



SISTM1040-173D-LRT

Hardened Managed Ethernet Switch

TRANSITION NETWORKS SISTM1040-173D-LRT

(7) 10/100Base-TX Ports and (3) 100/1000Base-X Combo SFP Ports

System Name	SISTM1040-173D-LRT
System Description	(7) 10/100Base-TX Ports and (3) 100/1000Base-X Combo SFP Ports
System Location	
System Contact	
System OID	1.3.6.1.4.1.868.2.120.0.0.51
Firmware Version	v1.30
Kernel Version	v3.50
MAC Address	00-C0-F2-5A-40-00

Close

User Guide

33678 Rev. A

Trademarks

All trademarks and registered trademarks are the property of their respective owners.

Copyright Notice/Restrictions

Copyright© 2016 Transition Networks. All rights reserved.No part of this work may be reproduced or used in any form or by any means (graphic, electronic or mechanical) without written permission from Transition Networks. The information contained herein is confidential property of Transition Networks, Inc. The use, copying, transfer or disclosure of such information is prohibited except by express written agreement with Transition Networks, Inc. Printed in the U.S.A.

SISTM1040-173D-LRT Hardened Managed Ethernet Switch User Guide, 33678 Rev. A

Revision History

Rev	Date	Description
A	7/22/16	Initial release at Firmware Version v1.30.

Contact Information

Transition Networks

10900 Red Circle Drive

Minnetonka, MN 55343 USA

Tel: 952-941-7600 or 1-800-526-9267

Fax: 952-941-2322

Web: <https://www.transition.com>

Table of Contents

- 1. Getting Started.....7**
 - 1.1 About the SISTM1040-173D-LRT7
 - 1.2 Software Features7
 - 1.3 Hardware Features7
 - 1.4 Safety Precautions and Warnings7
 - 1.5 Package Contents8
 - 1.6 Unpacking.....8
 - 1.7 Dimensions9
 - 1.8 Related Information.....9
- 2. Hardware Installation8**
 - 2.1 DIN-Rail Mounting8
 - 2.1.1 DIN-Rail Mount Procedure.....9
 - 2.2 Wall Mounting9
 - 2.2.1 Wall Mount Dimensions.....9
- 3. Hardware Overview10**
 - 3.1 Front Panel 10
 - 3.2 Front Panel LEDs 11
 - 3.3 Top Panel..... 12
 - 3.4 Warnings..... 12
 - 3.5 Wiring..... 13
 - 3.4.1 Fault Relay Contacts 13
 - 3.4.2 Grounding..... 13
 - 3.4.3 Redundant Power Inputs..... 13
- 4. Cables14**
 - 4.1 Ethernet Cables 14
 - 4.1.1 100BASE-TX/10BASE-T Pin Assignments..... 14
 - 4.2 SFPs 15
 - 4.3 Console Cable 16
- 5. Web Management17**
 - 5.1 Configuration by Web Browser 17
 - 5.1.1 About Web-based Management 17
 - 5.1.2 System Information 19
 - 5.1.3 Basic Setting 20
 - 5.1.3.1 Switch Setting..... 20

5.1.3.2	Admin Password	21
5.1.3.3	IP Setting	22
5.1.3.4	SNTP (Time).....	23
5.1.3.5	PTP Client	26
5.1.3.6	LLDP	27
5.1.3.7	Auto Provision	28
5.1.3.8	Backup & Restore	29
5.1.3.9	Upgrade Firmware.....	30
5.1.3.10	Upgrade HTTPS Certification.....	31
5.1.5	Redundancy.....	32
5.1.5.1	Redundant Ring	32
5.1.5.1	Multiple Ring.....	36
5.1.5.2	Multi-Ring	37
5.1.5.3	RSTP Setting.....	38
5.1.5.4	RSTP.....	39
5.1.5.5	MSTP	44
5.1.6	Multicast.....	53
5.1.6.1	IGMP Snooping	53
5.1.5.1	Static Group	54
5.1.6	Port Setting	55
5.1.6.1	Port Control	55
5.1.6.2	Port Status.....	56
5.1.6.3	Rate Limit	57
5.1.6.4	Port Trunk.....	58
5.1.7	VLAN.....	62
5.1.7.1	VLAN Setting - IEEE 802.1Q	62
5.1.7.2	VLAN Setting – Port Based.....	64
5.1.7.3	VLAN Table	66
5.1.8	Traffic Prioritization	67
5.1.8.1	Qos Policy	68
5.1.8.2	Port-based Priority.....	69
5.1.8.3	COS/802.1p.....	70
5.1.8.4	TOS/DSCP	71
5.1.9	DHCP Server	72
5.1.9.1	DHCP Server – Basic Setting	72
5.1.9.2	DHCP Server – Client List.....	73

5.1.9.3	DHCP Server – Port and IP Binding	74
5.1.10	SNMP	75
5.1.10.1	SNMP – Agent Setting.....	75
5.1.10.2	SNMP –Trap Setting	77
5.1.11	Security	78
5.1.11.1	IP Security	78
5.1.11.2	Port Security.....	79
5.1.11.3	MAC Blacklist	80
5.1.11.4	802.1x.....	81
5.1.12	Warning.....	84
5.1.13	Monitor and Diag	89
5.1.13.1	MAC Address Table.....	89
5.1.13.2	Port Statistics	90
5.1.13.3	Port Monitoring.....	91
5.1.13.4	System Event Log	92
5.1.13.5	SFP Monitor	93
5.1.5	Save Configuration	95
5.1.6	Factory Default.....	95
5.1.7	System Reboot	96
6.	Command Line Interface (CLI)	97
6.1	About CLI Commands	97
6.2	System Commands.....	104
6.3	Port Commands	106
6.4	Trunk Commands.....	108
6.5	VLAN Commands.....	110
6.6	Spanning Tree Commands	112
6.7	QoS Commands.....	114
6.8	IGMP Commands.....	114
6.9	MAC / Filter Table Commands	115
6.10	SNMP Commands	115
6.11	Port Mirroring Commands.....	116
6.12	802.1x Commands.....	117
6.13	TFTP Commands.....	119
6.14	SYSLOG, SMTP, and EVENT Commands	119
6.15	SNTP Commands	122
6.16	Redundant Ring Commands	123

- 6.17 CLI Command Summary..... 124
- 7. Technical Specifications126**
- 8. Troubleshooting.....129**
- 9. Service, Warranty & Tech Support.....130**
 - 9.1 Record Model and System Information..... 130
 - 9.2 Service 132
 - 9.3 Warranty..... 132
- 10. Regulatory Agency Information135**
 - 10.1 Regulatory Approvals 135
 - 10.2 Declaration of Conformity..... 135
- 11. Power Supply Information136**
 - 11.1 Industrial Power Supply 25130..... 136
 - 11.2 Industrial Power Supply 25083..... 137

1. Getting Started

1.1 About the SISTM1040-173D-LRT

The Transition Networks SISTM1040-173D-LRT is a hardened managed switch in a rugged enclosure used at the edge of a hardened network to provide fast Ethernet connections. This switch has (7) 10/100Base-TX ports and (3) combo Gigabit RJ-45/SFP ports. The SFP ports will accept 100MB or Gigabit SFP modules to provide multimode or single mode fiber communications. The SISTM1040-173D-LRT has redundant input power connections, and a fault alarm relay to ensure safe reliable operation in temperatures between -40°C and +70°C.

The SISTM1040-173D-LRT can be managed by Web, Telnet, Console or other third-party SNMP software as well. The switch can be managed by powerful network management software. With its friendly and powerful interface, you can easily configure multiple switches at the same time, and monitor switches' status.

1.2 Software Features

- Redundant Ethernet Ring (Recovery time < 10ms over 250 units connection)
- Supports Ring Coupling, Dual Homing over Redundant Ring
- Supports SNMPv1/v2/v3 & RMON & 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
- SNMPv3 encrypted authentication and access security
- RSTP (802.1w)
- Quality of Service (802.1p) for real-time traffic
- VLAN (802.1Q) with double tagging and GVRP supported
- IGMP Snooping for multicast filtering
- Port configuration, status, statistics, mirroring, security
- Remote Monitoring (RMON)
- PTP Client (Precision Time Protocol) clock synchronization
- 1024 bit encryption key for HTTPS certification

1.3 Hardware Features

- Redundant dual DC power inputs
- Wide Operating Temperature: -40 to 70°C
- Storage Temperature: -40 to 85°C
- Operating Humidity: 5% to 95%, non-condensing
- Casing: IP-30
- 10/100Base-T(X) Ethernet port
- 10/100/1000Base-T(X) Gigabit Ethernet port (combo)
- 1000Base-X on SFP port (combo)
- Console Port

1.4 Safety Precautions and Warnings

- The equipment can only be accessed by service person or users who have been properly and adequately instructed.
- The equipment should be installed in a location that needs a tool or lock and key, or other means of security, under control by a properly authorized person.
- **Elevated Operating Ambient:** If installed in a closed environment, make sure the operating ambient temperature is compatible with the maximum ambient temperature (T_{ma}) specified.
- **Reduced Air Flow:** Make sure the amount of air flow required for safe operation of the equipment is not compromised during installation.
- **Mechanical Loading:** Make sure the mounting of the equipment is not in a hazardous condition due to uneven mechanical loading.
- **Circuit Overloading:** Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

1.5 Package Contents

Contact your point of purchase if you have not received these items:

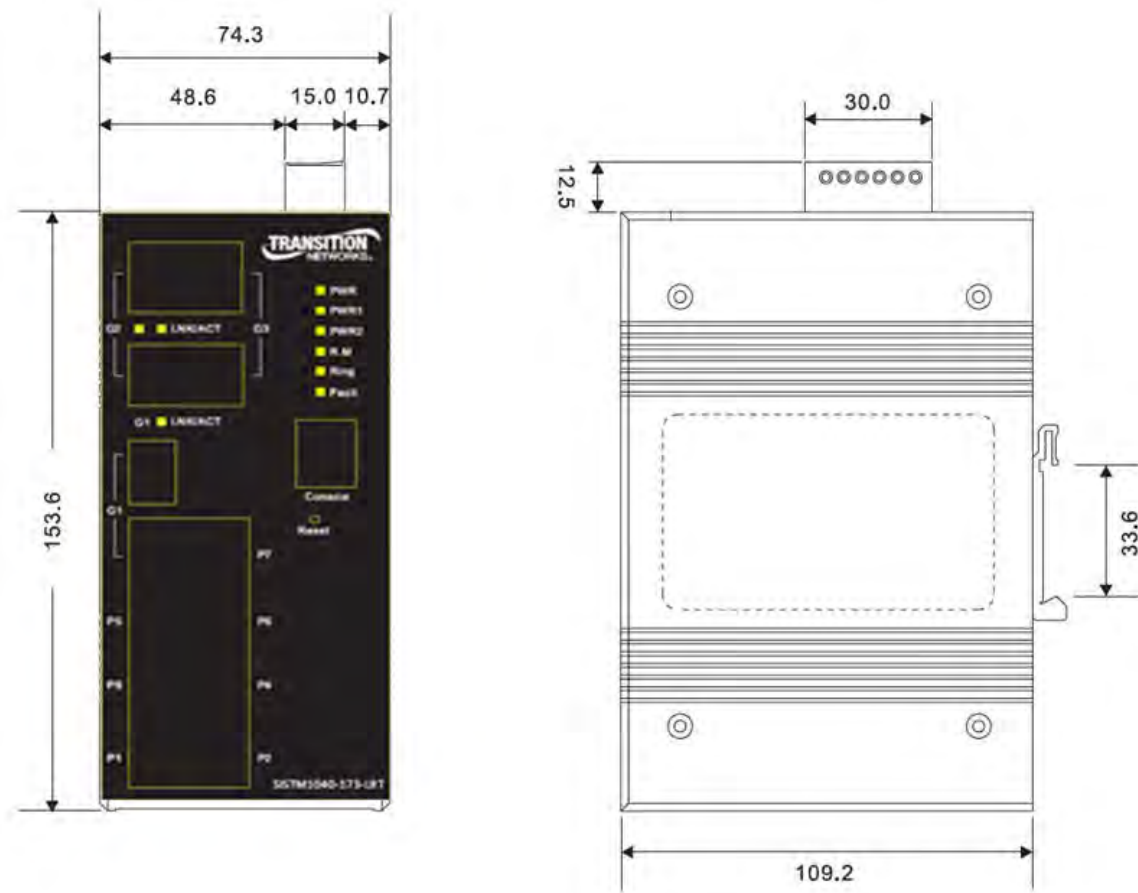
- One SISTM1040-173D-LRT Switch
- One printed Quick Start Guide
- One Console Cable
- One Wall Mount Kit
- One DIN Rail Mount Kit
- One four-pin Terminal Block
- Six Flat Screws (M3 X5)

1.6 Unpacking

Save the packaging for possible future use.



1.7 Dimensions



1.8 Related Information

A printed Quick Start Guide is shipped with each switch.

For Transition Networks Drivers, Firmware, Manual, etc. go to the [Product Support](#) webpage (no logon required). For Transition Networks Application Notes, Brocures, Data Sheets, Specifications, etc. go to the [Support Library](#) (no registration required). For SFP manuals see Transition Networks [SFP page](#).

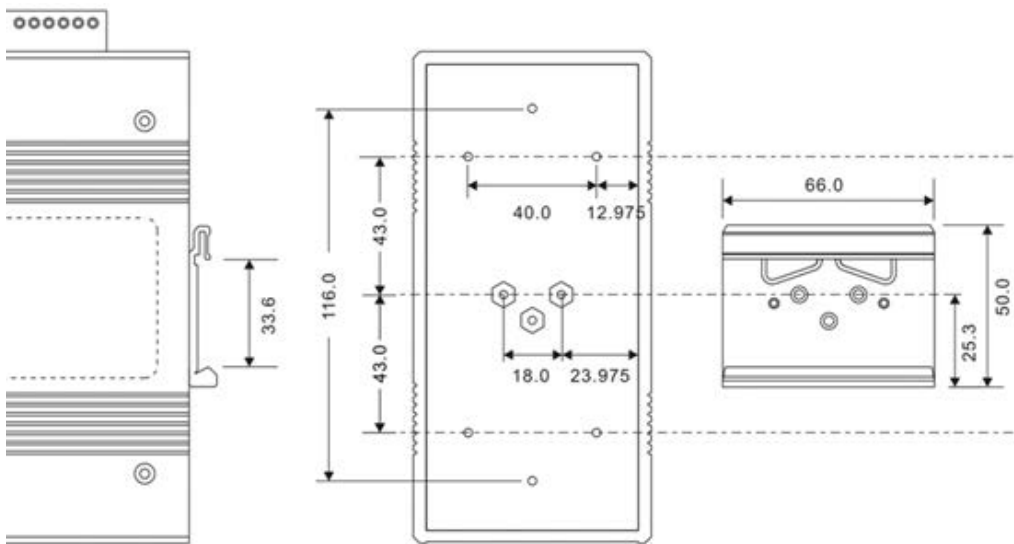
Note that this manual provides links to third party web sites for which Transition Networks is not responsible. **Note:** Information in this document is subject to change without notice. All information was deemed accurate and complete at the time of publication. This manual documents the latest software/firmware version at the time of publication.

2. Hardware Installation

Use the mounting kits attached with the package and follow the steps below to install the switch to a rail or to the wall.

2.1 DIN-Rail Mounting

Each switch has a Din-Rail clip on the rear panel. The Din-Rail clip can be used to mount the switch on a 35mm Din-Rail. Dimensions are shown below.

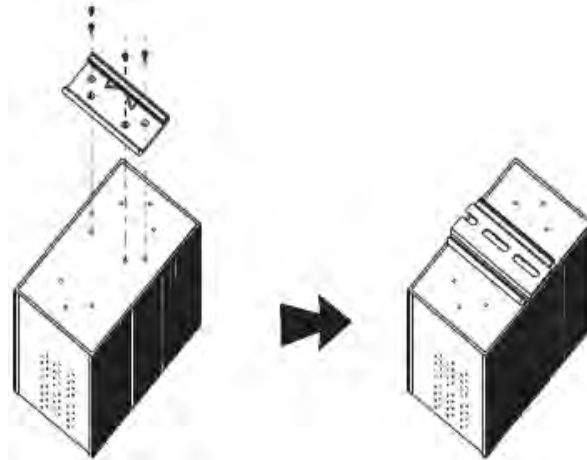


DIN-Rail Dimensions

2.1.1 DIN-Rail Mount Procedure

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

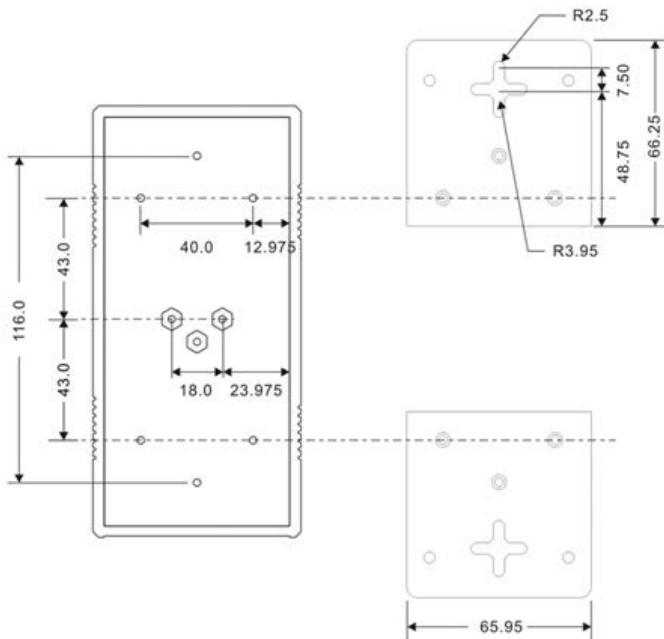
Step 2: Push the switch down on the Din-Rail until the bottom of the clip grips the bottom edge of the DIN Rail. You may hear a “click” sound when this happens.



2.2 Wall Mounting

Each switch also contains wall mount brackets that can be found in the package. The following steps show how to mount the switch on a panel or wall.

2.2.1 Wall Mount Dimensions



2.2.1 Wall Mount Procedure

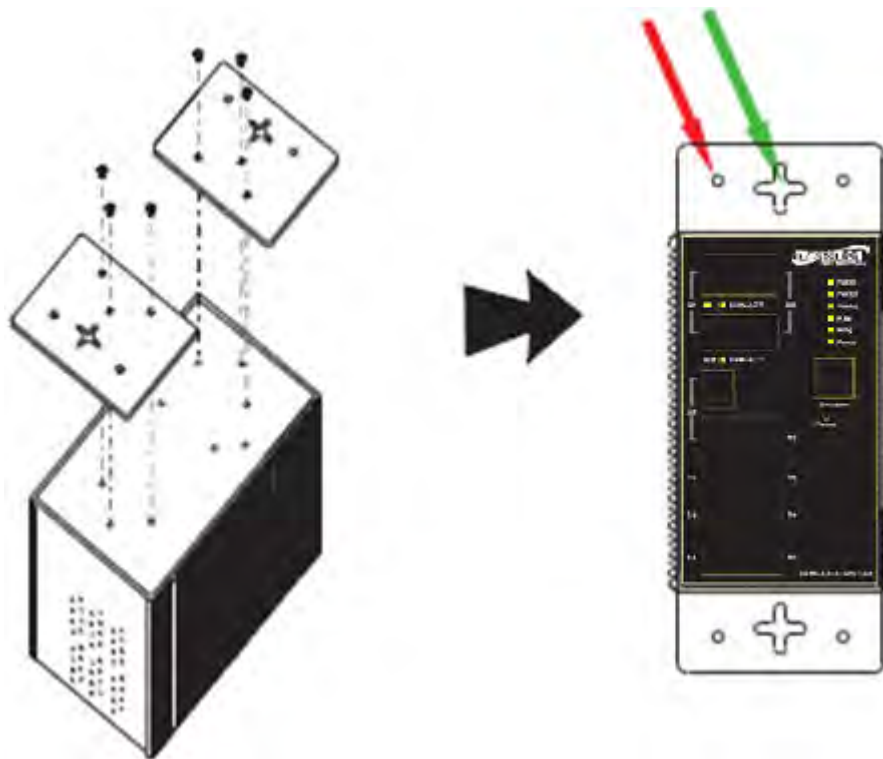
The following steps tell how to mount the switch on the wall:

Step 1: Fasten the two wall mount brackets to the back of the switch using the 6 screws provided.

Step 2: Using the switch with the brackets installed as a template, mark the location for the mounting screws on the wall or panel.

Step 3: Insert screws through the round screw holes (the red arrow as below) on the sides or through the cross-shaped aperture (the green arrow as below) in the middle of the plate and fasten the screw to the wall with a screwdriver.

Step 4: If the screw goes through the cross-shaped aperture, slide the switch down before tightening the screw. **Note:** Instead of screwing the screws in all the way, it is advised to leave a space of about 2mm to allow room for sliding the switch between the wall and the screws.



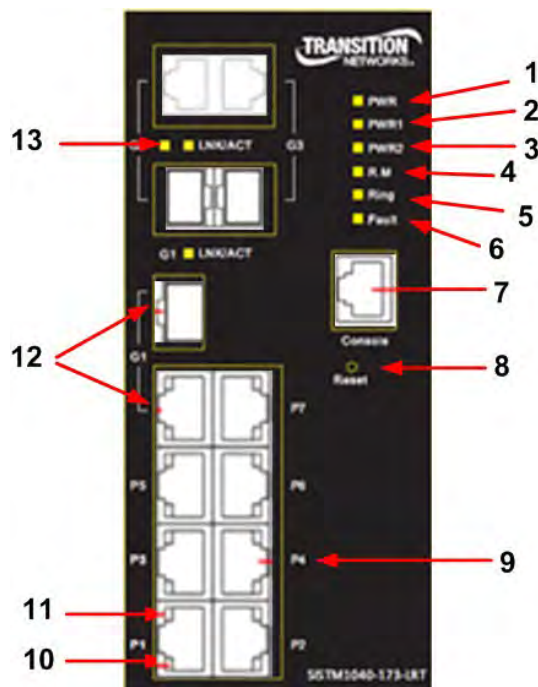
3. Hardware Overview

3.1 Front Panel

The following table describes the labeling on the S1STM1040-173D-LRT.

Port	Description
10/100 RJ-45 fast Ethernet ports	Eight 10/100Base-T(X) RJ-45 fast Ethernet ports with auto-negotiation. Default settings: Speed: auto; Duplex: auto; Flow control: disabled.
Gigabit RJ-45 port	Three 10/100/1000Base-TX Gigabit ports (combo port)
Fiber port	Three 100/1000Base-X on SFP port (combo port)
Console	Use RS-232 to RJ-45 connector to manage switch.
Reset button	Push and hold for 2 - 3 seconds to reset the switch. Push and hold for 5 seconds to reset the switch to Factory Defaults .

1. LED for **PWR** With any PWR ON, the green LED lights.
2. LED for **PWR1**. When PWR1 links, the green LED lights.
3. LED for PWR2. When the PWR2 links, the green LED lights.
4. LED for **RM** (Ring master). When lit, the switch is the Ring Master of Redundant Ring.
5. LED for **Ring**. When lit, the Redundant Ring is activated.
6. LED for **Fault** Relay. When a fault occurs, the amber LED lights.
7. **Console** Port (RJ-45)
8. **Reset** button
9. 10/100Base-T(X) Ethernet ports.
10. LED for Ethernet ports speed status.
11. LED for Ethernet ports Link status.
12. Gigabit combo ports with SFP and RJ-45 connectors.
13. Fiber port LED.



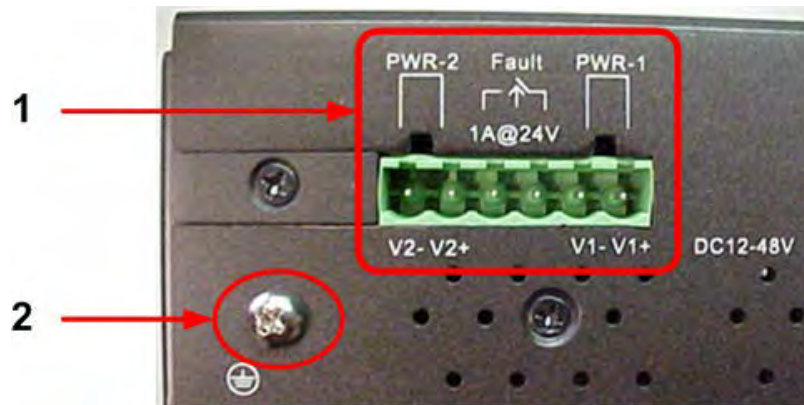
3.2 Front Panel LEDs

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	System running in Ring Master mode.
Ring	Green	On	System running in Ring mode.
		Blinking	Ring structure is broken (part of the ring is disconnected).
Fault	Amber	On	Fault relay. Power failure or Port malfunctioning.
10/100Base-T(X) Fast Ethernet ports			
LNK / ACT	Green	On	Ethernet link connected.
		Blinking	Transmitting data.
Full Duplex	Amber	On	Port works in full duplex mode
10/100/1000Base-T(X) Fast Ethernet ports			
LNK/ACT	Green	On	Ethernet link connected.
		Blinking	Transmitting data.
Full Duplex	Amber	On	Port works in full duplex mode
SFP Combo Ports			
LNK / ACT	Green	On	Ethernet links connected.
		Blinking	Transmitting data.

3.3 Top Panel

The top panel components are shown below:

1. Terminal block includes: PWR1 and PWR2 (12 ~ 48V DC)
2. Ground screw



3.4 Warnings



WARNING: Do not disconnect modules or wires unless power has been switched off or the area is known to be non-hazardous. The devices may only be connected to the supply voltage shown on the type plate.



ATTENTION

1. Be sure to disconnect the power cord before installing and/or wiring your switches.
2. Calculate the maximum possible current in each power wire and common wire. Observe all electrical codes dictating the maximum current allowable for each wire size.
3. If the current goes above the maximum ratings, the wiring could overheat, causing serious damage to your equipment.
4. Use separate paths to route wiring for power and devices. If power wiring and device wiring paths must cross, make sure the wires are perpendicular at the intersection point.
5. Do not run signal or communications wiring and power wiring through the same wire conduit. To avoid interference, wires with different signal characteristics should be routed separately.
6. You can use the type of signal transmitted through a wire to determine which wires should be kept separate. Usually, wiring with similar electrical characteristics can be bundled together.
7. You should separate input wiring from output wiring.
8. It is advised to label the wiring to all devices in the system.

3.5 Wiring

3.4.1 Fault Relay Contacts

The switch provides fail open and fail close options for you to form relay circuits based on your needs.

If you want the relay device to start operating at power failure, attach the two wires to COM and Fail Close to form a close circuit, vice versa. The relay contact of the 3-pin terminal block connector will respond to user-configured events according to the wiring. The two wires attached to the fault contacts form an open circuit when a user-configured event is triggered. If a user-configured event does not occur, the fault circuit remains closed. Fault Output - Relay output contacts: 1A@24VDC load capacity.

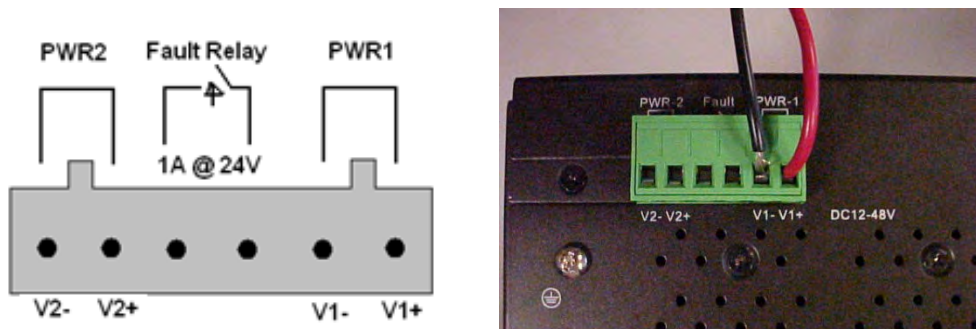
3.4.2 Grounding

Grounding and wire routing help limit the effects of noise due to electromagnetic interference (EMI). Run the ground connection from the ground screws to the grounding surface prior to connecting devices.

Ethernet network isolator module for inter-building applications (i.e., building to building, copper to copper endpoint connections) may be used for enhanced protection.

3.4.3 Redundant Power Inputs

The switch has two sets of power inputs, power input 1 and power input 2. The top two and the bottom two contacts of the 6-pin terminal block connector on the switch's top panel are used for dual power inputs.



Follow the steps below to wire redundant power inputs. **Caution:** before applying power, insert screw terminal connectors into the SISTM1040-173D-LRT switch and verify all connections.

Step 1: Remove the terminal block and screws from the ziplock bag.

Step 2: Insert the terminal block into the V1 / V2 receptical.

Step 3: Insert the negative and positive wires into the **V-** / **V+** terminals of **PWR-1**.

Step 4: Use a small flat-blade screwdriver to tighten the wire-clamp screws on the front of the terminal block connector.

Step 5: Repeat Steps 3 and 4 for **PWR-2** as required.

Step 6: Verify all connections and then apply power.

4. Cables

4.1 Ethernet Cables

The SISTM1040-173D-LRT switch has standard Ethernet ports. According to the link type, the switches use CAT 3, 4, 5,5e UTP cables to connect to any other network device (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 100BASE-TX/10BASE-T Pin Assignments

With 100BASE-TX/10BASE-T cable, pins 1 and 2 are used for transmitting data, and pins 3 and 6 are used for receiving data. For pin assignments for different types of cables, refer to the following tables.

1000 Base-T RJ-45	
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-

10/100 Base-T(X) RJ-45	
Pin Number	Assignment
1	TD+
2	TD-
3	RD+
4	Not used
5	Not used
6	RD-
7	Not used
8	Not used

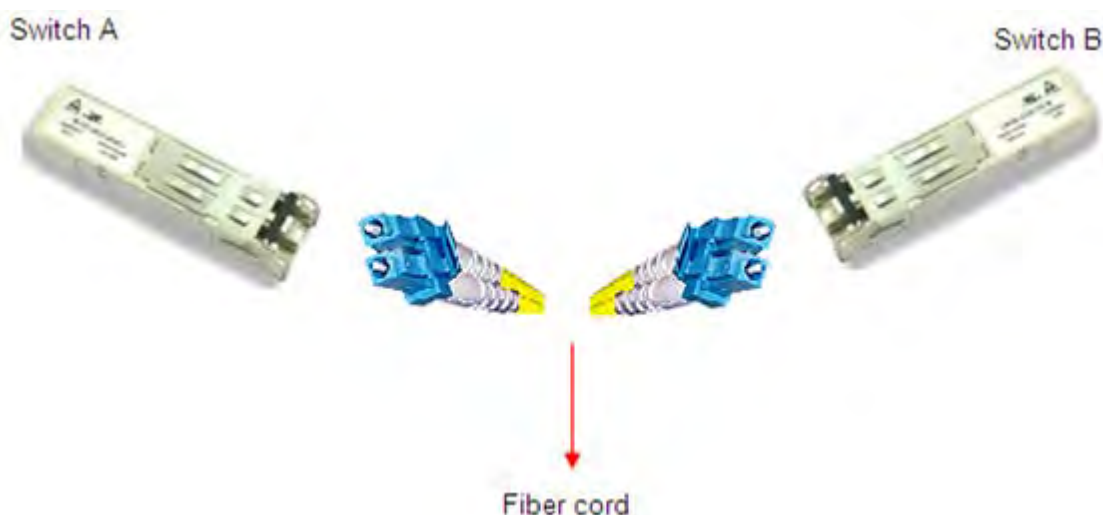
Most users configure these ports for Auto MDI/MDI-X mode, in which case the port's pinouts are adjusted automatically depending on the type of Ethernet cable used and the type of devices connected to the port. Below are the pin assignments for both MDI ports and MDI-X ports.

10/100 Base-T(X) MDI/MDI-X			1000Base-T MDI/MDI-X		
Pin Number	MDI port	MDI-X port	Pin Number	MDI port	MDI-X port
1	TD+(transmit)	RD+(receive)	1	BI_DA+	BI_DB+
2	TD-(transmit)	RD-(receive)	2	BI_DA-	BI_DB-
3	RD+(receive)	TD+(transmit)	3	BI_DB+	BI_DA+
4	Not used	Not used	4	BI_DC+	BI_DD+
5	Not used	Not used	5	BI_DC-	BI_DD-
6	RD-(receive)	TD-(transmit)	6	BI_DB-	BI_DA-
7	Not used	Not used	7	BI_DD+	BI_DC+
8	Not used	Not used	8	BI_DD-	BI_DC-

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

4.2 SFPs

The SISTM1040-173D-LRT has fiber optical ports with SFP connectors. The fiber optical ports are in multi-mode (0 to 550M, 850 nm with 50/125 μ m, 62.5/125 μ m fiber) and single-mode with LC connector. Note that the TX port of Switch A should be connected to the RX port of Switch B.

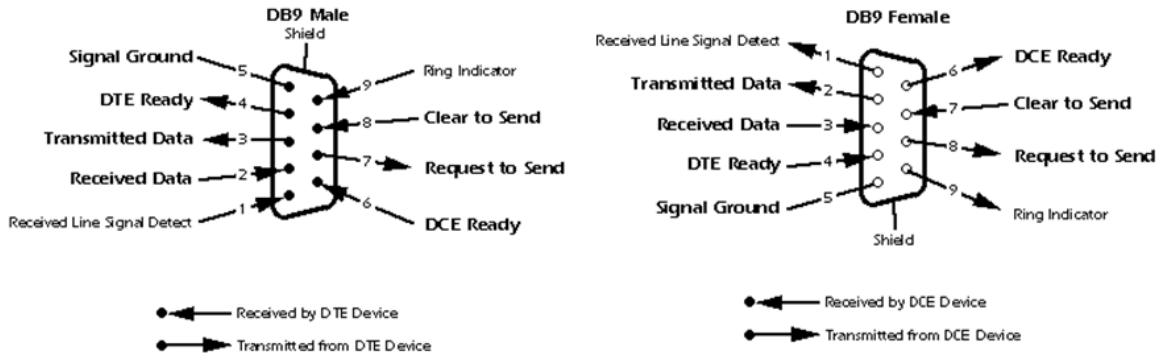


4.3 Console Cable

Console Port Pin Definition

To connect the console port to an external management device, you need an RJ-45 to DB-9 cable, which is included in the package. Below is the console port pin assignment information.

PC (male) pin assignment	RS-232 with DB9 (female) pin assignment (RJ45 - DB9 cable)	RJ 45 pin assignment
Pin #2 RxD	Pin #2 RxD	Pin #2 RxD
Pin #3 TxD	Pin #3 TxD	Pin #3 TxD
Pin #5 GND	Pin #5 GND	Pin #5 GND



RJ-45 to DB-9 Cable (included in the package)

5. Web Management

This section introduces configuration via the Web browser.



Warning! Before upgrading the firmware, remove the physical loop connection.



Warning! DO NOT power off equipment during firmware upgrade!

5.1 Configuration by Web Browser

5.1.1 About Web-based Management

An embedded HTML web site resides in flash memory on the CPU board. 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.

Default Values

The default values are:

IP Address: **192.168.1.77**

Subnet Mask: **255.255.255.0**

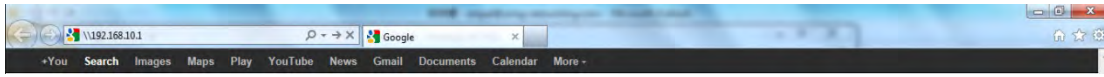
Default Gateway: **192.168.1.254**

User Name: **root**

Password: **root**

System Login

1. Launch the web browser (e.g., Internet Explorer).
2. Type the IP address (default is **192.168.1.77**) of the switch. Press **“Enter”**.



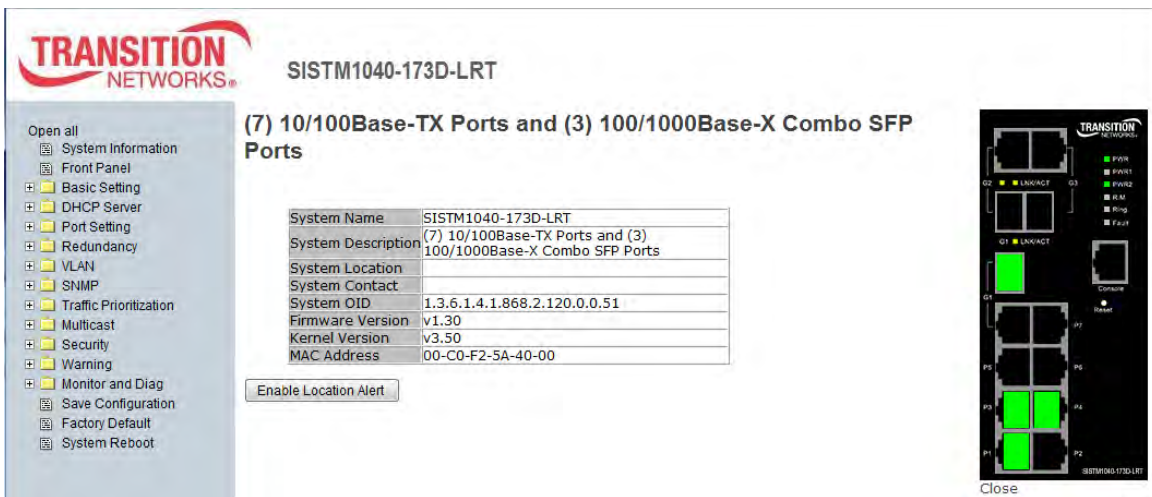
3. At the Login screen, type the username and password. The default for both is **root**.



4. Click the **OK** button; the Web-based management Main interface displays.

Startup Screen - System Information Page

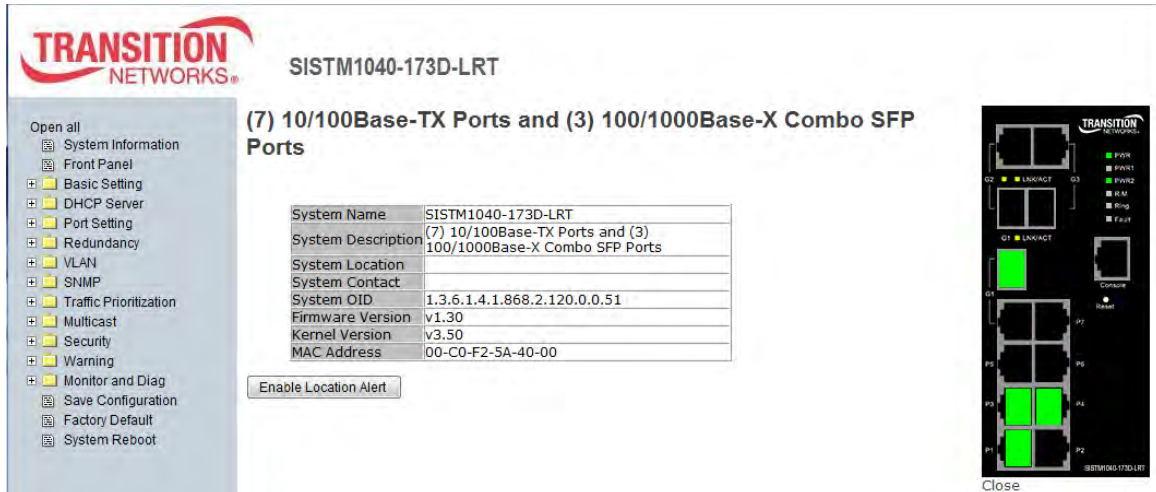
After successful login, by default, the main interface page displays the SISTM1040-173D-LRT System Information page with front panel status.



Startup Screen (System Information page)

5.1.2 System Information

The system information displays device configuration information similar to the Basic Setting > Switch Setting page.



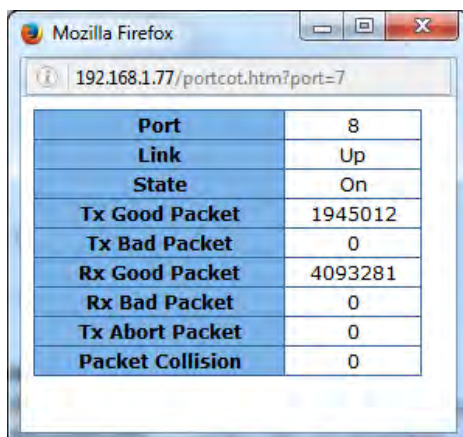
System Information page

Enable Location Alert

When you click **Enable Location Alert**, the PWR1, PWR2 and PWR3 LEDs will start to flash together; click **Disable Location Alert** and the LEDs will stop flashing.

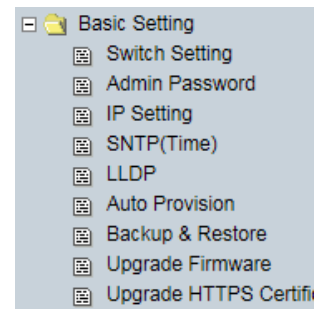
Click **Close** to close the front panel display on the web page. Click the Front Panel menu item to show the front panel display again.

Click on any port to display its status in a new window:



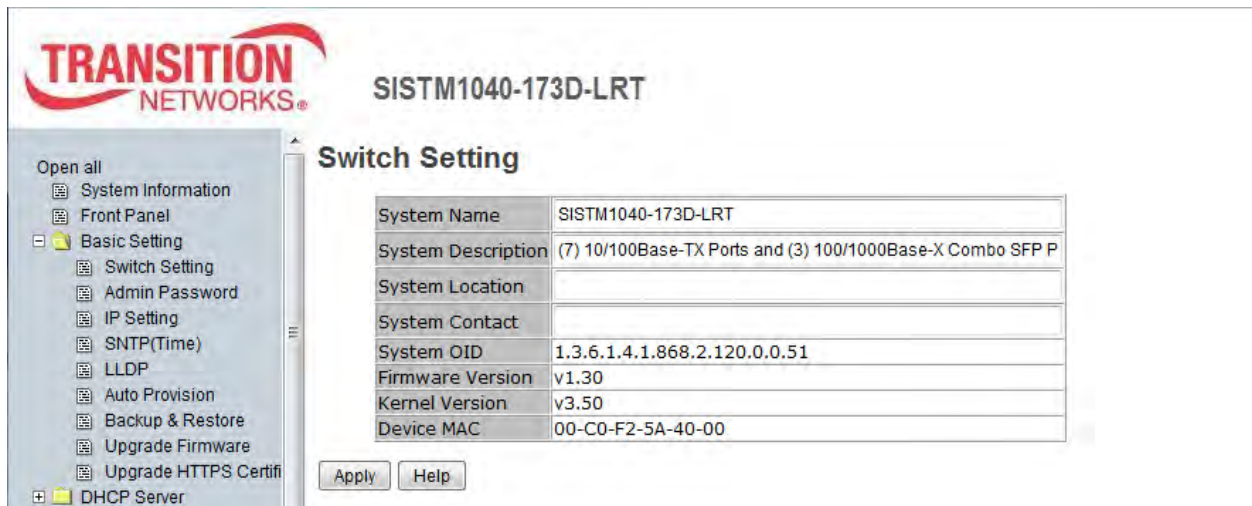
5.1.3 Basic Setting

From the left menu pane Basic Setting you can select Switch Setting, Admin Password, IP Setting, SNTP (Time), LLDP, Auto Provision, Backup & Restore, Upgrade Firmware, and Upgrade HTTPS Certificate.



5.1.3.1 Switch Setting

Here you can view system information and configure a system location and contact.



Switch Setting page

The following table describes the labels on this page.

Label	Description
System Name	Assign the name of switch. The maximum length is 64 bytes.
System Description	Displays the description of switch.
System Location	Assign the switch physical location; up to 64 bytes.
System Contact	Enter the name of contact person or organization.
System OID	Object Identifier (e.g., 1.3.6.1.4.1.868.2.120.0.0.51).
Firmware Version	The current switch firmware version (e.g., v1.30).
Kernel Version	The current switch kernel version (e.g., v3.50).
Device MAC	The current switch MAC address (e.g., 00-C0-F2-5A-40-01).

5.1.3.2 Admin Password

Change web management login User Name and Password for management security.



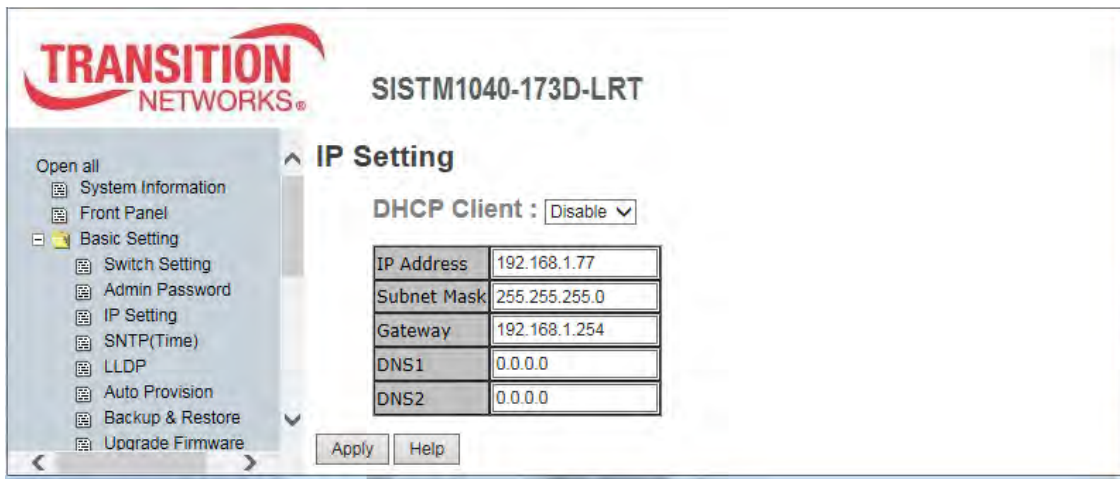
Admin Password page

The parameters are described below.

Label	Description
User Name	Type the new username (the default is root).
New Password	Type the new password (the default is root).
Confirm Password	Re-type the new password.
Apply	Click Apply to activate the configuration.

5.1.3.3 IP Setting

You can configure the IP Settings and DHCP Client function via IP Setting.



IP Setting page

The following table describes the labels on this page.

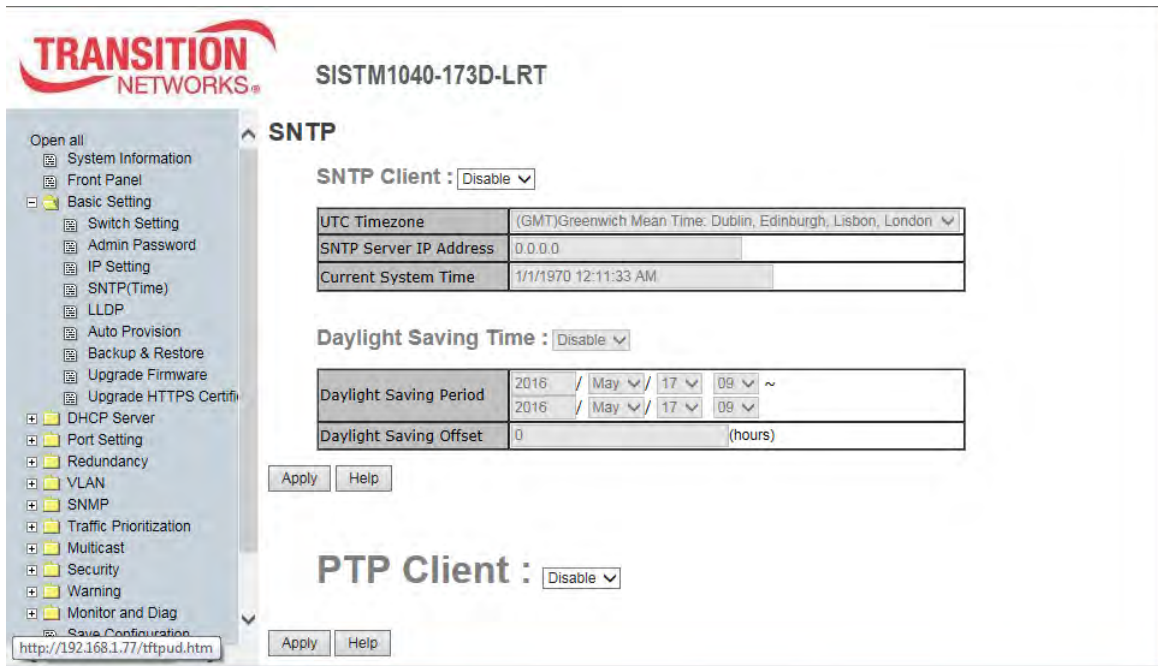
Label	Description
DHCP Client	To enable or disable the DHCP client function. When DHCP client function is enabling, the switch will be assigned the IP address from the network DHCP server. The default IP address will be replaced by the IP address which the DHCP server has assigned. After clicking “ Apply ” button, a popup dialog shows up to inform when the DHCP client is enabling. The current IP will lose and you should find a new IP on the DHCP server.
IP Address	Assign the IP address that the network is using. If DHCP client function is enabling, 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 display 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. Keep "0.0.0.0" if never used.
DNS2	Assign the secondary DNS IP address. Keep "0.0.0.0" if never used.
Apply	Click “ Apply ” to activate the configurations.

Message: Reconnect to <http://192.168.1.x>.

Recovery: 1. Click **OK** to accept the new IP address. 2. Log in again. 3. Continue operation.

5.1.3.4 SNTP (Time)

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



SNTP Configuration page

The following table describes the labels on this page.

Label	Description
SNTP Client	Select to enable or disable the SNTP client at the dropdown (enable or disable SNTP function to get the time from the SNTP server).
UTC Timezone	Dropdown to select the Coordinated Universal Time zone. Time zones around the world are expressed using positive or negative offsets from UTC, as in the list of time zones by UTC offset.
SNTP Server IP Address	Enter the IP address of the SNTP server.
Daylight Saving Time	Enable or disable daylight saving time function. When daylight saving time is enabling, you need to configure the daylight saving time period.
UTC Timezone	Set the switch location time zone. The table below lists the different location time zones for your reference. See also http://militarybenefits.info/military-time/ .

Time Zones

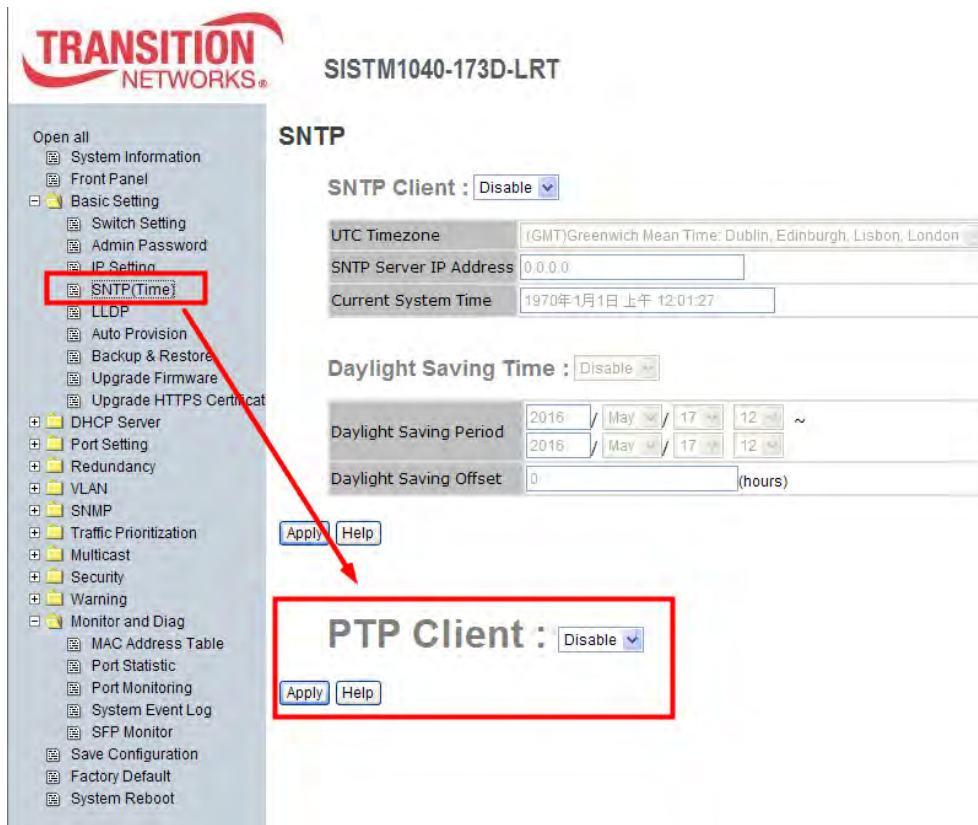
Local Time Zone	Conversion from UTC (Offset)	Time at 12:00 UTC
November Time Zone	- 1 hour	11 am
Oscar Time Zone	-2 hours	10 am
ADT - Atlantic Daylight	-3 hours	9 am
AST - Atlantic Standard EDT - Eastern Daylight	-4 hours	8 am
EST - Eastern Standard CDT - Central Daylight	-5 hours	7 am
CST - Central Standard MDT - Mountain Daylight	-6 hours	6 am
MST - Mountain Standard PDT - Pacific Daylight	-7 hours	5 am
PST - Pacific Standard ADT - Alaskan Daylight	-8 hours	4 am
ALA - Alaskan Standard	-9 hours	3 am
HAW - Hawaiian Standard	-10 hours	2 am
Nome, Alaska	-11 hours	1 am
CET - Central European FWT - French Winter MET - Middle European MEWT - Middle European Winter SWT - Swedish Winter	+1 hour	1 pm
EET - Eastern European, USSR Zone 1	+2 hours	2 pm
BT - Baghdad, USSR Zone 2	+3 hours	3 pm
ZP4 - USSR Zone 3	+4 hours	4 pm

ZP5 - USSR Zone 4	+5 hours	5 pm
ZP6 - USSR Zone 5	+6 hours	6 pm
WAST - West Australian Standard	+7 hours	7 pm
CCT - China Coast, USSR Zone 7	+8 hours	8 pm
JST - Japan Standard, USSR Zone 8	+9 hours	9 pm
EAST - East Australian Standard GST Guam Standard, USSR Zone 9	+10 hours	10 pm
IDLE - International Date Line NZST - New Zealand Standard NZT - New Zealand	+12 hours	Midnight

Label	Description
SNTP Sever IP Address	Set the SNTP server IP address.
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.
Switch Timer	Display the switch current time.
Apply	Click " Apply " to activate the configurations.

5.1.3.5 PTP Client

The SNTP(Time) page also lets you configure PTP Client (Precision Time Protocol). PTP (Precision Time Protocol) 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. A simplified PTP system frequently consists of ordinary clocks connected to a single network, and no boundary clocks are used. A grandmaster is elected and all other clocks synchronize directly to it.



SNTM page / PTP Configuration section

The following table describes the labels on this page.

Label	Description
Enable/Disable	To enable the PTP Client, select Enable at the dropdown and click the Apply button. The default setting is PTP Client Disabled.
Apply	Click " Apply " to set the configurations.
Help	Display the online help file for this page.

5.1.3.6 LLDP

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



LLDP configuration page

The following table describes the labels on this page.

Label	Description
LLDP Protocol	“Enable” or “Disable” the LLDP function.
LLDP Interval	The interval of resend LLDP (by default at 30 seconds). Sets the interval of learning the information time in second.
Apply	Click “ Apply ” to set the configurations.
Help	Display the online help file for this page.

5.1.3.7 Auto Provision

The Auto Provision feature lets you update the switch firmware automatically. You can put either a firmware or configuration file on a TFTP server; then when you reboot the switch, it will upgrade automatically. Before updating, make sure you have your TFTP server ready and the firmware image and configuration file on the TFTP server.

Auto Provision page

The following table describes the labels on this page.

Label	Description
Auto Install Config file from TFTP server?	Check to enable. The default is 192.168.1.66. If checked, the Configuration file will be automatically installed on reboot.
TFTP Server IP Address	Enter the IP address of the TFTP server.
Configuration File Name	Enter the filename (data.bin) for downloading.
Auto firmware image file from TFTP server?	Check to enable. The default is 192.168.1.66. If checked, the Firmware file will be automatically installed on reboot.
TFTP Server IP Address	Enter the IP address of the TFTP server.
Firmware File Name	Enter the filename (image.bin) for downloading.

5.1.3.8 Backup & Restore

You can save current EEPROM value from the switch to a TFTP server, then go to the TFTP Restore Configuration page to restore the EEPROM value.

Backup Configuration

To TFTP Server

TFTP Server IP Address	192.168.1.66
Backup File Name	data.bin
<input type="button" value="Backup"/> <input type="button" value="Help"/>	

Restore Configuration

From TFTP Server

TFTP Server IP Address	192.168.1.66
Restore File Name	data.bin
<input type="button" value="Restore"/> <input type="button" value="Help"/>	

Backup and Restore interfaces

The following table describes the labels on this page.

Label	Description
TFTP Server IP Address	Enter the IP address of the TFTP server.
Backup File Name	Enter the file name (e.g. <i>xxxxxx.bin</i>) to back up.
Backup	Click the Backup button to backup the configurations.
Restore File Name	Enter the file name (e.g. <i>xxxxxx.bin</i>) to restore.
Restore File Name	Enter the file name.
Restore	Click the Restore button to restore the configurations.

After the configuration data is downloaded successfully, the system **MUST** be restarted and the restored configuration will be applied in next start.

Message: *Apply fail - TFTP transmission fail.*

Recovery: Click **Retry**, enter a correct IP address and click the **Backup** button.

5.1.3.9 Upgrade Firmware

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



Upgrade Firmware page

The following table describes the labels on this page.

Label	Description
TFTP Server IP	Enter the IP address of the TFTP server.
Firmware File Name	Enter the file name (e.g. <i>xxxxxx.bin</i>) to upgrade the switch to.

After upgrading firmware successfully, the system **MUST** be restarted and the new firmware will be applied in next start.

Message: *Apply fail TFTP transmission fail*

Meaning: The firmware upgrade failed.

Recovery: **1.** Verify the IP address of the TFTP server. **2.** Verify the firmware filename (*x.bin*).

3. Make sure the TFTP server is configured correctly and is running. **4.** Re-try the upgrade.

5. Reboot the switch.

5.1.3.10 Upgrade HTTPS Certification

The Upgrade HTTPS Certification page lets you update an HTTPS certificate. The SISTM1040-173D-LRT supports 1024 bit encryption key for HTTPS certification.

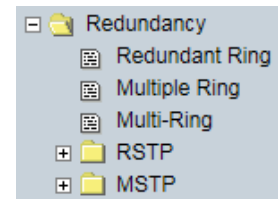
Upgrade HTTPS Certification page

The following table describes the labels on this page.

Label	Description
TFTP Server IP	Enter the IP address of the TFTP server.
Private Key File Name	The name of the file (e.g., private.key).
Pass Phrase for Private Key	Enter the Private Key passphrase (e.g., private.key).
Certification File Name	Self-signed or Authoritatively signed certificate (e.g., public.crt).
Upgrade	When the page information is entered, click the Upgrade button to start the HTTPS certification process.

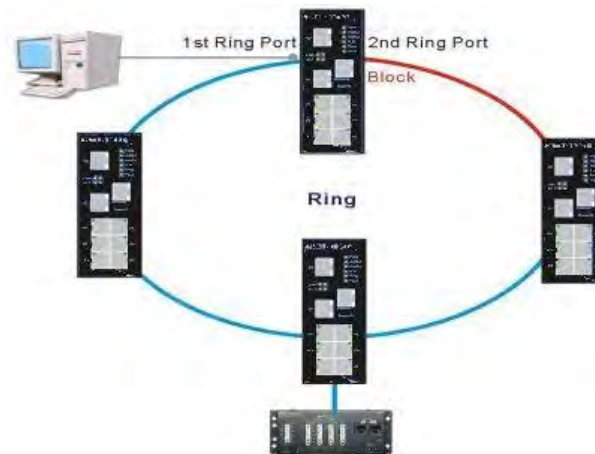
5.1.5 Redundancy

This section describes the Redundancy features (Redundant Ring, Multiple Ring, Multi-Ring, RSTP, and MSTP). Only one of these redundancy protocols can be enabled at the same time.



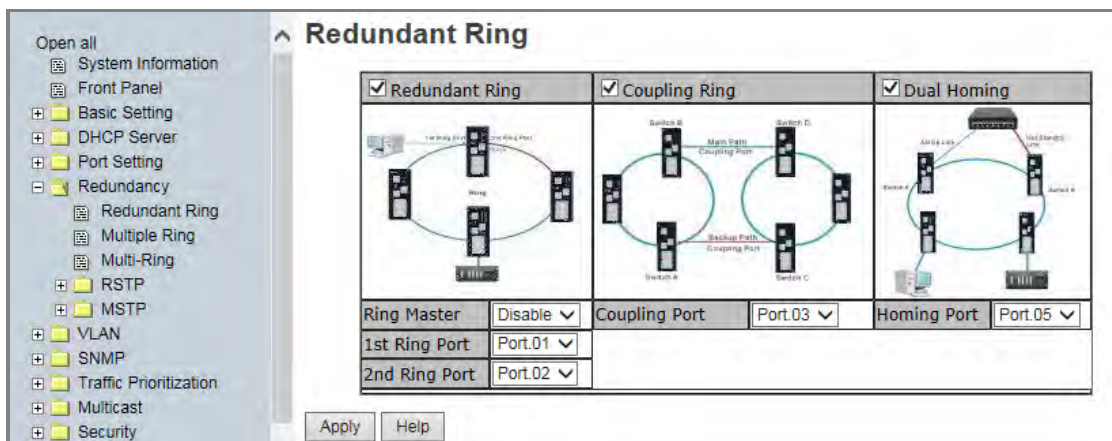
5.1.5.1 Redundant Ring

Redundant Ring recovery time is less than 10 ms. It can reduce unexpected damage caused by network topology changes. Redundant Ring supports three Ring topologies: Redundant Ring, Coupling Ring, and Dual Homing.



Redundant Ring

Note that no port can be assigned twice; the 1st Ring Port, 2nd Ring Port, Coupling Port, and Homing Port must not be assigned the same port number if Redundant Ring, Coupling Ring, and Dual Homing are all enabled.



The following table describes the labels on this page.

Label	Description
Enable Ring	Check to enable Ring support globally.
Ring Master	There should be one and only one Ring Master in a ring. However if there are two or more switches which 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	The primary port if this switch is Ring Master.
2nd Ring Port	The backup port ifn this switch is Ring Master.
Coupling Ring	Mark 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 change. It is a good application for connecting two Rings.
Coupling Port	Link to Coupling Port of the switch in another ring. Coupling Ring need four switch to build an active and a backup link. Set a port as coupling port. The coupled four ports of four switches will be run at active/backup mode.
Homing Port	Link to Control Port of the switch in the same ring. The Control Port used to transmit control signals.
Dual Homing	Mark to enable Dual Homing. By selecting Dual Homing mode, Redundant Ring will be connected to normal switches through two RSTP links (ex: backbone Switch). The two links work as active/backup mode, and connect each Redundant Ring to the normal switches in RSTP mode.
Apply	Click "Apply" to set the configurations.

Note: We don't suggest you to set one switch as a Ring Master and a Coupling Ring at the same time due to heavy load. **Note** that all switches in a ring must have Redundant Ring enabled.

Redundancy Messages

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

Meaning: Only one redundancy protocol can be enabled at any given time.

Recovery: **1.** Click the **Retry** button. **2.** Disable any other redundancy protocol(s). **3.** Click the **Apply** button.

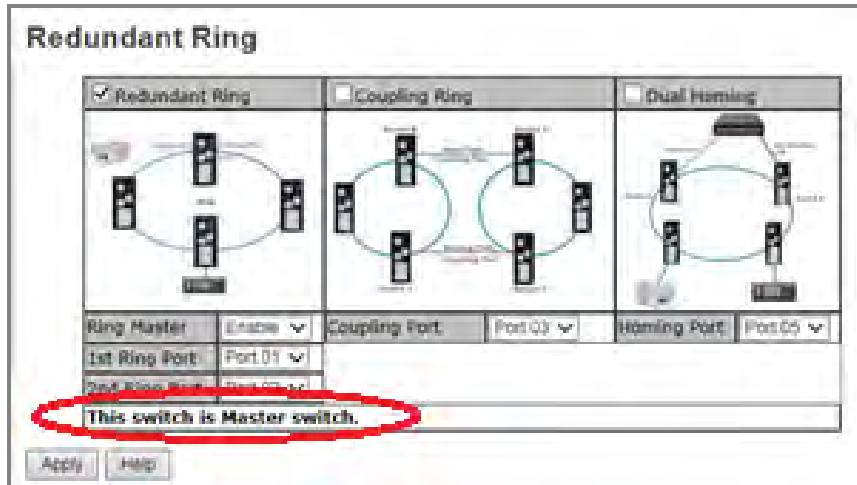
Message: *Apply fail Wrong data submitted*

Meaning: You mis-configured a parameter on the Redundant Ring page (e.g., 1st Ring Port and 2nd Ring Port set to the same Port number).

Recovery: 1. Click the **Retry** button. 2. Change the bad parameter; see above. 3. Click the **Apply** button.

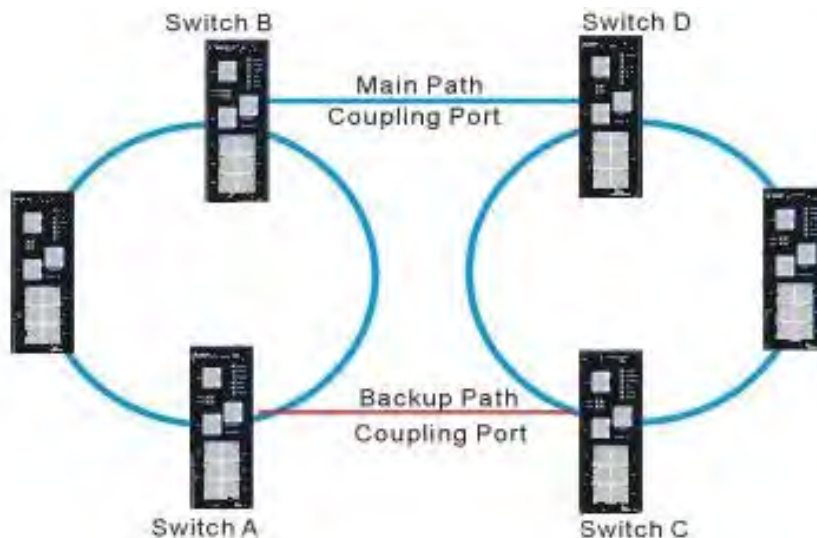
Message: *This switch is Master switch.*

Meaning: Information only; you have configured the Master switch. Continue Redundant Ring configuration.



Coupling Ring

At **Redundancy > Redundant Ring** check 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 change. It is a good application for connecting two Rings.

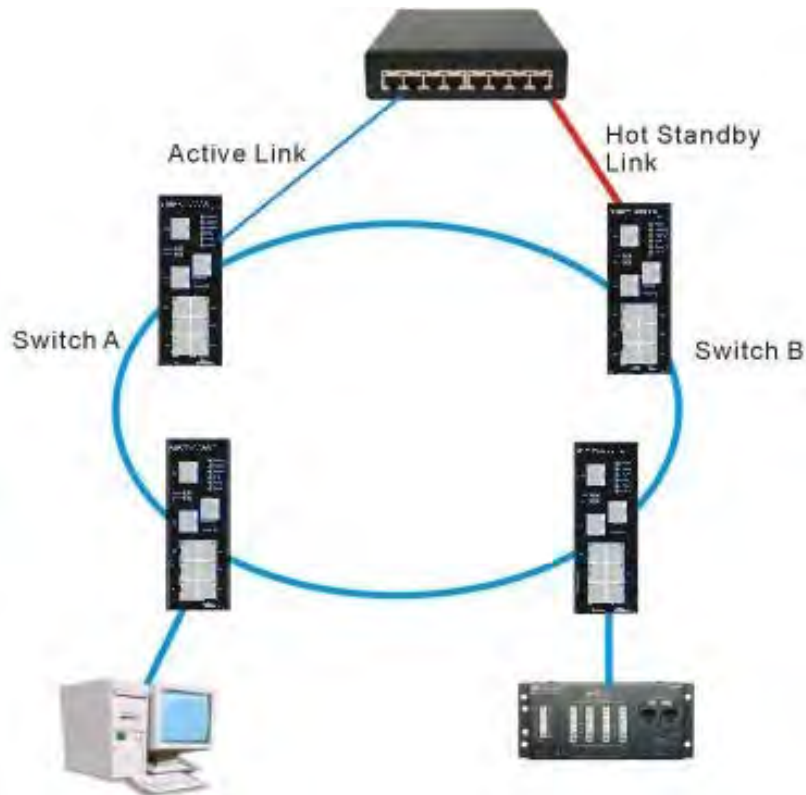


Coupling Ring

The Coupling Port is the link to the Coupling Port of the switch in another ring. Note that only two switches can enable Coupling Ring in a ring. More or less is invalid

Dual Homing

At **Redundancy > Redundant Ring** check to enable Dual Homing. By selecting Dual Homing mode, Redundant Ring will be connected to normal switches through two RSTP links (ex: backbone Switch). The two links work as active/backup mode, and connect each Redundant Ring to the normal switches in RSTP mode.



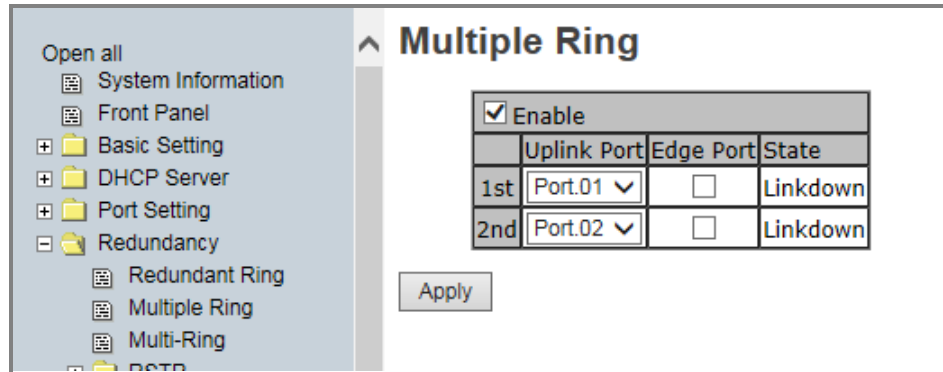
Dual Homing

Note:

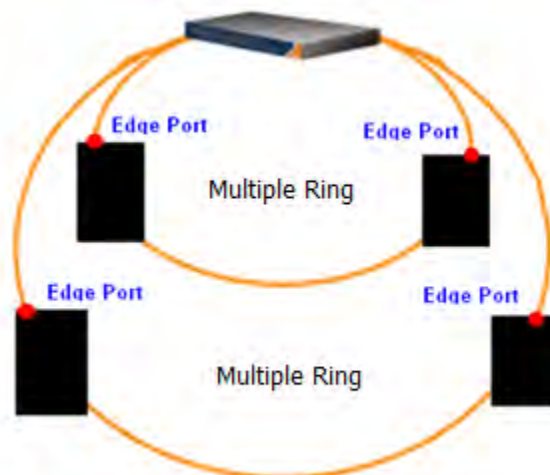
- Only two switches can enable Dual Homing in a ring. More or less is invalid.
- Network redundancy protocol should be well configured for all switches in redundant network before actually connecting any backup/redundant path in order to prevent inadvertently generating traffic loops.
- Multiple redundancy protocols, such as Redundant Ring and RSTP, can not be enabled at the same time.

5.1.5.1 Multiple Ring

Multiple Ring is the revolutionary network redundancy technology that provides the add-on network redundancy topology for any backbone network, providing ease-of-use while maximizing fault recovery speed, flexibility, compatibility, and cost-effectiveness in one set of network redundancy topologies. Multiple Ring allows multiple redundant network rings of different redundancy protocols to join and function together as a larger and more robust compound network topology (i.e. the creation of multiple redundant networks beyond the limitations of current redundant rings).

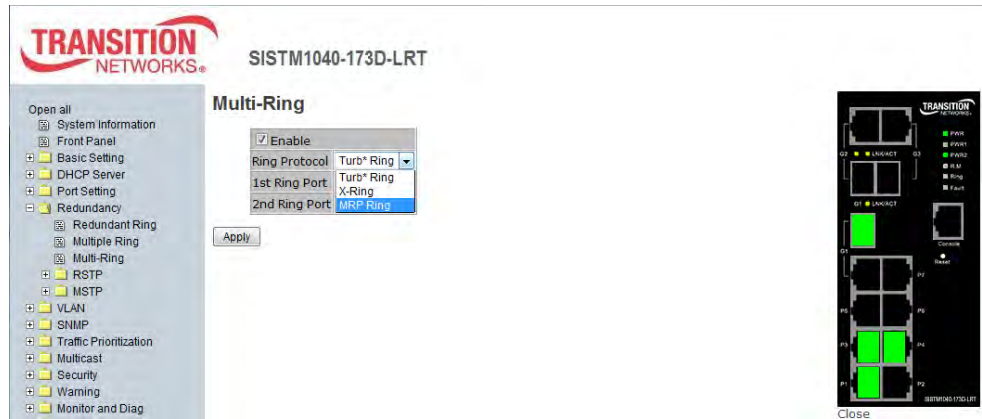


Label	Description
Enable	Check to enable the Multiple Ring function.
1st Uplink Port	Choose the first port to connect to the ring.
2nd Uplink Port	Choose the second port to connect to the ring. This port must be different than the 1 st Uplink port.
Edge Port	In the Multiple Ring application, the head and tail of two Switch Ports must start with the Edge, the Switch with the smaller MAC; the Edge port will be the backup and RM LED lights. Only one checkbox can be checked.
State	The port's current operating state (<i>Linkup, Linkdown, Forwarding</i>).



5.1.5.2 Multi-Ring

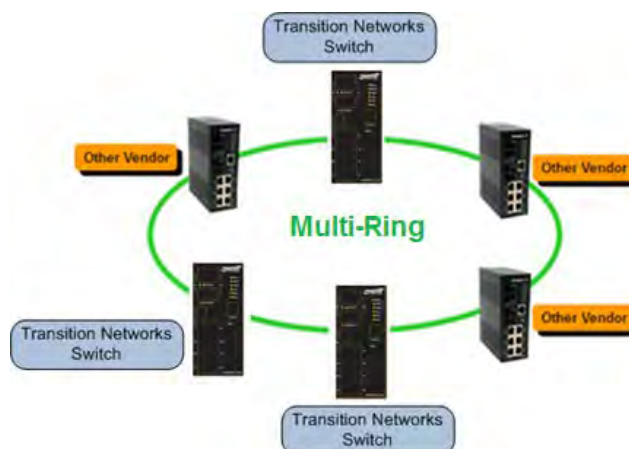
Multi-Ring technology can be applied for other vendor's proprietary ring. You can add SISTM1040-173D-LRT switches to a network constructed by another ring technology vendor and enable Multi-Ring to co-operate with other vendor's managed switch.



Multi-Ring page

Label	Description
Enable	Check to enable the Multi-Ring function.
Ring Protocol	At the dropdown select the vender that you want to join to the ring: Turb* Ring (MOXA) X-Ring (Advantech) MRP Ring (Hirschmann)
1st Ring Port	Choose the first port to connect to the ring (Port.01, Port.02, Port.03, Port.04, Port.05, Port.06, Port.07, G1, G2, G3).
2nd Ring Port	Choose the second port to connect to the ring (Port.01, Port.02, Port.03, Port.04, Port.05, Port.06, Port.07, G1, G2, G3).

A sample Multi-Ring application is shown below.



5.1.5.3 RSTP Setting

RSTP is a redundant ring technology that is different from standard STP/RSTP. The RSTP recovery time is less than 10mS and it supports more connected nodes in a ring topology.

Open all

- System Information
- Front Panel
- Basic Setting
- DHCP Server
- Port Setting
- Redundancy
 - Redundant Ring
 - Multiple Ring
 - Multi-Ring
 - RSTP
 - RSTP Setting
 - RSTP Information
- MSTP
- VLAN
- SNMP
- Traffic Prioritization
- Multicast
- Security
- Warning
- Monitor and Diag
- Save Configuration
- Factory Default
- System Reboot

RSTP Setting

RSTP Mode: Enable

Bridge Setting

Priority (0-61440)	32768
Max Age Time(6-40)	20
Hello Time (1-10)	2
Forward Delay Time (4-30)	15

Port Setting

Port No.	Enable	Path Cost(0:auto, 1-200000000)	Priority (0-240)	P2P	Edge
Port.01	enable	0	128	auto	true
Port.02	enable	0	128	auto	true
Port.03	enable	0	128	auto	true
Port.04	enable	0	128	auto	true
Port.05	enable	0	128	auto	true
Port.06	enable	0	128	auto	true
Port.07	enable	0	128	auto	true
G1	enable	0	128	auto	true
G2	enable	0	128	auto	true
G3	enable	0	128	auto	true

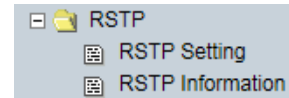
RSTP Setting page

An RSTP application is shown below.



RSTP connection

5.1.5.4 RSTP



The Rapid Spanning Tree Algorithm Protocol (RSTP) configures full, simple, symmetric connectivity throughout a Bridged Local Area Network that comprises individual LANs interconnected by Bridges. It is the most common network redundancy protocol. Refer to [IEEE 802.1W](http://www.ieee.org/802.1W).

Open all

- System Information
- Front Panel
- Basic Setting
- DHCP Server
- Port Setting
- Redundancy
 - Redundant Ring
 - Multiple Ring
 - Multi-Ring
 - RSTP
 - RSTP Setting
 - RSTP Information
 - MSTP
- VLAN
- SNMP
- Traffic Prioritization
- Multicast
- Security
- Warning
- Monitor and Diag
 - Save Configuration
 - Factory Default
 - System Reboot

RSTP Setting

RSTP Mode: Enable ▾

Bridge Setting

Priority (0-61440)	32768
Max Age Time(6-40)	20
Hello Time (1-10)	2
Forward Delay Time (4-30)	15

Port Setting

Port No.	Enable	Path Cost(0:auto, 1-200000000)	Priority (0-240)	P2P	Edge
Port.01	enable ▾	0	128	false ▾	false ▾
Port.02	disable ▾	0	128	auto ▾	true ▾
Port.03	enable ▾	0	128	true ▾	false ▾
Port.04	enable ▾	0	128	auto ▾	true ▾
Port.05	enable ▾	0	128	auto ▾	true ▾
Port.06	enable ▾	0	128	auto ▾	true ▾
Port.07	enable ▾	0	128	auto ▾	true ▾
G1	enable ▾	0	128	auto ▾	true ▾
G2	enable ▾	0	128	auto ▾	true ▾
G3	enable ▾	0	128	auto ▾	true ▾

Note that you can only run one redundancy protocol at a time. For example, if you try enable and configure both RSTP and MSTP at the same time, it would fail, displaying the message *“Apply fail Another redundancy protocol is running. Only one could be run at the same time”*. In this case you would click the **Retry** button to clear the error message, and disable one of the redundancy protocols.

RSTP - Bridge Setting

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

RSTP Mode: Enable ▾

Bridge Setting

Priority (0-61440)	32768
Max Age Time(6-40)	20
Hello Time (1-10)	2
Forward Delay Time (4-30)	15

RSTP Bridge Setting interface

The following table describes the labels on this page.

Label	Description
RSTP Mode	Enable or Disable RSTP. 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. Valid values are 0 ~ 61440 in steps of 4096 and the default value is 32768. Note: If bridge priority is changed, RSTP <u>must</u> be restarted.
Max Age Time(6-40)	The number of seconds a bridge waits without receiving BPDUs before attempting a reconfiguration. The valid value is 6 ~ 40 and the default value is 20 seconds.
Hello Time (1-10)	The number of seconds between transmissions of BPDUs. Valid values are 1 ~ 10 and the default value is 2 seconds.
Forwarding Delay Time (4-30)	The number of seconds a port waits before changing from its protocol learning and listening states to the forwarding state. The valid value is 4 ~ 30 and the default value is 15 seconds.
Apply	Click " Apply " to set the configurations.

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

$2 \times (\text{Forward Delay Time value} - 1) \geq \text{Max Age value} \geq 2 \times (\text{Hello Time value} + 1)$

RSTP - Port Setting

Note:

- Network redundancy protocol must be correctly configured for all switches in a redundant network before actually connecting any backup/redundant path to prevent the inadvertent generation of traffic loops.
- Both redundancy protocols, such as Redundant Ring and RSTP, can not be enabled at the same time.

Port Setting

Port No.	Enable	Path Cost(0:auto, 1-200000000)	Priority (0-240)	P2P	Edge
Port.01	enable ▼	0	128	auto ▼	true ▼
Port.02	enable ▼	0	128	auto ▼	true ▼
Port.03	enable ▼	0	128	auto ▼	true ▼
Port.04	enable ▼	0	128	auto ▼	true ▼
Port.05	enable ▼	0	128	auto ▼	true ▼
Port.06	enable ▼	0	128	auto ▼	true ▼
Port.07	enable ▼	0	128	auto ▼	true ▼
G1	enable ▼	0	128	auto ▼	true ▼
G2	enable ▼	0	128	auto ▼	true ▼
G3	enable ▼	0	128	auto ▼	true ▼

The following table describes the labels on this page.

RSTP Port Setting interface

Label	Description
Path Cost (0:auto, 1-200000000)	The cost of the path to the other bridge from this transmitting bridge at the specified port. Valid values are 1 ~ 200000000 and the default value is 200000 for mega-ports and 20000 for giga-ports (G1 - G3).
Priority (0-240)	Decide which port should be blocked by priority. The valid value is 0 ~ 240 in steps of 16 and the default value is 128.
P2P	Admin P2P: some of the rapid state transactions that are possible within RSTP are dependent upon whether the Port concerned can only be connected to exactly one other Bridge (i.e., it is served by a point-to-point LAN segment), or can be connected to two or more Bridges (i.e., it is served by a shared medium LAN segment). <i>True</i> means P2P enabled. <i>False</i> means P2P disabled. <i>Auto</i> means automatic selection.
Edge	Admin Edge: the value of this parameter is used by a Designated Port in order to determine how rapidly it may transition to the Forwarding Port State. All ports directly connected to end stations cannot create bridging loops in the network and can thus directly transition to forwarding, skipping the listening and learning stages. To configure the port as an edge port, set the port to “ True ”.

Label	Description
Admin Non STP	The port includes the STP mathematical calculation. Select true if this port will not participate in RSTP.
Apply	Click “ Apply ” to set the configurations.

RSTP Information

Displays the current RSTP Root Bridge Information and Port Information settings as described above.

Open all

- System Information
- Front Panel
- Basic Setting
- DHCP Server
- Port Setting
- Redundancy
 - Redundant Ring
 - Multiple Ring
 - Multi-Ring
- RSTP
 - RSTP Setting
 - RSTP Information
- MSTP
- VLAN
- SNMP
- Traffic Prioritization
- Multicast
- Security
- Warning
- Monitor and Diag
 - Save Configuration
 - Factory Default
 - System Reboot

RSTP Information

Root Bridge Information

Bridge ID	8000-00C0F25A4001
Root Priority	32768
Root Port	N/A
Root Path Cost	0
Max Age Time	20
Hello Time	2
Forward Delay Time	15

Port Information

Port	Path Cost	Port Priority	OperP2P	OperEdge	STP Neighbor	State	Role
Port.01	2000000	128	False	False	False	Disabled	Disabled
Port.02	2000000	128	False	True	False	Forwarding	Non Stp
Port.03	2000000	128	True	False	False	Disabled	Disabled
Port.04	2000000	128	True	True	False	Disabled	Disabled
Port.05	2000000	128	True	True	False	Disabled	Disabled
Port.06	2000000	128	True	True	False	Disabled	Disabled
Port.07	2000000	128	True	True	False	Disabled	Disabled
G1	200000	128	True	True	False	Forwarding	Designated
G2	2000000	128	True	True	False	Disabled	Disabled
G3	2000000	128	True	True	False	Disabled	Disabled

RSTP Setting interface

RSTP Root Bridge Information

Label	Description
Bridge ID	e.g., 8000-00C0F25A4001
Root Priority	e.g., 32768
Root Port	e.g., N/A if none assigned.
Root Path Cost	e.g., 0
Max Age Time	e.g., 20 seconds.
Hello Time	e.g., 2 seconds.
Forward Delay Time	e.g., 15 seconds.

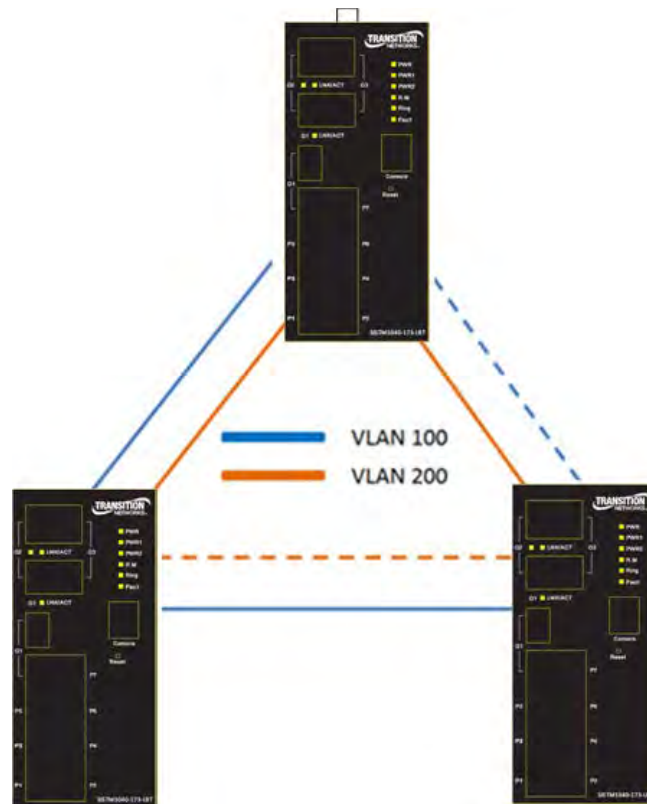
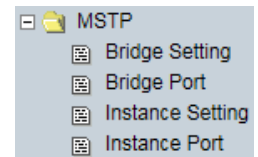
RSTP Port Information

Label	Description
Port	Displays one line for each port's configuration (Port.01 - Port.07, and G1 - G3).
Path Cost	The cost of the path to the other bridge from this transmitting bridge at the specified port. Valid values are 1 ~ 200000000 and the default value is 200000 for mega-ports and 20000 for giga-ports.
Port Priority	Displays port to be blocked by priority. Valid values are 0 ~ 240 in steps of 16 ; the default is 128 .
OperP2P	Displays <i>True</i> if enable or <i>False</i> if disabled.
OperEdge	Displays <i>True</i> if enable or <i>False</i> if disabled.
STP Neighbor	Displays <i>True</i> if enable or <i>False</i> if an STP neighbor has been discovered.
State	Displays the current state; e.g., <i>Forwarding</i> or <i>Disabled</i> .
Role	Displays the current role; e.g., <i>Disabled</i> , <i>Non STP</i> , <i>Designated</i> .

5.1.5.5 MSTP

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

The MSTP function allows several VLANs to be mapped to a reduced number of spanning tree instances because most networks do not need more than a few logical topologies. MSTP supports load balancing, and the CPU utilization is lower than PVST (Cisco proprietary technology). Section 13 of the ANSI/IEEE [802.1Q-2005 standard](#) discusses MSTP.



MSTP, originally defined in IEEE 802.1s and later merged into IEEE 802.1Q-2005, defines an extension to RSTP to further develop the usefulness of VLANs. MSTP configures a separate Spanning Tree for each VLAN group and blocks all but one of the possible alternate paths within each Spanning Tree.

If there is only one VLAN in the network, single (traditional) STP works appropriately. If the network contains more than one VLAN, the logical network configured by single STP would work, but it is possible to make better use of the alternate paths available by using an alternate spanning tree for different VLANs or groups of VLANs.

MSTP allows formation of MST *regions* that can run multiple MST *instances* (MSTI). Multiple regions and other STP bridges are interconnected using one single common spanning tree (*CST*).

MSTP > Bridge Setting

MSTP Setting	
MSTP Enable	Disable ▾
Force Version	MSTP ▾
Configuration Name	MSTP_SWITCH
Revision Level (0-65535)	0
Priority (0-61440)	32768
Max Age Time (6-40)	20
Hello Time (1-10)	2
Forward Delay Time (4-30)	15
Max Hops (1-40)	20

Priority must be a multiple of 4096.
 $2 * (\text{Forward Delay Time} - 1)$ should be greater than or equal to the Max Age.
 The Max Age should be greater than or equal to $2 * (\text{Hello Time} + 1)$.

Apply

MSTP Bridge Setting page

The following table describes the MSTP Bridge Setting screen labels.

Label	Description
MSTP Enable	You must enable the MSTP function before configuring the related parameters.
Force Version	This parameter can be used to force a VLAN Bridge that supports RSTP to operate in an STP-compatible manner (STP, RSTP, 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. See “MSTP Attribute Notes” below.
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 multiple of 4096 according to 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 seconds.
Hello Time (1-10)	This setting follows the rule below to configure the Max Age, Hello Time, and Forward Delay Time at controlled switch sends out the BPDU packet to check RSTP current status. Enter a value of 1 - 10. $2 \times (\text{Forward Delay Time value} - 1) \geq \text{Max Age value} \geq 2 \times (\text{Hello Time value} + 1)$

Label	Description
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 seconds.
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 configuration.

After you configure MSTP Bridge Setting page and click the **Apply** button, the CIST Root Bridge Information table displays the confured parameters:

MSTP Setting

MSTP Enable	Enable
Force Version	MSTP
Configuration Name	MSTP_SWITCH
Revision Level (0-65535)	0
Priority (0-61440)	32768
Max Age Time (6-40)	20
Hello Time (1-10)	2
Forward Delay Time (4-30)	15
Max Hops (1-40)	20

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).

CIST Root Bridge Information

MAC Address	00C0F25A4001
Priority	32768
Configuration Name	MSTP_SWITCH
Force Version	MSTP
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

Message: *Apply fail 802.1Q VLAN should be enabled first*

Meaning: You enabled MSTP without first enabling 802.1Q VLAN.

1. At **VLAN > VLAN Setting**, select 802.1Q as the VLAN Operation Mode.
2. At **Redundancy > MSTP > Bridge Setting** enable MSTP.
3. If necessary, reboot the device.

MSTP Attribute Notes

When switches have the same attributes they will be in the same region. It is possible to have one or more regions and these attributes must match: MST configuration name, MST configuration revision number (Level), and MST instance to VLAN mapping table.

When switches have the same attributes configured they will be in the same region. If the attributes are not the same the switch is seen as being at the boundary of the region.

The MST configuration name is just something you can make up to identify the MST region. The MST configuration revision number (Level) is also something you can make up so that you can change the number whenever you change your configuration. You can enter anything, as long as it's the same on all switches within the MST region.

MSTP > Bridge Port

- Open all
- System Information
- Front Panel
- Basic Setting
- DHCP Server
- Port Setting
- Redundancy
 - Redundant Ring
 - Multiple Ring
 - Multi-Ring
- RSTP
- MSTP
 - Bridge Setting
 - Bridge Port
 - Instance Setting
 - Instance Port
- VLAN
- SNMP
- Traffic Prioritization
- Multicast
- Security
- Warning
- Monitor and Diag
 - Save Configuration
 - Factory Default
 - System Reboot

MSTP Port

Port No.	Priority (0-240)	Path Cost (1-200000000, 0:Auto)	Admin P2P	Admin Edge	Admin Non Stp
Port.01					
Port.02	128	0	auto	true	false
Port.03					
Port.04					
Port.05					

priority must be a multiple of 16

Apply

Port Information

Port	Priority	Path Cost		P2P		Edge		Admin Non Stp
		Admin	Oper	Admin	Oper	Admin	Oper	
Port.01	128	Auto	2000000	Auto	False	True	True	False
Port.02	224	700000	700000	True	True	True	True	True
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	200000	Auto	True	True	True	False
G1	144	9000	9000	Auto	False	True	True	True
G2	144	9000	9000	Auto	False	True	True	True
G3	144	9000	9000	Auto	False	True	True	True

MSTP - Bridge Port page

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 (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 with RSTP depend on whether the port concerned 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. <i>true</i> means P2P enabled. <i>false</i> means P2P disabled.
Admin Edge	<i>true</i> means enabled. <i>false</i> means disabled.
Admin Non STP	<i>true</i> means enabled. <i>false</i> means disabled.
Apply	Click " Apply " to activate the configuration.

MSTP > Instance Setting

MSTP Instance

Instance	State	VLANs	Priority (0-61440)
1	Enable	1-4094	32768

Priority must be a multiple of 4096.

Apply

Instance Information

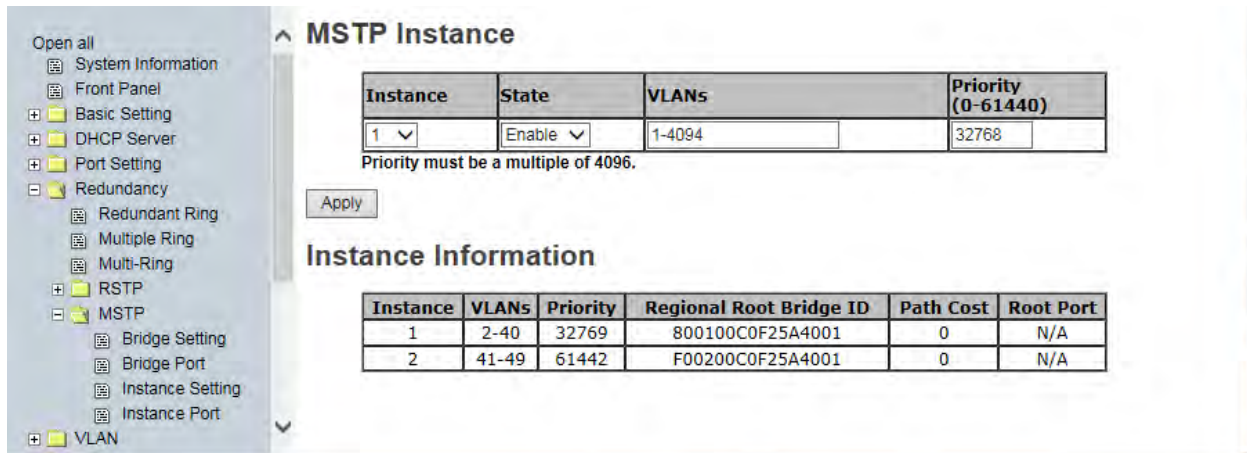
Instance	VLANs	Priority	Regional Root Bridge ID	Path Cost	Root Port
1	2-40	32769	800100C0F25A4001	0	N/A
2	41-49	61442	F00200C0F25A4001	0	N/A

MSTP - Instance Setting page

The following table describes the labels on this page.

Label	Description
Instance	Select an instance from 1 to 15.
State	At the dropdown, Enable or Disable the instance.
VLANs	Set which VLAN will belong to this instance (1-4094).
Proprietary (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.
Apply	Click “ Apply ” to activate the configuration.
Regional Root Bridge ID	Displays the Bridge ID, an 8 byte CIST Regional Root ID in MST/SPT BPDU. It includes the Bridge Priority, Bridge System ID Extension, and the Bridge MAC Address (e.g., 800100C0F25A4001.)
Path Cost	Displays the cost of the path to the other bridge from this transmitting bridge at this specific port (1 - 200000000 or 0 for Auto).
Root Port	When multiple paths from a bridge are least-cost paths, the chosen path uses the neighbor bridge with the lower bridge ID. The root port is thus the one connecting to the bridge with the lowest bridge ID.

For multiple MSTP instances, the MSTP instance VLAN can't overlap.



On the screen above, MSTP Instance 1 VLANs include VLANs 2-40 and MSTP Instance 2 VLANs include VLANs 41-49. If you tried to configure MSTP Instance 2 VLANs to include VLANs 40-49, VLAN 40 would be considered “overlapping” Instance 1 and an error message would display saying “*Apply fail MSTP instance VLAN can't overlap*”. In this case you would click the **Retry** button to clear the error message, and then re-enter the MSTP Instance 1 or 2 VLAN range so as to no longer overlap.

Message: *Bridge Max Age out of range*

Recovery: Click the **OK** button to clear the webpage message and re-configure the Max age parameter.

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

Recovery: Click the **OK** button to clear the webpage message and re-configure one of the parameters.

MSTP > Instance Port

MSTP Instance Port

Instance: 2

Port	Priority (0-240)	Path Cost (1-200000000, 0:Auto)
Port.01		
Port.02		
Port.03	128	0
Port.04		
Port.05		

Priority must be an multiple of 16

Apply

Instance Port Information

Port No.	Priority	Path Cost		State	Role
		Admin	Oper		
Port.01	128	Auto	2000000	Disabled	DisabledPort
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	200000	Forwarding	DesignatedPort
G1	128	Auto	2000000	Disabled	DisabledPort
G2	128	Auto	2000000	Disabled	DisabledPort
G3	128	Auto	2000000	Disabled	DisabledPort

MSTP Instance Port page

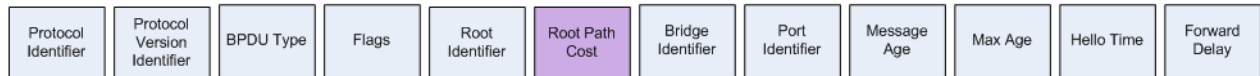
The following table describes the labels on this page.

Label	Description
Instance	Set the instance's information except CIST.
Port	Selecting the port that you want to configure. Use the Ctrl keyboard key with the left mouse button to select multiple ports.
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)	The cost of the path to the other bridge from this transmitting bridge at the specified port. Enter 0 for Auto or enter a number from 1 - 200000000 .
Apply	Click the Apply button to activate the current settings.

Spanning tree uses cost to determine the shortest path to the root bridge. The slower the interface, the higher the cost is. The path with the lowest cost will be used to reach the root bridge. Typically used:

<u>Bandwidth</u>	<u>Cost</u>
10 Mbps	100
100 Mbps	19
1000 Mbps	4

The BPDU has a field called “root path cost”, where each switch inserts the cost of its shortest path to the root bridge. Once the switches find out which switch is declared as *root bridge*, they look for the shortest path to get there.

BPDU:

Note that you can only run one redundancy protocol at a time. For example, if you try enable and configure both RSTP and MSTP at the same time, it would fail, displaying the message “*Apply fail Another redundancy protocol is running. Only one could be run at the same time*”. In this case you would click the **Retry** button to clear the error message, and disable one of the redundancy protocols.

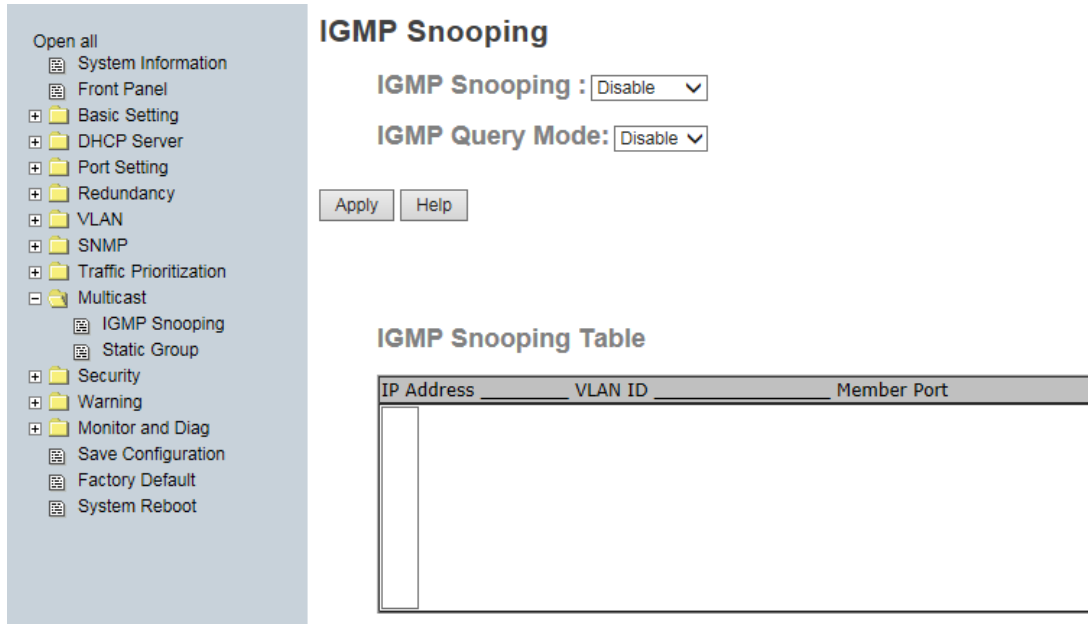
5.1.6 Multicast

5.1.6.1 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, v2 and v3. Refer to RFC 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.



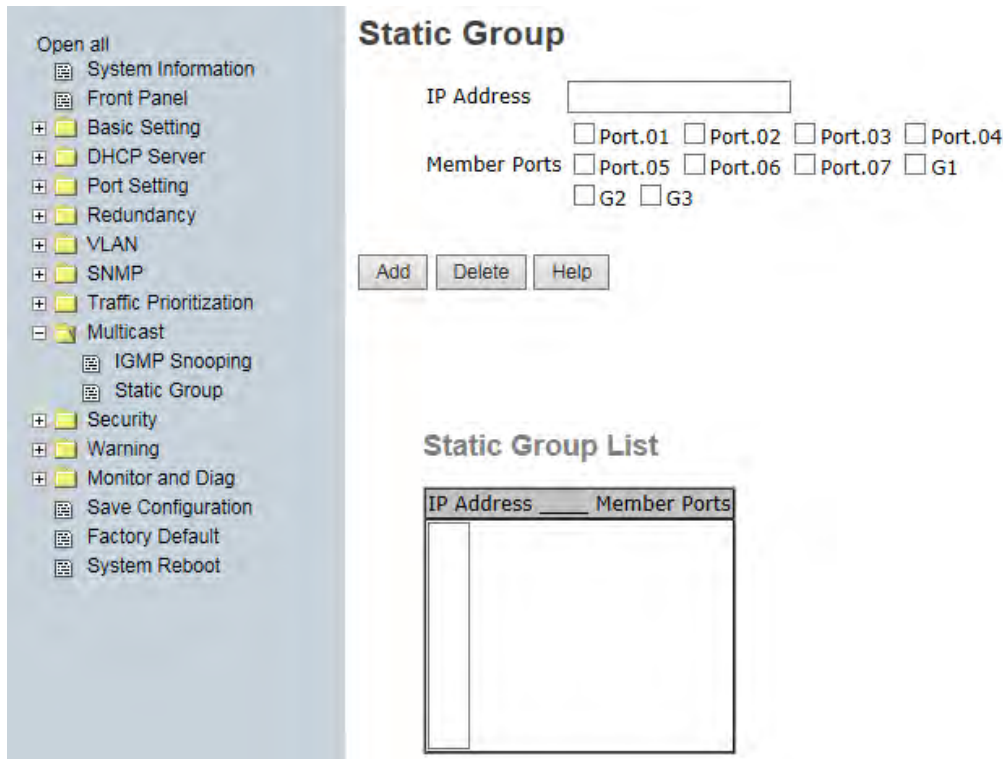
Multicast > IGMP Snooping page

The following table describes the labels on this page.

Label	Description
IGMP Snooping	Enable or 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 set the configurations.
Help	Show help file.

5.1.5.1 Static Group

Static Multicast filtering is the system by which end stations only receive multicast traffic if they register to join specific multicast groups. With multicast filtering, network devices only forward multicast traffic to the ports that are connected to registered end stations.



Multicast > Static Group page

The following table describes the labels on this page.

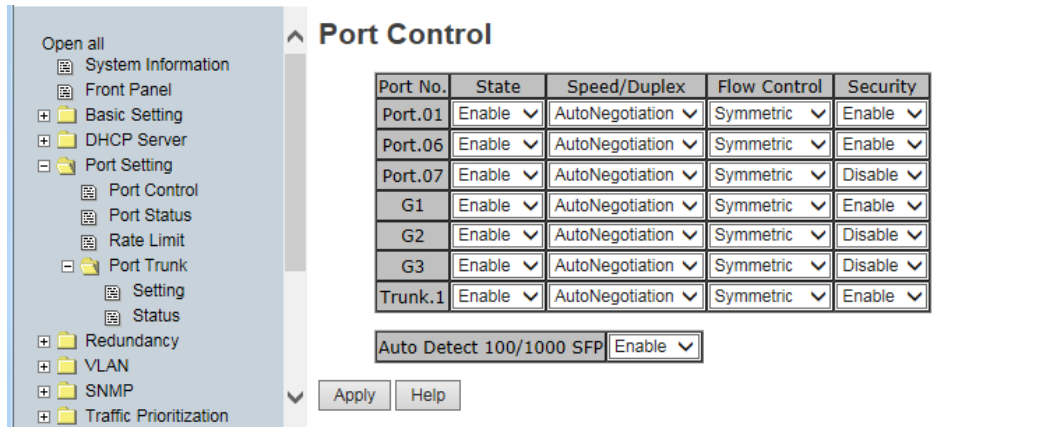
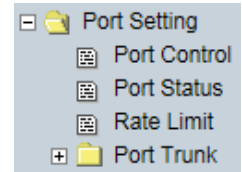
Label	Description
IP Address	Assign a multicast group IP address in the range of 224.0.0.0 ~ 239.255.255.255
Member Ports	Tick the check box beside the port number to include them as the member ports in the specific multicast group IP address.
Add	Show current IP multicast list.
Delete	Delete an entry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

Messages: If *Apply fail Table full* displays, click **Retry** and delete one or more instances.

5.1.6 Port Setting

5.1.6.1 Port Control

At Port Setting > Port Control you can set and monitor each port's state, speed/duplex, flow control, and security.



Port Control page

The following table describes the labels on this page.

Label	Description
Port No.	Port number for setting (e.g., Port.01 - Port.07 and G1 - G3). If a Trunk Port is configured and enabled it is also displayed (Trunk.1 shown above).
State	Enable or disable port transmission at the dropdown.
Speed/Duplex	Port.01 - Port.07: You can select AutoNegotiation, 100 Full, 100 Half, 10 Full, or 10 Half for speed and duplex. Also applies to a Trunk Port. G1 - G3: You can select AutoNegotiation, 1000 Full, 1000 Half, 100 Full, 100 Half, 10 Full, 10 Half, or 100 SFP.
Flow Control	Support symmetric and asymmetric mode to avoid packet loss when congestion occurs. Select "Disable", "Asymmetric", or "Symmetric" flow control. Disable will disable flow control ability. Symmetric means that flow control ability will be decided by the result of auto negotiation. Only both of linked up ports enable flow control, the flow control ability is just active. Asymmetric means that flow control ability is always active on this port whether the linked partner port enabled or not.
Security	Enabled port security will disable MAC address learning in this port. Thus only the frames with MAC addresses in port security list will be forwarded,

Label	Description
	otherwise will be discarded.
Auto Detect 100/1000 SFP	Enable or disable Automatic Detecting of SFP module speed (100M / 1000M).
Apply	Click " Apply " to activate the configurations.

5.1.6.2 Port Status

This page provides the current port status information from the **Port Setting > Port Control** menu path.

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
G1	1GTX/SFP	UP	Enable	1000 Full	Enable
G2	1GTX/SFP	Down	Enable	N/A	N/A
G3	1GTX/SFP	Down	Enable	N/A	N/A

Port Status page

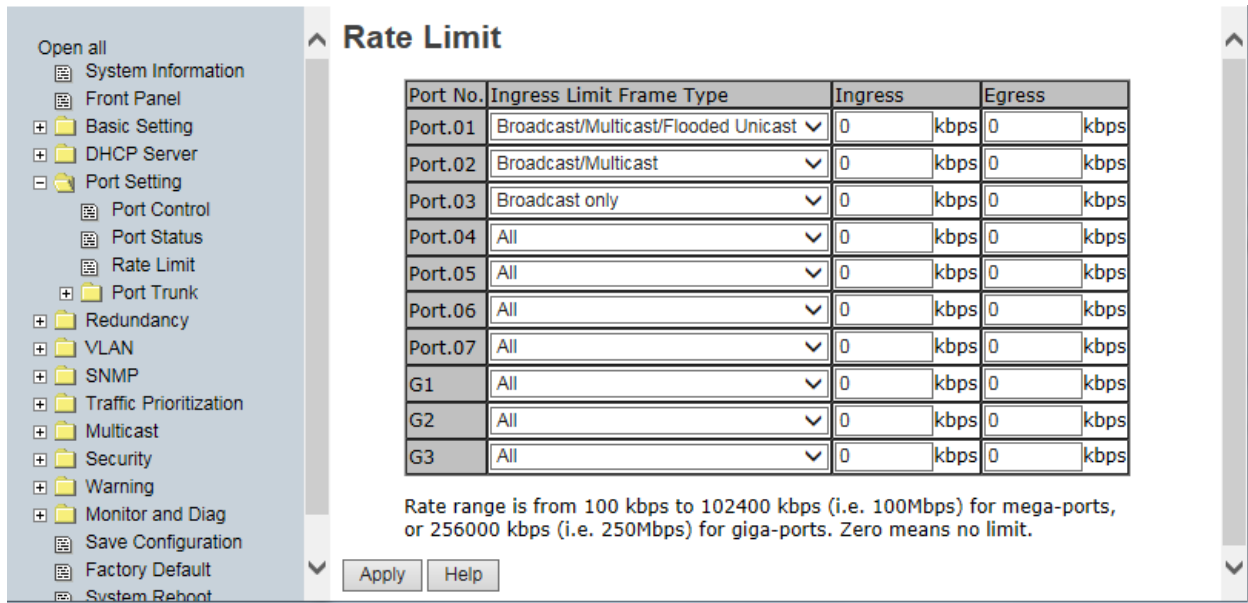
The following table describes the labels on this page.

Label	Description
Type	The type of port, such as 100TX or 1GTX/SFP.
Link	The current link status; <i>UP</i> or <i>Down</i> .
State	The current link state; <i>Enabled</i> or <i>Disabled</i> .
Speed/Duplex	The current speed setting and duplex mode; e.g., <i>1000 Full</i> for 1G speed and full duplex.
Flow Control	The current flow control setting; <i>Enabled</i> , <i>Disabled</i> , or <i>N/A</i> .

5.1.6.3 Rate Limit

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

The Rate range is from 100 kbps to 102400 kbps (100Mbps) for megabit ports, or 256000 kbps (250Mbps) for gigabit ports. Zero means no limit.



Rate Limit page

The following table describes the labels on this page.

Label	Description
Ingress Limit Frame Type	Select the types of frames to be limited against ingress rate limit. If an ingress frame is not included in this setting, it will not be limited. Note that this setting is only against ingress rate limit but not egress. You can set “ All ”, “ Broadcast only ”, “ Broadcast/Multicast ” or “ Broadcast/Multicast/Flooded Unicast ” mode.
Ingress	For the switch port received traffic, the value of ingress rate limit. The unit of measure is kbps; 1 Mbps is equal to 1024 kbps.
Egress	For the switch port transmitted traffic, the value of egress rate limit. The unit of measure is kbps; 1 Mbps is equal to 1024 kbps.

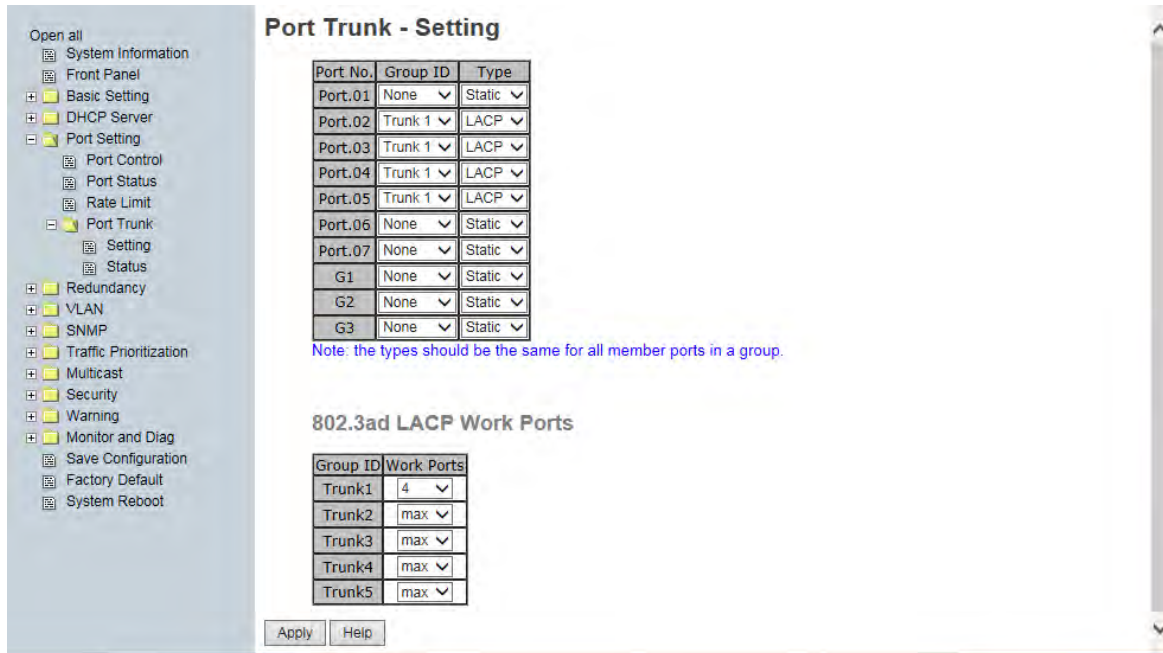
Message: If the *Apply fail BandWidth control rate is invalid.* displays, the Rate range entered is invalid for Ingress and/or Egress rate limiting. Click **Retry**, re-enter the invalid parameter, and click **Apply**

5.1.6.4 Port Trunk

Port Trunk > Setting

This page lets you select static trunk or 802.3ad LACP to combine several physical links with a logical link to increase the bandwidth. Note: the types should be the same for all member ports in a group.

Port trunk (Link Aggregation) is referred to in [IEEE 802.3ad](#). It allows one or more links to be aggregated together to form a Link Aggregation Group, such that a MAC client can treat the Link Aggregation Group as if it were a single link.



Port Trunk - Setting page

The following table describes the labels on this page.

Label	Description
Group ID	Select port to join a trunk group (None or Trunk 1 -Trunk 5).
Type	Select Static trunk or 802.3ad LACP . Join to a static trunk group directly or determine by IEEE 802.3ad LACP dynamically. Note that the types should be the same for all member ports in a group.
Work Ports	Select the number of active ports in dynamic group (LACP): max or 1-4 . The default value of Work Ports is maximum number of the group. If the number is not the maximum number of ports, the other inactive ports in the dynamic group will be suspended (no traffic). Once the active port is broken, the suspended port will be activated automatically.
Apply	Click the Apply button to set the configuration.

Port Trunk > Status

This page displays the selected Port Trunk Status (**Static** trunk or **802.3ad LACP**).

The screenshot shows a web interface with a left-hand navigation menu and a main content area titled "Port Trunk - Status". The navigation menu includes items like Port Setting, Port Control, Port Status, Rate Limit, Port Trunk, Setting, Status, Redundancy, VLAN, and SNMP. The main content area contains a table with the following data:

Group ID	Trunk Member	Type
Trunk 1	2, 3, 4, 5	802.3ad LACP
Trunk 2	N/A	Static
Trunk 3	N/A	Static
Trunk 4	N/A	Static
Trunk 5	N/A	Static

Port Trunk - Status page

Label	Description
Group ID	Trunk Group number (Trunk 1 - Trunk 5).
Trunk Member	Shows Group port information (e.g., Trunk 1 has ports 2, 3, 4 as members on the screen example above).
Type	Shows the current Trunk Type configured (Static or 802.3ad LACP).

LACP Notes

LACP works by sending LACPDU frames down all links that have the LACP protocol enabled. If LACP finds a device on the other end of the link that also has LACP enabled, it will also independently send frames along the same links enabling the two units to detect multiple links between themselves, and then combine them into a single logical link.

LACP can be configured in one of two modes: active or passive. In active mode it will always send frames along the configured links. In passive mode however, it "speaks when spoken to", and so can be used for controlling accidental loops (only if the other device is in active mode).

- The maximum number of bundled ports allowed in the port channel is typically 1-8.
- LACP packets are sent with multicast group MAC address 01-80-c2-00-00-02.
- During LACP detection period LACP packets are transmitted once per second.
- The Keep alive mechanism for link member default is slow=30 seconds, otherwise fast=1 second).
- The LACP active mode enables LACP unconditionally.
- The LACP passive mode enables LACP only when an LACP device is detected (the default).

An "aggregation mismatch" can occur if the aggregation type on both ends of the link does not match. Some switches do not implement the 802.1AX standard but support static configuration of link aggregation. Therefore, link aggregation between similarly statically configured switches will work, but will fail between a statically configured switch and a device that is configured for LACP.

See the IEEE standard at <http://standards.ieee.org/getieee802/download/802.1AX-2008.pdf>.

LACP and static link aggregation use the same algorithm, an XOR of the source and destination addresses.

In static link aggregation, all configuration parameters are stored just once on both devices involved in the LAG. As long as one link in a LAG is up, this link is also used for data transfer in static link aggregation. If media converters are used, if the link on the switch is up, but the connection to the switch at the other end is interrupted, the switch still sends data via this connection, and the data transfer is thus interrupted.

In dynamic link aggregation with LACP (which supports the exchange of information about link aggregation between the two parties involved) provides for more control than using static link aggregation.

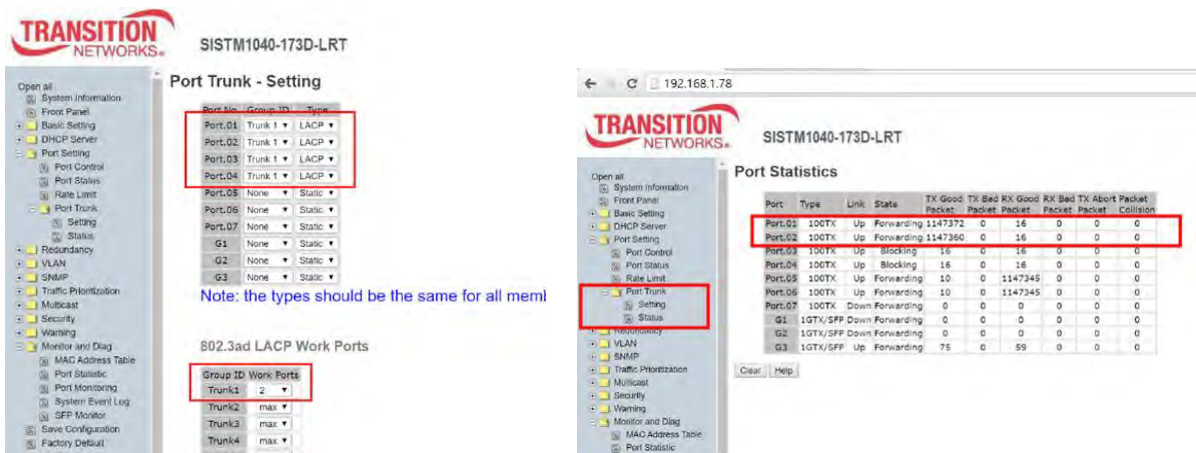
The primary reason for using LACP is the ability to configure fail-over links for the link aggregation "trunk". For example, with a switch that you can configure up to 6 "trunks" with 4 ports each, if you were to use LACP, you could configure more than 4 ports in the "trunk" and the additional ports will stay in a standby mode until one of the active ports fails.

When using static link aggregation, if one of the ports fails, the switch will continue to load-balance with the remaining links. You will simply decrease your bandwidth.

The failover scenario is one of the main reasons for LACP. While the algorithm may be the same, the difference is that static links do not require an LACP frame (a frame which includes LACP neighbor details and group ID). You must always have an active and a standby link with LACP and on any device supporting use of that protocol you need to bond two ports in an etherchannel/statically aggregated in at least two channels or else LACP will not function, hence the need for four ports.

The function is slightly different in a ring scenario, with RSTP and MSTP being disabled on an Redundant Ring device for example whereby only one protocol (e.g., Redundant Ring) is needed to actively disable ports like STP would. STP can be used in combination with aggregation but on the static links only (due to the first six digits of the MAC being the same as with the LACP protocol).

LACP Load Balance Example



LACP Messages

Message: *Apply fail Error: The number of WorkPort can't large than the number of members.*

Meaning: The number of work ports can not be less than zero or larger than the number of member ports.

Recovery. 1. Click the **Retry** button. 2. Change the 802.3ad LACP Work Ports settings; see above.

3. Click the **Apply** button to set the configuration.

Message: *Apply fail The number of member ports in a trunk group should be 2 to 4*

Recovery. 1. Click the **Retry** button. 2. Change the Member Ports settings; see above. 3. Click the **Apply** button to set the configuration.

Message: *Apply fail The port type and setting of member ports in a trunk group should be the same*

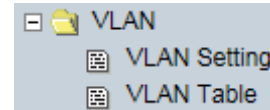
Meaning: You have a mis-configuration in the *Port Trunk - Setting* table and/or the *802.3ad LACP Work Ports* table at **Port Setting > Port Trunk > Settings**. The types should be the same for all member ports in a group.

Recovery. 1. Click the **Retry** button. 2. Change the Group ID, Type, and Work Ports settings; see above.

3. Click the **Apply** button to set the configuration.

5.1.7 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 VLAN will receive traffic from the same members of VLAN. Basically, creating a VLAN from a switch is logically equivalent of reconnecting a group of network devices to another Layer 2 switch. However, all the network devices are still plugged into the same switch physically.



The switch supports port-based and 802.1Q (tagged-based) VLAN. The default configuration of VLAN operation mode is at “802.1Q”.

5.1.7.1 VLAN Setting - IEEE 802.1Q

Tagged-based VLAN is an IEEE 802.1Q specification standard, and it is possible to create a VLAN across devices from different switch vendors. IEEE 802.1Q VLAN uses a technique to insert a “tag” into the Ethernet frames. The 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 can be configured. Enable 802.1Q VLAN, the all ports on the switch belong to default VLAN, VID is 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 Setting

VLAN Operation Mode : 802.1Q

GVRP Mode : Disable

Management VLAN ID : 0

VLAN Configuration

Port No.	Link Type	Untagged VID	Tagged VLANs
Port.01	Access	1	
Port.06	Access	1	
Port.07	Access	1	
G1	Access	1	
G2	Access	1	
G3	Access	1	
Trunk.1	Access	1	

Note: Use the comma to separate the multiple tagged VLANs.
E.g., 2-4,6 means joining the Tagged VLAN 2, 3, 4 and 6.

VLAN Configuration – 802.1Q page

The following table describes the labels on this page.

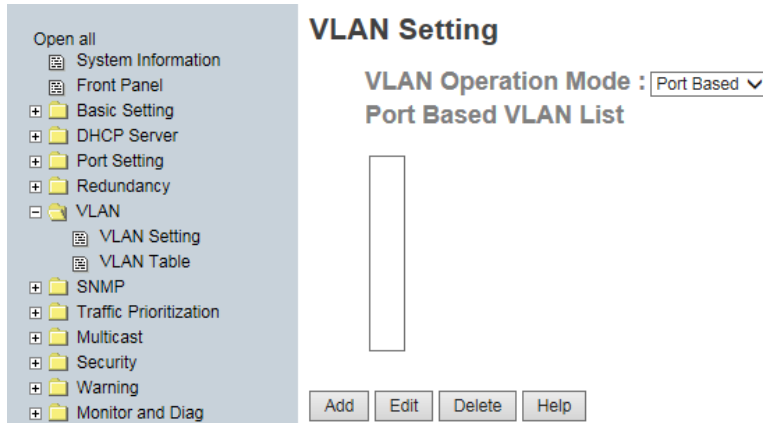
VLAN Configuration – 802.1Q interface

Label	Description
VLAN Operation Mode	At the dropdown select 802.1Q .
GVRP Mode	Enable or Disable the GVRP function.
Management VLAN ID	Management VLAN can provide network administrator a secure VLAN to management Switch. Only the devices in the management VLAN can access the switch. 0 means this function is disabled.
Port No.	Displays one line for each port (Port.01, Port.06, Port.07, G1, G2, G3, and Trunk.1).
Link Type	Select one of three link types: Access: the access link only supports an untagged VID. 1QTrunk: the 1Q trunk link only supports multiple tagged VIDs. Hybrid: 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 valid range is 1 - 4094.
Tagged VIDs	Set the tagged VIDs to carry different VLAN frames to another switch. Support 1~4094 and multiple VIDs. Use the comma to separate the multiple tagged VIDs (e.g., 2,3,4 means joining Tagged VLANs 2,3 and 4).
Apply	Click " Apply " to set the configurations.

Note: Use the comma to separate the multiple tagged VIDs (e.g., **2-4,6** means joining the Tagged VLANs 2, 3, 4 and 6).

5.1.7.2 VLAN Setting – Port Based

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

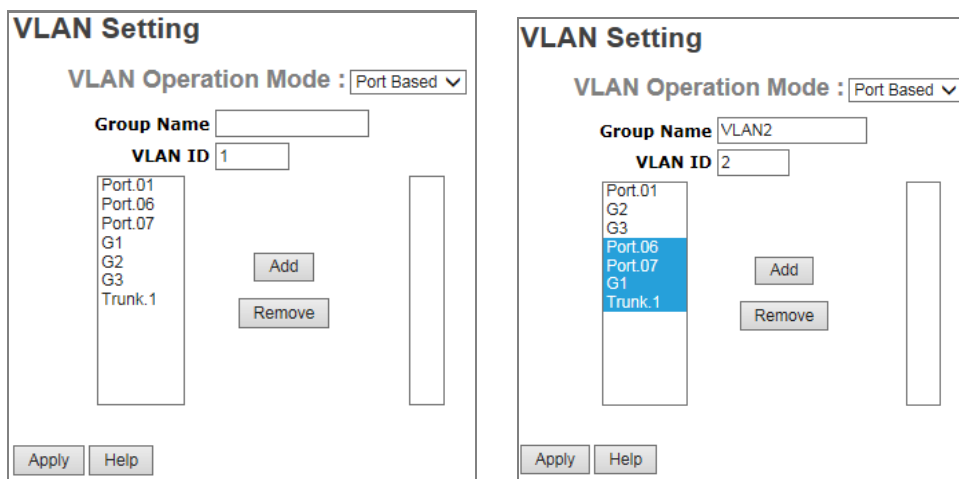


VLAN Configuration – Port Based page -1

Port-based VLAN Procedure

Traffic is forwarded to the member ports of the same vlan group.

1. At the VLAN Operation Mode dropdown select **Port Based**.
2. Create a VLAN (Group Name *VLAN2* below) and add member ports to it.
3. Click the **Add** button.
4. Type a name for the new VLAN.
5. Type a VID (VLAN ID 1-4094).
6. From the Available ports box, select one or more ports to add to the switch and click the **Add** button.
The port or ports selected move to the right-hand column (Port06, Port07, G1 and Trunk1 shown below right).
7. Click the **Apply** button.



VLAN Setting – Port Based page -2

VLAN Setting

VLAN Operation Mode : Port Based ▾

Group Name

VLAN ID

Available ports: Port.01, G2, G3

Selected ports: Port.06, Port.07, G1, Trunk.1

Buttons: Add, Remove, Apply, Help

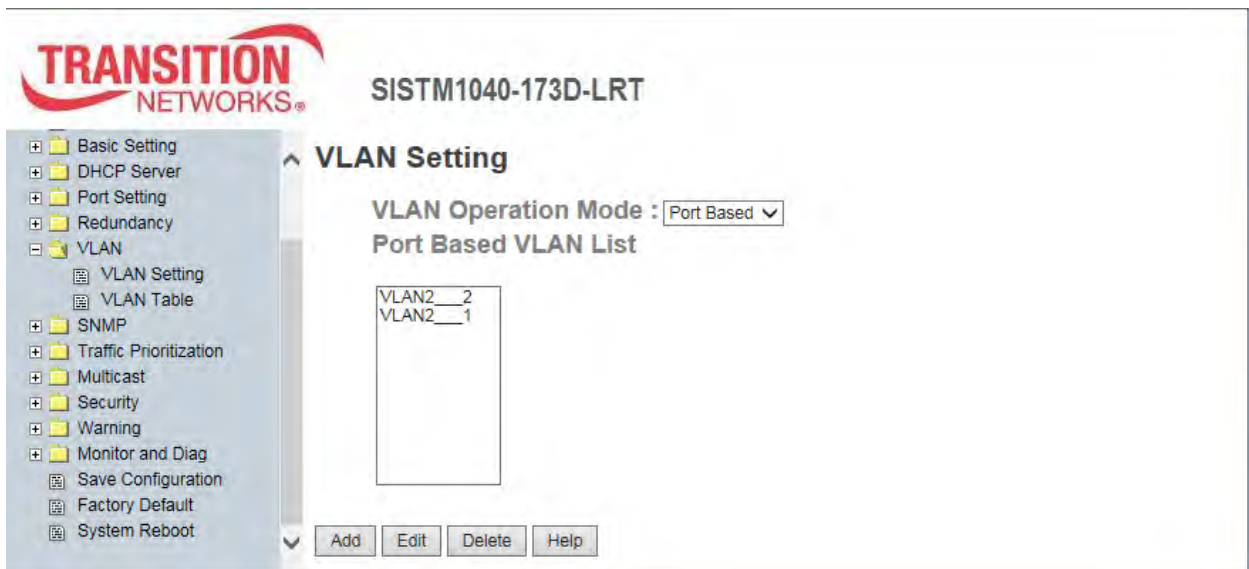
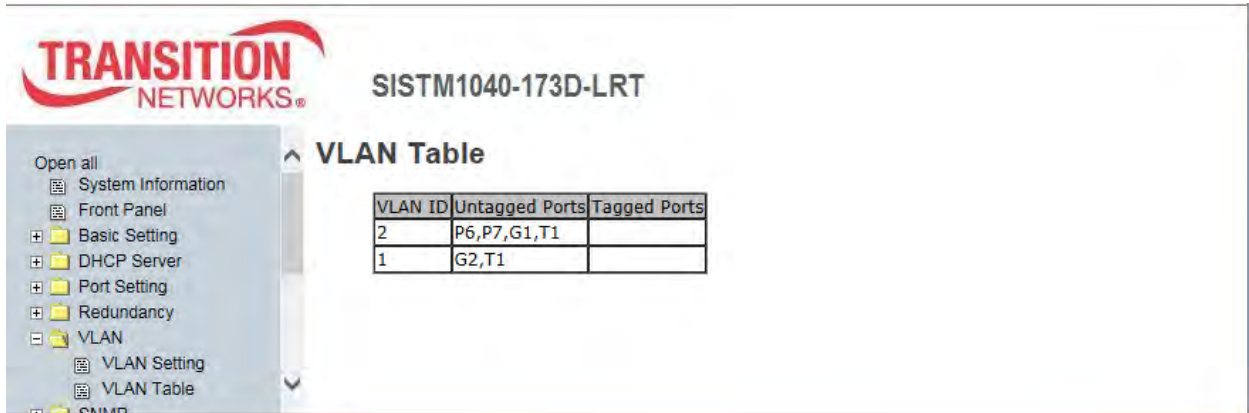
VLAN Setting – Port Based page -3

The following table describes the labels on this page.

Label	Description
VLAN Operation Mode	At the dropdown select Port Based .
Group Name	VLAN name (e.g., VLAN2 above right).
VLAN ID	Specify the VLAN ID (VID).
VLAN Port	The Available ports box for adding or removing ports to or from the VLAN (Port01, Port06, Port07, G1, G2, G3, and Trunk1).
Add	Select port(s) to join the VLAN group and click the Add button.
Remove	Click to remove selected port(s) from the VLAN group.
Apply	Click to set the configurations.
Help	Show the help file for this page.

5.1.7.3 VLAN Table

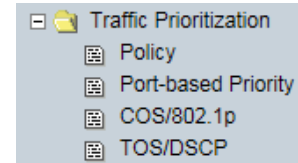
The VLAN Table displays the current VLAN settings (see above). The VLAN Table immediately below reflects the VLAN Settings in the screen below it.



You can use the **Add**, **Edit**, and **Delete** buttons to revise the VLAN Settings parameters.

5.1.8 Traffic Prioritization

Traffic Prioritization lets you configure Policy, Port-based Priority, COS /802.1p, and TOS/DSCP. With traffic prioritization, you can classify the traffic into four classes for differential network application. The switch supports four priority queues.



This switch supports a non-blocking, 4 priority, output port queue architecture. The traffic can be prioritized by port, COS field in VLAN tag, and TOS field in IP header.

Priority Types:

- 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.

Policy (Qos Policy)

- Using the 8,4,2,1 weight fair queue scheme: the output queues will follow 8:4:2:1 ratio to transmit packets from the highest to lowest queue. For 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 the strict priority scheme: always the packets in higher queue will be transmitted first until higher queue is empty.

COS/802.1p

COS (Class Of Service) is well known as 802.1p. It describes that the output priority of a packet is determined by user priority field in 802.1Q VLAN tag. Priority values 0~7 are supported.

COS Port Default

When an ingress packet has not VLAN tag, a default priority value is considered and determined by ingress port.

TOS/DSCP

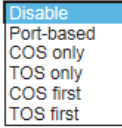
TOS (Type of Service) is a field in IP header of a packet. This TOS field is also used by Differentiated Services and is called the Diff Serv Code Point (DSCP). The output priority of a packet can be determined by this field and the priority value is supported 0~63.

5.1.8.1 Qos Policy

The screenshot shows a web interface for configuring QoS Policy. On the left, a navigation menu lists various settings, with 'Traffic Prioritization' expanded to show 'Policy'. The main area is titled 'Policy' and features a 'QoS Mode' dropdown menu currently set to 'Disable'. Below this, the 'QoS Policy' section has two radio button options: 'Use an 8,4,2,1 weighted fair queuing scheme' (unselected) and 'Use a strict priority scheme' (selected). At the bottom of the main area are 'Apply' and 'Help' buttons.

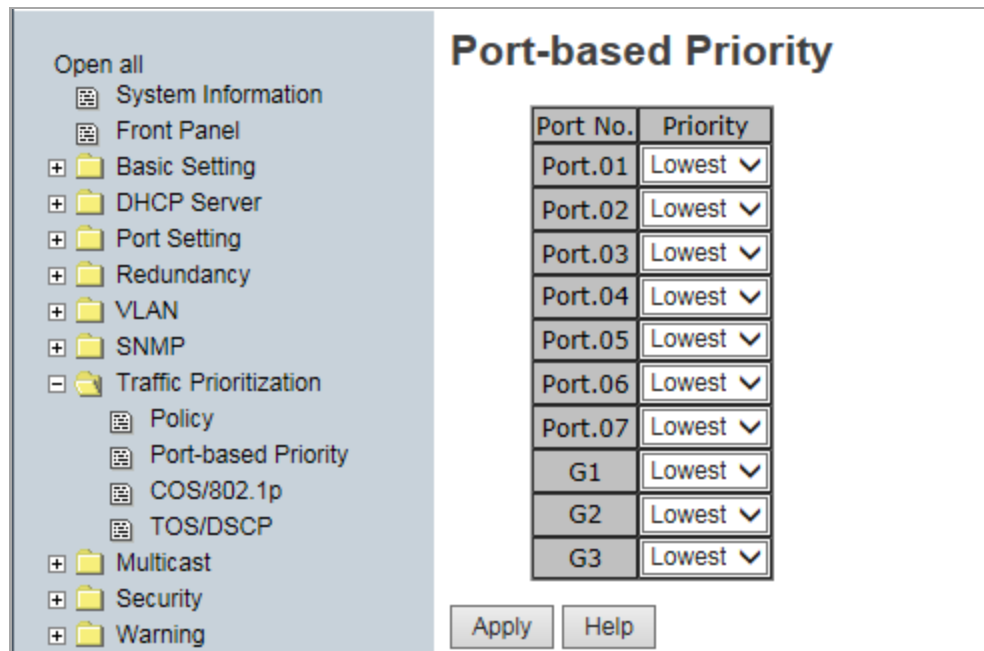
Traffic Prioritization > Policy page

The following table describes the labels on this page.

Label	Description
QoS Mode QoS Mode : 	Disable: QoS disabled (default). 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 weighted fair queuing scheme: the output queues will follow 8:4:2:1 ratio to transmit packets from the highest to lowest queue. For 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 the packets in higher queue will be transmitted first until higher queue is empty.
Apply	Click " Apply " to set the configurations.
Help	Show help file.

5.1.8.2 Port-based Priority

The Port-base Priority function lets you assign each Port with a priority queue. One of four priority queues can be assigned: High, Middle, Low, and Lowest.



Traffic Prioritization > Port-based Priority page

The following table describes the labels on this page

Label	Description
Priority	Assign each Port with one of four priority queues: High , Middle , Low , or Lowest .
Apply	Click " Apply " to set the configurations.
Help	Show help file.

5.1.8.3 COS/802.1p

COS (Class Of Service) is well known as 802.1p. It describes that the output priority of a packet is determined by user priority field in 802.1Q VLAN tag. The priority values supported are 0~7.

COS/802.1p

COS	Priority
0	Lowest
1	Lowest
2	Low
3	Low
4	Middle
5	Middle
6	High
7	High

COS Port Default

Port No.	COS
Port.01	0
Port.02	0
Port.03	0
Port.04	0
Port.05	0
Port.06	0
Port.07	0
G1	0
G2	0
G3	0

Traffic Prioritization > COS/802.1p page

The following table describes the labels on this page

Label	Description
COS/802.1p	COS (Class Of Service) is well known as 802.1p. It describes that the output priority of a packet is determined by user priority field in 802.1Q VLAN tag. The priority values supported are 0 - 7. COS value map to four priority queues: High, Middle, Low, and Lowest.
COS Port Default	When an ingress packet has not VLAN tag, a default priority value is considered and determined by ingress port.
Apply	Click Apply to set the configurations.
Help	Show help file.

5.1.8.4 TOS/DSCP

Traffic Prioritization > TOS/DSCP page

The following table describes the labels on this page

Label	Description
TOS/DSCP	TOS (Type of Service) is a field in 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 the priority value is supported 0to63. DSCP value map to four priority queues: High, Middle, Low, and Lowest.
Apply	Click “ Apply ” to set the configurations.
Help	Show help file.

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

Meaning: You mis-configured a Traffic Prioritization parameter.

Recovery: **1.** Click the **Retry** button to clear the message. **2.** Change traffic prioritization parameters to a valid combination; see above sections. **3.** Continue operation.

5.1.9 DHCP Server

5.1.9.1 DHCP Server – Basic Setting

The system provides with DHCP server function. Enable the DHCP server function, the switch system will be a DHCP server.

Label	Description
DHCP Server	Enable or Disable the DHCP Server function. <i>Enable</i> – the switch will be the DHCP server on your local network.
Start IP Address	The starting IP address of IP pool. The Start IP address is the beginning of the dynamic IP assigns range. For example: dynamic IP assign range is from 192.168.1.100 to 192.168.1.200. IP address 192.168.1.100 is the Starting IP address.
End IP Address	The ending IP address of IP pool. The End IP address is the end of the dynamic IP assigns range. For example: dynamic IP assign range is from 192.168.1.100 to 192.168.1.200. IP address 192.168.1.200 will be the End IP address
Subnet Mask	The dynamic IP assign range subnet mask.
Gateway	The gateway in your network.
DNS	Domain Name Server IP Address in your network.
Lease Time (Hour)	The period that system will reset the assigned dynamic IP to ensure the IP address is in used. The client will reclaim an IP address after lease time.
Apply	Click “ Apply ” to set the configurations.

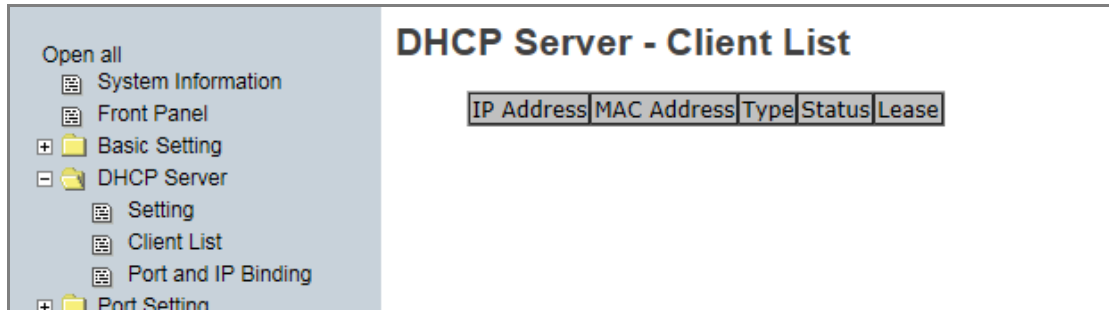
DHCP Server Configuration page

The following table describes the labels on this page.

Label	Description
DHCP Server	Enable or Disable the DHCP Server function. <i>Enable</i> – the switch will be the DHCP server on your local network.
Start IP Address	The starting IP address of IP pool. The Start IP address is the beginning of the dynamic IP assigns range. For example: dynamic IP assign range is from 192.168.1.100 to 192.168.1.200. IP address 192.168.1.100 is the Starting IP address.
End IP Address	The ending IP address of IP pool. The End IP address is the end of the dynamic IP assigns range. For example: dynamic IP assign range is from 192.168.1.100 to 192.168.1.200. IP address 192.168.1.200 will be the End IP address
Subnet Mask	The dynamic IP assign range subnet mask.
Gateway	The gateway in your network.
DNS	Domain Name Server IP Address in your network.
Lease Time (Hour)	The period that system will reset the assigned dynamic IP to ensure the IP address is in used. The client will reclaim an IP address after lease time.
Apply	Click “ Apply ” to set the configurations.

5.1.9.2 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 Entries page

The following table describes the labels on this page.

Label	Description
IP Address	The DHCP Server IP address.
MAC Address	The switch MAC address.
Type	The client type.
Status	The current status.
Lease	Lease Time; the client will reclaim an IP address after lease time.

5.1.9.3 DHCP Server – Port and IP Binding

You can assign the specific IP address which is in the assigned dynamic IP range to the specific port.

When the device is connecting to the port and asks for dynamic IP assigning, the system will assign the IP address that has been assigned before in the connected device.

Port No.	IP Address
Port.01	0.0.0.0
Port.02	0.0.0.0
Port.03	0.0.0.0
Port.04	0.0.0.0
Port.05	0.0.0.0
Port.06	0.0.0.0
Port.07	0.0.0.0
G1	0.0.0.0
G2	0.0.0.0
G3	0.0.0.0

DHCP Server Port and IP Binding page

The following table describes the labels on this page.

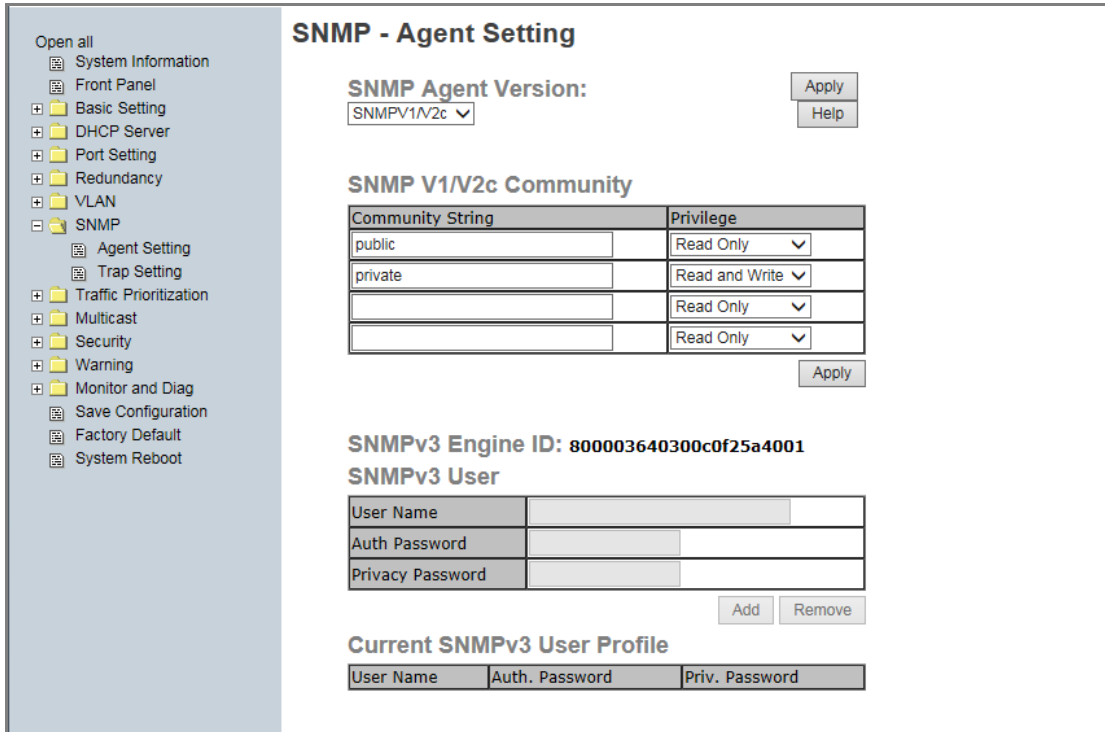
Label	Description
Port No.	Port.01 - Port.07 and G1 - G3.
IP Address	The DHCP Server IP address.

5.1.10 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 lets network administrators 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.

5.1.10.1 SNMP – Agent Setting

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



SNMP – Agent setting page

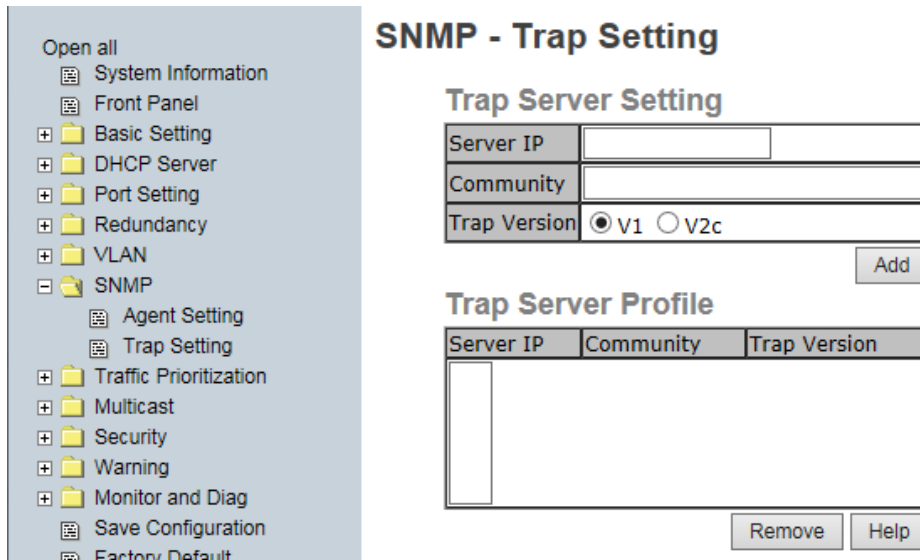
The following table describes the labels on this page.

Label	Description
SNMP Agent Version	The SNMP versions supported are SNMP V1/ V2c and SNMP V3. The SNMP V1/ V2c agent uses a community string match for authentication; that 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. Click Apply when done entering.
SNMP V1/V2c	SNMP Community should be set for SNMP V1/V2c. Four sets of

Community	"Community String/Privilege" are supported. Each Community String is maximum 32 characters. Keep empty to remove this Community string. Click Apply when done entering.
Community String	At the dropdown select Public or private.
Privilege	At the dropdown select Read Only or Read and Write.
SNMPv3 Engine ID	Displays the current SNMPv3 Engine ID (e.g., 800003640300c0f25a4001) (read only).
SNMPv3 User Name	The SNMPv3 User Name.
SNMPv3 Auth Password	The SNMPv3 Authentication Password.
SNMPv3 Privacy Password	The SNMPv3 privacy Password.
Current SNMPv3 User Profile - User Name / Auth. Password / Priv. Password	<p>If SNMP V3 agent is selected, the SNMPv3 user profile should be set for authentication.</p> <p>The User Name is necessary.</p> <p>The Auth Password is encrypted by MD5 and the Privacy Password which is encrypted by DES. There are up to 8 sets of SNMPv3 Users and up to 16 characters in User Name and Password. When SNMP V3 agent is selected, you can:</p> <ol style="list-style-type: none"> 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 than the Auth Password. <p>Click Add when done entering.</p> <p>Click Remove to undo the Add.</p>

5.1.10.2 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 issue. Create a trap manager by entering the IP address of the station and a community string. To define management stations as trap manager and enter SNMP community strings and selects the SNMP version.



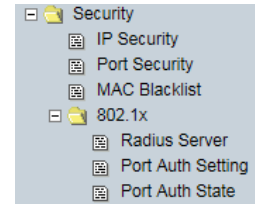
SNMP –Trap Setting page

The following table describes the labels on this page.

Label	Description
Server IP	The server IP address to receive Traps.
Community	Community for authentication.
Trap Version	Trap Version supports V1 or V2c .
Add	Add trap server profile.
Trap Server Profile	Displays the current trap server parameters.
Remove	Remove selected trap server profile.
Help	Show the help file for this page.

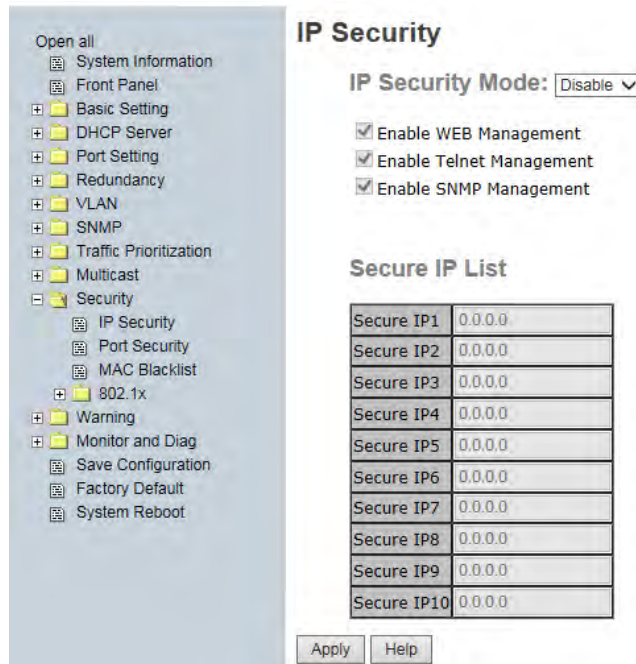
5.1.11 Security

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



5.1.11.1 IP Security

Only an IP in the Secure IP List can manage the switch through your defined management mode (Web, Telnet, SNMP). IP security can enable/disable remote management from WEB or Telnet or SNMP. Additionally, IP security can restrict remote management to some specific IP addresses. Then only these secure IP addresses can manage this switch remotely.



IP Security page

The following table describes the labels on this page.

Label	Description
IP Security Mode	Enable or Disable the IP security function.
Enable WEB Management	Check the box to enable Web Management.
Enable Telnet Management	Check the box to enable Telnet Management.
Enable SNMP Management	Check the box to enable SNMP Management.
Secure IP List	Enter an IP address in the Secure IP1 - Secure IP10 fields.
Apply	Click " Apply " to set the configurations.

5.1.11.2 Port Security

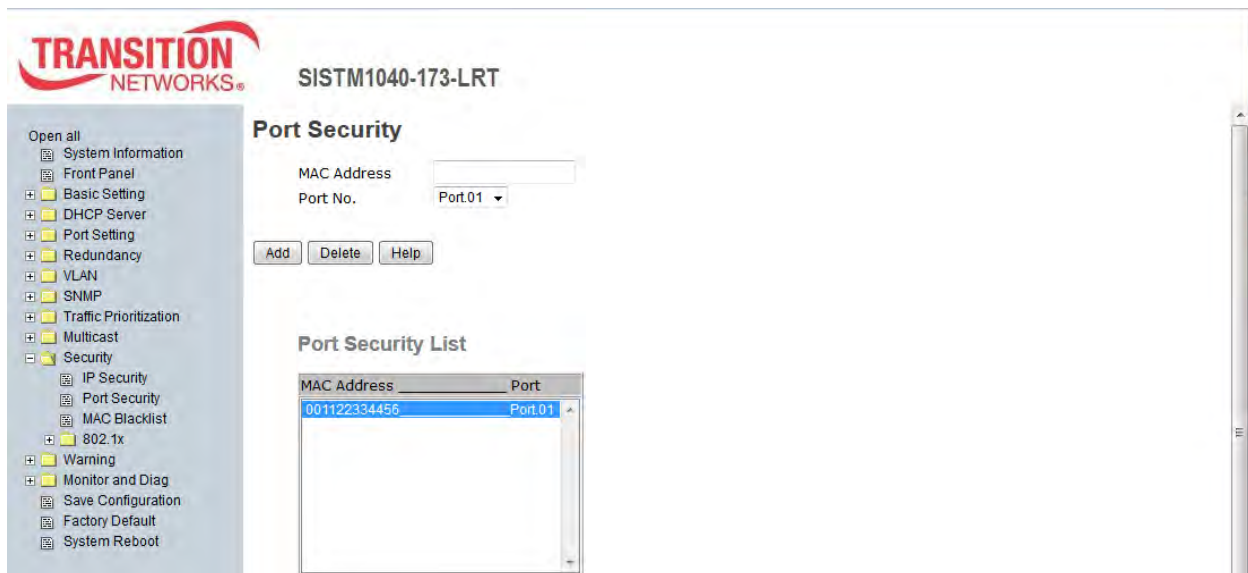
Port security is used to add static MAC addresses to hardware forwarding database. If port security is enabled at Port Control page, only the frames with MAC addresses in this list will be forwarded, otherwise they will be discarded.

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.



Port Security page

The following table describes the labels on this page.

Label	Description
MAC Address	Input MAC Address to a specific port.
Port No.	Select a switch port (Port.01, Port06, Port.07, G1, G2, G3, or Trunk.1).
Add	Add an entry of MAC and port information.
Delete	Delete the entry.

Message: *Apply fail Entry existed and can't be modified.* Click **Retry** and enter a different MAC address.

5.1.11.3 MAC Blacklist

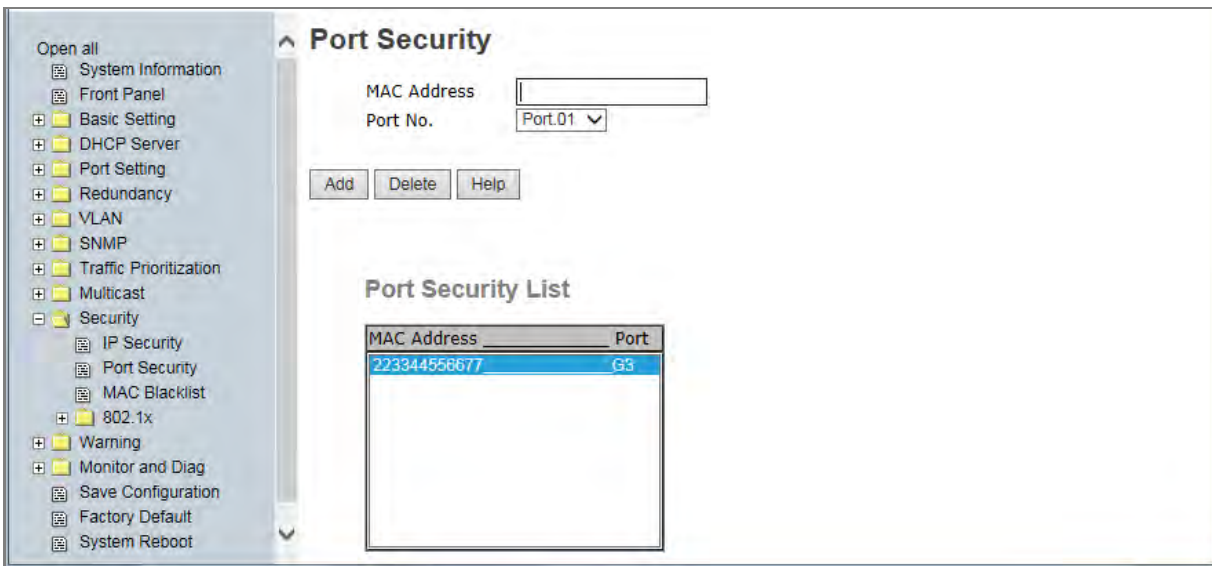
MAC Blacklist can eliminate traffic forwarding to specific MAC addresses in the list. Any frames forwarding to MAC addresses in this list will be discarded, so the target device will never receive any frames.

To add a MAC address filter:

1. In the MAC Address box, enter a MAC address, e.g. "001122334455".
2. Click the **Add** button.

To delete a filter MAC address:

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



MAC Blacklist page

The following table describes the labels on this page.

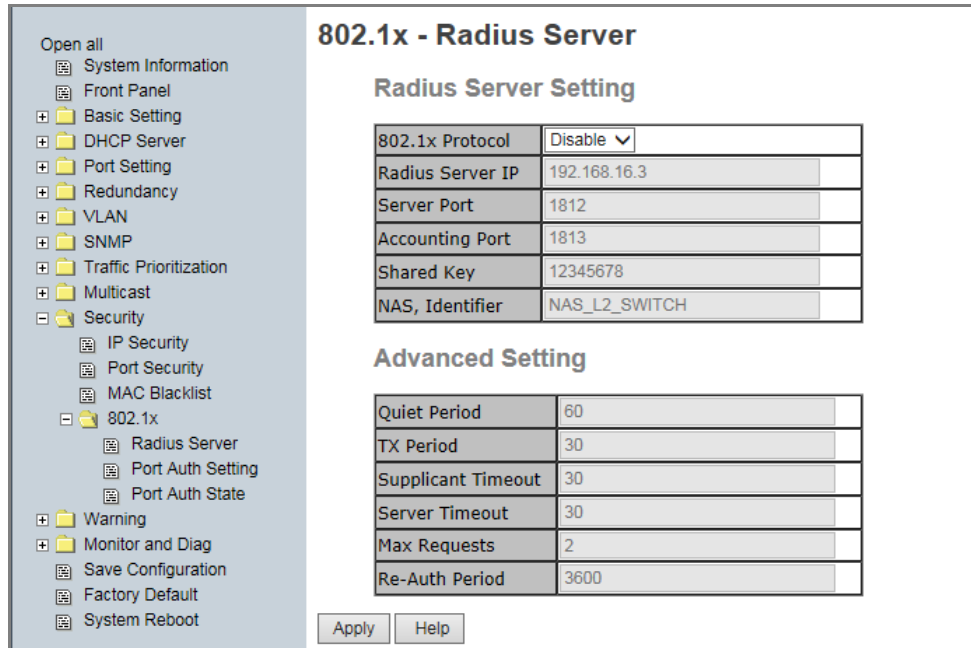
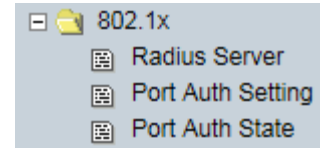
Label	Description
MAC Address	Input MAC Address to add to MAC Blacklist. The format is 112233445566.
Port No.	At the dropdown, select a Port No.(Port.01, Port.06, Port.07, G1, G2, G3, Trunk.1)
Add	Click the Add button to add an entry to the Blacklist table.
Delete	Delete the entry.
Help	Show help file.

Message: *Apply fail Entry existed and can't be modified.* Click **Retry** and enter a different MAC address.

5.1.11.4 802.1x

802.1x - Radius Server

802.1x makes use of the physical access characteristics of IEEE802 LAN infrastructures in order to provide a authenticated and authorized devices attached to a LAN port. Refer to IEEE 802.1X - Port Based Network Access Control.



802.1x Radius Server page

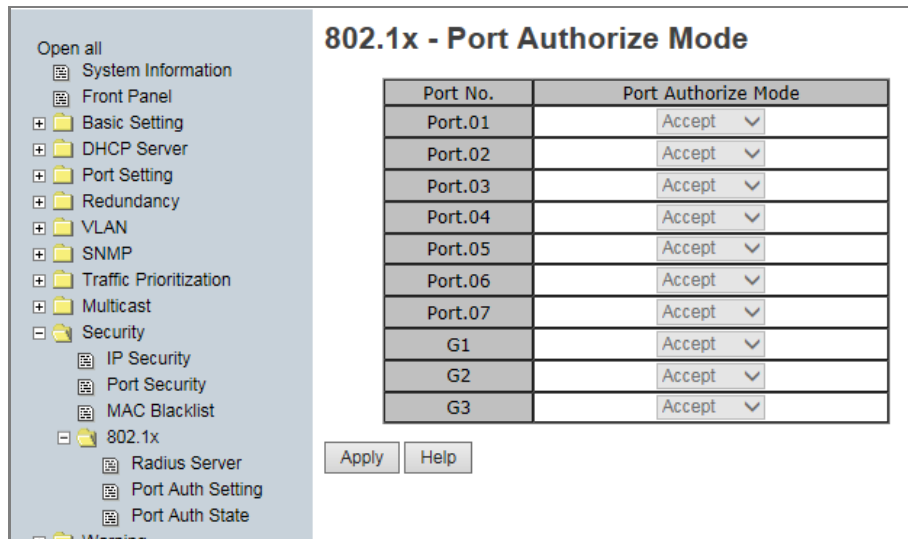
The following table describes the labels on this page.

Label	Description
802.1x Protocol	Enable or Disable 802.1X Radius Server function.
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.
Quiet Period	Set the time interval between authentication failure and the start of a new authentication attempt.

Label	Description
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.
Supplicant Timeout	Set the period of time the switch waits for a supplicant response to an EAP request.
Server Timeout	Set the period of time the switch waits for a Radius server response to an authentication request.
Max Requests	Set the maximum number of times to retry sending packets to the supplicant.
Re-Auth Period	Set the period of time after which clients connected must be re-authenticated.
Apply	Click " Apply " to set the configurations.

802.1x-Port Authorized Mode

This page lets you set the 802.1x authorized mode of each port.



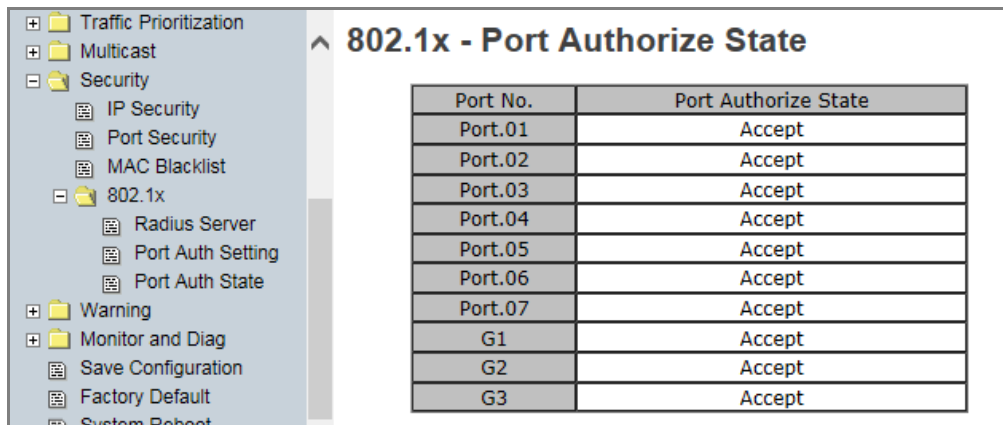
802.1x Port Authorize page

The following table describes the labels on this page.

Label	Description
Port Authorize Mode	<p>Reject: force this port to be unauthorized.</p> <p>Accept: force this port to be authorized.</p> <p>Authorize: the state of this port set by the outcome of 802.1x authentication.</p> <p>Disable: this port will not participate in 802.1x.</p>
Apply	Click “Apply” to set the configurations.

802.1x-Port Authorized State

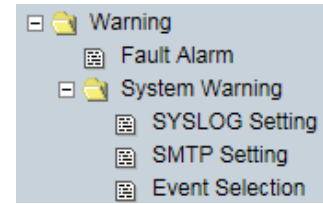
This page shows the 802.1x port authorized states as described in the previous section.



802.1x Port Authorize State page

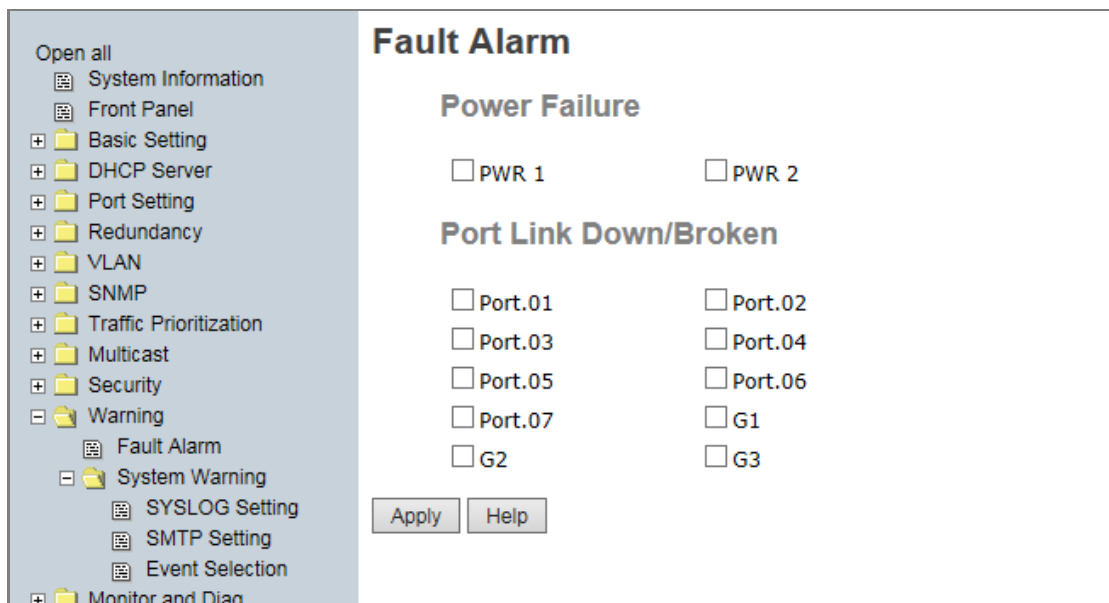
5.1.12 Warning

The Warning functions are important for managing the switch. You can manage the switch by SYSLOG, E-MAIL, and Fault Relay. It helps you monitor the switch status on a remote site. When events occur, a warning message is sent to your selected server, E-MAIL, or relay fault to switch panel. Fault alarm supports two warning settings: Syslog or SMTP E-Mail. You can monitor the switch through selected system events.



Warning > Fault Alarm

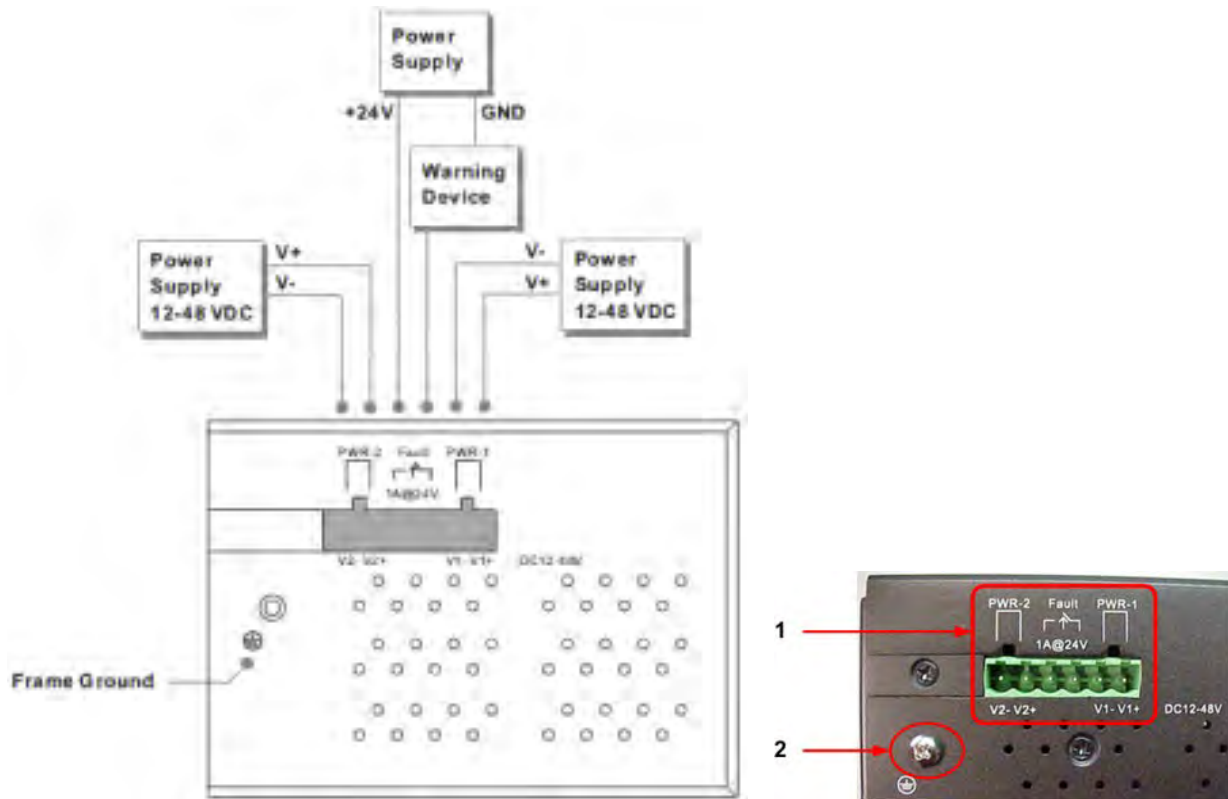
When any selected fault event occurs, the front panel Fault LED lights and the electric relay will signal at the same time.



The following table describes the labels on this page.

Label	Description
Power Failure	Fault alarm when any selected power failure. This switch supports dual power supplies. Check the checkbox to enable PWR 1 and/or PWR 2.
Port Link Down/Broken	Fault alarm when any selected port link is detected down or broken.
Apply	Click “ Apply ” to set the configurations.

The fault relay hardware aspects are shown below. See the related Quick Start Guide for more information.

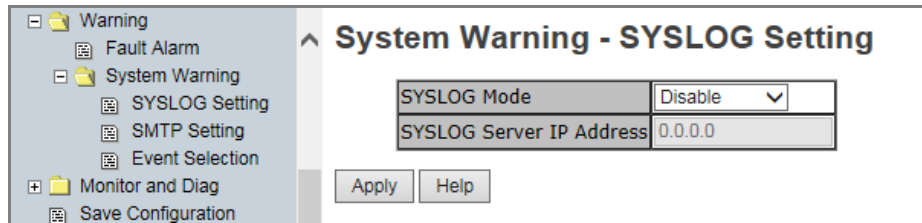


Fault contact: Relay output to carry capacity of 1A at 24VDC

Redundant Input Power: Dual DC inputs. 12 ~ 48VDC on 6-pin terminal block. **Note:** UL Approved power adapter (12-48Vdc, 1-0.25A, Amb. 70°C) required

System Warning > SYSLOG Setting

The SYSLOG is a protocol to transmit event notification messages across networks. Refer to RFC 3164 - The BSD SYSLOG Protocol.



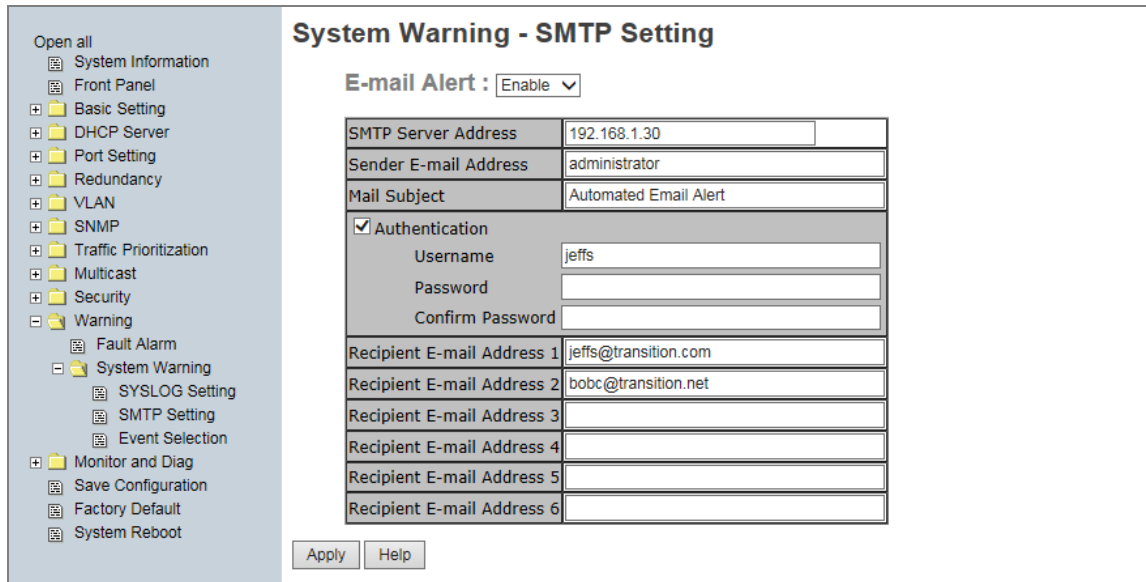
System Warning – SYSLOG Setting page

The following table describes the labels on this page.

Label	Description
SYSLOG Mode	<p>Disable: disable SYSLOG globally.</p> <p>Client Only: log to local system.</p> <p>Server Only: log to a remote SYSLOG server.</p> <p>Both: log to both local system and remote server.</p>
SYSLOG Server IP Address	The remote Syslog Server IP address.
Apply	Click “ Apply ” to set the configurations.
Help	Show the help file for this page.

System Warning > SMTP Setting

The SMTP (Short for Simple Mail Transfer Protocol) is a protocol for e-mail transmission across the Internet. Refer to RFC 821 - Simple Mail Transfer Protocol.



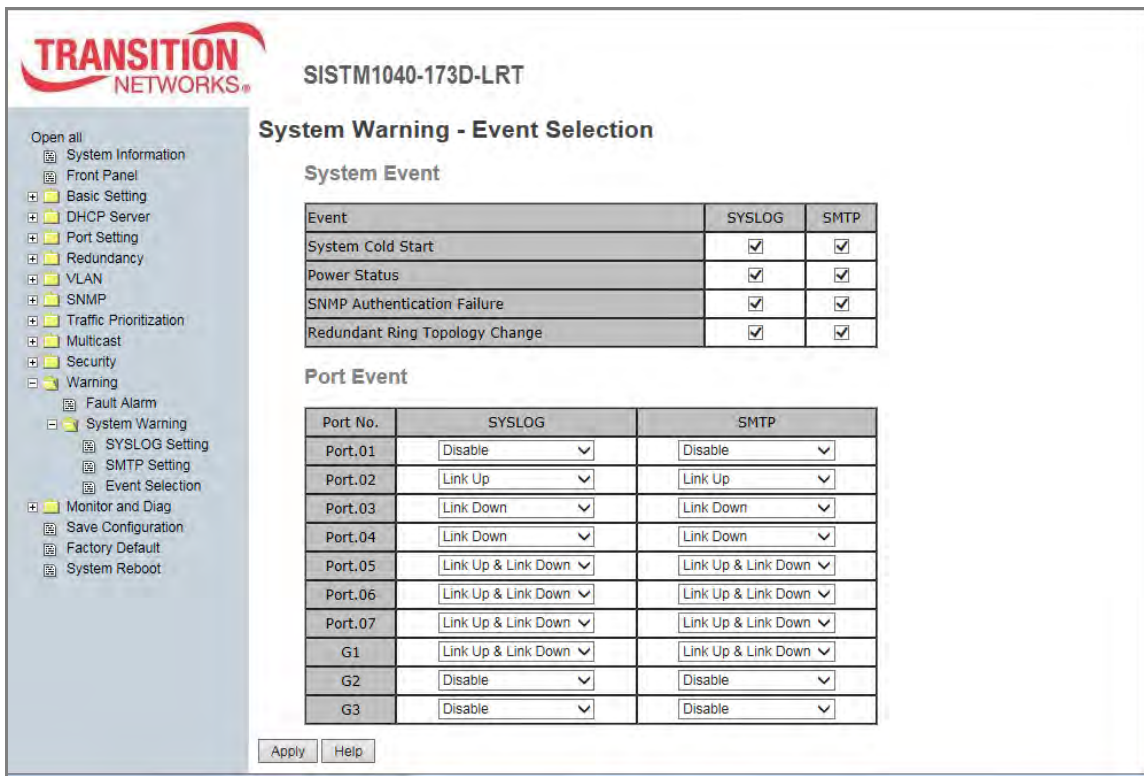
System Warning – SMTP Setting page

The following table describes the labels on this page.

Label	Description
E-mail Alert	Enable or Disable transmission of system warning events by e-mail.
SMTP Server Address	Setting up the mail server IP address.
Sender E-mail Address	Set up the email account to send the alert.
Mail Subject	The Subject of the mail.
Authentication	Username: enter the SMTP authentication username. Password: enter the SMTP authentication password. Confirm Password: re-enter password.
Recipient E-mail Address x	The recipient's E-mail address; up to 6 e-mail recipients supported.
Apply	Click “ Apply ” to set the configurations.
Help	Show help file.

System Warning > Event Selection

SYSLOG and SMTP are the two warning methods supported by the system. Check the corresponding box to enable system event warning method you wish to choose. **Note:** the checkboxes cannot be checked when SYSLOG or SMTP is disabled globally.



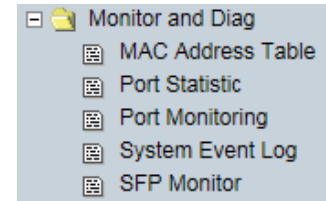
System Warning – Event Selection page

The following table describes the labels on this page.

Label	Description
System Cold Start	When the device executes a cold start, the system will issue an alert.
Power Status	If checked, the system will issue an alert when a power up or down occurs.
SNMP Authentication Failure	If checked, the system will issue an alert when an SNMP authentication failure is detected.
Redundant Ring Topology Change	If checked, the system will issue an alert when a Redundant Ring topology change is detected.
Port Event	At the dropdown, select Disable , Link Up , Link Down , and/or Link Up & Link Down
Apply	Click “ Apply ” to set the configurations.

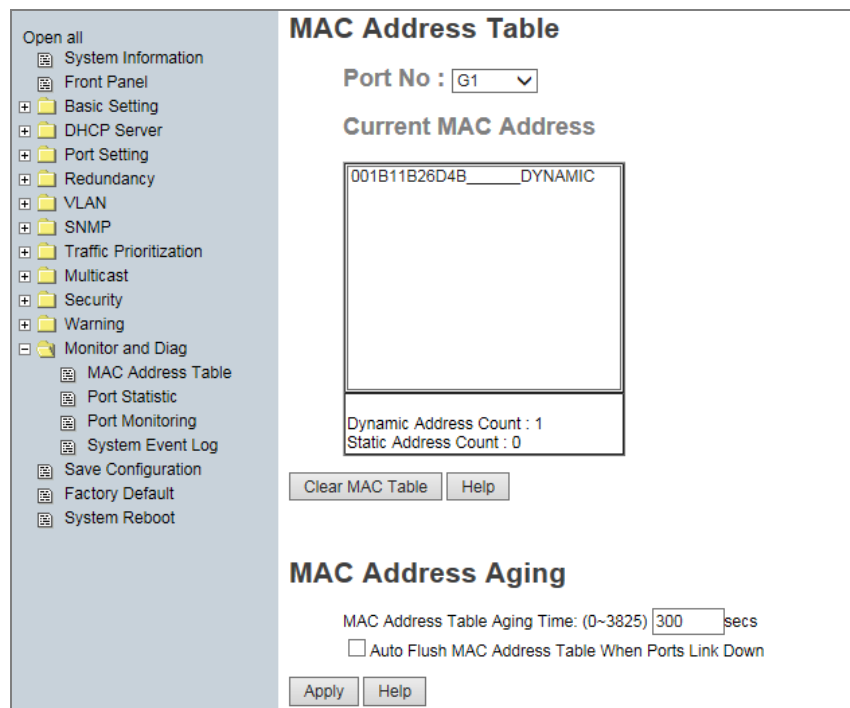
5.1.13 Monitor and Diag

The Monitor & Diag menu provides MAC Address Table, Port Statistics, Port Monitoring, System Event Log monitoring, and/or SFP Monitor.



5.1.13.1 MAC Address Table

Refer to IEEE 802.1 D Sections 7.9. The MAC Address Table, that is 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. This page shows all MAC addresses mapping to a selected port in table.



MAC Address Table page

The following table describes the labels on this page.

Label	Description
Port No.	Show all MAC addresses mapping to a selected port in table (Port No : Port.01, Port.06, Port.07, G1, G2, G3, Trunk.1).
Clear MAC Table	Click the button to clear all MAC addresses in the table.
MAC Address Aging Time	Assign aging time (0-3825 seconds); MUST be a multiple of 15.
Auto Flush Table When Ports Link Down	Enable this function when the port link is down; the switch will Flush the MAC table.

5.1.13.2 Port Statistics

The Port Statistics page displays several statistics counters for all ports. Note that this page automatically refreshes every 30 seconds which causes the screen to flash momentarily on refresh.

Port	Type	Link	State	TX Good Packet	TX Bad Packet	RX Good Packet	RX Bad Packet	TX Abort Packet	Packet Collision
Port.01	100TX	Down	Forwarding	0	0	0	0	0	0
Port.02	100TX	Down	Blocking	0	0	0	0	0	0
Port.03	100TX	Down	Blocking	0	0	0	0	0	0
Port.04	100TX	Down	Blocking	0	0	0	0	0	0
Port.05	100TX	Down	Blocking	0	0	0	0	0	0
Port.06	100TX	Down	Forwarding	0	0	0	0	0	0
Port.07	100TX	Up	Forwarding	36104	0	74636	0	0	0
G1	1GTX/SFP	Down	Forwarding	0	0	0	0	0	0
G2	1GTX/SFP	Down	Forwarding	0	0	0	0	0	0
G3	1GTX/SFP	Down	Forwarding	0	0	0	0	0	0

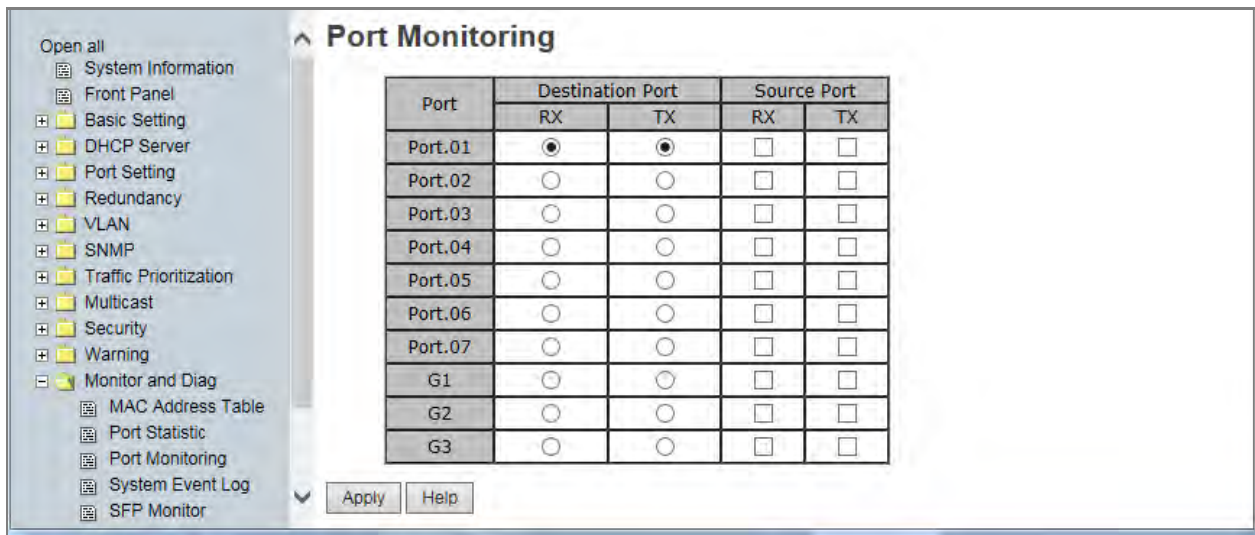
Port Statistics page

The following table describes the labels on this page.

Label	Description
Type	Show port speed and media type (100TX or 1GTX/SFP).
Link	Show port link status (Up or Down).
State	Show ports as Enable or Disable or Forwarding or Blocking.
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.
Help	Show help file.

5.1.13.3 Port Monitoring

The 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 keep all source ports unchecked to disable port monitoring.



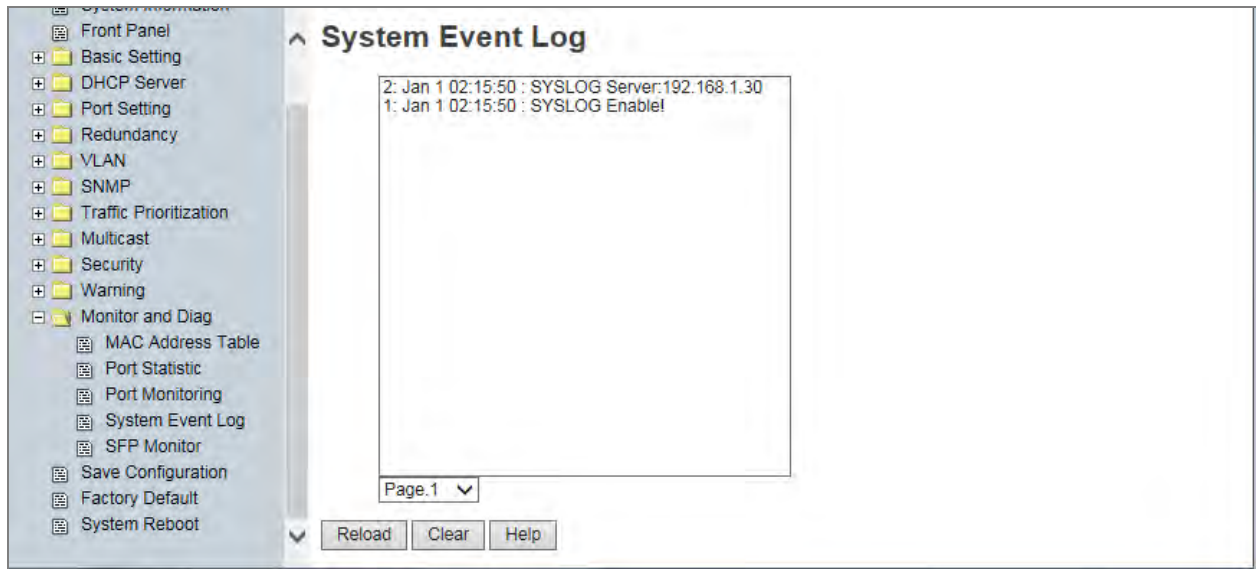
Port Monitoring page

The following table describes the labels on this page.

Label	Description
Destination Port	The port will receive a copied frame from source port for monitoring purposes.
Source Port	The port will be monitored. Mark the blank TX or RX box to be monitored.
TX	The frames come into switch port.
RX	The frames receive by switch port.
Apply	Click “ Apply ” to activate the configurations.
Clear	Clear all marked blank.(disable the function).
Help	Show help file.

5.1.13.4 System Event Log

If the System Log client is enabled, the system event logs display in this table.



System Event Log page

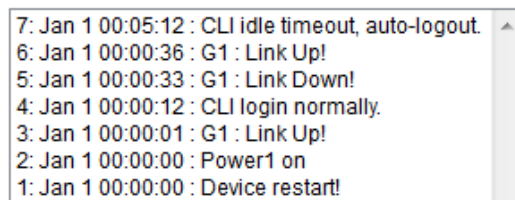
The following table describes the labels on this page.

Label	Description
Page	Select Log page.
Reload	Click to get the newest event logs and refresh this page.
Clear	Clear the displayed log.
Help	Show help file for this page.

Sample System Events Log:

- 7: Jan 1 00:05:12 : CLI idle timeout, auto-logout
- 6: Jan 1 00:05:36 : Link Up!
- 5: Jan 1 00:05:33 : Link Down!
- 4: Jan 1 00:05:12 : CLI login normally.
- 3: Jan 1 00:05:01 : Link Up!
- 2: Jan 1 00:05:00 : Power 1 on
- 1: Jan 1 00:05:00 : Device restart!

System Event Log



5.1.13.5 SFP Monitor

The [SFP Monitor page](#) displays DDMI diagnostics data and alarm settings for Gigabit Ethernet optical transceivers (SFP, SFP+, XFP, QSFP+, etc.) installed in the switch ports. A high alarm or low alarm generally indicates that the optics module is not operating properly. This information can be used to diagnose why an SFP transceiver is not working.

SFP Monitor

Port No.	Temperature (°C)	Vcc (V)	TX Bias (mA)	TX Power (µW)	RX Power (µW)
G1	31	3.2768	13.312	227.6	159.8
G2	53	3.2768	5.12	248	172.8
G3	N/A	N/A	N/A	N/A	N/A

Warning Temperature : °C(0~100)
 Event Alarm : Syslog SMTP

SFP Monitor page

The following table describes the labels on this page.

Label	Description
Port No.	The port number for the row being reported on (e.g., G1 - G3).
Temperature (C)	The temperature of the SFP/port (e.g., 50 °C).
Vcc (V)	Line voltage in Volts.
TX Bias (mA)	Transmit bias current in milliAmps.
TX Power (mW)	Transmit power in milliWatts.
RX Power (mW)	Receive power in milliWatts.
Warning Temperature	Enter the temperature to trigger a warning (0 - 100° C).
Event Alarm	Select alarm event reporting via Syslog, SMTP, or both.
Apply	Click the “Apply” button to activate the configuration changes.
Refresh	Click the “Refresh” button to update page report data.

Statement regarding SFP Temperatures:

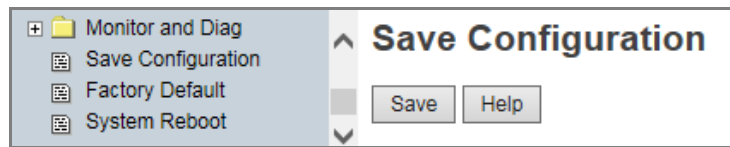
To keep hardened Transition Networks SFPs from overheating when installed, the SISTM1040-173D-LRT temperature rating should not exceed 55C. The ambient temperature rating for use with non-hardened SFPs should not exceed 35C.

Port	Temp	Model	Measured temp rise above ambient (24C)	Measured temperature distance from max rating
G1	58C	TN-SFP-LX8-C27	34C rise	12C (70C)
G2	53C	TN-SFP-SXD	29C rise	32C (85C)
G3	56C	TN-SFP-LX1	32C rise	29C (85C)

Model	Calculated ambient temp that causes SFP to reach max rated temp, when installed in SISTM1040-173D-LRT
TN-SFP-LX8-C27	36C
TN-SFP-SXD	56C
TN-SFP-LX1	53C

5.1.5 Save Configuration

If any configuration changed, “**Save Configuration**” should be clicked to save current configuration data to the permanent flash memory. Otherwise, the current configuration will be lost with a power off or a system reset.



System Configuration page

The following table describes the labels on this page.

Label	Description
Save	Click to save current configuration. When successful, displays the message <i>Save to Flash OK! Press Here to back to Previous Page.</i> Click to return to the Save Configuration page.

5.1.6 Factory Default



Factory Default page

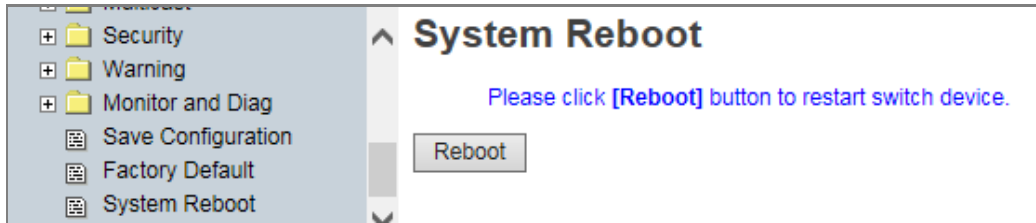
The Factory Default menu selection lets you reset switch to its default configuration.

Click **Reset** to reset all configurations to the default values. You can select “**Keep current IP address setting**” and “**Keep current username & password**” to keep current IP and username and password. After the **Reset** button is clicked, the system **MUST** be rebooted for the default configuration to be applied. When the webpage message “*Are you sure to Reset to Default?*” displays, click the **OK** button to start the reset process.

At the message “*Please click [Reboot] button to restart switch device.*” click the **Reboot** button to re-boot the switch.

5.1.7 System Reboot

At the prompt “Please click **[Reboot]** button to restart switch device.” click the **Reboot** button to restart the switch.



System Reboot page

The message: *Rebooting ... After several seconds, reconnect the system.* displays.

6. Command Line Interface (CLI)

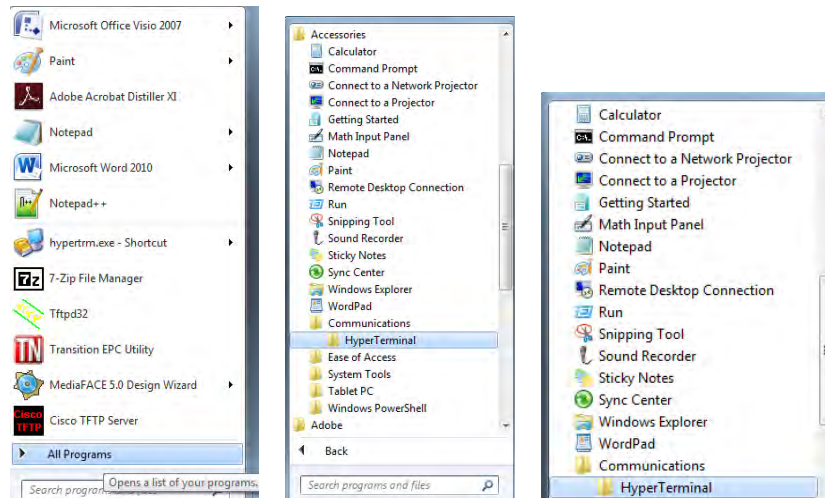
6.1 About CLI Commands

Besides Web-based management, the SISTM1040-173D-LRT also supports CLI management. You can use the console or telnet to manage that switch by CLI with the settings:

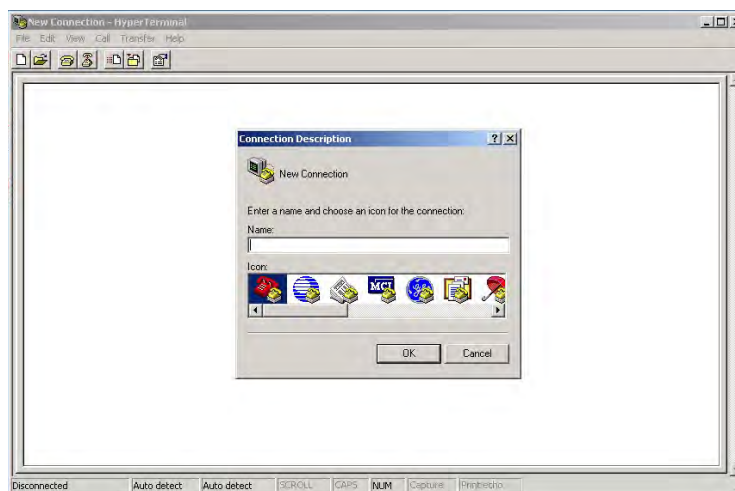
CLI Management by RS-232 Serial Console (9600, 8, none, 1, none)

Before configuring via the RS-232 serial console, use an RJ45 to DB9-F cable to connect the switch's RS-232 Console port to your PCs' COM port. Follow the steps below to access the console via RS-232 serial cable.

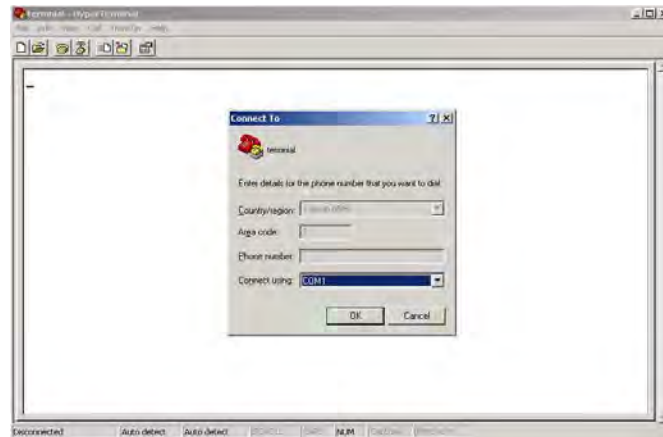
Step 1. From Windows desktop, click Start > All Programs -> Accessories -> Communications -> HyperTerminal:



Step 2. Enter a name for the new connection:



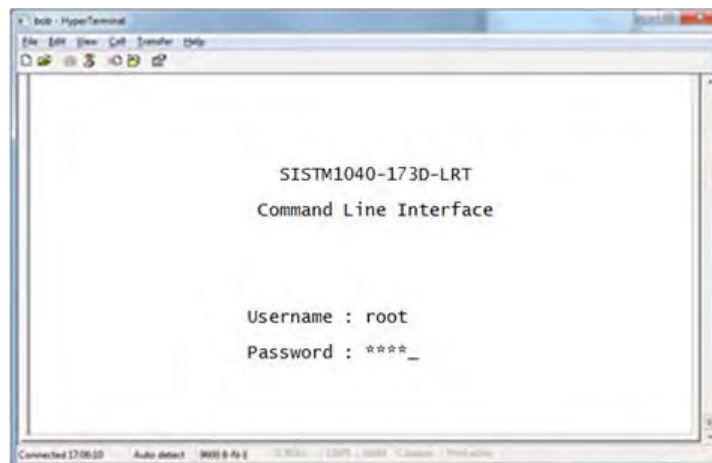
Step 3. At the Connect using dropdown, select the COM port number to use:



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 (**root**), press **Enter**, enter the Password (**root**), and then press **Enter** again.



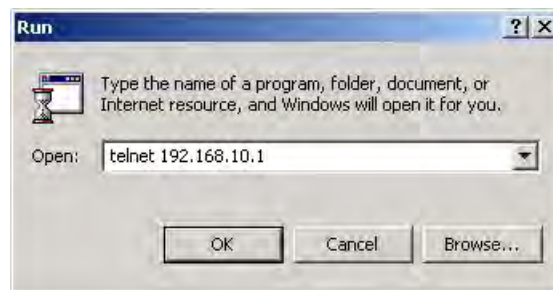
CLI Management by Telnet

You can use “**TELNET**” to configure the switches. 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**

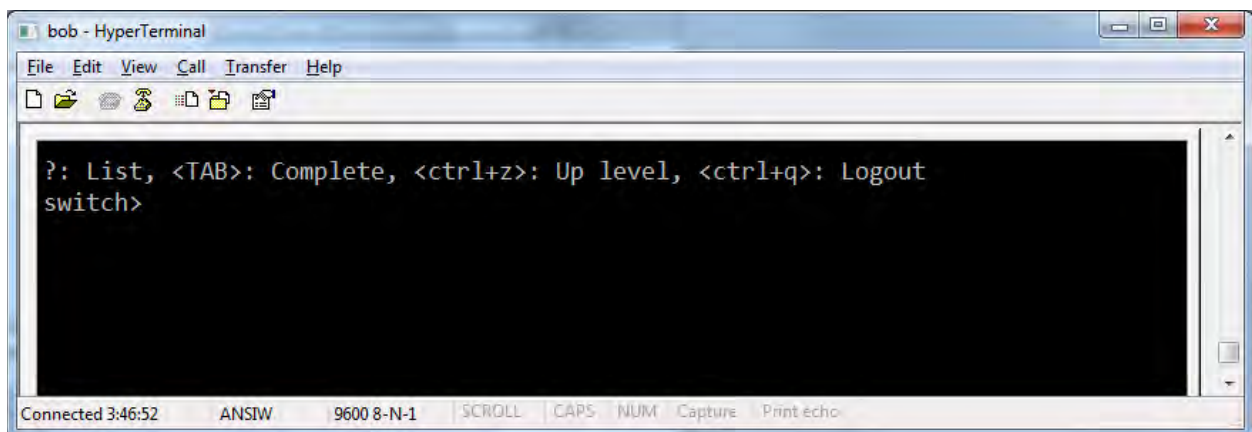
Follow the steps below to access the console via Telnet.

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 (**root**) and Password (**root**), and then press “**Enter**”.

The CLI main page displays:



The options displayed are:

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

Type a question mark (?) to display the User EXEC mode options. The question mark that you type does not actually display.

```
?: List, <TAB>: Complete, <ctrl+z>: Up level, <ctrl+q>: Logout
switch>?
enable          Enter Privileged EXEC mode
logout          Logout command line shell
ping           Ping function
quit           Logout command line shell
show           Show function
switch>
```

Type **show ?** to display the **show** command options

```
switch>show ?
config          Show switch configure
system-info     Show system information
switch>show
```

Priv Exec Mode Commands:

```
switch>enable
switch#
configure       Enter Global configuration mode
disable         Leave Privileged EXEC mode
show            Show function
vlan            Enter the vlan database command
write           Write current device configuration to memory
```


Config Mode Commands:

switch(config)#	
8021x	Configure IEEE802.1x function
admin	Configure administrator
aggregator	Configure aggregator port setting
auto-sfp	Enable/disable to auto detect 100/1000 SFP
check-concurrency	Check redundancy protocol concurrence
default	Restore to factory default configuration
dhcpserver	Configure DHCP server
end	Leave Global configuration mode
event	Configure system event selection
exit	Leave Global configuration mode
fault-relay	Configure Fault Relay Alarm function
igmp	IGMP function setting
interface	Enter the interface command (with a specific interface)
ip	Configure IP address
lldp	LLDP function setting
mac-address-table	Configure MAC address entry
mstp	Configure MSTP
multicast-filtering	Configure multicast filtering entry
multiple-ring	Configure Multiple Ring
no	Disable setting
open-ring	Configure Open-Ring
qos	Configure QOS function
reload	Reboot switch
ring	Configure Redundant Ring
rstp	Configure RSTP
security	Configure IP security
sfp-monitor	Configure SFP temperature alarm
smtp	Configure SMTP function
snmp	SNMP function
sntp	Set SNTP function
syslog	Configure SYSLOG function
system	Configure system detail information
tftp	Transfer file by TFTP
switch(config)#	

Command Levels

Modes	Access Method	Prompt	Exit Method	About This Mode
User EXEC	Begin a session with your switch.	switch>	Enter logout or quit .	The user command available at the level of user is a subset of those available at the privileged level. Use this mode to <ul style="list-style-type: none"> • Enter menu mode. • Display system info.
Privileged EXEC	Enter the enable command while in user EXEC mode.	switch#	Enter disable to exit.	The privileged command is an advanced mode That lets you: <ul style="list-style-type: none"> • display advanced function status • save configsettings
Global configuration	Enter the configure command while in privileged EXEC mode.	switch(co nfig)#	To exit to privileged EXEC mode, enter exit or end	Use this mode to configure parameters that apply to your switch as a whole.
VLAN database	Enter the vlan database command while in privileged EXEC mode.	switch(vla n)#	To exit to user EXEC mode, enter exit .	Use this mode to configure VLAN-specific parameters.
Interface configuration	Enter the interface command (with a specific interface)while in global configuration mode	switch(co nfig-if)#	To exit to global configuration mode, enter exit . To exist privileged EXEC mode or end .	Use this mode to configure parameters for the switch and Ethernet ports.

Command Level Symbols

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

6.2 System Commands

Commands	Level	Description	Example
show config	E	Show switch configuration	switch>show config
write memory	P	Save configuration into permanent memory (flash rom)	switch#write memory
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	Show system information	switch>show system-info
ip address [Ip-address] [Subnet-mask] [Gateway]	G	Configure the IP address of the 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	switch(config)#reload
default	G	Restore to default	Switch(config)#default
admin username [Username]	G	Changes a login username. (maximum 10 words)	switch(config)#admin username xxxxxx
admin password [Password]	G	Specifies a password (maximum 10 words)	switch(config)#admin password xxxxxx
show admin	P	Show admin info (user	switch#show admin

		name and password)	
dhcpserver enable	G	Enable DHCP Server	switch(config)#dhcpserver enable
dhcpserver lowip [Low IP]	G	Configure low IP address for IP pool	switch(config)# dhcpserver lowip 192.168.1.1
dhcpserver highip [High IP]	G	Configure high IP address for IP pool	switch(config)# dhcpserver highip 192.168.1.50
dhcpserver subnetmask [Subnet mask]	G	Configure subnet mask for DHCP clients	switch(config)#dhcpserver subnetmask 255.255.255.0
dhcpserver gateway [Gateway]	G	Configure gateway for DHCP clients	switch(config)#dhcpserver gateway 192.168.1.254
dhcpserver dnsip [DNS IP]	G	Configure DNS IP for DHCP clients	switch(config)# dhcpserver dnsip 192.168.1.1
dhcpserver leasetime [Hours]	G	Configure lease time (in hour)	switch(config)#dhcpserver leasetime 1
dhcpserver ipbinding [IP address]	I	Set static IP for DHCP clients by port	switch(config)#interface fastEthernet 2 switch(config-if)#dhcpserver ipbinding 192.168.1.1
show dhcpserver configuration	P	Show configuration of DHCP server	switch#show dhcpserver configuration
show dhcpserver clients	P	Show client entries of DHCP server	switch#show dhcpserver clinets
show dhcpserver ip-binding	P	Show IP-Binding information of DHCP server	switch#show dhcpserver ip-binding
no dhcpserver	G	Disable DHCP server function	switch(config)#no dhcpserver
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 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	switch#show security

		IP 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 telnet	G	Disable IP security of telnet server	switch(config)#no security telnet

6.3 Port Commands

Commands	Level	Description	Example
interface fastEthernet [Portid]	G	Choose the port for modification.	switch(config)#interface fastEthernet 2
duplex [full half]	I	Use the duplex configuration 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 configuration 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 giga port..	switch(config)#interface fastEthernet 2 switch(config-if)#speed 100
flowcontrol mode [Symmetric Asymmetric]	I	Use the flowcontrol configuration 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

bandwidth type all	I	Set interface ingress limit frame type to “accept all frame”	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type all
bandwidth type broadcast-multicast-flooded-unicast	I	Set interface ingress limit frame type to “accept broadcast, multicast, and flooded unicast frame”	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type broadcast-multicast-flooded-unicast
bandwidth type broadcast-multicast	I	Set interface ingress limit frame type to “accept broadcast and multicast frame”	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type broadcast-multicast
bandwidth type broadcast-only	I	Set interface ingress limit frame type to “only accept broadcast frame”	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type broadcast-only
bandwidth in [Value]	I	Set interface input bandwidth. Rate Range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports, and zero means no limit.	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth in 100
bandwidth out [Value]	I	Set interface output bandwidth. Rate Range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports, and zero means no limit.	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth out 100
show bandwidth	I	Show interfaces bandwidth control	switch(config)#interface fastEthernet 2 switch(config-if)#show bandwidth
state [Enable Disable]	I	Use the state interface configuration command to specify the state mode of operation for Ethernet ports. Use the disable	switch(config)#interface fastEthernet 2 switch(config-if)#state Disable

		form of this command to disable the port.	
show interface configuration	I	show interface configuration status	switch(config)#interface fastEthernet 2 switch(config-if)#show interface configuration
show interface status	I	show interface actual status	switch(config)#interface fastEthernet 2 switch(config-if)#show interface status
show interface accounting	I	show interface statistic counter	switch(config)#interface fastEthernet 2 switch(config-if)#show interface accounting
no accounting	I	Clear interface accounting information	switch(config)#interface fastEthernet 2 switch(config-if)#no accounting

6.4 Trunk Commands

Commands	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] :1-3 [Port-list]:Member port list, This parameter could be a port range(ex.1-4) or a port list separate by a comma(ex.2, 3, 6) [Workport]: The number of work ports, this value can not be less than zero or be larger than the number 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
aggregator group [GroupID] [Port-list]	G	Assign a static trunk group.	switch(config)#aggregator group 1 2-4 nolacp

nolacp		[GroupID] :1to3 [Port-list]:Member port list, This parameter could be a port range(ex.1-4) or a port list separate by a comma(ex.2, 3, 6)	or switch(config)#aggregator 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 aggregator lacp 1
no aggregator group [GroupID]	G	Remove a trunk group	switch(config)#no aggregator group 2

LACP Commands Summary

```

aggregator          Configure aggregator port setting
switch<config> # aggregator ?
activityport       Set activity port for LACP [Group ID] [Port List]
group              Assign group ID and port member list
priority          Set LACP priority

```

6.5 VLAN Commands

Commands	Level	Description	Example
vlan database	P	Enter VLAN configure mode	switch#vlan database
vlan [8021q gvrp]	V	To set switch VLAN mode.	switch(vlan)# vlanmode 802.1q or switch(vlan)# vlanmode gvrp
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 belong 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 belong 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 belong 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 aggregator [TrunkID] access-link untag [UntaggedVID]	V	Assign a access link for VLAN by trunk group	switch(vlan)#vlan 8021q aggregator 3 access-link untag 33
vlan 8021q aggregator [TrunkID] trunk-link tag [TaggedVID List]	V	Assign a trunk link for VLAN by trunk group	switch(vlan)#vlan 8021q aggregator 3 trunk-link tag 2,3,6,99 or switch(vlan)#vlan 8021q aggregator 3

			trunk-link tag 3-20
vlan 8021q aggregator [PortNumber] hybrid-link untag [UntaggedVID] tag [TaggedVID List]	V	Assign a hybrid link for VLAN by trunk group	switch(vlan)# vlan 8021q aggregator 3 hybrid-link untag 4 tag 3,6,8 or switch(vlan)# vlan 8021q aggregator 3 hybrid-link untag 5 tag 6-8
show vlan [VID] or show vlan	V	Show VLAN information	switch(vlan)#show vlan 23

VLAN Command Summary

```

switch<vlan># ?
exit                Exit the vlan database command mode
no                  Disable the vlan setting
show                show vlan database information
vlan                Configure a vlan
vlanmode            Change vlan mode
switch<vlan># vlan ?
802.1q              Configure IEEE802.1q vlan
port-based          Configure Port-Based vlan
switch<vlan># vlan 802.1q ?
aggregator          Specify aggregator ID
mnt-vid             Configure Management VID (0 is disabled)
name                Change the group name by VID
port                Specify the port number
switch<vlan># vlan port-based ?
grpname            Assign Group name

```

6.6 Spanning Tree Commands

Commands	Level	Description	Example
spanning-tree enable	G	Enable spanning tree	switch(config)#spanning-tree enable
spanning-tree priority [0to61440]	G	Configure spanning tree priority parameter	switch(config)#spanning-tree priority 32767
spanning-tree max-age [seconds]	G	Use the spanning-tree max-age global configuration command to change the interval between messages the spanning tree receives from the root switch. If a switch does not receive a bridge protocol data unit (BPDU) message from the root switch within this interval, it recomputed the Spanning Tree Protocol (STP) topology.	switch(config)# spanning-tree max-age 15
spanning-tree hello-time [seconds]	G	Use the spanning-tree hello-time global configuration command to specify the interval between hello bridge protocol data units (BPDUs).	switch(config)#spanning-tree hello-time 3
spanning-tree forward-time [seconds]	G	Use the spanning-tree forward-time global configuration command to set the forwarding-time for the specified spanning-tree instances. The forwarding time	switch(config)# spanning-tree forward-time 20

		determines how long each of the listening and learning states last before the port begins forwarding.	
stp-path-cost [1to200000000]	I	Use the spanning-tree cost interface configuration 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)#interface fastEthernet 2 switch(config-if)#stp-path-cost 20
stp-path-priority [Port Priority]	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)#interface fastEthernet 2 switch(config-if)# stp-path-priority 127
stp-admin-p2p [Auto True False]	I	Admin P2P of STP priority on this interface.	switch(config)#interface fastEthernet 2 switch(config-if)# stp-admin-p2p Auto
stp-admin-edge [True False]	I	Admin Edge of STP priority on this interface.	switch(config)#interface fastEthernet 2 switch(config-if)# stp-admin-edge True
stp-admin-non-stp [True False]	I	Admin NonSTP of STP priority on this interface.	switch(config)#interface fastEthernet 2 switch(config-if)# stp-admin-non-stp False
Show spanning-tree	E	Display a summary of the spanning-tree states.	switch>show spanning-tree
no spanning-tree	G	Disable spanning-tree.	switch(config)#no spanning-tree

6.7 QoS Commands

Commands	Level	Description	Example
qos policy [weighted-fair strict]	G	Select QoS policy scheduling	switch(config)#qos policy weighted-fair
qos prioritytype [port-based cos-only tos-only cos-first tos-first]	G	Setting of QoS priority type	switch(config)#qos prioritytype
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 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

Commands	Level	Description	Example
igmp enable	G	Enable IGMP snooping function	switch(config)#igmp enable
igmp-query auto	G	Set IGMP query to auto mode	switch(config)#igmp-query auto
igmp-query force	G	Set IGMP query to force mode	switch(config)#igmp-query force
show igmp configuration	P	Displays the details of an IGMP configuration.	switch#show igmp configuration
show igmp multi	P	Displays the details of an IGMP snooping entries.	switch#show igmp multi
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

Commands	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
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 an entry of MAC address table (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

Commands	Level	Description	Example
snmp agent-mode [v1v2c v3]	G	Select the agent mode of SNMP	switch(config)#snmp agent-mode v1v2c
snmp-server host [IP address] community [Community-string] trap-version	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)#

[v1 v2c]			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 Port Mirroring Commands

Commands	Level	Description	Example
monitor rx	G	Set RX destination port of monitor function	switch(config)#monitor rx
monitor tx	G	Set TX destination port of monitor function	switch(config)#monitor tx
show monitor	P	Show port monitor information	switch#show monitor
monitor	I	Configure source port of	switch(config)#interface fastEthernet 2

[RX TX Both]		monitor function	switch(config-if)#monitor RX
show monitor	I	Show port monitor information	switch(config)#interface fastEthernet 2 switch(config-if)#show monitor
no monitor	I	Disable source port of monitor function	switch(config)#interface fastEthernet 2 switch(config-if)#no monitor

6.12 802.1x Commands

Commands	Level	Description	Example
8021x enable	G	Use the 802.1x global configuration command to enable 802.1x protocols.	switch(config)# 8021x enable
8021x system radiousip [IP address]	G	Use the 802.1x system radius IP global configuration command to change the radius server IP.	switch(config)# 8021x system radiousip 192.168.1.1
8021x system serverport [port ID]	G	Use the 802.1x system server port global configuration 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 configuration command to change the accounting port	switch(config)# 8021x system accountport 1816
8021x system sharekey [ID]	G	Use the 802.1x system share key global configuration command to change the shared key value.	switch(config)# 8021x system sharekey 123456
8021x system nasid [words]	G	Use the 802.1x system nasid global configuration command to change the	switch(config)# 8021x system nasid test1

		NAS ID	
8021x misc quietperiod [sec.]	G	Use the 802.1x misc quiet period global configuration 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 configuration 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 configuration 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 configuration command to set the server timeout.	switch(config)#8021x misc servertimeout 20
8021x misc maxrequest [number]	G	Use the 802.1x misc max request global configuration command to set the MAX requests.	switch(config)# 8021x misc maxrequest 3
8021x misc reauthperiod [sec.]	G	Use the 802.1x misc reauth period global configuration 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 configuration 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

6.13 TFTP Commands

Commands	Level	Description	Defaults Example
backup flash:backup_cfg	G	Save configuration to TFTP and need to specify the IP of TFTP server and the file name of image.	switch(config)#backup flash:backup_cfg
restore flash:restore_cfg	G	Get configuration from TFTP server and need to specify the IP of TFTP server and the file name of image.	switch(config)#restore flash:restore_cfg
upgrade flash:upgrade_fw	G	Upgrade firmware by TFTP and need to specify the IP of TFTP server and the file name of image.	switch(config)#upgrade lash:upgrade_fw

6.14 SYSLOG, SMTP, and EVENT Commands

Commands	Level	Description	Example
systemlog ip [IP address]	G	Set System log server IP address.	switch(config)# systemlog ip 192.168.1.100
systemlog mode [client server both]	G	Specified the log mode	switch(config)# systemlog mode both
show systemlog	E	Display system log.	Switch>show systemlog
show systemlog	P	Show system log client & server information	switch#show systemlog
no systemlog	G	Disable systemlog functon	switch(config)#no systemlog
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 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-cold-start [Systemlog SMTP Both]	G	Set cold start event type	switch(config)#event device-cold-start both
event authentication-failure [Systemlog SMTP Both]	G	Set Authentication failure event type	switch(config)#event authentication-failure both
event Redundant Ring-topology-change [Systemlog SMTP Both]	G	Set s ring topology changed event type	switch(config)#event ring-topology-change both
event systemlog [Link-UP Link-Down Both]	I	Set port event for system log	switch(config)#interface fastethernet 3 switch(config-if)#event systemlog both
event smtp [Link-UP Link-Down Both]	I	Set port event for SMTP	switch(config)#interface fastethernet 3 switch(config-if)#event smtp both
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 Redundant Ring-topology-change	G	Disable Redundant Ring topology changed event type	switch(config)#no event ring-topology-change
no event systemlog	I	Disable port event for system log	switch(config)#interface fastethernet 3 switch(config-if)#no event systemlog
no event smpt	I	Disable port event for	switch(config)#interface fastethernet 3

		SMTP	switch(config-if)#no event smtp
show systemlog	P	Show system log client & server information	switch#show systemlog

```

switch<config> # mstp ?
config-name      Configure MSTP bridge configuration name parameter
enable          Enable MSTP
force-version    Configure MSTP bridge force version parameter
forward-time     Configure MSTP forward time parameter
hello-time       Configure MSTP hello time parameter
instance         Configure MSTP instance
max-age          Configure MSTP max age parameter
max-hops         Configure MSTP max hops parameter
priority         Configure MSTP bridge priority parameter
revision-level   Configure MSTP bridge revision level parameter

```

Messages: mstp is inactive

6.15 SNTP Commands

Commands	Level	Description	Example
sntp enable	G	Enable SNTP function	switch(config)#sntp enable
sntp daylight	G	Enable daylight saving time, if SNTP function is inactive, this command can't be applied.	switch(config)#sntp daylight
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
sntp ip [IP]	G	Set SNTP server IP, if SNTP function is inactive, this command can't be applied.	switch(config)#sntp ip 192.169.1.1
sntp timezone [Timezone]	G	Set timezone index, use "show sntp timzezone" command to get more information of index number	switch(config)#sntp timezone 22
show sntp	P	Show SNTP information	switch#show sntp
show sntp timezone	P	Show 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

6.16 Redundant Ring Commands

Commands	Level	Description	Example
Ring enable	G	Enable Redundant Ring	switch(config)# ring enable
Ring master	G	Enable ring master	switch(config)# ring master
Ring couplering	G	Enable couple ring	switch(config)# ring couplering
Ring dualhoming	G	Enable dual homing	switch(config)# ring dualhoming
Ring ringport [1st Ring Port] [2nd Ring Port]	G	Configure 1st/2nd Ring Port	switch(config)# ring ringport 7 8
Ring couplingport [Coupling Port]	G	Configure Coupling Port	switch(config)# ring couplingport 1
Ring controlport [Control Port]	G	Configure Control Port	switch(config)# ring controlport 2
Ring homingport [Dual Homing Port]	G	Configure Dual Homing Port	switch(config)# ring homingport 3
show Ring	P	Show the information of Redundant Ring	switch#show ring
no Ring	G	Disable Redundant Ring	switch(config)#no ring
no Ring master	G	Disable ring master	switch(config)# no ring master
no Ring couplering	G	Disable couple ring	switch(config)# no ring couplering
no Ring dualhoming	G	Disable dual homing	switch(config)# no ring dualhoming

Ring Commands Summary

```
switch<config> # ring ?
coupling-port    Configure coupling port
coupling-ring    Enable Coupling Ring
dual-homing      Enable dual homing
enable           Enable Redundant Ring
homing port      Configure dual homing port
master           Enable ring master
port             Configure 1st/2nd ring ports
```

Open Ring Commands Summary

```
switch<config> # open-ring ?
enable          Enable Open-Ring
port           Configure 1st/2nd ring ports
vendor         Configure vendor of Open-Ring [Moxx|Advantexx|Hirshmaxx]
```

6.17 CLI COMMAND SUMMARY

```
switch>?
enable          Enter Privileged EXEC mode
logout         Logout command line shell
ping          Ping function
quit          Logout command line shell
show          Show function
switch>
switch>enable
switch#
configure      Enter Global configuration mode
disable        Leave Privileged EXEC mode
show          Show function
vlan          Enter the vlan database command
write         Write current device configuration to memory
switch#
switch#configure
switch(config)#?
admin          Configure administrator
aggregator     Configure aggregator port setting
auto-sfp       Enable/disable to auto detect 100/1000 SFP
check-concurrence Check redundancy protocol concurrence
default        Restore to factory default configuration
dhcpserver     Configure DHCP server
end            Leave Global configuration mode
event          Configure system event selection
exit           Leave Global configuration mode
fault-relay    Configure Fault Relay Alarm function
igmp           IGMP function setting
interface      Enter the interface command (with a specific interface)
```


ip	Configure IP address
lldp	LLDP function setting
mac-address-table	Configure MAC address entry
mstp	Configure MSTP
multicast-filtering	Configure multicast filtering entry
multiple-ring	Configure Multiple Ring
no	Disable setting
open-ring	Configure Open-Ring
qos	Configure QOS function
reload	Reboot switch
ring	Configure Redundant Ring
rstp	Configure RSTP
security	Configure IP security
sfp-monitor	Configure SFP temperature alarm
smtp	Configure SMTP function
snmp	SNMP function
sntp	Set SNTP function
syslog	Configure SYSLOG function
system	Configure system detail information
tftp	Transfer file by TFTP
switch(config)#	

7. Technical Specifications

Note: The SISTM1040-173D-LRT is intended for indoor use.

Physical Ports	
10/100 Base-T(X) Port in RJ45 Auto MDI/MDIX	7
Gigabit combo Ports with 10/100/1000Base-T(X) and 100/1000Base-X SFP Port	3
Technology	
Ethernet Standards	IEEE 802.3 for 10Base-T IEEE 802.3u for 100Base-TX and 100Base-FX IEEE 802.3z for 1000Base-X IEEE 802.3ab for 1000Base-T IEEE 802.3x for Flow control IEEE 802.3ad for LACP (Link Aggregation Control Protocol) IEEE 802.1D for STP (Spanning Tree Protocol) IEEE 802.1p for COS (Class of Service) IEEE 802.1Q for VLAN Tagging IEEE 802.1w for RSTP (Rapid Spanning Tree Protocol) IEEE 802.1s for MSTP (Multiple Spanning Tree Protocol) IEEE 802.1x for Authentication IEEE 802.1AB for LLDP (Link Layer Discovery Protocol)
MAC Table	8192 MAC addresses
Priority Queues	4
Processing	Store-and-Forward
Switch Properties	Switching latency: 7 us Switching bandwidth: 7.4Gbps Max. Number of Available VLANs: 4096 IGMP multicast groups: 1024 Port rate limiting: User Defined
Security Features	Enable/disable ports, MAC based port security Port based network access control (802.1x) VLAN (802.1Q) to segregate and secure network traffic Supports Q-in-Q VLAN for performance & security to expand the VLAN space Radius centralized password management SNMP v1/v2c/v3 encrypted authentication and access security
Software Features	STP/RSTP/MSTP (IEEE 802.1D/w/s) Redundant Ring with recovery time less than 10ms over 250 units TOS/Diffserv supported Quality of Service (802.1p) for real-time traffic VLAN (802.1Q) with VLAN tagging and GVRP supported IGMP Snooping for multicast filtering Port configuration, status, statistics, monitoring, security

	SNTP for synchronizing of clocks over network Support PTP Client (Precision Time Protocol) clock synchronization DHCP Server / Client support Port Trunk support MVR (Multicast VLAN Registration) support
Network Redundancy	Redundant Ring + Multi-Ring; RSTP, STP, and MSTP
Warning / Monitoring System	Relay output for fault event alarming Syslog server / client to record and view events Include SMTP for event warning notification via email Event selection support
RS-232 Serial Console Port	RS-232 in RJ45 connector with console cable. 9600bps, 8, N, 1
LED Indicators	
Power LED	Green : Power LED x 3
R.M. LED	Green : Indicate system operated in Redundant Ring master mode
Fault LED	Amber : Indicate unexpected event occurred
10/100Base-T(X) RJ45 Port	Green for port Link/Act. Amber for Duplex/Collision
10/100/1000Base-T(X) RJ45 Port LED	Green for port Link/Act. Amber for 100Mbps indicator
100/1000Base-X SFP Port	Green for port Link/Act.
Fault contact	
Relay	Relay output to carry capacity of 1A at 24VDC
Power	
Redundant Input Power	Dual DC inputs. 12 ~ 48VDC on 6-pin terminal block. Note: need to use UL Approved power adapter (12-48Vdc, 1-0.25A, Amb. 70°C)
Power Consumption (Typ.)	12 Watts
Overload Current Protection	Present
Reverse Polarity Protection	Present on terminal block
Physical Characteristic	
Enclosure	IP-30
Dimension (W x D x H)	74.3(W)x109.2(D)x153.6(H) mm (2.93 x 4.3 x 6.05 inch)
Weight (g)	1045 g
Environmental	
Storage Temperature	-40 to 85°C (-40 to 185°F)
Operating Temperature	-40 to 70°C (-40 to 158°F)
Operating Humidity	5% to 95% Non-condensing
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
Shock	IEC60068-2-27
Free Fall	IEC60068-2-32
Vibration	IEC60068-2-6
Safety	EN60950-1

Warranty	Limited Lifetime Warranty
MTBF	670898.5679 hrs. at 25C; Env.: GFC; Category: Telcordia SR-332 Issue 2

8. Troubleshooting

If the SISTM1040-173D-LRT fails, isolate and correct the fault by determining the answers to the following questions and then taking the indicated action. First isolate the problem to the SISTM1040-173D-LRT; by troubleshoot any other network gear (e.g., other switches, remote devices like cameras, midspan injectors if used, etc.) to isolate the problem to the SISTM1040-173D-LRT.

- Make sure that the function you are trying to use is supported; see [About the SISTM1040-173D-LRT](#) on page 7.
- Verify the install procedures were performed correctly. See section [2. Hardware Installation](#) on page 8.
- Verify that you are using the right power cord/adaptor. Using a power adapter with DC voltage output higher than the rated voltage of the switch will damage the switch.
Check connections between the switch, the power cord and the wall outlet. See section [11. Power Supply Information](#) on page 136.
- Check that the proper cable type is used and its length does not exceed specified limits. See section [4. Cables](#) on page 14.
- Check for improper Network Topologies. Make sure that your network topology contains no data path loops.
- If the power LED does not light up when the power cord is plugged in, you may have a problem with power cord. Then check for loose power connections, power losses or surges at power outlet.
- Diagnosing LED Indicators: The Ethernet switch can be monitored via LEDs on the front panel to help identify problems. See section [Front Panel LEDs](#) on page 11.
- If the LED indicators are normal with network cables connected properly but packet delivery still fails, check the status of Ethernet device configurations or status on the network. See section [5. Web Management](#) on page 17 or section [6. Command Line Interface](#) on page 85.
- 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.
- If you still cannot resolve the problem, see section [9. Service, Warranty & Tech Support](#) on page 130 below.

9. Service, Warranty & Tech Support

9.1 Record Model and System Information

After performing the troubleshooting procedures above, and before calling or emailing Tech Support, record as much information as possible in order to help the Tech Support Specialist.

1. Record Model Information: Model name: _____

SN: _____

LED Status: _____

3. Provide additional information to your Technical Support Specialist.

Your Transition Networks service contract number: _____

Describe the failure: _____

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

The model # and serial # of all other Transition Networks products in the network:

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

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

Any previous Return Material Authorization (RMA) numbers: _____

List TN or third party equipment in the network (e.g., PCs, servers, switches, routers, or hubs, Remote devices (camera, etc.), Midspan Injectors, etc.): _____



9.2 Service

Direct Contact Numbers:

Domestic: + 1 800-260-1312

International: + 1 952-358-3601

Fax +1 952-941-2322

Email: techsupport@transition.com

Service Hours:

USA: 7 AM until 8 PM CST Monday to Friday.

Out of Hours the calls will be answered by an on-call engineer.

Live Help Online Support: Chat live with a Transition Networks representative at

<http://transition.com/TransitionNetworks/TechSupport/ContactUs.aspx>.

9.3 Warranty

This warranty is your only remedy. No other warranties, such as fitness for a particular purpose, are expressed or implied. Transition Networks is not liable for any special, indirect, incidental or consequential damages or losses, including loss of data, arising from any cause or theory. Authorized resellers are not authorized to extend any different warranty on transition networks' behalf.

Limited Lifetime Warranty

Effective for Products Shipped May 1, 1999 and After. Every Transition Networks labeled product purchased after May 1, 1999, and not covered by a fixed-duration warranty will be free from defects in material and workmanship for its lifetime. This warranty covers the original user only and is not transferable. This warranty does not cover damage from accident, acts of God, neglect, contamination, misuse or abnormal conditions of operation or handling, including over-voltage failures caused by use outside of the product's specified rating, or normal wear and tear of mechanical components. If the user is unsure about the proper means of installing or using the equipment, contact Transition Networks's free technical support services.

Transition Networks will, at its option:

- Repair the defective product to functional specification at no charge
- Replace the product with an equivalent functional product
- Refund a portion of purchase price based on a depreciated value

Return Authorization

To return a defective product for warranty coverage, contact Transition Networks's technical support department for a return authorization number. Transition's technical support department can be reached through any of the following means:

Service Hours

USA: 8:00 PM Sunday through 8:00 PM Friday CST

After Hours: Calls will be answered by an on call engineer.

Direct Contact Numbers

Domestic: + 1 800-260-1312

International: + 1 952-358-3601

Fax: +1 952-941-2322

Email: techsupport@transition.com Online Support

Live Help: [Chat live](#) with a Transition Networks representative.

Return Instructions

Send the defective product postage and insurance prepaid to the following address:

Transition Networks, Inc.

10900 Red Circle Drive

Minnetonka, MN 55343 USA

Attn: RETURNS DEPT: CRA/RMA # _____

Failure to properly protect the product during shipping may void this warranty. The return authorization number must be written on the outside of the carton to ensure its acceptance. We cannot accept delivery of any equipment that is sent to us without a CRA or RMA number.

CRA's are valid for 60 days from the date of issuance. An invoice will be generated for payment on any unit(s) not returned within 60 days.

Upon completion of a demo/ evaluation test period, units must be returned or purchased within 30 days. An invoice will be generated for payment on any unit(s) not returned within 30 days after the demo/ evaluation period has expired.

The customer must pay for the non-compliant product(s) return transportation costs to Transition Networks for evaluation of said product(s) for repair or replacement. Transition Networks will pay for the shipping of the repaired or replaced in-warranty product(s) back to the customer (any and all customs charges, tariffs, or/and taxes are the customer's responsibility).

Before making any non-warranty repair, Transition Networks requires a \$200.00 charge plus actual shipping costs to and from the customer. If the repair is greater than \$200.00, an estimate is issued to the customer for authorization of repair. If no authorization is obtained, or the product is deemed 'not repairable', Transition Networks will retain the \$200.00 service charge and return the product to the customer not repaired. Non-warranted products that are repaired by Transition Networks for a fee will carry a 180-day limited warranty. All warranty claims are subject to the restrictions and conventions set forth by this document.

Transition Networks reserves the right to charge for all testing and shipping incurred, if after testing, a return is classified as "No Problem Found."

THIS WARRANTY IS YOUR ONLY REMEDY. NO OTHER WARRANTIES, SUCH AS FITNESS FOR A PARTICULAR PURPOSE, ARE EXPRESSED OR IMPLIED. TRANSITION NETWORKS IS NOT LIABLE FOR ANY SPECIAL, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES OR LOSSES, INCLUDING LOSS OF DATA, ARISING FROM ANY CAUSE OR THEORY. AUTHORIZED RESELLERS ARE NOT AUTHORIZED TO EXTEND ANY DIFFERENT WARRANTY ON TRANSITION NETWORKS'S BEHALF.

10. Regulatory Agency Information

Compliant with 802.3at in Environment A when using an isolated power supply. For 802.3at Environment B applications: 1) use an isolated AC/DC power source, e.g. TN 25080, and/or 2) use mid-span injector (s), e.g. MIL-L100i, L1000i-at, between this switch's PSE port and link partner PD port.

10.1 Regulatory Approvals

Safety: EN 60950-1, CISPR/EN55022 Class A,
 FCC Part 15 Class A, EN61000-4-2, EN61000-4-3,
 EN61000-4-4, EN61000-4-5, EN61000-4-6,
 EN61000-4-8, EN61000-4-11,
 IEC60068-2-32 (Free fall), IEC60068-2-27 (Shock),
 IEC60068-2-6 (Vibration)

10.2 Declaration of Conformity

EU Declaration of Conformity

SISTM1040-173D-LRT
Model/Part Number

Transition Networks, Inc.
10900 Red Circle Drive, Minnetonka, Minnesota 55343 U.S.A.
Manufacturer's Name and Address

This declaration of conformity is issued under the sole responsibility of the manufacturer.



SISTM1040-173D-LRT
Hardened Managed Ethernet Switch

are in conformity with the relevant Union harmonisation legislation:

Electromagnetic Compatibility (EMC) Directive 2014/30/EU: EN 55022:2010, EN 55024:2010

Low-Voltage Directive (LVD) 2014/35/EU: EN 60950-1:2006

And hereby is declared compliant and carries the CE marking

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

Minnetonka, Minnesota
Place

2-10-16
Date


Signature

Stephen Anderson
Full Name

Vice President of Engineering
Position

11. Power Supply Information

Several power supply models are available from Transition Networks. **Warning:** You must use an isolated power supply in order for Transition Networks to honor the warranty.

The power supplies Transition Networks makes available are optional accessories (sold separately):

- 25130; 39.4 Watt 48VDC DIN-Rail Industrial Power Supply
- 25083; 10.8~13.2 VDC, 24 Watts Industrial Power Supply

See the *SISTM1040-173D-LRT Quick Start Guide* for Power Requirements, Isolation, Redundant Power Inputs, Power Connection, and Chassis Ground information. To access the manuals, firmware, datasheet or other documentation for your product, enter your model number: SISTM1040-173D-LRT in the “Search” box at our website at www.transition.com.

11.1 Industrial Power Supply 25130

Universal AC input/Full range

Protection: Short circuit / Overload / Over voltage

Class I, Div 2 Hazardous Locations T4

LED indicator for Power On

DC OK relay contact

No load power consumption <0.75W

Overload Protection: 105 ~ 150% rated output power.

Protection type: Constant current limiting, recovers automatically after fault condition is removed.

Over Voltage Protection:

57.6 ~ 64.8V. Protection type: Shut down o/p voltage, re-power on to recover.

Safety Standards: UL508, UL60950-1, TUV EN60950-1, Class I, Div. 2 Group A, B, C, D Hazardous Locations T4 approved.

EMC Emissions: Compliance to EN55011, EN55022 (CISPR22), EN61204-3 Class B, EN61000-3-2,-3.

EMC Immunity: Compliance to EN61000-4-2, 3, 4, 5, 6, 8, 11, EN55024, EN61000-6-2, EN61204-3, heavy industry level, criteria A.

MTBF: 301.7K hrs min. MIL-HDBK-217F (25°C).

Dimensions: 40*90*100mm (W*H*D)



11.2 Industrial Power Supply 25083

TN274 is a 12VDC@2A, Univ AC, Industrial, Din Rail Power Supply.

Max. output: 30 W

Output type: Single

Output description: 12V, 0-2.0A

Power supply type: AC/DC power supply

Enclosure type: DIN rail

Protection: Overload, Over Voltage

RoHS Compliant

Net weight (gr): 278

Output Voltage: 12 V

Output Current: 0 - 2 A

Dimensions: 79 x 93 x 56 mm (W x H x D)

Caution: Indoor use only. For use in a protected environment. Risk of shock. Do not open.





Transition Networks

10900 Red Circle Drive

Minnetonka, MN 55343 USA

Tel: 952-941-7600 or 1-800-526-9267

Fax: 952-941-2322

Copyright © 2016 Transition Networks. All rights reserved.

Printed in the U.S.A.

SISTM1040-173D-LRT Hardened Managed Ethernet Switch User Guide, 33678 Rev. A