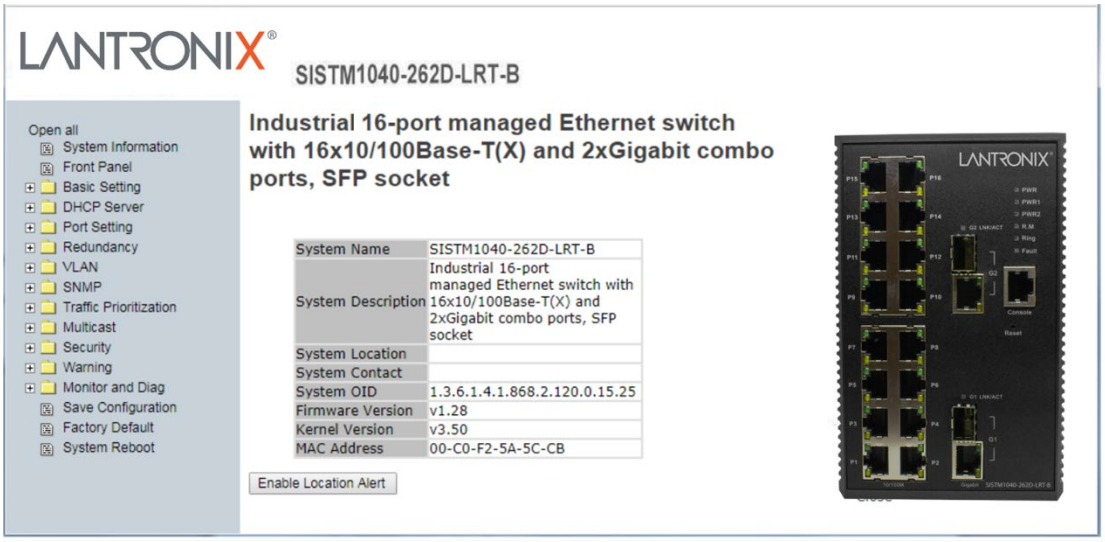
LANTRONIX®



SISTM1040-262D-LRT-B

Industrial Managed Ethernet Switch

User Guide

Part Number 33617

Revision C August 2025

Intellectual Property

Warranty

For details on the Lantronix warranty policy, go to http://www.lantronix.com/support/warranty.

Contacts

Lantronix Corporate Headquarters

48 Discovery, Suite 250

Irvine, CA 92618, USA

Toll Free: 800-526-8766

Phone: 949-453-3990

Fax: 949-453-3995

Technical Support

Email: techsupport@transition.com

Sales Offices

For a current list of our domestic and international sales offices, go to www.lantronix.com/about/contact.

Disclaimer

All information contained herein is provided “AS IS.” Lantronix undertakes no obligation to update the information in this publication. Lantronix does not make, and specifically disclaims, all warranties of any kind (express, implied or otherwise) regarding title, non-infringement, fitness, quality, accuracy, completeness, usefulness, suitability or performance of the information provided herein. Lantronix shall have no liability whatsoever to any user for any damages, losses and causes of action (whether in contract or in tort or otherwise) in connection with the user’s access or usage of any of the information or content contained herein. The information and specifications contained in this document are subject to change without notice.

Revision History

Date	Rev.	Description
6/1/15	A	Initial release for SISTM1040-262D-LRT-B at v 1.2.
3/14/22	B	Update specifications and Regulatory Agency information. FW v1.36: add Web UI port alias info, SSH and TACACS+. Add CLI commands security https, security ssh, no security https, no security ssh. Modify Redundant Ring description. FW Change SSH / Telnet Logout timeout to 5 minutes. Add PTP Client, Upgrade HTTPS Certification, TACACS+, Auto SFP, SFP Monitor, and HTTPS and SSH security. Remove IPv6 and G.8032 (ERPS) configuration. Change SSH / Telnet Logout timeout to 5 minutes. Initial Lantronix rebrand.
August 2025	C	Removed ATEX references.

Contents

1 Introduction

Product Description

The SISTM1040-262D-LRT-B Ethernet switch is powerful managed hardened switch with many features. It operates in a wide temperature range, and dusty and humid conditions. It can be managed via the Web, Telnet, Console port, or third-party SNMP software.

1.1 Software Features

- Redundant Ethernet Ring (Recovery time < 10ms over 250 units connection)
- Supports Ring Coupling, Dual Homing and standard STP/RSTP/MSTP
- Supports SNMPv1/v2c/v3 & Port base/802.1Q VLAN Network Management
- Event notification by Email, SNMP trap, and Relay Output
- Web-based, Telnet, Console, CLI configuration
- Enable/disable ports, MAC based port security
- Port based network access control (802.1x)
- VLAN (802.1Q) to segregate and secure network traffic
- RADIUS centralized password management
- TACACS+ Server and Client configuration
- SNMPv3 encrypted authentication and access security
- Quality of Service (802.1p) for real-time traffic
- VLAN (802.1Q) with double tagging and GVRP support
- IGMP Snooping for multicast filtering
- Port configuration, status, statistics, mirroring, security

1.2 Hardware Features

- Two redundant DC power inputs
- Wide Operating Temperature: -40 ºC to +60ºC
- Storage Temperature: -40 to 85ºC
- Operating Humidity: 5% to 95%, non-condensing
- Casing: IP-30
- 10/100/1000Base-T(X) Gigabit Ethernet port (combo ports)
- 10/100Base-T(X) Ethernet ports
- 100/1000Base-X on SFP port (combo ports)
- Console Port

1.4 Packing List

Verify that you have received the items below. Contact your sales representative if any item is missing or damaged. Please save the packaging for possible future use.

- One SISTM1040-262D-LRT-B Managed Hardened Switch
- One DIN-Rail Kit
- One Wall-mount Kit
- One Console Cable
- One 6-Pin Terminal block
- One printed Quick Start Guide
- One Documentation Postcard

1.5 Optional Accessories

- SFP Modules
- OCA-P181610 Outdoor Cabinet Assembly
- 25165 Universal AC/DC Input DIN Rail Mountable +12 VDC Power Supply
- SPS-UA12DHT External Power Supply (sold separately)

2. Hardware Installation

2.1 Installing the Switch on DIN-Rails

Each switch has a Din-Rail clip on the back panel. The Din-Rail clip can be used to mount the switch on a 35mm Din-Rail.

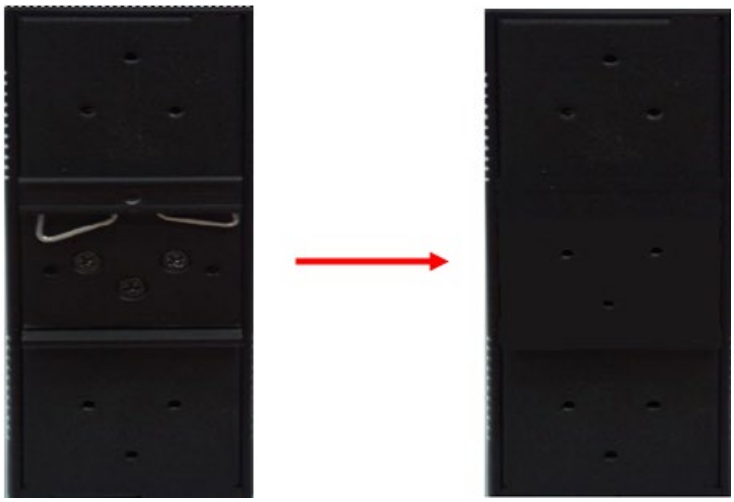
Step 1: Slant the switch and position the metal spring behind the top edge of the Din-Rail.

Step 2: Push the switch down on the Din-Rail until the bottom of the clip grips the bottom edge of the DIN Rail. You may hear a “click” sound when this happens.

2.1 Wall Mounting Installation

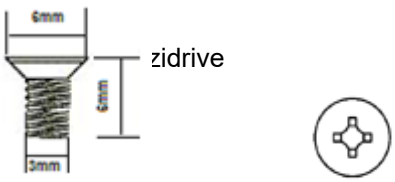
Each switch includes a wall mount bracket in the package. The following steps show how to mount the switch on a panel or wall:

Step 1: Remove the Din-Rail clip by removing the 3 screws.



Step 2: Use the screws that can be found in the package to install the wall mount bracket.

The screw specifications are shown below. In order to prevent damage to the SDSTX3110-121-LRT, the size of screws should not be larger or longer than the size used for the DIN Rail clip.

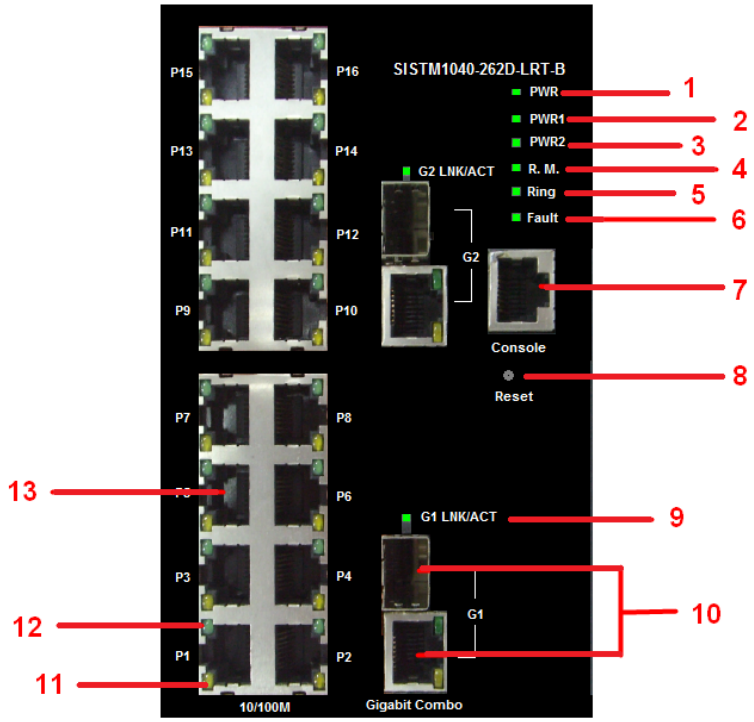


3. Hardware Overview

3.1 Front Panel

The SISTM1040-262D-LRT-B front panel is shown and described below.

Port	Description
10/100 RJ-45 Fast Ethernet ports	8 10/100Base-T(X) RJ-45 fast Ethernet ports support auto-negotiation. Default Settings: Speed: auto, Duplex: auto, Flow control: disabled.
Gigabit RJ-45 port	2 10/100/1000Base-TX Giga ports (combo).
Fiber port	2 100/1000Base-X on SFP port (combo).
Console	Use RS-232 to RJ-45 connecter to manage switch.
Reset	Push Reset button for 2 to 3 seconds to reset the switch. Push Reset button for 5 seconds to reset the switch to **Factory defaults.**



1. **PWR**: When the PWR is UP, the green LED lights.
2. **PWR1**: When the PWR2 links, the green LED lights.
3. **PWR2**: When the PWR2 links, the green LED lights.
4. **RM** (Ring Master): When lit, the switch is the Ring Master.
5. **Ring**: When lit, the Ring is activated.
6. **Fault**: Indicates a Power failure or Port down/fail when lit.
7. **Console** port (RJ-45).
8. **Reset** button. Push the button 3 seconds for reset; 5 seconds for factory default.
9. 1000Base-X COMBO SFP Port Link/Act LED.
10. 1000Base-T Gigabit Ethernet port COMBO 1000Base-X Fiber port on SFP.

11. 10/100/1000 Base-T(X) Ethernet ports **Link** LED.
12. 10/100/1000 Base-T(X) Ethernet ports **ACT** LED.
13. 10/100/1000 Base-T(X) Ethernet ports.

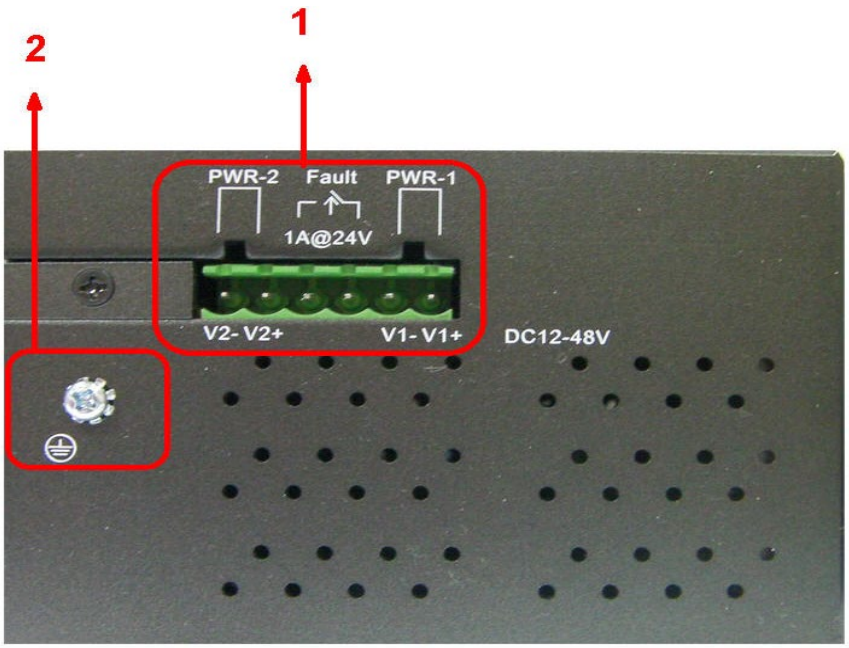
3.2 Front Panel LEDs

LED	Color	Status	Description
PWR	Green	On	DC power ready
PW1	Green	On	DC power module 1 activated.
PW2	Green	On	DC power module 2 activated.
R.M	Green	On	Ring Master.
Ring	Green	On	Ring enabled.
		Slowly blinking	Ring has only One link (lack of one link to build the ring).
		Fast blinking	Ring work normally.
Fault	Amber	On	Fault relay. Power failure or Port down/fail.
10/100Base-T(X) Fast Ethernet ports			
LNK / ACT	Green	On	Port link up.
		Blinking	Data transmitted.
Full Duplex	Amber	On	Port works under full duplex.
Gigabit Ethernet ports			
LNK/ACT	Green	On	Port link up.
		Blinking	Data transmitted.
Indicator	Amber	On	Port link on 100Mbps
SFP ports			
LNK / ACT	Green	On	Port link up.
		Blinking	Data transmitted.

3.3 Top Panel

The SISTM1040-262D-LRT-B top panel components are shown below.

1. Terminal block includes: PWR-1, PWR-2 (12-48V DC) and Fault connections.
2. Ground wire connector.



3.4 Terminal block Installation

1. Cable temperature rating not less than 80° C.
2. The Terminal Block (J9) – Cat. No. 2EHDRC-06P by Dinkle Enterprise Co., Ltd., rated 300 V, 15 A, 105°C, FW-1 mating with Cat. No. 2ESDV-06P by Dinkle Enterprise Co., Ltd., rated 300 V, 15 A, 105°C, FW-2, suitable for 12-28 AWG (3.3 mm² – 0.08 mm²) wire size, torque value 4.5 lb-in (0.508 N-m).
3. The min. cross-sectional area of the protective conductor used for earthing is same size as power conductor.

2EHDRC-06P

2ESDV-06P

3.5 Fault Relay

The SISTM1040-262D-LRT-B Fault Relay Output is 24Vdc, 1A.

Fault Alarms

When any selected fault event occurs, the front panel Fault LED lights and the electric relay is signaled. Fault Alarms are configurable via the CLI and/or Web GUI. The fault alarms include:

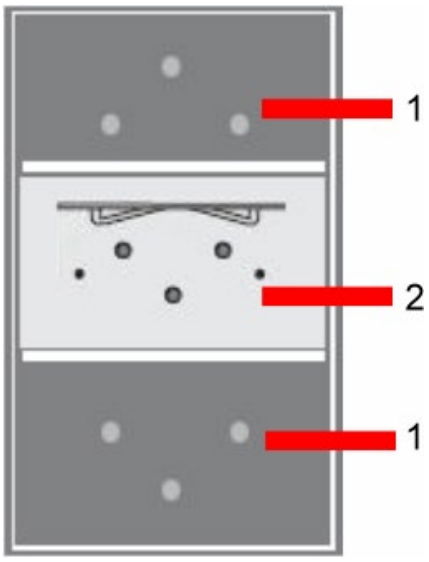
Power Failure: fault alarm when any selected power failure. This switch supports dual power supplies.

Port Link Down/Broken: fault alarm when any selected port link down/broken.

3.6 Back Panel

The SISTM1040-262D-LRT-B back panel components are shown below.

1. Screw holes for wall mount kit.
2. DIN-Rail kit.



4. Cables

4.1 Ethernet Cables

The SISTM1040-262D-LRT-B switch has standard Ethernet ports. Based on the link type, the switch uses CAT 3, 4, 5, or 5e UTP cables to connect to other network equipment (PCs, servers, switches, routers, or hubs). Refer to the following table for cable specifications.

Cable Types and Specifications:

Cable	Type	Max. Length	Connector
10BASE-T	Cat.3, 4, 5 100-ohm	UTP 100 m (328 ft)	RJ-45
100BASE-TX	Cat.5 100-ohm UTP	UTP 100 m (328 ft)	RJ-45
1000BASE-TX	Cat.5/Cat.5e 100-ohm UTP	UTP 100 m (328ft)	RJ-45

4.1.1 10/100/100BASE-TX/10BASE-T Pin Assignments

For 100BASE-TX/10BASE-T cables, pins 1 and 2 are used for transmitting data, and pins 3 and 6 are used for receiving data.

1000 Base-T RJ-45 Pin Assignments :

Pin Number	Assignment
1	BI_DA+
2	BI_DA-
3	BI_DB+
4	BI_DC+
5	BI_DC-
6	BI_DB-
7	BI_DD+
8	BI_DD-

The SISTM1040-262D-LRT-B supports auto MDI/MDI-X operation. Straight- through or cross-over cables can be used to connect the switch to other equipment. The table below shows the 10BASE-T/ 100BASE-TX MDI and MDI-X port pin outs.

10/100 Base-TX MDI/MDI-X pins assignment:

Pin Number	MDI port	MDI-X port
1	TD+(transmit)	RD+(receive)
2	TD-(transmit)	RD-(receive)
3	RD+(receive)	TD+(transmit)
4	Not used	Not used
5	Not used	Not used
6	RD-(receive)	TD-(transmit)
7	Not used	Not used
8	Not used	Not used

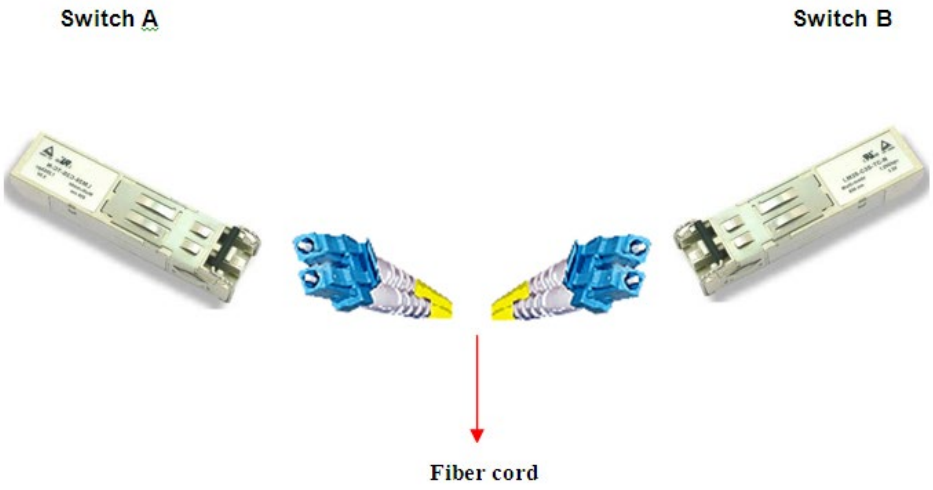
1000 Base-T MDI/MDI-X pins assignment:

Pin Number	MDI port	MDI-X port
1	BI_DA+	BI_DB+
2	BI_DA-	BI_DB-
3	BI_DB+	BI_DA+
4	BI_DC+	BI_DD+
5	BI_DC-	BI_DD-
6	BI_DB-	BI_DA-
7	BI_DD+	BI_DC+
8	BI_DD-	BI_DC-

Note: “**+**” and “**-**” signs represent the polarity of the wires that make up each wire pair.

4.2 SFPs

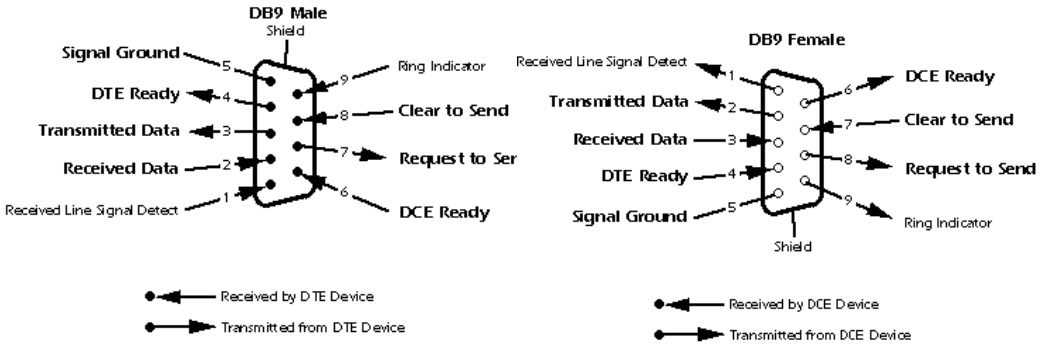
The ISTM1040-262D-LRT-B has fiber optical ports with SFP connectors. The fiber optical ports are in multi-mode and single-mode with LC connector. Note that the TX port of Switch A should be connected to the RX port of Switch B. **Note**. Optical Transceiver must be compliant with 21CFR(J) Laser Class 1.



4.3 Console Cable

SISTM1040-262D-LRT-B switch can be managed through the serial console port. A DB-9 to RJ-45 cable can be found in the package. This cable can be used to connect a PC via a RS-232 cable with DB-9 female connector and the other end (RJ-45 connector) connects to console port of switch. **Caution**: The Console port is for maintenance purposes only, and it may only be used when the area is known to be non-hazardous.

PC pin out (male)	RS-232 with DB9 female connector	DB9 to RJ-45
Pin #2 RD	Pin #2 TD	Pin #2
Pin #3 TD	Pin #3 RD	Pin #3
Pin #5 GD	Pin #5 GD	Pin #5



5. Web Management

Warning!!! While configuring or upgrading firmware, please remove physical loop connection first. DO NOT power off equipment during firmware upgrade!

5.1 Configuration by Web Browser

This section introduces the configuration via a Web browser.

5.1.1 About Web-based Management

The switch contains an embedded HTML web server. It contains advanced management features and allows you to manage the switch from anywhere on the network through a standard web browser such as Microsoft Internet Explorer. The Web-Based Management function supports Internet Explorer 5.0 or later. It is based on Java Applets with an aim to reduce network bandwidth consumption, enhance access speed and present an easy viewing screen. **Note:** By default, IE5.0 or later versions do not allow Java Applets to open sockets. You must explicitly modify the browser setting to enable Java Applets to use network ports.

Preparing for Web Management

The default values are:

IP Address: **192.168.1.77**

Subnet Mask: **255.255.255.0**

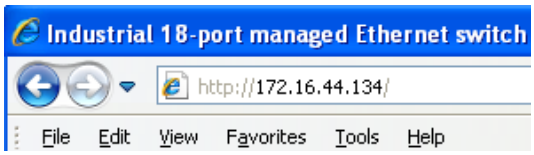
Default Gateway: **192.168.1.254**

User Name: **root**

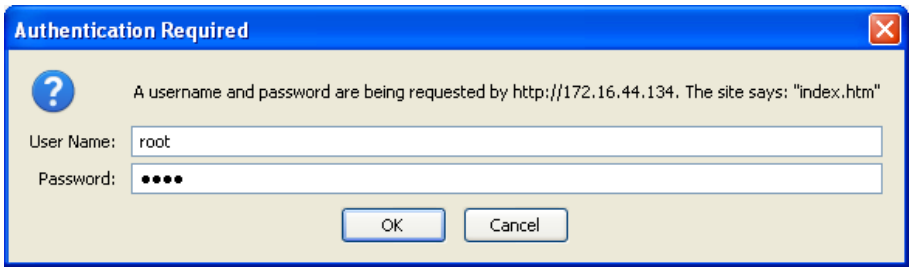
Password: **root**

System Login

1. Launch the web browser (e.g., Internet Explorer).
2. Type http:// and the IP address of the switch. Press "**Enter**".

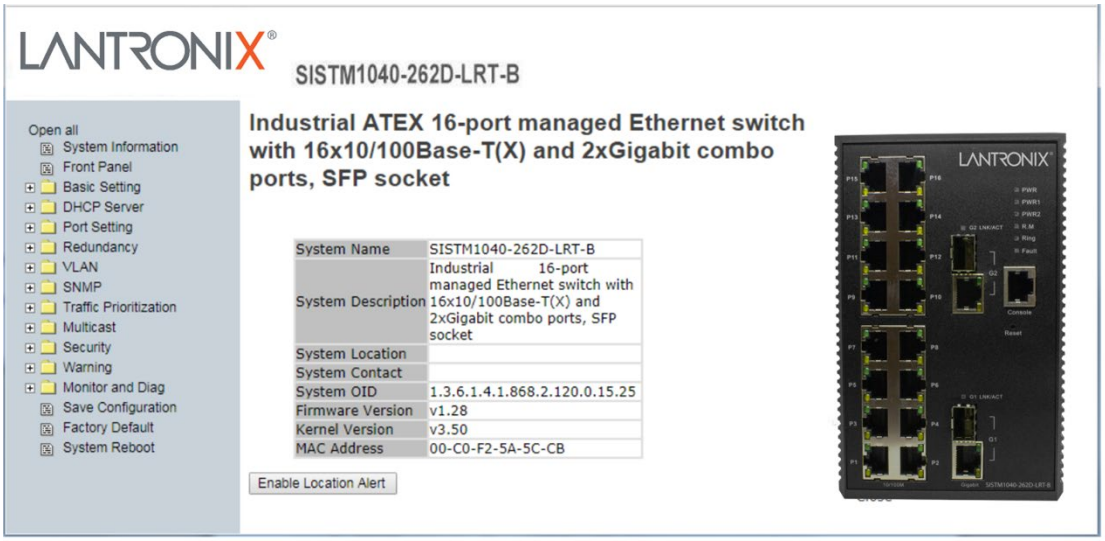


3. The login screen displays.



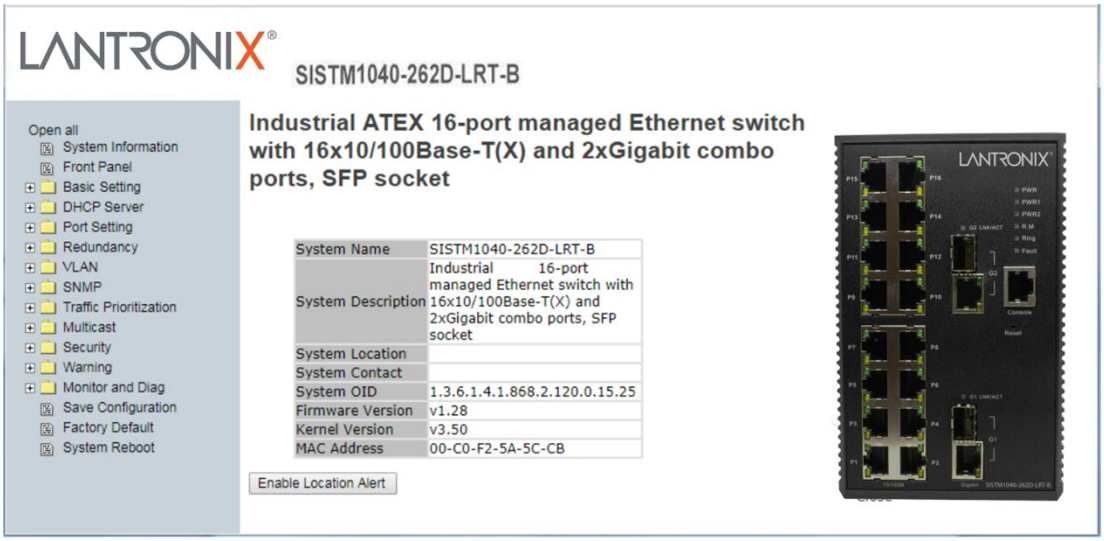
4. Key in the username and password. The default username and password is "**admin**".
5. Click the "**OK**" button. The main interface of the Web-based management displays.

Main Interface



5.1.2 System Information

Click System Information to display basic switch information (e.g., System Name, Description, and Location) and to display the Enable Location Alert button and front panel.

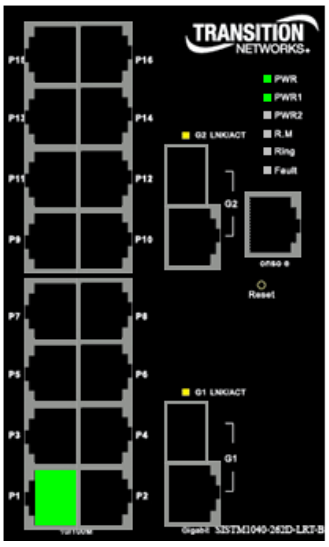


Enable Location Alert

When you click Enable Location Alert, the front panel PWR1, PWR2 and PWR3 LEDs start flashing. Click Disable Location Alert to cause the LEDs to stop flashing.

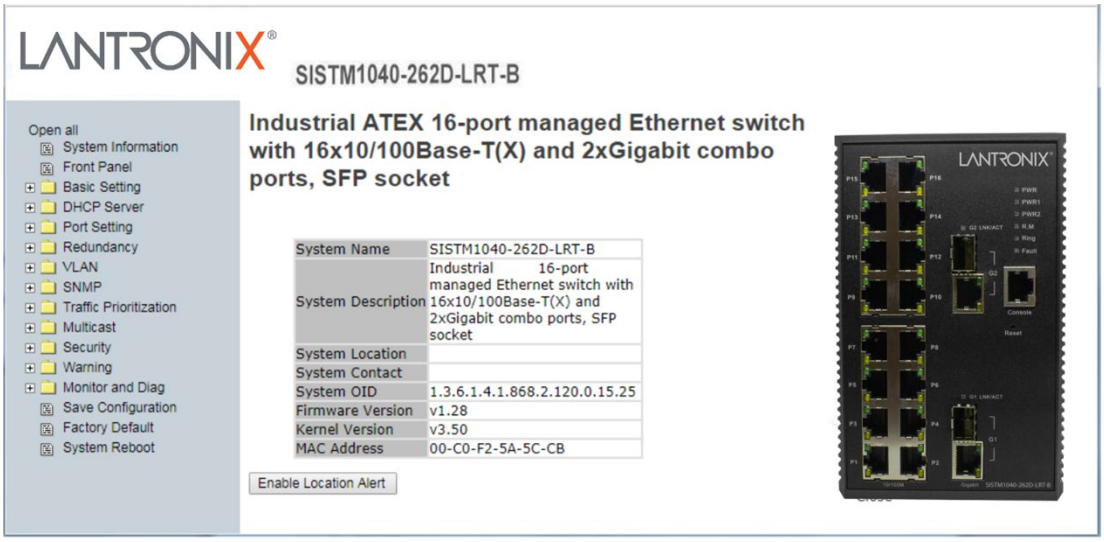
5.1.3 Front Panel

Show the panel of the SISTM1040-262D-LRT-B. Click "**Close**" to close the panel on the Web UI.



5.1.4 Basic Settings

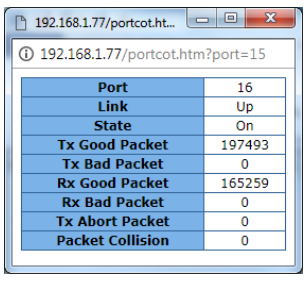
5.1.4.1 Switch Setting



The following table describes the labels in this screen.

Label	Description
System Name	Assign the name of switch. The maximum length is 64 bytes. The default is "*Industrial 16-port managed Ethernet switch with 16x10/100Base-T(X) and 2xGigabit combo ports, SFP socket*".
System Description	Display the description of switch.
System Location	Assign the switch physical location. The maximum length is 64 bytes.
System Contact	Enter the name of contact person or organization.
System OID	Displays the switch's OID (object identifier) information.
Firmware Version	Displays the switch's firmware version.
Kernel Version	Displays the kernel software version.
Device MAC	Displays the unique hardware address assigned by manufacturer (default).
Apply	Click "**Apply**" to activate the configurations.
Help	Displays the online help file for this page.

Note: you can click on any port on the front panel to display that port's status window.



5.1.4.2 Admin Password

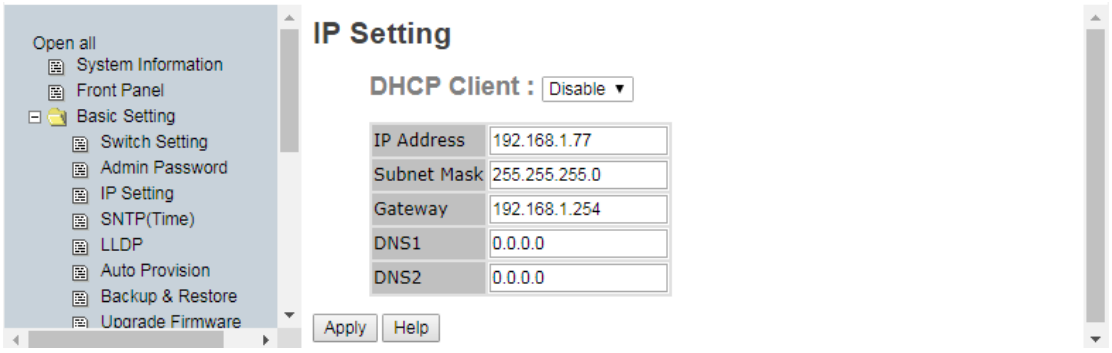
At Basic Setting > Admin Password you can change the Web management login User Name and Password for management security.

The following table describes the labels in this screen.

Label	Description
User Name	Key in the new username (the default is "**root**").
New Password	Key in the new password (the default is "**root**").
Confirm password	Re-type the new password.
Apply	Click "**Apply**" to activate the configurations.
Help	Displays the online help file for this page.

5.1.4.3 IP Setting

You can configure the IP Settings and DHCP client function via the Basic Setting > IP Setting menu path.



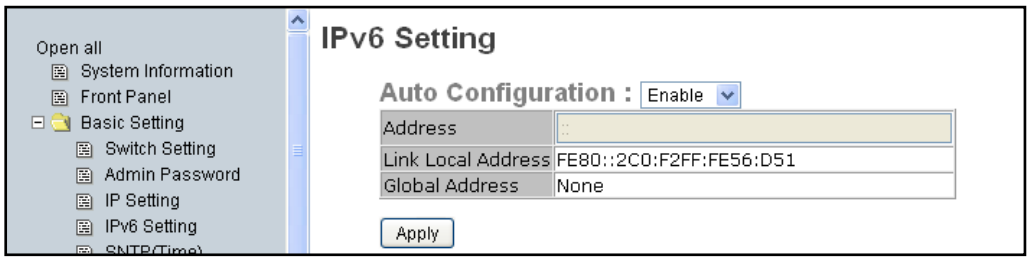
IP Configuration interface

The following table describes the labels in this screen.

Label	Description
DHCP Client	To enable or disable the DHCP client function. When DHCP client function is enabling, the switch will be assigned the IP address from the network DHCP server. The default IP address will be replaced by the IP address which the DHCP server has assigned. After clicking "**Apply**" button, a popup dialog displays to inform when the DHCP client is enabled. A new IP will be assigned by the DHCP server.
IP Address	Assign the IP address that the network is using. If DHCP client function is enabled, you do not need to assign the IP address. The network DHCP server will assign the IP address for the switch and it will be displayed in this column. The default IP address is 192.168.1.77.
Subnet Mask	Assign the subnet mask of the IP address. If DHCP client function is enabling, you do not need to assign the subnet mask
Gateway	Assign the network gateway for the switch. The default gateway is 192.168.1.254.
DNS1	Assign the primary DNS IP address.
DNS2	Assign the secondary DNS IP address.
Apply	Click "**Apply**" to activate the configurations.
Help	Displays the online help file for this page.

5.1.4.4 IPv6 Setting

You can configure the IPv6 configuration via IPv6 Settings.



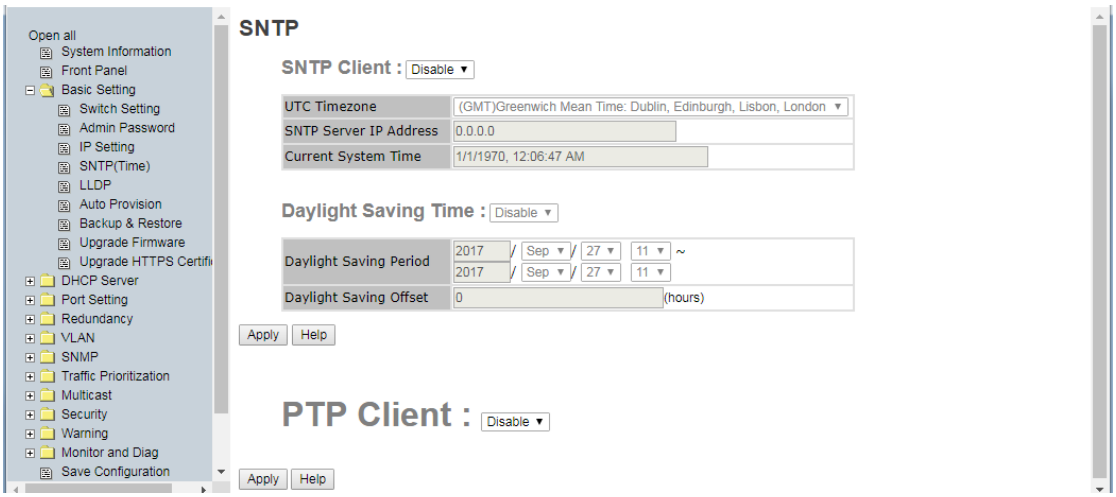
IPv6 Configuration interface

The following table describes the labels in this screen.

Label	Description
Auto Configuration :	At the dropdown select Enable or Disable of auto config.
Address	Grayed out if auto config is Enabled. Displays **::** by default if auto config is Disabled; enter the IPv6 address here manually.
Link Local Address	FE80::2C0:F2FF:FE56:D51
Global Address	None
Apply	Click "**Apply**" to activate the configuration.
Help	Displays the online help file.

5.1.4.5 SNTP (Time)

The SNTP (Simple Network Time Protocol) settings let you synchronize switch clocks via the Internet.



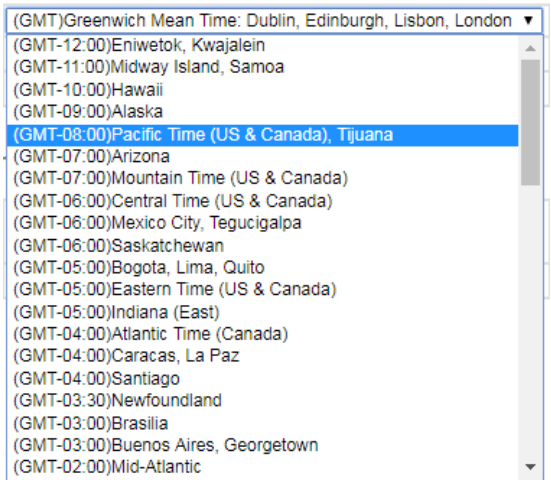
SNTP Configuration interface

The following table describes the labels in this screen.

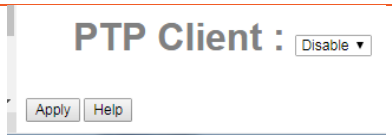
Label	Description
SNTP Client	Enable or disable SNTP function to get the time from the SNTP server.
UTC Timezone	Set the switch location time zone. The different location time zones are listed below.
SNTP Server IP Address	Set the SNTP server IP address.
Daylight Saving Time	Enable or disable daylight saving time function. When daylight saving time is enabled, you must configure the daylight saving time period.
Daylight Saving Period	Set up the Daylight Saving beginning time and Daylight Saving ending time. Both will be different each year.
Daylight Saving Offset	Set up the offset time.
Apply	Click “**Apply**” to activate the configurations.
Help	Displays the online help file for this page.

Local Time Zones

(GMT-12:00)Eniwetok, Kwajalein (GMT-11:00)Midway Island, Samoa (GMT-10:00)Hawaii (GMT-09:00)Alaska (GMT-08:00)Pacific Time (US & Canada), Tijuana (GMT-07:00)Arizona (GMT-07:00)Mountain Time (US & Canada) (GMT-06:00)Central Time (US & Canada) (GMT-06:00)Mexico City, Tegucigalpa (GMT-06:00)Saskatchewan (GMT-05:00)Bogota, Lima, Quito (GMT-05:00)Eastern Time (US & Canada) (GMT-05:00)Indiana (East) (GMT-04:00)Atlantic Time (Canada) (GMT-04:00)Caracas, La Paz (GMT-04:00)Santiago (GMT-03:30)Newfoundland (GMT-03:00)Brasilia (GMT-03:00)Buenos Aires, Georgetown (GMT-02:00)Mid-Atlantic (GMT-01:00)Azores, Cape Verde Is. (GMT)Casablanca, Monrovia (GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London (GMT+01:00)Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna (GMT+01:00)Belgrade, Bratislava, Budapest, Ljubljana, Prague (GMT+01:00)Brussels, Copenhagen, Madrid, Paris, Vilnius (GMT+01:00)Sarajevo, Skopje, Sofija, Warsaw, Zagreb (GMT+02:00)Athens, Istanbul, Minsk (GMT+02:00)Bucharest (GMT+02:00)Cairo (GMT+02:00)Harare, Pretoria (GMT+02:00)Helsinki, Riga, Tallinn (GMT+02:00)Jerusalem (GMT+03:00)Baghdad, Kuwait, Riyadh (GMT+03:00)Moscow, St. Petersburg, Volgograd (GMT+03:00)Mairobi (GMT+03:30)Tehran (GMT+04:00)Abu Dhabi, Muscat (GMT+04:00)Baku, Tbilisi (GMT+04:30)Kabul (GMT+05:00)Ekaterinburg (GMT+05:00)Islamabad, Karachi, Tashkent (GMT+05:30)Bombay, Calcutta, Madras, New Delhi (GMT+06:00)Astana, Almaty, Dhaka (GMT+06:00)Colombo (GMT+07:00)Bangkok, Hanoi, Jakarta (GMT+08:00)Beijing, Chongqing, Hong Kong, Urumqi (GMT+08:00)Perth (GMT+08:00)Singapore (GMT+08:00)Taipei (GMT+09:00)Osaka, Sapporo, Tokyo (GMT+09:00)Seoul (GMT+09:00)Yakutsk (GMT+09:30)Adelaide (GMT+09:30)Darwin (GMT+10:00)Brisbane (GMT+10:00)Canberra, Melbourne, Sydney (GMT+10:00)Guam, Port Moresby (GMT+10:00)Hobart (GMT+10:00)Vladivostok (GMT+11:00)Magadan, Solomon Is., New Caledonia (GMT+12:00)Auckland, Wllington (GMT+12:00)Fiji, Kamchatka, Marshall Is.



5.1.4.6 PTP Client



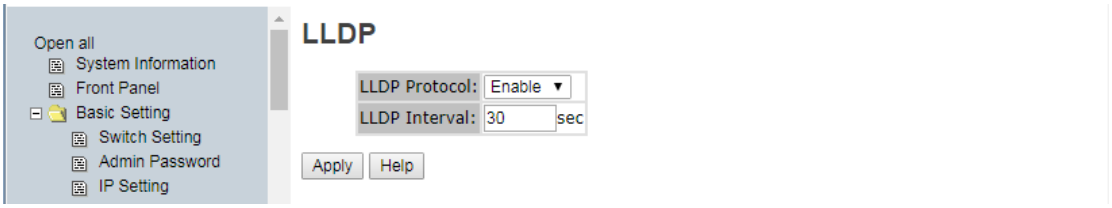
The Precision Time Protocol (PTP) is a protocol used to synchronize clocks throughout a computer network. On a local area network, it achieves clock accuracy in the sub-microsecond range, making it suitable for measurement and control systems.

PTP was originally defined in the IEEE 1588-2002 standard, officially entitled "Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems" and published in 2002. In 2008, IEEE 1588-2008 was released as a revised standard; also known as PTP Version 2, it improves accuracy, precision and robustness but is not backward compatible with the original 2002 version.

Label	Description
PTP Client	Enable or disable the PTP function to get the time from the PTP server.
Apply	Click “**Apply**” to activate the configurations.
Help	Displays the online help file for this page.

5.1.4.7 LLDP

LLDP (Link Layer Discovery Protocol) allows the switch to provide its information to other nodes on the network and store the information it discovers.



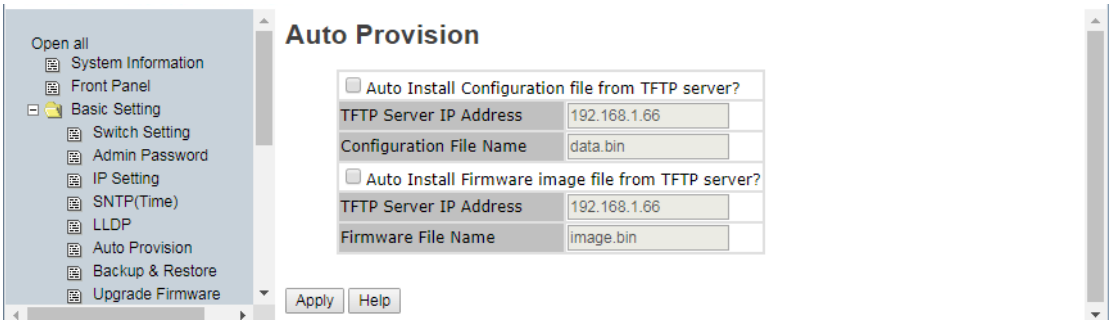
LLDP configuration interface

The following table describes the labels in this screen.

Label	Description
LLDP Protocol	"**Enable**" or "**Disable**" LLDP function.
LLDP Interval	The interval of sending LLDP information (the default is 30 seconds)
Apply	Click "**Apply**" to activate the configuration.
Help	Displays the online help file for this page.

5.1.4.8 Auto Provision

Auto Provision allows you to update the switch firmware automatically. You put the firmware or configuration file on a TFTP server, and then when you reboot the switch, it will upgrade automatically. Before updating, make sure your TFTP server is ready and the firmware image and configuration file are on the TFTP server.

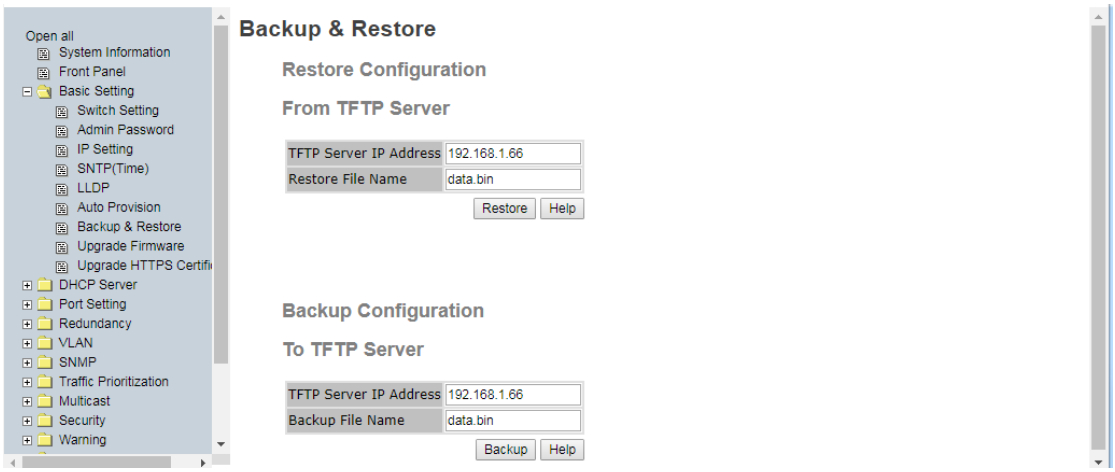


Auto Provision interface

Label	Description
Auto Install Configuration file from TFTP server?	Check to "**Enable**" or uncheck to "**Disable**" the Auto Install function.
TFTP Server IP Address	Enter the IP address of the TFTP server.
Configuration File Name	Enter the config filename with a .bin suffix.
Auto Install Firmware image file from TFTP server?	Check to "**Enable**" or uncheck to "**Disable**" the Auto Install function.
TFTP Server IP Address	Enter the IP address of the TFTP server.
Firmware File Name	Enter the config filename with a .bin suffix.
Apply	Click "**Apply**" to activate the configuration settings.
Help	Show help file.

5.1.4.9 Backup & Restore

You can save the current configuration from the switch to a TFTP server or restore the configuration from a TFTP server on this page.



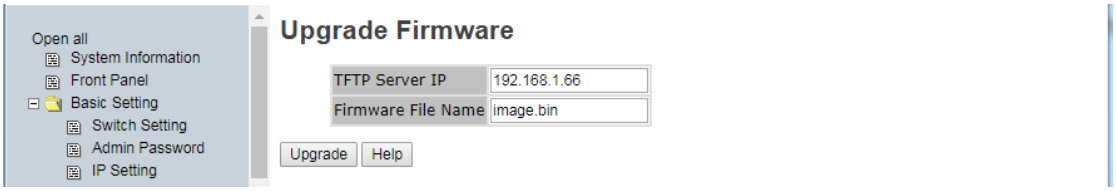
Backup & Restore interface

The following table describes the labels in this screen.

Label	Description
TFTP Server IP Address	Fill in the TFTP server IP address.
Restore File Name	Type in the file name (*xxxxx.bin*).
Restore	Click the "**Restore**" button to restore the configurations.
Backup File Name	Type in the file name (*xxxxx.bin*).
Backup	Click "**backup**" to back up the configurations.

5.1.4.10 Upgrade Firmware

Upgrade Firmware lets you update the firmware of the switch. Before updating, make sure your TFTP server is ready and the firmware image is on the TFTP server.

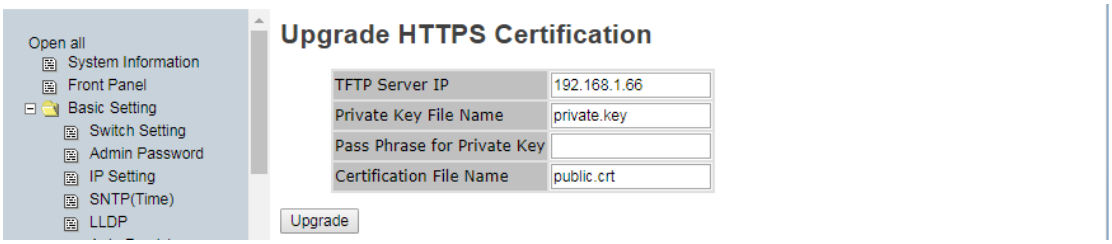


Update Firmware interface

Label	Description
TFTP Server IP	Enter the IP address of the TFTP server.
Firmware File Name	Enter the firmware filename with a .bin suffix.
Upgrade	Click the **Upgrade** button to update the switch firmware.

5.1.4.11 Upgrade HTTPS Certification

Upgrade HTTPS Certification lets you update the private key via the TFTP server. HTTP Secure is a communications protocol for secure communication over a computer network which is widely used on the Internet. HTTPS consists of communication over Hypertext Transfer Protocol (HTTP) within a connection encrypted by Transport Layer Security, or its predecessor, Secure Sockets Layer. The main use of HTTPS is authentication of a visited website and protection of the privacy and integrity of the exchanged data.



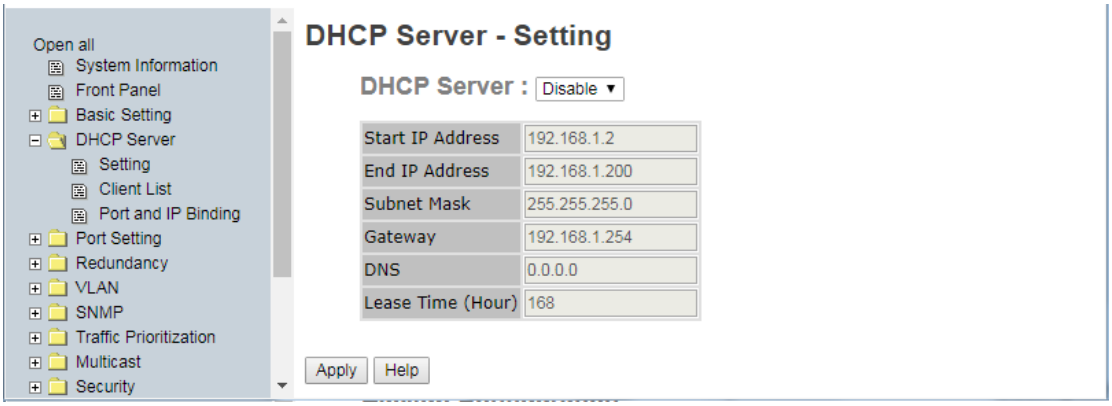
Upgrade HTTPS Certification interface

Label	Description
TFTP Server IP	Enter the IP address of the TFTP server (e.g., 192.168.1.66).
Private Key File Name	Enter the firmware filename with a .bin suffix.
Pass Phrase for Private Key	The passphrase (password) to access the Private Key.
Certification File Name	The filename of the certificate file. (e.g., *public.crt*).
Upgrade	Click the **Upgrade** button to start the process.

5.1.5 DHCP Server

5.1.5.1 DHCP Server – Setting

The system provides a DHCP server function. If enabled the switch system will be a DHCP server that can automatically assign an IP address to a DHCP client.



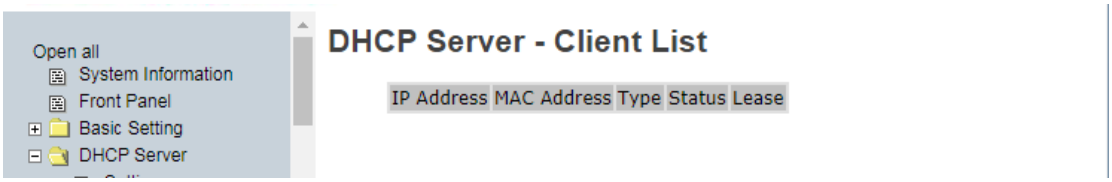
DHCP Server Configuration interface

The following table describes the labels in this screen.

Label	Description
DHCP Server	Enable or Disable the DHCP Server function. Enable – the switch will be the DHCP server on your local network
Start IP Address	The dynamic IP assign range. Low IP address is the beginning of the dynamic IP assigns range. For example: if the dynamic IP assign range is from 192.168.1.100 to 192.168.1.200, then 192.168.1.100 will be the Start IP address.
End IP Address	The dynamic IP assign range. High IP address is the end of the dynamic IP assigns range. For example: if the dynamic IP assign range is from 192.168.1.100 to 192.168.1.200, then 192.168.1.200 will be the End IP address
Subnet Mask	The dynamic IP assign range subnet mask.
Gateway	The IP address of the gateway in your network.
DNS	Domain Name Server IP Address in your network.
Lease Time (Hour)	The period of time before the system will reset the assigned dynamic IP to ensure the IP address is used.
Apply	Click “**Apply**” to activate the configurations.

5.1.5.2 DHCP Server – Client List

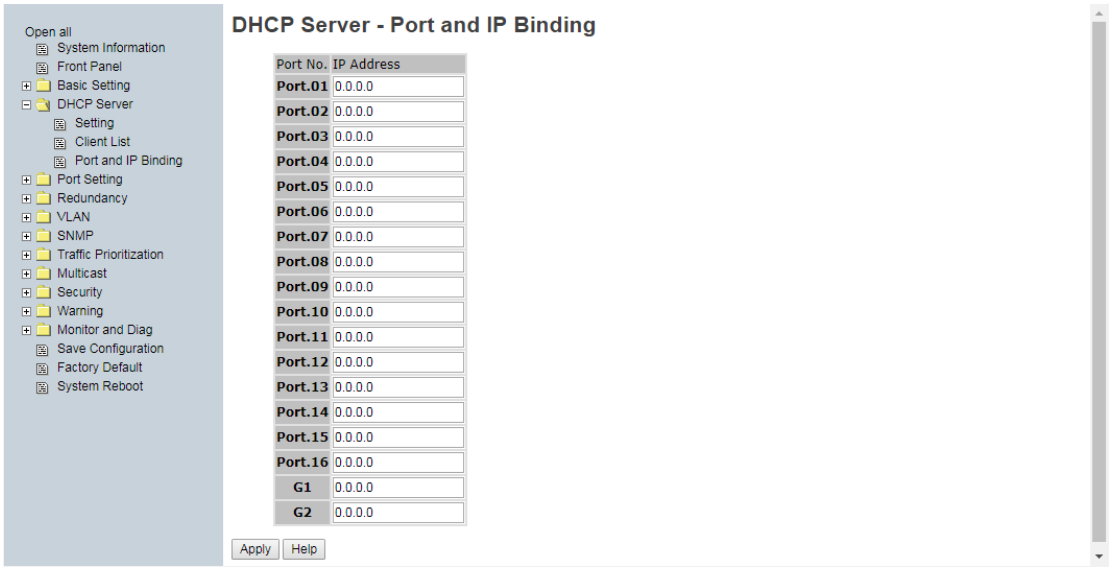
When the DHCP server function is activated, the system will collect the DHCP client information and display it here.



DHCP Server Client List interface

5.1.5.3 DHCP Server – Port and IP bindings

You can assign the specific IP addresses that are in the assigned dynamic IP range to specific ports. When a device is connecting to the port and asks for an IP address, the system will assign the IP address that was assigned to the previous device connected to that port.

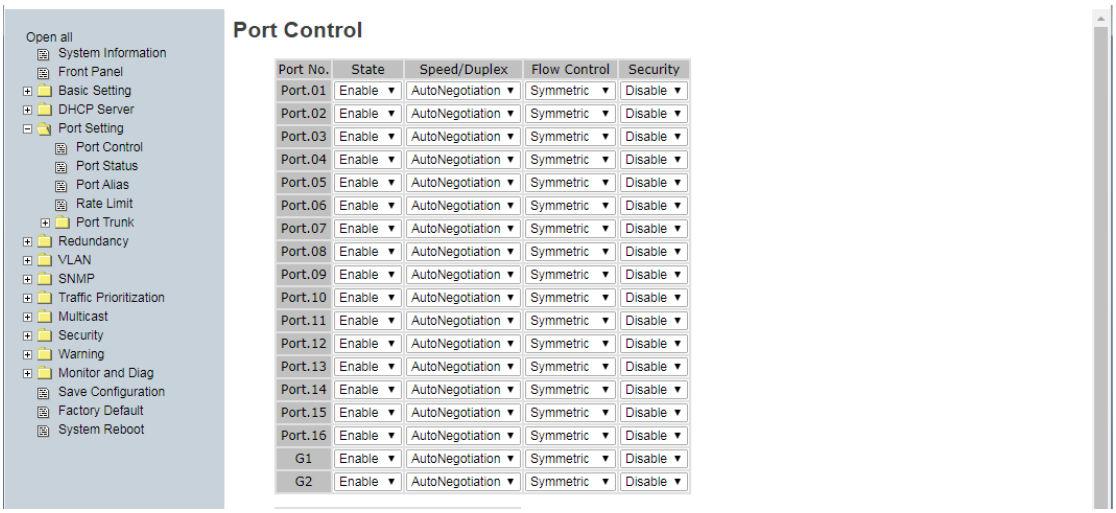


DHCP Server - Port and IP Binding interface

5.1.6 Port Setting

5.1.6.1 Port Control

This function lets you set the state, speed/duplex, flow control, and security of the ports.



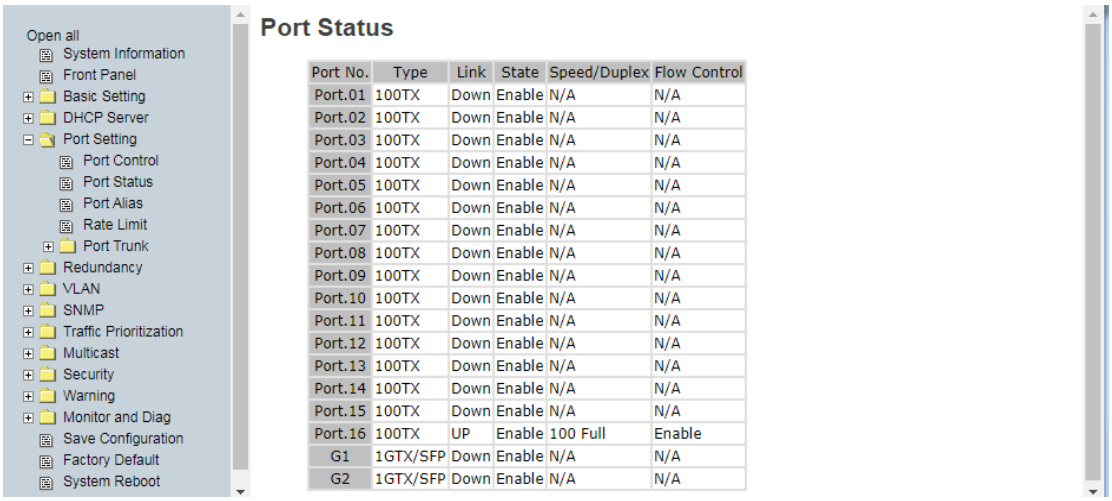
Port Control interface

The following table describes the labels in this screen.

Label	Description
Port No.	Port number for setting.
State	Dropdown to select **Enable** or **Disable**.
Speed/Duplex	You can set copper ports to **AutoNegotiation**, **100 full**, **100 half**, **10 full** or **10 half**. You can set fiber (SFP) ports to **AutoNegotiation**, **1000 full**, **1000 half**, **100 full**, **100 half**, **10 full**, **10 half** or **100 SFP**.
Flow Control	Select **Symmetric** or **Asymmetric** mode to avoid packet loss when congestion occurs.
Security	**Enable** or **Disable** port security function. When enabled, the port will STOP learning MAC address dynamically.
Auto Detect 100/1000 SFP	Enable or disable the automatic detection of 100/1000 Mbps SFP modules. The default is Enabled.
Apply	Click “**Apply**” to activate the configuration settings.

5.1.6.2 Port Status

This page displays the current port status information (read only).



Port No.	Type	Link	State	Speed/Duplex	Flow Control
Port.01	100TX	Down	Enable	N/A	N/A
Port.02	100TX	Down	Enable	N/A	N/A
Port.03	100TX	Down	Enable	N/A	N/A
Port.04	100TX	Down	Enable	N/A	N/A
Port.05	100TX	Down	Enable	N/A	N/A
Port.06	100TX	Down	Enable	N/A	N/A
Port.07	100TX	Down	Enable	N/A	N/A
Port.08	100TX	Down	Enable	N/A	N/A
Port.09	100TX	Down	Enable	N/A	N/A
Port.10	100TX	Down	Enable	N/A	N/A
Port.11	100TX	Down	Enable	N/A	N/A
Port.12	100TX	Down	Enable	N/A	N/A
Port.13	100TX	Down	Enable	N/A	N/A
Port.14	100TX	Down	Enable	N/A	N/A
Port.15	100TX	Down	Enable	N/A	N/A
Port.16	100TX	UP	Enable	100 Full	Enable
G1	1GTX/SFP	Down	Enable	N/A	N/A
G2	1GTX/SFP	Down	Enable	N/A	N/A

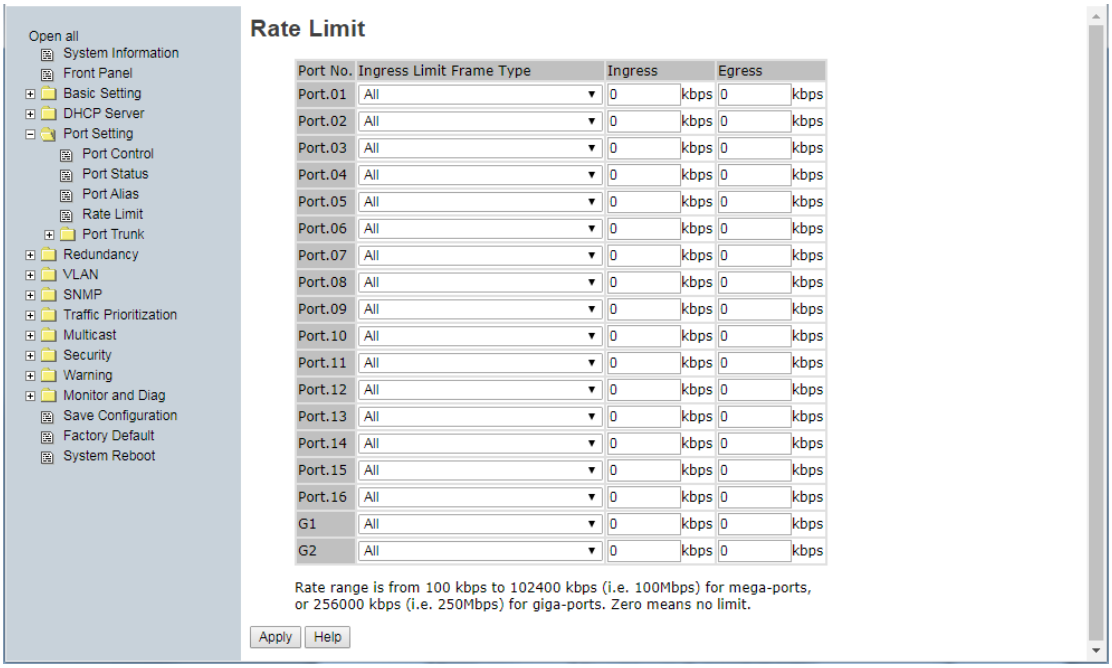
Port Status interface

The following table describes the labels in this screen.

Label	Description
Port No.	Port number for this row.
Type	The port type (e.g., 100TX or 1GTX/SFP).
Link	The port status (UP or Down).
State	The port state (Enable or Disable).
Speed/Duplex	Copper ports can display **AutoNegotiation**, **100 full**, **100 half**, **10 full** or **10 half**. Displays **N/A** if not applicable. Fiber (SFP) ports can display **AutoNegotiation**, **1000 full**, **1000 half**, **100 full**, **100 half**, **10 full**, **10 half** or **100 SFP**. Displays **N/A** if not applicable.
Flow Control	Select **Symmetric** or **Asymmetric** mode to avoid packet loss when congestion occurs.
Security	**Enable** or **Disable** port security function. When enabled, the port will STOP learning MAC address dynamically.
Auto Detect 100/1000 SFP	Enable or disable the automatic detection of 100/1000 Mbps SFP modules. The default is Enabled.
Apply	Click “**Apply**” to activate the configurations.

5.1.6.3 Rate Limit

This page lets you limit traffic of all ports, including broadcast, multicast, and flooded Unicast. You can also set “Ingress” or “Egress” to limit received or transmitted traffic rates.



Rate Limit interface

The following table describes the labels in this screen.

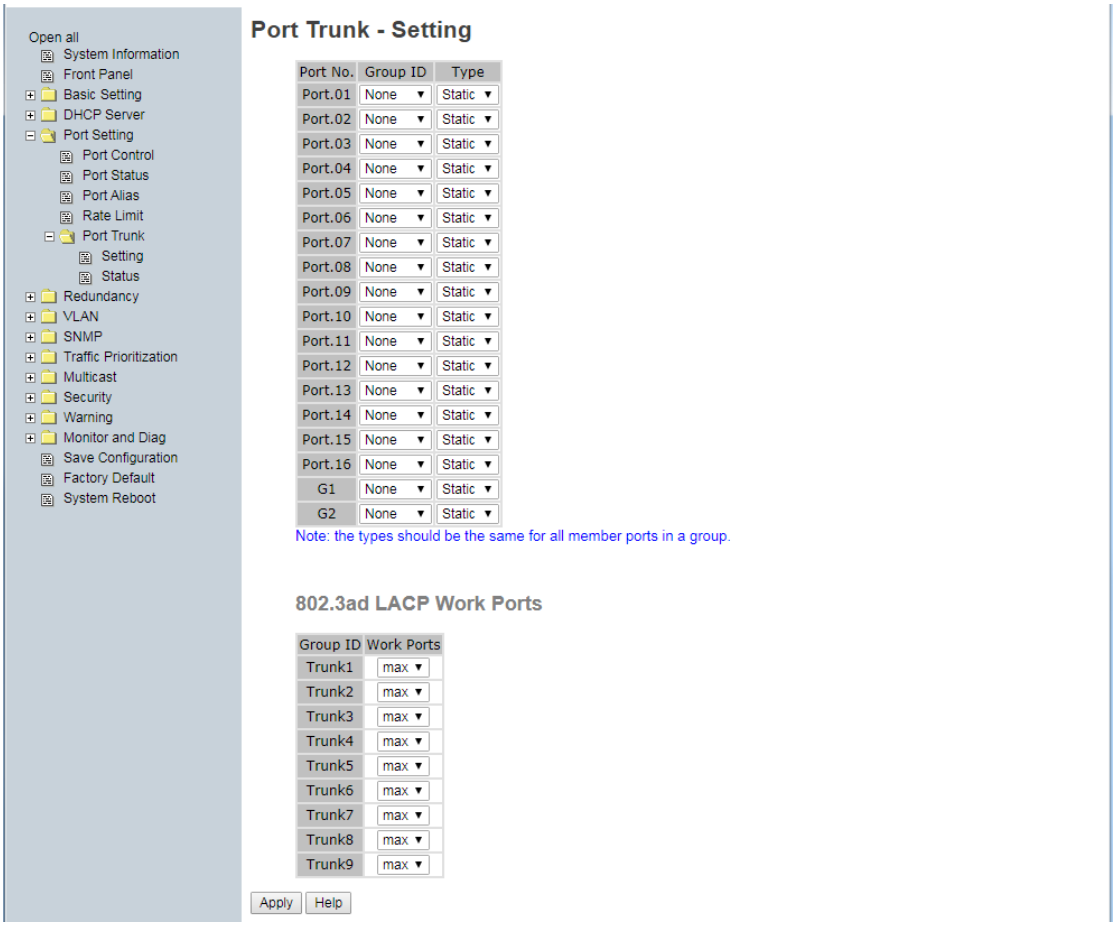
Label	Description
Ingress Limit Frame Type	You can select “**All**”, “**Broadcast only**”, ”**Broadcast/Multicast**” or ”**Broadcast/Multicast/Flooded Unicast**” mode.
Ingress	The switch port traffic receive rate in kbps.
Egress	The switch port traffic transmit rate in kbps.
Apply	Click “**Apply**” to activate the configuration settings.

The valid Rate Limit range is from 100 kbps to 102400 kbps (i.e. 100Mbps) mega-ports, or 256000 kbps (i.e. 250Mbps) for giga-ports. Zero means no limit.

5.1.6.4 Port Trunk

Port Trunk – Setting

You can select static trunk or 802.3ad LACP to combine several physical links with a logical link to increase the bandwidth.



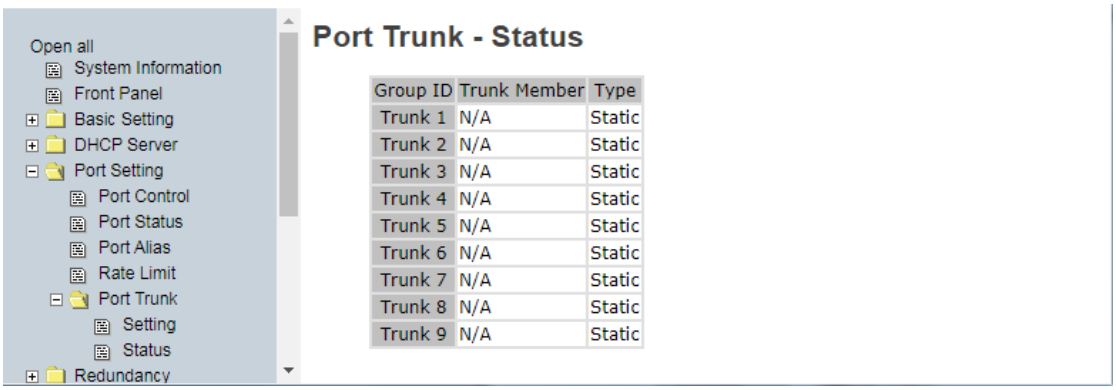
Port Trunk - Setting interface

The following table describes the labels in this screen.

Label	Description
Group ID	Select port(s) to join a trunk group (e.g., **Trunk1**).
Type	Select **Static** trunk or 802.3ad **LACP**. Note that **Type** selection should be the same for all member ports in a group.
Work Ports (for802.3ad LACP only)	Enter a work port number. The default is 0.
Apply	Click "**Apply**" to activate the configuration settings.

Port Trunk – Status

You can check the configuration of port trunk.



Port Trunk - Status interface

The following table describes the labels in this screen.

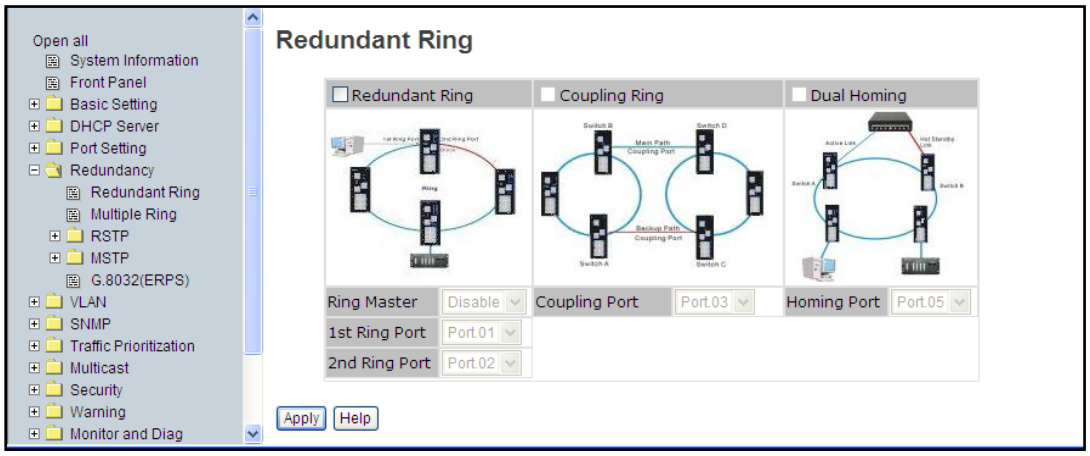
Label	Description
Group ID	Select port to join a trunk group.
Trunk Member	Whether a member of the trunk group.
Type	Support **Static** trunk and 802.3ad **LACP**.

5.1.7 Redundancy

5.1.7.1 Redundant Ring Technologies

This feature provides one of the most powerful Redundant Ring technologies in the world.

The recovery time is less than 10 ms over 250 units of connections. It can reduce unexpected malfunctions caused by network topology changes. Ring technology support includes three Ring topologies for network redundancy: Redundant Ring, Coupling Ring, and Dual Homing.



Redundant Ring interface

The following table describes the labels in this screen.

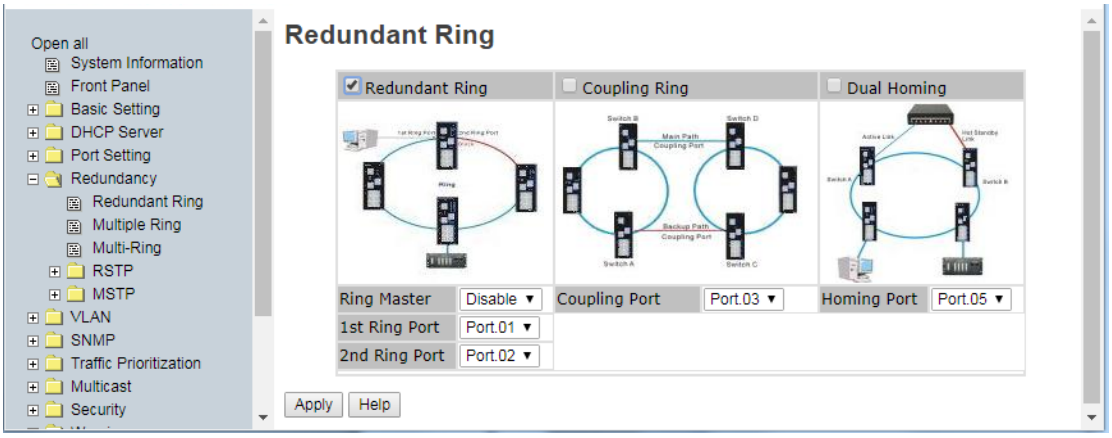
Label	Description
Redundant Ring	Tick the checkbox to enable Redundant Rings.
Ring Master	There should be one and only one Ring Master in a ring. However, if there are two or more switches set as the Ring Master, the switch with the lowest MAC address will be the actual Ring Master and others will be Backup Ring Masters.
1st Ring Port	The primary port, when this switch is configured for Redundant Ring.
2nd Ring Port	The backup port, when this switch is configured for Redundant Ring.
Coupling Ring	Tick the checkbox to enable Coupling Ring. Coupling Ring can be used to divide a big ring into two smaller Rings to avoid effecting all switches when network topology changes. It is a good application for connecting two Rings.
Coupling Port	Set a port as coupling port to link to the Coupling Port of the switch in another ring. Coupling Ring needs four switches to construct an active and a backup link. The coupled four ports of four switches will be operated at active/backup mode.

Dual Homing	Tick the checkbox to enable Dual Homing mode. By selecting Dual Homing mode, the Ring will be connected to normal switches through two RSTP links (i.e., backbone Switch). The two links provide an active mode and a backup mode, and connect each Ring to the normal switches in RSTP mode.
Homing Port	Set a port as Homing Port to link to the Homing Port of the switch in the same ring. The Homing Port used to transmit control signals.
Apply	Click the "**Apply**" button to activate the configuration.

Note: It is not recommended to set one switch as a Ring Master and as Coupling Ring at the same time due to heavy load of system.

5.1.7.2 Redundant Ring Configurations

Redundant Ring technology can be applied for other vendor's proprietary ring. Thus, you can add SISTM1040-262D-LRT-B switches into a network constructed by other ring technology and enable Redundant Ring to inter-operate with the other vendor's managed switches.



Note: Configure Network redundancy protocols completely for all switches in a redundant network before actually connecting any backup/redundant path to prevent inadvertently generating traffic loops.

Note: You cannot have more than one redundancy protocol (Redundant Ring, RSTP, MSTP) enabled at the same time.

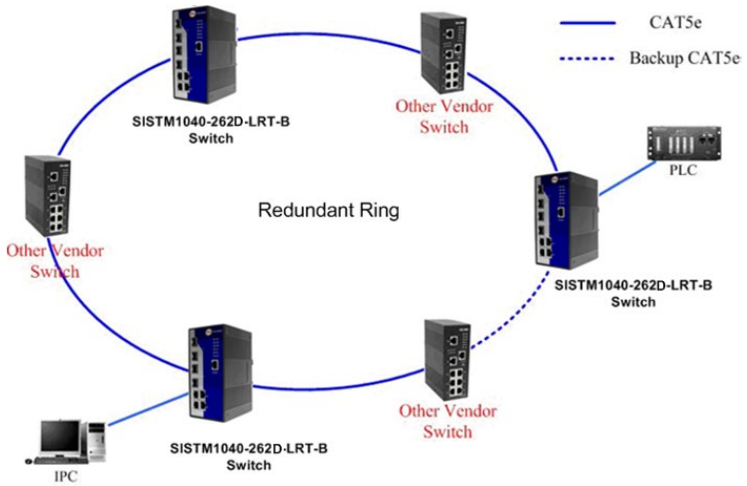
Redundant Ring

The Redundant Ring Protocol is a very fast network redundancy protocol that provides link fail-over protection with very fast self-healing recovery. Note that all switches must enable Redundant Ring in a ring.

Redundant Ring interface

Label	Description
Ring Master	Select Enable to select the Redundant Ring function. There should be one and only one Ring Master in a ring. If there are two or more switches set Ring Master to enable, the switch with the lowest MAC address will be the actual Ring Master and others will be Backup Masters.
1st Ring Port	Choose the port which connects to the ring. The 1st Ring Port is the *primary* port if this switch is Ring Master.
2nd Ring Port	Choose the port which connects to the ring. The 2nd Ring Port is the backup port if this switch is Ring Master.

A Redundant Ring connection application example is shown below.

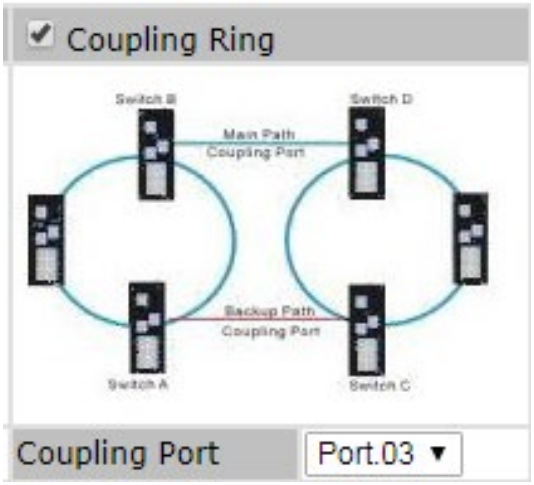


Redundant Ring connection

Coupling Ring

At Redundancy > Redundant Ring you can check the Coupling Ring checkbox and configure the Coupling Ring function. **Note** that only two switches can enable Coupling Ring in a ring. More or less is invalid. **Note**:

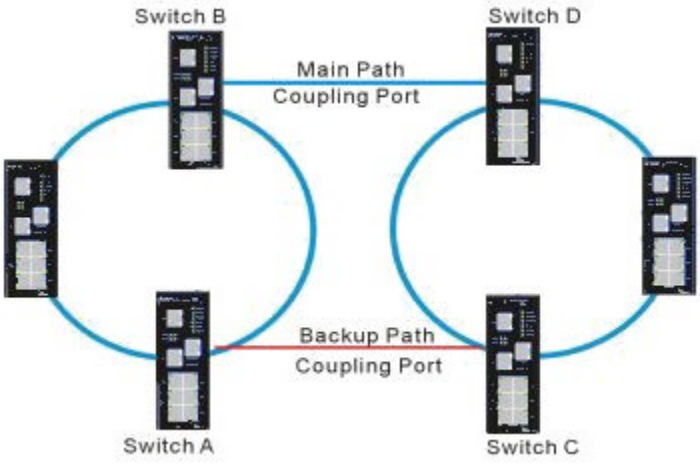
that it is not recommended to set one switch as a Ring Master and as Coupling Ring at the same time due to heavy load of system.



Coupling Ring interface

Label	Description
Coupling Port	This port provides the link to the Coupling Port of the switch in another ring.

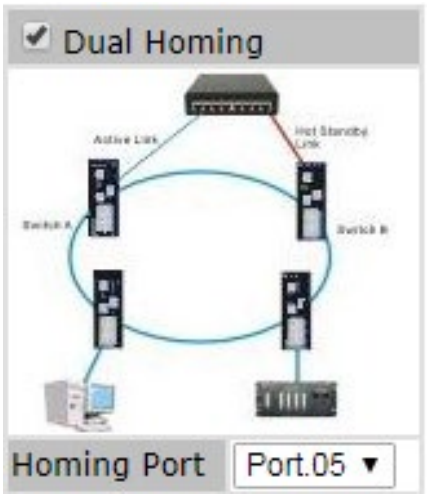
A Coupling Ring connection application example is shown below.



The message: *Apply fail Wrong data submitted* displays if you try to configure the same port for more than one function (e.g., port 2 configured as both 1st Ring Port and 2nd Ring Port, or port 3 configured as both Coupling Port and Homing Port). Click the Retry button and change one of the port settings.

Dual Homing

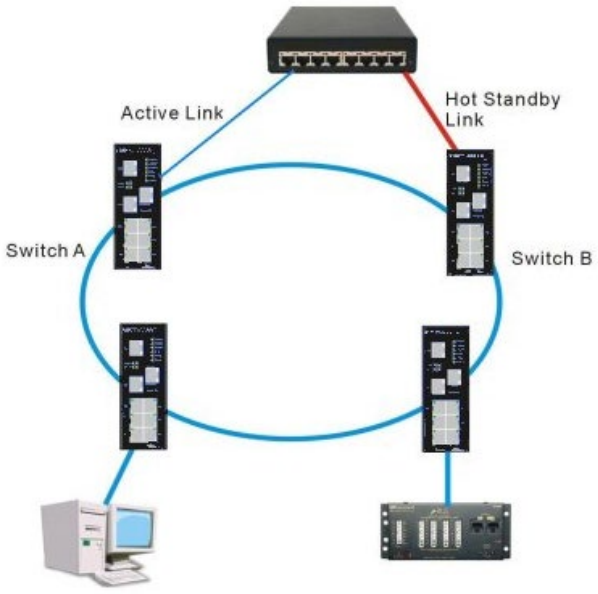
At Redundancy > Redundant Ring you can check the Dual Homing checkbox and configure the Dual Homing function. **Note** that only two switches can enable Dual Homing in a ring. More or less is invalid.



Dual Homing interface

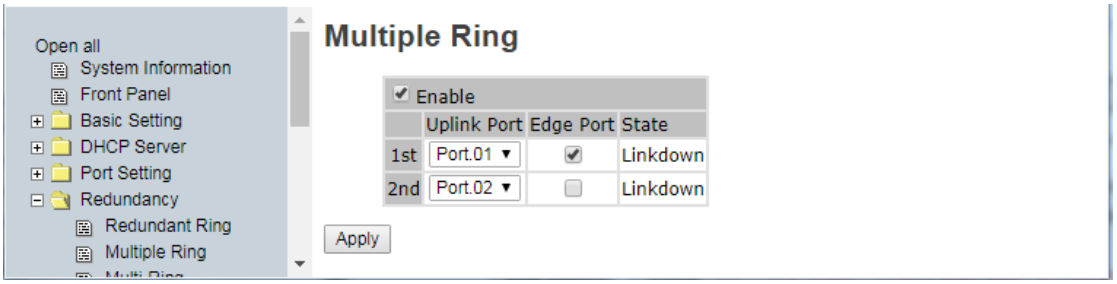
Label	Description
Homing Port	Set a port as Homing Port to link to the Homing Port of the switch in the same ring. The Homing Port is used to transmit control signals.

A Dual Homing connection application example is shown below.



Multiple Ring

The Redundancy > Multiple Ring menu path displays the Multiple Ring page. Here you can enable and configure Multiple Ring parameters.

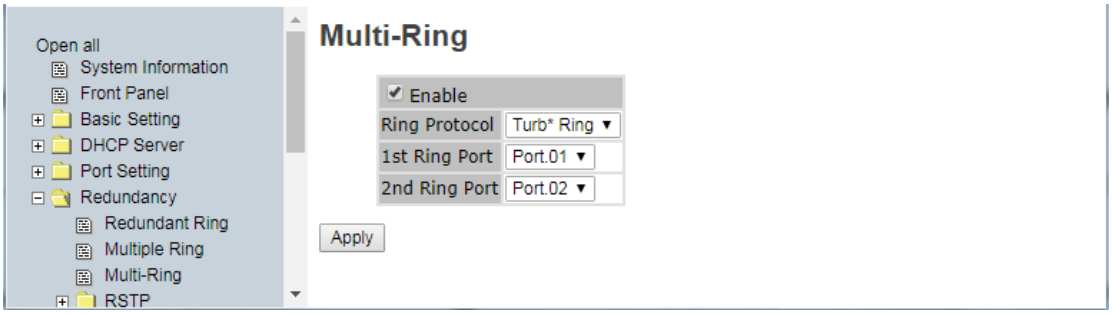


Multiple Ring interface

Label	Description
Enable	Check to Enable the Multiple Ring function.
1st	Choose the first Uplink port.
2nd	Choose the second Uplink port.
Uplink Port	At the dropdown, select the port number(s).
Edge Port	Check the checkbox if the port is to be an Edge Port.
State	The current state of an instance (e.g., *Forwarding*, *Linkdown*).

Multi-Ring

The Redundancy > Multi-Ring menu path displays the Multiple Ring page. Here you can enable and configure Multi-Ring parameters.



Multi-Ring interface

Label	Description
Enable	Check to Enable the Multi-Ring function.
Ring Protocol Turb* Ring Turb* Ring X-Ring MRP Ring	At the drop[down, select the desired Ring protocol: ***Turb* Ring***: Turbo Ring supports three topology options (ring coupling, dual-ring, and dual homing) to reduce redundant network cabling and ensure high reliability. ***X-Ring***: With X-Ring, enable X-Ring on every switch and assign two Member ports in the ring. Set one switch in the X-Ring group as a backup switch that would be blocked (the “backup port”), and assign another port as the “working port”. Other switches are “working switches” and their two member ports are “working ports”. When a network connection fails, the backup port automatically becomes a working port to recovery the failure. ***MRP Ring***: use the Media Redundancy Protocol (MRP) data network protocol standardized by IEC 62439-2.
1st Ring Port	Choose the port which connects to the ring.
2nd Ring Port	Choose the port which connects to the ring.
Apply	Click the “**Apply**” button to activate the configuration.

Message: *Apply fail Another redundancy protocol is running. Only one could be run at the same time*

Meaning: Multiple redundancy protocols are running, which is not supported.

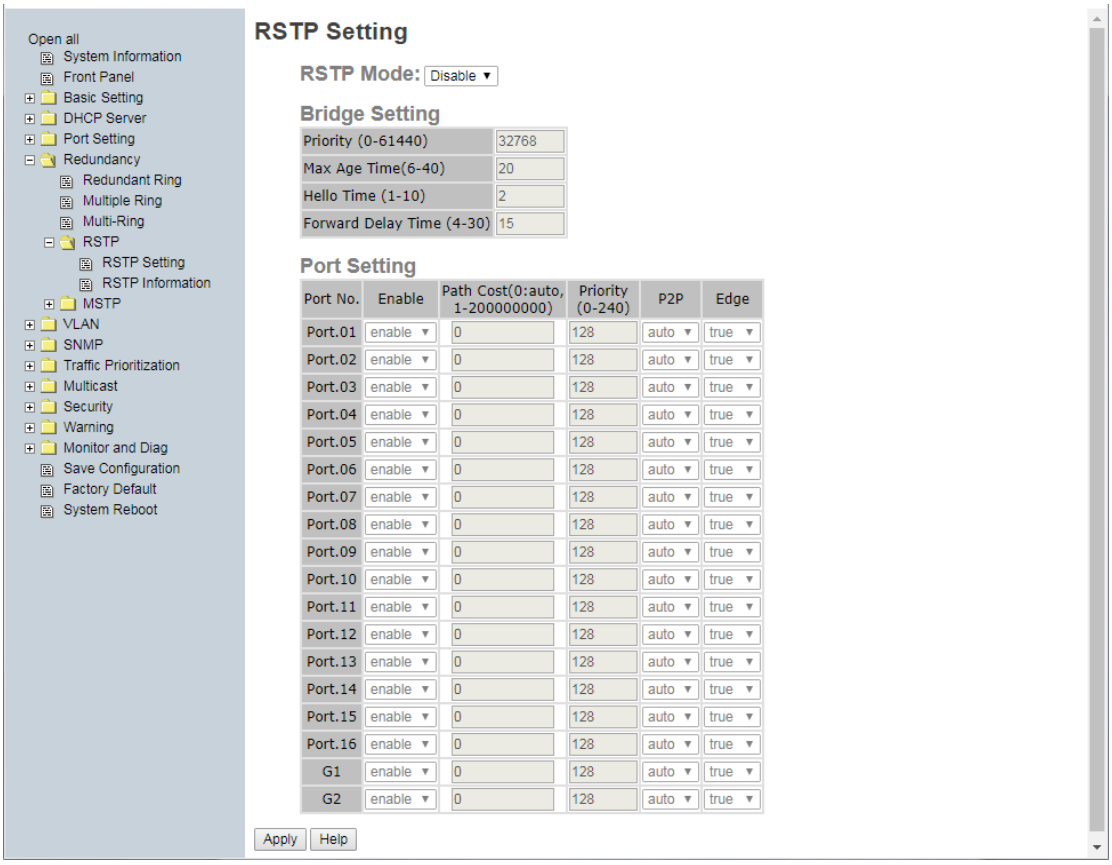
Recovery: Click the Retry button and disable all but one redundancy protocol (Redundant Ring, Multiple Ring, Multi-Ring, RSTP, MSTP).

5.1.7.3 RSTP

The Rapid Spanning Tree Protocol (RSTP) is an evolution of the Spanning Tree Protocol (STP). It provides faster convergence of spanning tree after a topology change. The system also supports STP and the system will detect if the connected device is running STP or RSTP protocol automatically.

RSTP Setting

You can enable/disable RSTP function, and set parameters for each port.



RSTP Setting interface

The following table describes the RSTP Setting screen labels.

Label	Description
RSTP Mode	You must enable the RSTP function before configuring the related parameters.
Priority (0-61440)	A value used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root. If the value changes, you must restart the switch. The Bridge Priority value must be a multiple of 4096 according to the protocol rules.
Max Age Time (6-40)	The number of seconds (6-40) for a bridge to wait without receiving Spanning-tree Protocol configuration messages before reconfiguration.
Hello Time (1-10)	The time interval when a switch sends out the BPDU (Bridge Protocol Data Unit) packet to check RSTP current status. Enter a value of 1 - 10.
Forwarding Delay Time (4-30)	The number of seconds a port waits before changing from its learning/listening state to forwarding state. Enter a value of 4 - 30.

Path Cost (1-200000000)	The cost of the path to the other bridge from this transmitting bridge at the specified port. Enter a number 1 - 200000000.
Priority (0-240)	Decide which port should be blocked by setting the priority in LAN. Enter a number 0 - 240. The Port Priority value must be a multiple of 16.
Admin P2P	Some of the rapid state transactions that are possible within RSTP depend on whether the port can only be connected to exactly one other bridge (i.e., it is served by a point-to-point LAN segment), or it can be connected to two or more bridges (i.e., it is served by a shared medium LAN segment). This function allows the P2P status of the link to be manipulated administratively. **True** means P2P enabled. **False** means P2P disabled.
Admin Edge	The port directly connected to end stations that cannot create a bridging loop in the network. To configure the port as an edge port, set the port to "**True**".
Admin Non STP	The port includes the STP mathematic calculation. **True**: STP algorithm is included, **False**: STP algorithm is not included.
Apply	Click "**Apply**" to activate the configurations.

NOTE: Follow the rule to configure the MAX Age, Hello Time, and Forward Delay Time:

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

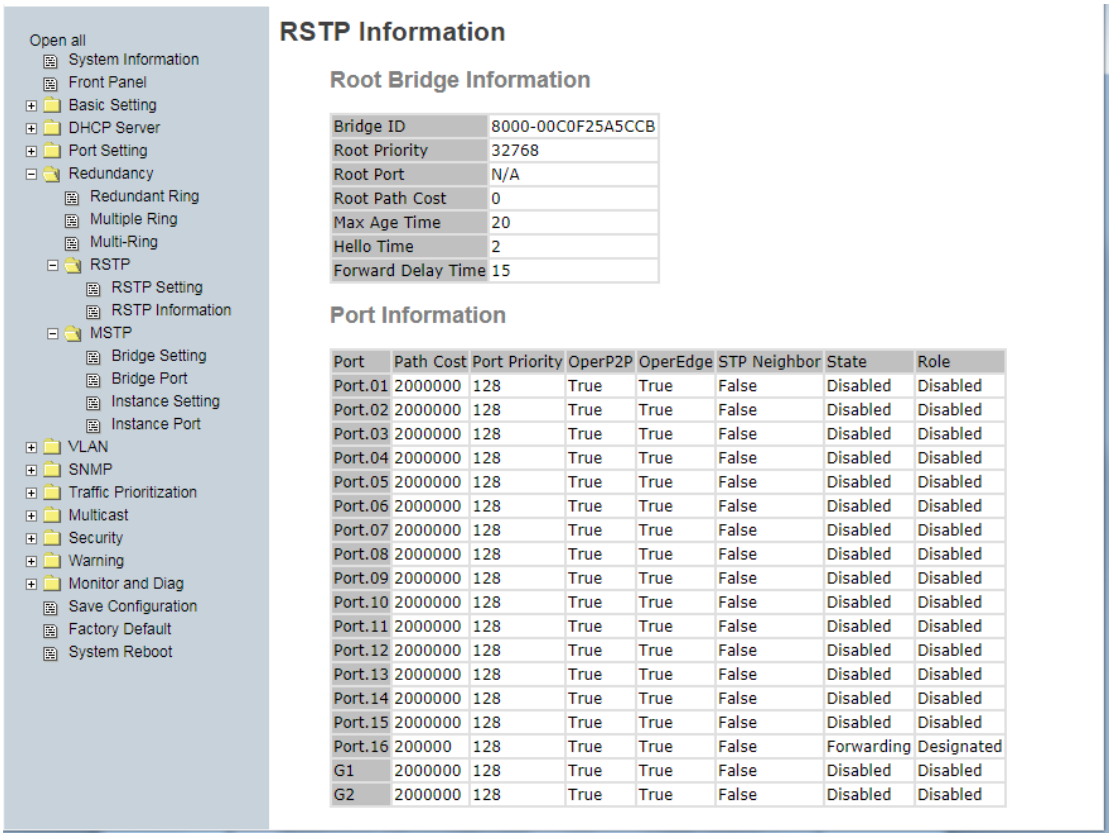
Messages

Bridge priority nust be multiple of 4096

Bridge priority nust be multiple of 4096

RSTP Information

This table shows the RSTP algorithm results.



RSTP Information interface

Label	Description
Root Bridge Information	
Bridge ID	e.g., 8000-00C0F25A5CCB.
Root Priority	e.g., 32768
Root Port	A port number or N/A.
Root Path Cost	e.g., 0
Max Age Time	The number of seconds (6-40) that a bridge waits without receiving Spanning-tree Protocol configuration messages before reconfiguring (e.g., 20 seconds).
Hello Time	The time interval when a switch sends out the BPDU (Bridge Protocol Data Unit) packet to check RSTP current status. A value of 1 - 10.
Forward Delay Time	e.g., 15

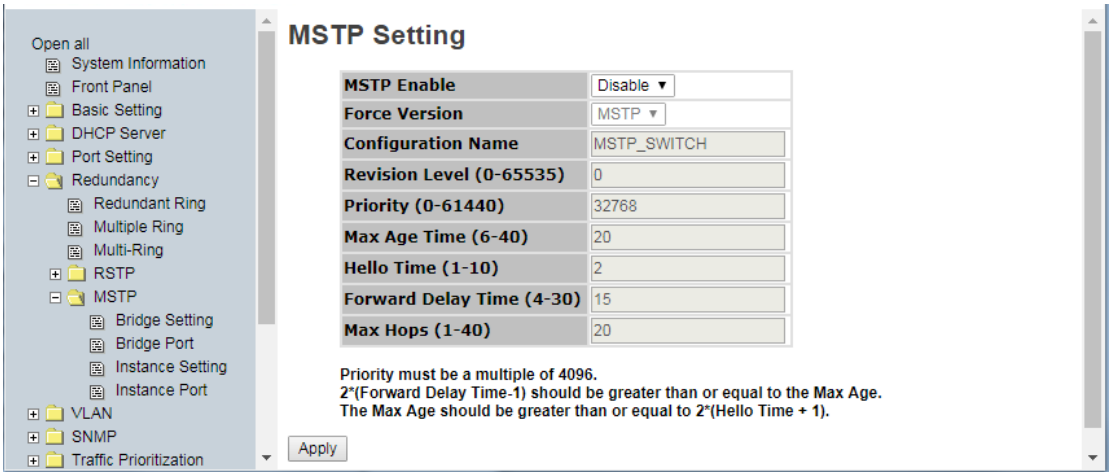
Port Information	
Port	The port number for an instance (row).
Path Cost	The cost of the path to the other bridge from this transmitting bridge at the specified port. Enter a number 1 - 200000000.
Port Priority	Defines which port should be blocked by setting the priority in LAN (a number 0 – 240; a multiple of 16).
OperP2P	True or false.
OperEdge	True or false.
STP Neighbor	True or false.
State	e.g., Disabled, Forwarding, etc.
Role	The RSTP Role (e.g., Designated, Disabled, etc.).

5.1.7.4 MSTP

Multiple Spanning Tree Protocol (MSTP) is a standard protocol based on IEEE 802.1s.

MSTP maps several VLANs to a reduced number of spanning tree instances since most networks do not need more than a few logical topologies. It supports a load balancing scheme and is less CPU intensive than PVST (Cisco proprietary technology).

MSTP > Bridge Setting



MSTP Setting interface

The following table describes the labels in this screen.

Label	Description
MSTP Enable	You must enable or disable MSTP function before configuring the related parameters.
Force Version	The Force Version parameter can be used to force a VLAN Bridge that supports RSTP to operate in an STP-compatible manner (**Stp**, **RSTP**, or **MSTP**).
Configuration Name	The same MST Region must have the same MST configuration name.
Revision Level (0-65535)	The same MST Region must have the same revision level.
Priority (0-61440)	A value used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root. If the value changes, You must reboot the switch. The value must be a multiple of 4096 per the protocol standard rule.

Max Age Time(6-40)	The number of seconds a bridge waits without receiving Spanning-tree Protocol configuration messages before attempting a reconfiguration. Enter a value of 6 - 40.
Hello Time (1-10)	The setting follows the rule below to configure the MAX Age, Hello Time, and Forward Delay Time before a controlled switch sends out the BPDU packet to check RSTP current status. Enter a value of 1 - 10. **2 x (Forward Delay Time value –1) ≥ Max Age value ≥ 2 x (Hello Time value +1)**
Forwarding Delay Time (4-30)	The number of seconds a port waits before changing from its Rapid Spanning-Tree Protocol learning and listening states to the forwarding state. Enter a value of 4 - 30.
Max Hops (1-40)	This parameter is additional to those specified for RSTP. A single value applies to all Spanning Trees within an MST Region (the CIST and all MSTIs) for which the Bridge is the Regional Root.
Apply	Click "**Apply**" to activate the configurations.

Priority must be a multiple of 4096.

2*(Forward Delay Time-1) should be greater than or equal to the Max Age.

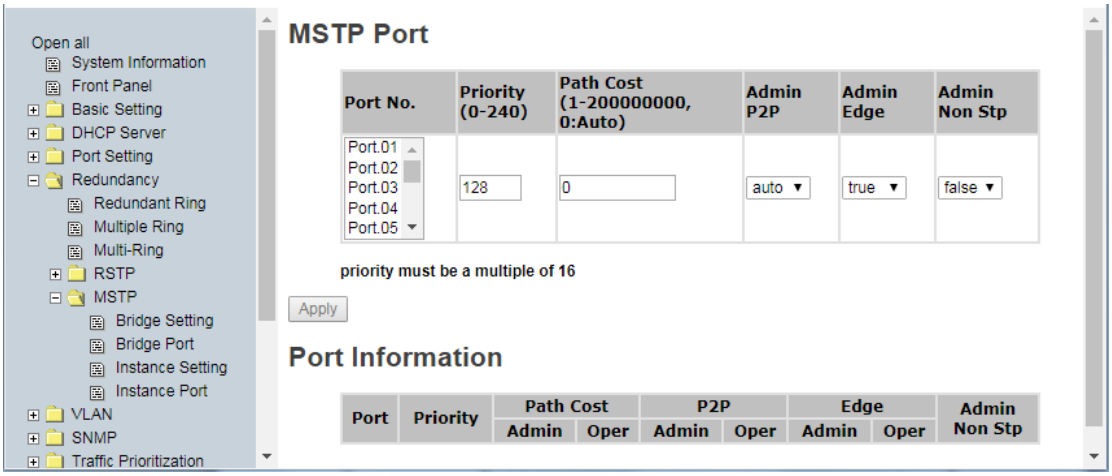
The Max Age should be greater than or equal to 2*(Hello Time + 1).

After the settings are applied, the CIST Root Bridge Information displays:

CIST Root Bridge Information

MAC Address	00C0F2560D51
Priority	32768
Configuration Name	MSTP_SWITCH
Force Version	STP
Revision Level	0
Max Age Time	20
Hello Time	2
Forward Delay Time	15
Max Hops	20
Root Port	N/A
Root Path Cost	0

MSTP > Bridge Port



MSTP Port interface

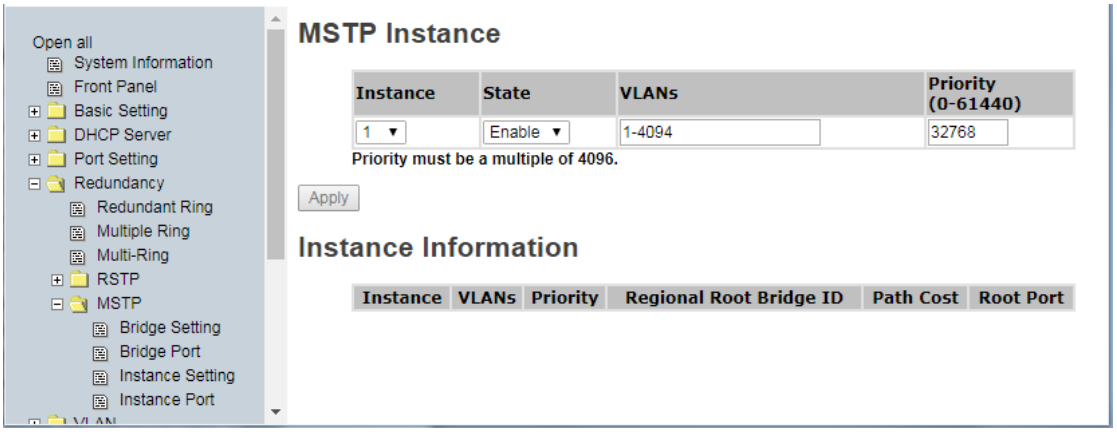
Label	Description
Port No.	Select the port that you want to configure.
Priority (0-240)	Decide which port should be blocked by priority in LAN. Enter a number **0-240**. The value of priority must be a multiple of **16**.
Path Cost (1-200000000, 0:Auto)	The cost of the path to the other bridge from this transmitting bridge at the specified port. Enter a number **1 - 200000000** or **0** for **Auto**.
Admin P2P	Some of the rapid state transactions that are possible within RSTP depend on whether a port can only be connected to exactly one other bridge (i.e., it is served by a point-to-point LAN segment), or it can be connected to two or more bridges (i.e., it is served by a shared medium LAN segment). This function allows the P2P status of the link to be manipulated administratively. ***auto*** means automatically selected. ***true*** means P2P enabled. ***false*** means P2P disabled.
Admin Edge	Controls whether the operEdge flag should start as set (***true***) or cleared (***false***).
Admin Non STP	The port is not STP-capable.
Apply	Click the "**Apply**" button to activate the configuration settings.

After the settings are applied, the CIST Root Bridge Information displays:

Port Information

Port	Priority	Path Cost		P2P		Edge		Admin Non Stp
		Admin	Oper	Admin	Oper	Admin	Oper	
Port.01	128	Auto	200000	Auto	True	True	True	False
Port.02	128	Auto	2000000	Auto	False	True	True	False
Port.03	128	Auto	2000000	Auto	False	True	True	False
Port.04	128	Auto	2000000	Auto	False	True	True	False
Port.05	128	Auto	2000000	Auto	False	True	True	False
Port.06	128	Auto	2000000	Auto	False	True	True	False
Port.07	128	Auto	2000000	Auto	False	True	True	False
Port.08	128	Auto	2000000	Auto	False	True	True	False
Port.09	128	Auto	2000000	Auto	False	True	True	False
Port.10	128	Auto	2000000	Auto	False	True	True	False
Port.11	128	Auto	2000000	Auto	False	True	True	False
Port.12	128	Auto	2000000	Auto	False	True	True	False
Port.13	128	Auto	2000000	Auto	False	True	True	False
Port.14	128	Auto	2000000	Auto	False	True	True	False
Port.15	128	Auto	2000000	Auto	False	True	True	False
Port.16	128	Auto	2000000	Auto	False	True	True	False
G1	128	Auto	2000000	Auto	False	True	True	False
G2	128	Auto	2000000	Auto	False	True	True	False

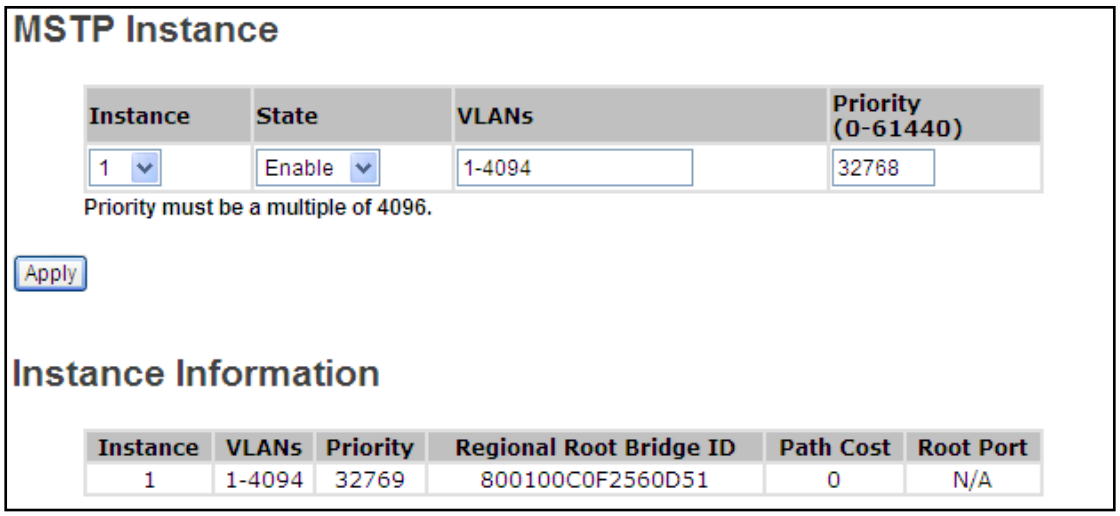
MSTP Instance Config



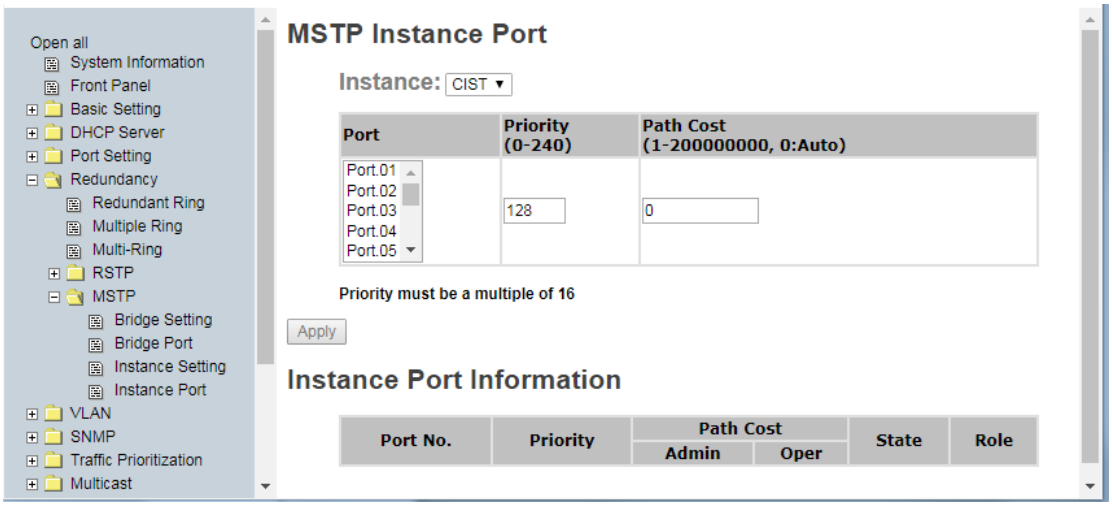
MSTP Instance interface

Label	Description
Instance	Set the instance from **1** to **15**.
State	Enable or disable the instance.
VLANs	Set which VLAN will belong to which instance (1-4094). The MSTP instance VLANs can't overlap.
Priority (0-61440)	A value used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root. If the value changes, You must reboot the switch. The value must be a multiple of 4096 according to the protocol standard rule.
Apply	Click "**Apply**" to activate the configuration settings.

If a VLAN exists and the MSTP Instance config is applied, the Instance Information displays:



MSTP Instance Port Config



MSTP Instance Port interface

Label	Description
Instance	Set the instance's information except CIST.
Port	Select the port that you want to configure.
Priority (0-240)	Select the port to be blocked by priority in LAN. Enter **0** - **240**. The value of priority must be a multiple of **16**.
Path Cost (1-200000000, 0:Auto	The cost of the path to the other bridge from this transmitting bridge at the specified port. Enter a number **1** - **200000000** or **0** for **Auto**.
Apply	Click the "**Apply**" button to set the configurations.

Message: *Apply fail - Another redundancy protocol is running. Only one could be run at the same time*

Meaning: Multiple redundancy protocols are running, which is not supported.

Recovery: Click the Retry button and disable all but one redundancy protocol (Redundant Ring, Multiple Ring, Multi-Ring, RSTP, MSTP).

After the settings are applied, the Instance Port Information displays:

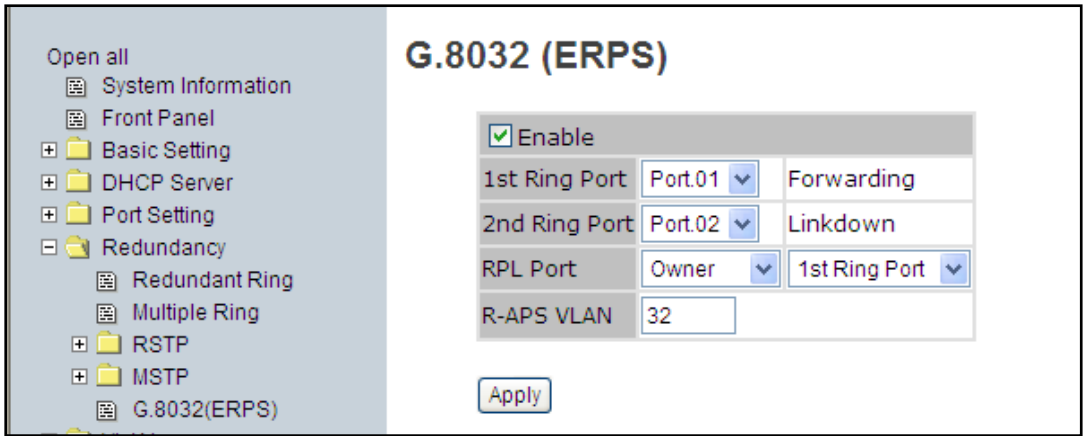
Instance Port Information

Port No.	Priority	Path Cost		State	Role
		Admin	Oper		
Port.01	128	Auto	200000	Forwarding	DesignatedPort
Port.02	128	Auto	2000000	Disabled	DisabledPort
Port.03	128	Auto	2000000	Disabled	DisabledPort
Port.04	128	Auto	2000000	Disabled	DisabledPort
Port.05	128	Auto	2000000	Disabled	DisabledPort
Port.06	128	Auto	2000000	Disabled	DisabledPort
Port.07	128	Auto	2000000	Disabled	DisabledPort
Port.08	128	Auto	2000000	Disabled	DisabledPort
Port.09	128	Auto	2000000	Disabled	DisabledPort
Port.10	128	Auto	2000000	Disabled	DisabledPort
Port.11	128	Auto	2000000	Disabled	DisabledPort
Port.12	128	Auto	2000000	Disabled	DisabledPort
Port.13	128	Auto	2000000	Disabled	DisabledPort
Port.14	128	Auto	2000000	Disabled	DisabledPort
Port.15	128	Auto	2000000	Disabled	DisabledPort
Port.16	128	Auto	2000000	Disabled	DisabledPort
G1	128	Auto	2000000	Disabled	DisabledPort
G2	128	Auto	2000000	Disabled	DisabledPort

5.1.7.5 G.8032 (ERPS)

Recommendation ITU-T G.8032/Y.1344 defines the automatic protection switching (APS) protocol and protection switching mechanisms for ETH layer Ethernet ring topologies. Included are details pertaining to Ethernet ring protection characteristics, architectures, and the ring APS (R-APS) protocol. This Recommendation defines the automatic protection switching (APS) protocol and protection switching mechanisms for ETH layer Ethernet ring topologies.

The protection protocol defined in the Recommendation enables protected point-to-point, point-to-multipoint and multipoint-to multipoint connectivity within a ring or interconnected rings. For the ITU Recommendation ITU-T G.8032/Y.1344 that describes Ethernet ring protection switching see http://www.itu.int/rec/T-REC-G.8032/en.



G.8032 (ERPS) interface

Label	Description
Enable	
1st Ring Port	Select a Port at the dropdown (Portx, G1, or G2) and view the status (e.g., *Forwarding*, *Linkdown*).
2nd Ring Port	Select a Port at the dropdown (Portx, G1, or G2) and view the status (e.g., *Forwarding*, *Linkdown*).
RPL Port	At the dropdown select **None**, **Owner**, or **Neighbor** for the RPL (Ring Protection Link).
R-APS VLAN	Enter the related VLAN ID (VID) for the R-APS (Ring APS) port.
Apply	Click the "**Apply**" button to set the configurations.

G.8032 uses standard 802.1 MAC, OAM frames and 802.1Q tagging. Using standard components reduces the cost and complexity of the solution and makes interoperability with other existing Ethernet solutions easier. Since G.8032 was specifically developed for use in a ring architecture, a procedure to prevent loops is very-straightforward; only one port on the ring needs to be blocked. This is why Spanning Tree Protocol is not required.

5.1.8 VLAN

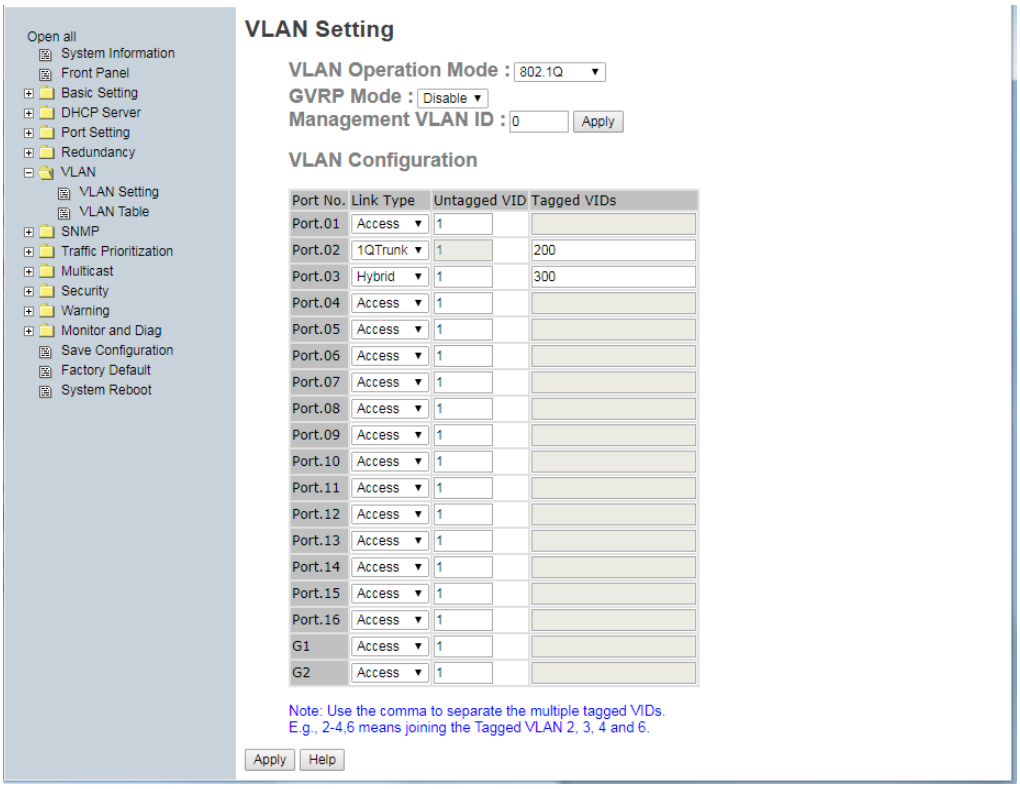
A Virtual LAN (VLAN) is a logical network grouping that limits the broadcast domain, which allows you to isolate network traffic. Only the members of the same VLAN will receive the traffic from the other members. Basically, to create a VLAN from a switch is logically equivalent to separating a group of network devices. However, all the network devices are still plugged into the same switch physically. This switch supports port-based and 802.1Q (tagged-based) VLAN. The default configuration of VLAN operation mode is at "**802.1Q**".

5.1.8.1 VLAN Setting

Tagged-based VLAN is an IEEE 802.1Q specification standard, and it is possible to create a VLAN across devices from different switch venders. IEEE 802.1Q VLAN uses a technique to insert a "tag" into the Ethernet frames. Tag contains a VLAN Identifier (VID) that indicates the VLAN numbers.

You can create Tag-based VLAN and enable or disable GVRP protocol. There are 256 VLAN groups available. Enable 802.1Q VLAN, all ports on the switch belong to default VLAN (VID 1). The default VLAN cannot be deleted.

GVRP allows automatic VLAN configuration between the switch and nodes. If the switch is connected to a device with GVRP enabled, you can send a GVRP request by using the VID of a VLAN defined on the switch; the switch will automatically add that device to the existing VLAN.



VLAN Configuration – 802.1Q interface

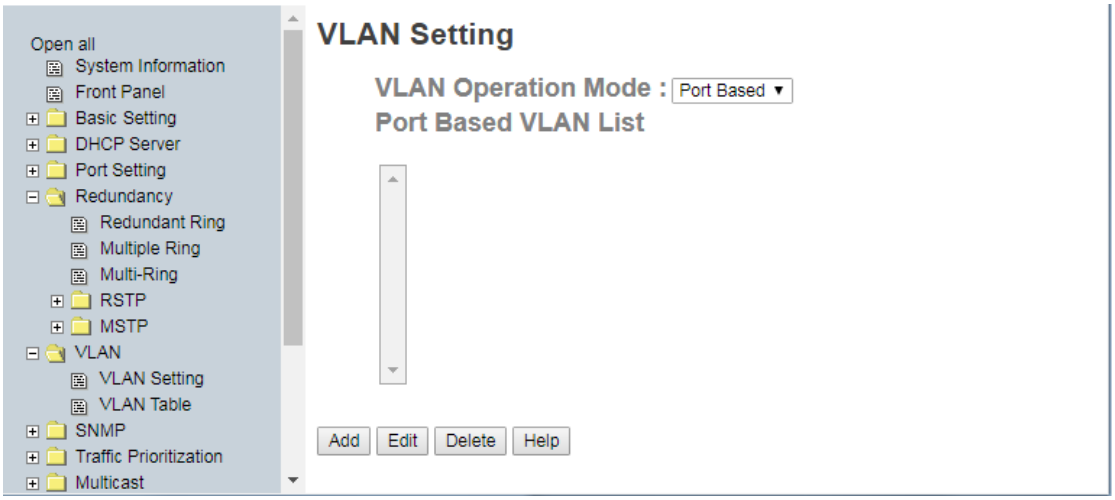
The following table describes the 802.1Q VLAN labels on this screen. Note that ports with the same VID means that they are in the same VLAN group.

Label	Description
VLAN Operation	Configure VLAN Operation Mode: **Disable**, **Port Based**, or **802.1Q**.

Mode	
GVRP Mode	Enable or Disable the GVRP function globally. GVRP enabled allows automatic VLAN configuration between the switch and nodes.
Management VLAN ID	Management VLAN provides network administrators a secured VLAN for switch management. Only the devices in the Management VLAN can access the switch. Zero (0) means this function is disabled.
Link Type	The available Link Types are: ***Access*:** single switch only; allows you to group ports by setting the same VID. The Access link only supports an untagged VID. ***1QTrunk*:** extended application of **Access** Link, allows you to group ports by setting the same VID with 2 or more switches. The 1Q Trunk link only supports multiple tagged VIDs. ***Hybrid*:** Both **Access Link** and **Trunk Link** are available. The Hybrid link supports an untagged VID and multiple tagged VIDs.
Untagged VID	Set the port default VLAN ID for untagged devices that connect to the port. The range is **1** - **4094**.
Tagged VIDs	Set the tagged VIDs to carry different VLAN frames to the other switch. Tagged VIDs support 1~4094 and multiple VIDs. Use the comma to separate the multiple tagged VIDs (e.g., 2,3,4 means joining the Tagged VLAN 2,3 and 4).
Apply	Click the "**Apply**" button to activate the configurations.

5.1.8.2 VLAN Setting – Port Based

Packets can go among only members of the same VLAN group. Note all unselected ports are treated as belonging to another single VLAN. If the port-based VLAN is enabled, the VLAN-tagging is ignored.



VLAN Configuration – Port Based interface-1

The following table describes the labels in this screen.

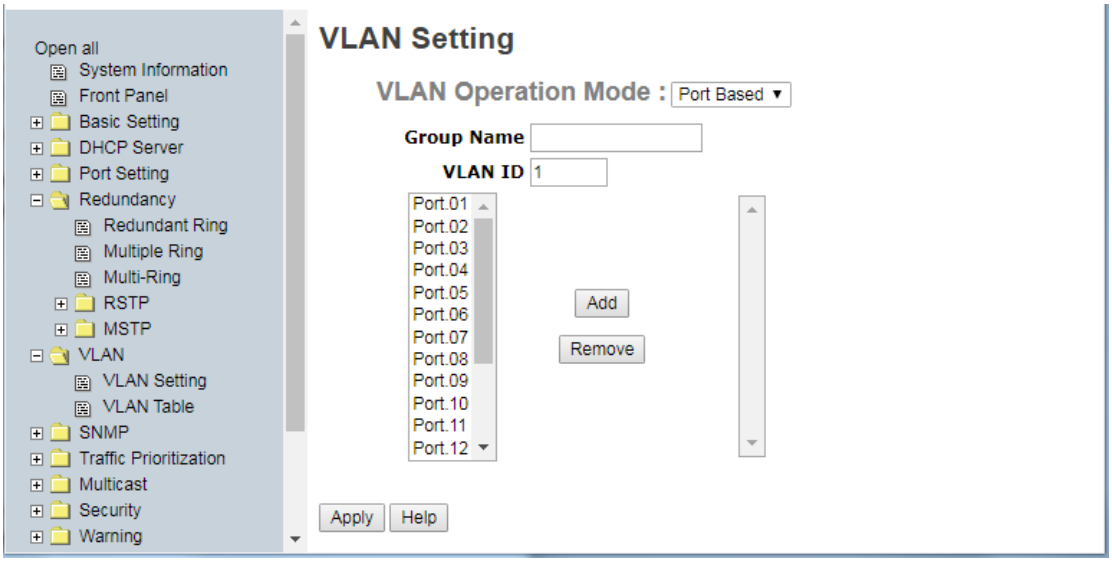
Label	Description
Add	Click "**Add**" to enter a VLAN add interface. See below.
Edit	Edit exist VLAN.
Delete	Delete exist VLAN.
Help	Show help file.

Port-based VLAN

Traffic is forwarded to the member ports of the same VLAN Group. To create a VLAN and add member ports to it:

1. Click the **Add** button.
2. Type a name for the new VLAN.
3. Type a VID (VLAN ID, 1-4094).
4. From the **Available ports** box, select ports to add to the switch and click the **Add** button.
5. Click the **Apply** button.

Click the **Add** button to continue configuration.



VLAN Configuration – Port Base interface-2

The following table describes the labels in this screen.

Label	Description
VLAN Operation Mode	The VLAN Operation Mode: **Disable**, **Port Based**, or **802.1Q**.
Group Name	VLAN group name.
VLAN ID	Specify the VLAN ID (VID).
Add	Select the port(s) to join the VLAN group.
Remove	Remove ports from the VLAN group.
Apply	Click "**Apply**" to activate the configurations.
Help	Show the online help file.

Messages:

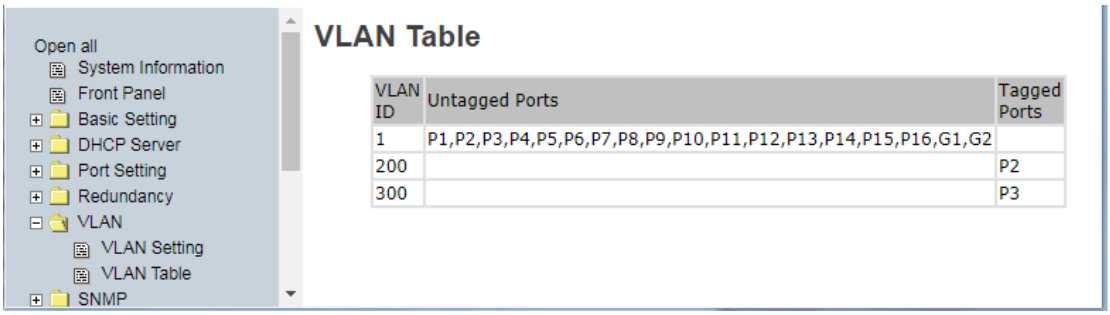
Message: *Please Select VLAN Port.*

Message: *Apply fail The VLAN name or VLAN ID has exist*

Message: *Apply fail Wrong port selection*

5.1.8.3 VLAN Table

The VLAN Table displays VLAN settings made.



VLAN Configuration – Port Base interface-2

The following table describes the labels in this screen.

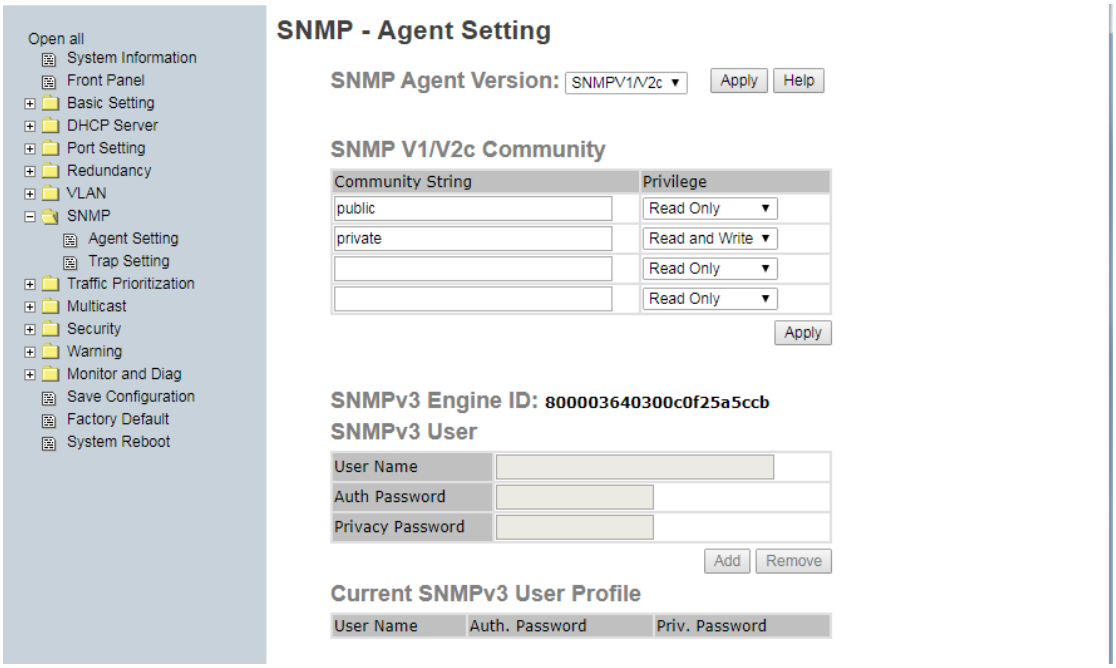
Label	Description
VLAN ID	Displays the VLAN IDs (VIDs).
Untagged Ports	Lists the set of un-tagged ports for each VLAN ID (VID).
Tagged Ports	Lists the set of tagged ports for each VLAN ID (VID).

5.1.9 SNMP

Simple Network Management Protocol (SNMP) is the protocol developed to manage nodes (servers, workstations, routers, switches and hubs etc.) on an IP network. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth. Network management systems learn of problems by receiving traps or change notices from network devices implementing SNMP.

5.1.9.1 SNMP – Agent Setting

You can set the SNMP agent related information with the Agent Setting Function.



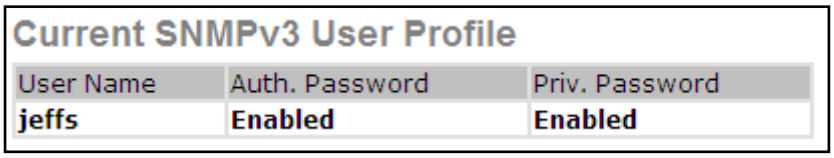
SNMP Agent Setting interface

The following table describes the labels in this screen.

Label	Description
SNMP Agent Version	Three SNMP versions are supported (SNMP v1, SNMP V1/ V2c, and SNMP V3). The SNMP V1/ V2c agent uses a community string match for authentication, which means SNMP servers access objects with read-only or read/write permissions with the community default string public/private. SNMP V3 requires an authentication level of MD5 or DES to encrypt data to enhance data security.

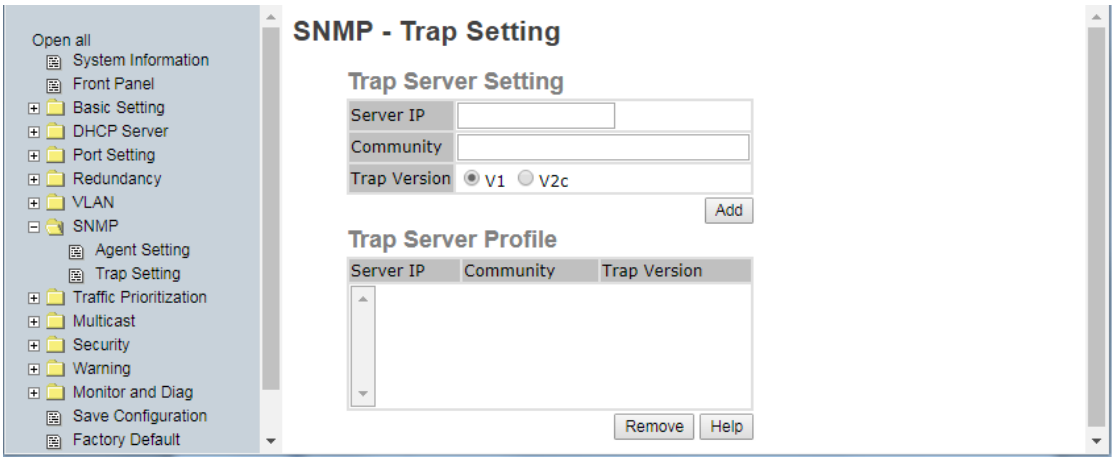
SNMP V1/V2c Community String	SNMP Community should be set for SNMP V1/V2c. Four sets of "Community String/Privilege" are supported. Each Community String can have up to 32 characters. Keep empty to remove this Community string.
SNMP V1/V2c Community Privilege	Select **Read Only** or **Read and Write** privilege level for each Community String.
SNMPv3User	If SNMP V3 agent is selected, the SNMPv3 you profiled should be set for authentication. The User Name is required. The Auth Password is encrypted by MD5 and the Privacy Password which is encrypted by DES. You can have up to 8 sets of SNMPv3 Users and up to 16 characters in the Username, and Password. When the **SNMP V3** agent is selected, you can: 1. Input SNMPv3 User Name only. 2. Input SNMPv3 User Name and Auth Password. 3. Input SNMPv3 User Name, Auth Password, and Privacy Password, which can be different from Auth Password. To remove a current user profile: 1. Input the SNMPv3 user name you want to remove. 2. Click "**Remove**" button
Current SNMPv3 User Profile	Show all SNMPv3 user profiles.
Apply	Click "**Apply**" to activate the configurations.
Add / Remove	Click to add or remove a selected SNMPv3User instance.
Help	Show the online help file.

Current SNMPv3 User Profile Example:



5.1.9.2 SNMP – Trap Setting

A trap manager is a management station that receives traps, the system alerts generated by the switch. If no trap manager is defined, no traps will be issued. Create a trap manager by entering the IP address of the station and a community string. Selects the SNMP version and click the Add button.

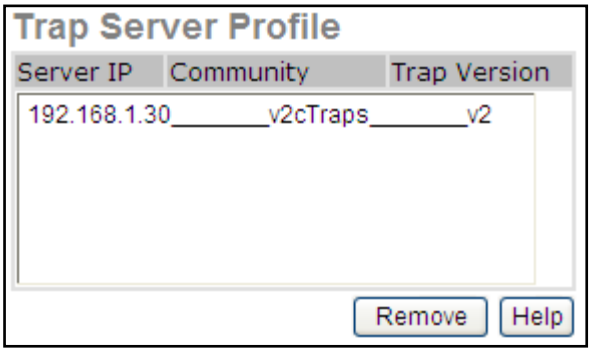


SNMP Trap Setting interface

The following table describes the labels in this screen.

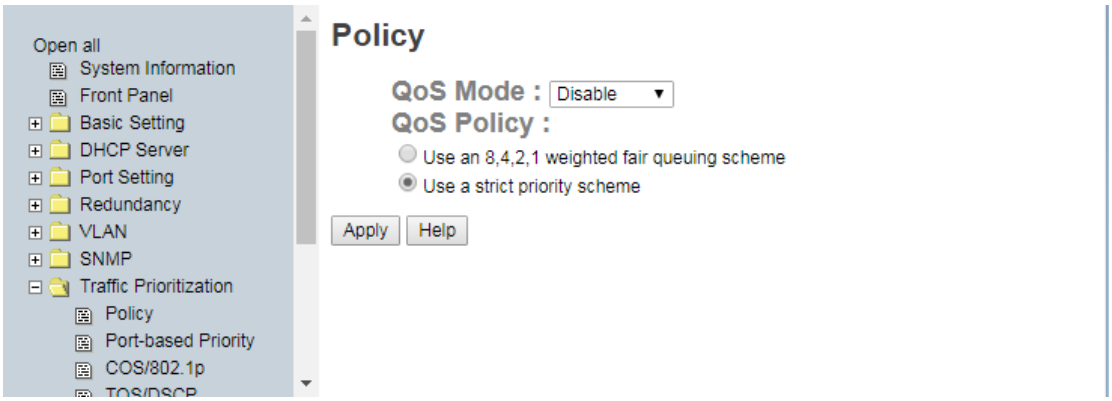
Label	Description
Server IP	The server IP address to receive Traps.
Community	Community for authentication.
Trap Version	Trap Version supports **V1** and **V2c**.
Add	Click to add a Trap Server Profile.
Remove	Click to remove an existing Trap Server Profile.
Help	Show the online help file.

Current SNMPv3 User Profile Example:



5.1.10 Traffic Prioritization

Traffic Prioritization includes three modes: Port-based, 802.1p/COS, and TOS/DSCP. You can use the traffic prioritization function to classify the traffic into four classes for different network applications. The SISTM1040-262D-LRT-B supports four priority queues.

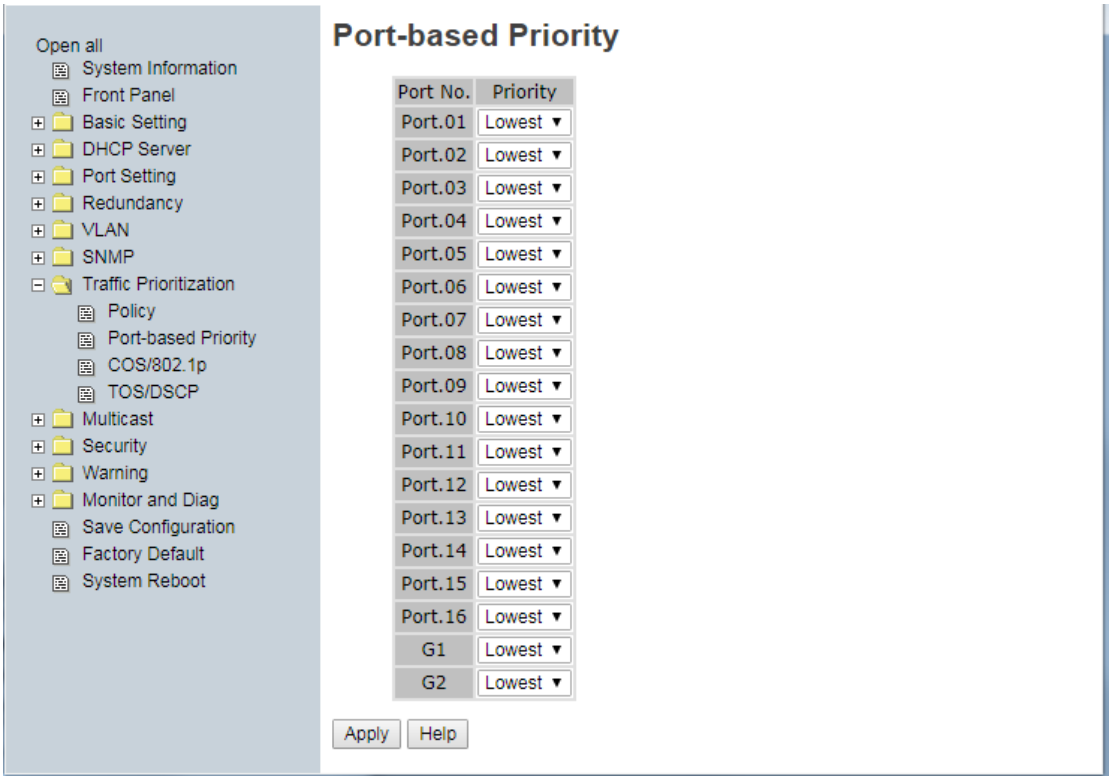


Policy Setting interface

Label	Description
QoS Mode Disable Port-based COS only TOS only COS first TOS first	**Port-based:** the output priority is determined by ingress port. **COS only:** the output priority is determined by COS only. **TOS only:** the output priority is determined by TOS only. **COS first:** the output priority is determined by COS and TOS, but COS first. **TOS first:** the output priority is determined by COS and TOS, but TOS first.
QoS policy	**Use an 8,4,2,1 weight fair queuing scheme:** the output queues will follow 8:4:2:1 ratio to transmit packets from the highest to lowest queue. Example: 8 high queue packets, 4 middle queue packets, 2 low queue packets, and the one lowest queue packets are transmitted in one turn. **Use a strict priority scheme:** always transmit the packets in the higher queue first until the higher queue is empty.
Help	Show the online help file.
Apply	Click "**Apply**" to activate the configuration settings.

Port-based Priority interface

Here you can assign each port with a priority queue. Four priority queues can be assigned: **High**, **Middle**, **Low**, and **Lowest**.

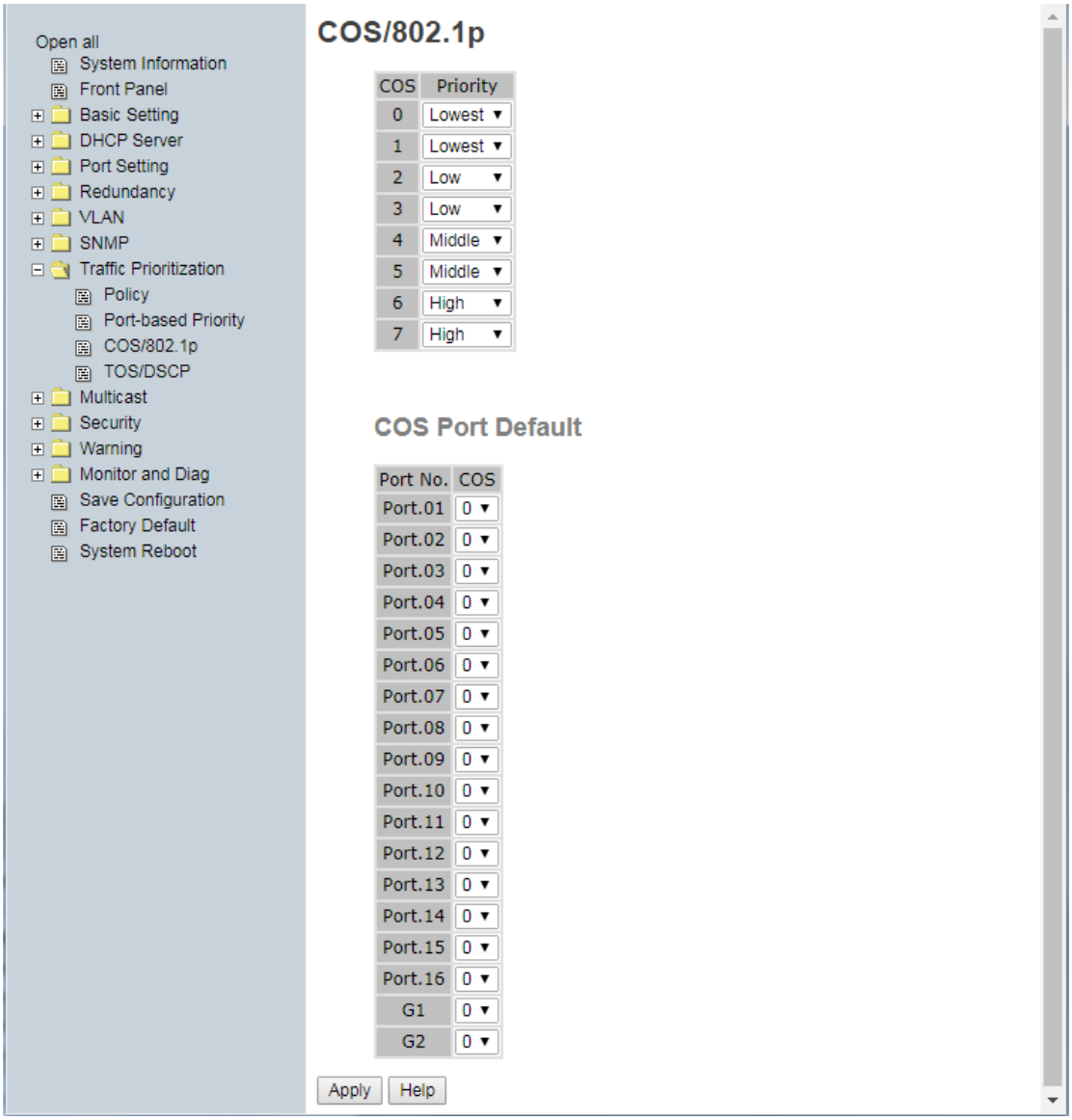


Port-based Priority interface

Label	Description
Priority	At the dropdown, for each port, select one of the four priority queues that can be assigned: **High**, **Middle**, **Low**, and **Lowest**.
Apply	Click "**Apply**" to activate the configurations. Save changes by clicking **Save** at the Save Configuration menu option.
Help	Show the online help file.

Messages: *Apply fail - This priority setting is not supported in current QoS mode*

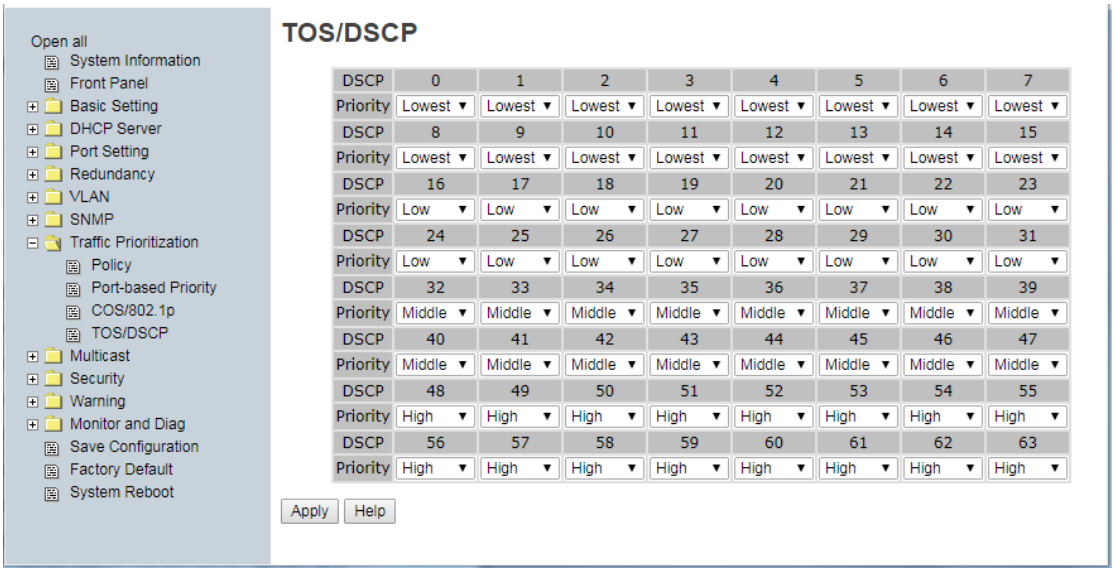
COS/802.1p interface



COS/802.1p interface

Label	Description
COS/802.1p	COS (Class Of Service) is known as 802.1p. It describes that the output priority of a packet is determined by the user priority field in a 802.1Q VLAN tag. The priority values 0 - 7 are supported. COS value maps to four priority queues: **High**, **Middle**, **Low**, and **Lowest**.
COS Port Default	When an ingress packet has no VLAN tag, a default priority value is considered and determined by the ingress port.
Apply	Click "**Apply**" to activate the configurations. Save changes by clicking **Save** at the Save Configuration menu option.
Help	Show help file.

TOS/DSCP interface



TOS/DSCP interface

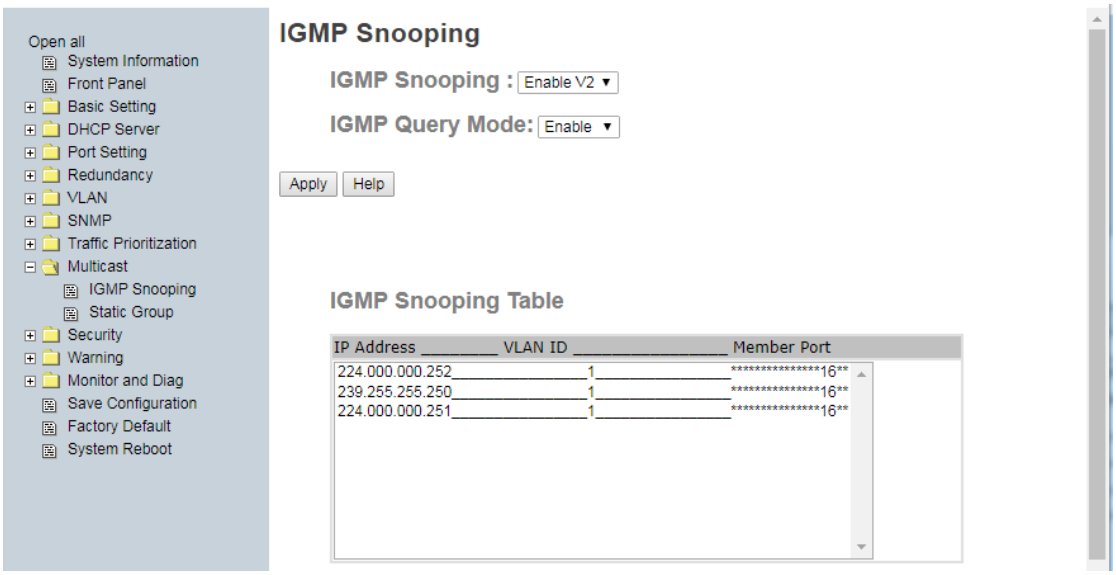
Label	Description
TOS/DSCP Priority	TOS (Type of Service) is a field in the IP header of a packet. This TOS field is also used by Differentiated Services and is called the Differentiated Services Code Point (DSCP). The output priority of a packet can be determined by this field and priority values 0 - 63 are supported. DSCP value maps to four priority queues: **High**, **Middle**, **Low**, and **Lowest**.
Apply	Click "**Apply**" to activate the configuration settings. Save changes by clicking **Save** at the Save Configuration menu option.
Help	Show the online help file.

Messages: *Apply fail - Table full*

5.1.11 Multicast

5.1.11.1 IGMP Snooping

Internet Group Management Protocol (IGMP) is used by IP hosts to register their dynamic multicast group membership. IGMP has 3 versions, IGMP v1, v2m and v3. Refer to IETF RFCs 1112, 2236 and 3376. IGMP Snooping improves the performance of networks that carry multicast traffic. It provides the ability to prune multicast traffic so that it travels only to those end destinations that require that traffic and reduces the amount of traffic on the Ethernet LAN.



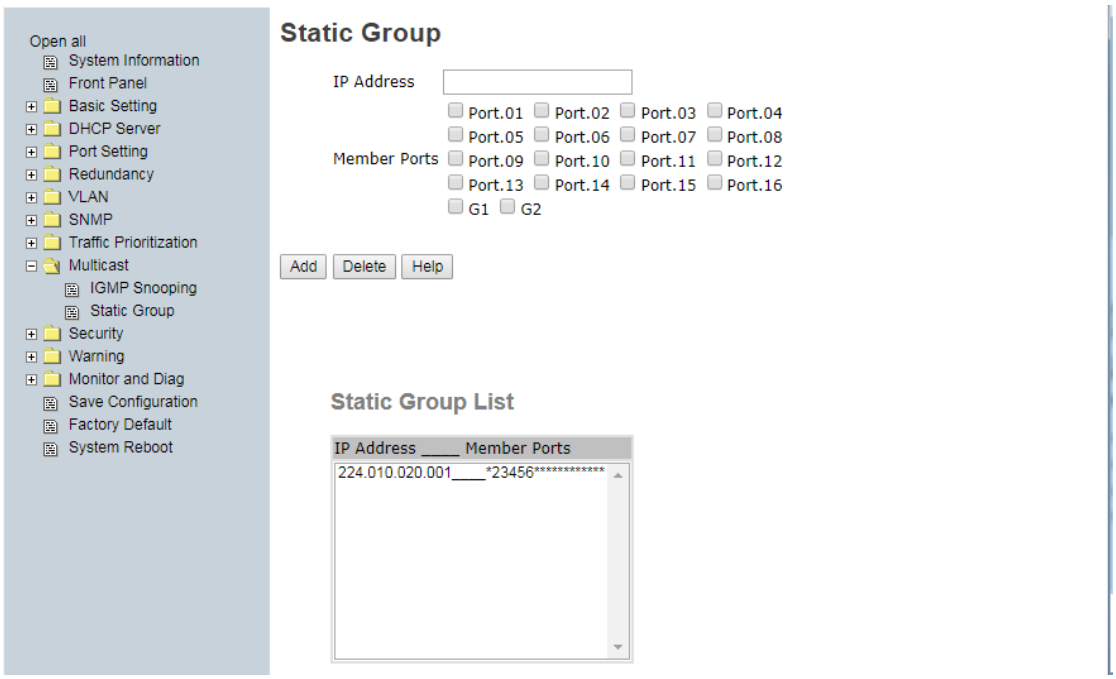
IGMP Snooping interface

The following table describes the labels in this screen.

Label	Description
IGMP Snooping	Enable/Disable IGMP snooping.
IGMP Query Mode	Switch will be IGMP querier or not. There should exist one and only one IGMP querier in an IGMP application. The "**Auto**" mode means that the querier is the one with lower IP address.
IGMP Snooping Table	Shows the current IP multicast list.
Apply	Click "**Apply**" to activate the configurations.
Help	Show the online help file.

5.1.11.2 Static Group List

Multicasts are like broadcasts; they are sent to all end stations on a LAN or VLAN. Static Group is the system by which end stations only receive multicast traffic if they register to join specific multicast groups. With Static Group, network devices only forward multicast traffic to the ports that are connected to registered end stations.



Multicast Filtering interface

The following table describes the labels in this screen.

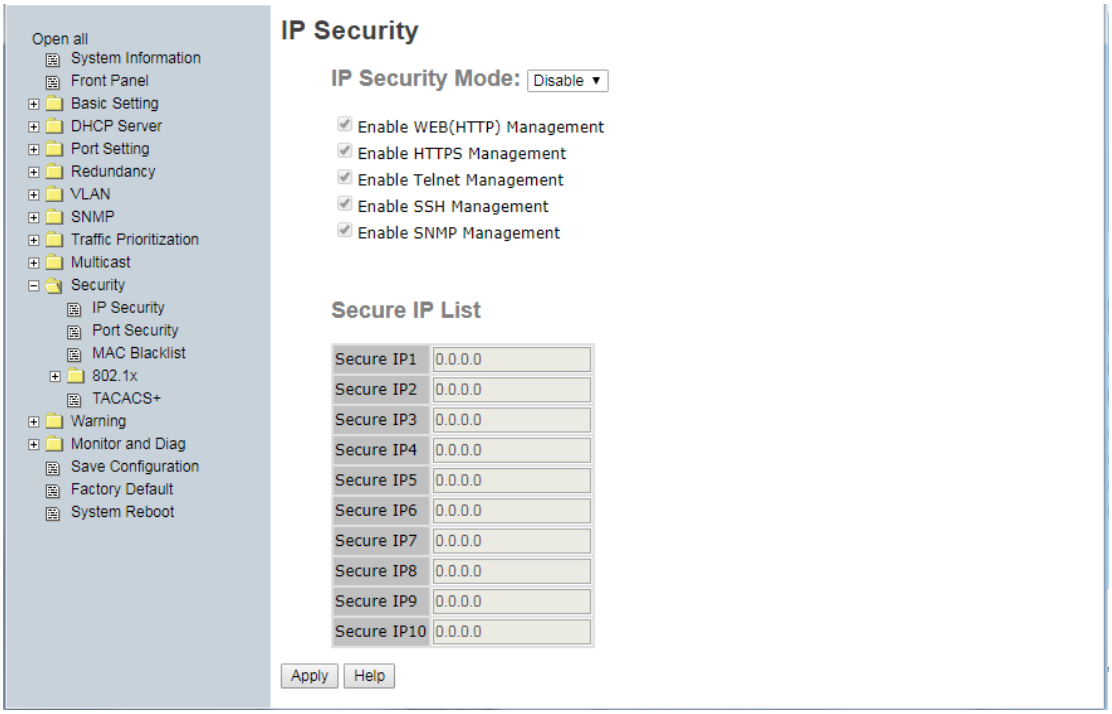
Label	Description
IP Address	Assign a multicast group IP address in the range of 224.0.0.0 ~ 239.255.255.255.
Member Ports	Tick the check box beside the port number to include it as a member port in the specific multicast group IP address.
Add	Show current IP multicast list.
Delete	Delete a selected entry from table.
Help	Show the online help file.

5.1.12 Security

These five functions can enhance security of the switch: IP Security, Port Security, MAC Blacklist, and MAC address Aging and 802.1x protocol.

5.1.12.1 IP Security

IP Security can enable/disable remote management via WEB (HTTP), HTTPS, Telnet, SSH, or SNMP. Additionally, IP security can restrict remote management to some specific IP addresses. Only these secure IP addresses can manage this switch remotely.



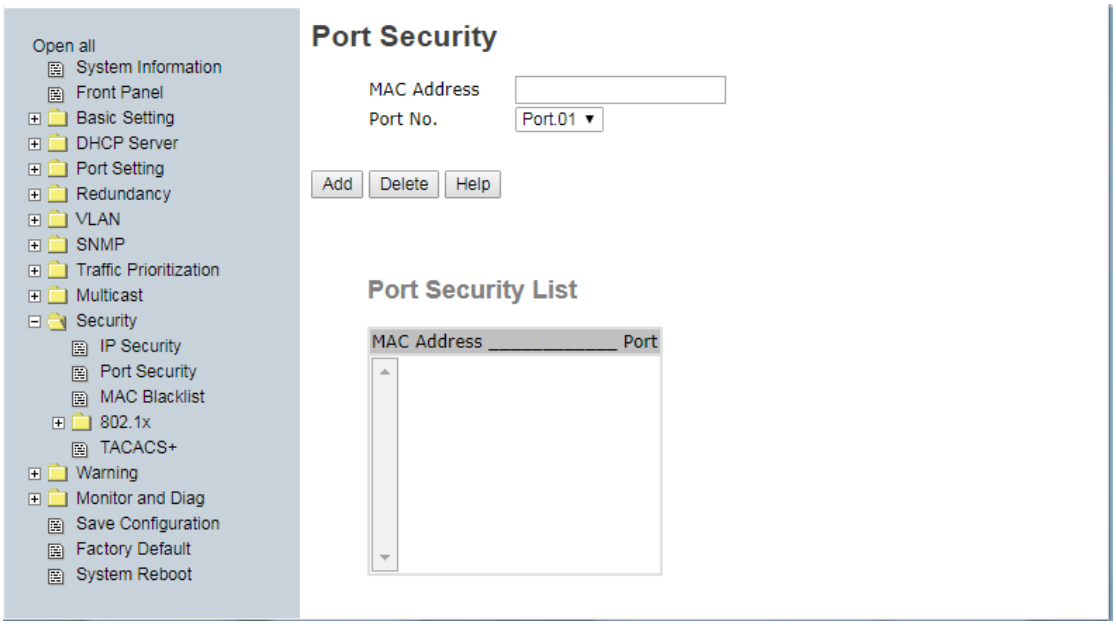
IP Security interface

The following table describes the labels in this screen.

Label	Description
IP Security Mode	Enable/Disable the IP Security function globally.
Enable WEB(HTTP) Management	Tick the check box to enable WEB Management.
Enable HTTPS Management	Tick the check box to enable HTTPS secure WEB Management.
Enable Telnet Management	Tick the check box to enable Telnet Management.
Enable SSH Management	Tick the check box to enable SSH secure WEB Management.
Enable SNMP Management	Tick the check box to enable SNMP Management.
Secure IP List	Enter IP addresses; restrict remote management to some specific IP addresses.
Apply	Click “**Apply**” to activate the configurations.
Help	Show the help file for this page.

5.1.12.2 Port Security

Port security is used to add static MAC addresses to the hardware forwarding database. If port security is enabled at **Port Control** page, only the frames with MAC addresses in this list will be forwarded, otherwise they will be discarded.



Port Security interface

The following table describes the labels in this screen.

Label	Description
MAC Address	Input a MAC Address to a specific port.
Port No.	Select a switch port from the dropdown.
Add	Click to add an entry of MAC and port information to the list.
Delete	Delete an existing entry from the list.
Help	Show the online help file.

To add a static MAC address

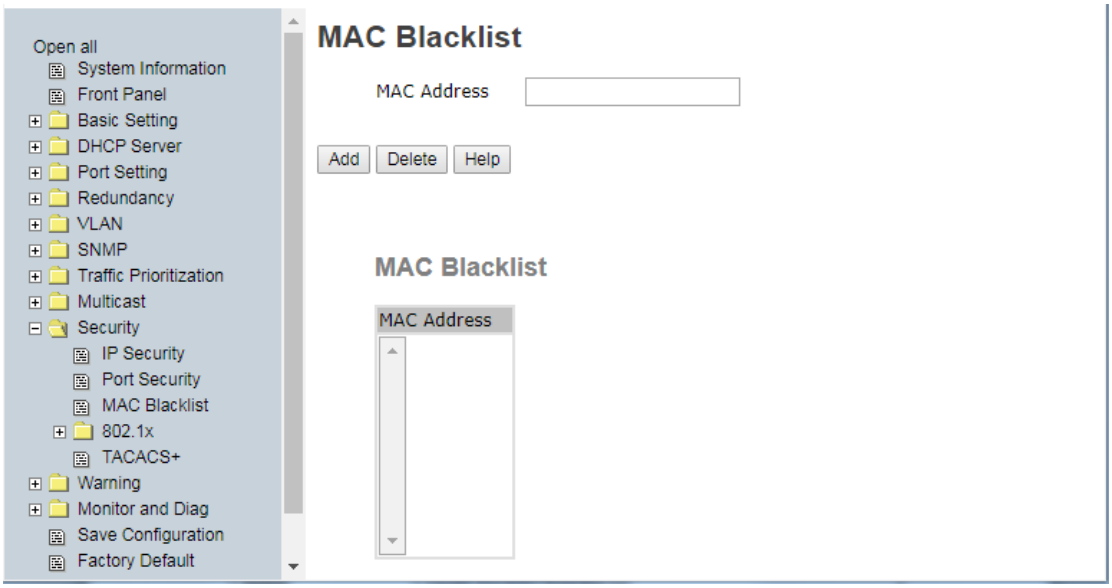
1. In the MAC address box, enter a MAC address, e.g. "**001122334455**".
2. In the Port Number box, select a port number.
3. Click the **Add** button.

To delete a static MAC address

1. In the MAC address box, enter a MAC address.
2. Click the **Delete** button.

5.1.12.3 MAC Blacklist

The MAC Blacklist can eliminate the traffic forwarding to specific MAC addresses in the list. Any frames forwarding to MAC addresses in this list will be discarded. Thus the target device will never receive any frame.



MAC Blacklist interface

The following table describes the labels in this screen.

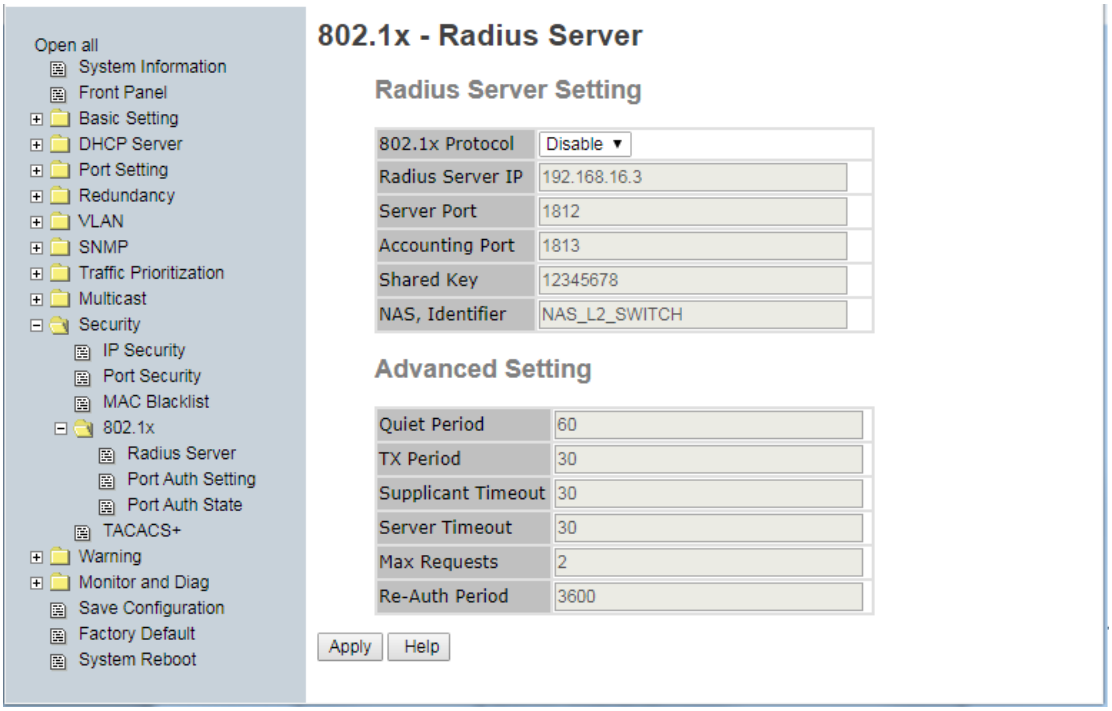
Label	Description
MAC Address	Input MAC Address to add to the MAC Blacklist (e.g. "001122334455".).
Add	Add an entry to Blacklist table.
Delete	Delete the entry from the list.
Help	Show the online help file.

Messages: *Apply fail - Entry existed and can't be modified*

5.1.12.4 802.1x

802.1x - Radius Server

IEEE 802.1x uses the physical access characteristics of IEEE802 LAN infrastructures to provide an authenticated and authorized device attached to a LAN port. Refer to IEEE 802.1X - Port Based Network Access Control for more information.



802.1x Radius Server interface

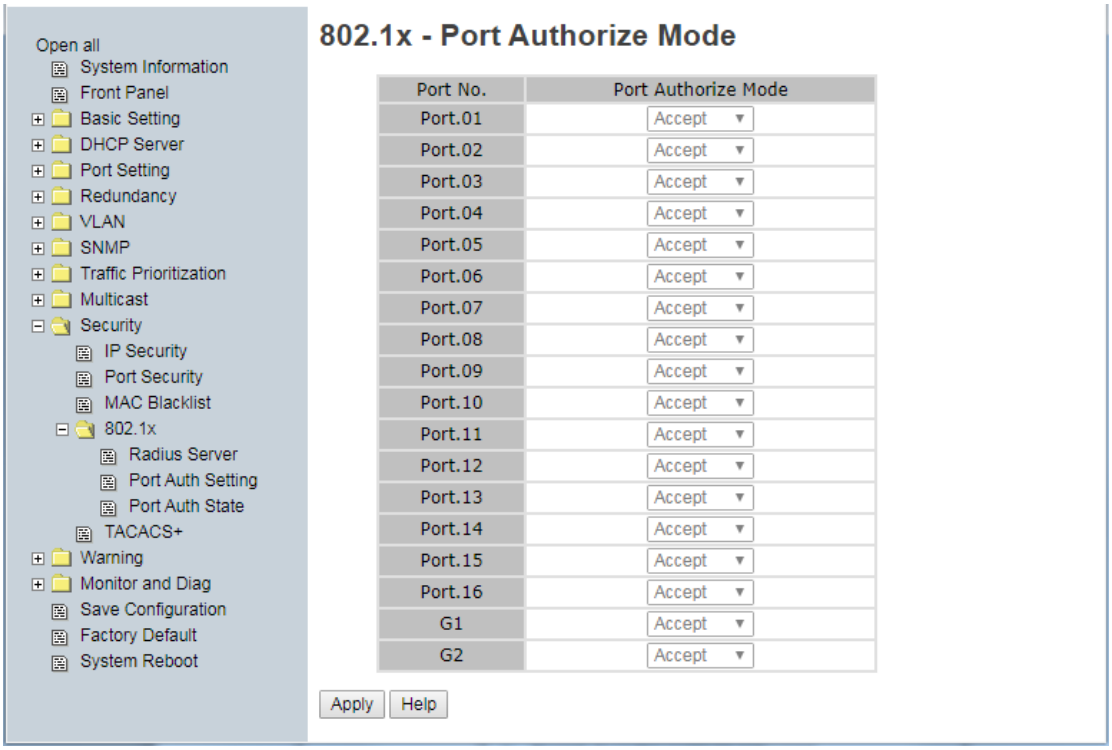
The following table describes the labels in this screen.

Label	Description
Radius Server Setting	
802.1X Protocol	Enable or Disable RADIUS at the dropdown.
Radius Server IP	The IP address of the authentication server.
Server Port	Set the UDP port number used by the authentication server to authenticate.
Accounting Port	Set the UDP destination port for accounting requests to the specified Radius Server.
Shared Key	A key shared between this switch and authentication server.
NAS, Identifier	A string used to identify this switch.

Advanced Setting	
Quiet Period	Set the time interval between authentication failure and the start of a new authentication attempt. The Quiet Period is the period of time during which it will not attempt to acquire a supplicant. The default time is 60 seconds.
Tx Period	Set the time that the switch can wait for response to an EAP request/identity frame from the client before resending the request. The TX Period is the period of time to transmit an EAPOL PDU. The default value is 30 seconds.
Supplicant Timeout	Set the period of time the switch waits for a supplicant response to an EAP request. Supplicant Timeout: the timeout conditions in the exchanges between the supplicant and authentication server. The default value is 30 seconds.
Server Timeout	Set the period of time the switch waits for a Radius server response to an authentication request. Server Timeout: is the timeout condition in the exchanges between the authenticator and authentication server. The default value is 30 seconds.
Max Requests	Set the maximum number of times to retry sending packets to the supplicant. **ReAuthMax** is the number of reauthentication attempts that are permitted before the specific port becomes unauthorized. The default value is 2 times).
Re-Auth Period	Set the period of time after which clients connected must be re-authenticated. Enter a nonzero number of seconds between periodic reauthentication of the supplications. The default value is 3600 seconds).
Apply	Click “**Apply**” to activate the configurations.
Help	Show the online help file.

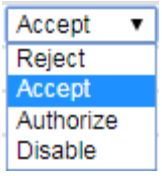
802.1x-Port Authorized Mode

Set the 802.1x authorized mode of each port.



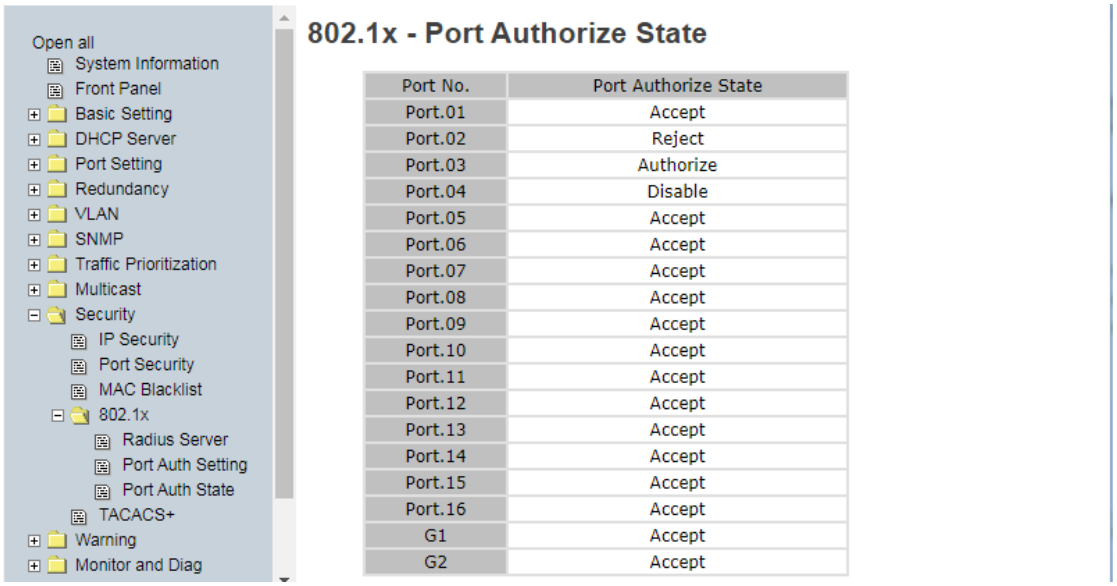
802.1x Port Authorize interface

The following table describes the labels in this screen.

Label	Description
Port Authorize Mode 	***Reject*:** force this port to be unauthorized. ***Accept*:** force this port to be authorized. ***Authorize*:** the state of this port was determined by the outcome of the 802.1x authentication. ***Disable*:** this port will not participate in 802.1x.
Apply	Click "**Apply**" to activate the configuration settings.
Help	Show the online help file.

802.1x-Port Authorized State

Shows the 802.1x port authorized state.

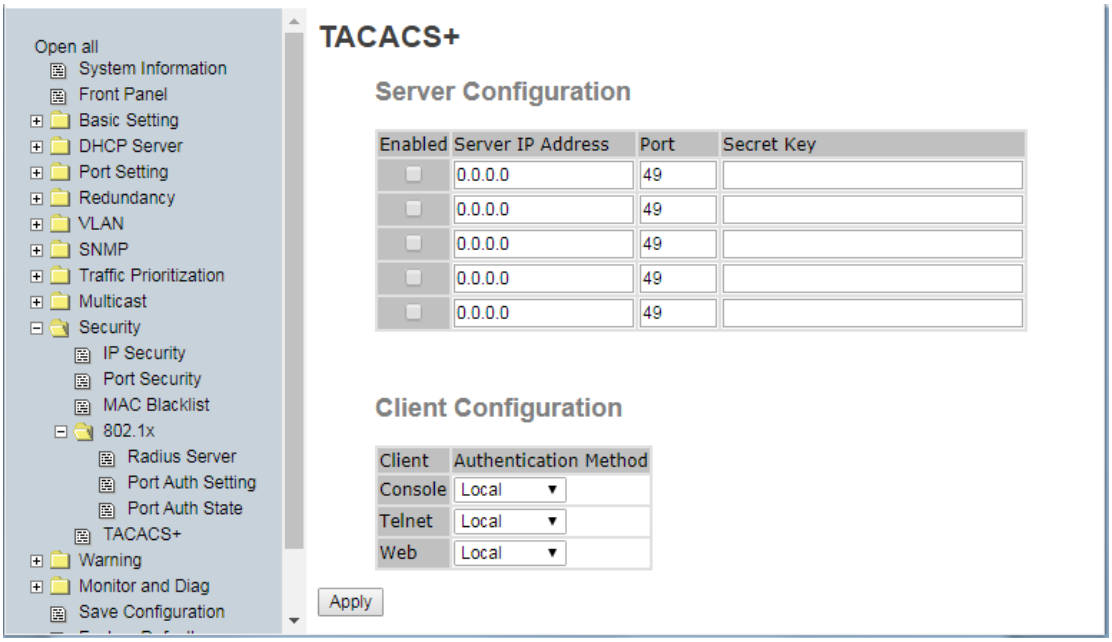


Port No.	Port Authorize State
Port.01	Accept
Port.02	Reject
Port.03	Authorize
Port.04	Disable
Port.05	Accept
Port.06	Accept
Port.07	Accept
Port.08	Accept
Port.09	Accept
Port.10	Accept
Port.11	Accept
Port.12	Accept
Port.13	Accept
Port.14	Accept
Port.15	Accept
Port.16	Accept
G1	Accept
G2	Accept

802.1x Port Authorize State interface

5.1.12.5 TACACS+

Terminal Access Controller Access-Control System Plus (TACACS+) is an open standard. Though derived from TACACS, TACACS+ is a separate protocol that handles authentication, authorization, and accounting (AAA) services.



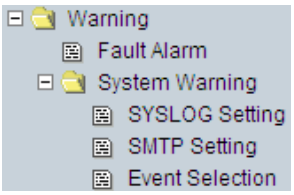
802.1x Port Authorize interface

The following table describes the labels in this screen.

Label	Description
Server Configuration	
Enabled	Check to enable up to five TACACS+ servers for configuration.
Server IP Address	Enter up to five TACACS+ server IP addresses.
Port	Use the default commonly-used TCP/IP port 49 or enter another port number.
Secret Key	Enter the TACACS+ secret key.
Client Configuration	
Client	For each client (Console, Telnet, and Web) select an Authentication Method (Local or TACACS+).
Authentication Method	Select an Authentication Method (Local or TACACS+) for each client (Console, Telnet, Web).

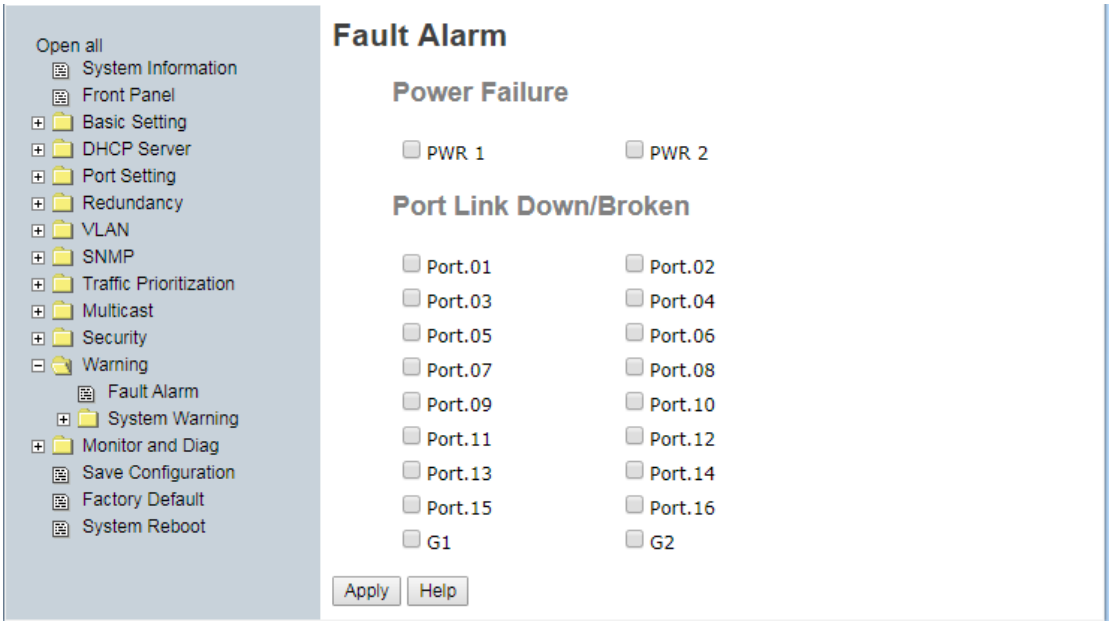
5.1.13 Warning

The Warning function is very important for managing the switch. You can monitor the switch via Syslog, E-Mail, and Fault Relay from a remote site. When events occur, the warning message is sent to the configured E-Mail server, or the fault is relayed to the switch panel.



5.1.13.1 Fault Alarm

When any selected fault event occurs, the Fault LED on the switch front panel lights and the electric relay will signal at the same time.



Fault Alarm interface

The following table describes the labels in this screen.

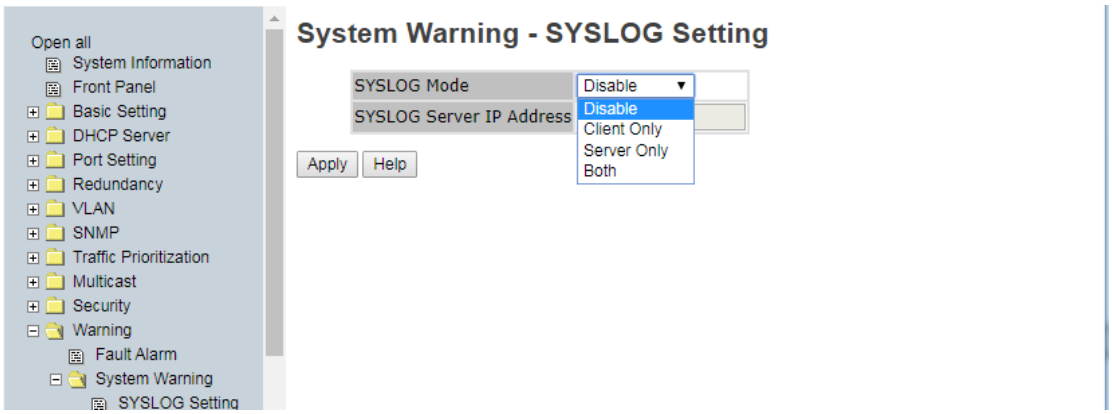
Label	Description
Power Failure	Tick the **PWR 1** or **PWR 2** checkbox to enable monitoring this fault.
Port Link Down/Broken	Tick the Port.01 to Port.18 checkbox to monitor for Port Link Down / Port Link Broken fault on the port.
Apply	Click "**Apply**" to activate the configurations.
Help	Show the online help file.

5.1.13.2 System Warning

System Warning supports two warning modes: SYSLOG and E-MAIL. You can monitor the switch via selected system events.

System Warning – SYSLOG Setting

The SYSLOG protocol is used to transmit event notification messages across networks. Please refer to RFC 3164 - The BSD SYSLOG Protocol.



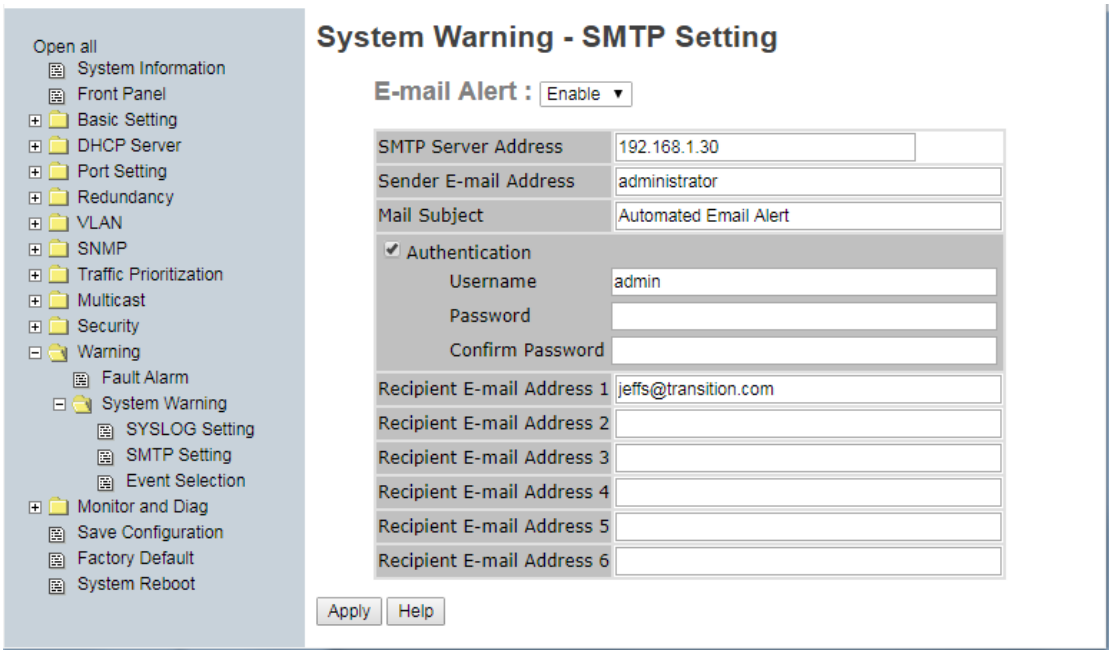
System Warning – SYSLOG Setting interface

The following table describes the labels in this screen.

Label	Description
SYSLOG Mode	***Disable***: disable SYSLOG logging. ***Client Only***: log to local system. ***Server Only***: log to a remote SYSLOG server. ***Both***: log to both the local and remote servers.
SYSLOG Server IP Address	The remote SYSLOG Server IP address.
Apply	Click "**Apply**" to activate the configurations.
Help	Show the online help file.

System Warning – SMTP Setting

The SMTP is the Simple Mail Transfer Protocol. It is a protocol for e-mail transmission across the Internet. Please refer to RFC 821 - Simple Mail Transfer Protocol.



System Warning – SMTP Setting interface

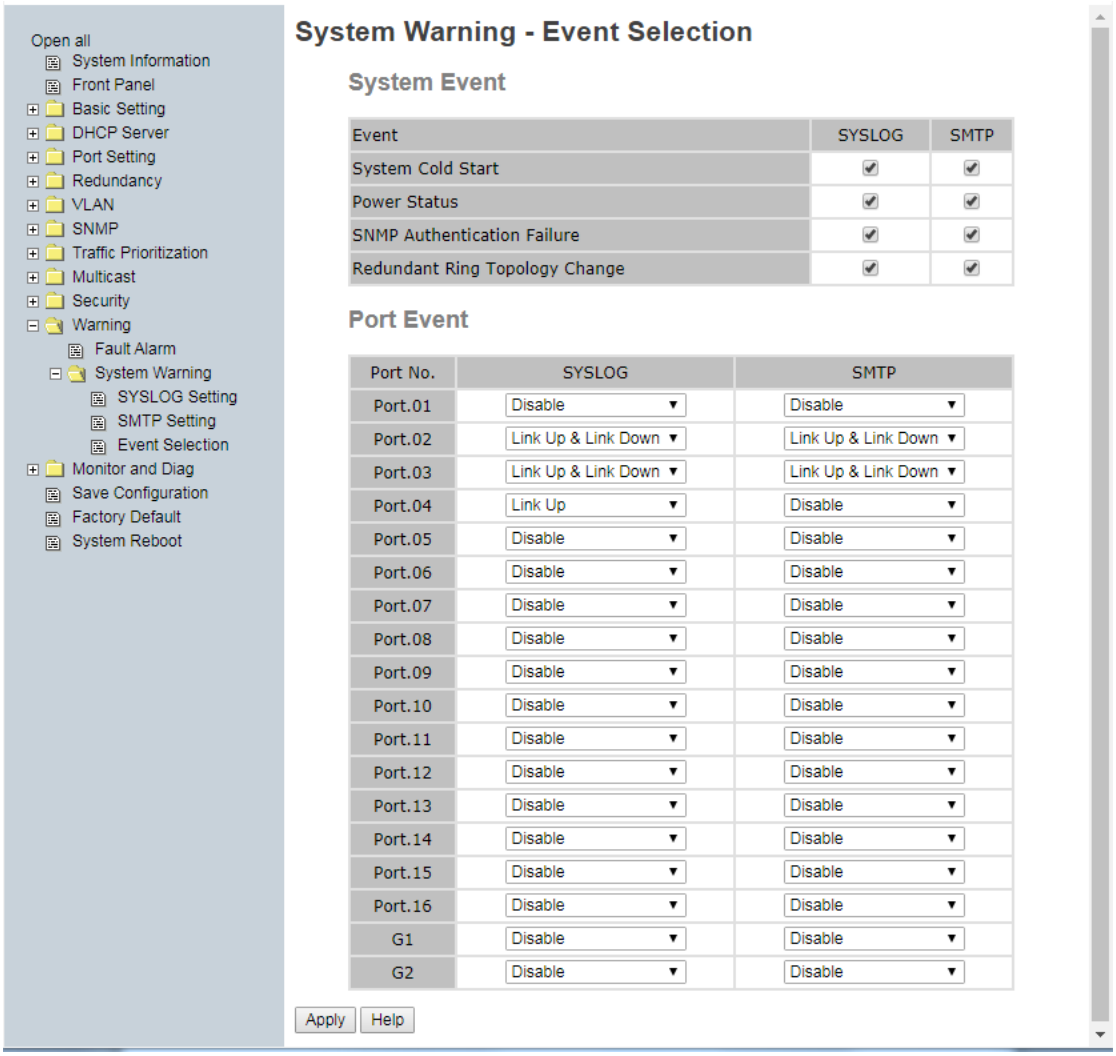
The following table describes the labels in this screen.

Label	Description
E-mail Alert	Enable/Disable transmission system warning events by e-mail.
Sender E-mail Address	Enter the SMTP server IP address.
Mail Subject	Enter the Subject of the mail.
Authentication	Tick the checkbox to enable Email login authentication and enter: ***Username*:** the authentication username. ***Password*:** the authentication password. ***Confirm Password*:** re-enter password.
Recipient E-mail Address *x*	Enter up to six E-mail recipients' E-mail addresses.
Apply	Click "**Apply**" to activate the configurations.
Help	Show the online help file.

System Warning – Event Selection

SYSLOG and SMTP are the two warning methods that the system supports.

Check the corresponding box to enable the system event warning method you wish to choose. Please note that the checkbox cannot be checked when SYSLOG or SMTP is disabled.



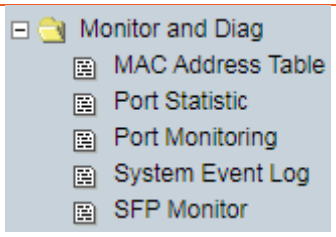
System Warning – Event Selection interface

The following table describes the labels in this screen.

Label	Description
System Event	
System Cold Start	Alert when system restarts (cold restart).
Power Status	Alert when a power up or down occurs.
SNMP Authentication Failure	Alert when an SNMP authentication failure occurs.
Redundant Ring Topology Change	Alert when Redundant Ring topology changes.
Port Event	
Port No.	For Port.01 - Port.16 select:

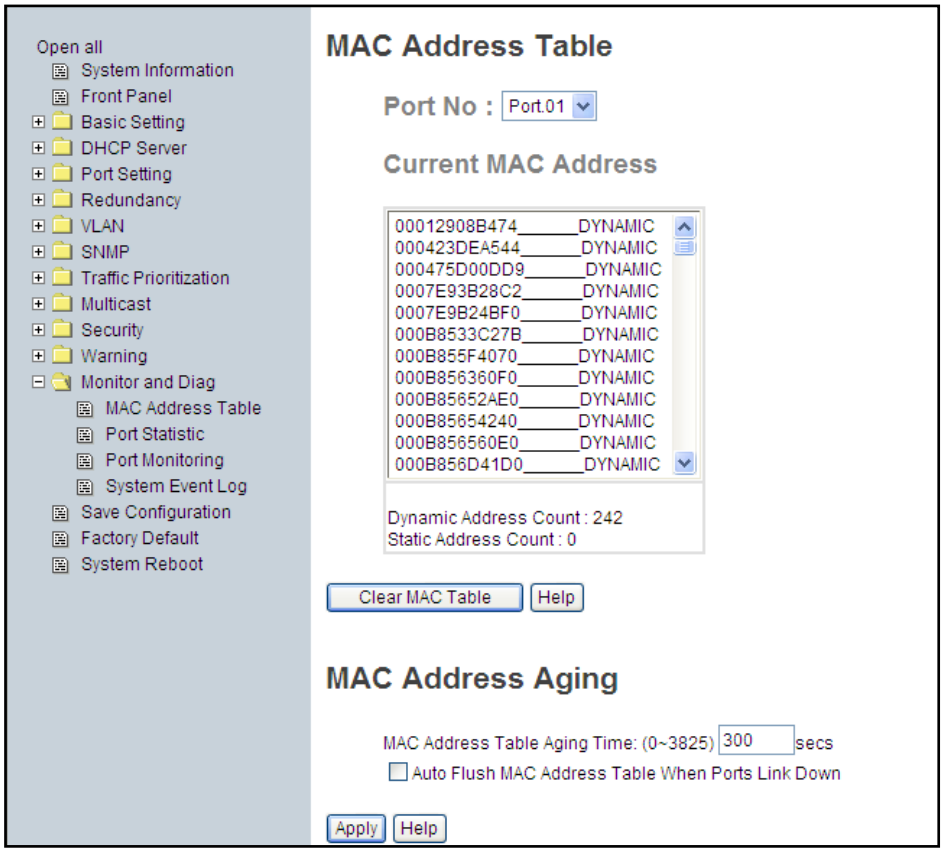
SYSLOG Event **SMTP event**	• **Disable** • **Link Up** • **Link Down** • **Link Up & Link Down**
Apply	Click "**Apply**" to activate the configuration settings.
Help	Show the online help file.

5.1.14 Monitor and Diagnostics



5.1.14.1 MAC Address Table

Refer to IEEE 802.1 D Sections 7.9. The MAC Address Table (Filtering Database) supports queries by the Forwarding Process, as to whether a frame received by a given port with a given destination MAC address is to be forwarded through a given potential transmission port.



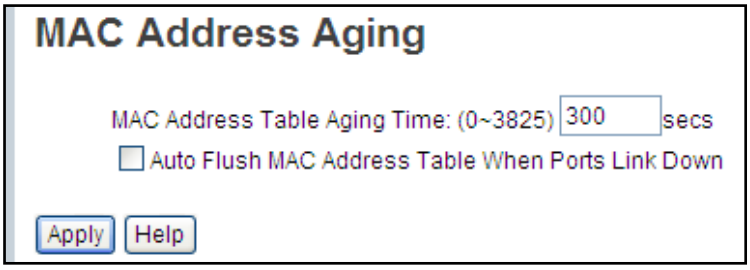
MAC Address Table interface

The following table describes the labels in this screen.

Label	Description
Port No :	Show all MAC addresses mapping to the selected port.
Current MAC Address	Displays the current MAC address for the port (if any).
Dynamic Address Count:	Displays the number of dynamically assigned IP addresses.
Static Address Count:	Displays the current number of statically assigned IP addresses.
Clear MAC Table	Click the button to clear all MAC addresses in table.
Help	Show the online help file.

5.1.14.2 MAC Address Aging

You can set the MAC Address aging timer so that after the specified time has expired, the unused MAC will be cleared from MAC table. The SISTM1040-262D-LRT-B also supports *Auto Flush MAC Address Table When ports Link Down*.



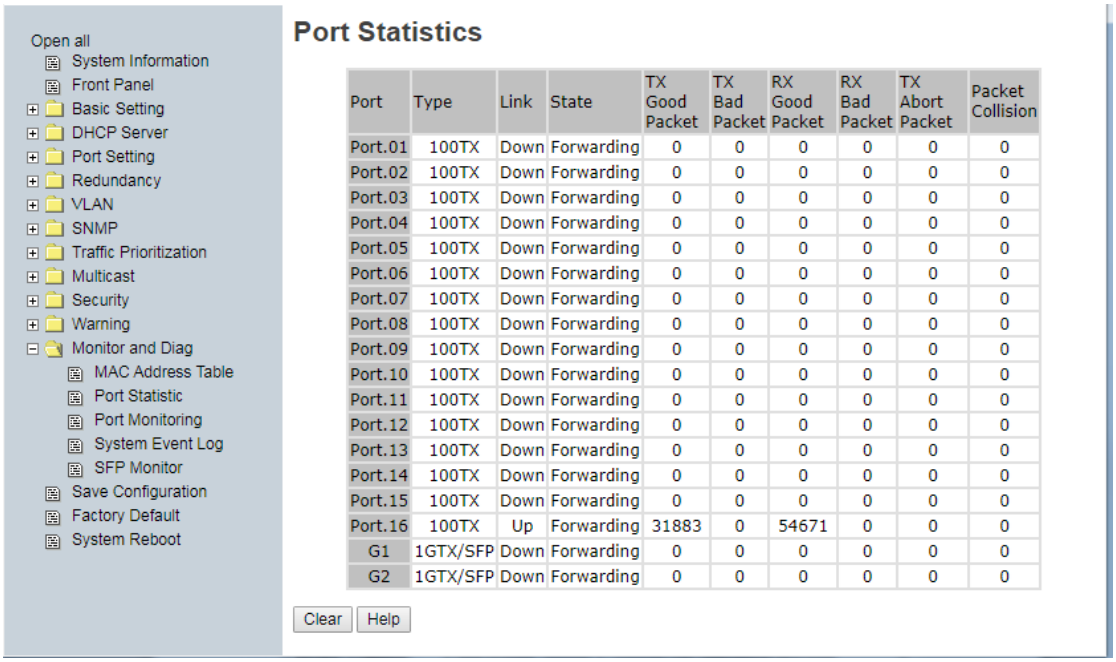
MAC Address Aging interface

The following table describes the labels in this screen.

Label	Description
MAC Address Table Aging Time	Set the aging time for MAC table. The value is **0** - **3825** seconds. The default setting is **300** seconds. Must be a multiple of 15.
Auto Flush MAC Address Table When Ports Link Down	Tick the checkbox to enable this function.
Apply	Click "**Apply**" to activate the configurations.
Help	Show the online help file.

5.1.14.3 Port Statistics

Port statistics show several statistics counters for all ports.



Port Statistics interface

The following table describes the labels in this screen.

Label	Description
Type	Show port speed and media type (e.g., **100TX** or **1GTX/SFP**).
Link	Show port link status (**Up** or **Down**).
State	Show ports' state (e.g., **Forwarding**).
TX Good Packet	The number of good packets sent by this port.
TX Bad Packet	The number of bad packets sent by this port.
RX Good Packet	The number of good packets received by this port.
RX Bad Packet	The number of bad packets received by this port.
TX Abort Packet	The number of packets aborted by this port.
Packet Collision	The number of times a collision was detected by this port.
Clear	Clear all counters in this table.
Help	Show the online help file.

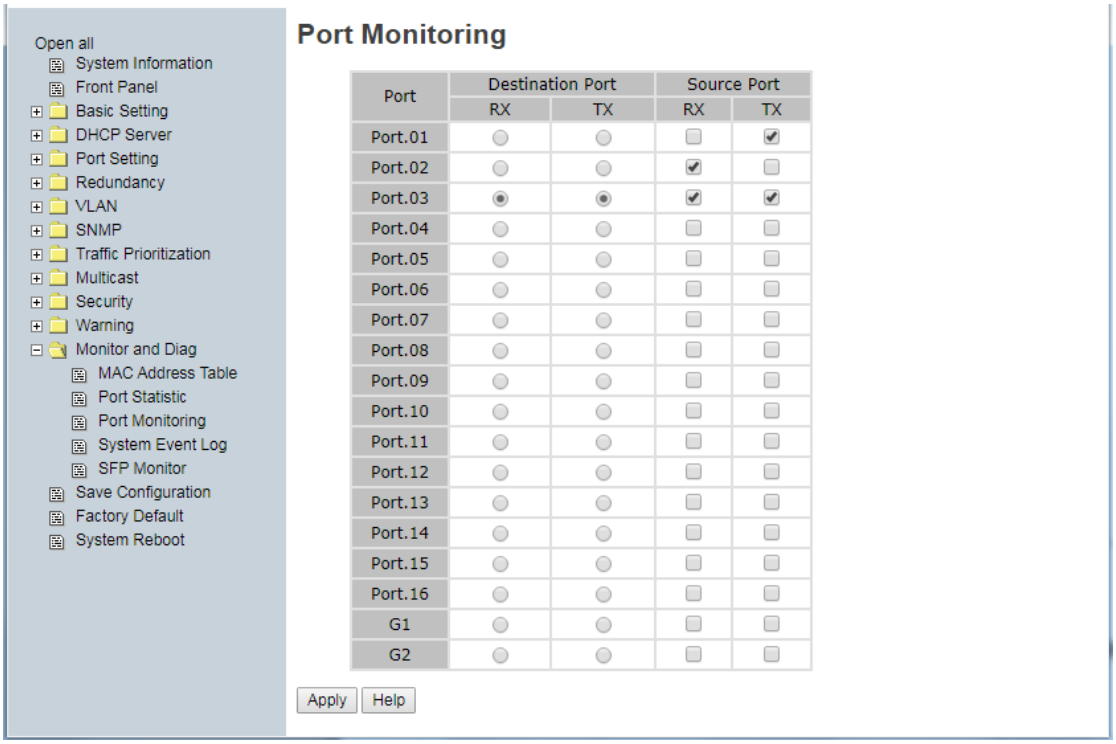
5.1.14.4 Port Monitoring

Port monitoring function supports TX (egress) only, RX (ingress) only, and both TX/RX monitoring.

TX monitoring sends any data that egress out checked TX source ports to a selected TX destination port as well.

RX monitoring sends any data that ingress in checked RX source ports out to a selected RX destination port as well as sending the frame where it normally would have gone.

Note: to disable port monitoring, keep all source ports unchecked.

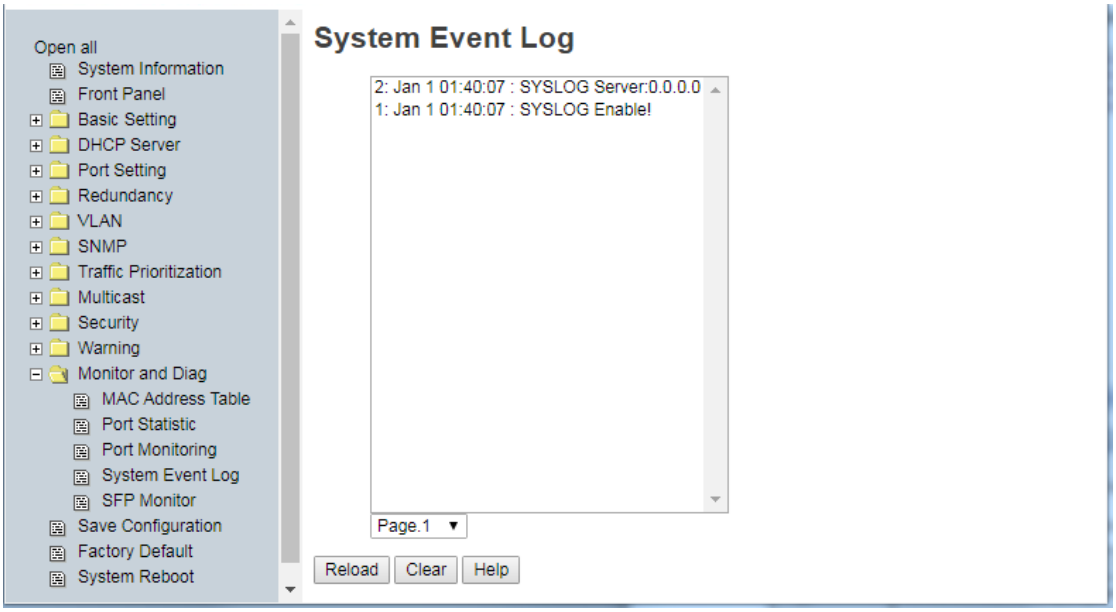


Port monitoring interface

Label	Description
Destination Port	The port(s) to receive a copied frame from Source port for monitoring purpose. Tick the desired radio buttons.
Source Port	The port(s) to be monitored. Tick the checkbox of for the ports whose TX or RX is to be monitored.
TX	The frames that come into switch port.
RX	The frames that are received by switch port.
Apply	Click "**Apply**" to activate the configuration.
Help	Show the online help file.

5.1.14.5 System Event Log

If the system log client is enabled, the system event logs will display in this table.



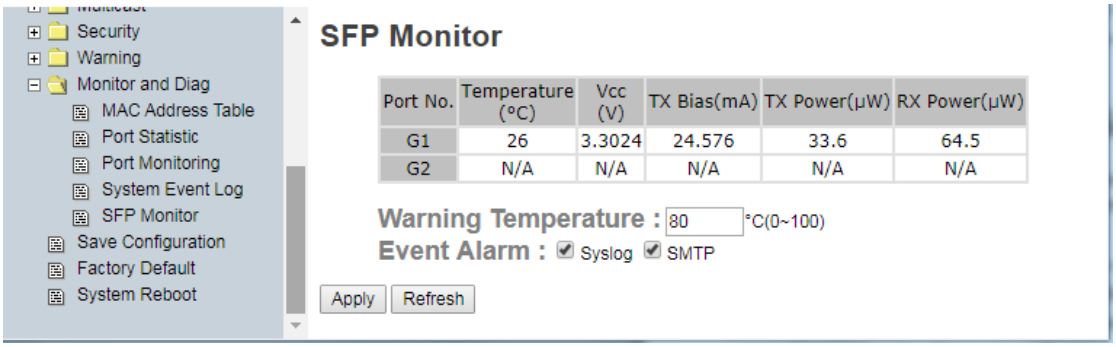
System Event Log interface

The following table describes the labels in this screen.

Label	Description
Page	Select the desired Log page at the dropdown.
Reload	Click the button to get the newest event logs and refresh this page.
Clear	Clear the log.
Help	Show the online help file.

5.1.14.6 SFP Monitor

The SFP Monitor page lets you set and view warning and event alarm parameters.



SFP Monitor interface

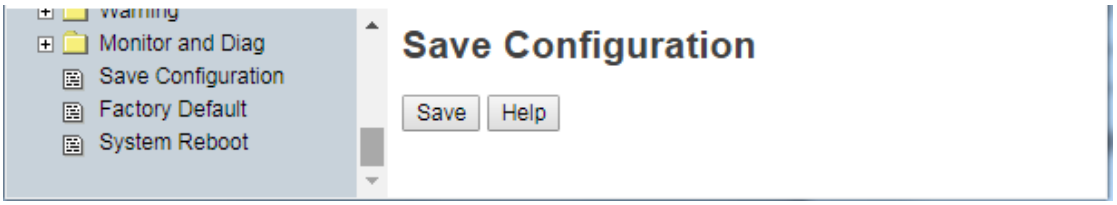
The following table describes the labels in this screen.

Label	Description
Temperature (°C)	The current reported SFP temperature in degrees Celsius.
Vcc (V)	The current reported SFP voltage in Volts.
TX Bias(mA)	The current reported transmit bias current in milliAmps.
TX Power(μW)	The current reported transmit power in microWatts.
RX Power(μW)	The current reported receive power in microWatts.
Warning Temperature	Enter the temperature at which you want a warning issued. The valid range is 0~100 °C. The default setting is 75 °C.
Event Alarm	Check the Syslog and/or SMTP checkbox for event reporting.
Apply	Click to activate the configuration settings.
Refresh	Click to update the page content.

5.1.15 Save Configuration

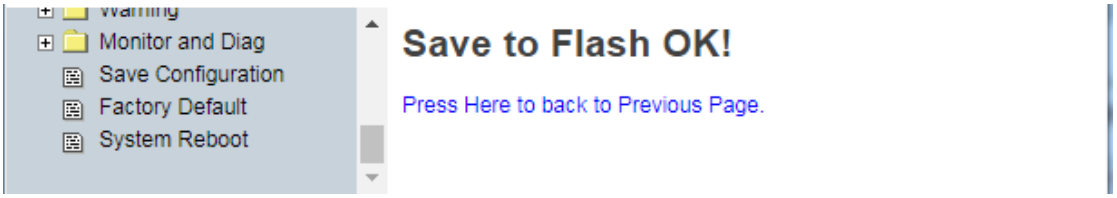
When you change a configuration, you can click "**Save Configuration**" to save the current configuration data to the permanent flash memory. Otherwise, the current configuration will be lost when power off or system reset.

At the default page, click the Save button.



When the Save completes, the page displays the message "Save to Flash OK!

Press Here to back to Previous Page."



Click the linked text "Press Here to back to Previous Page" to return to the default page.

Save Configuration interface

The following table describes the labels in this screen.

Label	Description
Save	Save all configurations.
Help	Show help file.

5.1.16 Factory Default

This page lets you reset the switch to factory default configuration. After you click the "Reset" button, the system MUST be restarted and the default configuration will be applied in next start.

Factory Default interface

You can click the **Reset** button to reset the switch to all of its default configuration parameters.

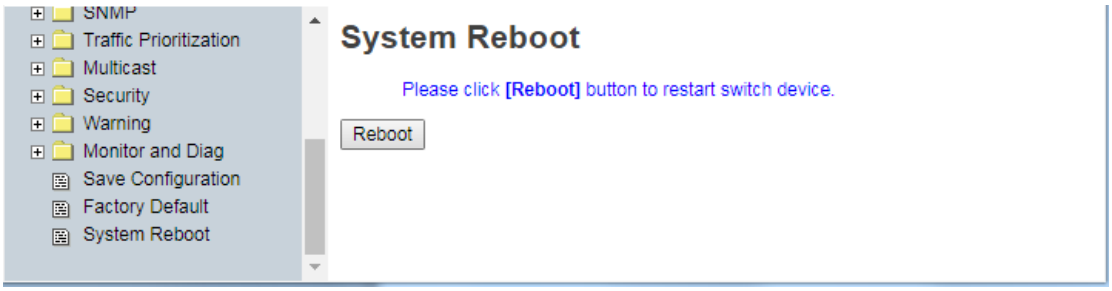
You can check the "**Keep current IP address setting**" checkbox and click **Reset** to reset to default parameters, but keep the currently-configured IP address.

You can select "**Keep current username & password**" checkbox and click **Reset** to reset to default parameters, but keep the currently-configured User Name and Password.

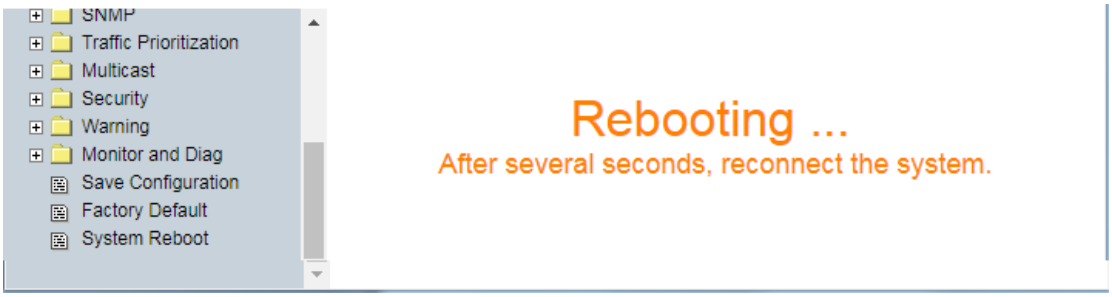
At the confirmation prompt (e.g., *Are you sure to Reset to Default?*), click the **OK** button.
When the message "*System Reboot Please click [Reboot] button to restart switch device.*" displays, click the **Reboot** button. The message "*Rebooting ... After several seconds, reconnect the system.*" displays momentarily.

5.1.17 System Reboot

This page lets you restart the switch device.



You can click the **Reboot** button to restart the switch.



When the message "*Rebooting ... After several seconds, reconnect the system.*" displays, click another menu selection and continue operation.

6. Command Line Interface Management

6.1 About CLI Management

Besides Web-based management, the SISTM1040-262D-LRT-B also supports CLI management. You can use a console or Telnet to manage the switch via the CLI.

Caution: The Console port is for maintenance purposes only, and it may only be used when the area is known to be non-hazardous.

CLI Management by RS-232 Serial Console (9600, 8, none, 1, none)

Before configuring by RS-232 serial console, use an RJ45 to DB9-F cable to connect the RS-232 Console port on the Switch to the COM Port on your PC.

Follow the steps below to access the console via RS-232 serial cable.

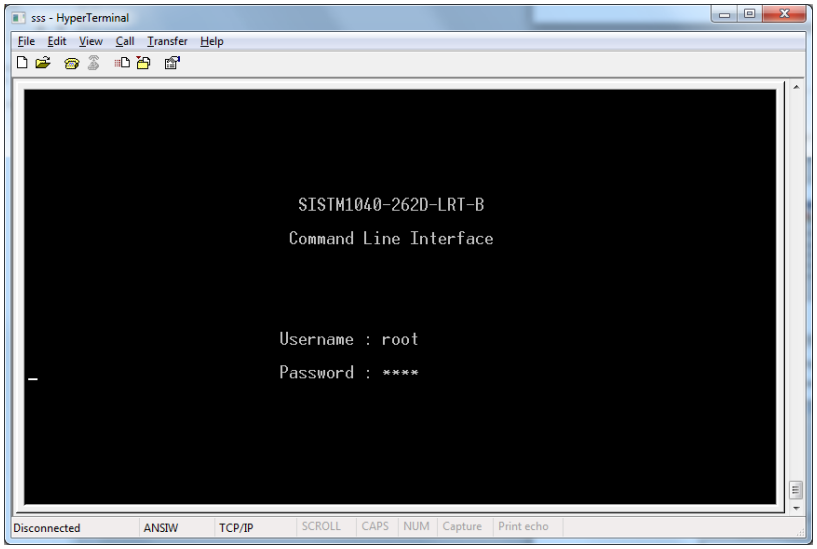
Step 1. From the Windows desktop, click on Start -> Programs -> Accessories -> Communications -> Hyper Terminal.

Step 2. Enter a name for new connection.

Step 3. Select to use COM port number.

Step 4. The COM port properties setting, 9600 for Bits per second, 8 for Data bits, None for Parity, 1 for Stop bits and none for Flow control.

Step 5. The Console login screen displays. Use the keyboard to enter the Username and Password (the same with the password for Web browser), then press "**Enter**".



CLI Management by Telnet

You can use "**TELNET**" to configure the switch. The default values are:

IP Address: **192.168.1.77**

Subnet Mask: **255.255.255.0**

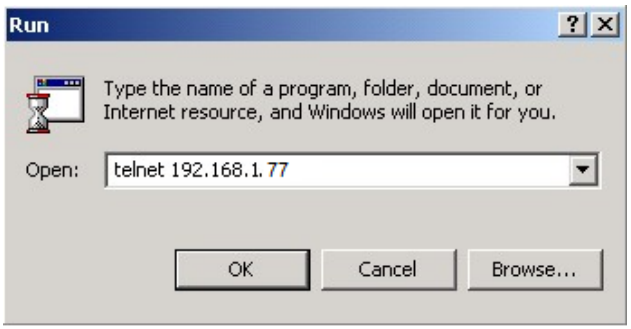
Default Gateway: **192.168.1.254**

User Name: **root**

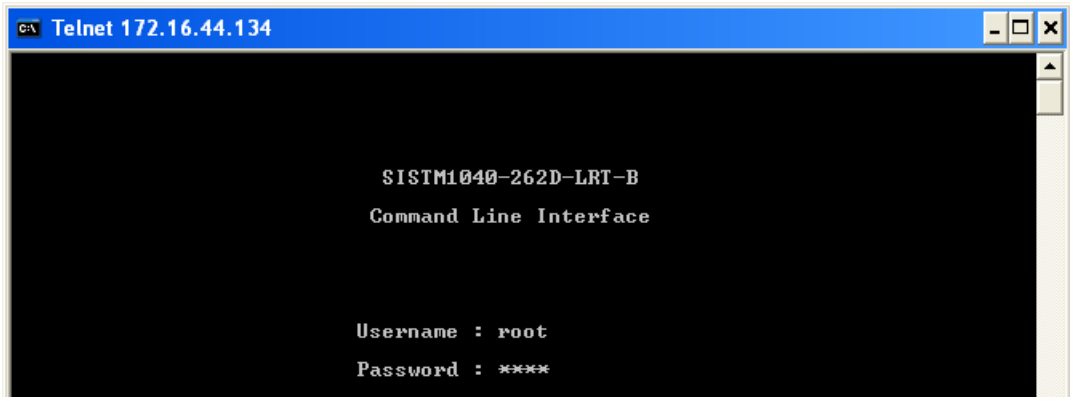
Password: **root**

Follow the steps below to access the console via Telnet.

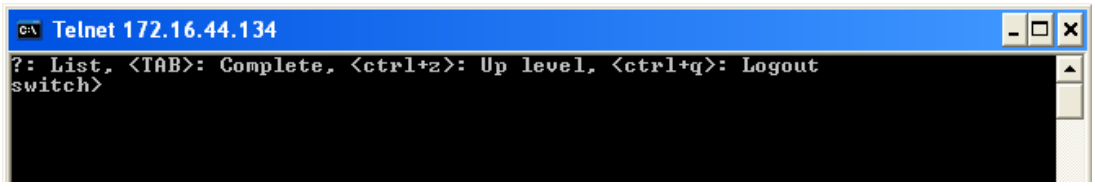
Step 1. Telnet to the IP address of the switch from the Windows "**Run**" command (or from the MS-DOS prompt) as below.



Step 2. The Login screen displays. Use the keyboard to enter the Username and Password (both **root**), and then press "**Enter**".



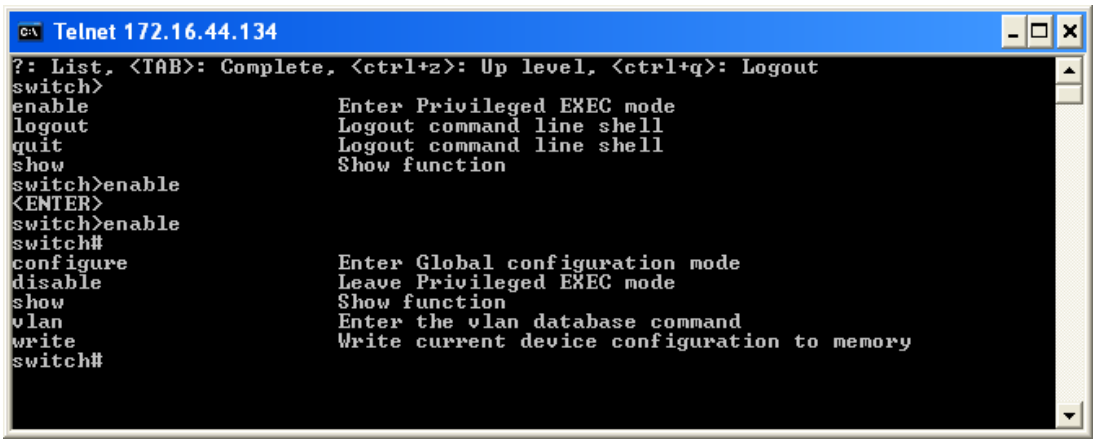
The initial CLI command screen displays:



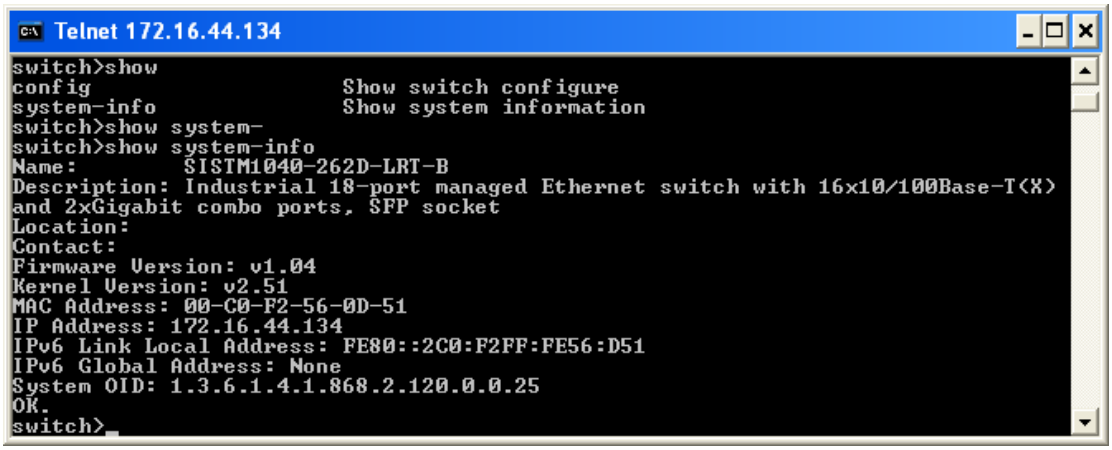
The CLI controls displayed are:

```
?: List, <TAB>: Complete, <ctrl+z>: Up level, <ctrl+q>: Logout
```

Step 3. Use the **?** command to list the varous available commands for the current mode.



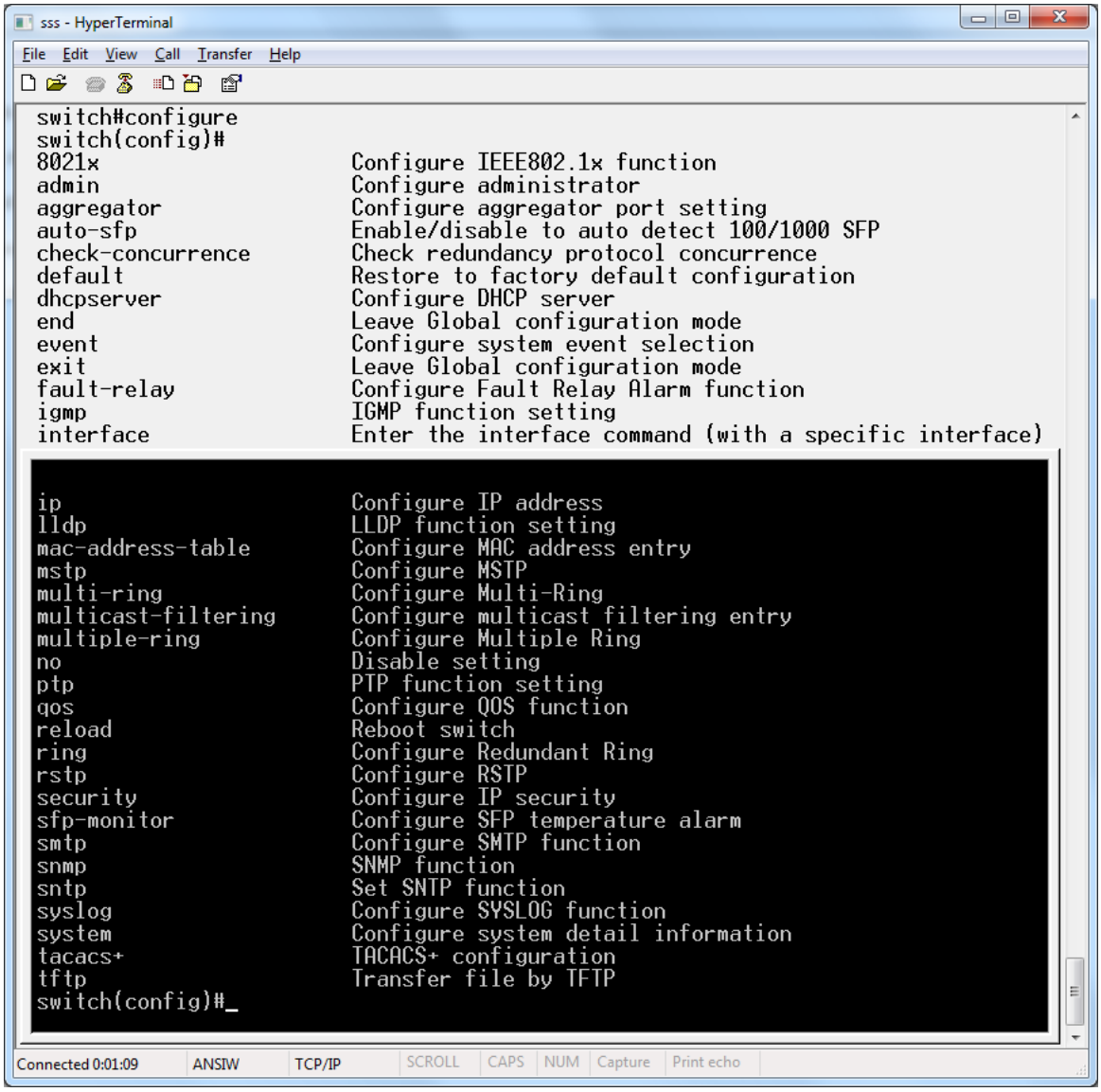
***show* commands**:



CLI Controls:

Entry	Action
?	List the available set of commands for the current mode.
<tab>	Complete the command syntax.
<ctrl+z>	Go Up one command level (e.g., from Privileged EXEC mode to User EXEC mode or from Global configuration mode to Privileged EXEC mode).
<ctrl+q>	Logout of the CLI session.
<space bar>	Display More on the same command subject.
q/Q	Quit displaying more of the command subject.

***Configure* commands**



Command Levels

Mode (Symbol)	Access Method	Prompt	Exit Method	About This Mode
User EXEC (E)	Begin a session with your switch.	switch>	Enter **logout** or **quit**.	The user commands available at this level are a subset of those available at the privileged level. Use this mode to • Enter menu mode. • Display system information.
Privileged EXEC (P)	Enter the **enable** command while in user EXEC mode.	switch#	Enter **disable** to exit.	The privileged commands are more advanced Use this mode to • Display advance function status • save configurations
Global configuration (G)	Enter the **configure** command while in privileged EXEC mode.	switch(config)#	To exit to privileged EXEC mode, enter **exit** or **end**	Use this mode to configure parameters that apply to the Switch as a whole.
VLAN database (V)	Enter the **vlan database** command while in privileged EXEC mode.	switch(vlan)#	To exit to user EXEC mode, enter **exit**.	Use this mode to configure VLAN-specific parameters.
Interface configuration (I)	Enter the **interface** command (with a specific interface)while in global configuration mode	switch(config-if)#	To exit to global configuration mode, enter **exit**. To exit privileged EXEC mode enter **end.**	Use this mode to configure parameters for the switch and Ethernet ports.

Command Level Symbols

Mode	Symbol for Command Level
User EXEC	E
Privileged EXEC	P
Global configuration	G
VLAN database	V
Interface configuration	I

6.2 System Commands

Command	Level	Description	Example
show config	**E**	Display switch configuration	switch>show config
show terminal	**P**	Display console information.	switch#show terminal
write memory	**P**	Save your configuration into permanent memory (flash ROM).	switch#write memory Update Complete switch#
system name **[System Name]**	**G**	Configure system name.	switch(config)#system name xxx
system location **[System Location]**	**G**	Set switch system location string.	switch(config)#system location xxx
system description **[System Description]**	**G**	Set switch system description string.	switch(config)#system description xxx
system contact **[System Contact]**	**G**	Set switch system contact window string.	switch(config)#system contact xxx
show system-info	**E**	Display system information.	switch>show system-info
ip address **[Ip-address] [Subnet-mask] [Gateway]**	**G**	Set the IP address of switch.	switch(config)#ip address 192.168.1.1 255.255.255.0 192.168.1.254
ip dhcp	**G**	Enable DHCP client function of switch	switch(config)#ip dhcp
show ip	**P**	Show IP information of switch	switch#show ip

no ip dhcp	**G**	Disable DHCP client function of switch	switch(config)#no ip dhcp
reload	**G**	Halt and perform a cold restart (Reboot switch).	switch(config)#reload
default [keepip|keepadmin|both]	**G**	Restore to factory defaults.	switch(config)#default both
admin username **[Username]**	**G**	Change a login username (max. 10 words).	switch(config)#admin username xxxxxx
admin password **[Password]**	**G**	Specify a password (max. 10 words)	switch(config)#admin password xxxxxx
show admin	**P**	Show administrator information	switch#show admin
dhcp enable	**G**	Enable DHCP Server	switch(config)#dhcp enable
dhcp lowip **[Low IP]**	**G**	Configure low IP address for IP pool	switch(config)# dhcp lowip 192.168.1.1
dhcp highip **[High IP]**	**G**	Configure high IP address for IP pool	switch(config)# dhcp highip 192.168.1.50
dhcp subnetmask **[Subnet mask]**	**G**	Configure subnet mask for DHCP clients	switch(config)#dhcp subnetmask 255.255.255.0
dhcp gateway **[Gateway]**	**G**	Configure gateway for DHCP clients	switch(config)#dhcp gateway 192.168.1.254
dhcp dnsip **[DNS IP]**	**G**	Configure DNS IP for DHCP clients	switch(config)# dhcp dnsip 192.168.1.1
dhcp leasetime **[Hours]**	**G**	Configure lease time (in hour)	switch(config)#dhcpleasetime 1
dhcp ipbinding **[IP address]**	**I**	Set static IP for DHCP clients by port	switch(config)#interface fastEthernet 2 switch(config-if)#dhcp ip binding 192.168.1.1
show dhcp configuration	**P**	Show configuration of DHCP server	switch#show dhcp configuration
show dhcp clients	**P**	Show client entries of DHCP server	switch#show dhcp clinets
show dhcp ip-binding	**P**	Show IP-Binding information of DHCP server	switch#show dhcp ip-binding
no dhcp	**G**	Disable DHCP server function	switch(config)#no dhcp
security enable	**G**	Enable IP security function	switch(config)#security enable
security http	**G**	Enable IP security of HTTP server	switch(config)#security http

security https	**G**	Enable IP security of HTTPS server	switch(config)#security https
security snmp	**G**	Enable SNMP server	switch(config)#security snmp
security ssh	**G**	Enable SSH server	switch(config)#security ssh
security telnet	**G**	Enable IP security of telnet server	switch(config)#security telnet
security ip **[Index(1..10)] [IP Address]**	**G**	Set the IP security list	switch(config)#security ip 1 192.168.1.55
show security	**P**	Show the information of IP security	switch#show security
no security	**G**	Disable IP security function	switch(config)#no security
no security http	**G**	Disable IP security of HTTP server	switch(config)#no security http
no security https	**G**	Disable IP security of HTTPS server	switch(config)#no security https
no security snmp	**G**	Disable SNMP server	switch(config)#no security snmp
no security ssh	**G**	Disable SSH server	switch(config)#no security ssh
no security telnet	**G**	Disable IP security of telnet server	switch(config)#no security telnet

6.3 Interface (Port) Commands

Command	Level	Description	Example
interface fastEthernet [Portid]	G	Choose the port for modification.	switch(config)#interface fastEthernet 2
duplex [full | half]	I	Use the duplex config command to specify the duplex mode of operation for Fast Ethernet.	switch(config)#interface fastEthernet 2 switch(config-if)#duplex full
speed [10|100|1000|auto]	I	Use the speed config command to specify the speed mode of operation for Fast Ethernet; the speed can't be set to 1000 if the port isn't a Gigabit port.	switch(config)#interface fastEthernet 2 switch(config-if)#speed 100
flowcontrol mode [Symmetric|Asymmetric]	I	Use the flowcontrol config command on Ethernet ports to control traffic rates during congestion.	switch(config)#interface fastEthernet 2 switch(config-if)#flowcontrol mode Asymmetric
no flowcontrol	I	Disable flow control of interface	switch(config-if)#no flowcontrol
security enable	I	Enable security of interface	switch(config)#interface fastEthernet 2 switch(config-if)#security enable
no security	I	Disable security of interface	switch(config)#interface fastEthernet 2 switch(config-if)#no security
ratelimit type all	I	Set interface ingress limit frame type to "accept all frame"	switch(config-if)#ratelimit type all
ratelimit type broadcast-only	I	Set interface ingress limit frame type to accept "broadcast only" frames.	switch(config-if)#ratelimit type b switch(config-if)#ratelimit type broadcast-only
ratelimit type broadcast-multicast	I	Set interface ingress limit frame type to "accept broadcast and multicast frames"	switch(config-if)#ratelimit type broadcast-multicast
ratelimit type multicast-flooded-unicast	I	Set interface ingress limit frame type to "only accept broadcast frames"	switch(config-if)#ratelimit type broadcast-multicast-flooded-unicast
ratelimit in [Value]	I	Set interface input rate. Rate Range is from 100 kbps to	switch(config-if)#ratelimit in 500

		102400 kbps or to 256000 kbps for giga ports, and zero means no limit.	
ratelimit out [Value]	**I**	Set interface output rate. Rate Range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports, and zero means no limit.	switch(config-if)#ratelimit out 100
show ratelimit	**I**	Show interface's bandwidth control	switch(config-if)#show ratelimit
state [Enable | Disable]	**I**	Use the state interface config command to specify the mode of operation for Ethernet ports. Use the disable form of this command to disable the port.	switch(config)#interface fastEthernet 2 switch(config-if)#state Disable
show interface configuration	**I / P**	Display the interface configuration status	switch(config)#interface fastEthernet 2 switch(config-if)#show interface configuration
show interface status	**I / P**	Display the interface actual status	switch(config)#interface fastEthernet 2 switch(config-if)#show interface status
show interface accounting	**I**	Display the interface statistic counter	switch(config)#interface fastEthernet 2 switch(config-if)#show interface accounting
show interface alias	**I / P**	Display interface alias	switch#show interface alias
show interface status	**I / P**	Display interface status	show interface status
show interface counters [portid]	**I**	Display the interface MIB counters	switch#show interface counters 2
no accounting	**I**	Clear interface accounting information	switch(config)#interface fastEthernet 2 switch(config-if)#no accounting

6.4 Trunk Commands

Command	Level	Description	Example
aggregator priority [1to65535]	G	Set port group system priority	switch(config)#aggregator priority 22
aggregator activityport [Port Numbers]	G	Set activity port	switch(config)#aggregator activityport 2
aggregator group [GroupID] [Port-list] **lacp** **workp** [Workport]	G	Assign a trunk group with LACP active. [GroupID] :1 to 3 [Port-list]:Member port list, This can be a port range (ex.1-4) or a port list separated by commas (ex.2, 3, 6). [Workport]: The # of work ports; cannot be less than 0 or be larger than the # of member ports.	switch(config)#aggregator group 1 1-4 lacp workp 2 or switch(config)#aggregator group 2 1,4,3 lacp workp 3 or aggregator group 1 3,1,2 lacp workport 1
aggregator group [GroupID] [Port-list] **nolacp**	G	Assign a static trunk group. [GroupID] :1to3 [Port-list]:Member port list. This can be a port range (ex.1-4) or a port list separated by commas (ex.2, 3, 6)	switch(config)#aggregator group 1 2-4 nolacp or switch(config)#aggreator group 1 3,1,2 nolacp
show aggregator	P	Show the information of trunk group	switch#show aggregator
no aggregator lacp [GroupID]	G	Disable the LACP function of trunk group	switch(config)#no aggreator lacp 1
no aggregator group [GroupID]	G	Remove a trunk group	switch(config)#no aggreator group 2

6.5 VLAN Commands

Command	Level	Description	Example
vlan database	P	Enter VLAN configure mode	switch#vlan database
vlan [8021q | port-based]	V	Configure IEEE802.1q vlan or	switch(vlan)#vlan port-based grpname SWDev grpid 1 port 16

		Configure Port-Based vlan	switch(vlan)#vlan 8021q aggreator 1 access-link untag 20
vlanmode [disable|portbase|802.1q|gvrp]		Change vlan mode.	switch(vlan)# vlanmode 802.1q switch(vlan)# vlanmode gvrp switch(vlan)#vlanmode portbase
no vlan [VID]	**V**	Disable vlan group(by VID)	switch(vlan)#no vlan 2
no gvrp	**V**	Disable GVRP	switch(vlan)#no gvrp
IEEE 802.1Q VLAN			
vlan 8021q port [PortNumber] **access-link untag** [UntaggedVID]	**V**	Assign a access link for VLAN by port, if the port belongs to a trunk group, this command can't be applied.	switch(vlan)#vlan 802.1q port 3 access-link untag 33
vlan 8021q port [PortNumber] **trunk-link tag** [TaggedVID List]	**V**	Assign a trunk link for VLAN by port, if the port belongs to a trunk group, this command can't be applied.	switch(vlan)#vlan 8021q port 3 trunk-link tag 2,3,6,99 or switch(vlan)#vlan 8021q port 3 trunk-link tag 3-20
vlan 8021q port [PortNumber] **hybrid-link untag** [UntaggedVID] **tag** [TaggedVID List]	**V**	Assign a hybrid link for VLAN by port, if the port belongs to a trunk group, this command can't be applied.	switch(vlan)# vlan 8021q port 3 hybrid-link untag 4 tag 3,6,8 or switch(vlan)# vlan 8021q port 3 hybrid-link untag 5 tag 6-8
vlan 8021q aggreator [TrunkID] **access-link untag** [UntaggedVID]	**V**	Assign a access link for VLAN by trunk group	switch(vlan)#vlan 8021q aggreator 3 access-link untag 33
vlan 8021q aggreator [TrunkID] **trunk-link tag** [TaggedVID List]	**V**	Assign a trunk link for VLAN by trunk group	switch(vlan)#vlan 8021q aggreator 3 trunk-link tag 2,3,6,99 or switch(vlan)#vlan 8021q aggreator 3 trunk-link tag 3-20
vlan 8021q aggreator [PortNumber] **hybrid-link untag** [UntaggedVID] **tag**	**V**	Assign a hybrid link for VLAN by trunk group	switch(vlan)# vlan 8021q aggreator 3 hybrid-link untag 4 tag 3,6,8 or switch(vlan)# vlan 8021q aggreator 3 hybrid-link untag 5 tag 6-8

[TaggedVID List]			
vlan 8021q mnt-vid **[VID]**	**V**	Configure a management VID (0 is disabled). Assign a VID and drop the connection.	switch(vlan)#vlan 8021q mnt-vid 100
show vlan [VID] or **show vlan [**GroupName] or **show vlan**	**V**	Show VLAN information	switch(vlan)#show vlan 23 switch(vlan)#show vlan switch#show vlan default

6.6 Spanning Tree Commands

Spanning Tree Protocol (STP) support includes Rapid Spanning Tree Algorithm Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP).

Command	Level	Description	Example
enable mstp	G	Enable MSTP	switch(config)#mstp enable
enable rstp	G	Enable RSTP	switch(config)#rstp enable
spanning-tree priority [0to61440]	**G**	Configure spanning tree priority parameter	switch(config)#spanning-tree priority 32767
mstp port-priority	**G or I**	Configure MSTP Port priority on this interface	switch(config-if)#mstp priority 16 or switch(config)#mstp priority 4096
rstp port-priority	**G or I**	Configure RSTP Port priority on this interface	
mstp config-name		Configure MSTP bridge config name parameter	switch(config)#mstp config-name chas
mstp max-age [seconds] **rstp max-age** [seconds]	**G**	Use the spanning-tree max-age global config command to change the interval between messages the spanning tree receives from the root switch. If a switch does not receive a BPDU message from the root switch within this interval, it re-computes the STP topology.	switch(config)#mstp max-age 10 or switch(config)#rstp max-age 20
mstp max-hops [seconds]		Configure MSTP max hops parameter	switch(config)#mstp max-hops 9 Old Max Hops: 20 New Max Hops: 9 OK. switch(config)#

spanning-tree hello-time [seconds]	**G**	Use the spanning-tree hello-time global config command to specify the interval between hello bridge protocol data units (BPDUs).	switch(config)#mstp hello-time 4 or switch(config)#rstp hello-time 6
mstp forward-time [seconds] or **rstp forward-time** [seconds]	**G**	Use the spanning-tree forward-time global config command to set the forwarding-time for the specified spanning-tree instances. The forwarding time determines how long each of the listening and learning states last before the port begins forwarding.	switch(config)#mstp forward-time 5 or switch(config)#rstp forward-time 25
mstp path-cost [1to200000000] or **rstp path-cost** [1to200000000]	**I**	Use the spanning-tree cost interface config command to set the path cost for Spanning Tree Protocol (STP) calculations. In the event of a loop, spanning tree considers the path cost when selecting an interface to place into the forwarding state.	switch(config-if)#mstp path-cost 500000 or switch(config-if)#rstp path-cost 0
mstp priority [0-240]	**I**	Use the spanning-tree port-priority interface configuration command to configure a port priority that is used when two switches tie for position as the root switch.	switch(config-if)#mstp priority 64
mstp admin-p2p [Auto|True|False] **rstp admin-p2p** [Auto|True|False]	**I**	Admin P2P of MSTP / RSTP priority on this interface.	switch(config-if)#rstp admin-p2p auto or switch(config-if)#mstp admin-p2p false
mstp admin-edge [True|False]	**G/I**	Admin Edge of MSTP / RSTP priority on this	switch(config-if)#mstp admin-edge true switch(config-if)#rstp admin-edge false

rstp-admin-edge [True|False]		interface.	
mstp admin-non-stp [True|False] **rstp admin non-stp** [True|False]	I	Admin NonSTP of MSTP / RSTP priority on this interface.	switch(config-if)#mstp admin-non-stp false switch(config-if)#rstp admin-non-stp false
rstp admin-p2p [Auto|True|False] **rstp admin-p2p** [Auto|True|False]	I	Admin P2P of MSTP / RSTP priority on this interface.	switch(config-if)#mstp admin-p2p false switch(config-if)#rstp admin-p2p false
rstp admin-edge [True|False] **mstp admin-edge** [True|False]	I	Admin Edge of MSTP or RSTP priority on this interface.	switch(config-if)#rstp admin-edge false switch(config-if)#mstp admin-edge true
rstp admin-non-stp [True|False]	I	Admin NonSTP of MSTP priority on this interface.	switch(config-if)#mstp admin-non-stp false switch(config-if)#rstp admin-non-stp false
show mstp	P	Show MSTP information	switch#show mstp
show rstp	P	Show RSTP information	switch#show rstp
no mstp	G	Disable MSTP.	switch(config)#no mstp
no rstp	G	Disable RSTP.	switch(config)#no rstp

Message: ERROR: Another redundancy protocol is running. Only one could be run at the same time.

6.7 QoS Commands

Command	Level	Description	Example
qos policy [weighted-fair|strict]	G	Select QOS policy scheduling	switch(config)#qos policy weighted-fair switch(config)#qos policy strict
qos prioritytype [port-based|cos-only|tos-only|cos-first|tos-first]	G	Setting of QOS priority type	switch(config)#qos prioritytype port-based
qos priority portbased [Port] [lowest|low|middle|high]	G	Configure Port-based Priority	switch(config)#qos priority portbased 1 low
qos priority cos [Priority][lowest|low|middle|high]	G	Configure COS Priority	switch(config)#qos priority cos 22 middle
qos priority cosportdefault [Port][Priority]	G	Configure COS Port default	switch(config)#qos priority cosportdefault Port
qos priority tos [Priority][lowest|low|middle|high]	G	Configure TOS Priority	switch(config)#qos priority tos 3 high
show qos	P	Display the information of QoS configuration	switch>show qos
no qos	G	Disable QoS function	switch(config)#no qos

6.8 IGMP Commands

Command	Level	Description	Example
igmp [v2 | v3]	G	Enable IGMP v2 or v3 snooping function	switch(config)#igmp v2 switch(config)#igmp v3
igmp query enable	G	Enable IGMP query	switch(config)#igmp query enable
igmp query-interval [1~250 sec.]	G	Configure Query Interval	switch(config)#igmp query-interval 100
igmp last-query-count	G	Configure Last Member Query Count	switch(config)#igmp last-query-count 1
igmp last-query-interval	G	Configure Last Member Query Interval	switch(config)#igmp last-query-interval 80
igmp query-response-interval	G	Configure Query Response Interval	switch(config)#igmp query-response-interval 175
igmp router-port [portlist]	G	Configure static IGMP router ports	switch(config)#igmp router-port 3
igmp unregister blocking	G	Set unregister stream blocking	switch(config)#igmp unregister blocking
igmp unregister flooding	G	Set unregister stream flooding	switch(config)#igmp unregister flooding
show igmp configuration	P	Displays the details of an IGMP configuration.	switch#show igmp configuration
show igmp table	P	Displays details of IGMP snooping table.	switch#show igmp table
no igmp	G	Disable IGMP snooping function	switch(config)#no igmp
no igmp-query	G	Disable IGMP query	switch#no igmp-query

6.9 MAC/Filter Table Commands

Command	Level	Description	Example
mac-address-table static hwaddr [MAC]	I	Configure MAC address table of interface (static).	switch(config)#interface fastEthernet 2 switch(config-if)#mac-address-table static hwaddr 000012345678
mac-address-table filter hwaddr [MAC]	G	Configure MAC address table(filter)	switch(config)#mac-address-table filter hwaddr 000012348678 switch(config)#mac-address-table filter hwaddr 112233445566
mac agingtime [0|1|2|3|5|10|20|30|60 minutes]	G	Configure mac address table aging time	switch(config)#mac agingtime 10
mac-address-table auto-flush [enable|disable]	G	Auto flush mac address table when ports link down	switch(config)#mac-address-table auto-flush disable
show mac-address-table	P	Show all MAC address table	switch#show mac-address-table
show mac-address-table static	P	Show static MAC address table	switch#show mac-address-table static
show mac-address-table filter	P	Show filter MAC address table.	switch#show mac-address-table filter
no mac-address-table static hwaddr [MAC]	I	Remove an entry of MAC address table of interface (static)	switch(config)#interface fastEthernet 2 switch(config-if)#no mac-address-table static hwaddr 000012345678
no mac-address-table filter hwaddr [MAC]	G	Remove MAC address table entry (filter)	switch(config)#no mac-address-table filter hwaddr 000012348678
no mac-address-table	G	Remove dynamic entry of MAC address table	switch(config)#no mac-address-table

6.10 SNMP Commands

Command	Level	Description	Example
snmp agent-mode [v1|v2c|v3]	G	Select the agent mode of SNMP	switch(config)#snmp agent-mode v1v2c
snmp-server host [IP address] **community** [Community-string] **trap-version** [v1|v2c]	G	Configure SNMP server host information and community string	switch(config)#snmp-server host 192.168.10.50 community public trap-version v1 (remove) Switch(config)#no snmp-server host 192.168.10.50
snmp community-strings [Community-string] **right** [RO|RW]	G	Configure the community string right	switch(config)#snmp community-strings public right RO or switch(config)#snmp community-strings public right RW
snmp snmpv3-user [User Name] **password** [Authentication Password] [Privacy Password]	G	Configure the userprofile for SNMPV3 agent. Privacy password could be empty.	switch(config)#snmp snmpv3-user test01 password AuthPW PrivPW
show snmp	P	Show SNMP configuration	switch#show snmp
show snmp-server	P	Show specified trap server information	switch#show snmp-server
no snmp community-strings [Community]	G	Remove the specified community.	switch(config)#no snmp community-strings public
no snmp snmpv3-user [User Name] **password** [Authentication Password] [Privacy Password]	G	Remove specified user of SNMPv3 agent. Privacy password could be empty.	switch(config)# no snmp snmpv3-user test01 password AuthPW PrivPW
no snmp-server host [Host-address]	G	Remove the SNMP server host.	switch(config)#no snmp-server 192.168.10.50

6.11 802.1x Commands

Command	Level	Description	Example
8021x enable	G	Use the 802.1x global config command to enable 802.1x protocols.	switch(config)# 8021x enable
8021x system radiusip [IP address]	G	Use the 802.1x system radius IP global config command to change the radius server IP.	switch(config)# 8021x system radiusip 192.168.1.1
8021x system serverport [port ID]	G	Use the 802.1x system server port global config command to change the radius server port	switch(config)# 8021x system serverport 1815
8021x system accountport [port ID]	G	Use the 802.1x system account port global config command to change the accounting port	switch(config)# 8021x system accountport 1816
8021x system sharedkey [ID]	G	Use the 802.1x system share key global config command to change the shared key value.	switch(config)# 8021x system sharedkey 123456
8021x system nasid [words]	G	Use the 802.1x system nasid global config command to change the NAS ID	switch(config)# 8021x system nasid test1
8021x misc quietperiod [sec.]	G	Use the 802.1x misc quiet period global config command to specify the quiet period value of the switch.	switch(config)# 8021x misc quietperiod 10
8021x misc txperiod [sec.]	G	Use the 802.1x misc TX period global config command to set the TX period.	switch(config)# 8021x misc txperiod 5
8021x misc supportimeout [sec.]	G	Use the 802.1x misc supp timeout global config command to set the supplicant timeout.	switch(config)# 8021x misc supportimeout 20
8021x misc servertimeout [sec.]	G	Use the 802.1x misc server timeout global config	switch(config)#8021x misc servertimeout 20

		command to set the server timeout.	
8021x misc maxrequest [number]	**G**	Use the 802.1x misc max request global config command to set the Maximum number of requests (1-10).	switch(config)# 8021x misc maxrequest 3
8021x misc reauthperiod [sec.]	**G**	Use the 802.1x misc reauth period global config command to set the reauth period.	switch(config)# 8021x misc reauthperiod 3000
8021x portstate [disable | reject | accept | authorize]	**I**	Use the 802.1x port state interface config command to set the state of the selected port.	switch(config)#interface fastethernet 3 switch(config-if)#8021x portstate accept
show 8021x	**E**	Display a summary of the 802.1x properties and also the port sates.	switch>show 8021x
no 8021x	**G**	Disable 802.1x function	switch(config)#no 8021x

6.12 TFTP Commands

Command	Level	Description	Defaults Example
tftp [server IP] **backup** [file name]	**G**	Backup configuration to TFTP server	switch(config)#tftp 192.168.1.30 backup firmwarex.bin

tftp [server IP] **restore** [file name]	G	Get and restore configuration from TFTP server	switch(config)#tftp 192.168.1.30 restore firmwarex.bin
tftp [server IP] **upgrade** [file name]	G	Update firmware from TFTP server	switch(config)#tftp 192.168.1.30 upgrade firmwarex.bin

6.13 SYSLOG, SMTP, Event Commands

Commands	Level	Description	Example
syslog ip [IP address]	G	Set System log server IP address.	switch(config)# syslog ip 192.168.1.100
syslog mode [client|server|both]	G	Specified the log mode	switch(config)# syslog mode both
show syslog	P	Show system log client & server information	switch#show syslog
no syslog	G	Disable syslog functon	switch(config)#no syslog
smtp enable	G	Enable SMTP function	switch(config)#smtp enable
smtp serverip [IP address]	G	Configure SMTP server IP	switch(config)#smtp serverip 192.168.1.5
smtp authentication	G	Enable SMTP authentication	switch(config)#smtp authentication
smtp account [account]	G	Configure authentication account	switch(config)#smtp account User
smtp password [password]	G	Configure authentication password	switch(config)#smtp password
smtp sender [sendername]		Configure sender of e-mail	switch(config)#smtp sender Bob
smtp subject [subject]		Configure subject of e-mail	switch(config)#smtp subject Meeting
smtp rcptemail [Index] [Email address]	G	Configure Rcpt e-mail Address	switch(config)#smtp rcptemail 1 Alert@test.com

show smtp	**P**	Show the information of SMTP	switch#show smtp
no smtp	**G**	Disable SMTP function	switch(config)#no smtp
event device-restart [Syslog|SMTP]	**G**	Set cold start event	switch(config)#event device-restart syslog
event authentication-failure [Syslog|SMTP]	**G**	Set Authentication failure event type	switch(config)#event authentication-failure syslog
event ring-topology-change [Syslog|SMTP]	**G**	Set Redundant Ring topology changed event type	switch(config)#event ring-topology-change syslog
event power-status [Syslog|SMTP]	**G**	Set power status event type	switch(config)#event power-status smtp
show event	**P**	Show event selection	switch#show event
no event device-cold-start	**G**	Disable cold start event type	switch(config)#no event device-cold-start
no event authentication-failure	**G**	Disable Authentication failure event typ	switch(config)#no event authentication-failure
no event ring-topology-change	**G**	Disable Ring topology changed event type	switch(config)#no event ring-topology-change
no event power-status		Disable power status event type	switch(config)#no event power-status syslog
no event syslog	**I**	Disable port event for system log	switch(config)#interface fastethernet 3 switch(config-if)#no event syslog
no event smpt	**I**	Disable port event for SMTP	switch(config)#interface fastethernet 3 switch(config-if)#no event smtp

6.14 SNTP Commands

Command	Level	Description	Example
sntp server-ip [IP-address] [Timezone(1~63)]		Enable and set SNTP server IP address and timezone	switch(config)#sntp server-ip 192.168.1.30 timezone 22

sntp daylight [Start time] [End time] (Format:yyyymmdd-hh:mm)	G	Enable daylight saving time, if SNTP function is inactive, this command can't be applied.	switch(config)#sntp daylight period 20171013-12:01 201806-12:59 offset 1
sntp daylight-period [Start time] [End time]	G	Set period of daylight saving time, if SNTP function is inactive, this command can't be applied. Parameter format: [yyyymmdd-hh:mm]	switch(config)# sntp daylight-period 20060101-01:01 20060202-01-01
sntp daylight-offset [Minute]	G	Set offset of daylight saving time, if SNTP function is inactive, this command can't be applied.	switch(config)#sntp daylight-offset 3
show sntp	P	Display SNTP info.	switch#show sntp
show sntp timezone	P	Display index number of time zone list.	switch#show sntp timezone
no sntp	G	Disable SNTP function	switch(config)#no sntp
no sntp daylight	G	Disable daylight saving time	switch(config)#no sntp daylight

6.15 Ring (Redundancy) Commands

Command	Level	Description	Example
ring enable	G	Enable Red. Ring	switch(config)# ring enable
ring master	G	Enable ring master	switch(config)# ring master
ring coupling-ring	G	Enable couple ring	switch(config)# ring coupling-ring
ring dual-homing	G	Enable dual homing	switch(config)# ring dual-homing
ring port [1st Ring Port] [2nd Ring Port]	G	Configure 1st/2nd Ring Port	switch(config)# ring ringport 7 8
ring coupling-port [Coupling Port]	G	Configure Coupling Port	switch(config)# ring coupling-port 1

ring homing-port [Dual Homing Port]	**G**	Configure Dual Homing Port	switch(config)# ring homing-port 3
show ring	**P**	Display Redundant Ring information.	switch#show ring
no ring	**G**	Disable Red. Ring	switch(config)#no ring
no ring master	**G**	Disable ring master	switch(config)# no ring master
no ring coupling-ring	**G**	Disable couple ring	switch(config)# no ring coupling ring
no ring dual-homing	**G**	Disable dual homing	switch(config)# no ring dual-homing
check-concurrence [Enable|Disable]	**G**	Check redundancy protocol concurrence	switch(config)#check-concurrence enable
multi-ring enable	**G**	Enable Multi-Ring	switch(config)#multi-ring enable
multi-ring port [1st ring port] [2nd ring port]	**G**	Configure 1st/2nd ring ports	switch(config)#multi-ring port 2 3
multi-ring vendor [Moxx|Advantexx|Hirschmaxx]	**G**	Configure Multi-Ring vendor	switch(config)#multi-ring vendor Hirschmaxx
multiple-ring edge-port [port id, 0:inactive]	**G**	Configure edge port connected to Redundant Ring	switch(config)#multiple-ring edge-port 2
multiple-ring enable	**G**	Enable Multiple Ring	switch(config)#multiple-ring enable
multiple-ring uplink-port [1st port] [2nd port]	**G**	Configure 1st/2nd uplink ports	switch(config)#multiple-ring uplink-port 1 2

Messages:

ERROR: Another redundancy protocol is running. Only one could be run at the same time

ERROR: The edge port should be one of uplink ports

6.16 Security Commands

Firmware version 1.28 added these security CLI commands: security https, security ssh, no security https, and no security ssh. The security commands are described below.

Command	Level	Description	Example
security https	G	Enable HTTPS security	switch(config)# security https
security ssh	G	Enable SecureShell	switch(config)# security ssh
no security https	G	Disable HTTPS security	switch(config)# no security https
no security ssh	G	Disable SecureShell	switch(config)# no security ssh
security enable	G	Enable IP security function	switch(config)#security enable
security http	G	Enable HTTP server	switch(config)#security http
security ip	G	Set IP security list	switch(config)#security ip [Index(1..10)] [IPAddr]
security snmp	G	Enable SNMP server	switch(config)#security snmp
security telnet	G	Enable TELNET server	switch(config)#security ssh
show security	E	Display current security	switch#show security

6.17 TACACS+ Commands

Firmware version 1.28 added these TACACS+ commands:

Command	Level	Description	Example
tacacs+ add	G	Add TACACS+ Server	switch(config)#tacacs+ add server-ip 192.168.1.30 port 3 secret-key ola22
tacacs+ authentication	G	Client authentication method	switch(config)#tacacs+ authentication web local
tacacs+ disable	G	Disable TACACS+ Server	switch(config)#tacacs+ disable server-ip 192.168.1.30
tacacs+ enable	G	Enable TACACS+ Server	switch(config)#tacacs+ enable server-ip 192.168.1.30
show tacacs+	E	Display current TACACS+ settings	switch#show tacacs+
no tacacs+ server-ip	G	Disable TACACS+ Server IP	switch(config)#no tacacs+ server-ip 192.168.1.30

6.18 Auto SFP Commands

Firmware version 1.28 added these auto-sfp commands:

Command	Level	Description	Example
auto-sfp disable	G	Disable auto detect 100/1000 SFP	switch(config)#auto-sfp disable
auto-sfp enable	G	Enable auto detect 100/1000 SFP	switch(config)#auto-sfp enable
show sfp	E	Display the current SFP Monitoring settings	switch#show sfp-monitor
no sfp-monitor-alarm	G	Disable SFP temperature alarm	switch(config)#no sfp-monitor-alarm

6.19 PTP Protocol Commands

Firmware version 1.28 added these PTP (Precision Timing Protocol) commands:

Command	Level	Description	Example
ptp enable	G	Enable PTP function	switch(config)#ptp enable
show ptp	E	Show PTP state	switch#show ptp
no ptp	G	Disable PTP	switch(config)#no ptp

6.20 Fault-Relay Commands

Firmware version 1.28 added these commands to view and configure the Fault Relay Alarm for power failure:

Command	Level	Description	Example
Fault-relay enable	G	Enable Fault relay alarm function	switch(config)#fault-relay power 1 enable
Fault-relay disable	G	Disable Fault relay alarm function	switch(config)#fault-relay power 1 disable
Show fault-relay	E	Show Fault Relay Alarm setting	switch#show fault-relay
No fault-relay	G	Disable Fault Relay Alarm function	switch(config)#no fault-relay

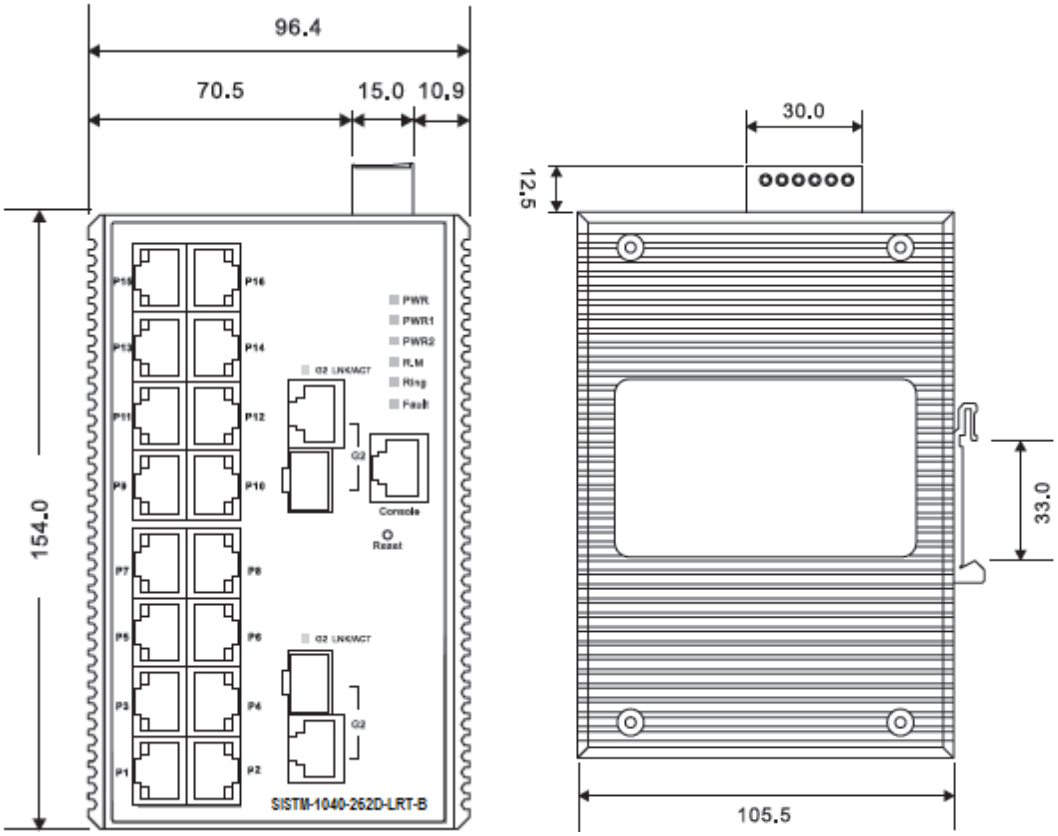
Message: Error power no.

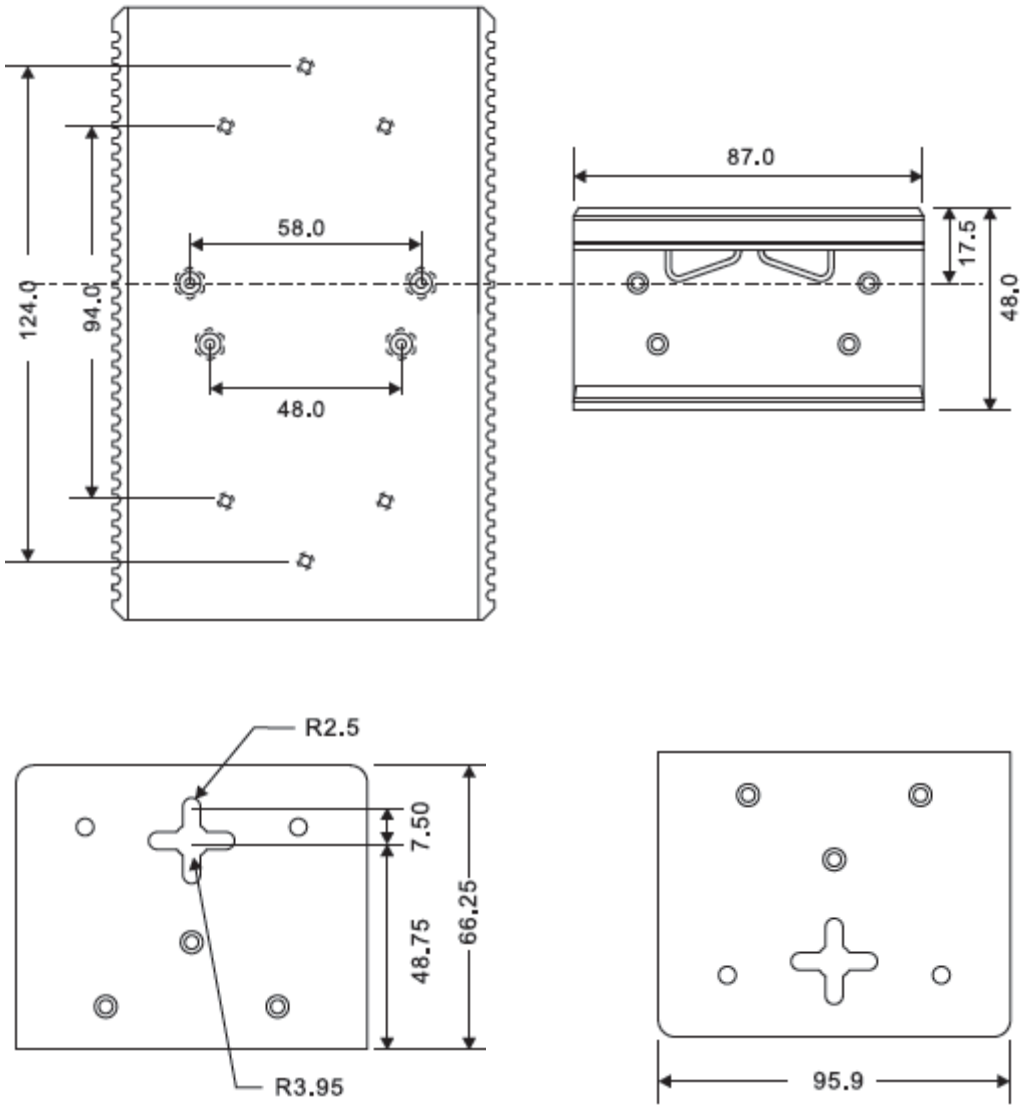
7. Technical Specifications

Technology	
Ethernet Standards	802.3 - 10Base-T, 802.3u - 100Base-TX, 100Base-FX, 802.3z - 1000Base-LX, 802.3ab - 1000Base-TX, 802.3ad - Link Aggregation Control Protocol 802.3x - Flow Control 802.1D - Spanning Tree Protocol 802.1p - Class of Service, 802.1Q - VLAN Tagging 802.1w - Rapid Spanning Tree Protocol, 802.1X - Authentication 802.1ad - VLAN QinQ 802.1AB - LLDP 802.1s - MSTP
MAC addresses	8192
Priority Queues	4
Flow Control	IEEE 802.3x Flow Control and Back-pressure
Processing	Store-and-Forward
Interface	
RJ45 Ports	10/100Base-T(X), Auto MDI/MDI-X
Giga SFP Ports	1000 Base-SFP & 1000 Base-T(X) combo
LED Indicators	Per Unit : Power x 3(Green) RJ45 Ports: Per Port : Link/Activity(Green/Blinking Green), Full duplex(Amber) Giga SFP Ports: Per Port : Activity(Green), Link (Green)
Power Requirements	
Power Input Voltage	PWR1/2: 12-48VDC in 6-pin Terminal Block
Reverse Polarity Protection	Not Present
Power Consumption	12 Watts
Environmental	
Operating Temperature	-40 °C to +70 °C
Storage Temperature	-40 °C to +85 °C
Operating Humidity	5% to 95%, non-condensing
Weight	3.85 Lbs. (1.75 Kg.)
Mechanical	
Dimensions(W x D x H)	96.4(W)x108.5(D)x154(H) mm (3.8 x 4.27 x 6.06 In.)
Casing	IP-30 protection

Regulatory Approvals	
Regulatory Approvals	FCC Part 15, CISPER (EN55022) class A
EMS	EN61000-4-2 (ESD), EN61000-4-3 (RS), EN61000-4-4 (EFT), EN61000-4-5 (Surge), EN61000-4-6 (CS), EN61000-4-8,EN61000-4-11
Shock	IEC 60068-2-27
Free Fall	IEC 60068-2-32
Vibration	IEC 60068-2-6
Warranty	Limited Lifetime

Dimensions




87.0
58.0
124.0
94.0
48.0
17.5
48.0
R2.5
7.50
48.75
66.25
R3.95
95.9

8. Troubleshooting

This section provides information to troubleshoot problems by taking actions based on the symptom. Many problems are caused by the following situations. Check for these items first when you start troubleshooting:

1. Make sure your switch model supports the feature or function attempted; see Software Features on page 7.
2. Verify the install process; see Installation Instructions on page 13.
3. Verify the initial switch installation; see Configuration by Web Browser on page 176 or Command Line Interface Management on page 93.
4. Troubleshoot connected network devices to pinpoint the problem to the switch.
5. Check LED status; see Front Panel LEDs on page 12. If the Power LED is Off, check connections between the switch, the power cord and the wall outlet. If the Link LED is Off, verify that the switch and attached device are powered on and be sure the cable is plugged into the switch and corresponding device. If the switch is installed in a rack, check the connections to the punch-down block and patch panel.
6. Check the cabling; look for faulty or loose cables and look for non-standard and miswired cables.
7. Verify that the proper cable type is used and its length does not exceed specified limits. Check the adapter on the attached device and cable connections for possible defects. Replace the defective adapter or cable if necessary.
8. Run the System Diagnostics. See the Web GUI section or the CLI section of this manual.
9. If using the CLI, try configuring / testing via the Web UI and vice versa. See the Web GUI section or the CLI section.
10. Make sure you have a valid network topology; check for improper Network Topologies, and make sure that your network topology contains no data path loops.
11. Check the port configuration; make sure ports have not been put into a “blocking” state by Spanning Tree, GVRP, or LACP. The normal operation of the Spanning Tree, GVRP, and LACP features may put the port in a blocking state. Verify that the port has not been configured as disabled via software.
12. Make sure connected devices (e.g., SFPs, switches, hubs) are cabled, powered, and operating properly.
13. Record model and system information (see below).

Record Device and System Information

After performing troubleshooting, and before calling or emailing Technical Support, please record as much information as possible to help the Tech Support Specialist.

1. Select the **System Information** page. From the CLI, use the **show** commands needed to gather the information below or as requested by the Tech Support Specialist.

2. Record Model Information: Model Name: _____

Serial Number: _____ Firmware Version: _____

3. Record LED Status: _____ _____

_____

4. Provide additional information to your Tech Support Specialist. See the "Troubleshooting" section above.

Your Transition Networks service contract number: _____

Describe the failure: _____

_____

_____

Describe any action(s) already taken to resolve the problem (e.g., changing mode, rebooting, etc.):

_____

_____

_____

The serial and revision numbers of all involved Transition Networks products in the network:

_____

_____

Describe your network environment (layout, cable type, etc.): _____

_____

_____

Network load and frame size at the time of trouble (if known): _____

_____

The device history (i.e., have you returned the device before, is this a recurring problem, etc.):

_____

_____

Any previous Return Material Authorization (RMA) numbers: _____

_____

9. Regulatory Agency Information

Regulatory approvals

EMI FCC Part 15, CISPR (EN55022) Class A

EMS EN61000-4-2 (ESD)

EN61000-4-3 (RS), EN61000-4-4 (EFT), EN61000-4-5 (Surge), EN61000-4-6 (CS),

EN61000-4-8, EN61000-4-11, EN60079-0:2012+A11:2013, EN 60079-15:2010

Shock IEC60068-2-27

Free Fall IEC60068-2-32

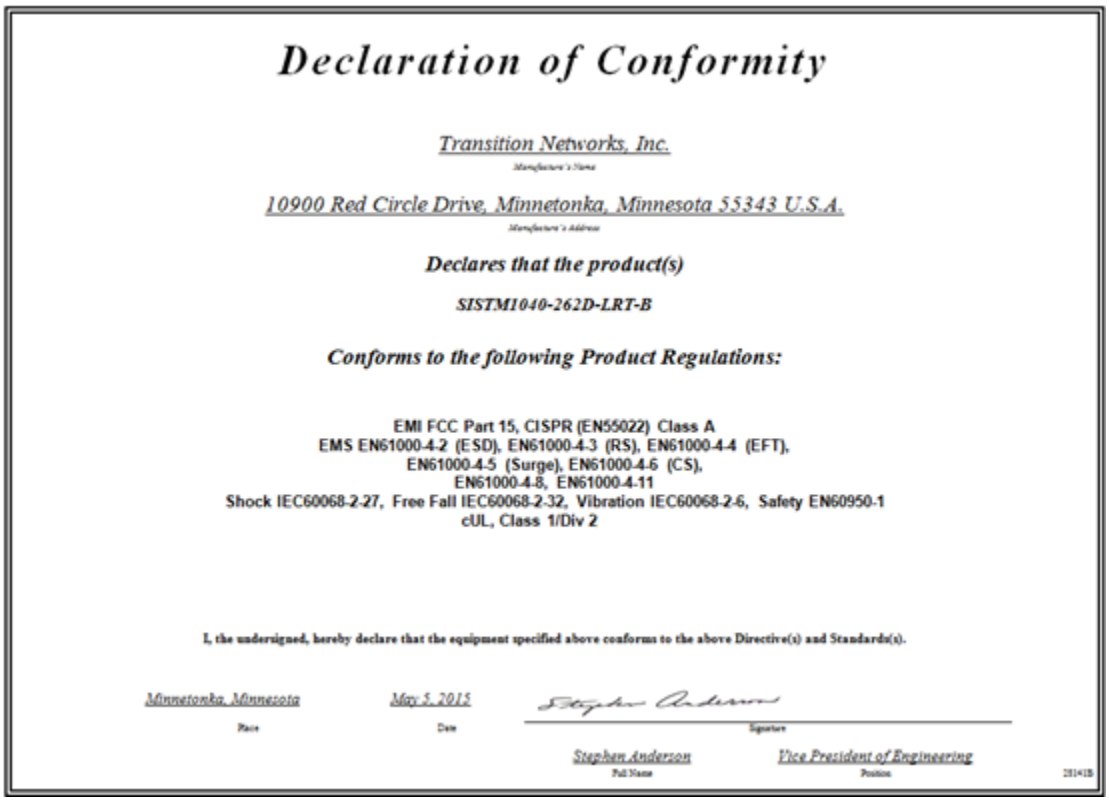
Vibration IEC60068-2-6

Safety EN60950-1

cUL

Class 1/Div 2

Declaration of Conformity



Declaration of Conformity

Transition Networks, Inc.
Manufacturer's Name

10900 Red Circle Drive, Minnetonka, Minnesota 55343 U.S.A.
Manufacturer's Address

Declares that the product(s)

SISTM1040-262D-LRT-B

Conforms to the following Product Regulations:

EMI FCC Part 15, CISPR (EN55022) Class A
EMS EN61000-4-2 (ESD), EN61000-4-3 (RS), EN61000-4-4 (EFT),
EN61000-4-5 (Surge), EN61000-4-6 (CS),
EN61000-4-8, EN61000-4-11
Shock IEC60068-2-27, Free Fall IEC60068-2-32, Vibration IEC60068-2-6, Safety EN60950-1
cUL, Class 1/Div 2

I, the undersigned, hereby declare that the equipment specified above conforms to the above Directive(s) and Standards(s).

Minnetonka, Minnesota — Place
May 5, 2015 — Date
Signature
Stephen Anderson — Full Name
Vice President of Engineering — Position

10. Differences between -A and -B Models

Feature	-A Model	-B Model
10/100Base-T Ports	16	16
100/1000Base-X Ports	2 Combo	2 Combo
Serial Console Port	√	√
Auto MDI	√	√
Auto Negotiation	√	√
Input Power Range	12~48VDC	12~48VDC
Relay Output		24Vdc, 1A
Reverse Polarity Protection	√	√
Overload Protection	√	√
Fault Relay	√	√
IEEE802.1AB LLDP		√
IEEE802.1D STP	√	√
IEEE802.1p COS (Class of Service)	√	√
IEEE802.1Q VLAN Tagging	√	√
IEEE802.1s MSTP		√
IEEE802.1w RSTP	√	√
IEEE802.1x RADIUS	√	√
IEEE802.3	√	√
IEEE802.3ab	√	√
IEEE802.3ad LACP	√	√
802.3af PoE		
802.3at PoE+		
IEEE802.3u	√	√
IEEE802.3x Flow Control	√	√
IEEE802.3z	√	√
MAC Table	8k	8192
Priority Queues		4
Processing	Store and Forward	Store and Forward
Switching Latency		9µs
Switching Bandwidth		7.2Gbps
IGMP snooping/query	√	1024 Groups
SNMPv1/v2/v3	√	√

SNTP	√	√
DHCP	√	√
PTP		√
MVR		√
SMTP		√
GVRP	√	√
VLAN	√	4096
Redundant Ring		√
Coupling Ring	√	
Dual Homing	√	√
Coupling Ring	√	√
MRP		√
IP Access Security	√	√
Port and IP Binding	√	√
SSL	√	
SYSLOG	√	√
IPv4/IPv6	√	√
Power LEDS	Power, P1, P2	Power, P1, P2
Ring Master LED	1	1
Ring Indicator		1
Fault Indicator	1	1
10/100/1000Base-T Link/Act/100Mbps	1/Port	1/Port
100/1000Base-X Link/Act	1/Port	1/Port
Enclosure	IP-30	IP-30
Dimensions	79 X 105 X 152	96.4 X 108.5 X 154
Operating Temperature	-40^{0}C to +75^{0}C	-40^{0}C to +60^{0}C
MTBF	295000 Hrs	181,205 Hrs

Feature	-A Model	-B Model
FCC Part 15	√	√
CISPR(EN55022) class A	√	√
EN61000-4-2 (ESD)	√	√
EN61000-4-3 (RS)	√	√
EN61000-4-4 (EFT)	√	√
EN61000-4-5 (Surge)	√	√
EN61000-4-6 (CS)	√	√
EN61000-4-8	√	√
EN61000-4-11		√
IEC60068-2-27 (Shock)	√	√
IEC60068-2-32 (Free Fall)	√	√
IEC60068-2-6 (Vibration)	√	√
IEC61000-6-2		
IEC61000-6-4		
UL	√	√
UL508		
cUL	√	√
Class 1/Div 2		√
CE Mark	√	√
GL		

12. Power Supply Information

These External AC/DC power supply models (sold separately) are available from Lantronix.

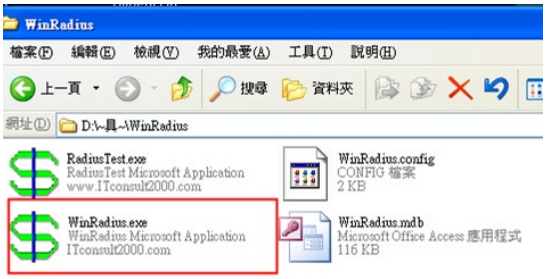
- 25165 (Universal AC/DC Input DIN Rail Mountable; +12 VDC Power Supply. See the related product page.
- SPS-UA12DHT (Input: 90 ~ 264 VAC; Output: 12 VDC, 1.3A, 18 Watts; 0ºC to +70ºC operating temperature). See the related product page.

13. RADIUS Server and Switch Settings

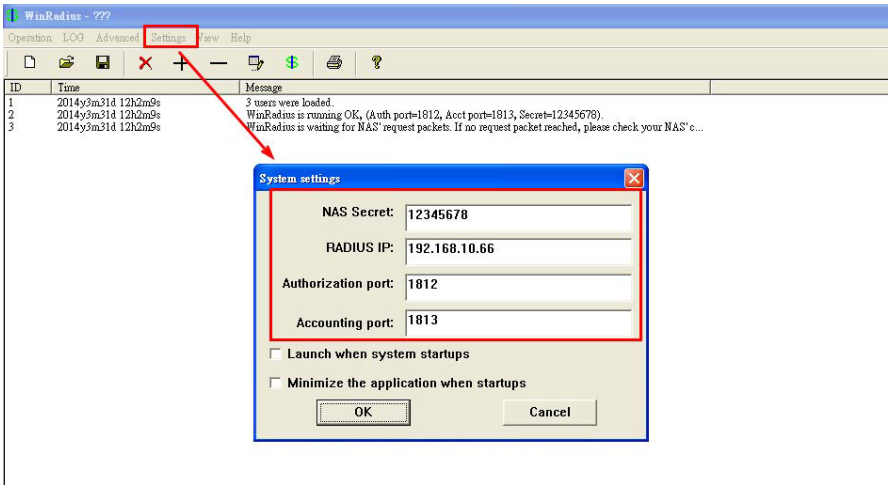
This section provides MS WinRadius and Windows / PC settings. See "802.1x - Radius Server" for the switch RADIUS parameter descriptions.

RADIUS Server and Switch Setting

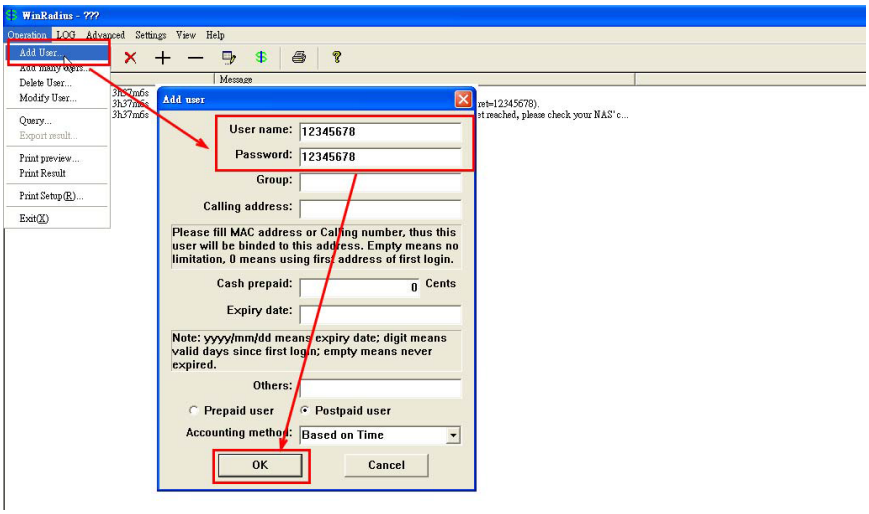
1. Enable the WinRadius tool.



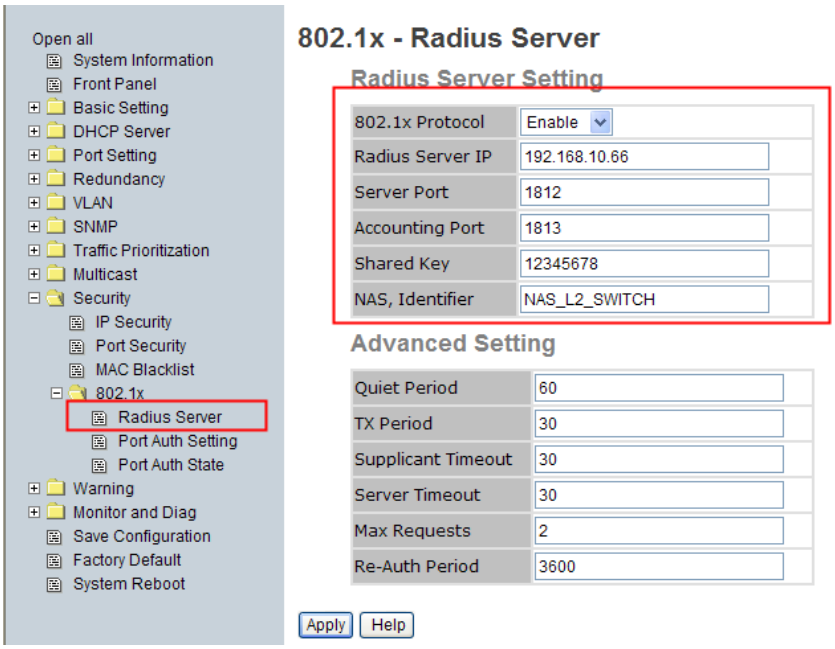
2. Set the Radius Server IP、NSA and Port.



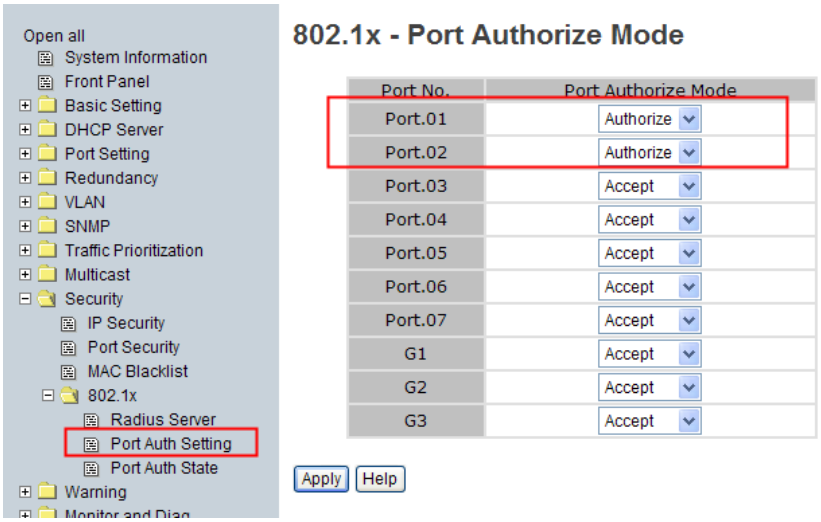
3. Create a new User.



4. Enter the Switch Radius Server settings. Note: all settings need the same Radius Server settings.



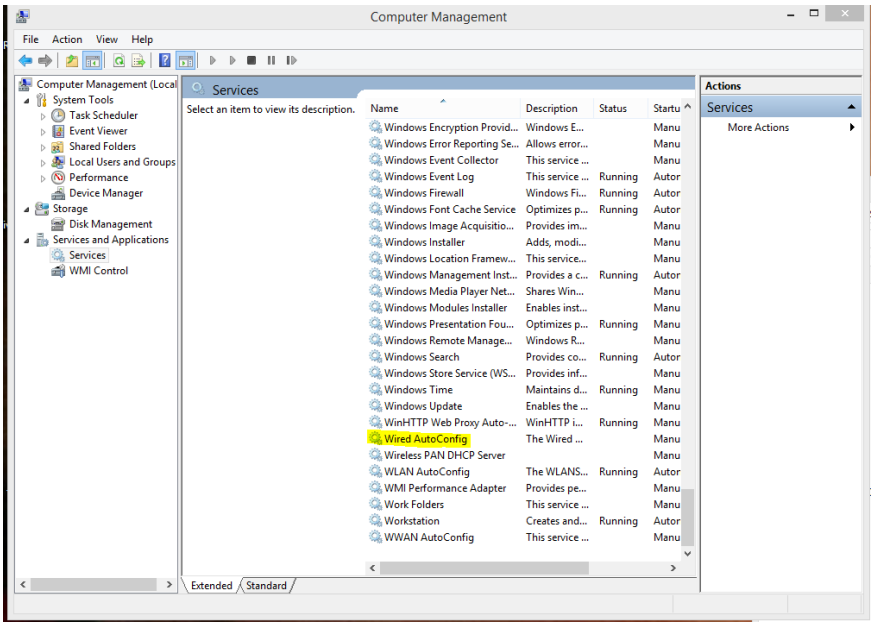
5. Select 802.1x Authorize Port (e.g., select Port 1 and Port 2 = Authorize).



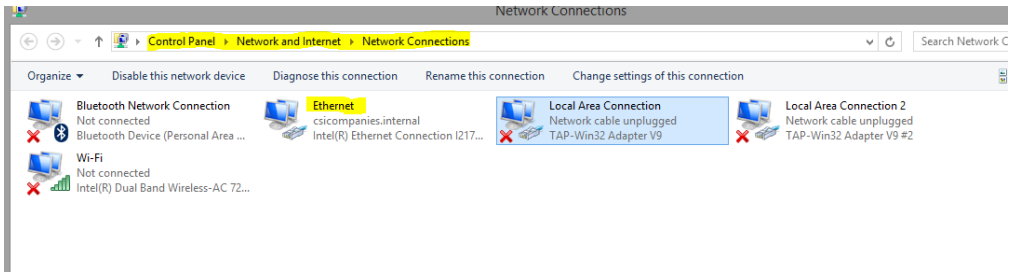
6. Continue with the User PC Setting section below.

User PC Settings

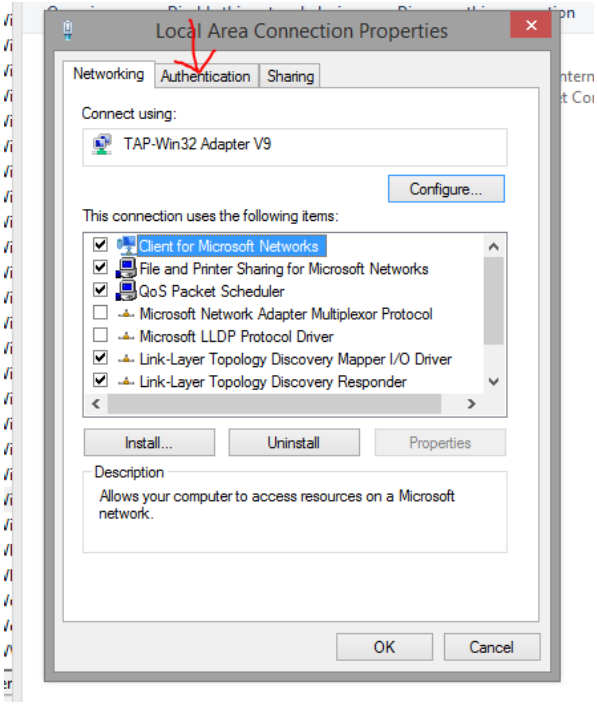
1. Enable Windows 802.1x Services: To complete this procedure, you must first enable the Wired AutoConfig service, which is turned off by default.
   a. Click the **Start** button. In the search box, type **services.msc**, and then press Enter. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.
   b. In the Services dialog box, click the **Standard** tab at the bottom of main pane, right-click **Wired AutoConfig**, and then click **Start**.

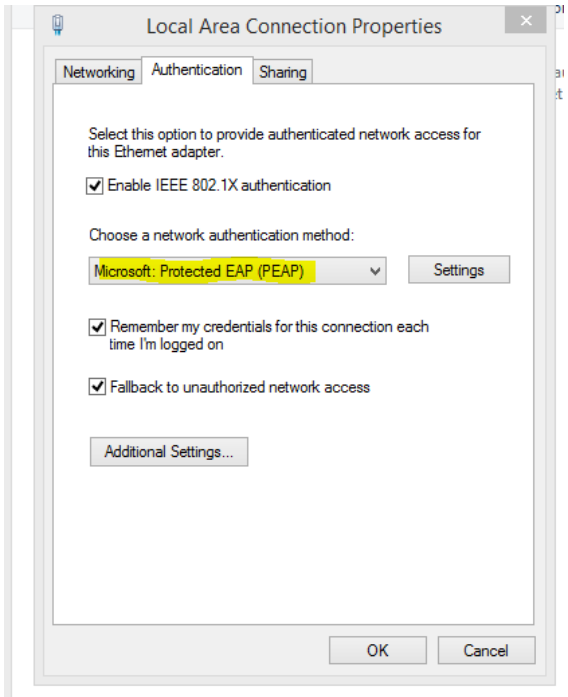


   c. Open Network Connections by clicking the **Start** button, and then clicking **Control Panel**. In the search box, type **adapter**, and then, under Network and Sharing Center, click **View network connections**.
   d. Right-click the connection that you want to enable 802.1X authentication for, and then click **Properties**. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.



a. Click the **Authentication** tab, and then select the **Enable IEEE 802.1X authentication** check box.



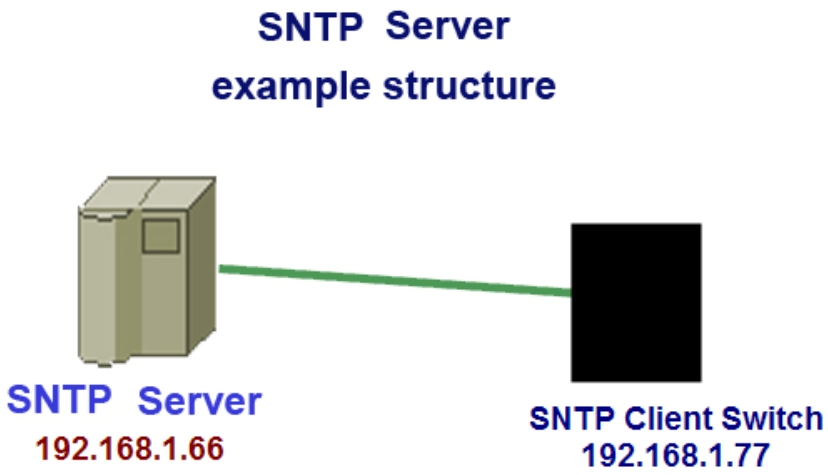


b. In the **Choose a network authentication method** list, click the method you want to use.

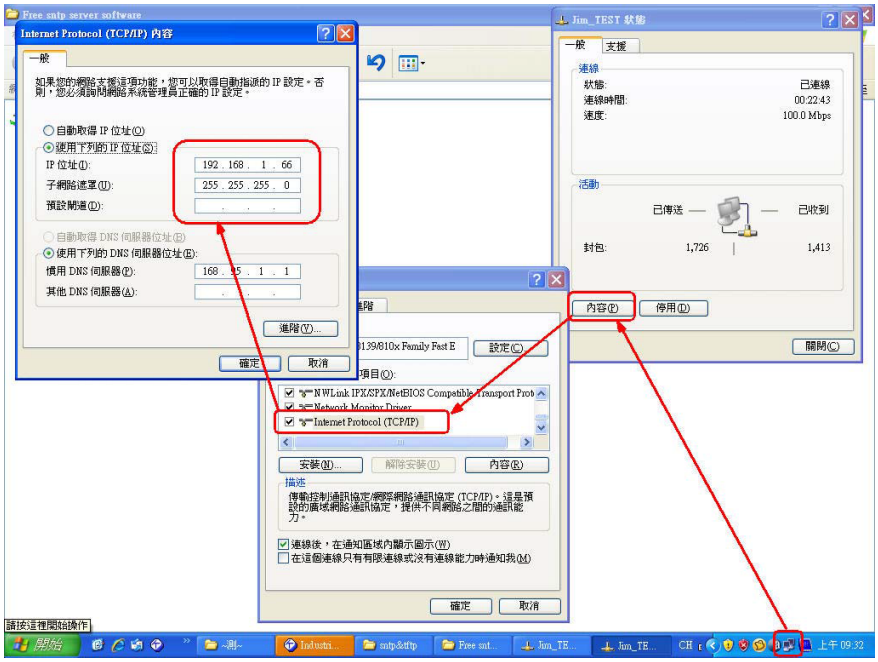
To configure additional settings, click **Settings**.

14. SNTP Server Setup

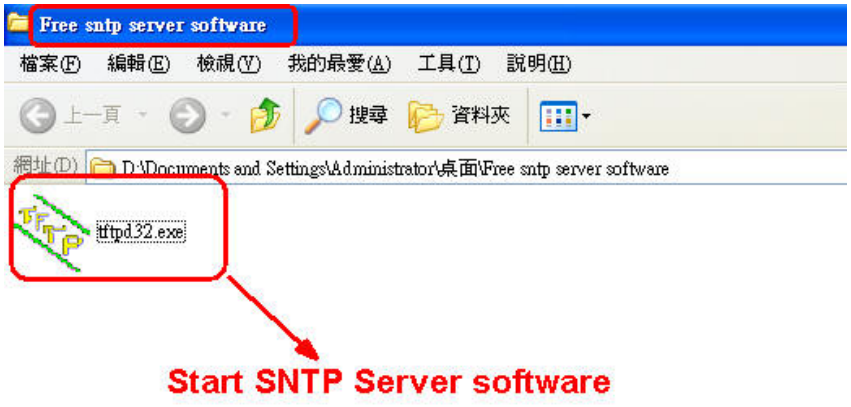
This section provides a sample setup procedure for the following SNTP server/client configuration.



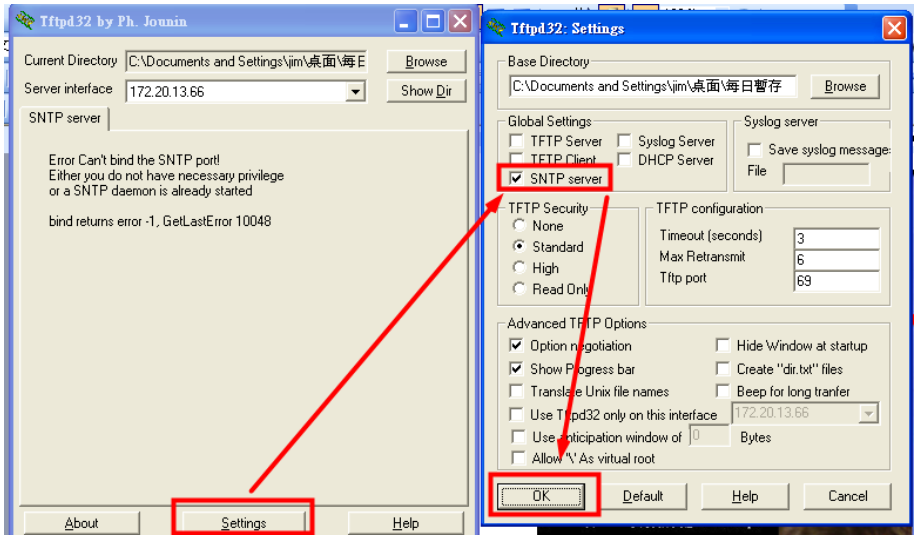
1. Set up IP of PC (e.g., 192.168.1.66 / 24).



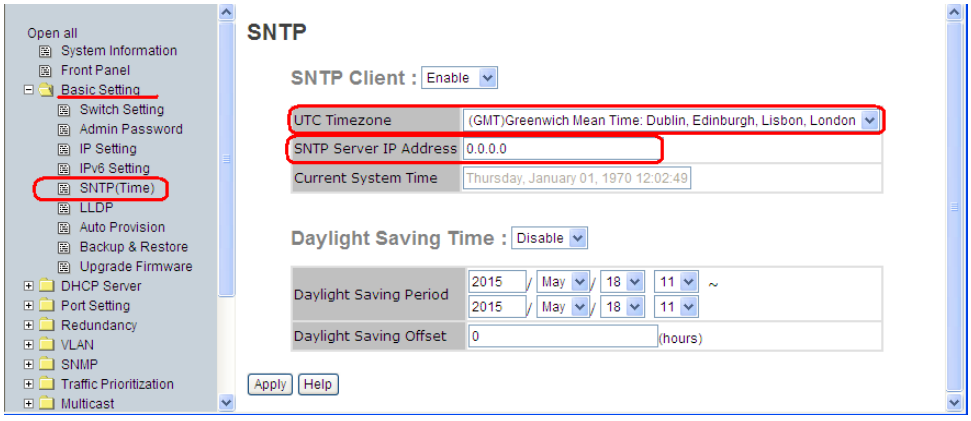
2. Start the SNTP Server software, making the PC into an SNTPand Syslog Server (this example uses the free tool tftpd32).



3. Confirm whether to open the SNTP function.



4. Set up and finish, then restart the software.
5. At the **Basic Setting** > **SNTP(Time)** page, set the SNTP Server IP Address and the set the UTC Timezone, and click the **Apply** button.



6. Observe the system time at the **System Information** page in the System Timezone Offset field.

Lantronix Corporate Headquarters

7535 Irvine Center Drive

Suite100

Irvine, CA 92618, USA

Toll Free: 800-526-8766

Phone: 949-453-3990

Fax: 949-453-3995

Technical Support

+1.952.358.3601, 1.800.260.1312, or techsupport@transition.com

Sales Offices

For a current list of our domestic and international sales offices, go to the Lantronix web site at www.lantronix.com/about/contact.