Korenix

JetNet 5020G Series

Industrial Managed Ethernet Switch

User Manual

Manual V1.2

Jul, 2017

www.korenix.com

Korenix

JetNet 5020G Series

Industrial Managed Ethernet Switch

User Manual

Copyright Notice

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

Welcome to Korenix *JetNet 5020G, Industrial 16+4G Gigabit 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 5020G, are specially designed for industrial environments requesting support of higher access point or multiple Gigabit ports. With fewer units installed and higher density of port numbers, the ports are sharing wider on-chip backplane bandwidth, shorter local transmission latency, and efficient upstream transmission.

JetNet 5020G, the **16+4G Managed Ethernet Switch** is equipped with 16 10/100TX Fast Ethernet ports and 4 10/100/ 1000Base-T/SFP combo ports. The SFP ports accept all types of Gigabit SFP and Fast Ethernet Fiber transceivers, including Gigabit SX, LX, LHX, ZX and XD for several connections and distances. The Ethernet Switch can identify the supported transmission speed of the inserted SFP transceiver, and the Switch's operating temperature extended from -40°C to 75°C.

Model Name	100TX	Gigabit TX	100M Fiber	1000M Fiber
JetNet 5020G **16+4G Managed Ethernet Switch**	16	4 (Combo with SFP)	4 100FX (SFP)	4 1000FX (SFP)

Note: 100FX means support 100Mbps SFP fiber transceiver, and 1000FX means support 1000Mbps SFP fiber transceiver.

The device is mounted onto 35mm DIN rail in accordance with DIN EN 60715, along with any public servers or network devices. When others are aggregated to JetNet 5020G, the 16+4G design allows connections up to 10 rings, with owned ring redundancy protection. This is unique because of Korenix patent-protected technology.

JetNet 5020G is a fan-less-designed Ethernet Switch, with low power consumption, wide operating temperature, and dynamic DC input voltage. Excellent margin is defined by 9Kbytes Jumbo Frame on large data transmission and 1.5Mbytes shared memory on packet buffering, which is the trend for future industrial applications.

The embedded software supports RSTP and Multiple Super Ring technology for ring redundancy protection. Full Layer 2 management includes, VLAN, IGMP Snooping, LACP for network control, SNMP, LLDP for network management. Secured access is achieved by Port Security, 802.1x and flexible Layer2/4 Access Control List. By utilizing JetNet 5020G, one can fulfill the technician's need by having best solutions for Industrial Ethernet Infrastructure.

1.2 Major Features

JetNet 5020G has following major features:

- 16-port 10/100 Base-TX and 4-port Gigabit RJ-45/SFP combo ports (100/1000 Base-TX, 1000Base-X)
- Non-Blocking, no collision or delay under wire-speed transmission
- Jumbo Frame size up to 9,712 byte
- RSTP and Multiple Super Ring (Rapid Super Ring, Rapid Dual Homing, MultiRing, TrunkRing)
- Maximum 8 x 100M Rings plus 2 Gigabit Rings aggregation capability
- VLAN, LACP, GVRP, QoS, IGMP Snooping, Rate Control, Online Multi Port Mirroring
- Link Layer Discovery Protocol (LLDP), SNMP V1/V2c/V3, RMON and KorenixView Discovering and Management
- Advanced Security supports IP/Port Security, 802.1x and Access Control List
- Event Notification by E-mail, SNMP Trap, Syslog and one DRY Relay Output
- Operating Temperature: -40° C ~75° C
- Rigid Aluminum Case complies with Ingress Protection – IP30
- Redundant Power Input, DC 24V (typical); range 9.6-60Vdc

Note: Detailed spec is listed in datasheet. Please download the latest version from Korenix Website.

1.3 Package List

JetNet 5020G Series products are shipped with following items:

1. JetNet 5020G (no SFP transceivers) with Din Rail Clip x1
2. Console Cable x1
3. Terminal Blocks for Power & DI/DO x2
4. Quick Installation Guide x1

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

System Diagnostic LED

PWR1 (Power 1): Power Ready (Green On)
PWR2 (Power 2): Power Ready (Green On)
SYS (System): System Ready (Green On)
System on Booting/Upgrade (Green Blinking)
DI (Digital Input): Digital Input (Red On)
DO (Digital Output): Relay activated (Red On)
R.S. (Ring Status): Ring normal (Green On)
Wrong ring port connected (Green Blinking)
Ring abnormal (Amber On)
Device ring port failed (Amber Blinking)
Fast Ethernet (Port1~16): Link/Active (Green on / Blinking),
Full Duplex (Amber on)
Gigabit Ethernet (Port17~20): Link/Active (Green on/ Blinking)
Speed 1000Mbps link (Amber on)
Speed 10/100Mbps link (Amber off)

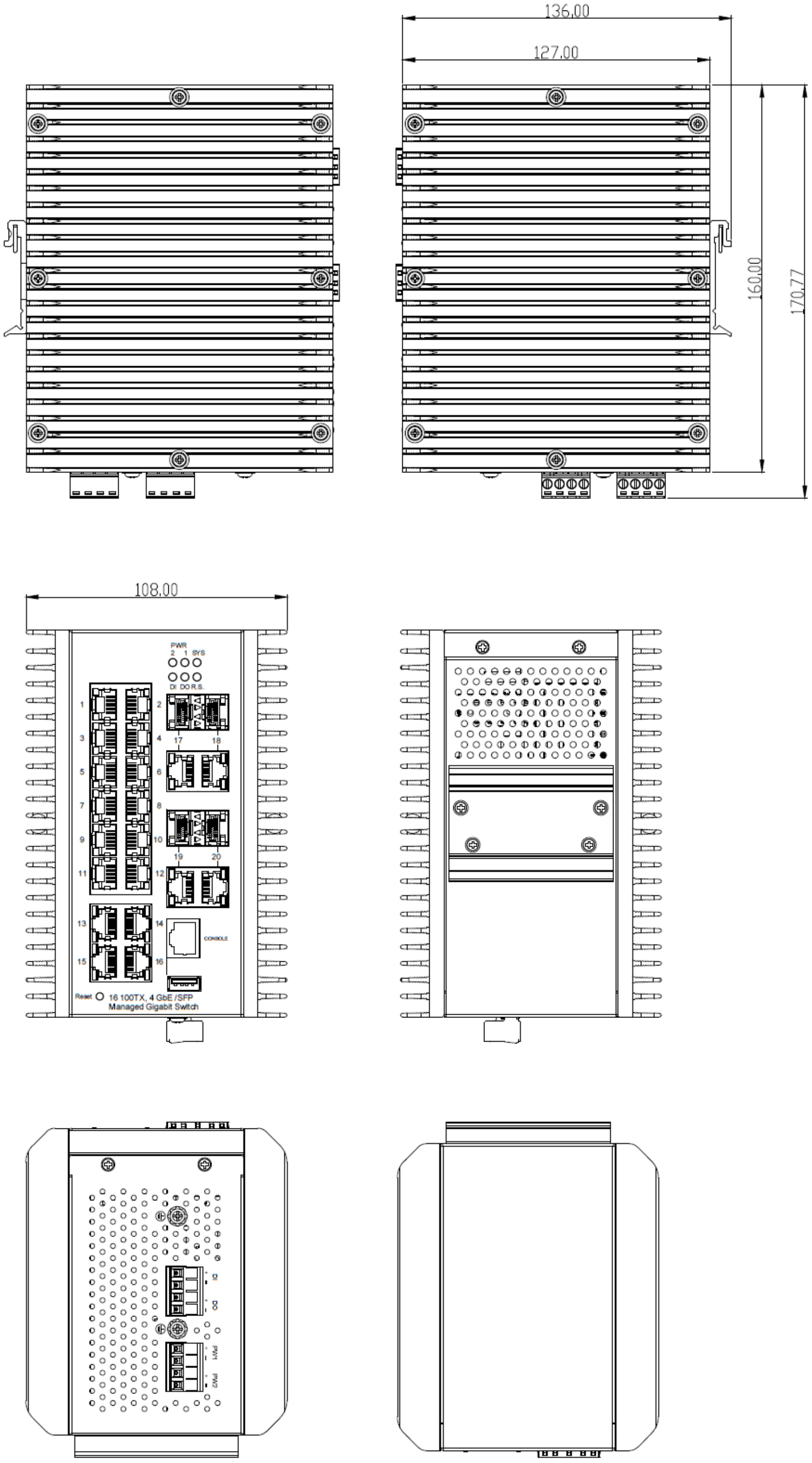
Dimension (HxWxD)mm

160(H) x 108 (W) x 127 (D)	without DIN rail clip
160(H) x 108 (W) x 136 (D)	with DIN rail clip

Panel Layout

The front panel includes RJ-45 based RS232 Console Port, System and Port LEDs, Hardware Reset, Fast/Gigabit Ethernet Port and Gigabit SFP Combo Port interfaces. Grounding, DI/DO and Power1/2 have been designed on the bottom side.

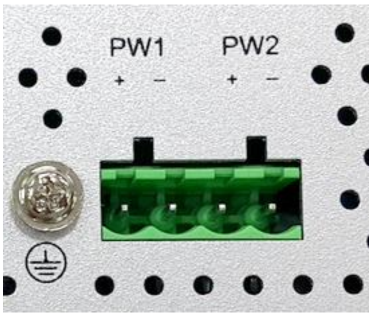
Figure of JetNet 5020G, 16+4G Managed Ethernet Switch

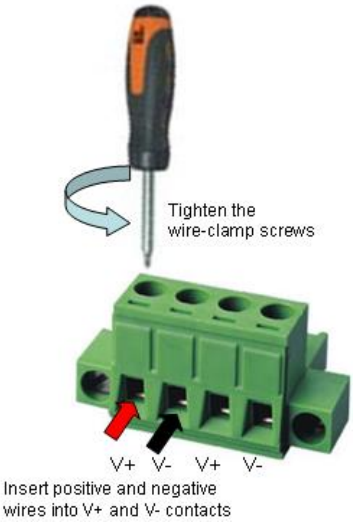


2.2 Wiring Power Inputs

For redundant DC power inputs.

1. Insert positive and negative wires into V+ and V- contacts respectively of the terminal block connector (Plug-side).




Tighten the wire-clamp screws
V+ V- V+ V-
Insert positive and negative wires into V+ and V- contacts

2. Tighten the clamping screws to prevent the loosening of the DC wires.
3. Power 1 and Power 2 support power redundancy and polarity-reverse protection functions.
4. Positive and negative power system inputs are both accepted, but Power 1 and Power 2 must apply the same mode.

Note 1: In order to protect the switch itself, a safe power-port connection can be achieved by following procedures:

1. Turn-off the power supply.
2. Connect the power wire to the Plug-side connector.
3. Plug the connector into the switch Power port.
4. Power-on the power supply.
5. VDE tested screwdriver is suggested for higher safety concern.

Note 2: Suitable DC electrical wire is ranging from 12 to 24 AWG.

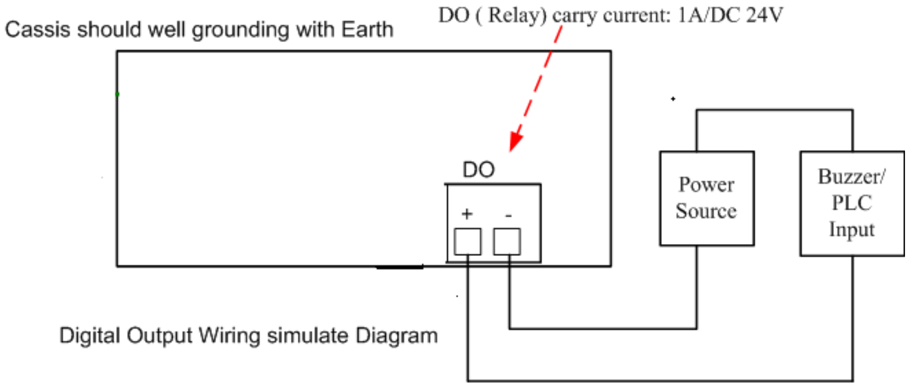
Note 3: If 2 power supplies are connected to the switch, it will be powered from the one with higher voltage level.

Note 4: When loss of either PWR1 or PWR2, an alarm will be given through Dry Relay Output (referring to 2.3. Wiring Digital Output), by the adequate setting in the management of user interface.

Note 5: This product is intended to be supplied by an UL60950-1 listed Power Unit rated output rating: 9.6-60Vdc or 24Vdc, 1.0A minimum / Maximum ambient temperature is 55°C minimum.

2.3 Wiring Digital Output

JetNet 5020G provides 1 digital output, also known as **Dry Relay Output**. The relay contacts are energized (open) under normal operation and will be closed in fault conditions. The fault conditions can be power failure, Ethernet port linkage down or other pre-defined events configured in management UI.


Cassis should well grounding with Earth
DO (Relay) carry current: 1A/DC 24V
DO
+
-
Power Source
Buzzer/ PLC Input

Digital Output Wiring simulate Diagram

2.4 Wiring Earth Ground

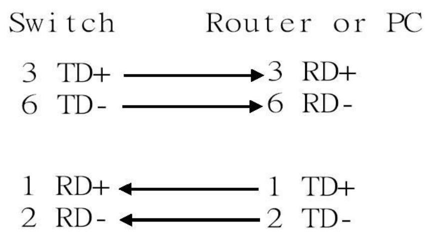
To ensure the system will not be damaged by noise or any electrical shock, we suggest you to make exact connection into JetNet 5020G with Earth Ground.

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

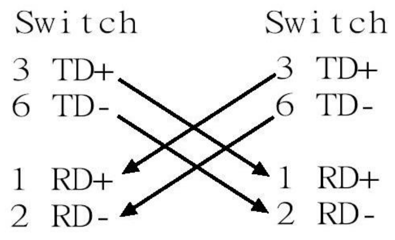
2.5 Wiring Fast Ethernet Ports

JetNet 5020G includes 16 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.

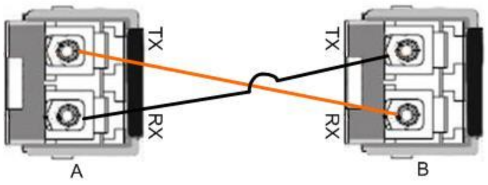
100 Base-TX: 2-pair UTP/STP Cat. 5 cable, EIA/TIA-568B 100-ohm (100m)
1000 Base-TX: 4-pair UTP/STP Cat. 5/Cat.5E cable, EIA/TIA-568B 100-ohm (100m)

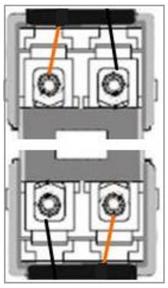
2.6 Wiring Fiber Ports

Small Form-factor Pluggable (SFP) Fiber Interface

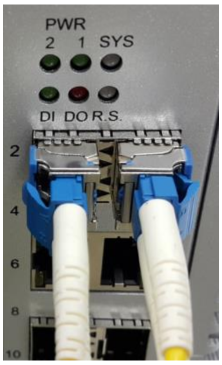
The SFP ports accept standardized Gigabit MINI GBIC SFP transceiver. However, to ensure system reliability, **it is recommended to use Korenix certificated Gigabit SFP Transceiver.** The web UI will show Unknown-Vendor type when choosing the SFP not certificated by Korenix. The certificated SFP transceiver includes 100Base-FX single/multi-mode, 100/Gigabit BIDI/WDM, 1000Base-SX/LX single/multi-mode ranger from 550m to 80KM.

The way to connect the SFP transceiver is to Plug in SFP fiber transceiver fist. Cross-connect the transmit channel at each end to the receive channel at the opposite end as illustrated in the figure below. The SPF cage is 2x1 designs; check the direction/angle of the fiber transceiver and fiber cable during the insertion.





Below figure is the SFP plug-in and Fiber Cable Plug-in Example.



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

Note 2: To ensure safety, the optional transceiver should compliance with Class I Laser diode with UL certification and EN 60825-1 standard.

2.7 Wiring Combo Ports

JetNet 5020G includes 4 RJ-45 Gigabit Ethernet ports. The speed of the gigabit Ethernet port supports 100Base-TX and 1000Base-TX. JetNet 5020G is also equipped with 4 Gigabit SFP ports combo with Gigabit Ethernet RJ-45 ports. **The speed of the SFP port supports 100MB and 1000Full Duplex, you need to configure SFP speed in CLI.** The available gigabit SFP supports Gigabit Single-mode, Multi-mode, and BIDI/WDM Single-mode SFP transceivers.

When the SFP transceivers installed, the Fiber ports enjoy higher priority than copper and the device switches to Fiber mode automatically.

.

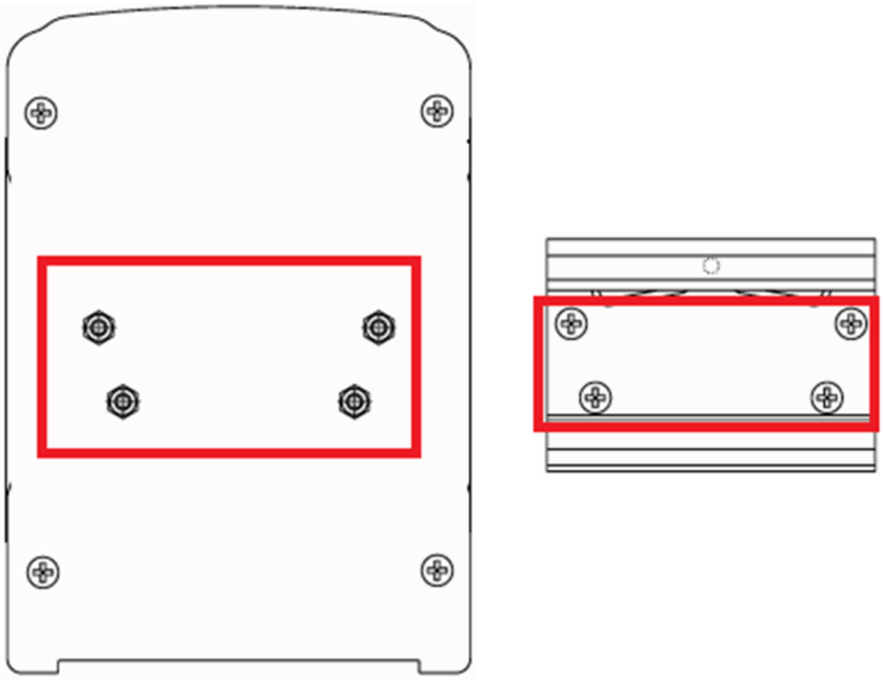
2.8 Wiring RS-232 Console Cable

JetNet 5020G attached one RS-232 DB-9 to RJ-45 cable in the unit box. Connect the RJ-45 connector to the COM port of your PC, open Terminal tool and set up serial settings to 9600, N,8,1. (Baud Rate: 9600 / Parity: None / Data Bit: 8 / Stop Bit: 1) Then you can access CLI interface by console able.

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

2.9 DIN-Rail Mounting Installation

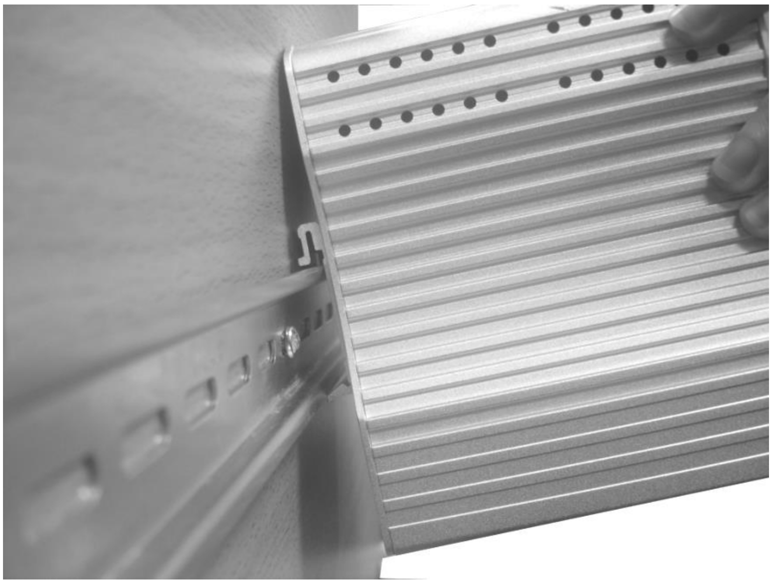
The DIN-Rail clip has been attached to JetNet 5020G mainframe in production. If the DIN-Rail clip is not screwed on JetNet 5020G, follow the instructions and the figure below to attach DIN-Rail clip to the device.



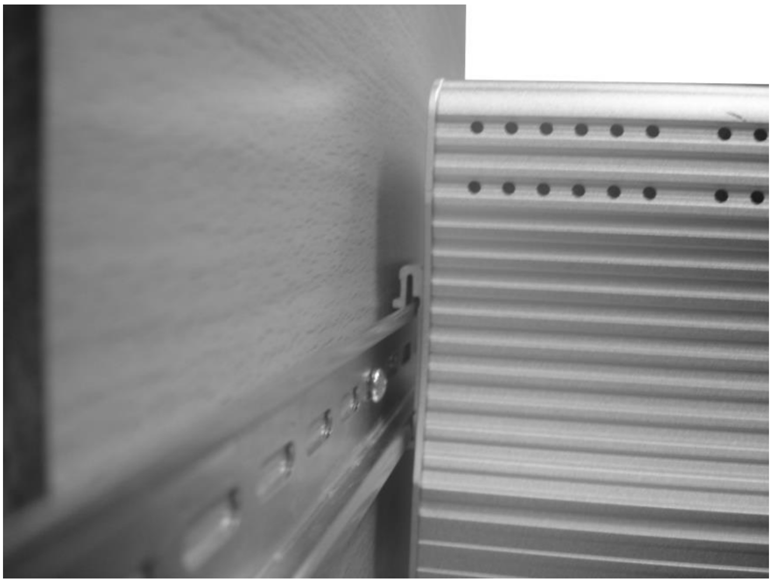
1. Use the screws to attach DIN-Rail clip to the real panel of JetNet Din Rail Switch.
2. To remove DIN-Rail clip, reverse step 1.

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

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



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

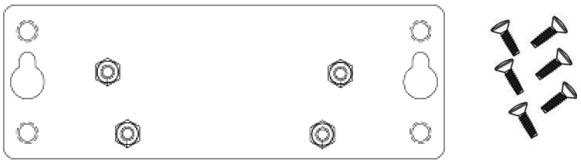


3. Check if DIN-Rail clip is tightly attached on the track.
4. To remove Switch from the track, reverse the steps above.

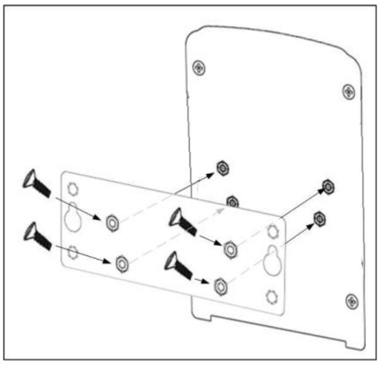
2.10 Wall Mounting Installation (Optional)

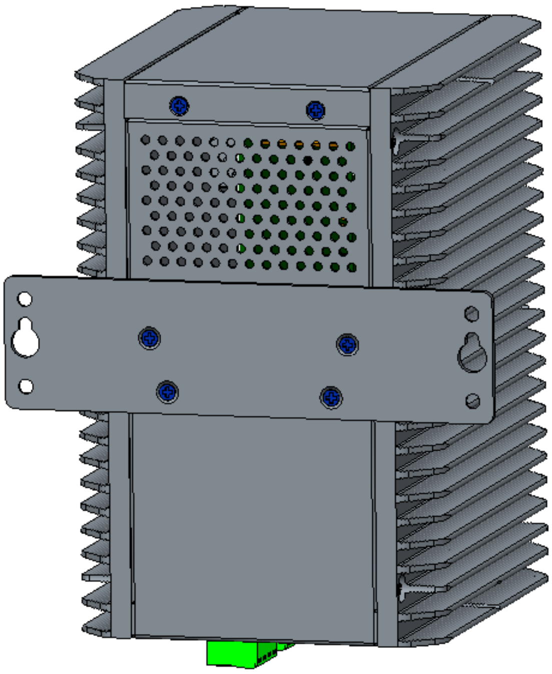
Follow the steps below to install JetNet 5020G with the wall-mounting plate.

1. Remove DIN-Rail clip from the switch, by loosening the screws.
2. Install the wall-mounting plate onto the rear panel of the switch. The screw positions are identical to the ones of DIN-Rail clip.
3. Makes sure that all the screws are tightened well.
4. Use the hook holes at the corners of the wall mounting plate to fix the switch on the wall.
5. Wall-mounting plate is optional. If there is a need, please contact Korenix local sales.



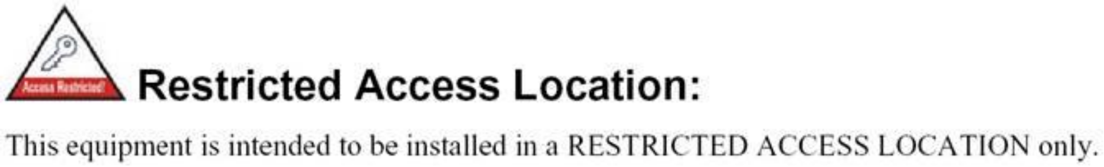
Wall-Mounting plate and screws





2.11 Safety Warning

The Equipment intended for installation in a Restricted Access Location.


Access Restricted!

Restricted Access Location:

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

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

”For tilslutning af de ovrige ledere, se medfolgende installationsvejledning”.

“Laite on liitettava suojamaadoitus-koskettimilla varustettuun pistorasiaan”

„Apparatet ma tilkoples jordet stikkontakt“

”Apparaten skall anslutas till jordat uttag”

3 Preparation for Management

JetNet 5020G Din Rail Industrial Managed Switch provides both in-band and out-band configuration methods. You can configure the device via RS232 console cable if you don’t attach the admin PC to your network, or if you lose network connection to your JetNet 5020G. This is so-called out-band management. It wouldn’t be affected by network performance.

The in-band management means you can remotely manage 5020G via the network. You can choose Telnet or Web-based management. You 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 5020G package, Korenix attached one RS-232 RJ-45 to DB-9 console cable. Please attach RS-232 DB-9 connector to your PC COM port, connect the other end to the Console port of the JetNet 5020G. Note: If you lost the cable, please contact with your sales or follow the pin assignment to buy a new one..

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 5020G is 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”.

```
Boot loader Rev. 2.0.0.1 (Tue Oct 13 16:19:29 CST 2015)
Starting....


Switch login: admin
Password:

JetNet5020G (version 0.0.21-20160118-11:00:03).
Copyright 2006-2015 Korenix Technology Co., Ltd.

Switch>
```

3.2 Preparation for Web Interface

JetNet 5020G provides HTTP Web Interface and Secured HTTPS Web Interface for web management.

3.2.1 Web Interface

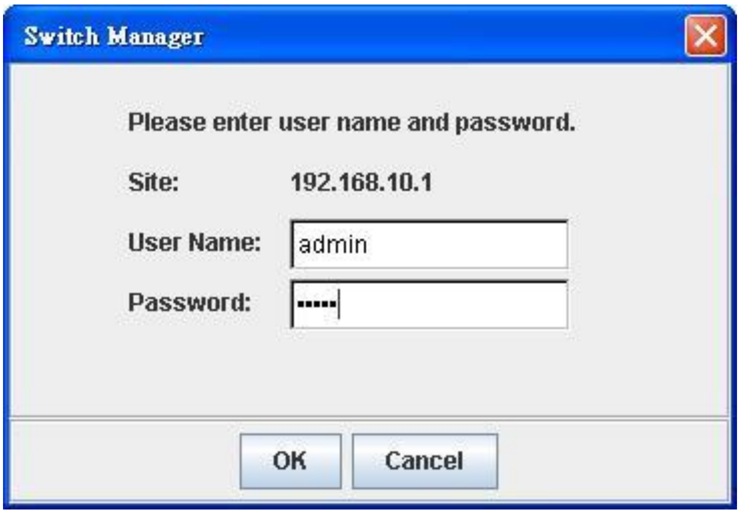
Korenix web management page is developed by JAVA. It allows you to use a standard web-browser such as Microsoft Internet Explorer, or Mozila, to configure and interrogate the switch from anywhere on the network.

Before you attempt to use the embedded web interface to manage switch operation, verify that your JetNet 5020G 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 Mozila 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**.



Switch Manager

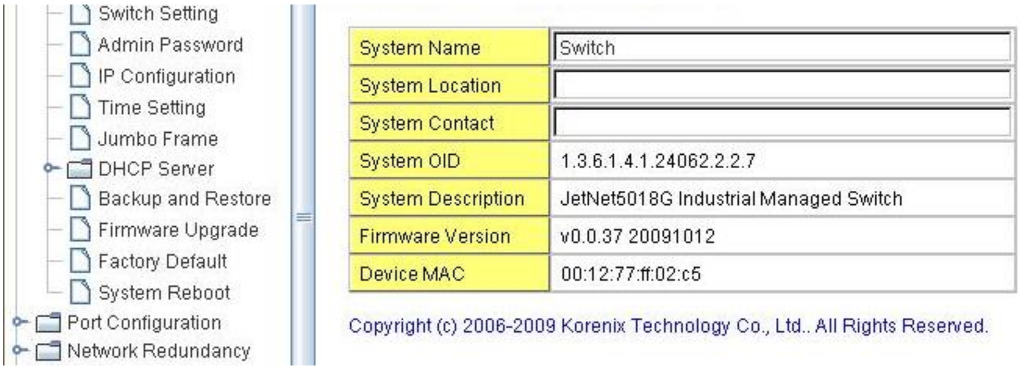
Please enter user name and password.

Site: 192.168.10.1

User Name: admin

Password: •••••

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



System Name	Switch
System Location	
System Contact	
System OID	1.3.6.1.4.1.24062.2.2.7
System Description	JetNet5018G Industrial Managed Switch
Firmware Version	v0.0.37 20091012
Device MAC	00:12:77:ff:02:c5

Copyright (c) 2006-2009 Korenix Technology Co., Ltd.. All Rights Reserved.

Once you enter the web-based management interface, you can freely change the Switch’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.

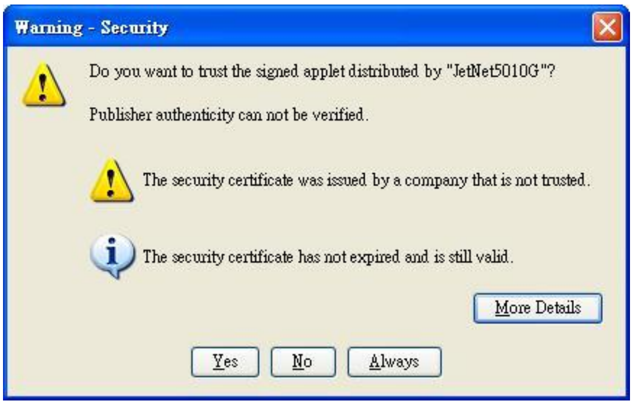
Note 2: The Web UI connection session of Managed Switch will be logged out automatically if you don’t give any input after 30 seconds. After logged out, you should re-login and key in correct user name and password again.

3.2.2 Secured Web Interface

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

Launch the web browser and Login.

1. Launch the web browser (Internet Explorer or Mozila Firefox) on the PC.
2. Type **https://192.168.10.1** (or the IP address of the switch). And then press **Enter**.
3. The pop up screen will appear and request you to trust the secured HTTPS connection distributed by Managed Switch first. Click “ **Yes”** to trust it.



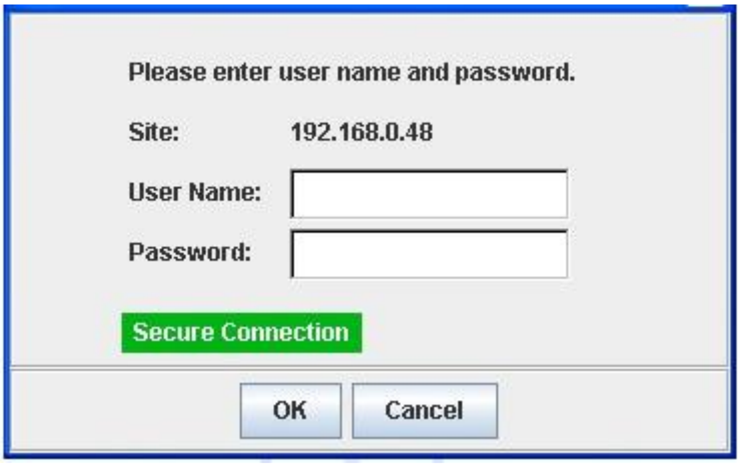
Do you want to trust the signed applet distributed by "JetNet5010G"?

Publisher authenticity can not be verified.

The security certificate was issued by a company that is not trusted.

The security certificate has not expired and is still valid.

4. The login screen will appear next.



Please enter user name and password.

Site: 192.168.0.48

User Name:

Password:

5. Key in the user name and the password. The default user name and password is **admin**.

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

7. Once you enter the web-based management interface, all the commands you see are the same as what you see by HTTP login.

3.3 Preparation for Telnet Console

3.3.1 Telnet

Korenix JetNet 5020G supports Telnet console. You can connect to the switch by Telnet and the command lines are the same as what you see by RS232 console port. Below are the steps to open Telnet connection to the switch.

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

3.3.2 SSH (Secure Shell)

Korenix JetNet 5020G 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.

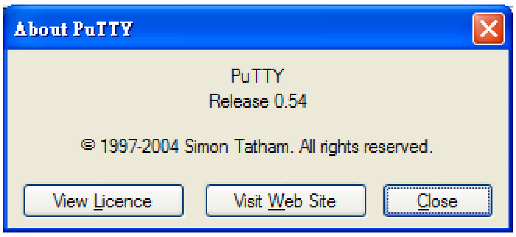
SSH is a client/server architecture while the Managed Switch is the SSH server. When you want to make SSH connection with the switch, you should download the SSH client tool first.

SSH Client

There are many free, sharewares, trials or charged SSH clients you can find on the internet. Fox example, PuTTY is a free and popular Telnet/SSH client. We'll use this tool to demonstrate how to login Managed Switch 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**



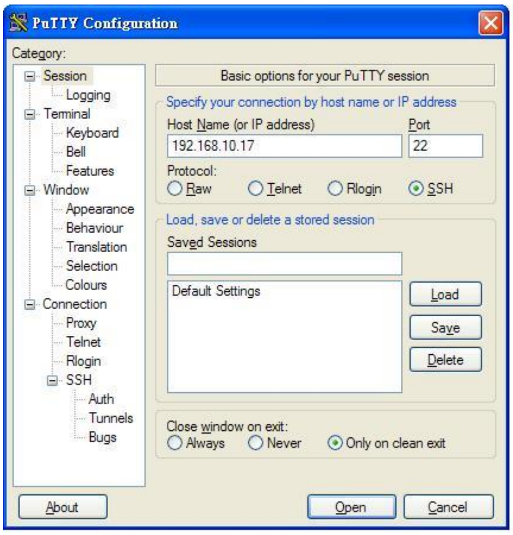
About PuTTY

PuTTY
Release 0.54

© 1997-2004 Simon Tatham. All rights reserved.

1. Open SSH Client/PuTTY

In the **Session** configuration, enter the **Host Name** (IP Address of your JetNet 5020G) and **Port number** (default = 22). Choose the "**SSH**" protocol. Then click on "**Open**" to start the SSH session console.



PuTTY Configuration

Basic options for your PuTTY session

Specify your connection by host name or IP address

Host Name (or IP address): 192.168.10.17

Port: 22

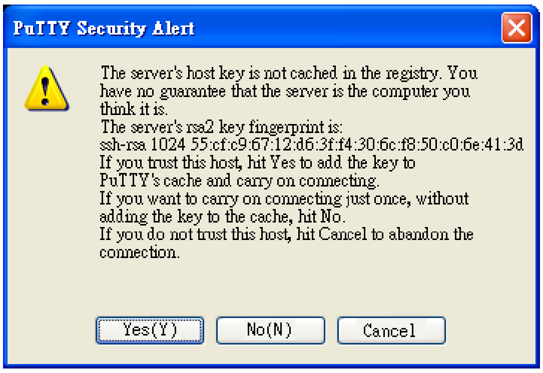
Protocol: ○ Raw ○ Telnet ○ Rlogin ● SSH

Load, save or delete a stored session

Saved Sessions: Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

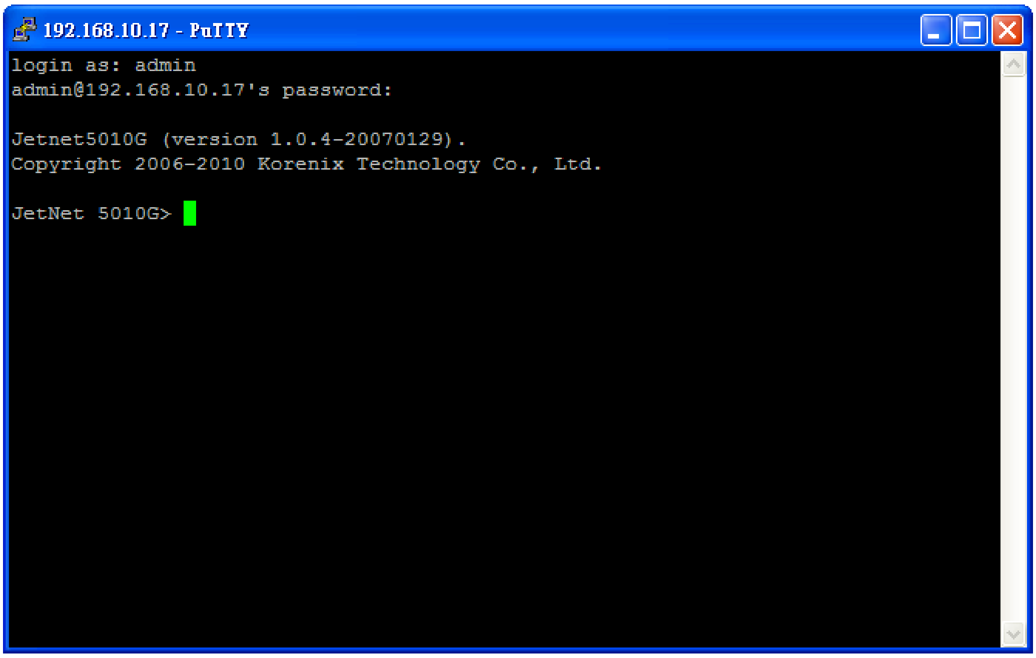
2. After click on **Open**, then you can see the cipher information in the popup screen. Press **Yes** to accept the Security Alert.



PuTTY Security Alert

The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.
The server's rsa2 key fingerprint is:
ssh-rsa 1024 55:cf:c9:67:12:d6:3f:f4:30:6c:f8:50:c0:6e:41:3d
If you trust this host, hit Yes to add the key to PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without adding the key to the cache, hit No.
If you do not trust this host, hit Cancel to abandon the connection.

3. After few seconds, the SSH connection to JetNet 5020G is opened. You can see the login screen as the below figure. (the following is refer to JetNet 5010G)



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

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

JetNet 5010G>
```

4. Type the Login Name and its Password. The default Login Name and Password are **admin / admin**.

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

4 Feature Configuration

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

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

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

The Web management page is developed by JAVA. It allows you to use a standard web-browser such as Microsoft Internet Explorer, or Mozila, to configure and interrogate the switch from anywhere on the network.

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

Following topics are covered in this chapter:

4.1 Command Line Interface (CLI) Introduction

4.2 Basic Setting

4.3 Port Configuration

4.4 Network Redundancy

4.5 VLAN

4.6 Private VLAN

4.7 Traffic Prioritization

4.8 Multicast Filtering

4.9 SNMP

4.10 Security

4.11 Warning

4.12 Monitor and Diag

4.13 Device Front Panel

4.14 Save

4.15 Logout

4.1 Command Line Interface Introduction

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

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

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

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

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

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 in" **configure terminal"** to enter next mode, and **"exit**" to leave. "**?** " to listing the command list

```
Switch#
       archive       manage archive files
       clear         Reset functions
       clock         Configure time-of-day clock
       configure     Configuration from vty interface
       copy          Copy from one file to another
       debug         Debugging functions (see also 'undebug')
       disable       Turn off privileged mode command
       dot1x         IEEE 802.1x standard access security control
       end           End current mode and change to enable mode
       exit          Exit current mode and down to previous mode
       list          Print command list
       mac           MAC interface commands
       no            Negate a command or set its defaults
       pager         Terminal pager
       ping          Send echo messages
       quit          Exit current mode and down to previous mode
       reboot        Reboot system
       reload        copy a default-config file to replace the current one
       show          Show running system information
       telnet        Open a telnet connection
       terminal      Set terminal line parameters
       traceroute    Trace route to destination
       write         Write running configuration to memory, network, or terminal
```

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

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

Available command lists of global configuration mode.

```
Switch# configure terminal
Switch(config)#
        access-list          Add an access list entry
        administrator        Administrator account setting
        clock                Configure time-of-day clock
        default              Set a command to its defaults
        dot1x                802.1x port-based authentication for the switch
        end                  End current mode and change to enable mode
        erps                 Ethernet Ring Protection Switching (ITU-T G.8032)
        ethernet-ip          Ethernet/IP Protocol
        exit                 Exit current mode and down to previous mode
        gmrp                 GMRP protocol
        gvrp                 GARP VLAN Registration Protocol
        hostname             Set system's network name
        interface            Select an interface to configure
        ip                   Global IP configuration subcommands
        ipv6                 IP information
        lacp                 Link Aggregation Control Protocol
        list                 Print command list
        lldp                 Link Layer Discovery Protocol
        log                  Logging control
        mac                  Global MAC configuration subcommands
        mac-address-table    mac address table
        mirror               Port mirroring
        modbus               Modbus TCP Slave
        multiple-super-ring  Configure Multiple Super Ring
        no                   Negate a command or set its defaults
        ntp                  Configure NTP
        ptp                  IEEE1588 Precision Time Protocol
        qos                  Quality of Service (QoS)
        relay                relay output type information
        service              System service
```

(Port) Interface Configuration: Press **interface IFNAME** in global configuration mode. You can then enter interface configuration mode. In this mode, you can configure port settings.

The port interface name of the fast Ethernet port is fa<Port Number>. Ex: Fast Ethernet Port 1 fa1, fast Ethernet port 7 is fa7, fast Ethernet port 17 is fa17.

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

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

Type **exit** to leave.

Type **?** to see the command list

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

```
Switch(config)# interface fa1
Switch(config-if)#
      acceptable          Configure 802.1Q acceptable frame types of a port.
      auto-negotiation    Enable auto-negotiation state of a given port
      description         Interface specific description
      dot1x               IEEE 802.1x access security control
      duplex              Specify duplex mode of operation for a port
      end                 End current mode and change to enable mode
      ethertype           Ethertype
      exit                Exit current mode and down to previous mode
      flowcontrol         Set flow-control value for an interface
      garp                General Attribute Registration Protocol
      ip                  Interface Internet Protocol config commands
      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
      sfp                 Small form-factor pluggable
      shutdown            Shutdown the selected interface
      spanning-tree       spanning-tree protocol
      speed               Specify the speed of a Fast Ethernet or a Gigabit Ethernet
port.
      storm-control       Enables packets flooding rate limiting features
```

(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
      ipv6          Interface Internet Protocol config commands
      list          Print command list
      no            Negate a command or set its defaults
      quit          Exit current mode and down to previous mode
      shutdown      Shutdown the selected interface
```

Summary of the 5 command modes.

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

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

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

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

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

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

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
```

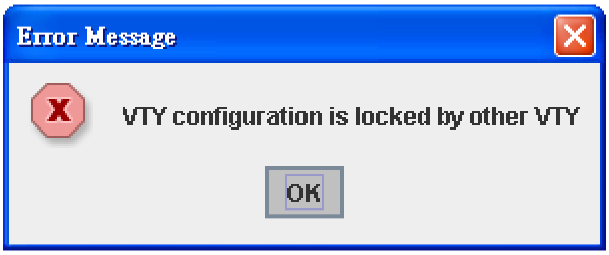
Ctrl+C To stop executing the unfinished command.

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. The Managed Switch allows only one administrator to configure the switch at a time.



VTY configuration is locked by other VTY

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 Load Default

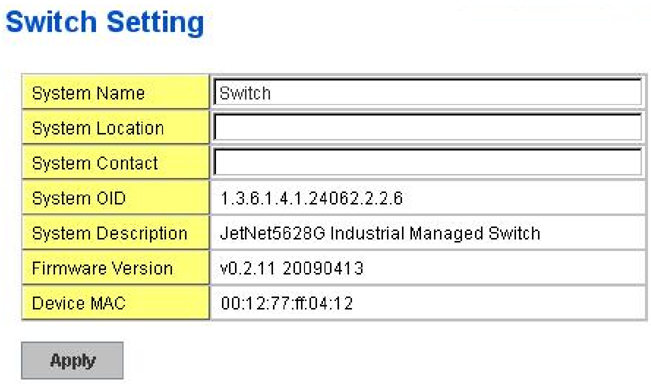
4.2.10 System Reboot

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



Switch Setting

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

System Name: You can assign a name to the device. The available character string length 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 character string length is 64.

System Contact: You can specify contact people here. You can type the name, mail address or other information of the administrator. The available character string length is 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: JetNet5020G Industrial Managed 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.

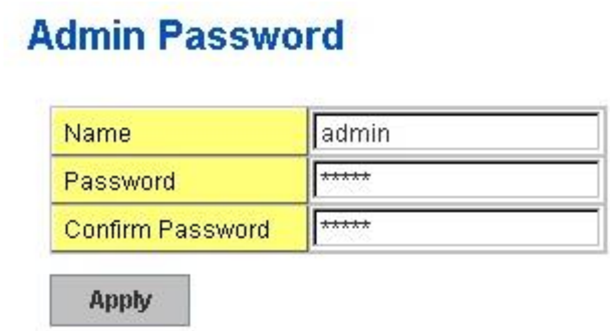
Once you finish the configuration, click on **Apply** to apply your settings.

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



Admin Password

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

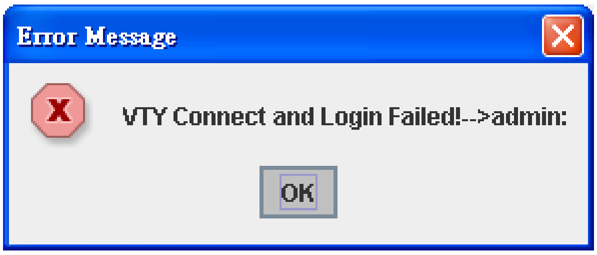
User name: You can key in new user name here. The default setting is **admin**.

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

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

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

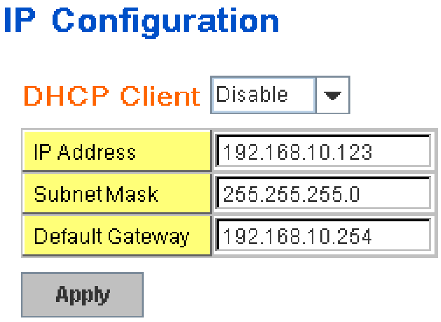
Figure 4.2.2.2 Popup alert window for Incorrect User name.



VTY Connect and Login Failed!-->admin:

4.2.3 IP Configuration

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



IP Configuration

DHCP Client: Disable

IP Address	192.168.10.123
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.254

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 5020G. If DHCP Client function is enabled, you don't need to assign an IP address to the JetNet 5020G, as it will be overwritten by DHCP server and shown here. The default IP address 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.

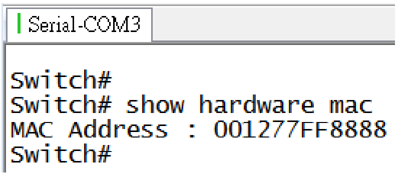
Default Gateway: You can assign the gateway for the switch here. The default gateway is 192.168.10.254.

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

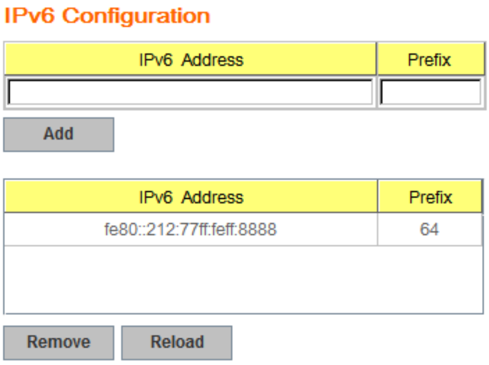
Once you finish configuring the settings, click on **Apply** to apply your configuration.

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.

The default IPv6 address of JetNet 5020G is generated from hardware MAC by IEEE-defined 64-bit Extended Unique Identifier (EUI-64), so that each JetNet 5020 owns her identicle default IPv6 address. (ex: 00:12:77:FF:88:88 -> fe80::212:77ff:feff:8888)



```
Switch#
Switch# show hardware mac
MAC Address : 001277FF8888
Switch#
```



IPv6 Configuration

IPv6 Address	Prefix

IPv6 Address	Prefix
fe80::212:77ff:feff:8888	64

IPv6 Address: a new IPv6 address can be assigned in this field.

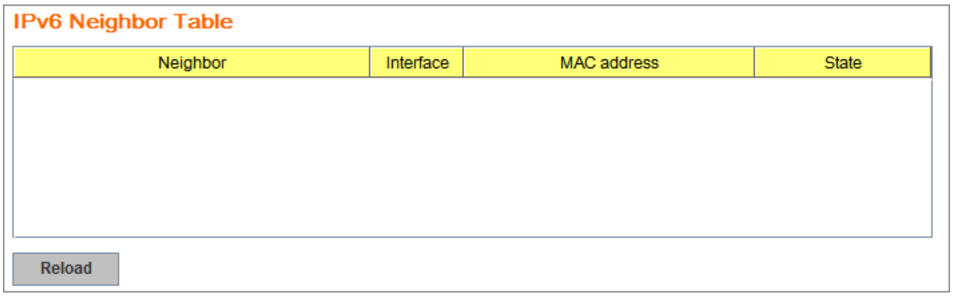
Prefix:the size of the subnet or network, and is equivalent to the subnet mask, but expressed in a different way. The default length of the subnet mask is 64bits, and written in decimal value - 64.

Add: after adding new IPv6 address and prefix, do not forget to click icon -"**Add**" to apply new address to the system.

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

Reload: refresh and reload IPv6 address listing.

IPv6 Neighbor Table: it shows the IPv6 address of the neighboring, connected interface, MAC address of the remote IPv6 device, and the current state of the neighboring devices.



IPv6 Neighbor Table

Neighbor	Interface	MAC address	State

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

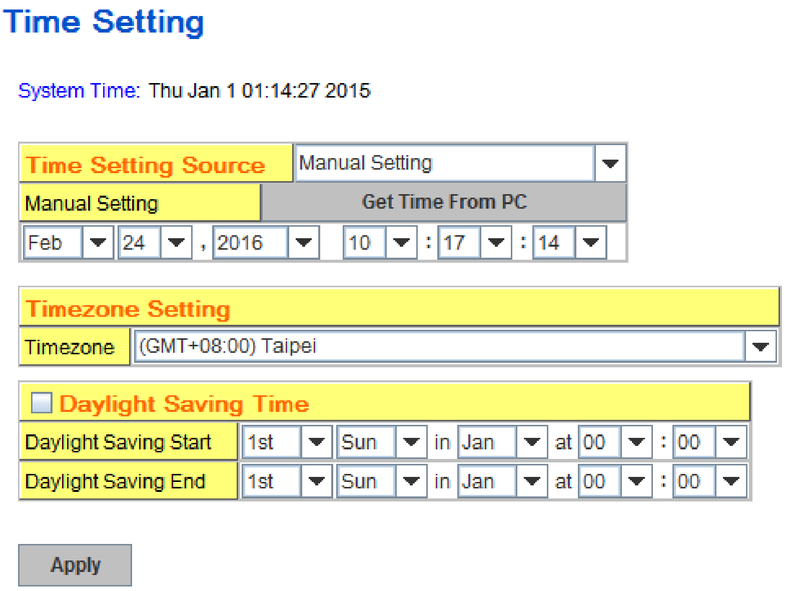
Time Setting source allow user to set the time manually or through NTP server. Network Time Protocol (NTP) is used to synchronize computer clocks on the internet. You can configure NTP settings here to synchronize the clocks of several switches on the network.

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.

JetNet 5020G also provides Daylight Saving function.

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



Time Setting

System Time: Thu Jan 1 01:14:27 2015

Time Setting Source	Manual Setting
Manual Setting	Get Time From PC
Feb 24 , 2016	10 : 17 : 14

Timezone Setting

Timezone	(GMT+08:00) Taipei

□ Daylight Saving Time

Daylight Saving Start	1st	Sun	in Jan	at 00	: 00
Daylight Saving End	1st	Sun	in Jan	at 00	: 00

Manual Setting: One can select "**Manual setting**" to change time by hand. Time setting in PC can also be acquired by clicking the button "**Get Time from PC**".. After applying the setting, the System Time displayed will be synchronized to PC.

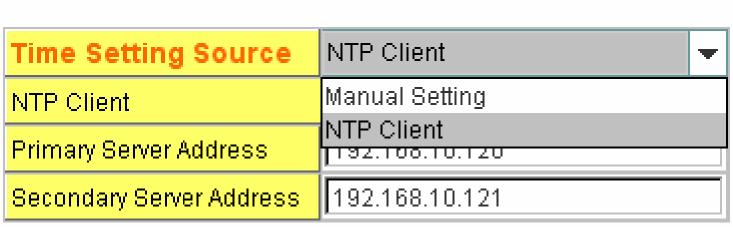
Time-zone: Select the time zone where the switch is located. Following table lists the time zones for different locations for your reference. The default time zone is GMT Greenwich Mean Time.

```
Switch(config)# clock timezone
   01   (GMT-12:00) Eniwetok, Kwajalein
   02   (GMT-11:00) Midway Island, Samoa
   03   (GMT-10:00) Hawaii
   04   (GMT-09:00) Alaska
   05   (GMT-08:00) Pacific Time (US & Canada) , Tijuana
   06   (GMT-07:00) Arizona
   07   (GMT-07:00) Mountain Time (US & Canada)
   08   (GMT-06:00) Central America
   09   (GMT-06:00) Central Time (US & Canada)
   10   (GMT-06:00) Mexico City
   11   (GMT-06:00) Saskatchewan
   12   (GMT-05:00) Bogota, Lima, Quito
   13   (GMT-05:00) Eastern Time (US & Canada)
   14   (GMT-05:00) Indiana (East)
   15   (GMT-04:00) Atlantic Time (Canada)
   16   (GMT-04:00) Caracas, La Paz
   17   (GMT-04:00) Santiago
   18   (GMT-03:00) NewFoundland
   19   (GMT-03:00) Brasilia
   20   (GMT-03:00) Buenos Aires, Georgetown
   21   (GMT-03:00) Greenland
   22   (GMT-02:00) Mid-Atlantic
   23   (GMT-01:00) Azores
   24   (GMT-01:00) Cape Verde Is.
   25   (GMT) Casablanca, Monrovia
   26   (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
   27   (GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
   28   (GMT+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague
   29   (GMT+01:00) Brussels, Copenhagen, Madrid, Paris
   30   (GMT+01:00) Sarajevo, Skopje, Sofija, Vilnius, Warsaw, Zagreb
   31   (GMT+01:00) West Central Africa
   32   (GMT+02:00) Athens, Istanbul, Minsk
   33   (GMT+02:00) Bucharest
   34   (GMT+02:00) Cairo
   35   (GMT+02:00) Harare, Pretoria
   36   (GMT+02:00) Helsinki, Riga, Tallinn
   37   (GMT+02:00) Jerusalem
   38   (GMT+03:00) Baghdad
   39   (GMT+03:00) Kuwait, Riyadh
   40   (GMT+03:00) Moscow, St. Petersburg, Volgograd
   41   (GMT+03:00) Nairobi
   42   (GMT+03:30) Tehran
   43   (GMT+04:00) Abu Dhabi, Muscat
   44   (GMT+04:00) Baku, Tbilisi, Yerevan
   45   (GMT+04:30) Kabul
   46   (GMT+05:00) Ekaterinburg
   47   (GMT+05:00) Islamabad, Karachi, Tashkent
   48   (GMT+05:30) Calcutta, Chennai, Mumbai, New Delhi
   49   (GMT+05:45) Kathmandu
   50   (GMT+06:00) Almaty, Novosibirsk
```

51 (GMT+06:00) Astana, Dhaka
52 (GMT+06:00) Sri Jayawardenepura
53 (GMT+06:30) Rangoon
54 (GMT+07:00) Bangkok, Hanoi, Jakarta
55 (GMT+07:00) Krasnoyarsk
56 (GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi
57 (GMT+08:00) Irkutsk, Ulaan Bataar
58 (GMT+08:00) Kuala Lumpur, Singapore
59 (GMT+08:00) Perth
60 (GMT+08:00) Taipei
61 (GMT+09:00) Osaka, Sapporo, Tokyo
62 (GMT+09:00) Seoul
63 (GMT+09:00) Yakutsk
64 (GMT+09:30) Adelaide
65 (GMT+09:30) Darwin
66 (GMT+10:00) Brisbane
67 (GMT+10:00) Canberra, Melbourne, Sydney
68 (GMT+10:00) Guam, Port Moresby
69 (GMT+10:00) Hobart
70 (GMT+10:00) Vladivostok
71 (GMT+11:00) Magadan, Solomon Is., New Caledonia
72 (GMT+12:00) Aukland, Wellington
73 (GMT+12:00) Fiji, Kamchatka, Marshall Is.
74 (GMT+13:00) Nuku'alofa

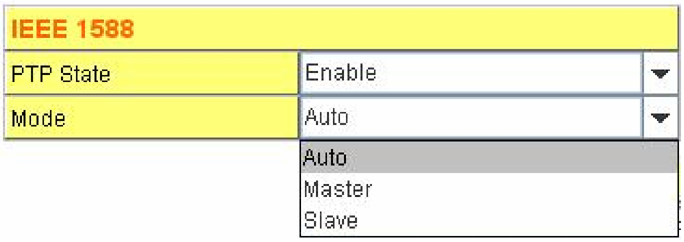
Click the check box to enable the Daylight Saving Function as the setting of start and end week or disable it.
Daylight Saving Start and **Daylight Saving End:** the functions allows the user to set up the daylight saving start- and end- week on a monthly basis.
Configuration can be accomplished by clicking on **Apply** button.

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



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

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
Master mode: switch performs PTP Master only.
Slave mode: switch performs PTP slave only.



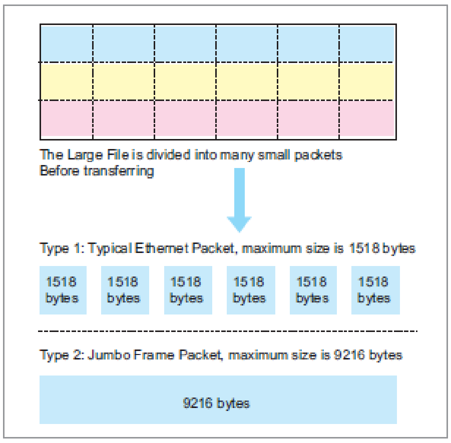
IEEE 1588	
PTP State	Enable
Mode	Auto

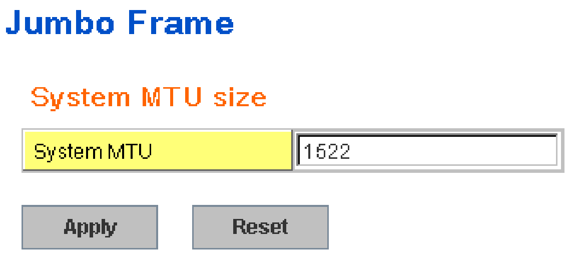
4.2.5 Jumbo Frame

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 2,000 bytes. The maximum Jumbo Frame size is 9,712 bytes. You can freely change the available packet size..


The Large File is divided into many small packets Before transferring
Type 1: Typical Ethernet Packet, maximum size is 1518 bytes
1518 bytes
1518 bytes
1518 bytes
1518 bytes
1518 bytes
1518 bytes
Type 2: Jumbo Frame Packet, maximum size is 9216 bytes
9216 bytes



Jumbo Frame

System MTU size

System MTU	1522

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

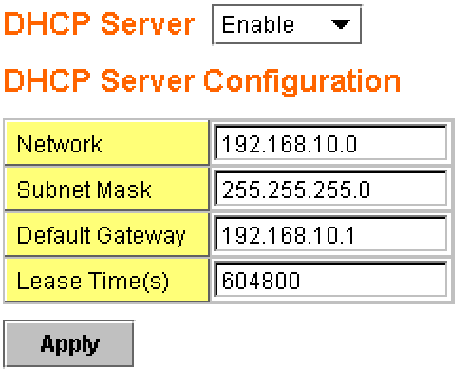
4.2.6 DHCP Server

You can select to **Enable** or **Disable** DHCP Server function. JetNet 5020G 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.

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



DHCP Server: Enable

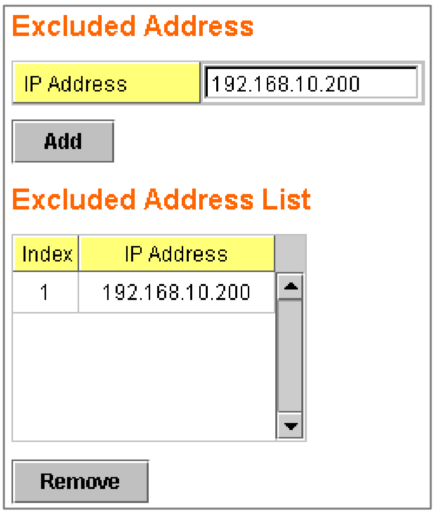
DHCP Server Configuration

Network	192.168.10.0
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.1
Lease Time(s)	604800

Excluded Address:

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

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



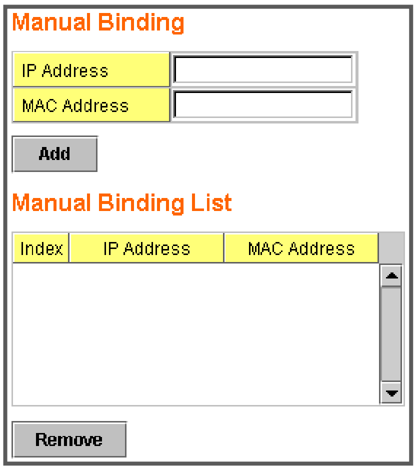
Excluded Address

IP Address	192.168.10.200

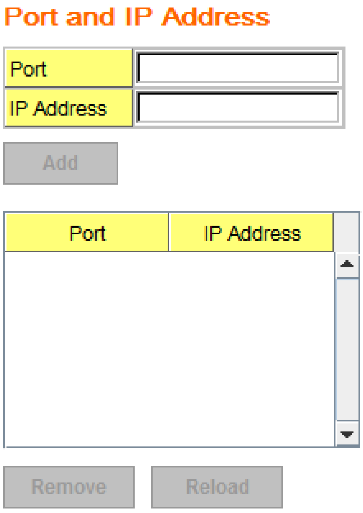
Excluded Address List

Index	IP Address
1	192.168.10.200

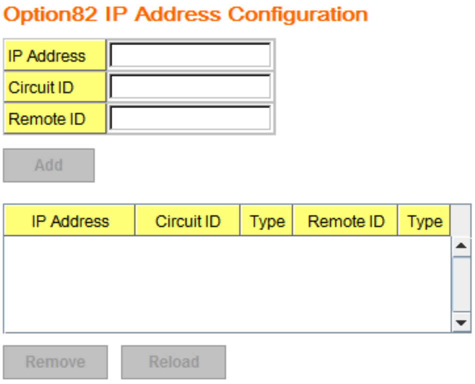
Manual Binding: the Managed Switch provides a MAC address and IP address binding and removing function. You can type in the specified IP and MAC address, and then click **Add** to add a new MAC&IP address binding rule for a specified link partner, like PLC or any device without **DHCP client** function.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



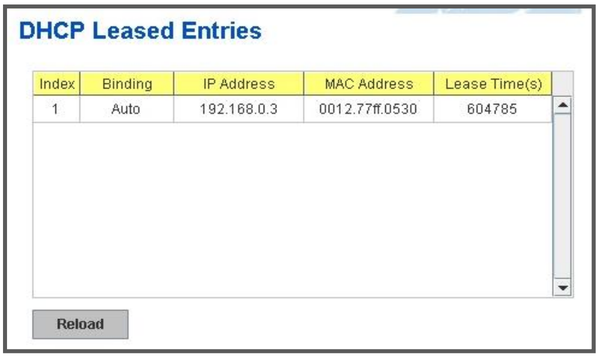
Port and IP Address (Port Based DHCP Server configuration): JetNet 5020G also supports port-based DHCP server function. It allows user assign specified IP address to specified port that DHCP client presented; and the DHCP server only offer the predefined IP address to the DHCP client.



Option 82 IP Address Configuration: The DHCP can assign IP address according to DHCP Option82 which sent from DHCP Relay Agent.



DHCP Leased Entries: JetNet 5020G provides assigned IP address list for user reference. It will show the MAC and IP address assigned by *5020G*. Click the **Reload** button to refresh the list.



DHCP Leased Entries

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

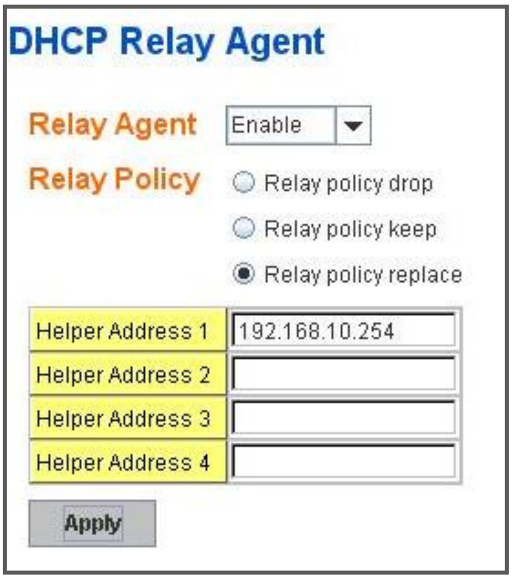
DHCP Relay Agent: The DHCP Relay Agent is also known as DHCP Option 82. It can help relay the DHCP Request to remote DHCP server located in different subnet.

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

Relay Agent: Choose Enable or Disable the relay agent.

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

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



DHCP Relay Agent

Relay Agent: Enable

Relay Policy:
○ Relay policy drop
○ Relay policy keep
● Relay policy replace

Helper Address 1	192.168.10.254
Helper Address 2	
Helper Address 3	
Helper Address 4	

DHCP Option82: You can configure the DHCP Option82 setting of the Relay Agent. Choose ‘Default’ or you can input any string for Circuit-ID and Remote-ID. By default, Circuit-ID is the combination of VLAN-ID/Port number, Remote-ID is the MAC address of Relay Agent.

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, the 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.

To activate the configuration after power reboot, **"Save to Flash" is a Must command**. Please check the description in Ch4.14

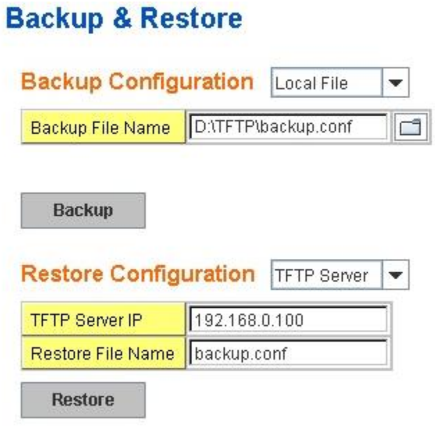
Technical Tip:

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.

Once you finish selecting and configuring the settings, click on **Backup** or **Restore** to run

Figure 4.2.7.1 Main UI of Backup & Restore



Backup & Restore

Backup Configuration: Local File

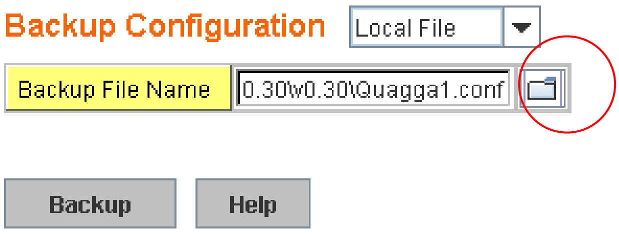
Backup File Name: D:\TFTP\backup.conf

Restore Configuration: TFTP Server

TFTP Server IP: 192.168.0.100

Restore File Name: backup.conf

Figure 4.2.7.2 Bacup/Restore Configuration – Local File mode.



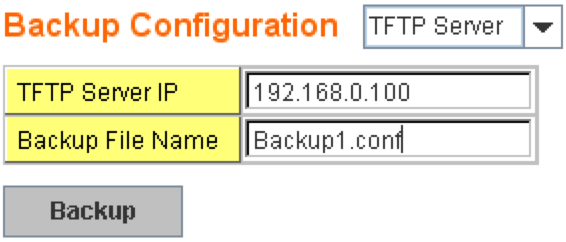
Backup Configuration: Local File

Backup File Name: 0.30\v0.30\Quagga1.conf

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

Note: It is not allowed to type in space key in the path of folder of backup file.

Figure 4.2.7.3 Backup/Restore Configuration – TFTP Server mode



Backup Configuration: TFTP Server

TFTP Server IP	192.168.0.100
Backup File Name	Backup1.conf

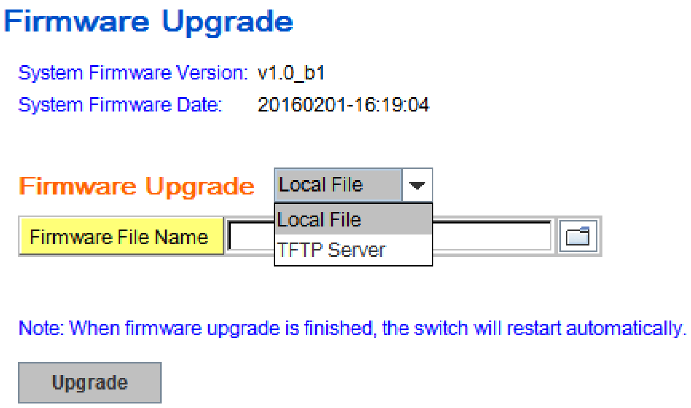
Type the IP address of TFTP Server IP. Then click on **Backup/Restore**.
Note: point to the wrong file can cause the entire configuration missed

4.2.8 Firmware Upgrade

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

Note that the system must be rebooted after you finished upgrading new firmware. Please remind the attached users before you reboot the switch.

Figure 4.2.8.1 Main UI of Firmware Upgrade



Firmware Upgrade

System Firmware Version: v1.0_b1
System Firmware Date: 20160201-16:19:04

Firmware Upgrade: Local File

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

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

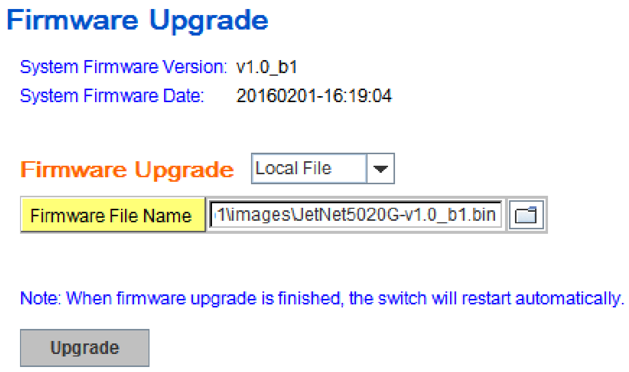
Local File mode: In this mode, the switch acts as the file server. Users can browse the target folder and then type the file name to backup the configuration. Users also can browse the target folder and select the existed configuration file to restore the configuration back to the switch. This mode is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

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

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

Firmware File Name: The file name of the new firmware.
The UI also shows you the current firmware version and built date of current firmware. Please check the version number after the switch is rebooted.

Figure 4.2.8.2 Firmware Upgrade – Local File mode.



Firmware Upgrade

System Firmware Version: v1.0_b1

System Firmware Date: 20160201-16:19:04

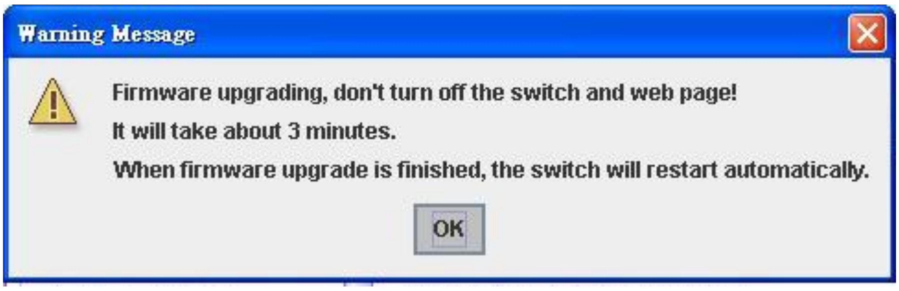
Firmware Upgrade: Local File

Firmware File Name: 1\images\JetNet5020G-v1.0_b1.bin

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

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

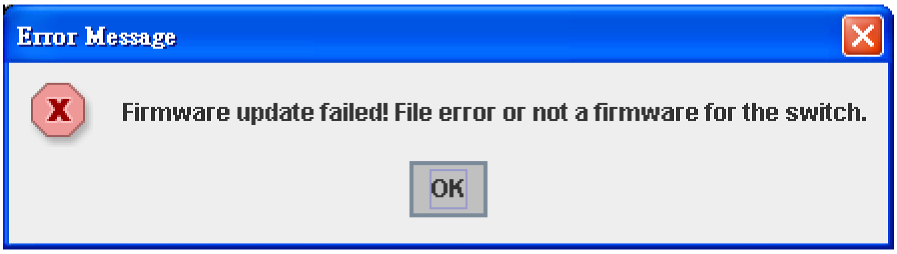
Figure 4.2.8.3 Warning Message.



Warning Message

Firmware upgrading, don't turn off the switch and web page!
It will take about 3 minutes.
When firmware upgrade is finished, the switch will restart automatically.

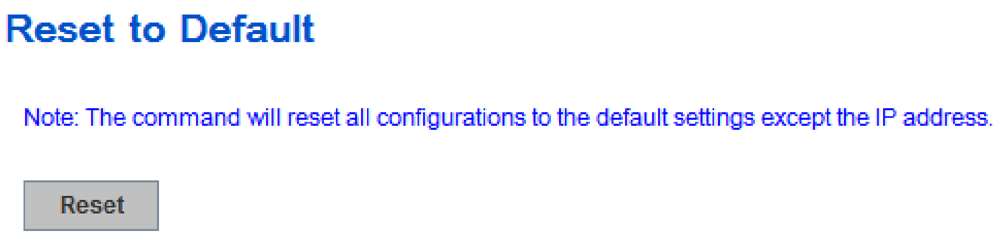
Figure 4.2.8.4 Error Message due to the file error or not a firmware for the switch.



Error Message

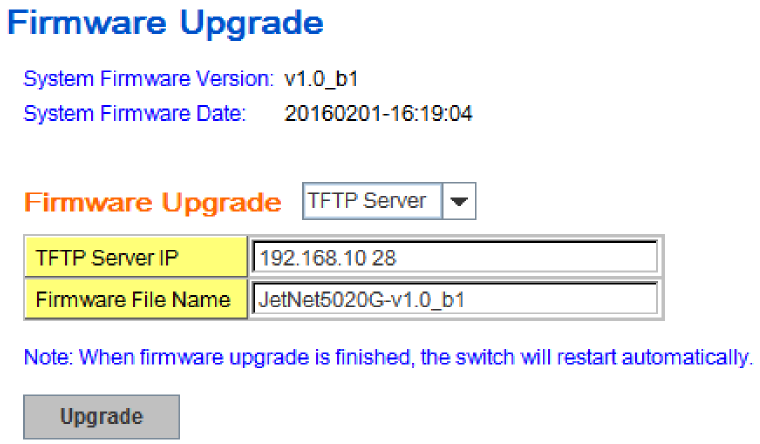
Firmware update failed! File error or not a firmware for the switch.

Before upgrading firmware, please check if the firmware matches JetNet 5020G. The switch provide protection when upgrading incorrect firmware file, the system would not crash even upload the incorrect firmware. Though we have the protection, we still ask you not trying to install the incorrect firmware to JetNet 5020G. Unexpected events may occur and cause damage to the system.



Reset to Default

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



Firmware Upgrade

System Firmware Version: v1.0_b1

System Firmware Date: 20160201-16:19:04

Firmware Upgrade: TFTP Server

TFTP Server IP	192.168.10 28
Firmware File Name	JetNet5020G-v1.0_b1

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

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

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

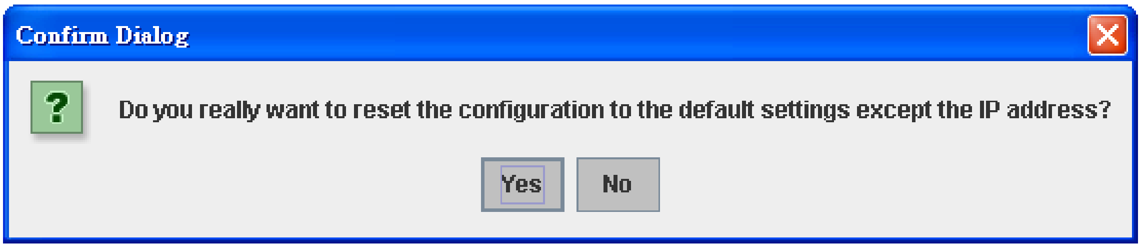
4.2.9 Laod Default

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

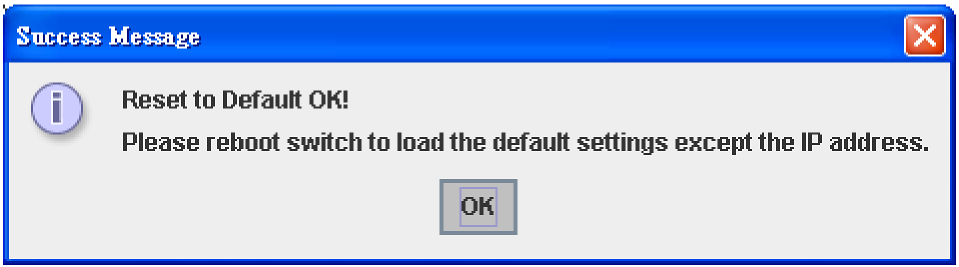
Figure 4.2.9.2 Popup alert screen to confirm the command. Click on **Yes** to start it.

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



Confirm Dialog

Do you really want to reset the configuration to the default settings except the IP address?



Success Message

Reset to Default OK!

Please reboot switch to load the default settings except the IP address.

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

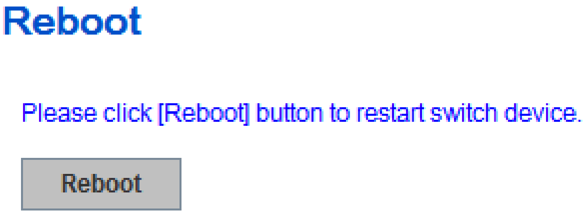
Note: If you already configured the IP of your device to other IP address, when you use this command by CLI and Web UI, our software will not reset the IP address to default IP. The system will remain the IP address so that you can still connect the switch via the network.

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.*

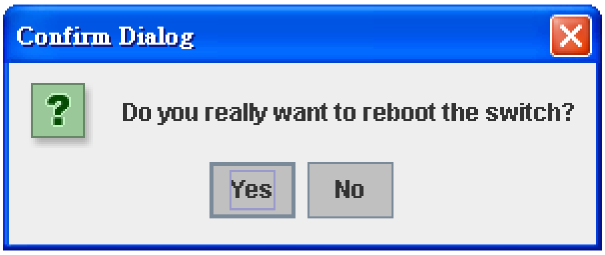
Figure 4.2.10.1 Main screen for Rebooting



Reboot

Please click [Reboot] button to restart switch device.

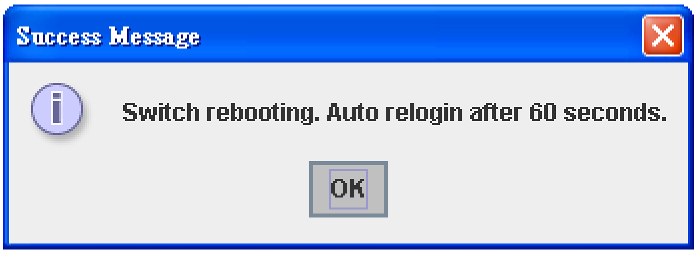
Figure 4.2.10.2 Pop-up alert screen to request confirmation. Click on **Yes**. Then the switch will be rebooted immediately.



Confirm Dialog

Do you really want to reboot the switch?

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



Switch rebooting. Auto relogin after 60 seconds.

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

4.2.11 CLI Commands for Basic Setting

Feature	Command Line
Switch Setting	
System Name	Switch(config)# hostname WORD Network name of this system Switch(config)# hostname JetNet 5020G Switch(config)#
System Location	Switch(config)# snmp-server location Taipei
System Contact	Switch(config)# snmp-server contact korecare@korenix.com
Display (System Name, Location, Contact; System Firmware and Loader version, MAC address, LED status)	Switch# show snmp-server name Switch Switch# show snmp-server location Taipei Switch# show snmp-server contact Korecare@korenix.com Switch# show version Hardware Information : Product Name : JetNet5020G Serial Number : 123412412 MAC Address : 001277FF8888 Manufacting Date : 2015/11/06 Software Information : Loader Version : 1.0.0.0 Firmware Version : 1.0_b1-20160201-16:19:04 Copyright 2006-2015 Korenix Technology Co., Ltd. Switc # show hardware led led information mac mac address Switch# show hardware led Power 1 : On Power 2 : Off DI 1 : Off

	DO 1 : Off RDY : On RM : Off RF : Off Switch# show hardware mac MAC Address : 001277FF8888
Admin Password	
User Name and Password	Switch(config)# administrator administrator Administrator account setting Switch(config)# administrator admin 8888 Change administrator account password ok **Note:** For JetNet 5020G, only password can be changed, but administrator cannot (default name/password: admin/admin). .
Display	Switch# show administrator Administrator account information name: admin password: 8888
IP Configuration	
IP Address/Mask (192.168.10.8, 255.255.255.0	Switch(config)# int vlan 1 Switch(config-if)# ip ip Interface Internet Protocol config commands ipv6 Interface Internet Protocol config commands Switch(config-if)# ip address 192.168.10.13/24 **(DHCP Client)** Switch(config-if)# ip dhcp client Switch(config-if)# ip dhcp client renew
Gateway	Switch(config)# ip route 0.0.0.0/0 192.168.10.254/24
Remove Gateway	Switch(config)# no ip route 0.0.0.0/0 192.168.10.254/24
Display (Management VLAN, Running-Config)	Switch# show int vlan 1 Interface vlan1 Description : N/A Administrative Status : Enable Operating Status : Up DHCP Client : Disable Primary IP Address : 192.168.10.13/24 IPv6 Address : fe80::212:77ff:feff:8888/64 Switch# show running-config Building configuration... Current configuration: hostname Switch ! vlan 1 ……… ! interface vlan1 ip address 192.168.10.13/24 no shutdown ! ip route 0.0.0.0/0 192.168.10.254 ! spanning-tree mst configuration exit !

	nameserver 1.1.1.1 nameserver 2.2.2.2 qos queue-sched sp qos trust-mode cos clock set 0:0:0 1 1 2015 administrator admin 1234 snmp-server community public ro snmp-server community private rw dot1x radius server-ip 192.168.10.100 key radius-key 1812 1813 !
IPv6 Address/Prefix	Switch(config)# interface vlan1 Switch(config-if)# ipv6 address 2001:0db8:85a3::8a2e:0370:7334/64
IPv6 Gateway	Switch(config)# ipv6 route 0::0/0 2001:0db8:85a3::8a2e:0370:FFFE
Remove IPv6 Gateway	Switch(config)#no ipv6 route 0::0/0 2001:0db8:85a3::8a2e:0370:FFFE
Display	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 ipv6 route ::/0 2001:db8:85a3::8a2e:370:fffe !
Time Setting	

NTP Server	Switch(config)# ntp peer
	    disable Disable NTP
	    enable Enable NTP
	    primary Primary peer
	    secondary Secondary peer
	Switch(config)# ntp peer primary
	    IPADDRESS IP address of peer
	Switch (config)# ntp peer primary 192.168.10.120

Time Zone	Switch(config)# clock timezone 60 60 (GMT+08:00) Taipei **Note:** By typing clock timezone ?, the timezone list will be shown for the user selections.
Jumbo Frame	
Jumbo Frame	Type the maximum MTU to enable Jumbo Frame: Switch(config)# system mtu 1518 bytes 2000 bytes 2032 bytes 9712 bytes Switch(config)# system mtu 9712 Switch(config)# exit Switch# show system mtu System MTU size is 9712 bytes

Disable Jumbo Frame	Switch(config)# no system mtu Switch(config)# exit Switch# show system mtu System MTU size is 2000 bytes
DHCP Server/Relay Agent	
DHCP Commands	Switch(config)# router dhcp Switch(config-dhcp)# default-router DHCP Default Router end Exit current mode and down to previous enable mode exit Exit current mode and down to previous mode ip IP protocol lease DHCP Lease Time list Print command list network dhcp network no remove quit Exit current mode and down to previous mode service enable service
DHCP Server Enable	Switch(config-dhcp)# service dhcp
DHCP Server Disable	Switch(config-dhcp)# no service dhcp
DHCP Server IP Pool (Network/Mask)	Switch(config-dhcp)# network A.B.C.D/M network/mask ex. 10.10.1.0/24 Switch(config-dhcp)# network 192.168.10.0/24
DHCP Server – Default Gateway	Switch(config-dhcp)# default-router A.B.C.D address Switch(config-dhcp)# default-router 192.168.10.254
DHCP Server – lease time	Switch(config-dhcp)# lease TIME seconds (60~31536000) Switch(config-dhcp)# lease 1000 (1000 second)
DHCP Server – Excluded Address	Switch(config-dhcp)# ip dhcp excluded-address A.B.C.D IP address Switch(config-dhcp)# ip dhcp excluded-address 192.168.10.123
DHCP Server – Static Port-IP binding	Switch(config-dhcp)# ip dhcp static port PORT IP Address Switch(config-dhcp)# ip dhcp static port 3 111.111.111.111
DHCP Server – Static MAC-IP binding	Switch(config-dhcp)# ip dhcp static 0012.7700.0001 A.B.C.D leased IP address Switch(config-dhcp)# ip dhcp static 0012.7700.0001 192.168.10.99
DHCP Relay – Enable DHCP Relay	Switch(config-dhcp)# ip dhcp relay information option
DHCP Relay – DHCP policy	Switch(config-dhcp)# ip dhcp relay information policy drop Relay Policy keep Drop/Keep/Replace option82 field replace Switch(config-dhcp)# ip dhcp relay information policy drop Switch(config-dhcp)# ip dhcp relay information policy keep Switch(config-dhcp)# ip dhcp relay information policy replace
DHCP Relay – IP Helper Address	Switch(config-dhcp)# ip dhcp helper-address A.B.C.D Switch(config-dhcp)# ip dhcp helper-address 192.168.10.200

Reset DHCP Settings	Switch(config-dhcp)# ip dhcp reset
DHCP Server Information	Switch# show ip dhcp server statistics DHCP Server ON Address Pool 1 network:192.168.10.0/24 default-router:192.168.10.254 lease time:604800 Excluded Address List IP Address --------------- 192.168.10.123 Manual Binding List IP Address MAC Address --------------- -------------- 192.168.10.99 0012.7701.0203 Leased Address List IP Address MAC Address Leased Time Remains --------------- -------------- --------------------
DHCP Relay Information	Switch# show ip dhcp relay DHCP Relay Agent ON -------------------------------------- IP helper-address : 192.168.10.200 Re-forwarding policy: Replace
Backup and Restore	
Backup Startup Configuration file	Switch# copy startup-config tftp: 192.168.10.33/default.conf Writing Configuration [OK] ***Note 1:*** *To backup the latest startup configuration file, you should save current settings to flash first. You can refer to 4.12 to see how to save settings to the flash.* *Note 2: 192.168.10.33 is the TFTP server's IP and default.conf is the name of the configuration file. In your environment, a different IP address or different file name may be used. Please type adequate TFTP server IP or file name in this command.*
Restore Configuration	Switch# copy tftp: 192.168.10.33/default.conf startup-config
Show Startup Configuration	Switch# show startup-config
Show Running Configuration	Switch# show running-config
Firmware Upgrade	
Firmware Upgrade	Switch# archive download-sw /overwrite tftp 192.168.10.33 JN5020G.bin Firmware upgrading, don't turn off the switch! Tftping file JN5020G.bin Firmware upgrading ....

	Firmware upgrade success!! Rebooting.......
Factory Default	
Factory Default	Switch# reload default-config file
System Reboot	
Reboot	Switch# reboot

4.3 Port Configuration

This chapter delivers guidance on the configuration of switch ports, including port state enable/disable, auto-negotiation, speed, duplex, flow control, rate limit control and port aggregation settings. The view on port status and aggregation information can be also achieved.

Following commands are included :

4.3.1 Understand the port mapping

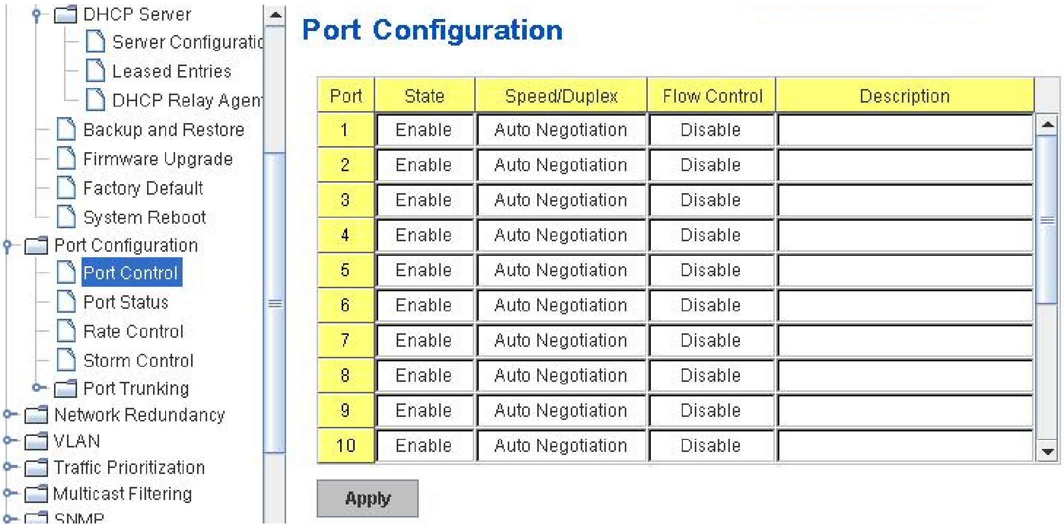
Before the port setting, please check the port allocation of JetNet 5020G, which is printed on the front panel. Follow the port ID to configure JetNet 5020G.

There are 16 Fast Ethernet ports and 4 Giga Combo ports. In Web UI, the port number is available from port 1~20. Port 1~16 represent Fast Ethernet ports, and 17~20 stand for Giga Combo ports. In CLI, fa1, fa2…fa16 represent Fast Ethernet ports and gi17, gi18…gi20 represent Giga Combo ports.

4.3.2 Port Control

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

Figure 4.3.2.1 The main Web UI of the Port Configuration.



Port Configuration

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

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

In **State** column, the selected port can be enabled or disabled. Once the port disabled, the port linkage is down and stop to forward any traffic. The default setting is Enable which means all the ports are functional when you receive the device.

In **Speed/Duplex** column, the port speed and duplex mode can be configured, including the following selections :

Fast Ethernet Port 1~16 (fa1~fa16): AutoNegotiation, 10M Full Duplex(10 Full), 10M Half Duplex(10 Half), 100M Full Duplex(100 Full) and 100M Half Duplex(100 Half).

Gigabit Ethernet Combo Port 17~20 (gi17~gi20): 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 is Auto Negotiation mode.

Note: Gigabit Ethernet Combo ports port (SFP 17, 18, 19 and 20) in JetNet 500-020G default support 1000M. You can use the command line to set speed to 100M. Remember to set it back to 1000M when you use the 1000M SFPthe transceiver you need to manually configure the speed in CLI by the speed type, please follow the steps at CLI command.

Fiber port speed adjustment (gi17~20)	
100Mbps **SFP Transceiver**	Switch# configure terminal Switch(config)# int gi17 Switch(config-if)# media-type sfp speed 100 Set the SFP speed ok!
1000Mbps **SFP Transceiver**	Switch# configure terminal Switch(config)# int gi17 Switch(config-if)# media-type sfp speed 1000 Set the SFP speed ok!

In **Flow Control** column, in order to enable flow control, **“Symmetric”** must be both applied on local and remote devices, cooresponding ly. If **“Disable”** on either one end, it cannot be assured that the flow control can work perfectly. It is recommended to enable flow control under Auto Negotiation mode. When using SFP, same speed models are suggested to utilized on both end devices.

In **Description** column, you can add description to indicate the port location, connected device or other information. This is a friendly design especially in remote management of the device.

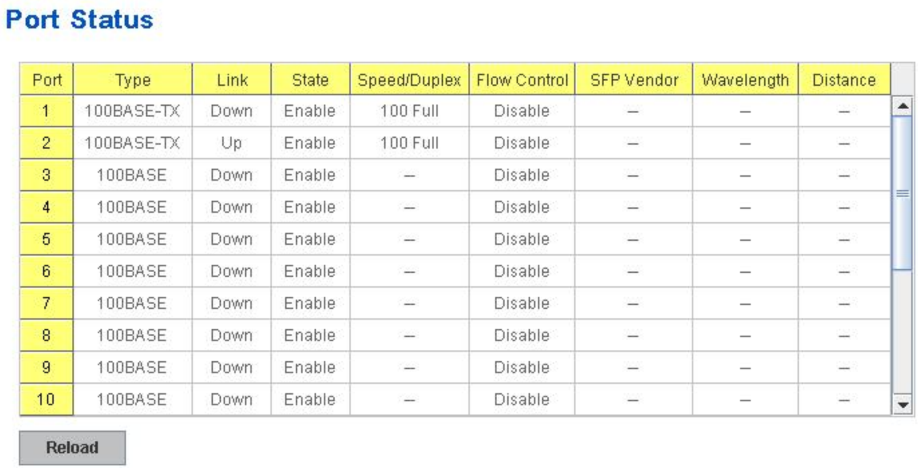
Once you finish the configuration, click on **Apply** to save the configuration.

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

4.3.3 Port Status

Port Status exposes the current port status after negotiations.

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



Port Status

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

The description of the columns is as below:
Port: Port interface number.
Type: 100BASE-TX -> Fast Ethernet copper port. 100BASE-FX -> 100Base-FX Fiber Port. 1000BASE-T -> Gigabit Ethernet Copper port. 1000BASE-X-> Gigabit Fiber Port
Link: Link status. Up -> Link UP. Down -> Link Down.
State: Enable -> State is enabled. Disable -> The port is disable/shutdown.
Speed/Duplex: Current working status of the port.
Flow Control: The state of the flow control.
SFP Vendor: Vendor name of the SFP transceiver you plugged. The information is only applied to on board ports.
Wavelength: The wave length of the SFP transceiver you plugged.
Distance: The transmission distance of the SFP transceiver you plugged.

Reload: reload the all SFP port information.

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

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

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

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

Rx Power (dBm): The specificat Figure 4.3.3.2 ver 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 SFP transceiver family. If you see Unknown info, it may mean that the vendor doesn't provide their information or that the information of their transceiver can't be read.

2. If the DDM SFP transceiver is not certified, the DDM function will not be supported. But the communication will keep working.

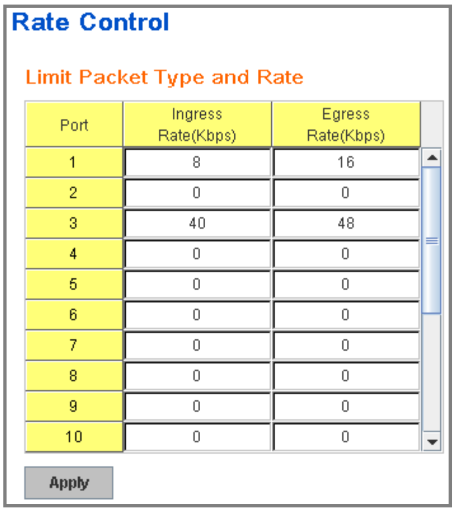
Note: Most of the SFP transceivers provide vendor information which allows your switch to read it. The UI can display vendor name, wave length and distance of all SFP transceiver family. If you see Unknown info, it may mean that the SFP transceiver is not certified by our Quality system, and the vendor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

DDM SFP transceiver.

4.3.4 Rate Control

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

Figure 4.3.4.1 shows you the Limit Rate of Ingress and Egress. You can type the volume in the blank. The volume space of JetNet 5020G is 8Kbps.



Rate Control

Limit Packet Type and Rate

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

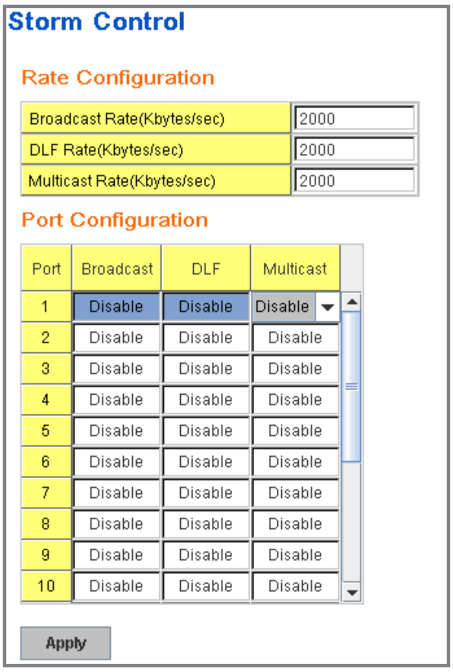
4.3.5 Storm Control

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

Figure 4.3.5.1

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

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



Storm Control

Rate Configuration

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

Port Configuration

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

Choose **Enable/Disable** to enable or disable the storm control packet type of the specific port. Click on **Apply** to apply the configuration of the ports.

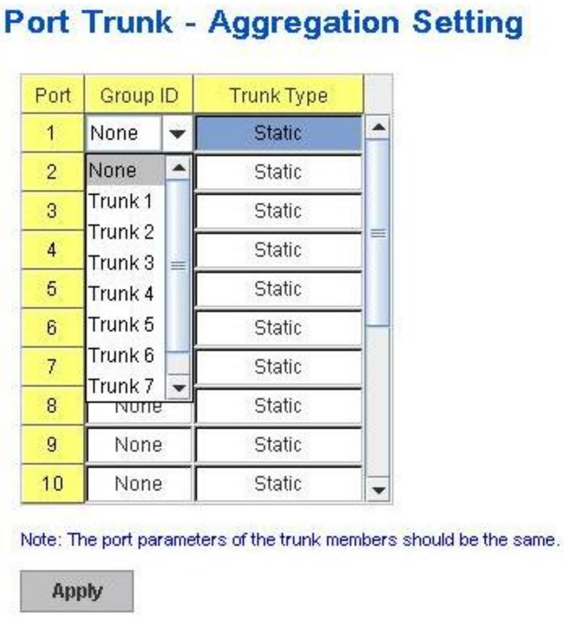
4.3.6 Port Trunking

Port Trunking configuration allows you to group multiple Ethernet ports in parallel to increase the link bandwidth. The aggregated ports can be viewed as one physical port so that the bandwidth is higher than 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 a 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 is compliant to IEEE standard, 802.3ad.

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

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



Port Trunk - Aggregation Setting

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

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

Aggregation Setting

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

Group ID: Group ID is the ID for the port trunking group. Ports with same group ID are in the same group. Trunk ID from Trunk 1 to Trunk 8 can be selected.

Trunk Type: Static and **802.3ad LACP.** Each Trunk Group can support either Static or 802.3ad LACP. Trunk Type of the non-active ports cannot be altered.

Load Balance Type: Each Trunk Group can support srcMAC, dstMAC, srcIP, dstIP and it's combination.

src-mac	-> load distribution is based on the source MAC address
dst-mac	-> load distribution is based on the destination-MAC address
src-dst-mac	-> load distribution is based on the source and destination MAC address
src-ip	-> load distribution is based on the source IP address
dst-ip	-> load distribution is based on the destination IP address
src-dst-ip	-> load distribution is based on the source and destination IP address

Extended setting in CLI:

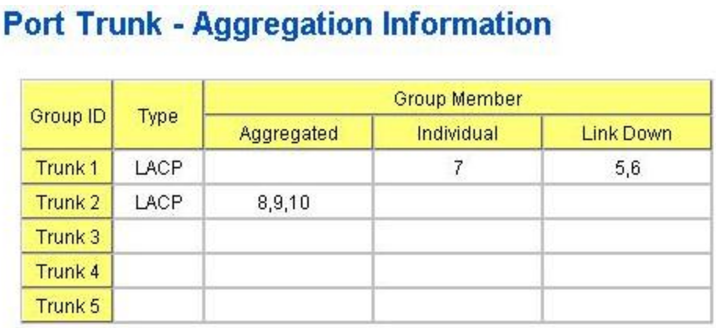
Port Priority: The command allows you to change the port priority setting of the specific port. LACP port priority is configured on each port using LACP. The port priority can be configured through the CLI. The higher the number, the lower the priority. The default value is 32768.

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

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

Aggregation Status

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



Port Trunk - Aggregation Information

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

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

Type: Static or LACP set up in Aggregation Setting.

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

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

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

4.3.7 Command Lines for Port Configuration

Feature	Command Line
Port Control	
Port Control – State	Switch(config-if)# shutdown -> Disable port state interface fastethernet1 is shutdown now.

	Switch(config-if)# no shutdown -> Enable port state interface fastethernet1 is up now.
Port Control – Auto Negotiation	Switch(config-if)# auto-negotiation Auto-negotiation of port 1 is enabled!
Port Control – Force Speed/Duplex	Switch(config-if)# speed 100 set the speed mode ok! Switch(config-if)# duplex full set the duplex mode ok!
Port Control – Flow Control	Switch(config-if)# flowcontrol on Flowcontrol on for port 1 set ok! Switch(config-if)# flowcontrol off Flowcontrol off for port 1 set ok!
Fiber port speed adjustment (gi17~20)	
100Mbps **SFP Transceiver**	Switch# configure terminal Switch(config)# int gi17 Switch(config-if)# media-type sfp speed 100 Set the SFP speed ok!
1000Mbps **SFP Transceiver**	Switch# configure terminal Switch(config)# int gi17 Switch(config-if)# media-type sfp speed 1000 Set the SFP speed ok!
Port Status	
Port Status	Switch# show interface fa1 Interface fastethernet1 Description : N/A Administrative Status : Enable Operating Status : Connected Duplex : Auto (Full) Speed : Auto (100) MTU : 2000 Flow Control : off Default Port VLAN ID: 1 Acceptable Frame Type : All Auto Negotiation : Enable Loopback Mode : None STP Status: Forwarding Default CoS Value for untagged packets is 0. Medium mode is Copper. Switch# show sfp ddm →show SFP DDM information Port 17 Temperature:N/A Tx power:N/A Rx power:N/A Port 18 Temperature:64.00 C <range :0.0-80.00> Tx power:-6.0 dBm <range : -9.0 - -4.0> Rx power:-30.0 dBm <range: -30.0 - -4.0>

	Switch(config-if)# sfp ddm Digital diagnostic and monitoring eject Eject SFP scan Scan SFP *Note: Administrative Status -> Port state of the port. Operating status -> Current status of the port. Duplex -> Duplex mode of the port. Speed -> Speed mode of the port. Flow control -> Flow Control status of the port.*
Rate Control	

Rate Control – Ingress or Egress	Switch(config-if)# rate-limit
	  egress Outgoing packets
	  ingress Incoming packets
	
	Note: To enable rate control, you should select the Ingress or Egress rule first; then assign the packet type and bandwidth.

Rate Control - Bandwidth	Switch(config-if)# rate-limit ingress bandwidth <0-1000000> Limit in kilobits per second (FE: 0-100000, GE: 0-1000000, 0 is no limit) Switch(config-if)# rate-limit ingress bandwidth 800 Set the ingress rate limit 800Kbps for Port 1.
Storm Control	
Strom Control – Rate Configuration (Packet Type)	Switch(config-if)# storm-control broadcast Broadcast packets dlf Destination Lookup Failure multicast Multicast packets SWITCH(config)# storm-control broadcast ? <1~1000000> Rate limit value 1~1000000 Kbits/sec SWITCH(config)# storm-control broadcast 1000 Enables rate limit for Broadcast packets for Port 1 SWITCH(config)# storm-control multicast 1000 Enables rate limit for Multicast packets for Port 1 SWITCH(config)# storm-control dlf 1000 Enables rate limit for Destination Lookup Failue packets for Port1.

Display – Rate Configuration and port status	SWITCH# show storm-control
	Storm-control rate limit:
	  Storm-control for Port 1
	    Broadcast packets: Enabled Rate: 992 (Kbps)
	  Destination Lookup Failure packets: Enabled Rate: 992 (Kbps)
	  Multicast packets: Enabled Rate: 992 (Kbps)
	Storm-control for Port 2
	  Broadcast packets: Disabled
	  Destination Lookup Failure packets: Disabled
	  Multicast packets: Disabled
	Storm-control for Port 3
	  Broadcast packets: Disabled
	  Destination Lookup Failure packets: Disabled
	  Multicast packets: Disabled

	Storm-control for Port 4
	  Broadcast packets: Disabled
	  Destination Lookup Failure packets: Disabled
	  Multicast packets: Disabled
	……….

Port Trunking	
LACP	Switch(config)# lacp group 1 fa8-10 Group 1 based on LACP(802.3ad) is enabled! *Note: The interface list is fa1,fa3-5, fa8-10* Note: different speed port can’t be aggregated together.
LACP – Port Setting	SWITCH(config-if)# lacp port-priority LACP priority for physical interfaces timeout assigns an administrative LACP timeout SWITCH(config-if)# lacp port-priority <1-65535> Valid port priority range 1 - 65535 (default is 32768) SWITCH(config-if)# lacp timeout long specifies a long timeout value (default) short specifies a short timeout value SWITCH(config-if)# lacp timeout short Set lacp port timeout ok.
Static Trunk	Switch(config)# trunk group <1-8> Valid group range 1-8 Switch(config)# trunk group 2 fa6-7 Trunk group 2 enable ok! Switch(config)# trunk group 1 fa11-12 Trunk group 1 enable ok! Switch(config)# trunk group 2 fa11-12 Can't set trunk group 2 enable! The group 2 is a static aggregation group.

Display – LACP	Switch# show lacp
	    counters LACP statistical information
	    group LACP group
	    internal LACP internal information
	    neighbor LACP neighbor information
	    port-setting LACP setting for physical interfaces
	    system-id LACP system identification
	    system-priority LACP system priority
	
	SWITCH# show lacp port-setting
	
	LACP Port Setting :
	Port Priority Timeout
	----- --------- --------
	      1 32768 Long
	      2 32768 Long
	      3 32768 Long
	……….
	Switch# show lacp internal
	LACP group 1 internal information:
	            LACP Port Admin Oper Port
	Port Priority Key Key State
	----- ----------- -------- -------- -------
	      8 1 8 8 0x45
	      9 1 9 9 0x45
	     10 1 10 10 0x45

	LACP group 2 is inactive LACP group 3 is inactive LACP group 4 is inactive
Display - Trunk	Switch# show trunk group 1 FLAGS: I -> Individual P -> In channel D -> Port Down Trunk Group TGID Protocol Load-Balance Ports -----+---------+------------+------------------------------------- 1 Static src-dst-mac 11(D) 12(P)

4.4 Network Redundancy

It is critical to build up a non-stop network for industrial applications. We develop several standard (STP, RSTP and MSTP) and patent redundancy protocol, Multiple Super Ring, to achieve the network redundancy protected well by management switch.

JetNet 5020G 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 3rd generation Ring redundancy technology. This is patent-protected by Korenix and 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 one Korenix switch can aggregate multiple Rings within itself. 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 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 Patented TrunkRing Technology.

Advanced Rapid Dual Homing(RDH) technology also facilitates *JetNet 5020G* to connect with a core managed switch easily and conveniently. With RDH technology, you can also couple several Rapid Super Rings or RSTP cloud together.

Following commands are included in this group:

4.4.1 STP Configuration

4.4.2 STP Port Configuration

4.4.3 STP Information

4.4.4 MSTP Configuration

4.4.5 MSTP Port Configuration

4.4.6 MSTP information

4.4.7 Multiple Super Ring

4.4.8 Multiple Super Ring Information

4.4.9 ERPS Configuration

4.4.9 Command Lines for Network Redundancy

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

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

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

4.4.1 STP Configuration

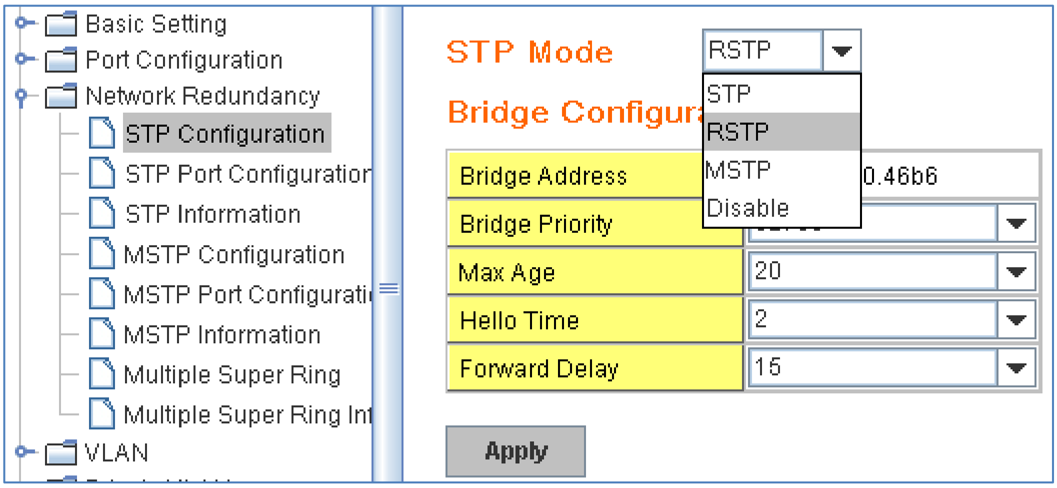
This page shows how to modify the STP mode and the global STP/RSTP Bridge Configuration.

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 Mode: RSTP

Bridge Configur

Bridge Address	0.46b6
Bridge Priority	
Max Age	20
Hello Time	2
Forward Delay	15

RSTP

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 convinent of the GUI design. When you configure the value through the CLI or SNMP, you may need to type the value directly. Please follow the n x 4096 ruls for the Bridge Priority.

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

If the managed Switch 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 the Managed Switch 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 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 of the Managed Switch will wait before checking to see if it should be changed to a different state.

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

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

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

4.4.2 STP Port Configuration

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

Port Configuration

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

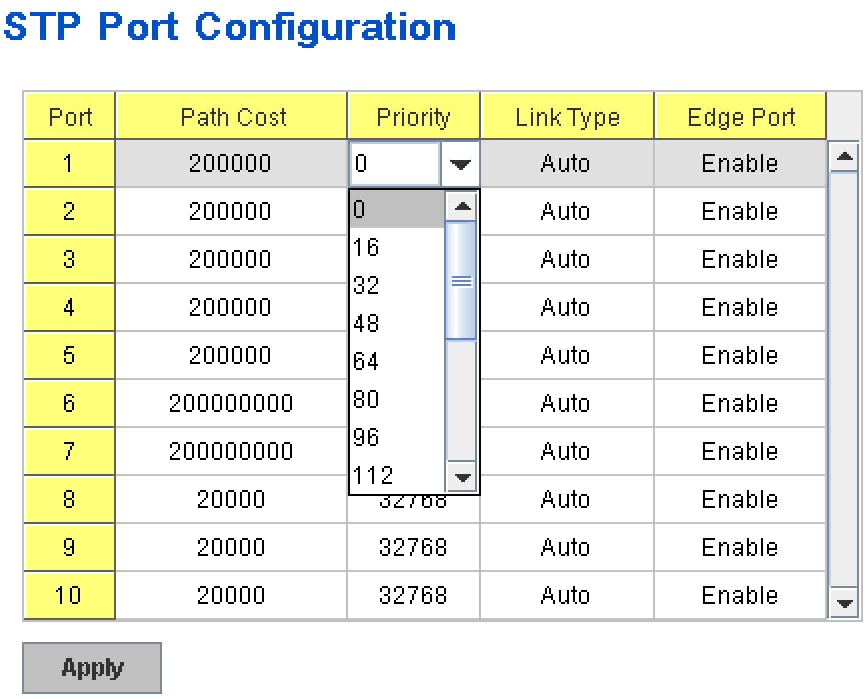
Path Cost: Enter a number between 1 and 200,000,000. This value represents the "cost" of the path to the other bridge from the transmitting bridge at the specified port.

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

Link Type: There are 3 link types for your selection-**Auto, P2P** and **Share.**

Some of the rapid state transitions that are possible within RSTP depend upon whether the port of concern can only be connected to another bridge (i.e. it is served by a point-to-point LAN segment), or if it can be connected to two or more bridges (i.e. it is served by a shared-medium LAN segment). This function allows link status of the link to be manipulated administratively. "**Auto**" means to auto select P2P or Share mode. "**P2P"** means P2P is enabled; the 2 ends work in full duplex mode. While "**Share"** is enabled, it means P2P is disabled; the 2 ends may connect through a share media and work in half duplex mode.

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



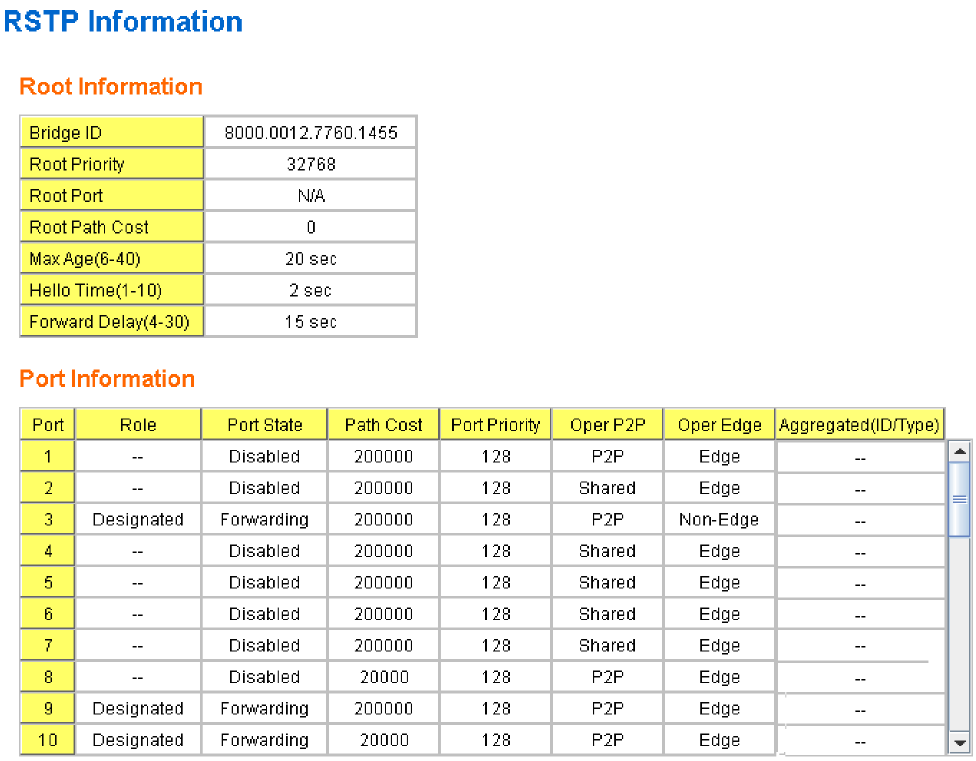
STP Port Configuration

Port	Path Cost	Priority	Link Type	Edge Port
1	200000	0	Auto	Enable
2	200000		Auto	Enable
3	200000		Auto	Enable
4	200000		Auto	Enable
5	200000		Auto	Enable
6	200000000		Auto	Enable
7	200000000		Auto	Enable
8	20000	32768	Auto	Enable
9	20000	32768	Auto	Enable
10	20000	32768	Auto	Enable

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

4.4.3 RSTP Info

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



RSTP Information

Root Information

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

Port Information

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

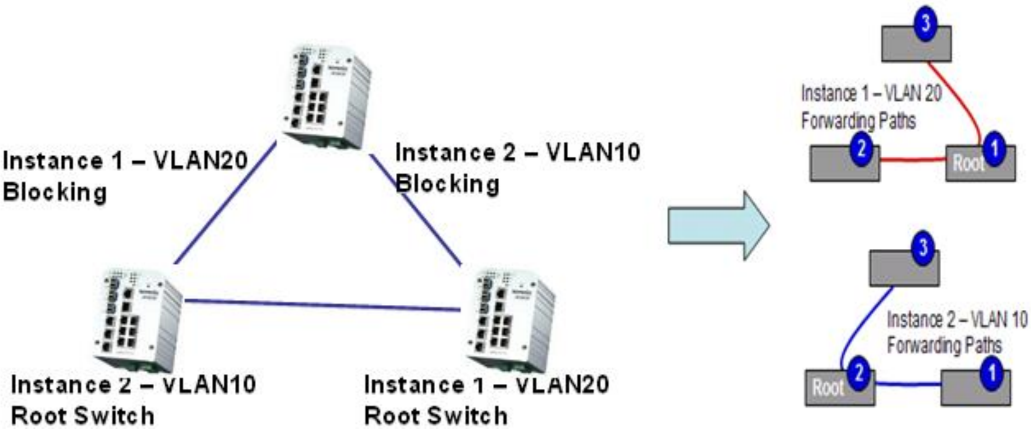
4.4.4 MSTP (Multiple Spanning Tree Protocol) Configuration

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

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

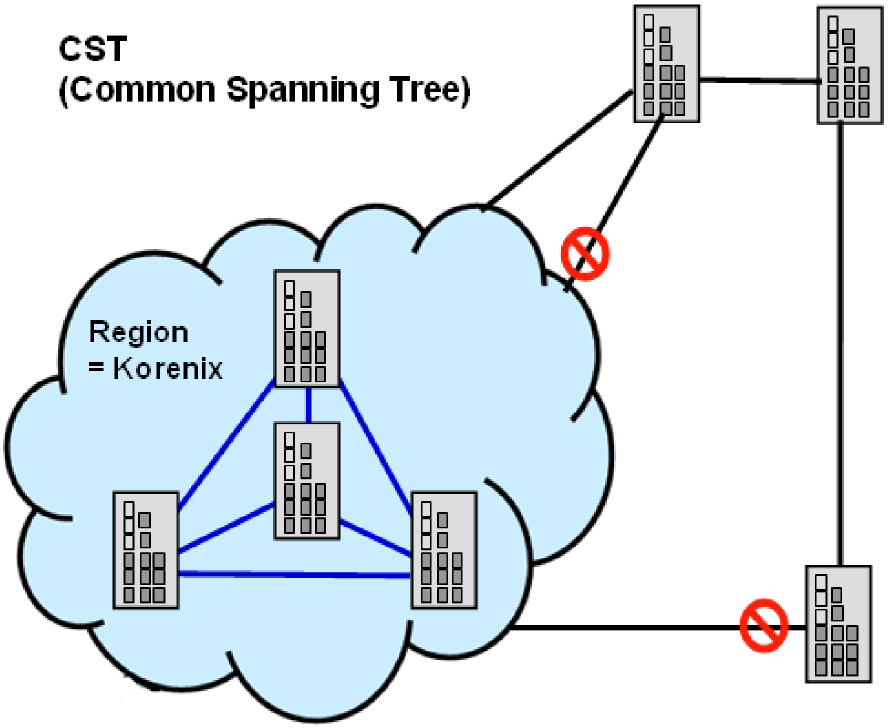
One VLAN can be mapped to a Multiple Spanning Tree Instance (MSTI). For example, the maximum Instance of the Managed Switch supports is usually 16, range from 0-15. The MSTP builds a separate Multiple Spanning Tree (MST) for each instance to maintain connectivity among each of the assigned VLAN groups.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

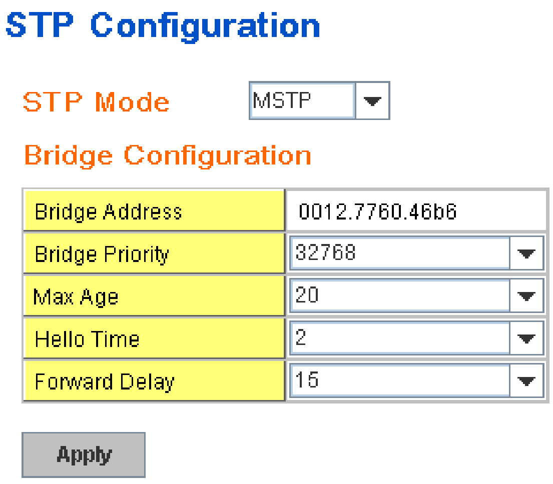


A Common Spanning Tree (CST) interconnects all adjuacent MST regions and acts as a virtual bridge node for communications with STP or RSTP nodes in the global network. MSTP connects all bridges and LAN segments with a single Common and Internal Spanning Tree (CIST). The CIST is formed as a result of 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 has different instances and its own forwarding path and table, however, it acts as a single Brige of CST.



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



STP Configuration

STP Mode: MSTP

Bridge Configuration

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

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

MSTP Region Configuration

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

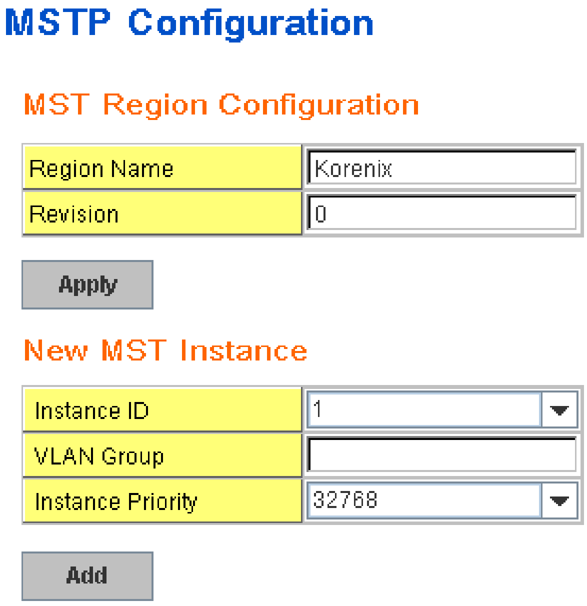
Region Name: The name for the Region. Maximum length: 32 characters.

Revision: The revision for the Region. Range: 0-65535; Default: 0)

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

New MST Instance

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



MSTP Configuration

MST Region Configuration

Region Name	Korenix
Revision	0

New MST Instance

Instance ID	1
VLAN Group	
Instance Priority	32768

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

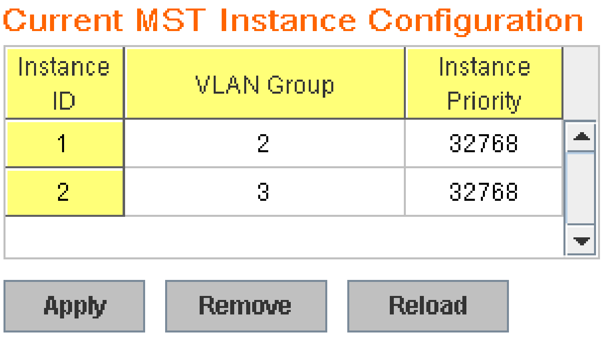
VLAN Group: Type the VLAN ID you want mapping to the instance.

Instance Priority: Assign the priority to the instance.

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

Current MST Instance Configuration

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



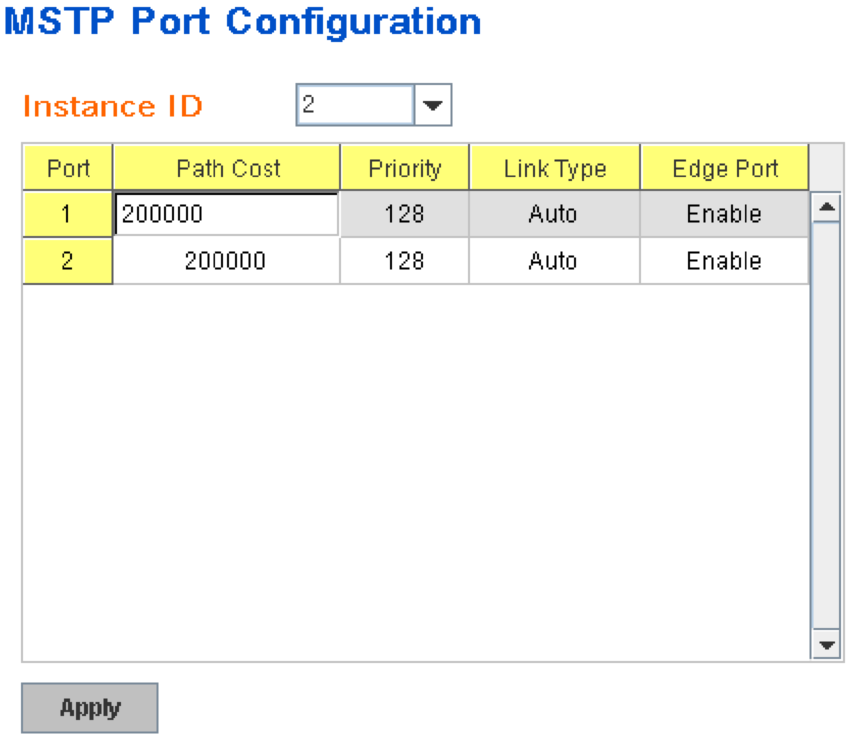
Current MST Instance Configuration

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

4.4.5 MSTP Port Configuration

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

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



MSTP Port Configuration

Instance ID: 2

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.**

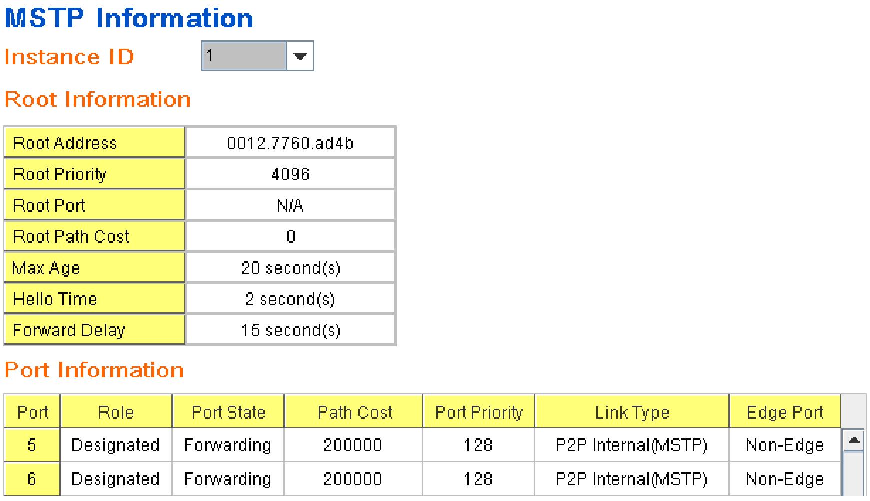
Some of the rapid state transitions that are possible within RSTP depend upon whether the port of concern can only be connected to another bridge (i.e. it is served by a point-to-point LAN segment), or if it can be connected to two or more bridges (i.e. it is served by a shared-medium LAN segment). This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

4.4.6 MSTP Information

This page allows you to see the current MSTP information.
Choose the **Instance ID** first. If the instance is not added, the information remains blank.
The **Root Information** shows the setting of the Root switch.
The **Port Information** shows the port setting and status of the ports within the instance.



MSTP Information

Instance ID: 1

Root Information

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

Port Information

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

Click on "**Reload**" to reload the MSTP information display.

4.4.7 Multiple Super Ring (MSR)

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

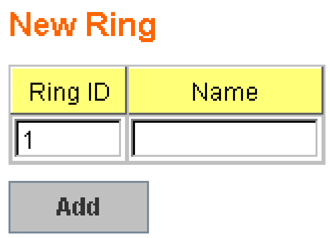
Multiple Super Ring (MSR) technology is 3rd generation Ring redundancy technology. This is patented and used in countries all over the world. MSR ranks the fastest restore and failover time in the world, 0 ms for restore and about milliseconds level for failover for 100Base-TX copper port. The other interface may take longer time due to the media characteristics.

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

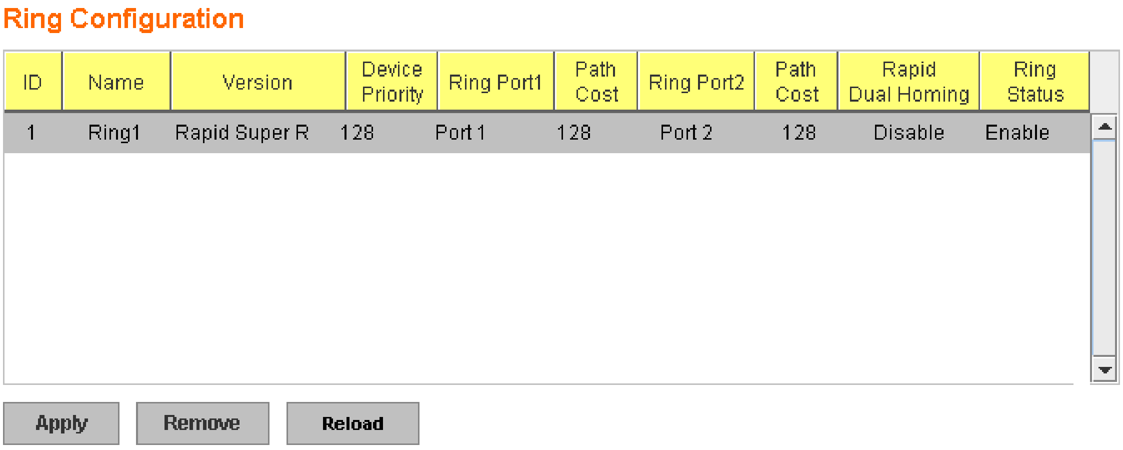
MultiRing is an outstanding technology. The Multiple rings can be aggregated within one switch by using different Ring ID. The maximum Ring number one switch can support is half of total port volume. For example, if the Managed Switch is a 24 Fast Ethernet + 4 Gigabit port design, that means maximum 14 Rings (12 x 100M Rings and 2 Gigabit Rings) can be aggregated to one 24+4G Managed Switch. The feature saves much effort when constructing complex network architecture.

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	



Ring Configuration

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

Ring Configuration

ID: Once a Ring is created, it appears and cannot 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”.

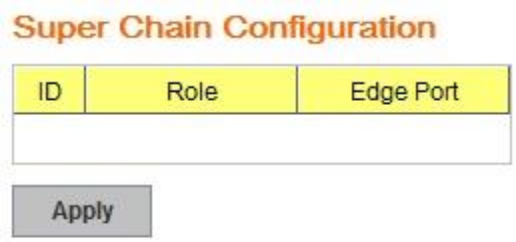
Version: The version of Ring can be changed here. There are two modes to choose:

Rapid Super Ring and Super Chain, the Rapid Super Ring as default.

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.



Super Chain Configuration

ID	Role	Edge Port

Ring Port2: Assign another port for ring connection

Path Cost: Change the Path Cost of Ring Port2

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

RDH Ext. ID: Rapid Dual Homing Extension ID. The Extension ID and Ring ID cannot be the same, when dual home to the same foreing network. The Extension ID range from 0 to 7. With the combination of Extension ID(0 to 7) and Ring ID(0 to 31), we can now support up to 256(8*32) different dual homing rings

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 the other entire link to avoid loop. If the primary link failed, Rapid Dual Homing will automatically forward the secondary link for network redundant. Of course, if there are more connections, they will be standby links and recover one of then if both primary and secondary links are broken.

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

Super Chain Configuration

ID: The Ring Identifier referring to this Ring(Chain).

Role: Super Chain has two node role Border and Member. Border is the node which connect to foreign network. Member is the node except the Border node in the Super Chain.

Edge Port: Edge Port is one of ring ports of Border node. It is used to connect to foreign network.

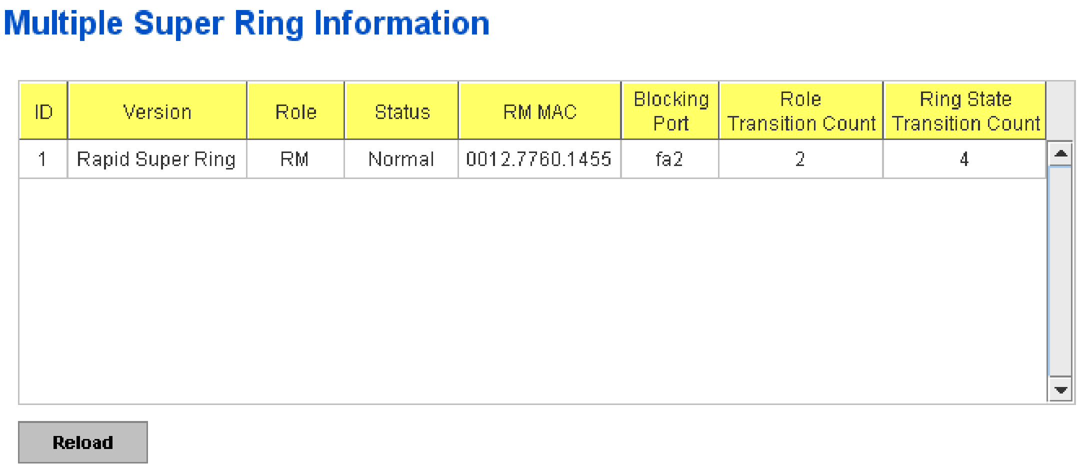
MultiRing: The MultiRing technology is one of the patterns of the MSR technology; the technology allows you to aggregate multiple rings within one switch. Create multiple Ring ID and assign different ring port 1 and port 2 to each ring, thus the switch can have multiple rings in one JetNet switch.

When implementing MultiRing, remember that the different rings can NOT use the same ring ID. The other settings are the same as above description. Technically, the maximum ring volume the MultiRing supported is up to 16 rings. Due to the port volume limitation, the mximum value is half of the port volume of a switch.

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

4.4.8 Ring Info

This page shows the MSR information.



Multiple Super Ring Information

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

ID: Ring ID.

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

Role: This Switch is RM or nonRM

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

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

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

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

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

4.4.9 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: Enable or disable ERPS function.

ERPS Configuration:

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

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

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

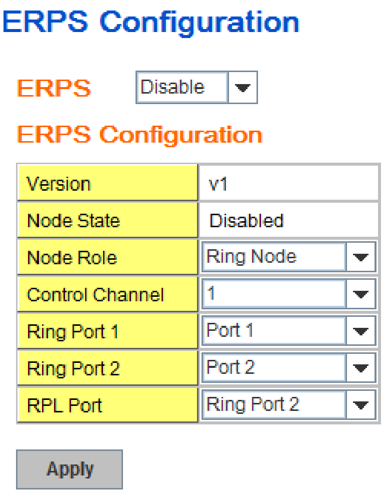
Control Channel: Control Channel provide a communication channel for ring automatic protection switching (R-APS) information.

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.

4.4.10 Command Lines:

Feature	Command Line
Global	
Enable	Switch(config)# spanning-tree enable
Disable	Switch (config)# spanning-tree disable
Mode (Choose the Spanning Tree mode)	Switch(config)# spanning-tree mode rst the rapid spanning-tree protocol (802.1w) stp the spanning-tree prtotcol (802.1d) mst the multiple spanning-tree protocol (802.1s)
Bridge Priority	Switch(config)# spanning-tree priority <0-61440> valid range is 0 to 61440 in multiple of 4096 Switch(config)# spanning-tree priority 4096
Bridge Times	Switch(config)# spanning-tree bridge-times (forward Delay) (max-age) (Hello Time) Switch(config)# spanning-tree bridge-times 15 20 2 This command allows you configure all the timing in one time.


ERPS Configuration

ERPS: Disable

ERPS Configuration

Version	v1
Node State	Disabled
Node Role	Ring Node
Control Channel	1
Ring Port 1	Port 1
Ring Port 2	Port 2
RPL Port	Ring Port 2

Forward Delay	Switch(config)# spanning-tree forward-time <4-30> Valid range is 4~30 seconds Switch(config)# spanning-tree forward-time 15
Max Age	Switch(config)# spanning-tree max-age <6-40> Valid range is 6~40 seconds Switch(config)# spanning-tree max-age 20
Hello Time	Switch(config)# spanning-tree hello-time <1-10> Valid range is 1~10 seconds Switch(config)# spanning-tree hello-time 2
MSTP	
Enter the MSTP Configuration Tree	Switch(config)# spanning-tree mst MSTMAP the mst instance number or range configuration enter mst configuration mode forward-time the forwa68oreneay 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)# na68orenixnix 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 68orenixnix] Revision 65535 Instance Vlans Mapped -------- ------------------------------------- 0 1,4-4094 1 2 2 -- 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 -- 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 69orenixnix] (->The nameis not applied after Abort settings.) Revision 65535 Instance Vlans Mapped -------- ------------------------------------- 0 1,4-4094 1 2 2 3 (-> The instance is not applied after Abort settings-- Config HMAC-MD5 Digest: 0xB41829F9030A054FB74EF7A8587FF58D ---
RSTP	
The mode should be rst, the timings can be configured in global settings listed in above.	
Global Information	
Active Information	Switch# show spanning-tree active Spanning-Tree : Enabled Protocol : MSTP Root Address : 0012.77ee.eeee Priority : 32768 Root Path Cost : 0 Root Port : N/A Root Times : max-age 20, hello-time 2, forward-delay 15 Bridge Address : 0012.77ee.eeee Priority : 32768 Bridge Times : max-age 20, hello-time 2, forward-delay 15 BPDU transmission-limit : 3 Port Role State Cost Prio.Nbr Type

	Aggregated ------ ---------- ---------- -------- ---------- ------------ ------------ fa1 Designated Forwarding 200000 128.1 P2P(RSTP) N/A fa2 Designated Forwarding 200000 128.2 P2P(RSTP) N/A
RSTP Summary	Switch# show spanning-tree summary Switch is in rapid-stp mode. BPDU skewing detection disabled for the bridge. Backbonefast disabled for bridge. Summary of connected spanning tree ports : #Port-State Summary Blocking Listening Learning Forwarding Disabled -------- --------- -------- ---------- -------- 0 0 0 2 8 #Port Link-Type Summary AutoDetected PointToPoint SharedLink EdgePort ------------ ------------ ---------- -------- 9 0 1 9
Port Info	Switch# show spanning-tree port detail fa7 (Interface_ID) Rapid Spanning-Tree feature Enabled Port 128.6 as Disabled Role is in Disabled State Port Path Cost 200000, Port Identifier 128.6 RSTP Port Admin Link-Type is Auto, Oper Link-Type is Point-to-Point RSTP Port Admin Edge-Port is Enabled, Oper Edge-Port is Edge Designated root has priority 32768, address 0012.7700.0112 Designated bridge has priority 32768, address 0012.7760.1aec Designated Port ID is 128.6, Root Path Cost is 600000 Timers : message-age 0 sec, forward-delay 0 sec Link Aggregation Group: N/A, Type: N/A, Aggregated with: N/A BPDU: sent 43759 , received 4854 TCN : sent 0 , received 0 Forwarding-State Transmit count 12 Message-Age Expired count
MSTP Information–	
MSTP Configuraiton–	Switch# show spanning-tree mst configuration Current MST configuration (MSTP is Running) Name 70orenixnix] Revision 65535 Instance Vlans Mapped -------- ------------------------------------- 0 1,4-4094 1 2 2 -- Config HMAC-MD5 Digest: 0xB41829F9030A054FB74EF7A8587FF58D ---
Display all MST Information	Switch# show spanning-tree mst ###### MST00 vlans mapped: 1,4-4094 Bridge address 0012.77ee.eeee priority 32768 (sysid 0) Root this switch for CST and IST Configured max-age 2, hello-time 15, forward-delay 20, max-hops 20 Port Role State Cost Prio.Nbr Type

	------ ---------- ---------- -------- ---------- ------------------ fa1 Designated Forwarding 200000 128.1 P2P Internal(MSTP) fa2 Designated Forwarding 200000 128.2 P2P Internal(MSTP) ###### MST01 vlans mapped: 2 Bridge address 0012.77ee.eeee priority 32768 (sysid 1) Root this switch for MST01 Port Role State Cost Prio.Nbr Type ------ ---------- ---------- -------- ---------- ------------------ fa1 Designated Forwarding 200000 128.1 P2P Internal(MSTP) fa2 Designated Forwarding 200000 128.2 P2P Internal(MSTP)
MSTP Root Information	Switch# show spanning-tree mst root MST Root Root Root Root Max Hello Fwd Instance Address Priority Cost Port age dly -------- -------------- -------- ----------- ------ ----- ----- ----- MST00 0012.77ee.eeee 32768 0 N/A 20 2 15 MST01 0012.77ee.eeee 32768 0 N/A 20 2 15 MST02 0012.77ee.eeee 32768 0 N/A 20 2 15
MSTP Instance Information	Switch# show spanning-tree mst 1 ###### MST01 vlans mapped: 2 Bridge address 0012.77ee.eeee priority 32768 (sysid 1) Root this switch for MST01 Port Role State Cost Prio.Nbr Type ------ ---------- ---------- -------- ---------- ------------------ fa1 Designated Forwarding 200000 128.1 P2P Internal(MSTP) fa2 Designated Forwarding 200000 128.2 P2P Internal(MSTP)
MSTP Port Information	Switch# show spanning-tree mst interface fa1 Interface fastethernet1 of MST00 is Designated Forwarding Edge Port : Edge (Edge) BPDU Filter : Disabled Link Type : Auto (Point-to-point) BPDU Guard : Disabled Boundary : Internal(MSTP) BPDUs : sent 6352, received 0 Instance Role State Cost Prio.Nbr Vlans mapped -------- ---------- ---------- -------- ---------- --------------------- 0 Designated Forwarding 200000 128.1 1,4- 4094 1 Designated Forwarding 200000 128.1 2 2 Designated Forwarding 200000 128.1 3
Multiple Super Ring	
Create or configure a Ring	Switch(config)# multiple-super-ring 1 Ring 1 created Switch(config-multiple-super-ring)# ***Note: 1 is the target Ring ID which is going to be created or***

	configured.
Delete a Ring	Switch(config-multiple-super-ring)# delete Ring 1 delete. Switch(config)# ***Note: It will exit from multiple-super-ring configuration mode after delete this ring.***
Enable a Ring	Switch(config-multiple-super-ring)# start Start Multiple Super Ring success
Disable a Ring	Switch(config-multiple-super-ring)# stop Stop Multiple Super Ring success.
Change Ring name	Switch(config-multiple-super-ring)# name MSR1 ***Note: Default Ring name is "Ring1", 1 is the Ring ID.***
Super Ring Version	Switch(config-multiple-super-ring)# version default set default to rapid super ring rapid-super-ring rapid super ring Switch(config-multiple-super-ring)# version rapid-super-ring
Priority	Switch(config-multiple-super-ring)# priority <0-255> valid range is 0 to 255 default set default Switch(config)# super-ring priority 100
Ring Port	Switch(config-multiple-super-ring)# port IFLIST Interface list, ex: fa1,fa3-5,gi8-10 cost path cost Switch(config-multiple-super-ring)# port fa1,fa2
Ring Port Cost	Switch(config-multiple-super-ring)# port cost <0-255> valid range is 0 or 255 default set default (128)valid range is 0 or 255 Switch(config-multiple-super-ring)# port cost 100 <0-255> valid range is 0 or 255 default set default (128)valid range is 0 or 255 Switch(config-super-ring-plus)# port cost 100 200 Set path cost success.
Rapid Dual Homing	Switch(config-multiple-super-ring)# rapid-dual-homing enable Switch(config-multiple-super-ring)# rapid-dual-homing disable Switch(config-multiple-super-ring)# rapid-dual-homing port IFLIST Interface name, ex: fastethernet1 or gi8 auto-detect up link auto detection IFNAME Interface name, ex: fastethernet1 or gi8 Switch(config-multiple-super-ring)# rapid-dual-homing port fa3,fa5-6 set Rapid Dual Homing port success. Switch(config-multiple-super-ring)#rapid-dual-homing extension <0-7> extension ID 0-7 (default is 0) default Note: auto-detect is recommended for dual Homing..
Super Chain	Switch(config-multiple-super-ring)# super-chain disable Switch(config-multiple-super-ring)# super-chain border Switch(config-multiple-super-ring)# super-chain member Switch(config-multiple-super-ring)# super-chain edge-port PLIST Port
Ring Info	
Ring Info	Switch# show multiple-super-ring [Ring ID] [Ring1] Ring1 Current Status : Disabled Role : Disabled

	Ring Status : Abnormal Ring Manager : 0000.0000.0000 Blocking Port : N/A Giga Copper : N/A Configuration : Version : Rapid Super Ring Priority : 128 Ring Port : fa1, fa2 Path Cost : 128, 128 Rapid Dual Homing : Disabled Extension ID : 0 Up Link : Auto Detect (N/A) Super Chain : Disabled Chain Role : N/A Chain Edge Port : N/A 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.
ERPS	
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 Cahnnel : VLAN 1 Ring Port 1 : fa1 is Link Down and Blocking 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#
Configure ERPS	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

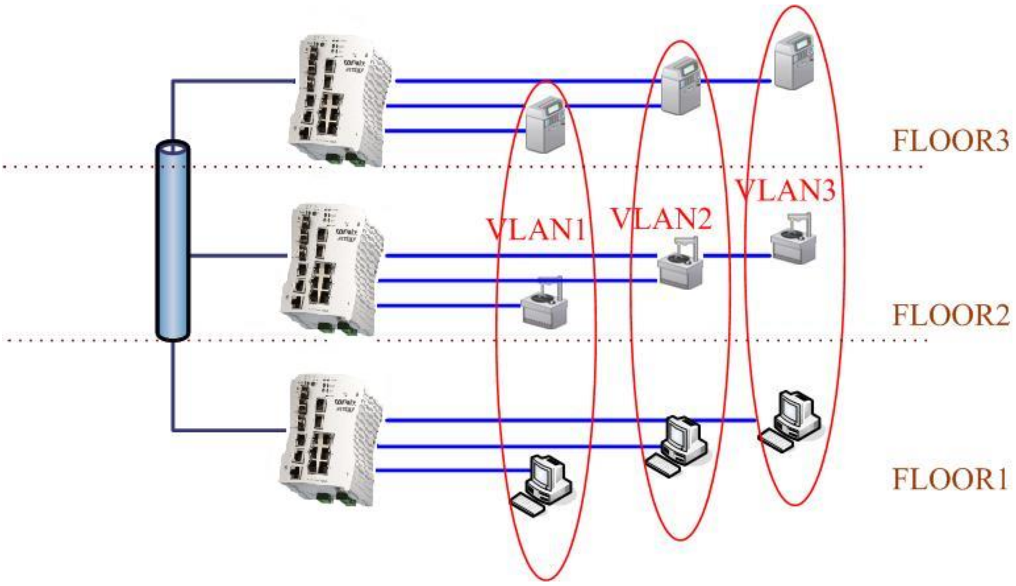
	Switch(config)# erps en enable Start the Multiple Super Ring for the switch Switch(config)# erps version 1 version 1 default Set default to version 1 Switch(config)# erps version 1 version 1 default Set default to version 1 Switch(config)# erps node-role rpl-owner ERPS RPL Owner ring-node ERPS ring node 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 <1-4095> 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

4.5 VLAN

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

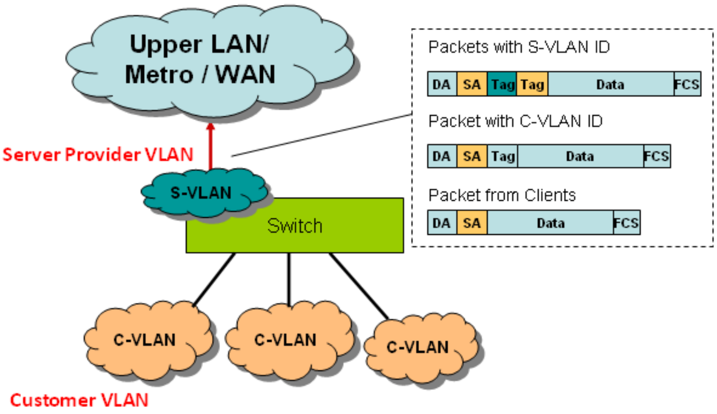
JetNet 5020G supports 802.1Q VLAN. 802.1Q VLAN is also known as Tag-Based VLAN. This Tag-Based VLAN allows VLAN to be created across different switches (see Figure 1). IEEE 802.1Q tag-based VLAN makes use of VLAN control information stored in a VLAN header attached to IEEE 802.3 packet frames. This tag contains a VLAN Identifier (VID) that indicates which VLAN a frame belongs to. Since each switch only has to check a frame's tag, without the need to dissect the contents of the frame, this also saves a lot of computing resources within the switch.

Figure 4.5.1 802.1Q VLAN



QinQ

The QinQ is originally designed to expand the number of VLANs by adding a tag to the 802.1Q packets. The original VLAN is usually identified as Customer VLAN (C-VLAN) and the new added t–g - as Service VLAN(S-VLAN). By adding the additional tag, QinQ increases the possible number of VLANs. After QinQ enabled, the Managed 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 port Ingress/Egress parameters and view VLAN table.

Following commands are included in this group:

4.5.1 VLAN Port Configuration

4.5.2 VLAN Configuration

4.5.3 GVRP Configuration

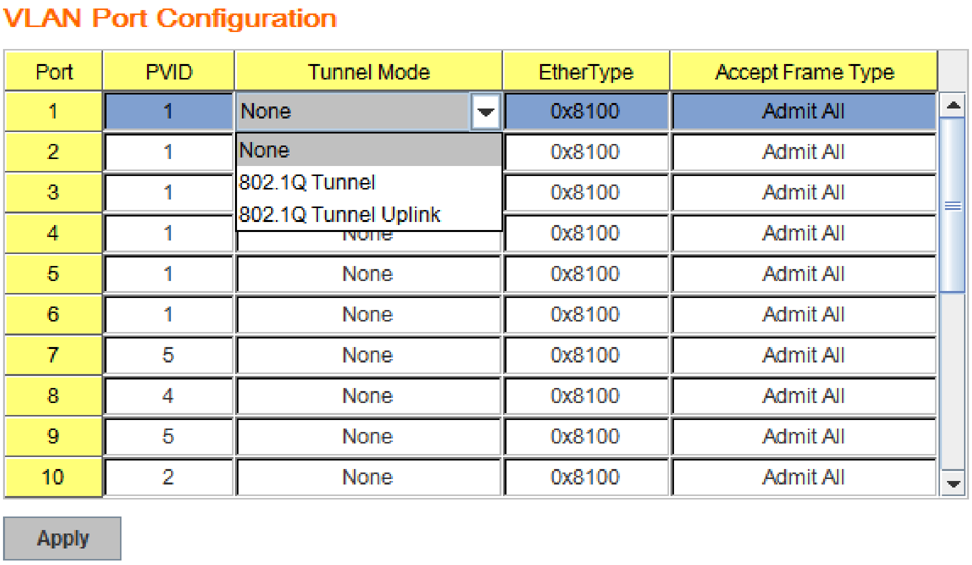
4.5.4 VLAN Table

4.5.5 CLI Commands of the VLAN

4.5.1 VLAN Port Configuration

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

Figure 4.5.2 Web UI of VLAN configuration.



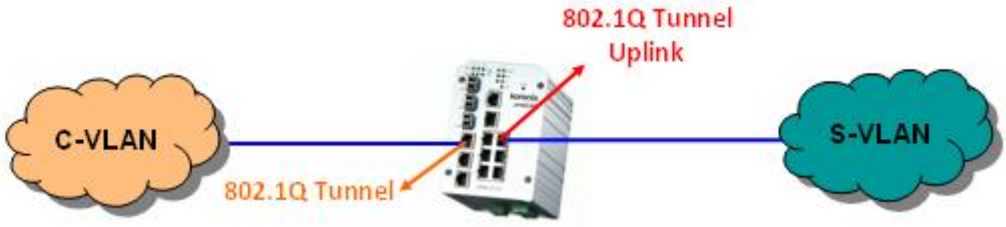
VLAN Port Configuration

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

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.

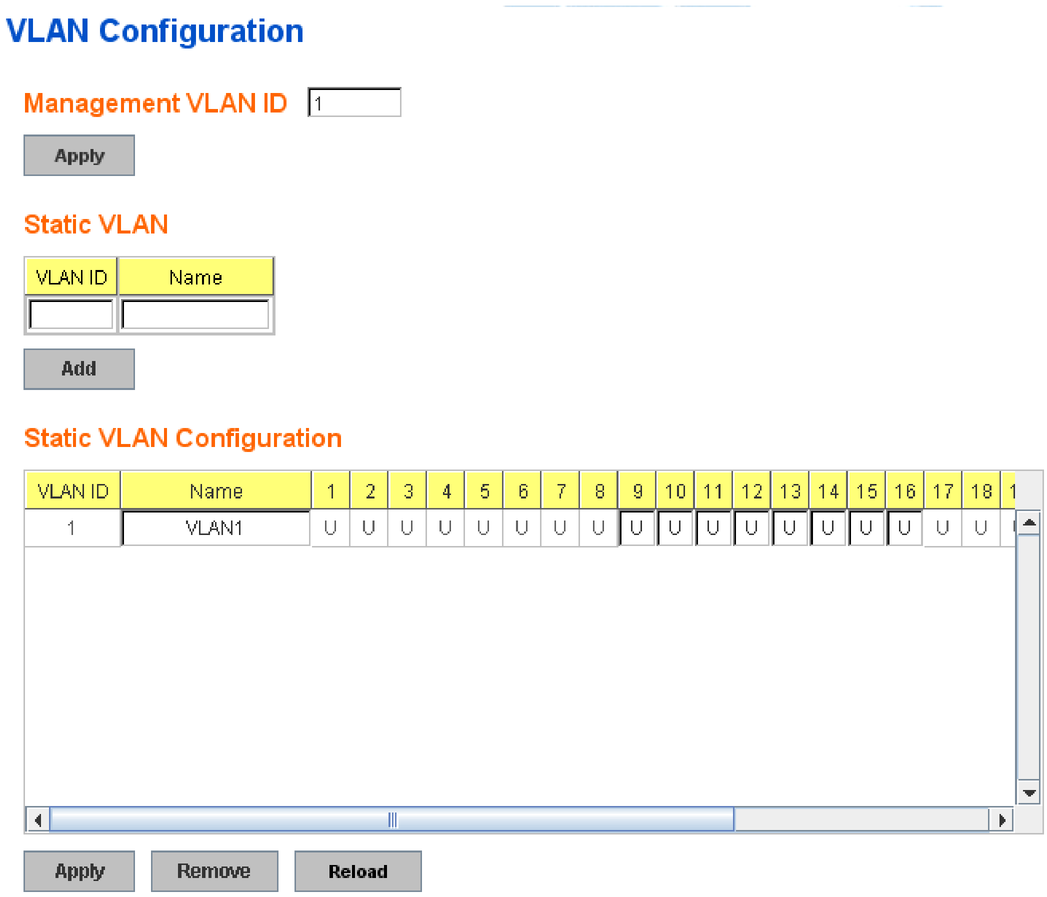
Accept Frame Type: This column defines the accepted frame type of the port. There are 2 modes you can select, **Admit All** and **Tag Only**. Admit All mode means that the port can accept both tagged and untagged packets. Tag Only mode means that the port can only accept tagged packets.

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.

4.5.2 VLAN Configuration

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

Figure 4.5.2.1 Web UI of the VLAN Configuration.



VLAN Configuration

Management VLAN ID: 1

Static VLAN

VLAN ID	Name

Static VLAN Configuration

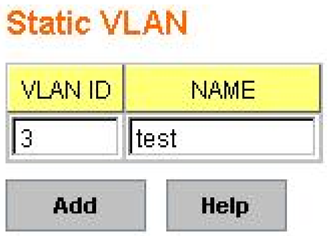
VLAN ID	Name	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	1
1	VLAN1	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	

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

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

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

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



Static VLAN

VLAN ID	NAME
3	test

Figure 4.5.2.2 The steps to create a new VLAN: Type VLAN ID and NAME, and press **Add** to create a new VLAN. Then you can see the new VLAN in the Static VLAN Configuration table. Refer to Figure 4.5.2.3

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

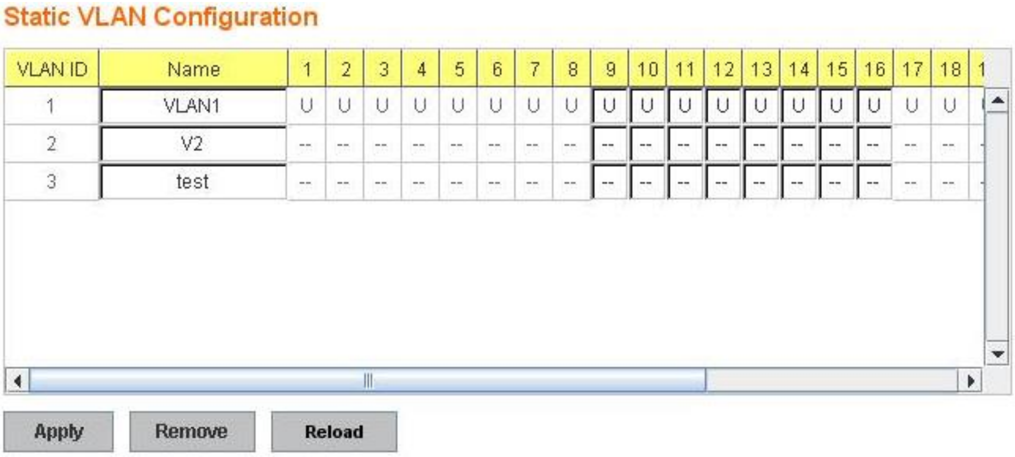
***Note:** Before you change the management VLAN ID by Web and Telnet, remember that the port attached by the administrator should be the member port of the management VLAN; otherwise the administrator can't access the switch via the network.*

***Note:** JetNet 5020G supports max 255 groups of VLAN.*

Static VLAN Configuration

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

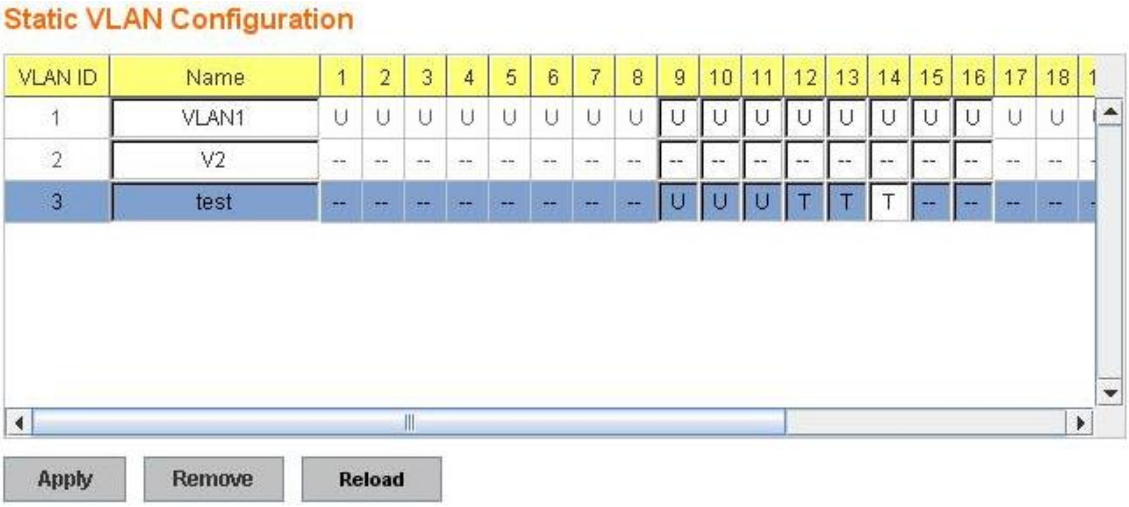
Figure 4.5.2.3 Static VLAN Configuration table. You can see that new VLAN 3 is created. VLAN name is test. Egress rules of the ports are not configured now.



Static VLAN Configuration

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

Figure 4.5.2.4 Configure Egress rule of the ports.



Static VLAN Configuration

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

-- : Not available

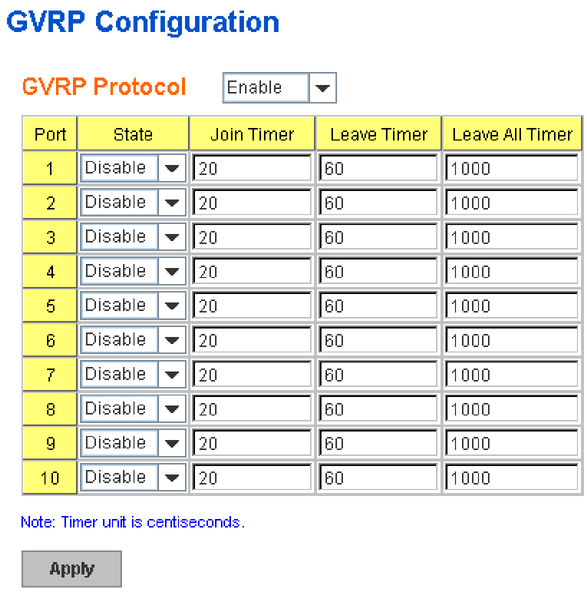
U: **Untag**: Indicates that egress/outgoing frames are not VLAN tagged.

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

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

4.5.3 GVRP configuration

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



GVRP Configuration

GVRP Protocol: Enable

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

Note: Timer unit is centiseconds.

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

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

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

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

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

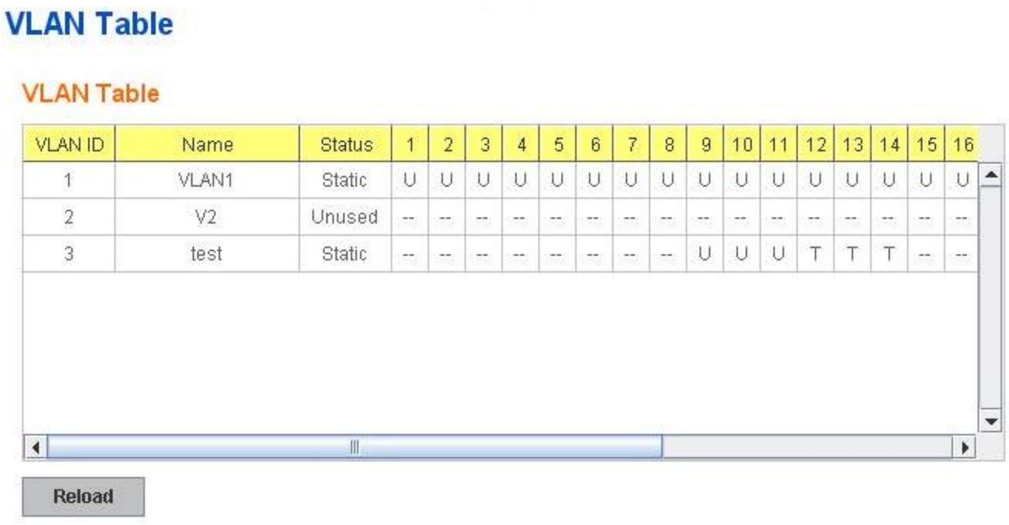
4.5.4 VLAN Table

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

VLAN ID: ID of the VLAN.
Name: Name of the VLAN.

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

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



VLAN Table

VLAN Table

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

4.5.5 CLI Commands of the VLAN

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

Feature	Command Line
VLAN Port Configuration	
Port Interface Configuration	Switch# con t Switch(config)# interface fa5 Switch(config-if)#
VLAN Port PVID	Switch(config-if)# switchport trunk native vlan 2 Set port default vlan id to 2 success
QinQ Tunnel Mode 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!
Egress rule – Untagged (for VLAN 2)	Switch(config-if)# switchport access vlan 2 switchport access vlan add 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 Description : N/A Administrative Status : Enable Operating Status : Not Connected

	Duplex : Auto Speed : Auto MTU : 2000 Flow Control :off Default Port VLAN ID: 2 Acceptable Frame Type : Vlan Tagged Only Auto Negotiation : Enable Loopback Mode : None STP Status: disabled Default CoS Value for untagged packets is 0. Mdix mode is Auto. Medium mode is Copper.
Display – Port Egress Rule (Egress rule, IP address, status)	Switch# show running-config …… ! interface fastethernet1 acceptable frame type vlantaggedonly switchport access vlan 1 switchport access vlan 3 switchport trunk native vlan 2 ……. interface vlan1 ip address 192.168.10.8/24 no shutdown
QinQ Information – 802.1Q Tunnel	Switch# show dot1q-tunnel Port Mode Ethertype ---- ------ --------- 1 normal 0x8100 2 normal 0x8100 3 normal 0x8100 4 normal 0x8100 5 access 0x8100 6 uplink 0x8100 7 normal 0x8100 8 normal 0x8100 9 normal 0x8100 10 normal 0x8100
QinQ Information – Show Running	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 !

VLAN Configuration	
Create VLAN (2)	Switch(config)# vlan 2 vlan 2 success Switch(config)# interface vlan 2 Switch(config-if)# *Note: In CLI configuration, you should create a VLAN interface first. Then you can start to add/remove ports. Default status of the created VLAN is unused until you add member ports to it.*
Remove VLAN	Switch(config)# no vlan 2 no vlan success *Note: You can only remove the VLAN when the VLAN is in unused mode.*
VLAN Name	Switch(config)# vlan 2 vlan 2 has exists Switch(config-vlan)# name v2 Switch(config-vlan)# no name *Note: Use no name to change the name to default name, VLAN VID.*
VLAN description	Switch(config)# interface vlan 2 Switch(config-if)# Switch(config-if)# description this is the VLAN 2 Switch(config-if)# no description ->Delete the description.
IP address of the VLAN	Switch(config)# interface vlan 2 Switch(config-if)# Switch(config-if)# ip address 192.168.10.18/24 Switch(config-if)# no ip address 192.168.10.8/24 ->Delete the IP address
Shut down VLAN	Switch(config)# interface vlan 2 Switch(config-if)# shutdown Switch(config-if)# no shutdown ->Turn on the VLAN
Display – VLAN table	Switch# sh vlan VLAN Name Status Trunk Ports Access Ports ---- ------------ ------- -------------------------- -------------------------- 1 VLAN1 Static - fa1-7,gi8-10 2 VLAN2 Unused - - 3 test Static fa4-7,gi8-10 fa1-3,fa7,gi8-10
Display – VLAN interface information	Switch# show interface vlan1 Interface vlan1 Description : N/A Administrative Status : Enable Operating Status : Up DHCP Client : Disable Primary IP Address : 192.168.10.1/24 IPv6 Address : fe80::212:77ff:feff:2222/64
GVRP configuration	
GVRP enable/disable	Switch(config)# gvrp mode disable Disable GVRP feature globally on the switch enable Enable GVRP feature globally on the switch

	Switch(config)# gvrp mode enable Gvrp is enabled on the switch!
Configure GVRP timer Join timer /Leave timer/ LeaveAll timer	Switch(config)# inter fa1 Switch(config-if)# garp join-timer <10-10000> the timer values Switch(config-if)# garp join-timer 20 Garp join timer value is set to 20 centiseconds on port 1!
Management VLAN	
Management VLAN	Switch(config)# int vlan 1 (Go to management VLAN) Switch(config-if)# no shutdown
Display	Switch# show running-config …. ! interface vlan1 ip address 192.168.10.17/24 ip igmp no shutdown ! ….

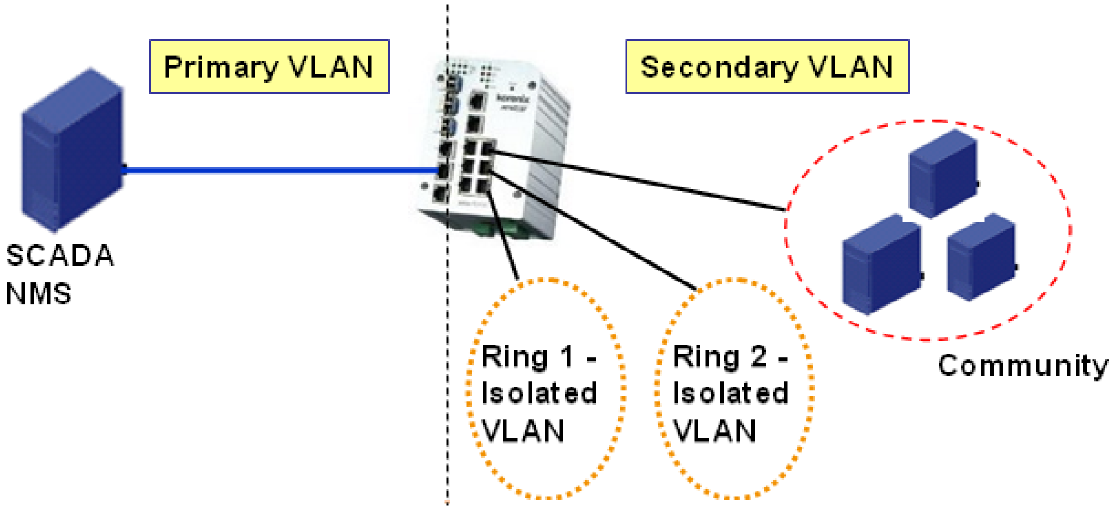
4.6 Private VLAN

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

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

Secondary VLAN: The client ports are usually defined within secondary VLAN. The secondary VLAN includes Isolated VLAN and Community VLAN. The client ports can be isolated VLANs or can be grouped in the same Community VLAN. The ports within the same community VLAN can communicate with each other. However, the isolated VLAN ports can Not.

The figure shows the typical Private VLAN network. The SCADA/Public Server or NMS workstation is usually located in primary VLAN. The clients PCs or Rings are located within Secondary.



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

Following commands are included in this group:

4.6.1 PVLAN Configuration

4.6.2 PVLAN Port Configuration

4.6.3 PVLAN Informtion

4.6.4 CLI Commands of the PVLAN

4.6.1 PVLAN Configuration

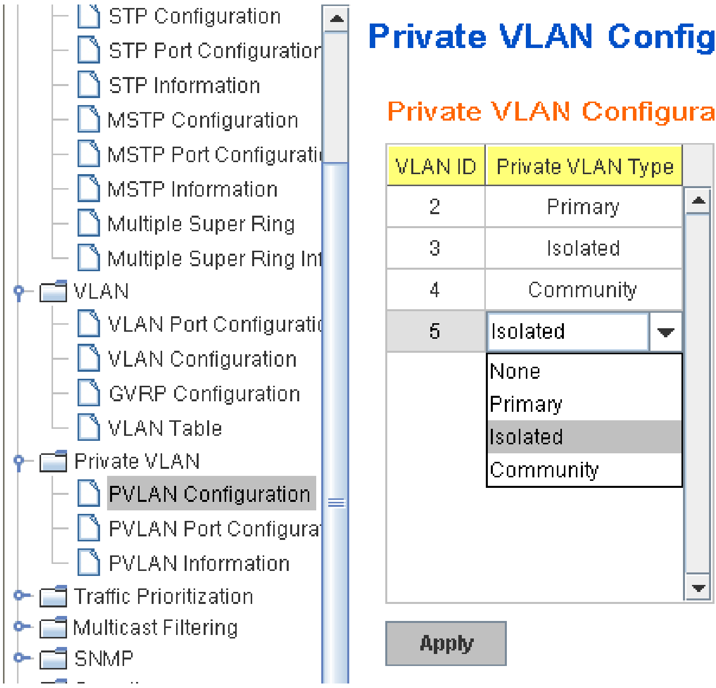
PVLAN Configuration allows you to assign Private VLAN type. After created VLAN in VLAN Configuraiton page, the available VLAN ID will display here. Choose the Private VLAN types for each VLAN you want configure.

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.



Private VLAN Configuration

VLAN ID	Private VLAN Type
2	Primary
3	Isolated
4	Community
5	Isolated

4.6.2 PVLAN Port Configuration

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

Private VLAN Association

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

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

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

Port Configuraion

PVLAN Port Type :

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

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

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

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

For example:

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

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

VLAN 2 is belonged to Primary VLAN.

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

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

4. Private VLAN Port Configuration

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

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

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

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

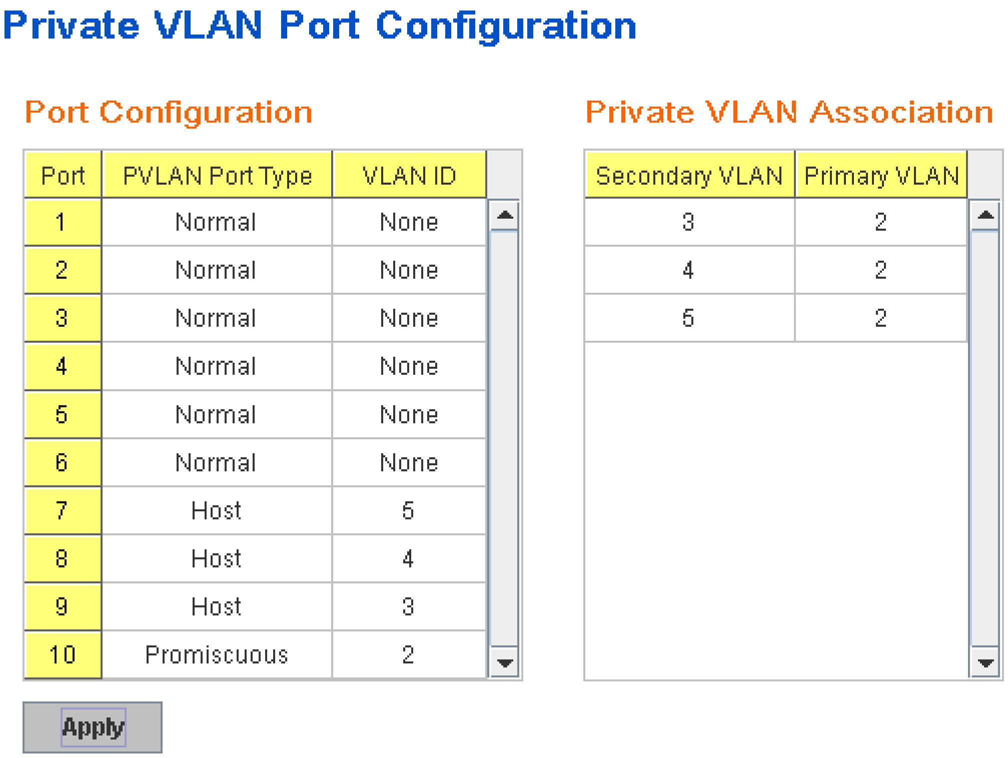
5. Result

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

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

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

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



Private VLAN Port Configuration

Port Configuration

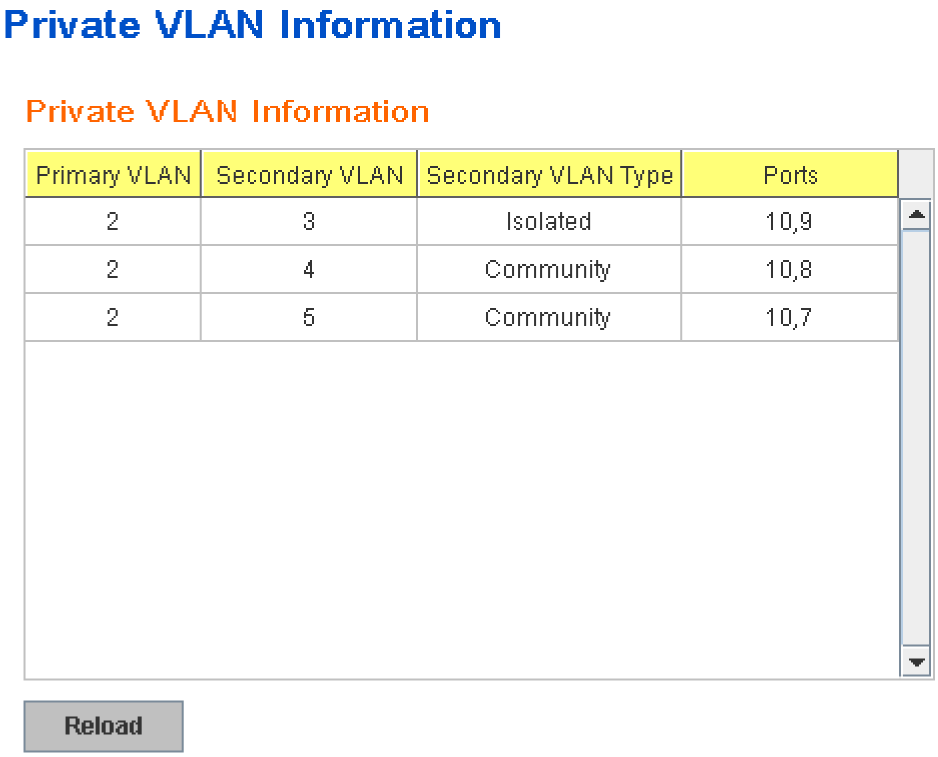
Port	PVLAN Port Type	VLAN ID
1	Normal	None
2	Normal	None
3	Normal	None
4	Normal	None
5	Normal	None
6	Normal	None
7	Host	5
8	Host	4
9	Host	3
10	Promiscuous	2

Private VLAN Association

Secondary VLAN	Primary VLAN
3	2
4	2
5	2

4.6.3 Private VLAN Information

This page allows you to see the Private VLAN information.



Private VLAN Information

Private VLAN Information

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

4.6.4 CLI Command of the PVLAN

Command Lines of the Private VLAN configuration

Feature	Command Line
Private VLAN Configuration	
Create VLAN	Switch(config)# vlan 2 vlan 2 success Switch(config-vlan)# end End current mode and change to enable mode exit Exit current mode and down to previous mode list Print command list name Assign a name to vlan no no private-vlan Configure a private VLAN
Private VLAN Type Choose the Types Primary Type	**Go to the VLAN you want configure first.** Switch(config)# vlan (VID) Switch(config-vlan)# private-vlan community Configure the VLAN as an community private VLAN isolated Configure the VLAN as an isolated private VLAN primary Configure the VLAN as a primary private VLAN

Isolated Type Community Type	Switch(config-vlan)# private-vlan primary Switch(config-vlan)# no private-vlan primary Switch(config-vlan)# private-vlan isolated Switch(config-vlan)# no private-vlan isolated Switch(config-vlan)# private-vlan community Switch(config-vlan)# no private-vlan community
Private VLAN Port Configuraiton	
Go to the port configuraiton	Switch(config)# interface (port_number, ex: gi9) Switch(config-if)# switchport private-vlan host-association Set the private VLAN host association mapping map primary VLAN to secondary VLAN
Private VLAN Port Type Promiscuous Port Type Host Port Type	Switch(config-if)# switchport mode svl Shared vlan learning private-vlan Set private-vlan mode Switch(config-if)# switchport mode private-vlan host Set the mode to private-vlan host promiscuous Set the mode to private-vlan promiscuous Switch(config-if)# switchport mode private-vlan promiscuous Switch(config-if)#no switchport mode private-vlan promiscuous Switch(config-if)# switchport mode private-vlan host
Private VLAN Port Configuration PVLAN Port Type Host Association primary to secondary (The command is only available for host port.)	Switch(config)# interface gi9 Switch(config-if)# switchport mode private-vlan host Switch(config-if)# switchport private-vlan host-association <2-4094> Primary range VLAN ID of the private VLAN port association Switch(config-if)# switchport private-vlan host-association 2 <2-4094> Secondary range VLAN ID of the private VLAN port association Switch(config-if)# switchport private-vlan host-association 2 3
Mapping primary to secondary VLANs (This command is only available for promiscuous port)	Switch(config)# interface gi10 Switch(config-if)# switchport mode private-vlan promiscuous Switch(config-if)# switchport private-vlan mapping 2 add 3 Switch(config-if)# switchport private-vlan mapping 2 add 4 Switch(config-if)# switchport private-vlan mapping 2 add 5
Private VLAN Information	
Private VLAN Information	Switch# show vlan private-vlan FLAGS: I -> Isolated P -> Promiscuous C -> Community Primary Secondary Type Ports ------- --------- ---------------- -------------------- 2 3 Isolated gi10(P),gi9(I) 2 4 Community gi10(P),gi8(C) 2 5 Community gi10(P),fa7(C),gi9(I) 10 - - -
PVLAN Type	Switch# show vlan private-vlan type Vlan Type Ports ---- ----------------- ----------------- 2 primary gi10

	3 isolated gi9 4 community gi8 5 community fa7,gi9 10 primary -
Host List	Switch# show vlan private-vlan port-list Ports Mode Vlan ----- ----------- ---- 1 normal - 2 normal - 3 normal - 4 normal - 5 normal - 6 normal - 7 host 5 8 host 4 9 host 3 10 promiscuous 2
Running Config Information Private VLAN Type Private VLAN Port Information	Switch# show run Building configuration... Current configuration: hostname Switch vlan learning independent ! vlan 1 ! vlan 2 private-vlan primary ! vlan 3 private-vlan isolated ! vlan 4 private-vlan community ! vlan 5 private-vlan community ! ……….. ……….. interface fastethernet7 switchport access vlan add 2,5 switchport trunk native vlan 5 switchport mode private-vlan host switchport private-vlan host-association 2 5 ! interface gigabitethernet8 switchport access vlan add 2,4 switchport trunk native vlan 4 switchport mode private-vlan host switchport private-vlan host-association 2 4 ! interface gigabitethernet9 switchport access vlan add 2,5 switchport trunk native vlan 5 switchport mode private-vlan host switchport private-vlan host-association 2 3

	! interface gigabitethernet10 switchport access vlan add 2,5 switchport trunk native vlan 2 switchport mode private-vlan promiscuous switchport private-vlan mapping 2 add 3-5 ……… ……..

4.7 Traffic Prioritization

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

The Managed Switch's QOS supports 8 physical queues, weighted fair queuing (WRR) and Strict Priority scheme, which follows 802.1p COS tag and IPv4 TOS/DiffServ information to prioritize the traffic of your industrial network.

Following commands are included in this group:

4.7.1 QoS Setting

4.7.2 QoS Priority Mode

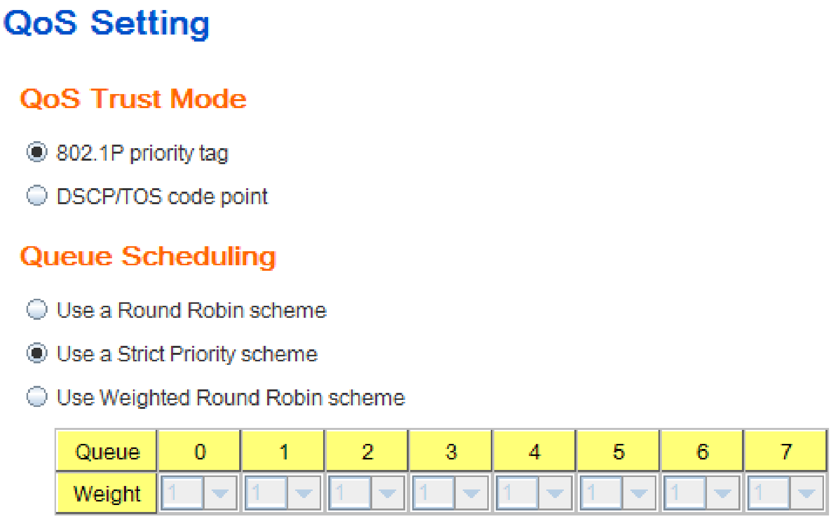
4.7.3 CoS-Queue Mapping

4.7.4 DSCP-Queue Mapping

4.7.5 CLI Commands of the Traffic Prioritization

4.7.1 QoS Setting

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



QoS Setting

QoS Trust Mode

● 802.1P priority tag

○ DSCP/TOS code point

Queue Scheduling

○ Use a Round Robin scheme

● Use a Strict Priority scheme

○ Use Weighted Round Robin scheme

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

Queue Scheduling

You can select the Queue Scheduling rule as follows:

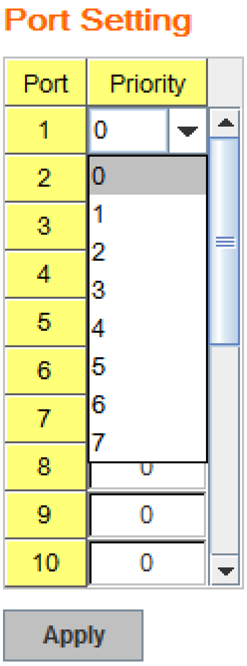
Use a strict priority scheme. Packets with higher priority in the queue will always be processed first, except that there is no packet with higher priority.

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

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

4.7.2 Port-based Queue Mapping

Choose the Queue value of each port, the port then has its default priority. The Queue 7 is the highest port-based queue, 0 is the lowest queue. The traffic injected to the port follows the queue level to be forwarded, but the outgoing traffic doesn't bring the queue level to next switch.



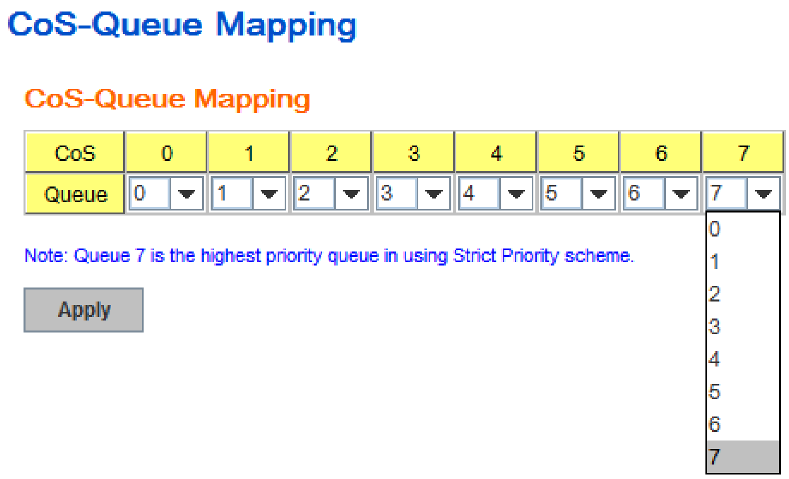
Port Setting

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

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

4.7.3 CoS-Queue Mapping

This page is to change CoS values to Physical Queue mapping table. JetNet 5020G switch fabric can support 8 physical queues, to allow Users CoS value to the different levels of the physical queue. In JetNet 5020G, users can freely assign the mapping table or follow the suggestion of the 802.1p standard.



CoS-Queue Mapping

CoS-Queue Mapping

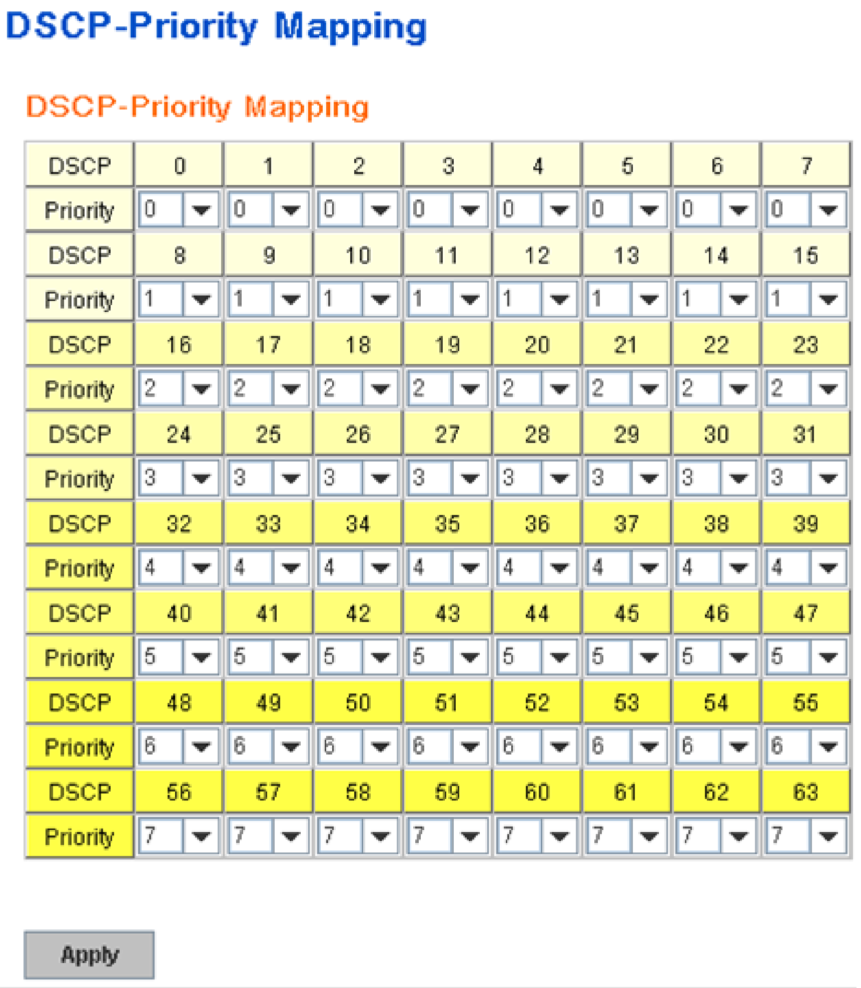
CoS	0	1	2	3	4	5	6	7
Queue	0	1	2	3	4	5	6	7

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

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

4.7.4 DSCP-Priority Mapping

This page allows you to modify DSCP values to Priority mapping table. The system provides 0~63 DSCP priority levels. Each DSCP level can be assigned into 8 different physical queue, from lowest 0 to highest 7.



DSCP-Priority Mapping

DSCP-Priority Mapping

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

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

4.7.5 CLI Commands of the Traffic Prioritization

Command Lines of the Traffic Prioritization configuration

Feature	Command Line
QoS Setting	
Queue Scheduling – Strict Priority	Switch(config)# qos queue-sched sp Strict Priority wrr Weighted Round Robin Switch(config)# qos queue-sched sp The queue scheduling scheme is setting to Strict Priority.
Queue Scheduli–g - WRR	Switch(config)# qos queue-sched wrr <1-10> Weights for COS queue 0 (queue_id 0) Switch(config)# qos queue-sched wrr 10 <1-10> Weights for COS queue 1 (queue_id 1) ……….. Switch(config)# qos queue-sched wrr 1 2 3 4 5 6 7 8 The queue scheduling scheme is setting to Weighted Round Robin. ***Assign the ratio for the 8 classes of service.***
Port Setting – CoS (Default Port Priority)	Switch(config)# interface **fa1** Switch(config-if)# qos priority <0-7> Assign a priority queue Switch(config-if)# qos priority 3 The priority queue is set 3 ok. ***Note: When change the port setting, you should Select the specific port first. Ex: fa1 means fast Ethernet port 1.***
QoS Trust Mode	Switch(config)# qos trust-mode cos CoS dscp DSCP/TOS Switch(config)# qos trust-mode dscp Set QoS trust mode dscp ok Switch# show trust-mode QoS Trust Mode: DSCP/TOS code point
Display - Queue Scheduling	Switch# show qos queue-sched QoS queue scheduling scheme : Weighted Round Robin COS queue 0 = 1 COS queue 1 = 2 COS queue 2 = 3 COS queue 3 = 4 COS queue 4 = 5 COS queue 5 = 6 COS queue 6 = 7 COS queue 7 = 8
Display – Port Priority Setting (Port Default Priority)	Switch# show qos port-priority Port Default Priority : Port Priority Queue -----+---- 1 7 2 0 ……….. 19 0 20 0
CoS-Queue Mapping	
Format	Switch(config)# qos cos-map PRIORITY Assign an priority (7 highest)

<table>
<tr><td></td><td>Switch(config)# qos cos-map 1
  QUEUE   Assign an queue (0-7)

<b><i>Note: Format: qos cos-map priority_value queue_value</i></b></td></tr>
<tr><td>Map CoS 0 to Queue 1</td><td>Switch(config)# qos cos-map 0 1
The CoS to queue mapping is set ok.</td></tr>
<tr><td>Map CoS 1 to Queue 0</td><td>Switch(config)# qos cos-map 1 0
The CoS to queue mapping is set ok.</td></tr>
<tr><td>Map CoS 2 to Queue 0</td><td>Switch(config)# qos cos-map 2 0
The CoS to queue mapping is set ok.</td></tr>
<tr><td>Map CoS 3 to Queue 1</td><td>Switch(config)# qos cos-map 3 1
The CoS to queue mapping is set ok.</td></tr>
<tr><td>Map CoS 4 to Queue 2</td><td>Switch(config)# qos cos-map 4 2
The CoS to queue mapping is set ok.</td></tr>
<tr><td>Map CoS 5 to Queue 2</td><td>Switch(config)# qos cos-map 5 2
The CoS to queue mapping is set ok.</td></tr>
<tr><td>Map CoS 6 to Queue 3</td><td>Switch(config)# qos cos-map 6 3
The CoS to queue mapping is set ok.</td></tr>
<tr><td>Map CoS 7 to Queue 3</td><td>Switch(config)# qos cos-map 7 3
The CoS to queue mapping is set ok.</td></tr>
<tr><td>Display – CoS-Queue mapping</td><td>Switch# sh qos cos-map
CoS to Queue Mapping :
CoS   Queue
  ---- +   ------
   0   1
   1   0
   2   0
   3   1
   4   2
   5   2
   6   3
   7   3</td></tr>
<tr><td colspan="2"><b>DSCP-Priority Mapping</b></td></tr>
<tr><td>Format</td><td>Switch(config)# qos dscp-map
  DSCP   DSCP code point in binary format (000000-111111)
Switch(config)# qos dscp-map 0
  PRIORITY   802.1p priority bit (0-7)

<b><i>Format: qos dscp-map priority_value queue_value</i></b></td></tr>
<tr><td>Map DSCP 0 to Queue 1</td><td>Switch(config)# qos dscp-map 0 1
The TOS/DSCP to queue mapping is set ok.</td></tr>
<tr><td>Display – DSCO-Queue mapping</td><td>Switch# show qos dscp-map
DSCP to Queue Mapping : (dscp = d1 d2)

     d2| 0 1 2 3 4 5 6 7 8 9
d1 |
-----+---------------------
     0 | 1 0 0 0 0 0 0 0 1 1
     1 | 1 1 1 1 1 1 2 2 2 2
     2 | 2 2 2 2 3 3 3 3 3 3
     3 | 3 3 4 4 4 4 4 4 4 4
     4 | 5 5 5 5 5 5 5 5 6 6
     5 | 6 6 6 6 6 6 7 7 7 7
     6 | 7 7 7 7</td></tr>
</table>

4.8 Multicast Filtering

For multicast filtering, JetNet 5020G uses IGMP Snooping technology. IGMP (Internet Group Management Protocol) is an Internet Protocol that provides a way for internet device to report its multicast group membership to adjacent routers. Multicasting allows one computer on the internet to send data to a multitude of other computers that have identified themselves as being interested in receiving the originating computers data.

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

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

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

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

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

Following commands are included in this group:

4.8.1 IGMP Snooping

4.8.2 IGMP Query

4.8.3 Unknown Multicast

4.8.4 GMRP Configuration

4.8.5 CLI Commands of the Multicast Filtering

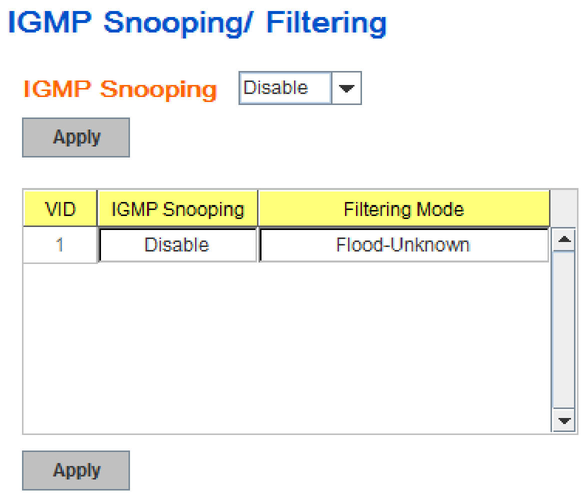
4.8.1 IGMP Snooping

This page is to enable IGMP Snooping feature, assign IGMP Snooping for specific VLAN, and view IGMP Snooping table from dynamic learnt or static manual key-in. JetNet 5020G supports IGMP snooping V1/V2/V3 and IGMP query V1/V2.

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

To assign IGMP Snooping to VLAN, please select VLAN ID to enable/disable IGMP

Snooping function, or select the “IGMP Snooping” global setting for all VLANs.. Then press **Apply**. In the same way, you can also **Disable** IGMP Snooping for certain VLANs.



IGMP Snooping/ Filtering

IGMP Snooping: Disable

VID	IGMP Snooping	Filtering Mode
1	Disable	Flood-Unknown

Filtering Mode Setting: you can select Filtering Mode on this Page.

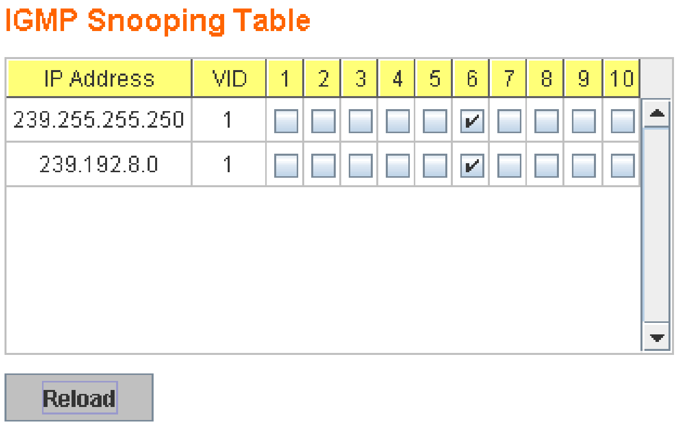
Send to Query Ports: The unknown multicast will be sent to the Query ports. The Query port means the port received the IGMP Query packets. It is usually the uplink port of the switch.

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

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

This page allows you to decide how to forward the unknown multicast traffic.

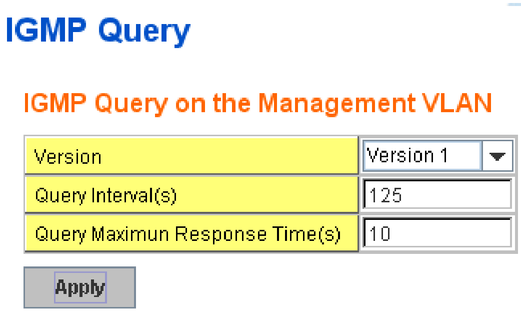
IGMP Snooping Table: In the table, you can see multicast group IP address, VLAN ID it belongs to, and member ports of the multicast group. JetNet 5020G supports 256 multicast groups. Click on **Reload** to refresh the table.



IGMP Snooping Table

IP Address	VID	1	2	3	4	5	6	7	8	9	10
239.255.255.250	1	□	□	□	□	□	☑	□	□	□	□
239.192.8.0	1	□	□	□	□	□	☑	□	□	□	□

4.8.2 IGMP Query



IGMP Query

IGMP Query on the Management VLAN

Version	Version 1
Query Interval(s)	125
Query Maximun Response Time(s)	10

This page allows users to configure **IGMP Query** feature. Since the Managed Switch can only be configured as the member port of the management VLAN, IGMP Query can only be enabled on the management VLAN. If you want to run IGMP Snooping feature in several VLANs, you should notice that whether each VLAN has its own IGMP Querier first.

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

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

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

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

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

4.8.3 Unknown Multicast

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

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

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

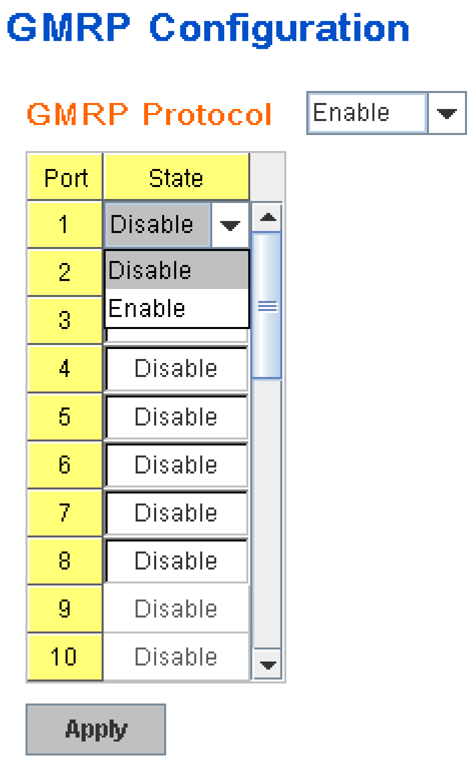
Discard: The unknown multicast will be discarded. Non-member ports will not receive the unknown multicast streams.

This page allows you to decide how to forward the unknown multicast traffic.

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

4.8.4 GMRP

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



GMRP Configuration

GMRP Protocol: Enable

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

4.8.5 CLI Commands of the Multicast Filtering

Command Lines of the multicast filtering configuration

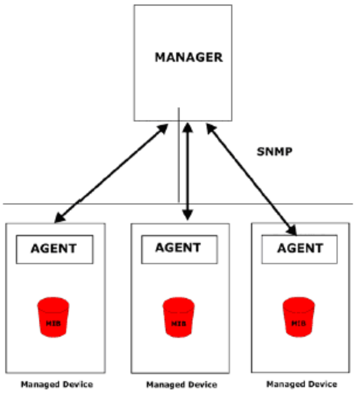
Feature	Command Line
IGMP Snooping	
IGMP Snoopi–g - Global	Switch(config)# ip igmp snooping IGMP snooping is enabled globally. Please specify on which vlans IGMP snooping enables Switch(config)# ip igmp snooping <?> immediate-leave leave group when receive a leave message last-member-query-interval the interval for which the switch waits before updating the table entry source-only-learning Source-Only-Learning vlan Virtual LAN
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 IGMP snooping is enabled on vlan 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	Switch# sh ip igmp interface vlan1 enabled: Yes version: IGMPv1

	query-interval; 125s query-max-response-time: 10s Switch# sh ip igmp snooping IGMP snooping is globally enabled Vlan1 is IGMP snooping enabled immediate-leave is disabled last-member-query-interval is 100 centiseconds Vlan2 is IGMP snooping enabled immediate-leave is disabled last-member-query-interval is 100 centiseconds Vlan3 is IGMP snooping disabled immediate-leave is disabled last-member-query-interval is 100 centiseconds
Display – IGMP Table	Switch# sh ip igmp snooping multicast all VLAN IP Address Type Ports ---- --------------- ------- ------------------------ 1 239.192.8.0 IGMP fa6, 1 239.255.255.250 IGMP fa6,
IGMP Query	
IGMP Query V1	Switch(config)# int vlan 1 (Go to management VLAN) Switch(config-if)# ip igmp v1
IGMP Query V2	Switch(config)# int vlan 1 (Go to management VLAN) Switch(config-if)# ip igmp
IGMP Query version	Switch(config-if)# ip igmp version 1 Switch(config-if)# ip igmp version 2
Disable	Switch(config)# int vlan 1 Switch(config-if)# no ip igmp
Display	Switch# sh ip igmp interface vlan1 enabled: Yes version: IGMPv2 query-interval: 125s query-max-response-time: 10s Switch# show running-config …. ! interface vlan1 ip address 192.168.10.17/24 ip igmp no shutdown ! …….
Unknown Multicast	
Send to Query Ports –	Switch(config)# ip igmp snooping source-only-learning vlan VLANLIST allowed VLAN list all all VLAN Switch(config)# ip igmp snooping source-only-learning vlan 1 IGMP Snooping Source-Only-Learning is enabled on VLAN 1
Discard (Force filtering)	Switch(config)# mac-address-table multicast filtering vlan VLANLIST allowed VLAN list

	all all VLAN Switch(config)# mac-address-table multicast filtering vlan 2
Send to All Ports (No Discard, No Send to Query Ports)	Switch(config)# no mac-address-table multicast filtering vlan VLANLIST allowed VLAN list all all VLAN Switch(config)# no mac-address-table multicast filtering vlan 1

4.9 SNMP

Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. The Managed Switch series support SNMP v1 and v2c and V3. (Web Managed Switch doesn't support SNMP feature.)



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

Following commands are included in this group:

4.9.1 SNMP Configuration

4.9.2 SNMPv3 Profile

4.9.3 SNMP Traps

4.9.4 SNMP CLI Commands for SNMP

4.9.1 SNMP Configuration

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

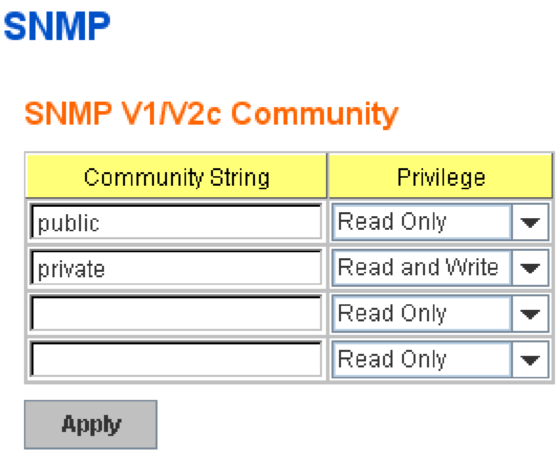
The community includes 2 privileges, Read Only and Read and Write.

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

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

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

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



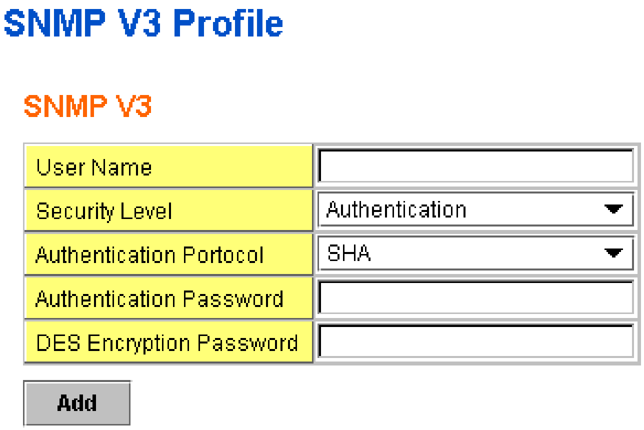
SNMP

SNMP V1/V2c Community

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

4.9.2 SNMP V3 Profile

SNMP v3 can provide more security functions when the user performs remote management through SNMP protocol. It delivers SNMP information to the administrator with user authentication; all of data between JetNet 5020G and the administrator are encrypted to ensure secure communication.



SNMP V3 Profile

SNMP V3

User Name	
Security Level	Authentication
Authentication Portocol	SHA
Authentication Password	
DES Encryption Password	

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

Authentication Protocol: Here the user can select either MD5 (Message-Digest algorithm 5) or SHA (Secure Hash Algorithm). MD5 is a widely used cryptographic hash function with a 128-bit hash value. SHA (Secure Hash Algorithm) hash functions refer to five Federal Information Processing Standard-approved algorithms for computing a condensed digital representation. JetNet 5020G provides 2 user authentication protocols in MD5 and SHA. You will need to configure SNMP v3 parameters for your SNMP tool with the same authentication method.

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

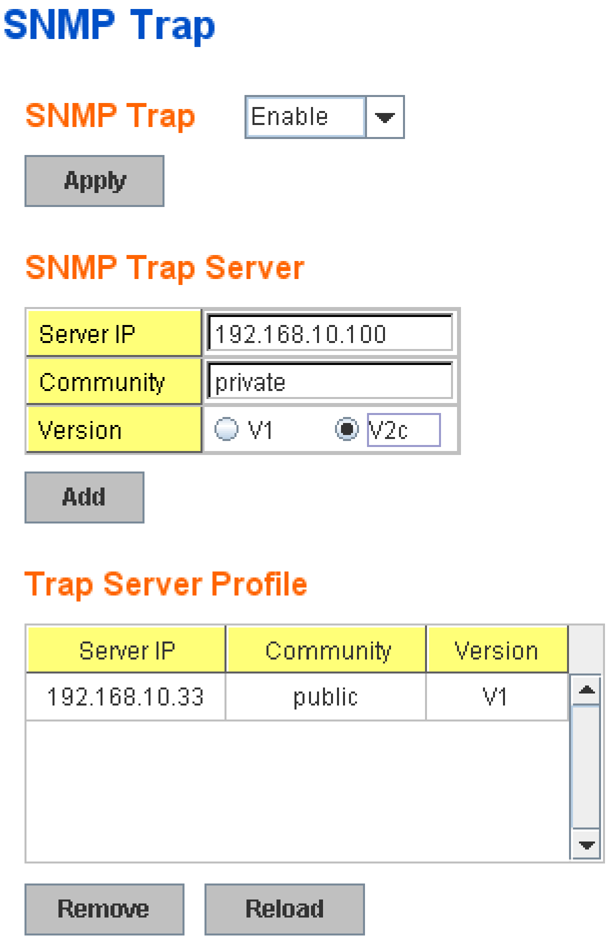
DES Encryption Password: Here the user enters the password for SNMP v3 user DES

Encryption.

4.9.3 SNMP Traps

SNMP Trap is the notification feature defined by SNMP protocol. All the SNMP management applications can understand such trap information. So you don't need to install new application to read the notification information.

This page allows users to **Enable SNMP Trap,** configure the **SNMP Trap server IP**, **Community** name, and trap version **V1 or V2c**. After 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: Enable

SNMP Trap Server

Server IP	192.168.10.100
Community	private
Version	○ V1 ● V2c

Trap Server Profile

Server IP	Community	Version
192.168.10.33	public	V1

4.9.4 CLI Commands of the SNMP

Command Lines of the SNMP configuration

Feature	Command Line
SNMP Community	
Read Only Community	Switch(config)# snmp-server community public ro community string add ok
Read Write Community	Switch(config)# snmp-server community private rw community string add ok
SNMP Trap	

Enable Trap	Switch(config)# snmp-server enable trap Set SNMP trap enable ok.
SNMP Trap Server IP without specific community name	Switch(config)# snmp-server host 192.168.10.33 SNMP trap host add OK.
SNMP Trap Server IP with version 1 and community	Switch(config)# snmp-server host 192.168.10.33 version 1 private SNMP trap host add OK. ***Note: private is the community name, version 1 is the SNMP version***
SNMP Trap Server IP with version 2 and community	Switch(config)# snmp-server host 192.168.10.33 version 2 private SNMP trap host add OK.
Disable SNMP Trap	Switch(config)# no snmp-server enable trap Set SNMP trap disable ok.
Display	Switch# sh snmp-server trap SNMP trap: Enabled SNMP trap community: public Switch# show running-config .... snmp-server community public ro snmp-server community private rw snmp-server enable trap snmp-server host 192.168.10.33 version 2 admin snmp-server host 192.168.10.33 version 1 admin ……..

4.10 Security

JetNet 5020G provides several security features for you to secure your connection. The Filter Set is also known as Access Control List. The ACL feature includes traditional Port Security and IP Security.

Following commands are included in this group:

4.10.1 Filter Set (Access Control List)

4.10.2 IEEE 802.1x

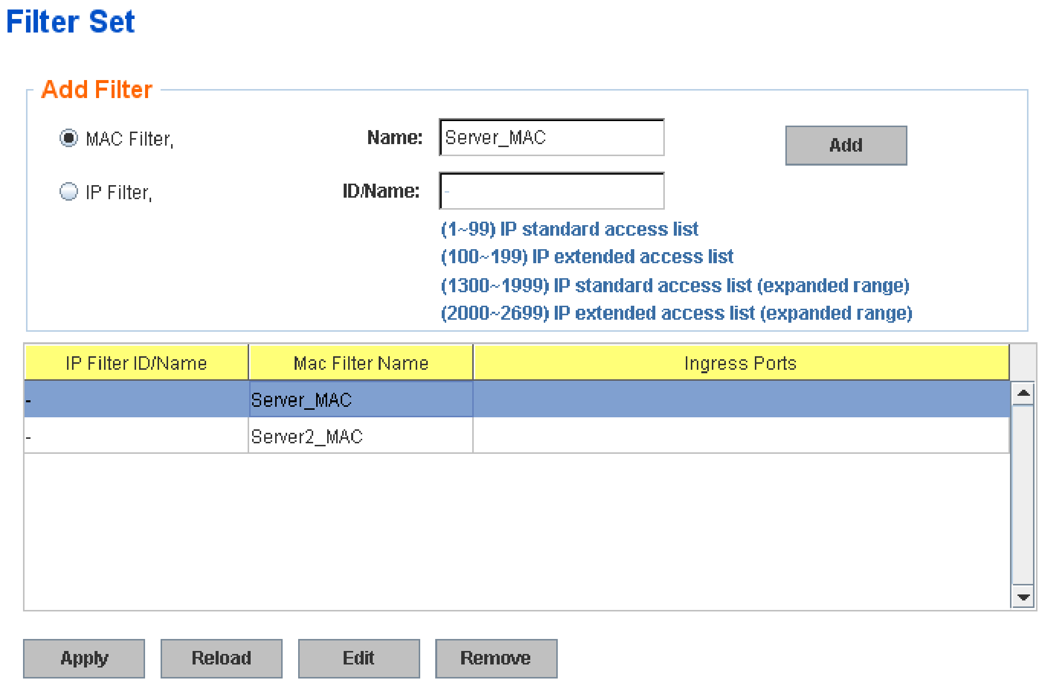
4.10.3 CLI Commands of the Security

4.10.1 Filter Set (Access Control List)

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

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

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



Filter Set

Add Filter

● MAC Filter, Name: Server_MAC

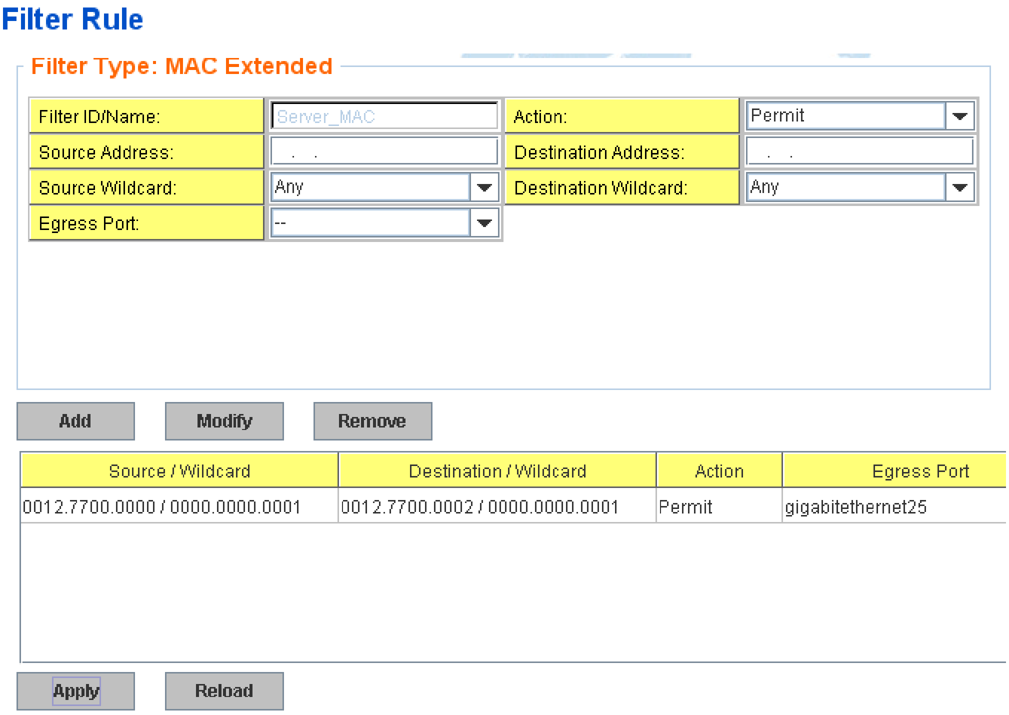
○ IP Filter, ID/Name: -

(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:	Server_MAC	Action:	Permit
Source Address:	. .	Destination Address:	. .
Source Wildcard:	Any	Destination Wildcard:	Any
Egress Port:	--		

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

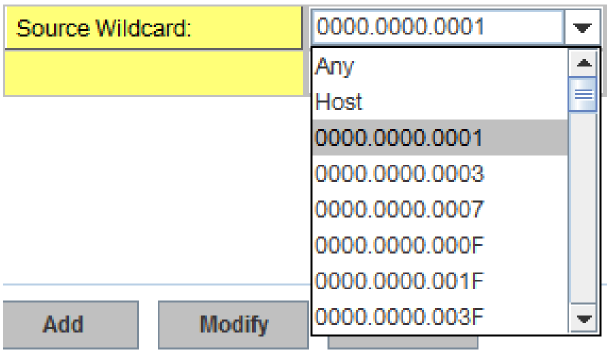
Filter ID/Name: The name for this MAC Filter entry.

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	
….			

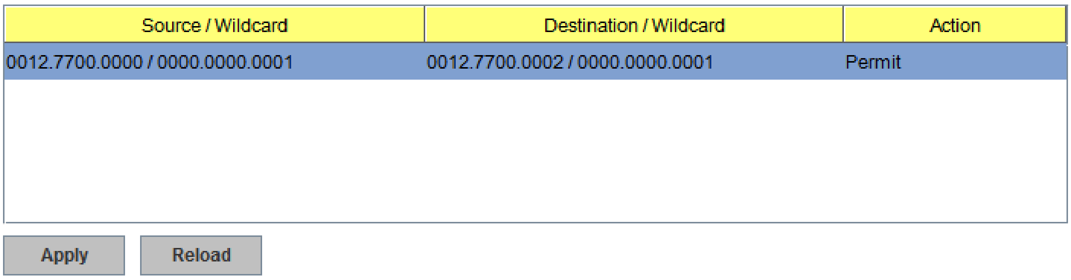


Source Wildcard: 0000.0000.0001

Once you finish the 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".



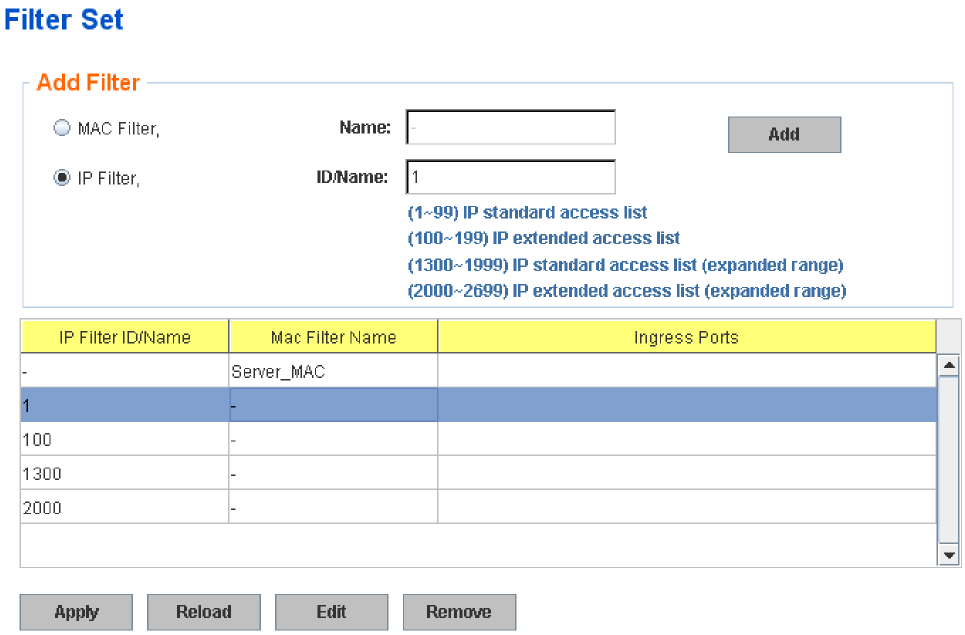
Source / Wildcard	Destination / Wildcard	Action
0012.7700.0000 / 0000.0000.0001	0012.7700.0002 / 0000.0000.0001	Permit

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

IP Filter:

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

Example :



Filter Set

Add Filter

○ MAC Filter, Name:

● IP Filter, ID/Name: 1

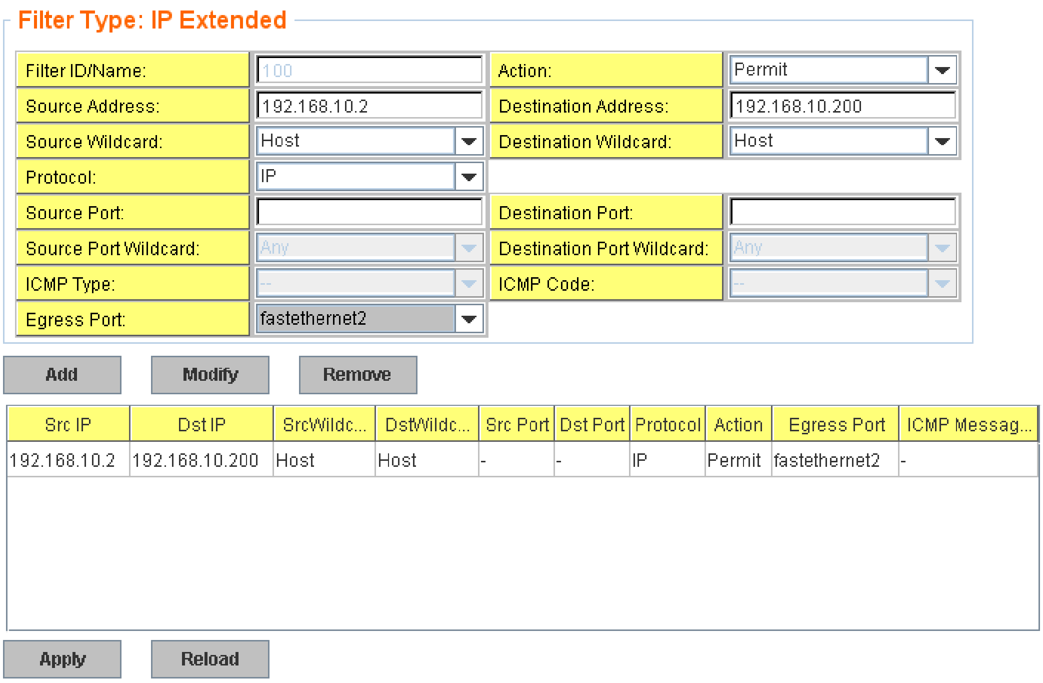
(1~99) IP standard access list
(100~199) IP extended access list
(1300~1999) IP standard access list (expanded range)
(2000~2699) IP extended access list (expanded range)

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.

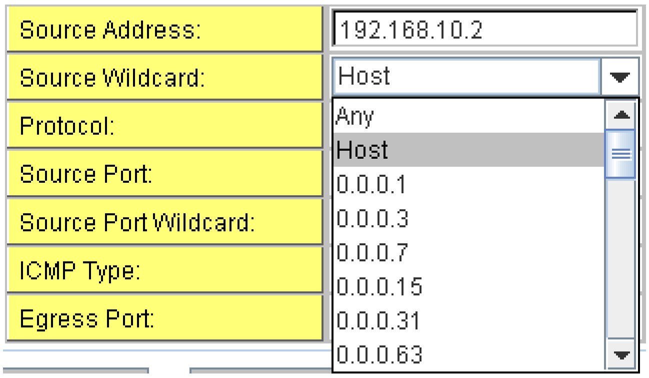
Action:

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:	
Source Port:	
Source Port Wildcard:	
ICMP Type:	
Egress Port:	

Wildcard	Bit	Number of	Note

		allowance	
Any	11111111.11111111.11111111.11111111	All	All IP addresses. Or a mask: 255.255.255.255
Host	0.0.0.0	1	Only the Source or Destination host.
0.0.0.3	0.0.0.(00000011)	3	
0.0.0.7	0.0.0.(00000111)	7	
0.0.0.15	0.0.0.(11111111)	15	
….			

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

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

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

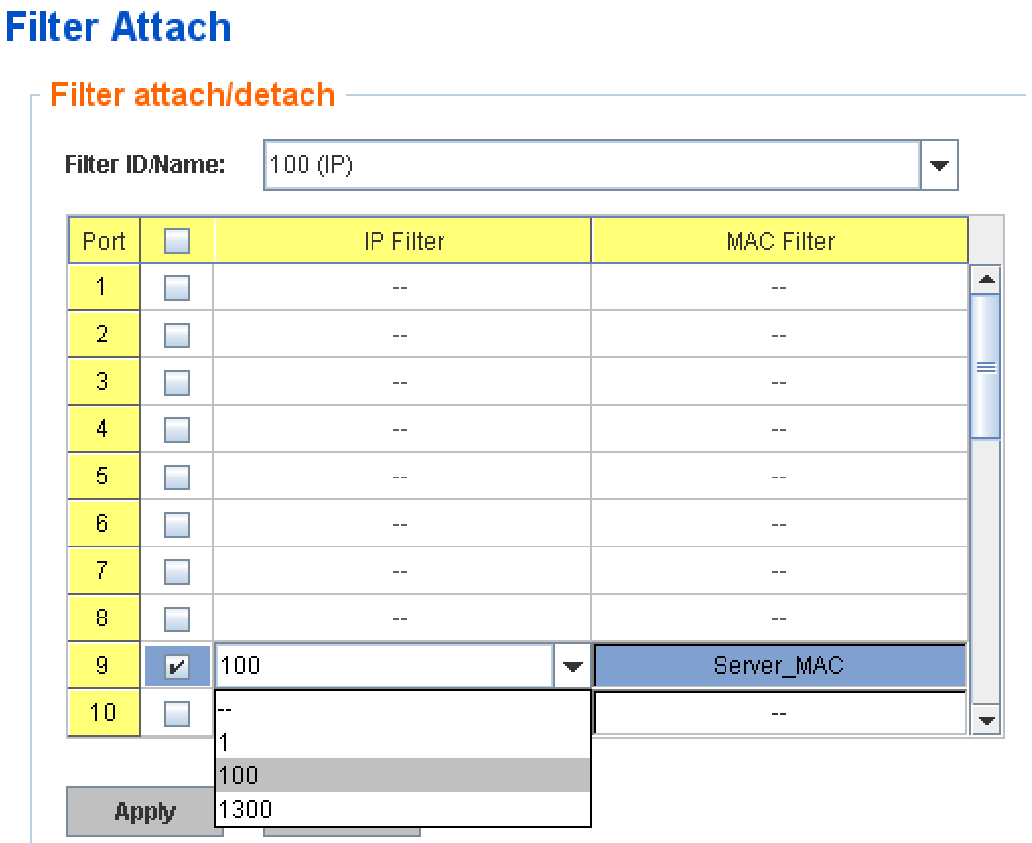
ICMP Type: The ICMP Protocol Type range from 1 ~ 255.

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

Egress Port: Bind this Filter to selected egress port.

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

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



Filter Attach

Filter attach/detach

Filter ID/Name: 100 (IP)

Port	□	IP Filter	MAC Filter
1	□	--	--
2	□	--	--
3	□	--	--
4	□	--	--
5	□	--	--
6	□	--	--
7	□	--	--
8	□	--	--
9	☑	100	Server_MAC
10	□		--

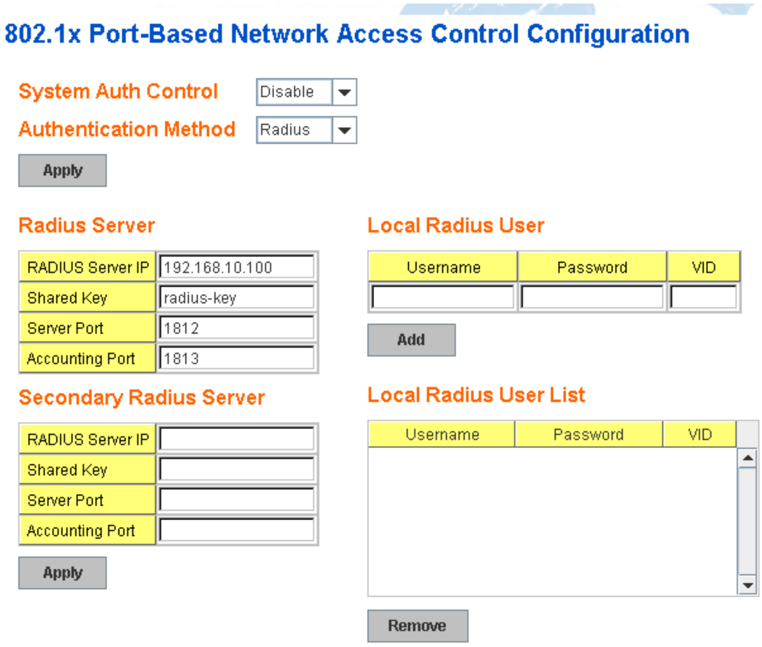
Filter Attach (Access Control List)

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

4.10.2 IEEE 802.1x

4.10.2.1 802.1X configuration

IEEE 802.1X is an IEEE standard for port based network access control, which provides authentication to the divices attached to a LAN port. It can establish a point-to-point connection or prevent any unauthenticated access from the specific port.



802.1x Port-Based Network Access Control Configuration

System Auth Control: Disable

Authentication Method: Radius

Radius Server

RADIUS Server IP	192.168.10.100
Shared Key	radius-key
Server Port	1812
Accounting Port	1813

Secondary Radius Server

RADIUS Server IP	
Shared Key	
Server Port	
Accounting Port	

Local Radius User

Username	Password	VID

Local Radius User List

Username	Password	VID

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

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

Radius Server IP: The IP address of Radius server

Shared Key: The password for the communication 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.

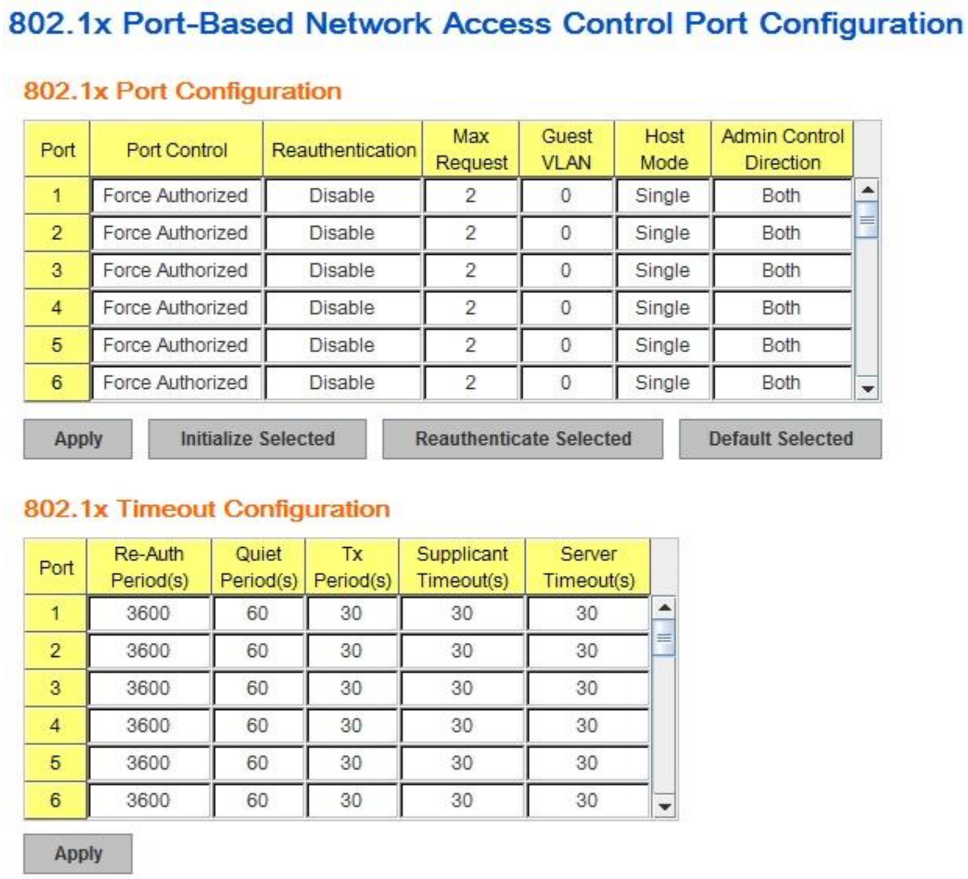
Secondary Radius Server IP: Secondary Radius Server could be set in case of the primary radius server down.

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

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

4.10.2.2 802.1x Port Configuration

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



802.1x Port-Based Network Access Control Port Configuration

802.1x Port Configuration

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

802.1x Timeout Configuration

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

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

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

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

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

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

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

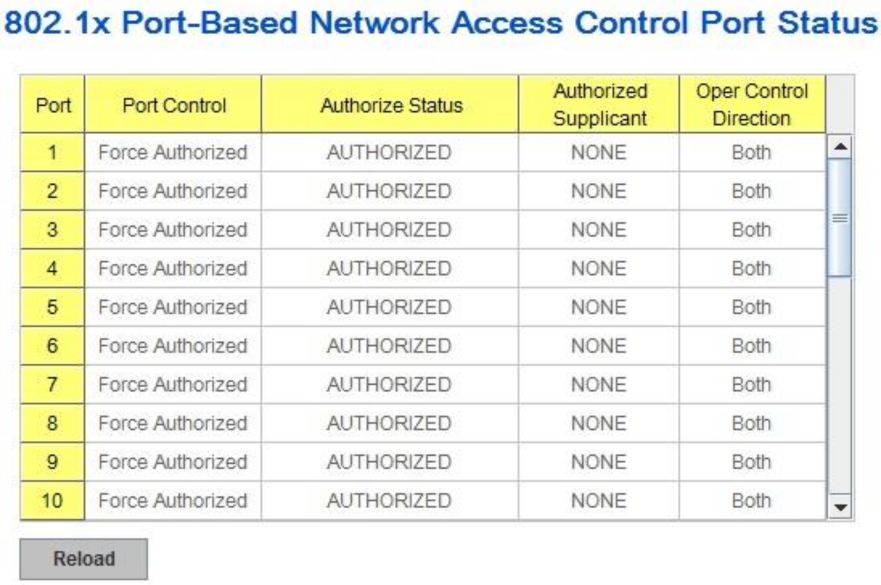
Re-Auth Period: control the Re-authentication time interval, 1~65535 is available.

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.

Click **Initialize Selected** to set the authorize state of selected port to initialize status.
Click **Reauthenticate Selected** to send EAP Request to supplicant to request reauthentication.
Click **Default Selected** to reset the configurable 802.1x parameters of selected port to the default values.

4.10.2.3 802.1X Port Status

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



802.1x Port-Based Network Access Control Port Status

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

4.10.3 CLI Commands of the Security

Command Lines of the Security configuration

Feature	Command Line
Port Security	
Add MAC access list	Switch(config)# mac access-list extended NAME access-list name Switch(config)# mac access-list extended server1 Switch(config-ext-macl)# permit Specify packets to forward deny Specify packets to reject end End current mode and change to enable mode exit Exit current mode and down to previous mode

	list Print command list no Negate a command or set its defaults quit Exit current mode and down to previous mode
Add IP Standard access list	Switch(config)# ip access-list extended Extended access-list standard Standard access-list Switch(config)# ip access-list standard <1-99> Standard IP access-list number <1300-1999> Standard IP access-list number (expanded range) WORD Access-list name Switch(config)# ip access-list standard 1 Switch(config-std-acl)# deny Specify packets to reject permit Specify packets to forward end End current mode and change to enable mode exit Exit current mode and down to previous mode list Print command list no Negate a command or set its defaults quit Exit current mode and down to previous mode remark Access list entry comment
Add IP Extended access list	Switch(config)# ip access-list extended <100-199> Extended IP access-list number <2000-2699> Extended IP access-list number (expanded range) WORD access-list name Switch(config)# ip access-list extended 100 Switch(config-ext-acl)# deny Specify packets to reject permit Specify packets to forward end End current mode and down to previous mode exit Exit current mode and down to previous mode list Print command list no Negate a command or set its defaults quit Exit current mode and down to previous mode remark Access list entry comment
Example 1: Edit MAC access list	Switch(config-ext-macl)#permit MACADDR Source MAC address xxxx.xxxx.xxxx any any source MAC address host A single source host Switch(config-ext-macl)#permit host MACADDR Source MAC address xxxx.xxxx.xxxx Switch(config-ext-macl)#permit host 0012.7711.2233 MACADDR Destination MAC address xxxx.xxxx.xxxx any any destination MAC address host A single destination host Switch(config-ext-macl)#permit host 0012.7711.2233 host MACADDR Destination MAC address xxxx.xxxx.xxxx Switch(config-ext-macl)#permit host 0012.7711.2233 host 0011.7711.2234 [IFNAME] Egress interface name Switch(config-ext-macl)#permit host 0012.7711.2233 host 0011.7711.2234 gi25 *Note: MAC Rule: Permit/Deny wildcard Source_MAC wildcard Dest_MAC Egress_Interface*
Example 1: Edit IP	Switch(config)# ip access-list extended 100

Extended access list	Switch(config-ext-acl)#permit ip Any Internet Protocol tcp Transmission Control Protocol udp User Datagram Protocol icmp Internet Control Message Protocol Switch(config-ext-acl)#permit ip A.B.C.D Source address any Any source host host A single source host Switch(config-ext-acl)#permit ip 192.168.10.1 A.B.C.D Source wildcard bits Switch(config-ext-acl)#permit ip 192.168.10.1 0.0.0.1 A.B.C.D Destination address any Any destination host host A single destination host Switch(config-ext-acl)#permit ip 192.168.10.1 0.0.0.1 192.168.10.100 0.0.0.1 [IFNAME] Egress interface name Switch(config-ext-acl)#permit ip 192.168.10.1 0.0.0.1 192.168.10.100 0.0.0.1 gi26 *Note: Follow the below rule to configure ip extended access list.* *IP Rule: Permit/Deny Source_IP wildcard Dest_IP wildcard Egress_Interface* *TCP Rule: Permit/Deny tcp Source_IP wildcard Dest_IP wildcard eq Given_Port_Number Egress_Interface* *UDP Rule: Permit/Deny udp Source_IP wildcard Dest_IP wildcard eq Given_Port_Number Egress_Interface* *ICMP Rule: Permit/Deny icmp Source_IP wildcard Dest_IP wildcard ICMP_Message_Type ICMP_Message_Code Egress_Interface*
Add MAC	Switch(config)# mac-address-table static 0012.7701.0101 vlan 1 interface fa1 mac-address-table unicast static set ok!
Port Security	Switch(config)# interface fa1 Switch(config-if)# switchport port-security Disables new MAC addresses learning and aging activities! ***Note: Rule: Add the static MAC, VLAN and Port binding first, then enable the port security to stop new MAC learning.***
Disable Port Security	Switch(config-if)# no switchport port-security Enable new MAC addresses learning and aging activities!
Display	Switch# show mac-address-table static Destination Address Address Type Vlan Destination Port ------------------- --------------- ------- ------------------------ 0012.7701.0101 Static 1 fa1
802.1x (shot of dot1x)	
enable diable	Switch(config)# dot1x system-auth-control Switch(config)# Switch(config)# no dot1x system-auth-control Switch(config)#
authentic-method	Switch(config)# dot1x authentic-method local Use the local username database for authentication radius Use the Remote Authentication Dial-In User

	Service (RADIUS) servers for authentication Switch(config)# dot1x authentic-method radius Switch(config)#
radius server-ip	Switch(config)# dot1x radius Switch(config)# dot1x radius server-ip 192.168.10.120 key 1234 RADIUS Server Port number NOT given. (default=1812) RADIUS Accounting Port number NOT given. (default=1813) RADIUS Server IP : 192.168.10.120 RADIUS Server Key : 1234 RADIUS Server Port : 1812 RADIUS Accounting Port : 1813 Switch(config)#
radius server-ip	Switch(config)# dot1x radius Switch(config)# dot1x radius server-ip 192.168.10.120 key 1234 RADIUS Server Port number NOT given. (default=1812) RADIUS Accounting Port number NOT given. (default=1813) RADIUS Server IP : 192.168.10.120 RADIUS Server Key : 1234 RADIUS Server Port : 1812 RADIUS Accounting Port : 1813 Switch(config)#
radius secondary-server-ip	Switch(config)# dot1x radius secondary-server-ip 192.168.10.250 key 5678 Port number NOT given. (default=1812) RADIUS Accounting Port number NOT given. (default=1813) Secondary RADIUS Server IP : 192.168.10.250 Secondary RADIUS Server Key : 5678 Secondary RADIUS Server Port : 1812 Secondary RADIUS Accounting Port : 1813
User name/password for authentication	Switch(config)# dot1x userna117orenixnix pass117orenixnix vlan 1
Display	Switch# show dot1x <cr> all Show Dot1x information for all interface authentic-method Dot1x authentic-method interface Interface name radius Remote Access Dial-In User Service statistics Interface name username User Name in local radius database Switch# show dot1x <cr> = Switch# show dot1x all You can check all dot1x information for all interfaces. Click Ctrl + C to exit the display Switch# show dot1x interface fa1 Supplicant MAC ADDR <NONE> STATE-MACHINE AM status : FORCE_AUTH BM status : IDLE PortStatus : AUTHORIZED

```
PortControl              : Force Authorized
Reauthentication      : Disable
MaxReq                       : 2
ReAuthPeriod            : 3600 Seconds
QuietPeriod              : 60 Seconds
TxPeriod                   : 30 Seconds
SupplicantTimeout    : 30 Seconds
ServerTimeout          : 30 Seconds
GuestVlan                  : 0
HostMode                    : Single
operControlledDirections : Both
adminControlledDirections : Both

Switch# show dot1x radius
RADIUS Server IP      : 192.168.10.100
RADIUS Server Key    : radius-key
RADIUS Server Port : 1812
RADIUS Accounting Port : 1813
Secondary RADIUS Server IP      : N/A
Secondary RADIUS Server Key    : N/A
Secondary RADIUS Server Port : N/A
Secondary RADIUS Accounting Port : N/A

Switch# show dot1x username
802.1x Local User List
  Username : orwell , Password : * , VLAN ID : 1
```

4.11 Warning

JetNet 5020G provides several types of Warning features for you to remotely monitor the status of end devices or the change of your network. The features include Fault Relay, System Log and SMTP E-mail Alert.

Following commands are included in this group:

4.11.1 Fault Relay

4.11.2 Event Selection

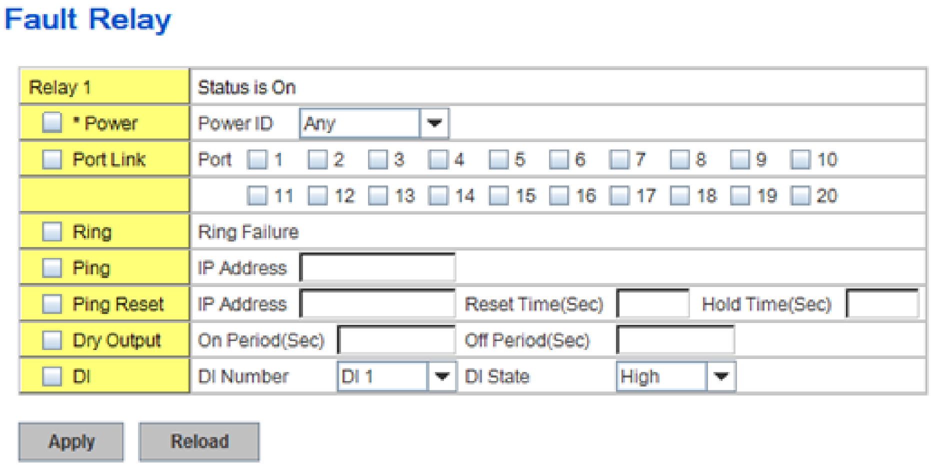
4.11.3 Syslog Configuration

4.11.4 SMTP Configuration

4.11.5 CLI Commands

4.11.1 Fault Relay

The Switch provides 1 digital output, also known as Relay Output or Fault Relay. The relay contacts are energized (open) for normal operation and will close when fault events occur. The fault event types include Power Failure, Port Link down, Ring Failure, specified IP address ping failure, DI State change or perform a period of on/off. Each Fault Relay could be trigger by multiple events.



Fault Relay

Relay 1	Status is On				
□ * Power	Power ID	Any ▾			
□ Port Link	Port □ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7 □ 8 □ 9 □ 10				
	□ 11 □ 12 □ 13 □ 14 □ 15 □ 16 □ 17 □ 18 □ 19 □ 20				
□ Ring	Ring Failure				
□ Ping	IP Address				
□ Ping Reset	IP Address		Reset Time(Sec)		Hold Time(Sec)
□ Dry Output	On Period(Sec)		Off Period(Sec)		
□ DI	DI Number	DI 1 ▾	DI State	High ▾	

Note : Select the event type and the corresponding configurations. Click on the "Apply" button to activate, and press Reload to ensure most updated status shown in Relay1 Status.

Relay1: Status Off means open relay, and Status On indicates closed relay (Led DO=Red)

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

Event Type: **Link Failure**
Select the checkbox of the Ethernet ports you want to monitor. Multiple-port selection is possible. When the selected ports are linked down or broken, the system will short Relay Output and light the DO LED.

Event Type: **Ring Failure**

Select Ring Failure. When the Ring topology is changed, the system will short Relay Output and light the DO LED.

Event Type: **Ping Failure**

IP Address: IP address of the target remote device. If pinging failure, the Relay will be activated in Status “On”(closed, LED DO=Red). If pinging successful, the Relay will stay in Status “Off” (open, LED DO=off).

Event Type: **Ping Reset Failure**

IP Address: IP address of the target device.

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

Hold Time (Sec): Waiting time to the ping duration on the target device reboot sequence.

How to configure: After selecting Ping Failure event, 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.

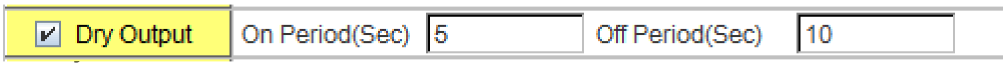
If pinging failure, which could mean the remote device does not reboot successfully, JetNet 5020G will keep **Reset/Hold cycle** until the remote device been detected. Once pinging successful, the Relay will be activated in Status “On”(closed, LED DO=Red).

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: Turn-on and turn-off period can assign the duration of the Relay output, in order to set up the control signal to external device. For example, if you connect JetNet 5020G DO to DI’ of the other terminal unit, the setting can help you to change DI’ state. If you connect JetNet 5020G DO to the power control of the other terminal units, this setting can help you to turn on or switch off the unit.

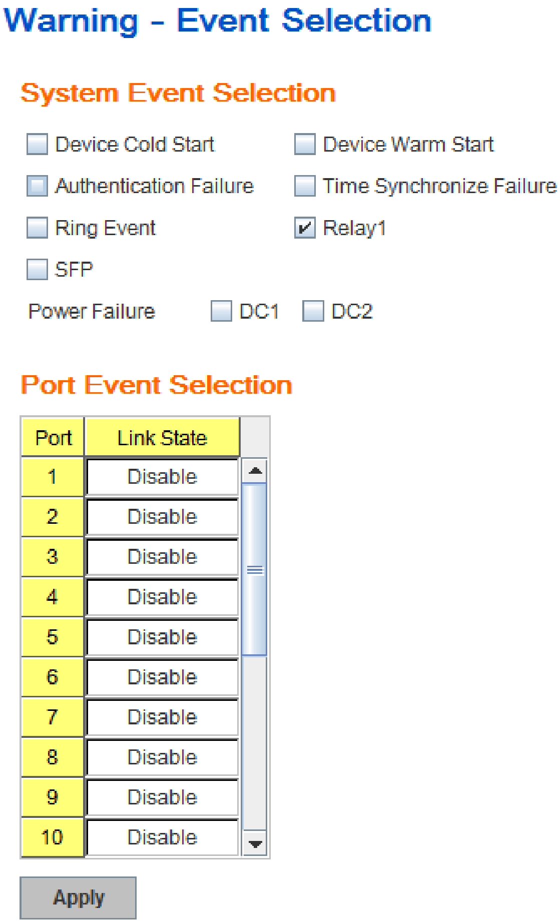


☑ Dry Output On Period(Sec) 5 Off Period(Sec) 10

How to turn On/Off the other device: Type “1” into the “On period” field and “0” into “Off Period” field and apply the setting, then it t will be triggered 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 triggered as a open circuit.
This function is also available in CLI, SNMP management interface. See the following setting.

4.11.2 Event Selection

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



Warning - Event Selection

System Event Selection

□ Device Cold Start □ Device Warm Start

□ Authentication Failure □ Time Synchronize Failure

□ Ring Event ☑ Relay1

□ SFP

Power Failure □ DC1 □ DC2

Port Event Selection

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

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.
Ring	If ring topology changed
Ping Reset	Ping target device and trigger relay to emulate power reset for remote device, if remote system crash. Note: once perform Ping reset, the relay output will form a short circuit.
Dry Output	Relay continuous perform On/Off behavior with different duration.

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)

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

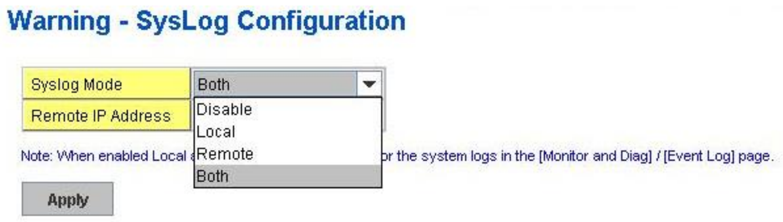
4.11.3 SysLog Configuration

System Log is useful to provide system administrator locally or remotely monitor switch events history. There are 2 System Log modes provided by JetNet 5020G, local mode and remote mode.

Local Mode: In this mode, JetNet 5020G will print the occurred events selected in the Event Selection page to System Log table of JetNet 5020G. You can monitor the system logs in [Monitor and Diag] / [Event Log] page.

Remote Mode: The remote mode is also known as Server mode in JetNet 5020G. In this mode, you should assign the IP address of the System Log server. JetNet 5020GG will send the occurred events selected in Event Selection page to System Log server you assigned.

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



Warning - SysLog Configuration

Syslog Mode	Both
Remote IP Address	

Note: When enabled Local

r the system logs in the [Monitor and Diag] / [Event Log] page.

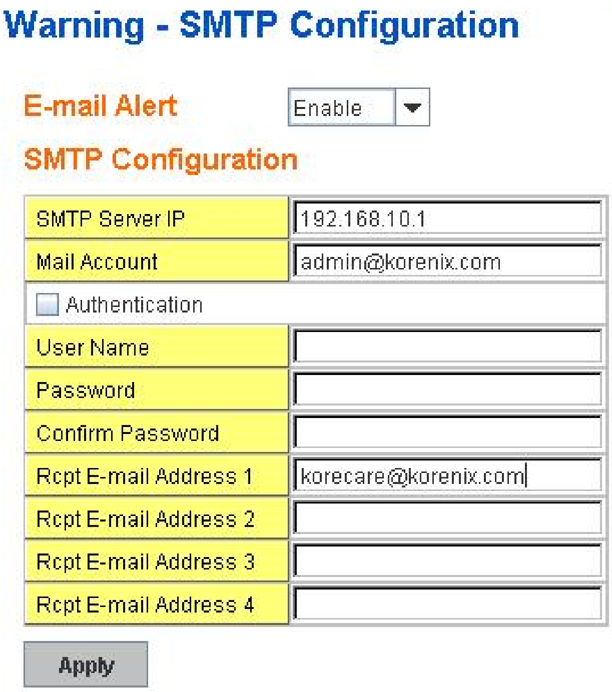
Once you finish configuring the settings, click on **Apply** to apply your configuration.

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

4.11.4 SMTP Configuration

Jet 5020G supports E-mail Warning feature. The switch will send the occurred events to remote E-mail server. The receiver can notified by E-mail. The E-mail warning machenism conforms 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 for authorizations, you can also set up the username and password in this page.



Warning - SMTP Configuration

E-mail Alert: Enable

SMTP Configuration

SMTP Server IP	192.168.10.1
Mail Account	admin@korenix.com
□ Authentication	
User Name	
Password	
Confirm Password	
Rcpt E-mail Address 1	korecare@korenix.com
Rcpt E-mail Address 2	
Rcpt E-mail Address 3	
Rcpt E-mail Address 4	

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 Managed Switch	
Rcpt E-mail Address 1	The first email address to receive email alert from Managed Switch (Max. 40 characters)
Rcpt E-mail Address 2	The second email address to receive email alert from Managed Switch (Max. 40 characters)
Rcpt E-mail Address 3	The third email address to receive email alert from Managed Switch (Max. 40 characters)
Rcpt E-mail Address 4	The fourth email address to receive email alert from Managed Switch (Max. 40 characters)

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

4.11.5 CLI Commands

Command Lines of the Warning configuration

Feature	Command Line
Relay Output	
Relay Output	Switch(config)# relay 1 dry dry output ping ping failure port port link failure ring ring failure
Dry Output	Switch(config)# relay 1 dry <0-65535> turn on period in second Switch(config)# relay 1 dry 5 <0-65535> 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, ex: fa1,fa3-5,gi17-20 Switch(config)# relay 1 port fa1-5
Ring Failure	Switch(config)# relay 1 ring
Disable Relay	Switch(config)# no relay 1 relay id Switch(config)# no relay 1
Display	Switch# show relay 1 Relay 1 Event : Power : Disabled Port Link : Disabled Ring : Disabled Ping : Disabled Ping Reset : Disabled Dry Output : Disabled DI : Disabled
Event Selection	
Event Selection	Switch(config)# warning-event coldstart Switch cold start event warmstart Switch warm start event authentication Authentication failure event linkdown Switch link down event linkup Switch link up event ring Switch ring event fault-relay Switch fault relay event time-sync Switch time synchronize event sfp Switch SFP event loop-protect Switch loop protection event
Ex: Cold Start event	Switch(config)# warning-event coldstart Set cold start event enable ok.

Ex: Link Up event	Switch(config)# warning-event linkup [IFNAME] Interface name, ex: fastethernet1 or gi8 Switch(config)# warning-event linkup fa5 Set fa5 link up event enable ok.
Display	Switch# show warning-event Warning Event: Cold Start: Disabled Warm Start: Disabled Authentication Failure: Disabled Link Down: Disabled Link Up: Disabled Ring: Disabled Fault Relay: Disabled Time Synchronize Failure: Disabled SFP: Disabled Loop Protection: Disabled
Syslog Configuration	
Local Mode	Switch(config)# log syslog local
Server Mode	Switch(config)# log syslog remote 192.168.10.33
Both	Switch(config)# log syslog local Switch(config)# log syslog remote 192.168.10.33
Disable	Switch(config)# no log syslog local
SMTP Configuration	
SMTP Enable	Switch(config)# smtp-server enable email-alert SMTP Email Alert set enable ok.
Sender mail	Switch(config)# smtp-server server 192.168.10.100 ACCOUNT SMTP server mail account, ex: admin@korenix.com Switch(config)# smtp-server server 192.168.10.100 admin@korenix.com SMTP Email Alert set Server: 192.168.10.100, Account: admin@korenix.com ok.
Receiver mail	Switch(config)# smtp-server receipt admin@example.com SMTP Email Alert set receipt 1: admin@example.com ok.
Authentication with username and password	Switch(config)# smtp-server authentication username admin password admin SMTP Email Alert set authentication Username: admin, Password: admin **Note: You can assign string to username and password.**
Disable SMTP	Switch(config)# no smtp-server enable email-alert SMTP Email Alert set disable ok.
Disable Authentication	Switch(config)# no smtp-server authentication SMTP Email Alert set Authentication disable ok.
Display	Switch# sh smtp-server SMTP Email Alert is Enabled Server: 192.168.10.100, Account: admin@example.com Authentication: Enabled Username: admin, Password: admin SMTP Email Alert Receipt: Receipt 1: admin@example.com Receipt 2: Receipt 3: Receipt 4:

4.12 Monitor and Diagnostic

JetNet 5020G provides several types of features for you to monitor the status of the switch or diagnose the problems encountered. The features include MAC Address Table, Port Statistics, Port Mirror, Event Log and Ping.

Following commands are included in this group:

4.12.1 MAC Address Table

4.12.2 Port Statistics

4.12.3 Port Mirroring

4.12.4 Event Log

4.12.5 Topology Discovery (LLDP)

4.12.6 Ping

4.12.7 Modbus/TCP

4.12.8 CLI Commands of the Monitor and Diag

4.12.1 MAC Address Table

JetNet 5020G 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

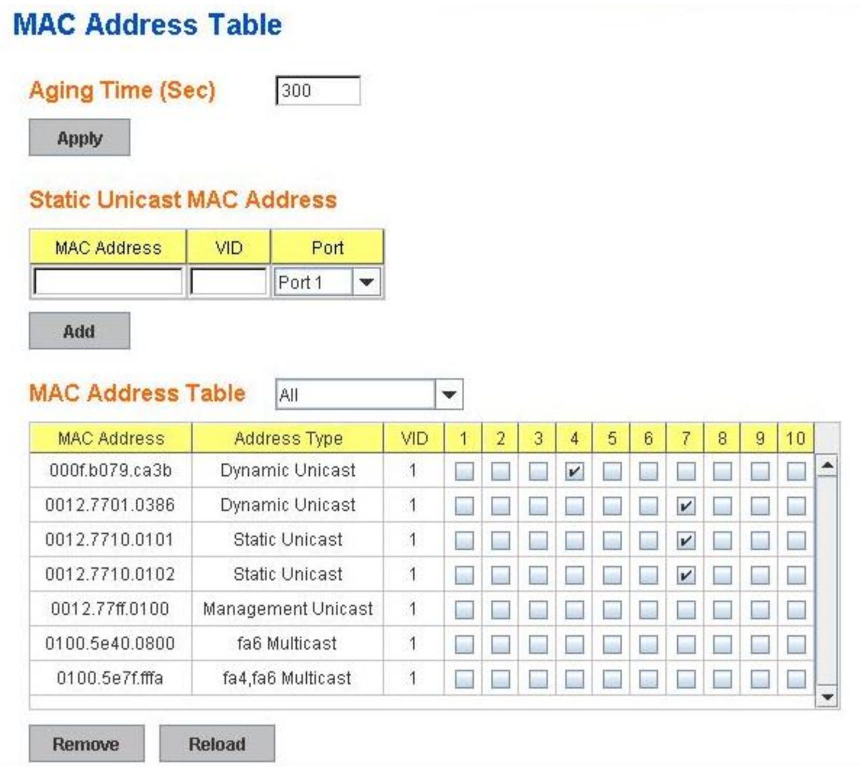
In some applications, users may need to type in the static Unicast MAC address to its MAC address table. In this page, you can type MAC Address (format: xxxx.xxxx.xxxx), select its VID and Port ID, and then click on **Add** to add it to MAC Address table.

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

Aging Time (Sec) 300

Static Unicast MAC Address

MAC Address	VID	Port
		Port 1

MAC Address Table All

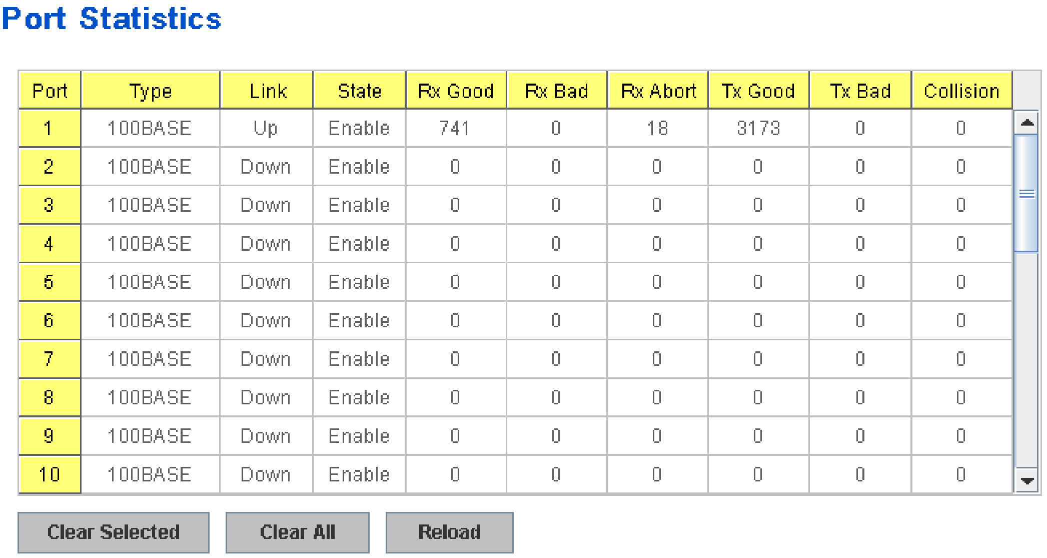
MAC Address	Address Type	VID	1	2	3	4	5	6	7	8	9	10
000f.b079.ca3b	Dynamic Unicast	1	□	□	□	☑	□	□	□	□	□	□
0012.7701.0386	Dynamic Unicast	1	□	□	□	□	□	□	☑	□	□	□
0012.7710.0101	Static Unicast	1	□	□	□	□	□	□	☑	□	□	□
0012.7710.0102	Static Unicast	1	□	□	□	□	□	□	☑	□	□	□
0012.77ff.0100	Management Unicast	1	□	□	□	□	□	□	□	□	□	□
0100.5e40.0800	fa6 Multicast	1	□	□	□	□	□	□	□	□	□	□
0100.5e7f.fffa	fa4,fa6 Multicast	1	□	□	□	□	□	□	□	□	□	□

4.12.2 Port Statistics

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

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

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



Port Statistics

Port	Type	Link	State	Rx Good	Rx Bad	Rx Abort	Tx Good	Tx Bad	Collision
1	100BASE	Up	Enable	741	0	18	3173	0	0
2	100BASE	Down	Enable	0	0	0	0	0	0
3	100BASE	Down	Enable	0	0	0	0	0	0
4	100BASE	Down	Enable	0	0	0	0	0	0
5	100BASE	Down	Enable	0	0	0	0	0	0
6	100BASE	Down	Enable	0	0	0	0	0	0
7	100BASE	Down	Enable	0	0	0	0	0	0
8	100BASE	Down	Enable	0	0	0	0	0	0
9	100BASE	Down	Enable	0	0	0	0	0	0
10	100BASE	Down	Enable	0	0	0	0	0	0

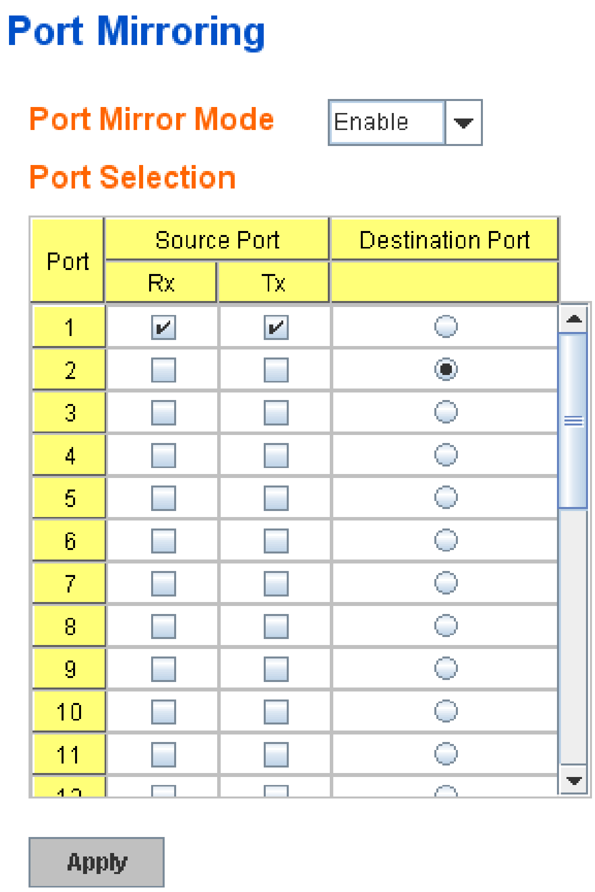
4.12.3 Port Mirroring

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

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

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

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



Port Mirroring

Port Mirror Mode: Enable

Port Selection

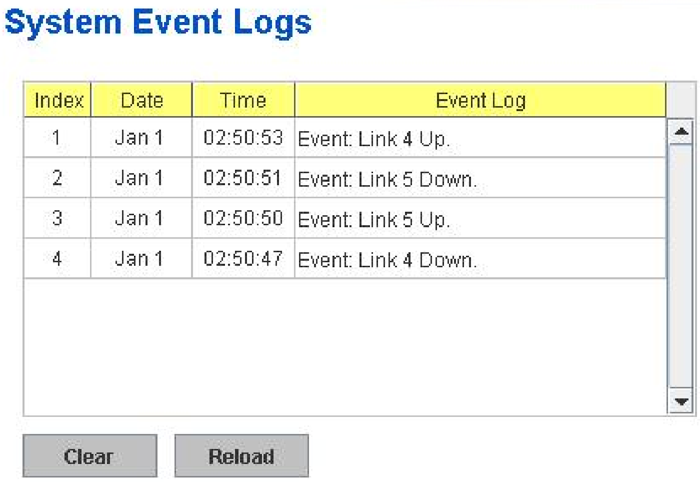
Port	Source Port		Destination Port
	Rx	Tx	
1	☑	☑	○
2	□	□	●
3	□	□	○
4	□	□	○
5	□	□	○
6	□	□	○
7	□	□	○
8	□	□	○
9	□	□	○
10	□	□	○
11	□	□	○
12	□	□	○

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

4.12.4 Event Log

In the 4.10.3, we have introduced System Log feature. When System Log Local mode is selected, JetNet 5020G will record occurred events in local log table. This page shows this log table. The entry includes the index, occurred data and time and content of the events.

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



System Event Logs

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

4.12.5 Topology Discovery (LLDP)

JetNet 5020G supports 802.1AB Link Layer Discovery Protocol, thus JetNet 5020G can be discovered by the Network Management System which support LLDP discovery. With LLDP supported, the NMS can easier maintain the topology map, display port ID, port description, system description, VLAN ID… Once the link failure, the topology change events can be updated to the NMS as well. The LLDP Port State can display the neighbor ID and IP leant from the connected devices.

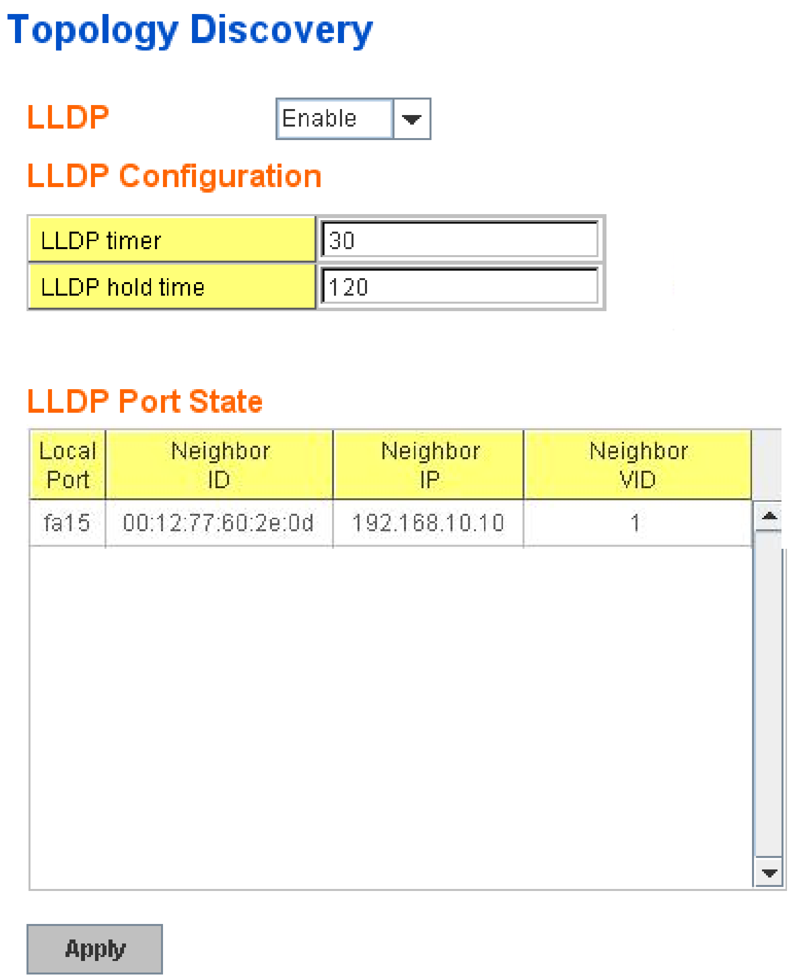
LLDP: Enable/Disable the LLDP topology discovery information.

LLDP Configuration: To configure the related timer of LLDP.

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

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

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



Topology Discovery

LLDP: Enable

LLDP Configuration

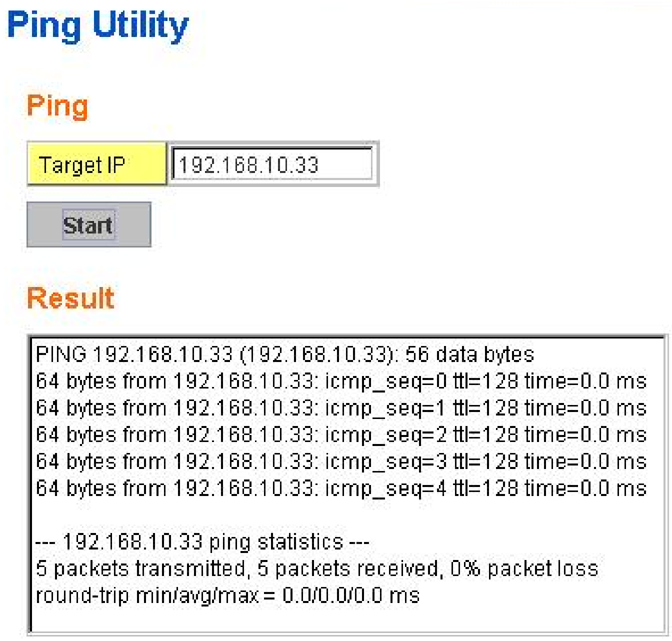
LLDP timer	30
LLDP hold time	120

LLDP Port State

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

4.12.6 Ping Utility

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



Ping Utility

Ping

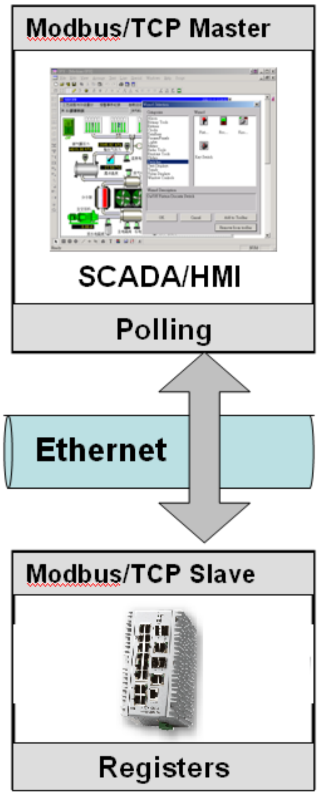
Target IP	192.168.10.33

Result

```
PING 192.168.10.33 (192.168.10.33): 56 data bytes
64 bytes from 192.168.10.33: icmp_seq=0 ttl=128 time=0.0 ms
64 bytes from 192.168.10.33: icmp_seq=1 ttl=128 time=0.0 ms
64 bytes from 192.168.10.33: icmp_seq=2 ttl=128 time=0.0 ms
64 bytes from 192.168.10.33: icmp_seq=3 ttl=128 time=0.0 ms
64 bytes from 192.168.10.33: icmp_seq=4 ttl=128 time=0.0 ms

--- 192.168.10.33 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

4.12.7 Modbus/TCP (CLI mode only)



The Modbus is the most popular industrial protocol being used today. Modbus is a “master-slave” architecture, where the “master” sends polling request with address and data it wants to one of multiple “slaves”. The slave device that is addressed responds to master. The master is often a PC, PLC, DCS or RTU… The salves are often the field devices. Some of them are “hybrid”.

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

Korenix JetNet 5428G implements the Modbus/TCP registers into the latest firmware. The registers include the System information, firmware information, IP address, interfaces’ status, port information, SFP information, inbound/outbound packet information.

With the supported registers, users can read the information through their own Modbus/TCP based progress/ display/ monitor applications and monitor the status of the switch easily.

There is no Web UI for Modbus/TCP configuration. The Modbus/TCP configuration can be changed through CLI.

Modbus/TCP Register Table

Word Address	Data Type	Description
System Information		
0x0000	16 words	Vender Name = “Korenix” Word 0 Hi byte = ‘K’ Word 0 Lo byte = ‘o’ Word 1 Hi byte = ‘r’ Word 1 Lo byte = ‘e’ Word 2 Hi byte = ‘n’ Word 2 Lo byte = ‘I’ Word 2 Hi byte = ‘x’ Word 2 Lo byte = ‘\0’ (other words = 0)
0x0010	16 words	Product Name = "JetNet5428GV2-AC" Word 0 Hi byte = ‘J’ Word 0 Lo byte = ‘e’

		Word 1 Hi byte = 'T' Word 1 Lo byte = 'N' Word 2 Hi byte = 'e' Word 2 Lo byte = 't' Word 3 Hi byte = '5' Word 3 Lo byte = '4' Word 4 Lo byte = '2' Word 4 Hi byte = '8' Word 5 Lo byte = 'G' Word 5 Hi byte = 'V' Word 6 Lo byte = '2' Word 6 Lo byte = '-' Word 7 Hi byte = 'A' Word 7 Lo byte = 'C' Word 8 Hi byte = '\0' (other words = 0)
0x0020	128 words	SNMP system name (string)
0x00A0	128 words	SNMP system location (string)
0x0120	128 words	SNMP system contact (string)
0x01A0	32 words	SNMP system OID (string)
0x01C0	2 words	System uptime (unsigned long)
0x01C2 to 0x01FF	60 words	Reserved address space
0x0200	2 words	hardware version
0x0202	2 words	S/N information
0x0204	2 words	CPLD version
0x0206	2 words	Boot loader version
0x0208	2 words	Firmware Version Word 0 Hi byte = major Word 0 Lo byte = minor Word 1 Hi byte = reserved Word 1 Lo byte = reserved
0x020A	2 words	Firmware Release Date Firmware was released on 2010-08-11 at 09 o'clock Word 0 = 0x0B09 Word 1 = 0x0A08
0x020C	3 words	Ethernet MAC Address

		Ex: MAC = 01-02-03-04-05-06 Word 0 Hi byte = 0x01 Word 0 Lo byte = 0x02 Word 1 Hi byte = 0x03 Word 1 Lo byte = 0x04 Word 2 Hi byte = 0x05 Word 2 Lo byte = 0x06
0x020F to 0x2FF	241 words	Reserved address space
0x0300	2 words	IP address Ex: IP = 192.168.10.1 Word 0 Hi byte = 0xC0 Word 0 Lo byte = 0xA8 Word 1 Hi byte = 0x0A Word 1 Lo byte = 0x01
0x0302	2 words	Subnet Mask
0x0304	2 words	Default Gateway
0x0306	2 words	DNS Server
0x0308 to 0x3FF	248 words	Reserved address space (IPv6 or others)
0x0400	1 word	AC1 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0401	1 word	AC2 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0402	1 word	DC1 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0403	1 word	DC2 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0404 to 0x040F	12 words	Reserved address space

0x0410	1 word	DI1 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0411	1 word	DI2 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0412	1 word	DO1 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0413	1 word	DO2 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0414 to 0x041F	12 words	Reserved address space
0x0420	1 word	RDY 0x0000:Off 0x0001:On
0x0421	1 word	RM 0x0000:Off 0x0001:On
0x0422	1 word	RF 0x0000:Off 0x0001:On
0x0423	1 word	RS
Port Information (32 Ports)		
0x1000 to 0x11FF	16 words	Port Description
0x1200 to 0x121F	1 word	Administrative Status 0x0000: disable 0x0001: enable
0x1220 to 0x123F	1 word	Operating Status 0x0000: disable 0x0001: enable

		0xFFFF: unavailable
0x1240 to 0x125F	1 word	Duplex 0x0000: half 0x0001: full 0x0003: auto (half) 0x0004: auto (full) 0x0005: auto 0xFFFF: unavailable
0x1260 to 0x127F	1 word	Speed 0x0001: 10 0x0002: 100 0x0003: 1000 0x0004: 2500 0x0005: 10000 0x0101: auto 10 0x0102: auto 100 0x0103: auto 1000 0x0104: auto 2500 0x0105: auto 10000 0x0100: auto 0xFFFF: unavailable
0x1280 to 0x129F	1 word	Flow Control 0x0000: off 0x0001: on 0xFFFF: unavailable
0x12A0 to 0x12BF	1 word	Default Port VLAN ID 0x0001-0xFFFF
0x12C0 to 0x12DF	1 word	Ingress Filtering 0x0000: disable 0x0001: enable
0x12E0 to 0x12FF	1 word	Acceptable Frame Type 0x0000: all 0x0001: tagged frame only
0x1300 to 0x131F	1 word	Port Security 0x0000: disable 0x0001: enable
0x1320 to 0x133F	1 word	Auto Negotiation 0x0000: disable

		0x0001: enable 0xFFFF: unavailable
0x1340 to 0x135F	1 word	Loopback Mode 0x0000: none 0x0001: MAC 0x0002: PHY 0xFFFF: unavailable
0x1360 to 0x137F	1 word	STP Status 0x0000: disabled 0x0001: blocking 0x0002: listening 0x0003: learning 0x0004: forwarding
0x1380 to 0x139F	1 word	Default CoS Value for untagged packets
0x13A0 to 0x13BF	1 word	MDIX 0x0000: disable 0x0001: enable 0x0002: auto 0xFFFF: unavailable
0x13C0 to 0x13DF	1 word	Medium mode 0x0000: copper 0x0001: fiber 0x0002: none 0xFFFF: unavailable
0x13E0 to 0x14FF	288 words	Reserved address space
SFP Information (32 Ports)		
0x1500 to 0x151F	1 word	SFP Type
0x1520 to 0x153F	1 words	Wave length
0x1540 to 0x157F	2 words	Distance
0x1580 to 0x167F	8 words	Vender
0x1680 to 0x17FF	384 words	Reserved address space

SFP DDM Information (32 Ports)		
0x1800 to 0x181F	1 words	Temperature
0x1820 to 0x185F	2 words	Alarm Temperature
0x1860 to 0x187F	1 words	Tx power
0x1880 to 0x18BF	2 words	Warning Tx power
0x18C0 to 0x18DF	1 words	Rx power
0x18E0 to 0x191F	2 words	Warning Rx power
0x1920 to 0x1FFF	1760 words	Reserved address space
Inbound packet information		
0x2000 to 0x203F	2 words	Good Octets
0x2040 to 0x207F	2 words	Bad Octets
0x2080 to 0x20BF	2 words	Unicast
0x20C0 to 0x20FF	2 words	Broadcast
0x2100 to 0x213F	2 words	Multicast
0x2140 to 0x217F	2 words	Pause
0x2180 to 0x21BF	2 words	Undersize
0x21C0 to 0x21FF	2 words	Fragments
0x2200 to 0x223F	2 words	Oversize
0x2240 to 0x227F	2 words	Jabbers
0x2280 to 0x22BF	2 words	Discards

0x22C0 to 0x22FF	2 words	Filtered frames
0x2300 to 0x233F	2 words	RxError
0x2340 to 0x237F	2 words	FCSError
0x2380 to 0x23BF	2 words	Collisions
0x23C0 to 0x23FF	2 words	Dropped Frames
0x2400 to 0x243F	2 words	Last Activated SysUpTime
0x2440 to 0x24FF	191 words	Reserved address space
Outbound packet information		
0x2500 to 0x253F	2 words	Good Octets
0x2540 to 0x257F	2 words	Unicast
0x2580 to 0x25BF	2 words	Broadcast
0x25C0 to 0x25FF	2 words	Multicast
0x2600 to 0x263F	2 words	Pause
0x2640 to 0x267F	2 words	Deferred
0x2680 to 0x26BF	2 words	Collisions
0x26C0 to 0x26FF	2 words	SingleCollision
0x2700 to 0x273F	2 words	MultipleCollision
0x2740 to 0x277F	2 words	ExcessiveCollision
0x2780 to 0x27BF	2 words	LateCollision
0x27C0 to	2 words	Filtered

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

4.12.8 CLI Commands of the Monitor and Diag

Command Lines of the Monitor and Diagnostic configuration

Feature	Command Line
MAC Address Table	
Ageing Time	Switch(config)# mac-address-table aging-time 350 mac-address-table aging-time set ok! *Note: 350 is the new ageing timeout value.*
Add Static Unicast MAC address	Switch(config)# mac-address-table static 0012.7701.0101 vlan 1 interface fastethernet7 mac-address-table ucast static set ok! ***Note: rule: mac-address-table static MAC_address VLAN VID interface interface_name***
Add Multicast MAC address	Switch(config)# mac-address-table multicast 0100.5e01.0101 vlan 1 interface fa6-7 Adds an entry in the multicast table ok! ***Note: rule: mac-address-table multicast MAC_address VLAN VID interface_list interface_name/range***
Show MAC Address Table – All types	Switch# show mac-address-table ***** UNICAST MAC ADDRESS ***** 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.fffa 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.fffa 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.
Port Statistics	

Port Statistics	Switch# show rmon statistics fa4 (select interface)
	Interface fastethernet4 is enable connected, which has
	  Inbound:
	    Good Octets: 178792, Bad Octets: 0
	    Unicast: 598, Broadcast: 1764, Multicast: 160
	    Pause: 0, Undersize: 0, Fragments: 0
	    Oversize: 0, Jabbers: 0, Disacrds: 0
	    Filtered: 0, RxError: 0, FCSError: 0
	  Outbound:
	    Good Octets: 330500
	    Unicast: 602, Broadcast: 1, Multicast: 2261
	    Pause: 0, Deferred: 0, Collisions: 0
	    SingleCollision: 0, MultipleCollision: 0
	    ExcessiveCollision: 0, LateCollision: 0
	    Filtered: 0, FCSError: 0
	Number of frames received and transmitted with a length of:
	    64: 2388, 65to127: 142, 128to255: 11
	    256to511: 64, 512to1023: 10, 1024toMaxSize: 42

Port Mirroring	
Enable Port Mirror	Switch(config)# mirror en Mirror set enable ok.
Disable Port Mirror	Switch(config)# mirror disable Mirror set disable ok.

Select Source Port	Switch(config)# mirror source fa1-2
	  both Received and transmitted traffic
	  rx Received traffic
	  tx Transmitted traffic

	Switch(config)# mirror source fa1-2 both Mirror source fa1-2 both set ok. ***Note: Select source port list and TX/RX/Both mode.***
Select Destination Port	Switch(config)# mirror destination fa6 both Mirror destination fa6 both set ok
Display	Switch# show mirror Mirror Status : Enabled Ingress Monitor Destination P rt : fa6 Egress Monitor Destination P rt : fa6 Ingress Source Po ts :fa1,fa2, Egress Source Po ts :fa1,fa2,
Event Log	
Display	Switch# show event-log <1>Jan 1 02:50:47 snmpd[101]: Event: Link 4 Down. <2>Jan 1 02:50:50 snmpd[101]: Event: Link 5 Up. <3>Jan 1 02:50:51 snmpd[101]: Event: Link 5 Down. <4>Jan 1 02:50:53 snmpd[101]: Event: Link 4 Up.
Topology Discovery (LLDP)	
Enable LLDP	Switch(config)# lldp holdtime Specify the holdtime of LLDP in seconds run Enable LLDP timer Set the transmission frequency of LLDP in seconds Switch(config)# lldp run LLDP is enabled!

Change LLDP timer	Switch(config)# lldp holdtime
	  <10-255> Valid range is 10~255
	Switch(config)# lldp timer
	  <5-254> Valid range is 5~254

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

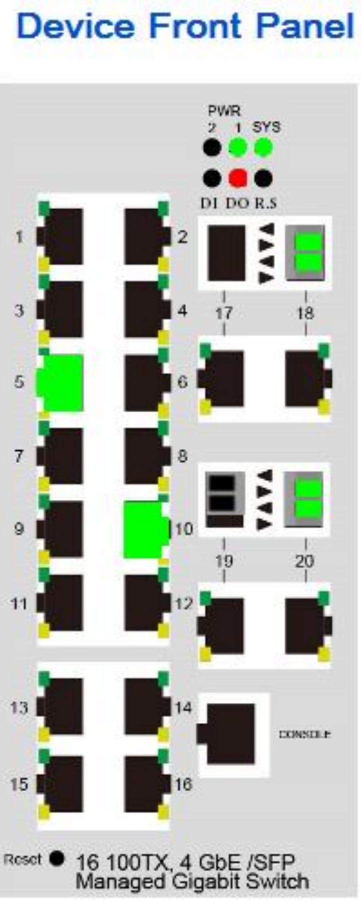
Number of the Modbus/TCP Master	Switch(config)# modbus
	  idle-timeout Max interval between requests
	  master Modbus TCP Master
	  port Listening Port
	Switch(config)# modbus master
	  <1-20> Max Modbus TCP Master

Modbus/TCP idle time	Switch(config)# modbus idle-timeout <200-10000> Timeout vlaue: 200-10000ms
Modbus/TCP port number	Switch(config)# modbus port <1-65535> Port Number

4.13 Device Front Panel

The command – “Device Front Panel” that allows you to check the LED status of the switch from Web browser. You can see LED and link status of the Power, DO, R.M. and Font Ports. Below is the example of managed Switch. Different model has its own front panel display

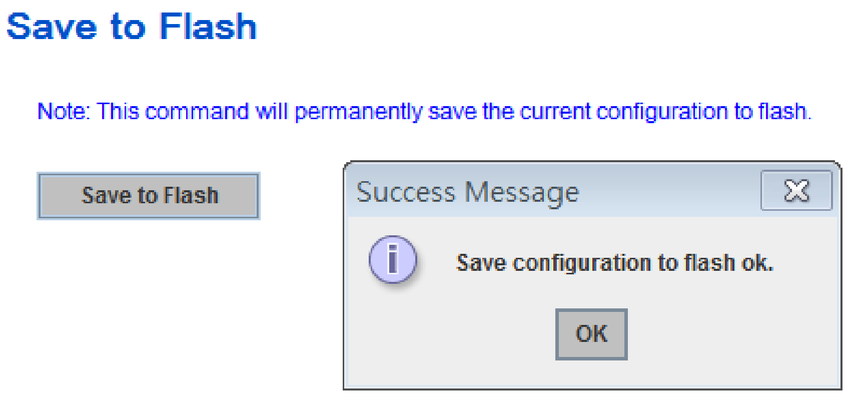
Feature	On / Link UP	Off / Link Down	Other
Power 1 (PWR1)	Green	Black	
Power 2 (PWR2)	Green	Black	
System (SYS)	Green	Black	
Digital Iutput (DI)	Red	Black	
Digital Output (DO)	Red	Black	
Ring Status (R.S.)	Green/Amber	Black	
Fast Ethernet	Green	Black	
Gigabit Ethernet	Green	Black	
SFP	Green	Black	Gray: Plugged but not link up yet.



JetNet 5020G front panel.

4.14 Save to Flash

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



Save to Flash

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

Success Message

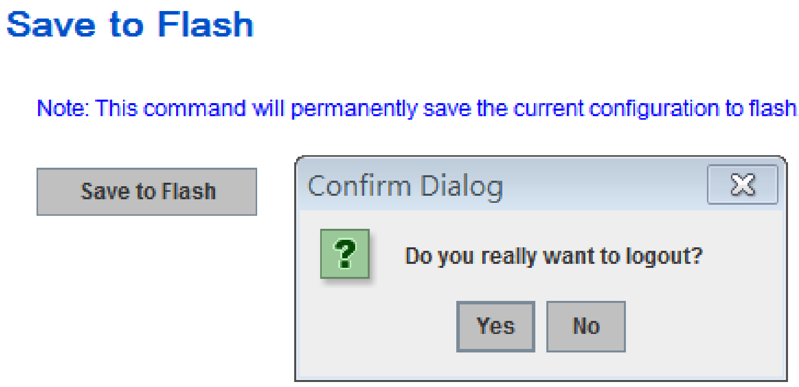
Save configuration to flash ok.

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.



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

Do you really want to logout?

Command Lines:

Feature	Command Line
Logout	SWITCH> exit SWITCH# exit

5 Appendix

5.1 The SFP family

Korenix have certificated many types of SFP transceiver. These certificated SFP transceivers can be identified by JetNet 5020G and displayed in the UI. The SFP transceivers we certificated can meet up the critical needs under industrial environment needs. It is recommend that use Korenix certificated SFP transceivers when constructing your network.

We will keep updating the certification process and posting the certificated SFP transceivers on our web site. You can refer to Korenix web site or contact local sale rep for the latest selection guide on SFP transceivers.

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

5.2 Korenix Private MIB

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

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

The path of the **JetNet 5020G** is 1.3.6.1.4.1.24062.2.2.24

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

5.3 Specification

Technology	
Standard	IEEE 802.3u 10Base-T Ethernet IEEE 802.3u 100Base-TX Fast Ethernet IEEE 802.3u 100Base-FX Fast Ethernet Fiber IEEE 802.3ab 1000Base-T Gigabit Ethernet copper IEEE 802.3z Gigabit Ethernet Fiber IEEE 802.3x Flow Control and back-pressure IEEE 802.1AB Link Layer Discovery Protocol (LLDP) IEEE 802.1p Class of Service (CoS) IEEE 802.1Q VLAN and GVRP IEEE 802.1Q Double Tag VLAN (QinQ) IEEE 802.1D Rapid Spanning Tree (RSTP) IEEE 802.1S Multiple Spanning Tree Protocol (MSTP) IEEE 802.3ad Link Aggregation Protocol (LACP) IEEE 802.1x Port based Network Access Protocol ITU-T G.8032 ERPS v1/v2 IEEE 1588 PTP
Performance	
Switch Technology	Store and Forward Technology with 6.6Gbps Non-Blocking Switching Fabric
System Throughput	16.6 Mega packet per second, 64Bytes packet length
CPU Performance	600Mhz MIPS CPU with 10 Seconds Hardware Based Watchdog Timer
System Memory	128Mbytes RAM, 32Mbytes Flash ROM
Transfer packet Size	64Bytes ~9728Bytes (include double Tag VLAN)
MAC address Table	16K
Packet Buffer	1.5Mbytes shared memory
Transfer performance	14,880 pps for Ethernet, 148,800 for Fast Ethernet, 1488,100 for Gigabit Ethernet
Management	
Configuration, monitoring interface	•In-Band Management: Telnet with SSH, Web-Browser with SSL, IPv4/IPv6 SNMP V1/V2c/V3 with SNMP Trap (4 Trap Stations), RMON Group 1,2,3,9 •Out-Band Management: Local RS-232/RJ-45 connector with Cisco like command
System Manage Secure	•Telnet/Local Console support command like interface with Cisco like commands, and offers 4 management sessions; the system supports SSL for HTTP security, SSH for Telnet security

	•Supports Manage Station with IP Secure function, up to 4 Manage Stations •Management Device Login Switch System by Remote Radius account/password, key for RADIUS Server authentication
SNMP MIB	MIB II, Bridge MIB, Ethernet Like MIB, VLAN MIB, IGMP MIB< Private MIB
Management Utility	Supports Korenix windows utility with IEEE 802.1AB link Layer Protocol for Device finding and Link Topology Discovery
Network Time Protocol	NTP protocol with daylight saving and localize time sync function
IEEE 1588 PTP	IEEE 1588 Precision Time Protocol v1/v2
E-mail Warning	4 receipt E-mail accounts with mail server authentication
System log	Local or remote log server with authentication
System Auto Maintenance	Power on Auto Firmware upgrade and Configure upload
Network Performance	
Port Configuration	Port Link Speed, Link Mode, Link Status and Port Enable/Disable
Port Trunk/ Link Aggregation	IEEE 802.3ad port aggregation and static port trunk, Trunk member up to 8 ports, maximum 10 trunk groups include Gigabit Ethernet port
VLAN	IEEE 802.1Q tag VLAN with 4K VLAN entries, 2K GVRP entries 3 VLAN modes – Trunk, Hybrid and Link access
Private VLAN	Direct Client ports in isolated /community VLAN to promiscuous port in primary VLAN
IEEE 802.1 QinQ	Double Tag for Private VLAN Access
Class of Service	IEEE 802.1p class of service, 8 priority queues/port
Traffic Prioritize	Supports 8 physical queues with weighted fair queuing (WRR) or Strict Priority Schemer, which follows IEEE 802.1p CoS tag ID and IPv4 Type of Service/Differ information to prioritize the traffic of your industrial network
IGMP Snooping	IGMP Snooping v1/v2c/v3 for multicast filtering and IGMP Query mode, also support unknown multicast forwarding policies- Drop, Flooding and Forward to route port
Rate Control	Ingress/Egress filtering for Broadcast, Multicast, Unknown DA or All packets
Port Mirroring	On-line traffic monitoring on multiple selected target ports
Port Security	Only permit the Link partner which with predefined MAC address to access the Ethernet interface
DHCP	DHCP Client/Server with IP & MAC address binding, DHCP Relay Agent function and DHCP Server with Static port based IP assigned function
IEEE 802.1x	Port Based Network Access Control with EAPoL to permit or Deny interface access with Remote RADIUS Server authentication
Industrial Protocol	Modbus/TCP, Ethernet/IP

Network Redundancy	
Multiple Super Ring (MSR™)	New generation Korenix Ring Redundancy Technology, Includes Rapid Super Ring, Rapid Dual Homing, TrunkRing™, MultiRing™ , Super Chain™ and backward compatible with legacy Super Ring™
Rapid Dual Homing (RDH™)	Multiple uplink paths to one or multiple upper Switch, up to 256 Groups RDH Peer protection
TrunkRing™	Integrate port aggregate function in ring path to get higher throughput ring architecture
MultiRing™	Couple or multiple up to 10 Rapid Super Rings in one device, JetNet 5020G supports up to 8 100M rings and 2 Gigabit rings
Super Chain	It is new ring technology with flexible and scalability, compatibility, and easy configurable. The ring includes 2 types of node Switch – Border Switch and Member Switch
Rapid Spanning Tree	IEEE 802.1D-2004 Rapid Spanning Tree Protocol. Compatible with Legacy Spanning Tree and IEEE 802.1w
Multiple Spanning Tree	IEEE 802.1s Multiple Spanning Tree, each MSTP instance can include one or more VLANs, and also supports multiple RSTP deployed in a VLAN or multiple VLANs
ITU-T G.8032 ERPS	Support ITU-T G.8032 ERPS V1 single ring topology, and ERPS v2 multiple rings with ladder topology
Loop Protection	The Loop Protection prevents any network looping caused by RSTP and MSR ring topology change
Interface	
Enclosure Port	10/100Base-TX Fast Ethernet: 16 x RJ-45 10/100Mbps, Auto MDI/MDI-X, Auto Negotiation 1000Base-T Gigabit Ethernet: 4 x RJ-45 100Mbps/1000Mbps, Auto MDI/MDI-X, Auto Negotiation SFP Fiber: 4 x SFP combo with RJ-45 with hot-swappable, and support digital diagnostic monitoring (DDM) function for fiber communicates quality management. The SFP Interface supports 100Mbps, 1000Mbps Fiber Transceiver RS-232 Console: RJ-45 (8P8C) Power Connector: 4-Pin Removable Terminal Block DI/DO Connector: 4-Pin Removable Terminal Block
Cable	100Base-TX: 4-Pair UTP/STP Cat.5 Cable (Maximum 100Meters) 1000Base-T: 4-Pair UTP/STP Cat.5 Cable (Maximum 100Meters) Fiber: Refers to SFP Fiber Transceiver Specification
Diagnostics LED	10/100Mbps Port: Link/Active (Green on / Blinking), Full Duplex (Amber on)

	1000Mbps Port: Link/Active (Green on/ Blinking), Speed (1000Mbps link Amber on, 10/100Mbps link Amber off) Pwr: Power Ready (Green On) Sys: System Ready (Green On), System on booting/update (Green Blinking) DI/DO: Digital Input (RED On), Dry Relay Active (RED On) R.S.: Green on (Ring normal)/Blinking (wrong ring port connective), Amber on (Ring abnormal) / Blinking (device's ring port failed)
Power Requirement	
System Power	Redundant Power Input: DC 24V (typical); Input voltage range (10~60Vdc)
Power Consumption	10Watts/DC12V, 11Watts / DC24V, 14Watts/DC48V, 16Watts/DC60V
Mechanical	
Installation	EN50022 DIN Rail Mounting
Enclosure Material	Steel Metal with Aluminum
Ingress Protection	IP-30
Dimension (HxWxD)mm	160 (H) x 108 (W) x 127 (D) without DIN Rail Clip 160 (H) x 108 (W) x 136 (D) with DIN Rail Clip
Environmental	
Operating Temperature	-40°C~75°C
Operating Humidity	0%~90%, Non-Condensing
Storage Temperature	-40°C~80°C
Hi-Pot Insulation	AC 1.2KV for Ethernet Interface to Power, Power to Chassis Ground, Ethernet Interface to Chassis Ground
Approvals	
EMC	EMI: IEC/EN61000-6-2, EN55022 FCC Class A, CE Radiation, Conduction
	EMS: IEC/EN61000-6-4 IEC61000-4-2, IEC61000-4-3, IEC61000-4-4, IEC61000-4-5, IEC61000-4-6, IEC61000-4-8, IEC61000-4-9
Vibration	IEC 60068-2-6 : 10~150Hz,20m/S^2,20 Sweeps/Axis
Shock	IEC 60068-2-27: 50g_n,18ms,Half-Sine wave
Free Fall	IEC 60068-2-32: 1 corner, 3 line, 6faces
Warranty	5 Years

5.4 Revision History

Edition	Date	Modifications
V1.0	Feb. 28-2016	The 1st version.
V1.1	Mar, 02-2016	Modified safety information
V1.2	Jul, 07-2017	Add SFP speed commands at Chapter 4
V1.1	Nov. 23-2016	1. Page 6, Add Note 5: This product is intended to be supplied by an UL60950-1 listed Power Unit rated output rating: 9.6-60Vdc or 24Vdc, 1.0A minimum / Maximum ambient temperature is 55°C minimum. 2. Page 8, Add Note 2: To ensure safety, the optional transceiver should compliance with Class I Laser diode with UL certification and EN 60825-1 standard. 3. Page 45, Change JetNet 5420G to JetNet 5020G 4. Page 45, Remove SFP port 100M/1000M Auto Negotiation, Add step to set SFP port seed in CLI

5.5 About Korenix

Less Time At Work! Fewer Budget on applications!

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

Fusion of Outstandings

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

Core Strength---Competitive Price and Quality

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

Global Sales Strategy

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

Quality Services

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

5 Years Warranty

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

Korenix Technologies Co., Ltd.

Business service : sales@korenix.com

Customer service: koreCARE@korenix.com