---	---	---	---	---				

Aplicar Ajuda

Configuração de VLANs

As seguintes informações são apresentadas na tela:

» **Configuração de VLAN**
VLAN ID: digite o VLAN ID desejado e clique no botão *Criar* para adicionar a VLAN desejada.
Descrição: digite uma descrição para a VLAN de no máximo 16 caracteres

» **VLANs configuradas**
VLAN ID selecionar: digite o VLAN ID desejado no campo correspondente e clique no botão *Selecionar* para selecionar a VLAN desejada.
Selecionar: selecione o VLAN ID desejado para realizar a configuração.
VLAN ID: exibe o VLAN ID da VLAN (identificação da VLAN).
Descrição: exibe a descrição definida para a VLAN.

Portas untagged: exibe as portas untagged da VLAN selecionada.

Portas tagged: exibe as portas tagged da VLAN selecionada.

Operação: após selecionado o VLAN ID, clique em *Remover* para excluir a VLAN.

» **Membros da VLAN**

VLAN ID: exibe o VLAN ID selecionado.

Nome da VLAN: exibe o nome da VLAN. Para alterar o nome da VLAN edite este campo e pressione o botão *Aplicar*.

Porta: exibe o número da porta.

Untagged: ao selecionar a opção, a porta será membro da VLAN selecionada e o modo de processamento do pacote será untagged.

Tagged: ao selecionar a opção, a porta será membro da VLAN selecionada e o modo de processamento do pacote será tagged.

Não membro: ao selecionar a opção, a porta não será membro da VLAN selecionada.

PVID: selecione o PVID desejado na porta correspondente.

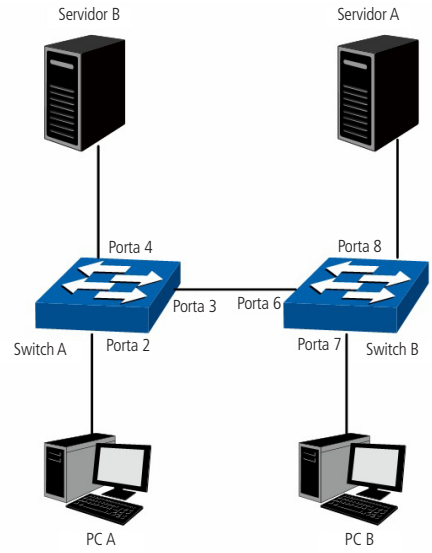
LAG: exibe o número do grupo LAG a qual a porta pertence.

6.2. Exemplos de aplicação para 802.1Q VLAN

» **Requisitos da rede**

- » O switch A está conectado ao PC A e Servidor B.
- » O switch B está conectado ao PC B e Servidor A.
- » O PC A e o Servidor A estão na mesma VLAN.
- » O PC B e o Servidor B estão na mesma VLAN.
- » Os PCs em VLANs diferentes não podem se comunicar uns com os outros.

» **Diagrama da rede**



Aplicação de VLAN 802.1Q

» **Procedimento de configuração**

» Configuração do switch A

Passo	Operação	Descrição
1	Definir o modo de funcionamento da porta	Obrigatório, *VLAN* ⟶ *802.1Q VLAN* ⟶ *Configurar VLAN*, configurar o modo de funcionamento da porta 2, porta 3 e porta 4 como Untagged, Tagged e Untagged respectivamente.
2	Criar a VLAN 10	Obrigatório, *VLAN* ⟶ *802.1Q VLAN* ⟶ *Configurar VLAN*, criar a VLAN com o VLANID 10 nas portas 2 e 3.
3	Criar a VLAN 20	Obrigatório, *VLAN* ⟶ *802.1Q VLAN* ⟶ *Configurar VLAN*, criar a VLAN com o VLANID 20 nas portas 3 e 4.

» Configuração do switch B

Passo	Operação	Descrição
1	Definir o modo de funcionamento da porta	Obrigatório, *VLAN* ⟶ *802.1Q VLAN* ⟶ *Configurar VLAN*, configurar o modo de funcionamento da porta 7, porta 6 e porta 8 como Untagged, Tagged e Untagged respectivamente.
2	Criar a VLAN 10	Obrigatório, *VLAN* ⟶ *802.1Q VLAN* ⟶ *Configurar VLAN*, criar VLAN com o VLANID 10 nas portas 6 e 8.
3	Criar a VLAN 20	Obrigatório, *VLAN* ⟶ *802.1Q VLAN* ⟶ *Configurar VLAN*, criar a VLAN com o VLANID 20 nas portas 6 e 7.

7. Spanning tree

STP (Spanning Tree Protocol), pertence à norma 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. Cada BPDU contém um campo chamado BID (Bridge ID) que identifica o switch que enviou o BPDU. O BID contém um valor de prioridade, o endereço MAC do switch de envio, e uma ID de Sistema Estendido opcional. Determina-se o valor o BID mais baixo através da combinação destes três campos.

» **Elementos STP**

Bridge ID: indica valor da prioridade e endereço MAC 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.

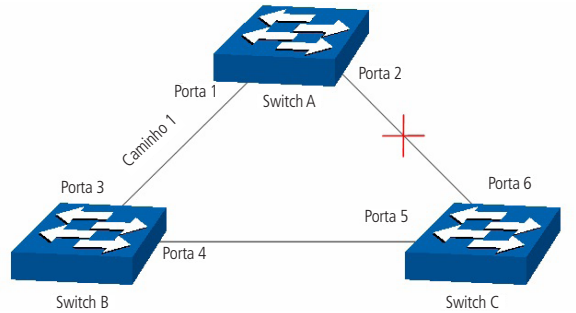
Prioridade da porta: a prioridade da porta pode ser ajustada em um intervalo de 0-255. O valor mais baixo para a Prioridade da Porta possui maior prioridade. A porta com maior prioridade possui maior chance de ser escolhida como Porta Root (Porta Raiz).

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.

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

» **Switches:** switch A é a Bridge Root, da rede e o switch B é a Bridge Designada do switch C.

» **Portas:** a porta 3 é a Porta Root (porta raiz) do switch B e a porta 5 é a Porta Root (porta raiz) do switch C; a porta 1 é a Porta Designada do switch A e a porta 4 é a Porta Designada do switch B; a porta 6 do switch C está bloqueada.



Rede spanning tree

» **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.

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

» **Principio de comparação de quadros BPDU**

Supondo dois BPDUs: BPDUx e BPDUy.

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

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

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

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

» **Convergência STP**

» **Iniciando**

Ao iniciar, cada switch se considera a Bridge Root e gera uma configuração BPDU para cada porta, com Custo do Caminho Root sendo 0 e o ID da Bridge Designada e Porta Designada sendo do próprio switch.

» **Comparando BPDUs**

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

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

» **Selecionando a Bridge Root**

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

» **Selecionando a Porta Toot e Porta Designada**

A operação é realizada da seguinte maneira.

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

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

O RSTP (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.

- » Condição para a Porta Root alterar o estado da porta para encaminhamento: quando a Porta Root do switch deixa de encaminhar dados a Porta Designada começa a transmitir dados imediatamente.
- » A condição para a Porta Designada alterar o estado da porta para encaminhamento: a Porta Designada pode operar de duas formas: Porta Edge (Porta de Acesso) e Link P2P (conexão direta com outro switch).
  - » Se a Porta Designada é uma Porta Edge: a porta altera imediatamente seus estado para encaminhamento.
  - » Se Porta Designada é um Link P2P: a porta somente mudará o estado para encaminhamento após realização do handshake entre as portas do switch.
- » **Elementos RSTP**
  - » **Porta 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.

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.

Funções do MSTP

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

Elementos MSTP

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

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

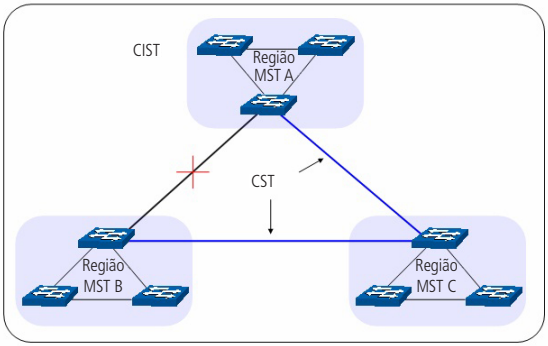


Diagrama de rede MSTP

» **MSTP**

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

» **Estado das portas**

No MSTP, as portas podem estar nos seguintes estados.

Encaminhamento: neste estado a porta pode enviar e receber dados da rede além de enviar e receber quadros BPDUs e aprender endereços MAC.

Aprendizado: neste estado a porta pode enviar e receber BPDUs e aprender endereços MAC.

Bloqueado: neste estado a porta somente pode receber pacotes BPDUs.

Desconectado: neste estado a porta não participa da execução do STP.

» **Funções das portas**

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

Porta root: indica a porta que tem o caminho com menor custo (Path Cost) até o Bridge Root.

Porta designada: indica a porta que encaminha pacotes para um segmento de rede do switch.

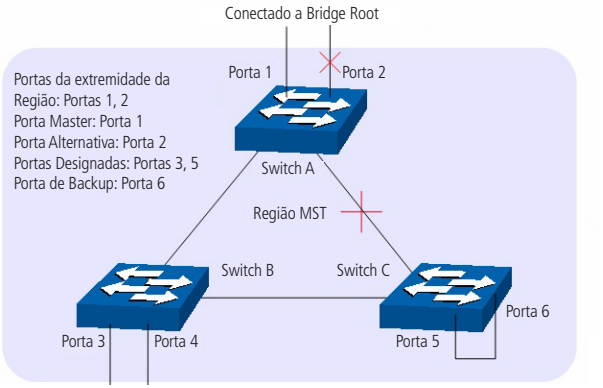
Porta master: indica a porta que se conecta a região MST de outro switch.

Porta alternativa: indica a porta que pode ser utilizada como backup da Porta Root ou Porta Master.

Porta de backup: indica a porta de backup da Porta Designada.

Desabilitada: indica a porta que não participa do STP.

O diagrama a seguir exibe as diferentes funções das portas.



Funções das portas em MSTP

A função Spanning Tree possui quatros submenus de configuração: *Spanning Tree, Portas STP, Instâncias MSTP e Segurança STP.*

7.1. Spanning Tree

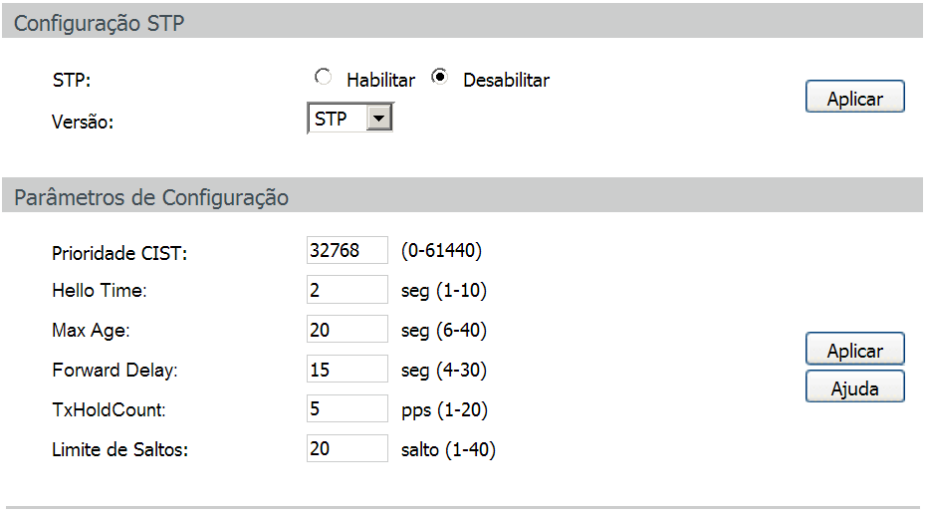
O submenu *Spanning Tree* é utilizado para realizar as configurações globais da função *Spanning Tree* e podem ser realizados através das páginas: *Configurar STP e Status STP.*

Configurar STP

Antes de configurar o Spanning Tree em uma rede, é necessário definir a função que cada switch irá desempenhar dentro de uma instância Spanning Tree. Apenas um switch pode ser a Bridge Root em cada instância Spanning Tree.

Nesta página você pode configurar globalmente a função de Spanning Tree e seus parâmetros.

Escolha o menu *Spanning Tree* → *Spanning Tree* → *Configurar STP* para carregar a seguinte página:



Configuração STP

As seguintes opções são exibidas na tela:

» **Configuração STP**

STP: selecione *Habilitar/Desabilitar* para habilitar ou desabilitar função STP no switch.

Versão: selecione a versão desejada do protocolo STP.

» **STP:** Spanning Tree Protocol.

» **RSTP:** Rapid Spanning Tree Protocol.

» **MSTP:** Multiple Spanning Tree Protocol.

» **Parâmetros de configuração**

Prioridade CIST: insira um valor de 0 a 61440 para especificar a prioridade do switch durante a troca de quadros BPDUs. A prioridade CIST é um critério importante na determinação da Bridge Root. O switch com a maior prioridade será escolhido como Bridge Root.

O valor mais baixo tem maior prioridade. O valor padrão é 32768 e deve ser um divisor exato de 4096.

Hello time: insira um valor de 1 a 10 em segundos para especificar o intervalo de envios de quadros BPDUs. A seguinte formula é utilizada para testar o link "2 * (Hello Time + 1) <= Max Age". O valor padrão é 2.

Max age: insira um valor de 6 a 40 em segundos para especificar o tempo máximo que o switch ficará aguardando um quadro BPDU antes de tentar se reconfigurar. O valor padrão é 20 segundos.

Forward delay: insira um valor de 4 a 30 segundos para especificar o tempo para a porta poder alterar seu estado após uma alteração na topologia da rede. A seguinte formula é utilizada "2 * (Forward Delay -1) >= Max Age". O valor padrão é 15 segundos.

TxHoldCount: insira um valor de 1 a 20 para definir o número máximo de pacotes BPDUs transmitidos por intervalo de Hello Time. O valor padrão é 5.

Limite de saltos: insira um valor de 1 a 40 para especificar o máximo de saltos possíveis em uma região específica antes do BPDU ser descartado. O valor padrão é 20 saltos.

Obs.: » *O parâmetro Forward Delay e o diâmetro da rede estão diretamente relacionados. Um pequeno Forward Delay poderá resultar em loops temporários. Um grande Forward Delay poderá resultar na incapacidade da rede voltar ao seu estado normal de operação, durante a convergência STP. O valor padrão é recomendado.*

» *Um Hello Time adequado faz com que o switch possa descobrir as falhas de link ocorridos na rede sem ocupar muito os recursos. Um grande Hello Time, pode resultar em links normais serem detectados como inválidos. Um Hello Time muito pequeno pode resultar em configurações duplicadas sendo enviadas com frequência, o que aumenta a carga nos switches, desperdiçando recursos da rede. O valor padrão é recomendado.*

» *Um Max Age pequeno poderá resultar em switches regenerando seus Spanning Tree frequentemente e causando um congestionamento na rede que pode ser confundido como um problema em um dos links. Um Max Age muito grande pode deixar os switches incapazes de encontrar os problemas nos links, causando limitações no Spanning Tree. O valor padrão é recomendado.*

» *Se o parâmetro TxHoldCount for muito alto, o número de pacotes MSTP sendo enviados em cada Hello Time aumentará a utilização da largura de banda da rede. O valor padrão é recomendado.*

Status STP

Nesta página é possível visualizar os parâmetros relacionados à função Spanning Tree.

Escolha no menu *Spanning Tree* → *Spanning Tree* → *Status STP* para carregar a seguinte página:

Resumo STP	
Status do STP:	Habilitar
Versão do STP:	STP
Bridge Local:	32768---a0-f3-c1-05-f9-90
Bridge Root:	32768---a0-f3-c1-05-f9-90
Custo do Caminho Externo:	0
Região Root:	---
Custo do Caminho Interno:	---
Bridge Designada:	32768---a0-f3-c1-05-f9-90
Porta Root:	---
Último Pacote TC:	2013-08-09 14:04:07
Pacotes TC:	3

Resumo das Instâncias MSTP	
ID da Instância	1
Status da Instância:	Desabilitar
Bridge Local:	---
Região Root:	---
Custo do Caminho Interno:	---
Bridge Designada:	---
Porta Root:	---
Último Pacote TC:	---
Pacotes TC:	---

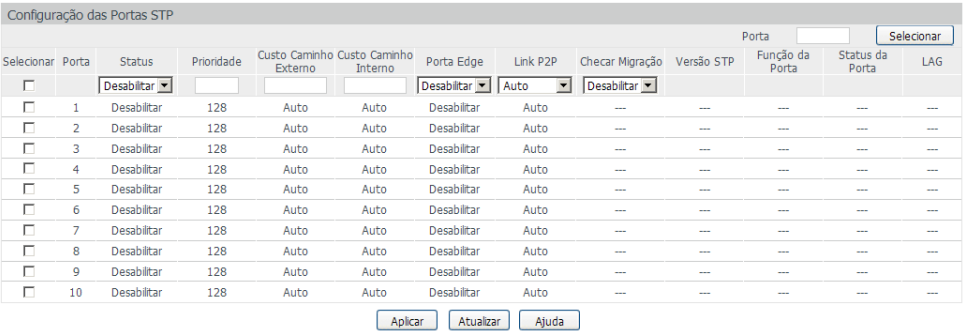
Atualizar

Status STP

7.2. Portas STP

Nesta página é possível configurar os parâmetros das portas STP e de todas as instâncias STP da rede.

Escolha no menu *Spanning Tree → Portas STP* para carregar a seguinte página:



Portas STP

As seguintes informações são exibidas na tela:

» **Configuração das portas STP**

Porta: digite a porta desejada no campo correspondente e clique no botão *Selecionar* para selecionar a porta.

Selecionar: selecione a porta desejada. É possível selecionar mais de uma porta simultaneamente.

Porta: exibe o número da porta.

Status: selecione *Habilitar/Desabilitar* para habilitar ou desabilitar a função STP na porta desejada.

Prioridade: digite um valor de 0 a 240 divisível por 16. Prioridade da Porta é um importante critério para determinar se a porta conectada será escolhida como Porta Root. O valor mais baixo terá maior prioridade.

Custo caminho externo: é utilizado para escolher o caminho e calcular o Custo do Caminho das portas em diferentes regiões MST. É um critério importante na definição da Porta Root. O valor mais baixo terá maior prioridade.

Custo caminho interno: é utilizado para escolher o caminho e calcular o Custo do Caminho das portas em uma região MST. É um critério importante na definição da Porta Root. O valor mais baixo terá maior prioridade.

Porta edge: selecione *Habilitar/Desabilitar* para habilitar ou desabilitar a função. Esta opção é utilizada conectar um equipamento final (normalmente computadores) na porta do switch. Este modo faz com que o estado da porta se modifique de "Bloqueada" para "Encaminhamento" de forma direta.

Link P2P: selecione *Auto/Habilitar/Desabilitar* para habilitar/desabilitar ou deixar em modo automático o link P2P (portas utilizadas na interconexão de switches). Se as duas portas do link P2P são Portas Root ou Portas Designadas, elas podem alterar o estado da porta para encaminhamento de forma mais rápida, reduzindo o tempo de convergência do Spanning Tree.

Checar migração: selecione *Habilitar/Desabilitar* para habilitar ou desabilitar a função de Checar Migração.

Versão STP: exibe a versão do Spanning Tree da porta.

Função da porta: exibe a função da porta na instância STP.

» **Porta root:** indica a porta que tem o menor Custo de Caminho para a Bridge Root.

» **Porta designada:** indica a porta do switch que encaminha pacotes para um segmento de rede.

» **Porta master:** indica a porta do switch, 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.

Status da porta: exibe o estado de funcionamento da porta.

» **Encaminhamento:** neste estado a porta pode receber e enviar dados, receber e enviar quadros BPDUs bem como aprender endereços MAC.

» **Aprendizado:** neste estado a porta pode receber e enviar quadros BPDUs e aprender o endereço MAC.
» **Bloqueado:** neste estado a porta somente pode receber quadros BPDUs.
» **Desconectado:** neste estado a porta não participa do Spanning Tree.

LAG: exibe o número do grupo LAG que a porta pertence.

Obs.: » *Configurar as portas que estão conectadas diretamente aos equipamentos finais (como por exemplo, computadores) como Porta Edge e habilitar a função BPDU Protect, além de alterar o estado da porta para encaminhamento de forma mais rápida, aumenta também a segurança na rede.*

» *Todas as portas pertencentes a grupos LAGs podem ser configuradas como links ponto a ponto (Link P2P).*

» *Quando um link de uma porta é configurado como ponto-a-ponto, as instâncias de Spanning Tree possuem suas portas configuradas como ponto a ponto (Link P2P). Se a conexão física da porta não for um link ponto a ponto, poderá ocorrer loops temporários na rede.*

7.3. Instâncias MSTP

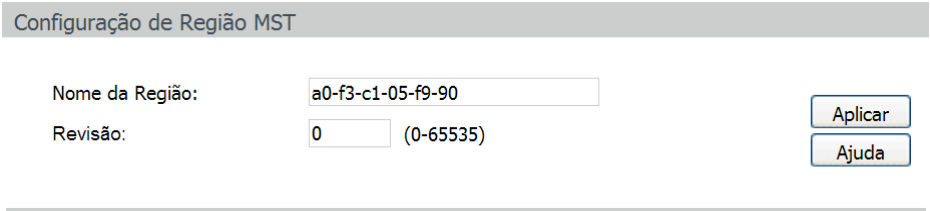
O MSTP cria uma tabela de mapeamento entre VLANs e o Spanning Tree. Ao adicionar uma instância MSTP, várias VLANs são conectadas a uma instância MSTP. Somente os switches que possuem o mesmo nome, revisão e tabela de mapeamento pertencem a mesma região MST.

A função de Instâncias MSTP pode ser configurada nas páginas: *Região MST, Instância MST e Portas MST.*

Região MST

Nesta página você pode configurar o nome e revisão da região MST.

Escolha o menu *Spanning Tree → Instâncias MSTP → Região MST* para carregar a seguinte página:



Região MST

As seguintes opções são exibidas na tela:

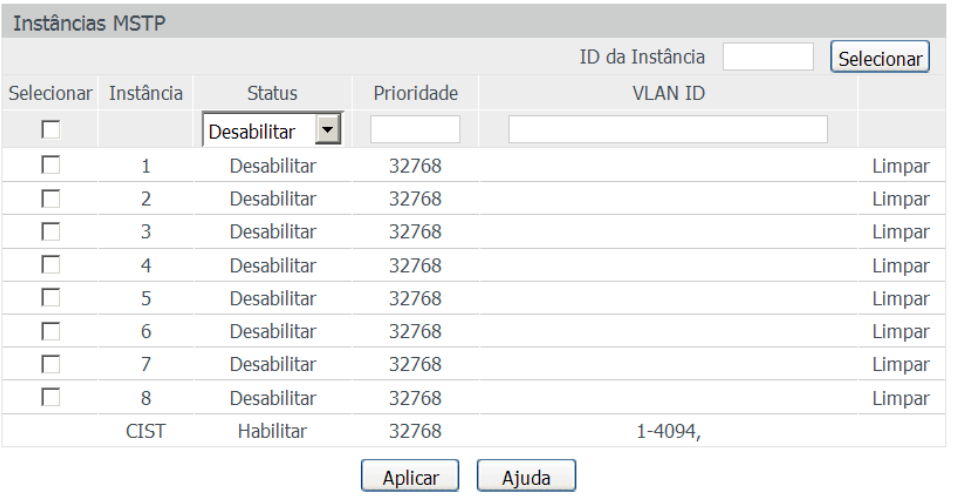
» **Configuração de região MST**
Nome da região: insira um nome para identificar a região MST, utilizando no máximo 32 caracteres.
Revisão: insira um valor de revisão de 0 a 65535 para identificar a região MST.

Instância MST

Nesta página é possível configurar as instâncias MSTP, uma propriedade da região MST, é utilizado para configurar o mapeamento de Instâncias. Você pode atribuir VLANs a diferentes instâncias de acordo com suas necessidades.

Cada Instância é um grupo de VLANs independente uma das outras e do CIST.

Escolha no menu *Spanning Tree* → *Instâncias MSTP* → *Instância MST* para carregar a seguinte página:



Instâncias MSTP

As seguintes informações são apresentadas na tela:

» **Instâncias MSTP**

ID da instância: digite o ID da instância desejada no campo correspondente e clique no botão *Selecionar* para selecioná-la.

Selecionar selecione a Instância desejada. É possível selecionar mais de uma Instância simultaneamente.

Instância: exibe o ID da instância MSTP.

Status: selecione *Habilitar/Desabilitar* para habilitar ou desabilitar o funcionamento da Instância desejada.

Prioridade: digite a prioridade da instância. É um critério importante para determinar se o switch será escolhido como Bridge Root na instância selecionada.

VLAN ID: digite o VLAN ID que pertence ao ID da instância correspondente. Após a modificação, a VLAN ID será apagada e mapeada para a CIST.

Limpar: clique no botão *Limpar* para apagar todas as VLANs ID da instância desejada.

» **Mapeamento de VLAN dentro de instância**

VLAN ID: digite a VLAN ID desejada, após a modificação, a nova VLAN ID será adicionada a identificação da instância correspondente e a VLAN ID anterior será substituída.

ID da instância: digite o ID da instância correspondente.

Obs.: *em uma rede com GVRP e MSTP habilitados, os pacotes GVRP serão encaminhados ao longo da CIST. Se você quiser transmitir pacotes de uma VLAN específica através do GVRP, por favor, certifique-se de mapear a VLAN para CIST durante a configuração da tabela de encaminhamento de VLAN.*

Portas MST

Uma porta pode desempenhar diferentes papéis na instância Spanning Tree. Nesta página você pode configurar os parâmetros das portas em ID's de instâncias diferentes, bem como visualizar o status das portas.

Escolha o menu *Spanning Tree → Instâncias MSTP → Portas MST* para carregar a seguinte página:

Obs.:

Se o Custo do Caminho de uma porta estiver definido como 0, o switch irá alterar automaticamente o valor do custo de acordo com a velocidade de conexão da porta.

Configuração das instâncias MSTP

As seguintes opções são exibidas na tela:

» **Configuração de portas MST**

ID da instância: selecione o ID da instância desejada para configurar os parâmetros da porta.

Porta: digite a porta deseja no campo correspondente e clique no botão *Selecionar* para selecionar a porta.

Selecionar: selecione a porta desejada. É possível selecionar mais de uma porta simultaneamente.

Porta: exibe o número da porta.

Prioridade: digite a prioridade da porta na instância. É um critério importante ao determinar se a porta conectada será escolhida como Porta Root.

Custo do caminho: digite o valor utilizado para determinar o custo do caminho da porta em uma região MST. É um critério importante na determinação da Bridge Root. O valor mais baixo terá maior prioridade.

Função da porta: exibe a função da porta em uma instância MSTP.

Status da porta: exibe o status de funcionamento da porta.

LAG: apresenta o número do grupo LAG a qual a porta pertence.

Obs.: *o Status da Porta de uma mesma porta pode ser diferente em instâncias MSTP distintas.*

Configuração global da função Spanning Tree

Passo	Operação	Descrição
1	Deixar claro os papéis de cada switch nas instâncias de STP: Bridge Root ou Bridge Designada.	Preparação
2	Configuração dos parâmetros globais de MSTP.	Obrigatório. Habilitar o STP no switch e configurar os parâmetros MSTP em: *Spanning Tree* ⟶ *Spanning Tree* ⟶ *Configurar STP.*
3	Configuração dos parâmetros MSTP por porta.	Obrigatório, Configurar os parâmetros MSTP para cada porta: *Spanning Tree* ⟶ *Portas STP* ⟶ *Configurar Portas STP.*
4	Configuração da região MST.	Obrigatório, Criar a região MST e configurar a função que o switch desempenhará na região MST em: *Spanning Tree* ⟶ *Instâncias MSTP* ⟶ *Região MST* e *Instância MST.*
5	Configuração dos parâmetros das portas para cada Instância MSTP.	Opcional, Configurar diferentes instâncias na região MST e configurar os parâmetros das portas para cada instância MSTP: *Spanning Tree* ⟶ *Instâncias MSTP* ⟶ *Portas MST.*

7.4. Segurança STP

Neste submenu é possível configurar a função de proteção STP, pode-se proteger o switch contra dispositivos maliciosos que tentem realizar ataque contra recursos STP. A função *Segurança STP* é configurada nas seguintes páginas: *Proteção STP* e *Intervalo TC Protect*.

Proteção STP evita que dispositivos maliciosos ataquem recursos do STP.

Proteção STP

Nesta página você pode configurar o recurso de proteção de loop, proteção de root, proteção TC, proteção de BPDU e filtro de BPDU por portas.

» **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.

» **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 prioridades 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.

» **TC protect**

O switch remove as entradas de endereços MAC ao receber pacotes TC-BPDU. Se um usuário mal intencionado envia uma grande quantidade de pacotes TC-BPDU para um switch em um curto intervalo de tempo, o switch ficará ocupado realizando a remoção das entradas de endereços MAC, ocasionando a diminuição do desempenho e estabilidade da rede.

Para evitar que o switch remova endereços MAC com frequência, você pode habilitar a função Intervalo TC Protect. Com o Intervalo TC Protect habilitado, será possível determinar a quantidade de pacotes TC-BPDU que a porta poderá receber, definindo um número máximo de recebimento de pacotes no campo TC Threshold, desta forma, o switch não executará a operação de remoção dos endereços MAC, impedindo que o switch fique removendo com frequência as entradas de endereços MAC.

» **BPDU protect**

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 e relata esses casos ao administrador. Se uma porta for desabilitada, somente o administrador poderá restaurá-la.

» **BPDU filter**

Esta proteção é utilizada para evitar uma inundação de BPDUs na rede STP. Se um switch recebe BPDUs maliciosos, ele encaminha estas BPDUs para outros switches conectados na rede, podendo fazer com que o Spanning Tree seja constantemente regenerado. Neste caso o processador do switch ficará sobrecarregado além destas BPDUs atrapalharem a convergência STP.

Com a função BPDU Filter habilitada, uma porta não pode receber ou transmitir BPDUs, apenas envia seus próprios BPDUs. Tal mecanismo evita que o switch seja atacado por BPDUs maliciosas, Garantido que a convergência STP esteja correta.

Entre no menu *Spanning Tree* → *Segurança STP* → *Proteção STP* para carregar a seguinte página:

Proteção STP

As seguintes opções são apresentadas a tela:

» **Configuração de proteção STP**

Porta: digite a porta desejada no campo correspondente e clique no botão *Selecionar* para selecionar a porta.

Selecionar: selecione a porta desejada. É possível selecionar mais de uma porta simultaneamente.

Porta: exibe o número da porta.

Loop protect: selecione *Habilitar/Desabilitar* para habilitar ou desabilitar a função Loop Protect na porta desejada. Esta função evita loops na rede, ocasionada por falhas nos links ou congestionamento na rede.

Root protect: selecione *Habilitar/Desabilitar* para habilitar ou desabilitar a função Root Protect na porta desejada. Esta função evita a alteração da topologia da rede de forma errada, causada pela alteração da Bridge Root atual.

TC protect: selecione *Habilitar/Desabilitar* para habilitar ou desabilitar a função Intervalo TC Protect na porta desejada. Esta função previne a diminuição do desempenho e estabilidade do switch ao receber um número grande de pacotes TC-BPDUs.

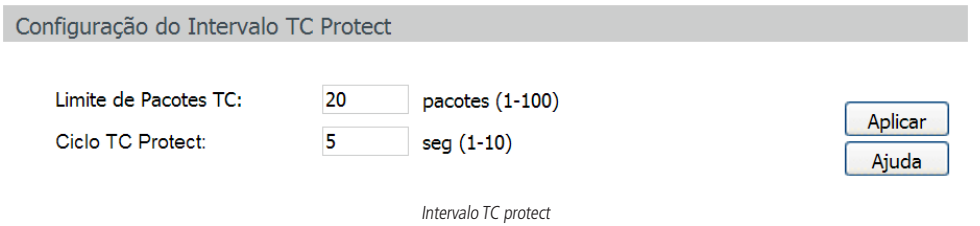
BPDU protect: selecione *Habilitar/Desabilitar* para habilitar ou desabilitar a função BPDU Protect na porta desejada. Esta função previne que a Porta Edge seja atacada por BPDUs maliciosas.

LAG: exibe o número do grupo LAG a qual a porta pertence.

Intervalo TC protect

Quando a porta do switch está com a função TC Protect habilitada, será necessário configurar a quantidade de pacotes TC-BPDUs e o intervalo de tempo de monitoramento utilizado pela função. Estes parâmetros são configurados na página de configuração Intervalo TC Protect.

Entre no menu *Spanning Tree* → *Segurança STP* → *Intervalo TC Protect* para carregar a seguinte página:



Intervalo TC protect

As seguintes opções são exibidas na tela:

» **Configuração do intervalo TC protect**

Limite de pacotes TC: digite o número máximo de pacotes TC-BPDUs que podem ser recebidos em um ciclo TC Protect. A quantidade varia de 1 a 100, o valor padrão é 20.

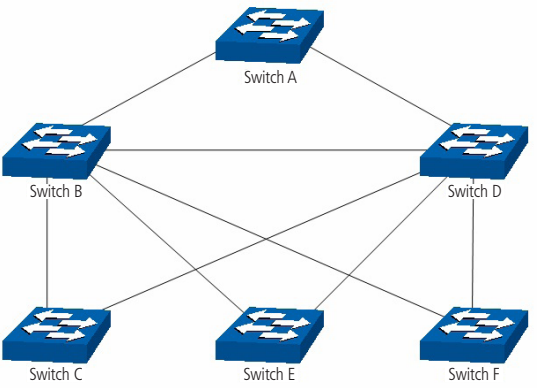
Ciclo TC protect: digite o tempo de duração de um ciclo TC Protect. O tempo varia de 1 a 10 segundos, o valor padrão é 5 segundos.

7.5. Exemplos de aplicações STP

» **Requisitos de rede**

- » Switch A, B, C, D e E todos com suporte a MSTP.
- » Switch A, será o switch central.
- » B e C são switches de convergência. D, E e F são switches da camada de acesso.
- » Existem 6 VLANs, rotuladas como VLAN101 a VLAN106 na rede.
- » Todos os switches executam o MSTP pertencem à mesma região MSTP.
- » Os dados da VLAN101, 103 e 105 são transmitidos pelo STP com o switch B sendo a Bridge Root. Os dados da VLAN102, 104 e 106 são transmitidos pelo STP com o switch C sendo a Bridge Root.

» **Diagrama de rede**



Exemplo de aplicação para STP

» **Procedimento de configuração**

» Configuração do switch A:

Passo	Operação	Descrição
1	Configuração do modo de funcionamento das portas	VLAN ⟶ 802.1Q VLAN, configure o modo de funcionamento das portas como Trunk e adicione nas portas correspondentes as VLAN 101 e VLAN 106. As instruções detalhadas podem ser encontradas na seção 802.1Q VLAN.
2	Habilitar a função STP	Spanning Tree ⟶ Spanning Tree ⟶ Configurar STP, habilite a função STP e selecione a versão MSTP. Spanning Tree ⟶ Portas STP ⟶ Configurar Portas STP, habilite a função MSTP para as portas.
3	Configuração do nome e revisão da região MST	Spanning Tree ⟶ Instâncias MSTP ⟶ Região MST, configure a região como INTELBRAS e mantenha a configuração de revisão padrão.
4	Configuração da Tabela de Encaminhamento da região MST	Spanning Tree ⟶ Instâncias MSTP ⟶ Instância MST, configure a tabela de encaminhamento. Adicione a VLAN 101, 103 e 105 para a instância 1 e mapeie a VLAN 102. 104 e 106 para instância 2.

» Configuração do switch B

Passo	Operação	Descrição
1	Configuração do modo de funcionamento das portas	VLAN ⟶ 802.1Q VLAN, configure o modo de funcionamento das portas como Trunk e adicione nas portas correspondentes as VLAN 101 e VLAN 106. As instruções detalhadas podem ser encontradas na seção 802.1Q
2	Habilitar a função STP	Spanning Tree ⟶ Spanning Tree ⟶ Configurar STP, habilite a função STP e selecione a versão MSTP. Spanning Tree ⟶ Portas STP ⟶ Configurar Portas STP, habilite a função MSTP para as portas.
3	Configuração do nome e revisão da região MST	Spanning Tree ⟶ Instâncias MSTP ⟶ Região MST, configure a região como INTELBRAS e mantenha a configuração de revisão padrão.
4	Configuração da Tabela de Encaminhamento da região MST	Spanning Tree ⟶ Instâncias MSTP ⟶ Instância MST, configure a tabela de encaminhamento. Adicione a VLAN 101, 103 e 105 para a instância e mapeie a VLAN 102. 104 e 106 para instância 2.
5	Configuração do switch B como Bridge Root para instância 1	Spanning Tree ⟶ Instâncias MSTP ⟶ Instância MST, configure a prioridade da instância 1 para 0.
6	Configuração das Bridges Designadas da instância 2	Spanning Tree ⟶ Instâncias MSTP ⟶ Instância MST, configure a prioridade da instância 2 para 4096.

» Configuração do switch C:

Passo	Operação	Descrição
1	Configuração do modo de funcionamento das portas	VLAN ⟶ 802.1Q VLAN, configure o modo de funcionamento das portas como Trunk e adicione nas portas correspondentes as VLAN 101 e VLAN 106. As instruções detalhadas podem ser encontradas na seção 802.1Q VLAN.
2	Habilitar a função STP	Spanning Tree ⟶ Spanning Tree ⟶ Configurar STP, habilite a função STP e selecione a versão MSTP. Spanning Tree ⟶ Portas STP ⟶ Configurar Portas STP, habilite a função MSTP para as portas.
3	Configuração do nome e revisão da região MST	Spanning Tree ⟶ Instâncias MSTP ⟶ Região MST, configure a região como INTELBRAS e mantenha a configuração de revisão padrão.
4	Configuração da Tabela de Encaminhamento da região MST	Spanning Tree ⟶ Instâncias MSTP ⟶ Instância MST, configure a tabela de encaminhamento. Adicione a VLAN 101, 103 e 105 para a instância 1 e mapeie a VLAN 102. 104 e 106 para instância 2.
5	Configuração do switch C como Bridge Root para instância 1	Spanning Tree ⟶ Instâncias MSTP ⟶ Instância MST, configure a prioridade da instância 1 para 0.
6	Configuração do switch C como Bridge Designada para a instância 2	Spanning Tree ⟶ Instâncias MSTP ⟶ Instância MST, configure a prioridade da instância 2 para 4096.

» Configuração do switch D

Passo	Operação	Descrição
1	Configuração do modo de funcionamento das portas	VLAN ⟶ 802.1Q VLAN, configure o modo de funcionamento das portas como Trunk e adicione nas portas correspondentes as VLAN 101 e VLAN 106. As instruções detalhadas podem ser encontradas na seção 802.1Q VLAN.
2	Habilitar a função STP	Spanning Tree ⟶ Spanning Tree ⟶ Configurar STP, habilite a função STP e selecione a versão MSTP. Spanning Tree ⟶ Portas STP ⟶ Configurar Portas STP, habilite a função MSTP para as portas.
3	Configuração do nome e revisão da região MST	Spanning Tree ⟶ Instâncias MSTP ⟶ Região MST, configure a região como INTELBRAS e mantenha a configuração de revisão padrão.
4	Configuração da Tabela de Encaminhamento da região MST	Spanning Tree ⟶ Instâncias MSTP ⟶ Instância MST, configure a tabela de encaminhamento. Adicione a VLAN 101, 103 e 105 para a instância 1 e mapeie a VLAN 102. 104 e 106 para instância 2.

Obs.: *O procedimento de configuração dos switches E e F são as mesmas do switch D.*

» **Diagrama da topologia das duas instâncias, após a convergência STP**

» Para a instância 1 (VLAN 101,103 e 105), os caminhos em vermelhos na figura a seguir são os links ativos, os caminhos cinza são os links bloqueados.

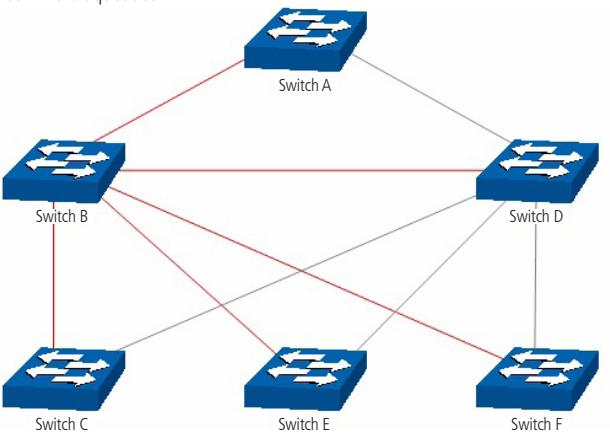


Diagrama da instância 1 após a convergência STP

» Para a instância 2 (VLAN 102, 104 e 106) os caminhos em azul na figura a seguir são os links ativos, os caminhos cinza são os links bloqueados.

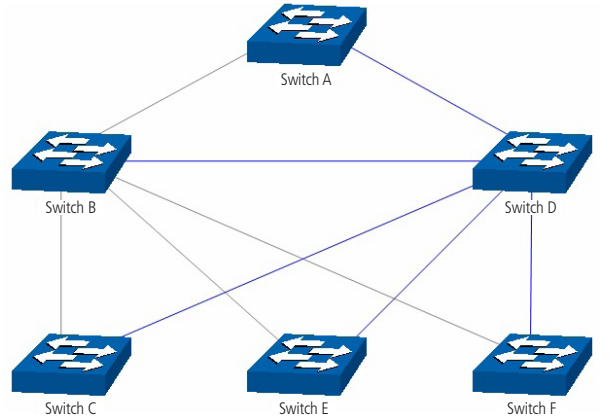


Diagrama da instância 2 após a convergência STP

» **Sugestões para configuração**
  » Habilitar o TC Protect para todas as portas dos switches.
  » Habilitar o Root Protect em todas as portas do switch Bridge Root.
  » Habilitar o Loop Protect nas portas Non-Edge.

Habilitar a BPDU Protect ou BPDU Filter para as portas que estão conectadas diretamente em computadores ou servidores.

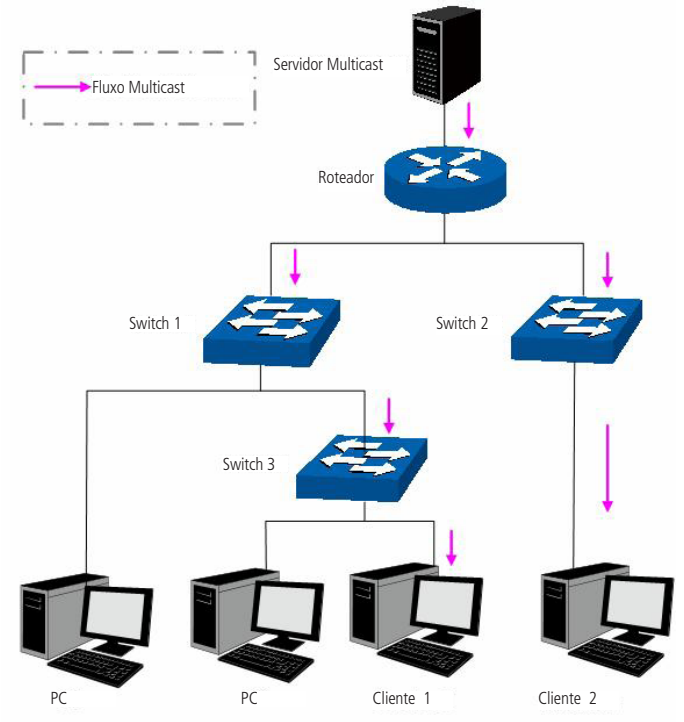
8. Multicast

» Visão global do multicast

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

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

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



Tráfego multicast

Funções do multicast

1. Em uma rede ponto a multiponto, o número de clientes solicitando um serviço é desconhecido, neste caso, o Multicast otimiza os recursos da rede.

2. Os clientes que recebem a mesma informação do servidor Multicast, formam um Grupo Multicast, Deste modo o servidor Multicast necessita enviar apenas uma única vez a mensagem.
3. Cada cliente pode entrar ou sair do Grupo Multicast a qualquer momento.
4. Em aplicações em tempo real, é aceitável ocorrer algumas perdas de pacotes (dentro de um limite que não prejudique o serviço).

» **Endereços multicast**

1. Endereços IP Multicast:

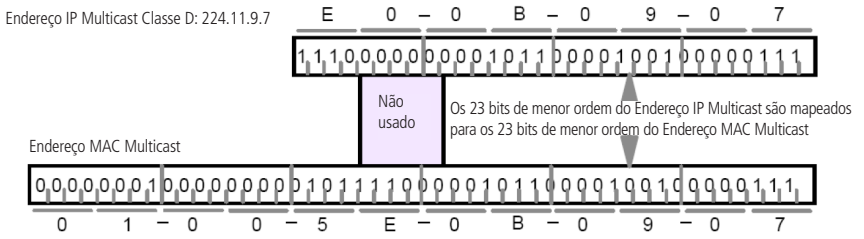
   Conforme especificado pelo IANA (Internet Assigned Numbers Authority), os endereços Ips de classe D são usados como endereços Multicast. O intervalo de endereços Multicast vai de 224.0.0.0 a 239.255.255.255. A tabela a seguir exibe o intervalo e descrição de vários endereços Multicast especiais.

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

2. Endereços MAC multicast:

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

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



Endereço MAC multicast

» **Tabela de endereços multicast:**

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

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

VLAN ID	Multicast IP	Porta

Tabela de endereços multicast

» **IGMP Snooping**

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

A função Multicast possui quatro submenus de configuração: *IGMP Snooping, Multicast Estático, Filtro Multicast e Estatísticas IGMP*.

8.1. IGMP Snooping

» **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.

» **Mensagens IGMP**

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

1. IGMP Query (Consulta IGMP): as mensagens IGMP Query (Consulta IGMP) enviadas pelo servidor Multicast podem ser classificadas de duas formas: IGMP General Query (Consulta Geral) ou Group-Specific-Query (Consulta a Grupo Específico). O servidor envia regularmente mensagens de consulta geral, para verificar se os grupos Multicast possuem membros. Ao receber mensagens IGMP Leave, o switch encaminhará as mensagens de consulta ao grupo Multicast específico enviadas pelo servidor Multicast para as portas pertencentes ao grupo, para verificar se outros membros do grupo ainda necessitam do serviço Multicast.
2. IGMP Report (Relatório IGMP): as mensagens IGMP Report são enviadas pelos clientes quando desejam se associar (join) a um grupo Multicast ou responder as mensagens de consulta IGMP (IGMP Query) do servidor Multicast. Ao receber uma mensagem IGMP Report, o switch encaminhará a mensagem de relatório através da porta denominada "Porta do Roteador" para o servidor Multicast, além de analisar a mensagem para obter o endereço do grupo Multicast que o cliente irá se juntar. A porta de recepção do switch procederá da seguinte maneira: se a porta que o cliente está conectado no switch é um novo membro para um grupo Multicast, a porta será adicionada a Tabela de endereços Multicast, se a porta que o cliente está conectado já pertence ao grupo Multicast, o tempo de permanência da porta ao grupo Multicast será reiniciado.
3. IGMP Leave (Remoção do Grupo Multicast): clientes que executam o IGMP v1 não enviam mensagens IGMP Leave ao sair de um grupo Multicast, como resultado, o switch somente removerá a porta da Tabela de endereços Multicast após o término do tempo de vida da porta na tabela de endereços. Os clientes que executam IGMP v2 ou IGMP v3, enviam mensagens IGMP Leave ao sair de um grupo Multicast para informar ao servidor Multicast a sua saída.Ao receber mensagens IGMP Leave, o switch encaminha as mensagens de consulta ao grupo Multicast específico enviadas pelo servidor Multicast para as portas pertencentes ao grupo, para verificar se outros membros do grupo ainda necessitam do serviço Multicast e reiniciar o tempo de permanência da porta na Tabela de endereços Multicast.

» **Fundamentos do IGMP Snooping**

1. 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.
2. 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.

A função IGMP Snooping pode ser configurada nas seguintes páginas: *IGMP Snooping, Portas IGMP, VLAN e Multicast VLAN.*

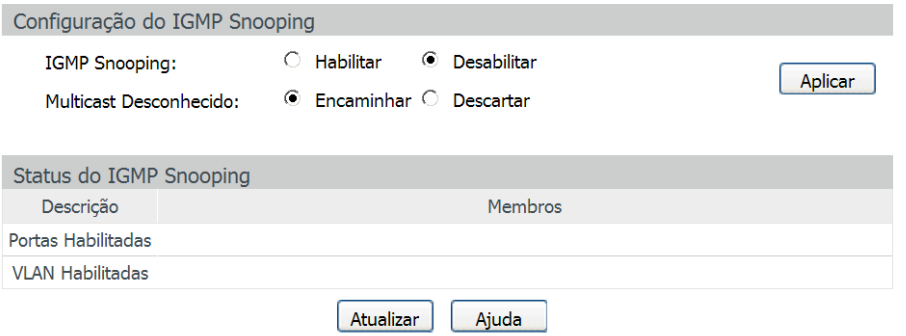
IGMP Snooping

Nesta página é possível habilitar a função IGMP Snooping no switch.

Se o endereço Multicast dos dados recebidos não estiver 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. Por favor, configure esse recurso de acordo com suas necessidades.

Escolha o menu *Multicast* → *IGMP Snooping* → *IGMP Snooping* para carregar a seguinte página.



Configuração IGMP snooping

» **Configuração do IGMP Snooping**

IGMP Snooping: selecione *Habilitar/Desabilitar* para habilitar ou desabilitar a função IGMP Snooping no switch.

Multicast desconhecido: selecione a operação que o switch irá fazer ao receber Multicast desconhecido:

» **Encaminhar:** 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.

» **Status do IGMP Snooping**

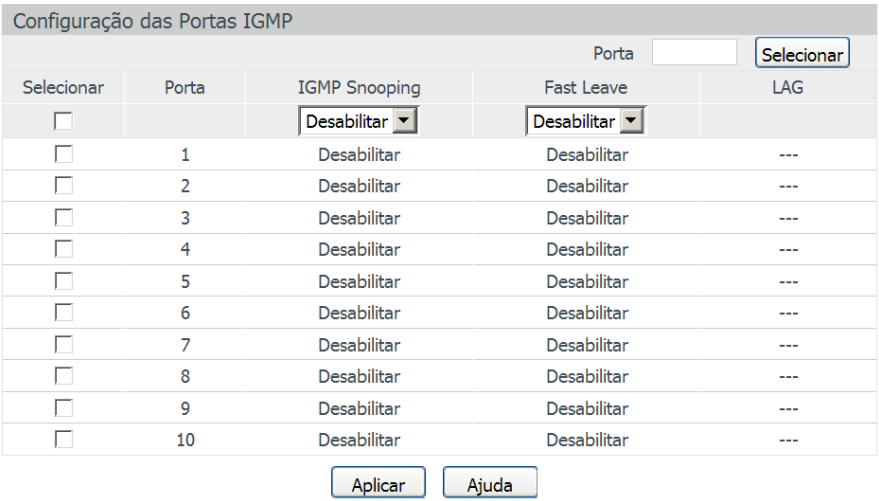
Descrição: exibe o status da configuração IGMP Snooping.

Membros: exibe as portas e VLANs habilitadas para a função IGMP Snooping.

Portas IGMP

Nesta página você pode configurar a função IGMP nas portas desejadas do switch.

Entre no menu *Multicast* → *IGMP Snooping* → *Portas IGMP* para carregar a seguinte página:



Portas IGMP

As seguintes opções são exibidas na tela:

» **Configuração das portas IGMP**

Porta: digite a porta deseja no campo correspondente e clique no botão *Selecionar* para selecionar a porta.

Selecionar: selecione a porta desejada. É possível selecionar mais de uma porta simultaneamente.

Porta: exibe o número da porta.

IGMP Snooping: selecione *Habilitar/Desabilitar* para habilitar ou desabilitar a função IGMP Snooping na porta desejada.

Fast Leave: selecione *Habilitar/Desabilitar* para habilitar ou desabilitar a função Fast Leave na porta 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.

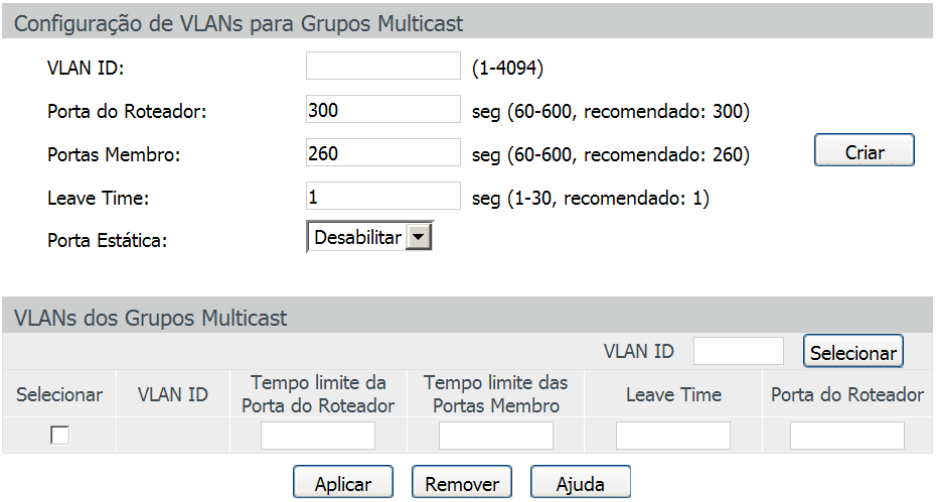
LAG: exibe o número do grupo LAG a qual a porta pertence.

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

VLAN

Grupos Multicast estabelecidos com a utilização de IGMP Snooping são baseados em VLANs. Nesta página você pode configurar diferentes parâmetros do IGMP para diferentes VLANs.

Escolha no menu *Multicast → IGMP Snooping → VLAN*, para carregar a seguinte página:



Obs.:

Estas configurações serão inválidas quando a função Multicast VLAN estiver habilitada.

VLANs de grupos multicast

As seguintes opções são exibidas na tela:

» **Configuração de VLANs para grupos multicast**

VLAN ID: digite a VLAN ID para habilitar o *IGMP Snooping* na VLAN desejada.

Porta do roteador: especifique o tempo de vida da Porta do Roteador. Se o switch não receber mensagens IGMP Query da porta em que o servidor Multicast estiver conectado dentro de um intervalo de tempo, a porta não será mais considerada como Porta da Roteador. O valor padrão é *300* segundos.

Portas membro: especifique o tempo de vida 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 será removida da Tabela de endereços Multicast. O valor padrão é *260* segundos.

Leave Time: especifique o intervalo de tempo entre o switch receber uma mensagem de Leave de um cliente e o servidor Multicast remover o cliente do grupo Multicast. O valor padrão é *1* segundo.

Porta estática: selecione a Porta do Roteador manualmente.

» **VLANs dos grupos multicast**

VLAN ID: digite a VLAN ID no campo correspondente e clique no botão *Selecionar* para selecionar a VLAN desejada.

Selecionar: selecione a VLAN ID desejada. É possível selecionar mais de uma VLAN ID simultaneamente.

Tempo limite da porta do roteador: exibe o tempo de vida configurado para a Porta do Roteador.

Tempo limite das portas membro: exibe o tempo de vida configurado para as Portas Membro.

Leave Time: exibe o Leave Time configurado.

Porta do roteador: exibe o número da porta configurado como Porta do Roteador.

Obs.: *essas configurações não serão válidas se a função* Multicast VLAN *estiver habilitada.*

Procedimento de configuração

Passo	Operação	Descrição
1	Habilitar a função IGMP snooping	Obrigatório, Habilitar as configurações globais do IGMP Snooping do switch e das portas em: Multicast ⟶ IGMP Snooping ⟶ IGMP Snooping e Portas IGMP.
2	Configurar os parâmetros de Multicast para as VLANs	Opcional, Configurar os parâmetros Multicast das VLANs em: Multicast⟶IGMP Snooping ⟶ VLAN, se uma VLAN não tem parâmetros de configuração Multicast, indica que o IGMP Snooping não está habilitado na VLAN, assim os dados Multicast na VLAN serão enviados em broadcast.

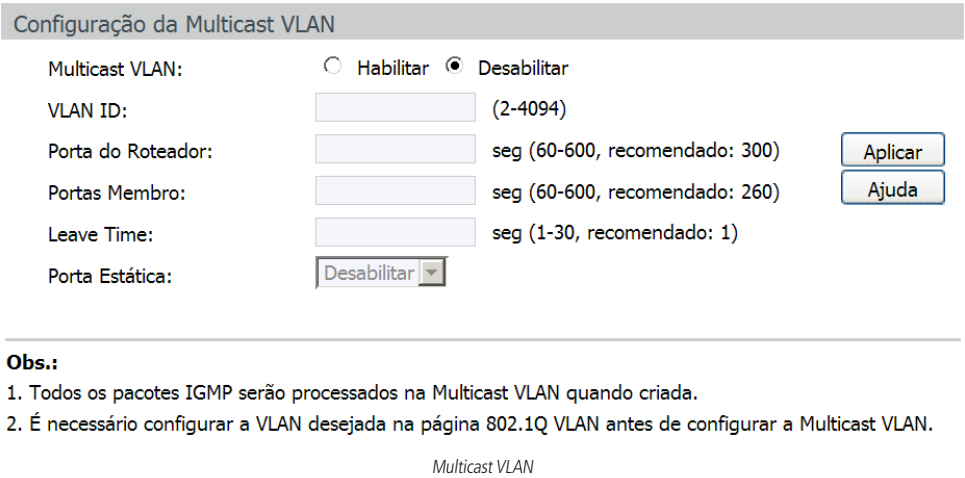
Multicast VLAN

Em transmissões Multicast, quando usuários de diferentes VLANs participam do mesmo grupo Multicast, o servidor Multicast irá duplicar as informações e encaminhará para as VLANs correspondentes, desperdiçando largura de banda e recursos do switch.

Este problema pode ser resolvido por meio do recurso Multicast VLAN. Ao adicionar as portas do switch para Multicast VLAN e habilitar o IGMP Snooping é possível compartilhar a Multicast VLAN entre clientes de diferentes VLANs, economizando largura de banda e recursos do switch, pois os fluxos Multicast são transmitidos somente na Multicast VLAN.

Antes de configurar uma Multicast VLAN é necessário criar uma VLAN (802.1Q) e adicionar as portas correspondentes. Ao ativar uma Multicast VLAN as configurações Multicast das outras VLANs serão desabilitadas, isto é, o tráfego Multicast somente será permitido dentro da Multicast VLAN.

Escolha no menu *Multicast* ⟶ *IGMP Snooping* ⟶ *Multicast VLAN* para carregar as páginas.



Multicast VLAN

As seguintes opções são exibidas na tela:

» **Configuração da multicast VLAN**

Multicast VLAN: selecione *Habilitar/Desabilitar* para habilitar ou desabilitar a função Multicast VLAN.

VLAN ID: digite o VLAN ID utilizado pelo Multicast VLAN.

Porta do roteador: especifique o tempo de vida 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 da Roteador. O valor padrão é *300*.

Portas membro: especifique o tempo de vida 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 será removida da Tabela de endereços Multicast. O valor padrão é *260* segundos.

Leave Time: especifique o intervalo de tempo entre o switch receber uma mensagem de Leave de um cliente e o servidor Multicast remover o cliente do grupo Multicast. O valor padrão é *1* segundo.

Porta estática: selecione a Porta do Roteador manualmente.

Obs.: » *A porta em que o servidor Multicast estiver conectado ao switch deve estar na Multicast VLAN, caso contrário, os clientes podem não receber o fluxo do Multicast.*

» *A função Multicast VLAN não terá efeito caso as portas correspondentes não estejam configuradas na VLAN (802.1Q) correspondente.*

» *O modo de funcionamento da porta deverá estar no modo Híbrida.*

» *Configure o modo de funcionamento da porta em que o servidor Multicast está conectado ao switch como Trunk ou como Híbrida com regra de saída TAG, caso contrário, todas as portas membros do Multicast VLAN não receberão tráfego Multicast.*

» *Depois que uma Multicast VLAN for criada, todos os pacotes IGMP serão processados pela Multicast VLAN.*

Procedimentos de configuração

Passo	Operação	Descrição
1	Habilitar a função IGMP Snooping	Obrigatório - Habilitar as configurações globais de IGMP Snooping e de portas em: Multicast ⟶ IGMP Snooping ⟶ IGMP Snooping e Portas IGMP.
2	Criar a VLAN que será utilizada pelo Multicast VLAN	Obrigatório - Criar a VLAN desejada que será utilizada na Multicast VLAN, adicionando as portas utilizadas pelo tráfego Multicast: VLAN ⟶ 802.1Q VLAN
3	Configura os parâmetros para o Multicast VLAN	Obrigatório - habilitar e configurar a Multicast VLAN em: Multicast ⟶ IGMP Snooping ⟶ Multicast VLAN. Recomenda-se manter os parâmetros de tempo padrão.
4	Visualizar as configurações	Se for configurado com êxito, o VLAN ID da Multicast VLAN será exibido na tela Status do IGMP Snooping em: Multicast ⟶ IGMP Snooping ⟶ IGMP Snooping.

Exemplo de aplicação para Multicast VLAN

» **Requerimentos de rede**

Servidores Multicast enviam fluxos de Multicast através de roteadores e os fluxos são transmitidos para o cliente A e B através do switch.

Roteador: a porta WAN é conectada ao servidor Multicast, a porta LAN é conectada no switch. Os pacotes Multicast são transmitidos na VLAN3.

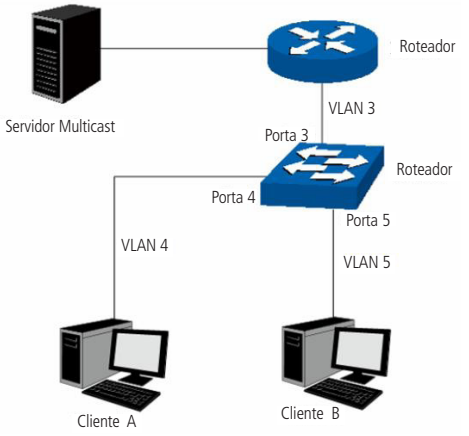
Switch: a porta 3 está conectada ao roteador e os pacotes são transmitidos na VLAN 3; a porta 4 é o cliente A e os pacotes são transmitidos na VLAN 4; a porta 5 está conectada ao cliente B e os pacotes são transmitidos na VLAN 5.

Cliente A: conectado na porta 4 do switch.

Cliente B: conectado na porta 5 do switch.

Configure o Multicast VLAN e os clientes A e B para receberem os fluxos de dados Multicast na Multicast VLAN.

» **Diagrama de rede**



Aplicação multicast

Procedimento de configuração

Passo	Operação	Descrição
1	Criar VLANs	Crie três VLANs (VLAN 3, 4 e 5 respectivamente) e especifique a descrição da VLAN 3 como Multicast VLAN em: VLAN ⟶ 802.1Q VLAN ⟶ Configurar VLAN.
2	Configurar o modo de funcionamento das portas	Configure em: VLAN ⟶ 802.1Q VLAN ⟶ Modo da Porta e PVID. Para a porta 3, configurar o modo de funcionamento da porta como Híbrida e regra de saída como TAG e adicione-a nas VLAN 3, VLAN 4 e VLAN 5. Para a porta 4, configurar o modo de funcionamento como Híbrida, e regra de saída como UNTAG e adicione-a nas VLAN 3 e VLAN 4. Para a porta 5, configurar o modo de funcionamento como Híbrida, e regra de saída como UNTAG e adicione-a nas VLAN 3 e VLAN 5.
3	Habilitar a função IGMP Snooping	Em Multicast ⟶ IGMP Snooping ⟶ IGMP Snooping, habilitar globalmente a função IGMP Snooping. Em Multicast ⟶ IGMP Snooping ⟶ Portas IGMP, habilitar o IGMP Snooping para as porta 3, porta 4 e porta 5.
4	Habilitar Multicast VLAN	Em Multicast ⟶ IGMP Snooping ⟶ Multicast VLAN, habilitar a Multicast VLAN e configurar o VLAN ID da Multicast VLAN como 3 e manter os demais parâmetros como padrão.
5	Checar a Multicast VLAN	A Multicast VLAN 3 será exibida na tabela de status do IGMP Snooping em: Multicast ⟶ IGMP Snooping ⟶ IGMP Snooping.

8.2. Multicast estático

Em uma rede, os clientes podem se juntar a diferentes grupos Multicast, dependendo da sua necessidade. O switch encaminha o trafego Multicast com base em sua Tabela de endereços Multicast. O IP Multicast pode ser configurado manualmente nas páginas: *Endereços Multicast e Multicast Estático.*

Endereços multicast

Nesta página você pode visualizar a Tabela de endereços Multicast do switch.

Escolha no menu: *Multicast ⟶ Multicast Estático ⟶ Endereços Multicast* para carregar a seguinte página.

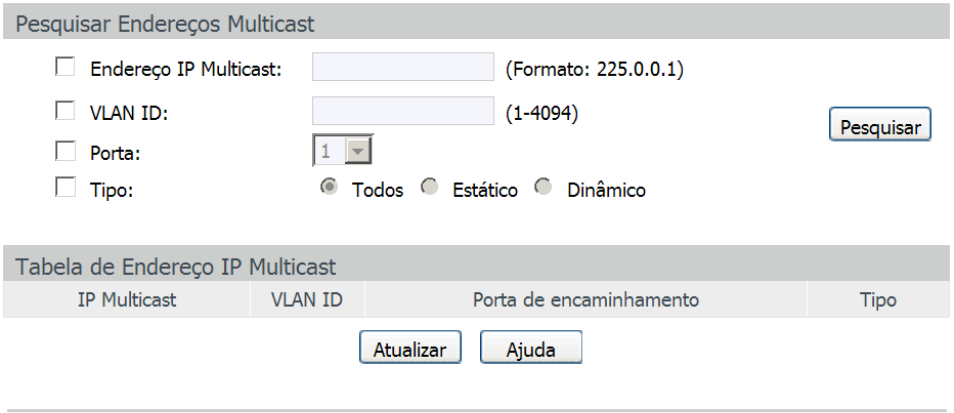


Tabela de endereços multicast

As seguintes opções são exibidas na tela:

» **Pesquisar endereços multicast**
Endereço IP multicast: digite endereço IP Multicast desejado para visualizar suas configurações.
VLAN ID: digite a VLAN ID desejada para visualizar as configurações Multicast.
Porta: selecione o número da porta desejada.
Tipo: selecione o tipo da entrada desejada.

- » **Todos:** exibe todas as entradas de endereços IP Multicast.
- » **Estático:** exibe todos os endereços IPs Multicast estático.
- » **Dinâmico:** exibe todos os endereços IPs Multicast dinâmicos.

» **Tabela de endereço IP multicast**

Multicast IP: exibe o endereço IP Multicast.

VLAN ID: exibe a VLAN ID do grupo Multicast.

Porta de encaminhamento: exibe as portas participantes do grupo Multicast.

Tipo: exibe o tipo de IP Multicast.

Obs.: *caso as configurações de VLANs e Multicast VLAN forem alteradas, o switch irá renovar os endereços dinâmicos na Tabela de endereços Multicast e aprenderá os novos endereços Multicast.*

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.

Escolha no menu *Multicast* → *Multicast Estático* → *Multicast Estático* para carregar a seguinte página:

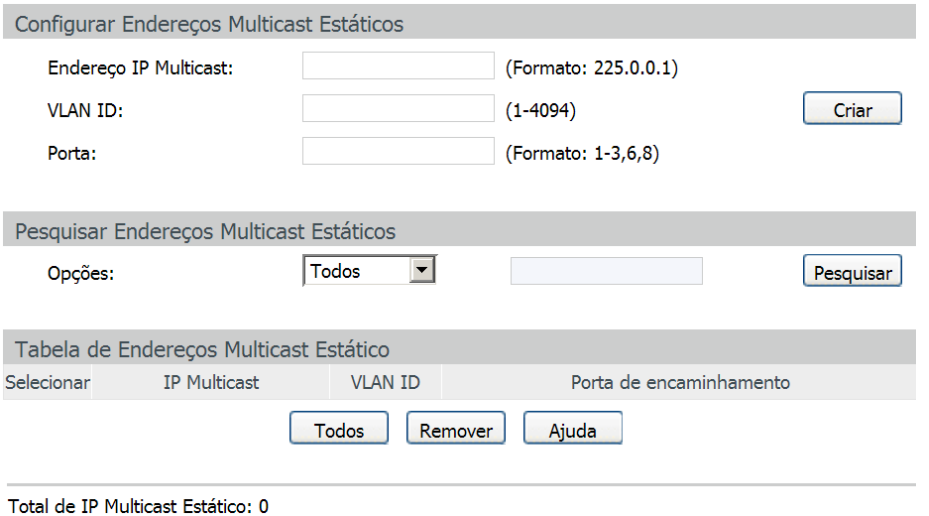


Tabela de endereços multicast estática

As seguintes opções são exibidas na tela:

» **Configurar endereços multicast estáticos**

Endereço IP multicast: digite o endereço IP Multicast desejado para adicioná-lo na Tabela de endereços Multicast Estático.

VLAN ID: digite a VLAN ID que pertence o endereço IP Multicast.

Porta: digite as portas de encaminhamento utilizado pelo grupo Multicast. Utilize o formato (1-3, 6, 9).

» **Pesquisar endereços multicast estáticos**

Opções: selecione o modo de pesquisa desejado para exibição da Tabela de endereços Multicast Estático e clique no botão *Pesquisar*.

- » **Todos:** exibe todos os endereços da Tabela de endereços Multicast Estáticos.
- » **IP multicast:** digite o endereço IP Multicast para visualizar a entrada correspondente da Tabela de endereços Multicast Estático.
- » **VLAN ID:** digite a VLAN ID para visualizar a entrada correspondente da Tabela de endereços Multicast Estático.
- » **Porta:** digite o número da porta desejada para visualizar os endereços correspondentes da Tabela de endereços Multicast Estático.

» **Tabela de endereços multicast estático**

Selecionar: selecione o endereço IP Multicast desejado e clique no botão *Remover* para removê-lo da Tabela de endereços Multicast Estático. É possível selecionar mais de uma entrada simultaneamente.

IP multicast: exibe o endereço IP Multicast.

VLAN ID: exibe a VLAN ID do Grupo Multicast.

Porta de encaminhamento: exibe as portas de encaminhamento utilizado pelo grupo Multicast.

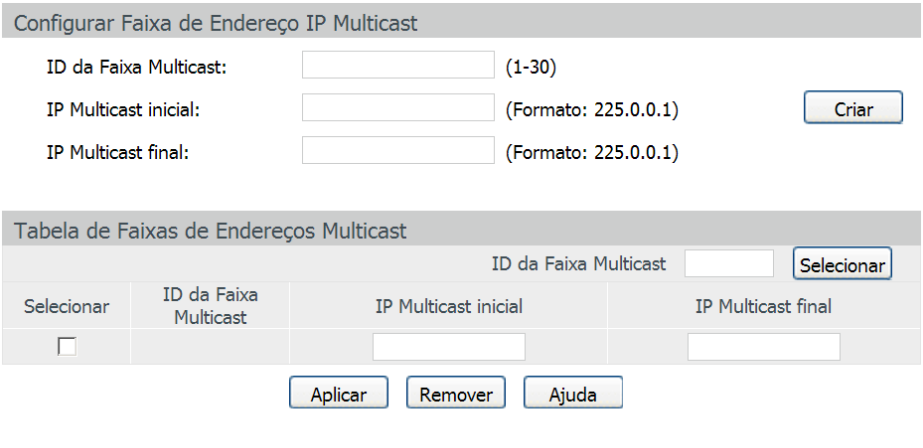
8.3. Filtro multicast

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

Faixa de IP multicast

Nesta página é possível configurar e visualizar a faixa de endereços IP Multicast utilizados pela função Filtro Multicast.

Entre no menu *Multicast* → *Filtro Multicast* → *Faixa de IP Multicast* para carregar a seguinte página:



Faixa de endereços multicast

As seguintes opções são exibidas na tela:

» **Configurar faixa de endereço IP multicast**

ID da faixa multicast: digite o ID da faixa de endereços Multicast que será criado.

IP multicast inicial: digite o endereço IP Multicast inicial utilizados pela faixa de endereços que será criada.

IP multicast final: digite o endereço IP Multicast final utilizados pela faixa de endereços que será criada.

Criar: clique no botão *Criar*, para criar a faixa de endereços.

» **Tabela de faixas de endereços multicast**

ID da faixa multicast: digite o ID da faixa de endereços Multicast e clique no botão *Selecionar* para selecionar a faixa desejada.

Selecionar: selecione a faixa de endereços Multicast desejada. É possível selecionar mais de uma faixa simultaneamente.

ID da faixa multicast: exibe o ID de identificação da faixa de endereços Multicast.

IP multicast inicial: exibe o endereço IP Multicast inicial da faixa criada.

IP multicast final: exibe o endereço IP Multicast final da faixa criada.

Porta filtrada

Nesta página é possível configurar as regras de Filtro Multicast para cada porta do switch.

Escolha o menu *Multicast* → *Filtro Multicast* → *Porta Filtrada* para carregar a seguinte página.

Obs.:

1. Porta filtrada não possui efeito sobre os Endereços IP Multicast Estáticos.
2. É possível vincular até 5 IDs de faixas Multicast. Por favor, utilize o formato 1,5,8.

Filtro multicast

As seguintes opções são apresentadas na tela:

» **Configuração da porta filtrada**

Porta: digite a porta deseja no campo correspondente e clique no botão *Selecionar* para selecionar a porta.

Selecionar: selecione a porta desejada. É possível selecionar mais de uma porta simultaneamente.

Porta: exibe o número da porta.

Filtrar: selecione *Habilitar/Desabilitar* para habilitar ou desabilitar função de filtro Multicast na porta desejada.

Ação: selecione o modo como o switch irá processar os pacotes Multicast quando o endereço IP Multicast estiver dentro da faixa de endereços:

» **Permitir:** apenas os pacotes Multicast que possuem endereço IP Multicast dentro da faixa configurada serão encaminhados pelo switch.

» **Negar:** apenas os pacotes Multicast, que possuem endereço IP Multicast dentro da faixa configurada serão descartados pelo switch.

Vincular ID da faixa multicast: digite o ID da faixa de endereços Multicast que a porta será vinculada.

Qtd. grupos: especifique o número máximo de grupos Multicast, para evitar que algumas portas utilizem muita largura de banda.

LAG: exibe o número do grupo LAG que a porta pertence.

Obs.: » *A função de Filtro Multicast somente funcionará em uma VLAN com IGPM Snooping habilitado.*

» *A função de Filtro Multicast não terá efeito sobre endereços IP Multicast Estático.*

» *Pode ser vinculado até 5 faixas de endereços Multicast em cada porta. Utilize o formato: 1, 5, 8.*

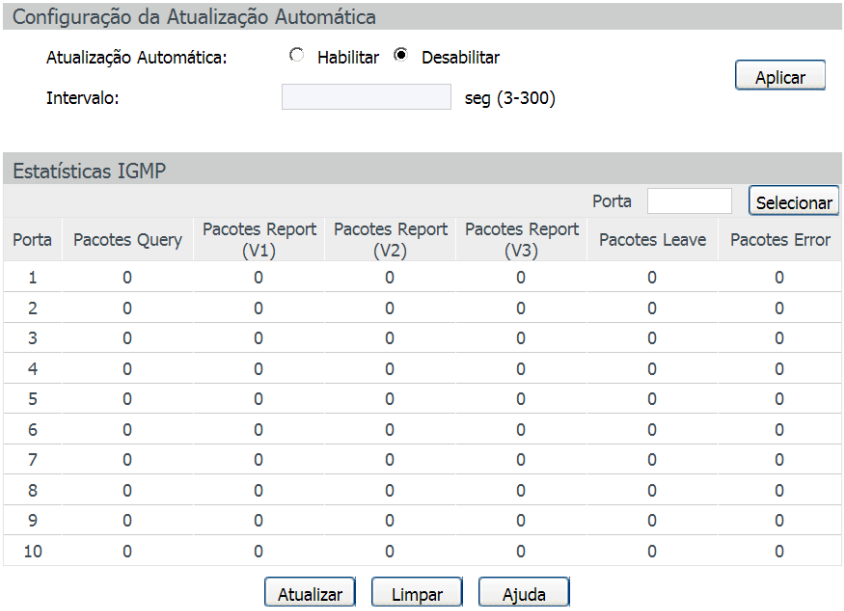
Procedimento de configuração

Passo	Operação	Descrição
1	Configure a faixa de endereços IP Multicast que será utilizada pelo Filtro Multicast.	Obrigatório, Configure a faixa de endereços que será filtrado: Multicast ⟶ Filtro Multicast ⟶ Faixa de IP Multicast.
2	Configure as regras de Filtro Multicast para cada porta do switch.	Obrigatório, Configure as regras de Filtro Multicast para as portas: Multicast ⟶ Filtro Multicast ⟶ Porta Filtrada.

8.4. Estatísticas IGMP

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

Escolha no menu *Multicast* ⟶ *Estatísticas IGMP* para carregar a seguinte página:



Estatísticas dos pacotes IGMP

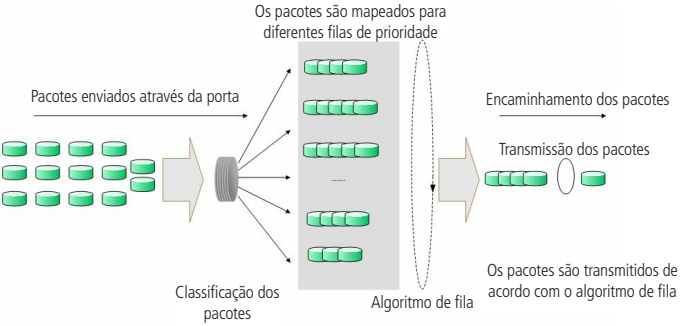
As seguintes opções são exibidas na tela:

» **Configuração da atualização automática**
Atualização automática: selecione *Habilitar/Desabilitar* para habilitar ou desabilitar a função de atualização automática.
Intervalo: digite um intervalo de 3 a 300 segundos, para especificar o período de atualização automática.

» **Estatísticas IGMP**
Porta selecionar: digite a porta desejada no campo correspondente e clique no botão *Selecionar* para selecionar a porta.
Porta: exibe o número da porta.
Pacotes query: exibe o número de pacotes IGMP Query que a porta recebeu.
Pacotes report (V1): exibe o número de pacotes IGMP Report v1 que a porta recebeu.
Pacotes report (V2): exibe o número de pacotes IGMP Report v2 que a porta recebeu.
Pacotes report (V3): exibe o número de pacotes IGMP Report v3 que a porta recebeu.
Pacotes Leave: exibe o número de pacotes IGMP Leave que a porta recebeu.
Pacotes error: exibe o número de pacotes IGMP Error que a porta recebeu.

9. QoS

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



QoS

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

» **Tipos de prioridades**

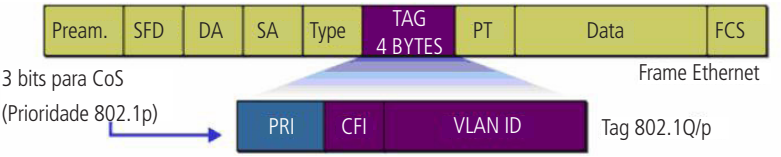
O switch implementa três modelos de prioridades, Prioridade por Porta, por 802.1P e DSCP. Por padrão, o modo de prioridade por portas vem ativado e os demais modos são opcionais.

1. Prioridade por porta

   Neste modo de prioridade o fluxo de dados será mapeado para as filas de saída conforme a regra de CoS definido para cada porta.

2. Prioridade 802.1P

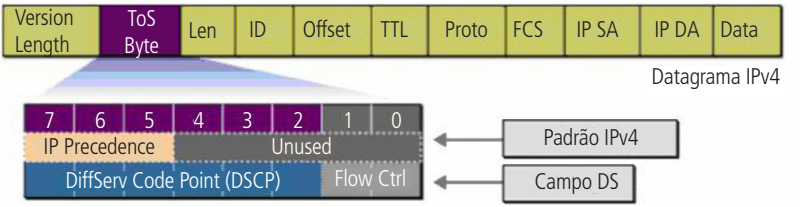
   De acordo com a figura a seguir, cada TAG 802.1Q inserida no quadro Ethernet possui um campo denominado *PRI*, este campo, possui 3 bits que são utilizados para a classificação e priorização do pacote, sendo possível configurar até 8 níveis de priorização (0 a 7). Na página de gerenciamento web, é possível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



TAG 802.1Q

3. Prioridade DSCP

De acordo com a figura a seguir. o campo *ToS* (Type Of Service) do cabeçalho IP possui 1 byte, ou seja 8 bits. Os três primeiros bits indicam a Precedência IP e variam dentro do intervalo que vai de 0 a 7, os cinco bits restantes não são utilizados. A RFC 2474 redefiniu o campo ToS do datagrama IP, chamando-o de campo *DS* (Differentiated Service), deste modo, os 6 primeiros bits mais significativos (bit 7 ao bit 2), diferenciam os pacotes recebidos em classes de tráfego, conforme informações de atraso, processamento e confiabilidade, os dois últimos bits menos significativos (bit 1 e bit 0) são reservados. É possível configurar até 64 classes de tráfego DSCP, este intervalo é configurado dentro da faixa que vai de 0 a 63.

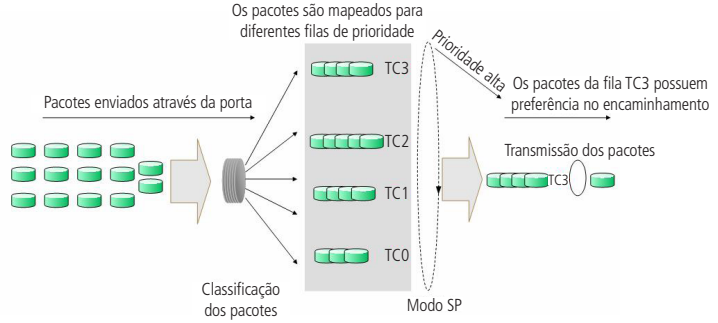


Datagrama IP

» **Algoritmo de fila**

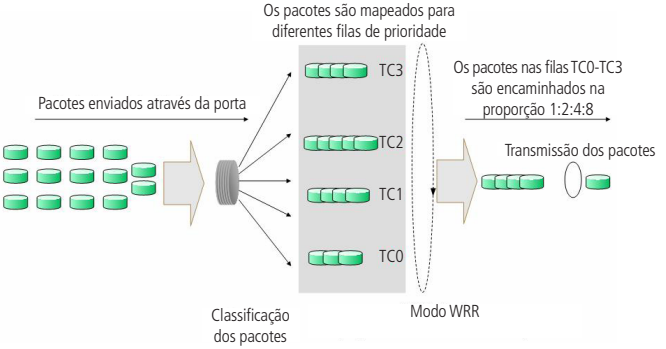
Quando a rede está congestionada, muitos pacotes podem ser perdidos ou chegarem com atrasos em seus destinos, ocasionando lentidão e prejudicando os serviços utilizados pela rede. Estes problemas podem ser resolvidos com a utilização de algoritmos de fila. O switch implementa 4 filas de prioridade: *TC0,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

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



Algoritmo SP

2. WRR: algoritmo *WRR* (Weight Round Robin). Neste modo, os pacotes de todas as filas serão enviados de acordo com o peso de cada fila, este peso indica a proporção ocupada pelo recurso. As filas de prioridades são atendidas em ordem pelo algoritmo WRR, caso uma fila estiver vazia, o algoritmo passa para a próxima fila. A relação de prioridade das filas com o peso de cada fila, seguem a ordem: TC0, TC1, TC2, TC3 = 1:2:4:8.



Algoritmo WRR

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

O menu Qos inclui três submenus: *DiffServ, Controle de Banda* e *Voice VLAN*.

9.1. DiffServ

O switch classifica os pacotes de ingresso, mapeando para diferentes filas de prioridades e em seguida encaminha os pacotes de acordo com o algoritmo de fila selecionado pela função QoS. Este switch implementa três modos de prioridades, prioridade por portas, por 802.1P e DSCP e suporta quatro algoritmos de fila.

As prioridades baseadas em portas são rotuladas como CoS0, CoS1... CoS7.

O DiffServ pode ser configurado nas páginas de configuração *Prioridade por Porta, Prioridade DSCP, Prioridade 802.1P* e *Algoritmo de Fila.*

Prioridade por porta

Nesta página você pode configurar a prioridade das portas.

Quando a prioridade por porta é especificada, os pacotes serão classificados com base no valor do CoS da porta de entrada e enviados para as filas de prioridade conforme a relação de mapeamento configurado entre o CoS e o TC nas configurações 802.1P.

Escolha o menu *QoS* → *DiffServ* → *Prioridade por Porta* para carregar a seguinte página:

Configuração de Prioridade por Porta

Selecionar	Porta	Prioridade	LAG
☐		CoS 0	
☐	1	CoS 0	---
☐	2	CoS 0	---
☐	3	CoS 0	---
☐	4	CoS 0	---
☐	5	CoS 0	---
☐	6	CoS 0	---
☐	7	CoS 0	---
☐	8	CoS 0	---
☐	9	CoS 0	---
☐	10	CoS 0	---

Aplicar Ajuda

Obs.:

Quando a Prioridade por Porta é especificado, os dados serão classificados em filas de saída (TC) com base no valor do CoS da porta de entrada. A relação entre os valores de CoS com as filas de saídas (TC) são configuradas na página Prioridade 802.1P.

Prioridade por porta

As seguintes opções são exibidas na tela:

» **Configuração de prioridade por porta**

Selecionar: selecione as portas desejadas para configurar a prioridade.

Porta: exibe o número da porta no switch.

Prioridade: selecione a prioridade para a porta.

LAG: exibe o número do grupo LAG a qual a porta pertence

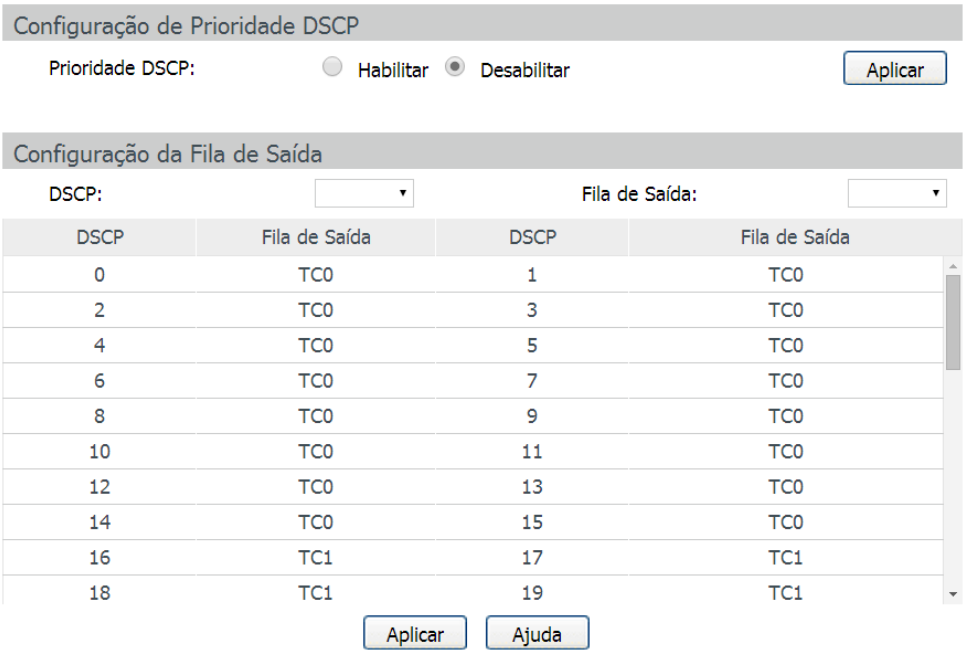
Procedimento de configuração

Passo	Operação	Descrição
1	Selecione a prioridade da porta	Obrigatório, QoS ⟶ DiffServ ⟶ Prioridade por Porta, para configurar a prioridade da porta.
2	Configure a relação de mapeamento entre a prioridade 802.1P e a fila de prioridade (TC).	Obrigatório, QoS ⟶ Diff Serv ⟶ Prioridade 802.1P, configure o mapeamento entre 802.1P e a fila de prioridade (TC).
3	Selecione o algoritmo de fila	Obrigatório, QoS ⟶ DiffServ ⟶ Algoritmo de Fila, selecione o algoritmo de fila desejado.

Prioridade DSCP

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

Escolha o menu *QoS* ⟶ *DiffServ* ⟶ *Prioridade DSCP* para carregar a seguinte página:



Obs.:

As Filas de Saídas são denominadas TC0, TC1, TC2 e TC3, quanto maior o valor da fila maior a prioridade.

Prioridade DSCP

As seguintes opções são exibidas na tela:

» **Configuração de prioridade DSCP**

Prioridade DSCP: selecione *Habilitar/Desabilitar* para habilitar ou desabilitar a prioridade DSCP.

» **Configuração da fila de saída**

DSCP: selecione a prioridade determinada pela região DS do datagrama IP. Varia de 0 a 63.

Fila de saída: selecione a fila de saída em que o pacote com a marcação DSCP será relacionado. Existem 4 filas, variando de 0 a 3, representados como TC0, TC1, TC2, TC3, quanto maior o valor da fila, maior a prioridade.

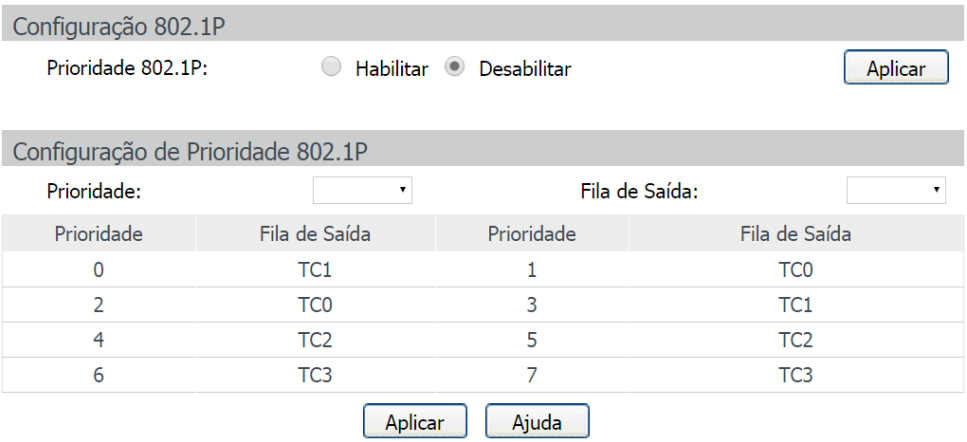
Procedimento de configuração

Passo	Operação	Descrição
1	Configure a relação de mapeamento entre o DSCP e a fila de saída	Obrigatório, QoS ⟶ DiffServ⟶ Prioridade DSCP, habilitar a prioridade DSCP e configurar a relação de mapeamento entre a marcação DSCP e a prioridade da fila.
2	Selecione o algoritmo de fila	Obrigatório, QoS ⟶ DiffServ⟶ Algoritmo de fila, selecione o algoritmo de fila desejado.

Prioridade 802.1P

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

Escolha o menu *QoS → DiffServ → Prioridade 802.1P* para carregar a seguinte página:



Obs.:

As Filas de Saídas são denominadas TC0, TC1, TC2 e TC3, quanto maior o valor da fila maior a prioridade.

Prioridade 802.1P

As seguintes opções são apresentadas na tela:

» **Configuração 802.1P**

Prioridade 802.1P: selecione *Habilitar/Desabilitar* para habilitar ou desabilitar a prioridade 802.1P.

» **Configuração de prioridade 802.1P**

Prioridade: selecione a prioridade definida pelo IEEE802.1p.

Fila de saída: selecione a fila de saída em que o pacote com a priorização 802.1p será relacionado. Existem 4 filas, variando de 0 a 3, representados como TC0, TC1, TC2, TC3, quanto maior o valor da fila, maior a prioridade.

Procedimento de configuração:

Passo	Operação	Descrição
1	Configurar a relação de mapeamento entre 802.1P e a fila de saída	Obrigatório, QoS → DiffServ → Prioridade 802.1P, habilitar a prioridade 802.1P e configurar a relação de mapeamento entre a prioridade 802.1P e a prioridade da fila.
2	Selecionar o algoritmo de fila	Obrigatório, QoS → DiffServ → Algoritmo de fila, selecione o algoritmo de fila desejado.

Algoritmo de fila

Nesta página é possível configurar até 4 tipos de algoritmos de filas. Estes algoritmos são responsáveis pela ordem de encaminhamento dos pacotes que estão dentro de diferentes filas de prioridade.

Escolha o menu *QoS → DiffServ → Algoritmo de Fila* para carregar a página seguinte:

Algoritmo de fila

» **Configuração do algoritmo de fila**

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

WRR: algoritmo WRR (Weight Round Robin). Neste modo, os pacotes de todas as filas serão enviados de acordo com o peso de cada fila, este peso indica a proporção ocupada pelo recurso. As filas de prioridades são atendidas em ordem pelo algoritmo WRR, caso uma fila estiver vazia, o algoritmo passa para a próxima fila. A relação de prioridade das filas com o peso de cada fila, seguem a ordem: TC0, TC1, TC2, TC3 = 1:2:4:8.

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

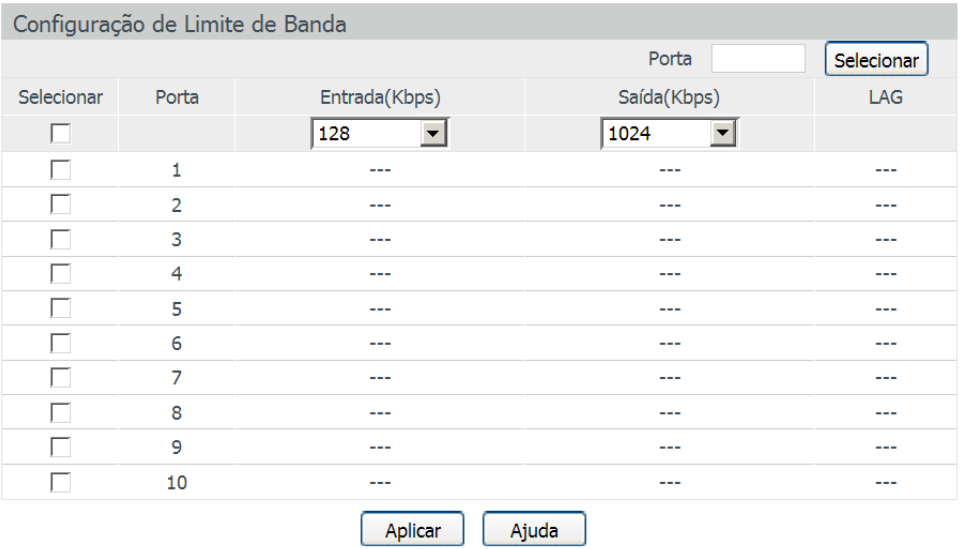
Uniforme: neste modo, todas as filas ocupam igualmente a largura de banda. A relação de prioridade das filas com o peso de cada fila, seguem a ordem: TC0, TC1, TC2 e TC3 = 1:1:1:1.

9.2. Controle de banda

A função de *Controle de Banda*, permite que você controle a largura de banda e o fluxo de transmissão de cada porta, sendo configurados nas seguintes páginas: *Limite de Banda* e *Storm Control*.

Limite de banda

A função *Limite de Banda* é utilizada para controlar a taxa do tráfego de entrada e de saída dos pacotes para cada porta.



Obs.:

1. Não é possível configurar o Limite de Banda entrante e o Storm Control em uma mesma porta.
2. Ao configurar manualmente o Limite de Banda de uma porta, o switch selecionará automaticamente um valor múltiplo de 64Kbps mais próximo do valor que você digitou.

As seguintes opções são exibidas na tela:

» **Configuração de limite de banda**

Porta: digite a porta desejada no campo correspondente e clique no botão *Selecionar* para selecionar a porta.

Selecionar: selecione a porta desejada. É possível selecionar mais de uma porta simultaneamente.

Porta: exibe o número da porta do switch.

Entrada (Kbps): selecione a largura de banda para recebimento de pacotes na porta.

Saída (Kbps): selecione a largura de banda para envio de pacotes na porta.

LAG: exibe o número do grupo LAG que a qual a porta pertence.

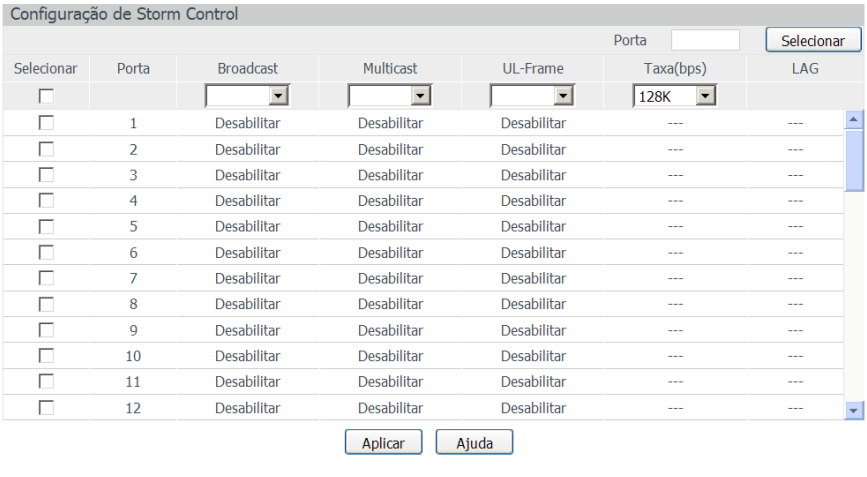
Obs.: » *Ao habilitar a função* Limite de Banda *com a função* Storm Control *habilitada, o Storm Control será desabilitado para a porta específica.*

» *Quando habilitar a opção Saída (Kbps) para uma ou mais portas, é desejável que se desabilite o controle de fluxo das portas para garantir que o switch funcione normalmente.*

Storm control

A função *Storm Control* permite que o switch filtre por porta os pacotes do tipo broadcast, Multicast e UL Frames (pacotes sem endereço IP definido). 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.

Escolha o menu *QoS* → *Controle de Banda* → *Storm Control* para carregar a seguinte página:



Storm control

As seguintes opções são exibidas na tela:

» **Configuração de storm control**

Porta: digite a porta desejada no campo correspondente e clique no botão *Selecionar* para selecionar a porta.

Selecionar: selecione a porta desejada. É possível selecionar mais de uma porta simultaneamente.

Porta: exibe o número de porta do switch.

Broadcast: selecione *Habilitar/Desabilitar* para habilitar ou desabilitar a função *Storm Control* para pacotes Broadcast na porta desejada.

Multicast: selecione *Habilitar/Desabilitar* para habilitar ou desabilitar a função *Storm Control* para pacotes Multicast na porta desejada.

UL-Frame: selecione *Habilitar/Desabilitar* para habilitar ou desabilitar a função *Storm Control* para Frames UL (pacotes sem endereço IP definido) na porta desejada.

Taxa (bps): selecione a largura de banda utiliada pela função *Storm Control*. O tráfego de pacotes superior à largura de banda especificada será descartado.

LAG: exibe o número do grupo LAG a qual a porta pertence.

Obs.: *ao habilitar a função Limite de Banda com a função Storm Control habilitado, o Storm Control será desabilitado para a porta específica.*

9.3. Voice VLAN

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

» **Endereço OUI (*Organizationally Unique Identifier*)**

O switch pode determinar se um pacote é ou não de voz, marcando seu endereço MAC de origem. Se a origem do endereço MAC corresponder com algum endereço OUI configurado no sistema, os pacotes serão classificados como pacotes de voz e serão transmitidos na VLAN de voz.

Um endereço OUI, é um identificador único atribuído pela IEEE (*Institute of Electrical and Electronics Engineers*) para um fornecedor de dispositivos. Ele compreende os 24 primeiros bits de um endereço MAC. Você pode reconhecer a qual fornecedor um dispositivo pertence, de acordo com o endereço OUI. A tabela a seguir, exibe os endereços OUI de vários fabricantes, que já estão pré-definidos no switch.

Endereço OUI	Fabricante
00-01-E3-00-00-00	Siemens Phone
00-03-6B-00-00-00	Cisco Phone
00-04-0D-00-00-00	Avaya Phone
00-60-B9-00-00-00	Philips/NEC Phone
00-D0-1E-00-00-00	Pingtel Phone
00-E0-75-00-00-00	Polycom Phone
00-E0-BB-00-00-00	3COM Phone

» **Modos da porta voice VLAN**

A VLAN de voz pode operar em dois modos: Automático e Manual.

Automático: neste modo o switch adiciona automaticamente a porta que recebe os pacotes de voz para a VLAN de Voz através do aprendizado do endereço MAC de origem dos pacotes UNTAG enviados do telefone IP. O Aging Time (tempo de envelhecimento) das portas pertencentes a VLAN de Voz podem ser configurados no switch. Se o switch não receber qualquer pacote de voz durante o intervalo especificado, a porta será removida da VLAN de Voz. Portas de voz são automaticamente adicionadas ou removidas na VLAN de Voz.

Manual: neste modo é necessário adicionar manualmente a porta em que o dispositivo de voz está conectado para ser membro da VLAN de Voz e atribuir regras de ACL para configurar as prioridades dos pacotes, conforme os endereços MAC de origem e OUI correspondentes. Na prática, a porta participante de uma VLAN de Voz é configurada de acordo com o tipo dos pacotes enviados a partir de um dispositivo de voz e do modo de funcionamento da porta. A tabela a seguir exibe informações detalhadas.

Modo da porta	Tipo dos dados de voz	Modo de funcionamento e processamento da porta
Automático	Pacotes de voz TAG	Untagged: não suportado
		Tagged: suportado. A VLAN padrão da porta não pode ser a Voice VLAN
	Pacotes de voz UNTAG	Untagged: suportado
		Tagged: não suportado
Manual	Pacotes de voz TAG	Untagged: não suportado
		Tagged: suportado. A VLAN padrão da porta não deve ser a voz VLAN
	Pacotes de voz UNTAG	Untagged: suportado
		Tagged: não suportado

» **Modo de segurança das portas voice VLAN**

Quando a Voice VLAN estiver habilitada em uma porta, será possível habilitar a opção *Modo de Segurança*, afim de filtrar o tráfego de dados. Quando o modo de segurança estiver habilitado, a porta apenas encaminha os pacotes de voz, e descarta os outros pacotes cujo endereço MAC de origem não corresponda ao endereço OUI configurado. Se o modo de segurança estiver desabilitado, a porta encaminha todos os pacotes recebidos.

Modo de segurança	Tipo de pacote	Modo de funcionamento e processamento da porta
Habilitar	Pacotes UNTAG	Quando o endereço MAC de origem do pacote corresponder com o endereço OUI configurado, o pacote poderá ser transmitido na Voice VLAN. Caso contrário, o pacote será descartado.
	Pacotes de voz TAG	
	Pacotes de dados TAG	O modo de processamento do pacote é determinado pela capacidade da porta permitir ou não a VLAN, independente do modo de segurança da Voice VLAN.
Desabilitar	Pacotes UNTAG	Não verifica o endereço MAC de origem dos pacotes e todos os pacotes podem ser transmitidos na Voice VLAN.
	Pacotes de voz TAG	
	Pacotes de dados TAG	O modo de processamento do pacote é determinado pela capacidade da porta permitir ou não a VLAN, independente do modo de segurança da Voice VLAN.

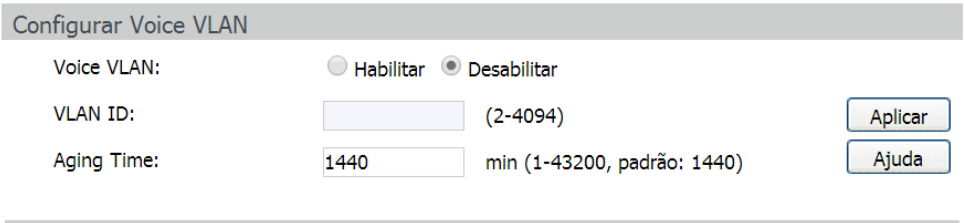
Obs.: *não utilize a VLAN de Voz para transmitir pacotes de dados de outras VLANs, exceto em casos especiais.*

A função Voice VLAN pode ser configurada nas seguintes páginas: Voice VLAN, Configurar Portas e Endereços OUI.

Voice VLAN

Nesta página é possível configurar os parâmetros globais da Voice VLAN, como por exemplo, VLAN ID e Aging Time.

Escolha no menu *QoS* → *Voice VLAN* → *Voice VLAN* para carregar a seguinte página:



Configuração da voice VLAN

As seguintes informações são apresentadas na tela:

» **Configurar voice VLAN**

Voice VLAN: selecione *Habilitar* ou *Desabilitar* a função *Voice VLAN.*

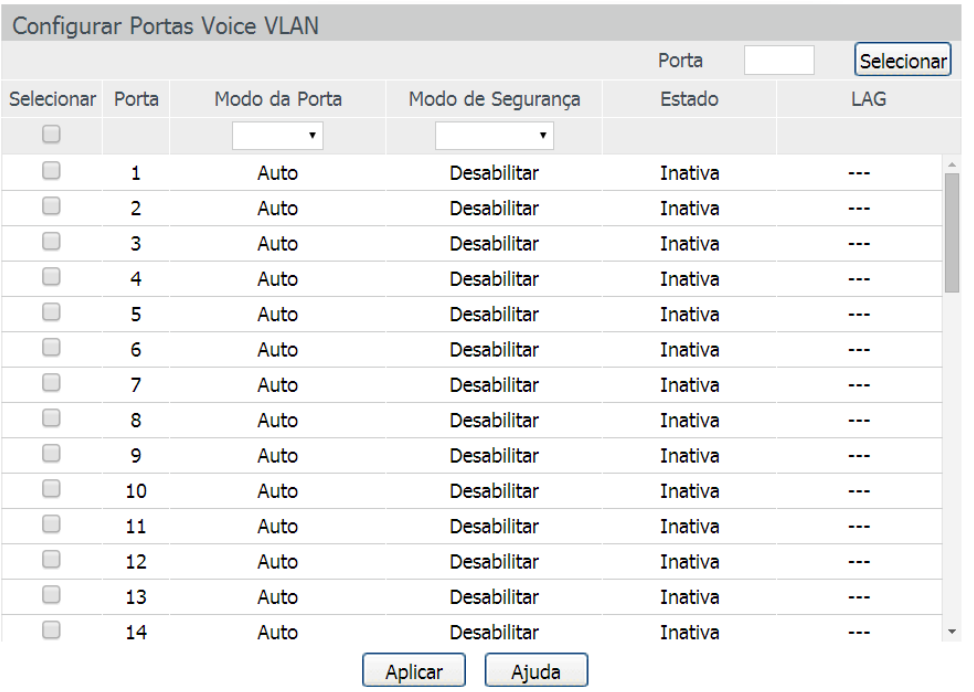
VLAN ID: digite o VLAN ID utilizado pela Voice VLAN.

Aging time: especifique o Aging Time (tempo de envelhecimento) das portas membro da Voice VLAN que estão no modo automático.

Configurar portas

Nesta página é possível configurar os parâmetros das portas participantes da Voice VLAN.

Escolha o menu *QoS* → *Voice VLAN* → *Configurar Portas* para carregar a seguinte página:



Portas da voice VLAN

Obs.: » *Ao habilitar a função* Voice VLAN *para um grupo LAG (Agregação da Link), certifique-se que todas as portas do grupo LAG estejam com o mesmo modo de configuração.*

» *Ao modificar o modo de uma porta membro de uma Voice VLAN para automático, fará com que a porta deixe a VLAN de Voz e somente volte quando a porta receber pacotes de voz.*

As seguintes informações são apresentadas na tela:

» **Configurar portas voice VLAN**

Porta: digite a porta desejada no campo correspondente e clique no botão *Selecionar* para selecionar a porta.

Selecionar: selecione a porta desejada. É possível selecionar mais de uma porta simultaneamente.

Modo da porta: selecione o modo da porta ao se juntar a uma Voice VLAN.

» **Auto:** neste modo, o switch adiciona ou remove automaticamente a porta da Voice VLAN, verificando se o tráfego recebido pela porta é de voz ou não.

» **Manual:** neste modo, é possível adicionar ou remover manualmente uma porta da Voice VLAN.

Modo de segurança: selecione o modo de segurança da porta para o encaminhamento dos pacotes.

» **Desabilitar:** todos os pacotes serão encaminhados.

» **Habilitar:** somente pacotes de voz serão encaminhados.

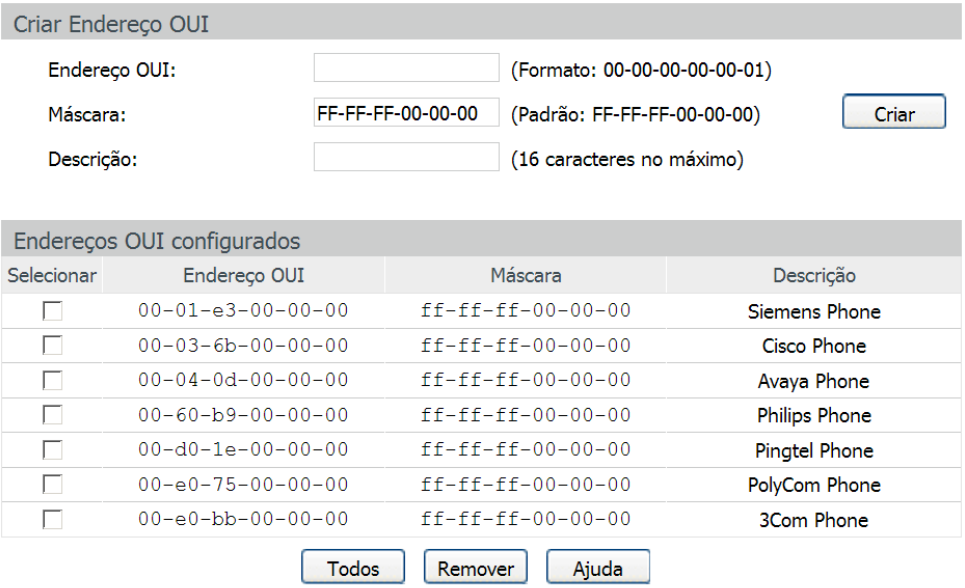
Estado: exibe o estado da porta da Voice VLAN atual.

LAG: exibe o número do grupo LAG a qual a porta pertence.

Endereços OUI

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

Escolha no menu *QoS* → *Voice VLAN* → *Endereços OUI* para carregar a seguinte página:



Endereços OUI

As seguintes informações são apresentadas na tela:

» **Criar endereço OUI**
Endereço OUI: digite o endereço OUI do dispositivo de voz.
Máscara: digite a máscara utilizada pelo endereço OUI do dispositivo de voz.
Descrição: digite uma descrição para identificação do endereço OUI.

» **Endereços OUI configurados**
Selecionar: selecione o endereço OUI desejado. Para remover a entrada, clique no botão *Remover*.
OUI: exibe o endereço OUI do dispositivo de voz.
Máscara: exibe a máscara utilizada pelo endereço OUI.
Descrição: exibe a descrição do endereço OUI.

Procedimentos de configuração da voice VLAN

Passo	Operação	Descrição
1	Definir o modo de funcionamento das portas	Obrigatório. Em *VLAN* → *802.1Q VLAN* → *Configurar VLAN*, defina o modo de funcionamento das portas que serão usadas com os dispositivos de voz.
2	Criar VLAN	Obrigatório. Em *VLAN* → *802.1Q VLAN* → *Configurar VLAN*, crie a VLAN utilizada na Voice VLAN.
3	Adicionar o endereço OUI	Opcional. Em *QoS* → *Voice VLAN* → *Endereços OUI*, verifique se o switch possui cadastrado o endereço OUI do dispositivo de voz. Caso não possua adicione o endereço.
4	Configurar os parâmetros das portas na Voice VLAN	Obrigatório. Em *QoS* → *Voice VLAN* → *Configurar Portas*, configure os parâmetros da porta na Voice VLAN.
5	Habilitar a Voice VLAN	Obrigatório. Em *QoS* → *Voice VLAN* → *Voice VLAN*, configure as opções globais para a Voice VLAN.

10. ACL

ACL (*Access Control List*) é utilizado para a configuração de regras e políticas para o filtro e processamento dos 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 encontradas em protocolos utilizados entre as camadas 2-4 do modelo de referência OSI.

O menu ACL possui 3 submenus de configuração: Configurar ACL, Políticas ACL e Vínculos ACL.

10.1. Configurar ACL

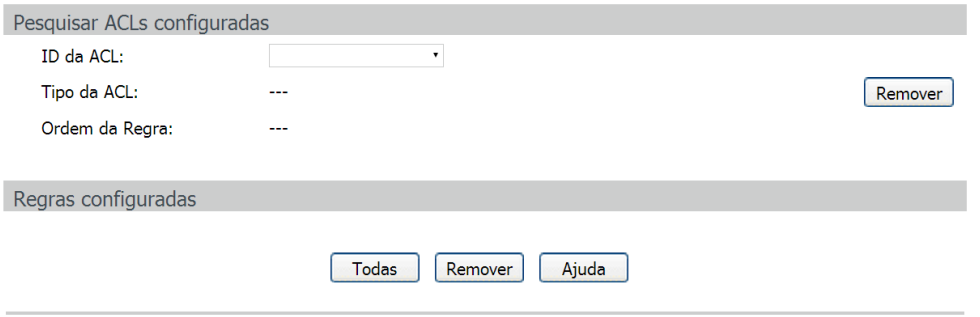
Cada ACL pode conter uma série de regras e cada regra pode especificar um conjunto de diferentes pacotes. Uma vez que a regra é correspondida, o switch processa os pacotes de acordo com a regra criada.

As regras ACL podem ser configuradas em: ACLs, Criar ACL, MAC ACL, ACL Padrão e ACL Estendida.

ACLs

Nesta página você pode visualizar as ACLs configuradas no switch.

Escolha o menu *ACL* → *Configurar ACL* → *ACLs* para carregar a seguinte página:



ACLs configuradas

As seguintes informações são apresentadas na tela:

» **Pesquisar ACLs configuradas**
ID da ACL: selecione a ACL desejada.
Tipo da ACL: exibe o tipo da ACL selecionada.
Ordem da regra: exibe a ordem das regras da ACL selecionada.

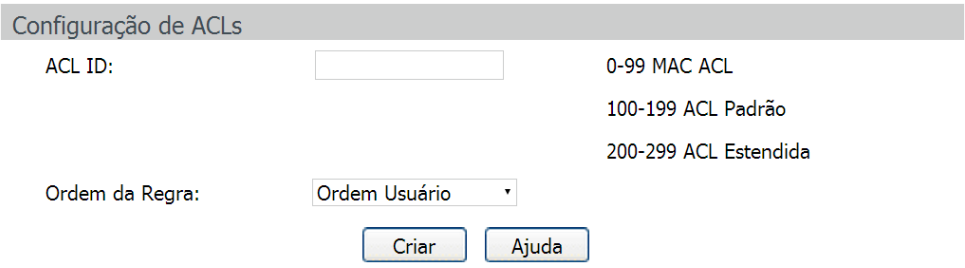
» **Regras configuradas**

Nesta tabela é possível visualizar as informações referentes as regras da ACL selecionada.

Criar ACL

Nesta página você pode criar ACLs.

Escolha o menu *ACL* → *Configurar ACL* → *Criar ACL* para carregar a seguinte página:



Criação da ACLs

As seguintes informações são apresentadas na tela:

» **Configuração de ACLs**

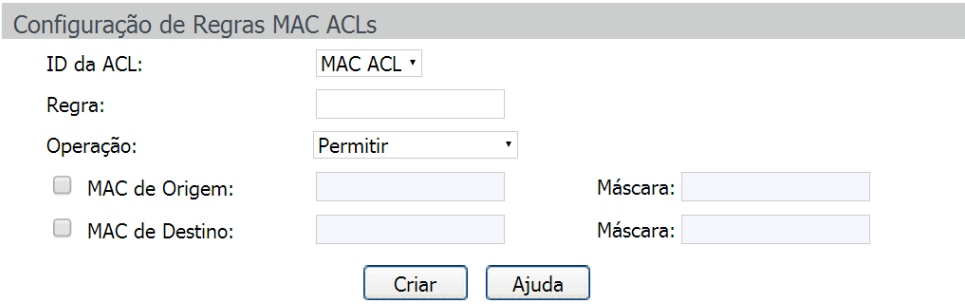
ACL ID: digite o ID da ACL que você deseja criar. O ID é a identificação da ACL, que pode variar de 0 a 299. Existem 3 tipos de ACL que o switch suporta e são classificados conforme o número de identificação, 0-99 MAC ACL, 100-199 ACL Padrão e de 200-299 ACL Estendida.

Ordem da regra: a opção *Ordem Usuário* é a ordem das regras criadas e definidas pelo usuário.

MAC ACL

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

Escolha o menu *ACL* → *Configurar ACL* → *MAC ACL* para carregar a seguinte página:



MAC ACL

As seguintes informações são apresentadas na tela:

» **Configuração de regras MAC ACLs**

ID da ACL: selecione o ID da ACL desejada para realizar a configuração.

Regra: digite o ID da regra utilizado pela ACL.

Operação: selecione o modo de operação do switch, quando um pacote corresponder com a regra criada.

» **Permitir:** permite o recebimento do pacote.

» **Negar:** descarta o pacote recebido.

MAC de origem: digite o endereço MAC de origem utilizado pela regra.

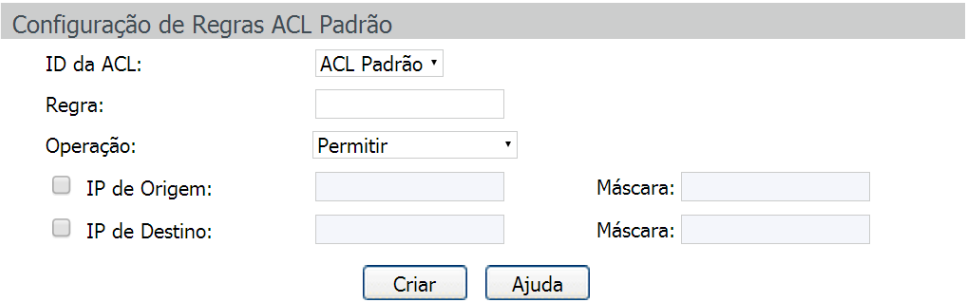
MAC de destino: digite o endereço MAC de destino utilizado pela regra.

Máscara: digite a máscara do endereço MAC.

ACL padrão

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

Escolha o menu *ACL* → *Configurar ACL* → *ACL Padrão* para carregar a seguinte página:



ACL padrão

As seguintes informações são apresentadas na tela:

» **Configuração de regras ACL padrão**

ID da ACL: selecione o ID da ACL desejada para realizar a configuração.

Regra: digite o ID da regra utilizado pela ACL

Operação: selecione o modo de operação do switch, quando um pacote corresponder com a regra criada.

» **Permitir:** permite o recebimento do pacote.

» **Negar:** descarta o pacote recebido.

IP de origem: digite o endereço IP de origem utilizado pela regra.

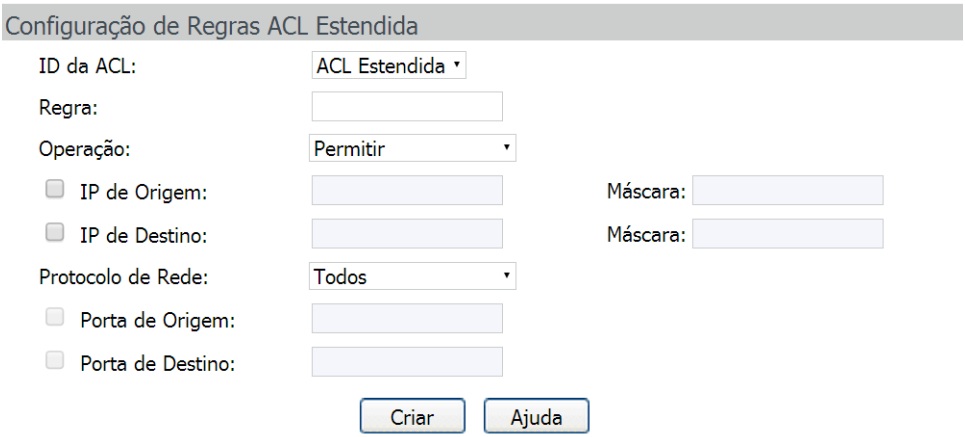
IP de destino: digite o endereço IP de destino utilizado pela regra.

Máscara de rede: digite a máscara do endereço IP.

ACL estendida

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

Escolha o menu *ACL* → *Configurar ACL* → *ACL Estendida* para carregar a seguinte página:



ACL estendida

As seguintes informações são exibidas na tela:

» **Configuração de regras ACL estendida**

ID da ACL: selecione o ID da ACL desejada para realizar a configuração.

Regra: digite o ID da regra utilizado pela ACL.

Operação: selecione o modo de operação do switch, quando um pacote corresponder com a regra criada.

» **Permitir:** permite o recebimento do pacote.

» **Negar:** descarta o pacote recebido.

IP de origem: digite o endereço IP de origem utilizado pela regra.

IP de destino: digite o endereço IP de destino utilizado pela regra.

Máscara de rede: digite a máscara do endereço IP.

Protocolo de rede: selecione o protocolo de rede utilizado pela regra.

Porta de origem: digite a porta de origem utilizada pela regra ACL, quando for selecionado o protocolo de rede TCP ou UDP.

Porta de destino: digite a porta de destino utilizada pela regra ACL, quando for selecionado o protocolo de rede TCP ou UDP.

10.2. Políticas ACL

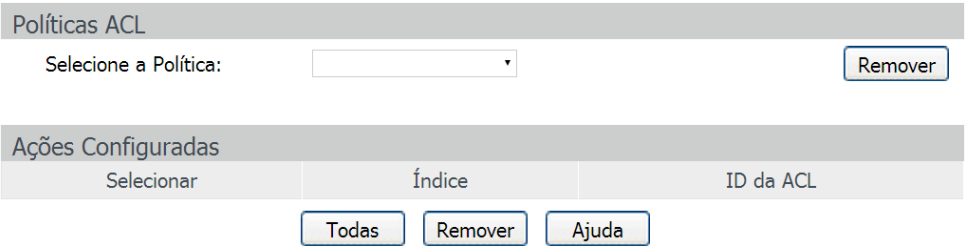
O submenu Políticas ACL é utilizado para controlar os pacotes que cumpram as regras ACLs correspondentes, configurando ações para um conjunto de ACLs.

A Política ACL pode ser configurada nas seguintes páginas: Políticas, Criar Políticas e Criar Ação.

Políticas

Nesta página é possível visualizar as ações criadas na política de ACL para uma determinada regra de ACL.

Escolha o menu *ACL* → *Políticas ACL* → *Políticas* para carregar a seguinte página:



Políticas de ACL

As seguintes informações são exibidas na tela:

» **Políticas ACL**

Selecione a política: selecione o nome da política desejada para exibição. Se você desejar excluir a política, clique no botão *Remover*.

» **Ações configuradas**

Selecionar: selecione a entrada desejada. Clique no botão *Modificar* para alterar uma ação ou em *Remover* para excluí-la.

Índice: exibe o índice da política criada.

ID da ACL: exibe o ID da ACL contida na política.

Operação: clique no botão *Modificar* para alterar a política desejada. Após realizar a modificação clique no botão *Modificar* para validar a alteração.

Criar políticas

Nesta página você pode criar as políticas de ACL.

Escolha no menu *ACL* → *Políticas ACL* → *Criar Políticas* para carregar a seguinte página:

Criação de políticas ACLs

As seguintes informações são exibidas na tela:

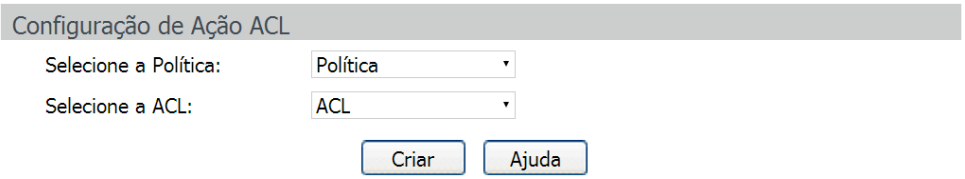
» **Configuração de políticas ACL**

Nome da política: digite o nome da política ACL.

Criar ação

Nesta página é possível criar as ações da política de ACL, associando a política a uma determinada regra de ACL configurada.

Escolha o menu *ACL* → *Políticas ACL* → *Criar Ação* para carregar a página seguinte:



Ação da política de ACL

As seguintes informações são exibidas na tela:

» **Configuração de ação ACL**
Selecione a política: selecione o nome da política criada.
Selecione a ACL: selecione a ACL que será associada a política de ACL.

10.3. Vínculos ACL

A função Vínculos ACL é utilizada para associar a política criada a uma porta do switch ou a uma VLAN específica, isto é, a política criada só funcionará após a política ser vinculada a uma destas duas opções: Vínculo por Porta ou Vínculo por VLAN.

A função Vínculos ACL pode ser configurada nas seguintes páginas: Vínculos, Vínculo por Porta e Vínculo por VLAN.

Vínculos

Nesta página é possível verificar os vínculos criados para as políticas de ACL.

Escolha o menu *ACL* → *Vínculos ACL* → *Vínculos* para carregar a seguinte página:

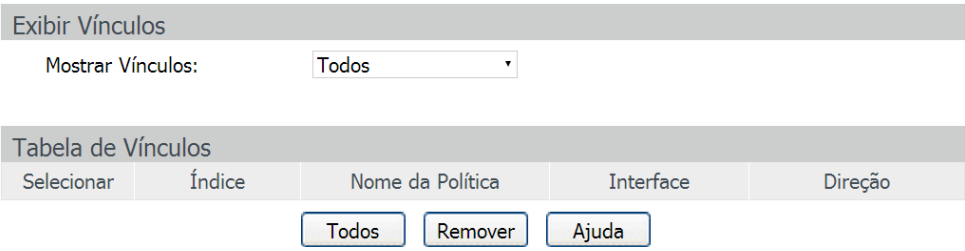


Tabela de vínculos ACL

As seguintes informações são apresentadas na tela:

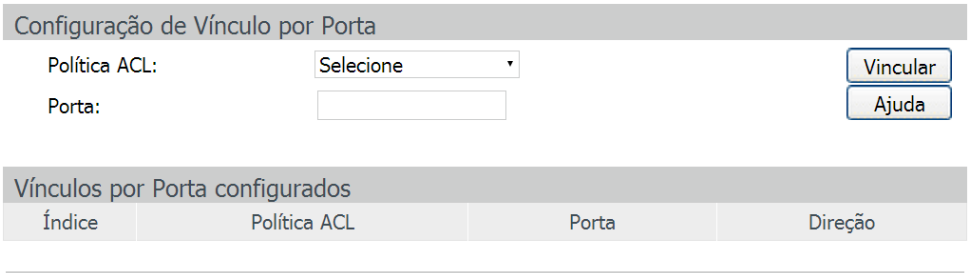
» **Exibir vínculos**
Mostrar vínculos: selecione o vínculo desejado para visualizar as informações.

» **Tabela de vínculos**
Selecionar: selecione o vínculo desejado. Para excluí-lo, clique em *Remover*.
Índice: exibe o índice do vínculo configurado.
Nome da política: exibe o nome da Política de ACL.
Interface: exibe o número da porta do switch ou o VLAN ID vinculados a política criada.

Vínculo por porta

Nesta página você pode vincular uma porta do switch a uma política criada.

Escolha o menu *ACL* → *Vínculos* ACL → *Vínculo por Porta* para carregar a seguinte página:



Vínculo por porta

As seguintes informações são exibidas na tela:

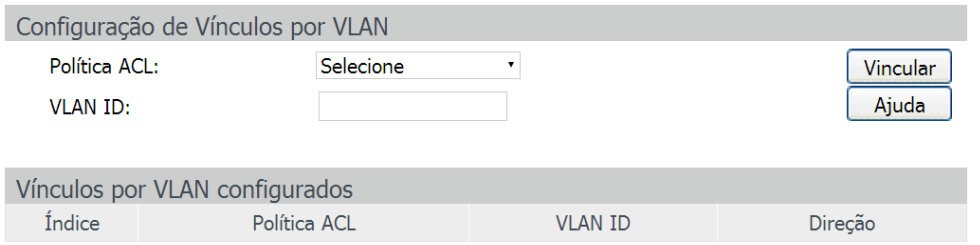
» **Configuração de vínculo por porta**
Política ACL: selecione a Política de ACL que você deseja vincular.
Porta: digite o número da porta que você deseja vincular. Utilize o formato: 1-3, 6, 8.

» **Vínculos por porta configurados**
Índice: exibe o índice do vínculo configurado.
Política ACL: exibe o nome da Política de ACL vinculada.
Porta: exibe o número da porta do switch vinculado a Política de ACL.
Direção: exibe a direção do vínculo.

Vínculo por VLAN

Nesta página você pode vincular uma VLAN a uma política criada.

Escolha o menu *ACL* → *Vínculos ACL* → *Vínculo por VLAN* para carregar a seguinte página:



Vínculo por VLAN

As seguintes informações são apresentadas na tela.

» **Configuração de vínculos por VLAN**
Política ACL: selecione a Política de ACL que você deseja vincular.
VLAN ID: digite o VLAN ID que você deseja vincular. Utilize o formato: 2-10, 100.

» **Vínculos por VLAN configurados**
Índice: exibe o índice do vínculo configurado.
Política ACL: exibe o nome da Política de ACL vinculada.
VLAN ID: exibe o VLAN ID vinculado a Política de ACL.
Direção: exibe a direção do vínculo.

Procedimento de configuração

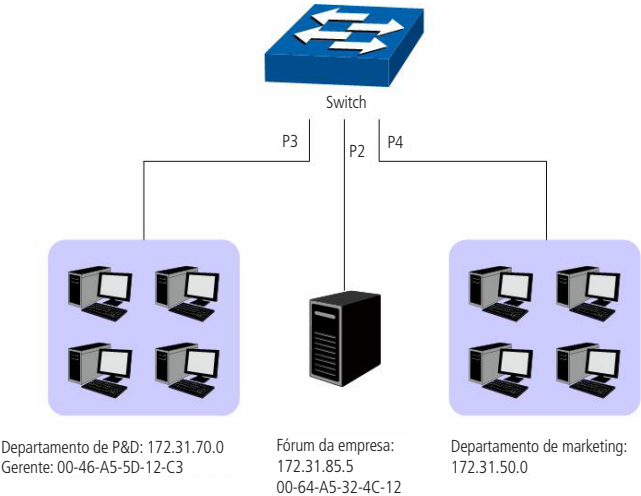
Passo	Operação	Descrição
1	Configuração do agendamento	Obrigatório, *ACL* ⟶ *Agendamentos*, configurar o agendamento desejado para o funcionamento das ACLs.
2	Configuração das regras ACL	Obrigatório, *ACL* ⟶ *Configurar ACL*, configurar as regras ACL correspondentes aos pacotes desejados.
3	Configuração de política ACL	Obrigatório, *ACL* ⟶ *Políticas ACL*, configurar as ações das políticas para controlar os pacotes que correspondam com as regras de ACL.
4	Vincular uma política a uma porta ou VLAN	Obrigatório, *ACL* ⟶ *Vínculos ACL*, configurar um vínculo para a Política de ACL conforme desejado.

10.4. Exemplos de aplicação para ACL

» **Requerimentos para rede**

1. O gerente do departamento de P&D poderá acessar o fórum da empresa e a internet sem nenhuma restrição. O endereço MAC do gerente é 00-46-A5-5D-12-C3.
2. O pessoal do time de P&D não poderá acessar a internet durante o horário de trabalho, mas poderão visitar o fórum o dia todo.
3. O pessoal de marketing poderá acessar a internet o dia todo, mas não poderão visitar o fórum durante o horário de trabalho.
4. O departamento de P&D e o departamento de marketing não poderão se comunicar uns com os outros.

» **Diagrama de rede**



Aplicação de regras ACLs

» **Procedimento de configuração**

Passo	Operação	Descrição
1	Configuração do requerimento 1	*ACL* ⟶ *Configurar ACL* ⟶ *Criar ACL*, configure a ACL 11. *ACL* ⟶ *Configurar ACL* ⟶ *MAC ACL*, selecione ACL 11, crie a regra 1, configure o campo Operação como Permitir, configure o MAC de Origem como 00-45-A5-5D-12-C3 e a Máscara como FF-FF-FF-FF-FF-FF, e configure o Agendamento como Nenhum. *ACL* ⟶ *Políticas ACL* ⟶ *Criar Políticas*, configure uma política com o nome gerente. *ACL* ⟶ *Políticas ACL* ⟶ *Criar Ação*, adicione na ACL 11 a política gerente. *ACL* ⟶ *Vínculos ACL* ⟶ *Vínculo por Porta*, selecione a política gerente e vincule a porta 3.
2	Configuração dos requerimentos 2 e 4	*ACL* ⟶ *Configurar ACL* ⟶ *Criar ACL*, configure a ACL 100. *ACL* ⟶ *Configurar ACL* ⟶ *ACL Padrão*, selecione a ACL 100, crie a regra 1, configure o campo Operação como Negar, configure o IP de Origem como 172.31.70.1 e a máscara como 255.255.255.0, configure o IP de Destino como 172.31.50.1 e a máscara como 255.255.255.0. *ACL* ⟶ *Configurar ACL* ⟶ *ACL Padrão*, selecione a ACL 100, crie a regra 2, configure o campo Operação como Negar, configure o IP de Origem como 172.31.70.1 e a máscara como 255.255.255.0. Configure o IP de Destino como 172.31.88.5 e a máscara como 255.255.255.0. *ACL* ⟶ *Configurar ACL* ⟶ *ACL Padrão*, selecione a ACL 100, crie a regra 3, configure o campo Operação como Permitir, configure o IP de Origem como 172.31.70.1 e a máscara como 255.255.255.0. Configure o IP de Destino como 172.31.88.5 e a máscara como 255.255.255.0. *ACL* ⟶ *Políticas ACL* ⟶ *Criar Ação*, adicione na ACL 100 a política limite1. *ACL* ⟶ *Configurar ACL* ⟶ *Criar Políticas*, configure uma política com o nome limite1. *ACL* ⟶ *Vínculos ACL* ⟶ *Vínculo por Porta*, selecione a limite1 e vincule a porta 3.
3	Configuração dos requerimentos 3 e 4	*ACL* ⟶ *Configurar ACL* ⟶ *ACL Create*, crie a ACL 101. *ACL* ⟶ *Configurar ACL* ⟶ *ACL Padrão*, selecione a ACL 101, crie a regra 1, configure o campo Operação como Negar, configure o IP de Origem como 172.31.70.1 e a máscara como 255.255.255.0. Configure o IP de Destino como 172.31.50.1 e a máscara como 255.255.255.0. *ACL* ⟶ *Configurar ACL* ⟶ *ACL Padrão*, selecione a ACL 101, crie a regra 2, configure o campo Operação como Negar, configure o IP de Origem como 172.31.70.1 e a máscara como 255.255.255.0. Configure o IP de Destino como 172.31.88.5 e a máscara como 255.255.255.0. *ACL* ⟶ *Políticas ACL* ⟶ *Criar Políticas*, configure uma política com o nome limite2. *ACL* ⟶ *Políticas ACL* ⟶ *Criar Ação*, adicione na ACL 101 a política limite1. *ACL* ⟶ *Vínculos ACL* ⟶ *Vínculo por Porta*, selecione a política limite2 e vincule a porta 4.

11. SNMP

» **Visão geral do SNMP**

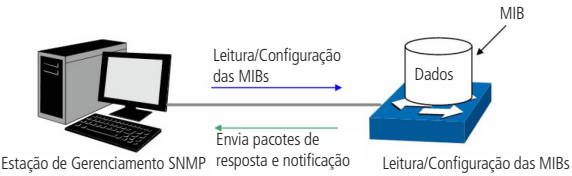
SNMP (*Simple Network Management Protocol*) é amplamente utilizado por aplicações executadas em redes UDP/IP. O SNMP fornece uma estrutura de gerenciamento para monitorar e manter os dispositivos de rede. É utilizado para gerenciar automaticamente vários dispositivos distintos de rede. Atualmente, a maioria dos sistemas de gerenciamento de rede são baseados em SNMP. Com a função SNMP habilitado, os administradores de rede podem facilmente monitorar o desempenho da rede, detectar as falhas e configurar os dispositivos de rede.

» **Estrutura de gerenciamento SNMP**

A estrutura de gerenciamento SNMP inclui três elementos de rede: estação de gerenciamento SNMP, agente SNMP e MIB (*Management Information Base*).

- » **Estação de Gerenciamento SNMP:** é a estação de trabalho que executa o programa cliente SNMP, fornecendo uma interface de gerenciamento amigável para o administrador gerenciar os dispositivos de rede mais conveniente.
- » **Agente SNMP:** é o processo executado pelo dispositivo de rede responsável por receber e processar os pacotes de solicitação da estação de gerenciamento SNMP. O Agente SNMP também poderá informar a estação de gerenciamento SNMP sobre possíveis eventos ocorridos com o dispositivo.
- » **MIB (Management Information Base):** é a base de informações de gerenciamento. O agente é capaz de responder ao gerente consultas SNMP sobre o conjunto de informações contido na MIB. Cada agente SNMP possui sua própria MIB. A estação de gerenciamento SNMP pode ler ou escrever os objetos da MIB com base em seus direitos de gestão.

Estação de gerenciamento SNMP é o gerente da rede SNMP, enquanto o agente SNMP é o objeto gerenciado. As informações entre a estação de gerenciamento SNMP e o agente SNMP são trocadas através do protocolo SNMP (Simple Network Management Protocol). A relação entre a estação de gerenciamento SNMP, agente SNMP e a MIB, é ilustrado na figura a seguir.



Relação entre os elementos de rede SNMP

» **Versões SNMP**

Este switch suporta SNMP v3 que é compatível com SNMP v1 e SNMP v2c. 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.

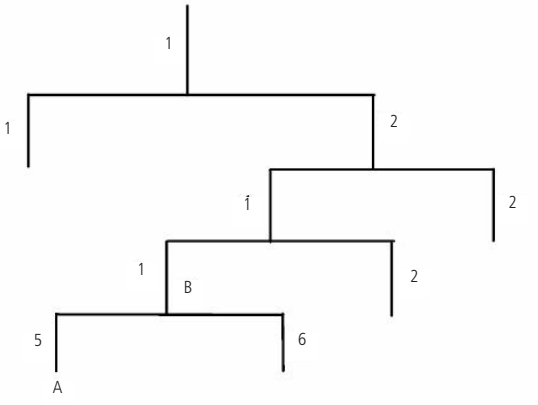
» **SNMP v1:** o SNMPv1 adota autenticação utilizando o nome da comunidade. O nome da comunidade é usado para definir a relação entre a estação de gerenciamento SNMP e o agente SNMP. Os pacotes SNMP que não conseguirem aprovação de autenticação serão descartados.

» **SNMP v2c:** 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.

» **SNMP v3:** baseado em SNMP v1 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.

» **Introdução MIB**

Para identificar os objetos de gerenciamento dos dispositivos em mensagens SNMP, o SNMP adota uma arquitetura hierárquica. É como se fosse uma árvore, e que cada nó da árvore representasse um objeto. Assim, o objeto pode ser identificado como único caminho a partir da raiz, e é indicado por uma sequencia de números. A sequência de números é o identificador do objeto. Na figura a seguir o OID do objeto gerenciado B é {1.2.1.1}. Enquanto o OID do objeto gerenciado A é {1.2.1.1.5}.



Arquitetura das MIBs

» **Configuração do SNMP**

1. Criação da view SNMP

   A view do SNMP é criada para a estação de gerenciamento SNMP gerenciar objetos da MIB. Os objetos gerenciados são identificados exclusivamente pelo seu OID. O OID do objeto gerenciado pode ser encontrado no programa cliente SNMP em execução na estação de gerenciamento SNMP.

2. Criação do grupo SNMP

   Após criada a view SNMP, é necessário que se crie um grupo SNMP. O nome do grupo, versão do protocolo SNMP e o nível de segurança compõem o identificador do grupo SNMP. Você pode configurar grupos SNMP para controlar o acesso à rede, fornecendo aos usuários em vários grupos distintos, várias formas de gerência, como por exemplo, leitura, escrita e notificação.

3. Criação de usuários SNMP

   O usuário que está em um grupo SNMP, pode gerenciar o switch através do programa cliente na estação de gerenciamento. O nome de usuário e a senha são utilizados para as estações de gerenciamentos SNMP, isso para terem acesso aos agentes SNMP.

O menu SNMP é utilizado para configurar a função de SNMP do switch, incluindo 3 submenus de configuração: *SNMP, Notificação e RMON.*

11.1. SNMP

As configurações SNMP podem ser configuradas nas seguintes páginas de configuração: *Configurar SNMP, View SNMP, Grupo SNMP, Usuário SNMP* e *Comunidade SNMP*.

Configurar SNMP

Esta página é utilizada para habilitar globalmente a função SNMP do switch.

Escolha o menu *SNMP* → *SNMP* → *Configurar SNMP* para carregar a página seguinte:

Configuração SNMP

As seguintes opções são apresentadas na tela.

» **Configuração SNMP**

SNMP: selecione *Habilitar/Desabilitar* para habilitar ou desabilitar a função SNMP.

» **Engine SNMP local**

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

» **Engine SNMP remoto**

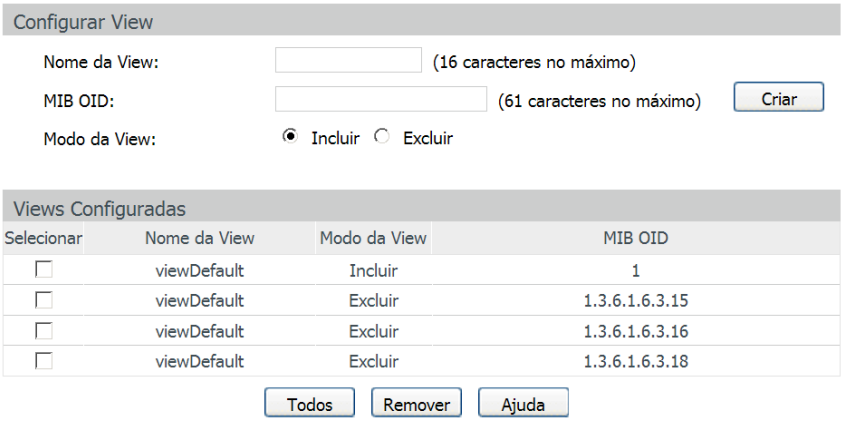
Engine ID remoto: digite a identificação do SNMP Engine do switch remoto (o Engine Remoto é utilizado para o envio de snmp inform V3 para o switch ou dispositivo remoto SNMP v3). O Engine ID é uma sequência de caracteres alfanuméricos únicos, usado para identificar o switch.

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

View SNMP

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

Escolha o menu *SNMP* → *SNMP* → *View SNMP* para carregar a seguinte página.



View SNMP

As seguintes informações são apresentadas na tela:

» **Configurar view**

Nome da view: digite o nome de identificação da view. Cada view pode incluir várias entradas com o mesmo nome.

MIB OID: digite o OID utilizado pela view.

Modo da view selecione o tipo de entrada da view.

» **Incluir:** inclui para o gerenciamento da view o OID especificado.

» **Excluir:** exclui do gerenciamento da view o OID especificado.

» **Views configuradas**

Selecionar: selecione a entrada desejada. Clique no botão *Remover* para excluir a view. Todas as entradas de uma mesma view, serão excluídas juntas.

Nome da view: exibe o nome da view.

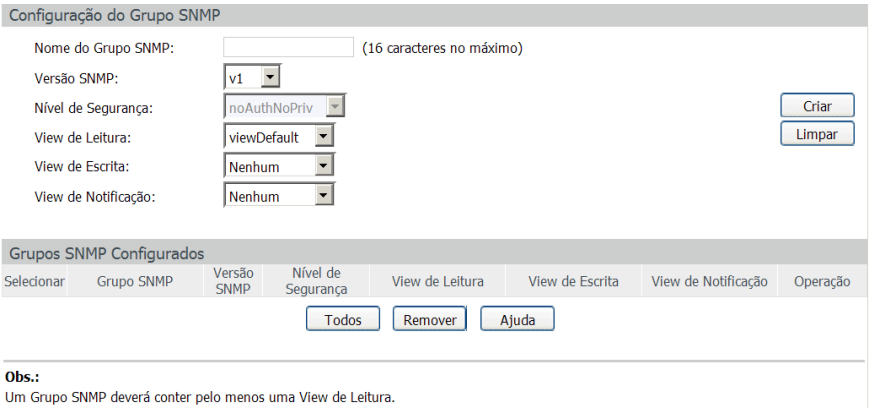
Modo da view: exibe o tipo de entrada da view.

MIB OID: exibe o OID da view.

Grupo SNMP

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

Escolha no menu *SNMP* → *SNMP* → *Grupo SNMP* para carregar a seguinte página.



Grupos SNMP

As seguintes informações são apresentadas na tela.

» **Configuração do grupo SNMP**

Nome do grupo SNMP: digite o nome do grupo SNMP.

Versão SNMP: selecione a versão do protocolo SNMP utilizado pelo grupo SNMP.

» **V1:** nesta versão, o nome da comunidade é utilizado para a autenticação. O SNMP v1 pode ser configurado diretamente na página de configuração Comunidade SNMP.

» **V2C:** nesta versão, o nome da comunidade é utilizado para a autenticação. O SNMP v2c pode ser configurado diretamente na página de configuração Comunidade SNMP.

» **V3:** nesta versão, o mecanismo USM é utilizado para realizar a autenticação. Ao habilitar o SNMP v3, o campo nível de segurança deverá ser configurado.

Nível de segurança: selecione o nível de segurança para grupos SNMPv3.

» **noAuthNoPriv:** este nível de segurança não realiza autenticação e criptografia.

» **authNoPriv:** este nível de segurança realiza autenticação porém não realiza criptografia.

» **AuthPriv:** este nível de segurança realiza autenticação e criptografia.

View de leitura: selecione a view desejada com acesso somente de leitura. A view definida como leitura somente poderá ser lida, não é possível modificá-la.

View de escrita: selecione a view desejada com acesso de escrita. A view definida como escrita poderá ser lida e alterada.

View de notificação: selecione a view desejada com permissão de notificação. A view definida como notificação poderá enviar notificações a estação de gerenciamento SNMP.

» **Grupos SNMP configurados**

Selecionar: selecione a entrada desejada. Clique no botão *Remover* para excluir o grupo SNMP.

Grupo SNMP: exibe o nome do grupo SNMP.

Versão SNMP: exibe a versão do protolo SNMP utilizada pelo grupo SNMP.

Nível de segurança: exibe o nível de segurança do grupo SNMP.

View de leitura: exibe a view de leitura.

View de escrita: exibe a view de escrita

View de notificação: exibe a view de notificação.

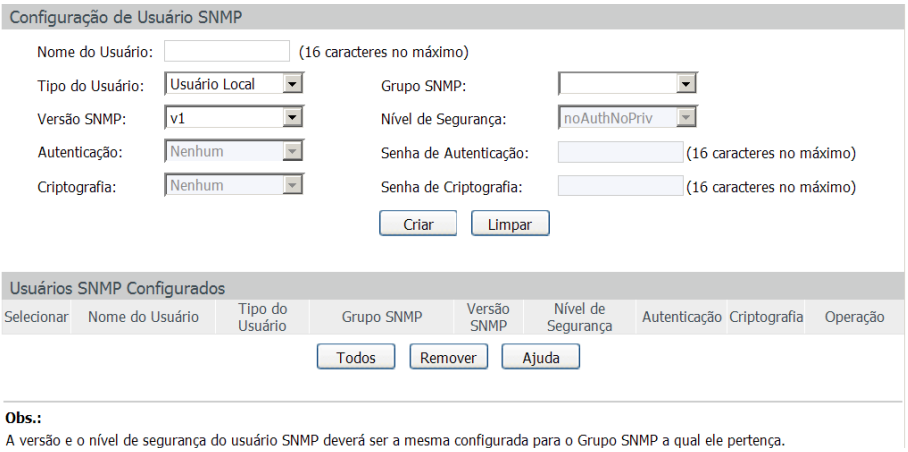
Operação: clique no botão *Modificar* para alterar a view desejada. Após realizado a modificação clique no botão *Modificar* para validar a alteração.

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

Usuário SNMP

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

Escolha o menu *SNMP* → *SNMP* → *Usuário SNMP* para carregar a seguinte página:



Usuários SNMP

As seguintes informações são exibidas na tela:

» **Configuração de usuário SNMP**

Nome de usuário: digite o nome de usuário.

Tipo de usuário: selecione o tipo de usuário.

» **Usuário local:** indica que o usuário está conectado ao Engine SNMP Local.

» **Usuário remoto:** indica que o usuário está conectado ao Engine SNMP Remoto.

Grupo SNMP: selecione o grupo SNMP desejado. O usuário é classificado para o grupo correspondente de acordo com o *Nome do Grupo, Versão e Nível de Segurança SNMP.*

Versão SNMP: selecione a versão do protocolo SNMP utilizado pelo usuário criado.

Nível de segurança: selecione o nível de segurança para o usuário SNMP v3.

Autenticação: selecione o modo de autenticação para o usuário SNMP v3.

» **Nenhum:** nenhum método de autenticação é usado.

» **MD5:** a autenticação da porta usa o algoritmo HMAC-MD5.

» **SHA:** a autenticação da porta é realizada através de SHA (Secure Hash Algorithm). Esse modo de autenticação tem uma segurança maior que o modo MD5.

Senha de autenticação: digite a senha configurada para autenticação.

Criptografia: selecione o modo de criptografia para o usuário SNMP v3.

» **Nenhum:** nenhum método de criptografia é utilizado.

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

Senha de criptografia: digite a senha configurada utilizada na criptografia.

» **Usuários SNMP configurados**

Selecionar: selecione a entrada desejada. Clique no botão *Remover* para excluir o usuário SNMP.

Nome de usuário: exibe o nome do usuário.

Tipo de usuário: exibe o tipo de usuário.

Grupo SNMP: exibe o nome do grupo do usuário.

Versão SNMP: exibe a versão do protocolo SNMP utilizado pelo usuário.

Nível de segurança: exibe o modo de segurança do usuário SNMP.

Autenticação: exibe o modo de autenticação do usuário.

Criptografia: exibe o modo de criptografia do usuário.

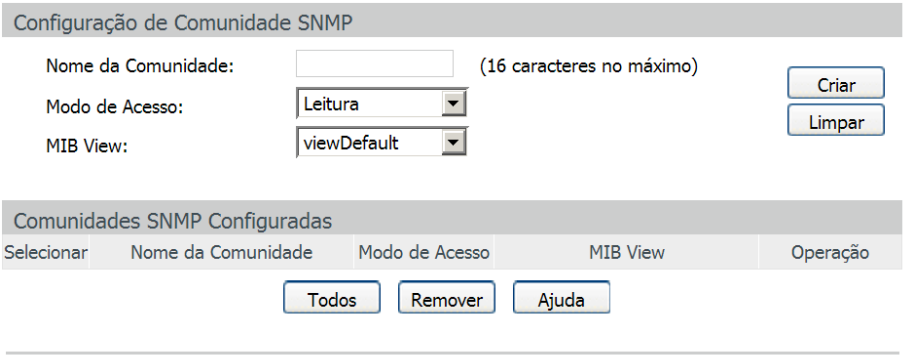
Operação: clique no botão *Modificar* para alterar o grupo do usuário e clique no botão *Modificar* para aplicar as configurações.

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

Comunidade SNMP

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

Escolha o menu *SNMP* → *SNMP* → *Comunidade SNMP* para carregar a seguinte página:



Comunidades SNMP

As seguintes opções são apresentadas na tela:

» **Configuração de comunidade SNMP**

Nome da comunidade: digite o nome da comunidade.

Modo de acesso: defina o tipo de permissão para a comunidade.

» **Leitura:** neste modo, a comunidade terá permissão somente de leitura, nenhuma alteração poderá ser feita.

» **Leitura/Escrita:** neste modo, a comunidade terá permissão de leitura e escrita, podendo realizar alterações.

MIB View: selecione a view de acesso da comunidade.

» **Comunidades SNMP configuradas**

Selecionar: selecione a entrada desejada. Clique no botão *Remover* para excluir a comunidade.

Nome da comunidade: exibe o nome da comunidade.

Modo de acesso: exibe o tipo de permissão da comunidade para acessar a view.

MIB view: exibe a view que a comunidade pode acessar.

Operação: clique no botão *Modificar* para alterar a view e a permissão de acesso da comunidade, em seguida, clique no botão *Modificar* para aplicar as configurações.

Obs.: *a view padrão para a comunidade SNMP é viewDefault.*

Procedimento de configuração:

» Caso for utilizado o SNMPv3, por favor, siga os seguintes passos.

Passo	Operação	Descrição
1	Habilitar a função global SNMP	Obrigatório, em SNMP ⟶ SNMP ⟶ Configurar SNMP, habilitar a função SNMP.
2	Criar a view SNMP	Obrigatório, em SNMP ⟶ SNMP ⟶ View SNMP, criar uma view SNMP para o agente de gerenciamento. O nome da view padrão é viewDefault e o OID padrão é 1.
3	Criar o grupo SNMP	Obrigatório, em SNMP ⟶ SNMP ⟶ Grupo SNMP, criar um grupo SNMP e especifique as views e o nível de segurança desejado.
4	Criar o usuário SNMP	Obrigatório, em SNMP ⟶ SNMP ⟶ Usuários SNMP, criar o usuário SNMP para o grupo e configurar o nível de segurança para o usuário.

» Caso for utilizado o SNMP v1 ou SNMP v2c, por favor, siga os seguintes passos.

Passo	Operação		Descrição
1	Habilitar a função global SNMP		Obrigatório, em SNMP ⟶ SNMP ⟶ Configurar SNMP, habilitar a função SNMP.
2	Criar a view SNMP		Obrigatório, em SNMP ⟶ SNMP ⟶ View SNMP, criar uma view SNMP para o agente de gerenciamento. O nome da view padrão é view Default e o OID padrão é 1.
3	Configure o nível de acesso para o usuário	Criar a comunidade SNMP diretamente.	- Criar a comunidade diretamente. Em SNMP⟶SNMP ⟶ Comunidade SNMP, criar a comunidade baseada em SNMP v1 e SNMPv2c
		Criar o grupo e usuário SNMP.	- Criar grupo e usuário SNMP. Semelhante à configuração do SNMPv3, você pode criar grupos e usuários SNMPv1/v2c. O nome de usuário limita o acesso aos agentes SNMP e a estação de gerenciamento SNMP. Funciona como o nome de comunidade. Os usuários podem gerenciar os dispositivos através de views de leituras, escritas e notificações definidas nos grupos SNMP.

11.2. Notificação

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

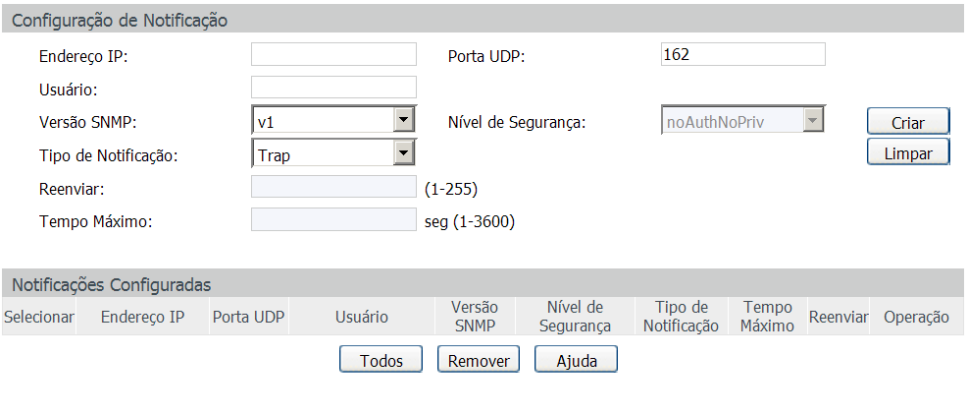
As informações de notificação incluem os seguintes tipos:

» **Trap:** é a informação que o dispositivo gerenciado envia para a estação de gerenciamento de rede sem nenhum tipo de solicitação.

» **Inform:** pacotes inform são enviados para informar a estação de gerenciamento sobre eventuais eventos e sempre aguardam uma resposta. A notificação Inform somente é utilizada com o SNMP v3 e possui uma maior segurança comparado ao Trap.

Nesta página, você pode configurar as notificações da função SNMP.

Escolha o menu *SNMP ⟶ Notificação ⟶ Configurar Notificação* para carregar a seguinte página:



Notificação

As seguintes opções são apresentadas na tela:

» **Configuração de notificação**

Endereço IP: digite o endereço da estação de gerenciamento SNMP.

Porta UDP: digite o número da porta UDP usada para enviar notificações. Padrão é *162*.

Usuário: digite o nome de usuário da estação de gerenciamento.

Versão SNMP: selecione a versão do protocolo SNMP.

Nível de segurança: selecione o nível de segurança para grupos SNMPv3.

» **noAuthNoPriv:** este nível de segurança não realiza autenticação e criptografia.

» **authNoPriv:** este nível de segurança realiza autenticação porém não realiza criptografia.

» **AuthPriv:** este nível de segurança realiza autenticação e criptografia.

Tipo de notificação: selecione o tipo de notificação.

» **Trap:** indica que o tipo de notificação utilizada é a Trap.

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

Reenviar: insira a quantidade de vezes que o switch reenvia uma solicitação inform.

Tempo máximo: insira o tempo máximo para o switch esperar pela resposta da estação de gerenciamento SNMP antes de reenviar um pedido.

» **Notificações configuradas**

Selecionar: selecione a estação de gerenciamento desejada. Clique no botão *Remover* para excluir a entrada.

Endereço IP: exibe o endereço IP da estação de gerenciamento SNMP.

Porta UDP: exibe a porta UDP usada para notificações.

Usuário: exibe o nome de usuário da estação de gerenciamento.

Versão SNMP: exibe a versão do protocolo SNMP.

Nível de segurança: exibe o nível de segurança SNMPv3.

Tipo de notificação: exibe o tipo de notificação.

Tempo máximo: exibe o tempo máximo para o switch esperar pela resposta da estação de gerenciamento SNMP antes de reenviar um pedido.

Reenviar: exibe a quantidade de vezes que o switch reenvia uma solicitação inform.

Operação: clique no botão *Modificar* para alterar as configurações.

11.3. 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.

» **Grupos RMON**

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

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

Os grupos RMON podem ser configurados em *Histórico RMON, Eventos RMON* e *Alarmes RMON*.

Histórico RMON

Nesta página você pode configurar o grupo *Histórico* da função *RMON*.

Escolha o menu *SNMP* → *RMON* → *Histórico RMON* para carregar a página seguinte:

Configuração de Históricos RMON

Selecionar	Índice	Porta	Intervalo (seg)	Dono	Status
☐		Porta 1			Desabilitar
☐	1	Porta 1	1800	monitor	Desabilitar
☐	2	Porta 1	1800	monitor	Desabilitar
☐	3	Porta 1	1800	monitor	Desabilitar
☐	4	Porta 1	1800	monitor	Desabilitar
☐	5	Porta 1	1800	monitor	Desabilitar
☐	6	Porta 1	1800	monitor	Desabilitar
☐	7	Porta 1	1800	monitor	Desabilitar
☐	8	Porta 1	1800	monitor	Desabilitar
☐	9	Porta 1	1800	monitor	Desabilitar
☐	10	Porta 1	1800	monitor	Desabilitar
☐	11	Porta 1	1800	monitor	Desabilitar
☐	12	Porta 1	1800	monitor	Desabilitar

Aplicar Ajuda

Históricos RMON

» **Configuração de históricos RMON**

Selecionar: selecione a entrada desejada para configuração.

Índice: exibe o índice da entrada.

Porta: selecione a porta desejada.

Intervalo (seg): especifique o intervalo de coleta das amostras.

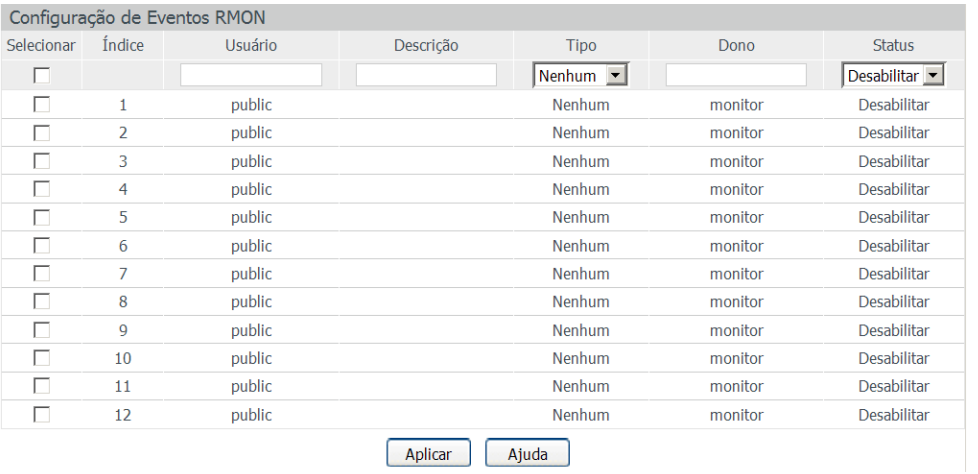
Dono: digite o nome do dispositivo ou usuário que definiu a regra.

Status: selecione *Habilitar/Desabilitar* para habilitar ou desabilitar a entrada correspondente.

Eventos RMON

Nesta página você pode configurar o grupo *Eventos* da função *RMON*.

Escolha o menu *SNMP* → *RMON* → *Eventos RMON* para carregar a página seguinte:



Eventos RMON

As seguintes opções são apresentadas na tela:

» **Configuração de eventos RMON**

Selecionar: selecione a entrada desejada para configuração.

Índice: exibe o índice.

Usuário: digite o nome do usuário ou a comunidade a qual pertence o evento.

Descrição: digite uma descrição para identificação.

Tipo: selecione o tipo de evento.

» **Nenhum:** nenhuma ação é realizada.

» **Log:** registra evento no Log.

» **Trap:** envio de mensagens Trap para a estação de gerenciamento.

» **Log/Trap:** registra o evento no Log e envia mensagens Trap para a estação de gerenciamento.

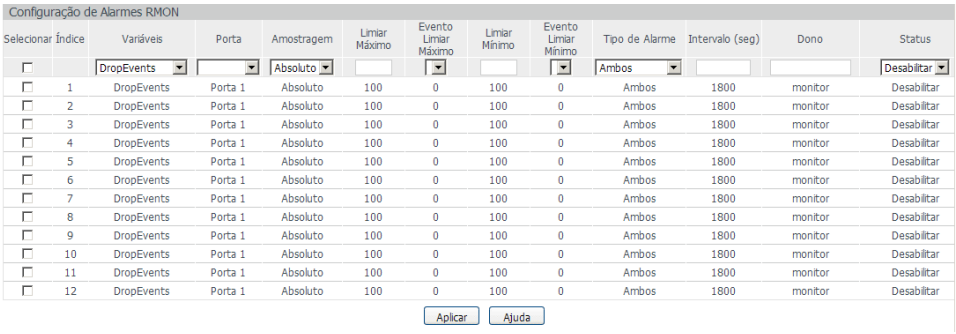
Dono: digite o nome do dispositivo ou usuário que definiu regra.

Status: selecione *Habilitar/Desabilitar* para habilitar ou desabilitar o evento correspondente.

Alarmes RMON

Nesta página você pode configurar os grupos *Estatísticas* e *Alarmes* da função *RMON*.

Escolha o menu *SNMP → RMON → Alarmes RMON* para carregar a seguinte página:


Configuração de Alarmes RMON

Selecionar	Índice	Variáveis	Porta	Amostragem	Limiar Máximo	Evento Limiar Máximo	Limiar Mínimo	Evento Limiar Mínimo	Tipo de Alarme	Intervalo (seg)	Dono	Status
☐		DropEvents		Absoluto					Ambos			Desabilitar
☐	1	DropEvents	Porta 1	Absoluto	100	0	100	0	Ambos	1800	monitor	Desabilitar
☐	2	DropEvents	Porta 1	Absoluto	100	0	100	0	Ambos	1800	monitor	Desabilitar
☐	3	DropEvents	Porta 1	Absoluto	100	0	100	0	Ambos	1800	monitor	Desabilitar
☐	4	DropEvents	Porta 1	Absoluto	100	0	100	0	Ambos	1800	monitor	Desabilitar
☐	5	DropEvents	Porta 1	Absoluto	100	0	100	0	Ambos	1800	monitor	Desabilitar
☐	6	DropEvents	Porta 1	Absoluto	100	0	100	0	Ambos	1800	monitor	Desabilitar
☐	7	DropEvents	Porta 1	Absoluto	100	0	100	0	Ambos	1800	monitor	Desabilitar
☐	8	DropEvents	Porta 1	Absoluto	100	0	100	0	Ambos	1800	monitor	Desabilitar
☐	9	DropEvents	Porta 1	Absoluto	100	0	100	0	Ambos	1800	monitor	Desabilitar
☐	10	DropEvents	Porta 1	Absoluto	100	0	100	0	Ambos	1800	monitor	Desabilitar
☐	11	DropEvents	Porta 1	Absoluto	100	0	100	0	Ambos	1800	monitor	Desabilitar
☐	12	DropEvents	Porta 1	Absoluto	100	0	100	0	Ambos	1800	monitor	Desabilitar

Aplicar Ajuda

Alarmes RMON

As seguintes opções são apresentadas na tela:

» **Configuração de alarmes RMON**

Selecionar: selecione a entrada desejada para configuração.

Índice: exibe o índice da entrada.

Variáveis: selecione as variáveis desejadas presentes na lista.

Porta: selecione a porta a qual a regra de alarme está associada.

Amostragem: especifique o método de amostragem da variável selecionada para comparar os valores entre os limites.

» **Absoluto:** compara os valores diretamente com os limiares configurados no final do intervalo de amostragem.

» **Delta:** subtrai o último valor amostrado a partir do valor atual. A diferença nos valores é comparada com os limiares configurados.

Limiar máximo: digite o valor para o contador disparar o alarme caso este valor seja excedido.

Evento limiar máximo: selecione o índice do evento correspondente, que será acionado se o valor amostrado for maior que o Limiar Máximo.

Limiar mínimo: digite o valor para o contador disparar o alarme caso esse valor seja menor que o especificado.

Evento limiar mínimo: selecione o índice do evento correspondente, que será acionado se o valor amostrado for menor que o Limiar Mínimo.

Tipo de alarme: especifique o tipo de alarme.

» **Ambos:** o evento será acionado se o valor amostrado ultrapassar o Limiar Máximo ou estiver abaixo do Limiar Mínimo.

» **Limiar máximo:** quando o valor amostrado exceder o limite do Limiar Máximo, um evento de alarme será acionado.

» **Limiar mínimo:** quando o valor amostrado estiver abaixo do valor especificado do Limiar Mínimo, um evento de alarme será acionado.

Intervalo (seg.): digite o intervalo de tempo do grupo Alarme em segundos.

Dono: digite o nome do dispositivo ou usuário que definiu a entrada.

Status: selecione *Habilitar/Desabilitar* para habilitar ou desabilitar a regra correspondente.

Obs.: *quando as variáveis excedem o limite de alarme continuamente, um evento de alarme será gerado somente na primeira vez.*

12. Manutenção

No menu *Manutenção* é possível utilizar ferramentas para o diagnóstico da rede, fornecendo métodos para localização e solução de problemas.

- **Monitoramento:** monitora o status de utilização da memória e da CPU do switch.
- **Log:** verifica os parâmetros de configuração do switch para descoberta de eventuais erros.
- **Testar cabo:** testa o status da conexão do cabo para localizar e diagnosticar problemas da rede.
- **Loopback:** testa se as portas do switch e seu dispositivo conectado estão disponíveis.
- **Diagnóstico:** testa se o dispositivo de destino é alcançável e detecta os saltos a partir do switch até o dispositivo de destino.

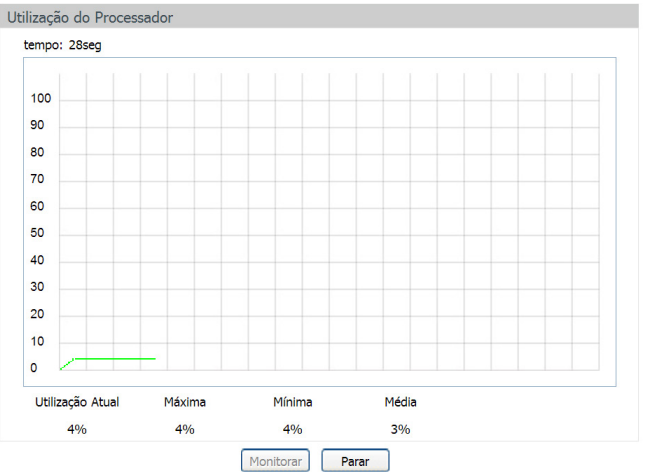
12.1. Monitoramento

A função *Monitoramento* exibe o status de utilização da memória e da CPU do switch através de gráfico de utilização. A taxa de utilização da CPU e a taxa de utilização da memória devem apresentar-se de forma estável em torno de um valor específico. Se a taxa de utilização da CPU ou a taxa de utilização da memória aumentar muito, por favor, verifique se a rede está sendo atacada.

A função *Monitoramento* é visualizada nas páginas *CPU* e *Memória*.

CPU

Escolha o menu *Manutenção* → *Monitoramento* → *CPU* para carregar a seguinte página.

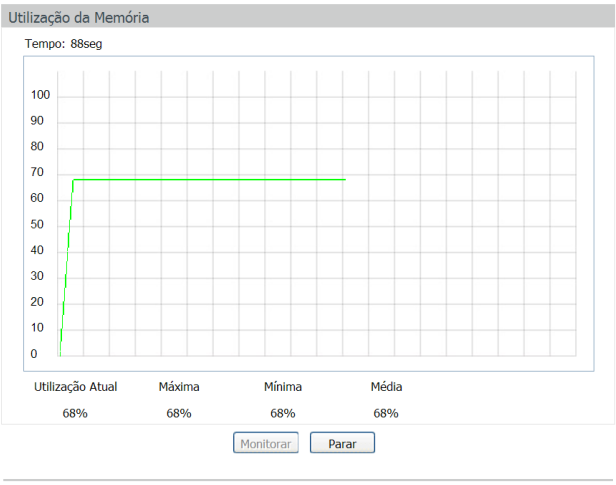


Monitoramento da CPU

Clique no botão *Monitorar* para habilitar a função, o switch irá monitorar e exibir a taxa de utilização da CPU a cada quatro segundos.

Memória

Escolha o menu *Manutenção* → *Monitoramento* → *Memória* para carregar a seguinte página:



Monitoramento da memória

Clique no botão *Monitorar* para habilitar a função, o switch irá monitorar e exibir a taxa de utilização da memória a cada quatro segundos.

12.2. 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.

Os logs do switch são classificados nos seguintes níveis.

Gravidade	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

A função *Log* é configurada em *Tabela de Log, Log Local, Log Remoto e Backup de Log.*

Tabela de log

O switch suporta dois canais para realização de Log, *Log de memória RAM e Log de memória FLASH*. As informações armazenadas na Memória RAM serão perdidas se o switch for reinicializado ou desligado, enquanto as informações em Memória FLASH serão mantidas.

Escolha o menu *Manutenção* → *Log* → *Tabela de Log* para carregar a seguinte página:

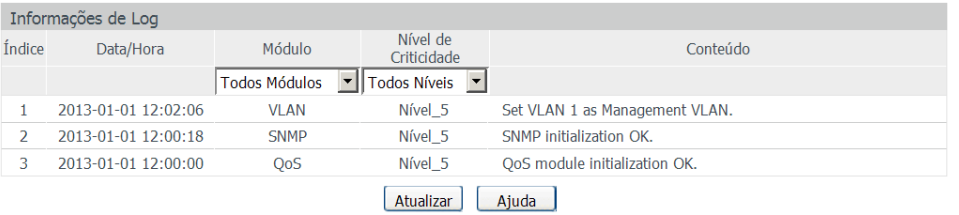


Tabela de logs

As seguintes informações são exibidas na tela:

» **Informações de log**

Índice: exibe o índice da informação de Log.

Data/Hora: exibe o momento em que o evento de Log ocorreu. O registro pode obter a hora correta após configurado a função *Data/Hora no menu Sistema → Informações → Data/Hora.*

Módulo: exibe o módulo que as informações de Log pertencem.

Nível de criticidade: exibe o nível de criticidade das informações.

Conteúdo: exibe o conteúdo das informações de Log.

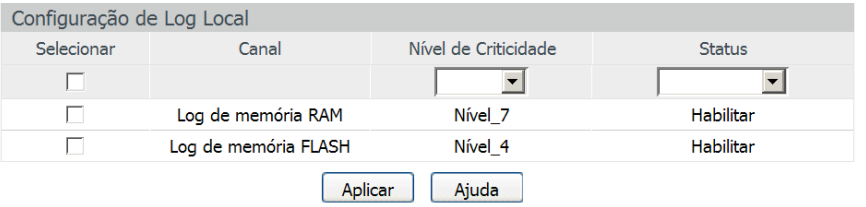
Obs.: » *Os registros de Logs são classificados em oito níveis de criticidade. Quanto maior a criticidade da informação, menor é o número do nível de criticidade.*

» *Esta página exibe apenas os logs de memória RAM. São exibidos no máximo 512 registros.*

Log local

O Log Local é a informação de log salva no próprio switch. Por padrão, todos os logs de sistemas são salvos no Log de Memória RAM e os logs com criticidade de nível 0 até o nível 4 são salvos no Log de Memória FLASH. Nesta página você pode definir o canal de saída para Logs.

Escolha o menu *Manutenção* → *Log* → *Log Local* para carregar a seguinte página:



Log local

As seguintes informações são apresentadas na tela:

» **Configuração de log local**

Selecionar: selecione o canal correspondente para a configuração do Log Local.

Log de memória RAM: indica que os Logs serão salvos na memória RAM. As informações de log de memória RAM serão exibidas na página Tabela de Log. Estas informações serão perdidas quando reiniciar o switch.

Log de memória FLASH: indica que os Logs serão salvos na memória Flash. As informações de log de memória FLASH não serão perdidas após o switch reiniciar e podem ser exportadas para um servidor Syslog através da página *Backup de Log*.

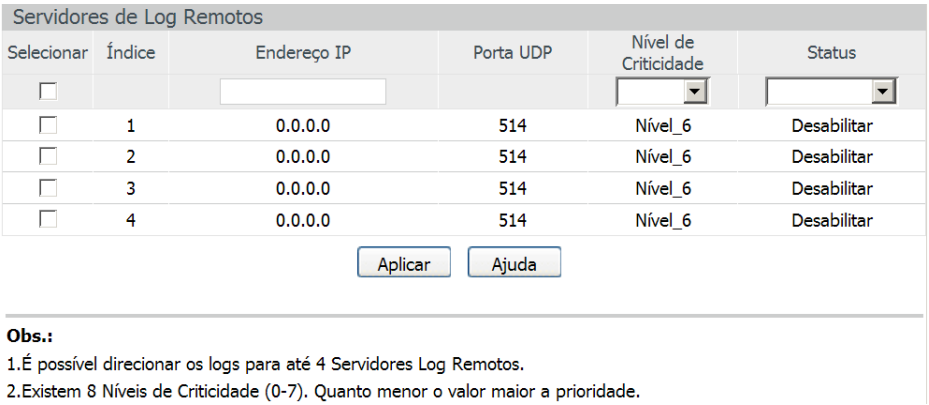
Nível de criticidade: selecione o nível de criticidade de registro da informação de Log. Apenas os logs com o nível de criticidade igual ou menor ao selecionado serão armazenados.

Status: selecione *Habilitar/Desabilitar* para habilitar ou desabilitar a função de Log Local no canal correspondente.

Log remoto

A função *Log Remoto* permite que o switch envie os Logs do sistema para um servidor de Log. O servidor de Log serve para centralizar os Logs do sistema de vários dispositivos da rede.

Escolha o menu *Manutenção* → *Log* → *Log Remoto* para carregar a seguinte página:



Log remoto

As seguintes informações são exibidas na tela:

» **Servidores de log remotos**

Selecionar: selecione o índice desejado para a configuração do servidor de Log remoto.

Índice: exibe o índice do servidor de Log. É possível configurar até 4 servidores de Log remoto.

Endereço IP: digite o endereço IP do servidor de Log.

Porta UDP: exibe a porta UDP usada para enviar/receber informações de Log. Por padrão, a porta utilizada é *514*.

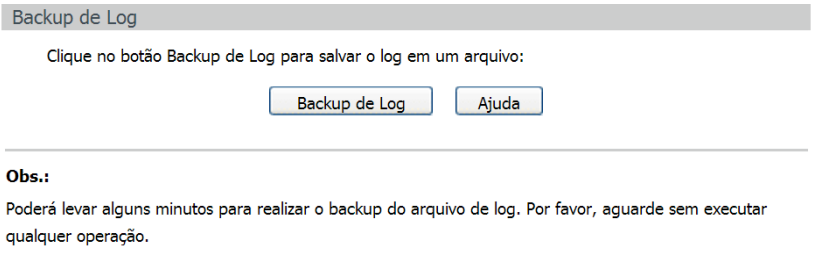
Nível de criticidade: selecione o nível de criticidade da informação de log enviada para o servidor de Log. Apenas os logs com o nível de criticidade igual ou menor ao selecionado serão enviados.

Status: selecione *Habilitar/Desabilitar* para habilitar ou desabilitar o Servidor de Log Remoto desejado.

Backup de log

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

Escolha o menu *Manutenção* → *Log* → *Backup de Log* para carregar a seguinte página.



Backup de log

As seguintes informações são apresentadas na tela:

» **Backup de log**

Backup de log: clique no botão *Backup de Log* para salvar um arquivo com as informações de Log no seu computador.

Obs.: » *Poderá levar alguns minutos para fazer o backup do arquivo de Log. Aguarde sem executar qualquer operação.*

» *Para efetuar o backup é necessário que a opção* Log de memória Flash *no menu* Manutenção → Log → Log local *esteja habilitada. Caso contrário o arquivo de log poderá vir vazio ou com informações antigas.*

12.3. Ferramentas

Este switch oferece as funções *Testar Cabo* e *Loopback* para o diagnóstico de conectividade das portas.

Testar cabo

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

Escolha o menu *Manutenção* → *Ferramentas* → *Testar Cabo* para carregar a seguinte página:

Teste de cabos

As seguintes informações são apresentadas na tela:

» **Teste do cabo**

Porta: selecione a porta desejada para testar o cabo de rede conectado.

Par: exibe a identificação do par do cabo de rede. Considerando o RJ 45 fêmea do Switch: *Par A* pinos 1 e 2, *Par B* pinos 3 e 6, *Par C* pinos 4 e 5, *Par D* pinos 7 e 8.

Status: exibe o status da conexão do cabo de rede conectado à porta. Os resultados do teste do cabo incluem: normal, fechado, aberto ou desconhecido.

Comprimento: se o status do link for normal, será exibido o comprimento do cabo.

Erro: se o status do link for aberto, mostrará a distância que o cabo está rompido (desde que na porta contenha um cabo com mais de 1 m de comprimento). Se o status do link for curto, mostrará a distância do curto. Se o status do link for desconhecido não será exibido o comprimento do cabo, pois o switch não recebeu sinais de retorno para o diagnóstico (um cabo muito longo ou uma alta impedância no final do cabo podem gerar esse sintoma).

Obs.: » *O teste fará com que a porta seja desativada por alguns segundos. Após o teste, a porta retornará à operação normal.*

» *O comprimento exibido é o comprimento dos pares interno do cabo, não do cabo físico em si .*

» *O resultado é apenas para sua referência.*

Loopback

A função Loopback é utilizada para testar a disponibilidade e analisar o status de uma porta física do switch. Esta função auxilia na solução de problemas na rede.

Escolha o menu *Manutenção* → *Ferramentas* → *Loopback* para carregar a seguinte página.

Loopback

As seguintes opções são apresentadas na tela:

» **Configuração de loopback**

Interno: selecione *Interno* para verificar se a porta do switch está disponível.

Externo: selecione *Externo* para verificar se o dispositivo conectado à porta do switch está disponível.

» **Portas**

Portas: selecione a porta desejada para realizar o teste de loopback.

Test: clique no botão *Testar* para iniciar o teste de loopback na porta.

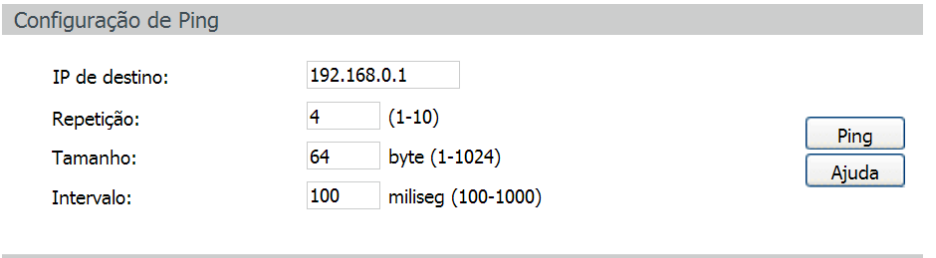
12.4. Diagnóstico

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

Ping

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

Escolha o menu *Manutenção* → *Diagnóstico* → *Ping* para carregar a seguinte página:



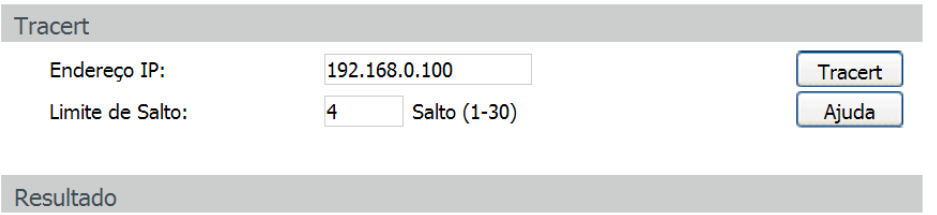
Ping

» **Configuração de ping**
IP de destino: digite o endereço IP do dispositivo de destino para o teste de Ping.
Repetição: digite a quantidade de pacotes enviados durante o Ping.
Tamanho: digite o tamanho dos pacotes enviados durante o Ping. O valor padrão é recomendado.
Intervalo: digite o intervalo de envio das requisições ICMP. O valor padrão é recomendado.

Tracert

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

Escolha o menu *Manutenção* → *Diagnóstico* → *Tracert* para carregar a seguinte página.



Tracert

As seguintes opções são apresentadas na tela:

» **Tracert**
Endereço IP: digite o endereço IP do dispositivo de destino.
Limite de salto: digite o número máximo de saltos que poderá ser realizado até o destino.

13. Restaurando para o padrão de fábrica

O botão *Reset e*stá localizado no painel frontal e é utilizado para restaurar as configurações do switch para o padrão de fábrica. Para retornar as configurações ao padrão de fábrica, pressione o botão *Reset* por mais de 5 segundos e solte-o, logo após o switch reiniciará automaticamente e a configuração estará restaurada para o padrão de fábrica.

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: chat.intelbras.com.br
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

01.22