Manual de Utilização
Switch JN4508F-M

Rev. B 07/2016

Cod. Doc.: MU225000

altus

www.altus.com.br

Conforme o Código de Defesa do Consumidor vigente no Brasil, informamos, a seguir, aos clientes que utilizam nossos produtos aspectos relacionados com a segurança de pessoas e instalações.

Os equipamentos de automação industrial fabricados pela Altus são robustos e confiáveis devido ao rígido controle de qualidade a que são submetidos. No entanto, equipamentos eletrônicos de controle industrial (controladores programáveis, comandos numéricos, etc.) podem causar danos às máquinas ou processos por eles controlados em caso de defeito em suas partes e peças ou de erros de programação ou instalação, podendo inclusive colocar em risco vidas humanas.

O usuário deve analisar as possíveis consequências destes defeitos e providenciar instalações adicionais externas de segurança que, em caso de necessidade, sirvam para preservar a segurança do sistema, principalmente nos casos da instalação inicial e de testes.

Os equipamentos fabricados pela Altus não trazem riscos ambientais diretos, não emitindo nenhum tipo de poluente durante sua utilização. No entanto, no que se refere ao descarte dos equipamentos, é importante salientar que quaisquer componentes eletrônicos incorporados em produtos contêm materiais nocivos à natureza quando descartados de forma inadequada. Recomenda-se, portanto, que quando da inutilização deste tipo de produto, o mesmo seja encaminhado para usinas de reciclagem que deem o devido tratamento para os resíduos.

É imprescindível a leitura completa dos manuais e/ou características técnicas do produto antes da instalação ou utilização do mesmo.

Os exemplos e figuras deste documento são apresentados apenas para fins ilustrativos. Devido às possíveis atualizações e melhorias que os produtos possam incorrer, a Altus não assume a responsabilidade pelo uso destes exemplos e figuras em aplicações reais. Os mesmos devem ser utilizados apenas para auxiliar na familiarização e treinamento do usuário com os produtos e suas características.

A Altus garante os seus equipamentos conforme descrito nas Condições Gerais de Fornecimento, anexada às propostas comerciais.

A Altus garante que seus equipamentos funcionam de acordo com as descrições contidas explicitamente em seus manuais e/ou características técnicas, não garantindo a satisfação de algum tipo particular de aplicação dos equipamentos.

A Altus desconsiderará qualquer outra garantia, direta ou implícita, principalmente quando se tratar de fornecimento de terceiros.

Os pedidos de informações adicionais sobre o fornecimento e/ou características dos equipamentos e serviços Altus devem ser feitos por escrito. A Altus não se responsabiliza por informações fornecidas sobre seus equipamentos sem registro formal.

DIREITOS AUTORAIS

Sumário

1. Introdução

O switch JN4508F-M é um switch industrial rápido gerenciável, equipado com 6 portas 10/100 Mbps mais 2 portas RJ-45 de uplink de fibra de 100Mbps. Combinado com recursos de gerenciamento de L2, juntamente com o LLDP e alta confiabilidade do sistema, incluindo a MSR e de rede MSTP tecnologias de redundância, para assegurar em tempo real e conectividade de alta qualidade em várias aplicações de redes.

O JN4508F-M adotou como padrão de fábrica 32Gbps para entregar em tempo real e sem parada de transmissão, alta performance, assim satisfazendo a necessidade de altas bandas de transmissão que as aplicações exigem, assegurando ao mesmo tempo alto desempenho de tráfego, sem perda de dados. Além disso, o novo projeto de hardware inclui um sistema de cão-de-guarda temporizado, para manter o sistema operacional em execução. Ele também fornece redundância de alimentação com ampla disponibilidade de tensão de entrada DC10V ~ 60V para garantir a continuidade de energia no sistema.

Com um design robusto com mecânica IP31, JN4508F-M fornece transmissão de dados com alta confiabilidade e segurança em ambientes industriais severos Para construir uma infraestrutura Ethernet industrial inteligente eficiente em termos de custo, JN4508F-M é a melhor escolha.

Características Inovadoras

O JN4508F-M apresenta as seguintes características:

- 32Gbps Non-Blocking, Tabela de endereços MAC de até 8K
- Multiple Super Ring (tempo de recuperação <5 ms), o Rapid Dual Homing, Multiple Ring, e MSTP / RSTP
- IEEE 1588 protocolo de precisão de tempo para a sincronização de tempo exata
- VLAN, VLAN privada, QinQ, GVRP, QoS, IGMP Snooping V1 / V2 / V3, controle de freqüência, Port Trunking, LACP, on-line Multi-Port Mirroring
- IEEE 802.1AB LLDP e JetView Pro NMS i2 para auto-topologia e gestão de grupo
- Suporta SNMP, Múltipla Línguagem Web UI, Telnet In-Band, Gerenciamento Out-Band Serial
- Suporta Modbus TCP / função de cliente para o sistema HMI
- Cão-de-guarda de Hardware incorporado para salvamento automático do sistema
- Dupla entrada DC10 ~ 60V, entradas de alimentação com redundância
- Alarme de Saída configurável por software

Dados para Compra

Itens Integrantes

A embalagem do produto contém os seguintes itens:

- Um switch - JN4508F-M
- Um clip para trilho DIN
- Um cabo RS-232 DB-9 para RJ-45 (console)

Se qualquer um dos itens acima estiver faltando ou danificado, entre em contato com seu representante de vendas local.

Documentos Relacionados a este Manual

Para obter informações adicionais sobre a Série Connect, outros documentos específicos, além deste, devem ser consultados. Esses documentos estão disponíveis em sua última revisão em www.altus.com.br.

Considerações Gerais sobre a Documentação ALTUS

Cada produto possui um documento denominado características técnicas (CT), o qual descreve as suas peculiaridades. Adicionalmente, o produto pode possuir Manuais de Utilização (os códigos dos manuais, se aplicável, são sempre citados nas CTs dos respectivos módulos).

Documentação de Suporte

É aconselhável consultar os seguintes documentos como fonte de informações adicionais:

Código	Descrição	Idioma
CE125000	Connect Series – Technical Characteristics	Inglês
CT125000	Série Connect – Características Técnicas	Português
CS125000	Serie Connect – Especificaciones Tecnicas	Espanhol

Inspeção Visual

Antes da instalação, recomenda-se realizar uma cuidadosa inspeção visual do equipamento, verificando se não há danos causados pelo transporte. Certifique-se de que todos os componentes solicitados estão em perfeitas condições. Em caso de defeitos, informe a companhia transportadora e o representante ou distribuidor Altus mais próximo.

CUIDADO: Antes de remover os módulos do pacote, é importante descarregar eventuais potenciais estáticos acumulados no corpo. Para isso, toque (com as mãos nuas) em uma superfície metálica aterrada qualquer antes de manipular os módulos. Tal procedimento garante que os níveis de eletricidade estática suportados pelo módulo não sejam ultrapassados.

É importante registrar o número de série de cada item recebido, bem como revisões de software, se existentes. Estas informações serão necessárias caso se necessite entrar em contato com o Suporte Técnico Altus.

Suporte Técnico

Para entrar em contato com o Suporte Técnico da Altus em São Leopoldo, RS, ligue + 55 51 3589-9500. Para conhecer os centros de Suporte Técnico Altus em outras localidades, consulte o nosso website (www.altus.com.br) ou envie um e-mail para altus@altus.com.br.

Se o equipamento já estiver instalado, tenha em mãos as seguintes informações ao solicitar assistência:

- Modelos dos equipamentos usados e a configuração do sistema instalado
- Número de série
- Revisão do equipamento e versão de software executivo, listados na etiqueta afixada na lateral do produto

Mensagens de Advertência Utilizadas neste Manual

Neste manual, as mensagens de aviso apresentarão os seguintes formatos e significados:

PERIGO:
Relatam causas potenciais que, se não observadas, geram danos com perda de integridade e saúde, patrimônio, meio ambiente e perda da produção.

CUIDADO:
Relatam detalhes de configuração, aplicação e instalação que devem ser seguidos para evitar condições que possam levar à falha do sistema e suas consequências relacionadas.

ATENÇÃO:
Indica detalhes importantes de configuração, aplicação ou instalação para obtenção do máximo desempenho operacional do sistema.

2. Instalação do Hardware

Introdução de Hardware

Dimensões

JN4508F-M industrial 6-port mais 2 portas para Fibra de 100Mbps com Gestão pela Switch Fast Ethernet:

L 55 mm x A 149 mm x P 131,2 mm / com trilho DIN com clipe

L 55 mm x A 149 mm x P 120,6 mm / sem trilho DIN com clipe

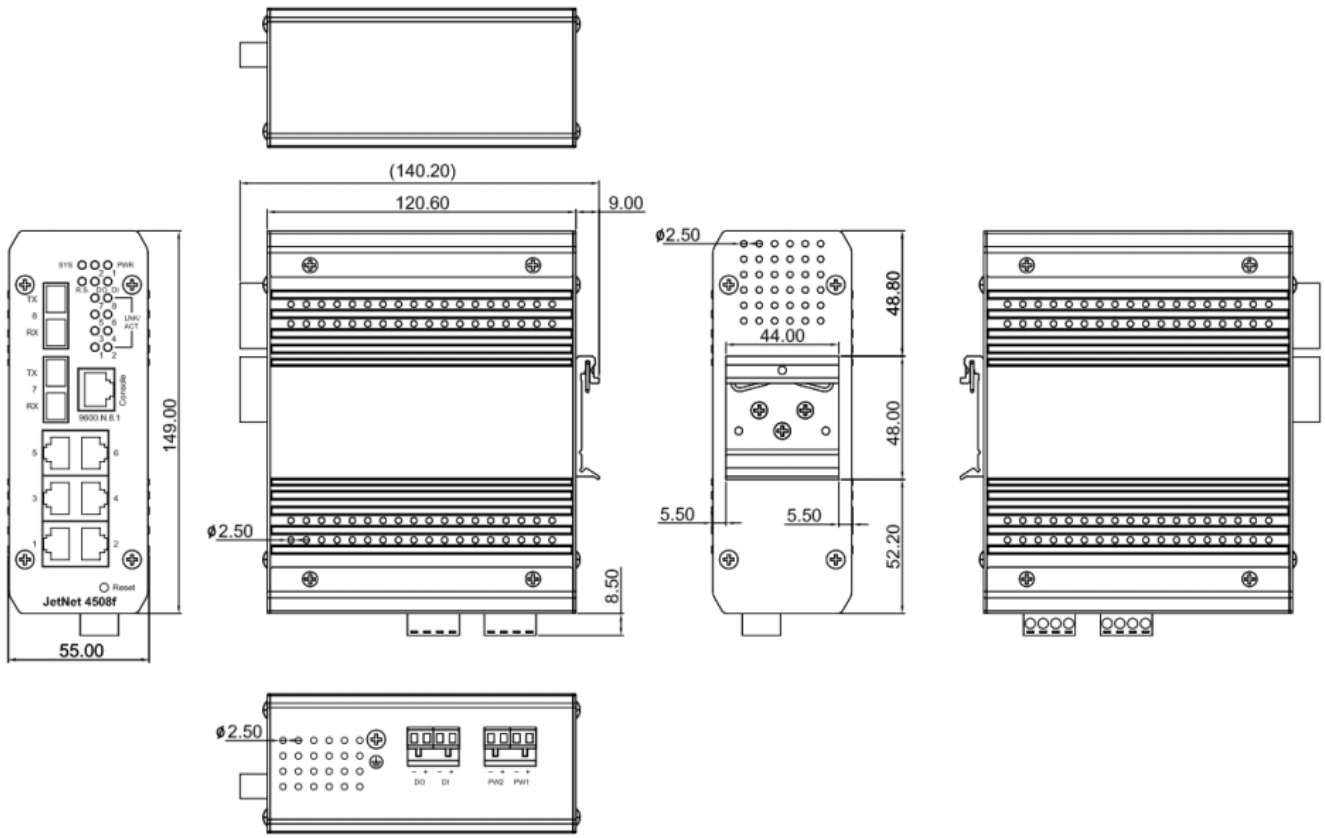

Figura 2-1. Visão Completa JN4508F-M

Layout do Painel Dianteiro

O painel frontal do JN4508F-M inclui 6 portas RJ-45 10/100Mbps Fast Ethernet (porta 1 à 6), 2 portas Fast Ethernet para fibra (portas 7 e 8), um console serial RS-232 com conector tipo RJ-45, um botão de reset e vários dos indicadores LED para o sistema e diagnóstico de portas. O painel frontal do JetNet 4508é mostrado no diagrama abaixo.

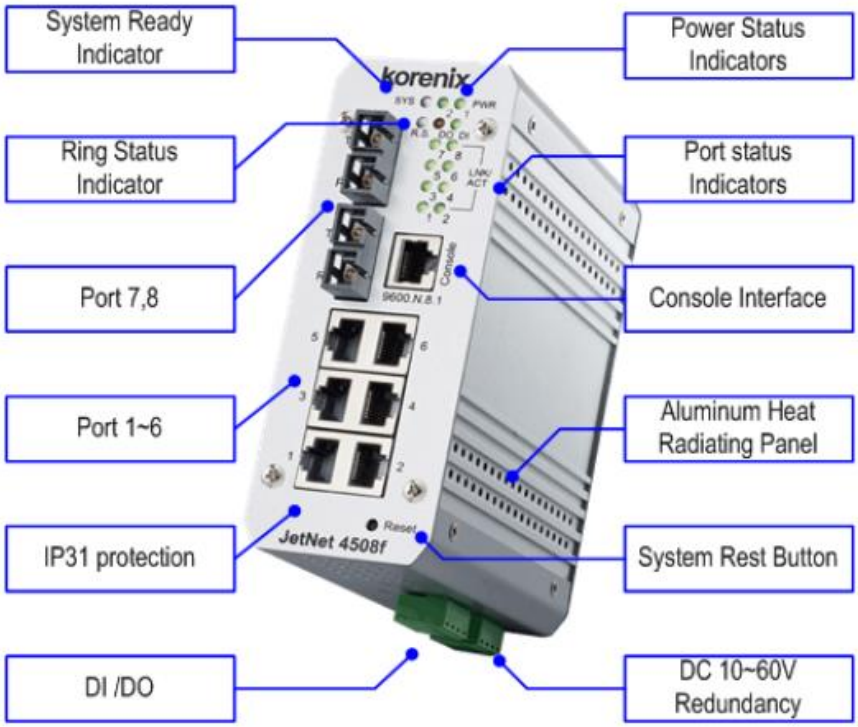

Figura 2-2. Vista do Painel Frontal do JN4508F-M

As funções dos LEDs estão descritas na tabela abaixo:

LED	Função	Comportamento
Power 1,2	Indica o estado da alimentação das entradas	Ligado: o conector de entrada está no poder aplicar
SYS	Indica o estado de funcionamento do sistema	Ligado: o sistema está pronto para operação
DI	Indica o estado de entrada digital	Ligado: Alto nível de sinal é aplicado
DO	Indica o estado da saída digital (saída de relé)	Vermelho Ligado: A saída é formada circuito fechado
R.S.	Indica o estado de funcionamento do anel	Normal (Verde Ligado), anormal (Amarelo Ligado), porta de anel errado está ligado (Verde Intermitente), um dos caminhos do dispositivo anel está inoperante (Amarelo piscando)
Link/active	Indicado o estado do fluxo e status do link	Ligado: porta está ligada com o parceiro Piscando: a porta está transmitindo ou recebendo dados

Tabela 2-1. Descrição do Funcionamento dos LEDs

Vista Inferior

A vista do fundo do JetNet 4508f-m consiste em dois conectores do bloco de terminais com duas entradas de corrente contínua de energia, uma entrada digital (DI), uma saída de relé (DO) e um parafuso de aterramento do chassi. No lado direito do Switch Industrial Gerenciado JN4508F-M, há uma borneira e parafuso de aterramento. A borneira inclui 2 entradas de alimentação e 1 saída de alarme a relé.

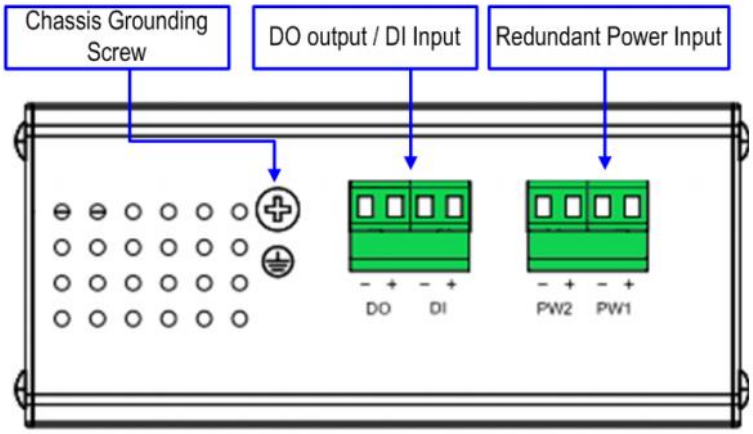

Figura 2-3. JN4508F-M - Vista Inferior

Cabeamento das Entradas de Alimentação

Siga os passos abaixo para conectar entradas de alimentação CC redundantes JN4508F-M.

1. Insira os cabos positivos e negativos nos respectivos bornes V+ e V-
2. Aperte os parafusos do fixador de cabo para evitar que os cabos de CC fiquem frouxos
3. Power 1 e Power 2 suportam redundância de alimentação e funções de proteção de reversão de polaridade, sendo assim, se a ligação estiver com a polaridade errada, o sistema não funcionará
4. Ambas as entradas de sistema de alimentação positiva e negativa são aceitas desde que Power1 e Power 2 apresentem o mesmo modo

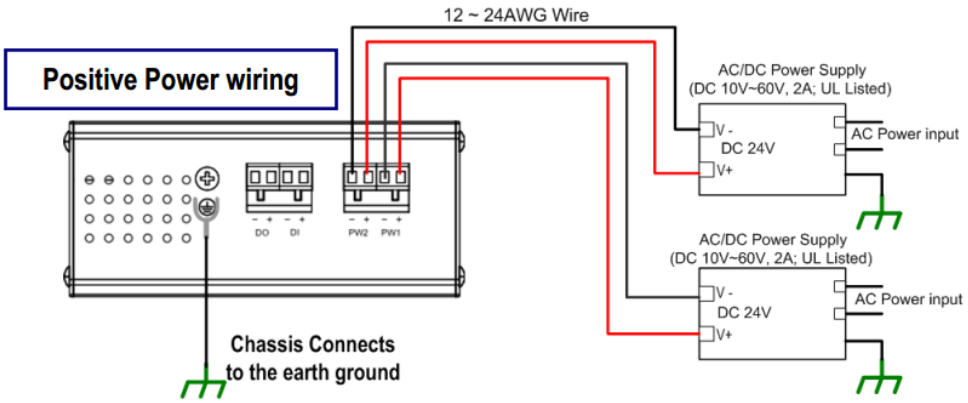

Figura 2-4. JN4508F-M Ligação Elétrica Positiva das Entradas

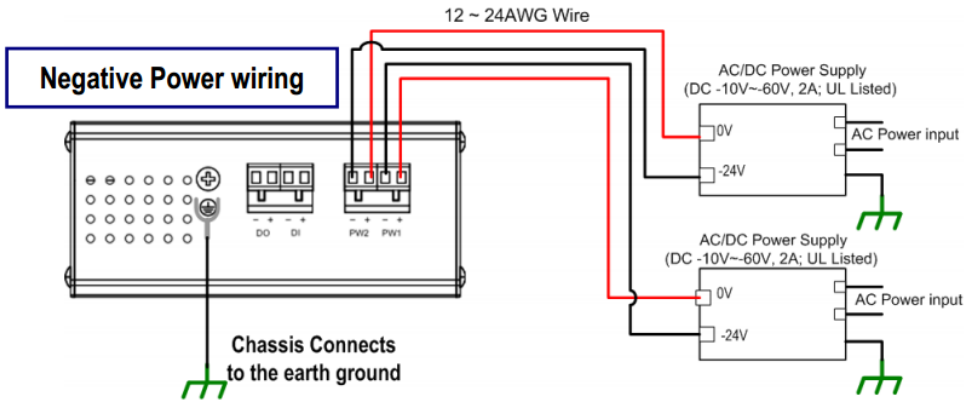

Figura 2-5. JN4508F-M Ligação Elétrica Negativa das Entradas

Nota:

É uma boa prática desligar a energia da entrada e a carga, e de desconectar o bloco terminal de alimentação antes de fazer as conexões dos fios. Caso contrário, sua chave de fenda pode acidentalmente encurtar suas conexões de terminais para o gabinete aterrado.

A bitola do fio elétrico apropriado é 12-24 AWG.

Se as duas entradas de energia estão conectadas, o switch JetNet será alimentado a partir da tensão mais elevada conectada. O alarme disparará no caso de perda de alimentação, ou da PWR1 ou da PWR2, ocasionando um backup automático com o outra alimentação.

Use a lista da UL Fonte de alimentação com saída de Avaliação 10-60 Vdc, mínimo de 2 A. Aqui, nós recomendamos o uso DC 24V como a tensão de operação.

Indicadores	Estado 1	Estado 2	Estado 3	Estado 4	Estado 5	Estado 6
Power LED	Ligado	Ligado	Ligado	Ligado	Ligado	Ligado
DI	Desligado	Ligado	Desligado	Desligado	Desligado	Desligado
DO	Desligado	Desligado	Ligado	Desligado	Desligado	Desligado
R.S.	Desligado	Desligado	Desligado	Ligado	Desligado	Desligado
SYS	Desligado	Desligado	Desligado	Desligado	Desligado	Ligado
Descrição	**Power On**	**Ex. Booter**	**Ld. Firmware**	**Ex. Firmware**	**Sistema Iniciando**	**Sistema Pronto**

Tabela 2-2. Sequencia de Diagnósticos de Inicialização

Através destes LEDs indicadores, podemos saber exatamente o estágio em que o sistema se encontra.

Cabeamento das Entradas Digitais

Para garantir que o sistema não seja danificado pelo ruído ou choque elétrico, sugere-se uma conexão O JN4508F-M fornece uma entrada digital. Ele permite que os usuários se conectem a saída digital as unidades de terminação 'e gerenciem / monitorem o status da unidade ligada. O pino de entrada digital pode ser colocado em nível alto ou baixo; assim, os equipamentos conectados podem conduzir livremente estes estados alto ou baixo. A interface do usuário de software embutido permite que seja lido e definido o valor para o dispositivo conectado.

A tensão de entrada de energia da lógica baixa é de DC 0 ~ 10V, para a lógica alta DC11 ~ 30V.

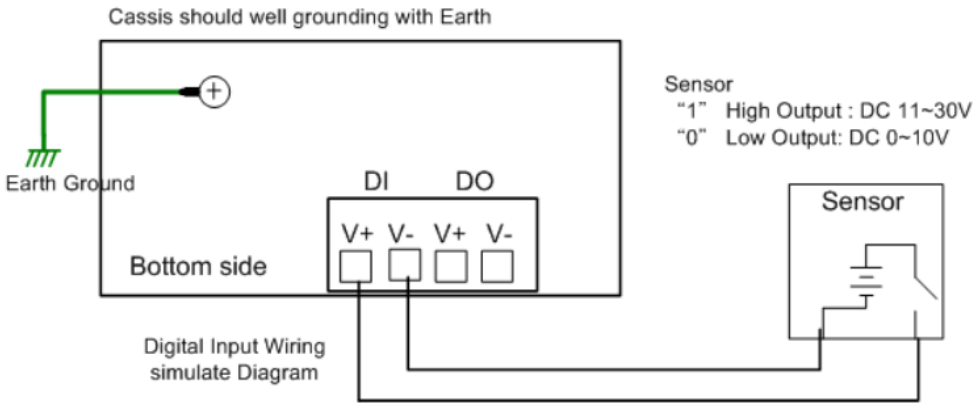

Figura 2-6. Cabeamento de Entrada Digital

Cabeamento do Relé de Saída

JN4508F-M fornecer uma saída digital, também conhecido como relé de saída não molhada. Os contatos do relé são energizados (aberto) para a operação normal e fechados para condições de falha.

As condições de falha incluem falta de energia, ligação de porta Ethernet ruptura ou outros eventos pré-definidos que podem ser configuradas na interface Web de usuário do JN4508F-M.

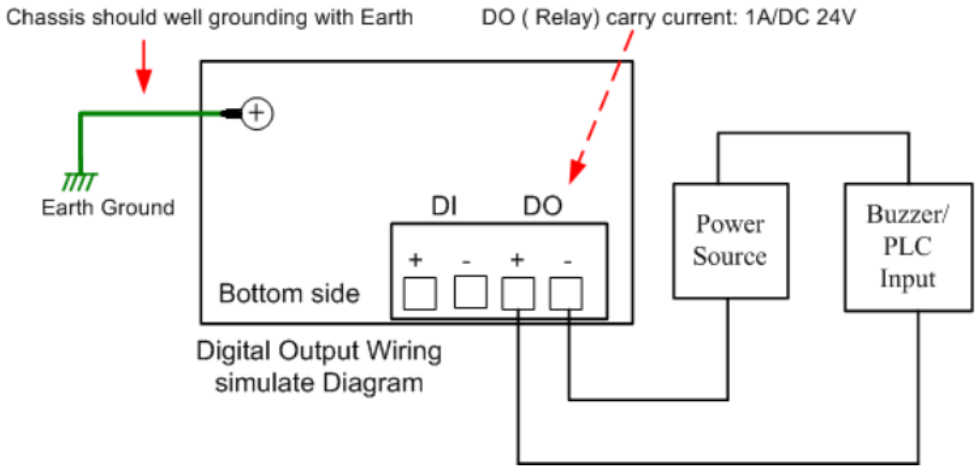

Figura 2-7. Cabeamento do Relé de Saída do JN4508F-M

Cabeamento de Aterramento

Para garantir que o sistema não será danificado por ruído ou qualquer dano elétrico, sugere-se uma conexão do JN4508F-M com à terra. No lado inferior do JN4508F-M, existe um parafuso de ligação ao terra. Solte o parafuso de ligação do terra; posicione o fio entre o parafuso e então o aperte firmemente até que esteja bem ligado. Sem o aterramento preciso da carcaça, a comunicação pode ser interferida pelo ruído externo, tais como iluminação, rápido chaveamento elétrico ou descarga eletrostática.

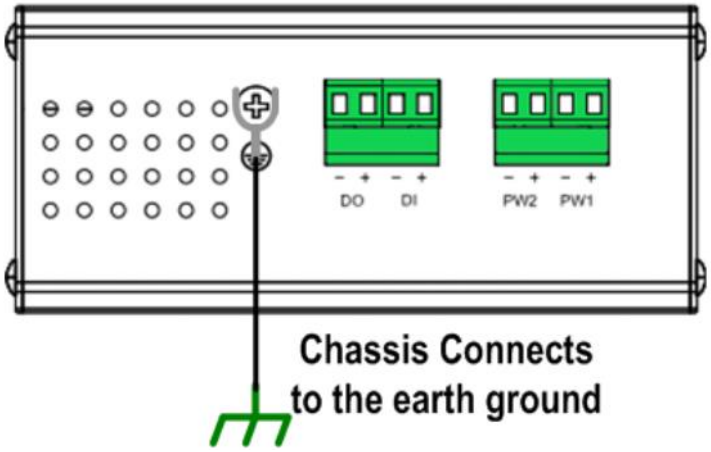

Figura 2-8. JN4508F-M Cabeamento de Aterramento

Cabeamento das Portas Ethernet RJ-45 de Alta Velocidade

O switch JN4508F-M adota vários dos conectores RJ-45 que suportam 10/100Base-TX com negociação automática de velocidade da conexão e auto funções MDI/MDI-X. Todas as portas RJ-45 irão detectar automaticamente o sinal dos dispositivos conectados para negociar a velocidade do link em modo duplex. Auto MDI/MDIX permite aos usuários conectar outro switch, hub ou estação de trabalho sem alteração direta através de cabo ou crossover.

Nota:

Os cabos cruzados simplesmente cruzam as ligações entre linhas de transmissão em cada extremidade para as linhas recebidas na extremidade oposta.

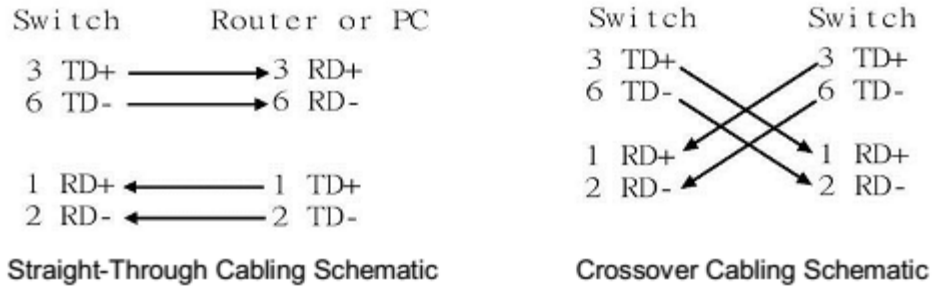

Figura 2-9. Cabeamento 10/100 Base Tx Alta Velocidade Ethernet

Pin MDI-X	Sinais	Sinais MDI
1	RD+	TD+
2	RD-	TD-
3	TD+	RD+
6	TD-	RD-

Tabela 2-3. Cabeamento da Porta Ethernet

Conecte uma extremidade do cabo Ethernet em qualquer porta do switch e ligue a outra extremidade no dispositivo conectado. O LED LNK acende-se quando o cabo está conectado corretamente. Consulte a seção Indicadores LED para descrições de cada indicador LED. Sempre certifique-se de que os cabos entre os switches e dispositivos conectados (por exemplo, switch, hub ou estação de trabalho) estão a menos de 100m (328 pés).

Os tipos de cabos suportados listados seguem abaixo:

10Base-T: 4-pair UTP/STP Cat. 3, 4 cable, EIA/TIA-568B 100-ohm (até 100m)

100Base-TX: 4-pair UTP/STP Cat. 5 cable, EIA/TIA-568B 100-ohm (até 100m)

Cabeamento da Porta Ethernet para Fibra de Alta Velocidade

JN4508F-M é equipado com 2 portas de fibra com conformidade com o padrão IEEE 802.3 100Base-FX e suporta multi-modo ou cabo de fibra monomodo. O conector de fibra suporta conector tipo SC. Para garantir a qualidade de ligação, as especificações do cabo e porta de fibra devem estar alinhados; o cabo de fibra errado pode causar uma má comunicação ou até mesmo não funcionar. As informações a seguir e a especificação incluem um cabo adequado e as características da porta de fibra.

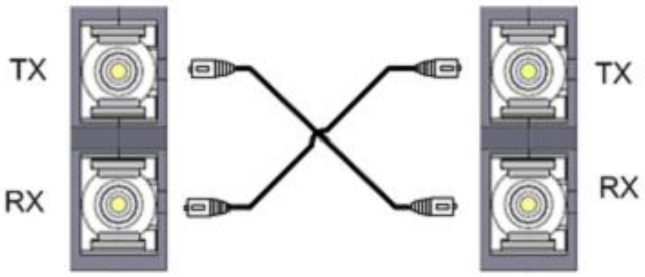

Figura 2-10. Cabeamento da Porta Ethernet para Fibra de Alta Velocidade no JN4508F-M

Cabeamento para Console RS-232

O JN4508F-M traz consigo um cabo RS-232 DB9 para RJ-45 fornecido com a caixa. Conecte o DB9 da porta COM do seu PC, abra a ferramenta Terminal e configure os parâmetros de comunicação

serial para 9600, N, 8, 1. (Taxa de transmissão: 9600bps / Paridade: Nenhum comprimento / Data: 8bits / Stop Bit: 1) Depois, será possível acessar a interface CLI via cabo console.

Nota:

Caso o cabo seja perdido, entre em contato com o setor de vendas ou siga o esquema de pinagem para comprar um novo. A identificação da pinagem é listada a seguir:

Pinos RJ-45	Pinos DB9	Descrição
1	8	N/A
2	9	N/A
3	**2**	**TxD**
4	1	N/A
5	**5**	**GND**
6	**3**	**RxD**
7	4	N/A
8	7	N/A

Tabela 2-4. Cabeamento do Console

Instalação e Montagem do Trilho DIN

O grampeamento do trilho DIN já é automaticamente feito na traseira do JN4508F-M. Se o clipe do trilho DIN não está parafusado no JN4508F-M, entre em contato com seu distribuidor para obter o conjunto de presilhas do trilho DIN. O grampo do trilho DIN suporta o padrão EN50022. No diagrama a seguir está incluso a dimensão do trilho DIN EN50022 para consulta.

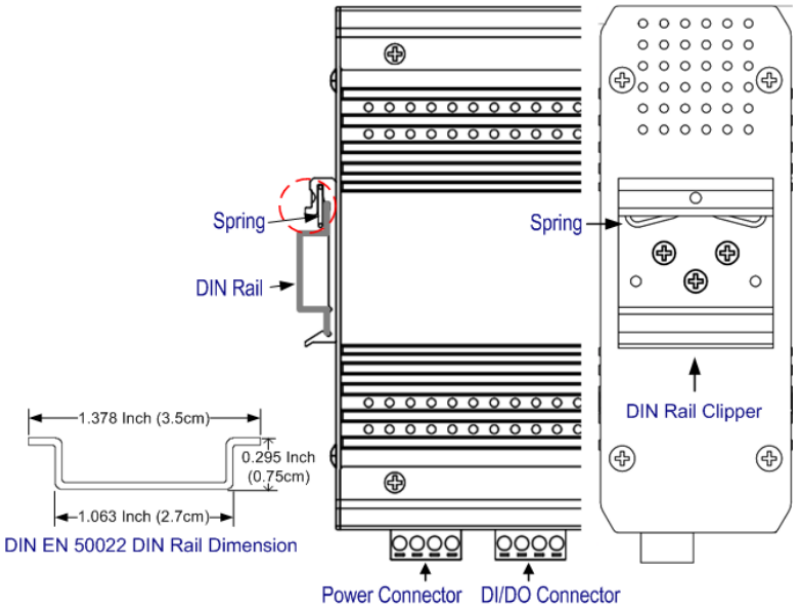

Figura 2-11. Exemplo de Montagem e Instalação

Siga os passos abaixo para montar o Switch Gerenciável JN4508F-M ao trilho DIN:

1. Primeiro, insira o trilho DIN do lado superior na extremidade superior do grampo do trilho DIN.
2. Empurre levemente a parte inferior do grampo do trilho DIN no encaixe.
3. Verifique se o trilho DIN está com o clipe firmemente conectado.
4. Para remover o JN4508F-M, inverta os passos acima.

Nota:

O trilho DIN deve ter as características conforme a norma DIN EN50022. A utilização de um trilho DIN não apropriado pode causar uma ligação do sistema insegura.

3. Preparação para Gerenciamento

O Switch Industrial Gerenciado JN4508F-M permite configurações de métodos na banda/fora da banda.

No gerenciamento fora da banda é possível configurar o switch via cabo RS232 (console) - desde que o usuário não tenha interesse em incluir seu PC como parte da rede. Além disto, em caso de perda de conexão com a rede, ainda é possível configurar o switch através deste cabo. O gerenciamento fora da banda não é afetado pelo desempenho da rede.

O gerenciamento na banda permite controlar o switch remotamente através da rede. O usuário pode escolher entre gerenciamento baseada em Web ou Telnet. Basta apenas saber o endereço IP do dispositivo para que o usuário possa se conectar remotamente às páginas web HTTP vinculadas ou console Telnet.

Preparação para Console Serial

No pacote JN4508F-M, oferece um cabo RS-232 DB-9 para RJ-45 (console). Encaixe o conector RS-232 DB-9 à porta COM do PC e, em seguida, conecte o RJ-45 à porta de console do JN4508F-M. Em caso de perda do cabo, consulte a pinagem do mesmo (ver apêndice).

1. Vá para Start-> Program -> Accessories -> Communication -> Hyper Terminal
2. Dê um nome à nova conexão de console
3. Escolha a porta de comunicação serial
4. Selecione as configurações seriais corretas. Configurações seriais para o JN4508F-M
5. Taxa de Transmissão: 9600 / Verificação de Paridade: Nenhum / Bit de Dados: 8 / Bits de Parada: 1
6. Depois de conectado, o usuário verá uma solicitação de login no switch
7. Realize o login no switch. O nome do usuário e a senha padrão são ambos, admin

Preparação para a Interface Web

Para gerenciamento via web, o JN4508F-M fornece Interface HTTP Web e Interface HTTPS Web Segura.

Interface Web

A página de gerenciamento da web utiliza a linguagem JavaScript, o que permite utilizar um navegador da Web padrão para configurar o switch de qualquer lugar enquanto estiver conectado à rede.

Antes de usar a interface da web incorporada para gerenciar a operação do switch, verifique se o JN4508F-M está instalado corretamente na rede e se todos os PCs da rede podem acessar o switch através do navegador Web.

1. Verifique se o cartão de interface de rede (NIC) está operacional e se o sistema operacional suporta o protocolo TCP/IP
2. Conecte a alimentação CC ao switch e, em seguida conecte este último ao computador
3. Certifique-se de que o endereço IP padrão do switch é 192.168.10.1
4. Altere o endereço IP do computador para o 192.168.10.2 ou outro endereço IP na subrede 192.168.10.x (máscara de rede: 255.255.255.0)
5. Alterne para modo de comando DOS e realize uma operação de ping em 192.168.10.1 para verificar se o tempo de resposta está adequado
6. Inicie o navegador web (Internet Explorer ou Mozilla Firefox) no PC
7. Digite http://192.168.10.1 (ou o endereço IP do switch) na janela de endereço da Web e pressione *Enter*
8. A tela de Login será mostrada

9. Digite o nome de usuário e senha. O nome do usuário e senha padrão são ambos admin
10. Selecione o idioma, o padrão é inglês (English). Esta característica está disponível a partir da versão de firmware v1.1

Figura 3-1. Tela do Gerenciador do Switch

Clique *OK* ou *Enter*. Será exibida a página de boas-vindas da interface web de gerenciamento.

Uma vez dentro da interface web de gerenciamento, é possível alterar o endereço IP do JN4508F-M para que o mesmo se adapte ao ambiente de rede.

Notas:

A versão 5.0 ou posterior do Internet Explorer, por padrão, não permite que os applets Java abram sockets. Para que possam utilizar portas de rede, os usuários devem modificar as configurações do navegador diretamente e ativar os applets Java.

A sessão de conexão Web UI de JN4508F-M será desconectado automaticamente se qualquer entrada for inserida após 30 segundos. Depois de autenticado, deve se logar novamente utilizando nome de usuário e senha correta novamente.

Interface Web Segura (Secure Web)

A página de gerenciamento de web oferece também um login HTTPS seguro. Todos os comandos de configuração são seguros, o que dificulta que hackers decifrem a senha de login e os comandos de configuração.

Inicie o navegador web e faça o Login.

1. Inicie um navegador web (Internet Explorer ou Mozilla Firefox) no PC
2. Digite *https://192.168.10.1* (ou o endereço IP do switch) na janela de endereço de web. Pressione *Enter*
3. Uma tela de pop-up aparecerá solicitando ao usuário que confie na conexão HTTPS segura distribuída pelo JN4508F-M. Pressione *Yes*

Figura 3-2. Tela de Alerta de Segurança

4. A seguir, será exibida a tela de Login

Figura 3-3. Switch Manager – Tela de Login

5. Digite o nome de usuário e senha. O nome do usuário e senha padrão são ambos *admin*
6. Clique em *Enter* ou *OK*. A página de boas-vindas da interface web de gerenciamento será mostrada
7. Uma vez que logado na interface de gerenciamento baseada na Web, todos os comandos que você vê serão os mesmos que aparecem através do Login HTTP

Preparação para Console Telnet

Telnet

O JN4508F-M suporta protocolo Telnet. O usuário pode conectar-se ao switch através do Telnet --as linhas de comando são as mesmas da porta RS232 (console). Siga os passos abaixo para iniciar uma conexão Telnet.

- Vá para *Start -> Run -> cmd* Pressione *Enter*
- Digite Telnet 192.168.10.1 (ou o endereço IP do switch). Pressione *Enter*

SSH (Secure Shell)

O JN4508F-M também oferece suporte a SSH. O usuário pode conectar-se remotamente ao switch via interface de linha de comando. A conexão SSH pode proteger todos os comandos de configuração enviados ao switch.

A conexão SSH é uma arquitetura cliente/servidor na qual o JN4508F-M é o servidor SSH. Para realizar uma conexão SSH com o switch, primeiramente baixe a ferramenta do cliente SSH (realize o download).

Cliente SSH

Há vários clientes SSH disponíveis na internet. Um exemplo é o PuTTY - um cliente Telnet/SSH gratuito e popular. Esta ferramenta será usada para demonstrar como fazer o login no JN4508F-M através do SSH.

Nota:

PuTTY, Copyright 1997-2006 Simon Tatham.

PuTTY download: http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

Abra o Cliente SSH / PuTTY

Na configuração da sessão, digite o nome do Host (endereço IP do JN4508F-M) e o número da Porta (padrão = 22). Escolha o protocolo *SSH*. Em seguida, clique em *Open* para iniciar o console da sessão SSH.

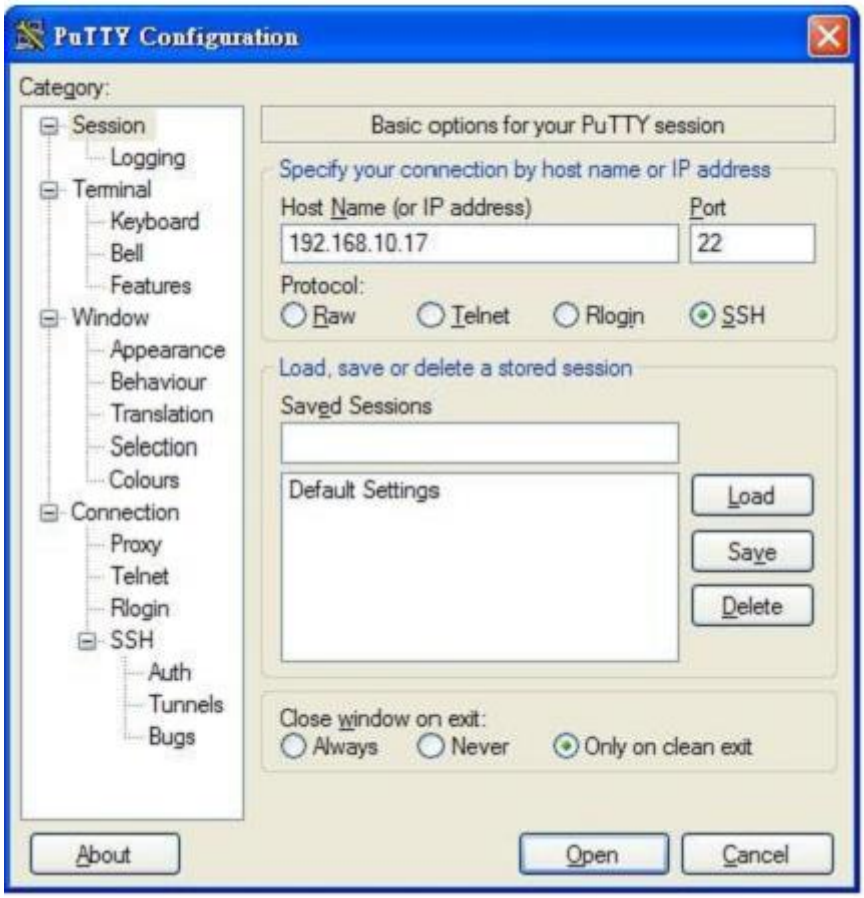

Figura 3-4. Interface Putty

Após clicar em *Open*, será exibida uma tela de pop-up com informações cifradas. Clique *Yes* para aceitar o alerta de segurança.

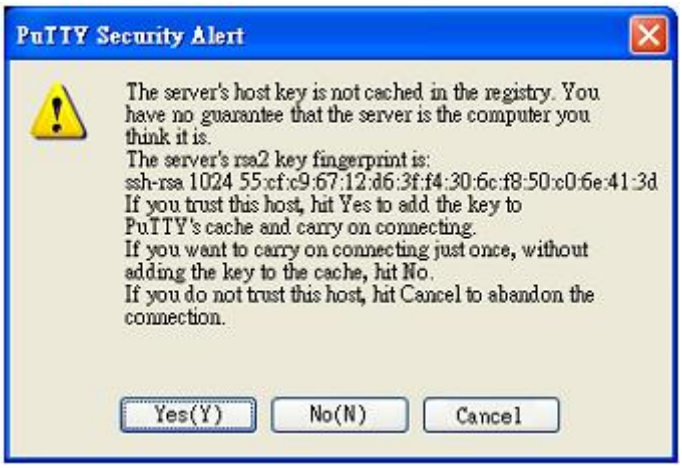

Figura 3-5. Alerta de Segurança PuTTY

Após alguns segundos será aberta a conexão entre SSH e o JN4508F-M.

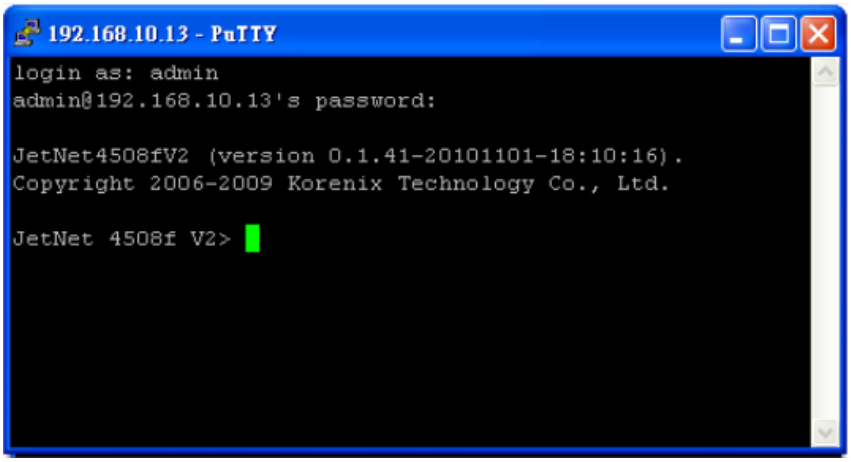

Figura 3-6. JN4508F-M SSH

Digite o nome de Login e senha. Por padrão, ambos são *admin*.

Os comandos SSH são idênticos aos comandos CLI via console RS232. O próximo capítulo mostrará em detalhes como usar a linha de comando para configurar o switch.

4. Configuração de Recursos

Este capítulo explica como configurar o software JN4508F-M e suas funcionalidades.

Introdução ao CLI (Command List Interface)

A Interface de linha de comando (CLI) é a interface de usuário do sistema de software incorporado ao switch. Através de teclas de comando é possível visualizar as informações do sistema e o status, assim como configurar o switch e receber uma resposta do sistema.

Existem diferentes modos de comando. Cada modo de comando possui sua própria habilidade de acesso e suas próprias linhas de comando disponíveis (diferentes para entrar e sair do sistema). A seguir, são detalhados os modos de comando EXEC Usuário, EXEC Privilegiado, Configuração Global e Configuração de Interface (Porta/VLAN).

Modo EXEC Usuário

O usuário estará neste modo quando realizar o Login no switch através da interface de linha de comando (CLI). Neste modo pode realizar uma operação de ping, um telnet no dispositivo remoto, além de visualizar algumas informações básicas.

Digite *enable*, este comando permite entrar no próximo modo, a opção *Exit* permite o Logout, *?* para ver a lista de comandos.

Switch	
enable	Ativa o modo de comando privilegiado
exit	Sai do modo atual e retorna ao modo anterior
list	Imprime a lista de comandos
ping	Envia mensagens de eco
quit	Sai do modo atual e retorna ao modo anterior
show	Visualiza informações do sistema em execução
telnet	Inicia uma conexão telnet
traceroute	Traça uma rota de rastreamento para o destino

Tabela 4-1. Lista de Comandos

Modo EXEC Privilegiado

Selecione *enable* no modo EXEC usuário para entrar no modo EXEC privilegiado. Neste modo, o sistema permite visualizar as configurações atuais, retornar para o padrão, recarregar o switch, mostrar as informações do sistema, salvar uma configuração e, por fim, entrar no modo de configuração global.

Selecione *Configure* para entrar no modo seguinte ou *Exit* para sair. Para ver uma lista de comandos disponíveis, clique *?*. A Tabela 4-2 mostra os comandos.

Switch#	
archive	Gerenciamento de Arquivos
clear	Reinicia as funções
clock	Configure hora do dia / relógio
configure	Configuração das interface vty
copy	Copiar de um arquivo para o outro
debug	Funções de depuração (veja também undebug)
disable	Desabilita o modo de comando privilegiado
end	Finaliza o modo corrente e chaveia para o modo enable

exit	Sair do modo corrente e volta ao modo anterior
list	Imprime lista de comandos
more	Mostra as características de um arquivo
no	Nega um comando ou configura para o padrão
ping	Envia uma mensagem de echo
quit	Sai do modo corrente e retorna ao modo anterior
reboot	Reinicia o sistema
reload	Copia uma configuração padrão de um arquivo para substituir do arquivo atual
show	Mostra as informações atuais do sistema em execução
telnet	Abre uma conexão telnet
terminal	Configura o terminal com linhas de parâmetros
traceroute	Traça rota destino
write	Escreve a configuração corrente na memória, network ou terminal

Tabela 4-2. Lista de Comandos Privilegiada

Modo de Configuração Global

Para entrar no modo de configuração global selecione digite *Configure* no terminal no modo EXEC privilegiado. No modo de configuração global é possível configurar todas as funcionalidades oferecidas pelo sistema.

Selecione a interface *IFNAME/VLAN* para entrar no modo de configuração, *Exit* para sair ou *?* para visualizar a lista de comandos.

Os comandos disponíveis para o modo de configuração global são mostrados na Tabela 4-3.

Switch# configure terminal Switch(config) #	
access-list	Adiciona um item na lista de acesso
administrator	Configuração da conta do administrador
arp	Define uma entrada ARP estática
clock	Configura o relógio de hora do dia
default	Retorna um comando para seus padrões
end	Encerra o modo atual e altera-o para o modo enable
exit	Sai do modo atual e retorna ao modo anterior
gvrp	Protocolo de Registro GARP VLAN
hostname	Define o nome da rede no sistema
interface	Seleciona uma interface a ser configurada
ip	Informações de IP
list	Imprime a lista de comandos
log	Controle de log
mac	Sub-comandos de configuração global MAC
mac-address-table	Tela de endereços MAC
mirror	Espelhamento de porta
no	Anula um comando ou redefine-o para o padrão
ntp	Configura NTP
password	Atribui a senha de conexão terminal
Qos	Qualidade de serviço (QoS)
relay	Informações de saída a relé
smtp-server	Configuração de servidor SMTP
snmp-tree	Servidor SNMP
spanning-tree	Algoritmo de árvore de abrangência
super-ring	Protocolo de Super Ring

trunk	Configuração de grupo Trunk
vlan	Virtual LAN
warning-event	Seleção de Alerta de Evento
write-config	Especifica arquivos de configuração a serem escritos

Tabela 4-3. Lista de Comandos de Configuração Global

Configuração de Interface (Porta)

Digite interface *IFNAME* no modo de configuração global para entrar no modo de configuração de interface. Neste modo são realizadas as configurações das portas.

O nome da interface da porta para a porta Fast Ethernet 1~8 é fa1~8. Digite o nome da interface correspondente àquela em cujo modo de configuração de específico deseja entrar.

Digite *Exit* para sair ou *?* para visualizar a lista dos comandos disponíveis.

A Tabela 4-3 mostra os comandos disponíveis para o modo de configuração de interface de porta.

Switch(config)# interface fa2 Switch(config-if)#	
acceptable	Configura 802.1Q padrão de frame aceitável pela porta
auto-negotiation	Habilita o estado de auto-negociação de uma determinada porta
Description	Descrição específica da interface
duplex	Especifica o modo duplex de operação para uma porta
end	Sai do modo atual e retorna ao modo anterior
exit	Define o valor de controle de fluxo para uma interface
flowcontrol	Imprime a lista de comandos
garp	General Attribute Registration Protocol
ingress	802.1Q entra no filtro de características
lacp	Link Aggregation Control Protocol
list	Imprime a lista de comandos
loopback	Especifica o modo de loopback de operação para uma porta
mac	Comandos da interface MAC
mdix	Permite o estado midx de uma determinada porta
no	Anula um comando ou redefine-o para o padrão
poe	Configura a energia sobre a Ethernet
qos	Qualidade de serviço (QoS)
quit	Sai do modo atual e retorna ao modo anterior
rate-limit	Configuração de limite de taxa
shutdown	Finalização da interface selecionada
spanning-tree	Protocolo de árvore de abrangência
speed	Especifica a velocidade de uma porta Fast Ethernet
switchport	Define as características de modo comutação

Tabela 4-3. Lista de Comandos da Interface Porta

Configuração de Interface (VLAN)

Digite *interface VLAN VLAN-ID* no modo de configuração global para entrar modo de configuração de interface VLAN. Neste modo são realizadas as configurações para uma porta VLAN específica.

O nome da interface VLAN para VLAN 1 é VLAN 1; para VLAN 2 é VLAN 2.

Digite *Exit* para sair ou *?* para visualizar a lista dos comandos disponíveis.

Os comandos disponíveis para o modo de configuração de interface VLAN são exibidos na Tabela 4-4.

Switch(config) # interface vlan 1 JN4508F-M (config-if) #	
Description	Descrição específica da interface
end	Encerra o modo atual e altera-o para o modo enable
exit	Sai do modo atual e retorna ao modo anterior
ip	Comandos de configuração de Protocolo de Interface de Internet
list	Imprime a lista de comandos
no	Anula um comando ou redefine-o para o padrão
quit	Sai do modo atual e retorna ao modo anterior
shutdown	Finalização da interface selecionada

Tabela 4-4. Lista de Comandos de Interface (VLAN)

A Tabela 4-5 resume os modos de comando.

Modo de Comando	Função Principal	Método de Entrada e Saída	Prompt
EXEC Usuário	Este é o primeiro nível de acesso do usuário, no qual pode ser realizada uma operação de ping, um dispositivo telnet remoto e também visualizadas algumas informações básicas	Entrar: Realizar o login Sair: Selecionar **Exit** Próximo Modo: Digite **enable** para entrar no modo EXEC privilegiado.	Switch>
Privilegiado EXEC	Neste modo, o sistema exibe a configuração atual, redefine a configuração para o padrão, recarrega o switch, mostrar as informações do sistema, salva uma configuração e entrar no modo de configuração global	Entrar: Selecionar **enable** no modo EXEC Usuário. Exec: Selecionar **disable** no modo EXEC Usuário.Exit: Selecionar **Exit** Próximo Modo: Selecionar **Configure Terminal** para entrar no comando de configuração global.	Switch#
Configuração Global	Neste modo de configuração podem ser configuradas todas as funcionalidades oferecidas pelo sistema	Entrar: Selecionar **Configure Terminal** no modo EXEC privilegiado Sair: Selecionar **Exit** ou as teclas **CTRL+Z.** Próximo Modo: Selecionar **IFNAME / VLAN VID** para entrar nos modo de configuração de interface	Switch(config) #
Configuração de Interface de Porta	Neste modo são realizadas as configurações relacionadas às portas	Entrar: Selecionar a interface **IFNAME** no modo de configuração global. Sair: Selecionar **Exit** ou **Ctrl + Z** para sair do modo EXEC privilegiado.	Switch(config-if) #
Configuração de Interface VLAN	Neste modo são definidas as configurações para uma VLAN específica	Entrar: Selecionar a interface **VLAN VID** no modo de configuração global. Sair: Selecionar **Exit** ou Ctrl + Z para sair do modo EXEC privilegiado.	Switch(config-vlan) #

Tabela 4-5. Lista de Nós de Comando

A tabela abaixo exibe alguns comandos úteis para visualizar todos ou alguns comandos específicos de comandos disponíveis. Além de economizar tempo, o usuário também evita erros de digitação.

? mostra todos os comandos disponíveis no modo atual, assim como o próximo comando a ser digitado.

Switch(config) # interface (?)	
IFNAME	Nome da interface
vlan	Seleciona a vlan a ser configurada

Tabela 4-6. Lista de Comandos Úteis 1

? mostra todos os comandos passíveis de serem usados como *caracteres*.

Switch(config) # a?	
access-list	Adiciona um item na lista de acesso
administrator	Configuração da conta do administrador
arp	Define uma entrada ARP estática

Tabela 4-7. Lista de Comandos Úteis 2

A aba *Key* facilita o uso dos comandos. Caso haja apenas um comando disponível, o usuário pode clicar nesta aba para gerar o comando automaticamente.

Switch# co (tab) (tab)
Switch# configure terminal
Switch(config) # ac (tab)
Switch(config) # access-list

Ctrl + C interrompe um comando inacabado.

Ctrl + S bloqueia a tela do terminal e impossibilita qualquer comando.

Ctrl + Q desbloqueia uma tela bloqueada.

Ctrl + Z sai do modo de configuração.

Uma mensagem de alerta será exibida quando vários usuários tentarem configurar o switch. Se o administrador estiver no modo de configuração, os usuários da Web, não poderão alterar as configurações. O JN4508F-M só permite ser configurado por um administrador de cada vez.

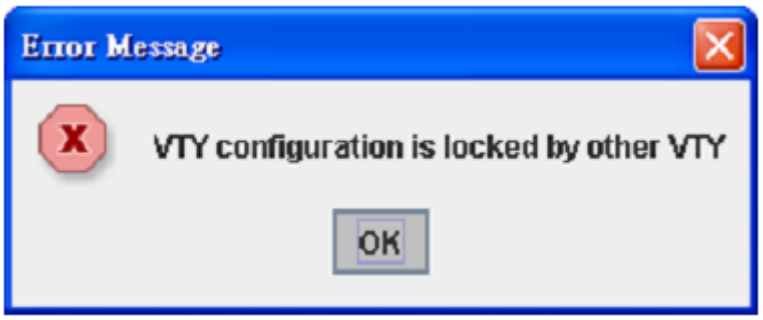

Figura 4-1. Mensagem de Alerta

Configurações Básicas

Esta seção fornece instruções sobre como configurar as informações do switch, definir o endereço IP e configurar o nome de usuário e senha do sistema. Adicionalmente, informa como atualizar o firmware, realizar um backup e restaurar/recarregar o sistema para as configurações padrão de fábrica, além de orientar como reiniciar o sistema.

Configuração do Switch

O usuário pode atribuir ao sistema um nome, local e contato, além de visualizar suas informações.

A Figura 4-2 ilustra a interface do usuário Web para a configuração do switch.

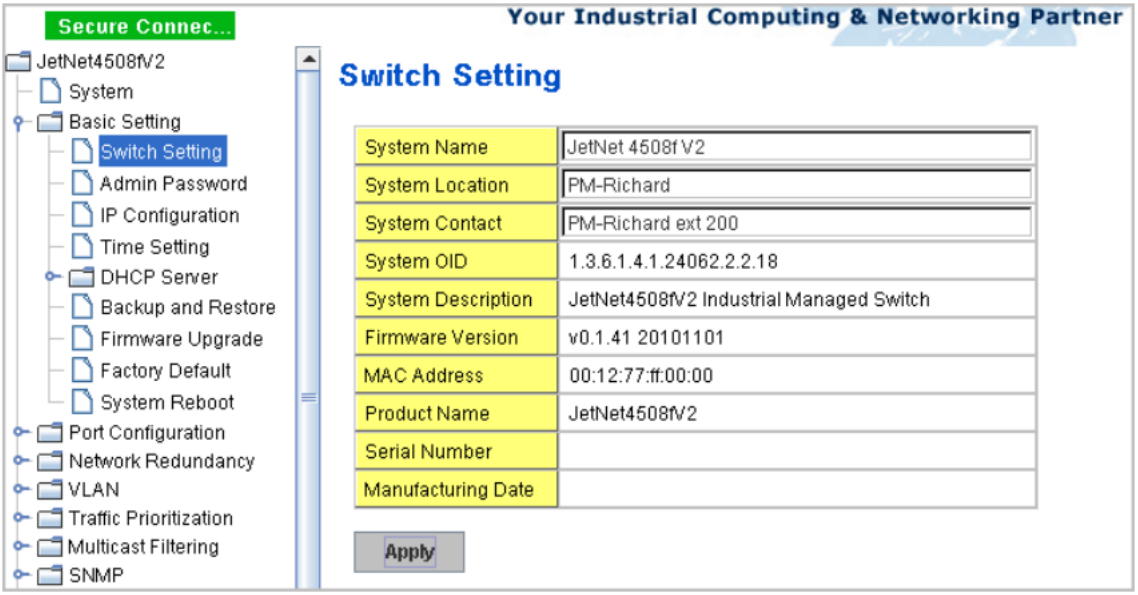

Figura 4-2. Interface de Configuração do Switch

System Name: Atribui um nome de até 64 caracteres ao dispositivo. Após configurar o nome, o sistema CLI selecionará os primeiro 12 caracteres como o nome para o sistema CLI

System Location: Especifica o local físico do switch. Da mesma forma que o campo anterior, o máximo permitido são 64 caracteres

System Contact: Especifica as pessoas de contato. Digite o nome, endereço de e-mail ou outras informações sobre o administrador (máximo 64 caracteres)

System OID: Defina a ID do objeto SNMP do switch. Siga o caminho para encontrar o MIB privada no navegador MIB. Observe que ao tentar visualizar um MIB privado, primeiramente os arquivos MIB privados deve estar compilados no navegador MIB

System Description: Exibe uma descrição do sistema. Neste caso, o Switch Ethernet Industrial Gerenciado JN4508F-M

Firmware Version: Exibe a versão do firmware instalada no dispositivo

MAC Address: Exibe o endereço exclusivo do hardware (endereço MAC) designado pelo fabricante

Product Name: Mostra o nome do modelo do switch

Serial Number: Mostra o número de série do switch

Manufacture Date: Mostra a data de produção do switch

Após finalizar as configurações, clique em *Apply*

Nota:

Lembre-se de salvar as configurações via botão *Save*. Caso contrário, as configurações feitas serão perdidas quando o switch for desligado.

Senha do Administrador

É possível alterar o nome do usuário e a senha para aumentar a segurança do sistema. A Figura 4-3 ilustra a interface do usuário da Web para a senha do Administrador.

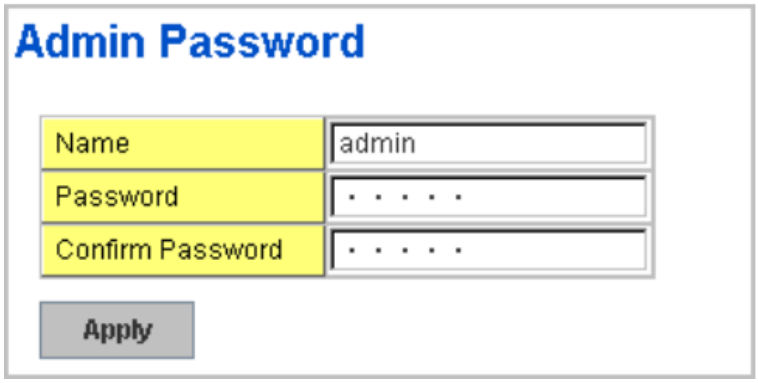

Figura 4-3. Alterando a Senha de Administrador

- **Name:** Digite um novo nome de usuário. A configuração padrão é admin
- **Password:** Digite uma nova senha. A configuração padrão é admin
- **Confirm Password:** Digite novamente a senha escolhida para confirmá-la

Após finalizar as configurações, clique em *Apply*.

A Figura 4-4 mostra a mensagem de alerta exibida na janela de pop-up quando o usuário entra com um nome incorreto.

Figura 4-4. Alerta de Nome de Usuário Incorreto

Configuração de IP

Esta função permite aos usuários configurar o endereço IP do switch.

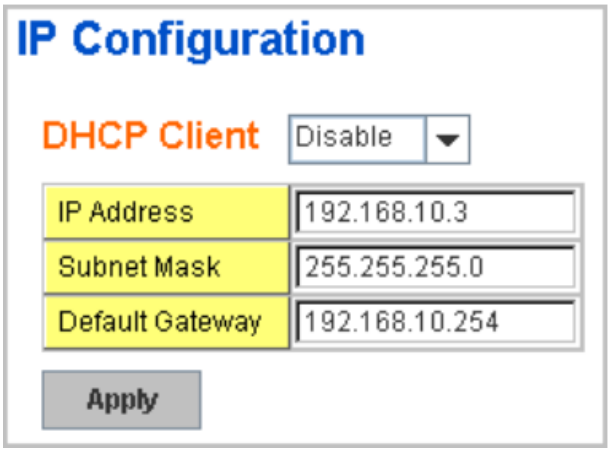

Figura 4-5. Tela de Configuração de IP

DHCP Client: Esta opção habilita ou desabilita a função Cliente DHCP. Se habilitada, um endereço IP será atribuído ao switch a partir servidor DHCP da rede. Neste modo, o endereço IP padrão será substituído por aquele atribuído pelo servidor DHCP. Se a função cliente DHCP está desabilitada, será usado o endereço IP especificado.

IP Address: Este campo atribui o endereço IP reservado pela rede para o JN4508F-M. Se a função cliente DHCP está habilitada não é necessário atribuir um endereço IP, pois ele será substituído pelo servidor DHCP. O endereço IP padrão é 192.168.10.1

Subnet Mask: Atribui a máscara de sub-rede para o endereço IP. Se a função cliente DHCP está habilitada, não é necessário atribuir uma máscara de sub-rede. O padrão de máscara de sub-rede é 255.255.255.0. Nota: Na interface CLI, a máscara de sub-rede habilitada é usada para representar o número exibido na interface do usuário web. Por exemplo, 8 corresponde a 255.0.0.0; 16 corresponde a 255.255.0.0 e 24 corresponde a 255.255.255.0

Gateway: Atribui o gateway ao switch. O gateway padrão é 192.168.10.254. Nota: Na interface CLI, 0.0.0.0/0 representa o gateway padrão

Nota:

No CLI, usamos 0.0.0.0 para representar o gateway default.

Após finalizar as configurações, clique em *Apply*.

Configurações de Tempo

A aba de configuração de tempo permite ao usuário definir o tempo manualmente ou através do servidor NTP. Também é possível a sincronização do tempo a partir do PC. O Protocolo de Tempo de Rede (Network Time Protocol - NTP) é usado para sincronizar os relógios dos computadores na internet. O protocolo NTP permite sincronizar os relógios de múltiplos switches na rede.

O IEEE1588 PTP (Precision Time Protocol) oferece suporte a sincronização de tempo muito preciso em uma rede Ethernet. Existem dois relógios, mestre e escravo. O dispositivo mestre lança periodicamente uma troca de mensagens com dispositivos escravos para ajudar cada relógio de escravo a recomputar o deslocamento entre o seu relógio e do mestre

Nota:

Habilite somente um protocolo de sincronização por vez apenas (PTP ou NTP)

O JN4508F-M também oferece a possibilidade de configurar o horário de verão.

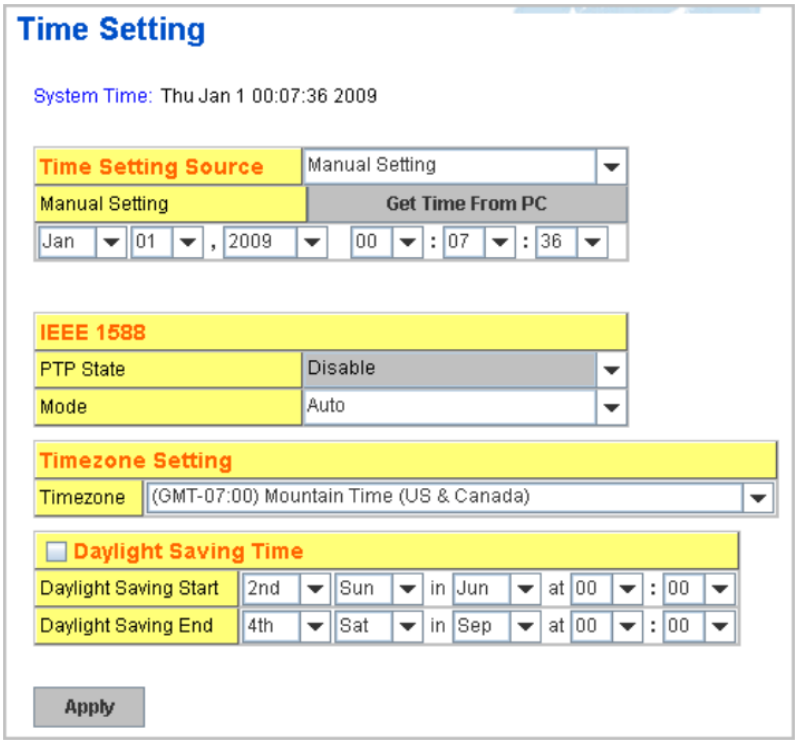

Figura 4-6. Configurações de Tempo

Manual Setting: Selecione a aba de configuração manual para especificar a hora desejada e clique no ícone *Get Time From PC* para sincronizar a hora com o PC

NTP Client: A aba *Time Setting Source* para o cliente NTP habilita o cliente NTP. Desta forma o JN4508F-M marca o tempo de 2 servidores NTP diferentes. O sistema enviará um pacote de solicitação para verificar a hora atual do servidor NTP

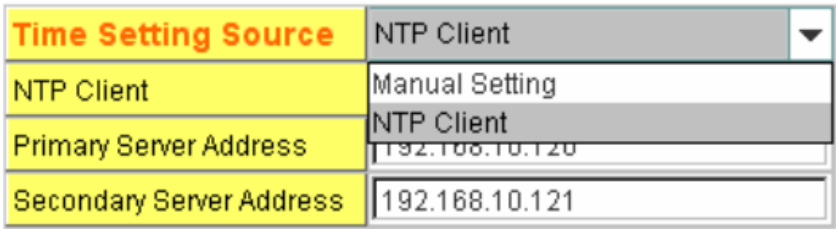

Figura 4-7. Opções de Configurações de Tempo

IEEE 1588: Selecione o Estado PTP para ativar essa função e selecione um modo de operação para sincronizar o tempo de precisão.

Auto mode: O switch executa o modo PTP Mestre e Escravo (Modo binário).

Master mode: O switch executa o modo PTP Mestre somente.

Slave mode: O switch executa o modo PTP Escravo somente.

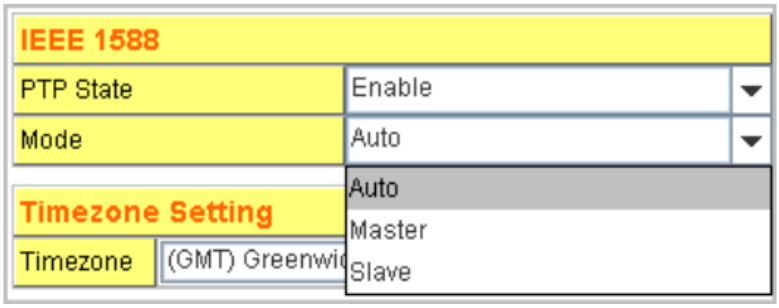

Figura 4-8. Opções de Configuração de Estados

Timezone: Selecione o fuso horário do local onde se encontra o switch. A Tabela 4-8 lista os fusos horários de diferentes locais. GMT (Greenwich Mean Time) é o fuso horário padrão.

Switch(config)# a?	
1	(GMT-12:00) Eniwetok, Kwajalein
2	(GMT-11:00) Midway Island, Samoa
3	(GMT-10:00) Havaí
4	(GMT-09:00) Alasca
5	(GMT-08:00) Hora do Pacífico (EUA e Canadá), Tijuana
6	(GMT-07:00) Arizona
7	(GMT-07:00) Mountain Time (EUA e Canadá)
8	(GMT-06:00) América Central
9	(GMT-06:00) Hora Central (EUA e Canadá)
10	(GMT-06:00) Cidade do México
11	(GMT-06:00) Saskatchewan
12	(GMT-05:00) Bogotá, Lima, Quito
13	(GMT-05:00) Hora do Leste (EUA e Canadá)
14	(GMT-05:00) Indiana (Leste)
15	(GMT-04:00) Horário do Atlântico (Canadá)
16	(GMT-04:00) Caracas, La Paz
17	(GMT-04:00) Santiago
18	(GMT-03:00) NewFoundland
19	(GMT-03:00) Brasília
20	(GMT-03:00) Buenos Aires, Georgetown
21	(GMT-03:00) Gronelândia
22	(GMT-02:00) Mid-Atlantic
23	(GMT-01:00) Açores (GMT-01:00) Cabo Verde.
25	(GMT) Casablanca, Monróvia
26	(GMT) Tempo Médio de Greenwich: Dublin, Edinburgh, Lisboa, Londres
27	(GMT + 01:00) Amsterdam, Berlim, Berna, Roma, Estocolmo, Viena
28	(GMT + 01:00) Belgrado, Bratislava, Budapeste, Ljubljana, Praga
29	(GMT + 01:00) Bruxelas, Copenhaga, Madrid, Paris
30	(GMT + 01:00) Sarajevo, Skopje, Sofija, Vilnius, Varsóvia, Zagreb
31	(GMT + 01:00) África Centro-Oeste
32	(GMT + 02:00) Atenas, Istambul, Minsk
33	(GMT + 02:00) Bucareste
34	(GMT + 02:00) Cairo
35	(GMT + 02:00) Harare, Pretoria
36	(GMT + 02:00) Helsinki, Riga, Tallinn
37	(GMT + 02:00) Jerusalém
38	(GMT + 03:00) Bagdá
39	(GMT + 03:00) Kuwait, Riyadh
40	(GMT + 03:00) Moscou, São Petersburgo, Volgograd

41	(GMT + 03:00) Nairobi
42	(GMT + 03:30) Teerã
43	(GMT + 04:00) Abu Dhabi, Muscat
44	(GMT + 04:00) Baku, Tbilisi, Yerevan
45	(GMT + 04:30) Kabul
46	(GMT + 05:00) Ekaterinburg
47	(GMT + 05:00) Islamabad, Karachi, Tashkent
48	(GMT + 05:30) Calcutá, Chennai, Mumbai, Nova Deli
49	(GMT + 05:45) Kathmandu
50	(GMT + 06:00) Almaty, Novosibirsk
51	(GMT + 06:00) Astana, Dhaka
52	(GMT + 06:00) Sri Jayawardenepura
53	(GMT + 06:30) Rangoon
54	(GMT + 07:00) Bangcoc, Hanói, Jacarta
55	(GMT + 07:00) Krasnoyarsk
56	(GMT + 08:00) Beijing, Chongqing, Hong Kong, Urumqi
57	(GMT + 08:00) Irkutsk, Ulaan Bataar
58	(GMT + 08:00) Kuala Lumpur, Cingapura
59	(GMT + 08:00) Perth
60	(GMT + 08:00) Taipei
61	(GMT + 09:00) Osaka, Sapporo, Tóquio
62	(GMT + 09:00) Seul
63	(GMT + 09:00) Yakutsk
64	(GMT + 09:30) Adelaide
65	(GMT + 09:30) Darwin
66	(GMT + 10:00) Brisbane
67	(GMT + 10:00) Canberra, Melbourne, Sydney
68	(GMT + 10:00) Guam, Port Moresby
69	(GMT + 10:00) Hobart
70	(GMT + 10:00) Vladivostok
71	(GMT + 11:00) Magadã, Ilhas Salomão, Nova Caledônia
72	(GMT + 12:00) Aukland, Wellington
73	(GMT + 12:00) Fiji, Kamchatka, Marshall é.
74	(GMT + 13:00) Nuku"alofa

Tabela 4-8. Lista de Fuso Horários

Daylight Savint Time: Define o início e término, do horário de verão. Durante este período a hora do dispositivo representa uma hora mais cedo do que o tempo real.

Daylight Savint Time Start e Daylight Saving End: as configurações de tempo permitem ao usuário selecionar as semanas do inicio e fim do horário de verão separadamente.

Figura 4-9. Configurações - Daylight Saving Time

Após finalizar as configurações, clique em *Apply*.

Servidor DHCP

Esta opção habilita ou desabilita a função *Servidor DHCP*. O Switch JN4508F-M atribui um novo endereço IP para vincular-se aos parceiros.

Configuração do Servidor DHCP

Após ativar a função do servidor DHCP, os seguintes campos estarão disponíveis para configuração: *Network* (endereço IP da rede para o pool IP do servidor DHCP), *Subnet Mask* (máscara de sub-rede), *Default Gateway* (endereço padrão) e *Lease Time* (tempo de concessão) para o cliente.

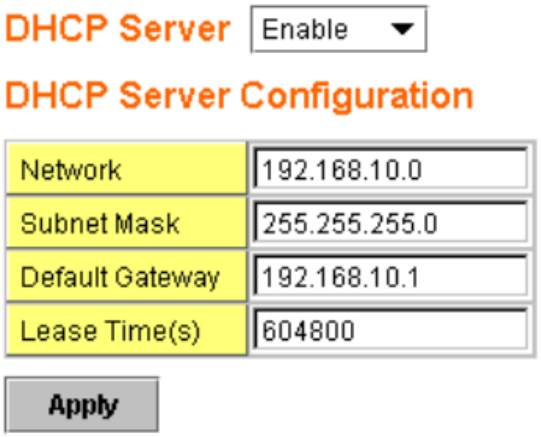

Figura 4-10. Configurações – DHCP Server

Após finalizar as configurações, clique em *Apply*.

Excluded Address: O usuário pode digitar um endereço específico para o endereço IP reservado do servidor DHCP, no campo correspondente.

Os endereços IP listados na tabela de endereços excluídos não serão atribuídos ao dispositivo de rede. É possível adicionar ou remover um endereço IP desta lista clicando nos botões correspondentes respectivamente (*Add* ou *Remove)*.

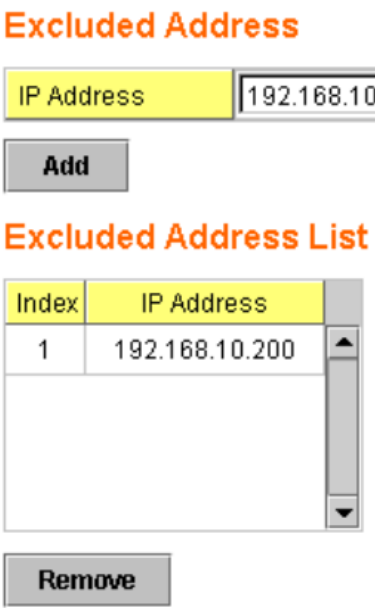

Figura 4-11. Configuração – Lista de Endereços Excluídos

Manual Binding: O JN4508F-M oferece a possibilidade de conectar e remover endereços MAC e IP. Digite o endereço IP e MAC especificado e clique no botão *Add* para adicionar uma nova regra de conexão dos novos endereços com um parceiro de link especificado (CLP ou qualquer dispositivo sem A função cliente DHCP. Para retirar o endereço da lista, selecione a regra e clique em *Remove*.

Figura 4-12. Configurações – Manual Binding

DCHP Leased Entries: O switch JN4508F-M disponibiliza uma lista de tempos para o usuário. Ele mostra os endereços MAC e IP atribuído pelo JN4508F-M. Clique em *Reload* para atualizar a listagem.

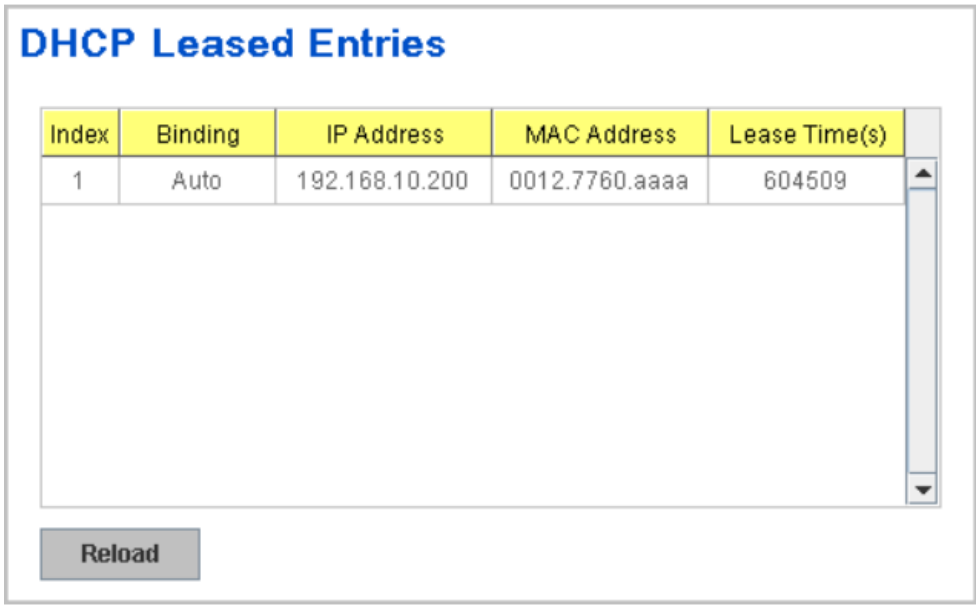

Figura 4-13. DHCP Leased Entries

DHCP Relay Agent: O usuário pode selecionar habilitar ou desabilitar a função de agente de retransmissão DHCP, e em seguida, selecione o tipo de modificação de opção 82 campo.

Figura 4-14. Configurações - DHCP Relay Agent

Relay Policy Drop: Libera o campo da opção 82 e não adiciona nenhuma opção ao campo 82.

Relay Policy Keep: Mantem a opção 82 original no campo e repassa ao servidor.

Relay Policy Replace: Sobrescreve a opção existe no campo 82 e adiciona uma nova opção a esse campo. (Configuração padrão).

Helper Address: existem 4 campos para o endereço IP do servidor DHCP. o usuário pode preencher o campo com o endereço IP preferido de servidor DHCP. Clique em *Apply* para ativar a função de agente de retransmissão DHCP. Todos os pacotes DHCP do cliente serão modificados por esta política e encaminhados para o servidor DHCP através da porta do gateway.

Backup e Recuperação

Através do comando de Backup, o usuário pode salvar os arquivos atuais de configuração salvos no flash do switch para o PC do administrador ou servidor TFTP. Desta forma é possível, posteriormente, utilizar o comando *Restore*, o qual recupera o arquivo de configuração do switch. Antes disto, no entanto, é necessário posicionar o arquivo de configuração de backup no PC ou servidor TFTP. O switch então baixará este arquivo para o flash.

Os usuários podem realizar o backup/recuperação do arquivo de configuração de 2 modos - o modo Arquivo Local e o modo Servidor TFTP.

Local File Mode: Neste modo, o switch atua como servidor de arquivos. Procure a pasta destino e em seguida, digite o nome do arquivo para fazer backup da configuração. Alternativamente, procure a pasta destino e selecione os arquivos de configuração existentes a serem recuperados. Este modo é suportado apenas pela interface Web do usuário; a interface CLI não é aceita.

TFTP Server Mode: Neste modo, o switch atua como cliente TFTP. Antes de fazê-lo, certifique-se de que o servidor TFTP está pronto. Em seguida, digite o endereço IP do servidor TFTP. O sistema usa o nome do arquivo de configuração padrão (Quagga.conf). Não é necessário digitar um novo nome de arquivo. Este modo pode ser usado tanto na interface Web do usuário quanto CLI.

TFTP Server IP Address: Neste campo, digite o endereço IP do servidor TFTP.

Backup/Restore File Name: O sistema usa um nome de arquivo padrão.

Configuration File: O arquivo de configuração do switch é um arquivo de texto que pode ser aberto com o Microsoft Word ou qualquer programa de leitura de arquivos .txt. Uma vez aberto, o arquivo de configuração é possível alterá-lo (adicionar/remover as definições feitas) e em seguida, recuperá-lo no switch.

Startup Configuration File: Após salvar as novas configurações do arquivo em execução no flash, as mesmas serão atualizadas após um ciclo de alimentação. Exiba as configurações de inicialização (através do comando correspondente) para visualizá-lo na CLI. O comando de Backup realiza o backup dos arquivos de configuração somente no PC ou servidor TFTP.

Informações Técnicas:

Default Configuration File: O switch fornece o arquivo de configuração padrão do sistema. Utilize o botão de *Reset* ou o comando *Reload* para reiniciar o sistema.

Running Configuration File: A interface CLI do switch permite visualizar as últimas configurações em execução no sistema. As informações mostradas referem-se às configurações realizadas. No entanto se o usuário não salvá-las no flash, elas não estarão disponíveis após o Backup/Recuperação para executar o ciclo do processo. Exiba as configurações de inicialização (através do comando correspondente) para visualizá-lo na CLI

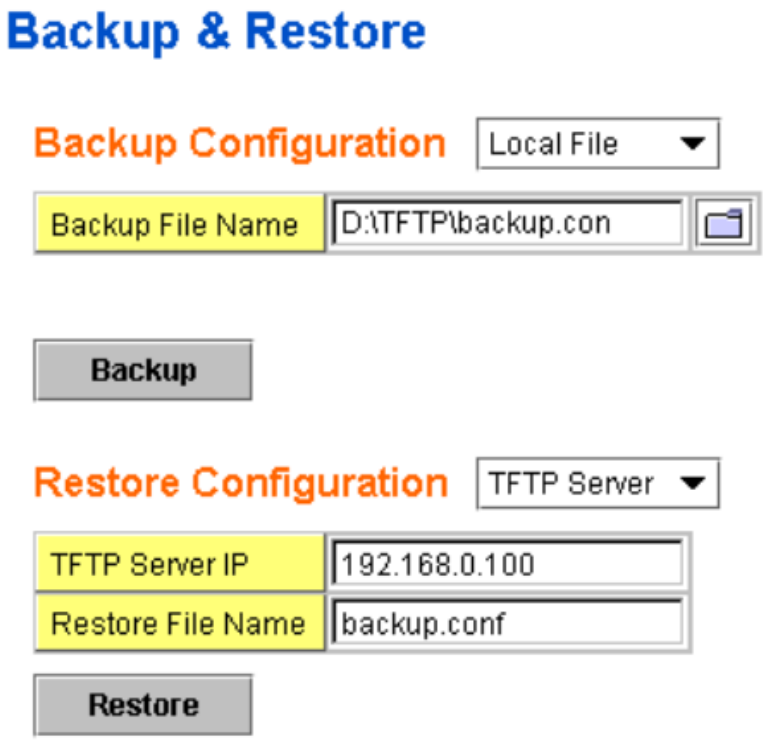

Figura 4-15. Configurações - Backup & Restore

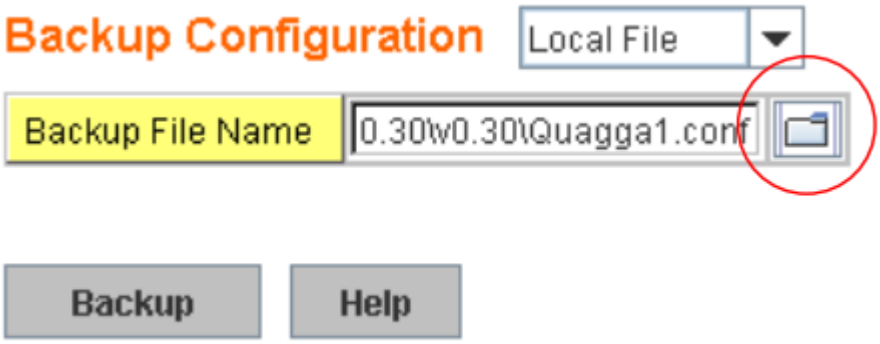

Figura 4-16. Interface Web do Usuário para Configuração de Backup e Recuperação - Modo Arquivo Local

Clique no ícone circulado acima (pasta) e selecione o arquivo destino a ser recuperado/realizado o backup.

Nota:

As pastas do caminho para o arquivo de destino não permitem que você digite a tecla de espaço.

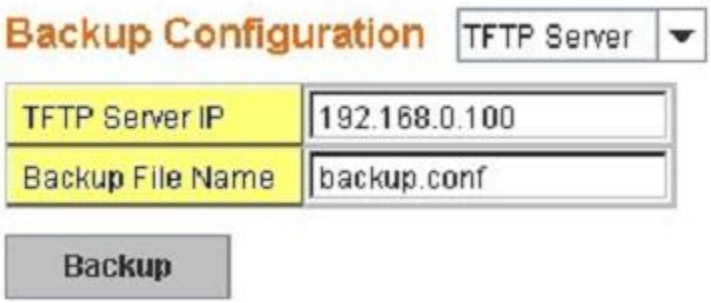

Figura 4-17. Interface Web do Usuário para Configuração de Backup e Recuperação - Modo Servidor TFTP

Digite o endereço IP do IP do servidor TFTP. Em seguida, clique no botão *Backup/Restore*.

Nota:

As pastas do caminho para o arquivo destino não permitem barra de espaço.

Atualização de Firmware

Esta seção fornece instruções sobre como atualizar o switch com a última versão de firmware. O firmware mais recente do JN4508F-M pode ser providenciado através do suporte técnico da Altus altus@altus.com.br. A última versão do firmware inclui novas funcionalidades, tais como correções de bugs e outras alterações no software. O site também fornece notas de lançamento para a atualização. Portanto, recomenda-se ao usuário que utilize a última versão de firmware antes de instalar o switch.

Nota:

O sistema reiniciará automaticamente após a atualização de versão. Todos os usuários conectados devem ser informados antes da realização deste procedimento.

Figura 4-18. Interface Web Principal para Atualização de Firmware

Os usuários podem realizar o backup/recuperação do arquivo de configuração de 2 modos - o modo *Local File* e o modo *TFTP Server*.

Local File Mode: Neste modo, o switch atua como servidor de arquivos. Procure a pasta destino e em seguida, digite o nome do arquivo para fazer backup da configuração. Alternativamente, procure a pasta destino e selecione os arquivos de configuração existentes a serem recuperados. Este modo é suportado apenas pela interface Web do usuário; a interface CLI não é aceita.

TFTP Server Mode: Neste modo, o switch atua como cliente TFTP. Antes de fazê-lo, certifique-se de que o servidor TFTP está pronto. Em seguida, digite o endereço IP do servidor TFTP. Este modo pode ser usado tanto na interface Web do usuário quanto CLI.

TFTP Server IP Address: Neste campo, digite o endereço IP do servidor TFTP.

Firmware File Name: Visualize o nome do arquivo do novo firmware.

Além da última versão de firmware, a interface do mostra também a data de compilação. Verifique o número de versão após reiniciar o switch.

Figura 4-19. Web UI para Atualização de Firmware – Local File Mode

Clique no ícone da pasta para selecionar o firmware a ser atualizado.

Figura 4-20. Interface Web UI para Atualização de Firmware – TFTP Server Mode

Digite o endereço IP do servidor TFTP e o nome do Arquivo de Firmware. Em seguida, clique no botão *Upgrade* para iniciar o processo.

Após finalizar a transmissão do firmware, o sistema copiará o arquivo de firmware e substituindo o firmware no flash. A interface CLI será mostrada até que o processo seja concluído.

Padrão de Fábrica (Factory Default)

Clicando no botão *Reset*, o sistema retornará todas as configurações para o padrão inicial, exceto o endereço IP. O sistema exibirá uma tela de pop-up após a execução deste comando. As configurações padrão serão aplicadas após a reinicialização do switch.

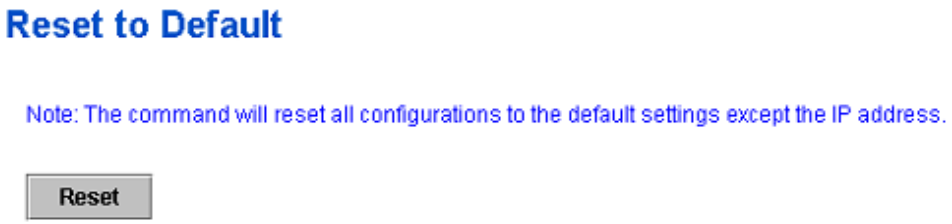

Figura 4-21. Web UI Interface para Reset to Default

A Figura 4-22 ilustra a tela de pop-up solicitando a confirmação do comando. Clique *Yes* para restaurar o sistema.

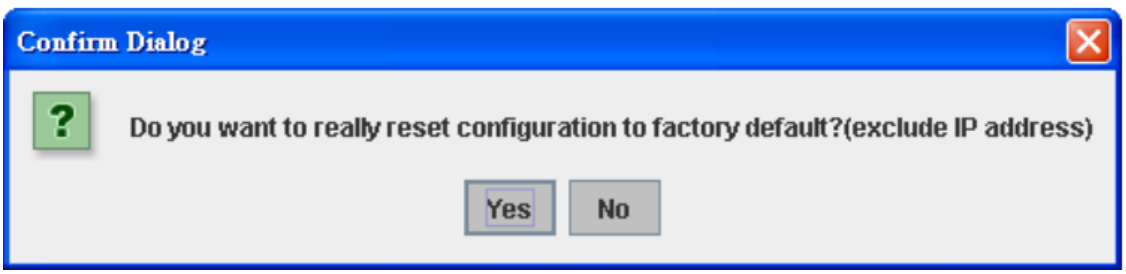

Figura 4-22. Diálogo do Comando de Reset do Sistema

A Figura 4-22. Diálogo do Comando de Reset do Sistema ilustra a tela de pop-up informando o sucesso da operação de reset. Clique *OK* para fechar a tela e, a seguir, vá para a página de reinicialização para reiniciar o switch.

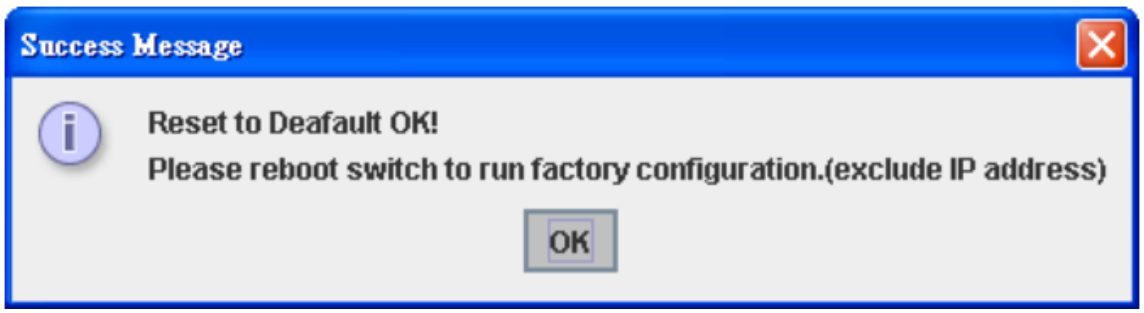

Figura 4-23. Confirmação do Reset Default

Clique *OK*. O sistema reiniciará automaticamente o dispositivo.

Nota:

Caso o usuário já tenha configurado o IP do dispositivo para outro endereço IP, ao utilizar este comando através das interfaces CLI e Web, o software não redefinirá o endereço IP para o padrão. O sistema manterá o endereço IP para que ainda seja possível conectar o switch via rede.

Reinicialização do Sistema (System Reboot)

A reinicialização do sistema permite reiniciar o dispositivo. Algumas das alterações nas funcionalidades exigem a reinicialização do sistema. Clique no botão *Reboot* botão para reiniciar o dispositivo.

Nota:

Lembre-se de salvar as configurações via botão *Save*. Caso contrário, as configurações feitas serão perdidas quando o switch for desligado.

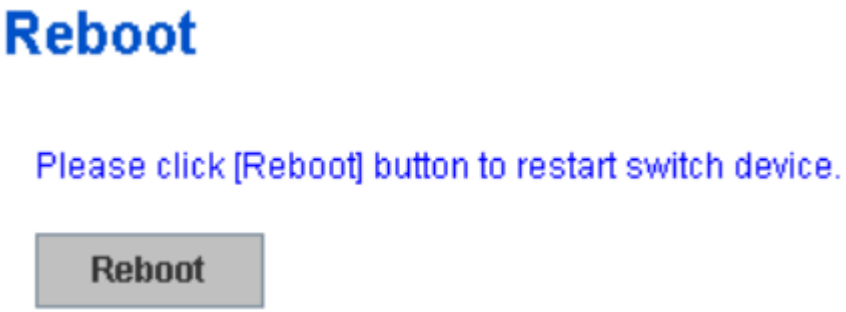

Figura 4-24. Tela Principal para Reinicialização

A Figura 4-25 ilustra a tela de pop-up solicitando confirmação da reinicialização do switch. Clique *Yes* para efetivar a operação.

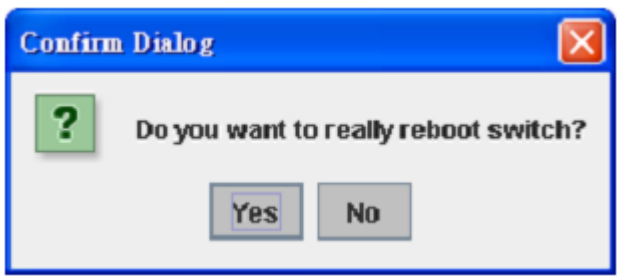

Figura 4-25. Tela de Reinicialização do Switch

A mensagem na tela de pop-up da Figura 4-26 será exibida quando o switch for reiniciado.

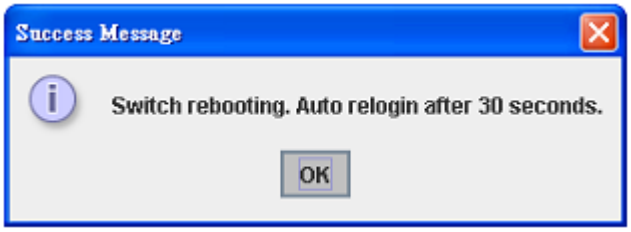

Figura 4-26. Confirmação de Reinicialização do Switch – Comando Aceito

Comandos CLI para Configurações Básicas

Característica	Linha de Comando
Configuração do Switch	
Nome do Sistema	Switch(config)# hostname WORD Network name of this system Switch(config)# hostname JN4508F-M Switch(config)#
Local do Sistema	Switch(config)# snmp-server location Brasil
Contato do Sistema	Switch(config)# snmp-server contact
Display	Switch# show snmp-server name Switch# Switch# show snmp-server location Brasil Switch# show snmp-server contact Switch> show version 0.31 -20061218 Switch# show hardware mac MAC Address: 00:12:77:FF:01:B0
Senha do Administrador	
Nome de usuário e senha	Switch(config)# administrator NAME Administrator account name Switch(config)# administrator admin % Command incomplete. Switch(config)# administrator orwell PASSWORD Administrator account password Switch(config)# administrator orwell orwell Change administrator account orwell and password orwell success.
Display	Switch# show administrator Administrator account information name: orwell password: orwell
Configuração de IP	
Endereço IP/Máscara 192.168.10.8 255.255.255.0	Switch(config)# int vlan 1 Switch(config-if)# ip address 192.168.10.8/24
Gateway	Switch(config)# ip route 0.0.0.0/0 192.168.10.254/24
Remover o Gateway	Switch(config)# no ip route 0.0.0.0/0 192.168.10.254/24
Display	Switch# show running-config …… ! interface vlan1 ip address 192.168.10.8/24 no shutdown ! ip route 0.0.0.0/0 192.168.10.254/24 !
Configurações de Tempo	

Servidor NTP	Switch(config)# ntp peer 192.168.10.100
Fuso horário	Switch(config)# clock timezone 26 Sun Jan 1 04:13:24 2006 (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London **Note:** By typing clock timezone ?, you can see the timezone list. Then choose the number of the timezone you want to select.
IEEE 1588 PTP	Switch (config) # ptpd run -> enable IEEE 1588 PTP with auto mode PTPd is enabled! Switch (config)# ptpd run preferred-clock -> master mode Switch (config)# ptpd run slave -> slave mode Switch (config)# no ptpd run -> disable IEEE 1588 PTP PTPd is disabled!
Display	Switch# sh ntp associations 1 192.168.10.100 2 192.168.10.101 Switch# show clock Sun Jan 1 04:14:19 2006 (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London Switch# show clock timezone clock timezone (26) (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
Daylight Saving	Switch(config)# clock summer-time 4 0 2 12:00 4 0 3 12:00 Clock summer-time <start week of month > <start weekday> <start month> <start Hour:Min> <end week of month> <end weekday> <end month> <end Hour:Min>
DHCP Server	
DHCP Server configuration	Enable DHCP Server on JetNet Switch Switch# Switch# configure terminal Switch(config)# router dhcp Switch(config-dhcp)# service dhcp Configure DHCP network address pool Switch(config-dhcp)#network 50.50.50.0/4 -(network/mask) Switch(config-dhcp)#default-router 50.50.50.1
Lease time configure	Switch(config-dhcp)#lease 300 (300 sec)
DHCP Relay Agent	Enable DHCP Relay Agent Switch# Switch# configure terminal Switch(config)# router dhcp Switch(config-dhcp)# service dhcp Switch(config-dhcp)# ip dhcp relay information option Enable DHCP Relay policy Switch(config-dhcp)# ip dhcp relay information policy replace drop Relay Policy keep Drop/Keep/Replace option82 field replace
Show DHCP server information	Switch# show ip dhcp server statistics Switch# show ip dhcp server statistics DHCP Server ON Address Pool 1 network:192.168.17.0/24 default-router:192.168.17.254 lease time:300 Excluded Address List IP Address ---------- (list excluded address) Manual Binding List IP Address MAC Address ---------- ---------- (list IP & MAC binding entry) Leased Address List

	IP Address MAC Address Leased Time Remains --------------- -------------- -------------------- (list leased Time remain information for each entry)
Backup e Recuperação	
Inicialização de Backup Arquivo de Configuração	Switch# copy startup-config tftp: 192.168.10.33 Writing Configuration [OK] Nota 1: Para fazer o backup do último arquivo de configuração de inicialização, primeiramente salve as configurações atuais no flash. Consulte a seção 4.12 para informações sobre salvamento. Nota 2: 192.168.10.33 é o IP do servidor TFTP. O ambiente pode usar diferentes endereços IP. Digite o IP do servidor TFTP destino neste comando.
Restaurar a Configuração	Switch# copy tftp: 192.168.10.33 startup-config
Mostrar a configuração de inicialização	Switch# show startup-config
Mostra a Configuração em Execução	Switch# show running-config
Atualização de Firmware	
Atualização de Firmware	Switch# archive download-sw /overwrite tftp 192.168.10.33 JN4508.bin Firmware upgrading, don't turn off the switch! Tftping file JN4508.bin Firmware upgrading .... Firmware upgrade success!! Rebooting.....
Padrão de Fábrica	
Padrão de Fábrica	Switch# reload default-config file Reload OK! Switch# reboot
Reinicialização do Sistema	
Reinicialização	Switch# reboot

Tabela 4-9. Comandos CLI para Configurações Básicas

Configuração de Porta

Esta seção fornece informações relativas às configurações da porta: ativação/desativação de estado, auto-negociação, velocidade, duplex, controle de fluxo, controle de limite de taxa e agregação. Adicionalmente, orienta como visualizar o status da porta e as informações de agregação.

Controle da Porta (Port Control)

Os comandos de controle de porta permitem habilitar/desabilitar o estado da porta ou configurar a auto-negociação, velocidade, duplex e controle de fluxo.

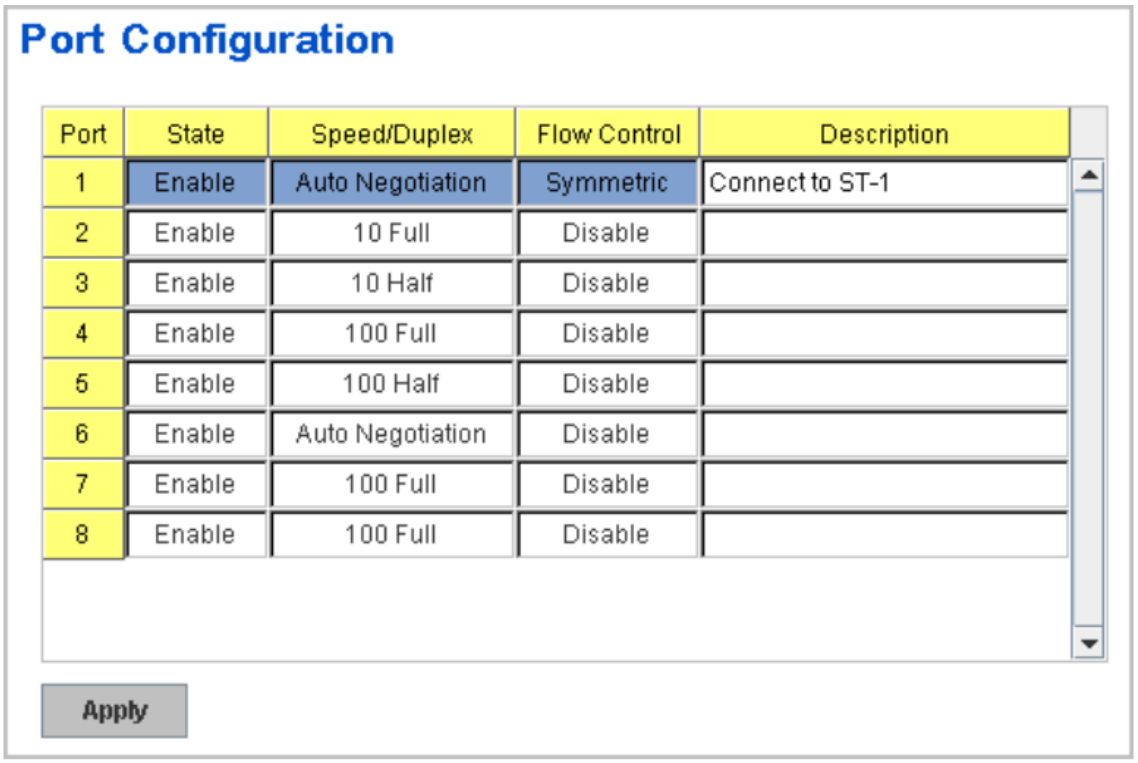

Figura 4-27. Configuração de Portas

Selecione a porta a ser configurada e realiza as alterações desejadas.

Coluna State: Ativa ou desativa o estado da porta atual. Quando desativado, a conexão e o encaminhamento do tráfego são interrompidos. A configuração padrão do dispositivo é habilitada (Enable), o que significa que todas as portas estão operacionais.

Coluna Speed/Duplex: Configura a velocidade da porta e o modo duplex da porta atual. Opções disponíveis:

Fast Ethernet Port 1~6 (fa1~fa6): Auto-negociação, 10M Full Duplex(10 Full), 10M Half Duplex(10 Half), 100M Full Duplex(100 Full) e100M Half Duplex(100 Half).

Fiber Port (fa7, fa8): 100Full (100Mbps, Full Duplex) somente.

Coluna Flow Control: Habilita ou não a função de controle de fluxo. *Symmetric* significa que é necessário ativar a função de controle de fluxo do dispositivo de rede remoto para permitir o controle de fluxo da porta correspondente para o switch. A opção *Disable* significa o oposto: não é necessário ativar esta função, pois o controle de fluxo da porta para o switch funcionará de qualquer forma.

Após finalizar as configurações, clique em *Apply*.

Informações Técnicas: Se ambas as extremidades estão em velocidades diferentes, elas não se conectarão. Se ambas as extremidades estiverem em diferentes modos duplex, elas serão conectadas pela metade do modo.

Status da Porta (Port Status)

Port Status mostra o status da porta atual. Inclui tipo de conexão, o status do link da porta, o modo de velocidade e modo duplex operando e a configuração de controle de fluxo.

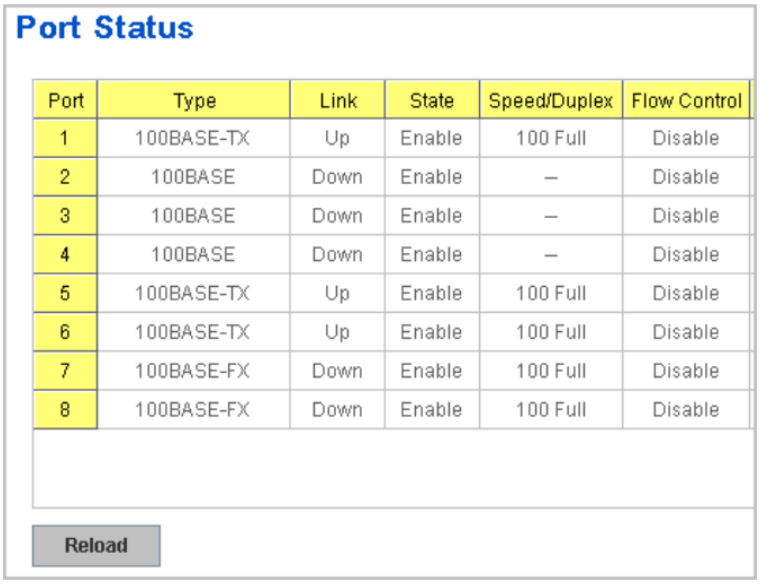

Figura 4-28. Port Status Exemplo

Descrição das colunas:

Port: Número de interface da porta

Type: 100BASE -> Porta Fast Ethernet

Link: Status do link. Up-> Link UP. Down -> Link Down

State: Enable -> Estado habilitado. Disable -> A porta é desabilitada pelo usuário configurado

Speed/Duplex: Status atual de operação da porta

Flow Control: Estado de controle de fluxo

Controle de Taxa (Rate Control)

Controle de taxa é uma forma de controle de fluxo usado para impor um limite de largura de banda a uma porta. O usuário pode programar os limites de taxa de transmissão e recepção (Egress/Ingress Rules) separadamente para cada porta e aplicar este limite para determinados tipos de pacotes, conforme descrito na Figura 4-29.

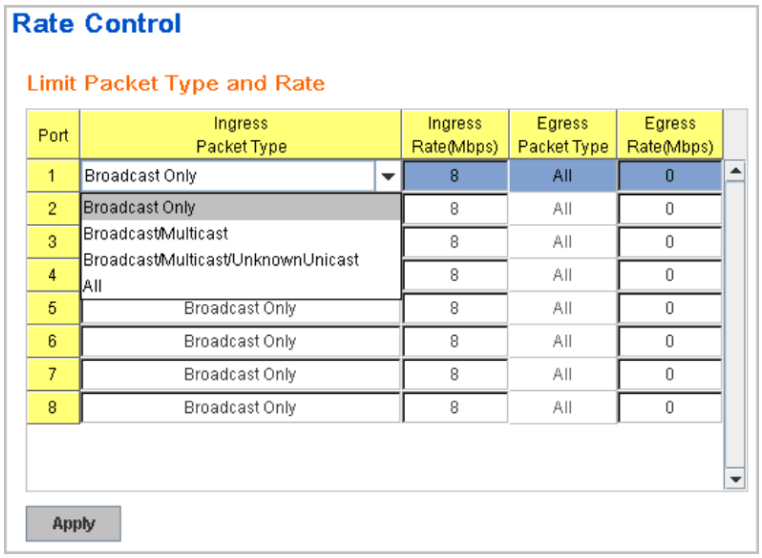

Figura 4-29. Exemplo de Controle de Taxa

O Rate Control é uma forma de controle de fluxo usada para restringir uma banda de usi a uma porta. É possível configurar regras separadamente para cada porta, como limites, quantia de pacotes, programa de transmissão separada (Egress Rule) e recepição (Ingress Rule)

Packet type: Selecione o tipo de pacote a ser filtrado. Os tipos de pacotes Ingress Rule (entrada) disponíveis são: Broadcast Only (somente), Broadcast/multicast, Broadcast/Multicast/Unknown (desconhecido), Unicast, e All (Todos). Já os Egress Rule (saída) suportam todos os tipos de pacotes (All).

Rate: Esta coluna permite atribuir manualmente a taxa limite da porta. Valores válidos suportados: 1Mbps – 100Mbps para porta Ethernet de Alta Velocidade. O passo de taxa é de 1 Mbps. O valor padrão de Ingress Regra é 8 Mbps; valor padrão da regra Egress é 0 Mbps. 0 significa a desativação do controle de velocidade para a porta

Para habilitar a função de controle de taxa, clique no botão *Apply*.

Entroncamento de Porta (Port Trunking)

A configuração de Port Trunking permite agrupar várias portas Ethernet em paralelo para aumentar a largura de banda do link. As portas de agregados podem ser vistas como uma porta física, de modo que a largura de banda é maior do que apenas uma única porta Ethernet. As portas membro do mesmo grupo de entrocamento podem equilibrar a carga e backup para outra. O recurso Port Trunking geralmente é usado quando se precisa de maior largura de banda para a rede backbone. Esta é uma maneira barata para que se possa transferir mais dados.

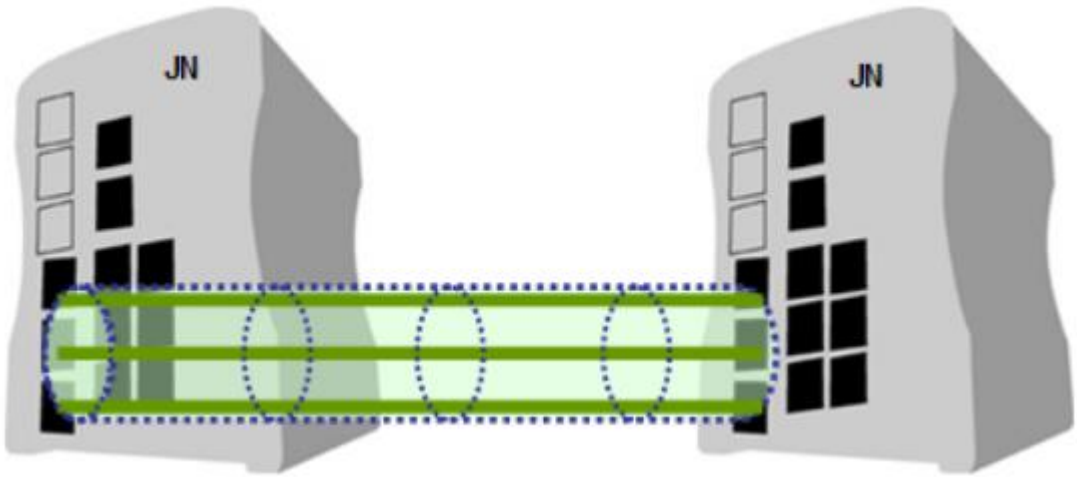

Figura 4-30. Exemplo de Port Trunking

Existem algumas descrições diferentes para o entroncamento de portas. Diferentes fabricantes podem usar diferentes descrições para seus produtos, como Link Aggregation Group (LAG), Link Aggregation Control Protocol, Ethernet Trunk, Ether Channel... etc. A maioria das implementações estão em conformidade com o padrão IEEE, 802.3ad.

As portas agregadas podem se interligar para outro interruptor que também suporta Port Trunking. Korenix Suporta dois tipos de porta de entroncamento. Um deles é estático Trunk, o outro é 802.3ad. Quando a outra extremidade usa 802.3ad LACP, deve se atribuir 802.3ad LACP para o tronco. Quando a outra extremidade usa não-802.3ad, você pode então usar estático Trunk.

Existem duas páginas de configuração, Aggregation Setting e Aggregation Status.

Aggregation Settings

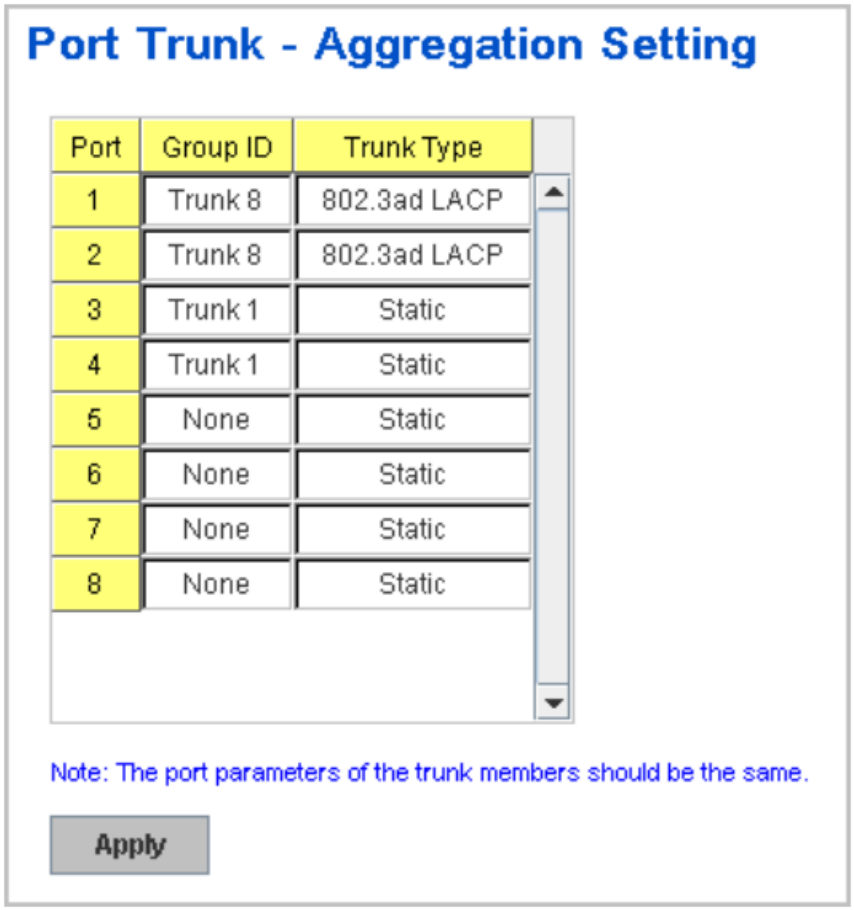

Figura 4-31. Configurações de Agregação de Portas

Trunk Size: O Switch pode suportar até 4 grupos de entroncamento e 8 portas como máxima quantia de membros por grupo.

Group ID: É a identificação do grupo de entroncamento de portas. Portas como o mesmo Group ID pertencem ao mesmo grupo.

Trunk Type: Static e 802.3ad LACP. Cada grupo de entroncamento suporta Static ou 802.3ad LACP. Escolha de acordo com a necessidade.

Agregação de Portas (Aggregation Status)

Esta página mostra o status de agregação de portas. Uma vez que as portas de agregação são negociadas, você verá o seguinte status.

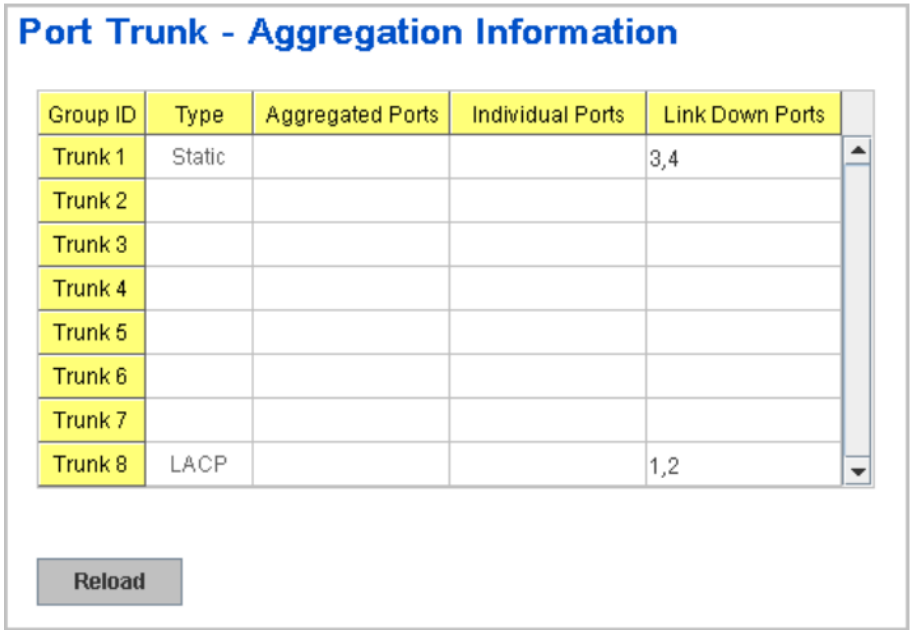

Figura 4-32. Informações de Status 0 Port Trunk Aggregation

Group ID: Exibe Trunk 1 à Trunk8 criado em Agregation Settings. Tipo: Static ou LACP criada em Aggregation Settings. (O JN4508 suporta apenas quatro grupos de entroncamentos).

Aggregated Ports: Quando os links LACP estão operando, se pode ver as portas membro na coluna *aggregated*.

Individual Ports: Quando LACP estiver habilitado, portas membro do grupo LACP que não estão ligados corretamente às portas membro de LACP serão exibidos na coluna *Individual*.

Link Down Ports: Quando LACP estiver habilitado, portas membro do grupo LACP que não estão conectadas serão exibidas na coluna *Link Down*.

Linhas de Comando para Configuração de Portas

Característica	Linha de Comando
Controle da Porta	
Controle da Porta - Estado	Switch(config-if)# shutdown -> Disable port state Port1 Link Change to DOWN interface fastethernet1 is shutdown now. Switch(config-if)# no shutdown -> Enable port state Port1 Link Change to DOWN Port1 Link Change to UP interface fastethernet1 is up now. Switch(config-if)# Port1 Link Change to UP
Controle de Porta – Auto Negociação	Switch(config)# interface fa1 Switch(config-if)# auto-negotiation Auto-negotiation of port 1 is enabled
Controle de Porta – Forçar Velocidade/Duplex	Switch(config-if)# speed 100 Port1 Link Change to DOWN set the speed mode ok! Switch(config-if)# Port1 Link Change to UP Switch(config-if)# duplex full Port1 Link Change to DOWN set the duplex mode ok! Switch(config-if)# Port1 Link Change to UP
Controle de Porta – Fluxo Controle	Switch(config-if)# flowcontrol on Flowcontrol on for port 1 set ok! Switch(config-if)# flowcontrol off

	Flowcontrol off for port 1 set ok!
Status da Porta	
Status da Porta	Switch# show interface fa1 Interface fastethernet1 Administrative Status: Enable Operating Status: Connected Duplex: Full Speed: 100 Flow Control:off Default Port VLAN ID: 1 Ingress Filtering: Disabled Acceptable Frame Type: All Port Security: Disabled Auto Negotiation: Disable Loopback Mode: None STP Status: forwarding Default CoS Value for untagged packets is 0 Mdix mode is Disable. Medium mode is Copper. Nota: StatusAdministrativo -> estado do porta. Estado de funcionamento -> status atual da porta. Duplex -> modo duplex da porta. Velocidade -> modo velocidade da porta. Controle de Fluxo -> Estado de controle de fluxo da porta
Controle de Taxa	
Controle de taxa – Entrada ou Saída	Switch(config-if)# rate-limit egress Outgoing packets ingress Incoming packets Nota: Para habilitar o controle de taxa, selecione a regra de Entrada ou Saída primeiro e, após, atribua o tipo de pacote e largura de banda
Controle de Taxa – Filtro Tipo de Pacote	Switch(config-if)# rate-limit ingress mode all Limit all frames broadcast Limit Broadcast frames flooded-unicast Limit Broadcast, Multicast and flooded unicast frames multicast Limit Broadcast and Multicast frames Switch(config-if)# rate-limit ingress mode broadcast Set the ingress limit mode broadcast ok
Controle de Taxa Largura da Banda	Switch(config-if)# rate-limit ingress bandwidth <0-100> Limit in magabits per second (0 is no limit) Switch(config-if)# rate-limit ingress bandwidth 8 Set the ingress rate limit 8Mbps for Port 1
Port Trunking	
LACP	Switch(config)# lacp group 1 fa6-8 Group 1 based on LACP(802.3ad) is enabled! **Nota:** A lista de interface é fa1-8 **Nota:** Diferentes velocidades de porta não podem ser agrupadas junto
Static Trunk	Switch(config)# trunk group 2 fa4-5 Trunk group 2 enable ok!
Display LACP	Swhitch# show lacp internal LACP group 1 internal information: LACP Port Admin Oper Port Port Priority Key Key State ------ ------ ------ ------ ------ 6 1 6 6 0x45 7 1 7 7 0x45 8 1 8 8 0x45 LACP group 2 is inactive LACP group 3 is inactive LACP group 4 is inactive

Display Trunk	Switch# show trunk group 1 FLAGS: I -> Individual P -> In channel D -> Port Down Trunk Group GroupID Protocol Ports -------- --------- --------- 1 LACP 6(D) 7(D) 8(D) Switch# show trunk group 2 FLAGS: I -> Individual P -> In channel D -> Port Down Trunk Group GroupID Protocol Ports -------- --------- --------- 2 Static 4(D) 5(P) Switch#

Tabela 4-10. Configuração de Linhas de Comandos por Porta

Redundância de Rede

No que se refere a aplicações industriais, é fundamental que as redes trabalhem continuamente. Os seguintes modos são suportados pelo JN4508F-M: RSTP padrão, Multiple Super Ring, Rapid Dual Homing e Legacy Super Ring Client.

A tecnologia de Múltiplos Super Anéis (MSR) é a 3ª geração do em redundância de anéis. Esta tecnologia foi patenteada e é protegida, sendo utilizada em diversos países ao redor do mundo. A tecnologia MSR é classificada mundialmente como a mais rápida em tempos de restauração (0 ms) e recuperação de falhas no mundo (> 5 ms).

A tecnologia avançada Rapid Dual Homing facilita a conexão do JN4508F-M com o núcleo gerenciado do switch (via Protocolo padrão de árvore de abrangência rápida. Com a tecnologia RDH, o usuário também pode executar RSTP para acoplar vários Rápidos Super Anéis, (também conhecido como Auto Ring Coupling).

Para se tornar compatível com a tecnologia Legacy Super Ring implementada nos switches o JN4508F-M também suporta o modo cliente Super Anel. As portas Super Anéis passam com facilidade através dos pacotes de controle.

Além da tecnologia de anel, o JN4508F-M também suporta 802.1 D-2004 versão Rapid Spanning Tree Protocol (RSTP). A nova versão do RSTP padrão inclui 802.1 D-1998 STP, 802.1 w RSTP, IEEE 802.1s MSTP (Multiple Spanning Tree). A função MSTP está disponível a partir da versão 1.1 de firmware.

Configuração STP (STP Configuration)

Esta página permite selecionar o modo de STP e configurar STP / RSTP Bridge global.

O modo de STP inclui o STP, RSTP, MSTP e Disable. Por favor, selecione o modo de STP para o seu sistema em primeiro lugar. O modo padrão é RSTP habilitado.

Depois de seleccionar o modo RSTP ou STP; continue a configurar os parâmetros globais de STP Bridge e RSTP.

Depois de selecionar o modo de MSTP, por favor, vá à página de configuração MSTP.

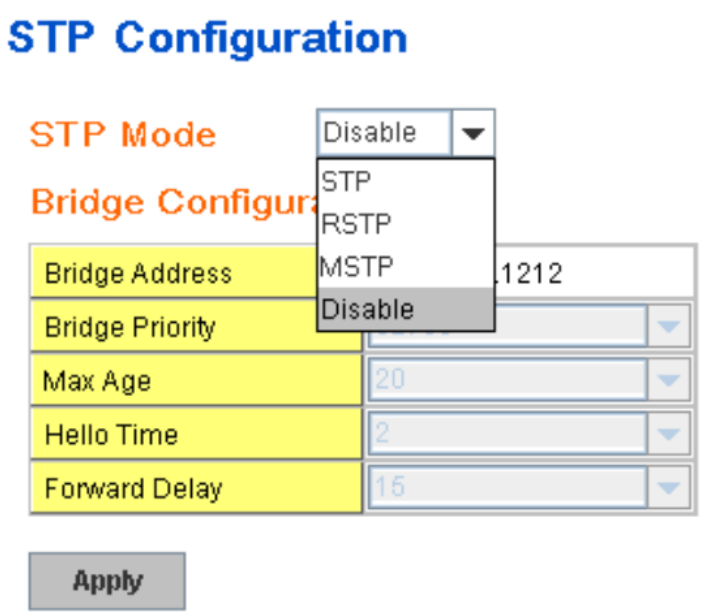

Figura 4-33. STP Configuration

RSTP

RSTP significa Rapid Spanning Tree Protocol. Se um switch tem mais de um caminho para um destino, ele pode gerar loopings de mensagens que podem gerar tempestades de difusão e rapidamente sobrecarregar uma rede. A árvore de expansão foi criado para combater os efeitos negativos de loops de mensagens em redes comutadas. Uma árvore de expansão usa um algoritmo de árvore estendida (STA) para detectar automaticamente se um switch tem mais de uma maneira de se comunicar com um nó. Ele irá, em seguida, selecionar o melhor caminho (primário), e bloquear o outro caminho (s). Ele também irá acompanhar o caminho bloqueado (s), caso o caminho principal pare de funcionar. Spanning Tree Protocol (STP) introduziu um método padrão para alcançar este objetivo. Ele é especificado na IEEE 802.1D-1998. Mais tarde, o Rapid Spanning Tree Protocol (RSTP), foi aprovado e representa a evolução do STP, que prevê uma convergência muito mais rápida em uma mudança de topologia. Isso é especificado na IEEE 802.1w. Em 2004, a 802.1we foi incluída na versão 802.1D-2004. Este switch suporta tanto RSTP e STP (todos os switches que suportam RSTP também são compatíveis com switches que suportam apenas STP).

Depois de selecionar o modo de MSTP, por favor, vá à página de configuração MSTP.

Configuração de Ponte

Bridge Address: Mostra o endereço MAC do switch.

Priority (0-61440): O RSTP utiliza uma ID para determinar a ponte raiz (aquela que apresentar o ID mais alto). A ponte ID é composta dos itens prioridade e endereço MAC (a ponte com prioridade superior se torna a ID mais alta). Se todos as IDs apresentarem a mesma prioridade, a ponte com o menor endereço MAC se tornará a ponte raiz.

Nota:

O valor da prioridade de ponte deve ser em múltiplos de 4096. Um dispositivo com um número inferior tem uma prioridade mais alta. Ex: 4096 é superior a 32768.

Max Age (6-40): Insira um valor entre 6 e 40 segundos. Esse valor representa o tempo de espera da suportado pela ponte sem receber as mensagens de configuração do protocolo STP antes de tentar reconfigurá-la.

Se o JN4508F-M não for a ponte raiz e não tiver recebido nenhuma mensagem (*Hello Message*) no período determinado no campo *Max Age*, ele será reconfigurado como a ponte raiz. Uma vez que

dois ou mais dispositivos na rede tenham sido reconhecidos como ponte raiz, os mesmos renegociarão a configuração da nova topologia.

Hello Time (1-10): Insira um valor ente 1 e 10 segundos. Este campo refere-se ao timer periódico que impulsiona o switch a enviar um pacote BPDU (Bridge Protocol Data Unit) para verificar o status STP atual.

A ponte raiz da topologia da árvore de abrangência envia, periodicamente, uma mensagem aos outros dispositivos da rede para verificar se a topologia é adequada. O tempo determinado em *hello time* refere-se ao intervalo de tempo de envio entre as mensagens.

Forward Delay Time (4-30): Insira um valor entre 4 e 30 segundos. Este valor refere-se ao tempo que a porta aguarda antes de ser alterada de Protocolo STP e escutar o estado de encaminhamento.

É o tempo aguardado pelo JN4508F-M antes de verificar para se deve ou não alterar seu estado.

Uma vez concluída a configuração, clique no botão *Apply*.

Nota:

Observe as regras abaixo em relação aos parâmetros *Hello Time*, *Forwarding Delay*, e *Max Age*.

2 × (Forward Delay Time – 1 seg) > = Max Age Time > = 2 × (Hello Time + 1 seg)

Configuração de Porta STP (STP Port Configuration)

Esta página permite a configuração de parâmetros da porta após habilitar STP ou RSTP.

Configuração de Porta (Port Configuration)

Ao selecionar a porta a ser configurada, o usuário visualizará as configurações atuais e o status da porta.

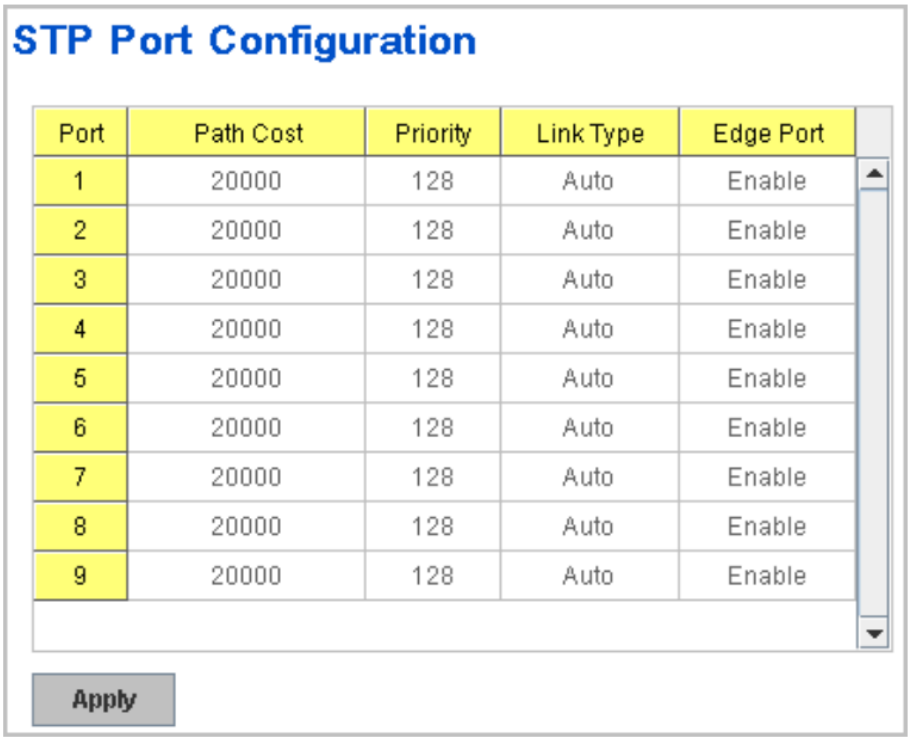

Figura 4-34. Configuração de Porta STP

Path Cost: Insira um valor entre 1 e 200.000.000. Esse valor representa o custo do caminho para a outra ponte pela porta de transmissão na porta especificada.

Priority: Insira um valor entre 0 e 240 usando múltiplos de 16. Este é o valor que decide qual porta deve ser bloqueada considerando a prioridade em uma LAN.

Link Type: Existem 3 tipos selecionáveis. Auto, P2P e Share.

Determinadas transições rápidas de estado no RSTP dependem de alguns fatores, a saber: se a porta em questão pode ser conectada somente a outra ponte (servida por um segmento LAN de ponto a ponto), ou se pode ser conectada a duas ou mais pontes (servida por um segmento LAN de mídia compartilhada). Esta função permite o estado P2P do link a ser manipulado administrativamente. A opção *Auto* significa a escolha automática do modo P2P (ativado) ou Share (P2P desabilitado).

Edge: Uma porta conectada diretamente as estações finais não é possível criar um loop de pontes na rede. Para configurar uma porta para este estado, selecione a opção *Enable* (habilitar). Quando o dispositivo «não-ponte» se conecta a uma porta *edge* de administrador, ela será bloqueada por 4 segundos e então será encaminhada ao próximo estado.

Após finalizar as configurações, clique em *Apply*.

Informações RSTP (RSTP Information)

Esta página exibe informações sobre o switch raiz e o estado da porta.

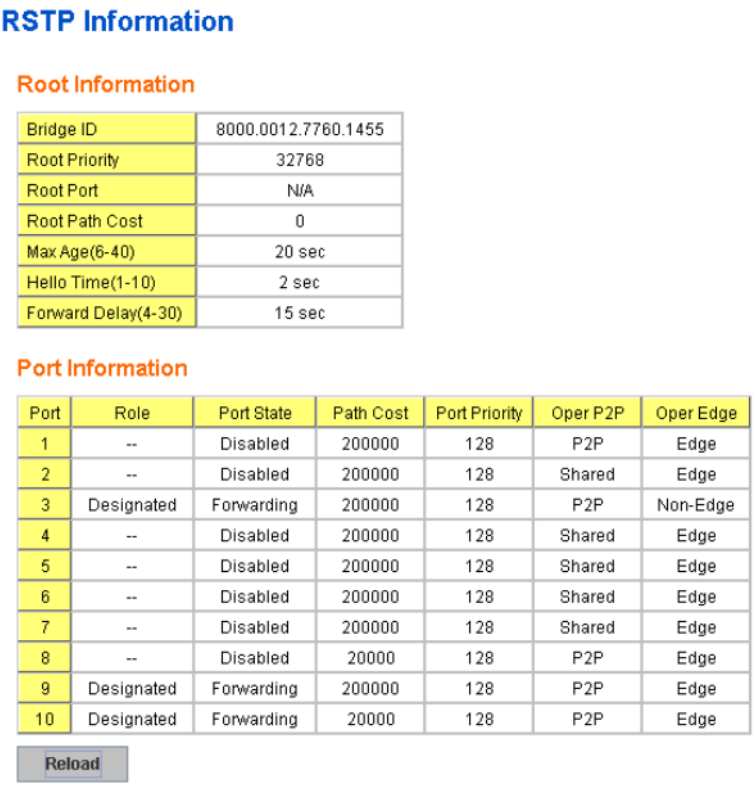

Figura 4-35. Informações de RSTP

Root Information: Exibe os campos *Root Bridge ID, Root Priority, Root Port, Root Path Cost* e *Max Age, Hello Time, Forward Delay* referentes BPDU enviados do switch raiz.

Port Information: Exibe os campos *Role, Port State, Path Cost, Port Priority,* e os modos *Oper P2P* e *Oper edge*.

Configuração MSTP (Multiple Spanning Tree Protocol)

MSTP é a abreviação de Multiple Spanning Tree Protocol. Este protocolo é uma extensão direta de RSTP. Ele pode fornecer uma árvore geradora independente para diferentes VLANs. Ele simplifica o gerenciamento de rede, prevê a convergência ainda mais rápido do que RSTP ao limitar o tamanho

de cada região, e impede que os membros da VLAN de serem segmentados do resto do grupo (como às vezes ocorre com IEEE 802.1D STP).

Enquanto estiver usando MSTP, existem alguns novos conceitos de arquitetura de rede. Um switch pode pertencer a grupo diferente, age como root switch ou designar, gerar BPDU para a rede para manter a tabela de encaminhamento da árvore de expansão. Com MSTP, ele também pode fornecer vários caminhos de encaminhamento e permitir balanceamento de carga. Compreender a arquitetura permite-lhe manter a árvore de expansão correta e operar de forma eficaz.

Uma VLAN pode ser mapeada para um Multiple Spanning Tree Instance (MSTI). A máxima quantia de instâncias suportada peloJN4508F-M é 16, faixa de 0-15. O MSTP constrói uma árvore separada Multiple Spanning (MST) para cada instância para manter a conectividade entre cada um dos grupos de VLANs atribuídas. Um Internal Spanning Tree (IST) é usado para conectar todos os interruptores MSTP dentro de uma região MST. Uma Região MST pode conter várias instâncias MSTP.

A Figura 4-36 mostra que há duas instâncias MSTP / VLANs e cada instância tem a sua raiz e encaminhamento caminhos.

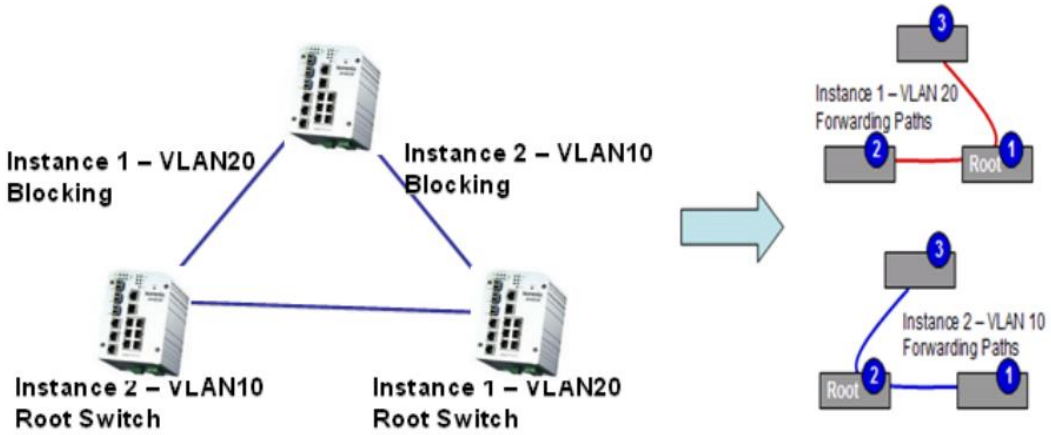

Figura 4-36. Exemplo MSTP

Uma Common Spanning Tree (CST) interliga todas as regiões adjacentes do MST e age como um nó/ponte virtual para comunicações com STP ou RSTP rede global. MSTP conecta todas as pontes e segmentos da LAN com um único Spanning Tree Comum e Interno (CIST). A CIST é formado como resultado do algoritmo de árvore estendida correndo entre os switches que suportam os protocolos STP, RSTP, MSTP.

A Figura 4-37 mostra a grande rede CST. Nessa rede, a Região pode ter diferentes instâncias e seu próprio caminho de encaminhamento e de tabela; no entanto, ela atua como uma única Bridge da CST.

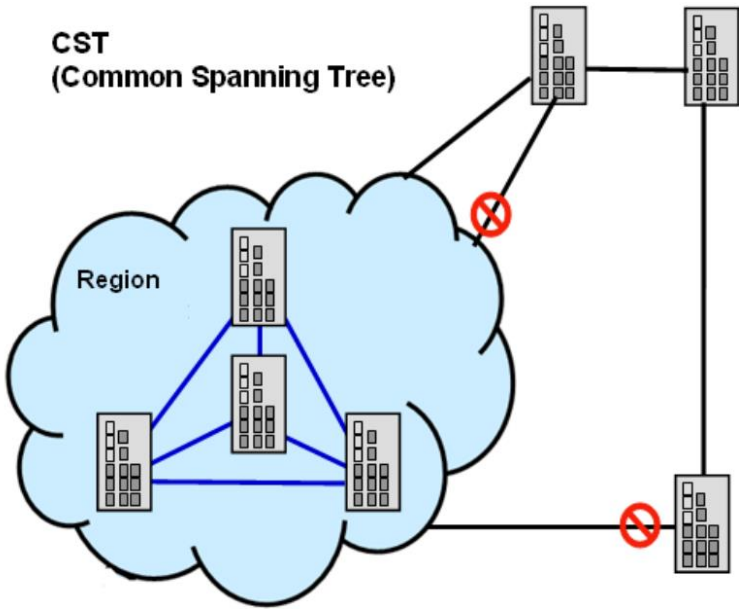

Figura 4-37. Exemplo CST

Para modificar as configurações de MSTP, o modo STP das configurações da página STP precisam ser alterados para MSTP primeiro.

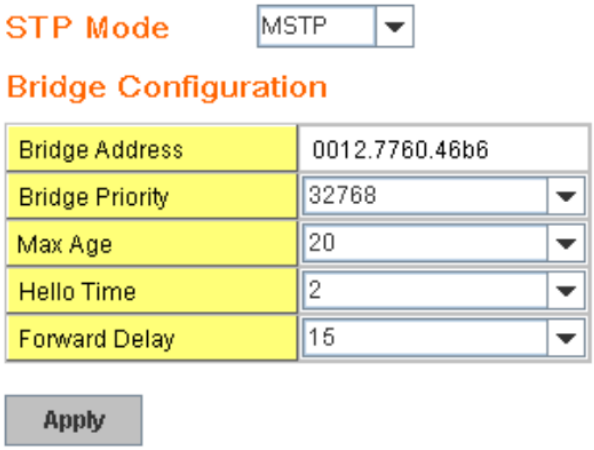

Figura 4-38. Modo STP – Configuração em Bridge

Configuração de Região MSTP (Region)

Esta página permite configurar o nome da região e sua revisão, o mapeamento da VLAN a Instância e verificar a configuração atual da Instância MST. A rede pode ser dividida virtualmente em diferentes regiões. Os switches dentro da Região devem ter a mesma *Region Name* e *Revision*.

Region Name: O nome para a Região. Comprimento máximo: 32 caracteres.

Revision: A revisão para a Região. Intervalo: 0-65535; Padrão: 0) Depois de terminar a configuração, clique em Aplicar para aplicar as configurações.

Nova MST Instância

Esta página permite o mapeamento da VLAN à Instância e atribuir prioridade à instância. Antes de do mapeamentoda VLAN para a instancia, deve se criar uma VLAN e atribuir as portas membro primeiro. Por favor, consulte a página de configuração de VLAN.

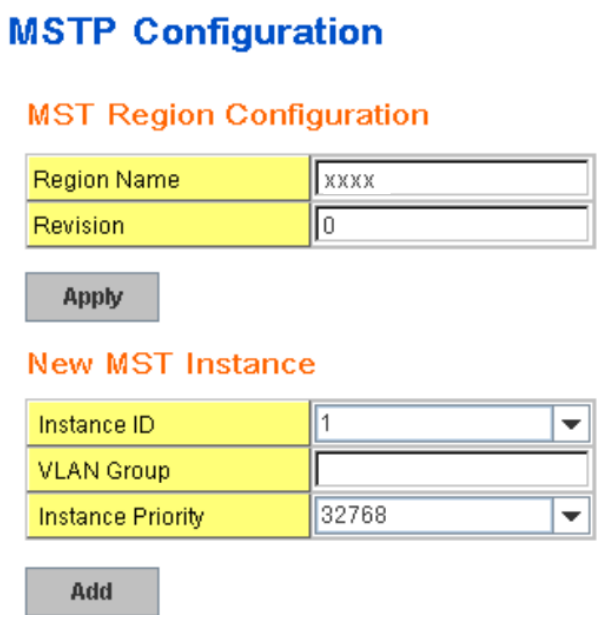

Figura 4-39. Configuração MSTP

Instance ID: Selecionar o ID da Instância, entre 1-15.

VLAN Group: ID da VLAN a ser mapeamado à instância.

Instance Priority: Atribui a prioridade a instância.

Após terminar a configuração, click em *Add* para aplicar as mudanças.

Configuração da Instância MST Corrente

Esta página permite a configuração da Instância MST adicionada anteriormente. Clique em Apply para aplicar as configurações. Pode se remover uma instância através do botão *Remove* ou recarregar uma configuração nesta pagina atrás do botão *Reload*.

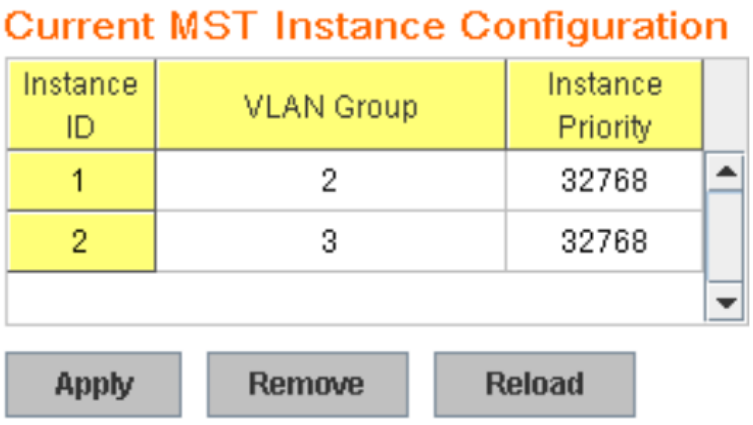

Figura 4-40. Configuração Atual da Instância MST

Multiple Super Ring (MSR)

A redundância de rede industrial mais comum é para formar um anel ou loop. Tipicamente, os switches de gestão são ligados em série, um switch conectado aoanterior e o último é ligado de volta para ao primeiro. Em tal conexão, você pode usar a tecnologia Super Ring para obter um desempenho de recuperação mais rápido.

Tecnologia Multiple Super Ring (MSR) é a tecnologia de redundânciade Anel de 3ª geração. Isto é usado em países de todo o mundo. A MSR classifica o tempo mais rápido e restaura a falha com a maior velocidade, 0 ms para restaurar e aproximadamente na casa de milissegundos para falha em portas 100Base-TX. A outra interface pode demorar mais tempo, devido às características do material, como o cobre.

A tecnologia Advanced Rapid Dual Homing (RDH) também facilita ao JN4508F-M Switch Gerenciável para se conectar com um switch de gestão fácil e conveniente. Com a tecnologia RDH, também se pode usar vários Super Rings rápidos ou RSTP em uma nuvem, juntos, o que também é conhecido como Auto Ring Coupling.

A tecnologia TrunkRing permite integrar MSR com LACP / Port Trunking. O LACP / Trunk agrega portas a uma interface virtual e pode funcionar como uma porta Anel do MSR.

MultiRing é uma tecnologia excelente que o Switch Korenix pode suportar. Vários anéis podem ser agregados no prazo de um switch usando diferentes ID Rings. O número máximo de anéis que um switch pode suportar é a metade do volume total das portas. Por exemplo, o JN4508F-M é com um projeto Switch Fast Ethernet para 8 porta terá no máximo de 4 Anéis (4 Anéis 100Mbps) podem ser agregados em um JN4508F-M. O recurso poupa muito esforço na construção de arquiteturas de redes complexas.

Para se tornar compatível com a tecnologia Super Ring implementada no JN4508F-M o modo Cliente Super Ring também deve ser suportado. As portas Super Ring podem passar pacotes de controle através do Super Ring de forma extremamente rápida e sem erros.

New Ring: Para criar um Super Ring. Apenas preencha o ID do anel entre a faixa de 0 a 31. Se o campo do nome é deixado em branco, o nome desse anel será automaticamente como Ring ID.

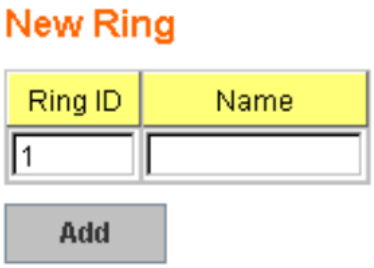

Figura 4-41. New Ring

Configuração do Anel (Ring Configuration)

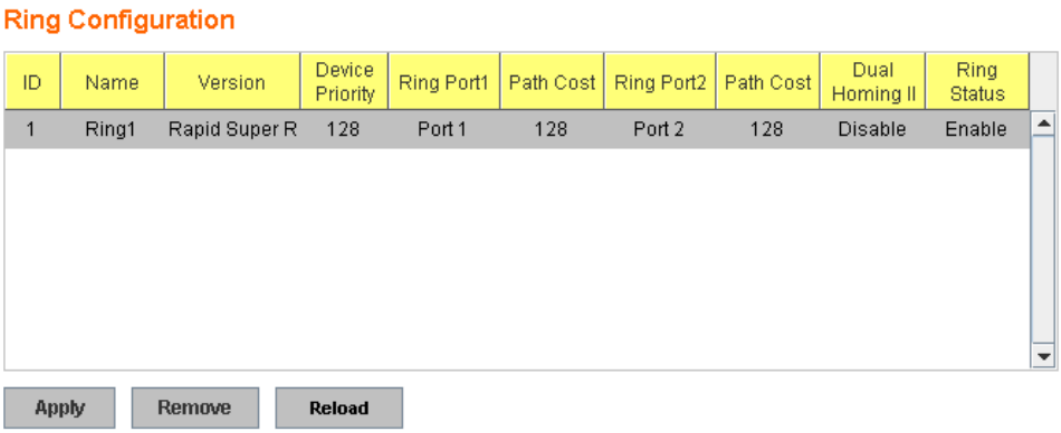

Figura 4-42. Ring Configuration

ID: Uma vez criado um Anel, os campos a seguir não poderão ser alterados.

Name: Este campo mostra o nome do anel. Se não foi preenchido no momento da criação, o anel será automaticamente nomeado pela regra de *RingID*.

Version: Altera a versão do anel. São disponibilizadas duas opções: Anel Super Rápido (padrão) e Super Anel (para ser compatível com a primeira geração de anéis).

Device Priority: O switch com prioridade mais alta (maior valor) será automaticamente selecionado como Anel Mestre. Uma das portas do anel neste switch será a porta de entrada e a outra será a porta de bloqueio. Se todos os switches apresentam prioridade igual, o switch com o endereço MAC maior será selecionado como anel mestre.

Ring Port1: No ambiente de Anel Super Rápido são necessárias 2 portas. Independentemente de ser o anel mestre ou não, devem ser selecionadas 2 portas para atuarem como Ring Ports no momento da configuração do RSR. Em relação ao anel mestre, uma das portas do anel será a porta de entrada e a outra será a porta de bloqueio.

Path Cost: Altere o *Path Cost* do anel Port1. Se este switch for o anel mestre, ele determinará o bloqueio da porta. A porta com o Path Cost mais elevado (em uma topologia de dois anéis) se tornará a porta de bloqueio. Caso apresentem o mesmo valor, a porta que apresentar número maior será a de bloqueio.

Ring Port2: Atribui outra porta para a conexão do anel

Path Cost: Altera o *Path Cost* do anel Port2

Rapid Dual Homing: Rápido Dual Homing é uma importante característica da terceira geração em tecnologia de redundância de anel. Esta funcionalidade permite vários links para redundância quando o usuário deseja se conectar a múltiplos RSR ou formar topologias redundantes com outros fornecedores. O uplink máximo é 7 por grupo.

Dual Homing: No Dual Homing é necessário configurar uma porta adicional (como porta Dual Homing) para dois switches de uplink. No Rapid Dual Homing, não é necessário configurar uma porta específica para conectar-se a outro protocolo. O Rapid Dual Homing inteligentemente escolhe o link mais rápido como link principal e bloqueia os outros para evitar loops. Caso haja uma falha no link principal, esta tecnologia encaminha automaticamente o link secundário para rede redundante. Naturalmente, se houverem mais links, estes permanecerão em espera para serem utilizados em caso de falha dos links principal e secundário.

Ring status: Habilita/desabilita o anel. Lembre-se de habilitar o anel depois de adicioná-lo.

MultiRing: A tecnologia MultiRing é um dos padrões da tecnologia MSR; ele permite que agregar múltiplos anéis dentro de um switch. Criar múltiplos RingIDs e atribuir uma porta diferente para cada anel, portanto, o switch JN4508F-M pode ter vários anéis.

Ao implementar o MultiRing, lembre-se que os diferentes anéis não pode usar o mesmo ID anel. As outras configurações são as mesmas que da descrição acima. Tecnicamente, o numero máximo dos anéis MultiRing suportado é de até 16 anéis. Devido ao número limitado de portas, o número da rede em anel, é a metade do número de portas.

TrunkRing: A tecnologia MultiRing é parte da tecnologia que combina a MSR com a tecnologia de entroncamento de porta. Depois de várias portas agregadas, este é o entroncamento de portas assim-chamado (Staticly ou aprendido por protocolo LACP), o Trunk ID pode ser um dos IDs da porta da tecnologia MSR. Configurando o entroncamento de portas primeiro, aí pode se adicionar o grupo Trunk como uma porta de anel no switch gerenciável.

Informações do Anel (Ring Information)

Esta página mostra informações do MSR.

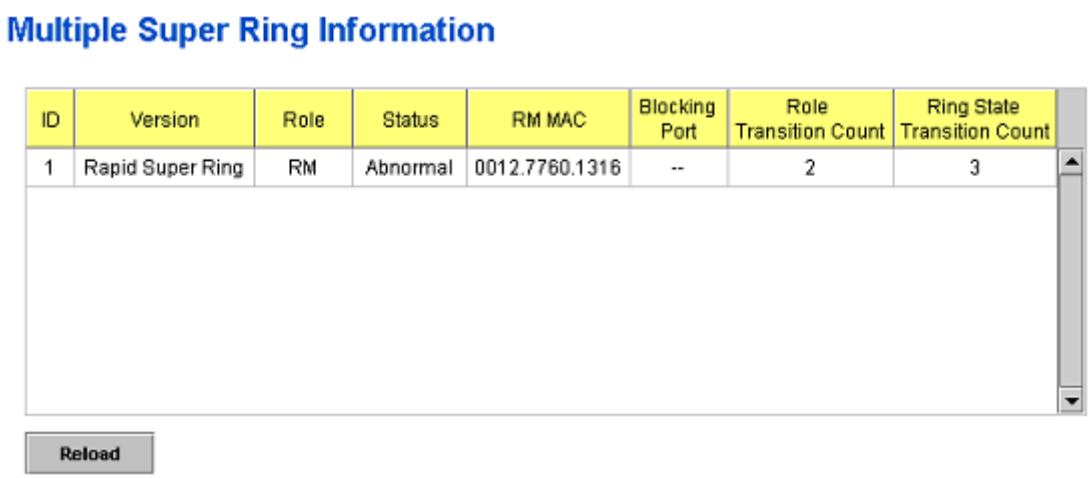

Figura 4-43. Informações MSR

ID: Identificação do anel.

Version: informa a versão do anel, (Rapid Super Ring ou Super Ring).

Role: Este switch é RM ou nonRM

Status: Se em estado Normal, a redundância está aprovada. Se qualquer um dos links do anel estiver interrompido, o status será anormal (*Abnormal*).

RM MAC: Endereço MAC do anel mestre deste anel. Ajuda a encontrar o caminho redundante.
Blocking Port: Este campo mostra qual porta do RM está bloqueada.

Role Transition Count: Informa quantas vezes o switch foi alterado de nonRM para RM e vice-versa.

Role State Transition Count: Informa quantas vezes o estado do anel foi alterado de normal e anormal.

Linhas de Comando para Redundância de Rede

Característica	Linha de Comando
Globa (STP, RSTP, MSTP)	
Habilita	Switch(config)# spanning-tree enable
Desabilita	Switch(config)# spanning-tree disable
Modo (Escolha Spanning Tree mode)	Switch(config)# spanning-tree mode rst the rapid spanning-tree protocol (802.1w) stp the spanning-tree prtotcol (802.1d) mst the multiple spanning-tree protocol (802.1s)
Prioridade da Bridge	Switch(config)# spanning-tree priority <0-61440> valid range is 0 to 61440 in multiple of 4096 Switch(config)# spanning-tree priority 4096
Tempo de Bridge	Switch(config)# spanning-tree bridge-times (forward Delay) (max-age) (Hello Time) Switch(config)# spanning-tree bridge-times 15 20 2 This command allows you configure all the timing in one time.
Delay à Frente	Switch(config)# spanning-tree forward-time <4-30> Valid range is 4~30 seconds Switch(config)# spanning-tree forward-time 15
Tempo máximo	Switch(config)# spanning-tree hello-time <1-10> Valid range is 1~10 seconds Switch(config)# spanning-tree hello-time 2
MSTP	
Configure a Árvore de	Switch(config)# spanning-tree mst

MSTP	MSTMAP the mst instance number or range Configuration-> enter mst configuration mode forward-time-> the forward dleay time hello-time-> the hello time max-age-> the message maximum age time max-hops-> the maximum hops sync-> sync port state of exist vlan entry Switch(config)# spanning-tree mst configuration Switch(config)# spanning-tree mst configuration Switch(config-mst)# abort-> exit current mode and discard all changes end-> exit current mode, change to enable mode and apply all changes exit-> exit current mode and apply all changes instance-> the mst instance list-> Print command list name-> the name of mst region no-> Negate a command or set its defaults quit-> exit current mode and apply all changes revision-> the revision of mst region show-> show mst configuration
Configuração de Região	Region Name: Switch(config-mst)# name NAME the name string Switch(config-mst)# name altus Region Revision: Switch(config-mst)# revision <0-65535> the value of revision Switch(config-mst)# revision 65535
Mapear Instância VLAN (Ex: Mapear VLAN 2 para Instância 1)	Switch(config-mst)# instance <1-15> target instance number Switch(config-mst)# instance 1 vlan VLANMAP target vlan number(ex.10) or range(ex.1-10) Switch(config-mst)# instance 1 vlan 2
Mostra a configuração MST atual	Switch(config-mst)# show current Current MST configuration Name [xxxx] Revision 65535 Instance Vlans Mapped ---------- 0 1,4-4094 1 2 2 3 ---------- Config HMAC-MD5 Digest: 0xB41829F9030A054FB74EF7A8587FF58D ----------
Remove o nome da Região	Switch(config-mst)# no name name configure revision revision configure instance the mst instance Switch(config-mst)# no name
Remove Instance example	Switch(config-mst)# no instance <1-15> target instance number Switch(config-mst)# no instance 2
Mostra as Configurações de MST pendentes	Switch(config-mst)# show pending Pending MST configuration Name [] (->The name is removed by no name) Revision 65535 Instance Vlans Mapped -------- ---------- 0 1,3-4094 1 2 (->Instance 2 is removed by no instance 2)

	---------- Config HMAC-MD5 Digest: 0x3AB68794D602FDF43B21C0B37AC3BCA8 ----------
Aplica as configurações e vai para o modo de configuração	Switch(config-mst)# quit apply all mst configuration changes Switch(config)#
Aplica as configurações e vai para o modo global	Switch(config-mst)# end apply all mst configuration changes Switch#
Abortar a definição e ir para o modo de configuração. Mostrar Pendencias para ver as novas configurações não aplicadas	Switch(config-mst)# abort discard all mst configuration changes Switch(config)# spanning-tree mst configuration Switch(config-mst)# show pending Pending MST configuration Name [korenix] (->The nameis not applied after Abort settings.) Revision 65535 Instance Vlans Mapped ---------- 0 1,4-4094 1 2 2 3 (-> The instance is not applied after Abort settings.) ---------- Config HMAC-MD5 Digest: 0xB41829F9030A054FB74EF7A8587FF58D ----------
RSTP	
Configurações de Sistema RSTP	The mode should be rst, the timings can be configured in global settings listed in above.
Configuração do Modo de Porta	
Configuração da Porta	Switch(config)# interface fa1 Switch(config-if)# spanning-tree bpdufilter-> a secure BPDU process on edge-port interface bpduguard-> a secure response to invalid configurations (received BPDU sent by self) cost-> change an interafce's spanning-tree port path cost edge-port-> interface attached to a LAN segment that is at the end of a bridged LAN or to an end node link-type-> the link type for the Rapid Spanning Tree mst-> the multiple spanning-tree port-priority-> the spanning tree port priority
Custo de Trajetória	Switch(config-if)# spanning-tree cost <1-200000000> 16-bit based value range from 1-65535, 32-bit based value range from 1-200,000,000 Switch(config-if)# spanning-tree cost 200000
Prioridade da Porta	Switch(config-if)# spanning-tree port-priority <0-240> Number from 0 to 240, in multiple of 16 Switch(config-if)# spanning-tree port-priority 128
Tipo de Link – Auto	Switch(config-if)# spanning-tree link-type auto
Tipo de Link – P2P	Switch(config-if)# spanning-tree link-type point-to-point
Tipo de Link – Share	Switch(config-if)# spanning-tree link-type shared
Porta da Extremidade	Switch(config-if)# spanning-tree edge-port enable Switch(config-if)# spanning-tree edge-port disable
Configuração de Porta MSTP	Switch(config-if)# spanning-tree mst MSTMAP cost <1-200000000> the value of mst instance port cost Switch(config-if)# spanning-tree mst MSTMAP port-priority <0-240> the value of mst instance port priority in multiple of 16
Informações Gerais	
Informações Ativas	Switch# show spanning-tree active Spanning-Tree: Enabled Protocol: MSTP

	Root Address: 0012.77ee.eeee Priority: 32768 Root Path Cost: 0 Root Port: N/A Root Times: max-age 20, hello-time 2, forward-delay 15 Bridge Address: 0012.77ee.eeee Priority: 32768 Bridge Times: max-age 20, hello-time 2, forward-delay 15 BPDU transmission-limit: 3 Port Role State Cost Prio.Nbr Type Aggregated ------ ---------- ---------- -------- ---------- ------------ ------------ fa1 Designated Forwarding 200000 128.1 P2P(RSTP) N/A fa2 Designated Forwarding 200000 128.2 P2P(RSTP) N/A
Resumo RSTP	Switch# show spanning-tree summary Switch is in rapid-stp mode. BPDU skewing detection disabled for the bridge. Backbonefast disabled for bridge. Summary of connected spanning tree ports: Port-State Summary Blocking Listening Learning Forwarding Disabled -------- --------- -------- ---------- -------- 0 0 0 2 8 Port Link-Type Summary AutoDetected PointToPoint SharedLink EdgePort ------------ ------------ ---------- -------- 9 0 1 9
Informações da Porta	Switch# show spanning-tree port detail fa7 (Interface_ID) Rapid Spanning-Tree feature Enabled Port 128.6 as Disabled Role is in Disabled State Port Path Cost 200000, Port Identifier 128.6 RSTP Port Admin Link-Type is Auto, Oper Link-Type is Point-to-Point RSTP Port Admin Edge-Port is Enabled, Oper Edge-Port is Edge Designated root has priority 32768, address 0012.7700.0112 Designated bridge has priority 32768, address 0012.7760.1aec Designated Port ID is 128.6, Root Path Cost is 600000 Timers: message-age 0 sec, forward-delay 0 sec Link Aggregation Group: N/A, Type: N/A, Aggregated with: N/A BPDU: sent 43759, received 4854 TCN: sent 0, received 0 Forwarding-State Transmit count 12 Message-Age Expired count
Informações MSTP	
Configuração MSTP	Switch# show spanning-tree mst configuration Current MST configuration (MSTP is Running) Name [xxxx] Revision 65535 Instance Vlans Mapped -------- --------------------------------------- 0 1,4-4094 1 2 2 3 Config HMAC-MD5 Digest: 0xB41829F9030A054FB74EF7A8587FF58D --
Mostra todas as informaçoes MSTP	Switch# show spanning-tree mst ###### MST00 vlans mapped: 1,4-4094 Bridge address 0012.77ee.eeee priority 32768 (sysid 0) Root this switch for CST and IST Configured max-age 2, hello-time 15, forward-delay 20, max-hops 20 Port Role State Cost Prio.Nbr Type ------ ---------- ---------- -------- ---------- ---------- fa1 Designated Forwarding 200000 128.1 P2P Internal(MSTP) fa2 Designated Forwarding 200000 128.2 P2P Internal(MSTP) ###### MST01 vlans mapped: 2 Bridge address 0012.77ee.eeee priority 32768 (sysid 1)

	Root this switch for MST01 Port Role State Cost Prio.Nbr Type ------ ---------- ---------- -------- ---------- ------------------ fa1 Designated Forwarding 200000 128.1 P2P Internal(MSTP) fa2 Designated Forwarding 200000 128.2 P2P Internal(MSTP)
MSTP Informações de Raíz	Switch# show spanning-tree mst root MST Root Root Root Root Max Hello Fwd Instance Address Priority Cost Port age dly -------- --------------- -------- ------------ ------ ----- ----- ----- MST00 0012.77ee.eeee 32768 0 N/A 20 2 15 MST01 0012.77ee.eeee 32768 0 N/A 20 2 15 MST02 0012.77ee.eeee 32768 0 N/A 20 2 15
MSTP Informações de Instância	Switch# show spanning-tree mst 1 ###### MST01 vlans mapped: 2 Bridge address 0012.77ee.eeee priority 32768 (sysid 1) Root this switch for MST01 Port Role State Cost Prio.Nbr Type ------ ---------- ---------- -------- ---------- ------------------ fa1 Designated Forwarding 200000 128.1 P2P Internal(MSTP) fa2 Designated Forwarding 200000 128.2 P2P Internal(MSTP)
MSTP Informações de Porta	Switch# show spanning-tree mst interface fa1 Interface fastethernet1 of MST00 is Designated Forwarding Edge Port: Edge (Edge) BPDU Filter: Disabled Link Type: Auto (Point-to-point) BPDU Guard: Disabled Boundary: Internal(MSTP) BPDUs: sent 6352, received 0 Instance Role State Cost Prio.Nbr Vlans Mapped -------- ---------- ---------- -------- ---------- ---------- 0 Designated Forwarding 200000 128.1 1,4-4094 1 Designated Forwarding 200000 128.1 2 2 Designated Forwarding 200000 128.1 3
Multiplos Super Ring	
Criar ou Configurar um Super Ring	Switch(config)# multiple-super-ring 1 Ring 1 created Switch(config-super-ring-plus)# Note: 1 is the target Ring ID which is going to be created or configured.
Versão do Super Ring	Switch(config-super-ring-plus)# version default set default to rapid super ring rapid-super-ring rapid super ring super-ring super ring Switch(config-super-ring-plus)# version rapid-super-ring
Prioridade	Switch(config-super-ring-plus)# priority <0-255> valid range is 0 to 255 default set default Switch(config-super-ring-plus)# priority 100
Porta do Anel	Switch(config-super-ring-plus)# port IFLIST Interface list, ex: fa1,fa3-5,fa8-10 cost path cost Switch(config)# super-ring port fa1,fa2
Custo de Porta do Anel	Switch(config-super-ring-plus)# port cost <0-255> valid range is 0 or 255 default set default (128)valid range is 0 or 255 Switch(config-super-ring-plus)# port cost 100 <0-255> valid range is 0 or 255 default set default (128)valid range is 0 or 255 Switch(config-super-ring-plus)# port cost 100 200 Set path cost success.
Rapid Dual Homing	Switch(config-super-ring-plus)# rapid dual-homing enable Switch(config-super-ring-plus)# rapid dual-homing disable Switch(config-super-ring-plus)# rapid dual-homing port

	IFLIST Interface name, ex: fastethernet1 or fa8 auto-detect up link auto detection IFNAME Interface name, ex: fastethernet1 or fa4 Switch(config-super-ring-plus)# rapid dual-homing port fa3,fa5-6 set Dual Homing port success. Switch(config-multiple-super-ring)# rapid-dual-homing port fa1 priority default Set Rapid Dual Homing port priority success. Note: auto-detect is recommended for Rapid Ddual Homing.
Informações de Anel (Ring)	
Informações de Anel	Switch# show multiple-super-ring [Ring ID] [Ring1] Ring1 Current Status: Disabled Role: Disabled Ring Status: Abnormal Ring Manager: 0000.0000.0000 Blocking Port: N/A Giga Copper: N/A Configuration: Version: Rapid Super Ring Priority: 128 Ring Port: fa1, fa2 Path Cost: 100, 200 Rapid Dual Homing: Disabled Statistics: Watchdog sent 0, received 0, missed 0 Link Up sent 0, received 0 Link Down sent 0, received 0 Role Transition count 0 Ring State Transition count 1 Ring ID is optional. If the ring ID is typed, this command will only display the information of the target Ring.

Tabela 4-11. Linhas de Comando para Redundância de Rede

VLAN

Uma LAN virtual (VLAN) é um agrupamento lógico de nós com a finalidade de limitar um domínio de transmissão para os membros específicos de um grupo sem agrupamento fisico dos membros. Isso significa que uma VLAN permite isolar o tráfego de rede, de modo que apenas os membros da VLAN podem receber o tráfego dos mesmos membros da VLAN. Basicamente, a criação de uma VLAN de um switch é o equivalente lógico de voltar a ligar fisicamente um grupo de dispositivos de rede para um outro switch de camada 2, sem realmente desligar esses dispositivos de seus links originais.

O JN4508F-M suporta a funcionalidade de Porta VLAN com a finalidade de limitar o domínio de transmissão para membros específicos de um grupo, agrupando-os fisicamente. Ele determina a composição de um frame de dados, examinando a configuração da porta que recebeu a transmissão, ou lendo uma parte do cabeçalho deste frame. A VLAN é identificada através do cabeçalho, por um campo de quatro bytes. Esta identificação indica a qual VLAN pertence o frame. Se não houver nenhum rótulo no cabeçalho, o switch verifica a configuração VLAN da porto que recebeu o frame. Se o switch foi configurado para suporte a VLAN, ele próprio atribui a identificação VLAN na porta para o novo frame.

A configuração de grupos de VLAN permitem adicionar ou removes uma VLAN, *Add* / *Remove*, bem como Inserir ou remover, *Ingress* / *Egress*, parâmetros as portas da tabela da VLAN.

Gerenciamento VLAN Baseado nas Portas

O gerenciamento das VLANs baseados nas portas permite configurar os parâmetros da porta da VLAN para a porta específica. Esses parâmetros incluem PVID, Frames Aceitos e Filtro de Ingresso.

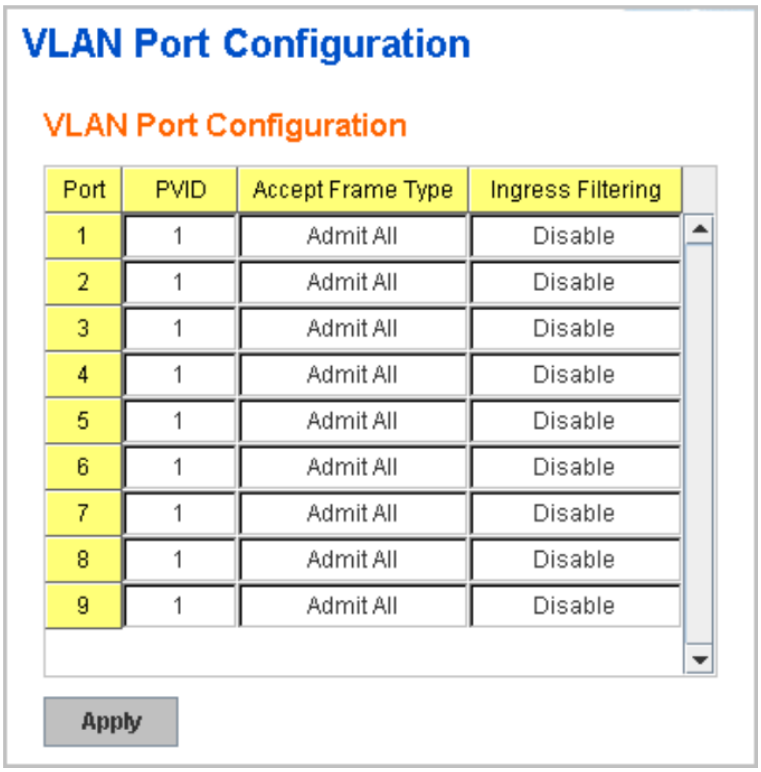

Figura 4-44. Configurações de Portas VLAN

PVID: Sigla referente à identificação da porta (Port VLAN ID). Neste campo, insira a ID VLAN da porta. A PVID permite aos switches identificar qual porta pertence a qual VLAN. Para facilitar o processo, é recomendável que PVID as IDs VLAN sejam equivalentes. Os valores possíveis de PVIDs variam de 1 a 4094, porém 0 e 4095 são reservados (não podem ser utilizados). 1 é o valor padrão; os valores entre 2 e 4094 são disponibilizados nesta coluna (válidos). Digite a PVID a ser configurada neste campo.

Accept Frame Type: Esta coluna define o tipo de frame aceito na porta. Existem dois modos selecionáveis, *Admit All* e *Tag Only*. *Admit All* significa que a porta pode aceitar ambos os pacotes marcados e não marcados. *Tag Only* significa que a porta só pode aceitar pacotes marcados.

Ingress Filtering: Este parâmetro ajuda a plataforma VLAN para filtrar o tráfego indesejado em uma porta. Quando Ingress Filtering está habilitado, a porta verifica se os frames de entrada pertencem à VLAN aceitando ou não. Em seguida, a porta determina se os frames podem ser processados ou não. Por exemplo, se um Frame com identificação de Engenharia VLAN é recebido, e Ingress Filtering está ativo, o detector vai determinar se a porta está na lista de Egresso Engenheiro da VLAN. Se for, o frame pode ser processado. Se não for, o frame será descartado.

Configuração VLAN

Neste capítulo, será mostrado o gerenciamento de VLAN, criação de uma VLAN estática e ingresso de regras as portas membro de uma VLAN.

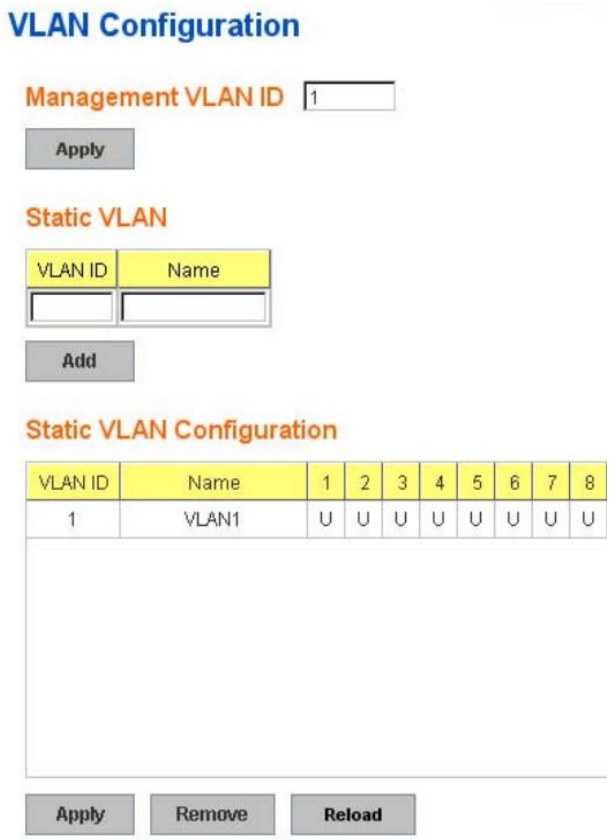

Figura 4-45. Configuração de VLAN

Management VLAN ID: O switch suporta gerenciamento de VLAN. O gerenciamento da VLAN ID é feito pela UCP da interface, assim, somente membros da VLAN gerenciada podem enviar mensagens de ping e acessar através do switch. O valor padrão para VLAN ID é 1.

Static VLAN: Pode se atribuir uma VLAN ID a uma nova VLAN através deste comando.

VLAN ID: É usado pelo switch para identificar diferentes VLANs. Valores validos de VLAN ID estão entre 1 e 4094, 1 é a VLAN padrão.

VLAN Name: É uma referência para o administrador da rede para identificar diferentes VLANs. 12 caracteres estão disponíveis para isto. Para um nome criado sem caracteres o sistema automaticamente atribui o nome VLAN. A regra é VLAN (VLAN ID).

Passo a Passo para criar uma nova VLAN: Digite VLAN ID e NAME, pressione *Add* para criar uma nova VLAN. Será possível ver uma nova VLAN na lista de VLAN estáticas.

Após criar a VLAN, o status da VLAN permanecerá em não usada (*Unused*) até que portas sejam adicionadas a esta VLAN.

Nota:

Antes de alterar o VLAN ID de gerenciamento por Web e Telnet, lembre-se de que a porta atribuída pelo administrador deve ser uma porta membro da VLAN de gestão; caso contrário, o administrador não poderá acessar o switch através da rede.

Atualmente o JN4508F-M suporta até 256 grupos de VLAN.

Configuração de VLAN Estática

Aqui é possível ver a lista de VLANs criadas e determinar a regra de egresso da porta como Untagged ou Tagged.

A Figura 4-46 abaixo mostra a tabela de configuração da VLAN estática. Nela, foi criada a VLAN 3 (test) e as regras de egresso das portas ainda não estão configuradas.

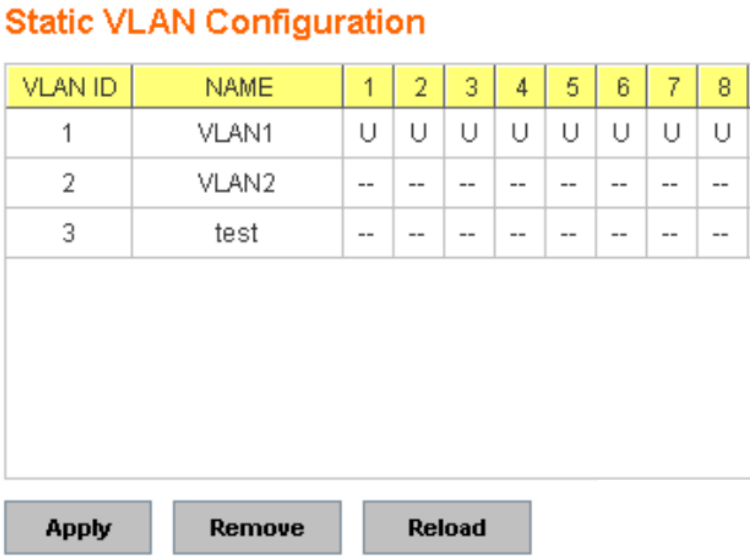

Figura 4-46. Configuração de VLAN Estática

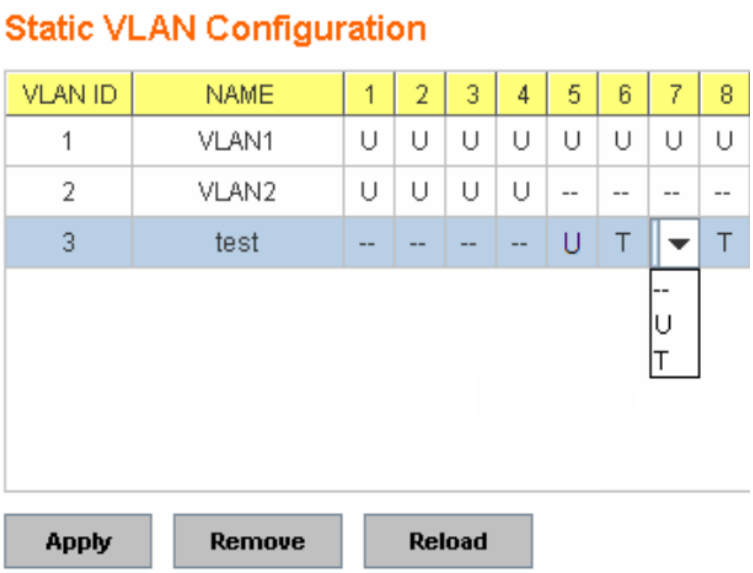

Figura 4-47. Configuração de Egresso de VLAN

-- Não disponível

U Untagged: Indica que egresso / frames de saída não são da VLAN marcada.

T Tagged: Indica que egresso / frames de saída são da VLAN marcada.

Passos para configurar regras de egresso: Selecione VLAN ID. Entrada da VLAN selecionada, muda para azul claro. Atribuir regra *Egress* das portas para L ou T. Clique em *Apply* para aplicar a definição. Se você deseja remover uma VLAN, selecione a entrada VLAN. Em seguida, pressione o botão *Remove*.

Configuração GVRP

GVRP permite ao usuário configurar VLANs automaticamente ao invés da configuração manual em todas as portas de cada switch na rede.

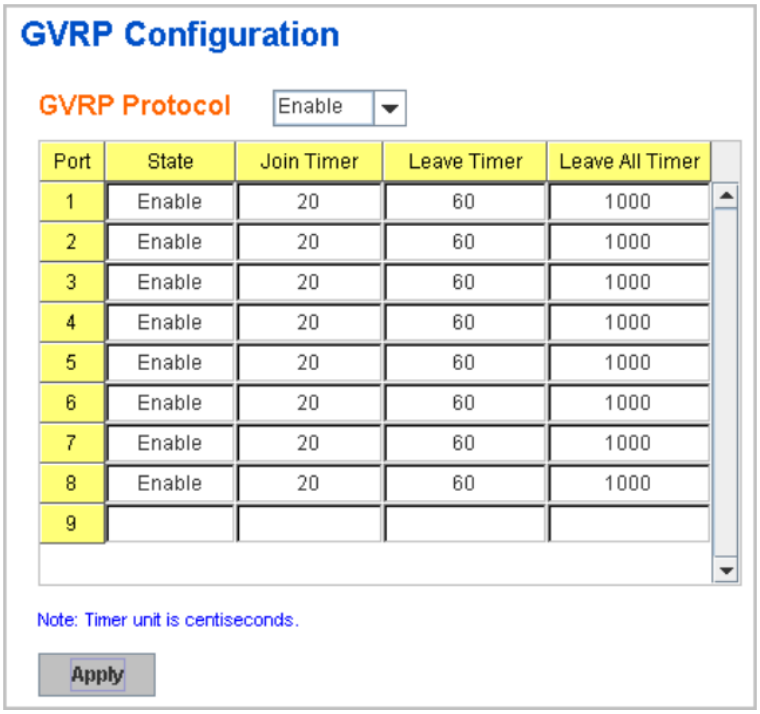

Figura 4-48. Configuração GVRP

GVRP Protocol: Permite o usuário habilitar / desabilitar globalmente o GVRP.

State: Depois de habilitar globalmente o GVRP, é possível habilitar / desabilitar o GVRP por porta.

Join Timer: Controla o intervalo de envio de GVRP, ingresso BPDU. Uma instância deste timer é necessária por porta, por participante GARP.

Leave Timer: Controla o tempo para liberar a reserve GVRP após receber um BPDU de GVRP. Uma instância de temporizador é necessária para cada estado da maquina no estado LV.

Leave All Timer: Controla o período para iniciar a coleta de lixo de VLAN registrado. O temporizador é necessária em uma base por Porta Participante GARP.

Tabela VLAN

Esta tabela mostra as configurações atuais da tabela VLAN, incluindo VLAN ID, nome, status, e regras dos portos.

Figura 4-49. Tabela VLAN

VLAN ID: ID da VLAN.

Name: Nome da VLAN.

Status: Mostra uma VLAN estática configurada manualmente. *Unused* significa que a VLAN foi criada por UI / CLI e não tem portas membro ativos. Esta VLAN não está disponível ainda. *Dynamic* significa que a VLAN é conhecida pelo GVRP.

Após criar a VLAN, o status permanecerá em *Unused* até que portas sejam adicionadas a VLAN.

Comandos CLI da Porta VLAN

Linhas de comando para configuração da porta VLAN, configuração VLAN e exibição da tabela VLAN.

Descrição	Comando CLI
VLAN Port Configuration	
Porta PVID VLAN	Switch(config-if)# switchport trunk native vlan 2 Set port default vlan id to 2 success
Aceitação de Frame pela Porta	Switch(config)# inter fa1 Switch(config-if)# acceptable frame type all any kind of frame type is accepted! Switch(config-if)# acceptable frame type vlantaggedonly only vlan-tag frame is accepted!
Filtro de Ingreso (para porta de alta velocidade Ethernet 1)	Switch(config)# interface fa1 Switch(config-if)# ingress filtering enable ingress filtering enable Switch(config-if)# ingress filtering disable ingress filtering disable
Regra de Egresso Desmarcada (para VLAN 2)	Switch(config-if)# switchport access vlan 2 switchport access vlan - success
Regra de Egresso Marcada (para VLAN 2)	Switch(config-if)# switchport trunk allowed vlan add 2
Mostra– Regras de Ingresso da Porta (PVID, Ingress Filtering, Acceptable Frame Type)	Switch# show interface fa1 Interface fastethernet1 Administrative Status: Enable Operating Status: Not Connected Duplex: Auto Speed: Auto Flow Control:off Default Port VLAN ID: 2 Ingress Filtering: Disabled

	Acceptable Frame Type: All Port Security: Disabled Auto Negotiation: Enable Loopback Mode: None STP Status: disabled Default CoS Value for untagged packets is 0. Mdix mode is Auto. Medium mode is Copper
Mostra– Regras de Egresso da Porta (Egress rule, IP address, status)	Switch# show running-config …… ! interface gigabitethernet1 switchport access vlan 1 switchport access vlan 3 switchport trunk native vlan 2 ……. interface vlan1 ip address 192.168.10.8/24 no shutdown
Configuração VLAN	
Criar VLAN (2)	Switch(config)# vlan 2 vlan 2 success Switch(config)# interface vlan 2 Switch(config-if)# Note: In CLI configuration, you should create a VLAN interface first. Then you can start to add/remove ports. Default status of the created VLAN is unused until you add member ports to it.
Remover VLAN	Switch(config)# no vlan 2 no vlan success Note: You can only remove the VLAN when the VLAN is in unused mode.
Nome da VLAN	Switch(config)# vlan 2 vlan 2 has exists Switch(config-vlan)# name v2 Switch(config-vlan)# no name Note: Use no name to change the name to default name, VLAN VID.
Descrição da VLAN	Switch(config)# interface vlan 2 Switch(config-if)# Switch(config-if)# description this is the VLAN 2 Switch(config-if)# no description ->Delete the description.
Endereço IP da VLAN	Switch(config)# interface vlan 2 Switch(config-if)# Switch(config-if)# ip address 192.168.10.18/24 Switch(config-if)# no ip address 192.168.10.8/24 ->Delete the IP address
Criar múltiplas VLANs (VLAN 5-10)	Switch(config)# interface vlan 5-10
Desligar VLAN	Switch(config)# interface vlan 2 Switch(config-if)# shutdown Switch(config-if)# no shutdown ->Turn on the VLAN
Mostrar – Tabela de VLAN	Switch# sh vlan VLAN Name Status Trunk Ports Access Ports 1 VLAN1 Static -------- fa1-7 2 VLAN2 Unused -------- -------- 3 test Static fa4-5 fa3,fa4,fa7-8
Mostrar – Informação de interface VLAN	Switch# show interface vlan1 interface vlan1 is up, line protocol detection is disabled index 14 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,MULTICAST> HWaddr: 00:12:77:ff:01:b0 inet 192.168.10.100/24 broadcast 192.168.10.255 input packets 639, bytes 38248, dropped 0, multicast packets 0 input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0

	output packets 959, bytes 829280, dropped 0 output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0 collisions 0
Configuração GVRP	
Habilita / Desabilita o GVRP	Switch(config)# gvrp mode disable: Disable GVRP feature globally on the switch enable: Enable GVRP feature globally on the switch Switch(config)# gvrp mode enable Gvrp is enabled on the switch!
Configura o Timer GVRP/ timer Join timer /Leave timer/ Leave All timer	Switch(config)# inter fa1 Switch(config-if)# garp timer <10-10000> Switch(config-if)# garp timer 20 60 1000 Note: The unit of these timer is centisecond
Gerenciamento da VLAN	
Gerencia a VLAN	Switch(config)# int vlan 1 (Go to management VLAN) Switch(config-if)# no shutdown
Mostrar	Switch# show running-config …. ! interface vlan1 ip address 192.168.10.17/24 ip igmp no shutdown ! ….

Tabela 4-12. Tabela de Comandos CLI da Porta VLAN

VLAN Privada

A VLAN privada ajuda a resolver a carência de uma VLAN ID primária, isolamento de portas de cliente e as questões de segurança de rede. A VLAN privada fornece VLAN primária e secundária dentro de um único switch.

Primary VLAN: A porta de uplink geralmente é a VLAN primária. A VLAN primária contém portas promíscuas que podem se comunicar com VLANs secundárias inferiores.

Secondary VLAN: As portas de cliente são geralmente definidas dentro da VLAN secundária. A VLAN secundária inclui VLAN Isoladas e Comunidades de VLAN. As portas de cliente podem ser VLANs isoladas ou podem ser agrupadas na mesma VLAN comunitária. As portas dentro da mesma comunidade de VLAN podem se comunicar uns com os outros. No entanto, as portas de VLAN isolada não podem. A figura mostra a típica rede VLAN privada. O SCADA / Servidor Público ou estação de trabalho NMS geralmente está localizada na VLAN primária. Os clientes PCs ou anéis estão localizados dentro da Secundária.

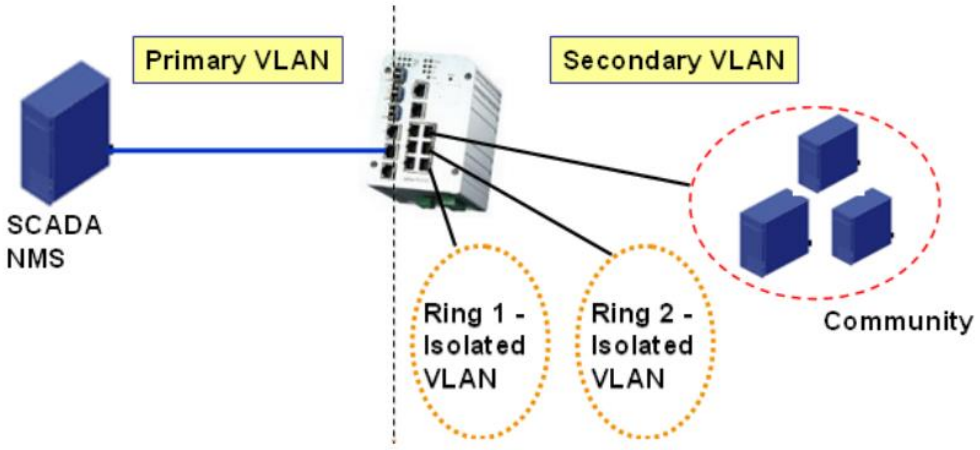

Figura 4-50. Exemplo de VLAN Privada

VLAN privada (PVLAN) permite a configuração de grupo habilitando a configurar PVLAN, PVLAN Porta e as informações PVLAN.

Configuração PVLAN

A configuração PVLAN permite que você atribua o tipo VLAN privada. Depois de criada uma VLAN na páginaVLAN Configuration, o VLAN ID disponível será exibido aqui. Escolha os tipos de VLAN privada para cada VLAN que desejar configurar.

None: A VLAN não está incluída na VLAN privada.

Primary: O VLAN é a VLAN Primária. As portas membro podem se comunicar com portas secundárias.

Isolated: A VLAN é a VLAN isolada. As portas membro da VLAN estão isoladas.

Community: A VLAN é a VLAN comunitária. As portas membro da VLAN podem se comunicar umas com as outras.

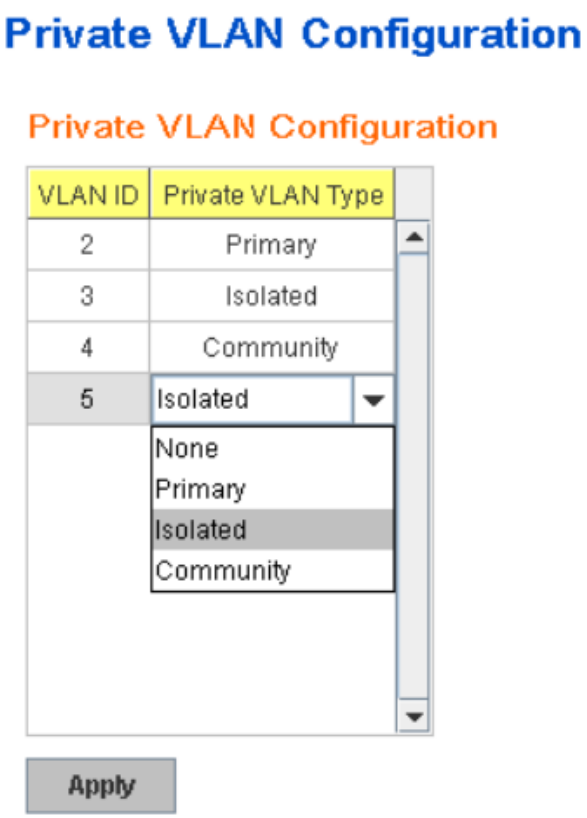

Figura 4-51. Configuração de VLAN Privada

Configuração de Porta PVLAN (PVLAN Port Configuration)

A aba PVLAN Port Configuration permite configurar *Port Configuration* e *Private VLAN Association*.

VLAN Associação Privada (Private VLAN Association)

Secondary VLAN: Após o *Isolated* e *Community* ser atribuído a VLAN na página de configuração da VLAN privada, as VLANs pertencerão à VLAN secundária e mostradas aqui.

Primary VLAN: Após o principal tipo de VLAN ser atribuído na página de configuração VLAN privada, a VLAN secundária pode associar à VLAN ID Primária. Selecione a VLAN Primária aqui.

Nota:

Antes de configurar o tipo de porta PVLAN, a VLAN Associação Privada deve ter sido configurada antes.

Configuração da Porta

Tipo de Porta PVLAN:

Normal: A porta normal é Nenhuma (*None*) porta da PVLAN, continua a ser a sua configuração de VLAN original.

Host: As portas do tipo host podem ser mapeadas para a VLAN secundária.

Promiscuous: A porta promíscua pode ser associada à VLAN primária.

VLAN ID: Após atribuído o tipo de porta, a interface do usuário web exibe a VLAN ID disponível a porta para associa-la.

Por exemplo:

1. **Create VLAN:** VLAN 2-5 são criadas na página de configuração VLAN.
2. **Private VLAN Type:** 2-5 VLAN tem seu tipo configuradas, Private VLAN. A VLAN 2 pertence à VLAN Primária. VLAN 3-5 pertencem a a VLAN secundária (isolada ou comunitária).
3. **Private VLAN Association:** VLAN Associado 5/3 à VLAN 2 em VLAN privada Associação primeiro.
4. **Private VLAN Port Configuration:** VLAN 2 - *Primary* -> A porta membro da VLAN 2 é uma porta promíscua. VLAN 3 - *Isolated* -> A porta do host pode ser mapeada para VLAN 3. VLAN 4 - *Community* -> A porta do host pode ser mapeada para VLAN 3. VLAN 5 - *Community* -> A porta do host pode ser mapeada para VLAN 3.
5. **Result:** VLAN 2 -> VLAN 3, 4, 5; portas membro podem se comunicar com os portas da VLAN secundária. VLAN 3 -> VLAN 2, portas membro são isoladas, mas podem se comunicar com portas membro da VLAN 2. VLAN 4 -> VLAN 2, portas membro da comunidade podem se comunicar umas com as outras e se comunicar com a porta membro da VLAN 2. VLAN 5 -> VLAN 2, portas membro dentro da comunidade podem se comunicar umas com as outras e se comunicar com a porta membro da VLAN 2.

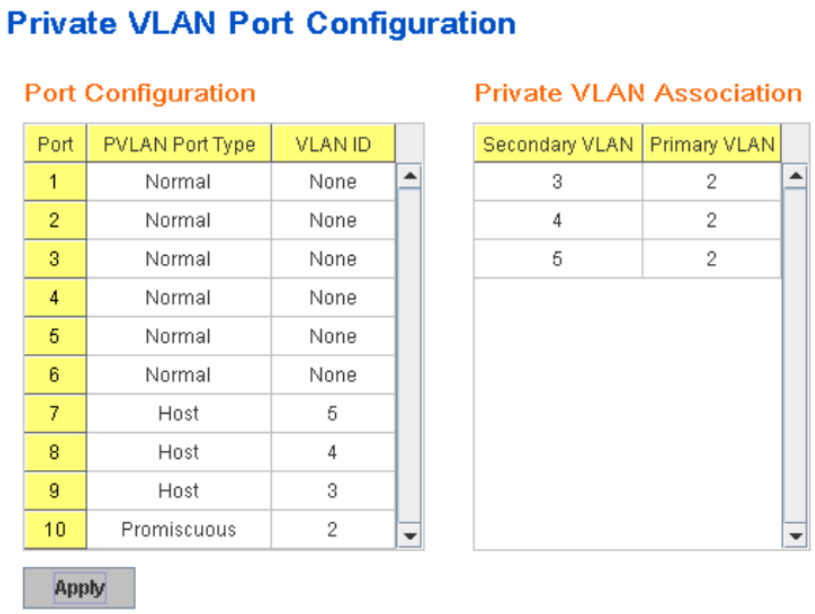

Figura 4-52. Configuração de Portas em VLAN Privada

Information de VLAN Privada (Private VLAN)

A Figura 4-53 mostra informações de uma VLAN privada.

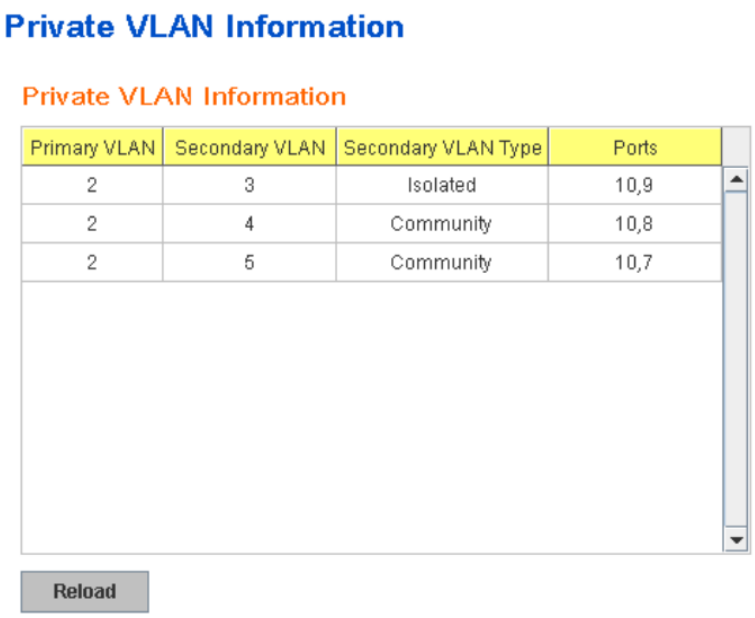

Figura 4-53. Private VLAN Information

Comando CLI – PVLAN

As linhas de comando de configuração de uma VLAN privada são mostradas na tabela abaixo.

Descrição	Comando CLI
Configuração VLAN Privada	
Criar VLAN	Switch(config)# vlan 2 vlan 2 success Switch(config-vlan)# end End current mode and change to enable mode exit Exit current mode and down to previous mode list Print command list name Assign a name to vlan no no private-vlan Configure a private VLAN
Private VLAN Type	Go to the VLAN you want configure first. Switch(config)# vlan (VID)
Choose the Types	Switch(config-vlan)# private-vlan community Configure the VLAN as an community private VLAN isolated Configure the VLAN as an isolated private VLAN primary Configure the VLAN as a primary private VLAN
Primary Type	Switch(config-vlan)# private-vlan primary <cr>
Isolated Type	Switch(config-vlan)# private-vlan isolated <cr>
Community Type	Switch(config-vlan)# private-vlan community <cr>
Configuração de Porta Privada VLAN	
Go to the port configuraiton	Switch(config)# interface (port_number, ex: gi9) Switch(config-if)# switchport private-vlan host-association Set the private VLAN host association mapping map primary VLAN to secondary VLAN
Private VLAN Port Type	Switch(config-if)# switchport mode private-vlan Set private-vlan mode Switch(config-if)# switchport mode private-vlan host Set the mode to private-vlan host

Promiscuous Port Type	promiscuous Set the mode to private-vlan promiscuous Switch(config-if)# switchport mode private-vlan promiscuous <cr>
Host Port Type	Switch(config-if)# switchport mode private-vlan host <cr>
Private VLAN Port Configuration	Switch(config)# interface gi9
PVLAN Port Type	Switch(config-if)# switchport mode private-vlan host
Host Association primary to secondary (The command is only available for host port.)	Switch(config-if)# switchport private-vlan host-association <2-4094> Primary range VLAN ID of the private VLAN port association Switch(config-if)# switchport private-vlan host-association 2 <2-4094> Secondary range VLAN ID of the private VLAN port association Switch(config-if)# switchport private-vlan host-association 2 3
Mapping primary to secondary VLANs (This command is only available for promiscuous port)	Switch(config)# interface gi10 Switch(config-if)# switchport mode private-vlan promiscuous Switch(config-if)# switchport private-vlan mapping 2 add 3 Switch(config-if)# switchport private-vlan mapping 2 add 4 Switch(config-if)# switchport private-vlan mapping 2 add 5
Informações de VLAN Privada	
Informações de VLAN Privada	Switch# show vlan private-vlan FLAGS: I -> Isolated P -> Promiscuous C -> Community Primary Secondary Type Ports --- --- --- --- 2 3 Isolated gi10(P),gi9(I) 2 4 Community gi10(P),gi8(C) 2 5 Community gi10(P),fa7(C),gi9(I) 10 --- --- ---
Tipo de PVLAN	Switch# show vlan private-vlan type Vlan Type Ports --- --- --- 2 primary gi10 3 isolated gi9 4 community gi8 5 community fa7,gi9 10 primary ---
Lista de Hosts	Switch# show vlan private-vlan port-list Ports Mode Vlan --- --- --- 1 Normal --- 2 Normal --- 3 Normal --- 4 Normal --- 5 Normal --- 6 Normal --- 7 Host 5 8 Host 4 9 Host 3 10 Promiscuous 2
Informações de Configurações Atuais Private VLAN Type	Switch# show run Building configuration... Current configuration: hostname Switch vlan learning independent vlan 1

	! vlan 2 private-vlan primary ! vlan 3 private-vlan isolated ! vlan 4 private-vlan community ! vlan 5 private-vlan community
Private VLAN Port Information	interface fastethernet7 switchport access vlan add 2,5 switchport trunk native vlan 5 switchport mode private-vlan host switchport private-vlan host-association 2 5 ! interface gigabitethernet8 switchport access vlan add 2,4 switchport trunk native vlan 4 switchport mode private-vlan host switchport private-vlan host-association 2 4 ! interface gigabitethernet9 switchport access vlan add 2,5 switchport trunk native vlan 5 switchport mode private-vlan host switchport private-vlan host-association 2 3 ! interface gigabitethernet10 switchport access vlan add 2,5 switchport trunk native vlan 2 switchport mode private-vlan promiscuous switchport private-vlan mapping 2 add 3-5 !

Tabela 4-13. Comandos CLI para PVLAN

Priorização de Tráfego

Qualidade de serviço (QoS) fornece um mecanismo de priorização de tráfego que permite ao usuário entregar o melhor serviço para determinados fluxos. QoS também pode ajudar a aliviar os problemas de congestionamento e garantir que o tráfego de alta prioridade seja entregue primeiro. Esta seção detalha as configurações de priorização de tráfego para cada porta no que diz respeito à definição das prioridades.

O JN4508F-M QoS suporta 4 filas físicas, de enfileiramento justo ponderado (WRR) e Esquema de Prioridade Estrita, em conformidade com 802.1p COS tag e informações IPv4 TOS/DiffServ para priorizar o tráfego da sua rede industrial.

Configuração de QoS (QoS Setting)

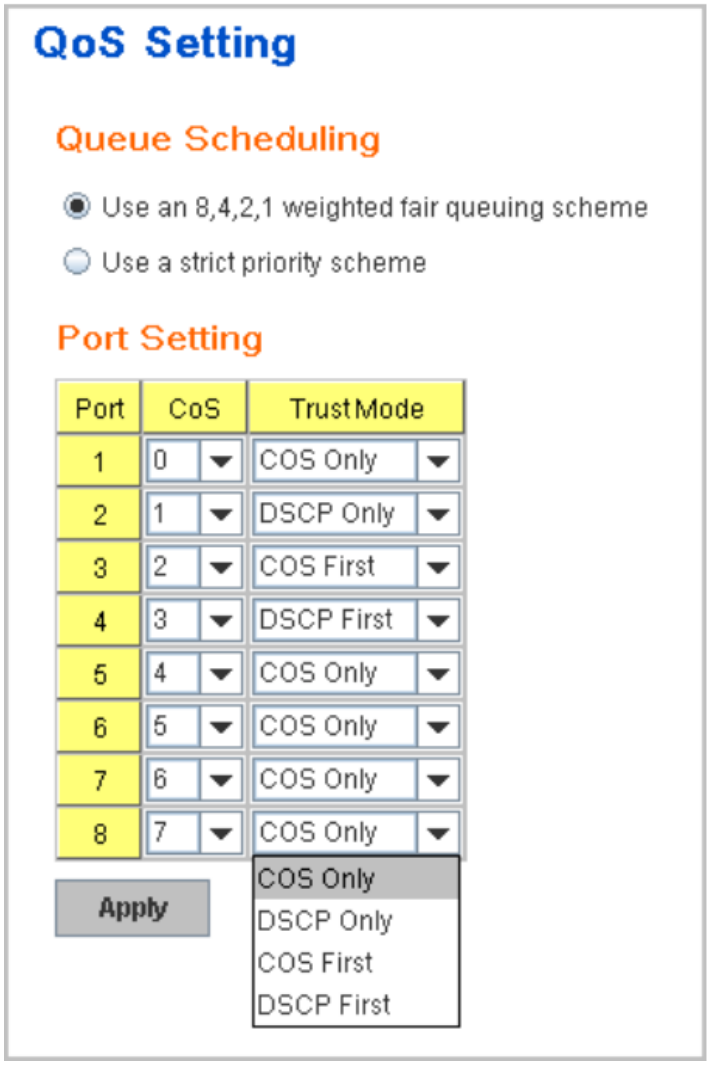

Figura 4-54. QoS Setting

Fila de Agendamento (Queue Schedulling)

Use um esquema de Enfileiramento Justo Ponderado 8,4,2,1. O qual também é conhecido como WRR (Weight Round Robin). JN4508F-M a taxa de 8:4:2:1 para processar os pacotes em uma fila da mais alta prioridade para a mais baixa. Por exemplo, o sistema processará simultaneamente 8 pacotes com a prioridade mais alta na fila, 4 pacotes com prioridade média, 2 pacotes com prioridade baixa e 1 pacote com a prioridade mais baixa.

Use um esquema de prioridade estrita. Pacotes com a prioridade mais alta na fila sempre serão processados primeiro.

Configuração da Porta (Port Setting)

A coluna *Priority* indica o valor de prioridade padrão da porta para frames não marcados ou de prioridade marcada. Quando JN4508F-M recebe os frames, ele irá atribuir o valor da prioridade. O usuário pode habilitar 0,1,2, 3, 4, 5,6 ou 7 para a porta.

Trust Mode: Indica os tipos de mapeamento de fila selecionáveis.

CoS Only: A prioridade da porta seguirá somente o mapeamento da fila CoS atribuído.

DSCP Only: A prioridade da porta seguirá somente o mapeamento da fila DSCP atribuído.

CoS First: A prioridade da porta seguirá, inicialmente, o mapeamento da fila CoS e, posteriormente, a regra de mapeamento da fila DSCP.

DSCP First: A prioridade da porta seguirá, inicialmente, o mapeamento da fila DSCP e depois a regra de mapeamento da fila CoS.

O tipo de prioridade padrão é CoS Only. O sistema irá fornecer uma tabela com a fila CoS padrão, a qual o usuário pode referenciar no próximo comando.

Depois de configurar, clique no botão *Apply* para habilitar as configurações.

Mapeamento da Fila CoS (CoS Queue Mapping)

Nesta área, o usuário pode definir valores CoS para a tabela de mapeamento da fila física. Uma vez que o switch JN4508F-M suporta 4 filas físicas (Menor, Baixa, Média e Alta), os usuários devem atribuir valores CoS ao nível da fila física.

Com o JN4508F-M, os usuários podem facilmente atribuir a tabela de mapeamento ou seguir as sugestões do padrão 802.1p. a normatização 802.p para seus valores padrão. Os valores CoS 1 e 2 são mapeados para a fila física 0 (menor fila). Os valores CoS 0 e 3 são mapeados para a fila física 1 (fila física baixa/normal), os valores CoS 4 e 5 são mapeados para fila física 2 (fila física média), e os valores CoS 6 e 7 são mapeados para a fila física 3 (fila física mais alta).

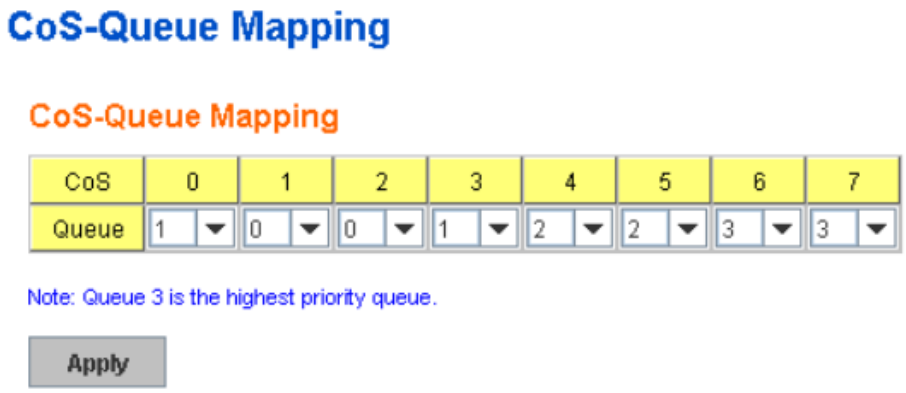

Figura 4-55. CoS Queue Mapping

Depois de configurar, clique no botão *Apply* para habilitar as configurações.

Mapeamento de Fila DSCP (DSCP Queue Mapping)

Nesta área, o usuário pode alterar os valores DSCP para uma tabela de mapeamento de fila física. Uma vez que o switch JN4508F-M suporta 4 filas físicas (Menor, Baixa, Média e Alta), os usuários devem atribuir valores DSCP ao nível da fila física. Com o JN4508F-M, os usuários podem facilmente alterar a tabela de mapeamento para seguir os switches de camada superior 3 ou a configuração de DSCP dos roteadores.

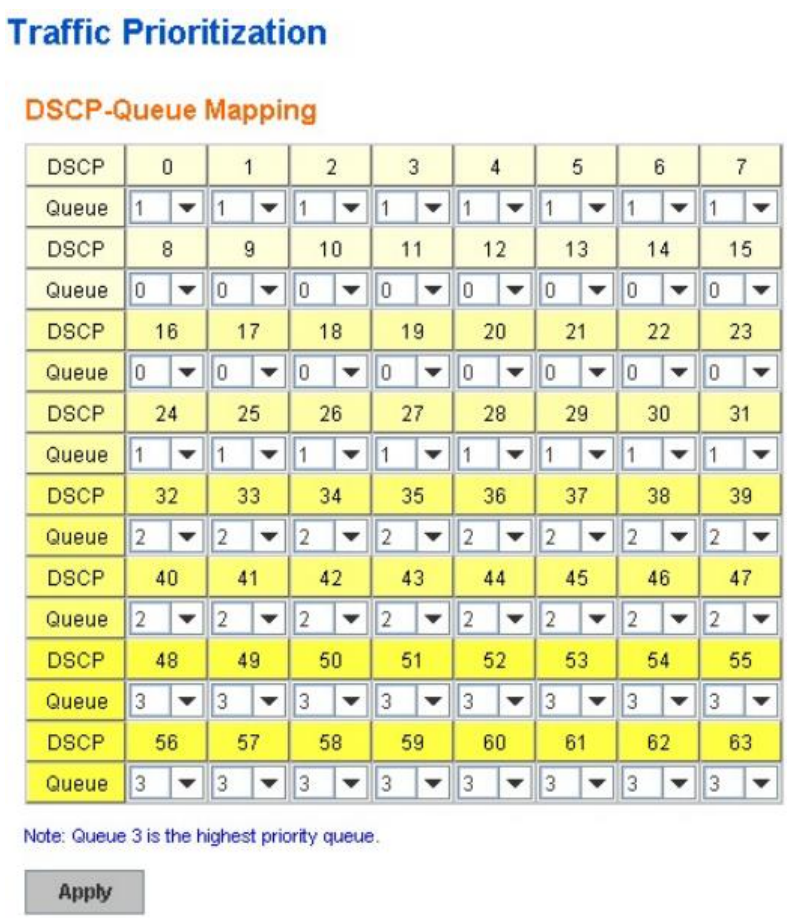

Figura 4-56. DSCP Queue Mapping

Depois de configurar, clique no botão *Apply* para habilitar as configurações.

Comandos CLI para Priorização de Tráfego

Funcionalidade	Linha de Comando
Ajuste QoS	
Agendamento de Fila – Prioridade Estrita	Switch(config)# qos queue-sched sp Strict Priority wrr Weighted Round Robin (Use an 8,4,2,1 weight) Switch(config)# qos queue-sched sp <cr>
Agendamento de Fila WRR	Switch (config)# qos queue-sched wrr
Ajuste de Porta – prioridade (Prioridade de Porta Padrão)	Switch(config) # interface fa1 Switch(config-if)# qos priority DEFAULT-PRIORITY atribui uma prioridade (3 ou maior) Switch(config-if)# qos cos 3 O valor padrão de prioridade de porta é 3. **Nota:** Ao alterar a configuração da porta, você deve selecionar Inicialmente, a porta específica. Ex: fa1 significa porta fast Ethernet 1.
Ajuste de Porta – Modo Confiar - Somente CoS	Switch(config)# interface fa1 Switch(config-if)# qos trust cos A port trust é definida como Somente CoS.
Ajuste de Porta – Confiar	Switch(config) # interface fa1
Modo - Primeiro CoS	Switch(config-if)# qos trust cos-first A port trust é definida como Primeiro CoS.
Ajuste de Porta – Modo Confiar - Somente DSCP	Switch(config)# interface fa1 Switch(config-if)# qos trust dscp

	A port trust é definida como Somente DSCP.
Ajuste de Porta – Modo Confiar - Primeiro DSCP	Switch(config)# interface fa1 Switch(config-if)# qos trust dscp-first A port trust é definida como Primeiro DSCP.
Ajuste de Porta – Modo Confiar - Baseado em Porta	Switch(config)# interface fa1 Switch(config-if)# qos trust port-based A port trust é definida como baseada em porta.
Display – Agendamento de Fila	Switch# show qos queue-sched Esquema de agendamento de fila QoS: Weighted Round Robin (usar peso 8,4,2,1)
Display – Ajuste de Porta Modo Confiar	Switch# show qos trust QoS Port Trust Mode: Port Trust Mode --------- --------- 1 DSCP first 2 COS only 3 COS only 4 COS only 5 COS only 6 COS only 7 COS only 8 COS only 9 COS only 10 COS only
Display – Ajuste de Porta –CoS (Prioridade Padrão de Porta)	Switch# show qos port-cos Port Default Cos: Port CoS 1 0 2 0 3 0 4 0 5 0 6 0
Mapeamento da Fila CoS	
Formato	Switch(config)# qos cos-map PRIORITY atribui uma prioridade (7 ou maior) Switch(config)# qos cos-map 1 QUEUE atribui uma fila (0-3) Nota: Format: qos cos-map priority_value queue_value
Map. CoS 0 p/ Queue 1	Switch(config)# qos cos-map 0 1 O CoS para mapeamento de fila é ajustado.
Map. CoS 1 p/ Queue 0	Switch(config)# qos cos-map 1 0 O CoS para mapeamento de fila é ajustado.
Map. CoS 2 p/ Queue 0	Switch(config)# qos cos-map 2 0 O CoS para mapeamento de fila é ajustado.
Map. CoS 3 p/ Queue 1	Switch(config)# qos cos-map 3 1 O CoS para mapeamento de fila é ajustado.
Map. CoS 4 p/ Queue 2	Switch(config)# qos cos-map 4 2 O CoS para mapeamento de fila é ajustado.
Map. CoS 5 p/ Queue 2	Switch(config)# qos cos-map 5 2 O CoS para mapeamento de fila é ajustado.
Map. CoS 6 p/ Queue 3	Switch(config)# qos cos-map 6 3 O CoS para mapeamento de fila é ajustado.
Map. CoS 7 p/ Queue 3	Switch(config)# qos cos-map 7 3 O CoS para mapeamento de fila é ajustado.
Display – CoS - Mapeamento de Fila	Switch# sh qos cos-map CoS to Queue Mapping:

	CoS Queue ---- + ------ 0 1 1 0 2 0 3 1 4 2 5 2 6 3 7 3
Mapeamento de Fila DSCP	
Formato	Switch(config)# qos dscp-map PRIORITY atribui uma prioridade (63 ou mais alto) Switch(config)# qos dscp-map 0 QUEUE atribui uma fila (0-3) Format: qos dscp-map priority_value queue_value
Map. DSCP 0 p/ Queue 1	Switch (config)# qos dscp-map 0 1 O TOS/DSCP para mapeamento de fila é ajustado.
Display – DSCO - Mapeamento de Fila	Switch# show qos dscp-map DSCP to Queue Mapping: (dscp = d1 d2) d2| 0 1 2 3 4 5 6 7 8 9 d1 | ----+---------- 0 | 1 1 1 1 1 1 1 1 0 0 1 | 0 0 0 0 0 0 0 0 0 0 2 | 0 0 0 0 1 1 1 1 1 1 3 | 1 1 2 2 2 2 2 2 2 2 4 | 2 2 2 2 2 2 2 2 3 3 5 | 3 3 3 3 3 3 3 3 3 3 6 | 3 3 3 3

Tabela 4-14. Linhas de Comando para Configuração de Priorização de Tráfego

Filtragem de Multicast (Multicast Filtering)

Para efeitos de filtragem de multicast, o JN4508F-M adota a tecnologia de filtragem IGMP Snooping. O IGMP (Internet Group Management Protocol) é um Protocolo de Internet que permite que um dispositivo de internet relate para roteadores adjacentes seus membros de grupo de multicast. O multicast permite que um computador na internet envie dados para uma infinidade de outros computadores que se identificaram como interessados em receber os dados originários deste computador.

O multicast é útil para aplicações tais como: atualização de catálogos de endereços de usuários de computadores móveis no campo, envio de newsletters para uma lista de distribuição e transmissão de streaming de mídia para o público sintonizado com o evento em função da associação ao grupo de multicast.

Com efeito, o IGMP Snooping gerencia o tráfego multicast, fazendo uso de switches, roteadores e hosts que oferecem suporte a IGMP. A habilitação do IGMP Snooping permite que as portas detectem consultas IGMP, pacotes de relatório e gerenciem o tráfego multicast através do switch. O IGMP tem três tipos fundamentais de mensagens, como mostrado na Tabela 4-15.

Mensagem	Descrição
Query	Uma mensagem enviada do consultante (um roteador IGMP ou um switch), que solicita uma resposta de cada host que pertence ao grupo de difusão seletiva
Report	Uma mensagem enviada pelo host para o consultante para indicar que o primeiro quer ser ou é um membro de um grupo determinado, indicado na mensagem de relatório
Leave Group	Uma mensagem enviada por um host para o consultante para indicar que o primeiro não é mais membro de um grupo multicast específico

Tabela 4-15. Mensagens IGMP

O usuário pode habilitar funções IGMP Snooping e Query IGMP neste contexto. Esta seção contém informações relativas à função IGMP Snooping, incluindo portas de membros de multicast diferentes e endereços IP multicast que variam de 224.0.0.0 a 239.255.255.255.

IGMP Snooping

Esta página serve para ativar o recurso IGMP, atribuir IGMP Snooping para VLAN específica, e visualizar a tabela IGMP Snooping dinâmica ou reconhecimento manual de key-in. O Switch JetNet suporta IGMP Snooping V1/V2/V3 automaticamente e lista IGMP V1/V2.

IGMP Snooping, você pode selecione Ativar (*Enable*) ou Desativar (*Disable*). Após ativar o IGMP Snooping, será possível então ativar o IGMP para a VLAN específica. É possível ativar o IGMP Snooping para algumas VLANs de modo que algumas das VLANs irão dar suporte ao IGMP Snooping e outras não.

Para atribuir o IGMP Snooping para uma VLAN, marque a caixa de VLAN ID ou selecione *Select All*, da caixa de seleção para todas as VLANs. Em seguida, pressione *Enable*. Da mesma forma, também pode se desativar o IGMP Snooping para determinadas VLANs.

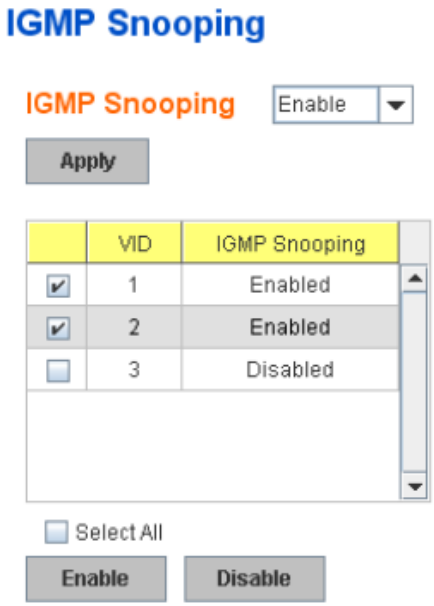

Figura 4-57. IGMP Snooping

IGMP Snooping Table: Na tabela, pode se ver o endereço IP multicast do grupo e as portas membro do grupo multicast. O JN4508F-M suporta 256 grupos de multicast. Clique no botão *Reload* para atualizar a tabela.

Figura 4-58. IGMP Snooping Table

IGMP Query

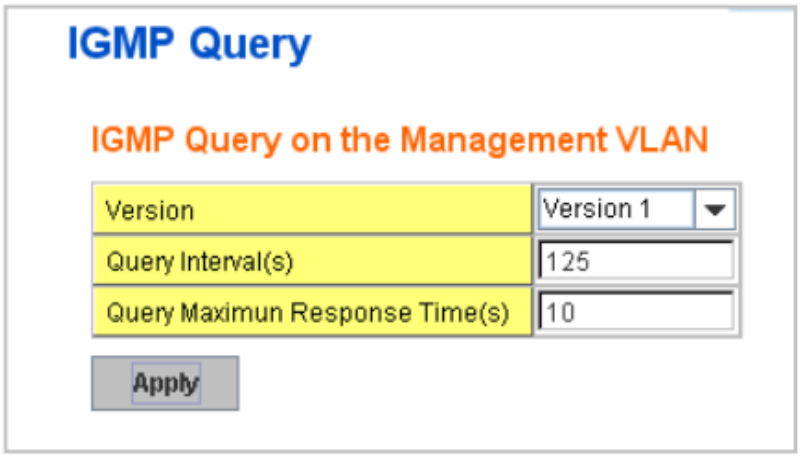

Figura 4-59. IGMP Query - Tela de Configuração

Este capítulo permite ao usuário configurar o recurso IGMP Query. Desde que o switch JN4508F-M pode ser configurado somente pelas portas membro da VLAN de gestão, desta forma IGMP só pode ser ativa na VLAN de gerenciamento. Se deseja-se executar o recurso IGMP Snooping em várias VLANs, deve se perceber que se cada VLAN tenha a sua própria IGMP Querier primeiro.

O IGMP requisitante envia periodicamente pacotes de consulta a todas as estações finais sobre as LANs ou VLANs que estão conectados a ele. Para redes com mais de um IGMP querier, o switch com o menor endereço IP se torna o IGMP querier.

Na seleção IGMP Query, pode se selecionar V1, V2 ou Desativar. V1 significa IGMP V1 para *General Query*. A requisição será encaminhada a todos os grupos multicast na VLAN. V2 significa IGMP V2 *Specific Query*. A requisição será encaminhada para grupos multicast específicos. *Disable* permite que se desabilite a consulta IGMP.

Query Interval(s): Período de intervalo de envio de requisição.

Query Maximum Response Time: O Intervalo de requisições detectou que os membros do grupo não estão mais diretamente ligado em uma LAN.

Após finalizar as configurações, clique em *Apply*.

Forçar Filtro (Force Filtering)

Figura 4-60. Force Filtering

A função para Forçar o filtro permite ao switch filtrar dados de fluxo multicast desconhecidos. Se *Force Filtering* está habilitado, todos os dados de fluxo multicast desconhecidos serão descartados.

Comandos CLI da Filtragem Multicast

Funcionalidade	Linha de Comando
IGMP Snooping	
IGMP Snooping Global	Switch(config)# ip igmp snooping IGMP Snooping é habilitado globalmente. Por favor, especifique em quais
IGMP Snooping - VLAN	Switch(config)# no ip igmp snooping vlan VLANs é permitido o IGMP Snooping all todas as vlans existem Switch(config)# ip igmp snooping vlan 1-2 IGMP Snooping desabilitado globalmente.
Desabilita o IGMP Snooping - Global	Switch(config)# no ip igmp snooping IGMP snooping is disabled globally ok.
Desabilita oIGMP Snooping - VLAN	Switch(config)# no ip igmp snooping vlan 3 IGMP snooping is disabled on VLAN 3.
Display – IGMP Configuração de Snooping	Switch# sh ip igmp interface vlan1 enabled: Yes version: IGMPv1 query-interval; 125s query-max-response-time: 10s Switch# sh ip igmp snooping IGMP snooping is globally enabled Vlan1 is IGMP snooping enabled Vlan2 is IGMP snooping enabled Vlan3 is IGMP snooping disabled
Display – IGMP Table	Switch# sh ip igmp snooping multicast all VLAN IP Address Type Ports ---------- ---------- ---------- ---------- 1 239.192.8.0 IGMP fa6 1 239.255.255.250 IGMP fa6
IGMP Query	
IGMP Query V1	Switch(config)# int vlan 1 (Vá para gerenciamento de VLAN) Switch(config-if)# ip igmp v1
IGMP Query V2	Switch(config)# int vlan 1 (Vá para gerenciamento de VLAN) Switch(config-if)# ip igmp
Versão do IGMP Query	Switch(config-if)# ip igmp version 1 Switch(config-if)# ip igmp version 2
Desabilitar	Switch(config)# int vlan 1 Switch(config-if)# no ip igmp
Display	Switch# sh ip igmp interface vlan1

	enabled: Yes version: IGMPv2 query-interval: 125s query-max-response-time: 10s Switch# show running-config …. ! interface vlan1 ip address 192.168.10.17/24 ip igmp no shutdown ! …….
Forçar Filtro	
Habilita Forçar Filtro Desabilita Forçar Filtro	Switch(config)# mac-address-table multicast filtering Filtering unknown multicast addresses ok! Switch(config)# no mac-address-table multicast filtering

Tabela 4-16. Linhas de Comando da Configuração de Filtragem de Multicast

SNMP

Simple Network Management Protocol (SNMP) é um protocolo usado para troca de informações de gerenciamento entre dispositivos de rede. SNMP é um componente da suíte do protocolo TCP/IP. JN4508F-M suporta SNMP v1, v2c e v3.

Uma rede com gerenciamento SNMP consiste em dois componentes principais: agentes e um gerente. Um agente é um módulo de software de gestão presente em um switch gerenciado. Um agente traduz as informações de gerenciamento local do dispositivo gerenciado em um formato compatível com SNMP. O gerente é o console através da rede.

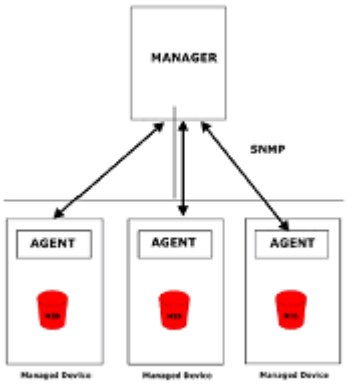

Figura 4-61. Exemplo de Arquitetura SNMP

Configuração do SNMP

Esta opção permite ao usuário configurar a comunidade SNMP V1/V2c. A string da comunidade pode ser vista como uma senha visto que o SNMP V1/V2c não solicita que seja digitada uma senha antes de acessar o agente SNMP.

A comunidade inclui 2 privilégios: Somente leitura e Leitura/Escrita.

Com privilégios de somente leitura, o usuário somente poderá ler os valores nas tabelas MIB. A string da comunidade padrão é definida como Public (público).

Com privilégios de leitura e escrita, o usuário poderá ler e escrever valores das tabelas MIB. A string da comunidade padrão é definida como Private (privado).

O JN4508F-M permite aos usuários a atribuição de quatro strings de comunidade. Para tanto, selecione, em cada string da comunidade desejada, o seu privilégio específico. Em seguida, pressione o botão *Apply* (aplicar).

Nota:

Quando o usuário instala o dispositivo em sua rede pela primeira vez, é altamente recomendável que seja alterada a string da comunidade. Isto se deve ao fato de que a maioria das aplicações de gestão SNMP usam as opções público e privado como nome de comunidade padrão, podendo constituir-se em uma falha de segurança na rede.

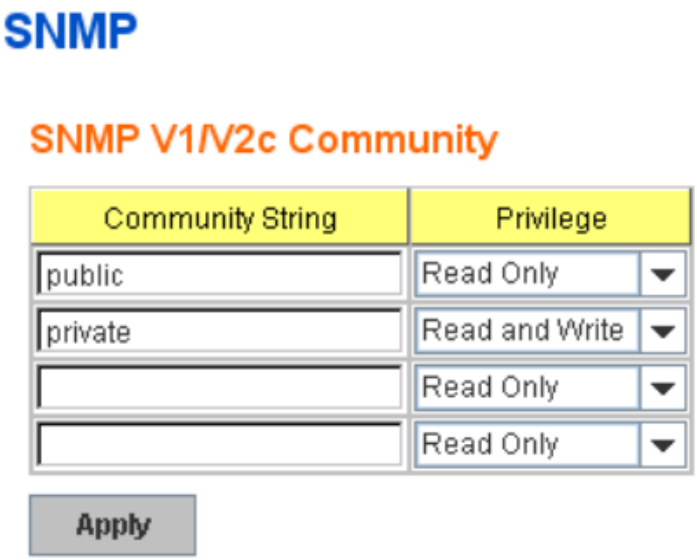

Figura 4-62. Configurações SNMP V1/V2c

Perfil SNMP v3 (SNMP V3 Profile)

O SNMP v3 pode fornecer mais funções de segurança quando o usuário executa o gerenciamento remoto através do protocolo SNMP. Ele oferece informações SNMP para o administrador com a autenticação de usuário; todos os dados entre o JN4508F-M e o administrador são criptografados para garantir uma comunicação segura.

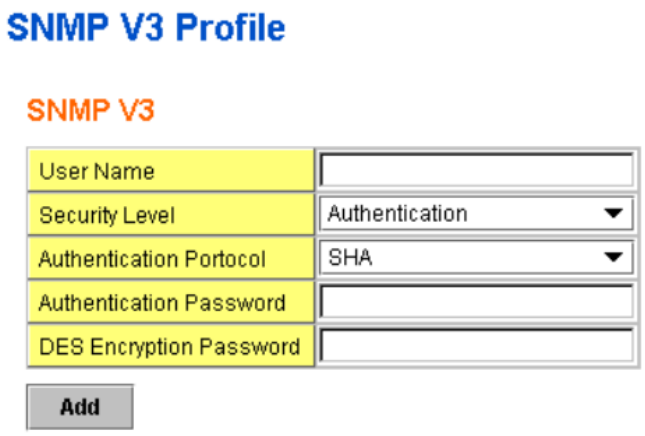

Figura 4-63. Configurações SNMP V3

Security Level: Esta opção permite ao usuário selecionar entre as opções de segurança: *None* (nenhum), *User Authentication* (autenticação de usuário), e *Authentication with privacy* (autenticação com privacidade).

Authentication Protocol: Este campo permite o usuário selecionar qualquer MD5 (*Message-Digest algorithm 5*) ou SHA (*Secure Hash Algorithm*). MD5 é uma função de hash de criptografia amplamente utilizado com um valor de hash de 128 bits. Funções de hash SHA (Secure Hash Algorithm) referem-se a cinco algoritmos aprovados pelo «Federal Information Processing Standard» para uma representação digital computacional condensada. O JN4508F-M fornece 2 protocolos de autenticação de usuário em MD5 e SHA. O usuário precisará configurar os parâmetros SNMP v3 para a sua ferramenta SNMP com o mesmo método de autenticação.

Authentication Password: Neste campo insere se a senha de autenticação de usuário SNMP v3.

DES Encryption Password: Neste campo insere se a senha para o usuário SNMP v3 com criptografia DES.

SNMP Trap

Trap SNMP é um recurso de notificação definido pelo protocolo SNMP. Todas as aplicações gerenciadas SNMP entendem este tipo de informação. O usuário não precisará instalar novos aplicativos para ler as informações de notificação.

Esta página permite ao usuário ativar o SNMP Trap, configurar o IP do servidor SNMP Trap, o nome da Comunidade e a versão do trap (V1 ou V2). Após a configuração, pode-se verificar as alterações realizadas nos SNMP traps normatizados predefinidos, bem como os traps pré-definidos. Os traps pré-definidos podem ser encontrados na MIB privada.

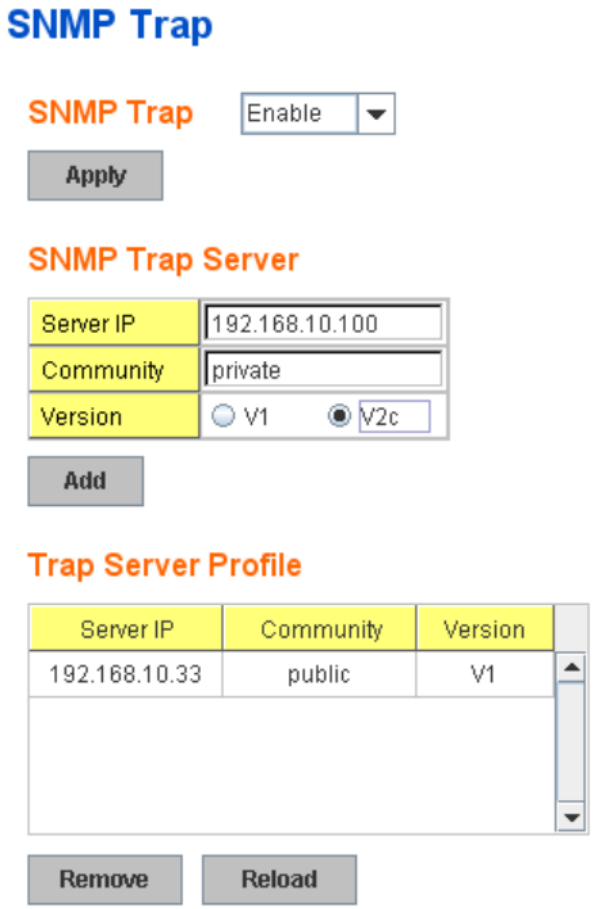

Figura 4-64. Configurações SNMP Trap

Comandos CLI para SNMP

Funcionalidade	Linha de Comando
Comunidade SNMP	
Comunidade Somente Leitura	Switch(config)# snmp-server community public ro Acrescentada string de comunidade
Comunidade Leitura Escrita	Switch(config)# snmp-server community private rw Acrescentada string de comunidade
SNMP Trap	
Habilitar Trap	Switch(config)# snmp-server enable trap Conjunto SNMP trap habilitado.
SNMP Trap Server IP sem nome de comunidade específico	Switch(config)# snmp-server host 192.168.10.33 Host SNMP trap acrescentado.
SNMP Trap Server IP com a versão 1 e comunidade	Switch(config)# snmp-server host 192.168.10.33 version 1 Private Host SNMP trap acrescentado. **Nota:** privado é o nome da comunidade, versão 1 é a versão do SNMP
SNMP Trap Server IP com a versão 2 e comunidade	Switch(config)# snmp-server host 192.168.10.33 version 2 Private Host SNMP trap acrescentado.
Desabilitar SNMP Trap	Switch(config)# no snmp-server enable trap SNMP trap desabilitado.
Display	Switch# sh snmp-server trap SNMP trap: Enabled SNMP trap community: public Switch# show running-config ..... snmp-server community public ro snmp-server community private rw snmp-server enable trap snmp-server host 192.168.10.33 version 2 admin snmp-server host 192.168.10.33 version 1 admin ……..

Tabela 4-17. Linhas de Comando para Configuração do SNMP

Segurança (Security)

JN4508f fornece vários recursos de segurança para proteger a conexão. As características incluem Segurança de Portas (*Port Security*) e Segurança de IP (*IP Security*).

Segurança de Portas (Port Security)

O recurso de Segurança de Portas permite parar o reconhecimento de endereços MAC da porta específica. Depois de parar o reconhecimento de MAC, apenas os endereços MAC listados na Lista Pontos de Seguros (*Port Security List*) podem acessar o switch e transmitir / receber o tráfego. Esta é uma maneira simples para proteger o seu ambiente de rede e para não ser acessado por hackers.

Esta página permite que se ative a porta de segurança e configure as entradas de porta de segurança.

Port Security State: Muda o estado de porta segura da porta antes de habilitar.

Add Port Security Entry: Selecione a porta, e digite VID e endereço MAC. Formato do endereço MAC é xxxx.xxxx.xxxx. Ex: 0012.7701.0101. O tamanho máximo de uma porta é 10. Assim, o sistema pode aceitar 100 endereços MAC de portas seguras no total.

Port Security List: Esta tabela mostra as entradas de segurança do porto habilitadas. Você pode clicar em Remover para excluir a entrada.

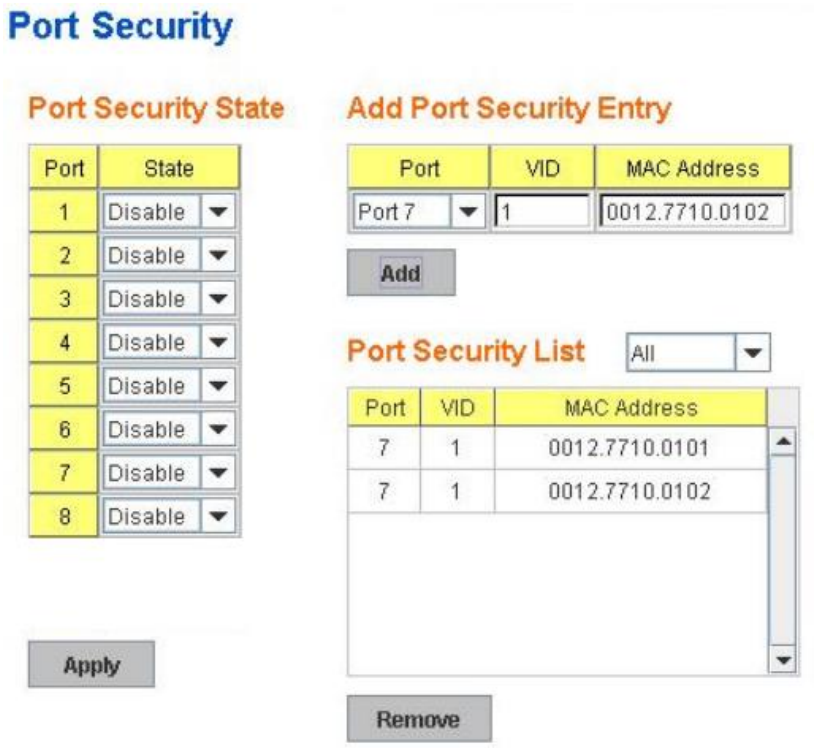

Figura 4-65. Configurações Port Security

Uma vez terminado de configurar as definições, clique em *Apply / Add* para aplicar a configuração.

Segurança IP (IP Security)

Na seção Segurança IP, é possível configurar endereços IP específicos para executar a autorização para acesso de gestão no JN4508F-M via web browser ou Telnet.

IP Security: Selecione *Enable* e *Apply* para habilitar a função de segurança IP.

Add Security IP: Pode-se atribuir qualquer PC como uma estação de trabalho do administrador, adicionando o endereço IP do PC no campo de segurança IP. Somente esses endereços IP serão capazes de acessar e gerenciar o JN4508F-M. O número máximo de segurança IP é 10.

Security IP List: Esta tabela mostra cada endereço IP seguro acrescentado. Pode-se selecionar *Remove* para excluir e *Reload* para recarregar a tabela.

Figura 4-66. Configurações IP Security

Ao finalizar a configuração clique no botão *Apply* para aplicar os ajustes realizados.

IEEE 802.1x

Configuração 802.1X

IEEE 802.1X é o protocolo que a execução da autenticação executa para obter acesso a LANs IEEE 802. É o controle de acesso à rede porta-base. Com a função, JN4508F-M pode controlar qual conexão está disponível ou não.

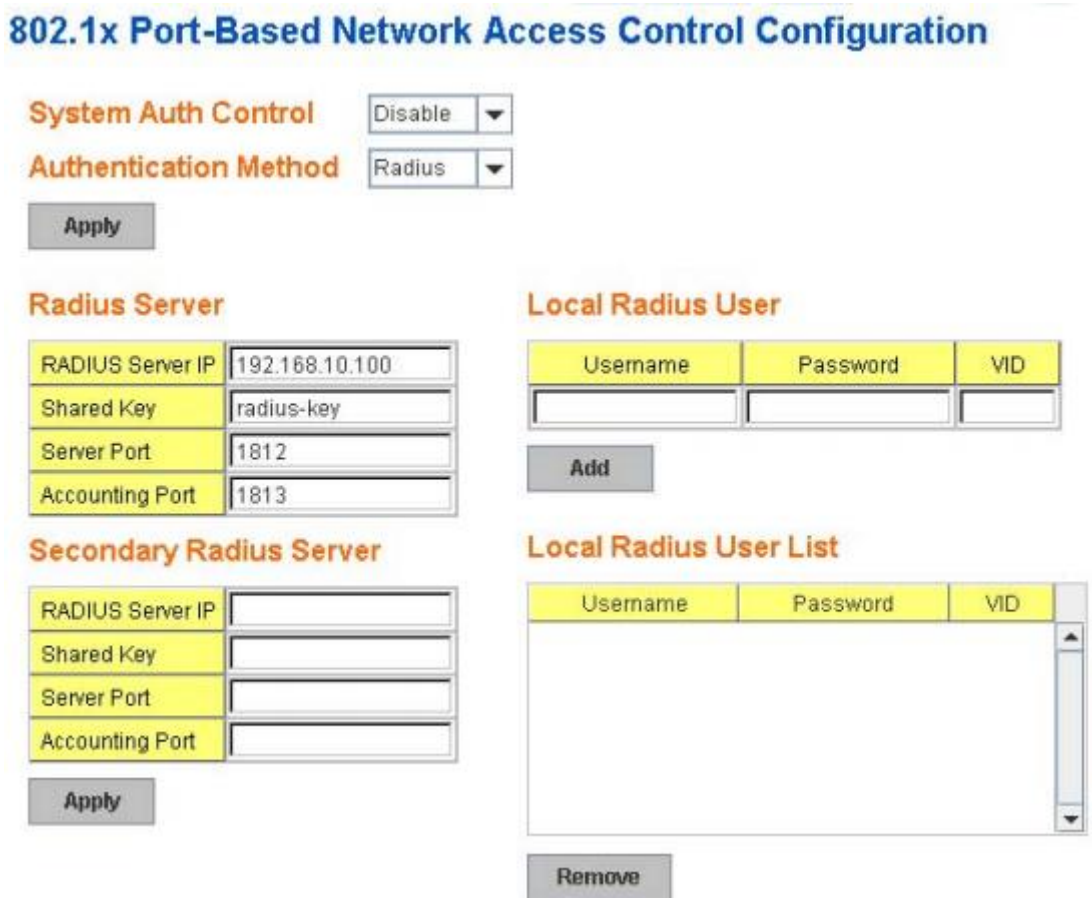

Figura 4-67. Port Based Network Access Control Configuration

System AuthControl: Para ativar ou desativar a autenticação 802.1x.

Authentication Method: Radius é um servidor de autenticação que fornecem uma chave para autenticação, com este método, o usuário deve se conectar ao switch servidor. Se o usuário selecionar Local para o método de autenticação, o switch usa a base de dados de usuário local que pode ser criada nesta página para autenticação.

Radius Server IP: O endereço IP do servidor Radius.

Shared Key: a senha para comunicar entre o switch e RadiusServer.

Server Port: Porta UDP do servidor Radius.

Accounting Port: Porta para pacotes que contêm as informações de conta de Login ou Logout.

Secondary Radius Server IP: Servidor Secundário Radius que pode ser definido no caso do servidor RADIUS primário não estar disponível.

802.1X Local User: Permite o usuário adicionar conta / senha (*Account / Password*) para a autenticação local.

802.1X Local User List: Esta é uma lista que mostra as informações da conta, o usuário também pode remover a conta selecionada aqui.

802.1x Port Configuration

Após a configuração do servidor Radius ou lista de usuário local, o usuário também precisa configurar o modo de autenticação, o comportamento de autenticação, aplicada a VLAN para cada porta e permitir a comunicação. As informações a seguir explicam a configuração da porta.

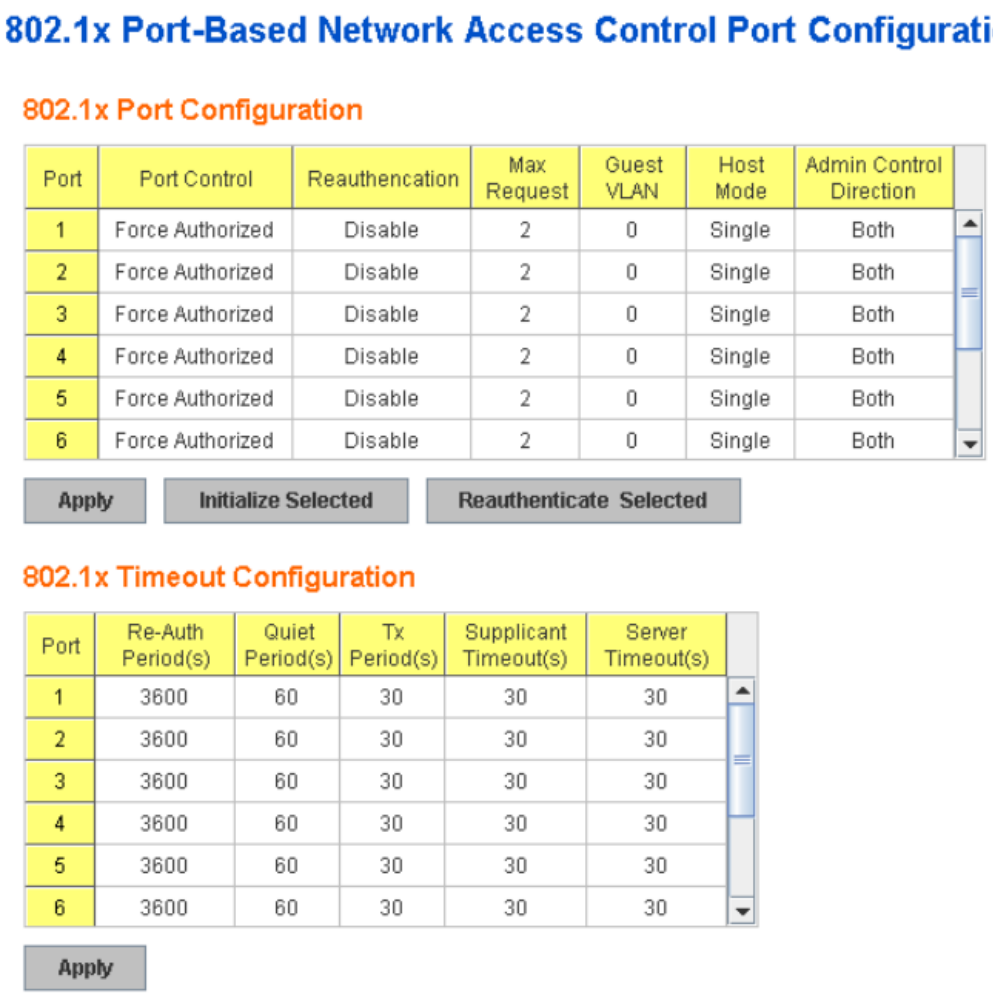

Figura 4-68. Port Based Network Access Control Port Configuration

Port Control: *Force Authorized* significa que esta porta está autorizada; os dados são livres para entrarem e saírem. *Force Unauthorized*, significa o contrário, a porta está bloqueada. Se os usuários querem controlar esta porta com o Radius Server, selecione *Auto* para o controle da porta.

Reauthentication: Se ativar este campo, o interruptor irá pedir ao cliente para autenticar novamente. O intervalo de tempo padrão é 3600 segundos.

Max Request: os tempos máximos que o switch permite as requisições de cliente.

Guest VLAN: valores entre 0-4094 estão disponíveis para este campo. Se este campo está definido como 0, isso significa que a porta está bloqueada se a autenticação falhar. Caso contrário, a porta estará definida para Guest VLAN.

Host Mode: se houver mais de um dispositivo conectado a essa porta, habilite o Host Mode para apenas o primeiro PC que autenticar com sucesso poder acessar esta porta. Se esta porta está definida como Multi Modes os dispositivos podem acessar essa porta, uma vez que qualquer um dos dispositivos passar pela autenticação.

Control Direction: Dispositivos de determinados podem colocar dados para fora ou apenas enviar e receber.

Re-Auth Period: controla o intervalo de tempo de Reautenticação (*Reahthentication*), faixa disponível é de 1 ~ 65535.

Quiet Period: Quando a autenticação falhou, Switch irá esperar por um período e tentar se comunicar com o servidor Radius novamente.

Tx Period: o intervalo de tempo de requisição de autenticação.

Suplicant Timeout: o tempo limite para a autenticação do cliente.

Server Timeout: O tempo limite para resposta do servidor para autenticação.

Uma vez que terminada a configuração e definições, clique em *Apply* para aplicar a configuração.

Clique em *Initialize Selected* para definir o estado da porta selecionada para inicializar o status.

Clique *Reauthenticate Selected* para enviar a solicitação EAP de requisição para uma nova autenticação.

Clique *Default Selected* para resetar os parâmetros configuráveis do 802.1x da porta selecionada para os valores padrão.

Status da porta 802.1X

O usuário pode observar o estado da porta de status para controle de porta (*Port Control*), Autorizar Status (*Authorize Status*), Requisição Autorizada (*Authorized*) e Controle de Direção (*Oper Control Direction*) de cada porta.

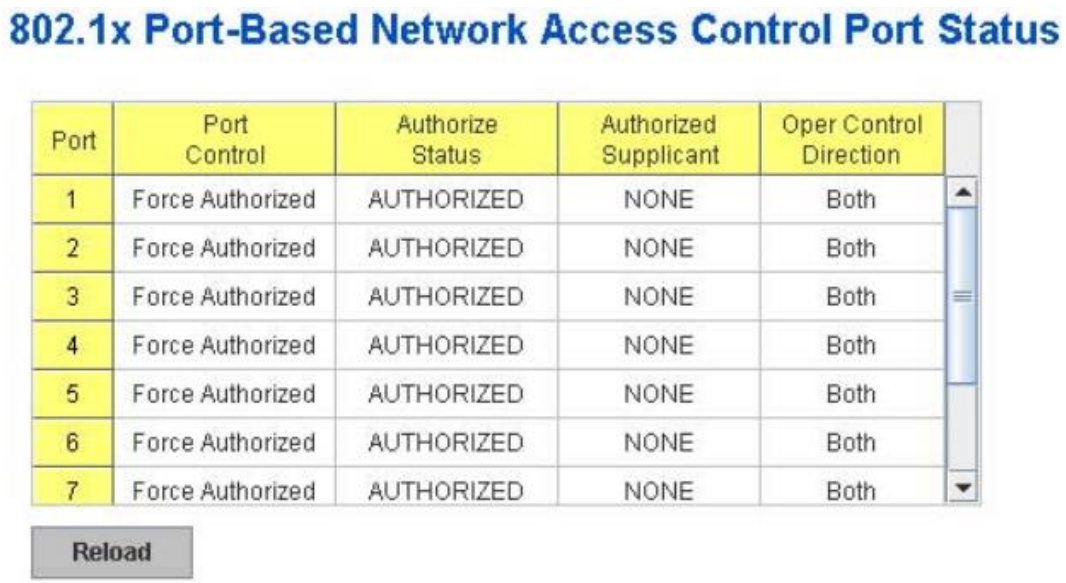

Figura 4-69. Port-Based Network Access Control Port Status

Comandos CLI de Segurança

Característica	Linha de Comando
Segurança de Porta (Port Security)	
Adicionar MAC	Switch(config)# mac-address-table static 0012.7701.0101 vlan 1 interface fa1 mac-address-table unicast static set ok!
Segurança de Porta (Port Security)	Switch(config)# interface fa1 Switch(config-if)# switchport port-security Disables new MAC addresses learning and aging activities! Note: Rule: Add the static MAC, VLAN and Port binding first, then enable the port security to stop new MAC learning.
Desabilitar Porta de Segurança (Disable Port Security)	Switch(config-if)# no switchport port-security Enable new MAC addresses learning and aging activities!
Mostrar (Display)	Switch# show mac-address-table static Destination Address / Address Type / Vlan / Destination Port 0012.7701.0101 / Static / 1 / fa1
Segurança de IP (IP Security)	

Segurança de IP (IP Security)	Switch(config)# ip security Set ip security enable ok. Switch(config)# ip security host 192.168.10.33 Add ip security host 192.168.10.33 ok.
Display	Switch# show ip security ip security is enabled ip security host: 192.168.10.33
802.1x	
Habilitar (Enable) Desabilitar (Disable)	Switch(config)# dot1x system-auth-control Switch(config)# Switch(config)# no dot1x system-auth-control Switch(config)#
Método de Autenticação (authentic-method)	Switch(config)# dot1x authentic-method local Use the local username database for authentication radius Use the Remote Authentication Dial-In User Service (RADIUS) servers for authentication Switch(config)# dot1x authentic-method radius Switch(config)#
radius server-ip	Switch(config)# dot1x radius Switch(config)# dot1x radius server-ip 192.168.10.120 key 1234 RADIUS Server Port number NOT given. (default=1812) RADIUS Accounting Port number NOT given. (default=1813) RADIUS Server IP: 192.168.10.120 RADIUS Server Key: 1234 RADIUS Server Port: 1812 RADIUS Accounting Port: 1813 Switch(config)#
radius server-ip	Switch(config)# dot1x radius Switch(config)# dot1x radius server-ip 192.168.10.120 key 1234 RADIUS Server Port number NOT given. (default=1812) RADIUS Accounting Port number NOT given. (default=1813) RADIUS Server IP: 192.168.10.120 RADIUS Server Key: 1234 RADIUS Server Port: 1812 RADIUS Accounting Port: 1813 Switch(config)#
radius secondary-server-ip	Switch(config)# dot1x radius secondary-server-ip 192.168.10.250 key 5678 Port number NOT given. (default=1812) RADIUS Accounting Port number NOT given. (default=1813) Secondary RADIUS Server IP: 192.168.10.250 Secondary RADIUS Server Key: 5678 Secondary RADIUS Server Port: 1812 Secondary RADIUS Accounting Port: 1813
User name/password for authentication	Switch(config)# dot1x username korenix passwd korenix vlan 1

Tabela 4-18. Linhas de Comando CLI para Configuração de Segurança

Advertência

O JN4508F-M fornece vários tipos de recursos de advertência para monitoramento remoto, e até mesmo fornece um mecanismo de alerta em tempo real. Esses recursos incluem um sistema de Log para servidores locais e remotos, alertas de e-mail SMTP e um alarme a relé de falha.

Configuração do Relé de Falha

O JN4508F-M fornece 1 saída digital, também conhecida como Saída a Relé. Os contatos do relé estão energizados (abertos) na operação normal e fecharão em condições de falha.

Condições de falha incluem a falha de energia, falha no link da porta Ethernet, falha de Ping e mudança de topologia de Super Anel.

Da versão de firmware 1.1ª em diante, o suporte padrão do relé passa a ser de múltiplos eventos de funções. Isso significa que o relé não suporta somente uma falha, ele pode ser usado para diversos eventos. As condições e terminologia são descritos a seguir.

Term	Condiction	Description
Power	Power DC1 Power DC2 Any	Detecta o estado da entrada de alimentação. Se uma das condições ocorreu, o relé é acionado.
Port Link	Port number	Monitora o evento de queda de link
Ring	Falha em Anel (Ring failure)	Se a topologia anel muda
Ping	IP Address: remote device's IP address	Se o IP destino não responde a requisição, o relé é acionado
Ping Reset	IP address: endereço de dispositivo remoto Reset Time: duração da saída em aberto Hold Time: duração de Ping hold time.	Dispositivo de ping destino e trigger de relé para emular reposição de energia para o dispositivo remoto, em caso de falha no sistema remoto. **Nota**: uma vez executado o reset de Ping, a saida do relé ficará em curto circuito.
Dry Output	On period: duração da saída do relé fechada Off period: duração da saída do relé aberta	Relé permanentemente executa On / Off com duração e comportamento diferente.
DI	DI number (JN4508F-M supports 1 DI)	Relé trigger quando a DI muda para nível alto ou baixo

Tabela 4-19. Condições de Falha do Relé

A configuração padrão do relé de usuário é mostrada abaixo:

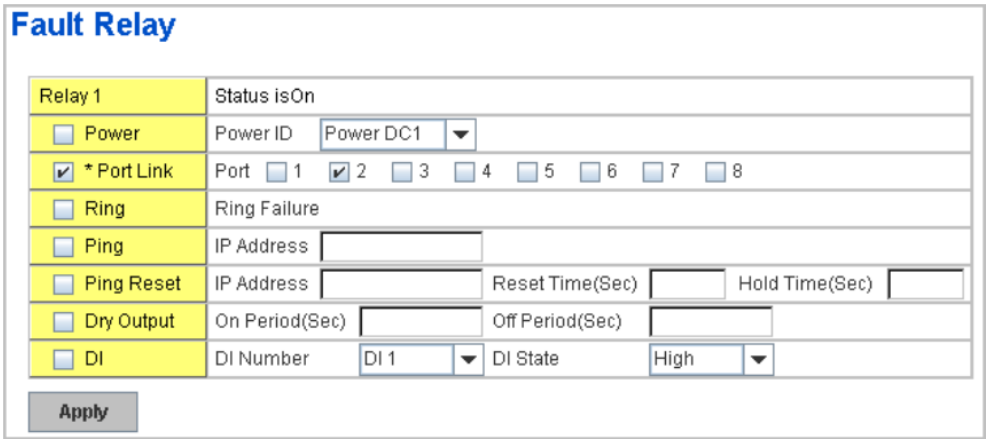

Figura 4-70. Configurações de Falha do Relé

Relay 1: Mostra o status real do relé.

On Period (Sec): Digite o tempo de período para ligar o Relé de Saída. Faixa possível 0-65535 segundos.

Off Period (Sec): Digite o tempo de período para desligar o Relé de Saída. Faixa possível 0-65535 segundos.

Hold Time (Sec): Digite o tempo de retenção antes de liberar um pacote de ping.

Seleção de Evento

Inclui as seguintes opções: Saída seca, falta de energia, falha de Link, falha de Ping e falha de Super Anel. Cada tipo de evento tem seus próprios parâmetros e são configuráveis. Cada relé pode ter um tipo de evento.

Evento de Sistema	Alerta de Evento é Enviado Quando...
Device Cold Start	Energia é cortada e então reconectada
Device Warm Start	Dispositivo é reiniciado via CLI ou Web UI.
Power 1 Failure	Power 1 is failure.
Power 2 Failure	Power 2 is failure.
Authentication failure	Uma senha incorrenta. A STRING da Community foi inserida no SNMP
Time Synchronize Failure	Acesso ao Servidor NTP falhou.
Fault Relay	A DO/Relé de falha está ligado.
Super Ring Topology Changes	Mestre de um Super Ring mudou ou o caminho alternativo está ativo
DI1 Change	A Entrada Digital#1 mudou de status.
Port Event	**Alerta de Evento é Enviado Quand…**
Link-Up	A porta é conectada a outro dispositvo
Link-Down	A porta é disconectada (ex. O cabo é removido ou os dispositivos são desligados)
Both	O Status do link mudou.

Tabela 4-20. Eventos de Porta e Sistema

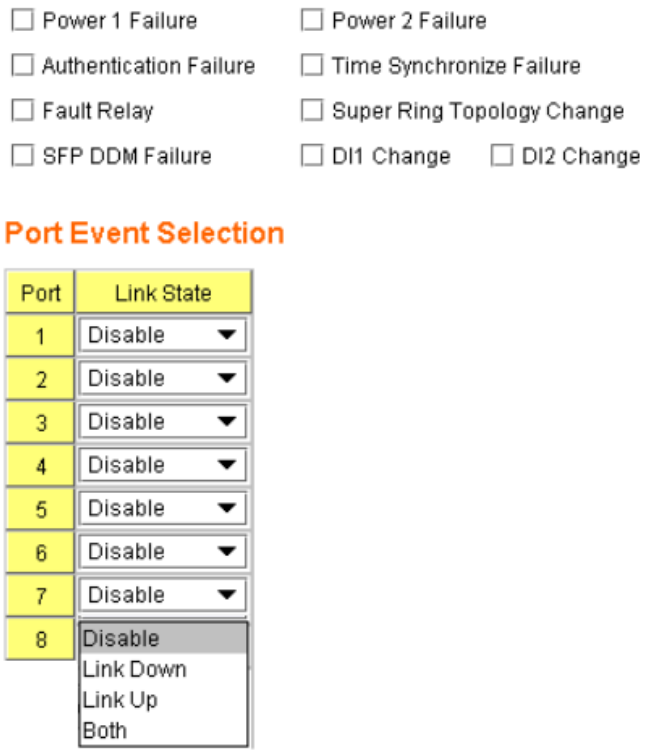

Figura 4-71. Seleção de Eventos de Sistema e Porta

Uma vez terminada a configuração, clique em *Apply* para aplicar as alterações.

Configuração do SysLog

O log do sistema é útil para informar ao administrador do sistema local e remoto, o monitoramento do histórico do switch. Existem 2 modos de Log do sistema fornecidos pelo JN4508F-M: modo local e remoto.

Local Mode: Neste modo, o JN4508F-M irá imprimir os eventos anteriores selecionados (via página de seleção de eventos) para a tabela de Log do sistema do switch. O usuário pode monitorar os logs de sistema na página « [Monitor and Diag] / [Event Log] ».

Remote Mode: O modo remoto é também conhecido como modo de servidor.

Neste modo, deve-se atribuir o endereço IP do servidor do log do sistema. O JN4508F-M enviará as ocorrências selecionadas, via página de seleção do evento, para o servidor de Log de sistema previamente definido.

Ambos: Os dois modos mencionados acima podem ser ativados ao mesmo tempo.

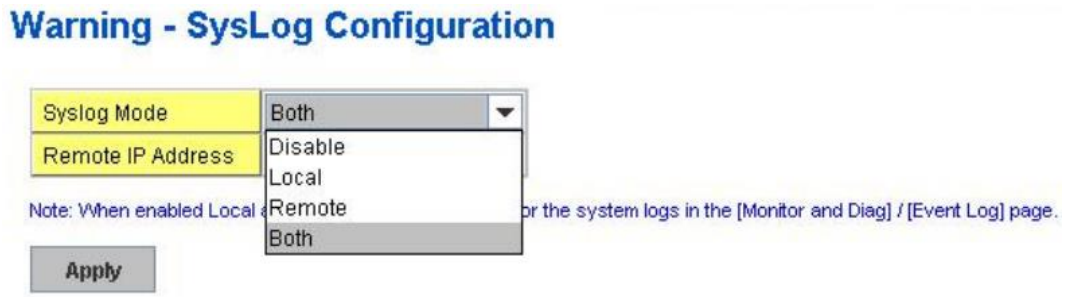

Figura 4-72. Tela de Configuração de Advertência do Syslog

Ao finalizar a configuração clique no botão *Apply* para aplicar os ajustes realizados.

Nota:

Ao habilitar local, ou ambos os modos, o usuário pode monitorar os logs do sistema na página « [Monitor and Diag] / [Event Log] ».

Configuração de SMTP

A JN4508F-M inclui um recurso de advertência via E-mail. O switch irá enviar ocorrências para um servidor de E-mail remoto. O receptor pode receber uma notificação por E-mail de acordo com a padronização SMTP.

Esse contexto, ilustrado na próxima imagem, permite que o usuário ative o alerta de E-mail e atribua o IP do servidor SMTP, bem como o E-mail do remetente e receptor. Se o servidor de SMTP solicita uma autorização prévia, também é possível configurar o nome de usuário e senha de acesso.

Figura 4-73. Tela de Configuração de Advertência SMTP

Campo	Descrição
SMTP Server IP Address	Digite o endereço IP do servidor de E-mail
Authentication	Clique a caixa de seleção para habilitar a senha
User Name	Digite o nome da conta de E-mail (máximo 40 caracteres)
Password	Digite a senha da conta de E-mail
Confirm Password	Re-digite a senha da conta de E-mail
O usuário pode definir até 4 endereços de E-mail para receber alarmes do JN4508F-M	
Rcpt E-mail Address 1	Primeiro endereço de E-mail que receberá o alerta do JN4508F-M (máximo 40 caracteres)
Rcpt E-mail Address 2	Segundo endereço de E-mail que receberá o alerta do JN4508F-M (máximo 40 caracteres)
Rcpt E-mail Address 3	Terceiro endereço de E-mail que receberá o alerta do JN4508F-M (máximo 40 caracteres)
Rcpt E-mail Address 4	Quarto endereço de E-mail que receberá o alerta do JN4508F-M (máximo 40 caracteres)

Tabela 4-21. Descrição dos Campos SMTP

Ao finalizar a configuração clique no botão *Apply* para aplicar os ajustes realizados.

Linhas de Comando (CLI) para Configuração de Advertências

Característica	Linha de Comando
Saída a Relé	
Saída a Relé	Switch(config)# relay 1 dry dry output ping ping failure port port link failure power power failure ring super ring failure
Saída Seca	Switch(config)# relay 1 dry < 0-4294967295 > ativar período (em segundos)

	Switch(config)# relay 1 dry 5 < 0-4294967295 > desativar período (em segundos) Switch(config)# relay 1 dry 5 5
Falha de Ping	Switch(config)# relay 1 ping 192.168.10.33 <cr> reset reset a device Switch(config)# relay 1 ping 192.168.10.33 reset tempo de reset < 1-65535 > Switch(config)# relay 1 ping 192.168.10.33 reset 60 < 0-65535 > Tempo de espera para nova tentativa Switch(config)# relay 1 ping 192.168.10.33 reset 60 60
Falha de Link de Porta	Switch(config)# relay 1 port PORTLIST port list Switch(config)# relay 1 port fa1 -5
Falha de Energia	Power Failure Switch(config)# relay 1 power ID da Alimentação < 1 -2 > Switch(config)# relay 1 power 1 Switch(config)# relay 1 power 2
Falha de Super Anel	Switch(config)# relay 1 ring
Desabilitar Relé	Switch(config)# no relay ID do relé < 1 -2 > Switch(config)# no relay 1 (Relay_ID: 1 ou 2) <cr>
Display	Switch# show relay 1 Relay Output Type: Port Link Port: 1, 2, 3, 4, Switch# show relay 2 Relay Output Type: Super Ring
Seleção de Evento	
Seleção de Evento	Switch(config)# warning-event coldstart Switch cold start event warmstart Switch warm start event linkdown Switch link down event linkup Switch link up event all Switch all event authentication Authentication failure event fault-relay Switch fault relay event power Switch power failure event super-ring Switch super ring topology change eve time-sync Switch time synchronize failure event
Ex: Evento de inicialização a frio	Switch(config)# warning-event coldstart Evento de inicialização a frio habilitado.
Ex: Evento de link ativo	Switch(config)# warning-event linkup [IFNAME] Interface name, ex: fastethernet1 or gi8 Switch(config)# warning-event linkup fa5 Evento de link ativo fa5 habilitado.
Display	Switch# show warning-event Warning Event: Cold Start: Enabled Warm Start: Disabled Authentication Failure: Disabled Link Down: fa4-5 Link Up: fa4-5 Power Failure: Super Ring Topology Change: Disabled Fault Relay: Disabled
Configuração do Syslog	
Modo Local	Switch(config)# log syslog local
Modo de Servidor	Switch(config)# log syslog remote 192.168.10.33
Ambos	Switch(config)# log syslog local

	Switch(config)# log syslog remote 192.168.10.33
Disable	Switch(config)# no log syslog local
Configuração de SNMTP	
Habilitar SMTP	Switch(config)# smtp-server enable email-alert Alerta de E-mail SMTP habilitado.
E-mail do remetente	Switch(config)# smtp-server server 192.168.10.100 Conta de E-mail do servidor SMTP, ex: admin@altus.com.br Switch(config)# smtp-server server 192.168.10.100 admin@altus.com.br SMTP Email Alert set Server: 192.168.10.100, Account: admin@altus.com.br ok.
E-mail do Receptor	Switch(config)# smtp-server receipt 1 receiver@altus.com.br Alerta de E-mail SMTP (receptor 1): receiver@altus.com.br.
Autenticação com nome de usuário e senha	Switch(config)# smtp-server authentication username admin senha admin Alerta de E-mail SMTP com autenticação de Usuário: admin, Senha: admin Nota: O usuário pode atribuir strings para nome de usuário e senha.
Desativar SMTP	Switch(config)# no smtp-server enable email-alert Alerta de E-mail SMTP desativado.
Desabilitar Autenticação	Switch(config)# no smtp-server authentication Alerta de E-mail SMTP com autenticação desativado.
Display	Switch# sh smtp-server SMTP Email Alert is Enabled Server: 192.168.10.100, Account: admin@altus.com.br Authentication: Enabled Username: admin, Password: admin SMTP Email Alert Receipt: Receipt 1: receiver@altus.con.br Receipt 2: Receipt 3: Receipt 4:

Tabela 4-22. Linhas de Comando (CLI) para Configuração de Advertências

Monitoramento e Diagnóstico

O JN4508F-M fornece vários recursos para monitoramento do status do switch ou criação de um diagnóstico para verificação de problemas quando estes ocorrerem. As funcionalidades incluem a tabela de endereços MAC, estatísticas de porta, Log de eventos e Ping.

Tabela de Endereços MAC

O JN4508F-M fornece 2K de entradas na tabela de endereços MAC. Nesta página, os usuários podem alterar o tempo de envelhecimento, adicionar o endereço MAC Estático Unicast, monitorar o endereço MAC ou classificá-los por portas e tipos de pacotes diferentes. Clique no botão *Apply* para alterar o valor.

Tempo de Envelhecimento (s) (Aging Time)

Cada switch tem uma quantidade limitada de espaço para escrever o endereço MAC aprendido. Para salvar mais entradas para novos endereços MAC, o switch envelhecerá quaisquer entradas de endereço MAC não utilizadas no que diz respeito ao tempo de envelhecimento. O Tempo de Envelhecimento padrão é 300 s. O Tempo de Envelhecimento pode ser modificado nesta página.

Endereço MAC Estático Unicast (Static Unicast MAC Address)

Para algumas aplicações, os usuários podem precisar digitar o endereço MAC estático unicast em sua tabela de endereços MAC. Nesta página, pode-se digitar o endereço MAC (formato: xxxx.xxxx.xxxx) e selecionar sua VID e ID de porta. Clique no botão *Add* para adicioná-lo à tabela de endereços MAC.

Tabela de Endereços MAC (MAC Address Table)

Na tabela de endereços MAC, pode-se ver todos os endereços MAC aprendidos pelo switch. Os tipos de pacotes incluem gerenciamento Unicast, Unicast estático, Unicast dinâmico, Multicast estático e dinâmico. A tabela permite que os usuários classifiquem os endereços pelos tipos de pacotes e a porta.

Tipos de Pacotes (Packet Types)

O gerenciamento Unicast está relacionado ao endereço MAC do switch. Ele está associado à porta da UCP apenas. O endereço MAC unicast estático pode ser adicionado e excluído. MAC Unicast Dinâmico é o endereço MAC aprendido pelo switch. O multicast estático pode ser adicionado através da CLI e pode ser eliminado através da Web e CLI. O Multicast dinâmico aparecerá depois que o usuário tiver habilitado o IGMP e depois da descoberta do relatório IGMP pelo switch.

Clique no botão *Remove* para remover o endereço MAC Unicast/Multicast estático. Clique no botão *Reload* para atualizar a tabela. Os endereços MAC Unicast/Multicast recém-aprendidos serão atualizados na tabela de endereços MAC.

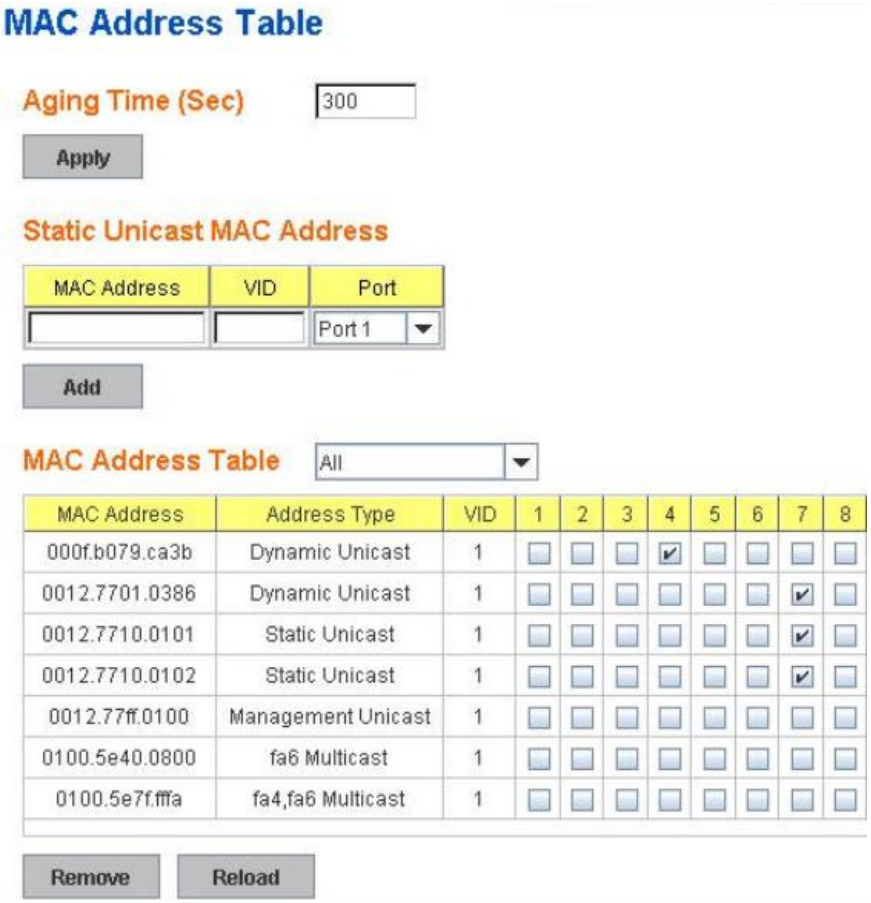

Figura 4-74. Configuração de Tabela de Endereços MAC

Estatísticas de Porta (Port Statistics)

Esta página exibe as estatísticas operacionais de cada porta. As estatísticas que podem ser vistas incluem o tipo e estado do Link, Rx OK, Rx NOK, Tx OK e Colisão. RX está relacionado aos pacotes recebidos enquanto TX refere-se aos pacotes transmitidos. As estatísticas somente mostram RX e TX (OK ou NOK) e Colisão.

Nota:

Se o usuário percebe um aumento no status *NOK* ou contagens de colisão, isto pode significar que o cabo de rede não está conectado corretamente, ou o desempenho de rede da porta está ruim. Verifique o cabo de rede, placa de Interface de rede conectada ao seu dispositivo, o aplicativo de rede, ou realoque o tráfego da rede.

Clique no botão *Clear Selected* para redefinir as contagens das portas selecionadas e no botão *Clear All* para reiniciar a contagem de todas as portas. Clique no botão *Reload* para atualizar as contagens.

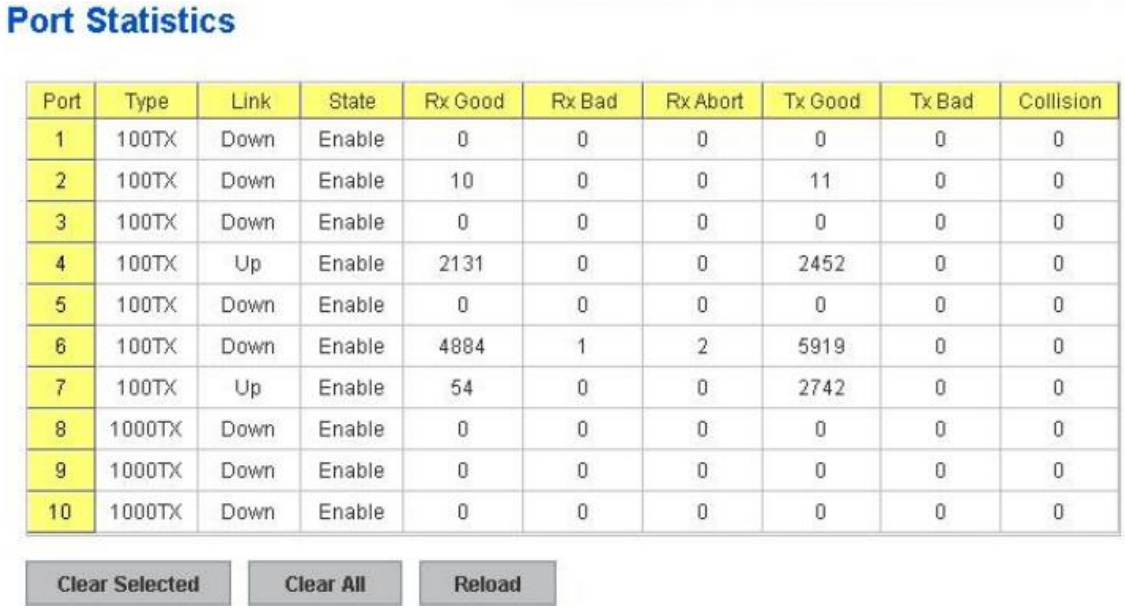

Figura 4-75. Tela de Estatísticas de Porta

Espelhamento de Porta (Port Mirroring)

Espelhamento de porta (também chamado *Port Spanning*) é uma ferramenta que lhe permite espelhar o tráfego a partir de uma ou mais portas para outra porta, sem interromper o fluxo do tráfego na porta original. Qualquer tráfego que vai para dentro ou fora da porta fonte será duplicada no Porta de Destino. Este tráfego pode então ser analisado na porta de destino utilizando um dispositivo de monitorização ou a aplicação. Um administrador de rede normalmente utiliza esta ferramenta para diagnósticos, depuração, ou evitar ataques.

Port Mirror Mode: Escolha *Enable* / *Disable* para ativar / desativar o modo de espelhamento de porta.

Source Port: Também conhecido como *Port Monitor*. Estas são as portas que deseja se monitorar. O tráfego de todas as portas de origem / monitoradas será copiado para portas de destino / análise. Pode se escolher uma única porta, ou qualquer combinação de portas, mas só se pode monitorá-los em Rx ou TX somente. Clique na caixa de seleção da Port ID, RX, Tx ou Both para selecionar as portas de origem.

Destination Port: Também conhecido como *Analysis Port*. Pode se analisar o tráfego de todas as portas monitoradas nesta porta, sem afetar o fluxo de tráfego na porta (s) a ser monitorado. Apenas um RX / TX da porta de destino pode ser selecionado. Um administrador de rede normalmente conecta um analisador de LAN ou dispositivo Netxray a esta porta.

Uma vez que terminada as configurações e definições, clique em *Apply* para aplicar as configurações.

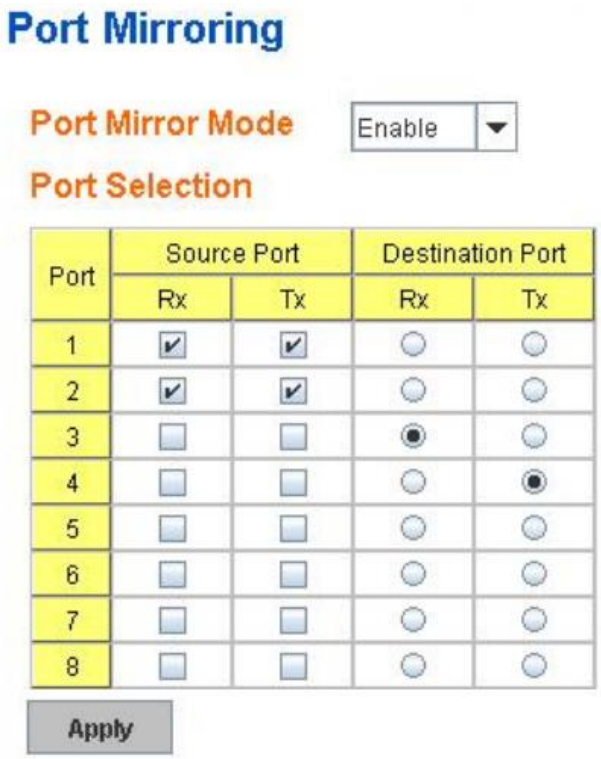

Figura 4-76. Espelhamento de Portas

Log de Eventos

Na seção IEEE 802.1x foi inserido o recurso de Log do Sistema. Quando é selecionado o modo Log de Sistema Local, o JN4508F-M irá gravar os eventos ocorridos na tabela de log local. Esta página mostra a tabela de log. As entradas incluem o índice e dados, tempo e conteúdo das ocorrências.

Clique no botão *Clear* para apagar as entradas. Clique no botão *Reload* para atualizar a tabela.

Figura 4-77. Tela de Log de Eventos do Sistema

Descoberta da Topologia (Topology Discovery)

JN4508F-M suporta a descoberta de topologia LLDP (IEEE 802.1AB Link Layer Discovery Protocol) função que pode ajudar o usuário na descoberta de dispositivos na rede de vários fornecedores no mesmo segmento por sistema NMS que suporta a função de LLDP, por exemplo NMS (IEEE 802.1AB Link Layer Discovery Protocol); Com a função de LLDP, NMS se torna mais fácil manter o mapa de topologia, exibir a ID da porta, descrição da porta, a descrição do sistema, VLAN ID.

Uma vez ocorrendo uma falha de ligação, os eventos de mudança de topologia podem ser atualizados para o NMS também. O LLDP Port State pode exibir o ID vizinho e IP conhecido partir dos dispositivos conectados.

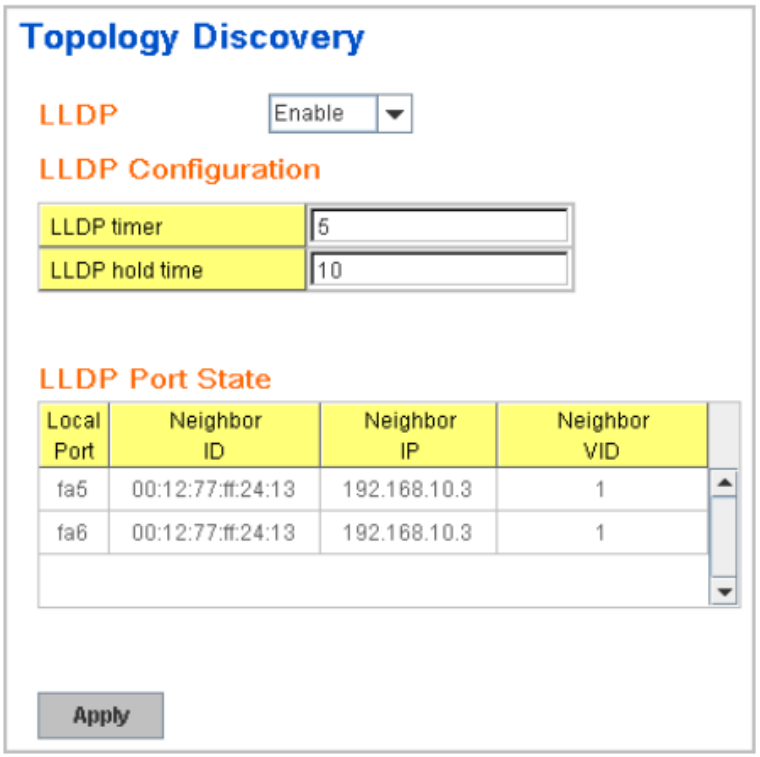

Figura 4-78. Tela de Topology Discover

LLDP: Selecione *Enable/Disable* para Habilitar / Desabilitar a função LLDP.

LLDP Configuration: Para configurar o temporizador relacionado de LLDP.

LLDP Timer: o intervalo de tempo de cada LLDP a contagem é em segundos; o número válido é de 5 a 254, padrão é 30 segundos.

LLDP Hold Time: Temporizador TTL (Time To Live). O estado LLDP será expirado uma vez que o LLDP não for recebido até o tempo de espera. O padrão é 120 segundos.

Local Port: o número da porta atual que liga o dispositivo de rede vizinho.

Neighbor ID: o endereço MAC do dispositivo vizinho no mesmo segmento de rede.

Neighbor IP: o endereço IP do dispositivo vizinho no mesmo segmento de rede.

Neighbor VID: o ID da VLAN do dispositivo vizinho no mesmo segmento de rede.

Utilitário Ping

Este utilitário permite aos usuários efetuar o ping em dispositivos remotos e verificar se o dispositivo está ativo ou não. Digite o endereço IP do dispositivo de destino no IP de Destino. Clique no botão *Start* para iniciar o ping. O usuário pode acompanhar os resultados no campo específico destes.

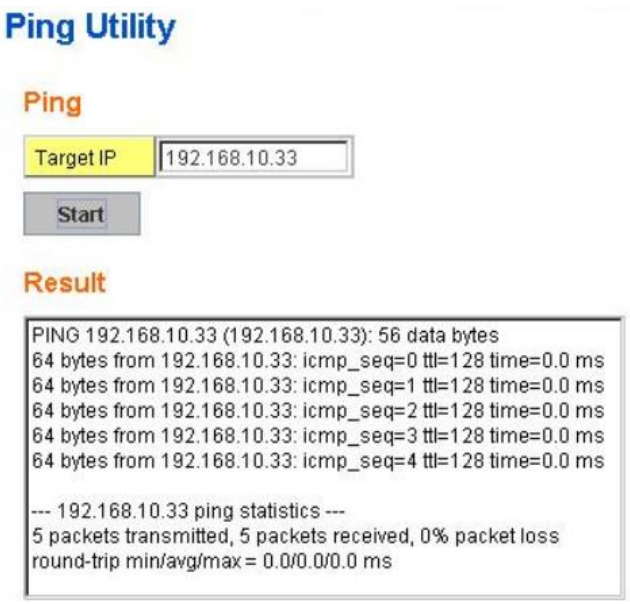

Figura 4-79. Tela do Utilitário Ping

Comandos CLI para Monitoramento e Diagnóstico

Funcionalidade	Linha de Comando
Tabela de Endereços MAC	
Tempo de Envelhecimento	Switch(config)# mac-address-table aging-time 350 tempo de envelhecimento MAC-address-table definido! **Nota:** 350 é o novo valor do tempo limite de envelhecimento.
Adicionar endereço MAC Unicast estático	Switch(config)# mac-address-table static 0012.7701.0101 vlan 1 interface fastethernet1 MAC-address-table unicast estático definido! Nota: regra... mac-address-table static MAC_address VLAN VID interface interface_name
Adicionar o endereço MAC Multicast	Switch(config)# mac-address-table multicast 0100.5e01.0101 vlan 1 interface fa1 -6 Adiciona uma entrada na tabela multicast! **Nota:** regra... mac-address-table multicast MAC_address VLAN VID interface_list interface_name/range
Mostra o endereço MAC (todos os tipos)	Switch# show mac-address-table ***** UNICAST MAC ADDRESS ***** Destination Address / Address Type / Vlan / Destination Port 000f.b079.ca3b / Dynamic / 1 / fa1 0012.7701.0386 / Dynamic / 1 / fa2 0012.7710.0101 / Static / 1 / fa6 0012.7710.0102 / Static / 1 / fa6 0012.77ff.0100 / Management / 1 / -------- ***** MULTICAST MAC ADDRESS ***** Vlan / Mac Address / COS Status / Ports 1 / 0100.5e40.0800 / 0 / fa6 1 / 0100.5e7f.fffa / 0 / fa4,fa6
Mostra o endereço MAC aprendido dinamicamente	Switch# show mac-address-table dy Destination Address / Address Type / Vlan / Destination Port 000f.b079.cb93 / Dynamic / SVL / fa1

<table>
<tr><td>Mostra o endereço MAC
MAC Multicast</td><td>Switch# show mac-address-table multicast
JN4508F-M Mana# show mac-address-table multicast
Vlan Mac Address COS Status Ports
---------- ---------- ---------- ----------
1 0100.5e40.0800 0 fa6-7
1 0100.5e7f.fffa 0 fa4,fa6-7</td></tr>
<tr><td>Mostra o endereço MAC Estático</td><td>Switch# show mac-address-table static
Destination Address Address Type Vlan Destination Port
---------- ---------- ---------- ----------
0012.7710.0101 Static 1 fa6
0012.7710.0102 Static 1 fa6</td></tr>
<tr><td>Mostra o Timeout de Envelhecimento</td><td>Switch# show mac-address-table aging-time
o tempo de envelhecimento mac-address-table é 304 s.</td></tr>
<tr><td colspan="2">Estatísticas de Porta</td></tr>
<tr><td>Estatísticas de Porta</td><td>Switch# show rmon statistics fa4 (select interface)
Interface fastethernet4 is enable connected, which has
Inbound:
Good Octets: 178792, Bad Octets: 0
Unicast: 598, Broadcast: 1764, Multicast: 160
Pause: 0, Undersize: 0, Fragments: 0
Oversize: 0, Jabbers: 0, Disacrds: 0
Filtered: 0, RxError: 0, FCSError: 0
Outbound:
Good Octets: 330500
Unicast: 602, Broadcast: 1, Multicast: 2261
Pause: 0, Deferred: 0, Collisions: 0
SingleCollision: 0, MultipleCollision: 0
ExcessiveCollision: 0, LateCollision: 0
Filtered: 0, FCSError: 0
Number of frames received and transmitted with a length of:
64: 2388, 65to127: 142, 128to255: 11
256to511: 64, 512to1023: 10, 1024toMaxSize: 42</td></tr>
<tr><td colspan="2">Port Mirroring</td></tr>
<tr><td>Enable Port Mirror</td><td>Switch(config)# mirror em Mirror set enable ok.</td></tr>
<tr><td>Disable Port Mirror</td><td>Switch(config)# mirror disable Mirror set disable ok.</td></tr>
<tr><td>Select Source Port</td><td>Switch(config)# mirror source fa1-2
both Received and transmitted traffic
rx Received traffic
tx Transmitted traffic
Switch(config)# mirror source fa1-2 both
Mirror source fa1-2 both set ok.
Nota: Select source port list and TX/RX/Both mode.</td></tr>
<tr><td>Select Destination Port</td><td>Switch(config)# mirror destination fa6 both
Mirror destination fa6 both set ok</td></tr>
<tr><td>Display</td><td>Switch# show mirror
Mirror Status: Enabled
Ingress Monitor Destination Port: fa6
Egress Monitor Destination Port: fa6
Ingress Source Ports:fa1,fa2,
Egress Source Ports:fa1,fa2,</td></tr>
<tr><td colspan="2">Log de Eventos</td></tr>
<tr><td>Display</td><td>Switch# show event-log
<1>Jan 1 02:50:47 snmpd[101]: Event Link 4 Down.
<2>Jan 1 02:50:50 snmpd[101]: Event: Link 5 Up.
<3>Jan 1 02:50:51 snmpd[101]: Event: Link 5 Down.
<4>Jan 1 02:50:53 snmpd[101]: Event: Link 4 Up.</td></tr>
<tr><td colspan="2">Ping</td></tr>
<tr><td>Ping IP</td><td>Switch# ping 192.168.10.33</td></tr>
</table>

	PING 192.168.10.33 (192.168.10.33): 56 bytes de dados 64 bytes de 192.168.10.33: icmp_seq=0 ttl=128 time=0.0 ms 64 bytes de 192.168.10.33: icmp_seq=1 ttl=128 time=0.0 ms 64 bytes de 192.168.10.33: icmp_seq = 2 ttl = 128 tempo = 0.0 ms 64 bytes de 192.168.10.33: icmp_seq = 3 ttl = 128 tempo = 0.0 ms 64 bytes de 192.168.10.33: icmp_seq = 4 ttl = 128 tempo = 0.0 ms --- estatísticas do ping 192.168.10.33 --- 5 pacotes transmitidos, 5 pacotes recebidos, 0% de perda de pacotes round-trip min/avg/max = 0.0/0.0/0.0 ms

Tabela 4-23. Linhas de Comando para Configuração de Monitoramento e Diagnóstico

Painel Frontal do Dispositivo

O painel frontal do dispositivo de comando permite que veja se o status LED do switch. Se pode ver o status da ligação do LED de energia e, DO, DI, RM e portas

Característica	Status
Power	Ligado: energia CC está conectada
Digital Output	Ligado: Dry Relay Output activated and the contact is formed a close circuit.
Digital Input	Ligado: Digital Input is triggered to “High” level
R.M.(Ring Master)	Verde Ligado: Status do Anel normal.Amarelo Anel está operando de forma anormal
Fast Ethernet	Verde Ligado: A porta está conectada.
Sys	Verde Ligado: O Sistema está pronto para operar.

Tabela 4-24. Descrição dos LEDs do Painel Frontal

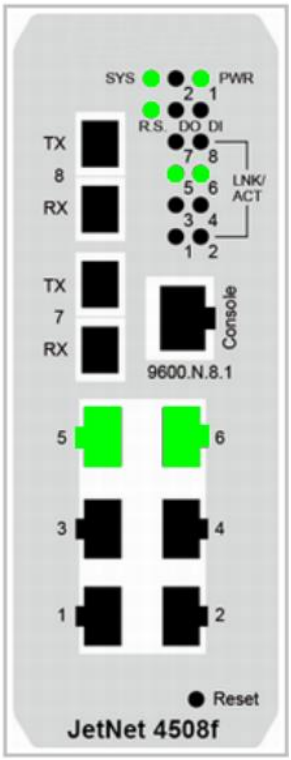

Figura 4-80. Painel Frontal do Switch

Salvar em Flash

A opção Salvar Configuração permite que o usuário grave qualquer configuração na memória Flash. O desligamento do switch sem a seleção da opção Salvar Configuração provocará a perda das configurações. Depois de selecionar *Salvar Configuração*, clique no botão *Save to Flash* para salvar a nova configuração.

Figura 4-81. Tela Salvar em Flash

Funcionalidade	Linha de Comando
Salvar	Switch# write Configuração de compilação... [OK] Switch# copy running-config startup-config Configuração de compilação... [OK]

Tabela 4-25. Linhas de Comando de Salvar em Flash

Logout

O switch fornece dois métodos de logout. Ocorrerá um logout da conexão com a web se o usuário não introduzir um comando no período de 30 s. O comando Logout permite que seja realizado um logout manual na conexão web. Clique *Yes* para efetuar o logout, e *No* para retornar à página de configuração.

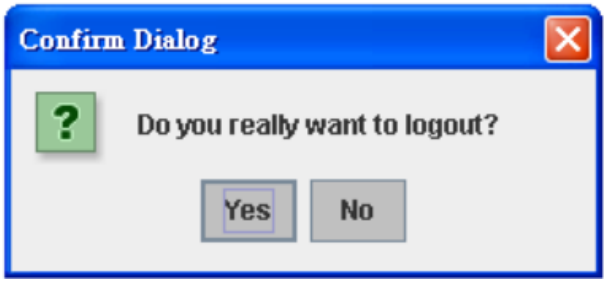

Figura 4-82. Tela de Logout

Funcionalidade	Linha de Comando
Logout	Switch> exit Switch# exit

Tabela 4-26. Linhas de Comando de Logout

5. Apêndice

Especificações do Produto

Tecnologia	
Normas	IEEE 802.3 10Base-T Ethernet IEEE 802.3u 100Base-TX Fast Ethernet IEEE 802.3u 100Base-FX Fast Ethernet IEEE 802.3x Flow Control and Back-pressure IEEE 802.1AB Link Layer Discovery Protocol (LLDP) IEEE 802.1p Class of Service (CoS) IEEE 802.1Q VLAN and GVRP IEEE 802.1Q-in-Q and Private VLAN IEEE 802.1D-2004 Rapid Spanning Tree Protocol (RSTP) IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) IEEE 802.3ad Link Aggregation Protocol (LACP) IEEE 802.1x Port Based Network Access Protocol IEEE 1588 Precision Time Protocol (PTP)
Desempenho	
Tecnologia do Switch	Armazenamento e tecnologia de transmissão de 3.2Gbps Switch Fabric
Taxa de Comunicação do Sistema	26 Mega packets por segundo, 64 bytes packet de tamanho. 14,880 PPS for 10Base-T 148,800 PPS for 100Base-TX (PPS: Packet Per Second)
Desempenho da CPU	32 bits ARM-9E running at 180 MHz and performance up to 200MIPS; Hardware Incorporado baseado em Temporizador do Cão de Guarda.
Memória do Sistema	8M bytes flash ROM, 64M bytes SDRAM.
MAC Address	Tabela de endereços MAC de 8K.
Packet Buffer	Embedded 1Mbits shared buffer
Desempenho de Transferência	64 bytes to 1522bytes (includes 1522 bytes VLAN Tag).
Alarme de Relé	Dry Relay output with 1A /24V DC ability
Entrada Digital (DI)	Uma entrada digital com isolamento foto copular Digital Hi: DC 11V~30V Digital Low: DC 10V~0V
Gerenciamento do Sistema	
Configuração e Monitoramento da Interface	Suporta 4 configurações e interfaces de monitoramento: RS-232 console serial, Telnet, SNMP e interface de Web Browser As interfaces RS-232 e suporta Telnet Cisco como instruções
Atualização/Backup de Sistema	Fornece TFTP / interface Web para upgrade de firmware e backup de configuração, restauração
Telnet & Local Console	Suporta interface de linha de comando com a Cisco como comandos e máximo de 4 sessões; a interface telnet também suporta SSH
SNMP	Suporta v1, v2c, V3 com a função de TRAP de SNMP, até 4 estações de TRAP podem ser configuradas manualmente e o endereço IP do servidor Trap
SNMP MIB	MIBII, Bridge MIB, Ethernet-like MIB, VLAN MIB, IGMP MIB, Private MIB
Utilidade	Supports JetView and JetView Pro with IEEE 802.1AB Link Layer Discovery Protocol for device finding and link topology discovery
Network Time Protocol	Suporta o protocolo NTP com função de economia de luz do dia e localizar a função de sincronização de tempo.
Management IP Security	Segurança de endereço IP para impedir o acesso não autorizado
Management interface	SNMP v1, v2c e v3, navegador Web e Gestão Console
Alerta por E-mail	Até 4 contas de email com autenticação de servidor de e-mail
System Log	Suporta tanto servidor local ou remoto com autenticação
Desempenho de Rede	
IEEE 802.3x	O controle de fluxo de pausa de frames em 10/100bps com Full Duplex e Back Pressure com suporte de 100/10Mbps, Half Duplex somente.

Configuração da Porta	Port link Speed, Link mode, current status and enable/disable
Port Trunk	IEEE 802.3ad port aggregation and static port trunk; trunk member up to 8 ports and maximum 4 trunk groups.
VLAN	IEEE 802.1Q Tag VLAN with 256 VLAN Entries and provides 2K GVRP entries 3 VLAN link modes- Trunk, Hybrid and Link access
IEEE 802.1 Q-in-Q	Supports Double VLAN Tag function for implementing Metro Network topologies.
Private VLAN	A VLAN privada suporta acesso a porta isolada com a porta de uplink no switch. Normalmente, cada VLAN privada contém muitas portas privadas e uma determinada porta uplink; cada porta privada é isolada com a outra e só se comunica com a porta de uplink para os dados de saída e dados de entrada para fornecer a porta de cliente isolado.
Class of Service	Classe IEEE 802.1p de serviço; 4 filas de prioridade por porta.
Priorização de Tráfego	Supports 4 physical queues, weighted run robin queuing (WRR 8:4:2:1) and Strict Priority scheme, which follows 802.1p COS tag and IPv4 ToS/ Diffserv information to prioritize the traffic of your industrial network.
IGMP Snooping	IGMP Snooping v1 / v2 / v3 para filtragem de multicast e IGMP modo de consulta; também suporte a processo de multicasting desconhecido encaminhamento policies- drop, flood e encaminhar ao roteador.
Rate Control	Ingress filtering for Broadcast, Multicast, Unknown DA or all packets. Egress filtering for all packet types.
Port Mirroring	Online traffic monitoring on multiple selected ports
Port Security	Port security to assign authorized MAC to specific port
DHCP	DHCP Client, DHCP Server with IP & MAC Address binding and DHCP agent (option 82).
IEEE 802.1x with Radius Server Authentication	Port based network access control and also supports user authenticate by the radius account, password and key for the radius server authentication.
Redundância de Rede	
Multiple Super Ring	New generation of Ring Redundancy Technology, Includes Rapid Super Ring, Rapid Dual Homing, TrunkRing, MultiRing and backward compatible with legacy Super Ring.
Rapid Dual Homing	Multiple uplink paths to one or multiple upper switch
TrunkRing	Integrate port aggregate function in ring path to get higher throughput ring architecture
IEEE802.1d Rapid Spanning Tree	IEEE802.1D-2004 Rapid Spanning Tree Protocol. Compatible with Legacy Spanning Tree and IEEE 802.1w
IEEE802.1s Multiple Spanning Tree	Supports multiple RSTP deployed in a VLAN or multiple VLANs. IEEE802.1s MSTP, each MSTP instance can include one or more VLANs.
Interface	
Enclosure Port	Portas de Comunição Fast Ethernet: 8 x RJ-45 RS-232 console interface: RJ-45 conector DI/DO port: 4- Pino de Bloco de terminais removivel Power port: 4- Pino de Bloco de terminais removivel
Cables	10Base-T: 2-pairs UTP/STP Cat. 3, 4, 5 cable, EIA/TIA-568B 100-ohm (100m) 100 Base-TX: 2-pairs UTP/STP Cat. 5 cable, EIA/TIA-568B 100-ohm (100m) JN4508F-M: multi-mode, 50~62.5/125um, 2KM
Fiber port characteristics	JN4508F-M Wavelength:1310nm Tx power: -20dBm ~ -14dBm Rx sensitivity: -31dBm ~ 0dBm Link Budget: 11dB
RS-232 serial interface	Supports Cisco like command line interface for out-band management
LEDs de Diagnósticos do Sistema	
Sistema	Power status (Green): On (power is on applying) Digital Input (Green): On (Digital signal is detected) Alarm Output (Red): On (Output conductor is formed as a close circuit) System (Green): On (the system is ready), Blinking (system is on firmware upgrade progress) Ring Status (Green/Yellow): Green on (Ring status is normal), Green Blinking (wrong ring port connected), Yellow on (Ring Fail is occurred), Yellow blinking (ring path broken occurred at this switch)

Porta Ethernet	Link (Green On) / Activity (Green Blinking)
Power Requirements	
System Power	Redundant power input with polarity auto reverse protection Input Range: DC 24V (10~60V DC) Power System Type: Positive or Negative power source
Power Consumption	JetNet 4508f-m: 10Watts / DC 24V
Mecânico	
Instalação	DIN Rail Mounting or Wall Mounting
Mecânica	Aluminum metal case with grade 31 protection
Dimensões (mm)	55(W) x 149(H) x 131.2 (D) / with DIN Rail Clip 55(W) x 149(H) x 120.6(D) / without DIN Rail Clip
Peso	JetNet 4508f-m: 0.885Kg
Ambiental	
Temperatura de Operação	-10~70 ℃ (JetNet 4508f-m)
Umidade de Operação	0% ~ 90%, non-condensing
Storage Temperature	-40 ℃ ~ 85 ℃
Hi-Pot Insulation	AC 1.5KV for all ports and power
Aprovações Regulamentares	
EMC	IEC 61000-6-2, IEC 61000-6-4, EN50121-4 EMI FCC Class A, EN55022 Radiation, Conduction EMS IEC 61000-4-2, IEC 61000-4-3, IEC 61000-4-4, IEC 61000-4-5, IEC 61000-4-6, IEC 61000-4-8, IEC 61000-4-9
Vibração	IEC60068-2-6 Note-2
Choque	IEC60068-2-27 Note-2
Queda Livre	IEC60068-2-32 with package Note-3

Tabela 5-1. Especificações do Produto

MIB Privado

São fornecidas muitas MIBs padrão para que os usuários configurem ou monitorem a configuração do switch através do SNMP. Mas, uma vez que alguns comandos não pode ser encontrados na norma MIB, é fornecida uma MIB privada para satisfazer as necessidades. Compile o arquivo MIB privado com a sua ferramenta SNMP.

A árvore MIB privada é a mesma que a árvore web. Isto é mais fácil de entender e usar. Caso não esteja familiarizado com o padrão MIB, use diretamente uma MIB privada para gerenciar / monitorar o switch, não há necessidade de aprender cada OIDs dos comandos.

O caminho de JN4508F-M é 1.3.6.1.4.1.24062.2.3.1. A Figura 5-1 mostra a árvore MIB privada para sua referência.

O JN4508F-M MIB privado suporta vários tipos de entradas MIB, que são configurações básicas do sistema, configuração da porta, redundância de rede, VLAN, priorização de tráfego, multicasting, SNMP, segurança, aviso do sistema, monitoramento e configuração de salvamento. O usuário pode monitorar e configurar o JN4508F-M por ferramentas com navegador MIB SNMP e através dessas entradas MIB trabalhar com uma gestão remota. A MIB privada inclui 12 grandes entradas para configuração e monitoramento como listado abaixo pelo sistema:

System information: Somente leitura.

Basic Setting MIB entry: Leitura e escrita.

Port Configuration MIB entry: Leitura e escrita.

Network redundancy MIB entry: Leitura e escrita.

Vlan MIB entry: Leitura e escrita.

Traffic prioritization MIB entry: Leitura e escrita.

Multicast Filtering MIB entry: Leitura e escrita.

SNMP MIB entry: Leitura e escrita.

Security MIB entry: Leitura e escrita.

Warning MIB entry: Leitura e escrita.

Monitor and Diag: Leitura e escrita.

Save MIB entry: Escrita somente.

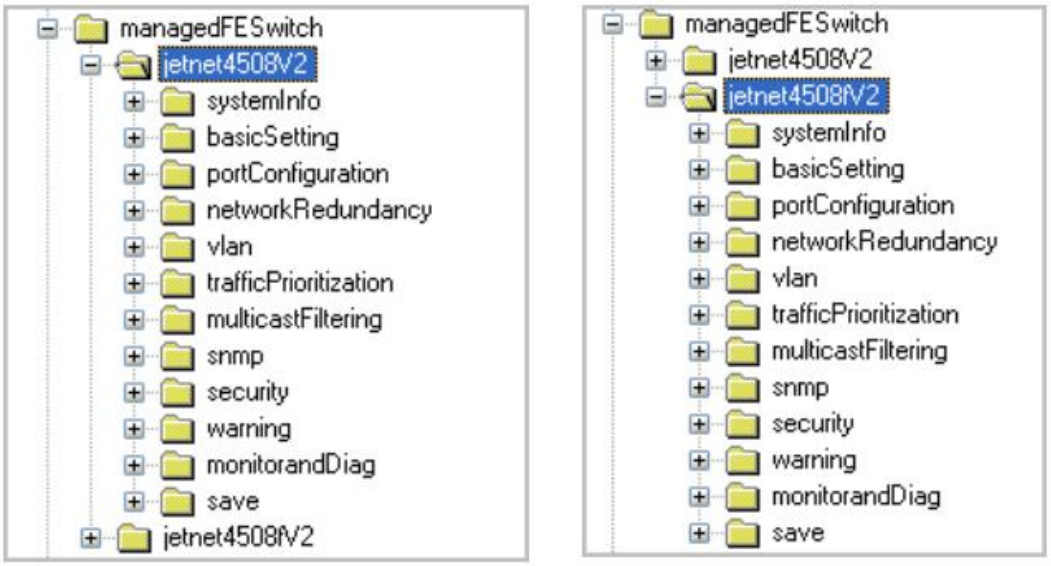

Figura 5-1. JN4508F-M Private MIB

Protocolo Modbus TCP

O Modbus TCP é muito semelhante ao Modbus RTU, mas transmite os dados dentro de pacotes TCP / IP de dados. Ele foi desenvolvido em 1979 para o sistema de comunicação automática industrial e tem se tornado um protocolo padrão para a comunicação industrial para os dispositivos de I/O analógicos discretos de transferência ou sistemas CLP. O Modbus define uma unidade de dados de protocolo simples independente da camada de enlace de dados subjacente. O pacote TCP modbus inclui três partes - cabeçalho MBAP, código de função e carga de dados, o cabeçalho MBAP é usado no cabeçalho TCP / IP para identificar Unidade de Dados de aplicação do Modbus e fornece algumas diferenças em comparação com a unidade de dados de aplicativo do Modbus RTU usado na linha serial. O cabeçalho MBAP também inclui identificador da unidade de reconhecimento e comunica entre várias unidades finais Modbus independentes.

Os dispositivos Modbus comunicam usando uma arquitetura mestre (cliente) / escravo (server), apenas um dispositivo pode iniciar as transações e os outros respondem ao mestre / cliente. Os outros dispositivos (escravo / servidor) respondem fornecendo os dados solicitados para o mestre / cliente, ou tomando as medidas solicitadas na requisição. O escravo / servidor pode ser qualquer dispositivo periférico (unidade DSC, unidade de CLP, Transdutor Tensão / Corrente, Switch de comunicação de rede), que processe a informação e envie os dados de saída para o mestre usando o protocolo TCP modbus. JN4508F-M Switch opera como dispositivo escravo / servidor, enquanto um dispositivo, tipicamente, mestre / cliente é o computador host que está executando o software aplicativo, como um sistema SCADA / HMI. A arquitetura de transação é mostrada como no desenho seguinte.

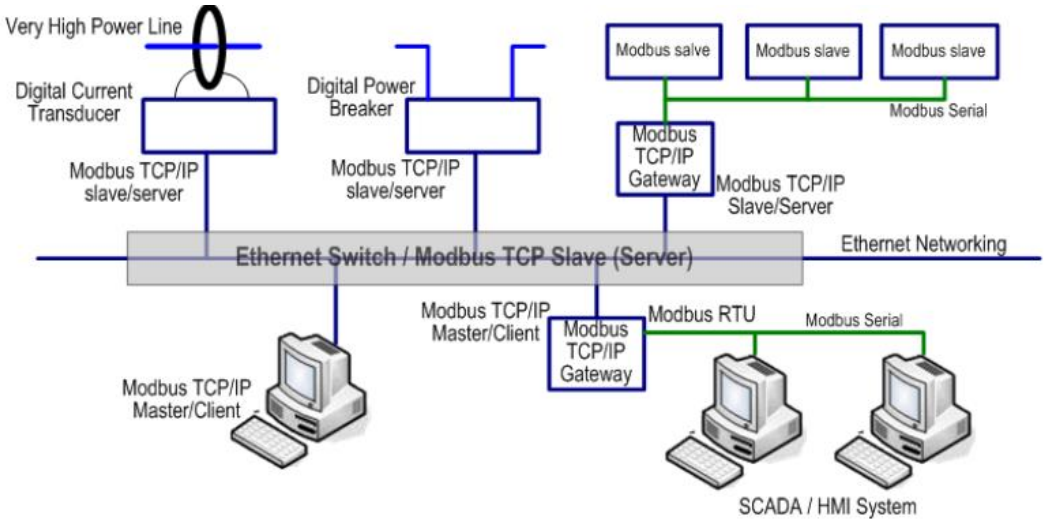

Figura 5-2. Comunicação Modbus

Existem três versões Modbus mais comuns, Modbus ASCII, Modbus RTU e Modbus TCP. Dispositivo baseado em Ethernet, Switch Ethernet industrial, por exemplo, suporta Modbus TCP que pode ser consultado através de Ethernet. Assim, o mestre Modbus TCP pode ler ou escrever os registradores Modbus fornecidos pelo Switch Ethernet Industrial.

O JN4508F-M Switch Gerenciável DIN-Rail Ethernet tem implementado o registo Modbus / TCP no firmware. Os mapeamentos de registo de algumas das informações operacionais do Switch Ethernet como descrição, endereço IP, status de alimentação, status da interface, informações de interface e estatísticas de pacotes de entrada / saída. Com os suportes de registo, o usuário pode ler as informações através de seu próprio progresso / display / aplicações monitoradas baseadas em Modbus TCP e monitorar o status de alterações com facilidade.

A configuração do Modbus / TCP está presente apenas em modo de gerenciamento CLI e nenhuma interface de usuário extra para configuração Web.

Código de Funções Modbus

Os dispositivos Modbus TCP utilizam uma referência normatizada para as funções Modbus TCP, códigos de acesso dependendo da informação. Os códigos de funções Modbus TCP são descritos abaixo.

FC	Nome	Uso
01	Read Coils	Lê o estado de uma saída digital
02	Read Input Status	Lê o estado de uma entrada digital
03	Read Holding Register	Lê um registro de saída com formato de 16 bits
04	Read Input Registers	Lê um registro de entrada com formato de 16 bits
05	Write Coil	Escreve dados para forçar uma saída digital para nível alto ou baixo
06	Write Single Register	Escreve um registro de saída com formato de 16 bits
15	Force Multiple Coils	Escreve uma sequencia consecutiva de saídas digitais

Tabela 5-2. Códigos de Funções Modbus TCP

O dispositivo JetNet suporta o código de função 04, Ler Registros de Entrada (*Read Input Registers*). Com este suporte, o SCADA ou outra aplicação Modbus TCP pode requisitar as informações do dispositivo e monitorar o estado principal do switch.

Verificação de Erros (Error Checking)

A utilização da verificação de erros ajudará a eliminar erros causados por ruído no link de comunicação. No modo Modbus TCP, as mensagens incluem um campo de verificação de erros, que é baseado num método de Verificação de Redundância Cíclica (*Cyclical Redundancy Check - CRC*). O CRC montado verifica o conteúdo de toda a mensagem. Aplicado independentemente de qualquer método de verificação de paridade utilizado para os caracteres- BYTE individuais da mensagem. O valor de CRC é calculado pelo dispositivo de transmissão, que acrescenta o CRC a mensagem. O dispositivo receptor recalcula um CRC durante a recepção da mensagem e compara o valor calculado para o valor real que recebeu no CRC arquivado.

Resposta à Exceção (Exception Response)

Se ocorrer um erro, o escravo envia uma mensagem de resposta de exceção para consistir o endereço do escravo, código de função, o código de resposta de exceção e o campo de verificação de erro. Em uma resposta de exceção, o escravo define a ordem de bit mais significativo (*Most Significative Bit - MSB*) do código de função de resposta. Os códigos de resposta de exceção estão listados abaixo.

FC	Nome	Descrição
01	Illegal Function	A função de mensagem recebida não é uma ação permitida.
02	Illegal Data Address	O endereço referido no campo de dados não é válido.
03	Illegal Data Value	O valor referenciado no local do dispositivo endereçado não está dentro da faixa esperada.
04	Slave Device Failure	Ocorreu um erro irrecuperável enquanto o escravo estava tentando executar a ação solicitada.
05	Acknowledge	O escravo aceitou o pedido e processou, mas um longo período de tempo será necessário para fazê-lo.
06	Slave Device Busy	O escravo está processando um comando do programa de longa duração.
07	Negative Acknowledge	O escravo não pode executar a função de programa recebido na requisição.
08	Memory Parity Error	O escravo tentou ler a memória estendida, mas detectou um erro de paridade na memória.

Tabela 5-3. Códigos de Resposta de Exceção Modbus

Tabela de Registro Modbus TCP

Word Address	Tipo de Dado	Descrição
Informações de Sistema (System Information)		
0x0000	16 words	Vender Name = “Korenix” Word 0 Hi byte = ‘K’ Word 0 Lo byte = ‘o’ Word 1 Hi byte = ‘r’ Word 1 Lo byte = ‘e’ Word 2 Hi byte = ‘n’ Word 2 Lo byte = ‘l’ Word 2 Hi byte = ‘x’ Word 2 Lo byte = ‘\0’ (other words = 0)
0x0010	16 words	Product Name = "JetNet5828G" Word 0 Hi byte = ‘J’ Word 0 Lo byte = ‘e’ Word 1 Hi byte = ‘T’ Word 1 Lo byte = ‘N’ Word 2 Hi byte = ‘e’ Word 2 Lo byte = ‘t’ Word 3 Hi byte = ‘5’ Word 3 Lo byte = ‘8’ Word 4 Lo byte = ‘2’

		Word 4 Hi byte = '8' Word 5 Lo byte = 'G' Word 5 Hi byte = '\0' (other words = 0)
0x0020	128 words	SNMP system name (string)
0x00A0	128 words	SNMP system location (string)
0x0120	128 words	SNMP system contact (string)
0x01A0	32 words	SNMP system OID (string)
0x01C0	2 words	System uptime (unsigned long)
0x01C2 to 0x01FF	60 words	Reserved address space
0x0200	2 words	hardware version
0x0202	2 words	S/N information
0x0204	2 words	CPLD version
0x0206	2 words	Boot loader version
0x0208	2 words	Firmware Version Word 0 Hi byte = major Word 0 Lo byte = minor Word 1 Hi byte = reserved Word 1 Lo byte = reserved
0x020A	2 words	Firmware Release Date Firmware was released on 2010-08-11 at 09 o'clock Word 0 = 0x0B09 Word 1 = 0x0A08
0x020C	3 words	Ethernet MAC Address Ex: MAC = 01-02-03-04-05-06 Word 0 Hi byte = 0x01 Word 0 Lo byte = 0x02 Word 1 Hi byte = 0x03 Word 1 Lo byte = 0x04 Word 2 Hi byte = 0x05 Word 2 Lo byte = 0x06
0x020F to 0x2FF	241 words	Reserved address space
0x0300	2 words	IP address Ex: IP = 192.168.10.1 Word 0 Hi byte = 0xC0 Word 0 Lo byte = 0xA8 Word 1 Hi byte = 0x0A Word 1 Lo byte = 0x01
0x0302	2 words	Subnet Mask
0x0304	2 words	Default Gateway
0x0306	2 words	DNS Server
0x0308 to 0x3FF	248 words	Reserved address space (IPv6 or others)
0x0400	1 word	AC1 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0401	1 word	AC2 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0402	1 word	DC1 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0403	1 word	DC2 0x0000:Off 0x0001:On 0xFFFF: unavailable

0x0404 to 0x040F	12 words	Reserved address space
0x0410	1 word	DI1 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0411	1 word	DI2 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0412	1 word	DO1 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0413	1 word	DO2 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0414 to 0x041F	12 words	Reserved address space
0x0420	1 word	RDY 0x0000:Off 0x0001:On
0x0421	1 word	RM 0x0000:Off 0x0001:On
0x0422	1 word	RF 0x0000:Off 0x0001:On
0x0423	1 word	RS
Port Information (32 Ports)		
0x1000 to 0x11FF	16 words	Port Description
0x1200 to 0x121F	1 word	Administrative Status 0x0000: disable 0x0001: enable
0x1220 to 0x123F	1 word	Operating Status 0x0000: disable 0x0001: enable 0xFFFF: unavailable
0x1240 to 0x125F	1 word	Duplex 0x0000: half 0x0001: full 0x0003: auto (half) 0x0004: auto (full) 0x0005: auto 0xFFFF: unavailable
0x1260 to 0x127F	1 word	Speed 0x0001: 10 0x0002: 100 0x0003: 1000 0x0004: 2500 0x0005: 10000 0x0101: auto 10 0x0102: auto 100 0x0103: auto 1000 0x0104: auto 2500 0x0105: auto 10000 0x0100: auto 0xFFFF: unavailable

0x1280 to 0x129F	1 word	Flow Control 0x0000: off 0x0001: on 0xFFFF: unavailable
0x12A0 to 0x12BF	1 word	Default Port VLAN ID 0x0001-0xFFFF
0x12C0 to 0x12DF	1 word	Ingress Filtering 0x0000: disable 0x0001: enable
0x12E0 to 0x12FF	1 word	Acceptable Frame Type 0x0000: all 0x0001: tagged frame only
0x1300 to 0x131F	1 word	Port Security 0x0000: disable 0x0001: enable
0x1320 to 0x133F	1 word	Auto Negotiation 0x0000: disable 0x0001: enable 0xFFFF: unavailable
0x1340 to 0x135F	1 word	Loopback Mode 0x0000: none 0x0001: MAC 0x0002: PHY 0xFFFF: unavailable
0x1360 to 0x137F	1 word	STP Status 0x0000: disabled 0x0001: blocking 0x0002: listening 0x0003: learning 0x0004: forwarding
0x1380 to 0x139F	1 word	Default CoS Value for untagged packets
0x13A0 to 0x13BF	1 word	MDIX 0x0000: disable 0x0001: enable 0x0002: auto 0xFFFF: unavailable
0x13E0 to 0x14FF	288 words	Reserved address space
SFP Information (32 Ports)		
0x1500 to 0x151F	1 word	SFP Type
0x1520 to 0x153F	1 words	Wave length
0x1540 to 0x157F	2 words	Distance
0x1580 to 0x167F	8 words	Vender
0x1680 to 0x17FF	384 words	Reserved address space
SFP DDM Information (32 Ports)		
0x1800 to 0x181F	1 words	Temperature
0x1820 to 0x185F	2 words	Alarm Temperature
0x1860 to 0x187F	1 words	Tx power
0x1880 to 0x18BF	2 words	Warning Tx power
0x18C0 to 0x18DF	1 words	Rx power

0x18E0 to 0x191F	2 words	Warning Rx power
0x1920 to 0x1FFF	1760 words	Reserved address space
Inbound packet information		
0x2000 to 0x203F	2 words	Good Octets
0x2040 to 0x207F	2 words	Bad Octets
0x2080 to 0x20BF	2 words	Unicast
0x20C0 to 0x20FF	2 words	Broadcast
0x2100 to 0x213F	2 words	Multicast
0x2140 to 0x217F	2 words	Pause
0x2180 to 0x21BF	2 words	Undersize
0x21C0 to 0x21FF	2 words	Fragments
0x2200 to 0x223F	2 words	Oversize
0x2240 to 0x227F	2 words	Jabbers
0x2280 to 0x22BF	2 words	Disacrds
0x22C0 to 0x22FF	2 words	Filtered frames
0x2300 to 0x233F	2 words	RxError
0x2340 to 0x237F	2 words	FCSError
0x2380 to 0x23BF	2 words	Collisions
0x23C0 to 0x23FF	2 words	Dropped Frames
0x2400 to 0x243F	2 words	Last Activated SysUpTime
0x2440 to 0x24FF	191 words	Reserved address space
Outbound packet information		
0x2500 to 0x253F	2 words	Good Octets
0x2540 to 0x257F	2 words	Unicast
0x2580 to 0x25BF	2 words	Broadcast
0x25C0 to 0x25FF	2 words	Multicast
0x2600 to 0x263F	2 words	Pause
0x2640 to 0x267F	2 words	Deferred
0x2680 to 0x26BF	2 words	Collisions
0x26C0 to 0x26FF	2 words	SingleCollision
0x2700 to 0x273F	2 words	MultipleCollision
0x2740 to 0x277F	2 words	ExcessiveCollision
0x2780 to	2 words	LateCollision

0x27BF		
0x27C0 to 0x27FF	2 words	Filtered
0x2800 to 0x283F	2 words	FCSError
0x2840 to 0x29FF	447 words	Reserved address space
Number of frames received and transmitted with a length(in octets)		
0x2A00 to 0x2A3F	2 words	64
0x2A40 to 0x2A7F	2 words	65 to 127
0x2A80 to 0x2ABF	2 words	128 to 255
0x2AC0 to 0x2AFF	2 words	256 to 511
0x2B00 to 0x2B3F	2 words	512 to 1023
0x2B40 to 0x2B7F	2 words	1024 to maximum size

Tabela 5-4. Tabela de Registro Modbus TCP

Nota:

O Servidor Modbus TCP retornará 0xFFFF ao Cliente Modbus se dados reservados forem requisitados.

Comandos CLI para Modbus TCP

Característica	Comando e Exemplo
Enable Modbus TCP	Switch(config)# modbus enable
Disable Modbus TCP	Switch(config)# modbus disable
Set Modbus interval time between request	Switch(config)# modbus idle-timeout <200-10000> Timeout vlaue: 200-10000ms Switch(config)# modbus idle-timeout 200 Æ set interval request time out duration to 200ms.
Set modbus TCP master communicate session.	Switch(config)# modbus master <1-20> Max Modbus TCP Master Switch(config)# modbus master 2 Æ set maximum modbus master up to 2; maximum support up to 20 modbus communicate sessions.
Set modbus TCP listening port	Switch(config)# modbus port port Listening Port Switch(config)# modbus port 502; default modbus TCP service port is 502.

Tabela 5-5. Comando CLI para Modbus TCP

6. Glossário

Acesso à mídia	Método usado por todos os nós em uma rede para sincronizar a transmissão de dados e resolver possíveis conflitos em transmissões simultâneas.
Baixar	Informações que são enviadas a um dispositivo/caminho.
Banco de dados	Um grupo de dados organizados em uma tabela.
Barramento	Conjunto de sinais elétricos que são parte de um grupo de lógica com a função de transferência de dados e controle entre diferentes elementos de um subsistema
Baud Rate	Taxa na qual informação bits são transmitidos através de uma rede de comunicação ou interface serial (medido em Bits/segundo, bps)
Bit	Unidade de informação básica, pode ser a nível de lógica 1 ou 0.
Byte	Unidade de informação composta por oito bits.
Canal serial	Interface de unidade que transfere dados serialmente.
CPU	Unidade central de processamento. Ele controla o fluxo de dados, interpreta e executa as instruções do programa bem como monitora os dispositivos do sistema.
Diagnóstico	Procedimentos para detectar e isolar falhas. Também se relaciona com o conjunto de dados usado para tais tarefas e serve para análise e correção ou problemas.
DIODO EMISSOR DE LUZ	Diodo emissor de luz. Tipo de diodo semicondutor que emite luz quando energizado. É usado para feedback visual.
E/S	Consulte a entrada/saída.
Endereço do módulo:	Endereço usado pela CPU para acessar um módulo de e/s específico.
Entrada/saída	Também conhecido como e/s. Dados de entrada ou saída de dispositivos em um sistema. Em CLPs, estes são normalmente os módulos analógicos ou digitais que monitorar ou acionar os dispositivos controlados pelo sistema.
ESD	Descarga eletrostática.
Estação de supervisão	Equipamento conectado a uma rede PLC, com o objetivo de monitorar e controlar as variáveis de processo
Fazer upload	Lendo um programa ou configuração do PLC.
Firmware	O sistema operacional de um CP. Ele controla as funções básicas do PLC e executa os programas de aplicação.
Gateway	Dispositivo para conectar duas redes de comunicação com protocolos diferentes.
Hard-chave	Conector normalmente conectado à porta paralela de um microcomputador para evitar o uso de cópias ilegais de software
Hardware	Equipamento físico usado para processar dados onde normalmente são executados programas (software)
Interface	Normalmente usado para se referir a um dispositivo que adapta-se eletricamente ou logicamente a transferência de sinais entre dois equipamentos.
Kbytes	Unidade de tamanho de memória. Representa 1024 bytes.
Linguagem de programação	Conjunto de regras, convenções e sintaxes utilizados ao escrever um programa.
Menu	Conjunto de opções disponíveis para um programa, eles podem ser selecionados pelo usuário para ativar ou executar uma tarefa específica
Mestre	Dispositivo conectado a uma rede de comunicação, originando todas as solicitações de comando para outras unidades da rede.
Módulo (hardware)	Elemento básico de um sistema com funcionalidade muito específica. Normalmente está conectado ao sistema por conectores e podem ser facilmente substituído.
Módulo (software)	Parte de um programa capaz de realizar uma tarefa específica. Ele pode ser executado independentemente ou em conjunto com outros módulos através de partilha pelos parâmetros de informação.
Nó	Qualquer estação em uma rede com capacidade de se comunicar usando um determinado protocolo.
Operandos	Elementos na qual software instruções de trabalho. Podem representar constantes, variáveis ou conjunto de variáveis.
Padrão	Um valor que é comumente usado como um padrão
Palavra	Unidade de informação composta por 16 bits.
PLC	Veja controlador programável.
Protocolo	Regras de procedimentos e formatos que permitem a recuperação de erro e transmissão de dados entre dispositivos com o uso de sinais de controle
Quadro	Unidade de informação transmitida na rede.
RAM	Memória de acesso aleatório. Memória onde todos os endereços podem ser acessados diretamente e em ordem aleatória na mesma velocidade. É volátil, em outras palavras, o seu conteúdo é apagado quando desligados, a menos que haja uma bateria para manter o seu conteúdo.

Rede de comunicação	Conjunto de dispositivos (nós) interligados por canais de comunicação.
Rede de comunicação mestre-escravo	Rede de comunicação onde a transferência de dados são iniciadas apenas por um nó (o mestre da rede). Os nós restantes da rede (escravos) resposta somente quando solicitada.
RX	Acrônimo usado para indicar a recepção serial.
Software	Programas de computador, procedimentos e regras relacionadas com o funcionamento de um sistema de processamento de dados
Sub-Rede	Segmento de uma rede de comunicação que conecta um grupo de dispositivos (nós) com o objetivo de isolar o tráfego de dados local ou usando diferentes protocolos ou mídia física.
Tag	Nome associado a um operando ou a lógica que identifica seu conteúdo.
Time-out	Máximo pré-estabelecido tempo para uma comunicação para tomar o lugar. Excedidas, repetir os procedimentos são iniciados ou diagnósticos são ativados.
Toggle	Elemento com dois Estados estáveis que se ligam a cada ativação.
TX	Acrônimo usado para indicar transmissão serial.