

Korenix
JetNet 3018G/4518/5012G/5018G/5018G 2.0
Industrial Managed Ethernet Switch

User Manual

Manual v1.4

Firmware v1.3

July, 2012



www.korenix.com

Korenix

JetNet 3018G/4518/5012G/5018G/5018G 2.0

Industrial Managed Ethernet Switch

User Manual

Copyright Notice

Copyright © 2006-2012 Korenix Technology Co., Ltd.

All rights reserved.

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

Federal Communications Commission (FCC) Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his expense.

The user is cautioned that changes and modifications made to the equipment without approval of the manufacturer could void the user's authority to operate this equipment.

Index

1	Introduction	1
1.1	Overview	1
1.2	Major Features	3
1.3	Package List	3
2	Hardware Installation	4
2.1	Hardware Introduction	4
2.2	Wiring Power Inputs	7
2.3	Wiring Digital Output	7
2.4	Wiring Earth Ground	7
2.5	Wiring Fast Ethernet Ports	8
2.6	Wiring Fiber Ports	8
2.7	Wiring Combo Ports	9
2.8	Wiring RS-232 Console Cable	9
2.9	DIN-Rail Mounting Installation	10
2.10	Wall Mounting Installation	11
2.11	Safety Warning	12
3	Preparation for Management	14
3.1	Preparation for Serial Console	14
3.2	Preparation for Web Interface	15
3.3	Preparation for Telnet Console	17
4	Feature Configuration	20
4.1	Command Line Interface Introduction	21
4.2	Basic Setting	26
4.3	Port Configuration	45
4.4	Network Redundancy	54
4.5	VLAN	71
4.6	Private VLAN	81
4.7	Traffic Prioritization	88
4.8	Multicast Filtering	93
4.9	SNMP	99
4.10	Security	103
4.11	Warning	116
4.12	Monitor and Diag	125
4.12	Device Front Panel	133
4.13	Save to Flash	134
4.14	Logout	135
5	Appendix	136
5.1	Korenix SFP family	136
5.2	Korenix Private MIB	138
5.3	ModBus TCP /IP	139
5.4	Revision History	150
5.5	About Korenix	151

1 Introduction

Welcome to Korenix *JetNet 3018G/4518/5012G/5018G/5018G v2.0 Series* Industrial Managed Ethernet Switch User Manual. Following models are applied to this document.

JetNet 3018G Industrial 16+2G Gigabit Ethernet Switch

JetNet 4518 Industrial 18-port Managed Fast Ethernet Switch

JetNet 5012G Industrial 8+4G Gigabit Managed Ethernet Switch

JetNet 5018G Industrial 16+2G Gigabit Managed Ethernet Switch

JetNet 5018G 2.0 Industrial 16+2G Gigabit Managed Ethernet Switch

Following topics are covered in this chapter:

1.1 Overview

1.2 Major Features

1.3 Package Checklist

1.1 Overview

The JetNet **3018G/4518/5012G/5018G/5018G v2.0**, the Korenix Industrial Ethernet Switches, are specially designed for industrial environments requesting support of high access ports or multiple Gigabit ports. With fewer unit installation capability, the access ports share wider on-chip backplane, faster local transmission latency, efficient upstream transmission. The summary of the model list are as below. The JetNet 3018G is gigabit plug-and-play Ethernet switch. The JetNet 4518/5012G/5018G/5018G v2.0 is managed switch which supports abundant software features and can be managed through a single management agent. You can refer to the chapter 3 and 4 for software management.

Model Name	10/100 Base-TX	10/100/1000 Base-T	100Base-FX SFP	1000 Base-X SFP	Note
JetNet 3018G	16	2 (Combo with SFP)	-	2	Unmanaged switch. Check chapter 1, 2 and 5.
JetNet 4518	18		2 (Combo Port 17,18)		Managed Switch. Check chapter 1, 2, 3, 4 and 5. All the models use different firmware file.
JetNet 5012G	8	2 (Combo with SFP)		4	
JetNet 5018G	16	2 (Combo with SFP)		2	
JetNet 5018G 2.0	16	2 (Combo with SFP)	2 (100M+1000M SFP)		

The **JetNet 3018G** equips with 16 ports 10/100TX Fast Ethernet ports and 2 ports 1000Base-T/Gigabit SFP combo ports. The SFP ports accept all type of Gigabit SFP transceivers, such as Gigabit SX, LX, LHX, ZX and XD for several connections and distances.

The on board gigabit port of the JetNet 3018G always acts as uplink port or server port, they are much important than other ports. The JetNet 3018G provides 2 Digital Output to indicate the alarm when gigabit port link failure. Additionally, the JetNet 3018G supports Jumbo frame, up to 9,216 bytes packet size for large size file transmission, pre-configured QoS policy to forward prioritized packets without any problem.

The **JetNet 4518** is equipped with 16 10/100Base-TX Fast Ethernet ports and 2 10/100Base-TX/ 100Base-FX SFP combo ports. The SFP ports accept all types of 100M SFP transceivers. The switch is high access ports switch, the 2 SFP ports help form 100M Fiber Ring, this is especially apply to the low data bandwidth request applications.

The **JetNet5012G**, the 8+4G Industrial Managed Ethernet Switch, is equipped with 8 10/100TX Fast Ethernet ports, 2 Gigabit SFP and 2 Gigabit RJ-45/SFP combo ports. The SFP ports accept all types of Gigabit SFP transceivers, including Gigabit SX, LX, LHX, ZX and XD for several connections and distances. The copper interface of the 2 Gigabit combo ports supports 10M,100M or 1000M speed. The switch can work as 8+4G, 7+3G or 10+2G switch. Besides, the speed is auto-negotiated or software configured and all the port types have non-blocking and wire-speed switching capability. The 8+4G design allows aggregating up to 4 100M rings plus 2 Gigabit rings, which is a unique and Korenix patent protected ring technology.

The **JetNet 5018G** is equipped with 16 10/100TX Fast Ethernet ports and 2 10/100/1000Base-T/Gigabit SFP combo ports. The SFP ports accept all types of Gigabit SFP transceivers, including Gigabit SX, LX, LHX, ZX and XD for several connections and distances. The **JetNet 5018G 2.0** is the enhanced version of the JetNet 5018G, the SFP port of the JetNet 5018G v2.0 can support both 100M and Gigabit SFP. The software can identify the speed of the inserted SFP transceiver.

The embedded software of **JetNet 4518/5012G/5018G/5018G 2.0** supports RSTP and Multiple Super Ring technology for ring redundancy protection. Besides, JetNet 4518/5012G/5018G/5018G v2.0 supports full layer 2 management features, such as the VLAN, IGMP Snooping, LACP for network control, SNMP, LLDP for network management. The secured access is protected by Port Security, 802.1x and flexible Layer 2/4 Access Control List. The switch can work with JetView Pro, the Korenix patented Industrial Innovation Network Management system which can draw the network topology, automatically update ring and port status, remotely manage the switch or monitor its status through LLDP and SNMP protocols. With JetNet 4518/5012G/5018G/5018G 2.0, you can fulfill the technicians' needs of having the best solution for the industrial Ethernet infrastructure.

1.2 Major Features

The following are the common major features:

- Auto Gigabit SFP transceiver detection (JetNet 5012G/5018G/5018G v2.0.0)
- Auto 100M SFP transceiver detection (JetNet 4518/5018G v2.0.0)
- Non-Blocking Switching Performance, high backplane single chip solution
- Jumbo Frame up to 9,216 byte
- Dual 24V (12-48V) DC power inputs
- 2 Relay Outputs indicate Gigabit port Link Failure (JetNet 3018G) or configured other failures by software (JetNet 4518/5012G/5018G/5018G v2.0.0)
- IEEE 802.1p Quality of Service (QoS) compliant (JetNet 3018G, the Tag Priority ID is as following: Higher (6,7), High (4,5), Low (0,3), Lowest (1,2))
- Rigid Aluminum Case complies with IP31
- -25~70°C operating temperature(3018G/5012G/5018G), -40~70°C operating temperature(5012G-w/5018G-w); -40~75°C operating temperature (JetNet 4518)

Software Features applied to JetNet 4518/5012G/5018G/5018G v2.0.0:

- Korenix Multiple Super Ring pattern aggregates multiple rings within one unit
- IEEE 1588 Precision Time Protocol for precise time synchronization
- RSTP/STP, 256 802.1Q VLANs, QoS and up to 6/8 trunk groups
- IGMP Snooping, GMRP Rate Control for multicast message management
- LLDP for network topology live update
- SNMP V1/V2c/V3, RMON for remote management
- Works with JetView Pro Network Management software
- Modbus TCP/IP client for Factory Automation (**new feature in firmware v1.3**)
- Multiple language for Web user interface (**new feature in firmware v1.3**)
- Advanced Security supports IP/Port Security, 802.1x and Access Control List

Note: The detail spec is listed in latest datasheet. Please download the latest datasheet in Korenix Web site.

1.3 Package List

The JetNet 3018G/4518/5012G/5018G/5018G v2.0.0 products are shipped with following items, if there is any item is missing or damaged, please contact your local sales representative.

JetNet 3018G/4518/5012G/5018G/5018G v2.0.0 without transceiver

Rack Mount Kit, screwed on the rear panel

Console Cable (Apply to JetNet 4518/5012G/5018G/5018G v2.0)

Quick Installation Guide

CD User Manual

2 Hardware Installation

This chapter includes hardware introduction, installation and configuration information.

Following topics are covered in this chapter:

2.1 Hardware Introduction

Dimension

Panel Layout

Bottom View

2.2 Wiring Power Inputs

2.3 Wiring Digital Input

2.4 Wiring Relay Output

2.5 Wiring Ethernet Ports

2.6 Wiring Combo Ports

2.7 Wiring RS-232 console cable

2.8 DIN-Rail Mounting Installation

2.9 Wall-Mounting Installation

2.10 Safety Warning

2.1 Hardware Introduction

LED

Diagnostic LED:

System: Power 1, Power 2, Ring Master (Green), Relay 1, Relay 2, Ring Failure (Red)

10/100/1000Base-T RJ-45: Link/Activity (Green/Green Blinking), Full Duplex/Collision (Yellow/Yellow Blinking)

100M/Gigabit SFP: Link/Activity (Green/Green Blinking)

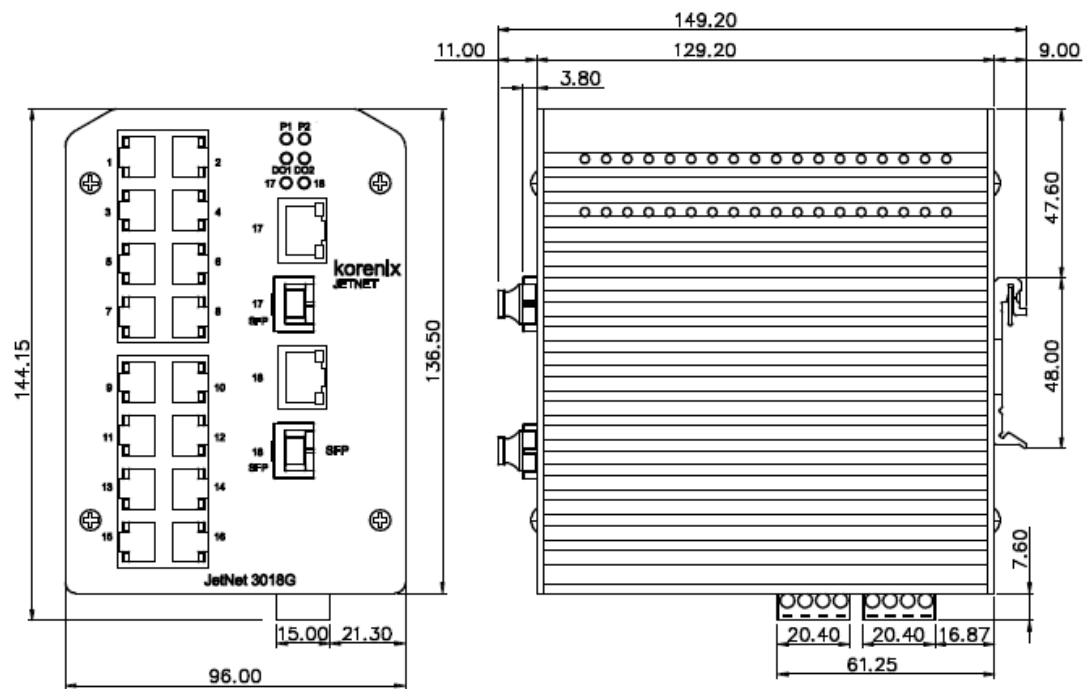
(JetNet 3018G/5012G/5018G supports Gigabit SFP only. JetNet 4518-w supports 100M SFP only. JetNet 5018G v2.0 supports both 100M and Gigabit SFP)

JetNet 3018G does not support R.M. and R.F. LED. The RO 1 indicates gigabit port 17 link down/failure, the RO 2 indicates gigabit port 18 link down/failure.

Dimension

JetNet 3018G/4518/5012G/5018G series Industrial Managed Ethernet Switch share the same mechanical. The dimension (W x H x D) is **137mm(H) x 96mm (W) x 129mm (D)**

Figure of the JetNet 3018G



Bottom view of the JetNet 3018G

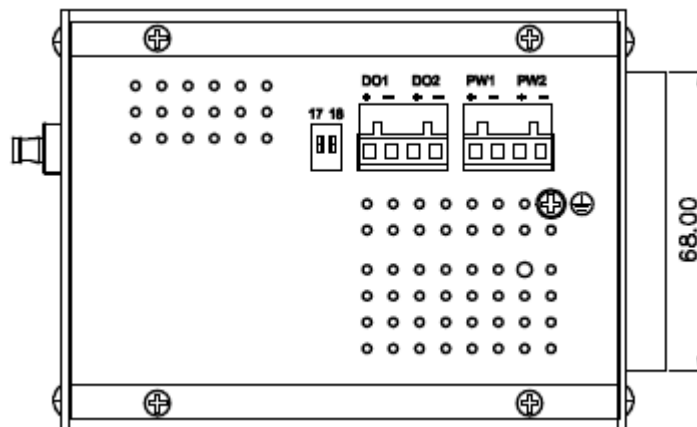


Figure of the JetNet 4518/5018G/5018G v2.0

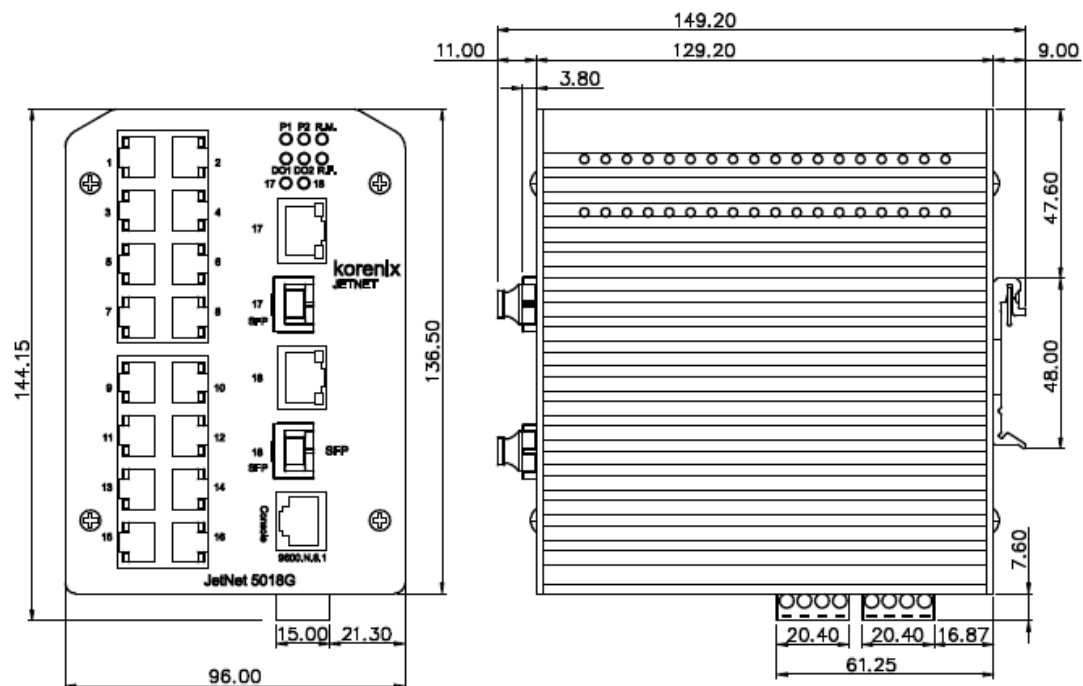
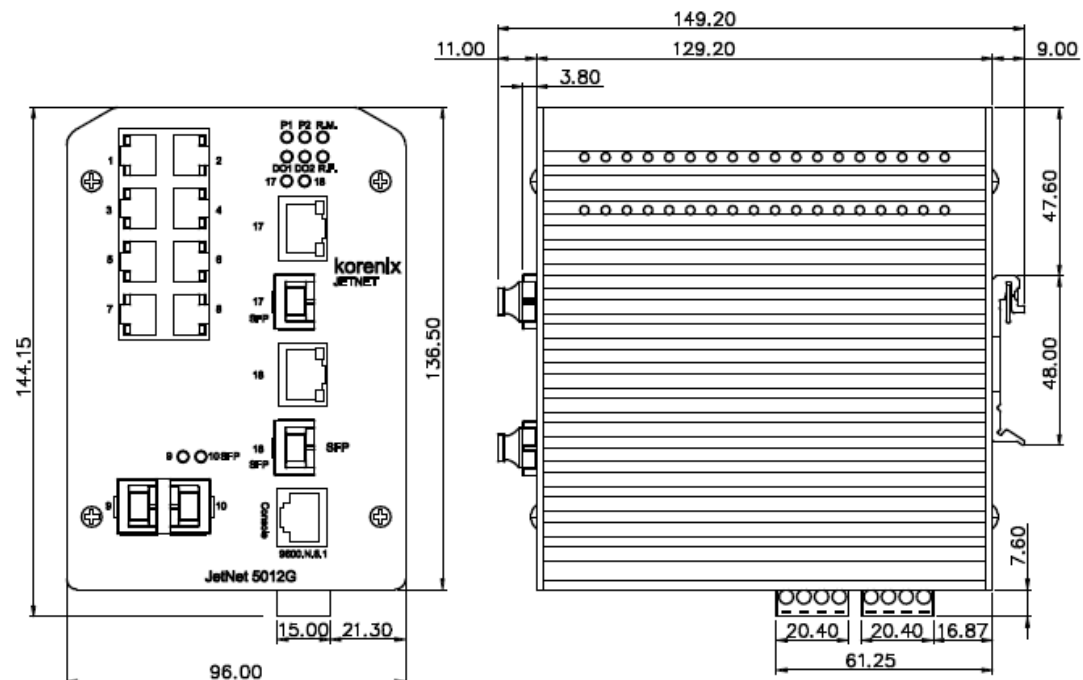


Figure of the JetNet 5012G



The Bottom dimension is the same as the JetNet 3018G.

Besides the DIP switch on JetNet 3018G, the other placement of JetNet 4518, 5018G and 5012G is the same as JetNet 3018G.

2.2 Wiring Power Inputs

DC Power Input

Follow below steps to wire redundant DC 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 DC wires from being loosened.
3. Power 1 and Power 2 support power redundancy and polarity reverse protection functions.
4. Positive and negative power system inputs are both accepted, but Power 1 and Power 2 must apply the same mode.

Note 1: 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.

Note 2: The range of the suitable DC electric wire is from 12 to 24 AWG.

Note 3: If the 2 power inputs are connected, the switch will be powered from the highest connected voltage. The unit will alarm for loss of power, either PWR1 or PWR2.

2.3 Wiring Digital Output

JetNet 3018G/4518/5012G/5018G provide 2 digital outputs, also known as Relay Output.

JetNet 4518/5012G/5018G/5018G v2.0.0:

In JetNet 4518/5012G/5018G, 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 management UI.

JetNet 3018G:

In JetNet 3018G, the Digital Output indicates gigabit port 17 and 18 link down or failure.



Click the equipped DIP 1 to ON to enable the port 17 link failure DO alarm, click the DIP 2 to ON to enable the port 18 link failure DO alarm.

The default (without power) state of the Digital Output is normal **CLOSE** state.

Wiring digital output is exactly the same as wiring power input introduced in chapter 2.2.

2.4 Wiring Earth Ground

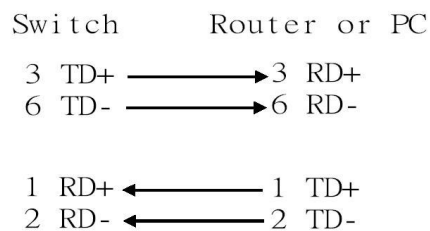
To ensure the system will not be damaged by noise or any electrical shock, we suggest you to make exact connection with switch with Earth Ground.

For DC input, loosen the earth ground screw by screw drive; then tighten the screw after earth ground wire is connected.

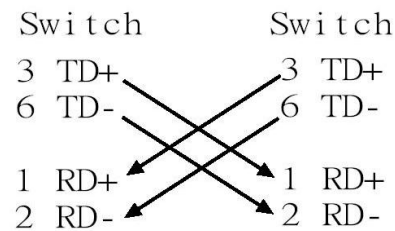
2.5 Wiring Fast Ethernet Ports

The fast Ethernet ports support 10Base-T and 100Base-TX, full or half duplex modes. All the fast Ethernet 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 cables.

Note that crossover cables simply cross-connect the transmit lines at each end to the received 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 RJ-45 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 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).

The wiring cable types are as below.

10Base-T: 2-pair UTP/STP Cat. 3, 4, 5 cable, EIA/TIA-568 100-ohm (100m)

100 Base-TX: 2-pair UTP/STP Cat. 5 cable, EIA/TIA-568 100-ohm (100m)

1000 Base-TX: 4-pair UTP/STP Cat. 5 cable, EIA/TIA-568 100-ohm (100m)

2.6 Wiring Fiber Ports

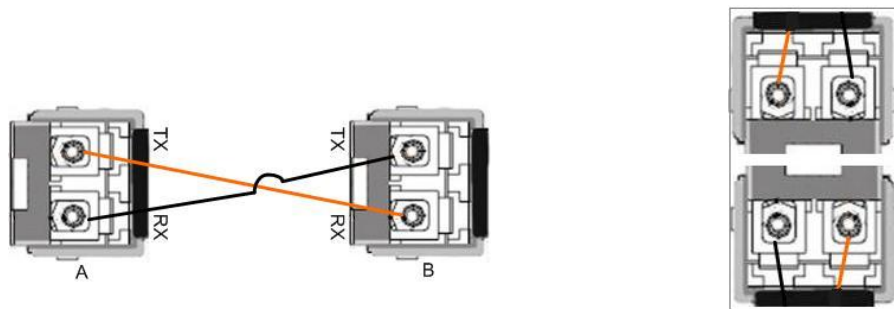
Small Form-factor Pluggable (SFP)

The SFP ports accept standard MINI GBIC SFP transceiver. But, to ensure system reliability, **Korenix recommends using the Korenix certificated SFP Transceiver**. The web UI will show Unknown vendor type when choosing the SFP which is not certificated by Korenix.

The JetNet 3018G/5012G/5018G support Gigabit SFP transceiver, JetNet 4518 supports 100M SFP transceiver, the JetNet 5018G v2.0 supports both 100M and 1000M SFP. The types of the SFP transceivers include single-/multi-mode fiber, the support range is from 550m to 120KM depends on the capability of the plugged transceiver.

Different type SFP transceiver can work together within the same device. Choose the types and distance you need. This is the flexibility of the SFP Fiber transceiver.

The way to connect the SFP transceiver is to Plug in SFP fiber transceiver first. Cross-connect the transmit channel at each end to the receive channel at the opposite end as illustrated in the figure below. The SPF cage of JetNet 5012G 2G SFP is 2x1 design, check the direction/angle of the fiber transceiver and fiber cable when inserted.



Note: This is a Class 1 Laser/LED product. Don't stare at the Laser/LED Beam.

2.7 Wiring Combo Ports

There is Combo Ports design in JetNet managed switch series. The combo port means the physical interface supports both copper and fiber types, but there is only one of the types, Copper or Fiber can be used in one time.

JetNet 3018G/5012G/5018G/5018G v2.0

The JetNet 3018G/5012G/5018G/5018G v2.0 include 2 Gigabit RJ-45/SFP Combo ports. The port number of the JetNet 3018G/5018G/5018G v2.0 is port 17 and 18. The port number of the JetNet 5012G is port 11 and 12.

The speed of the gigabit Ethernet copper port supports 10Base-TX, 100Base-TX and 1000Base-T. [The speed of the SFP Fiber port supports 1000M Full Duplex.](#) The available gigabit SFP supports Gigabit Single-mode, Multi-mode, BIDI/WDM single-mode SFP transceivers. [\(The 100Base-FX is not supported in JetNet 3018G/5012G/5018G Gigabit combo ports.\)](#)

The default value when both types are connected is the [active SFP port works first](#), only the Fiber link is available when SFP plugged and link up.

JetNet 4518

The JetNet 4518 includes 2 100M RJ-45/SFP combo ports. The speed of the Fast Ethernet port supports 10Base-TX, 100Base-TX. [The speed of the JetNet 4518/5018G v2.0 SFP port supports 100M Full Duplex.](#) [The JetNet 4518 only accept 100Mbps SFP Transceiver.](#)

The default value when both types are connected is the [plugged SFP port works first](#). After plugged SFP transceiver, even it is not connected and link up, only the Fiber link is available. This is the current design and this is not the same as JetNet3018G/ 5012G/ 5018G/ 5018G v2.0.

[When the SFP transceiver is plugged into SFP lot, the combo mode is changed to Fiber mode directly.](#) [Korenix suggest not connecting Copper and Fiber at the same time.](#)

2.8 Wiring RS-232 Console Cable

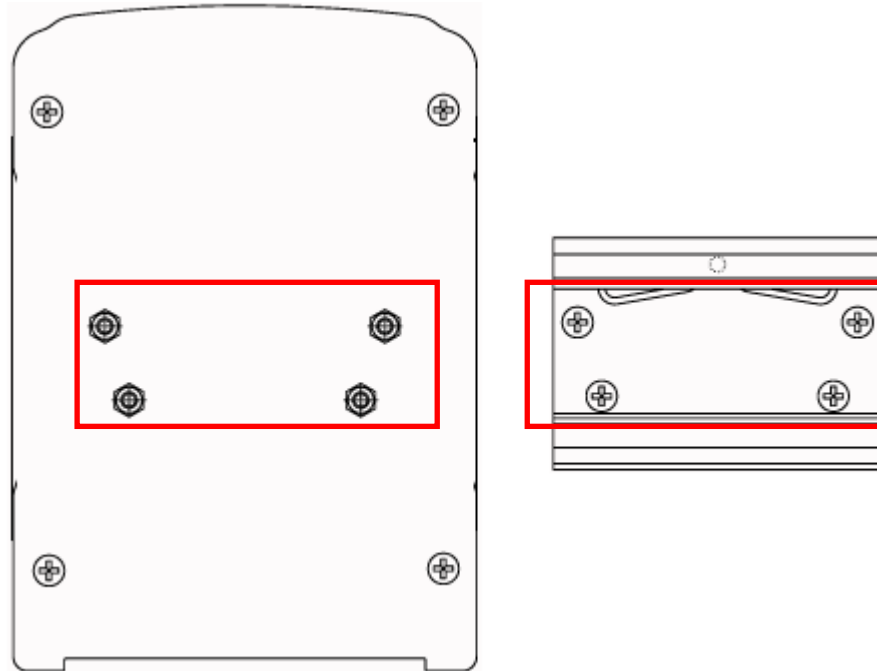
Korenix JetNet 4518/ 5012G/ 5018G/ 5018G v2.0 attached one RS-232 DB-9 to RJ-45 cable in the unit box. Connect the RJ-45 connector to the COM port of your PC, open Terminal tool and set up serial settings to 9600, N,8,1. (Baud Rate: 9600 / Parity: None / Data Bit: 8 / Stop Bit: 1) Then you can access 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 in the appendix.

2.9 DIN-Rail Mounting Installation

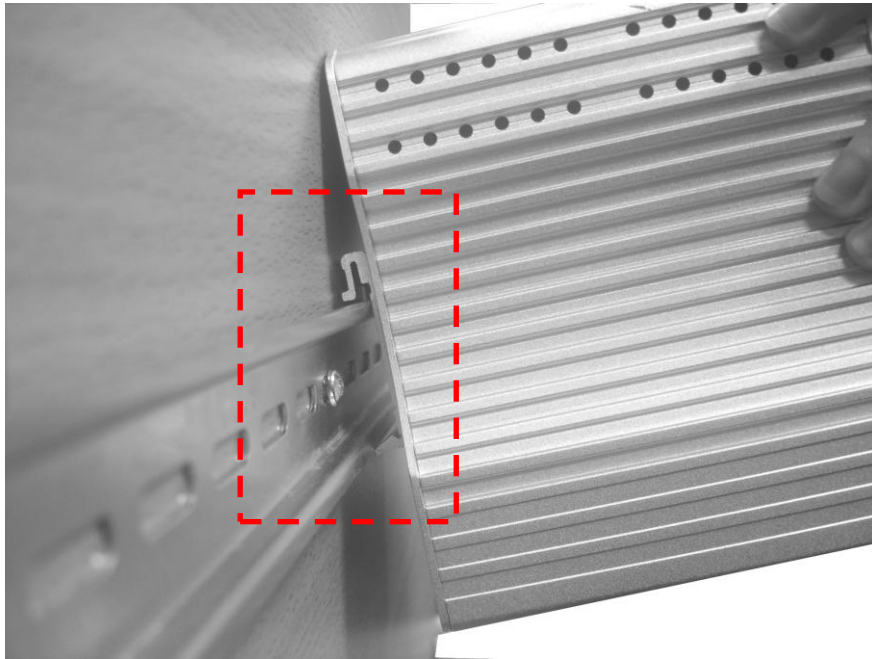
The DIN-Rail clip is already attached to the JetNet Switch when packaged. If the DIN-Rail clip is not screwed on the JetNet Switch, follow the instructions and the figure below to attach DIN-Rail clip to JetNet Switch.



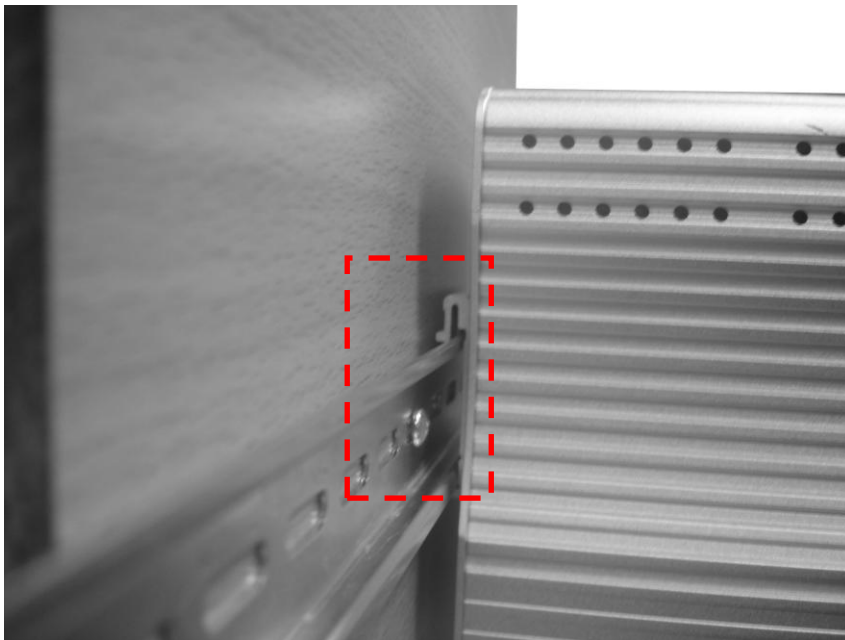
1. Use the screws to attach DIN-Rail clip to the rear panel of JetNet Din Rail Switch.
2. To remove DIN-Rail clip reverse step 1

Follow the steps below to mount JetNet Switch to the DIN-Rail track:

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



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 JetNet Switch from the track, reverse the steps above.

2.10 Wall Mounting Installation

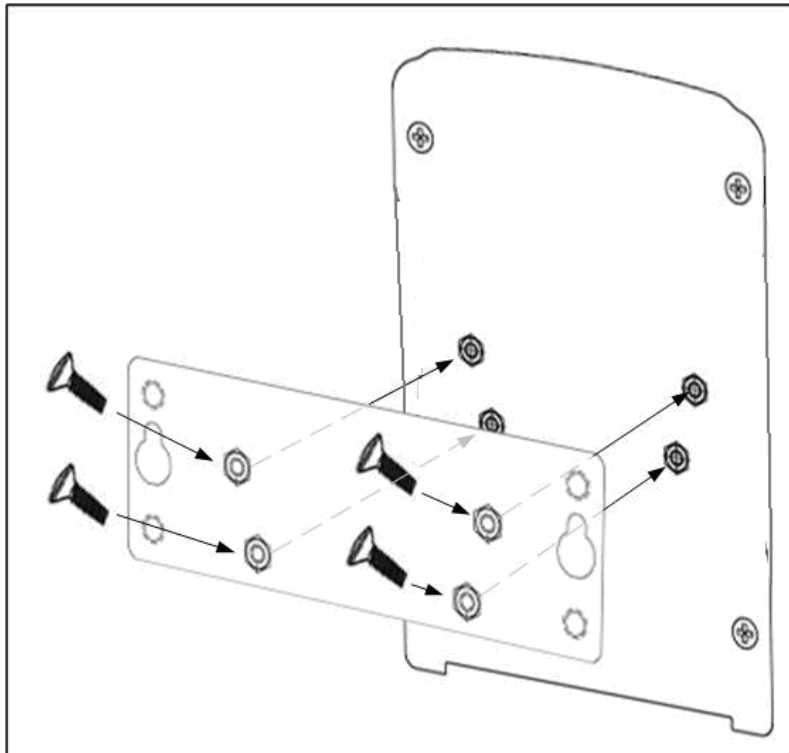
Follow the steps below to install JetNet Switch with the wall mounting plate.

1. To remove DIN-Rail clip from JetNet Switch, loosen the screws from DIN-Rail clip.

2. Place the wall mounting plate on the rear panel of JetNet Switch.
3. Use the screws to tighten the wall mounting plate onto JetNet Switch.
4. Use the hook holes at the corners of the wall mounting plate to hang JetNet Switch onto the wall.
5. To remove the wall mounting plate, reverse the steps above.



Wall-Mounting plate and screws.



2.11 Safety Warning

2.2.1 The Equipment intended for installation in a Restricted Access Location.



Restricted Access Location:

This equipment is intended to be installed in a RESTRICTED ACCESS LOCATION only.

2.2.2 The warning test is provided in user manual. Below is the information:

"For tilslutning af de ovrigte ledere, se medfølgende installationsvejledning".

“Laite on liitettava suojamaadoitus-koskettimilla varustettuun pistorasiaan”

„Apparatet må tilkoples jordet stikkontakt“

”Apparaten skall anslutas till jordat uttag”

3 Preparation for Management

JetNet Industrial Managed Switch provides both in-band and out-band configuration methods. You can configure the switch via RS232 console cable if you don't attach your admin PC to your network, or if you lose network connection to your JetNet managed switch. This is so-called out-band management. It wouldn't be affected by network performance.

The in-band management means you can remotely manage the switch via the network. You can choose Telnet or Web-based management. You just need to know the device's IP address and you can remotely connect to its embedded HTTP web pages or Telnet console.

Should you forget the IP address, you can use JetView Utility to discover the device, check its IP address or assign new IP address. The JetView Utility can discover the device across the subnet. Please download the newest version of JetView from Korenix's web site.

Following topics are covered in this chapter:

3.1 Preparation for Serial Console

3.2 Preparation for Web Interface

3.3 Preparation for Telnet console

3.1 Preparation for Serial Console

In JetNet Managed Switch package, Korenix attached one RS-232 DB-9 to DB-9/RJ-45 console cable. Please attach RS-232 DB-9 connector to your PC COM port, connect the other end to the Console port of the JetNet Managed Switch. If you lose the cable, please follow the console cable PIN assignment to find one. (Refer to the appendix).

1. Go to Start -> Program -> Accessories -> Communication -> Hyper Terminal
2. Give a name to the new console connection.
3. Choose the COM name
4. Select correct serial settings. The serial settings of JetNet Managed Switch are as below:

Baud Rate: 9600 / Parity: None / Data Bit: 8 / Stop Bit: 1

5. After connected, you can see Switch login request.
6. Login the switch. The default username is "admin", password, "admin".

```
Booting...
      Sun Jan  1 00:00:00 UTC 2006

Switch login: admin
Password:

JetNet5018G (version 0.2.25-20090414-11:04:13).
Copyright 2006-2009 Korenix Technology Co., Ltd.

Switch>
```

3.2 Preparation for Web Interface

JetNet Managed Switch provides HTTP Web Interface and Secured HTTPS Web Interface for web management.

3.2.1 Web Interface

Korenix web management page is developed by JAVA. It allows 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.

Before you attempt to use the embedded web interface to manage switch operation, verify that your JetNet Industrial Managed 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 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 or other IP address which is located in the 192.168.10.x (Network Mask: 255.255.255.0) subnet.
5. Switch to DOS command mode and ping 192.168.10.1 to verify a normal response time.

Launch the web browser and Login.

6. Launch the web browser (Internet Explorer or Mozilla Firefox) on the PC.
7. Type **http://192.168.10.1** (or the IP address of the switch). And then press **Enter**.
8. The login screen will appear next.
9. Key in user name and the password. Default user name and password are both **admin**.
10. Select Language type, this feature is available from **firmware v1.3**, and supports **English** and **Simplified Chinese** user interface.



Click on **Enter** or **OK**. Welcome page of the web-based management interface will then appear.



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

Note 1: 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.

Note 2: The Web UI connection session of JetNet Managed Switch will be logged out automatically if you don't give any input after 30 seconds. After logged out, you should re-login and key in correct user name and password again.

3.2.2 Secured Web Interface

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

Launch the web browser and Login.

1. Launch the web browser (Internet Explorer or Mozilla Firefox) on the PC.
2. Type **https://192.168.10.1** (or the IP address of the switch). And then press **Enter**.

3. The popup screen will appear and request you to trust the secured HTTPS connection distributed by JetNet Managed Switch first. Press **Yes** to trust it.



4. The login screen will appear next.



5. Key in the user name and the password. The default user name and password is **admin**.
6. Click on **Enter** or **OK**. Welcome page of the web-based management interface will then appear.
7. Once you enter the web-based management interface, all the commands you see are the same as what you see by HTTP login.

3.3 Preparation for Telnet Console

3.3.1 Telnet

Korenix JetNet managed Switch supports Telnet console. You can connect to the switch by Telnet and the command lines are the same as what you see by RS232 console port. Below are the steps to open Telnet connection to the switch.

1. Go to Start -> Run -> cmd. And then press **Enter**
2. Type the **Telnet 192.168.10.1** (or the IP address of the switch). And then press **Enter**

3.3.2 SSH (Secure Shell)

Korenix JetNet Managed Switch also support SSH console. You can remotely connect to the switch by command line interface. The SSH connection can secure all the configuration commands you sent to the switch.

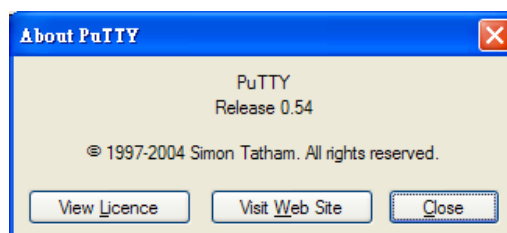
SSH is a client/server architecture while JetNet Managed Switch is the SSH server. When you want to make SSH connection with the switch, you should download the SSH client tool first.

SSH Client

There are many free, sharewares, trials or charged SSH clients you can find on the internet. For example, PuTTY is a free and popular Telnet/SSH client. We'll use this tool to demonstrate how to login JetNet by SSH. Note: *PuTTY is copyright 1997-2006 Simon Tatham.*

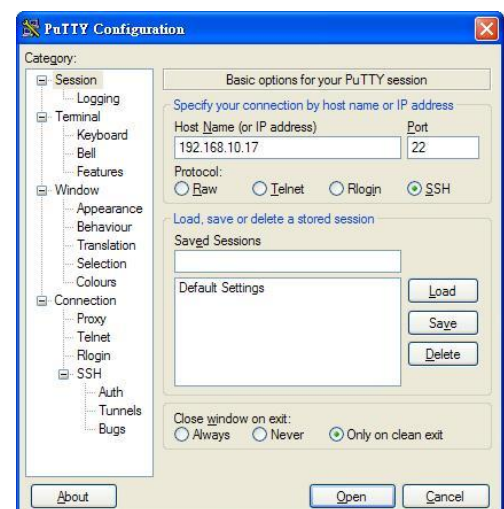
Download PuTTY: <http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>

The copyright of **PuTTY**

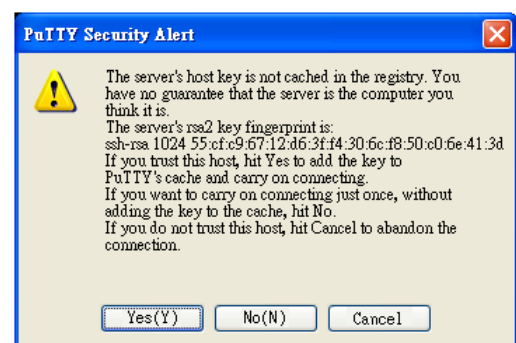


1. Open SSH Client/PuTTY


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



2. After click on **Open**, then you can see the cipher information in the popup screen. Press **Yes** to accept the Security Alert.



3. After few seconds, the SSH connection to JetNet Managed Switch is opened. You can see the login screen as the below figure.



```
192.168.10.17 - PuTTY
login as: admin
admin@192.168.10.17's password:

Jetnet5010G (version 1.0.4-20070129).
Copyright 2006-2010 Korenix Technology Co., Ltd.

JetNet 5010G>
```

4. Type the Login Name and its Password. The default Login Name and Password are **admin / admin**.
5. All the commands you see in SSH are the same as the CLI commands you see via RS232 console. The next chapter will introduce in detail how to use command line to configure the switch.

4 Feature Configuration

This chapter explains how to configure JetNet Managed Switch's software features. There are four ways to access the switch: Serial console, Telnet, Web browser and SNMP.

JetNet Industrial Managed Switch Series provides both in-band and out-band configuration methods. You can configure the switch via RS232 console cable if you don't attach your admin PC to your network, or if you lose the network connection to your JetNet Managed Switch. This is so-called out-band management. It wouldn't be affected by the network performance.

The in-band management means you can remotely manage the switch via the network. You can choose Telnet or Web-based management. You just need to know the device's IP address. Then you can remotely connect to its embedded HTML web pages or Telnet console.

Korenix web management page is developed by JAVA. It allows 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.

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.

Following topics are covered in this chapter:

- 4.1 Command Line Interface (CLI) Introduction
- 4.2 Basic Setting
- 4.3 Port Configuration
- 4.4 Network Redundancy
- 4.5 VLAN
- 4.6 Traffic Prioritization
- 4.7 Multicast Filtering
- 4.8 SNMP
- 4.9 Security
- 4.10 Warning
- 4.11 Monitor and Diag
- 4.12 Device Front Panel
- 4.13 Save
- 4.14 Logout

4.1 Command Line Interface Introduction

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

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

User EXEC mode: As long as you login the switch by CLI. You are in the User EXEC mode. You can ping, telnet remote device, and show some basic information.

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

JN5018G>

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

Privileged EXEC mode: Press enable in the User EXEC mode, then you can enter the Privileged EXEC mode. In this mode, the system allows you to view current configuration, reset default, reload switch, show system information, save configuration...and enter the global configuration mode.

Type **configure terminal** to enter next mode, **exit** to leave. **?** to see the command list

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

Global Configuration Mode: Press **configure terminal** in privileged EXEC mode. You can then enter global configuration mode. In global configuration mode, you can configure all the features that the system provides you.

Type **interface IFNAME/VLAN** to enter interface configuration mode, **exit** to leave. **?** to see the command list.

Available command lists of global configuration mode.

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
lacp	Link Aggregation Control Protocol
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-server	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

(Port) Interface Configuration: Press **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 of the fast Ethernet port is fa<Port Number>. Ex: Fast Ethernet Port 1 fa1, fast Ethernet port 7 is fa7, fast Ethernet port 17 is fa17.

The port interface name of the Gigabit Ethernet port is gi<Port Number>. Ex: Gigabit Port 8 is gi9, Gigabit Port 17 is gi17. Even you apply fixed 100M speed to the gigabit port, the port interface name is still gi<Port Number>.

Types interface name accordingly when you want to enter certain interface configuration mode.

Type **exit** to leave.

Type **?** to see the command list

Available command lists of the (port) Interface configuration mode.

```
Switch(config)# interface fa1
Switch(config-if)#
  acceptable      Configure 802.1Q acceptable frame types of a port.
  auto-negotiation Enable auto-negotiation state of a given port
  description      Interface specific description
  duplex          Specify 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      Set 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        Specify loopback mode of operation for a port
  mac             MAC interface commands
  mdix            Enable mdix state of a given port
  no              Negate a command or set its defaults
  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    spanning-tree protocol
  speed           Specify the speed of a Fast Ethernet port or a Gigabit
Ethernet port.
  switchport      Set switching mode characteristics
```

(VLAN) Interface Configuration: Press **interface VLAN VLAN-ID** in global configuration mode. You can then enter VLAN interface configuration mode. In this mode, you can configure the settings for the specific VLAN.

The VLAN interface name of VLAN 1 is VLAN 1, VLAN 2 is VLAN 2...

Type **exit** to leave the mode. Type **?** to see the available command list.

The command lists of the VLAN interface configuration mode.

```
Switch(config)# interface vlan 1
Switch(config-if)#
  description      Interface specific description
  end             End current mode and change to enable mode
  exit            Exit current mode and down to previous mode
  ip              Interface 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
```

Summary of the 5 command modes.

Command Mode	Main Function	Enter and Exit Method	Prompt
User EXEC	This is the first level of access. User can ping, telnet remote device, and show some basic information	Enter: Login successfully Exit: 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 default, reload switch, show system information, save 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 you	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)#

Here are some useful commands for you to see these available commands. Save your time in typing and avoid typing error.

? To see all the available commands in this mode. It helps you to see the next command you can/should type as well.

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

(Character)? To see all the available commands starts from this character.

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

Tab This tab key helps you to input the command quicker. If there is only one available command in the next, clicking on tab key can help to finish typing soon.

```
Switch# co (tab) (tab)
Switch# configure terminal

Switch(config)# ac (tab)
Switch(config)# access-list
```

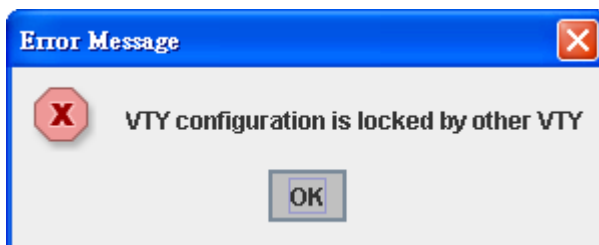
Ctrl+C To stop executing the unfinished command.

Ctrl+S To lock the screen of the terminal. You can't input any command.

Ctrl+Q To unlock the screen which is locked by Ctrl+S.

Ctrl+Z To exit configuration mode.

Alert message when multiple users want to configure the switch. If the administrator is in configuration mode, then the Web users can't change the settings. JetNet Managed Switch allows only one administrator to configure the switch at a time.



4.2 Basic Setting

The Basic Setting group provides you to configure switch information, IP address, User name/Password of the system. It also allows you to do firmware upgrade, backup and restore configuration, reload factory default, and reboot the system.

Following commands are included in this group:

4.2.1 Switch Setting

4.2.2 Admin Password

4.2.3 IP Configuration

4.2.4 Time Setting

4.2.5 Jumbo Frame

4.2.6 DHCP Server

4.2.7 Backup and Restore

4.2.8 Firmware Upgrade

4.2.9 Factory Default

4.2.10 System Reboot

4.2.11 CLI Commands for Basic Setting

4.2.1 Switch Setting

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

Figure 4.2.1.1 – Web UI of the Switch Setting

System Name	Switch
System Location	
System Contact	
System OID	1.3.6.1.4.1.24062.2.2.6
System Description	JetNet5628G Industrial Managed Switch
Firmware Version	v0.2.11 20090413
Device MAC	00:12:77:ff:04:12

Apply

System Name: You can assign a name to the device. The available characters you can input is 64. After you configure the name, CLI system will select the first 12 characters as the name in CLI system.

System Location: You can specify the switch's physical location here. The available characters you can input are 64.

System Contact: You can specify contact people here. You can type the name, mail address or other information of the administrator. The available characters you can input are 64.

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

System Description: JetNet (Model name) Industrial Managed Switch is the name of this product.

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

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

Once you finish the configuration, click on **Apply** 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.

4.2.2 Admin Password

You can change the user name and the password here to enhance security.

Figure 4.2.2.1 Web UI of the Admin Password



Admin Password	
Name	admin
Password	*****
Confirm Password	*****

Apply

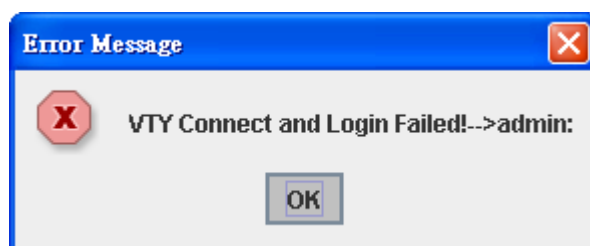
User name: You can key in new user name here. The default setting is **admin**.

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

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.

Figure 4.2.2.2 Popup alert window for Incorrect Username.



4.2.3 IP Configuration

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

IP Configuration

DHCP Client Disable ▼

IP Address	192.168.10.123
SubnetMask	255.255.255.0
Default Gateway	192.168.10.254

Apply

DHCP Client: You can select to **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 therefore be replaced by the one assigned by 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 JetNet. If DHCP Client function is enabled, you don't need to assign an IP address to the JetNet, as it will be overwritten by 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 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 bit of the subnet mask to represent the number displayed in 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.

Default Gateway: You can assign the gateway for the switch here. The default gateway is 192.168.10.254. **Note:** In CLI, we use 0.0.0.0/0 to represent for the default gateway.

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

4.2.4 Time Setting

Time Setting source allow user to set the time 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.

JetNet Managed Switch also provides Daylight Saving function.

System Time: The current time of the system. The time possibly synchronizes from PC, NTP Server, IEEE 1588 server or device startup duration.

Time Setting

System Time: Tue Jan 1 00:19:11 2008

Time Setting Source Manual Setting ▼

Manual Setting Get Time From PC

Jan ▼ 01 ▼ , 2008 ▼ 00 ▼ : 19 ▼ : 11 ▼

Manual Setting: User can select "**Manual setting**" to change time as user wants. User

also can click the button “**Get Time from PC**” to get PC’s time setting for switch. After click the “**Get Time from PC**” and apply the setting, the System time display the same time as your PC’s time.

NTP client: Select the Time Setting Source to NTP client can let device enable the NTP client service. NTP client will be automatically enabled if you change Time source to NTP Client. The system will send request packet to acquire current time from the NTP server you assigned.

Time Setting Source	NTP Client ▼
NTP Client	Manual Setting
Primary Server Address	NTP Client
	192.168.10.120
Secondary Server Address	192.168.10.121

IEEE 1588: With the **Precision Time Protocol IEEE 1588** there is now, for the first time, a standard available which makes it possible to synchronize the clocks of different end devices over a network at speeds faster than one microsecond.

To enable IEEE 1588, select Enable in PTP Status and choose Auto, Master or Slave Mode. After time synchronized, the system time will display the correct time of the PTP server.

IEEE 1588	
PTP State	Enable ▼
Mode	Auto ▼
	Auto
	Master
	Slave

Time-zone: Select the time zone where the switch is located. Following table lists the time zones for different locations for your reference. The default time zone is GMT Greenwich Mean Time.

```
Switch(config)# clock timezone
01 (GMT-12:00) Eniwetok, Kwajalein
02 (GMT-11:00) Midway Island, Samoa
03 (GMT-10:00) Hawaii
04 (GMT-09:00) Alaska
05 (GMT-08:00) Pacific Time (US & Canada) , Tijuana
06 (GMT-07:00) Arizona
07 (GMT-07:00) Mountain Time (US & Canada)
08 (GMT-06:00) Central America
09 (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) Auckland, Wellington
- 73 (GMT+12:00) Fiji, Kamchatka, Marshall Is.
- 74 (GMT+13:00) Nuku'alofa

Click the check box to enable the Daylight Saving Function as the setting of start and end week or disable it.

Daylight Saving Start and **Daylight Saving End**: the functions allows user to selects and apply the daylight saving start week and end week by monthly basis.

<input type="checkbox"/> Daylight Saving Time											
Daylight Saving Start	1st	▼	Sun	▼	in	Jan	▼	at	00	▼	: 00 ▼
Daylight Saving End	1st	▼	Sun	▼	in	Jan	▼	at	00	▼	: 00 ▼
Apply											

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

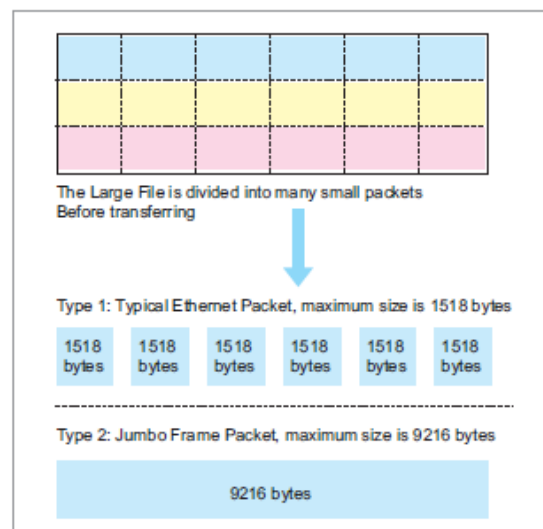
4.2.5 Jumbo Frame

What is Jumbo Frame?

The typical Ethernet frame is range from 64 to 1518 bytes. This is sufficient for general usages. However, when users want to transmit large files, the files may be divided into many small size packets. While the transmitting speed becomes slow, long size Jumbo frame can solve the issue.

The switch allows you configure the size of the MTU, Maximum Transmission Unit. The default value is 1,518bytes. The maximum Jumbo Frame size is 9,216 bytes. You can freely change the available packet size.

The Jumbo Frame application is often applied to Gigabit ports.



Jumbo Frame

System MTU size

System MTU	1522
Apply	
Reset	

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

Click "**Reset**" can change the MTU size back to normal (1522 bytes).

4.2.6 DHCP Server

You can select to **Enable** or **Disable** DHCP Server function. JetNet Managed 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.

DHCP Server

DHCP Server Configuration

Network	<input type="text" value="192.168.10.0"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Default Gateway	<input type="text" value="192.168.10.1"/>
Lease Time(s)	<input type="text" value="604800"/>

Apply

Once you have finished the configuration, click **Apply** 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 **Add** or **Remove**.

Excluded Address

IP Address	<input type="text" value="192.168.10.200"/>
------------	---

Add

Excluded Address List

Index	IP Address
1	192.168.10.200

Remove

Manual Binding: JetNet Managed Switch provides a MAC address and IP address binding and removing function. You can type in the specified IP and MAC address, then click **Add** 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 **Remove**.

Manual Binding

IP Address

MAC Address

Add

Manual Binding List

Index	IP Address	MAC Address

Remove

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

DHCP Leased Entries

Index	Binding	IP Address	MAC Address	Lease Time(s)
1	Auto	192.168.0.3	0012.77ff.0530	604785

Reload

DHCP Relay Agent

Relay Agent

Relay Policy ☐ Relay policy drop ☐ Relay policy keep ☒ Relay policy replace

Helper Address 1

Helper Address 2

Helper Address 3

Helper Address 4

Apply

DHCP Relay Agent: The DHCP Relay Agent is also known as DHCP Option 82. It can help relay the DHCP Request to remote DHCP server located in different subnet.

Note: The DHCP Server can not work with DHCP Relay Agent at the same time.

Relay Agent: Choose Enable or Disable the relay agent.

Relay Policy: The Relay Policy is used when the DHCP request is relayed through more than one switch. The switch can drop, keep or replace the MAC address of the DHCP Request packet.

Helper Address: Type the IP address of the target DHCP Server. There are 4 available IP addresses.

4.2.7 Backup and Restore

With Backup command, you can save current configuration file saved in the switch's flash to admin PC or TFTP server. This will allow you to go to **Restore** command later to restore the configuration file back to the switch. Before you restore the configuration file, you must place the backup configuration file in 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 the file name to backup the configuration. Users can also browse the target folder and select existed configuration file to restore the configuration back to the switch. This mode is only provided by Web UI while 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 please type the IP address of TFTP Server and Backup configuration file name. This mode can be used in both CLI and Web UI.

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

Backup/Restore File Name: Please type the correct file name of the configuration file..

Configuration File: The configuration file of the switch is a pure text file. You can open it by word/txt read file to check the settings. You can modify the file, add/remove the configuration settings, and then restore back to the switch.

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

Should you want the changed configuration can be activated after power recycle, **“Save to Flash” is a Must command**. Please check the description in Ch4.13.

Technical Tip:


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

Running Configuration File: The switch's CLI allows you to view the latest settings running by the system. The information shown here is the settings you set up but haven't saved to flash. The settings not yet saved to flash will not work after power recycle. You can use *show running-config* to view it in CLI.

Figure 4.2.7.1 Main UI of Backup & Restore

Backup & Restore

Backup Configuration Local File ▼

Backup File Name D:\TFTP\backup.conf 

Backup

Restore Configuration TFTP Server ▼


TFTP Server IP 192.168.0.100

Restore File Name backup.conf

Restore

Figure 4.2.7.2 Bacup/Restore Configuration – Local File mode.

Backup Configuration Local File ▼

Backup File Name 0.30\w0.30\Quagga1.conf 

Backup Help



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

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

Figure 4.2.5.3 Backup/Restore Configuration – TFTP Server mode

Backup Configuration TFTP Server ▼

TFTP Server IP 192.168.0.100

Backup File Name Backup1.conf

Backup

Type the IP address of TFTP Server IP. Then click on **Backup/Restore**.

Note: point to the wrong file will cause the entire configuration missed

4.2.8 Firmware Upgrade

In this section, you can update the latest firmware for your switch. Korenix provides the latest firmware in Korenix Web site. The new firmware may include new features, bug fixes or other software changes. We'll also provide the release notes for the update as well. For technical viewpoint, we suggest you use the latest firmware before installing the switch to the customer site.

Note that the system must be rebooted after you finished upgrading new firmware.


Please remind the attached users before you reboot the switch.

Figure 4.2.8.1 Main UI of Firmware Upgrade

Firmware Upgrade

System Firmware Version: v0.2.11
System Firmware Date: 20090413-15:04:17

Firmware Upgrade

Firmware File Name Local File Local File TFTP Server 

Note: When firmware upgrade is finished, the switch will restart automatically.

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 the file name to backup the configuration. Users also can browse the target folder and select the existed configuration file to restore the configuration back to the switch. This mode is only provided by Web UI while 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. And then please type the IP address of TFTP Server IP address. This mode can be used in both CLI and Web UI.

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

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

The UI also shows you the current firmware version and built date of current firmware. Please check the version number after the switch is rebooted.

Figure 4.2.8.2 Firmware Upgrade – Local File mode.

Firmware Upgrade

System Firmware Version: v0.2.11
System Firmware Date: 20090413-15:04:17

Firmware Upgrade

Firmware File Name Local File 

Note: When firmware upgrade is finished, the switch will restart automatically.

Upgrade



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

Figure 4.2.8.3 Warning Message.

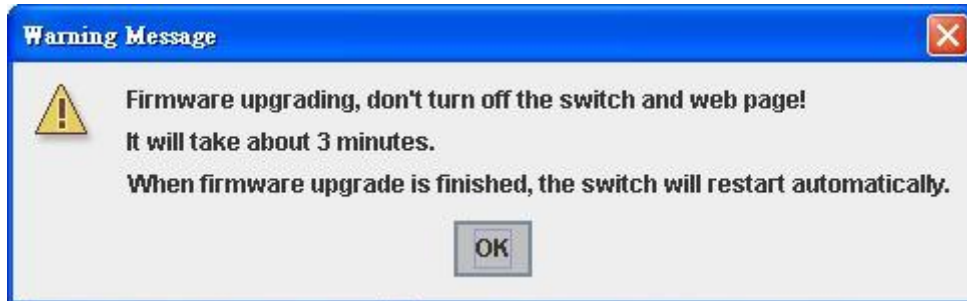
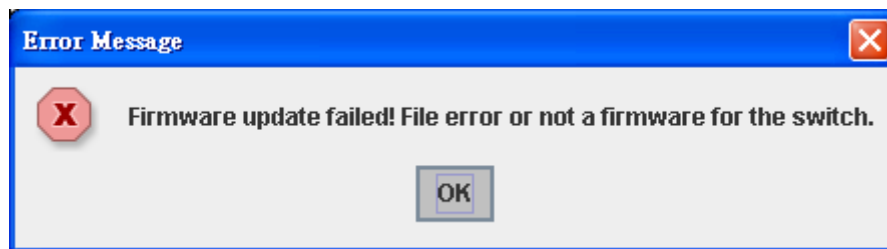


Figure 4.2.8.4 Error Message due to the file error or not a firmware for the switch.



Before upgrading firmware, please check the file name and switch model name first and carefully. Korenix switch provide protection when upgrading incorrect firmware file, the system would not crash even download the incorrect firmware. Even we have the protection, we still ask you don't try/test upgrade incorrect firmware, the unexpected event may occur or damage the system.

Figure 4.2.8.5 Firmware Upgrade – TFTP Server mode.

Firmware Upgrade

System Firmware Version: v0.2.11

System Firmware Date: 20090413-15:04:17

Firmware Upgrade		TFTP Server ▼
TFTP Server IP	<input type="text" value="192.168.10.20"/>	
Firmware File Name	<input type="text" value="J1etNet5628G-v1.0-image"/>	

Note: When firmware upgrade is finished, the switch will restart automatically.

Upgrade

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

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

4.2.9 Factory Default

In this section, you can reset all the configurations of the switch to default setting. Click on **Reset** the system will then reset all configurations to default setting. The system will show you popup message window after finishing this command. Default setting will work after rebooting the switch.

Figure 4.2.9.1 The main screen of the Reset to Default

Reset to Default

Note: The command will reset all configurations to the default settings except the IP address.

Reset

Figure 4.2.9.2 Popup alert screen to confirm the command. Click on **Yes** to start it.

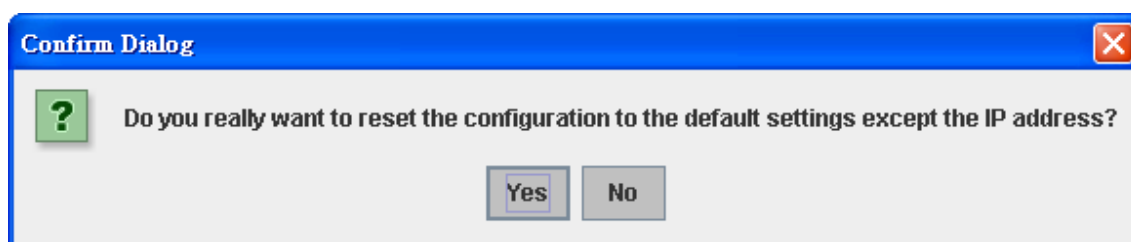
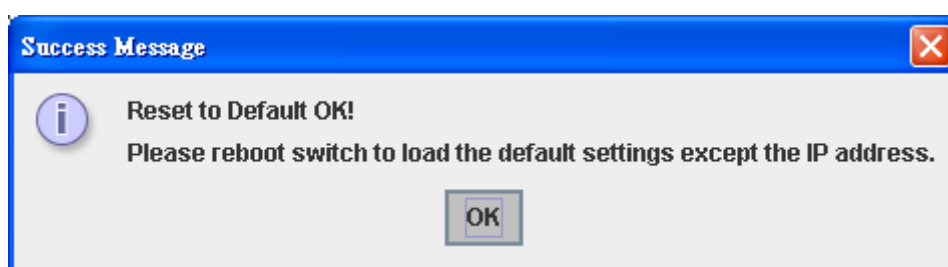


Figure 4.2.9.3 Popup message screen to show you that have done the command. Click on **OK** to close the screen. Then please go to **Reboot** page to reboot the switch.



Click on **OK**. The system will then auto reboot the device.

Note: If you already configured the IP of your device to other IP address, when you use this command by CLI and Web UI, our software will not reset the IP address to default IP. The system will remain the IP address so that you can still connect the switch via the network.

4.2.10 System Reboot

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

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

Figure 4.2.10.1 Main screen for Rebooting



Figure 4.2.10.2 Pop-up alert screen to request confirmation. Click on **Yes**. Then the switch will be rebooted immediately.

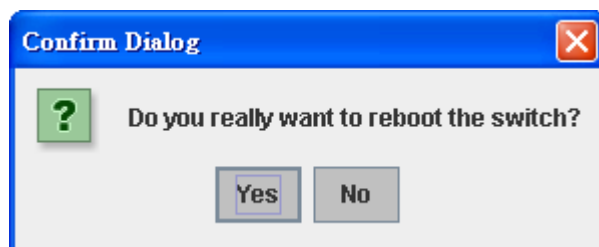
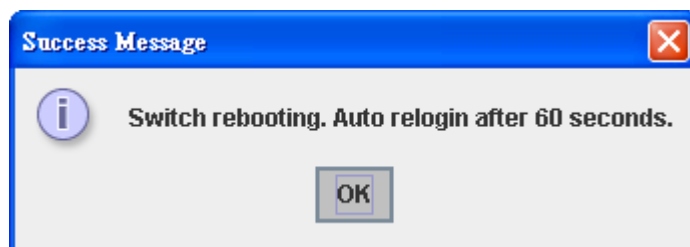


Figure 4.2.10.3 Pop-up message screen appears when rebooting the switch..



Note: Since different browser may has different behavior. If the Web GUI don't re-login well, please manually type the IP Address and login the system again.

4.2.11 CLI Commands for Basic Setting

Feature	Command Line
Switch Setting	
System Name	Switch(config)# hostname WORD Network name of this system Switch(config)# hostname JN5018G JN5018G(config)#

System Location	SWITCH(config)# snmp-server location Taipei
System Contact	SWITCH(config)# snmp-server contact korecare@korenix.com
Display (System Name, Location, Contact; System Firmware and Loader version, MAC address, LED status)	SWITCH# show snmp-server name SWITCH SWITCH# show snmp-server location Taipei SWITCH# show snmp-server contact korecare@korenix.com SWITCH> show version JetNet4518 Loader Version : 1.0.0.3 Firmware Version : 1.1.22-20100927-12:11:00 Copyright 2006-2009 Korenix Technology Co., Ltd. SWITCH# show hardware mac MAC Address : 001277FF1357 SWITCH# show hardware led led information mac mac address SWITCH# show hardware led Power 1 : On Power 2 : Off DO 1 : Off DO 2 : Off RDY : Off RM : Off RF : Off
Admin Password	
User Name and Password	SWITCH(config)# administrator NAME Administrator account name 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 dhcp igmp SWITCH(config-if)# ip address 192.168.10.8/24 (DHCP Client) SWITCH(config-if)# ip dhcp client SWITCH(config-if)# ip dhcp client renew
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 (Management VLAN, Running-Config)	<pre> SWITCH# show interface vlan1 interface vlan1 is up, line protocol detection is disabled index 22 metric 1 mtu 1500 <...> HWaddr: 00:12:77:ff:13:57 inet 192.168.10.1/24 broadcast 192.168.10.255 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 !</pre>
Time Setting	
NTP Server	<pre> SWITCH(config)# ntp peer enable disable primary secondary SWITCH(config)# ntp peer primary IPADDR SWITCH(config)# ntp peer primary 192.168.10.120</pre>
Time Zone	<pre> SWITCH(config)# clock timezone 26 Sun Jan 1 04:13:24 2006 (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London</pre> <p>Note: By typing clock timezone ?, you can see the timezone list. Then choose the number of the timezone you want to select.</p>
IEEE 1588	<pre> Switch(config)# ptpd run <cr> preferred-clock Preferred Clock slave Run as slave</pre>
Display	<pre> SWITCH# sh ntp associations Network time protocol Status : Disabled Primary peer : N/A Secondary peer : N/A SWITCH# show clock SWITCH# show clock Thu Oct 14 17:44:55 2010 (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London SWITCH# show clock timezone clock timezone (26) (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London Switch# show ptpd PTPd is enabled Mode: Slave</pre>
Jumbo Frame	

Jumbo Frame	<p>Type the maximum MTU to enable Jumbo Frame: SWITCH(config)# system mtu <64-9216> bytes (with VLAN tag) Switch(config)# system mtu 9216</p> <p>Disable Jumbo Frame: SWITCH(config)# no system mtu</p>
Display	<p>SWITCH# show system mtu System MTU size is 9216 bytes</p> <p>After disabled Jumbo Frame: SWITCH# show system mtu System MTU size is 1522 bytes</p>
DHCP Server/Relay Agent	
DHCP Commands	Switch(config)# router dhcp Switch(config-dhcp)# default-router DHCP Default Router end Exit current mode and down to previous enable mode exit Exit current mode and down to previous mode ip IP protocol lease DHCP Lease Time list Print command list network dhcp network no remove quit Exit current mode and down to previous mode service enable service
DHCP Server Enable	Switch(config-dhcp)# service dhcp <cr>
DHCP Server IP Pool (Network/Mask)	Switch(config-dhcp)# network A.B.C.D/M network/mask ex. 10.10.1.0/24 Switch(config-dhcp)# network 192.168.10.0/24
DHCP Server – Default Gateway	Switch(config-dhcp)# default-router A.B.C.D address Switch(config-dhcp)# default-router 192.168.10.254
DHCP Server – lease time	Switch(config-dhcp)# lease TIME second Switch(config-dhcp)# lease 1000 (1000 second)
DHCP Server – Excluded Address	Switch(config-dhcp)# ip dhcp excluded-address A.B.C.D IP address Switch(config-dhcp)# ip dhcp excluded-address 192.168.10.123 <cr>
DHCP Server – Static IP and MAC binding	Switch(config-dhcp)# ip dhcp static MACADDR MAC address Switch(config-dhcp)# ip dhcp static 0012.7700.0001 A.B.C.D leased IP address Switch(config-dhcp)# ip dhcp static 0012.7700.0001 192.168.10.99
DHCP Relay – Enable DHCP Relay	Switch(config-dhcp)# ip dhcp relay information option Option82 policy Option82 Switch(config-dhcp)# ip dhcp relay information option
DHCP Relay – DHCP policy	Switch(config-dhcp)# ip dhcp relay information policy drop Relay Policy keep Drop/Keep/Replace option82 field

	<pre> replace Switch(config-dhcp)# ip dhcp relay information policy drop <cr> Switch(config-dhcp)# ip dhcp relay information policy keep <cr> Switch(config-dhcp)# ip dhcp relay information policy replace <cr> </pre>
DHCP Relay – IP Helper Address	<pre> Switch(config-dhcp)# ip dhcp helper-address A.B.C.D Switch(config-dhcp)# ip dhcp helper-address 192.168.10.200 </pre>
Reset DHCP Settings	<pre> Switch(config-dhcp)# ip dhcp reset <cr> </pre>
DHCP Server Information	<pre> Switch# show ip dhcp server statistics DHCP Server ON Address Pool 1 network:192.168.10.0/24 default-router:192.168.10.254 lease time:604800 Excluded Address List IP Address ----- 192.168.10.123 Manual Binding List IP Address MAC Address ----- 192.168.10.99 0012.7701.0203 Leased Address List IP Address MAC Address Leased Time Remains ----- </pre>
DHCP Relay Information	<pre> Switch# show ip dhcp relay DHCP Relay Agent ON ----- IP helper-address : 192.168.10.200 Re-forwarding policy: Replace </pre>
Backup and Restore	
Backup Startup Configuration file	<pre> Switch# copy startup-config tftp: 192.168.10.33/default.conf Writing Configuration [OK] </pre> <p>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.</p> <p>Note 2: 192.168.10.33 is the TFTP server's IP and default.conf is name of the configuration file. Your environment may use different IP addresses or different file name. Please type target TFTP server IP or file name in this command.</p>
Restore Configuration	<pre> Switch# copy tftp: 192.168.10.33/default.conf startup-config </pre>
Show Startup Configuration	<pre> Switch# show startup-config </pre>
Show Running Configuration	<pre> Switch# show running-config </pre>

Firmware Upgrade	
Firmware Upgrade	Switch# archive download-sw /overwrite tftp 192.168.10.33 JN5018G.bin Firmware upgrading, don't turn off the switch! Tftping file JN5018G.bin Firmware upgrading Firmware upgrade success!! Rebooting.....
Factory Default	
Factory Default	Switch# reload default-config file
System Reboot	
Reboot	Switch# reboot

4.3 Port Configuration

Port Configuration group enables you to enable/disable port state, or configure port auto-negotiation, speed, and duplex, flow control, rate limit control and port aggregation settings. It also allows you to view port status and aggregation information.

Following commands are included in this group:

4.3.1 Understand the port mapping

4.3.2 Port Control

4.3.3 Port Status

4.3.4 Rate Control

4.3.5 Port Trunking

4.3.6 Command Lines for Port Configuration

4.3.1 Understand the port mapping

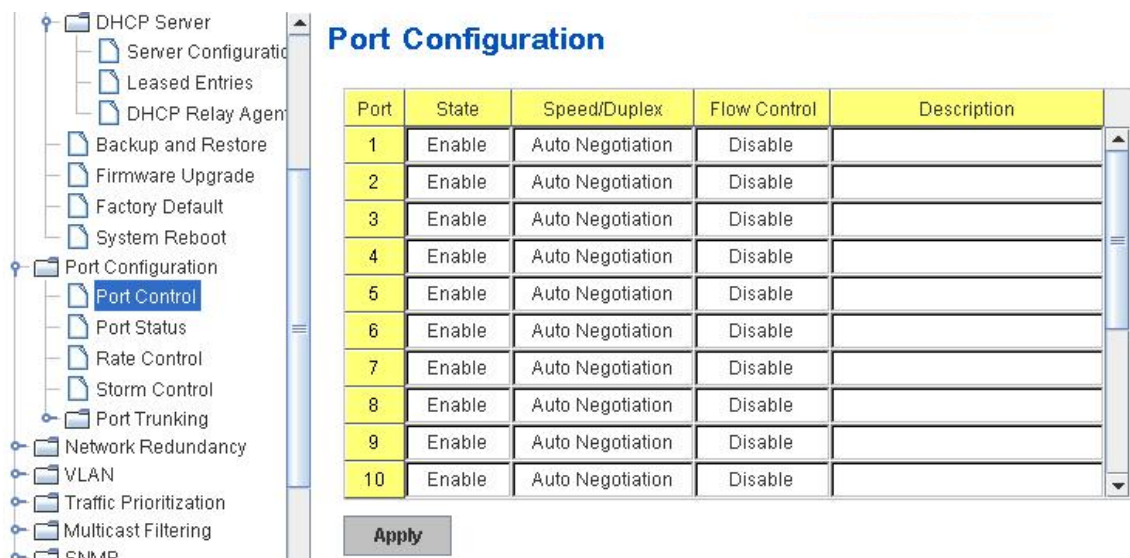
Before configuring the port settings, understand the port number in Managed Switch first.

The port ID is print on the front panel. Follow the port ID to configure your managed switch.

4.3.2 Port Control

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

Figure 4.3.2.1 The main Web UI of the Port Configuration.



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

In **State** column, you can enable or disable the state of this port. Once you disable, the port stop to link to the other end and stop to forward any traffic. The default setting is Enable which means all the ports are workable when you receive the device.

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

Fast Ethernet Port 1~N (fa1~faN): AutoNegotiation, 10M Full Duplex(10 Full), 10M Half Duplex(10 Half), 100M Full Duplex(100 Full) and 100M Half Duplex(100 Half).

Gigabit Ethernet Port 1~N (gi1~giN): AutoNegotiation, 10M Full Duplex(10 Full), 10M Half Duplex(10 Half), 100M Full Duplex(100 Full), 100M Half Duplex(100 Half), 1000M Full Duplex(1000 Full), 1000M Half Duplex(1000 Half).

The default mode is Auto Negotiation mode.

Note: The JetNet 5012G/5018G Gigabit SFP port only support 1000M Full mode. The JetNet 4518 SFP port only support 100M Full mode. The JetNet 5018G v2.0 supports both 100M Full and 1000M Full modes.

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 switch to work. “**Disable**” 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 switch will work anyway.

In **Description** column, you can add description to indicate the port’s location, connected device or other information. This is a friendly design especially when remotely managed the device.

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

Technical Tips: If both ends are not at the same speed, they can’t link with each other. If both ends are not in the same duplex mode, they will be connected by half mode.

4.3.3 Port Status

Port Status shows you current port status.

Figure 4.3.3.1 shows you the port status of the Fast Ethernet Ports. The blank area (port 1-8) means the module 1 are not inserted and the Figure 4.3.3.2 is for DDM SFP port status.

Port Status

Port	Type	Link	State	Speed/Duplex	Flow Control	SFP Vendor	Wavelength	Distance
1	100BASE-TX	Down	Enable	100 Full	Disable	—	—	—
2	100BASE-TX	Up	Enable	100 Full	Disable	—	—	—
3	100BASE	Down	Enable	—	Disable	—	—	—
4	100BASE	Down	Enable	—	Disable	—	—	—
5	100BASE	Down	Enable	—	Disable	—	—	—
6	100BASE	Down	Enable	—	Disable	—	—	—
7	100BASE	Down	Enable	—	Disable	—	—	—
8	100BASE	Down	Enable	—	Disable	—	—	—
9	100BASE	Down	Enable	—	Disable	—	—	—
10	100BASE	Down	Enable	—	Disable	—	—	—

Reload

Figure 4.3.3.1

The description of the columns is as below:

Port: Port interface number.

Type: 100BASE-TX -> Fast Ethernet copper port. 100BASE-FX -> 100Base-FX Fiber Port.

1000BASE-T -> Gigabit Ethernet Copper port. 1000BASE-X-> Gigabit Fiber Port

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

State: Enable -> State is enabled. Disable -> The port is disable/shutdown.

Speed/Duplex: Current working status of the port.

Flow Control: The state of the flow control.

SFP Vendor: Vendor name of the SFP transceiver you plugged. The information is only applied to on board ports.

Wavelength: The wave length of the SFP transceiver you plugged.

Distance: The transmission distance of the SFP transceiver you plugged.

17	100BASE-TX	Up	Enable	100 Full	Disable	--	--	--
18	1000BASE-SX	Down	Enable	--	Disable	Non-Certified	850nm	550m

SFP DDM

Port	SFP Scan / Eject	SFP DDM	Temperature (°C)		Tx Power (dBm)		Rx Power (dBm)	
			Current	Range	Current	Range	Current	Range
17	Scan	Disable	--	--	--	--	--	--
18	Eject	Disable	--	--	--	--	--	--

Reload Scan All Eject All

Figure 4.3.3.2

Reload: reload the all SFP port information.

Scan all: scan the SFP DDM transceiver and display the information.

Eject: Eject the SFP transceiver that you have selected. You can eject one port or eject all by click the icon "Eject All".

Temperature: The temperature specific and current detected of DDM SFP transceiver.

Tx Power (dBm): The specification and current transmit power of DDM SFP transceiver.

Rx Power (dBm): The specification and current received power of DDM SFP transceiver.

Note: 1. Most of the SFP transceivers provide vendor information which allows your switch to read it. The UI can display vendor name, wave length and distance of all Korenix SFP transceiver family. If you see Unknown info, it may mean that the vendor doesn't provide their information or that the information of their transceiver can't be read.

2. If the DDM SFP transceiver is not certified by Korenix, the DDM function will not be supported. But the communication will not be disabled.

Note: Most of the SFP transceivers provide vendor information which allows your switch to read it. The UI can display vendor name, wave length and distance of all Korenix SFP transceiver family. If you see Unknown info, it may mean that the SFP transceiver is not certified by Korenix Quality system, and the vendor information won't display except other technical information. Besides, the Digital Diagnostic Monitoring function only support Korenix certified DDM SFP transceiver.

4.3.4 Rate Control

Rate limiting 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.

Figure 4.3.4.1 shows you the Limit Rate of Ingress and Egress. You can type the volume in the blank. The volume of the JetNet 4518/5018G/5012G is step by 8Kbps.

Rate Control

Limit Packet Type and Rate

Port	Ingress Rate(Kbps)	Egress Rate(Kbps)
1	8	16
2	0	0
3	40	48
4	0	0
5	0	0
6	0	0
7	0	0
8	0	0
9	0	0
10	0	0

Apply

4.3.5 Storm Control

The Storm Control is similar to Rate Control. Rate Control filters all the traffic over the threshold you input by UI. Storm Control allows user to define the Rate for specific Packet Types. These kinds of packet types are legal packets, but they may useless and affect the network performance. It is suggested to limit them, at least limit the rate of the uplink ports.

Figure 4.3.5.1

Rate Configuration: This column allows you to manually assign the limit rate for the specific packet type base on Kbytes per second. The packet types of the Ingress Rule listed here include **Broadcast**, **DLF (Destination Lookup Failure)** and **Multicast**.

The limit range is from 0 to the maximum available speed of the port. For example, the Fast Ethernet port allows 0-100,000 Kbytes/sec. Zero means no limit.

Choose **Enable/Disable** to enable or disable the storm control packet type of the specific port.

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

Storm Control

Rate Configuration

Broadcast Rate(Kbytes/sec)	2000
DLF Rate(Kbytes/sec)	2000
Multicast Rate(Kbytes/sec)	2000

Port Configuration

Port	Broadcast	DLF	Multicast
1	Disable	Disable	Disable
2	Disable	Disable	Disable
3	Disable	Disable	Disable
4	Disable	Disable	Disable
5	Disable	Disable	Disable
6	Disable	Disable	Disable
7	Disable	Disable	Disable
8	Disable	Disable	Disable
9	Disable	Disable	Disable
10	Disable	Disable	Disable

Apply

4.3.6 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.

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. **In practical, the Static Trunk is suggested.**

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

Port Trunk - Aggregation Setting

Port	Group ID	Trunk Type
1	None	Static
2	None	Static
3	Trunk 1	Static
4	Trunk 2	Static
5	Trunk 3	Static
6	Trunk 4	Static
7	Trunk 5	Static
8	Trunk 6	Static
9	Trunk 7	Static
10	None	Static

Note: The port parameters of the trunk members should be the same.

Apply

Aggregation Setting

Trunk Size: The switch can support up to 8 trunk groups. Each trunk group can support up to 8 member ports. Since the member ports should use same speed/duplex, the maximum trunk size is decided by the port volume.

Group ID: Group ID is the ID for the port trunking group. Ports with same group ID are in the same group. Click None, you can select the Trunk ID from Trunk 1 to Trunk 8.

Trunk Type: Static and 802.3ad LACP. Each Trunk Group can only support Static or 802.3ad LACP. Choose the type you need here. The not active port can't be setup here.

Extended setting in CLI:

Port Priority: The command allows you to change the port priority setting of the specific port. LACP port priority is configured on each port using LACP. The port priority can be configured through the CLI. The higher the number, the lower the priority. The default value is 32768.

LACP Timeout: The LACPDU is generated and continue transmit within the LACP group. The interval time of the LACPDU Long timeout is 30 sec, this is default setting. The LACPDP Short timeout is 1 sec, the command to change from Long to Short is only applied to the CLI, the web GUI doesn't support this. Once the LACP port doesn't receive the LACPDP 3 times, that means the port may leave the group without earlier inform or does not detect by the switch, then the port will be removed from the group.

This command can be used when connect the switch by 2-port LACP through not-direct connected or shared media, like the Wireless AP or Hub. The end of the switch may not directly detect the failure, the LACP Short Timeout can detect the LACP group failure earlier within 3 seconds.

Aggregation Status

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

Port Trunk - Aggregation Information

Group ID	Type	Group Member		
		Aggregated	Individual	Link Down
Trunk 1	LACP		7	5,6
Trunk 2	LACP	8,9,10		
Trunk 3				
Trunk 4				
Trunk 5				

Group ID: Display Trunk 1 to Trunk 5 set up in Aggregation Setting.

Type: Static or LACP set up in Aggregation Setting.

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

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

4.3.7 Command Lines for Port Configuration

Feature	Command Line
Port Control	
Port Control – State	<p>Switch(config-if)# shutdown -> Disable port state Port1 Link Change to DOWN interface fastethernet1 is shutdown now.</p> <p>Switch(config-if)# no shutdown -> Enable port state Port1 Link Change to UP interface fastethernet1 is up now.</p>
Port Control – Auto Negotiation	<p>Switch(config)# interface fa1 Switch(config-if)# auto-negotiation Auto-negotiation of port 1 is enabled!</p>
Port Control – Force Speed/Duplex	<p>Switch(config-if)# speed 100 set the speed mode ok!</p> <p>Switch(config-if)# duplex full set the duplex mode ok!</p>
Port Control – Flow Control	<p>Switch(config-if)# flowcontrol on Flowcontrol on for port 1 set ok!</p> <p>Switch(config-if)# flowcontrol off Flowcontrol off for port 1 set ok!</p>

Port Status	
Port Status	<p>Switch# show interface fa1 Interface fastethernet1 Administrative Status : Enable Operating Status : Connected Duplex : Full Speed : 100 MTU: 1518 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.</p> <p>Switch# show sfp ddm →show SFP DDM information Port 17 Temperature:N/A Tx power:N/A Rx power:N/A Port 18 Temperature:64.00 C <range :0.0-80.00> Tx power:-6.0 dBm <range : -9.0 - -4.0> Rx power:-30.0 dBm <range: -30.0 - -4.0></p> <p>Switch(config-if)# sfp ddm Digital diagnostic and monitoring eject Eject SFP scan Scan SFP</p> <p><i>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.</i></p>
Rate Control	
Rate Control – Ingress or Egress	<p>Switch(config-if)# rate-limit egress Outgoing packets ingress Incoming packets</p> <p>Note: To enable rate control, you should select the Ingress or Egress rule first; then assign the packet type and bandwidth.</p>
Rate Control - Bandwidth	<p>Switch(config-if)# rate-limit ingress bandwidth <0-1000000> Limit in kilobits per second (FE: 0-100000, GE: 0-1000000, 0 is no limit) Switch(config-if)# rate-limit ingress bandwidth 800 Set the ingress rate limit 800Kbps for Port 1.</p>
Storm Control	
Strom Control – Rate Configuration (Packet	<p>Switch(config-if)# storm-control broadcast Broadcast packets dlf Destination Lookup Failure</p>

Type)	<p>multicast Multicast packets</p> <p>SWITCH(config)# storm-control broadcast ? <0-100000> Rate limit value 0~100000Kbyte/sec</p> <p>SWITCH(config)# storm-control broadcast 10000 limit_rate = 10000 Set rate limit for Broadcast packets.</p> <p>SWITCH(config)# storm-control multicast 1000 limit_rate = 1000 Set rate limit for Multicast packets.</p> <p>SWITCH(config)# storm-control dlf 1000 limit_rate = 1000 Set rate limit for Destination Lookup Failure packets.</p>
Storm Control – Enable Storm Control to a port	<p>SWITCH(config)# interface fa1 SWITCH(config-if)# storm-control broadcast Broadcast packets dlf Destination Lookup Failure multicast Multicast packets</p> <p>SWITCH(config-if)# storm-control broadcast <cr> SWITCH(config-if)# storm-control broadcast Enables rate limit for Broadcast packets for Port 1.</p> <p>(Continue apply to other ports)</p>
Display – Rate Configuration and port status	<p>SWITCH# show storm-control Storm-control rate limit: DLF:1000(Kbytes/sec) Multicast:1000(Kbytes/sec) Broadcast:1000(Kbytes/sec) -----</p> <p>Port 1: DLF Enable Broadcast Enable Multicast Enable</p> <p>Port 2: DLF Enable Broadcast Enable Multicast Enable </p>
Port Trunking	
LACP	<p>Switch(config)# lacp group 1 gi8-10 Group 1 based on LACP(802.3ad) is enabled!</p> <p><i>Note: The interface list is fa1,fa3-5,gi8-10</i> Note: different speed port can't be aggregated together.</p>
LACP – Port Setting	<p>SWITCH(config-if)# lacp port-priority LACP priority for physical interfaces timeout assigns an administrative LACP timeout</p> <p>SWITCH(config-if)# lacp port-priority <1-65535> Valid port priority range 1 - 65535 (default is 32768)</p> <p>SWITCH(config-if)# lacp timeout</p>

	<div>long specifies a long timeout value (default)</div> <div>short specifies a short timeout value</div> <div>SWITCH(config-if)# lacp timeout short</div> <div>Set lacp port timeout ok.</div>
Static Trunk	<div>Switch(config)# trunk group 2 fa6-7</div> <div>Trunk group 2 enable ok!</div> <div>Failure to configure due to the group ID is existed.</div> <div>SWITCH(config)# trunk group 1 fa11-12</div> <div>Can't set trunk group 1 enable!</div> <div>The group 1 is a lacp enabled group!</div> <div>SWITCH(config)# trunk group 2 fa11-12</div> <div>Can't set trunk group 2 enable!</div> <div>The group 2 is a static aggregation group.</div>
Display – LACP Information	<div>Switch# show lacp</div> <div><div>countersLACP statistical information</div><div>groupLACP group</div><div>internalLACP internal information</div><div>neighborLACP neighbor information</div><div>port-settingLACP setting for physical interfaces</div><div>system-idLACP system identification</div><div>system-priorityLACP system priority</div></div> <div>SWITCH# show lacp port-setting</div> <div>LACP Port Setting :</div> <div><div>PortPriorityTimeout</div><div>-----</div><div><div>132768Long</div><div>232768Long</div><div>332768Long</div></div><div>.....</div></div> <div>Switch# show lacp internal</div> <div>LACP group 1 internal information:</div> <div><div><div>LACP PortAdminOperPort</div><div>PortPriorityKeyKeyState</div><div>-----</div><div><div>81880x45</div><div>91990x45</div><div>10110100x45</div></div></div></div> <div>LACP group 2 is inactive</div> <div>LACP group 3 is inactive</div> <div>LACP group 4 is inactive</div>
Display - Trunk	<div>Switch# show trunk group 1</div> <div>FLAGS: I -> IndividualP -> In channel</div> <div>D -> Port Down</div> <div>Trunk Group</div> <div><div>GroupIDProtocolPorts</div><div>-----+-----</div><div><div>1LACP8(D) 9(D) 10(D)</div></div></div>

4.4 Network Redundancy

It is critical for industrial applications that network remains non-stop. Korenix develops multiple kinds of standard (STP, RSTP and MSTP) and Korenix patterned redundancy protocol, Multiple Super Ring to remain the network redundancy can be protected well by Korenix switch.

The JetNet Switch supports advanced Multiple Spanning Tree Protocol (MSTP). 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).

Multiple Super Ring (MSR) technology is *Korenix's 3rd* generation Ring redundancy technology. This is patented and protected by *Korenix* and 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 5 milliseconds for failover for copper.

The single Korenix switch can aggregate multiple Rings within one switch. All the ports can be configured as the ring port of a ring, each ring has its own Ring ID and the Ring ID will be added to the watchdog packet to monitor the ring status. This is Korenix Patterned MultiRing Technology.

The Ring ports can be LACP/Port Trunking ports, after aggregated ports to a group, the group of ports can act as the Ring port of the Ring. This is Korenix Patterned TrunkRing Technology.

Advanced Rapid Dual Homing(RDH) technology also facilitates *JetNet 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.

Following commands are included in this group:

4.4.1 STP Configuration

4.4.2 STP Port Configuration

4.4.3 STP Information

4.4.4 MSTP Configuration

4.4.5 MSTP Port Configuration

4.4.6 MSTP information

4.4.7 Multiple Super Ring

4.4.8 Multiple Super Ring Information

4.4.9 Command Lines for Network Redundancy

The STP Configuration, STP Port Configuration and STP Information pages are available while select the STP and RSTP mode.

The MSTP Configuration, MSTP Port Configuration and MSTP Information pages are available while select the MSTP mode.

The Multiple Super Ring and Multiple Super Ring Information are available while select the MSR mode.

4.4.1 STP Configuration

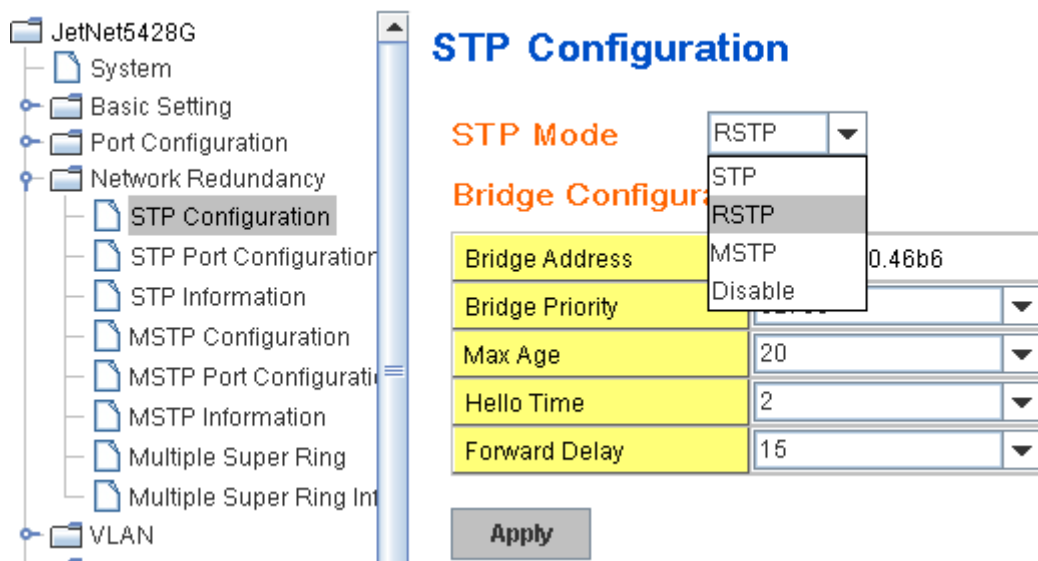
This page allows select the STP mode and configuring the global STP/RSTP Bridge Configuration.

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 4.4.1.1 show the web page which allows you to select the STP mode, configure the global STP/RSTP/MSTP settings. (Refers to JetNet 5428G user interface)



RSTP (Refer to the 4.4.1 of previous version manual.)

RSTP is the abbreviation of 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 much faster spanning tree convergence after a topology change. This is specified in IEEE 802.1w. In 2004, 802.1w is included into 802.1D-2004 version. This switch supports both RSTP and STP (all switches that support RSTP are also backward compatible with switches that support only STP).

Bridge Configuration

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 the bridge ID has 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.

Note: The Web GUI allows user select the priority number directly. This is the convenient 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 $n \times 4096$ rule 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 JetNet is not the root bridge, and if it has not received a hello message from the root bridge in an amount of time equal to Max Age, then JetNet 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.

The MAX Age value affects the maximum volume of the RSTP loop. In the RSTP BPDU packet, there is one field, message age which start from 0, add 1 after passed one hop in the RSTP loop. When the message age is larger than MAX Age, the BPDU would be ignored and the lower switches are separated to different RSTP domain. The switches in other RSTP domain can't be managed through upper switch.

Since different RSTP aware switches may have their own mechanism to calculate the message age. So that this is most possibly occurred when interoperate different vendors' RSTP aware switches together. The maximum volume of the Korenix RSTP domain is 23, configure the MAX Age lower than 23 is recommended.

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 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 during 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 JetNet will wait before checking to see if it should be changed 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 Hello Time, Forwarding Delay, and Max Age parameter

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

4.4.2 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 and you will be able to view 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 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 link types for your selection-**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 link status of the link to be manipulated administratively. “**Auto**” means to auto select P2P or Share mode. “**P2P**” means P2P is enabled; the 2 ends work in full duplex mode. While “**Share**” is enabled, it means P2P is disabled; the 2 ends may connect through a share media and work in half duplex mode.

Edge Port: 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.

STP Port Configuration

Port	Path Cost	Priority	Link Type	Edge Port
1	200000	0	Auto	Enable
2	200000	0	Auto	Enable
3	200000	16	Auto	Enable
4	200000	32	Auto	Enable
5	200000	48	Auto	Enable
6	200000000	64	Auto	Enable
7	200000000	80	Auto	Enable
8	20000	96	Auto	Enable
9	20000	112	Auto	Enable
10	20000	32768	Auto	Enable

Apply

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

4.4.3 RSTP Info

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	Aggregated(ID/Type)
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	200000	128	P2P	Edge	--
9	Designated	Forwarding	200000	128	P2P	Edge	--
10	Designated	Forwarding	200000	128	P2P	Edge	--

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 and Aggregated(ID/Type).

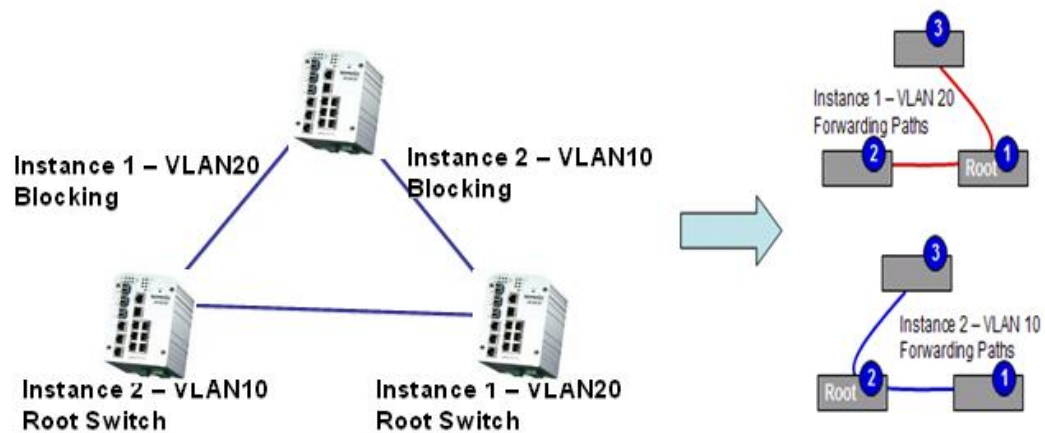
4.4.4 MSTP (Multiple Spanning Tree Protocol) Configuration

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 groups, act as root or designate switch, generate BPDU for the network to maintain the forwarding table of the spanning tree. With MSTP can also provide multiple forwarding paths and enable load balancing. Understand the architecture allows you to maintain the correct spanning tree and operate effectively.

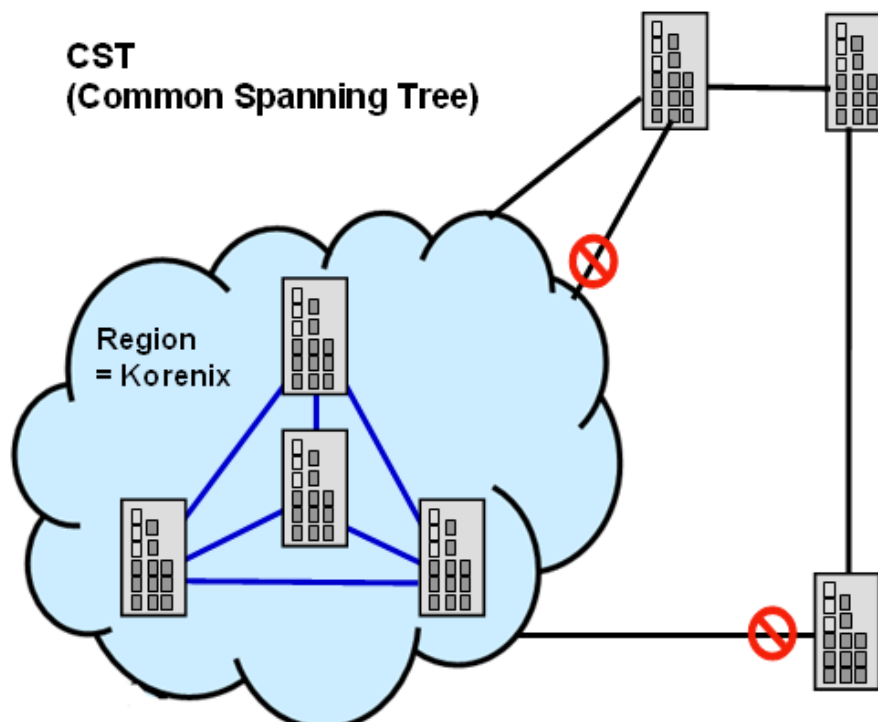
One VLAN can be mapped to a Multiple Spanning Tree Instance (MSTI). For example, the maximum Instance JetNet supports is usually 16, range from 0-15. The MSTP builds a separate Multiple Spanning Tree (MST) for each instance to maintain connectivity among each of the assigned VLAN groups. An Internal 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.



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.



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

STP Configuration

STP Mode

Bridge Configuration

Bridge Address	0012.7760.46b6
Bridge Priority	32768 ▼
Max Age	20 ▼
Hello Time	2 ▼
Forward Delay	15 ▼

Apply

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 level.

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.

MSTP Configuration

MST Region Configuration

Region Name	Korenix
Revision	0

Apply

New MST Instance

Instance ID	1 ▼
VLAN Group	
Instance Priority	32768 ▼

Add

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.

Current MST Instance Configuration

Instance ID	VLAN Group	Instance Priority	
1	2	32768	▲
2	3	32768	▼

Apply

Remove

Reload

4.4.5 MSTP Port Configuration

This page allows configure the Port settings. Choose the Instance ID you want to configure. The MSTP enabled and linked up ports within the instance will be listed in this table.

Note that the ports not belonged to the Instance, or the ports not MSTP activated will not display. The meaning of the Path Cost, Priority, Link Type and Edge Port is the same as the definition of RSTP.

MSTP Port Configuration

Instance ID

Port	Path Cost	Priority	Link Type	Edge Port	
1	200000	128	Auto	Enable	▲
2	200000	128	Auto	Enable	▼

Apply

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 link status of the link to be manipulated administratively. “**Auto**” means to auto select P2P or Share mode. “**P2P**” means P2P is enabled, the 2 ends work in Full duplex mode. While “**Share**” is enabled, it means P2P is disabled, the 2 ends may connect through a share media and work in Half duplex mode.

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 finish your configuration, click on **Apply** to save your settings.

4.4.6 MSTP Information

This page allows you to see the current MSTP information.

Choose the **Instance ID** first. If the instance is not added, the information remains blank.

The **Root Information** shows the setting of the Root switch.

The **Port Information** shows the port setting and status of the ports within the instance.

MSTP Information

Instance ID

Root Information

Root Address	0012.7760.ad4b
Root Priority	4096
Root Port	N/A
Root Path Cost	0
Max Age	20 second(s)
Hello Time	2 second(s)
Forward Delay	15 second(s)

Port Information

Port	Role	Port State	Path Cost	Port Priority	Link Type	Edge Port
5	Designated	Forwarding	200000	128	P2P Internal(MSTP)	Non-Edge
6	Designated	Forwarding	200000	128	P2P Internal(MSTP)	Non-Edge

Click on “**Reload**” to reload the MSTP information display.

4.4.7 Multiple Super Ring (MSR)

The most common industrial network redundancy is to form a ring or loop. Typically, the managed switches are connected in series and the last switch is connected back to the

first one. In such connection, you can implement Korenix Multiple Super Ring technology to get fastest recovery performance.

Multiple Super Ring (MSR) technology is *Korenix's* 3rd generation Ring redundancy technology. This is patented and protected by *Korenix* and 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 *JetNet 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 JetNet 5428G is a 24 Fast Ethernet + 4 Gigabit port design, that means maximum 14 Rings (12 x 100M Rings and 2 Gigabit Rings) can be aggregated to one JetNet 5428G. The feature saves much effort when constructing complex network architecture.

To become backwards compatible with the Legacy Super Ring technology implemented in *JetNet 4008/4508 V1* series switches, *JetNet 4510/4518/5000 Series* 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 Rapid 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 automatically naming with Ring ID.

New Ring

Ring ID	Name
<input type="text" value="1"/>	<input type="text"/>

Ring Configuration

ID	Name	Version	Device Priority	Ring Port1	Path Cost	Ring Port2	Path Cost	Rapid Dual Homing	Ring Status
1	Ring1	Rapid Super R	128	Port 1	128	Port 2	128	Disable	Enable

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 Korenix 1st 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 Port 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 Korenix 3rd generation Ring redundancy technology. When you want to connect multiple RSR or form a 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 JetNet 4000/4500 series, 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 them 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 pattern of the MSR technology, the technology 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 JetNet 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 to the port volume limitation, the maximum value is half of the port volume of a switch.

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 (Static 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.

4.4.8 Ring Info

This page shows the MSR information.

Multiple Super Ring Information

ID	Version	Role	Status	RM MAC	Blocking Port	Role Transition Count	Ring State Transition Count
1	Rapid Super Ring	RM	Normal	0012.7760.1455	fa2	2	4

Reload

ID: Ring ID.

Version: which version of this ring, this field could be Rapid Super Ring, Super Ring, or Any 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 is blocked port of RM.

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.

4.4.9 Command Lines:

Feature	Command Line
Global	
Enable	Switch(config)# spanning-tree enable
Disable	Switch (config)# 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 prtocol (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 max-age <6-40> Valid range is 6~40 seconds Switch(config)# spanning-tree max-age 20
Hello Time	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 Configuration Tree	Switch(config)# spanning-tree mst MSTMAP the mst instance number or range configuration enter mst configuration mode forward-time the forward delay 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 nixnix 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 Configuration	Switch(config-mst)# show current Current MST configuration Name nixnix] Revision 65535

	<pre> Instance Vlans Mapped ----- 0 1,4-4094 1 2 2 -- Config HMAC-MD5 Digest: 0xB41829F9030A054FB74EF7A8587FF58D ----- </pre>
Remove Region Name	<pre> Switch(config-mst)# no name name configure revision revision configure instance the mst instance Switch(config-mst)# no name </pre>
Remove Instance example	<pre> Switch(config-mst)# no instance <1-15> target instance number Switch(config-mst)# no instance 2 </pre>
Show Pending MST Configuration	<pre> 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 -- Config HMAC-MD5 Digest: 0x3AB68794D602FDF43B21C0B37AC3BCA8 ----- </pre>
Apply the setting and go to the configuration mode	<pre> Switch(config-mst)# quit apply all mst configuration changes Switch(config)# </pre>
Apply the setting and go to the global mode	<pre> Switch(config-mst)# end apply all mst configuration changes Switch# </pre>
<p>Abort the Setting and go to the configuration mode.</p> <p>Show Pending to see the new settings are not applied.</p>	<pre> Switch(config-mst)# abort discard all mst configuration changes Switch(config)# spanning-tree mst configuration Switch(config-mst)# show pending Pending MST configuration Name orenixnix] (->The name is 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 ----- </pre>
RSTP	
The mode should be rst, the timings can be configured in global settings listed in above.	
Global Information	
Active Information	<pre> 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 </pre>

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

	<pre> 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) </pre>
MSTP Root Information	<pre> 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 </pre>
MSTP Instance Information	<pre> 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) </pre>
MSTP Port Information	<pre> 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 </pre>
Multiple Super Ring	
Create or configure a Ring	<pre> Switch(config)# multiple-super-ring 1 Ring 1 created Switch(config-multiple-super-ring)# Note: 1 is the target Ring ID which is going to be created or configured. </pre>
Super Ring Version	<pre> Switch(config-multiple-super-ring)# version default set default to rapid super ring rapid-super-ring rapid super ring super-ring super ring Switch(config-multiple-super-ring)# version rapid-super-ring </pre>
Priority	<pre> Switch(config-multiple-super-ring)# priority <0-255> valid range is 0 to 255 </pre>

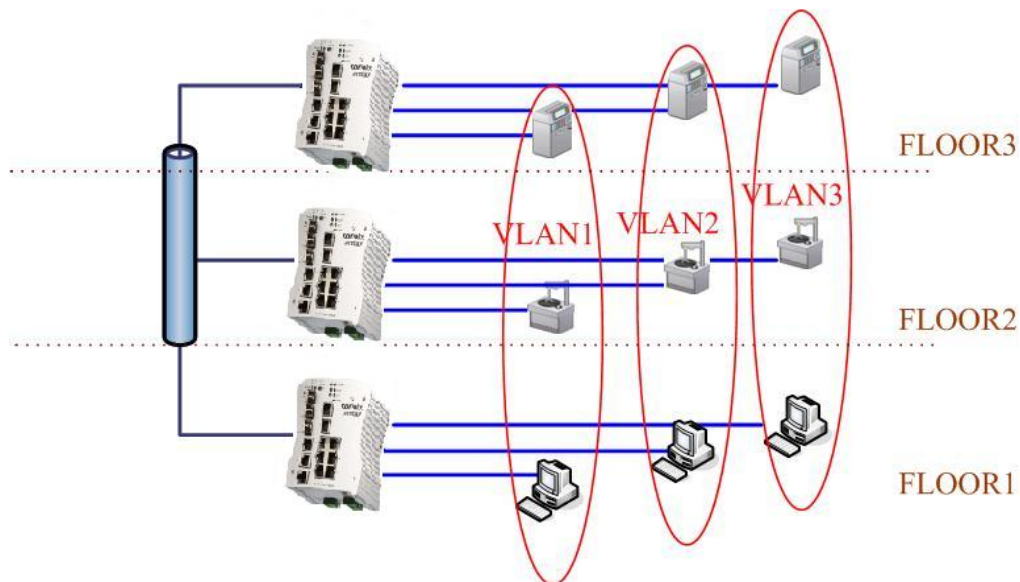
	default set default Switch(config)# super-ring priority 100
Ring Port	Switch(config-multiple-super-ring)# port IFLIST Interface list, ex: fa1,fa3-5,gi8-10 cost path cost Switch(config-multiple-super-ring)# port fa1,fa2
Ring Port Cost	Switch(config-multiple-super-ring)# port cost <0-255> valid range is 0 or 255 default set default (128)valid range is 0 or 255 Switch(config-multiple-super-ring)# 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-multiple-super-ring)# rapid-dual-homing enable Switch(config-multiple-super-ring)# rapid-dual-homing disable Switch(config-multiple-super-ring)# rapid-dual-homing port IFLIST Interface name, ex: fastethernet1 or gi8 auto-detect up link auto detection IFNAME Interface name, ex: fastethernet1 or gi8 Switch(config-multiple-super-ring)# rapid-dual-homing port fa3,fa5-6 set Rapid Dual Homing port success. Note: auto-detect is recommended for dual 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 Dual-Homing II : 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.

4.5 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.

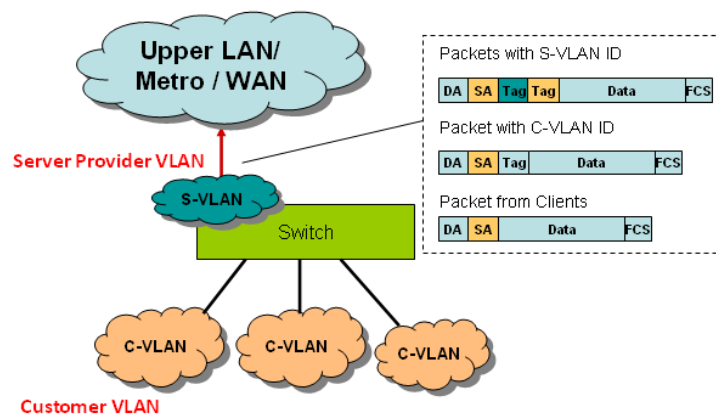
JetNet Industrial Ethernet Switch supports 802.1Q VLAN. 802.1Q VLAN is also known as Tag-Based VLAN. This Tag-Based VLAN allows VLAN to be created across different switches (see Figure 1). IEEE 802.1Q tag-based VLAN makes use of VLAN control information stored in a VLAN header attached to IEEE 802.3 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.

Figure 4.5.1 802.1Q VLAN



QinQ

The QinQ is originally designed to expand the number of VLANs by adding a tag to the 802.1Q packets. The original VLAN is usually identified as Customer VLAN (C-VLAN) and the new added tag - as Service VLAN (S-VLAN). By adding the additional tag, QinQ increases the possible number of VLANs. After QinQ enabled, the JetNet can reach up to 256x256 VLANs. With different standard tags, it also improves the network security.



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

Following commands are included in this group:

4.5.1 VLAN Port Configuration

4.5.2 VLAN Configuration

4.5.3 GVRP Configuration

4.5.4 VLAN Table

4.5.5 CLI Commands of the VLAN

4.5.1 VLAN Port 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 4.5.2 Web UI of VLAN configuration.

VLAN Port Configuration

VLAN Port Configuration

Port	PVID	Tunnel Mode	Accept Frame Type	Ingress Filtering
1	1	None	Admit All	Disable
2	1	None	Admit All	Disable
3	1	802.1Q Tunnel	Admit All	Disable
4	1	802.1Q Tunnel Uplink	Admit All	Disable
5	1	None	Admit All	Disable
6	1	None	Admit All	Disable
7	5	None	Admit All	Disable
8	4	None	Admit All	Disable
9	5	None	Admit All	Disable
10	2	None	Admit All	Disable

Apply

PVID: The abbreviation of the **Port VLAN ID**. Enter 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 can't 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.

Tunnel Mode: This is the new command for QinQ. The command includes None, 802.1Q Tunnel and 802.1Q Tunnel Uplink. The figure shows the relationship between 802.1Q Tunnel and 802.1Q Tunnel Uplink.



Following is the modes you can select.

None: Remain VLAN setting, no QinQ.

802.1Q Tunnel: The QinQ command applied to the ports which connect to the C-VLAN. The port receives tagged frame from the C-VLAN. Add a new tag (Port VID) as S-VLAN VID. When the packets are forwarded to C-VLAN, the S-VLAN tag is removed.

After 802.1Q Tunnel mode is assigned to a port, the egress setting of the port should be “**Untag**”, it indicates the egress packet is always untagged. This is configured in Static VLAN Configuration table. Please refer to the VLAN Configuration chapter in below.

802.1Q Tunnel Uplink: The QinQ command applied to the ports which connect to the S-VLAN. The port receives tagged frame from the S-VLAN. When the packets are forwarded to S-VLAN, the S-VLAN tag is kept.

After 802.1Q Tunnel Uplink mode is assigned to a port, the egress setting of the port should be “**Tag**”, it indicates the egress packet is always tagged. This is configured in Static VLAN Configuration table. Please refer to the VLAN Configuration chapter in below.

For example, the VID of S-VLAN/Tunnel Uplink is 10, the VID of C-VLAN/Tunnel is 5. The 802.1Q Tunnel port receives tag 5 from C-VLAN, add tag 10 to the packet. When the packets are forwarded to S-VLAN, tag 10 is kept.

EtherType: This column allows you to define the EtherType manually. This is advanced QinQ parameter which allows to define the transmission packet type.

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.

4.5.2 VLAN Configuration

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

Figure 4.5.2.1 Web UI of the VLAN Configuration.

VLAN Configuration

Management VLAN ID

Apply

Static VLAN

VLAN ID	Name
<input type="text"/>	<input type="text"/>

Add

Static VLAN Configuration

VLAN ID	Name	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
1	VLAN1	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U

Apply

Remove

Reload

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).

Static VLAN

VLAN ID	NAME
<input type="text" value="3"/>	<input type="text" value="test"/>

Add

Help

Figure 4.5.2.2 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. Refer to Figure 4.5.2.3

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.

Note: Currently JetNet 4518/5012/5018G/5018G v2.0 supports max 255 group VLAN.

Static VLAN Configuration

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

Figure 4.5.2.3 Static VLAN Configuration table. You can see that new VLAN 3 is created. VLAN name is test. Egress rules of the ports are not configured now.

Static VLAN Configuration

VLAN ID	Name	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
1	VLAN1	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U
2	V2	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
3	test	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Apply Remove Reload

Figure 4.5.2.4 Configure Egress rule of the ports.

Static VLAN Configuration

VLAN ID	Name	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
1	VLAN1	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U
2	V2	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
3	test	--	--	--	--	--	--	--	--	U	U	U	T	T	T	--	--	--	--	--

Apply Remove Reload

-- : 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.

4.5.3 GVRP configuration

GVRP allows users to set-up VLANs automatically rather than manual configuration on every port of every switch in the network. In low volume and stable network, the GVRP can reduce the configuration effort. For high volume and high secure request network, the Static VLAN configuration is always preferred.

GVRP Configuration

GVRP Protocol

Port	State	Join Timer	Leave Timer	Leave All Timer
1	Disable	20	60	1000
2	Disable	20	60	1000
3	Disable	20	60	1000
4	Disable	20	60	1000
5	Disable	20	60	1000
6	Disable	20	60	1000
7	Disable	20	60	1000
8	Disable	20	60	1000
9	Disable	20	60	1000
10	Disable	20	60	1000

Note: Timer unit is centiseconds.

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

4.5.4 VLAN Table

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

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.

VLAN Table

VLAN Table

VLAN ID	Name	Status	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	VLAN1	Static	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U
2	V2	Unused	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
3	test	Static	--	--	--	--	--	--	--	--	U	U	U	T	T	T	--	--

Reload

4.5.5 CLI Commands of the VLAN

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

Feature	Command Line
VLAN Port Configuration	
Port Interface Configuration	Switch# conf ter Switch(config)# interface fa5 Switch(config-if)#
VLAN Port PVID	Switch(config-if)# switchport trunk native vlan 2 Set port default vlan id to 2 success
QinQ Tunnel Mode	Switch(config-if)# switchport dot1q-tunnel mode Set the interface as an IEEE 802.1Q tunnel mode
802.1Q Tunnel = access	Switch(config-if)# switchport dot1q-tunnel mode access Set the interface as an access port of IEEE 802.1Q tunnel mode
802.1Q Tunnel Uplink = uplink	uplink Set the interface as an uplink port of IEEE 802.1Q tunnel mode
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 vl-n - success
Egress rule – Tagged	Switch(config-if)# switchport trunk allowed vlan add 2

(for VLAN 2)	
Display – Port Ingress Rule (PVID, Ingress Filtering, Acceptable Frame Type)	<pre>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. Mdx mode is Auto. Medium mode is Copper.</pre>
Display – Port Egress Rule (Egress rule, IP address, status)	<pre>Switch# show running-config ! interface fastethernet1 switchport access vlan 1 switchport access vlan 3 switchport trunk native vlan 2 interface vlan1 ip address 192.168.10.8/24 no shutdown</pre>
QinQ Information – 802.1Q Tunnel	<pre>Switch# show dot1q-tunnel dot1q-tunnel mode por 1 : normal por 2 : normal por 3 : normal por 4 : normal por 5 : access por 6 : uplink por 7 : normal por 8 : normal por 9 : normal port 10 : normal–</pre>
QinQ Information – Show Running	<pre>Switch# show running-config Building configuration... Current configuration: hostname Switch vlan learning independent interface fastethernet5 switchport access vlan add 1-2,10 switchport dot1q-tunnel mode access ! interface fastethernet6 switchport access vlan add 1-2</pre>

	switchport trunk allowed vlan add 10 switchport dot1q-tunnel mode uplink !																
VLAN Configuration																	
Create VLAN (2)	Switch(config)# vlan 2 vlan 2 success Switch(config)# interface vlan 2 Switch(config-if)# <i>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.</i>																
Remove VLAN	Switch(config)# no vlan 2 no vlan success <i>Note: You can only remove the VLAN when the VLAN is in unused mode.</i>																
VLAN Name	Switch(config)# vlan 2 vlan 2 has exists Switch(config-vlan)# name v2 Switch(config-vlan)# no name <i>Note: Use no name to change the name to default name, VLAN VID.</i>																
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 (Active Interface is the Managed 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 <table><thead><tr><th>VLAN Name</th><th>Status</th><th>Trunk Ports</th><th>Access Ports</th></tr></thead><tbody><tr><td>1 VLAN1</td><td>Static</td><td>-</td><td>fa1-7,gi8-10</td></tr><tr><td>2 VLAN2</td><td>Unused</td><td>-</td><td>-</td></tr><tr><td>3 test</td><td>Static</td><td>fa4-7,gi8-10</td><td>fa1-3,fa7,gi8-10</td></tr></tbody></table>	VLAN Name	Status	Trunk Ports	Access Ports	1 VLAN1	Static	-	fa1-7,gi8-10	2 VLAN2	Unused	-	-	3 test	Static	fa4-7,gi8-10	fa1-3,fa7,gi8-10
VLAN Name	Status	Trunk Ports	Access Ports														
1 VLAN1	Static	-	fa1-7,gi8-10														
2 VLAN2	Unused	-	-														
3 test	Static	fa4-7,gi8-10	fa1-3,fa7,gi8-10														
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 join-timer Join timer leave-timer Leave timer leaveall-timer Leaveall timer <10-10000> Switch(config-if)# garp join-timer <10-10000> the timer values Switch(config-if)# garp join-timer 20 Garp join timer value is set to 20 centiseconds on port 2! Switch(config-if)# garp leave-timer 60 Garp leave timer value is set to 60 centiseconds on port 2! Switch(config-if)# garp leaveall-timer 1000 Garp leaveall timer value is set to 1000 centiseconds on port 2! 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 vlan management Management vlan is on vlan 1! Switch# show running-config ! interface vlan1 ip address 192.168.10.17/24 ip igmp no shutdown !

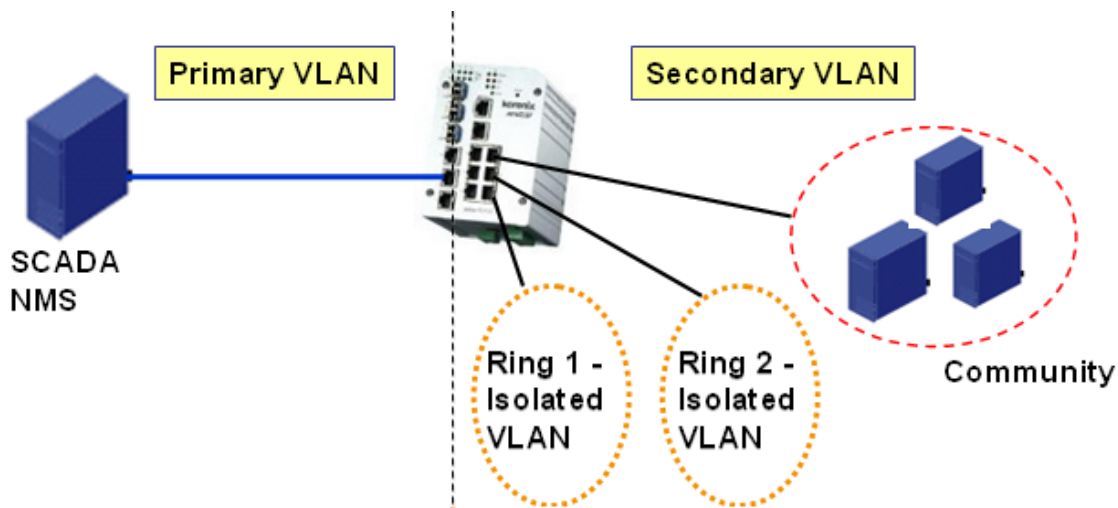
4.6 Private VLAN

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.



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

Following commands are included in this group:

4.6.1 PVLAN Configuration

4.6.2 PVLAN Port Configuration

4.6.3 CLI Commands of the PVLAN

4.6.1 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.

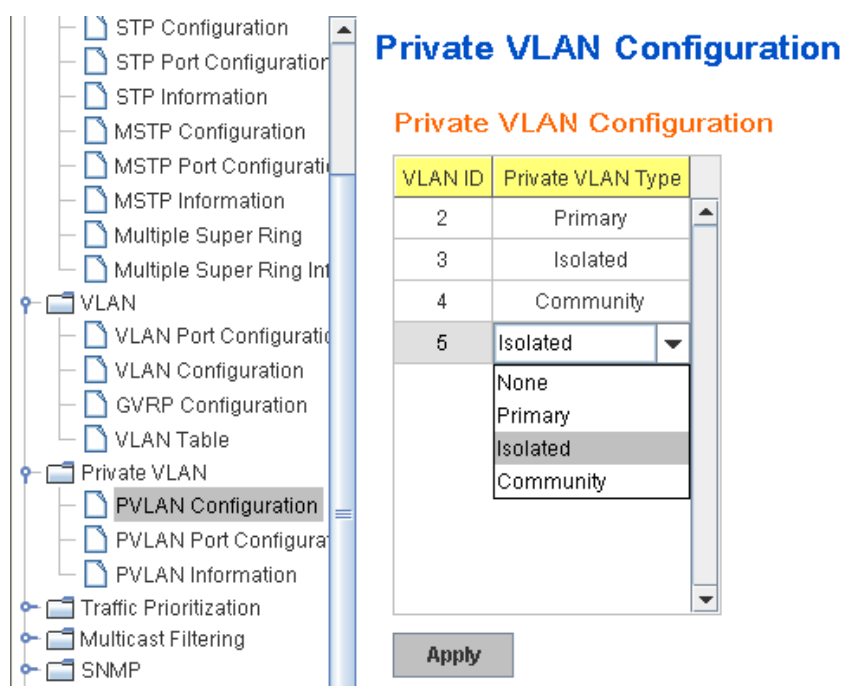
None: The VLAN is Not included in Private VLAN.

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.



4.6.2 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 Configuraion

PVLAN Port T pe :

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

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.

Private VLAN Port Configuration

Port Configuration

Port	PVLAN Port Type	VLAN ID
1	Normal	None
2	Normal	None
3	Normal	None
4	Normal	None
5	Normal	None
6	Normal	None
7	Host	5
8	Host	4
9	Host	3
10	Promiscuous	2

Apply

Private VLAN Association

Secondary VLAN	Primary VLAN
3	2
4	2
5	2

4.6.3 Private VLAN Information

This page allows you to see the Private VLAN information.

Private VLAN Information

Private VLAN Information

Primary VLAN	Secondary VLAN	Secondary VLAN Type	Ports
2	3	Isolated	10,9
2	4	Community	10,8
2	5	Community	10,7

Reload

4.6.4 CLI Command of the PVLAN

Command Lines of the Private VLAN configuration

Feature	Command Line
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 PVLAN Port Type	Switch(config)# interface gi9 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

	<pre> Vlan Type Ports ----- 2 primary gi10 3 isolated gi9 4 community gi8 5 community fa7,gi9 10 primary - </pre>
Host List	<pre> 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 </pre>
Running Config Information	<pre> Switch# show run Building configuration... Current configuration: hostname Switch vlan learning independent ! vlan 1 ! vlan 2 private-vlan primary ! vlan 3 private-vlan isolated ! vlan 4 private-vlan community ! vlan 5 private-vlan community ! </pre>
Private VLAN Type	
Private VLAN Port Information	<pre> 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 </pre>

	<pre>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</pre>
--	---

4.7 Traffic Prioritization

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

JetNet 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.

Following commands are included in this group:

4.7.1 QoS Setting

4.7.2 QoS Priority Mode

4.7.3 CoS-Queue Mapping

4.7.4 DSCP-Queue Mapping

4.7.5 CLI Commands of the Traffic Prioritization

4.7.1 QoS Setting

In QoS setting, you should choose the QoS Priority Mode first, **Port-Based**, **Cos** or **DSCP** modes. Choose the preferred mode and you can configure the next settings in its own configuration pages. The other page of the mode you don't select can't be configured.

Queue Scheduling

The screenshot shows two configuration panels. The left panel, titled 'QoS Setting', has a sub-header 'QoS Priority Mode' and three radio button options: 'Port-based' (selected), 'Cos', and 'DSCP'. The right panel, titled 'Queue Scheduling', has two radio button options: 'Use a Strict Priority scheme' and 'Use Weighted Round Robin scheme' (selected). Below these options is a table with 4 columns representing queues (0, 1, 2, 3) and 2 rows representing 'Queue' and 'Weight'. The 'Queue' row has yellow headers. The 'Weight' row has input fields with dropdown arrows, all currently set to '1'. Below the table is an 'Apply' button.

Queue	0	1	2	3
Weight	1 ▼	1 ▼	1 ▼	1 ▼

You can select the Queue Scheduling rule as follows:

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.

Use Weighted Round Robin scheme. This scheme allows users to assign new weight ratio for each class. The 10 is the highest ratio. The ratio of each class is as below:

$W_x / W_0 + W_1 + W_2 + W_3 + W_4 + W_5 + W_6 + W_7$ (Total volume of Queue 0-7)

4.7.2 Port-based Queue Mapping

Choose the Queue value of each port, the port then has its default priority. The Queue 3 is the highest port-based queue, 0 is the lowest queue. The traffic injected to the port follows the queue level to be forwarded, but the outgoing traffic doesn't bring the queue level to next switch.

Port-based Queue Mapping

Port-based Queue Mapping

Port	Queue
1	0
2	0
3	1
4	2
5	3
6	0
7	0
8	0
9	0
10	0

Apply

After configuration, press **Apply** to enable the settings.

4.7.3 CoS-Queue Mapping

This page is to change CoS values to Physical Queue mapping table. Since the switch fabric of JetNet only supports 4 physical queues, Lowest, Low, Middle and High. Users should therefore assign how to map CoS value to the level of the physical queue.

In JetNet, users can freely assign the mapping table or follow the suggestion of the 802.1p standard. Korenix uses 802.1p suggestion as default values. You can find CoS values 1 and 2 are mapped to physical Queue 0, the lowest queue. CoS values 0 and 3 are mapped to physical Queue 1, the low/normal physical queue. CoS values 4 and 5 are mapped to physical Queue 2, the middle physical queue. CoS values 6 and 7 are mapped to physical Queue 3, the high physical queue.

CoS-Queue Mapping

CoS-Queue Mapping

CoS	0	1	2	3	4	5	6	7
Queue	1	0	0	1	2	2	3	3

Note: Queue 3 is the highest priority queue.

Apply

After configuration, press **Apply** to enable the settings.

4.7.4 DSCP-Queue Mapping

This page is to change DSCP values to Physical Queue mapping table. Since the switch fabric of JetNet only supports 4 physical queues, Lowest, Low, Middle and High. Users should therefore assign how to map DSCP value to the level of the physical queue. In JetNet, users can freely change the mapping table to follow the upper layer 3 switch or routers' DSCP setting.

- JetNet5010G
 - System
 - Basic Setting
 - Port Configuration
 - Network Redundancy
 - VLAN
 - Traffic Prioritization
 - QoS Setting
 - CoS-Queue Mapping
 - DSCP-Queue Mapping**
 - Multicast Filtering
 - SNMP
 - Security
 - Warning
 - Monitor and Diag
 - Device Front Panel
 - Save
 - Logout

Traffic Prioritization

DSCP-Queue Mapping

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

Note: Queue 3 is the highest priority queue.

Apply

After configuration, press **Apply** to enable the settings.

4.7.5 CLI Commands of the Traffic Prioritization

Command Lines of the Traffic Prioritization configuration

Feature	Command Line
QoS Setting	
QoS Type	Switch(config)# qos cos-map Configure CoS to queue mapping dscp-map Configure TOS/DSCP to queue mapping priority Configure priority forwarding queue-sched Configure queue scheduling scheme
Queue Scheduling – Strict Priority	Switch(config)# qos queue-sched sp Strict Priority wrr Weighted Round Robin Switch(config)# qos queue-sched sp The queue scheduling scheme is setting to Strict Priority.
Queue Scheduling – Round Robin	Switch(config)# qos queue-sched rr The queue scheduling scheme is setting to Round Robin. (Note: Not all switch support this feature! Please check the specification first.)

Queue Scheduling - WRR	Switch(config)# qos queue-sched wrr <1-10> Weights for COS queue 0 (queue_id 0) Switch(config)# qos queue-sched wrr 10 <1-10> Weights for COS queue 1 (queue_id 1) Switch(config)# qos queue-sched wrr 1 2 3 4 The queue scheduling scheme is setting to Weighted Round Robin. Assign the ratio for the 4 classes of service.
Port Setting – CoS (Default Port Priority)	Switch(config)# interface fa1 Switch(config-if)# qos priority DEFAULT-PRIORITY Assign an priority (3 highest) Switch(config-if)# qos priority 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.
Display - Queue Scheduling	Switch# show qos queue-sched QoS queue scheduling scheme : Weighted Round Robin COS queue 0 = 1 COS queue 1 = 2 COS queue 2 = 3 COS queue 3 = 4
Display – Port Priority Setting (Port Default Priority)	Switch# show qos port-priority Port Default Priority : Port Priority -----+----- 1 7 2 0 3 0 4 0 5 0 6 0 7 0 8 0 9 0 10 0 11 0 12 0 13 0 14 0 15 0 16 0 17 0 18 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

4.8 Multicast Filtering

For multicast filtering, JetNet Managed Switch uses IGMP Snooping technology. IGMP (Internet Group Management Protocol) is an Internet Protocol that provides a way for 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 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 Snooping** 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.

In this section, Force filtering can determined whether the switch flooding unknown multicast or not.

Following commands are included in this group:

4.8.1 IGMP Snooping

4.8.2 IGMP Query

4.8.3 Unknown Multicast

4.8.4 CLI Commands of the Multicast Filtering

4.8.1 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. JetNet Managed Switch supports IGMP snooping V1/V2/V3 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.

IGMP Snooping

IGMP Snooping Enable ▼

Apply

	VID	IGMP Snooping
<input checked="" type="checkbox"/>	1	Enabled
<input checked="" type="checkbox"/>	2	Enabled
<input type="checkbox"/>	3	Disabled

☐ Select All

Enable

Disable

IGMP Snooping Table: In the table, you can see multicast group IP address, VLAN ID it belongs to, and member ports of the multicast group. JetNet 5018G/5018G v2.0/5012G supports 256 multicast groups. Click on **Reload** to refresh the table.

IGMP Snooping Table

IP Address	VID	1	2	3	4	5	6	7	8	9	10
239.255.255.250	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
239.192.8.0	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Reload

4.8.2 IGMP Query

IGMP Query

IGMP Query on the Management VLAN

Version	Version 1 ▼
Query Interval(s)	125
Query Maximum Response Time(s)	10

Apply

This page allows users to configure **IGMP Query** feature. Since JetNet Managed Switch can only be configured as the member port of the management VLAN, 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 has its 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 IGMP Query selection, you can select V1, V2 or Disable. **V1** means IGMP V1 General Query and **V2** means IGMP V2 General Query.. The query will be forwarded to all multicast groups in the VLAN. **Disable** allows you to disable 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 on **Apply** to apply your configuration.

4.8.3 Unknown Multicast

After enabled IGMP Snooping, the known multicast can be filtered by IGMP Snooping mechanism and forwarded to the member ports of the known multicast groups. The other multicast streams which are not learnt is so-called unknown multicast, the switch decide how to forward them based on the setting of this page.

Send to Query Ports: The unknown multicast will be sent to the Query ports. The Query port means the port received the IGMP Query packets. It is usually the uplink port of the switch.

Send to All Ports: The unknown multicast will be flooded to all ports even they are not the member ports of the groups.

Discard: The unknown multicast will be discarded. Non-member ports will not receive the unknown multicast streams.

This page allows you to decide how to forward the unknown multicast traffic. can be is still flooded to all ports. The **Force filtering** function allows the switch to filter the

Unknown Multicast

Unknown Multicast

☐ Send to Query Ports

☒ Send to All Ports

☐ Discard

Apply

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

4.8.4 GMRP

To enable the GMRP configuration, the Global GMRP Configuration should be enabled first. And all the port interfaces should enable GMRP learning as well. Then the switch exchange the IGMP Table with other switches which is also GMRP-aware devices.

GMRP Configuration

GMRP Protocol Enable ▼

Port	State
1	Disable ▼
2	Disable
3	Enable
4	Disable
5	Disable
6	Disable
7	Disable
8	Disable
9	Disable
10	Disable

Apply

4.8.5 CLI Commands of the Multicast Filtering

Command Lines of the multicast filtering configuration

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 Switch(config)# ip igmp snooping <?> immediate-leave leave group when receive a leave message last-member-query-interval the interval for which the switch waits before source-only-learning updating the table entry vlan Source-Only-Learning Virtual LAN
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

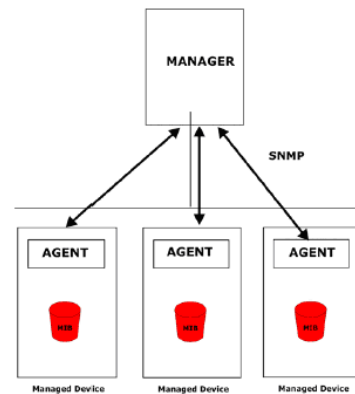
	IGMP snooping is enabled on vlan 2
Disable IGMP Snooping - Global	Switch(config)# no ip igmp snoopin IGMP snooping is disabled globally ok.
Disable IGMP Snooping - VLAN	Switch(config)# no ip igmp snooping vlan 3 IGMP snooping is disabled on VLAN 3.
Display – IGMP Snooping Setting	Switch# sh ip igmp interface 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 immediate-leave is disabled last-member-query-interval is 100 centiseconds Vlan2 is IGMP snooping enabled immediate-leave is disabled last-member-query-interval is 100 centiseconds Vlan3 is IGMP snooping disabled immediate-leave is disabled last-member-query-interval is 100 centiseconds
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 !

Unknown Multicast	
Unknown Multicast - Enable Force filtering (Send to All Ports)	Switch(config)# mac-address-table multicast filtering Filtering unknown multicast addresses ok!
Disable Force filtering (Discard)	Switch(config)# no mac-address-table multicast filtering Flooding unknown multicast addresses ok!
Unknown Multicast – Send to All Ports	Switch(config)# ip igmp snooping source-only-learning

4.9 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. JetNet Full Managed Switch series support SNMP v1 and v2c and V3. (Web Managed Switch doesn't support SNMP feature.)

An 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.



Following commands are included in this group:

4.9.1 SNMP Configuration

4.9.2 SNMPv3 Profile

4.9.3 SNMP Traps

4.9.4 SNMP CLI Commands for SNMP

4.9.1 SNMP Configuration

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

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

With **Read Only** privilege, you only have the ability to read the values of MIB tables. Default community string is Public.

With **Read and Write** privilege, you have the ability to read and set the values of MIB tables. Default community string is Private.

JetNet Managed Switch allows users to assign 4 community strings. Type the community string and select the privilege. Then press **Apply**.

Note: When you first install the device in your network, we highly recommend you to change the community string. Since most SNMP management application uses Public and Private as their default community name, this might be the leakage of the network security.

SNMP

SNMP V1/V2c Community

Community String	Privilege
public	Read Only ▼
private	Read and Write ▼
	Read Only ▼
	Read Only ▼

Apply

4.9.2 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 JetNet Managed Switch and the administrator are encrypted to ensure secure communication.

SNMP V3 Profile

SNMP V3

User Name	
Security Level	Authentication ▼
Authentication Protocol	SHA ▼
Authentication Password	
DES Encryption Password	

Add

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. JetNet Managed Switch 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.

4.9.3 SNMP Traps

SNMP Trap is the notification feature defined by SNMP protocol. All the SNMP management applications can understand such trap information. So you don't need to install new application 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 V2c**. After configured, choose “**Add**”, you can see the trap server profile in below.

The NMS or the trap server you assigned can receive the change of the SNMP pre-defined standard traps and Korenix pre-defined traps. The pre-defined traps can be found in Korenix private MIB.

SNMP Trap

SNMP Trap

Enable

▼

Apply

SNMP Trap Server

Server IP	192.168.10.100
Community	private
Version	<input type="radio"/> V1 <input checked="" type="radio"/> V2c

Add

Trap Server Profile

Server IP	Community	Version
192.168.10.33	public	V1

Remove

Reload

4.9.4 CLI Commands of the SNMP

Command Lines of the SNMP configuration

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

4.10 Security

JetNet Layer 2+ Managed Switch provides several security features for you to secure your connection. The features include Port Security and IP Security.

Following commands are included in this group:

4.10.1 Filter Set (Access Control List)

4.10.2 IEEE 802.1x

4.10.3 CLI Commands of the Security

4.10.1 Filter Set (Access Control List)

The Filter Set is known as Access Control List feature. There are 2 major types, one is MAC Filter, it is also known as Port Security in other JetNet series. It allows user to define the access rule based on the MAC address flexibility. Another one is IP Filter. It includes the IP security known in other JetNet series, IP Standard access list and advanced IP based access lists.

ACE is short of Access Control Entry, user defines the Permit or Deny rule for specific IP/MAC address or IP groups by network mask in each ACE. One ACL may include several ACEs, the system checks the ACEs one after one and forward based on the result. Once the rules conflict, the old entry is selected as the forward rule.

Type the **Name** when select **MAC Filter**, type **ID/Name** when select **IP Filter**. The ID for IP access list is listed as below of the field. Click **Add** to add the rule. Click **Edit** to edit the content for the rule. After configured, click **Apply** to apply all the rules. **Reload** to reload setting. **Remove** to remove one of the entries.

Filter Set

Add Filter

☒ MAC Filter,

☐ IP Filter,

Name:

ID/Name:

Add

(1~99) IP standard access list

(100~199) IP extended access list

(1300~1999) IP standard access list (expanded range)

(2000~2699) IP extended access list (expanded range)

IP Filter ID/Name	Mac Filter Name	Ingress Ports
-	Server_MAC	
-	Server2_MAC	

Apply

Reload

Edit

Remove

MAC Filter (Port Security):

The MAC Filter allows user to define the Access Control List for specific MAC address or a group of MAC addresses.

Filter Rule

Filter Type: MAC Extended

Filter ID/Name:	Server_MAC	Action:	Permit
Source Address:	..	Destination Address:	..
Source Wildcard:	Any	Destination Wildcard:	Any
Egress Port:	--		

Add **Modify** **Remove**

Source / Wildcard	Destination / Wildcard	Action	Egress Port
0012.7700.0000 / 0000.0000.0001	0012.7700.0002 / 0000.0000.0001	Permit	gigabitethernet25

Apply **Reload**

Filter ID/Name: The name for this MAC Filter entry.

Action: **Permit** to permit traffic from specified sources. **Deny** to deny traffic from those sources.

Source/Destination Address: Type the MAC address you want configure, the format is "AABB.CCDD.EEFF". Example: "Source to Destination" is "0012.7700.0000 to 0012.7700.0002".

Source/Destination Wildcard: This command allows user to define single host or a group of hosts based on the wildcard. Some of the allowance examples are as below:

Wildcard	Bit	Number of allowance	Note
Any	1111.1111.1111	All	
Host		1	Only the Source or Destination.
0000.0000.0003	0000.0000.000(00000011)	3	
0000.0000.0007	0000.0000.000(00000111)	7	
0000.0000.000F	0000.0000.000(11111111)	15	
....			

Source Wildcard:	Any
Egress Port:	Any

Host
0000.0000.0001
0000.0000.0003
0000.0000.0007
0000.0000.000F
0000.0000.001F
0000.0000.003F

Egress Port: Bind the MAC Filter rule to specific front port.

Egress Port:	--
--------------	----

fastethernet21
fastethernet22
fastethernet23
fastethernet24
gigabitethernet25
gigabitethernet26
gigabitethernet27
gigabitethernet28

Add
Modify

Once you finish configuring the ACE settings, click on **Add** to apply your configuration. You can see below screen is shown.

Example of the below Entry:

Permit Source MAC "0012.7700.0000" to Destination MAC "0012.7700.0002".

The Permit rule is egress rule and it is bind to Gigabit Ethernet Port 25.

Source / Wildcard	Destination / Wildcard	Action	Egress Port
0012.7700.0000 / 0000.0000.0001	0012.7700.0002 / 0000.0000.0001	Permit	gigabitethernet25

Apply
Reload

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

IP Filter:

Type **ID/Name** when select **IP Filter**. The ID for IP access list is listed as below of the field. You can also type ACL name in this field, it goes to IP Extended mode setting and support both IP Standard and IP Extended mode depend on the setting. Click **Add** to add the rule. Click **Edit** to edit the content for the rule. After configured, click **Apply** to apply all the rules. **Reload** to reload setting. **Remove** to remove one of the entries.

Example:

Filter Set

Add Filter

☐ MAC Filter, Name:

☒ IP Filter, ID/Name:

(1~99) IP standard access list
(100~199) IP extended access list
(1300~1999) IP standard access list (expanded range)
(2000~2699) IP extended access list (expanded range)

IP Filter ID/Name	Mac Filter Name	Ingress Ports
-	Server_MAC	
1	-	
100	-	
1300	-	
2000	-	

IP Standard Access List: This kind of ACL allows user to define filter rules according to the source IP address.

IP Extended Access List: This kind of ACL allows user to define filter rules according to the source IP address, destination IP address, Source TCP/UDP port, destination TCP/UDP port and ICMP type and code.

Click **Edit** to configure the IP Filter Rules.

Filter Rule

Filter Type: IP Extended

Filter ID/Name:	<input type="text" value="100"/>	Action:	<input type="text" value="Permit"/>
Source Address:	<input type="text" value="192.168.10.2"/>	Destination Address:	<input type="text" value="192.168.10.200"/>
Source Wildcard:	<input type="text" value="Host"/>	Destination Wildcard:	<input type="text" value="Host"/>
Protocol:	<input type="text" value="IP"/>		
Source Port:	<input type="text"/>	Destination Port:	<input type="text"/>
Source Port Wildcard:	<input type="text" value="Any"/>	Destination Port Wildcard:	<input type="text" value="Any"/>
ICMP Type:	<input type="text" value="-"/>	ICMP Code:	<input type="text" value="-"/>
Egress Port:	<input type="text" value="fastethernet2"/>		

Src IP	Dst IP	SrcWildc...	DstWildc...	Src Port	Dst Port	Protocol	Action	Egress Port	ICMP Messag...
192.168.10.2	192.168.10.200	Host	Host	-	-	IP	Permit	fastethernet2	-

Filter ID/Name: The ID or the name for this IP Filter entry.

Action: **Permit** to permit traffic from specified sources. **Deny** to deny traffic from those sources.

Source/Destination Address: Type the source/destination IP address you want configure.

Source/Destination Wildcard: This command allows user to define single host or a group of hosts based on the wildcard. Some of the allowance examples are as below:

Source Address:	192.168.10.2
Source Wildcard:	Host
Protocol:	Any
Source Port:	0.0.0.1
Source Port Wildcard:	0.0.0.3
ICMP Type:	0.0.0.7
Egress Port:	0.0.0.15
	0.0.0.31
	0.0.0.63

Wildcard	Bit	Number of allowance	Note
Any	11111111.11111111. 11111111.11111111	All	All IP addresses. Or a mask: 255.255.255.255
Host	0.0.0.0	1	Only the Source or Destination host.
0.0.0.3	0.0.0.(00000011)	3	
0.0.0.7	0.0.0.(00000111)	7	
0.0.0.15	0.0.0.(11111111)	15	
....			

Note: The mask is a wildcard mask: the high-order bits of the mask that are binary zeros determine how many corresponding high-order bits in the IP address are significant. The selected action applies to any source address with these high-order bits.

Protocol: Select a protocol you want associate with the filter. The field includes IP, TCP, UDP or ICMP type.

Destination Port: TCP/UDP port of the Destination Port field.

ICMP Type: The ICMP Protocol Type range from 1 ~ 255.

ICMP Code: The ICMP Protocol Code range from 1 ~ 255.

Egress Port: Bind this Filter to selected egress port.

Click the **Add** button to add the rule to the Filter. Click the **Remove** button to remove the selected rule from Filter. Click the **Modify** button to edit the rule which you selected. Click the **Reload** button to reload the rule table.

Click the **Apply** button to apply the Filter configurations.

Filter Attach

Filter attach/detach

Filter ID/Name: 100 (IP) ▼

Port	<input type="checkbox"/>	IP Filter	MAC Filter
1	<input type="checkbox"/>	--	--
2	<input type="checkbox"/>	--	--
3	<input type="checkbox"/>	--	--
4	<input type="checkbox"/>	--	--
5	<input type="checkbox"/>	--	--
6	<input type="checkbox"/>	--	--
7	<input type="checkbox"/>	--	--
8	<input type="checkbox"/>	--	--
9	<input checked="" type="checkbox"/>	100 ▼	Server_MAC
10	<input type="checkbox"/>	--	--

Apply

Filter Attach (Access Control List)

After configured the ACL filter rules, remember associate this filter with the physical ports. Then the port has the capability to filter traffic/attach based on the packets lost.

Note: Different model may support different access control capability, the above commands are applied to generic Korenix managed switch. But, due to the hardware restriction, some of the above command may not support in your product. Please check the web and CLI of your product.

4.10.2 IEEE 802.1x

4.10.2.1 802.1X 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, JetNet Managed Switch could control which connection is available or not.

802.1x Port-Based Network Access Control Configuration

System Auth Control

Authentication Method

Radius Server

RADIUS Server IP	<input type="text" value="192.168.10.100"/>
Shared Key	<input type="text" value="radius-key"/>
Server Port	<input type="text" value="1812"/>
Accounting Port	<input type="text" value="1813"/>

Secondary Radius Server

RADIUS Server IP	<input type="text"/>
Shared Key	<input type="text"/>
Server Port	<input type="text"/>
Accounting Port	<input type="text"/>

Local Radius User

Username	Password	VID
<input type="text"/>	<input type="text"/>	<input type="text"/>

Local Radius User List

Username	Password	VID
<div></div>		

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

Authentication Method: Radius is a 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 Radius Server.

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.

4.10.2.2 802.1x 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.

802.1x Port-Based Network Access Control Port Configuration

802.1x Port Configuration

Port	Port Control	Reauthentication	Max Request	Guest VLAN	Host Mode	Admin Control Direction
1	Force Authorized	Disable	2	0	Single	Both
2	Force Authorized	Disable	2	0	Single	Both
3	Force Authorized	Disable	2	0	Single	Both
4	Force Authorized	Disable	2	0	Single	Both
5	Force Authorized	Disable	2	0	Single	Both
6	Force Authorized	Disable	2	0	Single	Both

802.1x Timeout Configuration

Port	Re-Auth Period(s)	Quiet Period(s)	Tx Period(s)	Supplicant Timeout(s)	Server Timeout(s)
1	3600	60	30	30	30
2	3600	60	30	30	30
3	3600	60	30	30	30
4	3600	60	30	30	30
5	3600	60	30	30	30
6	3600	60	30	30	30

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 device 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, 1~65535 is available.

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

Sever 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.

4.10.2.3 802.1X Port Status

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

802.1x Port-Based Network Access Control Port Status

Port	Port Control	Authorize Status	Authorized Supplicant	Oper Control Direction
1	Force Authorized	AUTHORIZED	NONE	Both
2	Force Authorized	AUTHORIZED	NONE	Both
3	Force Authorized	AUTHORIZED	NONE	Both
4	Force Authorized	AUTHORIZED	NONE	Both
5	Force Authorized	AUTHORIZED	NONE	Both
6	Force Authorized	AUTHORIZED	NONE	Both
7	Force Authorized	AUTHORIZED	NONE	Both

1
al

Reload

4.10.3 CLI Commands of the Security

Command Lines of the Security configuration

Feature	Command Line
Port Security	
Add MAC access list	Switch(config)# mac access-list extended NAME access-list name Switch(config)# mac access-list extended server1 Switch(config-ext-macl)# permit Specify packets to forward deny Specify packets to reject end End current mode and change to enable mode exit Exit current mode and down to previous mode list Print command list no Negate a command or set its defaults quit Exit current mode and down to previous mode
Add IP Standard access list	Switch(config)# ip access-list extended Extended access-list standard Standard access-list Switch(config)# ip access-list standard <1-99> Standard IP access-list number <1300-1999> Standard IP access-list number (expanded)

	range) WORD Access-list name Switch(config)# ip access-list standard 1 Switch(config-std-acl)# deny Specify packets to reject permit Specify packets to forward end End current mode and change to enable mode exit Exit current mode and down to previous mode list Print command list no Negate a command or set its defaults quit Exit current mode and down to previous mode remark Access list entry comment
Add IP Extended access list	Switch(config)# ip access-list extended <100-199> Extended IP access-list number <2000-2699> Extended IP access-list number (expanded range) WORD access-list name Switch(config)# ip access-list extended 100 Switch(config-ext-acl)# deny Specify packets to reject permit Specify packets to forward end End current mode and down to previous mode exit Exit current mode and down to previous mode list Print command list no Negate a command or set its defaults quit Exit current mode and down to previous mode remark Access list entry comment
Example 1: Edit MAC access list	Switch(config-ext-macl)#permit MACADDR Source MAC address xxxx.xxxx.xxxx any any source MAC address host A single source host Switch(config-ext-macl)#permit host MACADDR Source MAC address xxxx.xxxx.xxxx Switch(config-ext-macl)#permit host 0012.7711.2233 MACADDR Destination MAC address xxxx.xxxx.xxxx any any destination MAC address host A single destination host Switch(config-ext-macl)#permit host 0012.7711.2233 host MACADDR Destination MAC address xxxx.xxxx.xxxx Switch(config-ext-macl)#permit host 0012.7711.2233 host 0011.7711.2234 [IFNAME] Egress interface name Switch(config-ext-macl)#permit host 0012.7711.2233 host 0011.7711.2234 gi25 <i>Note: MAC Rule: Permit/Deny wildcard Source_MAC wildcard Dest_MAC Egress_Interface</i>
Example 1: Edit IP Extended access list	Switch(config)# ip access-list extended 100 Switch(config-ext-acl)#permit ip Any Internet Protocol tcp Transmission Control Protocol udp User Datagram Protocol icmp Internet Control Message Protocol Switch(config-ext-acl)#permit ip A.B.C.D Source address any Any source host host A single source host

	Switch(config-ext-acl)#permit ip 192.168.10.1 A.B.C.D Source wildcard bits Switch(config-ext-acl)#permit ip 192.168.10.1 0.0.0.1 A.B.C.D Destination address any Any destination host host A single destination host Switch(config-ext-acl)#permit ip 192.168.10.1 0.0.0.1 192.168.10.100 0.0.0.1 [IFNAME] Egress interface name Switch(config-ext-acl)#permit ip 192.168.10.1 0.0.0.1 192.168.10.100 0.0.0.1 gi17 <i>Note: Follow the below rule to configure ip extended access list.</i> <i>IP Rule: Permit/Deny Source_IP wildcard Dest_IP wildcard</i> <i>Egress_Interface</i> <i>TCP Rule: Permit/Deny tcp Source_IP wildcard Dest_IP wildcard eq</i> <i>Given_Port_Number Egress_Interface</i> <i>UDP Rule: Permit/Deny udp Source_IP wildcard Dest_IP wildcard</i> <i>eq Given_Port_Number Egress_Interface</i> <i>ICMP Rule: Permit/Deny icmp Source_IP wildcard Dest_IP wildcard</i> <i>ICMP_Message_Type ICMP_Message_Code Egress_Interface</i>
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! <i>Note 1: Rule: Add the static MAC, VLAN and Port binding first, then enable the port security to stop new MAC learning.</i> <i>Note 2: Not all the model support this feature, check the product detail specification.</i>
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
802.1x (short of dot1x)	
Enable	Switch(config)# dot1x system-auth-control
Disable	The Port-Based Network Access Control is globally enabled Switch(config)# no dot1x system-auth-control The Port-Based Network Access Control is globally disabled
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 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
Display (802.x is short of dot1x)	Switch# show dot1x <cr> all Show Dot1x information for all interface authentic-method Dot1x authentic-method interface Interface name radius Remote Access Dial-In User Service statistics Interface name username User Name in local radius database Switch# show dot1x <cr> = Switch# show dot1x all You can check all dot1x information for all interfaces. Click Ctrl + C to exit the display Switch# show dot1x interface fa1 Supplicant MAC ADDR <NONE> STATE-MACHINE AM status : FORCE_AUTH BM status : IDLE PortStatus : AUTHORIZED PortControl : Force Authorized Reauthentication : Disable MaxReq : 2 ReAuthPeriod : 3600 Seconds QuietPeriod : 60 Seconds TxPeriod : 30 Seconds SupplicantTimeout : 30 Seconds ServerTimeout : 30 Seconds GuestVlan : 0 HostMode : Single operControlledDirections : Both adminControlledDirections : Both Switch# show dot1x radius RADIUS Server IP : 192.168.10.100 RADIUS Server Key : radius-key RADIUS Server Port : 1812 RADIUS Accounting Port : 1813

	Secondary RADIUS Server IP : N/A Secondary RADIUS Server Key : N/A Secondary RADIUS Server Port : N/A Secondary RADIUS Accounting Port : N/A Switch# show dot1x username 802.1x Local User List Username : orwell , Password : * , VLAN ID : 1
--	--

4.11 Warning

JetNet Managed Switch provides several types of Warning features for you to remote monitor the status of end devices or the change of your network. The features include Fault Relay, System Log and SMTP E-mail Alert.

Following commands are included in this group:

4.11.1 Fault Relay

4.11.2 Event Selection

4.11.3 Syslog Configuration

4.11.4 SMTP Configuration

4.11.5 CLI Commands

4.11.1 Fault Relay

JetNet 4518/5012G/5018G/5018G v2.0 provides 2 digital outputs, also known as Relay Output. The relay contacts are energized (open) for normal operation and will close under fault conditions. Fault conditions include Dry Output, Power Failure, Ethernet port Link Failure, Ping Failure and Super Ring Topology Change. You can configure these settings in this Fault Relay Setting. Each Relay can be assigned 1 fault condition.

Relay 1: Click on checkbox of the Relay 1, then select the Event Type and its parameters.

Relay 2: Click on checkbox of the Relay 2, then select the Event Type and its parameters.

Event Type: Dry Output, Power Failure, Link Failure, Ping Failure and Super Ring Failure. Each event type has its own parameters. You should also configure them. Currently, each Relay can has one event type.

Event Type: **Dry Output**

On Period (Sec): Type the period time to turn on Relay Output. Available range of a period is 0-4294967295 seconds.

Off Period (Sec): Type the period time to turn off Relay Output. Available range of a period is 0-4294967295 seconds.

How to configure: Type turn-on period and turn-off period when the time is reached, the system will turn on or off the Relay Output. If you connect DO to DI of the other terminal unit, the setting can help you to change DI state. If you connect DO to the power set of other terminal units, this setting can help you to turn on or off the unit.

<input checked="" type="checkbox"/> Relay 1	
Event Type	Dry Output ▼
On Period(Sec)	5
Off Period(Sec)	10

Relay turn on for 5 seconds then off for 10 seconds

How to turn On/Off the other device: Type "1" into the "On period" field and "0" into "Off Period" field and apply the setting, then it t will be trigger to form as a close circuit.

To turn off the relay, just type "0" into the "On period" field and "1" into "Off Period" field and apply the setting, the relay will be trigger to form as a open circuit.

This function is also available in CLI, SNMP management interface. See the following setting.

<input checked="" type="checkbox"/> Relay 1		<input checked="" type="checkbox"/> Relay 1	
Event Type	Dry Output	Event Type	Dry Output
On Period(Sec)	1	On Period(Sec)	0
Off Period(Sec)	0	Off Period(Sec)	1

Turn on the relay output

Turn off the relay output

Event Type: **Power Failure**

Power ID: Select Power DC 1, Power DC2 or Any you want to monitor. When the power you selected is shut down or broken, the system will short Relay Out and light the DO LED.

<input checked="" type="checkbox"/> Relay 1	
Event Type	Power Failure
Power ID	Power DC1

Event Type: **Like Failure**

Link: Select the port ID you want to monitor.

How to configure: Select the checkbox of the Ethernet ports you want to monitor. You can select one or multiple ports. When the selected ports are linked down or broken, the system will short Relay Output and light the DO LED.

Fault Relay Setting

<input checked="" type="checkbox"/> Relay 1										
Event Type	Link Failure									
Link	1	2	3	4	5	6	7	8	9	10
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	11	12	13	14	15	16	17	18		
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		

Event Type: **Ping Failure**

IP Address: IP address of the target device you want to ping.

Reset Time (Sec): Waiting time to short the relay output.

Hold Time (Sec): Waiting time to ping the target device for the duration of remote device boot

<input checked="" type="checkbox"/> Relay 1	
Event Type	Ping Failure ▼
IP Address	192.168.10.2
Reset Time(Sec)	5
Hold Time(Sec)	50

How to configure: After selecting Ping Failure event type, the system will turn Relay Output to short state and continuously ping the target device. When the ping failure occurred, the switch will turn the Relay Output to open state for a period of Reset Time.

After the Reset Time timeout, the system will turn the Relay Output to close state. After the Hold Time timer is timeout, the switch system will start ping the target device.

Ex: Reset Time is 5 sec, Hold Time is 50 sec.

If the ping failure occurred, the switch system will turn Relay output to open state to emulate power switch off for 5 sec periods. After Reset Time timeout, the Switch system will start ping target device after 50 sec periods. The period time is for target device system booting. During the period, the switch system will not ping target device until Hold Time is timeout.

Event Type: **Super Ring Failure**

Select Super Ring Failure. When the Rapid Super Ring topology is changed, the system will short Relay Out and lengthen DO LED.

<input checked="" type="checkbox"/> Relay 1	
Event Type	Super Ring Failure ▼

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

4.11.2 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 a specific ports

System Event	Warning Event is sent when.....
Device Cold Start	Device starts by power on.
Device Warm Start	Device starts by software reboot.

Authentication Failure	An incorrect password, SNMP Community String is entered.
Time Synchronize Failure	Accessing to NTP Server is failure.
Power 1 Failure	Selected Power ID is failure.
Power 2 Failure	Selected Power ID 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.
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	Either of Link Up or Link Down

Warning - Event Selection

System Event Selection

- | | |
|---|---|
| <input type="checkbox"/> Device Cold Start | <input type="checkbox"/> Device Warm Start |
| <input type="checkbox"/> Authentication Failure | <input type="checkbox"/> Time Synchronize Failure |
| <input type="checkbox"/> Power 1 Failure | <input type="checkbox"/> Power 2 Failure |
| <input type="checkbox"/> Fault Relay | <input type="checkbox"/> Super Ring Topology Change |

Port Event Selection

Port	Link State
1	Disable
2	Disable
3	Link Down
4	Link Up
5	Both
6	Disable
7	Disable
8	Disable
9	Disable
10	Disable

Apply

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

4.11.3 SysLog Configuration

System Log is useful to provide system administrator locally or remotely monitor switch events history. There are 2 System Log modes provided by JetNet Managed Switch, local mode and remote mode.

Local Mode: In this mode, JetNet Managed Switch will print the occurred events selected in the Event Selection page to System Log table of JetNet Managed Switch. You can monitor the system logs in [Monitor and Diag] / [Event Log] page.

Remote Mode: The remote mode is also known as Server mode in JetNet 4500 series. In this mode, you should assign the IP address of the System Log server. JetNet Managed Switch will send the occurred events selected in Event Selection page to System Log server you assigned.

Both: Above 2 modes can be enabled at the same time.

Warning - SysLog Configuration

Syslog Mode	Both
Remote IP Address	Disable Local Remote Both

Note: When enabled Local or Remote mode, you can monitor the system logs in the [Monitor and Diag] / [Event Log] page.

Apply

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

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

4.11.4 SMTP Configuration

JetNet Managed SwitchG supports E-mail Warning feature. The switch will send the occurred events to remote E-mail server. The receiver can then receive notification by E-mail. The E-mail warning is conformed to SMTP standard.

This page allows you to enable E-mail Alert, assign the SMTP Server IP, Sender E-mail, and Receiver E-mail. If SMTP server requests you to authorize first, you can also set up the username and password in this page.

Warning - SMTP Configuration

E-mail Alert

Enable ▼

SMTP Configuration

SMTP Server IP	192.168.10.1
Mail Account	admin@korenix.com
<input type="checkbox"/> Authentication	
User Name	
Password	
Confirm Password	
Rcpt E-mail Address 1	korecare@korenix.com
Rcpt E-mail Address 2	
Rcpt E-mail Address 3	
Rcpt E-mail Address 4	

Apply

Field	Description
SMTP Server IP Address	Enter the IP address of the email Server
Authentication	Click on 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 JetNet	
Rcpt E-mail Address 1	The first email address to receive email alert from JetNet (Max. 40 characters)
Rcpt E-mail Address 2	The second email address to receive email alert from JetNet (Max. 40 characters)
Rcpt E-mail Address 3	The third email address to receive email alert from JetNet (Max. 40 characters)
Rcpt E-mail Address 4	The fourth email address to receive email alert from JetNet (Max. 40 characters)

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

4.11.5 CLI Commands

Command Lines of the Warning configuration

Feature	Command Line
Relay Output	
Relay Output	Switch(config)# relay 1 di DI state (Not support in JetNet 4518/ 5012G/5018G/5018G v2.0) dry dry output ping ping failure port port link failure power power failure ring super ring failure Note: Select Relay 1 or 2 first, then select the event types.
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 <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	Switch(config)# relay 1 power <1-2> power id any Anyone power failure asserts relay Switch(config)# relay 1 power 1
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

	authentication Authentication failure event fault-relay Switch fault relay event power Switch power failure event super-ring Switch super ring topology change event time-sync Switch time synchronize 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 [IFLIST] Interface list, ex: fa1,fa3-5,gi17-18 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
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@korenix.com Switch(config)# smtp-server server 192.168.10.100 admin@korenix.com SMTP Email Alert set Server: 192.168.10.100, Account: admin@korenix.com ok.
Receiver mail	Switch(config)# smtp-server receipt 1 korecare@korenix.com SMTP Email Alert set receipt 1: korecare@korenix.com 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@korenix.com Authentication: Enabled Username: admin, Password: admin SMTP Email Alert Receipt: Receipt 1: korecare@korenix.com

	Receipt 2: Receipt 3: Receipt 4:
--	--

4.12 Monitor and Diag

JetNet Managed Switch provides several types of features for you to monitor the status of the switch or diagnostic for you to check the problem when encountering problems related to the switch. The features include MAC Address Table, Port Statistics, Port Mirror, Event Log and Ping.

Following commands are included in this group:

4.12.1 MAC Address Table

4.12.2 Port Statistics

4.12.3 Port Mirror

4.12.4 Event Log

4.12.5 Topology Discovery (LLDP)

4.12.6 Ping

4.12.7 CLI Commands of the Monitor and Diag

4.12.1 MAC Address Table

JetNet Managed Switch provides up to 4/8/16K entries in MAC Address Table. In 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 on **Apply** to change the value.

Aging Time (Sec)

Each switch fabric has limit size to write the learnt MAC address. To save more entries for new MAC address, the switch fabric will age out non-used MAC address entry per Aging Time timeout. The default Aging Time is 300 seconds. The Aging Time can be modified in this page.

Static Unicast MAC Address

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

MAC Address Table

In this MAC Address Table, you can see all the MAC Addresses learnt 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 address by the packet types and port.

Packet Types: **Management Unicast** means MAC address of the switch. It belongs to CPU port only. **Static Unicast** MAC address can be added and deleted. **Dynamic Unicast** MAC is MAC address learnt by the switch Fabric. **Static Multicast** can be added by CLI and can be deleted by Web and CLI. **Dynamic Multicast** will appear after you enabled IGMP and the switch learnt IGMP report.

Click on **Remove** to remove the static Unicast/Multicast MAC address. Click on **Reload** to refresh the table. New learnt Unicast/Multicast MAC address will be updated to MAC address table.

MAC Address Table

Aging Time (Sec)

300

Apply

Static Unicast MAC Address

MAC Address	VID	Port
<input type="text"/>	<input type="text"/>	Port 1 ▾

Add

MAC Address Table

All ▾

MAC Address	Address Type	VID	1	2	3	4	5	6	7	8	9	10
000f.b079.ca3b	Dynamic Unicast	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0012.7701.0386	Dynamic Unicast	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0012.7710.0101	Static Unicast	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0012.7710.0102	Static Unicast	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0012.77ff.0100	Management Unicast	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0100.5e40.0800	fa6 Multicast	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0100.5e7f.ffff	fa4,fa6 Multicast	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Remove

Reload

4.12.2 Port Statistics

In this page, you can view operation statistics for each port. The statistics that can be viewed include Link Type, Link State, Rx Good, Rx Bad, Rx Abort, Tx Good, Tx Bad and Collision. Rx means the received packet while Tx means the transmitted packets.

Note: If you see many Bad, Abort or Collision counts increased, that may mean your network cable is not connected well, the network performance of the port is poor...etc. Please check your network cable, Network Interface Card of the connected device, the network application, or reallocate the network traffic...etc.

Click on **Clear Selected** to reinitialize the counts of the selected ports, and **Clear All** to reinitialize the counts of all ports. Click on **Reload** to refresh the counts.

Port Statistics

Port	Type	Link	State	Rx Good	Rx Bad	Rx Abort	Tx Good	Tx Bad	Collision
1	100TX	Down	Enable	0	0	0	0	0	0
2	100TX	Down	Enable	10	0	0	11	0	0
3	100TX	Down	Enable	0	0	0	0	0	0
4	100TX	Up	Enable	2131	0	0	2452	0	0
5	100TX	Down	Enable	0	0	0	0	0	0
6	100TX	Down	Enable	4884	1	2	5919	0	0
7	100TX	Up	Enable	54	0	0	2742	0	0
8	1000TX	Down	Enable	0	0	0	0	0	0
9	1000TX	Down	Enable	0	0	0	0	0	0
10	1000TX	Down	Enable	0	0	0	0	0	0

Clear Selected

Clear All

Reload

4.12.3 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 single port or any combination of ports, you can monitor them in Rx only, TX only or both RX and TX. Click on checkbox of the RX, Tx 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 of the destination ports can be selected. A network administrator would typically connect a LAN analyzer or Netxray device to this port.

Port Mirroring

Port Mirror Mode

Port Selection

Port	Source Port		Destination Port
	Rx	Tx	
1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="radio"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="radio"/>
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/>
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/>
5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/>
6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/>
7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/>
8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/>
9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/>
10	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/>
11	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/>
12	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/>

Apply

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

4.12.4 Event Log

In the 4.10.3, we have introduced System Log feature. When System Log Local mode is selected, JetNet Managed Switch will record occurred events in local log table. This page shows this log table. The entry includes the index, occurred data and time and content of the events.

Click on **Clear** to clear the entries. Click on **Reload** to refresh the table.

System Event Logs

Index	Date	Time	Event Log
1	Jan 1	02:50:53	Event: Link 4 Up.
2	Jan 1	02:50:51	Event: Link 5 Down.
3	Jan 1	02:50:50	Event: Link 5 Up.
4	Jan 1	02:50:47	Event: Link 4 Down.

Clear

Reload

4.12.5 Topology Discovery (LLDP)

The Managed Switch supports 802.1AB Link Layer Discovery Protocol, thus the LLDP aware Switch can be discovered by the Network Management System which support LLDP discovery. With LLDP supported, the 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 learnt from the connected devices.

LLDP: Enable/Disable the LLDP topology discovery information.

LLDP Configuration: To configure the related timer of LLDP.

LLDP timer: The LLDPDP interval, the LLDP information is send per LLDP timer. The default value is 30 seconds.

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

LLDP Port State: Display the neighbor information learnt from the connected interface.

Topology Discovery

LLDP

Enable ▼

LLDP Configuration

LLDP timer	30
LLDP hold time	120

LLDP Port State

Local Port	Neighbor ID	Neighbor IP	Neighbor VID
fa15	00:12:77:60:2e:0d	192.168.10.10	1

Apply

4.12.6 Ping Utility

This page provides **Ping Utility** for users to ping remote device and check whether the device is alive or not. Type **Target IP** address of the target device and click on **Start** to start the ping. After few seconds, you can see the result in the **Result** field.

Ping Utility

Ping

Target IP 192.168.10.33

Start

Result

```
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
```

4.12.7 CLI Commands of the Monitor and Diag

Command Lines of the Monitor and Diag configuration

Feature	Command Line																																							
MAC Address Table																																								
Ageing Time	Switch(config)# mac-address-table aging-time 350 mac-address-table aging-time set ok! <i>Note: 350 is the new ageing timeout value.</i>																																							
Add Static Unicast MAC address	Switch(config)# mac-address-table static 0012.7701.0101 vlan 1 interface fastethernet7 mac-address-table ucast static set ok! Note: rule: mac-address-table static MAC_address VLAN VID interface interface_name																																							
Add Multicast MAC address	Switch(config)# mac-address-table multicast 0100.5e01.0101 vlan 1 interface fa6-7 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 ***** <table><thead><tr><th>Destination Address</th><th>Address Type</th><th>Vlan</th><th>Destination Port</th></tr></thead><tbody><tr><td>000f.b079.ca3b</td><td>Dynamic</td><td>1</td><td>fa4</td></tr><tr><td>0012.7701.0386</td><td>Dynamic</td><td>1</td><td>fa7</td></tr><tr><td>0012.7710.0101</td><td>Static</td><td>1</td><td>fa7</td></tr><tr><td>0012.7710.0102</td><td>Static</td><td>1</td><td>fa7</td></tr><tr><td>0012.77ff.0100</td><td>Management</td><td>1</td><td></td></tr></tbody></table> ***** MULTICAST MAC ADDRESS ***** <table><thead><tr><th>Vlan</th><th>Mac Address</th><th>COS</th><th>Status</th><th>Ports</th></tr></thead><tbody><tr><td>1</td><td>0100.5e40.0800</td><td>0</td><td>fa6</td><td></td></tr><tr><td>1</td><td>0100.5e7f.ffa</td><td>0</td><td>fa4,fa6</td><td></td></tr></tbody></table>	Destination Address	Address Type	Vlan	Destination Port	000f.b079.ca3b	Dynamic	1	fa4	0012.7701.0386	Dynamic	1	fa7	0012.7710.0101	Static	1	fa7	0012.7710.0102	Static	1	fa7	0012.77ff.0100	Management	1		Vlan	Mac Address	COS	Status	Ports	1	0100.5e40.0800	0	fa6		1	0100.5e7f.ffa	0	fa4,fa6	
Destination Address	Address Type	Vlan	Destination Port																																					
000f.b079.ca3b	Dynamic	1	fa4																																					
0012.7701.0386	Dynamic	1	fa7																																					
0012.7710.0101	Static	1	fa7																																					
0012.7710.0102	Static	1	fa7																																					
0012.77ff.0100	Management	1																																						
Vlan	Mac Address	COS	Status	Ports																																				
1	0100.5e40.0800	0	fa6																																					
1	0100.5e7f.ffa	0	fa4,fa6																																					
Show MAC Address Table – Dynamic Learnt MAC addresses	Switch# show mac-address-table dynamic <table><thead><tr><th>Destination Address</th><th>Address Type</th><th>Vlan</th><th>Destination Port</th></tr></thead><tbody><tr><td>000f.b079.ca3b</td><td>Dynamic</td><td>1</td><td>fa4</td></tr><tr><td>0012.7701.0386</td><td>Dynamic</td><td>1</td><td>fa7</td></tr></tbody></table>	Destination Address	Address Type	Vlan	Destination Port	000f.b079.ca3b	Dynamic	1	fa4	0012.7701.0386	Dynamic	1	fa7																											
Destination Address	Address Type	Vlan	Destination Port																																					
000f.b079.ca3b	Dynamic	1	fa4																																					
0012.7701.0386	Dynamic	1	fa7																																					
Show MAC Address Table – Multicast MAC addresses	Switch# show mac-address-table multicast <table><thead><tr><th>Vlan</th><th>Mac Address</th><th>COS</th><th>Status</th><th>Ports</th></tr></thead><tbody><tr><td>1</td><td>0100.5e40.0800</td><td>0</td><td>fa6-7</td><td></td></tr><tr><td>1</td><td>0100.5e7f.ffa</td><td>0</td><td>fa4,fa6-7</td><td></td></tr></tbody></table>	Vlan	Mac Address	COS	Status	Ports	1	0100.5e40.0800	0	fa6-7		1	0100.5e7f.ffa	0	fa4,fa6-7																									
Vlan	Mac Address	COS	Status	Ports																																				
1	0100.5e40.0800	0	fa6-7																																					
1	0100.5e7f.ffa	0	fa4,fa6-7																																					
Show MAC Address Table – Static MAC addresses	Switch# show mac-address-table static <table><thead><tr><th>Destination Address</th><th>Address Type</th><th>Vlan</th><th>Destination Port</th></tr></thead><tbody><tr><td>0012.7710.0101</td><td>Static</td><td>1</td><td>fa7</td></tr><tr><td>0012.7710.0102</td><td>Static</td><td>1</td><td>fa7</td></tr></tbody></table>	Destination Address	Address Type	Vlan	Destination Port	0012.7710.0101	Static	1	fa7	0012.7710.0102	Static	1	fa7																											
Destination Address	Address Type	Vlan	Destination Port																																					
0012.7710.0101	Static	1	fa7																																					
0012.7710.0102	Static	1	fa7																																					
Show Aging timeout time	Switch# show mac-address-table aging-time the mac-address-table aging-time is 300 sec.																																							

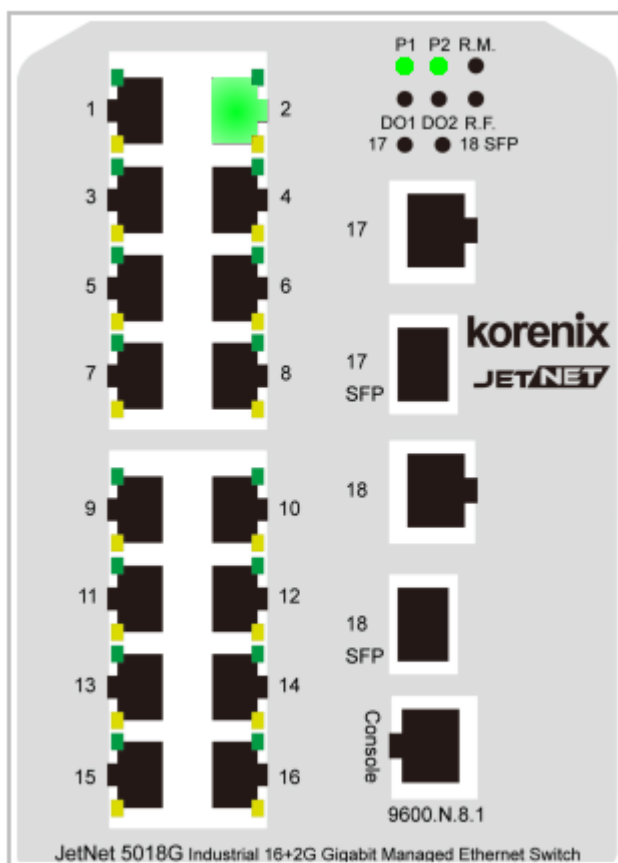
Port Statistics	
Port Statistics	Switch# show rmon statistics fa4 (select interface) Interface fastethernet4 is enable connected, which has Inbound: Good Octets: 178792, Bad Octets: 0 Unicast: 598, Broadcast: 1764, Multicast: 160 Pause: 0, Undersize: 0, Fragments: 0 Oversize: 0, Jabbers: 0, Disacrd: 0 Filtered: 0, RxError: 0, FCSError: 0 Outbound: Good Octets: 330500 Unicast: 602, Broadcast: 1, Multicast: 2261 Pause: 0, Deferred: 0, Collisions: 0 SingleCollision: 0, MultipleCollision: 0 ExcessiveCollision: 0, LateCollision: 0 Filtered: 0, FCSError: 0 Number of frames received and transmitted with a length of: 64: 2388, 65to127: 142, 128to255: 11 256to511: 64, 512to1023: 10, 1024toMaxSize: 42
Port Mirroring	
Enable Port Mirror	Switch(config)# mirror en Mirror set enable ok.
Disable Port Mirror	Switch(config)# mirror disable Mirror set disable ok.
Select Source Port	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.
Select Destination Port	Switch(config)# mirror destination fa6 both Mirror destination fa6 both set ok
Display	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,
Event Log	
Display	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.
Topology Discovery (LLDP)	
Enable LLDP	Switch(config)# lldp holdtime Specify the holdtime of LLDP in seconds run Enable LLDP timer Set the transmission frequency of LLDP in seconds Switch(config)# lldp run LLDP is enabled!
Change LLDP timer	Switch(config)# lldp holdtime <10-255> Valid range is 10~255 Switch(config)# lldp timer <5-254> Valid range is 5~254

Ping	
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

4.12 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, R.M. and Font Ports. Below is the example of JetNet 5018G. Different model has its own front panel display.

Feature	On / Link UP	Off / Link Down	Other
Power 1 (P1)	Green	Black	
Power 2 (P2)	Green	Black	
Digital Output 1(DO1)	Red	Black	
Digital Output 2(DO2)	Red	Black	
Ring Master(R.M.)	Green	Black	
Ring Fail(R.F.)	Red	Black	
Fast Ethernet	Green	Black	(Port 1-16)
Gigabit Ethernet	Green	Black	(Port 17,18)
SFP	Green	Black	Gray: Plugged but not link up yet.



Example of the JetNet 5018G front panel.

Note: No CLI command for this feature.

4.13 Save to Flash

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

Save to Flash

Note: This command will permanently save the current configuration to flash.

Save to Flash

Command Lines:

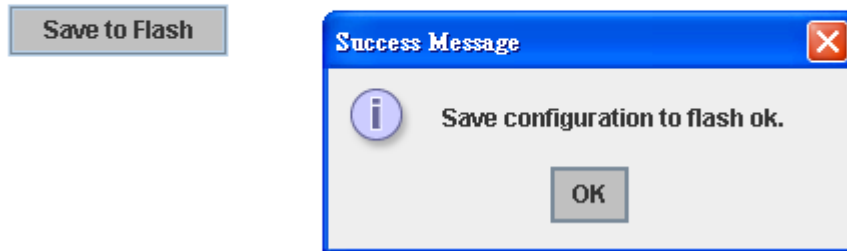
Feature	Command Line
Save	SWITCH# write Building Configuration... [OK] Switch# copy running-config startup-config Building Configuration... [OK]

4.14 Logout

The switch provides 2 logout methods. The web connection will be logged out if you don't input any command after 30 seconds. The Logout command allows you to manually logout the web connection. Click on **Yes** to logout, **No** to go back the configuration page.

Save to Flash

Note: This command will permanently save the current configuration to flash.



Command Lines:

Feature	Command Line
Logout	SWITCH> exit
	SWITCH# exit

5 Appendix

5.1 Korenix SFP family

Korenix certificated many types of SFP transceiver. These certificated SFP transceivers can be identified by JetNet Managed Switch and displayed in the UI. The SFP transceivers we certificated can meet up the industrial critical environment needs. We recommend you to use Korenix certificated SFP transceivers when you constructing your network.

Korenix will keep on certificating and updating the certificated SFP transceivers in Korenix web site and purchase list. You can refer to the web site to get the latest information about SFP transceivers.

Note: Poor SFP transceivers may result in poor network performance or can't meet up claimed distance or temperature.

Model Name	Spec
SFPGSX	1000Base-SX multi-mode SFP transceiver,550m, -10~70°C
SFPGSX-w	1000Base-SX multi-mode SFP transceiver, 550m, wide operating temperature, -40~85°C
SFPGSX2	1000Base-SX plus multi-mode SFP transceiver, 2Km, -10~70°C
SFPGSX2-w	1000Base-SX plus multi-mode SFP transceiver, 2Km,wide operating temperature, -10~70°C
SFPGLX10	1000Base-LX single-mode SFP transceiver 10Km, -10~70°C
SFPGLX10-w	1000Base-LX single-mode SFP transceiver, 10Km, wide operating temperature, -40~85°C
SFPGLHX30	1000Base-LHX single-mode SFP transceiver,30Km, -10~70°C
SFPGLHX30-w	1000Base-LHX single-mode SFP transceiver, 30Km, wide operating temperature, -40~85°C
SFPGXD50	1000Base-XD single-mode SFP transceiver, 50Km, -10~70°C
SFPGXD50-w	1000Base-XD single-mode SFP transceiver, 50Km, wide operating temperature, -40~85°C
SFP Gigabit BIDI/WDM	
SFPGLX10B13	1000Base-LX BIDI single-mode transceiver, 10km, TX:1310nm,

RX: 1550nm, -10~70°C

SFPGLX10B13-W	1000Base-LX BIDI single-mode transceiver 10km, TX:1310nm, RX: 1550nm, -40~85°
SFPGLX10B15	1000Base-LX BIDI single-mode transceiver 10km, TX:1550nm, RX: 1310nm, -10~70°C
SFPGLX10B15-W	1000Base-LX BIDI single-mode transceiver 10km, TX:1550nm, RX: 1310nm, -40~85°C
SFPGLX20B13	1000Base-LX BIDI single-mode transceiver 20km, TX:1310nm, RX: 1550nm, -10~70°C
SFPGLX20B13-W	1000Base-LX BIDI single-mode transceiver 20km, TX:1310nm, RX: 1550nm, -40~85°C
SFPGLX20B15	1000Base-LX BIDI single-mode transceiver 20km, TX:1550nm, RX: 1310nm, -10~70°C
SFPGLX20B15-W	1000Base-LX BIDI single-mode transceiver 20km, TX:1550nm, RX: 1310nm, -40~85°C
SFPGLX40B13	1000Base-LX BIDI single-mode transceiver 40km, TX:1310nm, RX: 1550nm, -10~70°C
SFPGLX40B13-W	1000Base-LX BIDI single-mode transceiver 40km, TX:1310nm, RX: 1550nm, -40~85°C
SFPGLX40B15	1000Base-LX BIDI single-mode transceiver 40km, TX:1550nm, RX: 1310nm, -10~70°C
SFPGLX40B15-W	1000Base-LX BIDI single-mode transceiver 40km, TX:1550nm, RX: 1310nm, -40~85°C
SFPGLX60B13	1000Base-LX BIDI single-mode transceiver 60km, TX:1310nm, RX: 1550nm, -10~70°C
SFPGLX60B13-W	1000Base-LX BIDI single-mode transceiver 60km, TX:1310nm, RX: 1550nm, -40~85°C
SFPGLX60B15	1000Base-LX BIDI single-mode transceiver 60km, TX:1550nm, RX: 1310nm, -10~70°C

5.2 Korenix Private MIB

Korenix provides many standard MIBs for users to configure or monitor the switch's configuration by SNMP. But, since some commands can't be found in standard MIB, Korenix provides Private MIB to meet up the need. Compile the private MIB file by your SNMP tool. You can then use it. Private MIB can be found in product CD or downloaded from Korenix Web site.

Private MIB tree is similar to the web tree. This is easier to understand and use. If you are not familiar with standard MIB, you can directly use private MIB to manage /monitor the switch, no need to learn or find where the OIDs of the commands are.

The path of the JetNet 5012G is **1.3.6.1.4.1.24062.2.2.12**

The path of the JetNet 5018G is **1.3.6.1.4.1.24062.2.2.7**

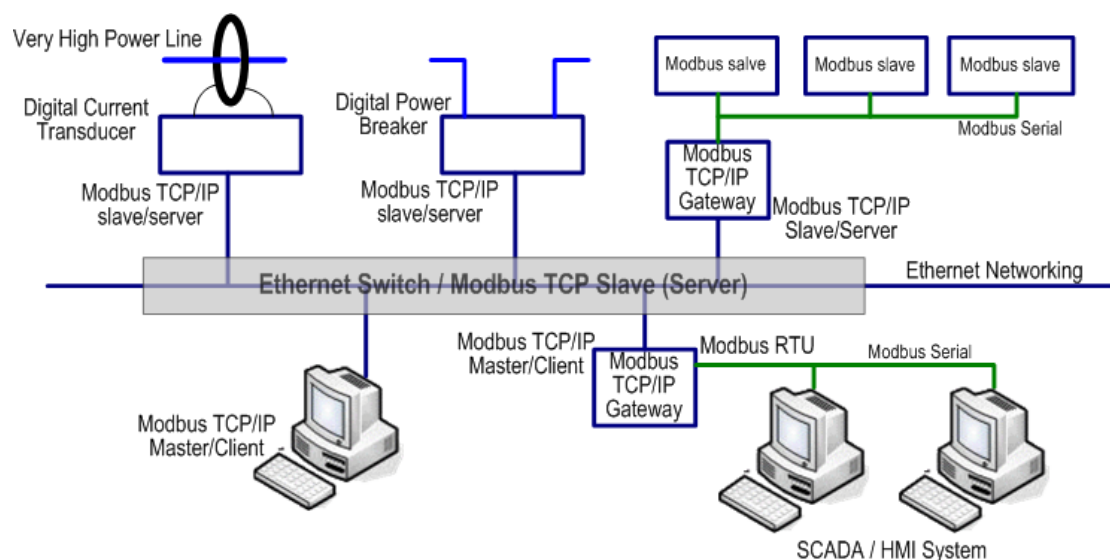
The path of the JetNet 4518 is **1.3.6.1.4.1.24062.2.2.16**

Compile the private MIB file and you can see all the MIB tables in MIB browser.

5.3 ModBus TCP /IP

The Modbus TCP/IP 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. Korenix JetNet 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.



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 JetNet Managed DIN-Rail Ethernet Switch has implement Modbus/TCP register in the firmware. Those register mapping to some of Ethernet Switch's 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.

5.3.1 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

The JetNet 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.

5.3.2 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 field checks the contents of the entire message. It applied regardless of any parity check method used for the individual BYTE actors 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 field.

5.3.3 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.

Code	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.

5.3.4 Modbus TCP register table

Since from firmware version 2.5, the JetNet 5010G and JetNet 4510 start support Modbus TCP/IP client service for the Factory automation applications. The command of modbus only supports in the command line interface-console and telnet mode that allows user to modify some parameters like as idle time, number of modbus master and modbus service port.

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 = 'l' Word 2 Hi byte = 'x' Word 2 Lo byte = '\0' (other words = 0)
0x0010	16 words	Product Name = "JetNet5828G" Word 0 Hi byte = 'J' Word 0 Lo byte = 'e' Word 1 Hi byte = 'T' Word 1 Lo byte = 'N' Word 2 Hi byte = 'e' Word 2 Lo byte = 't' Word 3 Hi byte = '5' Word 3 Lo byte = '8' Word 4 Lo byte = '2' Word 4 Hi byte = '8' Word 5 Lo byte = 'G' Word 5 Hi byte = '\0' (other words = 0)
0x0020	128 words	SNMP system name (string)
0x00A0	128 words	SNMP system location (string)
0x0120	128 words	SNMP system contact (string)
0x01A0	32 words	SNMP system OID (string)
0x01C0	2 words	System uptime (unsigned long)

0x01C2 to 0x01FF	60 words	Reserved address space
0x0200	2 words	hardware version
0x0202	2 words	S/N information
0x0204	2 words	CPLD version
0x0206	2 words	Boot loader version
0x0208	2 words	Firmware Version Word 0 Hi byte = major Word 0 Lo byte = minor Word 1 Hi byte = reserved Word 1 Lo byte = reserved
0x020A	2 words	Firmware Release Date Firmware was released on 2010-08-11 at 09 o'clock Word 0 = 0x0B09 Word 1 = 0x0A08
0x020C	3 words	Ethernet MAC Address Ex: MAC = 01-02-03-04-05-06 Word 0 Hi byte = 0x01 Word 0 Lo byte = 0x02 Word 1 Hi byte = 0x03 Word 1 Lo byte = 0x04 Word 2 Hi byte = 0x05 Word 2 Lo byte = 0x06
0x020F to 0x2FF	241 words	Reserved address space
0x0300	2 words	IP address Ex: IP = 192.168.10.1 Word 0 Hi byte = 0xC0 Word 0 Lo byte = 0xA8 Word 1 Hi byte = 0x0A Word 1 Lo byte = 0x01
0x0302	2 words	Subnet Mask
0x0304	2 words	Default Gateway
0x0306	2 words	DNS Server
0x0308 to 0x3FF	248 words	Reserved address space (IPv6 or others)
0x0400	1 word	AC1 0x0000:Off 0x0001:On 0xFFFF: unavailable

0x0401	1 word	AC2 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0402	1 word	DC1 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0403	1 word	DC2 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0404 to 0x040F	12 words	Reserved address space
0x0410	1 word	DI1 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0411	1 word	DI2 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0412	1 word	DO1 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0413	1 word	DO2 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0414 to 0x041F	12 words	Reserved address space
0x0420	1 word	RDY 0x0000:Off 0x0001:On
0x0421	1 word	RM 0x0000:Off 0x0001:On
0x0422	1 word	RF 0x0000:Off

		0x0001:On
0x0423	1 word	RS
Port Information (32 Ports)		
0x1000 to 0x11FF	16 words	Port Description
0x1200 to 0x121F	1 word	Administrative Status 0x0000: disable 0x0001: enable
0x1220 to 0x123F	1 word	Operating Status 0x0000: disable 0x0001: enable 0xFFFF: unavailable
0x1240 to 0x125F	1 word	Duplex 0x0000: half 0x0001: full 0x0003: auto (half) 0x0004: auto (full) 0x0005: auto 0xFFFF: unavailable
0x1260 to 0x127F	1 word	Speed 0x0001: 10 0x0002: 100 0x0003: 1000 0x0004: 2500 0x0005: 10000 0x0101: auto 10 0x0102: auto 100 0x0103: auto 1000 0x0104: auto 2500 0x0105: auto 10000 0x0100: auto 0xFFFF: unavailable
0x1280 to 0x129F	1 word	Flow Control 0x0000: off 0x0001: on 0xFFFF: unavailable
0x12A0 to 0x12BF	1 word	Default Port VLAN ID 0x0001-0xFFFF

0x12C0 to 0x12DF	1 word	Ingress Filtering 0x0000: disable 0x0001: enable
0x12E0 to 0x12FF	1 word	Acceptable Frame Type 0x0000: all 0x0001: tagged frame only
0x1300 to 0x131F	1 word	Port Security 0x0000: disable 0x0001: enable
0x1320 to 0x133F	1 word	Auto Negotiation 0x0000: disable 0x0001: enable 0xFFFF: unavailable
0x1340 to 0x135F	1 word	Loopback Mode 0x0000: none 0x0001: MAC 0x0002: PHY 0xFFFF: unavailable
0x1360 to 0x137F	1 word	STP Status 0x0000: disabled 0x0001: blocking 0x0002: listening 0x0003: learning 0x0004: forwarding
0x1380 to 0x139F	1 word	Default CoS Value for untagged packets
0x13A0 to 0x13BF	1 word	MDIX 0x0000: disable 0x0001: enable 0x0002: auto 0xFFFF: unavailable
0x13C0 to 0x13DF	1 word	Medium mode 0x0000: copper 0x0001: fiber 0x0002: none 0xFFFF: unavailable
0x13E0 to 0x14FF	288 words	Reserved address space

SFP Information (32 Ports)		
0x1500 to 0x151F	1 word	SFP Type
0x1520 to 0x153F	1 words	Wave length
0x1540 to 0x157F	2 words	Distance
0x1580 to 0x167F	8 words	Vender
0x1680 to 0x17FF	384 words	Reserved address space
SFP DDM Information (32 Ports)		
0x1800 to 0x181F	1 words	Temperature
0x1820 to 0x185F	2 words	Alarm Temperature
0x1860 to 0x187F	1 words	Tx power
0x1880 to 0x18BF	2 words	Warning Tx power
0x18C0 to 0x18DF	1 words	Rx power
0x18E0 to 0x191F	2 words	Warning Rx power
0x1920 to 0x1FFF	1760 words	Reserved address space
Inbound packet information		
0x2000 to 0x203F	2 words	Good Octets
0x2040 to 0x207F	2 words	Bad Octets
0x2080 to 0x20BF	2 words	Unicast
0x20C0 to 0x20FF	2 words	Broadcast
0x2100 to 0x213F	2 words	Multicast
0x2140 to 0x217F	2 words	Pause
0x2180 to 0x21BF	2 words	Undersize
0x21C0 to 0x21FF	2 words	Fragments
0x2200 to 0x223F	2 words	Oversize
0x2240 to 0x227F	2 words	Jabbers
0x2280 to 0x22BF	2 words	Disacrd

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	447 words	Reserved address space

0x29FF		
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

Note: the modbus TCP client will return 0xFFFF to modbus master when pulling reserved address.

5.3.5 CLI commands for Modbus TCP

The CLI commands of Modbus TCP are listed as following table.

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 → 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 → 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.

5.4 Revision History

Edition	Date	Modifications
V1.4	Feb. 13, 2012	Apply v1.3 firmware feature. Add JetNet 5018G v2.0 mode and its related changes. Add Multiple User Interface – Simplified Chinese. Add Modbus TCP function code into user manual. Add DDM SFP function into port control & status. Modify the description of SFP transceiver function.
V1.3a	Jul. 26, 2011	Correct the color of the Diagnostic LED.
V1.3	Jun. 15, 2011	Add New Features, Multiple Spanning Tree Protocol, Private VLAN, QinQ description and configuration Update the combo port behavior. Update Port Configuration, IGMP Unknown Multicast, GMRP description. Update new MSR description and commands.
V1.2	Oct.. 18, 2010	Add 4518 model and its related description and specification. JetNet 4518 is a Managed Fast Ethernet switch which only support 10/100Base-TX and 100Base-FX SFP. Correct DO info of the 3018G, DO GUI setting of the managed switch. Correct Combo Port, Fiber information of all models. Correct Broadcast Storm Control setting page. Add more information of the Multiple Super Ring. Add LACP Long/Short Feature & CLI setting. Correct some incorrect wordings.
V1.1	Dec. 24, 2009	Add 3018G model and its related description and specification. JetNet 3018G is the unmanaged gigabit switch. Follow the hardware installation to install switch, there is no software configuration available. Correct the curve mechanical to vertical. Add SFP BIDI
V1.0	Oct. 27, 2009	CLI command correction continue and changed the version to V1.0.
V0.2	Oct. 25, 2009	CLI Command correction.
V0.1	Oct. 23, 2009	The first version.

5.5 About Korenix

Less Time At Work! Fewer Budget on applications!

The Korenix business idea is to let you spend less time at work and fewer budget on your applications. Do you really want to go through all the troubles but still end up with low quality products and lousy services? Definitely not! This is why you need Korenix. Korenix offers complete product selection that fulfills all your needs for applications. We provide easier, faster, tailor-made services, and more reliable solutions. In Korenix, there is no need to compromise. Korenix takes care of everything for you!

Fusion of Outstandings

You can end your searching here. Korenix Technology is your one-stop supply center for industrial communications and networking products. Korenix Technology is established by a group of professionals with more than 10 year experience in the arenas of industrial control, data communications and industrial networking applications. Korenix Technology is well-positioned to fulfill your needs and demands by providing a great variety of tailor-made products and services. Korenix's industrial-grade products also come with quality services. No more searching, and no more worries. Korenix Technology stands by you all the way through.

Core Strength---Competitive Price and Quality

With our work experience and in-depth know-how of industrial communications and networking, Korenix Technology is able to combine Asia's research / development ability with competitive production cost and with quality service and support.

Global Sales Strategy

Korenix's global sales strategy focuses on establishing and developing trustworthy relationships with value added distributors and channel partners, and assisting OEM distributors to promote their own brands. Korenix supplies products to match local market requirements of design, quality, sales, marketing and customer services, allowing Korenix and distributors to create and enjoy profits together.

Quality Services

KoreCARE--- KoreCARE is Korenix Technology's global service center, where our professional staffs are ready to solve your problems at any time and in real-time. All of Korenix's products have passed ISO-9000/EMI/CE/FCC/UL certifications, fully satisfying your demands for product quality under critical industrial environments. Korenix global service center's e-mail is koreCARE@korenix.com

5 Years Warranty

Each of Korenix's product line is designed, produced, and tested with high industrial standard. Korenix warrants that the Product(s) shall be free from defects in materials and workmanship for a period of five (5) years from the date of delivery provided that the Product was properly installed and used. This warranty is voided if defects, malfunctions or failures of the warranted Product are caused by damage resulting from force measure (such as floods, fire, etc.), environmental and atmospheric disturbances, other external forces such as power line disturbances, host computer malfunction, plugging the board in under power, or incorrect cabling; or the warranted Product is misused, abused, or operated, altered and repaired in an unauthorized or improper way

Korenix Technologies Co., Ltd.

Business service : sales@korenix.com

Customer service: koreCARE@korenix.com