Korenix JetNet 7500 & 5500 Series
Industrial M12 Managed Ethernet Switch

User Manual

Version 1.0

April 20th ,2020

A Beijer Group Company

www.korenix.com

Korenix JetNet 7500 Series & 5500 Series

Industrial Managed Ethernet Switch

User Manual

Copyright Notice

Federal Communications Commission (FCC) Statement

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

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

Content

1 Introduction 6
2 Hardware Installation 10
2.1 Hardware Introduction 10
2.2 Wiring Power Inputs 10
2.3 Wiring Earth Ground 10
3 Preparation for Management 16
3.1 Preparation for serial console 16
3.2 Preparation for Web Interface 17
3.2.1 Web Interface 17
3.2.2 Secured Web Interface 18
3.3 Preparation for Telnet Console 19
3.3.1.1 Telnet/ SSH (Secure Shell) 19
4. Feature Configuration 22
4.1 Command Line Interface Introduction 23
4.2 Basic Setting 29
4.2.1 Switch Setting 29
4.2.2 Admin Password 30
4.2.3 IP Configuration 32
4.2.4 Time Setting 34
4.2.5 Jumbo Frame 37
4.2.6 DHCP Server 38
4.2.7 Backup and Restore 43
4.2.8 Firmware Upgrade 45
4.2.9 Load Default 47
4.2.10 CLI Commands for Basic Setting 47
4.3 Port Configuration 53
4.3.1 Understand the port mapping 53
4.3.2 Port Control 53
4.3.3 Port Status 55
4.3.4 Rate Control 56
4.3.5 Storm Control 58
4.3.6 Port Trunking 58

4.3.7 Command Lines for Port Configuration 63
4.4 Power over Ethernet 67
4.4.1 PoE Control 67
4.4.2 PoE Schedule 69
4.4.3 PoE Status 70
4.5 Network Redundancy 71
4.5.1 STP Configuration 71
4.5.2 STP Port Configuration 73
4.5.3 STP Information 74
4.5.4 MSTP Configuration 75
4.5.5 MSTP Port Configuration 78
4.5.6 MSTP Information 79
4.5.7 MSR Configuration 80
4.5.8 MSR Information 83
4.5.9 ERPS Configuration 84
4.5.10 Command Lines 87
4.6 VLAN 94
4.6.1 VLAN Configuration 95
4.6.2 VLAN Port Configuration 96
4.6.3 VLAN Information 98
4.6.4 PVLAN Configuration 98
4.6.5 PVLAN Port Configuration 99
4.6.6 PVLAN Information 100
4.6.7 GVRP Configuration 100
4.6.8 CLI Commands of VLAN 102
4.7 Traffic Prioritization 106
4.7.1 QoS Setting 106
4.7.2 CoS-Queue Mapping 107
4.7.3 DSCP-Priority Mapping 108
4.7.4 CLI Commands of the Traffic Prioritization 109
4.8 Multicast Filtering 112

4.8.1 IGMP Query 113

4.8.2 IGMP Snooping/ Filtering 113

4.8.2.1 IGMP Snooping VLAN Setting 115

4.8.2.2 IGMP Snooping Table 115

4.8.3 GMRP Configuration 115

4.8.4 CLI Commands of the Multicast Filtering 117

4.9 Routing 119

4.9.1 ARP 119

4.9.2 IP 120

4.9.3 Router 123

4.9.4 RIP 124

4.9.5 OSPF 126

4.10 SNMP 125

4.11 Security 129

4.11.1 Filters (Access Control List) 129

4.11.2 Port Security 136

4.11.3 IEEE 802.1x 137

4.11.4 DHCP Snooping 142

4.11.5 DHCP Binding 143

4.11.6 IP Source Guard 144

4.11.7 Dynamic APR Inspection 145

4.11.8 Dynamic APR Inspection Statistic 146

4.11.9 CLI Commands of the security 147

4.12 Warning 145

4.13 Monitor and Diag 152

4.13.1 LLDP Configuration 152

4.13.2 MAC Address Table 153

4.13.3 Port Statistics 154

4.13.4 Port Mirroring 152

4.13.5 Event Logs 153

4.13.6 Ping 153

4.13.7 CLI Commands of the Monitor and Diag 154
4.14 Device Front Panel 159
4.15 Save 160
4.16 Logout 161
4.17 Reboot 161
5. Appendix 133
5.1 Product Specification 133
5.2 Korenix Private MIB 137
5.3 About Korenix 145
5.4 Release History 146

1 Introduction

This user manual comprises L2 industrial ethernet switch JetNet 5500 series and L3 industrial ethernet switch JetNet 7500 series. JetNet 7520P-HVDC is the golden sample to indicate each function. The difference will be shown in chapter 1.1. For one of series cover following topics in this chapter:

- Overview
- Major Features
- Package Checklist

1.1 Overview

JetNet 7500 series or JetNet 5500 series, are designed for industrial environments in required support of medium number of access points or multiple Gigabit Ethernet ports with fewer units installed and higher density of port numbers; the ports are sharing via the wide bandwidth on-chip backplane, in shorter local transmission latency, and sufficiency upstream transmission in transportation application. The main difference between JetNet 5500 series and JetNet 7500 serise is routing functionality.

JetNet 7500 series switch comprises below combination including LVDC, HVDC, PoE and Non-PoE version. If you need L2 switch version, you can adjust the first character from “7” to “5” in below combination

L2 Switch series

Model Name	Power Input	100 Base-TX	1000 Base-T	802.3af/at	Power
	(A-Code)	(D-Code)	(X-code)	PoE	Budget
JetNet 5520P-LVDC	24 VDC	16	4	16	100 Watt
JetNet 5516P-LVDC		12		12	
JetNet 5512P-LVDC		8		8	
JetNet 5520-LVDC		16			
JetNet 5516-LVDC		12			
JetNet 5512-LVDC		8			
JetNet 5520P-HVDC	110 VDC	16		16	120 Watt
JetNet 5516P-HVDC		12		12	
JetNet 5512P-HVDC		8		8	
JetNet 5520-HVDC		16			
JetNet 5516-HVDC		12			
JetNet 5512-HVDC		8			

L3 Switch series

Model Name	Power Input (A-Code)	100 Base-TX (D-Code)	1000 Base-T (X-code)	802.3af/at PoE	Power Budget
JetNet 7520P-LVDC	24 VDC	16	4	16	100 Watt
JetNet 7516P-LVDC		12		12	
JetNet 7512P-LVDC		8		8	
JetNet 7520-LVDC		16			
JetNet 7516-LVDC		12			
JetNet 7512-LVDC		8			
JetNet 7520P-HVDC	110 VDC	16		16	120 Watt
JetNet 7516P-HVDC		12		12	
JetNet 7512P-HVDC		8		8	
JetNet 7520-HVDC		16			
JetNet 7516-HVDC		12			
JetNet 7512-HVDC		8			

The device is recommended to be wall-mount installed by using the installation kit within the shipment. If you have Din installed requirement, you can purchase it from sales. When the other switches are aggregated to JetNet 7500 series switch, the 16FE plus 4G design allows total connections up to 10 rings, with owned ring redundancy protection. This is unique high-availability design featured bases on Korenix patent-protected technology.

JetNet 7500 series switch is a fan-less-designed M12 Power over Ethernet (PoE) Switch, with 100W PoE budget(LVDC version) or 120W PoE budget (HVDC version) in compliance with IEEE 802.3af/at standard. If you have M12 L3 managed non-PoE switch demand, you can also refer to JetNet 7500 series switch. All series are designed in wide operating temperature, and dynamic DC input voltage to meet the requirement in transportation applications.

1.2 Major Features

- Up to 16 ports Fast Ethernet M12 D-Code, 4 Gigabit M12 X-Code
- Up to 16 IEEE 802.3at PSE embedded in Fast Ethernet
- Non-Blocking, High Speed Network Switching Fabric
- 2 Gigabit Ethernet interfaces support Device Fault Bypass function
- Network Redundancy – MSR (Multiple Super Ring),ITU-T G.8032 ERPS, RSTP, MSTP, Super Chain
- Fully Device Management – SNMP v1/v2c/v3, RMON, Web UI, Telnet and Local Console
- Friendly Device and Network Topology recovery utility – Korenix View, Korenix NMS
- Layer 2 Network Performance – IEEE802.1Q VLAN, Private VLAN, Trunk, Traffic Filtering, DHCP Server/Client, Traffic Prioritize, Forwarding Rate Control
- Layer 3 Network Routing Protocols – Static/Dynamic Route, VLAN Routing, Multicast Routing (JetNet 7500 series product)
- Advanced Cyber Network Security –MAC security, IEEE 802.1x Port Based access control , IEEE 802.1x Radius Server authentication, 802.1x MAB, Distributed Denial of Service (DDoS), IP Source Guard, Denial of ARP Inspection, TACACS+, RADIUS, ACL.
- IEEE 802.3 af/at support on JetNet 7500P series
- Power budget 120 Watt in HVDC series
- Power budget 100 Watt in LVDC series
- IEC-61375-2-5 Train Topology Discovery Protocol (TTDP)*
- Hardware Watchdog for System Auto-Recovery
- High Level Electromagnetic interference immunity
- Compliance with Railway EN50155:2017, EN50121-4, EN 50121-3-2, E-Mark 13 (LVDC version), Heavy Industrial EMC and CE, FCC for the Train/MRT IP Surveillance application

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

1.3 Package List

JetNet 7500 series or JetNet 5500 series product is shipped with following accessories:

1. One of JetNet 7500 or JetNet 5500 series switch
2. Mounting kits with screws
3. One Serial Console cable, M12-A-8 to DB-9
4. Quick Installation Guide

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

2 Hardware Installation

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

2.1 Hardware Introduction

2.2 Wiring Power Inputs

2.3 Wiring Earth Ground

2.4 Wiring Fast Ethernet Ports

2.5 Wiring RS-232 console cable

2.6 Bypass Fault Device in Daisy Chain or Ring

2.7 M12 USB Auto-Configuration

2.8 Wall Mounting Installation

2.9 Safety Warning

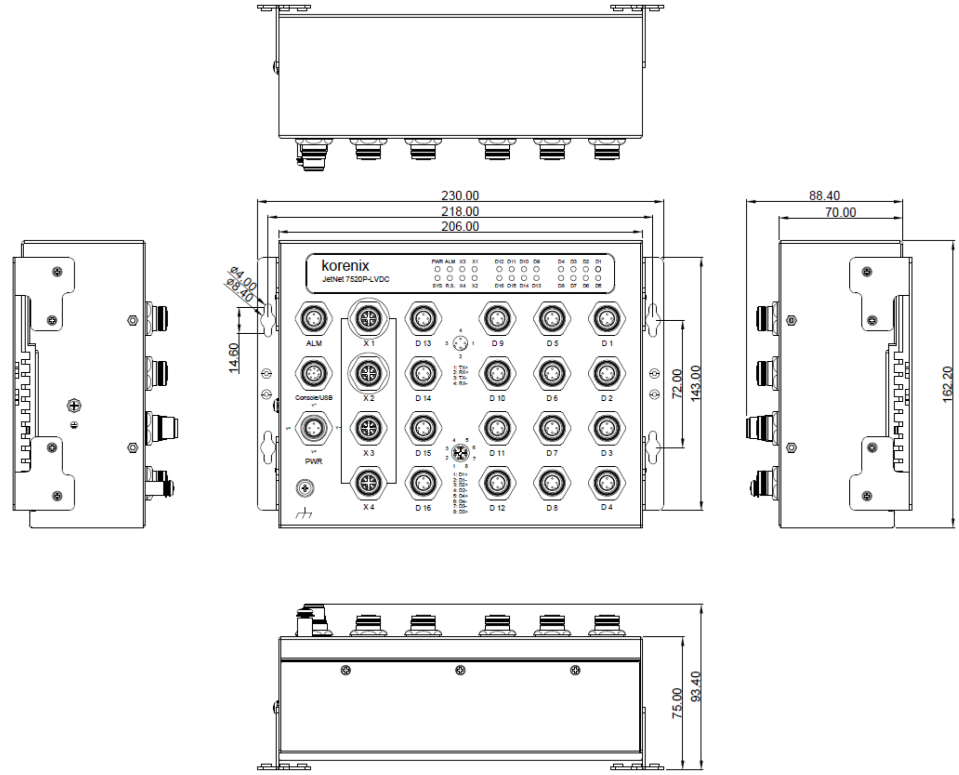
2.1 Hardware Introduction

System Diagnostic LED

- PWR (Power): Power Ready (Green On)
- ALM (Alarm): Power/Data Port abnormal (Red On)
- SYS (System): System Ready (Green On) System on Booting/Upgrade (Green Blinking)
- R.S. (Ring Status): Ring normal (Green On) Wrong ring port connected (Green Blinking) Ring abnormal (Amber On), Device ring port failed (Amber Blinking)
- Fast Ethernet (D1~D16): Link/Active (Green on / Blinking),
- Gigabit Ethernet (X1~X4): Link/Active (Green on/ Blinking)
- PoE (D1~D16, IEEE 802.3af/ Amber): Power forwarding (Amber on)
- PoE Detection (Amber Blinking) PoE (IEEE 802.3at/ Amber): Power forwarding (Amber on),PoE Detection (Amber Blinking)

Dimension (HxWxD) mm

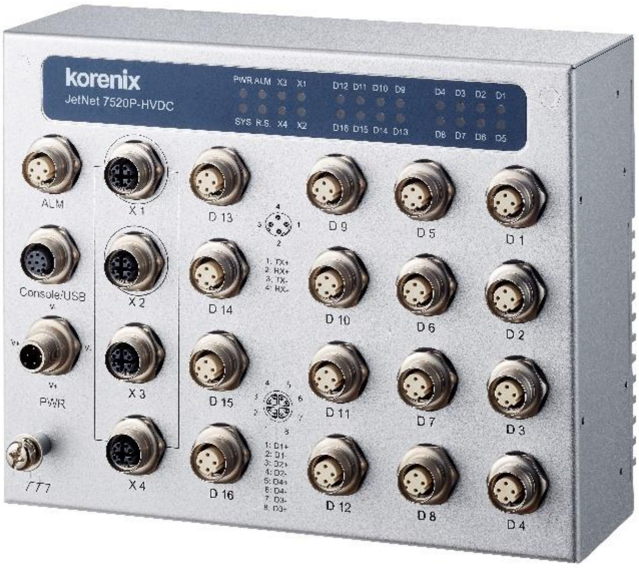
162.2 mm(H) x 206 mm (W) x 70 mm (D) without Bracket
162.2 mm(H) x 230 mm (W) x 75 mm (D) with Bracket
162.2 mm(H) x 206 mm (W) x 88.4 mm (D) from M12 to rear housing without Bracket
162.2 mm(H) x 230 mm (W) x 93.4 mm (D) from M12 to rear housing with Bracket



Panel Layout

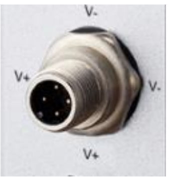
The front panel includes M12-based USB/Console Port, Fast/Gigabit Ethernet Port, Power and System/Port LEDs.

Figure of JetNet 7520P-HVDC, an Industrial ***16 FE/16 PoE, 4GbE, Managed L3 Switch***



2.2 Wiring Power Inputs

For DC power inputs.



1. Insert positive and negative wires into V+ and V- contacts respectively of the M12 connector (Plug-side).
2. Tighten the nuts to prevent the loosening of the M12 connectors while using typically M12 connector. If using a push-pull connector, please make sure the connector locked.
3. PWR input supports power redundancy and polarity- reverse protection functions.

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

1. Turn-off the power supply.
2. Connect the power wire to the Plug-side connector.
3. Plug the connector into the switch Power port.
4. Power-on the power supply.

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

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

2.3 Wiring Earth Ground

To ensure the system not being damaged by noise or any electrical shock, it is strongly recommended to assure exact connection into JetNet 7500 series with Earth Ground. To ensure the lighting/surge screw is tightened when connect the Earth Ground.

2.4 Wiring PoE/Fast/Gigabit Ethernet Ports

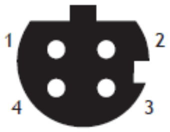
JetNet 7520 series includes **16 Fast Ethernet ports(D1~D16, M12 D-code)**, **4 M12 Gigabit Ethernet ports(X1~X4, M12 X-code),** and the PoE/ PSE function present at M12 D-Code Fast Ethernet port (D1~D16). The connectivity information of M12 and RJ-45 shown in below:

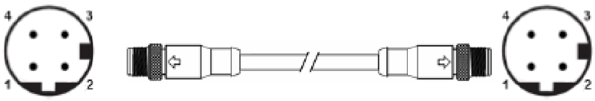
Fast Ethernet/ PoE ports, M12 D-code connector:

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

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

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

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



M12-M12 MDI

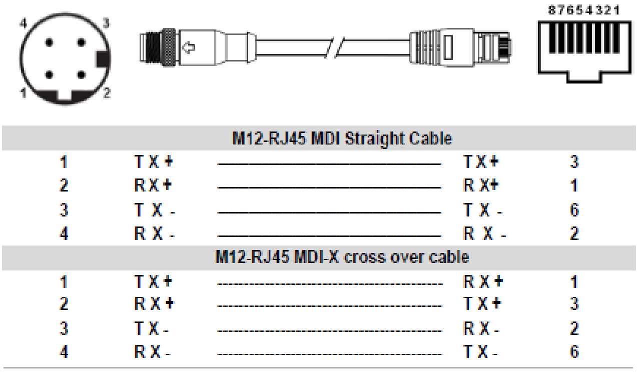
1	TX+	———	RX+	1
2	RX+	———	TX+	2
3	TX-	———	RX-	3
4	RX-	———	TX-	4

M12-M12 MDI-X

1	TX+	———	RX+	2
2	RX+	———	TX+	1
3	TX-	———	RX-	4
4	RX-	———	TX-	3

Picture 14 M12-to-M12 Ethernet Cable Wiring

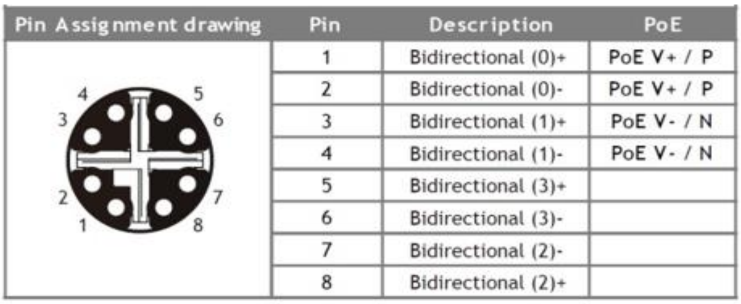
For Fast Ethernet M12-code to RJ45 connection, the pin assignment of the patch cable is shown below:



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

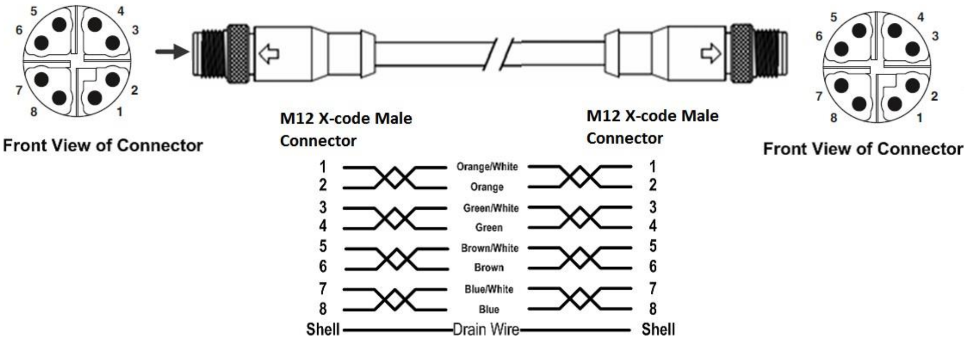
Picture 15 M12-to-RJ45 Ethernet Cable Wiring

Gigabit Ethernet ports, M12 X-code:

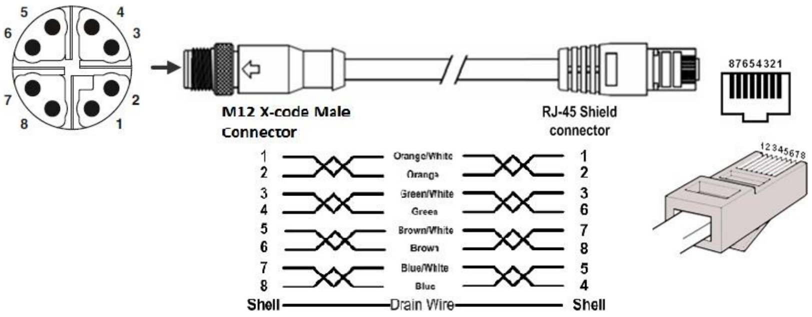


Pin Assignment drawing	Pin	Description	PoE
	1	Bidirectional (0)+	PoE V+ / P
	2	Bidirectional (0)-	PoE V+ / P
	3	Bidirectional (1)+	PoE V- / N
	4	Bidirectional (1)-	PoE V- / N
	5	Bidirectional (3)+	
	6	Bidirectional (3)-	
	7	Bidirectional (2)-	
	8	Bidirectional (2)+	

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



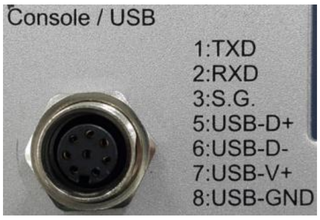
For Gigabit Ethernet M12 X-code to RJ45 connection, the pin assignment of the patch cable is shown below:



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

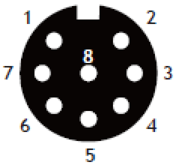
2.5 Wiring RS-232 Console Cable

JetNet 7500 series switch attached one RS-232 DB-9 to M12-A cable in the unit box. Connect the DB-9 connector to the COM port of your PC, connect M12-A to Switch's USB/Console port, open Terminal tool and set up serial settings to 115200, N,8,1. (Baud Rate: 115200 / Parity: None / Data Bit: 8 / Stop Bit: 1) Then you can access CLI interface by console able.



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

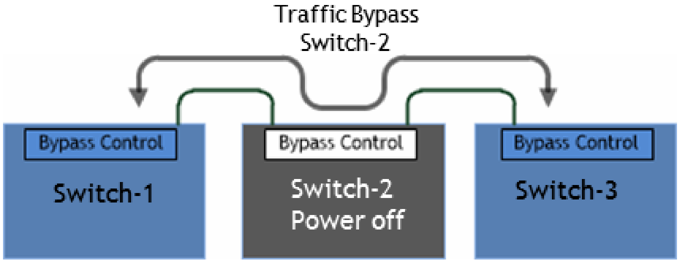
RS-232 Console

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

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

2.6 Bypass Fault Device in Daisy-Chain or Ring Topology

Auto-bypass function has been applied on X1 and X2 which mark an extra circle outside on housing for rolling stock applications. In the metro or ring network, the topology may be segmented into several fractions by one failure power node. As a result, some of the segments or nodes cannot communicate with each other. The port Bypass function can connect remote network fragments by linking uplink and downlink ports together when the Switch is powered down. With this feature, the Switch can ensure that train communication always works appropriately.



2.7 M12 USB Auto-Configuration

The JetNet 7500 series switch has enabled USB memory access function for the configuration restore/backup. The function brings benefits to the field engineers maintaining/upgrading the system without special tools or configuration knowledges. The system kernel will automatically restore the desired configuration if the

configuration files existing in the M12/USB memory stick with specified file name. It also makes the on-field Ethernet Switch replacement/ exchange process easy and friendly.

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

2. The configuration file Naming rules and respective detection behavior as below (a)Name: **AutoLoadSaveConfiguration.conf** Auto load the Configuration existed in the USB and save the configuration to the Ethernet Switch memory and apply the new configuration into system when boot up.

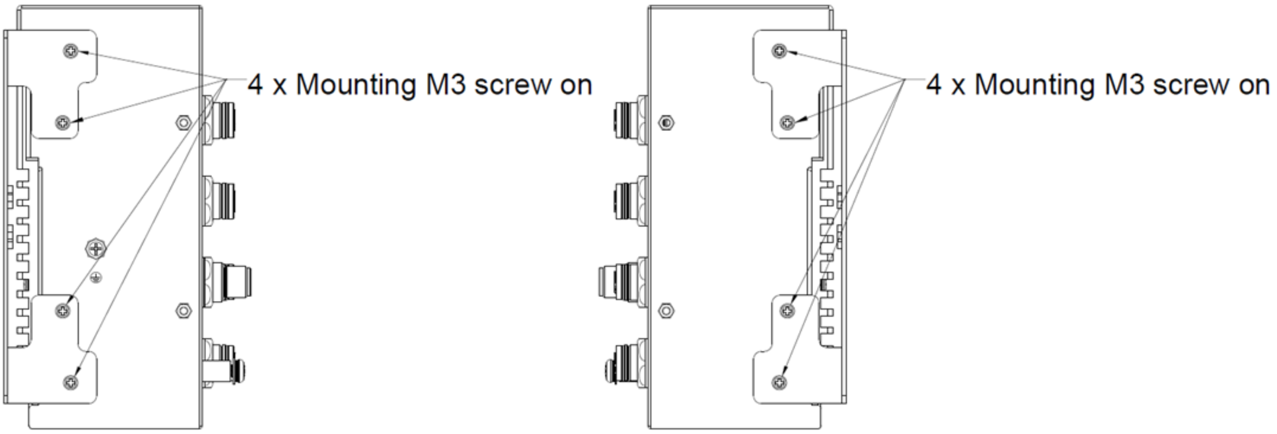
(b) Name: **AutoLoadConfiguration.conf** Auto Load Configuration and apply the configuration to Ethernet Switch without saving to memory.

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

2.8 Wall Mounting Installation

Follow the steps below to install JetNet 7500P series switch with the wall-mounting plate.

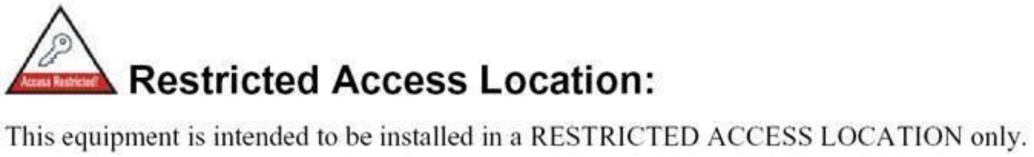
1. Install the wall-mounting plate onto the side panel of the switch.
2. Makes sure that all the screws are tightened well (M3 screw Φ5.8x0.5x6 mm-Ni) .
3. Use the hook holes at the corners of the wall mounting plate to fix the switch on the wall.



Wall Mounting Plate & Screws

2.9 Safety Warning

The Equipment intended for installation in a Restricted Access Location.


Access Restricted

Restricted Access Location:

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

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

All Ethernet cables are designed for intra-building connection to other equipment. Do not connect these ports directly to communication wiring or other wiring that exits the building where the appliance is located.

3 Preparation for Management

JetNet 7500 series Industrial Managed Switch provides both in-band and out-band configuration methods. You can configure the switch via RS232 console cable if you don't attach your admin PC to your network, or if you lose network connection to your JetNet 7500 series 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.

Following topics are covered in this chapter:

3.1 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 7500 series Switch. If the serial cable is lost, please follow the serial console cable PIN assignment to find one. (Refer to the appendix).

1. Go to Start -> Program -> Accessories -> Communication -> Hyper Terminal
2. Give a name to the new console connection.
3. Choose the COM name
4. Select correct serial settings. The serial settings of JetNet 7500P series switchesshows
   Baud Rate: 115200 / 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 1.0.0.2 (Dec 11 2019 - 10:05:37)
 Running simple memory test ..... OK
 Loading firmware .....Executing firmware ...
 Starting kernel ...
 Initializing USB Mass Storage driver...
PoE initial : OK
Port2 Link Change to UP
Port1 Link Change to UP
Port4 Link Change to UP
Port19 Link Change to UP
Port20 Link Change to UP
Loading system : Success

Switch login: admin
Password:

JetNet5520P-LVDC (version 1.0_b5-20200109-16:23:19).
Copyright 2006-2020 Korenix Technology Co., Ltd.

Switch#
```

3.2 Preparation for Web Interface

JetNet 7500 series Switch provides HTTP Web Interface and Secured HTTPS Web Interface for web management

3.2.1 Web Interface

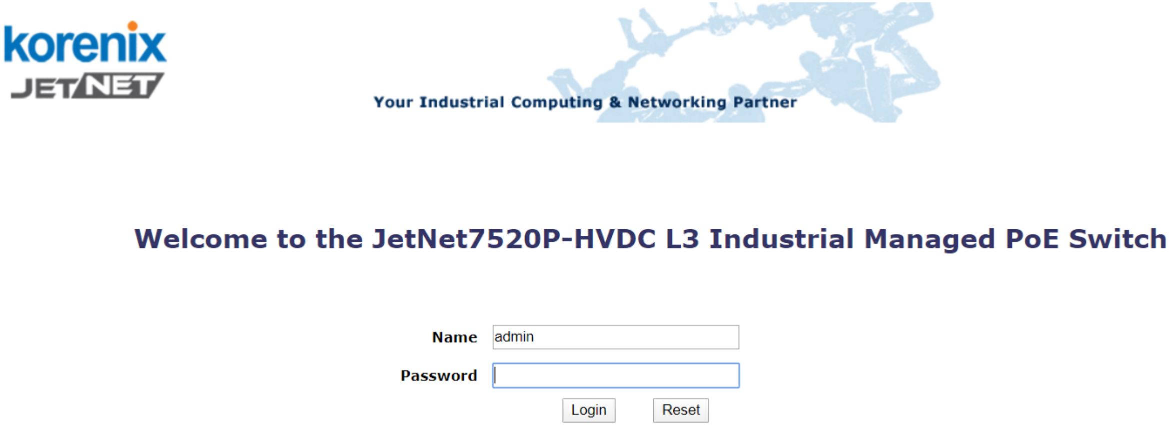
Korenix web management page is developed by CGI (Common Gateway Interface). It allows you to use a standard web-browser such as Microsoft Internet Explorer,Mozilla, and Google Chrome to configure and interrogate the switch from anywhere on the network.

Before you attempt to use the embedded web interface to manage switch operation, verify that your JetNet 7500 series 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.**



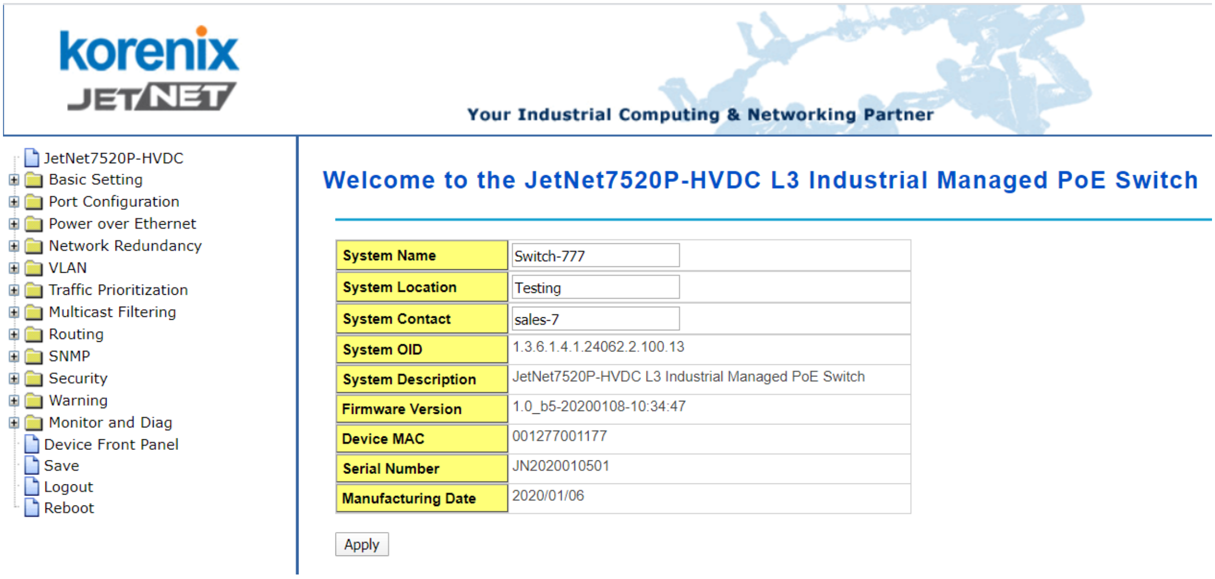
Welcome to the JetNet7520P-HVDC L3 Industrial Managed PoE Switch

Name admin

Password

<Login screen example – JetNet 7520P-HVDC>

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



Welcome to the JetNet7520P-HVDC L3 Industrial Managed PoE Switch

System Name	Switch-777
System Location	Testing
System Contact	sales-7
System OID	1.3.6.1.4.1.24062.2.100.13
System Description	JetNet7520P-HVDC L3 Industrial Managed PoE Switch
Firmware Version	1.0_b5-20200108-10:34:47
Device MAC	001277001177
Serial Number	JN2020010501
Manufacturing Date	2020/01/06

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.

3.2.2 Secured Web Interface

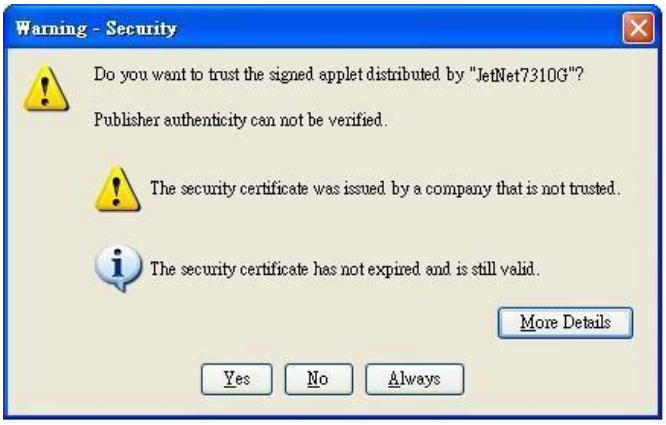
Korenix web management page also provides secured management HTTPS login. All the configuration commands will be secured and will be hard for the hackers to sniff the login password and configuration commands.

Launch the web browser and Login.

3.2.2.1 Launch the web browser on the PC.

3.2.2.2 Type https://192.168.10.1 (or the IP address of the switch). And then press **Enter**.

3.2.2.3 The popup screen will appear and request you to trust the secured HTTPS connection distributed by JetNet 7500P series first. Press **Yes** to trust it.



Do you want to trust the signed applet distributed by "JetNet7310G"?

Publisher authenticity can not be verified.

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

The security certificate has not expired and is still valid.

3.2.2.4 The login screen will appear.

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

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

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

3.3 Preparation for Telnet Console

3.3.1.1 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.

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.

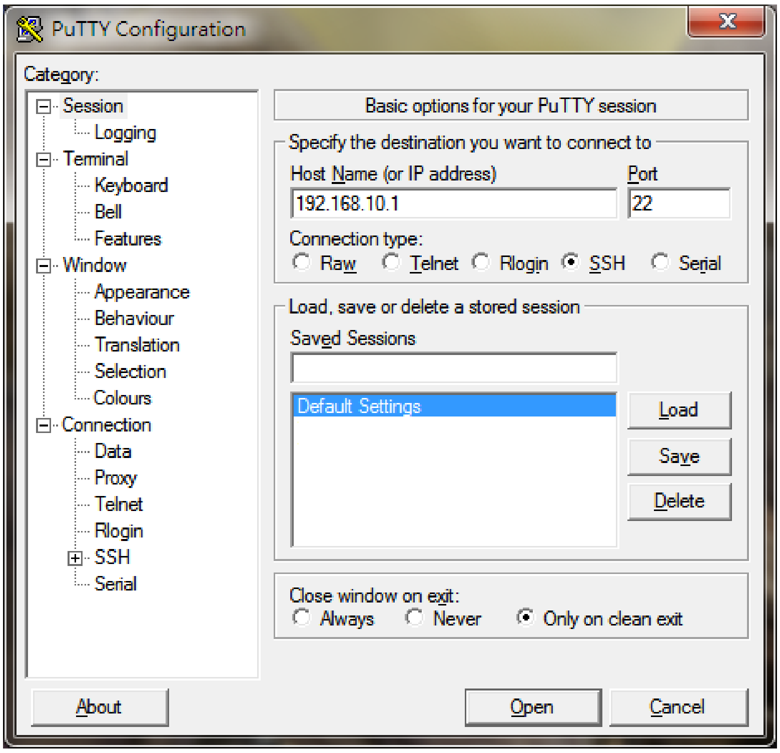
About PuTTY

PuTTY
Release 0.60

© 1997-2007 Simon Tatham. All rights reserved.

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 sessionconsole.Choose

the “Telnet” protocol.



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 192.168.10.1

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

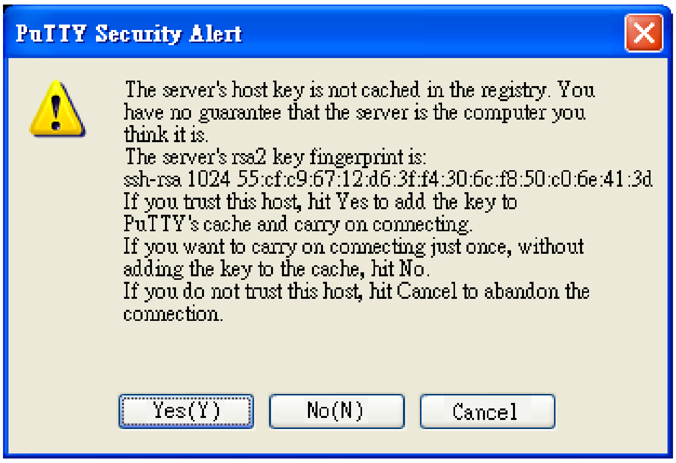
Load, save or delete a stored session

Saved Sessions

Default Settings

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

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

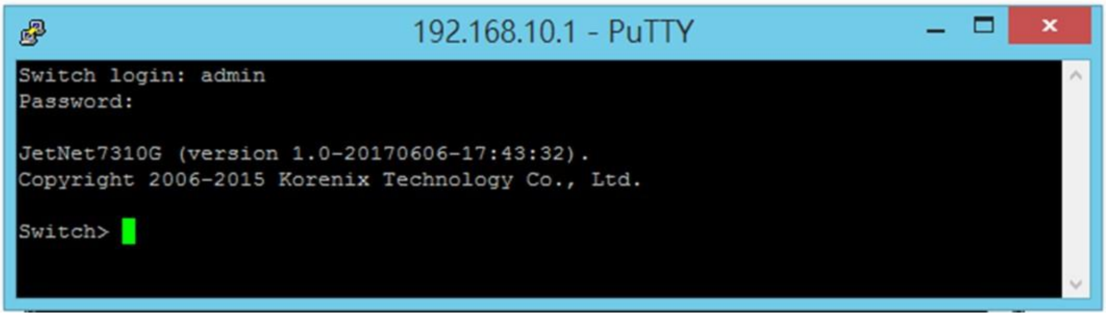


PuTTY Security Alert

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

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.



```
Switch login: admin
Password:

JetNet7310G (version 1.0-20170606-17:43:32).
Copyright 2006-2015 Korenix Technology Co., Ltd.

Switch>
```

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.

4. Feature Configuration

This chapter explains how to configure JetNet 7500 series Switch software features. There are four ways to access the switch: Serial console, Telnet, Web browser and SNMP.

JetNet 7500 series 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 7500 series 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:

4.1 Command Line Interface (CLI) Introduction

4.2 Basic Setting

4.3 Port Configuration

4.4 Power over Ethernet

4.5 Network Redundancy

4.6 VLAN

4.7 Traffic Prioritization

4.8 Multicast Filtering

4.9 Routing (JetNet 7500 series only)

4.10 SNMP

4.11 Security

4.12 Warning

4.13 Monitor and Diagnostic

4.14 Device Front Panel

4.15 Save

4.16 Logout

4.17 Reboot

4.1 Command Line Interface Introduction

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

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

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

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

```
Switch#
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')
     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
            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 then enter interface configuration mode. In this mode, you can configure port settings.

The port interface name of the fast Ethernet port is fa<Port Number>. Ex: Fast Ethernet D1 fa1, fast Ethernet D7 is fa7.

The port interface name of the Gigabit Ethernet port is gi<Port Number>. Ex: Gigabit Ethernet X1 is gi1, Gigabit Ethernet X1 is gi4. Even you apply fixed 100M speed to the Gigabit Ethernet port, the port interface name is still gi<Port Number>.

Types interface name accordingly for going to certain interface configuration mode. Type **exit**

to leave.

Type **?** to see the command list

Available command lists of the global configuration mode.

```
Switch(config)# interface fa1
Switch(config-if)#
        acceptable          Configure 802.1Q acceptable frame types of a port. auto-
        negotiation         Enable auto-negotiation state of a given port description
                            Interface specific description
        dot1x               IEEE 802.1x access security control
        duplex              Specify duplex mode of operation for a port
        end                 End current mode and change to enable mode
        ethertype           Ethertype
        exit                Exit current mode and down to previous mode
        flowcontrol         Set flow-control value for an interface
        garp                General Attribute Registration Protocol
        ip                  Interface Internet Protocol config commands
        lacp                Link Aggregation Control Protocol
        list                Print command list
        loopback            Specify loopback mode of operation for a port mac
                            MAC interface commands
        mdix                Enable mdix state of a given port
        no                  Negate a command or set its defaults
        qos                 Quality of Service (QoS)
        quit                Exit current mode and down to previous mode
        rate-limit          Rate limit configuration
        sfp                 Small    form-factor    pluggable
        shutdown            Shutdown  the  selected  interface
        spanning-tree       spanning-tree protocol
        speed               Specify the speed of a Fast Ethernet or a Gigabit Ethernet port.
        storm-control       Enables packets flooding rate limiting features
```

(VLAN) Interface Configuration: Press **interface 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	In this mode, you can	Enter: Type **interface VLAN VID**	Switch(config-vlan)#
Configuration	configure settings for specific VLAN.	in global configuration mode. Exit: Type **exit** or **Ctrl+Z** to global configuration mode. Type **end** to privileged EXEC mode.	

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

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

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

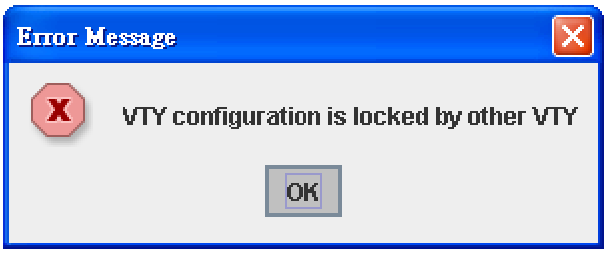
Ctrl+C To stop executing the unfinished command.

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.



VTY configuration is locked by other VTY

4.2 Basic Setting

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

Following commands are included in this group:

4.2.1 Switch Setting

4.2.2 Admin Password

4.2.3 IP Configuration

4.2.4 Time Setting

4.2.5 Jumbo Frame

4.2.6 DHCP Server

4.2.7 Backup and Restore

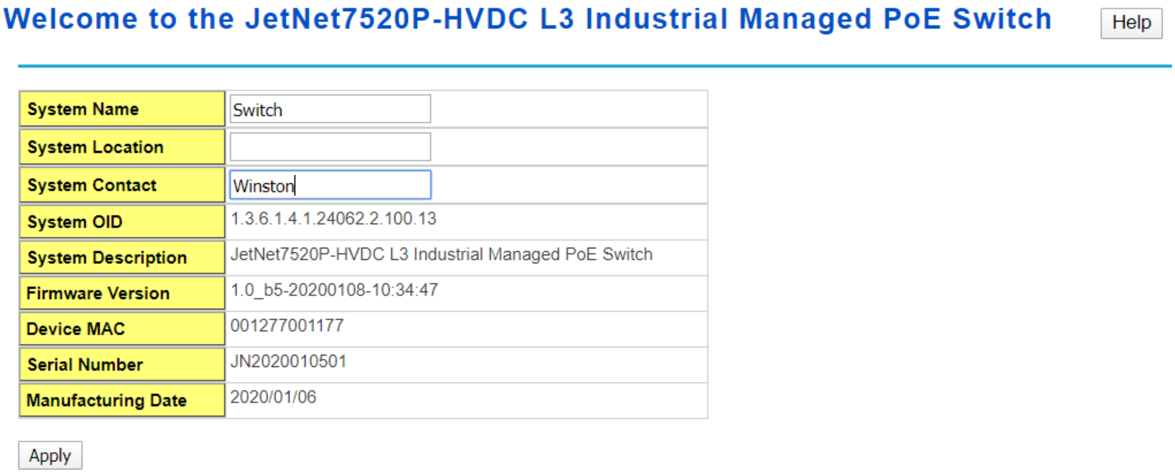
4.2.8 Firmware Upgrade

4.2.9 LoadDefault

4.2.10 CLI Commands for Basic Setting

4.2.1 Switch Setting

It allows user to assign System name, Location, Contact and view system information.



Welcome to the JetNet7520P-HVDC L3 Industrial Managed PoE Switch

System Name	Switch
System Location	
System Contact	Winston
System OID	1.3.6.1.4.1.24062.2.100.13
System Description	JetNet7520P-HVDC L3 Industrial Managed PoE Switch
Firmware Version	1.0_b5-20200108-10:34:47
Device MAC	001277001177
Serial Number	JN2020010501
Manufacturing Date	2020/01/06

< Web UI Example of the Switch Setting>

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

System Location: Specify the switch’s physical location here. The available characters you can input are 64.

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

System OID: The SNMP object ID of the switch. Follow the path to find its private MIB in MIB browser. (**Note:** When user attempt to view private MIB, please compile private MIB files into MIB browser first.)

System Description: The name of this managed product.

Firmware Version: Display the firmware versioninstalled 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:**

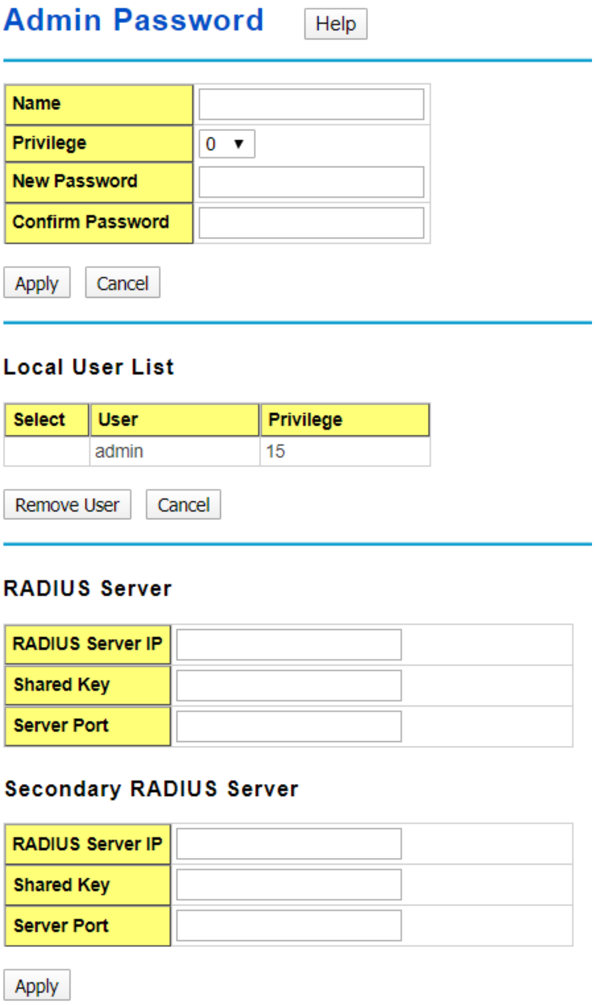
The manufacturing date of this managed product. Once the configuration has been

done, click on **Apply** to apply the settings.

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

4.2.2 Admin Password

Change the user name and the password here to enhance security.



Name	
Privilege	0 ▼
New Password	
Confirm Password	

Local User List

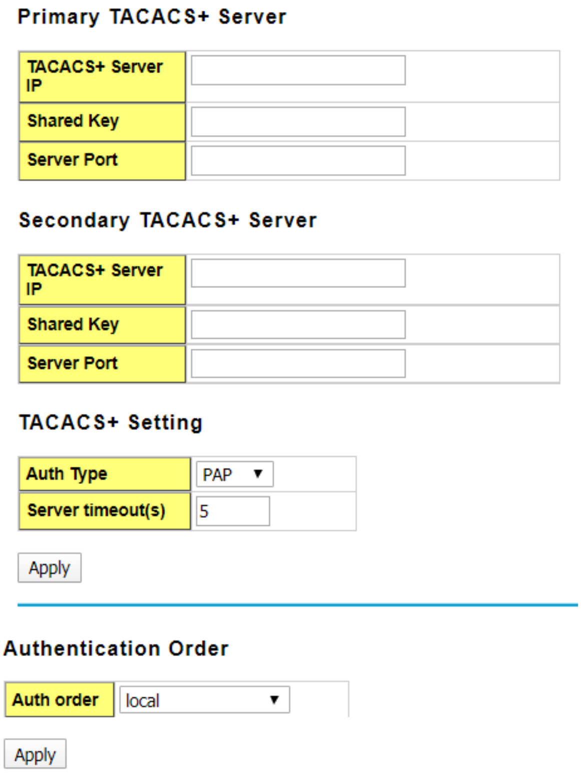
Select	User	Privilege
	admin	15

RADIUS Server

RADIUS Server IP	
Shared Key	
Server Port	

Secondary RADIUS Server

RADIUS Server IP	
Shared Key	
Server Port	



Primary TACACS+ Server

TACACS+ Server IP	
Shared Key	
Server Port	

Secondary TACACS+ Server

TACACS+ Server IP	
Shared Key	
Server Port	

TACACS+ Setting

Auth Type	PAP ▼
Server timeout(s)	5

Authentication Order

Auth order	local ▼

<Web UI of the Admin Password>

Name: Key in new user name here. The default setting is **admin**.

New Password: The default setting is **admin**, key in new password here.

Confirm Password: Type the new password again to confirm it.

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

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.

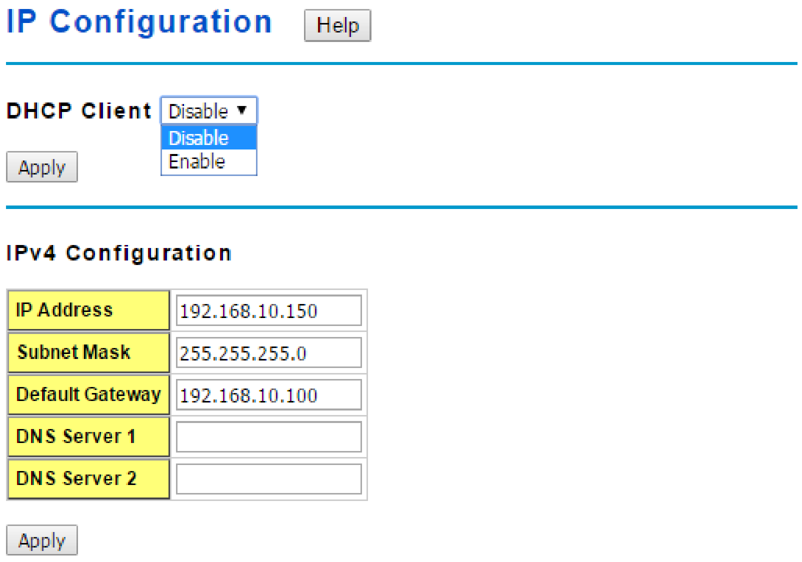
Server Port: UDP port of Radius server.

Primary TACACS+ Server/ Secondary TACACS+ Server

TACACS+ Server IP: The IP address of Radius server
Shared Key: It is the password for communicate between switch and TACACS+ Server.
Server Port: UDP port of TACACS+ server.

4.2.3 IP Configuration

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



IP Configuration

DHCP Client: Disable

IPv4 Configuration

IP Address	192.168.10.150
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.100
DNS Server 1	
DNS Server 2	

DHCP Client: 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 user specified will be used instead.

IP Address: Assign the IP address reserved by user's network for the JetNet 7500 series switch. If DHCP Client function is enabled, user don't need to assign an IP address to the JetNet 7500 series switch, as it will be overwritten by DHCP server and shown here. The default IP is 192.168.10.1.

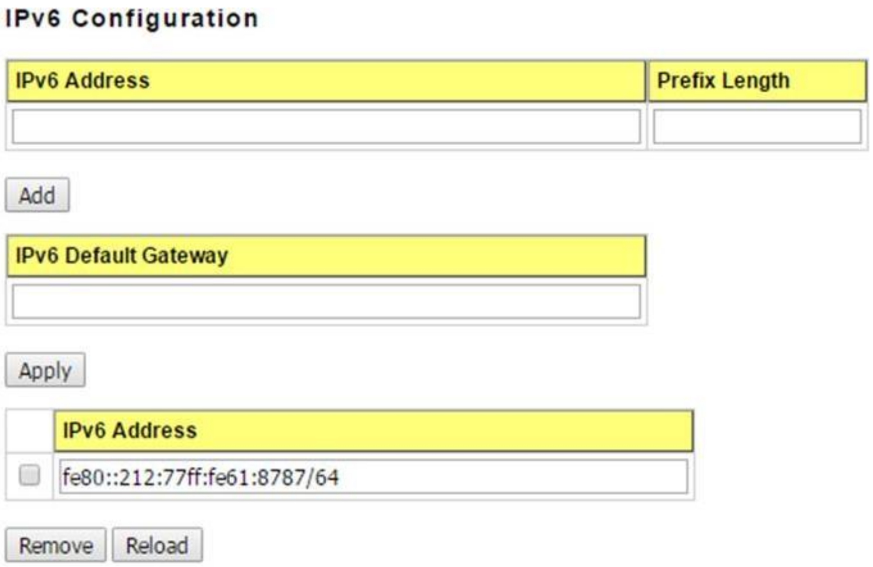
Subnet Mask: Assign the subnet mask for the IP address here. If DHCP Client function is enabled, user don't need to assign the subnet mask. The default Subnet Mask is 255.255.255.0.(**Note:** In the CLI, it use the enabled bit of the subnet mask to represent the number displayed in web UI. For example,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

Default Gateway: 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: Assign the DNS for the switch here.

Once user finish configuring the settings, click on **Apply** to apply the 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 Configuration

IPv6 Address	Prefix Length

IPv6 Default Gateway

	IPv6 Address
□	fe80::212:77ff:fe61:8787/64

IPv6 Address: Type new IPv6 address in this field.

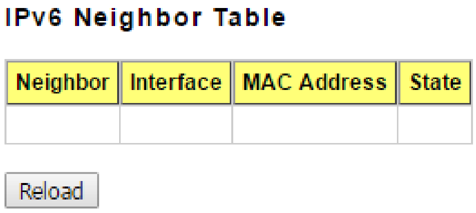
Prefix Length: The size of subnet or network, and it equivalent to the subnet mask, but written in different. The default subnet mask length is 64bits, and written in decimal value - 64.

Add: After add new IPv6 address and prefix, don’t forget click icon “**Add**” to apply new address to system.

Remove: Select existed IPv6 address and click icon “**Remove**” to delete IP address.

Reload: Refresh and reload IPv6 address listing.

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



IPv6 Neighbor Table

Neighbor	Interface	MAC Address	State

IPv6 Neighbor 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.

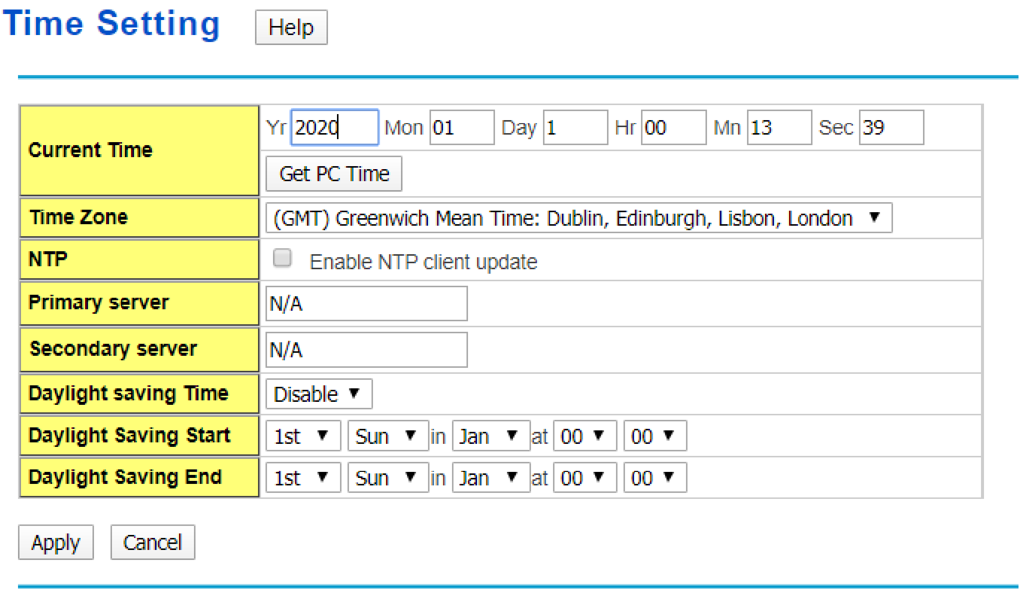
4.2.4 Time Setting

Time Setting source allow user to set the time manually or through NTP server. Network Time Protocol (NTP) is used to synchronize computer clocks on the internet. You can configure NTP settings here to synchronize the clocks of several switches on the network. Below figure is similar as JetNet 7500 series 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.

Time Setting



Time Setting

Current Time	Yr 2020 Mon 01 Day 1 Hr 00 Mn 13 Sec 39 Get PC Time
Time Zone	(GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London ▼
NTP	□ Enable NTP client update
Primary server	N/A
Secondary server	N/A
Daylight saving Time	Disable ▼
Daylight Saving Start	1st ▼ Sun ▼ in Jan ▼ at 00 ▼ 00 ▼
Daylight Saving End	1st ▼ Sun ▼ in Jan ▼ at 00 ▼ 00 ▼

The administrator can change time as the wants, it's also allowed to 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 the PC's time.

Time-zone: Select the time zone where the switch is located. Following table lists the time zones for different locations for 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) Saskatechewan
```

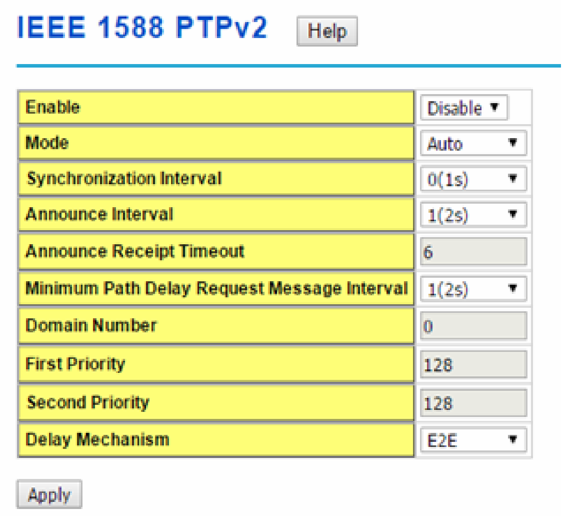
12	(GMT-05:00) Bogota, Lima, Quito
13	(GMT-05:00) Eastern Time (US & Canada)
14	(GMT-05:00) Indiana (East)
15	(GMT-04:00) Atlantic Time (Canada)
16	(GMT-04:00) Caracas, La Paz
17	(GMT-04:00) Santiago
18	(GMT-03:00) NewFoundland
19	(GMT-03:00) Brasilia
20	(GMT-03:00) Buenos Aires, Georgetown
21	(GMT-03:00) 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

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 user change Time source to NTP client. The system will send request packet to acquire current time from the NTP server that assigned by user.

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



IEEE 1588 PTPv2

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

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:

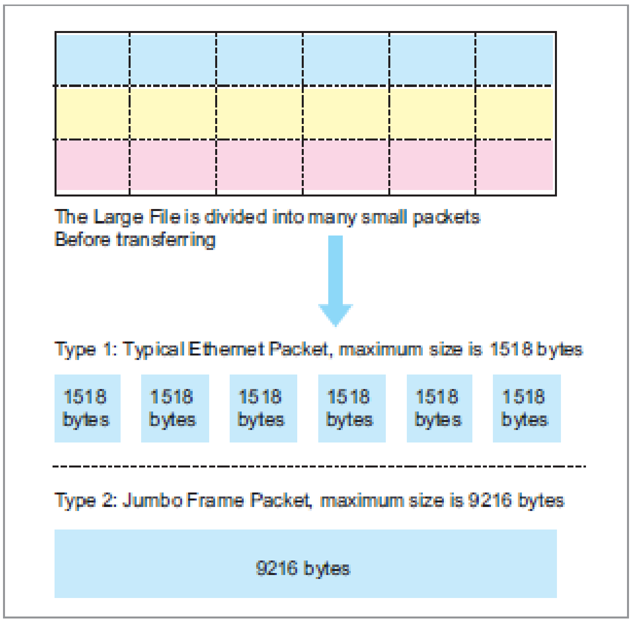
E2E: End-to-End

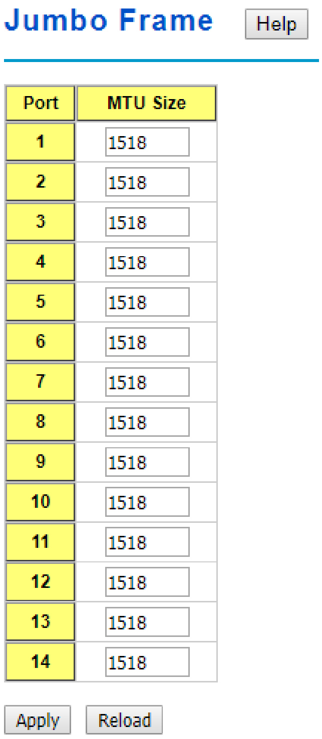
PTP: Peer-to-Peer

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

4.2.5 Jumbo Frame

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


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



Jumbo Frame

Port	MTU Size
1	1518
2	1518
3	1518
4	1518
5	1518
6	1518
7	1518
8	1518
9	1518
10	1518
11	1518
12	1518
13	1518
14	1518

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

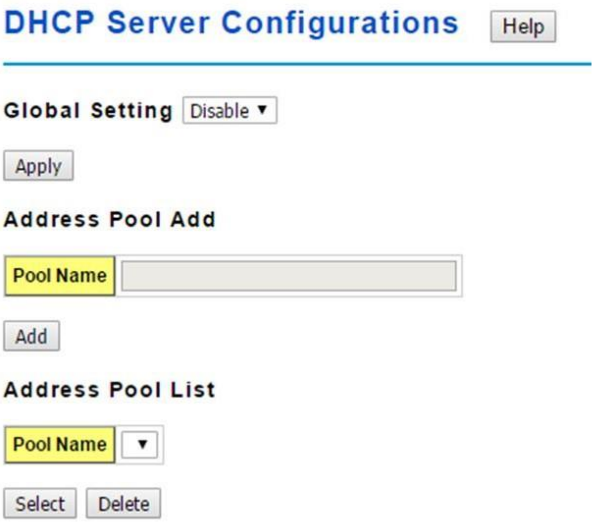
4.2.6 DHCP Server

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

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 the administrator finished the configuration, click **Apply** to activate the new configuration



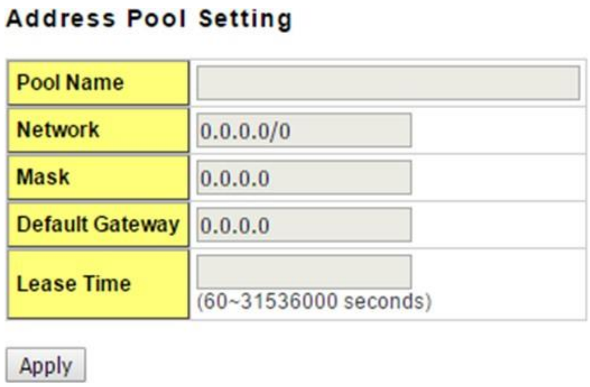
DHCP Server Configurations

Global Setting: Disable

Global Setting: Enable or disable the local DHCP server.

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

Address Pool List: Select an address pool setting here. Click the **Select** button to change address pool. Click the **Delete** button to delete the address pool.



Address Pool Setting

Pool Name	
Network	0.0.0.0/0
Mask	0.0.0.0
Default Gateway	0.0.0.0
Lease Time	(60~31536000 seconds)

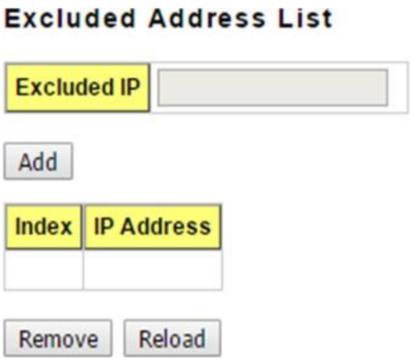
Pool Name: The address pool name.

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

Mask: The subnet mask of the network.

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

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



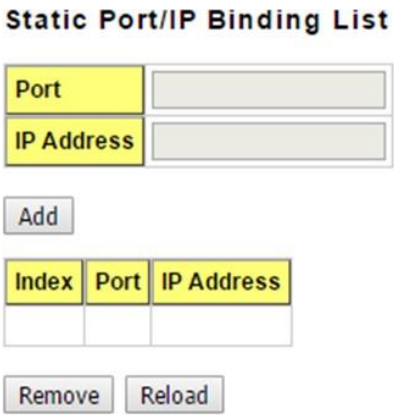
This section allows user to exclude IP addresses within the network range from being assigned to devices.

Excluded IP: An IP address that user wants 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.

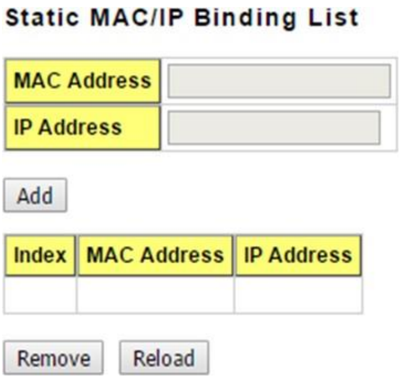
Click the **Remove** button to remove the selected IP address(es) or click the **Reload** button to reload the selected IP address(es).



This feature allows user 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 that assign the IP address to.

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

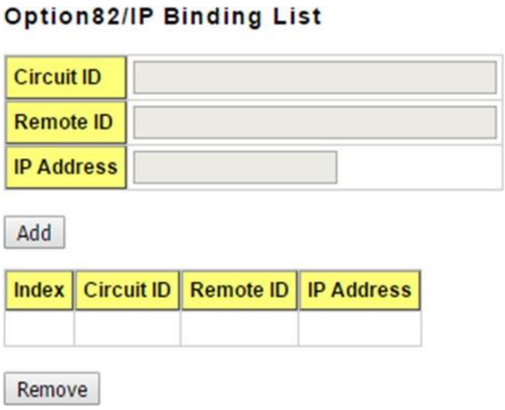


Static MAC/IP Binding List

MAC Address	
IP Address	

Index	MAC Address	IP Address

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**.



Option82/IP Binding List

Circuit ID	
Remote ID	
IP Address	

Index	Circuit ID	Remote ID	IP Address

This section 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.

The Option82/IP Binding List shows all of the configured Option 82 bindings. Click the **Remove** button to remove the selected Option82 binding(s) or click the **Reload** button to reload selected Option82 binding(s).

Index: The indexes of the Option 82 bindings.

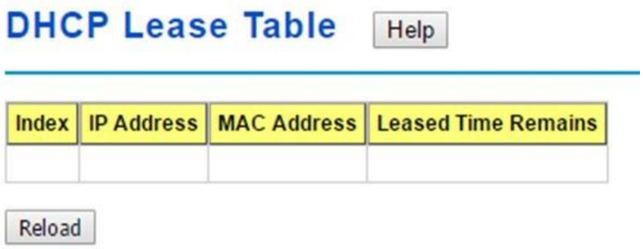
Circuit ID: The Circuit ID assigned to the IP address.

Remote ID: The Remote ID assigned to the IP address.

IP Address: The IP address the Circuit ID and Remote ID are assigned to.

Leased Entries

JetNet 7500 series Switch provides an assigned IP address list for user check. It will show the MAC and IP address that was assigned by JetNet 7500 series Switch. Click the **Reload** button to refresh the listing.



DHCP Lease Table

Index	IP Address	MAC Address	Leased Time Remains

Index: Index of the DHCP lease entry.

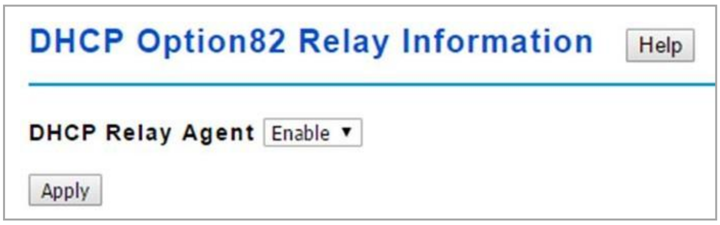
IP Address: The IP address assigned to the device that received the lease.

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 the administrator to configure DHCP Option 82 settings.

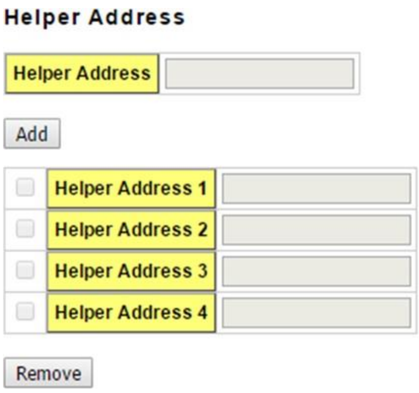


DHCP Option82 Relay Information

DHCP Relay Agent: Enable ▼

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.



Helper Address

Helper Address	

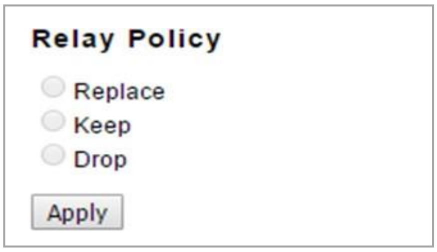
□	Helper Address 1	
□	Helper Address 2	
□	Helper Address 3	
□	Helper Address 4	

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.

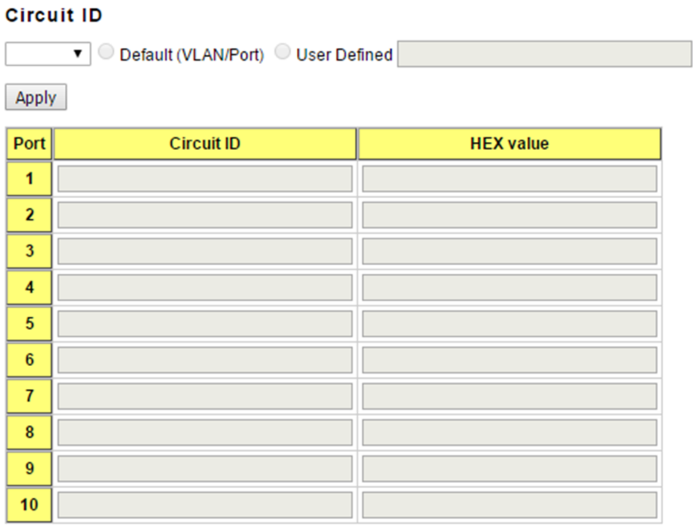
Drop: Drops the option 82 field and do not add any option 82 field.



Relay Policy

○ Replace
○ Keep
○ Drop

Circuit ID



Circuit ID

▾ ○ Default (VLAN/Port) ○ User Defined

Apply

Port	Circuit ID	HEX value
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

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.

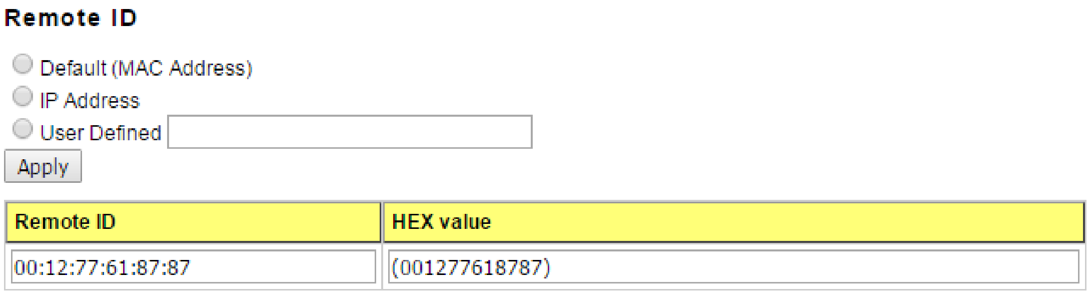
The Circuit ID table contains the following information:

Port: This is the logical port of the switch.

Circuit ID: The Circuit ID includes information specific to which circuit the request camein 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



Remote ID

○ Default (MAC Address)

○ IP Address

○ User Defined

Apply

Remote ID	HEX value
00:12:77:61:87:87	(001277618787)

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.

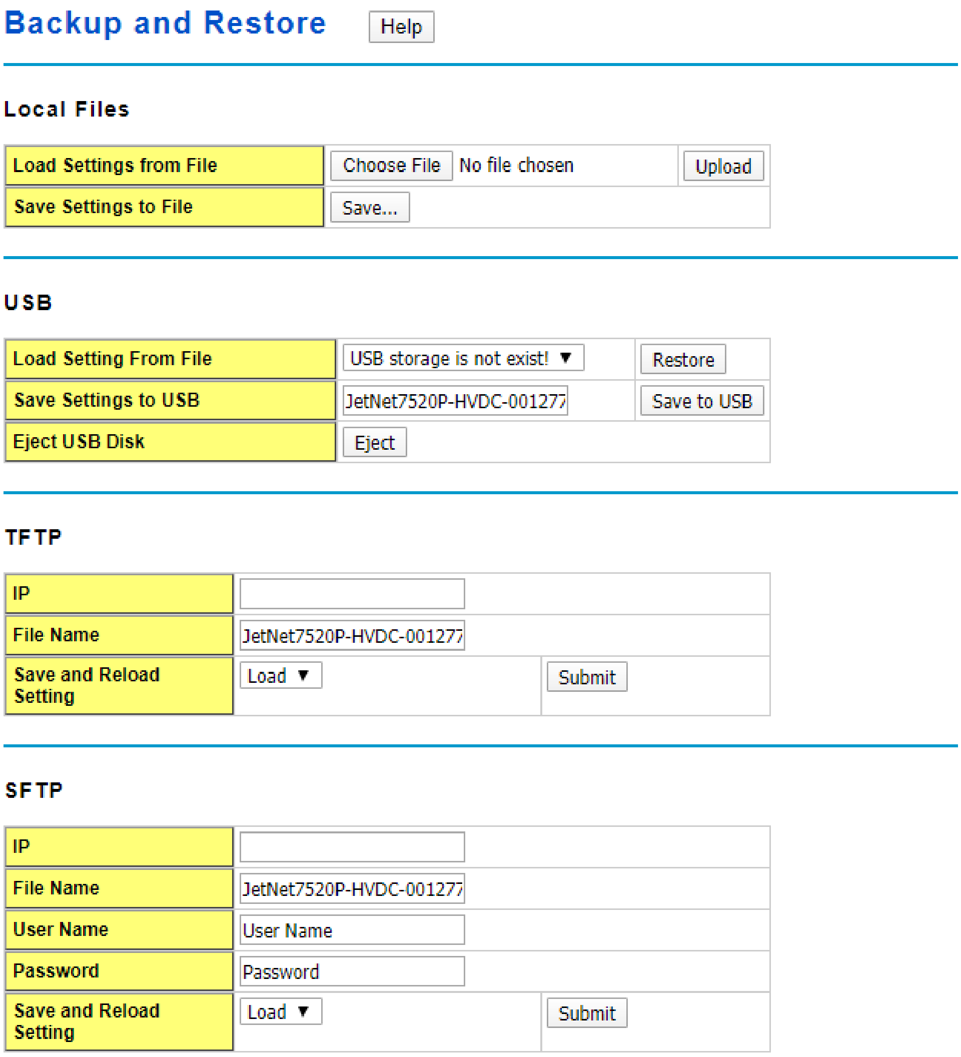
Remote ID: The Remote-ID carries information relating to the remote host end of the circuit, which is the MAC address of the relay.

HEX value: HEX value of the Remote ID.

4.2.7 Backup and Restore

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

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



Backup and Restore

Local Files

Load Settings from File	Choose File No file chosen	Upload
Save Settings to File	Save...	

USB

Load Setting From File	USB storage is not exist! ▼	Restore
Save Settings to USB	JetNet7520P-HVDC-001277	Save to USB
Eject USB Disk	Eject	

TFTP

IP		
File Name	JetNet7520P-HVDC-001277	
Save and Reload Setting	Load ▼	Submit

SFTP

IP		
File Name	JetNet7520P-HVDC-001277	
User Name	User Name	
Password	Password	
Save and Reload Setting	Load ▼	Submit

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.

USB

This section allows you to upload or save a configuration file that is stored in USB.

Load Setting From File: Click the **Browse...** button to select a configuration from USB.

Save Settings to USB: Click the **Save to USB** button to save current configuration to USB.

Eject USB Disk: Click the **Eject** button to eject USB.

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 the **Submit** button 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.

User Name: This is the user name for SFTP connection.

Password: This is the password for SFTP connection.

Load/Save Settings:

Select **Load** to load the configuration from the SFTP server onto the switch.

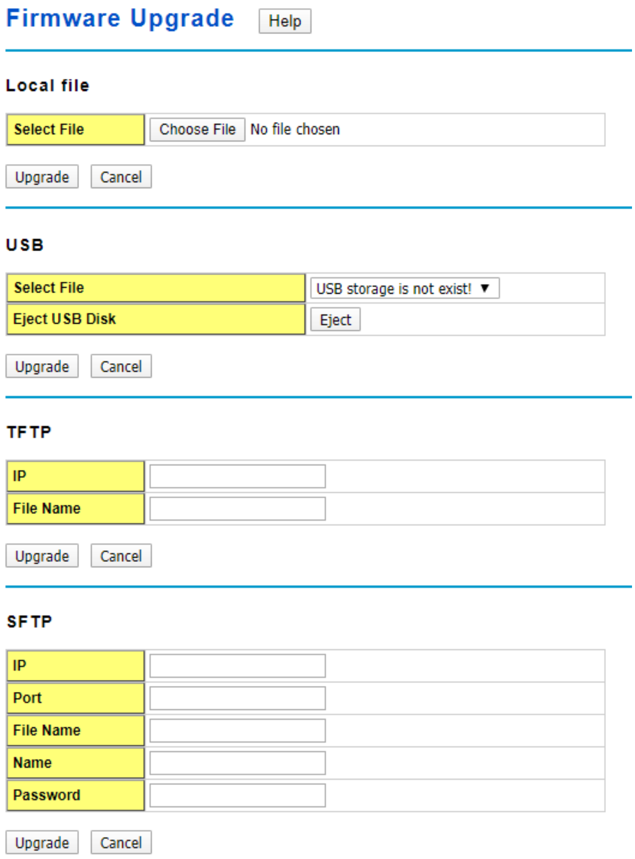
Select **Save** to save the configuration on the switch to the SFTP server.

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

4.2.8 Firmware Upgrade

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

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



Firmware Upgrade

Local file

Select File	Choose File No file chosen

USB

Select File	USB storage is not exist! ▼
Eject USB Disk	Eject

TFTP

IP	
File Name	

SFTP

IP	
Port	
File Name	
Name	
Password	

Local File

This section allows an administrator to upload a firmware image that is stored locally on computer.

Select File: Click the **Browse...** button to select a firmware image from your computer.

Click the **Upgrade** button to begin upgrading the firmware or click the **Cancel** button to clear the selected file. After the firmware has upgraded the switch will reboot automatically.

USB

This section allows you to upload a firmware image that is stored in USB.

Select File: Click the **Browse...** button to select a firmware image from USB.

Eject USB Disk: Click the **Eject** button to eject USB.

Click the **Upgrade** button to begin upgrading the firmware or click the **Cancel** button to clear the selected file. After the firmware has upgraded the switch will reboot automatically.

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 the **Upgrade** button to begin upgrading the firmware or click the **Cancel** button to clear the entered IP address and firmware file name. After the firmware has upgraded the switch will reboot automatically.

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: This is the Port of the SFTP server

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

Name: Name for SFTP connection

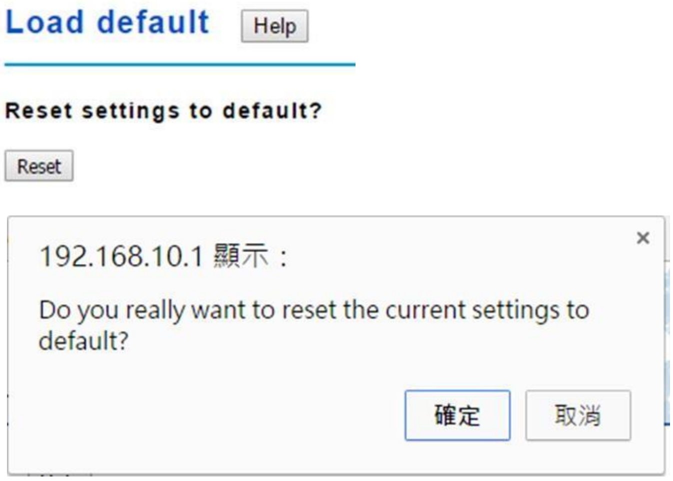
Password: Password for the SFTP connection

Click the **Upgrade** button to begin upgrading the firmware or click the **Cancel** button to clear the entered IP address and firmware file name. After the firmware has upgraded the switch will reboot automatically.

4.2.9 Load Default

In this section, an administrator can reset all the configurations of the switch to default setting. Click on **Reset** the system will then reset all configurations to default setting. The system will pop up message in a window after this command is accepted by the switch. Default setting will work effectively after rebooting the switch.

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



Load default Help

Reset settings to default?

Reset

192.168.10.1 顯示：

Do you really want to reset the current settings to default?

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

4.2.10 CLI Commands for Basic Setting

Feature	Command Line
Switch Setting	
System Name	Switch(config)# hostname WORD Network name of this system Switch(config)# hostname JetNet 7520P- HVDC 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 : (Refer to JN7714G) Product Name : JetNet7520P-HVDC Serial Number : 001277ff0004 MAC Address :001277FF0004 Manufacturing Date : 2020/03/02

	Software Information : Loader Version : 1.0.0.2 Firmware Version : 1.0-20170606-17:43:32 System OID : 1.3.6.1.4.1.24062.2.3.14 Copyright 2006-2015 Korenix Technology Co., Ltd. Switch# show hardware led led information mac macaddress Switch# show hardware mac MAC Address : 00:12:77:FF:01:B0 Switch# show hardware led Power 1 : On Power 2 : Off Alarm 1 : Off RDY : On RM : Off RF : Off
Admin Password	
User Name and Password	Switch(config)# administrator NAME Administrator account name Switch(config)# administrator orwell PASSWORD Administrator account password Switch(config)# administrator orwell orwell Change administrator account orwell and password orwell success.
Display	Switch# show administrator Administrator account information name: 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
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 Address 192.168.10.123 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 JN7520P-HVDC.bin Firmware upgrading, don’t turn off the switch! Tftping file JN7520P-HVDC.bin Firmware upgrading …………………………………………………………………… …………………………………………………………………… ……………………… Firmware upgrade success!! Rebooting.......
Factory Default	
Factory Default	Switch# reload default-config file Reload OK! Switch# reboot
System Reboot	
Reboot	Switch# reboot

4.3 Port Configuration

Port Configuration group enables an administrator 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 the administrator to view port status and aggregation information.

Following commands are included in this group:

4.3.1 Understand the port mapping

4.3.2 Port Control

4.3.3 Port Status

4.3.4 Rate Control

4.3.5 Storm Control

4.3.6 Port Trunking

4.3.7 Command Lines for Port Configuration

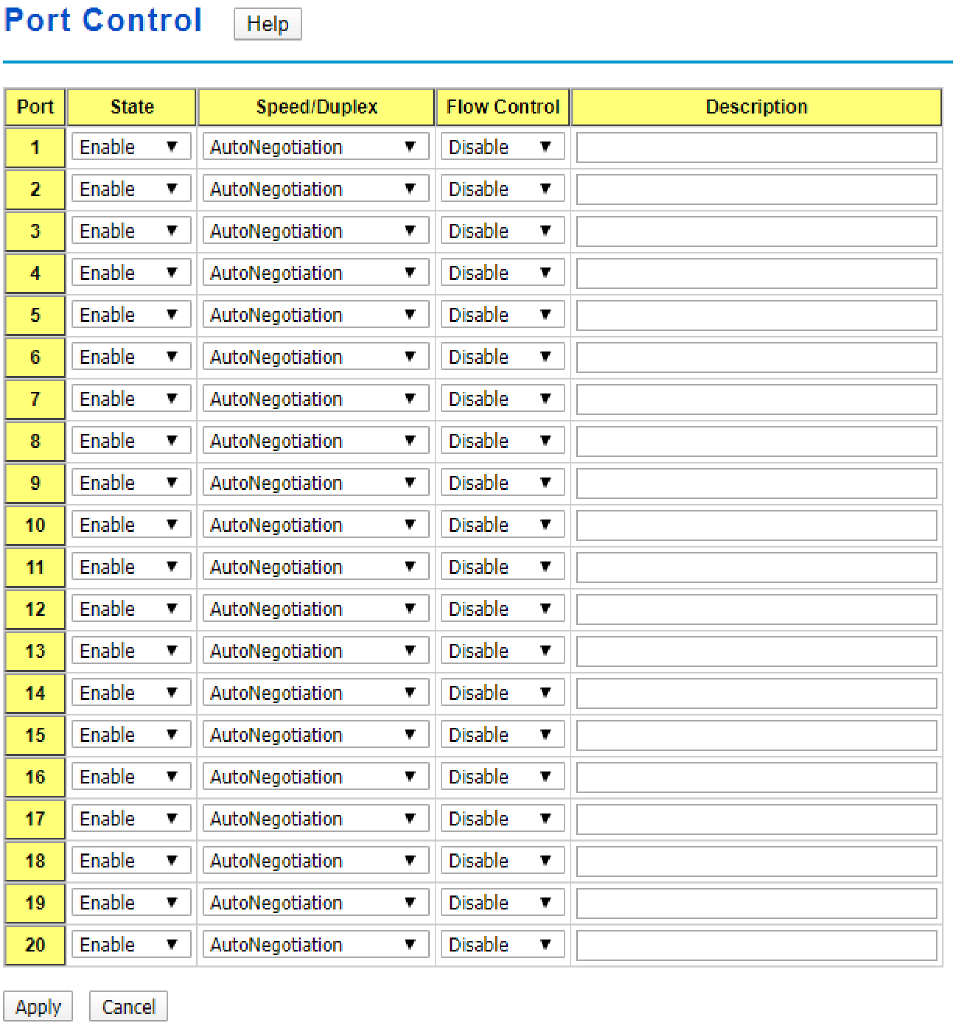
4.3.1 Understand the port mapping

Before the port setting, please check the port allocation of JetNet 7520 series switch before deployment. The port number is indicated as printing number on the front panel. Follow the port ID to configure JetNet 7520 series switch.

There are 16 Fast Ethernet ports and 4 Gigabit Ethernet ports. In Web UI, the port number is available from port D1~16 represents Fast Ethernet ports, and Port X1~X4 are referred for Gigabit Ethernet ports. In CLI, fa1, fa2…fa16 represent Fast Ethernet ports and gi17, gi18… gi20 represent Gigabit Ethernet ports.

4.3.2 Port Control

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



Port Control

Port	State	Speed/Duplex	Flow Control	Description
1	Enable ▼	AutoNegotiation ▼	Disable ▼	
2	Enable ▼	AutoNegotiation ▼	Disable ▼	
3	Enable ▼	AutoNegotiation ▼	Disable ▼	
4	Enable ▼	AutoNegotiation ▼	Disable ▼	
5	Enable ▼	AutoNegotiation ▼	Disable ▼	
6	Enable ▼	AutoNegotiation ▼	Disable ▼	
7	Enable ▼	AutoNegotiation ▼	Disable ▼	
8	Enable ▼	AutoNegotiation ▼	Disable ▼	
9	Enable ▼	AutoNegotiation ▼	Disable ▼	
10	Enable ▼	AutoNegotiation ▼	Disable ▼	
11	Enable ▼	AutoNegotiation ▼	Disable ▼	
12	Enable ▼	AutoNegotiation ▼	Disable ▼	
13	Enable ▼	AutoNegotiation ▼	Disable ▼	
14	Enable ▼	AutoNegotiation ▼	Disable ▼	
15	Enable ▼	AutoNegotiation ▼	Disable ▼	
16	Enable ▼	AutoNegotiation ▼	Disable ▼	
17	Enable ▼	AutoNegotiation ▼	Disable ▼	
18	Enable ▼	AutoNegotiation ▼	Disable ▼	
19	Enable ▼	AutoNegotiation ▼	Disable ▼	
20	Enable ▼	AutoNegotiation ▼	Disable ▼	

Select the port that needs to be configured and make changes.

State: Enable or disable the state of this port. Once the administrator 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: Configure port speed and duplex mode of each port. It allows manually configure the 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.

Flow control:

Enable means that the administrator need to activate the flow control function of the remote network device in order to let the flow control of that corresponding port on the switch to work. Disable (default) means the administrator 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.

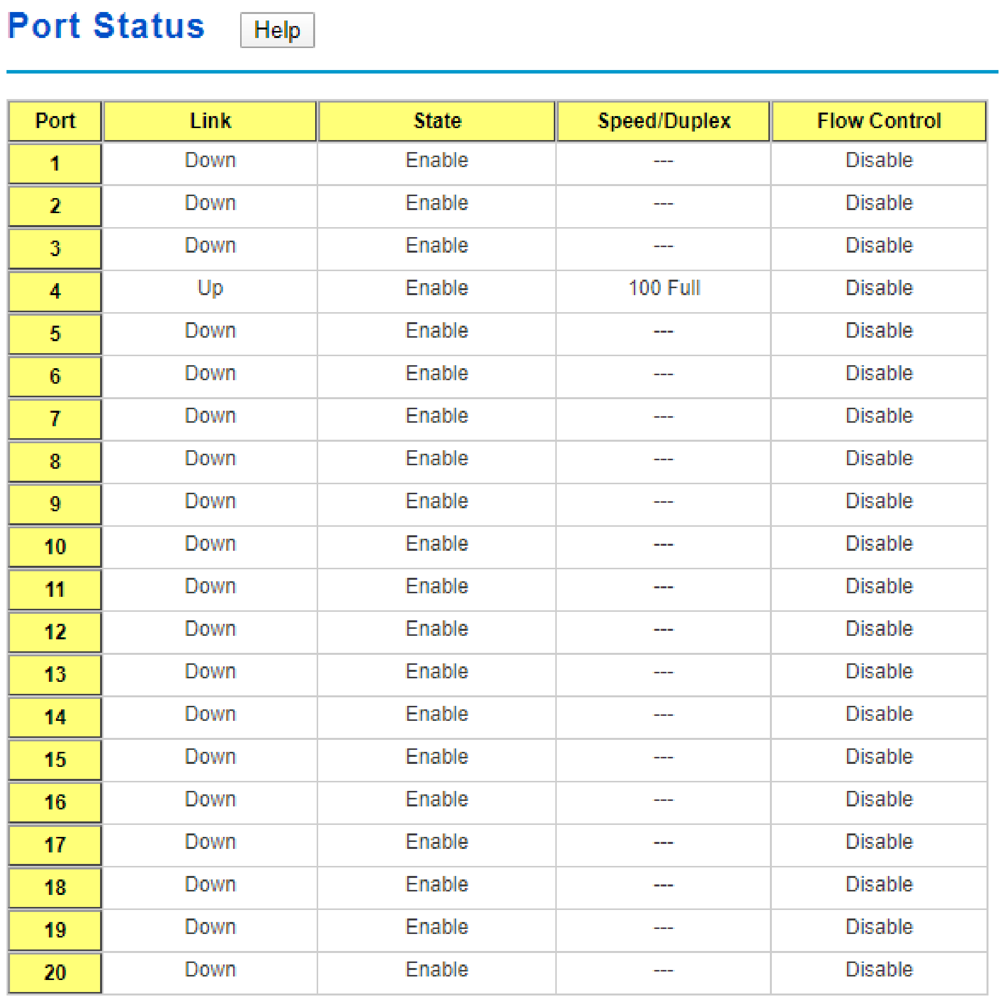
Description: The description of interface.

Click **Apply** to apply the settings.

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

4.3.3 Port Status

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



Port	Link	State	Speed/Duplex	Flow Control
1	Down	Enable	---	Disable
2	Down	Enable	---	Disable
3	Down	Enable	---	Disable
4	Up	Enable	100 Full	Disable
5	Down	Enable	---	Disable
6	Down	Enable	---	Disable
7	Down	Enable	---	Disable
8	Down	Enable	---	Disable
9	Down	Enable	---	Disable
10	Down	Enable	---	Disable
11	Down	Enable	---	Disable
12	Down	Enable	---	Disable
13	Down	Enable	---	Disable
14	Down	Enable	---	Disable
15	Down	Enable	---	Disable
16	Down	Enable	---	Disable
17	Down	Enable	---	Disable
18	Down	Enable	---	Disable
19	Down	Enable	---	Disable
20	Down	Enable	---	Disable

Select the port being configured and make changes to the port.

In **State** column, the selected port can be enabled or disabled. Once the port disabled, the port linkage is down and stop to forward any traffic. The default setting is Enable which all the ports are taken in functional upon transmission and receiving.

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

Fast Ethernet D1~D16 (fa1~fa16): AutoNegotiation, 10Mb Full Duplex(10 Full), 10Mb Half Duplex(10 Half), 100Mb Full Duplex(100 Full) and 100Mb Half Duplex(100 Half).

Gigabit Ethernet X1~X4 (gi17~gi20): AutoNegotiation, 100Mb Full Duplex(100 Full), 100Mb Half Duplex(100 Half), 1000Mb Full Duplex(1000 Full), 1000Mb Half Duplex(1000 Half).

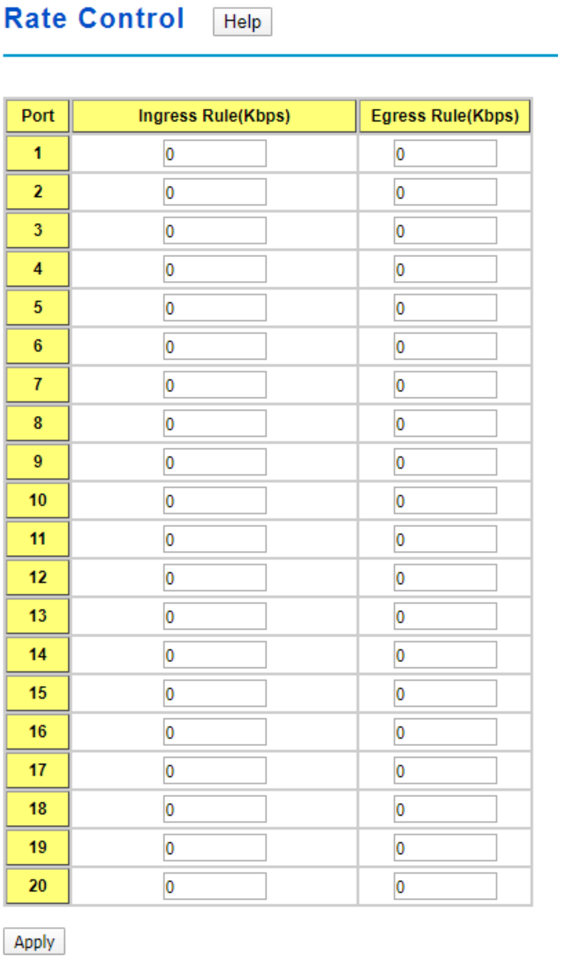
The default is recommended and set to Auto Negotiation mode. In **Flow Control** column, in order to enable flow control, **"Symmetric"** strategy on both ends of the ports connection must be both applied on local and remote devices, correspondingly. If **"Disable"** is set on ONLY either one end, it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

Once the configuration is completed, click on **Apply** to save the configuration.

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

4.3.4 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.



Rate Control

Port	Ingress Rule(Kbps)	Egress Rule(Kbps)
1	0	0
2	0	0
3	0	0
4	0	0
5	0	0
6	0	0
7	0	0
8	0	0
9	0	0
10	0	0
11	0	0
12	0	0
13	0	0
14	0	0
15	0	0
16	0	0
17	0	0
18	0	0
19	0	0
20	0	0

The ports support port ingress and egress rate control.

Ingress Rule(Kbps): Ingress rate in Kbps, the rate range is from 64 to 1000000 Kbps and zero means no limit. The rate automatically converts to a multiple of 64 Kbps value. The default value is no limit.

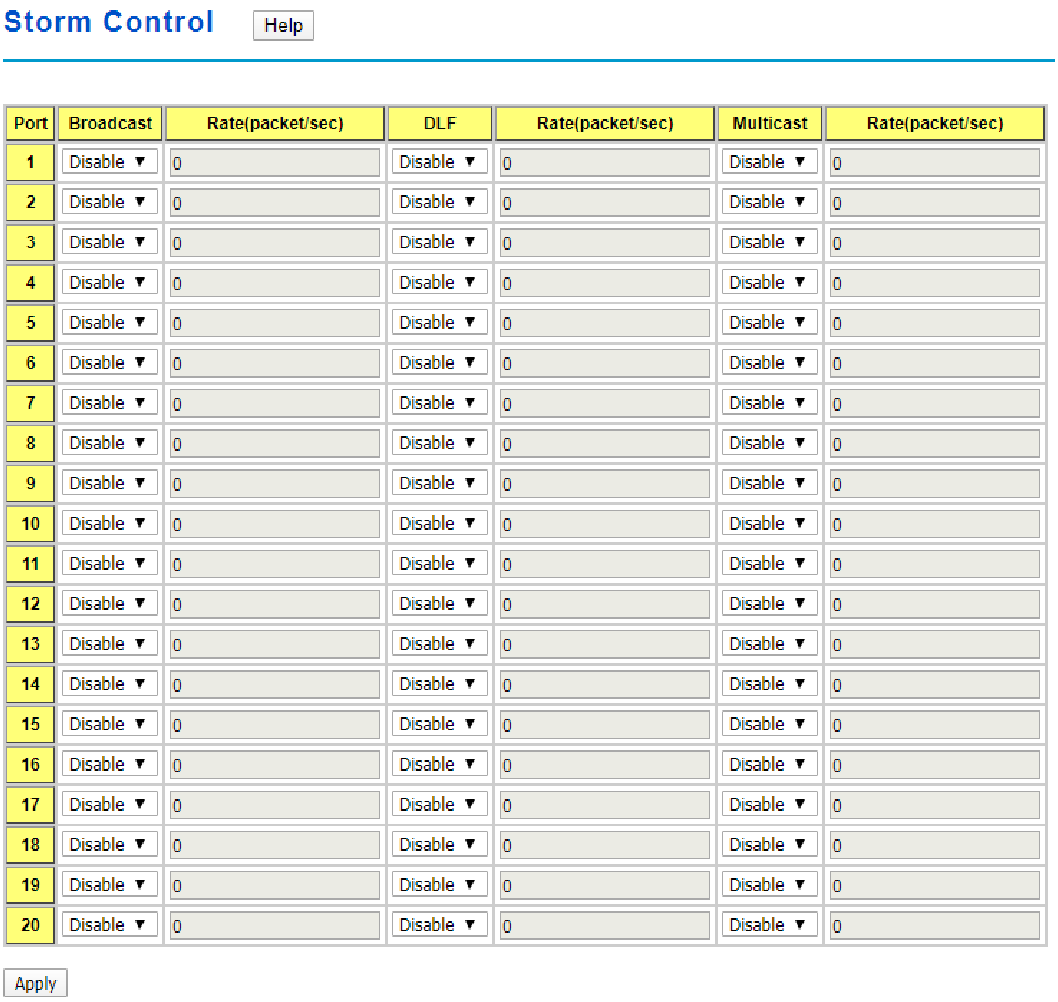
Egress Rule(Kbps): Egress rate in Kbps, the rate range is from 64 to 1000000 Kbps and zero means no limit. The rate will automatically convert to a multiple of 64 Kbps value. The default value is no limit.

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.

4.3.5 Storm Control

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



Port	Broadcast	Rate(packet/sec)	DLF	Rate(packet/sec)	Multicast	Rate(packet/sec)
1	Disable ▼	0	Disable ▼	0	Disable ▼	0
2	Disable ▼	0	Disable ▼	0	Disable ▼	0
3	Disable ▼	0	Disable ▼	0	Disable ▼	0
4	Disable ▼	0	Disable ▼	0	Disable ▼	0
5	Disable ▼	0	Disable ▼	0	Disable ▼	0
6	Disable ▼	0	Disable ▼	0	Disable ▼	0
7	Disable ▼	0	Disable ▼	0	Disable ▼	0
8	Disable ▼	0	Disable ▼	0	Disable ▼	0
9	Disable ▼	0	Disable ▼	0	Disable ▼	0
10	Disable ▼	0	Disable ▼	0	Disable ▼	0
11	Disable ▼	0	Disable ▼	0	Disable ▼	0
12	Disable ▼	0	Disable ▼	0	Disable ▼	0
13	Disable ▼	0	Disable ▼	0	Disable ▼	0
14	Disable ▼	0	Disable ▼	0	Disable ▼	0
15	Disable ▼	0	Disable ▼	0	Disable ▼	0
16	Disable ▼	0	Disable ▼	0	Disable ▼	0
17	Disable ▼	0	Disable ▼	0	Disable ▼	0
18	Disable ▼	0	Disable ▼	0	Disable ▼	0
19	Disable ▼	0	Disable ▼	0	Disable ▼	0
20	Disable ▼	0	Disable ▼	0	Disable ▼	0

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.

4.3.6 Port Trunking

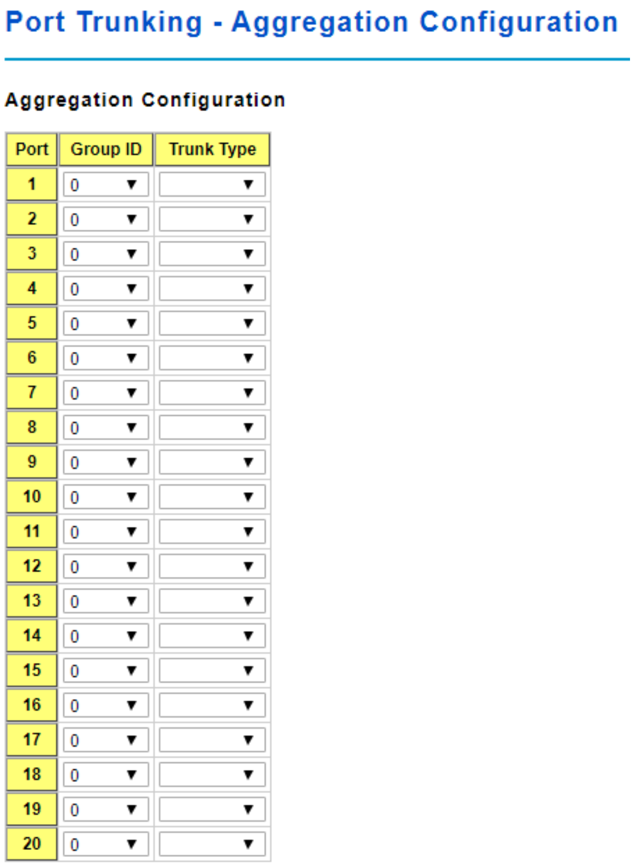
Port Trunking configuration allows an administrator to group multiple Ethernet ports in parallel to increase link bandwidth. The aggregated ports can be viewed as one physical port so that the bandwidth is higher than merely one single Ethernet port. The member ports of the same trunk group can balance the loading and backup for each other. Port Trunking feature is usually used when an administrator need higher bandwidth for backbone network. This is an inexpensive way for the administrator 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, an administrator **should** assign 802.3ad LACP to the trunk. When the other end uses non-802.3ad, the administrator can then use Static Trunk. **In practical, the Static Trunk is suggested.**

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

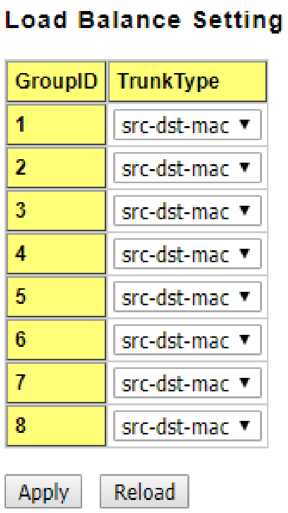
Aggregation Setting



Port Trunking - Aggregation Configuration

Aggregation Configuration

Port	Group ID	Trunk Type
1	0 ▼	▼
2	0 ▼	▼
3	0 ▼	▼
4	0 ▼	▼
5	0 ▼	▼
6	0 ▼	▼
7	0 ▼	▼
8	0 ▼	▼
9	0 ▼	▼
10	0 ▼	▼
11	0 ▼	▼
12	0 ▼	▼
13	0 ▼	▼
14	0 ▼	▼
15	0 ▼	▼
16	0 ▼	▼
17	0 ▼	▼
18	0 ▼	▼
19	0 ▼	▼
20	0 ▼	▼



Load Balance Setting

GroupID	TrunkType
1	src-dst-mac ▼
2	src-dst-mac ▼
3	src-dst-mac ▼
4	src-dst-mac ▼
5	src-dst-mac ▼
6	src-dst-mac ▼
7	src-dst-mac ▼
8	src-dst-mac ▼

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, the administrator should assign 802.3ad LACP to the trunk. When the other end uses non-802.3ad, the administrator can then use Static Trunk.

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

src-mac load distribution is based on the source MAC address

dst-mac load distribution is based on the destination-MAC address

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

src-ip load distribution is based on the source IP address

dst-ip load distribution is based on the destination IP address

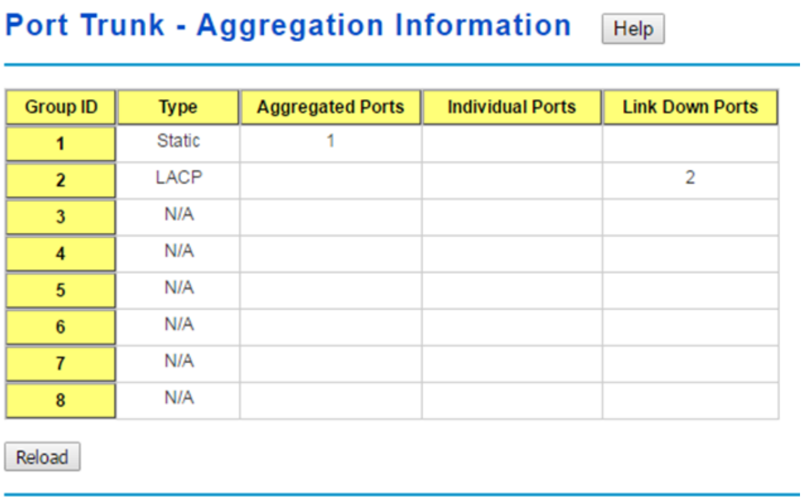
src-dst-ip load distribution is based on the source and destination IP address

Click **Apply** to apply your settings.

Note: Always remember to go to **Save** page to save the settings. Otherwise, the settings the administrator 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, the administrator will see following status.



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

Group ID: Display the Trunk Group ID in Aggregation Setting.

Type: Static or LACP set up in Aggregation Setting.

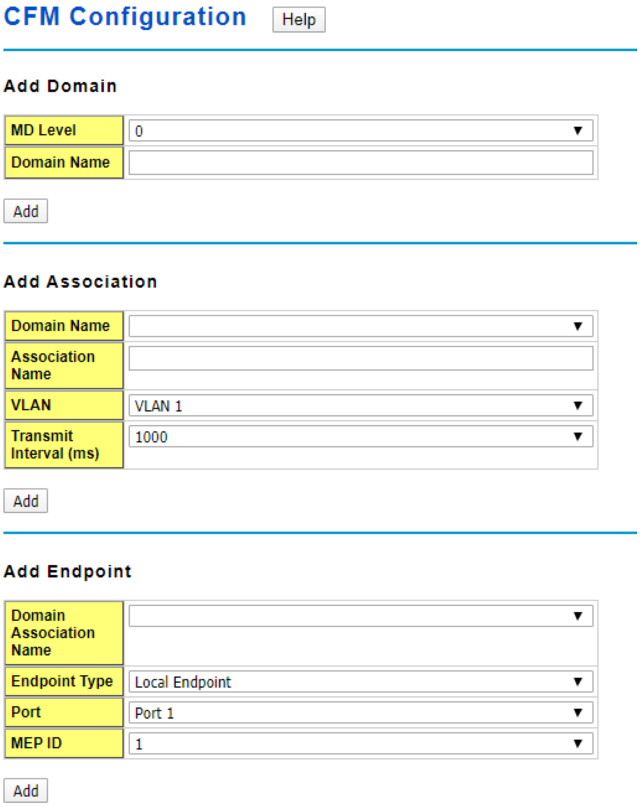
Aggregated: When LACP links well, the administrator can see the member ports in aggregated column.

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.

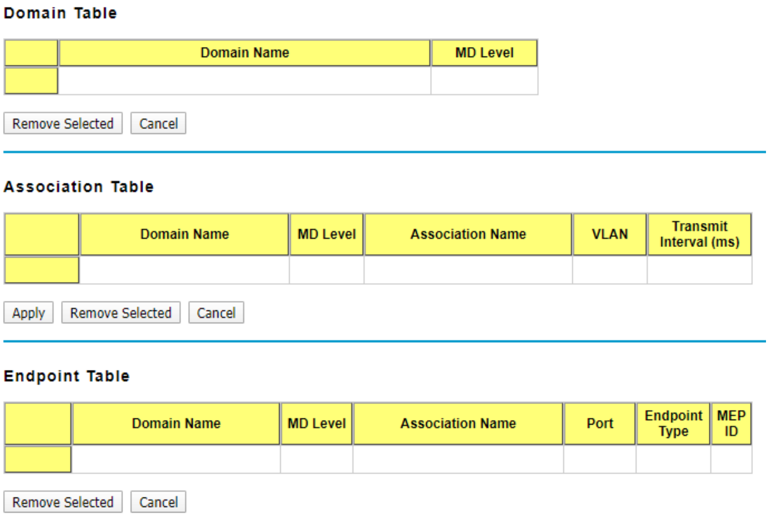
CFM Configuration



MD Level	0
Domain Name	

Domain Name	
Association Name	
VLAN	VLAN 1
Transmit Interval (ms)	1000

Domain Association Name	
Endpoint Type	Local Endpoint
Port	Port 1
MEP ID	1



Domain Table

	Domain Name	MD Level

Association Table

	Domain Name	MD Level	Association Name	VLAN	Transmit Interval (ms)

Endpoint Table

	Domain Name	MD Level	Association Name	Port	Endpoint Type	MEP ID

Add Domain

- **MD level:** set MD Level 0-7.
- **Domain Name:** Add Domain's name.

Click the **Add** button to add the CFM Domain.

Add Association

- **Domain Name:** Selection items of the Domain Name.
- **Association Name:** IEEE 802.1ag Association name.
- **VLAN:** Selection of the VLAN.
- **Transmit Interval(ms):** Configure Continuity Check Message transmit interval.

Click the **Add** button to add the Association Name.

Add Endpoint

- **Domain Association Name:** Selection items of IEEE 802.1ag Association name.
- **Endpoint Type:** Local or Remote
- **Port:** Selection items of Port ID.
- **MEP ID:** Selection items from 1 to 8191.

Click the **Add** button to apply the Endpoint's configuration changes.

Domain Table

- You can select/delete a domain entry from the Domain Table.

Click the **Remove Selected** button to remove an Entry.

Click the **Cancel** to cancel the modification.

Association Table

- You can modify an association entry from the Association Table.

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

Click the **Remove Selected** button to remove an Entry.

Click the **Cancel** to cancel the modification.

Endpoint Table

- You can select/delete an endpoint entry from the Endpoint Table.

Click the **Remove Selected** button to remove an Entry.

Click the **Cancel** to cancel the modification.

4.3.7 Command Lines for Port Configuration

Feature	Command Line
Port Control	
Port Control – State	Switch(config-if)# shutdown state -> Disable port interface fastethernet1 is shutdown now. Switch(config-if)# no shutdown interface fastethernet1 is up now. -> Enable port state
Port Control – Auto Negotiation	Switch(config-if)# auto-negotiation Auto-negotiation of port 1 is enabled!
Port Control – Force Speed/Duplex	Switch(config-if)# speed 100 set the speed mode ok! Switch(config-if)# duplex full set the duplex mode ok!
Port Control – Flow Control	Switch(config-if)# flowcontrol on Flowcontrol on for port 1 set ok! Switch(config-if)# flowcontrol off Flowcontrol off for port 1 set ok!

Port Status	
Port Status	Switch# show interface fa1 Interface fastethernet1 Description : N/A Administrative Status : Enable Operating Status : Connected Duplex : Auto (Full) Speed : Auto (100) MTU : 2000 Flow Control : off Default Port VLAN ID: 1 Acceptable Frame Type : All Auto Negotiation : Enable Loopback Mode : None STP Status: Forwarding Default CoS Value for untagged packets is 0. Medium mode is Copper. Note: Administrative Status -> Port state of the port. Operating status -> Current status of the port. Duplex -> Duplex mode of the port. Speed -> Speed mode of the port. Flow control -> Flow Control status of the port.
Rate Control	
Rate Control – Ingress or Egress	Switch(config-if)# rate-limit egress Outgoing packets ingress Incoming packets ***Note: To enable rate control, you should select the Ingress or Egress rule first; then assign the packet type and bandwidth.***
Rate Control - Bandwidth	Switch(config-if)# rate-limit ingress bandwidth <0-1000000> Limit in kilobits per second (FE: 0-100000, GE: 0-1000000, 0 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	SWITCH# show storm-control Storm-control for Port 1 Broadcast packets : Disabled Rate : 1000 (packets/s)

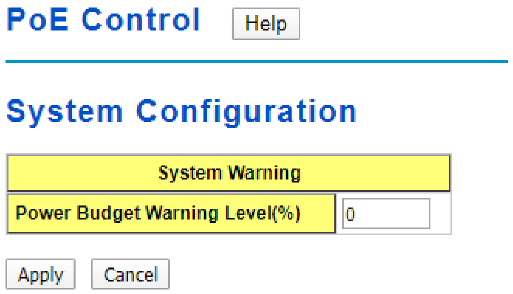
port status	Destination Lookup Failure packets : Enabled Rate : 1000 (packets/s) Multicast packets : Disabled Rate : 1000 (packets/s) Storm-control for Port 2 Broadcast packets : Disabled Rate : N/A (packets/s) Destination Lookup Failure packets : Disabled Rate :N/A (packets/s) Multicast packets : Disabled 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 <1-8> Valid group range 1-8 Switch(config)# trunk group 2 fa6-7 Trunk group 2 enable ok! Switch(config)# trunk group 1 fa9-10 Trunk group 1 enable ok!
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)
CFM Configuration	
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.

4.4 Power over Ethernet

Power over Ethernet is the key features of JetNet 7500P series only. 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.

4.4.1 PoE Control

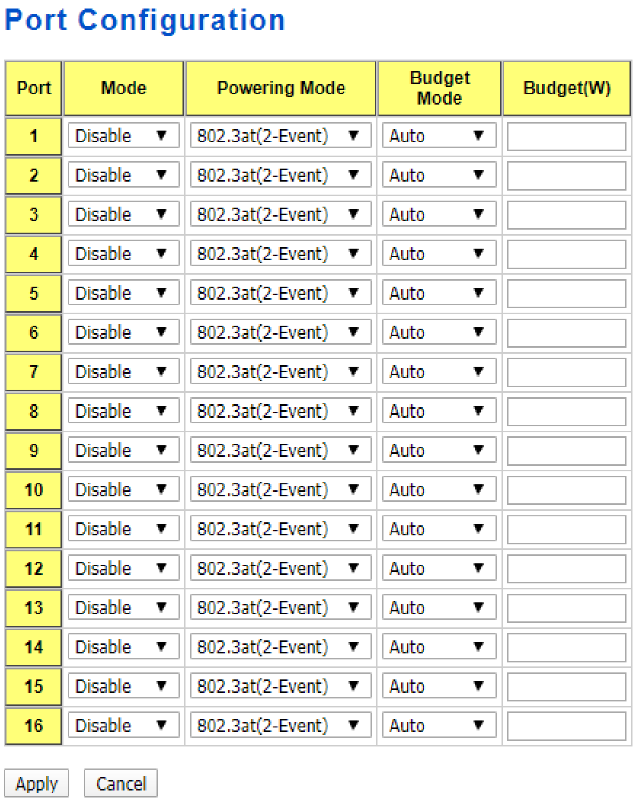


PoE Control

System Configuration

System Warning	
Power Budget Warning Level(%)	0

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.



Port Configuration

Port	Mode	Powering Mode	Budget Mode	Budget(W)
1	Disable	802.3at(2-Event)	Auto	
2	Disable	802.3at(2-Event)	Auto	
3	Disable	802.3at(2-Event)	Auto	
4	Disable	802.3at(2-Event)	Auto	
5	Disable	802.3at(2-Event)	Auto	
6	Disable	802.3at(2-Event)	Auto	
7	Disable	802.3at(2-Event)	Auto	
8	Disable	802.3at(2-Event)	Auto	
9	Disable	802.3at(2-Event)	Auto	
10	Disable	802.3at(2-Event)	Auto	
11	Disable	802.3at(2-Event)	Auto	
12	Disable	802.3at(2-Event)	Auto	
13	Disable	802.3at(2-Event)	Auto	
14	Disable	802.3at(2-Event)	Auto	
15	Disable	802.3at(2-Event)	Auto	
16	Disable	802.3at(2-Event)	Auto	

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.

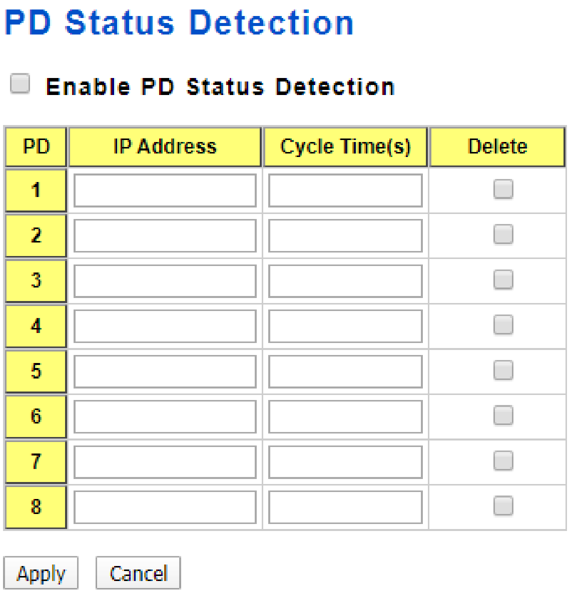
802.3at(LLDP): 802.3at(LLDP) is set powering mode to standard IEEE802.3at LLDP.

802.3at(2 Event):802.3at(2 Event) is set powering mode to standard IEEE 802.3at Physical.

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.



PD Status Detection

□ Enable PD Status Detection

PD	IP Address	Cycle Time(s)	Delete
1			□
2			□
3			□
4			□
5			□
6			□
7			□
8			□

The JetNet 7500P series switch supports an useful function named ***LPLD(Link Partner Line Detection)*** that helps user to maintain the PD's status and save the maintenance time and human resource. This function is patented by Korenix. Once enable this function, the PoE Switch will request PD system in the period 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 maintenance 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.

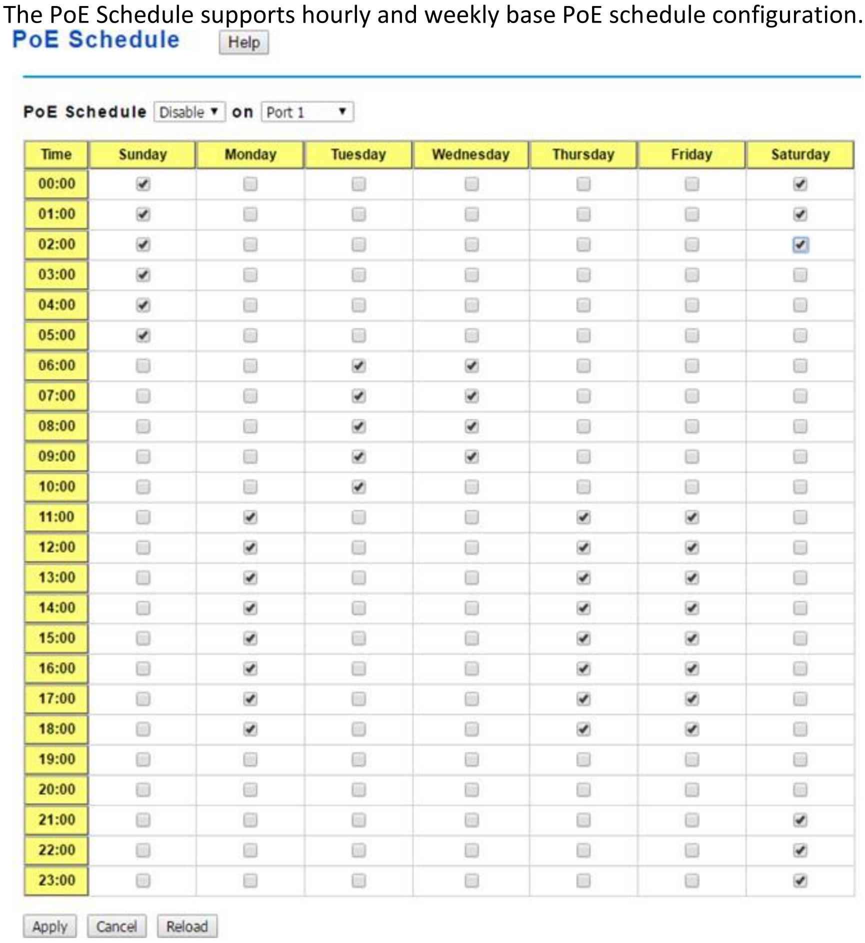
Cycle Time(s): One PD failure detection (in seconds) of period time. We suggest setting the cycle time to 90 seconds since most of PDs (IP camera) will take at least 40~50 seconds to restart.

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.

4.4.2 PoE Schedule

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



PoE Schedule

PoE Schedule Disable ▾ on Port 1 ▾

Time	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
00:00	☑	□	□	□	□	□	☑
01:00	☑	□	□	□	□	□	☑
02:00	☑	□	□	□	□	□	☑
03:00	☑	□	□	□	□	□	□
04:00	☑	□	□	□	□	□	□
05:00	☑	□	□	□	□	□	□
06:00	□	□	☑	☑	□	□	□
07:00	□	□	☑	☑	□	□	□
08:00	□	□	☑	☑	□	□	□
09:00	□	□	☑	☑	□	□	□
10:00	□	□	☑	□	□	□	□
11:00	□	☑	□	□	☑	☑	□
12:00	□	☑	□	□	☑	☑	□
13:00	□	☑	□	□	☑	☑	□
14:00	□	☑	□	□	☑	☑	□
15:00	□	☑	□	□	☑	☑	□
16:00	□	☑	□	□	☑	☑	□
17:00	□	☑	□	□	☑	☑	□
18:00	□	☑	□	□	☑	☑	□
19:00	□	□	□	□	□	□	□
20:00	□	□	□	□	□	□	□
21:00	□	□	□	□	□	□	☑
22:00	□	□	□	□	□	□	☑
23:00	□	□	□	□	□	□	☑

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.

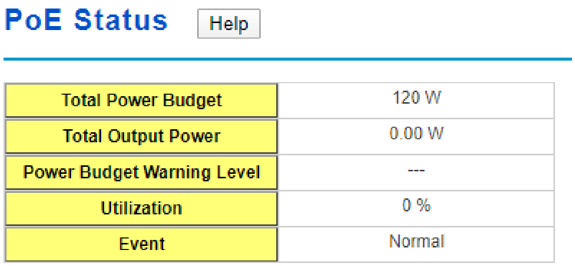
Click **Reload** to reload the information.

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 the PoE Schedule and follow the system clock. As this result, be sure the system clock has configured as your local time.

4.4.3 PoE Status

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



PoE Status

Total Power Budget	120 W
Total Output Power	0.00 W
Power Budget Warning Level	---
Utilization	0 %
Event	Normal

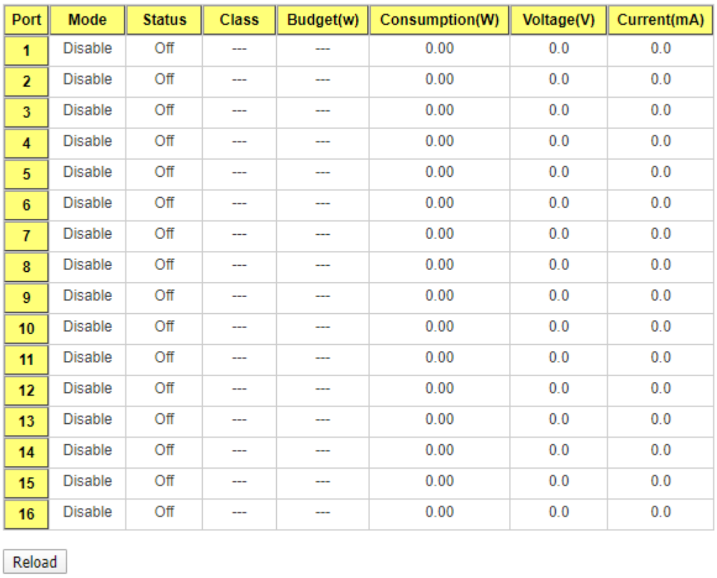
Total Power Budget: This is the maximum PoE output power (in watts).

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
9	Disable	Off	---	---	0.00	0.0	0.0
10	Disable	Off	---	---	0.00	0.0	0.0
11	Disable	Off	---	---	0.00	0.0	0.0
12	Disable	Off	---	---	0.00	0.0	0.0
13	Disable	Off	---	---	0.00	0.0	0.0
14	Disable	Off	---	---	0.00	0.0	0.0
15	Disable	Off	---	---	0.00	0.0	0.0
16	Disable	Off	---	---	0.00	0.0	0.0

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.

4.5 Network Redundancy

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

The JetNet 7500 series 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).

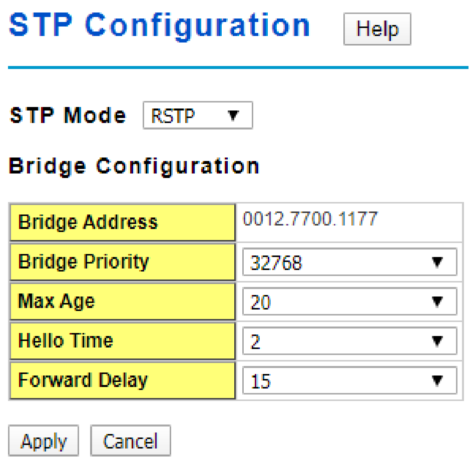
Multiple Super Ring (MSR) technology is *Korenix's*3rd generation Ring redundancy technology. This is patented and protected by *Korenix* and is used in countries all over the world. MSR ranks the fastest restore and failover time in the world, 0 ms for restore and about several milliseconds for failover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

Advanced Rapid Dual Homing(RDH) technology also facilitates JetNet 7500 series 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.

4.5.1 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 Configuration

STP Mode: RSTP

Bridge Configuration

Bridge Address	0012.7700.1177
Bridge Priority	32768
Max Age	20
Hello Time	2
Forward Delay	15

STP Mode: Select the spanning tree protocol: STP, RSTP or MSTP or Disable
Bridge Address: The MAC address 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 to select the priority number directly. This is the convenience 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 rules 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 7500 series switch is not the root bridge, and if it has not received a hello message from the root bridge in an amount of time equal to Max Age, then JetNet 7500 series switch will reconfigure itself as a root bridge. Once two or more devices on the network are recognized as a root bridge, the devices will renegotiate to set up a new spanning tree topology.

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

Since different RSTP aware switches may have their own mechanism to calculate the message age. So that this is most possibly occurred when interoperate different vendors' RSTP aware switches together. The maximum volume of the 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.

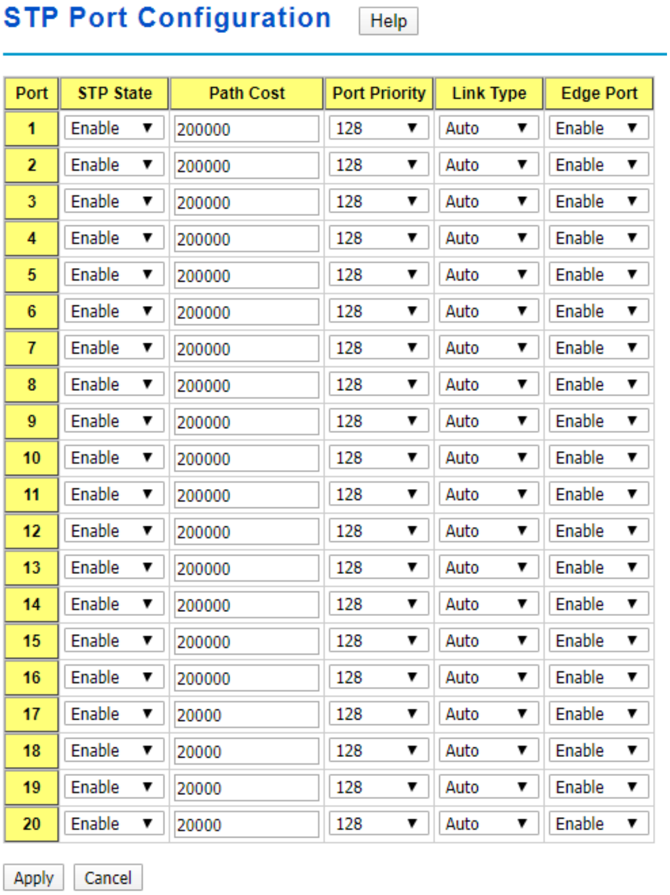
Note: You must observe the following rule to configure Max Age, Hello Time, and Forwarding Delay parameters.

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.

4.5.2 STP Port Configuration

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



STP Port Configuration

Port	STP State	Path Cost	Port Priority	Link Type	Edge Port
1	Enable	200000	128	Auto	Enable
2	Enable	200000	128	Auto	Enable
3	Enable	200000	128	Auto	Enable
4	Enable	200000	128	Auto	Enable
5	Enable	200000	128	Auto	Enable
6	Enable	200000	128	Auto	Enable
7	Enable	200000	128	Auto	Enable
8	Enable	200000	128	Auto	Enable
9	Enable	200000	128	Auto	Enable
10	Enable	200000	128	Auto	Enable
11	Enable	200000	128	Auto	Enable
12	Enable	200000	128	Auto	Enable
13	Enable	200000	128	Auto	Enable
14	Enable	200000	128	Auto	Enable
15	Enable	200000	128	Auto	Enable
16	Enable	200000	128	Auto	Enable
17	Enable	20000	128	Auto	Enable
18	Enable	20000	128	Auto	Enable
19	Enable	20000	128	Auto	Enable
20	Enable	20000	128	Auto	Enable

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.**

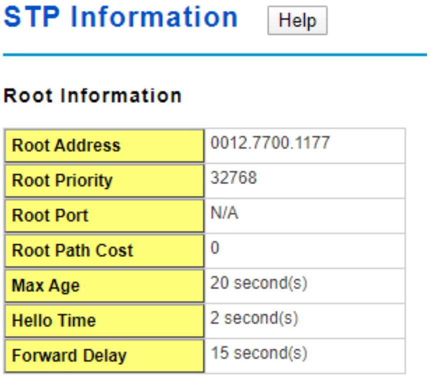
Some of the rapid state transitions that are possible within RSTP depend upon whether the port of concern can only be connected to another bridge (i.e. it is served by a point-to- point LAN segment), or if it can be connected to two or more bridges (i.e. it is served by a shared-medium LAN segment).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

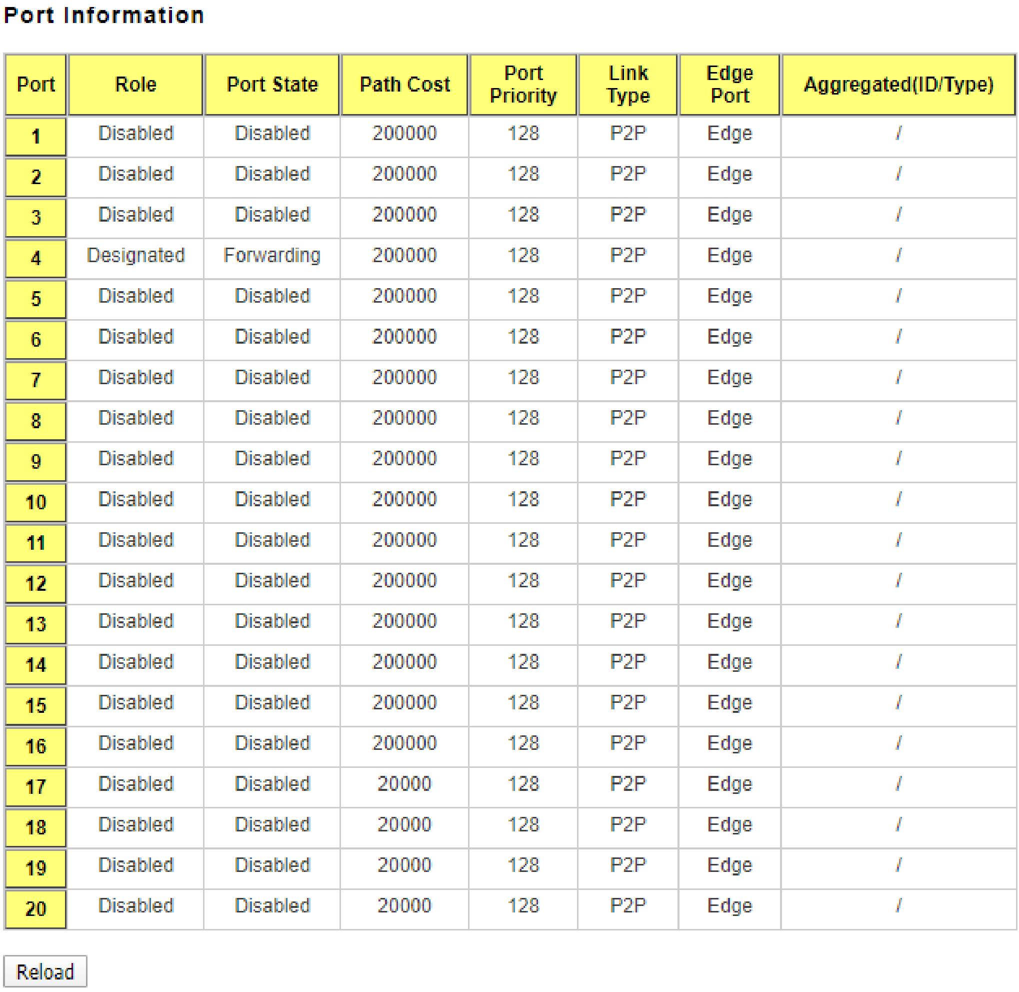
Note: Always remember to go to **Save** page to save the settings. Otherwise, the settings you made will be lost when the switch is powered off.

4.5.3 STP Information



Root Information

Root Address	0012.7700.1177
Root Priority	32768
Root Port	N/A
Root Path Cost	0
Max Age	20 second(s)
Hello Time	2 second(s)
Forward Delay	15 second(s)



Port Information

Port	Role	Port State	Path Cost	Port Priority	Link Type	Edge Port	Aggregated(ID/Type)
1	Disabled	Disabled	200000	128	P2P	Edge	/
2	Disabled	Disabled	200000	128	P2P	Edge	/
3	Disabled	Disabled	200000	128	P2P	Edge	/
4	Designated	Forwarding	200000	128	P2P	Edge	/
5	Disabled	Disabled	200000	128	P2P	Edge	/
6	Disabled	Disabled	200000	128	P2P	Edge	/
7	Disabled	Disabled	200000	128	P2P	Edge	/
8	Disabled	Disabled	200000	128	P2P	Edge	/
9	Disabled	Disabled	200000	128	P2P	Edge	/
10	Disabled	Disabled	200000	128	P2P	Edge	/
11	Disabled	Disabled	200000	128	P2P	Edge	/
12	Disabled	Disabled	200000	128	P2P	Edge	/
13	Disabled	Disabled	200000	128	P2P	Edge	/
14	Disabled	Disabled	200000	128	P2P	Edge	/
15	Disabled	Disabled	200000	128	P2P	Edge	/
16	Disabled	Disabled	200000	128	P2P	Edge	/
17	Disabled	Disabled	20000	128	P2P	Edge	/
18	Disabled	Disabled	20000	128	P2P	Edge	/
19	Disabled	Disabled	20000	128	P2P	Edge	/
20	Disabled	Disabled	20000	128	P2P	Edge	/

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.

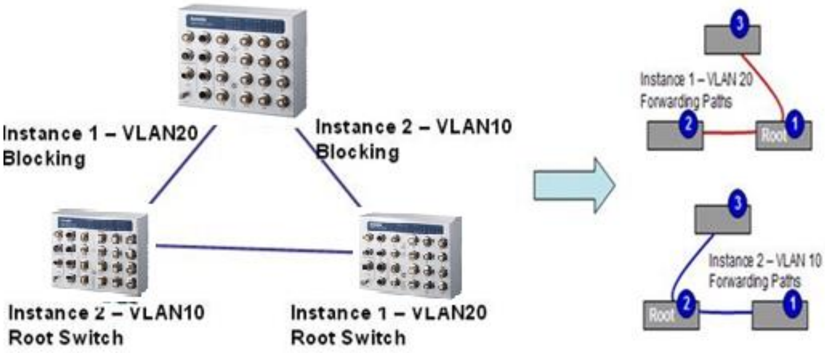
4.5.4 MSTP Configuration

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.

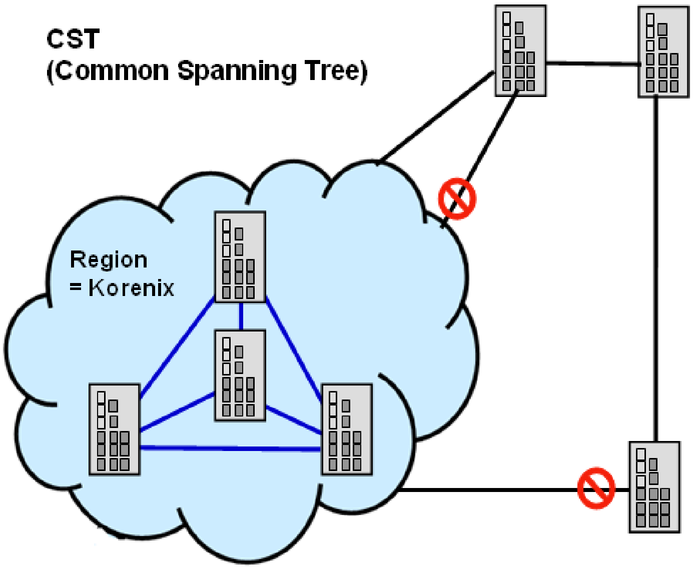
One VLAN can be mapped to a Multiple Spanning Tree Instance (MSTI). The maximum Instance of JetNet Managed Switch support is 16, range from 0-15. The MSTP builds a separate Multiple Spanning Tree (MST) for each instance to maintain connectivity among each of the assigned VLAN groups. An Internal Spanning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

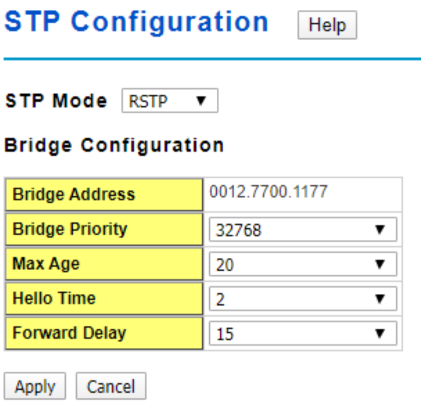


A Common Spanning Tree (CST) interconnects all adjacent MST regions and acts as a virtual bridge node for communications with STP or RSTP nodes in the global network.
MSTP connects all bridges and LAN segments with a single Common and Internal Spanning Tree (CIST). The CIST is formed as a result of the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

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



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



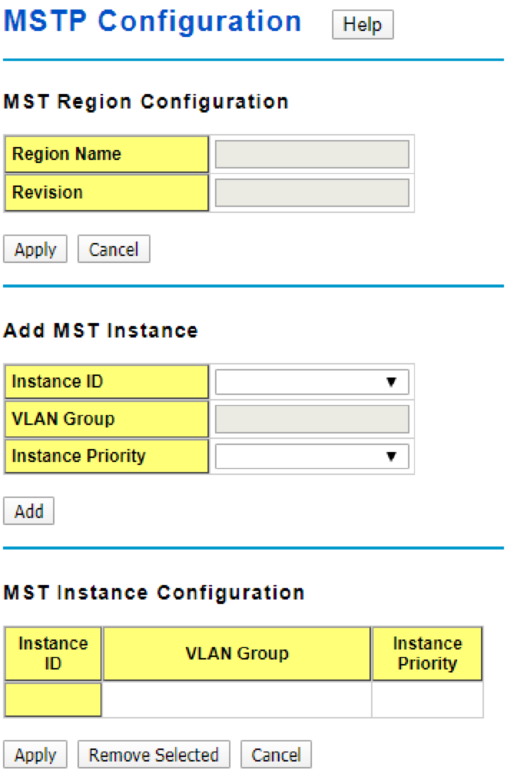
STP Configuration

STP Mode: RSTP

Bridge Configuration

Bridge Address	0012.7700.1177
Bridge Priority	32768
Max Age	20
Hello Time	2
Forward Delay	15

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



MSTP Configuration

MST Region Configuration

Region Name	
Revision	

Add MST Instance

Instance ID	
VLAN Group	
Instance Priority	

MST Instance Configuration

Instance ID	VLAN Group	Instance Priority

MSTP Region Configuration

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

Region Name: 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 is 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

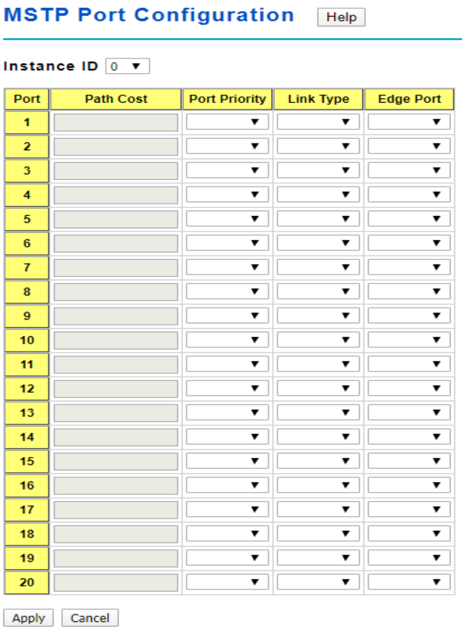
This page allows you to see the current MST Instance Configuration you added. Click "**Apply**" to apply the setting.

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

4.5.5 MSTP Port Configuration

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

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



MSTP Port Configuration

Instance ID 0 ▼

Port	Path Cost	Port Priority	Link Type	Edge Port
1		▼	▼	▼
2		▼	▼	▼
3		▼	▼	▼
4		▼	▼	▼
5		▼	▼	▼
6		▼	▼	▼
7		▼	▼	▼
8		▼	▼	▼
9		▼	▼	▼
10		▼	▼	▼
11		▼	▼	▼
12		▼	▼	▼
13		▼	▼	▼
14		▼	▼	▼
15		▼	▼	▼
16		▼	▼	▼
17		▼	▼	▼
18		▼	▼	▼
19		▼	▼	▼
20		▼	▼	▼

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.

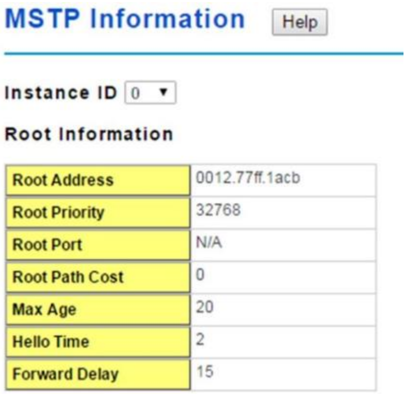
Click **Apply** to apply the settings. Click

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.

4.5.6 MSTP Information

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

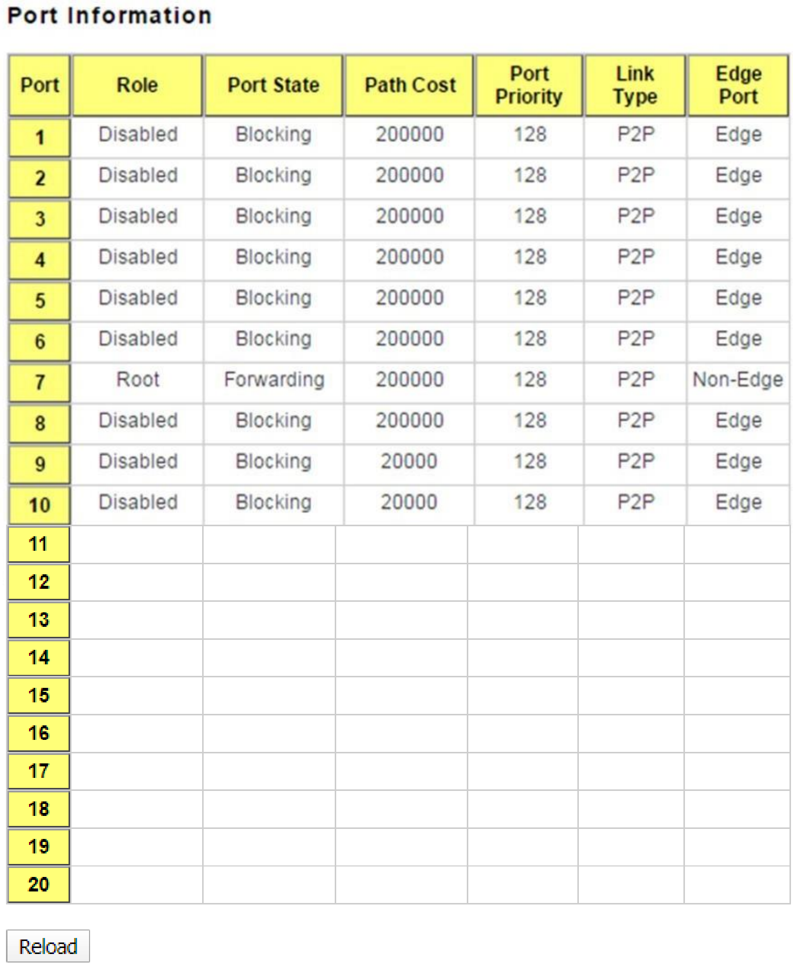


MSTP Information

Instance ID 0

Root Information

Root Address	0012.77ff.1acb
Root Priority	32768
Root Port	N/A
Root Path Cost	0
Max Age	20
Hello Time	2
Forward Delay	15



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
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						

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.

4.5.7 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.

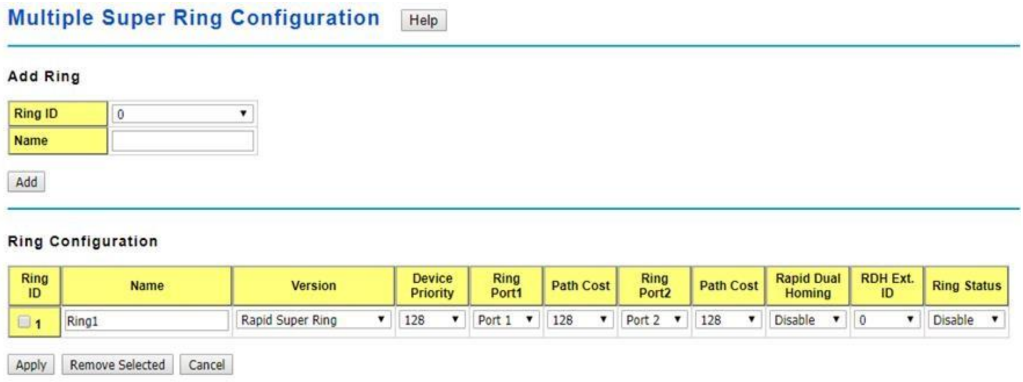
Multiple Super Ring (MSR) technology is *Korenix's* 3rd generation Ring redundancy technology. This is patented and protected by *Korenix* and is used in countries all over the world. MSR ranks the fastest restore and failover time in the world, 0 ms for restore and about milliseconds level for failover 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 7500 series 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.



Multiple Super Ring Configuration

Add Ring

Ring ID	0
Name	

Ring Configuration

Ring ID	Name	Version	Device Priority	Ring Port1	Path Cost	Ring Port2	Path Cost	Rapid Dual Homing	RDH Ext. ID	Ring Status
□ 1	Ring1	Rapid Super Ring	128	Port 1	128	Port 2	128	Disable	0	Disable

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.

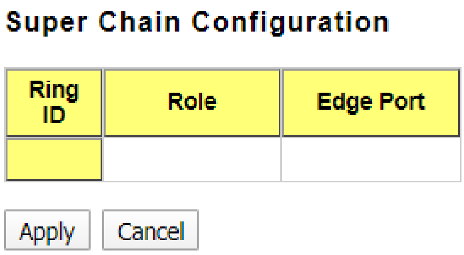
Click **Apply** to apply the settings.

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



Super Chain Configuration

Ring ID	Role	Edge Port

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.

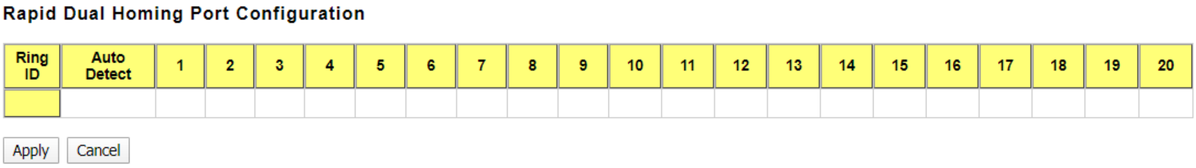
Edge Port: Edge Port is one of ring ports of Border node. It is used to connect to an external network.

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



Rapid Dual Homing Port Configuration

Ring ID	Auto Detect	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

Ring ID: The Ring Identifier referring to this Ring.

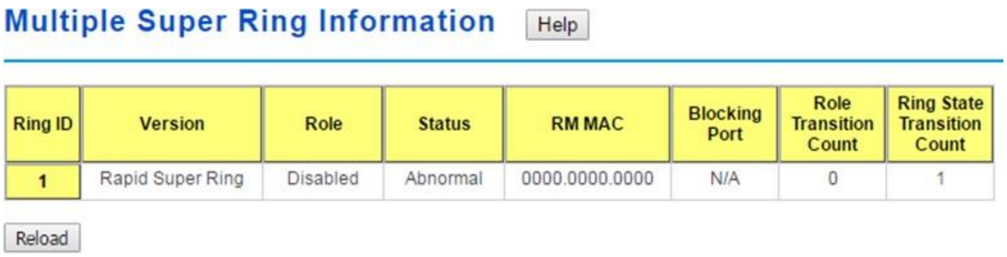
Auto Detect: Enable RDH auto detect RDH port mode.

Port: Enable RDH on specific ports. Click

“**Apply**” to apply the setting.

Click “**Cancel”** to clear the modification.

4.5.8 MSR Information



Multiple Super Ring Information

Ring ID	Version	Role	Status	RM MAC	Blocking Port	Role Transition Count	Ring State Transition Count
1	Rapid Super Ring	Disabled	Abnormal	0000.0000.0000	N/A	0	1

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.

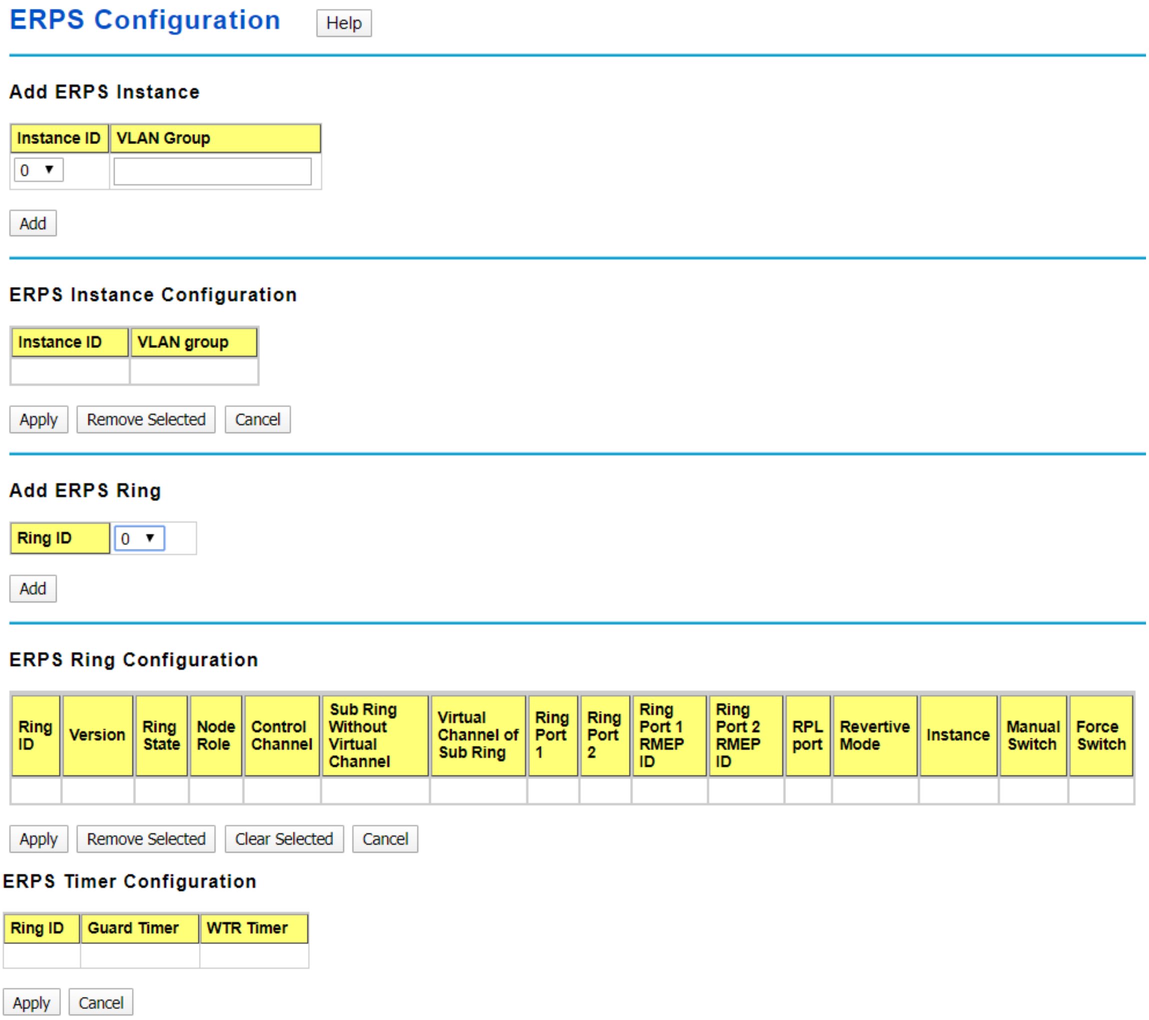
Role state Transition Count: This number means how many times the Ring status has been transformed between **Normal** and **Abnormal** state.

Click **Reload** to reload the information.

4.5.9 ERPS Configuration

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

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



ERPS Configuration Help

Add ERPS Instance

Instance ID	VLAN Group
0 ▼	

Add

ERPS Instance Configuration

Instance ID	VLAN group

Apply Remove Selected Cancel

Add ERPS Ring

Ring ID	0 ▼

Add

ERPS Ring Configuration

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

Apply Remove Selected Clear Selected Cancel

ERPS Timer Configuration

Ring ID	Guard Timer	WTR Timer

Apply Cancel

- **Add Instance:**
  - **Instance ID:** The ERPS instance identifies. Valid values start from 0 to 15.
  - **VLAN Group:** The VLAN ID members of the Instance ID
- Click the **Add** to add the ERPS Instance.

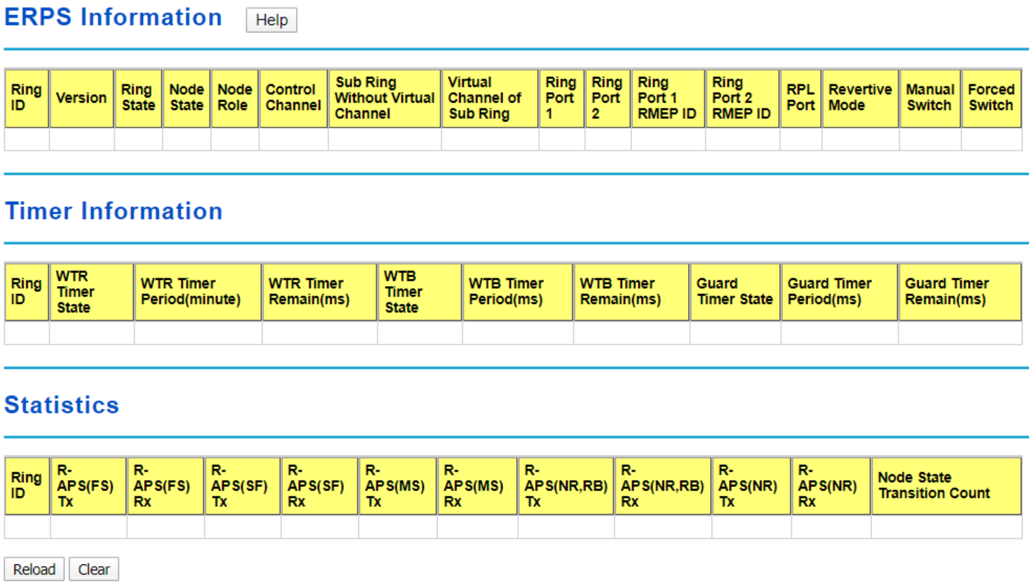
- **ERPS Instance Configuration:**
  - **Instance ID:** The ERPS instance identifies. Valid values start from 0 to 15.
  - **VLAN Group:** The VLAN ID members of the Instance ID
- Click the **Add** to add the ERPS Instance. To remove an MST instance check the checkbox of the Instance ID you want to remove and click the **Remove Selected** button. Click the **Cancel** button to reload the current settings.

- **Add Ring:**
  - **Ring ID:** The ERPS Ring identifies. Valid values are 0 to 31.
- Click the **Add** to add the ERPS Ring.

- **ERPS Ring Configuration:**
  - **Ring ID:** The ERPS Ring identifies.
  - **Version:** ERPS has version 1 and 2.
  - **Ring State:** The current state of ring, Disable, Major or Sub.
  - **Node Role:** The role of the node, RPL owner, RPL Neighbor and Ring node. The RPL owner is an Ethernet ring node adjacent to the RPL.
  - **Control Channel:** Control Channel provide a communication channel for ring automatic protection switching (R-APS) transmission.
  - **Sub Ring Without Virtual Channel:** Select to use virtual channel to transmit sub-ring ring automatic protection switching (R-APS) or not.
  - **Virtual Channel of Sub Ring:** Control Channel provide a communication channel for sub-ring ring automatic protection switching (R-APS) transmission.
  - **Ring Port:** A ring link is bounded by two adjacent nodes and a port for a ring link is called a ring port.
  - **RMEP ID:** The remote MEP ID of ring port.
  - **RPL Port:** The ring protection link (RPL) is the ring link which under normal conditions, i.e., without any failure or request, is blocked for traffic channel, to prevent the formation of loops.
  - **Revertive Mode:** In revertive mode, all ring links and nodes have recovered, the block link will revert to RPL link. In non-revertive mode, the ring does not automatically revert.
  - **Instance:** Select one ERPS instance to control it.
  - **Manual Switch:** Allows the operator to manually block a particular ring port.
  - **Force Switch:** Allows the operator to forcefully block a particular ring port.
- Click the **Apply** to apply the configurations.
- Click the **Remove Selected** to remove a ring.
- Click the **Clear** to cancel an existing FS or MS command on the ring port.
- Click the **Cancel** to cancel this modification.

- **ERPS Timer Configuration:**
  - **Ring ID:** The ERPS Ring identifies.
  - **Guard Timer:** The Guard Timer. Valid values are 10 to 2000 ms, default is 100 ms.
  - **WTR Timer:** The WTR(Wait-to-restore) Timer. Valid values are 1 to 12 minutes, default is 5 minutes.
- Click the **Apply** to apply the configurations.

ERPS Information



ERPS Information

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

Timer Information

Ring ID	WTR Timer State	WTR Timer Period(minute)	WTR Timer Remain(ms)	WTB Timer State	WTB Timer Period(ms)	WTB Timer Remain(ms)	Guard Timer State	Guard Timer Period(ms)	Guard Timer Remain(ms)

Statistics

Ring ID	R-APS(FS) Tx	R-APS(FS) Rx	R-APS(SF) Tx	R-APS(SF) Rx	R-APS(MS) Tx	R-APS(MS) Rx	R-APS(NR,RB) Tx	R-APS(NR,RB) Rx	R-APS(NR) Tx	R-APS(NR) Rx	Node State Transition Count

- **Ethernet Ring Protection Switching Information:**

- **Ring ID:** The Ring Identifier referring to this Ring.
- **Version:** Ring function version selection.
- **Ring State:** Major Ring/Sub Ring or Disable
- **Node State:** The current state of the node is in Disable, Initial, Idle, Pending, Protection, Manual Switch or Forced Switch.
- **Node Role:** Node Role in the Ring. RPL Owner/RPL Neighbour/Ring Node
- **Control Channel:** VLAN ID from 1-4094
- **Sub Ring Without Virtual Channel:** True or False
- **Virtual Channel of Sub Ring:** VLAN ID from 1-4094
- **Ring Port1:** The first port of the ring.
- **Ring Port2:** The second port of the ring.
- **Ring Port1 RMEP ID:** The remote MEP ID of first port of the ring.
- **Ring Port2 RMEP ID:** The remote MEP ID of second port of the ring.
- **RPL Port:** The blocking port of the ring ports.
- **Revertive Mode:** "Revertive" will take the reversion action, when ring nodes recover and no external requests are active
- **Manual Switch:** Manual switch status
- **Forced Switch:** Forced switch status

- **Timer Information:**

- **Ring ID:** The Ring Identifier referring to this Ring.
- **WTR Timer State:** WTR Timer state
- **WTR Timer Period:** WTR Timer period in minutes.
- **WTR Timer Remain:** WTR Timer remain in ms
- **WTB Timer State:** WTB Timer state
- **WTB Timer Period:** WTB Timer period in ms
- **WTB Timer Remain:** WTB Timer remain in ms
- **Guard Timer State:** Guard Timer state
- **Guard Timer Period:** Guard Timer period in ms
- **Guard Timer Remain:** Guard Timer remain in ms

- **Statistics:**

- **Ring ID:** The Ring Identifier referring to this Ring.
- **R-APS(FS) Tx:** Forced Switch Tx
- **R-APS(FS) Rx:** Force Switch Rx
- **R-APS(SF) Tx:** Signal Fail Tx
- **R-APS(SF) Rx:** Signal Fail Rx
- **R-APS(MS) Tx:** Manual Switch Tx
- **R-APS(MS) Rx:** Manual Switch Rx
- **R-APS(NR,RB) Tx:** No Request, RPL blocked Tx
- **R-APS(NR,RB) Rx:** No Request, RPL blocked Rx
- **R-APS(NR) Tx:** No Request Tx
- **R-APS(NR) Rx:** No Request Rx
- **Node State Transition Count:** Node State Transition count
- Click the **Reload** button to reload Ring information.

4.5.10 Command Lines

Feature	**Command Line**
Global	
Enable	Switch(config)# spanning-tree enable
Disable	Switch(config)# spanning-tree disable
Mode (Choose the Spanning Tree mode)	Switch(config)# spanning-tree mode rst the rapid spanning-tree protocol (802.1w) stp the spanning-tree 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)# name74korenix 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 74[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 74korenix(->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 76korenix 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

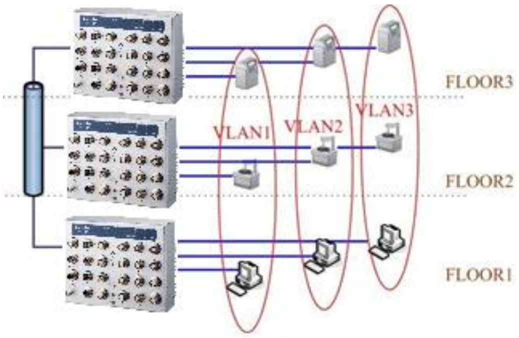
	<0-7> extension ID 0-7 (default is 0) default Note: auto-detect is recommended for dual Homing..
Super Chain	Switch(config-multiple-super-ring)# super-chain disable Switch(config-multiple-super-ring)# super-chain border Switch(config-multiple-super-ring)# super-chain member Switch(config-multiple-super-ring)# 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

4.6 VLAN

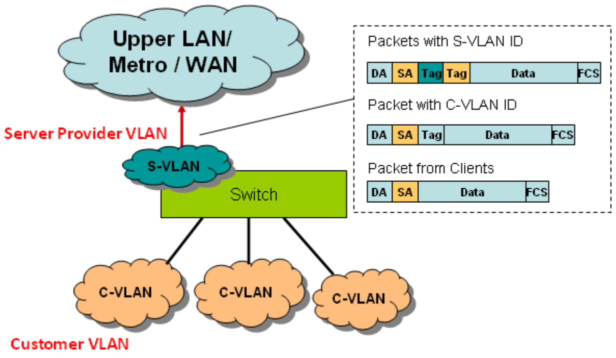
A Virtual LAN (VLAN) is a “logical” grouping of nodes for the purpose of limiting a broadcast domain to specific members of a group without physically grouping the members together. That means, VLAN allows you to isolate network traffic so that only members of VLAN could receive traffic from the same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

JetNet 7500 series 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 should 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.



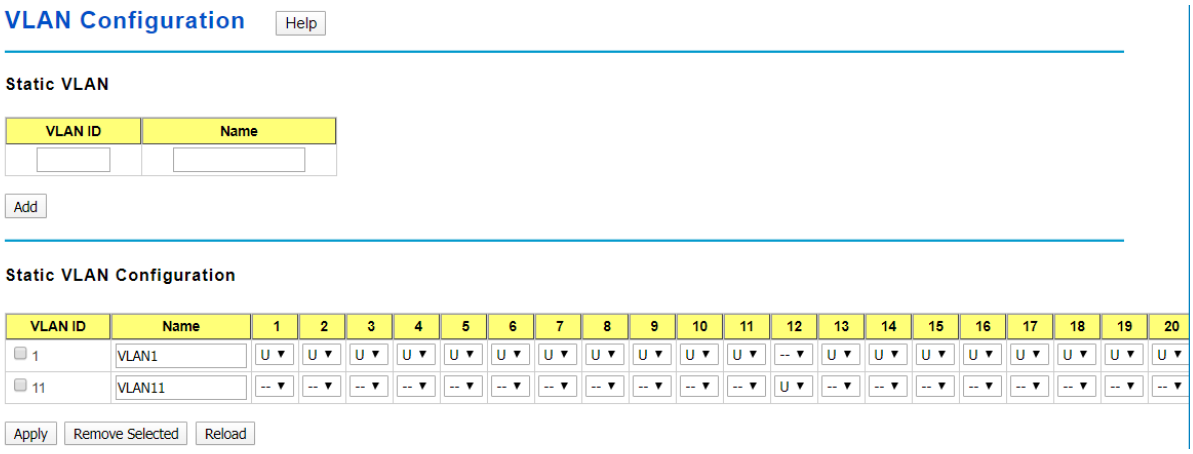
QinQ

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.



4.6.1 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.



Static VLAN

VLAN ID	Name

Static VLAN Configuration

VLAN ID	Name	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
□ 1	VLAN1	U ▾	U ▾	U ▾	U ▾	U ▾	U ▾	U ▾	U ▾	U ▾	U ▾	U ▾	-- ▾	U ▾	U ▾	U ▾	U ▾	U ▾	U ▾	U ▾	U ▾
□ 11	VLAN11	-- ▾	-- ▾	-- ▾	-- ▾	-- ▾	-- ▾	-- ▾	-- ▾	-- ▾	-- ▾	-- ▾	U ▾	-- ▾	-- ▾	-- ▾	-- ▾	-- ▾	-- ▾	-- ▾	-- ▾

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.

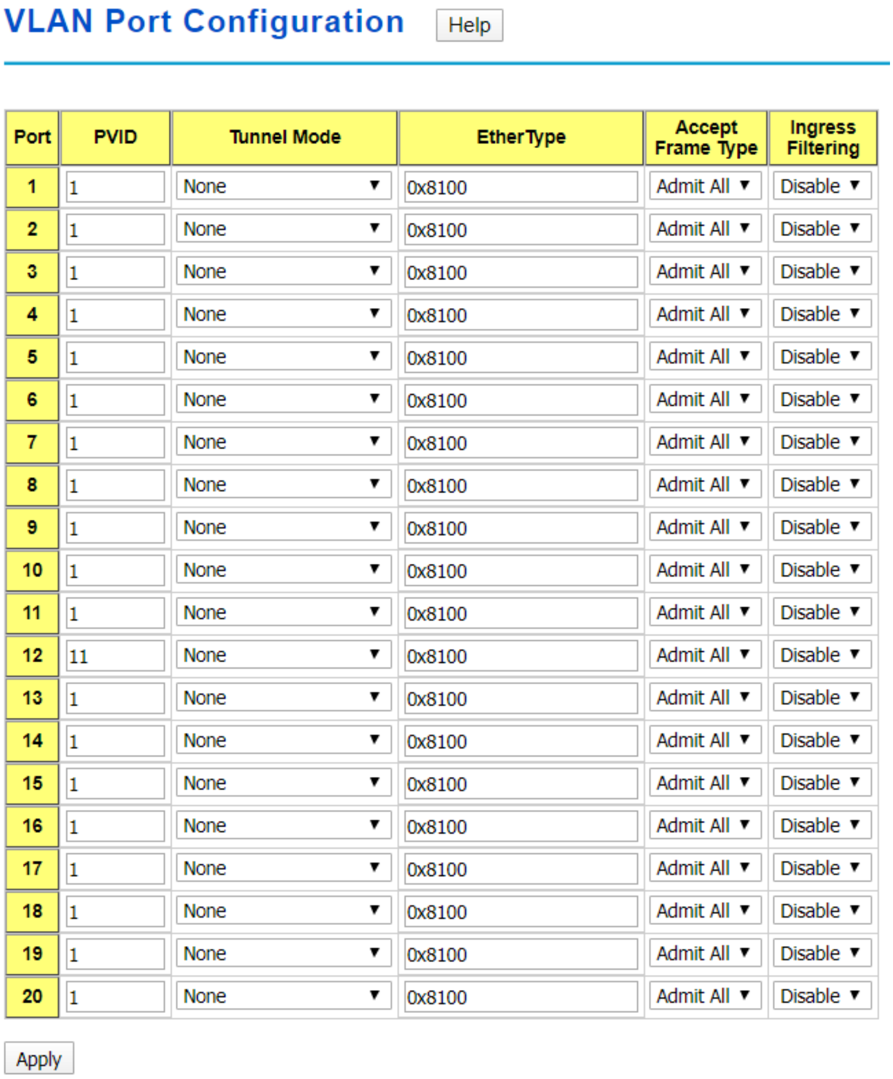
Click **Remove** Selected to remove the selected static VLAN. Click

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.

4.6.2 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.



VLAN Port Configuration

Port	PVID	Tunnel Mode	EtherType	Accept Frame Type	Ingress Filtering
1	1	None ▼	0x8100	Admit All ▼	Disable ▼
2	1	None ▼	0x8100	Admit All ▼	Disable ▼
3	1	None ▼	0x8100	Admit All ▼	Disable ▼
4	1	None ▼	0x8100	Admit All ▼	Disable ▼
5	1	None ▼	0x8100	Admit All ▼	Disable ▼
6	1	None ▼	0x8100	Admit All ▼	Disable ▼
7	1	None ▼	0x8100	Admit All ▼	Disable ▼
8	1	None ▼	0x8100	Admit All ▼	Disable ▼
9	1	None ▼	0x8100	Admit All ▼	Disable ▼
10	1	None ▼	0x8100	Admit All ▼	Disable ▼
11	1	None ▼	0x8100	Admit All ▼	Disable ▼
12	11	None ▼	0x8100	Admit All ▼	Disable ▼
13	1	None ▼	0x8100	Admit All ▼	Disable ▼
14	1	None ▼	0x8100	Admit All ▼	Disable ▼
15	1	None ▼	0x8100	Admit All ▼	Disable ▼
16	1	None ▼	0x8100	Admit All ▼	Disable ▼
17	1	None ▼	0x8100	Admit All ▼	Disable ▼
18	1	None ▼	0x8100	Admit All ▼	Disable ▼
19	1	None ▼	0x8100	Admit All ▼	Disable ▼
20	1	None ▼	0x8100	Admit All ▼	Disable ▼

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 tagis 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.

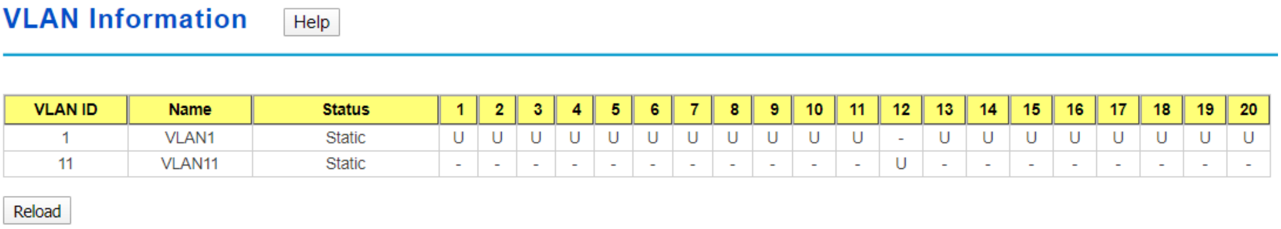
Accept Frame Type: This column defines the accepted frame type of the port. There are 2 modes you can select, **Admit All** and **Tag Only**.
Admit All mode means that the port can accept both tagged and untagged packets. **Tag Only** mode means that the port can only accept tagged packets.

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.

4.6.3 VLAN Information



VLAN Information

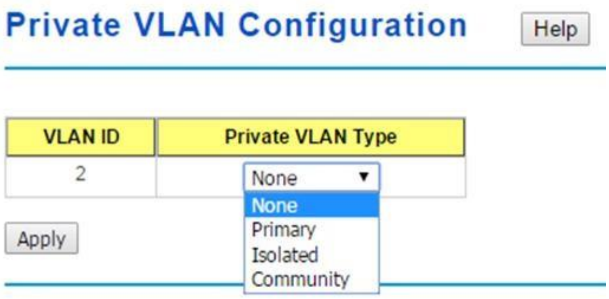
VLAN ID	Name	Status	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	VLAN1	Static	U	U	U	U	U	U	U	U	U	U	U	-	U	U	U	U	U	U	U	U
11	VLAN11	Static	-	-	-	-	-	-	-	-	-	-	-	U	-	-	-	-	-	-	-	-

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

4.6.4 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.



Private VLAN Configuration

VLAN ID	Private VLAN Type
2	None

VLAN ID:

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

- **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 PrimaryVLAN. The member ports can communicate withthe secondary VLANs
- **Isolated**: The member ports of the VLAN are isolated.

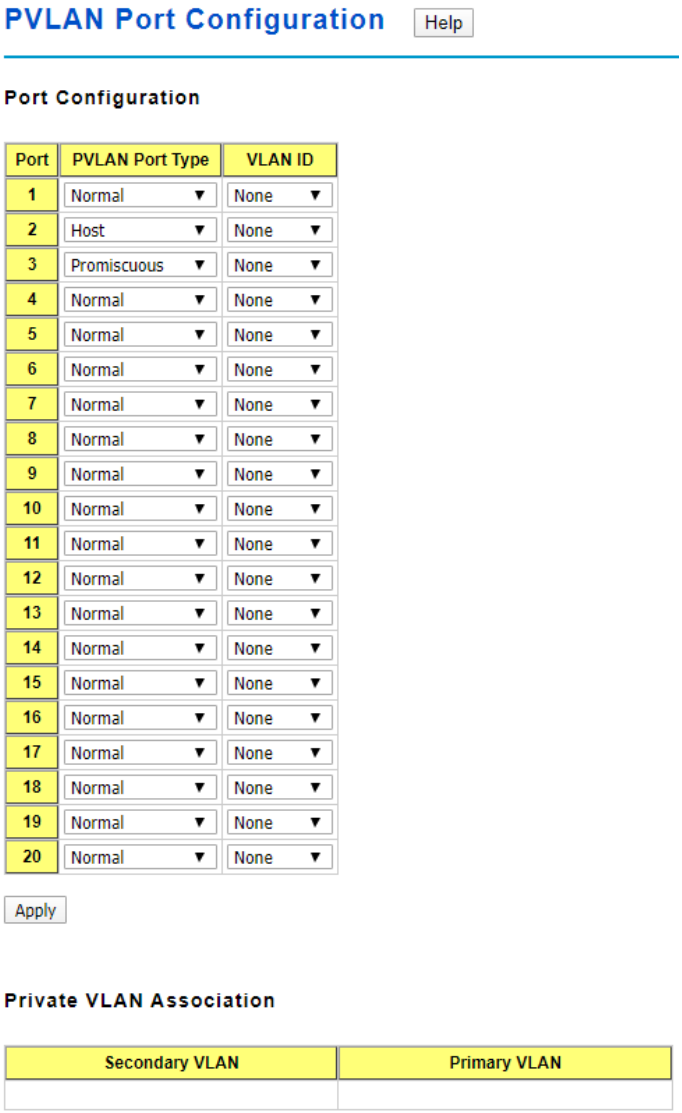
- **Community**: The member ports of the VLAN can communicate with each other. Click

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.

4.6.5 PVLAN Port Configuration

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



PVLAN Port Configuration

Port Configuration

Port	PVLAN Port Type	VLAN ID
1	Normal	None
2	Host	None
3	Promiscuous	None
4	Normal	None
5	Normal	None
6	Normal	None
7	Normal	None
8	Normal	None
9	Normal	None
10	Normal	None
11	Normal	None
12	Normal	None
13	Normal	None
14	Normal	None
15	Normal	None
16	Normal	None
17	Normal	None
18	Normal	None
19	Normal	None
20	Normal	None

Private VLAN Association

Secondary VLAN	Primary VLAN

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.

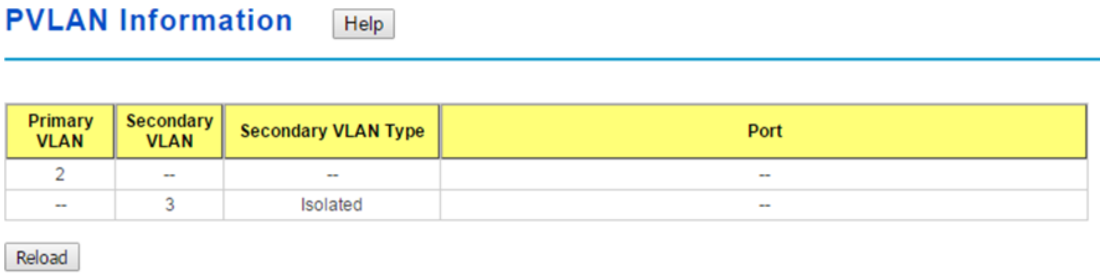
Primary VLAN: After the Primary VLAN Type is assigned in Private VLAN Configuration page, the secondary VLAN can associate to the primary VLAN ID.

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

4.6.6 PVLAN Information

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

Reload to refresh the page contents.



PVLAN Information

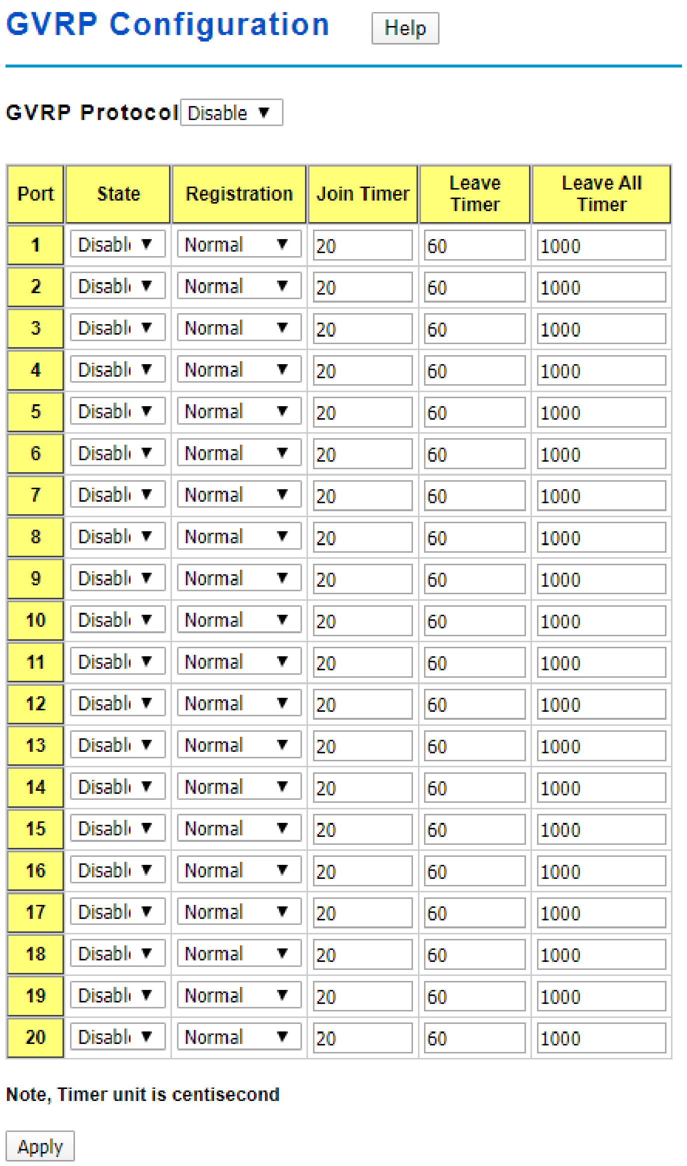
Primary VLAN	Secondary VLAN	Secondary VLAN Type	Port
2	--	--	--
--	3	Isolated	--

4.6.7 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 Configuration

GVRP Protocol Disable ▼

Port	State	Registration	Join Timer	Leave Timer	Leave All Timer
1	Disabl ▼	Normal ▼	20	60	1000
2	Disabl ▼	Normal ▼	20	60	1000
3	Disabl ▼	Normal ▼	20	60	1000
4	Disabl ▼	Normal ▼	20	60	1000
5	Disabl ▼	Normal ▼	20	60	1000
6	Disabl ▼	Normal ▼	20	60	1000
7	Disabl ▼	Normal ▼	20	60	1000
8	Disabl ▼	Normal ▼	20	60	1000
9	Disabl ▼	Normal ▼	20	60	1000
10	Disabl ▼	Normal ▼	20	60	1000
11	Disabl ▼	Normal ▼	20	60	1000
12	Disabl ▼	Normal ▼	20	60	1000
13	Disabl ▼	Normal ▼	20	60	1000
14	Disabl ▼	Normal ▼	20	60	1000
15	Disabl ▼	Normal ▼	20	60	1000
16	Disabl ▼	Normal ▼	20	60	1000
17	Disabl ▼	Normal ▼	20	60	1000
18	Disabl ▼	Normal ▼	20	60	1000
19	Disabl ▼	Normal ▼	20	60	1000
20	Disabl ▼	Normal ▼	20	60	1000

Note, Timer unit is centisecond

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.

4.6.8 CLI Commands of 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 802.1Q Tunnel = access	Switch(config-if)# switchport dot1q-tunnel mode Set the interface as an IEEE 802.1Q tunnel mode Switch(config-if)# switchport dot1q-tunnel mode access Set the interface as an access port of IEEE

802.1Q Tunnel Uplink = uplink	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 – Show Running	Switch# show running-config 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 NameStatus Trunk Ports Access Ports ---- ------------ ------- -------------------------- -----------------

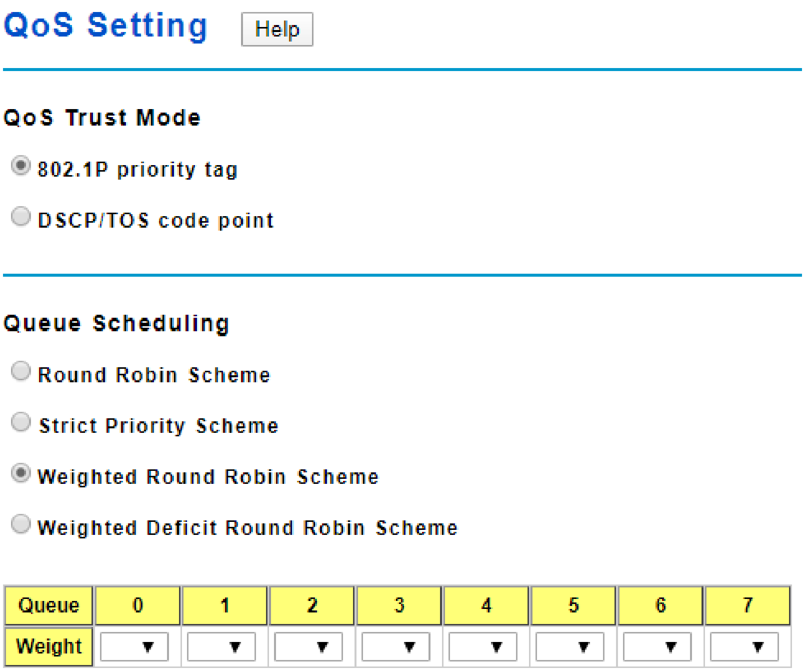
	--------- 1 VLAN1 Static - gi1-7,gi8-10 2 VLAN2 Unused - - 3 test Static gi4-7,gi8-10 gi1-3,gi7,gi8-10
Display – VLAN interface information	Switch# show interface vlan1 Interface vlan1 Description : N/A Administrative Status : Enable Operating Status : Up DHCP Client : Disable Primary IP Address : 192.168.10.1/24 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 theswitch 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 ! ….

4.7 Traffic Prioritization

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

JetNet 7500 series switch 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.

4.7.1 QoS Setting



QoS Setting

QoS Trust Mode

● 802.1P priority tag

○ DSCP/TOS code point

Queue Scheduling

○ Round Robin Scheme

○ Strict Priority Scheme

● Weighted Round Robin Scheme

○ Weighted Deficit Round Robin Scheme

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

QoS Trust Mode

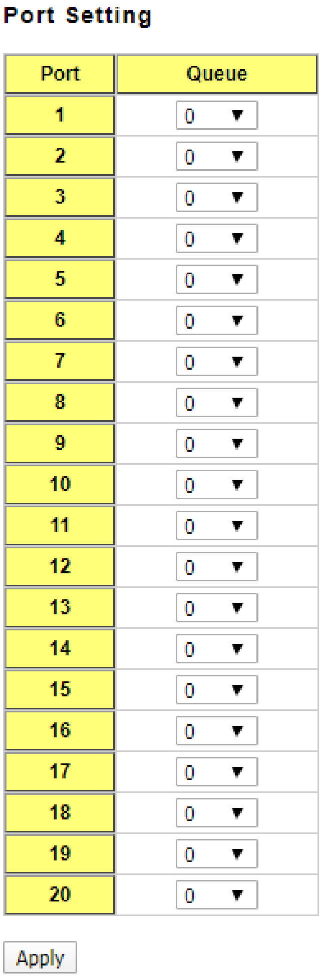
- **802.1P Priority Tag:** If 802.1P is selected the switch relies on a packet's CoS information to determine priority. This is related to the settings in the CoS-Queue Mapping page.
- **DSCP/TOS Code Point:** If DSCP/TOS is selected the switch relies on a packets differentiated services code point information to determine the priority. This is related to the settings in the DSCP-Priority Mapping page.

Queue Scheduling

Select the QoS scheduling mechanism.

- **Round Robin Scheme:** This scheme allows you to follow 1:1:1:1:1:1:1:1 rate to process priority queue from queue 7 to queue 0.
- **Strict Priority Scheme:** Packets with a higher priority in the queue are always processed first, unless there is a packet with a higher priority.

- **Weighted Round Robin Scheme:** This scheme allows you to assign a new weight ratio for each class. The 10 is the highest ratio. The ratio of each class is:
  Wx / W0 + W1 + W2 + W3 + W4 + W5 + W6 + W7 (Total volume of Queue 0-7)
- **Weighted Deficit Round Robin Scheme:** This scheme allows you to assign a new weight ratio for each class. The weight: 2032 is the maximum, the weight: 0 is the minimum and it has to be even. A setting of 0 establishes pure priority scheduling.
  The programmable weight setting ranges from 1 to 127.
  Total volume of Queue 0-7



Port Setting

Port	Queue
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	0
9	0
10	0
11	0
12	0
13	0
14	0
15	0
16	0
17	0
18	0
19	0
20	0

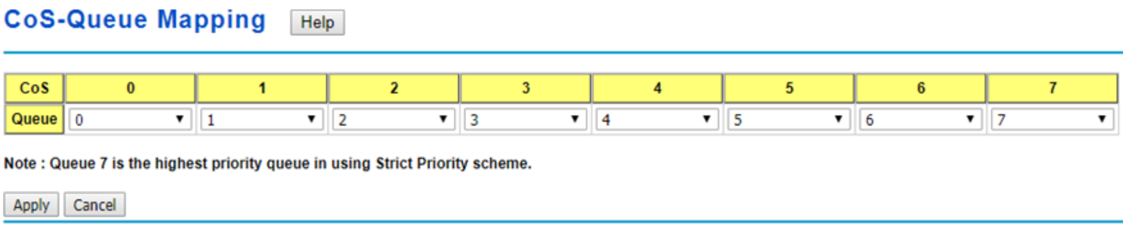
Choose the Queue value of each port, the port then has its default priority. The Queue 7 is the highest port-based queue, 0 is the lowest queue. The traffic injected to the port follows the queue level to be forwarded, but the outgoing traffic does not bring the queue level to next switch.

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

4.7.2 CoS-Queue Mapping

This page is to change CoS values to Physical Queue mapping table. Since the switch fabric of JetNet 7500 series switch 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 7500 series switch, 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.



CoS-Queue Mapping

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

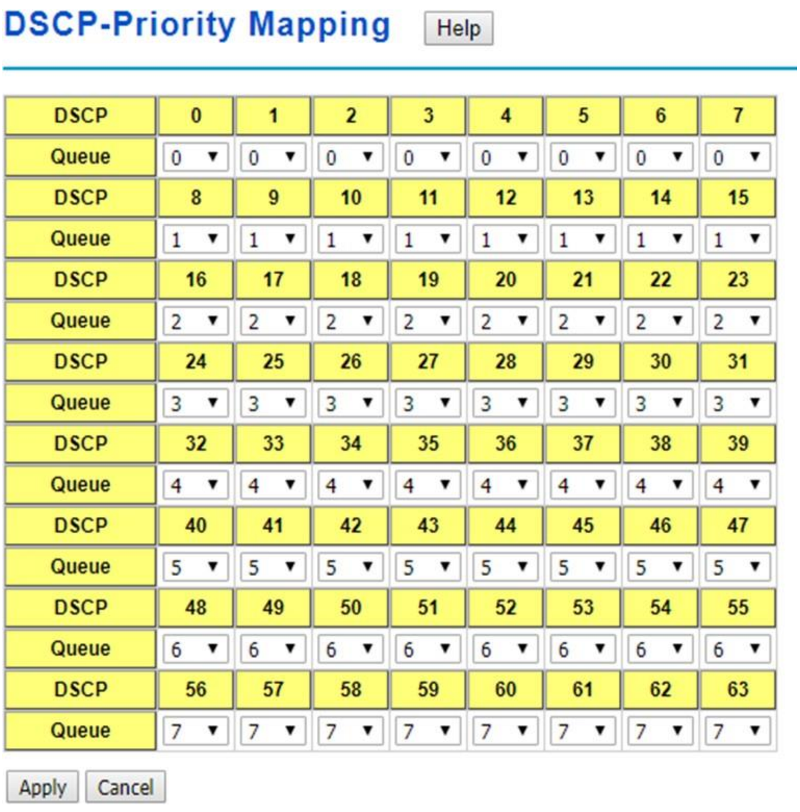
Note : Queue 7 is the highest priority queue in using Strict Priority scheme.

Click **Apply** to apply the setting.

Click **Cancel** to clear the modification.

4.7.3 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



DSCP-Priority Mapping

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

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

4.7.4 CLI Commands of the Traffic Prioritization

Command Lines of the Traffic Prioritization configuration

Feature	Command Line
QoS Setting	
Queue Scheduling – Strict Priority	Switch(config)# qos queue-sched rr Round Robin sp Strict Priority wrr Weighted Round Robin Switch(config)# qos queue-sched sp The queue scheduling scheme is setting to Strict Priority.
Queue Scheduling – Round Robin	Switch(config)# qos queue-sched rr The queue scheduling scheme is setting to Round Robin.
Queue 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
```

4.8 Multicast Filtering

For multicast filtering, JetNet 7500 series 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.

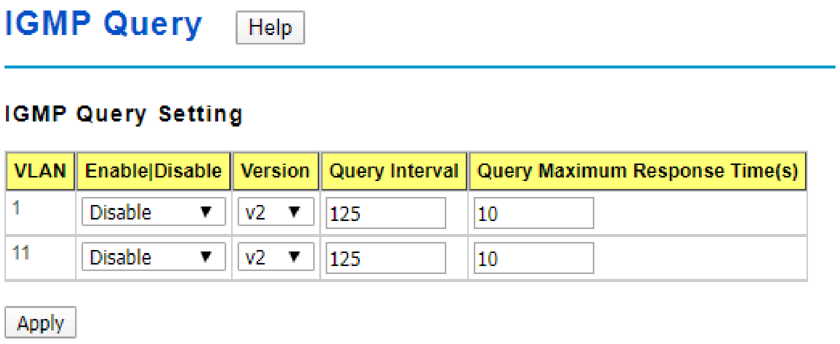
In effect, IGMP Snooping manages multicast traffic by making use of switches, routers, and hosts that support IGMP. Enabling IGMP Snooping allows the ports to detect IGMP queries, report packets, and manage multicast traffic through the switch. IGMP has three fundamental types of messages, as shown below:

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.

4.8.1 IGMP Query



IGMP Query Setting

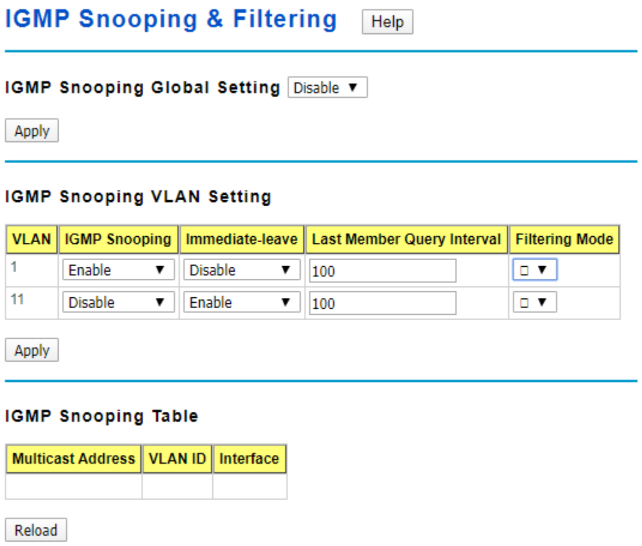
VLAN	Enable|Disable	Version	Query Interval	Query Maximum Response Time(s)
1	Disable ▼	v2 ▼	125	10
11	Disable ▼	v2 ▼	125	10

- **VLAN:** This is the VLAN interface.
- **Enable/Disable:** Set this to Enable to enable IGMP query messages on the switch's L3 VLAN or Disable to disable them.
- **Version:** This switch supports IGMP versions one and two. To use version one set this value to v1 or set it to v2 to use version two.
- **Query Interval(s):** This value determines how frequently in seconds IGMP query messages are sent out. This value should be greater than or equal to Query Maximum Response Time(s). Valid values are 1 to 65535.
- **Query Maximum Response Time(s):** The maximum response time in seconds advertised by IGMP query messages. Valid values are 1 to 25.

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

4.8.2 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 Disable ▼

IGMP Snooping VLAN Setting

VLAN	IGMP Snooping	Immediate-leave	Last Member Query Interval	Filtering Mode
1	Enable ▼	Disable ▼	100	□ ▼
11	Disable ▼	Enable ▼	100	□ ▼

IGMP Snooping Table

Multicast Address	VLAN ID	Interface

The Internet Group Management Protocol (IGMP) is an internal protocol of the Internet Protocol (IP) suite. IP manages multicast traffic by using switches, routers, and hosts that support IGMP. Enabling IGMP makes the switch gather multicast group membership information by snooping IGMP packets, which helps the device to switch IP multicast traffic to the ports where group members exist instead of flooding the traffic to every port.

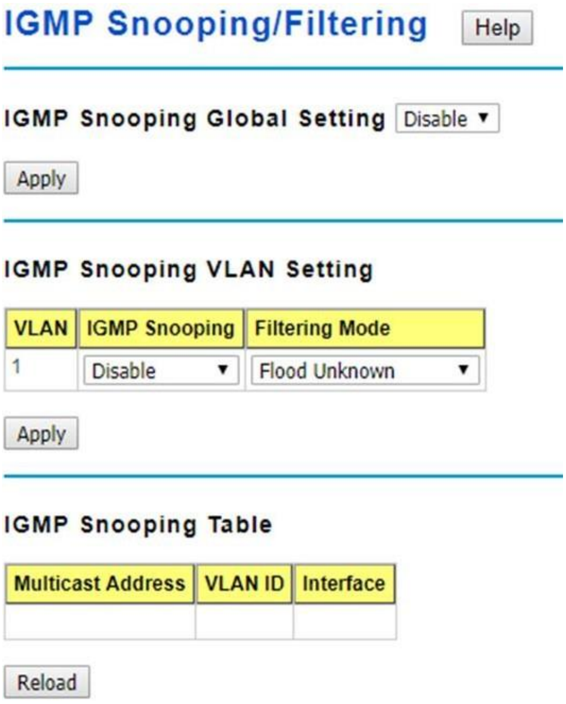
IGMP has three fundamental types of messages as follows:

Message	Description
Query	A message sent from the querier (IGMP router or switch) asking for a response from each host belonging 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 being a member of a specific multicast group.

The IGMP snooping/filtering functionality is configured on a VLAN basis.

By default IGMP snooping/filtering is disabled on the switch. To enable IGMP snooping/filtering you must first enable it globally and then enable it on each VLAN that you want IGMP snooping/filtering to operate on.

- **IGMP Snooping Global Setting:** Enable/Disable the IGMP snooping function and click the **Apply** button to change the IGMP snooping configuration.



IGMP Snooping/Filtering

IGMP Snooping Global Setting: Disable

IGMP Snooping VLAN Setting

VLAN	IGMP Snooping	Filtering Mode
1	Disable	Flood Unknown

IGMP Snooping Table

Multicast Address	VLAN ID	Interface

4.8.2.1 IGMP Snooping VLAN Setting

This section allows you to configure per VLAN settings for IGMP snooping/filtering.

- **VLAN:** The VLAN to configure IGMP snooping/filtering on.
- **IGMP Snooping:** Set this to Enable to enable IGMP snooping/filtering on the corresponding VLAN or to Disable to disable it.
- **Immediate-leave:** Leave group when receive a leave message.
- **Last Member Query Interval (centi seconds):** The interval for which the switch waits before updating the table entry.
- **Filtering Mode:** This setting determines how unknown multicast packets are handled. If the setting is **Flood 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 **Discard Unknown**, any unknown multicast packets will be discarded.

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

4.8.2.2 IGMP Snooping Table

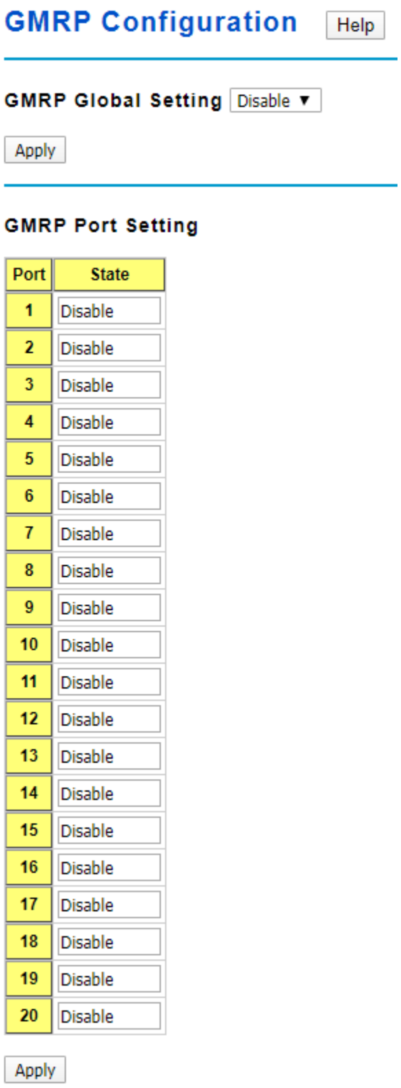
This table shows the IGMP groups the switch is aware of.

- **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 the **Reload** button to reload IGMP Snooping Table information.

4.8.3 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 Configuration

GMRP Global Setting: Disable

GMRP Port Setting

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

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.

4.8.4 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 nterface 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 nterface vlan1 enabled: Yes version: IGMPv2 query-interval: 125s query-max-response-time: 10s Switch# show running-config .... ! nterface 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

4.9 Routing

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

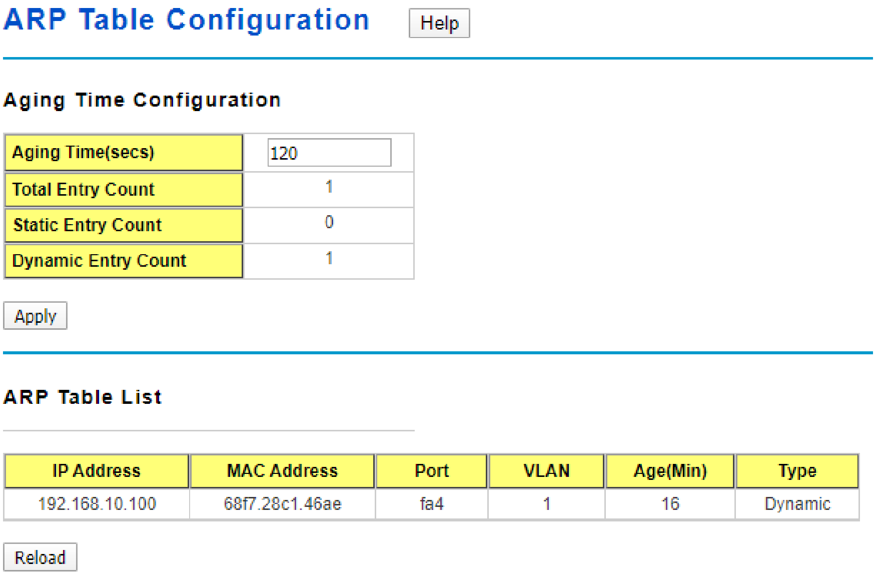
The JetNet 7500 series Layer 3 Switch equips with a Layer 3 chipset which can perform wire-speed layer 3 routing performance. The JetNet 7500 series Switch combines Layer 2 switching and Layer 3 routing within the single platform. In the Routing Configuration pages allows users create the Routing Interfaces, enable routing capability, enable unicast/multicast routing protocols, configure router redundancy policy and check the related routing information.

4.9.1 ARP

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

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

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



ARP Table Configuration

Aging Time Configuration

Aging Time(secs)	120
Total Entry Count	1
Static Entry Count	0
Dynamic Entry Count	1

ARP Table List

IP Address	MAC Address	Port	VLAN	Age(Min)	Type
192.168.10.100	68f7.28c1.46ae	fa4	1	16	Dynamic

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

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

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

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

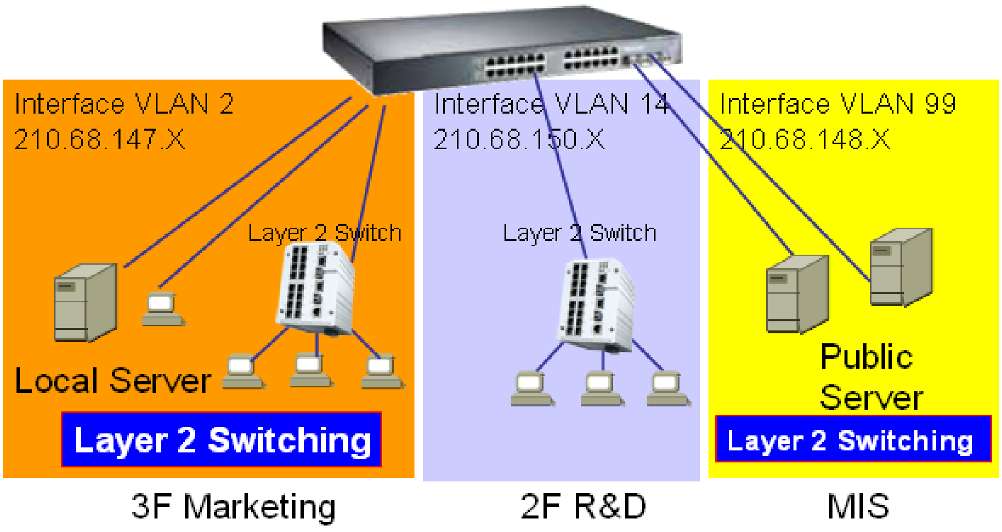
Dynamic Entry Count: This count represents for the count the ARP table dynamically learnt.

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

4.9.2 IP

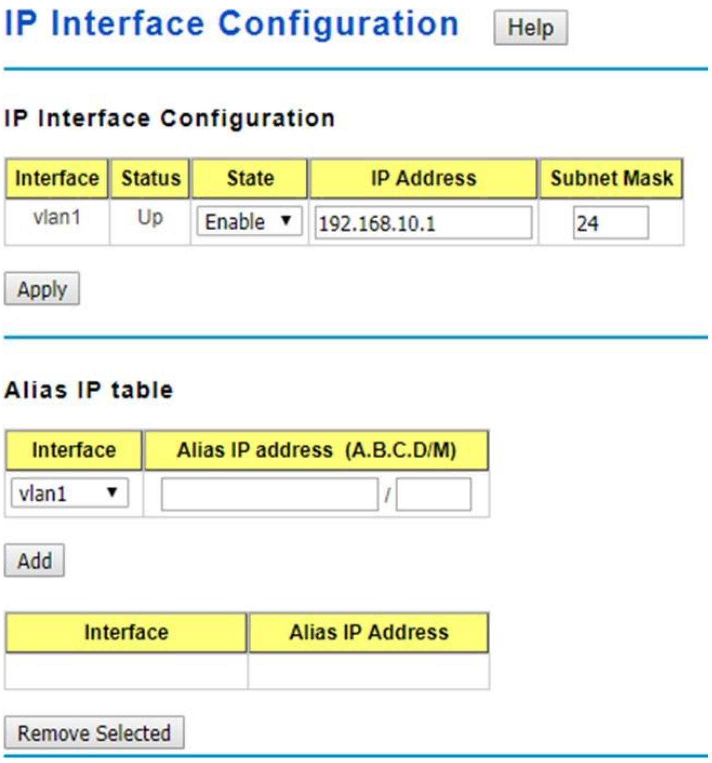
An IP Interface is the basic unit while routing, it is a logical interface which equips with an IP network and acts as the default gateway of the attached clients. The network interface can be a port or a single VLAN. All the client members connected to the IP network can be routed through the network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

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



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

IP Interface Configuration

Interface	Status	State	IP Address	Subnet Mask
vlan1	Up	Enable ▼	192.168.10.1	24

Alias IP table

Interface	Alias IP address (A.B.C.D/M)
vlan1 ▼	/

Interface	Alias IP Address

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

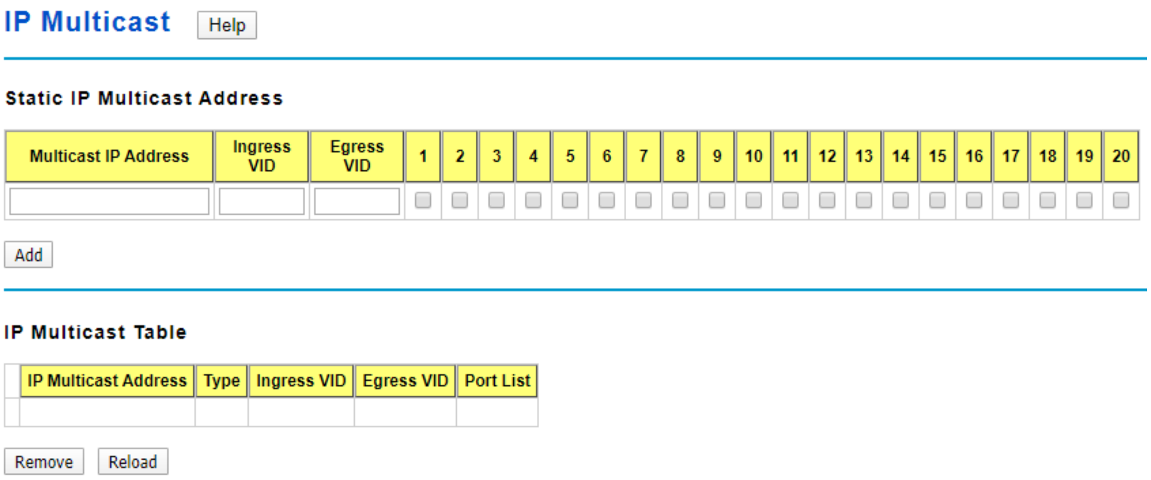
- **Interface:** The selected interface.
- **Alias IP Address:** The alias IP and its subnet mask.

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.

IP Multicast

This section allows you to manually add multicast IP addresses to the FIB. Manually entered addresses do not expire like automatically learned addresses do.



IP Multicast

Static IP Multicast Address

Multicast IP Address	Ingress VID	Egress VID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
			☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

IP Multicast Table

	IP Multicast Address	Type	Ingress VID	Egress VID	Port List

Static IP Multicast Address

- **Multicast IP Address:** The multicast IP address you want to manually enter into the FIB.
- **Ingress VID:** The Ingress VLAN you want to add the multicast IP address to.
- **Egress VID:** The Egress VLAN you want to add the multicast IP address to.
- **#:** The port number (where # is the port number) you want the mulitcast IP address to be associated with.

Click the **Add** button to add the static multicast IP address to the FIB.

IP Multicast Table

The IP Multicast Table displays the manually entered multicast IP addresses stored in the FIB.

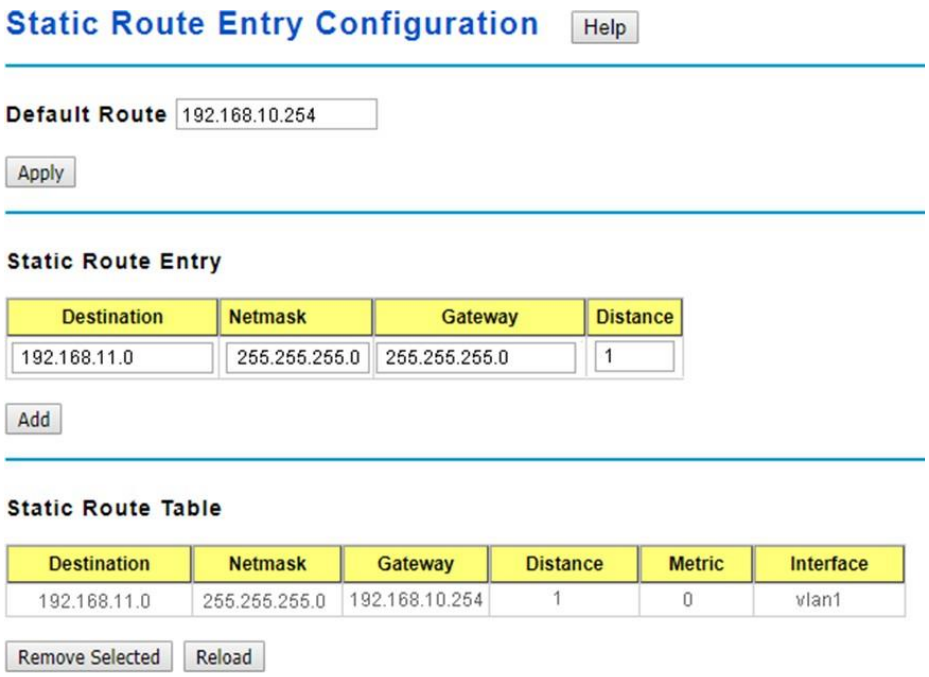
- **IP Multicast Address:** The multicast IP address of the FIB entry.
- **Type:** The type of address of the FIB entry, Static or Dynamic.
- **Ingress VID:** The Ingress VLAN.
- **Ingress VID:** The Egress VLAN.
- **Port List:** The port(s)that associated to this IP Address.

To remove an entry check the checkbox of the multicast IP address you want to remove and click the **Remove** button or click the **Reload** button to reload the table.

4.9.3 Router

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

4.9.3.1 Static Route Entry Configuration



Static Route Entry Configuration

Default Route 192.168.10.254

Static Route Entry

Destination	Netmask	Gateway	Distance
192.168.11.0	255.255.255.0	255.255.255.0	1

Static Route Table

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

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 to 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.

Click the **Apply** button to apply default route setting.

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

- **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.

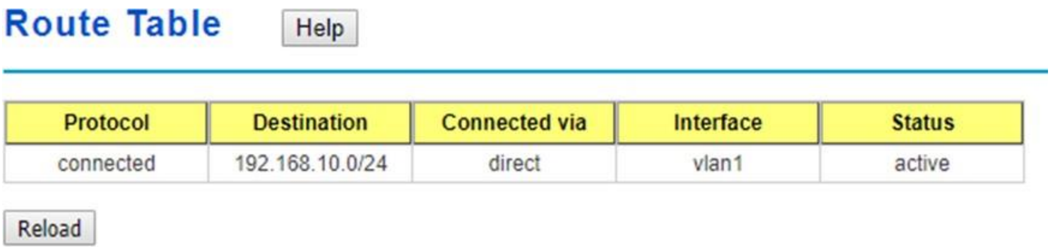
- **Distance:** The distance of static route entry.
- **Metric:** The metric of static route entry.
- **Interface:** The IP interface of static route entry via.

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

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

4.9.3.2 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.



Route Table

Protocol	Destination	Connected via	Interface	Status
connected	192.168.10.0/24	direct	vlan1	active

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

Destination: The destination network of this entry.

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

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

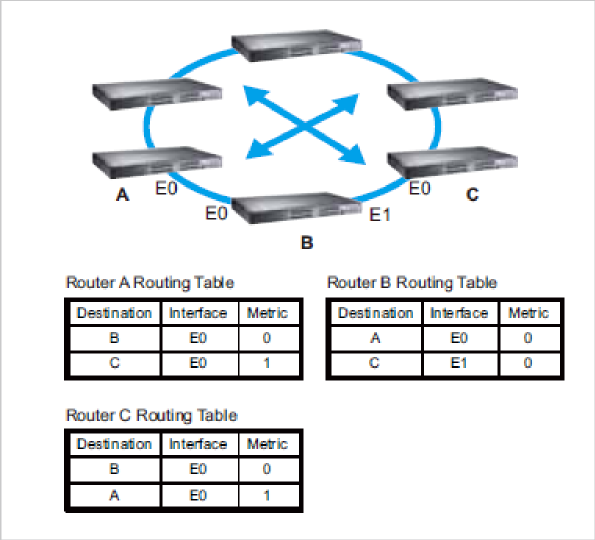
Status: Shows the entry is active or not.

4.9.4 RIP

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

RIP is the most known Distance Vector type dynamic routing protocol, or known as Hop Based routing protocol. It uses hop count as a distance metric, each router advertises its routing table every 30 seconds. The maximum routers RIP can support is 15, the 16th router represents Infinity. When a router receives a neighbor's table, it examines it entry by entry. If the destination is new, it is added to the local routing table. If the destination is known before and the update provides a smaller metric, the existing entry in the local routing table is replaced. Adds 1 (or sometimes more if the corresponding link is slow) to the metric. If no route updated within the cycles, the entry is removed.

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



Router A Routing Table

Destination	Interface	Metric
B	E0	0
C	E0	1

Router B Routing Table

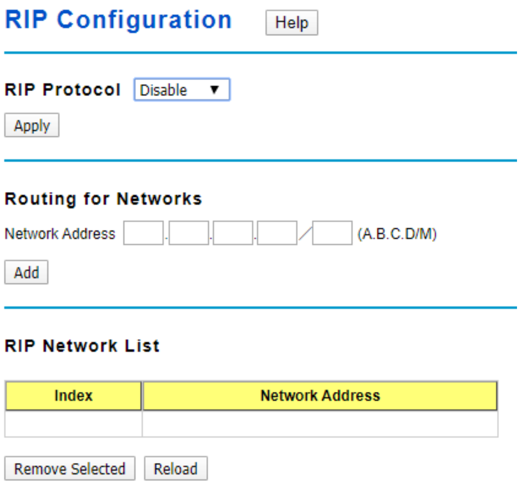
Destination	Interface	Metric
A	E0	0
C	E1	0

Router C Routing Table

Destination	Interface	Metric
B	E0	0
A	E0	1

4.9.4.1 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 Configuration

RIP Protocol: Disable ▼

Routing for Networks

Network Address [ ].[ ].[ ].[ ]/[ ] (A.B.C.D/M)

RIP Network List

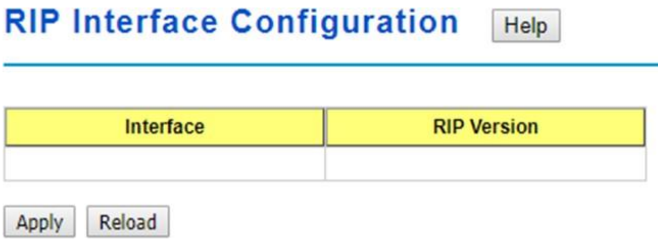
Index	Network Address

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.

4.9.4.2 RIP Interface Configuration

In RIP Interface Configuration, you can configure RIP version.



RIP Interface Configuration

Interface	RIP Version

Interface: The IP interface.

RIP Version: RIP version of IP interface.

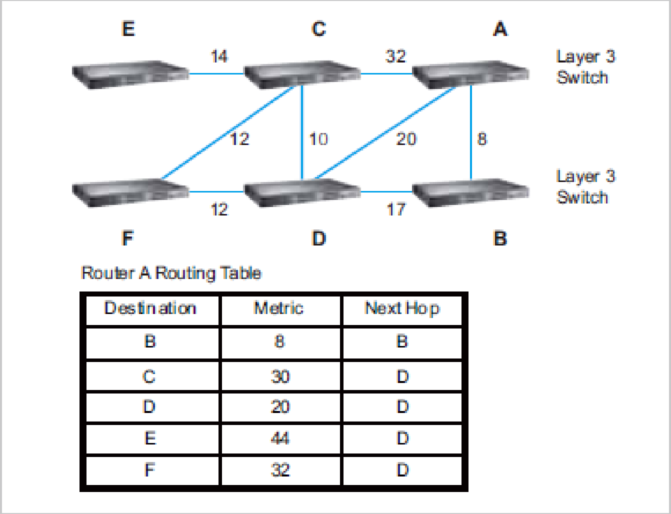
Click the **Apply** button to apply RIP interface settings.

Click the **Reload** button to reload RIP interface configuration.

4.9.5 OSPF

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

The figure in below 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.

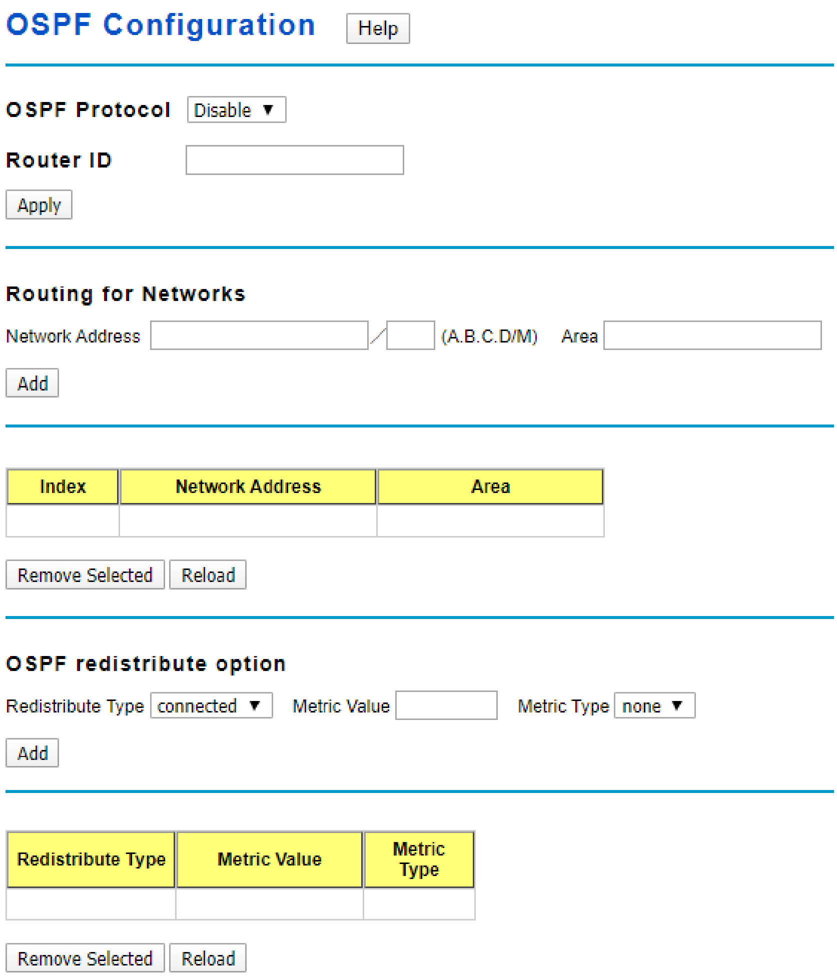
However, in link-state protocol, like the OSFP, the A to D to C is the shortest way. This is calculated by the *Dijkstra's SPF Algorithm.* After calculated and routing table updated, the metric from A to C is 32, the metric from A to D to C is 30. The A to D to C will be selected as the beast route from 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 7500 series 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.

4.9.5.1 OSPF Configuration

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



OSPF Configuration

OSPF Protocol: Disable

Router ID

Routing for Networks

Network Address / (A.B.C.D/M) Area

Index	Network Address	Area

OSPF redistribute option

Redistribute Type: connected Metric Value Metric Type: none

Redistribute Type	Metric Value	Metric Type

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.

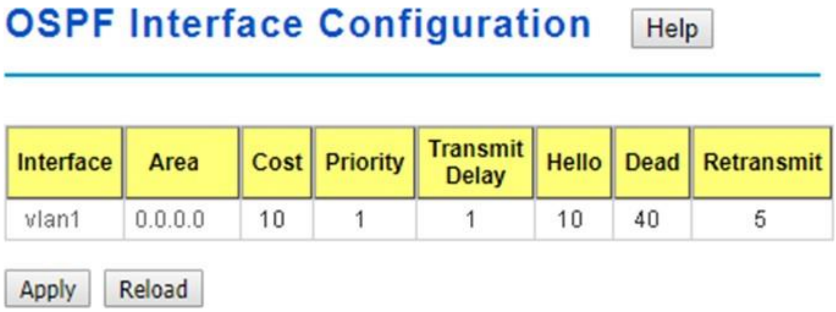
Redistribute Type: The type of routing entries for redistributing: connected, static or RIP.

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.

4.9.5.2 OSPF Interface Configuration

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



OSPF Interface Configuration

Interface	Area	Cost	Priority	Transmit Delay	Hello	Dead	Retransmit
vlan1	0.0.0.0	10	1	1	10	40	5

Interface: The VLAN Interface name.

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

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

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

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

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

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

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

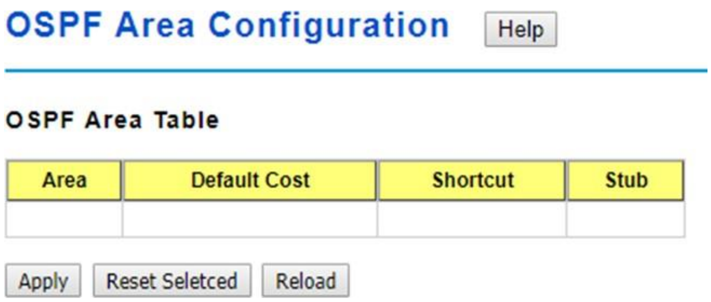
Once you finish configuring the settings, click on **Apply** to apply your configuration.

4.9.5.3 OSPF 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 7500 series 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.


OSPF Area Configuration

OSPF Area Table

Area	Default Cost	Shortcut	Stub

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

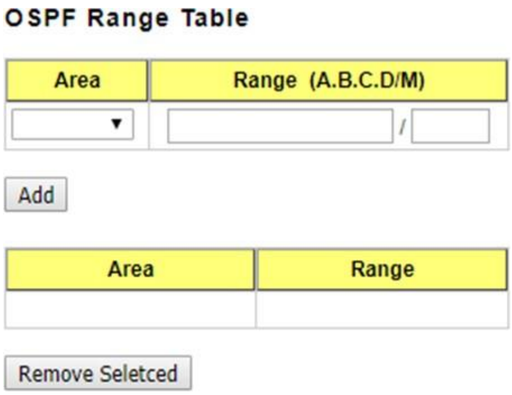
Default Cost: The default cost of the area ID.

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.

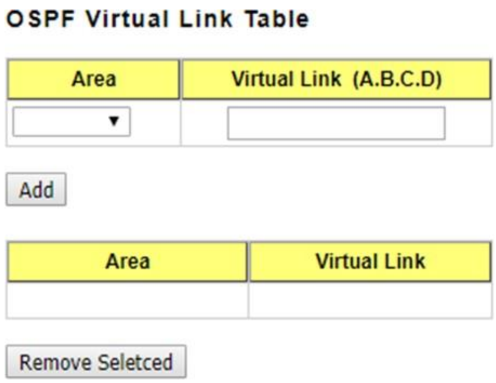

OSPF Range Table

Area	Range (A.B.C.D/M)
▾	/

Area	Range

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.



Area	Virtual Link (A.B.C.D)
▼	

Area	Virtual Link

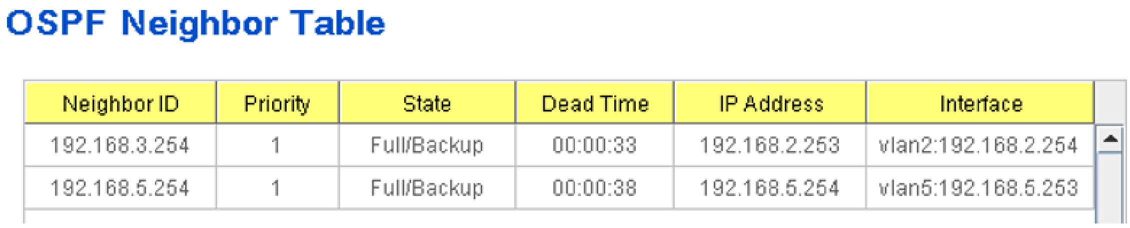
Virtual Link (A.B.C.D.): You can configure the virtual link. One area must be common area between two endpoint routers to create virtual links.

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.

4.9.5.4 OSPF Neighbor Table

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



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

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

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

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

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

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

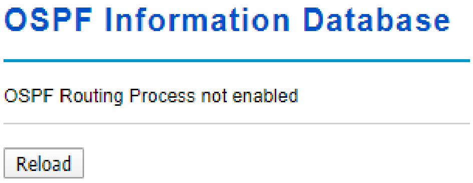
Full - the neighboring routers are fully adjacent and they will now appear in router-LSAs and network-LSAs.

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

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

4.9.5.5 OSPF Information Database

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



OSPF Information Database

OSPF Routing Process not enabled

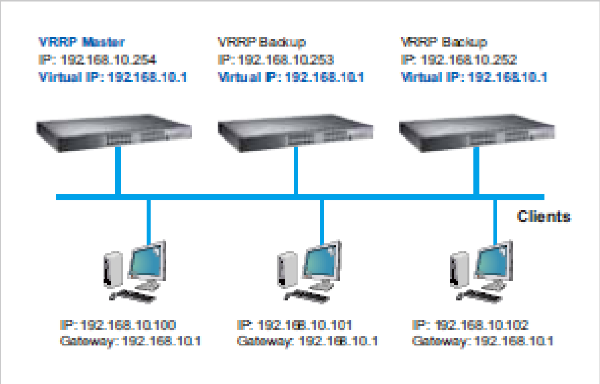
4.9.6 VRRP Configuration

The VRRP represent for the Virtual Router Redundancy Protocol.

To further ensure the high reliability of an environment, the JetNet 7500 series switch supports the VRRP protocol allowing the hosts to continuously direct traffic to the default gateway without the default gateway configuration change.

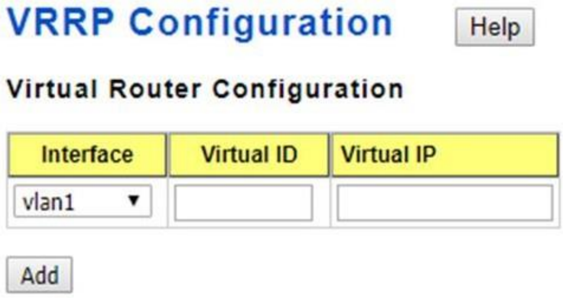
The figure for example, there are 3 VRRP-aware switches with the same Virtual IP of the VRRP, but different IP address of their VLAN/IP interface.

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.



4.9.6.1 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.



VRRP Configuration

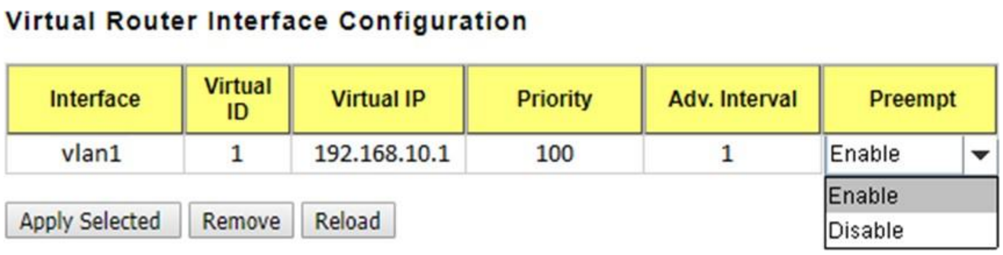
Virtual Router Configuration

Interface	Virtual ID	Virtual IP
vlan1		

Interface: Select the interface for the VRRP domain.

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

Virtual IP: This is the virtual IP of the VRRP domain. This is the Gateway IP of the clients. Click "**Add**" once you finish the configuration. Then you can see the entry is created in the Virtual Router Interface Configuration page



Virtual Router Interface Configuration

Interface	Virtual ID	Virtual IP	Priority	Adv. Interval	Preempt
vlan1	1	192.168.10.1	100	1	Enable

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

Interface: Select the interface for the VRRP domain.

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

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

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

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

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

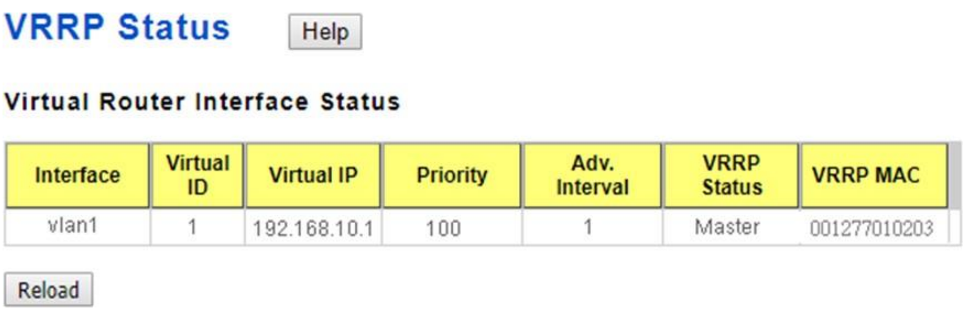
While the Preempt is **Enable** and the interface is VRRP Master, the interface will be recovered.

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.

4.9.6.2 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.



VRRP Status

Virtual Router Interface Status

Interface	Virtual ID	Virtual IP	Priority	Adv. Interval	VRRP Status	VRRP MAC
vlan1	1	192.168.10.1	100	1	Master	001277010203

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.

4.9.7 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 AgingTime 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

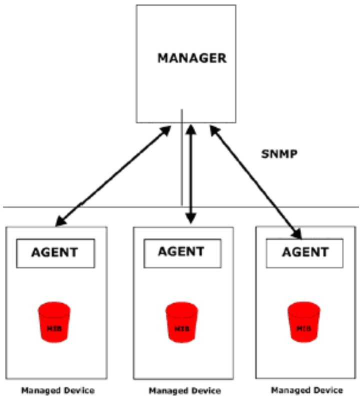
	default default for all interfaces Switch(config- router)# passive-interface default <cr>
RIP default Metric (usually = 1)	Switch(config-router)# default-metric <1-16> Default metric
RIP Setting	Switch# show ip rip status Routing Protocol is "rip" Sending updates every 30 seconds with +/-50%, next due 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 area0.0.0.0
Interface Configuration	
Hello Interface	Switch(config-if)# ip ospf hello-interval <1-65535> Seconds Switch(config-if)# ip ospf hello-interval 10
Link Cost Change	Switch(config-if)# ip ospf cost <1-65535> Cost
Link Priority	Switch(config-if)# ip ospf priority <0-255> Priority
Display	
IP OSPF Information	Switch# show ip ospf OSPF Routing Process, Router ID: 192.168.3.254 Supports only single TOS (TOS0) routes This implementation conforms to RFC2328 RFC1583Compatibility flag is disabled SPF schedule delay 1 secs, Hold time between two SPFs 1 secs Refresh timer 10 secs Number of external LSA 0 Number of areas attached to this router: 1 Area ID: 0.0.0.0 (Backbone) Number of interfaces in this area: Total: 3, Active: 3 Number of fully adjacent neighbors in this area: 1 Area has no authentication SPF algorithm executed 9 times Number of LSA 5
IP OSPF Datasheet	Switch# show ip ospf database

	OSPF Router with ID (192.168.3.254) Router Link States (Area 0.0.0.0) Link ID ADV Router Age Seq# CkSum Link count 192.168.3.253 192.168.3.253 928 0x80000009 0xf3b2 2 192.168.3.254 192.168.3.254 927 0x8000000a 0xd4aa 3 192.168.5.254 192.168.5.254 230 0x80000006 0xc248 2 Net Link States (Area 0.0.0.0) Link ID ADV Router Age Seq# CkSum 192.168.3.254 192.168.3.254 927 0x80000003 0x7437 192.168.4.253 192.168.5.254 235 0x80000003 0x7334
IP OSPF Interface Information	Switch# show ip ospf interface [IFNAME] Interface name Switch# show ip ospf interface vlan2 vlan2 is up Internet Address 192.168.2.253/24, Area 0.0.0.0 Router ID 192.168.3.253, Network Type BROADCAST, Cost 10 Transmit Delay is 1 sec, State DR, Priority 1 Designated Router (ID) 192.168.3.253, Interface Address 192.168.2.253 No backup designated router on this network Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5 Hello due in 00:00:02 Neighbor Count is 1, Adjacent neighbor count is 1
IP OSPF Neighbor Table	Switch# show ip ospf neighbor Neighbor ID Pri State Dead Time Address Interface -------------- --- -------------- --------- -------------- --------------- 0.0.0.0 1 Full/DROther 00:00:32 192.168.2.254 vlan2:192.168.2.25 3
IP OSPF Networking Routing Table	Switch# show ip ospf route ============ OSPF network routing table ============ N 192.168.2.0/24 [10] area: 0.0.0.0 directly attached to vlan2 N 192.168.3.0/24 [10] area: 0.0.0.0 directly attached to vlan3 N 192.168.11.0/24 [10] area: 0.0.0.0 directly attached to vlan1
OSPF Setting in Configuration file	Switch# show running-config …… router ospf router-id 192.168.3.253 network 192.168.2.0/24 area 0.0.0.0 network 192.168.3.0/24 area 0.0.0.0 network 192.168.11.0/24 area0.0.0.0

	! 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

4.10 SNMP



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

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.

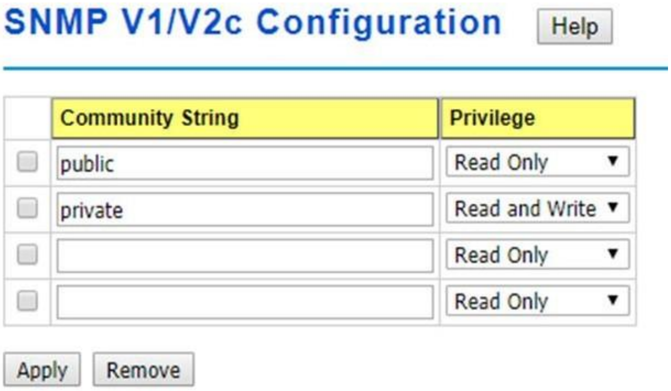
4.10.1 SNMP V1/V2c Configuration

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.



SNMP V1/V2c Configuration

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

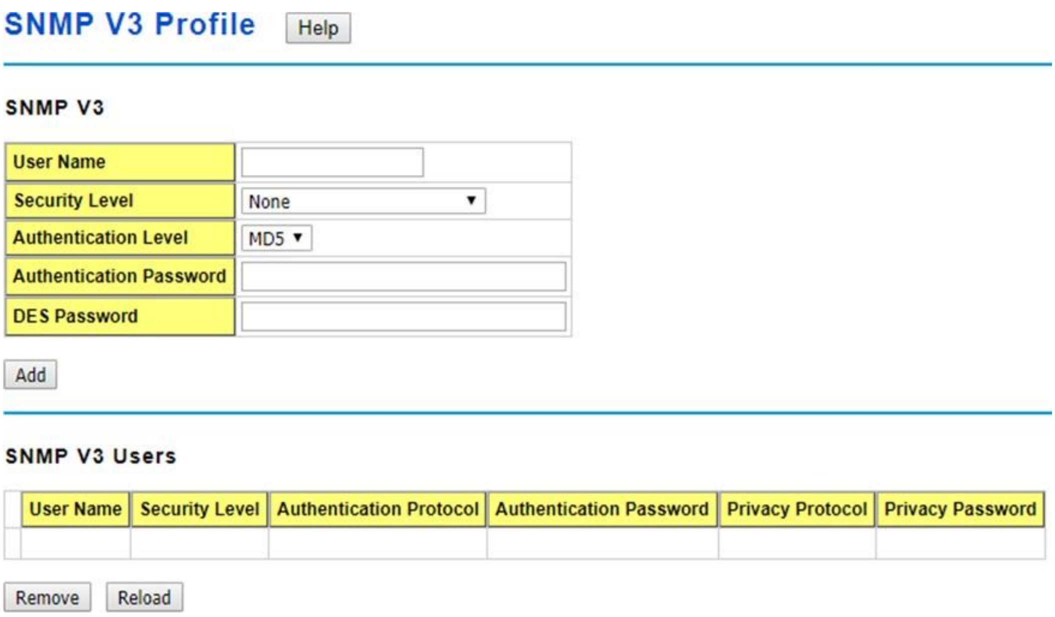
Click **“Apply”** to change the setting. Click **“Remove”** to remove the setting.

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.

4.10.2 SNMP V3 Profile

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



SNMP V3

User Name	
Security Level	None ▾
Authentication Level	MD5 ▾
Authentication Password	
DES Password	

SNMP V3 Users

	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password

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.

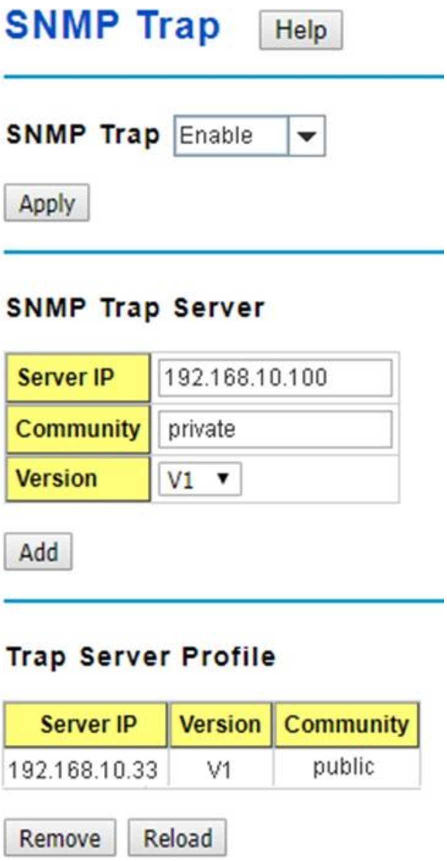
Privacy Password: This is the SNMP V3 user DES Encryption Password.

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

4.10.3 SNMP Traps

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

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



SNMP Trap: Enable

SNMP Trap Server

Server IP	192.168.10.100
Community	private
Version	V1

Trap Server Profile

Server IP	Version	Community
192.168.10.33	V1	public

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.

4.10.4 CLI Commands of the SNMP

Command Lines of the SNMP configuration

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

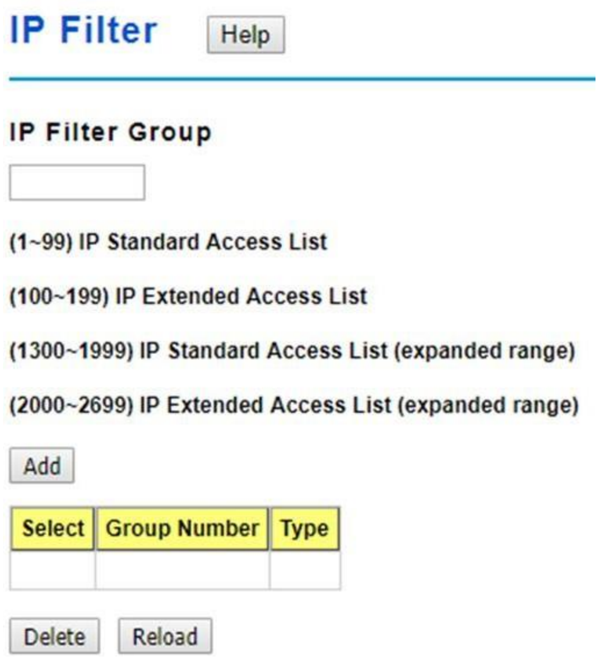
4.11 Security

JetNet 7500 series Switch provides 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.

4.11.1 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 7500 series Switch. 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 7500 series Switch, 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.

4.11.1.1 IP Filter



IP Filter

IP Filter Group

(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)

Select	Group Number	Type

You can create a group of IP Filters with following numbers. 1 - 99:

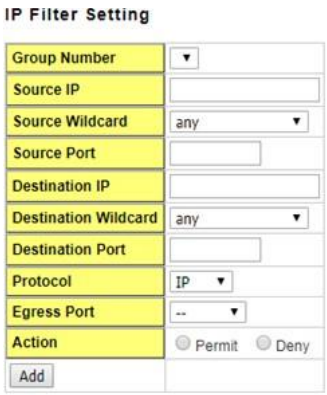
IP Standard Access List

100 – 199: IP Extended Access List

1300 – 1999: IP Standard Access List (expanded range) 2000 –

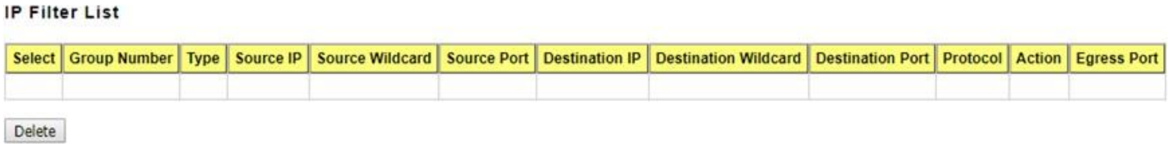
2699: IP Extended Access List (expanded range)

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



IP Filter Setting

Group Number	▾
Source IP	
Source Wildcard	any ▾
Source Port	
Destination IP	
Destination Wildcard	any ▾
Destination Port	
Protocol	IP ▾
Egress Port	-- ▾
Action	○ Permit ○ Deny
Add	



IP Filter List

Select	Group Number	Type	Source IP	Source Wildcard	Source Port	Destination IP	Destination Wildcard	Destination Port	Protocol	Action	Egress Port

Delete

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).

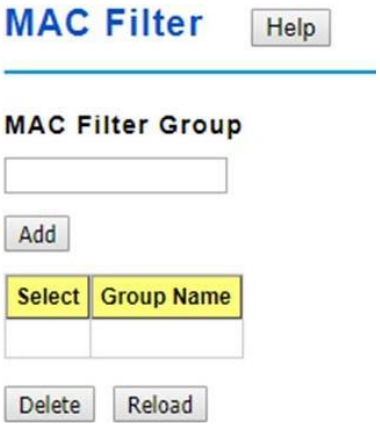
Protocol: This is the L4 protocol (TCP/UDP/ICMP).

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.

4.11.1.2 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.



Select	Group Name

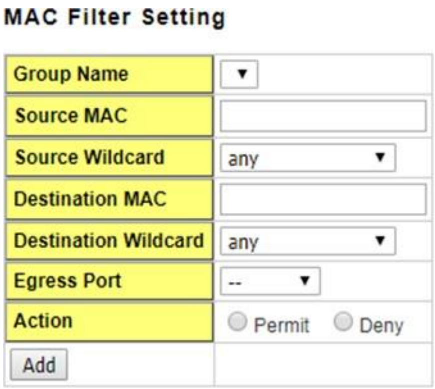
You can create a group of MAC Filters by entering a name and clicking the **Add** button to create a new Filter Group.

The MAC Filter Group table provides the following information.

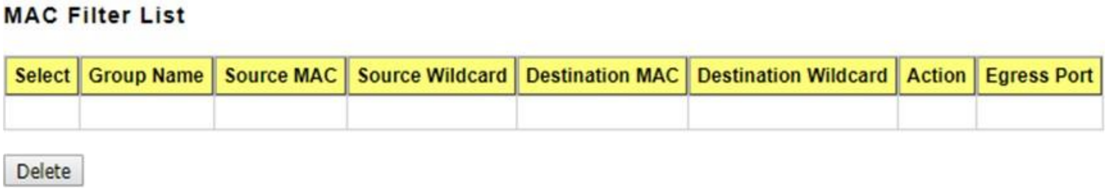
Select: If you select this and click the **Delete** button the corresponding Filter Group is deleted.

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

Reload button to reload the Filter Group table.



Group Name	▼
Source MAC	
Source Wildcard	any ▼
Destination MAC	
Destination Wildcard	any ▼
Egress Port	-- ▼
Action	○ Permit ○ Deny



Select	Group Name	Source MAC	Source Wildcard	Destination MAC	Destination Wildcard	Action	Egress Port

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

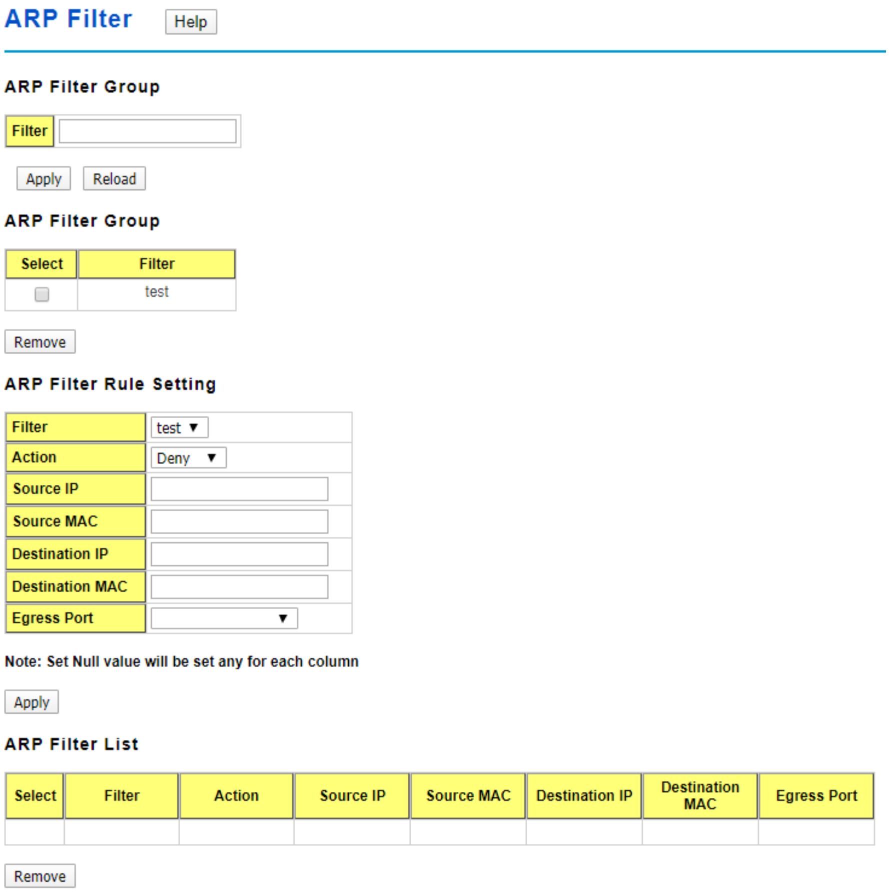
the filter action, which is to deny or permit the packet. **Egress Port**: This is

the outgoing (exiting) port number.

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

APR Filter

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



ARP Filter

ARP Filter Group

Filter	

ARP Filter Group

Select	Filter
□	test

ARP Filter Rule Setting

Filter	test ▼
Action	Deny ▼
Source IP	
Source MAC	
Destination IP	
Destination MAC	
Egress Port	▼

Note: Set Null value will be set any for each column

ARP Filter List

Select	Filter	Action	Source IP	Source MAC	Destination IP	Destination MAC	Egress Port

ARP Filter Group

You can create a group of ARP Filters with name.

- **Select:** Select this field to delete the entry and then click the **Delete** button.
- **Filter:** This is name that represents the Filter Group.

Click the **Remove** button to remove the Filter.

ARP Filter Rule Setting

You can configure the ARP Filter.

- **Filter:** Name of the Filter Group.
- **Action:** This is the filter action, which is to deny or permit the packet.
- **Source IP:** This is the source IP address of the packet.
- **Source MAC:** This for the source MAC of the packet.
- **Destination IP:** This is the destination IP address of the packet.
- **Destination MAC:** This is the destination MAC of the packet.
- **Egress Port:** This is the outgoing (exiting) port number.

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

ARP Filter List

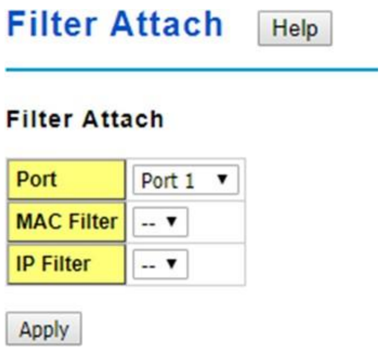
This is the ARP Filter List.

- **Select:** Selected for delete.
- **Filter:** Name of the Filter Group.
- **Action:** This is the filter action, which is to deny or permit the packet.
- **Source IP:** This is the source IP address of the packet.
- **Source MAC:** This for the source MAC of the packet.
- **Destination IP:** This is the destination IP address of the packet.
- **Destination MAC:** This is the destination MAC of the packet.
- **Egress Port:** This is the outgoing (exiting) port number.

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

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	Port 1 ▼
MAC Filter	-- ▼
IP Filter	-- ▼

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

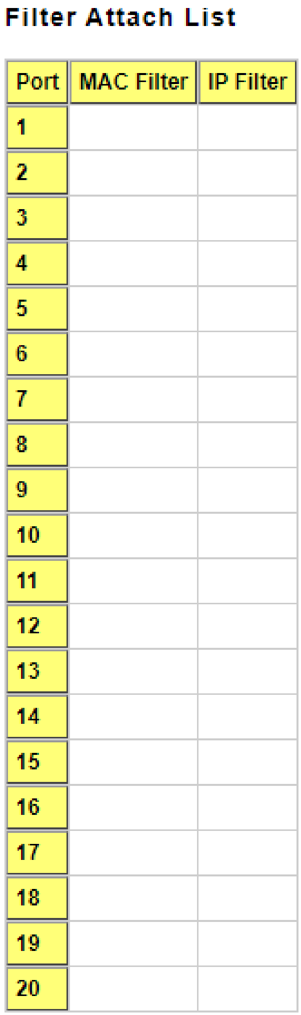
MAC Filter: Select a MAC address based filter to attach to the interface. Select "--" to remove an attached MAC address filter.

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.



Filter Attach List

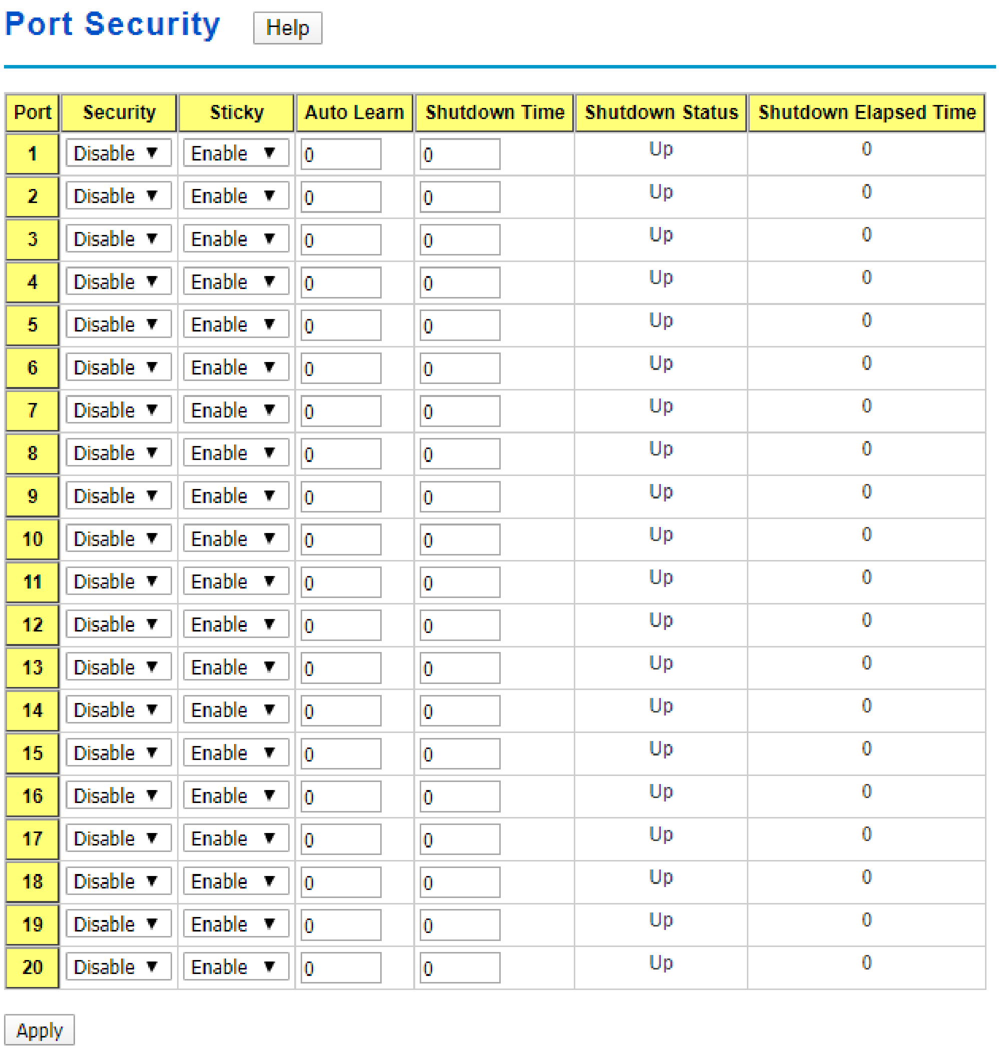
Port	MAC Filter	IP Filter
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		

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.

4.11.2 Port Security

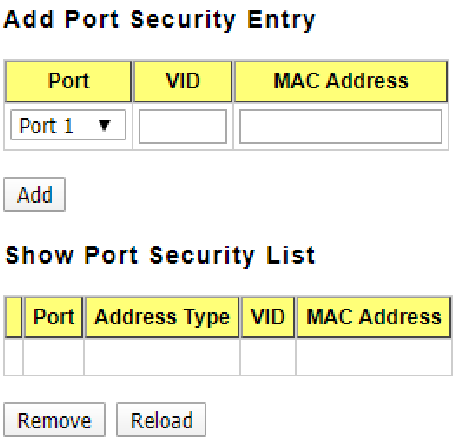


Port Security

Port	Security	Sticky	Auto Learn	Shutdown Time	Shutdown Status	Shutdown Elapsed Time
1	Disable ▼	Enable ▼	0	0	Up	0
2	Disable ▼	Enable ▼	0	0	Up	0
3	Disable ▼	Enable ▼	0	0	Up	0
4	Disable ▼	Enable ▼	0	0	Up	0
5	Disable ▼	Enable ▼	0	0	Up	0
6	Disable ▼	Enable ▼	0	0	Up	0
7	Disable ▼	Enable ▼	0	0	Up	0
8	Disable ▼	Enable ▼	0	0	Up	0
9	Disable ▼	Enable ▼	0	0	Up	0
10	Disable ▼	Enable ▼	0	0	Up	0
11	Disable ▼	Enable ▼	0	0	Up	0
12	Disable ▼	Enable ▼	0	0	Up	0
13	Disable ▼	Enable ▼	0	0	Up	0
14	Disable ▼	Enable ▼	0	0	Up	0
15	Disable ▼	Enable ▼	0	0	Up	0
16	Disable ▼	Enable ▼	0	0	Up	0
17	Disable ▼	Enable ▼	0	0	Up	0
18	Disable ▼	Enable ▼	0	0	Up	0
19	Disable ▼	Enable ▼	0	0	Up	0
20	Disable ▼	Enable ▼	0	0	Up	0

- **Port:** The port identifier.
- **Security:** Enable or disable port security on this port.
- **Sticky:** Enable or disable sticky on this port.
- **Auto Learn:** It specifies maximum number of MAC addresses that can be dynamically learned on the port, valid range is 0-10
- **Shutdown Time:** It specifies for how long to shutdown the port, valid range is 0-86400 seconds, if a security violation occurs.
- **Shutdown Status:** It displays the port is shutdown or not.
- **Shutdown Elapsed Time:** It displays the elapsed time of port shutdown.

Click the **Apply** button to apply Port Security State configurations.



Add Port Security Entry

Port	VID	MAC Address
Port 1 ▼		

Show Port Security List

	Port	Address Type	VID	MAC Address

Add Port Security Entry:

- **Port:** The port id, if you want to insert a new MAC entry, the port ID must be correct when creating a new entry.
- **VID:** The VLAN id, if you want to insert a new MAC entry, the VLAN id must be correct when creating a new entry.
- **MAC Address:** MAC address of the entry.

Click the **Add** button to add a Port Security Entry.

Show Port Security List:

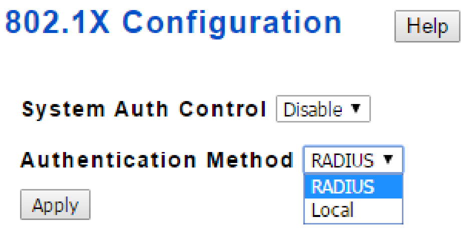
- **Port:** The port id of the entry.
- **Address Type:** Type of Security MAC address. Security is static security mac address. LSecurity is auto learned mac address
- **VID:** The VLAN ID of the entry.
- **MAC Address:** MAC address of the entry.

Click the **Remove** button to remove the selected Port Security Entry.

4.11.3 IEEE 802.1x

4.11.3.1 802.1XConfiguration

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 7500 series Switch could control which connection is available or not.



802.1X Configuration

System Auth Control: Disable ▼

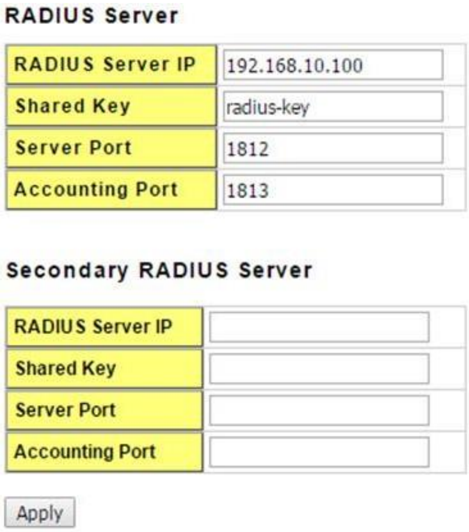
Authentication Method: RADIUS ▼

System Auth Control: 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

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

Secondary RADIUS Server

RADIUS Server IP	
Shared Key	
Server Port	
Accounting Port	

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.

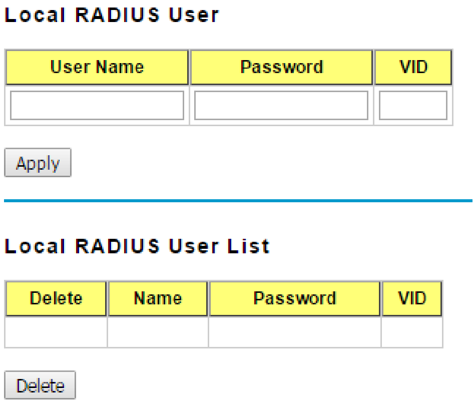
Accounting Port: Port for packets that contain the information of account login or logout.

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



Local RADIUS User

User Name	Password	VID

Local RADIUS User List

Delete	Name	Password	VID

User Name: The user name of the local

Password: The password of the local R

VID: The VLAN ID of the local RADIUS

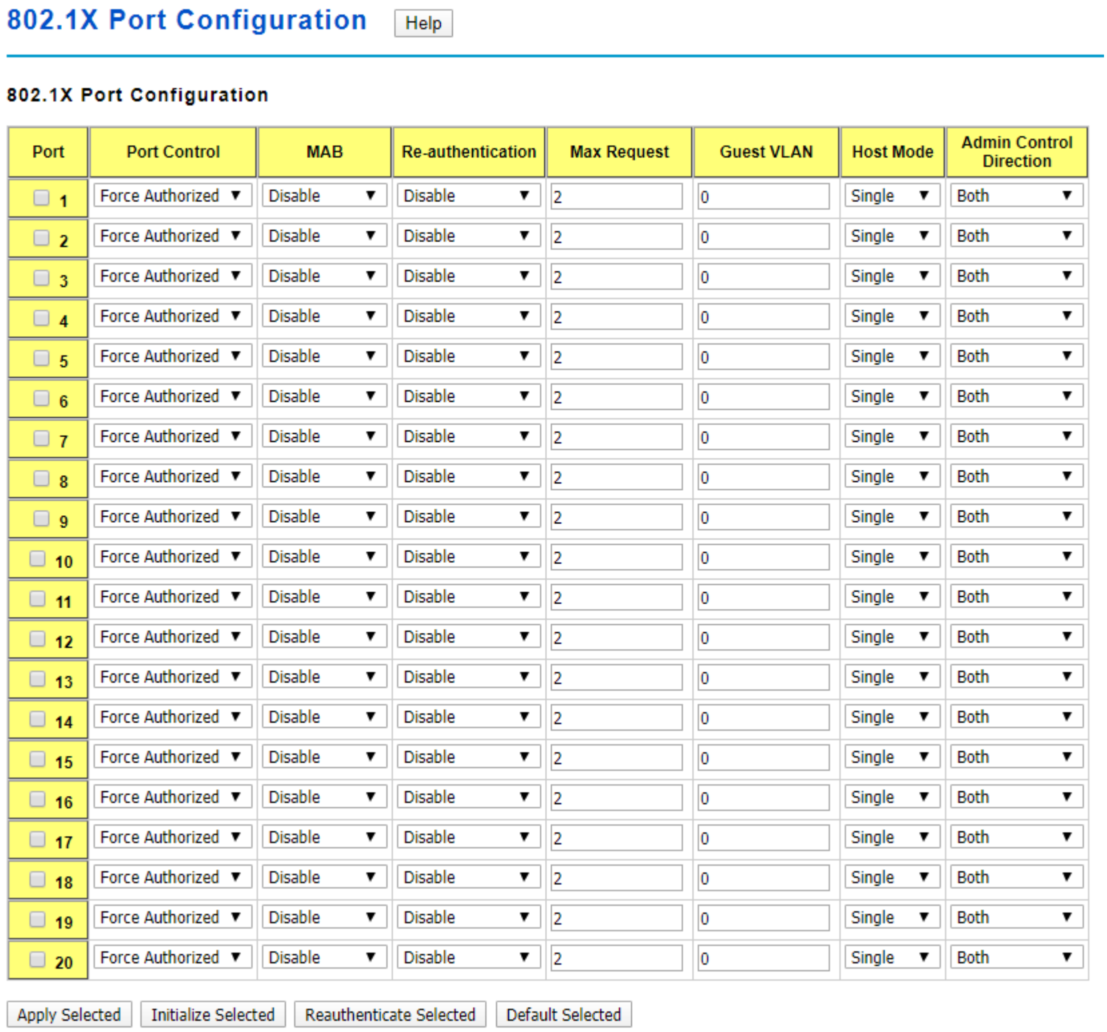
Click **Apply** to add a local RADIUS user.

802.1X Local user List: Shows the account information. Click

Delete to delete the selected user.

4.11.3.2 802.1X Port Configuration

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



802.1X Port Configuration

Port	Port Control	MAB	Re-authentication	Max Request	Guest VLAN	Host Mode	Admin Control Direction
☐ 1	Force Authorized	Disable	Disable	2	0	Single	Both
☐ 2	Force Authorized	Disable	Disable	2	0	Single	Both
☐ 3	Force Authorized	Disable	Disable	2	0	Single	Both
☐ 4	Force Authorized	Disable	Disable	2	0	Single	Both
☐ 5	Force Authorized	Disable	Disable	2	0	Single	Both
☐ 6	Force Authorized	Disable	Disable	2	0	Single	Both
☐ 7	Force Authorized	Disable	Disable	2	0	Single	Both
☐ 8	Force Authorized	Disable	Disable	2	0	Single	Both
☐ 9	Force Authorized	Disable	Disable	2	0	Single	Both
☐ 10	Force Authorized	Disable	Disable	2	0	Single	Both
☐ 11	Force Authorized	Disable	Disable	2	0	Single	Both
☐ 12	Force Authorized	Disable	Disable	2	0	Single	Both
☐ 13	Force Authorized	Disable	Disable	2	0	Single	Both
☐ 14	Force Authorized	Disable	Disable	2	0	Single	Both
☐ 15	Force Authorized	Disable	Disable	2	0	Single	Both
☐ 16	Force Authorized	Disable	Disable	2	0	Single	Both
☐ 17	Force Authorized	Disable	Disable	2	0	Single	Both
☐ 18	Force Authorized	Disable	Disable	2	0	Single	Both
☐ 19	Force Authorized	Disable	Disable	2	0	Single	Both
☐ 20	Force Authorized	Disable	Disable	2	0	Single	Both

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.

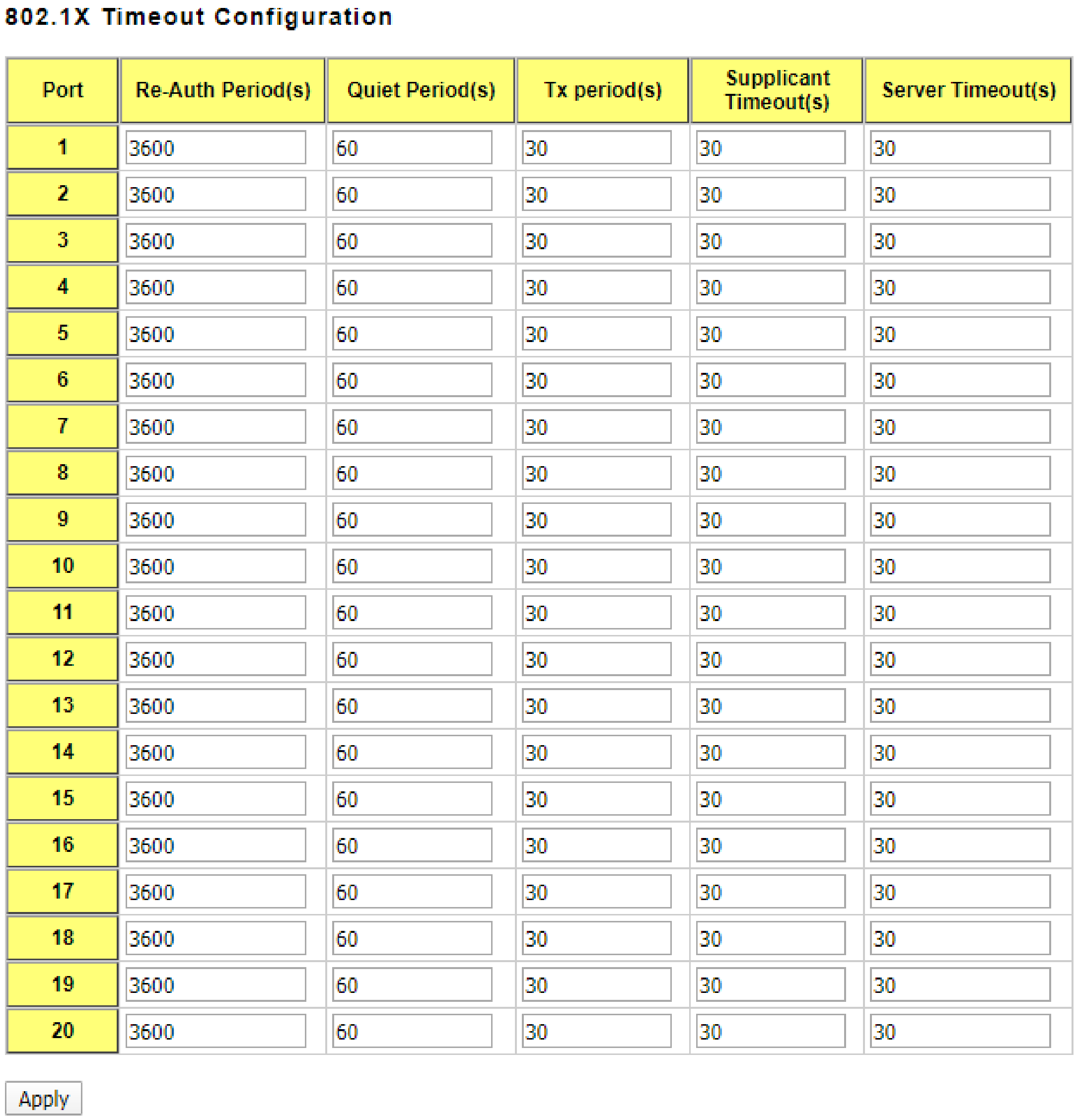
Admin Control Direction: Determined devices can end data out only or both send and receive.

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
11	3600	60	30	30	30
12	3600	60	30	30	30
13	3600	60	30	30	30
14	3600	60	30	30	30
15	3600	60	30	30	30
16	3600	60	30	30	30
17	3600	60	30	30	30
18	3600	60	30	30	30
19	3600	60	30	30	30
20	3600	60	30	30	30

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.

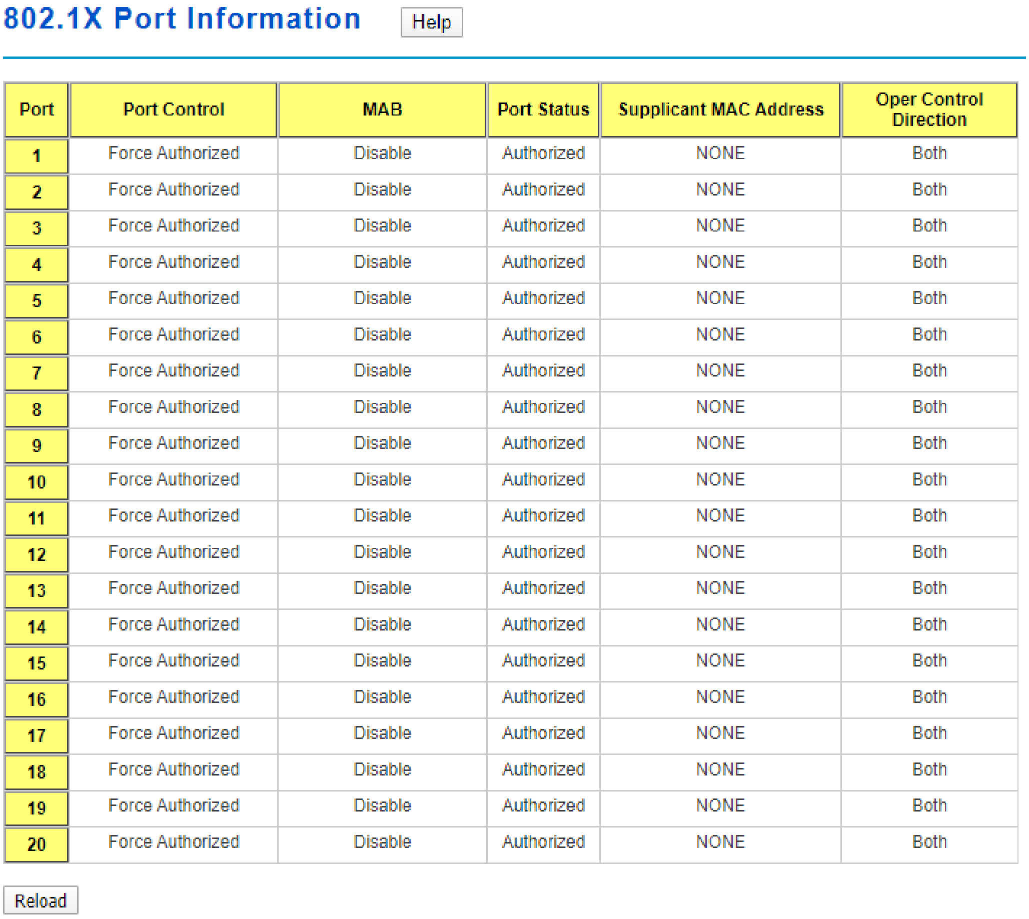
Supplicant Timeout(s): the timeout for the client authenticating **Sever**

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.

4.11.3.3 802.1X Port Information

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



Port	Port Control	MAB	Port Status	Supplicant MAC Address	Oper Control Direction
1	Force Authorized	Disable	Authorized	NONE	Both
2	Force Authorized	Disable	Authorized	NONE	Both
3	Force Authorized	Disable	Authorized	NONE	Both
4	Force Authorized	Disable	Authorized	NONE	Both
5	Force Authorized	Disable	Authorized	NONE	Both
6	Force Authorized	Disable	Authorized	NONE	Both
7	Force Authorized	Disable	Authorized	NONE	Both
8	Force Authorized	Disable	Authorized	NONE	Both
9	Force Authorized	Disable	Authorized	NONE	Both
10	Force Authorized	Disable	Authorized	NONE	Both
11	Force Authorized	Disable	Authorized	NONE	Both
12	Force Authorized	Disable	Authorized	NONE	Both
13	Force Authorized	Disable	Authorized	NONE	Both
14	Force Authorized	Disable	Authorized	NONE	Both
15	Force Authorized	Disable	Authorized	NONE	Both
16	Force Authorized	Disable	Authorized	NONE	Both
17	Force Authorized	Disable	Authorized	NONE	Both
18	Force Authorized	Disable	Authorized	NONE	Both
19	Force Authorized	Disable	Authorized	NONE	Both
20	Force Authorized	Disable	Authorized	NONE	Both

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.

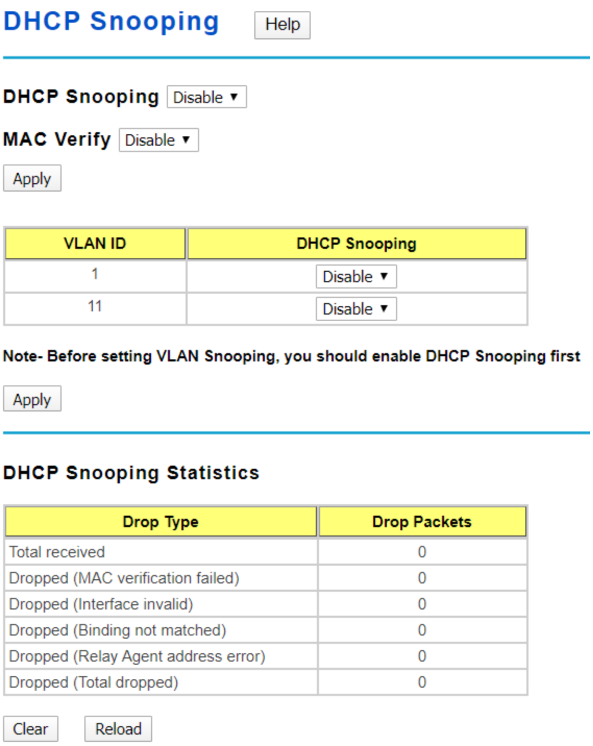
Authorized Supplicant: The MAC address of the authorized supplicant.

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

4.11.4 DHCP Snooping

DHCP snooping acts like a firewall between untrusted hosts and trusted DHCP servers. DHCP snooping provides a valuable security function and is required to support IP Source Guard.



DHCP Snooping Disable ▾

MAC Verify Disable ▾

VLAN ID	DHCP Snooping
1	Disable ▾
11	Disable ▾

Note- Before setting VLAN Snooping, you should enable DHCP Snooping first

DHCP Snooping Statistics

Drop Type	Drop Packets
Total received	0
Dropped (MAC verification failed)	0
Dropped (Interface invalid)	0
Dropped (Binding not matched)	0
Dropped (Relay Agent address error)	0
Dropped (Total dropped)	0

- **DHCP Snooping:** Enables/Disables DHCP snooping globally.
- **MAC Verify:** Enables/Disables MAC Verify globally. If this option is enabled, the Layer 2 DHCP Snooping module will verify the source MAC address against the client hardware address in the received DHCP packets.

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

DHCP Snooping Statistics

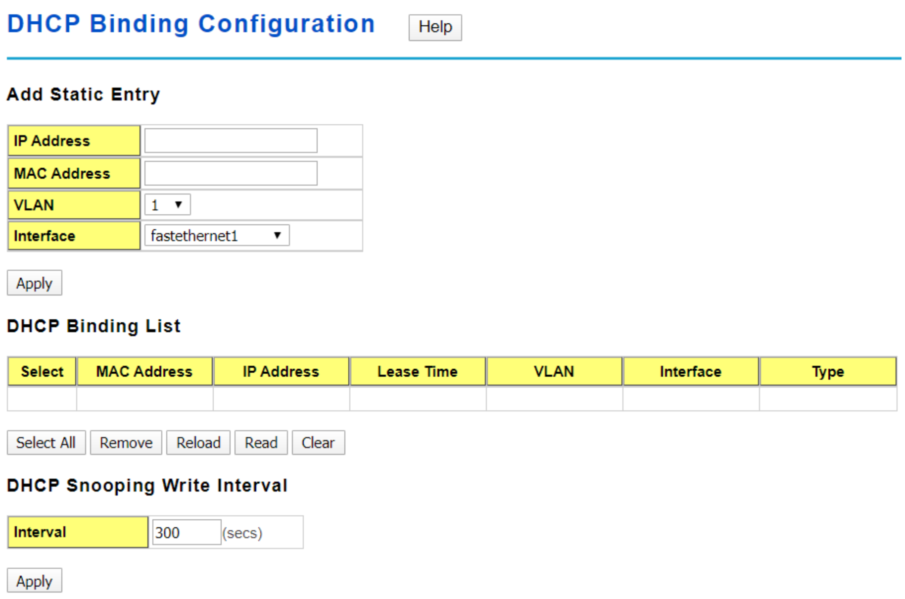
The table shows the drop reason of packets, including the following reason:

- **Total received:** The number of snooping packets which is received.
- **MAC verification failed:** The number of MAC verification failed packets.
- **Interface invalid:** Request packet is not matched to it's interface.
- **Binding not matched:** Counts the packets which the binding is not matched.
- **Relay Agent address error:** Counts the relay agent address error packets.
- **Total dropped:** The number of snooping packets which is dropped.

Click the **Clear** button to clear the drop-packet count.
Click the **Reload** button to refresh the drop-packet count.

4.11.5 DHCP Binding

DHCP Snooping Binding Configuration shows the snooping binding table. And also, you can add a static entry.



DHCP Binding Configuration

Add Static Entry

IP Address	
MAC Address	
VLAN	1 ▾
Interface	fastethernet1 ▾

DHCP Binding List

Select	MAC Address	IP Address	Lease Time	VLAN	Interface	Type

DHCP Snooping Write Interval

Interval	300 (secs)

Add Static Entry:

- **MAC Address:** MAC of the entry.
- **IP Address:** IP of the entry.
- **VLAN:**VLAN of the entry.
- **Interface:** Interface of the entry.

Click the **Apply** button to add a static entry.

DHCP Binding List:

- **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 belong VLAN's ID.
- **Interface:** Interface of the entry.
- **Type:** The entry type: Static/Dynamic.

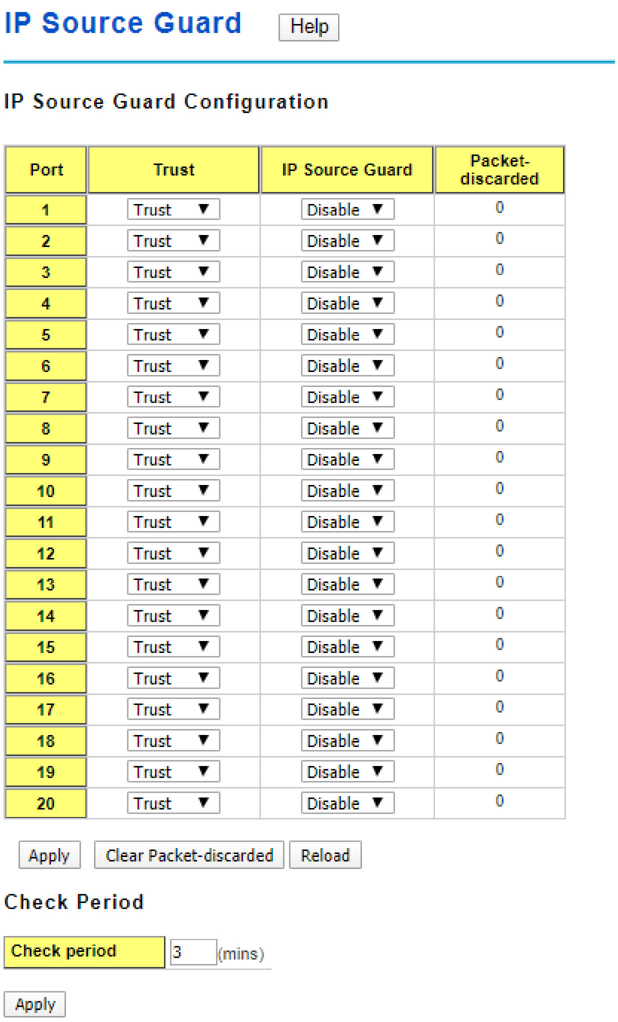
Click the **Select All** button to select all the entries.
Click the **Remove** button to remove the selected entries.
Click the **Reload** button to load the temporary entries.
Click the **Read** button to load the entries of DHCP binding database.
Click the **Clear** button to clear all entries and binding database.

DHCP Snooping Write Interval:

- **interval:** write current binding table to system. (secs.)
- Click the **Apply** button to apply change write interval.

4.11.6 IP Source Guard

IP Source Guard Configuration: It provides source IP address filtering on a Layer 2 port to prevent a malicious host from impersonating a legitimate host by assuming the legitimate host's IP address. IP Source Guard is an effective means of spoofing prevention at Layer 2



IP Source Guard Configuration

Port	Trust	IP Source Guard	Packet-discarded
1	Trust ▼	Disable ▼	0
2	Trust ▼	Disable ▼	0
3	Trust ▼	Disable ▼	0
4	Trust ▼	Disable ▼	0
5	Trust ▼	Disable ▼	0
6	Trust ▼	Disable ▼	0
7	Trust ▼	Disable ▼	0
8	Trust ▼	Disable ▼	0
9	Trust ▼	Disable ▼	0
10	Trust ▼	Disable ▼	0
11	Trust ▼	Disable ▼	0
12	Trust ▼	Disable ▼	0
13	Trust ▼	Disable ▼	0
14	Trust ▼	Disable ▼	0
15	Trust ▼	Disable ▼	0
16	Trust ▼	Disable ▼	0
17	Trust ▼	Disable ▼	0
18	Trust ▼	Disable ▼	0
19	Trust ▼	Disable ▼	0
20	Trust ▼	Disable ▼	0

Check Period

Check period	3 (mins)

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 a interface, incoming IP traffic on an interface are allowed when there is a matching entry in IP source binding database. Else, 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.

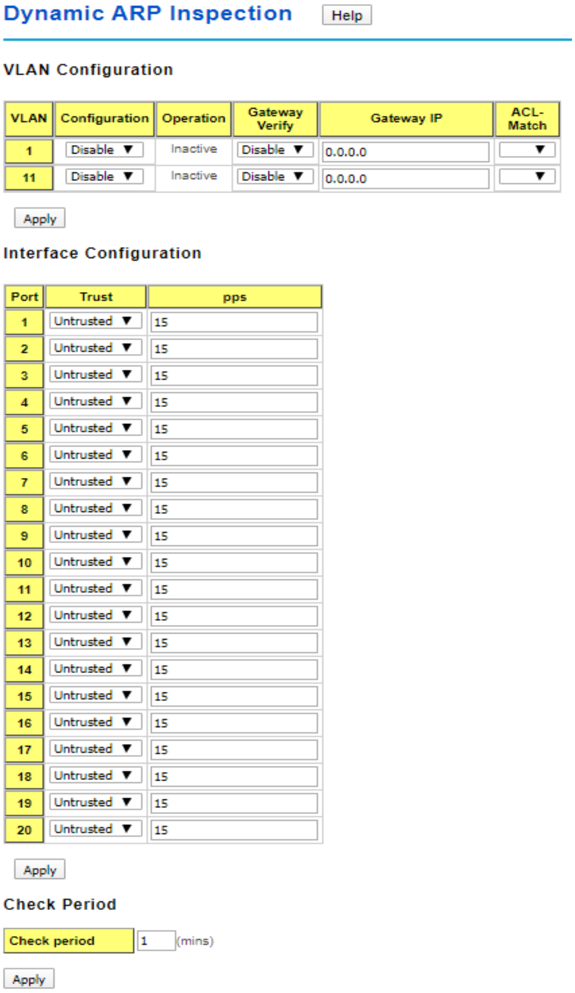
Check Period:

- **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.

4.11.7 Dynamic APR Inspection

You can configure DAI to drop ARP packets when the IP addresses in the packets are invalid or when the MAC addresses in the body of the ARP packets do not match the addresses specified in the Ethernet header
On this page, you can configure DAI for each VLAN and Port



Dynamic ARP Inspection

VLAN Configuration

VLAN	Configuration	Operation	Gateway Verify	Gateway IP	ACL-Match
1	Disable ▼	Inactive	Disable ▼	0.0.0.0	▼
11	Disable ▼	Inactive	Disable ▼	0.0.0.0	▼

Interface Configuration

Port	Trust	pps
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

Check Period

Check period	1 (mins)

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:

- **Trust:** Set Trust or un-trust for DAI for each port.
- **pps:** Packet per second.

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

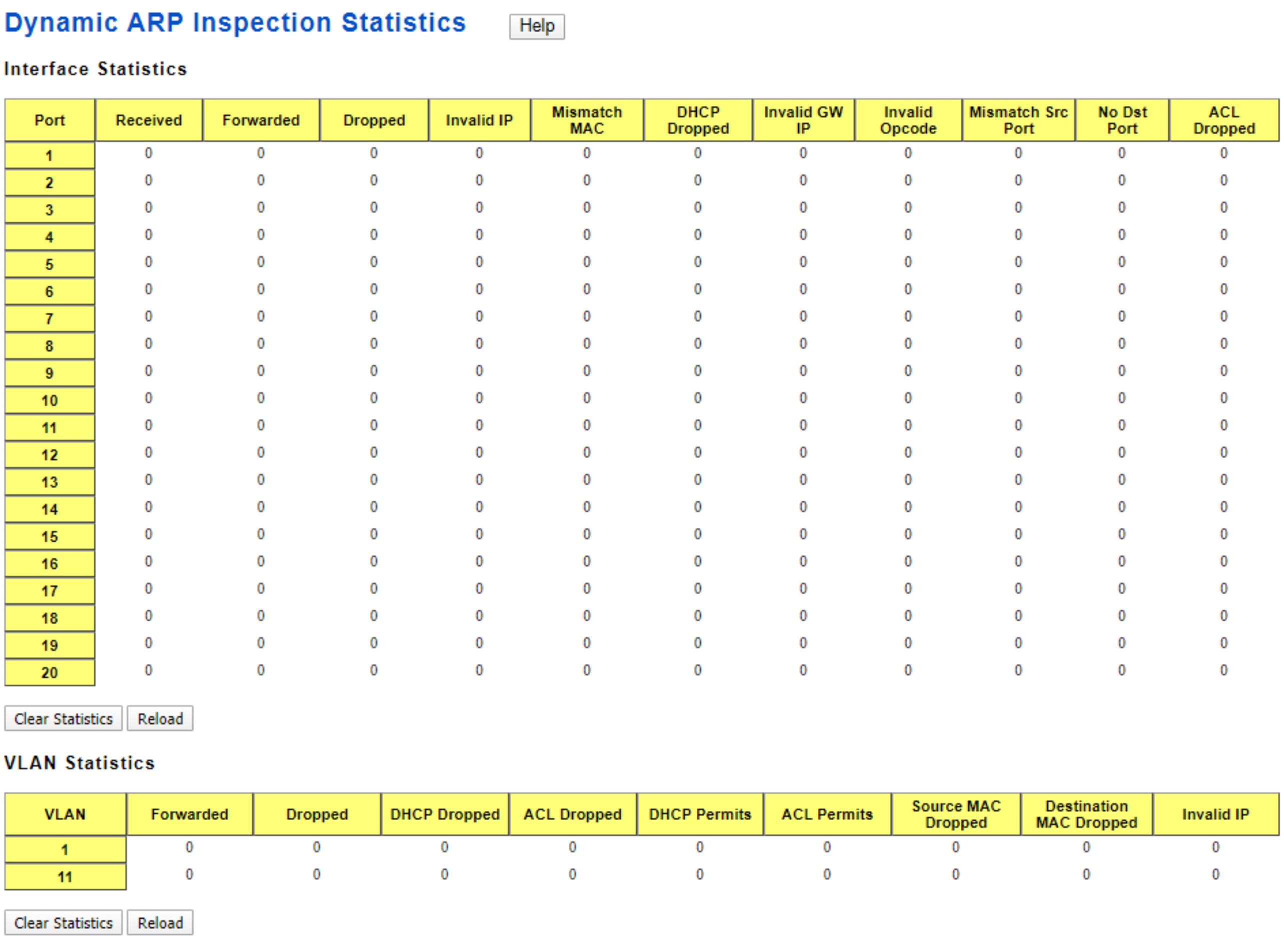
Check Period:

- **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.

4.11.8 Dynamic APR Inspection Statistic

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



Dynamic ARP Inspection Statistics

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

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
11	0	0	0	0	0	0	0	0	0

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:** 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 ehternet 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.

4.11.9 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 toforward 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 entrycomment

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 userna141orenixnix pass141orenixnix 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
DHCP Snooping	**DHCP Snooping**

Enable DHCP snooping - Global	Switch(config)# ip dhcp snooping
Disable DHCP snooping - Global	Switch(config)# ip dhcp snooping
Enable DHCP snooping – VLAN	Switch(config)# ip dhcp snooping vlan 1
Disable DHCP snooping – VLAN	Switch(config)# no ip dhcp snooping vlan 1
Setting DHCP snooping static entry	Switch(config)# ip dhcp snooping binding 0012.77ff.001a vlan 1 192.168.10.1 interface gi1 ***Note: rule: ip dhcp snooping binding MAC_address VLAN VID ip_address interface interface_name***
Remove DHCP snooping static entry	Switch(config)# no ip dhcp snooping binding 0012.77ff.001a vlan 1 192.168.10.1 interface gi1 ***Note: rule: no ip dhcp snooping binding MAC_address VLAN VID ip_address interface interface_name***
Setting DHCP snooping data base write period	Switch(config)# ip dhcp snooping database write-delay 60 <0-86400> seconds, zero means no auto-save, default=300
Enable DHCP snooping mac verify	Switch(config)# ip dhcp snooping verify mac-address
Disable DHCP snooping mac verify	Switch(config)# no ip dhcp snooping verify mac-address
Display – DHCP Snooping Setting	Switch# show ip dhcp snooping DHCP Snooping is disabled. MAC Address verification is disabled. Database write interval: 300 DHCP Snooping is configured on following VLAN(s): NONE Interface Trusted ----------------------- ------- gigabitethernet1 yes gigabitethernet2 yes gigabitethernet3 yes gigabitethernet4 yes gigabitethernet5 yes gigabitethernet6 yes gigabitethernet7 yes gigabitethernet8 yes gigabitethernet9 yes gigabitethernet10 yes gigabitethernet11 yes gigabitethernet12 yes [DHCP Snooping Statistics] Total received: 0 Dropped (MAC verification failed): 0 Dropped (Interface invalid): 0 Dropped (Binding not matched): 0

	Dropped (Relay Agent address error): 0 Total dropped: 0
Display – DHCP Snooping Table	Switch# show ip dhcp snooping binding Mac Address IP Address Lease Time VLAN Interface Type ----------------- --------------- ---------- ---- ------------------ ----- --
Display – DHCP snooping database write period	Switch# show ip dhcp snooping database write-delay DHCP Snooping database write interval:300
IP Source Guard	**IP Source Guard**
Setting IP source guard binding	Switch(config)# ip source binding 0012.77ff.0013 vlan 1 192.168.10.2 interface gi1 ***Note: rule: ip*** **source binding** ***MAC_address VLAN VID IP_address interface interface_name***
Remove IP source guard binding	Switch(config)# no ip dhcp snooping binding 0012.77ff.001a vlan 1 192.168.10.1 interface gi1 ***Note: rule: no ip dhcp snooping binding MAC_address VLAN VID ip_address interface interface_name***
Setting ip source fuard checking period	Switch(config)# ip verify source checking period 1 Set IPSG statistics checking period to 1 min(s)
Setting ip source guard security mode	Switch(config)# int gi1 **(Go to interface mode)** Switch(config-if)# ip verify source port-security ip ip IP or IP-MAC ip-mac IPSG cannot be enabled on a trusted port
Remove ip source guard security mode	Switch(config)# int gi1 **(Go to interface mode)** Switch(config-if)# no ip verify source port-security
Setting IP source guard trust mode	Switch(config)# int gi1 **(Go to interface mode)** Switch(config-if)# ip dhcp snooping trust trust Trust interface
Remove IP source guard trust mode	Switch(config)# int gi1 **(Go to interface mode)** Switch(config-if)# no ip dhcp snooping trust trust Trust interface
Display ip source guard discard count	Switch# show ip verify source interface gigabitethernet1 Disable 0 packets discarded gigabitethernet2 Disable 0 packets discarded gigabitethernet3 Disable 0 packets discarded gigabitethernet4 Disable 0 packets discarded gigabitethernet5 Disable 0 packets discarded gigabitethernet6 Disable 0 packets discarded gigabitethernet7 Disable 0 packets discarded gigabitethernet8 Disable 0 packets discarded gigabitethernet9 Disable 0 packets discarded gigabitethernet10 Disable 0 packets discarded gigabitethernet11 Disable 0 packets discarded gigabitethernet12 Disable 0 packets discarded
Display ip source guard checking period	Switch# show ip verify source checking period IPSG statistics checking period 3 min(s)
Dynamic ARP inspection	**Dynamic ARP inspection**
Enable Dymamic ARP inspection - VLAN	Switch(config)# ip arp inspection vlan 1 Enable DAI on vlan 1
Disable Dymamic ARP inspection - VLAN	Switch(config)# no ip arp inspection vlan 1 Disable DAI on vlan 1
Bind Dymamic ARP	Switch(config)# ip arp inspection filter rule1 vlan 1

inspection to acl rule	***Note: rule: ip arp inspection filter ACL_rule VLAN VID***
Remove Dymamic ARP inspection to acl rule	Switch(config)# no ip arp inspection filter vlan 1 ***Note: rule: ip arp inspection filter VLAN VID***
Enable Dymamic ARP inspection gate-way verify	Switch(config)# ip arp inspection gw-ip verify vlan 1 Enable DAI Gateway IP verification on vlan 1 ***Note: rule: ip arp inspection*** **gw-ip verify** ***VLAN VID***
Disable Dymamic ARP inspection gate-way verify	Switch(config)# no ip arp inspection gw-ip verify vlan 1 Disable DAI Gateway IP verification on vlan 1 ***Note: rule: no ip arp inspection*** **gw-ip verify** ***VLAN VID***
Setting gate way ip address	Switch(config)# ip arp inspection gw-ip 192.168.10.3 vlan 1 Set DAI Gateway IP on vlan 1 ***Note: rule: ip arp inspection*** **gw-ip IP_ADDRESS** ***VLAN VID***
Setting trust mode on interface	Switch(config)# int gi1 **(go to interface mode)** Switch(config-if)# ip arp inspection trust Trust this interface
Setting untrust mode on interface	Switch(config)# int gi1 **(go to interface mode)** Switch(config-if)# no ip arp inspection trust untrust this interface
Setting dynamic ARP no limit on interface	Switch(config)# int gi1 **(go to interface mode)** Switch(config-if)# ip arp inspection limit none Unlimited rate Rate (packet per second)
Setting dynamic ARP limit on interface	Switch(config)# int gi1 **(go to interface mode)** Switch(config-if)# ip arp inspection limit rate 65 <0-65> Valid range is from 0 to 65pps, default is 15pps
Disable dynamic ARP limit on interface	Switch(config)# int gi1 **(go to interface mode)** Switch(config-if)# no ip arp inspection limit
Display dynamic ARP inspection status - VLAN	Switch# show ip arp inspection vlan 1 Vlan Configuration Operation GW IP VER GW IP ACL Match ----- -------------- ---------- --------- -------------- ---------------- 1 Disabled Inactive Disabled 0.0.0.0
Display dynamic ARP inspection status - interface	Switch# show ip arp inspection interface gi1 Interface Trust State Rate (pps) --------- ----------- ---------- gi1 Untrusted 15
Display dynamic ARP inspection statistic - VLAN	Switch# show ip arp inspection statistics vlan 1 Vlan Forwarded Dropped DHCP Drops ACL Drops DHCP Permits ACL Permits ----- ---------- -------- ----------- ---------- ------------- ----------- - 1 0 0 0 0 0 0 Source MAC Failures Dest MAC Failures IP Validation Failures ------------------- ------------------ -----
Display dynamic ARP inspection statistic - interface	Switch# show ip arp inspection statistics interface gi1 Interface Received Forwarded Dropped Invalid IP Mismatch MAC DHCP Drop

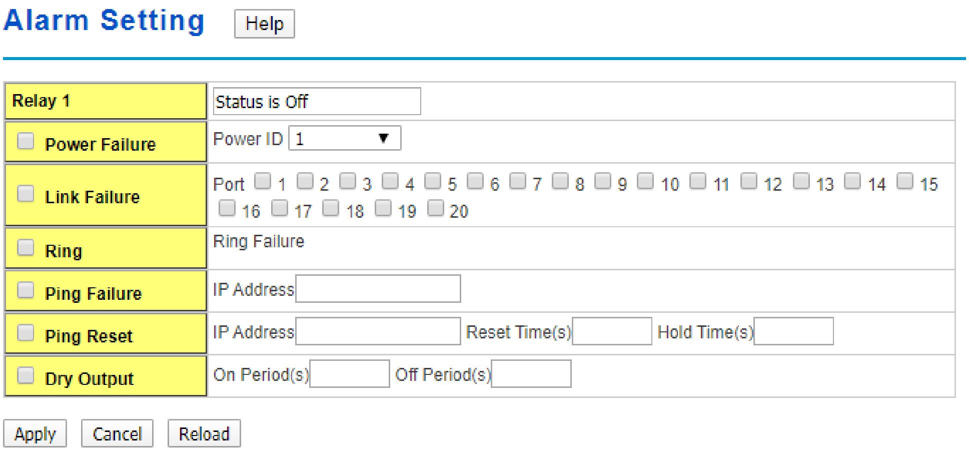
	--------- -------- --------- ------- ---------- ------------ --------- gi1 201 0 201 0 0 201 Invalid GW IP Invalid Opcode Mismatch Src Port No Dst Port ACL Drop ------------- -------------- ----------------- ----------- -------- 0 0 0 0 0

4.12 Warning

JetNet 7500 series 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.

4.12.1 Alarm Setting

The JetNe 7500 series 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 Setting

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

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 any power 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

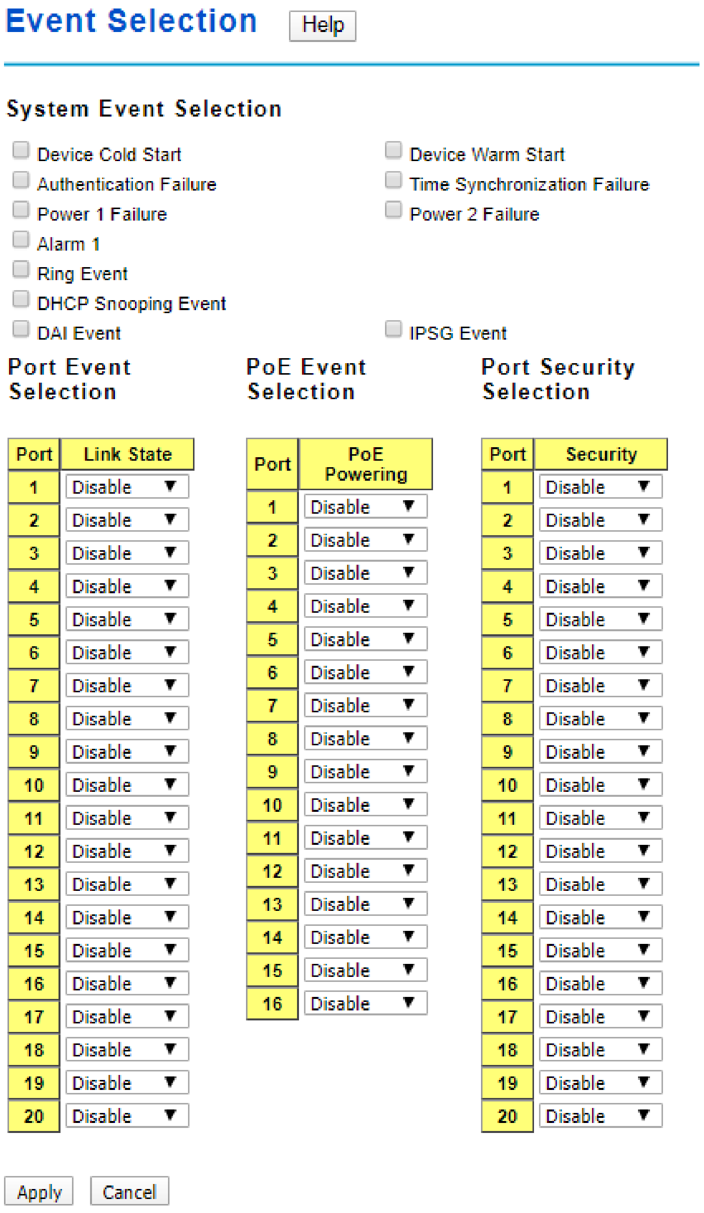
Cancel to clear the modification. Click

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.

4.12.2 Event Selection

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



Event Selection

System Event Selection

□ Device Cold Start
□ Authentication Failure
□ Power 1 Failure
□ Alarm 1
□ Ring Event
□ DHCP Snooping Event
□ DAI Event

□ Device Warm Start
□ Time Synchronization Failure
□ Power 2 Failure
□ IPSG Event

Port Event Selection

Port	Link State
1	Disable
2	Disable
3	Disable
4	Disable
5	Disable
6	Disable
7	Disable
8	Disable
9	Disable
10	Disable
11	Disable
12	Disable
13	Disable
14	Disable
15	Disable
16	Disable
17	Disable
18	Disable
19	Disable
20	Disable

PoE Event Selection

Port	PoE Powering
1	Disable
2	Disable
3	Disable
4	Disable
5	Disable
6	Disable
7	Disable
8	Disable
9	Disable
10	Disable
11	Disable
12	Disable
13	Disable
14	Disable
15	Disable
16	Disable

Port Security Selection

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

System Event Selection

Select events for which you want notifications to be generated.

- **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 Synchronization 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 1 Failure:** When selected, the switch generates a notification if a power failure occurs on power input 1.
- **Power 2 Failure:** When selected, the switch generates a notification if a power failure occurs on power input 2.
- **Fault Relay 1:** When selected, the switch generates a notification if the fault relay changes state.
- **DI 1 Change:** When selected, the switch generates a notification if the state changes on digital input 1.
- **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.
- **SFP Event:** 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.
- **DHCP Snooping Event:** When selected, the switch generates a notification if the state of an DHCP Snooping changes.
- **DAI Event:** When selected, the switch generates a notification if the state of an DAI statistics changes.
- **IPSG Event:** When selected, the switch generates a notification if the state of an IPSG statistics changes.

Port Event Selection

- **Port:** The port you want to generate notifications for.
- **Link State:** When set to **Disabled** no notifications will be generated for the selected port. When set to **Up** a notification will be generated when the port connection goes from down to up. When set to **Down** a notification is generated when the port connection goes from up to down. When set to **Both** a notification is generated if the port connection goes up or down.

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

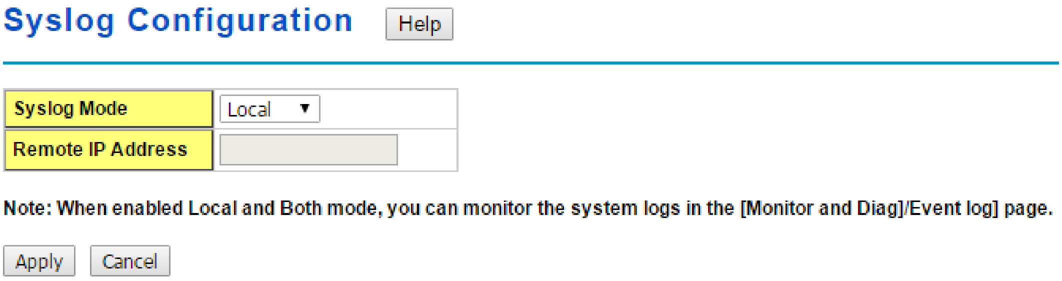
PoE Event Selection

- **Port:** The number of ports.
- **PoE Powering:** Select **Disable** or **Enable** to generate a PoE Powering event, when this event occurs, the switch sends notification.

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

4.12.3 SysLog Configuration

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



Syslog Configuration

Syslog Mode	Local ▼
Remote IP Address	

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

Syslog Mode: There are two System Log modes provided by JetNet 7500 series Switch, local mode and remote mode.

Local Mode - In this mode, JetNet 7500 series Switch will print the occurred events selected in the

Event Selection page to System Log table of JetNet 7500 series 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 7500 series switch. In this mode, you should assign the IP address of the System Log server. JetNet 7500 series 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

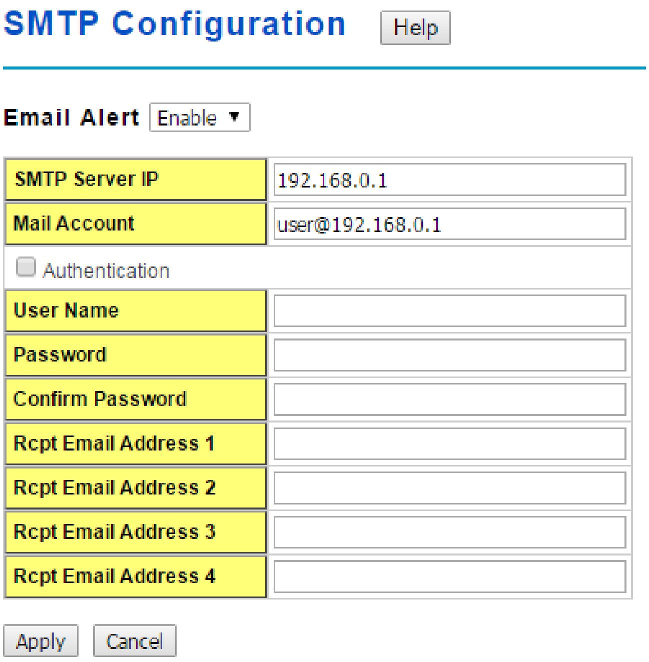
Cancel to clear the modification.

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.

4.12.4 SMTP Configuration

JetNet 7500 series 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.



SMTP Configuration

Email Alert Enable ▾

SMTP Server IP	192.168.0.1
Mail Account	user@192.168.0.1
□ Authentication	
User Name	
Password	
Confirm Password	
Rcpt Email Address 1	
Rcpt Email Address 2	
Rcpt Email Address 3	
Rcpt Email Address 4	

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 7500 series switch.

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.

4.12.5 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,gi17-20 Switch(config)# relay 1 port fa1-5
Ring Failure	Switch(config)# relay 1 ring
Disable Relay	Switch(config)# no relay 1 relay id Switch(config)# no relay 1
Display	Switch# show relay 1 Relay 1 Event :

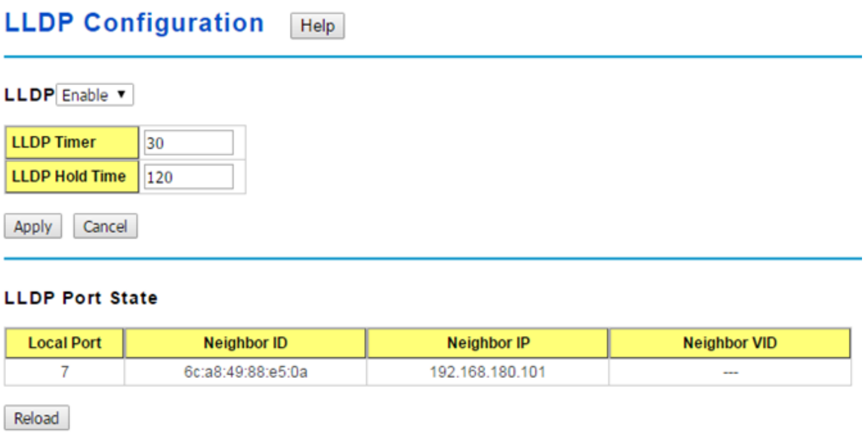
	Power : Disabled Port Link : Disabled Ring : Disabled Ping : Disabled Ping Reset : Disabled Dry Output : Disabled DI : Disabled
Event Selection	
Event Selection	Switch(config)# warning-event coldstart Switch cold start event warmstart Switch warm start event authentication Authentication failure event linkdown Switch link down event linkup Switch link up event 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:

4.13 Monitor and Diag

JetNet 7500 series 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.

4.13.1 LLDP Configuration



LLDP Configuration

LLDP: Enable

LLDP Timer	30
LLDP Hold Time	120

LLDP Port State

Local Port	Neighbor ID	Neighbor IP	Neighbor VID
7	6c:a8:49:88:e5:0a	192.168.180.101	---

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.

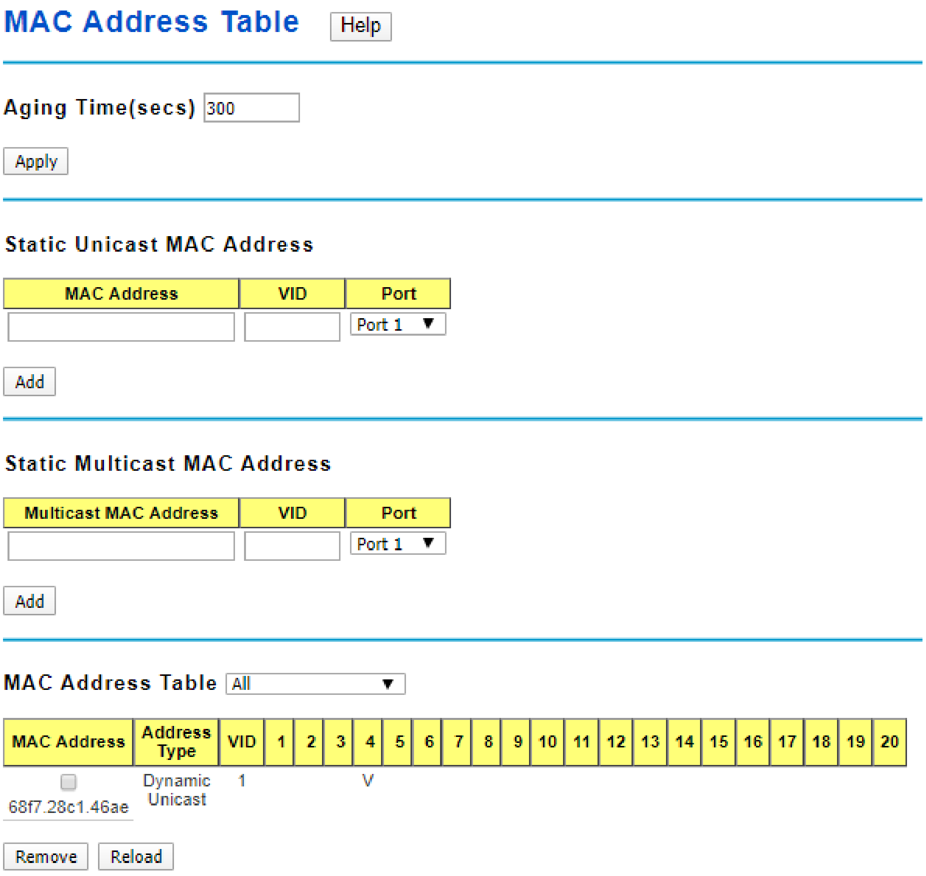
<u>LLDP Port State</u>

Local port: the current port number that linked with neighbor network device. **Neighbor ID**: the MAC address of neighbor device on the same network segment. **Neighbor IP**: the IP address of neighbor device on the same network segment.

Neighbor VID: the VLAN ID of neighbor device on the same network segment. Click **Reload** to reload the LLDP Port State Table.

4.13.2 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

Aging Time(secs) 300

Static Unicast MAC Address

MAC Address	VID	Port
		Port 1 ▼

Static Multicast MAC Address

Multicast MAC Address	VID	Port
		Port 1 ▼

MAC Address Table All ▼

MAC Address	Address Type	VID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
□ 68f7.28c1.46ae	Dynamic Unicast	1				V																

Aging Timer

The aging timer determines how long an automatically learned MAC address is stored in the forwarding information base (FIB). Every time a MAC address is used as a source address the aging timer is reset. If the aging timer expires the MAC address is removed from the FIB.

- **Aging Time:** The number of seconds an automatically learned MAC address will be stored in the FIB without being used as a source address. Valid values are multiples of 15 between 15 and 3825. The default value is 300.

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

Static Unicast MAC Address

This section allows you to manually add unicast MAC addresses to the FIB. Manually entered addresses do not expire like automatically learned addresses do. You can manually add up to 10 unicast MAC addresses per port.

- **MAC Address:** The unicast MAC address you want to manually enter into the FIB.
- **VID:** The VLAN you want to add the MAC address to.
- **Port:** The port you want the MAC address to be associated with.

Click the **Add** button to add the static unicast MAC address to the FIB.

MAC Address Table

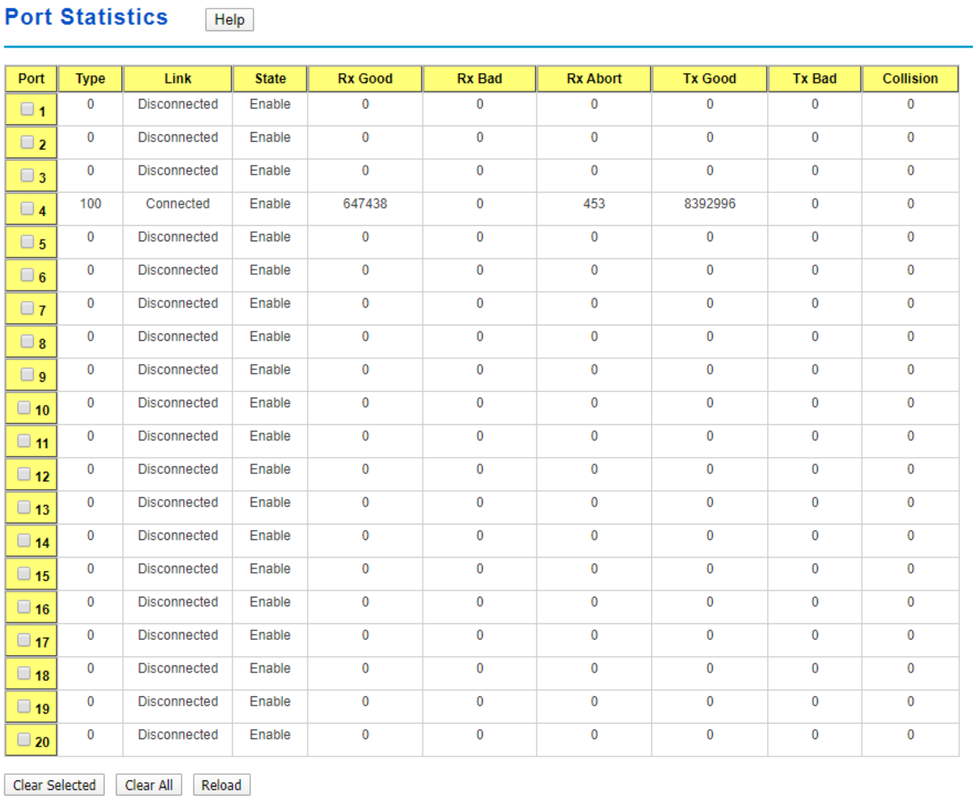
The MAC Address Table displays automatically all learned and manually entered MAC addresses stored in the FIB. You can filter the MAC addresses being displayed and remove MAC addresses from the FIB.

- **MAC Address Table:** You can filter what types of MAC addresses are displayed in the MAC Address Table. The following MAC address types are available:
    - **All:** All MAC addresses stored in the FIB.
    - **Dynamic Unicast:** Automatically learned unicast MAC addresses.
    - **Static Unicast:** Manually entered unicast MAC addresses.
    - **Dynamic Multicast:** Multicast MAC addresses that have been automatically learned using IGMP snooping.
    - **Static Multicast:** Manually entered multicast MAC addresses.
    - **Port #:** All MAC addresses associated with port # (where # is the port number).
- **MAC Address:** The MAC address of the FIB entry.
- **Address Type:** The type of address of the FIB entry. Addresses can be Dynamic Unicast, Static Unicast, Dynamic Multicast, and Static Multicast.
- **VID:** The VLAN the MAC address was learned on or manually added to.
- **#:** The port number (where # is the port number) the MAC address was learned on or manually added to.

To remove an entry check the checkbox of the MAC address you want to remove and click the **Remove** button or click the **Reload** button to reload the MAC Addresses table.

4.13.3 Port Statistics

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



Port	Type	Link	State	Rx Good	Rx Bad	Rx Abort	Tx Good	Tx Bad	Collision
☐ 1	0	Disconnected	Enable	0	0	0	0	0	0
☐ 2	0	Disconnected	Enable	0	0	0	0	0	0
☐ 3	0	Disconnected	Enable	0	0	0	0	0	0
☐ 4	100	Connected	Enable	647438	0	453	8392996	0	0
☐ 5	0	Disconnected	Enable	0	0	0	0	0	0
☐ 6	0	Disconnected	Enable	0	0	0	0	0	0
☐ 7	0	Disconnected	Enable	0	0	0	0	0	0
☐ 8	0	Disconnected	Enable	0	0	0	0	0	0
☐ 9	0	Disconnected	Enable	0	0	0	0	0	0
☐ 10	0	Disconnected	Enable	0	0	0	0	0	0
☐ 11	0	Disconnected	Enable	0	0	0	0	0	0
☐ 12	0	Disconnected	Enable	0	0	0	0	0	0
☐ 13	0	Disconnected	Enable	0	0	0	0	0	0
☐ 14	0	Disconnected	Enable	0	0	0	0	0	0
☐ 15	0	Disconnected	Enable	0	0	0	0	0	0
☐ 16	0	Disconnected	Enable	0	0	0	0	0	0
☐ 17	0	Disconnected	Enable	0	0	0	0	0	0
☐ 18	0	Disconnected	Enable	0	0	0	0	0	0
☐ 19	0	Disconnected	Enable	0	0	0	0	0	0
☐ 20	0	Disconnected	Enable	0	0	0	0	0	0

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

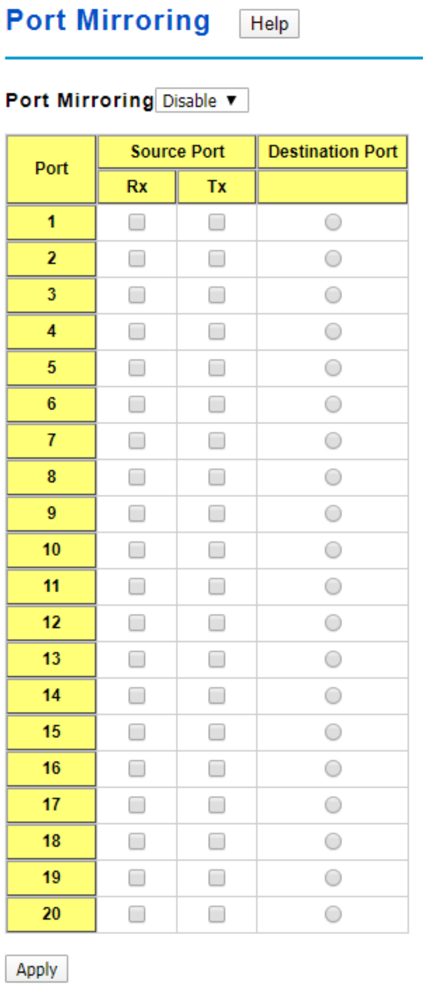
Clear All to clean all counts.

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.

4.13.4 Port Mirroring

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



Port Mirroring Disable ▼

Port	Source Port		Destination Port
	Rx	Tx	
1	□	□	○
2	□	□	○
3	□	□	○
4	□	□	○
5	□	□	○
6	□	□	○
7	□	□	○
8	□	□	○
9	□	□	○
10	□	□	○
11	□	□	○
12	□	□	○
13	□	□	○
14	□	□	○
15	□	□	○
16	□	□	○
17	□	□	○
18	□	□	○
19	□	□	○
20	□	□	○

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

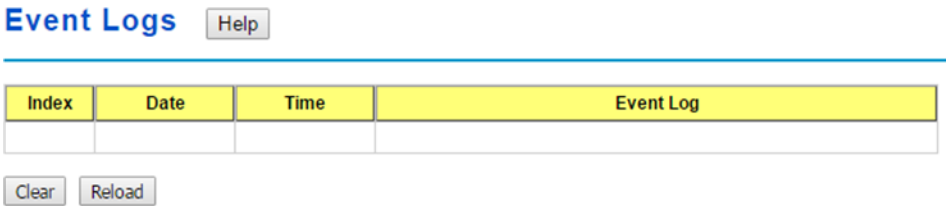
Source Port: This is also known as Monitor Port. These are the ports you want to monitor. The traffic of all source/monitor ports will be copied to destination/analysis ports. You can choose a single port, or any combination of ports, but you can only monitor them in Rx or TX only.

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 next device to this port.

Click **Apply** to apply the settings.

4.13.5 Event Logs

The System Log feature was introduced in 4.12.3 SysLog Configuration . When System Log Local mode is selected, JetNet 7500 series 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	Date	Time	Event Log

Index: The index of the log entry.

Date: The date the log was generated on.

Time: The time the log was generated at.

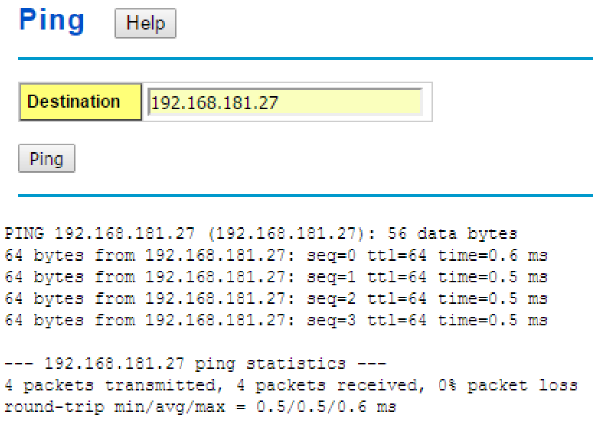
Event Log: The log entry.

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

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

4.13.6 Ping

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



Destination: 192.168.181.27

```
PING 192.168.181.27 (192.168.181.27): 56 data bytes
64 bytes from 192.168.181.27: seq=0 ttl=64 time=0.6 ms
64 bytes from 192.168.181.27: seq=1 ttl=64 time=0.5 ms
64 bytes from 192.168.181.27: seq=2 ttl=64 time=0.5 ms
64 bytes from 192.168.181.27: seq=3 ttl=64 time=0.5 ms

--- 192.168.181.27 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.5/0.5/0.6 ms
```

Destination: Enter the target IP address of the device that wants to ping. Click **Ping** to display the results.

4.13.7 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)

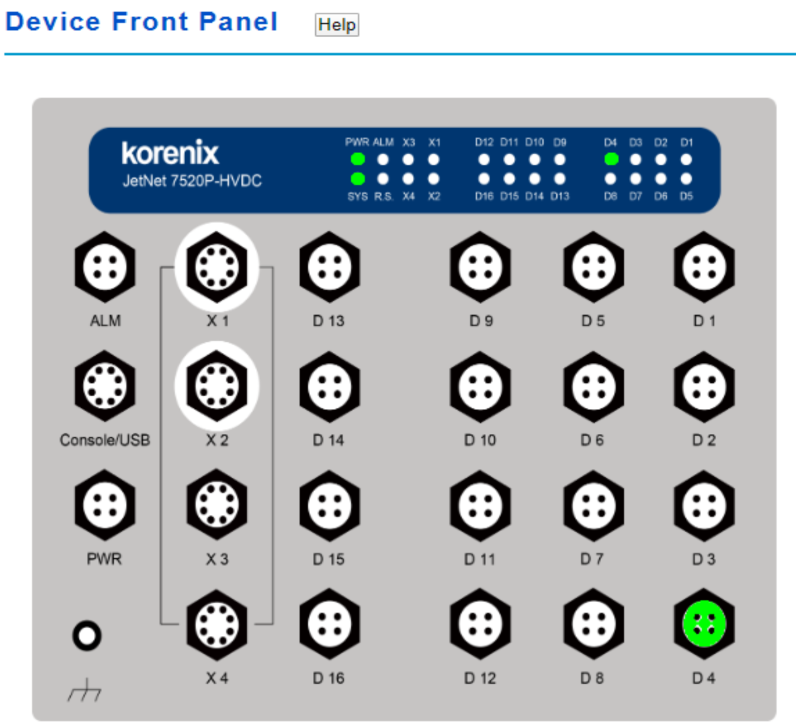
	Interface gigabitethernet4 is enable connected, which has Inbound: Good Octets: 178792, Bad Octets: 0 Unicast: 598, Broadcast: 1764, Multicast: 160 Pause: 0, Undersize: 0, Fragments: 0 Oversize: 0, Jabbers: 0, Disacrds: 0 Filtered: 0, RxError: 0, FCSError: 0 Outbound: Good Octets: 330500 Unicast: 602, 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

4.14 Device Front Panel

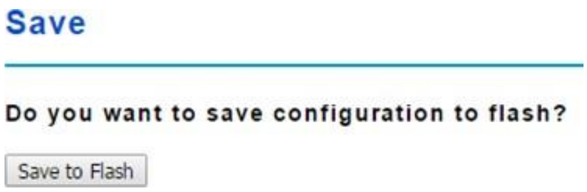
The Device Front Panel allows you to see the LED status of the switch For Example, JetNet 7520P-HVDC front panel status is shown as below



Click on **Reload** to reload the status.
Note: No CLI command for this feature

4.15 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.



Save

Do you want to save configuration to flash?

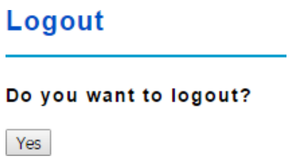
Click **Save to Flash** to save your new configuration.

Command Lines:

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

4.16 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.



Logout

Do you want to logout?

Click **Yes** to logout

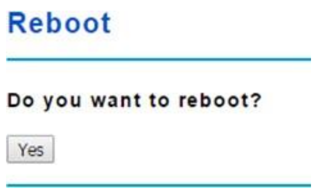
Command Lines:

Feature	Command Line
Logout	SWITCH> exit SWITCH# exit

4.17 Reboot

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

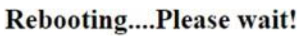
Note: Before rebooting, remember to go to **Save** page to save your settings. Otherwise, the settings will be lost when the switch is powered off.



Reboot

Do you want to reboot?

Click **Yes** to reboot the device.



Rebooting....Please wait!

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

5. Appendix

5.1 Product Specification

Technology	
Standard	IEEE 802.3 10 Base-T Ethernet IEEE 802.3u 100 Base-TX Fast Ethernet IEEE 802.3ab 1000 Base-T IEEE 802.3af Power over Ethernet IEEE 802.3at High Power PoE with 2-Event classification IEEE 802.3x Flow Control and Back-pressure IEEE 802.1AB Link Layer Discovery Protocol (LLDP) IEEE 802.1p Class of Service (CoS) IEEE 802.1Q VLAN and GVRP IEEE 802.1D-2004 Rapid Spanning Tree Protocol (RSTP) IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) IEEE 802.3ad Link Aggregation Protocol (LACP) IEEE 802.1x Port Based Network Access Protocol
Performance	
Switch Technology	Store and Forward technology with 11.2Gbps switching fabric (JetNet 7520P-HVDC)
CPU performance	ARM A9 1GHz with Hardware based Watch-dog timer with 10s reset down-counter
System Memory	32M bytes flash ROM, 256M bytes system RAM
Transfer packet size	64 bytes to 9K (9216) bytes Jumbo Frame
MAC Address	16K
Packet Buffer	1.5M Bytes shared memory for packet buffer with intelligent memory management unit for burst data traffic
Transfer performance	14,880 pps @10Mbps 148,800 pps @100Mbps 1,488,100 pps @1000Mbps
Management	
Management Interface	Telnet with SSH, Web Browser with SSL, SNMP V1/V2c/V3 with SNMP Trap (up to 4 trap stations), RMON (Group 1,2,3,9) for in-band management. Local RS-232 M12 connector for out-band management. Additional USB host interface for configuration Backup and Restore.
Management Security	The maximum management session up to four, and support management Host IP secure feature to prevent unauthorized remote login
SNMP MIB	MIB-II, Bridge MIB, Ethernet-like-MIB, VLAN MIB, IGMP MIB, Private MIB
NMS	Windows based NMS System –Korenix NMS and Korenix View for device discovery and network topology auto construct
Network Time Protocol	NTP with daylight saving and localize time sync function
Management IP Security	Predefined Host IP address for management host login security
E-mail Warning	4 Receipt E-mail accounts with E-mail server authentication
System Event Log	2 event log modes, Local and remote Log Server with authentication
System Auto Maintenance	System Power-On with configuration update, firmware auto upgrade when USB/M12 Flash installed
Network Performance	
Port Configuration	Port link Speed, Link mode, current status and enable/disable

Port Trunk	IEEE 802.3ad Link Aggregation Control Protocol (LACP) and Static port trunk; trunk member up to 8 ports in one group, maximum 128 trunk groups
VLAN	IEEE 802.1Q Tag VLAN with 4K VLAN Entries and provides 2K GVRP entries; 3 VLAN link modes- Trunk mode, Hybrid mode and Link access mode
Private VLAN	The Private VLAN is special for group uplink access with independent port security. With the private VLAN function, each VLAN community is isolated and only exchange by high level device with primary VLAN community
IEEE 802.1Q QinQ	Supports Double VLAN tag for VLAN isolation and security
IEEE 802.1p	The Ethernet Switch MAC controller supports IEEE 802.1p Class of Service function; Per interface with 4 queues
IP Multicasting	Supports IGMP Snooping v1/v2c /v3 for multicast filtering and IGMP Query mode; also support unknown multicasting process forwarding policies- drop, flooding and forward to router port, 1K Multicasting Groups
Rate Control	Ingress/Egress filtering for broadcast, multicast, unknown DA or all packets
Port Mirroring	On-line traffic monitoring on multiple selected ports
DHCP	DHCP Server DHCP Client DHCP Relay Agent
IEEE 802.1x/ Port Security	Port based network access control, and authenticated by localize pre-defined MAC address or remote RADIUS Server
Power over Ethernet	IEEE 802.3af/at, End-Span wiring architecture
PoE operating mode	Auto Mode: IEEE 802.3af/at behaviors with IEEE 802.3at 2-Event Classification for high power IEEE 82.3at PD device Forced Mode: User configured Power consumption budget control with IEEE 802.3 PoE /PD detection, or forced without PD detection
PoE forwarding conductor	M12 D-Code (Port 1~8): V+(1,3), V- (2,4)
Power forwarding capability	IEEE 802.3af:15W, IEEE802.3at:30W
PoE System Power Budget	Power Budget Reserve by PD declaration. The power budget control system will reserve power for connected PD device, once latest PD device (D16) claimed power over the system surplus power, then the latest PoE will not be active. System Power over Ethernet Power Budget: 120Watts (Max.)/ 75°C
Network Redundancy	
Multiple Super Ring (MSRTM)	New generation Korenix Ring Redundancy Technology, Includes Rapid Super Ring, Rapid Dual Homing, TrunkRingTM, MultiRingTM , Super ChainTM and backward compatible with legacy Super RingTM
Rapid Dual Homing (RDHTM)	Multiple uplink paths to one or multiple upper Switch, up to 256 Groups RDH Peer protection
TrunkRingTM	Integrate port aggregate function in ring path to get higher throughput ring architecture
MultiRingTM	Supports redundant ring up to 10 rings in one device includes 8 Fast Ethernet rings and 2 Gigabit Ethernet rings
Super Chain	It is new ring technology with flexible and scalability, compatibility, and easy configurable. The ring includes 2 types of node Switch – Border Switch and Member Switch
Rapid Spanning Tree	IEEE 802.1D-2004 Rapid Spanning Tree Protocol; it compatible with Legacy Spanning Tree and IEEE 802.1w

Multiple Spanning Tree	IEEE 802.1s Multiple Spanning Tree, each MSTP instance can include one or more VLANs, and also supports multiple RSTP deployed in a VLAN or multiple VLANs
ITU-T G.8032 ERPS	Support ITU-T G.8032 ERPS V1 single ring topology, and ERPS v2 multiple rings with ladder topology
System Fault Bypass	Link Partner Bypass function on Gigabit port X1, X2. Both of Gigabit ports will form as inter-connected mode when switch power shut-down or unstable /non-ready
Routing Protocols	**JetNet 7500 series only)**
IP Routing	Supports Default Static and Dynamic Route
Virtual LAN Routing	Incorporate both of IEEE802.1Q Bridge and Routing Function
Routing Information Protocol	Hop-Based IP Routing with RIPv1 and RIPv2; 1K /512 for IPv4/IPv6 routing
HW IP Routing Table	512 Routing entries (JetNet 7500 series)
IGMP	Multicast Group Management Protocol support IGMP v1,v2, v3
Multicast Routing	256 IP Multicast Routing entries
DVMRP	HOP-Based multicast routing protocol, short of distance vector multicast routing protocol
PIM-DM	Multicasting Routing Protocol, Short of Protocol Independent Multicast-Dense mode
VRRP	Short of Virtual Route Redundancy Protocol, Automatically Backup Routing route to specified router
OSPF	Link State based IP routing protocol support OSPFv1/V2/V3
IEC-61375-2-5 TTDP*	Support Train Topology Discovery Protocol to automatically reconfigure for topology changes
Security	
Cyber Security	The Cyber Security function includes- DHCP Snooping protection, Dynamic ARP inspect protection, IP Source Guard (IPSG), Distribute Denial-of-Service (DDoS), IEEE 802.1x MAB for non-IEEE 802.1x compliant device.
ACL	Up to 2K FP rules with 8 slices allowing 8 parallel lookup and match
TACACS+	Support
Interface	
Enclosure port	100Mbps Fast Ethernet port (D1~D16): up to 16 x M12 D-Code Female connectors with 16 ports IEEE 802.3at PoE/PSE (D1~D16) M12 D-Code (Conductor #): (#1) TX+/PoE V+, (#2) RX+/ PoE V-, (#3) TX-/PoE V+, (#4) RX-/ PoE V- 1000Mbps Gigabit Ethernet port (X1~X4): 4 x M12 X-Code Female Connectors M12 X-Code (Conductor #): (#1) 0P(D1+)/PoE V+, (#2) 0N(D1-)/PoE V+, (#3)1P(D2+)/PoE V-, (#4)1N(D2-)/PoE V-, (#5)3P(D4+) (#6)3N(D4-), (#7) 2N (D3-), (#8) 2P (D3+) Serial Console/USB: M12 A-Code 8-pins for console and USB Flash Disk Relay : M12 A-Code 4-pins Power input port: M12-A 4-pin Male
Cables	100Base-TX: 2 pairs STP Cat.5e/Cat.6 cable, EIA/TIA-568B 100-ohm (length:100Meters) 1000Base-T: 4 pairs STP Cat. 5e/Cat.6 cable, EIA/TIA-568B 100-ohm (length:100Meters)

	Power Interface: 4 pins, 18 AWG, Strand Electric power cable
Diagnostic Indicator	100Mbps port: Link/Activity (Green on, Green Blinking), PoE Power on (Amber on)/ Port D1-D16 1000Mbps port: Link/Activity (Green on, Green Blinking) Power: Power on (Green on) Sys: Ready (Green on) R.S: Green on (Ring Normal)/Blinking (wrong ring port connective), Amber on (Ring abnormal)/Blinking (ring port failed)
Power Requirements	
System Power	HVDC: DC 110V, Variation voltage from 77 VDC to 137.5 VDC LVDC : DC 24 V, Variation voltage from 10 VDC to 57 VDC
Power Consumption	23Watts (maximum) without PoE loading, 77 VDC - 137.5VDC 143Watts (maximum) with 120W PoE loading , 77 VDC-137.5VDC 123Watts (maximum) with 100W PoE loading , 10 VDC-57VDC
Mechanical	
Installation	Wall Mounting/ DinRail Mounting
Dimensions	162.2 mm(H) x 206 mm (W) x 70 mm (D)
Weight	2.522 kg
Material Housing	Steel Metal with Aluminum Heat Sink
Ingress Protection	IP41 protection, IP54 is optional
Environmental	
Operating temperature	-40~75°C: 120Watts with PoE Loading
Operating humidity	0%~90%, non-condensing
Storage Temperature	40~85°C
Hi-Pot	AC 1.2KV for ports-power, power-case
Approvals	
Railway Standard	EN50155:2017, EN 50121-4, EN50121-3-2
EMC	EMI: EN50121-3-2, FCC Class A, IEC/EN61000-6-4 EMS:EN50121-3-2/EN50121-1, IEC/EN61000-6-2 IEC/EN61000-4-2, IEC/EN61000-4-3, IEC/EN61000-4-4, IEC/EN61000-4-5, IEC/EN61000-4-6, IEC/EN61000-4-8, IEC/EN61000-4-9
Variation/Shock	Compliance with IEC 61373
Fire protection	Compliance with EN45545-2
Bus Standard	Compliance with E-Mark 13 (LVDC only) *
Free Fall	Compliance with IEC 60068-2-32
MTBF (hrs)	426,523
Warranty	5 Years

5.2 Korenix Private MIB

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

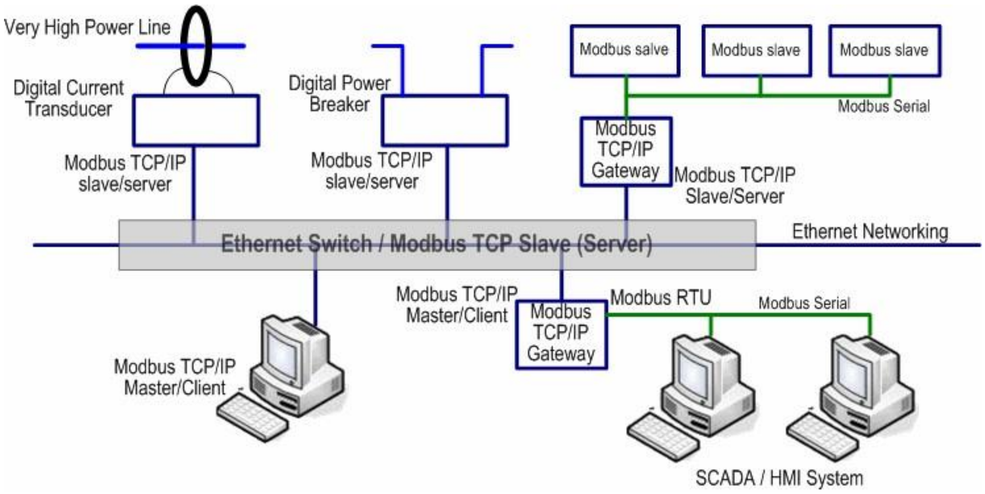
Private MIB tree is similar to the web tree. This is easier to understand and use. If you are not familiar with standard MIB, you can directly use private MIB to manage /monitor the switch, no need to learn or find where the OIDs of the commands are.

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

5.3 ModBus TCP /IP

The Modbus TCP/IP is very similar to Modbus RTU, but it transmits data within TCP/IP Data packets. It was developed in 1979 for industrial automatic communication system and have becomes a standard protocol for industrial communication for the transfer discrete analog I/O devices or PLC systems. It defines a simple protocol data unit independent of the underlying data link layer. The modbus TCP packet includes 3 parts - MBAP header, function code and data payload, the MBAP header is used on TCP/IP header to identify the Modbus application Data Unit and provides some differences compared to the MODBUS RTU application data unit used on serial line. The MBAP header also includes unit identified to recognize and communicate between multiple independent modbus end units.

The modbus devices communicate using a master (client) /slave (server) architecture, only one device can initiate transaction and the others respond to the master/client. The other devices (slave/server) respond by supplying the requested data to the master/client, or by taking the action requested in the query. The slave/server can be any peripheral device (DSC unit, PLC unit, Volt/Current Transducer, network communication switch) which process information and sends the output data to the master using modbus TCP protocol. Korenix JetNet Switch operating as slave/server devices, while a typical master/client device is host computer running appropriate application software, like as SCADA / HMI system. The transaction architecture like as the drawing following.


Very High Power Line
Digital Current Transducer
Digital Power Breaker
Modbus salve
Modbus slave
Modbus slave
Modbus Serial
Modbus TCP/IP Gateway
Modbus TCP/IP slave/server
Modbus TCP/IP slave/server
Modbus TCP/IP Slave/Server
Ethernet Switch / Modbus TCP Slave (Server)
Ethernet Networking
Modbus TCP/IP Master/Client
Modbus TCP/IP Gateway
Modbus RTU
Modbus Serial
Modbus TCP/IP Master/Client
SCADA / HMI System

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

The JetNet Managed DIN-Rail Ethernet Switch has implemented modbus/ TCP register in the firmware. Those register mapping to some of Ethernet Switchs' operating information, includes description, IP address, power status, interface status, interface information and inbound/outbound packet statistics. With the register supports, user can read the information through their own Modbus TCP based progress/ display/ monitor applications and monitor the status of the switch easily.

The configuration of Modbus/TCP only present in CLI management mode and the no extra user interface for Web configuration.

5.3.1 Modbus Function Code

The Modbus TCP device uses a subset of the standard Modbus TCP function code to access device-dependent information. Modbus TCP function code is defined as below.

FC	Name	Usage
01	Read Coils	Read the state of a digital output
02	Read Input Status	Read the state of a digital input
03	Read Holding Register	Read holding register in 16-bits register format
04	Read Input Registers	Read data in 16-bits register format
05	Write Coil	Write data to force a digital output ON/OFF
06	Write Single Register	Write data in 16-bits register format
15	Force Multiple Coils	Write data to force multiple consecutive coils

The JetNet device supports the function code 04, which name is Read Input Registers. With this support, the remove SCADA or other Modbus TCP application can poll the information of the device and monitor the major status of the switch.

5.3.2 Error Checking

The utilization of the error checking will help eliminate errors caused by noise in the communication link. In Modbus TCP mode, messages include an error-checking field that is based on a Cyclical Redundancy Check (CRC) method. The CRC filed checks the contents of the entire message. It applied regardless of any parity check method used for the individual BYTE acters of the message. The CRC value is calculated by the transmitting device, which appends the CRC to the message. The receiving device recalculates a CRC during receipt of the message, and compares the calculated value to the actual value it received in the CRC filed.

5.3.3 Exception Response

If an error occurs, the slave sends an exception response message to master consisting of the slave address, function code, exception response code and error check field. In an exception response, the slave sets the high-order bit (MSB) of the response function code to one. The exception response codes are listed below.

Code	Name	Descriptions
01	Illegal Function	The message function received is not allowable action.
02	Illegal Data Address	The address referenced in the data field is not valid.
03	Illegal Data Value	The value referenced at the addressed device location is no within range.
04	Slave Device Failure	An unrecoverable error occurred while the slave was attempting to perform the requested action.
05	Acknowledge	The slave has accepted the request and processing it, but a long duration of time will be required to do so.
06	Slave Device Busy	The slave is engaged in processing a long-duration program command.
07	Negative Acknowledge	The slave cannot perform the program function received in the query.
08	Memory Parity Error	The slave attempted to read extended memory, but detected a parity error in the memory.

5.3.4 Modbus TCP register table

Since from firmware version 1.1, the JetNet 7500 & JetNet 5500 series start support Modbus TCP/IP client service for the Factory automation applications. The command of modbus only supports in the command line interface- console and telnet mode that allows user to modify some parameters like as idle time, number of modbus master and modbus service port.

Word Address	Data Type	Description
		System Information
0x0001 - 0x0010	16 words	Vender Name = "Korenix" Word 0 Hi byte = 'K' Word 0 Lo byte = 'o' Word 1 Hi byte = 'r' Word 1 Lo byte = 'e' Word 2 Hi byte = 'n' Word 2 Lo byte = 'I' Word 2 Hi byte = 'x' Word 2 Lo byte = '\0' (other words = 0)
0x0011 – 0x0020	16 words	Product Name = "JetNet5828G" Word 0 Hi byte = 'J' Word 0 Lo byte = 'e' Word 1 Hi byte = 'T' Word 1 Lo byte = 'N' Word 2 Hi byte = 'e' Word 2 Lo byte = 't' Word 3 Hi byte = '5' Word 3 Lo byte = '8' Word 4 Lo byte = '2' Word 4 Hi byte = '8' Word 5 Lo byte = 'G' Word 5 Hi byte = '\0' (other words = 0)
0x0021 – 0x00A0	128 words	SNMP system name (string)
0x00A1 – 0x00120	128 words	SNMP system location (string)
0x0121 – 0x01A0	128 words	SNMP system contact (string)
0x01A1 – 0X01C0	32 words	SNMP system OID (string)
0x01C1 – 0x1C2	2 words	System uptime (unsigned long)

0x0201 – 0x0202	2 words	hardware version
0x0203 – 0x0204	2 words	S/N information
0x0205 – 0x0206	2 words	CPLD version
0x0207 – 0x0208	2 words	Boot loader version
0x0209 – 0x02A0	2 words	Firmware Version Word 0 Hi byte = major Word 0 Lo byte = minor Word 1 Hi byte = reserved Word 1 Lo byte = reserved
0x020B – 0x20C	2 words	Firmware Release Date Firmware was released on 2010-08-11 at 09 o'clock Word 0 = 0x0B09 Word 1 = 0x0A08
0x020D – 0x21F	3 words	Ethernet MAC Address Ex: MAC = 01-02-03-04-05-06 Word 0 Hi byte = 0x01 Word 0 Lo byte = 0x02 Word 1 Hi byte = 0x03 Word 1 Lo byte = 0x04 Word 2 Hi byte = 0x05 Word 2 Lo byte = 0x06
0x0301 – 0x0302	2 words	IP address Ex: IP = 192.168.10.1 Word 0 Hi byte = 0xC0 Word 0 Lo byte = 0xA8 Word 1 Hi byte = 0x0A Word 1 Lo byte = 0x01
0x0303 – 0x0304	2 words	Subnet Mask
0x0305 – 0x0306	2 words	Default Gateway
0x0307 – 0x0308	2 words	DNS Server
0x0401	1 word	PWR1 0x0000:Off 0x0001:On 0xFFFF: unavailable

0x0402	1 word	PWR2 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0403	1 word	PWR3 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0404	1 word	PWR4 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0411	1 word	DI1 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0412	1 word	DI2 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0413	1 word	DO1 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0414	1 word	DO2 0x0000:Off 0x0001:On 0xFFFF: unavailable
0x0421	1 word	RDY 0x0000:Off 0x0001:On
0x0422	1 word	RM 0x0000:Off 0x0001:On
0x0423	1 word	RF 0x0000:Off

		0x0001:On
Port Information (32 Ports)		
0x1001 - 0x1200	16 words	Port Description
0x1201- 0x1220	1 word	Administrative Status 0x0000: disable 0x0001: enable
0x1221 - 0x1240	1 word	Operating Status 0x0000: disable 0x0001: enable 0xFFFF: unavailable
0x1241 - 0x1260	1 word	Duplex 0x0000: half 0x0001: full 0x0003: auto (half) 0x0004: auto (full) 0x0005: auto 0xFFFF: unavailable
0x1261 - 0x1280	1 word	Speed 0x0001: 10 0x0002: 100 0x0003: 1000 0x0004: 2500 0x0005: 10000 0x0101: auto 10 0x0102: auto 100 0x0103: auto 1000 0x0104: auto 2500 0x0105: auto 10000 0x0100: auto 0xFFFF: unavailable
0x1281 - 0x12A0	1 word	Flow Control 0x0000: off 0x0001: on 0xFFFF: unavailable
0x12A1 - 0x12C0	1 word	Default Port VLAN ID 0x0001-0xFFFF
0x12C1 - 0x12E0	1 word	Ingress Filtering 0x0000: disable 0x0001: enable

0x12E1 - 0x1300	1 word	Acceptable Frame Type 0x0000: all 0x0001: tagged frame only
0x1301 - 0x1320	1 word	Port Security 0x0000: disable 0x0001: enable
0x1321 - 0x1340	1 word	Auto Negotiation 0x0000: disable 0x0001: enable 0xFFFF: unavailable
0x1341 - 0x1360	1 word	Loopback Mode 0x0000: none 0x0001: MAC 0x0002: PHY 0xFFFF: unavailable
0x1361 - 0x1380	1 word	STP Status 0x0000: disabled 0x0001: blocking 0x0002: listening 0x0003: learning 0x0004: forwarding
0x1381 - 0x13A0	1 word	Default CoS Value for untagged packets
0x13A1 - 0x13C0	1 word	MDIX 0x0000: disable 0x0001: enable 0x0002: auto 0xFFFF: unavailable
0x13C1 - 0x13E0	1 word	Medium mode 0x0000: copper 0x0001: fiber 0x0002: none 0xFFFF: unavailable

Modbus/TCP client will return 0xFFFF to modbus master as it sets reserved address.

5.3.5 CLI commands for Modbus TCP

The CLI commands of Modbus TCP are listed as following table.

Feature	Command & example
Enable Modbus TCP	Switch(config)# modbus enable
Disable Modbus TCP	Switch(config)# modbus disable
Set Modbus interval time between request	Switch(config)# modbus idle-timeout <200-10000> Timeout value: 200-10000ms Switch(config)#modbusidle-timeout200 → setinterval requesttimeoutdurationto200ms.

Set modbus TCP master communicate session.	Switch(config)# modbus master <1-20> Max Modbus TCP Master Switch(config)# modbus master 2→set maximum modbus master up to 2; maximum support up to 20 modbus communicate sessions.
Set modbus TCP listening port	Switch(config)# modbus port port Listening Port Switch(config)# modbus port 502 ; default modbus TCP service port is 502.

5.4 About Korenix

Less Time At Work! Fewer Budget on applications!

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

Fusion of outstandings

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

Core Strength---Competitive Price and Quality

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

Global Sales Strategy

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

Quality Services

KoreCARE--- KoreCARE is Korenix Technology's global service center, where our professional staffs are ready to solve your problems at any time and in real-time. All Korenix 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-year Warranty

All Korenix products are compliant with specific industrial standards from design, validation to manufacturing. Product series warranty are guaranteed to Korenix valued customers as the Hyperlink https://www.korenix.com/en/support/p02.aspx?kind=9
Exception please refer to the product datasheet or the <exception list>.
Accessory

- Power Supply: 3 years
- SFP: 1 year
- Antenna: 1 year

Note: Warranty starts from Korenix invoice date

Korenix Technologies Co., Ltd.

Business service:sales@korenix.com
Customer service:koreCARE@korenix.com

5.4 Release History

Edition	Date	Modifications
V0.1	25/03/2020	First Release
V1.0	24/04/2020	Second Release