Korenix
JetNet 7612GP-4F/7612G-4F/ 5612GP-4F/5612G-4F Series
Industrial Full Gigabit Managed Ethernet Switch

User Manual

Version1.2

Apr.,2020

www.korenix.com

Korenix
JetNet 7612GP-4F/7612G-4F/ 5612GP-4F/5612G-4F Series
Industrial Full Gigabit Managed Ethernet Switch
User's Manual

Copyright Notice

Copyright 2006-2017 Korenix Technology Co., Ltd.

All rights reserved.

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

Federal Communications Commission (FCC) Statement

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

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

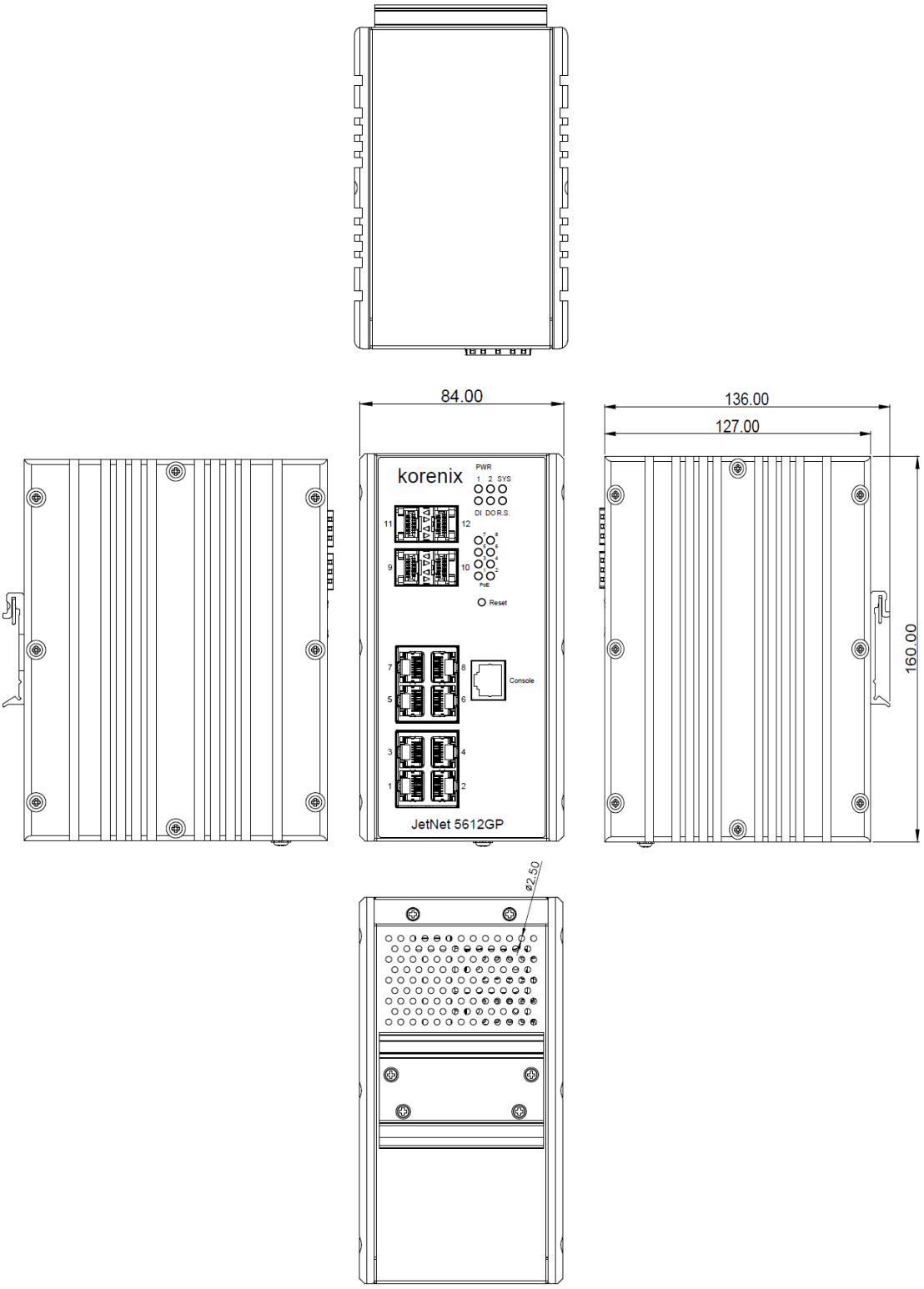
Index

1 Hardware Installation 1
1.1 Hardware Introduction 1
1.2 Wiring Power Inputs 3
1.3 Wiring the Relay Output (DO) 4
2 Preparation for Management 5
2.1 Preparation for Serial Console 5
2.2 Preparation for Web Interface 6
2.3 Preparation for Telnet Console 8
3 Feature Configuration 9
3.1 Command Line Interface Introduction 11
Primary TACACS+ Server 16
3.2 Basic Setting 19
Time Setting 22
IEEE 1588 PTPv2 24
Mode: 25
Synchronization Interval: 25
Announce Interval: 25
Announce Receipt Timeout: 25
Minimum Path Delay Request Message Interval: 25
Domain Number: 25
First Priority: 25
Second Priority: 25
DHCP Server configuration 27
Leased Entries 29
Option82 Information 29
Relay Policy 30
Circuit ID 30
Remote ID 31
Local Files 32
TFTP 32
SFTP 32
Local File 33
TFTP 33
SFTP 34
3.3 Port Configuration 41
3.4 Power over Ethernet (JetNet PoE Switch only) 52
3.5 Network Redundancy 57

3.7 Traffic Prioritization 89
3.8 Multicast Filtering 94
3.9 Routing (Layer3 Managed Switch only) 100
3.10 SNMP 122
3.11 Security 126
3.12 Warning 145
3.13 Monitor and Diag 152
3.14 Device Front Panel 160
3.15 Save 161
3.16 Logout 161
3.17 Reboot 162
4.1 Korenix Private MIB 162
4.2 About Korenix 162

1 Hardware Installation

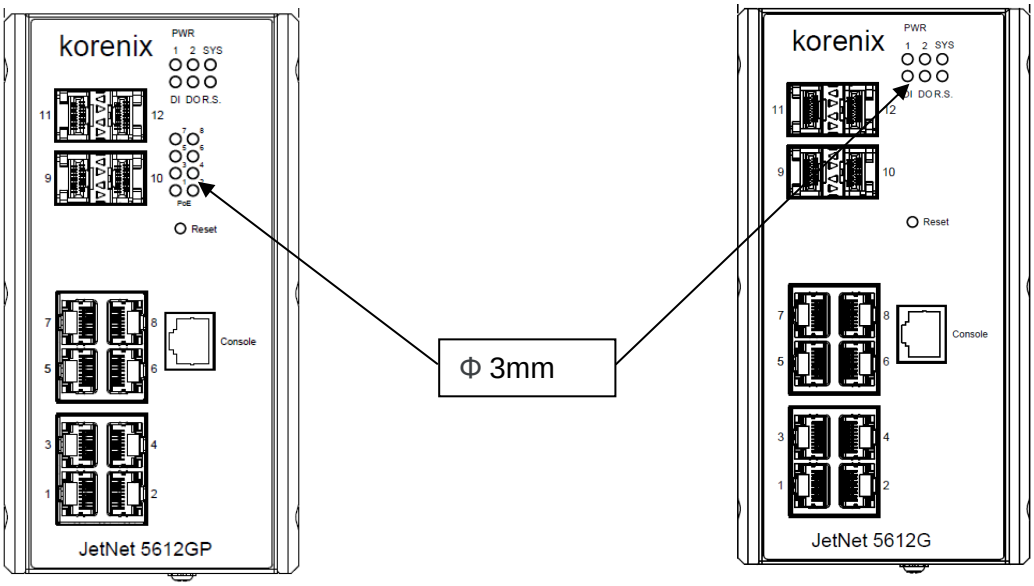
1.1 Hardware Introduction



Note:
Take JetNet5612GP-4F as an example, all the models are in same hardware construction.

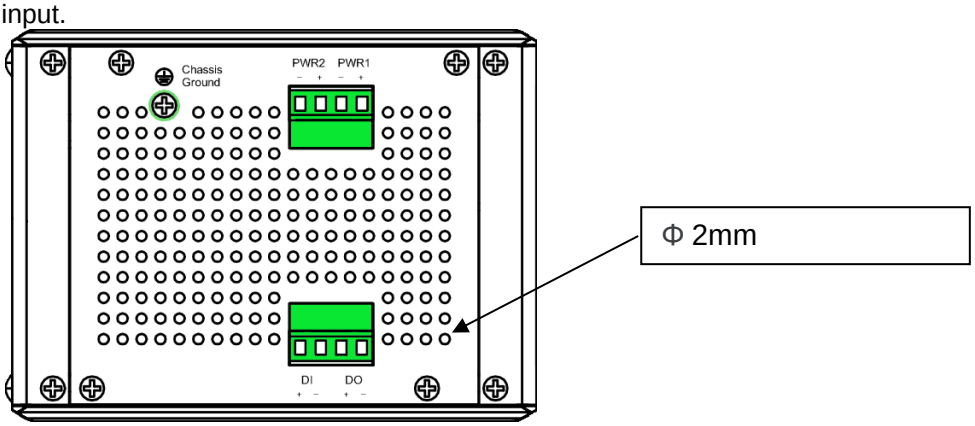
Panel Layout

The front panel includes 8 x 10/100Mbps RJ-45 PoE ports, 4 x Gigabit Ethernet SFP socket ports, 1 RJ-45 for RS232 console, System diagnostic LEDs, Port LEDs, PoE status LEDs.



Bottom view

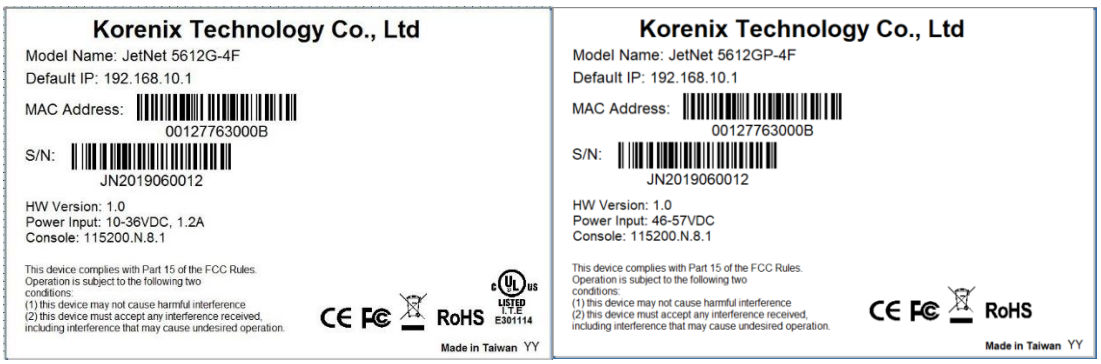
The bottom side includes 2 4-pin terminal block connectors and 1 chassis grounding screw. One of 4-pin terminal block connectors is for power inputs, and the rest is for alarm relay output and digital input.



Rear Side

The rear side back panel attached DIN rail clip and one lighting screw to make connection with chassis ground and Switch inner lighting protection circuit.

The product label also is pasted on the bottom side of DIN rail clip, in case if it is missed, please contact with your sales for product change.



1.2 Wiring Power Inputs

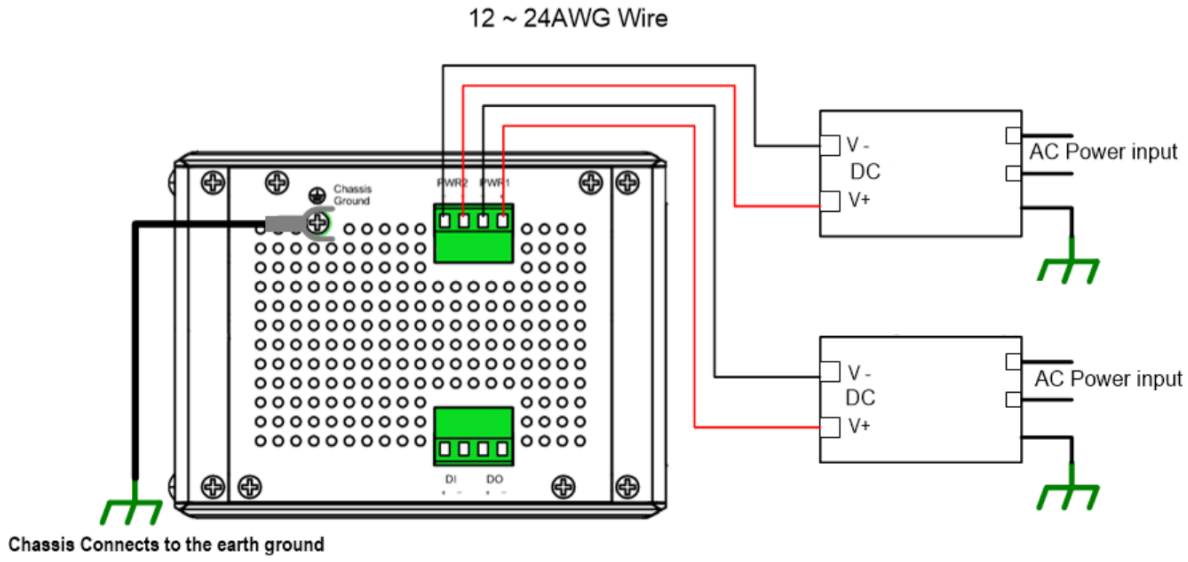
The Power input port is located at the bottom side and provides 2 power input connections in one 4-pin removable terminal block. The power port support polarity reverse protection; the Switch won't start if wrong polarity applied. The wiring architecture please refers to below figure.

Wiring the Power Inputs & Grounding

1. Insert the positive and negative wires into the V+ and V- contact on the terminal block connector.
2. Tighten the wire-clamp screws to prevent the power wires from being loosened.
3. Connect the power wires to suitable AC/DC Switching type power supply. The JetNet 5612G provides Power over Ethernet function and is compliant with IEEE802.3af/ IEEE802.3at standards.

For the safety issue, turn off AC power input source before connecting the AC/DC Power supply module and the terminal block connectors. Besides, don't turn-on the source of AC/DC power module and make sure all connections were well done then power on the AC source to powering the Switch device. Otherwise, your screwdriver blade may inadvertently short your terminal connections to the grounded enclosure and cause damage.

Note:
For PROTECTIVE EARTHING CONDUCTOR information, connect the grounding connector located on enclosure, used green-and-yellow wire minimum 20AWG, screw 3.5 mm.

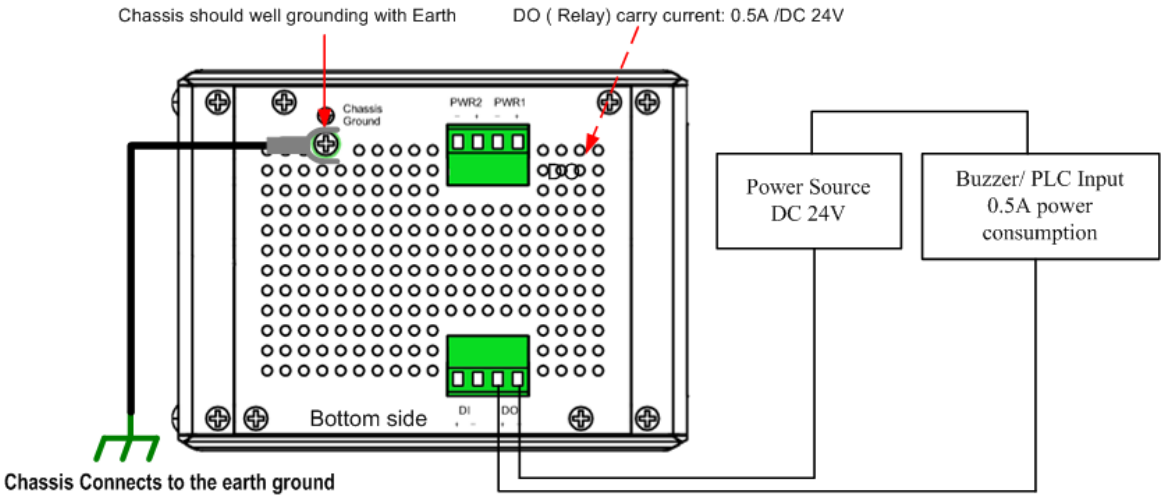


Note: Power adapter input range are listed as below.

Models	Typical Power Input	DC Power Input Range
JetNet5612G-4F/JetNet7612G-4F	24V DC	10-36V DC
JetNet5612GP-4F/JetNet7612GP-4F	48V DC	46-57V DC

1.3 Wiring the Relay Output (DO)

The relay output contacts are in the bottom side as shown on below figure. The relay output (DO) is controlled by the pre-defined operating rules. To activate relay output function, please refer to the CD User's Manual for more Relay Output management information.



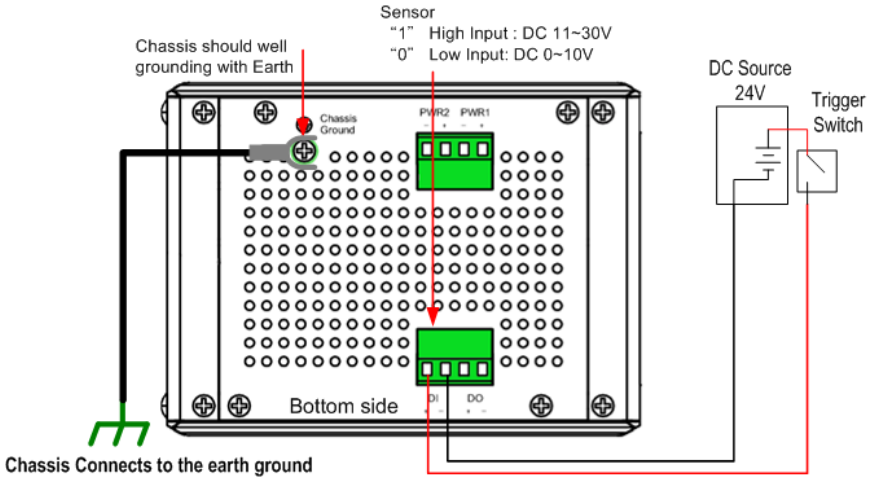
Digital Output Wiring simulate Diagram

Note:

The relay contact only supports 0.5 A current, DC 24V. It is not recommended to apply voltage and current higher than the specifications.

1.4 Wiring the Digital Input (DI)

The Digital Input (D.I.) contacts are in the bottom side of the device as shown in below figure. It accepts one external DC type signal input and can be configured to send alert message through Ethernet when the signal is changed. The signal may trigger and generated by external power switch, like as door open trigger switch for control cabinet.



Digital Inputt Wiring simulate Diagram

Note:

The DI accepts DC type signal and supports isolated input circuit with Digital High-Level input DC 11V~30V and Digital Low Level input DC 0V~10V. Do not apply voltage that higher than the specification; it may cause internal circuit damage or a wrong action of DI.

2 Preparation for Management

JetNet Industrial Managed Switch provides both in-band and out-band configuration methods. You can configure the switch via RS232 console cable if you don't attach your admin PC to your network, or if you lose network connection to your JetNet Managed Switch. This is so-called out-band management. It wouldn't be affected by network performance.
The in-band management means you can remotely manage the switch via the network. You can choose Telnet or Web-based management. You just need to know the device's IP address and you can remotely connect to its embedded HTTP web pages or Telnet console.

2.1 Preparation for Serial Console

In the unit package, Korenix attached one RJ-45 to RS-232 DB-9 console cable. Please attach RS-232 DB-9 connector to your PC's COM port, connect RJ-45 connector to the Console port of the JetNet Managed Switch. If the serial cable is lost, please follow the serial console cable PIN assignment to find one.

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

```
Boot Loader Rev 1.0.0.1 for JetNet7612GP-4F Starting....


Switch login: admin
Password:

JetNet7612GP-4F
Copyright 2006-2017 Korenix Technology Co., Ltd.

Switch>
```

2.2 Preparation for Web Interface

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

2.2.1 Web Interface

Korenix web management page is developed by CGI (Common Gateway Interface). It allows you to use a standard web-browser such as Microsoft Internet Explorer, Mozilla, and Google Chrome 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 Managed 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.

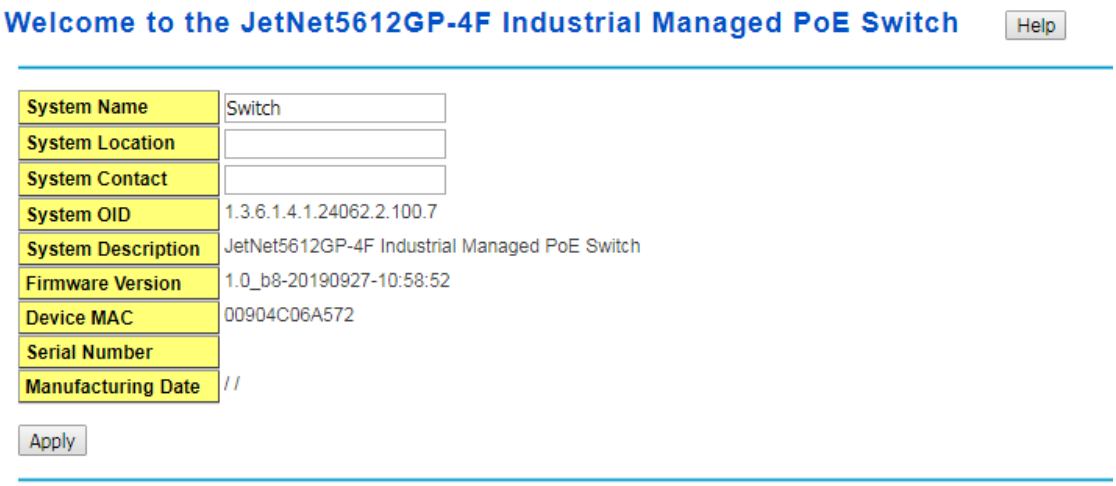
----------Launch the web browser and Login. ----------

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**.



<Login screen example>

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



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

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

2.2.2 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 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 first. Press **Yes** to trust it.
4. The login screen will appear.
5. Key in the user name and the password. The default user name and password are **admin**.
6. Click on **Enter** or **Login.** 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.



2.3 Preparation for Telnet Console

2.3.1 Telnet/ SSH (Secure Shell)

You can connect to the device 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

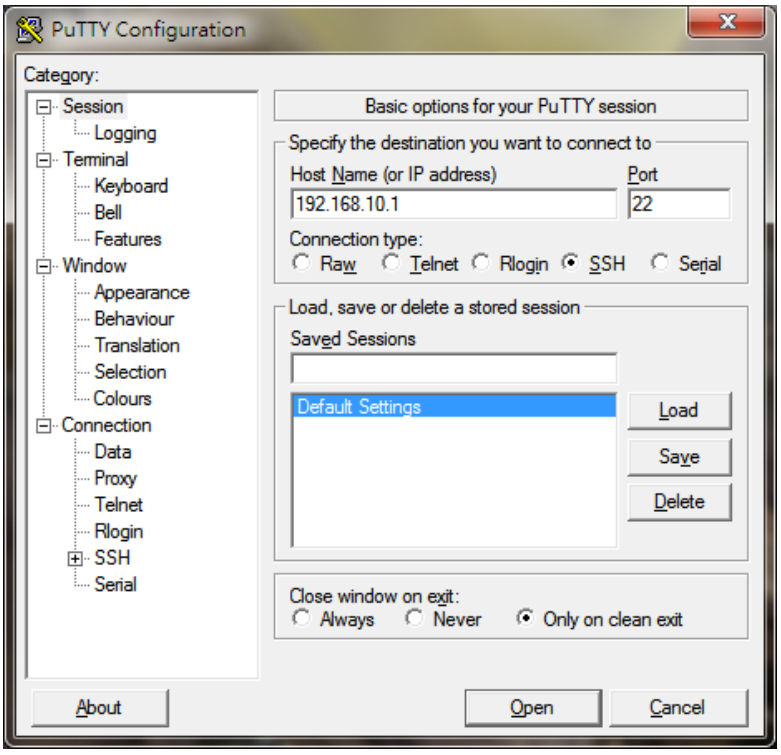
Note: the Telnet.exe file is not provided after Window 7. You can download it from Microsoft web site. Or you can use 3rd Party tool, for example the Putty.

3rd Party tool:
Download PuTTY: http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

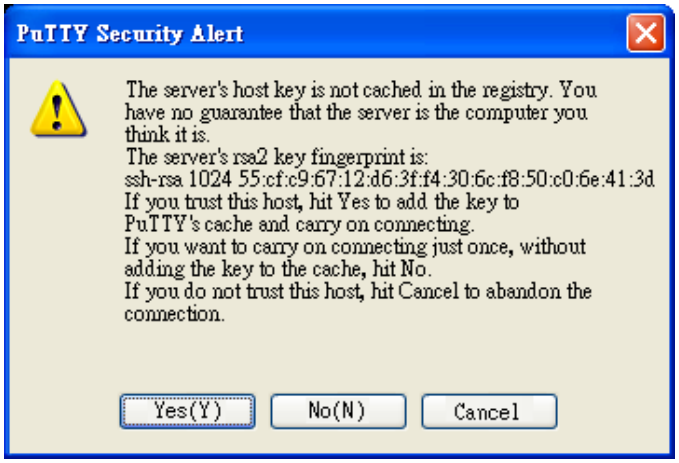


The copyright of PuTTY is belonged to Putty. We don't have any contract with them. Please follow the shareware policy of their company.

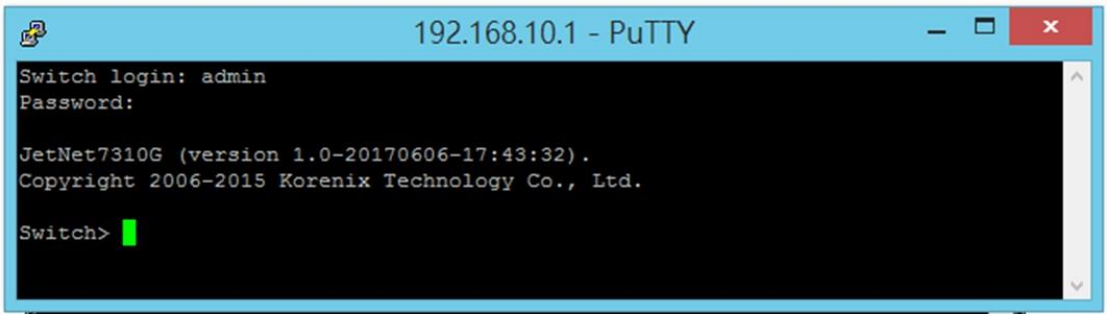
1. Open SSH Client/PuTTY. In the **Session** configuration, enter the **Host Name** (IP Address of your JetNet Managed Switch) and **Port number** (default = 22). Choose the "**SSH**" protocol. Then click on "**Open**" to start the SSH session console. Choose the "Telnet" protocol.



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



2. After few seconds, the SSH connection to JetNet Managed Switchis opened.
3. Type the Login Name and its Password. The default Login Name and Password are **admin** / **admin**. You can see the screen as the below figure.



4. 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.

3 Feature Configuration

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

JetNet 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 switch. This is so-called out-band management. It wouldn't be affected by the network performance.

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

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

Following topics are covered in this chapter:

3.1 Command Line Interface (CLI) Introduction

3.2 Basic Setting

3.3 Port Configuration

3.4 Power over Ethernet

3.5 Network Redundancy

3.6 VLAN

3.7 Traffic Prioritization

3.8 Multicast Filtering

3.9 Routing

3.10 SNMP

3.11 Security

3.12 Warning

3.13 Monitor and Diagnostic

3.14 Device Front Panel

3.15 Save

3.16 Logout

3.17 Reboot

3.1 Command Line Interface Introduction

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

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

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

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

```
Switch#
enableTurn on privileged mode command
exit            Exit current mode and down to previous mode
listPrint 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')
            dir           Display a list of files
            disable       Turn off privileged mode command
            dot1x         IEEE 802.1x standard access security control
            end           End current mode and change to enable mode
            exit          Exit current mode and down to previous mode
            list          Print command list
            mac           MAC interface commands
            no            Negate a command or set its defaults
            pager         Terminal pager
            ping          Send echo messages
            quit          Exit current mode and down to previous mode
            reboot        Reboot system
            reload        copy a default-config file to replace the current one
            show          Show running system information
            telnet        Open a telnet connection
            terminal      Set terminal line parameters
            traceroute    Trace route to destination
```

write	Write running configuration to memory, network, or terminal

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

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

Available command lists of global configuration mode.

```
Switch# configure terminal
Switch(config)#
        access-list             Add an access list entry
        administrator           Administrator account setting
        auth                    Authentication
        clock                   Configure time-of-day clock
        default                 Set a command to its defaults
        dot1x                   IEEE 802.1x standard access security control
        end                     End current mode and change to enable mode
        erps                    Ethernet Ring Protection Switching (ITU-T G.8032)
        ethernet-ip             Ethernet/IP Protocol
        exit                    Exit current mode and down to previous mode
        gmrp                    GMRP protocol
        gvrp                    GARP VLAN Registration Protocol
        hostname                Set system's network name
        interface               Select an interface to configure
        ip                      Global IP configuration subcommands
        ipv6                    IP information
        lacp                    Link Aggregation Control Protocollist
        list                    Print command list
        lldp                    Link Layer Discovery Protocol
        log                     Logging control
        loop-protect            Ethernet loop protection
        mac                     Global MAC configuration subcommands
        mac-address-table       mac address table
        mirror                  Port mirroring
        modbus                  Modbus TCP Slave
        multiple-super-ring     Configure Multiple Super Ring
        nameserver              DNS Server
        no                      Negate a command or set its defaults
        ntp                     Configure NTP
        poe                     Configure power over ethernet
        ptp                     IEEE1588 PTPv2
        qos                     Quality of Service (QoS)
        relay                   relay output type information
        router                  Enable a routing process
        service                 System service
        sfp                     Small form-factor pluggable
        smtp-server             SMTP server configuration
        snmp-server             the SNMP server
        spanning-tree           the spanning tree algorithm
        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 thenenter interface configuration mode. In this mode, you can configure port settings.

The port interface name for gigabit Ethernet port 1 is gi1..gigabit Ethernet port 10 is gi10. Type interface name accordingly when you want to enter certain interface configuration mode.

Type **exit** to leave.

Type" **?"** to see the command list

Available command lists of the global configuration mode.

```
Switch(config)# interface gi
Switch(config-if)#
        acceptable          Configures the 802.1Q acceptable frame types of a port.
          auto-negotiation  Enables auto-negotiation state of a given port
          description       Interface specific description
          dot1x             IEEE 802.1x standard access security control
          duplex            Specifies the duplex mode of operation for a port
          end               End current mode and change to enable mode
          ethertype         Ethertype
          exit              Exit current mode and down to previous mode
          flowcontrol       Sets the flow-control value for an interface
          garp              General Attribute Registration Protocol
          ingress           802.1Q ingress filtering features
          ip                Interface Internet Protocol config commands
          lacp              Link Aggregation Control Protocol
          list              Print command list
          loopback          Specifies the loopback mode of operation for a port
          mac               MAC interface commands
          media-type        Specify media type
        mtu                 Specifies the MTU on a port.
          no                Negate a command or set its defaults
          qos               Quality of Service (QoS)
          quit              Exit current mode and down to previous mode
          rate-limit        Rate limit configuration
          sfp               Small form-factor pluggable
          shutdown          Shutdown the selected interface
          spanning-tree     the spanning-tree protocol
          speed             Specifies the speed of a Fast Ethernet port or a Gigabit
                             Ethernet port.
          storm-control     Enables packets flooding rate limiting features
          switchport        Set switching mode characteristics
```

(VLAN) Interface Configuration: Press **interface VLANVLAN-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 vlan1
Switch(config-if)#
  description Interface specific description
  end          End current mode and change to enable mode
  exit         Exit current mode and down to previous mode
  ip           Interface Internet Protocol config commands
  ipv6         Interface Internet Protocol config commands
  list         Print command list
  no           Negate a command or set its defaults
  quit         Exit current mode and down to previous mode
  shutdown     Shutdown the selected interface
```

Summary of the 5 command modes:

Command Mode	Main Function	Enter and Exit Method	Prompt
User EXEC	This is the first level of access. User can ping, telnet remote device, and show some basic information	Enter: **Login** successfully Exit: **exit** to logout. Next mode: Type **enable** to enter privileged EXEC mode.	Switch>
Privileged EXEC	In this mode, the system allows you to view current configuration, reset default, reload switch, show system information, save configuration…and enter global configuration mode.	Enter: Type **enable** in User EXEC mode. Exec: Type **disable** to exit to user EXEC mode. Type **exit** to logout Next Mode: Type**configure terminal**to enter global configurationcommand.	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
auth              Authentication
```

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

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

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

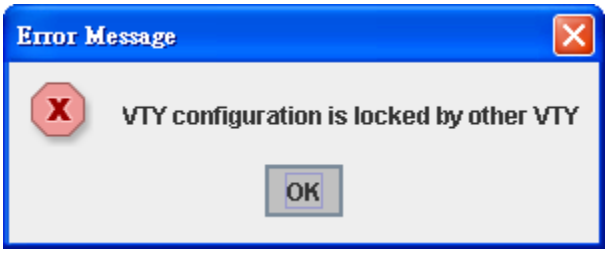
Ctrl+C To stop executing the unfinished command.

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

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

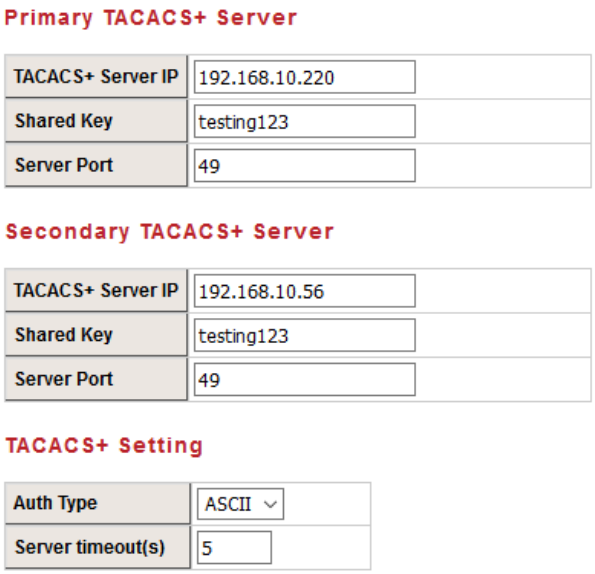
Ctrl+Z To exit configuration mode.

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



Primary TACACS+ Server

The TACACS+ mechanisms are centralized “AAA” (Authentication, Authorization and Accounting) systems for connecting to network services. The fundamental purpose of TACACS+ is to provide an efficient and secure mechanism for user account management.



Primary TACACS+ Server

TACACS+ Server IP: The IP address of the primary TACACS+ server.
Shared Key: The key used for communicating with the primary TACACS+ Server.
Server Port: The UDP port of the primary TACACS+ server.

Secondary TACACS+ Server

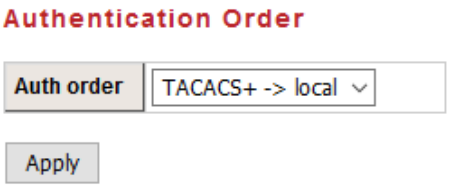
TACACS+ Server IP: The IP address of the backup TACACS+ server.
Shared Key: The key used for communicating with the backup TACACS+ Server.
Server Port: The UDP port of the backup TACACS+ server.

TACACS+ Setting

Auth Type: choose one of three kinds of authentication type: ASCII / PAP / CHAP
Server timeout: TACACS+ server timeout in seconds.

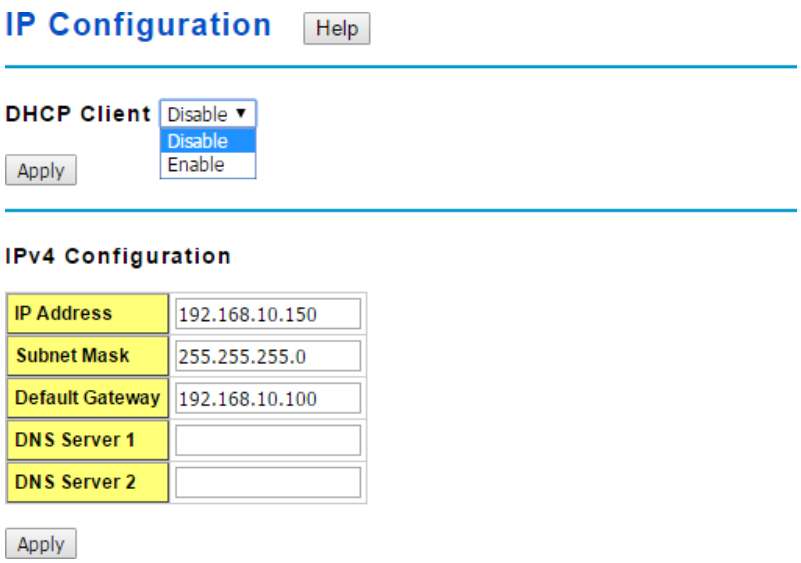
Click “Apply” to apply the TACACS+ Server configurations.

After TACACS+ has been configured, the Authentication Order will be changed to ‘TACACS+ → local’



3.1.1. IP Configuration

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



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 switch. If DHCP Client function is enabled, you don't need to assign an IP address to the JetNet switch, 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.)

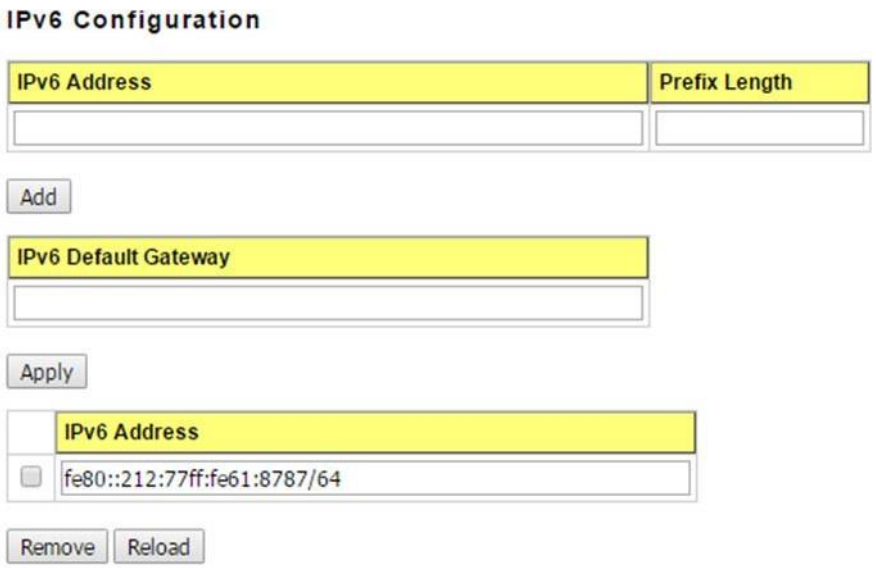
DNS Server 1/ DNS Server 2: You can assign the DNS for the switch here.

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

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

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

The Leading zeroes in a group may be omitted. Thus, for example,a IPv6 link-local address may be written as: fe80::212:77ff:fe60:ca90.



IPv6 Address: typing new IPv6 address in this field.

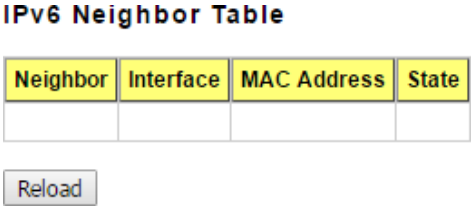
Prefix Length: The size of subnet or network, and it equivalent to the subnetmask, but writtenin different.The default subnet mask length is 64bits, and written in decimal value - 64.

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

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

Reload: Refresh and reload IPv6 address listing.

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



IPv6Neighbor Table: shows the IPv6 address of neighbor, connected interface, MAC address of remote IPv6 device, and current state of neighbor device.

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

3.1.2. 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. Below figure is similar as JetNet Switch.

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

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

3.2 Basic Setting

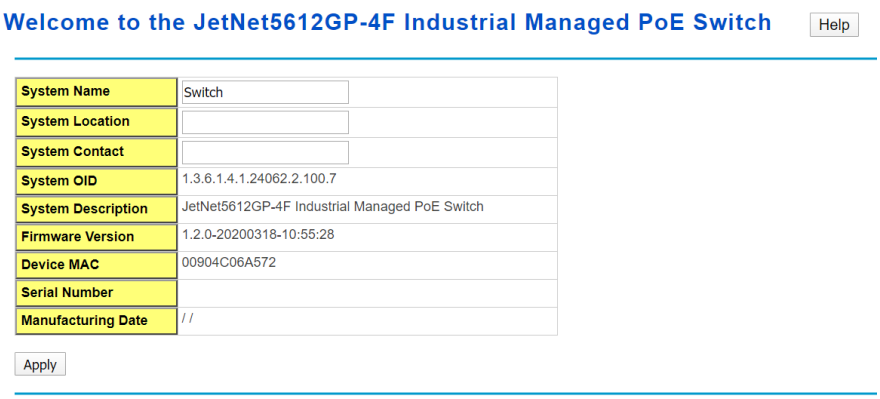
The Basic Setting group provides you to configure switch information, IP address, User name/Password of the system. It also allows you to do firmware upgrade, backup and restore configuration, reload factory default, and reboot the system.

Following commands are included in this group:

3.2.1. Switch Setting
3.2.2. Admin Password
3.2.3. IP Configuration
3.2.4. Time Setting
3.2.5. Jumbo Frame
3.2.6. DHCP Server
3.2.7. Backup and Restore
3.2.8. Firmware Upgrade
3.2.9. LoadDefault
3.2.10. CLI Commands for Basic Setting

3.2.1. Switch Setting

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



< Web UI Example 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: The name of this managed product.

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

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

Serial Number: The serial number of this managed product.

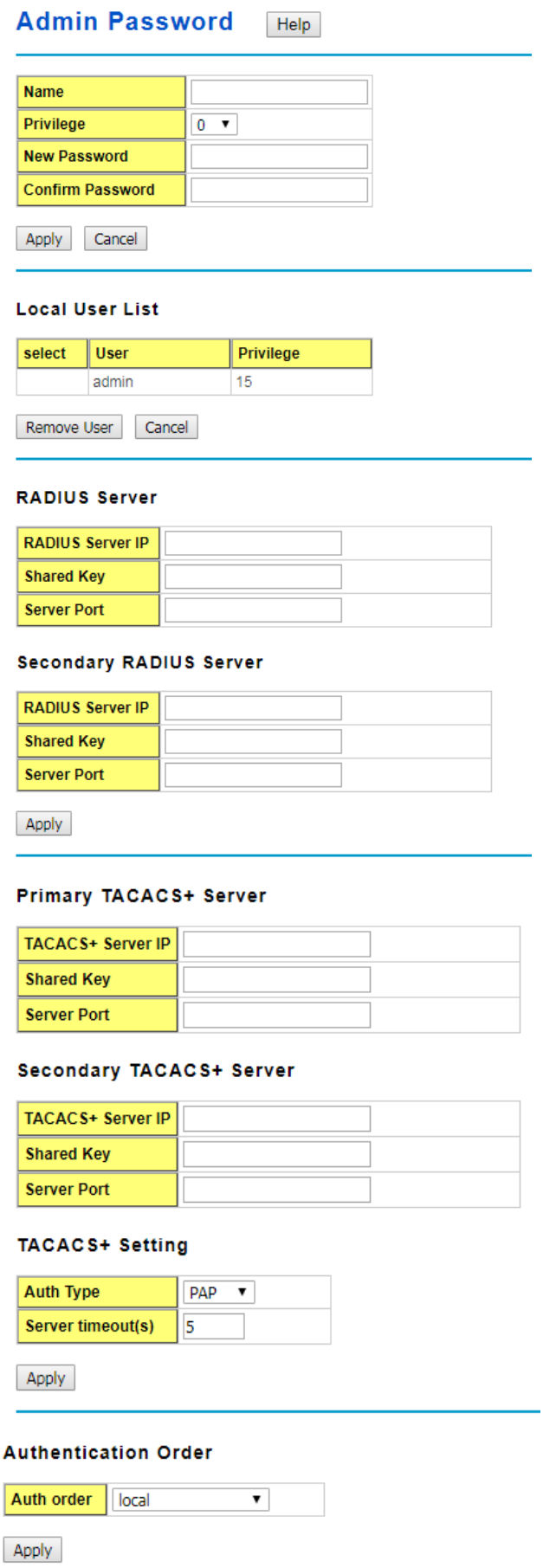
Manufacturing Date: The manufacturing date of this managed product.

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.

3.2.2. Admin Password

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



<Web UI of the Admin Password>

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

Privilege: You can choose 0 or 15 for user access. 0 for read only. 15 for read and write.

New Password: You can key in new password here. The default setting is **admin**.
Confirm Password: You need to type the new password again to confirm it.

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

Local User List

It will display the list of user name and permission. You can select and remove the user by click "Remove user".

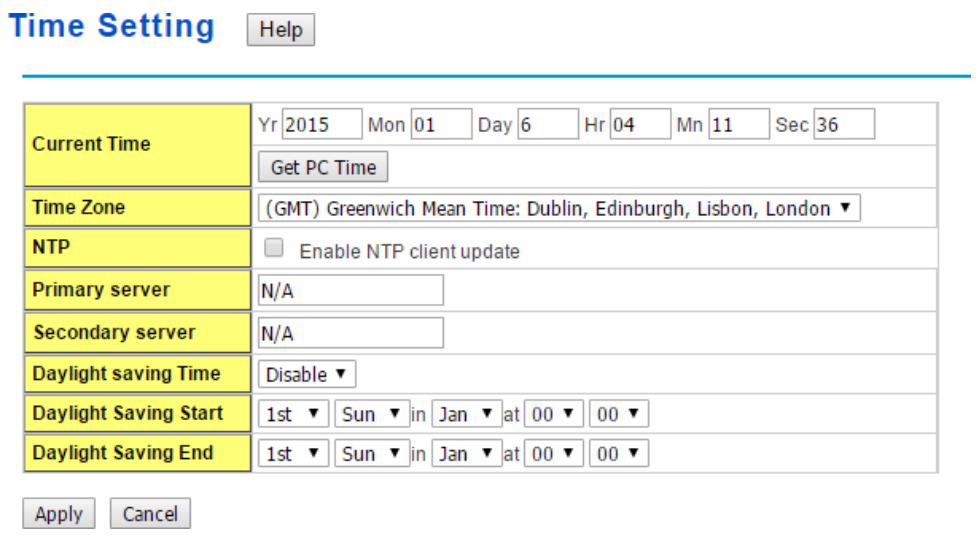
RADIUS Server/ Secondary RADIUS Server

RADIUS Server: The IP address of Radius server

Shared Key: It is the password for communicate between switch and Radius Server.

Server Port: UDP port of Radius server.

Time Setting



User canchange time as user wants. User alsocan click the button "**Get PC Time**" to get PC's time setting for switch. After click the "**Get PC Time**" and apply the setting, the System time display the same time as your PC's time.

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

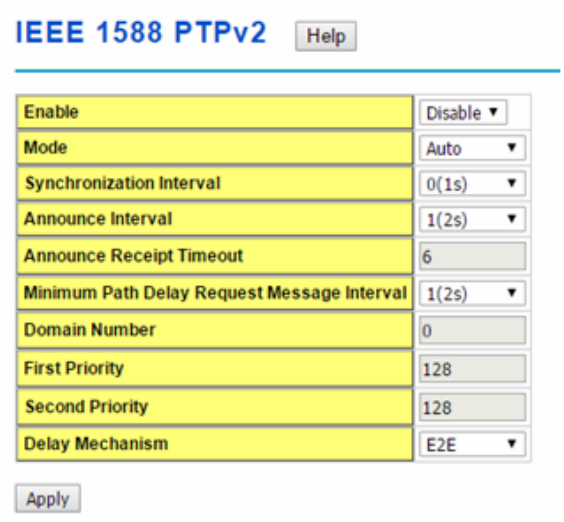
54	(GMT+07:00) Bangkok, Hanoi, Jakarta
55	(GMT+07:00) Krasnoyarsk
56	(GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi
57	(GMT+08:00) Irkutsk, Ulaan Bataar
58	(GMT+08:00) Kuala Lumpur, Singapore
59	(GMT+08:00) Perth
60	(GMT+08:00) Taipei
61	(GMT+09:00) Osaka, Sapporo, Tokyo
62	(GMT+09:00) Seoul
63	(GMT+09:00) 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

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.

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

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

IEEE 1588 PTPv2



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.

Mode:

Auto mode: the switch performs PTP Master and slave mode.
Master mode: switch performs PTP Master only.
Slave mode: switch performs PTP slave only.

Synchronization Interval:

Select items: -3(128ms) -2(256ms) -1(512ms) 0(1s) 1(2s) 2(4s) 3(8s) 4(16s)

Announce Interval:

Select items:0(1s) 1(2s) 2(4s) 3(8s) 4(16s)

Announce Receipt Timeout:

Select items:<2-10>

Minimum Path Delay Request Message Interval:

Select items: -1(512ms) 0(1s) 1(2s) 2(4s) 3(8s) 4(16s)

Domain Number:

Select items:<0-3>

First Priority:

First priority Select items:<0-255>

Second Priority:

Second priority Select items:<0-255>

Delay Mechanism:

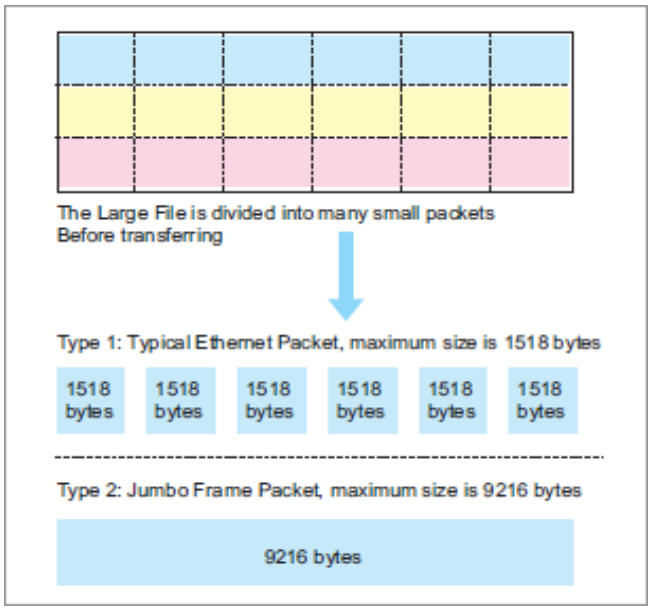
E2E: End-to-End

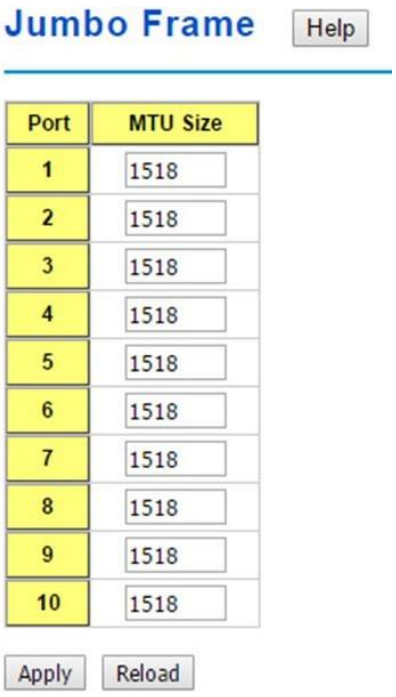
PTP: Peer-to-Peer

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

3.2.3. Jumbo Frame

The switchallows 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.

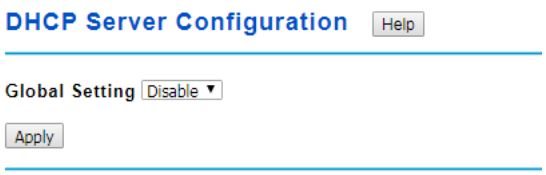
3.2.4. DHCP Server

You can select to **Enable** or **Disable** DHCP Server function. The Managed Switch will assign a new IP address to link partners.

DHCP Server configuration

After selecting to enable DHCP Server function, type in the Network IP address for the DHCP server IP pool, Subnet Mask, Default Gateway address and Lease Time for client.

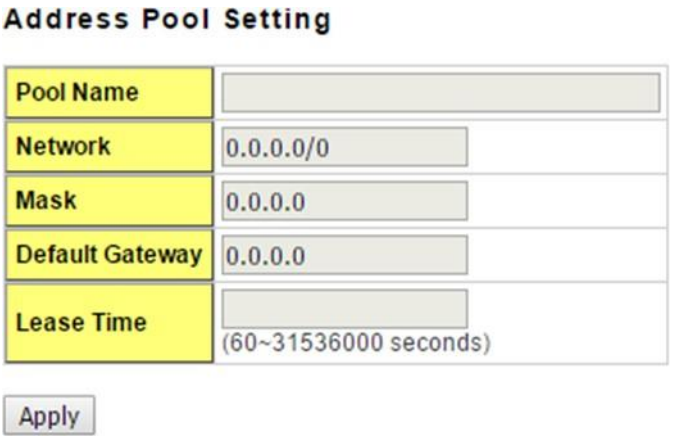
Once you have finished the configuration, click **Apply** to activate the new configuration



Global Setting: You can enable or disable the local DHCP server

Address Pool Add: Add a address pool setting into local DHCP server**.**

Address Pool List: You can select a address pool setting here. Click the **Select** button to change address pool. Click the **Delete** button to delete the address pool.



Pool Name: The address pool name.

Network: The network that you want the DHCP server to distribute.

Mask: The subnet mask of the network.

Default Gateway: The default gateway IP address that you want the DHCP server to distribute.

Lease Time: The time in seconds a DHCP lease is valid for.



This section allows you to exclude IP addresses within the network range from being assigned to devices.

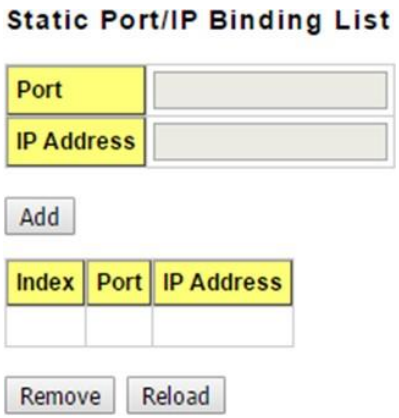
Excluded IP: An IP address you want to exclude from being leased. The

Excluded Address List table contains the following fields:

Index: The indexes of the excluded IP addresses.

IP Address: The excluded IP addresses.

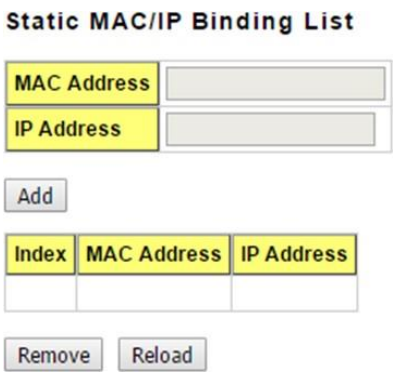
Click the Remove button to remove the selected IP address(es) or click the Reloadbutton to reload the selected IP address(es).



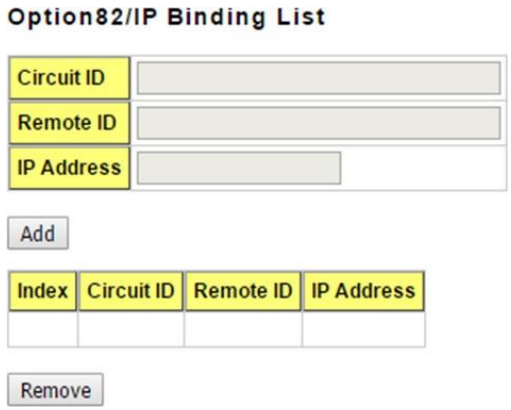
This feature allows you to bind an IP address to a specific port. A device connected to this port will be assigned the chosen IP address. Click the **Add** button to add a static port binding.

Port: The port you want to assign the IP address to.

IP Address: The IP address you want to assign to a device connected to the chosen port.



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



This"Option82/IP Binding List"allows you to bind a DHCP Option 82 Circuit ID and Remote ID to an IP address. Click the **Add** button to add an Option82 IP Address Configuration entry.

Circuit ID: The Circuit ID you want to bind to the IP address.

Remote ID: The Remote ID you want to bind to the IP address.

IP Address: The IP address you want to bind the Circuit ID and Remote ID to.

Leased Entries

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



Index: Index of the DHCP lease entry.

IP Address: The IP address assigned to the device that received the lease.

MAC Address: The MAC Address of the device that received the lease.

Leased Time Remains: How long in seconds until the lease expires.

Option82 Information

This page allows you to configure DHCP Option 82 settings.



You can **Enable** or **Disable** the DHCP Relay Agent function. Click the **Apply** button to apply the DHCP Relay Agent settings.

Helper Address: Type the IP address of the target DHCP Server. There are 4 available IP addresses that can be configured. Click **Add** to add the IP address and **Remove** to delete it.



Relay Policy

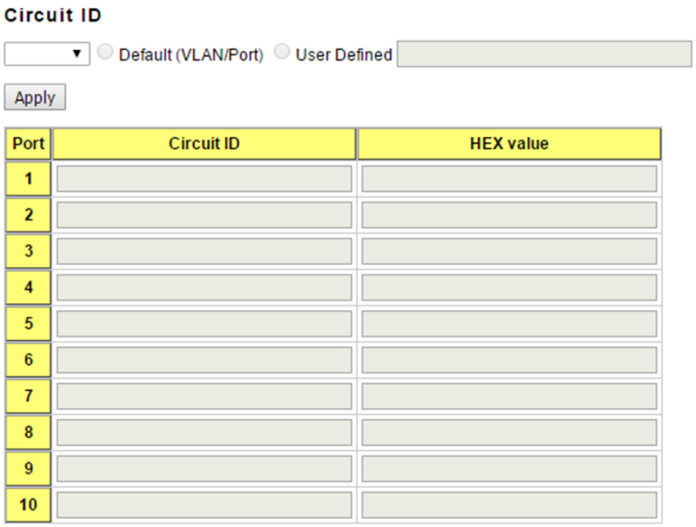
Replace: Replaces the existing option 82 field and adds new option 82 field. (This is the default setting)

Keep: Keeps the original option 82 field and forwards to server.

Drop: Drops the option 82 field and do not add any option 82 field.



Circuit ID



Click the **Apply** button to apply the Circuit ID setting for a port after selecting a port and the associated setting.

Port: This is the logical port of the switch.

Default (VLAN/Port): This is the default value of the Circuit ID.

User Defined: This is a user defined value of the Circuit ID.

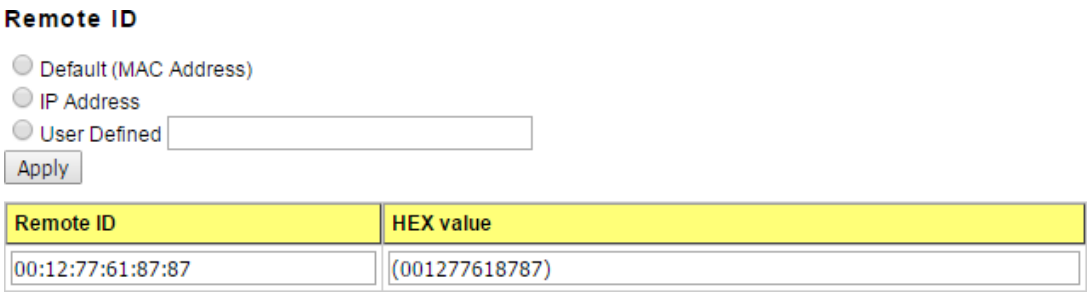
The Circuit ID table contains the following information:

Port: This is the logical port of the switch.

Circuit ID: The Circuit ID includes information specific to which circuit the request came in on. It is an identifier that is specific to the relay agent, so the type of circuit varies depending on the relay agent.

HEX value: This is the HEX value of the Circuit ID.

Remote ID



Default (MAC Address): Use the default value (MAC Address) as the Remote ID.

IP Address: Use the IP Address of the switch as the Remote ID.

User Defined: This is the user defined value of the Remote ID.

Click **Apply** to apply the Remote ID setting.

The Remote ID table provides this information.

Remote ID: The Remote-ID carries information relating to the remote host end of the circuit, which is the MAC address of the relay.

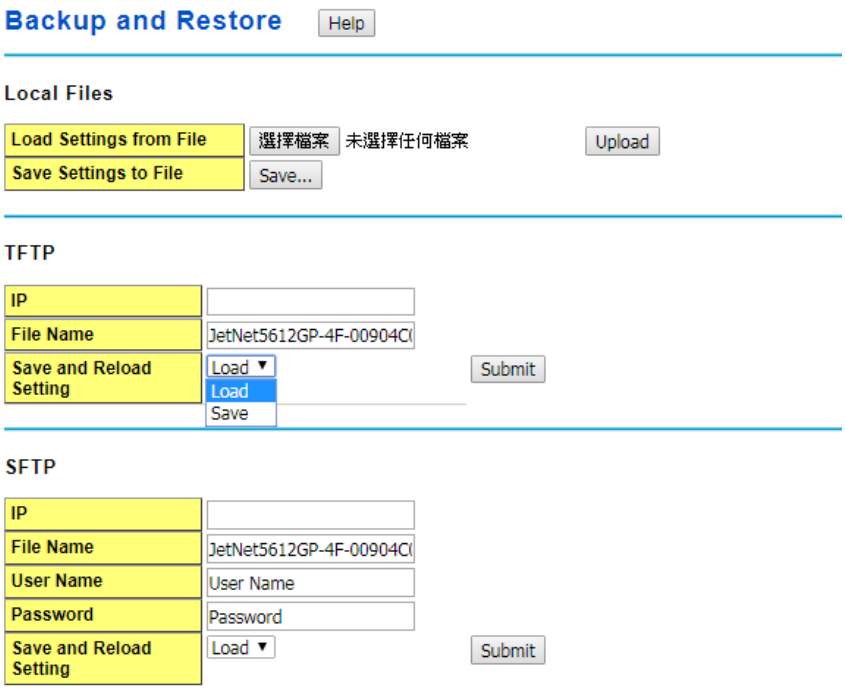
HEX value: HEX value of the Remote ID.

3.2.5. Backup and Restore

You can use the Backup option to save the current configuration saved in the device's flash to a PC or laptop or your TFTP server.

This allows you to use the Restore option to restore a configuration file back to thedevice or load the same settings to another device. Before you can restore a configuration file, you must place the backup configuration file in the PC or TFTP server. The device then can download this file back into the flash.

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



Local Files

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.

Load Settings from File: Click the **Browse** button to select the previously saved backup configuration file. After locating the configuration file, click the **Upload** button.

Save Settings to File: Click the **Save** button to save the configuration file.

TFTP

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.

IP: This is the IP address of the TFTP server where your configuration file has been previously saved or can be saved.

File Name: This is the file name of configuration file to be saved.

Load/Save Settings: Select **Load** to load the configuration from the TFTP server onto the switch. Select **Save** to save the configuration on the switch to the TFTP server.

Click **Submit** to load or save the configuration.

SFTP

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

IP: This is the IP address of the SFTP server where your configuration file has been previously saved or can be saved.

File Name: This is the file name of configuration file to be saved.

User Name: Insert the User name for SFTP

Password: Insert the password of SFTP

Load/Save Settings: Select **Load** to load the configuration from the TFTP server onto the switch. Select **Save** to save the configuration on the switch to the TFTP server.

Click **Submit** to load or save the configuration.

3.2.6. Firmware Upgrade

You can update the latest firmware for your device. Korenix provides the latest firmware on Korenix Web site. Updated firmware may include new features, bug fixes, or other software changes, please check the release notes for the information. We suggest you use the latest firmware before installing the switch to the customer site.



Local File

This section allows you to upload a firmware image that is stored locally on your computer.

Select File: Select a firmware image from your computer.

Click **Upgrade** to begin upgrading the firmware.

Click **Cancel** to clear the selected file.

After the firmware has upgraded the switch will reboot automatically.Please remind the attached network users before you perform this function.

TFTP

This section allows you to upload a firmware image that is stored on a TFTP server.

IP: This is the IP address of the TFTP server where your firmware image is stored.

File Name: This is the file name of the firmware image.

Click **Upgrade** to begin upgrading the firmware.

Click **Cancel** to clear the selected file.

After the firmware has upgraded the switch will reboot automatically. Please remind the attached network users before you perform this function.

SFTP

This section allows you to upload a firmware image that is stored on a SFTP server.

IP: This is the IP address of the SFTP server where your firmware image is stored.

Port: Insert the TCP Port number.

File Name: This is the file name of the firmware image.

Name: Insert the User name for SFTP

Password: Insert the password of SFTP

Click **Upgrade** to begin upgrading the firmware.

Click **Cancel** to clear the selected file.

After the firmware has upgraded the switch will reboot automatically. Please remind the attached network users before you perform this function.

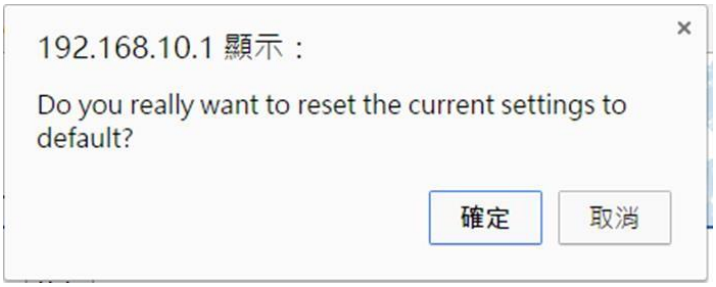
3.2.7. Load Default

In this section, you can reset all the configurations of the switch to default setting.

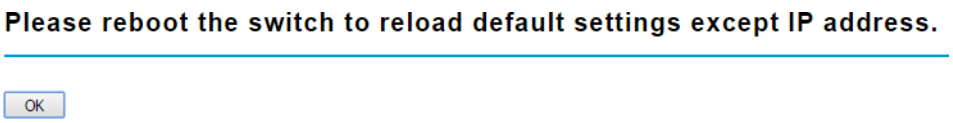
Click on **Reset** the system will then reset all configurations to default setting.work after rebooting the switch.



The system will show you a popup message to check if you really want to reset the current setting to default. Click on **Yes** to start it.



Default setting will work after rebooting the switch. The system will show the message to remind you to reboot it. Go to **Reboot** page to reboot the switch to reload default settings.



Note: The IP address will not be reset to default IP. The system will remain the IP address so that you can still connect the switch via the network.

3.2.8. CLI Commands for Basic Setting

Feature	Command Line
Switch Setting	
System Name	Switch(config)# hostname WORD Network name of this system Switch(config)# hostname JN7612GP-4F 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
	Hardware Information :
	  Product Name : JetNet 7612GP-4F
	  Serial Number: 001277ff0004
	  MAC Address : 001277FF0004
	  Manufacturing Date : 2017/06/06
	Software Information :
	  Loader Version: 1.0.0.2
	  Firmware Version: 1.0-20170606-17:43:32
	  System OID : 1.3.6.1.4.1.24062.2.3.12
	Copyright 2006-2015 Korenix Technology Co., Ltd.
	
	Switch# show hardware
	  led led information
	  mac mac address
	
	Switch# show hardware mac
	MAC Address : 00:12:77:FF:01:B0
	Switch# show hardware led
	  Power 1 : On
	  Power 2 : Off
	  DI 1 : Off
	  Alarm 1 : Off
	  RDY : On
	  RM : Off
	  RF : Off

Admin Password	
User Name and Password Display	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. Switch# show administrator Administrator account information name: admin password: admin
IP Configuration	
IP Address/Mask (192.168.10.8, 255.255.255.0	Switch(config)# int vlan 1 Switch(config-if)# ip address dhcp igmp Switch(config-if)# ip address 192.168.10.8/24 **(DHCP Client)** Switch(config-if)# ip dhcp client Switch(config-if)# ip dhcp client renew
Gateway	Switch(config)# ip route 0.0.0.0/0 192.168.10.254/24
Remove Gateway	Switch(config)# no ip route 0.0.0.0/0 192.168.10.254/24
Display	Switch# show interface vlan1 Interface vlan1
	Description : N/A Administrative Status : Enable Operating Status : Up DHCP Client : Disable Primary IP Address : 192.168.10.8/24 IPv6 Address : fe80::212:77ff:feff:6666/64 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 !
IPv6 Address/Prefix	Switch(config)# interface vlan1 Switch(config-if)# ipv6 address 2001:0db8:85a3::8a2e:0370:7334/64
IPv6 Gateway	Switch(config)# ipv6 route 0::0/0 2001:0db8:85a3::8a2e:0370:FFFE
Remove IPv6 Gateway	Switch(config)#no ipv6 route 0::0/0 2001:0db8:85a3::8a2e:0370:FFFE

Display	Switch# show running-config
	……
	interface vlan1
	  ip address 192.168.10.6/24
	  ipv6 address 2001:db8:85a3::8a2e:370:7334/64
	  no shutdown
	!
	ip route 0.0.0.0/0 192.168.10.254
	ipv6 route ::/0 2001:db8:85a3::8a2e:370:fffe
	!

Time Setting	

NTP Server	Switch(config)# ntp peer
	  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

JumboFrame	
Jumbo Frame	Type the maximum MTU to enable Jumbo Frame: Switch(config)# system mtu <1500-9216> Switch(config)# system mtu 9216 Disable Jumbo Frame: Switch(config)# no system mtu

Display	Switch# show system mtu System MTU size is 9712 bytes After disabled Jumbo Frame: Switch# show system mtu System MTU size is 2000 bytes
DHCP	
DHCP Commands	Switch(config)# router dhcp Switch(config-dhcp)# default-router DHCP Default Router end Exit current mode and down to previous enable mode exit Exit current mode and down to previous mode ip IP protocol lease DHCP Lease Time list Print command list network dhcp network no remove quit Exit current mode and down to previous mode service enable service
DHCP Server Enable	Switch(config-dhcp)# service dhcp <cr>
DHCP Server IP Pool (Network/Mask)	Switch(config-dhcp)# network A.B.C.D/M network/mask ex. 10.10.1.0/24 Switch(config-dhcp)# network 192.168.10.0/24
DHCP Server – Default Gateway	Switch(config-dhcp)# default-router A.B.C.D address Switch(config-dhcp)# default-router 192.168.10.254
DHCP Server – lease time	Switch(config-dhcp)# lease TIME second Switch(config-dhcp)# lease 1000 (1000 second)
DHCP Server – Excluded Address	Switch(config-dhcp)# ip dhcp excluded-address A.B.C.D IP address Switch(config-dhcp)# ip dhcp excluded-address 192.168.10.123 <cr>
DHCP Server – Static IP and MAC binding	Switch(config-dhcp)# ip dhcp static MACADDR MAC address Switch(config-dhcp)# ip dhcp static 0012.7700.0001 A.B.C.D leased IP address Switch(config-dhcp)# ip dhcp static 0012.7700.0001 192.168.10.99

DHCP Server – Option82 binding	Switch(config-dhcp)# ip dhcp option82 circuit-id
	  string string input (using "any" if you don't want to specify CID)
	  hex hexadecimal input
	Switch(config-dhcp)# ip dhcp option82 circuit-id hex 11:22:33
	  remote-id Remote-ID
	Switch(config-dhcp)# ip dhcp option82 circuit-id hex 11:22:33 remote-id
	  string string input (using "any" if you don't want to specify RID)
	  hex hexadecimal input
	Switch(config-dhcp)# ip dhcp option82 circuit-id hex 11:22:33 remote-id string relay-agent-a
	  A.B.C.D leased IP address
	Switch(config-dhcp)# ip dhcp option82 circuit-id hex 11:22:33 remote-id string relay-agent-a 192.168.10.6

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 Address192.168.10.123
	
	Manual Binding List
	  IP Address MAC Address
	--- ---
	  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 JN7612GP-4F.bin Firmware upgrading, don't turn off the switch! Tftping file JN7612GP-4F.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

2.3 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:

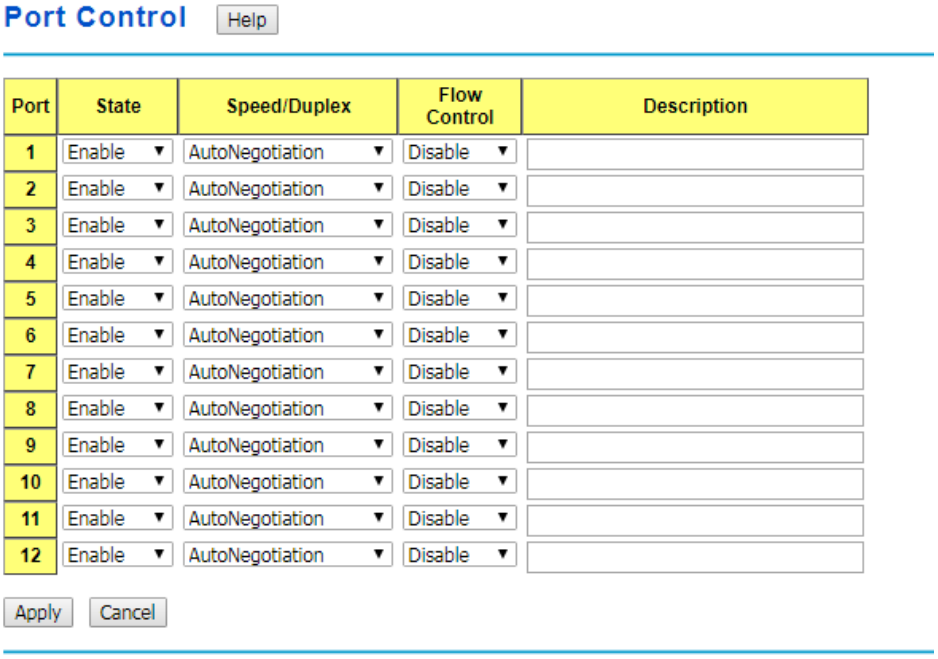
2.3.1 Understand the port mapping
2.3.2 Port Control
2.3.3 Port Status
2.3.4 Rate Control
2.3.5 Storm Control
2.3.6 Port Trunking
2.3.7 Command Lines for Port Configuration

2.3.1 Understand the port mapping

Before configuring the port settings, understand the port number in JetNet Managed Switch first. For example, there are 12 Gigabit Ethernet ports of JetNet 7612GP-4F/7612G-4F/5612GP-4F/5612G-4F. In Web UI, choose the port number you want to configure, the available number from port gi1, gi2…gi12 to present port 1 to port 12. Each Switch with different available ports that depends on the physical port number.

2.3.2 Port Control

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



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

State: You can enable or disable the state of this port. Once you click **Disable**, the port stops to link to the other end and stops to forward any traffic. The default setting is **Enable** which means all the ports are workable.

Speed/Duplex: You can configure port speed and duplex mode of each port. You can manually configure your speeds from using the options:

- Auto Negotiation (default)
- 10M full-duplex (10 Full)
- 10M half-duplex (10 Half)
- 100M full-duplex (100 Full)
- 100M half-duplex (100 Half)

The default mode is “Auto Negotiation mode”, which allows the two interfaces on the link to exchange the capabilities and characteristics of each side and selects the best operating mode automatically when a cable is connected.

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.

Fiber:

- Auto Negotiation (default)
- 100M Full

The default mode is “Auto Negotiation mode”, which allows the two interfaces on the link to exchange the capabilities and characteristics of each side and selects the best operating mode automatically when a cable is connected.

If user would like to use “100M” for fiber, please manual set to 100 Full.

Flow control:

Enable means that you need to activate the flow control function of the remote network device to let the flow control of that corresponding port on the switch to work. Disable (default) means that you do not need to activate the flow control function of the remote network device, as the flow control of that corresponding port on the switch works.

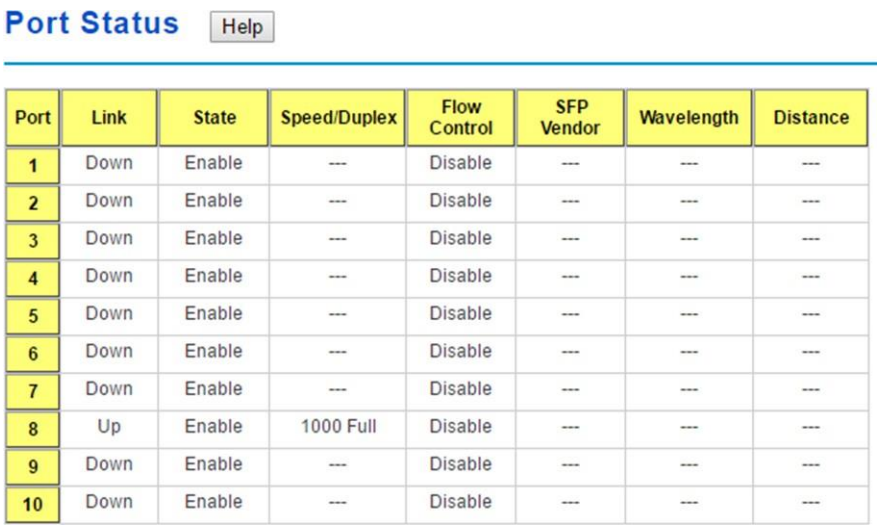
Description: The description of interface.

Click **Apply** to apply your settings.

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

2.3.3 Port Status

The Port Status page displays the current port status, including Small Form Factor (SFP) fiber transceiver with Digital Diagnostic Monitoring (DDM) function that provides real time information of SFP transceiver and allows you to diagnostic the optical fiber signal received and launched.



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

Link: Shows link status; **Up** means the link is up and **Down** means that the link is down.

State: Shows the port state. If the state is enabled it displays Enable. If the port is disabled or shutdown, it displays Disable.

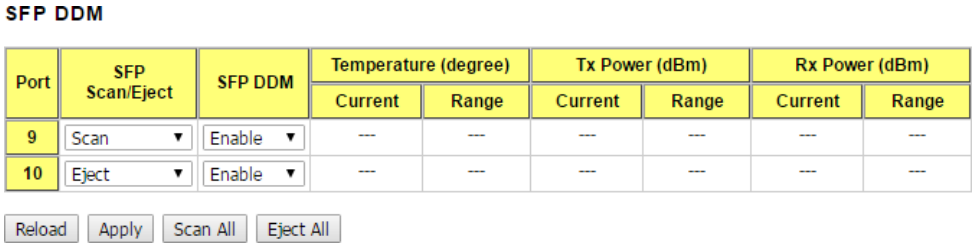
Speed/Duplex: Current working status of the port.

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 that is plugged into the SFP port or ports.

Distance: The distance of the SFP transceiver that is plugged into the SFP port or ports.



SFP Scan/Eject: Click the **Scan** / **Eject** button to scan or safely remove the SFP.

SFP DDM: Click the **Enable** / **Disabl**e button to enable or disable the SFP DDM function.

Temperature: Displays the current temperature detected and acceptable temperature range for the DDM SFP transceiver.

Tx Power (dBm): Displays the current transmit power detected and acceptable Tx power range for the DDM SFP transceiver.

Rx Power (dBm): Displays the current received power and acceptable Rx power range for the DDM SFP transceiver.

Click **Reload** to reload the all port information.

Click **Apply**to apply your settings.

Scan all: Scan the SFP transceiver and display.

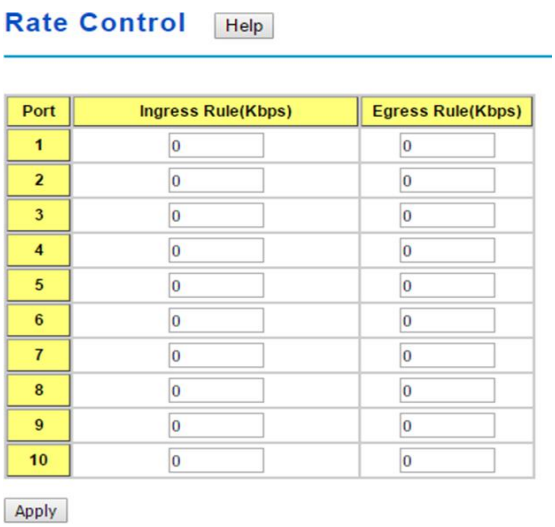
Eject All: Eject all of the SFPs.

Note: Most of the SFP transceivers provide vendor information that allows the switch to read it. The web interface can display vendor name, wave length, and distance of all SFP transceiver models. If you see Unknown info, it may mean that the vendor does not provide their information or that the information of their transceiver cannot be read.

If the plugged DDM SFP transceiver is not certified by Korenix, the DDM function is not supported, but the communication is not disabled.

2.3.4 Rate Control

Rate limiting is used to control the rate of traffic that is sent or received on a network interface. For ingress rate limiting, traffic that is less than or equal to the specified rate is received, whereas traffic that exceeds the rate is dropped. For egress rate limiting, traffic that is less than or equal to the specified rate is sent, whereas traffic that exceeds the rate is dropped.



The ports support port ingress and egress rate control.

Ingress Rule(Kbps): The rate range of Ingress rate is from 70 Kbps to 256000 Kbps and zero means no limit. The default value is 8 Mbps.

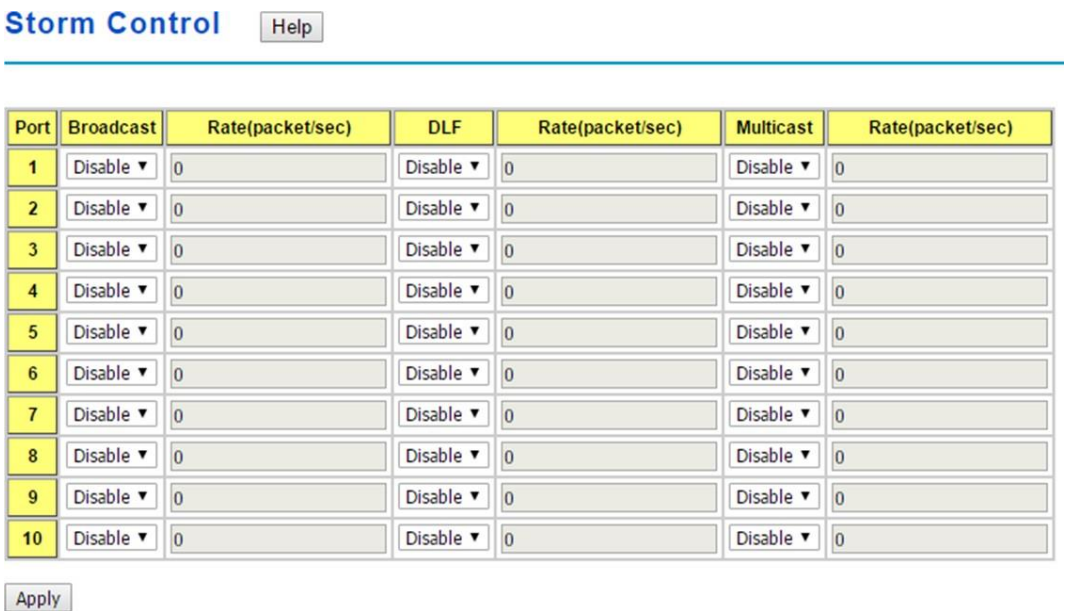
Egress Rule(Kbps): The rate range of Egress rate is from 70 Kbps to 256000 Kbps and zero means no limit. The default value is 0 Mbps which is "no-limit". Egress rate limiting has an effect on all types of packets, including unicast, multicast and broadcast packets.

Click **Apply** to apply your settings.

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

2.3.5 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.



Port: This is the port identifier.
Broadcast: To enable or disable broadcast storm control on this port. The valid Broadcast rate limit ranges from 2 to 262142 packet/sec, zero means no limit.
DLF: To enable or disable destination lookup failure storm control on the corresponding port. Destination lookup failure rate limit range from 2 to 262142 packet/sec, zero means no limit.
Multicast: To enable or disable multicast storm control on this port. The Multicast rate limit ranges from 2 to 262142 packet/sec, zero means no limit.

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

2.3.6 Port Trunking

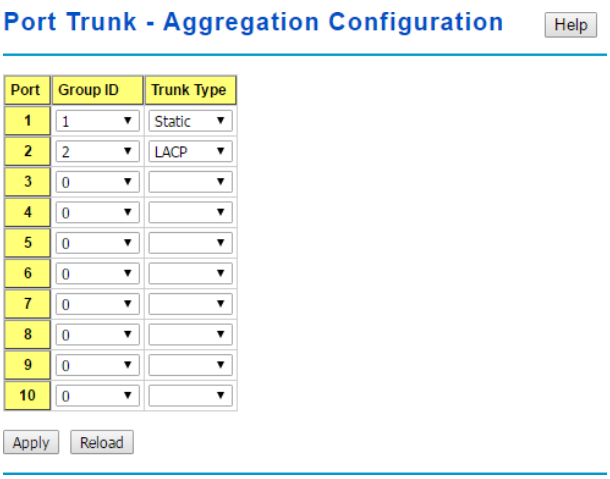
Port Trunking configuration allows you to group multiple Ethernet ports in parallel to increase link bandwidth. The aggregated ports can be viewed as one physical port so that the bandwidth is higher than merely one single Ethernet port. The member ports of the same trunk group can balance the loading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

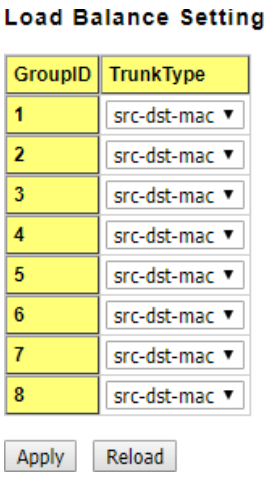
There are some different descriptions for the port trunking. Different manufacturers may use different descriptions for their products, like Link Aggregation Group (LAG), Link Aggregation Control Protocol, Ethernet Trunk, Ether Channel…etc. Most of the implementations now conform to IEEE standard, 802.3ad.

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

There are 2 configuration pages, Aggregation Configuration and Aggregation Information.

Aggregation Setting





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.
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.

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

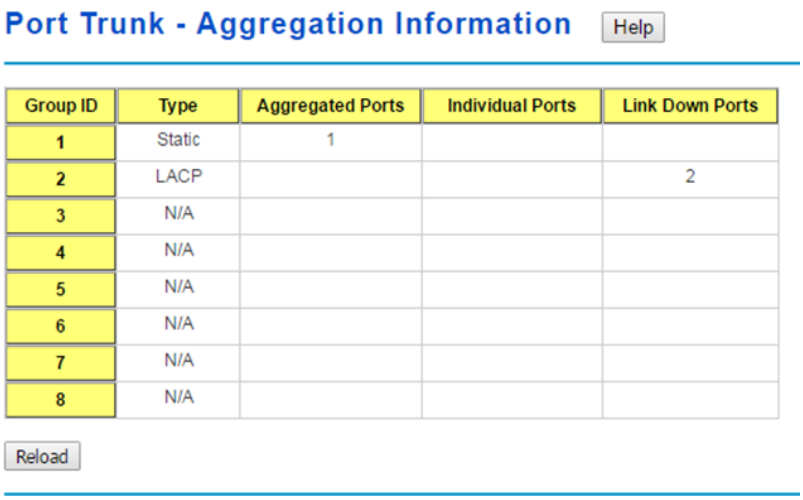
src-mac	load distribution is based on the source MAC address
dst-mac	load distribution is based on the destination-MAC address
src-dst-mac	load distribution is based on the source and destination MAC address
src-ip	load distribution is based on the source IP address
dst-ip	load distribution is based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

Click **Apply** to apply your settings.

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

Aggregation Information

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



Group ID: Display the Trunk Group ID 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.

Click **Reload** to reload aggregation settings.

2.3.7 Command Lines for Port Configuration

Feature	Command Line
Port Control	
Port Control – State	Switch(config-if)# shutdown -> Disable port state interfacegigabitethernet1 is shutdown now. Switch(config-if)# no shutdown -> Enable port state Interfacegigabitethernet1 is up now.

Port Control – Auto Negotiation	Switch(config)# interface gi1 Switch(config-if)# auto-negotiation Auto-negotiation of port 1 is enabled!
Port Control – Force Speed/Duplex	Switch(config-if)# speed 100 set the speed mode ok! Switch(config-if)# duplex full set the duplex mode ok!
Port Control – Flow	Switch(config-if)# flowcontrol on
Control	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 gi1 Interface gigabitethernet1 Description : N/A Administrative Status : Enable Operating Status : Connected Duplex : Full Speed : 100 MTU: 1518 Flow Control :off Default Port VLAN ID: 1 Acceptable Frame Type : All Auto Negotiation : Disable Loopback Mode : None STP Status: forwarding Default CoS Value for untagged packets is 0. Medium mode is Copper. *Note: Administrative Status -> Port state of the port. Operating status -> Current status of the port. Duplex ->Duplex mode of the port. Speed -> Speed mode of the port. Flow control -> Flow Control status of the port.*
Rate Control	
Rate Control – Ingress or Egress	Switch(config-if)# rate-limit egress Outgoing packets ingress Incoming packets ***Note: To enable rate control, you should select the Ingress or Egress rule first; then assign the packet type and bandwidth.***
Rate Control - Bandwidth	Switch(config-if)# rate-limit ingress bandwidth <0-1000000> Limit in kilobits per second (FE: 0-100000, GE: 0-1000000, 0 isno limit) Switch(config-if)# rate-limit ingress bandwidth1600 Set the ingress rate limit 1600Kbps for Port 1..
Storm Control	

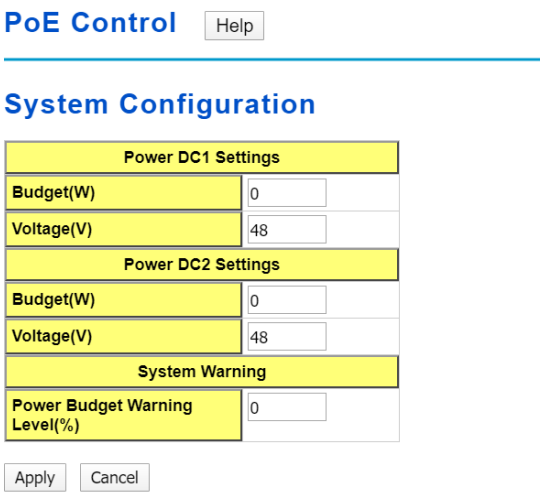
Strom Control – Rate Configuration (Packet Type)	Switch(config-if)# storm-control broadcast Broadcast packets dlf Destination Lookup Failure multicast Multicast packets SWITCH(config)# storm-control broadcast ? <0-262143> Rate limit value 0~262143 packet/sec SWITCH(config)# storm-control broadcast 1000 Enables rate limit for Broadcast packetsfor Port 1 SWITCH(config)# storm-control multicast 1000 Enables rate limit for Multicast packetsfor Port 1 SWITCH(config)# storm-control dlf 1000 Enables rate limit for Destination Lookup Failue packets for Port1.
Display – Rate Configuration and port status	SWITCH# show storm-control Storm-control for Port 1 Broadcast packets : Disabled Rate : 1000 (packets/s) Destination Lookup Failure packets : Enabled Rate : 1000 (packets/s) Multicast packets : Disabled Rate : 1000 (packets/s) Storm-control for Port 2 Broadcast packets : Disabled Rate : N/A (packets/s) Destination Lookup Failure packets : Disabled Rate : N/A (packets/s) Multicast packets : Disabled Rate : N/A (packets/s) Storm-control for Port 3 Broadcast packets : Disabled Rate : N/A (packets/s) Destination Lookup Failure packets : Disabled Rate : N/A (packets/s) Multicast packets : Disabled Rate : N/A (packets/s) ……
Port Trunking	
LACP	Switch(config)# lacp group 1 fa8-10 Group 1 based on LACP(802.3ad) is enabled! *Note: The interface list is fa1,fa3-5,fa8-10* Note: different speed port can't be aggregated together.
LACP – Port Setting	SWITCH(config-if)# lacp port-priority LACP priority for physical interfaces timeout assigns an administrative LACP timeout SWITCH(config-if)# lacp port-priority <1-65535> Valid port priority range–1 - 65535 (default is 32768) SWITCH(config-if)# lacp timeout long specifies a long timeout value (default) short specifies a short timeout value SWITCH(config-if)# lacp timeout short Set lacp port timeout ok.

Static Trunk	Switch(config)# trunk group 2 fa6-7 Trunk group 2 enable ok! Failure to configure due to the group ID is existed. SWITCH(config)# trunk group 1 fa11- 12 'an't set trunk group 1 enable! The group 1 is a lacp enabled group! SWITCH(config)# trunk group 2 fa11- 12 'an't set trunk group 2 enable! The group 2 is a static aggregation group.
Display - LACP	Switch# show lacp counters LACP statistical information group LACP group internal LACP internal information neighbor LACP neighbor information port-setting LACP setting for physical interfaces system-id LACP system identification system-priority LACP system priority SWITCH# show lacp port-setting LACP Port Setting : Port Priority Timeout ----- --------- -------- 1 32768 Long 2 32768 Long 3 32768 Long ……. Switch# show lacp internal LACP group 1 internal information: LACP Port Admin Oper Port Port Priority Key Key State ----- ----------- -------- -------- ------- 8 1 8 8 0x45 9 1 9 9 0x45 10 1 10 10 0x45 LACP group 2 is inactive LACP group 3 is inactive LACP group 4 is inactive
Display - Trunk	Switch# show trunk group 1 FLAGS: I -> Individual P -> In channel D -> Port Down Trunk Group GroupID Protocol Ports --------+---------+----------------------------------- 1 LACP 8(D) 9(D) 10(D)

2.4 Power over Ethernet (JetNet PoE Switch only)

Power over Ethernet is the key features of JetNet PoE Switch. It is fully compliance with IEEE 802.3af and IEEE 802.3at that include 1-event with IEEE 802.1AB LLDP classification and 2-event classification.

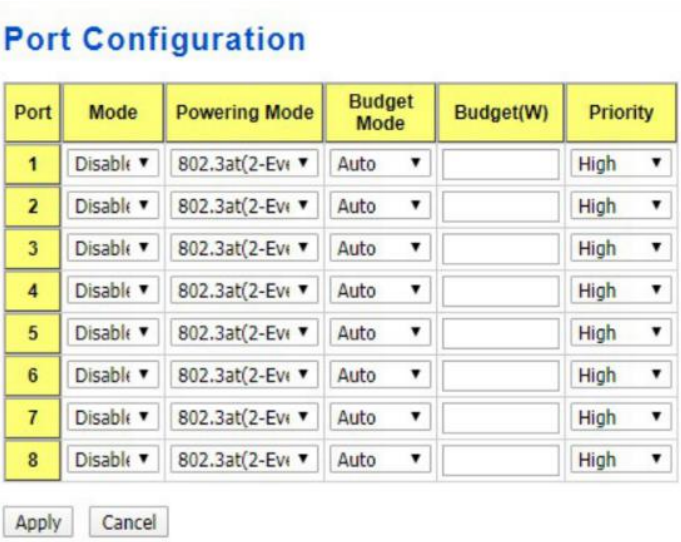
2.4.1 PoE Control



Budget(W): Total power budget of JetNet7612GP-4F and JetNet5612GP-4F is 240W. Power budget can separately set for both DC1 and DC2.

Voltage(V): Default setting as 48VDC input for PoE supply.

Power Budget Warning Level (%): If the power utilization is more than the Power Budget level, the system sends a warning event. The range is 0-100% (in percentage and 0 is disabled). Click the **Apply** button to apply the PoE System configuration changes.



Mode: You can set PoE port state to Enable, Disable or Schedule.

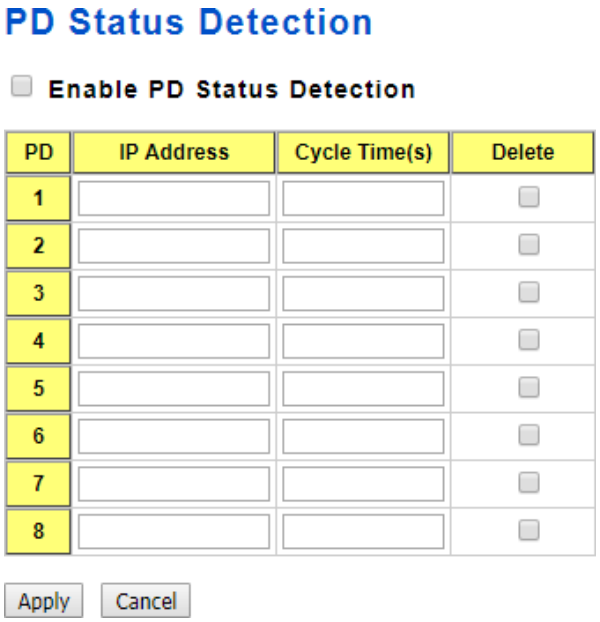
Powering Mode: The following modes are available:

- **802.3af**: 802.3af is set powering mode to standard IEEE 802.3af.
- **802.3at(LLDP)**: 802.3at(LLDP) is set powering mode to standard IEEE 802.3at LLDP.
- **802.3at(2 Event)**:802.3at(2 Event) is set powering mode to standard IEEE 802.3at Phyiscal.
- **Force**: Force mode directly delivers power without protocol negotiation.

Budget Mode: Auto or Manual

Budget(W): The limitation of output power (in watts). The range is from 0.44-35W. Click the Apply button to apply the port configurations.

Priority: There are three different priority can be chosen. From highest to lowest will be critical→High→Low.
If power source reduced, impacting total power budget. PoE power supply will be stopped from low priority (low-high-critical). If port priority is the same, PoE power will be stopped from higher port number (port8~port1).



The JetNet PoE Switch supports an useful function named***LPLD(Link Partner Line Detection)***that help user to mainten the PD's status and save the maintenance time and human resource.Thisfuction is patented by Korenix. Once enable this function, the PoE Switch will request PD system in the period of time (cycle time). If PD system does not echo the request, the switch will turn-off PoE power and then turn-on PoE power again. Which help PD to recovery automatically and reduce mainten efforts like assigning an engineer to reset the PD.

Select the checkbox to enable the PD Status Detection function.

IP address: The IP address of the detecting PD which installed on the port.

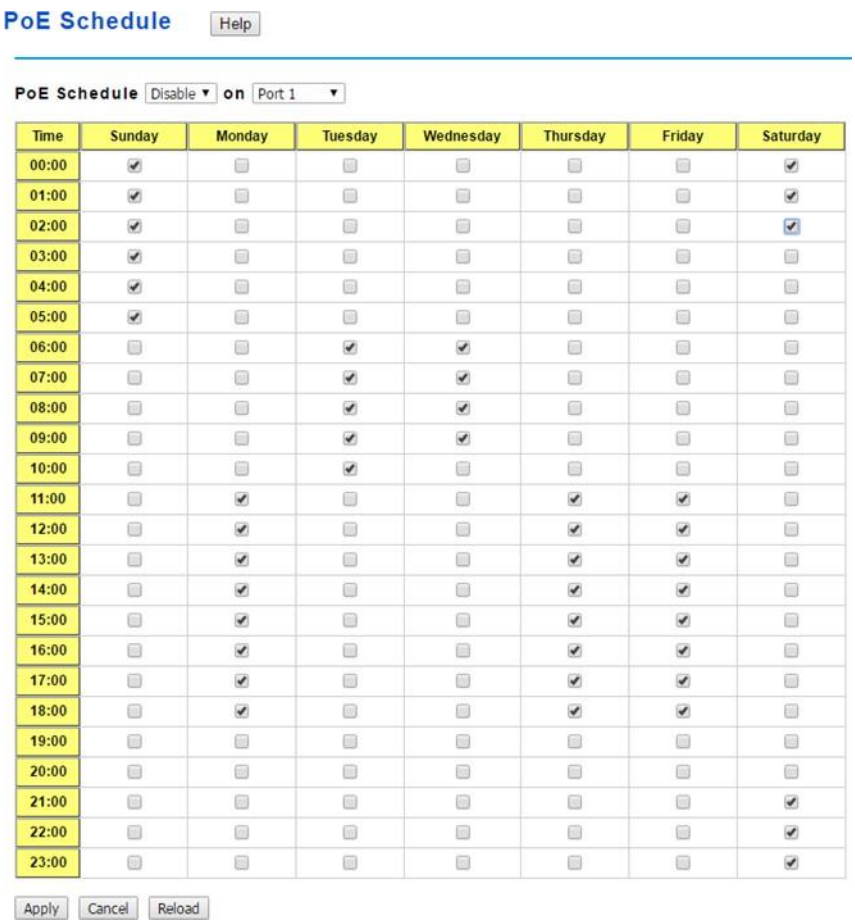
Cycle Time(s): The period of time one PD failure detection (in seconds). We suggest to set the cycle time to 90 secondssince most of PDs (IP camera) will take at least 40~50 seconds to restart.

Click the **Apply** button to apply the PoE PD failure detection configurations.

Note: During the PoE operating, the surface temperature will be high. Don’t touch device surface during PoE operating.

2.4.2 PoE Schedule

The PoE Schedule supports hourly and weekly base PoE schedule configuration.



Select **Enable**or **Disable** on the target port and select the checkbox on the target time.

Click**Apply** to apply the settings.

Click **Cancel** to clear the settings.

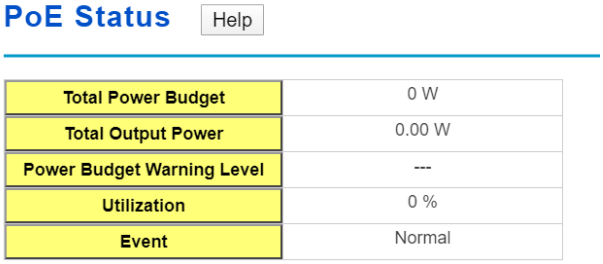
Click **Reload**to reload the information.

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

The PoE ports will working as thePoE Schedule and follow the system clock. As this result, be sure the system clock have configured as your local time.

2.4.3 PoE Status

The PoE Status page shows the system PoE status and the operating status of each PoE Port.



Total Power Budget: This is the maximum PoE output power (in watts).

Total Output Power: Total output power of PoE system (in watts).

Power Budget Warning Level: If power utilization is more than the warning level, the system sends a warning event. The range is 0-100% and 0 is means it is disabled.

Utilization: This is the utilization of the total power budget.

Event: The status of PoE system.

Port	Mode	Status	Class	Budget(w)	Consumption(W)	Voltage(V)	Current(mA)
1	Disable	Off	---	---	0.00	0.0	0.0
2	Disable	Off	---	---	0.00	0.0	0.0
3	Disable	Off	---	---	0.00	0.0	0.0
4	Disable	Off	---	---	0.00	0.0	0.0
5	Disable	Off	---	---	0.00	0.0	0.0
6	Disable	Off	---	---	0.00	0.0	0.0
7	Disable	Off	---	---	0.00	0.0	0.0
8	Disable	Off	---	---	0.00	0.0	0.0

Reload

Port: The number of the port.

Mode: This is the PoE mode of that port, which can be one of these settings: Enable, Disable or Schedule.

Status: This is the operation status of the PSE.

Class: This is the PD class determined by detection.

Budget(W): This is the output budget of the ports (in watts).

Consumption(W): This is the output consumption of the ports (in watts).

Voltage(V): This is the output voltage of the ports (in volts).

Current(mA): The output current of the ports (in milliamps).

Click **Reload** to reload the PoE status.

2.5 Network Redundancy

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

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

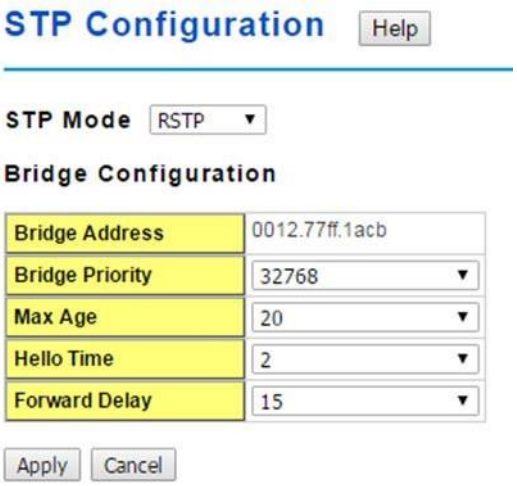
Multiple Super Ring (MSR) technology is *Korenix's* 3rd generation Ring redundancy technology. This is patented and protected by *Korenix* and is used in countries all over the world. MSR ranksthe fastest restore and failover time in the world, 0 ms for restore and about several milliseconds for failover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

2.5.1 STP Configuration

This page allows you to select the STP mode and configure the global STP/RSTP bridge configuration. Spanning Tree Protocol (STP; IEEE 802.1D) provides a loop-free topology for any LAN or bridged network.



STP Mode: Select the spanning tree protocol: STP, RSTP or MSTP or Disable

Bridge Address: The MAC addres used to identify the bridge. This value cannot be modified.

Bridge Priority: 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: 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: 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.

Forward Delay: 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.

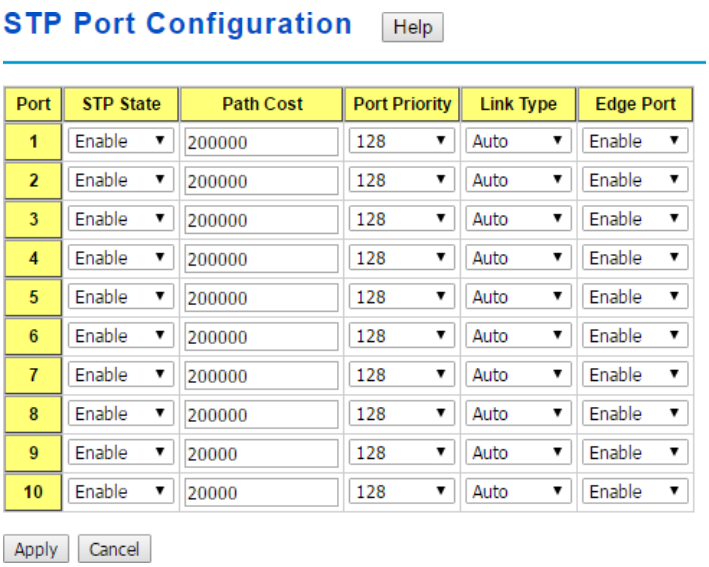
Note: You must observe the following rule to configure Max Age, Hello Time, and Forwarding Delay parameters.

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

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

2.5.2 STP Port Configuration

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



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.

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.**

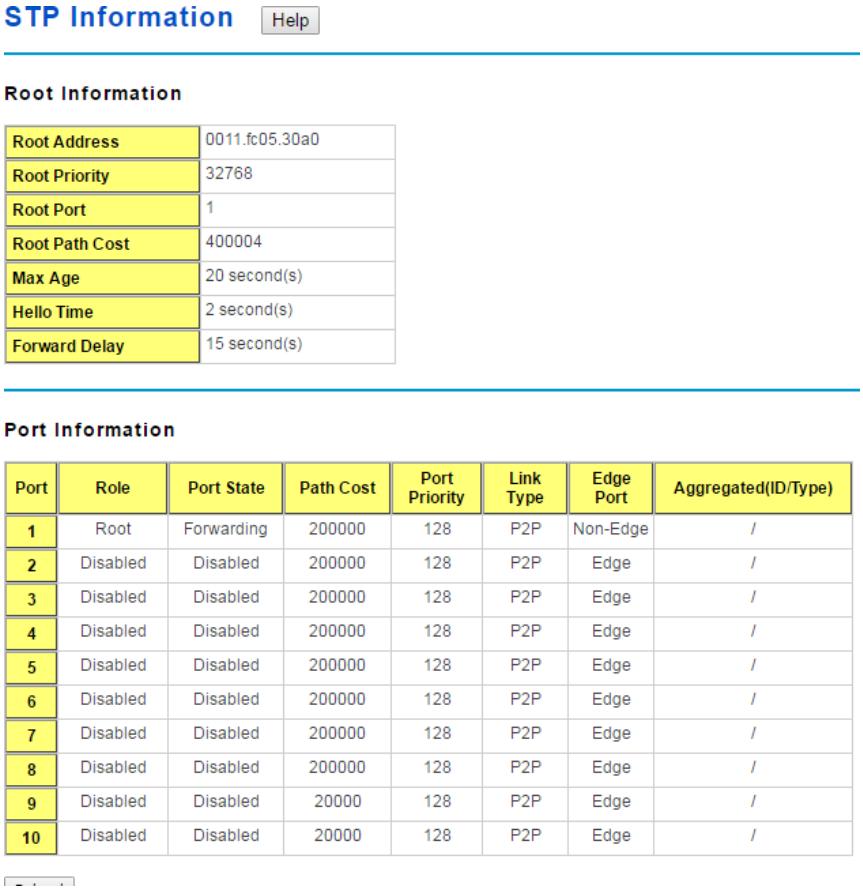
Some of the rapid state transitions that are possible within RSTP depend upon whether the port of concern can only be connected to another bridge (i.e. it is served by a point-to-point LAN segment), or if it can be connected to two or more bridges (i.e. it is served by a shared-medium LAN segment). This 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: Spanning tree bridges communicate data between themselves using Bridge Protocol Data Units (BPDU). If a port does not receive a BPDU it is considered an edge port and traffic is automatically forwarded to it. If a BPDU is received on a port it is considered a non-edge port. If you want to force the port to be a non-edge port set this value to **Disable**. Otherwise set it to **Enable**.

Click Apply to apply your settings.

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

2.5.3 STP Information



Root Information

You can see Root Address, 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, Link Type, Edge Port mode and Aggregated (ID/Type).

Click **Reload** to reload the information.

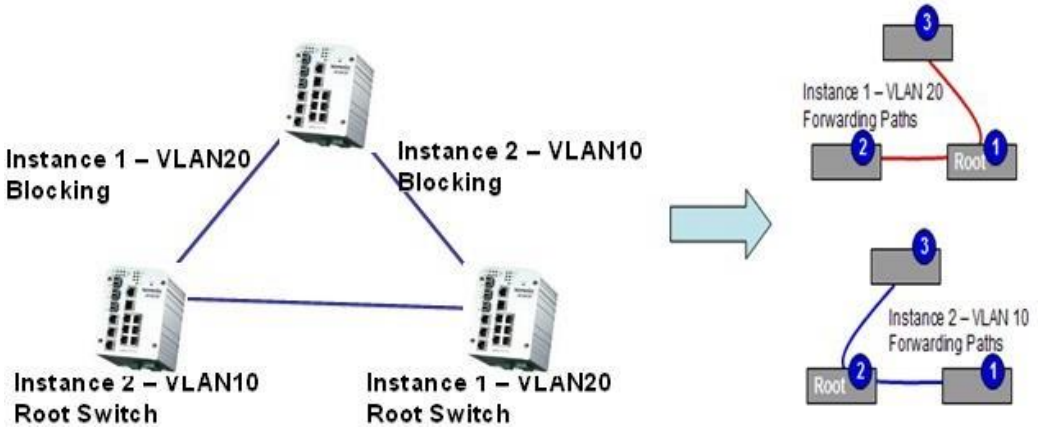
2.5.4 MSTP Configuration

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

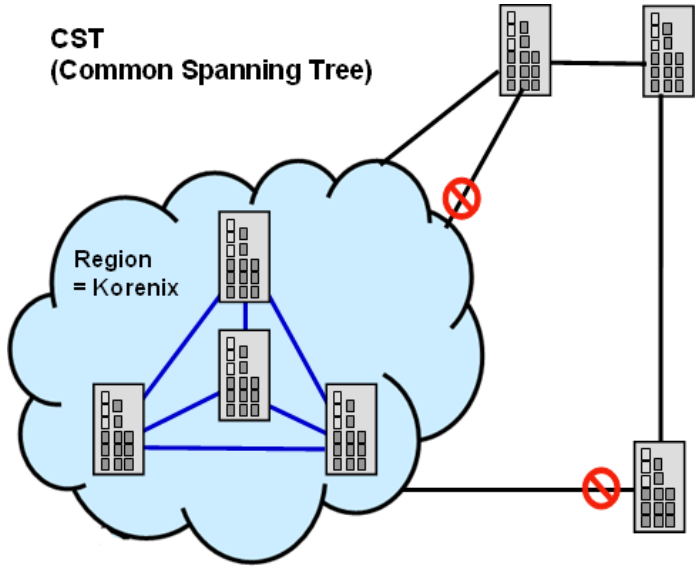
One VLAN can be mapped to a Multiple Spanning Tree Instance (MSTI). The maximum Instance of JetNet Managed Switch support is 16, range from 0-15. The MSTP builds a separate Multiple Spanning Tree (MST) for each instance to maintain connectivity among each of the assigned VLAN groups. An Internal Spanning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

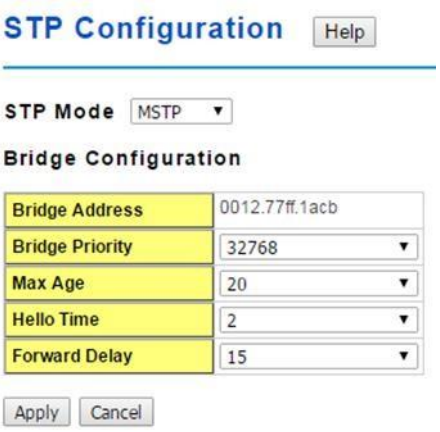


A Common Spanning Tree (CST) interconnects all adjuacent MST regions and acts as a virtual bridge node for communications with STP or RSTP nodes in the global network. MSTP connects all bridges and LAN segments with a single Common and Internal Spanning Tree (CIST). The CIST is formed as a result of the running spanning tree algorithm between switches that support the STP, RSTP, MSTP protocols.

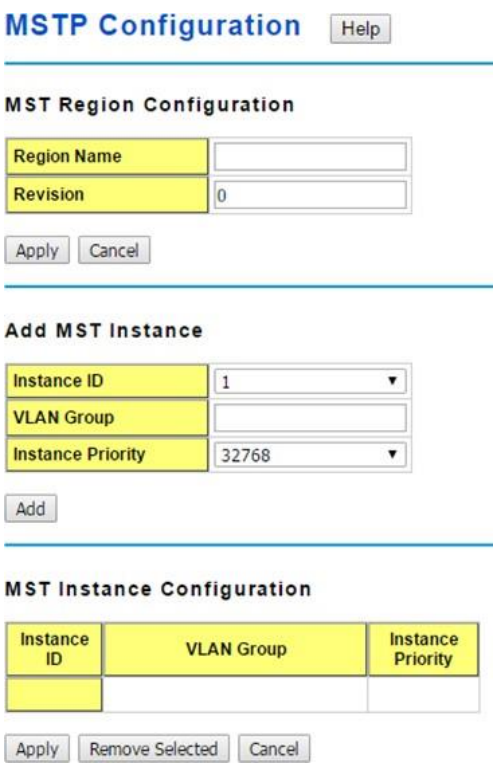
The figure shows the CST large network. In this network, a Region may have different instances and its own forwarding path and table; however, it acts as a single Brige of CST.



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: A name used to identify the MST Region. Maximum length: 32 characters.

Revision: A value used to identify the MST Region. Range: 0-65535; Default: 0).

Click **Apply** to apply the settings.

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

Add 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: A value used to identify the MST instance, valid value are 1 through 15. Instance 0(CIST, Common Internal Spanning Tree) is a special instance of spanning-tree known as IST or Internal Spanning Tree (=MSTI00).

VLAN Group: Provide a VLAN group to map this MST instance. Use the VLAN number, for example: 10. You can set a range, for example: 1-10) or set specific VLANs, for example: 2,4,6,4-7.

Instance Priority: A value used to identify the MST instance. The MST instance with the lowest value has the highest priority and is selected as the root. Enter a number 0 through 61440 in increments of 4096.

Click on **Add** to apply your settings.

MST Instance Configuration

This page allows you to see the current MST Instance Configuration you added.

Click "**Apply**" to apply the setting.

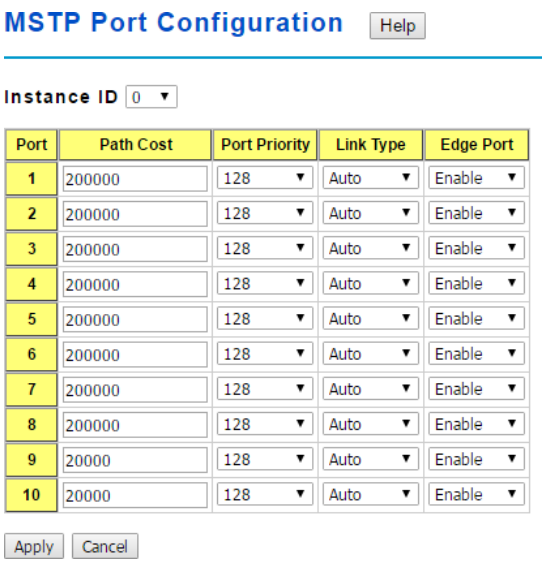
Click "**Remove Selected"** to remove the setting selected.

Click "**Cancel"** to clear the setting.

2.5.5 MSTP Port Configuration

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

Note: 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.



Instance ID: Select an Instance ID to display and modify MSTP instance setting.

Path Cost: The cost of the path to the other bridge from this transmitting bridge at the specified port. Enter a number from 1 through 200000000.

Port Priority: Decide which port should be blocked by priority on your LAN. Enter a number from 0 through 240 in increments of 16.

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.

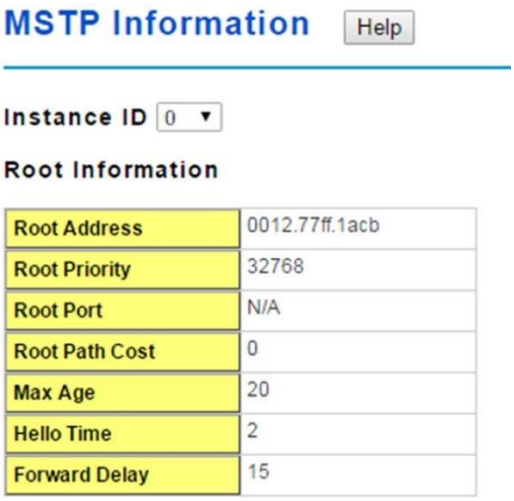
Click **Apply** to apply the settings.

Click **Cancel** to clear the settings.

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

2.5.6 MSTP Information

This page allows you to see the current MSTP information. Choose the **Instance ID** first. If the instance is not added, the information remains blank.



Port Information

Port	Role	Port State	Path Cost	Port Priority	Link Type	Edge Port
1	Disabled	Blocking	200000	128	P2P	Edge
2	Disabled	Blocking	200000	128	P2P	Edge
3	Disabled	Blocking	200000	128	P2P	Edge
4	Disabled	Blocking	200000	128	P2P	Edge
5	Disabled	Blocking	200000	128	P2P	Edge
6	Disabled	Blocking	200000	128	P2P	Edge
7	Root	Forwarding	200000	128	P2P	Non-Edge
8	Disabled	Blocking	200000	128	P2P	Edge
9	Disabled	Blocking	20000	128	P2P	Edge
10	Disabled	Blocking	20000	128	P2P	Edge

Reload

Instance ID

Select an **instance ID** to display MSTP instance information. Instance 0 (CIST, Common Internal Spanning Tree) is a special instance of spanning-tree known as IST or Internal Spanning Tree (=MSTI00).

Root Information

The Root Information shows the setting of the Root switch.

Port Information

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

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

2.5.7 MSR Configuration

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 fatest 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.

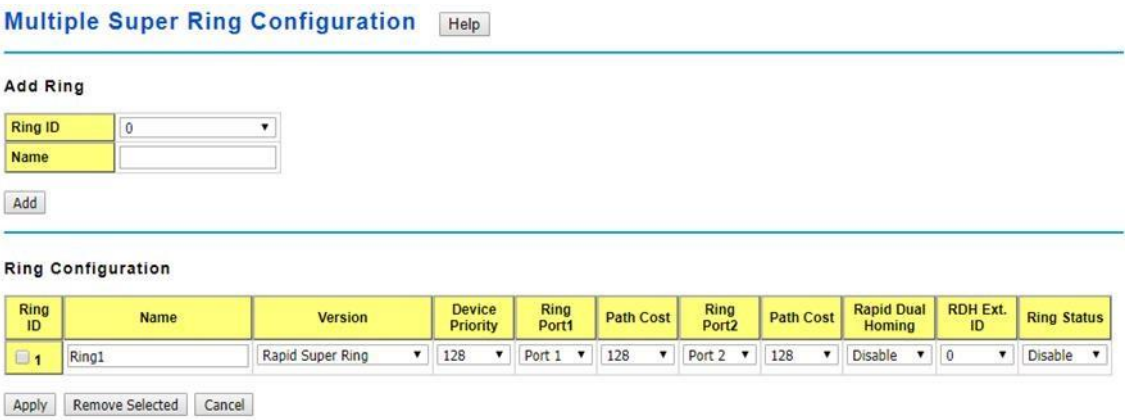
Rapid Dual Homing (RDH) technology also facilitates *JetNet Managed Switch* to connect with a core managed switch easily and conveniently. With RDH technology, you can also

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 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. The feature saves much effort when constructing complex network architecture.

To become backwards compatible with the Legacy Super Ring technology implemented in JetNet Managed 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.



Add Ring

New Ring: Select the **Ring ID**, which has range from 0 to 31. If the name field is left blank, the name of this ring is automatically named with the Ring ID.

Ring Configuration

Ring ID: Once a Ring is created, the Ring ID appears, and cannot be changed. In multiple ring environments, the traffic can only be forwarded under the same Ring ID. Remember to check the Ring ID when there are more than one ring in existence.

Name: This field shows the name of the Ring. If it is not entered when creating, it is 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 Port2: 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 Port2. 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 ports will become the blocking port, if the Path Cost is the same, the port with larger port number will become the blocking port.

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 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.

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

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

Click **Apply** to apply the settings.

Click **Remove Selected** to remove the setting selected.

Click **Cancel** to clear the settings.

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

Super Chain Configuration



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

Role: Super Chain has two node roles, Border and Member. Border is the node, which connects to an external network. Member is the node except the Border node in the Super Chain.

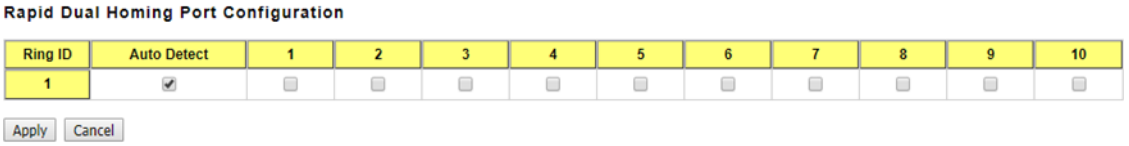
Edge Port: Edge Port is one of ring ports of Border node. It is used to connect to an external network.

Click **Apply** to apply the settings.

Click **Cancel** to clear the modification.

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

Rapid Dual Homing Port Configuration



Ring ID: The Ring Identifier referring to this Ring.

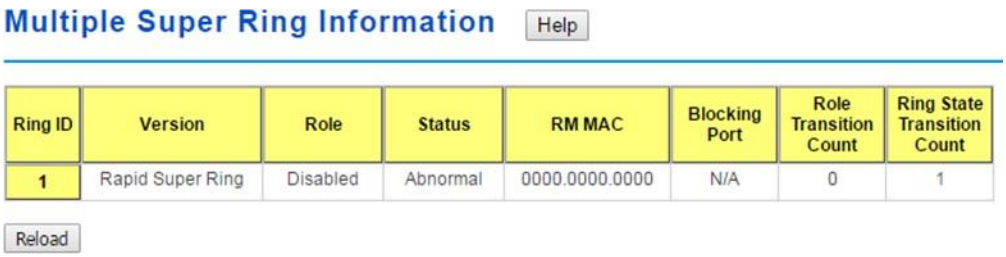
Auto Detect: Enable RDH auto detect RDH port mode.

Port: Enable RDH on specific ports.

Click "**Apply**" to apply the setting.

Click "**Cancel"** to clear the modification.

2.5.8 MSR Information



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

Version: Displays the ring version, this field could be Rapid Super Ring or Super Chain.

Role: This Switch is the RM (Ring Master) or nonRM (non-ring master).

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.

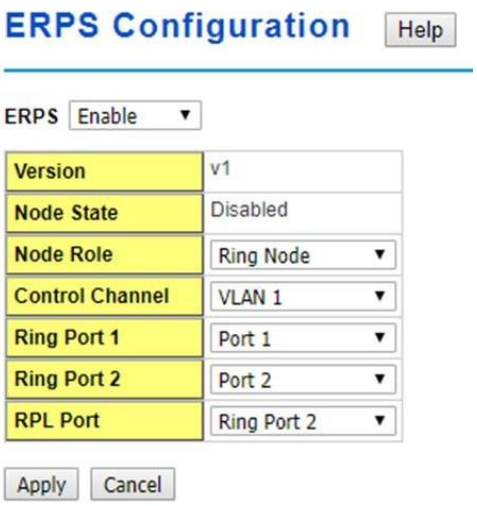
Role state Transition Count: This number means how many times the Ring status has been transformed between **Normal** and **Abnormal** state.

Click **Reload** to reload the information.

2.5.9 ERPS Configuration

Ethernet Ring Protection Switching (ERPS) is an Ethernet ring protocol defined in ITU-T G.8032. ERPS is capable of recovering from a network failure under 50ms and prevents loops from existing within the ring.

The page allows you to configure the switch to be a member of an ERPS ring



ERPS: **Enable** or **Disable** ERPS on the switch.

Version: The ERPS version. This switch supports version 1.

Node State: Whether the switch's ERPS state is in Disabled, Idle, or Protection mode.

Node Role: If the switch is the owner of the Ring Protection Link (RPL) of the ring, set this to RPL Owner. If not, set this to Ring Node. There must be one and only one RPL Owner in the ring.

Control Channel: The VLAN used as the ring's control channel. The control channel is used to transmit and receive Ring Automatic Protection Switching (R-APS) messages.

Ring Port 1: The first port connected to the ERPS ring.

Ring Port 2: The second port connected to the ERPS ring.

RPL Port: The RPL is the link that under normal circumstances blocks traffic to prevent the formation of a loop on the ring. This setting only takes effect if the switch is set to be the ring's RPL owner.

Click the **Apply** button to apply the configuration changes or click the Cancel button to cancel any modifications.

2.5.10 Command Lines

Feature	Command Line
Global	
Enable	Switch(config)# spanning-tree enable
Disable	Switch(config)# spanning-tree disable
Mode (Choose the Spanning Tree mode)	Switch(config)# spanning-tree mode rst the rapid spanning-tree protocol (802.1w) stp the spanning-tree protocol (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 forwarddelay 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)# name65korenix Region Revision: Switch(config-mst)# revision <0-65535> the value of revision Switch(config-mst)# revision 65535
Mapping Instance to VLAN (Ex: Mapping VLAN 2 to Instance 1)	Switch(config-mst)# instance <1-15> target instance number Switch(config-mst)# instance 1 vlan VLANMAP target vlan number(ex.10) or range(ex.1-10) Switch(config-mst)# instance 1 vlan 2
Display Current MST Configuration	Switch(config-mst)# show current Current MST configuration Name 65[korenix] Revision 65535 Instance Vlans Mapped -------- ---------- 0 1,4-4094 1 2 2 -- Config HMAC-MD5 Digest: 0xB41829F9030A054FB74EF7A8587FF58D ----------
Remove Region Name	Switch(config-mst)# no name name configure revision revision configure instance the mst instance Switch(config-mst)# no name
Remove Instance example	Switch(config-mst)# no instance <1-15> target instance number Switch(config-mst)# no instance 2
Show Pending MST Configuration	Switch(config-mst)# show pending Pending MST configuration Name []([->The name is removed by no name) Revision 65535 Instance Vlans Mapped -------- ---------- 0 1,3-4094 1 2 (->Instance 2 is removed by no instance -- Config HMAC-MD5 Digest: 0x3AB68794D602FDF43B21C0B37AC3BCA8 ----------
Apply the setting and go to the configuration mode	Switch(config-mst)# quit apply all mst configuration changes Switch(config)#
Apply the setting and go to the global mode	Switch(config-mst)# end apply all mst configuration changes Switch#
Abort the Setting and go to the configuration mode. Show Pending to see the new settings are not applied.	Switch(config-mst)# abort discard all mst configuration changes Switch(config)# spanning-tree mst configuration Switch(config-mst)# show pending Pending MST configuration Name 65korenix(->The nameis not applied after Abort settings.) Revision 65535 Instance Vlans Mapped -------- ---------- 0 1,4-4094

	1 2 2 3(-> The instance is not applied after Abort settings-- Config HMAC-MD5 Digest: 0xB41829F9030A054FB74EF7A8587FF58D ----------
RSTP	
The mode should be rst, the timings can be configured in global settings listed in above.	
Global Information	
Active Information	Switch# show spanning-tree active Spanning-Tree : Enabled Protocol : MSTP Root Address : 0012.77ee.eeee Priority : 32768 Root Path Cost : 0 Root Port : N/A Root Times : max-age 20, hello-time 2, forward-delay 15 Bridge Address : 0012.77ee.eeee Priority : 32768 Bridge Times : max-age 20, hello-time 2, forward-delay 15 BPDU transmission-limit : 3 Port Role State Cost Prio.Nbr Type Aggregated ------ ---------- ---------- -------- ---------- ------------ ------------ fa1 Designated Forwarding 200000 128.1 P2P(RSTP) N/A fa2 Designated Forwarding 200000 128.2 P2P(RSTP) N/A
RSTP Summary	Switch# show spanning-tree summary Switch is in rapid-stp mode. BPDU skewing detection disabled for the bridge. Backbonefast disabled for bridge. Summary of connected spanning tree ports : #Port-State Summary Blocking Listening Learning Forwarding Disabled -------- --------- -------- ---------- -------- 0 0 0 2 8 #Port Link-Type Summary AutoDetected PointToPoint SharedLink EdgePort ------------ ------------ ---------- -------- 9 0 1 9
Port Info	Switch# show spanning-tree port detail fa7 (Interface_ID) Rapid Spanning-Tree feature Enabled Port 128.6 as Disabled Role is in Disabled State Port Path Cost 200000, Port Identifier 128.6 RSTP Port Admin Link-Type is Auto, Oper Link-Type is Point-to-Point RSTP Port Admin Edge-Port is Enabled, Oper Edge-Port is Edge Designated root has priority 32768, address 0012.7700.0112 Designated bridge has priority 32768, address 0012.7760.1aec Designated Port ID is 128.6, Root Path Cost is 600000 Timers : message-age 0 sec, forward-delay 0 sec Link Aggregation Group: N/A, Type: N/A, Aggregated with: N/A BPDU: sent 43759 , received 4854 TCN : sent 0 , received 0 Forwarding-State Transmit count 12 Message-Age Expired count
MSTP Information–	
MSTP Configuraiton–	Switch# show spanning-tree mst configuration Current MST configuration (MSTP is Running)

	Name 67korenix Revision 65535 Instance Vlans Mapped -------- ------------------------------------ 0 1,4-4094 1 2 2 -- Config HMAC-MD5 Digest: 0xB41829F9030A054FB74EF7A8587FF58D ----------
Display all MST Information	Switch# show spanning-tree mst ###### MST00 vlans mapped: 1,4-4094 Bridge address 0012.77ee.eeee priority 32768 (sysid 0) Root this switch for CST and IST Configured max-age 2, hello-time 15, forward-delay 20, max-hops 20 Port Role State Cost Prio.Nbr Type ------ ---------- ---------- -------- ---------- ---------- fa1 Designated Forwarding 200000 128.1 P2P Internal(MSTP) fa2 Designated Forwarding 200000 128.2 P2P Internal(MSTP) ###### MST01 vlans mapped: 2 Bridge address 0012.77ee.eeee priority 32768 (sysid 1) Root this switch for MST01 Port Role State Cost Prio.Nbr Type ------ ---------- ---------- -------- ---------- ---------- fa1 Designated Forwarding 200000 128.1 P2P Internal(MSTP) fa2 Designated Forwarding 200000 128.2 P2P Internal(MSTP)
MSTP Root Information	Switch# show spanning-tree mst root MST Root Root Root Root Max Hello Fwd Instance Address Priority Cost Port age dly -------- -------------- -------- ----------- ------ ----- ----- ----- MST00 0012.77ee.eeee 32768 0 N/A 20 2 15 MST01 0012.77ee.eeee 32768 0 N/A 20 2 15 MST02 0012.77ee.eeee 32768 0 N/A 20 2 15
MSTP Instance Information	Switch# show spanning-tree mst 1 ###### MST01 vlans mapped: 2 Bridge address 0012.77ee.eeee priority 32768 (sysid 1) Root this switch for MST01 Port Role State Cost Prio.Nbr Type ------ ---------- ---------- -------- ---------- ---------- fa1 Designated Forwarding 200000 128.1 P2P Internal(MSTP) fa2 Designated Forwarding 200000 128.2 P2P Internal(MSTP)
MSTP Port Information	Switch# show spanning-tree mst interface fa1 Interface fastethernet1 of MST00 is Designated Forwarding Edge Port : Edge (Edge) BPDU Filter : Disabled

	Link Type : Auto (Point-to-point) BPDU Guard : Disabled Boundary : Internal(MSTP) BPDUs : sent 6352, received 0 Instance Role State Cost Prio.Nbr Vlans mapped -------- ---------- ---------- -------- ---------- ---------- 0 Designated Forwarding 200000 128.1 1,4-4094 1 Designated Forwarding 200000 128.1 2 2 Designated Forwarding 200000 128.1 3
Multiple Super Ring	
Create or configure a Ring	Switch(config)# multiple-super-ring 1 Ring 1 created Switch(config-multiple-super-ring)# ***Note: 1 is the target Ring ID which is going to be created or configured.***
Delete a Ring	Switch(config-multiple-super-ring)# delete Ring 1 delete. Switch(config)# ***Note: It will exit frommultiple-super-ring configuration mode after delete this ring.***
Enable a Ring	Switch(config-multiple-super-ring)# start Start Multiple Super Ring success
Disable a Ring	Switch(config-multiple-super-ring)# stop Stop Multiple Super Ring success.
Change Ring name	Switch(config-multiple-super-ring)# name MSR1 ***Note: Default Ring name is "Ring1",1 is the Ring ID.***
Super Ring Version	Switch(config-multiple-super-ring)# version default set default to rapid super ring rapid-super-ring rapid super ring Switch(config-multiple-super-ring)# version rapid-super-ring
Priority	Switch(config-multiple-super-ring)# priority <0-255> valid range is 0 to 255 default set default Switch(config)# super-ring priority 100
Ring Port	Switch(config-multiple-super-ring)# port IFLIST Interface list, ex: fa1,fa3-5,gi8-10 cost path cost Switch(config-multiple-super-ring)# port fa1,fa2
Ring Port Cost	Switch(config-multiple-super-ring)# port cost <0-255> valid range is 0 or 255 default set default (128)valid range is 0 or 255 Switch(config-multiple-super-ring)# port cost 100 <0-255> valid range is 0 or 255 default set default (128)valid range is 0 or 255 Switch(config-super-ring-plus)# port cost 100 200 Set path cost success.
Rapid Dual Homing	Switch(config-multiple-super-ring)# rapid-dual-homing enable Switch(config-multiple-super-ring)# rapid-dual-homing disable Switch(config-multiple-super-ring)# rapid-dual-homing port IFLIST Interface name, ex: fastethernet1 or gi8 auto-detect up link auto detection IFNAME Interface name, ex: fastethernet1 or gi8 Switch(config-multiple-super-ring)# rapid-dual-homing port fa3,fa5-6 set Rapid Dual Homing port success. Switch(config-multiple-super-ring)#rapid-dual-homing extension

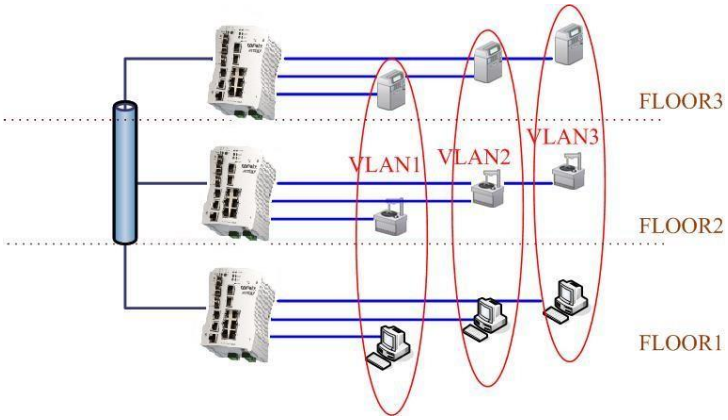
	<0-7> extension ID 0-7 (default is 0) default Note: auto-detect is recommended for dual Homing..
Super Chain	Switch(config-multiple-super-ring)# super-chain disable Switch(config-multiple-super-ring)# super-chain border Switch(config-multiple-super-ring)# super-chain member Switch(config-multiple-super-ring)# super-chain edge-port PLIST Port
Ring Info	
Ring Info	Switch# show multiple-super-ring [Ring ID] [Ring1] Ring1 Current Status : Disabled Role : Disabled Ring Status : Abnormal Ring Manager : 0000.0000.0000 Blocking Port : N/A Giga Copper : N/A Configuration : Version : Rapid Super Ring Priority 128 Ring Port : fa1, fa2 Path Cost : 128, 128 Rapid Dual Homing : Disabled Extension ID 0 Up Link : Auto Detect (N/A) Super Chain : Disabled Chain Role : N/A Chain Edge Port : N/A Statistics : Watchdog sent 0, received 0, missed 0 Link Up sent 0, received 0 Link Down sent 0, received 0 Role Transition count 0 Ring State Transition count 1 Ring ID is optional. If the ring ID is typed, this command will only display the information of the target Ring.
ERPS	
show erps	Switch# show erps Ethernet Ring Protection Switching (ITU-T G.8032) Version : v1 Ring State : Disabled Node State : Disabled Node Role : Ring Node Control Channel : VLAN 1 Ring Port 1 : fa1 is Link Down and Blocking Ring Port 2 : fa2 is Link Down and Blocking RPL Port : Ring Port 2 Timers WTR Timer : period is 1 minutes, timer is not running, remains 0 ms Guard Timer : period is 100 ms, timer is not running, remains 0 ms Statistics R-APS(SF) : sent 0, received 0 R-APS(NR,RB) : sent 0, received 0

	R-APS(NR) : sent 0, received 0 Node State Transition count 0 Switch#
ConfigureERPS	Switch(config)# erps enable Start the Multiple Super Ring for the switch disable Stop the Multiple Super Ring for the switch version the protocol version node-role The node role of ERPS node ring-port The ring port1 and port2 of the ERPS rpl The ring Ring Protection Link of the ERPS control-channel The ring control channel of the ERPS timer The period of timer Switch(config)# erps en enable Start the Multiple Super Ring for the switch Switch(config)# erps version 1 version 1 default Set default to version 1 Switch(config)# erps version 1 version 1 default Set default to version 1 Switch(config)# erps node-role rpl-owner ERPS RPL Owner ring-node ERPS ring node Switch(config)# erps ring-port PORT1 The ring port 1 Switch(config)# erps rpl ring-port Assign ring port as RPL Switch(config)# erps control-channel <1-4095> The VLAN ID of control channel, valid range is from 1 to 4094 Switch(config)# erps timer wtr-timer WTR(Wait-to-restore) Timer guard-timer Guard Timer

2.6 VLAN

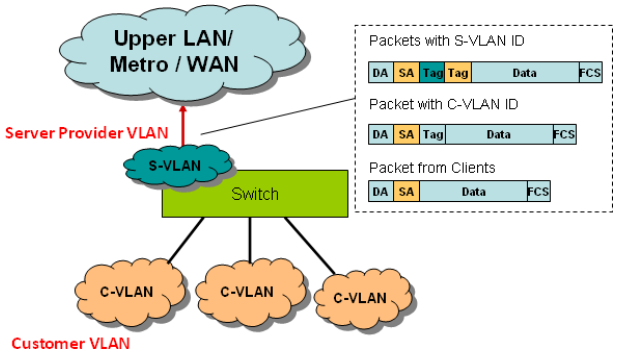
A Virtual LAN (VLAN) is a “logical” grouping of nodes for the purpose of limiting a broadcast domain to specific members of a group without physically grouping the members together. That means, VLAN allows you to isolate network traffic so that only members of VLAN could receive traffic from the same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

JetNet 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.



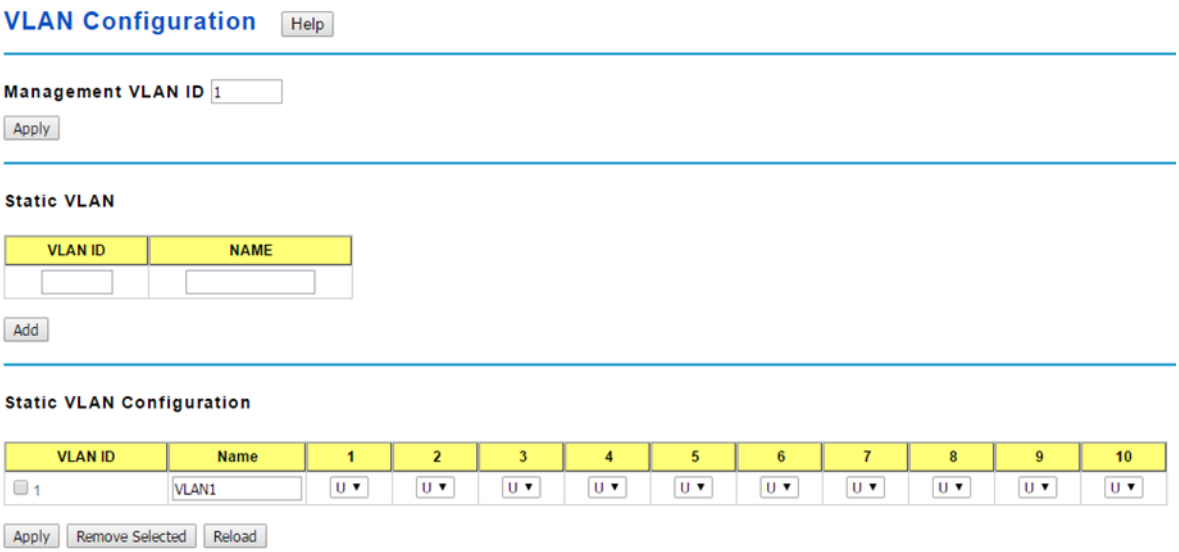
QinQ

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



2.6.1 VLAN Configuration

Use this page to assign the Management VLAN, create the static VLAN, and assign the Egress rule for the member ports of the VLAN.



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

Click **Apply** after you enter the VLAN ID.

Static VLAN

VLAN ID: This is used by the switch to identify different VLANs. A valid VLAN ID is between 1 and 4,094, 1 is the default VLAN.

Name: This is a reference for the network administrator to identify different VLANs. The VLAN name may up to 12 characters in length. If you do not provide a VLAN name, the system automatically assigns a VLAN name. The rule is VLAN (VLAN ID).

Click **Add** to create a new VLAN.

Static VLAN Configuration

VLAN ID: The VLAN identifier for this VLAN.

Name: The name of the VLAN.

Port Number: The corresponding port number on the VLAN.

- **--** Not available
- **U** Untag, indicates that egress/outgoing frames are not VLAN tagged.
- **T** Tag, indicates that egress/outgoing frames are LAN tagged.

Click **Apply** to apply the settings.

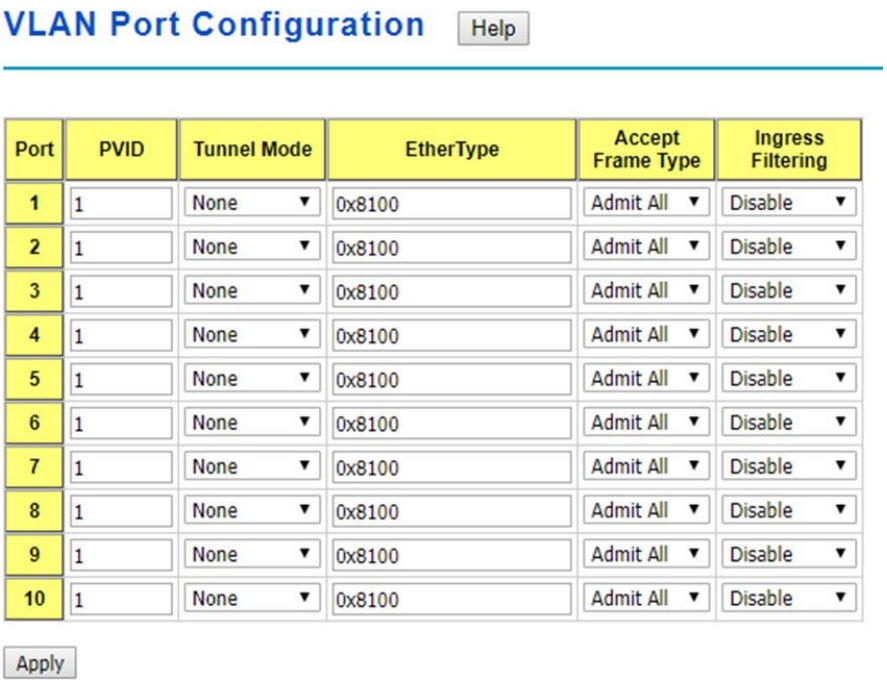
Click **Remove** Selected to remove the selected static VLAN.

Click **Reload** to reload static VLAN configuration.

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

2.6.2 VLAN Port Configuration

Tag-based VLANs are based on the IEEE 802.1Q specification. Traffic is forwarded to VLAN member ports based on identifying VLAN tags in data packets. You can also configure the switch to interoperate with existing tag-based VLAN networks and legacy non-tag networks.



PVID: Enter the port VLAN ID (PVID). The 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 default Port VID, the VLAN ID assigned to an untagged frame or a Priority-Tagged frame received on the port. The valid range is from 1 to 4094. Enter the PVID you want to configure.

Tunnel Mode:

- **None** - IEEE 802.1Q tunnel mode is disabled.
- **802.1Q Tunnel** - QinQ is applied to the ports which connect to the C-VLAN. The port receives a tagged frame from the C-VLAN. You need to add a new tag (Port VID) as an S-VLAN VID. When the packets are forwarded to the 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 that the egress packet is always untagged. This is configured in the Static VLAN Configuration table.

- **802.1Q Tunnel Uplink** - QinQ is applied to the ports which connect to the S-VLAN. The port receives a tagged frame from the S-VLAN. When the packets are forwarded to the 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 that the egress packet is always tagged. This is configured in the Static VLAN Configuration table. For example, if 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 CVLAN and adds Tag 10 to the packet. When the packets are forwarded to S-VLAN, Tag 10 is kept.

EtherType: This allows you to define the EtherType manually. This is an advanced QinQ parameter that allows defining the transmission packet type.

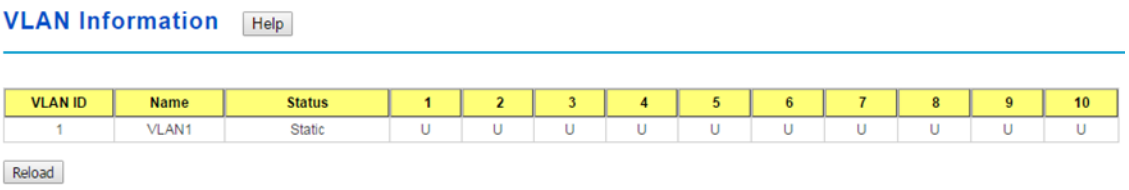
Accept Frame Type: This column defines the accepted frame type of the port. There are 2 modes you can select, **Admit All** and **Tag Only**.
Admit All mode means that the port can accept both tagged and untagged packets. **Tag Only** mode means that the port can only accept tagged packets.

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.

Click **Apply** to apply the settings.

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

2.6.3 VLAN Information

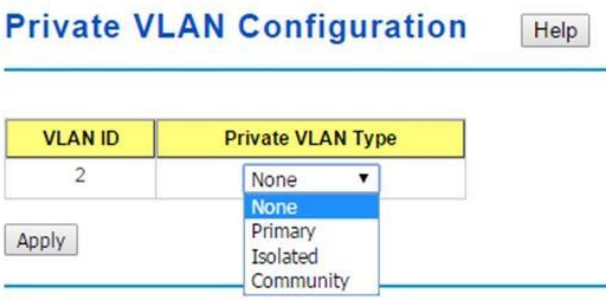


The VLAN Information page displays the current settings of your VLAN table, including VLAN ID, Name, Status, and Egress rule of the ports.

2.6.4 PVLAN Configuration

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.

Note: You must have previously configured a VLAN in the VLAN Configuration screen.



VLAN ID:

- **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 cannot.

Private VLAN Type:

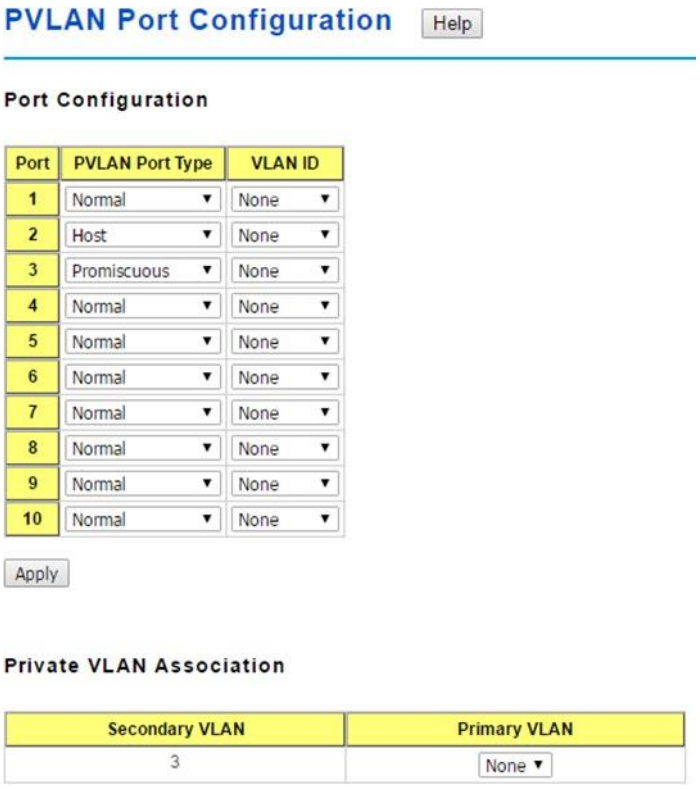
- **None**: The VLAN is not included in the Private VLAN.
- **Primary**: The VLAN is the Primary VLAN. The member ports can communicate withthe secondary VLANs
- **Isolated**: The member ports of the VLAN are isolated.
- **Community**: The member ports of the VLAN can communicate with each other.

Click **Apply** to apply the settings.

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

2.6.5 PVLAN Port Configuration

The PVLAN Port Configuration page allows you to configure the port configuration and private VLAN associations.



Port Configuration

PVLAN Port Type:
Normal: Normal ports remain in their original VLAN configuration.
Host: Host ports can be mapped to the secondary VLAN.
Promiscuous: Promiscuous ports can be associated to the primary VLAN.

VLAN ID: After assigning the port type, this displays the available VLAN ID for which the port can associate.

Click **Apply** to apply the settings.

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

Private VLAN Association

Secondary VLAN: After the isolated and community VLANs are configured in the Private VLAN Configuration page, the VLANs belonging to the second VLAN are displayed.

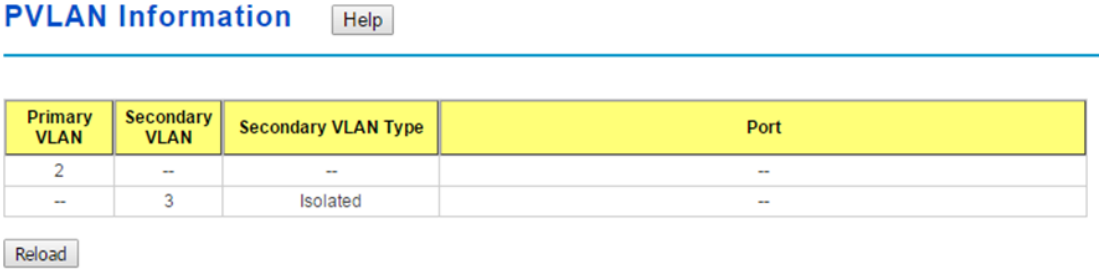
Primary VLAN: After the Primary VLAN Type is assigned in Private VLAN Configuration page, the secondary VLAN can associate to the primary VLAN ID.

Note: Before configuring PVLAN port type, the private VLAN Association

2.6.6 PVLAN Information

The PVLAN Information page allows you to see the private VLAN information.

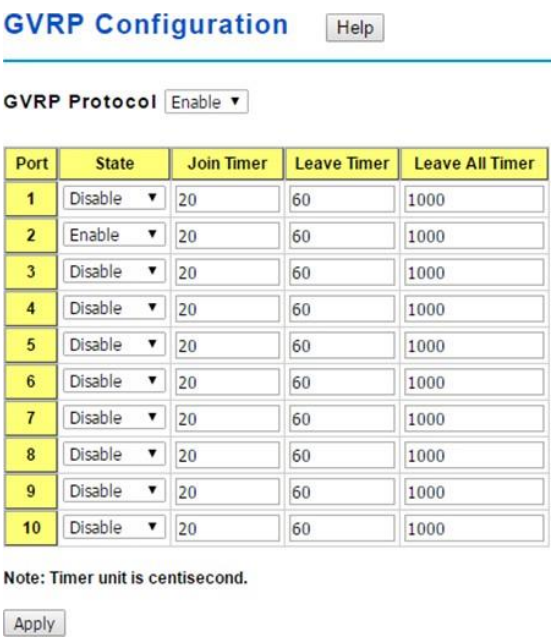
Click **Reload** to refresh the page contents.



2.6.7 GVRP Configuration

GARP VLAN Registration Protocol (GVRP) allows you to set-up VLANs automatically rather than manual configuration on every port on every switch in the network. GVRP conforms to the IEEE 802.1Q specification.This defines a method of tagging frames with VLAN configuration data that allows network devices to dynamically exchange VLAN configuration information with other devices.

GARP (Generic Attribute Registration Protocol), a protocol that defines procedures by which end stations and switches in a local area network (LAN) can register and de-register attributes, such as identifiers or addresses, with each other. Every end station and switch thus has a current record of all the other end stations and switches that can be reached. GVRP, like GARP, eliminates unnecessary network traffic by preventing attempts to transmit information to unregistered users. In addition, it is necessary to manually configure only one switch and all the other switches are configured accordingly.



GVRP Protocol: **Enable**/**Disable** GVRP globally.

State: After enabling GVRP globally, you can still **Enable**/**Disable** GVRP by port.

Join Timer: Controls the interval of sending the GVRP Join BPDU (Bridge Protocol Data Unit). 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

Click **Apply** to apply the settings.

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

2.6.8 CLI Commands of the VLAN

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

Feature	Command Line
VLAN Port Configuration	
Port Interface Configuration	Switch# conf ter Switch(config)# interface gi5 Switch(config-if)#
VLAN Port PVID	Switch(config-if)# switchport trunk native vlan 2 Set port default vlan id to 2 success
QinQ Tunnel Mode	Switch(config-if)# switchport dot1q-tunnel mode Set the interface as an IEEE 802.1Q tunnel mode

802.1Q Tunnel = access 802.1Q Tunnel Uplink = uplink	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 gi1 Switch(config-if)# acceptable frame type all any kind of frame type is accepted! Switch(config-if)# acceptable frame type vlantaggedonly only vlan-tag frame is accepted!
Egress rule – Untagged (for VLAN 2)	Switch(config-if)# switchport access vlan 2 switchport access vlan add success
Egress rule – Tagged (for VLAN 2)	Switch(config-if)# switchport trunk allowed vlan add 2
Display – Port Ingress Rule (PVID, Ingress Filtering, Acceptable Frame Type)	Switch# show interface gi1 Interface gigabitethernet1 Description : N/A Administrative Status : Enable Operating Status : Not Connected Duplex : Auto Speed : Auto MTU : 1518 Flow Control :off Default Port VLAN ID: 2 Acceptable Frame Type : Vlan Tagged Only Auto Negotiation : Enable Loopback Mode : None STP Status: disabled Default CoS Value for untagged packets is 0. Medium mode is Copper.
Display – Port Egress Rule (Egress rule, IP address, status)	Switch# show running-config …… ! interface gigabitethernet1 acceptable frame type vlantaggedonly switchport access vlan 1 switchport access vlan 3 switchport trunk native vlan 2 ……. interface vlan1 ip address 192.168.10.8/24 no shutdown
QinQ Information – 802.1Q Tunnel	Switch# show dot1q-tunnel Port Mode Ethertype ---- ------ --------- 1 normal 0x8100 2 normal 0x8100 3 normal 0x8100 4 normal 0x8100 5 access 0x8100 6 uplink 0x8100 7 normal 0x8100 8 normal 0x8100 9 normal 0x8100 10 normal 0x8100
QinQ Information –	Switch# show running-config

Show Running	Building configuration... Current configuration: hostname Switch vlan learning independent …… …… interface gigabitethernet5 switchport access vlan add 1-2,10 switchport dot1q-tunnel mode access ! interface gigabitethernet6 switchport access vlan add 1-2 switchport trunk allowed vlan add 10 switchport dot1q-tunnel mode uplink !
VLAN Configuration	
Create VLAN (2)	Switch(config)# vlan 2 vlan 2 success Switch(config)# interface vlan 2 Switch(config-if)# *Note: In CLI configuration, you should create a VLAN interface first. Then you can start to add/remove ports. Default status of the created VLAN is unused until you add member ports to it.*
Remove VLAN	Switch(config)# no vlan 2 no vlan success *Note: You can only remove the VLAN when the VLAN is in unused mode.*
VLAN Name	Switch(config)# vlan 2 vlan 2 has exists Switch(config-vlan)# name v2 Switch(config-vlan)# no name *Note: Use no name to change the name to default name, VLAN VID.*
VLAN description	Switch(config)# interface vlan 2 Switch(config-if)# Switch(config-if)# description this is the VLAN 2 Switch(config-if)# no description ->Delete the description.
IP address of the VLAN	Switch(config)# interface vlan 2 Switch(config-if)# Switch(config-if)# ip address 192.168.10.18/24 Switch(config-if)# no ip address 192.168.10.8/24 ->Delete the IP address
Shut down VLAN	Switch(config)# interface vlan 2 Switch(config-if)# shutdown Switch(config-if)# no shutdown ->Turn on the VLAN
Display – VLAN table	Switch# sh vlan VLAN Name Status Trunk Ports Access

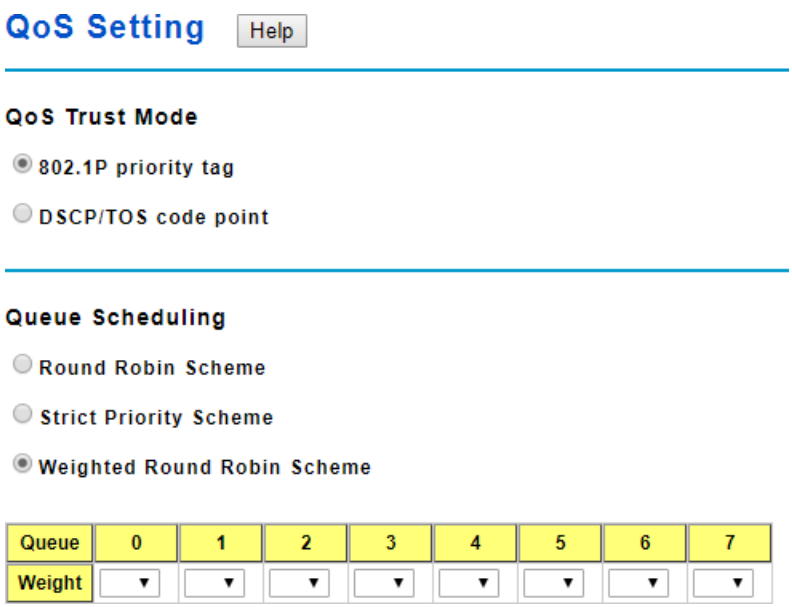
	Ports ---- ---------- ------- -------------------------- ------------------ --------- 1 VLAN1 Static - gi1-7,gi8-10 2 VLAN2 Unused - - 3 test Static gi4-7,gi8-10 gi1-3,gi7,gi8-10
Display – VLAN interface information	Switch# show interface vlan1 Interface vlan1 Description : N/A Administrative Status : Enable Operating Status : Up DHCP Client : Disable Primary IP Address : 192.168.10.1/24 IPv6 Address : fe80::212:77ff:feff:2222/64
GVRP configuration	
GVRP enable/disable	Switch(config)# gvrp mode disable Disable GVRP feature globally on the switch enable Enable GVRP feature globally on the switch Switch(config)# gvrp mode enable Gvrp is enabled on the switch!
Configure GVRP timer Join timer /Leave timer/ LeaveAll timer	Switch(config)# inter gi1 Switch(config-if)# garp join-timer <10-10000>the timer values Switch(config-if)# garp join-timer 20 Garp join timer value is set to 20 centiseconds on port 1!
Management VLAN	
Management VLAN	Switch(config)# int vlan 1 (Go to management VLAN) Switch(config-if)# no shutdown
Display	Switch# show running-config …. ! interface vlan1 ip address 192.168.10.17/24 ip igmp no shutdown ! ….

2.7 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.

2.7.1 QoS Setting



QoS Trust Mode

802.1P Priority Tag: If 802.1P is selected the switch relies on a packet's CoS information to determine priority. This is related to the settings in the CoS-Queue Mapping page

DSCP/TOS Code Point: If DSCP/TOS is selected the switch relies on a packets differentiated services code point information to determine the priority. This is related to the settings in the DSCP-Priority Mapping page.

Queue Scheduling

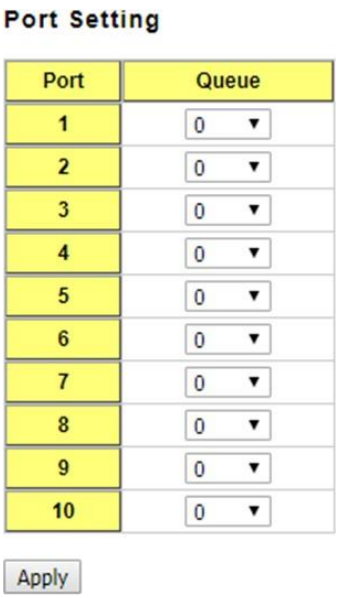
You can select the Queue Scheduling rule as follows:

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

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)



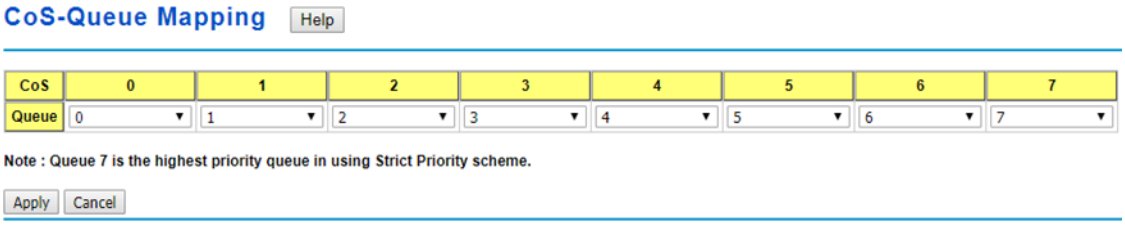
Choose the Queue value of each port, the port then has its default priority. The Queue 7 is the highest port-based queue, 0 is the lowest queue. The traffic injected to the port follows the queue level to be forwarded, but the outgoing traffic does not bring the queue level to next switch.

Click the **Apply** button to apply the configuration changes.

2.7.2 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.

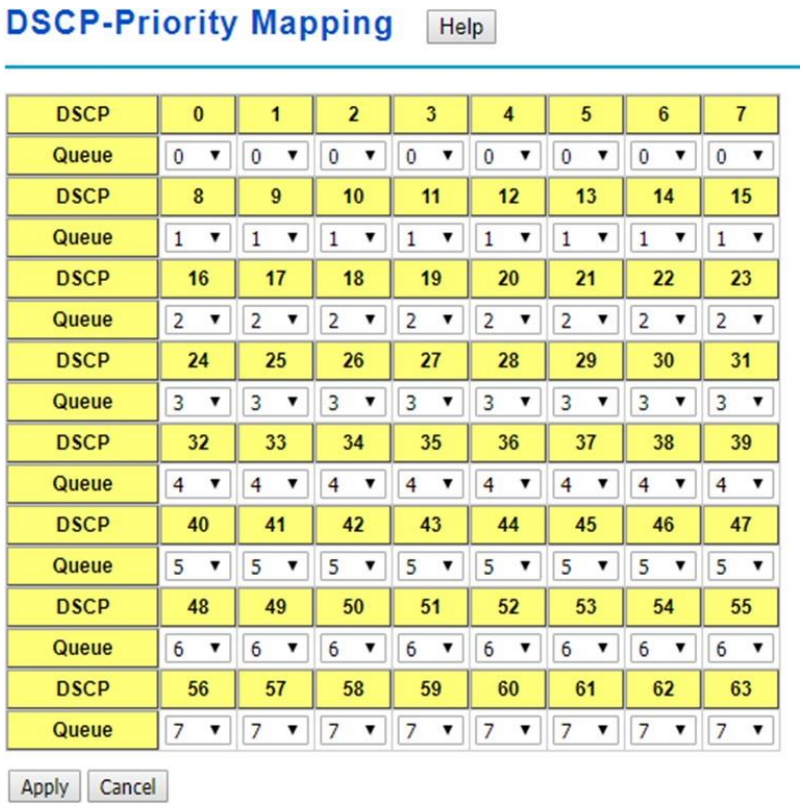


Click **Apply** to apply the setting.

Click **Cancel** to clear the modification.

2.7.3 DSCP-Priority Mapping

This page is to change DSCP values to Priority mapping table. The system provides 0~63 DSCP priority level. Each level can map to one priority ID



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

2.7.4 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 Scheduli–g - WRR	Switch(config)# qos queue-sched wrr <1-10> Weights for COS queue 0 (queue_id 0) Switch(config)# qos queue-sched wrr 10 <1-10> Weights for COS queue 1 (queue_id 1) …….. Switch(config)# qos queue-sched wrr 1 2 3 4 5 6 7 8 The queue scheduling scheme is setting to Weighted Round Robin. ***Assign the ratio for the 8 classes of service.***
Port Setting – CoS (Default Port Priority)	Switch(config)# interface **gi1** Switch(config-if)# qos priority <0-7> Assign a priority queue Switch(config-if)# qos priority 3 The priority queue is set 3 ok. ***Note: When change the port setting, you should Select the specific port first. Ex: gi1 means Gigabit Ethernet port 1.***
QoS Trust Mode	Switch(config)# qos trust-mode cos CoS dscp DSCP/TOS Switch(config)# qos trust-mode dscp Set QoS trust mode dscp ok Switch# show trust-mode QoS Trust Mode: DSCP/TOS code point
Displ–y - Queue Scheduling	Switch# show qos queue-sched QoS queue scheduling scheme : Weighted Round Robin COS queue 0 = 1 COS queue 1 = 2 COS queue 2 = 3 COS queue 3 = 4 COS queue 4 = 5 COS queue 5 = 6 COS queue 6 = 7 COS queue 7 = 8
Display – Port Priority Setting (Port Default Priority)	Switch# show qos port-priority Port Default Priority : Port Priority Queue -----+---- 1 7

	2 0 3 0 4 0 …….. 26 0 27 0 28 0
CoS-Queue Mapping	
Format	Switch(config)# qos cos-map PRIORITY Assign an priority (7 highest) Switch(config)# qos cos-map 1 QUEUE Assign an queue (0-7) ***Note: Format: qos cos-map priority_value queue_value***
Map CoS 0 to Queue 1	Switch(config)# qos cos-map 0 1 The CoS to queue mapping is set ok.
Map CoS 1 to Queue 0	Switch(config)# qos cos-map 1 0 The CoS to queue mapping is set ok.
Map CoS 2 to Queue 0	Switch(config)# qos cos-map 2 0 The CoS to queue mapping is set ok.
Map CoS 3 to Queue 1	Switch(config)# qos cos-map 3 1 The CoS to queue mapping is set ok.
Map CoS 4 to Queue 2	Switch(config)# qos cos-map 4 2 The CoS to queue mapping is set ok.
Map CoS 5 to Queue 2	Switch(config)# qos cos-map 5 2 The CoS to queue mapping is set ok.
Map CoS 6 to Queue 3	Switch(config)# qos cos-map 6 3 The CoS to queue mapping is set ok.
Map CoS 7 to Queue 3	Switch(config)# qos cos-map 7 3 The CoS to queue mapping is set ok.
Display – CoS-Queue mapping	Switch# sh qos cos-map CoS to Queue Mapping : CoS Queue ---- + ------ 0 1 1 0 2 0 3 1 4 2 5 2 6 3 7 3
DSCP-PriorityMapping	
Format	Switch(config)# qos dscp-map DSCP DSCP code point in binary format (000000-111111) Switch(config)# qos dscp-map 0 PRIORITY 802.1p priority bit (0-7) ***Format: qos dscp-map priority_value queue_value***
Map DSCP 0 to Queue 1	Switch(config)# qos dscp-map 0 1 The TOS/DSCP to queue mapping is set ok.
Display – DSCO-Queue mapping	Switch# show qos dscp-map DSCP to Queue Mapping : (dscp = d1 d2)

	d2| 0 1 2 3 4 5 6 7 8 9 d1 | -----+---------- 0 | 1 0 0 0 0 0 0 0 1 1 1 | 1 1 1 1 1 1 2 2 2 2 2 | 2 2 2 2 3 3 3 3 3 3 3 | 3 3 4 4 4 4 4 4 4 4 4 | 5 5 5 5 5 5 5 5 6 6 5 | 6 6 6 6 6 6 7 7 7 7 6 | 7 7 7 7

2.8 Multicast Filtering

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

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

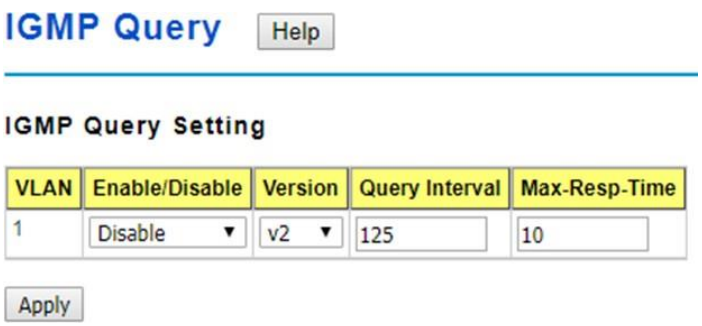
In effect, IGMP Snooping manages multicast traffic by making use of switches, routers, and hosts that support IGMP. Enabling IGMP Snooping allows the ports to detect IGMP queries, report packets, and manage multicast traffic through the switch. IGMP has three fundamental types of messages, as shown below:

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

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

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

2.8.1 IGMP Query



Enable/Disable: Select **Enable** or **Disable**.

Version: 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.

Query Interval(s): The period of query (seconds) sent by querier. Enter a number between 1and 65,535.

Max-Resp-Time(s): This option is available when you select Version 2. The span querier detect(seconds) to confirm there are no more directly connected group members ona LAN. Enter a number between 1 and 25.

Click **Apply** to apply the settings.

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

2.8.2 IGMP Snooping/Filtering

This page is to enable IGMP Snooping feature, assign IGMP Snooping for specific VLAN, and view the IGMP Snooping Table from a dynamic learnt or static that you provide.



IGMP Snooping Global Setting

Select **Enable**/**Disable** IGMP Snooping. After enabling IGMP Snooping, you can then enable IGMP Snooping for specific VLAN using the IGMP Snooping VLAN Setting table.

IGMP Snooping VLAN Setting

VLAN: Refers to the VLAN number that was configured using the VLAN Configuration page.

IGMP Snooping: Select **Enable** to start IGMP snooping on the selected VLAN.
Filtering Mode: This setting determines how unknown multicast packets are handled. If the setting is broadcast unknown, any unknown multicast packets received by the switch are broadcast to each port on the VLAN. If the setting is Source Only Learning, any unknown multicast packets received by the switch will be sent to multicast source ports and multicast router ports. If it the setting is drop unknown, any unknown multicast packets will be discarded.

- **Flood Unknown**: The unknown multicast is broadcast to all ports even if they are not member ports of the groups.
- **Discard Unknown**: The unknown multicast is discarded. Non-member ports do not receive the unknown multicast streams.
- **Source Only Learning**: This is forwarding unknown multicast traffic to all ports that are already members of a multicast group.

Click **Apply** to apply the settings.

Note: Always remember to go to **Save** page to save the settings. Otherwise, the settings

you made will be lost when the switch is powered off.

IGMP Snooping Table

This table shows the IGMP groups the switch is aware of.

Multicast Address: The multicast group's IP address.

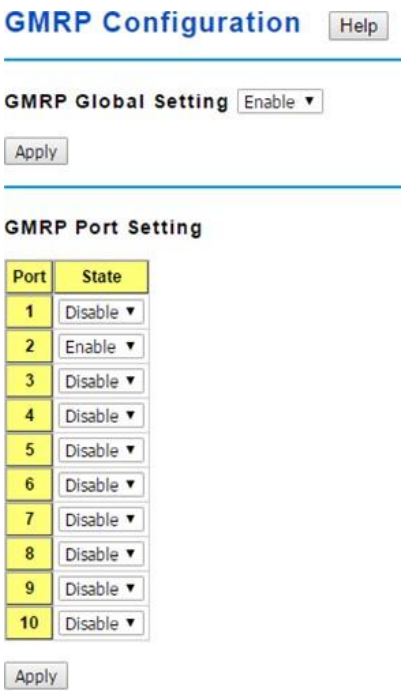
VLAN ID: The VLAN ID the multicast group is a member of.

Interface: The port the multicast group is a member of.

Click on **Reload** to reload the information.

2.8.3 GMRP Configuration

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



GMRP Global Setting

Select **Enable** or **Disable** GMRP protocol.

Click **Apply** to apply the settings.

GMRP Port Setting

State: The state of the GMRP operation on a selected port.

Click **Apply** to apply the settings.

2.8.4 CLI Commands of the Multicast Filtering

Command Lines of the multicast filtering configuration

Feature	Command Line
IGMP Snooping	
IGMP Snooping - Global	Switch(config)# ip igmp snooping IGMP snooping is enabled globally. Please specify on which vlans IGMP snooping enables Switch(config)# ip igmp snooping<?> immediate-leave leave group when receive a leave message last-member-query-interval the interval for which the switch waits before updating the table entry source-only-learning Source-Only-Learning vlan Virtual LAN
IGMP Snooping - VLAN	Switch(config)# ip igmp snooping vlan VLANLIST allowed vlan list all all existed vlan Switch(config)# ip igmp snooping vlan 1-2 IGMP snooping is enabled on vlan 1 IGMP snooping is enabled on vlan 2
Disable IGMP Snooping – Global	Switch(config)# no ip igmp snoopin IGMP snooping is disabled globally ok.
Disable IGMP Snooping - VLAN	Switch(config)# no ip igmp snooping vlan 3 IGMP snooping is disabled on VLAN 3.
Display – IGMP Snooping Setting	Switch# sh ip igmp interface vlan1 enabled: Yes version: IGMPv1 query-interval; 125s query-max-response-time: 10s Switch# sh ip igmp snooping IGMP snooping is globally enabled Vlan1 is IGMP snooping enabled immediate-leave is disabled last-member-query-interval is 100 centiseconds Vlan2 is IGMP snooping enabled immediate-leave is disabled last-member-query-interval is 100 centiseconds Vlan3 is IGMP snooping disabled immediate-leave is disabled last-member-query-interval is 100 centiseconds
Display – IGMP Table	Switch# sh ip igmp snooping multicast all VLAN IP Address Type Ports ---- --------------- ------- ---------- 1 239.192.8.0 IGMP fa6, 1 239.255.255.250 IGMP fa6,
IGMP Query	
IGMP Query V1	Switch(config)# int vlan 1 (Go to management VLAN) Switch(config-if)# ip igmp v1
IGMP Query V2	Switch(config)# int vlan 1 (Go to management VLAN) Switch(config-if)# ip igmp
IGMP Query version	Switch(config-if)# ip igmp version 1

	Switch(config-if)# ip igmp version 2
Disable	Switch(config)# int vlan 1 Switch(config-if)# no ip igmp
Display	Switch# sh ip igmp interface vlan1 enabled: Yes version: IGMPv2 query-interval: 125s query-max-response-time: 10s Switch# show running-config …. ! interface vlan1 ip address 192.168.10.17/24 ip igmp no shutdown ! …….
Unknown Multicast	
Send to Query Ports–	Switch(config)# ip igmp snooping source-only-learning vlan VLANLIST allowed VLAN list all all VLAN Switch(config)# ip igmp snooping source-only-learning vlan 1 IGMP Snooping Source-Only-Learning is enabled on VLAN 1
Discard (Force filtering)	Switch(config)# mac-address-table multicast filtering vlan VLANLIST allowed VLAN list all all VLAN Switch(config)# mac-address-table multicast filtering vlan 2
Send to All Ports (Flood to all VLAN member ports)	Switch(config)# no mac-address-table multicast filtering vlan VLANLIST allowed VLAN list all all VLAN Switch(config)# no mac-address-table multicast filtering vlan 1

2.9 Routing (Layer3 Managed Switch only)

Layer 3 Routing Feature is the most important feature of the the Layer 3Managed 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.

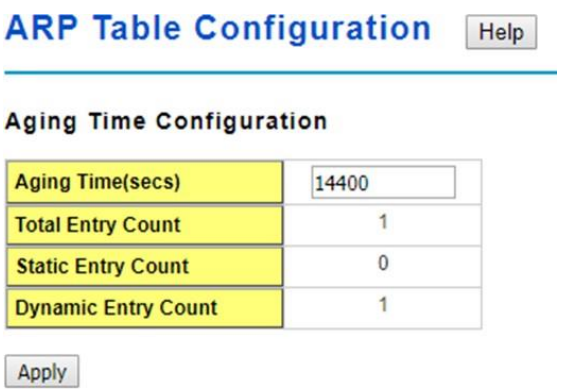
The JetNet Layer 3 Switch equips with a Layer 3 chipset which can perform wire-speed layer 3 routing performance. The JetNet Switch combines Layer 2 switching and Layer 3 routing within the single platform. In the Routing Configuration pages allows users create the Routing Interfaces, enable routing capability, enable unicast/multicast routing protocols, configure router redundancy policy and check the related routing information.

2.9.1 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.

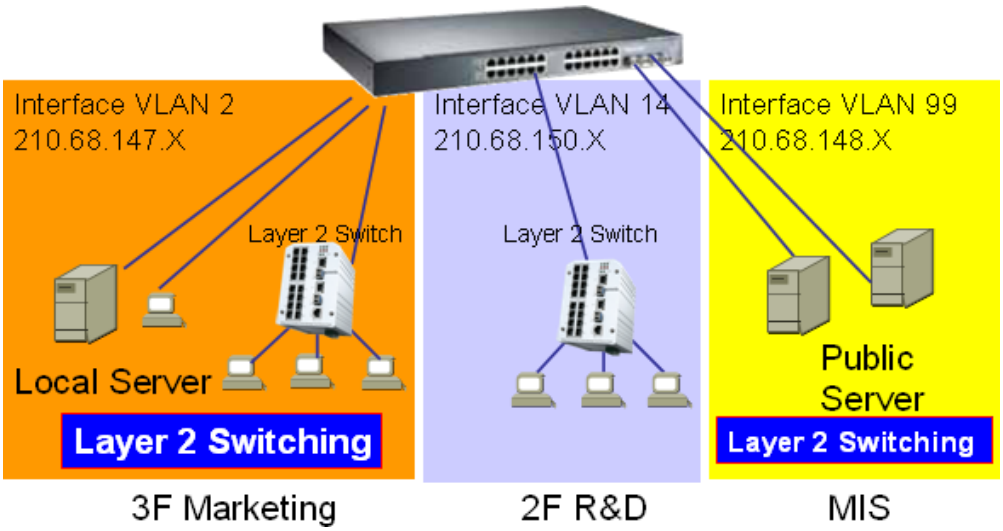
Dynamic Entry Count: This count represents for the count the ARP table dynamically learnt.

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

2.9.2 IP

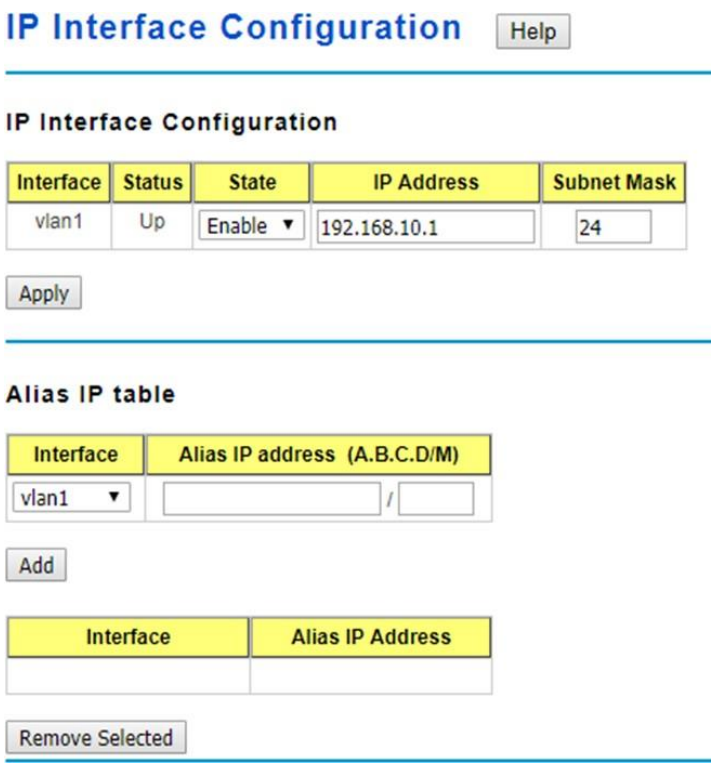
An IP Interface is the basic unit while routing, it is a logical interface which equips with an IP network and acts as the default gateway of the attached clients. The network interface can be a port or a single VLAN. All the client members connected to the IP network can be routed through the network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



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.



IP Interface Configuration

Interface: The name of the IP interface.

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 IP Interface.

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.

Click the **Apply** button to apply IP interface settings.

Alias IP table

Interface: The selected interface.

Alias IP Address (A.B.C.D/M): The alias IP and its subnet mask.

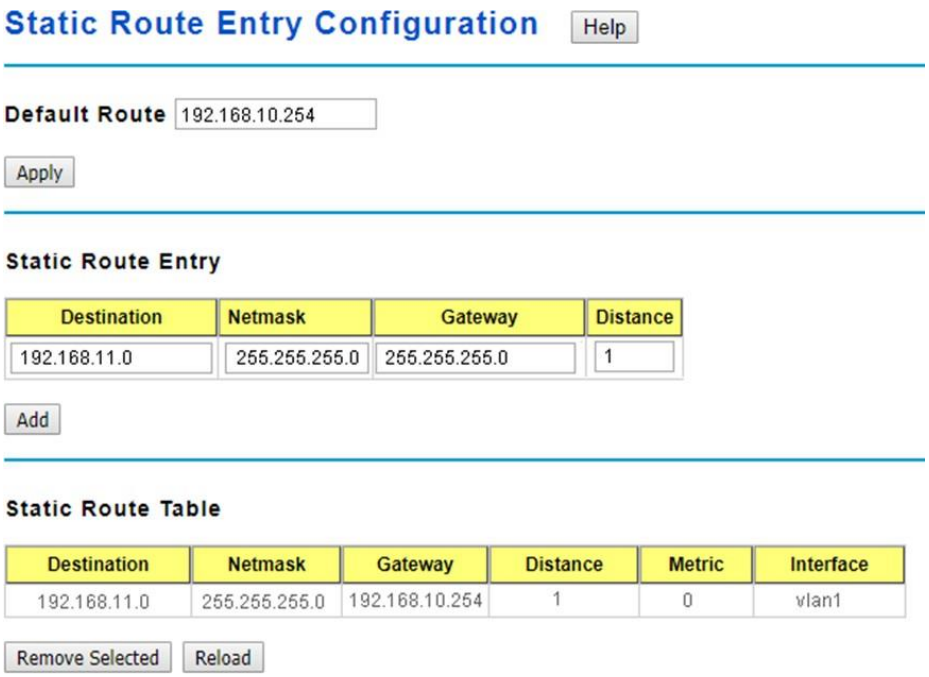
Click the **Add** button to add an alias IP address for the selected interface.

Click the **Remove Selected** button to remove the selected alias IP address of an interface.

2.9.3 Router

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

2.9.3.1 Static 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 Entry

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.

- **Destination**: The destination address of static route entry.
- **Netmask**: The destination address netmask of static route entry.
- **Gateway**: The gateway IP address of static route entry.
- **Distance**: The distance of static route entry.

Click the **Add** button to add a static route entry.

Static Route Table

This table displays the routing table information

Destination: The destination address of static route entry.

Netmask: The destination address netmask of static route entry.

Gateway: The gateway IP address of static route entry.

Distance: The distance of static route entry.

Metric: The metric of static route entry.

Interface: The IP interface of static route entry via.

Click the **Remove Selected** button to remove selected route entry.

Click the **Reload** button to reload Route Entry information.

2.9.3.2 Route Table

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.



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.

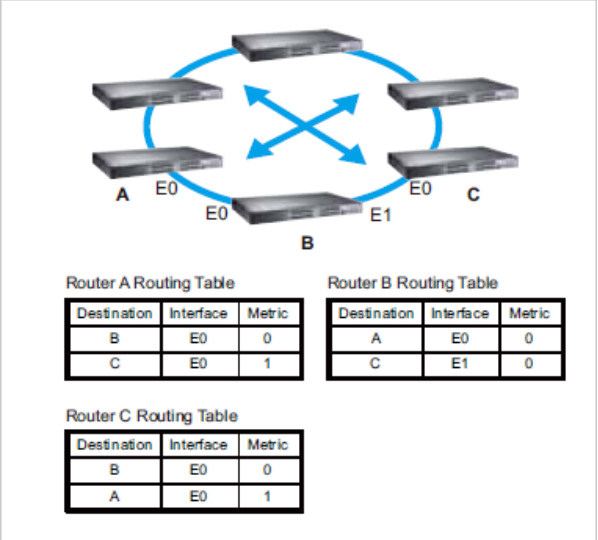
2.9.4 RIP

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.

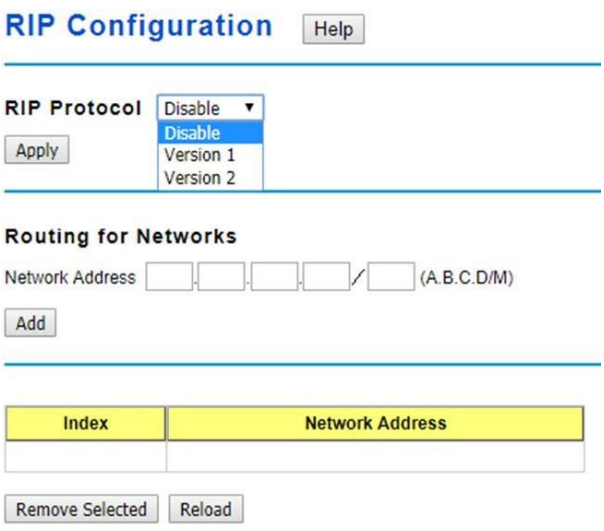
When a router receives a neighbor's table, it examines it entry by entry. If the destination is new, it is added to the local routing table. If the destination is known before and the update provides a smaller metric, the existing entry in the local routing table is replaced. Adds 1 (or sometimes more 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.



2.9.4.1 RIP Configuration

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.



RIP Protocol: Choose the RIP **Version 1** or **Version 2** or **Disable** RIP protocol in here.
Click the **Apply** button to apply RIP protocol setting.

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 the "Add" to add a routing network.
Click the **Add** button to add a routing network.
Click the **Remove Selected**button to remove selected network address.
Click the **Reload** button to reload RIP information.

2.9.4.2 RIP Interface Configuration

In RIP Interface Configuration, you can configure RIP version.

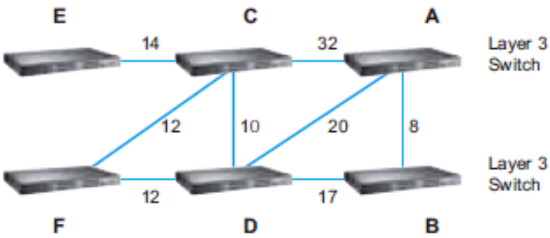


Interface: The IP interface.
RIP Version: RIP version of IP interface.
Click the **Apply** button to apply RIP interface settings.
Click the **Reload** button to reload RIP interface configuration.

2.9.5 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 asbelow is the example OSPF network.



Router A Routing Table

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

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.

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

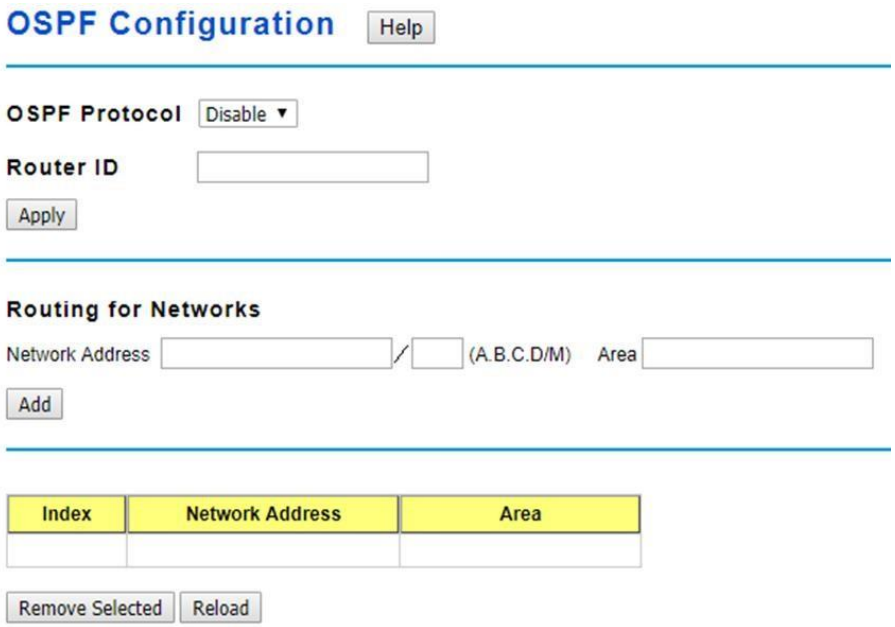
However, in link-state protocol, like the OSFP, the A to D to C is the shortest way. This is calculated by the *Dijkstra’s SPF Algorithm.* After calculated and routing table updated, the metric from A to C is 32, the metric from A to D to C is 30. The A to D to C will be selected as the beast route from 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 Layer3 Managed Switch design comforts to the OSPF Version 2 specification. Typically, the switch 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.

2.9.5.1 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.

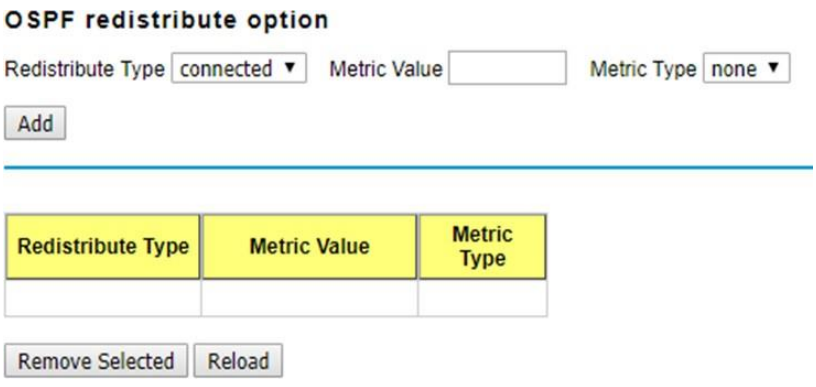
Router ID: The router ID can be any IP address, however, the IP address of the existed local interface is suggested. With such IP address, you can find the router/switch easier. Router ID is used while connected multiple OSPF routers/switches to the same broadcast domain, the lowest Router ID will be 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.

Click the **Remove** Selected button to remove the selected network.

Click the **Reload** button to reload this page.



Add a redistribute type to OSPF and assign the metric value/type of it.

Click the **Add** button to add a redistribute option.

Redistribute Type: The type of routing entries for redistributing: connected, static or RIP.

Metric Value: The default routing metric of the redistribute type (0 to 16777214).

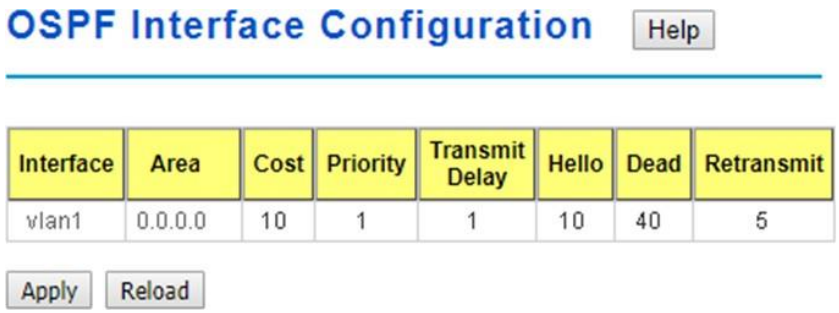
Metric Type: OSPF exterior metric type of the redistribute type: none, 1 or 2.

Click the **Remove Selected** button to remove the selected redistribute type.

Click the **Reload** button to reload this page.

2.9.5.2 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.

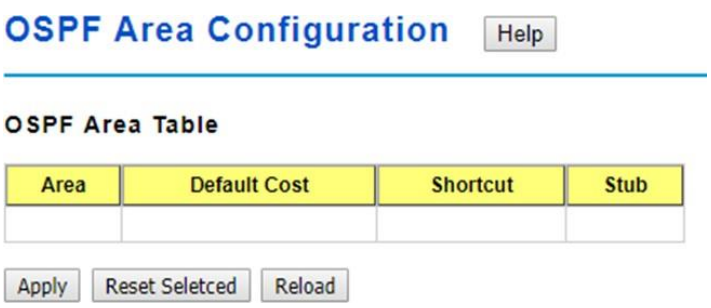
Once you finish configuring the settings, click on **Apply** to apply your configuration.

2.9.5.3 OSPF Area Configuration

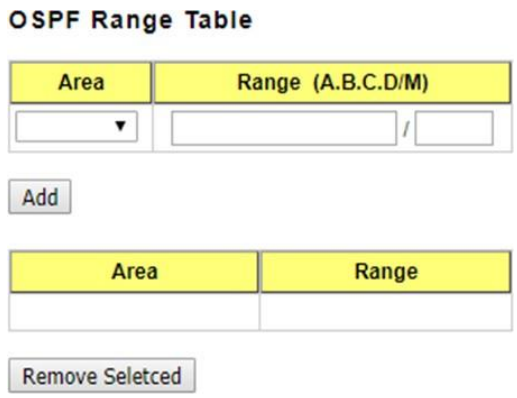
This page allows user to configure the OSPF Area information.

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.

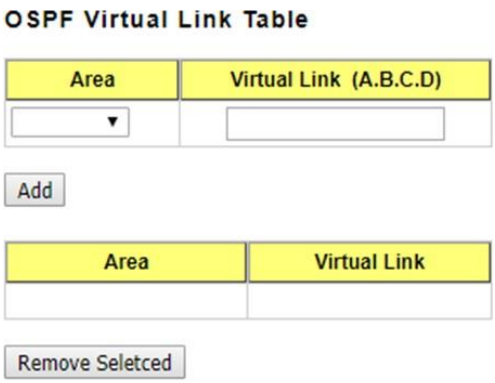
The JetNet Switch is usually installed as internal router of a single Area environment. While there are multiple areas in the network, this page allows modify the Area information and Virtual Link.



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.
Click the **Apply** button to apply OSPF area settings.
Click the **Remove Selected**button to remove selected area.
Click the **Reload** button to reload OSPF area configurations.



Range (A.B.C.D/M): Summarize routes matching address/mask (border routers only).
Click the **Add** button to add a range for the selected area.
Click the **Remove Selected** button to remove selected range of selected area.



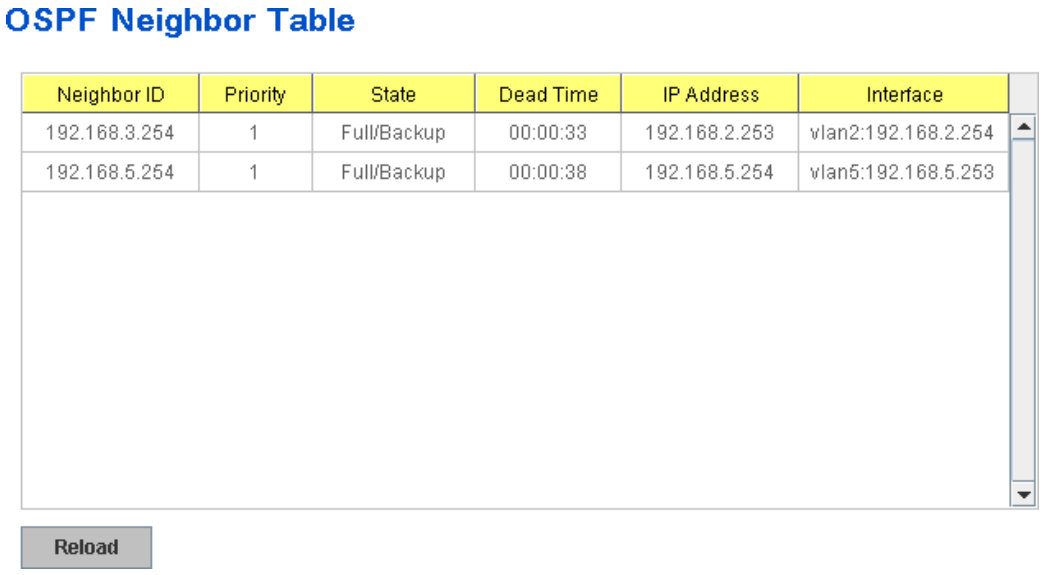
Virtual Link (A.B.C.D.): You can configure the virtual link. One area must be common area between two endpoint routers to create virtual links.

Click the **Add** button to add a virtual link for the selected area.

Click the **Remove Selected** button to remove selected virtual link of selected area.

2.9.5.4 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.

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.

2.9.5.5 OSPF Information Database

The page display the OSPF Information Database, click on **Reload** to update the information.

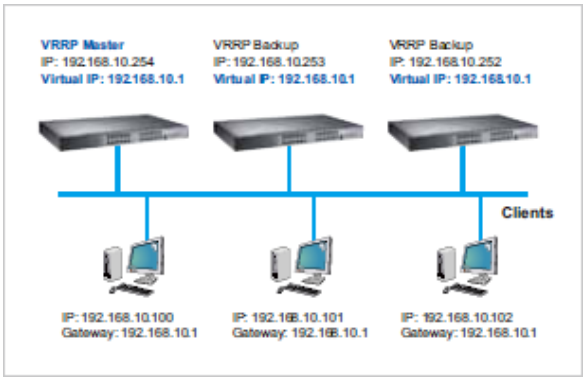
2.9.6 VRRP Configuration

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.

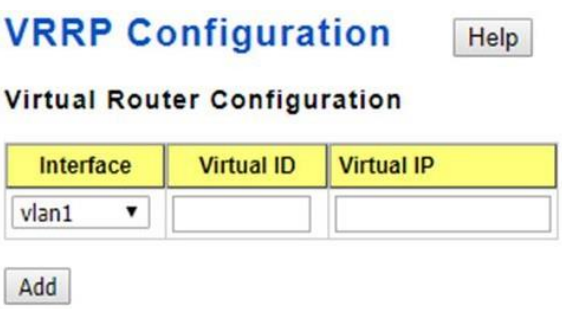
The figure for example, there are 3 VRRP-aware switches with the same Virtual IP of the VRRP, but different IP address of their VLAN/IP interface.

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.



2.9.6.1 VRRP Configuration

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.

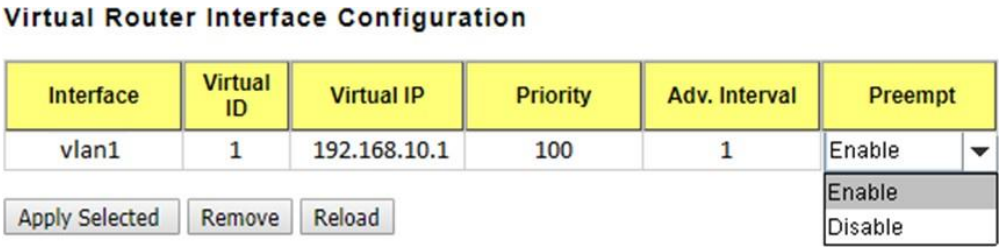


Interface: Select the interface for the VRRP domain.

VirtualID: 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



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.

VirtualID: 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.

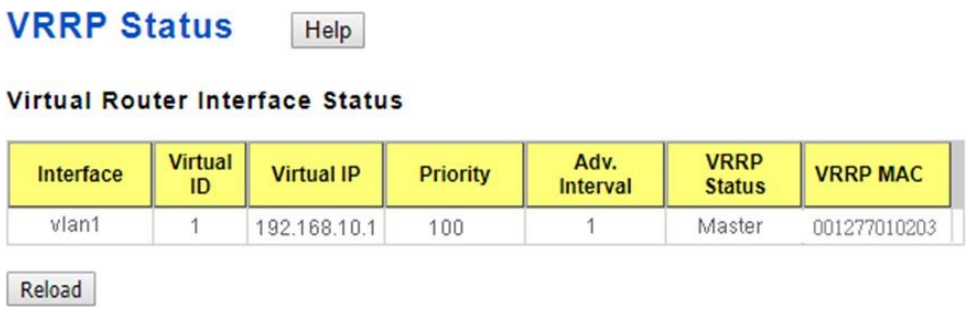
While the Preempt is **Enable**and the interface is VRRP Master, the interface will be recovered.

While the Preempt is **Disable** 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 Selected"** to change the setting. **"Remove"** to remove the entry. **"Reload"** to reload the new entry and settings.

2.9.6.2 VRRP Router Status

The VRRP represent for the Virtual Router Redundancy Protocol. To further ensure the high reliability of an environment, the Layer 3 switch supports the VRRP protocol allowing the hosts to continuously direct traffic to the default gateway without the default gateway configuration change.



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.

VRRP Status: While the VRRP Master link is failure, the VRRP Backup will take over its job immediately

VRRP MAC: This field indicates the VRRP MAC in this configuration entry.

2.9.7 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.

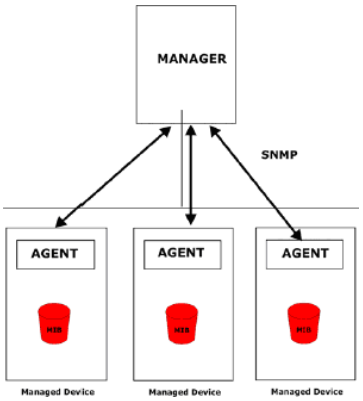
RIP Split Horizon	Switch(config-router)# passive-interface IFNAME Interface name default default for all interfaces Switch(config-router)# passive-interface default <cr>
RIP default Metric (usually = 1)	Switch(config-router)# default-metric <1-16> Default metric
RIP Setting	Switch# show ip rip status 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 vlan2:192.168.2.253
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 ……..
Multicast Routing **(Before enable MRoute, the IP Interfaces' setting should be configured and activated first.)**	
Enable the MRoute & Configure the static entry	witch(config)# ip multicast 224.0.1.10 vlan 1 interface gi2-3 vlan specify the ingress VLAN interface specify an interface list to add to IFLIST Interface list, ex: gi1,gi3-4
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

2.10 SNMP

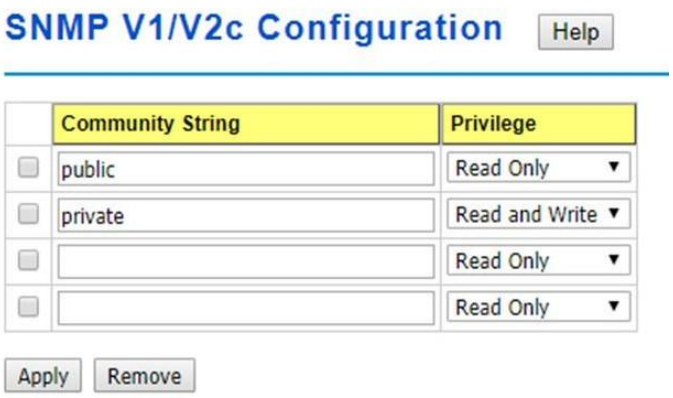


Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite.

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.

2.10.1 SNMP V1/V2c 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.



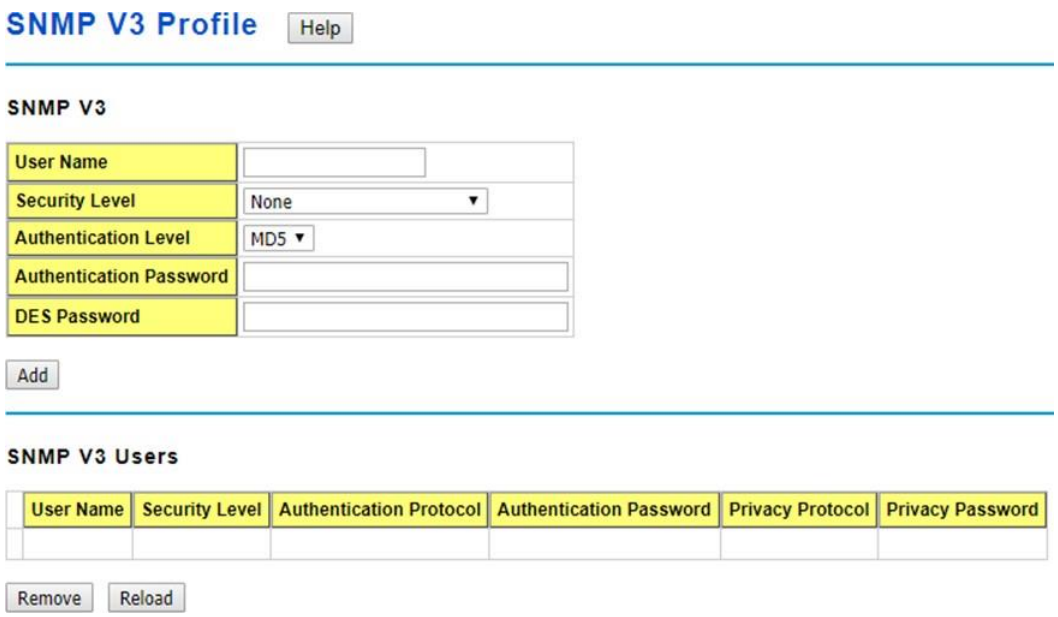
Click **"Apply"** to change the setting.
Click **"Remove"** to remove the setting.

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.

2.10.2 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 the JetNet Managed Switchand the administrator are encrypted to ensure secure communication.



SNMP V3

User Name: SNMP V3 user name.

Security Level: This is the SNMP V3 user Security Level, which can be one of the following: None, Authentication or Authentication and Privacy.

Authentication Level: This is the SNMP V3 user Authentication Level: MD5 or SHA1.

Authentication Password: This is the SNMP V3 user Authentication Password.

DES Password: This is the SNMP V3 user DES Encryption Password.

Click **"Add"** to add a SNMP V3 User.

SNMP V3 Users

This table provides SNMP V3 user information.

User Name: SNMP V3 user names.

Security Level: This is the SNMP V3 user Security Level: None, Authentication or Authentication and Privacy.

Authentication Protocol: This is the SNMP V3 user Authentication Protocol: MD5 or

SHA1.

Authentication Password: This is the SNMP V3 user Authentication Password.

Privacy Protocol: This is the SNMP V3 user Privacy Protocol, DES.

Privacy Password: This is the SNMP V3 user DES Encryption Password.

Click the **Remove** button to remove selected SNMP V3 user or click the **Reload** button to reload SNMP V3 user's information.

2.10.3 SNMP Traps

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

This page allows users to **Enable SNMP Trap,** configure the **SNMP Trap server IP**, **Community** name, and trap **Version V1 or V2**. After configuration, you can see the change of the SNMP pre-defined standard traps and Korenix pre-defined traps. The pre-defined traps can be found in Korenix private MIB.



SNMP Trap

Enable or **Disable** the SNMP trap function

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

SNMP Trap Server

Server IP: SNMP Trap Server IP address.

Community: SNMP Trap Server community string.

Version: SNMP Trap version, V1 or V2c

Click the **Add** button to add a SNMP Server.

Trap Server Profile

This table displays SNMP Trap server information.

Click the **Remove** button to remove selected SNMP Server or click the **Reload** button to reload SNMP Server information.

2.10.4 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

2.11 Security

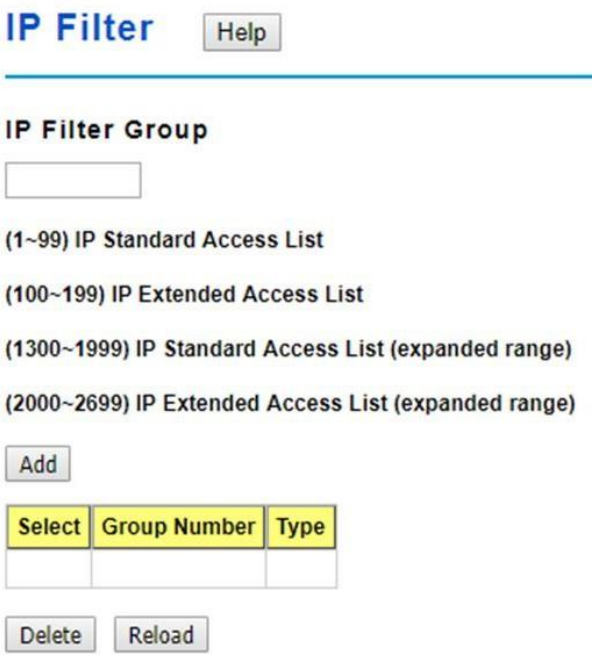
JetNet Managed Switchprovides several security features for you to secure your connection. The Filter Set is also known as Access Control List. The ACL feature includestraditional Port Security and IP Security.

2.11.1 Filters (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.

2.11.1.1 IP Filter



You can create a group of IP Filters with following numbers.

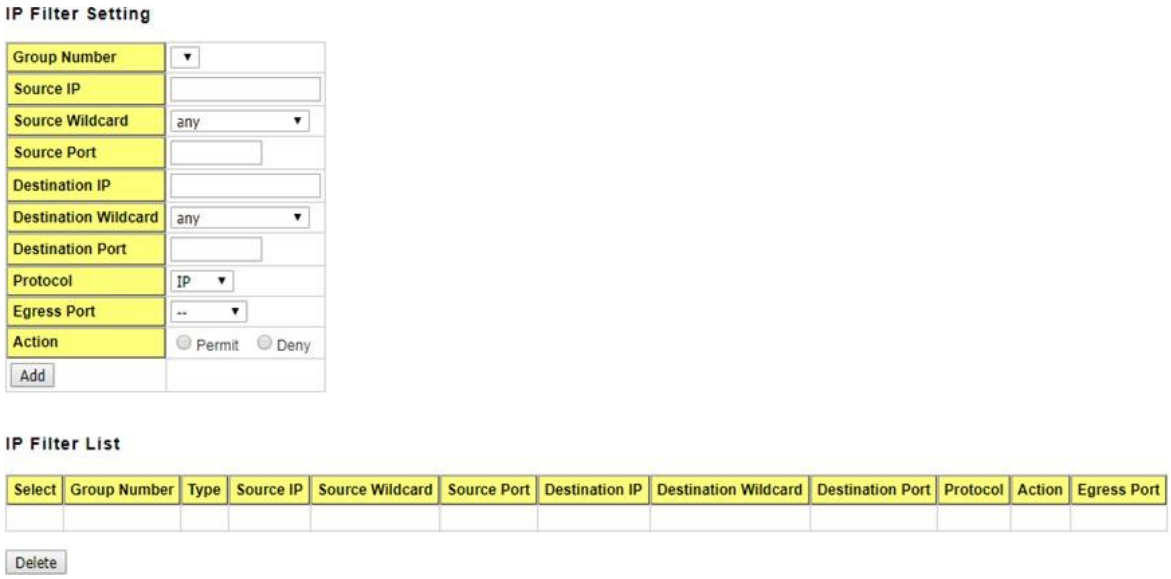
1 - 99: IP Standard Access List

100 – 199: IP Extended Access List

1300 – 1999: IP Standard Access List (expanded range)

2000 – 2699: IP Extended Access List (expanded range)

After entering the IP Filter Group number, click the **Add** to create the new Filter Group.



Group Number: Number of the Filter Group.

Source IP: This is the source IP address of the packet.

Source Wildcard: This is the mask of the IP address.

Source Port: This is the source port of L4 protocol (TCP/UDP).

Destination IP: This is the destination IP address of the packet.

Destination Wildcard: This is the mask of the IP address.

Destination Port: This is the destination port of L4 protocol (TCP/UDP).

Protocol: This is the L4 protocol (TCP/UDP/ICMP).

Action: This is the filter action, which is to deny or permit the packet.

Click the **Add** button to add a new Filter rule.

After IP Filter Setting applied, you can see the IP filter list shown on the table.

Select: Selected for delete.

Group Number: This is the number of the Filter Group.

Type: This is the filter group type (standard or extended).

Source IP: This is the source IP address of the packet.

Source Wildcard: This is the mask of the IP address.

Source Port: This is the source port of L4 protocol (TCP/UDP).

Destination IP: This is the destination IP address of the packet.

Destination Wildcard: This is the mask of the IP address.

Destination Port: This is the destination port of L4 protocol (TCP/UDP).

Protocol: This is the L4 protocol (TCP/UDP/ICMP).

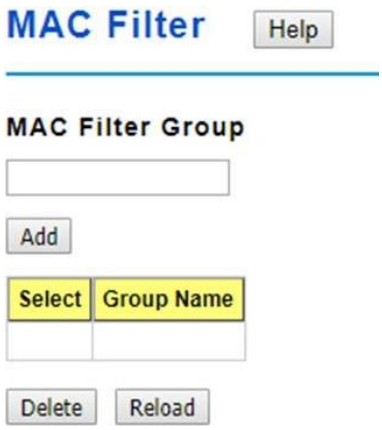
Egress Port: This is the outgoing (exiting) port number.

Action: This is the filter action, which is to deny or permit the packet.

Click the **Delete** button to remove the Filter you selected.

2.11.1.2 MAC Filter (Port Security)

Packet filtering can help limit network traffic and restrict network use by certain users or devices. The Add Filters feature filters traffic as it passes through a switch and permits or denies packets crossing specified interfaces.MAC Filters can filter layer 2 traffic.



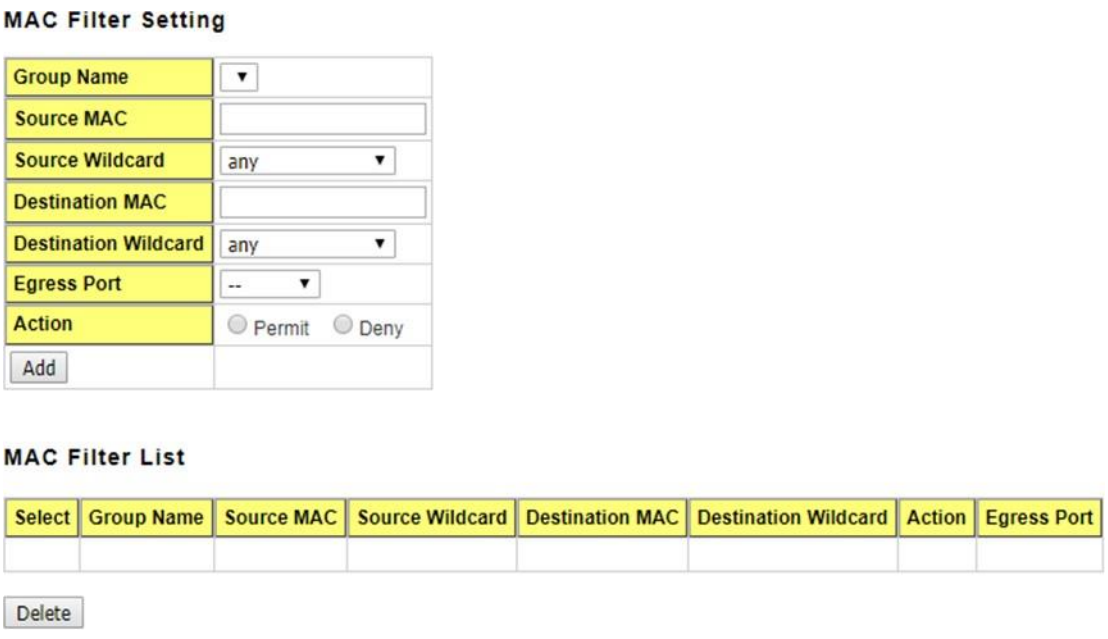
You can create a group of MAC Filters by entering a name and clicking the **Add** button to create a new Filter Group.

The MAC Filter Group table provides the following information.

Select: If you select this and click the **Delete** button the corresponding Filter Group is deleted.

Group Name: This is the name of the Filter Group.

Click the **Reload** button to reload the Filter Group table.



MAC Filter Setting

You can configure the MAC Filter.

Group Name: This is the name of the MACFilter Group.

Source MAC: This is the source MAC Address of the packet.

Source Wildcard: This is the mask of the MAC Address.

Destination MAC: This is the destination MAC Address of the packet.

Destination Wildcard: This is the mask of the MAC Address.

Egress Port: This is the outgoing (exiting) port number.

Action: This is the filter action, which is to deny or permit the packet.**Permit** to permit traffic from specified sources. **Deny** to deny traffic from those sources.

Note1: on Source MAC/ Destination MAC filed, 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".

Note2: on Source Wildcard /Destination Wildcard field, it 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	
….			

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

MAC Filter List

This is the MAC Filter List.

Select: If you select this and click the Delete button the corresponding is deleted.

Group Name: This is the name of the Filter Group.

Source MAC: This is the source MAC Address of the packet.

Source Wildcard: This is the mask of the MAC Address.

Destination MAC: This is the destination MAC Address of the packet.

Destination Wildcard: This is the mask of the MAC Address.

Action: This is the filter action, which is to deny or permit the packet.

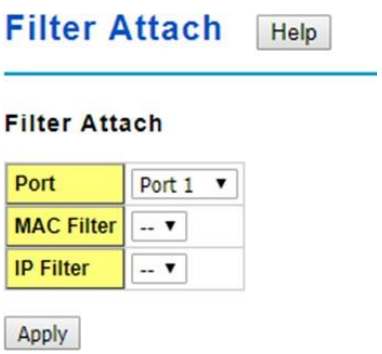
Egress Port: This is the outgoing (exiting) port number.

Click the **Delete** button to delete the filter rule.

2.11.1.3 Filter Attach

This page allows you to attach filters created on the IP Filter and MAC Filter pages to ports on the switch.

Filter Attach



Port: The port you want to attach a filter to.

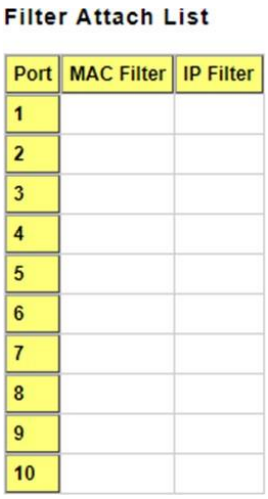
MAC Filter: Select a MAC address based filter to attach to the interface. Select "--" to remove an attached MAC address filter.

IP Filter: Select an IP address based filter to attach to the interface. Select "--" to remove an attached IP address filter.

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

Filter Attach List

This table displays what filters are currently attached to each port.



Port: The port the filters are attached to.

MAC Filter: The MAC address filter attached to the port.

IP Filter: The IP address filter attached to the port.

2.11.2 IEEE 802.1x

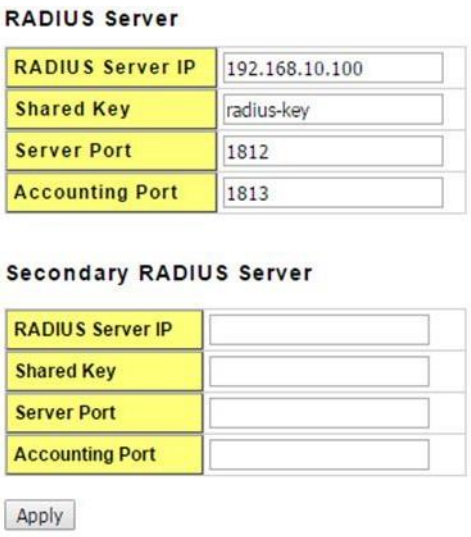
2.11.2.1 802.1XConfiguration

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 Switch could control which connection is available or not.



System AuthControl: Select **Enable** or **Disable** the 802.1x authentication.
Authentication Method: **RADIUS** is an authentication server that provide key for authentication, with this method, user must connect switch to server. If select**Local**for the authentication method, switch use the local user data base which can be create in this page for authentication.
Click **Apply** to apply the settings.

RADIUS Server



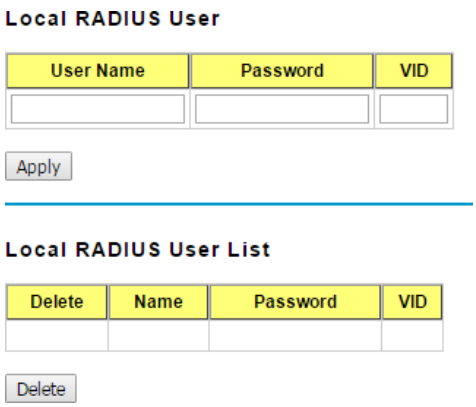
Radius Server IP: The IP address of Radius server
Shared Key: The password for communicate between switch and Radius Server.
Server Port: UDP port of Radius server.
Accounting Port: Port for packets that contain the information of account login or logout.
Secondary Radius Server IP: Secondary Radius Server could be set in case of the

primary radius server down.

Click **Apply** to apply the settings.

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

Local RADIUS User



User Name: The user name of the local RADIUS user.

Password: The password of the local RADIUS user.

VID: The VLAN ID of the local RADIUS user.

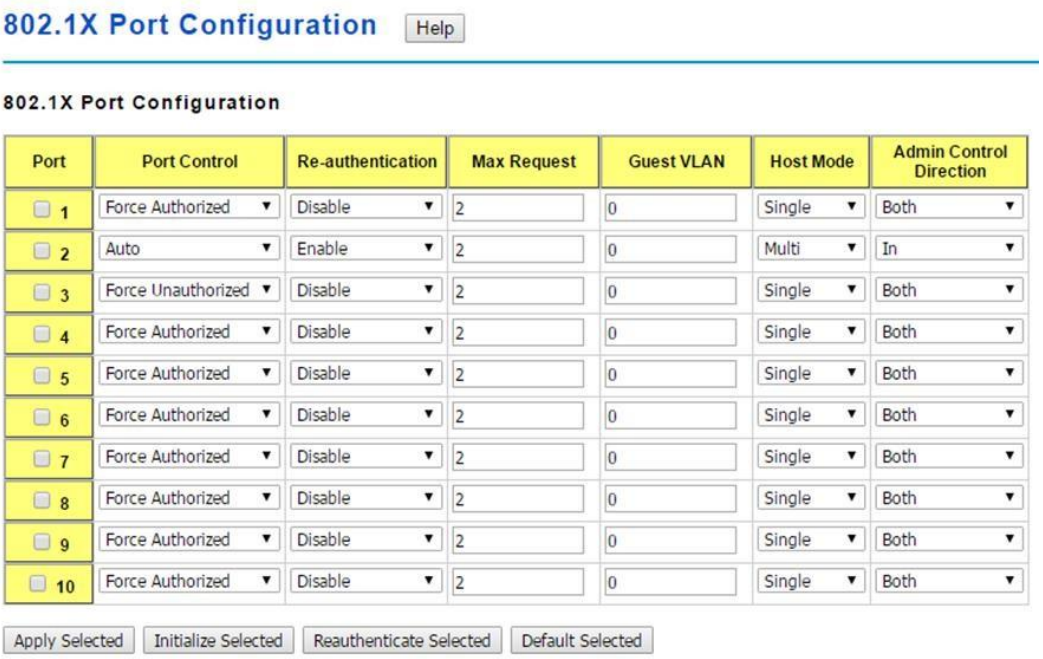
Click **Apply** to add a local RADIUS user.

802.1X Local user List: Shows the account information.

Click **Delete** to delete the selected user.

2.11.2.2 802.1X Port Configuration

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



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

Reauthentication: 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 devices can access this port once any one of them pass the authentication.

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

Click **Apply Selected** to apply the selected port configuration.

Click **Initialize Selected** to initialize the selected port.

Click **Reauthenticate Selected** to reauthenticate the selected port.

Click **Default Selected** to set the selected port configuration to default.

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
7	3600	60	30	30	30
8	3600	60	30	30	30
9	3600	60	30	30	30
10	3600	60	30	30	30

Apply

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

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

Tx period(s): the time interval of authentication request.

Supplicant Timeout(s): the timeout for the client authenticating

Sever Timeout(s): The timeout for server response for authenticating.

Click **Apply** to apply the settings.

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

2.11.2.3 802.1X Port Information

This page provides a summary of the current 802.1X port settings.

802.1X Port Information Help

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

Reload

Port: The port identifier.

Port Control: Force Authorized means that this port is Authorized and the data is free to travel in and out. Force unauthorized is just the opposite and the port is blocked.

Authorized Status: The authorize status of the port.

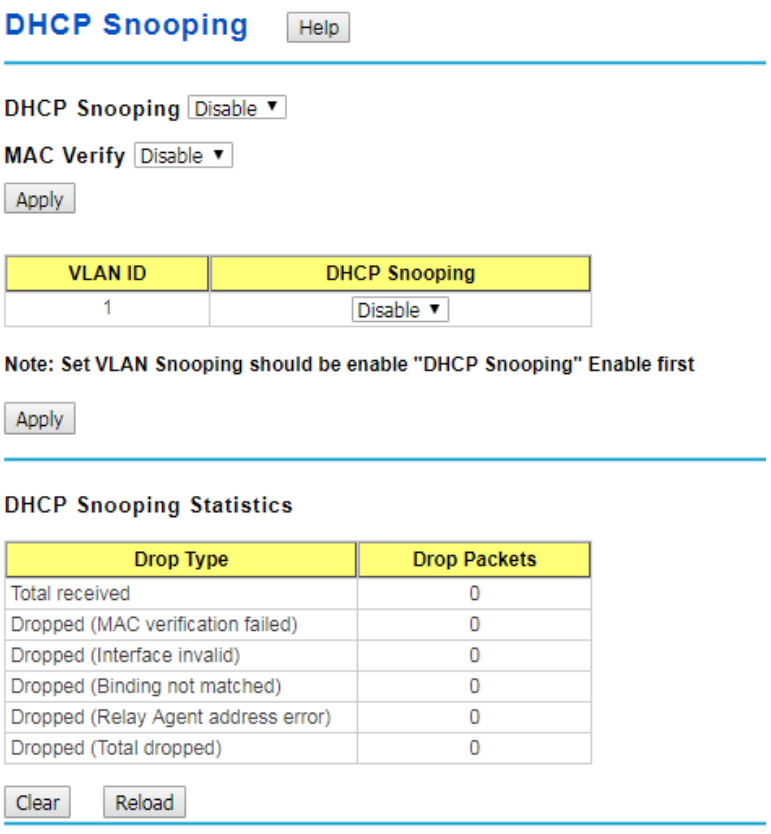
Authorized Supplicant: The MAC address of the authorized supplicant.

Oper Control Direction: Whether an unauthenticated port disables income and outgoing traffic or only incoming traffic. Both means income and outgoing traffic are blocked. In means incoming traffic is blocked.

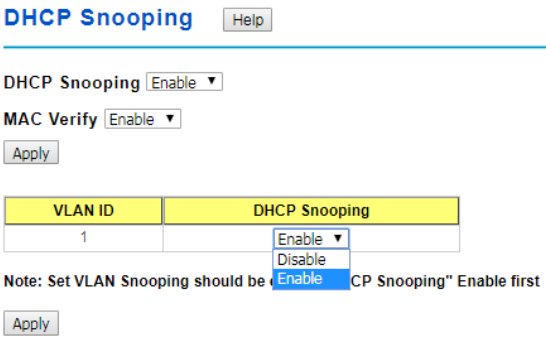
Click **Reload** to reload 802.1X port status

2.11.3 DHCP Snooping

The DHCP Snooping is a series of techniques applied to the security of an existing DHCP network . With the DHCP Snooping, the DHCP Server will manage the network access and permit the access with specific IP and specific MAC address from specific Switch port can access the network. It also provides the protection to avoid the intruder added fake DHCP server into secure network, and try to take over DHCP process. Once the Switch detects the phenomena, the port of intruder connected will be lock to protect network access.

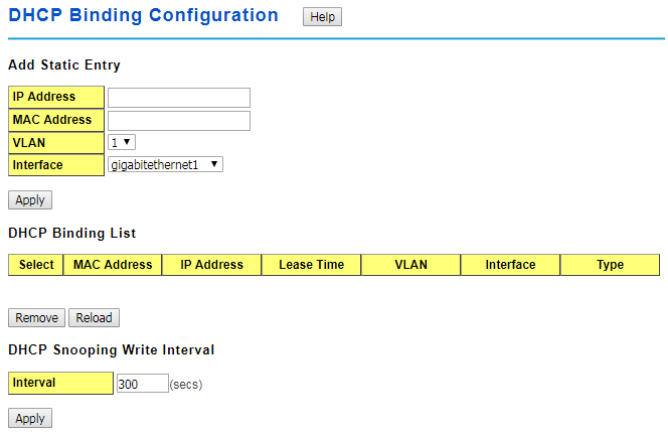


Set VLAN Snooping should be enable "DHCP Snooping" Enable first, and click “Apply” Bottom.



Choose “**Enable**” for VLAN ID. And click “Apply” bottom to save the setting and enable the DHCP Snooping.

2.11.4 DHCP Blinding



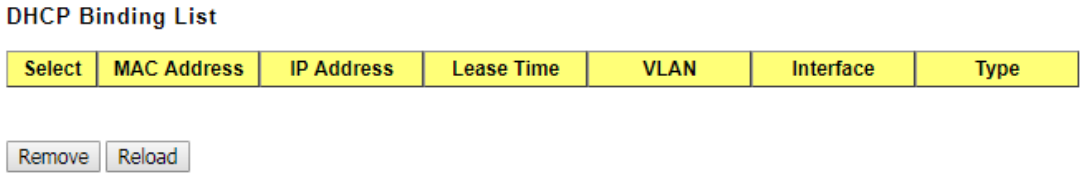
IP Address Type the address to which to bind the MAC address of the selected virtual machine.

MAC Address Type the MAC address of the selected virtual machine.

VLAN Select VLAN number which needs to enable DHCP Binding.

Interface Select the interface to bind.

Please click **“Apply”** bottom to save the change.



DHCP Binding List will be listed as above.

MAC Address: Shows the MAC of the entry.

IP Address: Shows the IP of the entry.

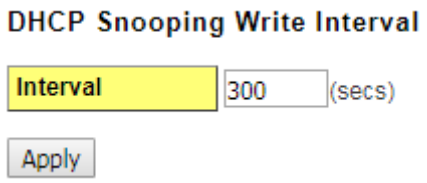
Lease Time: The Lease time of the entry.

VLAN: The entry belongs VLAN's ID.

Interface: Interface of the entry.

Type: The entry type: Static/Dynamic.

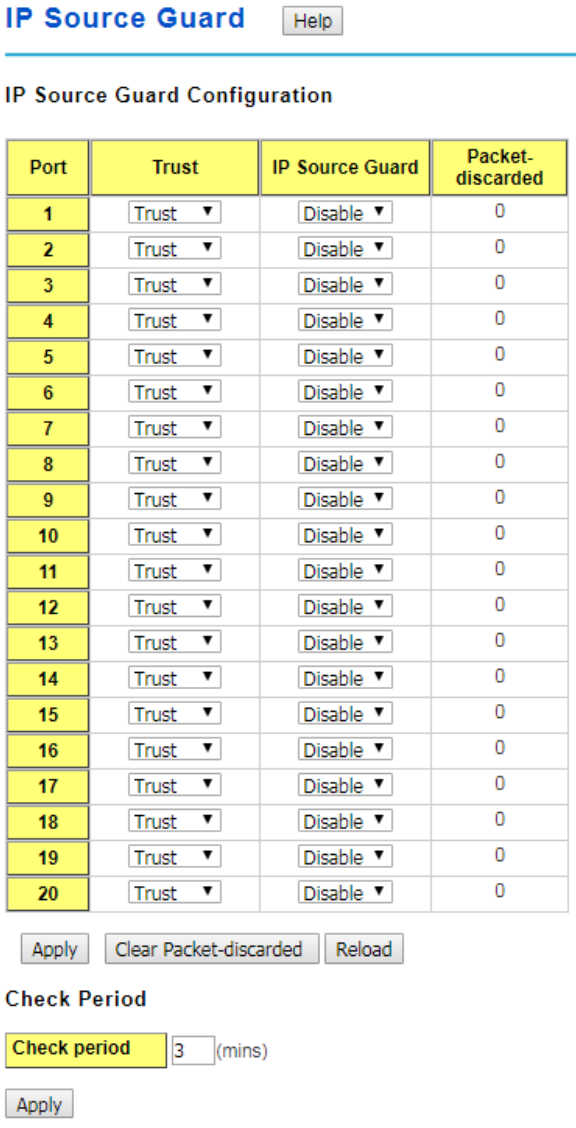
Select the item and click "**Remove**" bottom can remove that DHCP Binding Setting.



****Interval:** write current binding table to system. (secs.)

2.11.5 IP Source Guard

IP Source Guard is a security feature that restricts IP traffic on untrusted Switch port by filtering traffic based on the DHCP snooping binding database or manually configured IP source bindings. This feature helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.



IPSG configuration.

Trust: Enables/Disable Trust on each Port.

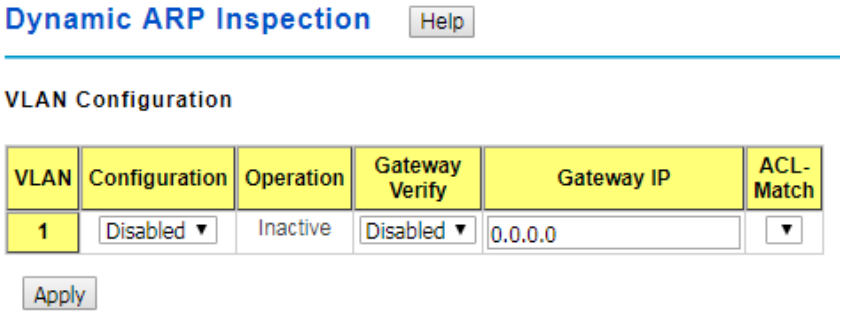
IP Source Guard: Configure the interface as Enables IPSG or Disables IPSG. If IP source guard is enabled on an interface, incoming IP traffic on an interface are allowed when there is a matching entry in IP source binding database. Otherwise, all incoming IP traffic on an interface are allowed irrespective of the IP binding database.

Packet-discarded: Shows discard packets for each port.
Click the “Apply” button to apply the configurations.
Click the Clear Packet-discarded button to clear packet discarded count.

Check Period: It's the timer for update discard-packet. It will calculate and accumulate to discard-packet in the duration.
Click the “Apply” button to apply the Check Period configurations

2.11.6 Dynamic ARP Inspection

The Dynamic ARP Inspection (DAI) is a security feature that prevents ARP attack. The Switch receives one ARP packet on an untrusted port, the switch compares the IP-to-MAC address binding with entries from the DHCP Snooping database or ARP access-lists. If there is no match, the ARP packet will be dropped by the Switch to ensure network performance.



VLAN Configuration:

VLAN: Shows the VLAN index.
Configuration: Enable or disable DAI for each VLAN.
Operation: Shows the DAI operation state.
Gateway Verify: Enable/disable verify Gateway .
Gateway IP: Gateway IP address .
ACL-Match: select the one of the ARP filter rule, the blank column is not to set the APR rule.

Interface Configuration

Port	Trust	Rate
1	Untrusted	15
2	Untrusted	15
3	Untrusted	15
4	Untrusted	15
5	Untrusted	15
6	Untrusted	15
7	Untrusted	15
8	Untrusted	15
9	Untrusted	15
10	Untrusted	15
11	Untrusted	15
12	Untrusted	15
13	Untrusted	15
14	Untrusted	15
15	Untrusted	15
16	Untrusted	15
17	Untrusted	15
18	Untrusted	15
19	Untrusted	15
20	Untrusted	15

Apply

Interface Configuration: Trust: Set Trust or Untrust for DAI for each port.
Rate: configure the DAI rate limit of incoming ARP packets.

Click the “Apply” button to apply change configuration.

Check Period

Check period	1 (mins)

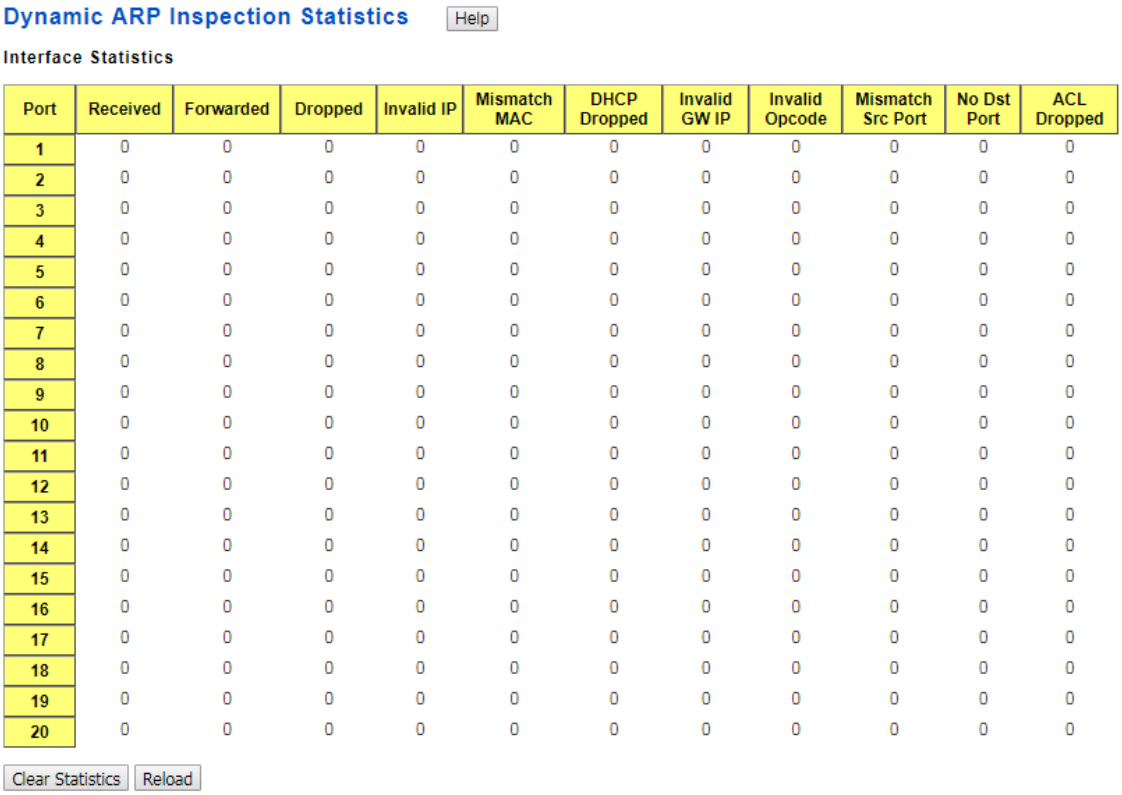
Apply

Check Period: It's the timer for update discard-packet. It will calculate and accumulate to discard-packet in the duration.

Click the “Apply” button to apply the Check Period configurations.

2.11.7 Dynamic ARP Inspection Status

On this page, it displays DAI statistics for the specified VLAN and Port



Dynamic ARP Inspection Statistics Help

Interface Statistics

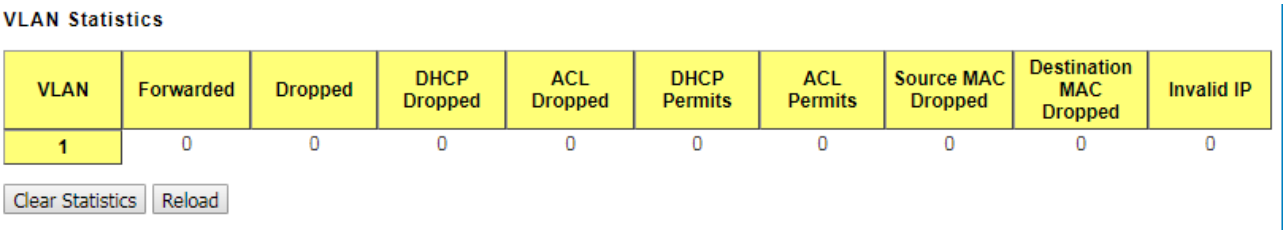
Port	Received	Forwarded	Dropped	Invalid IP	Mismatch MAC	DHCP Dropped	Invalid GW IP	Invalid Opcode	Mismatch Src Port	No Dst Port	ACL Dropped
1	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0	0	0

Clear Statistics Reload

Interface statistics

Port: This is the port identifier.
Received: The count of ARP packet received.
Forwarded: The count of ARP packet forwarded.
Dropped: The count of ARP packet dropped.
Invalid IP: The count of packet mismatch target IP address on DHCP binding table.
Mismatch MAC: The count of source MAC address of Ethernet header not same as sender MAC address.
DHCP Dropped: The count of ARP packet dropped by DHCP binding table mismatch.
Invalid GW IP: The count of invalid gateway IP address.
Invalid Opcode: The count of invalid opcode received.
Mismatch Src Port: The count of source port mismatch on DHCP binding table.
No Dst Port: The count of packet dropped by destination port not found.
ACL Dropped: The count of ARP packet dropped by ACL setting.

Click the Clear Statistics button to clear the interface statistics.
Click the Reload button to reload the statistics.



VLAN Statistics

VLAN	Forwarded	Dropped	DHCP Dropped	ACL Dropped	DHCP Permits	ACL Permits	Source MAC Dropped	Destination MAC Dropped	Invalid IP
1	0	0	0	0	0	0	0	0	0

Clear Statistics Reload

VLAN statistics

VLAN: This is the VLAN identifier.
Forwarded: The count of ARP packet forwarded.
Dropped: The count of ARP packet dropped.
DHCP Dropped: The count of ARP packet dropped by DHCP binding table mismatch.
ACL Dropped: The count of ARP packet dropped by ACL setting.
DHCP Permits: The count of ARP packet permits by DHCP binding table.
ACL Permits: The count of ARP packet permits by ACL setting.
Src MAC Dropped: The count of source MAC address of Ethernet header not same as sender MAC address.
Dest MAC Dropped: The count of ARP packet dropped by mismatch destination MAC address.
Invalid IP: The count of packet mismatch target IP address on DHCP binding table.

Click the Clear Statistics button to clear the VLAN statistics.
Click the Reload button to reload the statistics.

2.11.8 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 *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
Add MAC	Switch(config)# mac-address-table static 0012.7701.0101 vlan 1 interface fa1 mac-address-table unicast static set ok!

Port Security	Switch(config)# interface fa1 Switch(config-if)# switchport port-security Disables new MAC addresses learning and aging activities! ***Note: Rule: Add the static MAC, VLAN and Port binding first, then enable the port security to stop new MAC learning.***
Disable Port Security	Switch(config-if)# no switchport port-security Enable new MAC addresses learning and aging activities!
Display	Switch# show mac-address-table static Destination Address Address Type Vlan Destination Port ---------- ---------- ---- ---------- 0012.7701.0101 Static 1 fa1
802.1x (shot of dot1x)	
enable diable	Switch(config)# dot1x system-auth-control Switch(config)# Switch(config)# no dot1x system-auth-control Switch(config)#
authentic-method	Switch(config)# dot1x authentic-method local Use the local username database for authentication radius Use the Remote Authentication Dial-In User Service (RADIUS) servers for authentication Switch(config)# dot1x authentic-method radius Switch(config)#
radius server-ip	Switch(config)# dot1x radius Switch(config)# dot1x radius server-ip 192.168.10.120 key 1234 RADIUS Server Port number NOT given. (default=1812) RADIUS Accounting Port number NOT given. (default=1813) RADIUS Server IP : 192.168.10.120 RADIUS Server Key : 1234 RADIUS Server Port : 1812 RADIUS Accounting Port : 1813 Switch(config)#
radius server-ip	Switch(config)# dot1x radius Switch(config)# dot1x radius server-ip 192.168.10.120 key 1234 RADIUS Server Port number NOT given. (default=1812) RADIUS Accounting Port number NOT given. (default=1813) RADIUS Server IP : 192.168.10.120 RADIUS Server Key : 1234 RADIUS Server Port : 1812 RADIUS Accounting Port : 1813 Switch(config)#
radius secondary-server-ip	Switch(config)# dot1x radius secondary-server-ip 192.168.10.250 key 5678 Port number NOT given. (default=1812) RADIUS Accounting Port number NOT given. (default=1813) Secondary RADIUS Server IP : 192.168.10.250 Secondary RADIUS Server Key : 5678 Secondary RADIUS Server Port : 1812 Secondary RADIUS Accounting Port : 1813

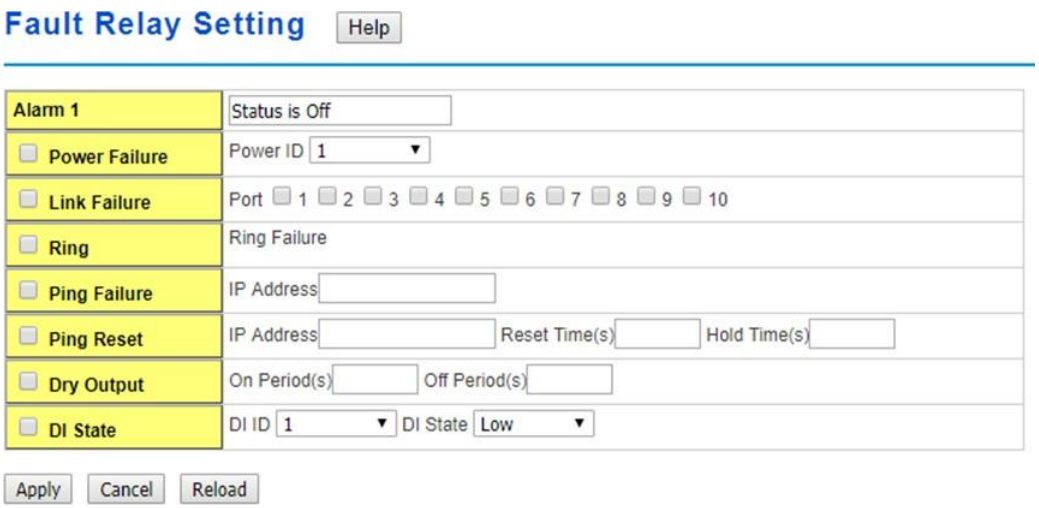
User name/password for authentication	Switch(config)# dot1x userna130orenixnix pass130orenixnix vlan 1
Display	Switch# show dot1x <cr> all Show Dot1x information for all interface authentic-method Dot1x authentic-method
	interface Interface name radius Remote Access Dial-In User Service statistics Interface name username User Name in local radius database Switch# show dot1x<cr> = Switch# show dot1x all You can check all dot1x information for all interfaces. Click Ctrl + C to exit the display Switch# show dot1x interface fa1 Supplicant MAC ADDR <NONE> STATE-MACHINE AM status : FORCE_AUTH BM status : IDLE PortStatus : AUTHORIZED PortControl : Force Authorized Reauthentication : Disable MaxReq 2 ReAuthPeriod : 3600 Seconds QuietPeriod : 60 Seconds TxPeriod : 30 Seconds SupplicantTimeout : 30 Seconds ServerTimeout : 30 Seconds GuestVlan 0 HostMode : Single operControlledDirections : Both adminControlledDirections : Both Switch# show dot1x radius RADIUS Server IP : 192.168.10.100 RADIUS Server Key : radius-key RADIUS Server Port : 1812 RADIUS Accounting Port : 1813 Secondary RADIUS Server IP : N/A Secondary RADIUS Server Key : N/A Secondary RADIUS Server Port : N/A Secondary RADIUS Accounting Port : N/A Switch# show dot1x username 802.1x Local User List Username : orwell , Password : * , VLAN ID 1

2.12 Warning

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

2.12.1 Fault Relay

The JetNet Switch provides alarm relay output (DO) that can support multiple fault conditions. The relay contacts are energized (open) for normal operation and close under fault conditions. The fault conditions include power failure, Ethernet port link faults, Ring topology changes, Ping failures, DI state changes or ping remote IP address failure



Alarm 1: This displays whether the Relay status is on or off. You must select a fault relay option and click Apply for the status to display as on.

Power Failure: Activates the fault relay when the selected power input stops receiving power. Select power input or anypower input.

Link Failure: Activates the fault relay when a link failure occurs on a selected port.

Ring: Activates the fault relay if a failure occurs on a Redundant Ring. This event is only applicable if a Redundant Ring is configured on the switch.

Ping Failure: Activates the fault relay if the switch is unable to ping the supplied IP address.

Ping Reset: Activates the fault relay if the switch is unable to ping the supplied IP address. When activated, the switch will wait for the Reset Time (1-65535 seconds) before deactivating the relay. It will then wait the Hold Time (1-65535 seconds) before attempting to ping the IP address again.

Dry Output: Allows you to continuously cycle the relay on and off. The relay will activate for the On Period (1-65535 seconds) and then deactivate for the Off Period (1-65535 seconds).

DI State: Activates the relay based on the state of the digital input. If DI State is set to Low the relay will activate when the digital input is off. If DI State is set to High the relay will activate when the digital input is on.

Click **Apply** to apply the settings.

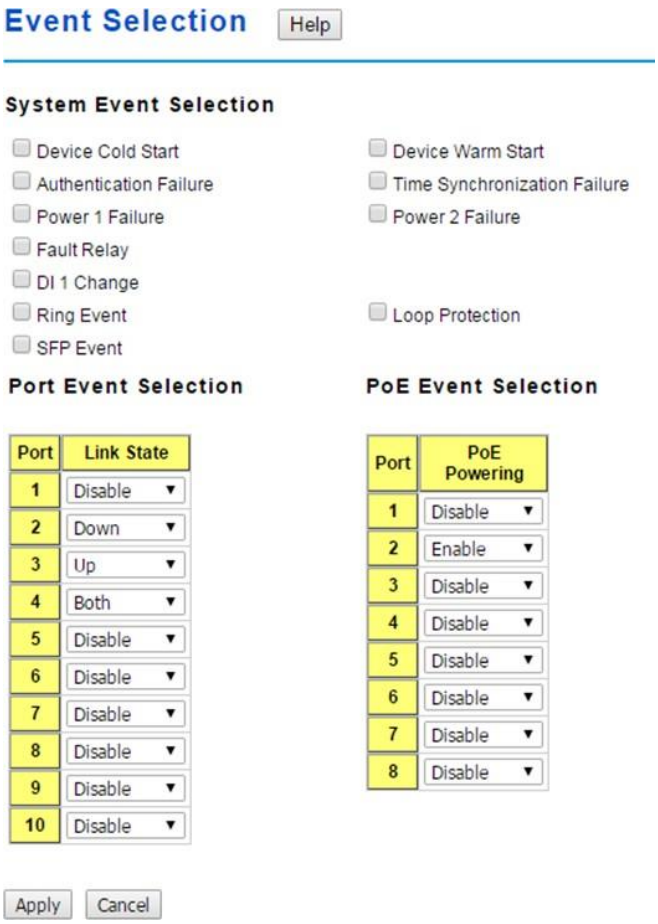
Click **Cancel** to clear the modification.

Click **Reload** to reload the settings.

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

2.12.2 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 specific ports



System Event Selection

Device Cold Start: When selected the switch generates a notification if the switch powers up from a completely powered down state.

Device Warm Start: When selected the switch generates a notification if the switch is

rebooted.

Authentication Failure: When selected the switch generates a notification if somebody attempts to log into the switch with incorrect credentials.

Time Synchronize Failure: When selected the switch generates a notification if it fails to synchronize with an NTP server. This event is only applicable if the switch is configured to synchronize with an NTP server.

Power Failure: When selected the switch generates a notification if a power failure occurs on it's power number.

Fault Relay: When selected the switch generates a notification if the fault relay changes state.

DI Change: When selected the switch generates a notification if the state changes on it's digital input number.

Ring Event: When selected the switch generates a notification if the state of a Redundant Ring changes. This event is only applicable if a Redundant Ring is configured on the switch.

Loop Protection: When selected the switch generates a notification if a loop protection event occurs.

SFP: When selected the switch generates a notification if the state of an SFP changes. This event is only applicable if an SFP module is inserted into one of the switch's SFP slots.

Port Event Selection

Link State: Select Disable, Down, Up or Both to generate a Port Event.
Disable: Disable the port event on the port.
Link-Down: The port is disconnected. For example, the cable is pulled out or the opposing devices is down.
Link-Up The port is connected to another device.
Both: The link status changed.

Click **Apply** to apply the settings.

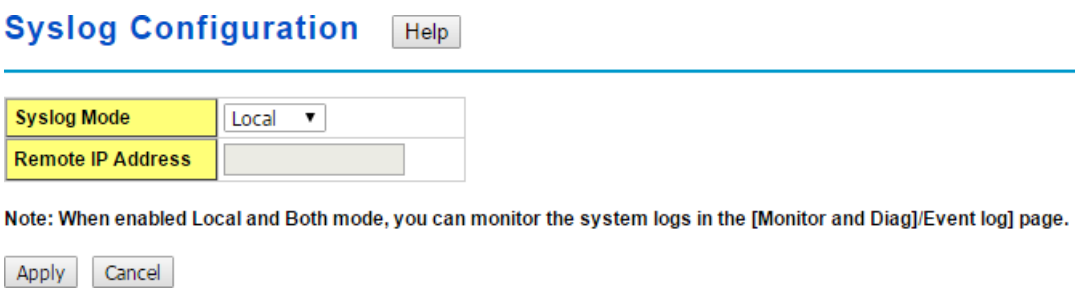
PoE Event Selection

PoE Powering: Select Disable or Enable to generate a PoE Powering event.

Click **Apply** to apply the settings.

2.12.3 SysLog Configuration

System Log is useful to provide system administrator locally or remotely monitor switch events history.



Syslog Mode: There are two System Log modes provided by JetNet Switch, local mode and remote mode.

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

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

Both: This enables both Local and Remote modes.

Remote IP Address: The IP address of the syslog server. It cannot be modified when the Syslog Mode is Disable or Local.

Click **Apply** to apply the settings.

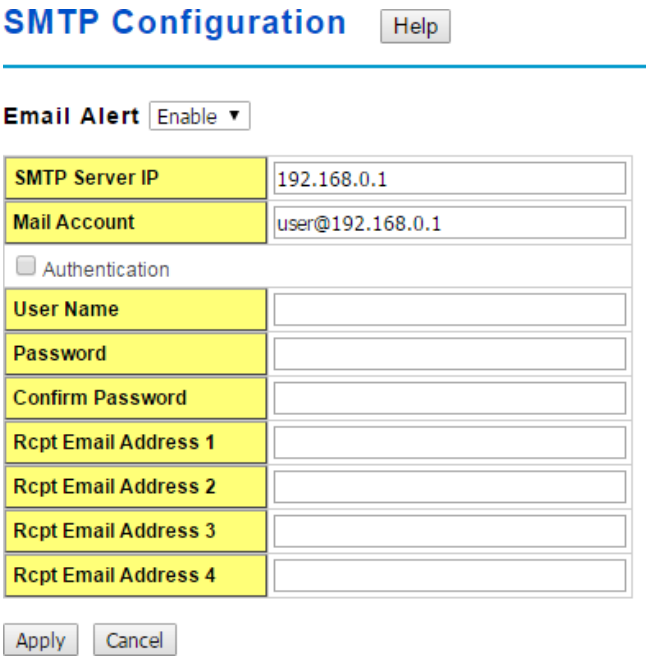
Click **Cancel** to clear the modification.

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

2.12.4 SMTP Configuration

JetNet Switch 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.



Email Alert: Select Enable / Disable to the email alert feature.

SMTP Server IP: Enter the IP address of the email Server.

Mail Account: Enter the Email account for SMTP server.

Authentication: Check to enable the authentication feature SMTP server.

User Name: Enter the Email account name for SMTP server.

Password: The Email authentication password for SMTP server.

Confirm Password: Re-type the password of the email account.

Rcpt Email Address 1 - 4: You can set up to 4 email addresses to receive email alarm from JetNet.

Click **Apply** to apply the settings.

Click **Cancel** to clear the modification.

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

2.12.5 CLI Commands

Command Lines of the Warning configuration

Feature	Command Line
Relay Output	
Relay Output	Switch(config)# relay 1 dry dry output ping ping failure port port link failure

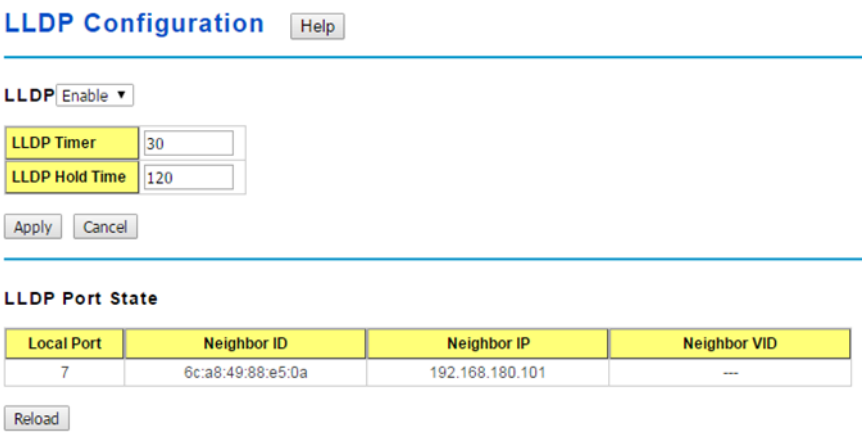
	ring ring failure
Dry Output	Switch(config)# relay 1 dry <0-65535> turn on period in second Switch(config)# relay 1 dry 5 <0-65535> turn off period in second Switch(config)# relay 1 dry 5 5
Ping Failure	Switch(config)# relay 1 ping 192.168.10.33 <cr> reset reset a device Switch(config)# relay 1 ping 192.168.10.33 reset <1-65535> reset time Switch(config)# relay 1 ping 192.168.10.33 reset 60 <0-65535> hold time to retry Switch(config)# relay 1 ping 192.168.10.33 reset 60 60
Port Link Failure	Switch(config)# relay 1 port PORTLIST Port list, ex: fa1,fa3-5,gi12 Switch(config)# relay 1 port fa1-5
Ring Failure	Switch(config)# relay 1 ring
Disable Relay	Switch(config)# no relay 1 relay id Switch(config)# no relay 1
Display	Switch# show relay 1 Relay 1 Event : Power : Disabled Port Link : Disabled Ring : Disabled Ping : Disabled Ping Reset : Disabled Dry Output : Disabled DI : Disabled
Event Selection	
Event Selection	Switch(config)# warning-event coldstart Switch cold start event warmstart Switch warm start event authentication Authentication failure event linkdown Switch link down event linkup Switch link up event authentication Authentication failure event ring Switch ring event fault-relay Switch fault relay event time-sync Switch time synchronize event sfp Switch SFP event loop-protect Switch loop protection event
Ex: Cold Start event	Switch(config)# warning-event coldstart Set cold start event enable ok.
Ex: Link Up event	Switch(config)# warning-event linkup [IFNAME] Interface name, ex: fastethernet1 or gi8 Switch(config)# warning-event linkup fa5 Set fa5 link up event enable ok.
Display	Switch# show warning-event Warning Event: Cold Start: Disabled Warm Start: Disabled Authentication Failure: Disabled Link Down: Disabled Link Up: Disabled

	Ring: Disabled Fault Relay: Disabled Time Synchronize Failure: Disabled SFP: Disabled Loop Protection: Disabled
Syslog Configuration	
Local Mode	Switch(config)# log syslog local
Server Mode	Switch(config)# log syslog remote 192.168.10.33
Both	Switch(config)# log syslog local Switch(config)# log syslog remote 192.168.10.33
Disable	Switch(config)# no log syslog local
SMTP Configuration	
SMTP Enable	Switch(config)# smtp-server enable email-alert SMTP Email Alert set enable ok.
Sender mail	Switch(config)# smtp-server server 192.168.10.100 ACCOUNT SMTP server mail account, ex: admin@korenix.com Switch(config)# smtp-server server 192.168.10.100 admin@korenix.com SMTP Email Alert set Server: 192.168.10.100, Account: admin@korenix.com ok.
Receiver mail	Switch(config)# smtp-server receiptadmin@example.com SMTP Email Alert set receipt 1: admin@example.com ok.
Authentication with username and password	Switch(config)# smtp-server authentication usernameadmin password admin SMTP Email Alert set authentication Username: admin, Password: admin **Note: You can assign string to username and password.**
Disable SMTP	Switch(config)# no smtp-server enable email-alert SMTP Email Alert set disable ok.
Disable Authentication	Switch(config)# no smtp-server authentication SMTP Email Alert set Authentication disable ok.
Display	Switch# sh smtp-server SMTP Email Alert is Enabled Server: 192.168.10.100, Account: admin@example.com Authentication: Enabled Username: admin, Password: admin SMTP Email Alert Receipt: Receipt 1: admin@example.com Receipt 2: Receipt 3: Receipt 4:

2.13 Monitor and Diag

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

2.13.1 LLDP Configuration



LLDP: Select Enable/Disable to the LLDP function.

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

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

Click **Apply** to apply the settings.

Click **Cancel** to clear the modification.

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

LLDP Port State

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

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

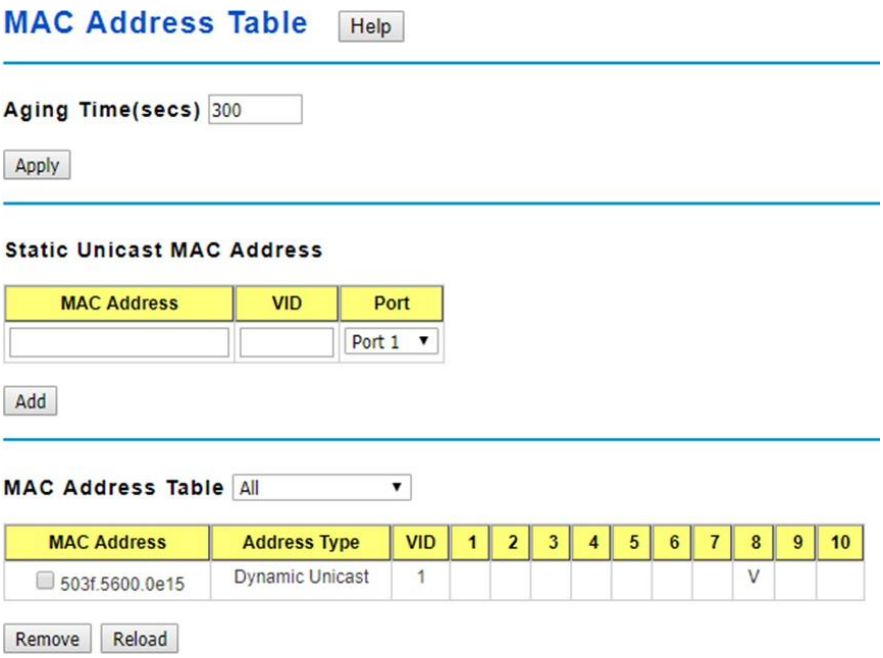
Neighbor IP: the IP address of neighbor device on the same network segment.

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

Click **Reload** to reload the LLDP Port State Table.

2.13.2 MAC Address Table

In this page, you can change the Aging time, add Static Unicast MAC Address, monitor the MAC address or sort them by different packet types and ports.



.

MAC Address Table

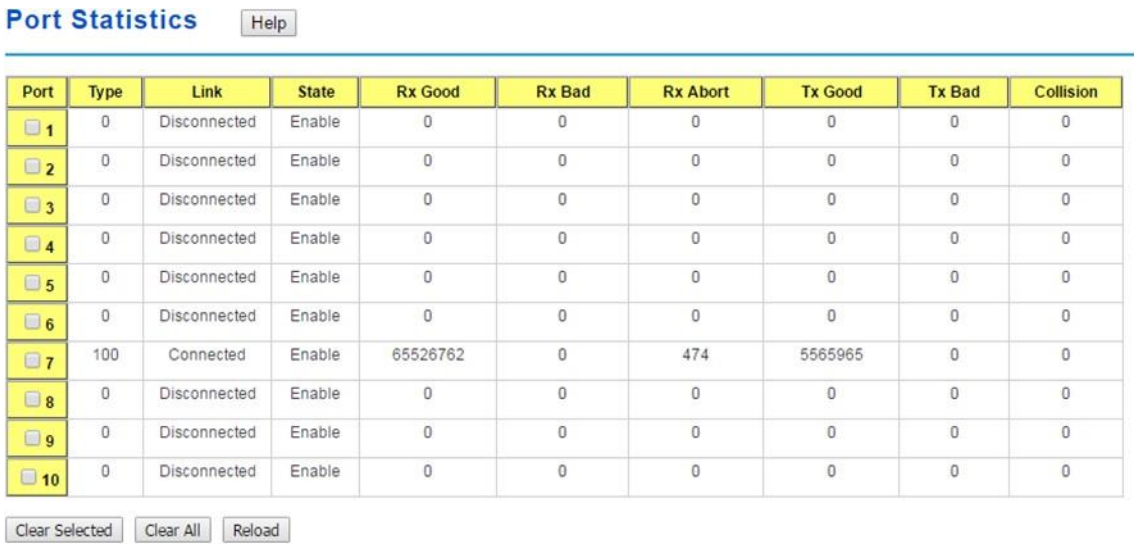
In this MAC Address Table, you can see all the MAC Addresses learnt by the switch fabric. The packet types include Management Unicast, Static Unicast, Dynamic Unicast, Static Multicast and Dynamic Multicast. The table allows users to sort the address by the packet types and port.

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.

2.13.3 Port Statistics

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



Type: Indicates the port type.

Link: Indicates the link status, Connected or Disconnected.

State: Indicates the link state, Enable or Disable.

RX Good: The count of good frames received, which is the total number of received unicast, broadcast, multicast and pause frames.

RX Bad: The count of bad frames received, which is the total number of undersize, fragment, oversize, jabber, RXErr and FCSErr frames.

RX Abort: The count of abort frames received, which is the total number of discarded and filtered frames.

TX Good: The count of good frames transmitted, which is the total number of transmitted unicast, broadcast, multicast and pause frames.

TX Bad: The count of FCSErr frames transmitted.

Collision: The count of collision frames. The Collision is the Collisions frames (include single, multiple, excessive, late collisions frames).

Click **Clear Selected** to clean selected port counts.

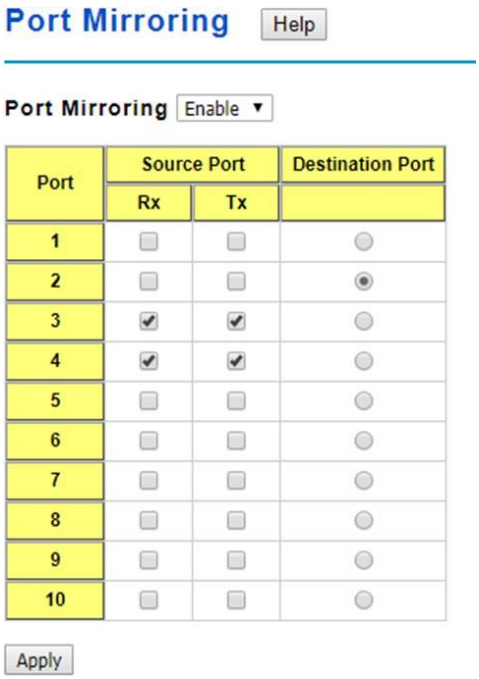
Click **Clear All** to clean all counts.

Click **Reload** to reload all counts.

Note: If you see many Bad, Abort or Collision counts increased, that may mean the network cable is not properly connected or the network performance of the port is poor. Check your network cable, the network interface card of the connected device, the network application, or reallocate the network traffic.

2.13.4 Port Mirroring

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

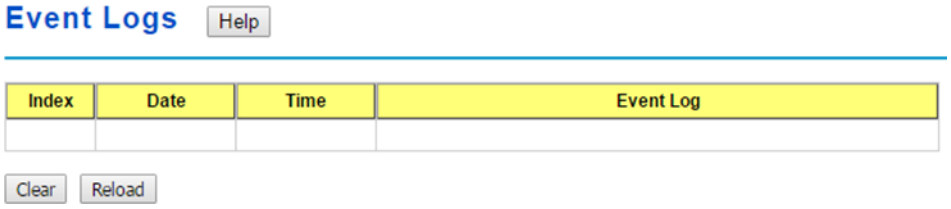


Port Mirror Mode: Select **Enable**/**Disable** to enable/disable Port Mirror.
Source Port: This is also known as Monitor Port. These are the ports you want to monitor. The traffic of all source/monitor ports will be copied to destination/analysis ports. You can choose a single port, or any combination of ports, but you can only monitor them in Rx or TX only.
Click on checkbox of the Port ID, Rx, Tx or Both to select the source ports.
Destination Port: This is also known as Analysis Port.You can analyze the traffic of all the monitored ports at this port without affecting the flow of traffic on the port(s) being monitored. Only one of the destination ports can be selected. A network administrator would typically connect a LAN analyzer or Netxray device to this port.

Click **Apply** to apply the settings.

2.13.5 Event Logs

The System Log feature was introduced in 4.12.3SysLog Configuration . When System Log Local mode is selected, JetNet Switch will record occurred events in local log table. This page shows this log table. The entry includes the index, occurred data and time and content of the events.



Index: The index of the log entry.

Date: The date the log was generated on.

Time: The time the log was generated at.

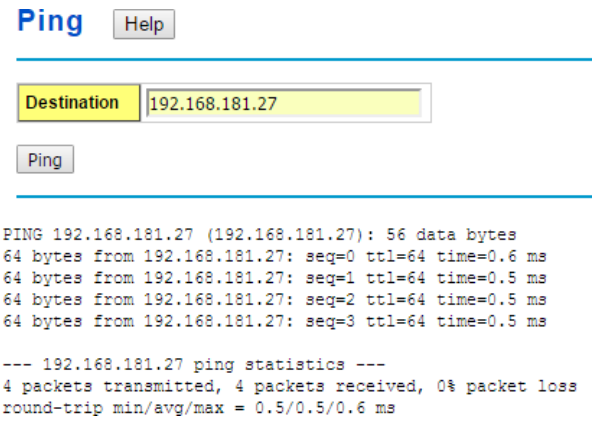
Event Log: The log entry.

Click **Clear** to clear all event logs.

Click **Reload** to reload the event log table.

2.13.6 Ping

This page provides **Ping Utility** for users to ping remote device and check whether the device is alive or not.



Destination: Enter the target IP address of the device that wants to ping.

Click **Ping** to display the results.

2.13.7 CLI Commands of the Monitor and Diag

Command Lines of the Monitor and Diag configuration

Feature	Command Line
MAC Address Table	
Ageing Time	Switch(config)# mac-address-table aging-time 350 mac-address-table aging-time set ok! *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 gi4 0012.7701.0386 Dynamic 1 gi7 0012.7710.0101 Static 1 gi7 0012.7710.0102 Static 1 gi7 0012.77ff.0100 Management 1 ***** MULTICAST MAC ADDRESS ***** Vlan Mac Address COS Status Ports ---- --------------- ---- ------- ------------------------- 1 0100.5e40.0800 0 gi6 1 0100.5e7f.fffa 0 gi4,gi6
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 gi4 0012.7701.0386 Dynamic 1 gi7
Show MAC Address Table – Multicast MAC addresses	Switch# show mac-address-table multicast Vlan Mac Address COS Status Ports ---- --------------- ---- ------- ------------------------- 1 0100.5e40.0800 0 gi6-7 1 0100.5e7f.fffa 0 gi4,gi6-7
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 gi7 0012.7710.0102 Static 1 gi7

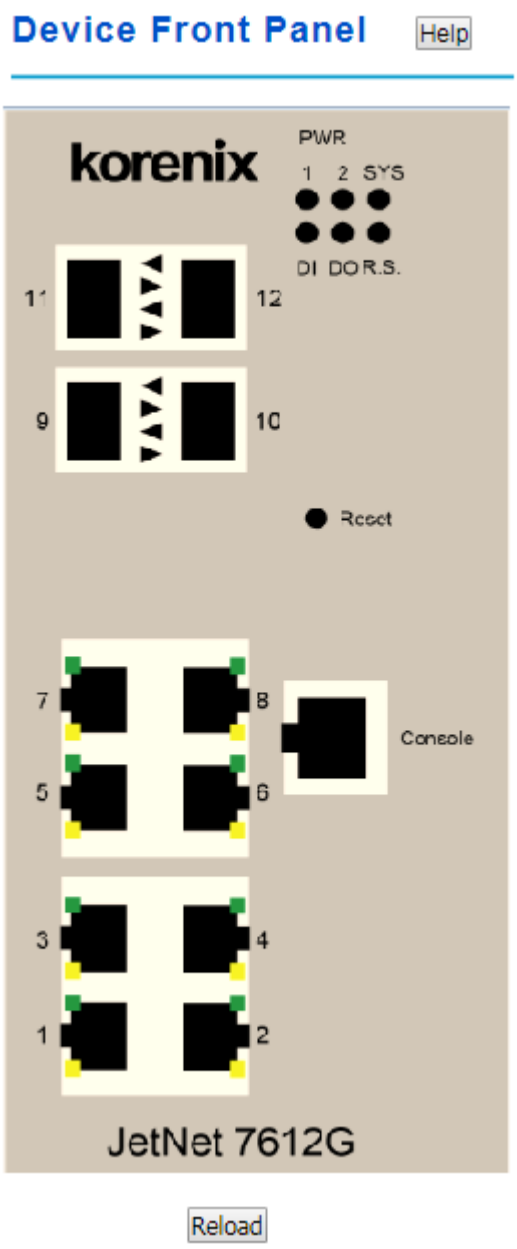
Show Aging timeout time	Switch# show mac-address-table aging-time the mac-address-table aging-time is 300 sec.
Port Statistics	
Port Statistics	Switch# show rmon statistics gi4 (select interface) Interface gigabitethernet4 is enable connected, which has Inbound: Good Octets: 178792, Bad Octets: 0 Unicast: 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 gi1-2 both Received and transmitted traffic rx Received traffic tx Transmitted traffic Switch(config)# mirror source gi1-2 both Mirror source gi1-2 both set ok. ***Note: Select source port list and TX/RX/Both mode.***
Select Destination Port	Switch(config)# mirror destination gi6 both Mirror destination fa6 both set ok
Display	Switch# show mirror Mirror Status : Enabled Ingress Monitor Destination Port : gi6 Egress Monitor Destination Port : gi6 Ingress Source Ports :gi1,gi2, Egress Source Ports :gi1,gi2,
Event Log	
Display	Switch# show event-log <1>Jan 1 02:50:47 snmpd[101]: Event: Link 4 Down. <2>Jan 1 02:50:50 snmpd[101]: Event: Link 5 Up. <3>Jan 1 02:50:51 snmpd[101]: Event: Link 5 Down. <4>Jan 1 02:50:53 snmpd[101]: Event: Link 4 Up.
Topology Discovery (LLDP)	
Enable LLDP	Switch(config)# lldp holdtime Specify the holdtime of LLDP in seconds run Enable LLDP timer Set the transmission frequency of LLDP in seconds Switch(config)# lldp run LLDP is enabled!
Change LLDP timer	Switch(config)# lldp holdtime <10-255> Valid range is 10~255

	Switch(config)# lldp timer <5-254> Valid range is 5~254
Ping	
Ping IP	Switch# ping 192.168.10.33 PING 192.168.10.33 (192.168.10.33): 56 data bytes 64 bytes from 192.168.10.33: icmp_seq=0 ttl=128 time=0.0 ms 64 bytes from 192.168.10.33: icmp_seq=1 ttl=128 time=0.0 ms 64 bytes from 192.168.10.33: icmp_seq=2 ttl=128 time=0.0 ms 64 bytes from 192.168.10.33: icmp_seq=3 ttl=128 time=0.0 ms 64 bytes from 192.168.10.33: icmp_seq=4 ttl=128 time=0.0 ms --- 192.168.10.33 ping statistics --- **4** packets transmitted, 5 packets received, 0% packet loss round-trip min/avg/max = 0.0/0.0/0.0 ms

2.14 Device Front Panel

The Device Front Panel allows you to see the LED status of the switch

For Example, JetNet 7612G front panel status is shown as below



Click on **Reload** to reload the status.

Note: No CLI command for this feature

2.15 Save

The Save Configuration page saves any changes to the configuration to the flash.If the switch loses power before clicking save configuration causes loss of the new settings. Applying changes on web user interface pages do not save the changes to the flash.



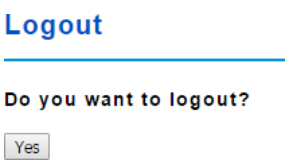
Click **Save to Flash** to save your new configuration.

Command Lines:

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

2.16 Logout

The Logout command allows you to manually logout the web connection. The web connection will be logged out automatically if you don't input any command after 30 seconds.



Click **Yes** to logout

Command Lines:

Feature	Command Line
Logout	SWITCH> exit SWITCH# exit

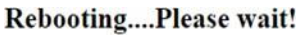
2.17 Reboot

System Reboot allows you to reboot the device. Most feature changes require a switch reboot to take effect.

Note: Before rebooting, remember to go to **Save**page to save your settings. Otherwise, the settings will be lost when theswitch is powered off.



Click **Yes**to reboot the device.



Please wait for rebooting. After rebooting complete, please login again.

3.1 Korenix Private MIB

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

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

3.2 About Korenix

Less Time At Work! Fewer Budget on applications!

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

Fusion of Outstanding's

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

3.3 Release History

Edition	Date	Modifications
V1.0	2019/10/20	First Release
V1.1	2020/03/31	Modify front panel issue
V1.2	2020/04/27	Add PoE Priority