

Korenix JetNet 4000 Series Industrial Ethernet Rail Switch

User's Manual

V1.6, Jun. 2007



www.korenix.com

Korenix JetNet 4000 Series Industrial Ethernet Rail Switch User's Manual

Copyright Notice

Copyright © 2005 Korenix Technology Co., Ltd.

All rights reserved.

Reproduction in any form or by any means without permission is prohibited.

Table of Contents

Chapter 1	Introduction	1-1
	Overview.....	1-2
	Ethernet Switching Technology.....	1-2
	Product Features.....	1-4
	Package Checklist.....	1-4
Chapter 2	Hardware Installation	2-1
	Introduction.....	2-2
	Panel Layout	2-2
	Reset Button.....	2-2
	LED Indicators.....	2-2
	DIP Switch	2-4
	Wiring the Power Inputs	2-4
	Wiring the Relay Output	2-4
	Wiring the Ethernet Ports	2-5
	Wiring the Fiber Ports.....	2-6
	DIN-Rail Mounting Installation	2-6
	Wall-Mounting Installation	2-7
Chapter 3	Web-based Management	3-1
	Introduction.....	3-2
	Preparation for Web Management	3-2
	System Login.....	3-2
	Configuration via the Web-based Management Interface	3-3
	Menu Bar Introduction.....	3-3
	Configuring Your JetNet 4000 Series Industrial Ethernet Switch	3-4
Chapter 4	Troubleshooting	4-1
	Power Connections	4-2
	Incorrect Connections.....	4-2
	Faulty or Loosen Cables	4-2
	Non-standard Cables.....	4-2
	Improper Network Design	4-2
	LED Indicators.....	4-3
Appendix A	Specifications	A-1
Appendix B	Revision History	B-1

1

Introduction

Welcome to Korenix JetNet 4000 Series Industrial Ethernet Rail Switch. JetNet 4000 Series is a web-managed rail switch that is specially designed for industrial applications.

The following topics are covered in this chapter:

- **Overview**
- **Ethernet Switching Technology**
- **Product Features**
- **Package Checklist**
- **Installation Guide**

Overview

JetNet 4000 Series are web-managed, industrial Ethernet rail switches that have six 10/100MBaseTX ports, plus two 100BaseFX ports (multi-mode “-M” or single-mode “-S” models), and are designed to operate under harsh environmental conditions. JetNet 4000 Series industrial Ethernet switches also include advanced support for media redundancy and offer communication recovery time less than 300 milliseconds. JetNet 4000 Series industrial Ethernet switches also have a wide operating ambient range and include redundant power inputs with reverse polarity protection. The unit includes a DC-IN jack and may be optionally powered from an AC-DC wall transformer for Small Office/Home Office (SOHO) applications. It is packaged in a rugged, IP-30 aluminum enclosure for increased protection from extreme temperature, vibration, dust, and debris. JetNet 4000 Series Industrial Ethernet Switch has also passed several safety certifications to help ensure safe and reliable data transmission for industrial applications.

In addition to supporting the Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP), JetNet 4000 Series Industrial Ethernet Switch includes a proprietary Super Ring technology that allows it to manage a media loop with other switches of the same type. A media loop is created when a message sent out on one port is received by the same switch at another port (two message paths exist). JetNet 4000 Series Industrial Ethernet Switch is smart enough to temporarily disable the second path, holding it as a backup in case the primary path fails. It also includes a normally closed alarm relay to signal a port failure (if enabled). JetNet 4000 Series Industrial Ethernet Switch will automatically fail-over to a secondary path within 300ms if the primary path is lost.

JetNet 4000 Series Industrial Ethernet Switch also supports SC-type fiber connections in both single-mode and multi-mode versions, useful for extending transmission distance. A web-based management interface ensures easy operation and reconfiguration via a standard internet web browser.

Ethernet Switching Technology

To better understand the operation of an Ethernet switch, we need to first differentiate it from a hub. An Ethernet hub (or repeater) is a device that is used to simply connect Ethernet nodes. Any message at one hub port is repeated on all ports. That is, hubs forward data packets they receive from a single station to all hub ports. As a result, all port devices connected to a single hub will share the same bandwidth. Then as nodes are added to the network hub, they compete for this finite amount of bandwidth and this can cause data collisions to occur, making network determinism impossible to attain, especially on busy networks. Now determinism is a term that is used to describe the ability to guarantee that a packet is sent or received in a finite and predictable amount of time. The inherent lack of determinism is the main reason that traditional Ethernet had problems being accepted for use in critical control applications, as most control systems have a defined time requirement for packet transmission, typically less than 100ms.

Switches on the other hand, are intelligent devices used to more efficiently connect distributed Ethernet nodes than a hub. Unlike a simple hub, a switch provides *targeted* data transfer, as it will forward a data packet to a specific port or network segment, rather than to all ports, thus freeing up bandwidth. The ability to target a packet to a specific port increases network throughput and helps to eliminate the collisions that have historically made Ethernet non-deterministic.

So we see that by targeting the data transfer between ports, switches act as intelligent repeaters to increase network distances. In doing this, they actually split networks into separate collision domains at each port. Thus, switches increase determinism by reducing collisions. Switches also increase network bandwidth and throughput, as well as provide supplemental error checking on data packets to help ensure the integrity of forwarded data. Each port of this switch functions just like any other Ethernet device. It is able to receive and decode Ethernet frames, test for frame integrity, plus assemble and transmit Ethernet frames.

With Ethernet, any device can try to send a data frame out at any time. If two devices happen to send a data frame at the same time, then a collision may occur. The arbitration protocol for carrier transmission access of the Ethernet network is called Carrier Sense Multiple Access with Collision Detect (CSMA/CD). With CSMA/CD, each device will first sense whether the line is idle and available for use. If it is, the device will begin to transmit its first frame. If another device also tries to send a frame at the same time, then a collision occurs and both frames are discarded. Each device then waits a random amount of time and retries its transmission until it is successfully sent.

Unlike other Ethernet devices, such as an Ethernet host adapter or Network Interface Card (NIC), the port of a switch does not require its own MAC address. During retransmission of a received packet, the switch port will instead look like the originating device by having assumed its source address. This is why the Ethernet collision domain is said to terminate at the switch port. That is, a two-port switch will effectively break a network into two distinct data links or segments. An eight port switch like JetNet 4008 Industrial Ethernet Switch can break a network into 8 distinct data links or segments (also called *collision domains*). Since all Ethernet nodes are able to recognize the occurrence of a collision, and since the detection of a collision is principal to the way Ethernet arbitrates media access, large domains containing many nodes can become quite cumbersome. Thus, using an Ethernet switch to subdivide a large network into separate collision domains will certainly help to increase throughput.

The current tendency in critical industrial control applications is to connect one Ethernet device per switch port. This will produce the most deterministic mode of operation as the switch can then operate full-duplex, with no chance of collisions. This ensures determinism, helping critical control applications to remain predictable and on-time.

Each port of a switch forwards data to another port based on the MAC address contained in the received data packet/frame. In order to know which port to forward a data packet to, the switch will learn and store the MAC addresses of every device it is connected to, along with the associated port number. However, until the switch actually learns the port a particular address resides at (the first packet), it forwards this traffic to all ports just like a hub. The switch will use its internal look-up table to quickly determine the location (port) of a node, establish a temporary connection between itself and the node, then terminate the connection once a packet is transferred. In this way, it increases network bandwidth and provides the network determinism required for critical control applications.

JetNet 4000 Series Industrial Ethernet Switch uses a *store and forward* algorithm to process Ethernet frames. That is, it first stores the Ethernet frame and examines it for errors before forwarding it to its destination. Although this method may seem to increase the forwarding time (latency) and possibly cause fragmentation, it effectively reduces the occurrence of error frames and improves overall throughput. This is particularly useful when there is heavy network traffic and or greater potential for noise and interference.

The industry-wide shift from Ethernet hubs to Ethernet switches has dramatically boosted the bandwidth of networks and helped to eliminate congestion problems inherent with the CSMA/CD protocol (Carrier Sense Multiple Access with Collision Detection). Since a switch operates by learning the location of addresses and forwarding messages directly, unnecessary traffic is greatly reduced. It will use auto-negotiation to regulate the speed and duplex of each port based on the capabilities of connected devices. These features combine with flow control allow a 100M node to effectively communicate with a 10M node without losing data. Connecting one device per switch port also allows two-way, simultaneous transmission to occur (full duplex), essentially doubling the bandwidth. Further, by segmenting a collision domain in this way, the need for non-deterministic carrier sensing (CSMA/CD) is eliminated. The utilization of a store-and-forward switching algorithm allows each packet to be inspected, and corrupt or redundant data to be filtered, further eliminating unnecessary traffic that often slows a network down.

Product Features

Korenix JetNet 4000 Series products have the following features:

- Provides redundant Ethernet Super Ring
- Supports VLAN/QoS/IGMP Snooping
- 1Mbits embedded buffer memory with 2K entry MAC address table
- Provides web-based reconfiguration with easy-to-use GUI
- Provides redundant DC Power Inputs
- Supports an alarm relay to signal port break and/or power failure
- Robust Aluminum case, IP31 standard
- DIN-Rail/Wall-mounting/Desktop Installation
- 5/8 10/100TX ports for JetNet 4005/4008
- 4/6 10/100TX ports and 1/2 100FX port(s) for JetNet 4005f/4008f
- Supports IEEE 802.3 10Base-T, 802.3u 100Base-TX/100Base-FX
- RJ-45 ports support auto MDI/MDI-X function
- Store-and-Forward switching architecture
- Provides fiber link ability
- IEEE 802.3x flow control supported
 - Flow control on full-duplex mode
 - Back pressure on half-duplex mode
- Supports Class of Service
- Supports IGMP with Query mode for multi media application
- Supports broadcast packet filtering
- Supports STP
- Provides reverse polarity protection
- Supports port-based VLAN / 802.1 Q Tag VLAN

Package Checklist

Korenix JetNet 4000 Series products are shipped with the following items:

- One industrial web-based Ethernet rail switch
- One DIN-Rail clip (attached to the switch)

- One wall mounting plate and six screws
- Documentation and Software CD
- Quick Installation Guide

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

2

Hardware Installation

This chapter includes information of installation and configuration.

The following topics are covered in this chapter:

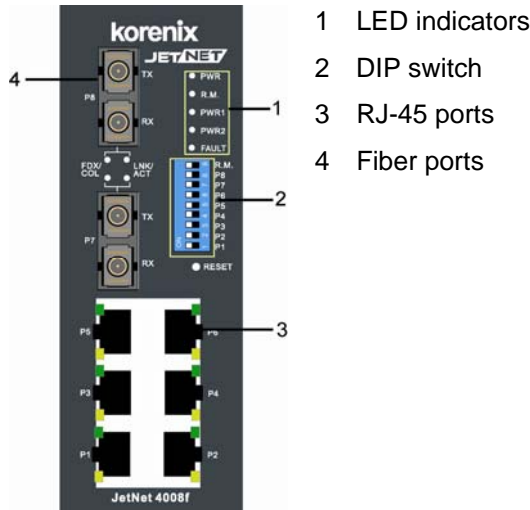
- **Introduction**
 - Panel Layout
 - Reset Button
 - LED Indicators
 - DIP Switch
- **Wiring the Power Inputs**
- **Wiring the Relay Output**
- **Wiring the Ethernet Ports**
- **Wiring the Fiber Ports**
- **DIN-Rail Mounting Installation**
- **Wall-Mounting Installation**

Introduction

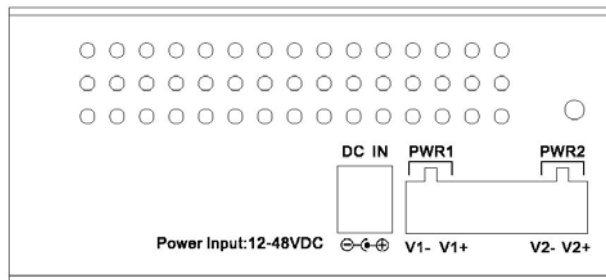
Panel Layout

Here we use JetNet 4008f Industrial Ethernet Switch as an example.

Front View



Bottom View



At the bottom of this switch is a ground screw and a 6-position plug-in terminal block connector with two DC power inputs and a relay connection. There is also a DC-IN power jack for connecting an optional AC-DC power adapter (wall transformer type).

Reset Button

The Reset button provides users with a quick and easy way to restart JetNet 4000 Series Industrial Ethernet Switch and restore the default settings.

To restart: press the Reset button for 2 seconds and release.

To restore the default settings: press the button for 5 seconds and release.

Note that you must always restart a switch after setting its Ring Master DIP switch in order to activate the new DIP switch setting or the redundant ring will not operate.

LED Indicators

There are 7 diagnostic LEDs and 8 Port LEDs located on the front panel of JetNet 4005 Industrial Ethernet Switch, while there are 9 diagnostic LEDs and 12 Port LEDs on JetNet 4008 Industrial Ethernet Switch. These LED indicators provide administrators with real-time system status. The following table describes the function of each LED indicator.

LED	Status	Description
PWR	Green	Any Power is ON (PWR1, PWR2, or DC-IN).
	Off	No power is being supplied.
PWR 1	Green	Power is on.
	Off	No power is being supplied.
PWR 2	Green	Power is on.
	Off	No power is being supplied.
R.M	Green	Indicates this switch is designated as the redundant Ring Master.
	Off	Indicates that this JetNet is NOT the master of the Super Ring.
Fault	Yellow	Power, RJ45, or fiber port failure has occurred.
	Off	Normal operation (no power or port failure).
Port LED	Status	Description
LNK/ACT of Port 7 (JetNet 4008f)	Green	A network device is detected.
	Blinks	This port is transmitting to, or receiving packets from another transmitting device.
	Off	No device is attached.
FDX/COL of Port 7 (JetNet 4008f)	Orange	The port is operating in full-duplex mode.
	Blinks	A collision of packets has occurred.
	Off	The port is in half-duplex mode or no device is attached.
LNK/ACT of Port 5 (JetNet 4005f) LNK/ACT of Port 8 (JetNet 4008f)	Green	A network device is detected.
	Blinks	The port is transmitting or receiving packets from the TX device.
	Off	No device is attached.
FDX/COL of Port 5 (JetNet 4005f) FDX/COL of Port 8 (JetNet 4008f)	Orange	The port is operating in full-duplex mode.
	Blinks	A collision of packets has occurred.
	Off	The port is in half-duplex mode or no device is attached.
Port Status	Orange	The port is operating in full-duplex mode.
	Blinking orange	A collision of packets has occurred.
	Off	The port is in half-duplex mode or no device is attached.
	Green	A network device is detected.
	Blinking green	This port is transmitting to, or receiving packets from another transmitting device.
	Off	No device is attached.

DIP Switch

The DIP switches are used to configure which JetNet in a Super Ring to be a master switch (Ring Master), and to separately enable the port alarms.

DIP SWITCH	Status	Description
R.M.	ON	Set this switch to be the Ring Master.
	Off	Set this switch NOT to be the Ring Master.
P1 to P8 (JetNet 4008f) P1 to P5 (JetNet 4005f)	ON	To enable port break alarm at this port.
	Off	To disable port break alarm at this port.

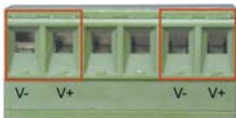
Notes (DIP Switches):

1. If the corresponding port alarm DIP switch is set ON, when that port connection fails, the Fault LED will light up and the alarm relay contacts will close.
2. After you set a switch to be the Ring Master in a redundant media ring, you must restart this switch to activate the settings (see Reset Button) or ring redundancy will not operate.
3. Only one switch in a media ring should have its Ring Master switch set to ON.
4. In order for a redundant ring to operate, all switches in the ring must be of the same type (employ the same redundant ring method).

Wiring the Power Inputs

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

1. Insert the positive and negative wires of your DC supply into the V+ and V- contacts of the terminal block connector. The acceptable wire range is 12 to 24 AWG.



2. Tighten the terminal screws to prevent the DC wires from coming loose.



3. **OPTIONAL – DC IN:** JetNet 4000 Series Industrial Ethernet Switch has an additional power jack for the connection of AC-DC power converters (wall-transformer type) designed for office use. Be sure that the output voltage is within the required 12-48V DC range and of sufficient capacity to power the unit. Refer to switch PWR LED to verify power via the DC-IN jack.

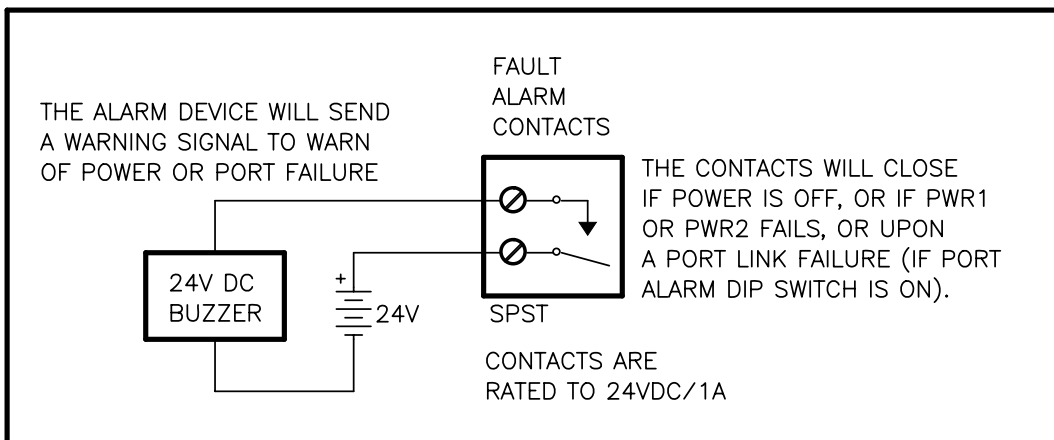
Note: If all three power inputs are connected (DC IN, PWR 1, PWR 2), the JetNet will be powered from the highest connected voltage. The unit will not alarm for loss of DC IN power, the alarm function only applies to loss of power at PWR1 or PWR2.

Wiring the Relay Output

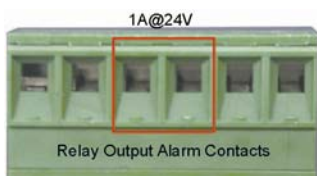
The alarm output relay contacts are located at the two middle terminals of the power terminal block, between PWR2 and PWR1 as shown in the figure below. These contacts are single-pole single-throw (SPST) and are energized (open-circuited) for normal operation. These contacts will close if the unit is not powered, or if either DC power 1 or power 2 fails, or if a port connection fails (if that port alarm DIP switch is ON). The figure below gives an example of how the output

alarm relay operates.

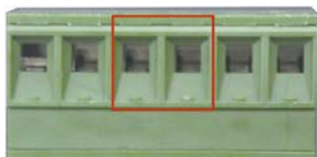
Note: The relay contacts are energized (open) for normal operation and will close for fault conditions. This contact does not supply any power and is rated up to 24V DC at 1A.



1. Connect to the SPST alarm relay terminals per your application. Insert your load wires and tighten the alarm terminal screws to prevent the wires from coming loose. These contacts are open for normal operation and close in alarm. Do not exceed 24V and 1A.

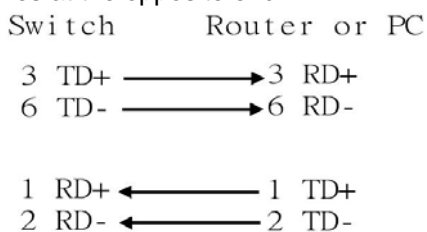


2. Verify that your load is wired to the center two terminals of this terminal block. After the power relay is wired, replace this terminal block into its socket.

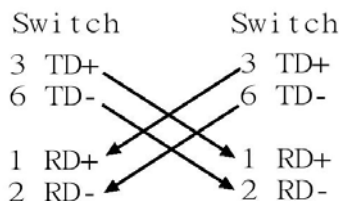


Wiring the Ethernet Ports

JetNet 4000 Series Industrial Ethernet Switch includes six RJ-45 ports with automatic MDI/MDI-X crossover, and automatic 10/100Mbps data rate sensing for 10Base-T or 100Base-TX connections. Automatic MDI/MDI-X crossover allows you to connect to other switches, hubs, or workstations, without regard to using straight-through or crossover cabling. The following figures depict the schematic diagram of straight-through and crossover cabling. Note that crossover cables simply cross-connect the transmit lines at each end to the receive lines at the opposite end.



Straight-through Cabling Schematic



Cross-over Cabling Schematic

Note that Ethernet cables use pins 1, 2, 3, and 6 of an 8-pin RJ45 connector. The signals of these pins are converted by the automatic MDI-X function, as shown in the table below:

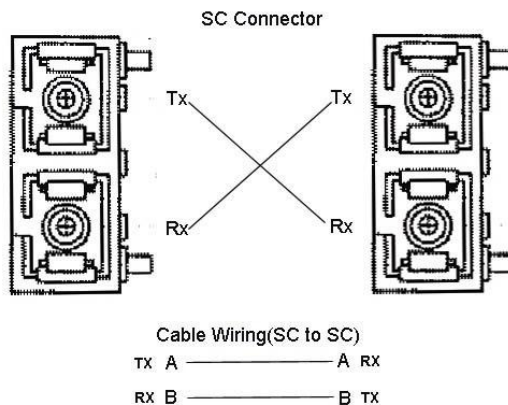
Pin MDI-X	Signals	MDI Signals
1	RD+	TD+
2	RD-	TD-
3	TD+	RD+
6	TD-	RD-

Connect one side of an Ethernet cable into any switch port and connect the other side to your attached device. The green 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 100 meters (328 feet).

Two switches are now up-linked together. If we change the up-link port manually at this time, the MAC address table will change as well. After the MAC address table changes, then the data can be transmitted between these two switches. This period of time is called the MAC address table aging time. The switch's default aging time is 5 minutes, which means that if you manually change the up-link port, you will need to wait up to 5 minutes before the data can be sent. If the aging time is too short, the MAC address table will constantly refresh, resulting in excess consumption of switch computing resources. For this reason, a longer aging time is recommended.

Wiring the Fiber Ports

The automatic MDI/MDI-X crossover function does not apply to fiber connections, as these must be crossed over manually. To connect the fiber port on one switch to the fiber port of another switch, simply cross-connect the transmit channel at each end to the receive channel at the opposite end as illustrated in the figure below.



JetNet 4000 Series fiber models have two 100Base-FX ports with SC type connectors (in multi-mode and single mode versions). Single-mode types have greater distance capability than multi-mode types, but single mode cable is generally more expensive.

A fiber segment using single-mode cable must use 9/125 or 10/125 micrometer single-mode fiber cables. For single-mode, the connection distance can be up to 30 km.

A fiber segment using multi-mode must use 50 or 62.5/125 micrometer multi-mode fiber cables. For multi-mode, the connection distance can be up to 2 km.

DIN-Rail Mounting Installation

The DIN-Rail clip is already attached to the JetNet 4000 Series products when packaged. If the

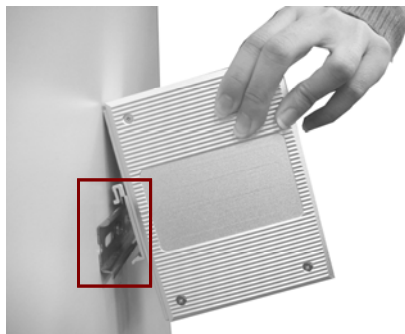
DIN-Rail clip is not screwed on the JetNet, follow the instructions and the figure below to attach the DIN-Rail clip to the JetNet. Here we use JetNet 4008 Industrial Ethernet Switch as an example.

1. Use the screws to attach the DIN-Rail clip to the rear panel of the JetNet 4008.
2. To remove the DIN-Rail clip, reverse step 1.



Follow the steps below to mount the JetNet to the DIN-Rail track.

1. First, insert the upper end of the DIN-Rail clip into the back of the DIN-Rail track from its upper side.



2. Lightly push the bottom of the DIN-Rail clip into the track.



3. Check if the DIN-Rail clip is tightly attached on the track.
4. To remove the JetNet from the track, reverse the steps above.

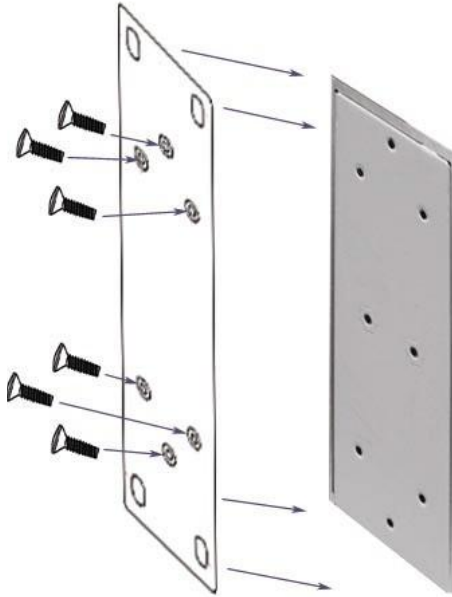
Wall-Mounting Installation

Follow these steps to mount the unit to a wall or other flat surface.

1. Use a screwdriver to remove the two screws that secure the DIN-Rail clip to the back of the

switch.

2. Use a screwdriver to attach the wall-mounting plate to the rear panel of the switch using the six screws provided. Tighten these screws to secure the switch to the wall-mounting plate.
3. Use the slotted holes at each corner of the wall-mounting plate to attach the unit to the wall or other flat surface.
4. To remove the unit from the wall and from the wall-mounting plate, reverse steps 1-3.



3

Web-based Management

This chapter includes information about how to configure and manage your JetNet 4000 Series Industrial Ethernet Switch via a web-based interface.

The following topics are covered in this chapter:

- **Introduction**
- **Preparation for Web Management**
- **System Login**
- **Configuration via the Web-based Management Interface**
 - Menu Bar Introduction
 - Configuring Your JetNet 4000 Series Industrial Ethernet Switch

Introduction

Embedded HTML web pages are stored in non-volatile memory within JetNet 4000 Series Industrial Ethernet Switch. These pages allow you to use a standard web-browser such as Microsoft Internet Explorer, or Mozilla, to configure and interrogate the switch from anywhere on the network.

The internal web-based management interface supports Internet Explorer 5.0 and Mozilla 1.7.5 (including the FireFox version). These easy-to-use management screens are based on Java applets to minimize the consumption of network bandwidth and increase your access speed.

Note: IE 5.0 or later versions do not allow Java applets to open sockets by default. Users have to directly modify the browser settings to selectively enable Java applets to use network ports.

Preparation for Web Management

Before you attempt to use the embedded web interface to manage switch operation, verify that your JetNet 4000 Series Industrial Ethernet Switch is properly installed on your network and that every PC on this network can access the switch via the web browser.

1. Verify that your network interface card (NIC) is operational, and that your operating system supports the TCP/IP protocol.
2. Wire DC power to the switch and connect your switch to your computer.
3. Make sure that the switch default IP address is 192.168.10.1.
4. Change your computer IP address to 192.168.10.2.
5. Switch to DOS command mode and ping 192.168.10.1 to verify a normal response time.

System Login

1. Launch the Internet Explorer on the PC.
2. Type **http://** and the IP address of the JetNet. And then press **Enter**.
3. The login screen will appear next.
4. Key in the user name and the password. The default user name and the password is **admin**.
5. Click on **Enter** or **OK**, and then the homepage of the web-based management interface will appear.
6. Once you enter the web-based management interface, change the JetNet's IP address to fit your network environment.

Function Menu Bar



Configuration via the Web-based Management Interface

Menu Bar Introduction

Home	Port Status	Port Statistics	Port Control	Switch Settings	Port Mirroring	VLAN Configuration
IP Configuration	SNTP	IP Security	RSTP	Super Ring	QoS	IGMP
Security Manager	Configuration Backup	TFTP Update Firmware	Factory Default	Save Configuration	System Reboot	Rate Control

Home

The home page of this embedded web-based management interface.

Port Status

This section is to display the port status and settings.

Port Statistics

This section is to display the JetNet's port data flow statistics.

Port Control

This section is to configure the JetNet's port settings.

Switch Settings

This section is to display the information of the JetNet's system.

Port Mirroring

This section is to enable and configure port mirroring settings.

VLAN Configuration

This section is to enable and configure VLAN settings.

IP Configuration

This section is to set up the JetNet's IP address.

SNTP

This section is to enable the network time server.

IP Security

This section is to set up the IP address which allows users to access the JetNet from the web.

RSTP

This section is to enable and configure the RSTP function.

Super Ring

This section is to enable and configure Super Ring settings.

QoS

This section is to enable and configure QoS(Quality of service) settings.

IGMP

This section is to enable and configure the JetNet's IGMP Snooping function.

Security Manager

This section is to change the username and the password.

Configuration Backup

This section is to backup the JetNet's settings to a file on your PC.

TFTP Update Firmware

This section is to use TFTP utility to update the latest firmware to the JetNet.

Factory Default

This section is to restore the factory default settings.

Save Configuration

This section is to save the JetNet's settings.

System Reboot

This section is to reboot the JetNet.

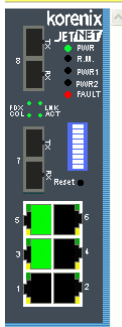
Rate Control

This section is to set up each port's bandwidth rate and packet limitation type.

Configuring Your JetNet 4000 Series Industrial Ethernet Switch

Port Status

Home	Port Status	Port Statistics	Port Control	Switch Settings	Port Mirroring	Vlan Configuration
Ip Configuration	SNTP	Ip Security	RSTP	Super Ring	QoS	IGMP
Security Manager	Configuration Backup	TFTP Update Firmware	Factory Default	Save Configuration	System Reboot	Rate Control



Port Status

Port	Type	Link	State	Negotiation	Speed Duplex		Flow Control	
					Config	Actual	Config	Actual
Port.01	100TX	Down	Enable	Auto	100 Full	N/A	Symmetric	N/A
Port.02	100TX	Down	Enable	Auto	100 Full	N/A	Symmetric	N/A
Port.03	100TX	Up	Enable	Auto	100 Full	100 Full	Symmetric	ON
Port.04	100TX	Down	Enable	Auto	100 Full	N/A	Symmetric	N/A
Port.05	100TX	Up	Enable	Auto	100 Full	100 Full	Symmetric	ON
Port.06	100TX	Down	Enable	Auto	100 Full	N/A	Symmetric	N/A
Port.07	100FX	Down	Enable	Force	100 Full	N/A	Asymmetric	N/A
Port.08	100FX	Down	Enable	Force	100 Full	N/A	Asymmetric	N/A

In this window, you can see each port's status.

Port: Indicates the port number.

Type: Indicates the speed mode of the port. For example, 100TX means 100 Mbps.

Link: **Down** Indicates that connection is not established; **“Up”** indicates that the connection is successfully established.

State: Indicates whether this port is **Enabled** or **Disabled**. A disconnection is also denoted as **Disabled**.

Negotiation: “Auto” means that the switch will auto-negotiate the speed (automatically select 10M or 100M bps), and the transmission mode (full or half duplex), with the remote device. Force means that the switch will run according to your own forced settings for speed and duplex.

Speed/Duplex: Indicates the port speed. **Config** column shows the configuration set up by

users. The **Actual** column shows the actual speed of the port.

Flow Control: Configured and Actual – “Symmetric” specifies 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 of the switch to work. “Asymmetric” indicates that you don’t need to activate the flow control function of the remote network device. The flow control of that corresponding port on the switch will work anyway.

Single Port Status

To get the single port status screen, you can click directly on any port number displayed at left to see port-specific information for that port and similar to that listed below:

Port	6
Link	Up
State	On
Tx Good Packet	2632
Tx Bad Packet	0
Rx Good Packet	2232
Rx Bad Packet	0
Tx Abort Packet	0
Packet Collision	0

Port Statistics

Port	Type	Link	State	Tx Good Packet	Tx Bad Packet	Rx Good Packet	Rx Bad Packet	Tx Abort Packet	Packet Collision
Port.01	100TX	Down	Enable	0	0	0	0	0	0
Port.02	100TX	Up	Enable	270	0	14376	0	0	0
Port.03	100TX	Down	Enable	0	0	0	0	0	0
Port.04	100TX	Down	Enable	0	0	0	0	0	0
Port.05	100TX	Down	Enable	0	0	0	0	0	0
Port.06	100TX	Down	Enable	0	0	0	0	0	0
Port.07	100FX	Down	Enable	0	0	0	0	0	0
Port.08	100FX	Down	Enable	0	0	0	0	0	0

In this section, you can view operation statistics for each port. Click on **Clear** to reinitialize and clear any counts.

Port Control

Port	State	Negotiation	Speed	Duplex	Flow Control
Port.01					
Port.02	Enable	Auto	100	Full	Symmetric
Port.03					
Port.04					

Port	Type	Link	State	Negotiation	Speed Duplex		Flow Control	
					Config	Actual	Config	Actual
Port.03	100TX	Up	Enable	Auto	100 Full	100 Full	Symmetric	ON

You can change the port settings here.

Simply select the port you want to configure and you will be able to view the current status and settings of the selected port, and make changes to port settings as required.

In **State** column, you can enable or disable the control over this port.

In **Negotiation** column, you can configure the auto negotiation mode to **Auto** to enable automatic negotiation, or Force (to directly specify the speed/duplex on this port).

In **Speed** column, you can configure the speed of this port.

In **Duplex** column, you can configure the full-duplex or half-duplex mode of this port.

In **Flow Control** column, “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 JetNet to work. “Asymmetric” means that you don’t need to activate the flow control function of the remote network device, as the flow control of that corresponding port on the JetNet will work anyway.

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

Note: Remember to click on the **Save Configuration** button to save your settings. Otherwise, the settings you made will be lost when the JetNet is powered off.

Switch Settings

Switch Settings

System Description	Industrial Managed Ethernet Switch JetNet 4508f
System Name	
System Location	
System Contact	

Firmware Version	v2.09
Kernel Version	v3.20
Hardware Version	A5.00
MAC Address	0012770114FA

You can assign the system name, location, and view the system information.

System Description: You can briefly describe the JetNet you are using.

System Name: You can assign a name to the JetNet industrial Ethernet switch.

System Location: You can specify the JetNet’s physical location here.

System Contact: You can specify the Contact people here.

Firmware Version: Displays the firmware version installed in this JetNet.

Kernel Version: Displays the kernel version in this JetNet.

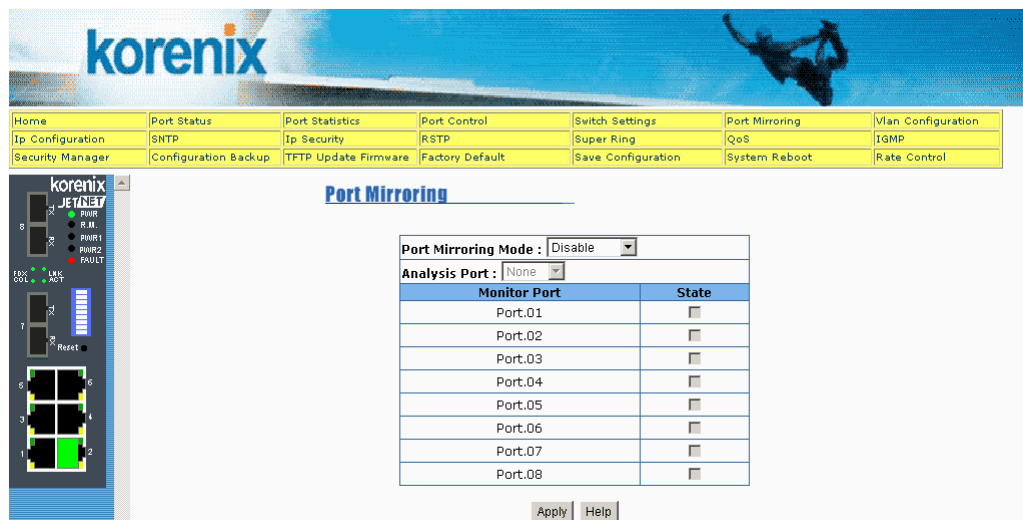
Hardware Version: Displays the hardware version of this JetNet.

MAC Address: Displays the unique hardware address (MAC address) assigned by the manufacturer (the default setting).

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

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

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 monitored port(s) will be duplicated at the mirror port. This traffic can then be analyzed at the mirror port using a monitoring device. A network administrator will typically utilize this tool for diagnostics or debugging, or to fend off attacks.

Port Mirroring State: Select mirroring mode, including Disable, Rx, Tx, or both Rx & Tx.

Analysis Port: This is the mirror 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. A network administrator would typically connect a LAN analyzer or Netxray device to this port.

Monitor Port: These are the ports you want to monitor. The traffic of all monitored ports will be copied to mirror ports. You can choose a single port, or any combination of ports, but you can only monitor them in one mirror mode. To disable this function, set the monitor port to **None**.

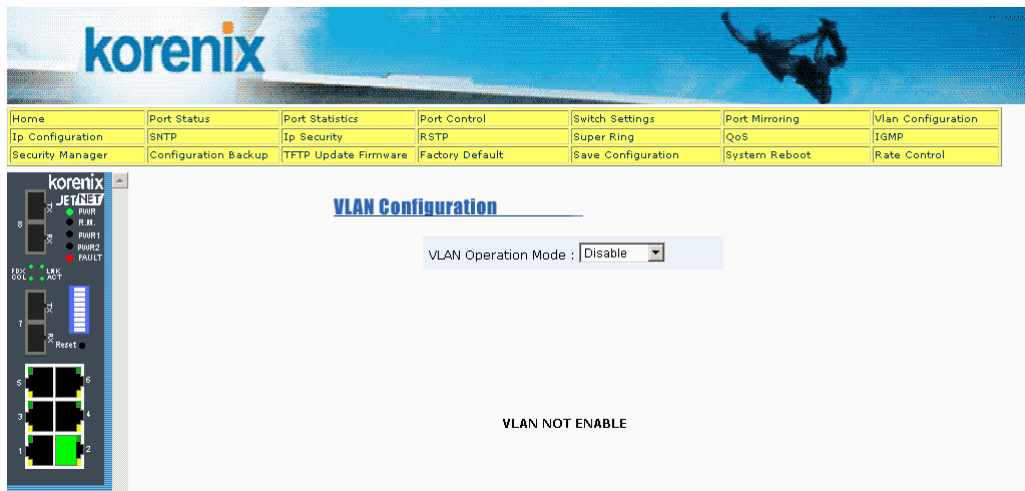
Once you finish configuring the settings, click on **Apply** to apply the settings.

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

VLAN Configuration

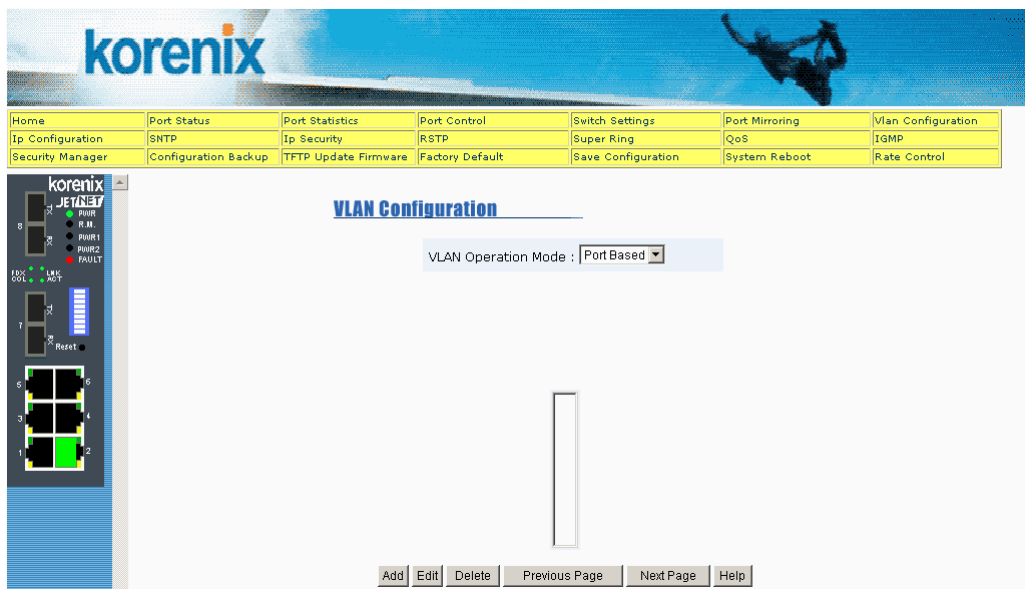
A Virtual LAN (VLAN) is a “logical” grouping of nodes for the purpose of limiting a broadcast domain to specific members of a group, but without physically grouping the members together. That is, a VLAN allows you to isolate network traffic so that only members of the VLAN would receive traffic from 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 switch.

JetNet 4000 Series Industrial Ethernet Switch supports both port-based and 802.1Q (tagged-based) VLAN’s. The VLAN Operation Mode is set to “**disable**” by default.



Port-based VLAN

Packets only go to the members of the same VLAN groups. Note that all of the unselected ports are treated as belonging to another single VLAN. If the port-based VLAN enabled, the VLAN-tagging will be ignored.



1. Click on **Add** to add a new VLAN group.
2. Enter the VLAN name, group IP, and then select the members for this VLAN group.
3. Click on **Apply** to adopt the settings.
4. Next you will see the VLAN group be displayed.
5. If the groups list is longer than one page, you can click on **Next Page** to view other VLAN groups.
6. Use **Delete** button to delete unwanted VLANs.
7. Use **Edit** button to modify the existing VLANs.

Note: Remember to click on the **Save Configuration** button to save your settings. Otherwise the settings you made will be lost when the JetNet is powered off.

Because the port-based VLAN is defined on the switch itself and does not use information contained in the packet frame to define its membership, it is restricted to ports of the same switch. Effectively, only the switch itself knows the architecture of a port-based VLAN, while the segments connected to the switch ports have no way of knowing the VLAN definition even exists. This is the key difference between port and tag based Virtual LAN's.

802.1Q VLAN

This tag-based VLAN is an IEEE 802.1Q standard, which allows VLAN's to be created across different switches (see Figure 1). IEEE 802.1Q tag-based VLAN's make 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 a 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.

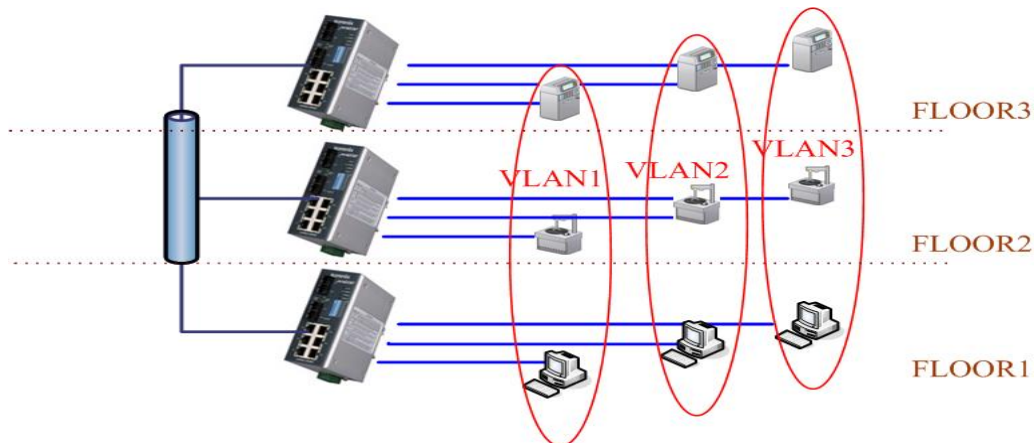
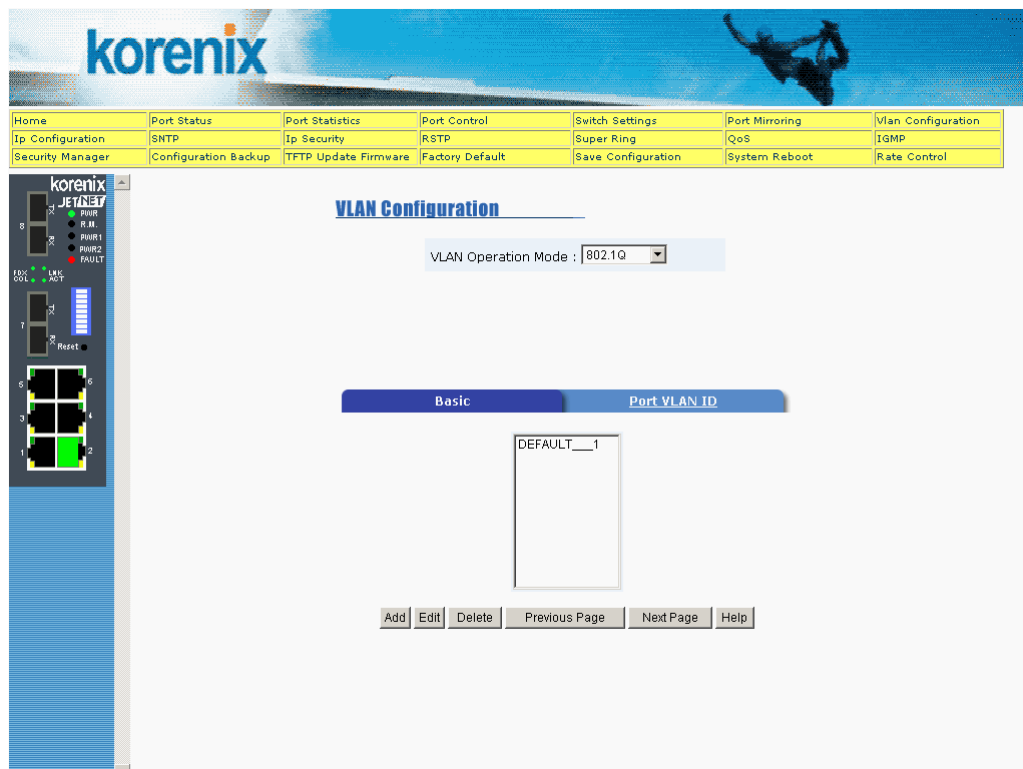
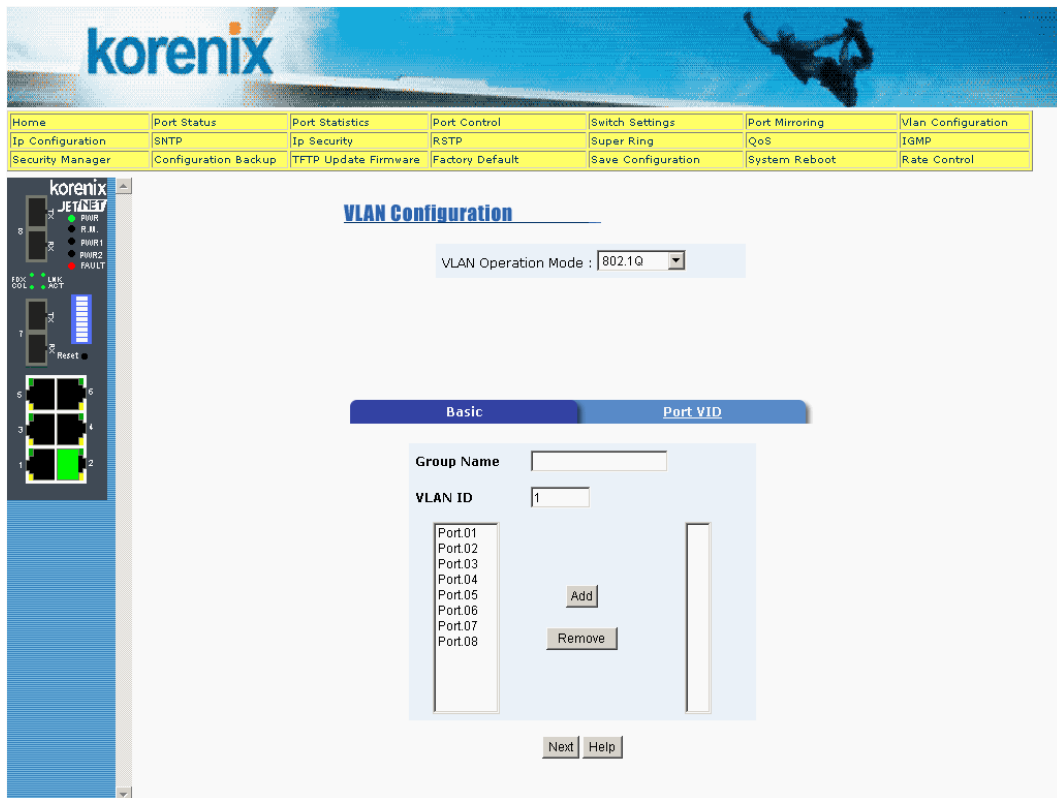


Figure.1 Tagged VLAN

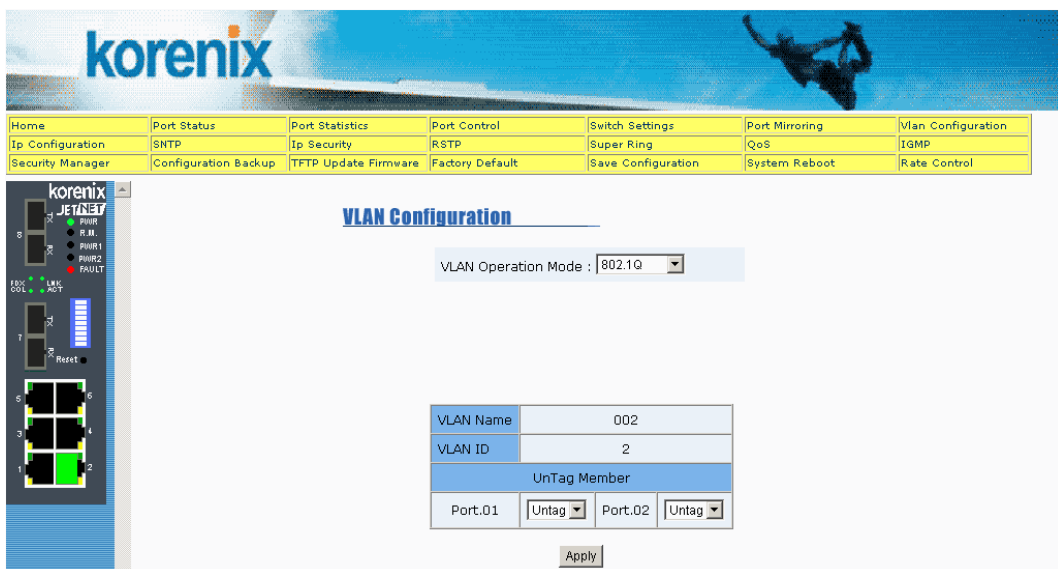


Basic

1. Click on **Add** button to add a new tag-based VLAN.



2. **Group Name:** You can assign a name for the new VLAN here. The Group Name is a reference for the network administrator to identify different VLANs.
3. **VLAN ID:** You can type in VLAN ID here (the value is between 2 and 4094). The default value is 1. The VLAN ID is used by switches to identify different VLANs.
4. Select specific ports of this switch to be included in the VLAN from the available ports box. Click **Add** to add ports to the VLAN, or **Remove** to remove ports from the VLAN. Then click **Next** to continue. Please note that each VLAN will require a “tagged port”. Different VLANs use these tagged ports to communicate with one another.

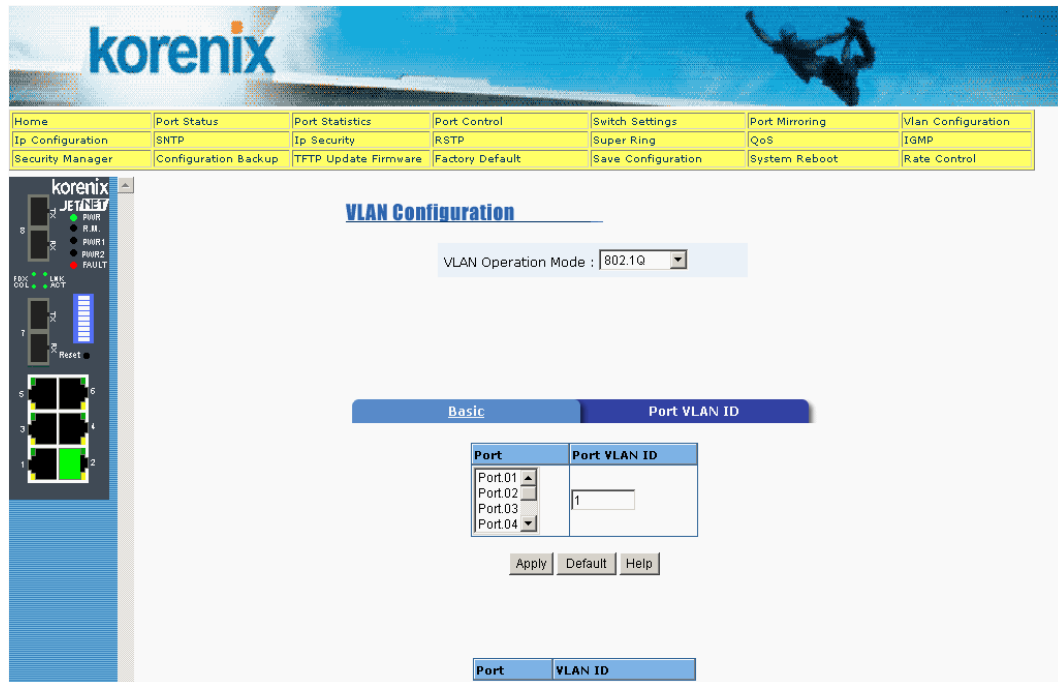


5. Here you can specify the egress (outgoing) VLAN frames to be **Tagged** frames or **Untagged** frames. And click on **Apply** to apply the settings.

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

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

Port VID



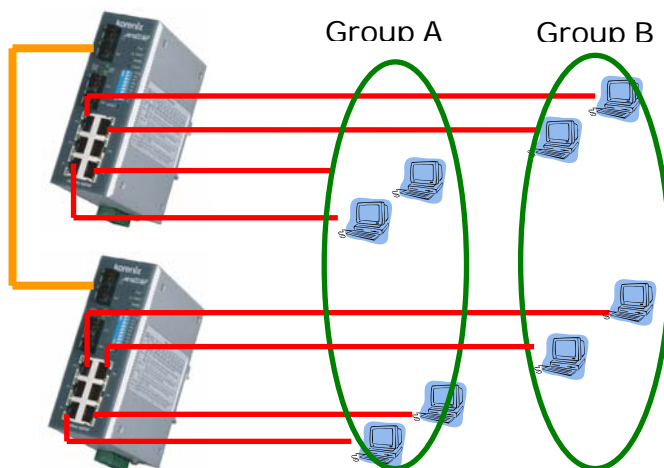
Port VLAN ID (PVID): Enter the port VLAN ID here. The Port VID (PVID) allows the switches to identify which port belongs to which VLAN. To keep things simple, it is recommended that you set the Port VID equivalent to the VLAN IDs. You can skip tagged ports, as tagged ports do not need Port VLAN IDs.

To reset to the default values, click on **Default**.

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

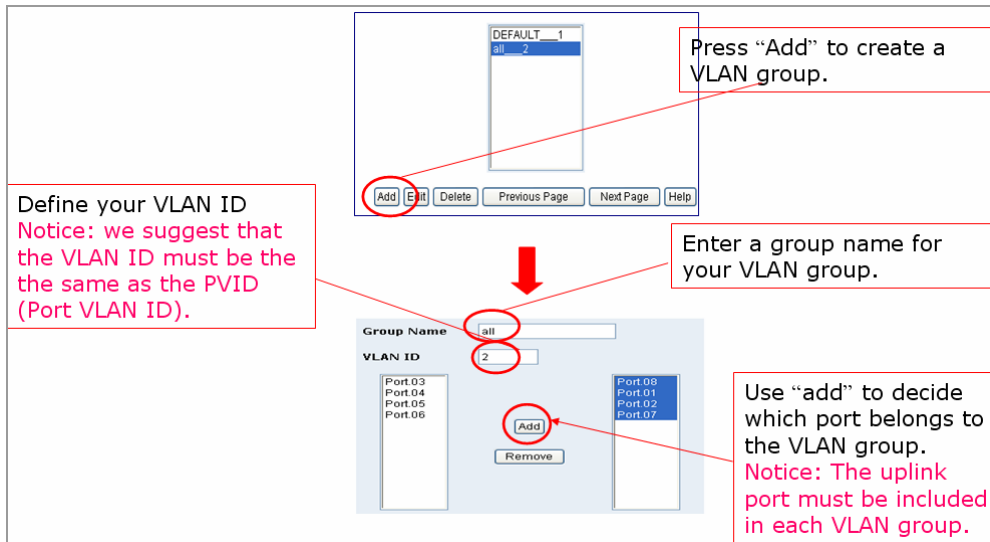
Note: Always remember to select **Save Configuration** to save your settings. Otherwise, the settings you made will be lost when the switch is powered off.

How To Set Up a 802.1Q VLAN—Reference Example.



To illustrate a tag-based VLAN, we would like to use all Port 1's and Port 2's of switch 1 and switch 2 to form a VLAN Group A, and all Port 5's and Port 6's to form a VLAN Group B. This will restrict VLAN A and VLAN B from communicating with each other, except through their port 8's which they will use to transmit data to each other (this is their tagged port). The tagged VLAN settings for switch 1 are as follows (settings for switch 2 are the same those for switch 1):

1. You must specify which port(s) belong to the VLAN.



1.1 Click **Add** to create VLAN A.

1.2 Enter a group name and a VLAN ID (VID) for VLAN A (you cannot use "1" as a VLAN ID, as "1" is reserved for the default VID).

1.3 Use **Add** to include the ports that belongs to this VLAN (Port 1 and Port 2). Don't forget to include the tagged/uplink port (uplink Port 8).

1.4 Repeat Step 1.1 to 1.3 to create VLAN B.

2. Set up Tagged Port. Be sure to set up the Tag (uplink) Port (port 8 for our example). Thus, VLAN A and VLAN B can only communicate with one another via transmission from their port 8.

The ports which you set up in step 1.

VLAN Name	sdw	
VLAN ID	2	
UnTag Member		
Port.01	Untag	Port.02 Untag
Port.08	Tag	

Apply

Set up the uplink port to be the "tag port".

Mark the tagged port in the VLAN A and VLAN B via the web management interface.

3. Set up Port VLAN ID

Follow the instructions described in Port VLAN ID (PVID) section to set up the port VLAN IDs for each Untag port. It is recommended that each port's port VLAN ID be set to the same value as the VLAN ID (VID) to which it belongs. Tag (uplink) ports do not need any port VLAN ID.

Set up each port's Port VLAN ID(PVID).
 Notice 1: Don't need to set up the uplink port's PVID.
 Notice 2: we suggest that the PVID must be the same as the VLAN ID.

The port which has been grouped by tagged VLAN.

When you change the Port VLAN ID, remember to press "Apply" to validate the change.

4. Always remember to select **Save Configuration** to save your settings. Otherwise, your settings will be lost when the JetNet is powered off.
5. Repeat step 1 to 4 to set up the second switch (the settings for the second switch are the same).
6. Since the settings for the second switch are exactly the same as the first one, you can use Configuration Backup function to copy the first switch's settings and restore them to the second switch. This will reduce the time required to set up the second switch. Refer to Configuration Backup section for more information.

IP Configuration

IP Configuration

DHCP Client:

IP Address:

Subnet Mask:

Gateway:

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

DHCP Client: You can select to **Enable** or **Disable** the DHCP Client function. When the DHCP Client function is enabled, an IP address will be assigned to the JetNet from the network's DHCP server. In this mode, the default IP address will therefore be replaced by the one assigned by the DHCP server. If the DHCP Client is disabled, then the IP address that you specify will be used instead.

IP Address: You can assign the IP address that your network has reserved for your JetNet. If the
 Korenix JetNet Series Industrial Web-Managed Ethernet Rail Switch User's Manual 3-13

DHCP Client function is enabled, you don't need to assign an IP address to the JetNet, as it will be overwritten by the DHCP server and shown here. The default IP is 192.168.10.1.

Subnet Mask: You can assign the subnet mask for the IP address here. If the DHCP Client function is enabled, you don't need to assign the subnet mask.

Gateway: You can assign the gateway for the JetNet here. The default gateway is 192.168.10.254.

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

SNTP

SNTP Configuration

SNTP Client : ▼

Daylight Saving Time : ▼

UTC Timezone	<input type="button" value="(GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London"/> ▼	
SNTP Server IP	<input type="text" value="0.0.0.0"/>	
Switch Timer	<input type="text"/>	
Daylight Saving Period	<input type="text" value="20040101 00:00"/>	<input type="text" value="20040101 00:00"/>
Daylight Saving Offset(mins)	<input type="text" value="0"/>	

The Simple Network Time Protocol (SNTP) is an adaptation of the Network Time Protocol (NTP), used to synchronize computer clocks on the internet. You can configure the SNTP settings here for the purpose of synchronizing the clocks of several switches on the network. SNTP is maintained by the Internet Engineering Task Force (IETF).

SNTP Client: Select **Enable** to acquire the current time from the SNTP server, or **Disable** to disable this feature.

Daylight Saving Time: You can activate **Daylight Savings Time** function here.

UTC Time-zone: Select the time zone where the JetNet is located. The following table lists the time zones for different locations for your reference.

Local Time Zone	Conversion from UTC	Time at 12:00 UTC
ADT - Atlantic Daylight	-3 hours	9 am
AST - Atlantic Standard EDT - Eastern Daylight	-4 hours	8 am
EST - Eastern Standard CDT - Central Daylight	-5 hours	7 am
CST - Central Standard MDT - Mountain Daylight	-6 hours	6 am
MST - Mountain Standard PDT - Pacific Daylight	-7 hours	5 am
PST - Pacific Standard ADT - Alaskan Daylight	-8 hours	4 am
ALA - Alaskan Standard	-9 hours	3 am
HAW - Hawaiian Standard	-10 hours	2 am
Nome, Alaska	-11 hours	1 am

CET - Central European FWT - French Winter MET - Middle European MEWT - Middle European Winter SWT - Swedish Winter	+1 hour	1 pm
EET - Eastern European, USSR Zone 1	+2 hours	2 pm
BT - Baghdad, USSR Zone 2	+3 hours	3 pm
ZP4 - USSR Zone 3	+4 hours	4 pm
ZP5 - USSR Zone 4	+5 hours	5 pm
ZP6 - USSR Zone 5	+6 hours	6 pm
WAST - West Australian Standard	+7 hours	7 pm
CCT - China Coast, USSR Zone 7	+8 hours	8 pm
JST - Japan Standard, USSR Zone 8	+9 hours	9 pm
EAST - East Australian Standard GST Guam Standard, USSR Zone 9	+10 hours	10 pm
IDLE - International Date Line NZST - New Zealand Standard NZT - New Zealand	+12 hours	Midnight

SNTP Server IP: You can set the IP address of the SNTP server here.

Switch Timer: The current time of the JetNet will be shown here.

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

IP Security

IP Security

Enable IP Security

Security IP1	0.0.0.0
Security IP2	0.0.0.0
Security IP3	0.0.0.0
Security IP4	0.0.0.0
Security IP5	0.0.0.0
Security IP6	0.0.0.0
Security IP7	0.0.0.0
Security IP8	0.0.0.0
Security IP9	0.0.0.0
Security IP10	0.0.0.0

Apply Help

management access to this JetNet via a web browser.

Enable IP Security: Check this option to enable the IP security function.

Security IP 1 to 10: You can assign up to 10 specific IP addresses. Only these 10 IP addresses can access and manage this JetNet via a web browser.

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

RSTP

The screenshot shows the Korenix JetNet web interface. At the top, there's a navigation menu with items like Home, Port Status, Port Statistics, Port Control, Switch Settings, Port Mirroring, and Vlan Configuration. Below the menu is a status bar with various system indicators. The main content area is titled "Spanning Tree" and has two tabs: "System Configuration" (selected) and "Per Port Configuration". Under "System Configuration", there are several configuration fields: RSTP Mode (set to "Disable"), Priority (0-61440) (set to 32768), Max Age (6-40) (set to 20), Hello Time (1-10) (set to 2), and Forward Delay Time (4-30) (set to 15). Below these fields is a note: "Priority must be a multiple of 4096" and "2*(Forward Delay Time-1) should greater than or equal to Max Age" and "Max Age should be greater than or equal to 2*(Hello Time + 1)". There is an "Apply" button. Below the configuration fields is a table titled "Root Bridge Information" with the following data:

Root Bridge Information	
Bridge ID	N/A
Root Priority	N/A
Root Port	N/A
Root Path Cost	N/A
Max Age	N/A
Hello Time	N/A
Forward Delay	N/A

If a switch has more than one path to a destination, this leads 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 that a switch has more than one way to communicate with a node. Then it selects the best path (primary), and blocks the other path(s). It also keeps track of the blocked path(s) in case the primary path fails. The Spanning Tree Protocol (STP) introduced a standard method for accomplishing this and this is specified in IEEE 802.1d. Later, the Rapid Spanning Tree Protocol (RSTP) was adopted and represents the evolution of STP, providing much faster spanning tree convergence after a topology change. This switch supports both RSTP and STP (all switches that support RSTP are also backward compatible with switches that support only STP).

System Configuration

Under the "System Configuration" tab, you can change the spanning tree settings and view the Root Bridge Information. Note that switches are also referred to as bridges. Root bridges are related to the spanning tree.

RSTP Mode: You must first enable the STP or RSTP mode, before configuring any related parameters. The parameter settings required for both STP and RSTP are the same. Note that 802.1d refers to STP mode, while 802.1w refers to the faster RSTP mode.

Priority (0-61440): This value must be in multiples of 4096 and represents the bridge ID number. This number is used to identify the root bridge. A root bridge continuously transmits network topology information to other bridges (switches) using the spanning tree protocol and serves to notify other bridges on the network when topology changes are required. It is located where the paths that frames take through the network are assigned, and usually centrally located to provide the shortest path to other links on the network. Like a hub, a root bridge will forward frames out to all of its ports. Every network should have one root bridge and it is usually assigned the lowest bridge ID. The bridge with the lowest bridge ID number has the highest priority, and is selected as the root bridge. If you happen to change this value, you must reboot the switch to cause the system to assign a new path priority number.

Note that you increase this switches priority by selecting a lower number. A device with a lower

number has a higher bridge priority and thus a greater chance of being established as the root bridge of the spanning tree topology.

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 a reconfiguration.

If this JetNet is not the root bridge, and it has not received a hello message from the root bridge in an amount of time equal to Max Age, then this JetNet will reconfigure itself as a root bridge. Then 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 the periodic timer that drives the switch to send out the BPDU (Bridge Protocol Data Unit) packet to check on the 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 waits 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 the Spanning Tree Protocol learning and listening states to the forwarding state.

This is the amount of time this JetNet will wait before checking to see if it should change to a different state.

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

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

$2 \times (\text{Forward Delay Time} - 1 \text{ sec}) \geq \text{Max Age Time} \geq 2 \times (\text{Hello Time value} + 1 \text{ sec})$

Suggested Strategy:

1. Select a Hello Time value and compute the rightmost portion of the rule above to get the lower limit of Max Age.
2. Select a Forward Delay time and compute the leftmost portion of the rule above to get the upper limit of Max Age.
3. Select a Max Age from 6 to 40 seconds that is between the limits computed above.

Per Port Configuration

The screenshot shows the 'Per Port Configuration' interface for a Korenix switch. It features a navigation menu at the top with options like Home, Port Status, Port Statistics, Port Control, Switch Settings, Port Mirroring, and Vlan Configuration. The main content area is titled 'Spanning Tree' and has two tabs: 'System Configuration' and 'Per Port Configuration'. The 'Per Port Configuration' tab is active, showing a table with columns for Port, Path Cost (1-20000000), Priority (0-240), Admin P2P, Admin Edge, and Admin Non Stp. The table shows settings for Port.01 through Port.05. Below the table, there is a note: 'priority must be a multiple of 16' and buttons for 'Apply' and 'Help'. At the bottom, there is an 'RSTP Port Status' table with columns for Port, Path Cost, Port Priority, Admin P2P, Admin Edge, Stp Neighbor, State, and Role. The RSTP Port Status table shows the current status for all ports from Port.01 to Port.08.

Port	Path Cost (1-20000000)	Priority (0-240)	Admin P2P	Admin Edge	Admin Non Stp
Port.01	2000000	128	Auto	True	False
Port.02	2000000	128	Auto	True	False
Port.03	2000000	128	Auto	True	False
Port.04	2000000	128	Auto	True	False
Port.05	2000000	128	Auto	True	False

priority must be a multiple of 16

Port	Path Cost	Port Priority	Admin P2P	Admin Edge	Stp Neighbor	State	Role
Port.01	2000000	128	True	True	False	Disabled	Disabled
Port.02	2000000	128	True	False	True	Forwarding	Designated
Port.03	2000000	128	True	True	False	Disabled	Disabled
Port.04	2000000	128	True	True	False	Disabled	Disabled
Port.05	2000000	128	True	True	False	Disabled	Disabled
Port.06	2000000	128	True	True	False	Disabled	Disabled
Port.07	2000000	128	True	True	False	Disabled	Disabled
Port.08	2000000	128	True	True	False	Disabled	Disabled

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

Path Cost: Enter a number between 1 and 200,000,000. This value represents the “cost” of the path to the other bridge from this 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.

Admin P2P: Some of the rapid state transitions that are possible within RSTP depend upon whether the port of concern can only be connected to one other 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 the P2P status of the link to be manipulated administratively. “**True**” means P2P is enabled, while “**False**” means P2P is disabled.

Admin 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 **True** state.

Admin Non STP: Status shown here indicates whether this port includes the STP mathematic calculation. **True** means that this port does NOT include the STP mathematic calculation. **False** means that this port includes the STP mathematic calculation.

Once you finish your configuration, click **Apply** to save your settings.

Note: Always remember to select **Save Configuration** to save your settings. Otherwise, your new settings will be lost when the switch is powered off.

Super Ring

Super Ring technology provides a faster redundant media fail-over recovery than the Spanning Tree Protocol (STP), or Rapid Spanning Tree Protocol (RSTP). But unlike STP/RSTP, it additionally requires that all switches in the media ring be of the same brand (have the same redundant ring method), as most redundant ring algorithms are proprietary and rarely interoperable. Since STP and RSTP are standard IEEE protocols, switches that employ these two methods of media redundancy are generally interoperable with one another.

With Super Ring, every switch in the ring must support the same redundant ring method and have two ring member ports. One switch in this ring is dedicated to serve as Ring Master, and one of its two member ports will be temporarily blocked--this is referred to as the backup port. The other member port is called the working port. The other switches in the ring are called working switches, and both their member ports are called working ports. When a segment of this

ring fails, the backup port/path will automatically become a working port/path to recover the failure.

Super Ring

<input checked="" type="checkbox"/> Enable Super Ring	
1st Ring Port	Port.05 ▼
2nd Ring Port	Port.06 ▼

Enable Super Ring: You can enable the Super Ring function by checking this option.

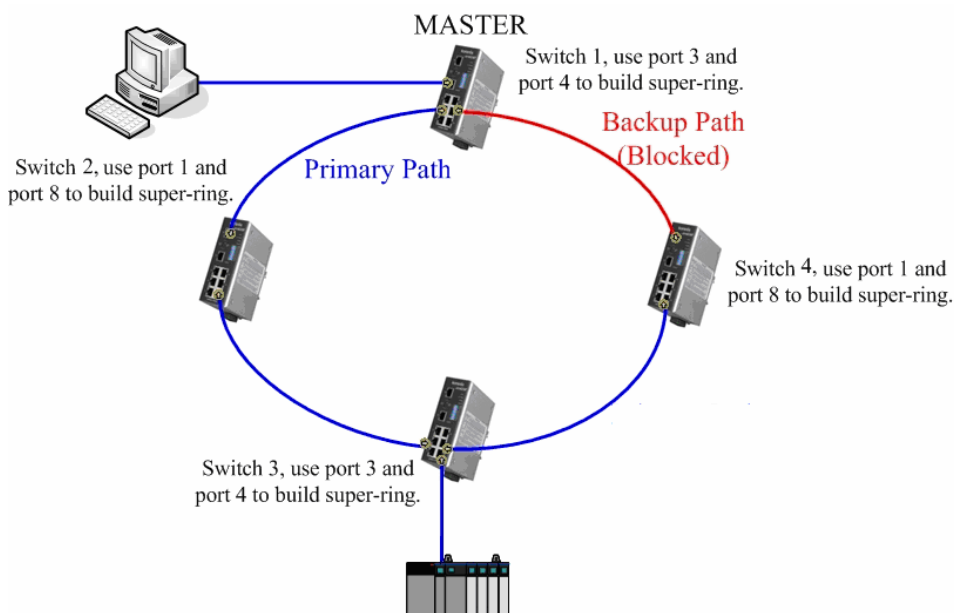
Note: You must enable the Super Ring function before connecting any backup path to prevent the inadvertent generation of message loops.

1st Ring Port / 2nd Ring Port: You can assign 2 ports, 1st Ring Port and 2nd Ring port as member ports here. 1st Ring port of the Ring Master will be the working port, and the 2nd Ring port of the Ring Master will be the backup port, the port will be blocked. The Ring Ports of the non-Ring Master will be the forwarding ports.

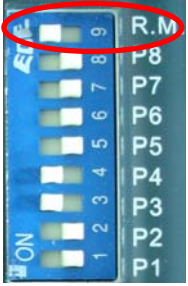
Once you finish configuring the settings, click on **Apply** to apply the configuration.

Note: When you enable the Super Ring function, you must disable RSTP. The Super Ring function and the RSTP function cannot be both enabled at the same time.

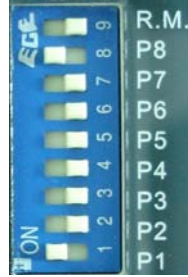
How to Set Up a Super Ring?



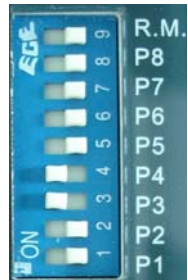
Here we use 4 JetNet 4008 Industrial Ethernet Switches to form a Super Ring topology. Switch 1 is configured to be the Ring Master, and the 1st Ring Port of the R.M. is the forwarding/primary path, the 2nd Ring Port of R.M. is the backup path. R.M. will continuously sent hello packet through port 3 to next switch and receive the returned hello packet from port 4.



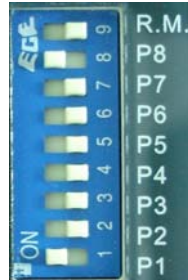
The settings of Switch 1, Ring Master.
 Click the R.M. DIP to ON. The web UI will show The switch is Ring Master. Port 3 and Port 4 are the Ring Ports.



The settings of Switch 2.
 The Port 1 and Port 8 are the Ring Ports. The 2 ports of non-R.M. are forwarding ports.



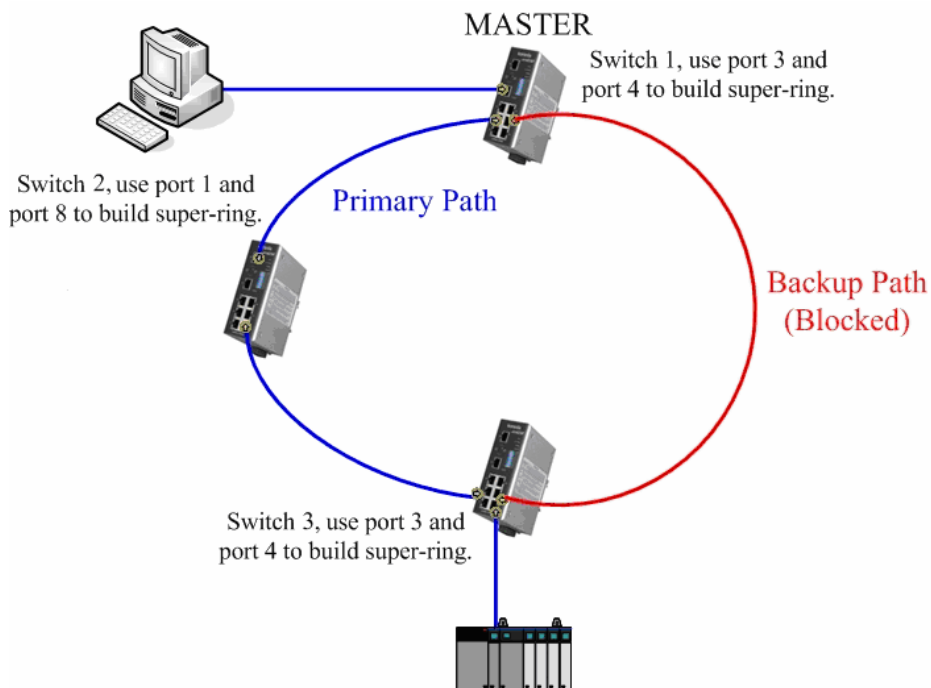
The settings of Switch 3.
 The Port 3 and Port 4 are the Ring Ports. The 2 ports of non-R.M. are forwarding ports.



The settings of Switch 4.
 The Port 1 and Port 8 are the Ring Ports. The 2nd Ring Port is connected back to R.M. So that the path between R.M and Switch 4 is Backup path (Blocked).

Note: Before you connect a backup path to complete the loop, you need to finish configuring the settings described above on all ring switches. Otherwise, it will cause an immediate message loop.

Can 3 Switches Form a Super Ring Topology?



Here we use 3 JetNet 4008 Industrial Ethernet Switches to form a Super Ring topology. Switch 1 is configured to be the Ring Master, and the backup path will be decided by this Ring Master. In this example, the path on the right is the backup path.

Enable Super Ring

1st Ring Port Port.03

2nd Ring Port Port.04

This switch is Ring Master.



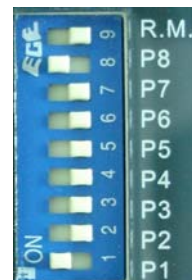
The settings of Switch 1, Ring Master.

Click the R.M. DIP to ON. The web UI will show The switch is Ring Master. Port 3 and Port 4 are the Ring Ports.

Enable Super Ring

1st Ring Port Port.01

2nd Ring Port Port.08



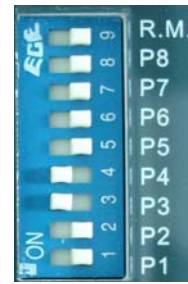
The settings of Switch 2.

The Port 1 and Port 8 are the Ring Ports. The 2 ports of non-R.M. are forwarding ports.

Enable Super Ring

1st Ring Port Port.03

2nd Ring Port Port.04



The settings of Switch 3.

The Port 3 and Port 4 are the Ring Ports. The 2nd Ring Port is connected back to R.M. So that the path between R.M and Switch 3 is Backup path (Blocked).

Note: Before you connect the backup path (last loop segment), you need to finish configuring the settings described above on all ring switches. Otherwise, it will cause an immediate message loop.

QoS

QoS (Quality of Service) is a broad term that refers to measures taken to specify a guaranteed throughput level. QoS with respect to this JetNet utilizes the prioritization of traffic to accomplish this. This section allows you to configure the QoS settings for each port with regard to setting priorities.

QoS

QoS Policy

- Use an 8,4,2,1 weighted fair queuing scheme
- Use a strict priority scheme

Priority Type:

Port.01	Port.02	Port.03	Port.04	Port.05	Port.06	Port.07	Port.08
Port-based	Port-based	Port-based	Port-based	Port-based	Port-based	Port-based	Port-based

Default Port Priority:

Port.01	Port.02	Port.03	Port.04	Port.05	Port.06	Port.07	Port.08
Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest

Apply Help

QoS Policy

You can select the QoS policy rule as follows:

Use an 8,4,2,1 weighted fair queuing scheme. The JetNet will follow 8:4:2:1 rate to process the packets in a queue from the highest priority to the lowest. For example, the system will process 8 packets with the highest priority in the queue, 4 with middle priority, 2 with low priority, and 1 with the lowest priority at the same time.

Use a strict priority scheme. Packets with higher priority in the queue will always be processed first, except that there is no packet with higher priority.

Priority Type

Each port has 5 priority types for you to select.

Port-based: The port priority will follow the default port priority that you have assigned – High, middle, low, or the lowest.

COS only: the port priority will only follow the COS priority that you have assigned.

TOS only: the port priority will only follow the TOS priority that you have assigned.

COS first: the port priority will follow the COS priority first, and then other priority rule.

TOS first: the port priority will follow the TOS priority first, and then other priority rule.

Default Priority Type

This is to decide the default priority of each port.

The CoS value of the Lowest priority is 1 or 2. The default is 2.

The CoS value of the Low priority is 0 or 3. The default is 0.

The CoS value of the Middle priority is 4 or 5. The default is 4.

The CoS value of the High priority is 6 or 7. The default is 6.

CoS-Queue Mapping

This is to map the CoS value to the physical queue. The switch supports 4 physical queues. So that you should map the CoS value to the physical queues when you want use this CoS feature. The physical queue include High, Middle, Low and Lowest.

The 802.1p suggests you to use CoS value 0 and 3 to Low, 1 and 2 to Lowest, 4 and 5 to Middle, 6 and 7 to High.

COS

Priority	0	1	2	3	4	5	6	7
	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾

Apply Help

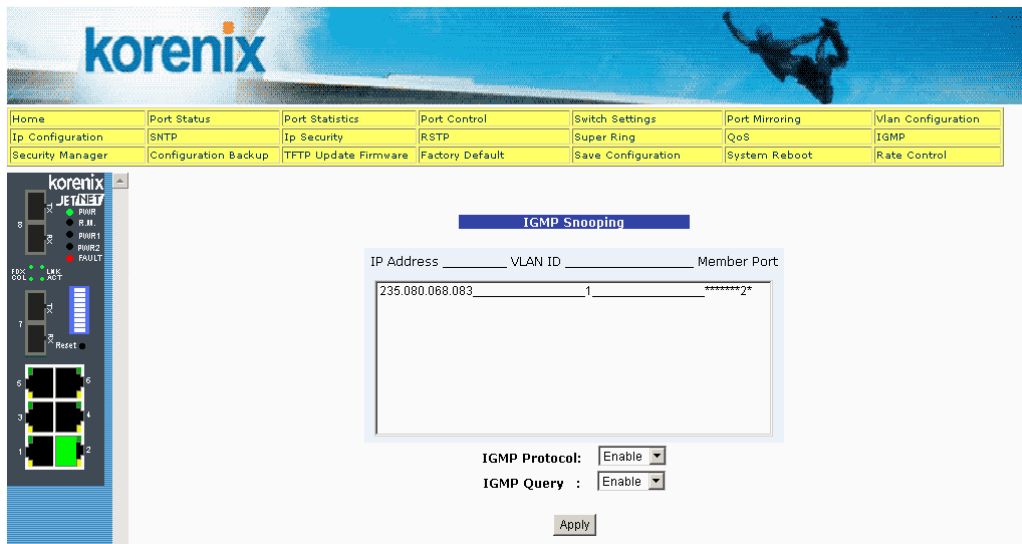
ToS-Queue Mapping

TOS is also known as DSCP. This is the field in the IP TOS packet. If the L3 switch or Router use this field as the QoS service. Then the L2 switches attached to the network should have the same policy as the L3 switch or Router. This table allows you to configure the queue level for each DSCP value.

TOS

Priority	0	1	2	3	4	5	6	7
	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾
Priority	8	9	10	11	12	13	14	15
	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾
Priority	16	17	18	19	20	21	22	23
	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾
Priority	24	25	26	27	28	29	30	31
	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾
Priority	32	33	34	35	36	37	38	39
	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾
Priority	40	41	42	43	44	45	46	47
	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾
Priority	48	49	50	51	52	53	54	55
	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾
Priority	56	57	58	59	60	61	62	63
	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾	Lowest ▾

IGMP



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.

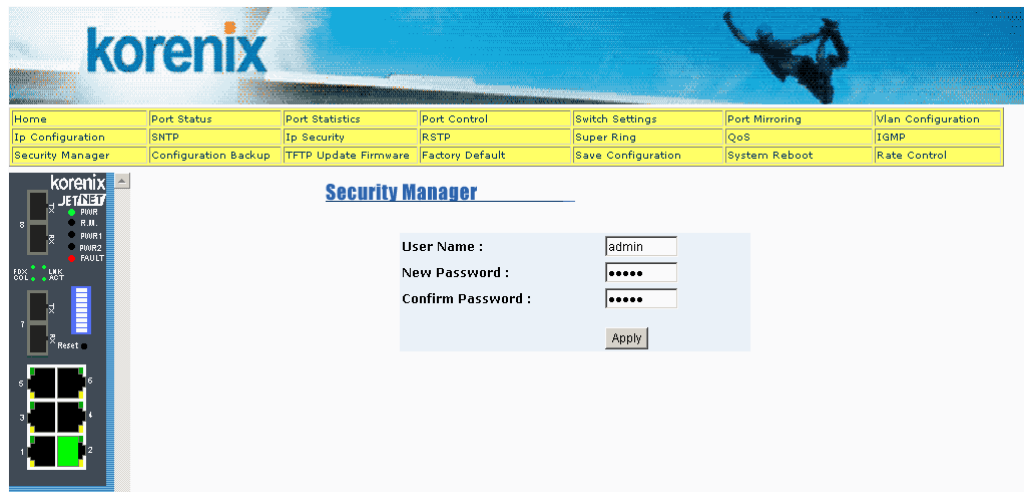
In effect, IGMP manages multicast traffic by making use of switches, routers, and hosts that support IGMP. Enabling IGMP allows the ports to detect IGMP queries, report packets, and manage multicast traffic through the switch. IGMP has three fundamental types of messages, as shown below:

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.

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

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

Security Manager



You can change the user name and the password here for increased security

User name: You can key in the new user name here. The default setting is **root**.

Password: You can key in the new password here. The default setting is **root**.

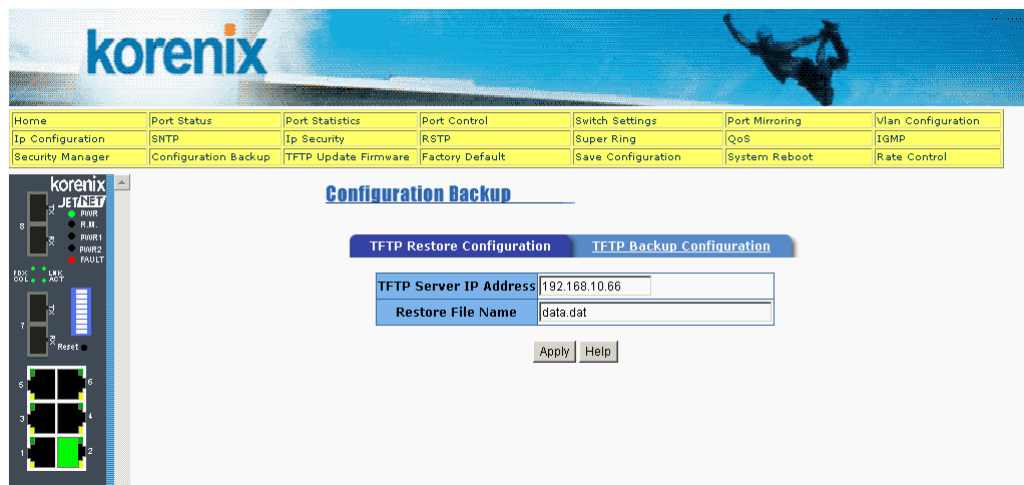
Confirm Password: You need to type the new password again to confirm it.

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

Configuration Backup

In Configuration Backup section, you can restore the backup configuration into the JetNet. You also can backup the configuration to the TFTP server as well.

TFTP Restore Configuration



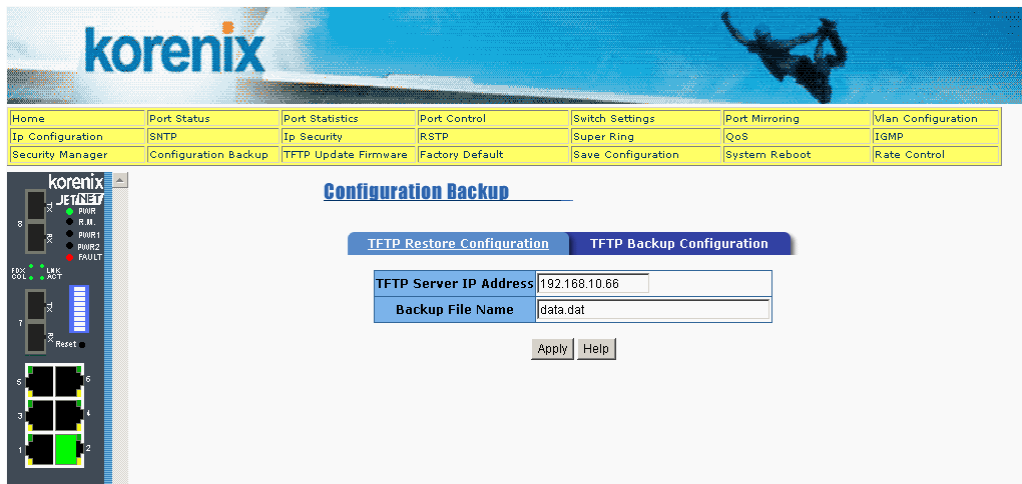
You can restore EEPROM values from the TFTP server. Before you can do that, you must place the backup image in the TFTP server, and then the JetNet will download the image back to the flash.

TFTP Server IP Address: You need to key in the IP address of your TFTP Server here.

Restore File Name: You need to specify the correct restore file name here.

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

TFTP Backup Configuration



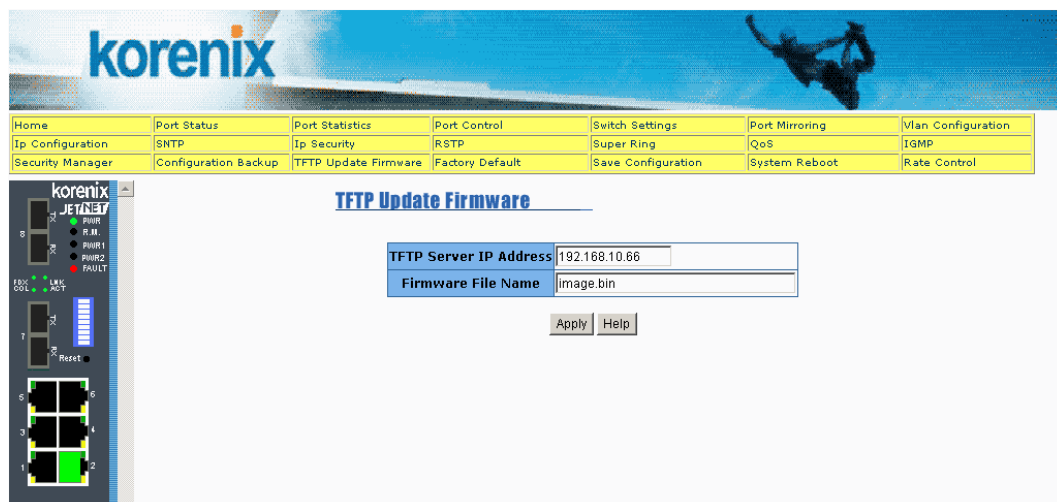
You can save the current flash ROM value from the JetNet to the TFTP server. This will allow you to later go to the **TFTP Restore Configuration** page to restore the image value back to the JetNet.

TFTP Server IP Address: You need to key in the IP address of your TFTP Server here.

Backup File Name: You need to specify the correct backup file name here.

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

TFTP Update Firmware



In this section, you can update the latest firmware for your JetNet 4000 Industrial Ethernet Switches. Before you do so, make sure that you have your TFTP server ready, and the firmware image is already installed on the TFTP server.

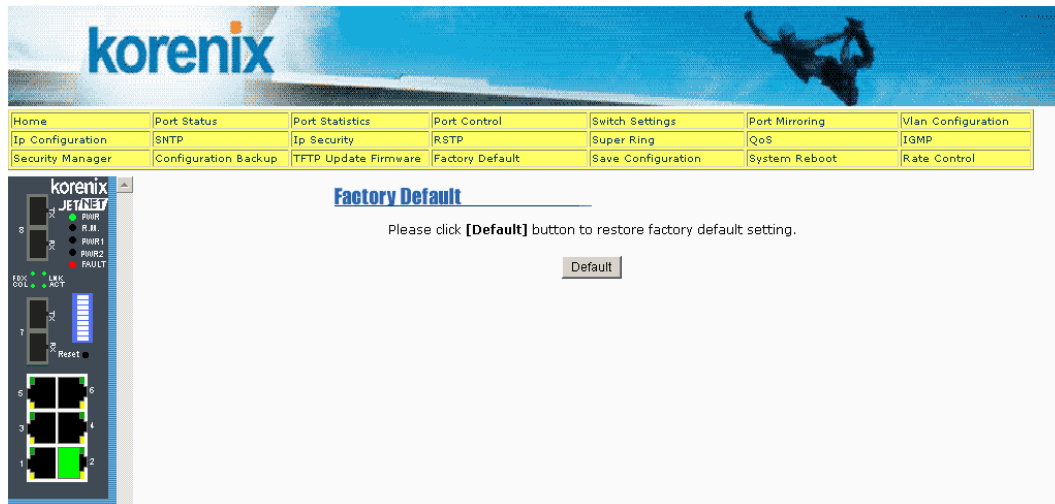
TFTP Server IP Address: Type in the IP address of your TFTP server here.

Firmware File Name: Type in the file name of the firmware image.

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

Note: Remember to click on the **Save Configuration** button to save your settings. Otherwise, the settings you made will be lost when the JetNet is powered off.

Factory Default



In this section, you can reset the JetNets to the default settings as shown below:

Default IP address: 192.168.10.1

Default Gateway: 192.168.10.254

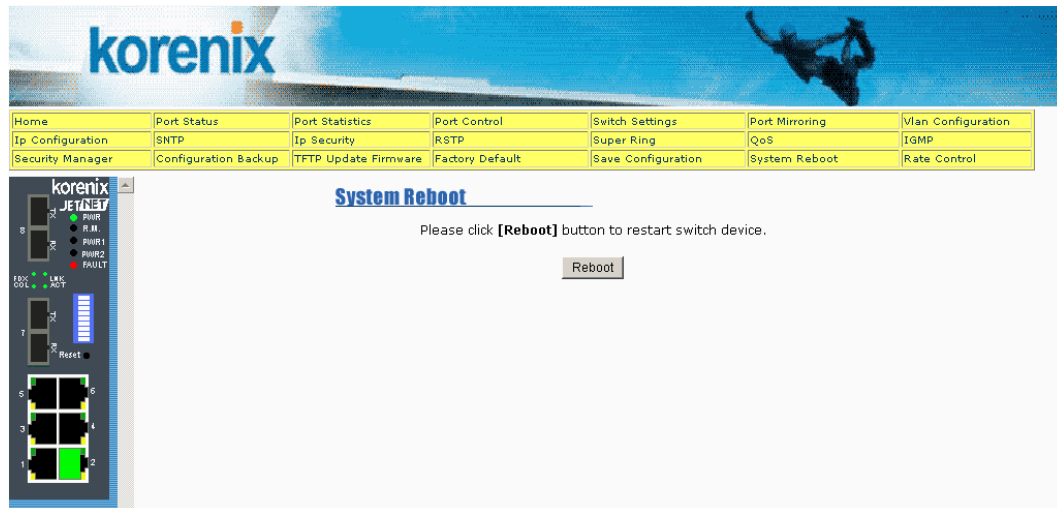
Subnet Mask: 255.255.255.0

Other switch settings will be set to disable or none.

Click on **Default** to reset your JetNets to the default settings.

Note: This provides a quick method for clearing the JetNet's internal settings. However, it will not restore the IP address to the default settings. If you want to restore all the settings to their default state, including the IP address, please use the reset button on the front panel of your JetNet (refer to the Reset Button section).

System Reboot



System Reboot allows you to reset JetNets' software. Click on **Reboot** to reboot your JetNets.

Note: Remember to click on the **Save Configuration** button to save your settings. Otherwise, the settings you made will be gone when the JetNet is powered off.

Save Configuration



Save Configuration allows you to save any configuration you just made to the flash memory. Powering off the JetNets without clicking on Save Configuration will cause the new settings to be lost. After selecting Save Configuration, click on **Save Flash** to save your new configuration.

Rate Control

The screenshot shows the Korenix JetNet web management interface. The main content area is titled "Rate Control" and contains a table for configuring rate limits for ports 01 through 08. The table has four columns: "Limit Packet Type", "Ingress", and "Egress for All". Each row represents a port, and the "Limit Packet Type" column has a dropdown menu set to "Broadcast only". The "Ingress" column has a dropdown menu set to "8Mbps", and the "Egress for All" column has a dropdown menu set to "Disable". Below the table are "Apply" and "Help" buttons.

	Limit Packet Type	Ingress	Egress for All
Port.01	Broadcast only	8Mbps	Disable
Port.02	Broadcast only	8Mbps	Disable
Port.03	Broadcast only	8Mbps	Disable
Port.04	Broadcast only	8Mbps	Disable
Port.05	Broadcast only	8Mbps	Disable
Port.06	Broadcast only	8Mbps	Disable
Port.07	Broadcast only	8Mbps	Disable
Port.08	Broadcast only	8Mbps	Disable

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

Limit packet type: You can select the packet type that you want it to be filtered. The packet types listed here include broadcast/multicast/unknown Unicast packet, broadcast/multicast packet, and broadcast packet only. The broadcast/multicast/unknown Unicast packet, broadcast/multicast packet, and broadcast packets are only for ingress packets (incoming packets). The egress (outgoing) rate only supports ALL packet types.

Bandwidth: Port 1 to Port 8 support port ingress (incoming traffic) and egress (outgoing traffic) rate control. For example, let's assume port 1 is 10 Mbps, you can set its effective egress rate to be 1 Mbps, and ingress rate to be 500 Kbps. The JetNet uses the packet counter to control the number of packets coming in so that the configured ingress rate can be achieved.

Ingress: Select the port effective ingress rate. The valid values are 128K, 256K, 512K, 1MB, 2MB, 4MB and 8MB bps. The default value is "**Broadcast Only**" and "**8Mbps**".

Egress for All: Select the port effective egress rate. The valid values are 128kbps, 256Kbps, 512Kbps, 1MB, 2MB, 4MB, and 8MB. The default value is "disable".

Click on **Apply** to apply the configuration.

Note: Remember to click on the **Save Configuration** button to save your settings. Otherwise, the settings you made will be lost when the JetNet is powered off.

4

Troubleshooting

This chapter includes the information on general troubleshooting.

The following topics are covered in this chapter:

- **Power Connections**
- **Incorrect Connections**
 - Faulty or Loose Cables
 - Non-standard Cables
 - Improper Network Design
- **LED Indicators**

Power Connections

JetNet is powered from 12-48V DC. You should verify that the output of your DC supply voltage, or AC-DC power adapter, remains within the required 12 to 48V DC range while under load.

IMPORTANT: Never exceed 48V DC or you will damage the switch.

If you are using an AC-DC power adapter and the DC-IN power indicator (PWR) of the JetNet does not light when the power cord is plugged in, you may have a faulty power cord. Check for loose or broken power connections. Also check for power loss or power surges at the AC power outlet. Verify that your AC-DC adapter is properly sized and outputs the correct voltage under load.

Incorrect Connections

Select Ethernet cables with specifications suitable for your application. In general, Ethernet cables are categorized into unshielded twisted-pair (UTP) and shielded twisted-pair (STP) types. Shielded cables are recommended. In general, Category 3, 4, and 5 Ethernet cables are suitable for systems with 10Mbps transmission speed. But for systems at 100Mbps, you should only use Category 5 or better Ethernet cables. Gigabit ports should use Cat-5 or Cat-5e cables for 1000Mbps connections. In addition, always make sure that the cable length between device ports does not exceed 100 meters (328 feet).

The RJ45 ports of this switch automatically detect straight-through or crossover cables and then cross-connect the transmit and receive channels when you connect the switch to another device. This feature does not apply to the fiber port connections. You must manually cross-connect transmit and receive cables between the fiber ports of connected devices. For fiber connections, make sure that the fiber cable type matches the fiber model (multi-mode or single-mode).

For the RJ-45 connectors, use the correct UTP or STP cables as required. For 10/100M ports, use 2 pairs of twisted cables. For Gigabit 1000T ports, use 4 pairs of twisted cables. If the RJ-45 connectors and cables are not correctly connected, the link will fail and the green LNK LED will not light.

Faulty or Loosen Cables

Visually inspect for loose or obviously faulty connections at all connectors and cables. If that does not correct the problem, try replacing the cable.

Non-standard Cables

Non-standard and incorrectly-wired cables may generate increased network collisions and other network problems which will impair network performance. A category 5 cable tester is a recommended tool for every 100Base-T network installation.

Improper Network Design

Verify that your network has been properly designed. Most errors simply result from poor quality cable, poor cable routing, network congestion, improper cable length, and too many repeater/hubs between end nodes. Errors may also result from inadvertent data path loops (redundant message paths). Message loops can generate broadcast storms that can bog down a network. There should be only one active message path between any two nodes on a network.

Excessive collisions may be indicative of a cable that is too long. It may also signal the presence of too many repeaters (hubs) between devices and can also be indicative of a congested network (too many nodes in one segment).

A high number of undersized and fragmented packets can result from interference induced into the network cable, by either passing it too close to noisy devices, or because of problems with the network devices themselves. In these instances, check for improper cabling, damaged cables, or cables routed too closely to noisy equipment or other wiring.

A high number of oversized packets can result from a bad transceiver, excessive cable noise, or

from a speed mismatch between the switch ports and the connected devices.

LED Indicators

JetNets can also be visually monitored via its own front-panel LED indicators. This can be useful to assist in identifying common problems and to help you find possible solutions.

Check the redundant PWR1 and PWR2 LED's to verify DC power. The PWR LED will light for any connected power (PWR1, PWR2, or DC-IN).

Check PWR for power via an AC adapter connected to DC-IN. If the power LED indicator does not light when the power cord is plugged in, you might have a problem with the power outlet, or the power cord. If the switch simply powers OFF on its own after running for a period of time, check for loose power connections, power losses, or surges at the power outlet. You should also verify that your supply voltage remains within the required 12-48VDC range while under load.

Refer to the port Link LED (LNK) to verify that a connection has been properly established (solid green). A blinking green LNK LED indicates communication activity. If the LNK LED remains off after making a connection, then no device has been detected and the cable may be bad or the connected device may be un-powered.

Refer to the Collision LED (COL) to monitor for excessive collisions. A blinking COL LED indicates that collisions have occurred. This LED will be solid ON for a full duplex connection, as collisions cannot occur for full-duplex. A full-duplex connection can be achieved by simply connecting one device per switch port, and this is the most deterministic mode of operation.

A

Specifications

Standards	IEEE 802.3 10BaseT Ethernet IEEE 802.3u 100BaseT(X) Fast Ethernet IEEE 802.3x Flow Control and back pressure IEEE 802.1p class of service IEEE 802.1Q VLAN
Protocols	CSMA/CD
Technology	Non-blocking, store-and-forward switching architecture
Transmission Rate	14,880 pps for Ethernet port 148,800 pps for Fast Ethernet port
Transfer Packet Size	64 bytes to 1522 bytes (with VLAN tag)
MAC Address Table Size	2K MAC address table
Memory Buffer	1024K bits
LEDs	<ul style="list-style-type: none">■ Per port: Link/Activity (Green) Full duplex/Collision (Orange)■ Per unit: Power 1, Power 2 , Power(Green) Fault(Red), RM(Ring Master, Green)
Network Cables	10BaseT: twisted-pair UTP/STP Cat. 3, 4, 5 cable EIA/TIA-568 100-ohm (100m) 100BaseT(X): twisted-pair UTP/STP Cat.5 cable EIA/TIA-568 100-ohm (100m)
Power Input	12 to 48 VDC, redundant dual DC power inputs with reverse polarity protection, and a removable terminal block for master and slave VDC power inputs.
Power Consumption	6 watts
Back-plane	1.6Gbps
Relay alarm current/voltage	Up to 1A and 24V DC
Operating Temperature	-10°C to 70°C (14°F to 158°F)
Operating Humidity	5 to 95% Relative Humidity, non-condensing
Storage Temperature	-40°C to 85°C
Dimensions	54 mm (W) x 135 mm (H) x 105 mm (D)
EMI	FCC Class A
EMS	CE EN6100-4-2, CE EN6100-4-3, CE EN6100-4-4, CE EN6100-4-5,

	CE EN6100-4-6
Safety	UL, cUL, CE/EN60950, IP-30
Stability	IEC60068-2-32 (free fall test), IEC60068-2-27 (shock test), IEC60068-2-6 (vibration test)

Note: As to the latest product spec, please refer to Korenix Web site. <http://www.korenix.com/>

B

Revision History

Edition	Date	Modifications
2 nd	Jun. 2005	Page 2-6 Changed the width of single mode fiber cables to 9/125 or 10/125 um.
3 rd	Sep. 2005	Added more detailed instructions for setting up VLANs.
4 th	Oct. 2005	Changed the figure in Super Ring section.
5 th	Mar. 2007	Modify: The Switch Setting web page is changed. Modify: Max available security IP is 10. Modify: Super Ring configuration method and change the figures of the Super Ring web pages. Modify: Modify the QoS configuration method and change the figures of the web page. Modify the Rate Control values and change the figures of the web page.
V1.6	Jun. 2007	Modify: Correct the font in RSTP section, the □ should be ≥. Modify: The switch number of the Super Ring figures is changed. Change the version to V1.6