

# **Korenix JetNet 6628X series Industrial Managed Ethernet Switch**

---

## **User Manual**

Ver. 1.0 , 2019

**korenix**

[www.korenix.com](http://www.korenix.com)

# **Korenix JetNet 6628X series Industrial Managed Ethernet Switch User Manual**

## **Copyright Notice**

Copyright © 2006-2019 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.....	2
1.1	Overview.....	2
1.2	Major Features.....	2
1.3	Package List.....	3
2	Hardware Installation.....	4
2.1	Hardware Introduction.....	5
2.2	Wiring Power Inputs.....	6
2.3	Power Supply Specifications.....	8
2.4	Wiring Digital Output.....	8
2.5	Wiring Earth Ground.....	9
2.6	Wiring Fast Ethernet Ports.....	9
2.7	Wiring Combo Ports.....	10
2.8	Data and Power Ports.....	10
2.9	Wiring RS-232 Console Cable.....	11
2.10	Rack Mounting Installation.....	11
3	Preparation for Management.....	12
3.1	Preparation for Serial Console.....	12
3.2	Preparation for Web Interface.....	13
3.3	Preparation for Telnet Console.....	15
4	Feature Configuration.....	18
4.1	Command Line Interface Introduction.....	19
4.2	Basic Setting.....	24
4.3	Port Configuration.....	43
4.4	Power over Ethernet.....	52
4.5	Network Redundancy.....	63
4.6	VLAN.....	82
4.7	Private VLAN.....	92
4.8	Traffic Prioritization.....	98
4.9	Multicast Filtering.....	102
4.10	SNMP.....	105
4.11	Security.....	109
4.12	Warning.....	120
4.13	Monitor and Diag.....	129
4.14	Device Front Panel.....	135
4.15	Save to Flash.....	136
4.16	Logout.....	137

5	Appendix.....	138
5.14	Pin Assignment of the RS-232 Console Cable .....	138
5.15	Korenix SFP family .....	139
5.16	Korenix Private MIB.....	141
5.17	Revision History .....	142
5.18	About Korenix .....	143

# **1 Introduction**

Welcome to Korenix *JetNet 6628X* Series Industrial Managed Ethernet Switch User Manual. Following topics are covered in this chapter:

## **1.1 Overview**

### **1.2 Major Features**

### **1.3 Package Checklist**

## **1.1 Overview**

JetNet 6628X series is Layer 2 rackmount 24-port Gigabit RJ-45 + 4-port 10\*Gigabit SFP Managed Industrial switch, it contains PoE model (JetNet 6628XP) and Non-PoE model (JetNet 6628X). JetNet 6628XP is 24-port PoE + 4-port 10\*Gigabit SFP, it supports IEEE 802.3af/at per PoE ports.

The 4 Gigabit Ethernet ports provide high speed uplink to connect with higher level backbone switches. With the Korenix patented MSR™ network redundancy technology, the switches can aggregate up to 12 fast ethernet and 2 gigabit rings while providing high quality data transmission with less than 5ms network recovery time. Furthermore, to ensure the traffic switching without data loss and blocking, the JetNet 6628X series provides 12.8G backplane with the integrated non-blocking switching function. JetNet 6628X incorporates LLDP function and perfectly works with the Korenix patented NMS for allowing administrators to automatically discover devices and efficiently manage the industrial network performance in large scale surveillance networks. To further ensure the non-stop power delivery, JetNet 6628X series supports dual 53VDC power inputs and provides alarm relay output signaling function. For high voltage requiring applications the PoE switch provides extra 100~240VAC power supply capability.

With the advanced Layer2 management features including IGMP Query/Snooping, DHCP, 256 VLAN, QoS, LACP, LPLD, etc. and the corrosion resistant robust design, JetNet 6628X highly outstands from other PoE switches and becomes the revolutionary solution for industrial surveillance applications.

## **1.2 Major Features**

Korenix JetNet 6628X Series products have the following features:

- Up to 24 10/100/1000 BaseTX and 4 10Gigabit uplink SFP ports
- Up to 24 ports support both 15.4W IEEE 802.3af and the 30W high power IEEE 802.3at, including 2-event and LLDP classification ( JetNet 6628XP)
- Flexible-bandwidth and long-distance data transmission by SFP transceivers
- Total power budget is 720W (Need add additional DC power source)
- LPLD (Link Partner Live Detect Function) for reliable PoE connection through Active Powered Device status detection and auto reset function

- 128Gbps Non-Blocking backplane, 16K MAC table for wire speed bidirectional switching
- IEEE 1588 PTP compliance for precise time synchronization
- Supports up to 9,216 bytes Jumbo Frame for secured large file transmission
- IEEE 802.1AB LLDP and optional Korenix NMS software for auto-topology and large network group management
- IGMP Query v1/v2 & Snooping v1/v2/v3 for advanced multicast filtering
- Up to 256 VLAN traffic isolation
- Advanced network management features support SNMP, RMON
- Supports DHCP client, DHCP Option 82 for automatic IP configuration
- Dual redundant low voltage range: 48VDC and HDC range: 100~240VAC
- IP40 rugged metal case with great heat dispersion

### **1.3 Package List**

Korenix JetNet 6628X Series products are shipped with following items:

- One industrial Managed Ethernet switch
- One RS-232 DB-9 console cable
- JetNet 6628X series 19" rack mount Kits

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

## **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 Power Supply Specifications**

### **2.4 Wiring Digital Output**

### **2.5 Wiring Earth Ground**

### **2.6 Wiring Fast Ethernet Ports**

### **2.7 Wiring Combo Ports**

### **2.8 Data and Power Ports**

### **2.9 Wiring RS-232 Console Cable**

### **2.10 Rack Mounting Installation**



## 2.1 Hardware Introduction

### Dimension

JetNet 6628X Series Industrial Gigabit Switch dimension (W x H x D) is **440 mm x 44mm x 378.5mm**

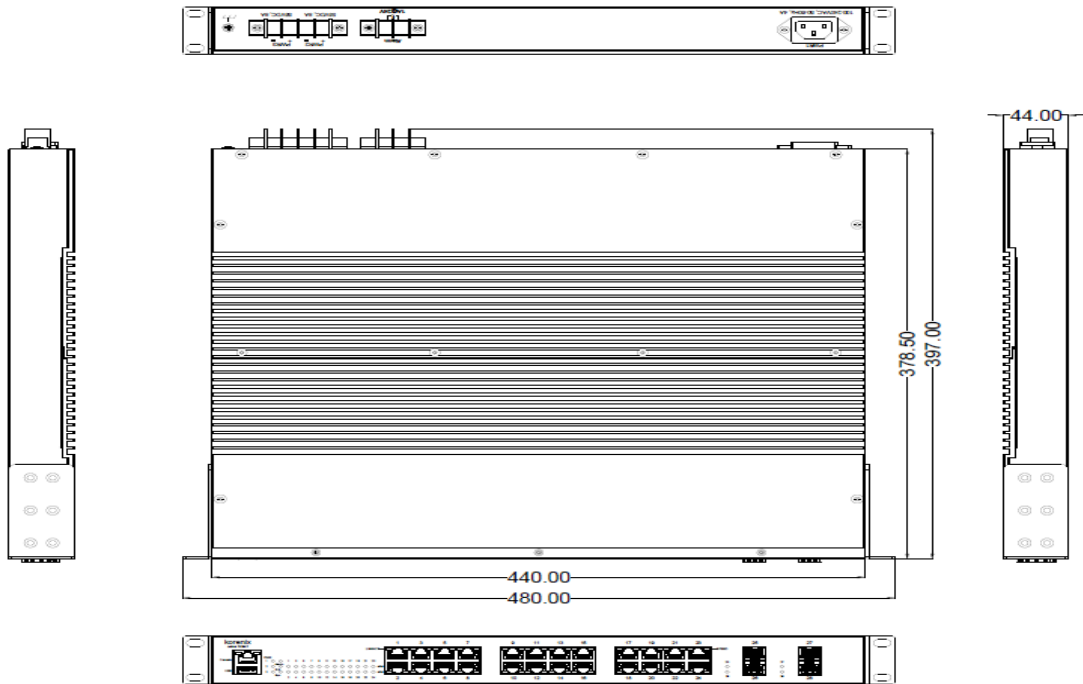


Diagram: JetNet 6628XP

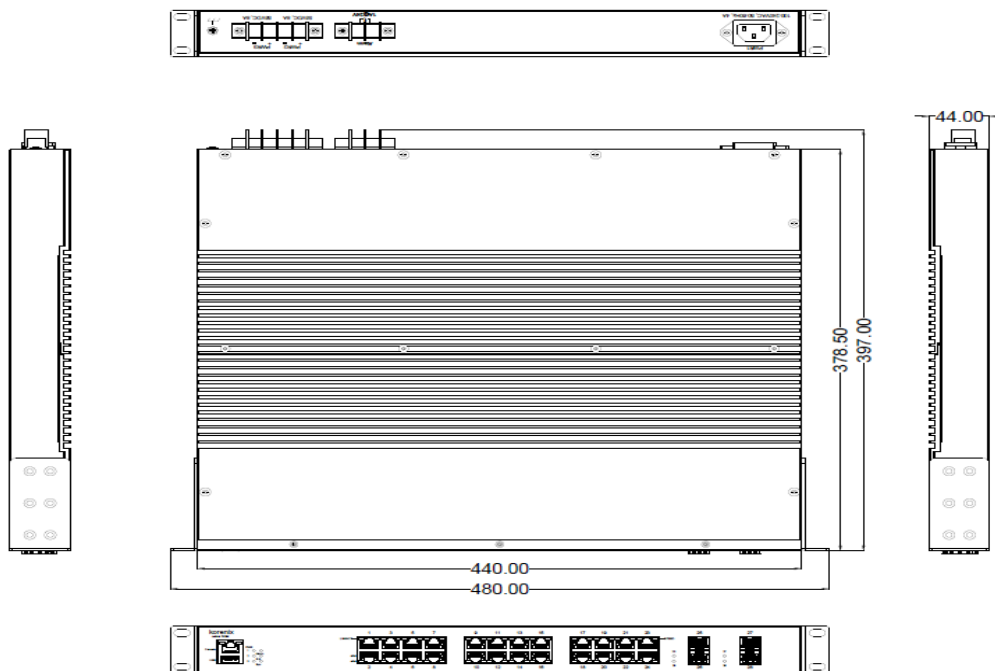
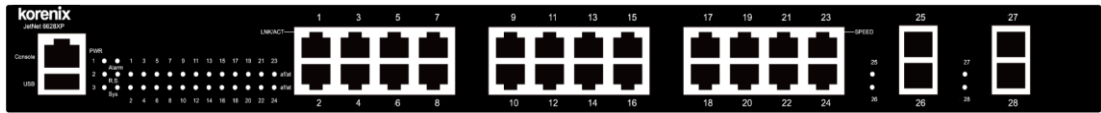


Diagram: JetNet 6628X

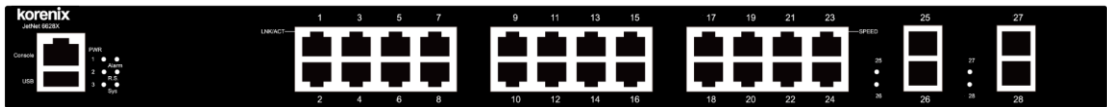
## Panel Layout

The front panel includes up to 24 10/100/1000Mbps Ethernet ports, 4\* 10 Gigabit SFP ports, RS-232 console port, System / Combo Port LED and up to 24 PoE LED.

JetNet 6628XP



JetNet 6628X



The back panel of the JetNet 6628X Industrial Gigabit Managed Switch consists of two DC power inputs, 1 AC Input, 1 Relay Output.



## 2.2 Wiring Power Inputs

JetNet 6628X provides 2 types power input, AC power input and DC power input. It also provides redundant or aggregated power inputs, depending on the voltage of power input. If there are over 2 power inputs are connected with different voltages, JetNet 6628X will be powered from the highest connected voltage (redundant power). If the voltages of power inputs are the same, the total power output will be aggregated (agggegaged power).

### AC Power Input

Connect the attached power cord to the AC power input connector, the available AC power input is range from 100-240VAC.

### High Voltage Power Input

The power input support both 100-240VAC power input. Connect the power cord to the PE for Protective Earth, L / V+ for LINE or V+, N/V- for Neutral or V-. For high power input, tighten the wire-clamp screws to prevent DC wires from being loosened is must.

### DC Power Inputs

The range of the available DC power input is from 46-57VDC. In the IEEE802.3at mode, the PoE power output is 50~57 VDC, 0.6A, therefore, the suggested DC power input ranges is

53VDC (52~57VDC). In the IEEE802.3af mode, the PoE power output is 44~57 VDC, 0.35A, therefore, the suggested DC power input is 48VDC (46~57VDC).

The nominal of AC power input is 55VDC, if you add additional DC power source , please set the DC input higher than 55VDC , then the unit can consume DC power source afterwards.

Follow below steps to wire JetNet 6628X redundant or aggregated 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. DC1 and DC2 support polarity reverse protection functions.

**Note 1:** It is a good practice to turn off input and load power.. Otherwise, your screwdriver blade can inadvertently short your terminal connections to the grounded enclosure.

**Note 2:** The range of the suitable electric wire is from 12 to 22 AWG.

**Note 3:** The unit will alarm for loss of power, for instance, PSU, DC1 or DC2.



## 2.3 Power Supply Specifications

Power Supply Type	Input Range		Max. Input Current	Fuse Rating	Max. Power Consumption
	Min	Max			All Ethernet Ports
48 VDC 53 VDC	46 VDC	57 VDC	8.2A	10A(T)	30W
HI (110/230 VAC), 47~63Hz	100 VAC	250 VAC	4A	4A(T)	

Table: Power Supply Specifications

Jetnet 6628X-24P

Power Supply Type	Input Range		Fuse Rating	Power Consumption	
	Min	Max		Worst Case	Max
48 VDC (IEEE802.3af)	46 VDC	57 VDC	1.5A(F)	369.6W	369.6W
53 VDC (IEEE802.3at)	52 VDC	57 VDC	1.5A(F)	568W	720W

Jetnet 6628X-16P

Power Supply Type	Input Range		Fuse Rating	Power Consumption	
	Min	Max		Worst Case	Max
48 VDC (IEEE802.3af)	46 VDC	57 VDC	1.5A(F)	246.4W	246.4W
53 VDC (IEEE802.3at)	52 VDC	57 VDC	1.5A(F)	364W	480W

Jetnet 5720G-8P

Power Supply Type	Input Range		Fuse Rating	Power Consumption	
	Min	Max		Worst Case	Max
48 VDC (IEEE802.3af)	46 VDC	57 VDC	1.5A(F)	123.2W	123.2W
53 VDC (IEEE802.3at)	52 VDC	57 VDC	1.5A(F)	182W	240W

Table: PoE/PoE Plus Power Supply Specifications

**Note 1:** (F) Denotes fast-acting fuse, (T) denotes time-delay fuse

**Note 2:** Power consumption varies based on configuration. 10/100Tx ports consume roughly 1W less than fiber optic ports

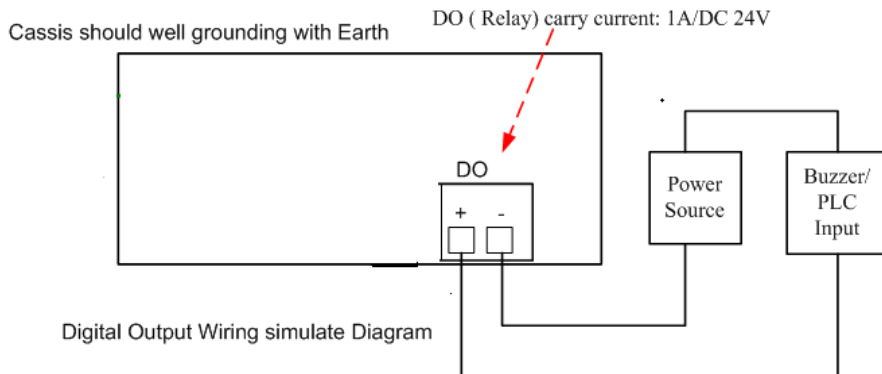
**Note 3:** For continued protection against risk of fire, replace only with same type and rating of fuse.

## 2.4 Wiring Digital Output

JetNet 6628X provides 1 digital output, also known as Relay Output. The relay contacts

are energized (open) for normal operation and will close for fault conditions. The fault conditions include power failure, Ethernet port link break or other pre-defined events which can be configured in JetNet 6628X UI.

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



## 2.5 Wiring Earth Ground

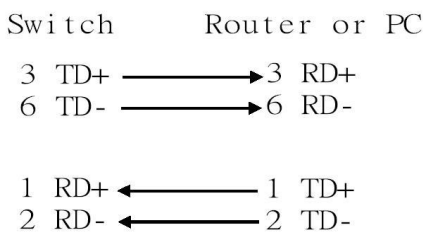
To ensure the system will not be damaged by noise or any electrical shock, we suggest you to make exact connection with JetNet 6628X with Earth Ground.

On the back panel of JetNet 6628X, there is one earth ground screw. Loosen the earth ground screw by screw driver; then tighten the screw after earth ground wire is connected.

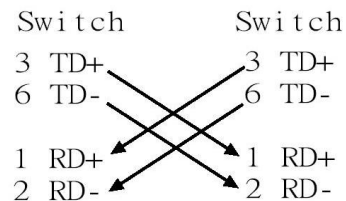
## 2.6 Wiring Fast Ethernet Ports

JetNet 6628X includes up to 24 RJ-45 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)

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

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

IEEE 802.3af : 4-pair UTP/STP Cat. 5 cable, EIA/TIA-568 100-ohm (100m)

IEEE 802.3at : 4-pair UTP/STP Cat. 5e / 6 cable, EIA/TIA-568 100-ohm (100m)

## 2.7 Wiring Combo Ports

JetNet 6628X includes 4 RJ-45 Gigabit Ethernet ports. The speed of the gigabit Ethernet port supports 10Base-T, 100Base-TX and 1000Base-TX. JetNet 6628X also equips 4 gigabit SFP ports combo with gigabit Ethernet ports. The speed of the SFP port supports 1000Base-SX/LX. The SFP ports accept standard MINI GBIC SFP transceiver. But, to ensure system reliability, Korenix recommends using the Korenix certificated Gigabit SFP Transceiver. The certificated SFP transceiver includes 1000Base-SX/LX single/multi mode ranger from 550m to 80KM.

## 2.8 Data and Power Ports

JetNet 6628X comes standard with up to 24 10/100BaseTX IEEE802.3af (PoE) and IEEE802.3at (PoE Plus) compliant Ethernet ports (ports 1-24). In addition to the 10/100BaseTX port features, the PoE ports provide normal 48 VDC at 350mA (max 15.4W/port) or provide normal 53 VDC at 606mA (max 30W/port), auto-sensing and automatic power off when cables are removed. The following table shows the RJ45 PoE pin-out assignment.

10/100BaseTx PoE Pin-out	
Pin	Description
1	RX + and Vport -
2	RX – and Vport -
3	TX + and Vport +
6	TX – and Vport +
4, 5, 7, 8	NC

Table: RJ45 PoE pin-out assignment

This product is designed for in building installation only and is not intended to be connected to exposed (outside plant) networks.

## 2.9 Wiring RS-232 Console Cable

Korenix attaches one RS-232 DB-9 cable in the box. Connect the DB-9 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 cable.

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.

## 2.10 Rack Mounting Installation

The Rack Mount Kit is attached inside the package.

2.8.1 Attach the brackets to the device by using the screws provided in the Rack Mount kit.



2.8.2 Mount the device in the 19" rack by using four rack-mounting screws provided by the rack manufacturer.



When installing multiple switches, mount them in the rack one below the other. It's requested to reserve 0.5U-1U free space for multiple switches installing. This is important to disperse the heat generated by the switch.

Notice when installing:

- Temperature: Check if the rack environment temperature conforms to the specified operating temperature range.
- Mechanical Loading: Do not place any equipment on top of the switch
- Grounding: Rack-mounted equipment should be properly grounded.

## **3 Preparation for Management**

JetNet 6628X series Industrial Managed Switch provides both in-band and out-band configuration methods. You can configure the switch via RS-232 console cable if you don't attach your admin PC to your network, or if you lose network connection to your JetNet 6628X. 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.

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 6628X package, Korenix attached one RS-232 DB-9 console cable. Please attach RS-232 DB-9 connector to your PC COM port, connect to the Console port of the JetNet 6628X. 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 6628X 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".



## 3.2 Preparation for Web Interface

JetNet 6628X 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 6628X Series Industrial Ethernet Switch is properly installed on your network and that every PC on this network can access the switch via the web browser.

1. Verify that your network interface card (NIC) is operational, and that your operating system supports 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**.

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 6628X 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 6628X first. Press **Yes** to trust it.
4. The login screen will appear next.



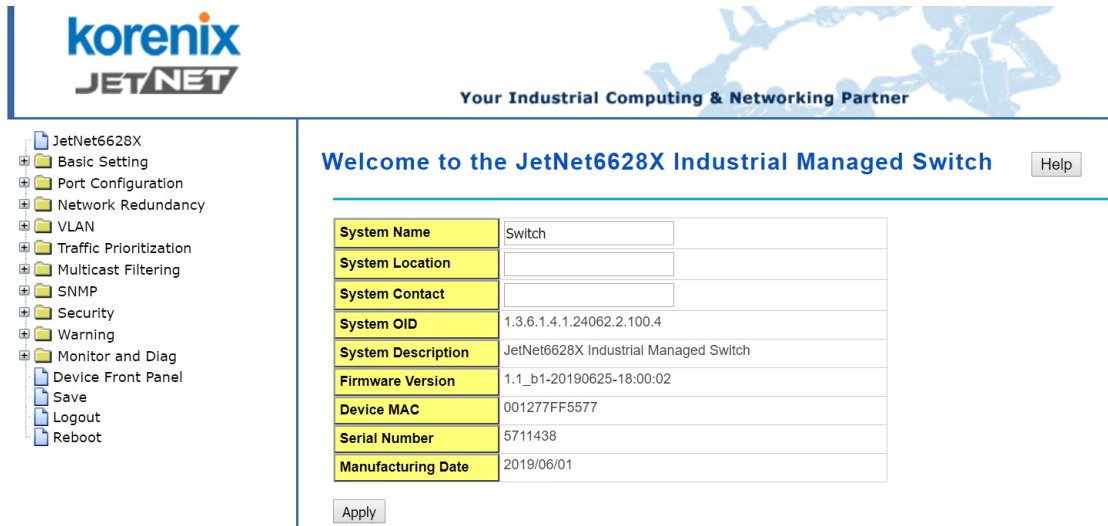
### Welcome to the JetNet6628X Industrial Managed Switch

Name

Password



5. Key in the user name and the password. The default user name and password is **admin**.
6. Click on **Login**. Welcome page of the web-based management interface will then appear.



- 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 6628X supports Telnet console. You can connect to the switch by Telnet and the command lines are the same as what you see by RS-232 console port. Below are the steps to open Telnet connection to the switch.

- Go to Start -> Run -> cmd. And then press **Enter**
- 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 6628X 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.

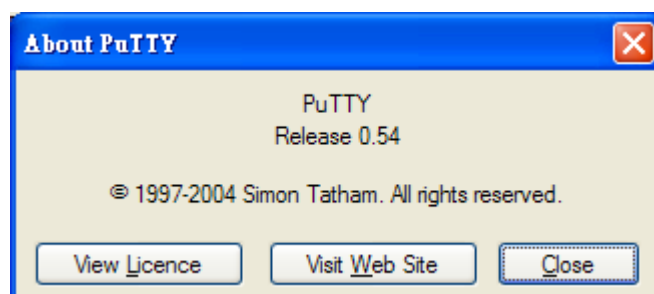
SSH is a client/server architecture while JetNet 6628X is the SSH server. When you want to make SSH connection with the switch, you should download the SSH client tool first.

##### 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.*

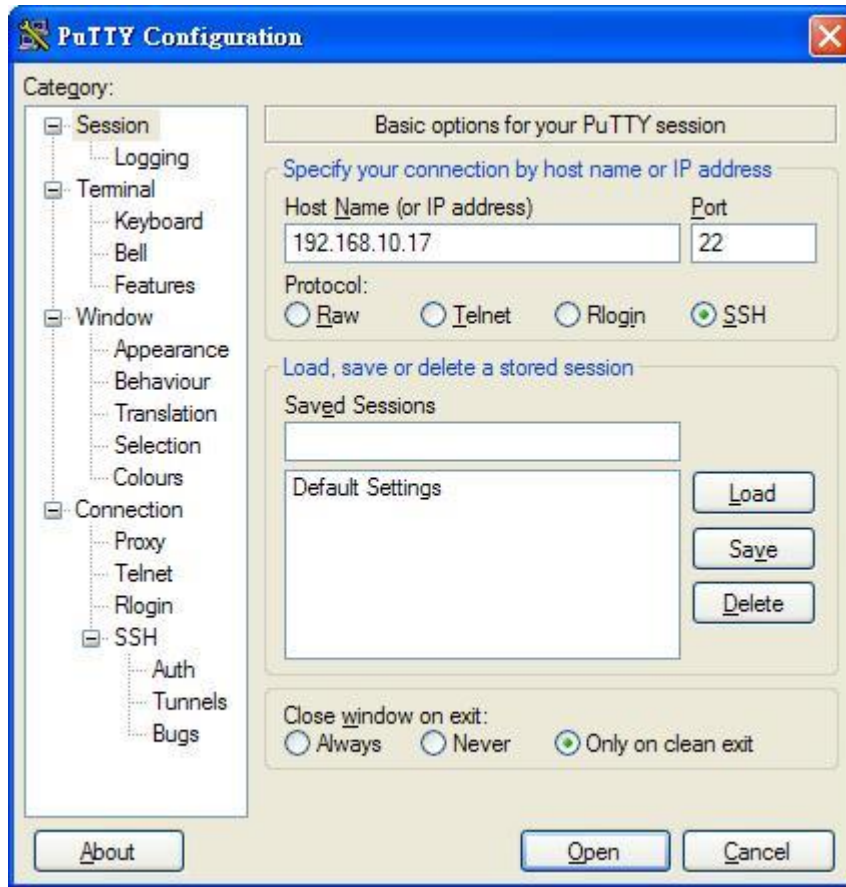
**Download PuTTY:** <http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>

The copyright of **PuTTY**

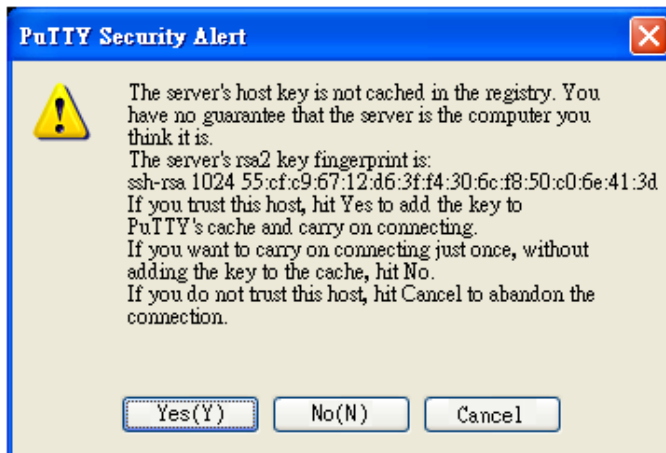


## R. Open SSH Client/PuTTY

In the **Session** configuration, enter the **Host Name** (IP Address of your JetNet 6628X) and **Port number** (default = 22). Choose the **SSH** protocol. Then click on **Open** to start the SSH session console.



R. 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 6628XP is opened. You can see the login screen as the below figure.

```
192.168.10.1 - PuTTY
Session Special Command Window Logging Files Transfer Hangup ?
login as: admin
admin@192.168.10.1's password:
JetNet6628X (version 1.1_b1-20190625-18:00:02).
Copyright 2006-2020 Korenix Technology Co., Ltd.
Switch# █
```

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 RS-232 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 6628X software features. There are four ways to access the switch: Serial console, Telnet, Web browser and SNMP.

JetNet 6628X series Industrial Managed Switch provides both in-band and out-band configuration methods. You can configure the switch via RS-232 console cable if you don't attach your admin PC to your network, or if you lose the network connection to your JetNet 6628X. 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 Power over Ethernet
- 4.5 Network Redundancy
- 4.6 VLAN
- 4.7 Private VLAN
- 4.8 Traffic Prioritization
- 4.9 Multicast Filtering
- 4.10 Routing
- 4.11 SNMP
- 4.12 Security
- 4.13 Warning
- 4.14 Monitor and Diag
- 4.15 Device Front Panel
- 4.16 Save
- 4.17 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 Privileged EXEC, Global Configuration, (Port/VLAN) Interface Configuration modes.

**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#	
<code>archive</code>	manage archive files
<code>clear</code>	Reset functions
<code>clock</code>	Configure time-of-day clock
<code>configure</code>	Configuration from vty interface
<code>copy</code>	Copy from one file to another
<code>debug</code>	Debugging functions (see also 'undebug')
<code>disable</code>	Turn off privileged mode command
<code>end</code>	End current mode and change to enable mode
<code>exit</code>	Exit current mode and down to previous mode
<code>list</code>	Print command list
<code>more</code>	Display the contents of a file
<code>no</code>	Negate a command or set its defaults
<code>ping</code>	Send echo messages
<code>quit</code>	Exit current mode and down to previous mode
<code>reboot</code>	Reboot system
<code>reload</code>	copy a default-config file to replace the current one
<code>show</code>	Show running system information
<code>telnet</code>	Open a telnet connection
<code>terminal</code>	Set terminal line parameters
<code>traceroute</code>	Trace route to destination
<code>write</code>	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 for fast Ethernet port 1 is fa1,... fast Ethernet 7 is fa7, gigabit Ethernet port 8 is gi8.. gigabit Ethernet port 10 is gi10. Type 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 global 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: <b>Login</b> successfully Exit: <b>exit</b> to logout. Next mode: Type <b>enable</b> 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 <b>enable</b> in User EXEC mode. Exec: Type <b>disable</b> to exit to user EXEC mode. Type <b>exit</b> to logout Next Mode: Type <b>configure terminal</b> 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 <b>configure terminal</b> in privileged EXEC mode Exit: Type <b>exit</b> or <b>end</b> or press <b>Ctrl-Z</b> to exit. Next mode: Type <b>interface IFNAME/ VLAN VID</b> to enter interface configuration mode	Switch(config)#
Port Interface configuration	In this mode, you can configure port related settings.	Enter: Type <b>interface IFNAME</b> in global configuration mode. Exit: Type <b>exit</b> or <b>Ctrl+Z</b> to global configuration mode. Type <b>end</b> to privileged EXEC mode.	Switch(config-if)#
VLAN Interface Configuration	In this mode, you can configure settings for specific VLAN.	Enter: Type <b>interface VLAN VID</b> in global configuration mode. Exit: Type <b>exit</b> or <b>Ctrl+Z</b> to global configuration mode. Type <b>end</b> 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
```

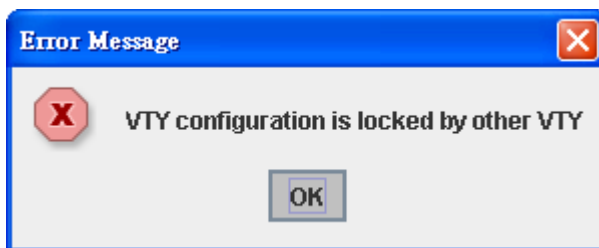
Ctrl+C To stop executing the unfinished command.

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 6628X 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.

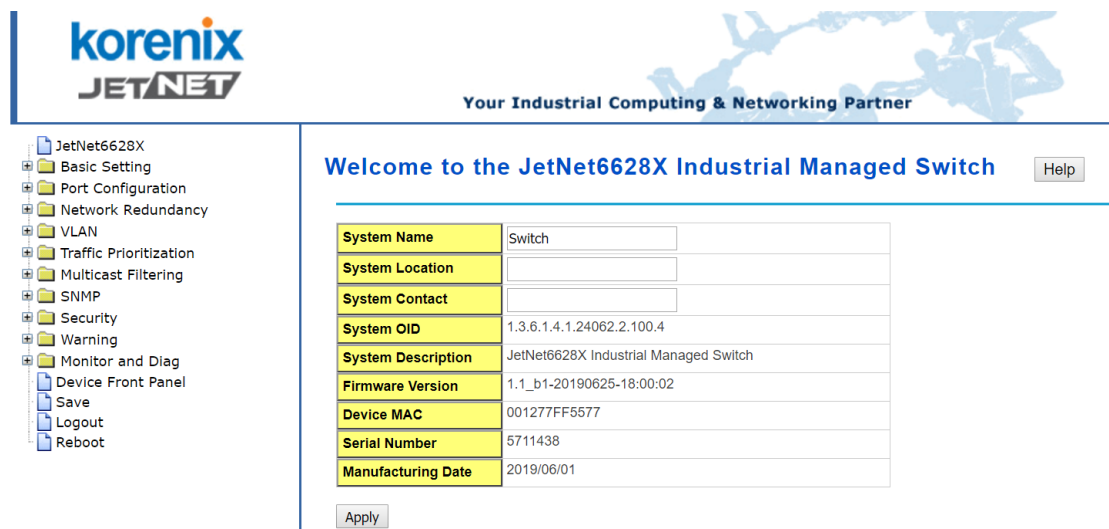
Following commands are included in this group:

- 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



The screenshot shows the web UI for the JetNet6628X Industrial Managed Switch. The page title is "Welcome to the JetNet6628X Industrial Managed Switch" with a "Help" button. The left navigation menu includes: JetNet6628X, Basic Setting (selected), Port Configuration, Network Redundancy, VLAN, Traffic Prioritization, Multicast Filtering, SNMP, Security, Warning, Monitor and Diag, Device Front Panel, Save, Logout, and Reboot. The main content area displays the following system information:

System Name	Switch
System Location	
System Contact	
System OID	1.3.6.1.4.1.24062.2.100.4
System Description	JetNet6628X Industrial Managed Switch
Firmware Version	1.1_b1-20190625-18:00:02
Device MAC	001277FF5577
Serial Number	5711438
Manufacturing Date	2019/06/01

An "Apply" button is located at the bottom of the table.

**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 6628X Industrial Management Ethernet 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

The screenshot shows a web interface titled "Admin Password" with a "Help" button. Below the title is a form with four rows:

Name	admin
Privilege	0 ▼
New Password	.....
Confirm Password	

At the bottom of the form are two buttons: "Apply" and "Cancel".

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

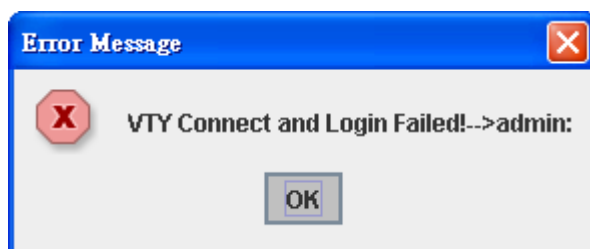
**Privilege:** You can assign different privilege levels to multiple users.

**New 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 Help

DHCP Client Disable ▾

Apply

### IPv4 Configuration

IP Address	192.168.10.1
Subnet Mask	255.255.255.0
Default Gateway	
DNS Server 1	
DNS Server 2	

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.

**IPv6 Configuration** –An IPv6 address is represented as eight groups of four hexadecimal digits, each group representing 16 bits (two octets). The groups are separated by colons (:), and the length of IPv6 address is 128bits.

An example of an IPv6 address is: 2001:0db8:85a3:0000:0000:8a2e:0370:7334.

The default IP address of JetNet Managed Switch is fe80::212:77ff:fe00:1277/64, and the Leading zeroes in a group may be omitted. Thus, the example address may be written as:

fe80::212:77ff:fe60:ca90.

## IPv6 Configuration

Prefix Length

IPv6 Address	
<input type="text"/>	<input type="text"/>

Add

IPv6 Default Gateway
<input type="text"/>

Apply

IPv6 Address
<input type="checkbox"/> fe80::212:77ff:fe00:1277/64

Remove

Reload

**IPv6 Address field:** typing new IPv6 address in this field.

**Prefix:**the size of subnet or network, and it equivalent to the subnetmask, but written in different. The default subnet mask length is 64bits, and written in decimal value -64.

**Add:** after add new IPv6 address and prefix, don't forget click icon-**"Add"**to apply new address to system.

**Remove:**select existed IPv6 address and click icon-**"Remove"**to delete IP address.

**Reload:**refresh and reload IPv6 address listing.

**IPv6 Default Gateway:** assign the IPv6 default gateway here. Type IPv6 address of the gateway then click **"Apply"**. Note: In CLI, we use ::/0 to represent for the IPv6 default gateway.

### IPv6 Default Gateway

Default Gateway
<input type="text"/>

Apply

**IPv6 Neighbor Table:** shows the IPv6 address of neighbor, connected interface, MAC address of remote IPv6 device, and current state of neighbor device.

## IPv6 Neighbor Table

Neighbor	Interface	MAC address	State
fe80::212:77ff:feff:101	vlan1	00:12:77:ff:01:01	REACHABLE

The system will update IPv6 Neighbor Table automatically, and user also can click the icon “**Reload**” to refresh the table.

### 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.

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

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

The JetNet 6628X series also provides Daylight Saving function for some territories use.

## Time Setting

<b>Current Time</b>	Yr 2015 Mon 01 Day 1 Hr 00 Mn 36 Sec 25 <input type="button" value="Get PC Time"/>
<b>Time Zone</b>	(GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London ▼
<b>NTP</b>	<input type="checkbox"/> Enable NTP client update
<b>Primary server</b>	N/A
<b>Secondary server</b>	N/A
<b>Daylight saving Time</b>	Disable ▼
<b>Daylight Saving Start</b>	1st ▼ Sun ▼ in Jan ▼ at 00 ▼ 00 ▼
<b>Daylight Saving End</b>	1st ▼ Sun ▼ in Jan ▼ at 00 ▼ 00 ▼

**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.

**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.



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

Auto mode: the switch performs PTP Master and slave mode (Bindary mode)

Master mode: switch performs PTP Master only.

Slave mode: switch performs PTP slave only.

## IEEE 1588 PTPv2

Help

Enable	Disable ▾
Mode	Auto ▾
Synchronization Interval	0(1s) ▾
Announce Interval	1(2s) ▾
Announce Receipt Timeout	6
Minimum Path Delay Request Message Interval	1(2s) ▾
Domain Number	0
First Priority	128
Second Priority	128
Delay Mechanism	E2E ▾

Apply

**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
R. (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.

**Daylight Saving Time:** click the check box to enable the Daylight Saving Function as the setting of start and end time or disable it.

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

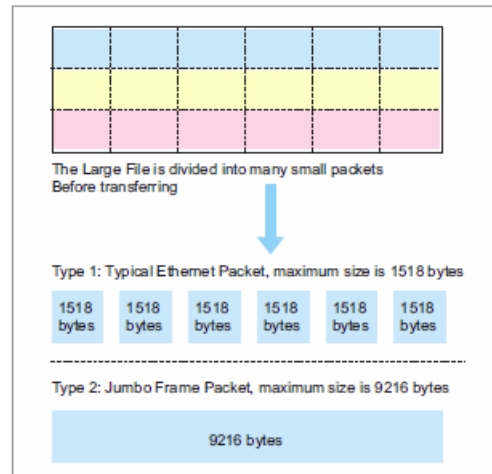
Once you finish those configurations, click on **Apply** to apply your configuration.

#### 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.



## Jumbo Frame

Help

Port	MTU Size
1	1518
2	1518
3	1518
4	1518

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

#### 4.2.6 DHCP Server

You can select to **Enable** or **Disable** DHCP Server function. *JetNet 6628X* 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 Configuration

Help

Global Setting Disable ▾

Apply

## Address Pool Add

Pool Name

Add

## Address Pool List

Pool Name ▾

Select

Delete

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 List

Excluded IP

Add

Index	IP Address

Remove

Reload

**Static MAC / IP Binding List** : *JetNet 6628X* provides a MAC address and IP address binding and removing function. You can type in the specified IP and MAC address, and 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**.

## Static MAC/IP Binding List

MAC Address

IP Address

Add

Index	MAC Address	IP Address

Remove

Reload

**DHCP Leased Entries:** *JetNet 6628X* provides an assigned IP address list for user check. It will show the MAC and IP address that was assigned by *JetNet 6628X*. Click the **Reload** button to refresh the listing.

## DHCP Leased Entries Help

Index	IP Address	MAC Address	Leased Time Remains

Reload

### Option82 Information

#### DHCP Relay Agent

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

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

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

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

**Helper Address:** there are 4 fields for the DHCP server's IP address. You can edit the field with device c IP address of DHCP Server, and then click "Apply" to activate the DHCP relay agent function. All the DHCP packets from client will be modified by the policy and forwarded to DHCP server through the gateway port.

## Option82 Information Help

DHCP Relay Agent Disable ▾

Apply

### Helper Address

**Helper Address**

Add

<input type="checkbox"/>	<b>Helper Address 1</b>	<input type="text"/>
<input type="checkbox"/>	<b>Helper Address 2</b>	<input type="text"/>
<input type="checkbox"/>	<b>Helper Address 3</b>	<input type="text"/>
<input type="checkbox"/>	<b>Helper Address 4</b>	<input type="text"/>

### Relay Policy

- Replace
- Keep
- Drop

Apply

### Circuit ID

Default (VLAN/Port)  User Defined

Apply

Port	Circuit ID	HEX value
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>

#### 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. You can also 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.

#### **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 and Restore

Help

---

### Local Files

Load Settings from File	<input type="button" value="Choose File"/> No file chosen <input style="float: right;" type="button" value="Upload"/>
Save Settings to File	<input type="button" value="Save..."/>

---

### USB

Load Setting From File	USB storage is not exist! ▼	<input type="button" value="Restore"/>
Save Settings to USB	JetNet6628X-001277FF557	<input type="button" value="Save to USB"/>
Eject USB Disk	<input type="button" value="Eject"/>	

Click on upload 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 4.2.7.3 Backup/Restore Configuration – TFTP Server mode

### TFTP

IP	<input type="text"/>	
File Name	JetNet6628X-001277FF557	
Save and Reload Setting	Load ▼	<input type="button" value="Submit"/>

---

### SFTP

IP	<input type="text"/>	
File Name	JetNet6628X-001277FF557	
User Name	<input type="text" value="User Name"/>	
Password	<input type="text" value="Password"/>	
Save and Reload Setting	Load ▼	<input type="button" value="Submit"/>

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 will be automatically rebooted after you finished upgrading new firmware. Please remind the attached users before you do this.**

Figure 4.2.8.1 Main UI of Firmware Upgrade

The screenshot displays the 'Firmware Upgrade' interface. At the top, there is a title 'Firmware Upgrade' and a 'Help' button. Below this, the interface is divided into four sections: 'Local file', 'USB', 'TFTP', and 'SFTP'. Each section contains specific input fields and buttons for file selection and upgrade actions.

**Firmware Upgrade** [Help]

---

**Local file**

[Select File] [Choose File] No file chosen

[Upgrade] [Cancel]

---

**USB**

[Select File] USB storage is not exist! ▼

[Eject USB Disk] [Eject]

[Upgrade] [Cancel]

---

**TFTP**

[IP] [ ]

[File Name] [ ]

[Upgrade] [Cancel]

---

**SFTP**

[IP] [ ]

[Port] [ ]

[File Name] [ ]

[Name] [ ]

[Password] [ ]

[Upgrade] [Cancel]

There are 4 modes for users to backup/restore the configuration file, Local File mode ,USB Mode ,TFTP mode and SFTP 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.

**USB mode:** In this mode, user can upgrade FW via USB drive.

**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.

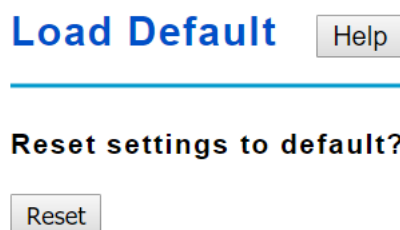
**SFTP Server mode:** In this mode, the switch acts as the SFTP client. Before you do so, make sure that your SFTP server is ready. And then please type the IP address of SFTP Server IP address, file name , password.

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 Load 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



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

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

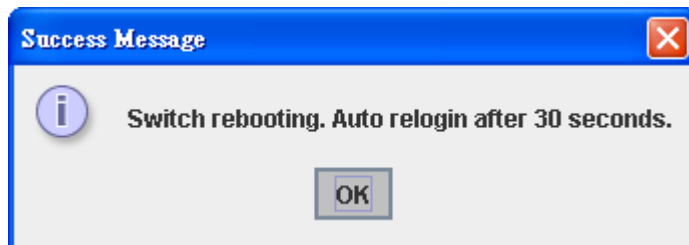
### Reboot

Do you want to reboot?

Yes

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..



#### 4.2.11 CLI Commands for Basic Setting

Feature	Command Line
<b>Switch Setting</b>	
System Name	Switch(config)# hostname WORD Network name of this system Switch(config)# hostname JN6628X Switch(config)#
System Location	Switch(config)# snmp-server location Taipei
System Contact	Switch(config)# snmp-server contact <a href="mailto:korecare@korenix.com">korecare@korenix.com</a>
Display	Switch# show snmp-server name Switch Switch# show snmp-server location Taipei

	<pre>Switch# show snmp-server contact korecare@korenix.com  Switch&gt; show version 0.31-20061218  Switch# show hardware mac MAC Address : 00:12:77:FF:01:B0</pre>
<b>Admin Password</b>	
User Name and Password	<pre>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.</pre>
Display	<pre>Switch# show administrator Administrator account information name: orwell password: orwell</pre>
<b>IP Configuration</b>	
IP Address/Mask (192.168.10.8, 255.255.255.0)	<pre>Switch(config)# int vlan 1 Switch(config-if)# ip address dhcp Switch(config-if)# ip address 192.168.10.8/24 Switch(config-if)# ip dhcp client Switch(config-if)# ip dhcp client renew</pre>
Gateway	<pre>Switch(config)# ip route 0.0.0.0/0 192.168.10.254/24</pre>
Remove Gateway	<pre>Switch(config)# no ip route 0.0.0.0/0 192.168.10.254/24</pre>
Display	<pre>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>
IPv6 Address/Prefix	<pre>Switch(config)# interface vlan1 Switch(config-if)# ipv6 address 2001:0db8:85a3::8a2e:0370:7334/64</pre>
IPv6 Gateway	<pre>Switch(config)# ipv6 route 0::0/0 2001:0db8:85a3::8a2e:0370:FFFFE</pre>
Remove IPv6 Gateway	<pre>Switch(config)#no ipv6 route 0::0/0 2001:0db8:85a3::8a2e:0370:FFFFE</pre>
Display	<pre>Switch# show running-config ..... interface vlan1 ip address 192.168.10.6/24 ipv6 address 2001:db8:85a3::8a2e:370:7334/64 no shutdown ! ip route 0.0.0.0/0 192.168.10.254</pre>

	<pre>ipv6 route ::/0 2001:db8:85a3::8a2e:370:ffe !</pre>
<b>Time Setting</b>	
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><b>Note:</b> 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 &lt;cr&gt; 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 Sun Jan 1 04:14:19 2006 (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London  Switch # show clock timezone clock timezone (26) (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London</pre>
<b>Jumbo Frame</b>	
Jumbo Frame	<pre>Switch(config)# system mtu jumbo &lt;1500-9216&gt; Switch(config)# system mtu jumbo 9000</pre>
<b>DHCP Server</b>	
DHCP Server configuration	<pre>Enable DHCP Server on JetNet Switch Switch# Switch# configure terminal Switch(config)# router dhcp Switch(config-dhcp)# service dhcp  Configure DHCP network address pool Switch(config-dhcp)#network 50.50.50.0/4 -( network/mask) Switch(config-dhcp)#default-router 50.50.50.1</pre>
Lease time configure	<pre>Switch(config-dhcp)#lease 300 (300 sec)</pre>
DHCP Relay Agent	<pre>Enable DHCP Relay Agent Switch# Switch# configure terminal</pre>

	<pre>Switch(config)# router dhcp Switch(config-dhcp)# service dhcp Switch(config-dhcp)# ip dhcp relay information option  Enable DHCP Relay policy Switch(config-dhcp)# ip dhcp relay information policy <u>replace</u> drop      Relay Policy keep      Drop/Keep/Replace option82 field replace</pre>
Show DHCP server information	<pre>Switch# show ip dhcp server statistics Switch# show ip dhcp server statistics DHCP Server ON Address Pool 1   network:192.168.17.0/24   default-router:192.168.17.254   lease time:300 Excluded Address List   IP Address ----- (list excluded address) Manual Binding List   IP Address      MAC Address ----- (list IP &amp; MAC binding entry) Leased Address List   IP Address      MAC Address      Leased Time Remains ----- (list leased Time remain information for each entry)</pre>
<b>Backup and Restore</b>	
Backup Startup Configuration file	<pre>Switch# copy startup-config tftp: 192.168.10.33/default.conf Writing Configuration [OK]</pre> <p><b>Note 1:</b> To backup the latest startup configuration file, you should save current settings to flash first. You can refer to 4.14 to see how to save settings to the flash.</p> <p><b>Note 2:</b> 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>
<b>Firmware Upgrade</b>	
Firmware Upgrade	<pre>Switch# archive download-sw /overwrite tftp 192.168.10.33 JN6628X.bin Firmware upgrading, don't turn off the switch! Tftping file JN6628X.bin Firmware upgrading ..... ..... ..... Firmware upgrade success!! Rebooting.....</pre>
<b>Factory Default</b>	

Factory Default	Switch# reload default-config file Reload OK! Switch# reboot
<b>System Reboot</b>	
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 Port Control

4.3.2 Port Status

4.3.3 Rate Control

4.3.4 Storm Control

4.3.5 Port Trunking

4.3.6 Command Lines for Port Configuration

### 4.3.1 Port Control

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

#### Port Control

Help

Port	State	Speed/Duplex	Flow Control	Description
1	Enable ▼	AutoNegotiation ▼	Disable ▼	
2	Enable ▼	AutoNegotiation ▼	Disable ▼	
3	Enable ▼	AutoNegotiation ▼	Disable ▼	
4	Enable ▼	AutoNegotiation ▼	Disable ▼	
5	Enable ▼	AutoNegotiation ▼	Disable ▼	
6	Enable ▼	AutoNegotiation ▼	Disable ▼	
7	Enable ▼	AutoNegotiation ▼	Disable ▼	
8	Enable ▼	AutoNegotiation ▼	Disable ▼	
9	Enable ▼	AutoNegotiation ▼	Disable ▼	
10	Enable ▼	AutoNegotiation ▼	Disable ▼	

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 1~24 (fa1~fa24) : 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 25~28: (gi25~gi28) : 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.

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.

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.*

### 4.3.2 Port Status

Port Status shows you current port status.

Figure 4.3.2.1 shows you the port status of the Gigabit Ethernet Ports, ex: Gigabit SFP Port 25, 26, 27 and 28. Also, it supports Small Form Factory (SFP) fiber transceiver with Digital Diagnostic Monitoring (DDM) function that provides real time information of SFP transceiver and allows user to diagnostic the optical fiber signal received and launched.

## Port Status

Help

Port	Link	State	Speed/Duplex	Flow Control	SFP Vendor	Wavelength	Distance
1	Up	Enable	1000 Full	Disable	---	---	---
2	Down	Enable	---	Disable	---	---	---
3	Down	Enable	---	Disable	---	---	---
4	Down	Enable	---	Disable	---	---	---
5	Down	Enable	---	Disable	---	---	---
6	Down	Enable	---	Disable	---	---	---
7	Down	Enable	---	Disable	---	---	---
8	Down	Enable	---	Disable	---	---	---
9	Down	Enable	---	Disable	---	---	---
10	Down	Enable	---	Disable	---	---	---

### SFP DDM

Port	SFP Scan/Eject	SFP DDM	Temperature (degree)		Tx Power (dBm)		Rx Power (dBm)	
			Current	Range	Current	Range	Current	Range
25	---	Enable	---	---	---	---	---	---
26	---	Enable	---	---	---	---	---	---
27	---	Enable	---	---	---	---	---	---
28	---	Enable	---	---	---	---	---	---

Reload

Apply

Scan All

Eject All



The description of the columns is as below:

**Port:** Port interface number.

**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.

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

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

**Eject:** Eject the DDM SFP transceiver. You can eject one port or eject all by click the icon "Eject All".

**Temperature:** The temperature, voltage 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 plugged DDM SFP transceiver is not certified by Korenix, the DDM function will not be supported. But the communication will not be disabled.**

#### 4.3.3 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 shows you the Limit Rate of Ingress and Egress. You can type the volume step by 64Kbps in the blank.

## Rate Control

Help

Port	Ingress Rule(Kbps)	Egress Rule(Kbps)
1	<input type="text" value="0"/>	<input type="text" value="0"/>
2	<input type="text" value="0"/>	<input type="text" value="0"/>
3	<input type="text" value="0"/>	<input type="text" value="0"/>
4	<input type="text" value="0"/>	<input type="text" value="0"/>
5	<input type="text" value="0"/>	<input type="text" value="0"/>
6	<input type="text" value="0"/>	<input type="text" value="0"/>
7	<input type="text" value="0"/>	<input type="text" value="0"/>
8	<input type="text" value="0"/>	<input type="text" value="0"/>
9	<input type="text" value="0"/>	<input type="text" value="0"/>
10	<input type="text" value="0"/>	<input type="text" value="0"/>

### 4.3.4 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.

## Storm Control

Help

Port	Broadcast	Rate(packet/sec)	DLF	Rate(packet/sec)	Multicast	Rate(packet/sec)
1	Disable ▼	<input type="text" value="0"/>	Disable ▼	<input type="text" value="0"/>	Disable ▼	<input type="text" value="0"/>
2	Disable ▼	<input type="text" value="0"/>	Disable ▼	<input type="text" value="0"/>	Disable ▼	<input type="text" value="0"/>
3	Disable ▼	<input type="text" value="0"/>	Disable ▼	<input type="text" value="0"/>	Disable ▼	<input type="text" value="0"/>
4	Disable ▼	<input type="text" value="0"/>	Disable ▼	<input type="text" value="0"/>	Disable ▼	<input type="text" value="0"/>
5	Disable ▼	<input type="text" value="0"/>	Disable ▼	<input type="text" value="0"/>	Disable ▼	<input type="text" value="0"/>
6	Disable ▼	<input type="text" value="0"/>	Disable ▼	<input type="text" value="0"/>	Disable ▼	<input type="text" value="0"/>
7	Disable ▼	<input type="text" value="0"/>	Disable ▼	<input type="text" value="0"/>	Disable ▼	<input type="text" value="0"/>
8	Disable ▼	<input type="text" value="0"/>	Disable ▼	<input type="text" value="0"/>	Disable ▼	<input type="text" value="0"/>
9	Disable ▼	<input type="text" value="0"/>	Disable ▼	<input type="text" value="0"/>	Disable ▼	<input type="text" value="0"/>
10	Disable ▼	<input type="text" value="0"/>	Disable ▼	<input type="text" value="0"/>	Disable ▼	<input type="text" value="0"/>

**Packet type:** You can assign the Rate for specific packet types based on packet number per second. The packet types of the Ingress Rule listed here include **Broadcast**, **DLF (Destination Lookup Failure)** and **Multicast**. Choose **Enable/Disable** to enable or

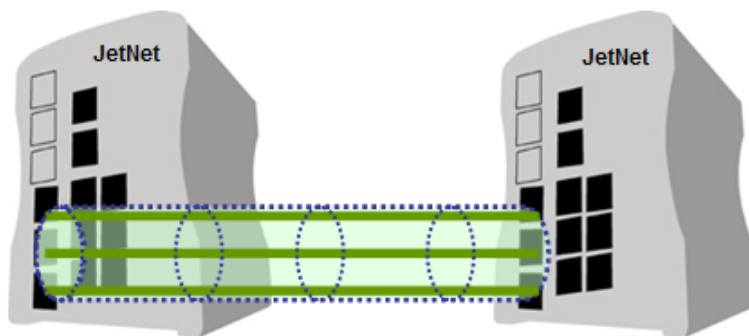
disable the storm control of specific port.

**Rate:** This column allows you to manually assign the limit rate of the port. The unit is packets per second. The limit range is from 1 to 262143 packet/sec, zero means no limit. The maximum available value of Fast Ethernet interface is 148810, this is the maximum packet number of the 100M throughput.

Enter the Rate field of the port you want assign, type the new value and click Enter key first. After assigned or changed the value for all the ports you want configure. [Click on Apply to apply the configuration of all ports.](#) The Apply command applied all the ports' storm control value, it may take some time and the web interface become slow, this is normal condition.

#### 4.3.5 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.

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

#### Aggregation Configuration

# Port Trunking - Aggregation Configuration

Help

## Aggregation Configuration

Port	Group ID	Trunk Type
1	1	Static
2	1	Static
3	2	LACP
4	2	LACP
5	0	
6	0	

**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, max groups for 100M ports would be 7, and 3 for gigabit ports.

**Group ID:** Group ID is the ID for the port trunking group. Ports with same group ID are in the same group.

**Trunk Type:** **Static** and **802.3ad LACP**. Each Trunk Group can only support Static or 802.3ad LACP. Choose the type you need here.

**Load Balance Type:** There are several load balance types based on dst-ip (Destination IP), dst-mac (Destination MAC), src-dst-ip (Source and Destination IP), src-dst-mac (Source and Destination MAC), src-ip (Source IP), src-mac (Source MAC).

## Load Balance Setting

Group ID	Type
1	src-dst-mac
2	src-mac dst-mac
3	src-dst-mac
4	src-ip dst-ip
5	src-dst-ip
6	src-dst-mac
7	src-dst-mac
8	src-dst-mac

Apply

Reload

## Aggregation Information

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

## Port Trunking - Aggregation Information

Help

Group ID	Type	Aggregated Ports	Individual Ports	Link Down Ports
1	N/A			
2	N/A			
3	N/A			
4	N/A			
5	N/A			
6	N/A			
7	N/A			
8	N/A			

Reload

**Group ID:** Display Trunk 1 to Trunk 8 set up in Aggregation Setting.

Type: Static or LACP set up in Aggregation Setting.

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

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

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

### 4.3.6 Command Lines for Port Configuration

Feature	Command Line
<b>Port Control</b>	
Port Control – State	<p>Switch(config-if)# shutdown -&gt; Disable port state            Port1 Link Change to DOWN            interface fastethernet1 is shutdown now.</p> <p>Switch(config-if)# no shutdown -&gt; Enable port state            Port1 Link Change to DOWN            Port1 Link Change to UP            interface fastethernet1 is up now.            Switch(config-if)# Port1 Link Change to UP</p> <p>Switch(config)# sfp            ddm Digital diagnostic and monitoring            Switch(config)# sfp ddm            Eject Reject DDM SFP            Switch(config)# sfp ddm eject → eject SFP DDM transceiver</p>

	<p>all All DDM interface  Example: Switch(config)# sfp ddm eject all  DDM SFP on Port 9 normally ejected.  DDM SFP on Port 9 normally ejected.  All DDM SFP normally ejected.</p> <p>Switch(config)# interface gigabitethernet10 → eject port 10  SFP DDM transceiver.  Switch(config-if)# sfp ddm eject  DDM SFP on Port 10 normally ejected.</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  Port1 Link Change to DOWN  set the speed mode ok!  Switch(config-if)# Port1 Link Change to UP</p> <p>Switch(config-if)# duplex full  Port1 Link Change to DOWN  set the duplex mode ok!  Switch(config-if)# Port1 Link Change to UP</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>
<b>Port Status</b>	
Port Status	<p>Switch# show interface fa1  Interface fastethernet1  Administrative Status : Enable  Operating Status : Connected  Duplex : Full  Speed : 100  Flow Control :off  Default Port VLAN ID: 1  Ingress Filtering : Disabled  Acceptable Frame Type : All  Port Security : Disabled  Auto Negotiation : Disable  Loopback Mode : None  STP Status: forwarding  Default CoS Value for untagged packets is 0.  Mdix mode is Disable.  Medium mode is Copper.</p> <p>Switch# show sfp ddm →show SFP DDM information  Port 8  Temperature:N/A  Tx power:N/A  Rx power:N/A  Port 9  Temperature:64.00 C &lt;range :0.0-80.00&gt;  Tx power:-6.0 dBm &lt;range : -9.0 - -4.0&gt;</p>

	<p>Rx power:-30.0 dBm &lt;range: -30.0 - -4.0&gt;  Port 10  Temperature:67.00 C &lt;range :0.0-80.00&gt;  Tx power:-6.0 dBm &lt;range : -9.0 - -4.0&gt;  Rx power:-2.0 dBm &lt;range: -30.0 - -4.0&gt;</p> <p><i>Note: Administrative Status -&gt; Port state of the port. Operating status -&gt; Current status of the port. Duplex -&gt; Duplex mode of the port. Speed -&gt; Speed mode of the port. Flow control -&gt; Flow Control status of the port.</i></p>
<b>Rate Control</b>	
Rate Control – Ingress or Egress	<p>Switch(config-if)# rate-limit  egress    Outgoing packets  ingress   Incoming packets</p> <p><b>Note: To enable rate control, you should select the Ingress or Egress rule first; then assign the packet type and bandwidth.</b></p>
Rate Control – Filter Packet Type	<p>Switch(config-if)# rate-limit ingress mode  all            Limit all frames  broadcast     Limit Broadcast frames  flooded-unicast Limit Broadcast, Multicast and flooded unicast frames  multicast     Limit Broadcast and Multicast frames</p> <p>Switch(config-if)# rate-limit ingress mode broadcast  Set the ingress limit mode broadcast ok.</p>
Rate Control – Bandwidth	<p>Switch(config-if)# rate-limit ingress bandwidth  &lt;0-100&gt;    Limit in magabits per second (0 is no limit)</p> <p>Switch(config-if)# rate-limit ingress bandwidth 8  Set the ingress rate limit 8Mbps for Port 1.</p>
<b>Storm Control</b>	
Strom Control – Packet Type	<p>Switch(config-if)# storm-control  broadcast :Broadcast packets  dlf :Destination Lookup Failure  multicast :Multicast packets</p>
Storm Contr–l - Rate	<p>Switch(config)# storm-control broadcast  &lt;0-100000&gt; Rate limit value 0~262143 packet/sec</p> <p>Switch(config)# storm-control broadcast 10000  limit_rate = 10000 packets/sec  Set rate limit for Broadcast packets.</p> <p>Switch(config)# storm-control multicast 10000  limit_rate = 10000 packets/sec  Set rate limit for Multicast packets.</p> <p>Switch(config)# storm-control dlf 10000  limit_rate = 10000 packets/sec  Set rate limit for Destination Lookup Failure packets.</p>
<b>Port Trunking</b>	
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></p>

	Note: different speed port can't be aggregated together.																				
Static Trunk	Switch(config)# trunk group 2 fa6-7 Trunk group 2 enable ok!																				
Display – LACP	etNet 6628X# show lacp internal LACP group 1 internal information: <table border="1"> <thead> <tr> <th>LACP Port</th> <th>Admin</th> <th>Oper</th> <th>Port</th> </tr> <tr> <th>Port</th> <th>Priority</th> <th>Key</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>8</td> <td>1</td> <td>8</td> <td>0x45</td> </tr> <tr> <td>9</td> <td>1</td> <td>9</td> <td>0x45</td> </tr> <tr> <td>10</td> <td>1</td> <td>10</td> <td>0x45</td> </tr> </tbody> </table> LACP group 2 is inactive LACP group 3 is inactive LACP group 4 is inactive	LACP Port	Admin	Oper	Port	Port	Priority	Key	State	8	1	8	0x45	9	1	9	0x45	10	1	10	0x45
LACP Port	Admin	Oper	Port																		
Port	Priority	Key	State																		
8	1	8	0x45																		
9	1	9	0x45																		
10	1	10	0x45																		
Display – Trunk	Switch# show trunk group 1 FLAGS: I -> Individual P -> In channel D -> Port Down  Trunk Group GroupID Protocol Ports -----+-----+----- 1 LACP 8(D) 9(D) 10(D) Switch# show trunk group 2 FLAGS: I -> Individual P -> In channel D -> Port Down  Trunk Group GroupID Protocol Ports -----+-----+----- 2 Static 6(D) 7(P) Switch#																				

## 4.4 Power over Ethernet

Power over Ethernet is one of the key features of *JetNet* 6628XP. It is fully IEEE802.3af-2003 compliant, and support IEEE802.3at, including 2-event and LLDP classification. *JetNet* 6628XP adopts up to 24-Port PoE injectors in port 1 to port 24.

The following commands are included in this section:

- 4.4.1 PoE Control
- 4.4.2 Emergency Power Management
- 4.4.3 PD Status Detection
- 4.4.4 PoE Scheduling
- 4.4.5 PoE Status
- 4.4.6 Command Line for PoE control

### 4.4.1 PoE Control

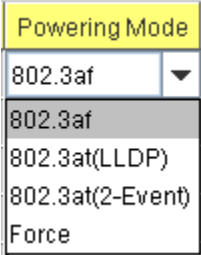
In WiMax systems, Wireless APs, and high-end PoE applications, there are various types of PDs, for instance, IEEE 802.3af, IEEE 802.3at 2-event, IEEE 802.3at LLDP, and



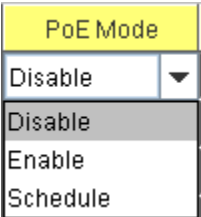
non-standard type. To be compatible with different PDs, *JetNet* 6628X series is the world's first rackmount High Power PoE switch, designed with 4 powering modes, including IEEE 802.3af mode, IEEE 802.3at 2-event mode, IEEE 802.3at LLDP classification mode as well as forced powering mode to meet all of the PD types in the industry. As a result, they can be flexibly used to deliver power for different PoE-enabled devices in various applications.

IEEE 802.3at LLDP provides smart power budget control behavior to fulfill the needs of higher end setups requiring exact high power delivery. By using the ongoing dynamic re-negotiation function of the IEEE802.3at LLDP, the *JetNet* 6628X series can perform more intelligently by dynamically reallocating power to the PDs. *JetNet* 6628X series implements the 2-event and Link Layer Discovery Protocol (LLDP) PoE into the system for efficient power budget negotiation between PSE and PD devices.

Pull down the **Powering Mode** column can change the Powering Mode to IEEE 802.3af, 802.3at(LLDP), 802.3at(2-Event) or forced mode. When the column is IEEE 802.3af, if and only if the PD is follow IEEE 802.3af then *JetNet* 6628X series could deliver power. If the Powering mode is 802.3at(LLDP) or 802.3at(2-Event), *JetNet* 6628X series would deliver power to PD that supports IEEE 802.3at LLDP or 2-Event feature. But if the Powering Mode changes to forced mode, once the PoE mode is enabled, the port will directly deliver power even there is no Ethernet cable plugged. Please be careful when using forced mode.



You can pull down the **PoE Mode** column to enable/disable ports, or set it to scheduling control mode.



The Power Budget can limit the consumption of poe and ensure the poe port can get the

pre-allocated power budget. The range of Power Budget is 0.4 to 32 Watt. The max effective power budget of 802.3af powering mode is 15.4 Watt even if the power budget is set to 32 Watts.

Power Budget(W)
32.0

Power Priority lets the poe port with higher priority can deplvery power under the limit power budget. There are three priorities (Critical, High and Low).

Power Priority
Critical ▼
Critical
High
Low

The following figure shows the Web UI interface for Power over Ethernet Control.

## Port Configuration

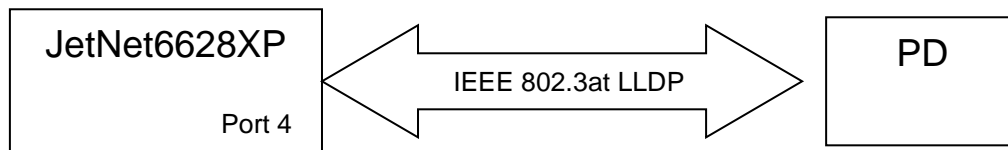
Port	Mode	Powering Mode	Budget(W)	Priority
1	Enable ▼	802.3at(2-Event) ▼	32.0	Critical ▼
2	Enable ▼	802.3at(2-Event) ▼	32.0	High ▼
3	Disable ▼	802.3af ▼	32.0	Low ▼
4	Enable ▼	802.3at(2-Event) ▼	32.0	Critical ▼
5	Disable ▼	802.3af ▼	32.0	High ▼
6	Disable ▼	802.3at(LLDP) ▼	32.0	Low ▼
7	Disable ▼	Forced ▼	32.0	High ▼
8	Disable ▼	802.3at(2-Event) ▼	32.0	High ▼
9	Disable ▼	802.3at(2-Event) ▼	32.0	High ▼
10	Disable ▼	802.3at(2-Event) ▼	32.0	High ▼

After configuring, please click the **Apply** button to enable and perform the configurations.



**DO NOT TOUCH DEVICE SURFACE DURING  
PoE PROGRESS HIGH POWER FEEDING**

Next, we illustrate how to configure IEEE 802.3at LLDP. Assume the PD is ready to the configuration for IEEE 802.3at LLDP, we only need to confirm JetNet6628X configuration.



For JetNet6628XP, enable the LLDP (refer to 4.12.5). By the port of JetNet6628XP connected to the PD (ex. Port 4), set **PoE Mode is Enable** and **Powering Mode is 802.3at(LLDP)**. When JetNet6628XP and the PD are ready to IEEE802.3at LLDP, IEEE 802.3at LLDP starts operation. Finally, see the result on **Poe Status** (refer to 4.4.5).

#### 4.4.2 Emergency Power Management

The *JetNet* 6628XP series is offered with dual power inputs for providing true network redundancy. An alarm relay output signals when a power input fails or other critical events occur. To ensure reliable power delivery, other advanced PoE power management features include individual port status monitoring, emergency power management (3 power supply indication inputs for quick shutdown of ports according to pre-defined priority table in cases where power supply failure occurs) and voltage/current monitoring and regulation. Power management allows the *JetNet* 6628XP to determine the exact power draw per port and to balance each port PoE power output accordingly. This, in turn, allows the switch to power higher and lower wattage devices according to user-definable parameters such as maximum available power, port priority (critical, high, low), and maximum allowable power per port. For the same level priority, the priority order is decided by port number.

You can configure the power budget and voltage of DC Power 1 and 2 by following Web GUI. The valid range of budget is 0 – 400 Watts (default is 0, and 0 mean power is disable). The valid range of power voltage is 46 - 57 V (default is 55 V). And the default power budget of inside AC power supply is 300 Watts and 53 V. Warning Water Level is used for power utilization monitoring, (valid range is 0 – 100 %, and 0 mean function is disable) If

the power utilization using is more than this water level, the warning event will happen.

## System Configuration

PoE System  ▾

Power DC1 Settings	
Budget(W)	<input type="text" value="0"/>
Voltage(V)	<input type="text" value="55"/>
Power DC2 Settings	
Budget(W)	<input type="text" value="0"/>
Voltage(V)	<input type="text" value="55"/>
System Warning	
Warning Water Level(%)	<input type="text" value="0"/>

### 4.4.3 PD Status Detection

*JetNet 6628XP* delivers a useful function – PD Status Detection. This provides automatic detection of a remote device powered by *JetNet 6628XP*. If the remote system crashes or is unstable, *JetNet 6628XP* will perform a system reboot by turning off and on again to trigger the remote device. The following figure shows the Web configure interface for Power over Ethernet PD Status Detection.

PD Status Detection  ▾

PD	IP Address	Cycle Time(s)
1	192.168.10.100	10
2	192.168.10.200	20
3	192.168.10.10	30
4	192.168.10.15	40
5		
6		
7		
8		
9		
10		

You can enable/disable PD Status Detection function and type in the IP address that you want to detect. The **Cycle Time** is the gap per detection. After configuring, please click the

**Apply** button to enable and perform the functions.

#### 4.4.4 PoE Scheduling

The PoE Scheduling control is a powerful function to help you save power and money. You need to configure **PoE Scheduling** and select a target port manually to enable this function.

### PoE Schedule

Help

PoE Schedule  on

Time	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
00:00	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
01:00	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
02:00	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
03:00	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
04:00	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
05:00	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
06:00	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
07:00	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
08:00	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
09:00	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

#### 4.4.5 PoE Status

The PoE Status page shows the operating status of each power and each PoE Port. The power information includes power input voltage and budget, power aggregation and redundancy status, Total Power budget, Total Output Power, Warning Water Level and Utilization. The PoE Port information includes PoE mode, Operation status, PD class, Power Consumption, Voltage and Current.

Power aggregation: if the powers are in the same priority level (primary, secondary or tertiary), the powers will be aggregated. Use the same voltage power will become power aggregation.

Power redundancy: if the powers are in the different priority level, the secondary power will be backup power for primary. The tertiary power will be backup power for primary or secondary.

## PoE Status

Help

<b>AC Power</b>	55 V, Budget 300 W
<b>DC1 Power</b>	55 V, Budget 0 W
<b>DC2 Power</b>	55 V, Budget 0 W
<b>Power Available</b>	AC
<b>Total Power Budget</b>	300 W
<b>Total Output Power</b>	0.0 W
<b>Warning Water Level</b>	---
<b>Utilization</b>	0 %
<b>Event</b>	Normal

Port	Mode	Status	Class	Budget(w)	Consumption(W)	Voltage(V)	Current(mA)
1	Disable	Off	---	---	0.0	0.0	0
2	Disable	Off	---	---	0.0	0.0	0
3	Disable	Off	---	---	0.0	0.0	0

### 4.4.6 Command Line for PoE control

<b>Syntax</b>	<b>show poe system</b>
<b>Parameters</b>	--
<b>Command Mode</b>	Enable mode
<b>Description</b>	Display the status of the PoE system.
<b>Examples</b>	<pre>Switch&gt; enable Switch# show poe system PoE System   PoE Admin : Enable   PoE Hardward : Normal   PoE Input Voltage :     Vmain 1 : 52.8 V     Vmain 2 : 53.0 V     Vmain 3 : 52.5 V   Ouput power : 0.0 Watts   Temperature 1 : 39 degree   Temperature 2 : 41 degree   Temperature 3 : 47 degree   Power information :     Budget :       DC Power 1 : 400 Watts (In Use)       DC Power 2 : 400 Watts       AC Power : 300 Watts (In Use)     Total : 1100 Watts       700 Watts in Use   Warning water level : N/A   Utilization : 0 %   Event : Normal</pre>

<b>Syntax</b>	<b>show poe interface IFNAME</b>
<b>Parameters</b>	IFNAME : interface name
<b>Command Mode</b>	Enable mode
<b>Description</b>	Display the PoE status of interface.
<b>Examples</b>	<pre>Switch&gt; enable Switch# show poe interface fa1 Interface fastethernet1 (POE Port 1)   Control Mode : User (Disable)   Powering Mode : 802.3af   Operation Status : Off   Detection Status : Valid   Classification : N/A   Priority : Highest   Output Power : 0.0 Watts, Voltage : 0.0 V, Current : 0 mA   Power Budget :     Budget : 32.0 Watts, effective 0 Watts     Warning water level : N/A     Utilization : 0 %     Event : Normal</pre>
<b>Syntax</b>	<b>show poe pd_detect</b>
<b>Parameters</b>	--
<b>Command Mode</b>	Enable mode
<b>Description</b>	Display the status of pd status detection.
<b>Examples</b>	<pre>Switch# show poe pd-detect PD Status Detection   Status : Enabled   Host 1 :     Target IP : 192.168.10.100     Cycle Time : 10   Host 2 :     Target IP : 192.168.10.200     Cycle Time : 20   Host 3 :     Target IP : 192.168.10.15     Cycle Time : 30   Host 4 :     Target IP : 192.168.10.20     Cycle Time : 40</pre>
<b>Syntax</b>	<b>show poe schedule IFNAME</b>
<b>Parameters</b>	IFNAME : interface name
<b>Command Mode</b>	Enable mode
<b>Description</b>	Display the status of schedule of interface.
<b>Examples</b>	<pre>Switch# show poe schedule fa1 Interface fastethernet1   POE Schedule     Status : Disable     Weekly Schedule :       Sunday : 0,1,2,3,4,5,6,7,8,19,20,21,22,23       Monday : 0,1,2,3,4,5,6,7,8,19,20,21,22,23       Tuesday : 0,1,2,3,4,5,6,7,8,19,20,21,22,23       Wednesday : 0,1,2,3,4,5,6,7,8,19,20,21,22,23</pre>

	Thursday : 0,1,2,3,4,5,6,7,8,19,20,21,22,23 Friday : 0,1,2,3,4,5,6,7,8,19,20,21,22,23 Saturday : 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20
<b>Syntax</b>	<b>poe powering-mode 802.3af/forced</b>
<b>Parameters</b>	802.3af: deliver power if and only if the attached PD comply with IEEE 802.3af forced: deliver power no matter what PD attached
<b>Command Mode</b>	Interface mode
<b>Description</b>	Set the Powering mode of PoE
<b>Examples</b>	EX 1: <i>Set 802.3af powering mode</i> Switch(config)# poe powering-mode 802.3af EX 2: <i>Set forced powering mode</i> Switch(config)# poe powering-mode forced
<b>Syntax</b>	<b>poe powering-mode 802.3at 2-event/lldp</b>
<b>Parameters</b>	2-event: deliver power if and only if the attached PD comply with IEEE 802.3at physical layer classification lldp: deliver power if and only if the attached PD comply with IEEE 802.3at data link layer classification
<b>Command Mode</b>	Interface mode
<b>Description</b>	Set the Powering mode of PoE
<b>Examples</b>	EX 1: <i>Set 802.3at 2-event powering mode</i> Switch(config)# poe powering-mode 802.3at 2-event EX 2: <i>Set 802.3at lldpforced powering mode</i> Switch(config)# poe powering-mode 802.3at lldp
<b>Syntax</b>	<b>poe control-mode user/schedule</b>
<b>Parameters</b>	user: user mode schedule: schedule mode
<b>Command Mode</b>	Interface mode
<b>Description</b>	Set the control mode of port
<b>Examples</b>	Set PoE port 2 to user mode. EX 1: Switch(config)# interface fa2 Switch(config-if)# poe control-mode user Set PoE port 2 to schedule mode. EX 2: Switch(config-if)# poe control-mode schedule
<b>Syntax</b>	<b>poe user enable/disable</b>
<b>Parameters</b>	enable: enable port in user mode disable: disable port in user mode
<b>Command Mode</b>	Interface mode
<b>Description</b>	Enable/Disable the PoE of the port in user mode. If in schedule mode, it will come into affect when the control mode changes to user mode.
<b>Examples</b>	To enable the PoE function in user mode Switch(config-if)# poe user enable To disable the PoE function in user mode Switch(config-if)# poe user disable
<b>Syntax</b>	<b>poe type TYPE</b>
<b>Parameters</b>	TYPE : port type string with max 20 characters



<b>Command Mode</b>	Interface mode
<b>Description</b>	Set the port type string.
<b>Examples</b>	Set the type string to "IPCam-1. Switch(config-if)# poe type IPCam-1
<b>Syntax</b>	<b>poe budget [POWER]</b>
<b>Parameters</b>	PO ER : 0.4 – 32
<b>Command Mode</b>	Interface mode
<b>Description</b>	Set the port budget. The max budget is different between 802.3af, 802.3at and forced powering mode. The max budget of 802.3af powering mode is 15.4. The max budget of 802.3at powering mode is 32. The max budget of force powering mode is 32.
<b>Examples</b>	Set the max value of power consumption to 12 W with manual mode. Switch(config-if)# poe budget 12
<b>Syntax</b>	<b>poe budget warning &lt;0-100&gt;</b>
<b>Parameters</b>	<0-100> 0 is disable, valid range is 1 to 100 percentage
<b>Command Mode</b>	Interface mode
<b>Description</b>	Set the warning water level of port budget.
<b>Examples</b>	Set the warning water level to 60% Switch(config-if)# poe budget warning 60
<b>Syntax</b>	<b>poe priority critical/high/low</b>
<b>Parameters</b>	Critical : Hightest priority level High : High priority level Low : Low priority level
<b>Command Mode</b>	Interface mode
<b>Description</b>	Set the powering priority. The port with higher priority will have the privilege to delivery power under limited power situation.
<b>Examples</b>	Set the priority to critical Switch(config-if)# poe priority critical
<b>Syntax</b>	<b>poe schedule weekday hour</b>
<b>Parameters</b>	Weekday : Valid range 0-6 (0=Sunday, 1=Monday, ..., 6=Saturday) Hour : Valid range 0-23, Valid format a,b,c-d
<b>Command Mode</b>	Interface mode
<b>Description</b>	Add a day schedule to an interface.
<b>Examples</b>	Add a schedule which enables PoE function at hour 1, 3, 5 and 10 to 23 on Sunday. Switch(config-if)# poe schedule 0 1,3,5,10-23
<b>Syntax</b>	<b>no poe schedule weekday</b>
<b>Parameters</b>	Weekday : Valid range 0-6 (0=Sunday, 1=Monday, ..., 6=Saturday)
<b>Command Mode</b>	Interface mode
<b>Description</b>	Remove a day schedule
<b>Examples</b>	Remove the Sunday schedule. Switch(config-if)# no poe schedule 0

<b>Syntax</b>	<b>poe budget DC1/DC2 [POWER]</b>
<b>Parameters</b>	DC1 : DC 1 power input DC2 : DC 2 power input POWER : 1 – 400
<b>Command Mode</b>	Configuration mode
<b>Description</b>	Set the power budget of DC1 or DC2
<b>Examples</b>	Set the power budget of DC1 to 400W Switch(config)# poe budget DC1 400
<b>Syntax</b>	<b>poe budget warning &lt;0-100&gt;</b>
<b>Parameters</b>	<0-100> 0 is disable, valid range is 1 to 100 percentage
<b>Command Mode</b>	Configuration mode
<b>Description</b>	Set the warning water level of total power budget.
<b>Examples</b>	Set the warning water level to 60% Switch(config-if)# poe budget warning 60
<b>Syntax</b>	<b>poe pd_detect enable/disable</b>
<b>Parameters</b>	enable: enable PD Status Detection function disable: disable PD Status Detection function
<b>Command Mode</b>	Configuration mode
<b>Description</b>	Enable/Disable the PD Status Detection function
<b>Examples</b>	To enable the function of pd status detect function Switch(config)# poe pd_detect enable To disable the function of pd status detect function Switch(config)# poe pd_detect disable
<b>Syntax</b>	<b>poe pd_detect ip_address cycle_time</b>
<b>Parameters</b>	IP address : A.B.C.D Cycle time : Valid range 10-3600 second and must be multiple of 10
<b>Command Mode</b>	Configuration mode
<b>Description</b>	Apply a rule of PD Status Detection.
<b>Examples</b>	Apply a rule which ping 192.160.1.2 per 20 seconds. And if 192.160.1.2 is timeout, pd status detection will re-enable the PoE. Switch(config)# poe pd_detect 192.160.1.2 20

## 4.5 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 6628X 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* 3<sup>rd</sup> 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:

4.5.1 STP Configuration

4.5.2 STP Port Configuration

4.5.3 STP Information

4.5.4 MSTP Configuration

4.5.5 MSTP Port Configuration

4.5.6 MSTP information

4.5.7 Multiple Super Ring

4.5.8 Multiple Super Ring Information

4.5.9 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.

#### 4.5.1 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.

**STP Configuration**

---

**STP Mode**  ▾  
Disable  
STP  
**RSTP**  
MSTP

<b>Bridge Address</b>	012.7700.1277
<b>Bridge Priority</b>	32768 ▾
<b>Max Age</b>	20 ▾
<b>Hello Time</b>	2 ▾
<b>Forward Delay</b>	15 ▾

#### **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 parameters.

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

#### 4.5.2 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 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 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

Help

Port	STP State	Path Cost	Port Priority	Link Type	Edge Port
1	Enable ▼	20000	128 ▼	Auto ▼	Enable ▼
2	Enable ▼	20000	128 ▼	Auto ▼	Enable ▼
3	Enable ▼	20000	128 ▼	Auto ▼	Enable ▼
4	Enable ▼	20000	128 ▼	Auto ▼	Enable ▼
5	Enable ▼	20000	128 ▼	Auto ▼	Enable ▼
6	Enable ▼	20000	128 ▼	Auto ▼	Enable ▼
7	Enable ▼	20000	128 ▼	Auto ▼	Enable ▼
8	Enable ▼	20000	128 ▼	Auto ▼	Enable ▼
9	Enable ▼	20000	128 ▼	Auto ▼	Enable ▼
10	Enable ▼	20000	128 ▼	Auto ▼	Enable ▼

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

### 4.5.3 STP Information

## STP Information

Help

### Root Information

Root Address	0012.7700.1277
Root Priority	32768
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	Aggregated(ID/Type)
1	Disabled	Forwarding	20000	128	P2P	Edge	/
2	Disabled	Disabled	20000	128	P2P	Edge	/
3	Disabled	Disabled	20000	128	P2P	Edge	/
4	Disabled	Disabled	20000	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).

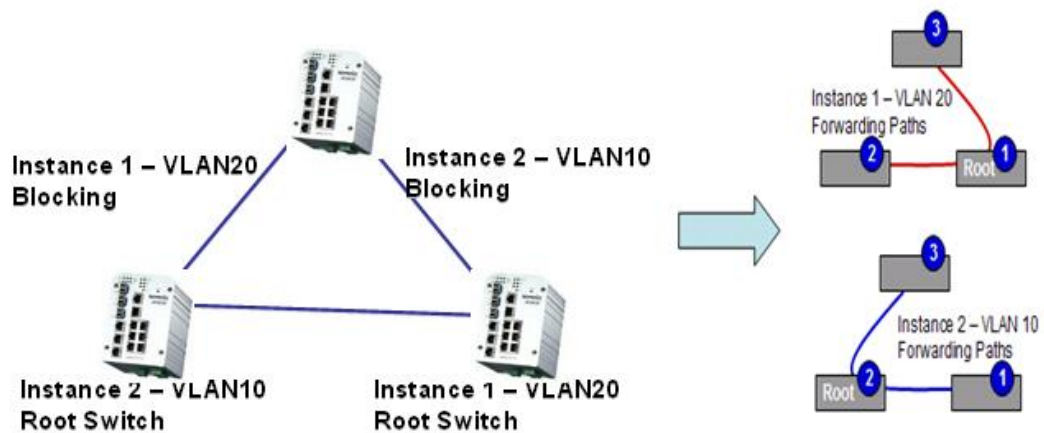
### 4.5.4 MSTP (Multiple Spanning Tree Protocol) Configuration

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.

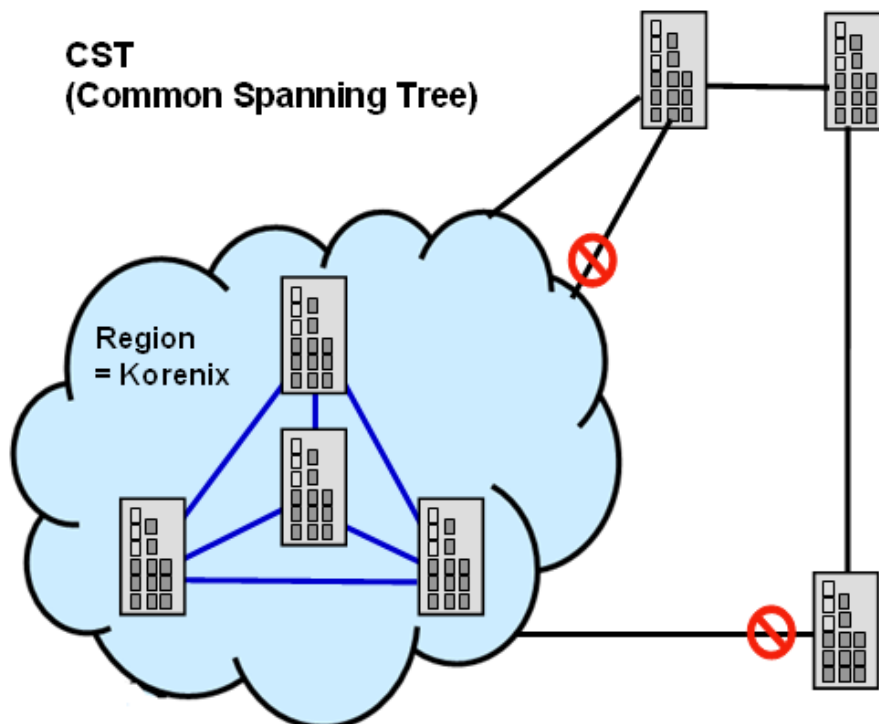
One VLAN can be mapped to a Multiple Spanning Tree Instance (MSTI). For example, the maximum Instance JetNet supports is usually 16, range from 0-15. The MSTP builds a separate Multiple Spanning Tree (MST) for each instance to maintain connectivity among each of the assigned VLAN groups. An Internal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



## MSTP Configuration Help

---

### MST Region Configuration

Region Name	<input type="text"/>
Revision	<input type="text"/>

---

### Add MST Instance

Instance ID	<input type="text"/>
VLAN Group	<input type="text"/>
Instance Priority	<input type="text"/>

---

### MST Instance Configuration

Instance ID	VLAN Group	Instance Priority
<input type="text"/>	<input type="text"/>	<input type="text"/>

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.

**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.

## 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.

### 4.5.5 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

**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.

#### 4.5.6 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.

#### 4.5.7 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* 3<sup>rd</sup> 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 6628X* 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 6628X. 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
1	

Add

### 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

Apply Remove Reload

### 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 1<sup>st</sup> 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 3<sup>rd</sup> generation Ring redundancy technology. When you want to connect multiple RSR or form redundant topology with other vendors, RDH could allow you to have maximum 7 multiple links for redundancy without any problem.

In Dual Homing I released with 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 6628X.

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.

#### 4.5.8 Multiple Super Ring Information

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.

### 4.5.9 ERPS Configuration:

Ethernet Ring Protection Switching, or ERPS, is an effort at ITU-T under G.8032 Recommendation to provide sub-50ms protection and recovery switching for Ethernet traffic in a ring topology and at the same time ensuring that there are no loops formed at the Ethernet layer.

## ERPS Configuration

Help

### Add ERPS Instance

Instance ID	VLAN group
0 ▼	<input type="text"/>

Add

### ERPS Instance Configuration

Instance ID	VLAN group
<input type="checkbox"/> 1	1

Apply

Remove Selected

Cancel

### Add ERPS Ring

Ring ID

### ERPS Ring Configuration

Ring ID	Version	Ring State	Node Role	Control Channel	Sub Ring Without Virtual Channel	Virtual Channel of Sub Ring	Ring Port 1	Ring Port 2	Ring Port 1 RMEP ID	Ring Port 2 RMEP ID	RPL port	Revertive Mode	Instance	Manual Switch	Force Switch

### ERPS Timer Configuration

Ring ID	Guard Timer	WTR Timer

**ERPS:** Enable or disable ERPS function.

### ERPS Configuration:

**Version:** ERPS has version 1 and 2. Now we just support ERPSv1

**Node State:** The current state of the node, Idle and Protection.

**Node Role:** The role of the node, RPL owner and Ring node. The RPL owner is an Ethernet ring node adjacent to the RPL.

**Control Channel:** Control Channel provide a communication channel for ring automatic protection switching (R-APS) information.

**Ring Port:** A ring link is bounded by two adjacent nodes and a port for a ring link is called a ring port.

**RPL Port:** The ring protection link (RPL) is the ring link which under normal conditions, i.e., without any failure or request, is blocked for traffic channel, to prevent the formation of loops.

### 4.5.10 Command Lines:

Feature	Command Line
<b>Global (STP, RSTP, MSTP)</b>	
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
<b>MSTP</b>	
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 dleay time hello-time the hello time max-age the message maximum age time max-hops the maximum hops sync sync port state of exist vlan entry Switch(config)# spanning-tree mst configuration Switch(config)# spanning-tree mst configuration Switch(config-mst)# abort exit current mode and discard all changes end exit current mode, change to enable mode and apply all changes exit exit current mode and apply all changes instance the mst instance list Print command list name the name of mst region no Negate a command or set its defaults quit exit current mode and apply all changes revision the revision of mst region show show mst configuration
Region Configuration	Region Name: Switch(config-mst)# name NAME the name string Switch(config-mst)# name korenix Region Revision: Switch(config-mst)# revision <0-65535> the value of revision Switch(config-mst)# revision 65535
Mapping Instance to VLAN (Ex: Mapping VLAN 2 to Instance 1)	Switch(config-mst)# instance <1-15> target instance number Switch(config-mst)# instance 1 vlan VLANMAP target vlan number(ex.10) or range(ex.1-10) Switch(config-mst)# instance 1 vlan 2
Display Current MST Configuraion	Switch(config-mst)# show current Current MST configuration Name [korenix] Revision 65535 Instance Vlans Mapped ----- 0 1,4-4094 1 2 2 3



	----- Config HMAC-MD5 Digest: 0xB41829F9030A054FB74EF7A8587FF58D -----
Remove Region Name	Switch(config-mst)# no name name configure revision revision configure instance the mst instance Switch(config-mst)# no name
Remove Instance example	Switch(config-mst)# no instance <1-15> target instance number Switch(config-mst)# no instance 2
Show Pending MST Configuration	Switch(config-mst)# show pending Pending MST configuration Name [] (->The name is removed by no name) Revision 65535 Instance Vlans Mapped ----- 0 1,3-4094 1 2 (->Instance 2 is removed by no instance 2) ----- Config HMAC-MD5 Digest: 0x3AB68794D602FDF43B21C0B37AC3BCA8 -----
Apply the setting and go to the configuration mode	Switch(config-mst)# quit apply all mst configuration changes Switch(config)#
Apply the setting and go to the global mode	Switch(config-mst)# end apply all mst configuration changes Switch#
Abort the Setting and go to the configuration mode.  Show Pending to see the new settings are not applied.	Switch(config-mst)# abort discard all mst configuration changes Switch(config)# spanning-tree mst configuration Switch(config-mst)# show pending Pending MST configuration Name [korenix] (->The 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 -----
<b>RSTP</b>	
System RSTP Setting	The mode should be rst, the timings can be configured in global settings listed in above.
<b>Global Information</b>	
<b>Active Information</b>	Switch# show spanning-tree active Spanning-Tree : Enabled Protocol : MSTP Root Address : 0012.77ee.eeee Priority : 32768 Root Path Cost : 0 Root Port : N/A Root Times : max-age 20, hello-time 2, forward-delay 15 Bridge Address : 0012.77ee.eeee Priority : 32768 Bridge Times : max-age 20, hello-time 2, forward-delay 15

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

	<pre> ----- 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>
<b>Multiple Super Ring</b>	
Create or configure a Ring	<pre> Switch(config)# multiple-super-ring 1 Ring 1 created Switch(config-multiple-super-ring)# <b>Note: 1 is the target Ring ID which is going to be created or configured.</b> </pre>
Super Ring Version	<pre> Switch(config-multiple-super-ring)# version any-ring any ring auto detection 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 &lt;0-255&gt; valid range is 0 to 255 default set default </pre>

	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..
<b>Ring Info</b>	
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.
<b>ERPS</b>	
show erps	Switch# show erps Ethernet Ring Protection Switching (ITU-T G.8032) Version : v1 Ring State : Disabled Node State : Disabled Node Role : Ring Node Control Channel : VLAN 1 Ring Port 1 : fa1 is Link Down and Blocking

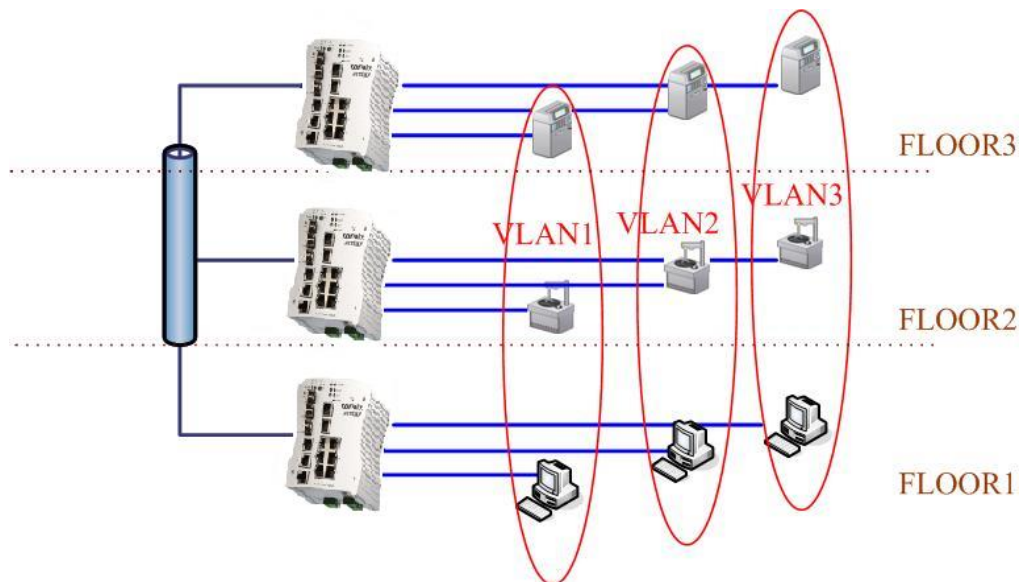
	<pre> Ring Port 2      : fa2 is Link Down and Blocking RPL Port        : Ring Port 2 Timers   WTR Timer      : period is 1 minutes, timer is not running, remains 0 ms   Guard Timer    : period is 100 ms, timer is not running, remains 0 ms Statistics   R-APS(SF)     : sent 0, received 0   R-APS(NR,RB) : sent 0, received 0   R-APS(NR)     : sent 0, received 0   Node State Transition count 0 Switch# </pre>
Configure ERPS	<pre> Switch(config)# erps   enable          Start the Multiple Super Ring for the switch   disable         Stop the Multiple Super Ring for the switch   version         the protocol version   node-role       The node role of ERPS node   ring-port       The ring port1 and port2 of the ERPS   rpl             The ring Ring Protection Link of the ERPS   control-channel The ring control channel of the ERPS   timer          The period of timer  Switch(config)# erps en   enable Start the Multiple Super Ring for the switch Switch(config)# erps version   1      version 1   default Set default to version 1 Switch(config)# erps version   1      version 1   default Set default to version 1 Switch(config)# erps node-role   rpl-owner ERPS RPL Owner   ring-node ERPS ring node Switch(config)# erps ring-port   PORT1 The ring port 1 Switch(config)# erps rpl   ring-port Assign ring port as RPL Switch(config)# erps control-channel   &lt;1-4095&gt; The VLAN ID of control channel, valid range is from 1 to 4094 Switch(config)# erps timer   wtr-timer WTR(Wait-to-restore) Timer   guard-timer Guard Timer </pre>

## 4.6 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.

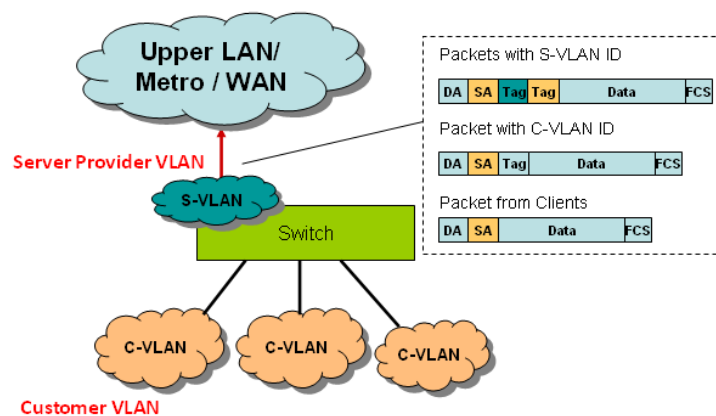
JetNet 6628X Series Industrial Ethernet Switch supports 802.1Q VLAN. 802.1Q VLAN is also known as Tag-Based VLAN. This Tag-Based VLAN allows VLAN to be created across different switches. IEEE 802.1Q tag-based VLAN makes use of VLAN control information stored in a VLAN header attached to IEEE 802.3 packet frames. This tag contains a VLAN Identifier (VID) that indicates which VLAN a frame belongs to. Since each switch only has to check a frame’s tag, without the need to dissect the contents of the frame, this also saves a lot of computing resources within the switch.

Figure 4.6.1 802.1Q 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 switch 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 QinQ, port Ingress/Egress parameters and view VLAN table.

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:

- 4.6.1 VLAN Port Configuration
- 4.6.2 VLAN Configuration
- 4.6.3 GVRP Configuration
- 4.6.4 VLAN Table
- 4.6.5 CLI Commands of the VLAN

#### 4.6.1 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.

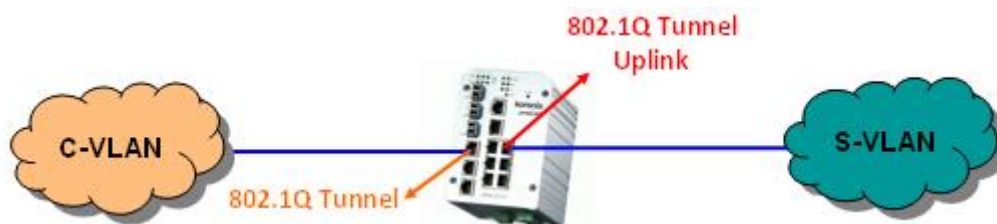
Figure 4.6.1.1 Web UI of VLAN configuration.

Port	PVID	Tunnel Mode	EtherType	Accept Frame Type	Ingress Filtering
1	1	None	0x8100	Admit All	Disable
2	1	None	0x8100	Admit All	Disable
3	1	None	0x8100	Admit All	Disable
4	1	None	0x8100	Admit All	Disable
5	1	None	0x8100	Admit All	Disable
6	1	None	0x8100	Admit All	Disable
7	1	None	0x8100	Admit All	Disable
8	1	None	0x8100	Admit All	Disable
9	1	None	0x8100	Admit All	Disable
10	1	None	0x8100	Admit All	Disable
11	1	None	0x8100	Admit All	Disable
12	1	None	0x8100	Admit All	Disable

**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:** Remian 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.

## 4.6.2 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 4.6.2.1 Web UI of the VLAN Configuration.

The screenshot displays the web UI for VLAN Configuration. On the left is a navigation tree with 'VLAN Configuration' selected. The main panel is titled 'VLAN Configuration' and contains a 'Help' button. Below this, there are two main sections: 'Static VLAN' and 'Static VLAN Configuration'. The 'Static VLAN' section features a table with columns 'VLAN ID' and 'Name', and an 'Add' button. The 'Static VLAN Configuration' section features a table with columns 'VLAN ID', 'Name', and 19 columns for ports (1-19), each with a dropdown menu. The table shows VLAN 1 with name 'VLAN1' and all ports set to 'U'. There are 'Apply', 'Remove Selected', and 'Reload' buttons at the bottom.

**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).

Figure 4.6.2.2 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 4.6.2.3

### Static VLAN

VLAN ID	Name
<input type="text" value="2"/>	<input type="text" value="Test"/>

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 6628X only support max 64 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 4.6.2.3 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
<input type="checkbox"/> 1	VLAN1	U ▼	U ▼	U ▼	U ▼	U ▼	U ▼	U ▼	U ▼

-- : 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.

#### 4.6.3 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.

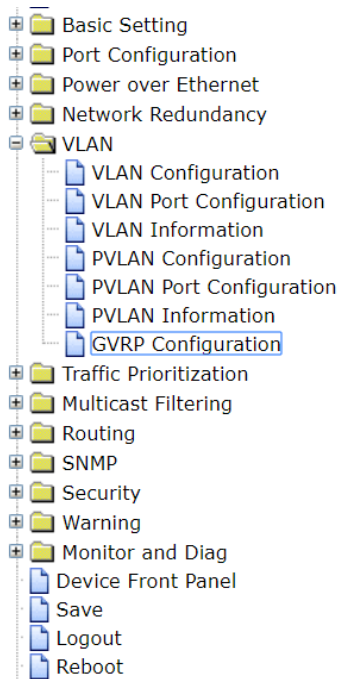
**Primary:** The VLAN is the Primary VLAN. The member ports can communicate with secondary ports.

**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.

#### 4.6.4 GVRP configuration

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



## GVRP Configuration

Help

GVRP Protocol Disable ▾

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

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

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

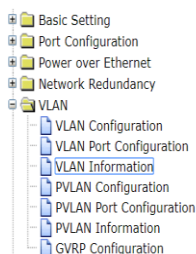
**Join Timer:** Controls the interval of sending the GVRP Join BPDU. An instance of this timer is required on a per-Port, per-GARP Participant basis

**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

### 4.6.5 VLAN Information

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



## VLAN Information

Help

VLAN ID	Name	Status	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
1	VLAN1	Static	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	

Reload

**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.

#### 4.6.6 CLI Commands of the VLAN

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

Feature	Command Line
<b>VLAN Port Configuration</b> (Go to the port interface configuration mode first.)	
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
<b>QinQ Tunnel Mode</b>  802.1Q Tunnel = access  802.1Q Tunnel Uplink = uplink	Switch(config-if)# switchport dot1q-tunnel mode Set the interface as an IEEE 802.1Q tunnel mode Switch(config-if)# switchport dot1q-tunnel mode access Set the interface as an access port of IEEE 802.1Q tunnel mode 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 vlan - success
Egress rule – Tagged (for VLAN 2)	Switch(config-if)# switchport trunk allowed vlan add 2
Display – Port Ingress Rule (PVID, Ingress Filtering, Acceptable Frame Type)	Switch# show interface fa1 Interface fastethernet1 Administrative Status : Enable Operating Status : Not Connected Duplex : Auto Speed : Auto Flow Control :off Default Port VLAN ID: 2 Ingress Filtering : Disabled Acceptable Frame Type : All Port Security : Disabled Auto Negotiation : Enable Loopback Mode : None STP Status: disabled

	<p>Default CoS Value for untagged packets is 0.  Mdx mode is Auto.  Medium mode is Copper.</p>
<p>Display – Port Egress Rule (Egress rule, IP address, status)</p>	<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>
<p>QinQ Information – 802.1Q Tunnel</p>	<pre>Switch# show dot1q-tunnel dot1q-tunnel mode port 1 : normal port 2 : normal port 3 : normal port 4 : normal port 5 : access port 6 : uplink port 7 : normal port 8 : normal port 9 : normal port 10 : normal</pre>
<p>QinQ Information – Show Running</p>	<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   switchport trunk allowed vlan add 10   switchport dot1q-tunnel mode uplink !</pre>
<p><b>VLAN Configuration</b></p>	
<p>Create VLAN (2)</p>	<pre>Switch(config)# vlan 2 vlan 2 success  Switch(config)# interface vlan 2 Switch(config-if)#</pre> <p><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></p>
<p>Remove VLAN</p>	<pre>Switch(config)# no vlan 2</pre>

	<p>no vlan success</p> <p><i>Note: You can only remove the VLAN when the VLAN is in unused mode.</i></p>
VLAN Name	<p>Switch(config)# vlan 2 vlan 2 has exists Switch(config-vlan)# name v2</p> <p>Switch(config-vlan)# no name</p> <p><i>Note: Use no name to change the name to default name, VLAN VID.</i></p>
VLAN description	<p>Switch(config)# interface vlan 2 Switch(config-if)# Switch(config-if)# description this is the VLAN 2</p> <p>Switch(config-if)# no description -&gt;Delete the description.</p>
IP address of the VLAN	<p>Switch(config)# interface vlan 2 Switch(config-if)# Switch(config-if)# ip address 192.168.10.18/24</p> <p>Switch(config-if)# no ip address 192.168.10.8/24 -&gt;Delete the IP address</p>
Create multiple VLANs (VLAN 5-10)	Switch(config)# interface vlan 5-10
Shut down VLAN	<p>Switch(config)# interface vlan 2 Switch(config-if)# shutdown</p> <p>Switch(config-if)# no shutdown -&gt;Turn on the VLAN</p>
Display – VLAN table	<pre>Switch# sh vlan 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</pre>
Display – VLAN interface information	<pre>Switch# show interface vlan1 interface vlan1 is up, line protocol detection is disabled index 14 metric 1 mtu 1500 &lt;UP,BROADCAST,RUNNING,MULTICAST&gt; 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</pre>
<b>GVRP configuration</b>	
GVRP enable/disable	<p>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!</p>
Configure GVRP timer Join timer /Leave timer/ LeaveAll timer	<p>Switch(config)# inter fa1 Switch(config-if)# garp timer &lt;10-10000&gt; Switch(config-if)# garp timer 20 60 1000 <i>Note: The unit of these timer is centisecond</i></p>
<b>Management VLAN</b>	
Management VLAN	Switch(config)# int vlan 1 (Go to management VLAN)

	Switch(config-if)# no shutdown
Display	Switch# show running-config ..... ! interface vlan1 ip address 192.168.10.17/24 ip igmp no shutdown ! .....

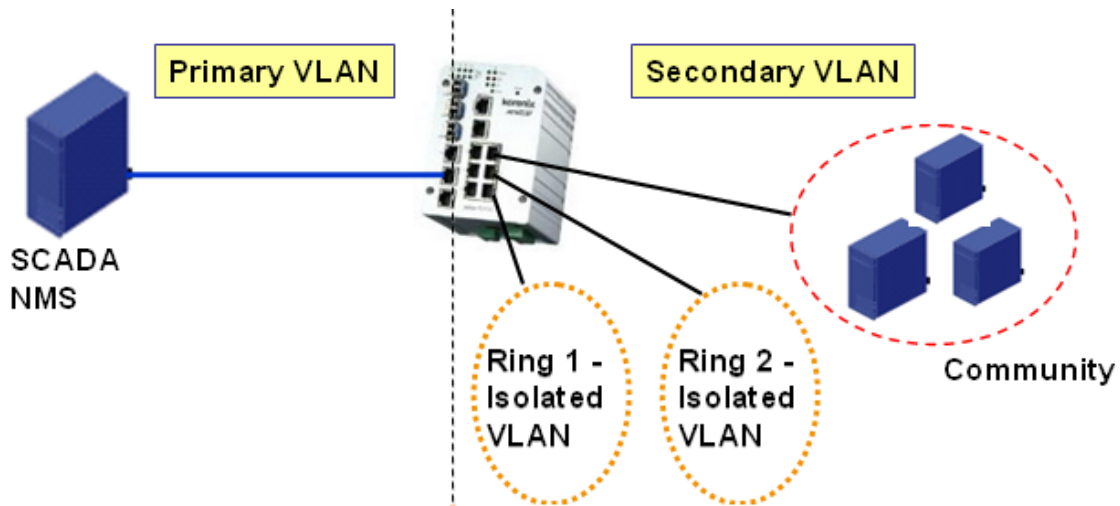
## 4.7 Private VLAN

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:

4.7.1 PVLAN Configuration

4.7.2 PVLAN Port Configuration

4.7.3 CLI Commands of the PVLAN

### 4.7.1 PVLAN Configuration

PVLAN Configuration allows you to assign Private VLAN type. After created VLAN in VLAN Configuraiton 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.

#### 4.7.2 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 Type :**

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

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

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

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

For example:

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

**2. Private VLAN Type:** VLAN 2-5 has its Private VLAN Type configured in Private VLAN Configuration page.

VLAN 2 is belonged to Primary VLAN.

VLAN 3-5 are belonged to secondary VLAN (Isolated or Community).

**3. Private VLAN Association:** Associate VLAN 3-5 to VLAN 2 in Private VLAN Association first.

##### **4. Private VLAN Port Configuraiton**

VLAN 2 – Primary -> The member port of VLAN 2 is promiscuous port.

VLAN 3 – Isolated -> The Host port can be mapped to VLAN 3.

VLAN 4 – Community -> The Host port can be mapped to VLAN 3.

VLAN 5 – Community -> The Host port can be mapped to VLAN 3.

##### **5. Result:**

VLAN 2 -> VLAN 3, 4, 5; member ports can communicate with ports in secondary VLAN.

VLAN 3 -> VLAN 2, member ports are isolated, but it can communicate with member port of VLAN 2..

VLAN 4 -> VLAN 2, member ports within the community can communicate with each other and communicate with member port of VLAN 2.

VLAN 5 -> VLAN 2, member ports within the community can communicate with each other and communicate with member port of VLAN 2.

## PVLAN Port Configuration

Help

### Port Configuration

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

### 4.7.3 Private VLAN Information

This page allows you to see the Private VLAN information.

## PVLAN Information

Help

Primary VLAN	Secondary VLAN	Secondary VLAN Type	Port

Reload

### 4.7.4 CLI Command of the PVLAN

Command Lines of the Private VLAN configuration

Feature	Command Line
<b>Private VLAN Configuration</b>	
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	<b>Go to the VLAN you want configure first.</b> Switch(config)# vlan (VID)
Choose the Types	Switch(config-vlan)# private-vlan

	<p>community Configure the VLAN as an community private VLAN</p> <p>isolated Configure the VLAN as an isolated private VLAN</p> <p>primary Configure the VLAN as a primary private VLAN</p>
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>
<b>Private VLAN Port Configuraiton</b>	
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
Promiscuous Port Type	Switch(config-if)# switchport mode private-vlan host Set the mode to private-vlan host promiscuous Set the mode to private-vlan promiscuous
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
<b>Private VLAN Information</b>	
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)

	<pre> 2      4      Community    gi10(P),gi8(C) 2      5      Community    gi10(P),fa7(C),gi9(I) 10     -      -              - </pre>
PVLAN Type	<pre> Switch# show vlan private-vlan type 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 ! Private VLAN Type vlan 2 private-vlan primary ! vlan 3 private-vlan isolated ! vlan 4 private-vlan community ! vlan 5 private-vlan community ! ..... ..... Private VLAN Port Information interface fastethernet7 switchport access vlan add 2,5 switchport trunk native vlan 5 switchport mode private-vlan host switchport private-vlan host-association 2 5 ! interface gigabitethernet8 switchport access vlan add 2,4 switchport trunk native vlan 4 </pre>

```
switchport mode private-vlan host
switchport private-vlan host-association 2 4
!
interface gigabitethernet9
  switchport access vlan add 2,5
  switchport trunk native vlan 5
  switchport mode private-vlan host
  switchport private-vlan host-association 2 3
!
interface gigabitethernet10
  switchport access vlan add 2,5
  switchport trunk native vlan 2
  switchport mode private-vlan promiscuous
  switchport private-vlan mapping 2 add 3-5
.....
.....
```

## 4.8 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:

4.8.1 QoS Setting

4.8.2 CoS-Queue Mapping

4.8.3 DSCP-Queue Mapping

4.8.4 CLI Commands of the Traffic Prioritization

### 4.8.1 QoS Setting

#### QoS Setting

Help

##### QoS Trust Mode

- 802.1P priority tag
- DSCP/TOS code point

##### Queue Scheduling

- Round Robin Scheme
- Strict Priority Scheme
- Weighted Round Robin Scheme
- Weighted Deficit Round Robin Scheme

Queue	0	1	2	3	4	5	6	7
Weight	▼	▼	▼	▼	▼	▼	▼	▼

##### Queue Scheduling

You can select the Queue Scheduling rule as follows:

**Use a Round Robin scheme.** The Round Robin scheme means all the priority has the same privilege, the traffic is forward cyclic from highest to lowest.

**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:

$$Wx / W0 + W1 + W2 + W3 + W4 + W5 + W6 + W7 \text{ (Total volume of Queue 0-7)}$$

### Port Setting

**Priority** column is to indicate default port priority value for untagged or priority-tagged frames. When JetNet receives the frames, JetNet will attach the value to the CoS field of the incoming VLAN-tagged packets. You can enable 0,1,2,3,4,5,6 or 7 to the port.

Default priority type is **COS**. The system will provide default COS-Queue table to which you can refer for the next command.

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

### 4.8.2 CoS-Queue Mapping

This page is to change CoS values to Physical Queue mapping table. Since the switch fabric of JetNet only supports 8 physical queues, Lowest, Low, Middle and High. Users should therefore assign how to map CoS value to the level of the physical queue.

#### CoS-Queue Mapping

Help

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

Note- Queue 7 is the highest priority queue in using Strict Priority scheme

Apply Cancel

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

### 4.8.3 DSCP-Priority Mapping

This page is to change DSCP values to Physical Queue mapping table. Since the switch fabric of JetNet only supports 8 physical queues. 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.

#### DSCP-Priority Mapping

Help

DSCP	0	1	2	3	4	5	6	7
Queue	0 ▾	0 ▾	0 ▾	0 ▾	0 ▾	0 ▾	0 ▾	0 ▾
DSCP	8	9	10	11	12	13	14	15
Queue	1 ▾	1 ▾	1 ▾	1 ▾	1 ▾	1 ▾	1 ▾	1 ▾
DSCP	16	17	18	19	20	21	22	23
Queue	2 ▾	2 ▾	2 ▾	2 ▾	2 ▾	2 ▾	2 ▾	2 ▾
DSCP	24	25	26	27	28	29	30	31
Queue	3 ▾	3 ▾	3 ▾	3 ▾	3 ▾	3 ▾	3 ▾	3 ▾
DSCP	32	33	34	35	36	37	38	39
Queue	4 ▾	4 ▾	4 ▾	4 ▾	4 ▾	4 ▾	4 ▾	4 ▾

#### 4.8.4 CLI Commands of the Traffic Prioritization

Command Lines of the Traffic Prioritization configuration

Feature	Command Line
<b>QoS Setting</b>	
Queue Scheduling – Round Robin	Switch(config)# qos queue-sched rr Round Robin sp Strict Priority wrr Weighted Round Robin Switch(config)# qos queue-sched rr The queue scheduling scheme is setting to Round Robin.
Queue Scheduling – Strict Priority	Switch(config)# qos queue-sched sp The queue scheduling scheme is setting to Strict Priority.
Queue Scheduling – WRR	Switch(config)# qos queue-sched wrr 1 1 1 1 1 1 1 1 The queue scheduling scheme is setting to Weighted Round Robin.
Port Setting – Priority	Switch(config)# interface <b>fa1</b> Switch(config-if)# qos priority DEFAULT-PRIORITY Assign an priority (7 highest) Switch(config-if)# qos priority 7 The default port priority value is set 7 ok.  <b>Note: When change the port setting, you should Select the specific port first. Ex: fa1 means fast Ethernet port 1.</b>
Display – Queue Scheduling	Switch# show qos queue-sched QoS queue scheduling scheme : Weighted Round Robin (Use an 8,4,2,1 weight)
Display – Port Setting	Switch# show qos port-priority Port Default Priority : Port Priority R. -----+--- 0 7 0 8 0 9 0 10 0 ... 26 0 27 0 28 0
<b>CoS-Queue Mapping</b>	
Format	Switch(config)# qos cos-map PRIORITY Assign an priority (7 highest) Switch(config)# qos cos-map 1 QUEUE Assign an queue (0-7)  <b>Note: Format: qos cos-map priority_value queue_value</b>
Map CoS 0 to Queue 0	Switch(config)# qos cos-map 0 0 The CoS to queue mapping is set ok.
Map CoS 1 to Queue 1	Switch(config)# qos cos-map 1 1 The CoS to queue mapping is set ok.
Map CoS 2 to Queue 2	Switch(config)# qos cos-map 2 2 The CoS to queue mapping is set ok.
Map CoS 3 to Queue 3	Switch(config)# qos cos-map 3 3 The CoS to queue mapping is set ok.



Map CoS 4 to Queue 4	Switch(config)# qos cos-map 4 4 The CoS to queue mapping is set ok.
Map CoS 5 to Queue 5	Switch(config)# qos cos-map 5 5 The CoS to queue mapping is set ok.
Map CoS 6 to Queue 6	Switch(config)# qos cos-map 6 6 The CoS to queue mapping is set ok.
Map CoS 7 to Queue 7	Switch(config)# qos cos-map 7 7 The CoS to queue mapping is set ok.
Display – CoS-Queue mapping	Switch# sh qos cos-map CoS to Queue Mapping : CoS Queue R. ---- + ---- 6 7 7
<b>DSCP-Queue Mapping</b>	
Format	Switch(config)# qos dscp-map PRIORITY Assign an priority (63 highest) Switch(config)# qos dscp-map 0 QUEUE Assign an queue (0-7)  <b>Format: qos dscp-map priority_value queue_value</b>
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  0 0 0 0 0 0 0 0 1 1 R. 1  1 1 1 1 1 1 2 2 2 2   2 2 2 2 3 3 3 3 3 3   3 3 4 4 4 4 4 4 4 4   5 5 5 5 5 5 5 6 5   6 6 6 6 6 6 7 7 7 7 6   7 7 7 7

## 4.9 Multicast Filtering

For multicast filtering, JetNet 6628X 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
<b>Query</b>	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.
<b>Report</b>	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.
<b>Leave Group</b>	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:

4.9.1 IGMP Snooping

4.9.2 IGMP Query

4.9.3 Unknown Multicast

4.9.4 CLI Commands of the Multicast Filtering

### 4.9.1 IGMP Snooping & Filtering

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. JetNet6628X support IGMP snooping V1/V2/V3 automatically and IGMP query V1/V2.

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

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

## IGMP Snooping & Filtering

Help

IGMP Snooping Global Setting Disable ▾

Apply

### IGMP Snooping VLAN Setting

VLAN	IGMP Snooping	Immediate-leave	Last Member Query Interval	Filtering Mode
1	Disable ▾	Disable ▾	100	Flood Unknown ▾

Apply

### IGMP Snooping Table

Multicast Address	VLAN ID	Interface

Reload

**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 6628X supports 256 multicast groups. Click on **Reload** to refresh the table.

## 4.9.2 IGMP Query

### IGMP Query

Help

#### IGMP Query Setting

VLAN	Enable Disable	Version	Query Interva	Max-Resp-Time
1	Disable ▾	v2 ▾	125	10

Apply

This page allows users to configure **IGMP Query** feature. Since JetNet 6628X can only be configured by member ports 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.

### 4.9.3 CLI Commands of the Multicast Filtering

Command Lines of the multicast filtering configuration

Feature	Command Line
<b>IGMP Snooping</b>	
IGMP Snoopi-g - Global	Switch(config)# ip igmp snooping IGMP snooping is enabled globally. Please specify on which vlans IGMP snooping enables
IGMP Snoopi-g - VLAN	Switch(config)# ip igmp snooping vlan VLANLIST allowed vlan list all all existed vlan Switch(config)# ip igmp snooping vlan 1-2 IGMP snooping is enabled on VLAN 1-2.
Disable IGMP Snoopi-g - Global	Switch(config)# no ip igmp snoopin IGMP snooping is disabled globally ok.
Disable IGMP Snoopi-g - VLAN	Switch(config)# no ip igmp snooping vlan 3 IGMP snooping is disabled on VLAN 3.
Display – IGMP Snooping Setting	Switc evic ip igmp interface vlan1 enabled: Yes version: IGMPv1 query-interval; 125s query-max-response-time: 10s  Switc evic ip igmp snooping IGMP snooping is globally enabled Vlan1 is IGMP snooping enabled Vlan2 is IGMP snooping enabled Vlan3 is IGMP snooping disabled
Display – IGMP Table	Switc evic ip igmp snooping multicast all VLAN IP Address Type Ports ----- 1 239.192.8.0 IGMP fa6, 1 239.255.255.250 IGMP fa6,
<b>IGMP Query</b>	
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	Switc evic ip igmp interface vlan1 enabled: Yes version: IGMPv2 query-interval: 125s

	<pre>query-max-response-time: 10s  Switch# show running-config .... ! interface vlan1  ip address 192.168.10.17/24  ip igmp  no shutdown ! .....</pre>
<b>Unknown Multicast</b>	
Send Unknown Multicast to Query Ports	<pre>Switch(config)# ip igmp snooping source-only-learning IGMP Snooping Source-Only-Learning enabled</pre>
Send Unknown Multicast to All Ports	<pre>Switch(config)# no ip igmp snooping source-only-learning IGMP Snooping Source-Only-Learning disabled  Switch(config)# no mac-address-table multicast filtering Flooding unknown multicast addresses ok!</pre>
Discard All Unknown Multicast	<pre>Switch(config)# mac-address-table multicast filtering Filtering unknown multicast addresses ok!</pre>

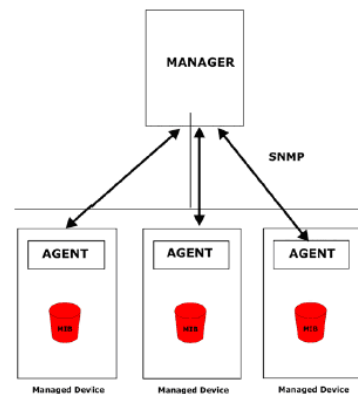
## 4.10 SNMP

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 6628X series support SNMP v1 and v2c and V3.

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:

- 4.10.1 SNMP Configuration
- 4.10.2 SNMPv3 Profile
- 4.10.3 SNMP Traps
- 4.10.4 SNMP CLI Commands for SNMP



### 4.10.1 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 6628X 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 V1/V2c Configuration

Help

	Community String	Privilege
<input type="checkbox"/>	public	Read Only ▼
<input type="checkbox"/>	private	Read and Write ▼
<input type="checkbox"/>		Read Only ▼
<input type="checkbox"/>		Read Only ▼

Apply

Remove

### 4.10.2 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 6628X* and the administrator are encrypted to ensure secure communication.

## SNMP V3 Profile

Help

### SNMP V3

User Name	<input type="text"/>
Security Level	None ▼
Authentication Level	MD5 ▼
Authentication Password	<input type="password"/>
DES Password	<input type="password"/>

Add

**Security Level:** Here the user can select the following levels of security: None,

Authentication, and “Authentication and Privacy”.

**Auth. 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 6628X* 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.

**Auth. 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.

### 4.10.3 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 V2**. After configuration, you can see 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

---

**SNMP Trap Server**

Server IP	<input type="text"/>
Community	<input type="text"/>
Version	V1 ▼

---

**Trap Server Profile**

Server IP	Version	Community

### 4.10.4 CLI Commands of the SNMP

Command Lines of the SNMP configuration

Feature	Command Line
<b>SNMP Community</b>	
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
<b>SNMP Trap</b>	
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. <b>Note: private is the community name, version 1 is the SNMP version</b>
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 .....



## 4.11 Security

JetNet 6628X 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:

4.11.1 Filter Set (Access Control List)

4.11.2 IEEE 802.1x

4.11.3 CLI Commands of the Security

### 4.11.1 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,      **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	
-	Server2_MAC	

### 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:	<input type="text" value="Server_MAC"/>	Action:	<input type="text" value="Permit"/>
Source Address:	<input type="text" value="."/>	Destination Address:	<input type="text" value="."/>
Source Wildcard:	<input type="text" value="Any"/>	Destination Wildcard:	<input type="text" value="Any"/>
Egress Port:	<input type="text" value="--"/>		

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

**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	
....			

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

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

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,
  IP Filter,

Name:

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:	100	Action:	Permit
Source Address:	192.168.10.2	Destination Address:	192.168.10.200
Source Wildcard:	Host	Destination Wildcard:	Host
Protocol:	IP		
Source Port:		Destination Port:	
Source Port Wildcard:	Any	Destination Port Wildcard:	Any
ICMP Type:	-	ICMP Code:	-
Egress Port:	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:

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"/>	<input type="text" value="100"/>	Server_MAC
10	<input type="checkbox"/>	--	--

### 4.11.2 IEEE 802.1x

#### IEEE 802.1 802.1X 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 6628X could control which connection is available or not.

## 802.1X Configuration

System Auth Control

Authentication Method

### RADIUS Server

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

**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 is for communicating 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.



#### 4.11.2.1 802.1x 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 Configuration Help

##### 802.1X Port Configuration

Port	Port Control	MAB	Re-authentication	Max Request	Guest VLAN	Host Mode	Admin Control Direction
<input type="checkbox"/> 1	Force Authorized ▼	Disable ▼	Disable ▼	2	0	Single ▼	Both ▼
<input type="checkbox"/> 2	Force Authorized ▼	Disable ▼	Disable ▼	2	0	Single ▼	Both ▼
<input type="checkbox"/> 3	Force Authorized ▼	Disable ▼	Disable ▼	2	0	Single ▼	Both ▼
<input type="checkbox"/> 4	Force Authorized ▼	Disable ▼	Disable ▼	2	0	Single ▼	Both ▼
<input type="checkbox"/> 5	Force Authorized ▼	Disable ▼	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

**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.

#### 4.11.2.2 802.1X Port Information

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

### 802.1X Port Information

Help

Port	Port Control	MAB	Port Status	Supplicant MAC Address	Oper Control Direction
1	Force Authorized	Disable	Authorized	NONE	Both
2	Force Authorized	Disable	Authorized	NONE	Both
3	Force Authorized	Disable	Authorized	NONE	Both
4	Force Authorized	Disable	Authorized	NONE	Both
5	Force Authorized	Disable	Authorized	NONE	Both
6	Force Authorized	Disable	Authorized	NONE	Both

#### 4.11.3 CLI Commands of the Security

Command Lines of the Security configuration

Feature	Command Line
<b>Port Security</b>	
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!  <b>Note: Rule: Add the static MAC, VLAN and Port binding first, then enable the port security to stop new MAC learning.</b>
Disable Port Security	Switch(config-if)# no switchport port-security Enable new MAC addresses learning and aging activities!
Display	Switch# show mac-address-table static Destination Address    Address Type    Vlan Destination Port ----- 0012.7701.0101        Static            1            fa1

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

## 4.12 Warning

JetNet 6628X 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:

- 4.13.1 Fault Relay
- 4.13.2 Event Selection
- 4.13.3 Syslog Configuration
- 4.13.4 SMTP Configuration
- 4.13.5 CLI Commands

### 4.12.1 Fault Relay

JetNet 6628X provides 1 digital output, also known as Relay Output. The relay contacts are energized (open) for normal operation and will close under fault conditions. Fault conditions include 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.

**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 has one event type.

#### Fault Relay Setting

Help

<b>Alarm 1</b>	Status is Off
<input type="checkbox"/> <b>Power Failure</b>	Power ID <input type="text" value="1"/>
<input type="checkbox"/> <b>Link Failure</b>	Port <input type="checkbox"/> 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 type="checkbox"/> 10 <input type="checkbox"/> 11 <input type="checkbox"/> 12 <input type="checkbox"/> 13 <input type="checkbox"/> 14 <input type="checkbox"/> 15 <input type="checkbox"/> 16 <input type="checkbox"/> 17 <input type="checkbox"/> 18 <input type="checkbox"/> 19 <input type="checkbox"/> 20 <input type="checkbox"/> 21 <input type="checkbox"/> 22 <input type="checkbox"/> 23 <input type="checkbox"/> 24 <input type="checkbox"/> 25 <input type="checkbox"/> 26 <input type="checkbox"/> 27 <input type="checkbox"/> 28
<input type="checkbox"/> <b>Ring</b>	Ring Failure
<input type="checkbox"/> <b>Ping Failure</b>	IP Address <input type="text"/>
<input type="checkbox"/> <b>Ping Reset</b>	IP Address <input type="text"/> Reset Time(s) <input type="text"/> Hold Time(s) <input type="text"/>
<input type="checkbox"/> <b>Dry Output</b>	On Period(s) <input type="text"/> Off Period(s) <input type="text"/>

Apply

Cancel

Reload

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.

**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 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 AC , Power DC1, Power DC2 or Any you want to monitor. When the power is shut down or broken, the system will short Relay Out and light the Alarm LED.

<input checked="" type="checkbox"/> Relay 1	
Event Type	Power Failure
Power ID	Power AC
	<ul style="list-style-type: none"> <li>Power AC</li> <li>Power DC1</li> <li>Power DC2</li> <li>Any</li> </ul>

**Apply**

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 Alarm LED.

<input checked="" type="checkbox"/> Relay 1										
Event Type	Link Failure									
Link	1	2	3	4	5	6	7	8	9	10
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" 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	19	20
	<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"/>
	21	22	23	24	25	26	27	28		
	<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 Alarm 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.

#### 4.12.2 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	Power is cut off and then reconnected.
Device Warm Start	Reboot the device by CLI or Web UI.
Authentication failure	An incorrect password, SNMP Community String is entered.
Time Synchronize Failure	Accessing to NTP Server is failure.
Fault Relay	The DO/Fault Relay is on.
Super Ring Topology Changes	Master of Super Ring has changed or backup path is activated.
SFP DDM Failure	The readed information of DDM SFP transceiver is over temperature or out the range of TX/RX power.
Power Failure	<b>Power (AC, DC1, DC2 or Any) is failure.</b>
Port Event	Warning Event is sent when.....
Link-Up	The port is connected to another device
Link-Down	The port is disconnected (e.g. the cable is pulled out, or the opposing devices turns down)
Both	The link status changed.
PoE Powering Event	Warning Event is sent when.....
Enable	The PoE port is powering.
Disable	The PoE port is not powering.

## Event Selection Help

### System Event Selection

- Device Cold Start
- Authentication Failure
- Power 1 Failure
- Power 3 Failure
- Fault Relay 1
- Ring Event
- SFP Event
- DHCP Snooping Event
- DAI Event
- Device Warm Start
- Time Synchronization Failure
- Power 2 Failure
- IPSG Event

### Port Event Selection

Port	Link State
1	Disable ▼
2	Disable ▼
3	Disable ▼
4	Disable ▼

### PoE Event Selection

Port	PoE Powering
1	Disable ▼
2	Disable ▼
3	Disable ▼

### Port Security Selection

Port	Security
1	Disable ▼
2	Disable ▼
3	Disable ▼
4	Disable ▼

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

### 4.12.3 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 6628X, local mode and remote mode.

**Local Mode:** In this mode, JetNet 6628X will print the occurred events selected in the Event Selection page to System Log table of JetNet 6628X. You can monitor the system logs in [Monitor and Diag] / [Event Log] page.

**Remote Mode:** In this mode, you should assign the IP address of the System Log server. JetNet 6628X 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.

## Syslog Configuration Help

Syslog Mode	Disable ▼
Remote IP Address	<input type="text"/>

**Note:** When enabled Local and Both mode, you can monitor the system logs in the [Monitor and Diag]/Event log] page.

Apply Cancel

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.

#### 4.12.4 SMTP Configuration

JetNet 6628X 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.

## SMTP Configuration

Help

Mail Alert Disable ▾

SMTP Server IP	192.168.0.1
Mail Account	user@192.168.0.1
<input type="checkbox"/> Authentication	
User Name	admin
Password	••••
Confirm Password	
Rcpt Email Address 1	
Rcpt Email Address 2	
Rcpt Email Address 3	
Rcpt Email Address 4	

Apply

Cancel

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.

#### 4.12.5 CLI Commands

Command Lines of the Warning configuration

Feature	Command Line
<b>Relay Output</b>	
Relay Output	Switch(config)# relay 1 dry dry output ping ping failure port port link failure power power failure ring super ring failure
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 <1-3> power id (1: AC, 2: DC1, 3:DC2) any Anyone power failure asserts relay Switch(config)# relay 1 power 1 Switch(config)# relay 1 power 2
Super Ring Failure	Switch(config)# relay 1 ring
Disable Relay	R. Switch(config)# no rel1 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, 5,
<b>Event Selection</b>	
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 poe-powering    Switch PoE powering or unpowering event power             Switch power failure event sfp-ddm          Switch SFP DDM abnormal 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 [IFNAME]    Interface list, ex: fa1,fa3-5,gi25-26 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 PoE Powering: SFP DDM: Enabled
<b>Syslog Configuration</b>	
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
<b>SMTP Configuration</b>	
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: <a href="mailto:admin@korenix.com">admin@korenix.com</a> Switch(config)# smtp-server server 192.168.10.100 <a href="mailto:admin@korenix.com">admin@korenix.com</a> SMTP Email Alert set Server: 192.168.10.100, Account: admin@korenix.com ok.
Receiver mail	Switch(config)# smtp-server receipt <a href="mailto:1_korecare@korenix.com">1_korecare@korenix.com</a> 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  <b>Note: You can assign string to username and password.</b>
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.

Dispaly	Switch# sh smtp-server SMTP Email Alert is Enabled Server: 192.168.10.100, Account: <a href="mailto:admin@korenix.com">admin@korenix.com</a> Authentication: Enabled Username: admin, Password: admin SMTP Email Alert Receipt: Receipt 1: <a href="mailto:korecare@korenix.com">korecare@korenix.com</a> Receipt 2: Receipt 3: Receipt 4:
---------	---

## 4.13 Monitor and Diag

JetNet 6628X 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:

4.14.1 MAC Address Table

4.14.2 Port Statistics

4.14.3 Port Mirror

4.14.4 Event Log

4.14.5 Topology Discovery

4.14.6 Ping

4.14.7 CLI Commands of the Monitor and Diag

### 4.13.1 MAC Address Table

JetNet 6628X provides 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 Help

Aging Time(secs)

### Static Unicast MAC Address

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

MAC Address Table

MAC Address	Address Type	VID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
<input type="checkbox"/> 3c52.8237.11cb	Dynamic Unicast	1	V																											

### 4.13.2 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 Help

Port	Type	Link	State	Rx Good	Rx Bad	Rx Abort	Tx Good	Tx Bad	Collision
<input type="checkbox"/> 1	1000	Connected	Enable	137252	0	3	1073609	0	0
<input type="checkbox"/> 2	0	Disconnected	Enable	0	0	0	0	0	0
<input type="checkbox"/> 3	0	Disconnected	Enable	0	0	0	0	0	0
<input type="checkbox"/> 4	0	Disconnected	Enable	0	0	0	0	0	0
<input type="checkbox"/> 5	0	Disconnected	Enable	0	0	0	0	0	0
<input type="checkbox"/> 6	0	Disconnected	Enable	0	0	0	0	0	0

### 4.13.3 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 a single port, or any combination of ports, but you can only monitor them in Rx or TX only. Click on checkbox of the Port ID, RX, Tx or Both to select the source ports.

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

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

## Port Mirroring

Help

Port Mirroring  ▾

Port	Source Port		Destination Port
	Rx	Tx	
1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="radio"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	<input 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"/>

### 4.13.4 Event Log

In the 4.11.3, we have introduced System Log feature. When System Log Local mode is selected, JetNet 6628X 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	02:27:13	Event: Link 1 Down.
2	Jan 1	02:27:12	Event: Link 2 Down.
3	Jan 1	02:27:09	Event: Link 1 Up.
4	Jan 1	02:27:08	Event: Link 2 Up.
5	Jan 1	02:26:55	Event: Link 1 Down.
6	Jan 1	02:26:54	Event: Link 2 Down.
7	Jan 1	02:26:49	Event: Link 2 Up.

Clear

Reload

### 4.13.5 LLDP Configuration

JetNet 6628X supports topology discovery or LLDP (IEEE 802.1AB Link Layer Discovery Protocol) function that can help user to discovery multi-vendor's network devices on same segment by NMS system which supports LLDP function; With LLDP function, NMS can

easier maintain the topology map, display port ID, port description, system description, VLAN ID... Once the link failure, the topology change events can be updated to the NMS as well. The LLDP Port State can display the neighbor ID and IP learnt from the connected devices.

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

**LLDP Configuration:** To configure the related timer of LLDP.

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

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

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

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

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

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

## LLDP Configuration

Help

LLDP

LLDP Timer	<input type="text" value="30"/>
LLDP Hold Time	<input type="text" value="120"/>

Apply

Cancel

### 4.13.6 Ping

This page provides **Ping** 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

Help

Destination	<input type="text"/>
-------------	----------------------

Ping



#### 4.13.7 CLI Commands of the Monitor and Diag

Command Lines of the Monitor and Diag configuration

Feature	Command Line
<b>MAC Address Table</b>	
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!  <b>Note: rule: mac-address-table static MAC_address VLAN VID interface interface_name</b>
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!  <b>Note: rule: mac-address-table multicast MAC_address VLAN VID interface_list interface_name/range</b>
Show MAC Address Table – All types	Switch# show mac-address-table  **** UNICAST MAC ADDRESS **** Destination Address    Address Type    Vlan    Destination Port ----- 000f.b079.ca3b        Dynamic        1        fa4 0012.7701.0386        Dynamic        1        fa7 0012.7710.0101        Static         1        fa7 0012.7710.0102        Static         1        fa7 0012.77ff.0100        Management    1  **** MULTICAST MAC ADDRESS **** 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 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 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 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.
<b>Port Statistics</b>	

Port Statistics	<pre>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</pre>
<b>Port Mirroring</b>	
Enable Port Mirror	<pre>Switch(config)# mirror en Mirror set enable ok.</pre>
Disable Port Mirror	<pre>Switch(config)# mirror disable Mirror set disable ok.</pre>
Select Source Port	<pre>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.</pre> <p><b>Note: Select source port list and TX/RX/Both mode.</b></p>
Select Destination Port	<pre>Switch(config)# mirror destination fa6 Mirror destination fa6 set ok</pre>
Display	<pre>Switch# show mirror Mirror Status : Enabled Ingress Monitor Destination P rt : fa6 Egress Monitor Destination P rt : fa6 Ingress Source Po ts :fa1,fa2, Egress Source Po ts :fa1,fa2,</pre>
<b>Event Log</b>	
Display	<pre>Switch# show event-log &lt;1&gt;Jan  1 02:50:47 snmpd[101]: Event: Link 4 Down. &lt;2&gt;Jan  1 02:50:50 snmpd[101]: Event: Link 5 Up. &lt;3&gt;Jan  1 02:50:51 snmpd[101]: Event: Link 5 Down. &lt;4&gt;Jan  1 02:50:53 snmpd[101]: Event: Link 4 Up.</pre>
<b>Ping</b>	
Ping IP	<pre>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</pre>

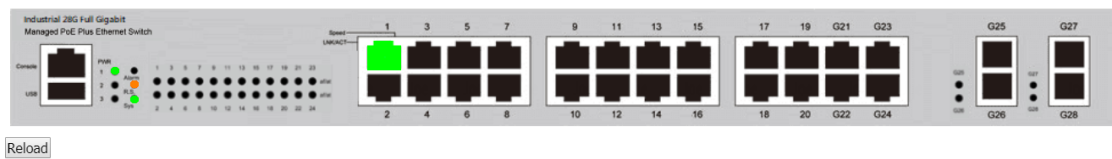
## 4.13 Device Front Panel

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

Feature	On / Link UP	Off / Link Down	Other
PSU	Green	Black	
DC1	Green	Black	
DC2	Green	Black	
Sys	Green	Black	
R.S.	Green: Ring state is normal Amber: Ring state is abnormal	Black	Green Flashing: Incorrect configuration Amber Flashing: One of the ring ports break has been detected
Alarm	Red	Black	

### Device Front Panel [Help](#)

This page shows the current status on the front panel of the device.



## 4.14 Save

**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

---

Do you want to save 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]

## 4.15 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.

### Logout

---

Do you want to logout?

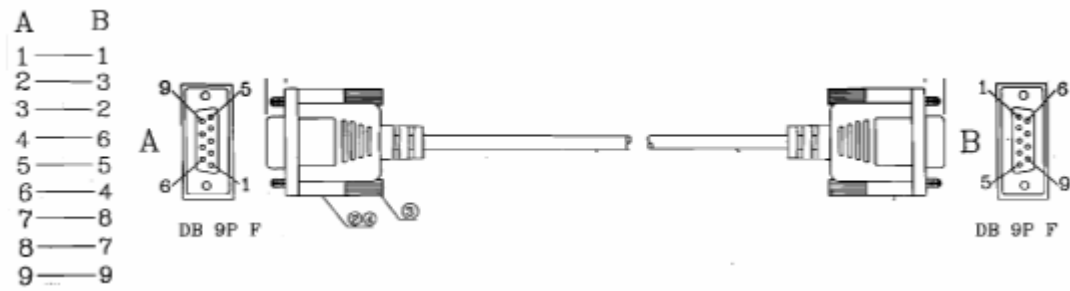
Command Lines:

Feature	Command Line
Logout	SWITCH> exit
	SWITCH# exit

# 5 Appendix

## 5.14 Pin Assignment of the RS-232 Console Cable

The total cable length is 150cm.



## 5.15 Korenix SFP family

Korenix certificated many types of SFP transceiver. These certificated SFP transceivers can be identified by JetNet 6628X 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	Gigabit SFP Transceiver
<b>SFPGSX</b>	1000Base-SX multi-mode SFP transceiver,550m, -10~70°C
<b>SFPGSX-w</b>	1000Base-SX multi-mode SFP transceiver,550m, wide operating temperature, -40~85°C
<b>SFPGSX2</b>	1000Base-SX plus multi-mode SFP transceiver,2Km, -10~70°C
<b>SFPGSX2-w</b>	1000Base-SX plus multi-mode SFP transceiver, 2Km,wide operating temperature, -10~70°C
<b>SFPG LX10</b>	1000Base-LX single-mode SFP transceiver 10Km, -10~70°C
<b>SFPG LX10-w</b>	1000Base-LX single-mode SFP transceiver, 10Km, wide operating temperature, -40~85°C
<b>SFPG LXH30</b>	1000Base-LHX single-mode SFP transceiver,30Km, -10~70°C
<b>SFPG LXH30-w</b>	1000Base-LHX single-mode SFP transceiver, 30Km, wide operating temperature, -40~85°C
<b>SFPGXD50</b>	1000Base-XD single-mode SFP transceiver, 50Km, -10~70°C
<b>SFPGXD50-w</b>	1000Base-XD single-mode SFP transceiver, 50Km, wide operating temperature, -40~85°C
<b>SFPGZX70</b>	1000Base-ZX single-mode SFP transceiver, 70Km, -10~70°C
<b>SFPGZX70-w</b>	1000Base-ZX single-mode SFP transceiver, 70Km, -40°C - 85°C
Model Name	Gigabit BIDI/WDM SFP Transceiver
<b>SFPG LX10B13</b>	1000Base-LX, single-mode, TX 1310nm/ RX 1550nm,10Km, -10~70°C

**SFPGLX10B13-w** 1000Base-LX single-mode, TX 1310nm/ RX 1550nm,10Km, -40°C - 85°C

**SFPGLX10B15** 1000Base-LX, single-mode, TX 1550nm/ RX 1310nm,10Km, -10~70°C

**SFPGLX10B15-w** 1000Base-LX single-mode, TX 1550nm/ RX 1310nm,10Km, -40°C - 85°C

**SFPGLX20B13** 1000Base-LX, single-mode, TX 1310nm/ RX 1550nm,10Km, -10~70°C

**SFPGLX20B13-w** 1000Base-LX single-mode, TX 1310nm/ RX 1550nm, 10Km, -40°C - 85°C

**SFPGLX20B15** 1000Base-LX, single-mode, TX 1550nm/ RX 1310nm, 20Km, -10~70°C

**SFPGLX20B15-w** 1000Base-LX single-mode, TX 1550nm/ RX 1310nm, 20Km, -40°C - 85°C

**SFPGLX40B13** 1000Base-LX, single-mode, TX 1310nm/ RX 1550nm,40Km, -10~70°C

**SFPGLX40B13-w** 1000Base-LX single-mode, TX 1310nm/ RX 1550nm, 40Km, -40°C - 85°C

**SFPGLX40B15** 1000Base-LX, single-mode, TX 1550nm/ RX 1310nm, 40Km, -10~70°C

**SFPGLX40B15-w** 1000Base-LX single-mode, TX 1550nm/ RX 1310nm, 40Km, -40°C - 85°C

**SFPGLX60B13** 1000Base-LX, single-mode, TX 1310nm/ RX 1550nm,60Km, -10~70°C

**SFPGLX60B15** 1000Base-LX, single-mode, TX 1550nm/ RX 1310nm, 60Km, -10~70°C



## 5.16 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 the same as 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 6628X is 1.3.6.1.4.1.24062.2.3.4.

## 5.17 Revision History

<b>Edition</b>	<b>Date</b>	<b>Modifications</b>
V1.0	June. 1, 2019	The first version

## 5.18 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](mailto: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

**Business service:** [sales@korenix.com](mailto:sales@korenix.com)

**Customer service:** [koreCARE@korenix.com](mailto:koreCARE@korenix.com)