Korenix JetNet 5628G/5828G Series
IEC61850-3 Modular Managed Ethernet Switch

User Manual

Version 1.4

Jun. 2011

korenix

www.korenix.com

Korenix JetNet 5628G/5828G
Industrial Modular Managed Ethernet Switch
User's Manual

Copyright Notice

Federal Communications Commission (FCC) Statement

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

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

Index

1 Introduction

Welcome to Korenix *JetNet 5628G/5828G* Industrial Modular Managed Ethernet Switch User Manual. Following topics are covered in this chapter:

1.1 Overview

JetNet 5628G/5828G is an IEC61850-3 Modular Managed Ethernet Switch, equipped with 4 on-board Gigabit RJ45 / MINI GBIC combo ports plus 3 modular slots for maximum 24 10/100 Base-TX Ports or 18 100Base-FX Fiber interfaces ports. The JNM5 series modules are flexible for different port volume, media types and application needs.

JetNet 5628G/5828G, a special design for substation automation and industrial control room, is compliant with the IEC61850-3, IEEE1613 high level environmental certifications. JetNet 5628G/5828G has the capability of forwarding Data, GOOSE, SCADA message without any loss or collision. JetNet 5628G/5828G also pass the NEMA TS-2 and EN50121-4 certification which are requested in Transportation and Railway market.

The advantage of choosing JetNet 5628G/5828G is that the switch supports on board 4 gigabit ports which allow users to trunk up to 8G uplink bandwidth or to form 2 independent Gigabit rings. The 24 100M interface allows to form 12 100M rings for a reliable network redundancy. This is the Korenix MultiRing redundancy design. The recovery time when ring failure can still remains 10ms high performance.

The JetNet 5628G/5828G series also supports the advanced management, control and security requirements in power substations and control rooms, such as the VLAN, QoS, IGMP, layer 2/4 Access Control List, 802.1x, SNMP V3, LLDP, etc. The JetNet 5828G support Layer 3 routing features, such as static route, dynamic unicast routing protocols, RIP and OSPF, dynamic multicast routing protocol, DVMRP and VRRP for router redundancy. With all the layer 2 and layer 3 features complete the demand and greatly satisfy technicians' requests.

The JetNet 5628G/5828G Series include below models with the different power input types. The model name and power input type is listed as below.

JetNet 5628G IEC61850-3 24+4G Modular Managed Ethernet Switch

Power Input: 1 x 85-264VAC/88-370VDC, Standard AC Plug + 2 x 24/48VDC

JetNet 5628G-2AC IEC61850-3 24+4G Modular Managed Ethernet Switch with Dual AC

input, Power Input: 2 x 85-264VAC/88-370VDC, Standard AC Plug

JetNet 5628G-2HDC IEC61850-3 24+4G Modular Managed Ethernet Switch with Dual 88-370VDC input, Power Input: 2 x 85-264VAC/88-370VDC, 3 Pin Terminal Block

JetNet 5828G IEC61850-3 24+4G Layer 3 Modular Managed Ethernet Switch

Power Input: 1 x 85-264VAC/88-370VDC, Standard AC Plug + 2 x 24/48VDC

JetNet 5828G-2AC IEC61850-3 24+4G Layer 3 Modular Managed Ethernet Switch with Dual AC input, Power Input: 2 x 85-264VAC/88-370VDC, Standard AC Plug

JetNet 5628G-R IEC61850-3 24+4G Modular Managed Ethernet Switch, Ethernet Ports on the Rear panel

Power Input: 2 x 85-264VAC/88-370VDC, 6-pin Terminal Block

JetNet 5828G-R IEC61850-3 24+4G Layer 3 Modular Managed Ethernet Switch, Ethernet Ports on the Rear panel

Power Input: 2 x 85-264VAC/88-370VDC, 6-pin Terminal Block

	PWR 1	**PWR 2**	**AC/HDC Connector**	**Low Voltage**	**DI/DO**
5628G 5828G	85~264VAC		1x Standard three-pronged AC plug	2x DC 24/48V	2DI + 2DO
5628G-2AC/ 5828G-2AC	85~264VAC	85~264VAC	2x Standard three-pronged AC plug		2DI + 2DO
5628G-2HDC	88~370VDC	88~370VDC	2x 3 pin Terminal Block		2DI + 2DO
5628G-R/ 5828G-R	88~370VDC	88~370VDC	6 pin Terminal Block		2 DO

Note: The PWR 1 and PWR2 can support both 85-264VAC and 88-370VDC High Voltage DC input. The AC connector is standard three-pronged AC connector, the High Voltage DC connector is 3-pin terminal block represent for L, N and PE. The LDC connector is a 4 pin terminal block for dual input.

1.2 Major Features

Korenix JetNet 5628G/5828G has the below different models as below.

Feature	5628G	5628G-R	5828G	5828G-R
IEC 61850-3 Design	V	V	V	V
Ethernet Port on the Rear		V		V
On Board free 4G combo ports	V	V	V	V
3 Flexible Modules	V	V	V	V
Max. Ring	14	14	14	14
Multiple Spanning Tree Protocol	V	V	V	V
256VLANs	V	V	V	V
8 physical priority queues	V	V	V	V
Private VLAN, QinQ	V	V	V	V
Modbus/TCP	V	V	V	V
Layer 2+ ACL, 802.1x	V	V	V	V
SNMP, LLDP & JetView Pro NMS	V	V	V	V
Layer 3 Unicast Routing Protocols - RIP, OSPF			V	V
Virtual Router Redundancy Protocol			V	V
Layer 3 Multicast Routing Protocols - DVMRP			V	V
Advanced PIM-DM/SM (coming soon)			V	V

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

1.3 Package List

Korenix JetNet 5628G/5828G Series products are shipped with following items:

JetNet 5628G/5828G (4G Combo on board, No Fast Ethernet modules, no SFP transceivers)

Rack Mount Kit

Console Cable

Power Cord

Quick Installation Guide

Document CD

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

1.4 Optional Module

Additional Fast Ethernet Modules:

JNM5-8TX: 8 ports 10/100Base-TX module

JNM5-4TX/4SFP: 4 ports 10/100TX + 4 100FX-SFP Socket

JNM5–2SFP/4MSC: 2 ports 100Base-FX + 4 ports 100Base-FX/SC Multi-mode

JNM5–2SFP/4SSC: 2 ports 100Base-FX + 4 ports 100Base-FX/SC Single-mode

Notice: The system only allow Maximum 12 SC type Fiber Links within one Switch. Less than 12 Fiber links is Korenix recommend in high temperature environment, especially no- air condition environment.

2 Hardware Installation

This chapter includes hardware introduction, installation and configuration information. Following topics are covered in this chapter:

2.1 Hardware Introduction

2.1.1 JetNet 5628G/5828G (Ethernet Ports on the Front) Series

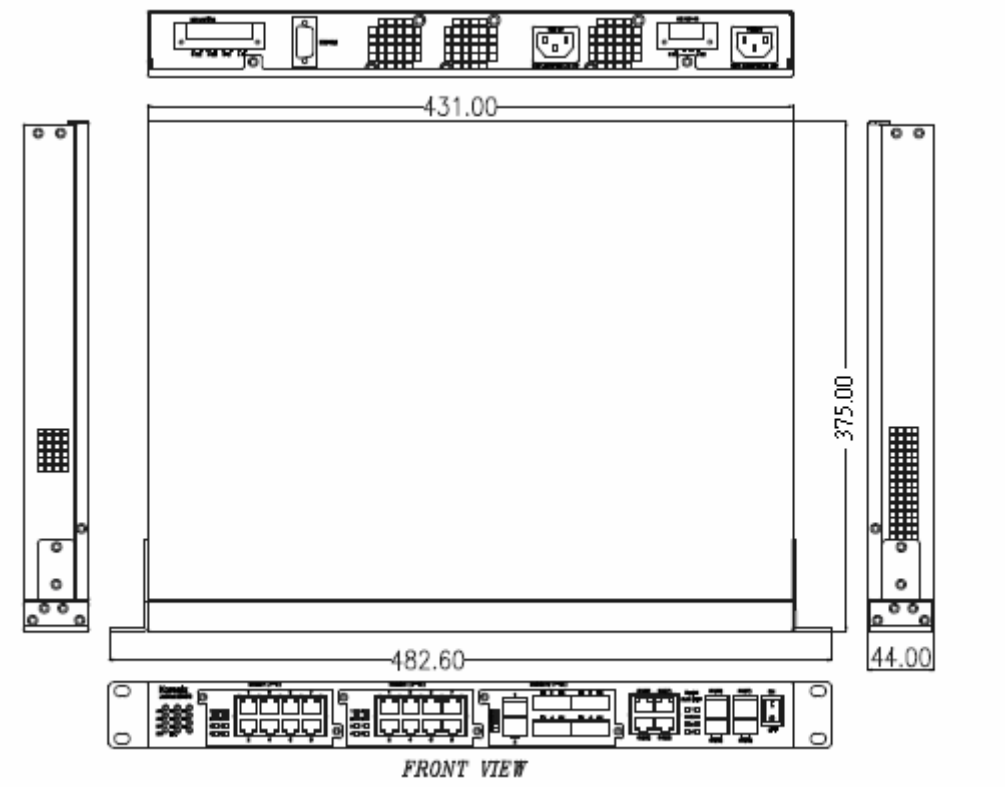
LED

System LED	Color	Port LED	Color
PWR/AC 1, PWR/AC 2	Green On/Off	Port 1~8 (JNM5-8TX)	Green/Green Blinking
LDC 1, LDC 2 (DC Power)	Green On/Off	Port 1~8 (JNM5-4TX/4SFP)	Green/Green Blinking
RDY (System Ready)	Green On/Off	Port 1~6 (JNM5-2SFP/4MSC)	Green/Green Blinking
DI 1, DI 2 (Digital Input)	Green On/Off	Port 1~6 (JNM5-2SFP/4SSC)	Green/Green Blinking
R.M. (Ring Master)	Green On/Off	Port 25~28 (Gigabit RJ45)	Green/Green Blinking
DO 1, DO 2 (Digital Output)	Red On/Off	Port 25~28 (Gigabit SFP)	Green/Green Blinking
R.F. (Ring Failure)	Red On/Off		

For one AC model, the PWR2/AC2 LED is always not light. For dual AC/HDC model, the LDC1/2 LED is always not light.

Dimension

JetNet 5628G/5828G Industrial Modular Managed Ethernet Switch dimension (W x H x D) is **44mm(H) x 431mm (W) x 375mm (D)**



Panel Layout

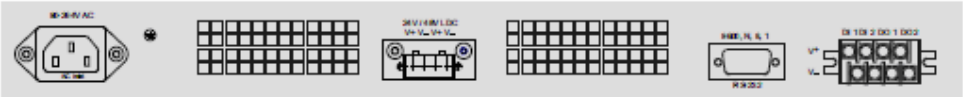
The front panel includes 3 modular slots for Fast Ethernet Module.

4 On-Board Gigabit Combo Port which support 10/100/1000 Copper and Gigabit SFP.

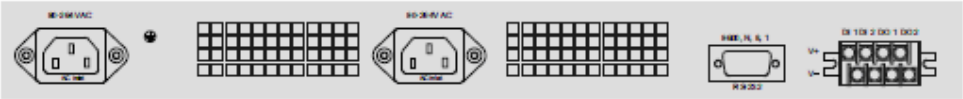
Power switch is used when you want change modular or save power.

In the back of the switch, there are AC, HDC or LDC power input socket, Digital Input/Output socket and RS232 console port.

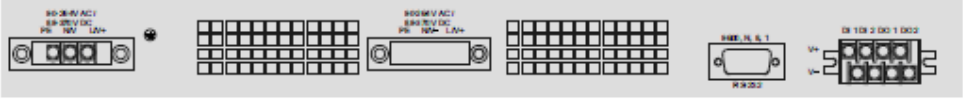
JetNet 5628G IEC61850-3 24+4G Modular Managed Ethernet Switch
Power Input: 1 x 90-264VAC+ 2 x 24/48VDC



JetNet 5628G-2AC IEC61850-3 24+4G Modular Managed Ethernet Switch with Dual AC input
Power Input: 2 x 90-264VAC



JetNet 5628G-2HDC IEC61850-3 24+4G Modular Managed Ethernet Switch with Dual 88-370VDC input
Power Input: 2 x 88-370VDC



2.1.1 JetNet 5628G-R/5828G-R (Ethernet Ports on the Rear) Series

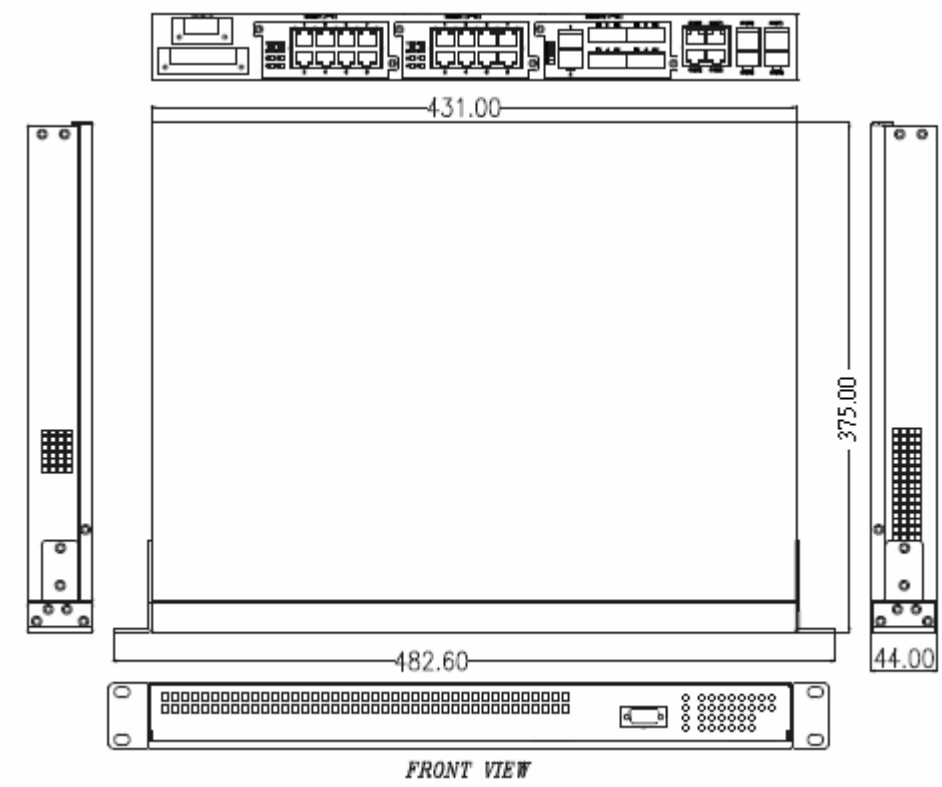
LED

LED on the Front	Color	LED on the Module	Color
P1, P2 (Power LED)	Green On/Off	Port 1~8 (JNM5-8TX)	Green/Green Blinking
DO 1 (Digital Output)	Red On/Off	Port 1~8 (JNM5-4TX/4SFP)	Green/Green Blinking
R.S. (Ring Status)	Green: Ring state is normal Green Flashing: Incorrect configuration Amber: Ring state is abnormal Amber Flashing: One of the ring ports break has been detected	Port 1~6 (JNM5-2SFP/4MSC)	Green/Green Blinking
Port 1-28	Green/Green Blinking	Port 1~6 (JNM5-2SFP/4SSC)	Green/Green Blinking

Note: Port 25-28 is gigabit combo port, there is no LED on the rear panel.

Dimension

JetNet 5628G-R/5828G-R Industrial Modular Managed Ethernet Switch dimension (W x H x D) is **44mm(H) x 431mm (W) x 375mm (D)**



Panel Layout

The front panel includes RS-232 console and LED information only.

The rear panel includes 3 modular slots for Fast Ethernet Module. 4 On-Board Gigabit Combo Port which support 10/100/1000 Copper and Gigabit SFP. And 6-pin High Voltage Power Input socket and 1 Digital Output socket

2.2 Wiring Power Inputs

JetNet 5628G/5828G provides 2 types power input, AC power input and DC power input. The front power switch can switch off all the power input at the same time.

AC Power Input

Connect the attached power cord to the AC power input connector, the available AC power input is range from 85-264VAC.

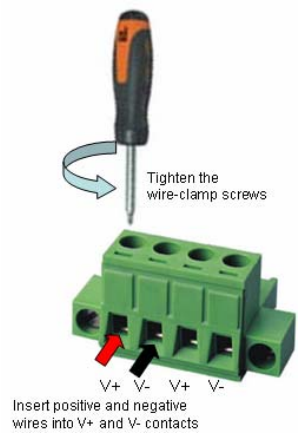
High Voltage Power Input

The power input support both 85-264VAC and 88-370VDC power input. Connect the power cord to the PE for Protective Earth, L / V+ for LINE or V+, N/V- for Neutral or V-. For high power input, tighten the wire-clamp screws to prevent DC wires from being loosened is must.

The pin assignment sequence of JetNet 5628G-R/5828G-R is N, L, PE for Power input 1 and PE, N, L for Power Input 2.

DC Power Input

Follow below steps to wire JetNet 5628G/5828G redundant DC power inputs.



1. Insert positive and negative wires into V+ and V- contacts respectively of the terminal block connector
2. Tighten the wire-clamp screws to prevent DC wires from being loosened.
3. Power 1 and Power 2 support power redundancy and polarity reverse protection functions.
4. Positive and negative power system inputs are both accepted, but Power 1 and Power 2 must apply the same mode.

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

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

Note 3: If the 2 power inputs are connected, JetNet 5628G/5828G will be powered from the highest connected voltage. The unit will alarm for loss of power, either PWR1 or PWR2.

2.3 Wiring Digital Input

JetNet 5628G/5828G provides 2 digital inputs. It allows users to connect the termination units' digital output and manage/monitor the status of the connected unit. The Digital Input pin can be pulled high or low; thus the connected equipments can actively drive these

pins high or low. The embedded software UI allows you to read and set the value to the connected device.

The power input voltage of logic low is DC 0~10V. Logic high is DC 11~30V.

Wire the digital input just like wiring the power input introduced in chapter 2.2.

The JetNet 5628G-R/5828G-R doesn't support Digital Input.

2.4 Wiring Digital Output

JetNet 5628G/5828G provides 2 digital outputs, also known as Relay Output. The relay contacts are energized (open) for normal operation and will close for fault conditions. The fault conditions include power failure, Ethernet port link break or other pre-defined events which can be configured in JetNet 5628G/5828G UI.

The default (without power) state of the Digital Output is normal **OPEN** state. The ON/OFF state is controlled by software configuration.

The **JetNet 5628G-R and JetNet 5828G-R support both OPEN and CLOSE mode.** Follow the installation guide print in the panel to wire.

Pin No.	State
1	NO (Normal Open)
2	COM
3	COM
4	NC (Normal Close)

Loosen the Digital Output screw by screw drive, then tighten the screw after digital output wire is connected.

Note: *When installed the Digital Output in your environment, remember to check the environment protection, like Surge protection of the connected device. The digital output contact of the JetNet 5628G/5828G do not provide high level Surge protection, this should be protected by connected device.*

2.5 Wiring Earth Ground

To ensure the system will not be damaged by noise or any electrical shock, we suggest you to make exact connection with JetNet 5628G/5828G with Earth Ground.

For AC input, the 3 pin include V+, V- and GND. The GND pin must be connected to the earth ground.

For High Voltage DC (HVDC) input, PE is Protective Earth pin.

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

2.6 Choosing Fast Ethernet Module

The JetNet 5628G/5828G provides several types of Fast Ethernet modules. There are 8 10/100Base-TX ports, 4 100Base-FX/SC ports plus 2 100Base-FX SFP and 4 10/100Base-TX plus 4 100Base-FX modules.

The module type includes:

JetNet 5628G Modules:

JNM5-8TX:
8 ports 10/100Base-TX module

JNM5–2SFP/4MSC:
2 ports 100Base-FX SFP + 4 ports 100Base-FX/SC Multi-mode
JNM5–2SFP/4SSC:
2 ports 100Base-FX SFP + 4 ports 100Base-FX/SC Single-mode

JNM5-4TX/4SFP: 4 ports 10/100Base-TX + 4 100FX-SFP

The modular design is more flexible for purchasing, less storage of stock and field installations. Once the distance is over 100 meters, users can exchange modules without replacing device. The 3 modules allow you connect maximum 24 10/100Base-TX Copper ports or maximum 18 100Base-FX Fiber ports.

As purchasing the JetNet 5628G/5828G, please confirm the media type and the port volume. Discuss the need with your customer and advise them your plan for the media ports is the consideration before purchasing the Ethernet module.

Note: The JetNet 5628G/5828G main board can support high temperature environment. There is no limitation to connect up to 3 x JNM5-8TX modules. Should you want connect the Fiber modules, please check the environment temperature first. The heat from the fiber interface is much higher than copper, using wide-temperature SFP transceiver is recommended. Korenix requests less than 12 Fiber connections within one JetNet 5628G/5828G box when install in high temperature environment, especially no- air condition environment. Should you need more fiber connections in one field station, please separate them to 2 or more JetNet 5628G/5828G box.

2.7 Mounting Fast Ethernet Module

2.7.1 Power down the switch or Turn off the front power switch of the 5628G/5828G series.

2.7.2 Unlock the front plate of the slot and plug the Fast Ethernet Module into the socket.

2.7.3 Turn the captive screw to lock the module.

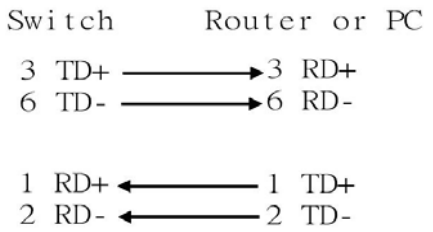
2.7.4 After locked the modules, turn on the switch.

Note: Each time when you plug or exchange module, be noticed that you should turn off the power first.

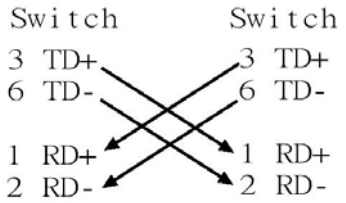
2.8 Wiring Fast Ethernet Ports

JetNet 5628G/5828G includes maximum 24 RJ-45 Fast Ethernet ports. The fast Ethernet ports support 10Base-T and 100Base-TX, full or half duplex modes. All the fast Ethernet ports will auto-detect the signal from connected devices to negotiate the link speed and duplex mode. Auto MDI/MDIX allows users to connect another switch, hub or workstation without changing straight through or crossover cables.

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



Straight-through Cabling Schematic



Cross-over Cabling Schematic

Note that Ethernet cables use pins 1, 2, 3, and 6 of an 8-pin RJ-45 connector. The signals of these pins are converted by the automatic MDI-X function, as shown in the table below:

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

Connect one side of an Ethernet cable into any switch port and connect the other side to your attached device. The LNK LED will light up when the cable is correctly connected. Refer to the **LED Indicators** section for descriptions of each LED indicator. Always make sure that the cables between the switches and attached devices (e.g. switch, hub, or workstation) are less than 100 meters (328 feet).

The wiring cable types are as below.

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

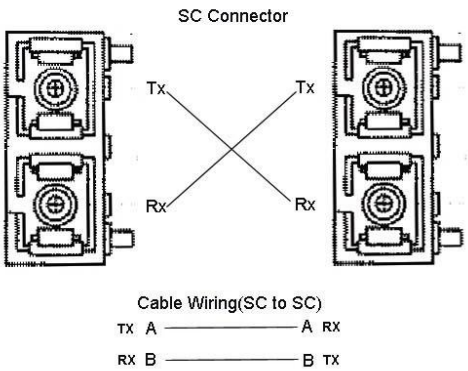
100 Base-TX: 2-pair UTP/STP Cat. 5 cable, EIA/TIA-568 100-ohm (100m)

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

2.9 Wiring Fiber Ports

100Base-FX-SC Fiber

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



JNM5-2SFP/4MSC and JNM5-2SFP/4SSC provides four 100Base-FX ports with SC type connectors (in multi-mode and single mode versions). Single-mode types have greater distance capability than multi-mode types, but single mode cable is generally more expensive.

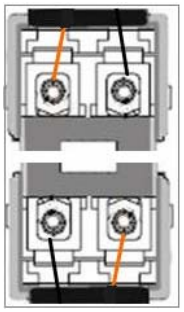
A fiber segment using single-mode cable must use 9/125 or 10/125 micrometer single-mode fiber cables. For single-mode, the connection distance can be up to 30 km.

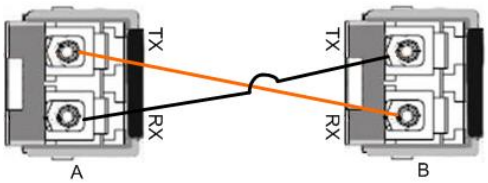
A fiber segment using multi-mode must use 50 or 62.5/125 micrometer multi-mode fiber cables. For multi-mode, the connection distance can be up to 2 km.

Small Form-factor Pluggable (SFP)

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

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





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

Laser/LED Beam.

2.10 Wiring Gigabit Combo Ports

JetNet 5628G/5828G includes 4 RJ-45 Gigabit Ethernet ports. The speed of the gigabit Ethernet port supports 10Base-T, 100Base-TX and 1000Base-TX. JetNet 5628G/5828G also equips 4 gigabit SFP ports combo with gigabit Ethernet ports. **The speed of the gigabit SFP port supports 1000Full Duplex.** The available gigabit SFP supports Gigabit Single-mode, Multi-mode, BIDI/WDM single-mode and DDM SFP transceivers. (The 100Base-FX is not supported in gigabit combo ports.)

While connect both RJ-45 and SFP at a time, the SFP will be chosen as the active media.

2.11 Wiring RS-232 Console Cable

Korenix JetNet 5628G/5828G attaches one RS-232 DB-9 to DB-9 cable in the box. Connect the DB-9 connector to the COM port of your PC, open Terminal tool and set up serial settings to 9600, N,8,1. (Baud Rate: 9600 / Parity: None / Data Bit: 8 / Stop Bit: 1) Then you can access CLI interface by console able.

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

2.12 Rack Mounting Installation

The Rack Mount Kit is attached inside the package.

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

2.2.2 Mount the device in the 19' rack by using four rack-mounting screws provided by the rack manufacturer.

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

Notice when installing:

- Temperature: Check if the rack environment temperature conforms to the specified operating temperature range.
- Mechanical Loading: Do no place any equipment on top of the switch
- Grounding: Rack-mounted equipment should be properly grounded.
- Fiber Port limitation: Maximum 12 Fiber ports are allowed to install under the highest temperature. Wide-Temperature SFP transceiver is always suggested.

2.13 Safety Warming

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

Restricted Access Location:

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

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

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

“Laite on liitettava suojamaadoitus-koskettimilla varustettuun pistorasiaan”

„Apparatet ma tilkoples jordet stikkontakt“

”Apparaten skall anslutas till jordat uttag”

3 Preparation for Management

JetNet 5628G/5828G Industrial Modular Managed Switch provides both in-band and out-band configuration methods. You can configure the switch via RS232 console cable if you don't attach your admin PC to your network, or if you lose network connection to your JetNet 5628G/5828G. This is so-called out-band management. It wouldn't be affected by network performance.

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

Following topics are covered in this chapter:

3.1 Preparation for Serial Console

In JetNet 5628G/5828G package, Korenix attached one RS-232 DB-9 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 5628G/5828G. If you lose the cable, please follow the console cable PIN assignment to find one. (Refer to the appendix).

1. Go to Start -> Program -> Accessories -> Communication -> Hyper Terminal
2. Give a name to the new console connection.
3. Choose the COM name
4. Select correct serial settings. The serial settings of JetNet 5628G/5828G are as below:

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

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

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


Switch login: admin
Password:


JetNet5628G (version 0.2.25-20090414-11:04:13).
Copyright 2006-2008 Korenix Technology Co., Ltd.

Switch>
```

3.2 Preparation for Web Interface

JetNet 5628G/5828G provides HTTP Web Interface and Secured HTTPS Web Interface for web management.

3.2.1 Web Interface

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

Before you attempt to use the embedded web interface to manage switch operation, verify that your JetNet 5628G/5828G Series Industrial Ethernet Switch is properly installed on your network and that every PC on this network can access the switch via the web browser.

1. Verify that your network interface card (NIC) is operational, and that your operating system supports TCP/IP protocol.
2. Wire DC power to the switch and connect your switch to your computer.
3. Make sure that the switch default IP address is 192.168.10.1.
4. Change your computer IP address to 192.168.10.2 or other IP address which is located in the 192.168.10.x (Network Mask: 255.255.255.0) subnet.
5. Switch to DOS command mode and ping 192.168.10.1 to verify a normal response time.

Launch the web browser and Login.

6. Launch the web browser (Internet Explorer or Mozila Firefox) on the PC.
7. Type **http://192.168.10.1** (or the IP address of the switch). And then press **Enter**.
8. The login screen will appear next.
9. Key in user name and the password. Default user name and password are both **admin**.

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

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

Note 1: IE 5.0 or later versions do not allow Java applets to open sockets by default. Users have to directly modify the browser settings to selectively enable Java applets to use network ports.

Note 2: The Web UI connection session of JetNet 5628G/5828G will be logged out automatically if you don't give any input after 30 seconds. After logged out, you should re-login and key in correct user name and password again.

3.2.2 Secured Web Interface

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

Launch the web browser and Login.

1. Launch the web browser (Internet Explorer or Mozila Firefox) on the PC.
2. Type **https://192.168.10.1** (or the IP address of the switch). And then press **Enter**.
3. The popup screen will appear and request you to trust the secured HTTPS connection distributed by JetNet 5628G/5828G first. Press **Yes** to trust it.

4. The login screen will appear next.

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

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

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

3.3 Preparation for Telnet Console

3.3.1 Telnet

Korenix JetNet 5628G/5828G 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 5628G/5828G also support SSH console. You can remotely connect to the switch by command line interface. The SSH connection can secure all the configuration commands you sent to the switch.

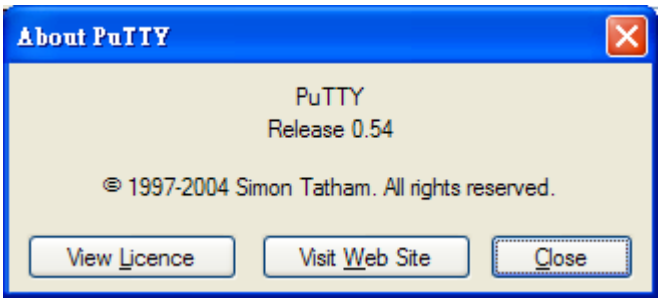
SSH is a client/server architecture while JetNet 5628G/5828G is the SSH server. When you want to make SSH connection with the switch, you should download the SSH client tool first.

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 JetNet by SSH. Note: *PuTTY is copyright 1997-2006 Simon Tatham*.

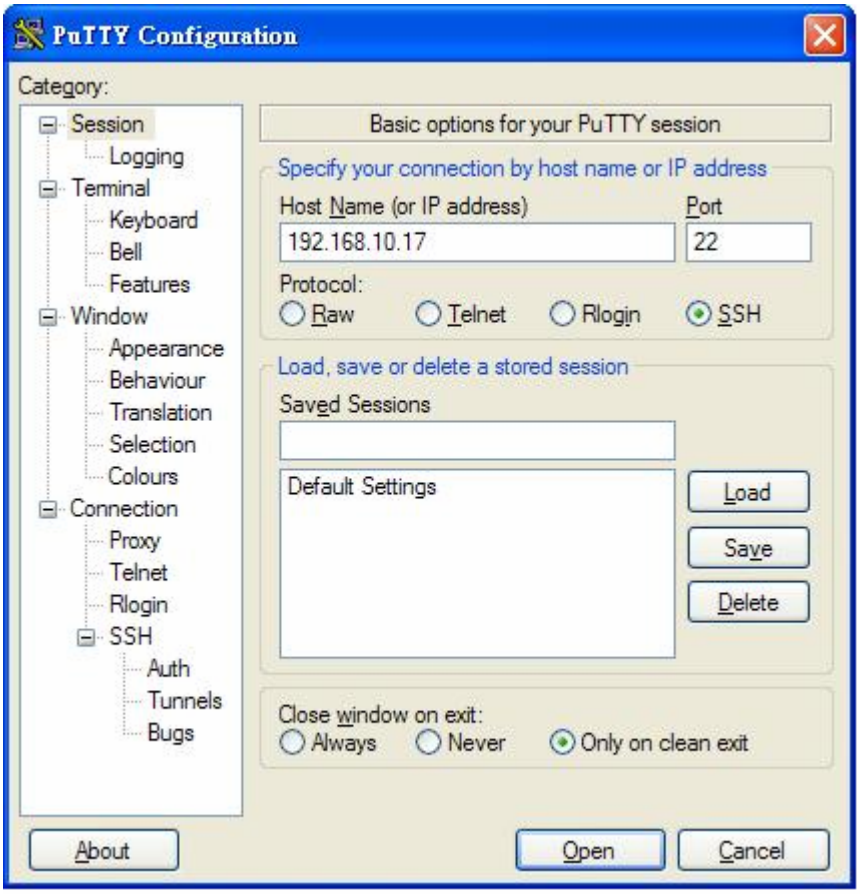
Download PuTTY: http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

The copyright of **PuTTY**

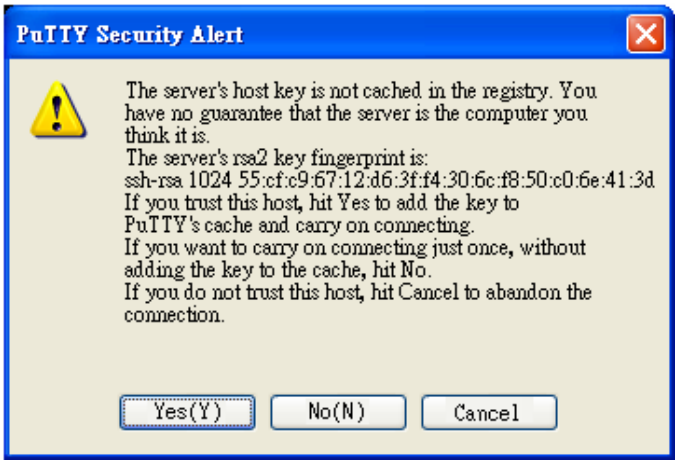


Open SSH Client/PuTTY

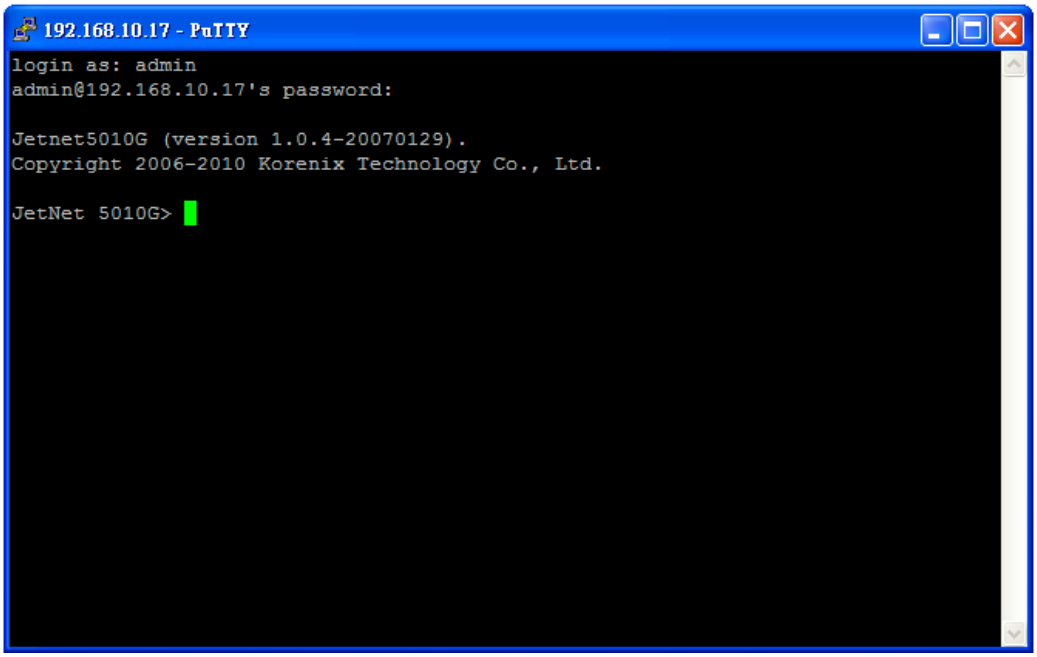
1. In the **Session** configuration, enter the **Host Name** (IP Address of your JetNet 5628G/5828G) and **Port number** (default = 22). Choose the "**SSH**" protocol. Then click on "**Open**" to start the SSH session console.



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 5628G/5828G is opened. You can see the login screen as the below figure.



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.

Note: The 5628G series is a layer 2 switch, only the IP address of the management VLAN can be accepted. The JetNet 5828G/5828G-R is a layer 3 switch. The IP address of each VLAN/IP interface can be added. The switch can accept multiple IP address for remote management.

4 Feature Configuration

This chapter explains how to configure JetNet 5628G/5828G software features. There are four ways to access the switch: Serial console, Telnet, Web browser and SNMP.

JetNet 5628G/5828G series Industrial Managed Switch provides both in-band and out-band configuration methods. You can configure the switch via RS232 console cable if you don't attach your admin PC to your network, or if you lose the network connection to your JetNet 5628G/5828G. This is so-called out-band management. It wouldn't be affected by the network performance.

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

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

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

Following topics are covered in this chapter:

4.1 Command Line Interface Introduction

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

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

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

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

```
JN5628G>
  enable      Turn on privileged mode command
  exit        Exit current mode and down to previous mode
  list        Print command list
  ping        Send echo messages
  quit        Exit current mode and down to previous mode
  show        Show running system information
  telnet      Open a telnet connection
  traceroute  Trace route to destination
```

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

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

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

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

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

Available command lists of global configuration mode.

```
Switch# configure terminal
Switch(config)#
   access-list          Add an access list entry
   administrator        Administrator account setting
   arp                  Set a static ARP entry
   clock                Configure time-of-day clock
   default              Set a command to its defaults
   end                  End current mode and change to enable mode
   exit                 Exit current mode and down to previous mode
   gvrp                 GARP VLAN Registration Protocol
   hostname             Set system's network name
   interface            Select an interface to configure
   ip                   IP information
   lacp                 Link Aggregation Control Protocol
   list                 Print command list
   log                  Logging control
   mac                  Global MAC configuration subcommands
   mac-address-table    mac address table
   mirror               Port mirroring
   no                   Negate a command or set its defaults
   ntp                  Configure NTP
   password             Assign the terminal connection password
   qos                  Quality of Service (QoS)
   relay                relay output type information
   smtp-server          SMTP server configuration
   snmp-server          SNMP server
   spanning-tree        spanning tree algorithm
   super-ring           super-ring protocol
   trunk                Trunk group configuration
   vlan                 Virtual LAN
   warning-event        Warning event selection
   write-config         Specify config files to write to
```

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

The port interface name for fast Ethernet port 1 is fa1,… fast Ethernet 7 is fa7, gigabit Ethernet port 25 is gi25.. gigabit Ethernet port 28 is gi28. Type interface name accordingly when you want to enter certain interface configuration mode.

Type **exit** to leave.

Type **?** to see the command list

Available command lists of the global configuration mode.

```
Switch(config)# interface fa1
Switch(config-if)#
   acceptable          Configure 802.1Q acceptable frame types of a port.
   auto-negotiation    Enable auto-negotiation state of a given port
   description         Interface specific description
   duplex              Specify duplex mode of operation for a port
   end                 End current mode and change to enable mode
   exit                Exit current mode and down to previous mode
   flowcontrol         Set flow-control value for an interface
   garp                General Attribute Registration Protocol
   ingress             802.1Q ingress filtering features
   lacp                Link Aggregation Control Protocol
   list                Print command list
   loopback            Specify loopback mode of operation for a port
   mac                 MAC interface commands
   mdix                Enable mdix state of a given port
   no                  Negate a command or set its defaults
   qos                 Quality of Service (QoS)
   quit                Exit current mode and down to previous mode
   rate-limit          Rate limit configuration
   shutdown            Shutdown the selected interface
   spanning-tree       spanning-tree protocol
   speed               Specify the speed of a Fast Ethernet port or a Gigabit
Ethernet port.
   switchport          Set switching mode characteristics
```

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

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

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

The command lists of the VLAN interface configuration mode.

```
Switch(config)# interface vlan 1
Switch(config-if)#
   description   Interface specific description
   end           End current mode and change to enable mode
   exit          Exit current mode and down to previous mode
   ip            Interface Internet Protocol config commands
   list          Print command list
   no            Negate a command or set its defaults
   quit          Exit current mode and down to previous mode
   shutdown      Shutdown the selected interface
```

Summary of the 5 command modes.

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

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

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

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

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

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

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

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

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

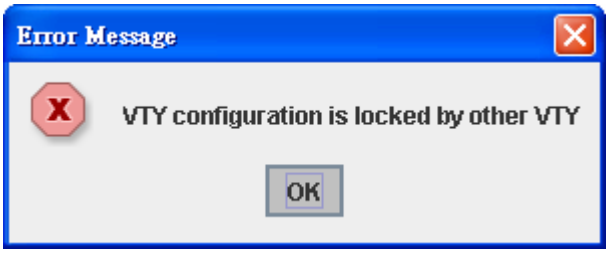
Ctrl+C To stop executing the unfinished command.

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

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

Ctrl+Z To exit configuration mode.

Alert message when multiple users want to configure the switch. If the administrator is in configuration mode, then the Web users can't change the settings. JetNet 5628G/5828G allows only one administrator to configure the switch at a time.



4.2 Basic Setting (Y2011, 0604)

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

Following commands are included in this group:

4.2.1 Switch Setting

4.2.2 Admin Password

4.2.3 IP Configuration

4.2.4 Time Setting

4.2.5 Jumbo Frame

4.2.6 DHCP Server

4.2.7 Backup and Restore

4.2.8 Firmware Upgrade

4.2.9 Factory Default

4.2.10 System Reboot

4.2.11 CLI Commands for Basic Setting

4.2.1 Switch Setting

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

Figure 4.2.1.1 – Web UI of the Switch Setting

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

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

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

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

System Description: JetNet 5628G/5828G Industrial Managed Switch is the name of this product.

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

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

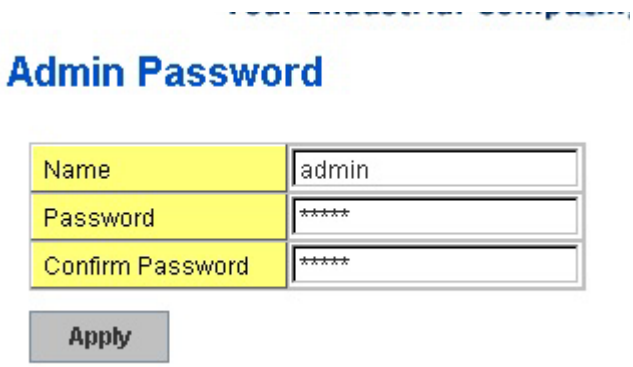
Once you finish the configuration, click on **Apply** to apply your settings.

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

4.2.2 Admin Password

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

Figure 4.2.2.1 Web UI of the Admin Password



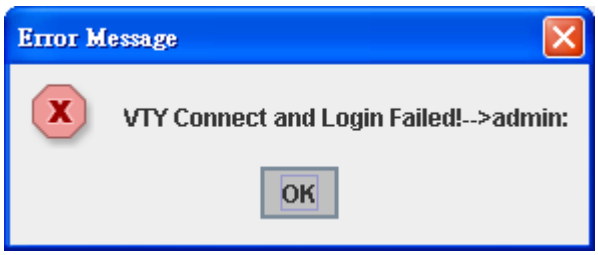
User name: You can key in new user name here. The default setting is **admin**.

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

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

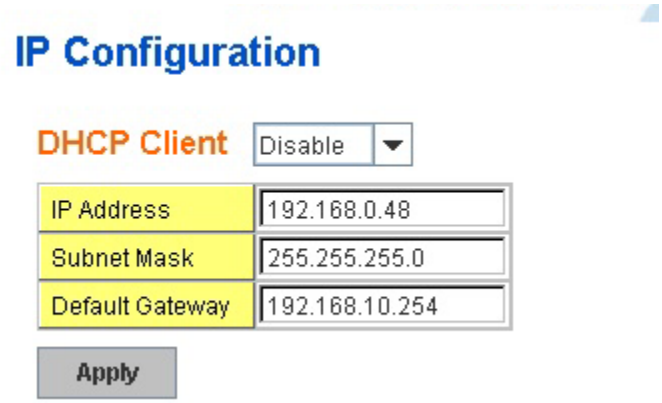
Once you finish configuring the settings, click on **Apply** to apply your configuration.

Figure 4.2.2.2 Popup alert window for Incorrect Username.



4.2.3 IP Configuration

This function allows users to configure the switch's IP address settings in JetNet 5628G Series. The JetNet 5828G series is a layer 3 switch, the IP address should be bind with VLAN interface, please go to "Routing -> IP -> IP Interface Configuration".



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

IP Address: You can assign the IP address reserved by your network for your JetNet. If DHCP Client function is enabled, you don't need to assign an IP address to the JetNet, as it will be overwritten by DHCP server and shown here. The default IP is 192.168.10.1.

Subnet Mask: You can assign the subnet mask for the IP address here. If DHCP Client function is enabled, you don't need to assign the subnet mask. The default Subnet Mask is 255.255.255.0. **Note:** In the CLI, we use the enabled bit of the subnet mask to represent the number displayed in web UI. For example, 8 stands for 255.0.0.0; 16 stands for 255.255.0.0; 24 stands for 255.255.255.0.

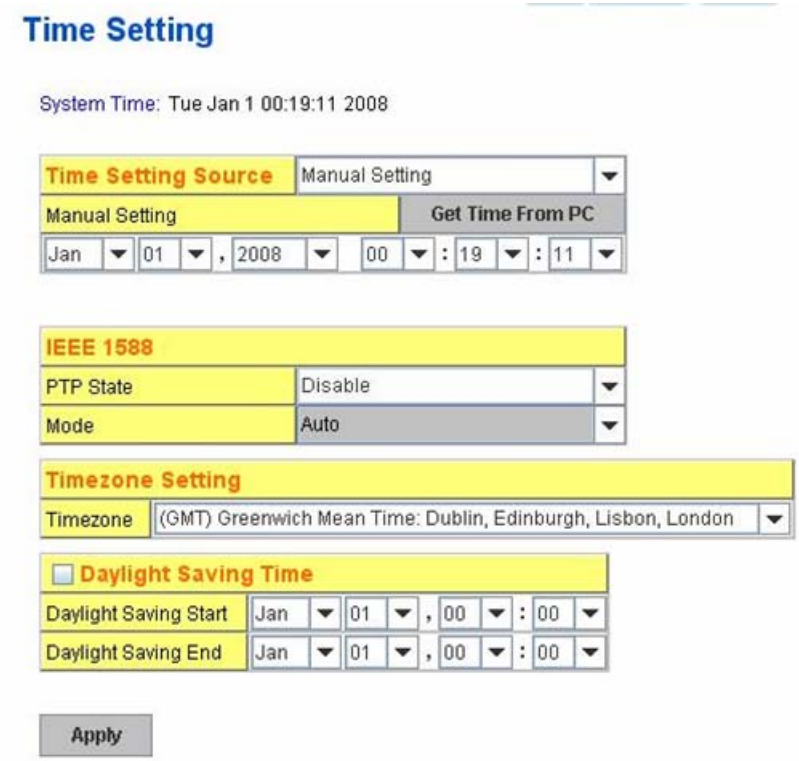
Default Gateway: You can assign the gateway for the switch here. The default gateway is 192.168.10.254. **Note:** In CLI, we use 0.0.0.0/0 to represent for the default gateway.

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

4.2.4 Time Setting

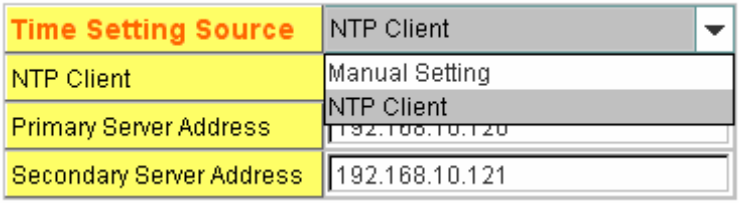
Time Setting source allow user to set the time manually or through NTP server. Network Time Protocol (NTP) is used to synchronize computer clocks on the internet. You can configure NTP settings here to synchronize the clocks of several switches on the network.

JetNet 5628G/5828G also provides Daylight Saving function.



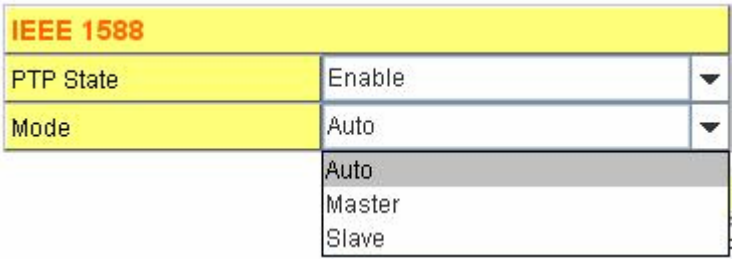
Manual Setting: User can select "**Manual setting**" to change time as user wants. User also can click the button "**Get Time from PC**" to get PC's time setting for switch.

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



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

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



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

Daylight Saving Time: Set when Enable Daylight Saving Time start and end, during the Daylight Saving Time, the device's time is one hour earlier than the actual time.

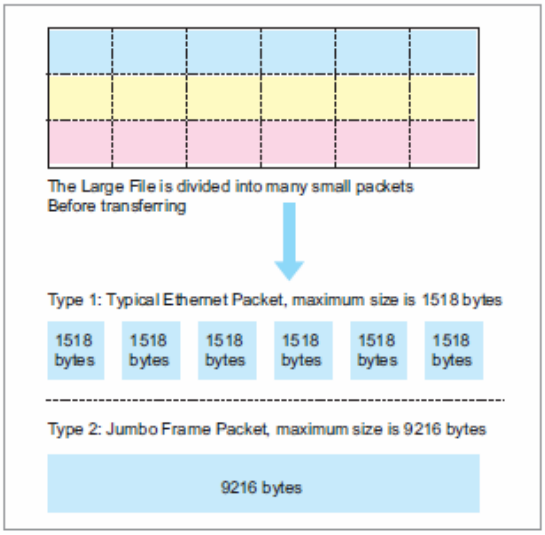
Once you finish your configuration, click on **Apply** to apply your configuration.

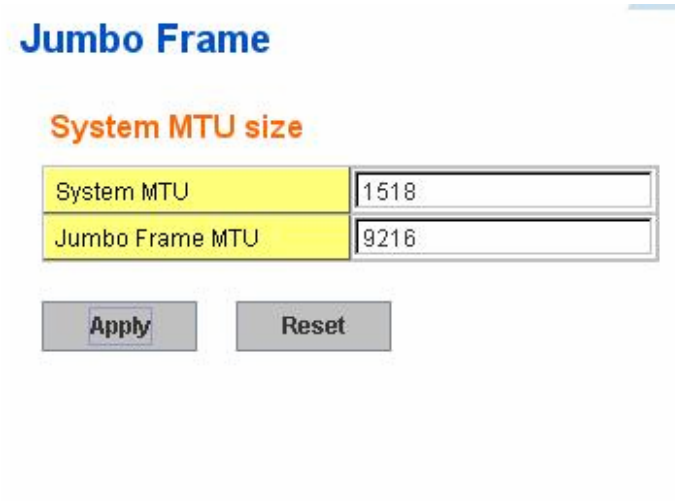
4.2.5 Jumbo Frame

What is Jumbo Frame?

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

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





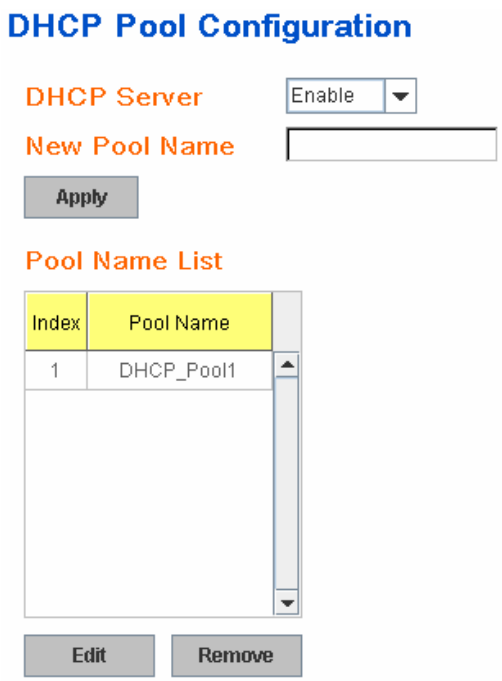
Once you finish your configuration, click on **Apply** to apply your configuration.

4.2.6 DHCP Server

You can select to **Enable** or **Disable** DHCP Server function. *JetNet 5628G/5828G* will assign a new IP address to link partners.

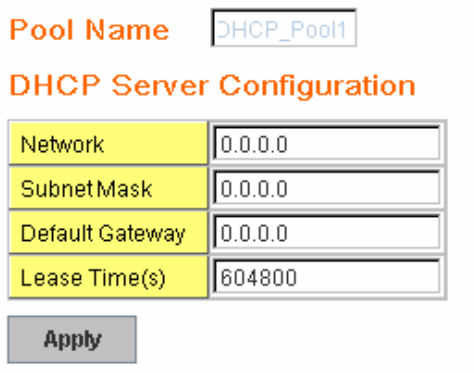
New Pool Name: Type a name for DHCP Server Pool, then press "**Apply**". The setting is only supported by JetNet 5828G series due to the layer 3 switch allows to setup multiple IP Interfaces.

Pool Name List: After pressed "**Apply**", you can see the name listed in the Pool Name List. Click the name and press "**Edit**" to edit the DHCP Server Configuration. Click "**Remove**" to remove the pool.



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.



In JetNet 5628G Series, there is only one IP pool available.

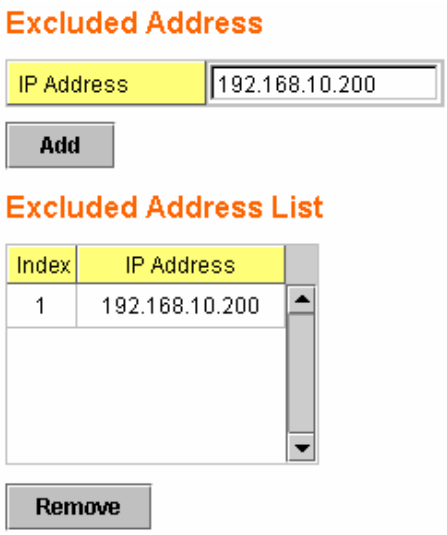
In JetNet 5828G Series, there is multiple IP pool available. The switch assigns the IP to the DHCP client automatically according to the IP subnet the DHCP client from. Configure the DHCP pool for each IP interface should you needed.

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

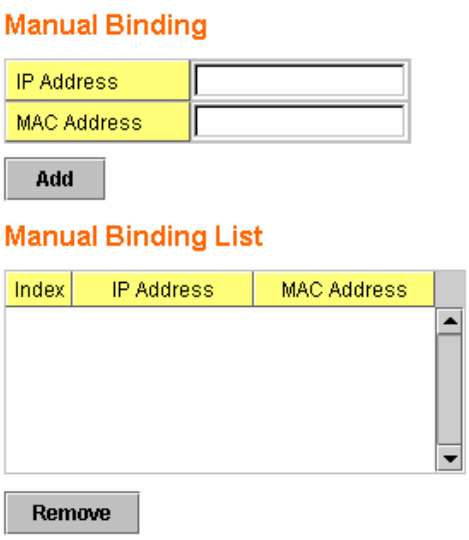
Excluded Address:

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

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



Manual Binding: *JetNet 5628G/5828G* provides a MAC address and IP address binding and removing function. You can type in the specified IP and MAC address, then click **Add** to add a new MAC&IP address binding rule for a specified link partner, like PLC or any device without **DHCP client** function. To remove from the binding list, just select the rule to remove and click **Remove**.

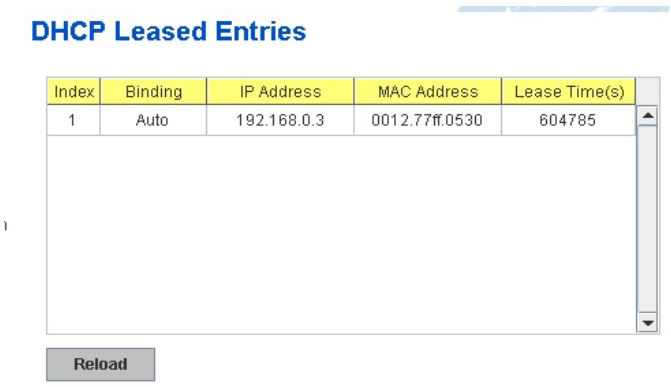


Leased Entries

DHCP Leased Entries: *JetNet 5628G/5828G* provides an assigned IP address list for user check. It will show the MAC and IP address that was assigned by *JetNet 5628G*.

In JetNet 5628G Series, there is only one IP pool available.

In JetNet 5828G series, choose the **Pool Name** and "**Apply**" first.



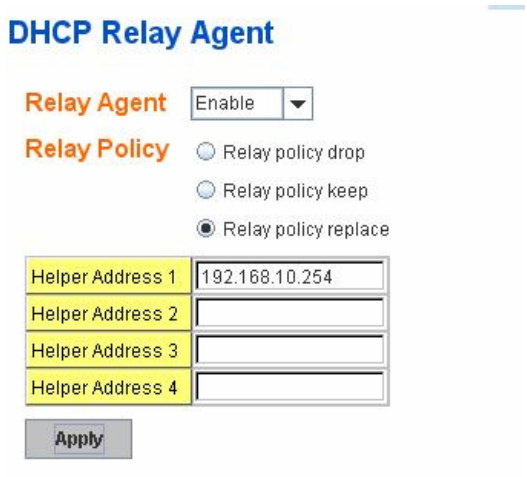
Click the **Reload** button to refresh the listing.

DHCP Relay Agent

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

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

> **Relay Agent:** Choose Enable or Disable the relay agent.
>
> **Relay Policy:** The Relay Policy is used when the DHCP request is relayed through more than one switch. The switch can drop, keep or replace the MAC address of the DHCP Request packet.
>
> **Helper Address:** Type the IP address of the target DHCP Server. There are 4 available IP addresses.



4.2.7 Backup and Restore

With Backup command, you can save current configuration file saved in the switch's flash to admin PC or TFTP server. This will allow you to go to **Restore** command later to restore the configuration file back to the switch. Before you restore the configuration file, you must place the backup configuration file in the PC or TFTP server. The switch will then download this file back to the flash.

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

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

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

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

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

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

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

Technical Tip:

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

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

Note: *Since the Fast Ethernet Port Volume of the 5628G is changeable. The Port volume may not the same when plug-in different module. In some condition when backup the switch ports' configuration from one to another, the configuration of the source unit will replace the configuration of target switch even the port volume is not the same. The port setting of the port 7, 8, 15, 16, 23 and 24 may be reset to default once the system can't find the port. Please take consideration carefully before you do backup/restore configuration.*

Figure 4.2.5.1 Main UI of Backup & Restore

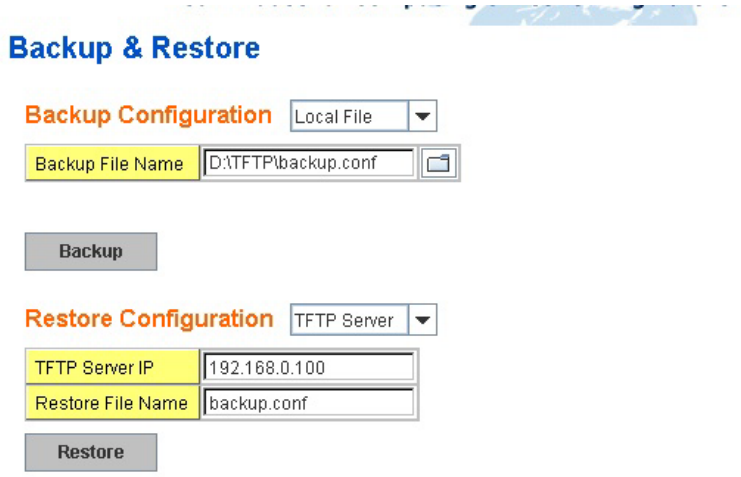
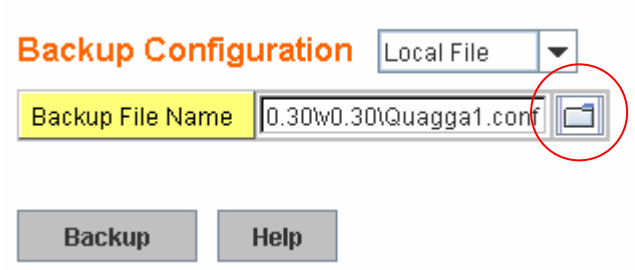


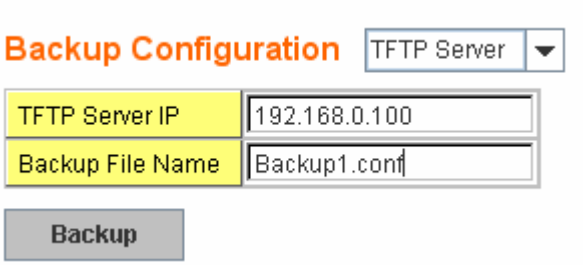
Figure 4.2.5.2 Bacup/Restore Configuration – Local File mode.



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

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

Figure 4.2.5.3 Backup/Restore Configuration – TFTP Server mode



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

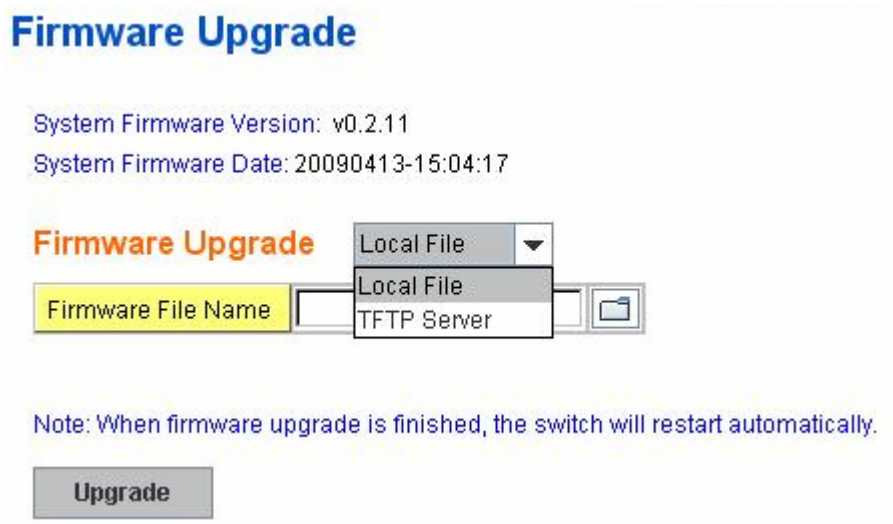
Note: point to the wrong file will cause the entire configuration missed

4.2.8 Firmware Upgrade

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

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

Figure 4.2.5.1 Main UI of Firmware Upgrade



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

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

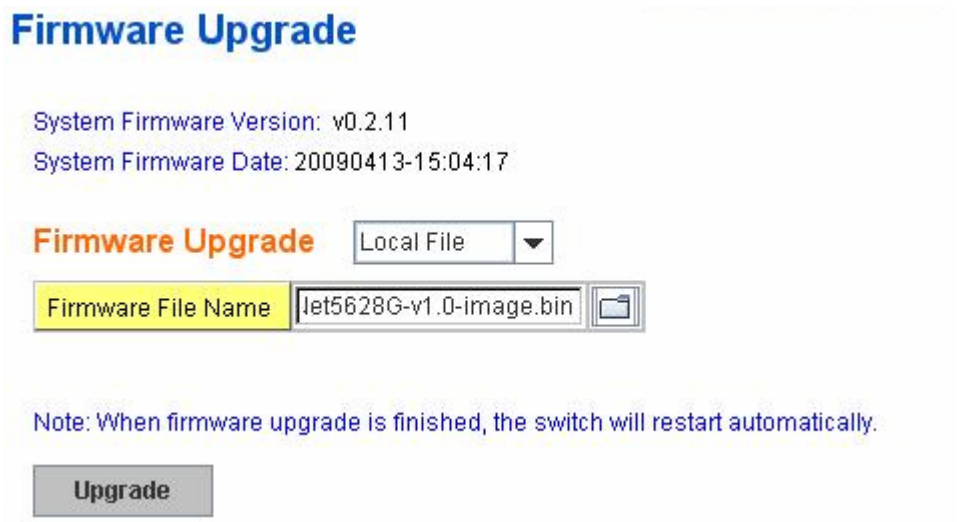
TFTP Server mode: In this mode, the switch acts as the TFTP client. Before you do so, make sure that your TFTP server is ready. And then please type the IP address of TFTP Server IP address. This mode can be used in both CLI and Web UI.

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

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

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

Figure 4.2.6.2 Firmware Upgrade – Local File mode.



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

Figure 4.2.6.3 Warning Message.

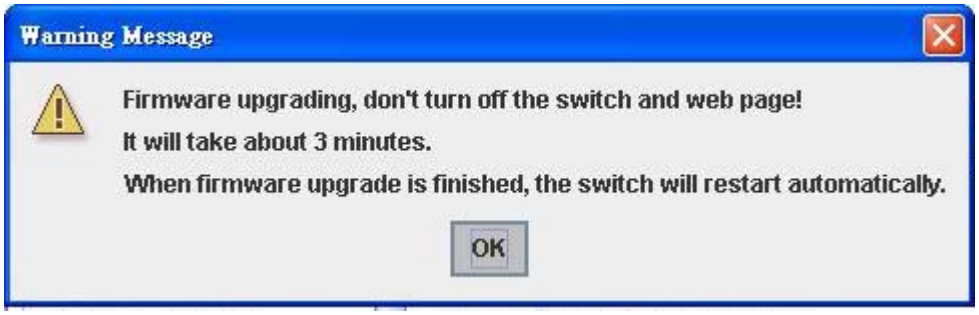
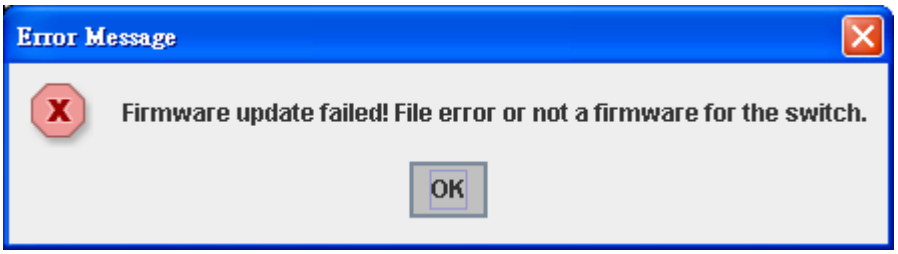
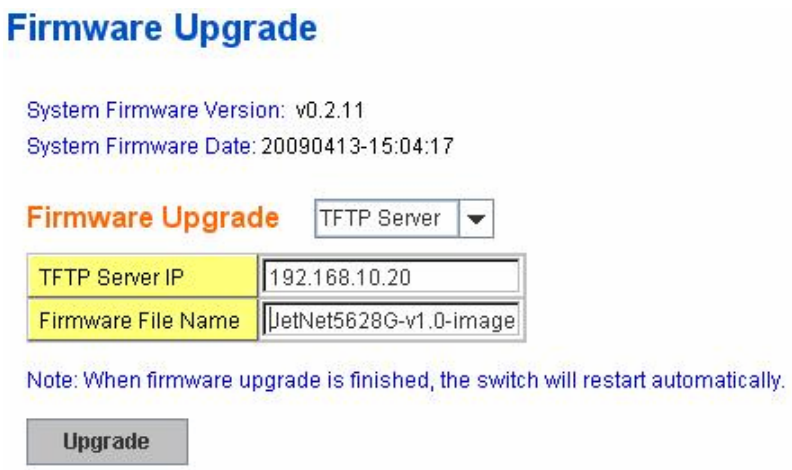


Figure 4.2.6.3 Error Message due to the file error or not a firmware for the switch.



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

Figure 4.2.6.5 Firmware Upgrade – TFTP Server mode.



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

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

4.2.9 Factory Default

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

Figure 4.2.7.1 The main screen of the Reset to Default

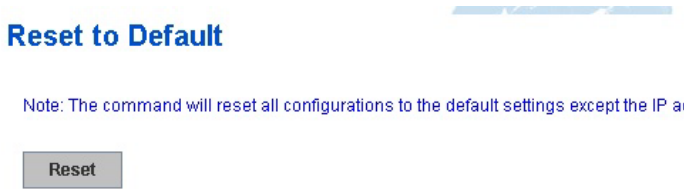


Figure 4.2.7.2 Popup alert screen to confirm the command. Click on **Yes** to start it.

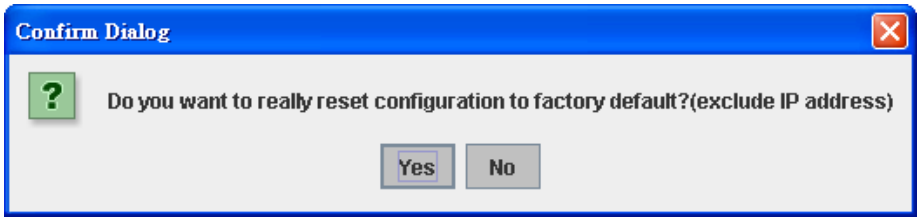
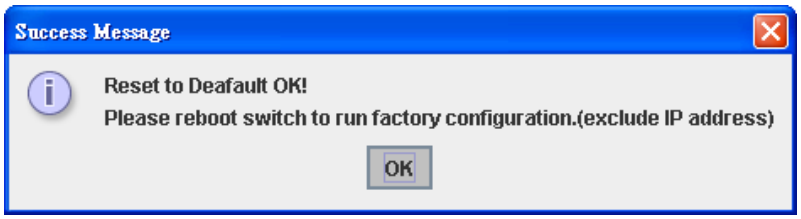


Figure 4.2.7.2 Popup message screen to show you that have done the command. Click on **OK** to close the screen. Then please go to **Reboot** page to reboot the switch.



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

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

4.2.10 System Reboot

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

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

Figure 4.2.8.1 Main screen for Rebooting

Figure 4.2.8.2 Pop-up alert screen to request confirmation. Click on **Yes**. Then the switch will be rebooted immediately.

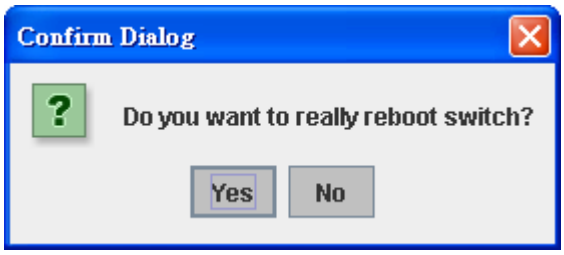
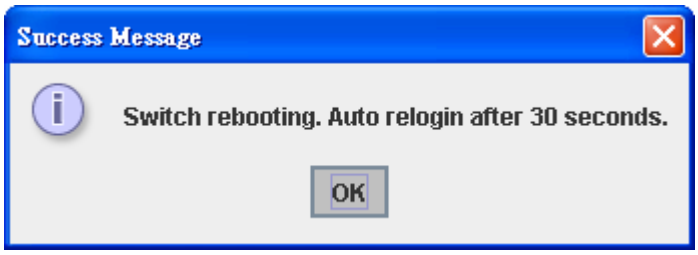


Figure 4.2.8.3 Pop-up message screen appears when rebooting the switch..



4.2.11 CLI Commands for Basic Setting

Feature	Command Line
Switch Setting	

System Name	Switch(config)# hostname WORD Network name of this system Switch(config)# hostname JN5628G/5828G SWITCH(config)#
System Location	SWITCH(config)# snmp-server location Taipei
System Contact	SWITCH(config)# snmp-server contact korecare@korenix.com
Display	SWITCH# show snmp-server name SWITCH SWITCH# show snmp-server location Taipei SWITCH# show snmp-server contact korecare@korenix.com SWITCH> show version 0.31-20061218 Switch# show hardware mac MAC Address : 00:12:77:FF:01:B0
Admin Password	
User Name and Password	SWITCH(config)# administrator NAME Administrator account name SWITCH(config)# administrator orwell PASSWORD Administrator account password SWITCH(config)# administrator orwell orwell Change administrator account orwell and password orwell success.
Display	SWITCH# show administrator Administrator account information name: orwell password: orwell
IP Configuration	
IP Address/Mask (192.168.10.8, 255.255.255.0	SWITCH(config)# int vlan 1 SWITCH(config-if)# ip address dhcp SWITCH(config-if)# ip address 192.168.10.8/24 **(DHCP Client)** SWITCH(config-if)# ip dhcp client SWITCH(config-if)# ip dhcp client renew
Gateway	SWITCH(config)# ip route 0.0.0.0/0 192.168.10.254/24
Remove Gateway	SWITCH(config)# no ip route 0.0.0.0/0 192.168.10.254/24
Display	SWITCH# show running-config …… ! interface vlan1 ip address 192.168.10.8/24 no shutdown ! ip route 0.0.0.0/0 192.168.10.254/24 !
Time Setting	
NTP Server	SWITCH(config)# ntp peer enable

	disable primary secondary SWITCH(config)# ntp peer primary IPADDR SWITCH(config)# ntp peer primary 192.168.10.120
Time Zone	SWITCH(config)# clock timezone 26 Sun Jan 1 04:13:24 2006 (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London **Note:** By typing clock timezone ?, you can see the timezone list. Then choose the number of the timezone you want to select.
IEEE 1588	Switch(config)# ptpd run <cr> preferred-clock Preferred Clock slave Run as slave
Display	SWITCH# sh ntp associations Network time protocol Status : Disabled Primary peer : N/A Secondary peer : N/A SWITCH# show clock Sun Jan 1 04:14:19 2006 (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London SWITCH# show clock timezone clock timezone (26) (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London Switch# show ptpd PTPd is enabled Mode: Slave
Jumbo Frame	
Jumbo Frame	Switch(config)# system mtu jumbo <1500-9216> Switch(config)# system mtu jumbo 9000
DHCP Server – JetNet 5628G Series (Go to next topic for JetNet 5828G)	
DHCP Commands	Switch(config)# router dhcp Switch(config-dhcp)# default-router DHCP Default Router end Exit current mode and down to previous enable mode exit Exit current mode and down to previous mode ip IP protocol lease DHCP Lease Time list Print command list network dhcp network no remove quit Exit current mode and down to previous mode service enable service
DHCP Server Enable	Switch(config-dhcp)# service dhcp <cr>
DHCP Server IP Pool	Switch(config-dhcp)# network

(Network/Mask)	A.B.C.D/M network/mask ex. 10.10.1.0/24 Switch(config-dhcp)# network 192.168.10.0/24
DHCP Server – Default Gateway	Switch(config-dhcp)# default-router A.B.C.D address Switch(config-dhcp)# default-router 192.168.10.254
DHCP Server – lease time	Switch(config-dhcp)# lease TIME second Switch(config-dhcp)# lease 1000 (1000 second)
DHCP Server – Excluded Address	Switch(config-dhcp)# ip dhcp excluded-address A.B.C.D IP address Switch(config-dhcp)# ip dhcp excluded-address 192.168.10.123 <cr>
DHCP Server – Static IP and MAC binding	Switch(config-dhcp)# ip dhcp static MACADDR MAC address Switch(config-dhcp)# ip dhcp static 0012.7700.0001 A.B.C.D leased IP address Switch(config-dhcp)# ip dhcp static 0012.7700.0001 192.168.10.99
DHCP Relay – Enable DHCP Relay	Switch(config-dhcp)# ip dhcp relay information option Option82 policy Option82 Switch(config-dhcp)# ip dhcp relay information option
DHCP Relay – DHCP policy	Switch(config-dhcp)# ip dhcp relay information policy drop Relay Policy keep Drop/Keep/Replace option82 field replace Switch(config-dhcp)# ip dhcp relay information policy drop <cr> Switch(config-dhcp)# ip dhcp relay information policy keep <cr> Switch(config-dhcp)# ip dhcp relay information policy replace <cr>
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 <cr>
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
DHCP Server – JetNet 5828G Series ***The JetNet 5828G allows Multiple IP DHCP pool, the command is different than JetNet 5628G Series. See the blue wording in below.***	
DHCP Service	Switch# configure terminal Switch(config)# service dhcp -> Enable DHCP Service Switch(config)# no service dhcp -> Disable DHCP Service
IP DHCP Pool *(While configuring JetNet 5828G DHCP Server configuration, need to create DHCP pool first, then you can assign other settings for the pool.)*	Switch(config)# ip dhcp helper-address DHCP server address for relay agent pool Address Pool relay Relay Agent Switch(config)# ip dhcp pool dhcp_pool1 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
DHCP Server IP Pool (Network/Mask)	Switch(config-dhcp)# network A.B.C.D/M network/mask ex. 10.10.1.0/24 Switch(config-dhcp)# network 192.168.10.0/24
DHCP Server – Default Gateway	Switch(config-dhcp)# default-router A.B.C.D address Switch(config-dhcp)# default-router 192.168.10.254
DHCP Server – lease time	Switch(config-dhcp)# lease TIME second Switch(config-dhcp)# lease 1000 (1000 second)
DHCP Server – Excluded Address	Switch(config-dhcp)# ip dhcp excluded-address A.B.C.D IP address Switch(config-dhcp)# ip dhcp excluded-address 192.168.10.123 <cr>
DHCP Server – Static IP and MAC binding	Switch(config-dhcp)# ip dhcp static MACADDR MAC address Switch(config-dhcp)# ip dhcp static 0012.7700.0001 A.B.C.D leased IP address Switch(config-dhcp)# ip dhcp static 0012.7700.0001 192.168.10.99
DHCP Relay – Enable DHCP Relay	Switch(config-dhcp)# ip dhcp relay information option Option82 policy Option82 Switch(config-dhcp)# ip dhcp relay information option
DHCP Relay – DHCP	Switch(config-dhcp)# ip dhcp relay information policy drop Relay Policy

policy	keep Drop/Keep/Replace option82 field replace Switch(config-dhcp)# ip dhcp relay information policy drop <cr> Switch(config-dhcp)# ip dhcp relay information policy keep <cr> Switch(config-dhcp)# ip dhcp relay information policy replace <cr>
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 <cr>
DHCP Server Information	Switch# show ip dhcp server statistics DHCP Server ON [dhcp_pool1] network:192.168.10.0/24 default-router:0.0.0.0 lease time:604800 Excluded Address List IP Address ---------- 192.168.10.123 Manual Binding List IP Address MAC Address ---------- ---------- 192.168.10.99 0012.7701.0203 Leased Address List IP Address MAC Address Leased Time Remains ---------- ---------- ----------
DHCP Relay Information	Switch# show ip dhcp relay DHCP Relay Agent ON ---------- IP helper-address : 192.168.10.200 Re-forwarding policy: Replace
Backup and Restore	
Backup Startup Configuration file	Switch# copy startup-config tftp: 192.168.10.33/default.conf Writing Configuration [OK] ***Note 1:*** *To backup the latest startup configuration file, you should save current settings to flash first. You can refer to 4.12 to see how to save settings to the flash.* *Note 2: 192.168.10.33 is the TFTP server's IP and default.conf is name of the configuration file. Your environment may use different IP addresses or different file name. Please type target TFTP server IP or file name in this command.*
Restore Configuration	Switch# copy tftp: 192.168.10.33/default.conf startup-config
Show Startup Configuration	Switch# show startup-config

Show Running Configuration	Switch# show running-config
Firmware Upgrade	
Firmware Upgrade	Switch# archive download-sw /overwrite tftp 192.168.10.33 JN5628G/5828G.bin Firmware upgrading, don't turn off the switch! Tftping file JN5628G/5828G.bin Firmware upgrading .... Firmware upgrade success!! Rebooting.....
Factory Default	
Factory Default	Switch# reload default-config file Reload OK! Switch# reboot
System Reboot	
Reboot	Switch# reboot

4.3 Port Configuration

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

Following commands are included in this group:

4.3.1 Understand the port mapping

4.3.2 Port Control

4.3.3 Port Status

4.3.4 Rate Control

4.3.5 Port Trunking

4.3.6 Command Lines for Port Configuration

4.3.1 Understand the port mapping

Before configuring the port settings, understand the port number in 5628G/5828G first.

There are 3 modules which provide 24 ports. The Module 1 presents port 1- 8, always start from port 1. The module 2 presents port 9-16, always start from port 9. The module 3 presents port 17-24, always start from port 17. In CLI, use fa1, fa2…fa24 to present port 1 to port 24.

Slot / Module	Slot 1		Slot 2		Slot 3		On Board	
	Web	CLI	Web	CLI	Web	CLI	Web	CLI
JNM5-8TX	1~8	fa1~fa8	9~16	fa9~fa16	17~24	fa17~fa24	25~28	gi1~gi4
JNM5-4TX/4SFP	1~8	fa1~fa8	9~16	fa9~fa16	17~24	fa17~fa24	25~28	gi1~gi4
JNM5-2SFP/4MSC **JNM5-2SFP/4SSC**	1~6	fa1~fa6	9~14	fa9~fa14	17~22	fa17~fa22	25~28	gi1~gi4

In some condition, you may plug in fiber module, like the JNM5-2SFP/4MSC which only supports 6 ports. The port number of this module is port 1-6 in module 1, port 9-14 in module 2, port 17-22 in module 3. The last 2 port numbers, like the Port 7, 8, 15, 16, 23 and 24 will not be used.

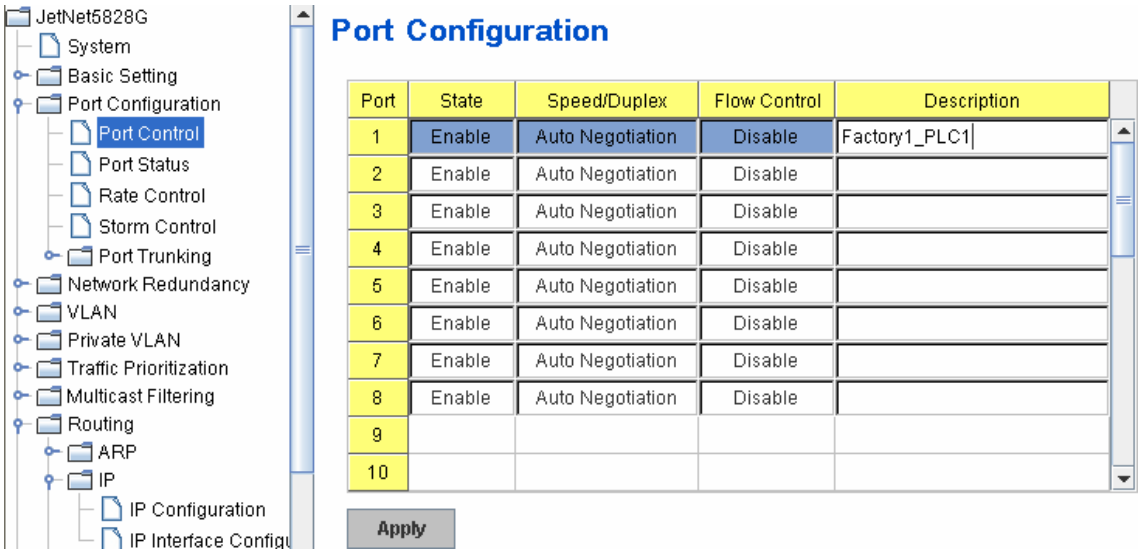
As to the Gigabit Compo ports, it always uses port 25, 26, 27 and 28. In CLI use gi25, gi26, gi27 and gi28 to present the port 25-28.

Another condition is when backup switch's configuration from one to another. The configuration of the source unit will replace the configuration of target switch even the port volume is not the same. The port setting of the port 7, 8, 15, 16, 23 and 24 may be reset to default once the system can't find the port. Please take consideration carefully before you do backup/restore configuration.

4.3.2 Port Control

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

Figure 4.3.2.1 The main Web UI of the Port Configuration .



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

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

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

Fast Ethernet Port 1~24 (fa1~fa24): AutoNegotiation, 10M Full Duplex(10 Full), 10M Half Duplex(10 Half), 100M Full Duplex(100 Full) and 100M Half Duplex(100 Half).

Gigabit Ethernet Port 25~28: (gi1~gi4): AutoNegotiation, 10M Full Duplex(10 Full), 10M Half Duplex(10 Half), 100M Full Duplex(100 Full), 100M Half Duplex(100 Half), 1000M Full Duplex(1000 Full).

The default mode is Auto Negotiation mode.

Note: The on board Gigabit SFP port (SFP 25, 26, 27 and 28) only support 1000M Full mode.

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

In **Description** column, you can add description for the port. You can know the target it attached to easier in remote.

The ports in gray area means there is no Ethernet module plugged in. You can’t configure any setting for them.

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

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

4.3.3 Port Status

Port Status shows you current port status.

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

Due to the design limitation, the Port Status fields can not display the SFP Vendor, Wavelength and Distance of the Fast Ethernet Fiber modules. It can only display the information of the on board Gigabit interfaces, ex: Gigabit SFP Port 25, 26, 27 and 28.

Port Status

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

Reload

Figure 4.3.3.2 shows you the port status of the On Board Gigabit Ethernet Ports.

Port Status

Port	Type	Link	State	Speed/Duplex	Flow Control	SFP Vendor	Wavelength	Distance
19								
20								
21								
22								
23								
24								
25	1000BASE-TX	Up	Enable	1000 Full	Disable	--	--	--
26	1000BASE	Down	Enable	--	Disable	--	--	--
27	1000BASE-TX	Up	Enable	1000 Full	Disable	--	--	--
28	1000BASE	Down	Enable	--	Disable	--	--	--

Reload

The description of the columns is as below:

Port: Port interface number.

Type: 100BASE-TX -> Fast Ethernet copper port. 100BASE-FX -> 100Base-FX Fiber Port. 1000BASE-TX -> Gigabit Ethernet Copper port. 1000BASE-LX,SX…-> Gigabit Fiber Type

(Depends on the SFP transceiver you plugged in.)

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

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

Speed/Duplex: Current working status of the port.

Flow Control: The state of the flow control.

SFP Vendor: Vendor name of the SFP transceiver you plugged.

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

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

Note: The UI can display vendor name, wave length and distance of all Korenix Gigabit SFP transceiver family. If you see Unknown information, it may mean that the vendor doesn't provide their information or that the information of their transceiver can't be read.

Note: The switch can not display the SFP Vendor, Wavelength and Distance of the Fast Ethernet Fiber ports due to hardware limitation. The SFP transceivers plugged into the JNM5-4TX/4SFP, JNM5-2SFP/4SSC and JNM5-2SFP/4MSC can't be read.

SFP DDM Information

The DDM represent for Digital Diagnostic & Monitoring.

The JetNet 5628G/5828G Gigabit SFP ports can read the **Korenix DDM SFP** information. The other vendors' DDM SFP which is not formally certificated by Korenix can't be read. The current JetNet 5628G/5828G UI can display the operating temperature, Tx Power and Rx Power of the SFP transceivers plugged in.

SFP DDM

Port	Remove	Temperature (°C)		Tx Power (dBm)		Rx Power (dBm)	
		Current	Range	Current	Range	Current	Range
26	Eject	--	--	--	--	--	--
27	Eject	58.00	0.00 ~ 80.00	-6.0	-9.0 ~ -4.0	-2.0	-30.0 ~ -4.0
28	Eject	62.00	0.00 ~ 80.00	-6.0	-9.0 ~ -4.0	-2.0	-30.0 ~ -4.0

Should you want to read the information through SNMP, please compile the private MIB first. The new firmware can be released in Q3, 2011.

4.3.4 Rate Control

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

Figure 4.3.4.1 shows you the Limit Rate of Ingress and Egress. You can type the volume step by 64Kbps in the blank. The gray area can't be changed because the port is not active.

Rate Control

Limit Packet Type and Rate

Port	Ingress Rate(Kbps)	Egress Rate(Kbps)
19	0	0
20	0	0
21	0	0
22	0	0
23	0	0
24	0	0
25	0	0
26	0	0
27	0	0
28	0	0

Apply

4.3.5 Storm Control

The Storm Control is similar to Rate Control. Rate Control filters all the traffic over the threshold you input by UI. Storm Control allows user to define the Rate for specific Packet Types.

Figure 4.3.5.1

Storm Control

Port	Broadcast	Rate (packet/sec)	DLF	Rate (packet/sec)	Multicast	Rate (packet/sec)
1	Disable	0	Disable	0	Disable	0
2	Disable	0	Disable	0	Disable	0
3	Disable	0	Disable	0	Disable	0
4	Disable	0	Disable	0	Disable	0
5	Disable	0	Disable	0	Disable	0
6	Disable	0	Disable	0	Disable	0
7	Disable	0	Disable	0	Disable	0
8	Disable	0	Disable	0	Disable	0
9	Disable	0	Disable	0	Disable	0
10	Disable	0	Disable	0	Disable	0

Apply

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

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

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

4.3.6 Port Trunking

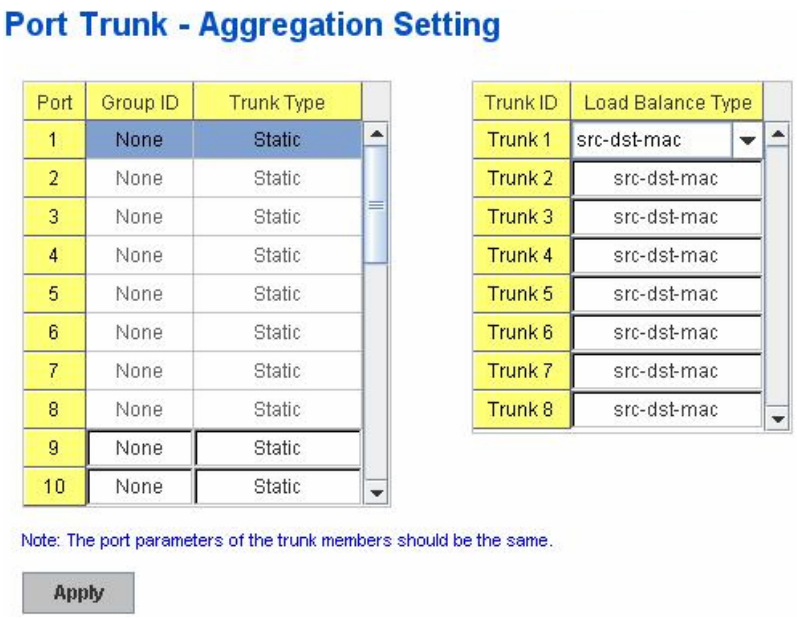
Port Trunking configuration allows you to group multiple Ethernet ports in parallel to increase link bandwidth. The aggregated ports can be viewed as one physical port so that the bandwidth is higher than merely one single Ethernet port. The member ports of the same trunk group can balance the loading and backup for each other. Port Trunking feature is usually used when you need higher bandwidth for backbone network. This is an inexpensive way for you to transfer more data.

There are some different descriptions for the port trunking. Different manufacturers may use different descriptions for their products, like Link Aggregation Group (LAG), Link Aggregation Control Protocol, Ethernet Trunk, Ether Channel…etc. Most of the implementations now conform to IEEE standard, 802.3ad.

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

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

Aggregation Setting

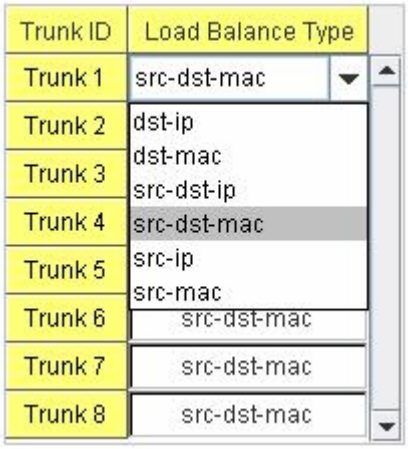


Trunk Size: The switch can support up to 8 trunk groups. Each trunk group can support up to 8 member ports. Since the member ports should use same speed/duplex, max groups for 100M ports would be 7, and 3 for gigabit ports.

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

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

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



Aggregation Status

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

Port Trunk - Aggregation Information

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

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

Type: Static or LACP set up in Aggregation Setting.

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

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

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

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.

4.3.7 Command Lines for Port Configuration

Feature	Command Line
Port Control	
Port Control – State	Switch(config-if)# shutdown -> Disable port state Port1 Link Change to DOWN interface fastethernet1 is shutdown now. Switch(config-if)# no shutdown -> Enable port state Port1 Link Change to DOWN Port1 Link Change to UP interface fastethernet1 is up now. Switch(config-if)# Port1 Link Change to UP
Port Control – Auto Negotiation	Switch(config)# interface fa1 Switch(config-if)# auto-negotiation Auto-negotiation of port 1 is enabled!
Port Control – Force Speed/Duplex	Switch(config-if)# speed 100 Port1 Link Change to DOWN set the speed mode ok! Switch(config-if)# Port1 Link Change to UP Switch(config-if)# duplex full Port1 Link Change to DOWN set the duplex mode ok! Switch(config-if)# Port1 Link Change to UP
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 Administrative Status : Enable Operating Status : Connected Duplex : Full Speed : 100 MTU: 1518 Flow Control :off Default Port VLAN ID: 1 Ingress Filtering : Disabled Acceptable Frame Type : All Port Security : Disabled Auto Negotiation : Disable Loopback Mode : None STP Status: forwarding Default CoS Value for untagged packets is 0. Mdix mode is Disable. Medium mode is Copper. *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.*
SFP Display	Switch# show sfp <cr> ddm Digital diagnostic and monitoring Switch# show sfp
DDM SFP display	Switch# show sfp ddm <cr>
Module Status	
Module Status	Switch# show module 1 Module slot 1 Module status : Not Present Module name : N/A Port information : N/A Switch# show module 2 Module slot 2 Module status : Present Module name : JNM5-4TX-4SFP Port information : fa9-16 fa9 (Fiber) fa10 (Fiber) fa11 (Fiber) fa12 (Fiber) fa13 (Copper) fa14 (Copper) fa15 (Copper) fa16 (Copper) Without module ID will display all modules' status.

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 <0-100> Limit in magabits per second (0 is no limit) Switch(config-if)# rate-limit ingress bandwidth 800 <0-1000000> Limit in kilobits per second (FE: 0-100000, GE: 0-1000000, 0 is no limit) Set the ingress rate limit 800Kbps for Port 1. Unit is Kbps.
Storm Control	
Strom Control – Packet Type	Switch(config-if)# storm-control broadcast Broadcast packets dlf Destination Lookup Failure multicast Multicast packets
Storm Control - Rate	Switch(config-if)# storm-control broadcast <0-262143> Rate limit value 0~262143 packet/sec Switch(config-if)# storm-control broadcast 10000 Enables rate limit for Broadcast packets for Port 13. Switch(config-if)# storm-control multicast 10000 Enables rate limit for Multicast packets for Port 13. Switch(config-if)# storm-control dlf 10000 Enables rate limit for Destination Lookup Failue packets for Port 13.
Port Trunking	
LACP	Switch(config)# lacp group 1 gi8-10 Group 1 based on LACP(802.3ad) is enabled! *Note: The interface list is fa1,fa3-5,gi8-10* Note: different speed port can't be aggregated together.
Static Trunk	Switch(config)# trunk group 2 fa6-7 Trunk group 2 enable ok!
Load Balance	Switch(config)# trunk load-balance group Trunk group Switch(config)# trunk load-balance group <1-8> Valid group range 1-8 Switch(config)# trunk load-balance group 1 dst-ip -> load distribution is based on the destination IP address dst-mac -> load distribution is based on the destination-MAC address src-dst-ip -> load distribution is based on the source and destination IP 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 src-mac -> load distribution is based on the source MAC address Switch(config)# trunk load-balance group 1 dst-ip <cr>

	Select the load balance type and “Enter”.
LACP – Port Setting Long/Short Timeout (New Feature in V2.4)	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.
Display - LACP	etNet 5628G/5828G# 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 GroupID Protocol Ports --------+---------+---------- 1 LACP 8(D) 9(D) 10(D) Switch# show trunk group 2 FLAGS: I -> Individual P -> In channel D -> Port Down Trunk Group GroupID Protocol Ports --------+---------+---------- 2 Static 6(D) 7(P) Switch#
Display – Load Balance	Switch# show trunk load-balance group 1 Group 1 load-balance is set to dst-ip.

4.4 Network Redundancy

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

The JetNet 5628G/5828G supports advanced Multiple Spanning Tree Protocol (MSTP). This protocol is a direct extension of RSTP. It can provide an independent spanning tree for different VLANs. It simplifies network management, provides for even faster convergence than RSTP by limiting the size of each region, and prevents VLAN members from being segmented from the rest of the group (as sometimes occurs with IEEE 802.1D STP).

Multiple Super Ring (MSR) technology is *Korenix's* 3rd generation Ring redundancy technology. This is patented and protected by *Korenix* and is used in countries all over the world. MSR ranks the fastest restore and failover time in the world, 0 ms for restore and about 5 milliseconds for failover for copper.

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

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

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

Following commands are included in this group:

4.4.1 STP Configuration

4.4.2 STP Port Configuration

4.4.3 STP Information

4.4.4 MSTP Configuration

4.4.5 MSTP Port Configuration

4.4.6 MSTP information

4.4.7 Multiple Super Ring

4.4.8 Multiple Super Ring Information

4.4.9 Command Lines for Network Redundancy

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

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

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

4.4.1 STP Configuration

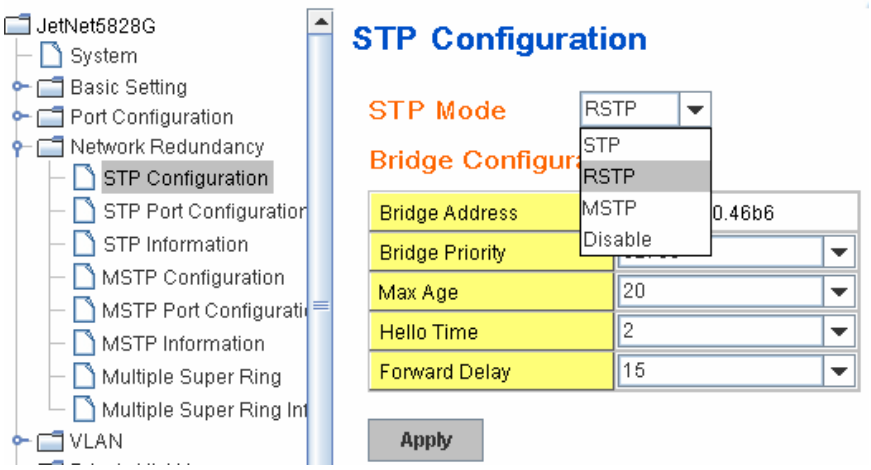
This page allows select the STP mode and configuring the global STP/RSTP Bridge Configuration.

The STP mode includes the **STP**, **RSTP**, **MSTP** and **Disable**. Please select the STP mode for your system first. The default mode is RSTP enabled.

After select the STP or RSTP mode, continue to configure the global Bridge parameters for STP and RSTP.

After select the MSTP mode, please go to MSTP Configuration page.

Figure 4.4.1.1 show the web page which allows you to select the STP mode, configure the global STP/RSTP/MSTP settings.



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

RSTP is the abbreviation of Rapid Spanning Tree Protocol. If a switch has more than one path to a destination, it will lead to message loops that can generate broadcast storms and quickly bog down a network. The spanning tree was created to combat the negative effects of message loops in switched networks. A spanning tree uses a spanning tree algorithm (STA) to automatically sense whether a switch has more than one way to communicate with a node. It will then select the best path (primary), and block the other path(s). It will also keep track of the blocked path(s) in case the primary path fails. Spanning Tree Protocol (STP) introduced a standard method to accomplish this. It is specified in IEEE 802.1D-1998. Later, Rapid Spanning Tree Protocol (RSTP) was adopted and represents the evolution of STP, providing much faster spanning tree convergence after a topology change. This is specified in IEEE 802.1w. In 2004, 802.1w is included into 802.1D-2004 version. This switch supports both RSTP and STP (all switches that support RSTP are also backward compatible with switches that support only STP).

Bridge Configuration

Priority (0-61440): RSTP uses bridge ID to determine the root bridge, the bridge with the highest bridge ID becomes the root bridge. The bridge ID is composed of bridge priority and bridge MAC address. So that the bridge with the highest priority becomes the highest bridge ID. If all the bridge ID has the same priority, the bridge with the lowest MAC address will then become the root bridge.

Note: The bridge priority value must be in multiples of 4096. A device with a lower number has a higher bridge priority. Ex: 4096 is higher than 32768.

Note: The Web GUI allows user select the priority number directly. This is the 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 JetNet is not the root bridge, and if it has not received a hello message from the root bridge in an amount of time equal to Max Age, then JetNet will reconfigure itself as a root bridge. Once two or more devices on the network are recognized as a root bridge, the devices will renegotiate to set up a new spanning tree topology.

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

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

Hello Time (1-10): Enter a value from 1 to 10 seconds here. This is a periodic timer that drives the switch to send out BPDU (Bridge Protocol Data Unit) packet to check current STP status.

The root bridge of the spanning tree topology periodically sends out a "hello" message to other devices on the network to check if the topology is "healthy". The "hello time" is the amount of time the root has waited during sending hello messages.

Forward Delay Time (4-30): Enter a value between 4 and 30 seconds. This value is the time that a port waits before changing from Spanning Tree Protocol learning and listening states to forwarding state.

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

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

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

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

4.4.2 STP Port Configuration

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

Port Configuration

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

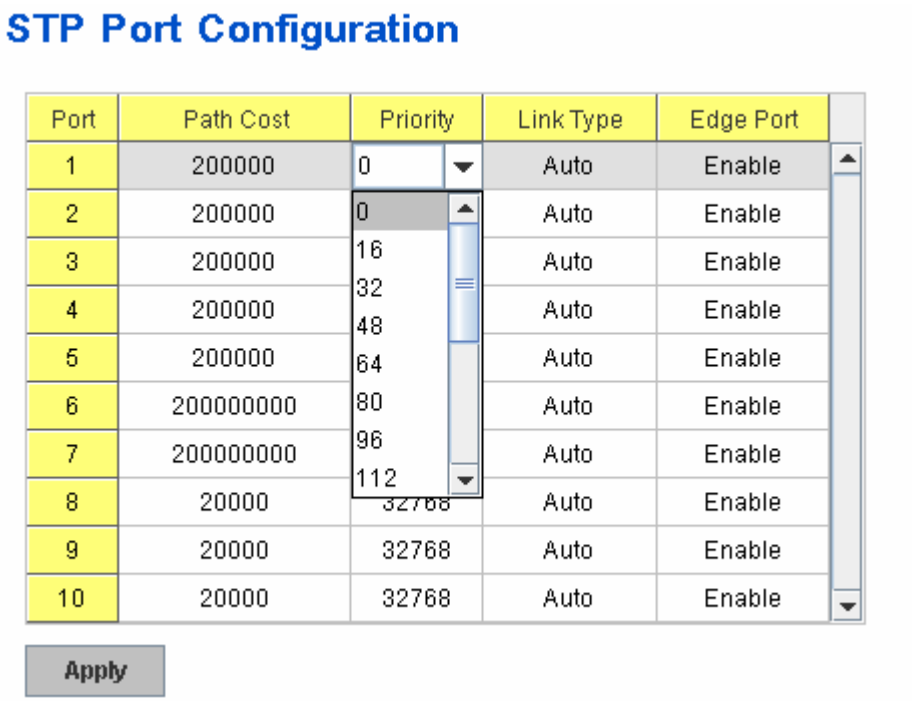
Path Cost: Enter a number between 1 and 200,000,000. This value represents the "cost" of the path to the other bridge from the transmitting bridge at the specified port.

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

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

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

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



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

4.4.3 RSTP Info

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

RSTP Information

Root Information

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

Port Information

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

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

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

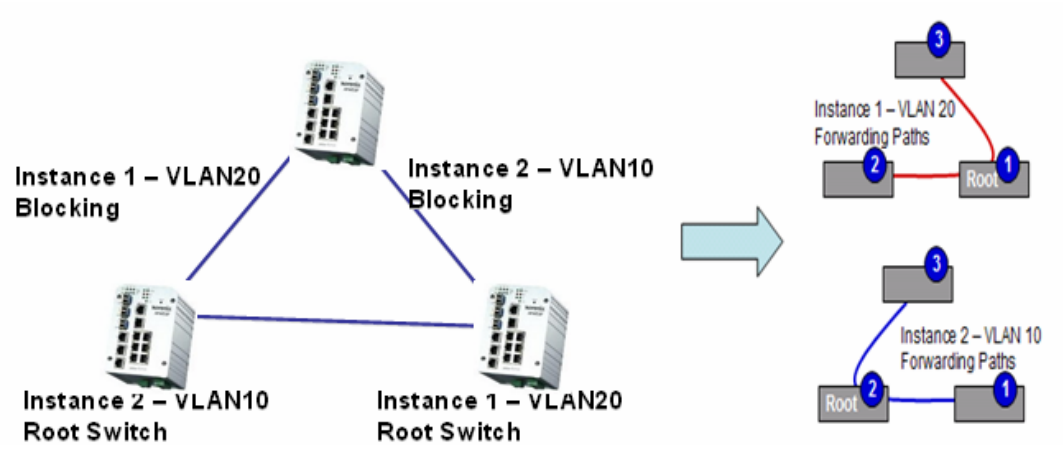
4.4.4 MSTP (Multiple Spanning Tree Protocol) Configuration

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

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

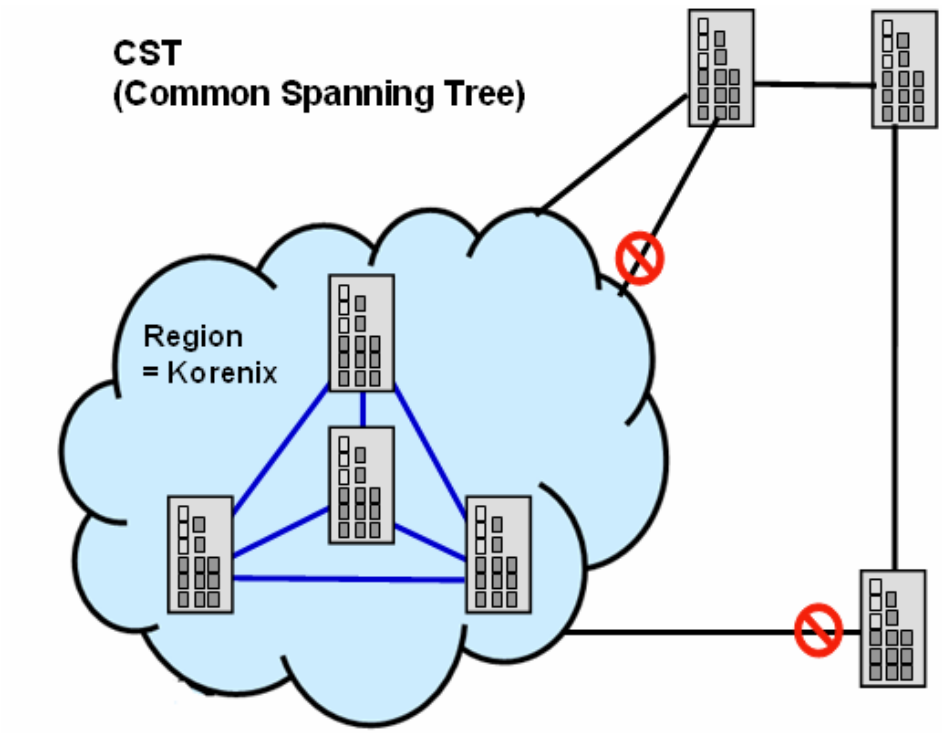
One VLAN can be mapped to a Multiple Spanning Tree Instance (MSTI). For example, the maximum Instance JetNet supports is usually 16, range from 0-15. The MSTP builds a separate Multiple Spanning Tree (MST) for each instance to maintain connectivity among each of the assigned VLAN groups. An Internal Spanning Tree (IST) is used to connect all the MSTP switches within an MST region. An MST Region may contain multiple MSTP Instances.

The figure shows there are 2 VLANs/MSTP Instances and each instance has its Root and forwarding paths.

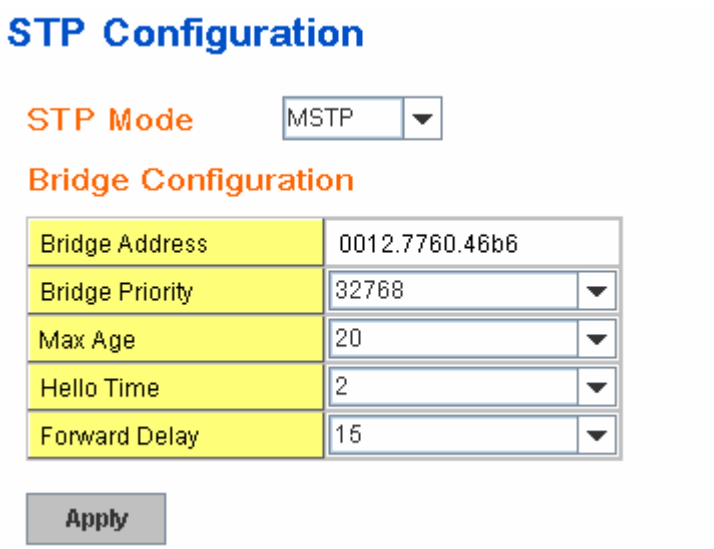


A Common Spanning Tree (CST) interconnects all adjuacent MST regions and acts as a virtual bridge node for communications with STP or RSTP nodes in the global network. MSTP connects all bridges and LAN segments with a single Common and Internal Spanning Tree (CIST). The CIST is formed as a result of 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 Configuraiton pages.

MSTP Region Configuration

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

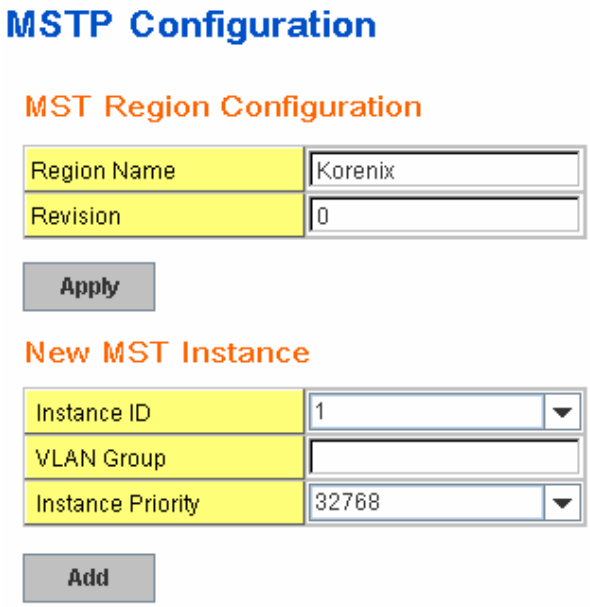
Region Name: The name for the Region. Maximum length: 32 characters.

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

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

New MST Instance

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



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

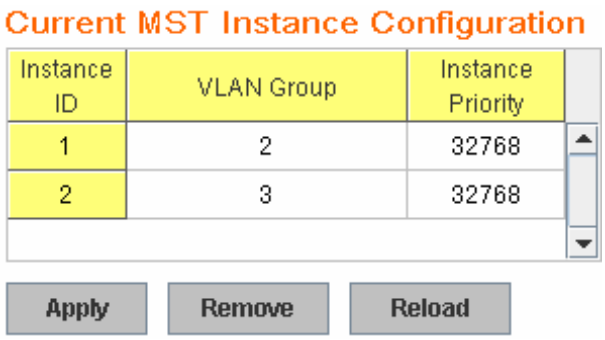
VLAN Group: Type the VLAN ID you want mapping to the instance.

Instance Priority: Assign the priority to the instance.

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

Current MST Instance Configuration

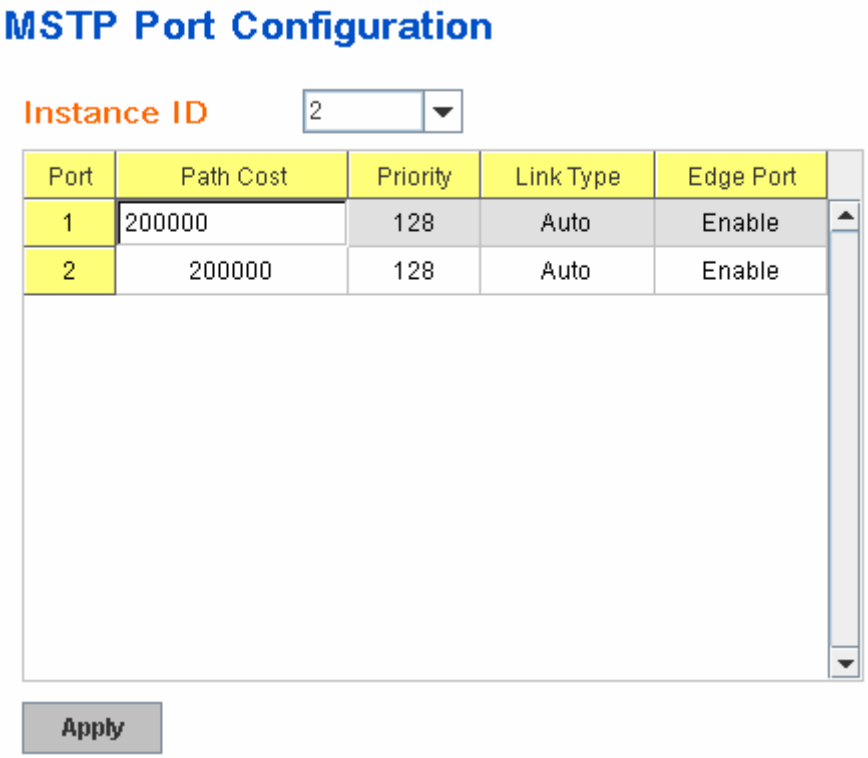
This page allows you to see the current MST Instance Configuration you added. Click on "**Apply**" to apply the setting. You can "**Remove"** the instance or "**Reload**" the configuration display in this page.



4.4.5 MSTP Port Configuration

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

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



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

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

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

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

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

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

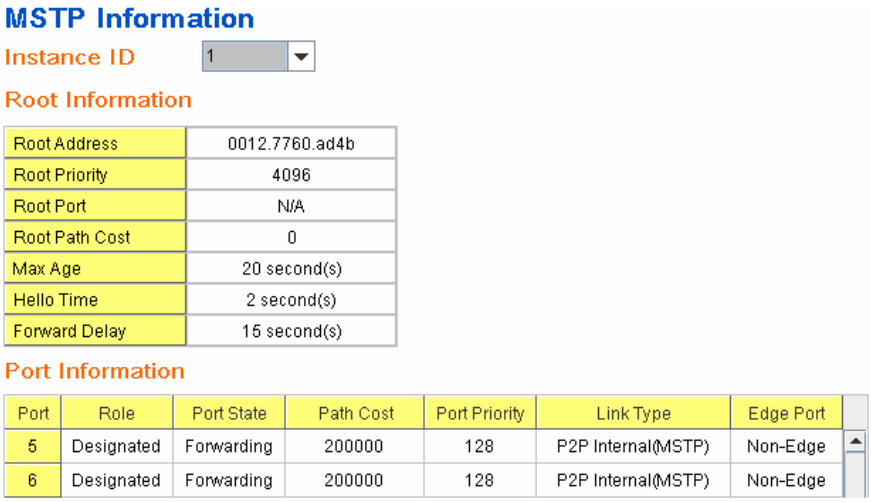
4.4.6 MSTP Information

This page allows you to see the current MSTP information.

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

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

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



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

4.4.7 Multiple Super Ring (MSR)

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

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

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

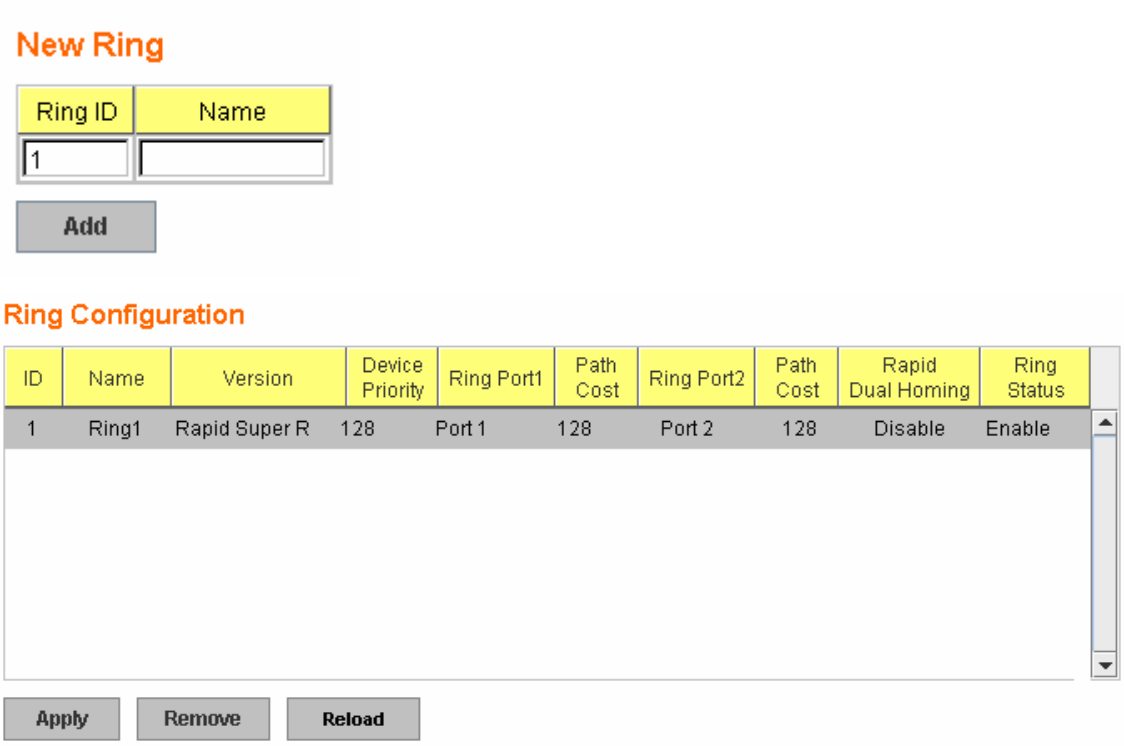
Advanced **Rapid Dual Homing (RDH)** technology also facilitates *JetNet Managed Switch* to connect with a core managed switch easily and conveniently. With RDH technology, you can also couple several Rapid Super Rings or RSTP cloud together, which is also known as Auto Ring Coupling.

TrunkRing technology allows integrate MSR with LACP/Port Trunking. The LACP/Trunk aggregated ports is a virtual interface and it can work as the Ring port of the MSR.

MultiRing is an outstanding technology Korenix can support. Multiple rings can be aggregated within one switch by using different Ring ID. The maximum Ring number one switch can support is half of total port volume. For example, the JetNet 5628G is a 24 Fast Ethernet + 4 Gigabit port design, that means maximum 14 Rings (12 x 100M Rings and 2 Gigabit Rings) can be aggregated to one JetNet 5628G. The feature saves much effort when constructing complex network architecture.

To become backwards compatible with the Legacy Super Ring technology implemented in *JetNet 4008/4508* V1 series switches, *JetNet 4510/4518/5000 Series* also supports Super Ring Client mode. The Super Ring ports can pass through Super Ring control packets extremely well and works with Super Ring.

New Ring: To create a Rapid Super Ring. Just fill in the Ring ID which has range from 0 to 31. If the name field is left blank, the name of this ring will automatically naming with Ring ID.



Ring Configuration

ID: Once a Ring is created, This appears and can not be changed.

Name: This field will show the name of the Ring. If it is not filled in when creating, it will be automatically named by the rule “RingID”.

Version: The version of Ring can be changed here. There are three modes to choose: Rapid Super Ring as default; Super ring for compatible with Korenix 1st general ring and Any Ring for compatible with other version of rings.

Device Priority: The switch with highest priority (highest value) will be automatically selected as Ring Master. Then one of the ring ports in this switch will become forwarding port and the other one will become blocking port. If all of the switches have the same priority, the switch with the biggest MAC address will be selected as Ring Master.

Ring Port1: In Rapid Super Ring environment, you should have 2 Ring Ports. No matter this switch is Ring Master or not, when configuring RSR, 2 ports should be selected to be Ring Ports. For Ring Master, one of the ring ports will become the forwarding port and the other one will become the blocking port.

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

Ring Port2: Assign another port for ring connection

Path Cost: Change the Path Cost of Ring Port2

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

In Dual Homing I released with JetNet 4000/4500 series, you have to configure additional port as Dual Homing port to two uplink switches. In Rapid Dual Homing, you don’t need to configure specific port to connect to other protocol. The Rapid Dual Homing will smartly choose the fastest link for primary link and block all the other link to avoid loop. If the primary link failed, Rapid Dual Homing will automatically forward the secondary link for network redundant. Of course, if there are more connections, they will be standby links and recover one of 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.

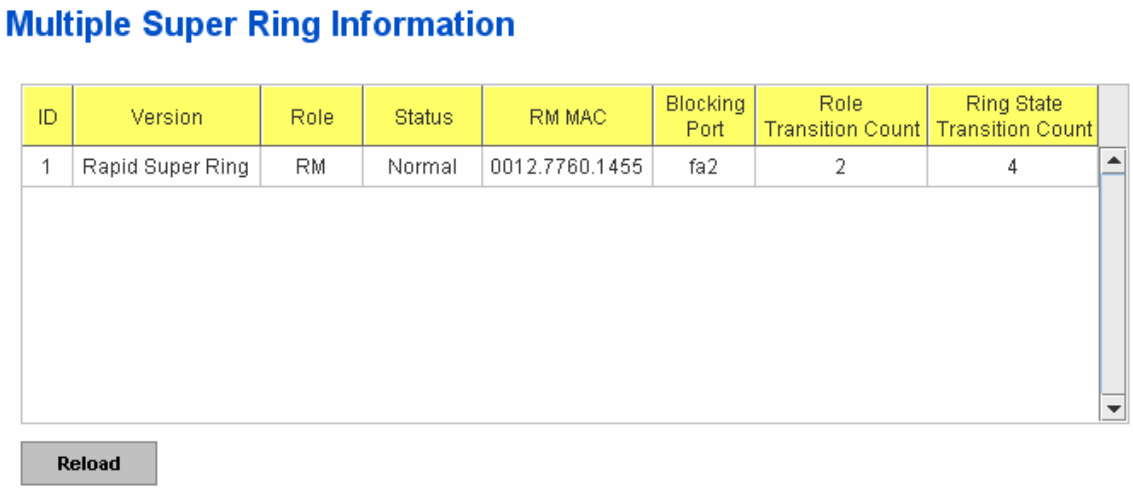
MultiRing: The MultiRing technology is one of the pattern of the MSR technology, the technology allows you to aggregate multiple rings within one switch. Create multiple ring ID and assign different ring port 1 and port 2 to each ring, thus the switch can have multiple rings in one JetNet 5628G.

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

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

4.4.8 Ring Info

This page shows the MSR information.



ID: Ring ID.

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

Role: This Switch is RM or nonRM

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

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

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

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

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

4.4.9 Command Lines:

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

	--- --- 0 1,4-4094 1 2 2 3 --- Config HMAC-MD5 Digest: 0xB41829F9030A054FB74EF7A8587FF58D ---
Remove Region Name	Switch(config-mst)# no name name configure revision revision configure instance the mst instance Switch(config-mst)# no name
Remove Instance example	Switch(config-mst)# no instance <1-15> target instance number Switch(config-mst)# no instance 2
Show Pending MST Configuration	Switch(config-mst)# show pending Pending MST configuration Name [] (->The name is removed by no name) Revision 65535 Instance Vlans Mapped --- --- 0 1,3-4094 1 2 (->Instance 2 is removed by no instance 2) --- Config HMAC-MD5 Digest: 0x3AB68794D602FDF43B21C0B37AC3BCA8 ---
Apply the setting and go to the configuration mode	Switch(config-mst)# quit apply all mst configuration changes Switch(config)#
Apply the setting and go to the global mode	Switch(config-mst)# end apply all mst configuration changes Switch#
Abort the Setting and go to the configuration mode. Show Pending to see the new settings are not applied.	Switch(config-mst)# abort discard all mst configuration changes Switch(config)# spanning-tree mst configuration Switch(config-mst)# show pending Pending MST configuration Name [korenix] (->The 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	
System RSTP Setting	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 [korenix] Revision 65535 Instance Vlans Mapped -------- ---------- 0 1,4-4094 1 2 2 3 ---------- 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 Instance Root Address Root Priority Root Cost Root Port Max age Hello Fwd 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.***
Super Ring Version	Switch(config-multiple-super-ring)# version any-ring any ring auto detection default set default to rapid super ring rapid-super-ring rapid super ring super-ring super ring

	Switch(config-multiple-super-ring)# version rapid-super-ring
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.
	Note: auto-detect is recommended for dual Homing..

Ring Info	

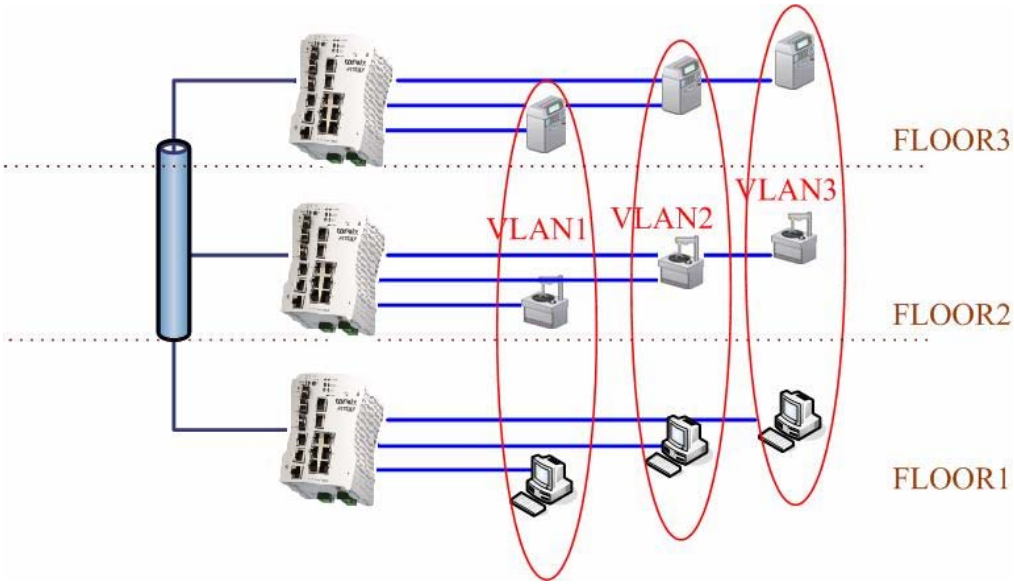
Ring Info	Switch# show multiple-super-ring [Ring ID]
	[Ring1] Ring1
	  Current Status : Disabled
	  Role : Disabled
	  Ring Status : Abnormal
	  Ring Manager : 0000.0000.0000
	  Blocking Port : N/A
	  Giga Copper : N/A
	  Configuration :
	  Version : Rapid Super Ring
	  Priority : 128
	  Ring Port : fa1, fa2
	  Path Cost : 100, 200
	  Dual-Homing II : Disabled
	  Statistics :
	  Watchdog sent 0, received 0, missed 0
	  Link Up sent 0, received 0
	  Link Down sent 0, received 0
	  Role Transition count 0
	  Ring State Transition count 1
	
	Ring ID is optional. If the ring ID is typed, this command will only display the information of the target Ring.

4.5 VLAN

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

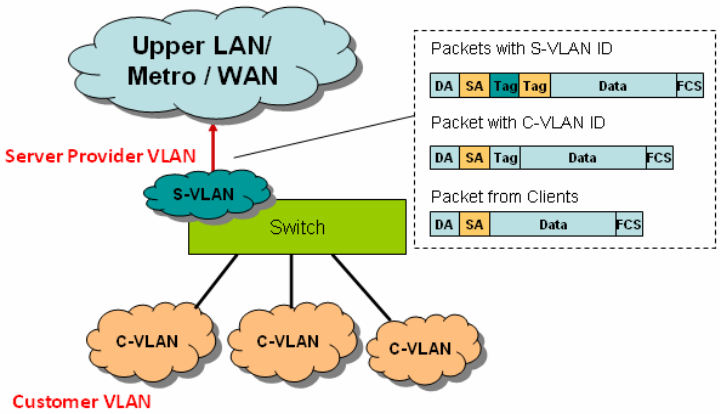
JetNet 5628G/5828G Series Industrial Ethernet Switch supports 802.1Q VLAN. 802.1Q VLAN is also known as Tag-Based VLAN. This Tag-Based VLAN allows VLAN to be created across different switches (see Figure 1). IEEE 802.1Q tag-based VLAN makes use of VLAN control information stored in a VLAN header attached to IEEE 802.3 packet frames. This tag contains a VLAN Identifier (VID) that indicates which VLAN a frame belongs to. Since each switch only has to check a frame’s tag, without the need to dissect the contents of the frame, this also saves a lot of computing resources within the switch.

Figure 4.5.1 802.1Q VLAN



QinQ

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



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

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

Following commands are included in this group:

4.5.1 VLAN Port Configuration

4.5.2 VLAN Configuration

4.5.3 GVRP Configuration

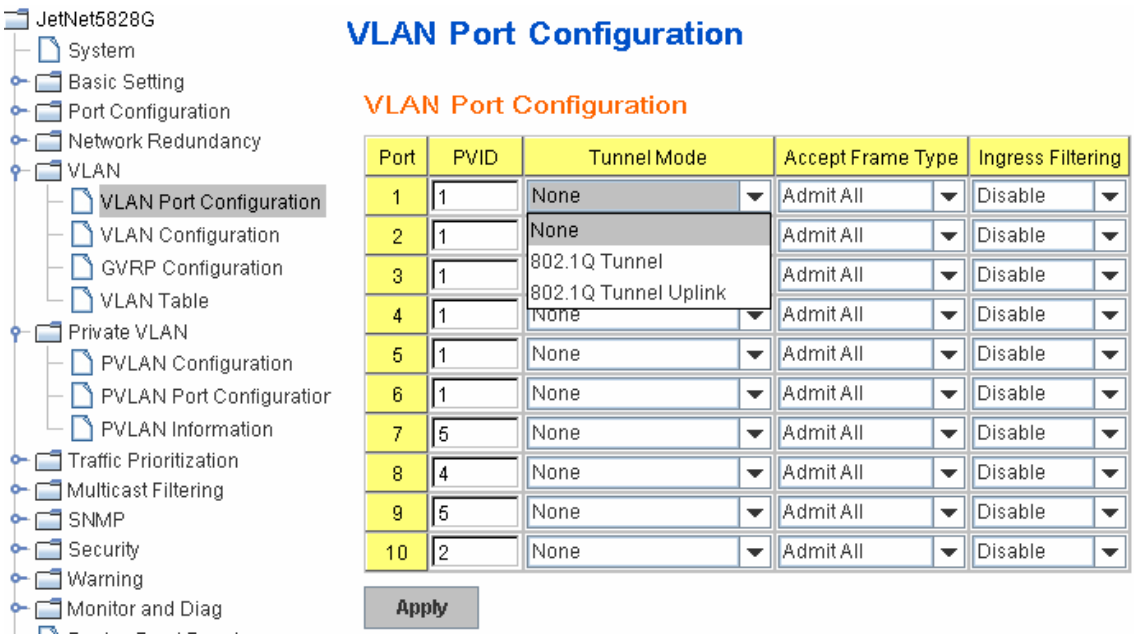
4.5.4 VLAN Table

4.5.5 CLI Commands of the VLAN

4.5.1 VLAN Port Configuration

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

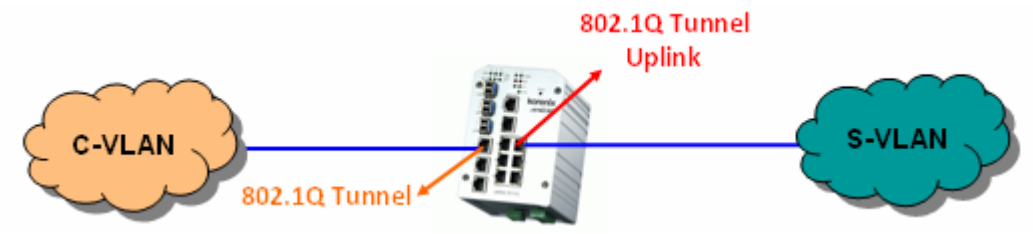
Figure 4.5.2 Web UI of VLAN configuration.



PVID: The abbreviation of the **Port VLAN ID**. Enter port VLAN ID here. PVID allows the switches to identify which port belongs to which VLAN. To keep things simple, it is recommended that PVID is equivalent to VLAN IDs.

The values of PVIDs are from 0 to 4095. But, 0 and 4095 are reserved. You can't input these 2 PVIDs. 1 is the default value. 2 to 4094 are valid and available in this column. Type the PVID you'd like to configure here.

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



Following is the modes you can select.

None: Remian VLAN setting, no QinQ.

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

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

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

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

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

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

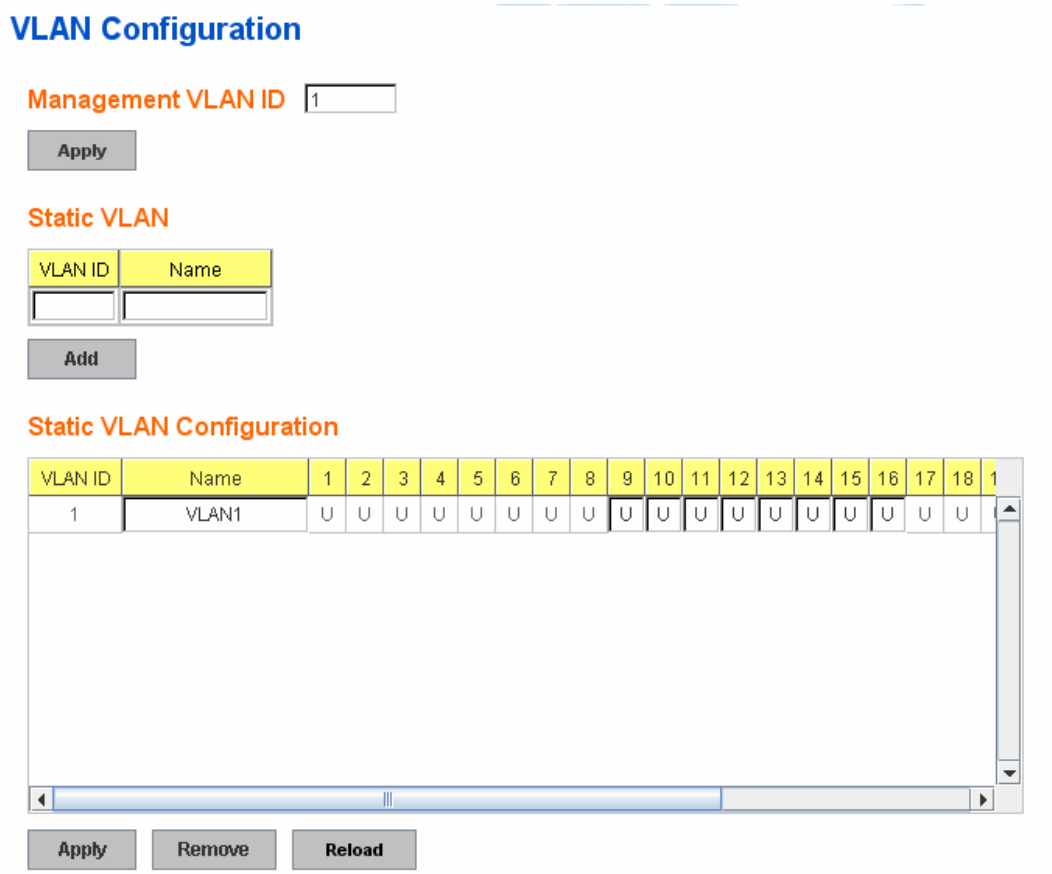
Accept Frame Type: This column defines the accepted frame type of the port. There are 2 modes you can select, **Admit All** and **Tag Only**. Admit All mode means that the port can accept both tagged and untagged packets. Tag Only mode means that the port can only accept tagged packets.

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

4.5.2 VLAN Configuration

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

Figure 4.5.2.1 Web UI of the VLAN Configuration.



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

Note: The management VLAN is only applied to JetNet 5628G Series. Go to "Routing -> IP -> IP Configuration" to configure management IP address for JetNet 5828G Series.

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

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

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

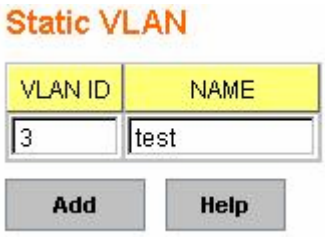


Figure 4.5.2.2 The steps to create a new VLAN: Type VLAN ID and NAME, and press **Add** to create a new VLAN. Then you can see the new VLAN in the Static VLAN Configuration table. Refer to Figure 4.5.2.3

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

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

Note: *Currently JetNet 5628G/5828G supports max 255 group VLAN.*

Static VLAN Configuration

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

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

Figure 4.5.2.4 Configure Egress rule of the ports.

-- : Not available

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

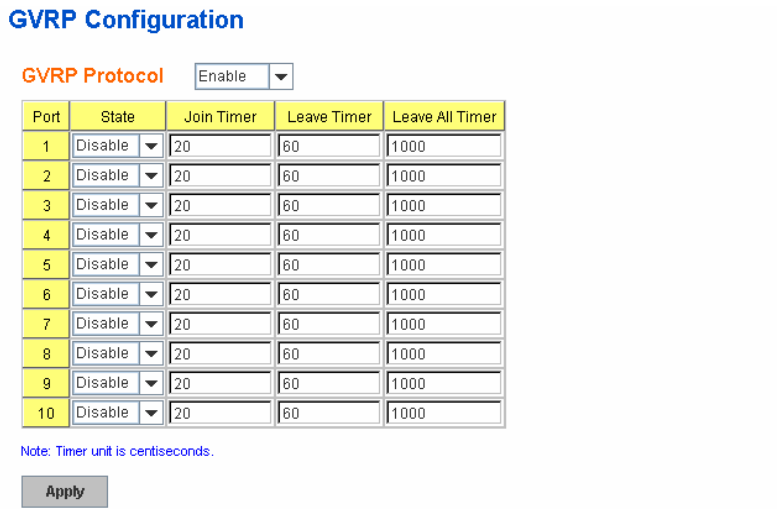
T : **Tag**: Indicates that egress/outgoing frames are to be VLAN tagged.

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.

4.5.3 GVRP configuration

GVRP allows users to set-up VLANs automatically rather than manual configuration on every port of every switch in the network. In low volume and stable network, the GVRP can

reduce the configuration effort. For high volume and high secure request network, the Static VLAN configuration is always preferred.



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

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

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

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

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

4.5.4 VLAN Table

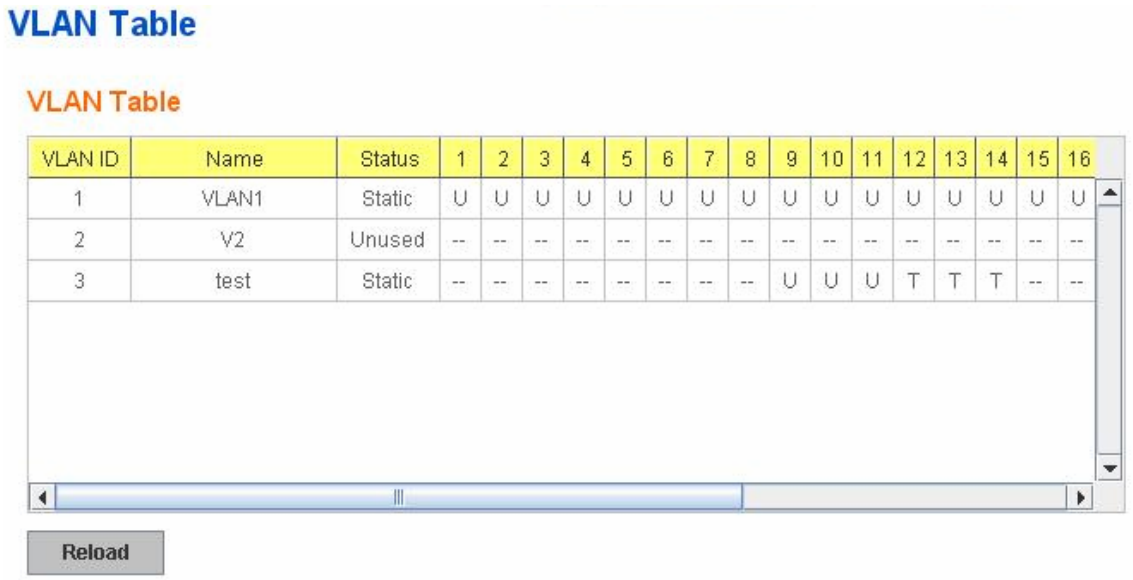
This table shows you current settings of your VLAN table, including VLAN ID, Name, Status, and Egress rule of the ports.

VLAN ID: ID of the VLAN.

Name: Name of the VLAN.

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

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



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

4.5.5 CLI Commands of the VLAN

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

Feature	Command Line
VLAN Port Configuration(Go to the port interface configuration mode first.)	
Port Interface Configuration	Switch# conf ter Switch(config)# interface fa5 Switch(config-if)#
VLAN Port PVID	Switch(config-if)# switchport trunk native vlan 2 Set port default vlan id to 2 success
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!
Ingress Filtering (for fast Ethernet port 1)	Switch(config)# interface fa1 Switch(config-if)# ingress filtering enable ingress filtering enable Switch(config-if)# ingress filtering disable ingress filtering disable

Egress rule – Untagged (for VLAN 2)	Switch(config-if)# switchport access vlan 2 switchport access vlan - success
Egress rule – Tagged (for VLAN 2)	Switch(config-if)# switchport trunk allowed vlan add 2
Display – Port Ingress Rule (PVID, Ingress Filtering, Acceptable Frame Type)	Switch# show interface fa1 Interface fastethernet1 Administrative Status : Enable Operating Status : Not Connected Duplex : Auto Speed : Auto Flow Control :off Default Port VLAN ID: 2 Ingress Filtering : Disabled Acceptable Frame Type : All Port Security : Disabled Auto Negotiation : Enable Loopback Mode : None STP Status: disabled 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 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 dot1q-tunnel mode port 1 : normal port 2 : normal port 3 : normal port 4 : normal port 5 : access port 6 : uplink port 7 : normal port 8 : normal port 9 : normal port 10 : normal
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
Create multiple VLANs (VLAN 5-10)	Switch(config)# interface vlan 5-10
Shut down VLAN	Switch(config)# interface vlan 2 Switch(config-if)# shutdown Switch(config-if)# no shutdown ->Turn on the VLAN
Display – VLAN table	Switch# sh vlan VLAN Name Status Trunk Ports Access Ports ---- ---------- ------- ---------- ---------- 1 VLAN1 Static - fa1-7,gi8-10 2 VLAN2 Unused - - 3 test Static fa4-7,gi8-10 fa1-3,fa7,gi8-10
Display – VLAN interface information	Switch# show interface vlan1 interface vlan1 is up, line protocol detection is disabled index 14 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,MULTICAST> HWaddr: 00:12:77:ff:01:b0

	inet 192.168.10.100/24 broadcast 192.168.10.255 input packets 639, bytes 38248, dropped 0, multicast packets 0 input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0 output packets 959, bytes 829280, dropped 0 output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0 collisions 0
GVRP configuration	
GVRP enable/disable	Switch(config)# gvrp mode disable Disable GVRP feature globally on the switch enable Enable GVRP feature globally on the switch Switch(config)# gvrp mode enable Gvrp is enabled on the switch!
Configure GVRP timer Join timer /Leave timer/ LeaveAll timer	Switch(config)# inter fa1 Switch(config-if)# garp timer <10-10000> Switch(config-if)# garp timer 20 60 1000 Note: The unit of these timer is centisecond
Management VLAN	
Management VLAN	Switch(config)# int vlan 1 (Go to management VLAN) Switch(config-if)# no shutdown
Display	Switch# show running-config …. ! interface vlan1 ip address 192.168.10.17/24 ip igmp no shutdown ! ….

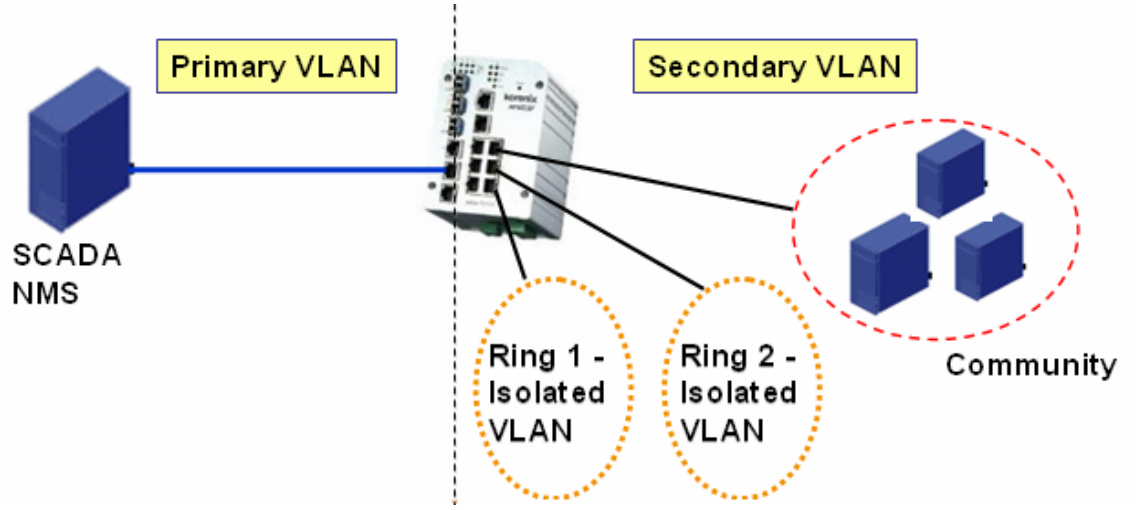
4.6 Private VLAN

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

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

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

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



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

Following commands are included in this group:

4.6.1 PVLAN Configuration

4.6.2 PVLAN Port Configuration

4.6.3 CLI Commands of the PVLAN

4.6.1 PVLAN Configuration

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

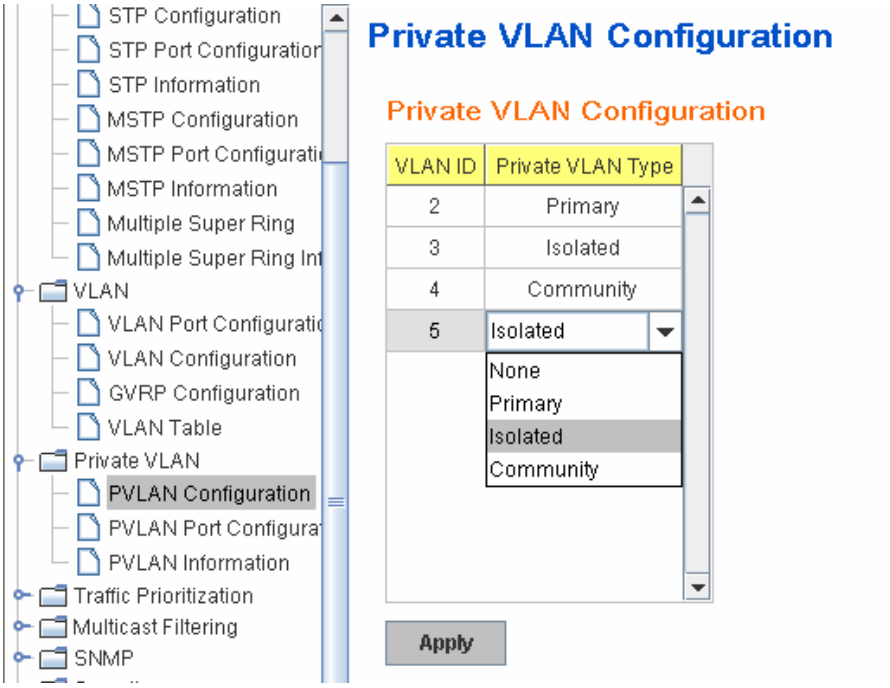
None: The VLAN is Not included in Private VLAN.

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

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

Community: The VLAN is the Community VLAN. The member ports of the VLAN can

communicate with each other.



4.6.2 PVLAN Port Configuration

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

Private VLAN Association

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

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

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

Port Configuraion

PVLAN Port Type :

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

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

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

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

For example:

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

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

VLAN 2 is belonged to Primary VLAN.

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

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

4. Private VLAN Port Configuraiton

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

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

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

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

5. Result:

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

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

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

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

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

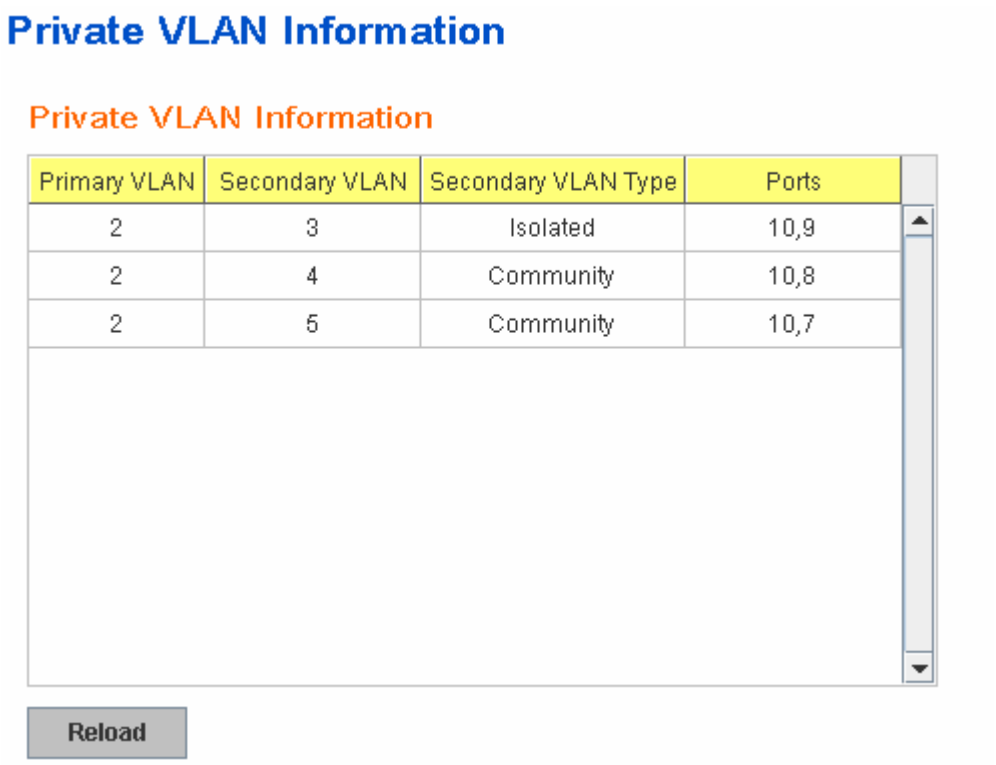
Private VLAN Association

Secondary VLAN	Primary VLAN
3	2
4	2
5	2

Apply

4.6.3 Private VLAN Information

This page allows you to see the Private VLAN information.



4.6.4 CLI Command of the PVLAN

Command Lines of the Private VLAN configuration

Feature	Command Line
Private VLAN Configuration	
Create VLAN	Switch(config)# vlan 2 vlan 2 success Switch(config-vlan)# end End current mode and change to enable mode exit Exit current mode and down to previous mode list Print command list name Assign a name to vlan no no private-vlan Configure a private VLAN
Private VLAN Type Choose the Types	**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

Primary Type Isolated Type Community Type	Switch(config-vlan)# private-vlan primary <cr> Switch(config-vlan)# private-vlan isolated <cr> Switch(config-vlan)# private-vlan community <cr>
Private VLAN Port Configuraiton	
Go to the port configuraiton	Switch(config)# interface (port_number, ex: gi9) Switch(config-if)# switchport private-vlan host-association Set the private VLAN host association mapping map primary VLAN to secondary VLAN
Private VLAN Port Type Promiscuous Port Type Host Port Type	Switch(config-if)# switchport mode private-vlan Set private-vlan mode Switch(config-if)# switchport mode private-vlan host Set the mode to private-vlan host promiscuous Set the mode to private-vlan promiscuous Switch(config-if)# switchport mode private-vlan promiscuous <cr> Switch(config-if)# switchport mode private-vlan host <cr>
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

```
Switch# show run
Building configuration...

Current configuration:
hostname Switch
vlan learning independent
!
vlan 1
!
```

Private VLAN Type

```
vlan 2
 private-vlan primary
!
vlan 3
 private-vlan isolated
!
vlan 4
 private-vlan community
!
vlan 5
 private-vlan community
!
………..
………..
```

Private VLAN Port Information

```
interface fastethernet7
  switchport access vlan add 2,5
  switchport trunk native vlan 5
 switchport mode private-vlan host
 switchport private-vlan host-association 2 5
!
interface gigabitethernet8
  switchport access vlan add 2,4
  switchport trunk native vlan 4
 switchport mode private-vlan host
 switchport private-vlan host-association 2 4
!
interface gigabitethernet9
  switchport access vlan add 2,5
```

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

4.7 Traffic Prioritization

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

JetNet QOS supports 4 physical queues, weighted fair queuing (WRR) and Strict Priority scheme, which follows 802.1p COS tag and IPv4 TOS/DiffServ information to prioritize the traffic of your industrial network.

Following commands are included in this group:

4.6.1 QoS Setting

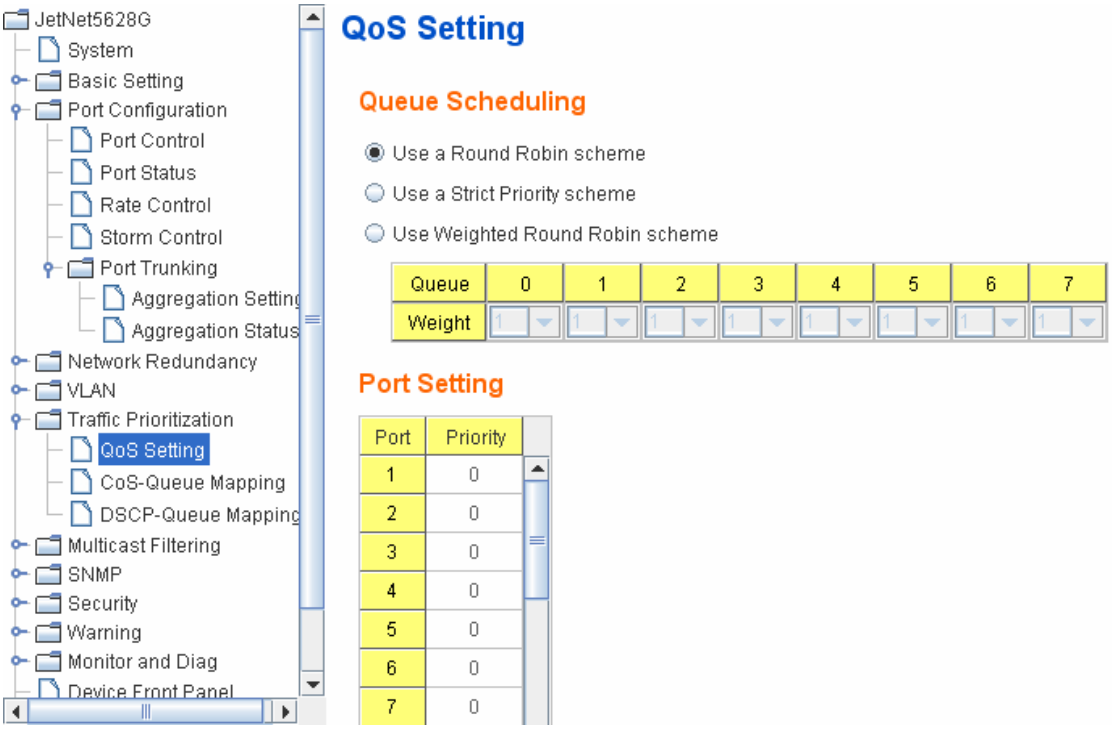
4.6.2 CoS-Queue Mapping

4.6.3 DSCP-Queue Mapping

4.6.4 CLI Commands of the Traffic Prioritization

4.7.1 QoS Setting

In QoS setting, you can assign the Queue Scheduling, WRR ratio, Port Priority Setting.



Queue Scheduling

You can select the Queue Scheduling rule as follows:

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

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

Use Weighted Round Robin scheme. This scheme allows users to assign new weight

ratio for each class. The 10 is the highest ratio. The ratio of each class is as below:

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

Port Setting

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

Trust Mode is to indicate Queue Mapping types for you to select.

COS Only: Port priority will only follow COS-Queue Mapping you have assigned.

DSCP Only: Port priority will only follow DSCP-Queue Mapping you have assigned.

COS first: Port priority will follow COS-Queue Mapping first, and then DSCP-Queue Mapping rule.

DSCP first: Port priority will follow DSCP-Queue Mapping first, and then COS-Queue Mapping rule.

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

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

4.7.2 CoS-Queue Mapping

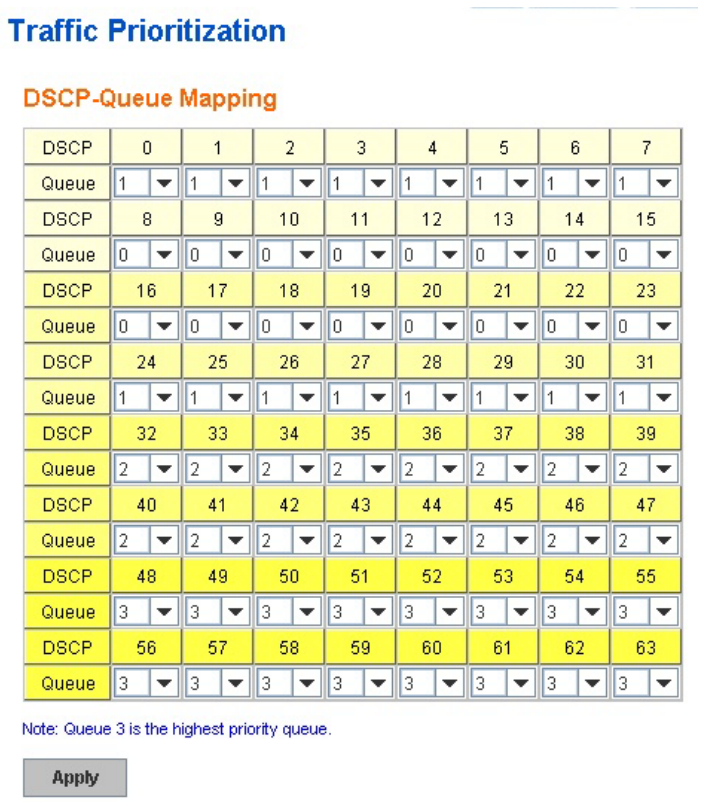
This page is to change CoS values to Physical Queue mapping table. Since the switch fabric of JetNet only supports 4 physical queues, Lowest, Low, Middle and High. Users should therefore assign how to map CoS value to the level of the physical queue.

In JetNet, users can freely assign the mapping table or follow the suggestion of the 802.1p standard. Korenix uses 802.p suggestion as default values. You can find CoS values 1 and 2 are mapped to physical Queue 0, the lowest queue. CoS values 0 and 3 are mapped to physical Queue 1, the low/normal physical queue. CoS values 4 and 5 are mapped to physical Queue 2, the middle physical queue. CoS values 6 and 7 are mapped to physical Queue 3, the high physical queue.

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

4.7.3 DSCP-Queue Mapping

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



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

4.7.4 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 rr Round Robin sp Strict Priority wrr Weighted Round Robin Switch(config)# qos queue-sched sp The queue scheduling scheme is setting to Strict Priority.
Queue Scheduling – Round Robin	Switch(config)# qos queue-sched rr The queue scheduling scheme is setting to Round Robin.
Queue Scheduling - WRR	Switch(config)# qos queue-sched wrr <1-10> Weights for COS queue 0 (queue_id 0) Switch(config)# qos queue-sched wrr 10 <1-10> Weights for COS queue 1 (queue_id 1) ……..

	Switch(config)# qos queue-sched wrr 1 2 3 4 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 DEFAULT-PRIORITY Assign an priority (7 highest) Switch(config-if)# qos priority 7 The default port priority value is set 7 ok. ***Note: When change the port setting, you should Select the specific port first. Ex: fa1 means fast Ethernet port 1.***
Display – Port Setting - Trust Mode	Switch# show qos trust QoS Port Trust Mode : Port Trust Mode -----+---------- 1 DSCP first 2 COS only 3 COS only 4 COS only 5 COS only 6 COS only 7 COS only 8 COS only 9 COS only 10 COS only
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 -----+---- 1 7 2 0 3 0 4 0 5 0 6 0 7 0 8 0 9 0 10 0
CoS-Queue Mapping	
Format	Switch(config)# qos cos-map PRIORITY Assign an priority (7 highest) Switch(config)# qos cos-map 1 QUEUE Assign an queue (0-3)

	Note: Format: qos cos-map priority_value queue_value
Map CoS 0 to Queue 1	Switch(config)# qos cos-map 0 1 The CoS to queue mapping is set ok.
Map CoS 1 to Queue 0	Switch(config)# qos cos-map 1 0 The CoS to queue mapping is set ok.
Map CoS 2 to Queue 0	Switch(config)# qos cos-map 2 0 The CoS to queue mapping is set ok.
Map CoS 3 to Queue 1	Switch(config)# qos cos-map 3 1 The CoS to queue mapping is set ok.
Map CoS 4 to Queue 2	Switch(config)# qos cos-map 4 2 The CoS to queue mapping is set ok.
Map CoS 5 to Queue 2	Switch(config)# qos cos-map 5 2 The CoS to queue mapping is set ok.
Map CoS 6 to Queue 3	Switch(config)# qos cos-map 6 3 The CoS to queue mapping is set ok.
Map CoS 7 to Queue 3	Switch(config)# qos cos-map 7 3 The CoS to queue mapping is set ok.
Display – CoS-Queue mapping	Switch# sh qos cos-map CoS to Queue Mapping : CoS Queue ---- + ------ 0 1 1 0 2 0 3 1 4 2 5 2 6 3 7 3
DSCP-Queue Mapping	
Format	Switch(config)# qos dscp-map PRIORITY Assign an priority (63 highest) Switch(config)# qos dscp-map 0 QUEUE Assign an queue (0-3) ***Format: qos dscp-map priority_value queue_value***
Map DSCP 0 to Queue 1	Switch(config)# qos dscp-map 0 1 The TOS/DSCP to queue mapping is set ok.
Display – DSCO-Queue mapping	Switch# show qos dscp-map DSCP to Queue Mapping : (dscp = d1 d2) d2| 0 1 2 3 4 5 6 7 8 9 d1 | -----+---------- 0 | 1 1 1 1 1 1 1 1 0 0 1 | 0 0 0 0 0 0 0 0 0 0 2 | 0 0 0 0 1 1 1 1 1 1 3 | 1 1 2 2 2 2 2 2 2 2 4 | 2 2 2 2 2 2 2 2 3 3 5 | 3 3 3 3 3 3 3 3 3 3 6 | 3 3 3 3

4.8 Multicast Filtering

For multicast filtering, JetNet 5628G/5828G uses IGMP Snooping technology. IGMP (Internet Group Management Protocol) is an Internet Protocol that provides a way for internet device to report its multicast group membership to adjacent routers. Multicasting allows one computer on the internet to send data to a multitude of other computers that have identified themselves as being interested in receiving the originating computers data.

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

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

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

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

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

Following commands are included in this group:

4.7.1 IGMP Snooping

4.7.2 IGMP Query

4.7.3 Force Filtering

4.7.4 CLI Commands of the Multicast Filtering

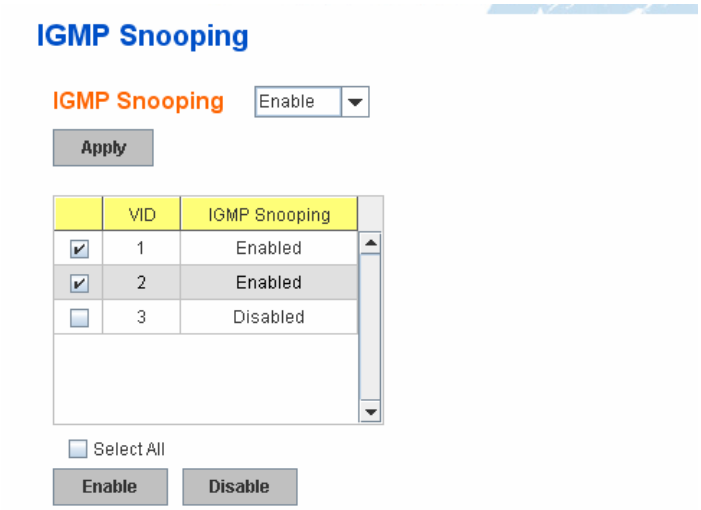
4.8.1 IGMP Snooping

This page is to enable IGMP Snooping feature, assign IGMP Snooping for specific VLAN, and view IGMP Snooping table from dynamic learnt or static manual key-in. JetNet5628G/5828G support IGMP snooping V1/V2/V3 automatically and IGMP query V1/V2.

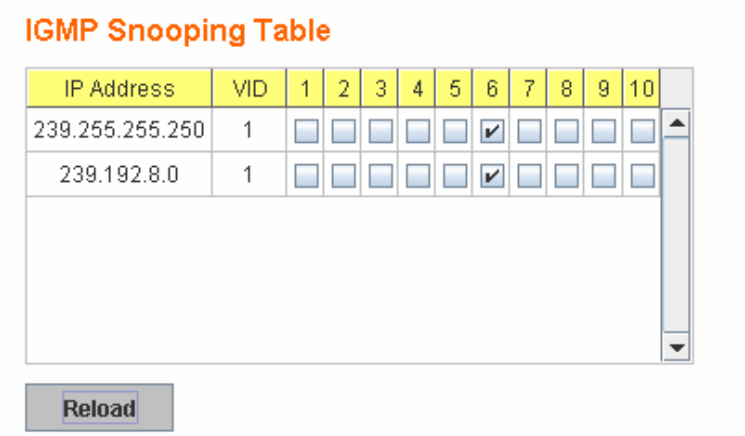
IGMP Snooping, you can select **Enable** or **Disable** here. After enabling IGMP Snooping, you can then enable IGMP Snooping for specific VLAN. You can enable IGMP Snooping for some VLANs so that some of the VLANs will support IGMP Snooping and others won't.

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

Disable IGMP Snooping for certain VLANs.



IGMP Snooping Table: In the table, you can see multicast group IP address, VLAN ID it belongs to, and member ports of the multicast group. JetNet 5628G/5828G supports 256 multicast groups. Click on **Reload** to refresh the table.

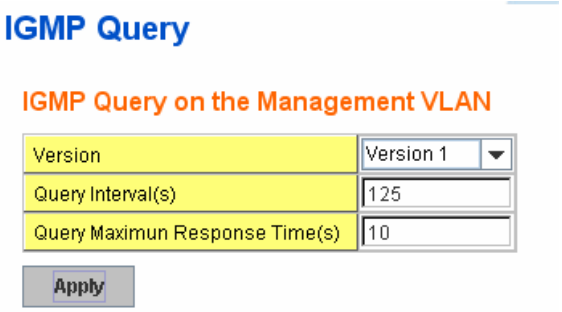


4.8.2 IGMP Query

In JetNet 5628G Series, there is only one IGMP Query, it is applied to management VLAN.

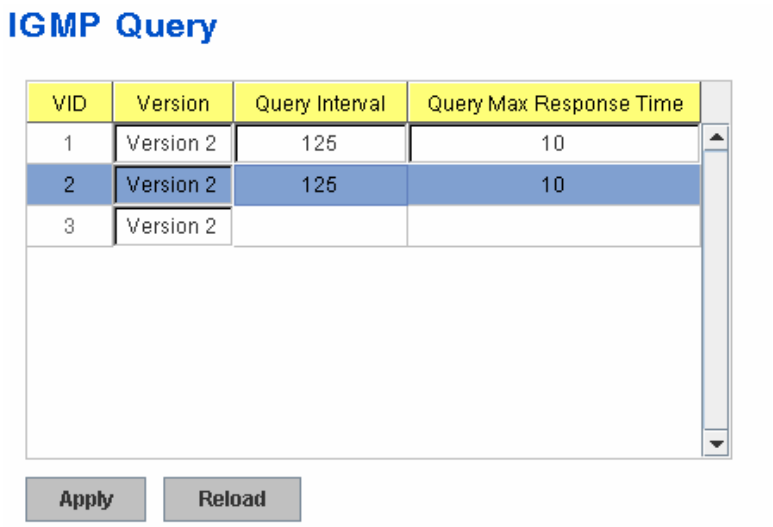
In JetNet 5828G Series, there are multiple IP/VLAN interfaces for layer 3 routing. Each IP/VLAN interface can act as the IGMP Query for its own VLAN. Each IP/VLAN interface should have its own IGMP Query.

This is the figure of JetNet 5628G series. IGMP Query is only applied to management VLAN.



This is the figure of JetNet 5828G Series. IGMP Query can be applied to each IP/VLAN interface. Select the Version of each VLAN ID and then “Apply” the setting.

Note that only the IGMP Query can only be enabled in active VLAN/IP interface. You should create VLAN and assign IP address to the VLAN interface first.



Below is the description of the IGMP Query parameters.

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

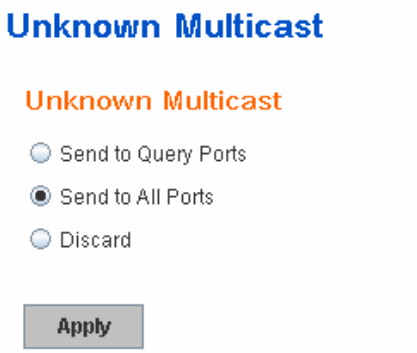
In IGMP Query selection, you can select V1, V2 or Disable. **V1** means IGMP V1 General Query and **V2** means IGMP V2 General Query.. The query will be forwarded to all multicast groups in the VLAN. **Disable** allows you to disable IGMP Query.

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

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

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

4.8.3 Unknown Multicast



After enabled IGMP Snooping, the known multicast can be filtered by IGMP Snooping mechanism, but how about the unknown multicast? This setting allows you to define how to forward the unknown multicast traffic.

Send to Query Port: The unknown Multicast traffic can be directed to the Query port. The Query port means the port learnt the IGMP Query. This is usually the uplink ports to other switches.

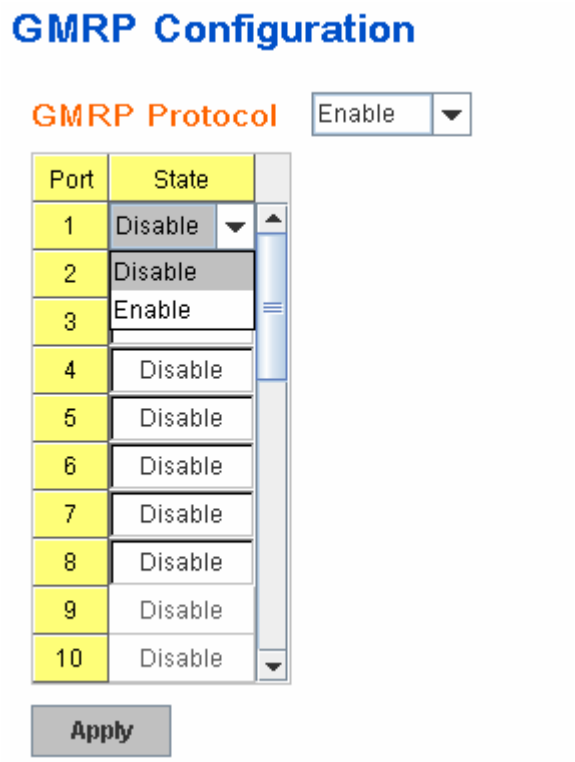
Send to All Ports: The unknown Multicast traffic will be flooded to all the ports.

Discard: If the Discard is selected, all the unknown multicast data will be discarded.

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

4.8.4 GMRP

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



4.8.5 CLI Commands of the Multicast Filtering

Command Lines of the multicast filtering configuration

Feature	Command Line
IGMP Snooping	
IGMP Snooping - Global	Switch(config)# ip igmp snooping IGMP snooping is enabled globally. Please specify on which vlans IGMP snooping enables
IGMP Snooping - VLAN	Switch(config)# ip igmp snooping vlan VLANLIST allowed vlan list

	all all existed vlan Switch(config)# ip igmp snooping vlan 1-2 IGMP snooping is enabled on VLAN 1-2.
Disable IGMP Snooping - Global	Switch(config)# no ip igmp snoopin IGMP snooping is disabled globally ok.
Disable IGMP Snooping - VLAN	Switch(config)# no ip igmp snooping vlan 3 IGMP snooping is disabled on VLAN 3.
Display – IGMP Snooping Setting	Switch# sh ip igmp interface vlan1 enabled: Yes version: IGMPv1 query-interval; 125s query-max-response-time: 10s Switch# sh ip igmp snooping IGMP snooping is globally enabled Vlan1 is IGMP snooping enabled Vlan2 is IGMP snooping enabled Vlan3 is IGMP snooping disabled
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 the target VLAN) Switch(config-if)# ip igmp v1
IGMP Query V2	Switch(config)# int vlan 1 (Go to the target 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# show ip igmp Interface vlan1 enabled: Yes version: IGMPv2 query-interval: 125s query-max-response-time: 10s Interface vlan2 enabled: Yes version: IGMPv2 query-interval: 125s query-max-response-time: 10s Interface vlan3 enabled: No Switch# show running-config ….

	!
	interface vlan1
	  ip address 192.168.10.43/24
	  no shutdown
	  ip igmp
	!
	interface vlan2
	  ip address 192.168.2.254/24
	  no shutdown
	  ip igmp
	!
	interface vlan3
	  ip address 192.168.3.254/23
	  no shutdown!
	…….
	ip routing
	qos queue-sched rr
	spanning-tree mst configuration
	  exit
	ip igmp snooping
	ip igmp snooping vlan 1
	ip igmp snooping vlan 2
	ip igmp snooping vlan 3
	…….

Unknown Multicast	
Send to Query Ports	Switch(config)# ip igmp snooping source-only-learning IGMP Snooping Source-Only-Learning enabled
Discard (Force filtering)	Switch(config)# mac-address-table multicast filtering Filtering unknown multicast addresses ok!
Send to All Ports (No Discard, No Send to Query Ports)	Switch(config)# no mac-address-table multicast filtering Switch(config)# no ip igmp snooping source-only-learning IGMP Snooping Source-Only-Learning disabled

4.9 Routing

Layer 3 Routing Feature is the most important feature of the the Layer 3 Modular Managed Ethernet Switch. Since the hosts located in different broadcast domain can't communicate by themselves, once there is a need to communicate among the different VLANs, the layer 3 routing feature is requested.

The JetNet 5828G equips with a Layer 3 chipset which can perform wire-speed layer 3 routing performance. The JetNet 5828G combines Layer 2 switching and Layer 3 routing within the single platform. No matter how many VLAN/IP interfaces created, how much layer 2 switching traffic or layer 3 routing traffic within the JetNet 5828G can be forwarded/routed without any packet lost.

In the Routing Configuration pages allows users create the Routing Interfaces, enable routing capability, enable unicast/multicast routing protocols, configure router redundancy policy and check the related routing information.

Following commands are included in this group:

4.9.1 ARP

4.9.2 IP

4.9.3 Router

4.9.4 RIP

4.9.5 OSPF

4.9.6 Multicast Route

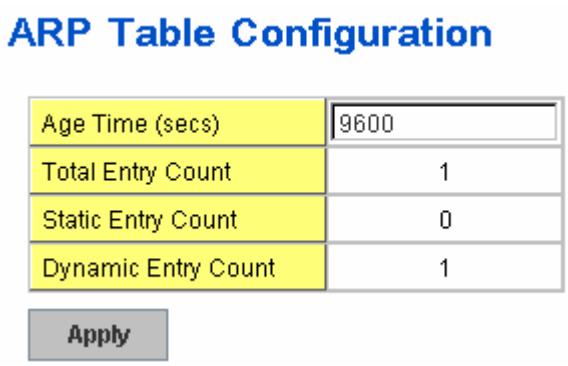
4.9.7 VRRP

4.9.1 ARP

ARP is the name of Address Resolution Protocol, it is a network layer protocol. ARP is query by broadcast and reply by unicast packet format. It assists IP protocol to find out the MAC address of an IP destination. It is important to find out the destination MAC address due to the MAC address is unique in the network, then the traffic can be correctly directed to the destination.

An ARP table must include the table with MAC Address/IP Address pair, storing information from the ARP reply, saving ARP operation for frequent communication and the entries are timeout with an aging mechanism.

The Web GUI below allows user to configure the Age Time of the ARP entry and see the count of static and dynamic ARP entries.



Age Time (secs): This is the Age time setting of the ARP entry. Once there is no packet (IP+MAC) hit the entry within the time, the entry will be aged out. Short ARP age time leads the entry aged out easier and re-learn often, the re-learn progress lead the communication stop. The default setting is 14,400 seconds (4hrs), it is also suggested value in the real world.

Type the new time and press "**Apply**" to change it.

Total Entry Count: This count represents for the count of total entries the ARP Table has.

Static Entry Count: This count represents for the count the static entries user configured.

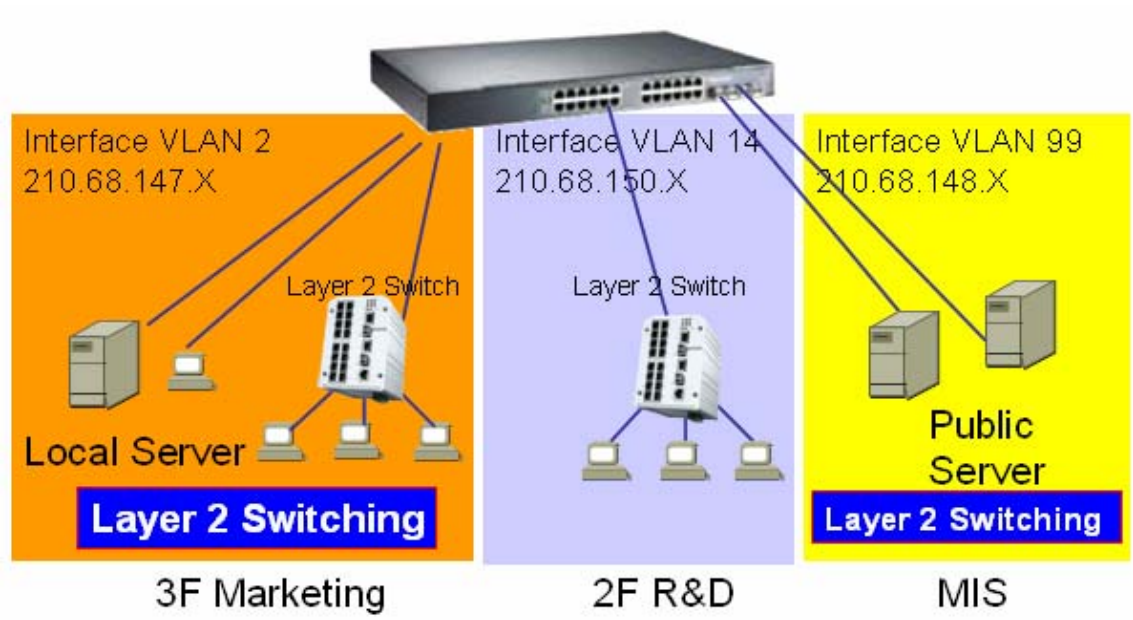
Dynamic Entry Count: This count represents for the count the ARP table dynamically learnt.

To configure the static ARP entry, or to see the entries of the ARP table, please use the Console CLI.

4.9.2 IP

An IP Interface is the basic unit while routing, it is a logical interface which equips with an IP network and acts as the default gateway of the attached clients. The network interface can be a port or a single VLAN. All the client members connected to the IP network can be routed through the network interface.

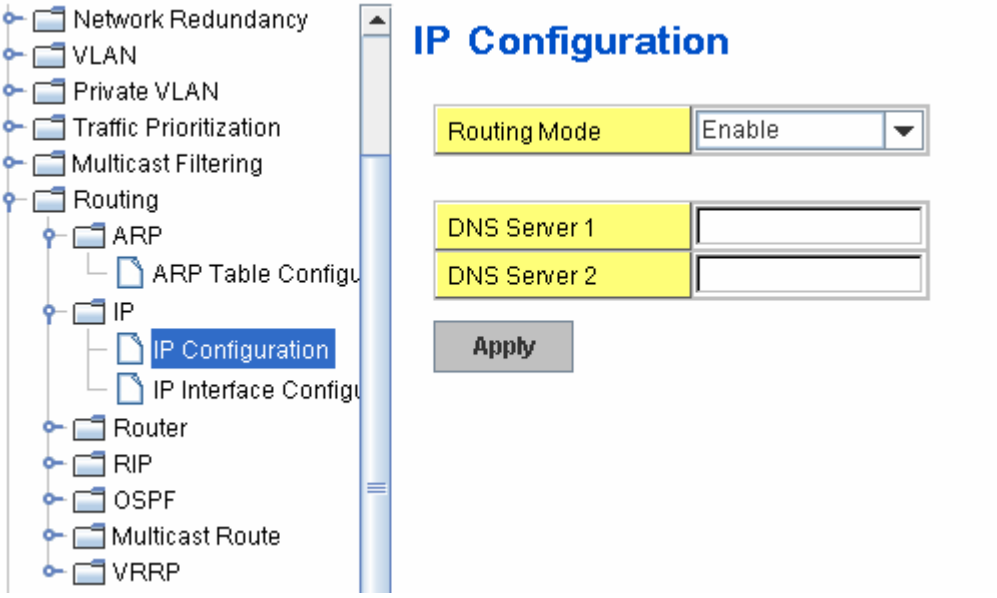
Below figure is a simple network which has 3 network interfaces. The interface VLAN 2 equips with 210.68.147.0 network, the interface VLAN 14 equips with 210.68.150.0 network and the interface VLAN 99 equips with 210.68.148.0 network. The VLAN ID is the logical interface which can be assigned with one IP address and subnet mask, the IP addresses within the subnet can be switched as a broadcast domain. Once the client wants within the subnet wants to communicate with another network, the traffic will be routed through the layer 3 switch.



4.9.2.1 IP Configuration

The IP Configuration page allows user enable the global IP Routing feature in the switch and create IP address to each network interface.

Routing Mode: This command allows user to **Enable** or **Disable** the global IP Routing mode. After Enabled, the switch can route traffic. If it is Disabled, the switch acts as a pure layer 2 switch, all the traffic can NOT be routed. All the network settings of routing protocols will be disabled and deleted.



DNS Server: Type the preferred IP address of the DNS Server here.

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

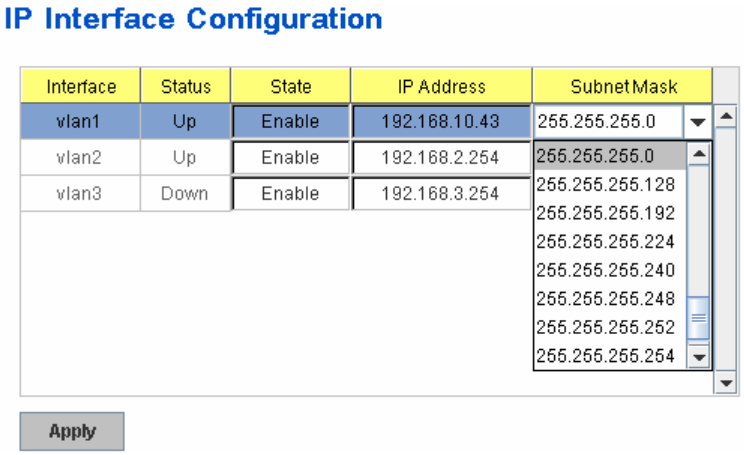
4.9.2.2 IP Interface Configuration

This page allows you Enable the IP Routing interface and assign the IP Address for it.

Before creating IP Interface, you should create VLAN Interface and assign the member port to the VLAN. Please refer to the VLAN Configuration for detail. The IP Interface table listed all the created VLAN automatically, you can change the setting for each VLAN here.

The JetNet 5828G allows you to create up to 128 IP Interfaces in whole system. Each VLAN Interface accepts up to 32 IP Address, one is the primary IP Address, the others are secondary IP Addresses. The IP Address is the default gateway of its attached members.

This is the IP Interface Configuration Table.



Interface: The name of the VLAN.

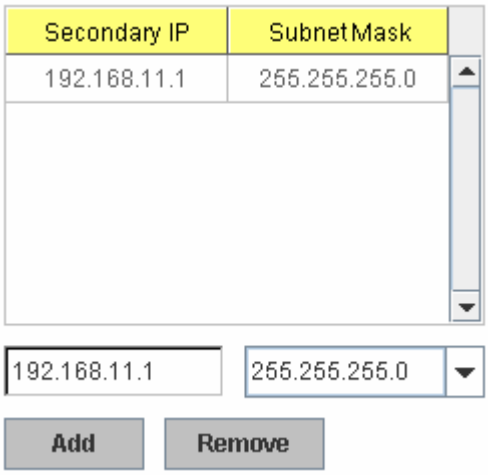
Status: After enabled the routing state, the Status shows "**Up**". After disabled the routing state, the status shows "**Down**".

State: Enable or **Disable** the IP Routing Interface state. After disabled, the interface just work as a layer 2 VLAN. After enabled, the interface can support IP routing feature.

IP Address: Assign the IP Address for the target VLAN.

Subnet Mask: You can choose the subnet mask here. For example, 255.255.255.0 represents for the typical Class C, or so-call 24-bits mask. There are 256 IP Addresses within the range.

This is the secondary IP interface table. Select the VLAN Interface in IP Interface table and then assign the secondary IP address and its subnet mask.



Secondary IP: Each Secondary IP interface, 192.168.11.1 for example. Type the IP address and select the subnet mask, then press "**Add**" to add it to the VLAN you selected.

Technical Tip: While configuring Inter-Routing progress, write the network plan first is suggested. The network plan includes how many VLAN you will create, who is the member port of the VLANs, what is their IP address and subnet mask. After VLAN created, then enable the Global IP Routing state and enable IP Routing state for each Interface. After done the progress, the switch can run wire-speed Inter-Routing for the interfaces.

4.9.3 Router

This page allows you configure the Route Entry and check the Routing table.

4.9.3.1 Route Entry Configuration

Default Route: The default route allows the stub network to reach all unknown networks through the route. The stub area has only one way and one route to other networks. Within the stub area, there are multiple networks and run their own routing protocols, however, while the want communicate with unknown network, the traffic will be forwarded to the default route.

While configuring Default Route, the IP address of the next hop router/switch is the only setting needs to be specified.

Static Route: A static route entry to and from a stub network to another stub network. The static route is usually configured to connect the neighbor router/switch, the both routers/switches then can communicate through the route.

While configuring Static Route, all the fields in Route entry like the destination network and its netmask, the valid route interface to the destination and distance are needed to be specified.

Route Entry Configuration

Default Route 192.168.10.254

Apply

Static Route Entry

Destination	Netmask	Gateway	Distance
192.168.11.0	255.255.255.0	192.168.10.254	1

Add

Route Entry Table

Destination	Netmask	Gateway	Distance	Metric	Interface
192.168.11.0	255.255.255.0	192.168.10.254	1	0	vlan1

Remove Reload

4.9.3.2 Route Table

This page displays the routing table information.

Routing Table

Routing Protocol	Destination	Connected via	Interface	Status
OSPF	192.168.2.0/24	-	vlan2	active
connected	192.168.2.0/24	-	vlan2	active
connected	192.168.3.0/24	-	vlan3	active
OSPF	192.168.3.0/24	-	vlan3	active
OSPF	192.168.4.0/24	192.168.3.253	vlan3	active
OSPF	192.168.5.0/24	192.168.2.254	vlan2	active
OSPF	192.168.10.0/24	192.168.2.254	vlan2	active
OSPF	192.168.12.0/24	-	vlan1	active
connected	192.168.12.0/24	-	vlan1	active
OSPF	192.168.13.0/24	192.168.3.253	vlan3	active

Reload

The system maintains the routing table information and updates it once the routing interfaces changed. The routing table information is important to find out the possible and best route in the field especially when troubleshooting the network problem.

The definition of the fields is listed in below:

Routing Protocol: The field shows the entry is a local interface or learnt from the routing protocol. Fox example: The "**connected**" represents for the local interface. The "**OSPF**" shows the entry is learnt from the routing protocol, OSPF.

Destination: The destination network of this entry.

Connected Via: The IP interface wherever the network learnt from. The interface is usually the next hop's IP address.

Interface: The VLAN Interface wherever the network connected to or learnt from.

Status: Shows the entry is active or not.

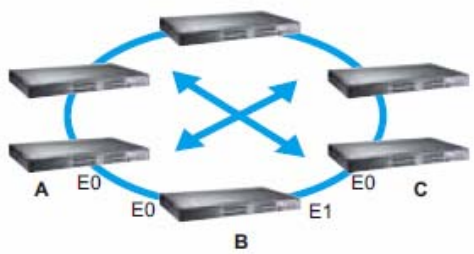
4.9.4 RIP

The RIP is short of the Routing Information Protocol. RIP was in widespread use years before it was standardized in as RFC 1058 in 1988. Version 2 of RIP was completed in 1994.

RIP is the most known Distance Vector type dynamic routing protocol, or known as Hop Based routing protocol. It uses hop count as a distance metric, each router advertises its routing table every 30 seconds. The maximum routers RIP can support is 15, the 16th router represents Infinity.

When a router receives a neighbor's table, it examines it entry by entry. If the destination is new, it is added to the local routing table. If the destination is known before and the update provides a smaller metric, the existing entry in the local routing table is replaced. Adds 1 (or sometimes more if the corresponding link is slow) to the metric. If no route updated within the cycles, the entry is removed.

The figure in the right shows the RIP routing table of router A, B and C.



Router A Routing Table

Destination	Interface	Metric
B	E0	0
C	E0	1

Router B Routing Table

Destination	Interface	Metric
A	E0	0
C	E1	0

Router C Routing Table

Destination	Interface	Metric
B	E0	0
A	E0	1

RIP Configuration

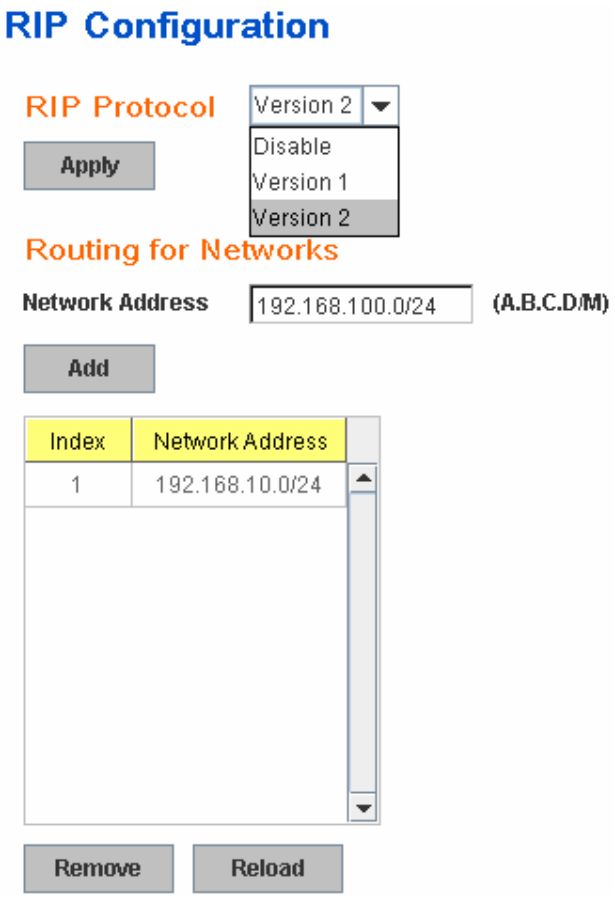
This page shows how to configure RIP protocol.

RIP Protocol: Choose the RIP **Version 1** or **Version 2** or **Disable** RIP protocol in here.

Routing for Networks: All the networks no matter directly connected or learnt from other router/switch should be added to the switch. The format is IP Network/bit mask. For example, 192.168.100.0/24. After type the network address, click "**Add**" to the RIP table.

Select the network address and click "**Remove**" to remove it.

Click "**Reload**" to see the updated RIP table.

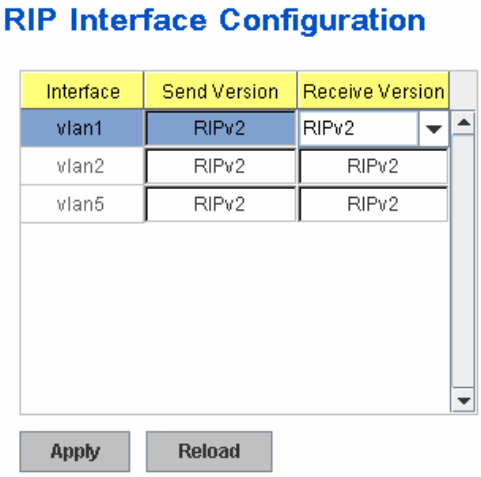


RIP Interface Configuration

In RIP Interface Configuration, you can configure Send Version and Receiver Version.

Select the RIP Version of the interface.

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

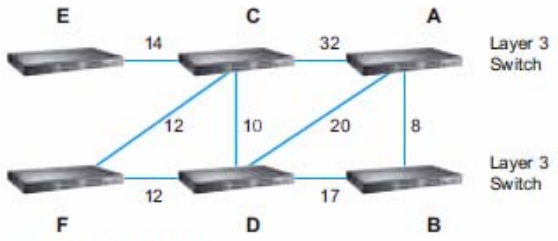


4.9.5 OSPF

The OSPF is short of the Open Shortest Path First.

OSPF is a link-state protocol. The Link is an interface on the router, it equips the IP, mask, the type of network, the routers connected to that network. The State is its relationship to its neighboring routers. The Metric is the distance between the 2 links, it is usually the bandwidth of the link in link-state protocol. The Link State Database is the collection of all these link states. The destination network address, the shortest metric to the network and the IP address of the next hop are specified in the link state database.

The figure in the right is the example OSPF network. There are 6 routing switch, A~F. The Routers/Switch periodically sends “Hello” packets to the neighbors and exchange OSPF link state with each other and then update the Routing table of each router/switch.



Router A Routing Table

Destination	Metric	Next Hop
B	8	B
C	30	D
D	20	D
E	44	D
F	32	D

Use the communication between A to C for example. In hop-based routing protocol, like RIP, the A to C is the shortest way.

However, in link-state protocol, like the OSFP, the A to D to C is the shortest way. This is calculated by the *Dijkstra’s SPF Algorithm.* After calculated and routing table updated, the metric from A to C is 32, the metric from A to D to C is 30. The A to D to C will be selected as the beast route from A to C.

The OSPF is a complex protocol which defines the role of the router/switch when it is installed in different Areas of the autonomous system. The Area is a group of routers, the OSPF uses flooding to exchange link-state updates between routers. The routers within the same area update its routing table. Any change in routing information is flooded to all routers in the same area.

The JetNet 5828G OSPF design comforts to the OSPF Version 2 specification. Typically, the JetNet 5828G acts as the Internal Router, a router within the area; the Designated Router, the Master router in the same broadcast domain within the area; the Area Board Router which is the boundary router between different area. While configuring the OSPF network, the area ID should be configured with the same IP address or the same area ID. The 0.0.0.0 is usually used.

4.9.5.1 OSPF Configuration

This page allows user to enable OSPF setting and configure the related settings and networks.

OSPF Protocol: Enable or **Disable** the OSFP routing protocol.

Router ID: The router ID can be any IP address, however, the IP address of the existed local interface is suggested. With such IP address, you can find the router/switch easier.

Router ID is used while connected multiple OSPF routers/switches to the same broadcast domain, the lowest Router ID will be selected as the Designated Router in the network.

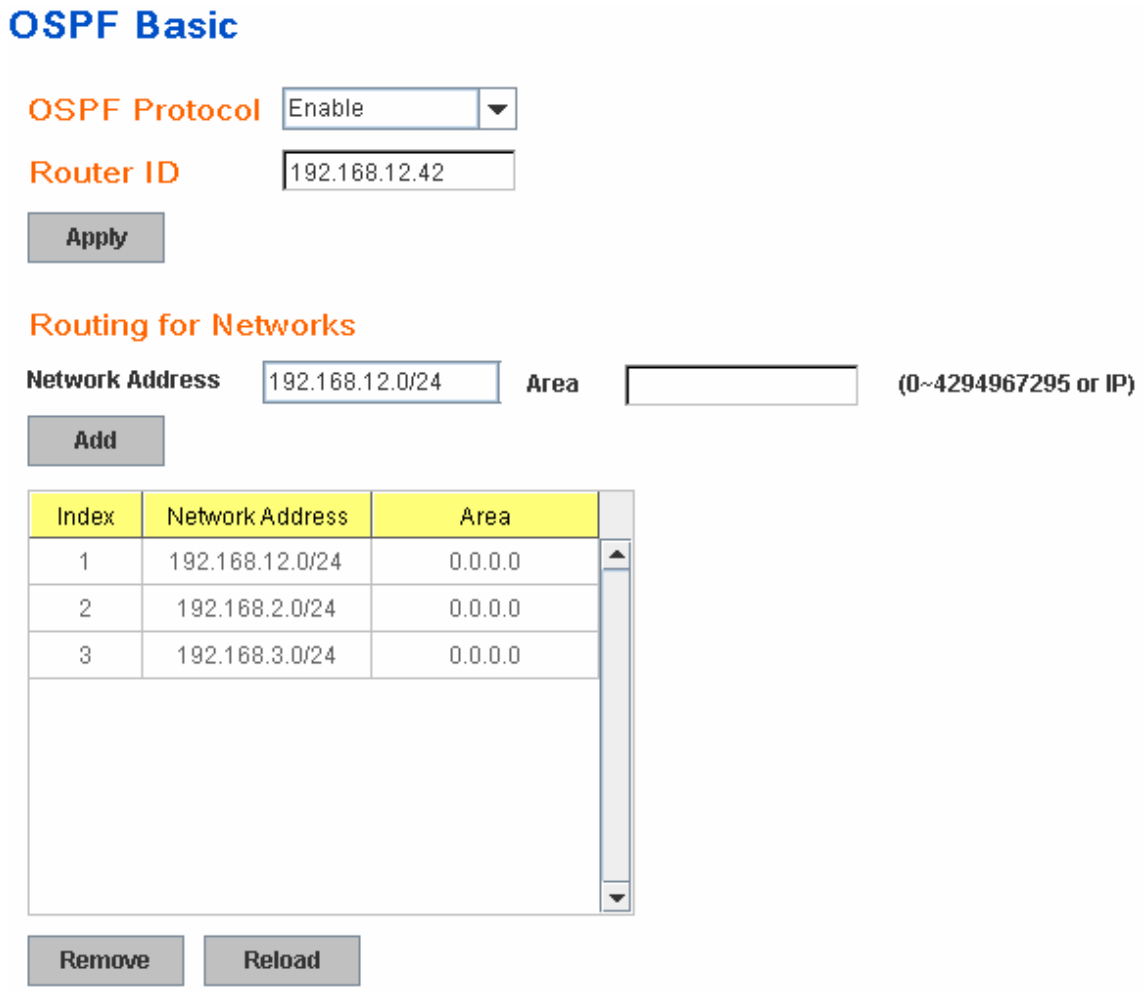
Routing for Network: Type the network address and the Area ID in the field. Click “Add” to apply the setting. You can see the network table in below.

Note: All the Area ID of the router/switch within the same area should use the same IP

address or ID. All the network address should be added.

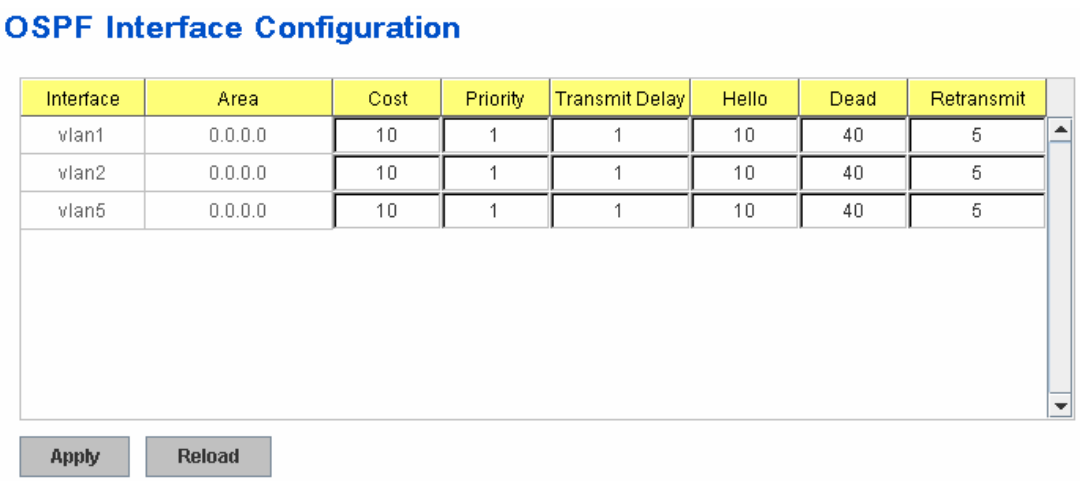
Select the Network Address, then you can **"Remove**" the setting.

Click **"Reload"** to reload the new entry.



4.9.5.2 OSPF Interface Configuration

This page allows user to see the OSPF network address and the parameters of each interface.



Interface: The VLAN Interface name.

Area: The area ID of the Interface you added. The Area ID must be the same for all routers/switches on a network.

Cost: The distance of this link/Interface, the default is identified depends on what the bandwidth is by the system. The value can be changed to decide the best router.

Priority: The priority of this link/Interface. Set priority to help find the OSPF designated router for a network. The default is 1. The range is 0 to 255.

Transmit Delay: The transmit delay timer of this link/Interface. Transmit Delay is the estimated number of seconds to wait before sending a link state update packet. The default value is 1 second.

Hello: The Hello timer of this link/Interface. The value must be the same for all routers/switches on a network. The default value is 10 seconds. The min. value is 1.

Dead: The Dead Interval Timer of this link/Interface. The Dead timer is the time to identify whether the interface is down or not before the neighbors declare the OSPF router to be down. The default value is 4 times (40 seconds) than the Hello interval (default is 10).

Retransmit: The count of Retransmit of this link/Interface. The Retransmit time specifies the number of seconds between link state advertisement transmissions. The default value is 5 seconds.

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

4.9.5.3 OSPF Neighbor Table

This page allows user to see the OSPF Neighbor information. The Neighbor interface and its state will be listed here.

Below is the example of a simple OSPF environment. The Hello packets are exchanged between the switch to next switches. While the **State** is changed to “Full”, that means the exchange progress is done. The **Neighbor ID** is the Router ID of the Neighbor routers/switches. The **Priority** is the priority of the link. The **Dead Time** is the activated time of the link. There are 2 interfaces attached the switch you check. The **IP address** shows the learnt IP interface of the next hops. And the **Interface** shows the connected local interface.

OSPF Neighbor Table

Neighbor ID	Priority	State	Dead Time	IP Address	Interface
192.168.3.254	1	Full/Backup	00:00:33	192.168.2.253	vlan2:192.168.2.254
192.168.5.254	1	Full/Backup	00:00:38	192.168.5.254	vlan5:192.168.5.253

Reload

State:

Down- initial state of the neighbor conversation - no recent information has been received from the neighbor.

Attempt - no recent information has been received from the neighbor but a more concerted effort should be made to contact the neighbor.

Init - an Hello packet has recently been seen from the neighbor, but bi-directional communication has not yet been established.

2 way - communication between the two routers is bi-directional.

Exchange start - the first step in creating an adjacency between the two neighboring routers, the goal is to decide which router is the master and to decide upon the initial DD sequence number.

Exchange - the router is describing its entire link state database by sending Database Description packets to the neighbor.

Loading - Link State Request packets are sent to the neighbor asking for the more recent LSAs that have been discovered (but not yet received) in the Exchange state.

Full - the neighboring routers are fully adjacent and they will now appear in router-LSAs and network-LSAs.

DR: Designated Router. This indicates the role of the coming interface is a DR.

Backup: Backup Designated Router. This indicates the role of the coming interface is a BDR.

4.9.5.4 OSPF Area Configuration

This page allows user to configure the OSPF Area information.

An OSPF domain is divided into different areas. Areas are logical grouping of hosts and networks, including their routers having interfaces connected to any of the included networks. Each area maintains its own link state database. In OSPF, all areas must be connected to a backbone area. The backbone area is responsible for distributing routing information between non-backbone areas.

The JetNet 5828G is usually installed as internal router of a single Area environment. While there are multiple areas in the network, this page allows modify the Area information and Virtual Link.

Area: This field indicates the area ID. Select the ID you want to modify here.

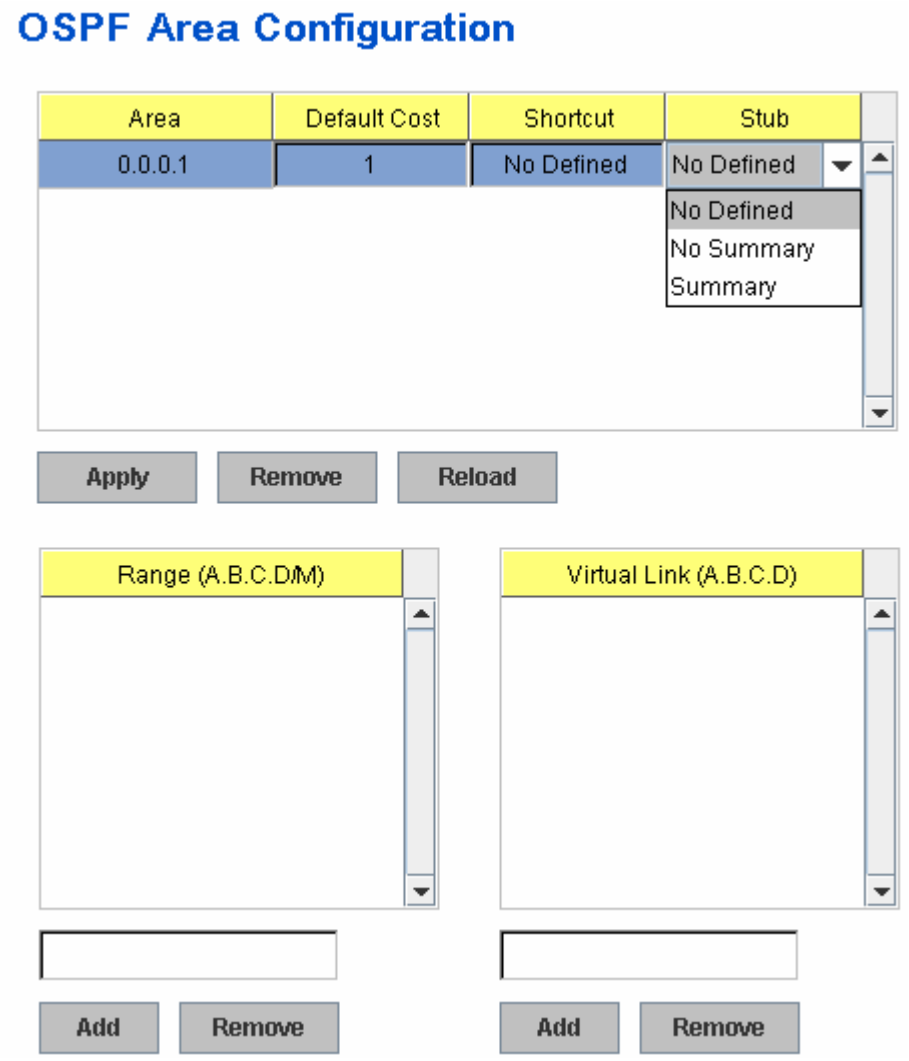
Default Cost: The default cost of the area ID.

Shortcut: No Defined, Disable, Enable. This indicates whether the area is the ospf ABR shortcut mode.

Stub: Represents whether the specified Area is a stub area or not. The possible values are No Defined, No Summary and Summary. Summary is used to advertise summary routes.

Virtual Link (A.B.C.D.): You can configure the virtual link. One area must be common area between two endpoint routers to create virtual links.

.



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

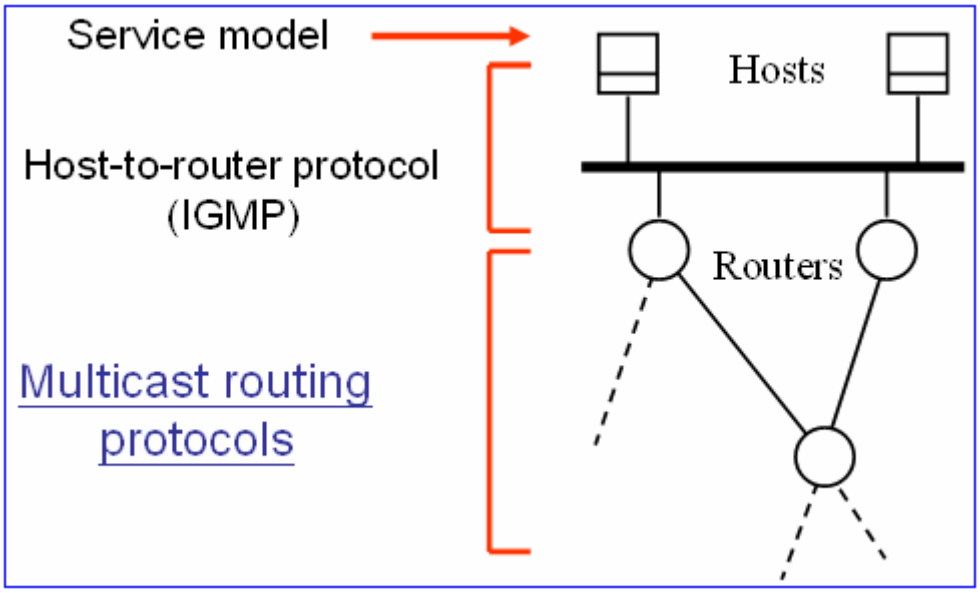
4.9.6 Multicast Route

JetNet 5828G supports both the IP Multicsat Filtering and the IP Multicsat Routing features.

The IP Multicast is a more efficient way to use network resource, it enables a host (source) to send packets to a group of hosts (clients) with the same multicast destination address. In layer 2 switch, we use IGMP Snooping (descript in chapter 4.7) to snoop the destination MAC address of the multicast stream and registered to the IGMP table.

In layer 3 switch, it supports full IGMP feature, not only snooping the MAC address of multicast group, but also decide whether the stream can be forwarded to the network or not. If the multicast stream comes from different network, then the Multicast Routing protocol is requested.

Below figure shows the difference between the IGMP and the Multicast Routing protocol. A layer 3 router/switch acts as the boundary router between the 2 types multicast services.



The typical Multicast Routing includes 2 types, one is Distance Vector based, like the DVMRP and PIM/DM. Another is Spars mode, like the PIM/SM.

In JetNet 5828G first firmware release, it only supports the DVMRP protocol. The PIM/DM and PIM/SM will be supported in later firmware. Please check Korenix News and Web site for future update.

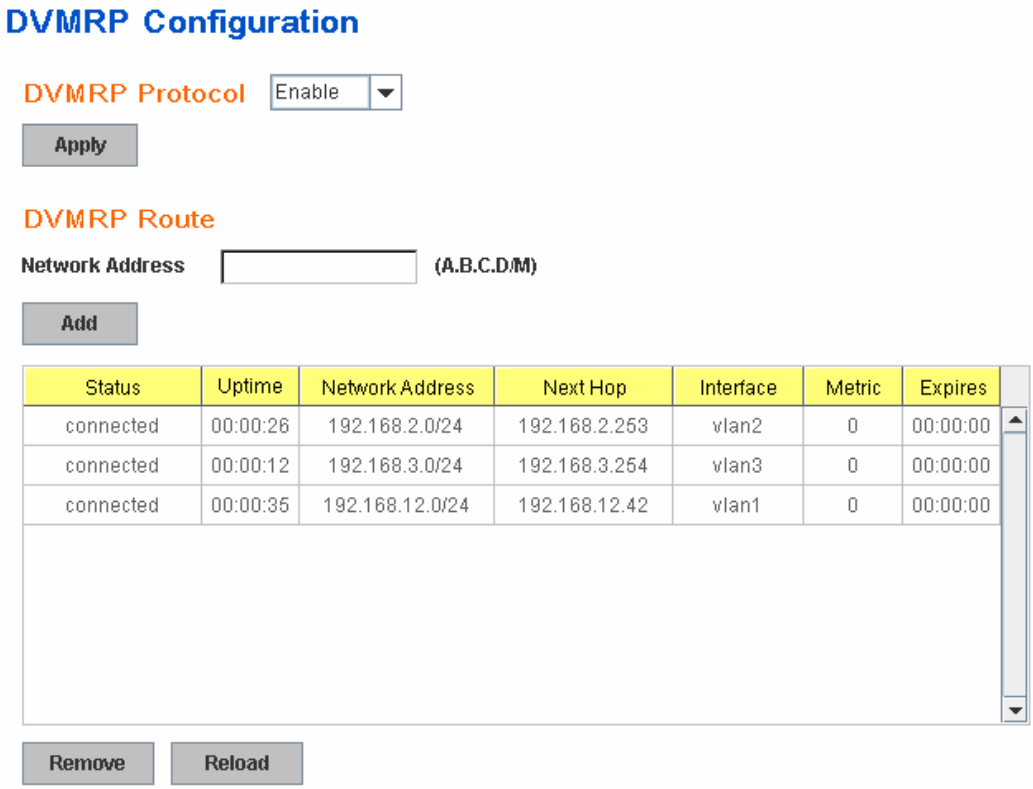
4.9.6.1 DVMRP

DVMRP is a Distance Vector-based Multicast Routing Protocol, it is similar to the RIP operating. The infinity of DVMRP is 32 hops. It uses Broadcast and Prune operation. The multicast stream from the source is pruned while there is no members of the multicast group on the network. It builds per-source broadcast trees based upon routing exchanges, then dynamically creates per-source-group multicast delivery trees by pruning (removing branches from) the source's truncated broadcast tree. It performs Reverse Path Forwarding checks to determine when multicast traffic should be forwarded to downstream interfaces. In this way, source-rooted shortest path trees can be formed to reach all group members from each source network of multicast traffic.

While configuring the DVMRP routing protocol, the IP interfaces should be activated and IP routing, IGMP of the system and interfaces should be enabled. Then enable the DVMRP service and type the DVMRP network.

DVMRP Configuration

This page allows user to enable DVMRP and add the DVMRP networks.

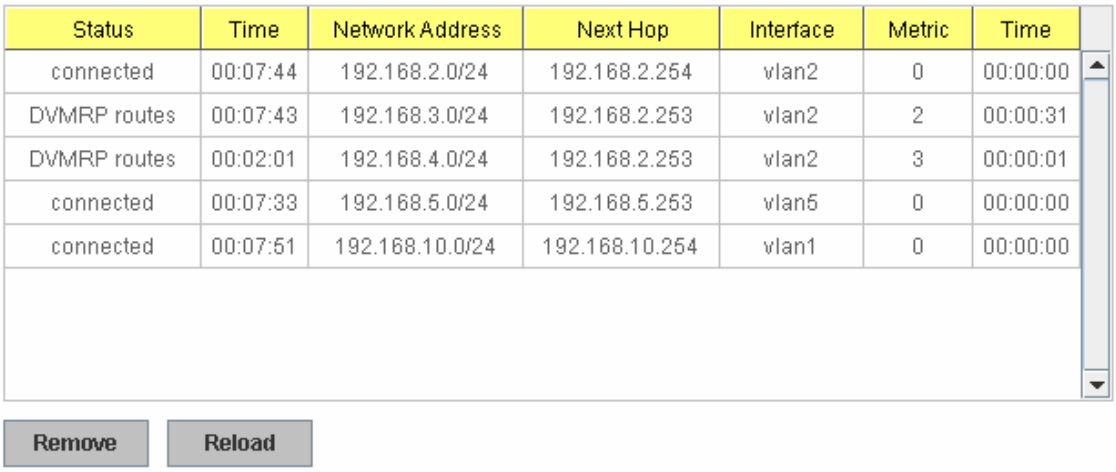


DVMRP Protocol: Enable or **Disable** the DVMRP protocol configuration.

DVMRP Route: Type the Network Address and its netmask. All the DVMRP networks should be added in the DVMRP configuration.

Click "**Add**" to add it. Then the entry is displayed in the DVMRP table.

After exchanged the DVMRP information, the table is updated as below.



DVMRP Neighbor Table

The Neighbor Table is a list to keep the neighboring multicast routers on every attached network. The information can be derived by the DVMRP routing messages that are received. A neighbor that has not been heard from in NEIGHBOR_TIMEOUT seconds should be considered to be down.

This page shows the DVMRP Neighbor Table.

Neighbor Address: The IP address of the DVMRP neighbor routers/switches.

Interface: The learnt VLAN interface.

Timeleft: This field indicates the Neighbor_Timeout second. When this timeout expires, packets will no longer be forwarded on the route, and routing updates will consider this route to have a metric of infinity.

Holdtime: This field indicates the Neighbor Holdtime second. When this timeout expires, routing updates will no longer contain any information on this route, and the route will be deleted.

DVMRP Neighbor Table

Neighbor Address	Interface	Timeleft	Holdtime	Index
192.168.2.253	vlan2	30	34	2
192.168.5.254	vlan5	29	34	3

Reload

4.9.6.2 Multicast Route Table

The Multicast Route Table is a list to display the Multicast Routing Table of the switch.

Multicast Route Table

Status	Time	Multicast Group	Source IP	Interface	Life	Hold	DownStream
Forwarding	00:00:31	224.10.10.10/32	192.168.10.111	vlan1	179	210	vlan2

Reload

Status:

The field indicates the status of the entry. There are 4 flags, Forwarding, Negative, Delete and Pruned.

Time: The active timer of the entry.

Multicast Group: The Multicast Group IP address of the steam.

Source IP: The source IP address of the stream.

Interface: The interface name of the source IP.

Life: The timer is decreased continuously. After the life timer is timeout, the entry will be deleted and the DVMRP probe will be generated again to add new Multicast route entry.

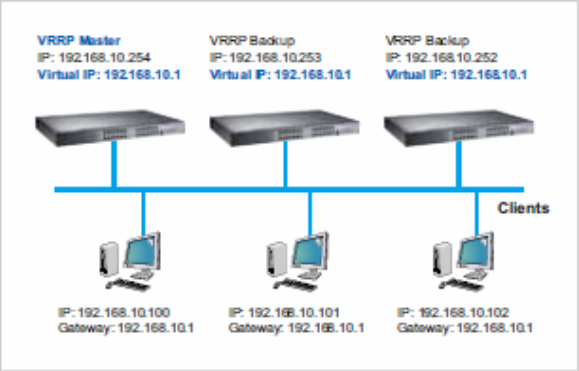
Hold: The entry will be held for a period of time until delete it. The default value is 210 seconds. After the timer timeout, the entry will be deleted and the DVMRP protocol prune

Downstream: The VLAN interface of the downstream.

4.9.7 VRRP

The VRRP represent for the Virtual Router Redundancy Protocol.

To further ensure the high reliability of an environment, the JetNet Layer 3 switch supports the VRRP protocol allowing the hosts to continuously direct traffic to the default gateway without the default gateway configuration change.



The figure for example, there are 3 VRRP-aware switches with the same Virtual IP of the VRRP, but different IP address of their VLAN/IP interface. One is selected as the VRRP Master and the others are VRRP Backup. The client PCs has the same gateway IP which is the virtual IP of the 3 switches. Once the VRRP Master switch or the VLAN interface failure, the VRRP Backup switch will act as the new Master immediately, thus the communication from the client PC will not stop.

Virtual Router Interface

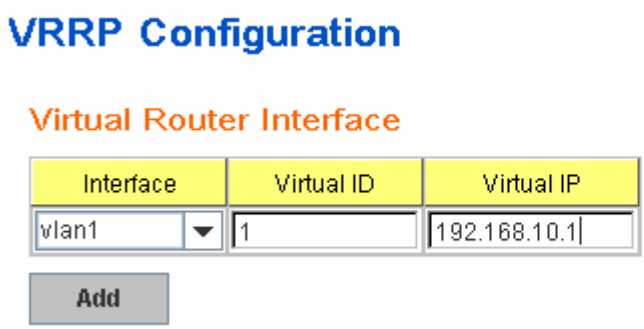
The fields allow you to create the Virtual Router Interface. All the layer 3 switches within the same VRRP domain should be located within the same IP network and equips with the same Virtual ID and Virtual IP address.

Interface: Select the interface for the VRRP domain.

Virtual ID: This is a virtual ID range from 1~255. The switches within the same VRRP domain should have the same Virtual ID.

Virtual IP: This is the virtual IP of the VRRP domain. This is the Gateway IP of the clients.

Click “Add” once you finish the configuration. Then you can see the entry is created in the Virtual Router Interface Configuration page



Virtual Router Interface Configuration

After the VRRP interface is created, you can see the new entry and adjust the settings to decide the policy of the VRRP domain.

Interface: Select the interface for the VRRP domain.

Virtual ID: This is a virtual ID range from 1~255. The switches within the same VRRP domain should have the same Virtual ID.

Virtual IP: This is the virtual IP of the VRRP domain. This is the Gateway IP of the clients.

Priority: The priority of the entry of this switch. In VRRP domain, the VRRP switches must have the same Virtual ID and Virtual IP settings and choose who should be the VRRP Master switch. The switch equips with the highest priority will be selected as the VRRP master. The priority setting field can be manually changed, the range is from 1~254, 255 for virtual IP owner and 100 for backup by default.

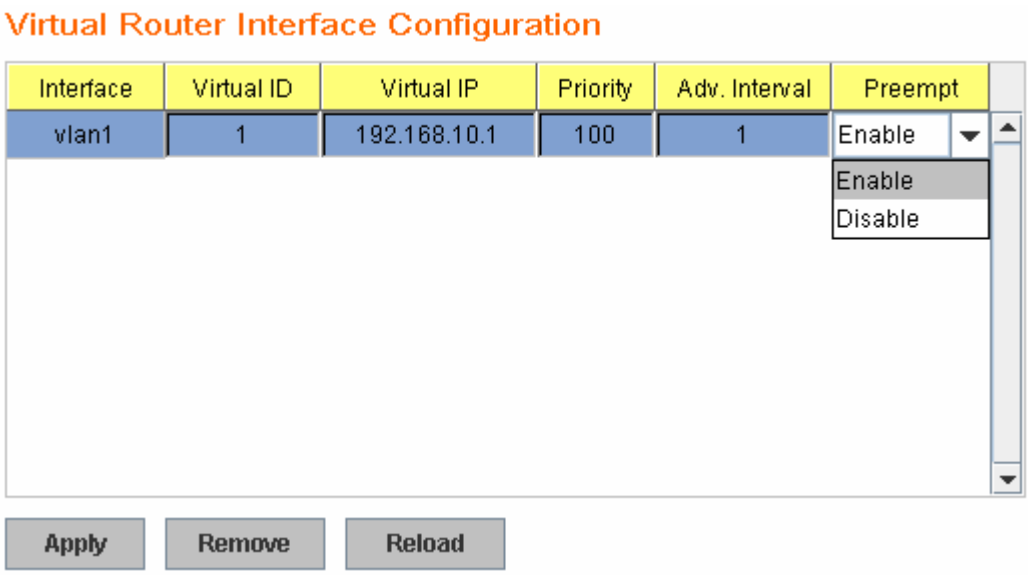
Adv. Interval: This field indicates how often the VRRP switches exchange the VRRP settings.

Preempt: While the VRRP Master link is failure, the VRRP Backup will take over its job immediately. However, while the VRRP master link is recovered, who should be the Master? The Preempt decide whether the VRRP master should be recovered or not.

While the Preempt is **Enabled** and the interface is VRRP Master, the interface will be recovered.

While the Preempt is **Disabled** and the interface is VRRP Master, there is no change while the link is recovered. The VRRP backup acts as the Master before restart the switches.

Click **"Apply"** to change the setting. **"Remove"** to remove the entry. **"Reload"** to reload the new entry and settings.



Virtual Router Status

This page displays the Virtual Router Status of the switch. You can see the related VRRP information after the VRRP switches exchanging information.

Virtual Router Status

Interface	VRID	Priority	Time	Owner	Preemption	State	Master IP address	Virtual IP address
vlan1	1	100	3.609	-	Enabled	Master	192.168.10.1	192.168.10.1

Reload

4.9.8 CLI Commands of the Routing Feature

Command Lines of the Routing configuration

Feature	Command Line
ARP	
Age Time	Switch(config)# arp aging-time <10-21600> seconds (10-21600) Switch(config)# arp aging-time 1200 (20min for example)

Static ARP Entry	Switch(config)# arp
	  A.B.C.D IP address of ARP entry
	  aging-time Aging Time
	Switch(config)# arp 192.168.100.1
	  MACADDR 48-bit hardware address of ARP entry
	Switch(config)# arp 192.168.100.1 0012-7712-3456
	  IFNAME L3 interface
	Switch(config)# arp 192.168.100.1 0012-7712-3456 fa1
	  PORT L2 port
	Switch(config)# arp 192.168.100.1 0012-7712-3456 vlan2 fa1
	
	=> The MAC address 0012-7712-3456 with IP 192.168.100.1 is bind to the port 1 of VLAN 2.

ARP Table	Switch# show arp IP address Mac Address Port Vlan Age(min) Type ---------- ---------- ---- ---- -------- ------- 192.168.10.111 000f.b079.ca3b gi28 1 0 Dynamic
ARP Table Status	Switch# show arp status Age Time (secs) : 9600 ARP entry count : 1 ARP static entry count : 0 ARP dynamic entry count : 1
IP	
Global IP Routing Configuration	Switch(config)# ip routing <cr>
Stop IP Routing	Switch(config)# no ip routing <cr> Note: After enabling the command, the networks of routing protocol will be deleted automatically.
IP Interface Configuration	
Go to the VLAN Interface	Switch(config)# interface vlan 1 Switch(config-if)#
Create IP Address	Switch(config-if)# ip address A.B.C.D/M IP address (e.g. 10.0.0.1/8) Switch(config-if)# ip address 192.168.10.43/24
Create Secondary IP Address	Switch(config-if)# ip address 192.168.101.43/24 secondary
Change Interface to DOWN	Switch(config-if)# shutdown <cr> Switch(config-if)# shutdown

	Interface vlan1 Change to DOWN
Activate the IP Interface	Switch(config-if)# no shutdown arping for the MAC arp: SIOCDARP(pub): No such file or directory ARPING to 192.168.10.254 from 192.168.10.43 via vlan1 Sent 3 probe(s) (3 broadcast(s)) Received 0 reply (0 request(s), 0 broadcast(s)) Interface vlan1 Change to UP
Show ip routing status	Switch# show ip routing IP routing is on
Show ip interface	Switch# show running-config …… ! interface vlan1 ip address 192.168.10.43/24 ip address 192.168.101.43/24 secondary ip address 192.168.11.1/24 secondary no shutdown ! interface vlan2 ip address 192.168.2.254/24 no shutdown ip igmp ! interface vlan3 ip address 192.168.3.254/23 no shutdown
Router	
Default Route	Switch(config)# ip route 0.0.0.0 0.0.0.0 192.168.100.1 The first 0.0.0.0 means all the unknown networks. The second 0.0.0.0 means all the masks. The last IP address is the IP address of the next hop.
Static Route	Switch# show ip route 192.168.11.0 (static network IP) Routing entry for 192.168.11.0/24 Known via "connected", distance 0, metric 0, best * directly connected, vlan1 Routing entry for 192.168.11.0/24 Known via "static", distance 1, metric 0 192.168.10.254, via vlan1
Show Static/Dynamic Route	Switch# show running-config …… ! ip route 0.0.0.0/0 192.168.100.1 ip route 192.168.11.0/24 192.168.10.254 !
Routing Table Display	Switch# show ip route Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF, B - BGP, > - selected route, * - FIB route O 192.168.2.0/24 [110/40] via 192.168.5.254, vlan5, 00:09:31

	C>* 192.168.2.0/24 is directly connected, vlan2 O>* 192.168.3.0/24 [110/30] via 192.168.5.254, vlan5, 00:09:31 O>* 192.168.4.0/24 [110/20] via 192.168.5.254, vlan5, 00:09:31 O 192.168.5.0/24 [110/10] is directly connected, vlan5, 00:09:31 C>* 192.168.5.0/24 is directly connected, vlan5 O 192.168.10.0/24 [110/10] is directly connected, vlan1, 00:07:15 C>* 192.168.10.0/24 is directly connected, vlan1 O>* 192.168.12.0/24 [110/40] via 192.168.5.254, vlan5, 00:09:31 O>* 192.168.13.0/24 [110/30] via 192.168.5.254, vlan5, 00:09:31 O>* 192.168.14.0/24 [110/20] via 192.168.5.254, vlan5, 00:09:31
RIP **(Before enable RIP, the IP Interfaces' setting should be configured and activated first.)**	
Enable RIP protocol	Switch(config)# router rip Switch(config-router)# default-information Control distribution of default route default-metric Set a metric of redistribute routes distance Administrative distance distribute-list Filter networks in routing updates end End current mode and change to enable mode exit Exit current mode and down to previous mode list Print command list neighbor Specify a neighbor router network Enable routing on an IP network no Negate a command or set its defaults offset-list Modify RIP metric passive-interface Suppress routing updates on an interface quit Exit current mode and down to previous mode redistribute Redistribute information from another routing protocol route RIP static route configuration route-map Route map set timers Adjust routing timers version Set routing protocol version
RIP Version	Switch(config-router)# version <1-2> version Switch(config-router)# version 2
RIP Network	Switch(config-router)# network 192.168.100.0/24
RIP Timer	Switch(config-router)# timers basic <5-2147483647> Routing table update timer value in second. Default is 30.
RIP Split Horizon	Switch(config-router)# passive-interface IFNAME Interface name default default for all interfaces

	Switch(config-router)# passive-interface default <cr>
RIP default Metric (usually = 1)	Switch(config-router)# default-metric <1-16> Default metric

RIP Setting	Switch# show ip rip status
	Routing Protocol is "rip"
	  Sending updates every 30 seconds with +/-50%, next due in 23 seconds
	  Timeout after 180 seconds, garbage collect after 120 seconds
	  Outgoing update filter list for all interface is not set
	  Incoming update filter list for all interface is not set
	  Default redistribution metric is 1
	  Redistributing:
	  Default version control: send version 2, receive version 2
	  Interface Send Recv Key-chain
	  vlan1 2 2
	  Routing for Networks:
	  192.168.10.0/24
	  192.168.100.0/24
	  Passive Interface(s):
	  sw0.1
	  Routing Information Sources:
	  Gateway BadPackets BadRoutes Distance Last Update
	  Distance: (default is 120)
	
	==========
	Switch# show running-config
	….
	!
	router rip
	  version 2
	  network 192.168.10.0/24
	  network 192.168.100.0/24
	  passive-interface default
	….

RIP Table	Switch# show ip rip
	Codes: R - RIP, C - connected, S - Static, O - OSPF, B - BGP
	Sub-codes:
	  (n) - normal, (s) - static, (d) - default, (r) - redistribute,
	  (i) - interface
	
	  Network Next Hop Metric From Tag Time
	C(i) 192.168.10.0/24 0.0.0.0 1 self 0

OSPF **(Before enable OSPF, the IP Interfaces' setting should be configured and activated first.)**	

Go to the OSPF command line	Switch(config)# router ospf
	Switch(config-router)#
	  area OSPF area parameters
	  auto-cost Calculate OSPF interface cost according to bandwidth
	  compatible OSPF compatibility list
	  default-information Control distribution of default

	information default-metric Set metric of redistributed routes distance Define an administrative distance distribute-list Filter networks in routing updates end End current mode and change to enable mode exit Exit current mode and down to previous mode list Print command list neighbor Specify neighbor router network Enable routing on an IP network no Negate a command or set its defaults passive-interface Suppress routing updates on an interface quit Exit current mode and down to previous mode redistribute Redistribute information from another routing protocol refresh Adjust refresh parameters router-id router-id for the OSPF process timers Adjust routing timers
Router ID for OSPF	Switch(config-router)# router-id 192.168.3.253
OSPF Network and its Area ID (0.0.0.0 for example)	Switch(config-router)# network 192.168.3.0/24 area <0-4294967295> OSPF area ID as a decimal value A.B.C.D OSPF area ID in IP address format Switch(config-router)# network 192.168.3.0/24 area 0.0.0.0
Interface Configuration	
Hello Interface	Switch(config-if)# ip ospf hello-interval <1-65535> Seconds Switch(config-if)# ip ospf hello-interval 10
Link Cost Change	Switch(config-if)# ip ospf cost <1-65535> Cost
Link Priority	Switch(config-if)# ip ospf priority <0-255> Priority
Display	
IP OSPF Information	Switch# show ip ospf OSPF Routing Process, Router ID: 192.168.3.254 Supports only single TOS (TOS0) routes This implementation conforms to RFC2328 RFC1583Compatibility flag is disabled SPF schedule delay 1 secs, Hold time between two SPFs 1 secs Refresh timer 10 secs Number of external LSA 0 Number of areas attached to this router: 1 Area ID: 0.0.0.0 (Backbone) Number of interfaces in this area: Total: 3, Active: 3 Number of fully adjacent neighbors in this area: 1 Area has no authentication SPF algorithm executed 9 times Number of LSA 5
IP OSPF Datasheet	Switch# show ip ospf database

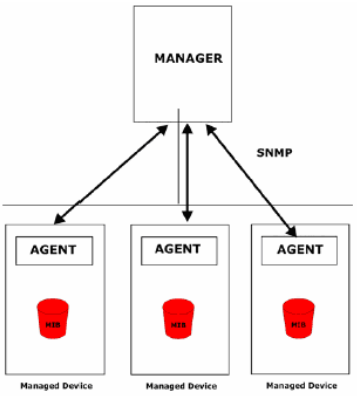
	OSPF Router with ID (192.168.3.254) Router Link States (Area 0.0.0.0) Link ID ADV Router Age Seq# CkSum Link count 192.168.3.253 192.168.3.253 928 0x80000009 0xf3b2 2 192.168.3.254 192.168.3.254 927 0x8000000a 0xd4aa 3 192.168.5.254 192.168.5.254 230 0x80000006 0xc248 2 Net Link States (Area 0.0.0.0) Link ID ADV Router Age Seq# CkSum 192.168.3.254 192.168.3.254 927 0x80000003 0x7437 192.168.4.253 192.168.5.254 235 0x80000003 0x7334
IP OSPF Interface Information	Switch# show ip ospf interface [IFNAME] Interface name Switch# show ip ospf interface vlan2 vlan2 is up Internet Address 192.168.2.253/24, Area 0.0.0.0 Router ID 192.168.3.253, Network Type BROADCAST, Cost 10 Transmit Delay is 1 sec, State DR, Priority 1 Designated Router (ID) 192.168.3.253, Interface Address 192.168.2.253 No backup designated router on this network Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5 Hello due in 00:00:02 Neighbor Count is 1, Adjacent neighbor count is 1
IP OSPF Neighbor Table	Switch# show ip ospf neighbor Neighbor ID Pri State Dead Time Address Interface --- --- --- --- --- --- 0.0.0.0 1 Full/DROther 00:00:32 192.168.2.254 vlan2:192.168.2.25 3
IP OSPF Networking Routing Table	Switch# show ip ospf route ========== OSPF network routing table ========== N 192.168.2.0/24 [10] area: 0.0.0.0 directly attached to vlan2 N 192.168.3.0/24 [10] area: 0.0.0.0 directly attached to vlan3 N 192.168.11.0/24 [10] area: 0.0.0.0 directly attached to vlan1
OSPF Setting in Configuration file	Switch# show running-config …… router ospf router-id 192.168.3.253 network 192.168.2.0/24 area 0.0.0.0 network 192.168.3.0/24 area 0.0.0.0 network 192.168.11.0/24 area 0.0.0.0 ! ip routing ……..

DVMRP **(Before enable DVMRP, the IP Interfaces' setting should be configured and activated first.)**	
Enable the DVMRP	Switch(config)# ip multicast-routing dvmrp DVMRP is successfully enabled on the switch
	Switch(config)# router dvmrp Switch(config-dvmrp)# end Exit current mode and down to previous enable mode exit Exit current mode and down to previous mode list Print command list network Enable multicast routing on an IP network no Disable multicast routing on an IP network quit Exit current mode and down to previous mode
Add DVMRP Network	Switch(config-dvmrp)# network 192.168.2.0/24 Switch(config-dvmrp)# network 192.168.3.0/24
DVMRP Information	Switch# show ip dvmrp <cr> neighbors DVMRP neighbors route DVMRP route Switch# show ip dvmrp DVMRP Enabled on: 192.168.10.0/24 192.168.2.0/24 192.168.5.0/24
DVMRP Routing Table	Switch# show ip dvmrp route Code: C - connected, D - DVMRP routes, h - hold-down F Time Prefix Next Hop IF Metric Time > C 03:53:40 192.168.2.0/24 192.168.2.254 vlan2 0 00:00:00 > D 03:52:40 192.168.3.0/24 192.168.5.254 vlan5 3 00:00:40 > D 03:53:39 192.168.4.0/24 192.168.5.254 vlan5 2 00:00:40 > C 03:53:40 192.168.5.0/24 192.168.5.253 vlan5 0 00:00:00 > C 03:53:40 192.168.10.0/24 192.168.10.254 vlan1 0 00:00:00
DVMRP Neighbor Table	Switch# show ip dvmrp neighbors Neighbor Address If Timeleft Holdtime Index 192.168.5.254 vlan5 33 34 1
VRRP **(Go to the Interface mode)**	
IP of VRRP	Switch(config-if)# vrrp 1 ip 192.168.10.1 The virtual router of vlan1 count is 1. Create virtual router 1 success.
Priority of the interface	Switch(config-if)# vrrp 1 priority <1-254> virtual router's priority value in range 1-254, 255 for virtual IP owner and 100 for backup by default
Preempt of the interface	Switch(config-if)# vrrp 1 preempt Set virtual router preemption mode to enabled success.
VRRP Information	Switch# show vrrp

	[1-255] virtual router identifier in the range 1-255 (decimal) brief display a summary view of the virtual router information Switch# show vrrp vlan1 - Virtual Router ID 1 State is Master Virtual IP address is 192.168.10.1 Virtual MAC address is 0000.5e00.0101 Priority is 100 Advertisement interval is 1 sec Preemption is enabled Master Router is 192.168.10.1 (local), priority is 100 Master Advertisement interval is 1.000 sec Master Down interval is 3.609 sec
VRRP Brief Information	Switch# show vrrp brief Interface VRID Priority Time Owner Preemption State Master addr Group addr vlan1 1 100 3.609 - enabled Master 192.168.10.1 192.168.10.1

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. JetNet 5628G/5828G series support SNMP v1 and v2c and V3.



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

Following commands are included in this group:

4.8.1 SNMP Configuration

4.8.2 SNMPv3 Profile

4.8.3 SNMP Traps

4.8.4 SNMP CLI Commands for SNMP

4.10.1 SNMP Configuration

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

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

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

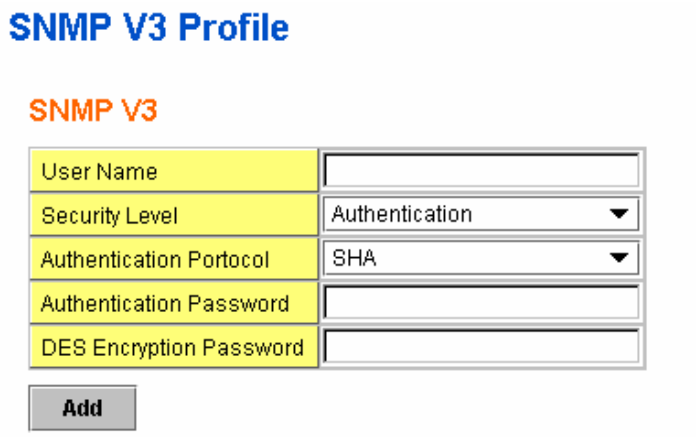
With **Read and Write** privilege, you have the ability to read and set the values of MIB tables. Default community string is Private.

JetNet 5628G/5828G allows users to assign 4 community strings. Type the community string and select the privilege. Then press **Apply**.

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

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 5628G/5828G* 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 5628G/5828G* 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.

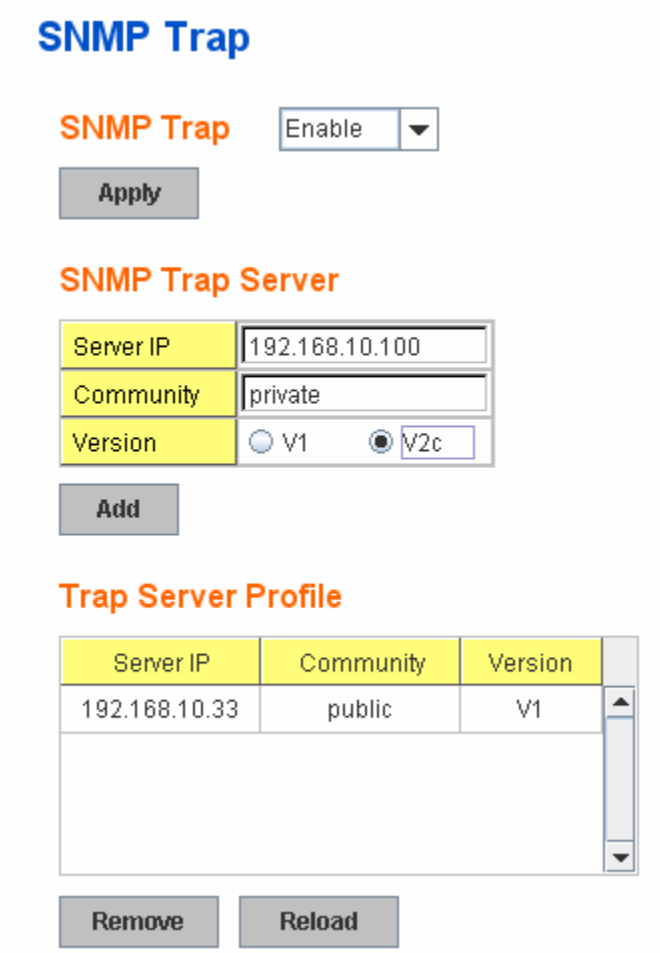
Authentication Password: Here the user enters the SNMP v3 user authentication password.

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 V2**. After configuration, you can see the change of the SNMP pre-defined standard traps and Korenix pre-defined traps. The pre-defined traps can be found in Korenix private MIB.



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 5628G/5828G provides several security features for you to secure your connection. The features include Port Security and IP Security.

Following commands are included in this group:

4.9.1 Filter Set (Access Control List)

4.9.2 IEEE 802.1x

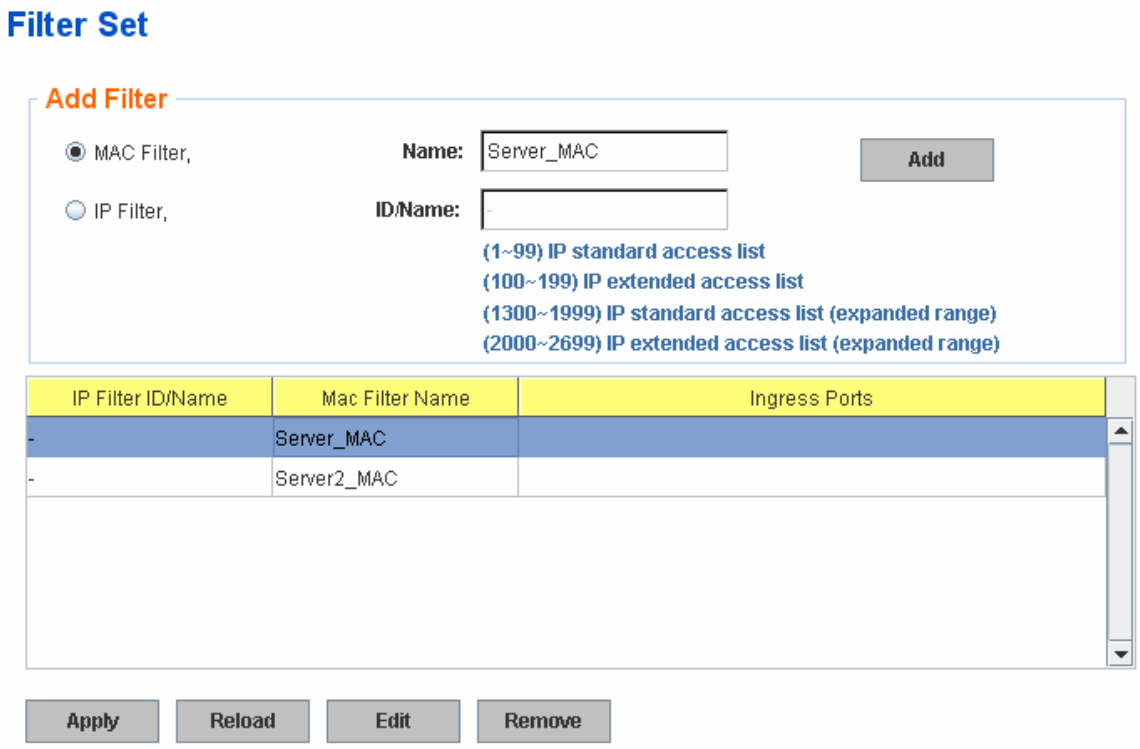
4.9.3 CLI Commands of the Security

4.11.1 Filter Set (Access Control List)

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

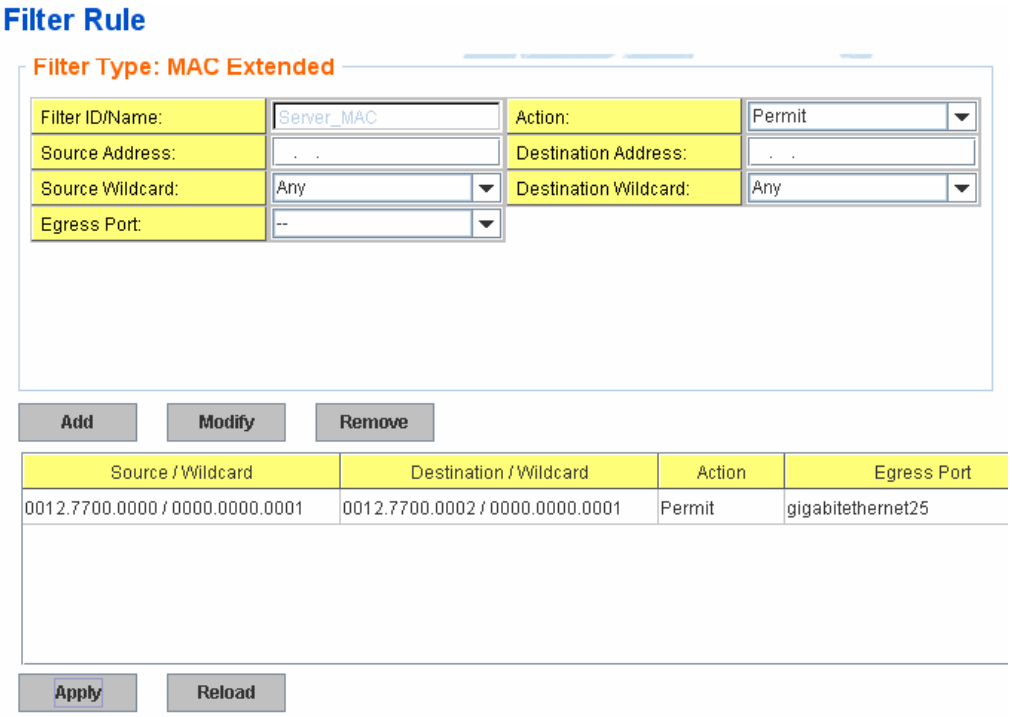
ACE is short of Access Control Entry, user defines the Permit or Deny rule for specific IP/MAC address or IP groups by network mask in each ACE. One ACL may include several ACEs, the system checks the ACEs one after one and forward based on the result. Once the rules conflict, the old entry is selected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

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



MAC Filter (Port Security):

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



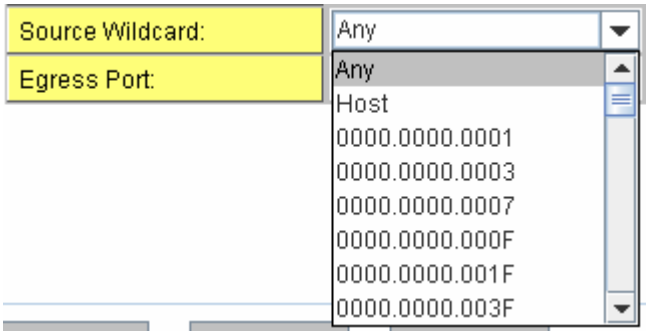
Filter ID/Name: The name for this MAC Filter entry.

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

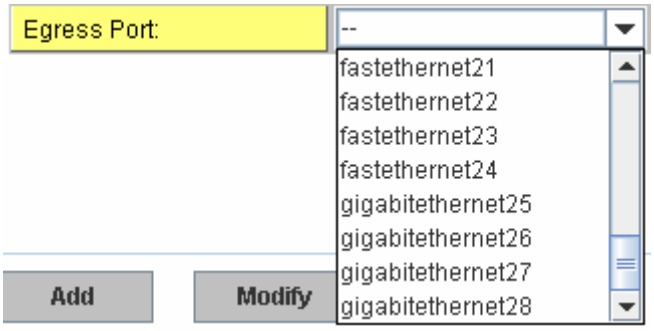
Source/Destination Address: Type the MAC address you want configure, the format is "AABB.CCDD.EEFF". Example: "Source to Destination" is "0012.7700.0000 to 0012.7700.0002".

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

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



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

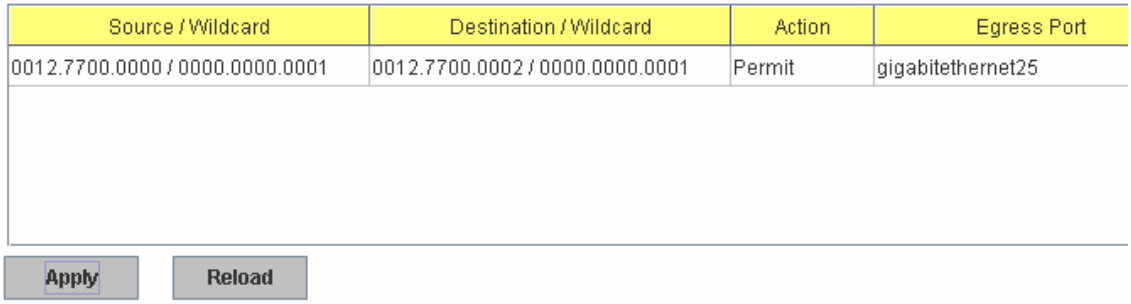


Once you finish configuring the ACE settings, click on **Add** to apply your configuration. You can see below screen is shown.

Example of the below Entry:

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

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



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

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

IP Filter:

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

Example:

Filter Set

Add Filter

MAC Filter, Name: - Add

IP Filter, ID/Name: 1

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

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

Apply Reload Edit Remove

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

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

Filter Rule

Filter Type: IP Extended

Filter ID/Name:	100	Action:	Permit
Source Address:	192.168.10.2	Destination Address:	192.168.10.200
Source Wildcard:	Host	Destination Wildcard:	Host
Protocol:	IP		
Source Port:		Destination Port:	
Source Port Wildcard:	Any	Destination Port Wildcard:	Any
ICMP Type:	--	ICMP Code:	--
Egress Port:	fastethernet2		

Add Modify Remove

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

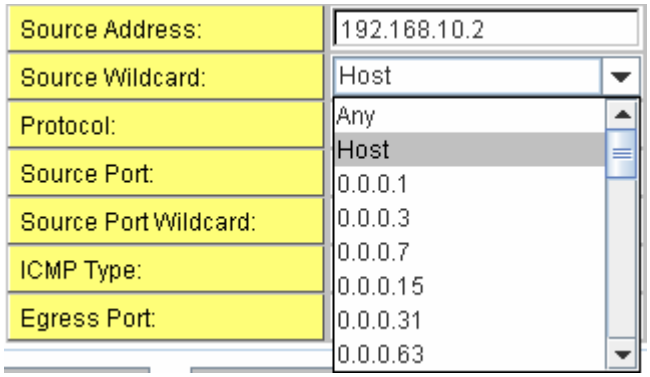
Apply Reload

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

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

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

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



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

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

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

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

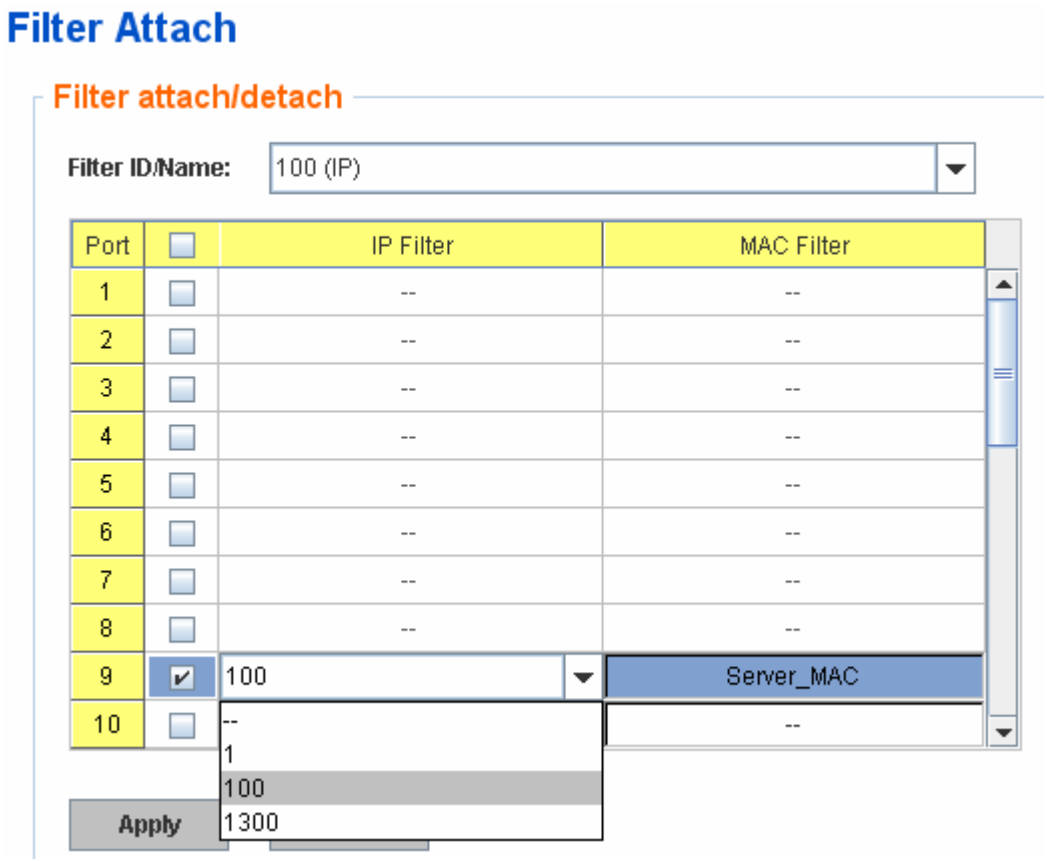
ICMP Type: The ICMP Protocol Type range from 1 ~ 255.

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

Egress Port: Bind this Filter to selected egress port.

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

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



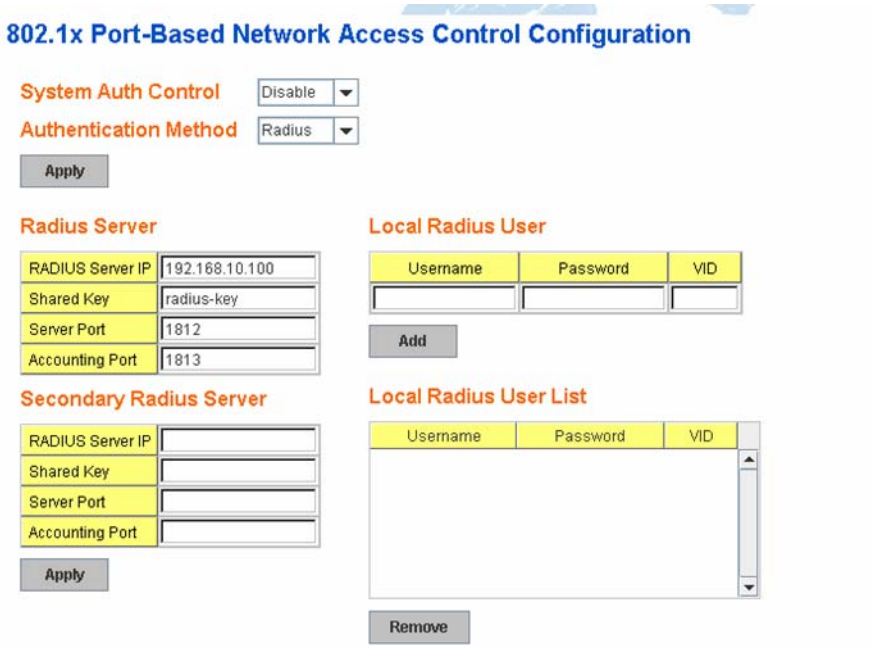
4.11.2 Filter Set (Access Control List)

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

4.11.3 IEEE 802.1x

4.9..1 802.1X configuration

IEEE 802.1X is the protocol that performing authentication to obtain access to IEEE 802 LANs. It is port-base network access control. With the function, JetNet 5628G/5828G could control which connection is available or not.



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

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

Radius Server IP: The IP address of Radius server

Shared Key: The password for communicate between switch and Radius Server.

Server Port: UDP port of Radius server.

Accounting Port: Port for packets that contain the information of account login or logout.

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

802.1X Local User: Here User can add Account/Password for local authentication.

802.1X Local user List: This is a list shows the account information, User also can remove selected account Here.

4.9.3.2 802.1x Port Configuration

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

802.1x Port Configuration

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

Apply | Initialize Selected | Reauthenticate Selected

802.1x Timeout Configuration

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

Apply

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

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

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

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

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

Control Direction: determined devices can end data out only or both send and receive.

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

Quiet Period: When authentication failed, Switch will wait for a period and try to communicate with radius server again.

Tx period: the time interval of authentication request.

Supplicant Timeout: the timeout for the client authenticating

Sever Timeout: The timeout for server response for authenticating.

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

Click **Initialize Selected** to set the authorize state of selected port to initialize status.

Click **Reauthenticate Selected** to send EAP Request to supplicant to request reauthentication.

Click **Default Selected** to reset the configurable 802.1x parameters of selected port to the default values.

4.9.3.3 802.1X Port Status

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

802.1x Port-Based Network Access Control Port Status

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

Reload

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	
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 username korenix passwd korenix vlan 1

4.12 Warning

JetNet 5628G/5828G provides several types of Warning features for you to remote monitor the status of end devices or the change of your network. The features include Fault Relay, System Log and SMTP E-mail Alert.

Following commands are included in this group:

4.10.1 Fault Relay

4.10.2 Event Selection

4.10.3 Syslog Configuration

4.10.4 SMTP Configuration

4.10.5 CLI Commands

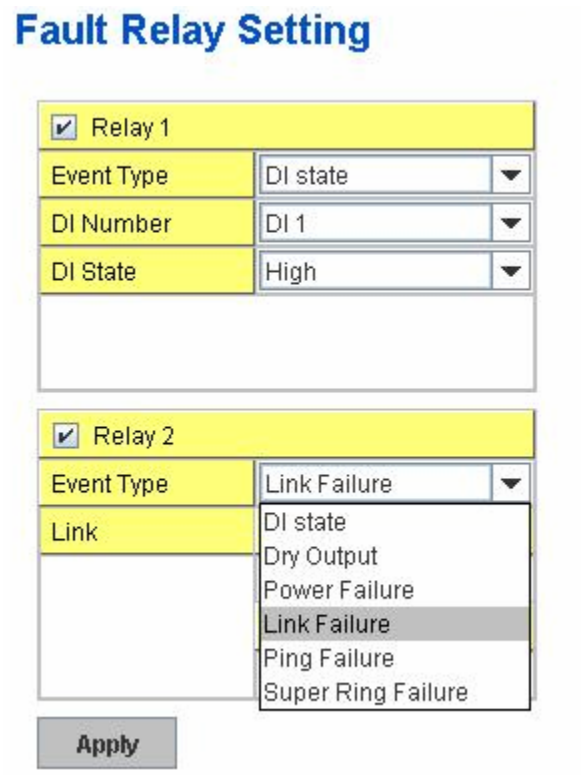
4.12.1 Fault Relay

JetNet 5628G/5828G provides 2 digital outputs, also known as Relay Output. The relay contacts are energized (open) for normal operation and will close under fault conditions. Fault conditions include DI State change, Periodical On/Off, Power Failure, Ethernet port Link Failure, Ping Failure and Super Ring Topology Change. You can configure these settings in this Fault Relay Setting. Each Relay can be assigned 1 fault condition.

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

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

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

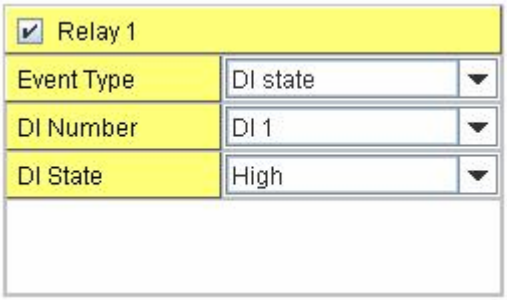


Event Type: **DI State**

DI Number: Select DI 1 or DI 2. Select which DI you want to monitor.

DI State: High or Low. Select the power voltage you want to monitor.

How to configure: Select the DI Number you want to monitor and DI State, High or Low. For example: When DI 1 and High are selected, it means when DI 1 is pulled high, the system will short Relay Output and light DO LED.

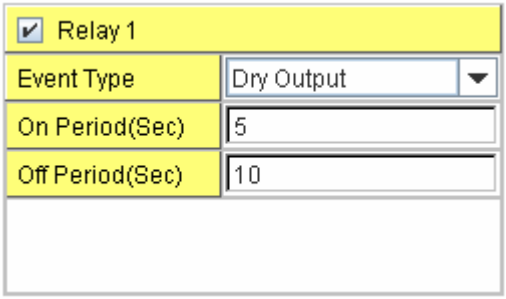


Event Type: **Dry Output**

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

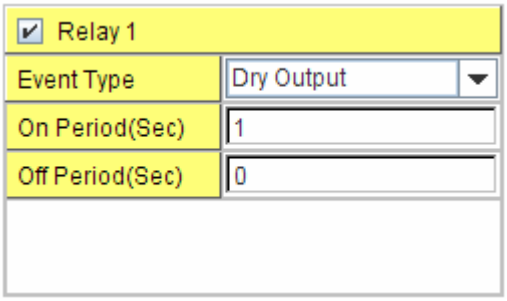
Off Period (Sec): Type the period time to turn off Relay Output. Available range of a period is 0-4294967295 seconds.

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

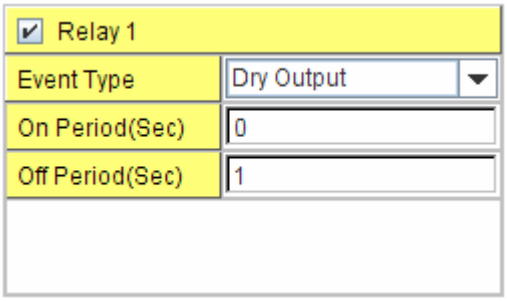


Relay turn on for 5 seconds then off for 10 seconds

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



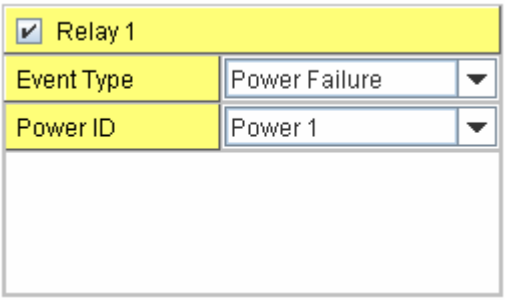
Turn on the relay output



Turn off the relay output

Event Type: **Power Failure**

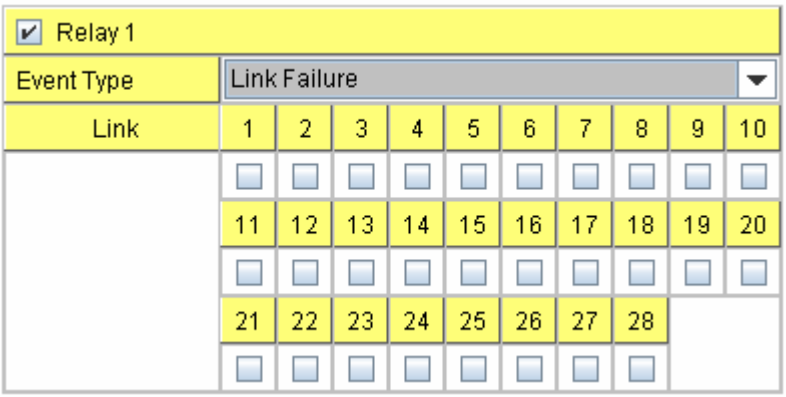
Power ID: Select Power AC1, Power AC2, Power DC 1, Power DC2 or Any you want to monitor. When the power you selected is shut down or broken, the system will short Relay Out and light the DO LED.



Event Type: **Like Failure**

Link: Select the port ID you want to monitor.

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

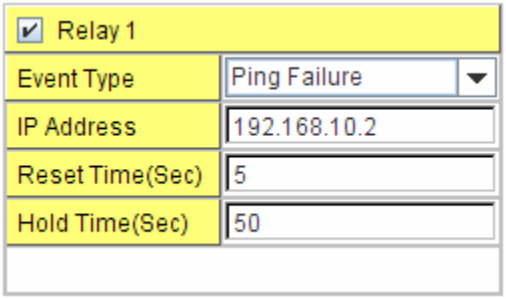


Event Type: **Ping Failure**

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

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

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



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

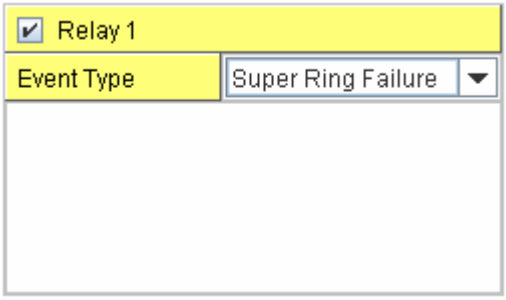
After the Reset Time timeout, the system will turn the Relay Output to close state. After the Hold Time timer is timeout, the switch system will start ping the target device.

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

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

Event Type: **Super Ring Failure**

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



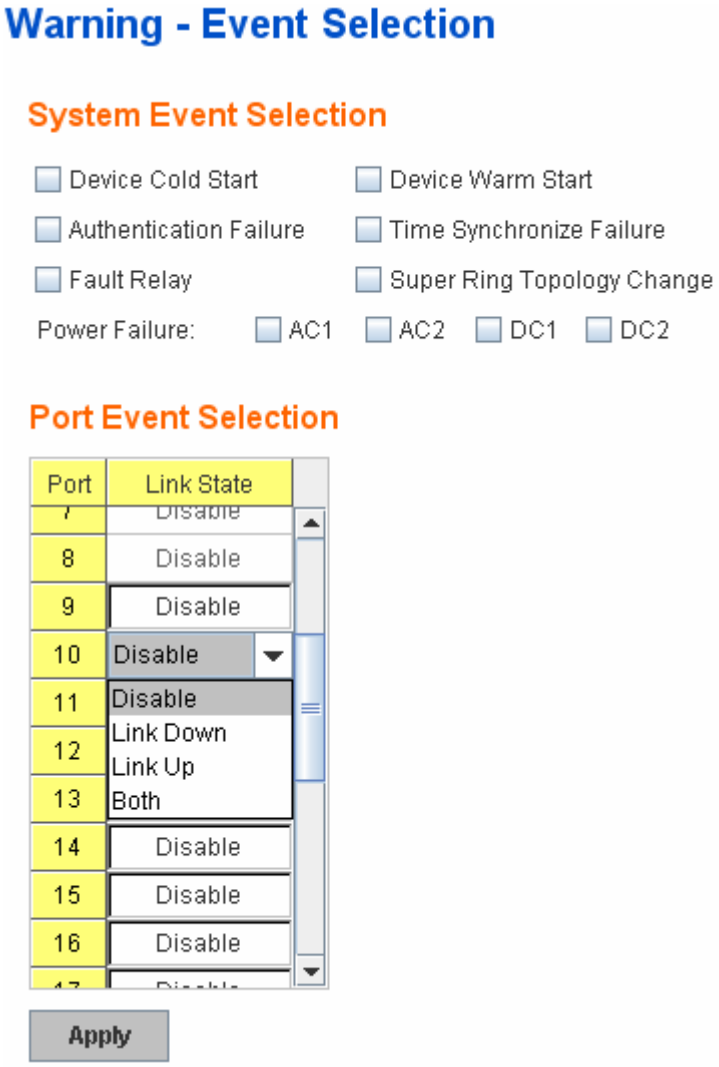
Once you finish configuring the settings, click on **Apply** to apply your configuration.

4.12.2 Event Selection

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

System Event	Warning Event is sent when…..
Device Cold Start	Power is cut off and then reconnected.
Device Warm Start	Reboot the device by CLI or Web UI.
Authentication failure	An incorrect password, SNMP Community String is entered.
Time Synchronize Failure	Accessing to NTP Server is failure.
Fault Relay	The DO/Fault Relay is on.
Super Ring Topology Changes	Master of Super Ring has changed or backup path is activated.
Power Failure AC1, AC2,	Selected Power ID is failure.

DC1, DC2	
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.

4.12.3 SysLog Configuration

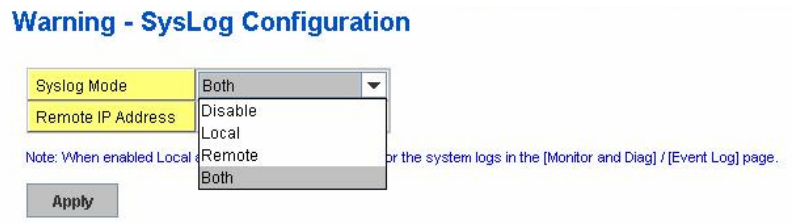
System Log is useful to provide system administrator locally or remotely monitor switch events history. There are 2 System Log modes provided by JetNet 5628G/5828G, local mode and remote mode.

Local Mode: In this mode, JetNet 5628G/5828G will print the occurred events selected in the Event Selection page to System Log table of JetNet 5628G/5828G. You can monitor the system logs in [Monitor and Diag] / [Event Log] page.

Remote Mode: The remote mode is also known as Server mode in JetNet 4500 series. In this mode, you should assign the IP address of the System Log server. JetNet

5628G/5828G 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.



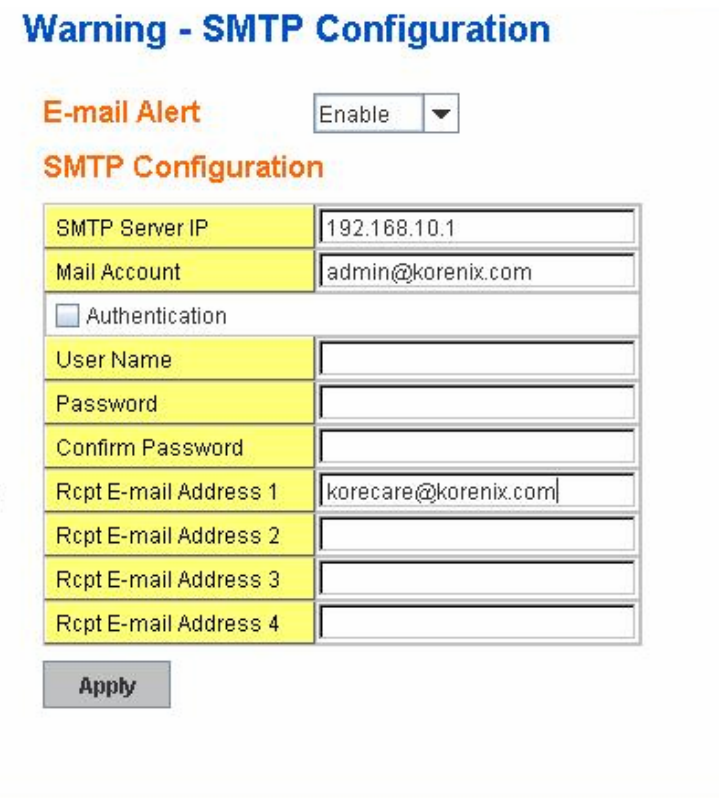
Once you finish configuring the settings, click on **Apply** to apply your configuration.

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

4.12.4 SMTP Configuration

JetNet 5628G/5828G supports E-mail Warning feature. The switch will send the occurred events to remote E-mail server. The receiver can then receive notification by E-mail. The E-mail warning is conformed to SMTP standard.

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



Field	Description
SMTP Server IP Address	Enter the IP address of the email Server
Authentication	Click on check box to enable password
User Name	Enter email Account name (Max.40 characters)
Password	Enter the password of the email account
Confirm Password	Re-type the password of the email account
You can set up to 4 email addresses to receive email alarm from JetNet	
Rcpt E-mail Address 1	The first email address to receive email alert from JetNet (Max. 40 characters)
Rcpt E-mail Address 2	The second email address to receive email alert from JetNet (Max. 40 characters)
Rcpt E-mail Address 3	The third email address to receive email alert from JetNet (Max. 40 characters)
Rcpt E-mail Address 4	The fourth email address to receive email alert from JetNet (Max. 40 characters)

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

4.12.5 CLI Commands

Command Lines of the Warning configuration

Feature	Command Line
Relay Output	
Relay Output	Switch(config)# relay 1 di DI state dry dry output ping ping failure port port link failure power power failure ring super ring failure ***Note: Select Relay 1 or 2 first, then select the event types.***
DI State	Switch(config)# relay 1 di <1-2> DI number Switch(config)# relay 1 di 1 high high is abnormal low low is abnormal Switch(config)# relay 1 di 1 high
Dry Output	Switch(config)# relay 1 dry <0-4294967295> turn on period in second Switch(config)# relay 1 dry 5 <0-4294967295> turn off period in second Switch(config)# relay 1 dry 5 5
Ping Failure	Switch(config)# relay 1 ping 192.168.10.33

	<cr> reset reset a device Switch(config)# relay 1 ping 192.168.10.33 reset <1-65535> reset time Switch(config)# relay 1 ping 192.168.10.33 reset 60 <0-65535> hold time to retry Switch(config)# relay 1 ping 192.168.10.33 reset 60 60
Port Link Failure	Switch(config)# relay 1 port PORTLIST port list Switch(config)# relay 1 port fa1-5
Power Failure	Switch(config)# relay 1 power <1-4> power id (1: AC1, 2: AC2, 3:DC1, 4:DC2) any Anyone power failure asserts relay Switch(config)# relay 1 power 1
Super Ring Failure	Switch(config)# relay 1 ring
Disable Relay	Switch(config)# no relay <1-2> relay id Switch(config)# no relay 1 *(Relay_ID: 1 or 2)* <cr>
Display	Switch# show relay 1 Relay Output Type : Port Link Port : 1, 2, 3, 4, Switch# show relay 2 Relay Output Type : Super Ring
Event Selection	
Event Selection	Switch(config)# warning-event coldstart Switch cold start event warmstart Switch warm start event linkdown Switch link down event linkup Switch link up event authentication Authentication failure event fault-relay Switch fault relay event power Switch power failure event super-ring Switch super ring topology change event time-sync Switch time synchronize event
Ex: Cold Start event	Switch(config)# warning-event coldstart Set cold start event enable ok.
Ex: Link Up event	Switch(config)# warning-event linkup [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: Enabled Warm Start: Disabled Authentication Failure: Disabled Link Down: fa4-5 Link Up: fa4-5 Power Failure: Super Ring Topology Change: Disabled Fault Relay: Disabled Time synchronize Failure: Disable
Syslog Configuration	
Local Mode	Switch(config)# log syslog local
Server Mode	Switch(config)# log syslog remote 192.168.10.33
Both	Switch(config)# log syslog local

	Switch(config)# log syslog remote 192.168.10.33
Disable	Switch(config)# no log syslog local
SMTP Configuration	
SMTP Enable	Switch(config)# smtp-server enable email-alert SMTP Email Alert set enable ok.
Sender mail	Switch(config)# smtp-server server 192.168.10.100 ACCOUNT SMTP server mail account, ex: admin@korenix.com Switch(config)# smtp-server server 192.168.10.100 admin@korenix.com SMTP Email Alert set Server: 192.168.10.100, Account: admin@korenix.com ok.
Receiver mail	Switch(config)# smtp-server receipt 1 korecare@korenix.com SMTP Email Alert set receipt 1: korecare@korenix.com ok.
Authentication with username and password	Switch(config)# smtp-server authentication username admin password admin SMTP Email Alert set authentication Username: admin, Password: admin ***Note: You can assign string to username and password.***
Disable SMTP	Switch(config)# no smtp-server enable email-alert SMTP Email Alert set disable ok.
Disable Authentication	Switch(config)# no smtp-server authentication SMTP Email Alert set Authentication disable ok.
Dispaly	Switch# sh smtp-server SMTP Email Alert is Enabled Server: 192.168.10.100, Account: admin@korenix.com Authentication: Enabled Username: admin, Password: admin SMTP Email Alert Receipt: Receipt 1: korecare@korenix.com Receipt 2: Receipt 3: Receipt 4:

4.13 Monitor and Diag

JetNet 5628G/5828G provides several types of features for you to monitor the status of the switch or diagnostic for you to check the problem when encountering problems related to the switch. The features include MAC Address Table, Port Statistics, Port Mirror, Event Log and Ping.

Following commands are included in this group:

4.13.1 MAC Address Table

JetNet 5628G/5828G provides 16K entries in MAC Address Table. In this page, users can change the Aging time, add Static Unicast MAC Address, monitor the MAC address or sort them by different packet types and ports. Click on **Apply** to change the value.

Aging Time (Sec)

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

Static Unicast MAC Address

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

MAC Address Table

In this MAC Address Table, you can see all the MAC Addresses learnt by the switch fabric. The packet types include Management Unicast, Static Unicast, Dynamic Unicast, Static Multicast and Dynamic Multicast. The table allows users to sort the address by the packet types and port.

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

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

MAC Address Table

Aging Time (Sec) 300

Apply

Static Unicast MAC Address

MAC Address	VID	Port
		Port 1

Add

MAC Address Table All

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

Remove Reload

4.13.2 Port Statistics

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

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

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

Port Statistics

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

Clear Selected Clear All Reload

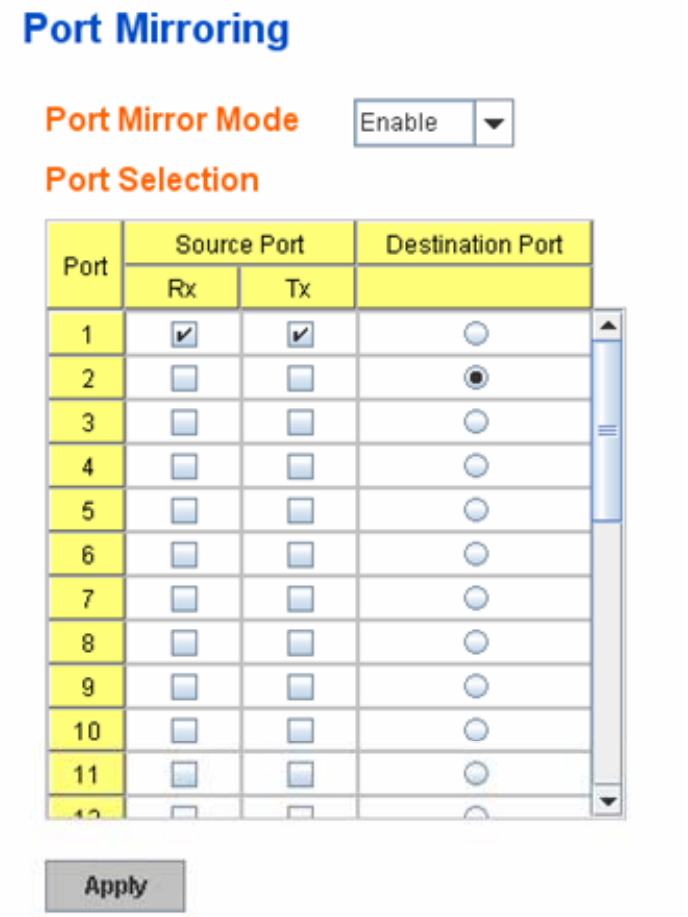
4.13.3 Port Mirroring

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

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

Source Port: This is also known as Monitor Port. These are the ports you want to monitor. The traffic of all source/monitor ports will be copied to destination/analysis ports. You can choose 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.

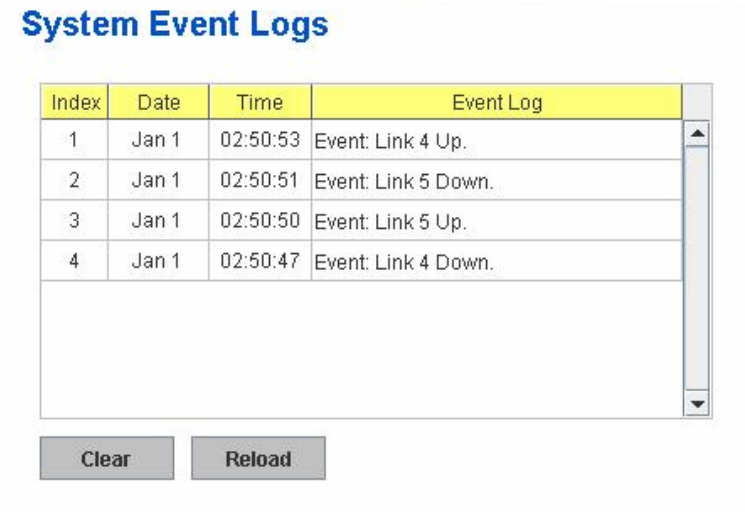


Once you finish configuring the settings, click on **Apply** to apply the settings.

4.13.4 Event Log

In the 4.10.3, we have introduced System Log feature. When System Log Local mode is selected, JetNet 5628G/5828G 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.



4.13.5 Topology Discovery (LLDP)

The 5628G/5828G supports 802.1AB Link Layer Discovery Protocol, thus the 5628G/5828G 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.

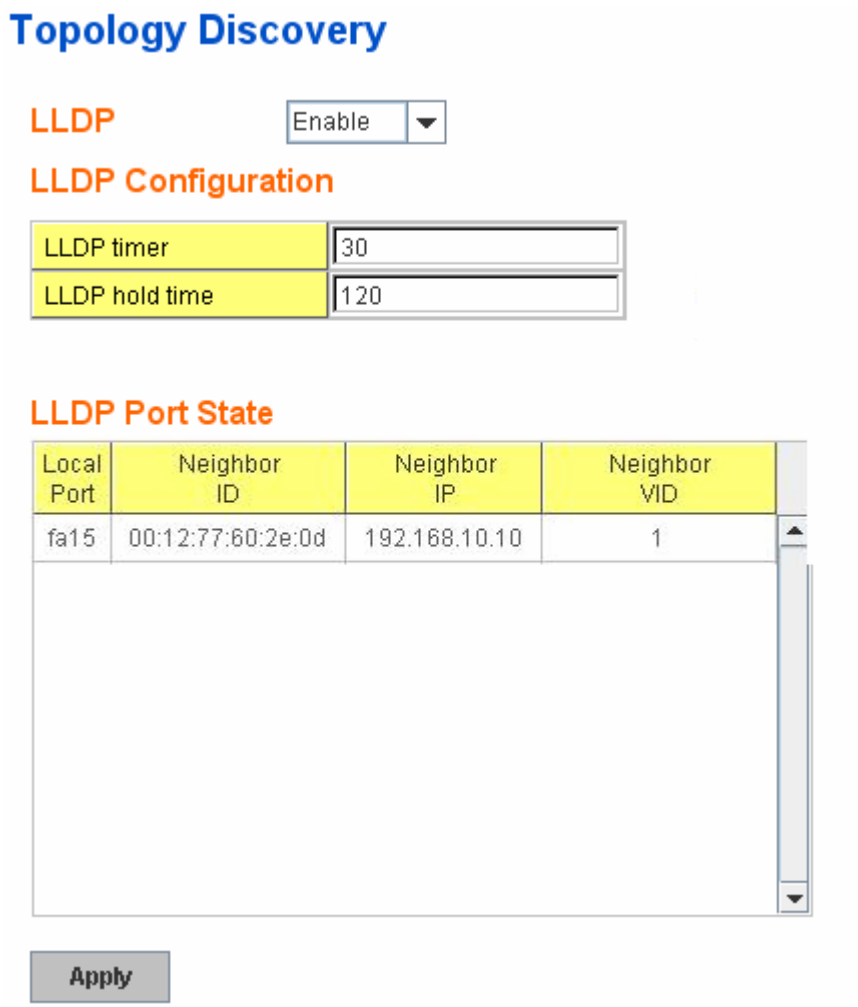
LLDP: Enable/Disable the LLDP topology discovery information.

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.

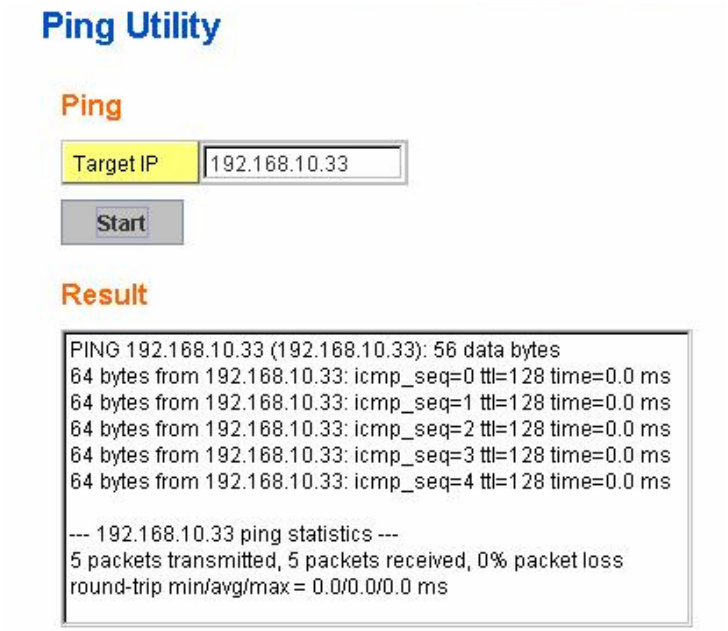
LLDP hold time: The TTL (Time To Live) timer. The LLDP state will be expired once the LLDPDP is not received by the hold time. The default is 120 seconds.

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



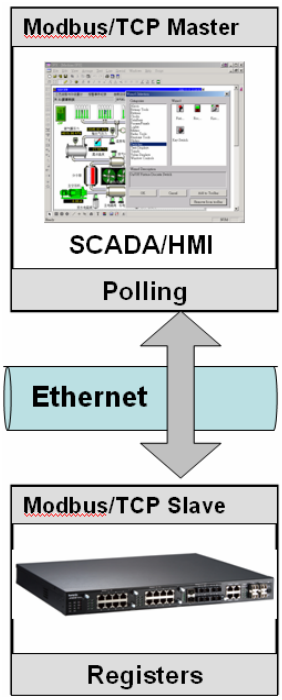
4.13.6 Ping Utility

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

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



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

Korenix JetNet 5628G/5828G implement the Modbus/TCP registers into the latest firmware. The registers include the System information, firmware information, IP address, power status, interfaces’ status, port information, SFP information, inbound/outbound packet information.

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

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

Modbus/TCP Register Table

Word Address	Data Type	Description
System Information		
0x0000	16 words	Vender Name = “Korenix” Word 0 Hi byte = ‘K’ Word 0 Lo byte = ‘o’ Word 1 Hi byte = ‘r’ Word 1 Lo byte = ‘e’ Word 2 Hi byte = ‘n’ Word 2 Lo byte = ‘I’ Word 2 Hi byte = ‘x’ Word 2 Lo byte = ‘\0’ (other words = 0)
0x0010	16 words	Product Name = "JetNet5828G" Word 0 Hi byte = ‘J’

		Word 0 Lo byte = ‘e’ Word 1 Hi byte = ‘T’ Word 1 Lo byte = ‘N’ Word 2 Hi byte = ‘e’ Word 2 Lo byte = ‘t’ Word 3 Hi byte = ‘5’ Word 3 Lo byte = ‘8’ Word 4 Lo byte = ‘2’ Word 4 Hi byte = ‘8’ Word 5 Lo byte = ‘G’ Word 5 Hi byte = ‘\0’ (other words = 0)
0x0020	128 words	SNMP system name (string)
0x00A0	128 words	SNMP system location (string)
0x0120	128 words	SNMP system contact (string)
0x01A0	32 words	SNMP system OID (string)
0x01C0	2 words	System uptime (unsigned long)
0x01C2 to 0x01FF	60 words	Reserved address space
0x0200	2 words	hardware version
0x0202	2 words	S/N information
0x0204	2 words	CPLD version
0x0206	2 words	Boot loader version
0x0208	2 words	Firmware Version Word 0 Hi byte = major Word 0 Lo byte = minor Word 1 Hi byte = reserved Word 1 Lo byte = reserved
0x020A	2 words	Firmware Release Date Firmware was released on 2010-08-11 at 09 o’clock Word 0 = 0x0B09 Word 1 = 0x0A08
0x020C	3 words	Ethernet MAC Address Ex: MAC = 01-02-03-04-05-06 Word 0 Hi byte = 0x01 Word 0 Lo byte = 0x02 Word 1 Hi byte = 0x03

		Word 1 Lo byte = 0x04 Word 2 Hi byte = 0x05 Word 2 Lo byte = 0x06
0x020F to 0x2FF	241 words	Reserved address space
0x0300	2 words	IP address Ex: IP = 192.168.10.1 Word 0 Hi byte = 0xC0 Word 0 Lo byte = 0xA8 Word 1 Hi byte = 0x0A Word 1 Lo byte = 0x01
0x0302	2 words	Subnet Mask
0x0304	2 words	Default Gateway
0x0306	2 words	DNS Server
0x0308 to 0x3FF	248 words	Reserved address space (IPv6 or others)
0x0400	1 word	AC1 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0401	1 word	AC2 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0402	1 word	DC1 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0403	1 word	DC2 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0404 to 0x040F	12 words	Reserved address space
0x0410	1 word	DI1 0x0000:Off 0x0001:On 0xFFFF: unavailable

0x0411	1 word	DI2 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0412	1 word	DO1 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0413	1 word	DO2 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0414 to 0x041F	12 words	Reserved address space
0x0420	1 word	RDY 0x0000:Off 0x0001:On
0x0421	1 word	RM 0x0000:Off 0x0001:On
0x0422	1 word	RF 0x0000:Off 0x0001:On
0x0423	1 word	RS
Port Information (32 Ports)		
0x1000 to 0x11FF	16 words	Port Description
0x1200 to 0x121F	1 word	Administrative Status 0x0000: disable 0x0001: enable
0x1220 to 0x123F	1 word	Operating Status 0x0000: disable 0x0001: enable 0xFFFF: unavailable
0x1240 to 0x125F	1 word	Duplex 0x0000: half 0x0001: full

		0x0003: auto (half) 0x0004: auto (full) 0x0005: auto 0xFFFF: unavailable
0x1260 to 0x127F	1 word	Speed 0x0001: 10 0x0002: 100 0x0003: 1000 0x0004: 2500 0x0005: 10000 0x0101: auto 10 0x0102: auto 100 0x0103: auto 1000 0x0104: auto 2500 0x0105: auto 10000 0x0100: auto 0xFFFF: unavailable
0x1280 to 0x129F	1 word	Flow Control 0x0000: off 0x0001: on 0xFFFF: unavailable
0x12A0 to 0x12BF	1 word	Default Port VLAN ID 0x0001-0xFFFF
0x12C0 to 0x12DF	1 word	Ingress Filtering 0x0000: disable 0x0001: enable
0x12E0 to 0x12FF	1 word	Acceptable Frame Type 0x0000: all 0x0001: tagged frame only
0x1300 to 0x131F	1 word	Port Security 0x0000: disable 0x0001: enable
0x1320 to 0x133F	1 word	Auto Negotiation 0x0000: disable 0x0001: enable 0xFFFF: unavailable
0x1340 to 0x135F	1 word	Loopback Mode 0x0000: none

		0x0001: MAC 0x0002: PHY 0xFFFF: unavailable
0x1360 to 0x137F	1 word	STP Status 0x0000: disabled 0x0001: blocking 0x0002: listening 0x0003: learning 0x0004: forwarding
0x1380 to 0x139F	1 word	Default CoS Value for untagged packets
0x13A0 to 0x13BF	1 word	MDIX 0x0000: disable 0x0001: enable 0x0002: auto 0xFFFF: unavailable
0x13C0 to 0x13DF	1 word	Medium mode 0x0000: copper 0x0001: fiber 0x0002: none 0xFFFF: unavailable
0x13E0 to 0x14FF	288 words	Reserved address space
SFP Information (32 Ports)		
0x1500 to 0x151F	1 word	SFP Type
0x1520 to 0x153F	1 words	Wave length
0x1540 to 0x157F	2 words	Distance
0x1580 to 0x167F	8 words	Vender
0x1680 to 0x17FF	384 words	Reserved address space
SFP DDM Information (32 Ports)		
0x1800 to 0x181F	1 words	Temperature
0x1820 to	2 words	Alarm Temperature

0x185F		
0x1860 to 0x187F	1 words	Tx power
0x1880 to 0x18BF	2 words	Warning Tx power
0x18C0 to 0x18DF	1 words	Rx power
0x18E0 to 0x191F	2 words	Warning Rx power
0x1920 to 0x1FFF	1760 words	Reserved address space
Inbound packet information		
0x2000 to 0x203F	2 words	Good Octets
0x2040 to 0x207F	2 words	Bad Octets
0x2080 to 0x20BF	2 words	Unicast
0x20C0 to 0x20FF	2 words	Broadcast
0x2100 to 0x213F	2 words	Multicast
0x2140 to 0x217F	2 words	Pause
0x2180 to 0x21BF	2 words	Undersize
0x21C0 to 0x21FF	2 words	Fragments
0x2200 to 0x223F	2 words	Oversize
0x2240 to 0x227F	2 words	Jabbers
0x2280 to 0x22BF	2 words	Disacrds
0x22C0 to 0x22FF	2 words	Filtered frames
0x2300 to 0x233F	2 words	RxError

0x2340 to 0x237F	2 words	FCSError
0x2380 to 0x23BF	2 words	Collisions
0x23C0 to 0x23FF	2 words	Dropped Frames
0x2400 to 0x243F	2 words	Last Activated SysUpTime
0x2440 to 0x24FF	191 words	Reserved address space
Outbound packet information		
0x2500 to 0x253F	2 words	Good Octets
0x2540 to 0x257F	2 words	Unicast
0x2580 to 0x25BF	2 words	Broadcast
0x25C0 to 0x25FF	2 words	Multicast
0x2600 to 0x263F	2 words	Pause
0x2640 to 0x267F	2 words	Deferred
0x2680 to 0x26BF	2 words	Collisions
0x26C0 to 0x26FF	2 words	SingleCollision
0x2700 to 0x273F	2 words	MultipleCollision
0x2740 to 0x277F	2 words	ExcessiveCollision
0x2780 to 0x27BF	2 words	LateCollision
0x27C0 to 0x27FF	2 words	Filtered
0x2800 to 0x283F	2 words	FCSError
0x2840 to	447 words	Reserved address space

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

4.13.8 CLI Commands of the Monitor and Diag

Command Lines of the Monitor and Diag configuration

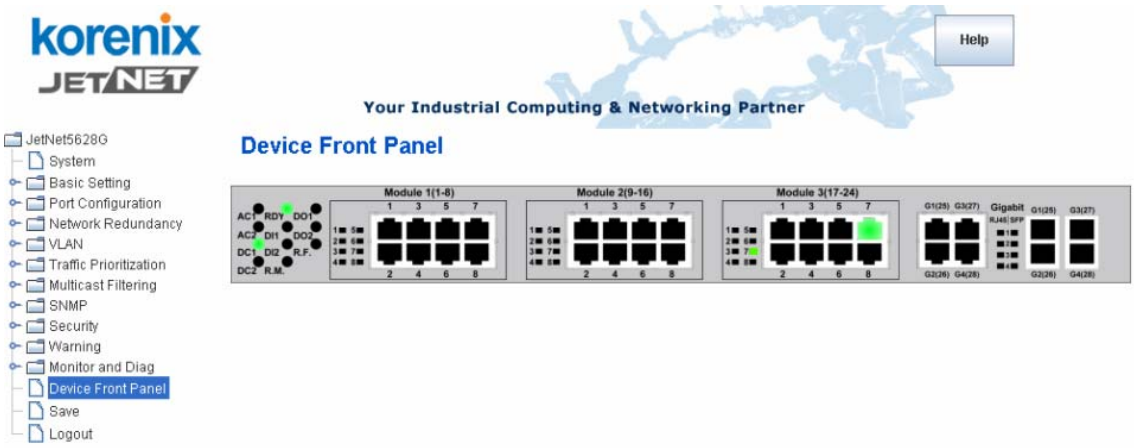
Feature	Command Line
MAC Address Table	
Ageing Time	Switch(config)# mac-address-table aging-time 350 mac-address-table aging-time set ok! *Note: 350 is the new ageing timeout value.*
Add Static Unicast MAC address	Switch(config)# mac-address-table static 0012.7701.0101 vlan 1 interface fastethernet7 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 Port : fa6 Egress Monitor Destination Port : fa6 Ingress Source Ports :fa1,fa2, Egress Source Ports :fa1,fa2,
Event Log	
Display	Switch# show event-log <1>Jan 1 02:50:47 snmpd[101]: Event: Link 4 Down. <2>Jan 1 02:50:50 snmpd[101]: Event: Link 5 Up. <3>Jan 1 02:50:51 snmpd[101]: Event: Link 5 Down. <4>Jan 1 02:50:53 snmpd[101]: Event: Link 4 Up.
Topology Discovery (LLDP)	
Enable LLDP	Switch(config)# lldp holdtime Specify the holdtime of LLDP in seconds run Enable LLDP timer Set the transmission frequency of LLDP in seconds Switch(config)# lldp run LLDP is enabled!
Change LLDP timer	Switch(config)# lldp holdtime <10-255> Valid range is 10~255 Switch(config)# lldp timer <5-254> Valid range is 5~254
Ping	
Ping IP	Switch# ping 192.168.10.33 PING 192.168.10.33 (192.168.10.33): 56 data bytes 64 bytes from 192.168.10.33: icmp_seq=0 ttl=128 time=0.0 ms 64 bytes from 192.168.10.33: icmp_seq=1 ttl=128 time=0.0 ms 64 bytes from 192.168.10.33: icmp_seq=2 ttl=128 time=0.0 ms 64 bytes from 192.168.10.33: icmp_seq=3 ttl=128 time=0.0 ms 64 bytes from 192.168.10.33: icmp_seq=4 ttl=128 time=0.0 ms --- 192.168.10.33 ping statistics --- 5 packets transmitted, 5 packets received, 0% packet loss round-trip min/avg/max = 0.0/0.0/0.0 ms
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

4.12 Device Front Panel

Device Front Panel command allows you to see LED status of the switch. You can see LED and link status of the Power, DO, DI, R.M. and Ports.



JetNet 5628G/5828G Series LED Display

Feature	On / Link UP	Off / Link Down	Other
AC 1 (AC Power)	Green	Black	
AC 2 (AC Power)	Green	Black	
DC 1 (DC Power)	Green	Black	
DC 2 (DC Power)	Green	Black	
DI 1 (Digital Input)	Green	Black	
DI 2 (Digital Input)	Green	Black	
R.M. (Ring Master)	Green	Black	
DO 1 (Digital Output)	Red	Black	
DO 2 (Digital Output)	Red	Black	
R.F. (Ring Failure)	Red	Black	
Fast Ethernet	Green	Black	
Gigabit Ethernet	Green	Black	
SFP	Green	Black	Gray: Plugged but not link up yet.

JetNet 5628G-R/5828G-R Series LED Display

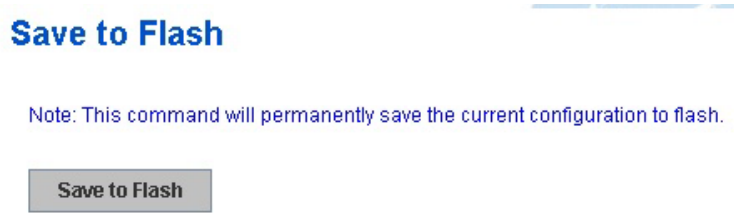
Feature	On / Link UP	Off / Link Down	Other
PWR 1	Green	Black	
PWR 2	Green	Black	
RS	Green: Ring state is normal Amber: Ring state is abnormal	Green Flashing: Incorrect configuration Amber Flashing: One of the ring ports break has	

		been detected	
DO (Digital Output)	Red	Black	
Fast Ethernet	Green	Black	
Gigabit Ethernet	Green	Black	
SFP	Green	Black	Gray: Plugged but not link up yet.

Note: No CLI command for this feature.

4.13 Save to Flash

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



Command Lines:

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

4.14 Logout

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

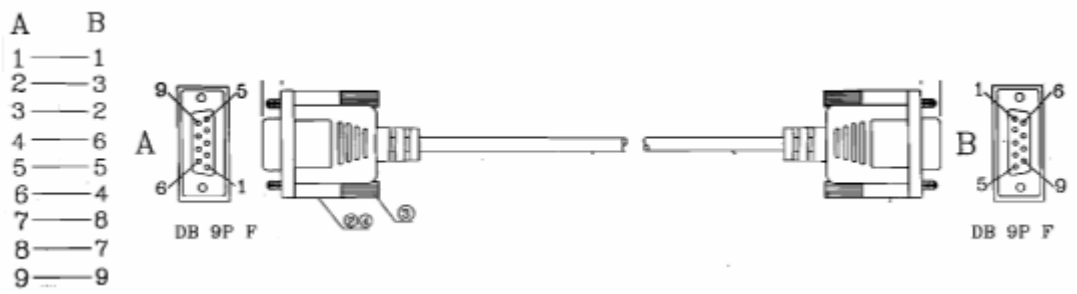
Command Lines:

Feature	Command Line
Logout	SWITCH> exit SWITCH# exit

5 Appendix

5.1 Pin Assignment of the RS-232 Console Cable

The total cable length is 150cm.



5.2 Korenix SFP family

Korenix certificated many types of SFP transceiver. These certificated SFP transceivers can be identified by JetNet 5628G/5828G and displayed in the UI. The SFP transceivers we certificated can meet up the industrial critical environment needs. We recommend you to use Korenix certificated SFP transceivers when you constructing your network.

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

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

Model Name	Spec
SFPGSX	1000Base-SX multi-mode SFP transceiver,550m, -10~70℃
SFPGSX-w	1000Base-SX multi-mode SFP transceiver,550m, wide operating temperature, -40~85℃
SFPGSX2	1000Base-SX plus multi-mode SFP transceiver,2Km, -10~70℃
SFPGSX2-w	1000Base-SX plus multi-mode SFP transceiver, 2Km,wide operating temperature, -10~70℃
SFPGLX10	1000Base-LX single-mode SFP transceiver 10Km, -10~70℃
SFPGLX10-w	1000Base-LX single-mode SFP transceiver, 10Km, wide operating temperature, -40~85℃
SFPGLHX30	1000Base-LHX single-mode SFP transceiver,30Km, -10~70℃
SFPGLHX30-w	1000Base-LHX single-mode SFP transceiver, 30Km, wide operating temperature, -40~85℃
SFPGXD50	1000Base-XD single-mode SFP transceiver, 50Km, -10~70℃
SFPGXD50-w	1000Base-XD single-mode SFP transceiver, 50Km, wide operating temperature, -40~85℃
SFP100MM	Multi-mode 100Mbps 2KM Fiber Transceiver, 0~70℃.
SFP100MM-w	Multi-mode 100Mbps 2KM Fiber Transceiver, wide operating temperature -40~85℃.
SFP100SM30	Single mode 100Mbps 30KM Fiber Transceiver 0~70℃.
SFP100SM30-w	Single mode 100Mbps 30Km Fiber Transceiver, wide operating temperature. -40~85℃

5.3 Korenix Private MIB

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

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

The path of the JetNet 5628G/5828G is **1.3.6.1.4.1.24062.2.2.6**.

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

5.4 Revision History

Edition	Date	Modifications
V1.4	Jun. 17, 2011	Add Modbus/TCP description & Register Table. Update new UI settings of OSPF, VRRP and DVMRP.
V1.3	Jun. 13, 2011	Add JetNet 5628G-R/5828G-R, 5828G models and related hardware/software specification and information. Update DHCP Server setting, Extended LACP setting, IGMP Unknown Multicast settings. Add JetNet 5828G Routing (ARP, IP, Router, RIP, OSPF, Multicast Route, VRRP) Features description and commands. Add JetNet 5628G/5828G Multiple Spanning Tree Protocol, Private VLAN, QinQ, new MSR description and commands.
V1.2	May. 18, 2010	Add model JetNet 5628G/5828G for China project
V1.1	May. 14, 2010	Add 5628G V1.1 New Features
V1.0	Dec. 25, 2009	Change V0.8 to V1.0.

5.5 About Korenix

Less Time At Work! Fewer Budget on applications!

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

Fusion of Outstandings

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

Core Strength---Competitive Price and Quality

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

Global Sales Strategy

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

Quality Services

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

5 Years Warranty

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

Korenix Technologies Co., Ltd.

Business service : sales@korenix.com

Customer service: koreCARE@korenix.com