Korenix
JetNet 6910G-M12 Series
Industrial Managed Ethernet Switch

User Manual

Manual v1.0

Aug, 2017

www.korenix.com

Korenix
JetNet 6910G-M12 Series
Industrial Managed Ethernet Switch

User Manual

Copyright Notice

Copyright © 2006-2017 Korenix Technology Co., Ltd.

All rights reserved.

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

Federal Communications Commission (FCC) Statement

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

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

Index

1 Introduction 2
1.1 Overview 2
1.2 Major Features 3
1.3 Package List 4
2 Hardware Installation 5
2.1 Hardware Introduction 5
2.2 Wiring Power Inputs 7
2.3 Wiring Earth Ground 7
2.4 Wiring PoE/Fast/Gigabit Ethernet Ports 7
2.5 Wiring RS-232 Console Cable 10
2.6 Bypass Fault Device in Daisy-Chain or Ring Topology 10
2.7 M12 USB Auto-Configuration 10
2.8 Wall Mounting Installation 11
2.9 Safety Warning 12
3 Preparation for Management 13
3.1 Preparation for Serial Console 13
3.2 Preparation for Web Interface 14
3.3 Preparation for Telnet Console 15
4 Feature Configuration 18
4.1 Command Line Interface Introduction 19
4.2 Basic Setting 24
4.3 Port Configuration 42
4.4 Power Over Ethernet 50
4.5 Network Redundancy 57
4.6 VLAN 75
4.7 Private VLAN 84
4.8 Traffic Prioritization 90
4.9 Multicast Filtering 95
4.10 SNMP 100
4.11 Security 104
4.12 Warning 113
4.13 Monitor and Diagnostic 118
4.14 Device Front Panel 133
4.15 Save (Save to Flash) 134
4.16 Logout 135
5 Appendix 136
5.1 Korenix Private MIB 136
5.2 Specification 136
5.3 Revision History 141

5.4 About Korenix 141

1 Introduction

Korenix JetNet 6910G-M12, Industrial 7 FE, + 3GbE and 8 PoE Managed High Power PoE Switch User Manual covers following topics in this chapter:

1.1 Overview

1.2 Major Features

1.3 Package Checklist

1.1 Overview

JetNet 6910G-M12, are specially designed for industrial environments in required support of medium number of access points or multiple Gigabit Ethernet ports. With fewer units installed and higher density of port numbers, the ports are sharing via the wide bandwidth on-chip backplane, in shorter local transmission latency, and sufficient upstream transmission.

JetNet 6910G-M12, the **7+3G Managed Ethernet Switch** is equipped with 7 10/100TX Fast Ethernet ports and 3 10/100/1000Base-T Gigabit Ethernet ports. 8 of 10 ports in JetNet 6910-M12 offer PoE in compliant with 802.3af/at. The Switch can resist in harsh environment in ranging operating temperature is from -40°C to 70°C.

Model Name	100TX FE	802.3af/at PoE	Gigabit Ethernet
JetNet 6910G-M12 **7+3G Managed Ethernet Switch**	7 (M12 D-4 female)	8 (on 7xM12 D-4, and 1xM12 X-8 female)	3 (M12 X-8, female)

The device is recommended to be wall-mount installed by using the installation kit within the shipment. When the other switches are aggregated to JetNet 6910G-M12, the 7+3G design allows total connections up to 5 rings, with owned ring redundancy protection. This is unique high-availability design featured base on Korenix patent-protected technology.

JetNet 6910G-M12 is a fan-less-designed M12 Power over Ethernet (PoE) Switch, with 100W PoE budget in compliance with IEEE 802.3af/at standard. The wide operating temperature, and dynamic DC input voltage meet the requirement in railway on-board electrical system..

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 MAC Security and IEEE 802.1x. By utilizing JetNet 6910G-M12, one can fulfill the technician's need by having best solutions for Industrial Ethernet Infrastructure.

1.2 Major Features

JetNet 6910G-M12 has following major features:

- 7 Fast Ethernet ports in M12 D-code , 3 Gigabit Ethernet ports in M12- X-code ,
- Power in M12-A, Console/USB port in M12-A
- Rugged M12 Ethernet, Power, Management connector to protect from vibration and shock application
- 8 IEEE 802.3at PSE allocated in 7 ports Fast Ethernet and 1 Gigabit Ethernet
- 2 Gigabit Ethernet interfaces support Device Fault Bypass function
- Railway Power System design with 100W PoE power and compliance with safety requirement
- Network Redundancy – MSR (Multiple Super Ring), ITU-T G.8032 ERPS, RSTP, MSTP, Super Chain
- Fully Device Management – SNMP v1/v2c/v3, RMON, Web UI, Telnet and Local Console
- Friendly Device and Network Topology recovery Utility – Korenix View, Korenix NMS
- Advanced Network Security –MAC Security, IEEE 802.1x Port Based access control , IEEE 802.1x Radius Server authentication
- Layer 2 Network Performance – IEEE802.1Q VLAN, Private VLAN, Trunk, Traffic Filtering, DHCP Server/Client, Traffic Prioritize, Forwarding Rate Control
- Real Hardware Watchdog against internal system malfunction
- Railway power system – 110V (77~137Vdc) JetNet 6910G-M12 HVDC

  24V (16.8~30Vdc) JetNet 6910G-M12 LVDC
- Railway Standards- EN50155, EN50121-3-2,IEC61373
- Operating Temperature: -40°C ~70°C
- Rigid Steel Metal Case complies with Ingress Protection – IP30

Note: Detailed spec can be referred to datasheet. For any possible change or update, please download the latest version for reference from Korenix Website.

1.3 Package List

JetNet 6910G-M12 Series products are shipped with following accessories:

1. JetNet 6910G-M12 x1
2. Mounting kits with screws
3. Serial Console cable, M12-A-8 to DB-9 x1
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

2.2 Wiring Power Inputs

2.3 Wiring Earth Ground

2.4 Wiring Fast Ethernet Ports

2.5 Wiring RS-232 console cable

2.6 Bypass Fault Device in Daisy Chain or Ring

2.7 M12 USB Auto-Configuration

2.8 Wall Mounting Installation

2.9 Safety Warning

2.1 Hardware Introduction

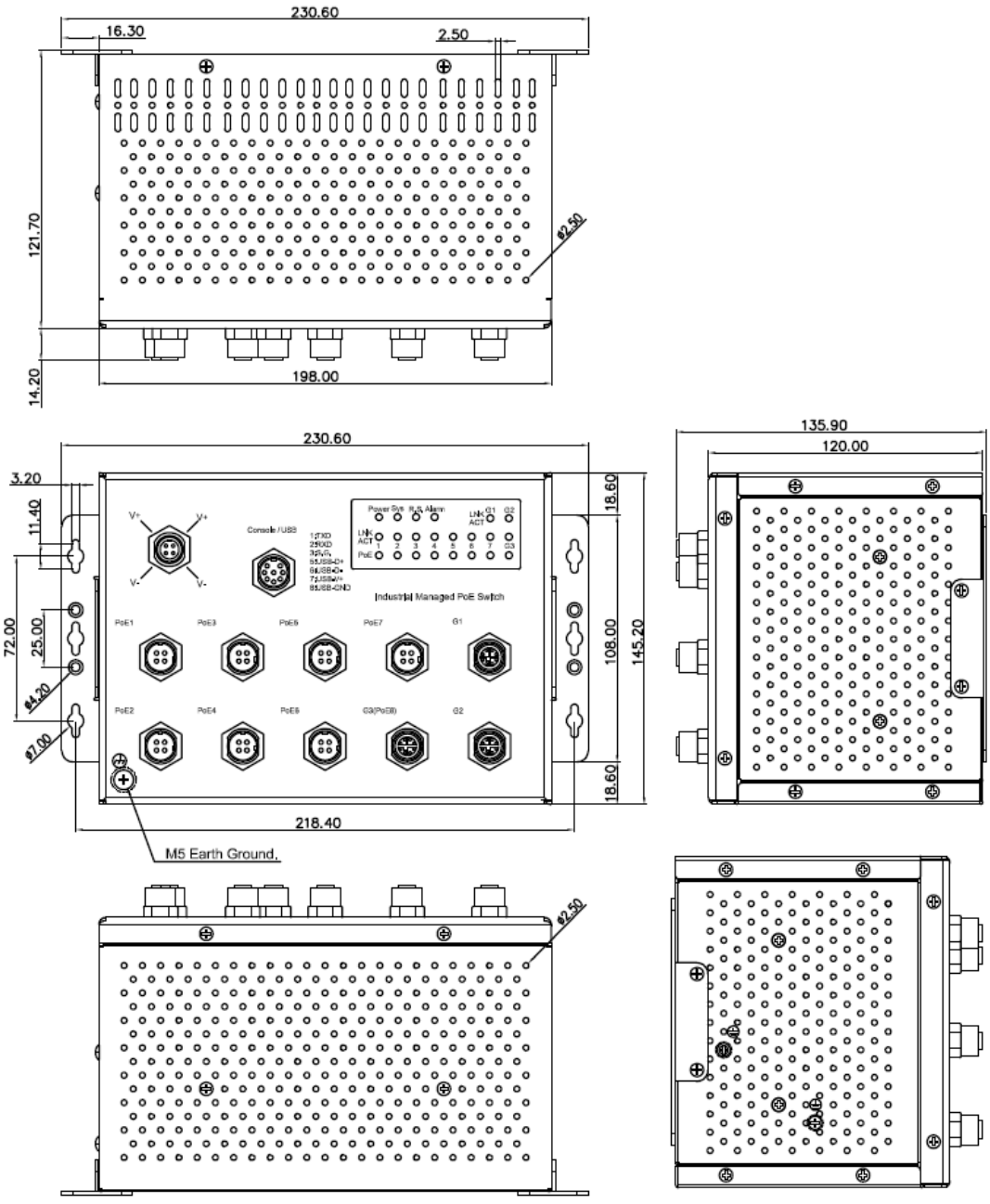
System Diagnostic LED

PWR (Power): Power Ready (Green On)
ALM (Alarm): Power/Data Port abnormal (Red On)
SYS (System): System Ready (Green On)
System on Booting/Upgrade (Green Blinking)
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 (PoE1~PoE7): Link/Active (Green on / Blinking),
Gigabit Ethernet (G1~G3): Link/Active (Green on/ Blinking)
PoE (PoE1~PoE7, G3(PoE8))
PoE (IEEE 802.3af/ Green): Power forwarding (Green on),
PoE Detection (Green Blinking)
PoE (IEEE 802.3at/ Blue): Power forwarding (Blue on),
PoE Detection (Blue Blinking)

Dimension (HxWxD) mm

145.2(H) x 198 (W) x 120 (D) without Bracket

145.2(H) x 230.6 (W) x 121.7 (D) with Bracket



Panel Layout

The front panel includes M12-based USB/Console Port, Fast/Gigabit Ethernet Port, Power and System/Port LEDs.

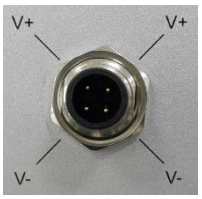
Figure of JetNet 6910G-M12, 7+3G Managed Ethernet Switch



2.2 Wiring Power Inputs

For DC power inputs.

1. Insert positive and negative wires into V+ and V- contacts respectively of the M12 connector (Plug-side).
2. Tighten the nuts to prevent the loosening of the M12 connectors.
3. PWR input supports power redundancy and polarity-reverse protection functions.



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.

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

Note 3: The connection of LVDC (24V) model should be dual input supplied to obtain higher enough current in order to perform high power PoE loading.

2.3 Wiring Earth Ground

To ensure the system not being damaged by noise or any electrical shock, it is strongly recommended to assure exact connection into JetNet 6910G-M12 with Earth Ground.

Ensure the lighting/surge enable screw is tightened when connect the Earth Ground.

2.4 Wiring PoE/Fast/Gigabit Ethernet Ports

JetNet 6910G-M12 includes **7 Fast Ethernet ports(#1~#7, M12 D-code)**, **3 M12**

Gigabit Ethernet ports(#8~#10, M12 X-code), and the PoE/ PSE function present at M12 D-Code Fast Ethernet port (#1~7) and M12 X-code Gigabit Ethernet port (#8).

The connectivity information of M12 and RJ-45 shown in below:

Fast Ethernet/ PoE ports, M12 D-code connector:

For Fast Ethernet M12 D-code to M12 D-code connection, you can use either version below:

Fast Ethernet - M12 D-Code 4-PIN, Female

Cat-6, Cat-7 Shielding Twisted Cable, 24~26AWG

Pin Assignment drawing	Pin	Description	PoE
	1	TX+	PoE V+ / P
	2	RX+	PoE V- / N
	3	TX-	PoE V+ / P
	4	RX-	PoE V- / N

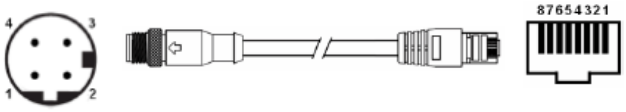




M12-M12 MDI				
1	TX+	———	RX+	1
2	RX+	———	TX+	2
3	TX-	———	RX-	3
4	RX-	———	TX-	4
M12-M12 MDI-X				
1	TX+	———	RX+	2
2	RX+	———	TX+	1
3	TX-	———	RX-	4
4	RX-	———	TX-	3

Picture 14 M12-to-M12 Ethernet Cable Wiring

For Fast Ethernet M12-code to RJ45 connection, the pin assignment of the patch cable is shown below:



M12-RJ45 MDI Straight Cable				
1	TX+	———	TX+	3
2	RX+	———	RX+	1
3	TX-	———	TX-	6
4	RX-	———	RX-	2
M12-RJ45 MDI-X cross over cable				
1	TX+	----------	RX+	1
2	RX+	----------	TX+	3
3	TX-	----------	RX-	2
4	RX-	----------	TX-	6

Picture 15 M12-to-RJ45 Ethernet Cable Wiring

Gigabit Ethernet ports, M12 X-code:

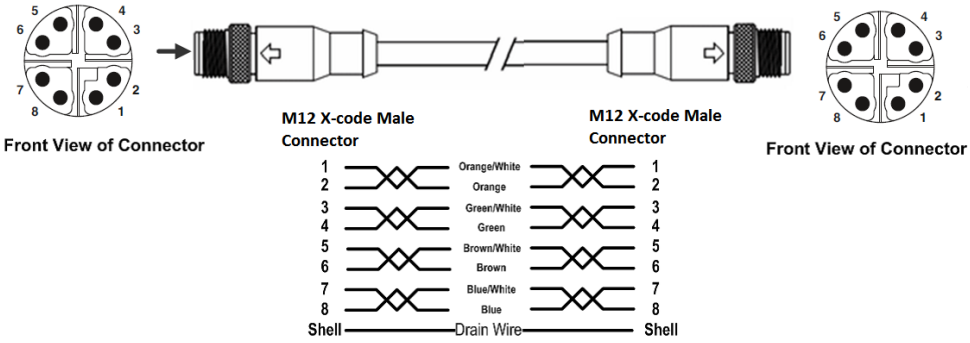


JetNet 6910G GbE - M12 X-Code 8-PIN, Female

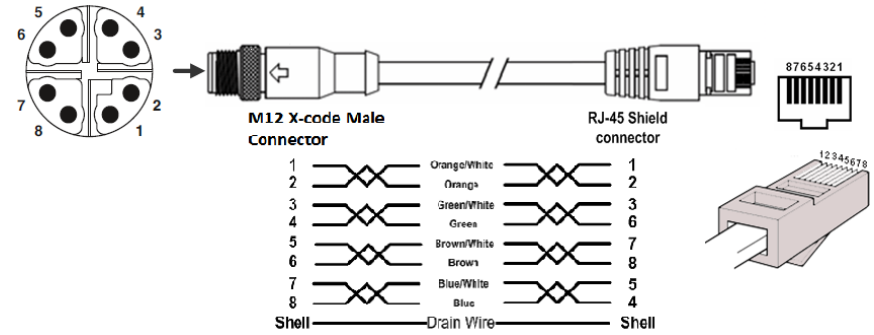
Cat-6, Cat-7 Shielding Twisted Cable, 24-26AWG

Pin Assignment drawing	Pin	Description	PoE
	1	Bidirectional (0)+	PoE V+ / P
	2	Bidirectional (0)-	PoE V+ / P
	3	Bidirectional (1)+	PoE V- / N
	4	Bidirectional (1)-	PoE V- / N
	5	Bidirectional (3)+	
	6	Bidirectional (3)-	
	7	Bidirectional (2)-	
	8	Bidirectional (2)+	

For Gigabit Ethernet M12 X-code to M12 X-code connections, the pin assignment of the patch cable is shown below:



For Gigabit Ethernet M12 X-code to RJ45 connection, the pin assignment of the patch cable is shown below:



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).

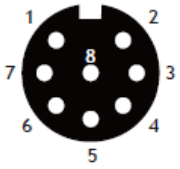
2.5 Wiring RS-232 Console Cable

JetNet 6910G-M12 attached one RS-232 DB-9 to M12-A cable in the unit box. Connect the DB-9 connector to the COM port of your PC, connect M12-A to Switch's USB/Console port, 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.



Console/ USB Backup Port - M12 A-Code 8 PIN, Female

RS-232 Console

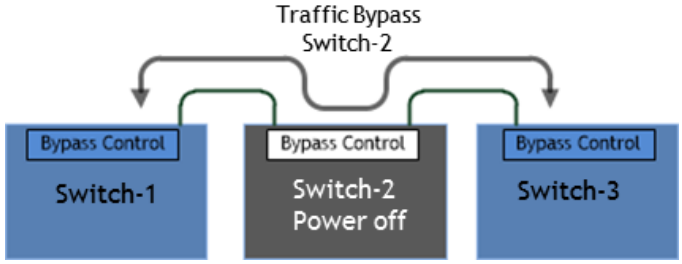
Pin Assignment drawing	Pin	Description
	1	RS232_TX
	2	RS232_RX
	3	RS232_GND
	4	N/A
	5	USB Data+
	6	USB Data-
	7	USB power (5V)
	8	USB Ground

Note: If the cable is lost, please contact with your sales or follow the pin assignment to buy a new one.

2.6 Bypass Fault Device in Daisy-Chain or Ring Topology

Auto-bypass function has been applied on G1 and G2 for rolling stock applications. In the metro or ring network, the topology may be segmented into several fractions by one failure power node. As a result, some of the segments or nodes cannot communicate with each other. The port Bypass function can connect remote network fragments by linking uplink and downlink ports together when the Switch is powered down. With this feature, the Switch can ensure that train communication always works appropriately.

2.7 M12 USB Auto-Configuration



The JetNet 6910G has enabled USB memory access function for the configuration restore/backup. The function brings benefits to the field engineers maintaining/upgrading the system without special tools or configuration knowledges. The system kernel will automatically restore the desired configuration if the configuration files existing in the M12/USB memory stick with specified file name. It also makes the on-field Ethernet Switch replacement/ exchange process easy and friendly.

1. The Max length of the configuration file name: 40 characters

2. The configuration file Naming rules and respective detection behavior as below

(a)Name: **AutoLoadSaveConfiguration.conf** Auto load the Configuration existed in the

USB and save the configuration to the Ethernet Switch memory and apply the new configuration into system when boot up.

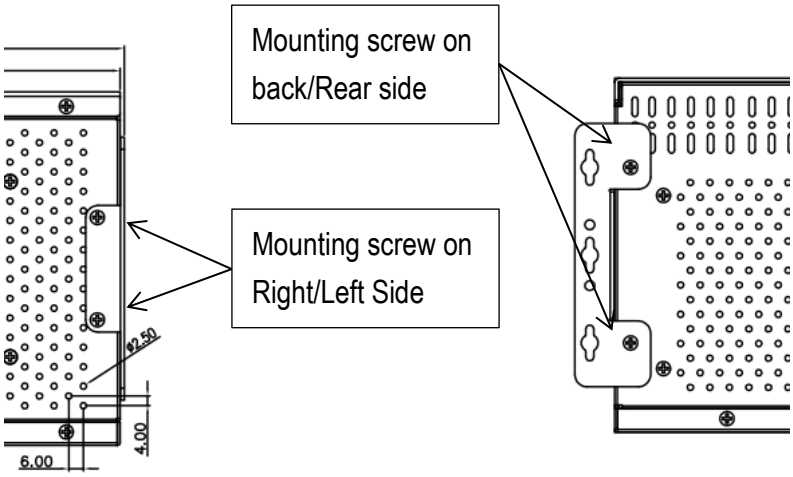
(b)Name: **AutoLoadConfiguration.conf** Auto Load Configuration and apply the configuration to Ethernet Switch without saving to memory.

(c)If both files exist in the USB, then the **AutoLoadSaveConfiguration.conf** has the higher priority and will perform Auto load and saving actions.

2.8 Wall Mounting Installation

Follow the steps below to install JetNet 6910G-M12 with the wall-mounting plate.

1. Install the wall-mounting plate onto the side panel of the switch.
2. Makes sure that all the screws are tightened well.
3. Use the hook holes at the corners of the wall mounting plate to fix the switch on the wall.



Wall Mounting Plate & Screws

2.9 Safety Warning

The Equipment intended for installation in a Restricted Access Location.



Restricted Access Location:

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

This Ethernet Switch is intended for Railway/Train on-board application. Thus, all of the installation should be performed by professional Engineer who is familiar Train communication and electrical power system.

3 Preparation for Management

JetNet 6910G-M12 Din Rail Industrial Managed Switch provides both in-band and out-band configuration methods. It is possible to configure the device via RS232 console cable if there's not an admin PC attached in the network to manage JetNet 6910G-M12. This console connectivity via RS232 port is a way called out-band management. It wouldn't be affected by network performance.

The in-band management in this manual refer the way of remotely managing 6910G-M12 via a remote PC attaching in the network. Telnet or Web-based GUI are provided for management. The device's IP address is required before remotely connecting 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 6910G-M12 package, Korenix attached one RS-232 M12 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 6910G-M12. 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 6910G-M12 is as below:

   Baud Rate: 9600 / Parity: None / Data Bit: 8 / Stop Bit: 1
5. After connected, Switch login request is expected seen on the screen.
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:

JetNet6910G-M12
  (version 0.0.21-20160118-11:00:03).
Copyright 2006-2017 Korenix Technology Co., Ltd.

Switch>
```

3.2 Preparation for Web Interface

JetNet 6910G-M12 provides HTTP Web Interface and Secured HTTPS Web Interface for web management.

Web Interface

Korenix web management GUI page is developed by JAVA or *CGI. It allows to use a standard web-browser such as Microsoft Internet Explorer, or Mozilla, Chrome to configure and interrogate the switch from anywhere on the network in the same domain.

*Note: Contact sales representative or check Korenix website for CGI GUI availability.

Before you attempt to use the embedded web interface to manage switch operation, verify that your JetNet 6910G-M12 is properly installed on your network and that every PC on this network can access the switch via the web browser.

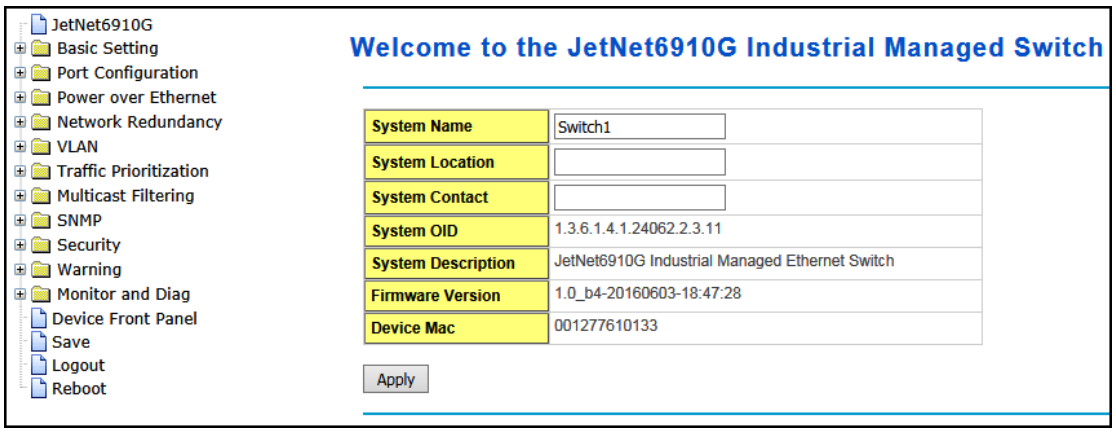
1. Verify that your network interface card (NIC) is operational, and that your operating system supports TCP/IP protocol.
2. Wire DC power to the switch and connect your switch to your computer.
3. Make sure that the switch default IP address is 192.168.10.1.
4. Change your computer IP address to 192.168.10.2 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, Google Chrome or Mozilla Firefox) on the PC.
7. Type **http://192.168.10.1** (or the IP address of the switch). And then press **Enter**.
8. The login screen will appear next.
9. Key in user name and the password. Default user name and password are both **admin**.



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



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

Note : The Web UI connection session of Managed Switch will be logged out automatically if you don't give any input after 10 minutes. After logged out, you should re-login and key in correct user name and password again.

3.3 Preparation for Telnet Console

3.3.1 Telnet

Korenix JetNet 6910G-M12 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 6910G-M12 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.

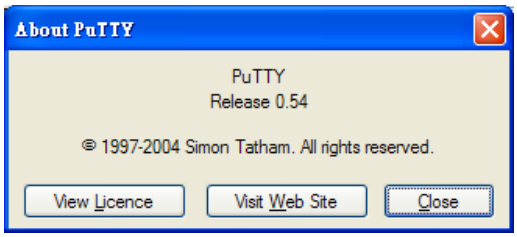
SSH is a client/server architecture while the Managed Switch is the SSH server. When you want to make SSH connection with the switch, you should download the SSH client tool first.

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*.

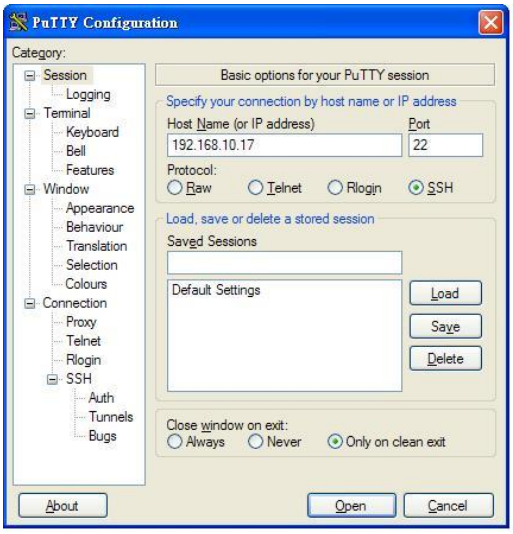
Download PuTTY: http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

The copyright of **PuTTY**

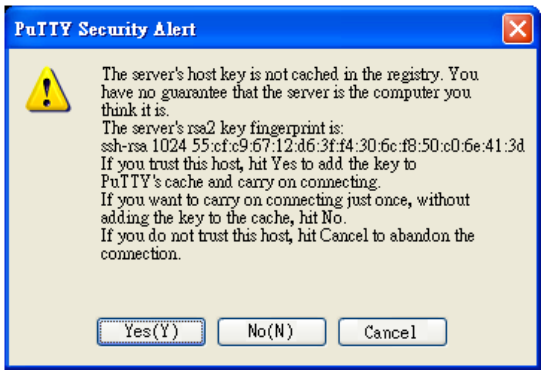


1. Open SSH Client/PuTTY

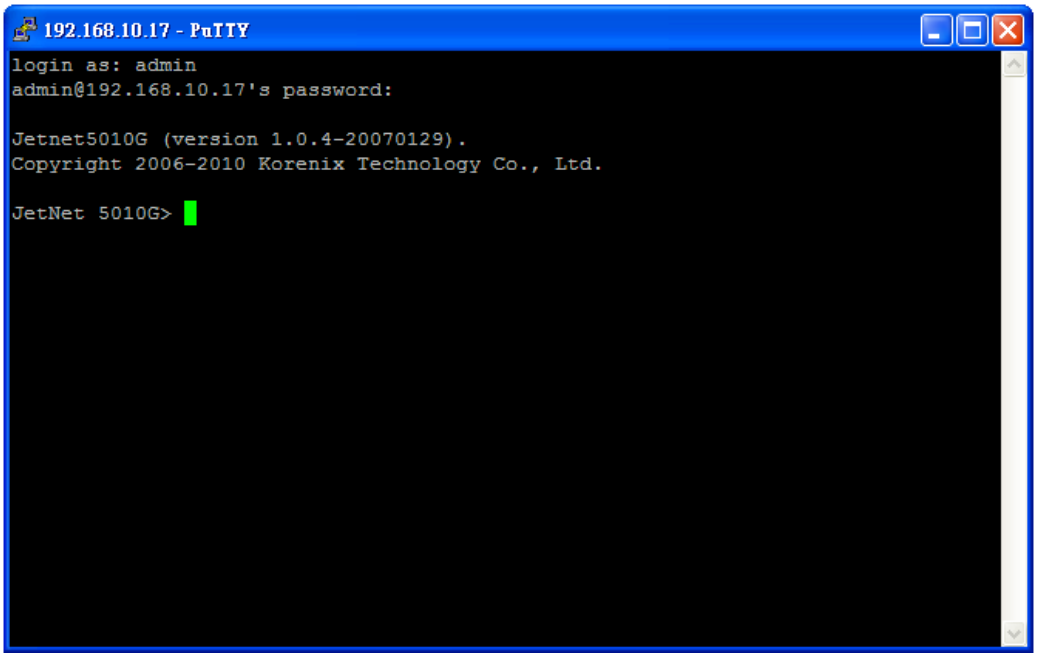
In the **Session** configuration, enter the **Host Name** (IP Address of your JetNet 6910G-M12) and **Port number** (default = 22). Choose the "**SSH**" protocol. Then click on "**Open**" to start the SSH session console.



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



3. After few seconds, the SSH connection to JetNet 6910G-M12 is opened. You can see the login screen as the below figure. (the following is refer to 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. The connectivity of both in-band and out-band is described in previous chapter.

Assign the device an IP address, then this switch can be remotely connected and managed via its embedded HTML web pages or Telnet console.

The Web management page can be shown at a standard web-browser such as Microsoft Internet Explorer, or Mozilla, Chrome to configure and interrogate the switch from anywhere on the network.

Following topics are covered in this chapter:

4.1 Command Line Interface (CLI) Introduction

4.2 Basic Setting

4.3 Port Configuration

4.4 Power Over Ethernet

4.5 Network Redundancy

4.6 VLAN

4.7 Private VLAN

4.8 Traffic Prioritization

4.9 Multicast Filtering

4.10 SNMP

4.11 Security

4.12 Warning

4.13 Monitor and Diagnostic

4.14 Device Front Panel

4.15 Save

4.16 Logout

4.1 Command Line Interface Introduction

The Command Line Interface (CLI) is the user interface to the switch's embedded software system. An network administrator can view the system information, show the status, configure the switch and receive a response back from the system by input a CLI 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 administrator login the switch by CLI. it is in the User EXEC mode. Administrator 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"** command in the User EXEC mode, then administrator can transit into the Privileged EXEC mode. In this mode, the system allows 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. Adminstrator can then enter global configuration mode. In global configuration mode, administrator can configure all the features that the system provides.

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. Administrator can then enter interface configuration mode. In this mode, administrator 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.

The port interface name of the Gigabit Ethernet port is gi<Port Number>. Ex: Gigabit Ethernet Port 8 is gi8, Gigabit Ethernet Port 17 is gi17. Even you apply fixed 100M speed to the Gigabit Ethernet port, the port interface name is still gi<Port Number>.

Types interface name accordingly for going to 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 to see the possible, available commands for use.

```
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 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
```

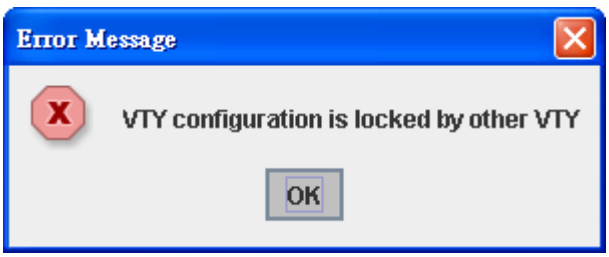
Ctrl+C To stop executing the unfinished command.

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.



4.2 Basic Setting

The Basic Setting group provides the way 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

It can be assigned System name, Location, Contact and view system information.

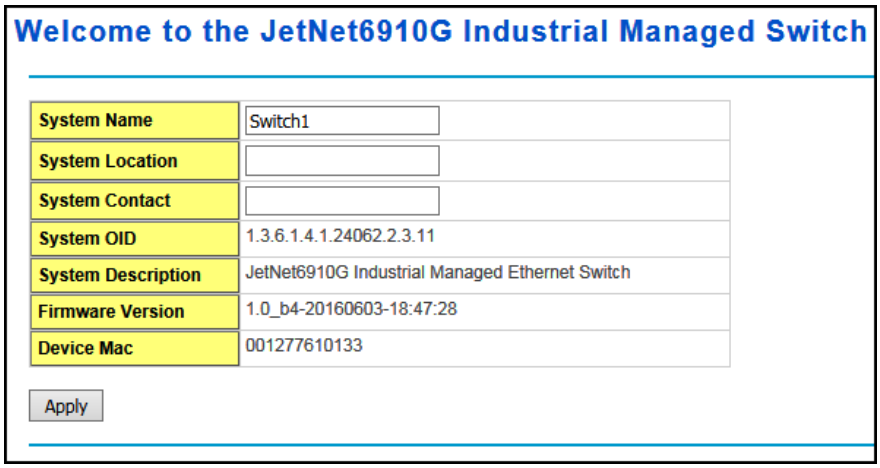


Figure 4.2.1.1 – Web UI of the Switch Setting

System Name: Administrator can assign a name to the device. The available character string length is 64. After configuring the name, CLI system will select the first 12 characters as the name in CLI system.

System Location: Administrator can specify the switch's physical location here. The available character string length is 64.

System Contact: Administrator can specify contact people here. Administrator 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. Administrator can follow the path to find its private MIB in MIB browser. (**Note:** When administrator attempt to view private MIB, yit's required to compile private MIB files into the MIB browser first.)

System Description: JetNet6910G-M12 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.

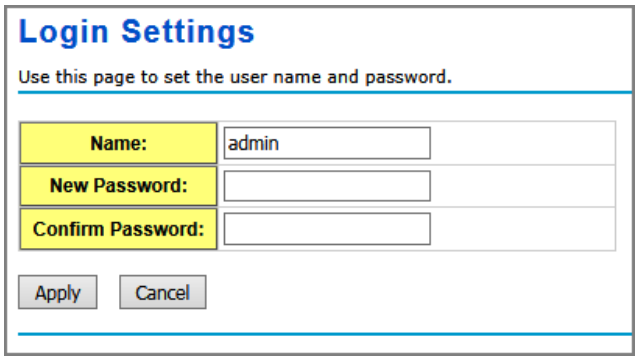
Once the configuration is finished, click on **Apply** to apply for taking settings effective.

Note: Always remember to select **Save** to save all the settings. Otherwise, the settings made can be lost when the switch is powered off.

4.2.2 Admin Password

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

Figure 4.2.2.1 Web UI of the Admin Password



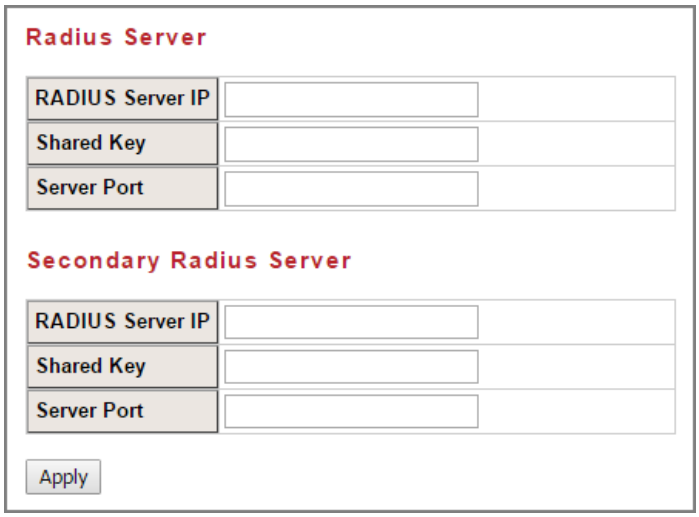
User name: Administrator can key in new user name here. The default setting is **admin**.

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

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

Once configuring the settings is finished, click on **Apply** to apply configuration in effective.

Administrator can use RADIUS server's user name and password for your management security.

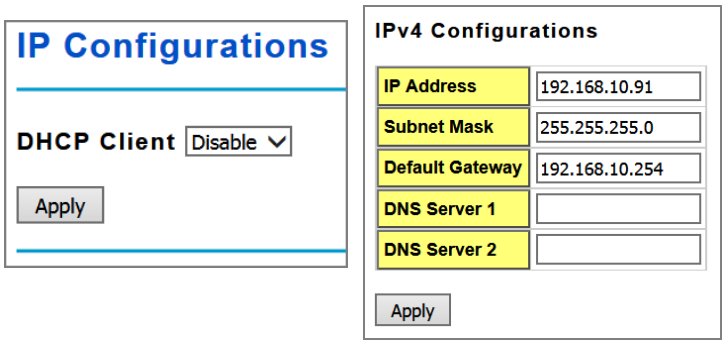


RADIUS Server IP: The IP address of the RADIUS server.

Shared Key: The password for communication between the switch and the RADIUS Server.

Server Port: UDP port of the RADIUS server.

Apply: button to apply the RADIUS Server and Secondary RADIUS Server configurations.



4.2.3 IP Configuration

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

DHCP Client: Administrator 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: Administrator can assign the IP address reserved by the network applied for the JetNet 6910G-M12 being deployed. If DHCP Client function is enabled, it is not necessary to assign an IP address to the JetNet 6910G-M12, as it will be overwritten by DHCP server and shown here. The default IP address is 192.168.10.1.

Subnet Mask: Administrator can/shall assign a correct subnet mask for the IP address here. If DHCP Client function is enabled, it is not necessary to assign the subnet mask. The default Subnet Mask is 255.255.255.0. **Note:** In the CLI, the enabled bit of the subnet mask is used 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: Administrator 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 Administrator finish configuring the settings, click on **Apply** to apply configuration into effective.

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 6910G-M12 is generated from hardware MAC by IEEE-defined 64-bit Extended Unique Identifier (EUI-64), so that each JetNet 5020 owns her

identical default IPv6 address. (ex: 00:12:77:FF:88:88 -> fe80::212:77ff:feff:8888)

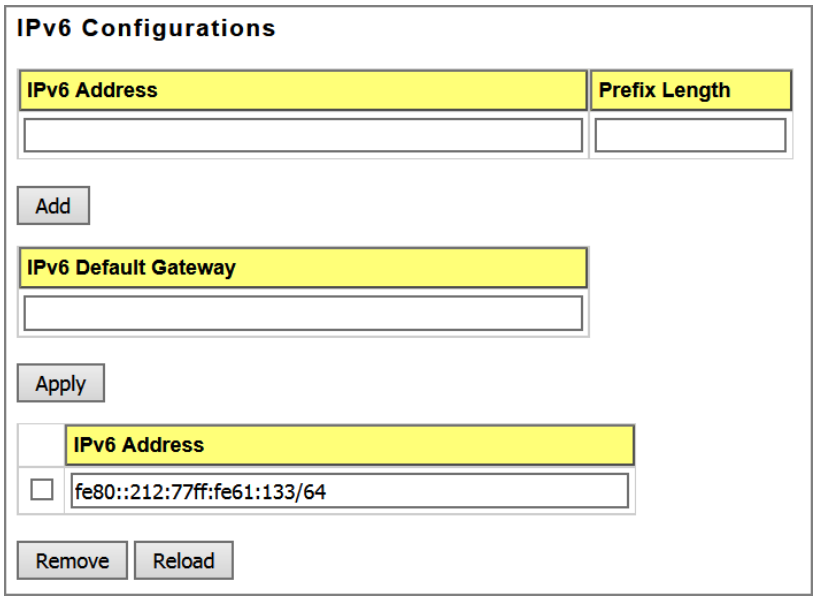
IPv6 Address: a new IPv6 address can be assigned in this field.

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.

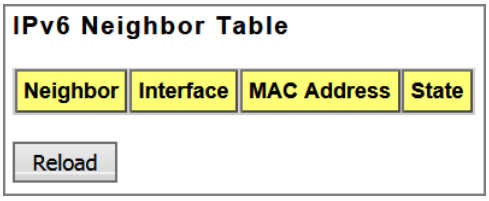
Add: after adding new IPv6 address and prefix, do not forget to click icon -"**Add**" to apply new address to the system.

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.



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. An administrator 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.

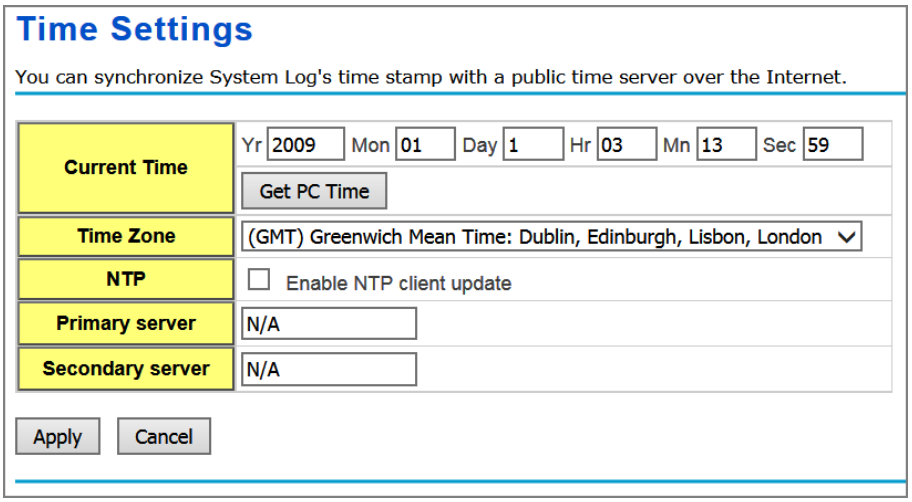
*Note: Please enable one synchronization protocol (PTP/NTP) only.

JetNet 6910G-M12 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.

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 PC Time**".. 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

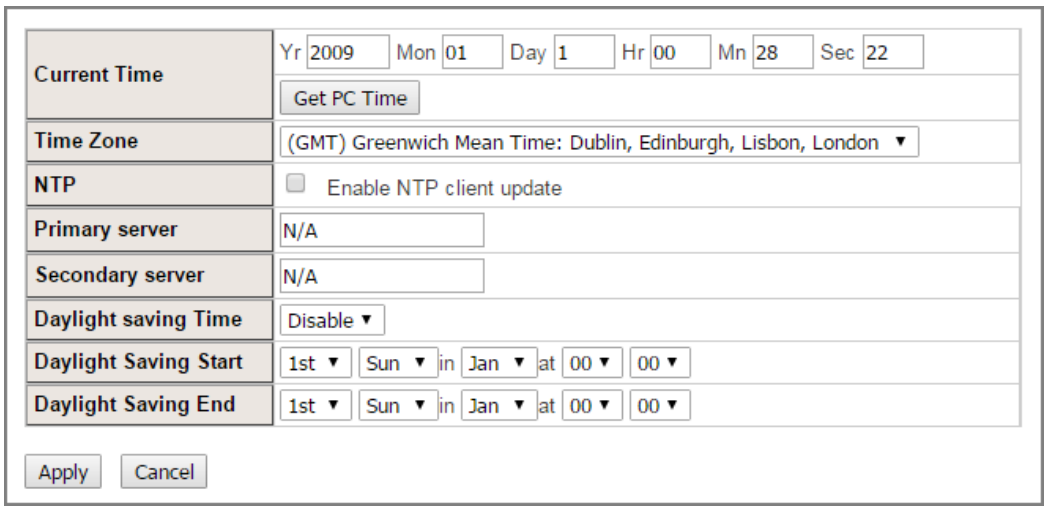
24 (GMT-01:00) Cape Verde Is.
25 (GMT) Casablanca, Monrovia
26 (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
27 (GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
28 (GMT+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague
29 (GMT+01:00) Brussels, Copenhagen, Madrid, Paris
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 function 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 Time source is changed to NTP

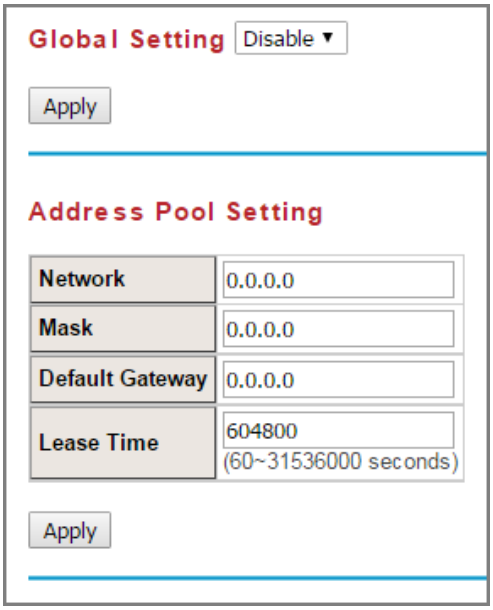


Client. The system will send request packet to acquire current time from the NTP server that the administrator assigned.

4.2.5 DHCP Server

You can select to **Enable** or **Disable** DHCP Server function. JetNet 6910G-M12 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 the configuration

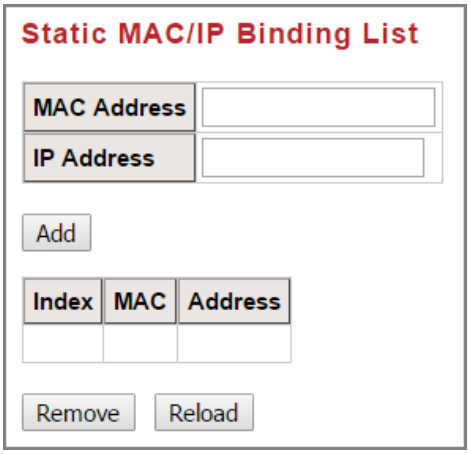
Excluded Address:

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

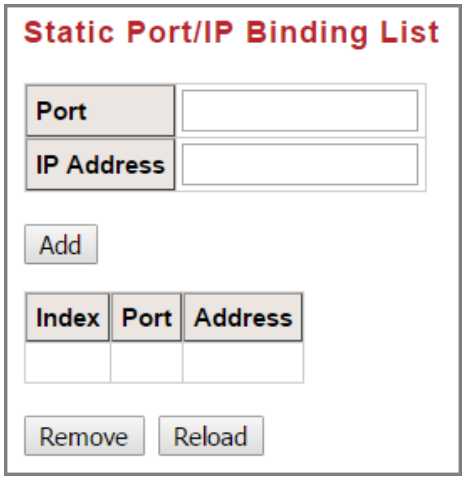


The IP address that is listed in the **Excluded Address List Table** will not be assigned to the network device. Add or remove an IP address from the **Excluded Address List** by clicking **Add** or **Remove**.

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 6910G-M12 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.

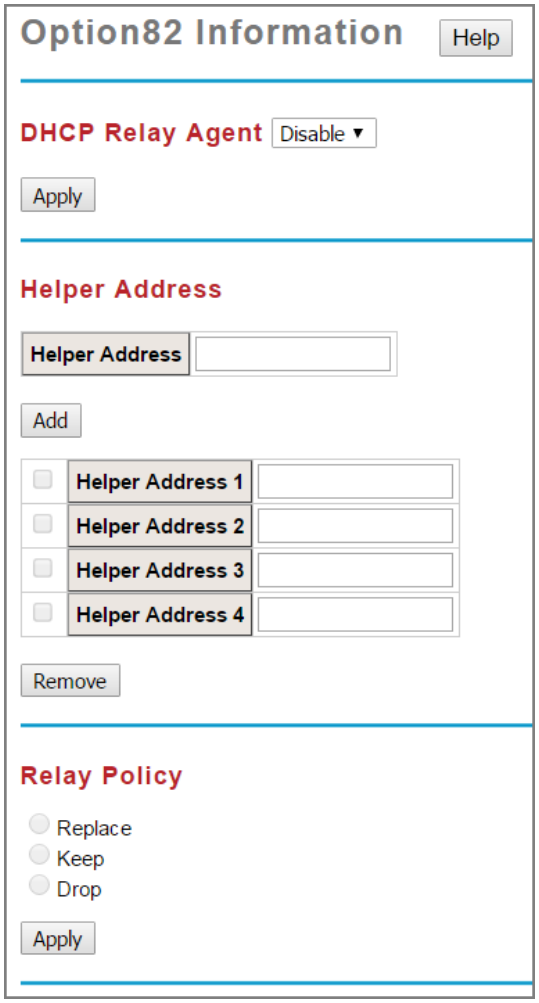
DHCP Leased Entries: JetNet 6190G-M12 provides assigned IP address list for user reference. It will show the MAC and IP address assigned by *6910G-M12*. Click the **Reload** button to refresh the list.

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 Option82: Administrator 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.

4.2.6 Backup and Restore

With Backup command, an administrator can save current configuration file saved in the switch's flash to admin PC or TFTP server. This will allow administrator to go by **Restore** command later to restore the configuration file back to the switch. Before restoring the configuration file, it is required to place the backup configuration file in the PC or TFTP server. The switch will then download this file back to the flash from restored location.

There are 3 modes for users to backup/restore the configuration file, the Local File mode, USB 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 back up the configuration. Users can also browse the target folder and select existed configuration file to restore the configuration back to the switch. Note that this mode is only provided in Web UI, CLI is not supported.

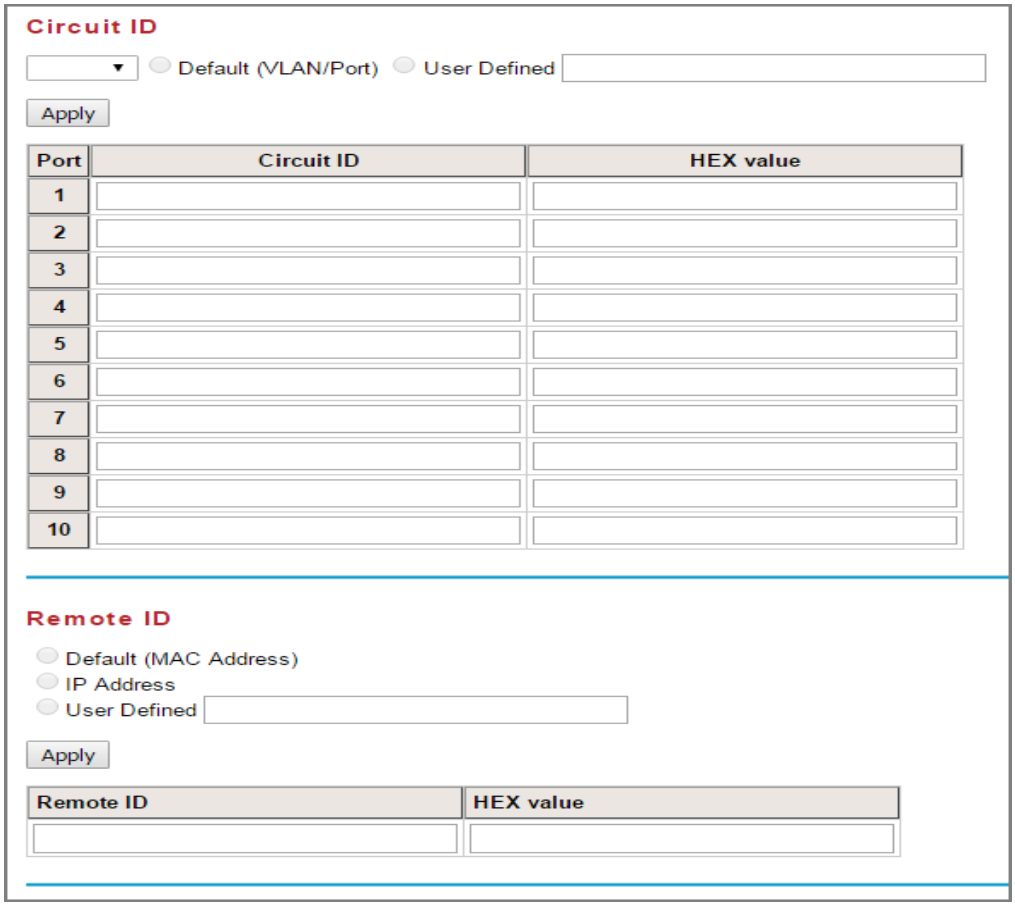
USB mode: In this mode, the switch acts as USB control viewer. By plugging the USB storage into the switch, select the file to Backup configuration file name, or to Restore Configuration. This mode can be used in both CLI and Web UI. Please select the file to Backup configuration file name, or to Restore Configuration.

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: the IP address of TFTP Server is required to fill up 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 format file. It can be



openned by text editor to read the file. Administrator can also modify the file, add/remove the configuration settings, and then restore back to the switch.

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

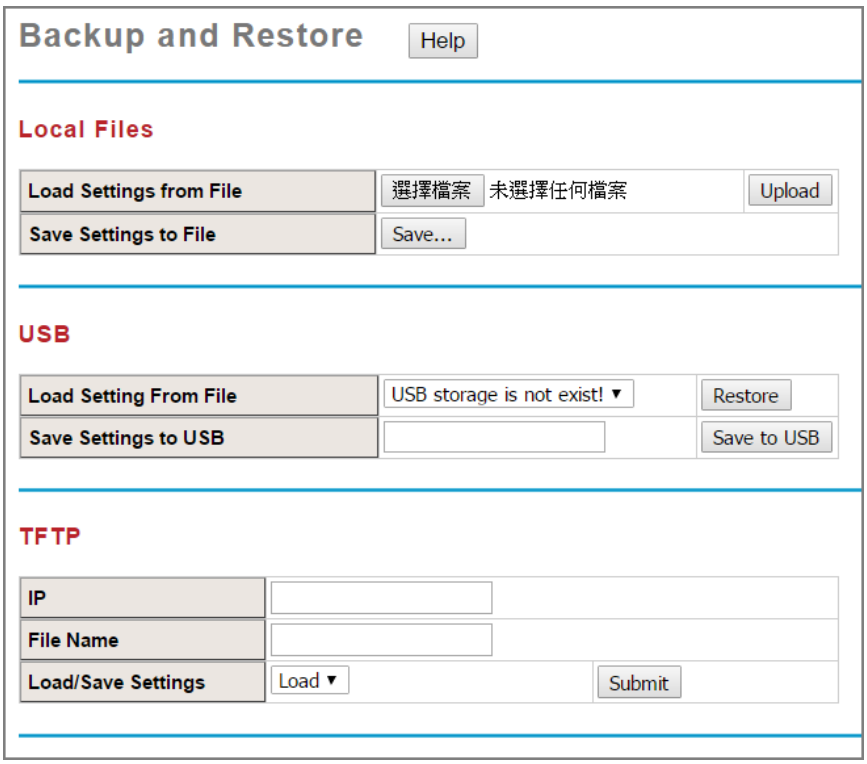
To activate the configuration after power reboot, **"Save to Flash" is a Must command**. Please check the description in Ch4.14

> ***Technical Tip:***
>
> ***Default Configuration File:*** *The switch provides the default configuration file in the system. Reset button, or "Reload" command can be used to reset the system.*
>
> ***Running Configuration File:*** *The switch's CLI allows viewing 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 selecting and configuring the settings are done, click on **Backup** or **Restore** to run

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

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



4.2.7 Firmware Upgrade

In this section, an administrator can update the latest firmware for the switch. Korenix provides the latest firmware at Korenix Web site. The new firmware may include new features, bug fixes or other software changes. The release notes is along with the update as well. For technical viewpoint, it is recommended to apply the latest firmware before installing the switch to the field and site.

Note that the system must be rebooted after upgrading the new firmware. Please remind relevant users whose nodes are attached on the switch before reboot the switch.

There are 3 modes for users to backup/restore the configuration file: Local File mode, USB 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.

USB mode: In this mode, the switch acts as USB control viewer. Before you do so, make sure that your USB already inserted into the switch. Then please select the file to Backup configuration file name, or to Restore Configuration. This mode can be used in both CLI and Web UI. FW upgrade in USB mode: please select the firmware file name, then type the upgrade button to upgrade the firmware. It will start the firmware upgrade process.



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

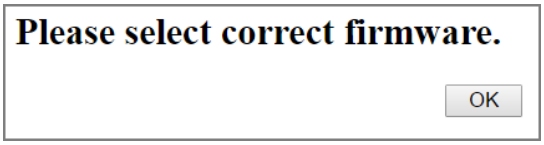
TFTP Server IP Address: The IP address of TFTP Server here.

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

Warning Message.



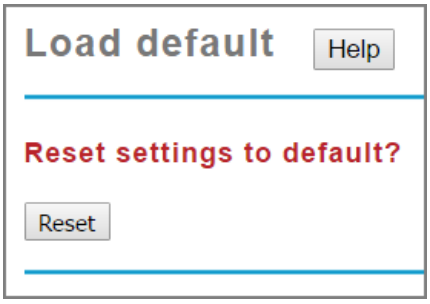
Error Message due to the file error or not a firmware for the switch.



Before upgrading firmware, please assure that the firmware specific is for JetNet 6910G-M12. The switch provide protection when an incorrect firmware file is being upgraded, the system crash would not be expected by an incorrect firmware being updated. There's protection to warning "not trying" to install the incorrect firmware to JetNet 6910G-M12. Unexpected events may occur and cause damage to the system.

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.

4.2.8 Load Default



In this section, an administrator 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 pop up message in a window after this command is accepted by the switch. Default setting will work effectively after rebooting the switch.

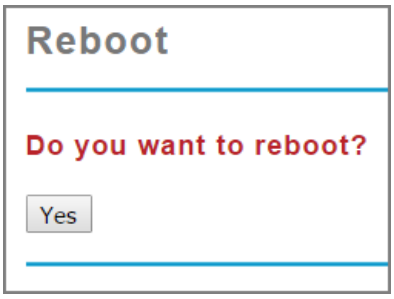
Click on **Reset.** The system will then auto reboot the device.

Note: If the IP address of target switch has been configured, using this "Reset" command by CLI and Web UI won't reset the switch IP address to default IP address. The switch system will record and remain the original configured IP address to be taken effectively after re-boot, so that the switch on the network doesn't have to be re-configured and re-discovered.

4.2.9 System Reboot

System Reboot allows to reboot the switch when 're-boot required' appears at some of the features selected or changed. Click on **Reboot** to reboot the switch.

Caution: *Remember to click on* ***Save*** *button to save your settings before "Reboot" command. Otherwise, the settings made will not be saved when the switch is powered off.*





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

4.2.10 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 6910G-M12 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 : JetNet6910G-M12
	  Serial Number : 123412412
	  MAC Address : 001277FF8888
	  Manufacturing 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 6910G-M12, 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.
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	Switch# copy startup-config tftp: 192.168.10.33/default.conf Writing Configuration [OK]

Configuration file	***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
Backup Startup Configuration file from USB	Switch# copy startup-config usb CONFIGURATION Confiuration file
Restore Configuration file from USB	Switch# copy usb CONFIGURATION Configuration file
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 JN6910G-M12.bin Firmware upgrading, don't turn off the switch! Tftping file JN6910G-M12.bin Firmware upgrading .... Firmware upgrade success!! Rebooting.....
Firmware Upgrade from USB	Switch# archive download-sw /overwrite usb IMAGE Image file
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 setting of switch ports, including port state enable/disable, auto-negotiation, speed, duplex, flow control, rate limit control and port aggregation settings. The port status and aggregation information can be also achieved.

Following commands are mentioned in this chapter :

4.3.2 Port Control
4.3.3 Port Status
4.3.4 Rate Control
4.3.5 Port Trunking
4.3.6 Command Lines for Port Configuration

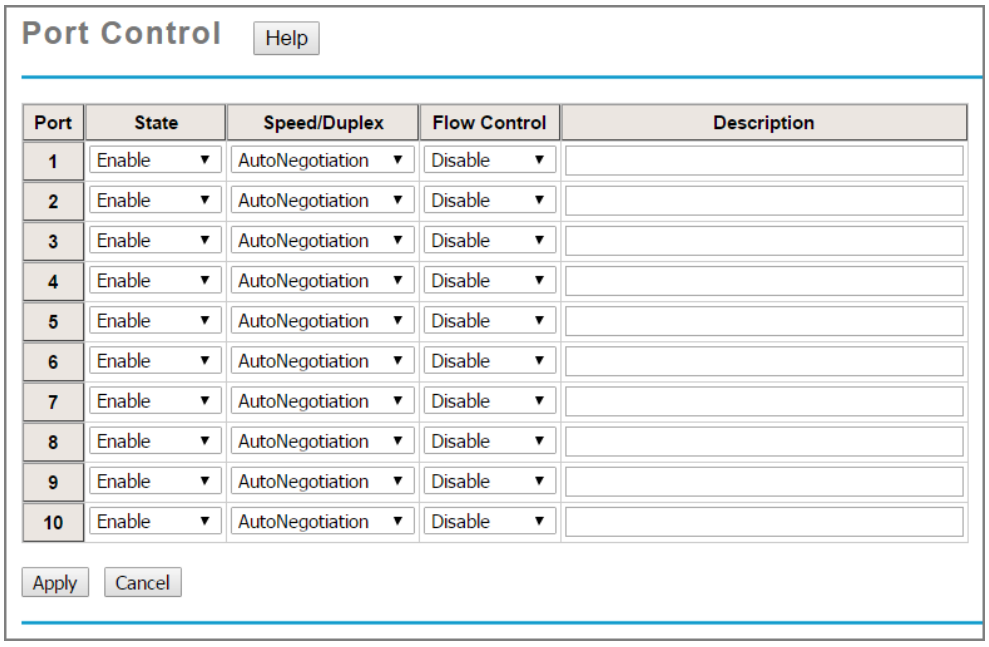
4.3.1 Understand the port mapping

Before the port setting, please check the port allocation of JetNet 6910G-M12 before deployment. The port number is indicated as printing number on the front panel. Follow the port ID to configure JetNet 6910G-M12.

There are 7 Fast Ethernet ports and 3 Gigabit Ethernet ports. In Web UI, the port number is available from port 1~10, Port 1~7 represents Fast Ethernet ports, and Port 8~10 are referred for Gigabit Ethernet ports. In CLI, fa1, fa2…fa7 represent Fast Ethernet ports and gi8, gi9… gi10 represent Gigabit Ethernet ports.

4.3.2 Port Control

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



Select the port being configured 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 all the ports are taken in functional upon transmission and receiving.

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

Fast Ethernet Port 1~7 (fa1~fa7): AutoNegotiation, 10Mb Full Duplex(10 Full), 10Mb Half Duplex(10 Half), 100Mb Full Duplex(100 Full) and 100Mb Half Duplex(100 Half).

Gigabit Ethernet Port 8~10 (gi8~gi10): AutoNegotiation, 100Mb Full Duplex(100 Full), 100Mb Half Duplex(100 Half), 1000Mb Full Duplex(1000 Full), 1000Mb Half Duplex(1000 Half).

The default is recommended and set to Auto Negotiation mode.
For speed determination of SFP operation, same speed setting must be applied at both ends of the ports connection as it is not covered with AutoNegotiation clause of 802.3 standard.

In **Flow Control** column, in order to enable flow control, **"Symmetric"** strategy on both ends of the ports connection must be both applied on local and remote devices, correspondingly. If **"Disable"** is set on ONLY either one end, it is incomplete for the flow control working appropriately. It is recommended to leave the flow control under Auto Negotiation mode.

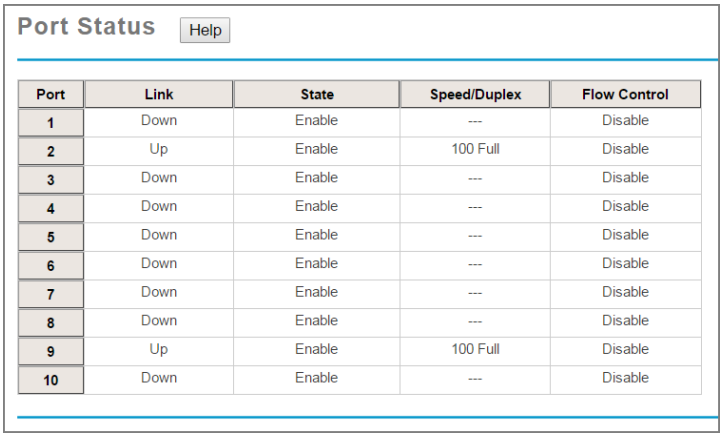
In **Description** column, description can be added to indicate the port location, connected device or other information. This is a friendly design especially in remote management of the devices.

Once the configuration is completed, 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.



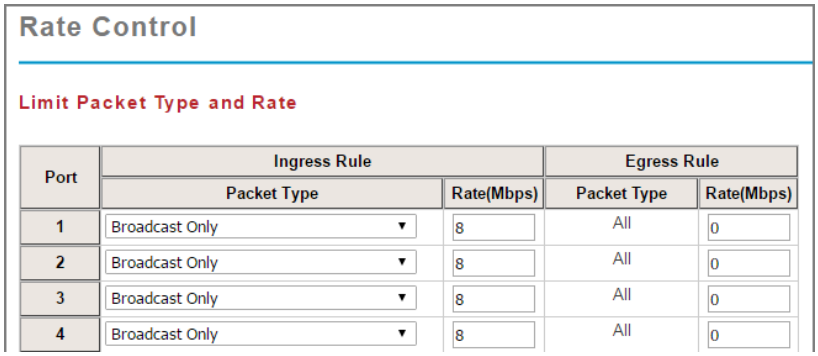
Port	Link	State	Speed/Duplex	Flow Control
1	Down	Enable	---	Disable
2	Up	Enable	100 Full	Disable
3	Down	Enable	---	Disable
4	Down	Enable	---	Disable
5	Down	Enable	---	Disable
6	Down	Enable	---	Disable
7	Down	Enable	---	Disable
8	Down	Enable	---	Disable
9	Up	Enable	100 Full	Disable
10	Down	Enable	---	Disable

The description of the columns is as below:
Port: Port interface number.
Type: 100BASE-TX -> Fast Ethernet copper port. 1000BASE-T -> Gigabit Ethernet Copper port.
Link: Link status. Up -> Link UP. Down -> Link Down.

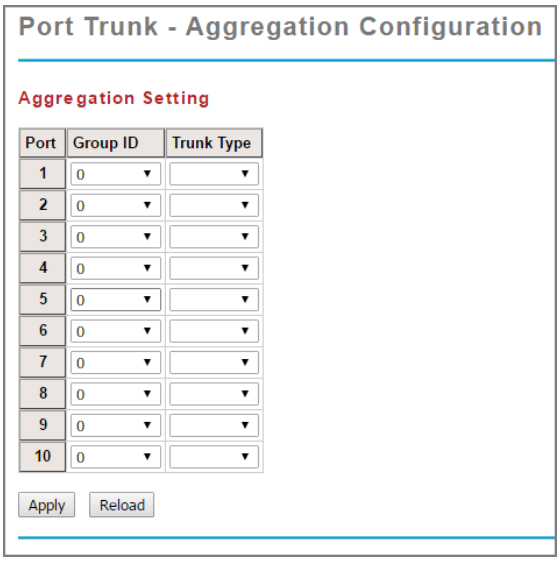
State: Enable -> State is enabled. Disable -> The port is disable/shutdown.
Speed/Duplex: Current working status of the port.
Flow Control: The state of the flow control.

4.3.4 Rate Control

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



4.3.5 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 for the need of higher bandwidth for a backbone network. This is an inexpensive way for higher transferring data needed.

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 802.3ad standard.

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, it **should** be assigned the same 802.3ad LACP to the trunk. When the other end uses non-802.3ad, it can be then applied the Static Trunk. **In practical, the Static Trunk is suggested.**

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

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.

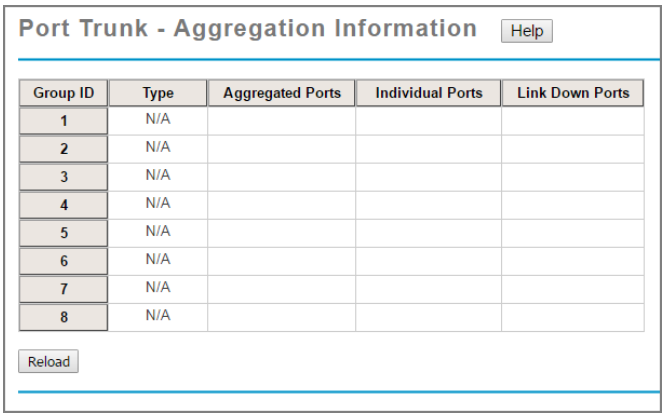
LACP Timeout: The LACPDU is generated and continue transmit within the LACP group. The interval time of the LACPDU Long timeout is 30 sec, this is default setting. The LACPDP Short timeout is 1 sec, the command to change from Long to Short is only applied to the CLI, the web GUI doesn't support this. 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.

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.



4.3.6 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!
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. *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 Power Over Ethernet

Power over Ethernet is one of the key features of JetNet 6910G-M12. It is fully IEEE802.3af-2003 compliant, and support IEEE802.3at, including 1-event with IEEE 802.1AB LLDP classification for PoE MDI signaling. The JetNet 6910G-M12 adopts 8-Port PoE injectors from port 1 to port 8, each port with the ability is able to deliver 30W power per IEEE 802.3at 2-event plus LLDP function. Note that: the total power output budget for JetNet 6910G-M12 shall be limited within 100W at 70˚C ambient temperature.Detail calculation and verification to total PDs power consumption required from JetNet6910G-M12 before deployment is highly recommended.

The following commands are included in this section:

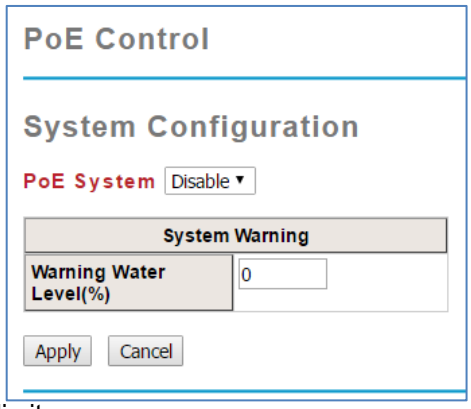
4.4.1 PoE Control

4.4.2 PoE Scheduling

4.4.3 PoE Status

4.4.4 Command Line for PoE control

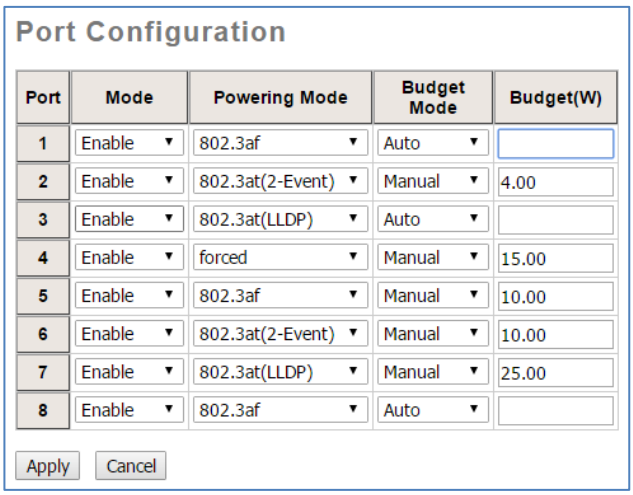
4.4.1 PoE Control



PoE System: Enable/Disable PoE Internal power system.

Power Budget (W): The JetNet 6910G-M12 predefined power budget is 100W without any change; therefor the power source must offer and satisfy the system power inquires- 120W at least, includes Ethernet Switch system consumption.

Warning Water Level (%): setting the power consumption warning water level. With the event warning enabled, the system will send warning information to NMS if power consumption is over the limit.



Port Configuration: it includes PoE mode selection, Powering mode, Power Budget mode selection and power budget setting for the Power budget manual mode.

PoE mode: includes per port PoE En/disable and control by scheduling.

Powering mode: includes 802.3af, 802.3at (2-Event), 802.3at (LLDP) and forced mode. If forced mode is selected, the port power budget value will need to be filled specifically to activate PoE force mode effectively.

Power Budget mode: it supports 2 selections- Auto and Manual. The manual mode is for user defined power budget to be set and beyond 802.3af/at PD's declaration.

Power Budget: the limit of per port PoE output. Without the value, the PoE forced mode

powering will not be activated.

Note: During the PoE operating, the surface will accumulate heat and caused surface temperature becomes higher than ambient temperature. Do remember don't touch device surface during PoE operating.

Note: To enable the IEEE 802.3at High Power PoE function, the power input voltage is required to be larger than DC 54V to obtain better performance. Applies voltage lower than DC 54V to PoE Switch but connecting to a PD in performing 30W high power output may cause the PoE function of the switch to be disabled automatically, due to the OCP (output current protect) mechanism is activated (0.686A current is design as OCP design). To avoid this issue, it is required a professional engineer to adjust the power supply output to 54V DC, by setting variable resistor equipped in the switching power supply.

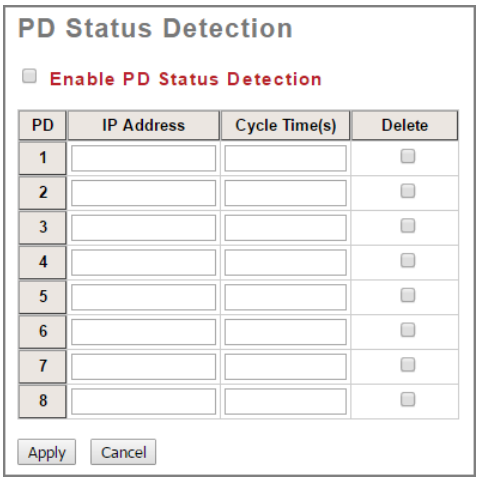
For the JetNet 6910G-M12 series, the internal DC/DC output voltage is required DC 54V at minimum; so the a lower value in "power budget" may not impact when a high DC 110V input is presented.



DO NOT TOUCH DEVICE SURFACE DURING PoE PROGRESS HIGH POWER FEEDING

PD Status Detection (Link Partner Line Detect)

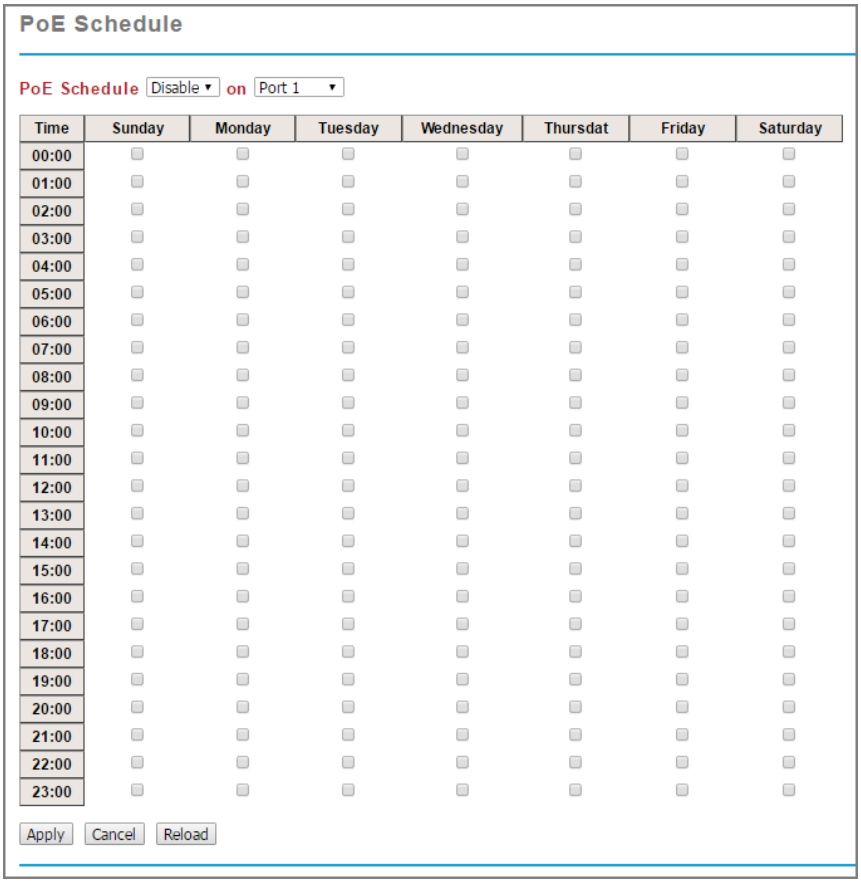
JetNet 6910G-M12 delivers a convenient function – PD Status Detection. This provides automatic detection of a remote device powered by JetNet 6910G-M12. If the remote system crashes or is unstable, JetNet PoE Switch will perform a remote system reboot by turning off and on again to trigger the remote device. The following figure shows the Web configure interface for Power over Ethernet PD Status Detection.



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

4.4.2 PoE Scheduling

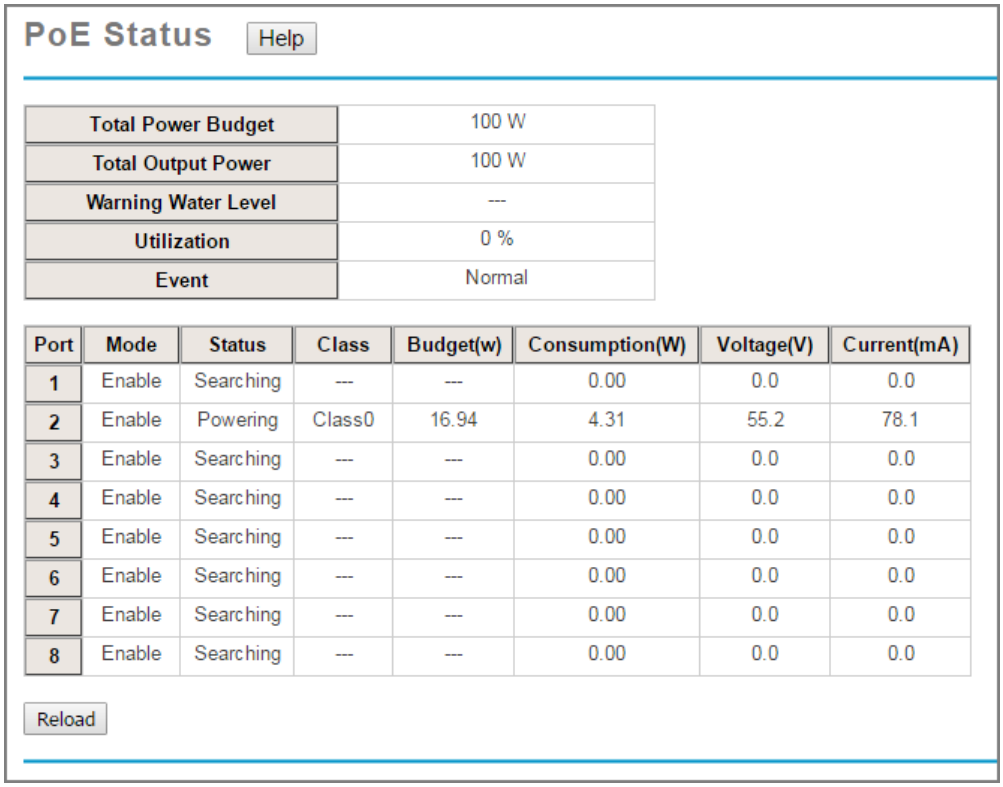
The PoE Scheduling control is a powerful function to help you save power and money. Administrator can configure **PoE Scheduling** with selecting a target port manually to enable this function.



The Power over Ethernet schedule supports hourly and weekly base PoE schedule configuration. Select the target port and marking the time frame, then click **Apply** to activate the PoE scheduling function. The PoE port will working as the predefined behavior and follows the system clock. As this result, be sure the system clock have configured as the local time for the reference of scheduling control.

4.4.3 PoE Status

The PoE Status page shows the operating status of each PoE Port. The information includes PoE mode, Operation status, PD class, Power Consumption, Voltage and Current.



4.4.4 Command Line for PoE Control

Syntax	**show poe system**
Parameters	--
Command Mode	Enable mode
Description	Display the status of the PoE system.
Examples	Switch> enable Switch# show poe system PoE System PoE Admin : Enable PoE Hardward : Normal Ouput power : 0.0 Watts Power Budget : Budget: 100 Watts Warning water level : N/A Utilization : 0 % Event : Normal
Syntax	**show poe interface** IFNAME
Parameters	IFNAME : interface name
Command Mode	Enable mode
Description	Display the PoE status of interface.
Examples	Switch> enable Switch# show poe interface fa1 Interface fastethernet1 (POE Port 1) Control Mode : User (Disable) Powering Mode : 802.3af

	Operation Status : Off Detection Status : Valid Classification : N/A Priority : Highest Output Power : 0.0 Watts, Voltage : 0.0 V, Current : 0 mA Power Budget : Budget : 32.0 Watts, effective 0 Watts Warning water level : N/A Utilization : 0 % Event : Normal
Syntax	**show poe pd_detect**
Parameters	--
Command Mode	Enable mode
Description	Display the status of pd status detection.
Examples	Switch# show poe pd-detect PD Status Detection Status : Enabled Host 1 : Target IP : 192.168.10.100 Cycle Time : 10 Host 2 : Target IP : 192.168.10.200 Cycle Time : 20 Host 3 : Target IP : 192.168.10.15 Cycle Time : 30 Host 4 : Target IP : 192.168.10.20 Cycle Time : 40
Syntax	**show poe schedule IFNAME**
Parameters	IFNAME : interface name
Command Mode	Enable mode
Description	Display the status of schedule of interface.
Examples	Switch# show poe schedule fa1 Interface fastethernet1 POE Schedule Status : Disable Weekly Schedule : Sunday : 0,1,2,3,4,5,6,7,8,19,20,21,22,23 Monday : 0,1,2,3,4,5,6,7,8,19,20,21,22,23 Tuesday : 0,1,2,3,4,5,6,7,8,19,20,21,22,23 Wednesday : 0,1,2,3,4,5,6,7,8,19,20,21,22,23 Thursday : 0,1,2,3,4,5,6,7,8,19,20,21,22,23 Friday : 0,1,2,3,4,5,6,7,8,19,20,21,22,23 Saturday : 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20
Syntax	**poe powering-mode 802.3af/forced**
Parameters	802.3af: deliver power if and only if the attached PD comply with IEEE 802.3af forced: deliver power no maater what PD attached
Command Mode	Interface mode
Description	Set the Powring mode of PoE

Examples	EX 1: *Set 802.3af powring mode* Switch(config)# poe powering-mode 802.3af EX 2: *Set forced powering mode* Switch(config)# poe powering-mode forced
Syntax	**poe powering-mode 802.3at 2-event/lldp**
Parameters	2-event: deliver power if and only if the attached PD comply with IEEE 802.3at physical layer classification lldp: deliver power if and only if the attached PD comply with IEEE 802.3at data link layer classification
Command Mode	Interface mode
Description	Set the Powering mode of PoE
Examples	EX 1: *Set 802.3at 2-event powering mode* Switch(config)# poe powering-mode 802.3at 2-event EX 2: *Set 802.3at lldpforced powering mode* Switch(config)# poe powering-mode 802.3at lldp
Syntax	**poe control-mode user/schedule**
Parameters	user: user mode schedule: schedule mode
Command Mode	Interface mode
Description	Set the control mode of port
Examples	Set PoE port 2 to user mode. E X 1: Switch(config)# interface fa2 Switch(config-if)# poe control-mode user Set PoE port 2 to schedule mode. EX 2: Switch(config-if)# poe control-mode schedule
Syntax	**poe user enable/disable**
Parameters	ena ble: enable port in user mode disa ble: disable port in user mode
Command Mode	Interface mode
Description	Enable/Disable the PoE of the port in user mode. If in schedule mode, it will come into affect when the control mode changes to user mode.
Examples	To enable the PoE function in user mode Switch(config-if)# poe user enable To disable the PoE function in user mode Switch(config-if)# poe user disable
Syntax	**poe type TYPE**
Parameters	T PE : port type string with max 20 characters
Command Mode	Interface mode
Description	Set the port type string.
Examples	Set the type string to “IPCam-1. Switch(config-if)# poe type IPCam-1
Syntax	**poe budget [POWER]**
Parameters	PO ER : 0.4 – 32
Command Mode	Interface mode
Description	Set the port budget. The max budget is different between 802.3af, 802,3at and

	forced powering mode. The max budget of 802.3af powering mode is 15.4. The max budget of 802.3at powering mode is 32. The max budget of force powering mode is 32.
Examples	Set the max value of power consumption to 12 W with manual mode. Switch(config-if)# poe budget 12
Syntax	**poe budget warning <0-100>**
Parameters	<0-100> 0 is disable, valid range is 1 to 100 percentage
Command Mode	Interface mode
Description	Set the warning water level of port budget.
Examples	Set the warning water level to 60% Switch(config-if)# poe budget warning 60
Syntax	**poe priority critical/high/low**
Parameters	Critical : Hightest priority level High : High priority level Low : Low priority level
Command Mode	Interface mode
Description	Set the powering priority. The port with higher priority will have the privilege to delivery power under limited power situation.
Examples	Set the priority to critical Switch(config-if)# poe priority critical
Syntax	**poe schedule weekday hour**
Parameters	Weekday : Valid range 0-6 (0=Sunday, 1=Monday, …, 6=Saturday) Hour : Valid range 0-23, Valid format a,b,c-d
Command Mode	Interface mode
Description	Add a day schedule to an interface.
Examples	Add a schedule which enables PoE function at hour 1, 3, 5 and 10 to 23 on Sunday. Switch(config-if)# poe schedule 0 1,3,5,10-23
Syntax	**no poe schedule** weekday
Parameters	Weekday : Valid range 0-6 (0=Sunday, 1=Monday, …, 6=Saturday)
Command Mode	Interface mode
Description	Remove a day schedule
Examples	Remove the Sunday schedule. Switch(config-if)# no poe schedule 0
Syntax	**poe budget DC1/DC2 [POWER]**
Parameters	DC1 : DC 1 power input DC2 : DC 2 power input PO ER : 1 – 400
Command Mode	Configuration mode
Description	Set the power budget of DC1 or DC2
Examples	Set the power budget of DC1 to 400W Switch(config)# poe budget DC1 400
Syntax	**poe budget warning <0-100>**
Parameters	<0-100> 0 is disable, valid range is 1 to 100 percentage

Command Mode	Configuration mode
Description	Set the warning water level of total power budget.
Examples	Set the warning water level to 60% Switch(config-if)# poe budget warning 60
Syntax	**poe pd_detect enable/disable**
Parameters	enable: enable PD Status Detection function disable: disable PD Status Detection function
Command Mode	Configuration mode
Description	Enable/Disable the PD Status Detection function
Examples	To enable the function of pd status detect function Switch(config)# poe pd_detect enable To disable the function of pd status detect function Switch(configf)# poe pd_detect disable
Syntax	**poe pd_detect ip_address cycle_time**
Parameters	IP address : A.B.C.D Cycle time : Valid range 10-3600 second and must be multiple of 10
Command Mode	Configuration mode
Description	Apply a rule of PD Status Detection.
Examples	Apply a rule which ping 192.160.1.2 per 20 seconds. And if 192.160.1.2 is timeout, pd status detection will re-enable the PoE. Switch(config)# poe pd_detect 192.160.1.2 20

4.5 Network Redundancy

It is critical to build up a high-availability network for industrial applications. Korenix developed several standards (STP, RSTP and MSTP) and patented redundancy protocol - Multiple Super Ring, to achieve the network redundancy protection.

JetNet 6910G-M12 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 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 in copper connectivity.

A single 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 6910G-M12* to connect with a core managed switch easily and conveniently. With RDH technology, coupling several Rapid Super Rings or RSTP cloud together is possible.

Following commands are included in this group:

4.5.1 STP Configuration

4.5.2 STP Port Configuration

4.5.3 STP Information

4.5.4 MSTP Configuration

4.5.5 MSTP Port Configuration

4.5.6 MSTP information

4.5.7 Multiple Super Ring

4.5.8 Multiple Super Ring Information

4.5.9 Loop Protection

4.5.10 Command Lines for Network Redundancy

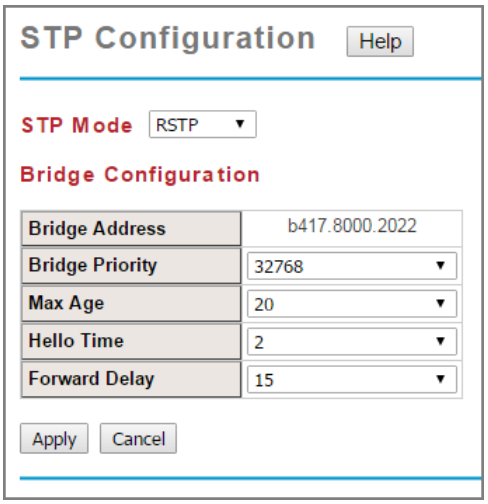
The STP Configuration, STP Port Configuration and STP Information pages are available while select the STP and RSTP mode.

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

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

4.5.1 STP Configuration

This page 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 to select the STP mode, configure the global STP/RSTP/MSTP settings.

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.

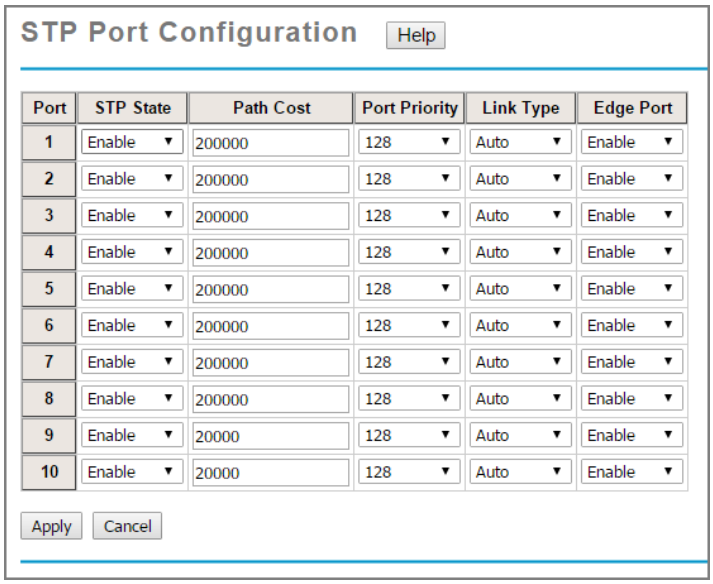
Once configuration setting is completed, click on **Apply** to apply your settings.

Caution: The rule to configure Hello Time, Forwarding Delay, and Max Age parameter, is highly recommended to follow.

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

4.5.2 STP Port Configuration

To configure the port parameter, it is required that STP or RSTP is enabled and taken effectively.



Port Configuration

Select the port being configured then current settings and status of the port are visible on the screen.

Path Cost: Enter a number between 1 and 200,000,000. This value of the path "cost" **is** the shortest path of the port selected to the root bridge. The slower the interface, the higher the cost is. The path with the lowest cost will be used to reach the root bridge.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.

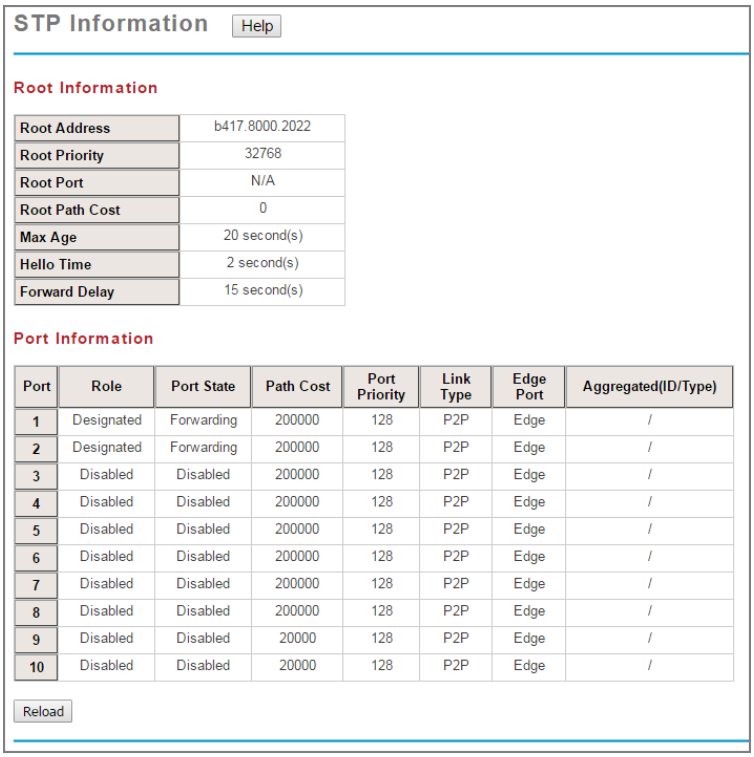
Once you finish your configuration, click on **Apply** to save your settings.

4.5.3 RSTP Info

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

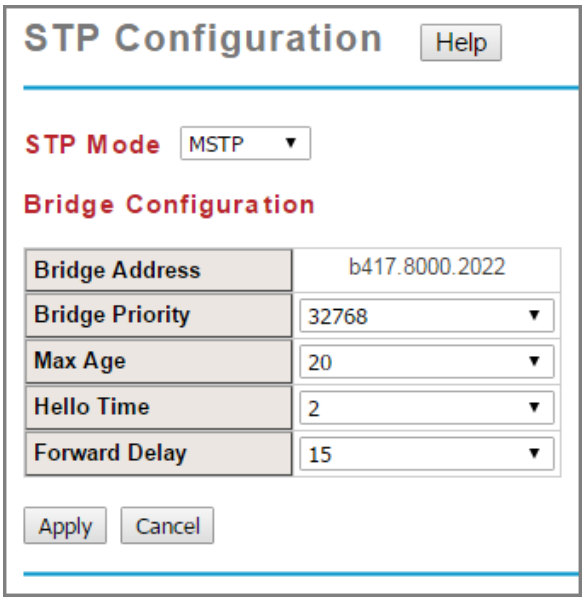
Root Information: You can see root Bridge ID, Root Priority, Root Port, Root Path Cost and the Max Age, Hello Time and Forward Delay of BPDU sent from the root switch.

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



4.5.4 MSTP (Multiple Spanning Tree Protocol) Configuration

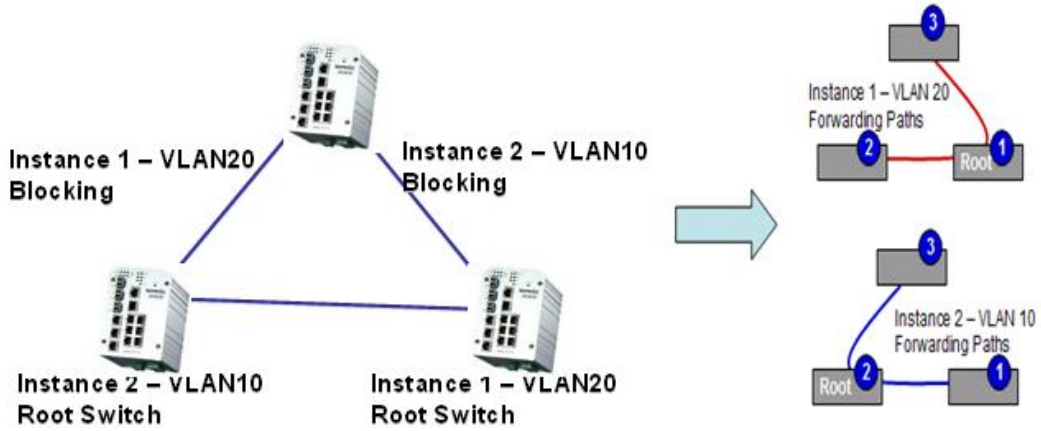
MSTP is the abbreviation of Multiple Spanning Tree Protocol. This protocol is a direct extension of RSTP. It can provide an independent spanning tree for different VLANs. It simplifies network management, provides for even faster convergence than RSTP by limiting the size of each region, and prevents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



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

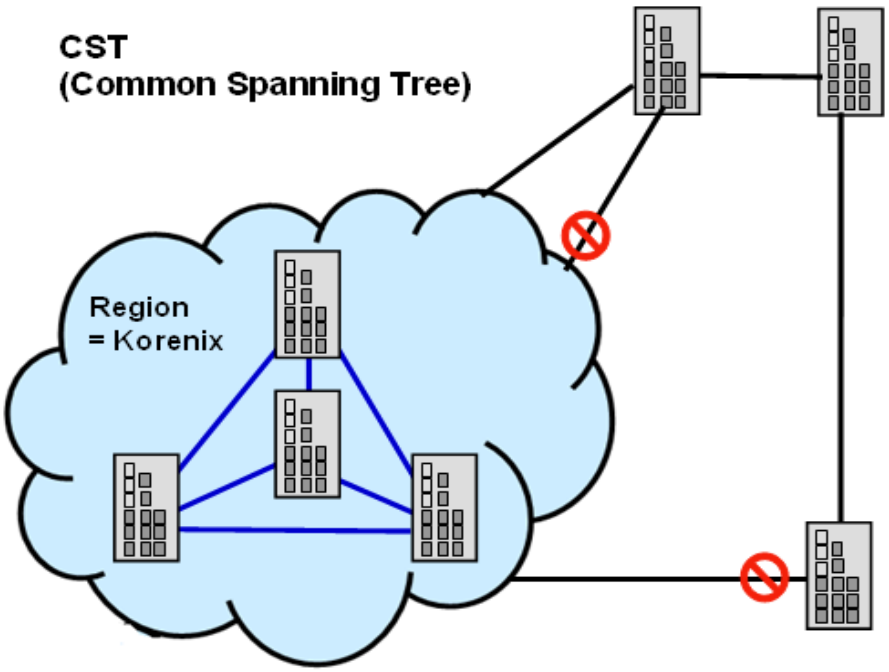
One VLAN can be mapped to a Multiple Spanning Tree Instance (MSTI). For example, the maximum Instance of the Managed Switch supports is usually 16, range from 0-15. The MSTP builds a separate Multiple Spanning Tree (MST) for each instance to maintain connectivity among each of the assigned VLAN groups.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

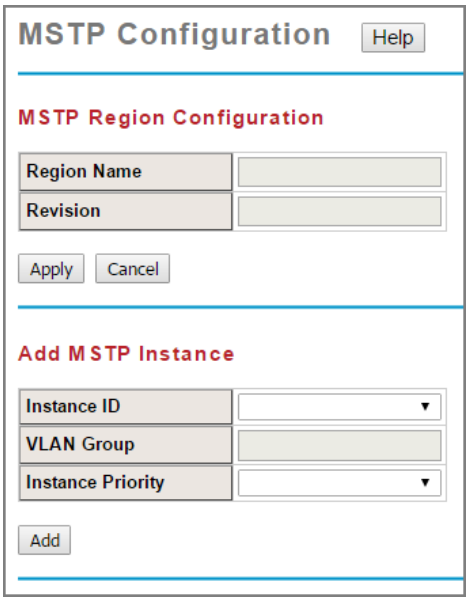
The figure shows the CST large network. In this network, a Region may has different instances and its own forwarding path and table, however, it acts as a single Brige of CST.



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

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

MSTP Region Configuration



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

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

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

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

Add MSTP Instance

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

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

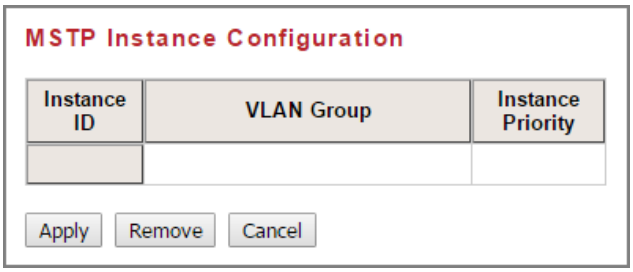
VLAN Group: Type the VLAN ID you want mapping to the instance.

Instance Priority: Assign the priority to the instance.

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

MSTP Instance Configuration

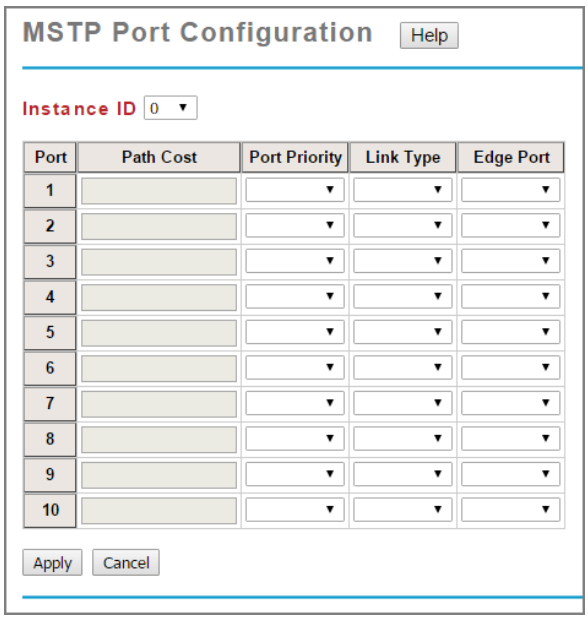
This page allows you to see the current MST Instance Configuration you added. Click on "**Apply**" to apply the setting. You can "**Remove"** the instance or "**Reload**" the configuration display in this page.



4.5.5 MSTP Port Configuration

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

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



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

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

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

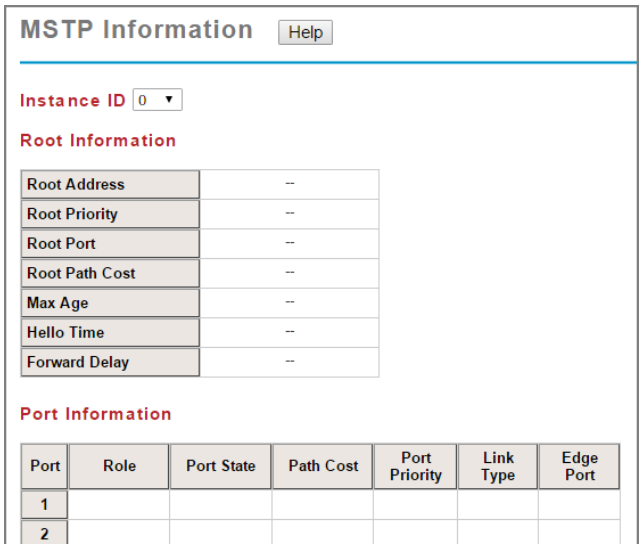
Some of the rapid state transitions that are possible within RSTP depend upon whether the port of concern can only be connected to another bridge (i.e. it is served by a point-to-point LAN segment), or if it can be connected to two or more bridges (i.e. it is served by a shared-medium LAN segment). This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

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

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

4.5.6 MSTP Information

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



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

4.5.7 Multiple Super Ring (MSR)

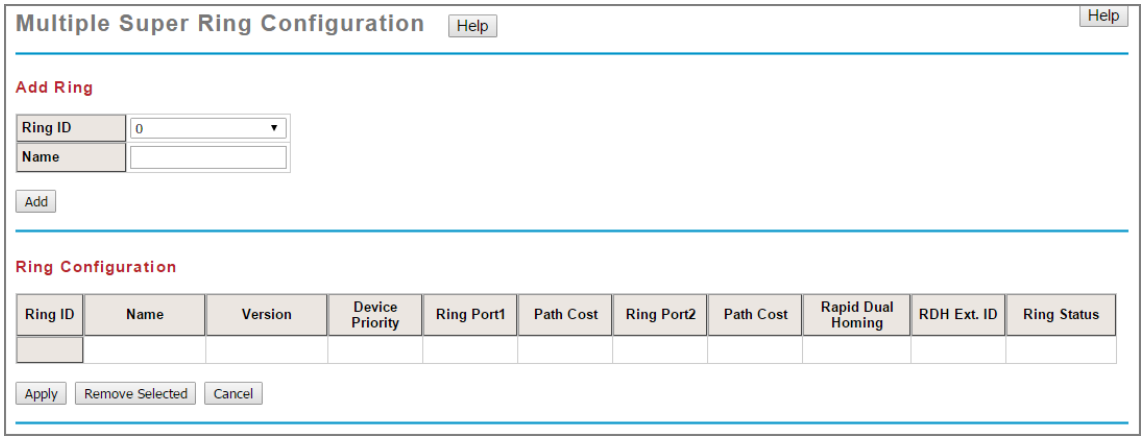
The most common industrial network redundancy is to form a ring or loop. Typically, the managed switches are connected in series and the last switch is connected back to the first one. In such connection, you can implement the Multiple Super Ring technology to get fastest recovery performance. The Ring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

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: 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.

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 Ethernet port design, that means maximum 14 Rings (12 x 100M Rings and 2 Gigabit Ethernet Rings) can be aggregated to one 24+4G Managed Switch. The feature saves much effort when constructing complex network architecture.



Add 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 names of this ring will automatically naming with Ring ID.

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: Redundant Ring and Redundant Chain, the Redundant 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 Redundant Ring environment, you should have 2 Ring Ports. No matter this switch is Ring Master or not. For Ring Master, one of the ring ports will become the forwarding port and the other one will become the blocking port.

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

Ring Port2: Assign another port for ring connection

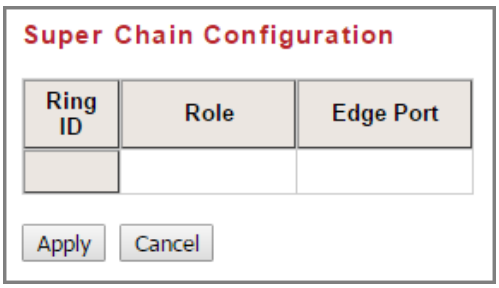
Path Cost: Change the Path Cost of Ring Port2

Rapid Dual Homing: Rapid Dual Homing is an important feature of 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).

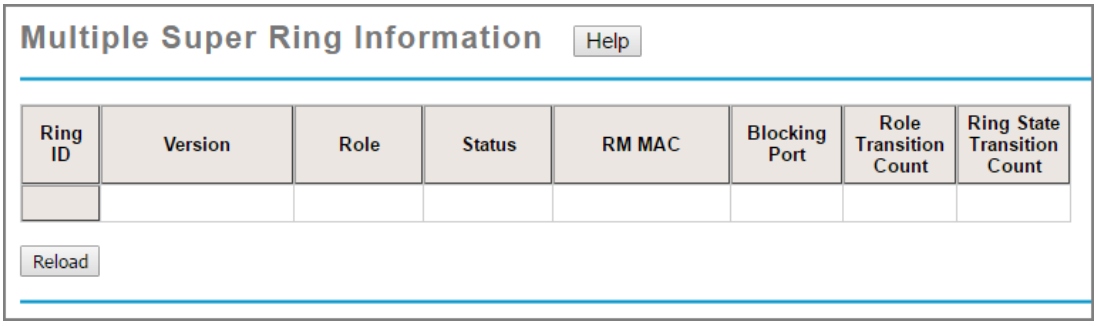
Role: Super Chain has two node role Border

and Member. Border is the node which connects 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.

4.5.8 Ring Info

This page shows the MSR information.



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.

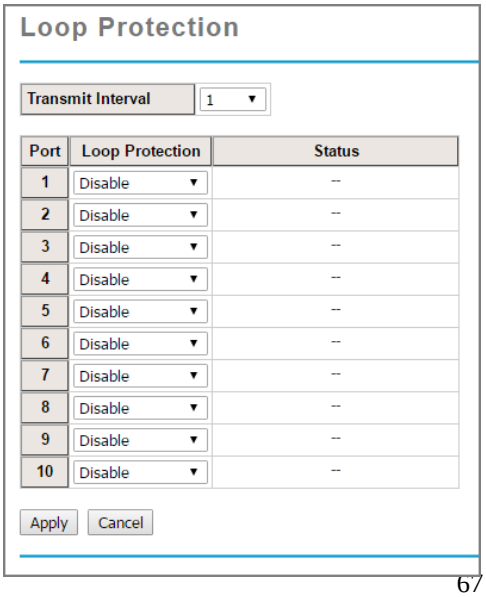
Blocking Port: This field shows which is blocked port of RM.

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.

4.5.9 Loop Protection

The Loop Protection is a mechanism to prevent traffic looping occurred. The default interval detective time is 1 second, and the duration can up to 10 seconds. Enable the Loop Protection function and click “Apply”, then the function will be activate.



4.5.10 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.
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)# na69orenixnix 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 69orenixnix] 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 71orenixnix] 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 Gigabit Ethernet 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

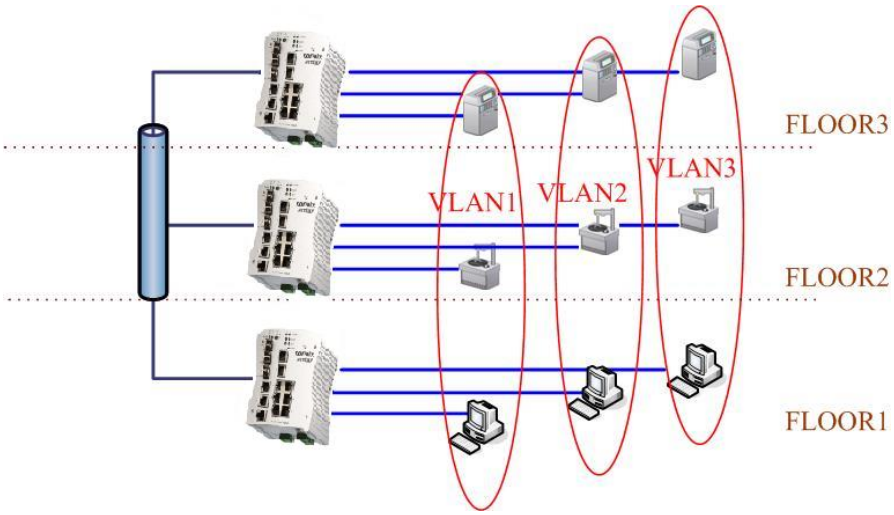
	Timers WTR Timer : period is 1 minutes, timer is not running, remains 0 ms Guard Timer : period is 100 ms, timer is not running, remains 0 ms Statistics R-APS(SF) : sent 0, received 0 R-APS(NR,RB) : sent 0, received 0 R-APS(NR) : sent 0, received 0 Node State Transition count 0 Switch#
Configure ERPS	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

4.6 VLAN

A Virtual LAN (VLAN) is a “logical” grouping of nodes for the purpose of limiting a broadcast domain to specific members of a group without physically grouping the members together. It means that VLAN can 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.

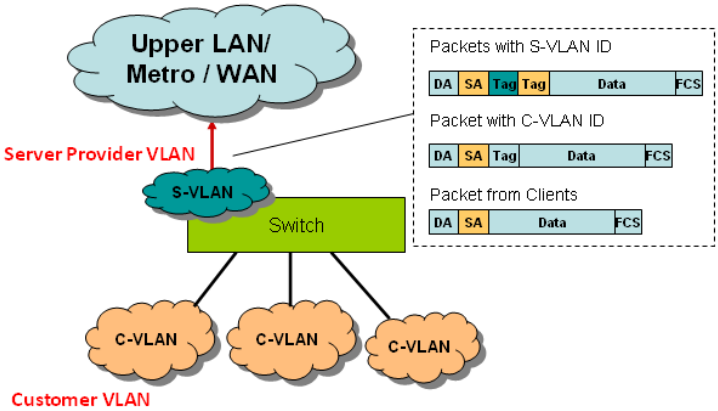
JetNet 6910G-M12 supports 802.1Q VLAN. 802.1Q VLAN is also known as Tag-Based VLAN. This Tag-Based VLAN allows VLAN to be created across different switches (see Figure 1). IEEE 802.1Q tag-based VLAN makes use of VLAN control information stored in a VLAN header attached to IEEE 802.3 packet frames. This 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 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:

4.6.1 VLAN Port Configuration

4.6.2 VLAN Configuration

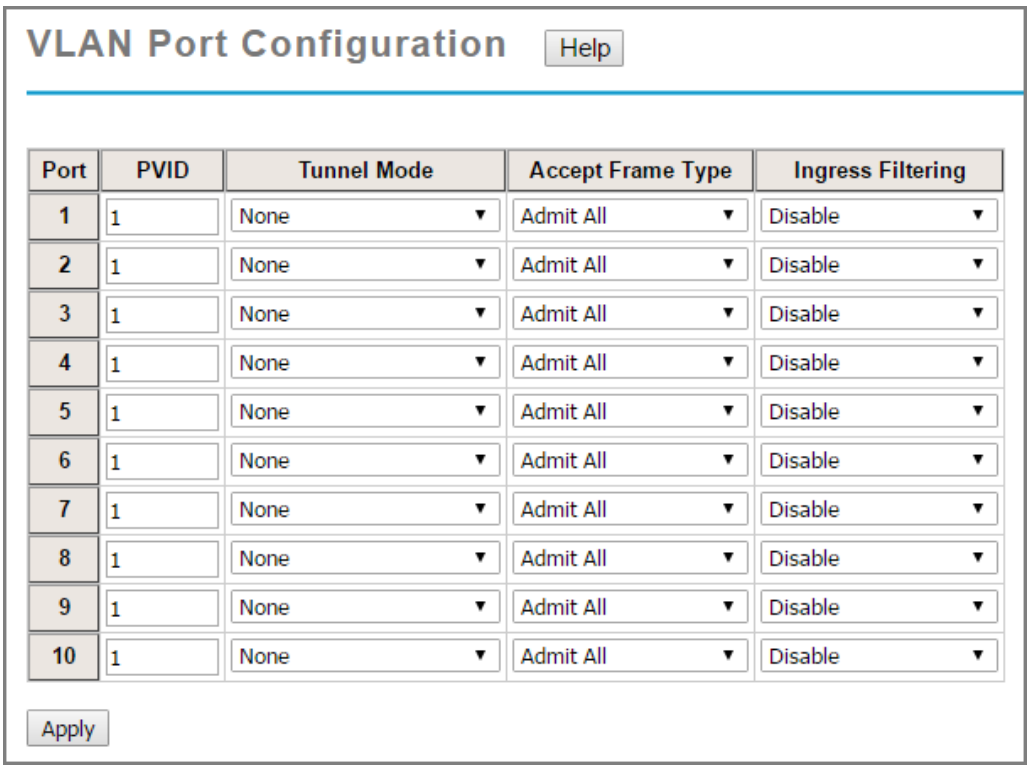
4.6.3 GVRP Configuration

4.6.4 VLAN Table

4.6.5 CLI Commands of the VLAN

4.6.1 VLAN Port Configuration

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



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. However, these 2 PVIDs: 0 and 4095 are reserved and applicable. 1 is the default value. 2 to 4094 are valid and available in this column.

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.

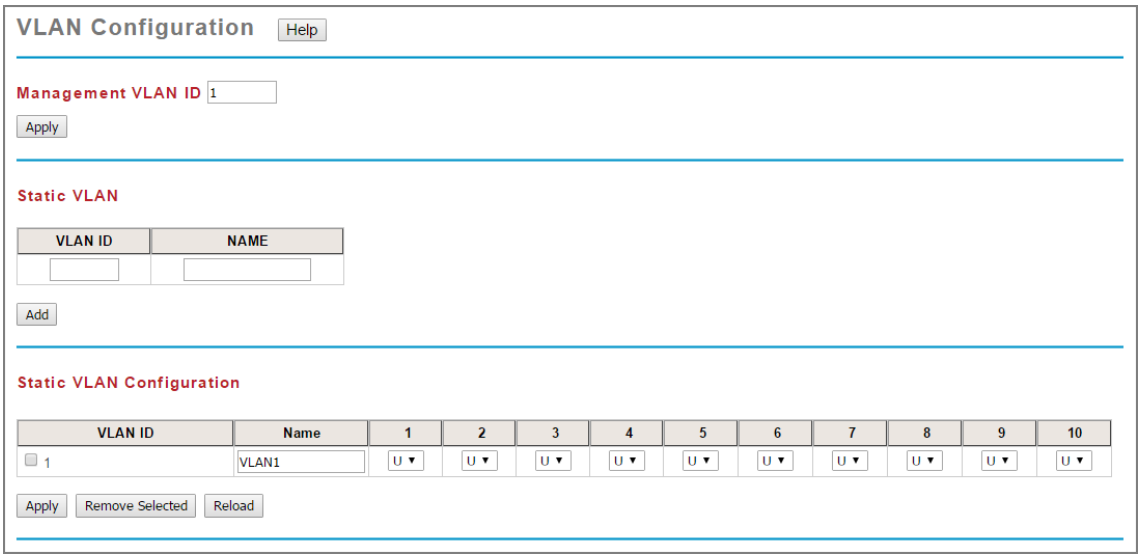
Accept Frame Type: This column defines the accepted frame type of the port. There are 2 modes to select, **Admit All** and **Tag Only**. Admit All mode enables the port to be capable to accept both tagged and untagged packets. Tag Only mode means that the port can only accept tagged packets.

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

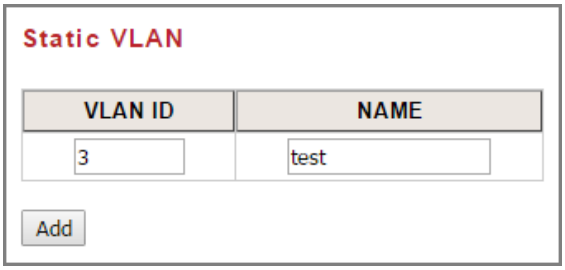
4.6.2 VLAN Configuration

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

Figure 4.6.2.1 Web UI of the VLAN Configuration.



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



Static VLAN: 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. For VLAN name without setting or blank, the system will automatically assign VLAN name for the VLAN. The rule is VLAN (VLAN ID).

Figure 4.6.2.2 The steps to create a new VLAN: Type VLAN ID and NAME, and press **Add** to create a new VLAN. Then the new VLAN in the Static VLAN Configuration table can be displayed. Refer to Figure 4.6.2.3

After VLAN is created, the status of the VLAN remains in Unused until further ports are added to the VLAN.

Caution: *Before changing the management VLAN ID via 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.*

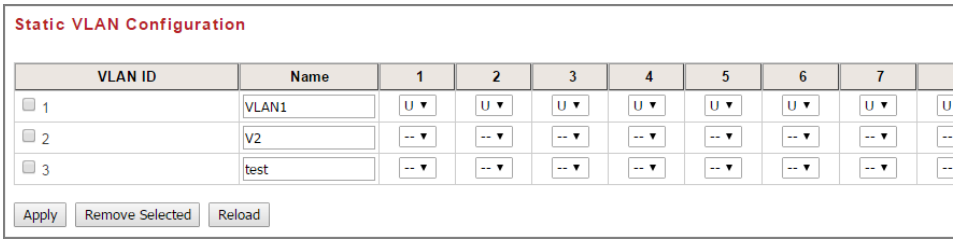
Note: *JetNet 6910G-M12 supports max 255 groups of VLAN.*

Static VLAN Configuration

You can see the created VLANs and specify the egress (outgoing) port rule to be

Untagged or Tagged here.

Figure 4.6.2.3 Static VLAN Configuration table. The new VLAN 3 is created. VLAN name is " **test**". Egress rules of the ports are not configured now.



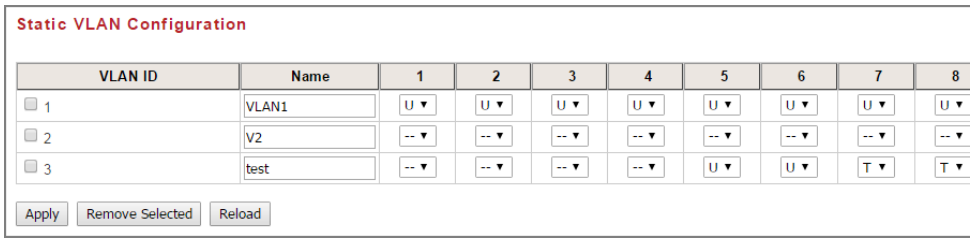


Figure 4.6.2.4 Configure Egress rule of the ports.

-- : Not available

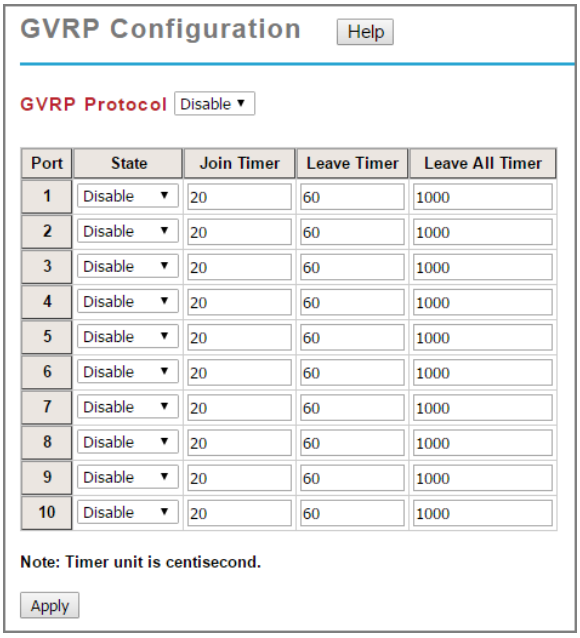
U: **Untag**: Indicates that egress/outgoing frames are not VLAN tagged.

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

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

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

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

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

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

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

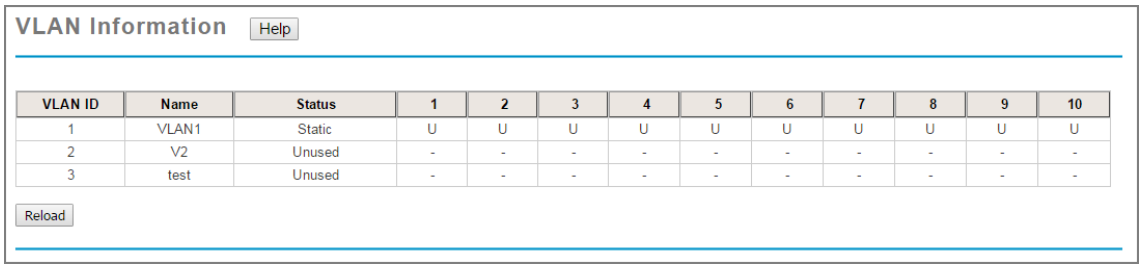
4.6.4 VLAN Table

This table shows 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.



4.6.5 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 ! ….

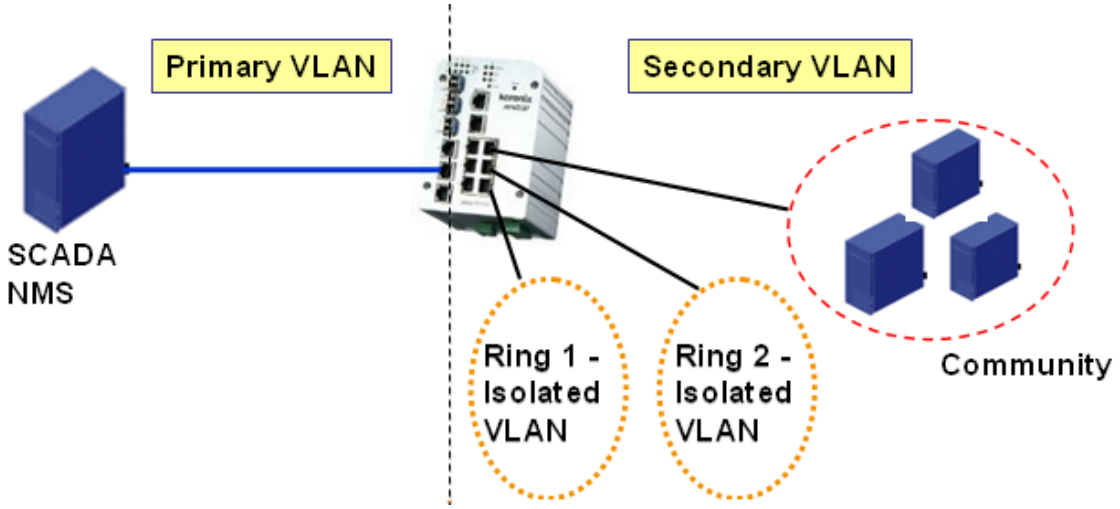
4.7 Private VLAN

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

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

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

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



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

Following commands are included in this group:

4.7.1 PVLAN Configuration

4.7.2 PVLAN Port Configuration

4.7.3 PVLAN Informtion

4.7.4 CLI Commands of the PVLAN

4.7.1 PVLAN Configuration

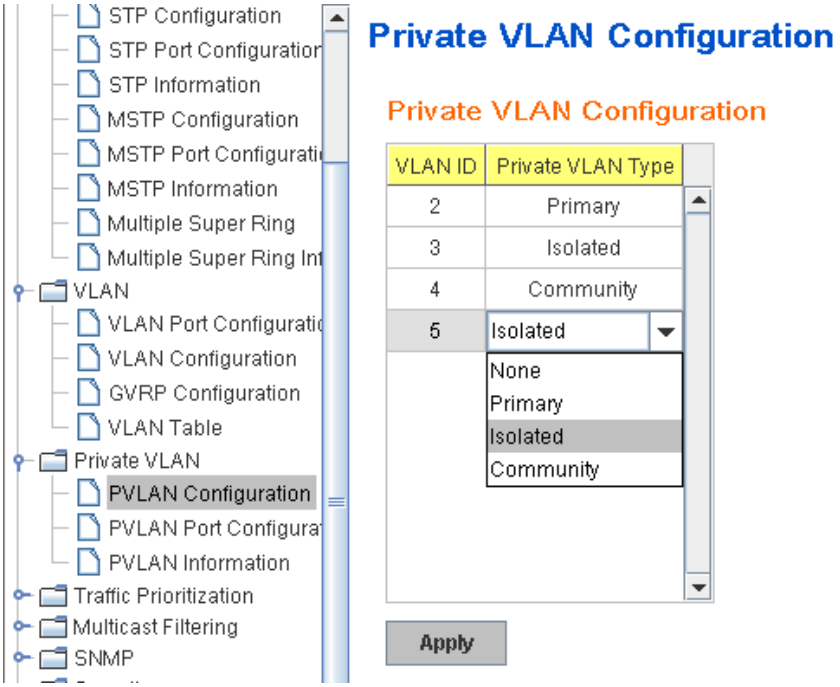
PVLAN Configuration is to assign Private VLAN type. After created VLAN in VLAN Configuraiton page, the available VLAN ID will display here. Choose the Private VLAN types for each VLAN to be configured.

None: The VLAN is Not included in Private VLAN.

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

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

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



4.7.2 PVLAN Port Configuration

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

Private VLAN Association

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

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

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

Port Configuraion

PVLAN Port Type ：

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

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

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

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

For example:

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

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

VLAN 2 is belonged to Primary VLAN.

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

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

4. Private VLAN Port 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

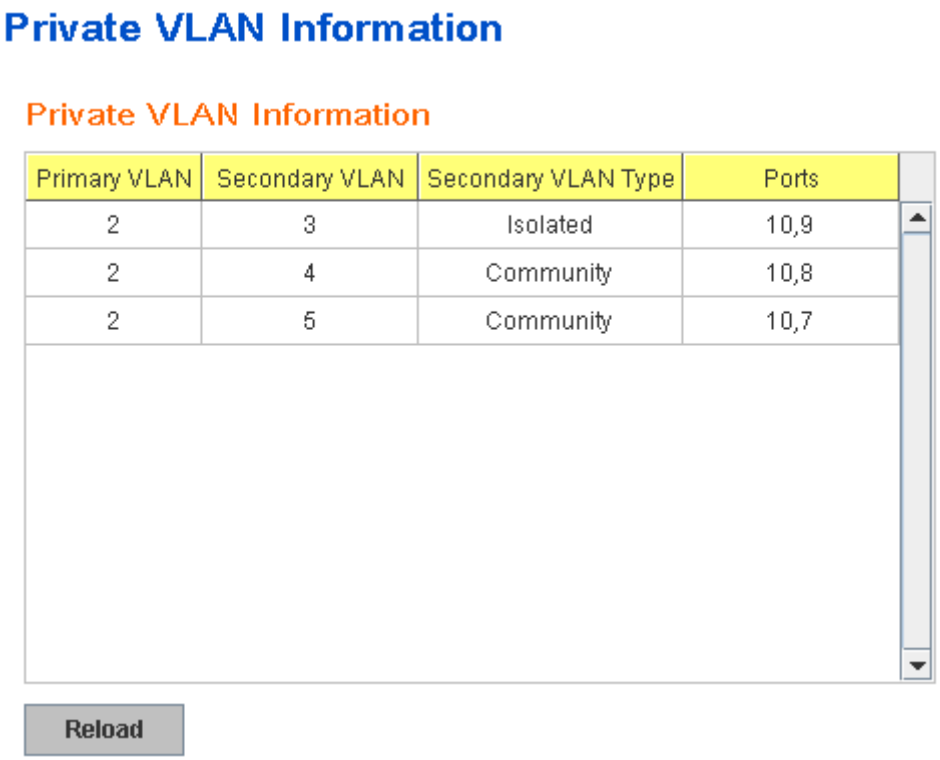
Private VLAN Association

Secondary VLAN	Primary VLAN
3	2
4	2
5	2

Apply

4.7.3 Private VLAN Information

This page allows you to see the Private VLAN information.



4.7.4 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 Gigabit Ethernetbitethernet8 switchport access vlan add 2,4 switchport trunk native vlan 4 switchport mode private-vlan host switchport private-vlan host-association 2 4 ! interface Gigabit Ethernetbitethernet9 switchport access vlan add 2,5 switchport trunk native vlan 5 switchport mode private-vlan host

	switchport private-vlan host-association 2 3 ! interface Gigabit Ethernetbitethernet10 switchport access vlan add 2,5 switchport trunk native vlan 2 switchport mode private-vlan promiscuous switchport private-vlan mapping 2 add 3-5 …… ……..

4.8 Traffic Prioritization

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

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 the industrial network.

Following commands are included in this group:

4.8.1 QoS Setting

4.8.2 QoS Priority Mode

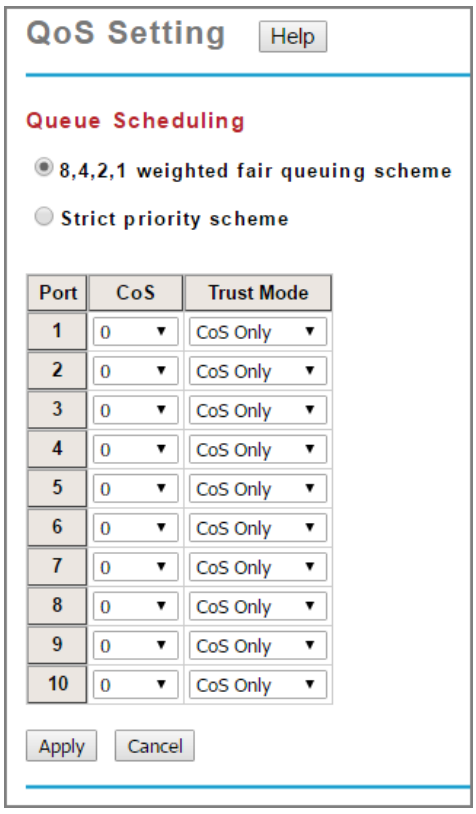
4.8.3 CoS-Queue Mapping

4.8.4 DSCP-Queue Mapping

4.8.5 CLI Commands of the Traffic Prioritization

4.8.1 QoS Setting

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



Queue Scheduling

A administrator 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:

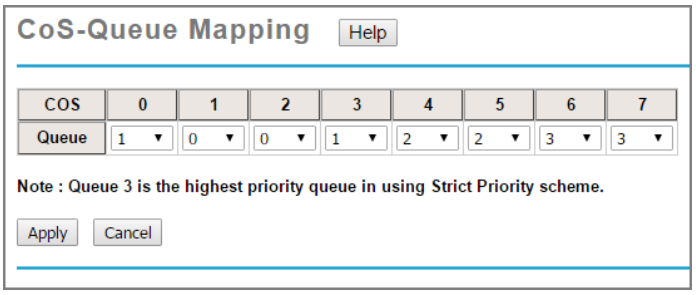
Wx / W0 + W1 + W2 + W3 + W4 + W5 + W6 + W7 (Total volume of Queue 0-7)

4.8.2 Port-based Queue Mapping

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

4.8.3 CoS-Queue Mapping

This page is to change CoS values to Physical Queue mapping table. JetNet 6910G-M12 switch fabric can support 4 physical queues, to allow Users CoS value to the different levels of the physical queue. In JetNet 6910G-M12, users can freely assign the mapping table or follow the suggestion of the 802.1p standard.

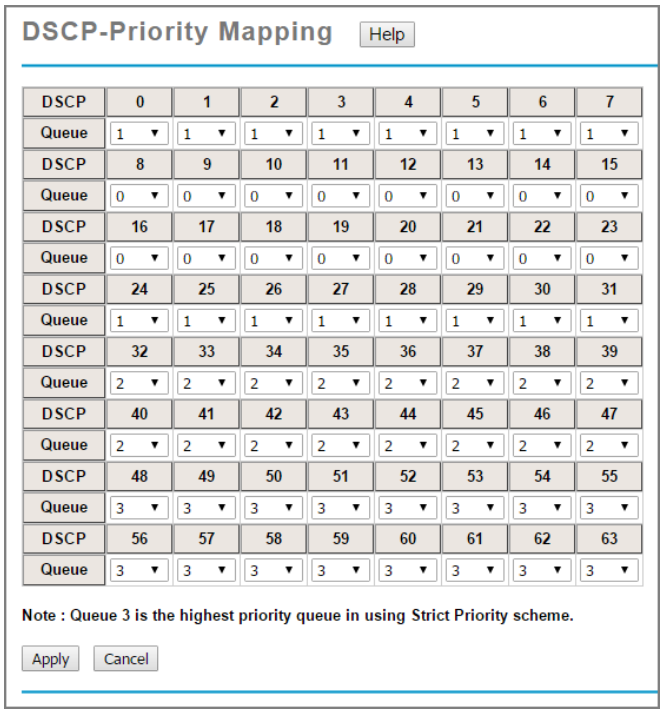


After configuration, press **Apply** to enable the settings.

4.8.4 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 4 different physical queue, from lowest 0 to highest 3.

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



4.8.5 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 3 0 4 0

	…….. 18 0 19 0 20 0
CoS-Queue Mapping	
Format	Switch(config)# qos cos-map PRIORITY Assign an priority (7 highest) Switch(config)# qos cos-map 1 QUEUE Assign an queue (0-7) ***Note: Format: qos cos-map priority_value queue_value***
Map CoS 0 to Queue 1	Switch(config)# qos cos-map 0 1 The CoS to queue mapping is set ok.
Map CoS 1 to Queue 0	Switch(config)# qos cos-map 1 0 The CoS to queue mapping is set ok.
Map CoS 2 to Queue 0	Switch(config)# qos cos-map 2 0 The CoS to queue mapping is set ok.
Map CoS 3 to Queue 1	Switch(config)# qos cos-map 3 1 The CoS to queue mapping is set ok.
Map CoS 4 to Queue 2	Switch(config)# qos cos-map 4 2 The CoS to queue mapping is set ok.
Map CoS 5 to Queue 2	Switch(config)# qos cos-map 5 2 The CoS to queue mapping is set ok.
Map CoS 6 to Queue 3	Switch(config)# qos cos-map 6 3 The CoS to queue mapping is set ok.
Map CoS 7 to Queue 3	Switch(config)# qos cos-map 7 3 The CoS to queue mapping is set ok.
Display – CoS-Queue mapping	Switch# sh qos cos-map CoS to Queue Mapping : CoS Queue ---- + ------ 0 1 1 0 2 0 3 1 4 2 5 2 6 3 7 3
DSCP-Priority Mapping	
Format	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) ***Format: qos dscp-map priority_value queue_value***
Map DSCP 0 to Queue 1	Switch(config)# qos dscp-map 0 1 The TOS/DSCP to queue mapping is set ok.
Display – DSCO-Queue mapping	Switch# show qos dscp-map DSCP to Queue Mapping : (dscp = d1 d2) d2| 0 1 2 3 4 5 6 7 8 9 d1 |

	-----+---------- 0|1 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

4.9 Multicast Filtering

For multicast filtering, JetNet 6910G-M12 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.

Administrator can enable **IGMP Snooping** and **IGMP Query** functions followed by this section. 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 are mentioned below.

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

Following commands are included in this group:

4.9.1 IGMP Snooping

4.9.2 IGMP Query

4.9.3 Unknown Multicast

4.9.4 GMRP Configuration

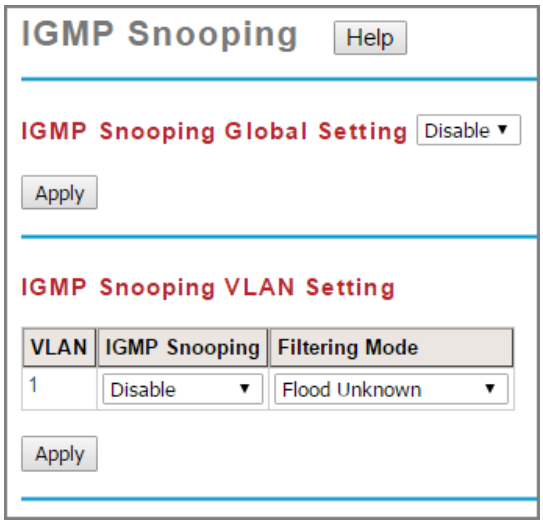
4.9.5 CLI Commands of the Multicast Filtering

4.9.1 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 keinput. JetNet 6910G-M12 supports IGMP snooping V1/V2/V3 and IGMP query V1/V2.

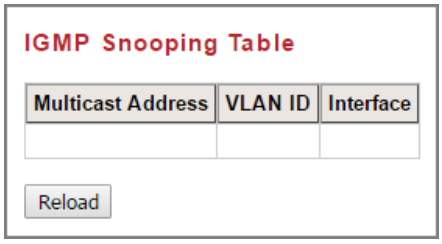
IGMP Snooping, administrator can select **Enable** or **Disable** here. After enabling IGMP Snooping, then enable IGMP Snooping for specific VLAN. It's possible to enable IGMP Snooping for some VLANs so that these specified VLANs can support IGMP Snooping and others don't.

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.



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.

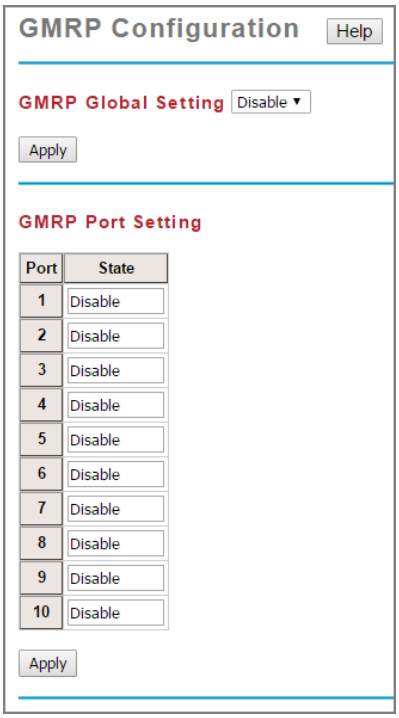
IGMP Snooping Table: In the table, you can see multicast group IP address, VLAN ID it belongs to, and member ports of the multicast group. JetNet 6910G-M12 supports 256 multicast groups. Click on **Reload** to refresh the table.



4.9.2 IGMP Query

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 administrator want to run IGMP Snooping feature in several VLANs, administrator 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, administrator 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 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 the settings is configured, click on **Apply** to apply configuration for taking effective.

4.9.3 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.

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

4.9.4 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 exchanges the IGMP Table with other switches which is also GMRP-aware devices.

4.9.5 CLI Commands of the Multicast Filtering

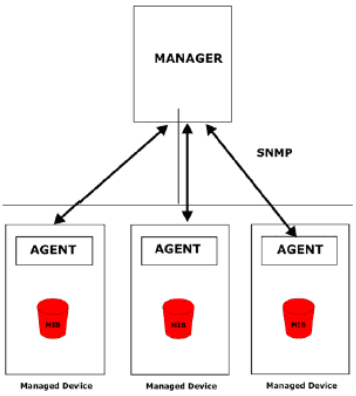
Command Lines of the multicast filtering configuration

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

4.10 SNMP



Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. 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:

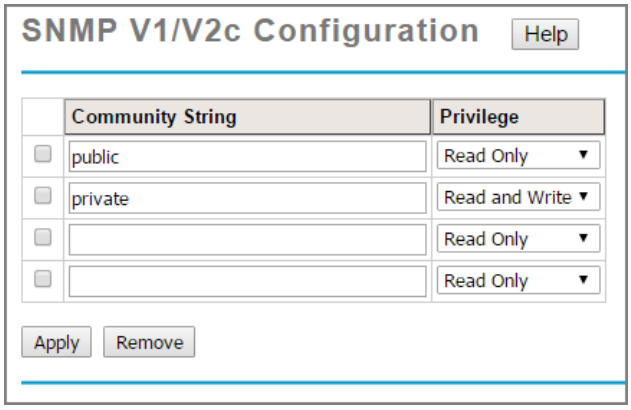
4.10.1 SNMP Configuration

4.10.2 SNMPv3 Profile

4.10.3 SNMP Traps

4.10.4 SNMP CLI Commands for SNMP

4.10.1 SNMP Configuration



This page allows administrator 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 trying to access SNMP agent.

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

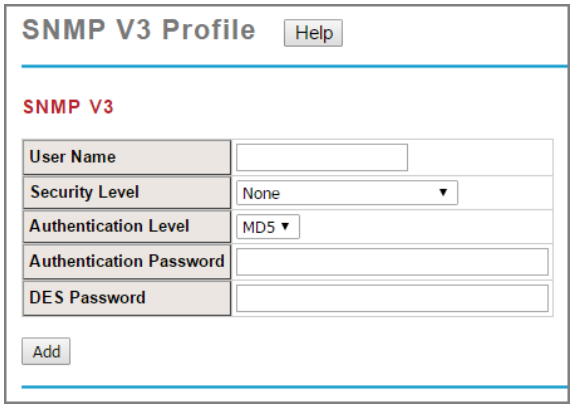
With **Read Only** privilege, only the ability to read the values of MIB tables. Default community string is Public.

With **Read and Write** privilege, 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: *For first installing the switch with device in the network, it's highly recommended to change the community string. Since most SNMP management application uses Public and Private as their default community name, this might be the hole or leakage of the network in security concern.*

4.10.2 SNMP V3 Profile

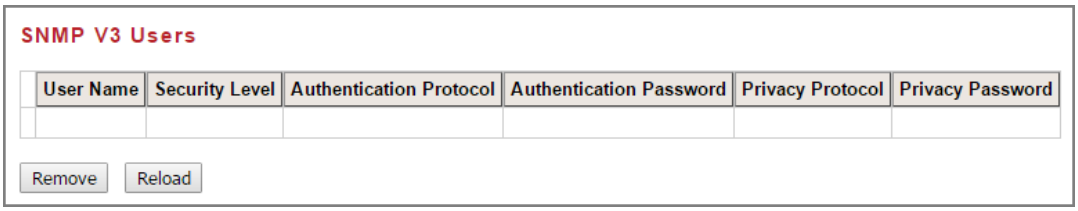


SNMP v3 can provide more security functions when the user performs remote management through SNMP protocol. It delivers SNMP information to the administrator with user authentication; all of data between JetNet 6910G-M12 and the administrator are encrypted to ensure secure communication.

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 6910G-M12 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.

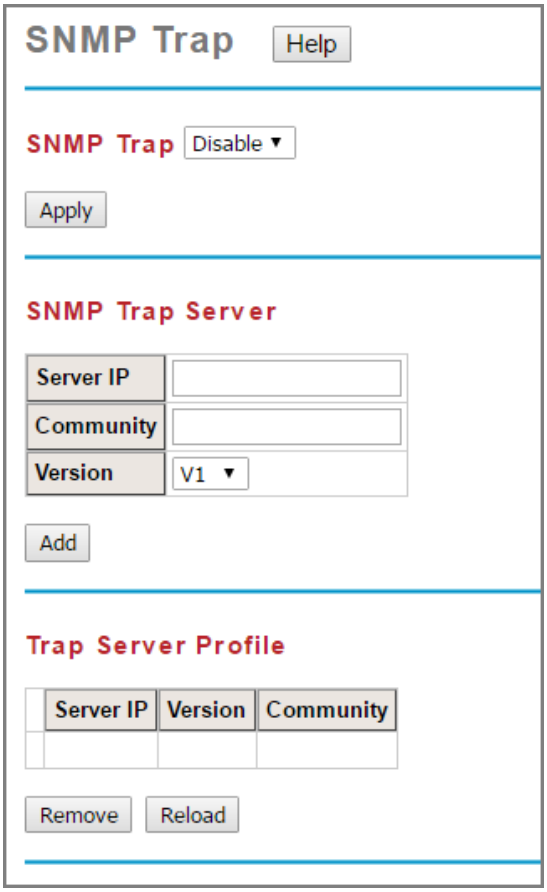


DES Encryption Password: Here the user enters the password for SNMP v3 user DES Encryption.

4.10.3 SNMP Traps

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

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



4.10.4 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 ……..

4.11 Security

JetNet 6910G-M12 provides several security features to secure the connection. The security design features Port Based MAC address Security, IP security and IEEE 802.1x.

Following commands are included in this group:

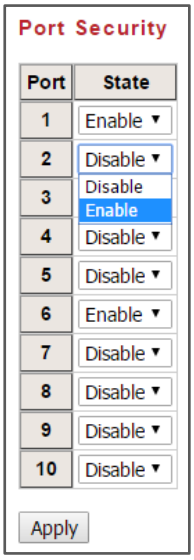
4.11.1 Port Security

4.11.2 IP Security

4.11.3 IEEE 802.1x

4.11.4 CLI Commands of the Security

4.11.1 Port Security



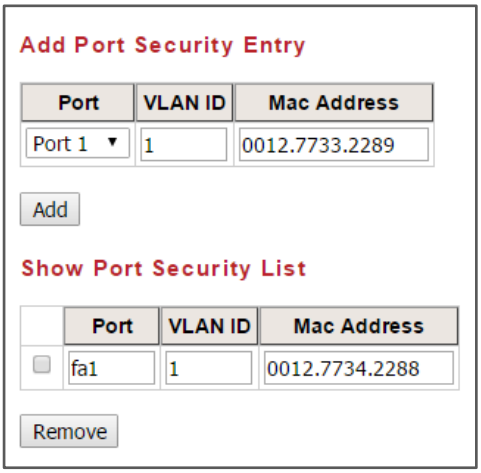
Port Security feature is to stop the MAC address learning for specific port. After stopping MAC learning, only the MAC address listed in Port Security List can access the switch and transmit/receive traffic. This is a simple way to secure the network environment and not to be accessed by hackers.

Enable/Disable Port Security: select the port and enable /disable the port security, then click “Apply” to active Port Security to change the State.

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

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

Port Security List: This table shows those enabled port security entries. It’s easy to click on “Remove” to delete the entry.



4.11.2 IP Security



In IP Security section, it is required to have a specific IP addresses to grant authorization for management access to this JetNet via a web browser or Telnet.

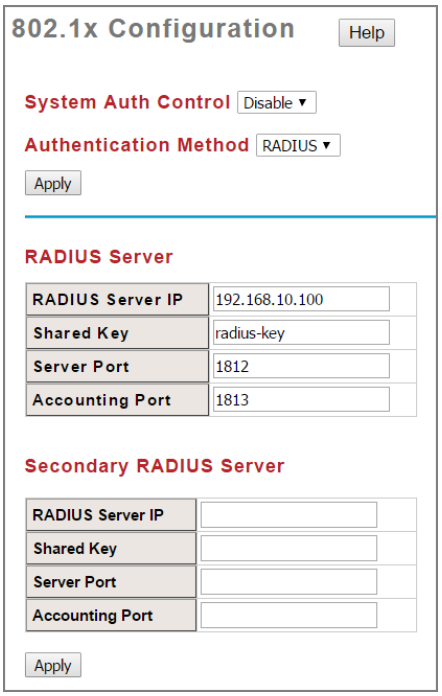
IP Security: Select Enable and Apply to enable IP security function.

Add Security IP: specific IP addresses for security can be assigned here, and then click "Add" to add a new IP entry. Only these IP addresses can access and manage JetNet via a Web browser or Telnet sessions. The maximum security IP address entry is 10 addresses.

Security IP List: This table shows added security IP addresses. Select the entry to be removed, then click "Remove" icon to delete Security IP address entry.

4.11.3 IEEE 802.1x

802.1X configuration



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

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

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

Radius Server IP: The IP address of Radius server

Shared Key: The password for 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.

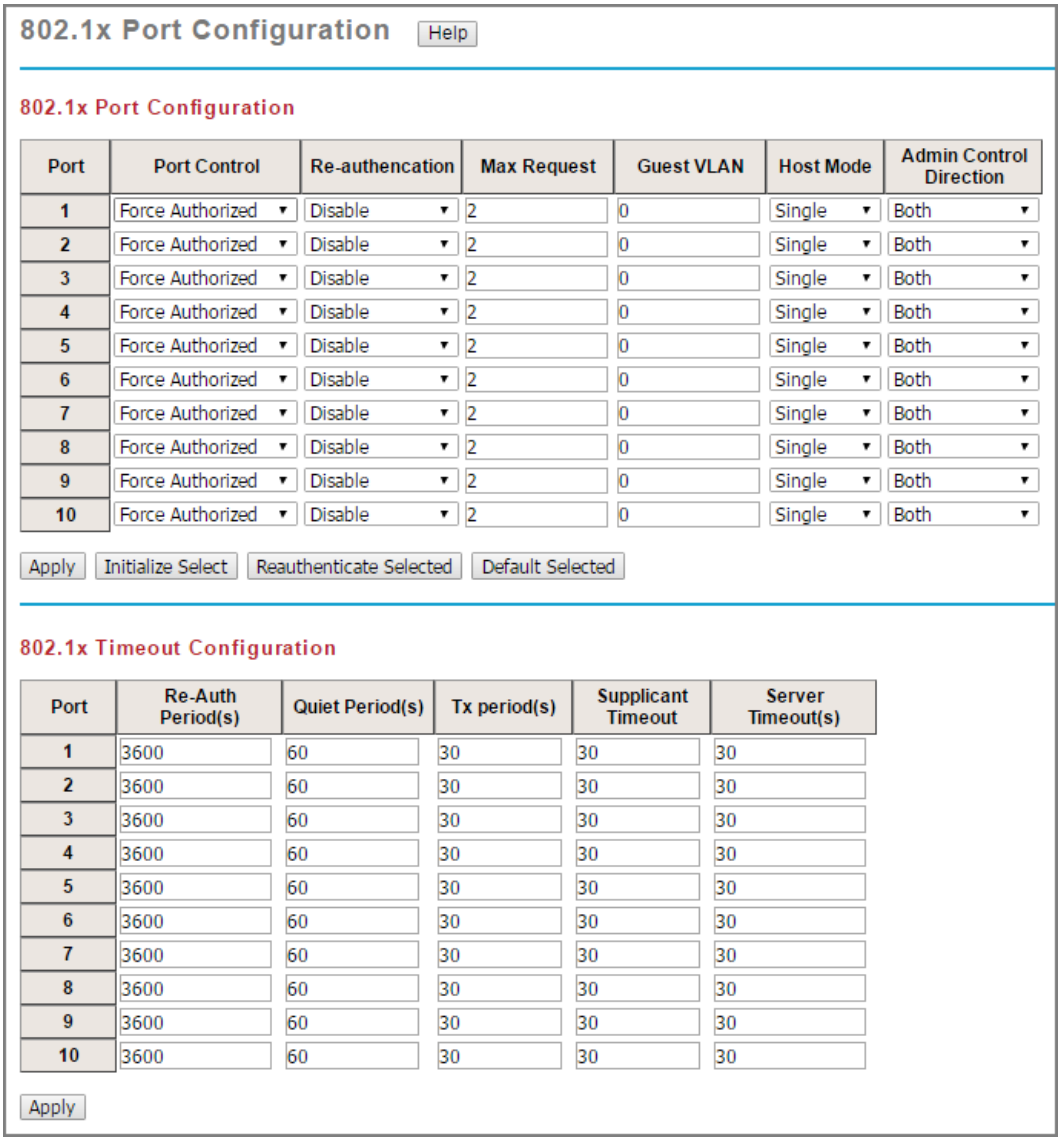
Secondary Radius Server IP: Secondary Radius Server could be set in case of the primary radius server down.

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.

802.1x Port Configuration

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



Once these settings are configured, click on **Apply** to take effective for these changes.

Port control: Force Authorized indicates this specified 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.

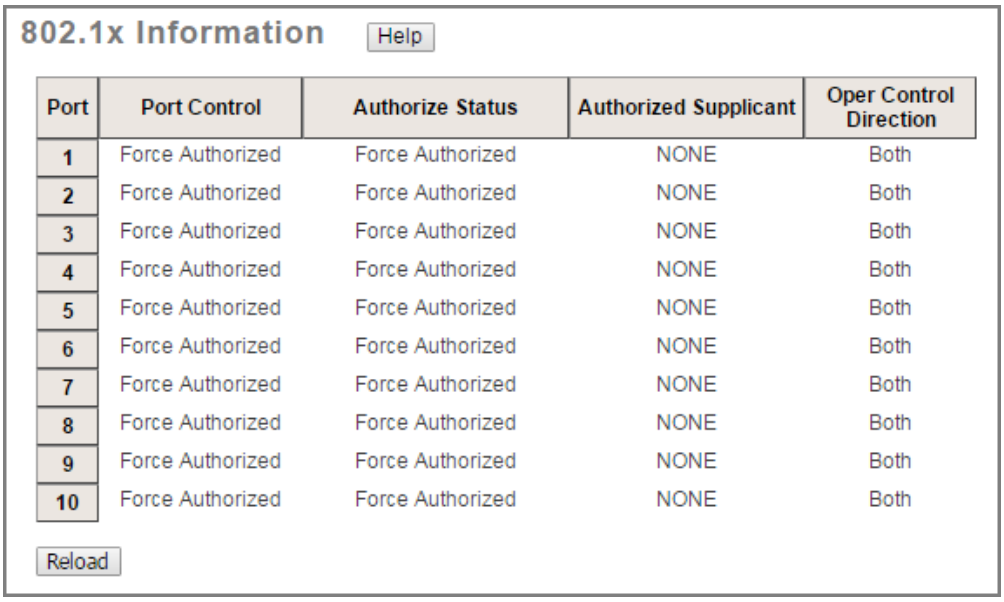
Guest VLAN: 0 to 4094 is available for this field. If this field is set to 0, that means the port is blocked after authentication fail. Otherwise, the port will be set to Guest VLAN.

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.

802.1X Port Status

The port status for Port control status, Authorize Status, Authorized Supplicant and Oper Control Direction each port can be browsed.



4.11.4 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 Extended access list	Switch(config)# ip access-list extended 100 Switch(config-ext-acl)#permit ip Any Internet Protocol tcp Transmission Control Protocol udp User Datagram Protocol icmp Internet Control Message Protocol Switch(config-ext-acl)#permit ip A.B.C.D Source address any Any source host host A single source host Switch(config-ext-acl)#permit ip 192.168.10.1 A.B.C.D Source wildcard bits Switch(config-ext-acl)#permit ip 192.168.10.1 0.0.0.1 A.B.C.D Destination address any Any destination host host A single destination host Switch(config-ext-acl)#permit ip 192.168.10.1 0.0.0.1 192.168.10.100 0.0.0.1 [IFNAME] Egress interface name Switch(config-ext-acl)#permit ip 192.168.10.1 0.0.0.1 192.168.10.100 0.0.0.1 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 userna111orenixnix pass111orenixnix 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

4.12 Warning

JetNet 6910G-M12 offers several types of Warning features to remotely monitor the status of end devices or the change of your network. The features include System Log and SMTP E-mail Alert.

Following commands are included in this group:

4.12.1 Event Selection

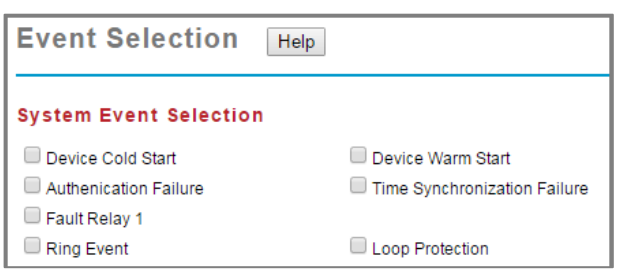
4.12.2 Syslog Configuration

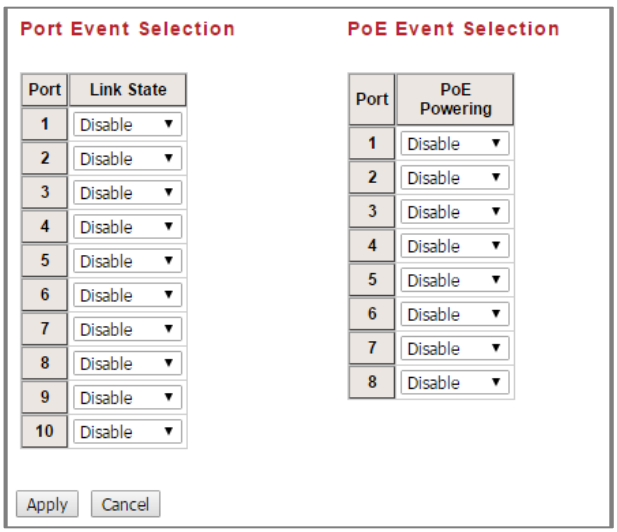
4.12.3 SMTP Configuration

4.12.4 CLI Commands

4.12.1 Event Selection

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





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

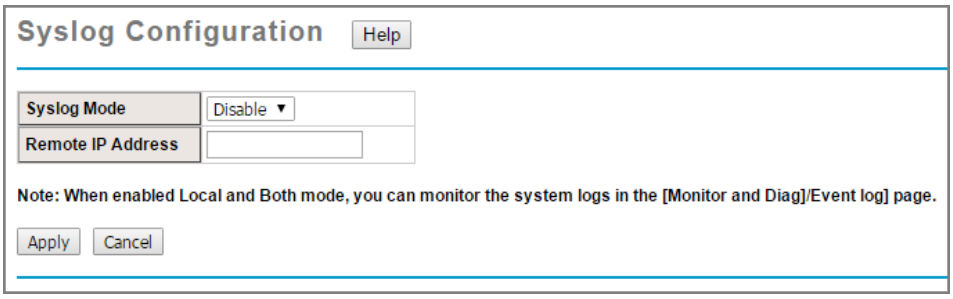
4.12.2 SysLog Configuration

System Log is useful to provide system administrator locally or remotely monitor switch events history. There are 2 System Log modes provided by JetNet 6910G-M12, local mode and remote mode.

Local Mode: In this mode, JetNet 6910G-M12 will print the occurred events selected in the Event Selection page to System Log table of JetNet 6910G-M12. 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 6910G-M12. In this mode, you should assign the IP address of the System Log server. JetNet 6910G-M12G 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.



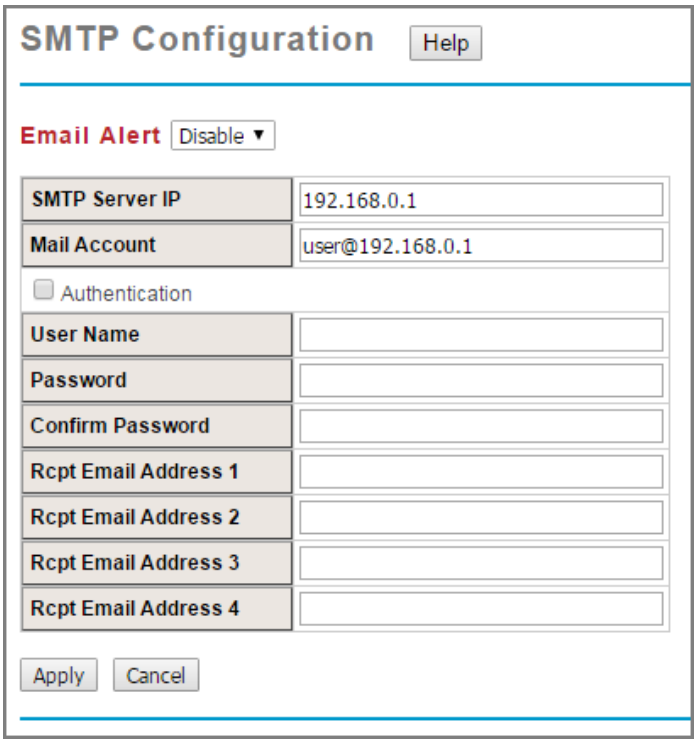
Once you finish configuring the settings, click on **Apply** to apply your configuration.

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

4.12.3 SMTP Configuration

Jet 6910G-M12 supports E-mail Warning feature. The switch will send the occurred events to remote E-mail server. The receiver can be notified by E-mail. The E-mail warning mechanism 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.



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.

4.12.4 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:

4.13 Monitor and Diagnostic

JetNet 6910G-M12 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:

4.13.1 LLDP Configuration

4.13.2 MAC Address Table

4.13.2 Port Statistics

4.13.3 Port Mirroring

4.13.4 Event Log

4.13.6 Ping

4.13.7 Modbus/TCP

4.13.8 CLI Commands of the Monitor and Diag

4.13.1 LLDP Configuration

JetNet 6910G-M12 supports 802.1AB Link Layer Discovery Protocol, thus JetNet 6910G-M12 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.

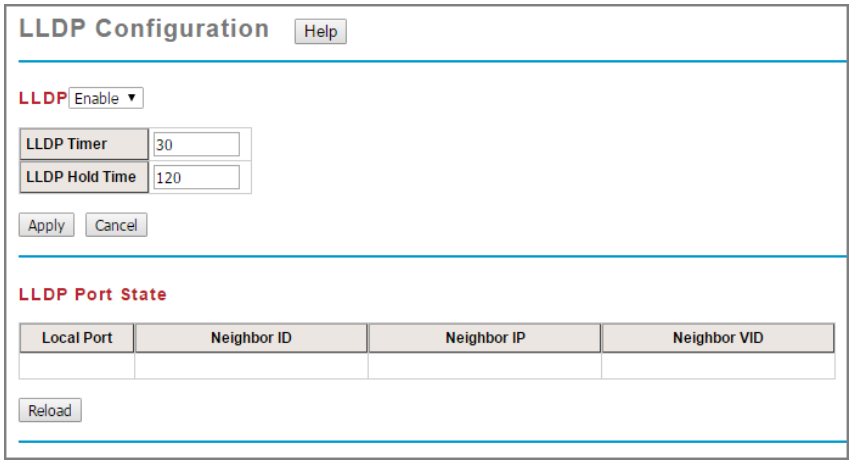
LLDP: Enable/Disable the LLDP topology discovery information.

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.



4.13.2 MAC Address Table

JetNet 6910G-M12 provides 8K 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

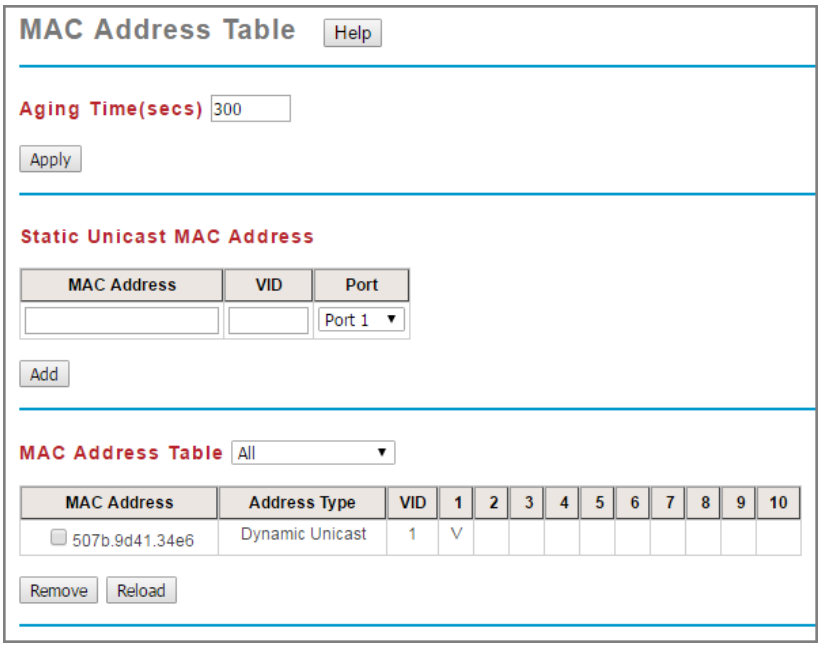
In some applications, users may need to type in the static Unicast MAC address to its MAC address table. In this page, you can type MAC Address (format: xxxx.xxxx.xxxx), select its VID and Port ID, and then click on **Add** to add it to MAC Address table.

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.

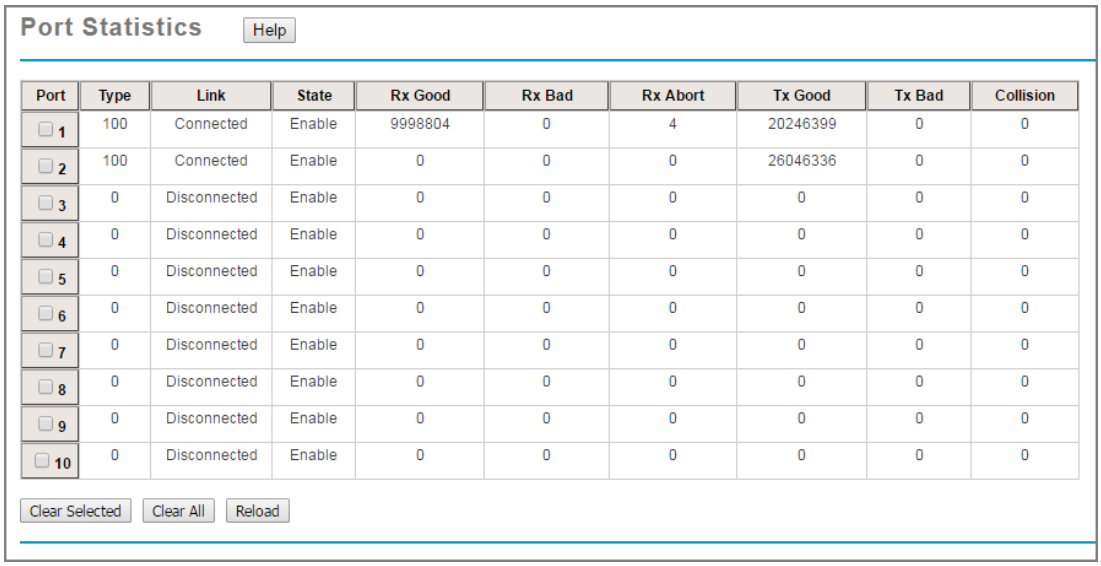


4.13.3 Port Statistics

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.

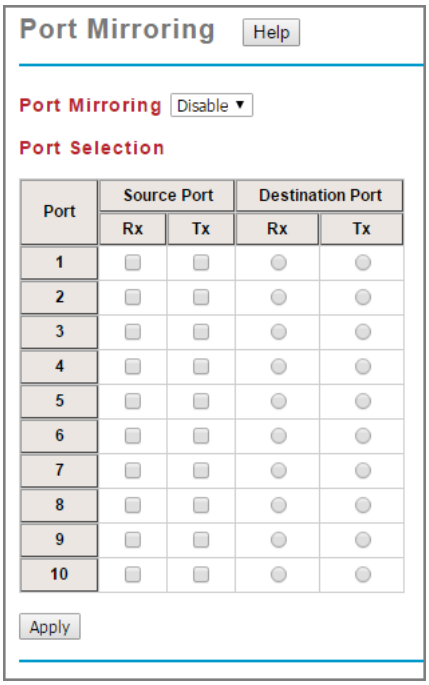
Click on **Clear Selected** to reinitialize the counts of the selected ports, and **Clear All** to reinitialize the counts of all ports. Click on **Reload** to refresh the counts.



Port	Type	Link	State	Rx Good	Rx Bad	Rx Abort	Tx Good	Tx Bad	Collision
1	100	Connected	Enable	9998804	0	4	20246399	0	0
2	100	Connected	Enable	0	0	0	26046336	0	0
3	0	Disconnected	Enable	0	0	0	0	0	0
4	0	Disconnected	Enable	0	0	0	0	0	0
5	0	Disconnected	Enable	0	0	0	0	0	0
6	0	Disconnected	Enable	0	0	0	0	0	0
7	0	Disconnected	Enable	0	0	0	0	0	0
8	0	Disconnected	Enable	0	0	0	0	0	0
9	0	Disconnected	Enable	0	0	0	0	0	0
10	0	Disconnected	Enable	0	0	0	0	0	0

4.13.4 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.

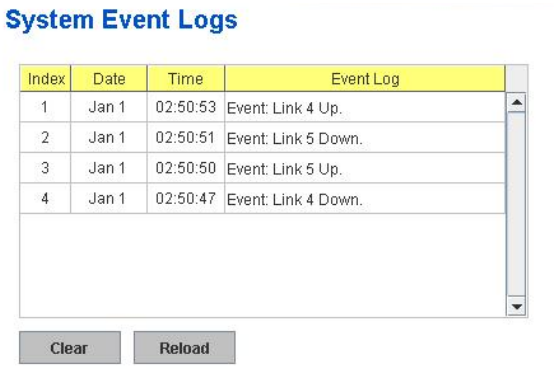
Destination Port: This is also known as Analysis Port. You can analyze the traffic of all the monitored ports at this port without affecting the flow of traffic on the port(s) being monitored. Only one of the destination ports can be selected. A network administrator would typically connect a LAN analyzer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

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

4.13.5 Event Log

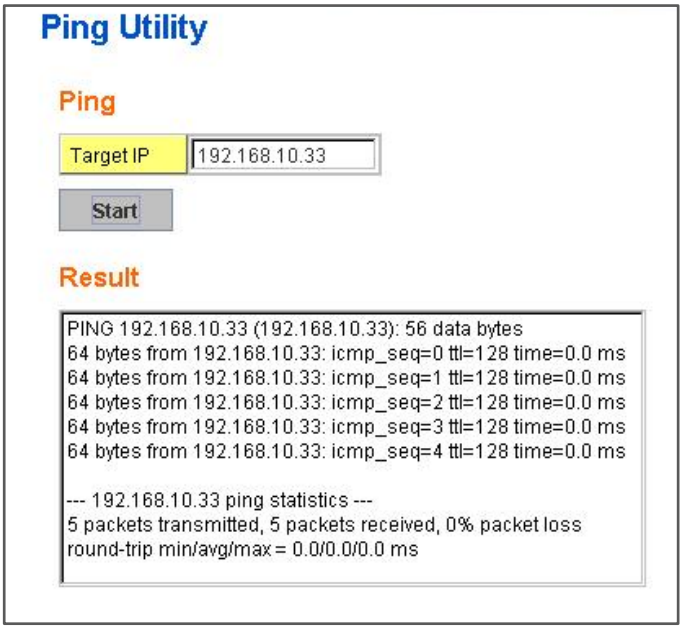
In the 4.10.3, we have introduced System Log feature. When System Log Local mode is selected, JetNet 6910G-M12 will record occurred events in local log table. This page shows this log table. The entry includes the index, occurred data and time and content of the events.

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

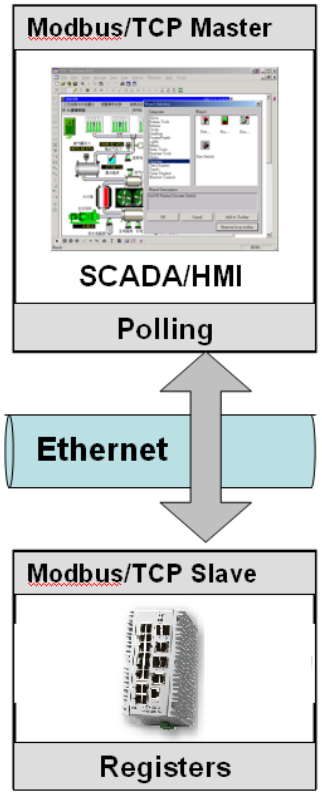


4.13.6 Ping Utility

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.



4.13.7 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.

This Ethernet Switch has 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 = ‘l’ 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
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	2 words	Deferred

0x267F		
0x2680 to 0x26BF	2 words	Collisions
0x26C0 to 0x26FF	2 words	SingleCollision
0x2700 to 0x273F	2 words	MultipleCollision
0x2740 to 0x277F	2 words	ExcessiveCollision
0x2780 to 0x27BF	2 words	LateCollision
0x27C0 to 0x27FF	2 words	Filtered
0x2800 to 0x283F	2 words	FCSError
0x2840 to 0x29FF	447 words	Reserved address space
Number of frames received and transmitted with a length(in octets)		
0x2A00 to 0x2A3F	2 words	64
0x2A40 to 0x2A7F	2 words	65 to 127
0x2A80 to 0x2ABF	2 words	128 to 255
0x2AC0 to 0x2AFF	2 words	256 to 511
0x2B00 to 0x2B3F	2 words	512 to 1023
0x2B40 to 0x2B7F	2 words	1024 to maximum size

4.13.8 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!

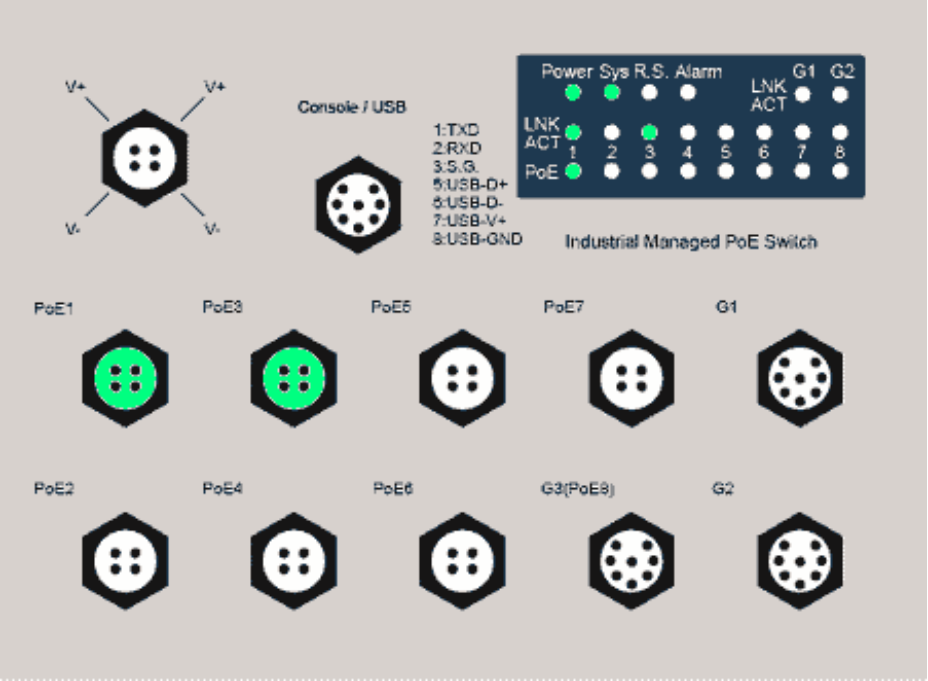
	Note: 350 is the new ageing timeout value.
Add Static Unicast MAC address	Switch(config)# mac-address-table static 0012.7701.0101 vlan 1 interface fastethernet7 mac-address-table ucast static set ok! ***Note: rule: mac-address-table static MAC_address VLAN VID interface interface_name***
Add Multicast 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

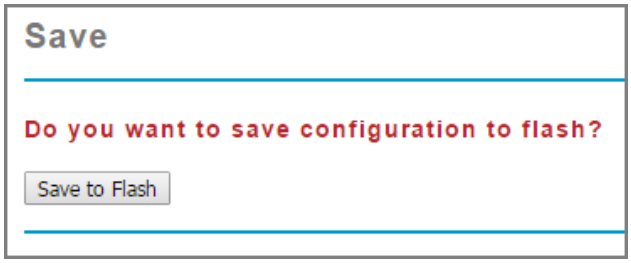
4.14 Device Front Panel

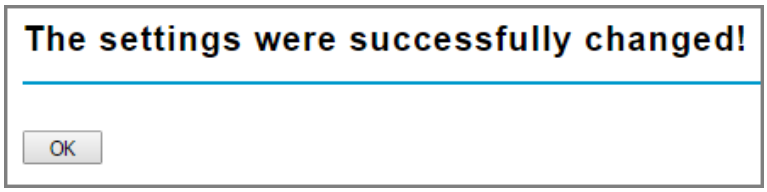
The command – “Device Front Panel” that allows you to check the LED status of the switch from Web browser. Please see LED and link status of the Power, PoE, R.S. and Font Ports. Below is the example of managed Switch. Different model has its own front panel display



4.15 Save (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.



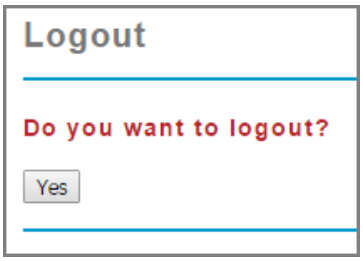


Command Lines:

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

4.16 Logout

The switch provides 2 logout methods. The web connection will be logged out if you don't input any command after 300 seconds. The Logout command allows you to manually logout the web connection. Click on **Yes** to logout, **No** to go back the configuration page.



Command Lines:

Feature	Command Line
Logout	SWITCH> exit SWITCH# exit

5 Appendix

5.1 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 6910G-M12** is 1.3.6.1.4.1.24062.2.3.11.13.1

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

5.2 Specification

Technology	
Standard	IEEE 802.3u 100Base-TX IEEE 802.3ab 1000Base-T IEEE 802.3x Flow Control and Back-pressure IEEE 802.3af Power over Ethernet IEEE 802.3at High power PoE IEEE 802.1AB Link Layer Discovery Protocol (LLDP) IEEE 802.1Q VLAN and GVRP IEEE 802.1D Rapid Spanning Tree Protocol (RSTP) IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) IEEE 802.3ad Link Aggregation Protocol (LACP) IEEE 802.1x Port Based Network Access Protocol
Performance	
Switch Technology	Store and Forward technology with 32Gbps switching fabric
System Throughput	8.3Mega packets per second, 64Bytes packet length
CPU performance	180Mhz ARM-9E /200MIPS performance with 10 seconds hardware based Watch-dog timer
System Memory	8Mega Bytes Flash ROM, 64Mega Bytes RAM
Transfer packet size	64Bytes ~1522Bytes (include double Tag VLAN)
MAC Address	8K MAC address table

Packet Buffer	1Mega bits shared packet buffer
Transfer performance	14,880pps for Ethernet, 148,800 for Fast Ethernet and 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 Groups (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 only; the system support SSL for HTTP security, SSH for Telnet security • Mange station secure by IP address and up to 4 Manage stations • Remote Management login authentication by 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	Korenix View and Korenix NMS for device finding and network topology discovery
Network Time Protocol	NTP with daylight saving, localize time synchronize function
IEEE 1588 PTP	IEEE 1588 v1
E-mail Warning	4 receipts E-mail accounts with mail server authentication
System event log	Local and remote log server with authentication
System Auto Maintenance	Power on firmware upgrade, and configuration update by USB/Memory sticker
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 trunking, trunk member up to 8 ports, maximum trunk group up to 4 include Gigabit Ethernet port
VLAN	IEEE 802.1Q Tag VLAN with 256 VLAN entries, GVRP supported VLAN Link Modes: Trunk, Hybrid and Link Access

IEEE 802.1 QinQ	Double VLAN Tag with 1522 bytes frame size
Traffic Prioritize	4 physical queues, supports weighted fair queuing (WRR) and strict priority scheme, follows COS tag ID, IPv4 ToS/DiffServ information to prioritize the traffic
Multicasting	IGMP Snooping v1/v2c/v3 for multicasting filtering and forwarding with IGMP Query mode, and also support unknown multicasting forwarding policies- drop, flooding to all ports and forward to router port
Rate Control	Ingress/Egress filtering for Broadcast, Multicast, Unknown DA or all packets
Port Mirroring	Online Traffic monitoring on multiple selected target ports
Port Security	Only permit 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
Power over Ethernet	IEEE 802.3af/at, End-Span wiring architecture
PoE operating mode	Auto Mode: IEEE 802.3af/at behaviors with IEEE 802.3at 1-Event for high power IEEE 802.3at 1-event PD device Forced Mode: User configured Power consumption budget control with IEEE 802.3 PoE /PD detection, or forced without PD detection
PoE forwarding conductor	M12 D-Code (Port 1~7): V+(1,3), V- (2,4) / M12 X-Code (Port 8): V+ (1,2), V- (3,4)
Power forwarding capability	IEEE 802.3af:15W, IEEE802.3at:30W
PoE System Power Budget	Power Budget Reserve by PD declaration. The power budget control system will reserve power for connected PD device, once latest PD device (PoE 8) claimed power over the system surplus power, and then the latest PoE will not be active. System Power Budget: 100Watts / 70°C
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™	Up to 5 100M rings or 4 100M rings, 1 1000M ring
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
System Fault Bypass	Link Partner Bypass function on Gigabit port 9,10. Both of Gigabit ports will form as interconnected mode when switch power shut-down or unstable /non-ready
Interface	
Enclosure Port	• 100 Base-TX/100Mbps Fast Ethernet: 7 x M12 D-Code, 4-pin, Female M12-D (Conductor #): (#1) TX+/PoE V+, (#2) RX+/ PoE V-, (#3) TX-/PoE V+, (#4) RX-/ PoE V- • 1000 Base-T/Gigabit Ethernet (Port #8~#10): 3 x M12-X Code 8-pin Female M12-X (Conductor #): (#1) 0P(DA+)/PoE V+, (#2) 0N(DA-)/PoE V+, (#3)1P(DB+)/PoE V- , (#4)1N(DB-)/PoE V-, (#5)3P(DC+) (#6)3N(DC-), (#7) 2N (DB-), (#8) 2P (DC+) • Console & USB: M12 A-Code 8-pin Female for RS-232 and USB 2.0 Host for firmware/configuration update

	• Power: M12 A-Code 4-pin Male
	• 100 Base-TX: 2-pair Cat.5E / Cat.6 FTP/STP cable, EIA/TIA 568B 100-ohm, 100Meters • 1000 Base-T: 4-pair Cat.5E/Cat.6 FTP/STP cable, EIA/TIA 568B 100Ohm, 100Meters It is recommended uses FTP/STP cable for the railway on-board application
RS-232 & USB	M12 A-Code female 8-pin connector • RS-232: TxD (Pin-1), RxD (Pin-2), Signal Ground (Pin-3) • USB Host: USB-DATA+ (Pin-5),USB-DATA- (Pin-6), USB-5V(Pin-7), USB-GND (Pin-8)
LED Indicators	100Mbps (Port 1~7): Link (Green on)/Activity (Green Blinking) 1000Mbps (Port 8~10): Link (Green on)/Activity (Green Blinking) PoE (IEEE 802.3af/ Green): Power forwarding (Green on), PoE Detection (Green Blinking) PoE (IEEE 802.3at/ Blue): Power forwarding (Blue on), PoE Detection (Blue Blinking) Power: System Power Ready (Green on) Sys: System Ready (Green on) System Updating (Green Blinking) R.S.: Ring Normal(Green on)/ Wrong ring port connective(Green blinking) Ring abnormal (Amber on)/ Device's ring port disconnect (Amber blinking)
Power Requirement	
System Power	• JetNet 6910G-M12 HVDC Typical Input voltage: DC 110V (Un), Variation voltage 77V (0.7Un)~137.5V (1.25Un) • JetNet 6910G-M12 LVDC Typical Input voltage: DC24V (Un), Variation voltage 16.8V (0.7Un)~30V (1.25Un)
Power consumption	HVDC: 25Watts without PoE/PD loading LVDC: 20Watts without PoE /PD loading
Mechanical	
Installation	Wall Mounting

Enclosure Material	Steel Metal with textured paint
Ingress Protection	IP-30
Dimension (mm)	145.2 mm (H) x 198 mm (W) x 120 mm (D)
Environmental	
Operating Environment	-40°C~70°C (100Watts PoE/PD Loading), 0~90%, Non-condensing
Storage Environment	-40°C~80°C, 0~90% Non-Condesing
Hi-Pot	AC 1.2KV for ports-power, power-case
Approvals	
Railway Standard	EN50155, IEC 61373, EN50121-3-2
EMC	EMI: EN50121-3-2/EN50121-1, FCC Class A, IEC/EN61000-6-4 EMS:EN50121-3-2/EN50121-1, IEC/EN61000-6-2 IEC/EN61000-4-2,IEC/EN61000-4-4, IEC/EN61000-4-5, IEC/EN61000-4-6, IEC/EN61000-4-8, IEC/EN61000-4-9
Variation/Shock	IEC 61373
Warranty	5 Years

5.3 Revision History

Edition	Date	Modifications
V1.0	Aug. 11 2017	The 1st version.

5.4 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 Outstanding

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