SISPM1040-382-LRT

Industrial 10-port Managed PoE Ethernet Switch

User Guide

33576 Rev. D

Trademarks

Copyright Notice/Restrictions

Contact Information

Transition Networks
10900 Red Circle Drive
Minnetonka, MN 55343 USA
tel: +1.952.941.7600 | toll free: 1.800.526.9267 | fax: 952.941.2322
sales@transition.com | techsupport@transition.com | customerservice@transition.com

SISPM1040-382-LRT Industrial 10-port Managed PoE Ethernet Switch User Guide 33576 Rev. D

Revision History

Rev	Date	Description
A	10/22/13	Manual released at Rev. A.
B	10/20/14	Added information on SSL.
C	6/10/15	Added sections 8 and 9 and Appendix A.
D	1/19/17	Update specs and add isolation information for firmware version 1.27. Update for firmware version 1.33 and add power supply info.

Table of Contents

1. Introduction

The SISPM1040-382-LRT is a managed PoE switch suitable for connecting and powering devices in challenging environments. The two gigabit speed combo ports provide the ultimate flexibility by allowing copper or fiber SFP uplink ports. The two uplink ports can also be used in a redundant ring for maximum network reliability. The switch has a PoE power budget of 240 Watts, provides up to 30 Watts per port on all ports simultaneously, has redundant input power connections, and a fault alarm relay to ensure safe reliable operation in temperatures between -40°C and +75°C (without SFPs). Transition Networks' industrial switches are certified to operate reliably in harsh environments such as those found on factory floors, outdoor enclosures or other challenging environments.

1.1 Description

The SISPM1040-382-LRT is a powerful managed industrial switch with many features.
The switch can operate in wide temperatures, dusty environments and humid conditions. SISPM1040-382-LRT supports Power over Ethernet, a system to transmit electrical power with data to remote devices over standard twisted-pair cable. The SISPM1040-382-LRT has eight 10/100Base-T(X) PoE+ ports. The SISPM1040-382-LRT can be managed via the Web, Telnet, Console or other third-party SNMP software.

1.2 Features

- Store-and-Forward Architecture with 5.6 Gbps Switching Bandwidth
- Dual, Redundant 50 to 57 VDC Power Inputs with Current Overload Protection
- 6 PIN Terminal Block input power connections
- Fault Output Relay rated 1A@24VDC
- Eight PSE ports, providing up to 30 Watts per port
- PoE Ping Alive Check (Auto power Reset - APR)
- DIN Rail and Wall Mount Brackets included
- Extended operating temperature (-40°C to 75°C)
- Redundant Ring with recovery time less than 10ms over 250 units
- STP/RSTP/MSTP (IEEE 802.1D/w/s)
- TOS/DSCP
- QoS Quality of Service (802.1p)
- VLAN with VLAN Tagging and GVRP (802-1Q)
- MVR (Multicast VLAN Registration) support
- IGMP v2/v3 (IGMP Snooping)
- IP-based bandwidth management

- Port configuration, status, statistics, monitoring, and security
- SNTP for synchronizing of clocks over the network
- PTP (Precision Time Protocol) Client clock synchronization
- System Alarms via SYSLOG / SNMP / Trap / Fault Output Relay
- LLDP protocol
- DHCP Client/Server
- Port based network access control (802.1x)
- SSH Security
- RADUIS centralized password management
- SNMPv3 encrypted authentication and access security
- Web / SNMP v1, v2c, v3 / Telnet / CLI SSL/HTTPS device management

1.3 Install Cautions and Warnings

Warning: Risk of Electrical Shock. Disconnect power before installing the SISPM1040-382-LRT. Failure to observe this warning could result in an electrical shock.

CAUTION Only qualified persons should install the SISPM1040-382-LRT. Failure to observe this caution could result in poor performance or damage to the equipment.

CAUTION Install the SISPM1040-382-LRT in an operating environment where the temperature range is from *-40°C to +75°C (-104°F to +167 °F)*, with relative humidity of 5% to 90% non-condensing. Failure to observe this caution could result in poor equipment performance.

CAUTION DO NOT install the SISPM1040-382-LRT in areas where strong electromagnetic fields (EMF) exist. Failure to observe this caution could result in poor equipment performance and data corruption.

WARNING Disconnect power before installing and wiring the SISPM1040-382-LRT for power. Failure to observe this warning could result in an electrical shock.

Attention: this product, like all electronic products, uses semiconductors that can be damaged by ESD (electrostatic discarge). Always observe appropriate precautions when handling.

1.4 Electrical Safety Warnings

Electrical Safety

IMPORTANT: This equipment must be installed in accordance with safety precautions.

Elektrische Sicherheit

WICHTIG: Für die Installation dieses Gerätes ist die Einhaltung von Sicherheitsvorkehrungen erforderlich.

Elektrisk sikkerhed

VIGTIGT: Dette udstyr skal 13nstallers I overensstemmelse med sikkerhedsadvarslerne.

Elektrische veiligheid

BELANGRIJK: Dit apparaat moet in overeenstemming met de veiligheidsvoorschriften worden geïnstalleerd.

Sécurité électrique

IMPORTANT : Cet équipement doit être utilisé conformément aux instructions de sécurité.

Sähköturvallisuus

TÄRKEÄÄ : Tämä laite on asennettava turvaohjeiden mukaisesti.

Sicurezza elettrica

IMPORTANTE: questa apparecchiatura deve essere installata rispettando le norme di sicurezza.

Elektrisk sikkerhet

VIKTIG: Dette utstyret skal 13nstallers I samsvar med sikkerhetsregler.

Segurança eléctrica

IMPORTANTE: Este equipamento tem que ser instalado segundo as medidas de precaução de segurança.

Seguridad eléctrica

IMPORTANTE: La instalación de este equipo deberá llevarse a cabo cumpliendo con las precauciones de seguridad.

Elsäkerhet

OBS! Alla nödvändiga försiktighetsåtgärder måste vidtas när denna utrustning används.

2. Hardware Installation

2.0 Package Contents

Contact your sales representative if you have not received these items:

□ One SISPM1040-382-LRT Switch

□ One printed Quick Start Guide

□ One DIN Rail Mount Kit

□ One Console cable

□ Five M3 Flat Screws

□ One Wall Mount Kit.

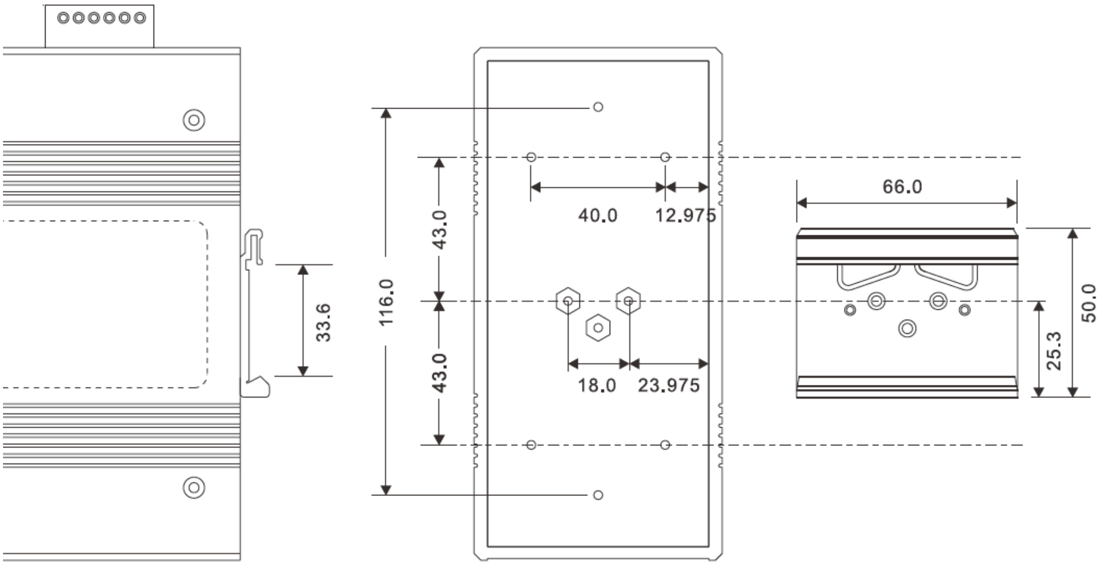
□ One 6-pin Terminal Block

Please save the packaging for possible future use.

2.1 Installing Switch on DIN-Rail

Each switch has a DIN-Rail kit that can be mounted on the rear panel. The DIN-Rail kit provides for easy installation on the DIN-Rail.

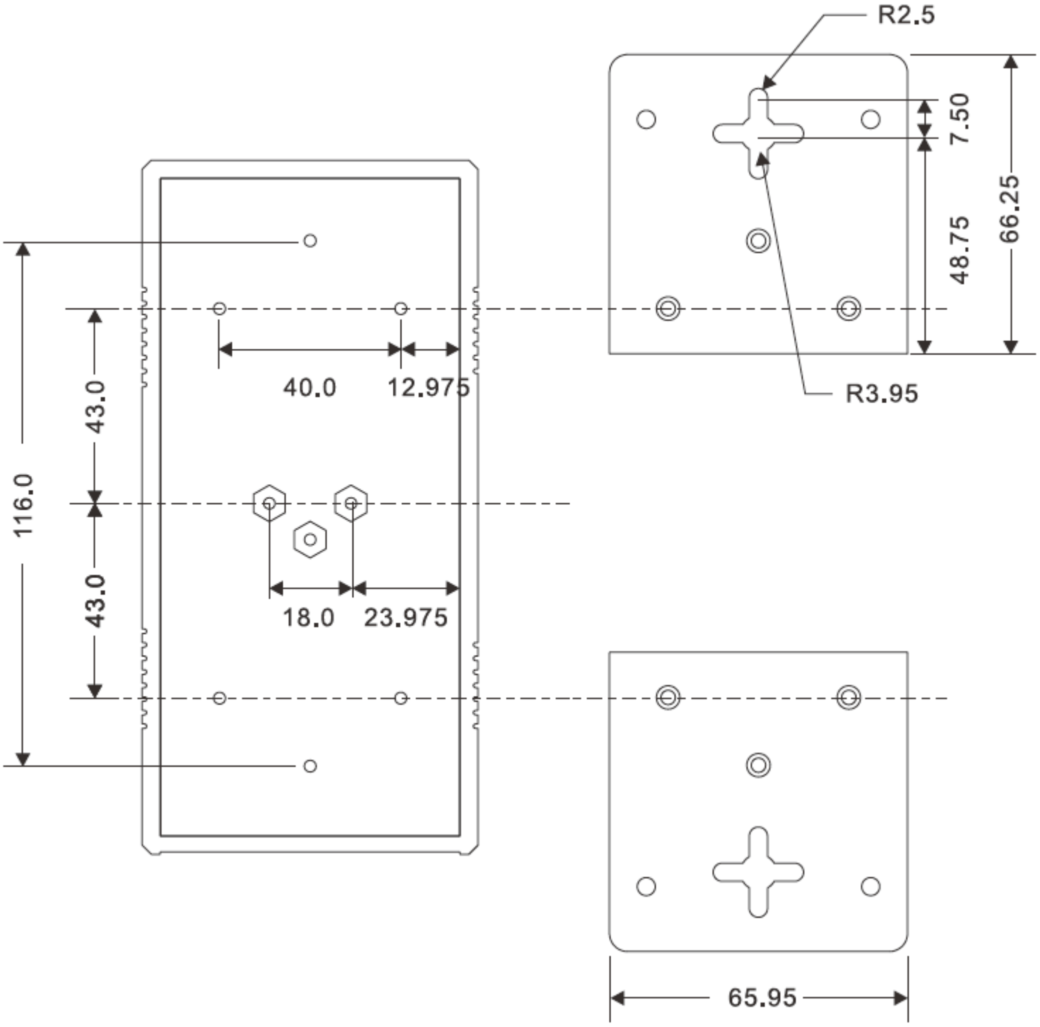
2.1.1 Mount the DIN-Rail Clip



DIN-Rail Size

2.2 Wall Mounting Installation

A wall mount bracket can be used to mount the switch on a panel or wall. The bracket is mounted to the switch using the enclosed screws.



Wall-Mounting size

Product Alert Notification

We have been advised by the manufacturer of the Power Over Ethernet Controller chip used in the SISPM1040-382-LRT that direct copper network connections between legacy detect PoE enabled ports is not recommended.

If your network configuration requires a copper connection between two SISPM1040-382-LRT switches, it is necessary to disable PoE on both of the connected ports. It is also recommended that if your network configuration requires a copper port on the SISPM1040-382-LRT to be connected to any other PSE (Power Sourcing Equipment) device, that PoE is disabled on the SISPM1040-382-LRT port.

Based on the notice from our supplier, connections of this type may result in damage to the connected equipment and, in some cases, other PoE equipment connected to different PoE ports on the same SISPM1040-382-LRT.

Related Information

See the SISPM1040-382-LRT Quick Start Guide (33721) for summary installation information.

For Transition Networks Drivers, Firmware, Manual, etc. go to the Product Support webpage (logon required). For Transition Networks Application Notes, Brochures, Data Sheets, Specifications, etc. go to the Support Library (no registration required).
Note that this manual provides links to third party web sites for which Transition Networks is not responsible.

3. Hardware Overview

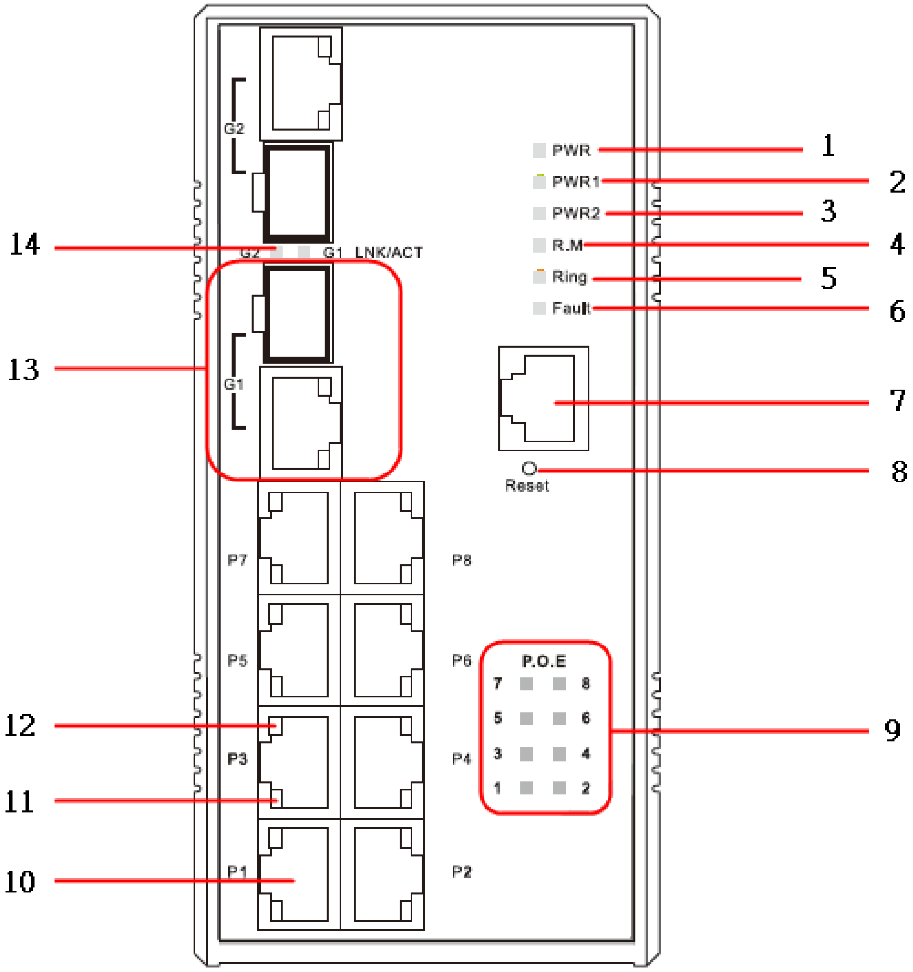
The SISPM1040-382-LRT front panel, LEDs, and top panel are described below.

3.1 Front Panel

The following table describes the SISPM1040-382-LRT front panel.

Port	Description
10/100 RJ-45 fast Ethernet ports	8 10/100Base-T(X) RJ-45 fast Ethernet ports support auto-negotiation. The default settings are: Speed: auto Duplex: auto Flow control: disable
Gigabit RJ-45 ports	2 10/100/1000Base-T(X) Gigabit ports (combo ports)
SFP ports	2 100/1000Base-X on SFP port (combo)
PoE Ports	Ports 1-8 support the PoE+ function. Compliant with IEEE802.3at PoE+ specifications. 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 25104, 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. PoE must not be enabled if two 382-LRT copper ports are connected.
Console	Use RS-232 to RJ-45 connecter to manage the switch.
Reset	Push the Reset button for 2 to 3 seconds to reset the switch. Push the Reset button for 5 seconds to reset the switch to its Factory Default settings**.** The front panel LEDs light momentarily. You may have to refresh your browser to display the System Information page.

The SISPM1040-382-LRT front panel components are shown and described below.



1. LED for PWR. When the PWR links, the green LED will light.
2. LED for PWR1. When the PWR1 links, the green LED will light.
3. LED for PWR2. When the PWR2 links, the green LED will light.
4. LED for R.M (Ring master). This LED lights if the switch is the Ring Master.
5. LED for Ring. This LED lights when the Ring is activated.
6. LED for Fault Relay. When a fault occurs, the amber LED will light.
7. Console port (RJ-45).
8. Reset button. Push the button for 2-3 seconds for reset; push for 5 seconds for factory defaults.
9. LED for PoE power supplied.
10. 10/100Base-T(X) PSE Ethernet ports.
11. LED for Ethernet port speed.
12. LED for Ethernet port link status.
13. 1000 COMBO ports with SFP.
14. LED for SFP ports Link/Act status.

3.2 Front Panel LEDs

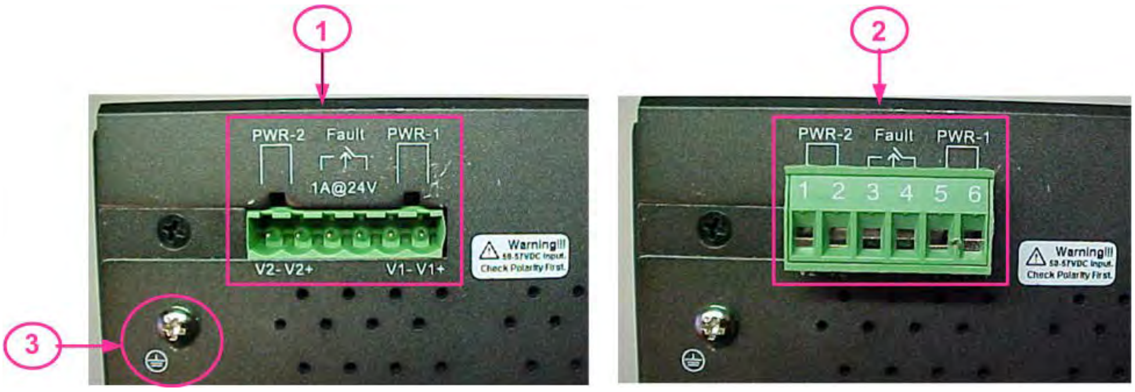
The SISPM1040-382-LRT front panel LEDs are described below.

LED	Color	Status	Description
PWR	Green	On	DC power ready.
PW1	Green	On	DC power module 1 activated.
PW2	Green	On	DC power module 2 activated.
R.M	Green	On	Ring Master.
Ring	Green	On	Ring enabled.
		Slowly blinking	Ring topology has problem.
		Fast blinking	Ring working normally.
Fault	Amber	On	Fault relay. Power failure or Port down/fail.
10/100Base-T(X) Fast Ethernet ports			
LNK / ACT	Green	On	Port link up.
		Blinking	Data transmitted.
Full Duplex	Amber	On	Port working under full duplex.
Gigabit Ethernet ports			
ACT	Green	On	Port link up.
		Blinking	Data transmitted.
LNK	Amber	On	Port link up.
SFP ports			
LNK / ACT	Green	On	Port link up.
		Blinking	Data transmitted.

3.3 Top Panel

The SISPM1040-382-LRT top panel components are shown below:

1. Terminal block opening
2. Terminal block installed
3. Chassis/Frame Ground



4. Cables

4.1 Ethernet Cables

The SISPM1040-382-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.

10/100 P.S.E. Base-TX RJ-45 Pin Assignments

Pin Number	Assignment
1	P.O.E Power input +
2	P.O.E Power input +
3	P.O.E Power input -
4	Not used
5	Not used
6	P.O.E Power input -
7	Not used
8	Not used

1000 Base-T RJ-45 Pin Assignments

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

The SISPM1040-382-LRT switch supports auto MDI/MDI-X operation. You can use a straight-through cable to connect a PC to the switch.

10/100 Base-TX MDI/MDI-X Pins Assignments

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

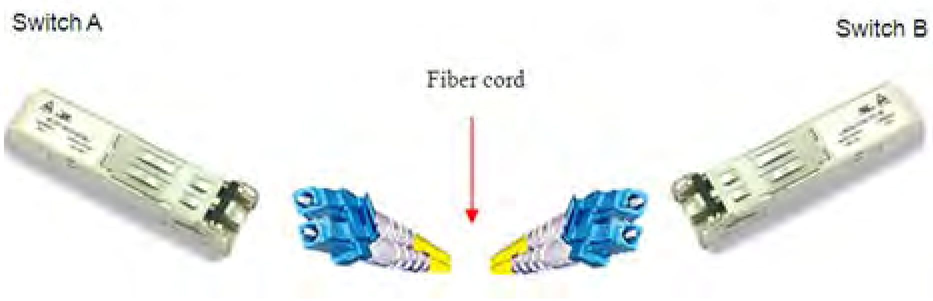
1000 Base-T MDI/MDI-X Pin Assignments

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

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

4.2 SFPs

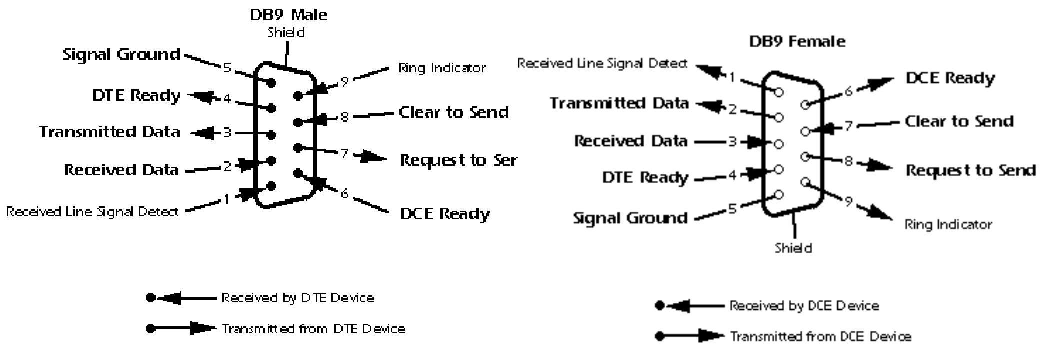
The switch has fiber optical ports with SFP connectors. The fiber optical ports are in multi-mode (0 to 550M, 850 nm with 50/125 μm, 62.5/125 μm fiber) and single-mode with LC connector. Make sure each SFP is correctly oriented before inserting fully. **Note** that the TX port of Switch A should be connected to the RX port of Switch B. See the Transition Networks SFP page for more information. See the related SFP manual for important safety cautions and warnings.



4.3 Console Cable

The SISPM1040-382-LRT can be managed via the console port. One DB-9 to RJ-45 cable is included in the package. Connect the cable to a serial port on the PC via the RS-232 DB-9 female connector and the other end (RJ-45 connector) connects to the switch console port.

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



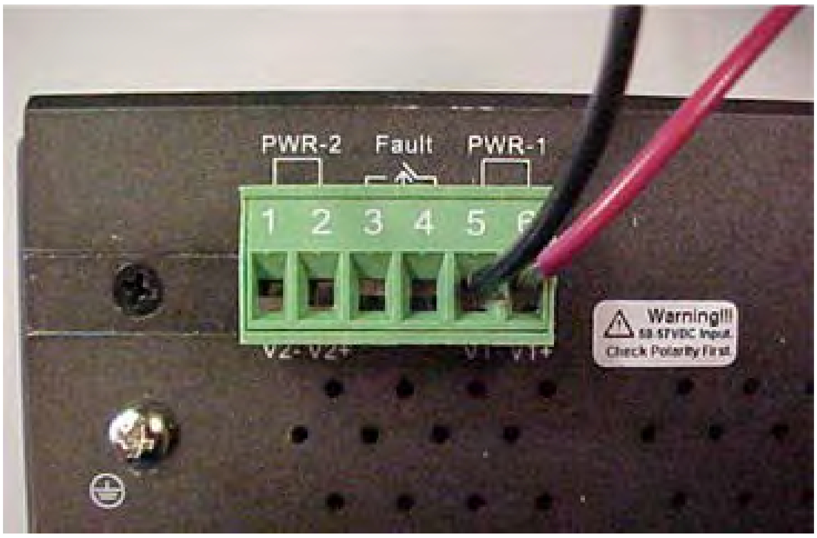
4. Power / Ground / Fault Relay

4.1 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. Observe wiring electrical codes. Do not exceed current limits for chosen wiring gauge. Beware of bundling too many high current wires. If the temperature exceeds the maximum ratings, serious damage to your equipment could result.
3. Rules of thumb:
   - □ 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.
   - □ 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.
   - □ Bundle wires of similar electrical characteristics together.
   - □ Separate input wiring from output wiring.
   - □ Label the wiring to all devices in the system.



4.2 Proper Earth Ground Isolation

For PoE applications, to achieve full isolation between PSE (switch port) and load (PD), the switch must be powered with a 1500 VAC / 2250 VDC isolated power supply.

For applications requiring additional isolation, 1) use an isolated AC/DC power source, e.g. TN 25104, 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. In addition, earth ground should be connected to the switch chassis.

WARNING

This case must be earth grounded.

No DC input may be earth grounded.

Use Isolated Power Supply.

WARNING

This case must be earth grounded

No DC input may be earth grounded

Use Isolated Power Supply

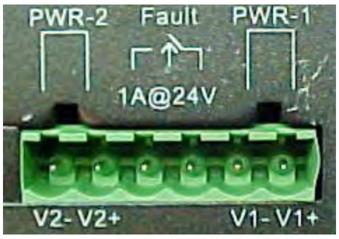
4.3 Grounding

Grounding and wire routing help limit the effects of noise due to electromagnetic interference (EMI). Run the ground connection from the ground screw to the grounding surface prior to connecting devices. Tie earth ground to both AC/DC power supply and switch.

Chassis Ground: There is a chassis ground screw, circled in red in the image above, which can be used to ground the device enclosure. Only negative grounding should be used.

The switch does not support positive grounding. Caution: to achieve required input power to RJ45 electrical isolation, the chassis ground must be isolated from the input power. • Connecting the chassis to earth ground is required. • Connecting the power source's negative rail to earth ground is prohibited. • Connecting the power source's positive rail to earth ground is prohibited.

4.4 Fault Relay



The switch provides connection for Fault Output Relay rated 1A@24VDC. The two relay contacts of the 6-pin terminal block connector are used to detect user-configured events. The two wires attached to the fault contacts form an open circuit when a user-configured when an event is triggered. If a user-configured event does not occur, the fault circuit remains closed.

4.5 Redundant Power Inputs

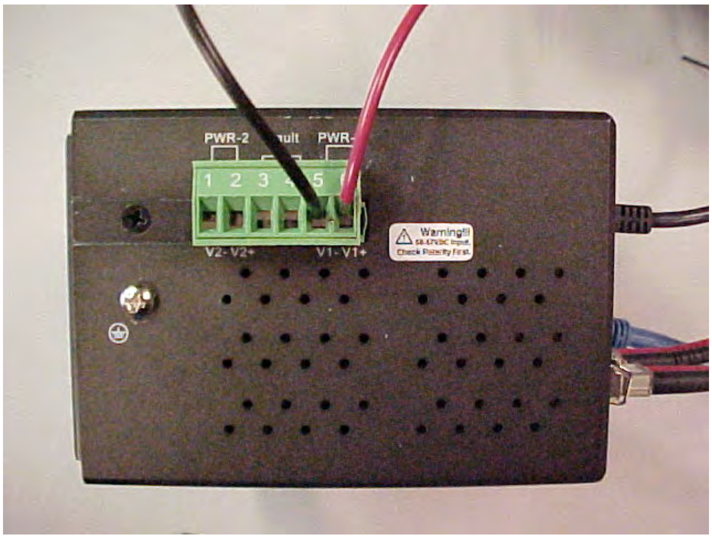
The switch has two sets of power inputs, power input 1 and power input 2. The top two contacts and the bottom two contacts of the 6-pin terminal block connector on the switch's top panel are used for the two digital inputs. Positive and negative terminals are labeled **V+** and **V-** for each input. Note polarity on the chassis of the switch. Suitable wire sizes to use for the power connection are 12~22AWG. 16AWG or 18AWG is preferred. Make cable connections before connecting Power.

4.6 Power Connection

Connect wires between the **+** terminals on the power supply and the **+** terminals on the switch terminal block. Do the same with the **–** terminals. Maintain correct polarity (not reverse polarity protected). Ensure the screws are tight and the wires secure. Follow the steps below to wire redundant power inputs.

Caution: before applying power, insert screw terminal connectors into the switch and verify all connections. Plugging in power connection after energizing power supply(s) may damage the switch.

Step 1: Remove the terminal block from its packaging and insert it into the power teminal.
Step 2: Insert the negative/positive wires into the V**-** and V**+** terminals, respectively.
Step 3: To keep the DC wires from pulling loose, use a small flat-blade screwdriver to tighten the wire-clamp screws on the front of the terminal block connector.



6. Web Management

5.1 Configuration by Web Browser

⚠ **Warning!** Remove physical loop connection before making any connection and upgrading firmware. Do **not** power off equipment while firmware is upgrading.

5.1.1 About Web-based Management

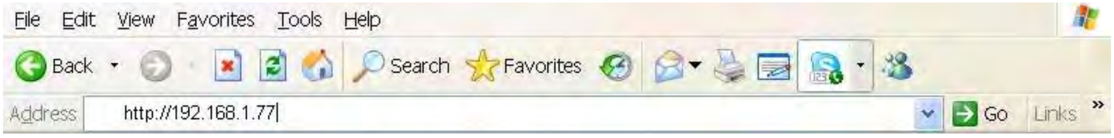
An embedded HTML web server resides in flash memory on the CPU board. It contains advanced management features and allows you to manage the switch from anywhere on the network through a standard web browser.

Web Management Defaults

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**.

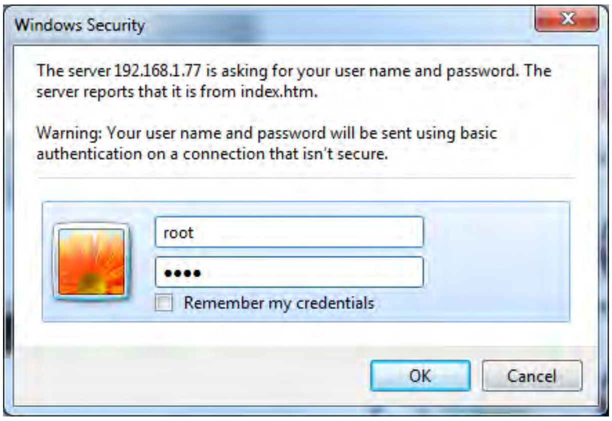
System Login

1. Launch a web browser such as Internet Explorer.
2. At the prompt http:// type the IP address of the switch. Press "**Enter**".



Address: http://192.168.1.77

3. At the login screen, enter the User name and Password. The default username and password are both "**root**".



The server 192.168.1.77 is asking for your user name and password. The server reports that it is from index.htm.

Warning: Your user name and password will be sent using basic authentication on a connection that isn't secure.

root

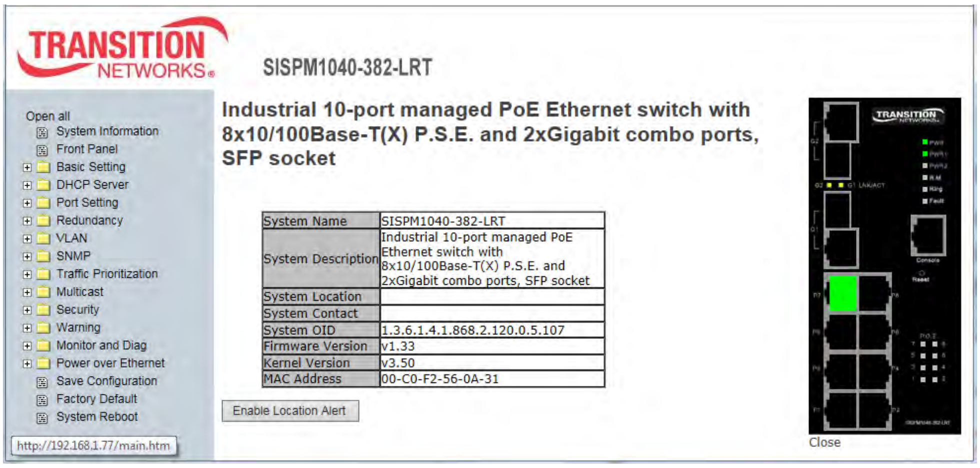
••••

□ Remember my credentials

Login screen

4. Press "**Enter**" or select the "**OK**" button; the main interface of the Web-based management displays.

Main Interface



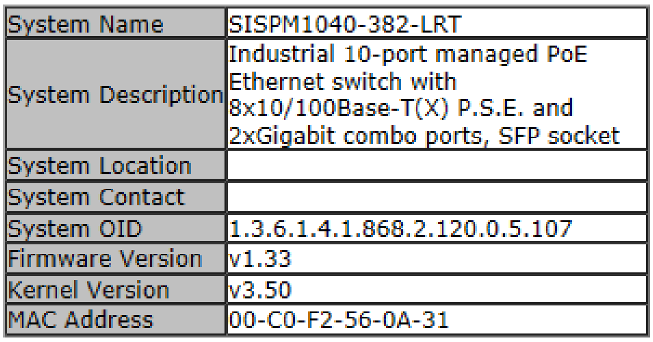
Industrial 10-port managed PoE Ethernet switch with 8x10/100Base-T(X) P.S.E. and 2xGigabit combo ports, SFP socket

System Name	SISPM1040-382-LRT
System Description	Industrial 10-port managed PoE Ethernet switch with 8x10/100Base-T(X) P.S.E. and 2xGigabit combo ports, SFP socket
System Location	
System Contact	
System OID	1.3.6.1.4.1.868.2.120.0.5.107
Firmware Version	v1.33
Kernel Version	v3.50
MAC Address	00-C0-F2-56-0A-31

Main interface - System information page

5.1.2 System Information

The system Information page displays the current system, hardware, Time, and software information.



System Name	SISPM1040-382-LRT
System Description	Industrial 10-port managed PoE Ethernet switch with 8x10/100Base-T(X) P.S.E. and 2xGigabit combo ports, SFP socket
System Location	
System Contact	
System OID	1.3.6.1.4.1.868.2.120.0.5.107
Firmware Version	v1.33
Kernel Version	v3.50
MAC Address	00-C0-F2-56-0A-31

System Information interface

The system information will display the configuration of Basic Setting / Switch Setting page.

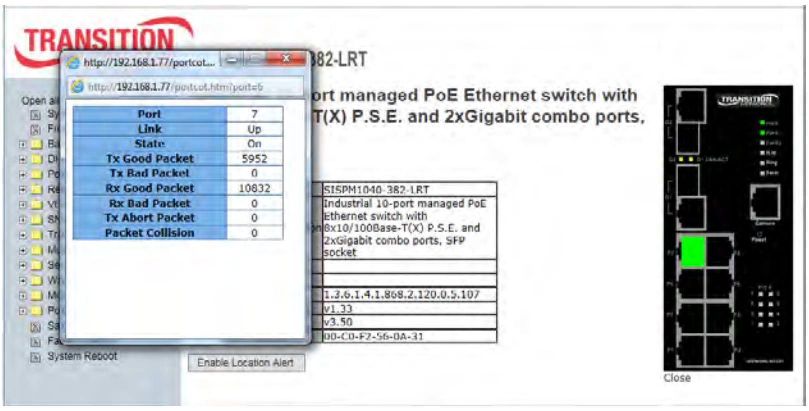
Enable Location Alert

This function can be used to physically locate the switch being configured. When you click the **Enable Location Alert** button, the **PWR1**, **PWR2** and **PWR3** LEDs will start to flash together to visibly identify the switch. To stop the location alert, click the **Disable Location Alert** button; the LEDs will stop flashing.

5.1.3 Front Panel

The Main interface page displays the SISPM1040-382-LRT front panel by default. Click “**Close**” to close the front panel display on the web pages. Click Front Panel to display it again.

You can click on a port to display its current status.



http://192.168.1.77/portcot...

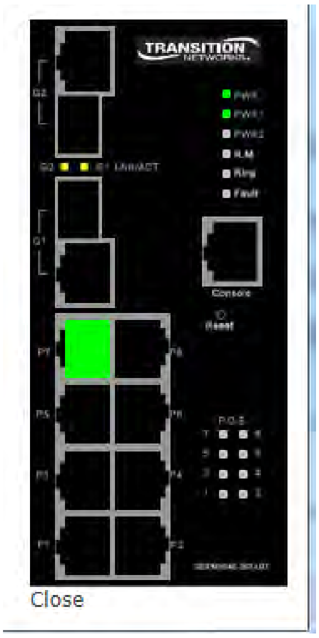
http://192.168.1.77/portcot.htm?port=6

Port	7
Link	Up
State	On
Tx Good Packet	5952
Tx Bad Packet	0
Rx Good Packet	10832
Rx Bad Packet	0
Tx Abort Packet	0
Packet Collision	0

382-LRT

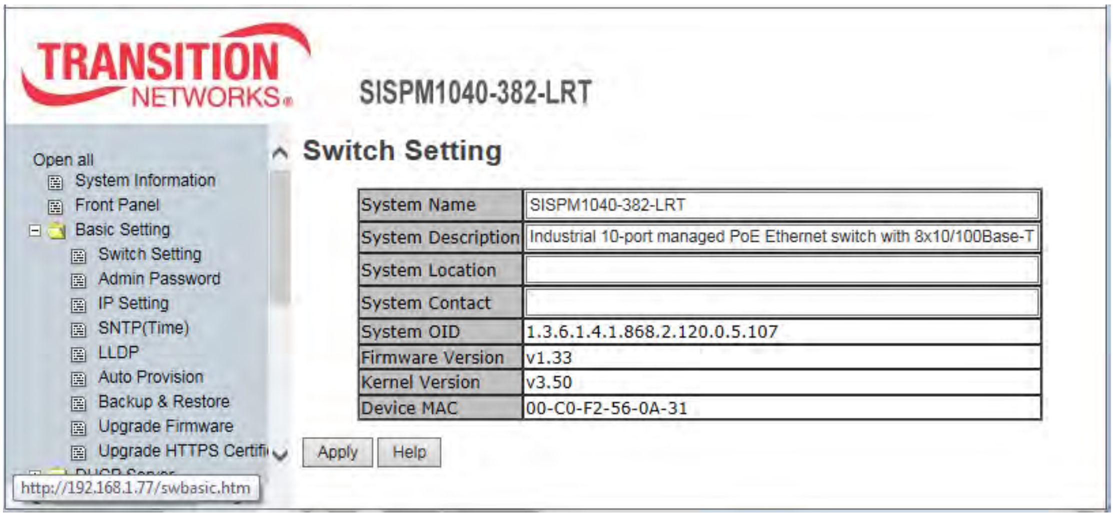
ort managed PoE Ethernet switch with T(X) P.S.E. and 2xGigabit combo ports.

SISPM1040-382-LRT
Industrial 10-port managed PoE Ethernet switch with 8x10/100Base-T(X) P.S.E. and 2xGigabit combo ports, SFP socket
1.3.6.1.4.1.868.2.120.0.5.107
v1.33
v3.50
00-C0-F2-56-0A-31



5.1.4 Basic Setting

5.1.4.1 Switch Setting



Switch Setting

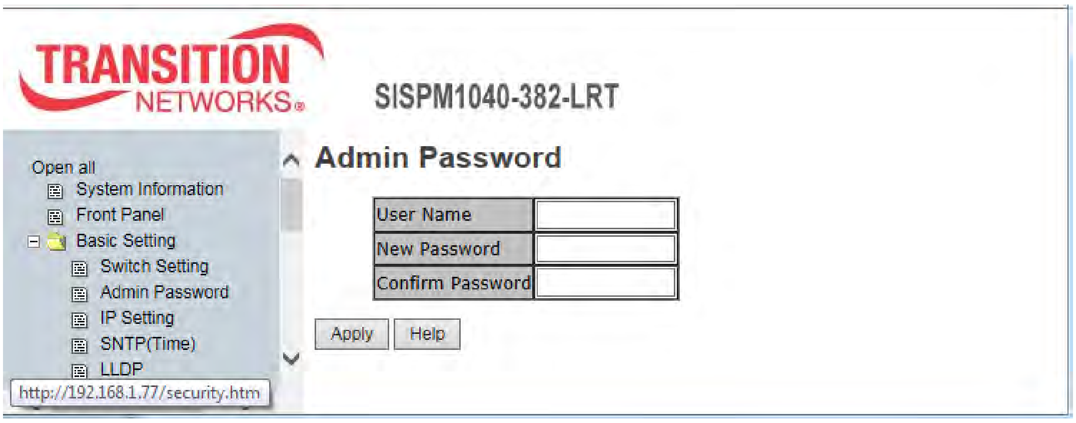
System Name	SISPM1040-382-LRT
System Description	Industrial 10-port managed PoE Ethernet switch with 8x10/100Base-T
System Location	
System Contact	
System OID	1.3.6.1.4.1.868.2.120.0.5.107
Firmware Version	v1.33
Kernel Version	v3.50
Device MAC	00-C0-F2-56-0A-31

Switch Setting interface

Label	Description
System Name	Assign the name of switch. The maximum length is 64 bytes.
System Description	Assign the description of switch. The maximum length is 256 bytes.
System Location	Assign the switch physical location. The maximum length is 64 bytes.
System Contact	Enter the name of contact person or organization. The maximum length is 256 bytes.
System OID	Displays the SNMP Object ID of enterprise private MIB in the format 1.3.6.1.4.1.868.2.120.0.5.107.
Firmware Version	Displays firmware release version (e.g., v1.33).
Kernel Version	Displays the current system kernel version (e.g., v3.50).
Device MAC	Displays the unique Ethernet hardware address in the format 00-C0-F2-56-0A-31.

5.1.4.2 Admin Password

Use this function to change web management login username and password for web, console, and Telnet management security

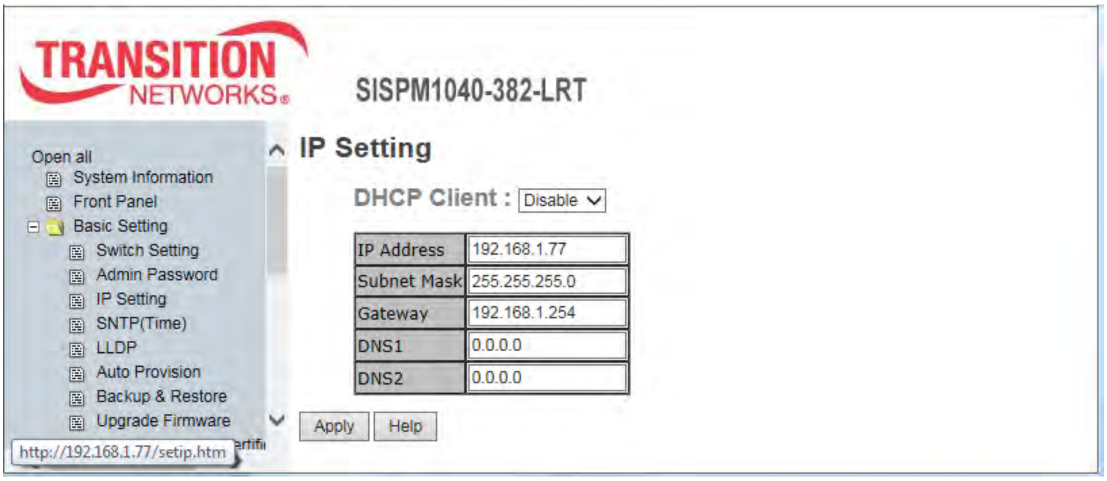


Admin Password interface

Label	Description
User Name	Enter the new username (the default is “**root**”).
New Password	Enter the new password (the default is “**root**”).
Confirm Password	Re-enter the new password.
Apply	Click “**Apply**” to activate the configurations.

5.1.4.3 IP Setting

You can configure the IP Settings and DHCP client using the IP Setting screen.



IP Setting

DHCP Client : Disable

IP Address	192.168.1.77
Subnet Mask	255.255.255.0
Gateway	192.168.1.254
DNS1	0.0.0.0
DNS2	0.0.0.0

IP Setting interface

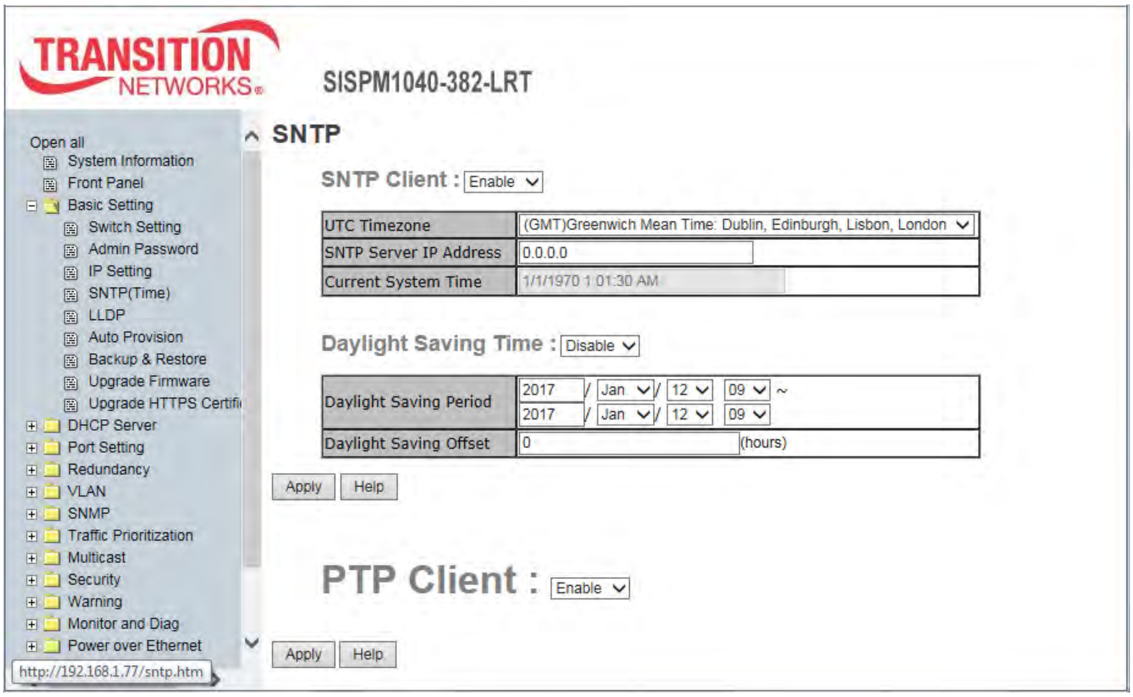
Label	Description
DHCP Client	To enable or disable the DHCP client function. When DHCP client function is enabled, the switch will be assigned the IP address from the network DHCP server. The default IP address will be replaced by the IP address which the DHCP server has assigned. After clicking the “**Apply**” button, a popup dialog is displayed to indicate the DHCP client is enabled. The IP address will be updated with the DHCP assigned address.
IP Address	Assign a static IP address that the switch will use. If the DHCP client function is enabled, you do not need to assign the IP address. If a static address needs to be assigned, enter the address in the IP Address box and select the **OK** button. The default IP address is 192.168.1.77.
Subnet Mask	Assign the subnet mask of the IP address. If DHCP client function is enabled, you do not need to assign the subnet mask.
Gateway	Assign the network gateway address for the switch. The default gateway address 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.
Apply	Click “**Apply**” to activate the configurations.

5.1.4.4 SNTP and PTP Client Setting

This page includes configuration for SNTP Client, system time, and PTP client.

SNTP(Time)

The SNTP (Simple Network Time Protocol) settings let you synchronize the system clock to an SNTP server.



SNTP Client : Enable

UTC Timezone	(GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
SNTP Server IP Address	0.0.0.0
Current System Time	1/1/1970 1:01:30 AM

Daylight Saving Time : Disable

Daylight Saving Period	2017 / Jan / 12 09 ~ 2017 / Jan / 12 09
Daylight Saving Offset	0 (hours)

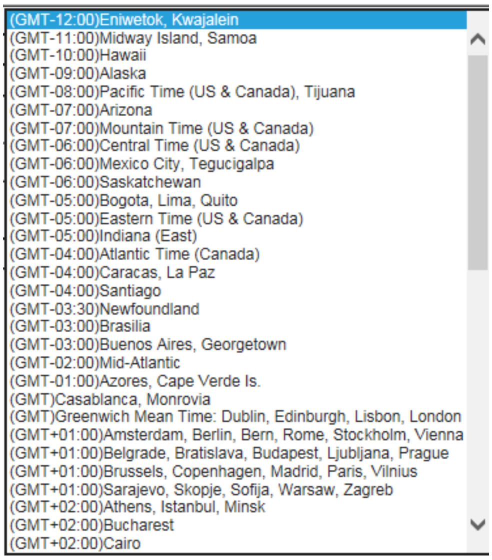
PTP Client : Enable

SNTP Configuration interface

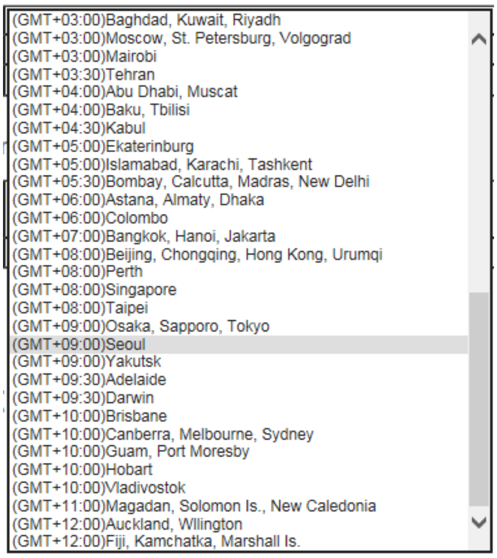
Label	Description
SNTP Client	Enable/Disable SNTP client.
UTC Timezone	Choose the UTC timezone of your city. Local time zone settings are provided below.
SNTP Server IP Addres	Enter the SNTP server IP address (or domain name address).
Daylight Saving Time	Enable or disable the daylight saving time function. When daylight saving time is enabled, you must configure the daylight saving time period.
Daylight Saving Period	Set the Daylight Saving beginning time and ending time. Both will be different each year.
Daylight Saving Offset	Set up the offset time in hours (turn system clock forward).
Switch Timer	Display the switch current time.
Apply	Click "**Apply**" to activate the configurations.

UTC Timezones:

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



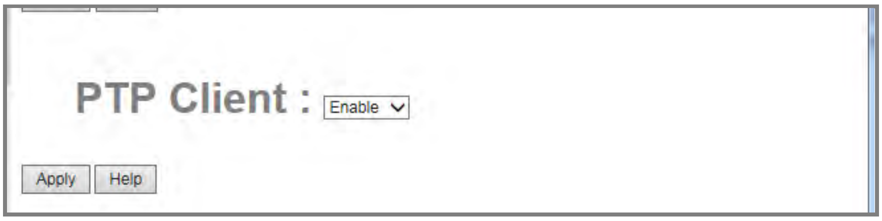
(GMT-12:00)Eniwetok, Kwajalein
(GMT-11:00)Midway Island, Samoa
(GMT-10:00)Hawaii
(GMT-09:00)Alaska
(GMT-08:00)Pacific Time (US & Canada), Tijuana
(GMT-07:00)Arizona
(GMT-07:00)Mountain Time (US & Canada)
(GMT-06:00)Central Time (US & Canada)
(GMT-06:00)Mexico City, Tegucigalpa
(GMT-06:00)Saskatchewan
(GMT-05:00)Bogota, Lima, Quito
(GMT-05:00)Eastern Time (US & Canada)
(GMT-05:00)Indiana (East)
(GMT-04:00)Atlantic Time (Canada)
(GMT-04:00)Caracas, La Paz
(GMT-04:00)Santiago
(GMT-03:30)Newfoundland
(GMT-03:00)Brasilia
(GMT-03:00)Buenos Aires, Georgetown
(GMT-02:00)Mid-Atlantic
(GMT-01:00)Azores, Cape Verde Is.
(GMT)Casablanca, Monrovia
(GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
(GMT+01:00)Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
(GMT+01:00)Belgrade, Bratislava, Budapest, Ljubljana, Prague
(GMT+01:00)Brussels, Copenhagen, Madrid, Paris, Vilnius
(GMT+01:00)Sarajevo, Skopje, Sofija, Warsaw, Zagreb
(GMT+02:00)Athens, Istanbul, Minsk
(GMT+02:00)Bucharest
(GMT+02:00)Cairo



(GMT+03:00)Baghdad, Kuwait, Riyadh
(GMT+03:00)Moscow, St. Petersburg, Volgograd
(GMT+03:00)Mairobi
(GMT+03:30)Tehran
(GMT+04:00)Abu Dhabi, Muscat
(GMT+04:00)Baku, Tbilisi
(GMT+04:30)Kabul
(GMT+05:00)Ekaterinburg
(GMT+05:00)Islamabad, Karachi, Tashkent
(GMT+05:30)Bombay, Calcutta, Madras, New Delhi
(GMT+06:00)Astana, Almaty, Dhaka
(GMT+06:00)Colombo
(GMT+07:00)Bangkok, Hanoi, Jakarta
(GMT+08:00)Beijing, Chongqing, Hong Kong, Urumqi
(GMT+08:00)Perth
(GMT+08:00)Singapore
(GMT+08:00)Taipei
(GMT+09:00)Osaka, Sapporo, Tokyo
(GMT+09:00)Seoul
(GMT+09:00)Yakutsk
(GMT+09:30)Adelaide
(GMT+09:30)Darwin
(GMT+10:00)Brisbane
(GMT+10:00)Canberra, Melbourne, Sydney
(GMT+10:00)Guam, Port Moresby
(GMT+10:00)Hobart
(GMT+10:00)Vladivostok
(GMT+11:00)Magadan, Solomon Is., New Caledonia
(GMT+12:00)Auckland, Wllington
(GMT+12:00)Fiji, Kamchatka, Marshall Is.

PTP Client

The Precision Time Protocol (PTP) is a time-transfer protocol defined in the IEEE 1588-2002 standard that allows precise synchronization of networks (e.g., Ethernet). Accuracy within the nanosecond range can be achieved with this protocol when using hardware generated timestamps.

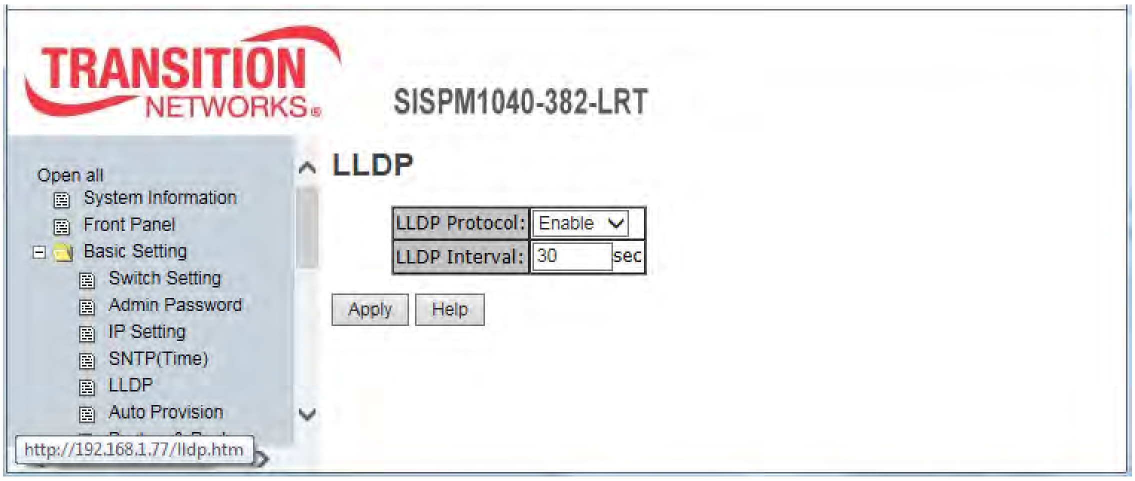


PTP Client : Enable

Label	Description
PTP Client	Enable or Disable the PTP Client. The default is disabled.
Apply	Click “**Apply**” to activate the configuration.

5.1.4.5 LLDP

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



LLDP

LLDP Protocol: Enable

LLDP Interval: 30 sec

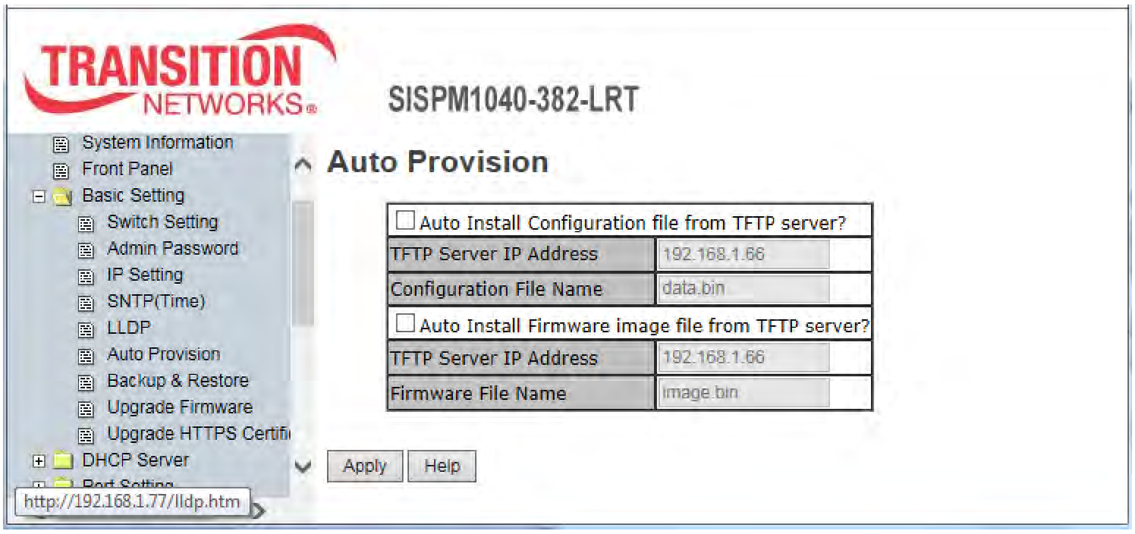
Apply Help

LLDP configuration interface

Label	Description
LLDP Protocol	"Enable" or "Disable" LLDP function.
LLDP Interval	The interval of resend LLDP (by default at 30 seconds)
Apply	Click "**Apply**" to set the configurations.
Help	Show help file.
Neighbor Info table	Can show neighbor device information.

5.1.4.6 Auto Provision

Auto Provision lets you update the switch firmware automatically. You can put firmware or configuration files on a TFTP server. 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 can make sure the configuration data and firmware image file is the newest version automatically from the TFTP server.



Auto Provision

☐ Auto Install Configuration file from TFTP server?	
TFTP Server IP Address	192.168.1.66
Configuration File Name	data.bin
☐ Auto Install Firmware image file from TFTP server?	
TFTP Server IP Address	192.168.1.66
Firmware File Name	image.bin

Auto Provision interface

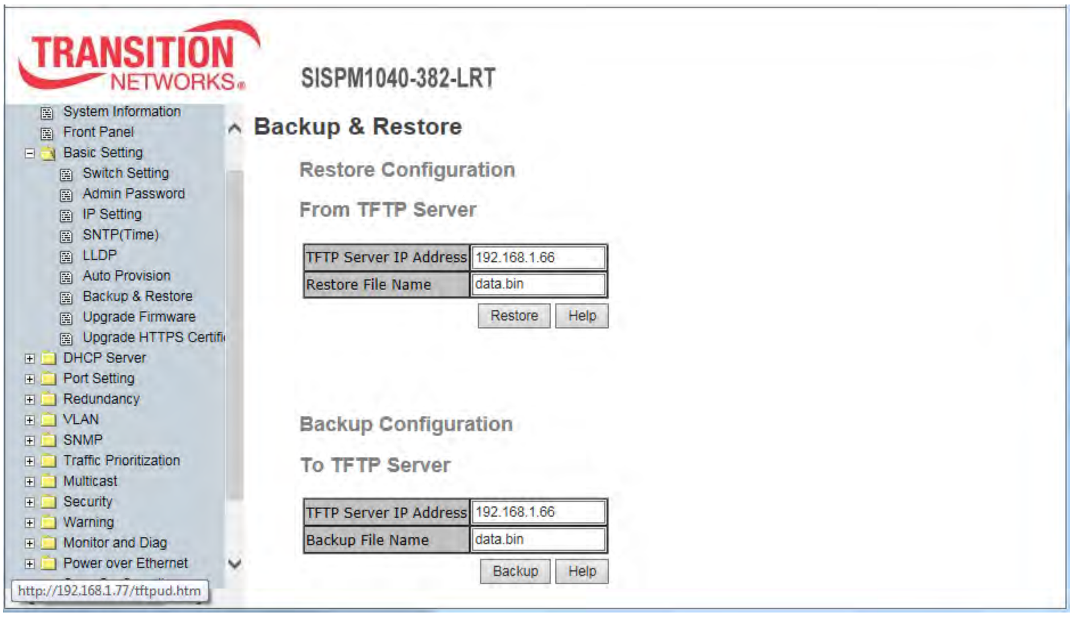
Label	Description
Auto Install Configuration file from TFTP server?	Check the box to automatically install the config file from the specified TFTP server.
TFTP Server IP Address	Enter the TFTP server IP address.
Configuration File Name	Enter the Configuration file name for downloading.
Auto Install Firmware Image file from TFTP server?	Check the box to automatically install the firmware image file from the specified TFTP server.
Firmware File Name	Enter the Firmware image file name for downloading.
Apply	Click "**Apply**" to set the configuration.

5.1.4.7 Backup & Restore

TFTP (Trivial File Transfer Protocol) can download user configuration data of the switch from a TFTP server to restore to system.

Backup Configuration uploads user configuration data of the switch to a TFTP server for backup.

Restore Configuration uses TFTP to download user configuration data of switch from the TFTP server to restore to system. After the configuration data is downloaded successfully, you must restart the switch for the restored configuration to be applied.



Backup & Restore

Restore Configuration

From TFTP Server

TFTP Server IP Address	192.168.1.66
Restore File Name	data.bin

Backup Configuration

To TFTP Server

TFTP Server IP Address	192.168.1.66
Backup File Name	data.bin

Backup & Restore interface

Label	Description
TFTP Server IP Address	Enter the TFTP server IP address.
Backup File Name	Fill the backup file name for downloading.
Restore	Click "**Restore**" to restore the configurations.
Restore File Name	Enter the file name.
Backup	Click "**Backup**" to backup the configuration.

***Message**: Apply fail TFTP transmission fail*

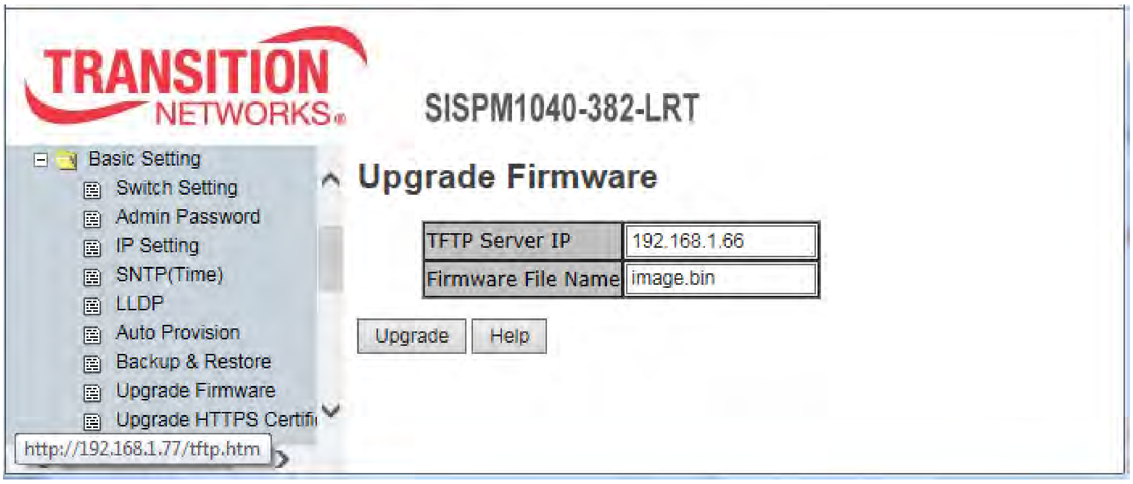
Meaning: The Backup or Restore function failed.

Recovery: 1. Click the **Retry** button. 2. Verify the filename and TFTP Server IP address. 3. Retry the Backup or Restore function.

5.1.4.8 Upgrade Firmware

TFTP (Trivial File Transfer Protocol) can download a firmware image file from a TFTP server to upgrade the switch. After successfully upgrading firmware, restart the system for the new firmware to be applied.

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



TFTP Server IP	192.168.1.66
Firmware File Name	image.bin

Upgrade Firmware interface

Label	Description
TFTP Server IP	Enter the TFTP server IP address.
Firmware File Name	Enter the firmware image file name for downloading.
Upgrade	Click “**Upgrade**” to restore the configuration. After a successful firmware upgrade, restart the system for the new firmware to be applied.

Backup / Upgrade / Restore Procedure

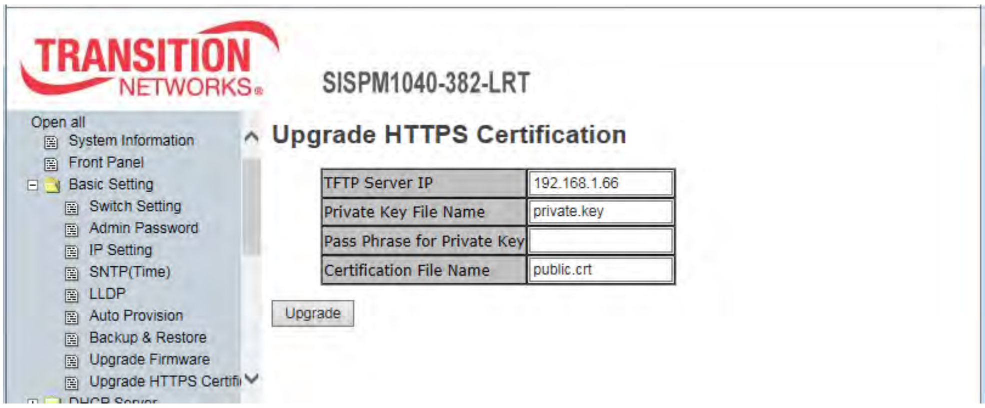
Note: To backup your config file before upgrading the firmware and then restore it after the firmware upgrade, use the following procedure:

1. Make any config changes desired.
2. Save the config.
3. Backup the current config.
4. Upgrade the firmware.
5. Reset to Factory Defaults.
6. Restore the backed-up config (from step 3 above).
7. Reboot the SISPM1040-382-LRT switch.

An ‘Apply Fail - Flash is already updated with this file’ message will display after the firmware upgrade if you attempt to restore the config (Step 6) before defaulting it (Step 5).

5.1.4.9 Upgrade HTTPS Certification

At Basic Setting > Upgrade HTTPS Certification you can upgrade the HTTPS certificate.



Upgrade HTTPS Certification

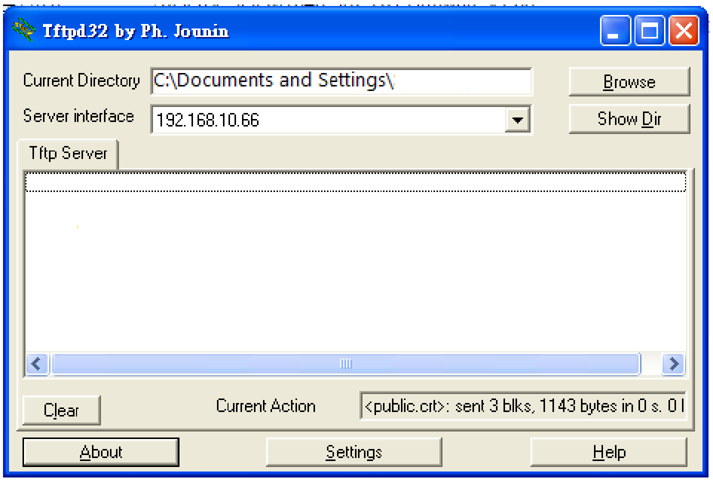
TFTP Server IP	192.168.1.66
Private Key File Name	private.key
Pass Phrase for Private Key	
Certification File Name	public.crt

Label	Description
TFTP Server IP	Enter the TFTP server IP address.
Private Key File Name	Enter the filename of the HTTPS private key.
Pass Phrase for Private Key	Enter the pass phrase for the HTTPS private key.
Certification File Name	Enter the filename of the HTTPS certificate.
Upgrade	Click the **Upgrade** button when done.

HTTPS Certificat Upgrade Procedure

HTTPS makes use of the Secure Socket Layer (SSL) functionality and allows the use of a custom SSL certificate created by the User. The switch uses the OpenSSL format for the customized certificate. To upgrade the HTTPS Certificate:

1. Start the TFTP Server software.

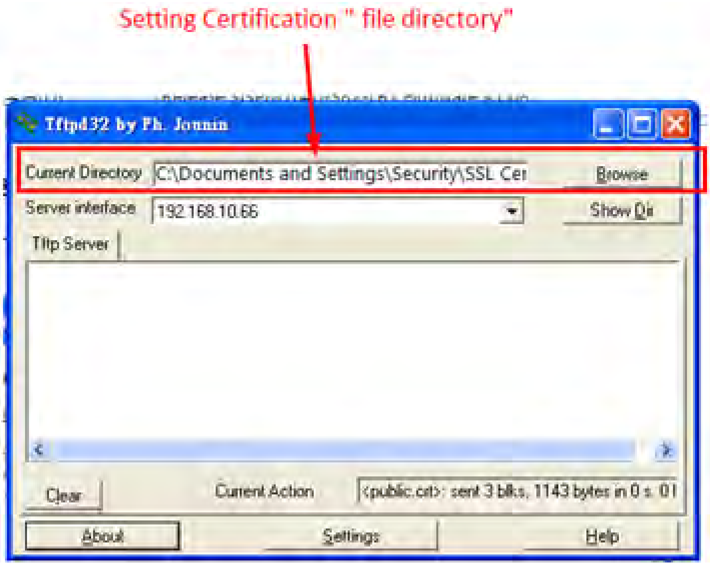


Current Directory: C:\Documents and Settings\

Server interface: 192.168.10.66

Current Action: <public.crt>: sent 3 blks, 1143 bytes in 0 s. 0 I

2. Browse to the directory where the SSL Certificates and Keys are located.

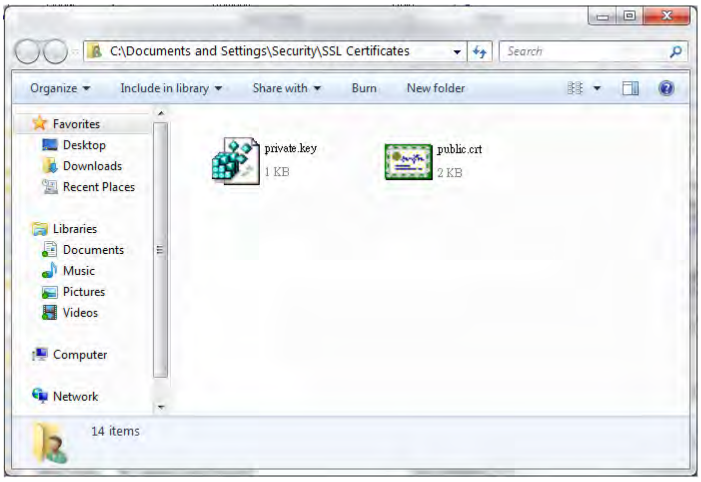


Setting Certification " file directory"

Current Directory: C:\Documents and Settings\Security\SSL Cer

Server interface: 192.168.10.66

Current Action: <public.crt>: sent 3 blks, 1143 bytes in 0 s. 0 1



C:\Documents and Settings\Security\SSL Certificates

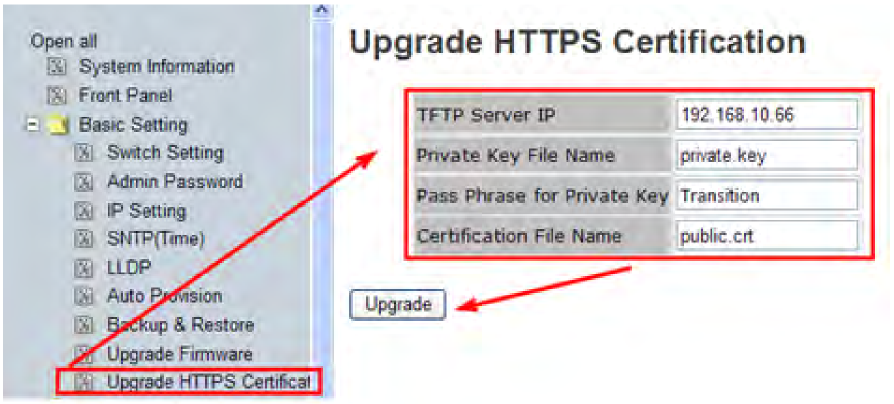
private.key 1 KB

public.crt 2 KB

14 items

3. Connect to the SISPM1040-382-LRT with an HTTP Browser and navigate to the Basic Settings.
4. Select the Upgrade HTTPS Certificate.
5. Enter the following information on the Upgrade HTTPS Certification screen:

- IP Address of the TFTP Server
- Private key file name
- Pass phrase for Private key
- Certification File name



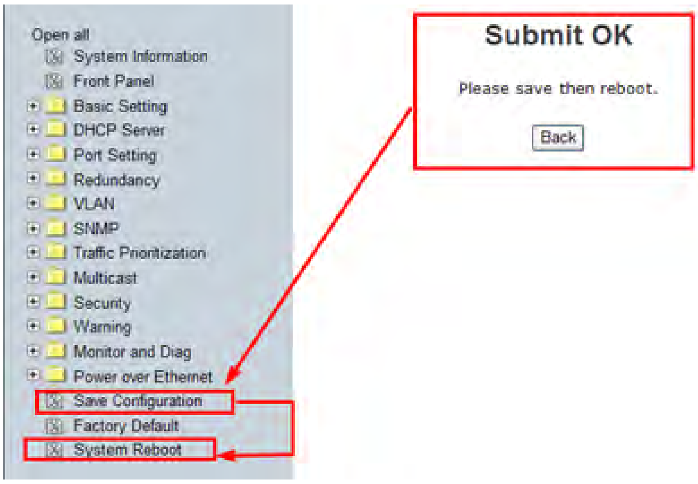
Upgrade HTTPS Certification

TFTP Server IP	192.168.10.66
Private Key File Name	private.key
Pass Phrase for Private Key	Transition
Certification File Name	public.crt

6. Once all the information has been entered select the **Upgrade** button.

The SISPM1040-382-LRT will connect to the TFTP server and look for the private key file and Certificate file in the TFTP server's current directory. The files will be uploaded to the SISPM1040-382-LRT.

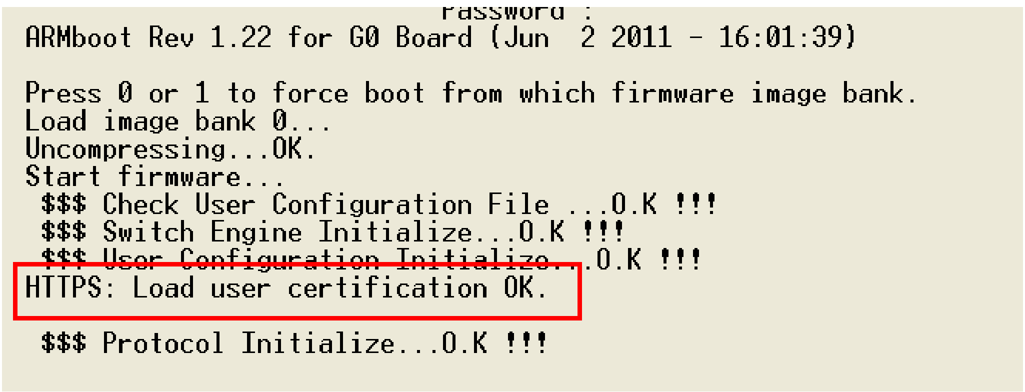
7. Once the upload of the files has completed and the Submit OK message is displayed, save the SISPM1040-382-LRT configuration and restart switch.



Submit OK

Please save then reboot.

8. The system will restart. In console mode, it will show that the Certification loaded properly by displaying **OK**.



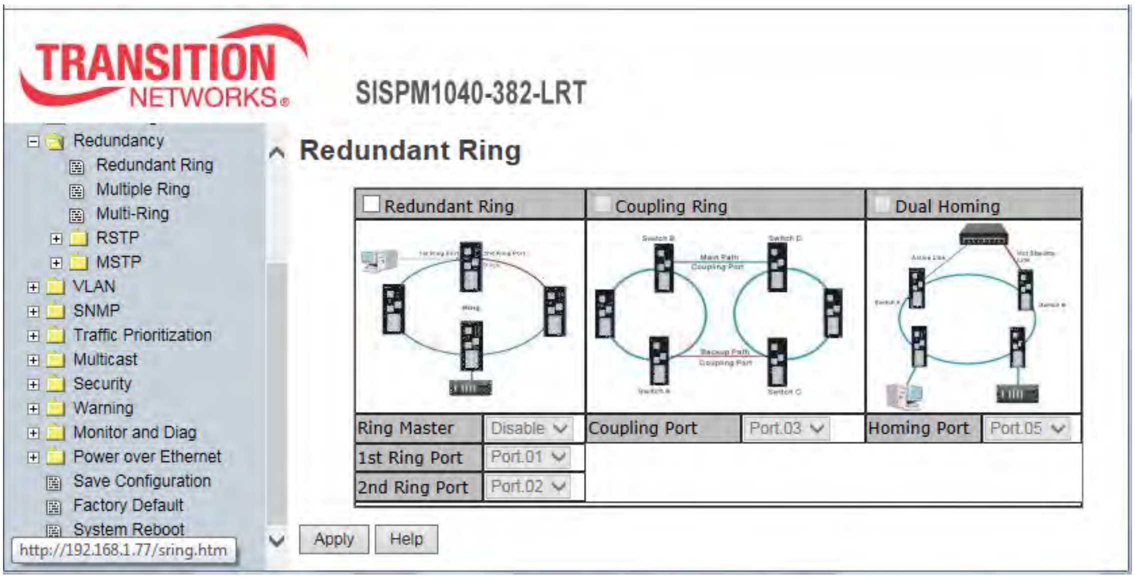
```
                       Password :
ARMboot Rev 1.22 for G0 Board (Jun  2 2011 - 16:01:39)

Press 0 or 1 to force boot from which firmware image bank.
Load image bank 0...
Uncompressing...OK.
Start firmware...
 $$$ Check User Configuration File ...O.K !!!
 $$$ Switch Engine Initialize...O.K !!!
 $$$ User Configuration Initialize...O.K !!!
HTTPS: Load user certification OK.

 $$$ Protocol Initialize...O.K !!!
```

5.1.1 Redundancy

Ring support includes three Ring topologies: Redundant Ring, Coupling Ring, and Dual Homing.

5.1.1.1 Redundant Ring

The Redundant Ring Protocol is a very fast network redundancy protocol that provides link fail-over protection with very fast self-healing recovery. This can reduce unexpected damage caused by network topology changes. Note that all switches in a ring should have Redundant Ring enabled.



Redundant Ring

☐ Redundant Ring		Coupling Ring		Dual Homing	
Ring Master	Disable	Coupling Port	Port.03	Homing Port	Port.05
1st Ring Port	Port.01				
2nd Ring Port	Port.02				

Redundant Ring interface

The following table describes the labels in this screen.

Label	Description
Redundant Ring	Check the checkbox to enable the Redundant Ring function.
Ring Master	There should be one and only one Ring Master in a ring. However if there are two or more switches set to be the Ring Master, the switch with the lowest MAC address will be the actual Ring Master and the others will be Backup Masters.
1st Ring Port	The primary port if this switch is Ring Master.
2nd Ring Port	The backup port if this switch is Ring Master.
Coupling Ring	Check the checkbox to enable Coupling Ring. Coupling Ring can be used to divide a large ring into two smaller rings to avoid affecting all switches when network topology changes. It is a good application for connecting two Rings.

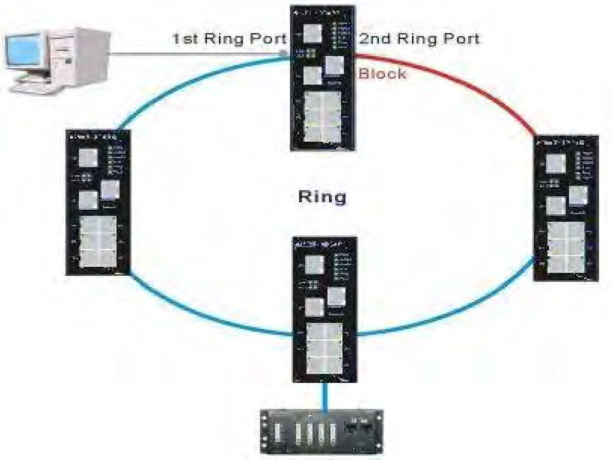
Coupling Port	Link to Coupling Port of a switch in another ring. Coupling Ring needs four switches to build an active and a backup link. Set a port as the Coupling port. The coupled four ports of four switches will be run in active/backup mode. Note that only two switches can enable Coupling Ring in a ring. More or less than two is invalid.
Dual Homing	Check the checkbox to enable Dual Homing. By selecting Dual Homing mode, the Ring will be connected to normal switches through two RSTP links (e.g., the backbone Switch). The two links work in active/backup mode, and connect each Ring to the normal switches in RSTP mode. Note that only two switches can enable Dual Homing in a ring. More or less than two is invalid.
Homing Port	At the dropdown select the port you want as the Dual Homing Port.
Apply	Click “Apply” to set the configurations.

Messages: *Apply fail Wrong data submitted* and *This switch is Master switch.*
Meaning: The same port has both Primary port and Backup port assignments.
Recovery: Change the 1st Ring Port setting or the 2nd Ring Port setting.

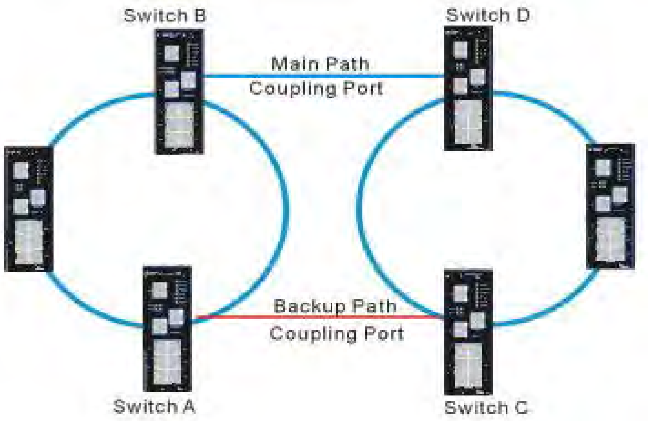
Note:

- We suggest you not set one switch as both a Ring Master and a Coupling Ring at the same time due to heavy load.
- Network redundancy protocol should be correctly configured for all switches in the redundant network before actually connecting any backup/redundant path in order to prevent the inadvertent generation of traffic loops.
- Do not enable more than one redundancy protocol (e.g., Redundant Ring and RSTP) at the same time.

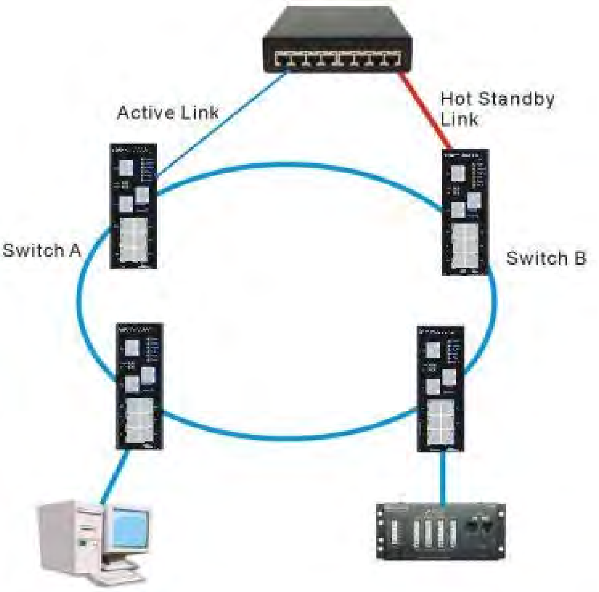
<u>Redundant Ring</u>:



<u>Coupling Ring</u>:

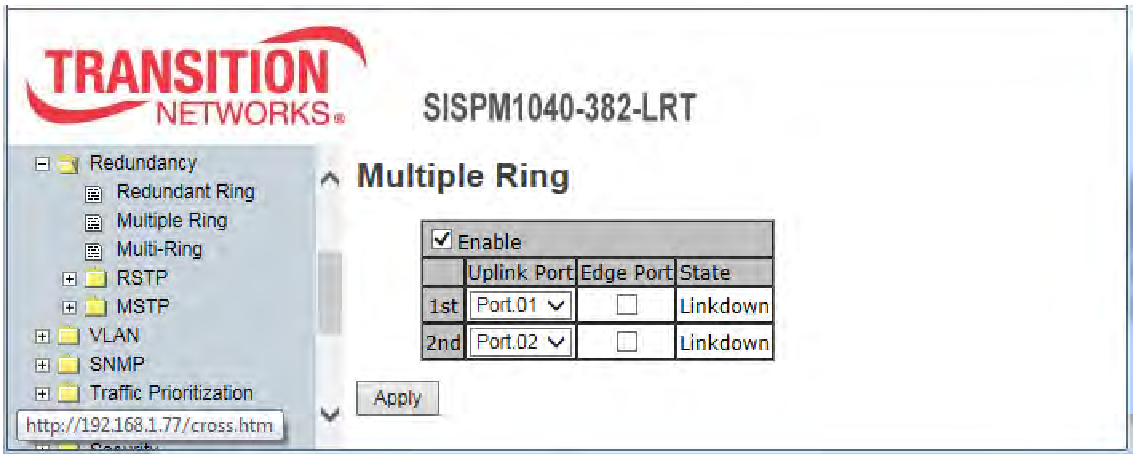


<u>Dual Homing</u>:



5.1.1.1 Multiple Ring

Navigate to the Redundancy > Multiple Ring menu path to display the Multiple Ring configuration table.



Multiple Ring

☑ Enable

	Uplink Port	Edge Port	State
1st	Port.01	□	Linkdown
2nd	Port.02	□	Linkdown

Multiple Ring interface

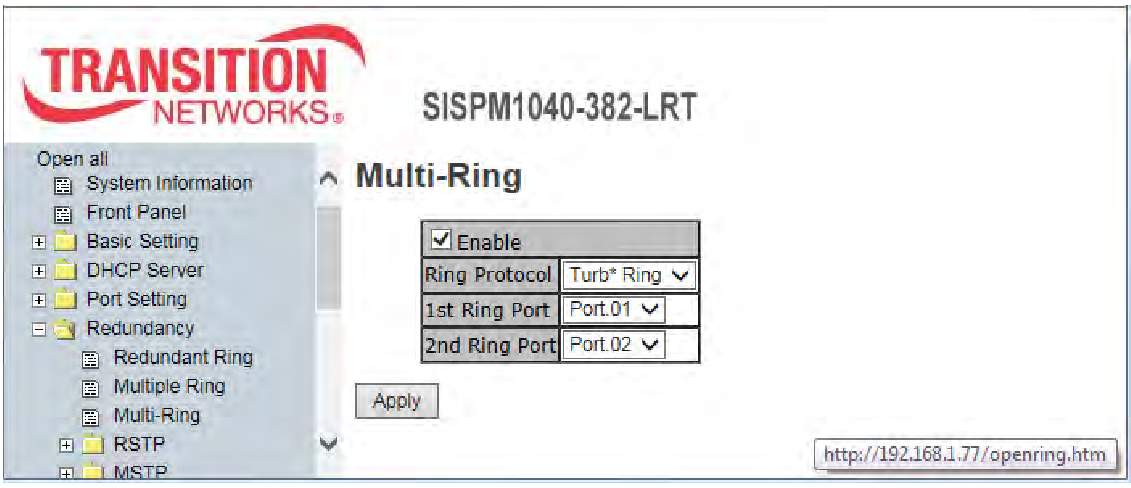
The following table describes the labels in this screen.

Label	Description
Enable	Check the checkbox to enable Multiple Rings.
Uplink Port	At the dropdowns, select a first and second uplink port (must be different port numbers).
Edge Port	Check one of the checkboxes for the port to become the Ring Edge Port.
State	The state of the ring port (e.g., Linkup, Linkdown).

If the message "*Apply fail The selected ports should be different to each other*" displays, click the **Retry** button, change one of the parameters above, and click the **Apply** button again.

5.1.1.2 Multi-Ring

Navigate to the Redundancy > Multi-Ring menu path to display the Multi Ring configuration table.



Multi-Ring

☑ Enable

Ring Protocol	Turb* Ring
1st Ring Port	Port.01
2nd Ring Port	Port.02

Multi-Ring interface

The following table describes the labels in this screen.

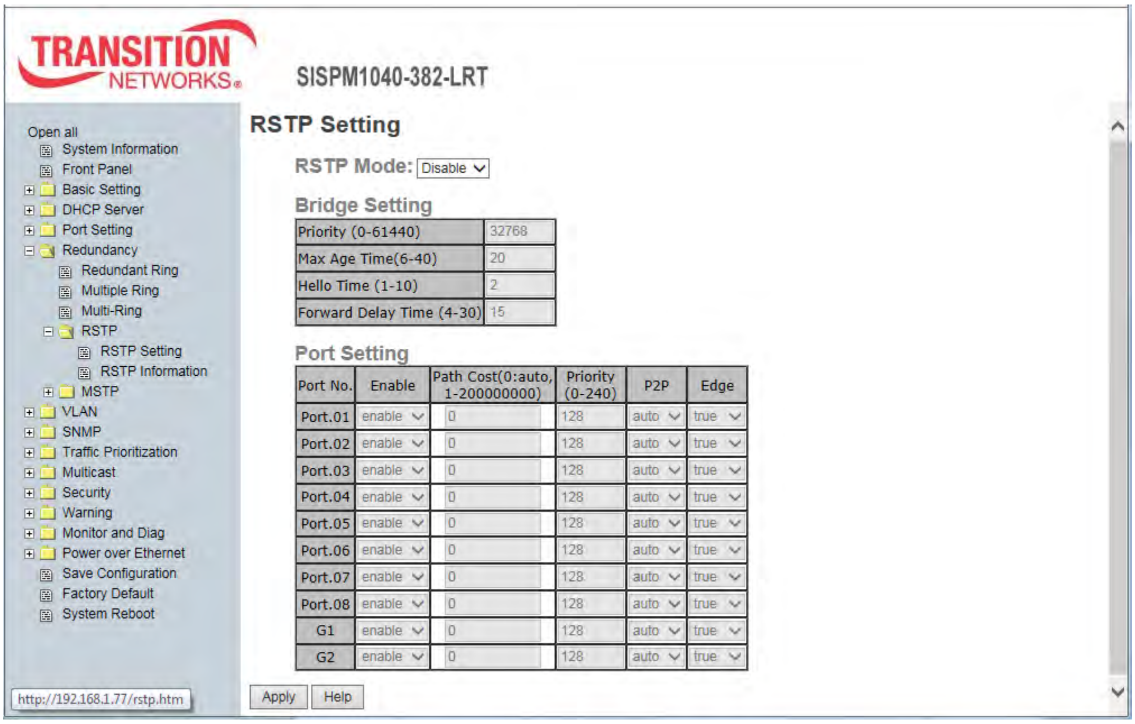
Label	Description
Enable	Check the checkbox to enable Multi-Ring.
Ring Protocol	At the dropdown, select the redundant ring protocol to be used: ***Turb* Ring***: use the Turb* Ring protocol. ***X-Ring***: use the X- Ring protocol. ***MRP Ring***: use the MRP Ring protocol.
1st Ring Port	At the dropdown, select the first ring port (Port.01 - Port.08, G1, or G2).
2nd Ring Port	At the dropdown, select the second ring port (Port.01 - Port.08, G1, or G2; must be a different port than the 1st Ring Port selected).

5.1.1.3 RSTP

The Rapid Spanning Tree Protocol (RSTP) is an evolution of the Spanning Tree Protocol. It provides faster spanning tree convergence after a topology change. The system also supports STP and the system will auto detect the connected device that is running STP or RSTP protocol. RSTP configures full, simple, and 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 for details.

RSTP Setting

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



RSTP Setting

RSTP Mode: Disable

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
Port.08	enable	0	128	auto	true
G1	enable	0	128	auto	true
G2	enable	0	128	auto	true

RSTP Setting interface

The following table describes the labels in this screen.

Label	Description
RSTP Mode	You must enable the RSTP function before configuring the related parameters. The default is Disable.
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. Note that if bridge priority is changed, the RSTP must be restarted. This value must be a 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 between 6 and 40. The default is 20.

Hello Time (1-10)	The time that controls how often the switch sends out the BPDU packet to check RSTP current status. Enter a value between 1 and 10 seconds. The default is 2 seconds.
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 between 4 and 30. The default is 15 seconds.
Apply	Click "**Apply**" to set the configurations.

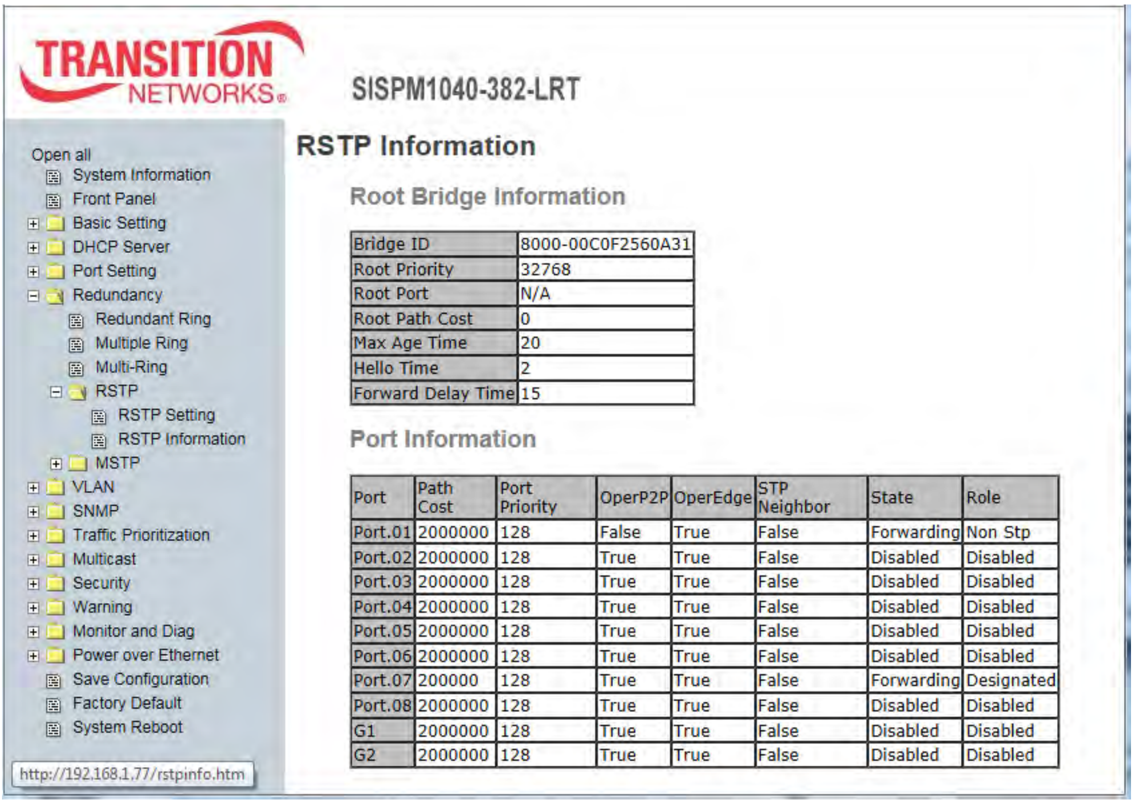
NOTE: Follow the rule to configure the Max Age, Hello Time, and Forward Delay Time:
2 x (Forward Delay Time value –1) > = Max Age value >= 2 x (Hello Time value +1)

Note:

- Network redundancy protocol should be correctly configured for all switches in a redundant network before actually connecting any backup/redundant path in order to prevent the inadvertent generation of traffic loops.
- Two redundancy protocols (e.g., Redundant Ring and RSTP) can not be enabled at the same time. The message "*Apply fail Another redundancy protocol is running. Only one could be run at the same time*" displays if this occurs. Disable one or more redundancy protocols and continue.

RSTP Information

Show RSTP algorithm results at this table:



RSTP Information

Root Bridge Information

Bridge ID	8000-00C0F2560A31
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	True	False	Forwarding	Non Stp
Port.02	2000000	128	True	True	False	Disabled	Disabled
Port.03	2000000	128	True	True	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	200000	128	True	True	False	Forwarding	Designated
Port.08	2000000	128	True	True	False	Disabled	Disabled
G1	2000000	128	True	True	False	Disabled	Disabled
G2	2000000	128	True	True	False	Disabled	Disabled

Label	Description
Path Cost (1-200000000)	The cost of the path to the other bridge from this transmitting bridge at the specified port. Enter a number 1 - 200000000. The default value is 200000 for mega-ports and 20000 for giga-ports.
Port Priority (0-240)	Decide which ports should be blocked by priority in the LAN. Valid values are 0 ~ 240 in steps of 16. The default value is 128.
Admin P2P	Some of the rapid state transactions that are possible within RSTP are dependent on whether the port configured can only be connected to exactly one other bridge (i.e., it is served by a point-to-point LAN segment), or it can be connected to two or more bridges (i.e., It is served by a shared medium LAN segment). This function allows the P2P status of the link to be manipulated administratively. **True** means P2P enabled. **False** means P2P disabled.
Admin Edge	The port directly connected to end stations, and it cannot create bridging loop in the network. To configure the port as an edge port, set the port to "**True**". 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.

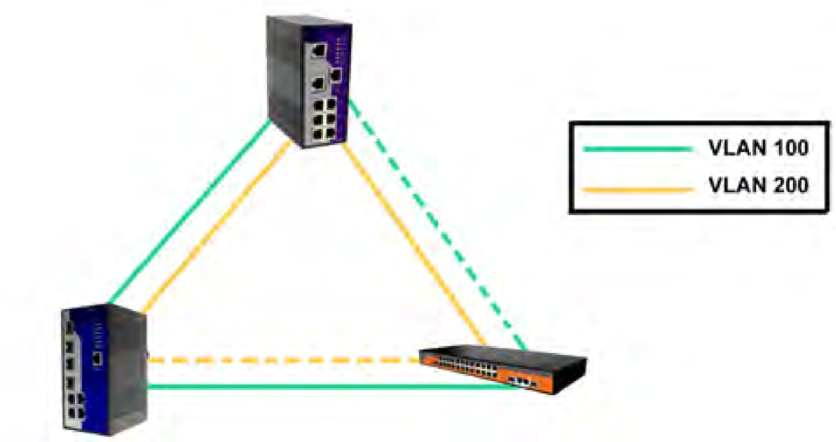
	All ports directly connected to end stations cannot create bridging loops in the network and can thus directly transition to forwarding, skipping the listening and learning stages.
Admin Non Stp	The port can include or exclude STP mathematic calculation. **True** excludes STP mathematic calculation (this port will not participate in RSTP). **False** includes the STP mathematic calculation.
Apply	Click "**Apply**" to set the configuration.

5.1.1.4 MSTP

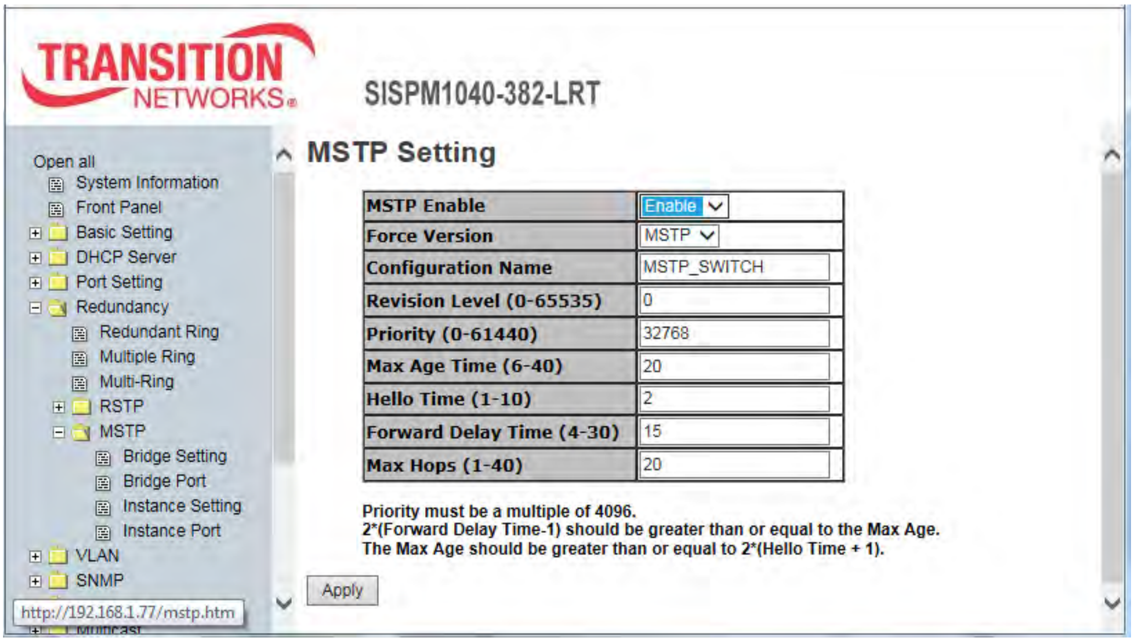
Multiple Spanning Tree Protocol (MSTP) is a standard protocol base on IEEE 802.1s.

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 a load balancing scheme and is less CPU intensive than PVST (Cisco proprietary technology).



MSTP Bridge Setting



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).

Apply

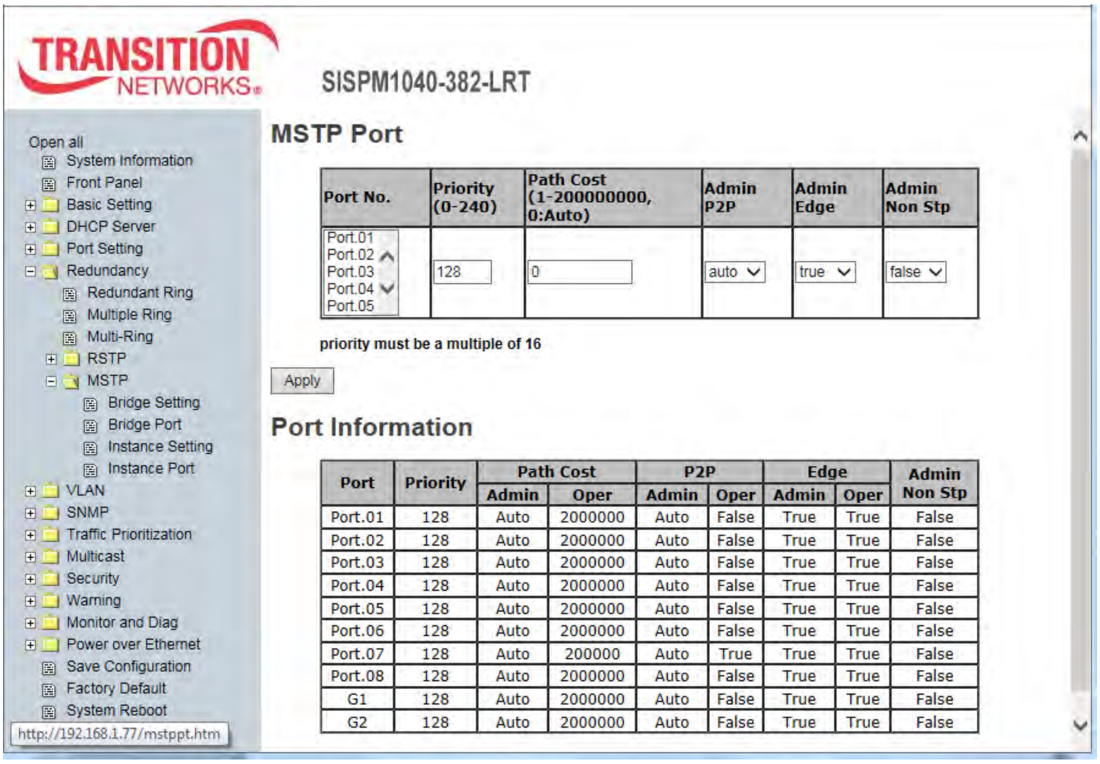
MSTP Setting interface

The following table describes the labels in the MSTP > Bridge Setting screen.

Label	Description
MSTP Enable	You must enable or disable MSTP function before configuring the related parameters.
Force Version	The Force Version parameter can be used to force a VLAN Bridge

	that supports RSTP to operate in an STP-compatible manner.
Configuration Name	The same MST Region must have the same MST configuration name.
Revision Level (0-65535)	The same MST Region must have the same revision level.
Priority (0-61440)	A value used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root. If the value changes, you must reboot the switch. The value must be a multiple of 4096 according to the protocol standard rule.
Max Age Time (6-40)	The number of seconds a bridge waits without receiving a Spanning-tree Protocol configuration message before attempting a reconfiguration. Enter a value of 6 - 40 seconds.
Hello Time (1-10)	The setting follows the rule below to configure the Max Age, Hello Time, and Forward Delay Time as the controlled switch sends out the BPDU packet to check RSTP current status. Enter a value 1 - 10. **2 x (Forward Delay Time value –1) ≥ Max Age value ≥ 2 x (Hello Time value +1)**
Forward 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 settings.

MSTP Bridge Port



MSTP Port

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

priority must be a multiple of 16

Apply

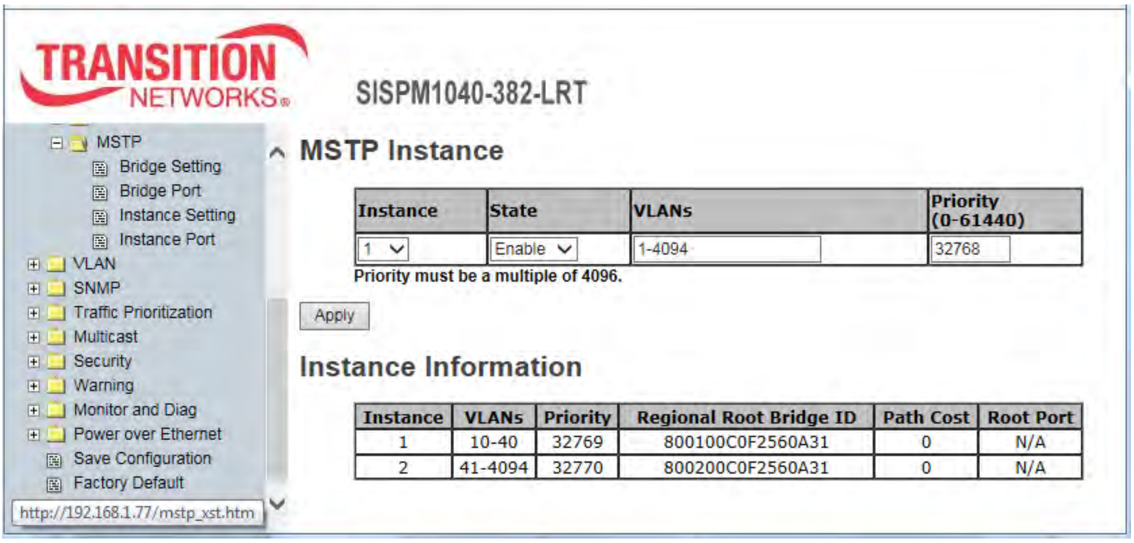
Port Information

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	128	Auto	2000000	Auto	False	True	True	False
Port.03	128	Auto	2000000	Auto	False	True	True	False
Port.04	128	Auto	2000000	Auto	False	True	True	False
Port.05	128	Auto	2000000	Auto	False	True	True	False
Port.06	128	Auto	2000000	Auto	False	True	True	False
Port.07	128	Auto	200000	Auto	True	True	True	False
Port.08	128	Auto	2000000	Auto	False	True	True	False
G1	128	Auto	2000000	Auto	False	True	True	False
G2	128	Auto	2000000	Auto	False	True	True	False

MSTP Port interface

Label	Description
Port No.	Select the port that you want to configure.
Priority (0-240)	Decide which port should be blocked by priority in the 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 a number between1 and 200000000.
Admin P2P	Some of the rapid state transactions that are possible within RSTP are dependent upon whether the port configured can only be connected to exactly one other bridge (i.e., it is served by a point-to-point LAN segment), or it can be connected to two or more bridges (i.e., it is served by a shared medium LAN segment). This function allows the P2P status of the link to be manipulated administratively. **True** means P2P enabling. **False** means P2P disabling.
Admin Edge	Select **true** or **false** at the dropdown.
Admin Non Stp	The port can include or exclude STP mathematic calculation. **True** excludes STP mathematic calculation. **False** includes the STP mathematic calculation.
Apply	Click “**Apply**” to activate the configurations.

MSTP Instance Setting



MSTP Instance

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

Priority must be a multiple of 4096.

Instance Information

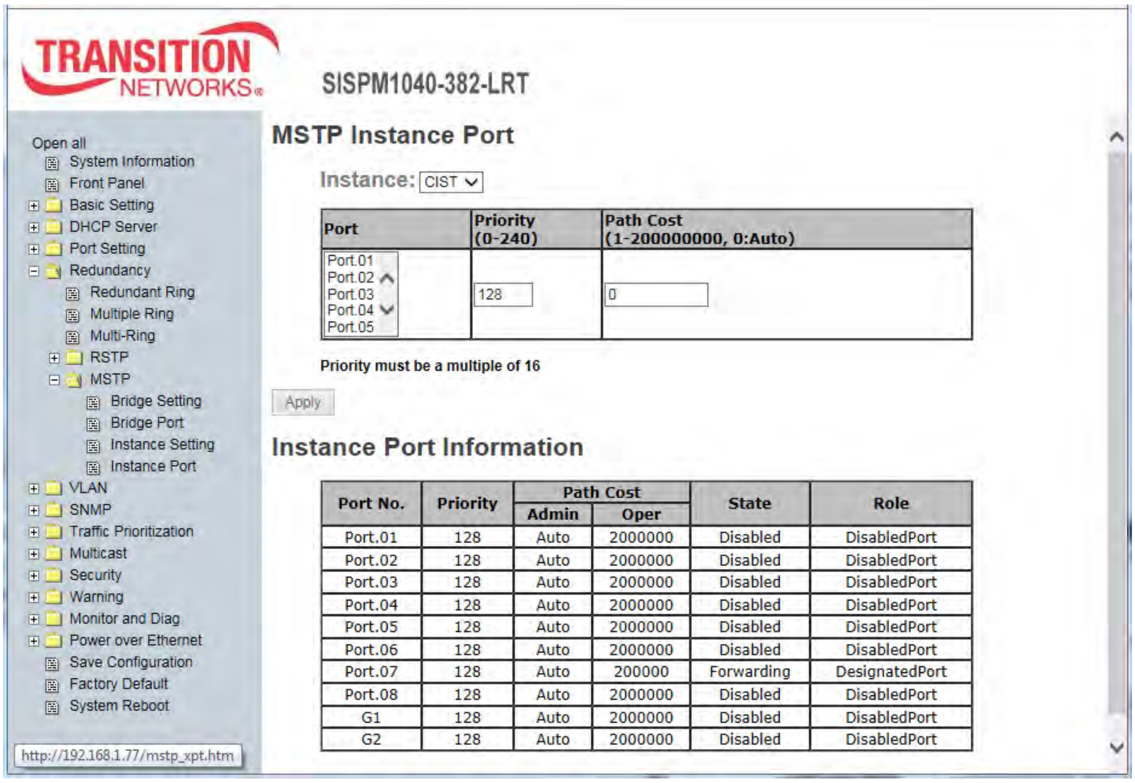
Instance	VLANs	Priority	Regional Root Bridge ID	Path Cost	Root Port
1	10-40	32769	800100C0F2560A31	0	N/A
2	41-4094	32770	800200C0F2560A31	0	N/A

MSTP Instance interface

Label	Description
Instance	Select the MSTP instance (1 – 15).
State	Enable or disable the instance.
VLANs	Set which VLAN(s) will belong which instance. Two different instances can not include the same VLAN ID.
Priority (0-61440)	A value used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root. If the value changes, you must reboot the switch. The value must be a multiple of 4096 according to the protocol standard rule.
Apply	Click "**Apply**" to activate the configurations.

The message "*Apply fail MSTP instance VLAN can't overlap*" displays if the VLANs in two different instances include the same VLAN IDs.

MSTP Instance Port



MSTP Instance Port

Instance: CIST

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

Priority must be a multiple of 16

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
Port.08	128	Auto	2000000	Disabled	DisabledPort
G1	128	Auto	2000000	Disabled	DisabledPort
G2	128	Auto	2000000	Disabled	DisabledPort

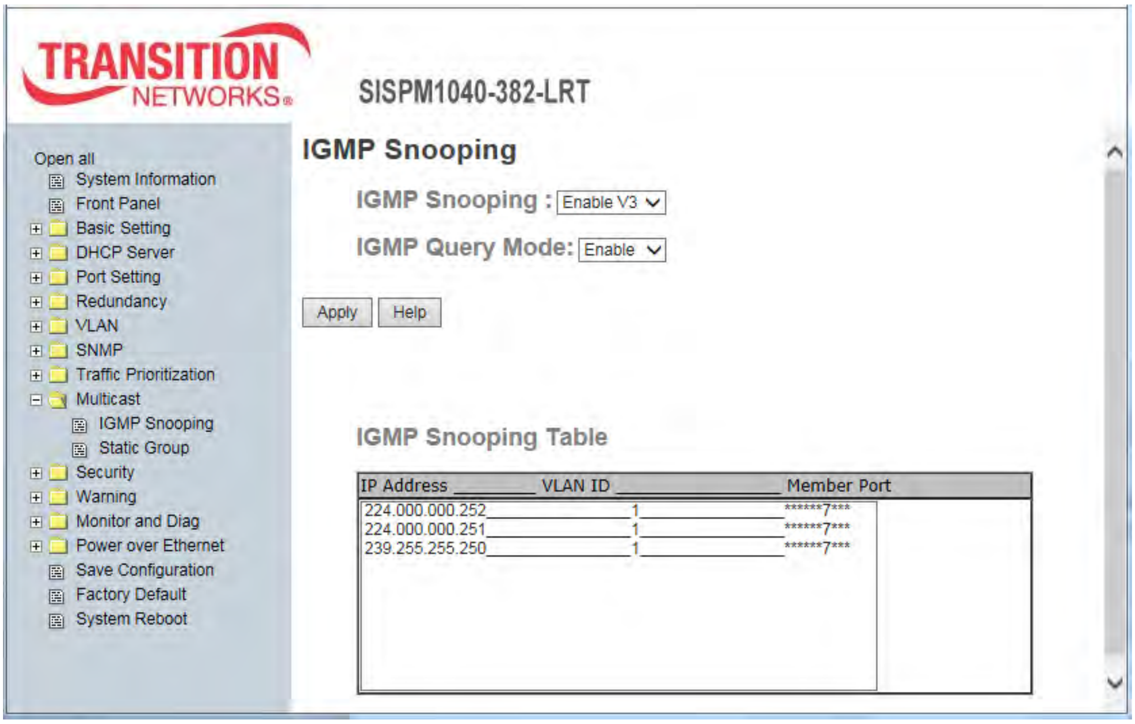
MSTP Instance Port interface

Label	Description
Instance	Set the instance’s information except CIST.
Port	Selecting the port that you want to configure.
Priority (0-240)	Decide which port should be blocked by priority in the LAN. Enter a number from 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 a number from 1 - 200000000.
Apply	Click “**Apply**” to set the configurations.

5.1.2 Multicast

5.1.2.1 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 the traffic and it reduces the amount of traffic on the Ethernet LAN.



IGMP Snooping

IGMP Snooping : Enable V3

IGMP Query Mode: Enable

IGMP Snooping Table

```
IP Address __________ VLAN ID ____________________ Member Port
224.000.000.252__________________1____________________******7***
224.000.000.251__________________1____________________******7***
239.255.255.250__________________1____________________******7***
```

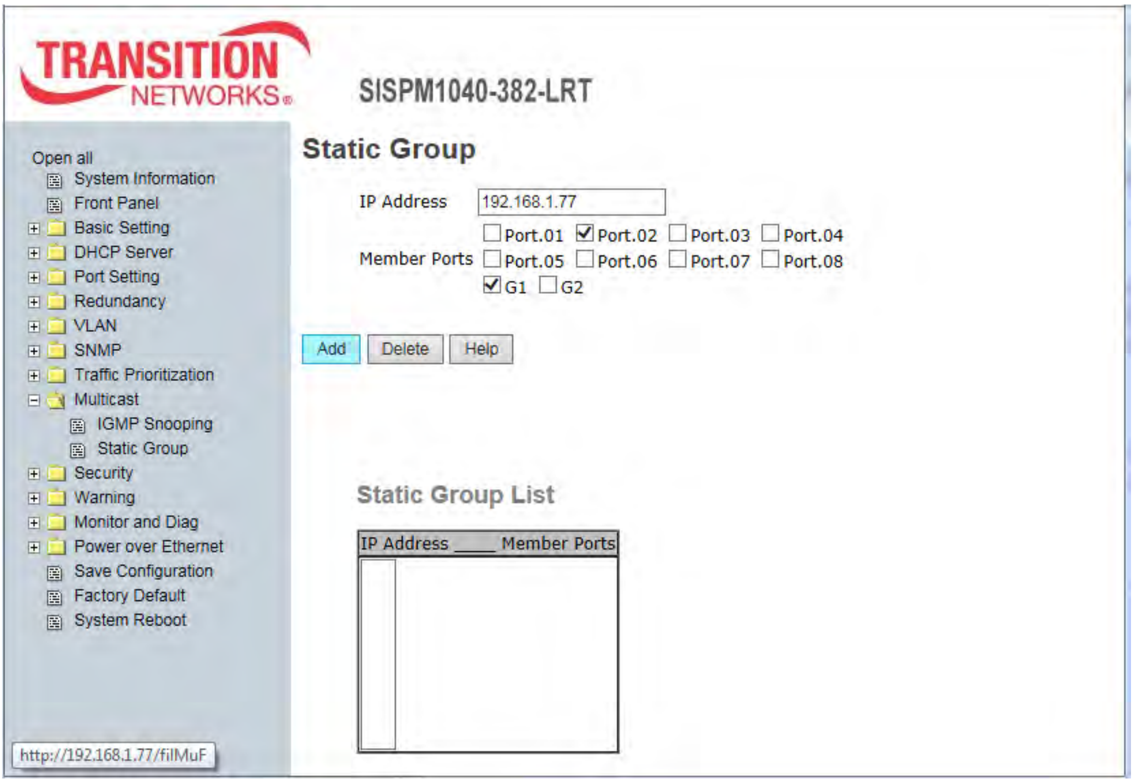
IGMP Snooping interface

The following table describes the labels in this screen.

Label	Description
IGMP Snooping	Enable/Disable IGMP snooping. At the dropdown select Enable V2, Enable v3, or Disable for the current IP multicast list.
IGMP Query Mode	Switch will be IGMP querier or not. There should be one and only one IGMP querier in an IGMP application. The "Auto" mode means that the querier is the one with a lower IP address.
IGMP Snooping Table	Shows the current IP multicast list.
Apply	Click “**Apply**” to set the configurations.

5.1.2.2 Static Group

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



Static Group

IP Address: 192.168.1.77

Member Ports: □ Port.01 ☑ Port.02 □ Port.03 □ Port.04 □ Port.05 □ Port.06 □ Port.07 □ Port.08 ☑ G1 □ G2

Static Group List

IP Address	Member Ports

Procedure:

1. **IP Address**: Assign a multicast group IP address in the range of 224.0.0.0 ~ 239.255.255.255.
2. **Member Ports**: Tick the check box beside the port number to include them as the member ports in the specific multicast group IP address.
3. Click "Add".
4. If you want to delete an entry from table, select the entry and click "Delete".

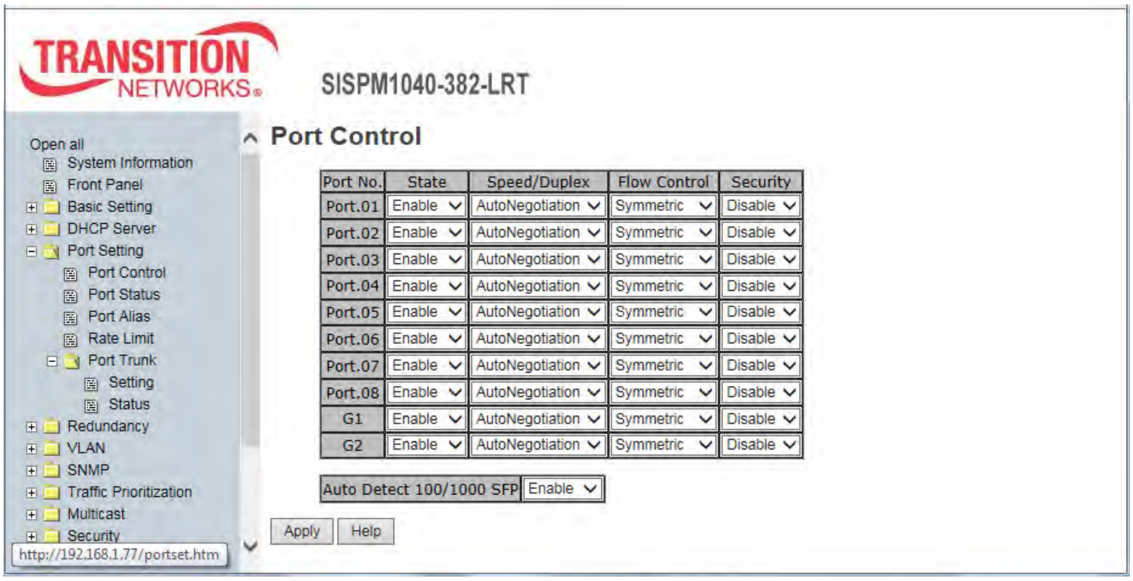
Message: *Apply fail Table full*

Message: *Apply fail string must contain 1 - 3 dots (.)*

5.1.3 Port Setting

5.1.3.1 Port Control

This function lets you set port state, speed/duplex, flow control, and security.



Port Control

Port No.	State	Speed/Duplex	Flow Control	Security
Port.01	Enable	AutoNegotiation	Symmetric	Disable
Port.02	Enable	AutoNegotiation	Symmetric	Disable
Port.03	Enable	AutoNegotiation	Symmetric	Disable
Port.04	Enable	AutoNegotiation	Symmetric	Disable
Port.05	Enable	AutoNegotiation	Symmetric	Disable
Port.06	Enable	AutoNegotiation	Symmetric	Disable
Port.07	Enable	AutoNegotiation	Symmetric	Disable
Port.08	Enable	AutoNegotiation	Symmetric	Disable
G1	Enable	AutoNegotiation	Symmetric	Disable
G2	Enable	AutoNegotiation	Symmetric	Disable

Auto Detect 100/1000 SFP: Enable

Port Control interface

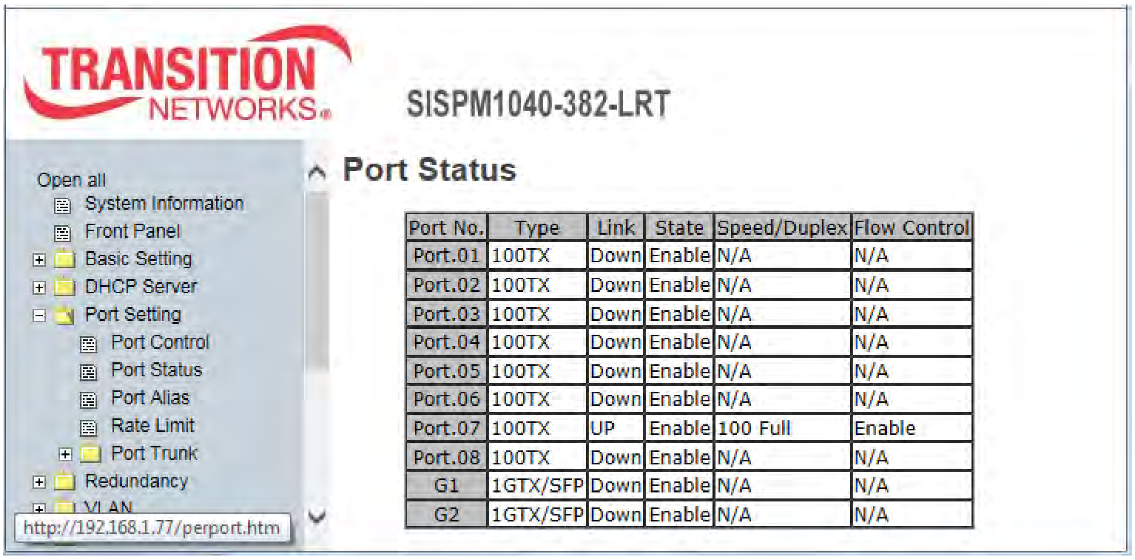
The following table describes the labels in this screen.

Label	Description
Port No.	Port number for this setting.
State	Enable or Disable port transmission.
Speed/Duplex	You can set to AutoNegotiation, 100-full, 100-half, 10-full, or 10-half mode.
Flow Control	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 on this port. So only the frames with MAC addresses in the port security list will be forwarded, otherwise packets will be discarded.
Auto Detect 100/1000 SFP	Select Enable to automatically detect the SFP port’s SFP Module speed (100M or 1000M).

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

5.1.3.2 Port Status

The Port Status table displays the current port status information (Type, Link state, Speed/Duplex setting, and Flow Control setting). See the previous section for parameter descriptions.



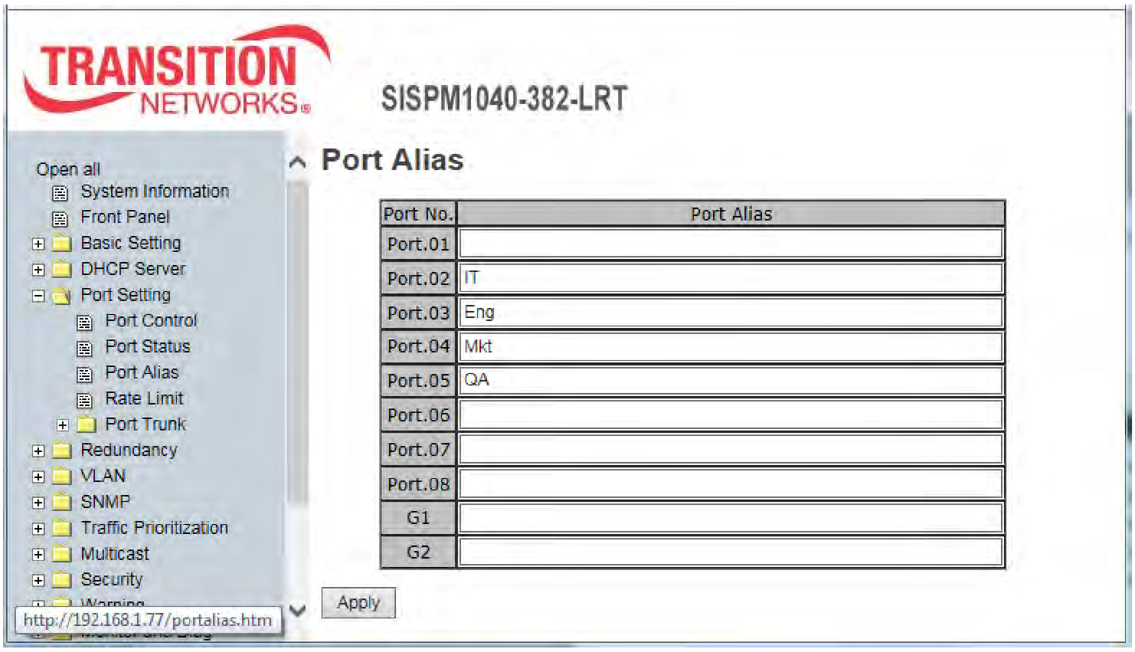
Port Status

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	UP	Enable	100 Full	Enable
Port.08	100TX	Down	Enable	N/A	N/A
G1	1GTX/SFP	Down	Enable	N/A	N/A
G2	1GTX/SFP	Down	Enable	N/A	N/A

Port Status interface

5.1.3.3 Port Alias

Here you can define a name for each port.



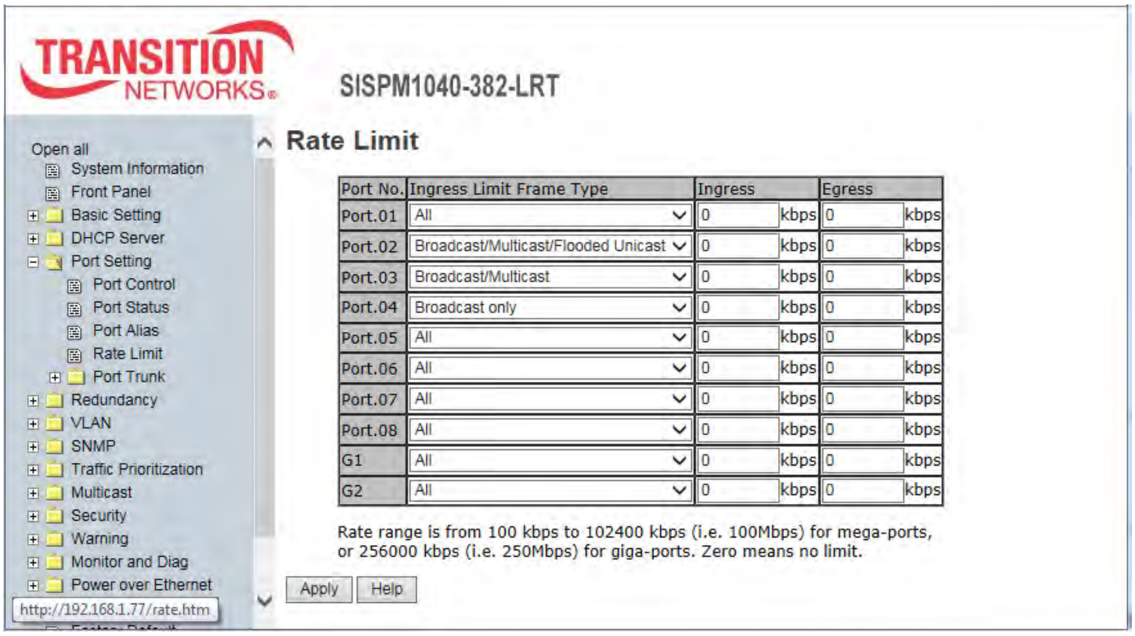
Port Alias

Port No.	Port Alias
Port.01	
Port.02	IT
Port.03	Eng
Port.04	Mkt
Port.05	QA
Port.06	
Port.07	
Port.08	
G1	
G2	

5.1.3.4 Rate Limit

Here you can limit traffic on all ports, including broadcast, multicast and flooded unicast.

You can also set “Ingress” or “Egress” to limit traffic received or transmitted bandwidth.



Rate Limit

Port No.	Ingress Limit Frame Type	Ingress		Egress	
Port.01	All	0	kbps	0	kbps
Port.02	Broadcast/Multicast/Flooded Unicast	0	kbps	0	kbps
Port.03	Broadcast/Multicast	0	kbps	0	kbps
Port.04	Broadcast only	0	kbps	0	kbps
Port.05	All	0	kbps	0	kbps
Port.06	All	0	kbps	0	kbps
Port.07	All	0	kbps	0	kbps
Port.08	All	0	kbps	0	kbps
G1	All	0	kbps	0	kbps
G2	All	0	kbps	0	kbps

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

Rate Limit interface

The following table describes the labels in this screen.

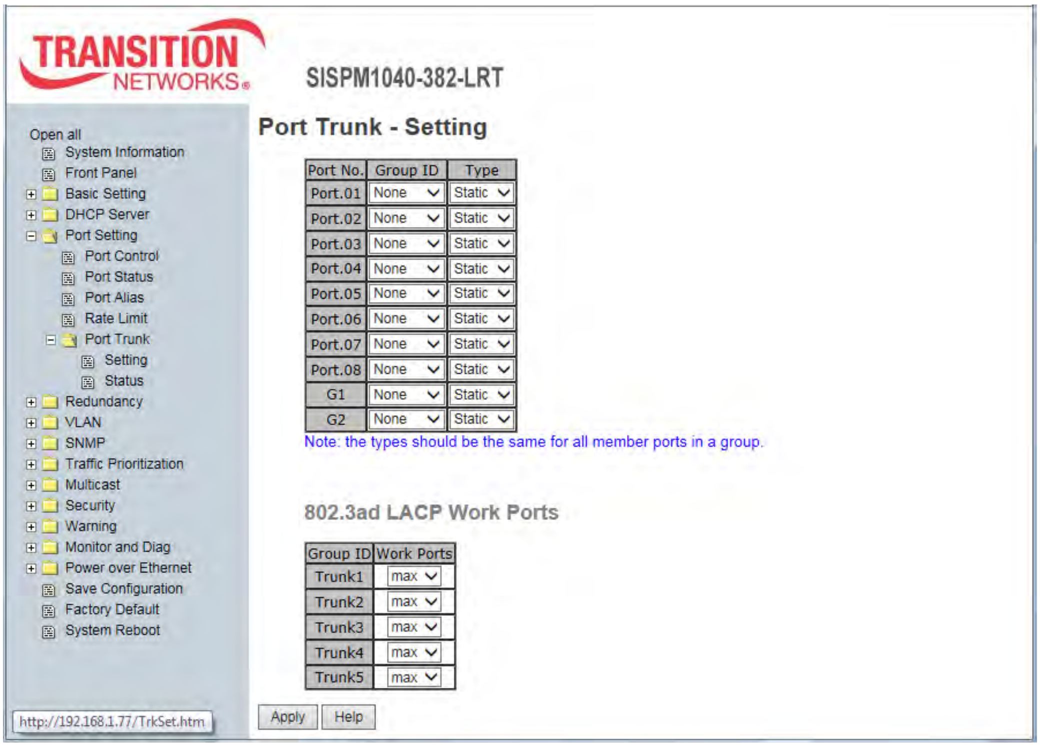
Label	Description
Ingress Limit Frame Type	You can select “**All**”, “**Broadcast only**”, ”**Broadcast/Multicast**” or ”**Broadcast/Multicast/Flooded Unicast**” mode. Select what kinds of frames are limited against ingress rate limit. If an ingress frame is not included in this setting, it will not be limited. Note that this setting is only against ingress rate limit but not egress.
Ingress	The switch port received traffic rate. The value of ingress rate limit. The unit of rate is kbps, and 1 Mbps is equal to 1024 kbps.
Egress	The switch port transmitted traffic rate. The value of egress rate limit. The unit of rate is kbps, and 1 Mbps is equal to 1024 kbps.
Apply	Click “**Apply**” to activate the configuration settings.

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

5.1.3.5 Port Trunk

Port Trunk – Setting

You can select static trunk or 802.3ad LACP to combine several physical links with a logical link to increase the bandwidth. Port trunking (aka, Link Aggregation) is specified in IEEE 802.3ad. Port trunking 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.



SISPM1040-382-LRT

Port Trunk - Setting

Port No.	Group ID	Type
Port.01	None	Static
Port.02	None	Static
Port.03	None	Static
Port.04	None	Static
Port.05	None	Static
Port.06	None	Static
Port.07	None	Static
Port.08	None	Static
G1	None	Static
G2	None	Static

Note: the types should be the same for all member ports in a group.

802.3ad LACP Work Ports

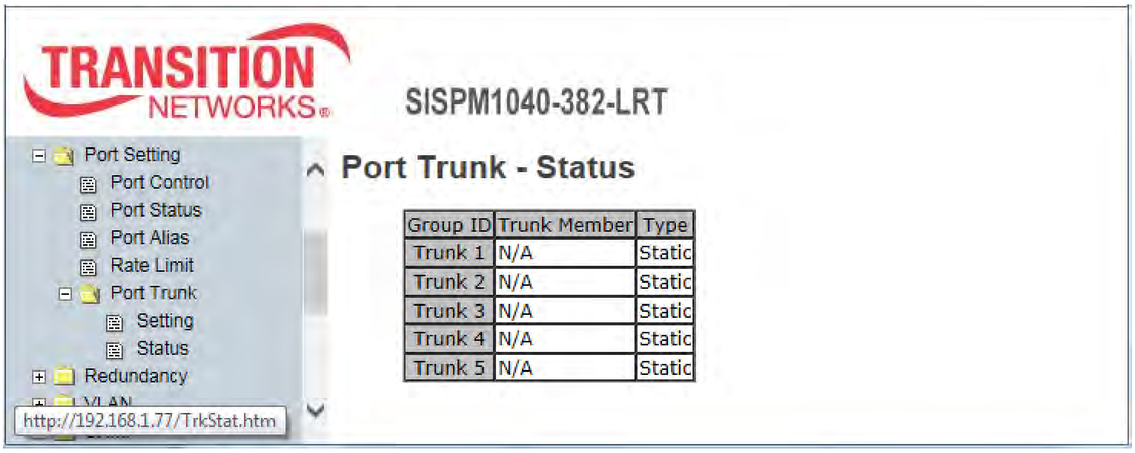
Group ID	Work Ports
Trunk1	max
Trunk2	max
Trunk3	max
Trunk4	max
Trunk5	max

Port Trunk - Setting interface

The following table describes the labels in this screen.

Label	Description
Group ID	Select the ports to join a trunk group.
Type	The switch supports Static trunk and 802.3ad LACP. Join 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. The port type and setting of member ports in a trunk group should be the same.
Work Ports	Select the number of active ports in a dynamic group (LACP). The default value of work ports is the maximum number of ports for 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. The number of member ports in a trunk group should be 2 - 4.
Apply	Click “**Apply**” to set the configurations.

Port Trunk – Status



Port Trunk - Status

Group ID	Trunk Member	Type
Trunk 1	N/A	Static
Trunk 2	N/A	Static
Trunk 3	N/A	Static
Trunk 4	N/A	Static
Trunk 5	N/A	Static

Port Trunk - Status interface

The following table describes the labels in this screen.

Label	Description
Group ID	Trunk Group number.
Trunk Member	Shows the Group port information.
Type	Shows the current port trunk type (e.g., Static).

5.1.4 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 the VLAN. Basically, creating a VLAN from a switch is logically equivalent to connecting 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**".

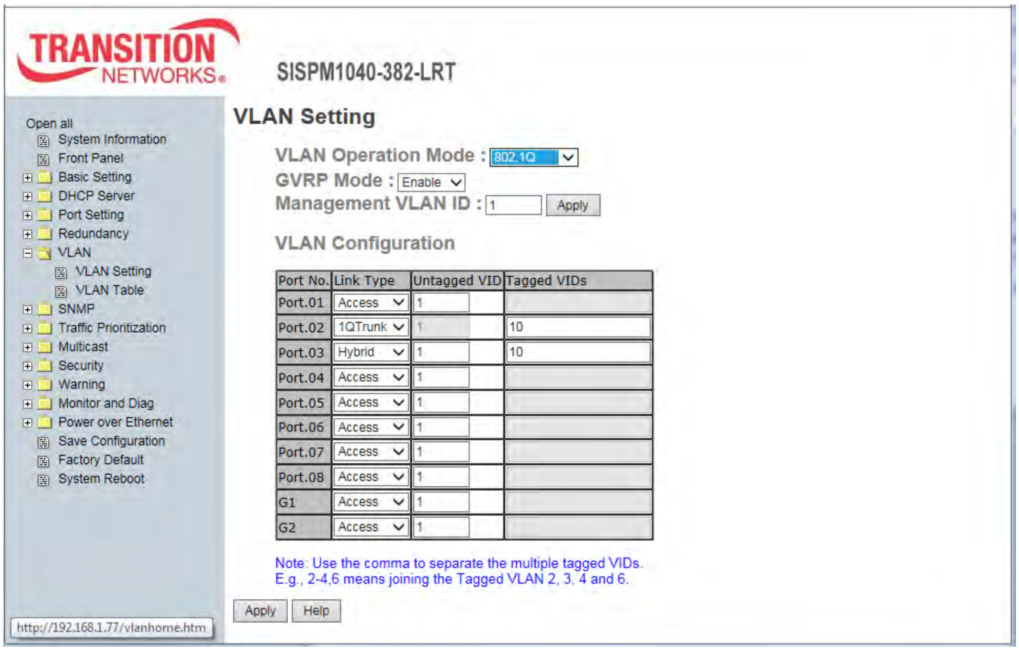
IEEE 802.1Q defines the operation of Virtual LAN (VLAN) Bridges that permit the definition, operation and administration of Virtual LAN topologies within a Bridged LAN infrastructure. The GARP (Generic Attribute Registration Protocol) VLAN Registration Protocol (GVRP) defines a GARP application that provides the 802.1Q-compliantVLAN pruning and dynamic VLAN creation on 802.1Q trunk ports. Refer to IEEE 802.1Q for details.

5.1.4.1 VLAN Setting - IEEE 802.1Q

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

You can create Tag-based VLAN, and enable or disable GVRP protocol. There are 256 VLAN groups to available. Enable 802.1Q VLAN, then 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.



SISPM1040-382-LRT

VLAN Setting

VLAN Operation Mode : 802.1Q

GVRP Mode : Enable

Management VLAN ID : 1

VLAN Configuration

Port No.	Link Type	Untagged VID	Tagged VIDs
Port.01	Access	1	
Port.02	1QTrunk	1	10
Port.03	Hybrid	1	10
Port.04	Access	1	
Port.05	Access	1	
Port.06	Access	1	
Port.07	Access	1	
Port.08	Access	1	
G1	Access	1	
G2	Access	1	

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

VLAN Setting – 802.1Q interface

Label	Description
VLAN Operation Mode	Select the VLAN operating mode: Disabled, Port Based, or **802.1Q** mode.
GVRP Mode	Enable or Disable the GVRP function.
Management VLAN ID	Management VLAN can provide the network administrator a secure VLAN to manage the switch. Only this VLAN can manage this switch. Zero means this function is disabled.
Port No.	Select the port to configure.
Link Type	At the dropdown, select one of the three link types supported: **Access** Link: the access link only supports an untagged VID. **1QTrunk** Link: the 1Q trunk link only supports multiple tagged VIDs. **Hybrid** Link: the hybrid link supports an untagged VID and multiple tagged VIDs.
Untagged VIDs	Set the port default VLAN ID for untagged devices that connect to the port. The range is 1 to 4094.
Tagged VIDs	Set the tagged VIDs to carry different VLAN frames to other switches. The switch supports 1~4094 and multiple VIDs.
Apply	Click "**Apply**" to set the configurations.

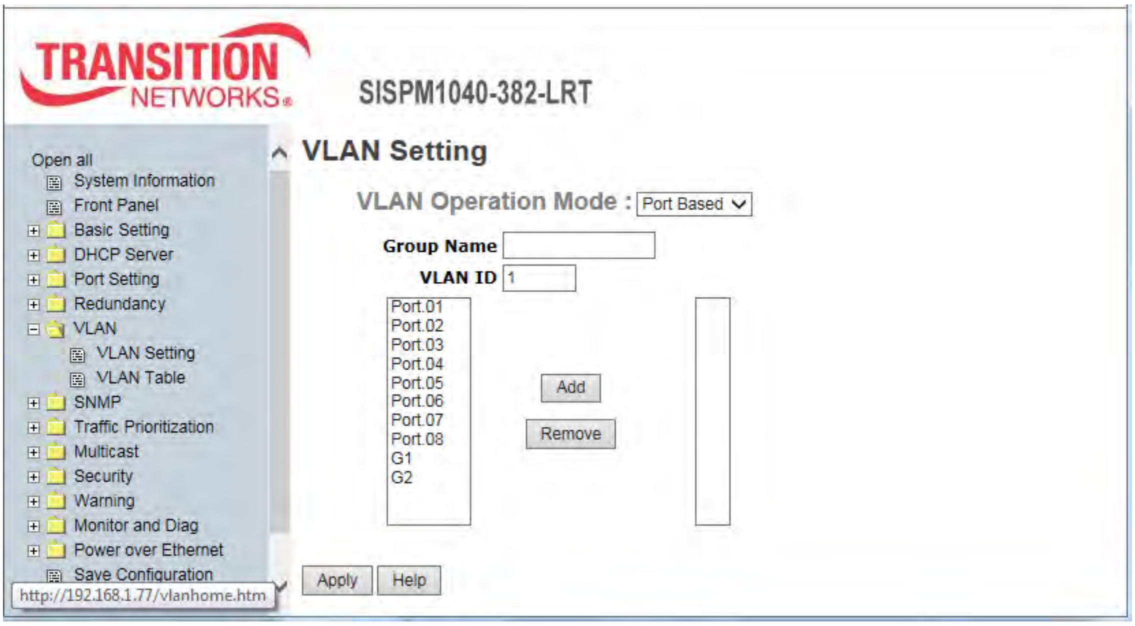
Note: Use the comma to separate multiple tagged VIDs (e.g.,, 2-4,6 means joining Tagged VLAN 2, 3, 4 and 6).

Note: ports with the same VID means they are in the same VLAN group.

VLAN Setting – Port Based

Packets only go to the 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, the VLAN-tagging is ignored.

From the default page, click the **Add** button to display the config page:



VLAN Setting

VLAN Operation Mode : Port Based

Group Name

VLAN ID 1

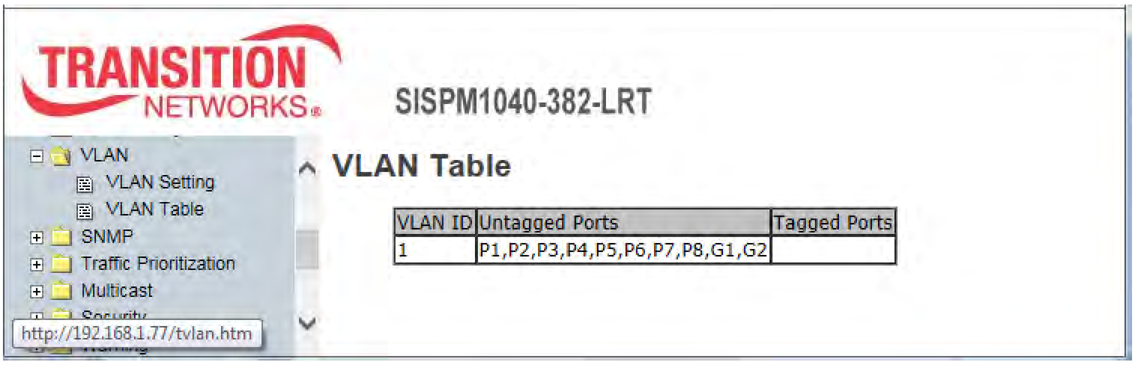
VLAN Configuration – Port Based interface

The following table describes the labels in this screen.

Label	Description
VLAN Operation Mode	Select the mode at the dropdown (**Disabled**, **Port Based**, or **802.1Q** mode).
Group Name	Enter the VLAN name.
VLAN ID	Specify the VLAN ID
Add	Click “Add” to enter VLAN add interface.
Edit	Click to edit the existing VLAN.
Delete	Click to delete the existing VLAN.
Help	Show the related help file.
Add	Select port to join the VLAN group.
Remove	Remove port from the VLAN group
Apply	Click “**Apply**” to set the configurations.
Help	Show help file.

5.1.4.2 VLAN Table

VLAN > VLAN Table displays the VLAN Table parameters: VLAN ID, Untagged Ports, and Tagged Ports.



VLAN Table

VLAN ID	Untagged Ports	Tagged Ports
1	P1,P2,P3,P4,P5,P6,P7,P8,G1,G2	

5.1.5 Traffic Prioritization

Traffic Prioritization includes three modes: port based, 802.1p/COS, and TOS/DSCP. Using the traffic prioritization function, you can classify the traffic into four classes for differential network applications. The SISPM1040-382-LRT 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 Type:

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.

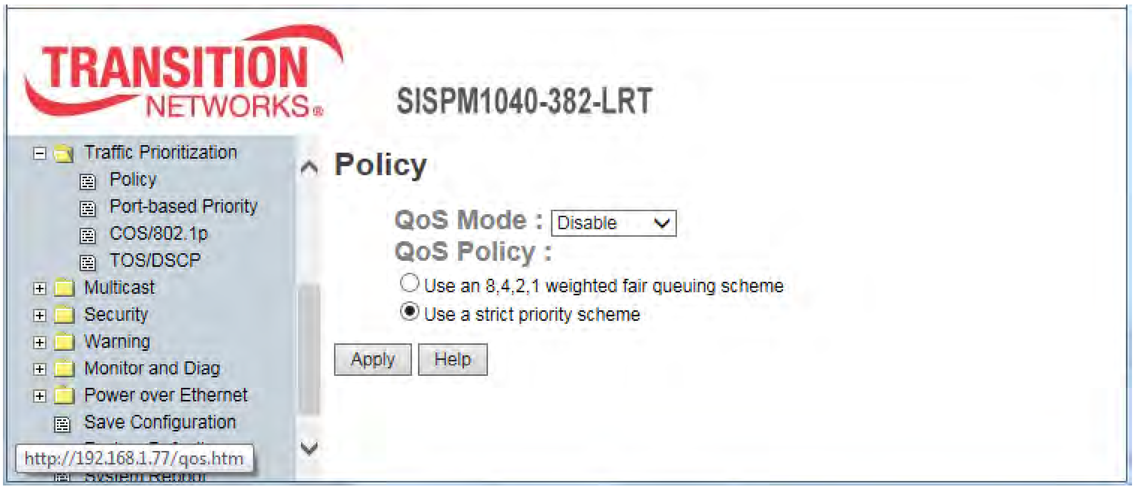
TOS first: the output priority is determined by COS and TOS, but TOS first.

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 value is supported 0~7.

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.

5.1.5.1 QoS Policy



Policy

QoS Mode : Disable

QoS Policy :

○ Use an 8,4,2,1 weighted fair queuing scheme

● Use a strict priority scheme

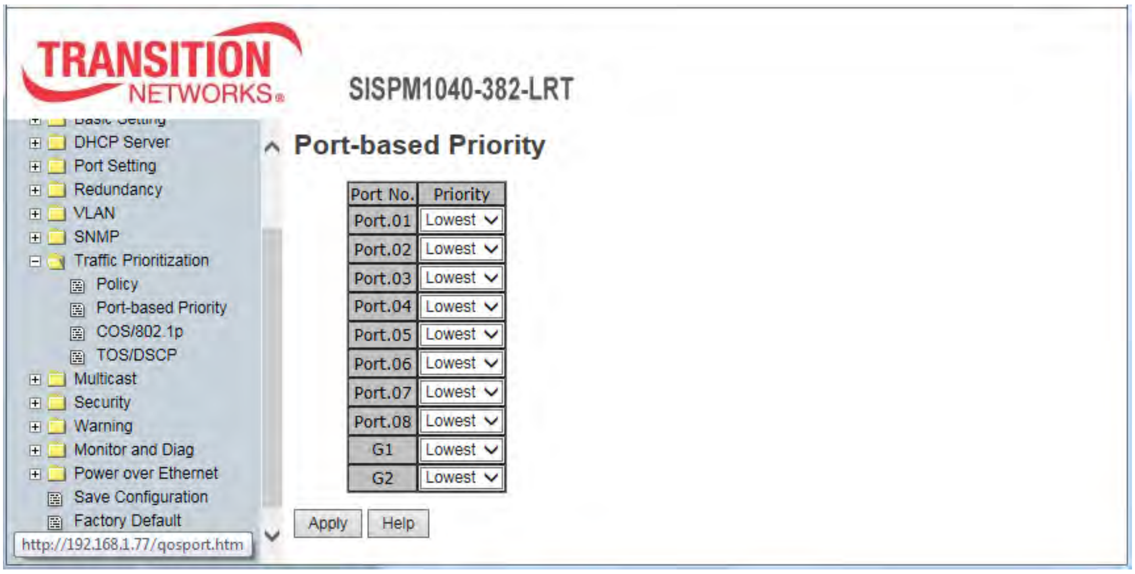
Traffic Prioritization interface

The following table describes the labels in this screen.

Label	Description
QOS Mode	**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	**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**: the packets in a higher queue will always be transmitted first until the higher queue is empty.
Apply	Click "**Apply**" to set the configuration settings.
Help	Show the related help file.

5.1.5.2 Port-based Priority

When Priority Type is set to Port-based, the output priority is determined by the ingress port.



Port-based Priority

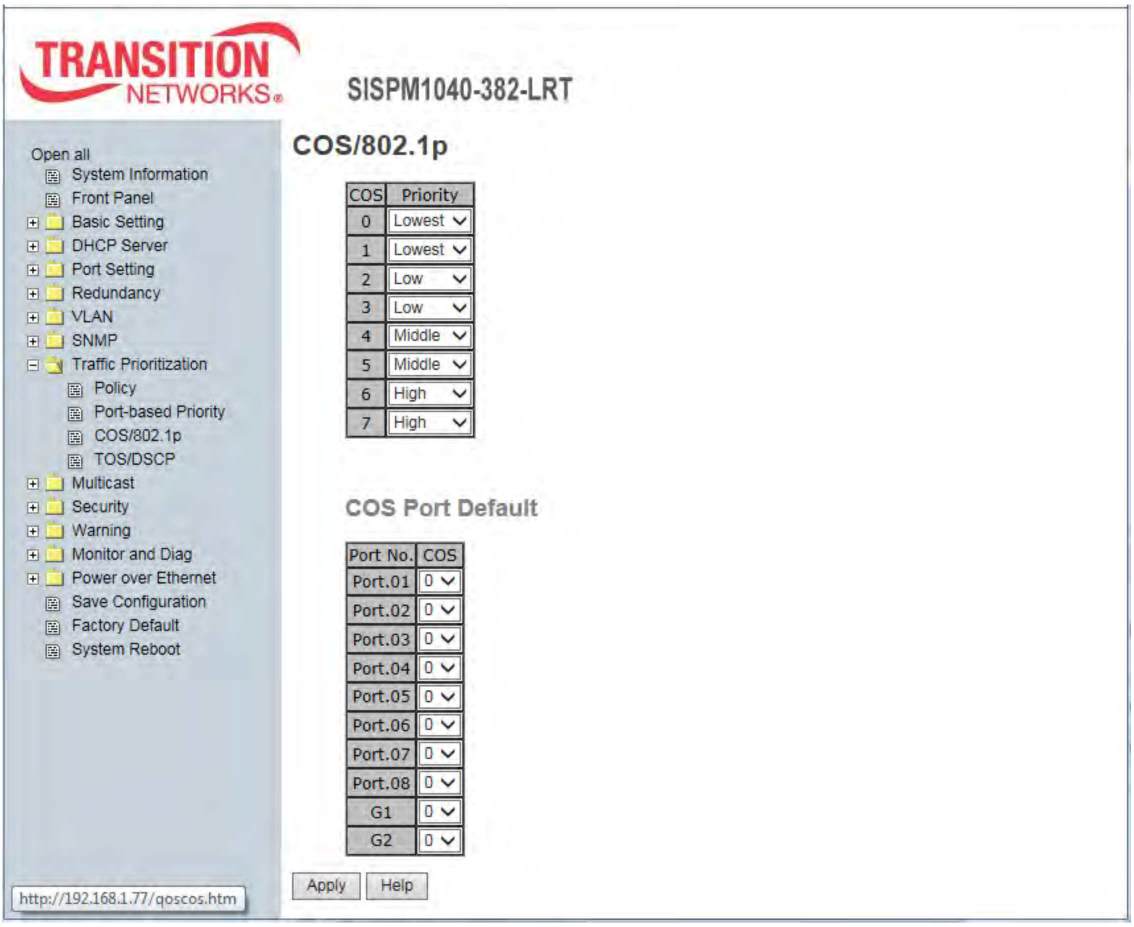
Port No.	Priority
Port.01	Lowest
Port.02	Lowest
Port.03	Lowest
Port.04	Lowest
Port.05	Lowest
Port.06	Lowest
Port.07	Lowest
Port.08	Lowest
G1	Lowest
G2	Lowest

Port-based Priority interface

The following table describes the labels in this screen.

Label	Description
Priority	Assign Port with a priority queue. Four priority queues can be assigned: High, Middle, Low, and Lowest.
Apply	Click "**Apply**" to set the configuration.
Help	Show help file.

5.1.5.3 COS/802.1p



COS/802.1p

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

COS Port Default

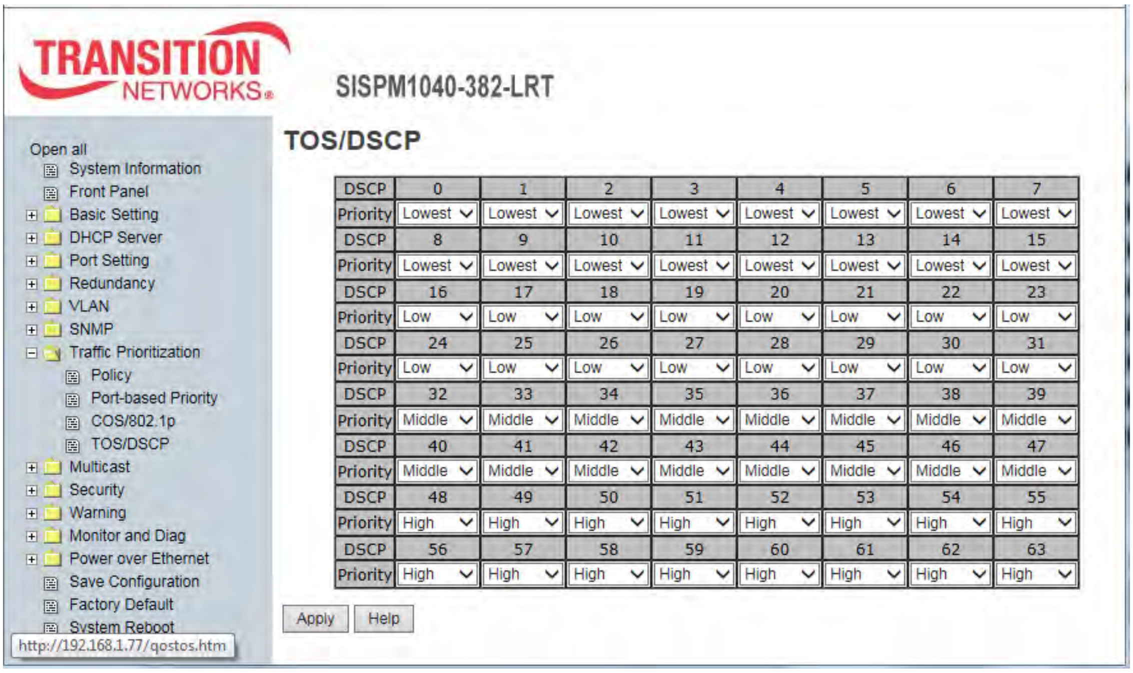
Port No.	COS
Port.01	0
Port.02	0
Port.03	0
Port.04	0
Port.05	0
Port.06	0
Port.07	0
Port.08	0
G1	0
G2	0

COS/802.1p interface

The following table describes the labels in this screen.

Label	Description
COS/802.1p	COS (Class Of Service) is well known as IEEE 802.1p. It describes that the output priority of a packet is determined by the user priority field in the 802.1Q VLAN tag. The priority values range from 0 to 7. The COS value maps to 4 priority queues: High, Middle, Low, and Lowest.
COS Port Default	When an ingress packet does not have a VLAN tag, a default priority value is determined by ingress port. At the dropdown, select 0-7.
Apply	Click "**Apply**" to set the configurations.
Help	Show help file.

5.1.5.4 TOS/DSCP



TOS/DSCP

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

TOS/DSCP interface

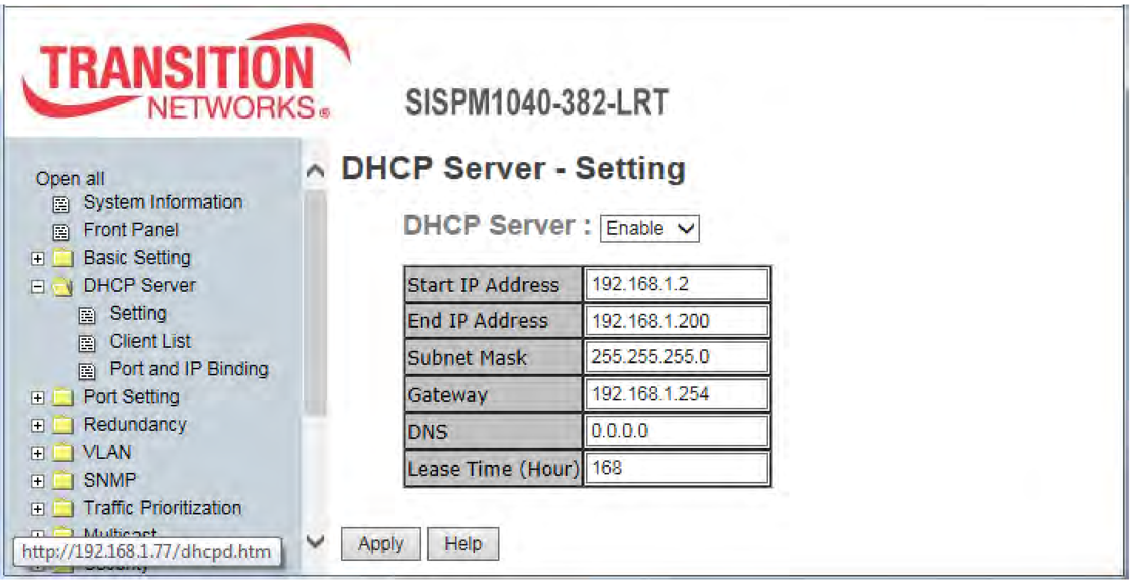
The following table describes the labels in this screen.

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 has values from 0 to 63. DSCP value maps to 4 priority queues: High, Middle, Low, and Lowest.
Apply	Click "**Apply**" to set the configurations.
Help	Show help file.

5.1.6 DHCP Server

5.1.6.1 DHCP Server – Setting

The system can provide a DHCP server function. If enabled, the switch will be a DHCP server.



DHCP Server - Setting

DHCP Server : Enable

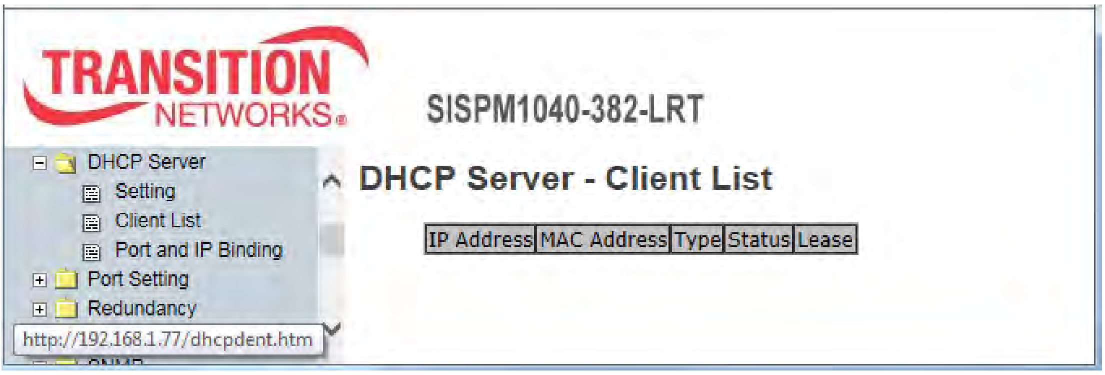
Start IP Address	192.168.1.2
End IP Address	192.168.1.200
Subnet Mask	255.255.255.0
Gateway	192.168.1.254
DNS	0.0.0.0
Lease Time (Hour)	168

DHCP Server Configuration interface

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

5.1.6.2 DHCP Server – Client List

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



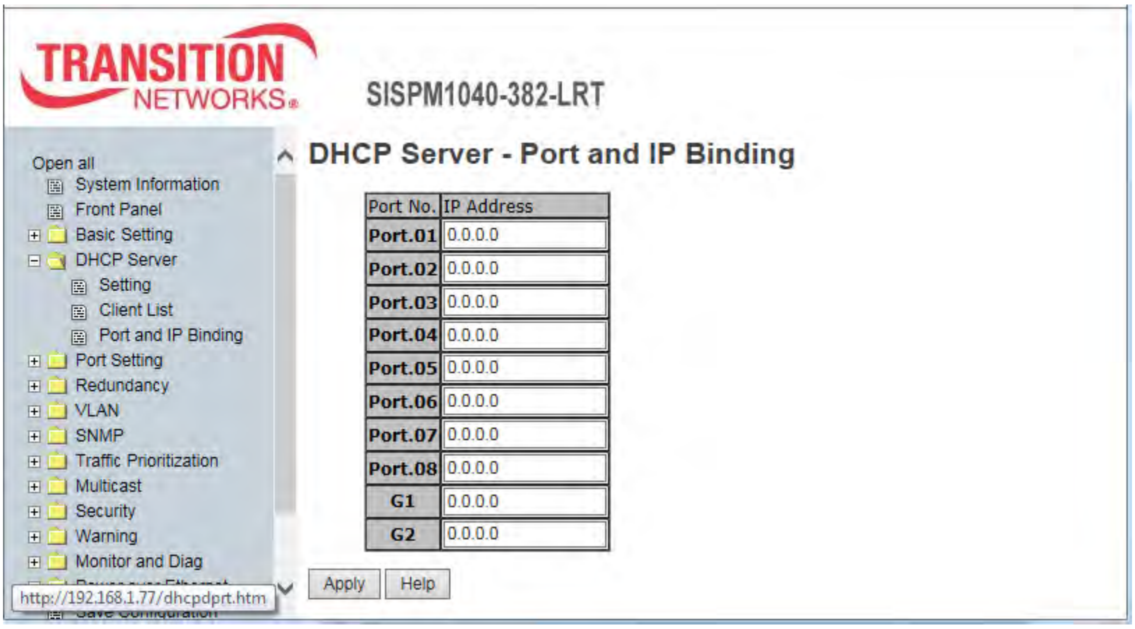
DHCP Server - Client List

IP Address	MAC Address	Type	Status	Lease

DHCP Server Client Entries interface

5.1.6.3 DHCP Server – Port and IP bindings

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 to the connected device.



DHCP Server - Port and IP Binding

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
Port.08	0.0.0.0
G1	0.0.0.0
G2	0.0.0.0

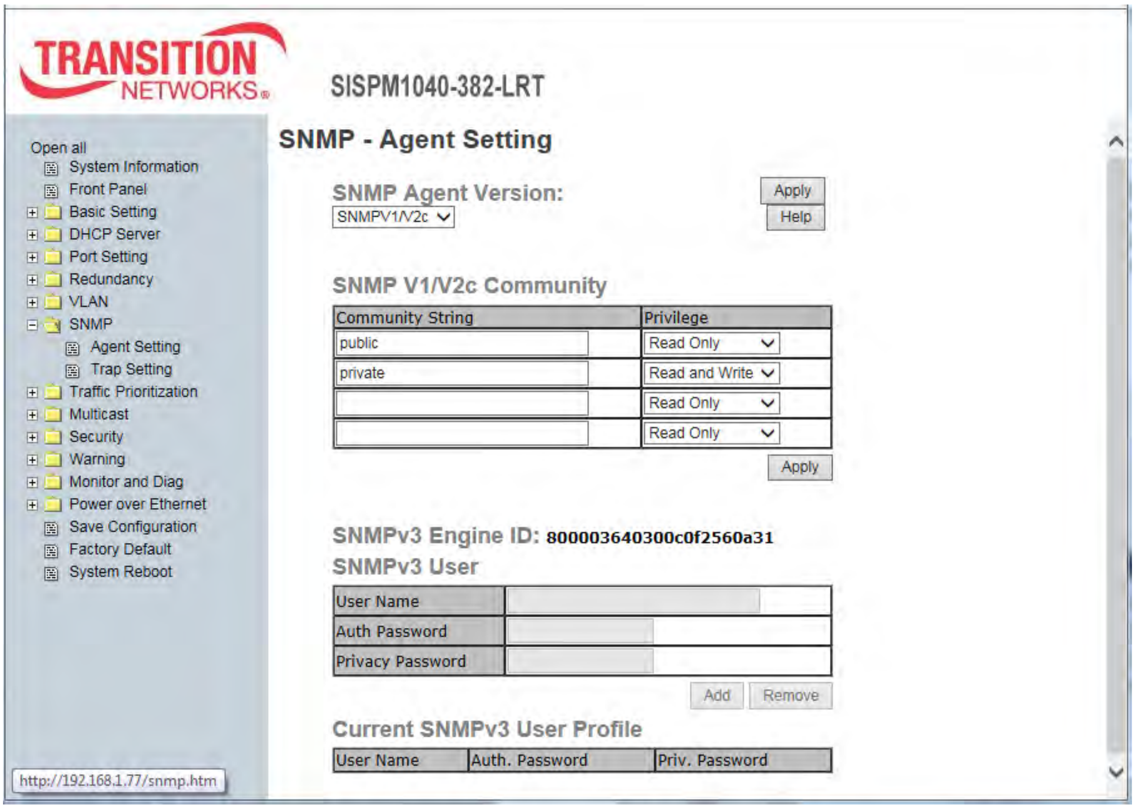
DHCP Server Port and IP Binding interface

5.1.7 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.

5.1.7.1 SNMP – Agent Setting

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



SNMP - Agent Setting

SNMP Agent Version: SNMPV1/V2c

SNMP V1/V2c Community

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

SNMPv3 Engine ID: 800003640300c0f2560a31

SNMPv3 User

User Name	
Auth Password	
Privacy Password	

Current SNMPv3 User Profile

User Name	Auth. Password	Priv. Password

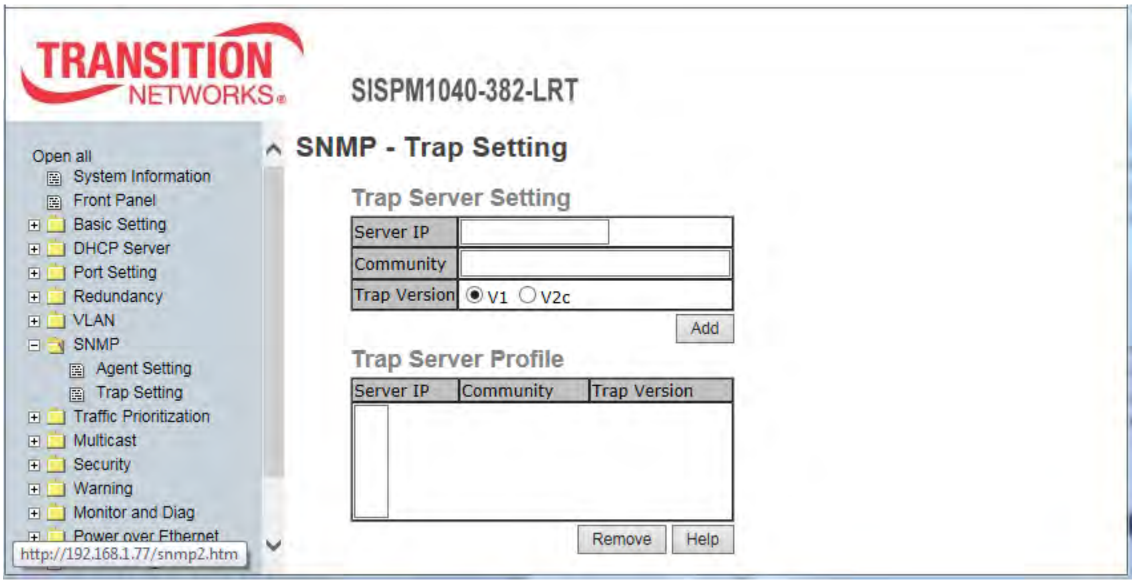
SNMP – Agent Setting interface

Label	Description
SNMP Agent Version	The switch supports SNMP V1/V2c, and SNMP V3. The SNMP V1/ V2c agent use a community string match for authentication, which means SNMP servers access objects with read-only or read/write permissions with the community default string public/private. SNMP V3 requires an authentication level of MD5 or DES to encrypt data to enhance data security.
SNMP V1/V2c Community	SNMP Community should be set for SNMP V1/V2c. Four sets of "Community String/Privilege" are supported. Each Community String is maximum 32 characters. Keep empty to remove this Community string.

SNMPv3 Engine ID	The SNMPv3 Engine ID in the format 800003640300c0f2560a31.
SNMP v3 User	If SNMP V3 agent is selected, the SNMPv3 user profile should be set for authentication. The User Name is required. The Auth Password is encrypted by MD5 and the Privacy Password which is encrypted by DES. There are maximum 8 sets of SNMPv3 User and maximum 16 characters in user name, and password. When SNMP V3 agent is selected, you can: 1. Enter the SNMPv3 user name only. 2. Enter the SNMPv3 user name and Auth Password. 3. Enter the SNMPv3 user name, Auth Password and Privacy Password (which can be different than the Auth Password). To remove a current user profile: 1. Enter the SNMPv3 user name you want to remove. 2. Click the "Remove" button.
Current SNMPv3 User Profile	Displays a table with the User Name, Auth. Password, and Priv. Password.
Apply	Click to make the settings.
Add	Click to add an instance.
Remove	Click to delete the selected instance.

5.1.7.2 SNMP –Trap Setting

A trap manager is a management server that receives traps, the system alerts generated by the switch. If no trap manager is defined, no traps will be issued. Create a trap manager by entering the IP address of the SNMP trap receiving server and a community string. To define management systems, enter the server's IP address, SNMP community strings and select the SNMP version.



SNMP - Trap Setting

Trap Server Setting

Server IP	
Community	
Trap Version	● V1 ○ V2c

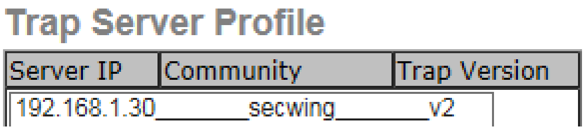
Add

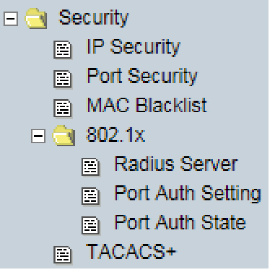
Trap Server Profile

Server IP	Community	Trap Version

Remove Help

SNMP –Trap Setting interface

Label	Description
Server IP	The server IP address to receive Traps.
Community	The Community for authentication.
Trap Version	Trap Version supports V1 and V2c.
Trap Server Profile	Displays all SNMP Trap servers configured:  Trap Server Profile Server IP: 192.168.1.30 Community: secwing Trap Version: v2
Add	Add a trap server profile.
Remove	Remove a selected trap server profile.
Help	Show help file.



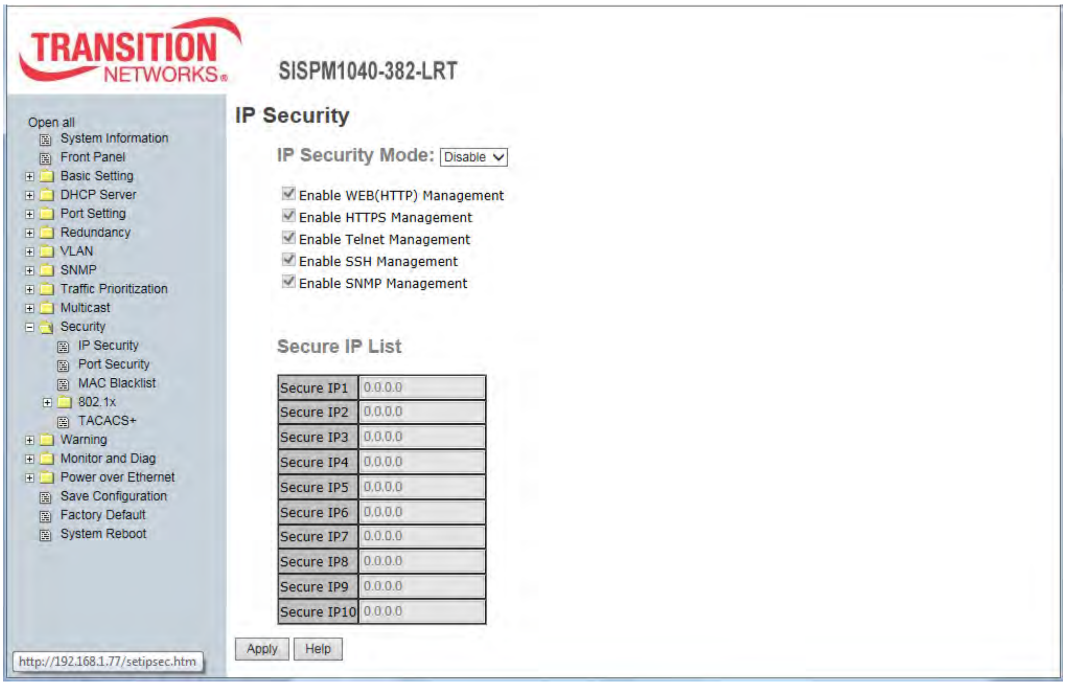
5.1.8 Security

Five useful functions that can enhance the security of the switch:

IP Security, Port Security, MAC Blacklist, 802.1x protocol, and TACACS+.

5.1.8.1 IP Security

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



IP Security

IP Security Mode: Disable

☑ Enable WEB(HTTP) Management
☑ Enable HTTPS Management
☑ Enable Telnet Management
☑ Enable SSH Management
☑ Enable SNMP Management

Secure IP List

Secure IP1	0.0.0.0
Secure IP2	0.0.0.0
Secure IP3	0.0.0.0
Secure IP4	0.0.0.0
Secure IP5	0.0.0.0
Secure IP6	0.0.0.0
Secure IP7	0.0.0.0
Secure IP8	0.0.0.0
Secure IP9	0.0.0.0
Secure IP10	0.0.0.0

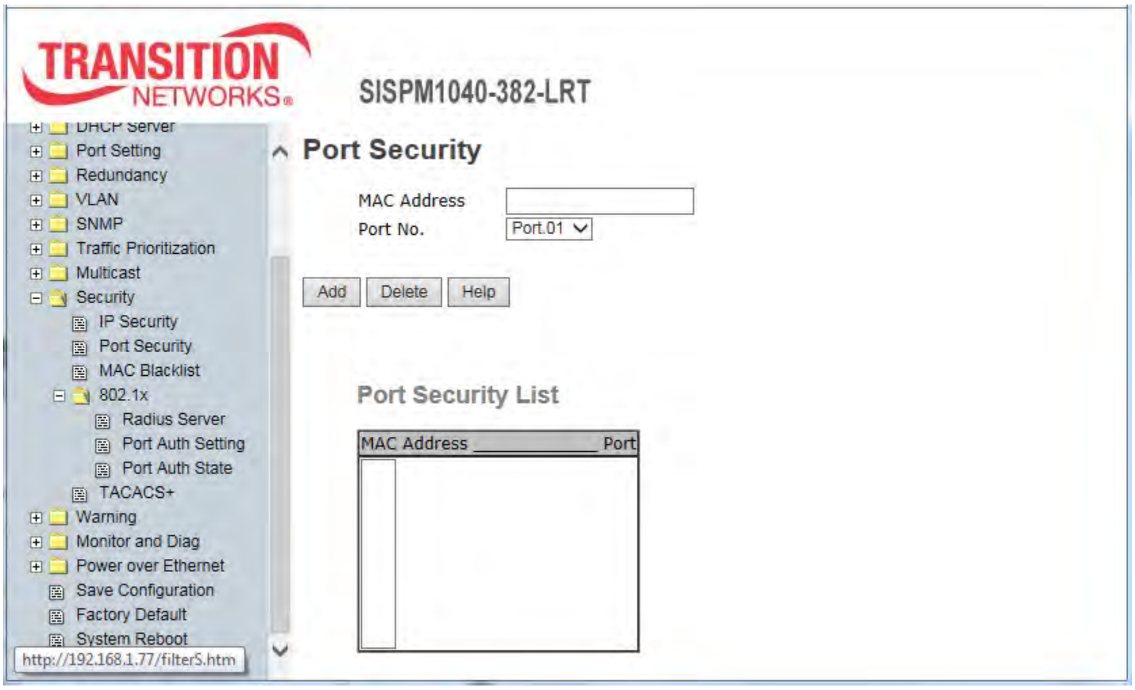
IP Security interface

Label	Description
IP Security Mode	Enable/Disable the IP security function.
Enable WEB(HTTP) Management	Enable/Disable remote management from a Web browser. Check the box to enable WEB Management.
Enable HTTPS Management	Enable/Disable remote management from a secure Web browser. Check the box to enable Secure HTTP Web Management.
Enable Telnet Management	Enable/Disable remote management from Telnet. Check the box to enable Telnet Management.
Enable SSH Management	Enable/Disable remote management via SSH (Secure Shell). Check the box to enable SSH Management.

Enable SNMP Management	Enable/Disable remote management from SNMP. Check the box to enable SNMP Management.
Secure IP List	Assign up to 10 secure IP addresses. Only these IP addresses will be able to manage the switch after clicking “Apply”.
Apply	Click “**Apply**” to set the configurations.
Help	Show help file.

5.1.8.2 Port Security

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



Port Security

MAC Address

Port No. Port.01

Port Security List

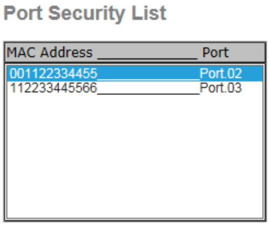
MAC Address	Port

Port Security interface

Label	Description
MAC Address	Input MAC Address to a specific port.
Port No.	Select port of switch.
Add	Add an entry of MAC and port information.
Delete	Delete the entry.
Help	Show help file.

To add a static MAC address:

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


Port Security List

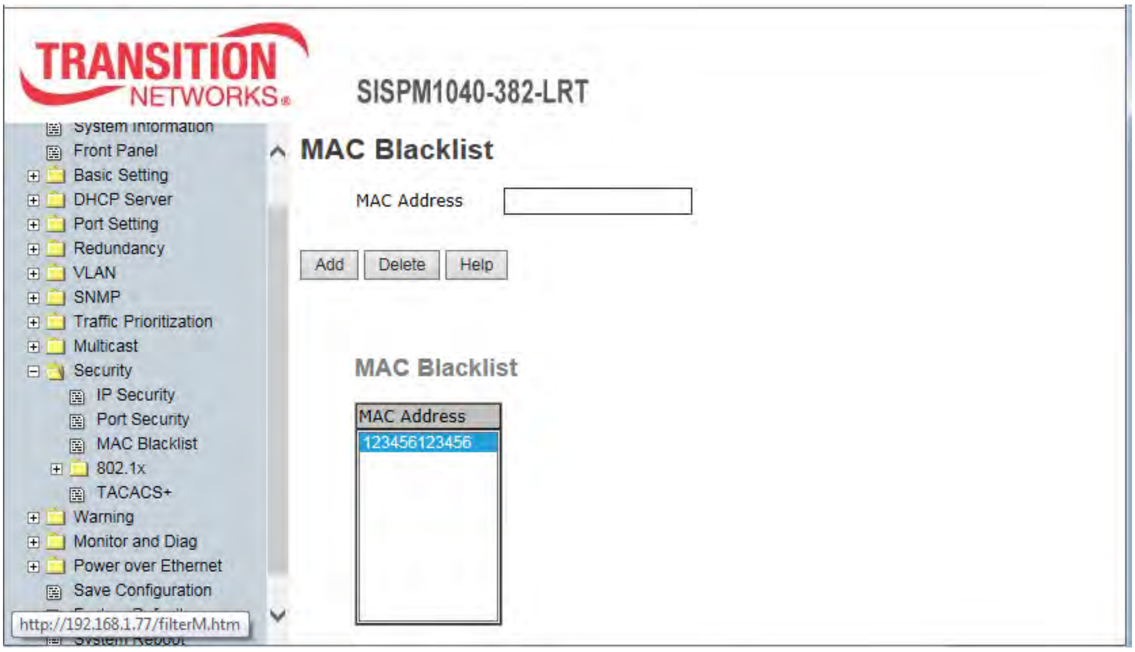
MAC Address	Port
001122334455	Port.02
112233445566	Port.03

To delete a static MAC address:

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

5.1.8.3 MAC Blacklist

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



MAC Blacklist interface

Label	Description
MAC Address	Enter a MAC Address to add to the MAC Blacklist.
Add	Add an entry to Blacklist table.
Delete	Delete the entry.
Help	Show help file.

To add a MAC address filter:

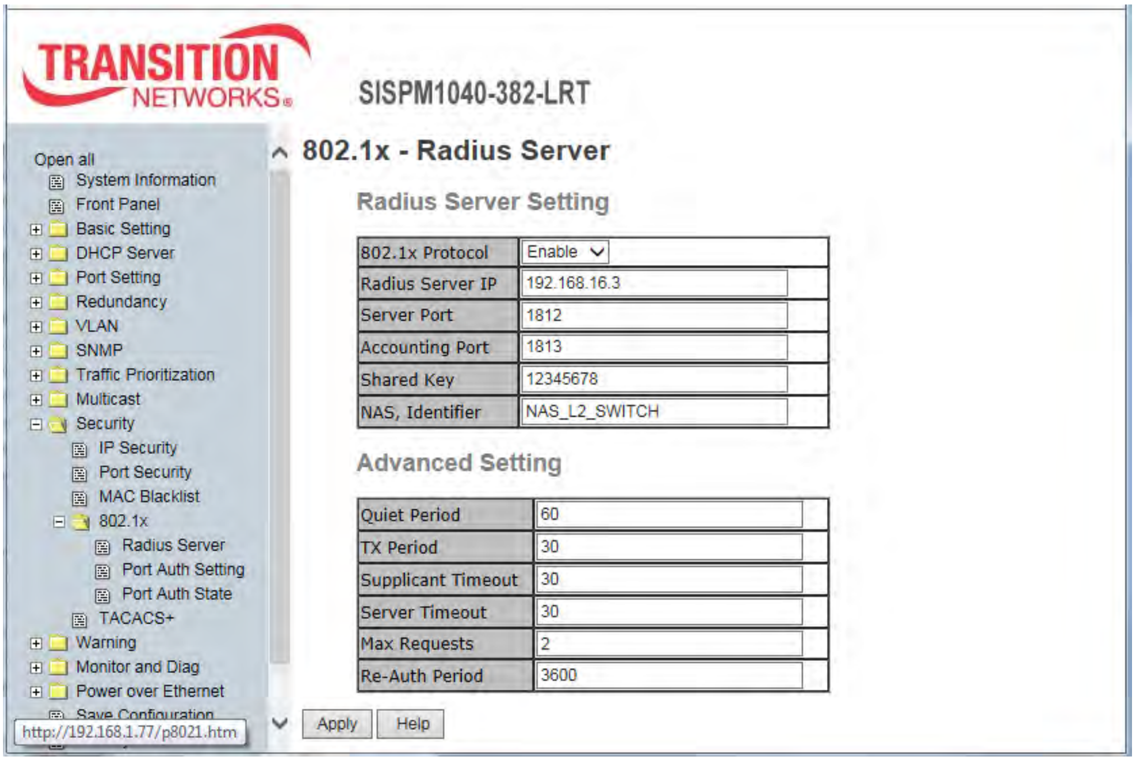
1. In the MAC Address box, enter a MAC address (e.g. 001122334455).
2. Click the "Add" button.

To delete a filter MAC address:

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

5.1.8.4 802.1x Radius Server

IEEE 802.1x makes use of the physical access characteristics of IEEE802 LAN infrastructures in order to provide a means of authenticating and authorizing devices attached to a LAN port that has point-to-point connection characteristics, and of preventing access to that port in cases in which the authentication and authorization process fails. Refer to IEEE 802.1X - Port Based Network Access Control.



802.1x - Radius Server

Radius Server Setting

802.1x Protocol	Enable
Radius Server IP	192.168.16.3
Server Port	1812
Accounting Port	1813
Shared Key	12345678
NAS, Identifier	NAS_L2_SWITCH

Advanced Setting

Quiet Period	60
TX Period	30
Supplicant Timeout	30
Server Timeout	30
Max Requests	2
Re-Auth Period	3600

802.1x Radius Server interface

Note: firmware version v1.32 provided a fix for TLS v1.1 and v1.2 vulnerability for secure communications applications.Note that EAP MD5 must be set as the default authentication method on any Radius server. This applies to Radius servers such as FreeRadius which may accept MD5 and have TLS as the default setting in EAP configuration.

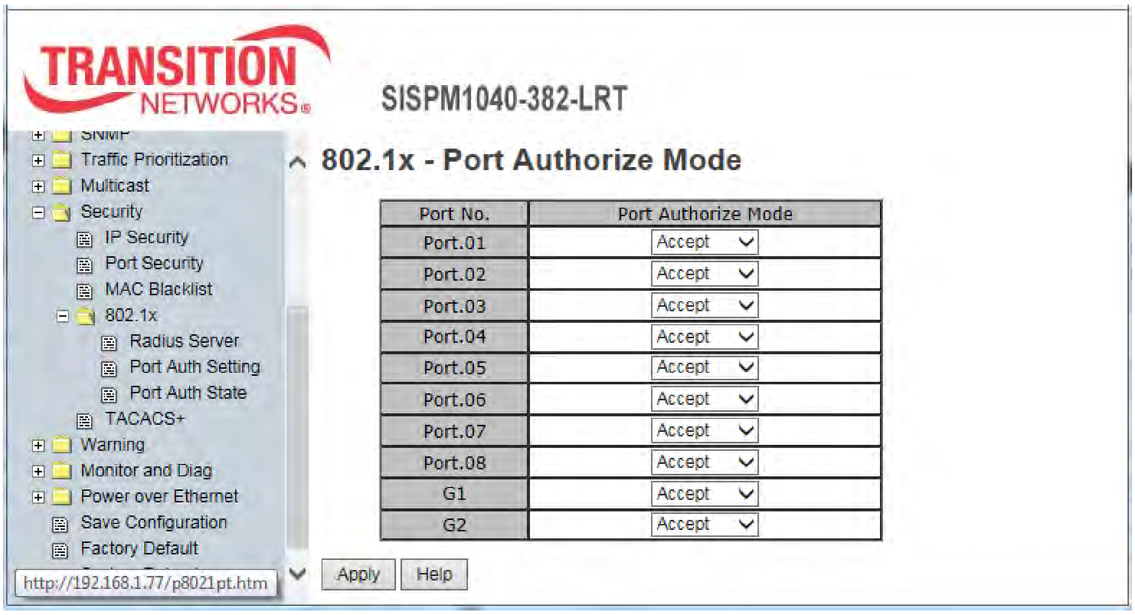
The RADIUS parameters are described in the table below. See "Appendix A - Radius Server and Switch Settings" for more setup details.

Label	Description
802.1x Protocol	Enable or Disable 802.1X Radius Server functionality.
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 port number used by the authentication server to retrieve accounting information.
Shared Key	A key shared between this switch and authentication server.
NAS, Identifier	A string used to identify this switch.
Advanced Setting	
Quiet Period	Set the time interval between authentication failure and the start of a new authentication attempt. During this period of time it will not attempt to acquire a supplicant. The default time is 60 seconds.
Tx Period	Set the time that the switch can wait for response to an EAP request/identity frame from the client before resending the request. This is the period of time to transmit an EAPOL PDU. The default is 30 seconds.
Supplicant Timeout	Set the period of time the switch waits for a supplicant response to an EAP request. The timeout conditions in the exchanges between the supplicant and authentication server. The default is 30 seconds.
Server Timeout	Set the period of time the switch waits for a Radius server response to an authentication request. The timeout conditions in the exchanges between the authenticator and authentication server. The default is 30 seconds.
Max Requests	Set the maximum number of times to retry sending packets to the supplicant. This is the number of reauthentication attempts that are permitted before the specific port becomes unauthorized. The default is 2 times.
Re-Auth Period	Set the period of time after which clients connected must be re-authenticated. Enter a nonzero number of seconds between periodic reauthentication of the supplications. The default is 3600 seconds.
Apply	Click "**Apply**" to set the configurations.
Help	Show help file.

802.1x-Port Authorized Setting

Set the 802.1x authorized mode of each port.



802.1x - Port Authorize Mode

Port No.	Port Authorize Mode
Port.01	Accept
Port.02	Accept
Port.03	Accept
Port.04	Accept
Port.05	Accept
Port.06	Accept
Port.07	Accept
Port.08	Accept
G1	Accept
G2	Accept

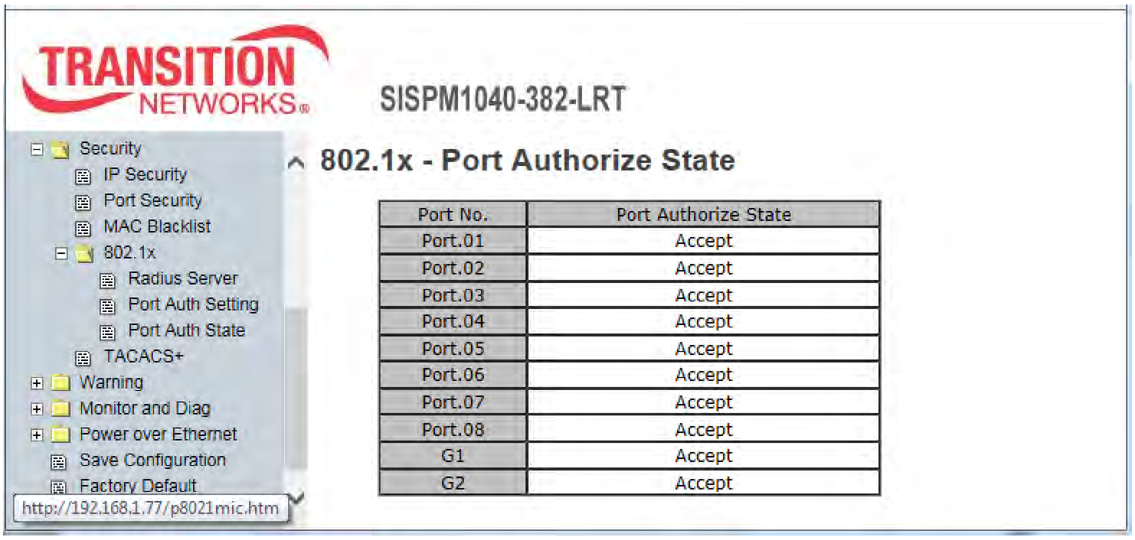
802.1x Port Authorize interface

The following table describes the labels in this screen.

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

802.1x-Port Authorized State

Displays the 802.1x port authorized state. See the parameter descriptions above.



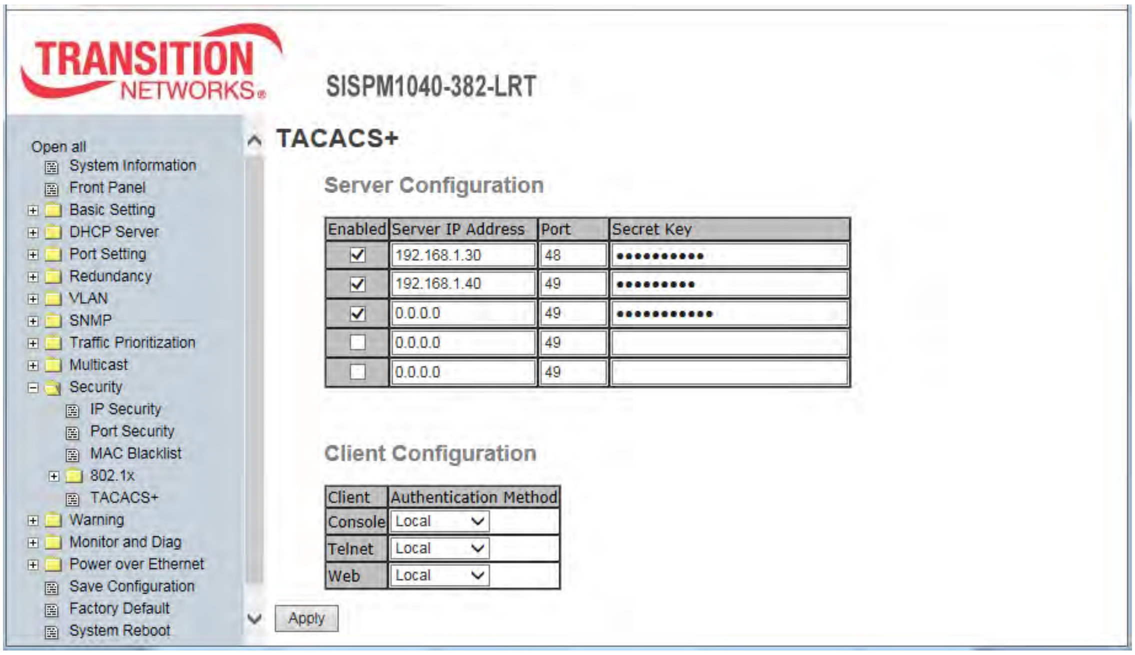
802.1x - Port Authorize State

Port No.	Port Authorize State
Port.01	Accept
Port.02	Accept
Port.03	Accept
Port.04	Accept
Port.05	Accept
Port.06	Accept
Port.07	Accept
Port.08	Accept
G1	Accept
G2	Accept

802.1x Port Authorize State interface

5.1.8.5 TACACS+

This page lets you configure TACACS+ Server and Client authentication parameters.



TACACS+

Server Configuration

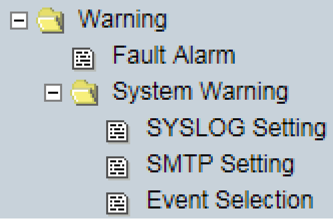
Enabled	Server IP Address	Port	Secret Key
☑	192.168.1.30	48	●●●●●●●●●●●
☑	192.168.1.40	49	●●●●●●●●●●
☑	0.0.0.0	49	●●●●●●●●●●●●●
□	0.0.0.0	49	
□	0.0.0.0	49	

Client Configuration

Client	Authentication Method
Console	Local
Telnet	Local
Web	Local

TACACS+ interface

Label	Description
Server Configuration	
Enabled	Check the box to enable each TACACS+ Server instance. Up to five TACACS+ Servers can be configured.
Server IP Address	Enter the TACACS+ Server IP address.
Port	Enter the TACACS+ Server UDP port number. The default is commonly-used port # 48 or 49.
Secret Key	Enter the auth secret key for the TACACS+ Server.
Client Configuration	
Client	For each client (Console, Telnet , Web) select an authentication method.
Authentication Method	At the dropdown, select either **Local** or **TACACS+** as the method for TACACS+ user authentication.
Apply	Click “Apply” to set the configurations.



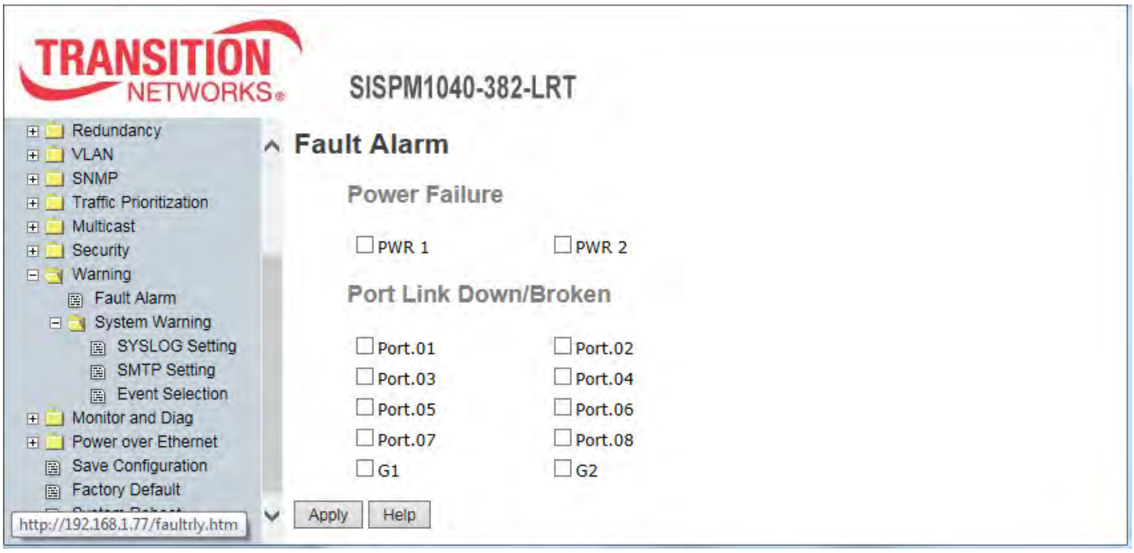
5.1.9 Warning

The Warning function is a very important tool for managing the switch. You can manage the switch by SYSLOG, SMTP (e-mail), and Fault Alarm.

Warnings help you to monitor the switch status from a remote site. When events occur, the warning message is sent to your designated server, E-MAIL, or relay fault switch panel. System alarm supports two warning modes: SYSLOG and 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.



Fault Alarm

Power Failure

□ PWR 1 □ PWR 2

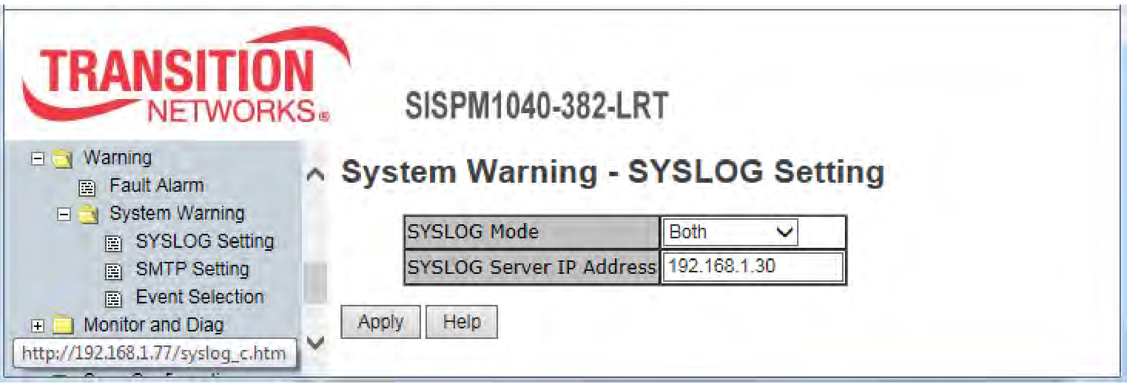
Port Link Down/Broken

□ Port.01 □ Port.02
□ Port.03 □ Port.04
□ Port.05 □ Port.06
□ Port.07 □ Port.08
□ G1 □ G2

Label	Description
Power Failure	Fault alarm when any selected power failure. This switch support dual power inputs. Check the box for PWR 1 and/or PWR 2.
Port Link Down/Broken	Fault alarm when any selected port link down or broken. Check the box for Port.01 - Port.08, G1, and/or G2.
Apply	Click “**Apply**” to set the configurations.
Help	Show help file.

System Warning – SYSLOG Setting

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



System Warning - SYSLOG Setting

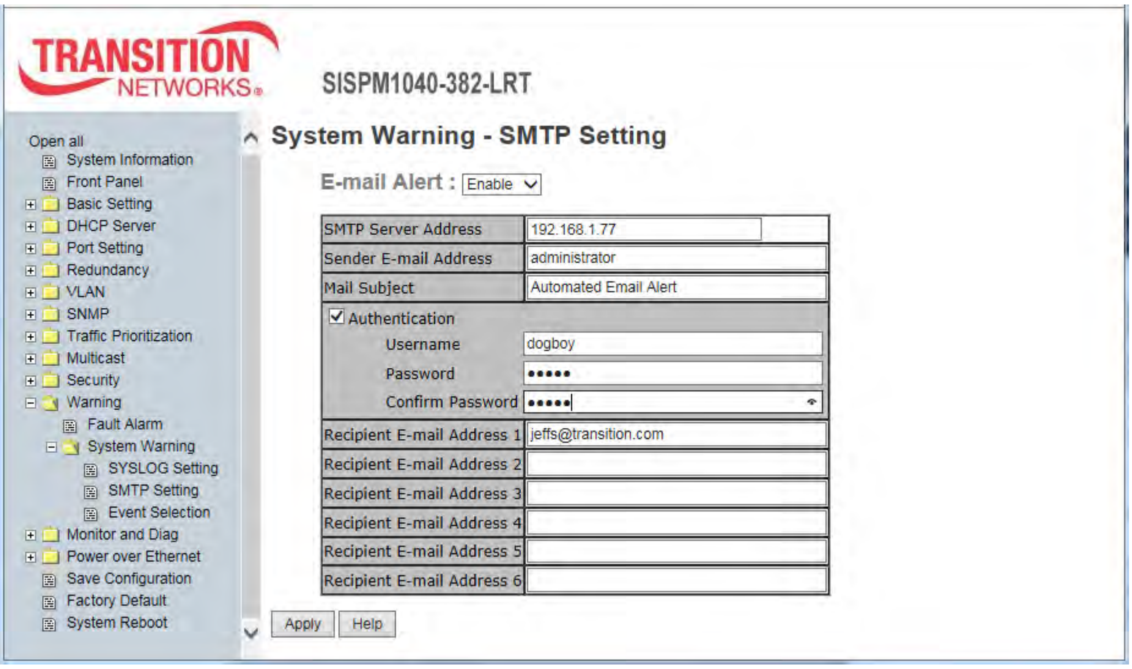
SYSLOG Mode	Both
SYSLOG Server IP Address	192.168.1.30

System Warning – SYSLOG Setting interface

Label	Description
Syslog Mode	**Disable:** disable SYSLOG. **Client Only:** log to local system. **Server Only:** log to a remote SYSLOG server. **Both:** log to both of local and remote server.
SYSLOG Server IP Address	The remote SYSLOG Server IP address.
Apply	Click “**Apply**” to set the configurations.
Help	Show help file.

System Warning – SMTP Setting

SMTP (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

E-mail Alert : Enable

SMTP Server Address	192.168.1.77
Sender E-mail Address	administrator
Mail Subject	Automated Email Alert
☑ Authentication	
Username	dogboy
Password	•••••
Confirm Password	•••••
Recipient E-mail Address 1	jeffs@transition.com
Recipient E-mail Address 2	
Recipient E-mail Address 3	
Recipient E-mail Address 4	
Recipient E-mail Address 5	
Recipient E-mail Address 6	

System Warning – SMTP Setting interface

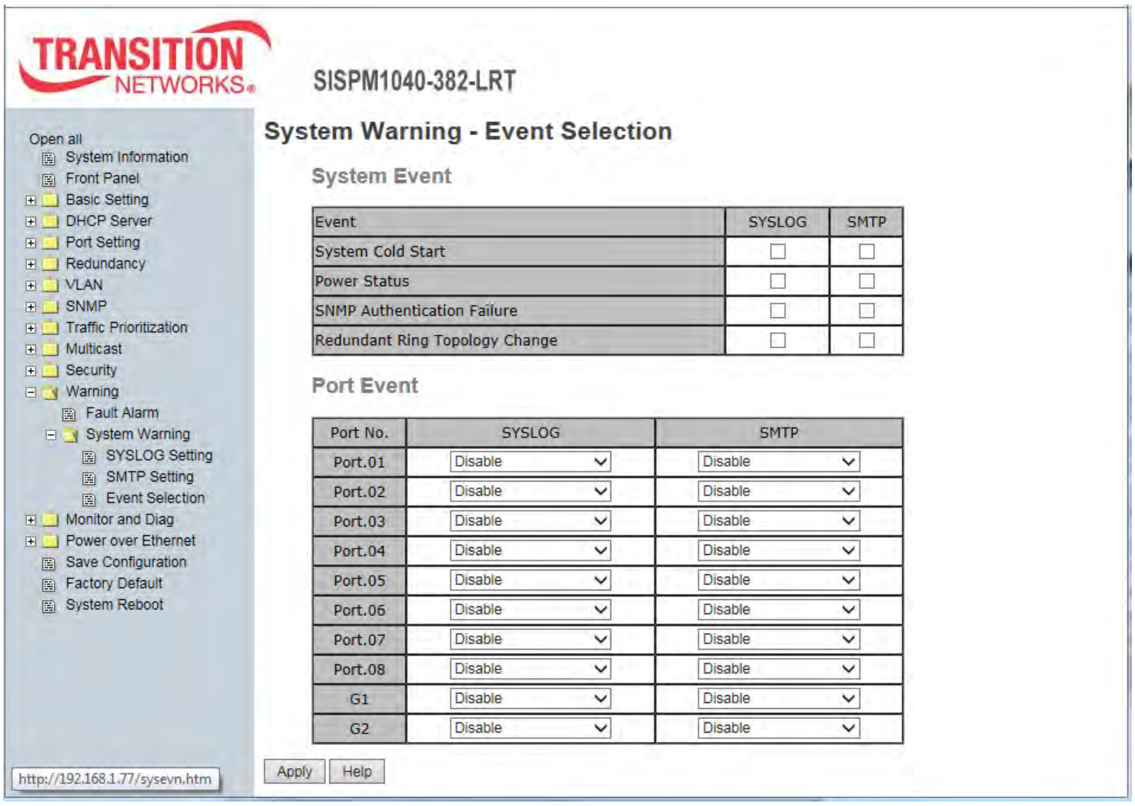
Label	Description
E-mail Alert	Enable/Disable transmission system warning events by e-mail.
Sender E-mail Address	Enter the mail server address.
Mail Subject	The Subject of the mail (e.g., Automated Email Alert).
Sender	Set up the email account to send the alert.
Authentication	Check the box if the SMTP server needs authentication; enter: **Username:** the authentication username. **Password:** the authentication password. **Confirm Password:** re-enter password.
Recipient E-mail Address 1 - 6	The recipient's E-mail address. Up to six e-mail recipients are 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 the system event warning method you want.

Note that the checkbox can not be checked when SYSLOG or SMTP is disabled.



System Warning - Event Selection

System Event

Event	SYSLOG	SMTP
System Cold Start	□	□
Power Status	□	□
SNMP Authentication Failure	□	□
Redundant Ring Topology Change	□	□

Port Event

Port No.	SYSLOG	SMTP
Port.01	Disable	Disable
Port.02	Disable	Disable
Port.03	Disable	Disable
Port.04	Disable	Disable
Port.05	Disable	Disable
Port.06	Disable	Disable
Port.07	Disable	Disable
Port.08	Disable	Disable
G1	Disable	Disable
G2	Disable	Disable

System Warning – Event Selection interface

Label	Description
System Cold Start	Issue a log event when the device executes a cold start.
Power Status	Issue an alert when a power up or down is detected.
SNMP Authentication Failure	Issue an alert when there is a SNMP authentication failure.
Redundant Ring Topology Change	Issue an alert when a Redundant Ring topology change is detected.
Port Event	At the dropdown, select the action to be taken when an event occurs: Disable, Link Up, Link Down, Link Up & Link Down.
Apply	Click "**Apply**" to set the configurations.

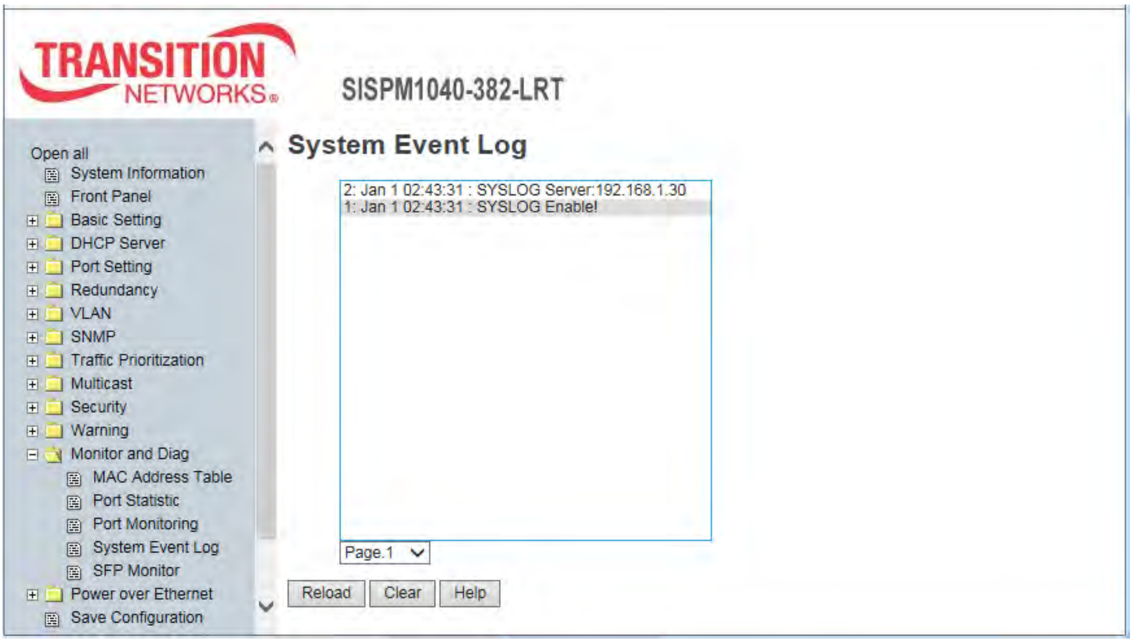
5.1.10 Monitor and Diag

5.1.10.1 System Event Log

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

Click the "Reload" button to get the newest event logs and refresh this page.

Click the "Clear" button to clear all logs in system.



```
2: Jan 1 02:43:31 : SYSLOG Server:192.168.1.30
1: Jan 1 02:43:31 : SYSLOG Enable!
```

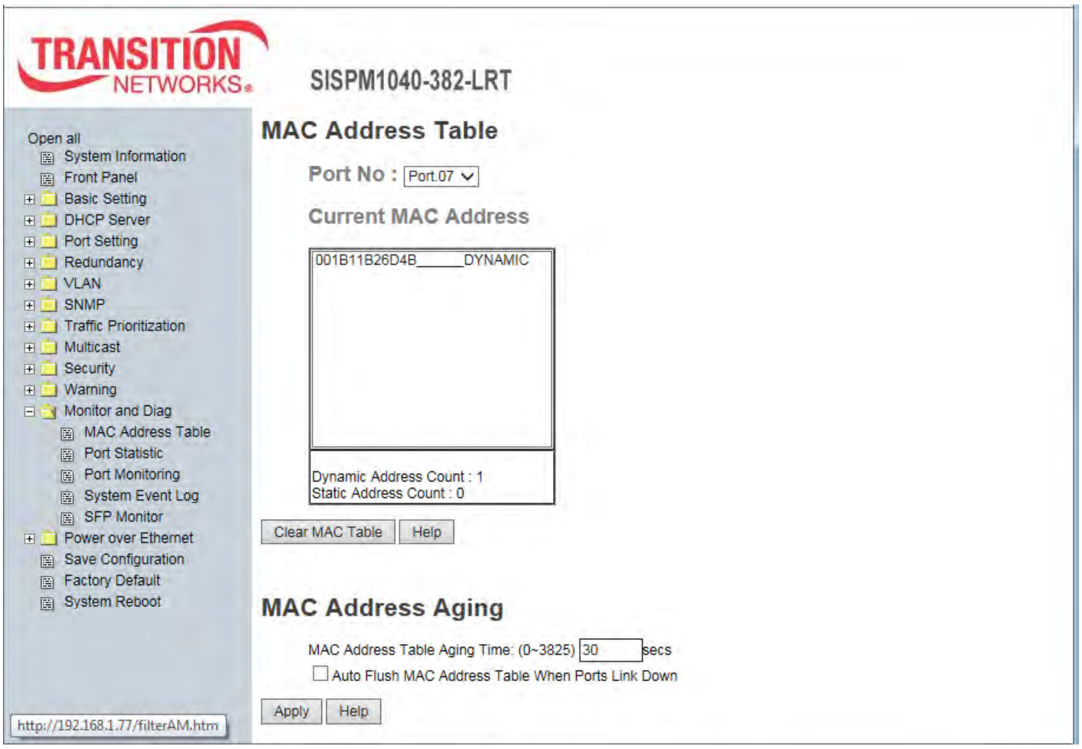
System Event Log interface

Label	Description
Page	At the dropdown, select which log page to display.
Reload	Click to display the newest event logs and refresh this page.
Clear	Click to clear the log table.
Help	Show help file.

5.1.10.2 MAC Address Table

Refer to IEEE 802.1 D Section 7.9. The MAC Address Table is a filtering database that supports queries by the Forwarding Process, to determine 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

Port No : Port.07

Current MAC Address

001B11B26D4B_____DYNAMIC

Dynamic Address Count : 1
Static Address Count : 0

MAC Address Aging

MAC Address Table Aging Time: (0~3825) 30 secs

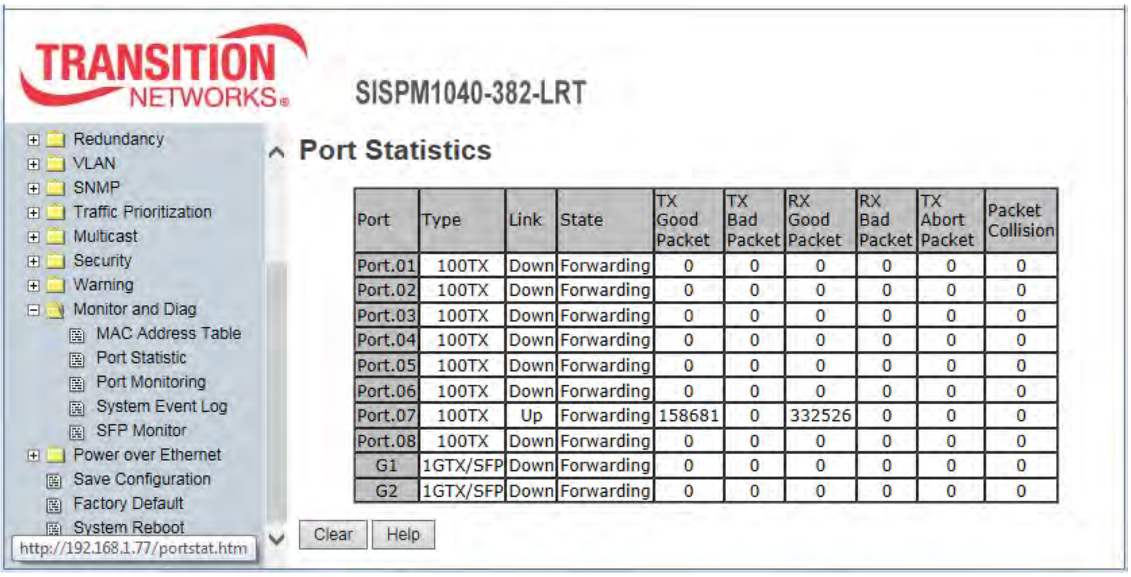
□ Auto Flush MAC Address Table When Ports Link Down

MAC Address Table interface

Label	Description
Port No.	Show all MAC addresses mapping to a selected port in table.
Clear MAC Table	Click to clear all MAC addresses in the table.
MAC Address Table Aging Time	Assign an aging time; it must be a multiple of 5 minutes.The valid range is 0-3825 seconds.
Auto Flush MAC Adress Table When Ports Link Down	Check the checkbox to enable the function to the Flush MAC table when the port links down.
Apply	Click “Apply” to set the configuration.

5.1.10.3 Port Statistic

Port statistics show several statistics counters for all ports.



Port Statistics

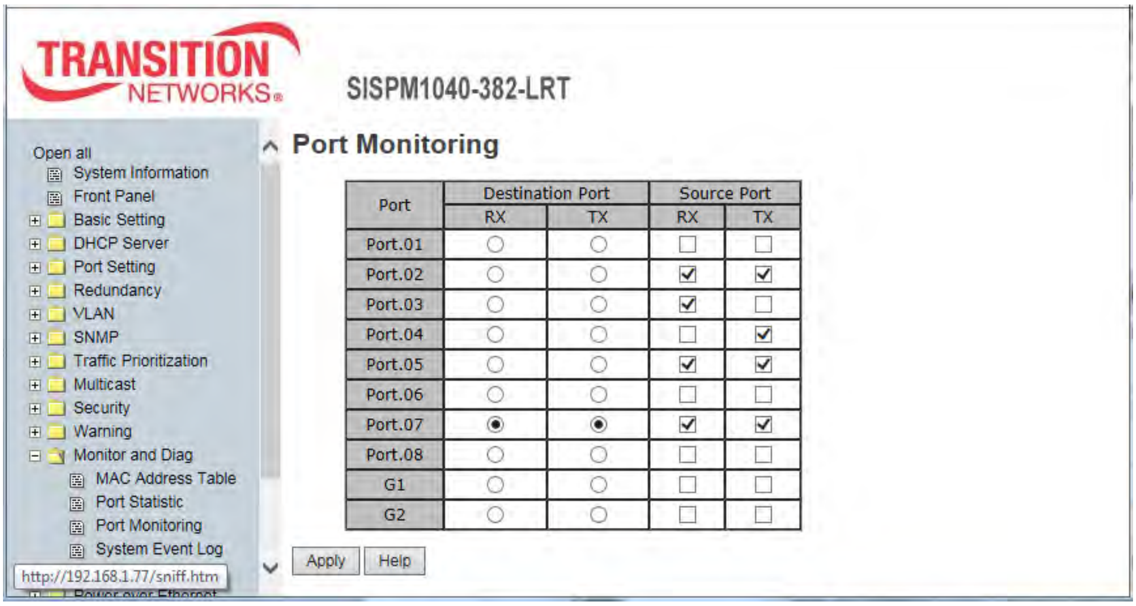
Port	Type	Link	State	TX Good Packet	TX Bad Packet	RX Good Packet	RX Bad Packet	TX Abort Packet	Packet Collision
Port.01	100TX	Down	Forwarding	0	0	0	0	0	0
Port.02	100TX	Down	Forwarding	0	0	0	0	0	0
Port.03	100TX	Down	Forwarding	0	0	0	0	0	0
Port.04	100TX	Down	Forwarding	0	0	0	0	0	0
Port.05	100TX	Down	Forwarding	0	0	0	0	0	0
Port.06	100TX	Down	Forwarding	0	0	0	0	0	0
Port.07	100TX	Up	Forwarding	158681	0	332526	0	0	0
Port.08	100TX	Down	Forwarding	0	0	0	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

Port Statistics interface

Label	Description
Type	Show port speed and media type.
Link	Show port link status.
State	Show ports as Forwarding, Listening, or Learning.
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	Click to reset all counters to zero for all ports.
Help	Show help file.

5.1.10.4 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**: keep all source ports unchecked in order to disable port monitoring.



Port Monitoring

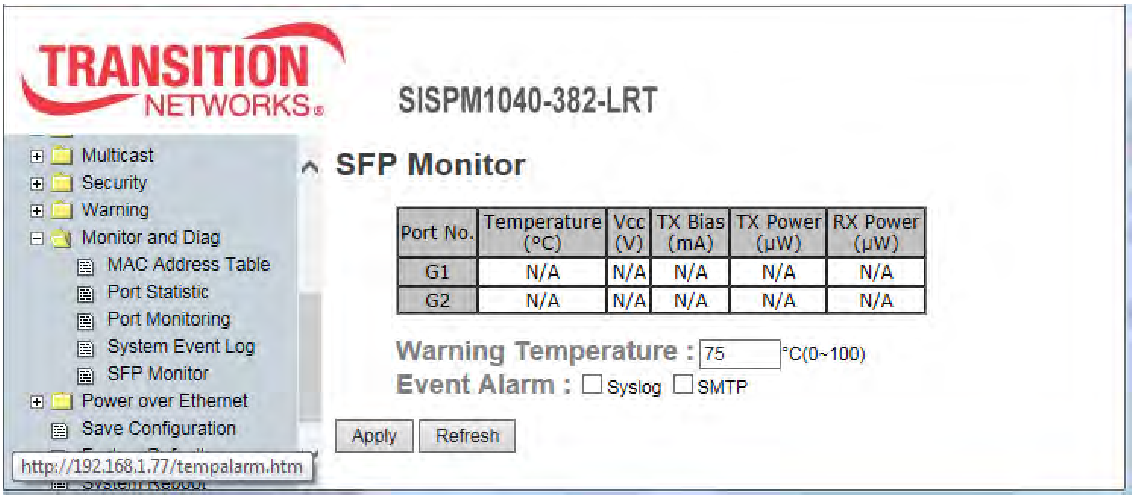
Port	Destination Port		Source Port	
	RX	TX	RX	TX
Port.01	○	○	□	□
Port.02	○	○	☑	☑
Port.03	○	○	☑	□
Port.04	○	○	□	☑
Port.05	○	○	☑	☑
Port.06	○	○	□	□
Port.07	●	●	☑	☑
Port.08	○	○	□	□
G1	○	○	□	□
G2	○	○	□	□

Port monitoring interface

Label	Description
Destination Port	The port will receive a copied frame from source port for monitoring purposes.
Source Port	The port will be monitored. Check the box for TX or RX to be monitored.
TX	The frames coming into the switch port.
RX	The frames received by switch port.
Apply	Click "**Apply**" to activate the configuration settings.
Help	Show help file.

5.1.10.5 SFP Monitor

This function can measure the temperature of SFP modules that support the DDM function. You can manage and set up the event alarm module through DDM Web page.



SFP Monitor

Port No.	Temperature (°C)	Vcc (V)	TX Bias (mA)	TX Power (µW)	RX Power (µW)
G1	N/A	N/A	N/A	N/A	N/A
G2	N/A	N/A	N/A	N/A	N/A

Warning Temperature : 75 °C(0~100)

Event Alarm : □ Syslog □ SMTP

Apply Refresh

SFP Monitor interface

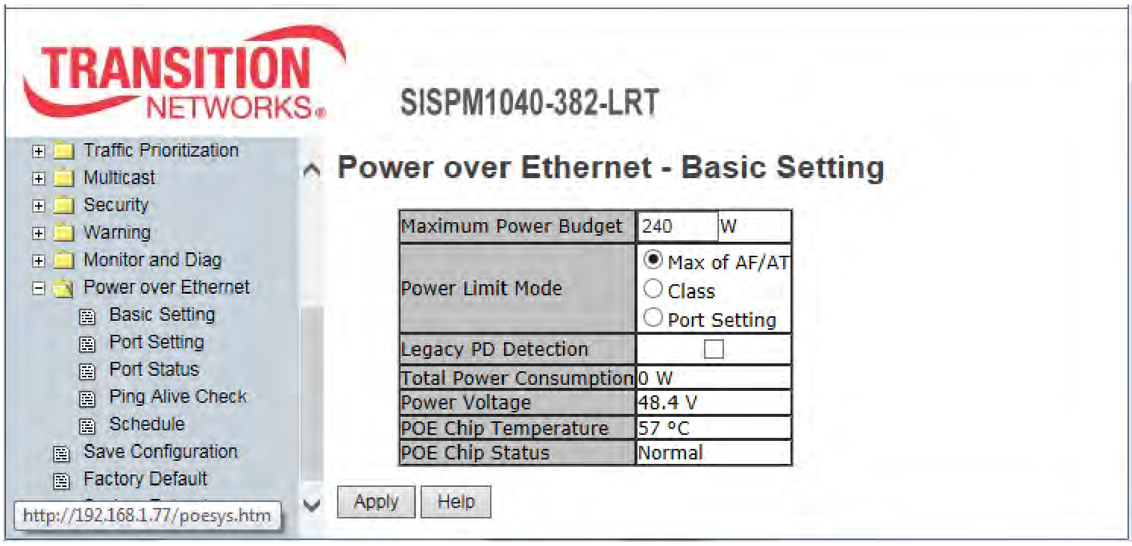
Label	Description
Temperature (℃)	The measured (reported) SFP temperature in degrees Celsius.
Vcc (V)	The measured (reported) SFP votage in Volts.
TX Bias (µ W)	The measured (reported) SFP transmit bias in microWatts.
TX Power (µ W)	The measured (reported) SFP transmit power in microWatts.
RX Power (µ W)	The measured (reported) SFP receive power in microWatts.
Warning Temperature	Set the Warning Temperature in degrees C. The valid range is 0~100 degrees C.
Event Alarm	Select the warning method; either Syslog and/or SMTP (E-mail).
Apply	Click "**Apply**" to activate the configuration settings.
Refresh	Click to update the page data.

5.1.11 Power over Ethernet (PoE)

5.1.11.1 Basic Setting

This page is for setting PoE parameters. The switch has eight ports (Port 1 - 8) that act as PSE (Power Sourcing Equipment) ports. **Note** that direct copper network connections between legacy detect PoE enabled ports is not recommended. See the "Product Alert Notification" on page 16 for details.

PoE (Power over Ethernet) technology is used to transmit electrical power to remote devices over standard Ethernet cables. PoE eliminates the need for an additional power supply for each connected PD (Powered Device), making it a cost-effective and convenient solution for deploying networks in places where placing a power supply is difficult or expensive to deploy. This page lets you set up basic PoE functions and view switch PoE status.



Power over Ethernet - Basic Setting

Maximum Power Budget	240 W
Power Limit Mode	● Max of AF/AT ○ Class ○ Port Setting
Legacy PD Detection	□
Total Power Consumption	0 W
Power Voltage	48.4 V
POE Chip Temperature	57 °C
POE Chip Status	Normal

PoE Basic Setting interface

Label	Description
Maximum Power Budget	Setting for maximum power available. This is the maximum amount of power that can be allocated to all switch ports. Allocated power to each port will be subtracted from the total power budget.

Power Limit Mode	This switch offers three power limit modes to provide power catering for different use scenarios. **Max of AF/AT**: the switch supports both the IEEE 802.3af and 802.3at standards. The 802.3af allows for a maximum continuous output power of 15.40 W and the 802.3at allows for 34.20 W. **Class**: by enabling this option, the switch will provide power to PDs in accordance to their classes, restricting the power supply to each PD to their maximum power levels. PD classes rang from 0 to 4. **Port Setting**: by enabling this option, the switch will provide power to PDs in accordance to the value you have specified. For more information on the settings, please refer to Power Limit in Port Setting.
Legacy PD Detection	Check the checkbox to enable legacy PD detection. Legacy PDs refers to powered devices manufactured before the IEEE standard was finalized and do not have the expected PD signature required by the PSE's detection signal. Such PDs usually feature large capacitance as the detection signature that does not completely comply with the 802.3af specs. By enabling this option, the switch will probe for legacy PDs and if a legacy PD is detected, the switch will provide power to the PD.
Total Power Consumption	Displays the total amount of power provided by the switch to PDs in Watts.
Power Voltage	Displays the output voltage of the switch for PoE ports.
POE Chip Temperature	Displays the temperature (in ℃) of the chip during operation, allowing you to monitor the temperature, helping prevent port overheating.
POE Chip Status	Displays the status of the chip during operation. The statuses include Normal, Resetting, No response, PoE controller error, and PoE device error, as described below: **Normal**: the chip is functioning normall.y **Resetting**: the chip is reinitiating. **No response**: the chip is not responding. **PoE controller error**: the PoE controller chip fails to operate functionally. **PoE device error**: the PoE device chip fails to operate functionally.
Apply	Click "**Apply**" to activate the configuration settings.
Help	Show help file.

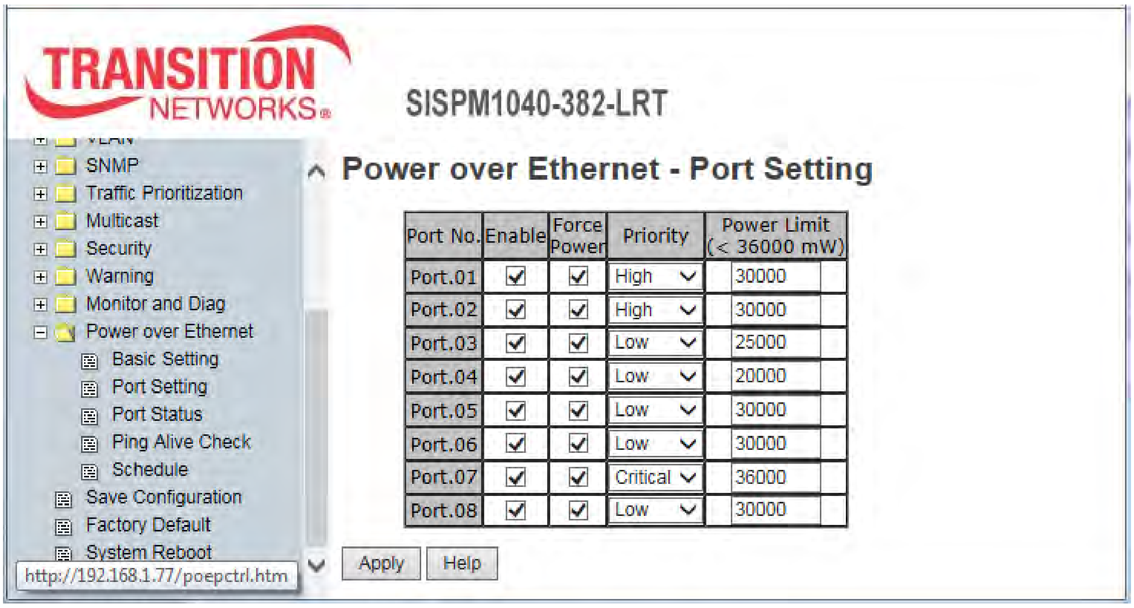
802.3af Classification

A PD can optionally present a classification signature to the PSE to indicate the maximum power it will draw while operating. The IEEE specification defines this signature as a constant current draw when the PSE port voltage is in the VCLASS range (between 15.5V and 20.5V), with the current level indicating one of five possible PD classes. For example, a typical PD load line, starting with the slope of the 25kΩ signature resistor below 10V, then transitioning to the classification signature current (e.g., Class 3) in the VCLASS range. The table below shows the possible classification values:

Class	Result
Class 0	No Class Signature Present; Treat Like Class 3
Class 1	3W
Class 2	7W
Class 3	13W
Class 4	25.5W (Type 2)

5.1.11.2 Power over Ethernet - Port Setting

This interface is for setting the 8 PoE ports (Port.01 - Port.08) that act as PSE (Power Sourcing Equipment) ports.



Power over Ethernet - Port Setting

Port No.	Enable	Force Power	Priority	Power Limit (< 36000 mW)
Port.01	☑	☑	High	30000
Port.02	☑	☑	High	30000
Port.03	☑	☑	Low	25000
Port.04	☑	☑	Low	20000
Port.05	☑	☑	Low	30000
Port.06	☑	☑	Low	30000
Port.07	☑	☑	Critical	36000
Port.08	☑	☑	Low	30000

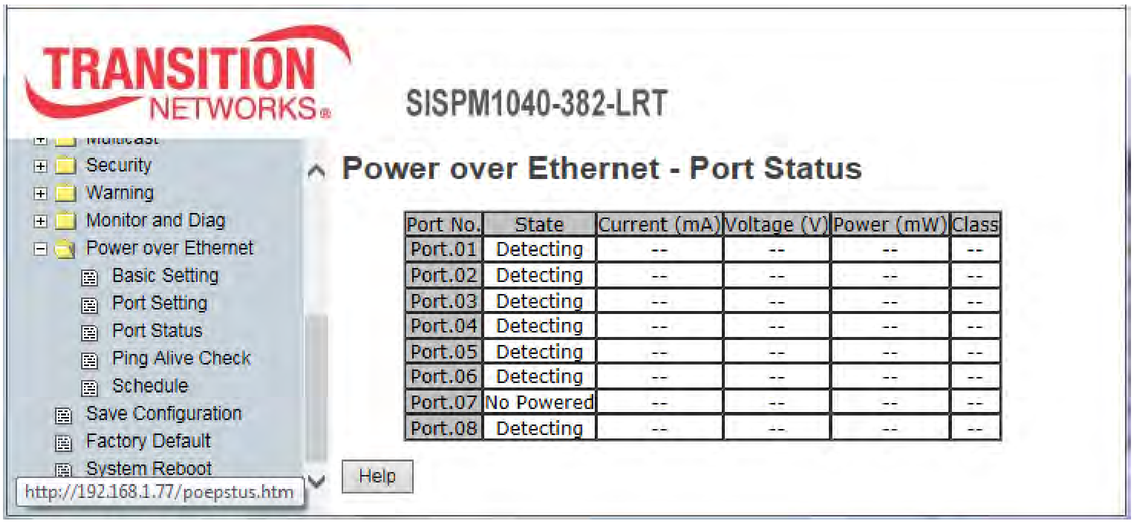
PoE Port Setting interface

Label	Description
Port No.	Displays the PoE port number to which the settings on this row will be applied.
Enable	Check the box to enable the PoE function on a per-port basis. The checkbox allows you to enable or disable the PoE function of each port. When checked, the PoE function is enabled.
Force Power	When the function is enabled, the system will force PSE to feed power to the PD even if the power requested by the PD is higher than the value defined by its class.
Priority	This drop-down list provides options for the power supply priority for each port. There are three levels of power priority: Low, High, and Critical (highest). The priority is useful when the switch is fully loaded and cannot supply sufficient power to every port. When enabled, the switch supplies power to ports with higher priority, and powers down some ports with lower priority. **Critical** is the highest priority level. Ports set to this level are guaranteed power before any ports assigned to the other two priority levels. **High** is the second highest level. Ports set to this level receive power only if all the ports set to the Critical level are already receiving power. If there is not enough power to support all of the ports set to the High priority level, power is provided to the ports based on port number, in ascending order.

	Low is the lowest priority level. This is the default setting. Ports set to this level only receive power if all the ports assigned to the other two levels are already receiving power. Like other levels, if there is not enough power to support all of the ports set to the Low priority level, power is provided to the ports based on port number, in ascending order.
Power Limit	Enter the maximum power in watts that can be delivered to a port (< 36000 mW).
Apply	Click "**Apply**" to activate the configuration settings.
Help	Show help file.

5.1.11.3 Port Status

This page displays detailed PoE status for each each Port. The information for individual ports varies with their PoE states.



Power over Ethernet - Port Status

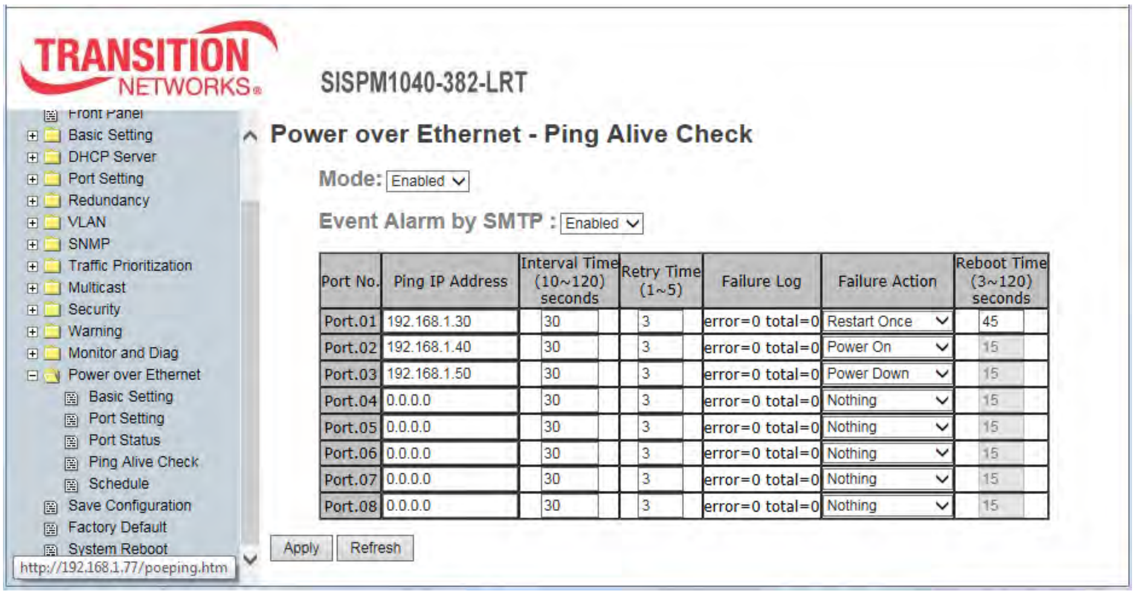
Port No.	State	Current (mA)	Voltage (V)	Power (mW)	Class
Port.01	Detecting	--	--	--	--
Port.02	Detecting	--	--	--	--
Port.03	Detecting	--	--	--	--
Port.04	Detecting	--	--	--	--
Port.05	Detecting	--	--	--	--
Port.06	Detecting	--	--	--	--
Port.07	No Powered	--	--	--	--
Port.08	Detecting	--	--	--	--

PoE Port Status interface

Label	Description
Port No.	Port number (Port.01 - Port.08).
State	Displays the PoE state of individual ports. The state can be: **Detecting**: the port is not connected to any PD or is detecting the PD. **No Powered**: power is not delivered. The connected device maybe not a PD or an error may have occurred when detecting. **Powered**: power is delivered to a PD. In this case, other columns in the same row will show related values.
Current (mA)	Displays the current used by the PD for this port in milliamps (mA).
Voltage (V)	Displays the voltage used by the PD for this port in Volts.
Power (mW)	Displays the power consumed by the PD for this port. The power is measured in milliwatts (mW).
Class	Displays the class of the PD for this port and the power consumed by the PD. When Bypass classification is enabled, the class value will not be shown.

5.1.11.4 PoE Ping Alive Check (Auto Power Reset - APR)

You can control the PoE function by using this feature to turn ON or OFF other PoE devices which connect with the assigned port. With APR enabled, it automatically pings the device on a configured schedule and if the device does not respond to the configured number of pings, the switch toggles PoE power on the port which automatically resets the device.



Power over Ethernet - Ping Alive Check

Mode: Enabled

Event Alarm by SMTP : Enabled

Port No.	Ping IP Address	Interval Time (10~120) seconds	Retry Time (1~5)	Failure Log	Failure Action	Reboot Time (3~120) seconds
Port.01	192.168.1.30	30	3	error=0 total=0	Restart Once	45
Port.02	192.168.1.40	30	3	error=0 total=0	Power On	15
Port.03	192.168.1.50	30	3	error=0 total=0	Power Down	15
Port.04	0.0.0.0	30	3	error=0 total=0	Nothing	15
Port.05	0.0.0.0	30	3	error=0 total=0	Nothing	15
Port.06	0.0.0.0	30	3	error=0 total=0	Nothing	15
Port.07	0.0.0.0	30	3	error=0 total=0	Nothing	15
Port.08	0.0.0.0	30	3	error=0 total=0	Nothing	15

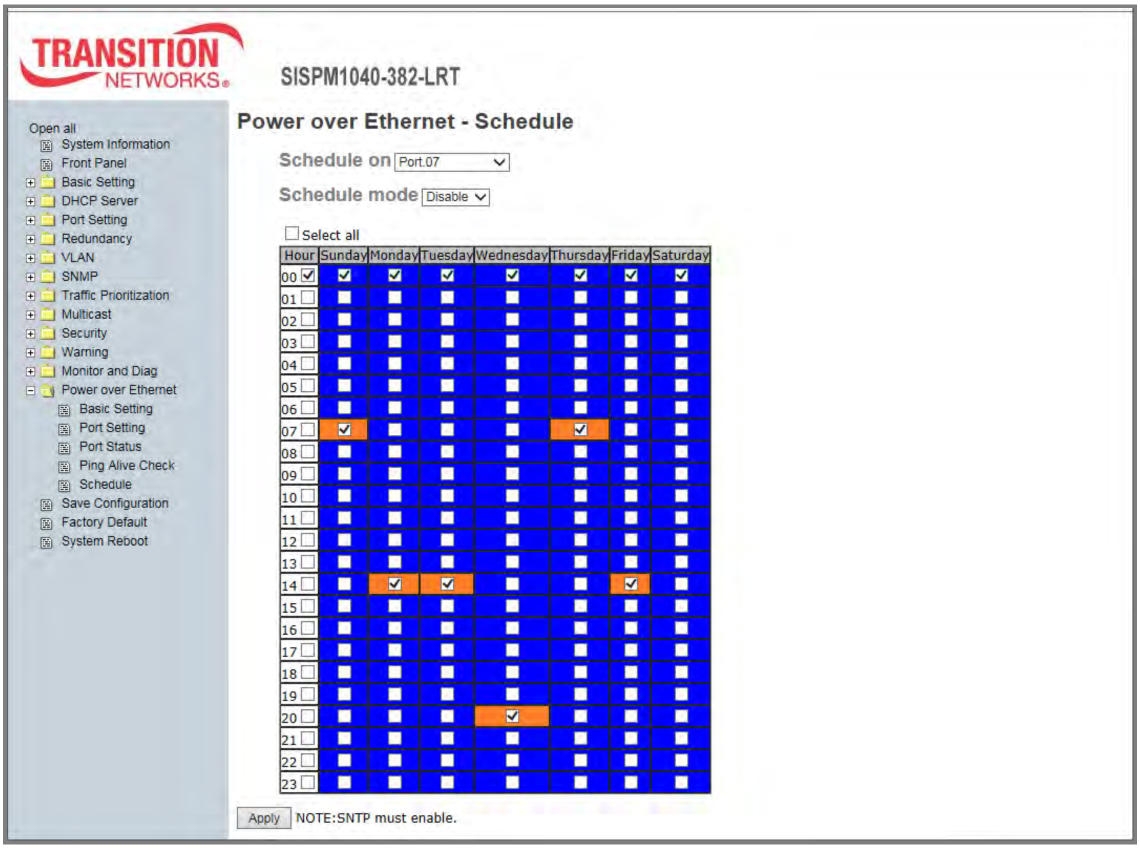
PoE Ping Alive Check interface

Label	Description
Mode	Enable or disable the PoE Ping Alive Check function globally.
Event Alarm by SMTP	At the dropdown select Enable to send alarm message via SMTP. When Enabled and a “ping" fails, you are notified by e-mail.
Port No.	You can configure the Ping function per PoE port number.
Ping IP Address	Enter the IP Address to Ping.
Interval Time	Enter the interval between Pings sent (10 ~120 seconds).
Retry Time	Set the amount of time before a Ping retry is attempted (1~5 seconds).
Failure Log	Tracks “Ping Check " failures.
Failure Action	Set the action to take when a failure occurs: Nothing, Restart Forever, Restart Once, Power On, or Power Down.
Reboot Time	Set the amount of time to wait after a ping check failure before rebooting the switch. Only valid if “Failure Action” is set to “Restart Forever” or “Restart Once”. The valid range is 3-120 seconds. The default is 15 seconds.

5.1.11.5 PoE Schedule

You can schedule a date and time to enable or disable the Power over Ethernet function.

Note that the SNTP function must be Enabled for PoE scheduling to work.



Power over Ethernet - Schedule

Schedule on Port.07

Schedule mode Disable

□ Select all

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

NOTE:SNTP must enable.

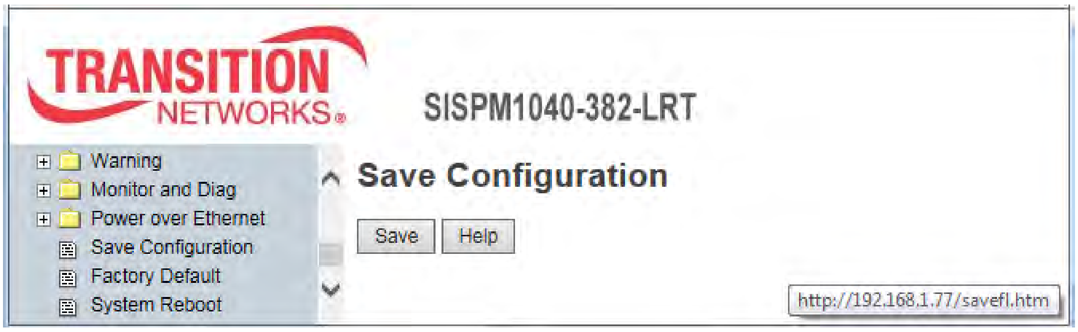
PoE Schedule interface

The following table describes the labels in this screen.

Label	Description
Schedule on	At the dropdown, select the Port to configure PoE scheduling. Schedule on Port.01, Port.02, Port.03, Port.04, Port.05, Port.06, Port.07, Port.08, or Port.01~Port.08.
Schedule mode	At the dropdown, select Enable or disable PoE schedule mode.
Select all	Check the box to select all dates and times. Uncheck the box to de-select all dates and times.
Hour	Check to enable the time(s) for PoE scheduling (00 - 23).
Sunday - Saturday	Check to enable PoE function for one or more days.
Apply	Click "**Apply**" to activate the configuration settings.

5.1.12 Save Configuration

If any configuration changes are made, you must click the “**Save Configuration**” button to save the current configuration data to the permanent flash memory. Otherwise, the current configuration is lost when the switch is powered off or when the system is reset.



Save Configuration interface

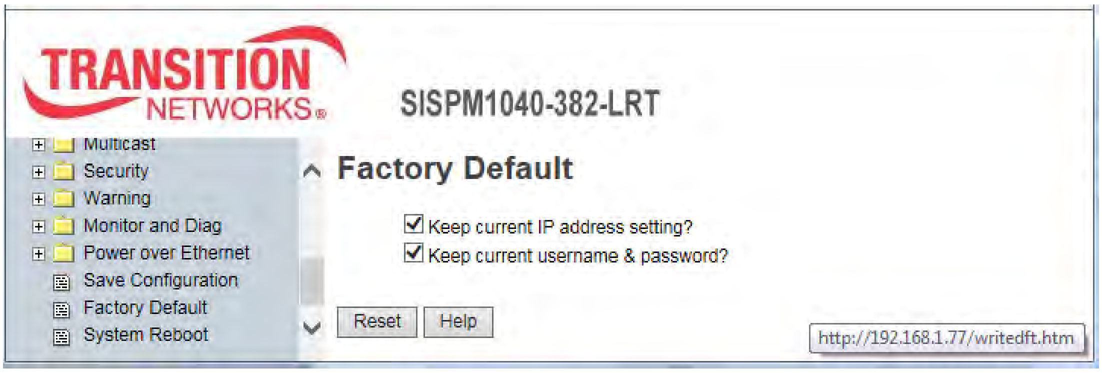
The following table describes the labels in this screen.

Label	Description
Save	Save all configuration changes.
Help	Show help file.

The message “*Save to Flash OK!   Press Here to back to Previous Page*.” displays when successfully completed. Click the link to return to the Save Configuration page. .

5.1.13 Factory Default

Here you can reset switch to its factory default configuration. After clicking the "Reset" button, you must restart the system for the default configuration to be applied at next start.

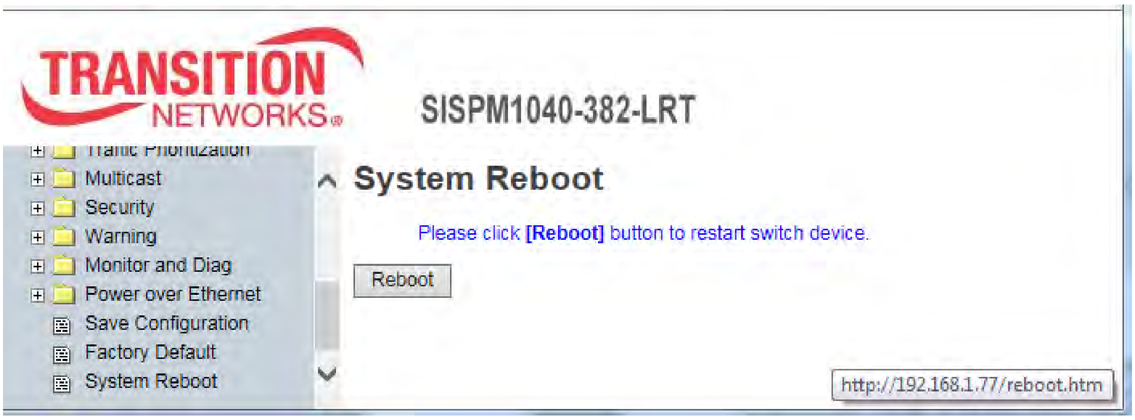


Factory Default interface

To reset the switch to its default configuration, click the **Reset** button to reset all configurations to the default values. You can check the boxes to “**Keep current IP address setting?**” and “**Keep current username & password?**”.

5.1.14 System Reboot

Here you can click the [Reboot] button to restart the switch.



Please click **[Reboot]** button to restart switch device.

System Reboot interface

The following table describes the labels in this screen.

Label	Description
Reboot	Click the button to start an immediate re-boot.

During the re-boot process, the message "*Rebooting ... After several seconds, reconnect the system.*" displays. **Note** that you may need to refresh your web bowser to display the System information page again.

6. Command Line Interface (CLI)

6.1 About CLI Management

In addition to Web-based management, the SISPM1040-382-LRT also supports CLI management. Before configuring by RS-232 serial console, use an RJ45 to DB9-F cable to connect the Switches' RS-232 Console port to your PCs' COM port. You can use HyperTerminal, PuTTY, Tera Term, Telnet, or similar program.

Follow the steps below to access the console via **HyperTerminal**.

1. At Windows desktop, click Start -> Programs -> Accessories -> Communications -> Hyper Terminal.

2. Enter a name for new connection

3. Select COM port number to use.

4. Use the COM port properties settings: 9600 for Bits per second, 8 for Data bits, None for Parity, 1 for Stop bits, and None for Flow control.

5. The Console login screen displays. Use the keyboard to enter the Username and Password (both **root**), then press "**Enter**".

CLI Management by Telnet

You can use "**TELNET**" to configure the switch. The default IP Address is **192.168.1.77**.

Follow the steps below to access the console via Telnet.

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

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

Note: firmware version v1.27 made CLI enhancements: add port alias in web UI, add port alias info for port event log in syslog, add port alias info for port linkup/down SNMP trap, add SSH and TACACS+, add setting check in POE Setting page, add CLI commands (security https, security ssh, no security https, no security ssh).

CLI Command Levels

Modes	Access Method	Prompt	Exit Method	About This Model
User EXEC	Begin a session with your switch.	switch>	Enter **logout** or **quit**.	The user commands available at the level of user is the subset of those available at the privileged level. Use this mode to • Enter menu mode. • Display system information.
Privileged EXEC	Enter the **enable** command while in user EXEC mode.	switch#	Enter **disable** to exit.	The privileged command is advance mode. Use Privileged mode to • Display advance function status • save configures
Global configuration	Enter the **configure** command while in privileged EXEC mode.	Switch (config)#	To exit to privileged EXEC mode, enter **exit** or **end**	Use this mode to configure parameters that apply to your Switch as a whole.
VLAN database	Enter the **vlan database** command while in privileged EXEC mode.	Switch (vlan)#	To exit to user EXEC mode, enter **exit**.	Use this mode to configure VLAN-specific parameters.
Interface configuration	Enter the **interface** command (with a specific interface)while in global configuration mode	Switch (config-if) #	To exit to global configuration mode, enter **exit**. To exit privileged EXEC mode enter **exit** 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 Command Set

SISPM1040-382-LRT Commands	Level	Description	Example
show config	**E**	Show switch configuration	switch>show config
show terminal	**P**	Show console information	switch#show terminal
write memory	**P**	Save your 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 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 administrator information	switch#show admin
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	switch#show dhcpserver ip-binding

		server	
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 IP security	switch#show security
no security	**G**	Disable IP security function	switch(config)#no security
no security http	**G**	Disable IP security of HTTP server	switch(config)#no security http
no security telnet	**G**	Disable IP security of telnet server	switch(config)#no security telnet

6.3 Port CommandSet

SISPM1040-382-LRT 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	switch(config)#interface fastEthernet 2 switch(config-if)#speed 100

		operation for Fast Ethernet., the speed can’t be set to 1000 if the port isn’t a giga port.	
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	switch(config)#interface fastEthernet 2

		Range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports, and zero means no limit.	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 form of this command to disable the port.	switch(config)#interface fastEthernet 2 switch(config-if)#state Disable
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 Command Set

SISPM1040-382-LRT 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] :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) [Workport]: The amount of work ports, this value could not be less than zero or be large than the amount 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]** **nolacp**	G	Assign a static trunk group. [GroupID] :1to3 [Port-list]:Member port list, This parameter could be a port range(ex.1-4) or a port list separate by a	switch(config)#aggregator group 1 2-4 nolacp or switch(config)#aggreator group 1 3,1,2 nolacp

		comma(ex.2, 3, 6)	
show aggregator	**P**	Show the information of trunk group	switch#show aggregator
no aggregator lacp **[GroupID]**	**G**	Disable the LACP function of trunk group	switch(config)#no aggreator lacp 1
no aggregator group **[GroupID]**	**G**	Remove a trunk group	switch(config)#no aggreator group 2

6.5 VLAN Command Set

SISPM1040-382-LRT 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 aggreator **[TrunkID]** **access-link untag** **[UntaggedVID]**	**V**	Assign a access link for VLAN by trunk group	switch(vlan)#vlan 8021q aggreator 3 access-link untag 33
vlan 8021q aggreator **[TrunkID]** **trunk-link tag** **[TaggedVID List]**	**V**	Assign a trunk link for VLAN by trunk group	switch(vlan)#vlan 8021q aggreator 3 trunk-link tag 2,3,6,99 or switch(vlan)#vlan 8021q aggreator 3 trunk-link tag 3-20
vlan 8021q aggreator **[PortNumber]** **hybrid-link untag** **[UntaggedVID]** **tag** **[TaggedVID List]**	**V**	Assign a hybrid link for VLAN by trunk group	switch(vlan)# vlan 8021q aggreator 3 hybrid-link untag 4 tag 3,6,8 or switch(vlan)# vlan 8021q aggreator 3 hybrid-link untag 5 tag 6-8
show vlan [VID] or **show vlan**	**V**	Show VLAN information	switch(vlan)#show vlan 23

6.6 Spanning Tree Command Set

SISPM1040-382-LRT 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	switch(config)# spanning-tree max-age 15

		receive a bridge protocol data unit (BPDU) message from the root switch within this interval, it recomputed the Spanning Tree Protocol (STP) topology.	
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 determines how long each of the listening and learning states last before the port begins forwarding.	switch(config)# spanning-tree forward-time 20
stp-path-cost **[1to200000000]**	**I**	Use the spanning-tree cost interface configuration command to set the path cost for Spanning Tree	switch(config)#interface fastEthernet 2 switch(config-if)#stp-path-cost 20

		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.	
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 Command Set

SISPM1040-382-LRT 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 Command Set

SISPM1040-382-LRT 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 Command Set

SISPM1040-382-LRT 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 Command Set

SISPM1040-382-LRT 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** [v1|v2c]	G	Configure SNMP server host information and community string	switch(config)#snmp-server host 192.168.10.50 community public trap-version v1 (remove) Switch(config)# no snmp-server host 192.168.10.50
snmp community-strings [Community-string] **right** [RO|RW]	G	Configure the community string right	switch(config)#snmp community-strings public right RO or switch(config)#snmp community-strings public right RW
snmp snmpv3-user [User Name] **password** [Authentication Password] [Privacy Password]	G	Configure the userprofile for SNMPV3 agent. Privacy password could be empty.	switch(config)#snmp snmpv3-user test01 password AuthPW PrivPW
show snmp	P	Show SNMP configuration	switch#show snmp
show snmp-server	P	Show specified trap server information	switch#show snmp-server
no snmp community-strings [Community]	G	Remove the specified community.	switch(config)#no snmp community-strings public
no snmp snmpv3-user [User Name] **password** [Authentication Password] [Privacy Password]	G	Remove specified user of SNMPv3 agent. Privacy password could be empty.	switch(config)# no snmp snmpv3-user test01 password AuthPW PrivPW
no snmp-server host	G	Remove the SNMP	switch(config)#no snmp-server

[Host-address]		server host.	192.168.10.50

6.11 Port Mirror CommandSet

SISPM1040-382-LRT 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 [RX|TX|Both]	I	Configure source port of monitor function	switch(config)#interface fastEthernet 2 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 Command Set

SISPM1040-382-LRT 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 radiusip [IP address]	G	Use the 802.1x system radius IP global configuration command to change the radius server IP.	switch(config)# 8021x system radiusip 192.168.1.1
8021x system serverport [port ID]	G	Use the 802.1x system server port global 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 NAS ID	switch(config)# 8021x system nasid test1
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 Command Set

SISPM1040-382-LRT 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, EVENT Command Set

SISPM1040-382-LRT 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 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 Ring-topology-change	**G**	Disable 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 SMTP	switch(config)#interface fastethernet 3

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

6.15 SNTP Command Set

SISPM1040-382-LRT 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 Ring Command Set

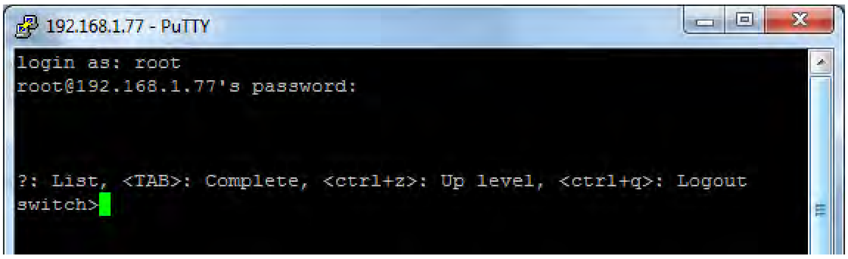
SISPM1040-382-LRT Commands	**Level**	**Description**	**Example**
Ring enable	**G**	Enable ing	switch(config)# ring enable
Ring master	**G**	Enable ring master	switch(config)# ring master
Ring couplering	**G**	Enable couple ring	switch(config)# ring couplering
Ring dualhoming	**G**	Enable dual homing	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 Ring information	switch#show ring
no Ring	**G**	Disable 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

6.17 CLI Command Summary

6.17.1 Terminal Emulator Examples

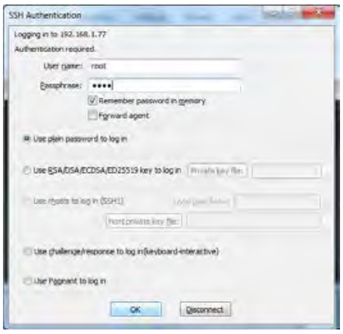
Examples from HyperTerminal, PuTTY, Tera Term, and Telnet are provided below.

PuTTY login successful prompt:



```
login as: root
root@192.168.1.77's password:


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

TeraTerm SSH Auth Login:



Logging in to 192.168.1.77

Authentication required.

User name: root

Passphrase: ••••

☑ Remember password in memory

□ Forward agent

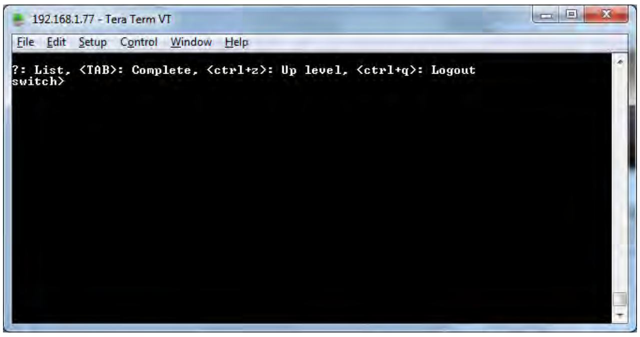
● Use plain password to log in

○ Use RSA/DSA/ECDSA/ED25519 key to log in

○ Use rhosts to log in (SSH1)

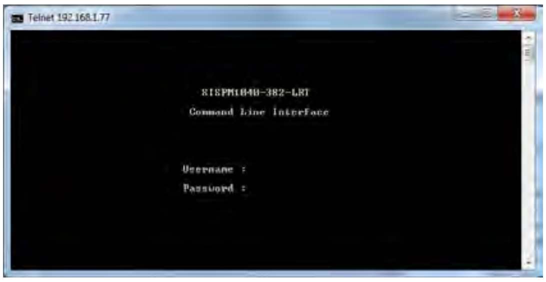
○ Use challenge/response to log in(keyboard-interactive)

○ Use Pageant to log in

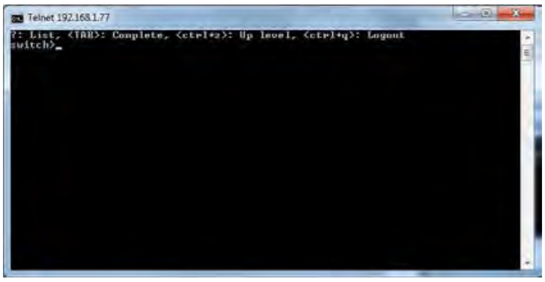


```
?: List, <TAB>: Complete, <ctrl+z>: Up level, <ctrl+q>: Logout
switch>
```

Telnet login:

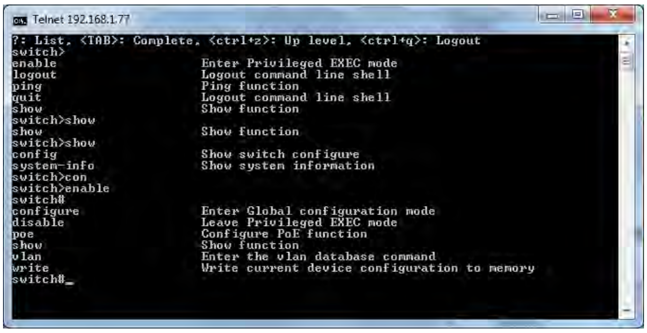


```
                SISPM1040-382-LRT
             Command Line Interface


            Username :
            Password :
```



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

Telnet *list* command:



```
?: 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>show
show                      Show function
switch>show
config                    Show switch configure
system-info               Show system information
switch>con
switch>enable
switch#
configure                 Enter Global configuration mode
disable                   Leave Privileged EXEC mode
poe                       Configure PoE function
show                      Show function
vlan                      Enter the vlan database command
write                     Write current device configuration to memory
switch#_
```

6.17.2 CLI Examples

Example 1: show the available top-level commands using the **?**:

```
?: 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
```

Example 2: show the available show commands:

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

Example 3: show the available config commands:

```
switch> enable
switch#con
switch#configure ?
<ENTER>
switch#configure
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-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
multi-ring              Configure Multi-Ring
multicast-filtering     Configure multicast filtering entry
multiple-ring           Configure Multiple Ring
---- More (q/Q to quit) ----
no                     Disable setting
ptp                    PTP function setting
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
tacacs+                TACACS+ configuration
tftp                   Transfer file by TFTP
switch(config)#
```

Example 4: show system information:

```
switch>show system <tab>
switch>show system-info
Name:        SISPM1040-382-LRT
Description: Industrial 10-port managed PoE Ethernet switch with 8x10/100Base-T(X) P.S.E.
and 2xGigabit combo ports, SFP socket
Location:
Contact:
Firmware Version: v1.33
Kernel Version: v3.50
MAC Address: 00-C0-F2-56-0A-31
IP Address: 192.168.1.77
System OID: 1.3.6.1.4.1.868.2.120.0.5.107
OK.
switch>
```

Example 5: show config information:

```
switch>show config

==================System Information==================

Name:       SISPM1040-382-LRT
Description: Industrial 10-port managed PoE Ethernet switch with 8x10/100Base-T(X) P.S.E.
and 2xGigabit combo ports, SFP socket
Location:
Contact:
Firmware Version: v1.33
Kernel Version: v3.50
MAC Address: 00-C0-F2-56-0A-31
IP Address: 192.168.1.77
System OID: 1.3.6.1.4.1.868.2.120.0.5.107
OK.
---- More (q/Q to quit) ----

==================IP Information======================

DHCP client is inactive
Address ip:192.168.1.77
Address subnet:255.255.255.0
Address gateway:192.168.1.254
Address DNS1:0.0.0.0
Address DNS2:0.0.0.0

OK.
---- More (q/Q to quit) ----

==================Terminal Information================

Baudrate(bits/sec): 9600
Data Bits: 8
Parity Check: none
Stop Bits: 1
Flow Control: none
```

```
OK.
---- More (q/Q to quit) ----

===================Interface Configuration==============

Port    | State |Link State|Auto Neg.| Speed Status|Duplex Status| Flow Control
       |Cfg|Act|          |         |Config|Actual|Config|Actual|Config|Actual
Port.01| ON| ON|       N/A|     Auto|   100|   N/A|  Full|   N/A|   SYM|  N/A|
Port.02| ON| ON|       N/A|     Auto|   100|   N/A|  Full|   N/A|   SYM|  N/A|
Port.03| ON| ON|       N/A|     Auto|   100|   N/A|  Full|   N/A|   SYM|  N/A|
Port.04| ON| ON|       N/A|     Auto|   100|   N/A|  Full|   N/A|   SYM|  N/A|
Port.05| ON| ON|       N/A|     Auto|   100|   N/A|  Full|   N/A|   SYM|  N/A|
Port.06| ON| ON|       N/A|     Auto|   100|   N/A|  Full|   N/A|   SYM|  N/A|
Port.07| ON| ON|        UP|     Auto|   100|   100|  Full|  Full|   SYM|   On|
Port.08| ON| ON|       N/A|     Auto|   100|   N/A|  Full|   N/A|   SYM|  N/A|
G1     | ON| ON|       N/A|     Auto|  1000|   N/A|  Full|   N/A|   SYM|  N/A|
G2     | ON| ON|       N/A|     Auto|  1000|   N/A|  Full|   N/A|   SYM|  N/A|

Auto Detect 100/1000 SFP: enabled

OK.
---- More (q/Q to quit) ----

===================Interface Status=====================

                            Speed    Flow
Port    Type     Link State    Duplex   Ctrl Security
-----------------------------------------------------------
Port.01 100TX    Down Enable   N/A      N/A  ON
Port.02 100TX    Down Enable   N/A      N/A  ON
Port.03 100TX    Down Enable   N/A      N/A  ON
Port.04 100TX    Down Enable   N/A      N/A  ON
Port.05 100TX    Down Enable   N/A      N/A  ON
Port.06 100TX    Down Enable   N/A      N/A  ON
Port.07 100TX    Up   Enable   100/FULL ON   ON
Port.08 100TX    Down Enable   N/A      N/A  ON
```

```
G1     1GTX/SFP Down Enable   N/A     N/A  ON
G2     1GTX/SFP Down Enable   N/A     N/A  ON


OK.
---- More (q/Q to quit) ----
```

7. Technical Specifications

Physical Ports	
10/100 Base-T(X) Ports in RJ45 Auto MDI/MDIX with PSE	**8**
Gigabit Combo Ports with 10/100/1000Base-T(X) and 100/1000Base-X SFP port	**2**
Technology	
Ethernet Standards	IEEE 802.3 for 10Base-T, 802.3u for 100Base-TX and 100Base-FX IEEE 802.3z for 1000Base-X, 802.3ab for 1000Base-T IEEE 802.3x for Flow control, 802.3ad for LACP (Link Aggregation Control Protocol) IEEE 802.1D for STP (Spanning Tree Protocol), 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: 5.6Gbps Max. Number of Available VLANs: 4096 IGMP multicast groups: 1024 Port rate limiting: User Define
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, monitTransition Networks, security SNTP for synchronizing of clocks over network PTP Client (Precision Time Protocol) clock synchronization support DHCP Server / Client support Port Trunk support MVR (Multicast VLAN Registration) support
Network Redundancy	Redundant Ring, Multiple Ring, Multi-Ring, STP, RSTP, MSTP, Coupling Ring, Dual Homing. Only one redundancy protocol can be enabled at a time.

Warning / Monitoring	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
DDM Function	Voltage / Current / Temperature
RS-232 Serial Console Port	RS-232 in RJ45 connector with console cable. 9600bps, 8, N, 1
LED indicators	
Power/PoE LED	Green : Power LED x 3, Green : PoE LED x 8
Ring LED	Green : Indicates system operating in Ring mode
R.M. LED	Green : Indicates system operating in Ring Master mode
Fault LED	Amber : Indicates unexpected event occurred
10/100Base-T(X) RJ45 Port	Green LED for port Link/Act. Amber for Duplex/Collision.
10/100/1000Base-T(X) RJ45 Port LED	Green for Link/Act. Amber for 100Mbps indicator
100/1000Base-X Fiber Port	Green LED for port Link/Act.
Fault contact	
Relay	Relay output to carry capacity of 1A at 24VDC
Power	
Redundant Input Power	Dual DC inputs. 50 ~ 57VDC on 6-pin terminal block
Power Consumption (Typ.)	7.68 Watts (power consumption of P.S.E. is not included)
Overload Current Protection	Present
Reverse polarity protection	Not Present
Physical Characteristic	
Enclosure	IP-30
Dimension (W x D x H)	74.3 (W) x 109.2 (D) x 153.6 (H) mm (2.93 x 4.3 x 6.05 inch)
Weight (g)	1185 g
Environmental	
Storage Temperature	-40 to 85°C (-40 to 185°F)
Operating Temperature	-40 to 75°C (-40 to 167°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	Lifetime

Power Supply Features and Specifications

Use the +V ADJ access to the small Phillips screw; turn clockwise to increase voltage. It is adjustable 48-55V. Recommend adjusting output to a minimum of 53VDC out for PoE+ applications.

Industrial DIN Rail Mounted Power Supply 25104:

Power Supply Features

94% High Efficiency / 150% Peak Load

Convection air cooling

UL 508 approved / RoHS compliant

Protected against Short Circuit, Overload, Over Voltage, and Overheating

MTBF 169.3 Khrs

Power Supply Specifications

Power Output	Output Voltage 48VDC Current Rating 5A Power Rating 240 Watts Ripple & Noise Max 120mVp-p Voltage Range 48~55VDC Voltage Tolerance ±1.0% Line Regulation ±0.5% Load Regulation ±1.0% Setup, Rise Time 300ms, 60ms Hold Up Time 20ms
Power Input	Voltage Range Switch Selectable 88~132VAC 124~370VDC Frequency Range 47~63Hz Efficiency 94% AC Current (Typical) 2.6A@115VAC 1.3A@230VAC Inrush Current (Cold) 33A@115VAC 65A@230VAC
Protection	Overload 105~160% Overvoltage 56~65V
Dimensions	Width: 2.48” [63 mm] x Depth: 5.26” [113.5 mm] x Height: 4.93” [125.2 mm]

Environment	Operating: -25°C to +60°C Storage: -40°C to +85°C Humidity: 20% to 95% (non-condensing)
Weight	2.27 lbs. [1.03 kg]
Compliance	Safety: UL508, TUV EN60950-1, IEC60068-2-6 (Vibration) EMC Emission: EN55022, CISPR22 Class B, EN61000-3-2, EN61000-3-3; EMC Immunity: EN61000-4-2, EN61000-4-3, EN61000-4-4, EN61000-4-5, EN61000-4-6, EN61000-4-8, EN61000-4-11, EN55024, EN61000-6-2, EN50082-2, EN61204-3, SEMI F47, GL Approved
Warranty	Lifetime

Power Supply Standards

Safety: UL508

TUV EN60950-1

Vibration: IEC60068-2-6

EMC EmissionEN55022

CISPR22 Class B

EN61000-3-2

EN61000-3-3

EMC ImmunityEN61000-4-2

EN61000-4-3, EN61000-4-4, EN61000-4-5, EN61000-4-6, EN61000-4-8, EN61000-4-11

EN55024

EN61000-6-2

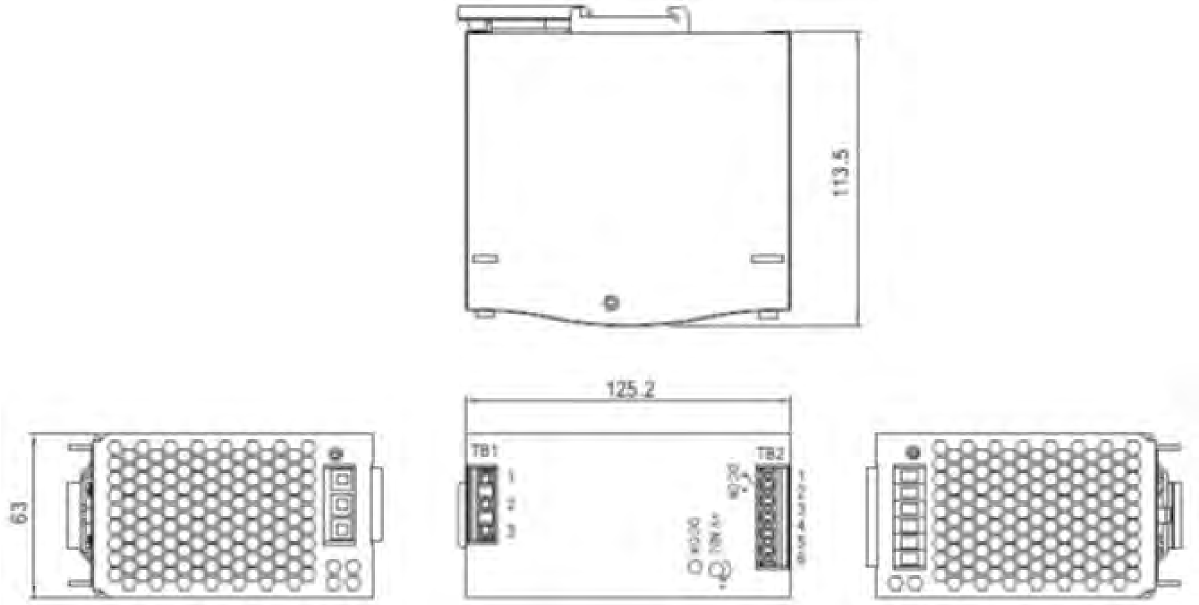
EN50082-2

EN61204-3

SEMI F47

GL Approved

Power Supply Dimensions



8. Troubleshooting

1. Verify the Hardware Installation information on page 14.

2. Check the status of the Front Panel LEDs on page 19.

3. Check the cabling; see section 4. Cables on page 21.

4. Verify the proper operation of other network equipment.

5. Verify proper operation of any third party packages (e.g., web browser, terminal emulation software, servers, etc.).

6. Run available system tests and check the various statistics pages.

7. Try switching modes (from CLI to web UI or vice versa).

8. Check the Syslog and/or System Event Log.

9. See if a firmware upgrade is available and upgrade the switch if possible.

10. Save your config and then try a Reset to Factory Defaults and/or a System Reboot.

11. Collect system and device information; see below.

12. Contact Transition Networks Tech Support; see Contact Us on page 142 below.

Record System and Device Information

After performing the Troubleshooting steps above, and before contacting Transition Networks Technical Support, please record system and device information to help the Tech Support specialist.

1. Model name: ____

2. System Name: ____

3. System OID: ____

4. Firmware Version: ____

5. IP Address of switch: ____

6. DNS Server or DHCP Server configured? _______________________________

7. Record anyerror messages displayed: ________________________________

____

8. Your Transition Networks service contract number: ____________________

Describe the failure: ____

____

____

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

____

____

The serial and revision numbers of all involved TN products in the network: ______________

____

____

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

____

____

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

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

____

____

Any previous Return Material Authorization (RMA) numbers: ____________________________

____

8. Service, Warranty & Compliance Information

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.

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

To return a defective product for warranty coverage, contact Transition Networks' Customer Support for a return authorization number.

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 a $50 fee 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.

Contact Us

Technical Support: Technical support is available 24-hours a day
US and Canada: 1-800-260-1312
International: 00-1-952-941-7600

Main Office
tel: +1.952.941.7600 | toll free: 1.800.526.9267 | fax: 952.941.2322
sales@transition.com | techsupport@transition.com | customerservice@transition.com

Address
Transition Networks
10900 Red Circle Drive
Minnetonka, MN 55343, U.S.A.
Web: https://www.transition.com

9. Regulatory Agency Information

Switch 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),

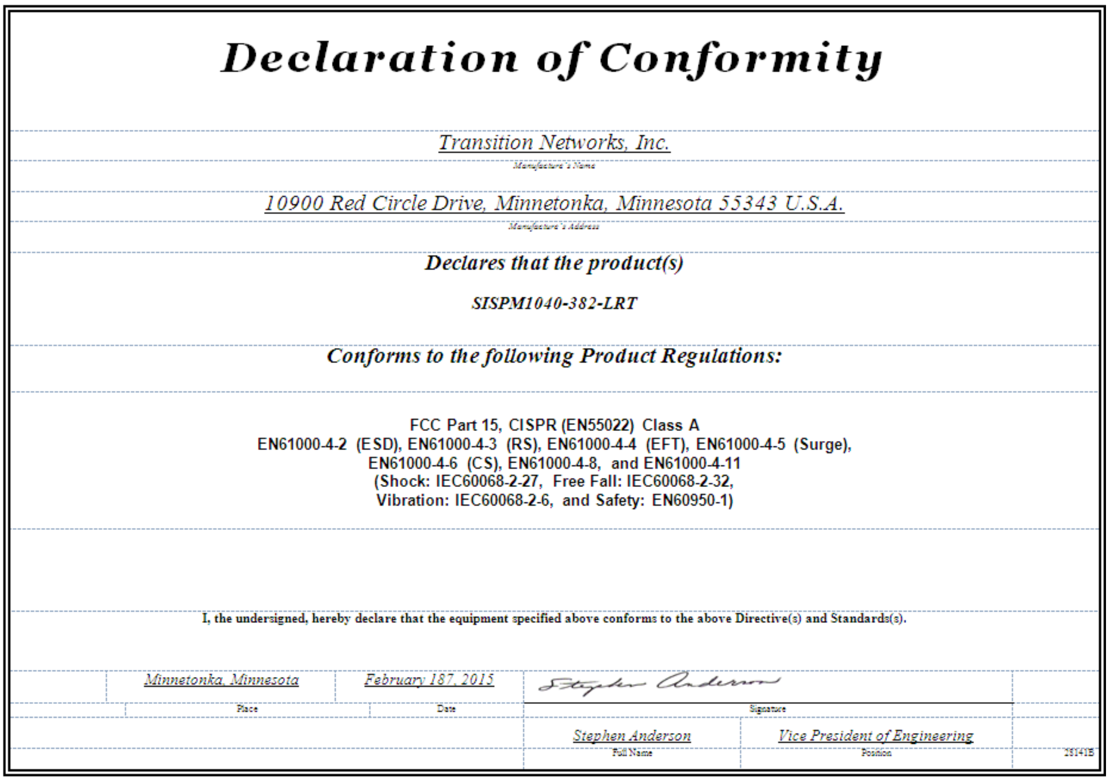
EN61000-4-6 (CS),

EN61000-4-8,

EN61000-4-11

Shock	IEC60068-2-27
Free Fall	IEC60068-2-32
Vibration	IEC60068-2-6
Safety	EN60950-1

Declaration of Conformity



Declaration of Conformity

Transition Networks, Inc.
Manufacture's Name

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

Declares that the product(s)

SISPM1040-382-LRT

Conforms to the following Product Regulations:

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

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

Minnetonka, Minnesota	*February 187, 2015*	Stephen Anderson
Place	Date	Signature

Stephen Anderson	*Vice President of Engineering*
Full Name	Position

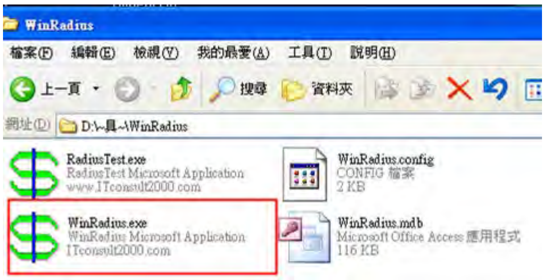
28141B

Appendix A - RADIUS Server and Switch Settings

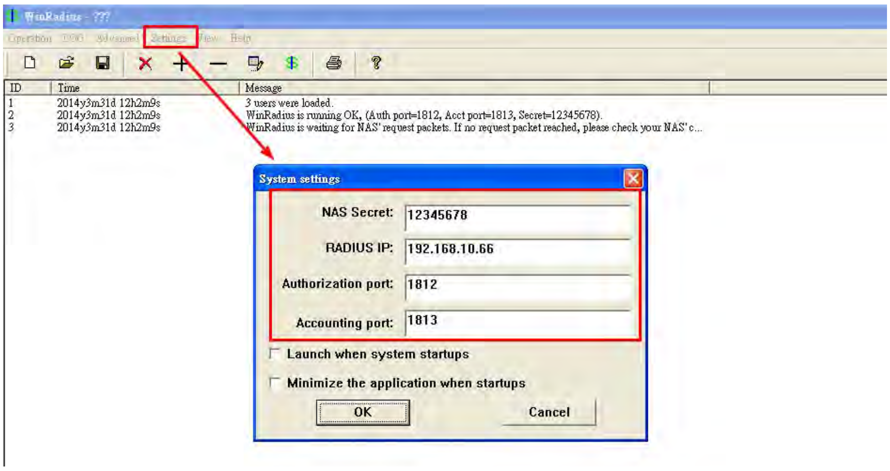
This section provides MS WinRadius and Windows / PC settings. See section 5.1.8.6 - “802.1x 802.1x - Radius Server” for the SISPM1040 RADIUS parameter descriptions.

Radius Server and Switch Setting

1. Enable the WinRadius tool.



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



ID	Time	Message
1	2014y3m31d 12h2m9s	3 users were loaded.
2	2014y3m31d 12h2m9s	WinRadius is running OK, (Auth port=1812, Acct port=1813, Secret=12345678).
3	2014y3m31d 12h2m9s	WinRadius is waiting for NAS' request packets. If no request packet reached, please check your NAS' c...

System settings

NAS Secret: 12345678

RADIUS IP: 192.168.10.66

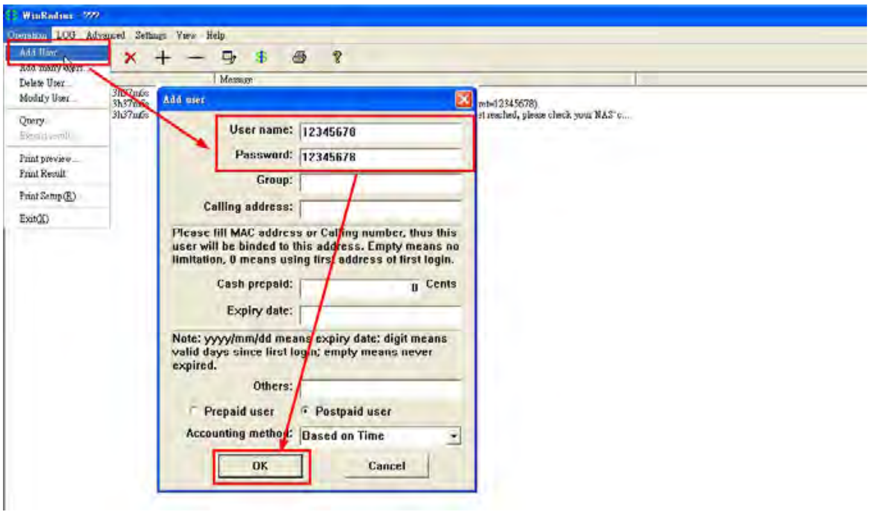
Authorization port: 1812

Accounting port: 1813

□ Launch when system startups

□ Minimize the application when startups

3. Create a new User.



Add user

User name: 12345678

Password: 12345678

Group:

Calling address:

Please fill MAC address or Calling number, thus this user will be binded to this address. Empty means no limitation, 0 means using first address of first login.

Cash prepaid: 0 Cents

Expiry date:

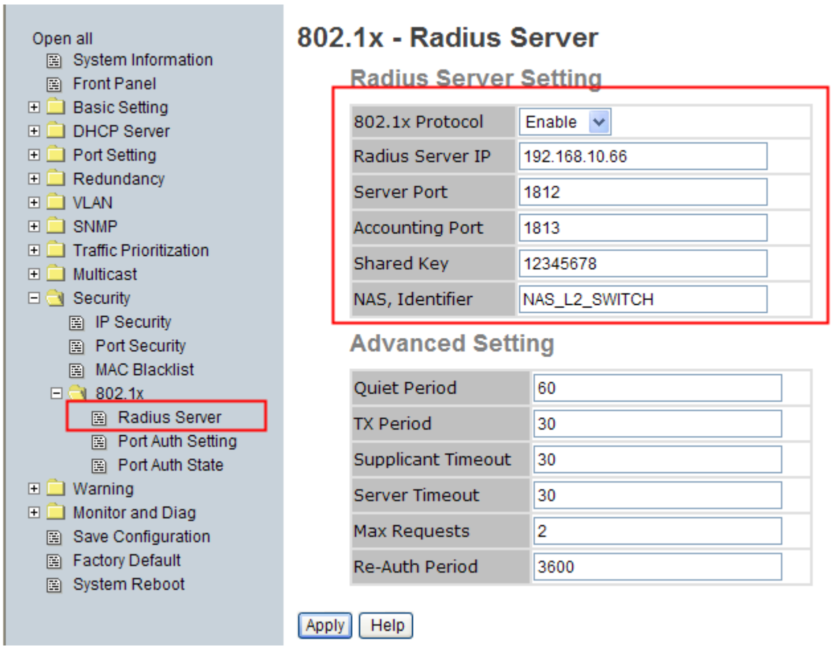
Note: yyyy/mm/dd means expiry date: digit means valid days since first login; empty means never expired.

Others:

○ Prepaid user ● Postpaid user

Accounting method: Based on Time

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



802.1x - Radius Server

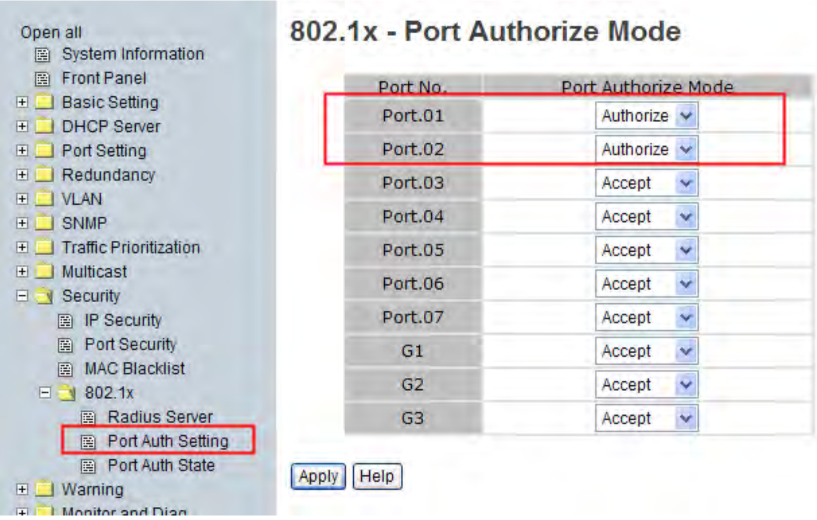
Radius Server Setting

802.1x Protocol	Enable
Radius Server IP	192.168.10.66
Server Port	1812
Accounting Port	1813
Shared Key	12345678
NAS, Identifier	NAS_L2_SWITCH

Advanced Setting

Quiet Period	60
TX Period	30
Supplicant Timeout	30
Server Timeout	30
Max Requests	2
Re-Auth Period	3600

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



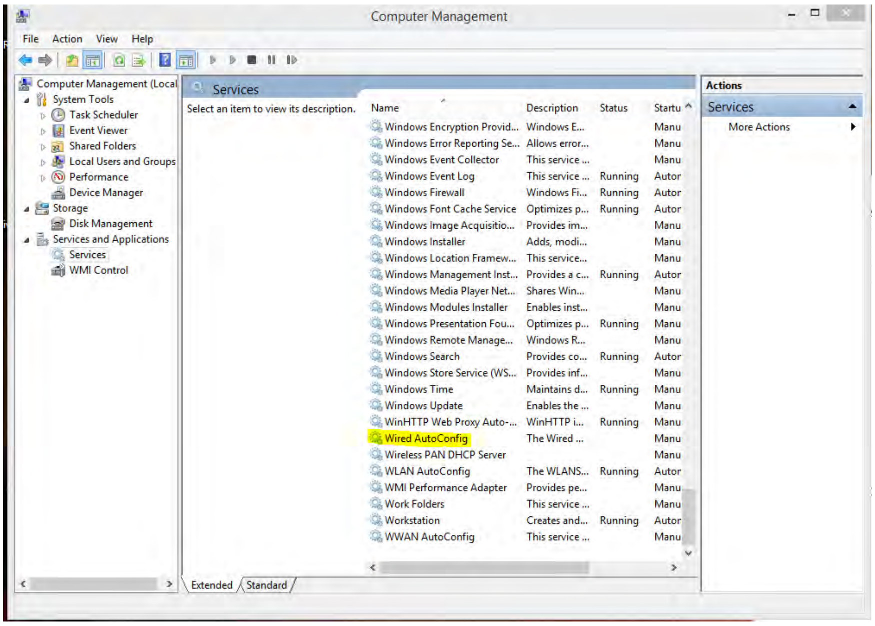
802.1x - Port Authorize Mode

Port No.	Port Authorize Mode
Port.01	Authorize
Port.02	Authorize
Port.03	Accept
Port.04	Accept
Port.05	Accept
Port.06	Accept
Port.07	Accept
G1	Accept
G2	Accept
G3	Accept

6. Continue with the User PC Settings section below.

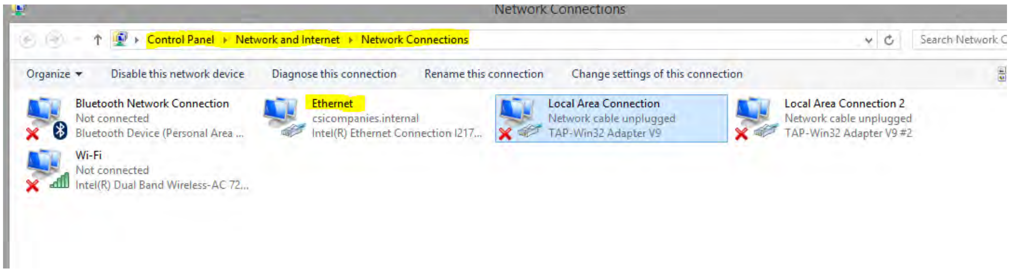
User PC Settings

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



Name	Description	Status	Startu
Windows Encryption Provid...	Windows E...		Manu
Windows Error Reporting Se...	Allows error...		Manu
Windows Event Collector	This service ...		Manu
Windows Event Log	This service ...	Running	Autor
Windows Firewall	Windows Fi...	Running	Autor
Windows Font Cache Service	Optimizes p...	Running	Autor
Windows Image Acquisitio...	Provides im...		Manu
Windows Installer	Adds, modi...		Manu
Windows Location Framew...	This service...		Manu
Windows Management Inst...	Provides a c...	Running	Autor
Windows Media Player Net...	Shares Win...		Manu
Windows Modules Installer	Enables inst...		Manu
Windows Presentation Fou...	Optimizes p...	Running	Manu
Windows Remote Manage...	Windows R...		Manu
Windows Search	Provides co...	Running	Autor
Windows Store Service (WS...	Provides inf...		Manu
Windows Time	Maintains d...	Running	Manu
Windows Update	Enables the ...		Manu
WinHTTP Web Proxy Auto-...	WinHTTP i...	Running	Manu
Wired AutoConfig	The Wired ...		Manu
Wireless PAN DHCP Server			Manu
WLAN AutoConfig	The WLANS...	Running	Autor
WMI Performance Adapter	Provides pe...		Manu
Work Folders	This service ...		Manu
Workstation	Creates and...	Running	Autor
WWAN AutoConfig	This service ...		Manu

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


Network Connections
Control Panel › Network and Internet › Network Connections
Search Network C
Organize
Disable this network device
Diagnose this connection
Rename this connection
Change settings of this connection

Bluetooth Network Connection
Not connected
Bluetooth Device (Personal Area ...

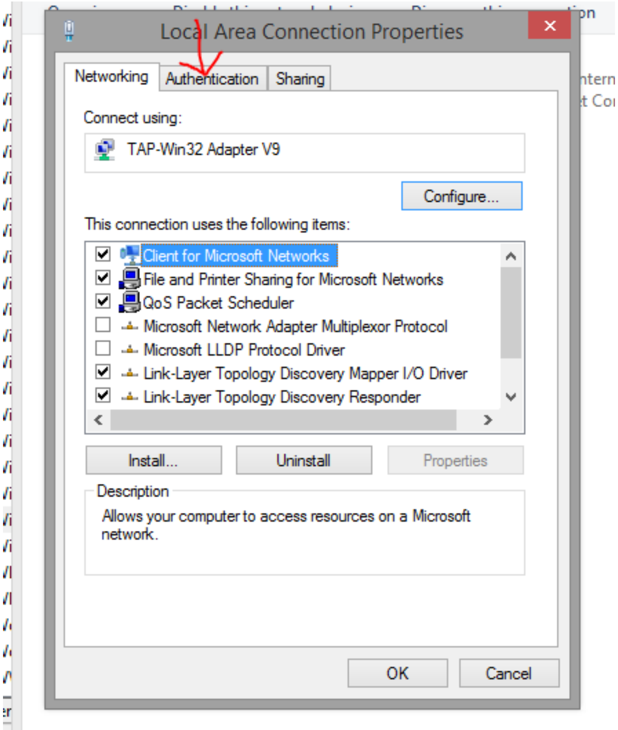
Ethernet
csicompanies.internal
Intel(R) Ethernet Connection I217...

Local Area Connection
Network cable unplugged
TAP-Win32 Adapter V9

Local Area Connection 2
Network cable unplugged
TAP-Win32 Adapter V9 #2

Wi-Fi
Not connected
Intel(R) Dual Band Wireless-AC 72...

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



Local Area Connection Properties

Networking | Authentication | Sharing

Connect using:

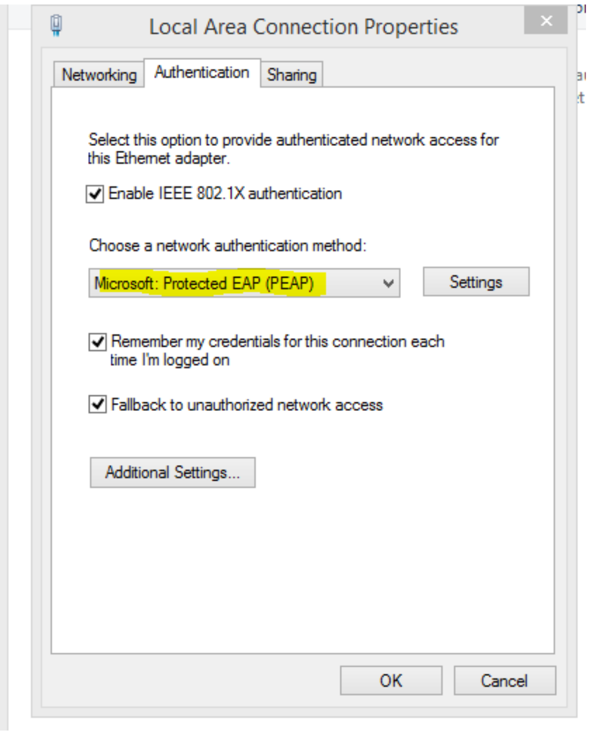
TAP-Win32 Adapter V9

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- □ Microsoft Network Adapter Multiplexor Protocol
- □ Microsoft LLDP Protocol Driver
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

Allows your computer to access resources on a Microsoft network.



Local Area Connection Properties

Networking | Authentication | Sharing

Select this option to provide authenticated network access for this Ethernet adapter.

☑ Enable IEEE 802.1X authentication

Choose a network authentication method:

Microsoft: Protected EAP (PEAP)

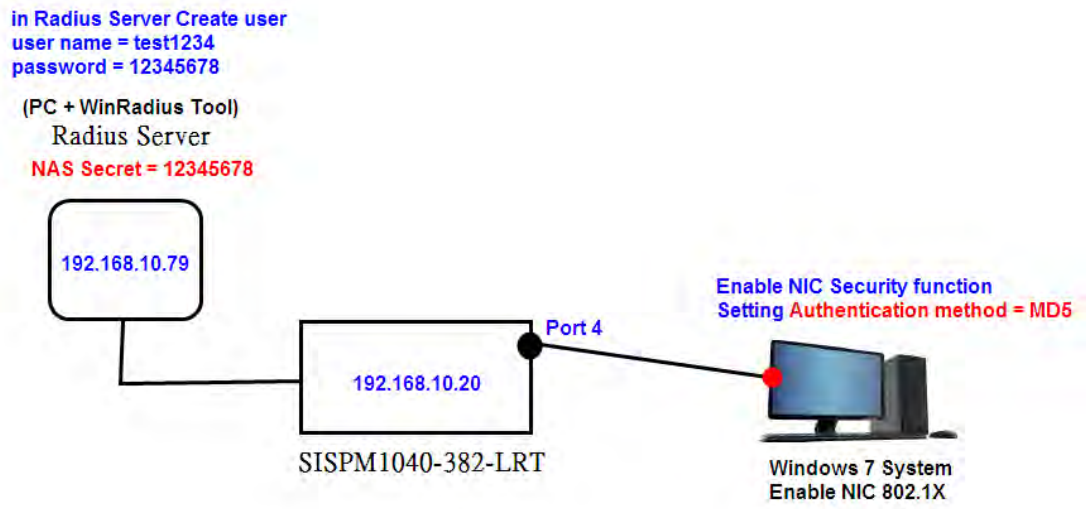
☑ Remember my credentials for this connection each time I'm logged on

☑ Fallback to unauthorized network access

b. In the **Choose a network authentication method** list, click the method you want to use. To configure additional settings, click **Settings**.

Appendix B - RADIUS - Windows 7 Wired AutoConfig

This section provides a procedure fo configuring RADIUS in Windows 7 using Wired AutoConfig. Windows Wired AutoConfig (dot3svc) is a service that configures (IEEE 802.1X port-based security settings on IEEE 802.3 Ethernet adapters.



1. Radius Server Setting

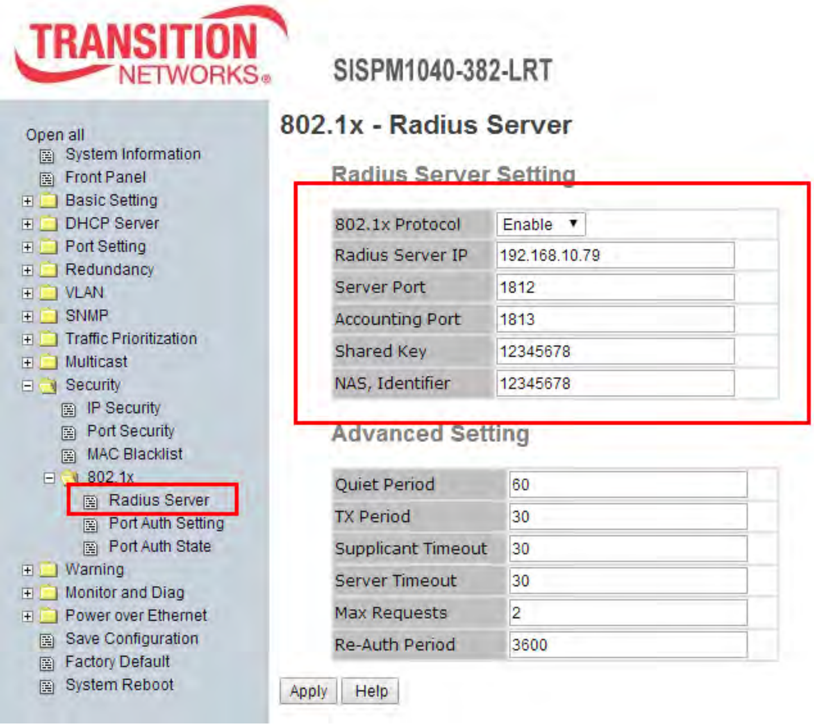
Create a new user:

- □ User name = test1234
- □ Password = 12345678
- □ Shared key = 12345678 (need the same switch settings)
- □ NAS Secret = 12345678 (need the same switch settings)

2. Switch Radius Setting

Use the switch with all default settings except Setting Radius Server settings as below:

- □ 802.1x Protocol = enable
- □ Radius Server IP = 192.168.10.79
- □ Shared key = 12345678 (need the same Radius Server settings)
- □ NAS Secret = 12345678 (need the same Radius Server setting)



802.1x - Radius Server

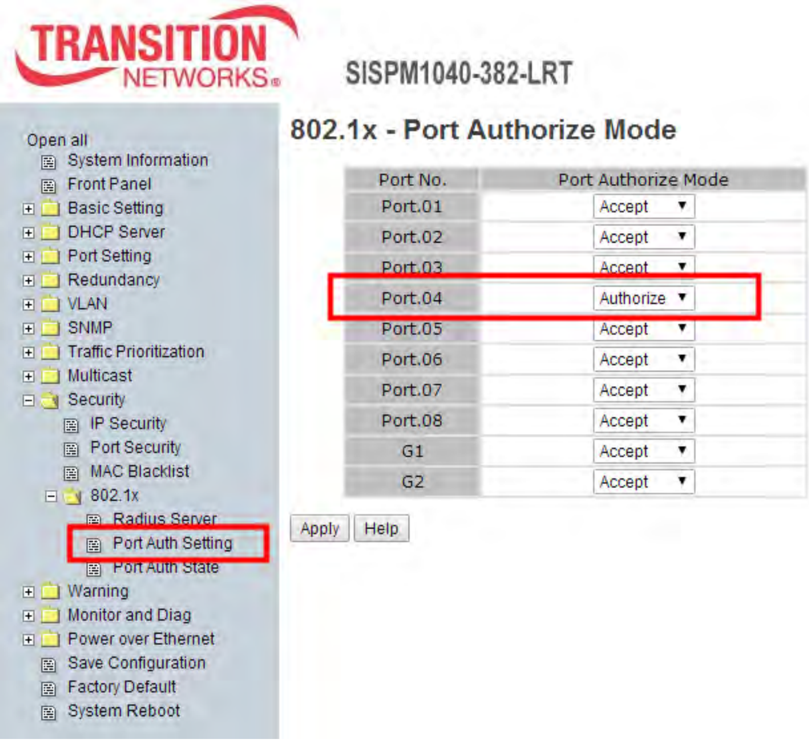
Radius Server Setting

802.1x Protocol	Enable
Radius Server IP	192.168.10.79
Server Port	1812
Accounting Port	1813
Shared Key	12345678
NAS, Identifier	12345678

Advanced Setting

Quiet Period	60
TX Period	30
Supplicant Timeout	30
Server Timeout	30
Max Requests	2
Re-Auth Period	3600

3. Connect Port 4 to Client PC; on Port 04 set Port Authorize Mode to **Authorize** and click the **Apply** button:



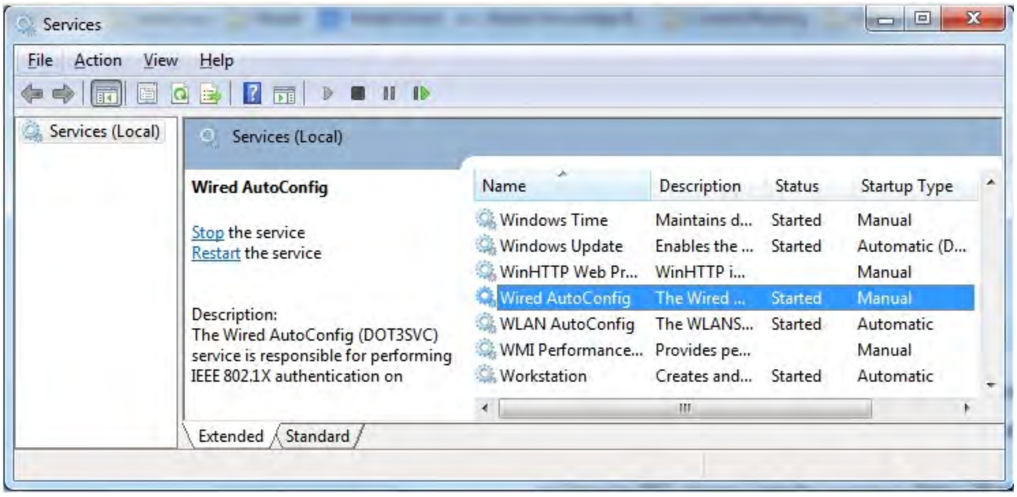
802.1x - Port Authorize Mode

Port No.	Port Authorize Mode
Port.01	Accept
Port.02	Accept
Port.03	Accept
Port.04	Authorize
Port.05	Accept
Port.06	Accept
Port.07	Accept
Port.08	Accept
G1	Accept
G2	Accept

4. Client User Setting (Windows 7)

Enable Wired AutoConfig on your Computer

- Click the Windows Start button and type services.msc into the search box.
- In the services window locate the service named Wired AutoConfig.
- Right click on this service and click on properties.



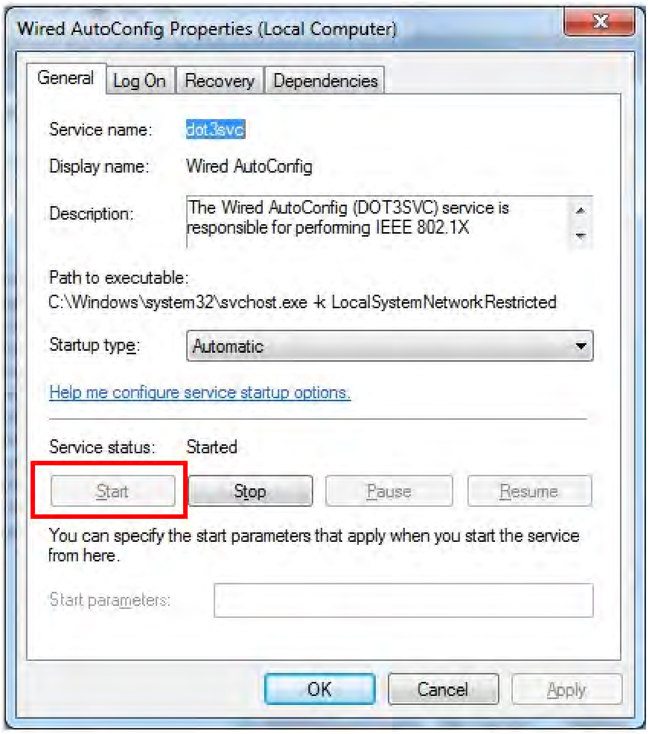
Wired AutoConfig

Stop the service
Restart the service

Description:
The Wired AutoConfig (DOT3SVC) service is responsible for performing IEEE 802.1X authentication on

Name	Description	Status	Startup Type
Windows Time	Maintains d...	Started	Manual
Windows Update	Enables the ...	Started	Automatic (D...
WinHTTP Web Pr...	WinHTTP i...		Manual
Wired AutoConfig	The Wired ...	Started	Manual
WLAN AutoConfig	The WLANS...	Started	Automatic
WMI Performance...	Provides pe...		Manual
Workstation	Creates and...	Started	Automatic

- Start this Service.


Wired AutoConfig Properties (Local Computer)
General
Log On
Recovery
Dependencies
Help me configure service startup options.
Start
Stop
Pause
Resume
OK
Cancel
Apply

Service name: dot3svc

Display name: Wired AutoConfig

Description: The Wired AutoConfig (DOT3SVC) service is responsible for performing IEEE 802.1X

Path to executable:
C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted

Startup type: Automatic

Service status: Started

You can specify the start parameters that apply when you start the service from here.

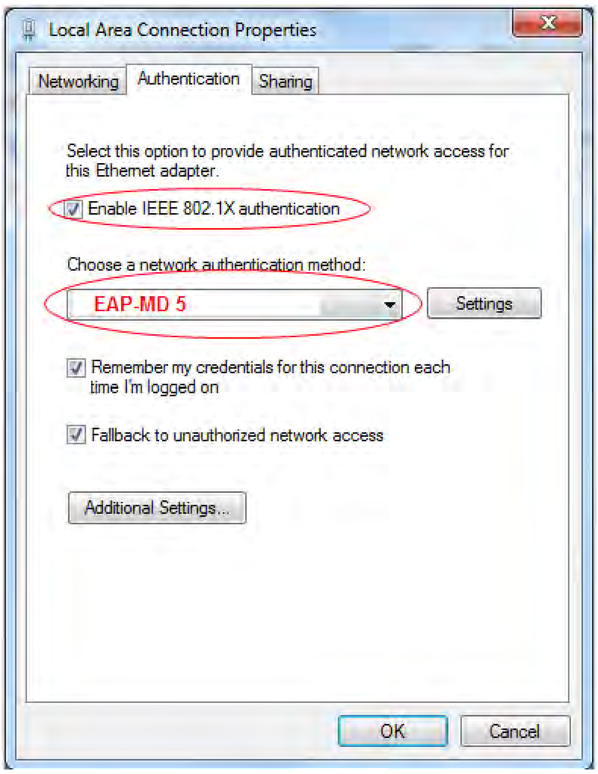
Start parameters:

5. Configure the Local LAN connection for 802.1X authentication

・Right click on your network adapter and select Properties.

・Click on the Authentication tab and select the option for IEEE 802.1X authentication.

・Choose the network authentication method Microsoft: EAP-**MD5**:



Local Area Connection Properties

Select this option to provide authenticated network access for this Ethernet adapter.

☑ Enable IEEE 802.1X authentication

Choose a network authentication method:

EAP-MD 5

☑ Remember my credentials for this connection each time I'm logged on

☑ Fallback to unauthorized network access

Transition Networks
10900 Red Circle Drive
Minnetonka, MN 55343 USA
tel: 952- 941-7600 or 1-800-526-9267
fax: 952-941-2322

SISPM1040-382-LRT Industrial 10-port Managed PoE Ethernet Switch User Guide