



Manual do usuário

SG 1002 MR



Switch Gerenciável 8 Portas Gigabit Ethernet com 2 Portas Mini-GBIC SG 1002 MR

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

O switch SG 1002 MR possui 10 portas Gigabit Ethernet, sendo 8 portas RJ45 e 2 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 para os demais dispositivos conectados a ele (dependendo do tipo de acesso e equipamento de banda larga disponível). Este switch integra múltiplas funções com excelente desempenho e fácil configuração.

Índice

1. Sobre o manual	5
1.1. Público destinado para o manual	5
1.2. Convenções	5
1.3. Estrutura do manual	5
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	10
3. Acesso à interface de gerenciamento	11
3.1. Login	11
3.2. Configuração	12
4. Sistema	12
4.1. Informações	12
4.2. Usuários	16
4.3. Ferramentas	18
4.4. Gerenciamento	20
5. Switching	27
5.1. Portas	27
5.2. Agregação de link	32
5.3. Tráfego	35
5.4. Endereço MAC	37
6. VLAN	43
6.1. 802.1Q VLAN	43
6.2. MAC VLAN	48
6.3. Protocolo VLAN	49
6.4. Exemplos de aplicação para 802.1Q VLAN	53
6.5. Exemplos de aplicação para MAC VLAN	54
6.6. Exemplos de aplicação de VLAN por protocolo	55
6.7. GVRP	57
7. Spanning tree	59
7.1. Spanning Tree	63
7.2. Portas STP	65
7.3. Instâncias MSTP	66
7.4. Segurança STP	69
7.5. Exemplos de aplicações STP	71
8. Multicast	74
8.1. IGMP Snooping	76
8.2. Multicast estático	82
8.3. Filtro multicast	84
8.4. Estatísticas IGMP	86

9. QoS	87
9.1. DiffServ	89
9.2. Controle de banda	93
9.3. Voice VLAN	95
10. ACL	99
10.1. Agendamentos	99
10.2. Configurar ACL	101
10.3. Políticas ACL	105
10.4. Vínculos ACL	107
10.5. Exemplos de aplicação para ACL	108
11. Segurança	110
11.1. Associação ARP	110
11.2. Inspeção ARP	117
11.3. DoS	123
11.4. 802.1X	124
12. SNMP	130
12.1. SNMP	131
12.2. Notificação	137
12.3. RMON	139
13. Cluster	142
13.1. NDP	143
13.2. NTDP	145
13.3. Cluster	148
13.4. Exemplo de aplicação da função cluster	151
14. Manutenção	152
14.1. Monitoramento	152
14.2. Log	153
14.3. Ferramentas	157
14.4. Diagnóstico	158
15. Restaurando para o padrão de fábrica	160
Termo de garantia	162

1. Sobre o manual

Este manual contém informações para instalação e gerenciamento do switch SG 1002 MR. Por favor, leia este manual 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*.
- » *Ítálico* 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 1002 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. A seguir as principais informações: - 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. A seguir as principais informações: - 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.
6 - VLAN	Este módulo é utilizado para configurar VLANs. A seguir as principais informações: - 802.1Q VLAN: configuração de VLANs baseada em portas. - MAC VLAN: configuração de VLANs baseado em endereços MAC, sem alterar a configuração 802.1Q VLAN. - Protocolo VLAN: configuração de VLANs baseada em protocolos de rede. - GVRP: permite o switch adicionar, remover ou propagar VLANs através de informações de registro dinâmicos de VLAN, sem a necessidade de configurar individualmente cada VLAN.
7 - Spanning Tree	Este módulo é utilizado para configurar a função Spanning Tree no switch. A seguir as principais informações: - 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. A seguir as principais informações: - 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. A seguir as principais informações: - 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 Voice VLAN, 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 de ACL predeterminadas, a fim de controlar o tráfego de dados na rede. A seguir as principais informações: - Agendamentos: configuração de período de tempos para a aplicação das regras de ACL. - Configurar ACL: criação e configuração de regras para as ACLs. - Políticas ACL: configuração de políticas de ACL. - Vínculos ACL: configuração de vínculos de Políticas ACL a uma determinada VLAN ou porta do switch.
11 - Segurança	Este módulo é utilizado para configurar medidas de proteção para a segurança da rede. A seguir as principais informações: - Associação ARP: permite vincular o endereço IP, endereço MAC, VLAN ID e o número da porta do switch que o host está conectado, permitindo o acesso à rede. - Inspeção ARP: utilizado para prevenir ataques ARP na rede. - DoS: configuração de proteção a ataques de negação de serviço (Denial of Service). - 802.1X: configuração de controle de acesso à rede, provendo um mecanismo de autenticação, aumentando a segurança da rede.
12 - SNMP	Este módulo é utilizado para configurar a função SNMP, provendo um monitoramento e gerenciamento do switch na rede. A seguir as principais informações: - 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.
13 - CLUSTER	Este módulo é utilizado para configurar a função Cluster, utilizando os protocolos NDP e NTDP para descoberta de vizinhos e manutenção da Topologia que envolve os dispositivos do Cluster. A seguir as principais informações: - NDP: protocolo utilizado para obter informações dos dispositivos vizinhos diretamente conectados. - NTDP: protocolo utilizado para coletar as informações da topologia da rede. - Cluster: configuração do modo de operação do switch dentro de um Cluster.
14 - Manutenção	Este módulo é utilizado para monitorar o switch e diagnosticar possíveis problemas na rede. A seguir as principais informações: - 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.
15 - Restaurando para o padrão de fábrica	Restaurando o switch ao padrão de fábrica.

2. Introdução

2.1. Especificações técnicas

Chipset		Broadcom BCM53312S
Dimensões (C x A x L)		294 x 180 x 44 mm
Material		Aço
LED	Power	Verde
	SYS	Verde
	Link/Act	Verde
	1000 Mbps	Verde
	Mini-GBIC	Verde
Portas	10/100/1000M (RJ45)	8
	Mini GBIC (SFP)	2 (independentes)
	Console (RJ45)	1
Cabeamento suportado	10BASE-T	Cabo UTP/STP categoria 3, 4, 5 (máximo 100m) EIA/TIA-568 100Ω STP (máximo 100m)
	100BASE-TX	Cabo UTP/STP categoria 5, 5e (máximo 100m) EIA/TIA-568 100Ω STP (máximo 100m)
	1000BASE-T	Cabo UTP/STP categoria 5e, 6 (máximo 100m) EIA/TIA-568 100Ω STP (máximo 100m)
	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, 802.1x, 802.1d, 802.1w, 802.1s, 802.1v, 802.3ac
	Padrão IETF	RFC1541, RFC1112, RFC2236, RFC2618, RFC1757, RFC1157, RFC2571, RFC2030
	Outros padrões e protocolos	CSMA/CD, TCP/IP, SNMPv1/v2c/v3, HTTP, HTTPS, SSHv1/v2
Características básicas	Método de comutação	Armazena e envia (Store-and-Forward)
	Capacidade comutação	20 Gbps
	Tabela de Endereço MAC	8 K
	Jumbo Frame	10240 Bytes
	Taxa de encaminhamento de pacote	14,9 Mpps
	VLAN	4 K VLANs ativas 4 K VID
	Agregação de link (LAG)	8 grupos 8 portas por grupos
	Multicast	256 grupos
	QOS (Quality of Service)	4 Filas de prioridade
	Associação ARP	200 entradas
	Número de ACL	64
Características	Configuração de portas	Auto negociação Controle de fluxo Espelhamento de portas Estatísticas de tráfego
		Agregação de Link Manual
		Agregação de Link Dinâmica (LACP)
	Agregação de link	Algoritmo baseado em endereço MAC de origem e destino Algoritmo baseado em endereço IP de origem e destino
		Filtro de endereço MAC
	Tabela MAC	Endereço MAC Estático Endereço MAC Dinâmico

Características	VLAN	4K VLANs Ativa e 4K VLANs IDs
		VLAN baseado em Tag 802.1Q
		VLAN baseado em Endereço MAC
		VLAN baseado em Protocolo de Rede
		VLAN de gerenciamento
		Voice VLAN
	Spanning tree	GARP/GVRP
		802.1d Spanning Tree Protocol (STP)
		802.1w Rapid Spanning Tree Protocol (RSTP)
		802.1s Multiple Spanning Tree Protocol (MSTP)
		Loop Guard
		Root Guard
	Gerenciamento Multicast	TC-BPDU Guard
		BPDU Guard
		BPDU Filter
		IGMP v1/v2/v3
		IGMP Snooping
		Fast Leave
	QoS	Multicast VLAN
		Multicast Estático
		Filtro Multicast
		Estatísticas IGMP
		4 Filas de prioridade
		Algoritmos de fila: SP, WRR, SP+WRR
	Segurança	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 das Portas
	Gerenciamento	Isolamento das Portas
		Associação ARP (Manual, ARP scanning, DHCP snooping)
		Proteção ARP
		DoS (Denial of Service)
		ACL (L2/L3/L4)
		Classificação de pacotes baseados em: End. MAC, End. IP, Portas TCP/UDP, Tipo de Protocolo
	Manutenção	Autenticação 802.1x (Baseado em Porta e Endereço MAC)
		Autenticação RADIUS
		Guest VLAN
		SSLv2/SSLv3/TLSv1
		SSHv1/SSHv2
		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, Console, SSHv1/v2)
		Espelhamento de porta
		Atualização de firmware via TFTP/web
	Manutenção	Configuração backup/reload
		DHCP Cliente
		DHCP Snooping
		DHCP Option 82
		SNTP Cliente
		BOOTP Cliente
	Manutenção	Testes de Ping e Tracert
		Sistema de Log (Local e Remoto)
		Monitoramento de CPU e Memória

Alimentação	Entrada	100-240 VAC, 50/60 Hz
	Temperatura de operação	0°C a 40°C
Ambiente	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 1002 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. ACL, 802.1x e Inspeção ARP fornecem uma robusta estratégia de segurança. QoS e IGMP Snooping/Filtro otimizam as aplicações de voz e vídeo. O LACP aumenta a largura de banda agregada, otimizando o transporte de dados, evitando gargalos na rede. SNMP, RMON, WEB/CLI/TELNET/SSH trazem uma grande variedade de políticas de gerenciamento. O SG 1002 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 (LACP), 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

- » GVRP, (GARP VLAN Registration Protocol) permite a criação automática de VLANs.
- » Suporte a 4K 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.

Segurança

- » Suporta vários padrões estabelecidos pela indústria e métodos de autenticação de usuário, como 802.1X e RADIUS.
- » Inspeção ARP, impedindo mensagens ARP não autorizado.
- » Lista de Controle de Acesso (ACL) nas camadas 2/3/4 permitindo ou bloqueando determinados tráfegos da rede.
- » Fornece criptografia de acesso SSHv1/v2, SSL 2.0/3.0 e TLS v1.

Gerenciamento

- » Suporte a SSH, Telnet, SNMP v1/v2c/v3, RMON e acesso web (http e https).

2.4. Descrição do produto

Painel frontal

O painel frontal do SG 1002 MR possui 10 portas Gigabit Ethernet, sendo 8 portas RJ45 e 2 slots Mini-GBIC independentes, 1 porta console (RJ45) para gerenciamento via linha de comando, além de LEDs de monitoramento.

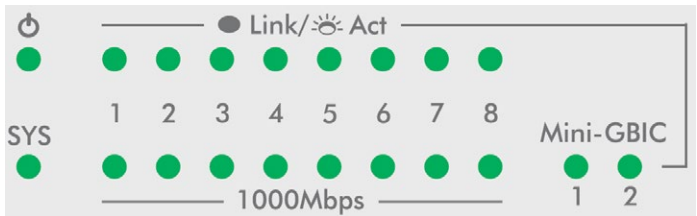


Painel frontal

- » **Portas 10/100/1000 Mbps:** 8 portas 10/100/1000 Mbps para conectar dispositivos com velocidade de 10 Mbps, 100 Mbps ou 1000 Mbps. Cada porta possui 2 LEDs correspondente.
- » **Portas SFP:** 2 portas Mini-Gbic para conectar módulos SFP 1000 Mbps. Cada porta possui 1 LED correspondente.
- » **Porta Console:** 1 porta RJ45 para conectar com a porta serial de um computador para o gerenciamento e monitoramento do switch.

LEDs

No painel frontal são apresentados 20 LEDs de monitoramento, que seguem o comportamento abaixo:



LEDs

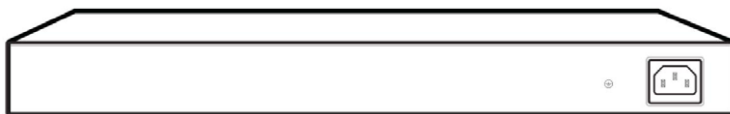
LED	STATUS	INDICAÇÃO
PWR	Aceso	Switch conectado a energia elétrica
	Piscando	Switch com problema na fonte de alimentação
	Apagado	Switch desligado ou com problema na fonte de alimentação
SYS	Aceso	Switch está funcionando de forma anormal
	Piscando	Switch funcionando normalmente
	Apagado	Switch está funcionando de forma anormal
Link/Act	Aceso	Conexão válida estabelecida, sem recepção/transmissão de dados
	Piscando	Conexão válida estabelecida, com transmissão/recepção de dados
	Apagado	Nenhuma conexão válida nesta porta, ou a porta está desativada
1000 Mbps	Aceso	Conexão válida estabelecida a 1000 Mbps estabelecida
	Apagado	A porta está conectada a um dispositivo 10/100 Mbps
	Apagado	Nenhuma conexão válida nesta porta, ou a porta está desativada
Mini-GBIC	Aceso	Conexão válida estabelecida, sem recepção/transmissão de dados
	Piscando	Conexão válida estabelecida, com transmissão/recepção de dados
	Apagado	Nenhuma conexão válida nesta porta, ou a porta está desativada

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

Por padrão, a velocidade e o modo de transmissão de uma porta SFP é 1000 MFD.

Painel posterior

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



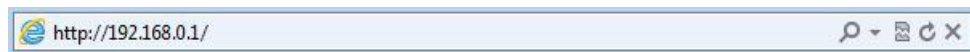
Painel posterior

- » **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 192.168.0.x (x sendo qualquer número de 2 à 254), e máscara de rede igual a 255.255.255.0.

2. Após digitado o endereço IP do switch no navegador, será exibido a tela de login, conforme imagem a seguir. Digite *admin* para o nome de usuário e senha, ambos em letras minúsculas. 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.

intelbras

Switch Gerenciável
8 portas Giga + 2 portas Mini-Gbic

SG 1002 MR

Sistema

- Informações
- Usuários
- Ferramentas
- Gerenciamento

Switching

VLAN

Spanning Tree

Multicast

QoS

ACL

Segurança

SNMP

Cluster

Manutenção

Salvar

Logout

Status | Descrição | Data/Hora | Endereço IP

123456789(SFP)10(SFP)

Informações do Sistema

Descrição:	Switch Gerenciável 8 portas GE + 2 Mini-Gbic
Nome do Dispositivo:	SG 1002 MR
Localização do Dispositivo:	Brasil
Contato do Dispositivo:	www.intelbras.com.br
Versão de Hardware:	SG 1002 MR 1.0
Versão de Firmware:	1.8.2 Build 20130801 Rel.41158
Endereço IP:	192.168.0.1
Máscara de Rede:	255.255.255.0
Gateway Padrão:	
Endereço MAC:	A0-F3-C1-05-F9-90
Data/Hora:	2013-01-01 12:00:28
Tempo ativo:	0 dia(s) - 0 hora(s) - 0 min - 34 seg

Atualizar

Ajuda

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 sub-menus: *Informações*, *Usuários*, *Ferramentas* e *Gerenciamento*.

4.1. Informações

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

Status

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

O diagrama de portas, mostra o status das 8 portas 10/100/1000 Mbps RJ45 e das 2 portas Mini-GBIC (SFP) do switch.

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

123456789(SFP)10(SFP)

Informações do Sistema

Descrição:	Switch Gerenciável 8 portas GE + 2 Mini-Gbic
Nome do Dispositivo:	SG 1002 MR
Localização do Dispositivo:	Brasil
Contato do Dispositivo:	www.intelbras.com.br
Versão de Hardware:	SG 1002 MR 1.0
Versão de Firmware:	1.8.2 Build 20130801 Rel.41158
Endereço IP:	192.168.0.1
Máscara de Rede:	255.255.255.0
Gateway Padrão:	
Endereço MAC:	A0-F3-C1-05-F9-90
Data/Hora:	2013-01-01 12:12:58
Tempo ativo:	0 dia(s) - 0 hora(s) - 13 min - 4 seg

Atualizar

Ajuda

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.

Porta: 1

Tipo: 1000M RJ45

Velocidade: 1000M, Full Duplex

Status: Conectado, Habilitar

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.

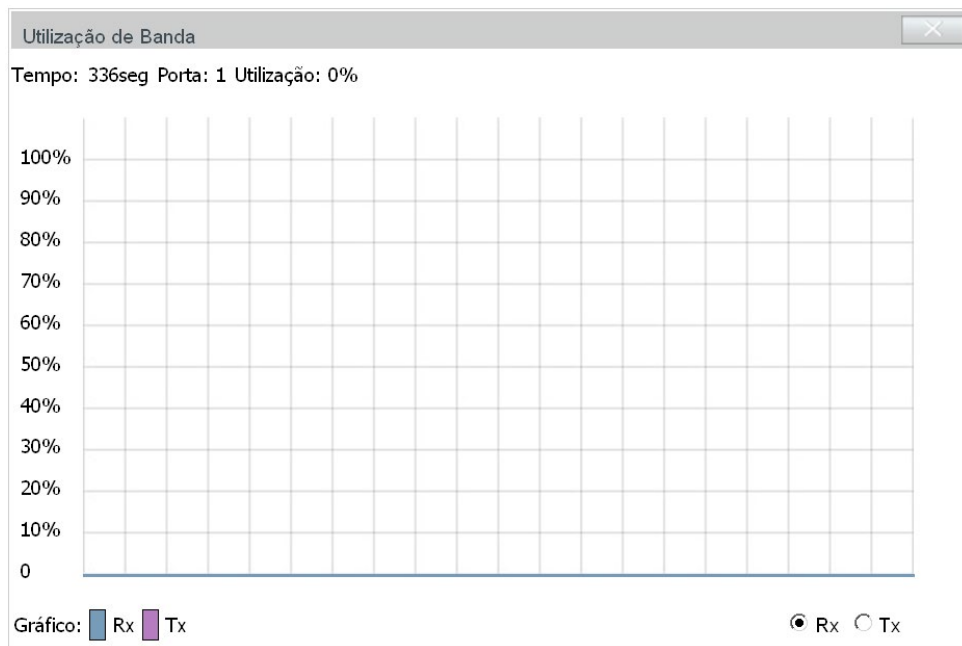


Gráfico de utilização da porta

» Utilização de banda

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

Tx: selecione Tx para exibir a banda utilizada na 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.

Configurar Descrição

Nome do Dispositivo: SG 1002 MR

Localização do Dispositivo: Brasil

Contato do Dispositivo: www.intelbras.com.br

Aplicar

Obs.:

O nome, localização e contato do dispositivo não deverá ter mais que 32 caracteres.

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, ACL.

A configuração poderá ser realizada de forma automática, conectando-se a um servidor NTP, 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:

Informações de Data/Hora
Data e Hora: 2013-08-07 17:22:13 Quarta
Tipo de Data/Hora: Manual

Configuração de Data/Hora
☒ Manual
Data: 2013 08 07
Hora: 17 22 13
☐ Servidor NTP
Fuso Horário: (GMT-03:00) Brasilia, Buenos Aires
Servidor Primário: 133.100.9.2
Servidor Secundário: 139.78.100.163
☐ Sincronizar com Data/Hora do PC

Configurar Horário de Verão
Horário de Verão: Desabilitar
Data/Hora inicial: 04 01 00:00
Data/Hora final: 10 01 00:00

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 somente 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.

» **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.

» Configurar horário de verão

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

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

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

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

» Quando a opção Servidor NTP está selecionada e nenhum servidor NTP for encontrado, o switch receberá a data e hora do servidor de internet, se o switch estiver conectado a internet.

Endereço IP

Nesta página você pode configurar o endereço IP do switch. 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:

Configuração de rede	
Endereço MAC:	A0-F3-C1-05-F9-90
Modo de endereçamento:	☒ IP Estático ☐ DHCP ☐ BOOTP
VLAN de Gerenciamento:	1 (VLAN ID: 1-4094)
Endereço IP:	192.168.0.1
Máscara de Rede:	255.255.255.0
Gateway Padrão:	

Aplicar

Ajuda

Obs.:

Ao alterar o Endereço IP para um segmento de 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

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 dinamicamente, 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 sub-menu *Usuários* é utilizado para realizar configurações de usuários e senhas com níveis de acessos diferentes ao login na página de gerenciamento web. Este sub-menu 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			
ID	Nome de Usuário	Nível de Acesso	Status
1	admin	Admin	Habilitar

Atualizar

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 de Usuário

Nome de Usuário:

Nível de Acesso:

Convidado

Status do Usuário:

☒ Habilitar ☐ Desabilitar

Senha:

Confirmar senha:

Criar

Limpar

Usuários Configurados					
Selecionar	ID	Nome de Usuário	Nível de Acesso	Status	Operação
☐	1	admin	Admin	Habilitar	Modificar

Remover

Ajuda

Obs.:
O Nome de Usuário e Senha devem conter no máximo 16 caracteres. Somente é permitido caracteres

Configuração dos usuários

As seguintes opções são exibidas na tela:

» 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 sub-menu *Ferramentas*, é possível gerenciar os arquivos de configuração do switch, atualizar o firmware, reiniciar e restaurar ao padrão de fábrica. Este sub-menu possui cinco itens de configuração: *Restaurar*, *Backup*, *Atualizar Firmware*, *Reiniciar* e *Restaurar Padrão*.

Restaurar

Nesta página você pode realizar o upload 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:

Restaurar as configurações do switch

Restaurar as configurações do switch através de um arquivo previamente salvo.

Selecione o arquivo previamente salvo no seu computador e clique no botão restaurar.

Arquivo de backup:

Obs.:

Não realize nenhuma operação durante a restauração das configurações. Este processo poderá levar alguns minutos.

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.

Realizar Backup das configurações do switch

Backup das configurações do switch

Clique no botão de backup para salvar as configurações do switch em seu computador.

Obs.:

Não realize nenhuma operação enquanto é realizado o backup das configurações. Este processo poderá levar alguns minutos.

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 de Firmware

O novo firmware somente estará disponível após pressionar o botão *Atualizar*.

Carregar Firmware:

Procurar...

Atualizar

Firmware Versão: 1.8.2 Build 20130801 Rel.41158

Ajuda

Hardware Versão: SG 1002 MR 1.0

Obs.:

1. Certifique-se que o arquivo de atualização do firmware é correspondente ao modelo do switch.
2. Para evitar danos, por favor, não desligue o switch durante a atualização.
3. Após a atualização, o switch irá reiniciar automaticamente.
4. Sugerimos que você faça um backup das configurações antes de atualizar o switch.

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 no menu *Sistema* → *Ferramentas* → *Reiniciar* para carregar a seguinte página.

Reiniciar o switch

Salvar as modificações:



Reiniciar:

Reiniciar

Obs.:

Para evitar danos, por favor, não desligue o switch durante a reinicialização.

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.

Restaurar Padrão de Fábrica

Padrão de Fábrica:

Restaurar

Obs.:

Ao restaurar para o Padrão de Fábrica, todas as configurações atuais serão perdidas.

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 sub-menu *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.

Configuração do Controle de Acesso

Modo:

Desabilitado

Endereço IP:

Máscara:

Endereço MAC:

Porta:

☐ 1	☐ 2	☐ 3	☐ 4	☐ 5	☐ 6	☐ 7	☐ 8
☐ 9	☐ 10						

Configurar limite de Sessão

Tempo ocioso:

10 min (5-30)

Limitar número de usuários

Controle de Usuários:

☐ Habilitar ☒ Desabilitar

Usuários Admin:

(1-16)

Usuários Convidado:

(0-15)

Aplicar

Ajuda

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.

» **Configurar limite 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. Criptografia 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

SSL:

☒ Habilitar ☐ Desabilitar

Aplicar

Ajuda

Alterar Certificado

Certificado:

Procurar...

Download

Alterar Chave Criptográfica

Chave Criptográfica:

Procurar...

Download

Obs.:

1. Ao alterar o Certificado e a Chave, será necessário reiniciar o switch para validar a modificação.
2. O Certificado e a Chave devem ser correspondentes, caso contrário, a conexão HTTPS não funcionará.

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 irá utilizar. Após realizar com sucesso a autonegociação, o cliente envia a solicitação de autenticação ao servidor para realização do login. Somente após autenticado, a comunicação entre o cliente e o servidor será estabelecida.

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

SSH: ☐ Habilitar ☒ Desabilitar

Protocolo V1: ☒ Habilitar ☐ Desabilitar

Protocolo V2: ☒ Habilitar ☐ Desabilitar

Tempo Ocioso: seg (1-999)

Limite de Conexão: (1-5)

Aplicar

Ajuda

Alterar Chave Criptográfica

Selecione o Tipo da Chave Pública e faça o download para o switch.

Tipo da Chave:

Download

Chave Pública:

Procurar...

Obs.:

Poderá levar alguns minutos para realizar o download da chave criptográfica. Por favor, aguarde sem executar qualquer operação.

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.*

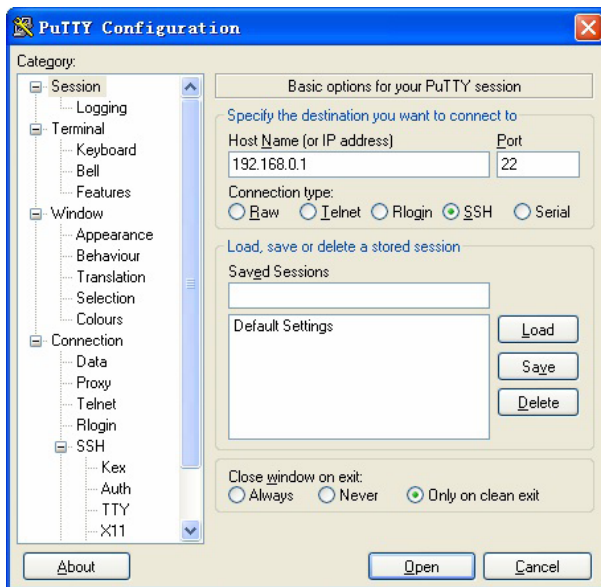
Primeiro exemplo de aplicação SSH

» 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.

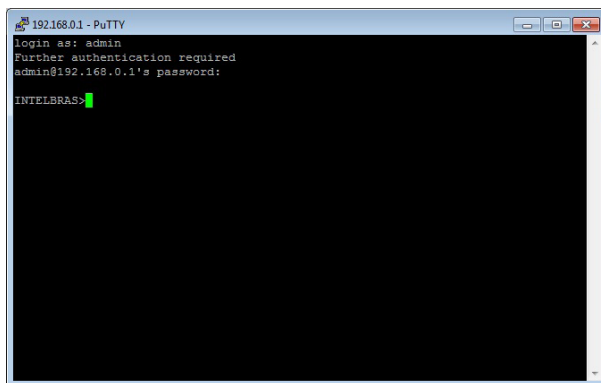
» Procedimento de configuração

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 realizado o login, será possível gerenciar o switch através do terminal de linha de comando, conforme imagem a seguir.



Terminal de linha de comandos

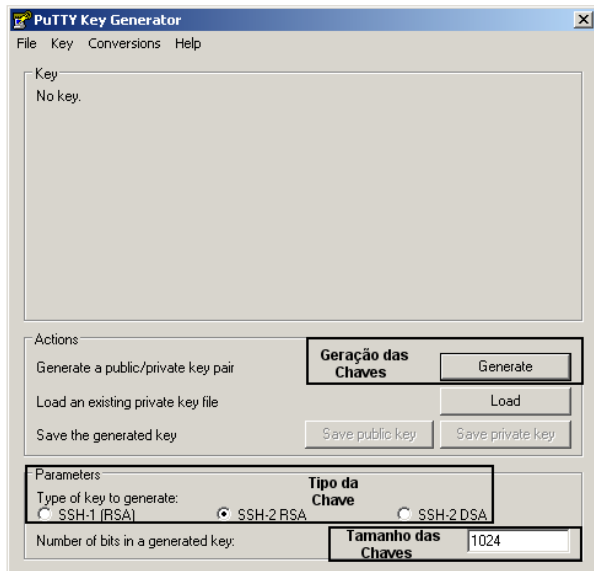
Segundo exemplo de aplicação SSH

» 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

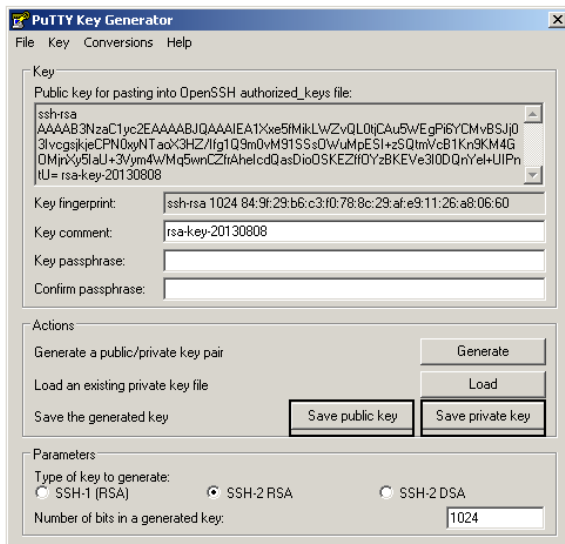
1. Abra o programa PuTTY Key Generator e selecione o tipo e o comprimento da chave SSH e clique no botão *Generate*, conforme imagem a seguir:



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:

Alterar Chave Criptográfica

Selecione o Tipo da Chave Pública e faça o download para o switch.

Tipo da Chave:

Chave Pública:

Obs.:

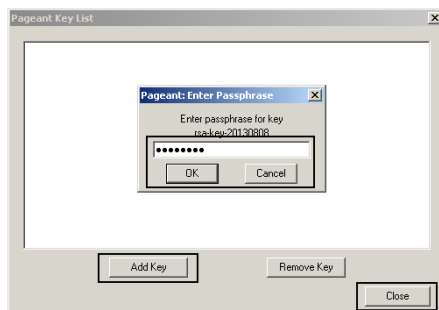
Poderá levar alguns minutos para realizar o download da chave criptográfica. Por favor, aguarde sem executar qualquer operação.

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.*

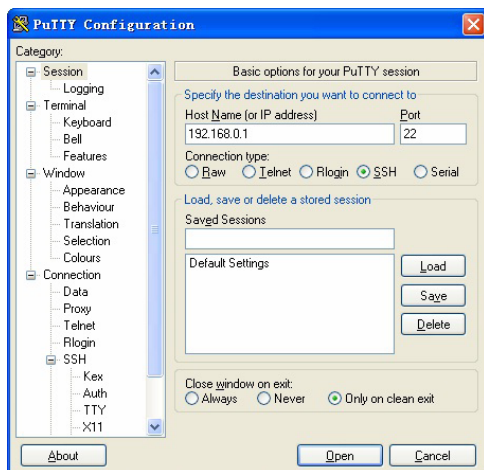
» *Não interrompa o download da chave SSH.*

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



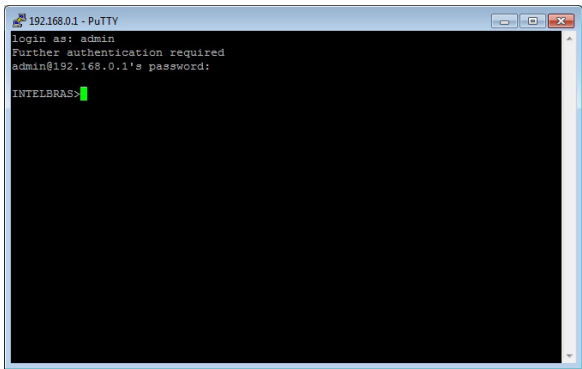
Carregando a chave privada

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 quatro sub-menus: *Portas, Agregação de Link, Tráfego e Endereço MAC*.

5.1. Portas

O sub-menu *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 e Isolamento das Portas*.

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:

Configuração das Portas

Porta Selecionar

Selecionar	Porta	Descrição	Status	Velocidade e Duplex	Controle de Fluxo	LAG
☐			Desabilitar	10 MHD	Desabilitar	
☐	1		Habilitar	Auto	Desabilitar	---
☐	2		Habilitar	Auto	Desabilitar	---
☐	3		Habilitar	Auto	Desabilitar	---
☐	4		Habilitar	Auto	Desabilitar	---
☐	5		Habilitar	Auto	Desabilitar	---
☐	6		Habilitar	Auto	Desabilitar	---
☐	7		Habilitar	Auto	Desabilitar	---
☐	8		Habilitar	Auto	Desabilitar	---
☐	9(SFP)		Habilitar	1000 MFD	Desabilitar	---
☐	10(SFP)		Habilitar	1000 MFD	Desabilitar	---

Aplicar Ajuda

Obs.:

A Descrição da Porta deverá ter no máximo 16 caracteres.

As seguintes informações são exibidas na tela:

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:

Grupo de Espelhamento

Grupo:

1

Configuração da Porta Espelho

Porta Espelho:

Desabilitar

Configuração da Porta Espelhada

Porta

Selecionar

Selecionar	Porta	Entrada	Saída	LAG
☐		Desabilitar	Desabilitar	
☐	1	Desabilitar	Desabilitar	---
☐	2	Desabilitar	Desabilitar	---
☐	3	Desabilitar	Desabilitar	---
☐	4	Desabilitar	Desabilitar	---
☐	5	Desabilitar	Desabilitar	---
☐	6	Desabilitar	Desabilitar	---
☐	7	Desabilitar	Desabilitar	---
☐	8	Desabilitar	Desabilitar	---
☐	9	Desabilitar	Desabilitar	---
☐	10	Desabilitar	Desabilitar	---

Aplicar

Voltar

Ajuda

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 várias 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:

Configuração de Segurança das Portas					
Selecionar	Porta	Número Máximo de End. MAC	End. MAC Aprendidos	Modo de Aprendizado	Status
☐				Dinâmico	Desabilitar
☐	1	64	0	Dinâmico	Desabilitar
☐	2	64	0	Dinâmico	Desabilitar
☐	3	64	0	Dinâmico	Desabilitar
☐	4	64	0	Dinâmico	Desabilitar
☐	5	64	0	Dinâmico	Desabilitar
☐	6	64	0	Dinâmico	Desabilitar
☐	7	64	0	Dinâmico	Desabilitar
☐	8	64	0	Dinâmico	Desabilitar
☐	9	64	0	Dinâmico	Desabilitar
☐	10	64	0	Dinâmico	Desabilitar

Aplicar

Ajuda

Obs.:

O número máximo de Endereços MAC aprendidos por cada porta é 64.

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.

» A função *Segurança das Portas* será desabilitada quando a função 802.1X está ativada.

Isolamento das portas

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:

Configuração de Isolamento das Portas

Porta: 1

Portas de Encaminhamento:

☐ 1

☐ 2

☐ 3

☐ 4

☐ 5

☐ 6

☐ 7

☐ 8

☐ 9

☐ 10

Todas

Aplicar

Ajuda

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.

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, GVRP, VLAN, Tipo de Endereço MAC*. Seguem as explicações.

- » Portas que estiverem habilitadas as funções *GVRP, 802.1Q VLAN, Voice VLAN, Spanning Tree, QoS, DHCP Snooping 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, Endereço MAC Estático e 802.1X*, não poderão ser adicionadas a um grupo LAG.
- » Não é recomendado adicionar portas a um grupo LAG que estejam habilitadas com as funções *Inspecção ARP e DoS (Denial of Service)*.

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 ($2000 \text{ Mbps} * 4$) 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:

Distribuição do tráfego

Algoritmo de Hash:

MAC_Origem + MAC_Destino

Aplicar

Agregação de Link existente

Selecionar	Grupo LAG	Descrição	Membros	Operação
☐	LAG1	Agregado 1	9, 10	Modificar Detalhes

Todos

Remover

Ajuda

Obs.:

1. Agregação de Link criada por LACP não poderá ser removida nesta 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. O recurso LACP estará desabilitado para as portas membros de grupos LAG Estáticos.

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

Configuração de Grupo LAG Estático

Grupo LAG:

Descrição:

 (16 caracteres no máximo)

Portas Membro

☐ 1	☐ 2	☐ 3	☐ 4	☐ 5	☐ 6
☐ 7	☐ 8	☒ 9 (LAG1)	☒ 10 (LAG1)		

Aplicar

Limpar

Ajuda

Obs.:

1. LAG* Indica o Grupo LAG a qual a porta pertence.
2. Não é aconselhado utilizar portas de 100M e 1000M em um mesmo Grupo LAG.
3. Não é possível modificar um Grupo LAG criado por LACP.

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, caso a porta seja membro de um grupo LAG ou se está configurada para um grupo de agregação dinâmica (LACP), a porta terá seu número exibido em cinza e não poderá ser selecionada.

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 ativado, o switch enviará pacotes contendo a identificação da agregação de link (ID) para o seu parceiro e outras informações como Prioridade, endereço MAC do switch e Chave Administrativa. Uma agregação de link dinâmica somente será realizada entre portas de switches com o mesmo ID de agregação de link.

É possível formar até oito 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 oito 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.

Nesta página você pode configurar a função LACP para o switch.

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

Prioridade da Agregação de Link Dinâmica (LACP)

Prioridade: 32768 (0 - 65535) Aplicar

Configuração LACP

Selecionar

Porta

Chave Admin.

Prioridade da Porta (0-65535)

Status

LAG

☐				Desabilitar	
☐	1	1	32768	Desabilitar	---
☐	2	1	32768	Desabilitar	---
☐	3	1	32768	Desabilitar	---
☐	4	1	32768	Desabilitar	---
☐	5	1	32768	Desabilitar	---
☐	6	1	32768	Desabilitar	---
☐	7	1	32768	Desabilitar	---
☐	8	1	32768	Desabilitar	---
☐	9	1	32768	Desabilitar	LAG1
☐	10	1	32768	Desabilitar	LAG1

Aplicar Ajuda

Obs.:

- 1. Para evitar tempestades de broadcast quando a função LACP estiver habilitada, Ative a função Spanning Tree.
- 2. A função LACP não pode ser habilitada em uma porta pertencente a um grupo de Agregação de Link Estático.

LACP (agregação de link dinâmica)

As seguintes informações são exibidas 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 constituem o ID de agregação. A agregação dinâmica somente será formada com grupos de agregação contendo o mesmo ID de agregação.

» **Configuração LACP**

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 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 de 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 dinâmica. 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.

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

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

5.3. Tráfego

No sub-menu *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:

Atualização Automática do Resumo do Tráfego

Atualização Automática:

☐ Habilitar ☒ Desabilitar

Aplicar

Atualizar:

seg (3-300)

Resumo do Tráfego

Porta

Selecionar

Porta	Pacotes Rx	Pacotes Tx	Bytes Rx	Bytes Tx	Estatísticas
1	30793	29122	4787531	11334473	Estatísticas
2	0	0	0	0	Estatísticas
3	0	0	0	0	Estatísticas
4	0	0	0	0	Estatísticas
5	0	0	0	0	Estatísticas
6	0	0	0	0	Estatísticas
7	697	672	389652	86973	Estatísticas
8	10379	1097	710486	124646	Estatísticas
9	0	0	0	0	Estatísticas
10	0	0	0	0	Estatísticas

Atualizar

Limpar

Ajuda

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 *Switching* → *Tráfego* → *Estatísticas por Porta* para carregar a seguinte página:

Atualização Automática:

☐ Habilitar ☒ Desabilitar

Aplicar

Atualizar:

seg (3-300)

Estatísticas				
		Porta	1	Selecionar
Recebidos		Enviados		
Broadcast	396	Broadcast	7	
Multicast	0	Multicast	449	
Unicast	30461	Unicast	28738	
Erros de Alinhamento	0	Colisões	0	
Pacotes < 64 Bytes	0			
Pacotes 64 Bytes	175			
Pacotes 65 a 127 Bytes	25121			
Pacotes 128 a 255 Bytes	105			
Pacotes 256 a 511 Bytes	3014			
Pacotes 512 a 1023 Bytes	2442			
Pacotes > 1023 Bytes	0			

Atualizar

Ajuda

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 sub-menu *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:

Opções de Pesquisa de Endereços MAC

☐ Endereço MAC:

(Formato: 00-00-00-00-00-01)

☐ VLAN ID:

(1-4094)

☐ Porta:

Porta 1

☐ Tipo:

☒ Todos

☐ Estático

☐ Dinâmico

☐ Filtrado

Pesquisar

Ajuda

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:

Configuração de Endereços MAC Estáticos

Endereço MAC: (Formato: 00-00-00-00-00-01)

VLAN ID: (1-4094)

Criar

Porta:

Pesquisar Endereços MAC Estáticos

Pesquisar por:

Pesquisar

Tabela de Endereços MAC Estáticos

Selecionar	Endereço MAC	VLAN ID	Porta	Tipo	Aging Time
☐			Porta 1		

Aplicar

Remover

Ajuda

Total de Endereços MAC: 0

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 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:

Configuração do Aging Time (Tempo de Envelhecimento)

Aging Time: ☒ Habilitar ☐ Desabilitar

Intervalo: seg (10-630, padrão: 300)

Aplicar

Pesquisar Endereços MAC Dinâmicos

Pesquisar por:

Pesquisar

Tabela de Endereços MAC Dinâmicos

Selecionar	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

Todos

Remover

Vincular

Ajuda

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:

Configuração de Filtro de Endereços MAC

Endereço MAC:

(Formato: 00-00-00-00-00-01)

VLAN ID:

(1-4094)

Criar

Pesquisar Endereços MAC Filtrados

Pesquisar por:

Todos

Pesquisar

Tabela de Filtro de Endereços MAC

Selecionar	Endereço MAC	VLAN ID	Porta	Tipo	Aging Time
Todos Remover Ajuda					

Total de Endereços MAC: 0

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.

Filtro de endereço MAC

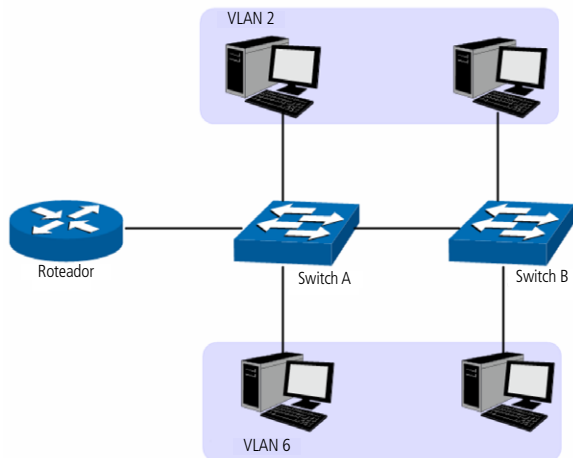
As seguintes informações são exibidas:

- » **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.*
- » *O recurso Filtro MAC não estará disponível se a função 802.1X estiver habilitada.*

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.

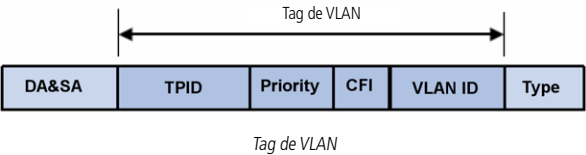
Este switch suporta três modos de classificação de VLAN: *802.1Q VLAN*, *MAC VLAN* e *Protocolo VLAN*.

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.



- 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 indentifica 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 três modos diferentes, a seguir a descrição de cada um dos modos:

- 1. **Acesso:** a porta em modo Acesso somente pode ser adicionada em uma única VLAN, e a regra de saída da porta é UNTAG. O PVID é o mesmo que o ID de VLAN atual. Se a VLAN atual é excluída, o PVID será definido como 1 por padrão.
- 2. **Trunk:** a porta em modo Trunk pode ser adicionada em várias VLANs, e a regra de saída da porta é TAG. O PVID pode ser definido como o número VID de qualquer VLAN que a porta pertença.
- 3. **Híbrida:** a porta em modo Híbrida pode ser adicionada em várias VLANs e estabelecer regras de saídas diferentes de acordo com as diferentes VLANs. A regra de saída padrão é UNTAG. O PVID pode ser definido como o número VID de qualquer VLAN a qual a porta pertence.

» **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.

- 1. 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.
- 2. 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 mostra como são tratados os pacotes.

Tipo de Porta	Recebendo pacotes		
	Pacotes UNTAG	Pacotes TAG	Enviando pacotes
Acesso		Se o VID do pacote é o mesmo que o PVID da porta, o pacote será recebido. Se o VID do pacote não for o mesmo que o PVID da porta, o pacote será descartado.	O pacote será enviado após retirar sua tag de VLAN.
Trunk	Quando pacotes untagged são recebidos, a porta irá adicionar a TAG padrão da porta, isto é, o PVID da porta de entrada.	Se o VID do pacote é permitido pela porta, o pacote será recebido. Se o VID do pacote é proibido pela porta, o pacote será descartado.	O pacote será enviado com a sua tag de VLAN atual.
Híbrido			Se a regra de saída da porta é TAG, o pacote será enviado com a sua tag de VLAN atual. Se a regra de saída da porta é UNTAG, o pacote será enviado após retirar sua tag de VLAN.

A função IEEE802.1Q VLAN pode ser configurada nas páginas *Configurar VLAN* e *Modo da Porta e PVID*.

Configurar VLAN

Nesta página você poderá configurar e visualizar as VLANs.
Escolha no menu *VLAN → 802.1Q VLAN → Configurar VLAN* para carregar a seguinte página.

Configuração de VLAN

Selecionar

VLAN ID

Descrição

Membros

Operação

☐

1

Default VLAN

1-10

Modificar | Detalhes

Criar

Todas

Remover

Ajuda

Total de VLAN: 1

Visualização das VLANs

Para garantir a comunicação com o switch, por padrão, a VLAN de Gerenciamento e todas as portas do switch estão configuradas na VLAN 1, sendo esta a única VLAN que não pode ser excluída.

As seguintes informações são exibidas na tela:

» Configuração de VLAN

- VLAN ID:** digite o VLAN ID desejado no campo correspondente e clique no botão *Selecionar* para selecionar a VLAN desejada.
- Selecionar:** selecione a VLAN desejada. É possível selecionar mais de uma VLAN simultaneamente.
- VLAN ID:** exibe o VLAN ID da VLAN (identificação da VLAN).
- Descrição:** exibe a descrição definida para a VLAN.
- Membros:** exibe as portas membros da VLAN criada.
- Operação:** permite visualizar ou modificar as configurações de cada VLAN.
 - » **Modificar:** clique em *Modificar* para alterar as configurações da VLAN desejada.
 - » **Detalhes:** clique em *Detalhes* para visualizar as informações da VLAN desejada.

Criar

Ao clicar no botão *Criar* ou *Modificar* será exibido a página de configuração de VLAN, conforme imagem a seguir.

Criar VLAN

VLAN ID:

(2-4094)

Verificar

Descrição:

(16 caracteres no máximo)

Membros da VLAN

Porta

Selecionar

Selecionar	Porta	Modo da Porta	Regra de Saída	LAG
☐	1	Acesso	UNTAG	---
☐	2	Acesso	UNTAG	---
☐	3	Acesso	UNTAG	---
☐	4	Acesso	UNTAG	---
☐	5	Acesso	UNTAG	---
☐	6	Acesso	UNTAG	---
☐	7	Acesso	UNTAG	---
☐	8	Acesso	UNTAG	---
☐	9	Acesso	UNTAG	---
☐	10	Acesso	UNTAG	---

Aplicar

Todos

Voltar

Ajuda

Obs.:

O Modo da Porta pode ser modificado na página 'Modo da Porta e PVID'.

Configuração de VLAN

As seguintes informações são exibidas na tela:

» Criar VLAN

VLAN ID: digite o ID de identificação da VLAN.

Descrição: digite uma descrição para a VLAN de no máximo 16 caracteres.

Verificar: clique no botão *Verificar* para certificar se o VLAN ID digitado é válido ou não.

» Membros da 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.

Porta: exibe o número de porta.

Modo da porta: exibe o modo de funcionamento da porta. Este campo é definido na página de configuração "Modo da Porta e PVID".

Regra de saída: exibe a regra de saída configurada para a porta. Se o modo de funcionamento da porta estiver configurado como Híbrido, será possível modificar esta opção.

» **TAG:** os pacotes transmitidos pela porta serão marcados (tagged – pacotes contendo informações de VLAN).

» **UNTAG:** os pacotes transmitidos pela porta não serão marcados (untagged).

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

Modo da porta e PVID

Nesta página é possível configurar e visualizar o modo de funcionamento das portas e seus respectivos PVID. Escolha no menu *VLAN → 802.1Q VLAN → Modo da Porta e PVID* para carregar a página seguinte:

Configurar o Modo e PVID da porta

Porta

Selecionar

Selecionar	Porta	Modo da Porta	PVID	LAG	VLAN
☐		Acesso			
☐	1	Acesso	1	---	Detalhes
☐	2	Acesso	1	---	Detalhes
☐	3	Acesso	1	---	Detalhes
☐	4	Acesso	1	---	Detalhes
☐	5	Acesso	1	---	Detalhes
☐	6	Acesso	1	---	Detalhes
☐	7	Acesso	1	---	Detalhes
☐	8	Acesso	1	---	Detalhes
☐	9	Acesso	1	---	Detalhes
☐	10	Acesso	1	---	Detalhes

Aplicar

Ajuda

Modo de funcionamento das portas

As seguintes informações são exibidas:

» Configurar o modo e PVID da porta

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.

Modo da porta: selecione o modo de funcionamento da porta.

- » **Acesso:** a porta em modo *Acesso* somente pode ser adicionada em uma única VLAN, e a regra de saída da porta é UNTAG. O PVID é o mesmo que o ID de VLAN. Se a VLAN atual é excluída, o PVID será definido como 1 por padrão.
- » **Trunk:** a porta em modo *Trunk* pode ser adicionada em várias VLANs, e a regra de saída da porta é TAG. O PVID pode ser definido como o número VID de qualquer VLAN que a porta pertença.
- » **Híbrida:** a porta em modo *Híbrida* pode ser adicionada em várias VLANs e estabelecer regras de saídas diferentes de acordo com as diferentes VLANs. A regra de saída padrão é UNTAG. O PVID pode ser definido como o número VID de qualquer VLAN a qual a porta pertença.

PVID: digite o PVID a qual a porta pertence.

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

VLAN: clique em *Detalhes* para exibir as informações da VLAN a qual a porta pertence.

Ao clicar em *Detalhes* serão exibidas as informações de VLAN da porta correspondente, conforme imagem a seguir:

VLAN da Porta 1

VLAN ID

Selecionar

VLAN ID	Descrição da VLAN	Operação
1	Default VLAN	Remover

Voltar

Ajuda

Obs.:

Total de VLAN da Porta 1: 1

Detalhes da VLAN (porta 1)

As seguintes informações são exibidas na tela:

» **VLAN da porta**

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

VLAN ID: exibe o VLAN ID da VLAN (identificação da VLAN).

Descrição da VLAN: exibe a descrição definida para a VLAN.

Operação: permite remover a porta da VLAN correspondente.

Procedimento de configuração

Passo	Operação	Descrição
1	Definir o modo de funcionamento da porta.	Obrigatório, no menu VLAN → 802.1Q VLAN → Modo da Porta e PVID, defina o modo de funcionamento da porta baseado no dispositivo conectado ao switch.
2	Criação da VLAN	Obrigatório, no menu VLAN → 802.1Q VLAN → Configurar VLAN, clique no botão <i>Criar</i> para configurar a VLAN. Digite a VLAN ID e a descrição para a VLAN e especifique as portas membros da VLAN.
3	Modificar/Visualizar a VLAN	Opcional, no menu VLAN → 802.1Q VLAN → Configurar VLAN, clique no botão <i>Modificar/Detalhes</i> para modificar ou visualizar as informações da VLAN correspondente.
4	Remover a VLAN	Opcional, no menu VLAN → 802.1Q VLAN → Configurar VLAN, selecione a VLAN que deseja excluir e clique no botão <i>Remover</i> .

6.2. MAC VLAN

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

Os pacotes do MAC VLAN são processados da seguinte maneira:

1. Ao receber um pacote untagged, o switch verifica se o endereço MAC do pacote possui uma entrada correspondente nas configurações de MAC VLAN. Se o endereço MAC corresponder, o switch adicionará a tag de VLAN no pacote de acordo com o VLAN ID do MAC VLAN configurado. Se o endereço MAC não corresponder, o switch adicionará a tag de VLAN no pacote de acordo com o PVID configurado para a porta. Assim o pacote será atribuído automaticamente para a VLAN correspondente.
2. Ao receber um pacote tagged, o switch irá processá-lo de acordo com as configurações 802.1Q VLAN. Se a porta que recebeu o pacote é membro da VLAN, o pacote será transmitido normalmente, caso contrário, o pacote será descartado.
3. Ao criar um MAC VLAN é necessário habilitar a porta para ser membro da VLAN 802.1Q correspondente, de modo a garantir que os pacotes sejam encaminhados normalmente.

Escolha no menu VLAN → MAC VLAN para carregar a seguinte página.

Configuração de MAC VLAN

Endereço MAC:

(Formato: 00-00-00-00-00-01)

Descrição:

(8 caracteres no máximo)

VLAN ID:

(1-4094)

Criar

Limpar

MAC VLAN

Endereço MAC

Selecionar

Selecionar

Endereço MAC

Descrição

VLAN ID

Operação

Nenhum MAC VLAN configurado.

Todos

Remover

Ajuda

Configuração MAC VLAN

Nesta página, você pode criar e visualizar as configurações de MAC VLAN.

As seguintes informações são exibidas na tela.

» **Configuração de MAC VLAN**

Endereço MAC: digite o endereço MAC do dispositivo participante do MAC VLAN. Utilize o formato: 00-00-00-00-00-01.

Descrição: digite uma descrição para a identificação do endereço MAC.

VLAN ID: digite a VLAN ID desejado para o MAC VLAN.

» **MAC VLAN**

Endereço MAC: digite o endereço MAC desejado no campo correspondente e clique no botão *Selecionar* para selecionar o MAC VLAN.

Selecionar: selecione o MAC VLAN desejado. É possível selecionar mais de uma entrada simultaneamente.

Endereço MAC: exibe o endereço MAC do dispositivo participante do MAC VLAN.

Descrição: exibe a descrição do MAC VLAN configurado.

VLAN ID: exibe o VLAN ID do endereço MAC corresponde.

Operação: clique em *Modificar*, para alterar as configurações, após realizado as modificações, clique no botão *Modificar* para aplicar as configurações.

Procedimento de configuração

Passos	Operação	Descrição
1	Definir o modo de funcionamento da porta.	Obrigatório, no menu VLAN → 802.1QVLAN → Modo da Porta e PVID, defina o modo de funcionamento da porta baseado no dispositivo conectado ao switch.
2	Criar a VLAN	Obrigatório, no menu VLAN → 802.1Q VLAN → Configurar VLAN, clique no botão Criar para configurar a VLAN. Digite o VLAN ID e a descrição para a VLAN e especifique as portas membros da VLAN.
3	Criar o MAC VLAN	Obrigatório, no menu VLAN → MAC VLAN, digite o endereço MAC do dispositivo, a descrição e o VLAN ID utilizado pelo MAC VLAN. Ao criar um MAC VLAN é necessário habilitar a porta para ser membro da VLAN 802.1Q correspondente, de modo a garantir que os pacotes sejam encaminhados normalmente.

6.3. Protocolo VLAN

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

» **Formato de encapsulamento dos dados ethernet**

Esta seção introduz a forma de encapsulamento comum dos dados Ethernet. Estes formatos são utilizados para a identificação de cada protocolo presente nos pacotes recebidos pelo switch.

Atualmente existem dois formatos de encapsulamento dos dados Ethernet. O encapsulamento Ethernet II e o encapsulamento 802.2/802.3, conforme imagem a seguir:

» Encapsulamento Ethernet II



» Encapsulamento 802.2/802.3



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

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

O encapsulamento 802.2/802.3 possui 3 possíveis formatos estendidos:

» Encapsulamento 802.3 Raw

DA&SA (12)	Length (2)	DATA
------------	------------	------

Apenas o campo Length é encapsulado após o campo DA/SA (endereço MAC de destino e origem) seguido pelo campo DATA sem qualquer outro campo. Atualmente apenas o protocolo IPX suporta encapsulamento 802.3 Raw. Os dois últimos bytes do campo Length é 0xFFFF

» Encapsulamento 802.2 LLC (Logic Link Control)

DA&SA (12)	Length (2)	DSAP (1)	SSAP (1)	Control (1)	DATA
------------	------------	----------	----------	-------------	------

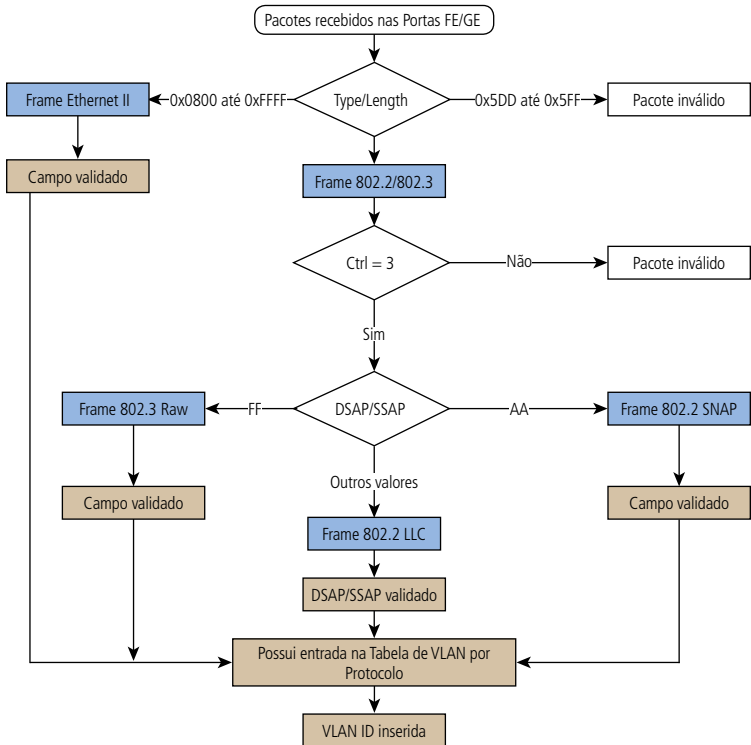
Apenas os campos Length, DSAP (Destination Service Access Point), SSAP (Source Service Access Point) e Control são encapsulados após o campo DA/SA (endereço MAC de destino e origem). O valor do campo Control é sempre 3. Os campos DSAP e SSAP do encapsulamento 802.2 LLC são utilizados para identificar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

» Encapsulamento 802.2 SNAP (Sub-Network Access Protocol)

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

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

» Procedimento de identificação do pacote pelo switch.



Identificação do encapsulamento ethernet

» Implementação da VLAN por protocolo

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

A seguinte tabela mostra os formatos comuns de encapsulamento suportados pelos protocolos de rede. O switch possui alguns modelos de protocolos pré-determinados, sendo possível adicionar outros modelos conforme sua necessidade.

Protocolo	Encapsulamento			
	Ethernet II	802.3 Raw	802.2 LLC	802.2 SNAP
IP (0x0800)	Suportado	Sem suporte	Sem suporte	Suportado
IPX (0x8137)	Suportado	Suportado	Suportado	Suportado
AppleTalk (0x809B)	Suportado	Sem suporte	Sem suporte	Suportado

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

1. Ao receber um pacote untagged, o switch verifica se o protocolo de rede do pacote possui uma entrada correspondente nas configurações de VLAN por Protocolo. Se o protocolo de rede corresponder, o switch adicionará a tag de VLAN no pacote de acordo com o VLAN ID da VLAN por Protocolo configurado. Se o protocolo de rede não corresponder, o switch adicionará a tag de VLAN no pacote de acordo com o PVID configurado para a porta. Assim o pacote é atribuído automaticamente para a VLAN correspondente.
2. Ao receber um pacote tagged, o switch irá processá-lo de acordo com as configurações 802.1Q VLAN. Se a porta que recebeu o pacote é membro da VLAN, o pacote será transmitido normalmente, caso contrário, o pacote será descartado.
3. Ao criar VLANs por Protocolo, é necessário habilitar a porta para ser membro da VLAN 802.1Q correspondente, de modo a garantir que os pacotes sejam encaminhados normalmente.

Criar VLAN por protocolo

Nesta página é possível criar VLANs por Protocolo clicando no botão *Criar* ou visualizar as configurações das atuais VLANs por Protocolos.

Escolha no menu *VLAN* → *Protocolo VLAN* → *Criar VLAN por Protocolo* para carregar a seguinte página.

Lista de VLANs por Protocolo				
Selecionar	Modelo de Protocolo	VLAN ID	Membros	Operação
Nenhuma VLAN por Protocolo configurada.				
<button>Criar</button><button>Todos</button><button>Remover</button><button>Ajuda</button>				

Tabela das VLANs por protocolo

As seguintes informações são exibidas.

» Lista de VLANs por protocolo

Selecionar: selecione a VLAN por Protocolo desejada. É possível selecionar mais de uma entrada simultaneamente.

Modelo de protocolo: exibe o nome do protocolo de rede configurado para a VLAN por Protocolo.

VLAN ID: exibe o VLAN ID (identificação de VLAN) correspondente ao protocolo de rede.

Membros: exibe as portas membros da VLAN por Protocolo.

Operação: clique em *Modificar* para alterar as configurações das VLANs por Protocolo. Após realizado as modificações, clique em *Aplicar* para validar as modificações.

VLAN por protocolo

Nesta página é possível criar VLANs por Protocolo de acordo com os protocolos pré-definidos pelo switch ou com os modelos de protocolos previamente configurados. O switch possui os seguintes modelos de protocolos por padrão: IP, ARP, RARP, IPX e AT.

Escolha no menu *VLAN → Protocolo VLAN → VLAN por Protocolo* para carregar a seguinte página.

Configurar VLAN por Protocolo

Modelo de Protocolo: IP (Ethernet II,0800)

VLAN ID: (1-4094)

Portas da VLAN por Protocolo

☐ 1	☐ 2	☐ 3	☐ 4	☐ 5	☐ 6
☐ 7	☐ 8	☐ 9	☐ 10		

Aplicar

Todos

Limpar

Ajuda

Criação de VLAN por protocolo

As seguintes informações são apresentadas na tela.

» Configurar VLAN por protocolo

Modelo de protocolo: selecione o protocolo de rede utilizado pela VLAN por Protocolo.

VLAN ID: digite a VLAN ID (identificação de VLAN) da VLAN por Protocolo.

» Portas da VLAN por protocolo

Selecione as portas habilitadas para a VLAN por Protocolo. Todas as portas estão desabilitadas por padrão. É possível selecionar mais de uma porta simultaneamente.

Modelos de protocolos

Esta página é utilizada para criar os modelos de protocolos desejados. Os modelos de protocolo devem ser criados antes de configurar a VLAN por Protocolo. O switch por padrão tem definidos os seguintes modelos de protocolos: IP, ARP, RARP, IPX, AT.

Escolha no menu *VLAN → Protocolo VLAN → Modelos de Protocolos* para carregar a seguinte página.

Configuração de Modelos de Protocolo

Modelo de Protocolo: (8 caracteres no máximo)

Protocolo: (4 caracteres hexadecimal)

Encapsulamento: Ethernet II

Criar

Modelos de Protocolos Configurados

Selecionar	ID	Modelo de Protocolo	Protocolo Ethernet	Encapsulamento
☐	1	IP	0800	Ethernet II
☐	2	ARP	0806	Ethernet II
☐	3	RARP	8035	Ethernet II
☐	4	IPX	8137	SNAP
☐	5	AT	809B	SNAP

Todos

Remover

Ajuda

Criação e visualização dos modelos de protocolos

As seguintes informações são exibidas na tela.

» Configuração de modelos de protocolo

Modelo de protocolo: digite o nome para o modelo de protocolo que será criado. Este campo deve possuir no máximo 8 caracteres.

Protocolo: digite a valor em hexadecimal referente ao tipo de protocolo de rede desejado.

Encapsulamento: selecione o tipo de encapsulamento utilizado pelo modelo de protocolo.

» **Modelos de protocolos configurados**

Selecionar: selecione o modelo de protocolo desejado. É possível selecionar mais de um modelo simultaneamente.

ID: exibe o índice do modelo de protocolo.

Modelo de protocolo: exibe o nome do modelo de protocolo criado.

Protocolo ethernet: exibe as informações do protocolo de rede utilizado pelo modelo.

Encapsulamento: exibe informações sobre o tipo de encapsulamento utilizado pelo quadro Ethernet.

Obs.: não é possível remover um modelo de protocolo quando este modelo está vinculado a uma VLAN.

Procedimento de configuração

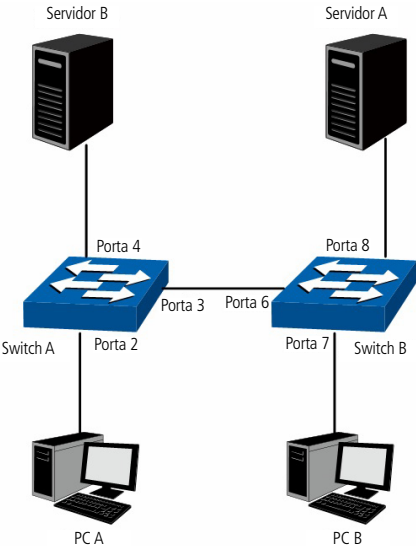
Passo	Operação	Descrição
1	Definir o modo de funcionamento da porta	Obrigatório, VLAN → 802.1Q VLAN → Modo da Porta e PVID, defina o modo de funcionamento da porta baseado no dispositivo conectado ao switch.
2	Criação da VLAN	Obrigatório, VLAN → 802.1Q VLAN → Configurar VLAN, clique no botão <i>Criar</i> para configurar a VLAN. Entre com a VLAN ID e a descrição para a VLAN.
3	Criação do Modelo de Protocolo	Obrigatório, VLAN → Protocolo VLAN → Modelos de Protocolos, Defina o Modelo de Protocolo antes de configurar a VLAN por Protocolo.
4	Criação da VLAN por Protocolo	Obrigatório, VLAN → Protocolo VLAN → VLAN por Protocolo, selecione o modelo de protocolo, a VLAN ID e as portas participantes da VLAN por Protocolo.
5	Modificação/Visualização da VLAN por Protocolo	Opcional, VLAN → Protocolo VLAN → Criar VLAN por Protocolo, clique em <i>Modificar</i> para alterar ou visualizar a VLAN por Protocolo correspondente.
6	Remover a VLAN por Protocolo	Opcional, VLAN → Protocolo VLAN → Criar VLAN por Protocolo, selecione a VLAN por Protocolo desejada e clique no botão <i>Remover</i> .

6.4. 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 → Modo da Porta e PVID, configurar o modo de funcionamento da porta 2, porta 3 e porta 4 como Acesso, Trunk e Acesso 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

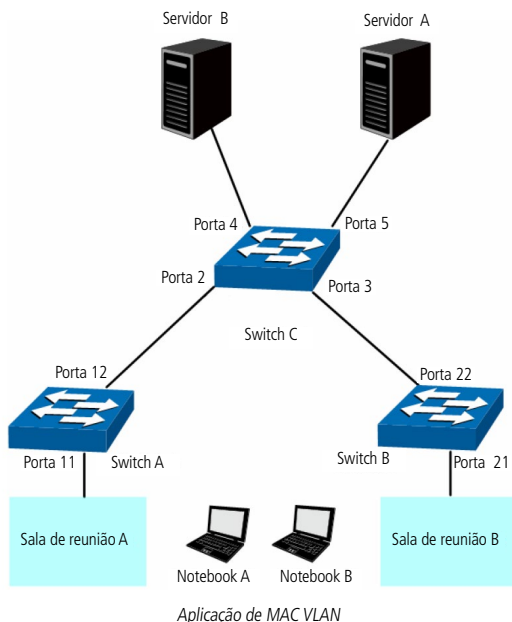
Passo	Operação	Descrição
1	Definir o modo de funcionamento da porta	Obrigatório, VLAN → 802.1Q VLAN → Modo da Porta e PVID, configurar o modo de funcionamento da porta 7, porta 6 e porta 8 como Acesso, Trunk e Acesso respectivamente.
2	Criar a VLAN 10	Obrigatório, VLAN → 802.1Q VLAN → Configurar VLAN, 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.

6.5. Exemplos de aplicação para MAC VLAN

» Requisitos de rede

- » O switch A e o switch B estão localizados respectivamente na sala de reunião A e B, estas salas são utilizadas por todos os departamentos.
- » O notebook A e o notebook B são utilizados em ambas as salas de reunião e apenas acessam seus respectivos servidores, A e B.
- » Os servidores A e B estão respectivamente na VLAN 10 e 20.
- » O endereço MAC do notebook A é 00-19-56-8A-4C-71 e do notebook B é 00-19-56-82-3B-70.

» Diagrama da rede



» Procedimento de configuração

» Configuração do switch A

Passo	Operação	Descrição
1	Definir o modo de funcionamento da porta	Obrigatório, VLAN → 802.1Q VLAN → Modo da Porta e PVID, configurar o modo de funcionamento das portas 11 e 12 como Híbrida e Trunk respectivamente.
2	Criar a VLAN 10	Obrigatório, VLAN → 802.1Q VLAN → Configurar VLAN, criar a VLAN com o VLANID 10 nas portas 11 e 12 e configurar a regra de saída da porta 11 como UNTAGGED.
3	Criar a VLAN 20	Obrigatório, VLAN → 802.1Q VLAN → Configurar VLAN, criar a VLAN com o VLANID 20 nas portas 11 e 12 e configurar a regra de saída da porta 11 como UNTAGGED.
4	Configurar MAC VLAN 10	Obrigatório, VLAN → MAC VLAN, criar o MAC VLAN 10 com o endereço MAC 00-19-56-8A-4C-71.
5	Configurar MAC VLAN 20	Obrigatório, VLAN → MAC VLAN, criar o MAC VLAN 20 com o endereço MAC 00-19-56-82-3B-70.

» Configuração do switch B

Passo	Operação	Descrição
1	Definir o modo de funcionamento da porta	Obrigatório, VLAN → 802.1Q VLAN → Modo da Porta e PVID, configurar o modo de funcionamento das portas 21 e 22 como Híbrida e Trunk respectivamente.
2	Criar a VLAN 10	Obrigatório, VLAN → 802.1Q VLAN → Configurar VLAN, criar a VLAN com o VLANID 10 nas portas 21 e 22 e configurar a regra de saída da porta 21 como UNTAGGED.
3	Criar a VLAN 20	Obrigatório, VLAN → 802.1Q VLAN → Configurar VLAN, criar a VLAN com o VLANID 20 nas portas 21 e 22 e configurar a regra de saída da porta 21 como UNTAGGED.
4	Configurar MAC VLAN 10	Obrigatório, VLAN → MAC VLAN, criar o MAC VLAN 10 com o endereço MAC 00-19-56-8A-4C-71.
5	Configurar MAC VLAN 20	Obrigatório, VLAN → MAC VLAN, criar o MAC VLAN 20 com o endereço MAC 00-19-56-82-3B-70.

» Configuração do switch C

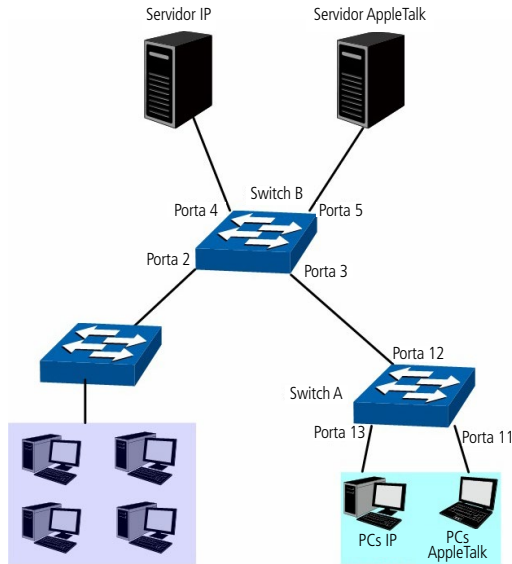
Passo	Operação	Descrição
1	Definir o modo de funcionamento da porta	Obrigatório, VLAN → 802.1Q VLAN → Modo da Porta e PVID, configurar o modo de funcionamento das portas 2 e 3 como Híbrida e as portas 4 e 5 como Acesso.
2	Criar a VLAN 10	Obrigatório, VLAN → 802.1Q VLAN → Configurar VLAN, criar a VLAN com o VLANID 10 nas portas 2 e 3 e 5.
3	Criar a VLAN 20	Obrigatório, VLAN → 802.1Q VLAN → Configurar VLAN, criar a VLAN com o VLANID 20 nas portas 2 e 3 e 4.

6.6. Exemplos de aplicação de VLAN por protocolo

» Requisitos da rede

- » O departamento A está conectado a rede da empresa pela porta 12 do switch A.
- » O departamento A possui computadores que utilizam o protocolo IP e AppleTalk.
- » Os computadores que utilizam o protocolo IP são membros da VLAN 10 e utilizam o servidor “Servidor IP”, enquanto os computadores que utilizam AppleTalk são membros da VLAN 20 e utilizam o servidor “Servidor AppleTalk”.
- » Os servidores “IP e AppleTalk” estão conectados ao switch B.

» Diagrama da rede



Aplicação de VLAN por protocolo

» Procedimento de configuração

» Configuração do switch A

Passo	Operação	Descrição
1	Definir o modo de funcionamento da porta	Obrigatório, VLAN→802.1Q VLAN→Modo da Porta e PVID, configurar o modo de funcionamento das portas 11 e 13 como Acesso, e da porta 12 como Híbrida.
2	Criar a VLAN 10	Obrigatório, VLAN→802.1Q VLAN→Configurar VLAN, criar a VLAN com o VLANID 10 nas portas 12 e 13 e configurar a regra de saída da porta 12 como UNTAGGED.
3	Criar a VLAN 20	Obrigatório, VLAN→802.1Q VLAN→Configurar VLAN, criar a VLAN com o VLANID 20 nas portas 11 e 12 e configurar a regra de saída da porta 12 como UNTAGGED.

» Configuração do switch B

Passo	Operação	Descrição
1	Definir o modo de funcionamento da porta	Obrigatório, VLAN→802.1Q VLAN→Modo da Porta e PVID, configurar o modo de funcionamento das portas 4 e 5 como Acesso, e da porta 3 como Híbrida.
2	Criar a VLAN 10	Obrigatório, VLAN→802.1Q VLAN→Configurar VLAN, criar a VLAN com o VLANID 10 nas portas 3 e 4 e configurar a regra de saída da porta 3 como UNTAGGED.
3	Criar a VLAN 20	Obrigatório, VLAN→802.1Q VLAN→Configurar VLAN, criar a VLAN com o VLANID 20 nas portas 3 e 5 e configurar a regra de saída da porta 3 como UNTAGGED.
4	Criação do modelo de protocolo	Obrigatório, VLAN → Protocolo VLAN → Modelos de Protocolos, criar os Modelos de Protocolos utilizados. Ex: pacotes que utilizam o protocolo de rede IP são encapsulados utilizando o formato Ethernet II e possuem o campo EtherType igual a 0800. Já os pacotes que utilizam o protocolo AppleTalk são encapsulados utilizando o formato 802.2 SNAP e possuem o PID (Protocol Identification) igual a 809B. Por padrão estes dois modelos de protocolos já estão definidos.
5	Criar a VLAN por Protocolo 10	Obrigatório, VLAN→Protocolo VLAN→VLAN por Protocolo, criar a VLAN por Protocolo com VLANID 10 para o protocolo de rede IP e selecionar a porta 3.
6	Criar a VLAN por Protocolo 20	Obrigatório, VLAN→Protocolo VLAN→VLAN por Protocolo, criar a VLAN por Protocolo com VLANID 20 para o protocolo de rede Apple Talk e selecionar a porta 3.

6.7. GVRP

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

» GARP

GARP fornece mecanismo de auxílio a switches membros de uma LAN a entregar, propagar e registrar as informações de atributos de registros entre os switches. A aplicação que utiliza GARP é chamada de implementação GARP e o GVRP é uma implementação GARP. Quando o GARP é implementado na porta do switch, a porta é chamada de entidade GARP. A troca de informações entre as entidades GARP é complementada por três tipos de mensagens: *Join*, *Leave* e *LeaveAll*.

- » **Mensagem Join:** uma entidade GARP envia mensagens Join para registrar seus atributos a outras entidades GARP, esta mensagem também pode ser enviada quando a entidade GARP recebe mensagens Join de outras entidades ou quando o registro de seus atributos são configurado manualmente.
- » **Mensagem Leave:** uma entidade GARP envia mensagens Leave para remover seus atributos registrados por outras entidades GARP, esta mensagem também pode ser enviada quando a entidade GARP recebe mensagens Leave de outras entidades ou quando os registros de seus atributos são removidos manualmente.
- » **Mensagem LeaveAll:** durante a inicialização, a entidade GARP inicia o timer LeaveAll, quando este timer expira é enviada uma mensagem LeaveAll para cancelar todos os seus atributos registrados a todas as entidades GARP participantes.

Através destas trocas de mensagens, todas as informações de registro dos atributos podem ser propagadas para todos os switches da mesma rede.

- » **Hold timer:** quando uma entidade GARP recebe partes de informações de registro de outras entidades, ele não envia imediatamente a mensagem Join. Para economizar recursos de largura de banda ele inicia um temporizador e armazena todas as informações de registro recebidas, após o término deste temporizador é enviado a mensagem de Join.
- » **Join timer:** para transmitir as mensagens Join de forma confiável, a entidade GARP envia duas vezes a mensagem *Join*. O Join Timer é o temporizador usado para definir o intervalo entre o envio das mensagens.
- » **Leave timer:** quando uma entidade GARP deseja remover informações de registro de um atributo, ele envia uma mensagem Leave. Quando a entidade GARP recebe essa mensagem, é iniciado um temporizador, caso nenhuma mensagem Join for recebida pela entidade até o temporizador expirar, o registro do atributo será removido da entidade GARP.
- » **LeaveAll timer:** durante a inicialização de uma entidade GARP, é iniciado o temporizador LeaveAll, após o término deste temporizador é enviado a mensagem LeaveAll, a fim de informar a todas as outras entidades GARP para que possam voltar a registrar as informações de atributos da entidade. Após esta etapa a entidade reinicia o LeaveAll Timer e começa um novo ciclo.

» GVRP

GVRP é uma implementação GARP que mantém o registro de informações dinâmicas de VLANs, podendo inclusive propagar estas informações para outros switches, adotando o mesmo mecanismo do GARP.

Depois que a função GVRP é habilitada, o switch recebe as informações de registro de VLAN de outros switches para atualizar dinamicamente suas informações de registro local de VLAN, incluindo os membros da VLAN e as portas através dos quais os membros de VLANs podem ser alcançados e assim por diante. O switch também propaga as informações de VLAN local para outros switches, até que todos os switches na mesma rede tenham as mesmas informações de VLANs. Informações sobre a inclusão, não inclui somente as informações de registro estático configurado localmente, mas também as informações de registro dinâmico recebido de outros switches.

Neste switch, somente a porta configurada como Trunk pode ser habilitada para o uso do GVRP. O switch possui os seguintes modos de registro de porta. *Normal*, *Fixo* e *Restrito*.

- » **Normal:** neste modo, a porta pode registrar ou remover dinamicamente uma VLAN, além de propagar as informações referente às VLANs dinâmicas e estáticas.
- » **Fixo:** neste modo, a porta não pode registrar ou remover dinamicamente uma VLAN, somente propaga informações referente às suas próprias VLANs configuradas manualmente.
- » **Restrito:** neste modo a porta não pode registrar ou remover VLANs, somente propaga informações da VLAN Padrão "VLAN 1".

Escolha o menu *VLAN* → *GVRP* para acessar a seguinte página:

Configuração GVRP

GVRP:

Habilitar

Desabilitar

Aplicar

Configuração das portas GVRP

Porta

Selecionar

Selecionar	Porta	Status	Modo de Registro	LeaveAll Timer (centesegundos)	Join Timer (centesegundos)	Leave Timer (centesegundos)	LAG
☐		Desabilitar	Normal				
☐	1	Desabilitar	Normal	1000	20	60	---
☐	2	Desabilitar	Normal	1000	20	60	---
☐	3	Desabilitar	Normal	1000	20	60	---
☐	4	Desabilitar	Normal	1000	20	60	---
☐	5	Desabilitar	Normal	1000	20	60	---
☐	6	Desabilitar	Normal	1000	20	60	---
☐	7	Desabilitar	Normal	1000	20	60	---
☐	8	Desabilitar	Normal	1000	20	60	---
☐	9	Desabilitar	Normal	1000	20	60	---
☐	10	Desabilitar	Normal	1000	20	60	---

Aplicar

Ajuda

Configuração GVRP

Obs.: se o recurso GVRP for habilitado em uma porta membro de um grupo LAG, por favor, certifique-se que todas as portas membros deste grupo LAG estejam com as mesmas configurações e modos de registro.

As seguintes informações são exibidas na tela:

» **Configuração GVRP**

GVRP: selecione *Habilitar/Desabilitar* para habilitar ou desabilitar a função GVRP no switch e clique em *Aplicar*.

» **Configuração das portas GVRP**

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 GVRP na porta desejada. O tipo de porta deve estar definido como Trunk para aceitar o recurso GVRP.

Modo de registro: selecione o modo de registro da porta.

» **Normal:** neste modo a porta pode registrar/remover dinamicamente uma VLAN e propagar as informações de VLANs dinâmicas e estáticas.

» **Fixo:** neste modo a porta não pode registrar/remover dinamicamente uma VLAN. Somente propaga as informações de VLANs estáticas.

» **Restrito:** neste modo a porta não pode registrar/remover VLANs. Somente propaga informações da VLAN 1.

LeaveAll timer: quando o LeaveAll Timer é definido, a porta com GVRP habilitado pode enviar uma mensagem LeaveAll após o término do temporizador, para que outras portas GARP possam registrar as informações de atributos. Após esta etapa, o temporizador LeaveAll é reiniciado, iniciando um novo ciclo. O temporizador LeaveAll varia de 1000 a 30000 centésimos de segundo.

Join timer: para garantir a transmissão, a porta GARP envia a mensagem Join duas vezes. O Join Timer é usado para definir o intervalo entre o envio das duas mensagens. O Join Timer pode estar na faixa de 20 a 1000 centésimos de segundo.

Leave timer: quando o Leave Timer for definido, a porta GARP ao receber uma mensagem de Leave iniciará o seu temporizador e removerá os atributos de informação caso não receba uma mensagem Join antes do temporizador terminar. O Leave Timer está na faixa de 60 a 3000 centésimos de segundos.

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

Obs.: LeaveAll Timer tem que ser ≥ 10 vezes o Leave Timer. Já o Leave Timer tem que ser ≥ 2 vezes o Join Timer.

Procedimento de configuração

Passo	Operação	Descrição
1	Configurar o modo de funcionamento da porta	Obrigatório, VLAN → 802.1Q VLAN → Modo da Porta e PVID, configurar o modo de funcionamento da porta como Trunk.
2	Habilitar a função GVRP	Obrigatório, VLAN → GVRP, habilitar a função GVRP.
3	Configurar o modo de registro e os tempos para porta.	Obrigatório, VLAN → GVRP, configurar os parâmetros da porta baseado nas aplicações atuais.

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.

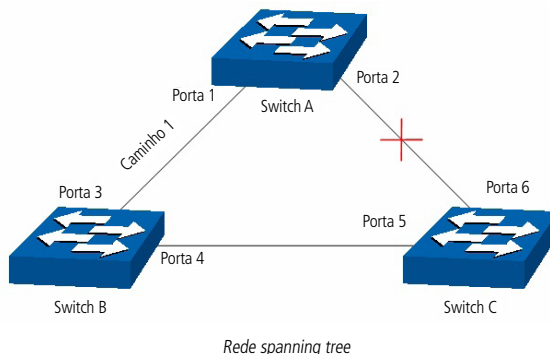
Porta designada: são todas as portas (Não-Raiz) que não são definidas como Portas Root e que ainda podem encaminhar tráfego na rede.

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 mostra 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.



» 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.

» Princípio de comparação de quadros BPDU

Supondo dois BPDUs: BPDUX e BPDUY.

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

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

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

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

» Convergência STP

» Iniciando

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

» Comparando BPDUs

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

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

» Selecionando a bridge root

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

» Selecionando a porta root e 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 BPDU 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 seu 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:

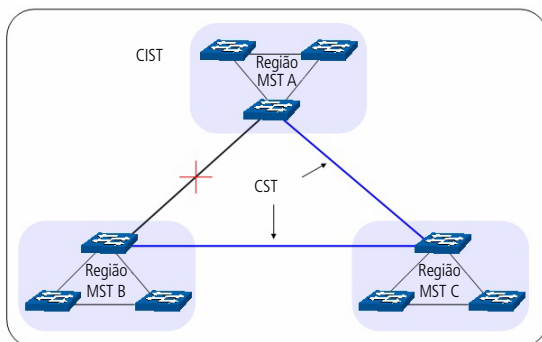


Diagrama de rede MSTP

» 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 BPDUs do MSTP transporta as informações de configuração MSTP dos switches.

» Estado das portas

No MSTP, as portas podem estar nos seguintes estados.

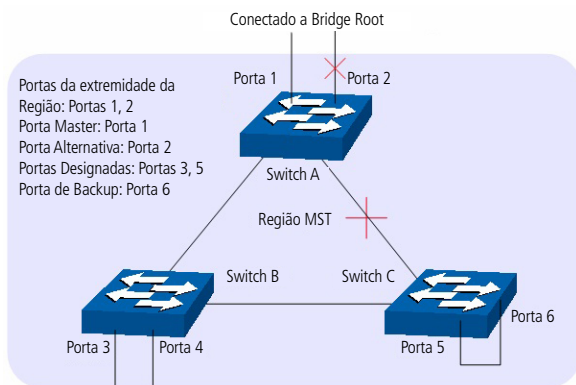
- » **Encaminhamento:** neste estado a porta pode enviar e receber dados da rede além de enviar e receber quadros BPDUs e aprender endereços MAC.
- » **Aprendizado:** neste estado a porta pode enviar e receber BPDUs e aprender endereços MAC.
- » **Bloqueado:** neste estado a porta somente pode receber 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 sub-menus de configuração: *Spanning Tree*, *Portas STP*, *Instâncias MSTP* e *Segurança STP*.

7.1. Spanning Tree

O sub-menu *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

STP:

☐ Habilitar ☒ Desabilitar

Aplicar

Versão:

STP

Parâmetros de Configuração

Prioridade CIST:

32768

(0-61440)

Hello Time:

2

seg (1-10)

Max Age:

20

seg (6-40)

Forward Delay:

15

seg (4-30)

TxHoldCount:

5

pps (1-20)

Limite de Saltos:

20

salto (1-40)

Aplicar

Ajuda

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 " $2 * (\text{Hello Time} + 1) \leq \text{Max Age}$ ". 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 " $2 * (\text{Forward Delay} - 1) \geq \text{Max Age}$ ". 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

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:

Configuração das Portas STP

Porta Selecionar

Selecionar	Porta	Status	Prioridade	Custo Caminho Externo	Custo Caminho Interno	Porta Edge	Link P2P	Checar Migração	Versão STP	Função da Porta	Status da Porta	LAG
☐	1	Desabilitar	128	Auto	Auto	Desabilitar	Auto	---	---	---	---	---
☐	2	Desabilitar	128	Auto	Auto	Desabilitar	Auto	---	---	---	---	---
☐	3	Desabilitar	128	Auto	Auto	Desabilitar	Auto	---	---	---	---	---
☐	4	Desabilitar	128	Auto	Auto	Desabilitar	Auto	---	---	---	---	---
☐	5	Desabilitar	128	Auto	Auto	Desabilitar	Auto	---	---	---	---	---
☐	6	Desabilitar	128	Auto	Auto	Desabilitar	Auto	---	---	---	---	---
☐	7	Desabilitar	128	Auto	Auto	Desabilitar	Auto	---	---	---	---	---
☐	8	Desabilitar	128	Auto	Auto	Desabilitar	Auto	---	---	---	---	---
☐	9	Desabilitar	128	Auto	Auto	Desabilitar	Auto	---	---	---	---	---
☐	10	Desabilitar	128	Auto	Auto	Desabilitar	Auto	---	---	---	---	---

AplicarAtualizarAjuda

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.

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:

Configuração de Região MST

Nome da Região:

Revisão:

(0-65535)

Aplicar

Ajuda

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

ID da Instância

Selecionar

Selecionar	Instância	Status	Prioridade	VLAN ID	
☐		Desabilitar			
☐	1	Desabilitar	32768		Limpar
☐	2	Desabilitar	32768		Limpar
☐	3	Desabilitar	32768		Limpar
☐	4	Desabilitar	32768		Limpar
☐	5	Desabilitar	32768		Limpar
☐	6	Desabilitar	32768		Limpar
☐	7	Desabilitar	32768		Limpar
☐	8	Desabilitar	32768		Limpar
	CIST	Habilitar	32768	1-4094,	

Aplicar

Ajuda

Mapeamento de VLAN dentro de Instância

VLAN ID:

(1-4094)

ID da Instância:

(0-8, 0 é a cist)

Aplicar

- Obs.:
- É possível adicionar mais de uma VLAN em uma Instância, para isto utilize o formato '1, 3, 4-7, 11-30' dentro do intervalo de 1 a 4094.
- 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.
- 67

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:

Configuração de Portas MST

ID da Instância

1

Porta

Selecionar

Selecionar	Porta	Prioridade	Custo do Caminho	função da Porta	Status da Porta	LAG
☐						
☐	1	128	Auto	---	---	---
☐	2	128	Auto	---	---	---
☐	3	128	Auto	---	---	---
☐	4	128	Auto	---	---	---
☐	5	128	Auto	---	---	---
☐	6	128	Auto	---	---	---
☐	7	128	Auto	---	---	---
☐	8	128	Auto	---	---	---
☐	9	128	Auto	---	---	---
☐	10	128	Auto	---	---	---

Aplicar

Atualizar

Ajuda

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 deseje 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 sub-menu 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:

Configuração de Proteção STP

Porta

Selecionar

Selecionar	Porta	Loop Protect	Root Protect	TC Protect	BPDU Protect	BPDU Filter	LAG
☐		Desabilitar	Desabilitar	Desabilitar	Desabilitar	Desabilitar	
☐	1	Desabilitar	Desabilitar	Desabilitar	Desabilitar	Desabilitar	---
☐	2	Desabilitar	Desabilitar	Desabilitar	Desabilitar	Desabilitar	---
☐	3	Desabilitar	Desabilitar	Desabilitar	Desabilitar	Desabilitar	---
☐	4	Desabilitar	Desabilitar	Desabilitar	Desabilitar	Desabilitar	---
☐	5	Desabilitar	Desabilitar	Desabilitar	Desabilitar	Desabilitar	---
☐	6	Desabilitar	Desabilitar	Desabilitar	Desabilitar	Desabilitar	---
☐	7	Desabilitar	Desabilitar	Desabilitar	Desabilitar	Desabilitar	---
☐	8	Desabilitar	Desabilitar	Desabilitar	Desabilitar	Desabilitar	---
☐	9	Desabilitar	Desabilitar	Desabilitar	Desabilitar	Desabilitar	---
☐	10	Desabilitar	Desabilitar	Desabilitar	Desabilitar	Desabilitar	---

Aplicar

Ajuda

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:

Configuração do Intervalo TC Protect

Limite de Pacotes TC: pacotes (1-100)

Ciclo TC Protect: seg (1-10)

Aplicar

Ajuda

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.

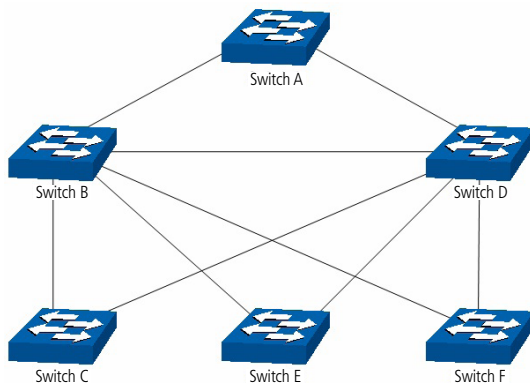
Ciclo TC protect: digite o tempo de duração de um ciclo TC Protect. O tempo varia de 1 a 10 segundos, o valor padrão é 5 segundos.

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.

» 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.

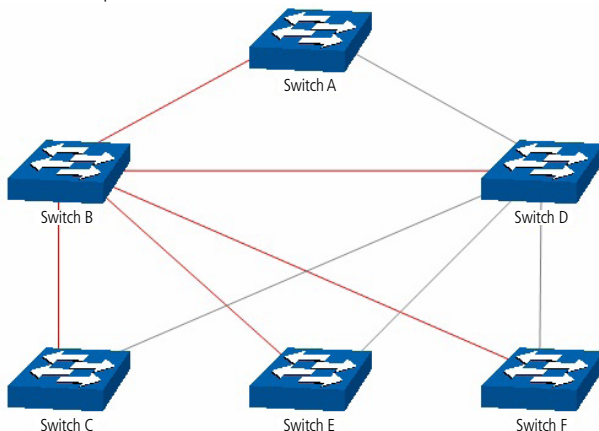


Diagrama da instância 1 após a convergência STP

» 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.

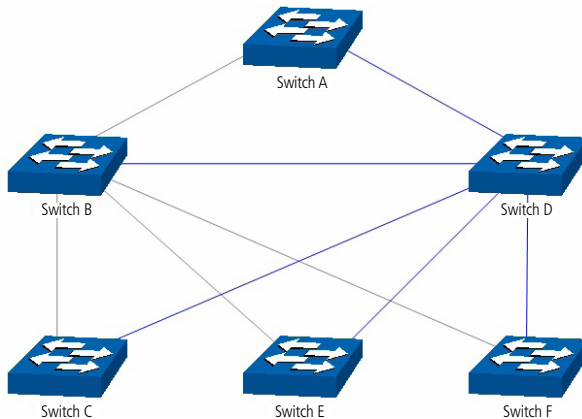


Diagrama da instância 2 após a convergência STP

» 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.

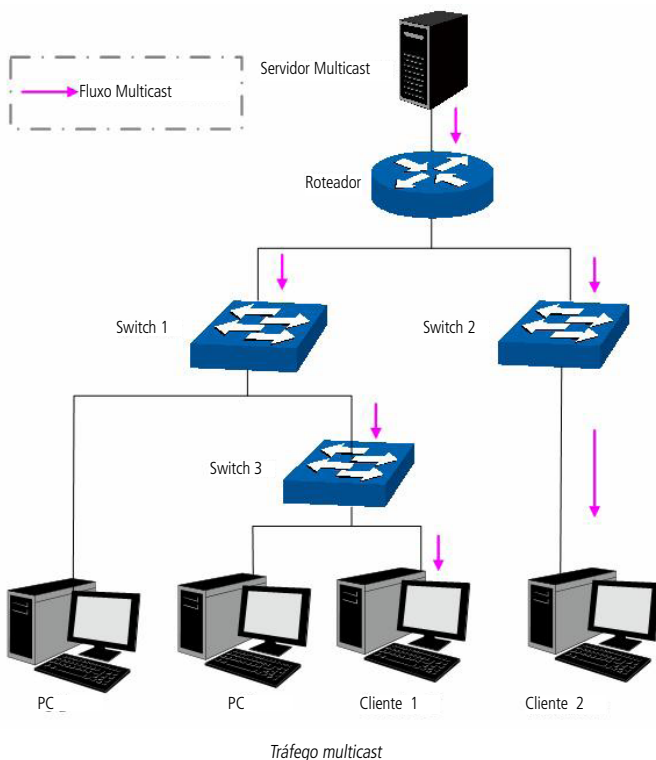
8. Multicast

» 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 protocolo o switch consegue identificar em qual porta o cliente está conectado para receber a transmissão Multicast, a partir desta identificação, o switch encaminha o tráfego Multicast apenas para as portas onde houver solicitante.

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



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:

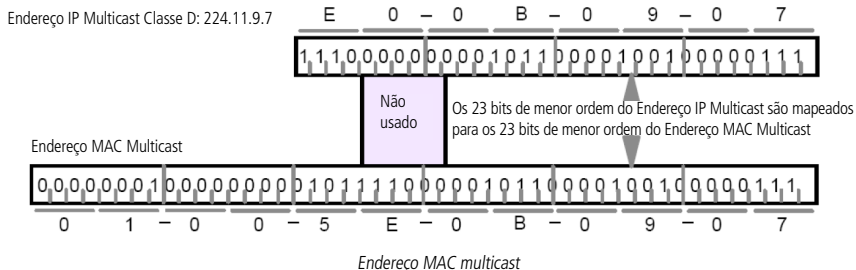
Conforme especificado pelo IANA (Internet Assigned Numbers Authority), os endereços Ips de classe D são usados como endereços Multicast. O intervalo de endereços Multicast vai de 224.0.0.0 a 239.255.255.255. A tabela a seguir exibe o intervalo e descrição de vários endereços Multicast especiais.

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. Enderecos 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 mostra a figura a seguir:



» Tabela de endereços multicast

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

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

VLAN ID	Multicast IP	Porta
---------	--------------	-------

Tabela de enderecos 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 sub-menus 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 específico para verificar se os outros clientes do grupo ainda necessitam das mensagens Multicast: se sim, o servidor Multicast receberá mensagem IGMP Report, se não, o servidor Multicast não receberá mensagens IGMP Report, portanto o switch removerá a porta específica da Tabela de endereços Multicast.

O servidor Multicast envia regularmente mensagens IGMP Query, após o envio destas mensagens, o switch irá remover a porta da Tabela de endereços Multicast, caso não escute nenhuma mensagem IGMP Report do cliente em um determinado período de tempo.

» Mensagens IGMP

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

1. IGMP Query (Consulta IGMP)

As mensagens IGMP Query (Consulta IGMP) enviadas pelo servidor Multicast podem ser classificadas de duas formas: IGMP General Query (Consulta Geral) ou Group-Specific-Query (Consulta a Grupo Específico). O servidor envia regularmente mensagens de consulta geral, para verificar se os grupos Multicast possuem membros. Ao receber mensagens IGMP Leave, o switch encaminhará as mensagens de consulta ao grupo Multicast específico enviadas pelo servidor Multicast para as portas pertencentes ao grupo, para verificar se outros membros do grupo ainda necessitam do serviço Multicast.

2. IGMP Report (Relatório IGMP)

As mensagens IGMP Report são enviadas pelos clientes quando desejam se associar (join) a um grupo Multicast ou responder as mensagens de consulta IGMP (IGMP Query) do servidor Multicast.

Ao receber uma mensagem IGMP Report, o switch encaminhará a mensagem de relatório através da porta denominada "Porta do Roteador" para o servidor Multicast, além de analisar a mensagem para obter o endereço do grupo Multicast que o cliente irá se juntar.

A porta de recepção do switch procederá da seguinte maneira: se a porta que o cliente está conectado no switch é um novo membro para um grupo Multicast, a porta será adicionada a Tabela de endereços Multicast, se a porta que o cliente está conectado já pertence ao grupo Multicast, o tempo de permanência da porta ao grupo Multicast 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 do IGMP Snooping

IGMP Snooping:

☐ Habilitar ☒ Desabilitar

Multicast Desconhecido:

☒ Encaminhar ☐ Descartar

Aplicar

Status do IGMP Snooping	
Descrição	Membros
Portas Habilitadas	
VLAN Habilitadas	

Atualizar

Ajuda

Obs.:

A função IGMP Snooping somente estará ativa quando as opções IGMP Snooping, Portas IGMP e VLAN estiverem configuradas.

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:

Configuração das Portas IGMP

Porta

Selecionar

Selecionar	Porta	IGMP Snooping	Fast Leave	LAG
☐		Desabilitar	Desabilitar	
☐	1	Desabilitar	Desabilitar	---
☐	2	Desabilitar	Desabilitar	---
☐	3	Desabilitar	Desabilitar	---
☐	4	Desabilitar	Desabilitar	---
☐	5	Desabilitar	Desabilitar	---
☐	6	Desabilitar	Desabilitar	---
☐	7	Desabilitar	Desabilitar	---
☐	8	Desabilitar	Desabilitar	---
☐	9	Desabilitar	Desabilitar	---
☐	10	Desabilitar	Desabilitar	---

Aplicar

Ajuda

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:

Configuração de VLANs para Grupos Multicast

VLAN ID:

(1-4094)

Porta do Roteador:

300

seg (60-600, recomendado: 300)

Portas Membro:

260

seg (60-600, recomendado: 260)

Leave Time:

1

seg (1-30, recomendado: 1)

Porta Estática:

Desabilitar

Criar

VLANs dos Grupos Multicast

VLAN ID

Selecionar

Selecionar	VLAN ID	Tempo limite da Porta do Roteador	Tempo limite das Portas Membro	Leave Time	Porta do Roteador
☐					

Aplicar

Remover

Ajuda

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.

Configuração da Multicast VLAN

Multicast VLAN:

☐ Habilitar ☒ Desabilitar

VLAN ID:

Porta do Roteador:

Aplicar

Portas Membro:

Ajuda

Leave Time:

Porta Estática:

Desabilitar

Obs.:

- 1. Todos os pacotes IGMP serão processados na Multicast VLAN quando criada.
- 2. É necessário configurar a VLAN desejada na página 802.1Q VLAN antes de configurar a Multicast VLAN.

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.

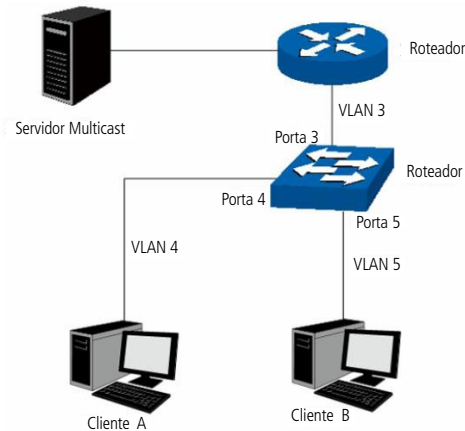
Switch: a porta 3 está conectada ao roteador e os pacotes são transmitidos na VLAN 3; a porta 4 é o cliente A e os pacotes são transmitidos na VLAN 4; a porta 5 está conectada ao cliente B e os pacotes são transmitidos na VLAN 5.

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 tráfego 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.

Pesquisar Endereços Multicast

☐ Endereço IP Multicast:

(Formato: 225.0.0.1)

☐ VLAN ID:

(1-4094)

☐ Porta:

1

▼

☐ Tipo:

☒ Todos

☐ Estático

☐ Dinâmico

Pesquisar

Tabela de Endereço IP Multicast

IP Multicast	VLAN ID	Porta de encaminhamento	Tipo
Atualizar Ajuda			

Total de IP Multicast: 0

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:

Configurar Endereços Multicast Estáticos

Endereço IP Multicast:

(Formato: 225.0.0.1)

VLAN ID:

(1-4094)

Porta:

(Formato: 1-3,6,8)

Criar

Pesquisar Endereços Multicast Estáticos

Opções:

Todos

Pesquisar

Tabela de Endereços Multicast Estático

Selecionar	IP Multicast	VLAN ID	Porta de encaminhamento

Todos

Remover

Ajuda

Total de IP Multicast Estático: 0

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 ao 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:

Configurar Faixa de Endereço IP Multicast

ID da Faixa Multicast:

(1-30)

IP Multicast inicial:

(Formato: 225.0.0.1)

IP Multicast final:

(Formato: 225.0.0.1)

Criar

Tabela de Faixas de Endereços Multicast

		ID da Faixa Multicast		Selecionar
Selecionar	ID da Faixa Multicast	IP Multicast inicial	IP Multicast final	
☐				

Aplicar

Remover

Ajuda

Total de Faixas de IP Multicast:0

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.

Configuração da Porta Filtrada

Porta

Selecionar

Selecionar	Porta	Filtrar	Ação	Vincular ID da Faixa Multicast	Qtd Grupos	LAG
☐		Desabilitar	Permitir			
☐	1	Desabilitar	Permitir	---	---	---
☐	2	Desabilitar	Permitir	---	---	---
☐	3	Desabilitar	Permitir	---	---	---
☐	4	Desabilitar	Permitir	---	---	---
☐	5	Desabilitar	Permitir	---	---	---
☐	6	Desabilitar	Permitir	---	---	---
☐	7	Desabilitar	Permitir	---	---	---
☐	8	Desabilitar	Permitir	---	---	---
☐	9	Desabilitar	Permitir	---	---	---
☐	10	Desabilitar	Permitir	---	---	---

Aplicar

Ajuda

- 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:

Configuração da Atualização Automática

Atualização Automática: ☐ Habilitar ☒ Desabilitar

Intervalo: seg (3-300)

Aplicar

Estatísticas IGMP

Porta

Selecionar

Porta	Pacotes Query	Pacotes Report (V1)	Pacotes Report (V2)	Pacotes Report (V3)	Pacotes Leave	Pacotes Error
1	0	0	0	0	0	0
2	0	0	0	0	0	0
3	0	0	0	0	0	0
4	0	0	0	0	0	0
5	0	0	0	0	0	0
6	0	0	0	0	0	0
7	0	0	0	0	0	0
8	0	0	0	0	0	0
9	0	0	0	0	0	0
10	0	0	0	0	0	0

AtualizarLimparAjuda

Estatísticas dos pacotes IGMP

As seguintes opções são exibidas na tela:

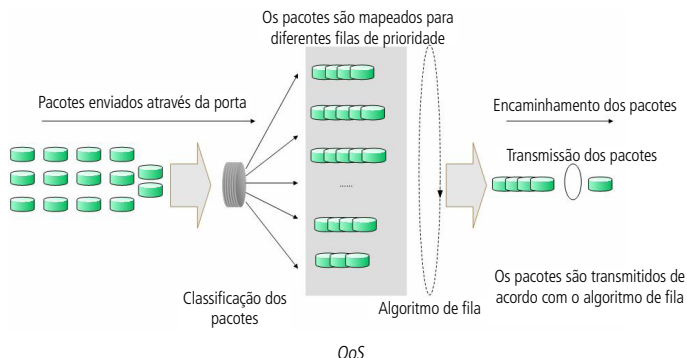
- » **Configuração da atualização automática**
 - Atualização automática:** selecione *Habilitar/Desabilitar* para habilitar ou desabilitar a função de atualização automática.
 - Intervalo:** digite um intervalo de 3 a 300 segundos, para especificar o período de atualização automática.
- » **Estatísticas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

» QoS

Este switch classifica e mapeia os pacotes entrantes e coloca-os em diferentes filas de prioridades, em seguida encaminha os pacotes de acordo com o algoritmo de fila selecionado, implementando a função de QoS.



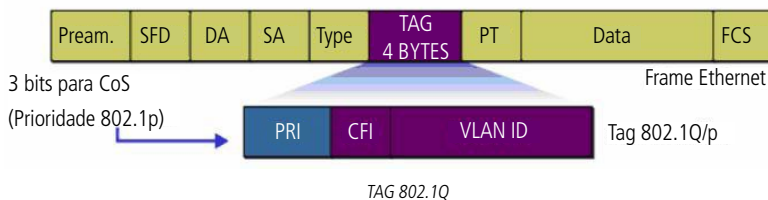
- » **Classificação de tráfego:** identifica pacotes em conformidades com determinadas regras.
- » **Mapeamento:** o usuário pode mapear os pacotes entrantes para filas de prioridades diferentes, com base nos modelos de prioridade. Este switch implementa três modelos de prioridades: *Prioridade por Porta*, *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

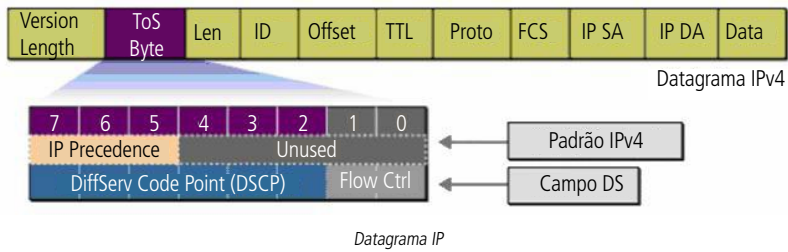
Neste modo de prioridade o fluxo de dados será mapeado para as filas de saída conforme a regra de CoS definido para cada porta.

2. Prioridade 802.1P



De acordo com a figura anterior, cada TAG 802.1Q inserida no quadro Ethernet possui um campo denominado *PRI*, este campo, possui 3 bits que são utilizados para a classificação e priorização do pacote, sendo possível configurar até 8 níveis de priorização (0 a 7). 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.

3. Prioridade DSCP

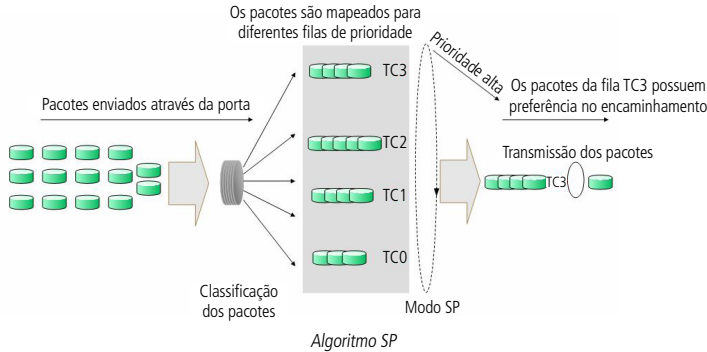


De acordo com a figura acima, o campo *ToS* (Type Of Service) do cabeçalho IP possui 1 byte, ou seja 8 bits. Os três primeiros bits indicam a Precedência IP e variam dentro do intervalo que vai de 0 a 7, os cinco bits restantes não são utilizados. A RFC 2474 redefiniu o campo *ToS* do datagrama IP, chamando-o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

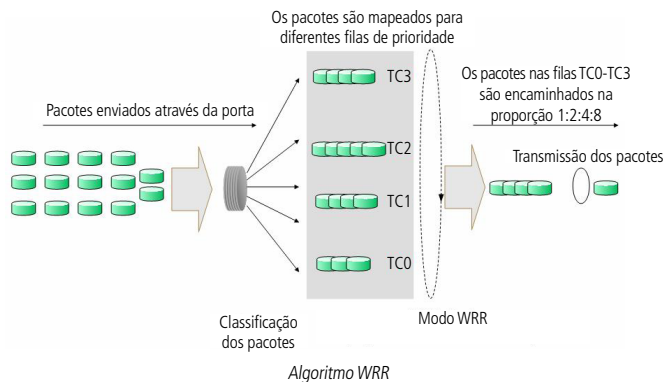
» Algoritmo de fila

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

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



2. *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.



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 sub-menus: *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*, *Algoritmo de Fila*, *Prioridade 802.1P* e *DSCP*.

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.

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:

Configuração do Algoritmo de Fila

Algoritmo de Fila:

SP+WRR

Aplicar

Ajuda

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 definidas 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.

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:

Configuração de Prioridade 802.1P

Prioridade:

Fila de Saída:

Prioridade	Fila de Saída	Prioridade	Fila de Saída
0	TC1	1	TC0
2	TC0	3	TC1
4	TC2	5	TC2
6	TC3	7	TC3

Aplicar

Ajuda

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 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 prioridade 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 prioridade (TC)	Obrigatório, QoS → DiffServ → Prioridade 802.1P, configure a relação de mapeamento entre a 802.1P e a fila de prioridade (TC).
2	Selecionar 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 → DiffeServ → Prioridade DSCP* para carregar a seguinte página:

Configuração de Prioridade DSCP

Prioridade DSCP: ☐ Habilitar ☒ Desabilitar Aplicar

Configuração de Prioridade

DSCP: Prioridade:

DSCP	Prioridade	DSCP	Prioridade
0	CoS0	1	CoS0
2	CoS0	3	CoS0
4	CoS0	5	CoS0
6	CoS0	7	CoS0
8	CoS1	9	CoS1
10	CoS1	11	CoS1
12	CoS1	13	CoS1
14	CoS1	15	CoS1
16	CoS2	17	CoS2
18	CoS2	19	CoS2

Aplicar Ajuda

Obs.:

Quando a Prioridade DSCP é configurada, os dados com marcação DSCP serão mapeados conforme a priorização CoS. A relação entre os valores de CoS com as filas de saídas (TC) são configuradas na página Prioridade 802.1P.

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 de prioridade

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

Prioridade: selecione a prioridade CoS. Os pacotes serão classificados com base no valor DSCP da porta de entrada e enviados para as filas de prioridade conforme relação de mapeamento configurado entre o CoS e o TC nas configurações 802.1P.

Procedimento de configuração

Passo	Operação	Descrição
1	Configure a relação de mapeamento entre o DSCP e 802.1P	Obrigatório, QoS → DiffServ→ Prioridade DSCP, habilitar a prioridade DSCP e configurar a relação de mapeamento entre a prioridade DSCP e 802.P
2	Configurar a relação de mapeamento entre 802.1P e a fila de prioridade (TC)	Obrigatório, QoS → DiffServ → Prioridade DSCP, configurar a relação de mapeamento entre a prioridade 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.

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.

Configuração de Limite de Banda

Porta

Selecionar

Selecionar	Porta	Entrada(Kbps)	Saída(Kbps)	LAG
☐		128	1024	
☐	1	---	---	---
☐	2	---	---	---
☐	3	---	---	---
☐	4	---	---	---
☐	5	---	---	---
☐	6	---	---	---
☐	7	---	---	---
☐	8	---	---	---
☐	9	---	---	---
☐	10	---	---	---

Aplicar

Ajuda

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.

Controle de tráfego

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:

Configuração de Storm Control						
					Porta	Selecionar
Selecionar	Porta	Taxa Broadcast(bps)	Taxa Multicast(bps)	Taxa UL-Frame(bps)	LAG	
☐		128K ▾	128K ▾	128K ▾		
☐	1	---	---	---	---	
☐	2	---	---	---	---	
☐	3	---	---	---	---	
☐	4	---	---	---	---	
☐	5	---	---	---	---	
☐	6	---	---	---	---	
☐	7	---	---	---	---	
☐	8	---	---	---	---	
☐	9	---	---	---	---	
☐	10	---	---	---	---	

Obs.:

Não é possível configurar o Storm Control e o Limite de Banda entrante em uma mesma porta.

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.

Taxa broadcast (bps): selecione a largura de banda de recebimento de pacotes de broadcast na porta. O tráfego de pacotes superior a largura de banda serão descartados. Selecione *Desabilitar* para desativar a função de Storm Control para a porta.

Taxa multicast (bps): selecione a largura de banda de recebimento de pacotes de Multicast na porta. O tráfego de pacotes superior a largura de banda serão descartados. Selecione *Desabilitar* para desativar a função de Storm Control para a porta.

Taxa UL-frame (bps): selecione a largura de banda de recebimento de pacotes de UL-Frames na porta. O tráfego de pacotes superior a largura de banda serão descartados. Selecione *Desabilitar* para desativar a função de Storm Control para a porta.

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 corresponde a algum OUI configurado no sistema, os pacotes serão determinados 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, mostra os endereços OUI de vários fabricantes que já estão pré-definidos no switch.

Number	Endereço OUI	Fabricante
1	00-01-E3-00-00-00	Siemens Phone
2	00-03-6B-00-00-00	Cisco Phone
3	00-04-0D-00-00-00	Avaya Phone
4	00-60-B9-00-00-00	Philips/NEC Phone
5	00-D0-1E-00-00-00	Pingtel Phone
6	00-E0-75-00-00-00	Polycom Phone
7	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 do pacote e determina a prioridade dos pacotes enviados não marcados (untagged).

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 adicionados ou removidos na VLAN de Voz.

Manual: neste modo, será 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 partir de um dispositivo de voz e do modo de funcionamento da porta. A tabela a seguir mostra informações detalhadas.

Modo da porta	Tipo dos dados de voz	Modo de funcionamento e processamento da porta
Automático	Pacotes de voz TAG	Acesso: não suportado.
		Trunk: suportado, a VLAN padrão da porta não pode ser a Voice VLAN.
	Pacotes de voz UNTAG	Híbrida: suportado, a VLAN padrão da porta não pode ser a Voice VLAN e a regra de saída na porta de acesso da Voice VLAN deverá ser TAG.
		Acesso: suportado.
Manual	Pacotes de voz TAG	Trunk: não suportado.
		Híbrida: suportado, a VLAN padrão da porta não pode ser a Voice VLAN e a regra de saída na porta de acesso da Voice VLAN deverá ser UNTAG.
	Pacotes de voz UNTAG	Acesso: não suportado.
		Trunk: suportado, a VLAN padrão da porta não pode ser a Voice VLAN.
	Pacotes de voz TAG	Híbrida: suportado, a VLAN padrão da porta não pode ser a Voice VLAN e a regra de saída na porta de acesso da Voice VLAN deverá ser TAG.
		Acesso: suportado.
	Pacotes de voz UNTAG	Trunk: não suportado.
		Híbrida: suportado, a VLAN padrão da porta não pode ser a Voice VLAN e a regra de saída na porta de acesso da Voice VLAN deverá ser UNTAG.

» Modo de segurança das portas voice VLAN

Quando a Voice VLAN estiver habilitada para uma porta, você pode habilitar a opção Modo de Segurança da porta, para filtrar fluxos de dados.

Se 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,
	Pacotes de voz TAG	o pacote poderá ser transmitido na Voice VLAN. Caso contrário, o pacote será descartado.
	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
	Pacotes de voz TAG	transmitidos na Voice VLAN.
	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 Voice VLAN pode ser configurada em *Voice VLAN*, *Configurar Portas e Endereços OUI*.

Voice VLAN

Nesta página é possível configurar os parâmetros globais da Voice VLAN como por exemplo o VLAN ID, Aging Time (tempo de envelhecimento) e a prioridade de transmissão dos pacotes de voz.

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

Configurar Voice VLAN

Voice VLAN:	☐ Habilitar ☒ Desabilitar	
VLAN ID:		(2-4094)
Aging Time:	1440	min (1-43200, padrão: 1440)
Prioridade:	6	

Aplicar

Ajuda

Configuração da voice VLAN

As seguintes informações são apresentadas na tela:

» Configurar voice VLAN

Voice VLAN: selecione *Habilitar/Desabilitar* para 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.

Prioridade: selecione a prioridade de transmissão dos pacotes de voz na Voice VLAN.

Configurar portas

Nesta página é possível configurar os parâmetros das portas participantes da Voice VLAN.
Escolha no menu *QoS* → *Voice VLAN* → *Configurar Portas* para carregar a seguinte página:

Configurar Portas Voice VLAN

Porta

Selecionar

Selecionar	Porta	Modo da Porta	Modo de Segurança	Estado	LAG
☐					
☐	1	Auto	Desabilitar	Inativa	---
☐	2	Auto	Desabilitar	Inativa	---
☐	3	Auto	Desabilitar	Inativa	---
☐	4	Auto	Desabilitar	Inativa	---
☐	5	Auto	Desabilitar	Inativa	---
☐	6	Auto	Desabilitar	Inativa	---
☐	7	Auto	Desabilitar	Inativa	---
☐	8	Auto	Desabilitar	Inativa	---
☐	9	Auto	Desabilitar	Inativa	---
☐	10	Auto	Desabilitar	Inativa	---

Aplicar

Ajuda

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. 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:

Criar Endereço OUI

Endereço OUI: (Formato: 00-00-00-00-00-01)

Máscara: FF-FF-FF-00-00-00 (Padrão: FF-FF-FF-00-00-00)

Descrição: (16 caracteres no máximo)

Endereços OUI configurados

Selecionar	Endereço OUI	Máscara	Descrição
☐	00-01-e3-00-00-00	ff-ff-ff-00-00-00	Siemens Phone
☐	00-03-6b-00-00-00	ff-ff-ff-00-00-00	Cisco Phone
☐	00-04-0d-00-00-00	ff-ff-ff-00-00-00	Avaya Phone
☐	00-60-b9-00-00-00	ff-ff-ff-00-00-00	Philips Phone
☐	00-d0-1e-00-00-00	ff-ff-ff-00-00-00	Pingtel Phone
☐	00-e0-75-00-00-00	ff-ff-ff-00-00-00	PolyCom Phone
☐	00-e0-bb-00-00-00	ff-ff-ff-00-00-00	3Com Phone

Configuração OUI

» 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*.

Endereço 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 → Modo da Porta e PVID, defina o modo de funcionamento das portas que serão usadas com o dispositivos de voz.
2	Criar VLAN	Obrigatório. VLAN → 802.1Q VLAN → Configurar VLAN, clique no botão <i>Criar</i> para criar a VLAN.
3	Adicionar o endereço OUI	Opcional. Em QoS → Voice VLAN → Endereços OUI, verificar se o switch possui cadastrado o endereço OUI do seu dispositivo de voz. Caso não possua adicione esse endereço.
4	Configurar os parâmetros de portas para a Voice VLAN	Obrigatório. Em QoS → Voice VLAN → Configurar Portas, configurar os parâmetros da porta na Voice VLAN
5	Habilitar a Voice VLAN	Obrigatório. Em QoS → Voice VLAN → Voice VLAN, configurar 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 encontrados em protocolos utilizados entre as camadas 2-4 do modelo de referência OSI.

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

O menu ACL possui 4 sub-menus de configuração: *Agendamentos*, *Configurar ACL*, *Políticas ACL* e *Vínculos ACL*.

10.1. Agendamentos

Uma ACL baseada em intervalo de tempo permite controlar o tráfego em uma data ou hora específica. Cada regra ACL pode possuir um intervalo de tempo e este intervalo é baseado na data e hora configurado no switch.

Os intervalos de tempo podem ser configurados das seguintes formas:

Períodos, intervalo de dias da semana e feriados.

A configuração do intervalo de tempo pode ser configurado no sub-menu *Agendamentos*, através das seguintes páginas de configuração: *Agendamentos*, *Criar Agendamento* e *Feridos*.

Agendamentos

Nesta página você pode visualizar os agendamentos configurados.

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

Agendamentos configurados								
Selecionar	Índice	Agendamento	Intervalo 1	Intervalo 2	Intervalo 3	Intervalo 4	Modo	Operação
			Todos	Remover	Ajuda			

Agendamentos de ACL

As seguintes informações são exibidas na tela:

» **Agendamentos configurados**

Selecionar: selecione o agendamento desejado.

Índice: exibe o índice do agendamento.

Agendamento: exibe o nome do agendamento.

Intervalo: exibe o intervalo de tempo do agendamento.

Modo: exibe o modo de funcionamento do agendamento.

Operação: clique no botão *Modificar* para alterar as configurações do agendamento desejado ou clique em *Detalhes* para exibir as informações do agendamento.

Criar agendamento

Nesta página você pode criar os agendamentos.

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

Configurar Agendamento

Nome:

☐ Feriado

☐ Período

☐ Semana

Data inicial: / /

Data final: / /

☐ Seg ☐ Ter ☐ Qua ☐ Qui ☐ Sex ☐ Sab ☐ Dom

Configurar Intervalos de Tempo

Horário inicial: :

Horário final: :

Criar

Intervalos de Tempo configurado

Índice	Horário inicial	Horário final	Remover
Aplicar Ajuda			

Configuração do intervalo de tempo

Obs.: para configurar com êxito o agendamento, por favor, em primeiro lugar especifique os intervalos de tempo.

As seguintes opções são apresentadas na tela:

» Configurar agendamento

Nome: digite o nome para o agendamento.

Feriado: selecione *Feriado* para configurar o agendamento conforme feriado previamente configurado no switch. A regra de ACL baseada neste agendamento terá efeito apenas quando a data/hora do switch estiver dentro do intervalo configurado para o feriado.

Período: selecione *Período* para configurar o agendamento em um determinado período de tempo. A regra de ACL baseada neste agendamento terá efeito apenas quando data/hora do switch estiver dentro do período de tempo configurado.

Semana: selecione *Semana* para configurar o agendamento em um intervalo de dias de semana. A regra de ACL baseada neste agendamento, terá efeito apenas quando a data/hora do switch estiver dentro da faixa de dias da semana configurado.

» Configurar intervalos de tempo

Horário inicial: define o horário de início do intervalo de tempo.

Horário final: define o horário de término do intervalo de tempo.

» Intervalos de tempo configurado

Índice: exibe o índice do intervalo de tempo.

Horário inicial: exibe o horário de início do intervalo de tempo.

Horário final: exibe o horário de término do intervalo de tempo.

Remover: clique no botão *Remover* para excluir o intervalo de tempo correspondente.

Feriados

Nesta página é possível configurar os feriados em que regra de ACL será aplicada, conforme sua necessidade. Escolha no menu *ACL → Agendamentos → Feriados* para carregar a página:

Configuração de Feriados

Data inicial:

01

/

01

Data final:

01

/

01

Nome do feriado:

Criar

Feriados configurados

Selecionar	Índice	Nome do feriado	Data inicial	Data final
TodosRemoverAjuda				

Configuração de feriados

As seguintes opções são exibidas na tela:

- » **Configuração de feriados**
 - Data inicial:** selecione a data de início do feriado.
 - Data final:** selecione a data de término do feriado.
 - Nome do feriado:** digite o nome do feriado.
- » **Feriados configurados**
 - Selecionar:** selecione o feriado desejado. Para remover a entrada criada, clique no botão *Remover*.
 - Índice:** exibe o índice do feriado.
 - Nome do feriado:** exibe o nome do feriado.
 - Data inicial:** exibe o início do feriado.
 - Data final:** exibe o final do feriado.

10.2. Configurar ACL

Cada ACL pode conter uma série de regras e cada regra pode especificar um intervalo de tempo diferente. Os pacotes são combinados em ordem. Uma vez que uma regra é correspondida o switch processa os pacotes de acordo com as regras criadas. Sem levar em conta as demais regras, otimizando o desempenho do switch.

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:

Pesquisar ACLs configuradas

ID da ACL:

Tipo da ACL:

Ordem da Regra:

Remover

Regras configuradas

TodasRemoverAjuda

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:

Configuração de ACLs

ID da ACL:		0-99 MAC ACL
		100-199 ACL Padrão
		200-299 ACL Estendida
Ordem da Regra:	Ordem Usuário	
	Criar	Ajuda

Criação da ACL

As seguintes informações são apresentadas na tela:

» **Configuração de ACLs**

ID da ACL: 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 classificadas 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, VLAN ID e protocolo de rede.

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

Configuração de Regras MAC ACLs

ID da ACL:	MAC ACL	
Regra:		
Operação:	Permitir	
☐ MAC de Origem:		Máscara:
☐ MAC de Destino:		Máscara:
☐ VLAN ID:		
☐ Protocolo:		(4 caracteres hexadecimais)
Prioridade:	Nenhum	
Agendamento:	Nenhum	
	Criar	Ajuda

MAC ACL

» 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.

VLAN ID: digite a VLAN ID utilizada pela regra.

Protocolo: digite o protocolo de rede utilizado pela regra.

Prioridade: selecione a prioridade (tag) contida no pacote utilizada pela regra.

Agendamento: selecione o agendamento para que a regra tenha efeito.

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:

Configuração de Regras ACL Padrão

ID da ACL:	ACL Padrão	
Regra:		
Operação:	Permitir	
☐ IP de Origem:		Máscara de rede:
☐ IP de Destino:		Máscara de rede:
Agendamento:	Nenhum	
Criar Ajuda		

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.

Agendamento: selecione o agendamento para que a regra tenha efeito.

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, Flags TCP, portas de origem e destino.

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

Configuração de Regras ACL Estendida

ID da ACL:	ACL Estendida ▼	
Regra:		
Operação:	Permitir ▼	
☐ IP de Origem:		Máscara de rede:
☐ IP de Destino:		Máscara de rede:
Protocolo de Rede:	Todos ▼	
Flag TCP:	URG * ▼ ACK * ▼ PSH * ▼ RST * ▼ SYN * ▼ FIN * ▼	
☐ Porta de Origem:		
☐ Porta de Destino:		
DSCP:	Todos ▼	
Tipo de Serviço IP:	Todos ▼	Precedência IP: Todos ▼
Agendamento:	Nenhum ▼	
Criar Ajuda		

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.

Flag TCP: configure as flags TCP, quando o protocolo TCP for selecionado na lista.

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.

DSCP: selecione o valor DSCP contido no pacote utilizado pela regra.

Tipo de serviço IP: selecione o Tipo de Serviço contido no pacote utilizado pela regra.

Precedência IP: selecione a Precedência IP contida no pacote utilizado pela regra.

Agendamento: selecione o Agendamento para que a regra tenha efeito.

10.3. Políticas ACL

O sub-menu *Políticas ACL* é utilizado para controlar os pacotes que cumpram as regras ACLs correspondentes, configurando ações para um conjunto de ACLs. Estas ações incluem *Espelhar para*, *Condição* e *Redirecionar*, entre outros. A Política ACL pode ser configurada nas seguintes páginas: *Políticas*, *Criar Políticas* e *Criar Ação*.

Políticas

Nesta página é possível visualizar as ações criada na política de ACL para uma determinada regra de ACL. Escolha o menu *ACL* → *Políticas ACL* → *Políticas* para carregar a página seguinte:

Políticas ACL

Selecione a Política:

Remover

Ações Configuradas

Selecionar	Índice	ID da ACL	Espelhar para	Condição	Redirecionar	Marcação QoS	Operação
TodasRemoverAjuda							

Políticas de ACL

- » **Políticas ACL**
Selecione a política: selecione o nome da politica 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.
Espelhar para: exibe a porta que irá receber o fluxo de dados que corresponderem com a política.
Condição: exibe a condição acrescentado à política.
Redirecionar: exibe o redirecionamento adicionado a política.
Marcação QoS: exibe a marcação QoS adicionada a política.
Operação: clique no botão *Modificar* para alterar a política desejada. Após realizado 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:

Configuração de Políticas ACL

Nome da Política:

Criar

Ajuda

Criação de políticas ACLs

- As seguinte opções 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, atrelando a política a uma determinada regra de ACL configurada.

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

Configuração de Ação ACL

Selecione a Política:

Política

Selecione a ACL:

ACL

☐ Espelhar para

Porta:

Porta 1

☐ Condição

Taxa:

Kbps(1-1000000)

Se exceder taxa:

Manter

☐ Redirecionar

Porta de destino:

Porta 1

☐ Marcação QoS

DSCP:

Nenhum

Fila de Prioridade:

Padrão

Criar

Ajuda

Ação da política de ACL

As seguintes opções 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 atrelada a política de ACL.

Espelhar para: selecione a porta que irá receber o fluxo dos dados espelhados que corresponderem com a Política de ACL criada.

Condição: selecione a taxa de transmissão dos pacotes de dados na política.

» **Taxa:** especifique a taxa de transmissão dos pacotes de dados a coincidirem com a ACL correspondente.

» **Se exceder taxa:** especifique se haverá descarte dos pacotes que são transmitidos além da taxa estipulada.

Redirecionar: selecione a porta que receberá o fluxo dos dados que correspondam com a Política de ACL.

Marcação QoS: selecione a *Marcação QoS* que será adicionada aos pacotes que corresponderem com a Política de ACL.

» **DSCP:** selecione a marcação DSCP adicionada aos pacotes que coincidam com as Políticas de ACL configuradas.

» **Fila de prioridade:** selecione a fila de prioridade dos pacotes a coincidir com a ACL desejada.

10.4. Vínculos ACL

A função *Vínculos ACL* é utilizada para atrelar a política criada a uma porta do switch ou a uma VLAN específica, isto é, a política criada somente 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:

Exibir Vínculos

Mostrar Vínculos:

Todos

Selecionar	Índice	Nome da Política	Interface	Direção
------------	--------	------------------	-----------	---------

Todos

Remover

Ajuda

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 exclui-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:

Configuração de Vínculo por Porta

Política ACL:

Selecione

Vincular

Porta:

(Formato:1-3,6,8)

Ajuda

Vínculos por Porta configurados

Índice	Política ACL	Porta	Direção
--------	--------------	-------	---------

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:

Configuração de Vínculos por VLAN

Política ACL:

Selecione

Vincular

VLAN ID:

(Formato:2-10,100)

Ajuda

Vínculos por VLAN configurados

Índice	Política ACL	VLAN ID	Direção
--------	--------------	---------	---------

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 a 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 a VLAN ID vinculada a Política de ACL.
 - Direção:** exibe a direção do vínculo.

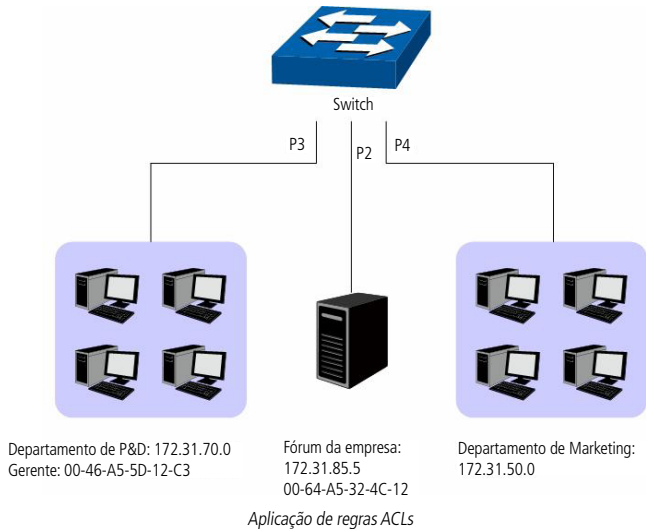
Procedimento de configuração

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.

10.5. 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



» Procedimento de configuração

Passo	Operação	Descrição
1	Configuração do Agendamento	Em ACL → Agendamentos → Criar Agendamento, configurar o nome do agendamento como expediente. Selecione o modo Semana e marque os dias de semana de segunda a sexta-feira. Adicione o Intervalo de Tempo das 08:00 ~ 18:00.
2	Configuração do requerimento 1	ACL → Configurar ACL → Criar ACL, configurar 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, e configure o Agendamento como Nenhum. ACL → Políticas ACL → Criar Políticas, configurar uma política com o nome gerente. ACL → Políticas ACL → Criar Ação , adicionar na ACL 11 a política gerente. ACL → Vínculos ACL → Vínculo por Porta, selecionar a política gerente e vincule a porta 3.
3	Configuração dos requerimentos 2 e 4	ACL → Configurar ACL → Criar ACL, configurar 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, configure o Agendamento como Nenhum. 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, configure o Agendamento como Nenhum. 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, configure o Agendamento como Expediente. ACL → Políticas ACL → Criar Ação , adicionar na ACL 100 a política limite1. ACL → Configurar ACL → Criar Políticas, configurar uma política com o nome limite1. ACL → Vínculos ACL → Vínculo por Porta, selecionar a limite1 e vincule a porta 3.
4	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, configure o Agendamento como Nenhum. 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, configure o Agendamento como Nenhum. ACL → Políticas ACL → Criar Políticas, configurar uma política com o nome limite2. ACL → Políticas ACL → Criar Ação , adicionar na ACL 101 a política limite1. ACL → Vínculos ACL → Vínculo por Porta, selecionar a política limite2 e vincule a porta 4.

11. Segurança

O menu Segurança é utilizado para fornecer e configurar várias medidas de proteção para a segurança da rede. Este menu inclui 4 sub-menus: *Associação ARP*, *Inspeção ARP*, *DoS* e *802.1X*. Por favor, configure as funções conforme sua necessidade.

11.1. Associação ARP

A função Associação ARP permite vincular o endereço IP, o endereço MAC e o VLAN ID de um host com uma determinada porta do switch, restringindo o acesso à rede.

Os seguintes métodos de Associação ARP são suportados pelo switch.

- 1. Manual: você pode vincular o endereço IP, endereço MAC e VLAN ID do host com a porta do switch manualmente.
- 2. Scanning: você pode vincular o endereço IP, endereço MAC, VLAN ID e a porta em que o host está conectado no switch de forma dinâmica, bastando apenas especificar a faixa de endereços IPs a ser pesquisada bem como o VLAN ID. Após realizado a pesquisa, selecionar quais entradas deseja vincular.
- 3. DHCP Snooping: você pode utilizar a função de DHCP Snooping para monitorar o processo em que o host recebe o endereço IP de um servidor DHCP e registrar o endereço IP, endereço MAC, VLAN ID e o número da porta em que o host está conectado no switch, realizando assim, um vínculo automático.

Esses três métodos são utilizados para elaboração da Tabela ARP, vinculando o endereço IP, endereço MAC, VLAN ID e porta do switch onde o host está conectado. As entradas provenientes de várias origens devem ser diferenciadas umas das outras para que se evitem colisões, somente a origem com maior prioridade será validada. Os três métodos (manual, scanning e snooping) estão respectivamente em ordem decrescente de prioridade.

A função Associação ARP pode ser configurada em *Tabela ARP*, *ARP Manual*, *ARP Scanning* e *DHCP Snooping*.

Tabela ARP

Nesta página você pode visualizar as informações referente a Tabela ARP.

Escolha o menu *Segurança* → *Associação ARP* → *Tabela ARP* para carregar a seguinte página:

Tipo de pesquisa

Selecionar origem:

Todas

Procurar

Tabela de Associações

Selecionar

Nome do Host

Endereço IP

Endereço MAC

VLAN ID

Porta

IP:

Selecionar

Tipo de Proteção

Origem

Colisão

☐

Aplicar

Remover

Ajuda

Total de entradas: 0

Obs.:

1. Entre as entradas com colisão de nível crítico, a que possuir origem com maior prioridade é a que estará em vigor.

2. Entre as entradas com a mesma prioridade de origem, somente a última entrada adicionada ou modificada estará em vigor.

Tabela ARP

As seguintes opções são apresentadas na tela:

- » **Tipo de pesquisa**
 - » **Selecionar origem:** selecione o método de busca para a visualização da Tabela ARP e clique no botão *Procurar*.
 - » **Todas:** exibe todas as entradas da tabela.
 - » **Manual:** exibe somente as entradas configuradas manualmente.
 - » **Scanning:** exibe somente as entradas configuradas a partir da função ARP Scanning.
 - » **Snooping:** exibe somente as entradas configuradas a partir da função DHCP Snooping.
- » **Tabela de associações**
 - » **IP:** digite o endereço IP no campo correspondente e clique no botão *Selecionar* para selecionar o endereço IP desejado.

Selecionar: selecione a entrada desejada. É possível selecionar mais de uma entrada simultaneamente. Também é possível criar uma descrição para o host utilizando o campo *Nome do Host* e alterar o tipo de proteção através do campo *Tipo de Proteção* ou remover a entrada desejada clicando no botão *Remover*.

Nome do host: exibe o nome do computador.

Endereço IP: exibe o endereço IP do computador.

Endereço MAC: exibe o endereço MAC do computador.

VLAN ID: exibe a VLAN ID que o computador pertence.

Porta: exibe o número da porta do switch em que o computador está conectado.

Tipo de proteção: permite visualizar ou alterar o tipo de proteção da porta.

Origem: exibe o método utilizado para a obtenção da entrada na Tabela ARP.

Colisão: exibe o status de colisão.

» **Aviso:** indica que a colisão pode ter sido causada pela função MSTP.

» **Crítico:** indica que uma entrada está em colisão com outra entrada.

Obs.: » *Dentre as entradas com nível crítico de colisão, aquelas com prioridades mais altas terão preferência.*

» *Dentre as entradas conflitantes com o mesmo nível de prioridade, apenas a última entrada adicionada ou modificada terá efeito.*

ARP manual

Nesta página você pode vincular manualmente o endereço IP, endereço MAC, e o VLAN ID do host com a porta do switch desejada. Escolha o menu *Segurança* → *Associação ARP* → *ARP Manual* para carregar a página:

Configuração de Associação ARP Manual

Nome do Host:

(20 caracteres no máximo)

Endereço IP:

(Formato: 192.168.0.1)

Endereço MAC:

(Formato: 00-00-00-00-00-01)

VLAN ID:

(1-4094)

Porta:

1

Tipo de Proteção:

Desabilitar

Vincular

Associações ARP Manual configuradas

Selecionar	Nome do Host	Endereço IP	Endereço MAC	VLAN ID	Porta	Tipo de Proteção	Colisão
TodasRemoverAjuda							

Total de entradas: 0

Obs.:

1. Entre as entradas com colisão de nível crítico, a que possuir origem com maior prioridade é a que estará em vigor.

2. Entre as entradas com a mesma prioridade de origem, somente a última entrada adicionada ou modificada estará em vigor.

Tabela de vínculos manuais

As seguintes opções são exibidas na tela:

» **Configuração de associação ARP manual**

Nome do host: digite um nome para identificar o computador desejado.

Endereço IP: digite o endereço IP do computador.

Endereço MAC: digite o endereço MAC do computador.

VLAN ID: digite a VLAN ID que o computador pertence.

Porta: selecione a porta do switch em que o computador está conectado.

Tipo de proteção: selecione o tipo de proteção.

» Associações ARP Manual configuradas

Selecionar: selecione a entrada desejada. É possível selecionar mais de uma entrada simultaneamente. Também é possível criar uma descrição para o host utilizando o campo *Nome do Host* e alterar o tipo de proteção através do campo *tipo de proteção* ou remover a entrada desejada clicando no botão *Remover*.

Nome do host: exibe o nome do computador.

Endereço IP: exibe o endereço IP do computador.

Endereço MAC: exibe o endereço MAC do computador.

VLAN ID: exibe a VLAN ID que o computador pertence.

Porta: exibe o número da porta do switch em que o computador está conectado.

Tipo de proteção: exibe o tipo de proteção.

Colisão: exibe o status de colisão.

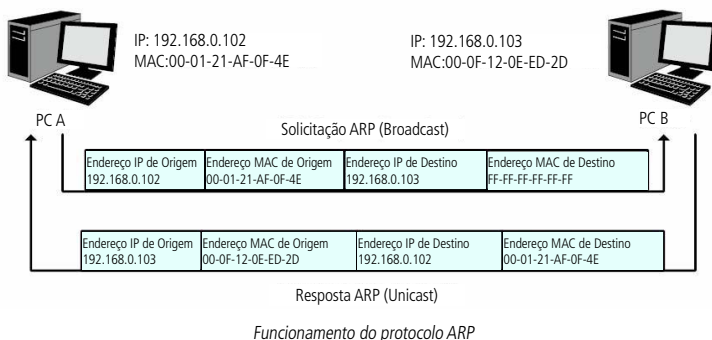
» **Aviso:** indica que a colisão pode ter sido causada pela função MSTP.

» **Crítico:** indica que uma entrada está em colisão com outra entrada.

ARP scanning

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

Quando um computador se comunica com outro, o protocolo ARP funciona conforme imagem e explicação a seguir:



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

A função ARP Scanning permite que o switch envie requisições ARP com o campo endereço IP preenchido conforme desejado, dentro de uma rede ou VLAN.

Ao receber pacotes de resposta ARP, o switch consegue, obter o endereço IP, endereço MAC, VLAN ID e o número da porta em que o computador está conectado no switch.

Escolha o menu *Segurança* → *Associação ARP* → *ARP Scanning* para carregar a seguinte página:

Pesquisa de Endereço IP

Endereço IP Inicial:

Endereço IP Final:

VLAN ID:

(1-4094)

Pesquisar

Resultado da pesquisa IP

Selecionar	Nome do Host	Endereço IP	Endereço MAC	VLAN ID	Porta	Tipo de Proteção	Colisão
☐							

Vincular

Remover

Ajuda

Total de entradas: 0

Obs.:

1. A opção VLAN ID é utilizado para realizar a busca dos Endereços IP pertencentes a uma determinada VLAN.

2. VLAN ID afeta a Tag de VLAN nos pacotes de ARP Request utilizados na função ARP Scanning, e é independente da configuração de VLAN.

3. Se o VLAN ID estiver em branco, o switch transmitirá em broadcast pacotes Untagged de ARP Request utilizados na função ARP Scanning.

ARP Scanning

As seguintes opções são exibidas na tela:

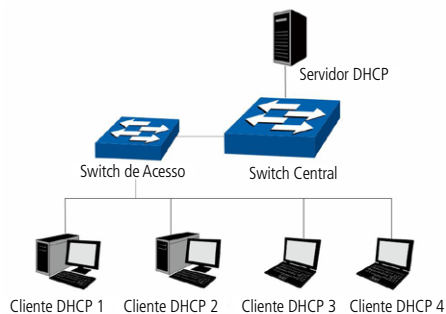
- » **Pesquisa de endereço IP**
 - Endereço IP inicial:** digite o endereço IP inicial da faixa de endereços IPs desejado.
 - Endereço IP final:** digite o endereço IP final da faixa de endereços IPs desejado.
 - VLAN ID:** digite a VLAN ID desejada. Se este campo estiver em branco, o switch irá enviar pacotes untag para análise.
 - Pesquisar:** clique no botão *Pesquisar* para o switch começar a realizar a consulta desejada.
- » **Resultado da pesquisa IP**
 - Selecionar:** selecione a entrada desejada. Para remover a entrada correspondente, clique no botão *Remover*.
 - Nome do host:** exibe o nome do computador.
 - Endereço IP:** exibe o endereço IP do computador.
 - Endereço MAC:** exibe o endereço MAC do computador.
 - VLAN ID:** exibe a VLAN ID que o computador pertence.
 - Porta:** exibe o número da porta do switch em que o computador está conectado.
 - Tipo de proteção:** exibe o tipo de proteção.
 - Colisão:** exibe o status de colisão.
 - » **Aviso:** indica que a colisão pode ter sido causada pela função MSTP.
 - » **Crítico:** indica que um entrada está em colisão com outra entrada.

DHCP Snooping

Atualmente as redes estão ficando cada vez maiores e mais complexas. As configurações de endereços IP e parâmetros de redes utilizados devem ser analisados e atualizados com frequência, permitindo o perfeito funcionamento dos computadores e recursos da rede. O protocolo DHCP (Dynamic Host Configuration Protocol) foi desenvolvido baseando-se no protocolo BOOTP e é utilizado para otimizar e resolver os problemas mencionados acima.

» **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:

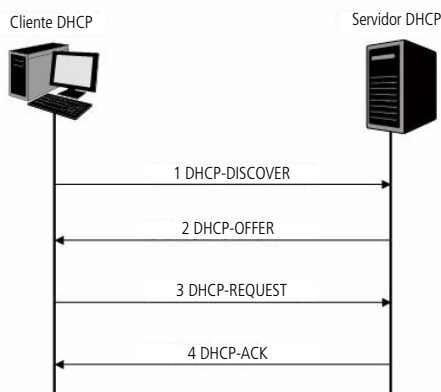


Funcionamento do DHCP

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

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

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



Negociação DHCP

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

» Option 82

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

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

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

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

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

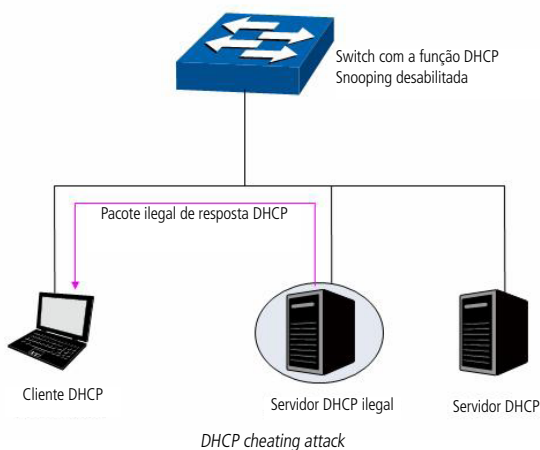
Circuit ID é definido para ser o número da porta do switch que recebe os pacotes de solicitação DHCP juntamente com o VLAN ID.

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

» DHCP cheating attack

Durante o processo de funcionamento do DHCP, geralmente não há nenhum mecanismo de autenticação entre o cliente e servidor. Se houver vários servidores DHCP na rede, acontecerá certa confusão e insegurança na rede. Os casos mais comuns que podem ocorrer estão listados a seguir.

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



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

Escolha o menu *Segurança* → *Associação ARP* → *DHCP Snooping* para carregar a seguinte página:

Configuração DHCP Snooping

DHCP Snooping:

☐ Habilitar ☒ Desabilitar

Controle de Fluxo DHCP:

Desabilitar

 pps

Limiar Mínimo DHCP:

Desabilitar

 pps

Limitar Pacotes DHCP:

5

 pps

Aplicar

Configuração Option 82

Option 82:

☐ Habilitar ☒ Desabilitar

Campo Option 82 existente:

Manter

Customização:

☐ Habilitar ☒ Desabilitar

Circuit ID:

Remote ID:

Aplicar

Configuração das portas

Porta

Selecione

Selecione	Porta	Porta Confiável	Verificar MAC	Controle de Fluxo	Limite de Proteção	LAG
☐	1	Desabilitar	Desabilitar	Desabilitar	Desabilitar	---
☐	2	Habilitar	Desabilitar	Desabilitar	Desabilitar	---
☐	3	Habilitar	Desabilitar	Desabilitar	Desabilitar	---
☐	4	Habilitar	Desabilitar	Desabilitar	Desabilitar	---
☐	5	Habilitar	Desabilitar	Desabilitar	Desabilitar	---
☐	6	Habilitar	Desabilitar	Desabilitar	Desabilitar	---
☐	7	Habilitar	Desabilitar	Desabilitar	Desabilitar	---
☐	8	Habilitar	Desabilitar	Desabilitar	Desabilitar	---
☐	9	Habilitar	Desabilitar	Desabilitar	Desabilitar	---
☐	10	Habilitar	Desabilitar	Desabilitar	Desabilitar	---

Aplicar Ajuda

DHCP snooping

Obs.: se você desejar habilitar a função DHCP Snooping para uma porta membro de um grupo LAG, por favor, certifique-se que as configurações das portas membros são as mesmas.

As seguintes informações são apresentadas na tela:

» **Configuração DHCP Snooping**

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

Controle de fluxo DHCP: selecione a velocidade máxima de mensagens DHCP que o switch pode transmitir por segundo. As mensagens excessivas serão descartadas.

Limiar mínimo DHCP: selecione um valor que especifique a taxa mínima de transmissão, acima disso será habilitada a função *Limite de Proteção* para a porta especificada.

Limitar pacotes DHCP: selecione um valor para limitar as mensagens DHCP. A transmissão será limitada a este valor se taxa de transmissão exceder o Limiar Mínimo DHCP.

» **Configuração option 82**

Option 82: selecione *Habilitar/Desabilitar* para habilitar ou desabilitar a função Option 82.

Campo option 82 existente: selecione a operação para o campo Option 82 dos pacotes DHCP-REQUEST enviados dos clientes.

» **Manter:** é utilizado para manter o campo Option 82 dos pacotes DHCP.

» **Substituir:** é utilizado para substituir o campo Option 82 dos pacotes DHCP com o que foi definido pelo switch.

» **Descartar:** é utilizado para descartar os pacotes DHCP incluindo o campo Option 82

Customização: selecione *Habilitar/Desabilitar* para habilitar ou desabilitar a customização do campo Option 82 pelo switch.

Circuit ID: digite a sub-opção Circuit ID para personalização do campo Option 82.

Remote ID: digite a sub-opção Remote ID para personalização do campo Option 82.

» Configuração das portas

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

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

Porta: exibe o número da porta.

Porta confiável: selecione *Habilitar/Desabilitar* para habilitar ou desabilitar a função *Porta Confiável*. Somente as portas confiáveis podem receber pacotes DHCP dos servidores DHCP.

Verificar MAC: selecione *Habilitar/Desabilitar* para habilitar ou desabilitar a função *Verificar MAC*. No pacote DHCP existem dois campos contendo o endereço MAC do cliente, esta função irá comparar estes dois campos e descartar o pacote se os campos forem diferentes.

Controle de fluxo: selecione *Habilitar/Desabilitar* para habilitar ou desabilitar a função *Controle de Fluxo* para os pacotes DHCP. Os pacotes DHCP em excesso serão descartados.

Limite de proteção: selecione *Habilitar/Desabilitar* para habilitar ou desabilitar a função de *Limite de Proteção*.

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

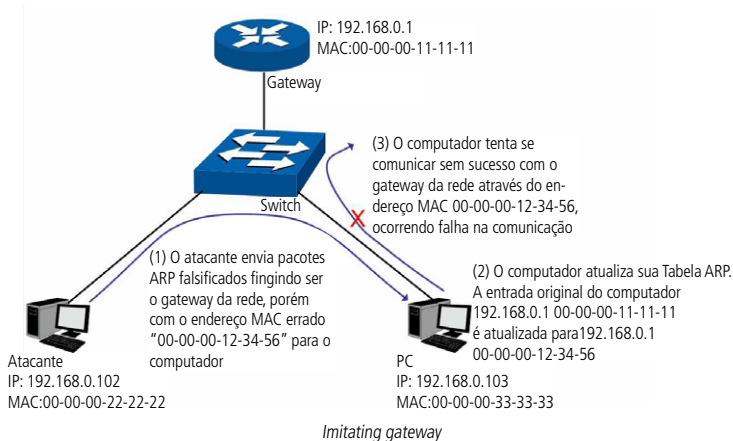
11.2. Inspeção ARP

De acordo com a implementação ARP, mencionado no Capítulo 11 ARP Scanning, o protocolo ARP auxilia na comunicação entre os computadores em uma mesma rede ou ainda no acesso a redes externa através do uso do gateway. Assim ataques de falsificação ARP, tais como Imitating Gateway, Cheating Gateway, Cheating Terminal Hosts e ARP Flooding Attack, ocorrem com frequência em redes de grandes dimensões.

A seguir, explicação de alguns dos ataques.

» Imitating gateway

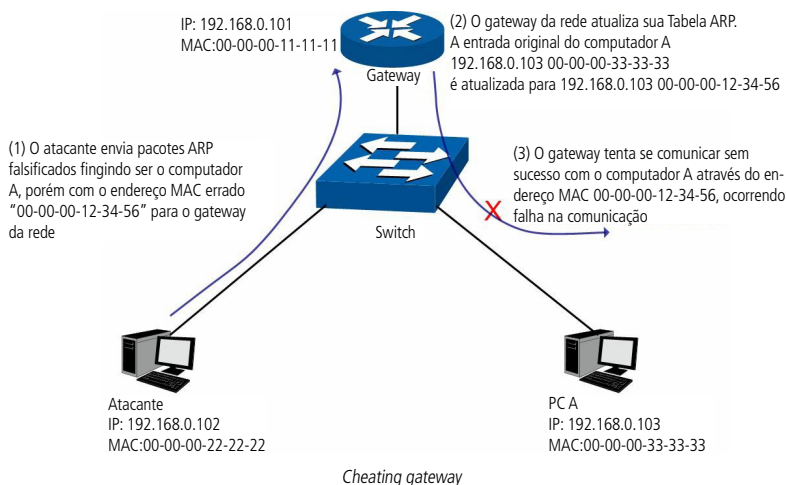
O atacante envia um endereço MAC falso de um gateway para um determinado computador na rede, em seguida este computador atualizará automaticamente a sua tabela ARP, fazendo com que o computador não acesse a rede de forma normal. O Imitating Gateway está sendo ilustrado na figura a seguir.



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

» Cheating gateway

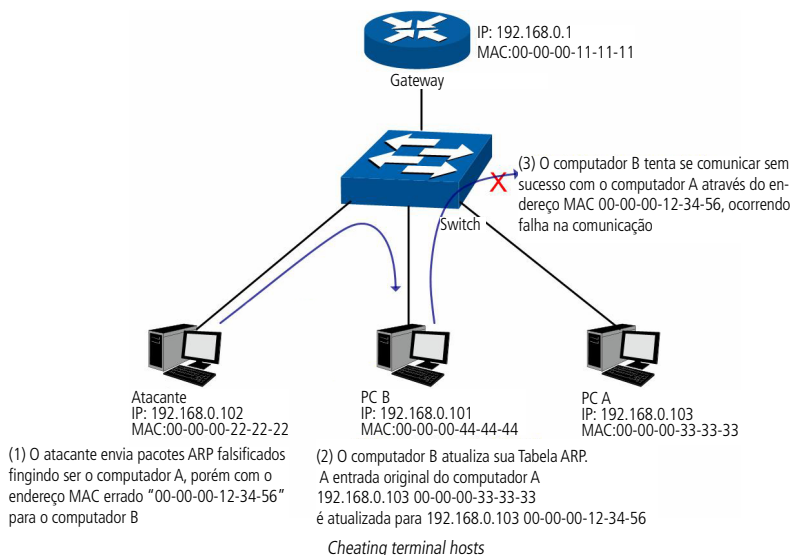
O atacante envia um endereço MAC falso de um computador para o gateway da rede, em seguida, este gateway atualizará sua tabela ARP, fazendo com que o gateway não consiga responder as solicitações deste computador. O Cheating Gateway é ilustrado na figura a seguir:



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

» Cheating terminal host

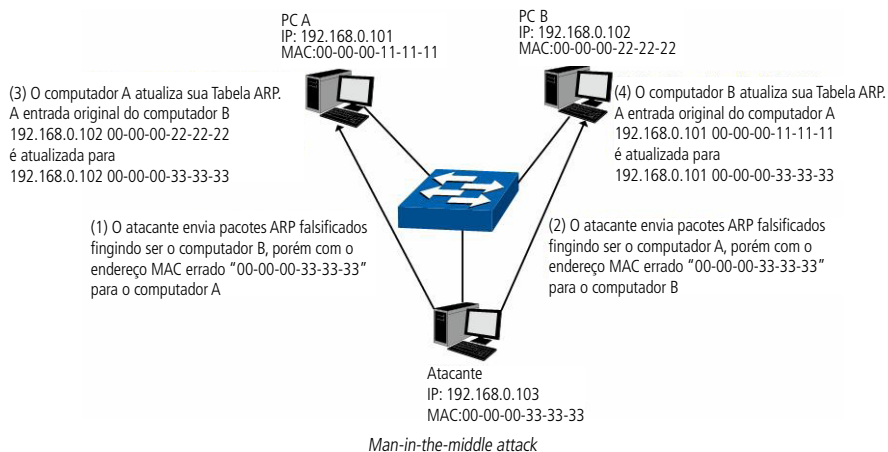
O atacante envia um endereço MAC falso de um computador para outro computador da rede, fazendo com que estes computadores que estão na mesma rede não se comuniquem. O Cheating Terminal Hosts é ilustrado na figura a seguir.



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

» Man-in-the-middle attack

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



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

Computador A: o seu endereço IP é 192.168.0.101 e o endereço MAC é 00-00-00-11-11-11

Computador B: o seu endereço IP é 192.168.0.102 e o endereço MAC é 00-00-00-22-22-22

Atacante: o seu endereço IP é 192.168.0.103 e o endereço MAC é 00-00-00-33-33-33

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

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

» ARP flooding attack

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

A função *Associação ARP* permite que o switch possa vincular o endereço IP, endereço MAC, VLAN ID, e o número da porta do switch que o computador está conectado. Com base nas associações ARP predefinidas, a função *Inspecção ARP* poderá detectar os pacotes ARP ilegais, evitando assim, ataques ARP na rede.

A função de *Inspecção ARP* pode ser configurada nas seguintes páginas: *Detecção ARP*, *Proteção ARP* e *Estatísticas ARP*.

Detecção ARP

A função *Detecção ARP* permite ao switch detectar os pacotes ARP com base nas entradas de sua Tabela de Associações ARP e filtrar os pacotes ARP falsificados, evitando que a rede sofra ataque do tipo ARP, tais como Network Gateway Spoofing e Man-In-The-Middle Attack, etc.

Escolha o menu *Segurança* → *Inspecção ARP* → *Detecção ARP* para carregar a seguinte página:

Configuração de Detecção ARP

Detecção ARP: ☐ Habilitar ☒ Desabilitar

Portas de Confiança

☐ 1

☐ 2

☐ 3

☐ 4

☐ 5

☐ 6

☐ 7

☐ 8

☐ 9

☐ 10

Aplicar

Todas

Limpar

Ajuda

Obs.:
É recomendado configurar as portas de up-link e portas membros de um grupo LAG como Portas de Confiança.

Detecção ARP

As seguintes opções são exibidas na tela:

- » **Configuração de detecção ARP**
Detecção ARP: selecione *Habilitar/Desabilitar* para habilitar ou desabilitar a função Detecção ARP e clique no botão *Aplicar*.
- » **Portas de confiança**
Portas de confiança: selecione a porta que não fará parte da Detecção ARP. As portas de up-link e LAG deverão ser definidas como Portas de Confiança, para garantir a comunicação normal com o switch, por favor, configure as portas de confiança antes de ativar a função Detecção ARP.

Obs.: as funções *Detecção ARP* e *Proteção ARP* não podem ser habilitadas ao mesmo tempo.

Procedimento de configuração

Passo	Operação	Descrição
1	Realizar a Associação ARP da entrada desejada	Obrigatório, em Associação ARP, vincular o endereço IP, endereço MAC, VLAN ID e o número da porta do switch que o computador está conectado, através de uma das páginas de configuração: ARP Manual, ARP Scanning ou DHCP Snooping.
2	Habilitar o Tipo de Proteção	Obrigatório, em Segurança → Associação ARP → Tabela ARP, especificar o tipo de proteção para a entrada correspondente.
3	Especificar as Portas de Confiança	Obrigatório, em Segurança → Inspecção ARP → Detecção ARP, especificar as portas de confiança. As portas up-link e LAG deverão ser definidas como portas de confiança.
4	Habilitar a função Detecção ARP	Obrigatório, em Segurança → Inspecção ARP → Detecção ARP, habilitar a função Detecção ARP.

Proteção ARP

Com a função *Proteção ARP* habilitada, o switch não recebe pacotes ARP por 300 segundos, quando a velocidade de transmissão de pacotes ARP exceder o valor definido, evitando que ocorra inundação de pacotes ARP na rede.

Escolha o menu *Segurança* → *Inspeção ARP* → *Proteção ARP* para carregar a seguinte página:

Configuração de Proteção ARP

Porta

Selecionar

Selecionar	Porta	Proteção	Velocidade (10-100)pps	Velocidade Atual (pps)	Status	LAG	Operação
☐		Desabilitar					
☐	1	Desabilitar	15	---	---	---	---
☐	2	Desabilitar	15	---	---	---	---
☐	3	Desabilitar	15	---	---	---	---
☐	4	Desabilitar	15	---	---	---	---
☐	5	Desabilitar	15	---	---	---	---
☐	6	Desabilitar	15	---	---	---	---
☐	7	Desabilitar	15	---	---	---	---
☐	8	Desabilitar	15	---	---	---	---
☐	9	Desabilitar	15	---	---	---	---
☐	10	Desabilitar	15	---	---	---	---

Atualizar

Aplicar

Ajuda

Obs.:
Não é recomendado habilitar a Proteção ARP para uma porta membro de um grupo LAG.

Proteção ARP

As seguintes entradas são exibidas na tela:

- » **Configuração de proteção ARP**
 - 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.
 - Proteção:** selecione *Habilitar/Desabilitar* para habilitar ou desabilitar a função Proteção ARP.
 - Velocidade (10-100) pps:** digite a quantidade máxima de pacotes ARP recebidos por segundo pela porta.
 - Velocidade atual (pps):** exibe quantidade de pacotes ARP recebidos por segundo pela porta.
 - Status:** exibe o status da porta na função Proteção ARP.
 - LAG:** exibe o grupo LAG a qual pertence à porta.
 - Operação:** clique em *Recuperar* para restaurar o estado normal da porta. A função Proteção ARP para essa porta será reativada.
- Obs.:** » Não é recomendado habilitar a função Proteção ARP para portas membros de um grupo LAG.
- » As funções Detecção ARP e Proteção ARP não podem ser habilitadas ao mesmo tempo.

Estatísticas ARP

A função Estatísticas ARP exibe informações sobre o número de pacotes ARP ilegais recebidos em cada porta, o que facilita a localização de problemas na rede.

Escolha o menu *Segurança* → *Inspecção ARP* → *Estatísticas ARP* para carregar a página seguinte.

Atualização Automática de pacotes ARP Ilegais

Atualização Automática: ☐ Habilitar ☒ Desabilitar

Intervalo: seg (3-300)

Aplicar

Tabela de Pacotes ARP Ilegais

Porta	Porta de Confiança	Pacotes ARP Ilegal	Porta	Porta de Confiança	Pacotes ARP Ilegal
1	Não	---	2	Não	---
3	Não	---	4	Não	---
5	Não	---	6	Não	---
7	Não	---	8	Não	---
9	Não	---	10	Não	---

Atualizar Limpar Ajuda

Estatísticas ARP

As seguintes opções são apresentadas na tela:

- » **Atualização automática de pacotes ARP ilegais**
 - Atualização automática:** selecione *Habilitar/Desabilitar* para habilitar ou desabilitar a função atualização automática.
 - Intervalo:** digite o intervalo de atualização das estatísticas ARP.
- » **Tabela de pacotes ARP ilegais**
 - Porta:** exibe o número da porta.
 - Porta de confiança:** exibe se a porta está configurada como porta de confiança ou não.
 - Pacotes ARP ilegal:** exibe o número de pacotes ARP ilegais recebidos pela porta.

11.3. DoS

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

O switch pode detectar alguns tipos de ataques DoS, conforme mostrado na tabela a seguir.

Tipo de ataque DoS	Descrição
Land Attack	O atacante envia um pacote TCP falso com a flag SYN habilitada para um host de destino. Uma vez que este pacote possua os campos endereço IP de origem e destino configurado de acordo com o endereço IP do host atacado, este host ficará preso em um loop infinito, afetando drasticamente o desempenho da rede.
Scan SYNFIN	O atacante envia um pacote TCP com as flags SYN e FIN habilitadas. A flag SYN é utilizada para iniciar uma nova conexão, enquanto a flag FIN é utilizada para solicitar uma desconexão. Portanto o pacote deste tipo é ilegal. O switch pode se defender desse tipo de pacote.
Xmascan	O atacante envia o pacote TCP com as seguintes flags habilitadas: FIN, URG e PSH.
NULL Scan Attack	O atacante envia o pacote TCP com todas as flags de controle como 0. Durante a conexão e a transmissão de dados, os pacotes com todos os controles definidos como 0 serão considerados pacotes ilegais.
SYN packet with source port less than 1024	O atacante envia um pacote TCP com a flag SYN habilitada para uma porta de origem menor que 1024.
Blat Attack	O atacante envia um pacote TCP falso com os campos Porta de origem e destino configurados com o mesmo valor e com a flag URG habilitada para um host de destino. Semelhante ao Land Attack, o desempenho do host atacado cairá drasticamente, uma vez que o host sempre tentará iniciar uma nova conexão com o atacante.
Ping Flooding	O atacante faz uma inundação na rede com pings em broadcast, impedindo que o switch responda as verdadeiras comunicações.
SYN/SYN-ACK Flooding	O atacante utiliza um endereço IP falso para enviar pacotes de solicitação ao servidor. Ao receber os pacotes de solicitação, o servidor responde com pacotes SYN-ACK. Como o endereço IP é falso, nenhuma resposta será enviada ao servidor, portanto o servidor continuará enviando pacotes SYN-ACK aguardando uma resposta. Se o atacante ficar enviando muitos pacotes com solicitações falsas, os clientes que realmente desejam utilizar o serviço, terão seus acessos negados.

Nesta página você pode habilitar a proteção DoS mais adequada para as suas necessidades.

Escolha o menu *Segurança* → *DoS* → *DoS* para carregar a seguinte página:

Configuração DoS

Proteção DoS: ☐ Habilitar ☒ Desabilitar

Tipos de Ataques DoS

Selecionar	Nome do Ataque DoS
☐	Land Attack
☐	Scan SYNFIN
☐	Xmascan
☐	NULL Scan
☐	SYN sPort less 1024
☐	Blat Attack
☐	Ping Flooding
☐	SYN/SYN-ACK Flooding

Atualizar

Aplicar

Ajuda

Ataques DoS

As seguintes opções são apresentadas na tela:

» **Configuração DoS**

Proteção DoS: selecione *Habilitar/Desabilitar* para habilitar ou desabilitar a função de proteção DoS.

» **Tipos de ataques DoS**

Selecionar: selecione o tipo de ataque que o switch irá se defender.

Nome do ataque DoS: exibe o nome do tipo de ataque.

Obs.: » *Sugerimos que você tome as seguintes medidas para garantir a segurança da rede.*

- » *É recomendado inspecionar e reparar vulnerabilidades na rede regularmente, bem como adotar métodos de backup das configurações importantes.*
- » *O administrador de rede deve inspecionar o ambiente físico e bloquear serviços desnecessários.*
- » *Para uma melhor segurança, utilize firewall na rede.*

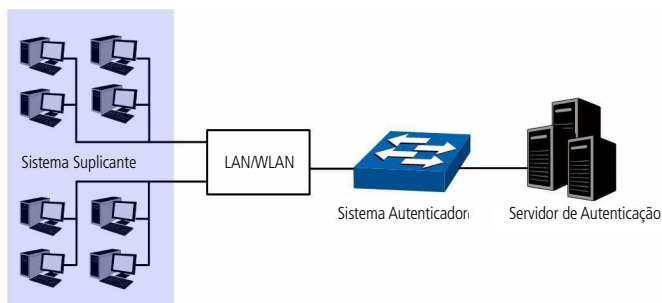
11.4. 802.1X

O protocolo 802.1X foi desenvolvido pela IEEE802 comissão LAN/WAN, para lidar com as questões de segurança de redes sem fio. Em seguida foi utilizado como mecanismo de controle de acesso utilizado pelo Ethernet, resolvendo problemas de autenticação e segurança.

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

» **Arquitetura de autenticação 802.1X**

802.1X adota uma arquitetura de Cliente/Servidor com três entidades: um sistema suplicante, um sistema autenticador e um servidor de autenticação, a figura a seguir ilustra esse processo.



Arquitetura 802.1X

1. Sistema Suplicante: é uma entidade da LAN e é autenticado pelo sistema autenticador. O sistema suplicante geralmente é o computador de um usuário da rede. Uma autenticação 802.1X é iniciada quando um usuário lança um programa cliente no sistema suplicante. Note que o programa cliente deve suportar a autenticação 802.1X.
2. Sistema Autenticador: é um dispositivo de rede como esse switch. Ele fornece a porta física ou lógica para o suplicante acessar a LAN e se autenticar.
3. Servidor de Autenticação: é normalmente a entidade que provê o serviço de autenticação. Normalmente é formado por um servidor RADIUS. O servidor de autenticação pode armazenar informações de usuários e serve para realizar autenticação e autorização. Para garantir um sistema de autenticação estável, é recomendado possuir um servidor de autenticação alternativo, utilizado como backup.

» **Mecanismos de autenticação 802.1X**

O sistema de autenticação IEEE802.1X utiliza o protocolo EAP (Extensible Authentication Protocol) para trocar informações entre o sistema suplicante e o servidor de autenticação.

1. O protocolo EAP transmitido entre o sistema suplicante e o sistema autenticador são encapsulados como pacotes EAPOL.
2. O protocolo EAP, transmitido entre o sistema autenticador e o servidor RADIUS são encapsulados como EAPOR (EAP over RADIUS) ou através de PAP (Password Authentication Protocol) ou CHAP (Challenge Handshake Authentication Protocol).

- Quando um sistema suplicante é processado pelo servidor de autenticação, o servidor de autenticação passa a informação sobre o sistema suplicante para o sistema autenticador. O sistema autenticador, por sua vez determina o estado (autorizado ou não autorizado) da porta de acordo com as instruções (accept ou reject) recebidos do servidor Radius.

» Procedimento de autenticação 802.1X

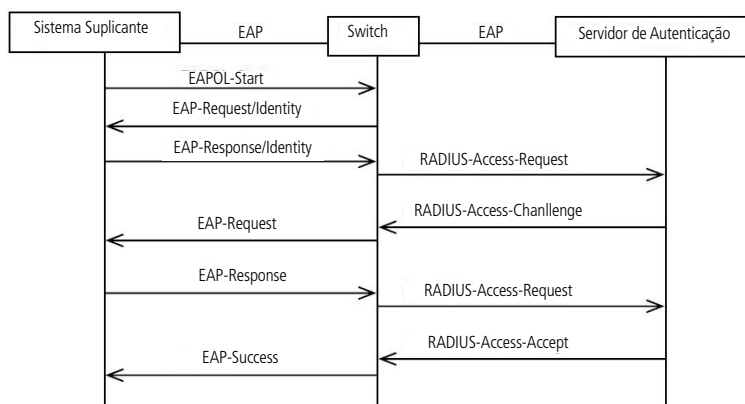
Uma autenticação 802.1X pode ser iniciada pelo sistema suplicante ou pelo sistema autenticador.

Quando um sistema autenticador (switch) detecta um suplicante não autenticado e conectado em sua porta, ele irá iniciar o procedimento de autenticação 802.1X enviando pacotes EAP-Request/Identity. O sistema suplicante também pode iniciar o procedimento de autenticação 802.1X, iniciando um programa cliente de autenticação 802.1X, através do envio de pacotes EAPOL-Start para o switch.

A seguir duas ilustrações de autenticação 802.1X iniciada pelo sistema suplicante.

1. Modo de transmissão EAP:

Neste modo, os pacotes EAP são encapsulados no protocolo de nível superior (EAPOR) para conseguir chegar ao servidor de autenticação. Este modo normalmente exige que o servidor Radius tenha suporte aos dois tipos de mensagens. O campo mensagem EAP e o campo Message-authenticator. Esse switch suporta a forma de autenticação EAP-MD5 para o modo de transmissão EAP. A figura a seguir descreve o procedimento básico de autenticação EAP-MD5.



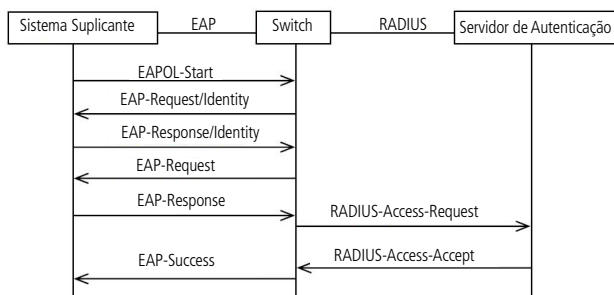
Procedimento de autenticação EAP-MD5

- Um sistema suplicante inicia um programa cliente de autenticação 802.1X, através de seu nome de usuário e senha cadastrados no servidor de autenticação, enviando um pacote EAPOL-Start para o switch. O programa cliente 802.1X encaminha os pacotes para o switch iniciar o processo de autenticação.
- Ao receber o pacote de solicitação de autenticação, o switch envia um pacote EAP-Request/Identity para solicitar ao programa cliente 802.1X o nome de seu usuário.
- O programa 802.1X cliente envia um pacote EAP-Response/Identity para o switch com o nome de usuário. O switch então encapsula o pacote em um pacote RADIUS Access-Request e encaminha o pacote para o servidor RADIUS.
- Ao receber o nome de usuário do switch, o servidor RADIUS verifica a senha correspondente do usuário em seu banco de dados e criptografa a senha utilizando uma chave aleatória, e encaminha esta chave ao switch através do pacote RADIUS Access-Challenge. O switch em seguida, envia a chave para o programa 802.1X cliente.
- O receber a chave (encapsulada no pacote EAP-Request/MD5 Challenge) do switch, o programa 802.1X cliente criptografa a senha do sistema suplicante com a chave recebida e envia a senha criptografada (contida no pacote EAP-Response/MD5 Challenge) para o servidor RADIUS através do switch (a criptografia é irreversível).
- O servidor RADIUS compara a senha criptografada recebida (contida no pacote RADIUS Access-Request) com a senha criptografada localmente. Se as duas combinarem, ele enviará a resposta (através de um pacote RADIUS Access-Accept e do pacote EAP-Success), informando ao switch que o sistema suplicante está autorizado.
- O switch muda o estado da porta correspondente ao estado accept para permitir que o sistema suplicante tenha acesso à rede. Então o switch irá monitorar o status do suplicante enviando pacotes hand-shake periodicamente. Por padrão, o switch vai forçar o suplicante fazer logoff se não obter a resposta do suplicante em duas tentativas.
- O sistema suplicante também pode encerrar o estado de autenticação, enviando pacotes EAPOL-Logoff para o switch. O switch então muda o estado da porta para reject.

2. Modo de terminação EAP:

Neste modo, a transmissão de pacotes é encerrada no sistema autenticador e os pacotes EAP são mapeados em pacotes RADIUS. Autenticação e contabilidade são realizadas através de protocolos RADIUS.

Neste modo, o método de autenticação PAP ou CHAP é utilizado entre o switch e o servidor RADIUS. Este switch suporta o modo de encerramento PAP. O procedimento de autenticação PAP é ilustrado na figura a seguir.



Procedimento de autenticação PAP

No modo PAP, o switch criptografa a senha com uma chave gerada aleatoriamente e envia o nome do usuário ao sistema suplicante, o sistema suplicante criptografa a senha para o servidor RADIUS, utilizado para uma autenticação adicional.

Considerando que a chave gerada aleatoriamente no modo de transmissão EAP-MD5 é realizada pelo servidor de autenticação, o switch é o responsável por encapsular o pacote de autenticação e enviá-lo para o servidor RADIUS.

» Temporizadores 802.1X

Na autenticação 802.1X, os seguintes temporizadores são utilizados para assegurar que o sistema suplicante, o switch e o servidor RADIUS interagem de uma maneira ordenada.

1. Timeout Suplicante: este temporizador é acionado pelo switch após o switch enviar um pacote de solicitação ao sistema suplicante. O switch irá reenviar o pacote de solicitação ao sistema suplicante se o sistema suplicante não responder no período de tempo limite especificado.
2. Timeout Autenticador: este temporizador é acionado pelo switch após o switch enviar um pacote de solicitação de autenticação para o servidor RADIUS. O switch irá reenviar o pacote de solicitação de autenticação se o servidor RADIUS não responder no período de tempo limite especificado.
3. Intervalo de Silêncio: este temporizador define o período de silêncio. Enquanto o sistema suplicante não processa a autenticação, o switch fica em silêncio (não envia pacotes 802.1X) por um período especificado antes de processar outra solicitação de autenticação.

» Guest VLAN

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

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

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

A função 802.1X pode ser configurada nas seguintes páginas: *Configurar 802.1X*, *Portas 802.1X* e *Servidor Radius*.

Configurar 802.1X

Nesta página você pode habilitar a função de autenticação 802.1X para controlar o processo de autenticação, especificando o Tipo de Autenticação, Guest VLAN e diferentes Temporizadores.

Escolha o menu *Segurança* → *802.1X* → *Configurar 802.1X* para carregar a seguinte página:

Configuração Global

802.1X: ☐ Habilitar ☒ Desabilitar

Tipo de Autenticação:

EAP-MD5

Guest VLAN: ☐ Habilitar ☒ Desabilitar

Guest VLAN ID: (2-4094)

Aplicar

Configuração de Autenticação

Tempo de Silêncio: ☐ Habilitar ☒ Desabilitar

Intervalo de Silêncio: seg (1-999)

Repetição: (1-9)

Timeout Suplicante: seg (1-9)

Timeout Autenticador: seg (1-9)

Aplicar

Ajuda

Habilitando a autenticação radius

As seguintes informações são apresentadas na tela:

» Configuração global

802.1X: selecione *Habilitar/Desabilitar* para habilitar ou desabilitar a função 802.1X

Tipo de autenticação: selecione o método de autenticação.

» **EAP-MD5:** este método de autenticação utiliza o protocolo Extensible Authentication Protocol (EAP) para trocar informações entre o switch e o cliente. Estes pacotes EAP transportam dados de autenticação e podem ser encapsulados por um outro protocolo, como o RADIUS para serem transmitidos para o servidor de autenticação.

» **PAP:** este método de autenticação utiliza o protocolo Extensible Authentication Protocol (EAP) para trocar informações entre o switch e o cliente. A transmissão dos pacotes EAP é finalizada pelo switch e os Pacotes EAP são convertidos para o outro protocolo (por exemplo, RADIUS) para a transmissão de pacotes.

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

Guest VLAN ID: digite o ID desejado para a Guest VLAN. Os suplicantes na Guest VLAN podem acessar recursos da rede específica.

» Configuração de autenticação

Tempo de silêncio: selecione *Habilitar/Desabilitar* para habilitar ou desabilitar o tempo de silêncio.

Intervalo de silêncio: digite um valor para o período de silêncio, uma vez que o suplicante falhar ao tentar se autenticar via 802.1X, o switch não irá responder a mais pedidos do suplicante em um determinado período de tempo.

Repetição: especifica o tempo máximo entre pedidos de autenticações repetidas.

Timeout suplicante: digite o tempo máximo para o switch esperar pela resposta do suplicante antes de reenviar o pacote de solicitação ao suplicante.

Timeout autenticador: digite o tempo máximo para o switch esperar pela resposta do servidor de autenticação antes de reenviar o pacote de solicitação ao servidor de autenticação.

Portas 802.1X

Nesta página você pode configurar os recursos de autenticação 802.1X para as portas com base nas suas necessidades. Escolha o menu *Segurança* → *802.1X* → *Portas 802.1X* para carregar a seguinte página.

Configuração de Portas 802.1X

Porta

Selecionar

Selecionar	Porta	Status	Guest VLAN	Modo da Porta	Tipo de Controle	Autorizado	LAG
☐		Desabilitar	Desabilitar	Auto	Baseado em MAC		
☐	1	Desabilitar	Desabilitar	Auto	Baseado em MAC	Sim	---
☐	2	Desabilitar	Desabilitar	Auto	Baseado em MAC	Sim	---
☐	3	Desabilitar	Desabilitar	Auto	Baseado em MAC	Sim	---
☐	4	Desabilitar	Desabilitar	Auto	Baseado em MAC	Sim	---
☐	5	Desabilitar	Desabilitar	Auto	Baseado em MAC	Sim	---
☐	6	Desabilitar	Desabilitar	Auto	Baseado em MAC	Sim	---
☐	7	Desabilitar	Desabilitar	Auto	Baseado em MAC	Sim	---
☐	8	Desabilitar	Desabilitar	Auto	Baseado em MAC	Sim	---
☐	9	Desabilitar	Desabilitar	Auto	Baseado em MAC	Sim	---
☐	10	Desabilitar	Desabilitar	Auto	Baseado em MAC	Sim	---

Aplicar

Ajuda

Obs.:

A função 802.1X não pode ser habilitada em uma porta membro de um grupo LAG.

Portas 802.1X

As seguintes informações são apresentadas na tela:

» Configuração de portas 802.1X

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 802.1X na porta desejada.

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

Modo da porta: selecione o modo de funcionamento da porta desejada.

» **Auto:** neste modo, a porta irá operar normalmente após a realização da autenticação 802.1X.

» **Forçar autorização:** neste modo a porta irá operar normalmente sem a realização da autenticação 802.1X.

» **Não autorizado:** neste modo a porta estará inoperante e não participará do processo de autenticação 802.1X.

Tipo de controle: selecione o tipo de controle da porta desejada.

» **Baseado em MAC:** qualquer cliente conectado na porta deverá passar pela autenticação 802.1X para ter acesso na rede.

» **Baseado em porta:** todos os clientes conectados na porta podem acessar a rede, com a condição de que qualquer um dos clientes tenha passado na autenticação 802.1X.

Autorizado: exibe o status de autenticação da porta.

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

Servidor radius

Servidor RADIUS (Remote Authentication Dial-In User Service) fornece serviço de autenticação para o switch através de informações de clientes armazenadas, tais como o nome de usuário, senha, etc. Com a finalidade de controlar o estado de autenticação e contabilizar os clientes. Nesta página você pode configurar os parâmetros do servidor de autenticação.

Escolha o menu *Segurança* → *802.1X* → *Servidor Radius* para carregar a seguinte página.

Configuração do Servidor de Autenticação

Endereço IP Primário:

0.0.0.0

(Formato: 192.168.0.1)

Endereço IP Secundário:

0.0.0.0

(Formato: 192.168.0.1)

Porta de Autenticação:

1812

(1-65535)

Senha de Autenticação:

Aplicar

Configuração do Servidor de Contabilização

Contabilização:

☐ Habilitar ☒ Desabilitar

Endereço IP Primário:

0.0.0.0

(Formato: 192.168.0.1)

Endereço IP Secundário:

0.0.0.0

(Formato: 192.168.0.1)

Porta de Contabilização:

1813

(1-65535)

Senha de Contabilização:

Aplicar

Ajuda

Configuração do servidor radius

As seguintes informações são exibidas na tela:

- » **Configuração do servidor de autenticação**
 - Endereço IP primário:** digite o endereço IP do servidor de autenticação.
 - Endereço IP secundário:** digite o endereço IP do servidor de autenticação alternativo.
 - Porta de autenticação:** defina a porta UDP utilizada para a autenticação. Por padrão a porta é 1812.
 - Senha de autenticação:** digite a senha configurada no servidor de autenticação, para a realização da troca de mensagens.
 - » **Configuração do servidor de contabilização**
 - Contabilização:** selecione *Habilitar/Desabilitar* para habilitar ou desabilitar a função de contabilização.
 - Endereço IP primário:** endereço IP do servidor de contabilidade.
 - Endereço IP secundário:** digite o endereço IP do servidor de contabilidade alternativo.
 - Porta de contabilização:** defina a porta UDP utilizada para a contabilização. Por padrão a porta é 1813.
 - Senha de contabilização:** digite a senha configurada no servidor de contabilização, para a realização da troca de mensagens.
- Obs.:** » A função de 802.1X somente estará em funcionamento quando habilitada a função e também as portas participantes.
- » A função 802.1X não poderá ser habilitada para portas membros de um grupo LAG.
 - » A função 802.1X não deve ser habilitada na porta conectada ao servidor de autenticação. Além disso, os parâmetros de autenticação do switch e do servidor de autenticação devem ser os mesmos.

Procedimento de configuração

Passo	Operação	Descrição
1	Configurar Servidor Radius	Obrigatório, Registrar as informações dos clientes no servidor de autenticação e configurar o nome de usuário e senha de autenticação dos clientes no Servidor Radius.
2	Instalar software 802.1X cliente	Obrigatório, Para os computadores, é necessário instalar o software cliente de autenticação 802.1X, disponível para download no site www.intelbras.com.br
3	Habilitar a função 802.1X	Obrigatório, em Segurança → 802.1X → Configurar 802.1X, configurar a função 802.1X globalmente.
4	Configure os parâmetros para a autenticação no Servidor Radius	Obrigatório, em Segurança → 802.1X → Servidor Radius, configurar os parâmetros do servidor.
5	Configurar as Portas 802.1X	Obrigatório, em Segurança → 802.1X → Portas 802.1X, configurar a função 802.1X para a porta do switch baseado em suas necessidades.

12. 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

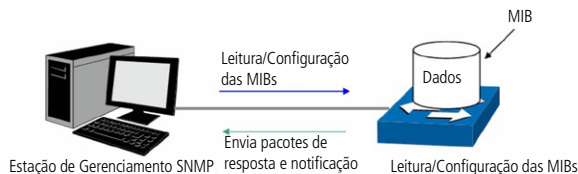
A estrutura de gerenciamento SNMP inclui três elementos de rede: estação de gerenciamento SNMP, agente SNMP e MIB (Management Information Base).

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 adequados às suas exigências de aplicação.

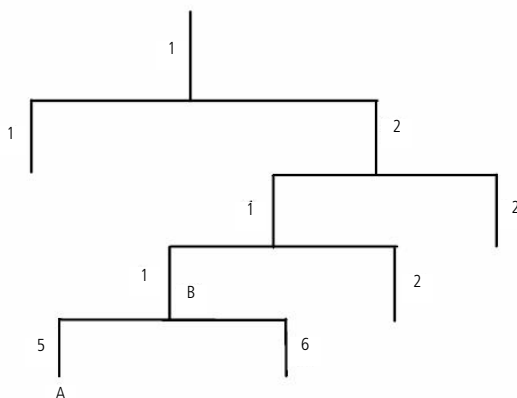
SNMP v1: o SNMPv1 adota autenticação utilizando o nome da comunidade. O nome da comunidade é usado para definir a relação entre a estação de gerenciamento SNMP e o agente SNMP. Os pacotes SNMP que não conseguirem aprovação de autenticação serão descartados.

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 sequência 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 sub-menus de configuração: *SNMP*, *Notificação* e *RMON*.

12.1. 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

SNMP: ☐ Habilitar ☒ Desabilitar Aplicar

Engine SNMP Local

Engine ID Local: (10-64 Hex) ID Padrão
Aplicar

Engine SNMP Remoto

Engine ID Remoto: (0 ou 10-64 Hex) Aplicar
Ajuda

Obs.:

O total dos caracteres hexadecimais dos Engines ID deverão ser o mesmo.

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.

Configurar View

Nome da View:

(16 caracteres no máximo)

MIB OID:

(61 caracteres no máximo)

Criar

Modo da View:

☒ Incluir ☐ Excluir

Views Configuradas

Selecionar	Nome da View	Modo da View	MIB OID
☐	viewDefault	Incluir	1
☐	viewDefault	Excluir	1.3.6.1.6.3.15
☐	viewDefault	Excluir	1.3.6.1.6.3.16
☐	viewDefault	Excluir	1.3.6.1.6.3.18

Todos

Remover

Ajuda

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.

Configuração do Grupo SNMP

Nome do Grupo SNMP:

(16 caracteres no máximo)

Versão SNMP:

v1

Nível de Segurança:

noAuthNoPriv

View de Leitura:

viewDefault

View de Escrita:

Nenhum

View de Notificação:

Nenhum

Criar

Limpar

Grupos SNMP Configurados

Selecionar	Grupo SNMP	Versão SNMP	Nível de Segurança	View de Leitura	View de Escrita	View de Notificação	Operação
Todos Remover Ajuda							

Obs.:

Um Grupo SNMP deverá conter pelo menos uma View de Leitura.

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:

Configuração de Usuário SNMP

Nome do Usuário: (16 caracteres no máximo)

Tipo do Usuário:

Usuário Local

Versão SNMP:

v1

Autenticação:

Nenhum

Criptografia:

Nenhum

Grupo SNMP:

Nível de Segurança:

noAuthNoPriv

Senha de Autenticação: (16 caracteres no máximo)

Senha de Criptografia: (16 caracteres no máximo)

Criar

Limpar

Usuários SNMP Configurados

Selecionar	Nome do Usuário	Tipo do Usuário	Grupo SNMP	Versão SNMP	Nível de Segurança	Autenticação	Criptografia	Operação

Todos

Remover

Ajuda

Obs.:

A versão e o nível de segurança do usuário SNMP deverá ser a mesma configurada para o Grupo SNMP a qual ele pertença.

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.

135

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:

Configuração de Comunidade SNMP

Nome da Comunidade:

(16 caracteres no máximo)

Modo de Acesso:

Leitura

MIB View:

viewDefault

Criar

Limpar

Comunidades SNMP Configuradas

Selecionar	Nome da Comunidade	Modo de Acesso	MIB View	Operação

Todos

Remover

Ajuda

Obs.:

A MIB View padrão é a viewDefault.

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 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.

12.2. 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:

Configuração de Notificação

Endereço IP:

Porta UDP:

162

Usuário:

Versão SNMP:

v1

Nível de Segurança:

noAuthNoPriv

Criar

Tipo de Notificação:

Trap

Limpar

Reenviar:

(1-255)

Tempo Máximo:

seg (1-3600)

Notificações Configuradas

Selecionar	Endereço IP	Porta UDP	Usuário	Versão SNMP	Nível de Segurança	Tipo de Notificação	Tempo Máximo	Reenviar	Operação
Todos Remover Ajuda									

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.

12.3. 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:

Configuração de Eventos RMON						
Selecionar	Índice	Usuário	Descrição	Tipo	Dono	Status
☐				Nenhum ▾		Desabilitar ▾
☐	1	public		Nenhum	monitor	Desabilitar
☐	2	public		Nenhum	monitor	Desabilitar
☐	3	public		Nenhum	monitor	Desabilitar
☐	4	public		Nenhum	monitor	Desabilitar
☐	5	public		Nenhum	monitor	Desabilitar
☐	6	public		Nenhum	monitor	Desabilitar
☐	7	public		Nenhum	monitor	Desabilitar
☐	8	public		Nenhum	monitor	Desabilitar
☐	9	public		Nenhum	monitor	Desabilitar
☐	10	public		Nenhum	monitor	Desabilitar
☐	11	public		Nenhum	monitor	Desabilitar
☐	12	public		Nenhum	monitor	Desabilitar

Aplicar

Ajuda

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	Porta 1	Absoluto	100	0	100	0	Ambos	1800	monitor	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.

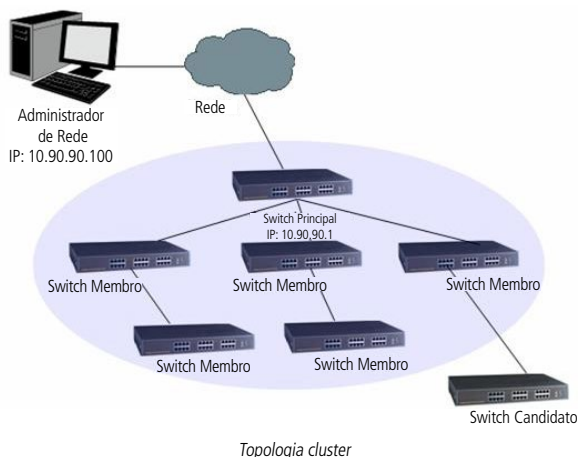
Obs.: quando as variáveis excedem o limite de alarme continuamente, um evento de alarme será gerado somente na primeira vez.

13. Cluster

Com o desenvolvimento das tecnologias, as redes foram ganhando grandes proporções, tornando-se necessário o aumento da quantidade de dispositivos e dificultando ainda mais a gestão destas redes. A função *Gerenciamento de Cluster* pode resolver esta questão. O administrador pode gerenciar e manter os switches no Cluster através do Switch Principal, que gerencia os demais switches da rede.

Obs.: o switch SG 1002 MR não possui a função de Switch Principal.

A figura a seguir, exibe uma topologia de cluster.



» Funções do switch

De acordo com as suas funções e status, o cluster de switches desempenham papéis diferentes. Você pode estabelecer a função que o switch deverá exercer.

Switch principal: indica que o switch pode configurar e gerenciar todos os dispositivos através do cluster. Descobre e determina quais os switches estão presentes na rede através das informações coletadas pelos protocolos NDP (Neighbor Discovery Protocol) e NTDP (Neighbor Topology Discovery Protocol).

Switch membro: indica os dispositivos gerenciados pelo Cluster.

Switch candidato: indica quais dispositivos não pertencem ao Cluster, porém podem ser incluídos no grupo.

Switch individual: indica o dispositivo que não deseja participar de nenhum Cluster.

As funções podem ser trocadas de um switch para o outro, seguindo as regras estabelecidas.

- » O switch que você criar o cluster será o Switch Principal.
- » O Switch Principal descobre e determina quais os switches estão presentes na rede através de determinados protocolos.
- » Após ser adicionado ao cluster, o Switch Candidato torna-se um Switch Membro.
- » Após ser removido do cluster, o Switch Membro torna-se um Switch Candidato.
- » O Switch Principal passa a ser o único Switch Candidato quando o cluster for excluído.

Introdução ao cluster: a função de cluster utiliza três protocolos de gerenciamento: NDP (Neighbor Discovery Protocol), NTDP (Neighbor Topology Discovery Protocol) e CMP (Cluster Management Protocol).

- » NDP: os switches utilizam o NDP para coletar informações dos switches diretamente conectados a ele, informações como, versão de Software, hostname, endereço MAC e número da porta conectada.
- » NTDP: os switches utilizam o NTDP para coletar informações dos switches que não estão diretamente conectados a ele, informações referente a topologia da rede e dispositivos com NTDP ativo.
- » CMP: protocolo utilizado pelo Switch Principal para gerenciamento dos switches dentro do cluster.

Obs.: o switch SG 1002 MR não pode ser configurado como Switch Principal para gerenciar demais switches em cluster.

13.1. NDP

Os switches utilizam o NDP para coletar informações dos switches diretamente conectados a ele, informações como, versão de software, hostname, endereço MAC e número da porta conectada. Caso sejam adicionados mais dispositivos na rede, o NDP coleta os dados e inclui na tabela. Caso seja retirado algum dispositivo, o NDP atualizará a tabela, removendo os dados do dispositivo antigo.

Esta função pode ser implementada nas páginas *Informações*, *Resumo NDP* e *Configurar NDP*.

Informações

Nesta página você pode visualizar as informações coletadas pelo protocolo NDP:

Escolha o menu *Cluster* → *NDP* → *Informações* para carregar a seguinte página:

Pesquisa de Dispositivo Vizinho

Opção de procura:

Todas

Procurar

Informações NDP					
Porta Nativa	Porta Remota	Nome do Dispositivo	Endereço MAC	Versão de Firmware	Aging Time(seg)
Porta 08	Porta 07	SF 2842 MR	90-F6-52-30-41-F0	1.0.0 Build 20130624 Rel.40517	139

Atualizar

Ajuda

Informações dos vizinhos

As seguintes opções são exibidas na tela:

- » Pesquisa de dispositivo vizinho
 - Opção de procura:** selecione a opção desejada. Em seguida, clique no botão *Procurar* para exibir as informações da tabela.
- » Informações NDP
 - Porta nativa:** exibe o número da porta do switch local.
 - Porta remota:** exibe o número da porta do switch remoto.
 - Nome do dispositivo:** exibe o nome do switch remoto.
 - Endereço MAC:** exibe o endereço MAC do switch remoto.
 - Versão de firmware:** exibe a versão do firmware do switch remoto.
 - Aging Time (seg.):** exibe o período que o switch local manterá as informações coletadas do switch remoto.

Resumo NDP

Nesta página você pode visualizar a configuração NDP do switch.
Escolha o menu *Cluster* → *NDP* → *Resumo NDP* para carregar a seguinte página:

Resumo da configuração NDP

NDP:

Desabilitar

Aging Time:

180seg

Hello Time:

60seg

Portas NDP

Porta	NDP	Pacotes NDP enviados	Pacotes NDP recebidos	Pacotes NDP Erros	Vizinhos	Detalhes
1	Habilitar	0	0	0	0	Detalhes
2	Habilitar	0	0	0	0	Detalhes
3	Habilitar	0	0	0	0	Detalhes
4	Habilitar	0	0	0	0	Detalhes
5	Habilitar	0	0	0	0	Detalhes
6	Habilitar	0	0	0	0	Detalhes
7	Habilitar	0	0	0	0	Detalhes
8	Habilitar	0	0	0	0	Detalhes
9	Habilitar	0	0	0	0	Detalhes
10	Habilitar	0	0	0	0	Detalhes

Atualizar

Ajuda

Estatísticas NDP

- As seguintes opções são exibidas na tela:
- » **Resumo da configuração NDP**
 - NDP:** exibe o status do NDP (Habilitado/Desabilitado).
 - Aging time:** exibe o período que o switch local manterá as informações coletadas do switch remoto.
 - Hello time:** exibe o intervalo de envio de pacotes NDP.
 - » **Portas NDP**
 - Porta:** exibe o número da porta do switch.
 - NDP:** exibe o status do NDP (Habilitado/Desabilitado) na porta desejada.
 - Pacotes NDP enviados:** exibe a quantidade de pacotes NDP enviados.
 - Pacotes NDP recebidos:** exibe a quantidade de pacotes NDP recebidos.
 - Pacotes NDP erros:** exibe a quantidade de pacotes de erro NDP recebidos.
 - Vizinhos:** exibe a quantidade de dispositivos conectados a rede.
 - Detalhes:** exibe as informações completas coletadas pelo protocolo NDP na porta correspondente.

Configurar NDP

Nesta página você pode configurar a função NDP.
Escolha o menu *Cluster* → *NDP* → *Configurar NDP* para carregar a seguinte página:

Configuração NDP

NDP:

☐ Habilitar ☒ Desabilitar

Aging Time:

seg (5-255, padrão: 180)

Hello Time:

seg (5-254, padrão: 60)

Aplicar

Configuração das Portas NDP

Selecionar	Porta	NDP	Selecionar	Porta	NDP
☐	1	Habilitar	☐	2	Habilitar
☐	3	Habilitar	☐	4	Habilitar
☐	5	Habilitar	☐	6	Habilitar
☐	7	Habilitar	☐	8	Habilitar
☐	9	Habilitar	☐	10	Habilitar

TodasHabilitarDesabilitarAjuda

Configuração NDP

As seguintes opções são exibidas na tela:

- » **Configuração NDP**
NDP: selecione Habilitar/Desabilitar para habilitar ou desabilitar a função NDP.
Aging time: digite o período que será mantido as informações NDP coletadas do switch remoto.
Hello time: digite o intervalo de envio de pacotes NDP.
 - » **Configuração das portas NDP**
Selecionar: selecione a porta que deseja habilitar o NDP.
Porta: exibe o número da porta do switch.
NDP: exibe o status do NDP (Habilitado/Desabilitado).
Habilitar: selecione a porta desejada e clique no botão *Habilitar* para ativar a função NDP.
Desabilitar: selecione a porta desejada e clique no botão *Desabilitar* para desativar a função NDP.
- Obs.:** a função NDP somente estará em operação após as portas participantes serem habilitadas.

13.2. NTDP

Os switches utilizam o NTDP para coletar informações dos switches que não estão diretamente conectados a ele, informações referente a topologia da rede e dispositivos com NTDP ativo.

Saltos NTDP intervalo: indica o tempo de resposta entre a solicitação do switch e o recebimento dos pacotes informando os saltos dos dispositivos conectados à rede.

Portas NTDP intervalo: indica o tempo de resposta entre a porta que solicita os pacotes do switch e o recebimento dos pacotes enviados pelos switches conectados diretamente à rede.

A função NTDP pode ser implementada na página *Dispositivos*, *Resumo NTDP* e *Configurar NTDP*.

Dispositivos

Nesta página você pode visualizar as informações dos switches conectados diretamente às redes, coletadas através do NTDP. Não importa se o Cluster está estabelecido. Você pode receber as informações NTDP a qualquer momento, desde que a função esteja habilitada.

Selecione o menu *Cluster* → *NTDP* → *Dispositivos* para carregar a seguinte página:

Tabela de Dispositivo NTDP					
Dispositivo	Endereço MAC	Nome do Cluster	Função	Salto	Informações
SF 2842 MR 1.0	90-F6-52-30-41-F0		Candidato	1	Detalhes
SG 1002 MR 1.0	A0-F3-C1-05-F9-90		Candidato	0	Detalhes

Coletar Topologia

Atualizar

Ajuda

Tabela de dispositivos

As seguintes opções são exibidas na tela:

» Tabela de dispositivo NTDP

- Dispositivo:** exibe a descrição coletada do dispositivo através do NTDP.
- Endereço MAC:** exibe o endereço MAC do dispositivo.
- Nome do cluster:** exibe o nome do Cluster do dispositivo.
- Função:** exibe a função do dispositivo no cluster.
- » **Switch principal:** indica o dispositivo que pode configurar e gerenciar todos os dispositivos no Cluster.
 - » **Membro:** indica o dispositivo que é membro do Cluster.
 - » **Candidato:** indica os dispositivos que não estão incluídos no Cluster, porém podem ser adicionados.
 - » **Individual:** indica os dispositivos que não participam de nenhum Cluster.
- Salto:** exibe a quantidade de saltos até o switch remoto.
- Informações:** clique no botão *Detalhes* para visualizar todas as informações dos dispositivos.
- Coletar topologia:** clique no botão *Coletar Topologia* para o protocolo NTDP iniciar a coleta de informações dos switches e de sua topologia de rede mais recente.

Clique no botão *Detalhes* para visualizar todas as informações dos dispositivos.

Informação dos Dispositivos					
Nome do Dispositivo:	SF 2842 MR				
Endereço MAC:	90-F6-52-30-41-F0				
Salto:	1				
Dispositivo:	1.0				
Endereço IP:	192.168.0.1				
Versão de Firmware:	1.0.0 Build 20130624 Rel.40517				
Informações do Cluster:	Candidato				

Informações				
Porta Nativa	Porta Remota	Endereço MAC	Velocidade (Mbit/s)	Duplex
Porta 07	Porta 08	A0-F3-C1-05-F9-90	100	Full Duplex

Voltar

Informações do dispositivo corrente

Resumo NTDP

Nesta página você pode visualizar a configuração do NTDP.
Escolha o menu *Cluster* → *NTDP* → *Resumo NTDP* para carregar a seguinte página:

Resumo NTDP

NTDP:

Desabilitar

Intervalo NTDP:

1min

Saltos NTDP:

3salto

Salto NTDP Intervalo:

200ms

Portas NTDP Intervalo:

20ms

Portas NTDP

Porta	NTDP	Porta	NTDP
1	Habilitar	2	Habilitar
3	Habilitar	4	Habilitar
5	Habilitar	6	Habilitar
7	Habilitar	8	Habilitar
9	Habilitar	10	Habilitar

Atualizar

Ajuda

Resumo NTDP

- » **Resumo NTDP**
NTDP: exibe o status do NTDP (Habilitado/Desabilitado).
Intervalo NTDP: exibe o intervalo de tempo para coletar as informações de topologia.
Saltos NTDP: exibe a contagem de saltos da topologia coletada.
Salto NTDP intervalo: indica o tempo de resposta entre a solicitação do switch e o recebimento dos pacotes informando os saltos dos dispositivos conectados à rede.
Portas NTDP intervalo: indica o tempo de resposta entre a porta de solicitação de pacotes do switch e o recebimento dos pacotes enviados pelos switches conectados diretamente à rede.
- » **Portas NTDP**
Porta: exibe o número da porta do switch.
NTDP: exibe o status do NTDP Habilitado/Desabilitado.

Configurar NTDP

Nesta página você pode configurar o NTDP.
Escolha o menu *Cluster* → *NTDP* → *Configurar NTDP* para carregar a seguinte página:

Configuração NTDP

NTDP:

☐ Habilitar ☒ Desabilitar

Intervalo NTDP:

min (1-60, padrão: 1)

Salto NTDP:

saltos (1-16, padrão: 3)

Salto NTDP Intervalo:

ms (1-1000, padrão: 200)

Porta NTDP Intervalo:

ms (1-100, padrão: 20)

Aplicar

Configuração das portas NTDP

Selecionar	Porta	NTDP	Selecionar	Porta	NTDP
☐	1	Habilitar	☐	2	Habilitar
☐	3	Habilitar	☐	4	Habilitar
☐	5	Habilitar	☐	6	Habilitar
☐	7	Habilitar	☐	8	Habilitar
☐	9	Habilitar	☐	10	Habilitar

Todas

Habilitar

Desabilitar

Ajuda

Configuração NTDP

As seguintes opções são exibidas na tela:

- » **Configuração NTDP**
NTDP: selecione Habilitar/Desabilitar para habilitar ou desabilitar a função NDP.
Intervalo NTDP: selecione o intervalo de tempo para coleta de informações da topologia da rede.
Salto NTDP: digite a quantidade de saltos utilizado pela coleta de informações.
Salto NTDP intervalo: digite o tempo de resposta entre a solicitação do switch e o recebimento dos pacotes informando os saltos dos dispositivos conectados à rede.
Porta NTDP intervalo: digite o tempo de resposta entre a porta de solicitação de pacotes do switch e o recebimento dos pacotes enviados pelos switches conectados diretamente à rede.
 - » **Configuração das portas NTDP**
Selecionar: selecione a porta desejada.
Porta: exibe o número da porta do switch.
NTDP: exibe o status da função NTDP.
Habilitar: selecione a porta desejada e clique no botão *Habilitar* para ativar a função NTDP.
Desabilitar: selecione a porta desejada e clique no botão *Desabilitar* para desativar a função NTDP.
- Obs.:** a função NTDP somente estará em operação após as portas participantes serem habilitadas.

13.3. Cluster

O Switch Principal é capaz de reconhecer e adicionar automaticamente Switches Candidato ao Cluster baseados nas informações NDP e NTDP. Também é possível adicionar manualmente um Switch candidato a um Cluster. Se o switch é adicionado com êxito ao Cluster, ele irá obter um Endereço IP atribuído pelo Switch Principal.

Obs.: o switch SG 1002 MR não pode ser configurado como Switch Principal.

A função de Cluster pode ser implementada na página *Status* e *Configurar Cluster*.

Status

Nesta página você pode visualizar o status do Cluster corrente.
Escolha o menu *Cluster* → *Cluster* → *Status* para carregar as seguintes páginas:
» Para o switch configurado como *Candidato*, a seguinte página será exibida.

Configuração Global

Cluster:	Habilitar
Função do Cluster:	Candidato

Atualizar

Ajuda

Status do switch candidato

As seguintes opções são exibidas na tela:
» **Configuração global**
Cluster: exibe o status do Cluster Habilitado ou Desabilitado.
Função do cluster: exibe a função do switch no Cluster.
» Para o switch configurado como *Membro*, a seguinte página será exibida:

Configuração Global

Cluster:	Habilitar
Função do Cluster:	Membro
Nome do Cluster:	INTELBRAS
MAC Switch Principal:	00-EB-A5-C5-55-C0

Atualizar

Ajuda

Status do switch membro

As seguintes opções são exibidas na tela:
» **Configuração global**
Cluster: exibe o status do Cluster Habilitado ou Desabilitado.
Função do cluster: exibe a função do switch no Cluster.
Nome do cluster: exibe o nome do Cluster do qual o switch pertence.
MAC switch principal: exibe o endereço MAC do Switch Principal.
» Para o switch configurado como *Individual*, a seguinte página será exibida:

Configuração Global

Cluster:	Desabilitar
Função do Cluster:	Individual

Atualizar

Ajuda

Status do switch individual

As seguintes opções são exibidas na tela:

» **Configuração global**

Cluster: exibe o status do Cluster Habilitado ou Desabilitado.

Função do cluster: exibe a função do switch no Cluster.

Configurar cluster

Nesta página você pode configurar a função do switch no Cluster

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

- » Para o switch configurado como *Candidato*, a seguinte página será exibida:

Função Atual

Função:

Candidato

Alterar Função

Alterar Função:

☒ Individual

Aplicar

Ajuda

Configurar o switch como candidato

As seguintes opções são exibidas na tela:

» **Função atual**

Função: exibe a função atual do switch no Cluster.

» **Alterar função**

Individual: ao clicar no botão *Aplicar*, o switch mudará sua função para *Individual*.

- » Para o switch configurado como *Individual*, a seguinte página será exibida:

Função Atual

Função:

Individual

Alterar Função

☒ Candidato

Aplicar

Ajuda

Configurar o switch como individual

As seguintes opções são exibidas na tela:

» **Função atual**

Função: exibe a função atual do switch no Cluster.

» **Alterar função**

Candidato: ao clicar no botão *Aplicar*, o switch mudará sua função para *Candidato*.

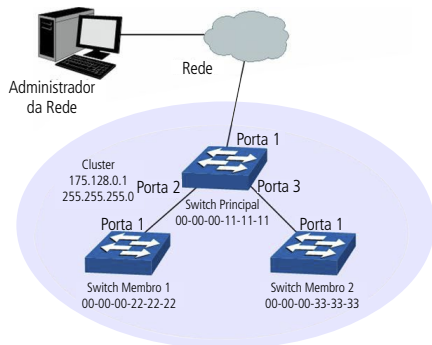
13.4. Exemplo de aplicação da função cluster

» **Requisitos de rede**

Três switches formam um Cluster. Um será o Switch Principal e dois serão membros. O administrador gerencia todos os switches do Cluster através do Switch Principal.

- » Na porta 1 do Switch Principal conecta-se a rede externa, na porta 2 conecta-se ao switch membro 1 e na porta 3 o switch membro 2.
- » Endereço IP: 175.128.0.1, Máscara: 255.255.255.0

» **Diagrama da rede**



Aplicação da função cluster

» **Procedimento de configuração**

- » Configuração dos Switches Membros:

Step	Operation	Description
1	Habilitar a função NDP no switch na porta 1.	Na página Cluster→NDP→NDP Configurar NDP, habilitar a função NDP.
2	Habilitar a função NTDP no switch na porta 1.	Na página Cluster→NTDP→ Configurar NTDP, habilitar a função NTDP.

- » Configuração do Switch Principal:

Step	Operation	Description
1	Habilitar a função NDP no switch nas portas 1, 2 e 3.	Na página Cluster→NDP→ Configurar NDP, habilitar a função NDP.
2	Habilitar a função NTDP no switch nas portas 1, 2 e 3.	Na página Cluster→NTDP→ Configurar NTDP, habilitar a função NTDP.
3	Crie um Cluster e configure os parâmetros relacionados.	Na página Cluster→Cluster→ Configurar Cluster, configure a função do switch como Switch Principal e insira as informações relacionadas. Endereço IP: 175.128.0.1 Máscara: 255.255.255.0
4	Configuração do Switch Membro.	Na página Cluster→Cluster→ Configurar Membro, selecionar o Switch Membro e clicar em Gerenciar para logar na interface de gerenciamento.

14. Manutenção

No menu *Manutenção* é possível utilizar ferramentas para o diagnóstico da rede, fornecendo métodos para localização e solução de problemas.

- 1. Monitoramento: monitora o status de utilização da memória e da CPU do switch.
- 2. Log: verifica os parâmetros de configuração do switch para descoberta de eventuais erros.
- 3. Testar cabo: testa o status da conexão do cabo para localizar e diagnosticar problemas da rede.
- 4. Loopback: testa se as portas do switch e seu dispositivo conectado estão disponíveis.
- 5. Diagnóstico: testa se o dispositivo de destino é alcançável e detecta os saltos a partir do switch até o dispositivo de destino.

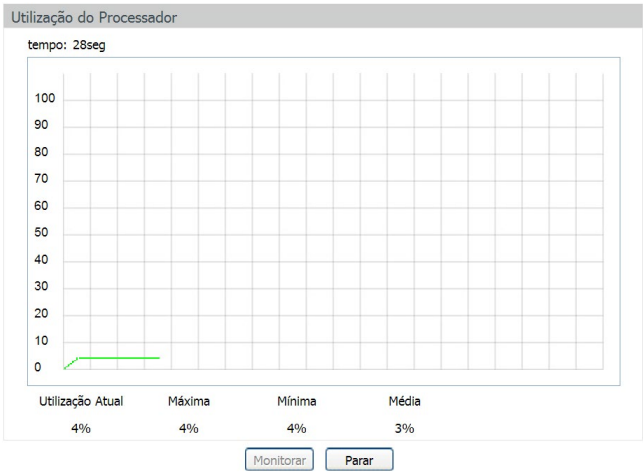
14.1. Monitoramento

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.

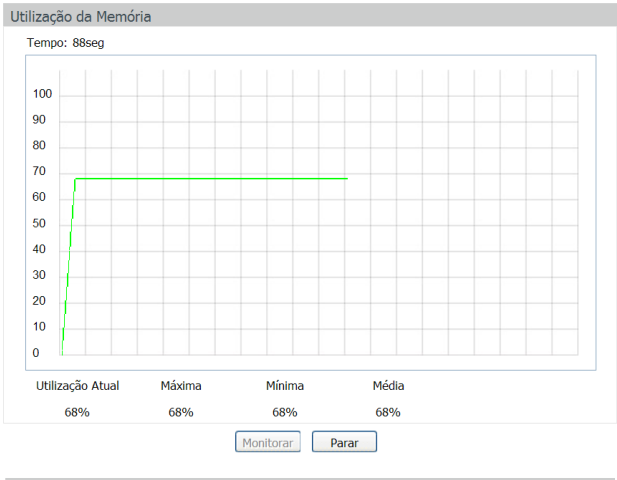


Monitoramento da CPU

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.

14.2. 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:

Informações de Log				
Índice	Data/Hora	Módulo	Nível de Criticidade	Conteúdo
		Todos Módulos	Todos Níveis	
1	2013-08-20 17:00:19	ARP&IP	Nível_5	Enable ARP Defend on port 3, speed value is 15pps.
2	2013-08-20 11:37:32	Cluster	Nível_4	Succeed to change role to individual.
3	2013-08-20 11:35:29	Cluster	Nível_4	Succeed to change role to candidate.
4	2013-08-20 11:33:34	Cluster	Nível_4	Succeed to change role to individual.
5	2013-08-20 11:32:42	Cluster	Nível_4	Succeed to change role to candidate.
6	2013-08-20 11:13:51	Cluster	Nível_4	Succeed to change role to individual.
7	2013-08-20 09:59:31	Cluster	Nível_4	Succeed to set NTDP global config.
8	2013-08-20 09:59:26	Cluster	Nível_4	Succeed to set NDP global config.
9	2013-08-19 16:26:59	ACL	Nível_5	Created new ACL 199.
10	2013-08-19 16:26:55	ACL	Nível_5	Created policy testes.
11	2013-01-01 12:00:10	SNMP	Nível_5	SNMP initialization OK.
12	2013-01-01 12:00:00	Binding	Nível_5	DHCP Snooping intialzation OK.
13	2013-01-01 12:00:00	Binding	Nível_5	DHCP Snooping message register OK.
14	2013-01-01 12:00:00	Binding	Nível_5	ARP Scanning initialization OK.
15	2013-01-01 12:00:00	Binding	Nível_5	ARP Scanning message register OK.
16	2013-01-01 12:00:00	LACP	Nível_5	LACP register OK.
17	2013-01-01 12:00:00	GVRP	Nível_5	GVRP module initialization OK.
18	2013-01-01 12:00:00	QoS	Nível_5	QoS module initialization OK.
		Atualizar	Ajuda	

Obs.:

- 1.Existem 8 Níveis de Criticidade (0-7). Quanto menor o valor maior a prioridade.
- 2.Esta tabela apresenta os últimos 512 eventos ocorridos no Log de Memória RAM.

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:

Configuração de Log Local			
Selecionar	Canal	Nível de Criticidade	Status
☐			
☐	Log de memória RAM	Nível_7	Habilitar
☐	Log de memória FLASH	Nível_4	Habilitar

Aplicar

Ajuda

Obs.:

- 1.Existem 2 Canais de Log Local: Log de Memória RAM e Log de Memória FLASH.
- 2.Existem 8 Níveis de Criticidade (0-7). Quanto menor o valor maior a prioridade.

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:

Servidores de Log Remotos					
Selecionar	Índice	Endereço IP	Porta UDP	Nível de Criticidade	Status
☐					
☐	1	0.0.0.0	514	Nível_6	Desabilitar
☐	2	0.0.0.0	514	Nível_6	Desabilitar
☐	3	0.0.0.0	514	Nível_6	Desabilitar
☐	4	0.0.0.0	514	Nível_6	Desabilitar

Aplicar

Ajuda

Obs.:

- 1.É possível direcionar os logs para até 4 Servidores Log Remotos.
- 2.Existem 8 Níveis de Criticidade (0-7). Quanto menor o valor maior a prioridade.

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

Clique no botão Backup de Log para salvar o log em um arquivo:

Backup de Log

Ajuda

Obs.:

Poderá levar alguns minutos para realizar o backup do arquivo de log. Por favor, aguarde sem executar qualquer operação.

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 realizar o backup do arquivo de Log. Por favor, aguarde sem executar qualquer operação.

14.3. 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 do Cabo

Porta: --

Unidade: metros

Par	Status	Comprimento	Erro
Par A	--	--	--
Par B	--	--	--
Par C	--	--	--
Par D	--	--	--

Testar

Ajuda

Obs.:

- 1. O intervalo entre dois testes de cabo deverá ser maior que 3 segundos.
- 2. O resultado terá maior precisão quando o par do cabo de rede estiver com o status normal.
- 3. O resultado é apenas para sua informação.

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.

Status: exibe o status da conexão do cabo de rede conectado à porta. Os resultados do teste do cabo incluem: normal, fechado, aberto ou impedância.

Comprimento: se o status do link for normal, será exibido o comprimento do cabo.

Erro: se o status do link for fechado, aberto ou impedância não será exibido o comprimento do cabo.

Obs.: » *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.

Configuração de Loopback

Tipo do Loopback: ☒ Interno ☐ Externo

Portas					
☐ 1	☐ 2	☐ 3	☐ 4	☐ 5	☐ 6
☐ 7	☐ 8	☐ 9	☐ 10		

Testar

Ajuda

Resultado do teste Loopback

Porta: N/A
Tipo: N/A
Resultado: N/A

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.

14.4. 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:

Configuração de Ping

IP de destino:

Repetição: (1-10)

Tamanho: byte (1-1024)

Intervalo: miliseg (100-1000)

Ping

Ajuda

Resultado do Ping

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

Endereço IP:

Limite de Salto: Salto (1-30)

Tracert

Ajuda

Resultado

Tracert

As seguintes opções são apresentadas na tela:

» Tracert

Endereço IP: digite o endereço IP do dispositivo de destino.

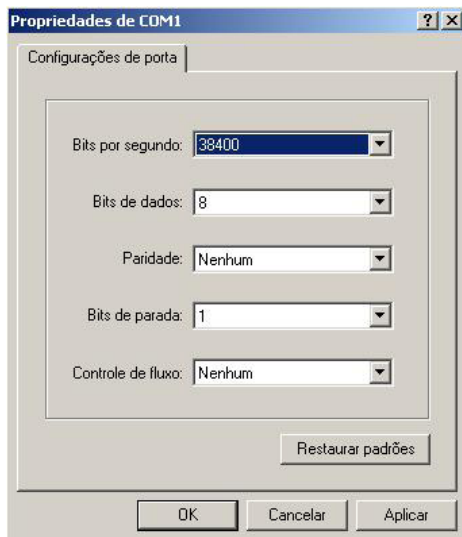
Limite de salto: digite o número máximo de saltos que poderá ser realizado até o destino.

15. Restaurando para o padrão de fábrica

Para restaurar as configurações de fábrica do switch, deverá ser acessado o menu BootUtil via porta console, conforme instruções a seguir:

Acessando o menu BootUtil utilizando o hyper terminal:

Para exibir a interface de linha de comandos, conecte a extremidade (DB-9 fêmea) do cabo console na respectiva porta serial (COM) do computador e a outra extremidade (RJ45) na porta console (RJ45), localizada no painel frontal do switch. Abra o software Hyper Terminal com as seguintes configurações:



Configurando o hyper terminal

Taxa de dados: 38400 bits por segundo.

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

Controle de fluxo: nenhum.

Para restaurar as configurações de fábrica do switch, é necessário entrar no menu BootUtil do switch, conforme os passos a seguir:

1. Com o PC conectado ao switch através da porta console, abra o software Hyper Terminal previamente configurado.
2. Desconecte e conecte o switch da rede elétrica. Quando lhe for pedido "Press CTRL-B to enter the bootUtil" no Hyper Terminal, por favor pressione as teclas **CTRL + B** para acessar o menu bootUtil, conforme imagem a seguir:

```
*****
*      INTELBRAS  BOOTUTIL(v1.0.0)      *
*****
Copyright (c) 2012 Intelbras S.A.
Create Date: Mar 30 2012 17:35:10

help          - print this list
reboot        - reboot the system
ifconfig      - config the interface
ftp           - config the remote host ip, the user name, user password
and the image file name
upgrade       - upgrade the firmware
start         - start the system
reset         - reset the system to the factory config.

[INTELBRAS]:
```

Menu BootUtil

Obs.: o processo entre ligar o switch e pressionar as teclas CTRL + B é extremamente rápido, recomendamos que as teclas CTRL + B sejam pressionadas no momento em que o switch está sendo ligado.

Após ter acessado o menu BootUtil, realize os seguintes comandos:

- » **Reset** (para restaurar o switch com as configurações de fábrica, conforme imagem a seguir).

```
*****
*      INTELBRAS  BOOTUTIL(v1.0.0)      *
*****
Copyright (c) 2012 Intelbras S.A.
Create Date: Mar 30 2012 17:35:10

help          - print this list
reboot        - reboot the system
ifconfig      - config the interface
ftp           - config the remote host ip,the user name,user password
and the image file name
upgrade       - upgrade the firmware
start         - start the system
reset         - reset the system to the factory config.

[INTELBRAS]: reset_
```

Menu BootUtil - restaurar

- » **Reiniciar** (para reiniciar o switch com as configurações de fábrica, conforme imagem a seguir).

```
*****
*      INTELBRAS  BOOTUTIL(v1.0.0)      *
*****
Copyright (c) 2012 Intelbras S.A.
Create Date: Mar 30 2012 17:35:10

help          - print this list
reboot        - reboot the system
ifconfig      - config the interface
ftp           - config the remote host ip,the user name,user password
and the image file name
upgrade       - upgrade the firmware
start         - start the system
reset         - reset the system to the factory config.

[INTELBRAS]: reset
[INTELBRAS]: reboot_
```

Menu BootUtil - reiniciar

Termo de garantia

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

Nome do cliente:

Assinatura do cliente:

Nº da nota fiscal:

Data da compra:

Modelo:

Nº de série:

Revendedor:

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

1. Todas as partes, peças e componentes do produto são garantidos contra eventuais defeitos de fabricação que porventura venham a apresentar, pelo prazo de 3 (três) anos, sendo este prazo de 3 (três) meses de garantia legal mais 33 (trinta e três) meses de garantia contratual, contado a partir da data de entrega do produto ao Senhor Consumidor, conforme consta na nota fiscal de compra do produto, que é parte integrante deste Termo em todo território nacional. Esta garantia contratual implica na troca gratuita das partes, peças e componentes que apresentarem defeito de fabricação, além da mão-de-obra utilizada nesse reparo. Caso não seja constatado defeito de fabricação, e sim defeito(s) proveniente(s) de uso inadequado, o Senhor Consumidor arcará com estas despesas.
2. Constatado o defeito, o Senhor Consumidor deverá imediatamente comunicar-se com o Serviço Autorizado mais próximo que consta na relação oferecida pelo fabricante - somente estes estão autorizados a examinar e sanar o defeito durante o prazo de garantia aqui previsto. Se isto não for respeitado esta garantia perderá sua validade, pois o produto terá sido violado.
3. Na eventualidade do Senhor Consumidor solicitar o 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, transporte, segurança de ida e volta do produto, ficam sob a responsabilidade do Senhor Consumidor.
4. A garantia perderá totalmente sua validade se ocorrer qualquer das hipóteses a seguir: a) se o defeito não for de fabricação, mas sim, ter sido causado pelo Senhor Consumidor ou 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 decorrente 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 houver sido adulterado ou rasurado; e) se o aparelho houver sido violado.

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

O processo de fabricação deste produto não está coberto pelo sistema de gestão ambiental da Intelbras.

Todas as imagens deste manual são ilustrativas.

intelbras



eco amigável



uma das melhores
empresas para se trabalhar



fale com a gente

Suporte a clientes: (48) 2106 0006

Contato e chat: www.intelbras.com.br/suporte

Sugestões, reclamações e rede autorizada: 0800 7042767

Intelbras S/A – Indústria de Telecomunicação Eletrônica Brasileira
Rodovia BR 101, km 213 - Área Industrial - São José/SC - 88104-800
www.intelbras.com.br