User Manual
Switch JN4508F-M

Rev. B 07/2016

Cód. Doc.: MU225600

altus

www.altus.com.br

No part of this document may be copied or reproduced in any form without the prior written consent of Altus Sistemas de Automação S.A. who reserves the right to carry out alterations without prior advice.

According to current legislation in Brazil, the Consumer Defense Code, we are giving the following information to clients who use our products, regarding personal safety and premises.

The industrial automation equipment, manufactured by Altus, is strong and reliable due to the stringent quality control it is subjected to. However, any electronic industrial control equipment (programmable controllers, numerical commands, etc.) can damage machines or processes controlled by them when there are defective components and/or when a programming or installation error occurs. This can even put human lives at risk.

The user should consider the possible consequences of the defects and should provide additional external installations for safety reasons. This concern is higher when in initial commissioning and testing.

The equipment manufactured by Altus does not directly expose the environment to hazards, since they do not issue any kind of pollutant during their use. However, concerning the disposal of equipment, it is important to point out that built-in electronics may contain materials which are harmful to nature when improperly discarded. Therefore, it is recommended that whenever discarding this type of product, it should be forwarded to recycling plants, which guarantee proper waste management.

It is essential to read and understand the product documentation, such as manuals and technical characteristics before its installation or use.

The examples and figures presented in this document are solely for illustrative purposes. Due to possible upgrades and improvements that the products may present, Altus assumes no responsibility for the use of these examples and figures in real applications. They should only be used to assist user trainings and improve experience with the products and their features.

Altus warrants its equipment as described in General Conditions of Supply, attached to the commercial proposals.

Altus guarantees that their equipment works in accordance with the clear instructions contained in their manuals and/or technical characteristics, not guaranteeing the success of any particular type of application of the equipment.

Altus does not acknowledge any other guarantee, directly or implied, mainly when end customers are dealing with third-party suppliers.

The requests for additional information about the supply, equipment features and/or any other Altus services must be made in writing form. Altus is not responsible for supplying information about its equipment without formal request.

COPYRIGHTS

Nexto, Ponto Series, MasterTool, Grano and WebPLC are the registered trademarks of Altus Sistemas de Automação S.A.

Windows, *Windows NT* and *Windows Vista* are registered trademarks of Microsoft Corporation.

Table of Contents

1. Introduction

The JN4508F-M is an industrial managed Fast Ethernet switch equipped with 6 ports 10/100 Mbps ports RJ45 plus 2 100Mbps Fiber uplink ports. Combined the outstanding L2 management features along with the LLDP and high system reliability, including MSR and MSTP network redundancy technologies, for ensuring real-time and high quality connectivity in various networking applications.

The JN4508F-M adopted 32Gbps switch fabric to provide real time non-blocking transmission performance for satisfying the needs of high bandwidth data transmission requiring applications while ensuring traffic switching without data loss. Besides, the new system design includes a hardware based watchdog timer for keeping the operating system live. It also provides power redundancy with wide range 10 to 60 Vdc inputs for ensuring the power continuity in the system.

With a ruggedized design with IP31 enclosure, JN4508F-M provide highly reliable and secure data transmission under severe industrial environments To build a smart, cost-efficient industrial Ethernet infrastructure, JN4508F-M is the best choice.

Innovative Features

The JN4508F-M has the following features:

- 32Gbps Non-Blocking, 8K MAC address table
- Multiple Super Ring (recovery time < 5 ms), Rapid Dual Homing, Multiple Ring, and MSTP / RSTP
- IEEE 1588 Precision Time Protocol for precise time synchronization
- VLAN, Private VLAN, QinQ, GVRP, QoS, IGMP Snooping V1/V2/V3, Rate Control, Port Trunking, LACP, Online Multi-Port Mirroring
- IEEE 802.1AB LLDP and JetView Pro NMS for auto-topology and group management
- Supports SNMP, Multiple Language Web UI, Telnet In-Band, Serial Out-Band Management
- Supports MODBUS TCP/Client function for HMI system
- Embedded Hardware Watchdog for System Auto Rescue
- Dual 10 to 60Vdc Power Inputs with Redundancy
- Software configurable Alarm Output

Package Checklist

Integrant Itens

The JN4508F-M includes the following items:

- One switch- JN4508F-M
- One DIN-Rail clip
- One RS-232 DB-9 to RJ45 console cable

If any of the above items are missing or damaged, please contact your local sales representative.

Documents Related to this Manual

For additional information about JN4508F-M, you can examine other specific documents in addition to this one. These documents are available in its last review on www.altus.com.br.

General Regards on ALTUS Documentation

Each product has a document called Technical Characteristics (CT), where there are the characteristics for the product in question. Additionally, the product may have User Manuals (manual’s codes, if applicable, are always mentioned at CTs from the respective modules).

Support Documentation

It is advisable to consult the following documents as a source of additional information:

Code	Description	Language
CE125000	Connect Series – Technical Characteristics	English
CT125000	Série Connect – Características Técnicas	Portuguese
CS125000	Serie Connect – Especificaciones y Configuraciones	Spanish

Visual Inspection

Prior to installation, we recommend performing a careful visual inspection of equipment, by checking if there is damage caused by shipping. Make sure all components of your order are in perfect condition. In case of defects, inform the transportation company and the nearest Altus representative or distributor.

CAUTION: Before removing modules from the package, it is important to discharge eventual static potentials accrued in the body. For this, touch (with nude hands) in a metallic surface grounded before modules handling. Such procedure ensures that the levels of static electricity supported by the module will not be overcome.

It is important to record the serial number of each item received, as well as software revisions, if any. This information will be necessary if you need to contact Altus Technical Support.

Technical Support

To contact Altus Technical Support in São Leopoldo, RS, call +55 51 3589-9500. To find the existent centers of Altus Technical Support in other locations, see our website (www.altus.com.br) or send an email to altus@altus.com.br.

If the equipment is already installed, please have the following information when requesting assistance:

- Models of equipment used and the configuration of installed system
- Serial number
- Equipment review and executive software version, listed on the label affixed to the product side

Warning Messages Used in this Manual

In this manual, warning messages will present the following formats and meanings:

DANGER:
Relates potential causes that if not noted, generate damages to physical integrity and health, property, environment and production loss.

CAUTION:
Relates configuration details, application and installation that shall be followed to avoid condition that could lead to system fail, and its related consequences.

ATTENTION:
Indicate important details to configuration, application or installation to obtain the maximum operation performance from the system.

2. Hardware Installation

Hardware Introduction

Dimensions

JN4508F-M Industrial 6-port plus 2 100Mbps Fiber Managed Fast Ethernet Switch dimensions:

55mm W x 149mm H x 131.2mm D /with DIN Rail Clip

55mm W x 149mm H x 120.6mm D /without DIN Rail Clip

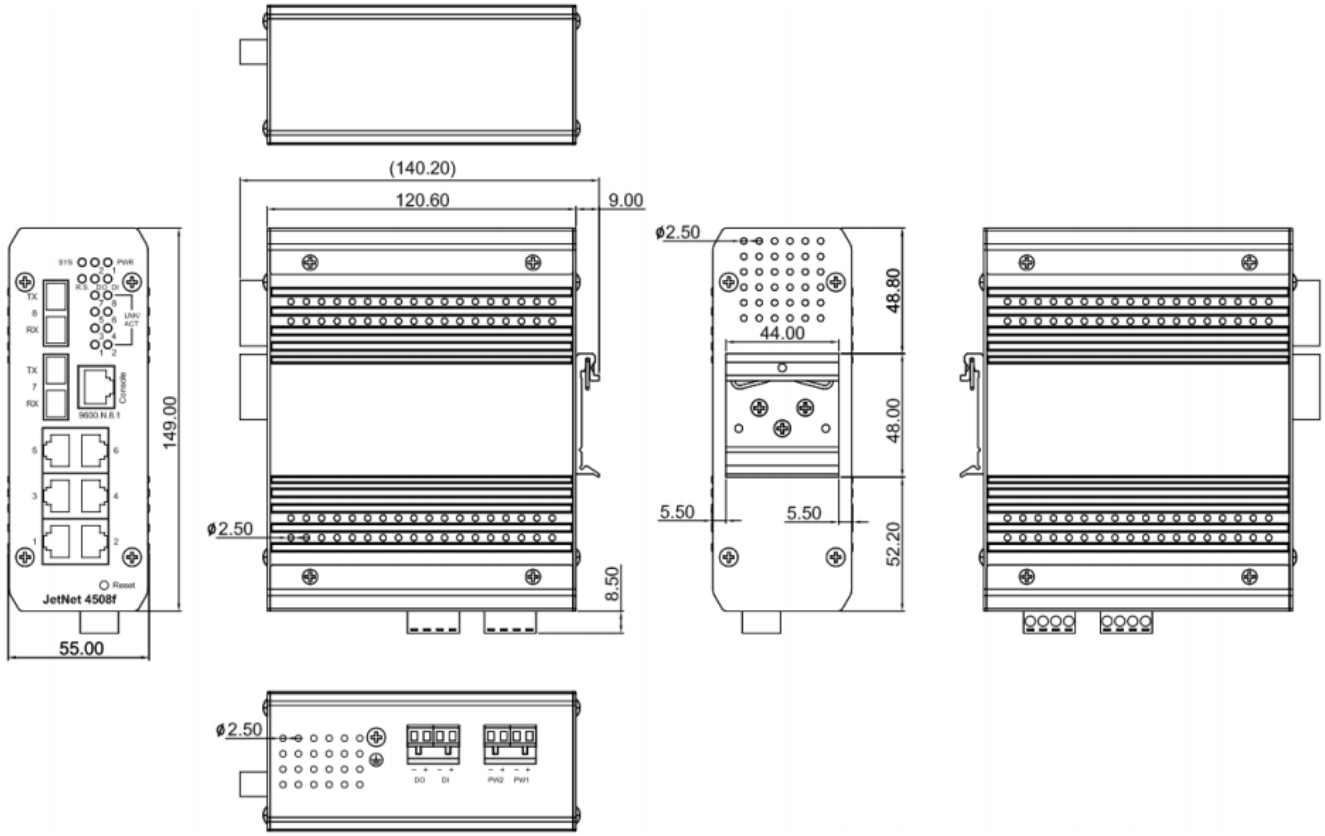


Figure 2-1. JN4508F-M Complete View

Front Panel Layout

The front panel of JN4508F-M includes 6 10/100Mbps Fast Ethernet RJ45 ports (port 1 to 6), 2 Fast Ethernet fiber ports (port 7, 8), one RS232 serial console in RJ45 type connector, one reset button and several of LED indicators for the system and port diagnostic. The JN4508F-M front panel shows as following diagram.

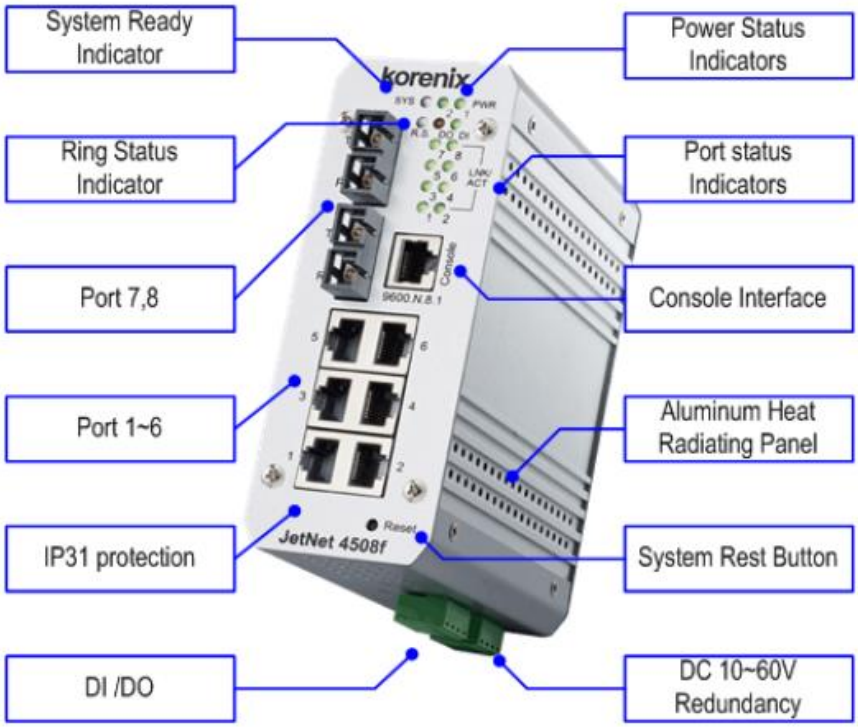


Figure 2-2. JN4508F-M Panel

The LED function is described as following table:

LED	Funtion	Behaviors
Power 1, 2	Indicates the power inputs status	On: the input connector is on applying power
SYS	Indicates the system operating status	On: System is ready to operating
DI	Indicates the digital input status	On: High level signal is applied
DO	Indicates the digital output (Relay output) status	Red On: The output is formed close circuit
R.S.	Indicates the ring operating status	Normal (Green on), Abnormal (Yellow on), wrong ring port is connected (Green blinking), one of device's ring path is broken (Yellow blinking)
Link/active	Indicated the traffic status and link status	On: port is linked with partner Blinking: the port is on transmitting or receiving data

Table 2-1. LED Function Description

Bottom View

The bottom view of the JN4508F-M consists of two terminal block connectors with two Vdc power inputs, one Digital Input (DI), one Relay Output (DO) and one chassis grounding screw

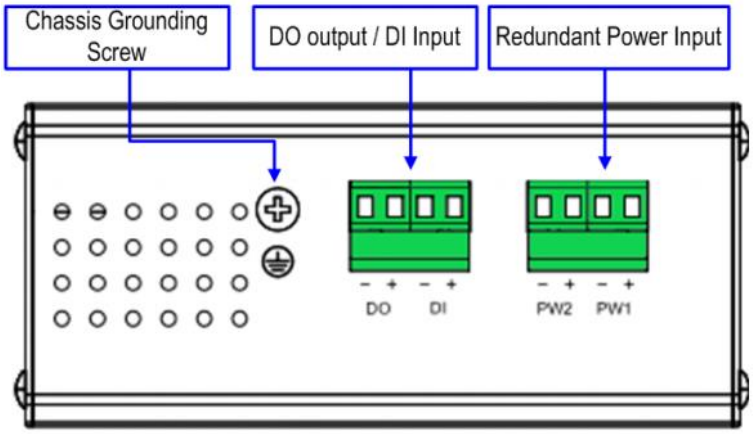


Figure 2-3. JN4508F-M Bottom View

Wiring the Power Inputs

Follow below steps to wire JN4508F-M redundant Vdc power inputs.

1. Insert positive and negative wires into V+ and V- contacts respectively of the terminal block connector.
2. Tighten the wire-clamp screws to prevent Vdc wires from being loosened.
3. Power 1 and Power 2 support power redundancy and polarity reverse protect function. That means with wrong polarity, the system won't work.
4. Positive and negative power system inputs are both accepted, but Power 1 and Power 2 must apply with same mode as following figures.

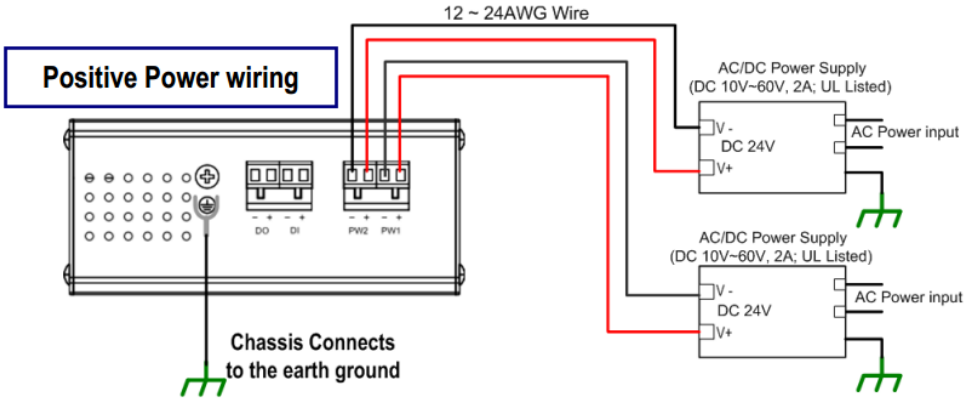


Figure 2-4. JN4508F-M Positive Power Wiring

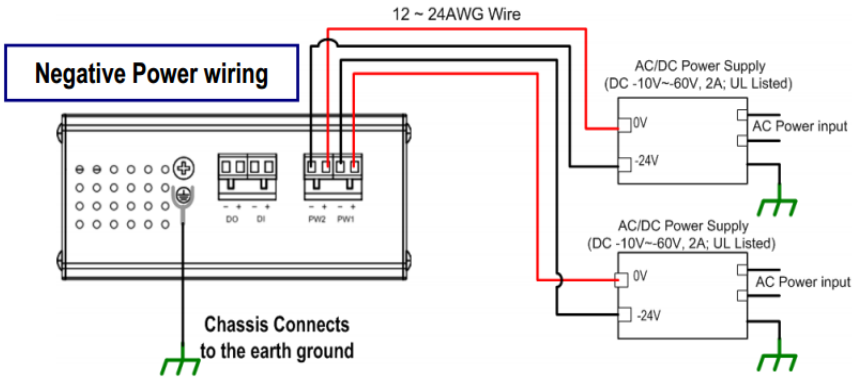


Figure 2-5. JN4508F-M Negative Power Wiring

Note:

It is a good practice to turn off input and load power, and to unplug power terminal block before making wire connections. Otherwise, your screwdriver blade can inadvertently short your terminal connections to the grounded enclosure.

The range of the suitable electric wire is from 12 to 24 AWG.

If the 2 power inputs are connected, JN4508F-M Switch will be powered from the highest connected voltage. The unit will alarm for loss of power, either PWR1 or PWR2 and auto backup with each other.

Uses the UL Listed Power supply with output Rating 10 to 60 Vdc, minimum 2 A. Here, we recommended use 24 Vdc as the operating voltage.

Once the system powering on, the system diagnostic LEDs will activate as the sequence shown in the following table:

Indicators	Stage 1	Stage 2	Stage 3	Stage 4	Stage 5	Stage 6
Power LED	On	On	On	On	On	On
DI	Off	On	Off	Off	Off	Off
DO	Off	Off	On	Off	Off	Off
R.S.	Off	Off	Off	On	Off	Off
SYS	Off	Off	Off	Off	Off	On
Description	**Power On**	**Ex. Booter**	**Ld. Firmware**	**Ex. Firmware**	**System Booting**	**System Ready**

Table 2-2. LED Power Sequence Diagnostic

By those LED indicators, we can know the exactly stage is performed during the system power on.

Wiring Digital Input

The JN4508F-M provides one digital input. It allows users to connect the termination units' digital output and manage/monitor the status of the connected unit. The Digital Input pin can be pulled high or low; thus the connected equipments can actively drive these pins high or low. The embedded software UI allows you to read and set the value to the connected device.

The power input voltage of logic low is 0 to 10 Vdc. Logic high is 11 to 30 Vdc.

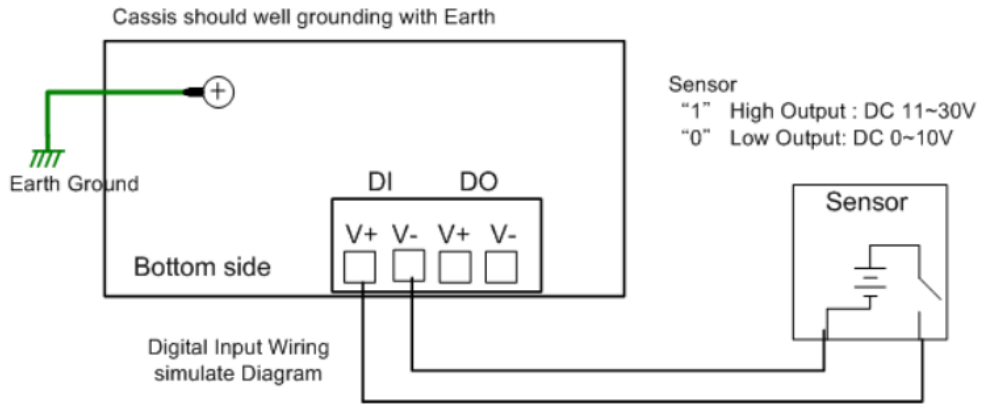


Figure 2-6. Digital Input Wiring

Wiring Relay Output

JN4508F-M provide one Digital output, also known as Dry Relay Output. The relay contacts are energized (open) for normal operation and will close for fault conditions. The fault conditions

include power failure, Ethernet port link break or other pre-defined events which can be configured in JN4508F-M Web user interface.

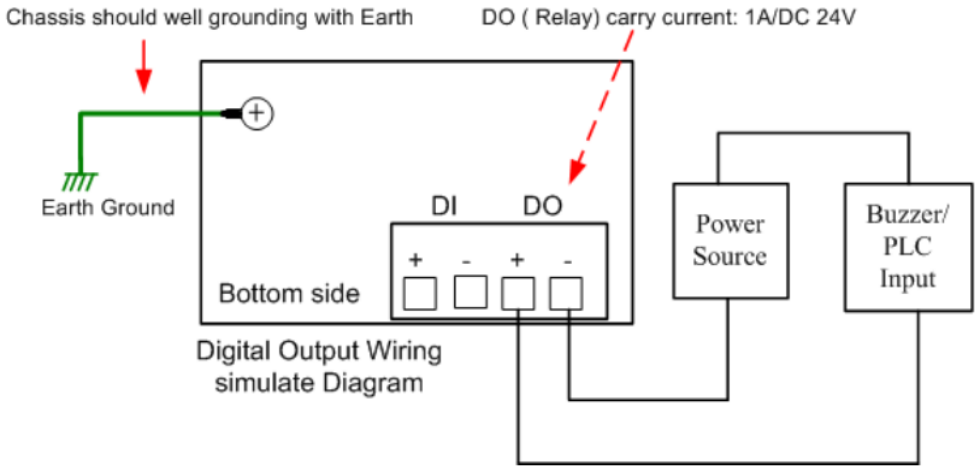


Figure 2-7. JN4508F-M Wiring Relay Output

Wiring Earth Ground

To ensure the system will not be damaged by noise or any electrical shock, it is suggested to make exact connection with JN4508F-M with Earth Grounding. On the bottom side of JN4508F-M, there is one earth ground screw. Loosen the earth ground screw by screw drive; then tighten the screw after earth ground wire is well connected. Without the exact system chassis grounding, the communication may interfered by the external noise, such as lighting, fast electrical filed transient or electrostatic discharge.

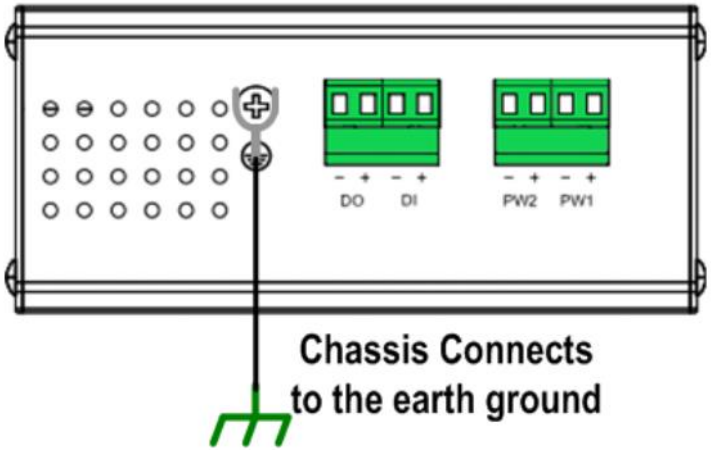


Figure 2-8. JN4508F-M Wiring Earth Ground

Wiring Fast Ethernet RJ45 Ports

The JN4508F-M switch adopts several of RJ45 connectors which support 10/100Base-TX with link speed auto negotiation and auto MDI/MDI-X functions. All the RJ45 ports will auto-detect the signal from connected devices to negotiate the link speed and duplex mode. Auto MDI/MDIX allows users to connect another switch, hub or workstation without changing straight through or crossover cable.

Note:

That crossover cables simply cross-connect the transmit lines at each end to the received lines at the opposite end.

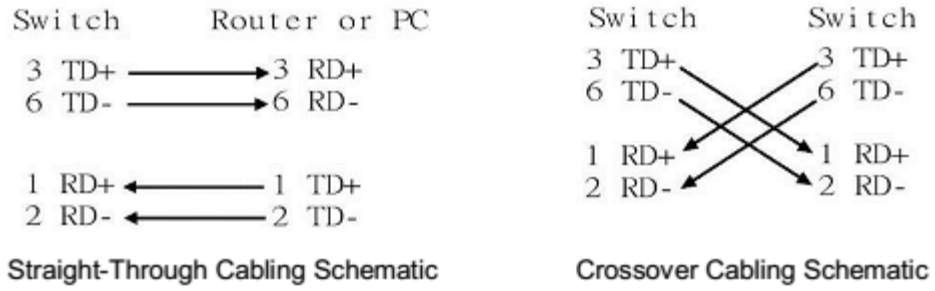


Figure 2-9. Wiring 10/100 Base Tx Fast Ethernet

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

Table 2-3. Ethernet Port Wiring

Connect one side of an Ethernet cable into any switch port and connect the other side to your attached device. The LNK LED will light up when the cable is correctly connected. Refer to the LED Indicators section for descriptions of each LED indicator. Always make sure that the cables between the switches and attached devices (e.g. switch, hub, or workstation) are less than 100m (328 feet).

The supported cable types listed as below:

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

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

Wiring Fast Ethernet Fiber port

JN4508F-M equipped 2 ports fiber which compliance with IEEE 802.3 100Base-FX standard and supports multi-mode or single mode fiber cable. The fiber connector supports SC type connector. To ensure the quality of connection, the specifications of cable and fiber port must matched; with wrong fiber cable may caused the communication does not work well. The following information is the specification includes suitable cable and the characteristics of fiber port.

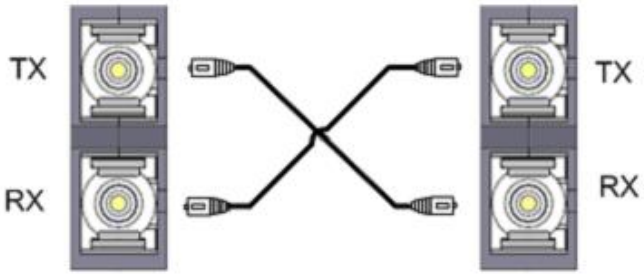


Figure 2-10. Wiring the Fiber Port of JN4508F-M

Wiring RS-232 Console Cable

There is one RS-232 DB9 to RJ45 cable shipped with the box. Connects the DB-9 connector to the COM port of your PC, open Terminal tool and configure the serial communication parameter to 9600, N, 8, 1. (Baud Rate: 9600bps / Parity: None / Data length: 8bits / Stop Bit: 1) Then you can access CLI interface by console able.

Note:

If you lost the cable, please contact with your sales or follow the pin assignment to buy a new one. The Pin assignment spec is listed following.

RJ45 Pln	DB-9 Pin	Description
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

Table 2-4. Wiring Console Cables

DIN-Rail Mounting Installation

The DIN-Rail clip is already screwed tighten on the rear side of JN4508F-M when shipping. If the DIN-Rail clip is not screwed on the JN4508F-M, please contact your distributor to get the DIN rail clip set. The DIN rail clip supports EN50022 standard. In the diagram following includes the dimension of EN50022 DIN rail for your refer.

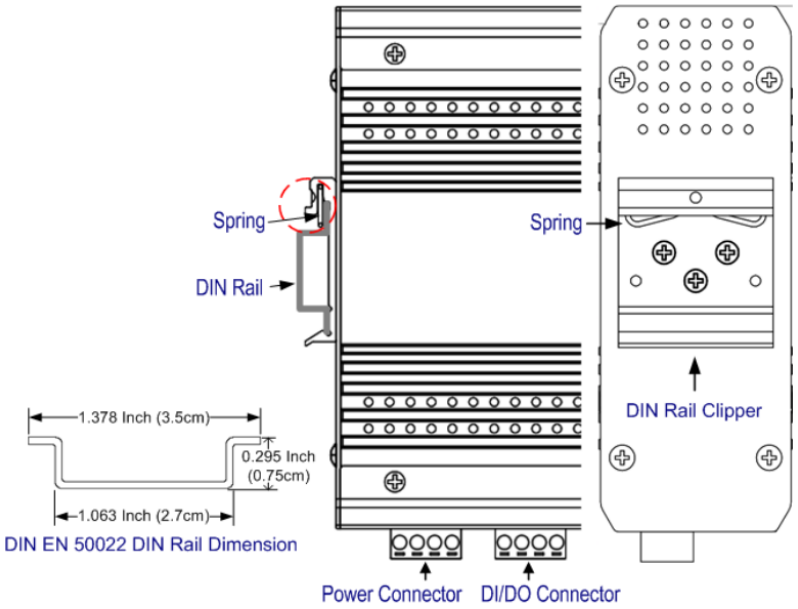


Figure 2-11. Mounting Installation Example

Follow the steps below to mount JN4508F-M Managed Switch to the DIN-Rail track:

1. First, insert the DIN-Rail track upper side into the upper end of DIN-Rail clip.
2. Lightly push the bottom of DIN-Rail clip into the track.
3. Check if DIN-Rail clip is tightly attached on the track.
4. To remove JN4508F-M from the track, reverse the steps above.

Note:

The DIN Rail should compliance with DIN EN50022 standard. Using wrong DIN rail may cause system install unsafe

3. Preparation for Management

The JN4508F-M Industrial Managed Fast Ethernet Switch provides both in-band and out-band configurations methods.

With out-band management; it is possible configure the switch via RS232 console cable if the admin PC is not in the network or in case of lost network connection. Out-band management is not affected by network performance.

In-band management allows to remotely managing the switch via the network. It is possible choose Telnet or Web-based management. Just need to know the device's IP address and connect remotely to its embedded HTTP web pages or Telnet console.

Preparation for Serial Console

In the JN4508F-M package, has included one RS-232 DB-9 to RJ45 console cable. Attach the RS-232 DB-9 connector to PC COM port, and then connect the RJ45 to the console port of JN4508F-M. If the cable is not available, please follow the console cable Pin assignment to find one.

1. Go to Start -> Program -> Accessories -> Communication -> Hyper Terminal
2. Give a name to the new console connection
3. Choose the serial communication port
4. Select correct serial settings. The serial settings for the JN4508F-M are
5. Baud Rate: 9600 / Parity Check: None / Data Bit: 8 / Stop Bit: 1
6. After connected, you will see a switch login request
7. Login to the switch. The default username and password are admin

Preparation for Web Interface

The JN4508F-M provides HTTP Web Interface and Secure HTTPS Web Interface for web management.

Web Interface

The web management page uses JavaScript. This allows you to use a standard Web browser to configure the switch from anywhere while connected to the network.

Before you attempt to use the embedded web interface to manage switch operation, verify that JN4508F-M Industrial Ethernet Switch is properly installed on your network and that every PC on the network can access the switch via Web browser.

1. Verify that the network interface card (NIC) is operational, and the operating system supports TCP/IP protocol
2. Wire the Vdc power to the switch and connect the switch to the computer
3. Make sure that the switch default IP address is 192.168.10.1
4. Change the computer IP address to 192.168.10.2 or another IP address in the 192.168.10.x subnet (Network Mask: 255.255.255.0)
5. Switch to DOS command mode and ping 192.168.10.1 to verify a normal response time
6. Launch a web browser (Internet Explorer or Mozilla Firefox) on PC
7. Type http://192.168.10.1 (or the IP address of the switch) into the Web address window. Press *Enter*
8. The login screen will appear next
9. Key in the username and password. The default username and password are *admin*
10. Select language type, the default is English. This feature is available from firmware v1.1.

Figure 3-1. Switch Manager Screen

Click *Enter* or *OK*. The welcome page of the web-based management interface will now appear.

Once you enter the web-based management interface, you can change the JN4508F-M's IP address to fit your network environment.

Notes:

Internet Explorer Version 5.0 or later does not allow Java applets to open sockets by default. Users must directly modify the browser settings to selectively enable Java applets in order to use network ports.

The Web UI connection session of JN4508F-M will be logged out automatically if any input is inserted after 30 seconds. After logged out, should re-login and key in correct user name and password again.

Secured Web Interface

The web management page also provides a secure HTTPS login. All the configuration commands will be secure and will be hard for the hackers to sniff the login password and configuration commands.

Launch the web browser and Login.

1. Launch a web browser (Internet Explorer or Mozilla Firefox) on your PC
2. Type *https://192.168.10.1* (or the IP address of the switch) and press *Enter*
3. A popup screen will appear and request you to trust the secure HTTPS connection distributed by JN4508F-M. Press Yes

Figure 3-2. Warning Security Screen

4. The login screen will appear next

Figure 3-3. Switch Manager Secure Connection Screen

5. Key in the username and password. The default username and password are *admin*
6. Click *Enter* or *OK*. The welcome page of the web-based management interface will now appear
7. Once you enter the web-based management interface, all the commands you see will be the same as what appeared through HTTP login.

Preparation for Telnet Console

Telnet

The JN4508F-M supports Telnet console. It is possible connect to the switch through Telnet and the command lines are the same as the RS232 console port. Below are the steps to open Telnet connection to the switch.

Go to *Start -> Run -> cmd*. Press *Enter*

Type Telnet 192.168.10.1 (or the IP address of the switch). Press *Enter*

SSH (Secure Shell)

The JN4508F-M also supports SSH console. It is possible remotely connect to the switch by command line interface. The SSH connection can secure all the configuration commands you send to the switch.

SSH is a client/server architecture in which JN4508F-M is the SSH server. To make a SSH connection with the switch, it is necessary download the SSH client tool first.

SSH Client

There are many free SSH clients, they can be find on the internet. For example, PuTTY is a free and popular Telnet/SSH client. We will use this tool to demonstrate how to login to the JN4508F-M through SSH.

Note:

PuTTY, Copyright 1997-2006 Simon Tatham.

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

Open SSH Client/PuTTY

In Session configuration, enter the Host Name (IP Address of your JN4508f -m) and Port number (default = 22). Choose the SSH protocol. Then click on *Open* to start the SSH session console.

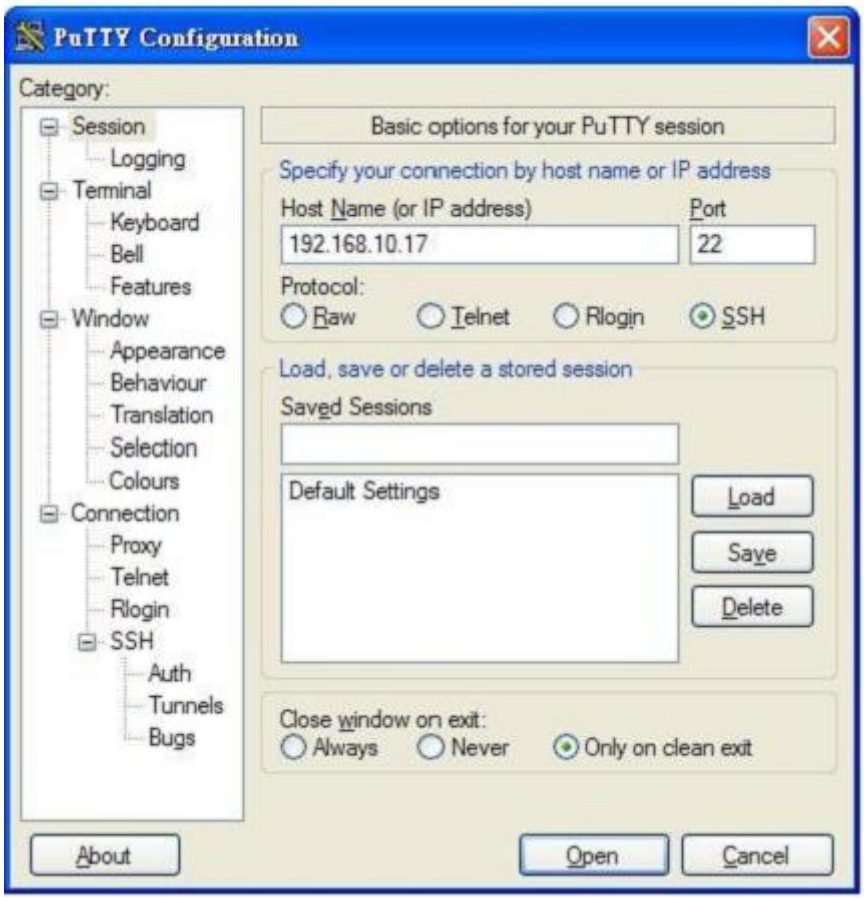


Figure 3-4. PuTTy Interface

After clicking on *Open*, you will see the cipher information in the popup screen. Press *Yes* to accept the Security Alert.

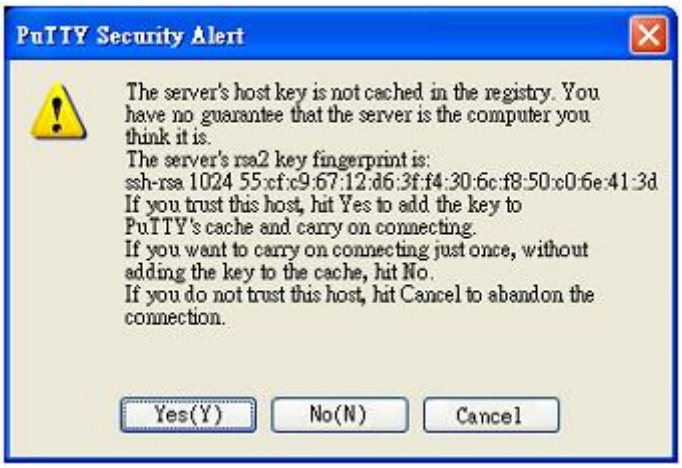


Figure 3-5. PuTTY Security Alert

After few seconds, the SSH connection to JN4508f -m will open.

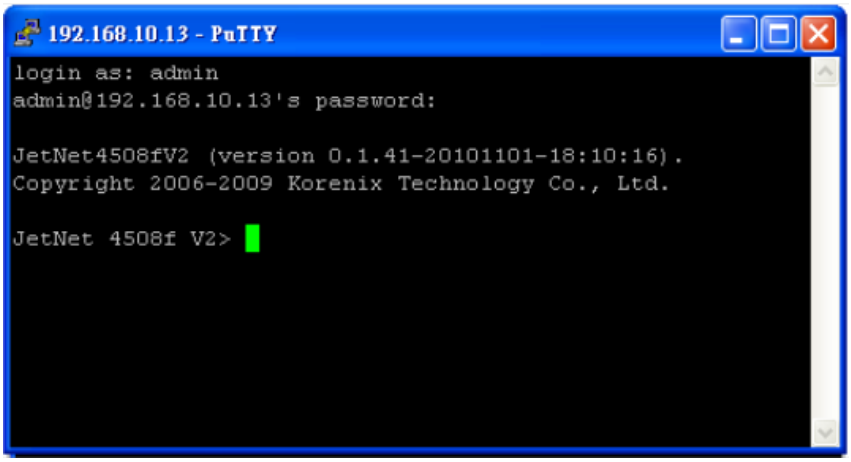


Figure 3-6. JN4508F-M SSH

Type the login name and password. The default login name and password are *admin* / *admin*.

All the commands in SSH are the same as the CLI commands via RS232 console. The next chapter will introduce in detail how to use the command line to configure the switch.

4. Feature Configuration

This chapter explains how to configure the JN4508f -m software and its features.

Command Line Interface Introduction

The Command Line Interface (CLI) is the user interface of the switch's embedded software system. It is possible to view the system information, see the status, configure the switch and receive a response back from the system by keying in a command.

There are different command modes. Each command mode has its own access ability, its own available command lines, and its own different command lines to enter and exit. These modes are User EXEC, Privileged EXEC, Global Configuration, and (Port/VLAN) Interface Configuration modes.

User EXEC mode

As long as you login to the switch through CLI, you will be in the User EXEC mode. You can ping, telnet remote device, and show some basic information.

Types *enable* to enter the next mode, and *exit* to logout. *?* to see the command list.

Switch>	
enable	Turn on privileged mode command.
exit	Exit current mode and down to previous mode.
list	Print command list.
ping	Send echo messages.
quit	Exit current mode and down to previous mode.
show	Show running system information.
telnet	Open a telnet connection.
traceroute	Trace route to destination.

Table 4-1. Command List

Privileged EXEC mode

Type enable in the User EXEC mode to enter the Privileged EXEC mode. In this mode, the system allows you to view current configurations, reset to default, reload the switch, show the system's information, save a configuration, and enter the global configuration mode.

Type *configure terminal* to enter the next mode or *exit* to leave, to see a list of available command by types *?*. Table 4-2 diagram shows the commands.

Switch#	
archive	manage archive files
clear	Reset functions
clock	Configure time-of-day clock
configure	Configuration from vty interface
copy	Copy from one file to another
debug	Debugging functions (see also 'undebug')
disable	Turn off privileged mode command
end	End current mode and change to enable mode
exit	Exit current mode and down to previous mode
list	Print command list
more	Display the contents of a file
no	Negate a command or set its defaults

ping	Send echo messages
quit	Exit current mode and down to previous mode
reboot	Reboot system
reload	copy a default-config file to replace the current one
show	Show running system information
telnet	Open a telnet connection
terminal	Set terminal line parameters
traceroute	Trace route to destination
write	Write running configuration to memory, network, or terminal

Table 4-2. Privileged Command List

Global Configuration mode

Type *configure terminal* in privileged EXEC mode. You can then enter the global configuration mode. In global configuration mode, you can configure all the features that the system provides.

Type *interface IFNAME/VLAN* to enter interface configuration mode and *exit* to leave, or *?* for command list.

Available commands for global configuration mode are shown in Table 4-3.

Switch# configure terminal Switch(config)#	
access-list	Add an access list entry
administrator	Administrator account setting
arp	Set a static ARP entry
clock	Configure time-of-day clock
default	Set a command to its defaults
end	End current mode and change to enable mode
exit	Exit current mode and down to previous mode
gvrp	GARP VLAN Registration Protocol
hostname	Set system's network name
interface	Select an interface to configure
ip	IP information
list	Print command list
log	Logging control
mac	Global MAC configuration subcommands
mac-address-table	mac address table
mirror	Port mirroring
no	Negate a command or set its defaults
ntp	Configure NTP
password	Assign the terminal connection password
Qos	Quality of Service (QoS)
relay	relay output type information
smtp-server	SMTP server configuration
snmp-tree	SNMP server
spanning-tree	Spanning tree algorithm
super-ring	Super-ring protocol
trunk	Trunk group configuration
vlan	Virtual LAN
warning-event	Warning event selection
write-config	Specify config files to write to

Table 4-3. Global Configuration Commands List

(Port) Interface Configuration

Type *interface IFNAME* in global configuration mode. You can then enter interface configuration mode. In this mode, you can configure port settings.

The port interface name for fast Ethernet port 1~8 are fa1~fa8. You can type the interface name accordingly when you want to enter a specific interface configuration mode.

You can type *exit* to leave or *?* for a list of available commands.

Table 4-4 shows the available commands for port interface configuration mode.

Switch(config)# interface fa2 Switch(config-if)#	
acceptable	Configure 802.1Q acceptable frame types of a port
auto-negotiation	Enables auto-negotiation state of a given port
Description	Interface specific description
duplex	Specifies the duplex mode of operation for a port
end	End current mode and change to enable mode
exit	Exit current mode and down to previous mode
flowcontrol	Sets the flow-control value for an interface
garp	General Attribute Registration Protocol
ingress	802.1Q ingress filtering features
lacp	Link Aggregation Control Protocol
list	Print command list
loopback	Specifies the loopback mode of operation for a port
mac	MAC interface commands
mdix	Enables mdix state of a given port
no	Negate a command or set its defaults
poe	Configure power over Ethernet
qos	Quality of Service (QoS)
quit	Exit current mode and down to previous mode
rate-limit	Rate limit configuration
shutdown	Shutdown the selected interface
spanning-tree	the spanning-tree protocol
speed	Specifies the speed of a Fast Ethernet port
switchport	Set switching mode characteristics

Table 4-4. Port Interface Commands List

(VLAN) Interface Configuration

Type *interface VLAN VLAN-ID* in global configuration mode. You can then enter the VLAN interface configuration mode. In this mode, you can configure the settings for a specific VLAN.

The VLAN interface name for VLAN 1 is VLAN 1; VLAN 2 is VLAN 2.

You can type *exit* to leave or *?* for a list of available commands.

Available commands for the VLAN interface configuration mode appears in Table 4-5.

Switch(config)# interface vlan 1 JN4508F-M (config-if)#	
Description	Interface specific description
end	End current mode and change to enable mode
exit	Exit current mode and down to previous mode Interface
ip	Internet Protocol config commands
list	Print command list
no	Negate a command or set its defaults

quit	Exit current mode and down to previous mode
shutdown	Shutdown the selected interface

Table 4-5. (VLAN) Interface Commands List

The Table 4-6 is a summary of command modes.

Command Mode	Main Function	Enter and Exit Method	Prompt
User EXEC	This is the first level of access Users can ping, telnet remote device, and show basic information	Enter: Type **login** to login Exit: Type **exit** to logout Next mode: Type **enable** to enter privileged EXEC mode.	Switch>
Privileged EXEC	In this mode, the system allows you to view current configuration, reset to default, reload the switch, show the system's information, save a configuration, and enter global configuration mode.	Enter: Type **enable** in User EXEC mode. Exec: Type **disable** to exit to user EXEC mode. Type **exit** to logout Next Mode: Type **configure terminal** to enter global configuration command.	Switch#
Global configuration	In global configuration mode, you can configure all the features that the system provides	Enter: Type **configure terminal** in privileged EXEC mode Exit: Type **exit** or **end** or press **Ctrl-Z** to exit. Next mode: Type **interface IFNAME/ VLAN VID** to enter interface configuration mode.	Switch(config)#
Port Interface configuration	In this mode, you can configure port-related settings.	Enter: Type **interface IFNAME** in global configuration mode. Exit: Type **exit** or **Ctrl+Z** to global configuration mode. Type **end** to privileged EXEC mode.	Switch(config-if)#
VLAN Interface Configuration	In this mode, you can configure settings for specific VLAN.	Enter: Type **interface VLAN VID** in global configuration mode. Exit: Type **exit** or **Ctrl+Z** to global configuration mode. Type **end** to privileged EXEC mode.	Switch(config-vlan)#

Table 4-6. Command Nodes List

Here are some useful commands for you to see all or specific commands available to you. Save time and avoid typing errors.

? Shows all the available commands in the mode you are currently in. It also shows you the next command you can/should type.

Switch(config)# interface (?)	
IFNAME	Interface's name
vlan	Select a vlan to configure

Table 4-7. Useful Commands List 1

(Character) *?* Shows all the available commands for what you input as *Character*.

Switch(config)# a?	
access-list	Add an access list entry
administrator	Administrator account setting
arp	Set a static ARP entry

Table 4-8. Useful Commands List 2

Tab Key Helps you input commands quicker. If there is only one available command, hitting the tab key can help you automatically generate the command.

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

Ctrl + C: Stops an unfinished command.

Ctrl + S: Locks the screen of the terminal. You will not be able to input a command.

Ctrl + Q: Unlocks a locked screen.

Ctrl + Z: Exits configuration mode.

An alert message appears when multiple users try to configure the switch. If the administrator is in configuration mode, then Web users will not be able to change the settings. JN4508F-M only allows one administrator at a time to configure the switch.

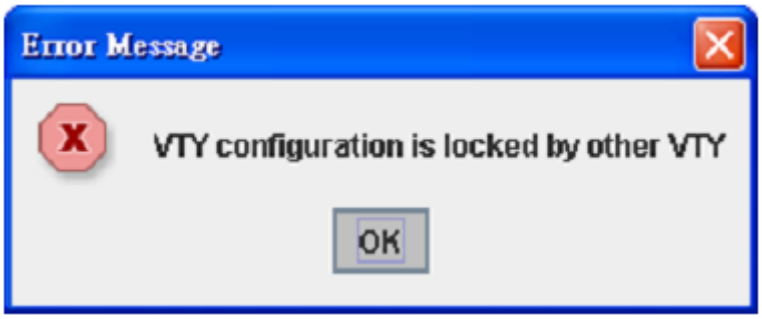


Figure 4-1. Alert Message for Multiple Users Trying to Configure the Switch

Basic Settings

This section provides you with instructions on how to configure switch information, set the IP address, and configure the username and password of the system. It also allows you to upgrade the firmware, backup and restore a configuration, reload the system to factory default, and reboot the system.

Switch Setting

You can assign a System name, Location, Contact and view the system information.

The Figure 4-2 is the Web UI for Switch Setting.

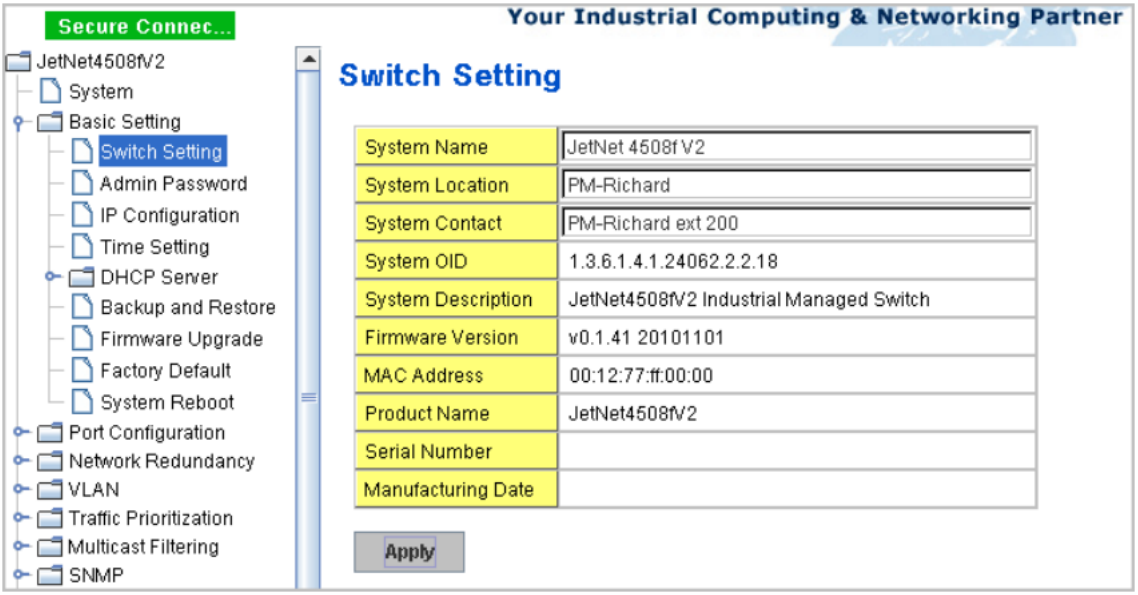


Figure 4-2. Switch Setting Interface

System Name: Assign a name to the device. You can input up to 64 characters. After you configure the name, the CLI system will select the first 12 characters as the name for the CLI system.

System Location: Specify the switch's physical location. You can input up to 64 characters.

System Contact: Specify contact people. Enter the name, e-mail address or other information about the administrator. You can input up to 64 characters.

System OID: Set the SNMP object ID of the switch. You can follow the path to find its private MIB in the MIB browser. Note: When you attempt to view a private MIB, you should compile private MIB files into your MIB browser first.

System Description: The real product model name of this product.

Firmware Version: Display the firmware version installed on this device.

MAC Address: Display the unique hardware address (MAC address) assigned by the manufacturer.

Product Name: Display the Switch's model name.

Serial Number: Display the Switch's serial number.

Manufacture Date: Display the Switch's production date.

Once you have finished the configuration, click the *Apply* button to apply your settings.

Note:

Always remember to select *Save* to save your settings. Otherwise, the settings you made will be lost when the switch is powered off.

Admin Password

You can change the username and password to enhance security. The Figure 4-3 is the Web UI for Admin Password.

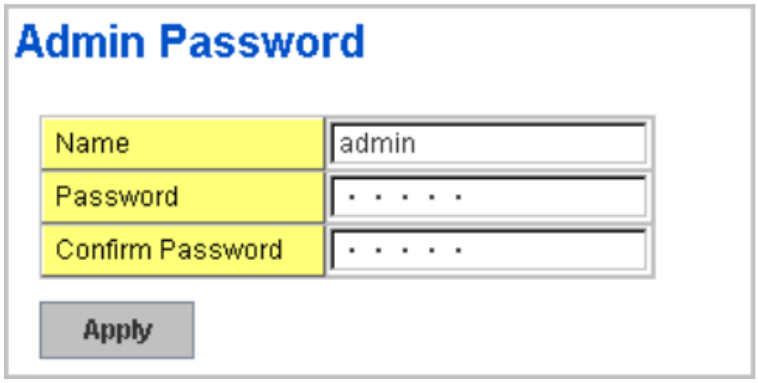


Figure 4-3. Changing Admin Password

Name: Key in a new username. The default setting is *admin.*

Password: Key in a new password. The default setting is *admin.*

Confirm Password: Re-enter the new password to confirm it.

Once you finish configuring the settings, click the *Apply* button to apply your configuration.

The Figure 4-4 is the popup alert window when the incorrect username is entered.

Figure 4-4. Alert of Wrong Username

IP Configuration

This function allows users to configure the switch's IP address settings.

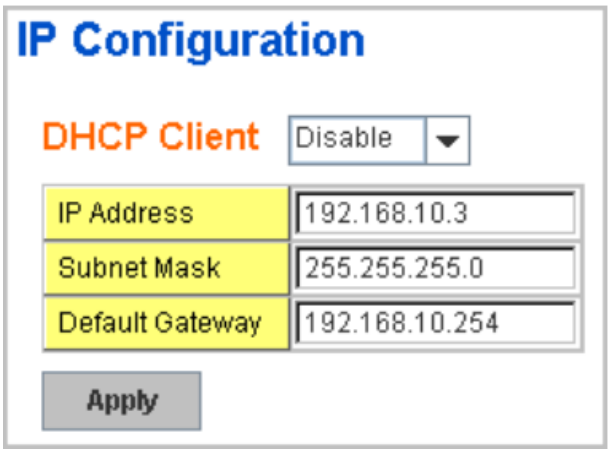


Figure 4-5. IP Configuration Screen

DHCP Client: Enable or Disable DHCP Client function. When DHCP Client function is enabled, an IP address will be assigned to the switch from the network's DHCP server. In this mode, the default

IP address will be replaced by the one assigned by the DHCP server. If DHCP Client is disabled, then the IP address that you specified will be used instead.

IP Address: You can assign the IP address reserved by your network for your JN4508F-M. If DHCP Client function is enabled, you don't need to assign an IP address, as it will be overwritten by the DHCP server. The default IP address is 192.168.10.1.

Subnet Mask: Assign the subnet mask for the IP address. If DHCP Client function is enabled, you don't need to assign the subnet mask. The default Subnet Mask is 255.255.255.0.

Note: In the CLI, we use the enabled subnet mask to represent the number displayed in the web UI. For example, 8 stands for 255.0.0.0; 16 stands for 255.255.0.0; 24 stands for 255.255.255.0

Gateway: Assign the gateway for the switch. The default gateway is 192.168.10.254.

Note:

In the CLI, we use 0.0.0.0/0 to represent the default gateway.

Once you finish configuring the settings, click the *Apply* button to apply your configuration.

Time Setting

Time Setting source allow user to set the time by manually or through NTP server. Network Time Protocol (NTP) is used to synchronize computer clocks on the internet. You can configure NTP settings here to synchronize the clocks of several switches on the network.

The IEEE1588 PTP (Precision Time Protocol) supports very precise time synchronization in an Ethernet network. There are two clocks, Master and Slave. The master device periodically launches an exchange of messages with slave devices to help each slave clock re-compute the offset between its clock and the master's clock.

Note: Please enable one synchronization protocol (PTP/NTP) only.

JN4508F-M also provides Daylight Saving function.

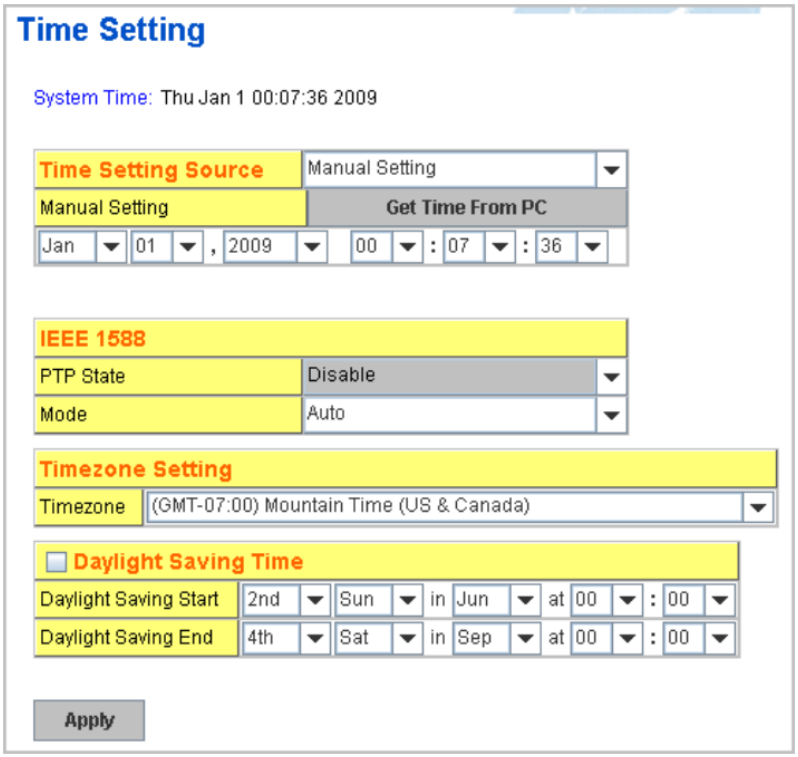


Figure 4-6. Time Setting Configuration

Manual Setting: User can select Manual setting to change time as user want and also click the icon *Get Time From PC* to sync time from your PC.

NTP client: Select the *Time Setting Source* to NTP client can let device enable the NTP client. It allow JN4508F-M get time from 2 different NTP servers. The system will send request packet to acquire current time from the NTP server.

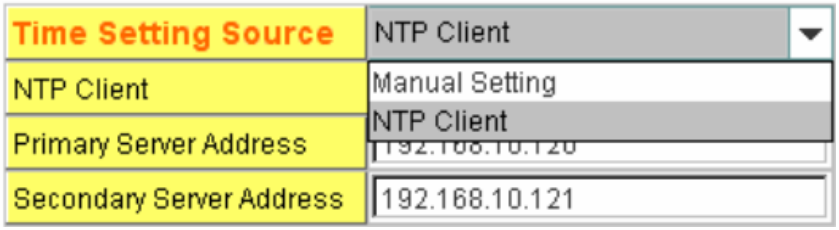


Figure 4-7. Time Setting Configuration Options

IEEE 1588: Select the *PTP State* to enable this function and select one operating mode for the precision time synchronizes.

Auto mode: The switch performs PTP Master and slave mode (Binary mode).

Master mode: Switch performs PTP Master only.

Slave mode: Switch performs PTP slave only.

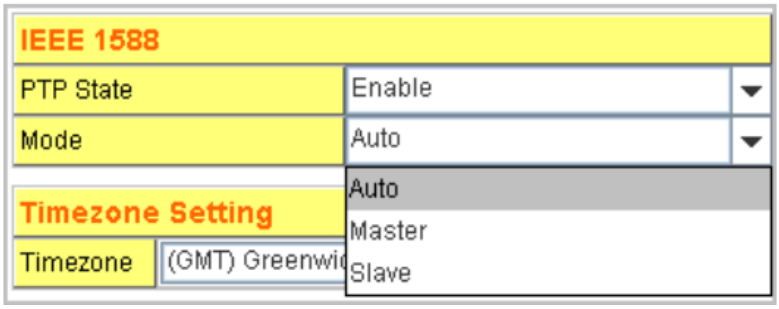


Figure 4-8. PTP State Configuration Options

Time zone: Select the time zone where the switch is located. For your reference, Table 4-9 lists the time zones of different locations. The default time zone is GMT (Greenwich Mean Time).

Switch(config)# clock timezone	
1	(GMT-12:00) Eniwetok, Kwajalein
2	(GMT-11:00) Midway Island, Samoa
3	(GMT-10:00) Hawaii
4	(GMT-09:00) Alaska
5	(GMT-08:00) Pacific Time (US & Canada) , Tijuana
6	(GMT-07:00) Arizona
7	(GMT-07:00) Mountain Time (US & Canada)
8	(GMT-06:00) Central America
9	(GMT-06:00) Central Time (US & Canada)
10	(GMT-06:00) Mexico City
11	(GMT-06:00) Saskatchewan
12	(GMT-05:00) Bogota, Lima, Quito
13	(GMT-05:00) Eastern Time (US & Canada)
14	(GMT-05:00) Indiana (East)
15	(GMT-04:00) Atlantic Time (Canada)
16	(GMT-04:00) Caracas, La Paz
17	(GMT-04:00) Santiago

18	(GMT-03:00) NewFoundland
19	(GMT-03:00) Brasilia
20	(GMT-03:00) Buenos Aires, Georgetown
21	(GMT-03:00) Greenland
22	(GMT-02:00) Mid-Atlantic
23	(GMT-01:00) Azores 24 (GMT-01:00) Cape Verde Is.
25	(GMT) Casablanca, Monrovia
26	(GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
27	(GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
28	(GMT+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague
29	(GMT+01:00) Brussels, Copenhagen, Madrid, Paris
30	(GMT+01:00) Sarajevo, Skopje, Sofija, Vilnius, Warsaw, Zagreb
31	(GMT+01:00) West Central Africa
32	(GMT+02:00) Athens, Istanbul, Minsk
33	(GMT+02:00) Bucharest
34	(GMT+02:00) Cairo
35	(GMT+02:00) Harare, Pretoria
36	(GMT+02:00) Helsinki, Riga, Tallinn
37	(GMT+02:00) Jerusalem
38	(GMT+03:00) Baghdad
39	(GMT+03:00) Kuwait, Riyadh
40	(GMT+03:00) Moscow, St. Petersburg, Volgograd
41	(GMT+03:00) Nairobi
42	(GMT+03:30) Tehran
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) Calcutta, Chennai, Mumbai, New Delhi
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) Bangkok, Hanoi, Jakarta
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, Singapore
59	(GMT+08:00) Perth
60	(GMT+08:00) Taipei
61	(GMT+09:00) Osaka, Sapporo, Tokyo
62	(GMT+09:00) Seoul
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) Magadan, Solomon Is., New Caledonia
72	(GMT+12:00) Aukland, Wellington

73	(GMT+12:00) Fiji, Kamchatka, Marshall Is.
74	(GMT+13:00) Nuku'alofa

Table 4-9. TimeZones Configuration List

Daylight Saving Time: Set when Enable Daylight Saving Time start and end, During the Daylight Saving Time, the device's time is one hour earlier than the actual time.

Daylight Saving Start and Daylight Saving End: the time setting allows user to selects the week that monthly basis, and sets the End and Start time individually.

Figure 4-9. Daylight Saving Time Configuration

Once you have finished the configuration, click the *Apply* button to apply your configuration.

DHCP Server

You can select to *Enable* or *Disable* DHCP Server function. JN4508F-M switch will assign a new IP address to link partners.

DHCP Server configuration

After selecting to enable DHCP Server function, type in the Network IP address for the DHCP server IP pool, Subnet Mask, Default Gateway address and Lease Time for client.

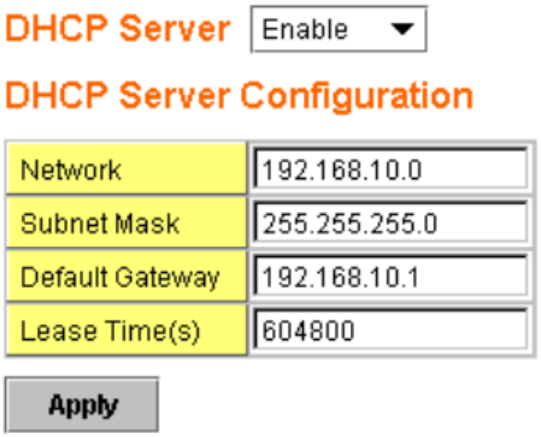


Figure 4-10. DHCP Server Configuration

Once you have finished the configuration, click the *Apply* button to apply your configuration.

Excluded Address: You can type a specific address into the IP Address field for the DHCP server reserved IP address.

The IP address that is listed in the Excluded Address List Table will not be assigned to the network device. Add or remove an IP address from the Excluded Address List by clicking the *Add* or *Remove* button.

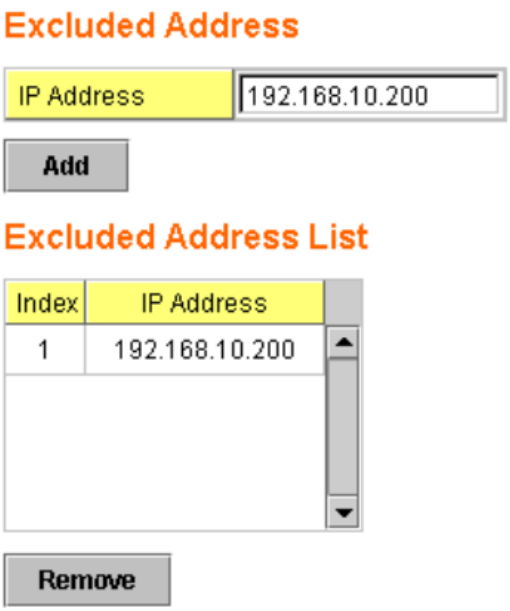


Figure 4-11. Excluded Address Configuration

Manual Binding: JN4508F-M provides a MAC address and IP address binding and removing function. You can type in the specified IP and MAC address, and then click the *Add* button to add a new MAC&IP address binding rule for a specified link partner, like PLC or any device without DHCP client function. To remove from the binding list, just select the rule to remove and click the *Remove* button.

Figure 4-12. Manual Blinding Configuration

DHCP Leased Entries: JN4508F-M Switch provides an assigned IP address list for user check. It will show the MAC and IP address that was assigned by JN4508F-M. Click the *Reload* button to refresh the listing.

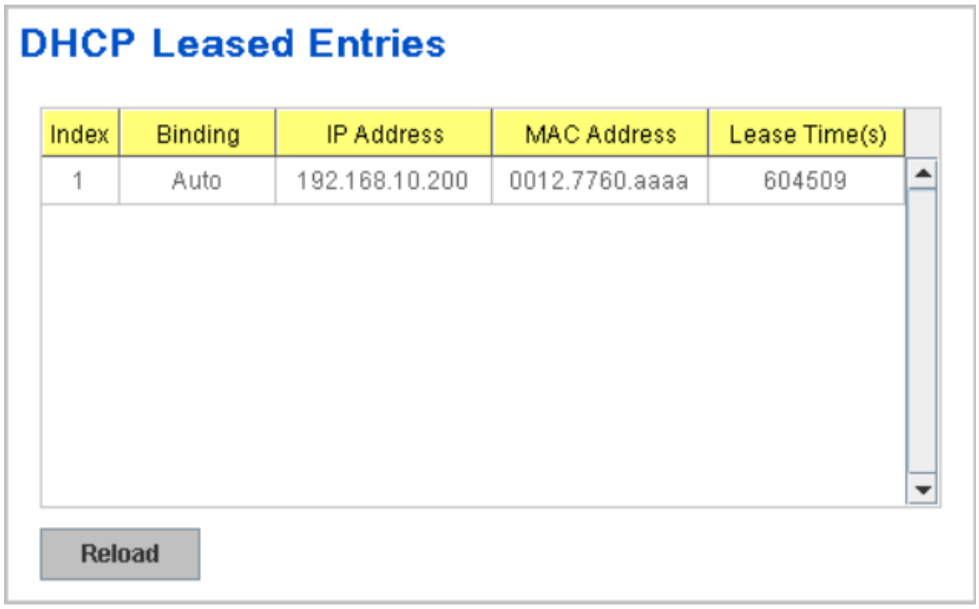


Figure 4-13. DHCP Leased Entries

DHCP Relay Agent: You can select to *Enable* or *Disable* DHCP relay agent function, and then select the modification type of option 82 field.

Figure 4-14. DHCP Relay Agent

Relay policy drop: Drops the option 82 field and do not add any option 82 field.

Relay policy keep: Keeps the original option 82 field and forwards to server.

Relay policy replace: Replaces the existing option 82 field and adds new option 82 field. (This is the default setting).

Helper Address: there are 4 fields for the DHCP server's IP address. You can fill the field with preferred IP address of DHCP Server, and then click *Apply* to activate the DHCP relay agent

function. All the DHCP packets from client will be modified by the policy and forwarded to DHCP server through the gateway port.

Backup and Restore

With the Backup command, you can save current configuration files saved in the switch's flash to the admin PC or TFTP server. This will allow you to go to the Restore command later, in order to restore the configuration file back to the switch. Before you restore the configuration file, you must place the backup configuration file into the PC or TFTP server. The switch will then download this file back to the flash.

There are 2 modes for users to backup/restore the configuration file, Local File mode and TFTP Server mode.

Local File mode: In this mode, the switch acts as the file server. Users can browse the target folder and then type in the file name to backup the configuration. Users can also browse the target folder and select existing configuration files to restore the configuration back to the switch. This mode is only provided by Web UI; CLI is not supported.

TFTP Server mode: In this mode, the switch acts as TFTP client. Before you do so, make sure that your TFTP server is ready. Then type in the IP address of the TFTP Server. The system uses the default configuration file name, Quagga.conf. You do not need to enter a new file name. This mode can be used in both Web UI and CLI.

TFTP Server IP Address: Key in the IP address of your TFTP Server here.

Backup/Restore File Name: Type de correct file name of the configuration file.

Configuration File: The configuration file of the switch is a text file. You can open it with Microsoft Word or any program that can read .txt files, modify the file, add/remove configuration settings, and then restore it back on to the switch.

Startup Configuration File: After you have saved the running-config to flash, the new settings will be updated after a power cycle. You can use show startup-config to view it in the CLI. The Backup command can only backup such configuration files to your PC or TFTP server.

Technical Tip:

Default Configuration File: The switch provides the default configuration file in the system. You can use the Reset button, Reload command to reset the system.

Running Configuration File: The switch's CLI allows you to view the latest settings running on the system. The information shown here are the settings you set up but once you finish have not saved selecting and to flash. The settings configuring the settings, click on not yet saved to flash will not work after a power Backup or Restore to run the process cycle. You can use show running-config to view it in the CLI.

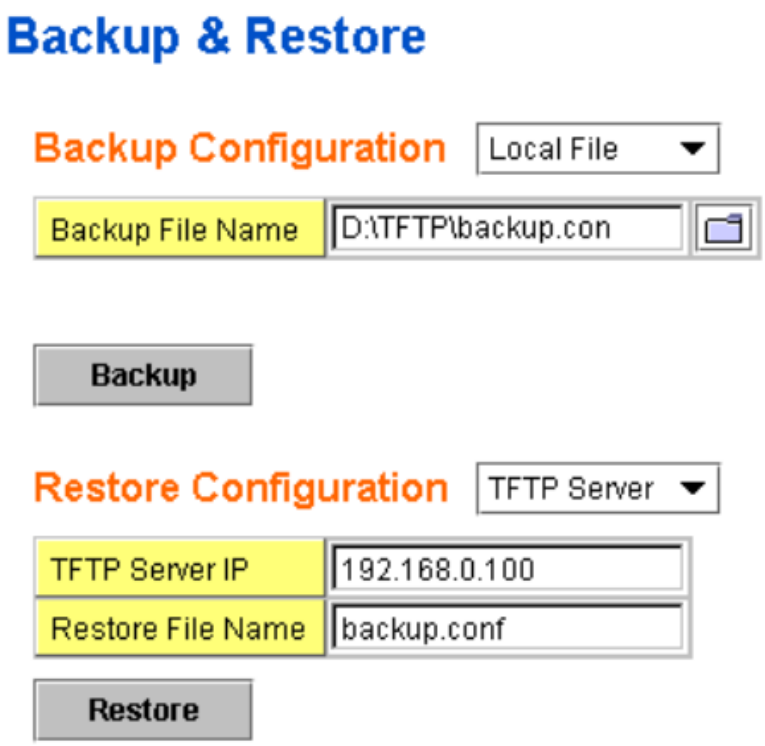


Figure 4-15. Backup and Restore Configuration

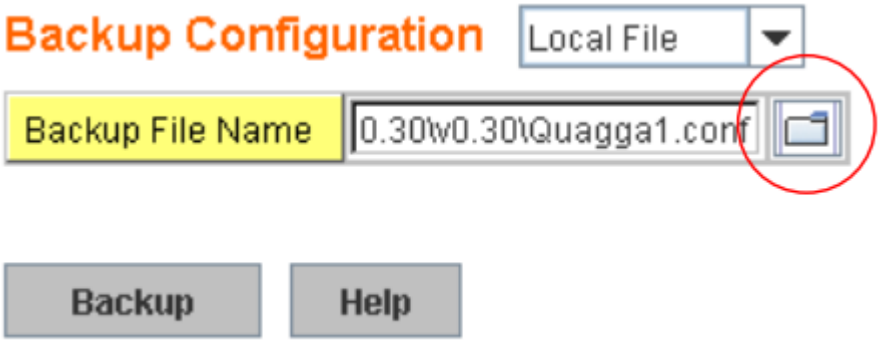


Figure 4-16. WEB UI for Backup/Restore Configuration - Local File Mode

Click on the Folder icon to select the target file you want to backup/restore.

Note:

The folders of the path to the target file do not allow you to input space key.

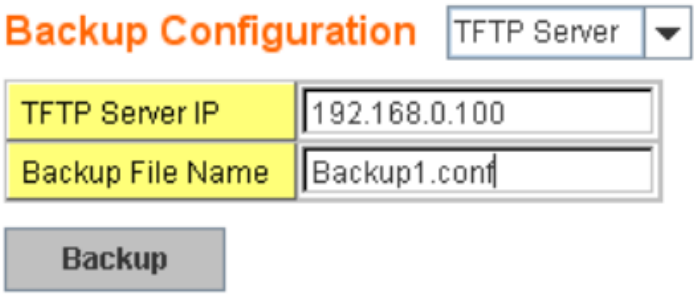


Figure 4-17. Web UI for Backup/Restore Configuration - TFTP Server Mode

Type-in the IP address of TFTP Server IP. Then click the *Backup/Restore* button.

Note:

Point to the wrong file will cause the entire configuration missed.

Firmware Upgrade

In this section, you can update the switch with the latest firmware. It is provided the latest firmware by altus technical support altus@altus.com.br. New firmware may include new features, bug fixes or other software changes. The Web site also provides release notes for the update as well. We suggest you use the latest firmware before installing the switch.

Note:

The system will automatically reboot after you finish upgrading the new firmware. Please inform all attached users before doing this.

Figure 4-18. Web Main UI for Firmware Upgrade

There are 2 modes for users to backup/restore the configuration file, Local File mode and TFTP Server mode.

Local File mode: In this mode, the switch acts as the file server. Users can browse the target folder and then type in the file name to backup the configuration. Users can also browse the target folder and select the existing configuration file to restore the configuration back to the switch. This mode is only provided by Web UI; CLI is not supported.

TFTP Server mode: In this mode, the switch acts as the TFTP client. Before you do so, make sure that your TFTP server is ready. Then, type in the TFTP Server IP address. This mode can be used in both Web UI and CLI.

TFTP Server IP Address: Key in the IP address of your TFTP Server here.

Firmware File Name: View the file name of the new firmware.

The UI also shows you the latest firmware version and build date. Please check the version number after you reboot the switch.

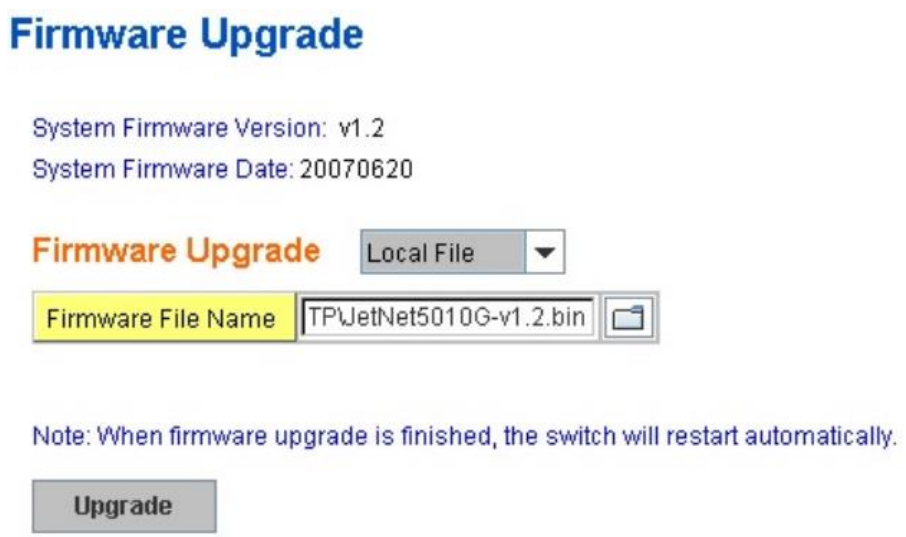


Figure 4-19. Web UI is for Firmware Upgrade - Local File Mode

Click on the Folder icon to select the correct firmware you want to upgrade.

Figure 4-20. Web UI is for Firmware Upgrade – TFTP Server Mode

Type in the IP address of the TFTP Server and the Firmware File Name. Then click the *Upgrade* button to start the process.

After finishing the transmission of the firmware, the system will copy the firmware file and replace the firmware in the flash. The CLI will show until the process is finished.

Factory Default

By clicking the *Reset* button, the system will reset all configurations to default settings. The system will show you a popup message window after running this command. Default settings will be in effect after rebooting the switch.

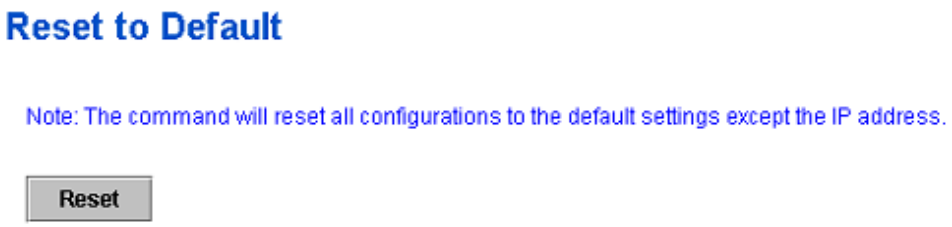


Figure 4-21. Web UI for Reset to Default

The Figure 4-22 is the popup alert screen to confirm the command. Click *Yes* to reset the system.

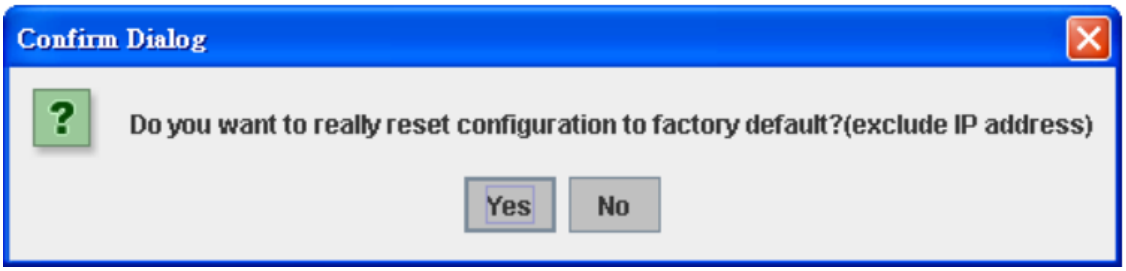


Figure 4-22. Reset System Command Dialog

The Figure 4-23UI is a popup message screen to show you that the reset is complete. Click *OK* to close the screen. Then go to the *Reboot* page to reboot the switch.

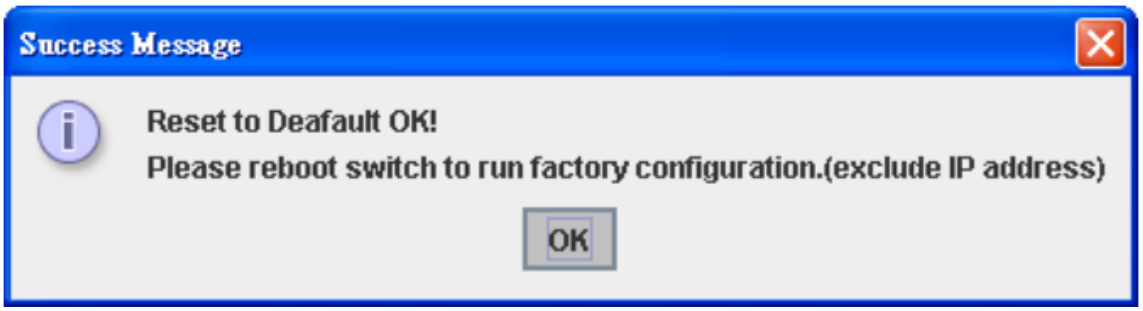


Figure 4-23. Confirmation of Factory Reset

Click *OK*. The system will then automatically reboot the device.

Note:

If you have already configured the IP of your device to another IP address; when you use this command through CLI and Web UI, our software will not reset the IP address to the default IP. The system will maintain the IP address so that you can still connect to the switch via the network.

System Reboot

System Reboot allows you to reboot the device. Some of the feature changes require you to reboot the system. Click the *Reboot* button to reboot your device.

Note:

Remember to click the *Save* button to save your settings. Otherwise, the settings you made will be gone once the switch is powered off.

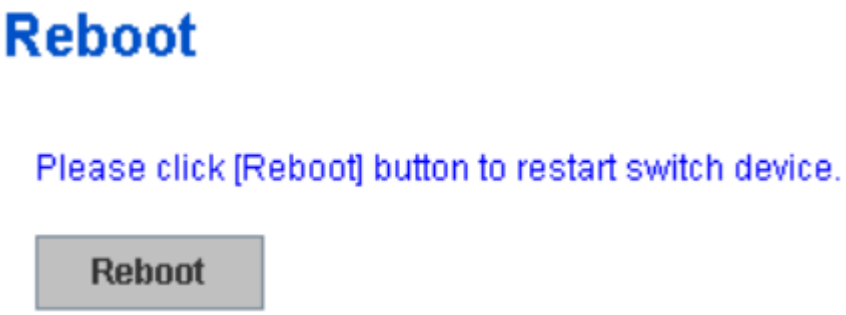


Figure 4-24. Main Screen for Reboot

Figure 4-25 is the popup alert screen to request confirmation for the Switch Reboot. Click *Yes* to reboot the switch.

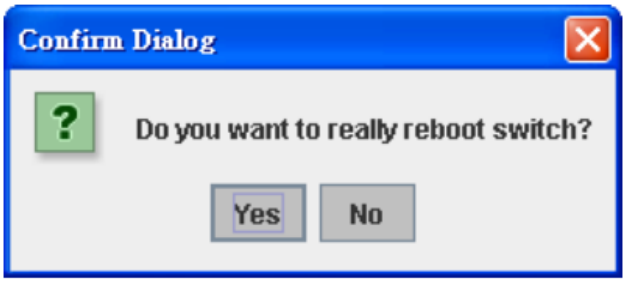


Figure 4-25. Reboot Switch Screen

The popup message screen in Figure 4-26 appears when rebooting the switch.

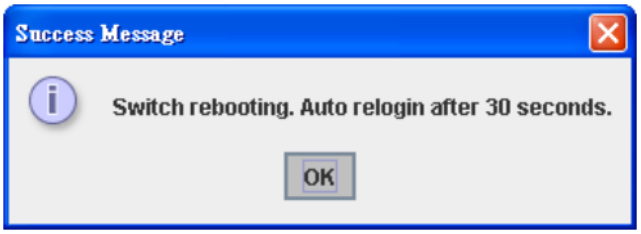


Figure 4-26. Confirmation of Switch Rebooting Command Accepted

CLI Commands for Basic Settings

Feature	Command Line
Switch Setting	
System Name	Switch(config)# hostname WORD Network name of this system Switch(config)# hostname JN4508F-M Switch(config)#
System Location	Switch(config)# snmp-server location Brasil
System Contact	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

Admin Password	
User Name and Password	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
IP Configuration	
IP Address/Mask 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
Remove 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 !
Time Setting	
NTP Server	Switch(config)# ntp peer 192.168.10.100
Time Zone	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 Connect 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 and Restore	
Backup Startup Configuration File	Switch# copy startup-config tftp: 192.168.10.33 Writing Configuration [OK] **Note 1**: To backup the latest startup configuration file, you should save current settings to flash first. You can refer to 4.12 to see how to save settings to the flash. **Note 2**: 192.168.10.33 is the TFTP server's IP. Your environment may use different IP addresses. Please type target TFTP server IP in this command.
Restore Configuration	Switch# copy tftp: 192.168.10.33 startup-config
Show Startup Configuration	Switch# show startup-config
Show Running Configuration	Switch# show running-config
Firmware Upgrade	
Firmware Update	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.....
Factory Default	
Factory Default	Switch# reload default-config file Reload OK! Switch# reboot
System Reboot	
Reboot	Switch# reboot

Table 4-10. CLI Comands for Basic Settings

Port Configuration

This section shows you how to enable/disable port state, or configure port auto-negotiation, speed, duplex, flow control, rate limit control and port aggregation settings. It also allows you to view port status and aggregation information.

Port Control

Port Control commands allow you to enable/disable port state, or configure port auto-negotiation, speed, duplex, and flow control.

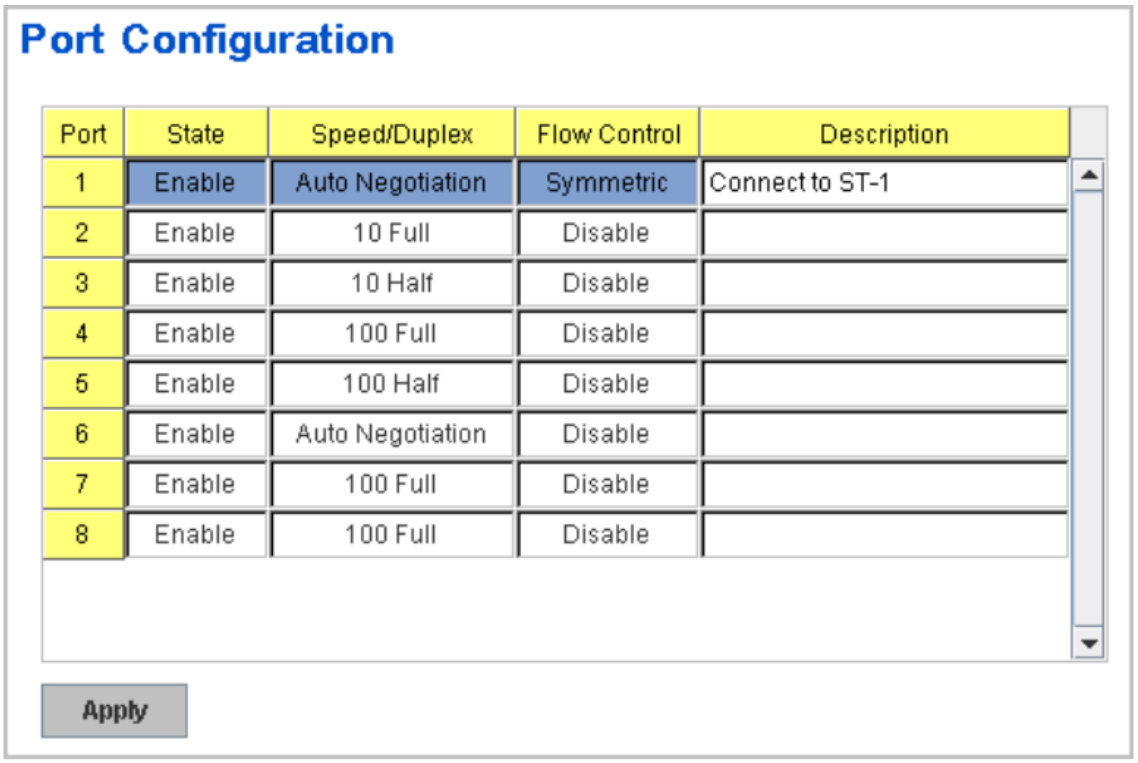


Figure 4-27. Port Configuration

Select the port you want to configure and make changes to the port.

State column: Enable or disable the state of this port. Once you disable the port, it stops linking and forwarding traffic. The default setting when you receive the device is Enable, which means all the ports are working.

Speed/Duplex column: Configure the port speed and duplex mode of this port. Below are the selections you can choose:

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

Fiber port (fa7, fa8): 100Full (100Mbps, Full Duplex) only.

Flow Control column: Symmetric or disable the flow control function. *Symmetric* means that you need to activate the flow control function of the remote network device in order to let the flow control of that corresponding port on the switch work. *Disable* means that you do not need to activate the flow control function of the remote network device, as the flow control of that corresponding port on the switch will work anyway.

Once you have finished configuring the settings, click the *Apply* button to save the configuration.

Technical Tips: If both ends are going at different speeds, they will not link to each other. If both ends are in different duplex modes, they will be connected by half mode.

Port Status

Port Status shows you the current port status. It includes connection type, port link status, exactly operating speed and duplex mode and the flow control setting.

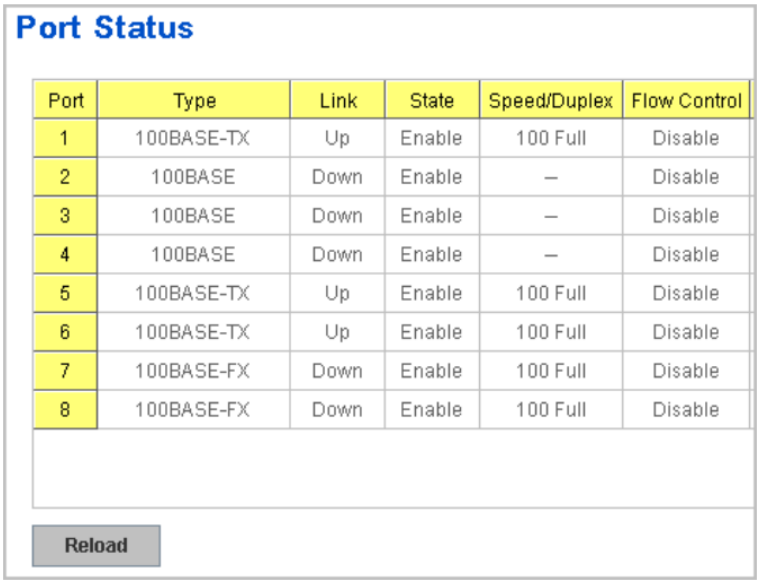


Figure 4-28. Port Status Example

A description of each column is as follows:

Port: Port interface number.

Type: 100BASE -> Fast Ethernet port.

Link: Link status. *Up* -> Link UP. *Down* -> Link Down.

State: *Enable* -> State is enabled. *Disable* -> The port is disabled by user configured.

Speed/Duplex: Current working status of the port.

Flow Control: The state of the flow control.

Rate Control

The Rate Control feature allows user to limit the each port's data rate; the limitation mechanism is based on specified packet type. With the Ingress / Egress rate control feature, the network performance can be improved. The packet types are listed in Figure 4-29.

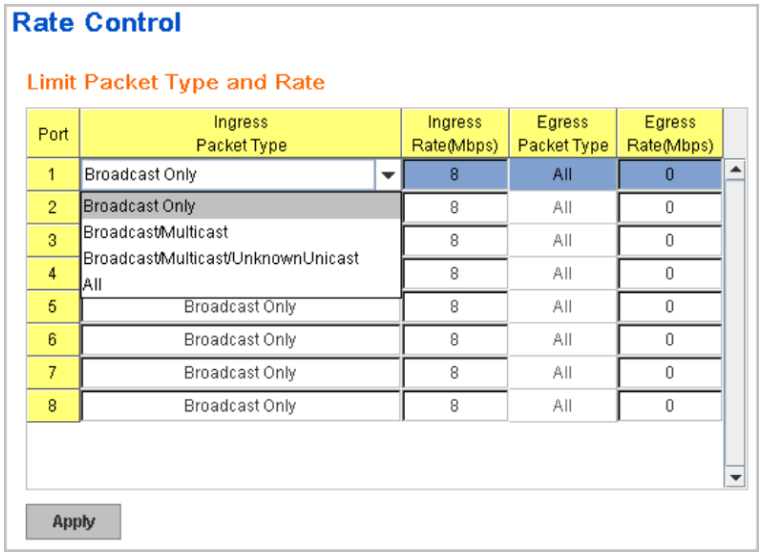


Figure 4-29. Rate Control Example

Rate Control is a form of flow control used to enforce a strict bandwidth limit at a port. You can program separate transmit (Egress Rule) and receive (Ingress Rule) rate limits at each port, and even apply the limit to certain packet types as described below.

Packet type: You can select the packet type that you want to filter. The packet types of the Ingress Rule (incoming) listed here includes Broadcast Only, Broadcast/multicast, Broadcast/Multicast/Unknown Unicast or All. The packet types of the Egress Rule (outgoing) only support All packet types.

Rate: This column allows you to manually assign the limit rate of the port. Valid values are from 1Mbps – 100Mbps for fast Ethernet ports. The step of the rate is 1 Mbps. Default value of Ingress Rule is 8 Mbps; default value of Egress Rule is 0 Mbps. 0 stands for disabling the rate control for the port.

To enable rate control function, please click the *Apply* button to apply the configuration.

Port Trunking

Port Trunking configuration allows you to group multiple Ethernet ports in parallel to increase link bandwidth. The aggregated ports can be viewed as one physical port so that the bandwidth is higher than merely one single Ethernet port. The member ports of the same trunk group can balance the loading and backup for each other. Port Trunking feature is usually used when you need higher bandwidth for backbone network. This is an inexpensive way for you to transfer more data.

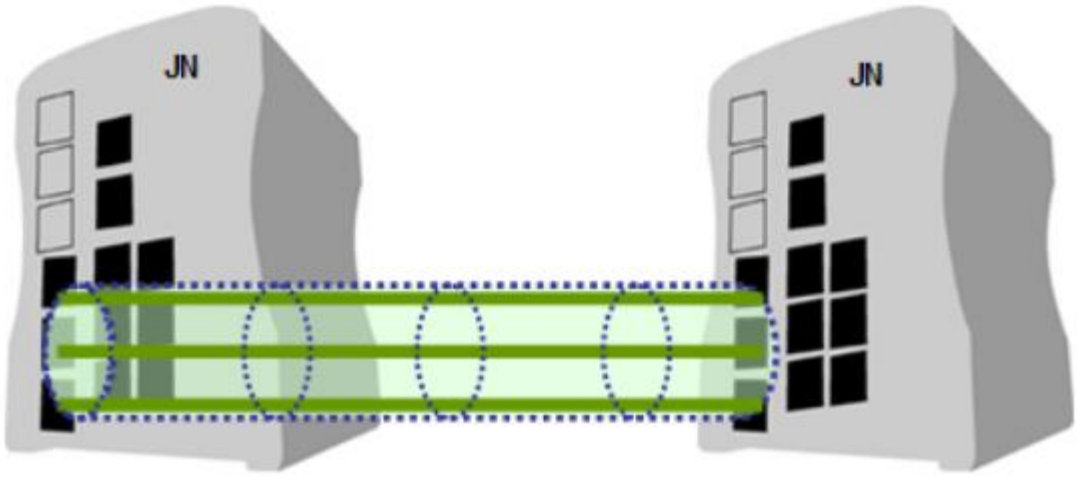


Figure 4-30. Port Trunking Example

There are some different descriptions for the port trunking. Different manufacturers may use different descriptions for their products, like Link Aggregation Group (LAG), Link Aggregation Control Protocol, Ethernet Trunk, Ether Channel…etc. Most of the implementations now conform to IEEE standard, 802.3ad.

The aggregated ports can interconnect to the other switch which also supports Port Trunking. Korenix Supports 2 types of port trunking. One is Static Trunk, the other is 802.3ad. When the other end uses 802.3ad LACP, you should assign 802.3ad LACP to the trunk. When the other end uses non-802.3ad, you can then use Static Trunk.

There are 2 configuration pages, Aggregation Setting and Aggregation Status.

Aggregation Settings

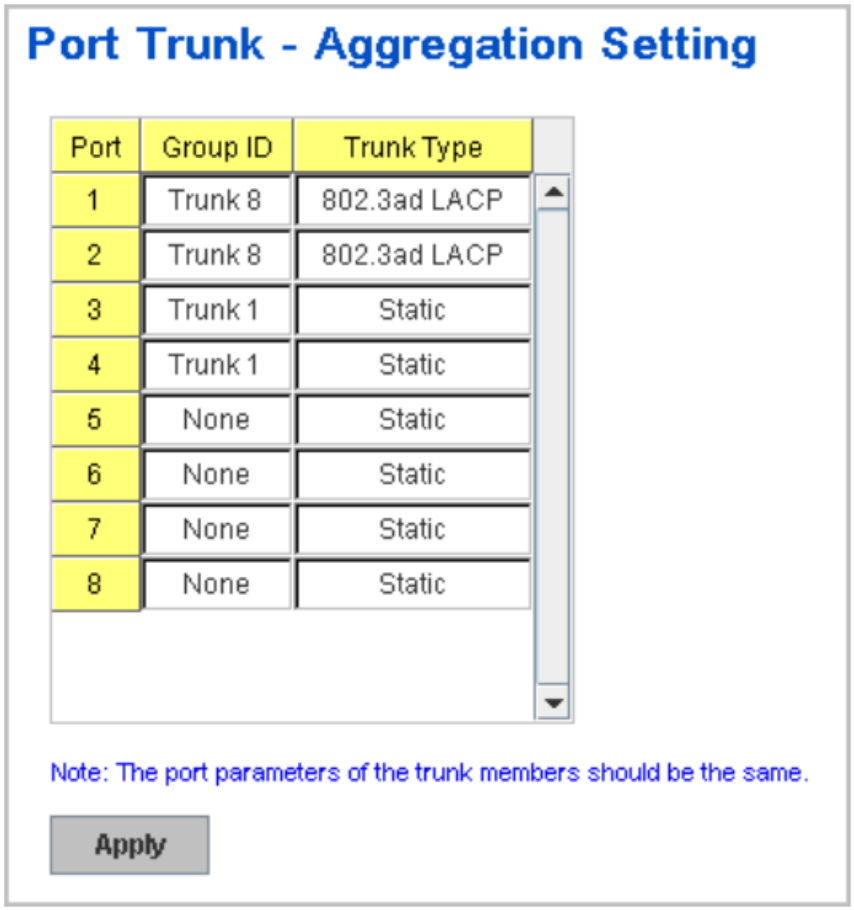


Figure 4-31. Aggregation Settings Configuration

Trunk Size: The switch can support up to 4 trunk groups and maximum trunk member up to 8 ports.
Group ID: Group ID is the ID for the port trunking group. Ports with same group ID are in the same group.
Trunk Type: Static and 802.3ad LACP. Each Trunk Group can only support Static or 802.3ad LACP. Choose the type you need here.

Aggregation Status

This page shows the status of port aggregation. Once the aggregation ports are negotiated well, you will see following status.

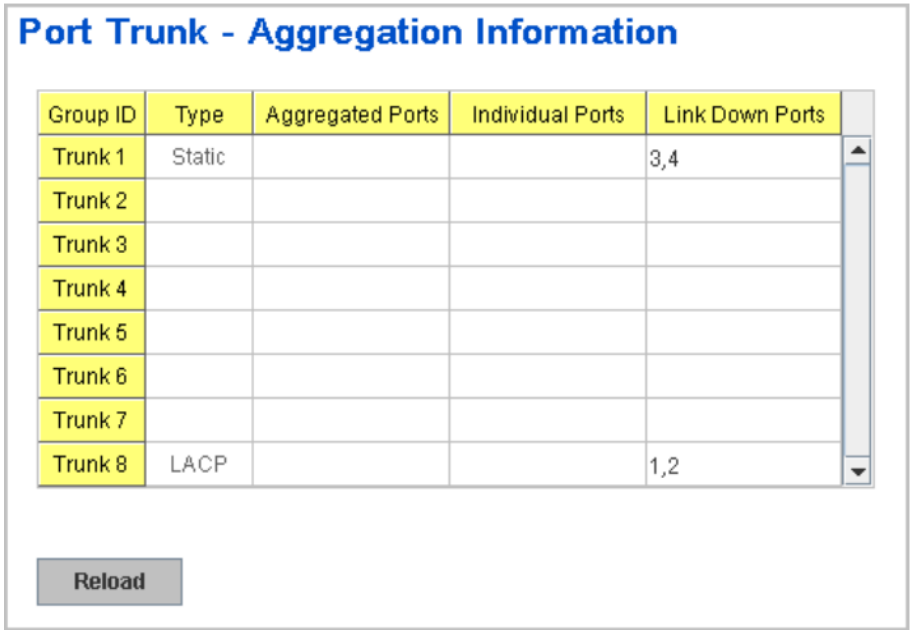


Figure 4-32. Aggregation Status Information

Group ID: Display Trunk 1 to Trunk 8 set up in Aggregation Settings. Type: Static or LACP set up in Aggregation Setting. (The JN4508 only support 4 trunk groups.).

Aggregated Ports: When LACP links well, you can see the member ports in aggregated column.

Individual Ports: When LACP is enabled, member ports of LACP group which are not connected to correct LACP member ports will be displayed in the Individual column.

Link Down ports: When LACP is enabled, member ports of LACP group which are not linked up will be displayed in the Link Down column.

Command Lines for Port Configuration

Feature	Command Line
Port Control	
Port Control - State	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
Port Control – AutoNegotiation	Switch(config)# interface fa1 Switch(config-if)# auto-negotiation Auto-negotiation of port 1 is enabled!
Port Control – ForceSpeed/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
Port Control – FlowControl	Switch(config-if)# flowcontrol on Flowcontrol on for port 1 set ok! Switch(config-if)# flowcontrol off Flowcontrol off for port 1 set ok!

Port Status	
Port Status	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. **Note**: Administrative Status -> Port state of the port. Operating status -> Current status of the port. Duplex -> Duplex mode of the port. Speed -> Speed mode of the port. Flow control -> Flow Control status of the port.
Rate Control	
Rate Control –Ingress or Egress	Switch(config-if)# rate-limit egress Outgoing packets ingress Incoming packets **Note**: To enable rate control, you should select the Ingress or Egress rule first; then assign the packet type and bandwidth.
Rate Control – FilterPacket Type	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.
Rate ControlBandwidth	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! Note: The interface list is fa1-8 Note: different speed port can't be aggregated together.
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#

Table 4-11. Command Lines for Port Configuration

Network Redundancy

It is critical for industrial applications for networks to continue working non-stop. JN4508F-M supports standard RSTP, Multiple Super Ring, Rapid Dual Homing and Legacy Super Ring Client modes.

Multiple Super Ring (MSR) technology is a 3rd generation Ring redundancy technology. is used in countries all over the world. MSR ranks the fastest restore and failover time in the world, 0 ms for restore and less than 5 milliseconds for failover.

Advanced Rapid Dual Homing technology also facilitates JN4508F-M to connect with a core managed switch via standard Rapid Spanning Tree Protocol. With RDH technology, you can also run RSTP to couple several Rapid Super Rings, which is also known as Auto Ring Coupling.

To become backwards compatible with the Legacy Super Ring technology implemented in JN4508F-M also supports Super Ring Client mode. The Super Ring ports can pass through Super Ring control packets extremely well and works with Super Ring.

Besides the ring technology, JN4508F-M also supports 802.1D-2004 version Rapid Spanning Tree Protocol (RSTP). The new version of RSTP standard includes 802.1D-1998 STP, 802.1w RSTP, IEEE 802.1s MSTP (Multiple Spanning Tree). The MSTP function is available from 1.1 version firmware.

STP Configuration

This page allows select the STP mode and configuring the global STP/RSTP Bridge Configuraiton.

The STP mode includes the *STP*, *RSTP*, *MSTP* and *Disable*. Please select the STP mode for your system first. The default mode is RSTP enabled.

After select the STP or RSTP mode; continue to configure the global Bridge parameters for STP and RSTP.

After select the MSTP mode, please go to MSTP Configuration page.

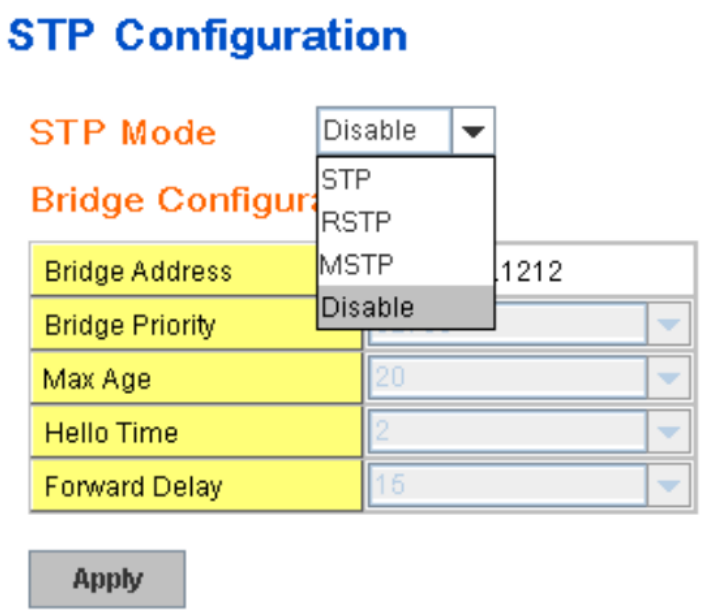


Figure 4-33. STP Configuration

RSTP

RSTP stands for Rapid Spanning Tree Protocol. If a switch has more than one path to a destination, it will lead to message loops that can generate broadcast storms and quickly bog down a network. The spanning tree was created to combat the negative effects of message loops in switched networks. A spanning tree uses a spanning tree algorithm (STA) to automatically sense whether a switch has more than one way to communicate with a node. It will then select the best path (primary), and block the other path(s). It will also keep track of the blocked path(s) in case the primary path fails. Spanning Tree Protocol (STP) introduced a standard method to accomplish this. It is specified in IEEE 802.1D-1998. Later, Rapid Spanning Tree Protocol (RSTP) was adopted and represents the evolution of STP, providing for a much faster spanning tree convergence after a topology change. This is specified in IEEE 802.1w. In 2004, 802.1w was included into the 802.1D-2004 version. This switch supports both RSTP and STP (all switches that supports RSTP are also backwards compatible with switches that support only STP).

Bridge Configuration

Bridge Address: This shows the switch's MAC address.

Priority (0-61440): RSTP uses bridge ID to determine the root bridge, the bridge with the highest bridge ID becomes the root bridge. The bridge ID is composed of bridge priority and bridge MAC address. So that the bridge with the highest priority becomes the highest bridge ID. If all of the bridges IDs have the same priority, the bridge with the lowest MAC address will then become the root bridge.

Note:

The bridge priority value must be in multiples of 4096. A device with a lower number has a higher bridge priority. Ex: 4096 is higher than 32768.

The Web GUI allows user select the priority number directly. This is the convinent of the GUI design. When you configure the value through the CLI or SNMP, you may need to type the value directly. Please follow the n x 4096 ruls for the Bridge Priority.

Max Age (6-40): Enter a value from 6 to 40 seconds here. This value represents the time that a bridge will wait without receiving Spanning Tree Protocol configuration messages before attempting to reconfigure.

If JN4508F-M is not the root bridge, and if it has not received a hello message from the root bridge in the amount of time equal to the Max Age, then JN4508F-M will reconfigure itself as a root bridge. Once two or more devices on the network are recognized as a root bridge, the devices will renegotiate to set up a new spanning tree topology.

Hello Time (1-10): Enter a value from 1 to 10 seconds here. This is a periodic timer that drives the switch to send out a BPDU (Bridge Protocol Data Unit) packet to check current STP status.

The root bridge of the spanning tree topology periodically sends out a *hello message* to other devices on the network to check if the topology is healthy. The *hello time* is the amount of time the root has waited in between sending hello messages.

Forward Delay Time (4-30): Enter a value between 4 and 30 seconds. This value is the time that a port waits before changing from Spanning Tree Protocol learning and listening states to forwarding state.

This is the amount of time JN4508F-M will wait before checking to see if it should be changed to a different state.

Once you have completed your configuration, click the *Apply* button to apply your settings.

Note:

You must observe the following rules to configure Hello Time, Forwarding Delay, and Max Age parameters.

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

STP Port Configuration

This page allows you to configure the port parameter after enabled STP or RSTP.

Port Configuration

Select the port you want to configure; you will be able to view the current settings and status of the port.

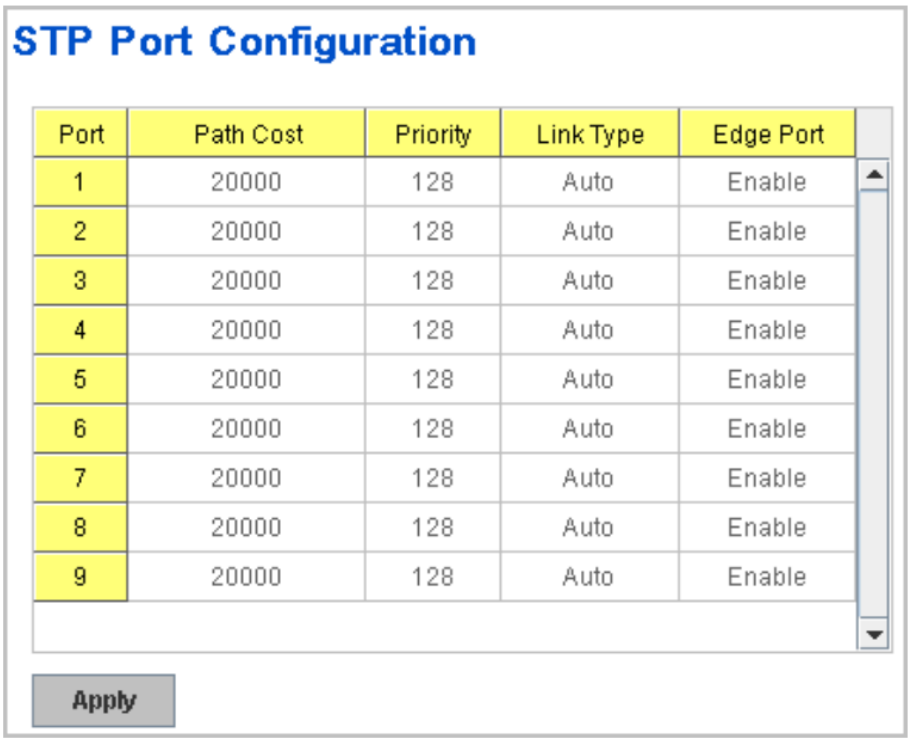


Figure 4-34. STP Port Configuration

Path Cost: Enter a number between 1 and 200,000,000. This value represents the cost of the path to the other bridge from the transmitting bridge at the specified port.

Priority: Enter a value between 0 and 240 using multiples of 16. This is the value that decides which port should be blocked by priority in a LAN.

Link Type: There are 3 types for you select. *Auto*, *P2P* and *Share*.

Some of the rapid state transitions that are possible within RSTP depend upon whether the port of concern can only be connected to another bridge (i.e. it is served by a point-to-point LAN segment), or if it can be connected to two or more bridges (i.e. it is served by a shared-medium LAN segment). This function allows P2P status of the link to be manipulated administratively.

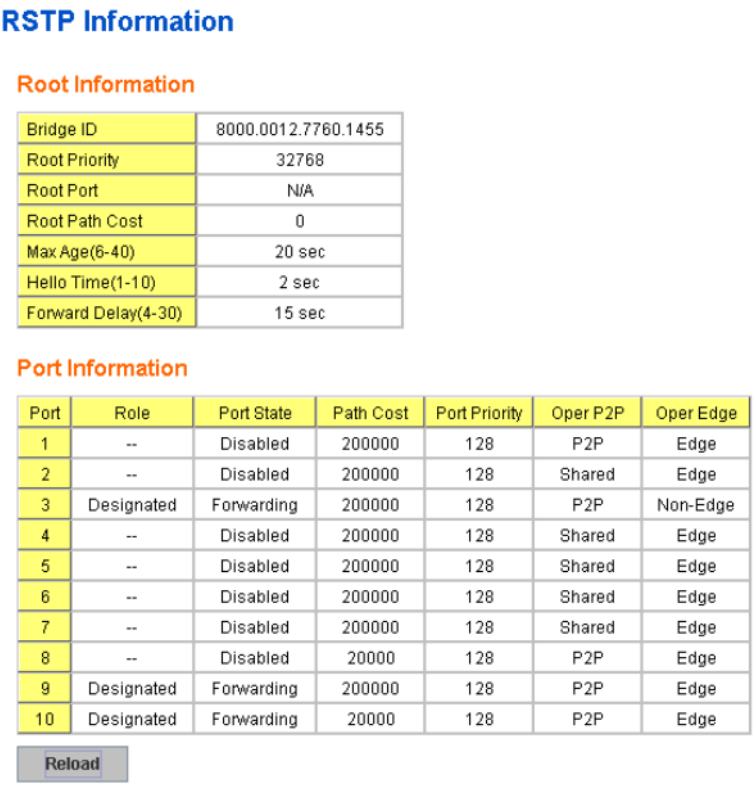
Auto means to auto select P2P or Share mode. P2P means P2P is enabled, while Share means P2P is disabled.

Edge: A port directly connected to the end stations cannot create a bridging loop in the network. To configure this port as an edge port, set the port to the Enable state. When the non-bridge device connects an admin edge port, this port will be in blocking state and turn to forwarding state in 4 seconds.

Once you have finished your configuration, click the *Apply* button to save your settings.

RSTP Information

This page allows you to see the information of the root switch and port status.


RSTP Information

Root Information

Bridge ID	8000.0012.7760.1455
Root Priority	32768
Root Port	N/A
Root Path Cost	0
Max Age(6-40)	20 sec
Hello Time(1-10)	2 sec
Forward Delay(4-30)	15 sec

Port Information

Port	Role	Port State	Path Cost	Port Priority	Oper P2P	Oper Edge
1	--	Disabled	200000	128	P2P	Edge
2	--	Disabled	200000	128	Shared	Edge
3	Designated	Forwarding	200000	128	P2P	Non-Edge
4	--	Disabled	200000	128	Shared	Edge
5	--	Disabled	200000	128	Shared	Edge
6	--	Disabled	200000	128	Shared	Edge
7	--	Disabled	200000	128	Shared	Edge
8	--	Disabled	20000	128	P2P	Edge
9	Designated	Forwarding	200000	128	P2P	Edge
10	Designated	Forwarding	20000	128	P2P	Edge

Reload

Figure 4-35. RSTP Information Screen

Root Information: You can see Root Bridge ID, Root Priority, Root Port, Root Path Cost and the Max Age, Hello Time and Forward Delay of BPDU sent from the root switch.

Port Information: You can see port Role, Port State, Path Cost, Port Priority, Oper P2P mode, Oper edge port mode, Oper edge port mode and Aggregated (ID/Type).

MSTP (Multiple Spanning Tree Protocol) Configuration

MSTP is the abbreviation of Multiple Spanning Tree Protocol. This protocol is a direct extension of RSTP. It can provide an independent spanning tree for different VLANs. It simplifies network management, provides for even faster convergence than RSTP by limiting the size of each region, and prevents VLAN members from being segmented from the rest of the group (as sometimes occurs with IEEE 802.1D STP).

While using MSTP, there are some new concepts of network architecture. A switch may belong to different group, acts as root or designate switch, generate BPDU for the network to maintain the forwarding table of the spanning tree. With MSTP, it can also provide multiple forwarding paths and enable load balancing. Understand the architecture allows you to maintain the correct spanning tree and operate effectively.

One VLAN can be mapped to a Multiple Spanning Tree Instance (MSTI). The maximum Instance of JN4508F-M supports is 16, range from 0-15. The MSTP builds a separate Multiple Spanning Tree (MST) for each instance to maintain connectivity among each of the assigned VLAN groups. An Internal Spanning Tree (IST) is used to connect all the MSTP switches within an MST region. An MST Region may contain multiple MSTP Instances.

The figure shows there are 2 VLANs/MSTP Instances and each instance has its Root and forwarding paths.

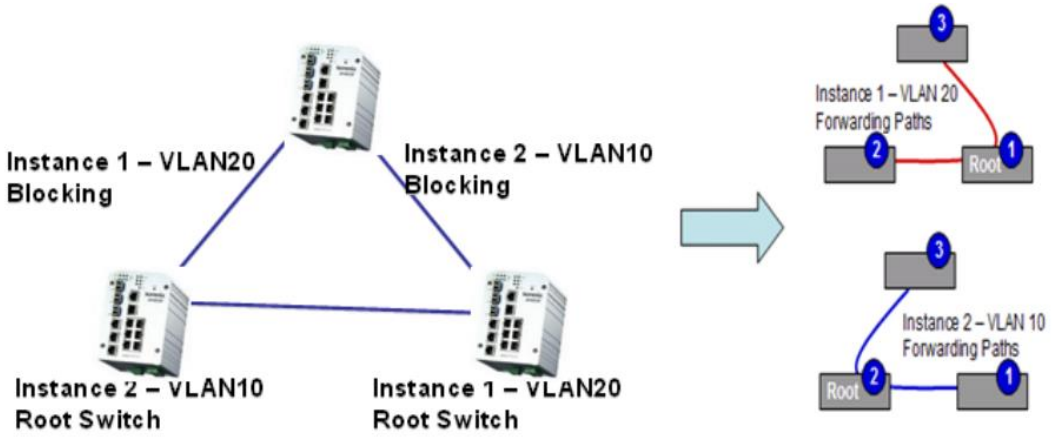


Figure 4-36. MSTP Example

A Common Spanning Tree (CST) interconnects all adjacent MST regions and acts as a virtual bridge node for communications with STP or RSTP nodes in the global network. MSTP connects all bridges and LAN segments with a single Common and Internal Spanning Tree (CIST). The CIST is formed as a result of the running spanning tree algorithm between switches that support the STP, RSTP, MSTP protocols.

The figure shows the CST large network. In this network, a Region may have different instances and its own forwarding path and table; however, it acts as a single Bridge of CST.

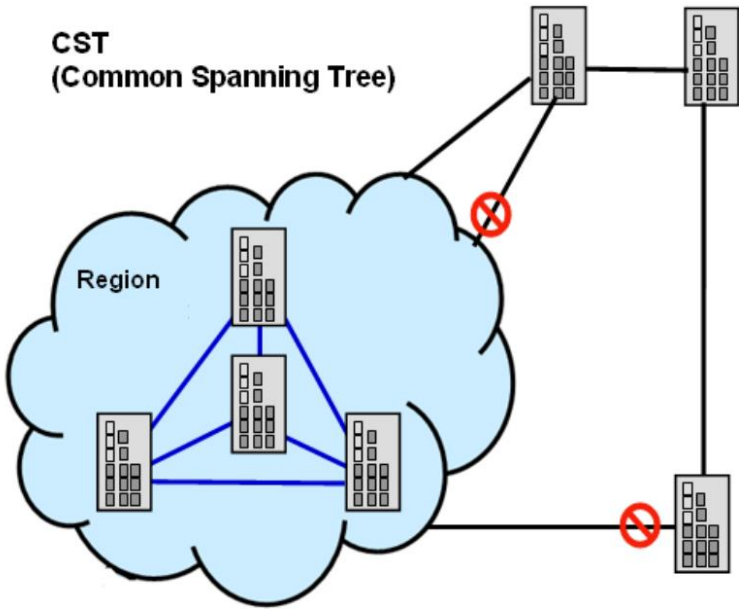


Figure 4-37. CST Example

To configure the MSTP setting, the STP Mode of the STP Configuration page should be changed to MSTP mode first.

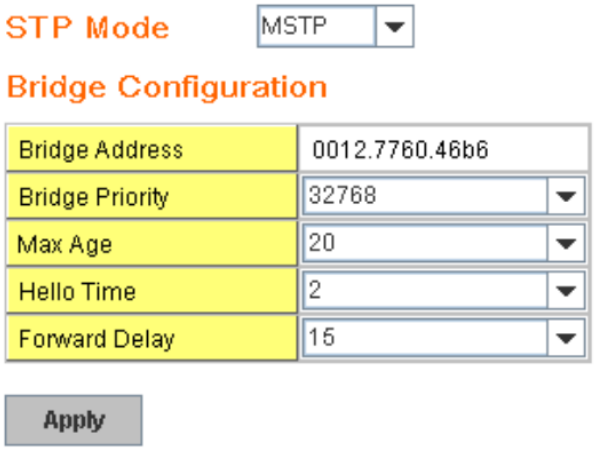


Figure 4-38. STP Configuration Mode

After enabled MSTP mode, then you can go to the MSTP Configuration pages.

MSTP Region Configuration

This page allows configure the Region Name and its Revision, mapping the VLAN to Instance and check current MST Instance configuration. The network can be divided virtually to different Regions. The switches within the Region should have the same Region and Revision leve.

Region Name: The name for the Region. Maximum length: 32 characters.

Revision: The revision for the Region. Range: 0-65535; Default: 0) Once you finish your configuration, click on *Apply* to apply your settings.

New MST Instance

This page allows mapping the VLAN to Instance and assign priority to the instance. Before mapping VLAN to Instance, you should create VLAN and assign the member ports first. Please refer to the VLAN setting page.

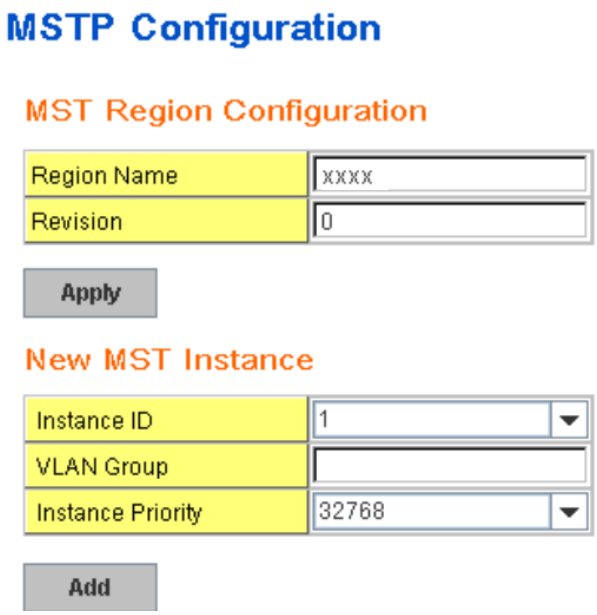


Figure 4-39. MSTP Region Configuration

Instance ID: Select the Instance ID, the available number is 1-15

VLAN Group: Type the VLAN ID you want mapping to the instance.

Instance Priority: Assign the priority to the instance.

After finish your configuration, click on *Add* to apply your settings

Current MST Instance Configuration

This page allows you to see the current MST Instance Configuration you added. Click on *Apply* to apply the setting. You can *Remove* the instance or *Reload* the configuration display in this page.

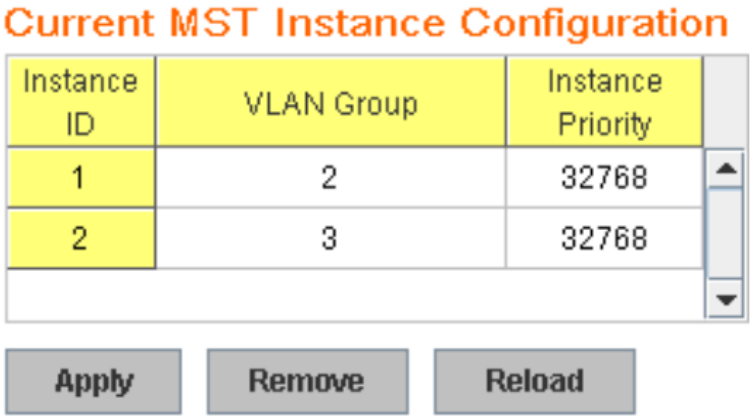


Figure 4-40. MST Instance Configuration

Multiple Super Ring (MSR)

The most common industrial network redundancy is to form a ring or loop. Typically, the managed switches are connected in a series and the last switch is connected back to the first one. In such a connection, you can use Super Ring technology to get fatest recovery performance.

Multiple Super Ring (MSR) technology is the 3rd generation Ring redundancy technology. This is used in countries all over the world. MSR ranks the fastest restore and failover time in the world, 0

ms for restore and about milliseconds level for failover for 100Base-TX copper port. The other interface may take longer time due to the media characteristics.

Advanced Rapid Dual Homing (RDH) technology also facilitates JN4508F-M Managed Switch to connect with a core managed switch easily and conveniently. With RDH technology, you can also couple several Rapid Super Rings or RSTP cloud together, which is also known as Auto Ring Coupling.

TrunkRing technology allows integrate MSR with LACP/Port Trunking. The LACP/Trunk aggregated ports is a virtual interface and it can work as the Ring port of the MSR.

MultiRing is an outstanding technology Korenix can support. Multiple rings can be aggregated within one switch by using different Ring ID. The maximum Ring number one switch can support is half of total port volume. For example, the JN4508F-M is an 8 port Fast Ethernet Switch design, which means maximum 4 Rings (4 100Mbps Rings) can be aggregated in one JN4508F-M. The feature saves much effort when constructing complex network architecture.

To become backwards compatible with the Legacy Super Ring technology implemented in JN4508F-M also supports Super Ring Client mode. The Super Ring ports can pass through Super Ring control packets extremely well and works with Super Ring.

New Ring: To create a Rapdis Super Ring. Just fill in the Ring ID which has range from 0 to 31. If the name field is left blank, the name of this ring will be automatically naming with Ring ID.

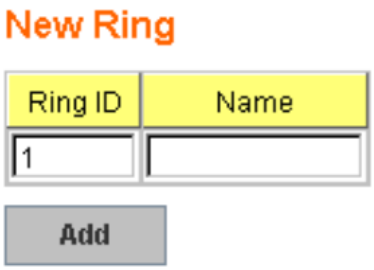


Figure 4-41. New Ring

Ring Configuration

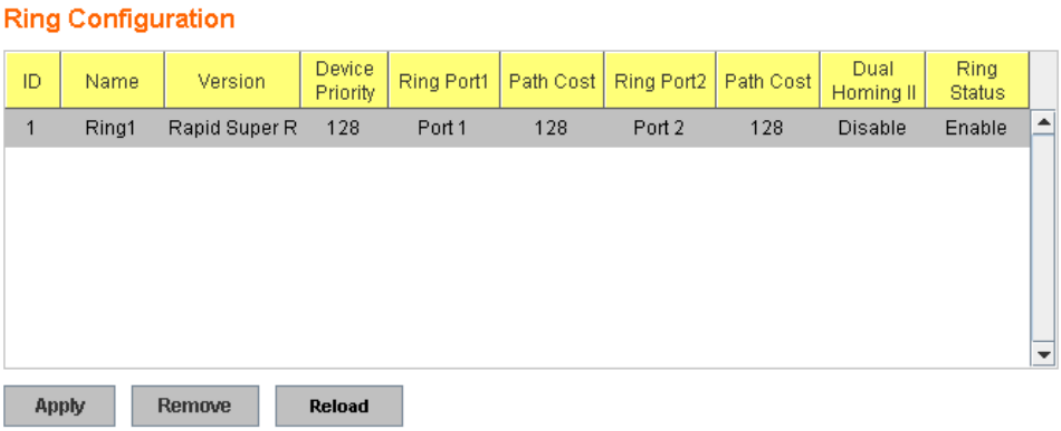


Figure 4-42. Ring Configuration

ID: Once a Ring is created, This appears and can not be changed.

Name: This field will show the name of the Ring. If it is not filled in when creating, it will be automatically named by the rule *RingID*.

Version: The version of Ring can be changed here. There are three modes to choose: Rapid Super Ring as default; Super ring for compatible with 1 st general ring and Any Ring for compatible with other version of rings.

Device Priority: The switch with highest priority (highest value) will be automatically selected as Ring Master. Then one of the ring ports in this switch will become forwarding port and the other one will become blocking port. If all of the switches have the same priority, the switch with the biggest MAC address will be selected as Ring Master.

Ring Port1: In Rapid Super Ring environment, you should have 2 Ring Ports. No matter this switch is Ring Master or not, when configuring RSR, 2 ports should be selected to be Ring Ports. For Ring Master, one of the ring ports will become the forwarding port and the other one will become the blocking port.

Path Cost: Change the Path Cost of Ring Port1. If this switch is the Ring Master of a Ring, then it determines the blocking port. The Port with higher Path Cost in the two ring ports will become the blocking port, If the Path Cost is the same, the port with larger port number will become the blocking port.

Ring Port2: Assign another port for ring connection.

Path Cost: Change the Path Cost of Ring Port2.

Rapid Dual Homing: Rapid Dual Homing is an important feature of 3rd generation Ring redundancy technology. When you want to connect multiple RSR or form redundant topology with other vendors, RDH could allow you to have maximum 7 multiple links for redundancy without any problem.

In Dual Homing I released with JN4508F-M, you have to configure additional port as Dual Homing port to two uplink switches. In Rapid Dual Homing, you don't need to configure specific port to connect to other protocol. The Rapid Dual Homing will smartly choose the fastest link for primary link and block all the other link to avoid loop. If the primary link failed, Rapid Dual Homing will automatically forward the secondary link for network redundant. Of course, if there are more connections, they will be standby links and recover one of then if both primary and secondary links are broken.

Ring status: To enable/disable the Ring. Please remember to enable the ring after you add it.

MultiRing: The MultiRing technology is one of the patterns of the MSR technology; it allows you to aggregate multiple rings within one switch. Create multiple ring ID and assign different ring port 1 and port 2 to each ring, thus the switch can have multiple rings in one JN4508F-M Switch.

When implementing MultiRing, remember that the different rings can NOT use the same ring ID. The other settings are the same as above description. Technically, the maximum ring volume the MultiRing supported is up to 16 rings. Due the limited number of ports, the number of ring network is the half of port number.

TrunkRing: The MultiRing technology is part of the MSR technology which combines the MSR with the port trunking technology. After multiple ports aggregated, this is so-call port trunking (Staticly or learnt by LACP protocol), the Trunk ID can be one of the port ID of the MSR technology. Configured the port trunking first then you can add the Trunk group as a Ring Port in managed switch.

Ring Information

The next image shows MSR information.

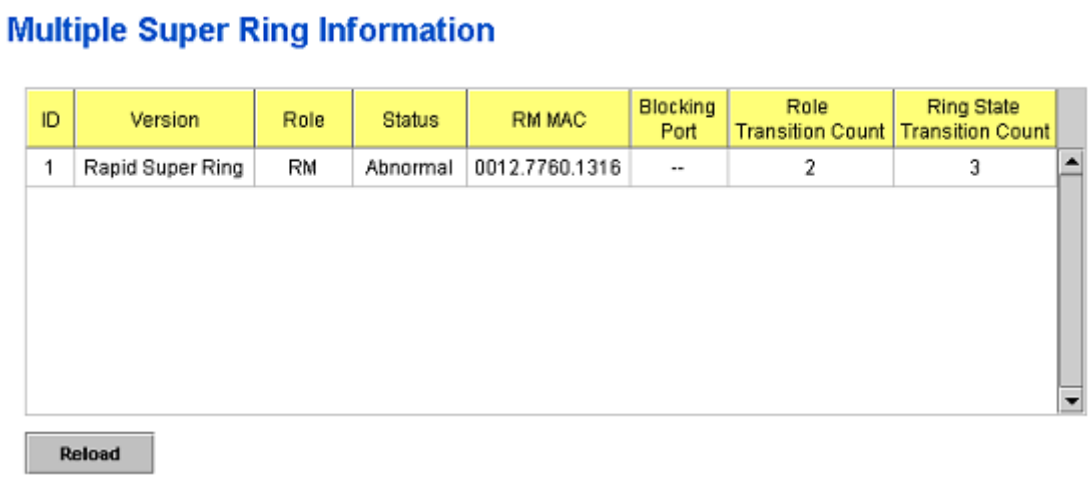


Figure 4-43. MSR Information Screen

ID: Ring ID.

Version: which version of this ring, this field could be Rapid Super Ring or Super Ring.

Role: This Switch is RM or nonRM.

Status: If this field is Normal which means the redundancy is approved. If any one of the link in this Ring is broken, then the status will be Abnormal.

RM MAC: The MAC address of Ring Master of this Ring. It helps to find the redundant path.

Blocking Port: This field shows which port of RM.is blocked.

Role Transition Count: This means how many times this switch has changed its Role from nonRM to RM or from RM to nonRM.

Role state Transition Count: This number means how many times the Ring status has been transformed between Normal and Abnormal state.

Command Lines for Network Redundancy

Feature	Command Line
Globa (STP, RSTP, MSTP)	
Enable	Switch(config)# spanning-tree enable
Disable	Switchconfig)# spanning-tree disable
Mode (Choose the 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)
Bridge Priority	Switch(config)# spanning-tree priority <0-61440> valid range is 0 to 61440 in multiple of 4096 Switch(config)# spanning-tree priority 4096
Bridge Times	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.
Forward Delay	Switch(config)# spanning-tree forward-time <4-30> Valid range is 4~30 seconds Switch(config)# spanning-tree forward-time 15
Max Age	Switch(config)# spanning-tree hello-time <1-10> Valid range is 1~10 seconds Switch(config)# spanning-tree hello-time 2
MSTP	
Enter the MSTP	Switch(config)# spanning-tree mst

Configuration Tree	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
Region Configuration	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
Mapping Instance to VLAN (Ex: Mapping VLAN 2 to Instance 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
Display Current MST Configuraion	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 Region Name	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
Show Pending MST Configuration	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 ----------
Apply the setting and go to the configuration mode	Switch(config-mst)# quit apply all mst configuration changes Switch(config)#
Apply the setting and go to the global mode	Switch(config-mst)# end apply all mst configuration changes Switch#
Abort the Setting and go to the configuration mode. Show Pending to see the new settings are not applied.	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	
System RSTP Setting	The mode should be rst, the timings can be configured in global settings listed in above.
Port Configuration Mode	
Port Configuraiton	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
Port Path Cost	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
Port Priority	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
Link Type – Auto	Switch(config-if)# spanning-tree link-type auto
Link Type – P2P	Switch(config-if)# spanning-tree link-type point-to-point
Link Type – Share	Switch(config-if)# spanning-tree link-type shared
Edge Port	Switch(config-if)# spanning-tree edge-port enable Switch(config-if)# spanning-tree edge-port disable
MSTP Port Configuration	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
Global Information	
Active Information	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
RSTP Summary	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
Port Info	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
MSTP Information	
MSTP Configuraiton	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 ----------
Display all MST Information	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 Root Information	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 Instance Information	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 Port Information	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
Multiple Super Ring	
Create or configure a 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.
Super Ring Version	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
Priority	Switch(config-super-ring-plus)# priority <0-255> valid range is 0 to 255 default set default Switch(config-super-ring-plus)# priority 100
Ring Port	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
Ring Port Cost	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.
Ring Info	
Ring Info	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.

Table 4-12. Command Lines for Network Redundancy

VLAN

A Virtual LAN (VLAN) is a logical grouping of nodes for the purpose of limiting a broadcast domain to specific members of a group without physically grouping the members together. That means, VLAN allows you to isolate network traffic so that only members of VLAN could receive traffic from the same VLAN members. Basically, creating a VLAN from a switch is the logical equivalent of physically reconnecting a group of network devices to another Layer 2 switch, without actually disconnecting these devices from their original switches.

JN4508F-M Industrial Ethernet Switch supports 802.1Q VLAN. 802.1Q VLAN is also known as Tag-Based VLAN. This Tag-Based VLAN allows VLAN to be created across different switches. IEEE 802.1Q tag-based VLAN makes use of VLAN control information stored in a VLAN header attached to IEEE 802.3 packet frames. This tag contains a VLAN Identifier (VID) that indicates which VLAN a frame belongs to. Since each switch only has to check a frame's tag, without the need to dissect the contents of the frame, this also saves a lot of computing resources within the switch.

VLAN Configuration group enables you to Add/Remove VLAN, configure port Ingress/Egress parameters and view VLAN table.

Port Based VLAN Configuration

VLAN Port Configuration allows you to set up VLAN port parameters to specific port. These parameters include PVID, Accept Frame Type and Ingress Filtering.

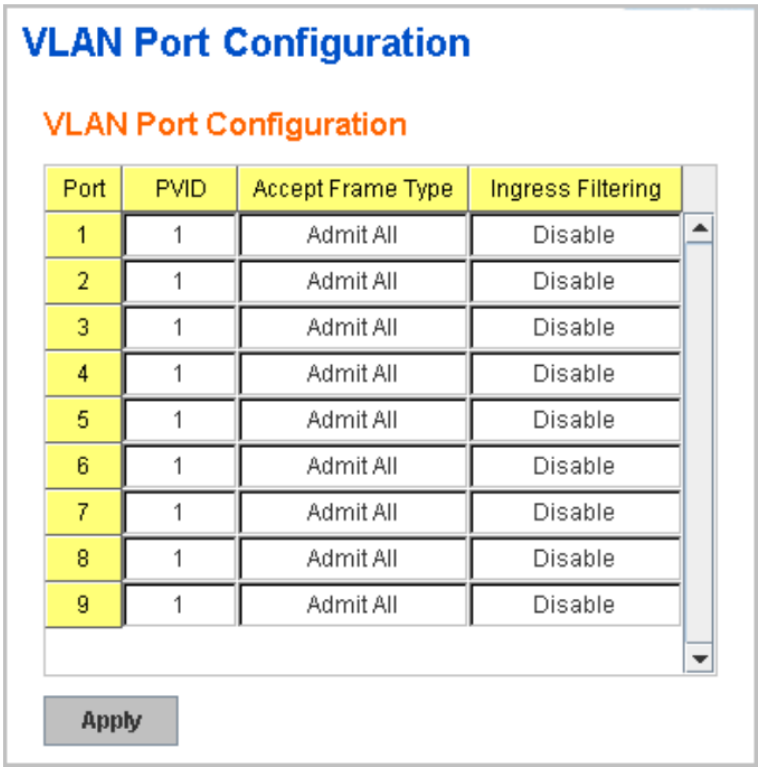


Figure 4-44. VLAN Port Configuration Screen

PVID: The abbreviation of Port VLAN ID. Enter the port VLAN ID here. PVID allows the switches to identify which port belongs to which VLAN. To keep things simple, it is recommended that PVID is equivalent to VLAN IDs.

The values of PVIDs are from 0 to 4095. But, 0 and 4095 are reserved. You cannot input these 2 PVIDs. 1 is the default value. 2 to 4094 are valid and available in this column. Type the PVID you'd like to configure here.

Accept Frame Type: This column defines the accepted frame type of the port. There are 2 modes you can select, Admit All and Tag Only. Admit All mode means that the port can accept both tagged and untagged packets. Tag Only mode means that the port can only accept tagged packets.

Ingress Filtering: Ingress filtering helps VLAN engine to filter out undesired traffic on a port. When Ingress Filtering is enabled, the port checks whether the incoming frames belong to the VLAN they claimed or not. Then the port determines if the frames can be processed or not. For example, if a tagged frame from Engineer VLAN is received, and Ingress Filtering is enabled, the switch will determine if the port is on the Engineer VLAN's Egress list. If it is, the frame can be processed. If it's not, the frame would be dropped.

VLAN Configuration

In this chappter , you can assign Management VLAN, create the static VLAN, and assign the Egress rule for the member ports of the VLAN.

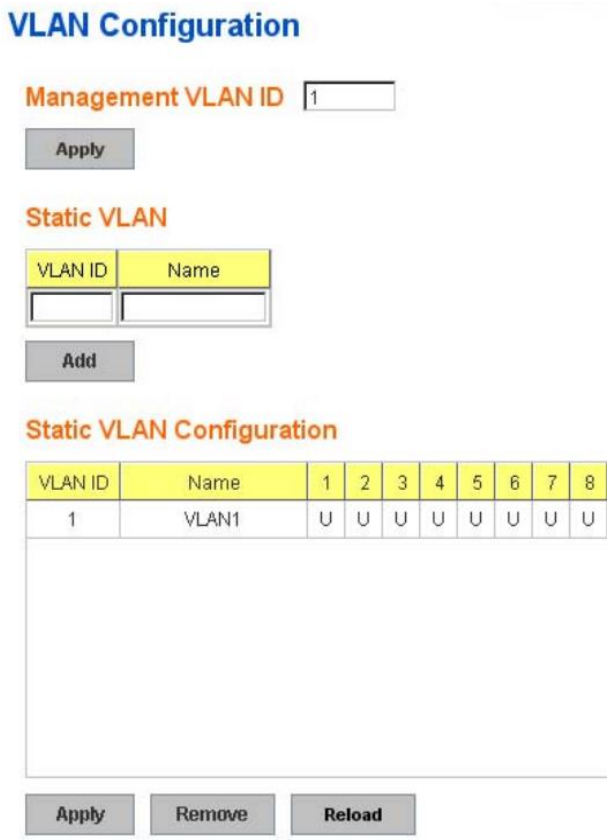


Figure 4-45. VLAN Configuration Screen

Management VLAN ID: The switch supports management VLAN. The management VLAN ID is the VLAN ID of the CPU interface so that only member ports of the management VLAN can ping and access the switch. The default management VLAN ID is 1.

Static VLAN: You can assign a VLAN ID and VLAN Name for new VLAN here.

VLAN ID: Is used by the switch to identify different VLANs. Valid VLAN ID is between 1 and 4094. 1 is the default VLAN.

VLAN Name: Is a reference for network administrator to identify different VLANs. The available character is 12 for you to input. If you don't input VLAN name, the system will automatically assign VLAN name for the VLAN. The rule is VLAN (VLAN ID).

The steps to create a new VLAN: Type VLAN ID and NAME, and press *Add* to create a new VLAN. Then you can see the new VLAN in the Static VLAN Configuration table.

After created the VLAN, the status of the VLAN will remain in Unused until you add ports to the VLAN.

Note:

Before you change the management VLAN ID by Web and Telnet, remember that the port attached by the administrator should be the member port of the management VLAN; otherwise the administrator can't access the switch via the network.

Currently JN4508F-M only support max 256 groups VLAN.

Static VLAN Configuration

You can see the created VLANs and specify the egress (outgoing) port rule to be Untagged or Tagged here.

The Figure 4-46 below shows the Static VLAN Configuration table. You can see that new VLAN 3 (test) is created and the Egress rules of the ports are not configured now.

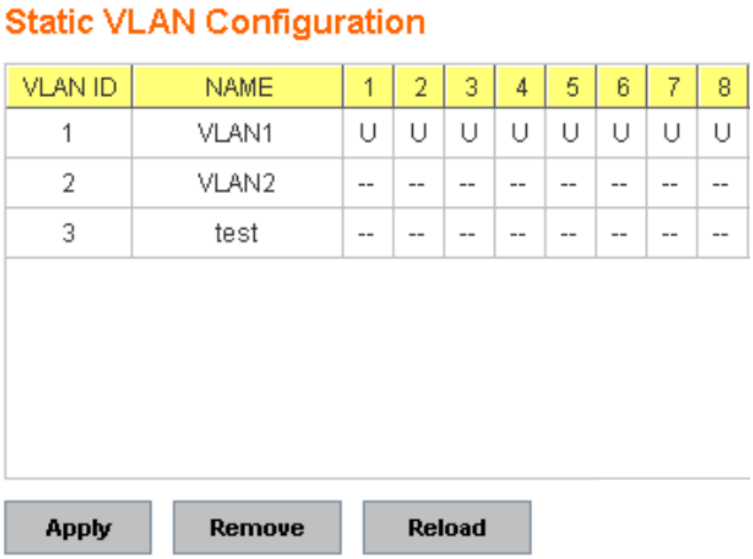


Figure 4-46. Static VLAN Configuration

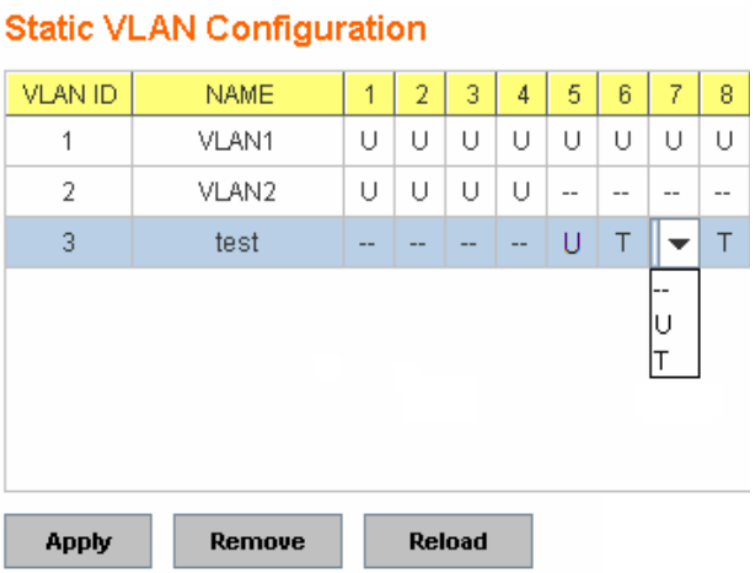


Figure 4-47. Static VLAN Egress Configuration

-- Not available

U Untag: Indicates that egress/outgoing frames are not VLAN tagged.

T Tag: Indicates that egress/outgoing frames are to be VLAN tagged.

Steps to configure Egress rules: Select the VLAN ID. Entry of the selected VLAN turns to light blue. Assign Egress rule of the ports to U or T. Press *Apply* to apply the setting. If you want to remove one VLAN, select the VLAN entry. Then press *Remove* button.

GVRP configuration

GVRP allows users to set-up VLANs automatically rather than manual configuration on every port of every switch in the network.

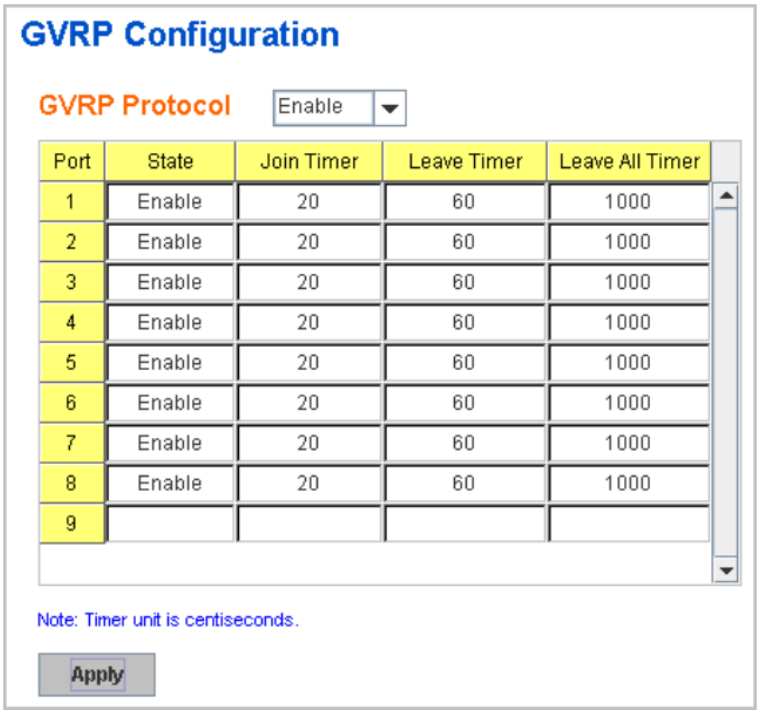


Figure 4-48. GVRP Configuration

GVRP Protocol: Allow user to enable/disable GVRP globally.

State: After enable GVRP globally, here still can enable/disable GVRP by port.

Join Timer: Controls the interval of sending the GVRP Join BPDU. An instance of this timer is required on a per-Port, per-GARP Participant basis.

Leave Timer: Control the time to release the GVRP reservation after received the GVRP Leave BPDU. An instance of the timer is required for each state machine that is in the LV state.

Leave All Timer: Controls the period to initiate the garbage collection of registered VLAN. The timer is required on a per-Port, per-GARP Participant basis.

VLAN Table

This table shows you current settings of your VLAN table, including VLAN ID, Name, Status, and Egress rule of the ports.

Figure 4-49. VLAN Table

VLAN ID: ID of the VLAN.

Name: Name of the VLAN.

Status: Static shows this is a manually configured static VLAN. Unused means this VLAN is created by UI/CLI and has no member ports. This VLAN is not workable yet. Dynamic means this VLAN is learnt by GVRP.

After created the VLAN, the status of this VLAN will remain in Unused status until you add ports to the VLAN.

CLI Commands of the VLAN

Command Lines of the VLAN port configuration, VLAN configuration and VLAN table display.

Description	CLI Command
VLAN Port Configuration	
VLAN Port PVID	Switch(config-if)# switchport trunk native vlan 2 Set port default vlan id to 2 success
Port Accept Frame Type	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!
Ingress Filtering (for fast Ethernet port 1)	Switch(config)# interface fa1 Switch(config-if)# ingress filtering enable ingress filtering enable Switch(config-if)# ingress filtering disable ingress filtering disable
Egress rule – Untagged (for VLAN 2)	Switch(config-if)# switchport access vlan 2 switchport access vlan - success
Egress rule – Tagged (for VLAN 2)	Switch(config-if)# switchport trunk allowed vlan add 2
Display – Port Ingress Rule (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
Display – Port Egress Rule (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
VLAN Configuration	
Create 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.
Remove VLAN	Switch(config)# no vlan 2 no vlan success Note: You can only remove the VLAN when the VLAN is in unused mode.
VLAN Name	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.
VLAN description	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.
IP address of the 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
Create multiple VLANs (VLAN 5-10)	Switch(config)# interface vlan 5-10
Shut down VLAN	Switch(config)# interface vlan 2 Switch(config-if)# shutdown Switch(config-if)# no shutdown ->Turn on the VLAN
Display – VLAN table	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
Display – VLAN interface information	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
GVRP configuration	
GVRP enable/disable	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!
Configure GVRP timer Join timer /Leave timer/ LeaveAll 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
Management VLAN	
Management VLAN	Switch(config)# int vlan 1 (Go to management VLAN) Switch(config-if)# no shutdown
Display	Switch# show running-config …. ! interface vlan1 ip address 192.168.10.17/24 ip igmp no shutdown ! ….

Table 4-13. CLI Commands for VLAN Port

Private VLAN

The private VLAN helps to resolve the primary VLAN ID shortage, client ports' isolation and network security issues. The Private VLAN provides primary and secondary VLAN within a single switch.

Primary VLAN: The uplink port is usually the primary VLAN. A primary VLAN contains promiscuous ports that can communicate with lower Secondary VLANs.

Secondary VLAN: The client ports are usually defined within secondary VLAN. The secondary VLAN includes Isolated VLAN and Community VLAN. The client ports can be isolated VLANs or can be grouped in the same Community VLAN. The ports within the same community VLAN can communicate with each other. However, the isolated VLAN ports can Not. The figure shows the typical Private VLAN network. The SCADA/Public Server or NMS workstation is usually located in primary VLAN. The clients PCs or Rings are located within Secondary.

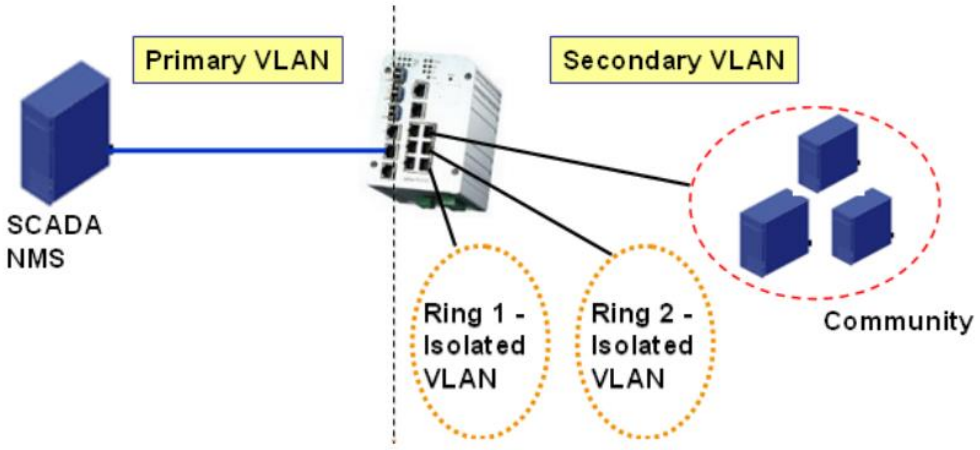


Figure 4-50. Private VLAN Example

Private VLAN (PVLAN) Configuration group enables you to Configure PVLAN, PVLAN Port and see the PVLAN Information.

PVLAN Configuration

PVLAN Configuration PVLAN Configuration allows you to assign Private VLAN type. After created VLAN in VLAN Configuration page, the available VLAN ID will display here. Choose the Private VLAN types for each VLAN you want configure.

None: The VLAN is Not included in Private VLAN.

Primary: The VLAN is the Primary VLAN. The member ports can communicate with secondary ports.

Isolated: The VLAN is the Isolated VLAN. The member ports of the VLAN are isolated.

Community: The VLAN is the Community VLAN. The member ports of the VLAN can communicate with each other.

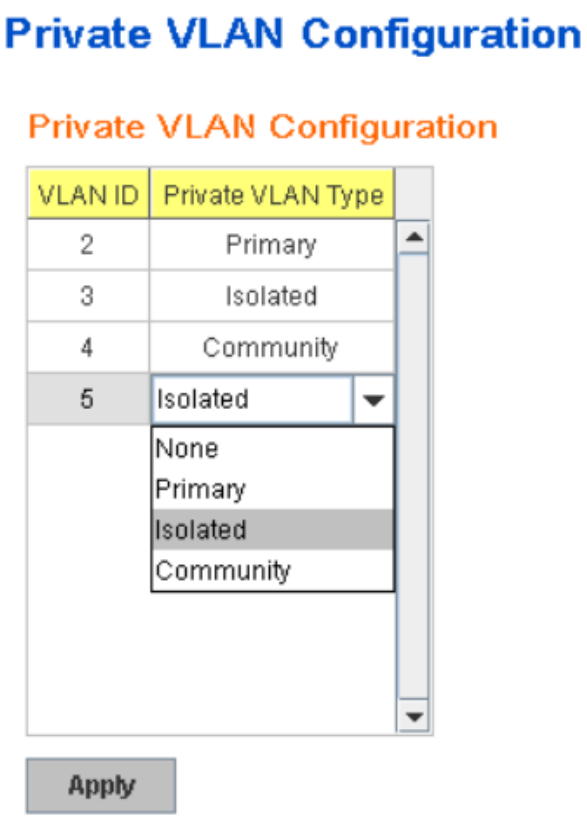


Figure 4-51. Private VLAN Configuration

PVLAN Port Configuration

PVLAN Port Configuration page allows configure Port Configuration and Private VLAN Association.

Private VLAN Association

Secondary VLAN: After the Isolated and Community VLAN Type is assigned in Private VLAN Configuration page, the VLANs are belonged to the Secondary VLAN and displayed here.

Primary VLAN: After the Primary VLAN Type is assigned in Private VLAN Configuration page, the secondary VLAN can associate to the Primary VLAN ID. Select the Primary VLAN ID here.

Note:

Before configuring PVLAN port type, the Private VLAN Association should be done first.

Port Configuration

PVLAN Port Type:

Normal: The Normal port is None PVLAN ports, it remains its original VLAN setting.

Host: The Host type ports can be mapped to the Secondary VLAN.

Promiscuous: The promiscuous port can be associated to the Primary VLAN.

VLAN ID: After assigned the port type, the web UI display the available VLAN ID the port can associate to.

For example:

1. **VLAN Create**: VLAN 2-5 are created in VLAN Configuration page.

2. **Private VLAN Type**: VLAN 2-5 has its Private VLAN Type configured in Private VLAN Configuration page. VLAN 2 is belonged to Primary VLAN. VLAN 3-5 are belonged to secondary VLAN (Isolated or Community).
3. **Private VLAN Association**: Associate VLAN 3-5 to VLAN 2 in Private VLAN Association first.
4. **Private VLAN Port Configuration** VLAN 2 – Primary -> The member port of VLAN 2 is promiscuous port. VLAN 3 – Isolated -> The Host port can be mapped to VLAN 3. VLAN 4 – Community -> The Host port can be mapped to VLAN 3. VLAN 5 – Community -> The Host port can be mapped to VLAN 3.
5. **Result**: VLAN 2 -> VLAN 3, 4, 5; member ports can communicate with ports in secondary VLAN. VLAN 3 -> VLAN 2, member ports are isolated, but it can communicate with member port of VLAN 2.. VLAN 4 -> VLAN 2, member ports within the community can communicate with each other and communicate with member port of VLAN 2. VLAN 5 -> VLAN 2, member ports within the community can communicate with each other and communicate with member port of VLAN 2.

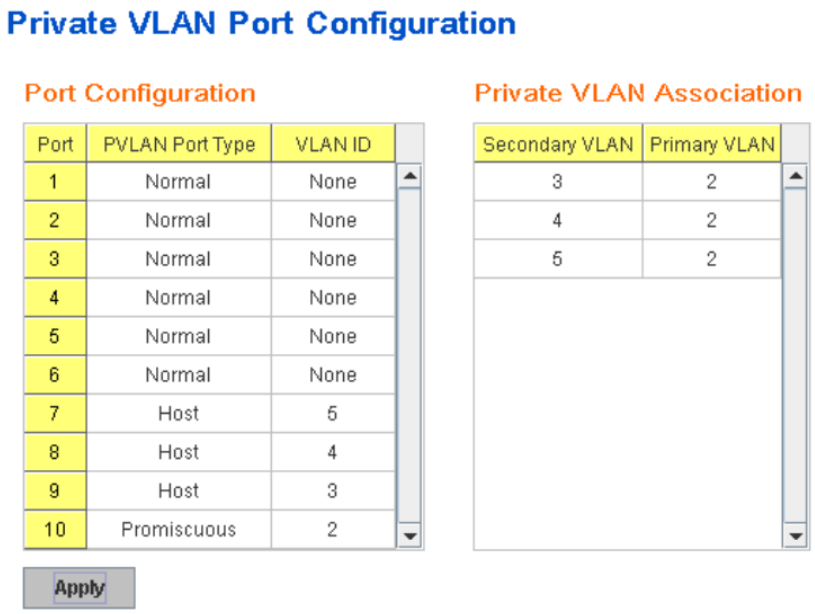


Figure 4-52. Private VLAN Ports Configuration

Private VLAN Information

The Figure 4-53 shows the Private VLAN information.

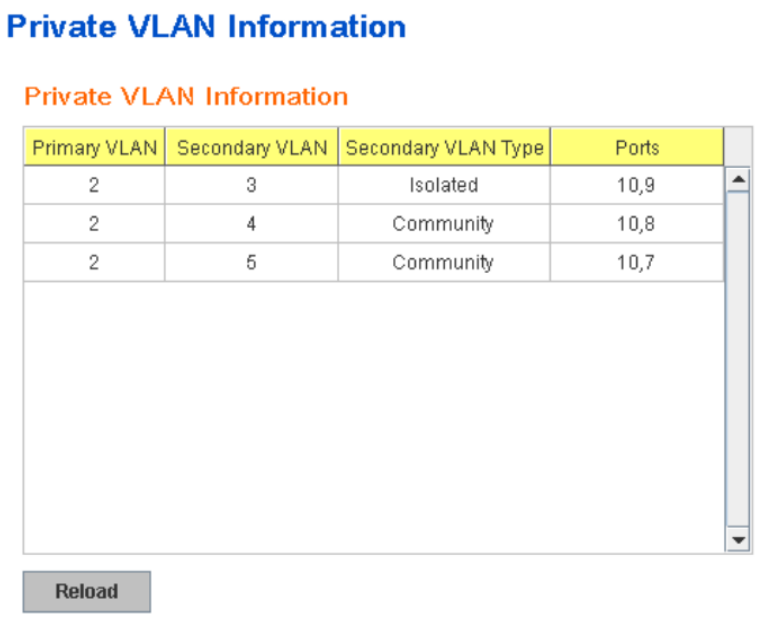


Figure 4-53. Private VLAN Information

CLI Command of the PVLAN

Command Lines of the Private VLAN configuration.

Description	CLI Command
Private VLAN Configuration	
Create 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>
Private VLAN Port Configuraiton	
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 Set the mode to private-vlan promiscuous
Promiscuous Port Type	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
Private VLAN Information	
Private VLAN Information	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 -------- -------- --------
PVLAN Type	Switch# show vlan private-vlan type Vlan Type Ports -------- -------- -------- 2 primary gi10 3 isolated gi9 4 community gi8 5 community fa7,gi9 10 primary --------
Host List	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
Running Config Information	Switch# show run Building configuration Current configuration:

Private VLAN Type	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

Table 4-14. CLI Commands for PVLAN

Traffic Prioritization

Quality of Service (QoS) provides a traffic prioritization mechanism that allows users to deliver better service to certain flows. QoS can also help to alleviate congestion problems and ensure that high priority traffic is delivered first. This section allows you to configure Traffic Prioritization settings for each port in regards to setting priorities.

The JN4508F-M QoS supports 4 physical queues, weighted fair queuing (WRR) and Strict Priority scheme, which follows 802.1p COS tag and IPv4 TOS/DiffServ information to prioritize the traffic of your industrial network.

QoS Setting

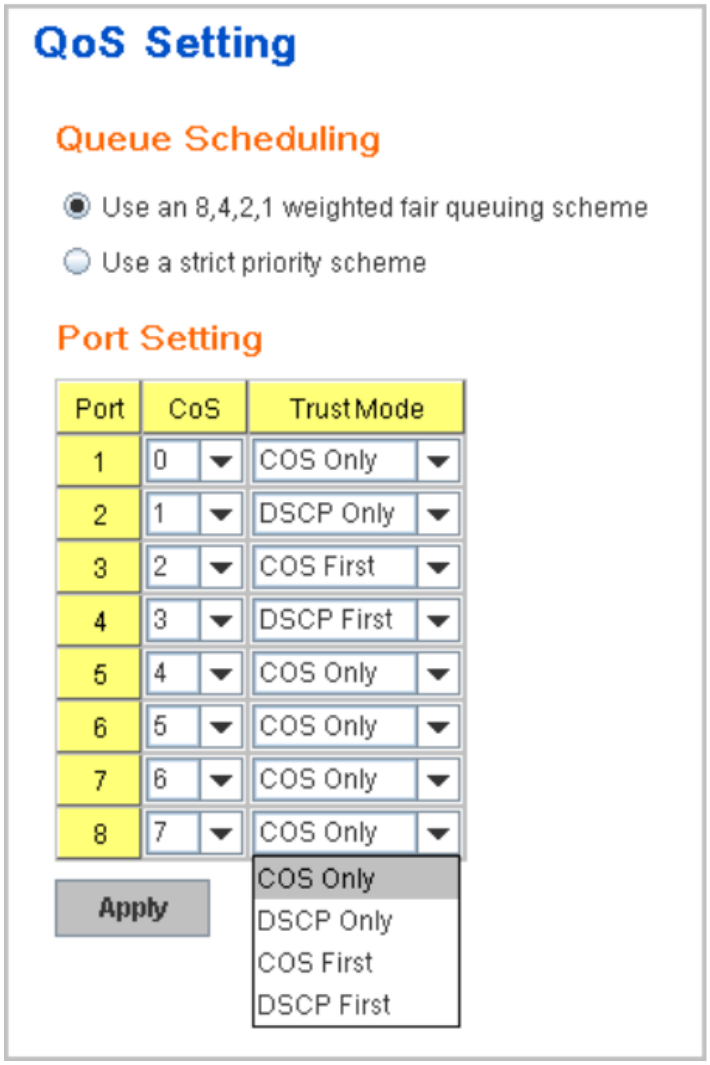


Figure 4-54. QoS Setting Screen

Queue Scheduling

Use an 8,4,2,1 weighted fair queuing scheme. This is also known as WRR (Weight Round Robin). JN4508F-M will follow the 8:4:2:1 rate to process the packets in a queue from the highest priority to the lowest. For example, the system will simultaneously process 8 packets with the highest priority in the queue, 4 packets with middle priority, 2 packets with low priority, and 1 packet with the lowest priority.

Use a strict priority scheme. Packets with the highest priority in the queue will always be processed first.

Port Setting

The Priority column is to indicate the default port priority value for untagged or priority-tagged frames. When JN4508F-M receives the frames, JN4508F-M will assign the value to the priority. You can enable 0, 1, 2, 3, 4, 5, 6 or 7 to the port.

Trust Mode: This indicates Queue Mapping types for you to select.

CoS Only: Port priority will only follow CoS-Queue Mapping that you have assigned.

DSCP Only: Port priority will only follow DSCP-Queue Mapping that you have assigned.

CoS first: Port priority will follow CoS-Queue Mapping first, and then DSCP-Queue Mapping rule.

DSCP first: Port priority will follow DSCP-Queue Mapping first, and then CoS-Queue Mapping rule.

The default priority type is CoS Only. The system will provide a default CoS-Queue table that you can refer to for the next command.

After configuring, click the *Apply* button to enable the settings.

CoS-Queue Mapping

This area is where the user can set CoS values to the Physical Queue mapping table. Since the switch fabric of JN4508F-M supports 4 physical queues (Lowest, Low, Middle and High), users should assign CoS value to the level of the physical queue.

With the JN4508F-M users can easily assign the mapping table or follow suggestions from the 802.1p standard. It uses 802.1p standards for its default values. You will find that the CoS values 1 and 2 are mapped to physical Queue 0 (lowest queue). CoS values 0 and 3 are mapped to physical Queue 1, (low/normal physical queue), CoS values 4 and 5 are mapped to physical Queue 2 (middle physical queue), and CoS values 6 and 7 are mapped to physical Queue 3 (highest physical queue).

Figure 4-55. CoS Queue Mapping Screen

After configuring, click the *Apply* button to enable the settings.

DSCP-Queue Mapping

This is where users can change DSCP values to a Physical Queue mapping table. Since the switch fabric of the JN4508F-M supports 4 physical queues, (lowest, low, middle and high), users should assign a DSCP value to the level of the physical queue. With the JN4508F-M users can easily change the mapping table to follow the upper layer 3 switches or routers' DSCP setting.

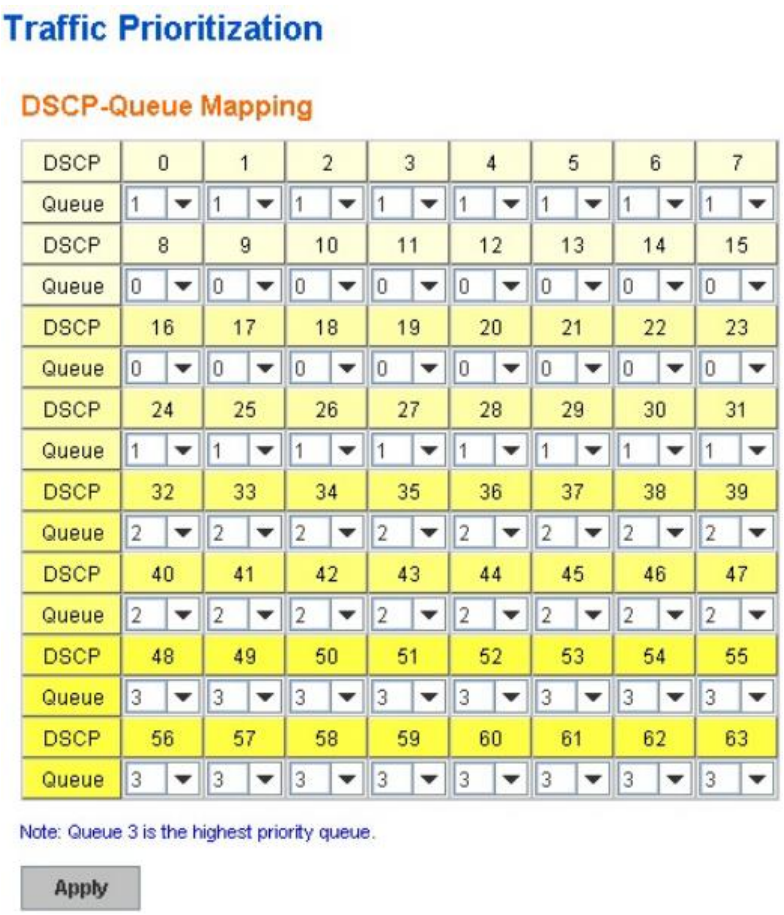


Figure 4-56. DSCP Queue Mapping Example

After configuring, click the *Apply* button to enable the settings.

CLI Commands for Traffic Prioritization

Feature	Command Line
QoS Setting	
Queue Scheduling – Strict Priority	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>
Queue Scheduling WRR	Switch (config)# qos queue-sched wrr
Port Setting – priority (Default Port Priority)	Switch(config)# interface fa1 Switch(config-if)# qos priority DEFAULT-PRIORITY Assign an priority (3 highest Switch(config-if)# qos cos 3 The default port priority value is set 3 ok. **Note**: When change the port setting, you should Select The specific port first. Ex: fa1 means fast Ethernet port 1.
Port Setting – Trust Mode- CoS Only	Switch(config)# interface fa1 Switch(config-if)# qos trust cos The port trust is set CoS only ok.
Port Setting – Trust Mode- CoS Frist	Switch(config)# interface fa1 Switch(config-if)# qos trust cos-first The port trust is set CoS first ok.
Port Setting – Trust Mode- DSCP Only	Switch(config)# interface fa1 Switch(config-if)# qos trust dscp The port trust is set DSCP only ok.
Port Setting – Trust	Switch(config)# interface fa1

Mode- DSCP First	Switch(config-if)# qos trust dscp-first The port trust is set DSCP first ok.
Display – Queue Scheduling	Switch# show qos queue-sched QoS queue scheduling scheme: Weighted Round Robin (Use an 8,4,2,1 weight)
Display – Port Setting Trust Mode	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
Display – Port Setting – CoS (Port Default Priority)	Switch# show qos port-cos Port Default Cos: Port CoS ----- ----- 1 0 2 0 3 0 4 0 5 0 6 0 7 0 8 0
CoS-Queue Mapping	
Format	Switch(config)# qos cos-map PRIORITY Assign an priority (7 highest) Switch(config)# qos cos-map 1 QUEUE Assign an queue (0-3) **Note**: Format: qos cos-map priority_value queue_value
Map CoS 0 to Queue 1	Switch(config)# qos cos-map 0 1 The CoS to queue mapping is set ok.
Map CoS 1 to Queue 0	Switch(config)# qos cos-map 1 0 The CoS to queue mapping is set ok.
Map CoS 2 to Queue 0	Switch(config)# qos cos-map 2 0 The CoS to queue mapping is set ok.
Map CoS 3 to Queue 1	Switch(config)# qos cos-map 3 1 The CoS to queue mapping is set ok.
Map CoS 4 to Queue 2	Switch(config)# qos cos-map 4 2 The CoS to queue mapping is set ok.
Map CoS 5 to Queue 2	Switch(config)# qos cos-map 5 2 The CoS to queue mapping is set ok.
Map CoS 6 to Queue 3	Switch(config)# qos cos-map 6 3 The CoS to queue mapping is set ok.
Map CoS 7 to Queue 3	Switch(config)# qos cos-map 7 3 The CoS to queue mapping is set ok.
Display – CoS-Queue mapping	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
DSCP-Queue Mapping	
Format	Switch(config)# qos dscp-map PRIORITY Assign an priority (63 highest) Switch(config)# qos dscp-map 0 QUEUE Assign an queue (0-3) Format: qos dscp-map priority_value queue_value
Map DSCP 0 to Queue 1	Switch (config)# qos dscp-map 0 1 The TOS/DSCP to queue mapping is set ok.
Display – DSCO-Queue mapping	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

Table 4-15. Command Lines for Traffic Prioritization Configuration

Multicast Filtering

For multicast filtering, JN4508F-M uses IGMP Snooping technology. The IGMP (Internet Group Management Protocol) is an Internet Protocol that provides a way for an internet device to report its multicast group membership to adjacent routers. Multicasting allows one computer on the internet to send data to a multitude of other computers that have identified themselves as being interested in receiving the originating computers data.

Multicasting is useful for such applications as updating the address books of mobile computer users in the field, sending out newsletters to a distribution list, and broadcasting streaming media to an audience that has tuned into the event by setting up multicast group membership.

In effect, IGMP Snooping manages multicast traffic by making use of switches, routers, and hosts that support IGMP. Enabling IGMP Snooping allows the ports to detect IGMP queries, report packets, and manage multicast traffic through the switch. IGMP has three fundamental types of messages, as shown in Table 4-16:

Message	Description
Query	A message sent from the querier (an IGMP router or a switch) which asks for a response from each host that belongs to the multicast group
Report	A message sent by a host to the querier to indicate that the host wants to be or is a member of a given group indicated in the report message
Leave Group	A message sent by a host to the querier to indicate that the host has quit as a member of a specific multicast group

Table 4-16. IGMP Messages

You can enable IGMP Snooping and IGMP Query functions here. You will see the information of the IGMP Snooping function in this section, including different multicast member ports and IP multicast addresses that range from 224.0.0.0 to 239.255.255.255.

IGMP Snooping

This page is to enable IGMP Snooping feature, assign IGMP Snooping for specific VLAN, and view IGMP Snooping table from dynamic learnt or static manual key-in. JN4508F-M Managed Switch support IGMP snooping V1/V2/V3 automatically and IGMP query V1/V2.

IGMP Snooping, you can select Enable or Disable here. After enabling IGMP Snooping, you can then enable IGMP Snooping for specific VLAN. You can enable IGMP Snooping for some VLANs so that some of the VLANs will support IGMP Snooping and others won't.

To assign IGMP Snooping to VLAN, please select the checkbox of VLAN ID or select *Select All* checkbox for all VLANs. Then press *Enable*. In the same way, you can also *Disable* IGMP Snooping for certain VLANs.

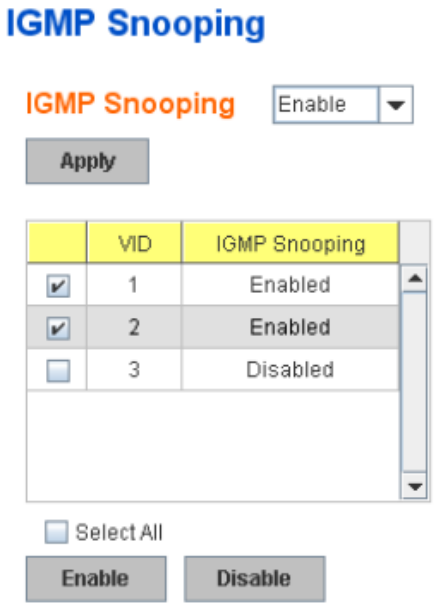


Figure 4-57. IGMP Snooping Configuration Screen

IGMP Snooping Table: In the table, you can see the multicast group IP address and the member ports of the multicast group. The JN4508F-M supports 256 multicast groups. Click the *Reload* button to refresh the table.

Figure 4-58. IGMP Snooping Table

IGMP Query

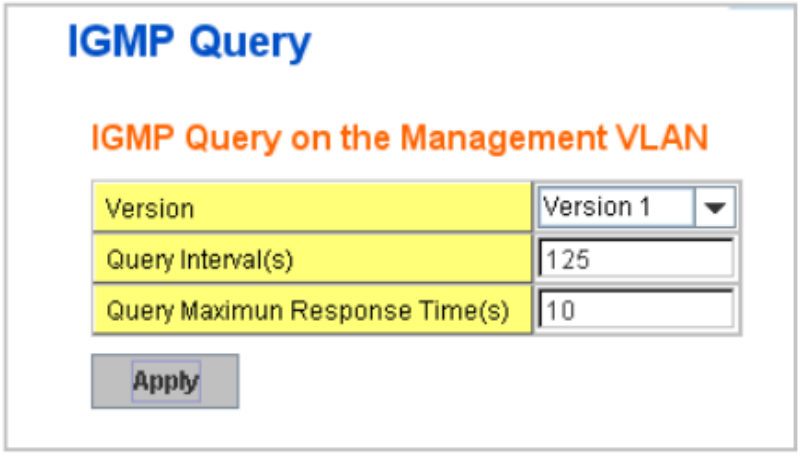


Figure 4-59. IGMP Query Configuration Screen

This chapter allows user to configure the IGMP Query feature. Since JN4508F-M can only be configured by the member ports of the management VLAN, so that the IGMP Query can only be enabled on the management VLAN. If you want to run IGMP Snooping feature in several VLANs, you should notice that whether each VLAN have their own IGMP Querier first.

The IGMP querier periodically sends query packets to all end-stations on the LANs or VLANs that are connected to it. For networks with more than one IGMP querier, a switch with the lowest IP address becomes the IGMP querier.

In the IGMP Query selection, you can select V1, V2 or Disable. V1 means IGMP V1 General Query. The query will be forwarded to all multicast groups in the VLAN. V2 means IGMP V2 Specific Query. The query will be forwarded to specific multicast groups. Disable allows you to disable the IGMP Query.

Query Interval(s): The period of query sent by querier.

Query Maximum Response Time: The span querier detect to confirm there are no more directly connected group members on a LAN.

Once you finish configuring the settings, click the *Apply* button to apply your configuration.

Force Filtering

Figure 4-60. Force Filtering

The Force filtering function allows the switch to filter the unknown-multicast data flow. If Force filtering is enabled, all the unknown multicast data will be discarded.

CLI Commands of the Multicast Filtering

Feature	Command Line
IGMP Snooping	

IGMP Snooping Global	Switch(config)# ip igmp snooping IGMP snooping is enabled globally. Please specify on which vlans IGMP snooping enables
IGMP Snooping - VLAN	Switch(config)# ip igmp snooping vlan VLANLIST allowed vlan list all all existed vlan Switch(config)# ip igmp snooping vlan 1-2 IGMP snooping is enabled on VLAN 1-2
Disable IGMP Snooping - Global	Switch(config)# no ip igmp snooping IGMP snooping is disabled globally ok.
Disable IGMP Snooping - VLAN	Switch(config)# no ip igmp snooping vlan 3 IGMP snooping is disabled on VLAN 3.
Display – IGMP Snooping Setting	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 (Go to management VLAN) Switch(config-if)# ip igmp v1
IGMP Query V2	Switch(config)# int vlan 1 (Go to management VLAN) Switch(config-if)# ip igmp
IGMP Query version	Switch(config-if)# ip igmp version 1 Switch(config-if)# ip igmp version 2
Disable	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 ! …….
Force filtering	
Enable Force filtering Disable Force filtering	Switch(config)# mac-address-table multicast filtering Filtering unknown multicast addresses ok! Switch(config)# no mac-address-table multicast filtering Flooding unknown multicast addresses ok!

Table 4-17. Command Lines of the Multicast Filtering Configuration

SNMP

Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. JN4508F-M supports SNMP v1, v2c and v3.

A SNMP managed network consists of two main components: agents and a manager. An agent is a management software module that resides in a managed switch. An agent translates the local management information from the managed device into a SNMP-compatible format. The manager is the console through the network.

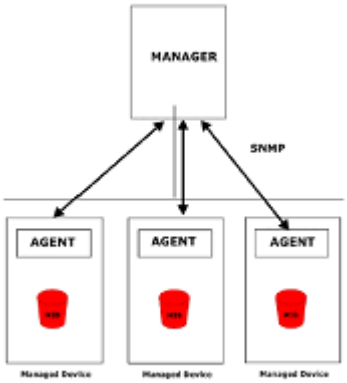


Figure 4-61. SNMP Architecture Example

SNMP Configuration

This allows users to configure the SNMP V1/V2c Community. The community string can be viewed as a password because SNMP V1/ V2c doesn't request you to enter a password before accessing the SNMP agent.

The community includes 2 privileges: Read Only, and Read and Write.

With Read Only privileges, you will only have the ability to read the values in the MIB tables. The default community string is set to Public.

With Read and Write privileges, you will have the ability to read and set the values in the MIB tables. The default community string is set to Private.

JN4508F-M allows users to assign 4 community strings. Type in each community string and select its privilege. Then press the *Apply* button.

Note:

When you first install the device onto your network, we highly recommend that you change the community string. Because most SNMP management applications use Public and Private as their default community name, this may cause a leak in network security.

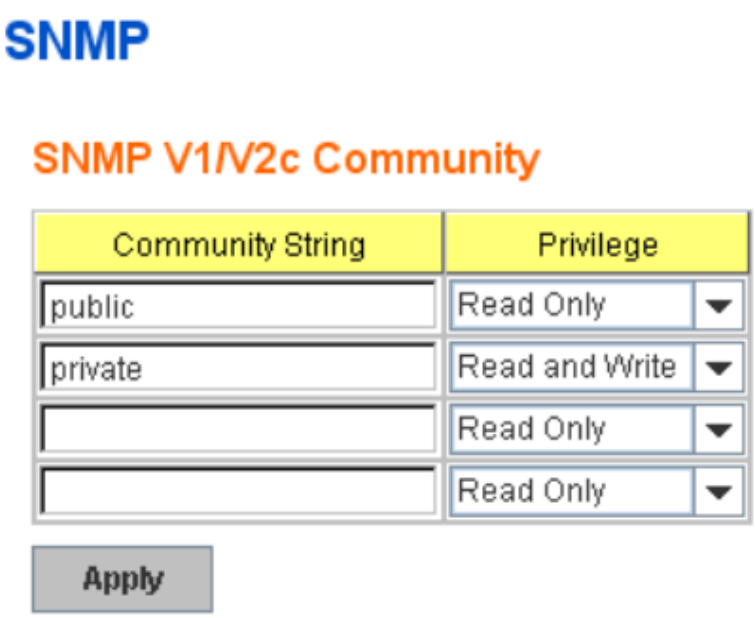


Figure 4-62. SNMP V1/V2c Configurations

SNMP v3 Profile

SNMP v3 can provide more security functions when the user performs remote management through SNMP protocol. It delivers SNMP information to the administrator with user authentication; all of data between JN4508F-M and the administrator are encrypted to ensure secure communication.

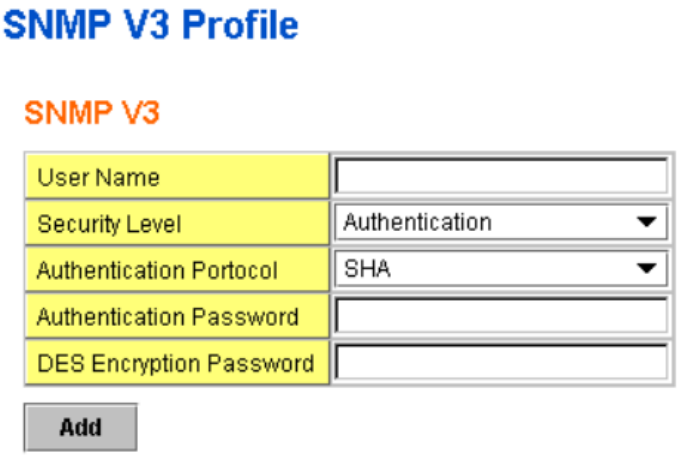


Figure 4-63. SNMP V3 Configurations

Security Level: Here the user can select the following levels of security: None, User Authentication, and Authentication with privacy.

Authentication Protocol: Here the user can select either MD5 (Message-Digest algorithm 5) or SHA (Secure Hash Algorithm). MD5 is a widely used cryptographic hash function with a 128-bit hash value. SHA (Secure Hash Algorithm) hash functions refer to five Federal Information Processing Standard-approved algorithms for computing a condensed digital representation. JN4508F-M provides 2 user authentication protocols in MD5 and SHA. You will need to configure SNMP v3 parameters for your SNMP tool with the same authentication method.

Authentication Password: Here the user enters the SNMP v3 user authentication password.

DES Encryption Password: Here the user enters the password for SNMP v3 user DES Encryption.

SNMP Traps

SNMP Trap is a notification feature defined by SNMP protocol. All SNMP management applications can understand this type of trap information. You will not need to install new applications to read the notification information.

This page allows users to Enable SNMP Trap, configure the SNMP Trap server IP, Community name, and trap Version V1 or V2. After the configuration, you will be able to see the changes made to the SNMP pre-defined standard traps and the pre-defined traps. The pre-defined traps can be found in private MIB.

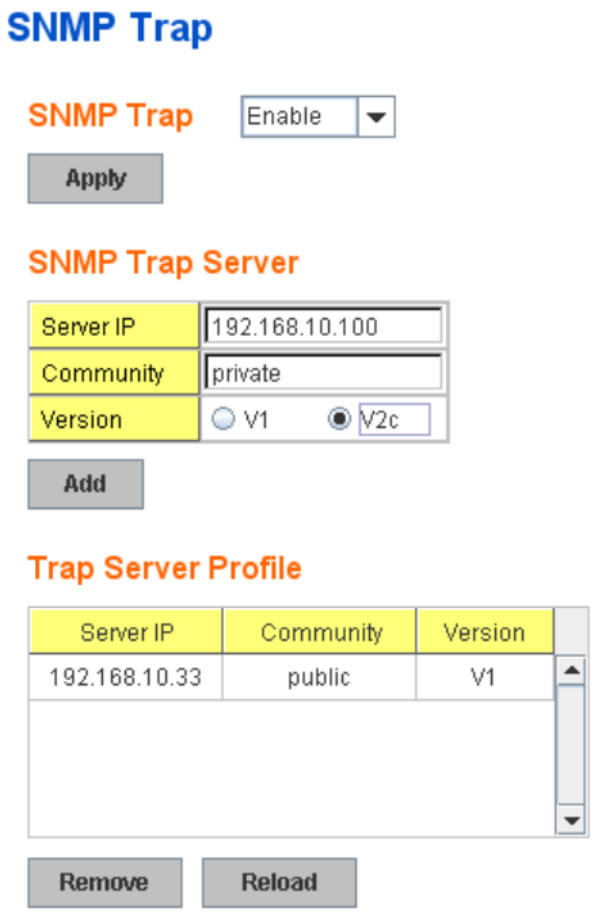


Figure 4-64. SNMP Traps Configuration Screen

CLI Commands for SNMP

Feature	Command line
SNMP Community	
Read Only Community	Switch(config)# snmp-server community public ro community string add ok
Read Write Community	Switch(config)# snmp-server community private rw community string add ok
SNMP Trap	
Enable Trap	Switch(config)# snmp-server enable trap Set SNMP trap enable ok.
SNMP Trap Server IP without specific community name	Switch(config)# snmp-server host 192.168.10.33 SNMP trap host add OK.
SNMP Trap Server IP with version 1 and community	Switch(config)# snmp-server host 192.168.10.33 version 1 Private SNMP trap host add OK. **Note**: private is the community name, version 1 is the SNMP version

SNMP Trap Server IP with version 2 and community	Switch(config)# snmp-server host 192.168.10.33 version 2 Private SNMP trap host add OK.
Disable SNMP Trap	Switch(config)# no snmp-server enable trap Set SNMP trap disable ok.
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 ……..

Table 4-18. Command Lines for SNMP Configuration

Security

JN4508f provides several security features for you to secure your connection. The features include Port Security and IP Security.

Port Security

Port Security feature allows you to stop the MAC address learning for specific port. After stopping MAC learning, only the MAC address listed in Port Security List can access the switch and transmit/receive traffic. This is a simple way to secure your network environment and not to be accessed by hackers.

This page allows you to enable Port Security and configure Port Security entry.

Port Security State: Change Port Security State of the port to enable first.

Add Port Security Entry: Select the port, and type VID and MAC address. Format of the MAC address is xxxx.xxxx.xxxx. Ex: 0012.7701.0101. Max volume of one port is 10. So the system can accept 100 Port Security MAC addresses in total.

Port Security List: This table shows you those enabled port security entries. You can click on Remove to delete the entry.

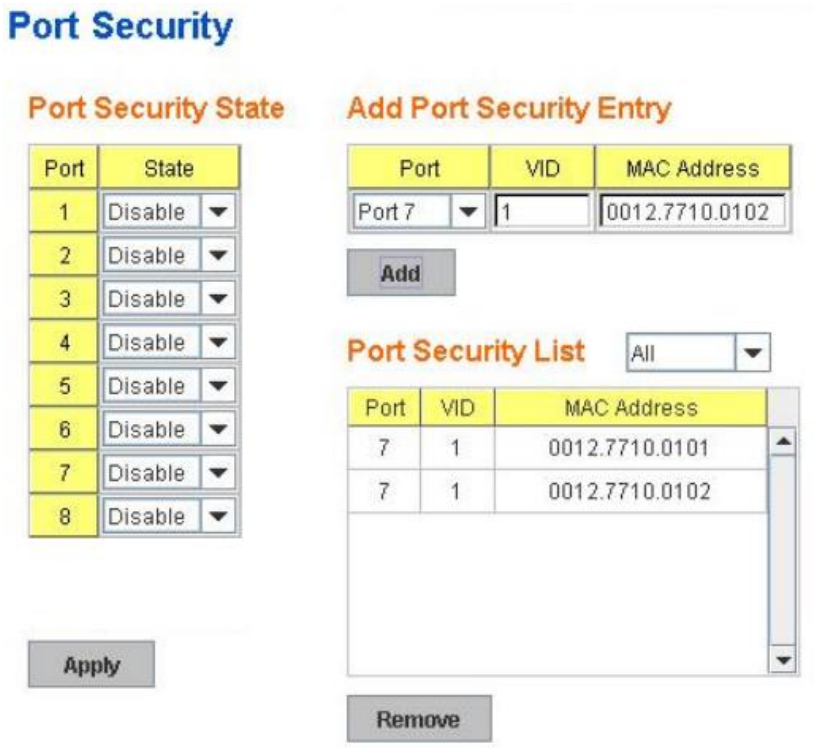


Figure 4-65. Port Security Configurations

Once you finish configuring the settings, click on *Apply*/*Add* to apply your configuration.

IP Security

In the IP Security section, you will be able to set up specific IP addresses to perform authorization for management access to JN4508F-M via web browser or Telnet.

IP Security: Select Enable and Apply to enable IP security function.

Add Security IP: You can assign any PC as an administrator workstation by adding a PC's IP address into the Security IP field. Only these IP addresses will be able to access and manage JN4508F-M. The maximum number of security IP is 10.

Security IP List: This table shows you each security IP address you have added. You can hit *Remove* to delete, and *Reload* to reload the table.

Figure 4-66. IP Security Configuration Screen

Once you have finished configuring the settings, click the *Apply* button to apply your configuration.

IEEE 802.1x

802.1X configuration

IEEE 802.1X is the protocol that performing authentication to obtain access to IEEE 802 LANs. It is port-base network access control. With the function, JN4508F-M could control which connection is available or not.

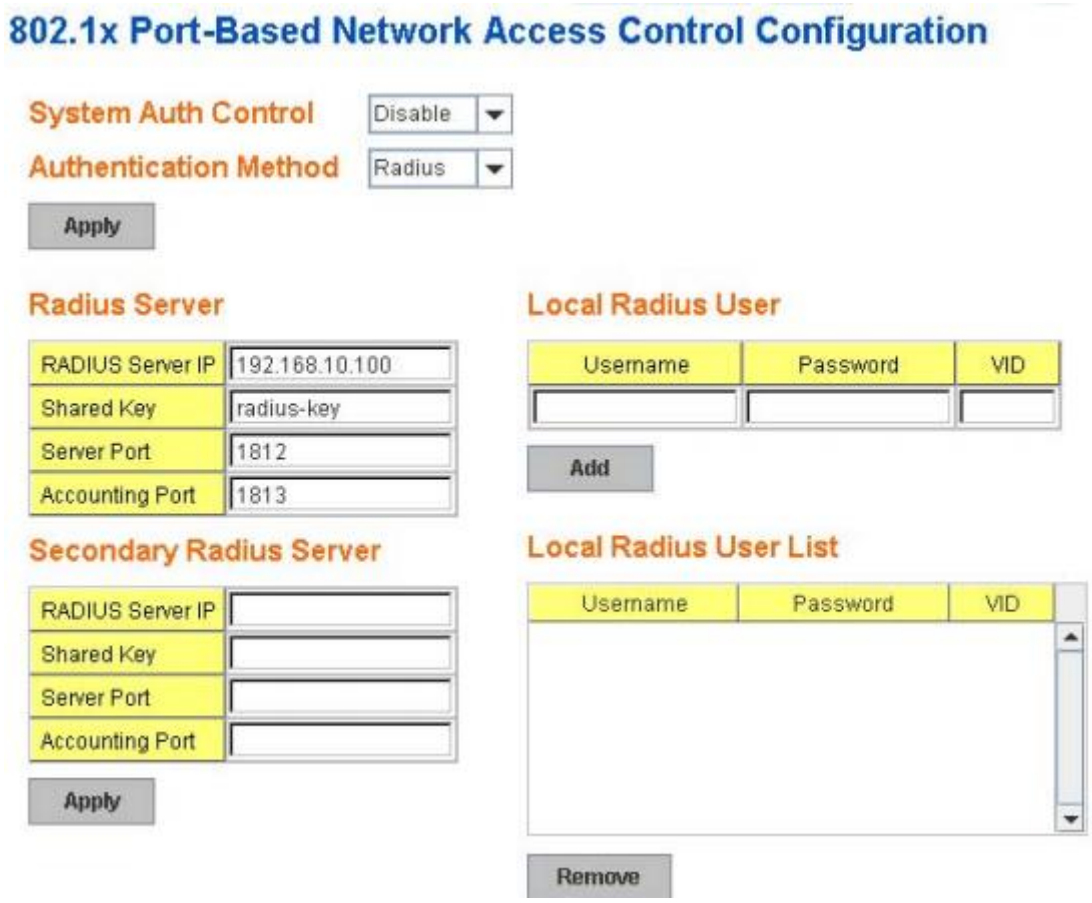


Figure 4-67. Port-Based Network Access Control Configuration

System AuthControl: To enable or disable the 802.1x authentication.

Authentication Method: Radius is an authentication server that provide key for authentication, with this method, user must connect switch to server. If user select Local for the authentication method, switch use the local user data base which can be create in this page for authentication.

Radius Server IP: The IP address of Radius server.

Shared Key: the password for communicate between switch and RadiusServer.

Server Port: UDP port of Radius server.

Accounting Port: Port for packets that contain the information of account login or logout.

Secondary Radius Server IP: Secondary Radius Server could be set in case of the primary radius server down.

802.1X Local User: Here User can add Account/Password for local authentication.

802.1X Local user List: This is a list shows the account information, User also can remove selected account Here.

802.1x Port Configuration

After the configuration of Radius Server or Local user list, user also need configure the authentication mode, authentication behavior, applied VLAN for each port and permitted communication. The following information will explain the port configuration.

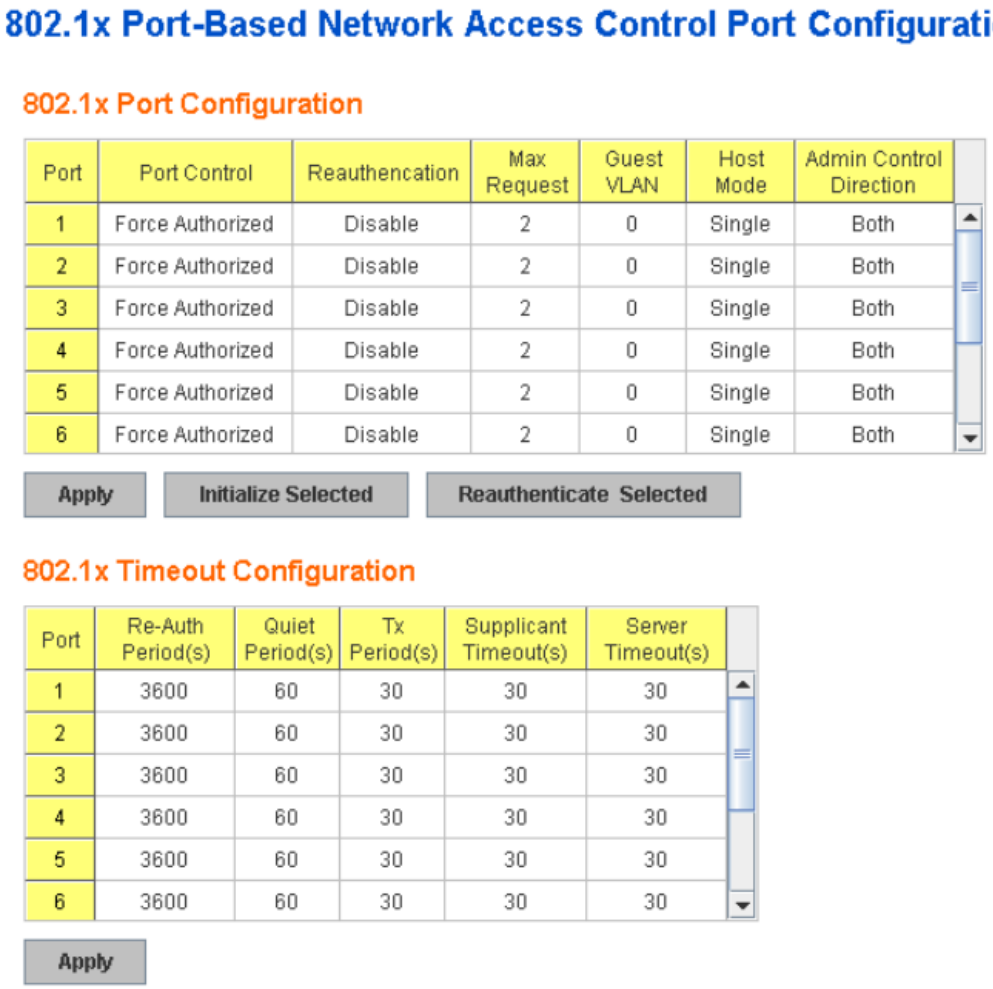


Figure 4-68. Port-Based Network Access Control Port Configuration

Port control: Force Authorized means this port is authorized; the data is free to in/out. Force unauthorized just opposite, the port is blocked. If users want to control this port with Radius Server, please select Auto for port control.

Reauthentication: If enable this field, switch will ask client to re-authenticate. The default time interval is 3600 seconds.

Max Request: the maximum times that the switch allow client request.

Guest VLAN: 0 to 4094 is available for this field. If this field is set to 0, that means the port is blocked after authentication fail. Otherwise, the port will be set to Guest VLAN.

Host Mode: if there are more than one device connected to this port, set the Host Mode to single means only the first PC authenticate success can access this port. If this port is set to multi, all the devices can access this port once any one of them pass the authentication.

Control Direction: determined devices can end data out only or both send and receive.

Re-Auth Period: control the Re-authentication time interval, available number is 1~65535.

Quiet Period: When authentication failed, Switch will wait for a period and try to communicate with radius server again.

Tx period: the time interval of authentication request.

Supplicant Timeout: the timeout for the client authenticating.

Server Timeout: The timeout for server response for authenticating.

Once you finish configuring the settings, click on *Apply* to apply your configuration.

Click Initialize Selected to set the authorize state of selected port to initialize status.

Click Reauthenticate Selected to send EAP Request to supplicant to request reauthentication.

Click Default Selected to reset the configurable 802.1x parameters of selected port to the default values.

802.1X Port Status

Here user can observe the port status for Port control status, Authorize Status, Authorized Supplicant and Oper Control Direction each port.

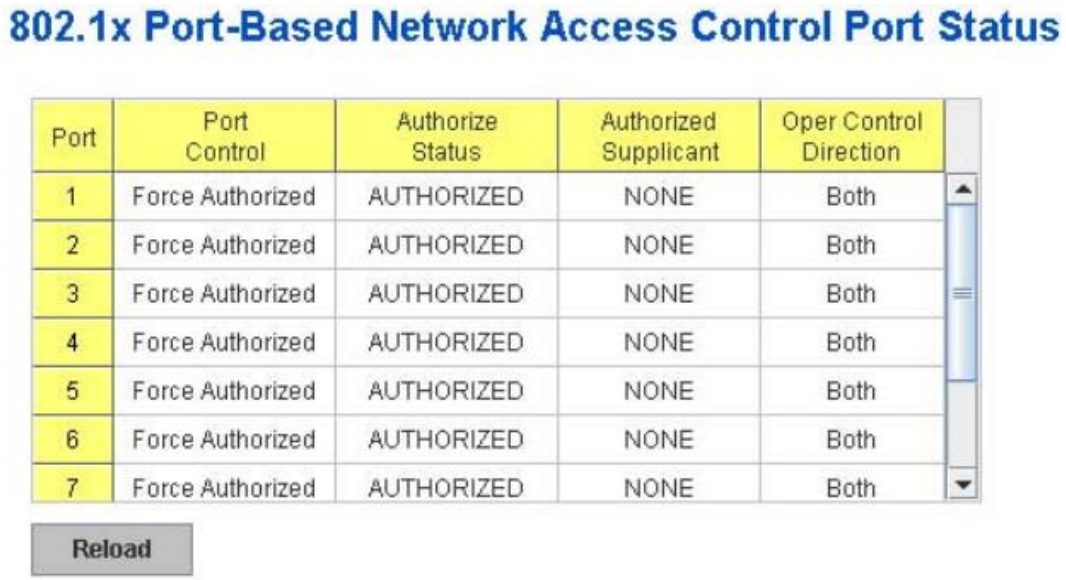


Figure 4-69. Port-Based Network Access Control Port Status

CLI Commands of the Security

Feature	Command line
Port Security	
Add MAC	Switch(config)# mac-address-table static 0012.7701.0101 vlan 1 interface fa1 mac-address-table unicast static set ok!
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.
Disable Port Security	Switch(config-if)# no switchport port-security Enable new MAC addresses learning and aging activities!
Display	Switch# show mac-address-table static Destination Address / Address Type / Vlan / Destination Port 0012.7701.0101 / Static / 1 / fa1
IP Security	
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	
enable disable	Switch(config)# dot1x system-auth-control Switch(config)# Switch(config)# no dot1x system-auth-control Switch(config)#
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

Table 4-19. CLI Command Lines for Security Configuration

Warning

JN4508F-M provides several types of warning features for remote monitoring the status of end devices or the change of your network. The features include Fault Relay, System Log and SMTP E-mail Alert.

Fault Relay Setting

JN4508F-M provides 1 digital output, also known as Relay Output. The relay (DO) contact is energized from normal and will form a close circuit under system fault conditions.The fault conditions include power failure, Ethernet port link fault, Ring topology change, Ping Failure, DI state change or ping remote IP address failure.

From the firmware version 1.1a, the fault relay supports multiple event relay binding function. That means fault realy not only support one event only, it can be assigned multiple event. The condition or term described as following.

Term	Condiction	Description
Power	Power Vdc1 Power Vdc2 Any	Detect power input status. If one of condiction occurred, relay triggered.
Port Link	Port number	Monitoring port link down event
Ring	Ring failure	If ring topology changed
Ping	IP Address: remote device's IP address	If target IP does not reply ping request, then relay active
Ping Reset	IP address: remote device's address Reset Time: duration of output open. Hold Time: duration of Ping hold time.	Ping target device and trigger relay to emulate power reset for remote device, if remote system crash. **Note**: once perform Ping reset, the relay output will form a short circuit.
Dry Output	On period: duration of relay output short (close). Off period: duration of relay output open.	Relay continuous perform On/Off behavior with different duration.
DI	DI number (JN4508F-M supports 1 DI)	Relay trigger when DI states change to Hi or Low

Table 4-20. Faulty Relay Conditions

The Fault relay configuration UI has shown as below:

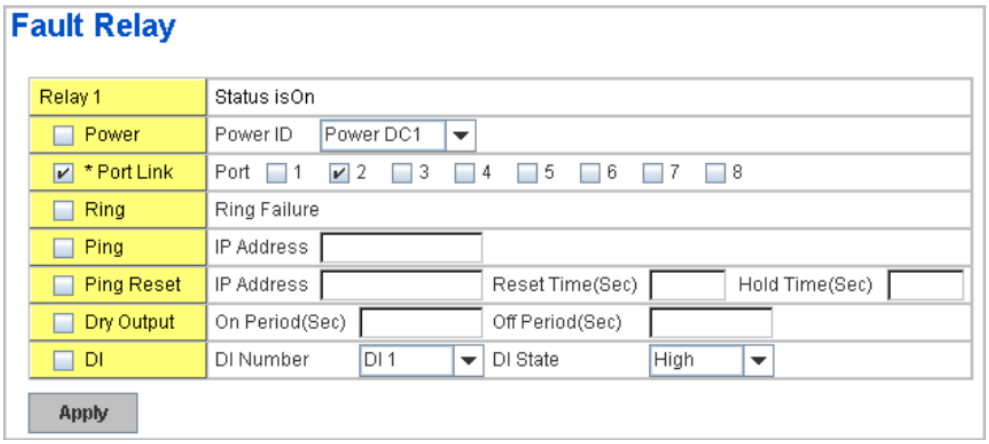


Figure 4-70. Fault Relay Setting Configuration Screen

Relay 1: Show current relay state.

On Period (Sec): Type the period time to turn on Relay Output. Available range of a period is 0-65535 seconds.

Off Period (Sec): Type the period time to turn off Relay Output. Available range of a period is 0-65535 seconds.

Hold Time (Sec): Type the hold time to halts the ping packet.

Event Selection

Event Types can be divided into two basic groups: System Events and Port Events. System Events are related to the overall function of the switch, whereas Port Events related to the activity of specific ports.

System Event	Warning Event is sent when…
Device Cold Start	Power is cut off and then reconnected.
Device Warm Start	Reboot the device by CLI or Web UI.
Power 1 Failure	Power 1 is failure.
Power 2 Failure	Power 2 is failure.

Authentication failure	An incorrect password, SNMP Community String is entered.
Time Synchronize Failure	Accessing to NTP Server is failure.
Fault Relay	The DO/Fault Relay is on.
Super Ring Topology Changes	Master of Super Ring has changed or backup path is activated.
DI1 Change	The Digital Input#1 status is changed.
Port Event	**Warning Event is sent when…**
Link-Up	The port is connected to another device
Link-Down	The port is disconnected (e.g. the cable is pulled out, or the opposing devices turns down)
Both	The link status changed.

Table 4-21. System and Port Events

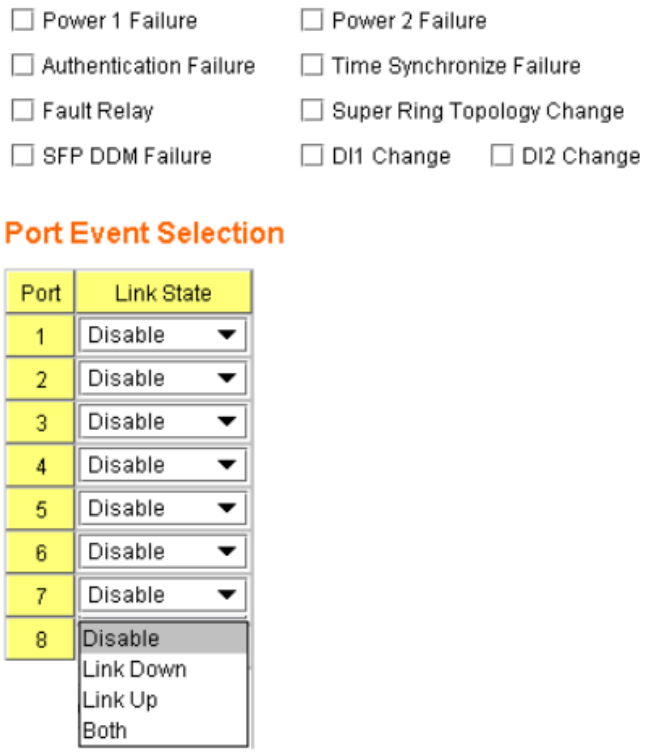


Figure 4-71. System and Port Event Selection

Once you finish configuring the settings, click on *Apply* to apply your configuration.

SysLog Configuration

System Log is useful in providing the system administrator both local and remote monitoring of the switch's history. There are 2 System Log modes provided by JN4508F-M: local mode and remote mode.

Local Mode: In this mode, JN4508F-M will print selected past events (selected in the Event Selection page) to the System Log table of JN4508F-M. You can monitor the system logs in the [Monitor and Diag] / [Event Log] page.

Remote Mode: The remote mode is also known as Server mode in JN4508F-M. In this mode, you should assign the IP address of the System Log server. JN4508F-M will send the selected occurrences, selected on the Event Selection page, to the System Log server that you have assigned.

Both: The 2 modes mentioned above can be enabled at the same time.

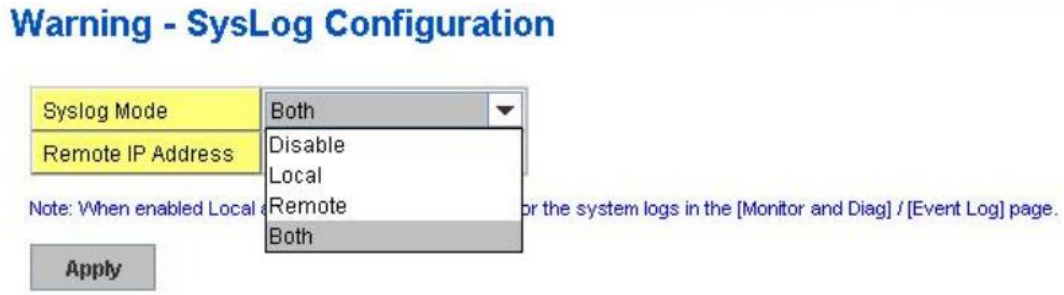


Figure 4-72. Warning Syslog Configuration Screen

Once you have finished configuring the settings, click the *Apply* button to apply your configuration.

Note:

When enabling Local or Both modes, you can monitor the system logs in [Monitor and Diag] / [Event Log] page.

SMTP Configuration

The JN4508F-M includes an E-mail Warning feature. The switch will send occurrences to a remote E-mail server. The receiver can then receive an E-mail notification by E-mail to SMTP standard.

This section, shown in the next image, allows you to enable the E-mail Alert, and assign the SMTP Server IP, Sender E-mail, and Receiver E-mail. If the SMTP server requests your authorization first, here you can also set up the username and password for that.

Figure 4-73. Warning SMTP Configuration Screen

Field	Description
SMTP Server IP Address	Enter the IP address of the email Server
Authentication	Click the check box to enable password
User Name	Enter email Account name (Max.40 characters)
Password	Enter the password of the email account

Confirm Password	Re-type the password of the email account
You can set up to 4 email addresses to receive email alarm from JN4508F-M	
Rcpt E-mail Address 1	The first email address to receive email alert from JN4508F-M (Max. 40 characters)
Rcpt E-mail Address 2	The second email address to receive email alert from JN4508F-M (Max. 40 characters)
Rcpt E-mail Address 3	The third email address to receive email alert from JN4508F-M (Max. 40 characters)
Rcpt E-mail Address 4	The fourth email address to receive email alert from JN4508F-M (Max. 40 characters)

Table 4-22. SMTP Field Description

Once you have finished configuring the settings, click the *Apply* button to apply your configuration.

CLI Commands Lines for Warning Configuration

Feature	Command Line
Relay Output	
Relay Output	Switch(config)# relay 1 dry dry output ping ping failure port port link failure power power failure ring super ring failure
DI State	Switch(config)# relay 1 di <1-2> DI number Switch(config)# relay 1 di 1 high high is abnormal low low is abnormal Switch(config)# relay 1 di 1 high
Dry Output	Switch(config)# relay 1 dry <0-4294967295> turn on period in second Switch(config)# relay 1 dry 5 <0-4294967295> turn off period in second Switch(config)# relay 1 dry 5 5
Ping Failure	Switch(config)# relay 1 ping 192.168.10.33 n <cr> reset reset a device Switch(config)# relay 1 ping 192.168.10.33 reset <1 -65535> reset time Switch(config)# relay 1 ping 192.168.10.33 reset 60 <0-65535> hold time to retry Switch(config)# relay 1 ping 192.168.10.33 reset 60 60
Port Link Failure	Switch(config)# relay 1 port PORTLIST port list Switch(config)# relay 1 port fa1 -5
Power Failure	Power Failure Switch(config)# relay 1 power <1 -2> power id Switch(config)# relay 1 power 1 Switch(config)# relay 1 power 2
Super Ring Failure	Switch(config)# relay 1 ring
Disable Relay	Switch(config)# no relay <1 -2> relay id Switch(config)# no relay 1 (Relay_ID: 1 or 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
Event Selection	

Event Selection	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: Cold Start event	Switch(config)# warning-event coldstart Set cold start event enable ok.
Ex: Link Up event	Switch(config)# warning-event linkup [IFNAME] Interface name, ex: fastethernet1 or gi8 Switch(config)# warning-event linkup fa5 Set fa5 link up event enable ok.
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 Time synchronize Failure: Disable DI:DI1
Syslog Configuration	
Local Mode	Switch(config)# log syslog local
Server Mode	Switch(config)# log syslog remote 192.168.10.33
Both	Switch(config)# log syslog local Switch(config)# log syslog remote 192.168.10.33
Disable	Switch(config)# no log syslog local
SMTP Configuration	
SMTP Enable	Switch(config)# smtp-server enable email-alert SMTP Email Alert set enable ok.
Sender mail	Switch(config)# smtp-server server 192.168.10.100 ACCOUNT SMTP server mail account, 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.
Receiver mail	Switch(config)# smtp-server receipt 1 receiver@altus.com.br SMTP Email Alert set receipt 1: receiver@altus.com.br ok.
Authentication with username and password	Switch(config)# smtp-server authentication username admin password admin SMTP Email Alert set authentication Username: admin, Password: admin **Note**: You can assign string to username and password.
Disable SMTP	Switch(config)# no smtp-server enable email-alert SMTP Email Alert set disable ok.
Disable Authentication	Switch(config)# no smtp-server authentication SMTP Email Alert set Authentication disable ok.
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:

Table 4-23. CLI Commands Lines for Warning Configuration

Monitoring and Diagnostic

JN4508F-M provides several types of features for you to monitor the status of the switch or create a diagnostic for you to check the problem when issues with the switch occur. Features include MAC Address Table, Port Statistics, Event Log and Ping.

MAC Address Table

JN4508F-M provides 2K of entries in the MAC Address Table. On this page, users can change the Aging time, add Static Unicast MAC Address, monitor the MAC address or sort them by different packet types and ports. Click the *Apply* button to change the value.

Aging Time (Sec)

Each switch fabric has a limited amount of space to write the learnt MAC address. To save more entries for new MAC address, the switch fabric will age out any unused MAC address entries with respect to the Aging Time. The default Aging Time is 300 seconds. The Aging Time can be modified on this page.

Static Unicast MAC Address

For some applications, users may need to type the static Unicast MAC address into its MAC address table. On this page, you can type in the MAC Address (format: xxxx.xxxx.xxxx), and select its VID and Port ID. Click the *Add* button to add it to the MAC Address table.

MAC Address Table

In the MAC Address Table, you can see all the MAC Addresses learned by the switch fabric. The packet types include Management Unicast, Static Unicast, Dynamic Unicast, Static Multicast and Dynamic Multicast. The table allows users to sort the addresses by the packet types and the port.

Packet Types

Management Unicast refers to the MAC address of the switch. It belongs to the CPU port only. The Static Unicast MAC address can be added and deleted. Dynamic Unicast MAC is the MAC address learned by the switch Fabric. Static Multicast can be added through CLI and can be deleted through the Web and CLI. Dynamic Multicast will appear after you have enabled IGMP and after the switch learns the IGMP report.

Click the *Remove* button to remove the Static Unicast/Multicast MAC address.

Click the *Reload* button to refresh the table. Newly learned Unicast/Multicast MAC address will be updated to the MAC address table.

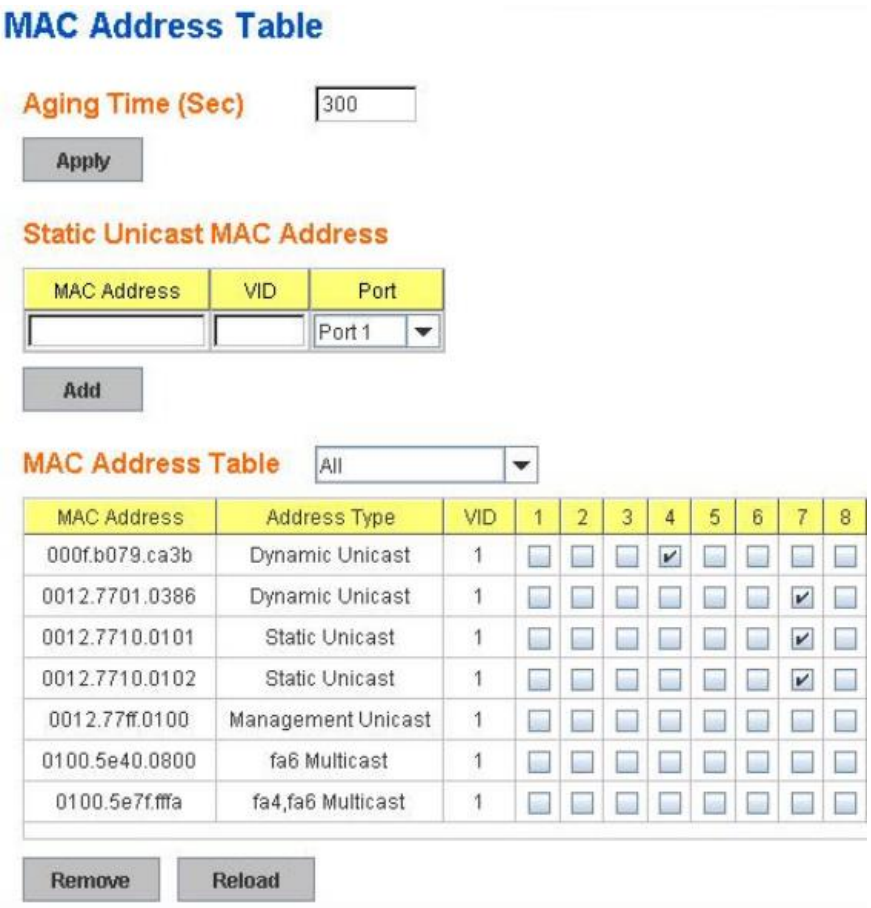


Figure 4-74. MAC Address Table Screen

Port Statistics

On this page, you can view operational statistics for each port. The statistics that can be viewed include Link Type, Link State, Rx Good, Rx Bad, Tx Good, and Collision. Rx means the received packets while Tx means the transmitted packets. The statistics can just show Rx Good and Tx Good or Rx Bad and Collision.

Note:

If you see an increase in Bad or Collision counts, this may mean that your network cable is not connected correctly or the network performance of the port is poor. Please check your network cable, Network Interface Card connected to your device, the network application, or reallocate the network traffic.

Click the *Clear Selected* button to reset the counts of the selected ports and the *Clear All* button to reset the counts of all ports. Click the *Reload* button to refresh the counts.

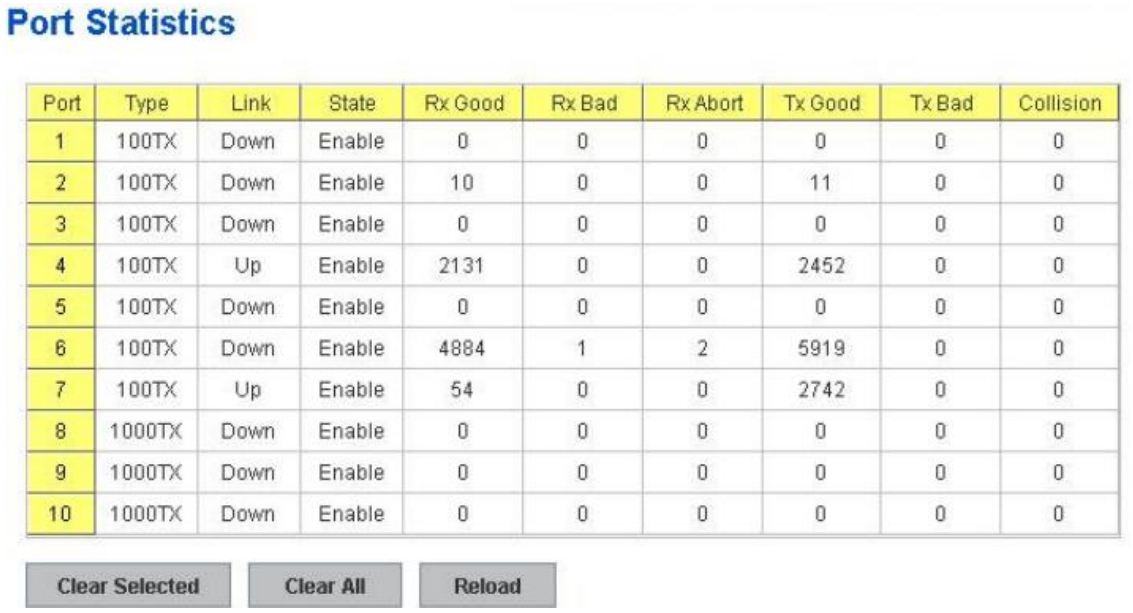


Figure 4-75. Port Statistics Screen

Port Mirroring

Port mirroring (also called port spanning) is a tool that allows you to mirror the traffic from one or more ports onto another port, without disrupting the flow of traffic on the original port. Any traffic that goes into or out of the Source Port(s) will be duplicated at the Destination Port. This traffic can then be analyzed at the Destination port using a monitoring device or application. A network administrator will typically utilize this tool for diagnostics, debugging, or fending off attacks.

Port Mirror Mode: Select Enable/Disable to enable/disable Port Mirror.

Source Port: This is also known as Monitor Port. These are the ports you want to monitor. The traffic of all source/monitor ports will be copied to destination/analysis ports. You can choose a single port, or any combination of ports, but you can only monitor them in Rx or TX only. Click on checkbox of the Port ID, RX, Tx or Both to select the source ports.

Destination Port: This is also known as Analysis Port. You can analyze the traffic of all the monitored ports at this port without affecting the flow of traffic on the port(s) being monitored. Only one RX/TX of the destination port can be selected. A network administrator would typically connect a LAN analyzer or Netxray device to this port.

Once you finish configuring the settings, click on *Apply* to apply the settings.

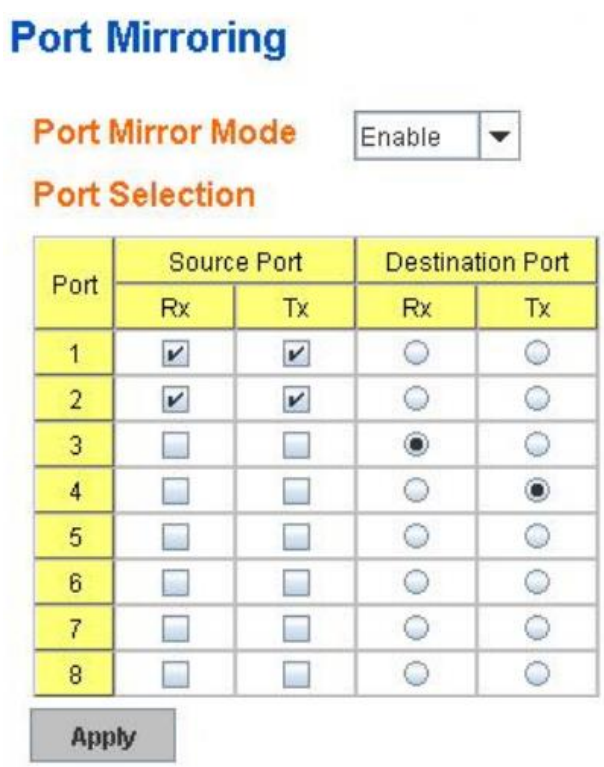


Figure 4-76. Port Mirroring Screen

Event Log

In section IEEE 802.1x, we introduced the System Log feature. When System Log Local mode is selected, JN4508F-M will record past events in the local log table. This page shows the log table. The entries include the index, and data, time and content of the occurrences.

Click the *Clear* button to delete the entries. Click the *Reload* button to refresh the table.

Figure 4-77. System Event Logs Screen

Topology Discovery

JN4508F-M supports topology discovery or LLDP (IEEE 802.1AB Link Layer Discovery Protocol) function that can help user to discovery multi-vendor's network devices on same segment by NMS system which supports LLDP function, for example NMS; With LLDP function, NMS can easier maintain the topology map, display port ID, port description, system description, VLAN ID.

Once the link failure, the topology change events can be updated to the NMS as well. The LLDP Port State can display the neighbor ID and IP leant from the connected devices.

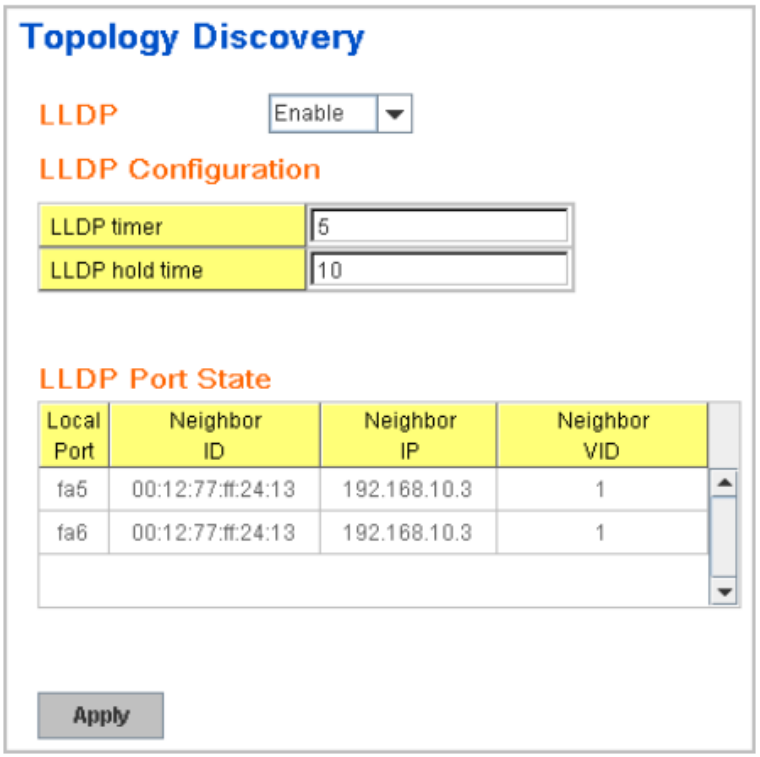


Figure 4-78. Topology Discovery Screen

LLDP: Select Enable/Disable to enable/disable LLDP function.

LLDP Configuration: To configure the related timer of LLDP.

LLDP Timer: the interval time of each LLDP and counts in second; the valid number is from 5 to 254, default is 30 seconds.

LLDP Hold time: The TTL (Time To Live) timer. The LLDP state will be expired once the LLDP is not received by the hold time. The default is 120 seconds.

Local port: the current port number that linked with neighbor network device.

Neighbor ID: the MAC address of neighbor device on the same network segment.

Neighbor IP: the IP address of neighbor device on the same network segment.

Neighbor VID: the VLAN ID of neighbor device on the same network segment.

Ping Utility

This page provides Ping Utility for users to ping remote devices and to check whether the device is alive or not. Type the target IP address of the target device into Target IP. Click the *Start* button to start the ping. You will be able to see the results in the Result field.

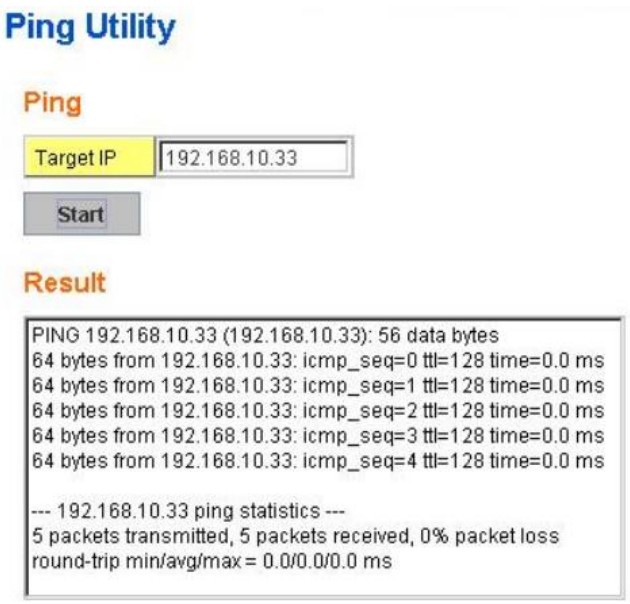


Figure 4-79. Ping Utility Screen

CLI Commands for Monitoring and Diagnostic

Feature	Command Line
MAC Address Table	
Ageing Time	Switch(config)# mac-address-table aging-time 350 mac-address-table aging-time set ok! **Note**: 350 is the new ageing timeout value.
Add Static Unicast MAC address	Switch(config)# mac-address-table static 0012.7701.0101 vlan 1 interface fastethernet1 mac-address-table ucast static set ok! **Note**: rule: mac-address-table static MAC_addres VLAN VID interface interface_name
Add Multicast MAC address	Switch(config)# mac-address-table multicast 0100.5e01.0101 vlan 1 interface fa1 -6 Adds an entry in the multicast table ok! Note: rule: mac-address-table multicast MAC_address VLAN VID interface_list interface_name/range
Show MAC Address Table – All types	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
Show MAC Address Table – Dynamic Learnt MAC addresses	Switch# show mac-address-table dy Destination Address / Address Type / Vlan / Destination Port 000f.b079.cb93 / Dynamic / SVL / fa1

<table>
<tr><td>Show MAC Address Table – Multicast MAC addresses</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 0 fa4,fa6-7</td></tr>
<tr><td>Show MAC Address Table – Static MAC addresses</td><td>Switch# show mac-address-table static
Destination Address Address Type Vlan Destination Por
---------- ---------- ---------- ----------
0012.7710.0101 Static 1 fa6
0012.7710.0102 Static 1 fa6</td></tr>
<tr><td>Show Aging timeout time</td><td>Switch# show mac-address-table aging-time the mac-address-table aging-time is 304 sec.</td></tr>
<tr><td colspan="2">Port Statistics</td></tr>
<tr><td>Port Statistics</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
ause: 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 Mirrorin</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.
Note: 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">Event Log</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>
</table>

Ping IP	Switch# ping 192.168.10.33 PING 192.168.10.33 (192.168.10.33): 56 data bytes 64 bytes from 192.168.10.33: icmp_seq=0 ttl=128 time=0.0 ms 64 bytes from 192.168.10.33: icmp_seq=1 ttl=128 time=0.0 ms 64 bytes from 192.168.10.33: icmp_seq=2 ttl=128 time=0.0 ms 64 bytes from 192.168.10.33: icmp_seq=3 ttl=128 time=0.0 ms 64 bytes from 192.168.10.33: icmp_seq=4 ttl=128 time=0.0 ms --- 192.168.10.33 ping statistics --- 5 packets transmitted, 5 packets received, 0% packet loss round-trip min/avg/max = 0.0/0.0/0.0 ms

Table 4-24. Command Lines for Monitoring and Diagnostic Configuration

Device Front Panel

Device Front Panel command allows you to see LED status of the switch. You can see LED and link status of the Power, DO, DI, R.S. and Ports.

Feature	Status
Power	On: the Vdc power is on applying
Digital Output	On: Dry Relay Output activated and the contact is formed a close circuit.
Digital Input	On: Digital Input is triggered to High level
R.S.(Ring Status)	Green on: Ring status normal. Yellow (Amber)on: Ring is abnormal
Fast Ethernet	Green on: Port is link up.
Sys	Green on: the system is ready for working.

Table 4-25. Device Front Panel LEDs

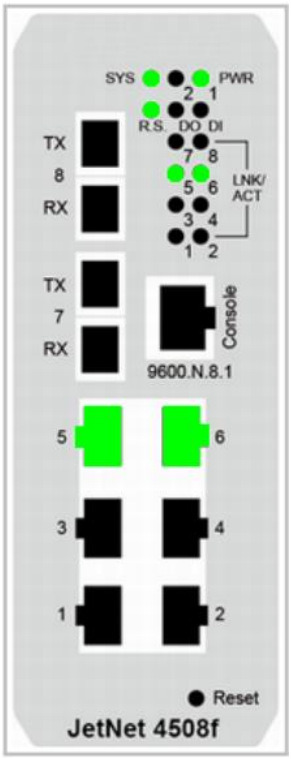


Figure 4-80. Device Front Panel

Save to Flash

Save Configuration allows you to save any configuration you just made to the Flash. Powering off the switch without clicking *Save Configuration* will cause loss of new settings. After selecting Save Configuration, click the *Save to Flash* button to save your new configuration.

Figure 4-81. Save to Flash Screen

Feature	Command Line
Save	Switch# write Building Configuration... [OK] Switch# copy running-config startup-config Building Configuration... [OK]

Table 4-26. Save to Flash Command Lines

Logout

The switch provides 2 logout methods. Your web connection will log out if you do not input a command for 30 seconds. The Logout command allows you to manually log out the web connection. Click *Yes* to logout, and *No* to go back to the configuration page.

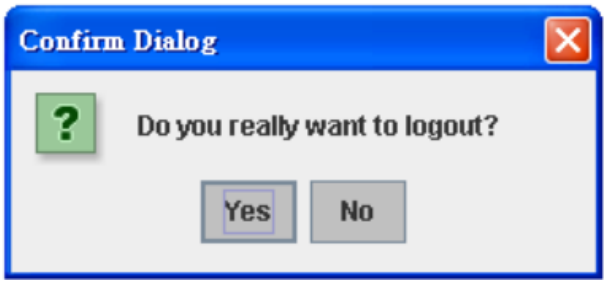


Figure 4-82. Logout Screen

Feature	Command Line
Logout	Switch> exit Switch# exit

Table 4-27. Logout Command Lines

5. Appendix

Product Specifications

Technology	
Standard	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)
Performance	
Switch Technology	Store and Forward Technology with 3.2Gbps Switch Fabric
System Throughput	26 Mega packets per second, 64 bytes packet size. 14,880 PPS for 10Base-T 148,800 PPS for 100Base-TX (PPS: Packet Per Second)
CPU performance	32 bits ARM-9E running at 180 MHz and performance up to 200MIPS; Embedded hardware based watchdog timer.
System Memory	8M bytes flash ROM, 64M bytes SDRAM.
MAC Address	8K MAC address table.
Packet Buffer	Embedded 1Mbits shared buffer
Transfer performance	64 bytes to 1522bytes (includes 1522 bytes VLAN Tag).
Relay Alarm	Dry Relay output with 1A /24 Vdc ability
Digital Input (DI)	One Digital Input with Photo Copular isolation Digital Hi: 11 to 30 Vdc Digital Low: 10 to 0 Vdc
System Management	
Configuration and monitoring interface	Supports 4 configuration and monitoring interfaces: RS-232 serial console, Telnet, SNMP and Web Browser interface The RS-232 and Telnet interfaces support Cisco like instructions
System upgrade/Backup	Provides TFTP/Web interface for firmware upgrade and configuration backup, restore
Telnet & Local Console	Supports command line interface with Cisco like commands and maximum 4 sessions; the telnet interface also supports SSH
SNMP	Supports v1, v2c, V3 with SNMP trap function, trap station up to 4 and can be manually configured the trap server IP address
SNMP MIB	MIBII, Bridge MIB, Ethernet-like MIB, VLAN MIB, IGMP MIB, Private MIB
Utility	Supports JetView and JetView Pro with IEEE 802.1AB Link Layer Discovery Protocol for device finding and link topology discovery
Network Time Protocol	Supports NTP protocol with daylight saving function and localize time sync function.
Management IP Security	IP address security to prevent unauthorized access
Management interface	SNMP v1, v2c and v3, Web browser and Console Management
E-mail Warning	4 receipt E-mail accounts with mail server authentication
System Log	Supports both Local or remote Server with authentication
Network Performance	
IEEE 802.3x	Flow control pause frame supports on 10/100bps with Full Duplex and Back-pressure supports on 100 / 10Mbps Half Duplex only

Port Configuration	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	The private VLAN supports isolated port access with the uplink port in the switch. Typically, each private VLAN contains many private ports and one given uplink port; each private port is isolated with each other and only communicates with the uplink port for the outgoing data and incoming data to provide client port isolated feature.
Class of Service	IEEE 802.1p class of service; per port 4 priority queues.
Traffic Prioritize	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 for multicast filtering and IGMP Query mode; also support unknown multicasting process forwarding policies- drop, flooding and forward to router p
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.
Network Redundancy	
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	Fast Ethernet communication port: 8 x RJ45 RS-232 console interface: RJ45 connector DI/DO port: 4-pin removable terminal block Power port: 4-pin removable terminal block
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
RS232 serial interface	Supports Cisco like command line interface for out-band management
System Diagnostic LEDs	
System	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)
Ethernet port	Link (Green On) / Activity (Green Blinking)

Power Requirements	
System Power	Redundant power input with polarity auto reverse protection Input Range: 24 Vdc (10 to 60 Vdc) Power System Type: Positive or Negative power source
Power Consumption	JN4508F-M: 10 Watts / 24 Vdc
Mechanical	
Installation	DIN Rail Mounting or Wall Mounting
Case	Aluminum metal case with grade 31 protection
Dimension (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
Weight	JN4508F-M: 0.885Kg
Environmental	
Operating Temperature	-10~70 ℃ (JN4508F-M)
Operating Humidity	0% ~ 90%, non-condensing
Storage Temperature	-40 ℃ ~ 85 ℃
Hi-Pot Insulation	AC 1.5KV for all ports and power
Regulatory Approvals	
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
Vibration	IEC60068-2-6 Note-2
Shock	IEC60068-2-27 Note-2
Free Fall	IEC60068-2-32 with package Note-3

Table 5-1. Product Specification

Private MIB

It is provided many standard MIBs for users to configure or monitor the switch's configuration through SNMP. But, since some commands cannot be found in standard MIB, it is provided Private MIB to meet the needs. Compile the private MIB file with your SNMP tool. You will then be able to use it.

The private MIB tree is the same as the web tree. This is easier to understand and use. If you are not familiar with the standard MIB, directly use the private MIB to manage /monitor the switch, there is no need to learn where the OIDs of the commands are.

The path of JN4508F-M is 1.3.6.1.4.1.24062.2.3.1. Figure 5-1 show the Private MIB tree for your reference.

The JN4508f -m's private MIB supports various of MIB entries, which are system basic setting, port configuration, network redundancy, VLAN, traffic priority,multicasting, snmp, security, system warning, monitoring and configuration saving. User can monitoring and configures JN4508F-M by SNMP MIB browser tools and through those MIB entries to achieve remote management. The Private MIB includes 12 major entries for system configuration and monitoring as below listing:

System information: read only.

Basic Setting MIB entry: read and write.

Port Configuration MIB entry: Read and Write.

Network redundancy MIB entry: Read and Write.

Vlan MIB entry: Read and Write.

Traffic prioritization MIB entry: Read and Write.

Multicast Filtering MIB entry: Read and Write.

SNMP MIB entry: Read and write.

Security MIB entry: Read and write.

Warning MIB entry: Read and write.

Monitor and Diag: Read and write.

Save MIB entry: write only.

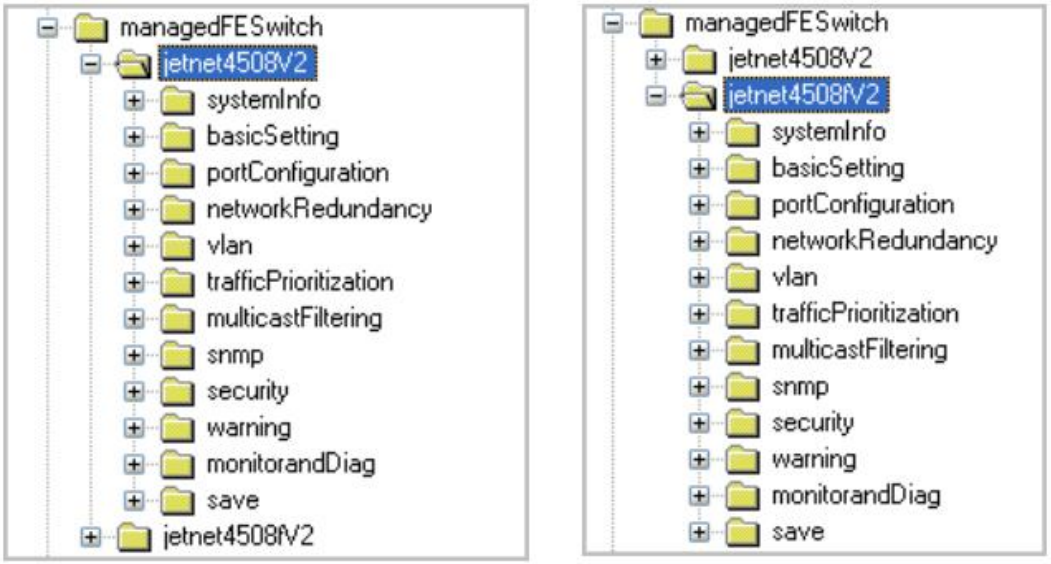


Figure 5-1. JN4508F-M Private MIB

MODBUS TCP Protocol

The MODBUS TCP is very similar to MODBUS RTU, but transmits data within TCP/IP Data packets. It was developed in 1979 for industrial automatic communication system and have becomes a standard protocol for industrial communication for the transfer discrete analog I/O devices or PLC systems. It defines a simple protocol data unit independent of the underlying data link layer. The MODBUS TCP packet includes 3 parts - MBAP header, function code and data payload, the MBAP header is used on TCP/IP header to identify the MODBUS application Data Unit and provides some differences compared to the MODBUS RTU application data unit used on serial line. The MBAP header also includes unit identifier to recognize and communicate between multiple independent MODBUS end units.

The MODBUS devices communicate using a master (client) /slave (server) architecture, only one device can initiate transaction and the others respond to the master/client. The other devices (slave/server) respond by supplying the requested data to the master/client, or by taking the action requested in the query. The slave/server can be any peripheral device (DSC unit, PLC unit, Volt/Current Transducer, network communication switch) which process information and sends the output data to the master using MODBUS TCP protocol. JN4508F-M Switch operating as slave/server devices, while a typical master/client device is host computer running appropriate application software, like as SCADA / HMI system. The transaction architecture like as the drawing following.

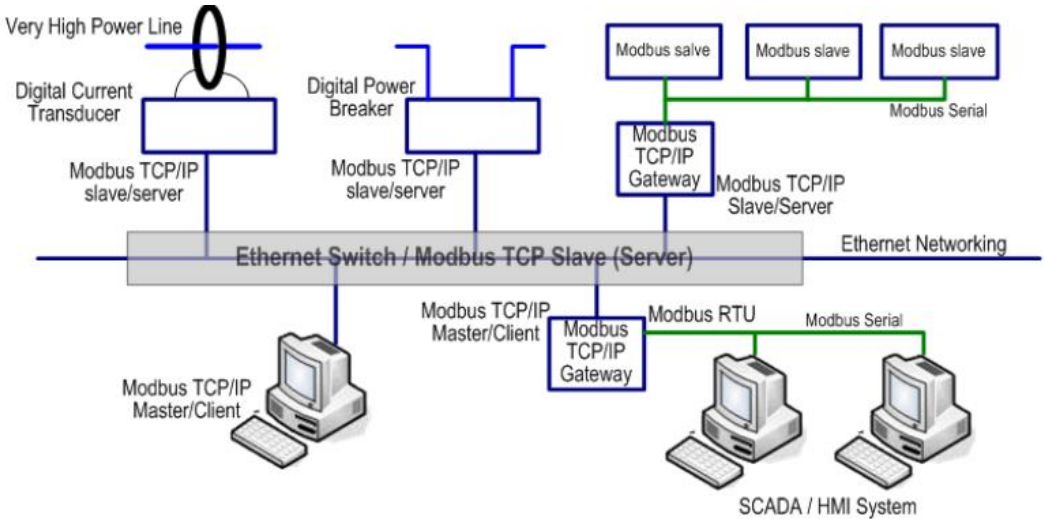


Figure 5-2. MODBUS Communication

There are three most common MODBUS versions, MODBUS ASCII, MODBUS RTU and MODBUS TCP. Ethernet based device, Industrial Ethernet Switch for example, supports MODBUS TCP that it can be polled through Ethernet. Thus the MODBUS TCP master can read or write the MODBUS registers provided by the Industrial Ethernet Switch.

The JN4508F-M Managed DIN-Rail Ethernet Switch has implement MODBUS/TCP register in the firmware. Those register mapping to some of Ethernet Switchs operating information, includes description, IP address, power status, interface status, interface information and inbound/outbound packet statistics. With the register supports, user can read the information through their own MODBUS TCP based progress/ display/ monitor applications and monitor the status of the switch easily.

The configuration of MODBUS/TCP only present in CLI management mode and the no extra user interface for Web configuration.

MODBUS Function Code

The MODBUS TCP device uses a subset of the standard MODBUS TCP function code to access device-dependent information. MODBUS TCP function code is defined as below.

FC	Name	Usage
01	Read Coils	Read the state of a digital output
02	Read Input Status	Read the state of a digital input
03	Read Holding Register	Read holding register in 16-bits register format
04	Read Input Registers	Read data in 16-bits register format
05	Write Coil	Write data to force a digital output ON/OFF
06	Write Single Register	Write data in 16-bits register format
15	Force Multiple Coils	Write data to force multiple consecutive coils

Table 5-2. MODBUS Function Code

The JN4508F-M device supports the function code 04, which name is Read Input Registers. With this support, the remove SCADA or other MODBUS TCP application can poll the information of the device and monitor the major status of the switch.

Error Checking

The utilization of the error checking will help eliminate errors caused by noise in the communication link. In MODBUS TCP mode, messages include an error-checking field that is based on a Cyclical Redundancy Check (CRC) method. The CRC filed checks the contents of the entire message. It

applied regardless of any parity check method used for the individual BYTE acters of the message. The CRC value is calculated by the transmitting device, which appends the CRC to the message. The receiving device recalculates a CRC during receipt of the message, and compares the calculated value to the actual value it received in the CRC filed.

Exception Response

If an error occurs, the slave sends an exception response message to master consisting of the slave address, function code, exception response code and error check field. In an exception response, the slave sets the high-order bit (MSB) of the response function code to one. The exception response codes are listed below.

FC	Name	Descriptions
01	Illegal Function	The message function received is not allowable action.
02	Illegal Data Address	The address referenced in the data field is not valid.
03	Illegal Data Value	The value referenced at the addressed device location is no within range.
04	Slave Device Failure	An unrecoverable error occurred while the slave was attempting to perform the requested action.
05	Acknowledge	The slave has accepted the request and processing it, but a long duration of time will be required to do so.
06	Slave Device Busy	The slave is engaged in processing a long-duration program command.
07	Negative Acknowledge	The slave cannot perform the program function received in the query.
08	Memory Parity Error	The slave attempted to read extended memory, but detected a parity error in the memory.

Table 5-3. MODBUS Exception Response

MODBUS TCP Register Table

Word Address	Data Type	Description
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 = ‘I’ Word 2 Hi byte = ‘x’ Word 2 Lo byte = ‘\0’ (other words = 0)
0x0010	16 words	Product Name = "JN4508F-M" Word 0 Hi byte = ‘J’ Word 0 Lo byte = ‘N’ Word 1 Hi byte = ‘4’ Word 1 Lo byte = ‘5’ Word 2 Hi byte = ‘0’ Word 2 Lo byte = ‘8’ Word 3 Hi byte = ‘5f Word 3 Lo byte = ‘-’ Word 4 Lo byte = ‘m’ 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	2 words	Bad Octets

0x207F		
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 0x27BF	2 words	LateCollision
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

Table 5-4. MODBUS TCP Register Table

Note:

The MODBUS TCP client will return 0xFFFF to MODBUS master when pulling reserved address.

CLI commands for MODBUS TCP

Feature	Command & example
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.

Table 5-5. Commands for MODBUS

6. Glossary

Baud rate	Rate in which information bits are transmitted through a serial interface or communication network (measured in Bits/second, bps)
Bit	Basic information unit, it may be at 1 or 0 logic level.
Bus	Set of electrical signals that are part of a logic group with the function of transferring data and control between different elements of a subsystem
Byte	Information unit composed by eight bits.
Communication Network	Set of devices (nodes) interconnected by communication channels.
CPU	Central Processing Unit. It controls the data flow, interprets and executes the program instructions as well as monitors the system devices.
Database	A group of data organized in a table.
Default	A value that is commonly used as a standard
Diagnostic	Procedures to detect and isolate failures. It also relates to the data set used for such tasks, and serves for analysis and correction or problems.
Download	Information that is sent to some device/path.
ESD	Electrostatic Discharge.
Firmware	The operating system of a PLC. It controls the PLC basic functions and executes the application programs.
Frame	Information unit transmitted in the network.
Gateway	Device to connect two communication networks with different protocols.
Hardware	Physical equipment used to process data where normally programs (software) are executed
I/O	See Input/Output.
Input/output	Also known as I/O. Data input or output devices in a system. In PLCs these are typically the digital or analog modules that monitor or actuate the devices controlled by the system.
Interface	Normally used to refer to a device that adapts electrically or logically the transferring of signals between two equipments.
Kbytes	Memory size unit. Represents 1024 bytes.
LED	Light Emitting Diode. Type of semiconductor diode that emits light when energized. It's used for visual feedback.
Master	Device connected to a communication network originating all the command requests to other network units.
Master-slave communication network	Communication network where the data transfer are initiated only by one node (the network master). The remaining network nodes (slaves) only reply when requested.
Media access	Method used by all nodes in a network to synchronize data transmission and solve possible conflicts in simultaneous transmissions.
Menu	Set of available options for a program, they may be selected by the user in order to activate or execute a specific task
Module (hardware)	Basic element of a system with very specific functionality. It's normally connected to the system by connectors and may be easily replaced.
Module (software)	Part of a program capable of performing a specific task. It may be executed independently or in conjunction with other modules through information sharing by parameters.
Module address:	Address used by the CPU in order to access a specific I/O module.
Node	Any station in a network with the capacity to communicate using a determined protocol.
Operands	Elements on which software instructions work. They may represent constants, variables or set of variables.
PLC	See Programmable Controller.
Programming Language	Set of rules, conventions and syntaxes utilized when writing a program.
Protocol	Procedures and formats rules that allow data transmission and error recovery among devices with the use of control signals
RAM	Random Access Memory. Memory where all the addresses may be accessed directly and in random order at the same speed. It is volatile, in other words, its content is erased when powered off, unless there is a battery to keep its contents.
RX	Acronym used to indicate serial reception.
Serial Channel	Unit interface that transfers data serially.
Software	Computer programs, procedures and rules related to the operation of a data processing system
Sub network	Segment of a communication network that connects a group of devices (nodes) with the goal of isolating the local data traffic or using different protocols or physical media.

Supervisory Station	Equipment connected to a PLC network with the goal of monitoring and controlling the process variables
Tag	Name associated to an operand or to logic that identifies its content.
Time-out	Maximum preset time to a communication to take place. When exceeded, then retry procedures are started or diagnostics are activated.
Toggle	Element with two stable states that are switched at each activation.
TX	Acronym used to indicate serial transmission.
Upload	Reading a program or configuration from the PLC.
Word	Information unit composed by 16 bits.