User Manual
GFK-3128A
Jan 2020

SLM162

INDUSTRIAL MANAGED ETHERNET SWITCH
USER'S MANUAL, GFK-SLM162CNTEP

EMERSON

Contents

Warnings, Notes as Used in this Publication

Warning

Warning notices are used in this publication to emphasize that hazardous voltages, currents, temperatures, or other conditions that could cause personal injury exist in this equipment or may be associated with its use.
In situations where inattention could cause either personal injury or damage to equipment, a Warning notice is used.

Notes: Notes merely call attention to information that is especially significant to understanding and operating the equipment.

These instructions do not purport to cover all details or variations in equipment, nor to provide for every possible contingency to be met during installation, operation, and maintenance. The information is supplied for informational purposes only, and Emerson makes no warranty as to the accuracy of the information included herein. Changes, modifications, and/or improvements to equipment and specifications are made periodically and these changes may or may not be reflected herein. It is understood that Emerson may make changes, modifications, or improvements to the equipment referenced herein or to the document itself at any time. This document is intended for trained personnel familiar with the Emerson products referenced herein.

Emerson may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not provide any license whatsoever to any of these patents.

Emerson provides the following document and the information included therein as-is and without warranty of any kind, expressed or implied, including but not limited to any implied statutory warranty of merchantability or fitness for particular purpose.

Chapter 1:Getting to Know Your Switch

1.1 About the SLM162 Managed Industrial Switch

The SLM162 is powerful managed industrial switch with many features. This switch can work under wide temperature, dusty environment and humid condition.

The SLM162can be managed by WEB, Console or other third-party SNMP software as well. Besides, these switches can be managed by a useful utility that we called PACSystems Ethernet Switch Configuration Tool. which is powerful network management software. With its friendly and powerful interface, you can easily configure multiple switches at the same time, and monitor switches' status.

1.2 Software Features

- World's fastest Redundant Ethernet Ring: Redundant Ring (Recovery time < 10ms over 250 units connection)
- Supports Ring Coupling, Dual Homing over Redundant Ring
- Supports SNMPv1/v2/v3 & RMON & Port base/802.1Q VLAN Network Management
- Event notification by Email, SNMP trap and Relay Output
- Web-based, Console (CLI) configuration
- Enable/disable ports, MAC based port security
- Port based network access control (802.1x)
- VLAN (802.1Q) to segregate and secure network traffic
- Radius centralized password management
- SNMPv3 encrypted authentication and access security
- RSTP (802.1w)
- Quality of Service (802.1p) for real-time traffic
- VLAN (802.1Q) with double tagging and GVRP supported
- IGMP Snooping for multicast filtering
- Port configuration, status, statistics, mirroring, security

1.3 Hardware Features

- Redundant two DC power inputs
- Wide Operating Temperature: -40 to 70oC
- Storage Temperature: -40 to 85oC
- Operating Humidity: 5% to 95%, non-condensing
- Casing: IP-30
- 100/1000BaseX SFP Port
- 1000BaseX SFP Port

- Console Port
- Dimensions 96.4mm(W)X108.5mm(D)X154mm(H)

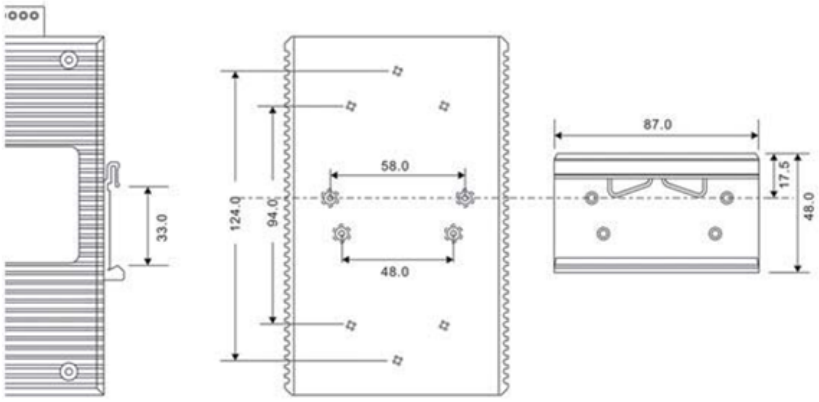
Chapter 2: Hardware Installation

2.1 Installing Switch on DIN-Rail

Each switch has a DIN-Rail kit on rear panel. The DIN-Rail kit helps switch to fix on the DIN-Rail. It is easy to install the switch on the DIN-Rail:

2.1.1 Mount Switch on DIN-Rail

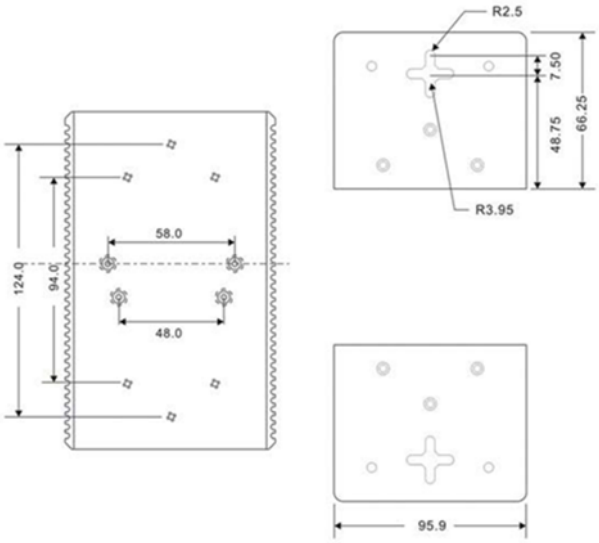
Figure 1 DIN-Rail Size



2.2 Wall Mounting Installation

Each switch has another installation method for users to fix the switch. A wall mount panel can be found in the package. The following steps show how to mount the switch on the wall:

Figure 2 Wall-Mounting size



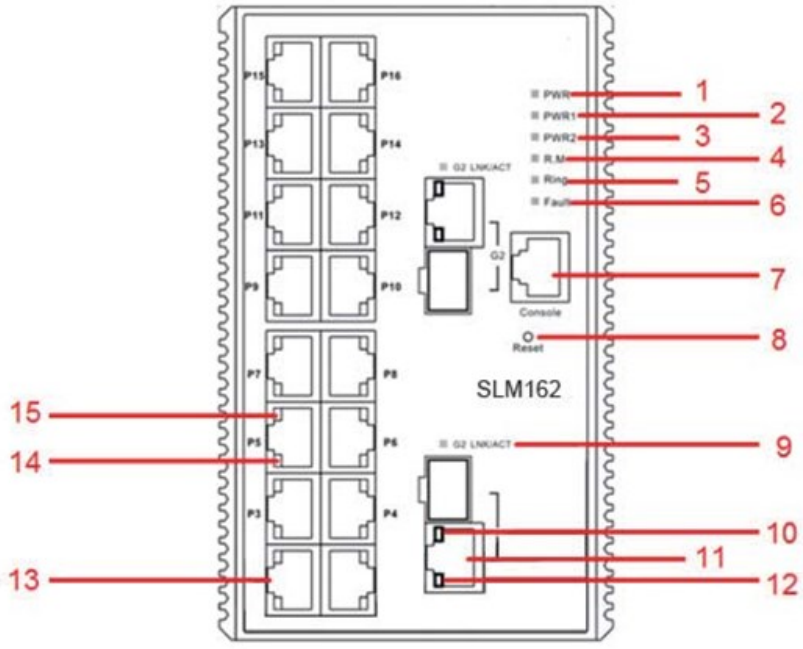
Chapter 3: Hardware Overview

3.1 Front Panel

The following table describes the labels that stick on the Switch

Port	Description
10/100 RJ-45 fast Ethernet ports	10/100Base-T(X) RJ-45 fast Ethernet ports support auto-negotiation. Default Setting : Speed: auto Duplex: auto Flow control : disable
SFP port	100/1000Base-X
Console	Use RS-232 to RJ-45 connecter to manage switch.
Reset	Push reset button 2 to 3 seconds to reset the switch. Push reset button 5 seconds to reset the switch into Factory Default .

Figure 3 SLM162



1. LED for PWR. When the PWR links, the green led will be light on.
2. Led for PWR1 when the PWR1 links, the green led will be light on
3. Led for PWR2 when the PWR2 links, the green led will be light on
4. LED for R.M (Ring master). When the LED light on, it means that the switch is the ring master of Ring. LED for Ring.
5. When the led light on, it means the Ring is activated.
6. LED for Fault Relay. When the fault occurs, the amber LED will be light on.
7. Console port (RJ-45).
8. Reset button. Push the button 3 seconds for reset; 5 seconds for factory default.
9. 1000 Combo ports LED with SFP.
10. 1000 Combo Port ACT/Link LED.
11. 1000 Combo Port.
12. 1000 Combo Port Duplex LED.
13. 10/100 COPPER Port.
14. 10/100 Port Duplex LED.
15. 10/100 Port ACT/Link LED.

3.2 Front Panel LEDs

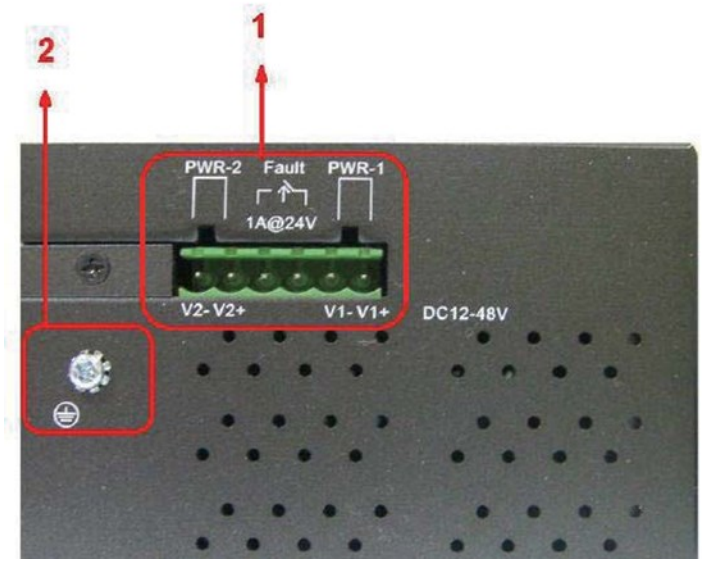
LED	Color	Status	Description
PW1	Green	On	DC power module 1 activated.
PW2	Green	On	DC power module 2 activated.
R.M	Green	On	Redundant Ring Master.
Ring	Green	On	Redundant Ring enabled.
		Slowly blinking	Redundant Ring topology has problem
		Fast blinking	Redundant Ring work normally.
Fault	Amber	On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

3.3 Top view Panel

The bottom panel components of SLM162 are shown as below:

1. Terminal block includes: PWR1, PWR2 (12-48V DC) and Relay output (1A@24VDC).

Figure 4



Chapter 4: Cables

4.1 Ethernet Cables

The SLM162 switches hasve 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). Please refer to the following table for cable specifications.

Table 1 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

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.

Table 2 RJ-45 Pin Assignments

Pin Number	Assignment
1	TD+
2	TD-
3	RD+
4	Not used
5	Not used
6	RD-
7	Not used
8	Not used

The SLM162 switches support auto MDI/MDI-X operation. You can use a straight-through cable to connect PC to switch. The following table below shows the 10BASE-T/ 100BASE-TX MDI and MDI-X port pin outs.

Table 3 10/100 Base-TX MDI/MDI-X pins assignment

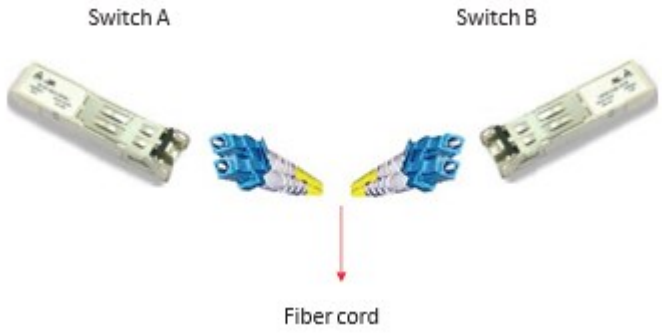
Pin Number	MDI port	MDI-X port
1	TD+(transmit)	RD+(receive)
2	TD-(transmit)	RD-(receive)
3	RD+(receive)	TD+(transmit)
4	Not used	Not used
5	Not used	Not used
6	RD-(receive)	TD-(transmit)
7	Not used	Not used
8	Not used	Not used

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

4.2 SFP

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. Please remember that the TX port of Switch A should be connected to the RX port of Switch B.

Figure 5

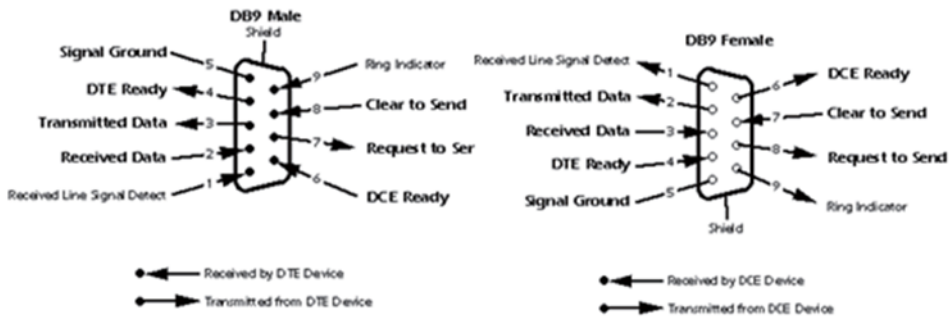


4.3 Console Cable

SLM162switches can be management by console port . The DB-9 to RJ-45 cable can be found in the package. You can connect them to PC via a RS-232 cable with DB-9 female connector and the other end (RJ-45 connector) connects to console port of switch.

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

Figure 6



Chapter 5: WEB Management

⚠ WARNING

While marking any establishment and upgrading firmware, please remove physical loop connection first.

DO NOT power off equipment during firmware is upgrading!

5.1 Configuration by Web Browser

This section introduces the configuration by Web browser.

5.1.1 About Web-based Management

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

The Web-Based Management function supports Internet Explorer 5.0 or later. It is based on Java Applets with an aim to reduce network bandwidth consumption, enhance access speed and present an easy viewing screen.

Note: *By default , IE5.0 or later version does not allow Java Applets to open sockets. You need to explicitly modify the browser setting in order to enable Java Applets to use network ports. And also the switch can support the HTTP and HTTPs mode at the same time, you can use any mode to manage switch.*

Preparing for Web Management

The default value is as below: IP Address: 192.168.0.100

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.0.254

User Name: admin

Password: admin

System Login

1. Launch the Internet Explorer.
2. Type http:// or https:// and the IP address of the switch. Press “Enter”.

Figure 7

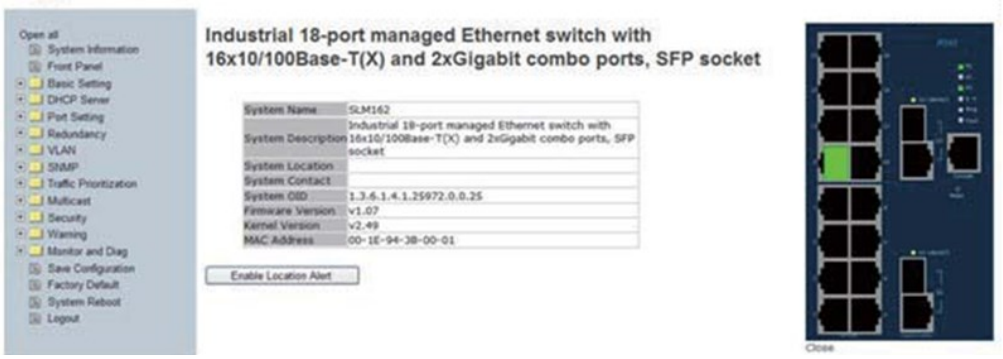
3. The login screen appears.
4. Key in the username and password. The default username and password is “admin”.

5. Click “Enter” or”OK” button, then the main interface of the Web-based management appears.

Figure 8 Login screen

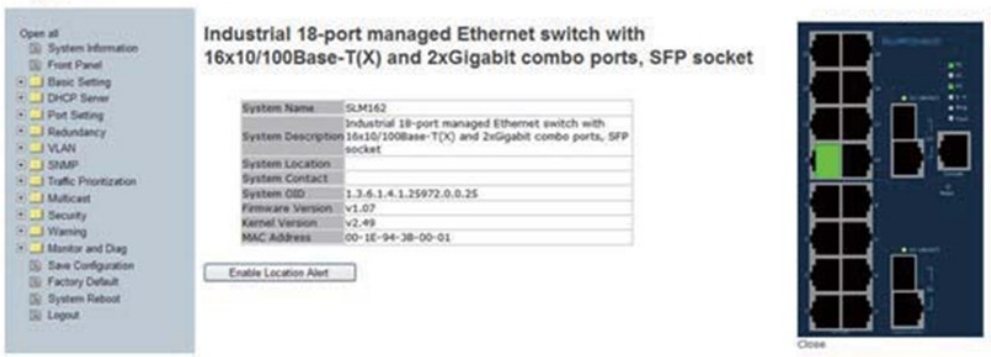
Main Interface

Figure 9 Main Interface



5.1.2 System Information

Figure 10 System Information interface



System Information

The system information will display the basic configuration and the switch panel status

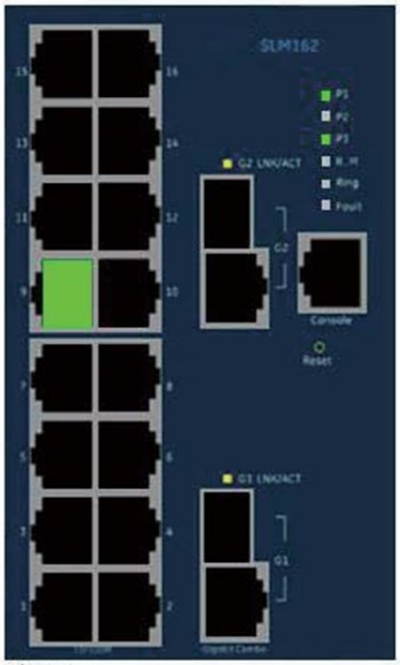
Enable Location Alert

When click Enable Location Alert PWR1 and PWR2 LEDs of the switch will start to flash to flash together, and click Disable Location Alert , the LEDs will stop flashing.

5.1.3 Front Panel

Front Panel Show the panel of switch, Click “Close” to close panel on web.

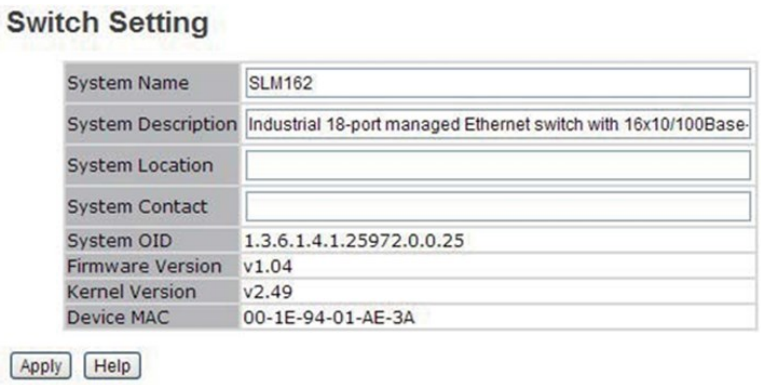
Figure 11



5.1.4 Basic setting

Switch Setting

Figure 12 Switch setting interface



The following table describes the labels in this screen.

Label	Description
System Name	Assign the name of switch. The maximum length is 64 bytes
System Description	Display the description of switch.
System Location	Assign the switch physical location. The maximum length is 64 bytes
System Contact	Enter the name of contact person or organization
System OID	Display the SNMP Object ID of enterprise private MIB.
Firmware Version	Display the switch's firmware version
Kernel Version	Display the kernel software version
MAC Address	Display the unique hardware address assigned by manufacturer (default)

Admin Password

Change web management login username and password for the management security issue.

Figure 13 Admin Password interface

The following table describes the labels in this screen.

Label	Description
Old Username	Enter the current system Username. If this is incorrect, the new Username will not be set.
Old Password	Enter the current system password. If this is incorrect, the new password will not be set.
New Username	Enter the new system Username
New Password	Enter the new system password, and the password must meet the requirement: Minimum 8 characters; At least one Upper case letter. At least one numeric character. At least one special character such as @, #, $,
Confirm password	Re-type the new password.
Save	Click to save changes.

IP Setting

You can configure the IP Settings and DHCP client function through IP configuration

Figure 14 IP Configuration interface

The following table describes the labels in this screen.

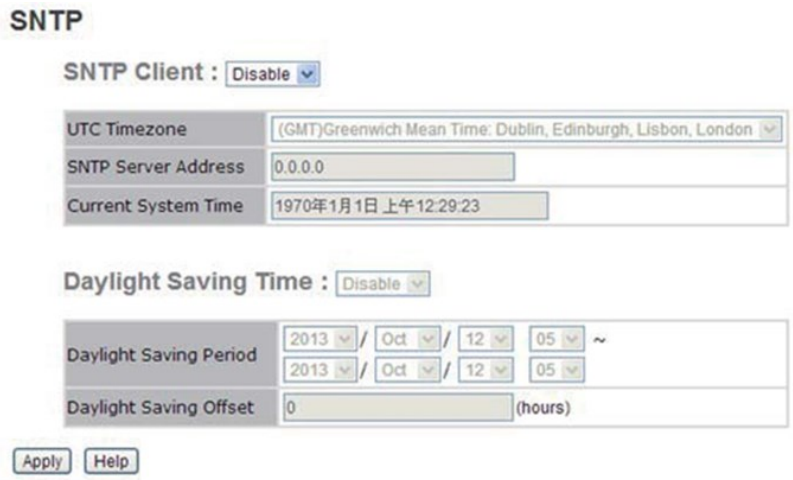
Label	Description
DHCP Client	To enable or disable the DHCP client function. When DHCP client function is enabling, the switch will be assigned the IP address from the network DHCP server. The default IP address will be replaced by the IP address which the DHCP server has assigned. After clicking “Apply” button, a popup dialog shows up to inform when the DHCP client is enabling. The current IP will lose, and you should find a new IP on the DHCP server.
IP Address	Assign the IP address that the network is using. If DHCP client function is enabling, you do not need to assign the IP address. The network DHCP server will assign the IP address for the switch and it will be display in this column. The default IP is 192.168.0.100
Subnet Mask	Assign the subnet mask of the IP address. If DHCP client function is enabling, you do not need to assign the subnet mask

Label	Description
Gateway	Assign the network gateway for the switch. The default gateway is 192.168.0.254
DNS1	Assign the primary DNS IP address
DNS2	Assign the secondary DNS IP address
Apply	Click “Apply” to activate the configurations.

SNTP

The SNTP (Simple Network Time Protocol) settings allow you to synchronize switch clocks in the Internet.

Figure 15 SNTP Configuration interface



The following table describes the labels in this screen.

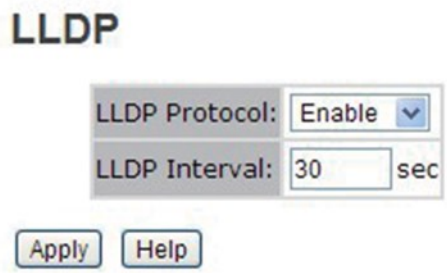
Label	Description
SNTP Client	Enable or disable SNTP function to get the time from the SNTP server.
UTC Time zone	Set the switch location time zone. The following table lists the different location time zone for your reference.
SNTP Sever Address	Set the SNTP server IP address.
Current System Time	Display the switch current time.
Daylight Saving Time	Enable or disable daylight saving time function. When daylight saving time is enabling, you need to configure the daylight-saving time period.
Daylight Saving Period	Set up the Daylight-Saving beginning time and Daylight-Saving ending time. Both will be different each year.
Daylight Saving Offset	Set up the offset time.
Apply	Click “Apply” to activate the configurations.

Local Time Zone	Conversion from UTC	Time at 12:00
November Time Zone	- 1 hour	11 am
Oscar Time Zone	-2 hours	10 am
ADT - Atlantic Daylight	-3 hours	9 am
AST - Atlantic Standard EDT - Eastern Daylight	-4 hours	8 am
EST - Eastern Standard CDT - Central Daylight	-5 hours	7 am
CST - Central Standard MDT - Mountain Daylight	-6 hours	6 am
MST - Mountain Standard PDT - Pacific Daylight	-7 hours	5 am
PST - Pacific Standard ADT - Alaskan Daylight	-8 hours	4 am
ALA - Alaskan Standard	-9 hours	3 am
HAW - Hawaiian Standard	-10 hours	2 am
Nome, Alaska	-11 hours	1 am
CET - Central European FWT - French Winter MET - Middle European MEWT - Middle European Winter SWT - Swedish Winter	+1 hour	1 pm
EET - Eastern European, USSR Zone 1	+2 hours	2 pm
BT - Baghdad, USSR Zone 2	+3 hours	3 pm
ZP4 - USSR Zone 3	+4 hours	4 pm
ZP5 - USSR Zone 4	+5 hours	5 pm
ZP6 - USSR Zone 5	+6 hours	6 pm
WAST - West Australian Standard	+7 hours	7 pm
CCT - China Coast, USSR Zone 7	+8 hours	8 pm
JST - Japan Standard, USSR Zone 8	+9 hours	9 pm
EAST - East Australian Standard GST Guam Standard, USSR Zone 9	+10 hours	10 pm
IDLE - International Date Line NZST - New Zealand Standard NZT - New Zealand	+12 hours	Midnight

LLDP

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

Figure 16 LLDP Configuration Interface



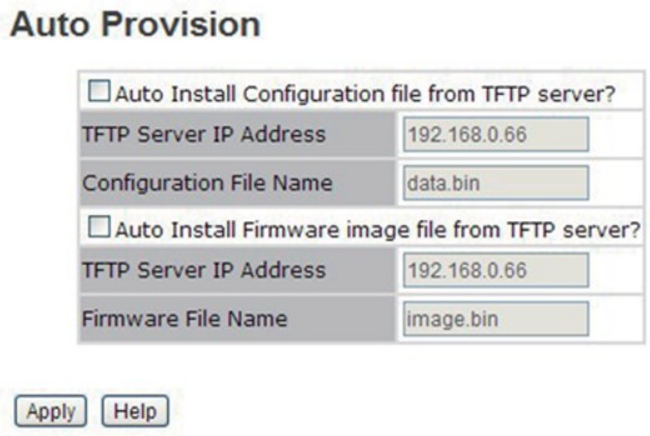
The following table describes the labels in this screen.

Label	Description
LLDP Protocol	"Enable" or "Disable" LLDP function.
LLDP Interval	The interval of resend LLDP (by default at 30 seconds)
Apply	Click "Apply" to set the configurations.
Help	Show Help File.

Auto Provision

Auto Provision allows you to update the switch firmware automatically. You can put firmware or configuration file on 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 is on the TFTP server.

Figure 17 Auto Provision interface



The following table describes the labels in this screen.

Label	Description
TFTP Server IP Address	Fill in the TFTP server IP
Configuration File Name	Fill the configuration file name.
Firmware File Name	Fill the Firmware file name.

Backup & Restore

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

Figure 18 Backup & Restore interface

The following table describes the labels in this screen.

Label	Description
TFTP Server IP Address	Fill in the TFTP server IP
Restore File Name	Fill the file name.
Restore	Click “restore” to restore the configurations.
Backup File Name	Fill the configuration file name.
Backup	Click “backup” to back up the configurations.

Upgrade Firmware

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

Figure 19 Update Firmware interface

The following table describes the labels in this screen.

Label	Description
TFTP Server IP Address	Fill in the TFTP server IP
Firmware File Name	Fill the Firmware file name.
Upgrade	Click “Upgrade” to update the Firmware

5.1.5 DHCP Server

DHCP Server – Setting

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

Figure 20 DHCP Server Configuration interface

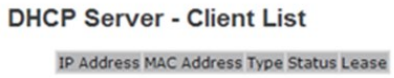
The following table describes the labels in this screen.

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

DHCP Server – Client List

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

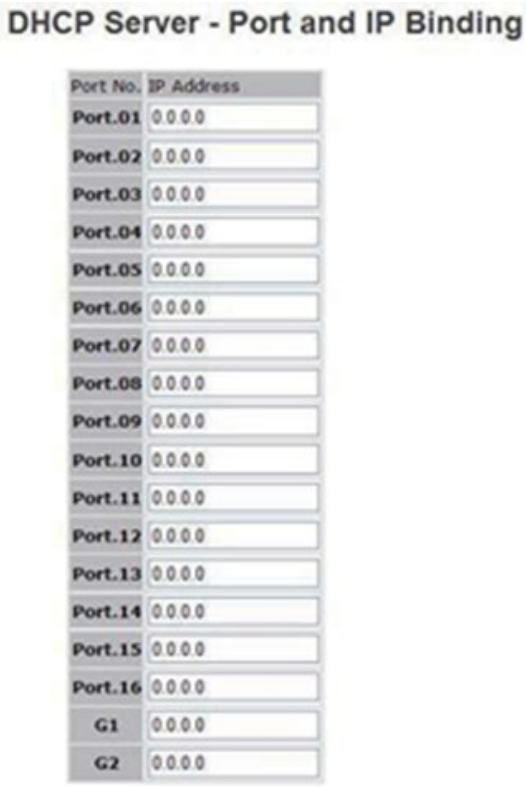
Figure 21 DHCP Server Client Entries interface



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 in the connected device.

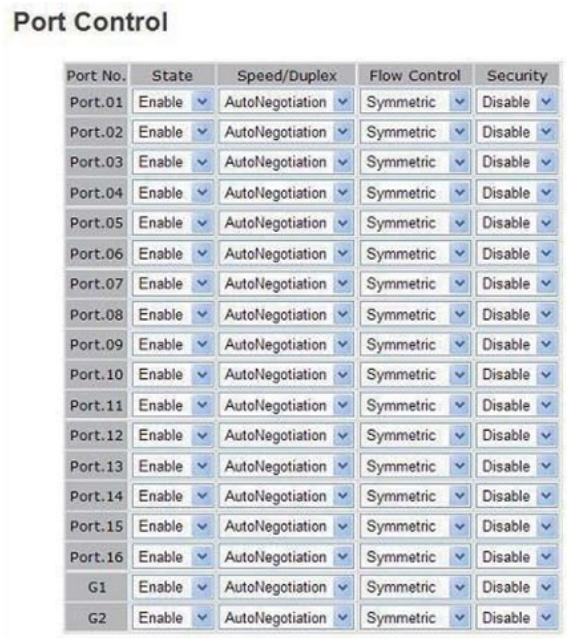
Figure 22



5.1.6 Port Setting

Port Control

Figure 23 Port Control interface



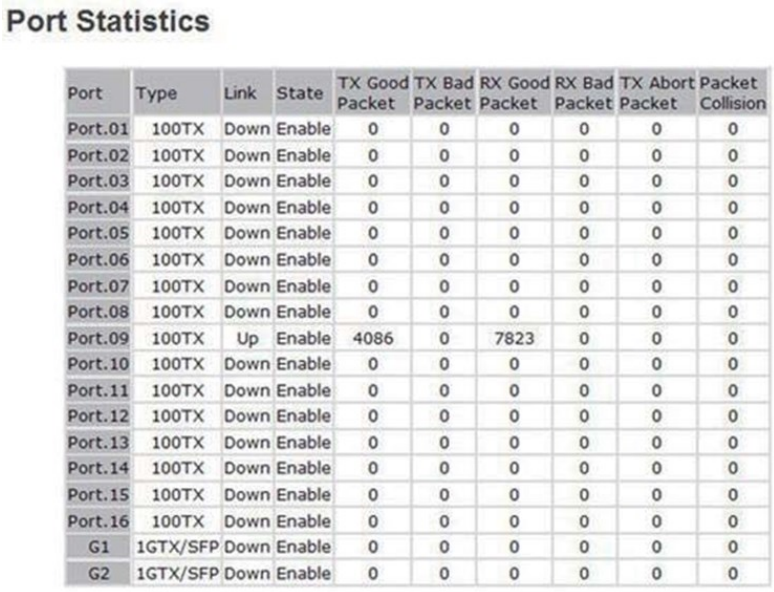
The following table describes the labels in this screen.

Label	Description
Port NO.	Port number for setting.
State	Enable/Disable the port.
Speed/Duplex	You can set Auto-negotiation, 100-full, 100-half, 10-full, 10-half mode.
Flow Control	Support symmetric and asymmetric mode to avoid packet loss when congestion occurred.
Security	Enabled port security will disable MAC address learning in this port. Thus, only the frames with MAC addresses in port security list will be forwarded, otherwise will be discarded.
Apply	Click “Apply” to activate the configurations.

Port Status

The following information provides the current port status information

Figure 24 Port Status interface



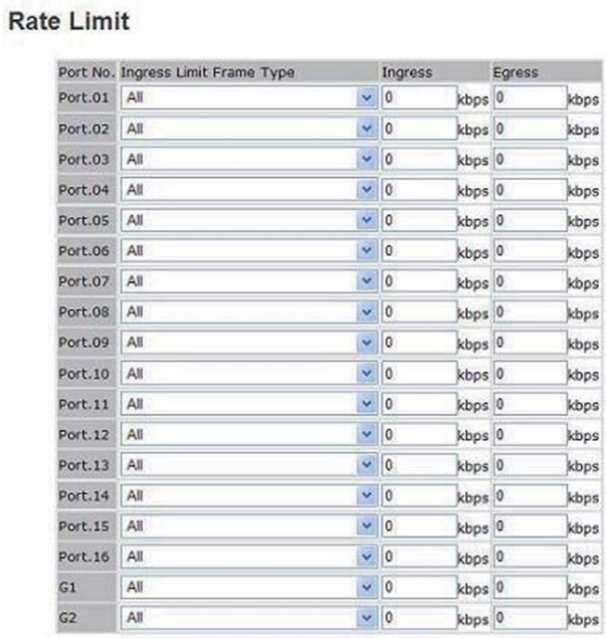
Port Statistics

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	Enable	0	0	0	0	0	0
Port.02	100TX	Down	Enable	0	0	0	0	0	0
Port.03	100TX	Down	Enable	0	0	0	0	0	0
Port.04	100TX	Down	Enable	0	0	0	0	0	0
Port.05	100TX	Down	Enable	0	0	0	0	0	0
Port.06	100TX	Down	Enable	0	0	0	0	0	0
Port.07	100TX	Down	Enable	0	0	0	0	0	0
Port.08	100TX	Down	Enable	0	0	0	0	0	0
Port.09	100TX	Up	Enable	4086	0	7823	0	0	0
Port.10	100TX	Down	Enable	0	0	0	0	0	0
Port.11	100TX	Down	Enable	0	0	0	0	0	0
Port.12	100TX	Down	Enable	0	0	0	0	0	0
Port.13	100TX	Down	Enable	0	0	0	0	0	0
Port.14	100TX	Down	Enable	0	0	0	0	0	0
Port.15	100TX	Down	Enable	0	0	0	0	0	0
Port.16	100TX	Down	Enable	0	0	0	0	0	0
G1	1GTX/SFP	Down	Enable	0	0	0	0	0	0
G2	1GTX/SFP	Down	Enable	0	0	0	0	0	0

Rate Limit

By this function, you can limit traffic of all ports, including Broadcast, Multicast and flooded Unicast , You can also set “Ingress” or “Egress” to limit traffic received or transmitted bandwidth.

Figure 25 Rate Limit interface



Rate Limit

Port No.	Ingress Limit Frame Type	Ingress		Egress	
Port.01	All	0	kbps	0	kbps
Port.02	All	0	kbps	0	kbps
Port.03	All	0	kbps	0	kbps
Port.04	All	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
Port.09	All	0	kbps	0	kbps
Port.10	All	0	kbps	0	kbps
Port.11	All	0	kbps	0	kbps
Port.12	All	0	kbps	0	kbps
Port.13	All	0	kbps	0	kbps
Port.14	All	0	kbps	0	kbps
Port.15	All	0	kbps	0	kbps
Port.16	All	0	kbps	0	kbps
G1	All	0	kbps	0	kbps
G2	All	0	kbps	0	kbps

The following table describes the labels in this screen.

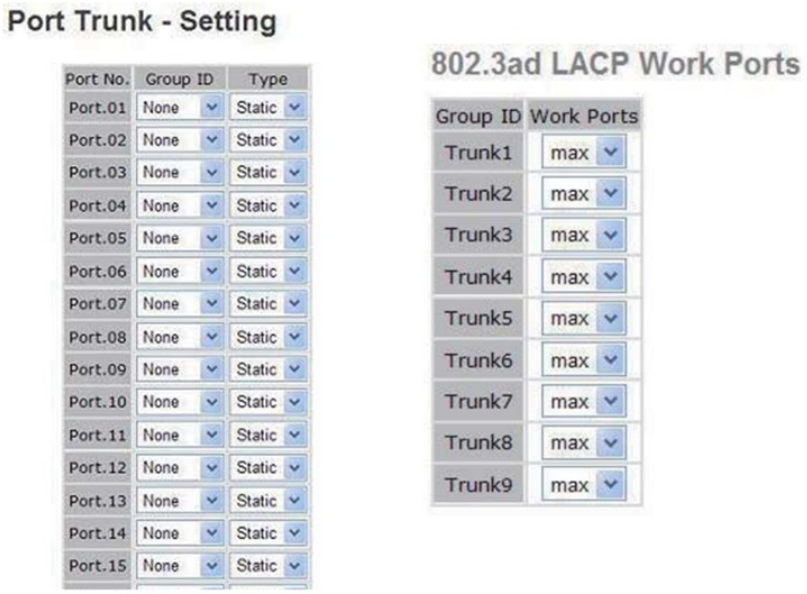
Label	Description
Ingress Limit Frame Type	You can set “all”, “Broadcast only”,”Broadcast/Multicast” or ”Broadcast/Multicast/Flooded Unicast” mode.
Ingress	The switch port received traffic.
Egress	The switch port transmitted traffic.
Apply	Click “Apply” to activate the configurations.

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.

Figure 26 Port Trunk - Setting interface



The following table describes the labels in this screen.

Label	Description
Group ID	Select port to join a trunk group.
Type	Support static trunk and 802.3ad LACP
Work Port	Select the number of active ports in dynamic group (L ACP). The default value of works ports is maximum number of the group. If the number is not maximum number of ports, the other inactive ports in dynamic group will be suspended (no traffic). Once the active port is broken, the suspended port will be active automatically.
Apply	Click “Apply” to set the configurations.

Port Trunk – Status

Figure 27 Port Trunk - Status interface

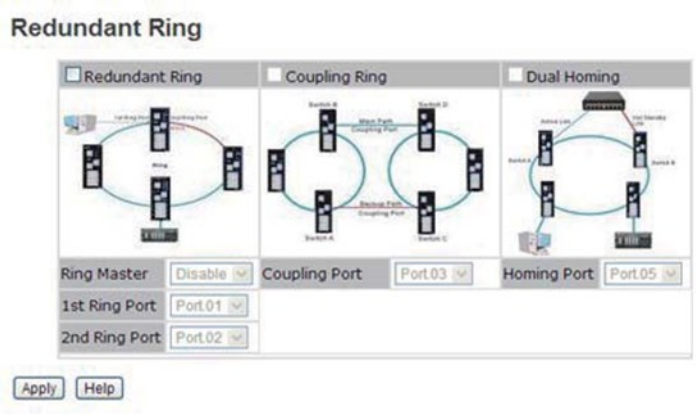
Label	Description
Group ID	Trunk Group number
Port Member	Show Group port Info

5.1.7 Redundancy

Redundant Ring

Redundant Ring is the most powerful Ring in the world. The recovery time of Ring is less than 10ms. It can reduce unexpected damage caused by network topology change. Redundant Ring Supports 3 Ring topology: Ring, Coupling Ring and Dual Homing.

Figure 28



The following table describes the labels in this screen.

Label	Description
Redundant Ring	Mark to enable Ring.
Ring Master	There should be one and only one Ring Master in a ring. However if there are two or more switches which set Ring Master to enable, the switch with the lowest MAC address will be the actual Ring Master and others will be Backup Masters.
1stRingPort	The primary port, when this switch is Ring Master.
2ndRingPort	The backup port, when this switch is Ring Master.

Label	Description
Coupling Ring	Mark to enable Coupling Ring. Coupling Ring can be used to divide a big ring into two smaller rings to avoid effecting all switches when network topology change. It is a good application for connecting two Rings.
Coupling Port	Link to Coupling Port of the switch in another ring. Coupling Ring need four switch to build an active and a backup link. Set a por t as coupling port. The coupled four ports of four switches will be run at active/backup mode.
Dual Homing	Mark to enable Dual Homing. By selecting Dual Homing mode, Ring will be connected to normal switches through two RSTP links (ex: backbone Switch). The two links work as active/backup mode, and connect each Ring to the normal switches in RSTP mode.
Apply	Click “Apply” to set the configurations.

Note: *We don’t suggest you to set one switch as a Ring Master and a Coupling Ring at the same time due to heavy load.*

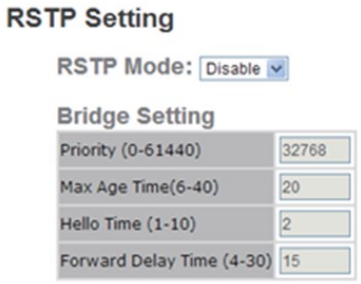
RSTP

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 setting

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

Figure 29 RSTP Setting Interface



The following table describes the labels in this screen.

Label	Description
RSTP mode	You must enable or disable RSTP function before configuring the related parameters.
Priority (0-61440)	A value used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root . If the value changes, You must reboot the switch. The value must be multiple of 4096 according to the protocol standard rule.

Label	Description
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 through 40.
Hello Time (1-10)	The time that controls switch sends out the BPDU packet to check RSTP current status. Enter a value between 1 through 10.
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 through 30.
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)

Figure 30

The following table describes the labels in this screen.

Label	Description
Path Cost (1-200000000)	The cost of the path to the other (GFK-SLM162CNTEP) bridge from this transmitting bridge at the specified port. Enter a number 1 through
Port Priority (0-240)	Decide which port should be blocked by priority in LAN. Enter a number 0 through 240. The value of priority must be the multiple of 16

Label	Description
Admin P2P	Some of the rapid state transactions that are possible within RSTP are dependent upon whether the port concerned can only be connected to exactly one other bridge (i.e. It is served by a point-to-point LAN segment), or 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	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”.
Admin Non STP	The port includes the STP mathematic calculation. True is not including STP mathematic calculation. False is including the STP mathematic calculation.
Apply	Click “Apply” to set the configurations.

5.1.8 VLAN

A Virtual LAN (VLAN) is a logical network grouping that limits the broadcast domain, which allows you to isolate network traffic. Only the members of the VLAN will receive traffic from the same members of VLAN. Basically, creating a VLAN from a switch is logically equivalent of reconnecting a group of network devices to another Layer 2 switch. However, all the network devices are still plugged into the same switch physically.

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

VLAN Setting- IEEE 802.1Q

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

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

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

Figure 31 VLAN Configuration – 802.1Q interface

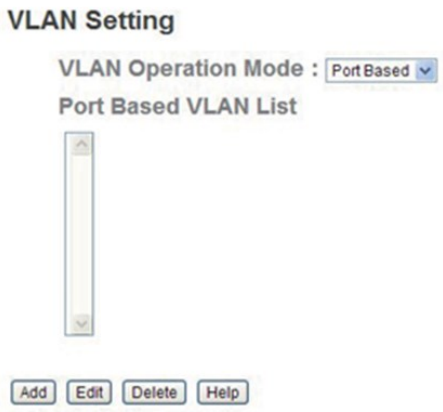
The following table describes the labels in this screen.

Label	Description
VLAN Operation Mode	Configure VLAN Operation Mode: disable, Port Base,802.1Q
GVRP Mode	Enable/Disable GVRP function.
Management VLAN ID	Management VL AN can provide network administrator a secure VLAN to management Switch. Only the devices in the management VLAN can access the switch.
Port	Select the port to configure.
Link type	There are 3 types of link type: Access Link: single switch only, allows you to group ports by setting the same VID. Trunk Link: extended application of Access Link, allows you to group ports by setting the same VID with 2 or more switches. Hybrid Link: Both Access Link and Trunk Link are available. Hybrid (QinQ) Link: enable QinQ mode allow you to insert one more VLAN tag in a original VLAN frame.
Untagged VID	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 another
Apply	Click “Apply” to set the configurations.

VLAN Setting – Port Based

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

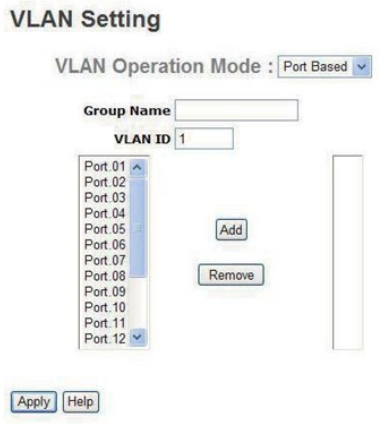
Figure 32 VLAN Configuration – Port Base interface-1



The following table describes the labels in this screen.

Label	Description
Add	Click “add” to enter VLAN add interface.
Edit	Edit exist VLAN
Delete	Delete exist VLANn
Help	Show help file.

Figure 33 VLAN Configuration – Port Base interface-2



The following table describes the labels in this screen.

Label	Description
Group Name	VLAN name.
VLAN ID	Specify the VLAN ID
Add	Select port to join the VLAN group.
Remove	Remove port of the VLAN group
Apply	Click “Apply” to set the configurations.
Help	Show help file.

5.1.9 SNMP

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

SNMP – Agent Setting

You can set SNMP agent related information by Agent Setting Function.

Figure 34 SNMP – Agent setting interface

The following table describes the labels in this screen.

Label	Description
SNMP agent Version	Three SNMP versions are supported such as SNMP V1/SNMP V2c, and SNMP V3. SNMP V1/SNMP V2c agent use a community string match for authentication, that means SNMP ser vers 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.

Label	Description
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.
Apply	Click “Apply” to activate the configurations.
Help	Show help file.

SNMP –Trap Setting

A trap manager is a management station that receives traps, the system alerts generated by the switch. If no trap manager is defined, no traps will issue. Create a trap manager by entering the IP address of the station and a community string. To define management stations as trap manager and enter SNMP community strings and selects the SNMP version.

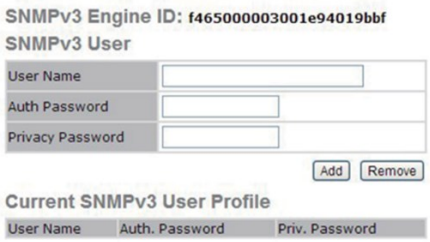
Figure 35 SNMP –Trap Setting interface

The following table describes the labels in this screen.

Label	Description
Server IP	The server IP address to receive Trap
Community	Community for authentication
Trap Version	Trap Version supports V1 and V2c and V3
Add	Add trap server profile.
Remove	Remove trap server profile.
Help	Show help file.

SNMPV3

Figure 36



The following table describes the labels in this screen

Label	Description
Context Table	Configure SNMP v3 context table. Assign the context name of context table. Click "Apply" to change context name
User Table	1. Configure SNMP v3 user table. 2. User ID: set up the user name. 3. Authentication Password: set up the authentication password. 4. Privacy Password: set up the private password. 5. Click "Add" to add context name. 6. 6. Click "Remove" to remove unwanted context name.
Group Table	1. Configure SNMP v3 group table. 2. Security Name (User ID): assign the user name that you have set up in user table. 3. Group Name: set up the group name. 4. Click "Add" to add context name. 5. Click "Remove" to remove unwanted context name.
Access Table	1. Configure SNMP v3 access table. 2. Context Prefix: set up the context name. 3. Group Name: set up the group. 4. Security Level: select the access level. 5. Context Match Rule: select the context match rule. 6. Read View Name: set up the read view. 7. Write View Name: set up the write view. 8. Notify View Name: set up the notify view. 9. Click "Add" to add context name. 10. Click "Remove" to remove unwanted context name.
MIBview Table	1. Configure MIB view table. 2. ViewName: set up the name. 3. Sub-Oid Tree: fill the Sub OID. 4. Type: select the type – exclude or included. 5. Click "Add" to add context name. 6. Click "Remove" to remove unwanted context name.
Help	Show help file.

5.1.10 Traffic Prioritization

Traffic Prioritization includes 3 modes: port base, 802.1p/COS, and TOS/DSCP. By traffic prioritization function, you can classify the traffic into four classes for differential network application.

Qos policy

Figure 37 Traffic Prioritization interface

The following table describes the labels in this screen.

Label	Description
QOS Mode	• Port-base: 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: always the packets in higher queue will be transmitted first until higher queue is empty.
Apply	Click “Apply” to set the configurations.
Help	Show help file.

Port-base priority

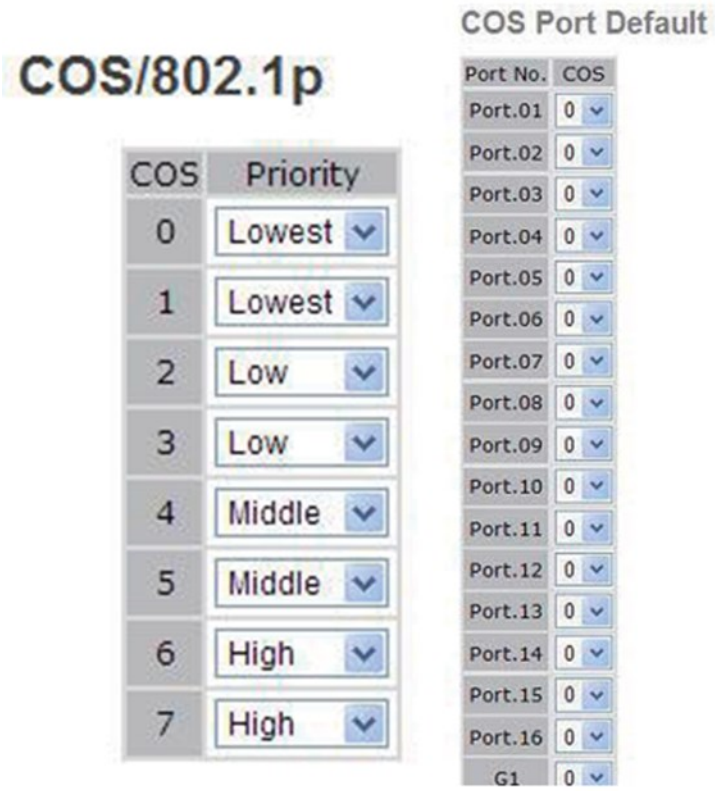
Figure 38 Port-based Priority interface

The following table describes the labels in this screen

Port base Priority	Assign Por t with a priority queue. 4 priority queues can be assigned: High, Middle, Low, and Lowest .
Apply	Click “Apply” to set the configurations.
Help	Show help file.

COS/802.1p

Figure 39



The following table describes the labels in this screen

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 0to7.COS value map to 4 priority queues: High, Middle, Low, and Lowest.
COS Port Default	When an ingress packet has not VLAN tag, a default priority value is considered and determined by ingress port.
Apply	Click “Apply” to set the configurations.
Help	Show help file.

TOS/DSCP

Figure 40 TOS/DSCP interface

The following table describes the labels in this screen

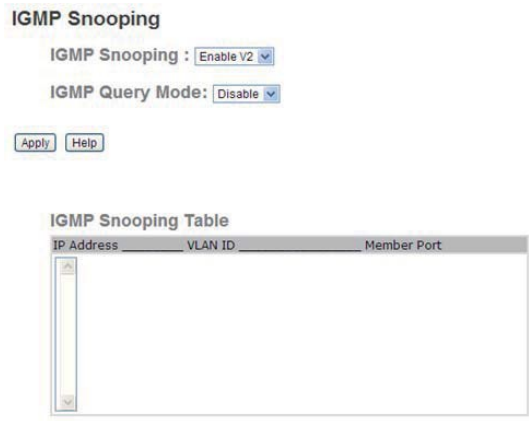
TOS/DSCP	TOS (Type of Service) is a field in IP header of a packet. This TOS field is also used by Differentiated Services and is called the Differentiated Services Code Point (DSCP). The output priority of a packet can be determined by this field and the priority value is supported 0to63. DSCP value map to 4 priority queues: High, Middle, Low, and Lowest.
Apply	Click “Apply” to set the configurations.
Help	Show help file.

5.1.11 Multicast

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. Please refer to RFC 1112, 2236 and 3376. IGMP Snooping improves the performance of networks that carry multicast traffic. It provides the ability to prune multicast traffic so that it travels only to those end destinations that require that traffic and reduces the amount of traffic on the Ethernet LAN.

Figure 41 IGMP Snooping interface



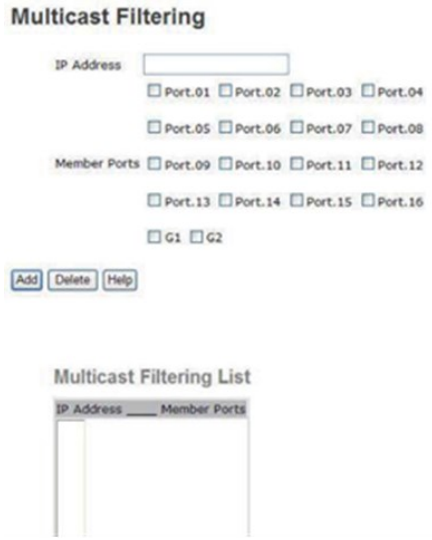
The following table describes the labels in this screen.

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

Static Multicast Filtering

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

Figure 42 Multicast Filtering Interface



The following table describes the labels in this screen.

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

5.1.12 Security

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

IP Security

Only IP in the Secure IP List can manage the switch through your defined management mode. (WEB, SNMP)

Figure 43 IP Security interface

The following table describes the labels in this screen.

Label	Description
IP security MODE	Enable/Disable the IP security function.
Enable WEB Management	Mark the blank to enable WEB Management.
Enable SNMP Management	Mark the blank to enable SNMP Management.
Apply	Click “Apply” to set the configurations.
Help	Show help file.

Port Security

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

Figure 44 Port Security interface

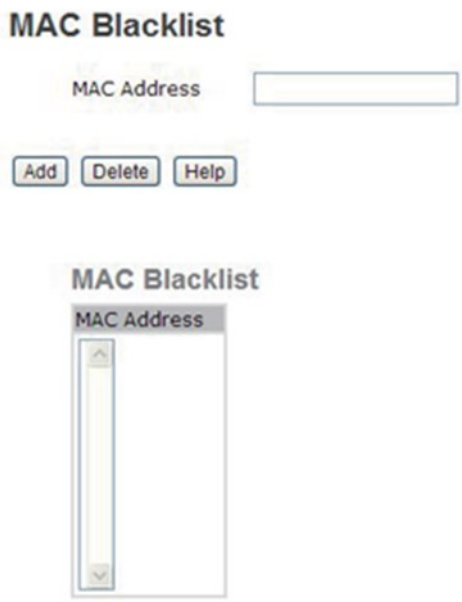
The following table describes the labels in this screen.

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.

MAC Blacklist

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

Figure 45 MAC Blacklist interface



The following table describes the labels in this screen.

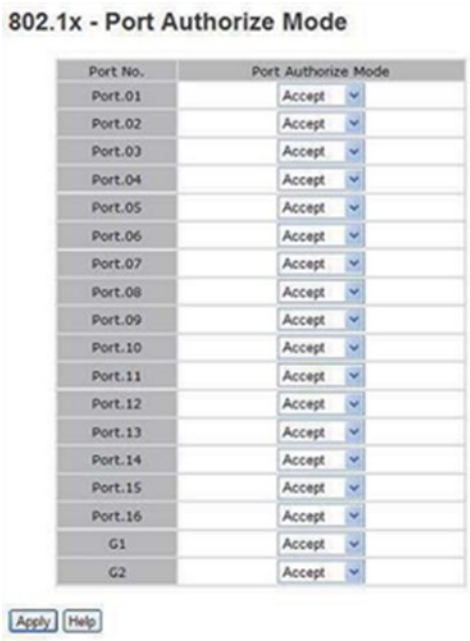
Label	Description
MAC Address	Input MAC Address to add to MAC Blacklist .
Port NO.	Select port of switch.
Add	Add an entry to Blacklist table.
Delete	Delete the entry.
Help	Show help file.

802.1x

802.1x - Radius Server

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

Figure 46 802.1x Radius Server interface



The following table describes the labels in this screen.

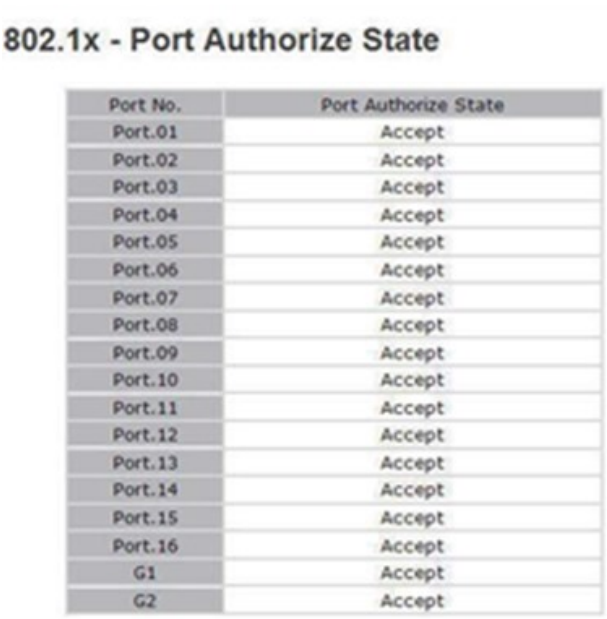
Label	Description
802.1x Protocol	Enable or Disable 802.1X Radius Server function.
Radius Server IP	The IP address of the authentication server.
Server port	Set the UDP port number used by the authentication server to authenticate.
Account port	Set the UDP destination port for accounting requests to the specified Radius Server.
Shared Key	A key shared between this switch and authentication server.
NAS, Identifier	A string used to identify this switch.
Advanced Setting	
Quiet Period	Set the time interval between authentication failure and the start of a new authentication attempt.
Tx Period	Set the time that the switch can wait for response to an EAP request/identity frame from the client before resending the request.
Supplicant Timeout	Set the period of time the switch waits for a supplicant response to an EAP request.
Server Timeout	Set the period of time the switch waits for a Radius ser ver response to an authentication request.

Label	Description
Max Requests	Set the maximum number of times to retry sending packets to the supplicant.
Re-Auth Period	Set the period of time after which clients connected must be re-authenticated.
Apply	Click “Apply” to set the configurations.
Help	Show help file.

802.1x-Port Authorized Mode

Set the 802.1x authorized mode of each port.

Figure 47 802.1x Port Authorize interface



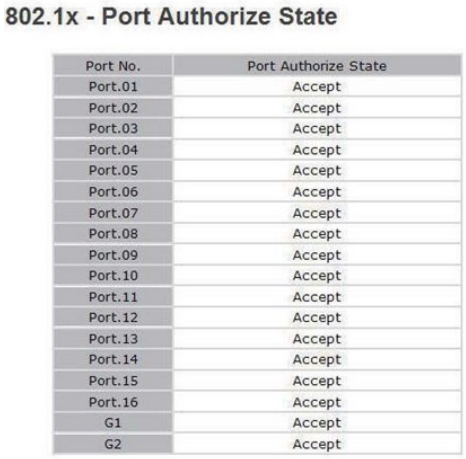
The following table describes the labels in this screen.

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

802.1x-Port Authorized Mode

Show 802.1x port authorized state.

Figure 48 802.1x Port Authorize State interface



5.1.13 Warning

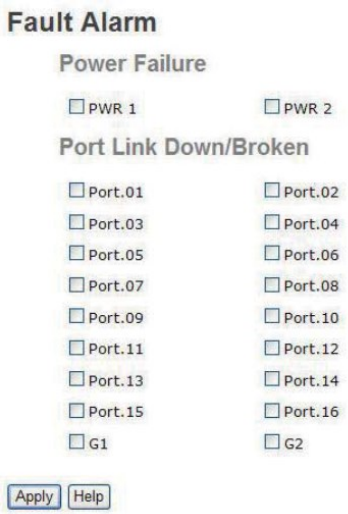
Warning function is very important for managing switch. You can manage switch by SYSLOG, E-MAIL, and Fault Relay. It helps you to monitor the switch status on remote site. When events occurred, the warning message will send to your appointed server, E-MAIL, or relay fault to switch panel.

System alarm support two warning mode: 1. SYSLOG. 2. E-MAIL. You can monitor switch through selected system events.

Warning – Fault Relay Alarm

When any selected fault event is happened, the Fault LED in switch panel will light up and the electric relay will signal at the same time.

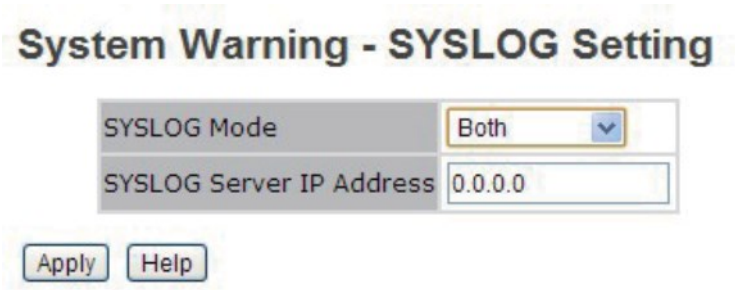
Figure 49



System Warning – SYSLOG Setting

The SYSLOG is a protocol to transmit event notifi cation messages across networks. Please refer to RFC 3164 - The BSD SYSLOG Protocol.

Figure 50 System Warning – SYSLOG Setting interface



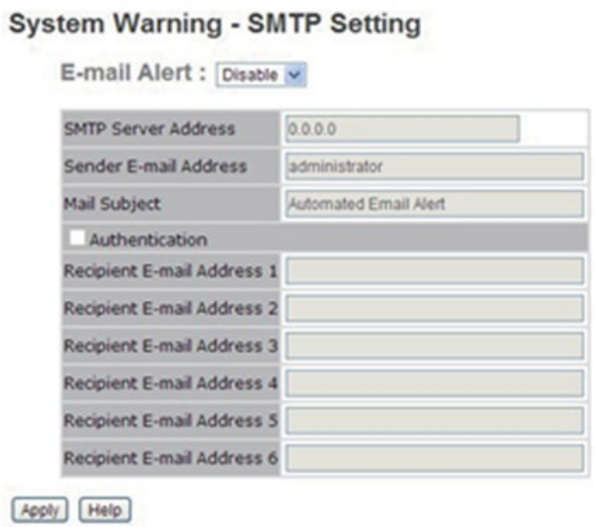
The following table describes the labels in this screen.

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

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

Figure 51 System Warning – SMTP Setting interface



The following table describes the labels in this screen.

Label	Description
E-mail Alart	Enable/Disable transmission system warning events by e-mail.
SMTP Server IP Address	Setting up the mail server IP address
Mail Subject	The Subject of the mail
Sender	Set up the email account to send the alert.
Authentication	• Username: the authentication username. • Password: the authentication password. • Confirm Password: re-enter password.
Recipient E-mail Address	The recipient's E-mail address. It supports 6 recipients for a mail.
Apply	Click “Apply” to set the configurations.

System Warning – Event Selection

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

Figure 52

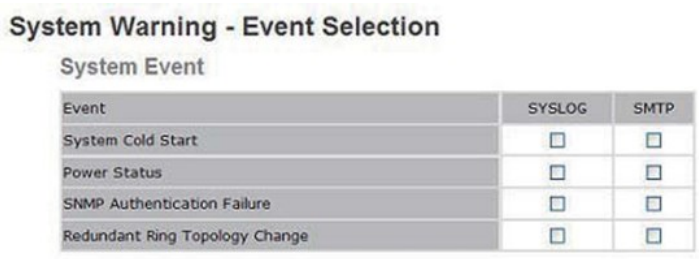


Figure 53 System Warning – Event Selection interface

The following table describes the labels in this screen.

Label	Description
System Cold Start	When the device executes cold start, the system will issue a log event.
Power Status	Alert When the power failure
Authentication Failure	Alert when SNMP authentication failure.
Redundant Ring topology change	Alert when Redundant Ring topology changes.
Port Event	• Disable • Link Up • Link Down • Link Up & Link Down
Apply	Click “Apply” to set the configurations.
Help	Show help file.

5.1.14 Monitor and Diag

MAC Address Table

The MAC Address Table, that is Filtering Database, supports queries by the Forwarding Process, as to whether a frame received by a given port with a given destination MAC address is to be forwarded through a given potential transmission port.

Figure 54 MAC Address Table interface

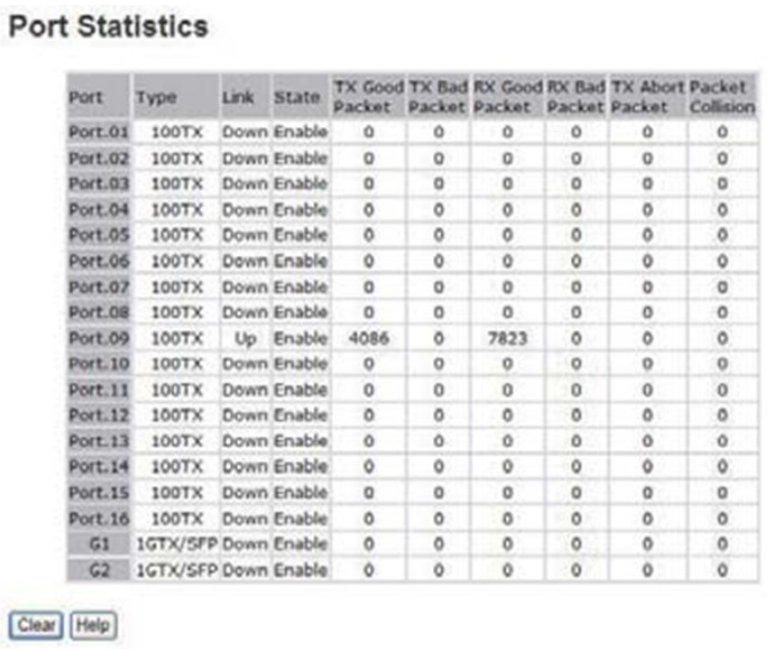
The following table describes the labels in this screen.

Label	Description
Port NO. :	Show all MAC addresses mapping to a selected port in table.
Flush MAC Table	Clear all MAC addresses in table
MAC Address Aging Time	Assign aging time MUST be multiple of 15.
Auto Flush Table When Ports Link Down	Enable this function, when port link down, switch will Clear Mac Table.

Label	Description
Apply	Click “Apply” to set the configurations.

Port Statistics

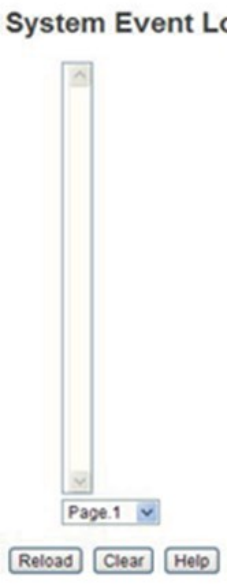
Figure 55



System Event Log

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

Figure 56 System event log interface



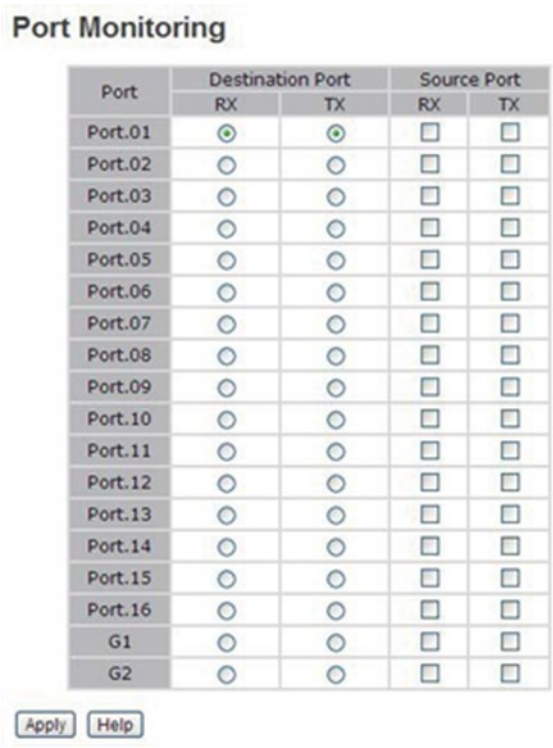
The following table describes the labels in this screen.

Label	Description
Page	Select LOG page.
Reload	To get the newest event logs and refresh this page.
Clear	Clear log.
Help	Show help file.

Port Monitoring

Port monitoring function supports TX (egress) only, RX (ingress) only, and both TX/RX monitoring. TX monitoring sends any data that egress out checked TX source ports to a selected TX destination port as well. RX monitoring sends any data that ingress in checked RX source ports out to a selected RX destination port as well as sending the frame where it normally would have gone. Note that keep all source ports unchecked in order to disable port monitoring.

Figure 57 Port Monitoring Interface



The following table describes the labels in this screen.

Label	Description
Destination Port	The por t will receive a copied frame from source por t for monitoring purpose.
Source Port	The port will be monitored. Mark the blank of TX or RX to be monitored.
TX	The frames come into switch port.

Label	Description
RX	The frames receive by switch port .
Apply	Click “Apply” to activate the configurations.
Clear	Clear all marked blank. (disable the function)
Help	Show help file.

5.1.15 Save Configuration

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

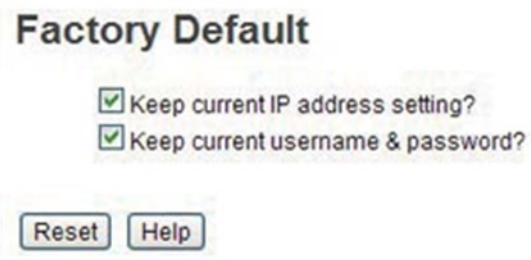
Figure 58 System Configuration interface

The following table describes the labels in this screen.

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

5.1.16 Factory Default

Figure 59 Factory Default interface



Reset switch to default configuration. Click Reset to reset all configurations to the default value. You can select “Keep current IP address setting” and “Keep current username & password” to keep current IP and username and password.

5.1.17 System Reboot

Figure 60 System Reboot interface

Chapter 6: Command Line Interface Management

6.1 About CLI Management

Besides WEB-based management, SLM162 also supports CLI management. You can use console to management switch by CLI.

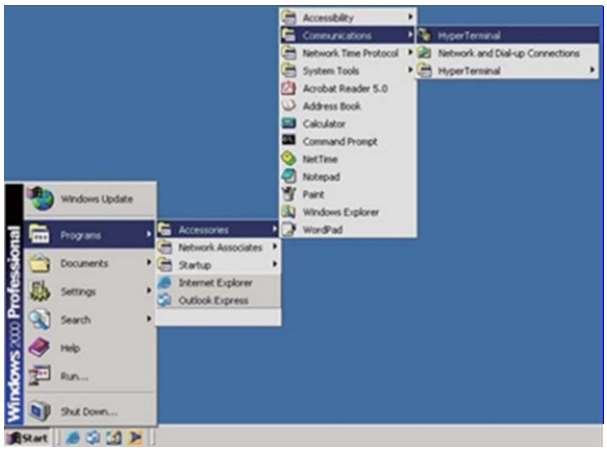
6.1.1 CLI Management by RS-232 Serial Console (9600, 8, none, 1, none)

Before Configuring by RS-232 serial console, use an RJ45 to DB9-F cable to connect the Switches' RS-232 Console port to your PCs' COM port.

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

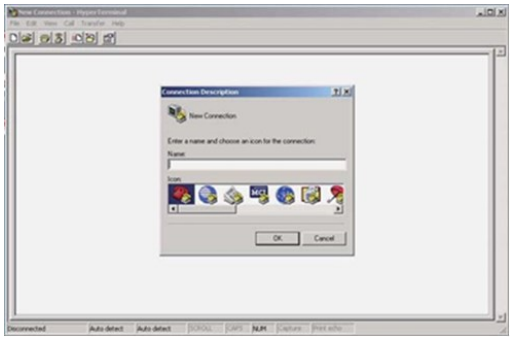
Step 1. From the Windows desktop, click on Start -> Programs -> Accessories -> Communications -> Hyper Terminal

Figure 61



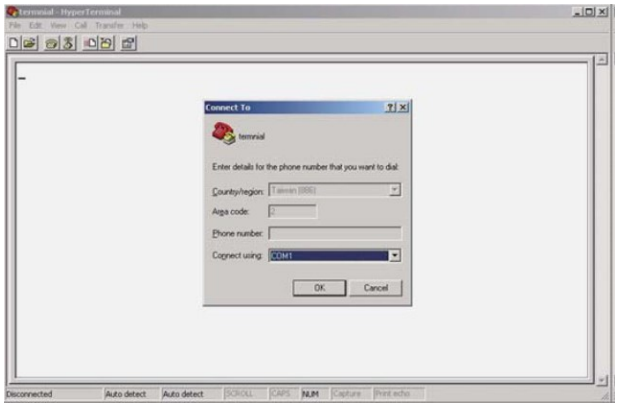
Step 2. Input a name for new connection

Figure 62



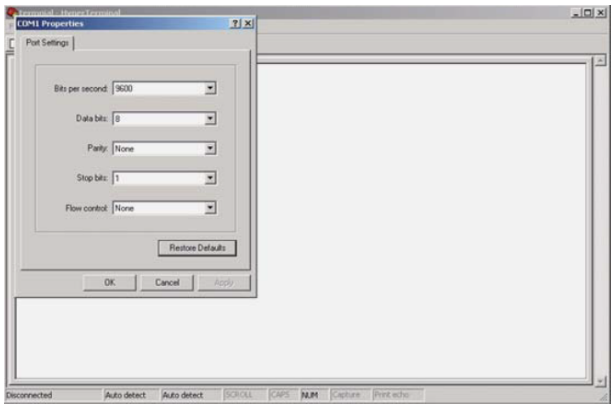
Step 3 Select to use COM port number

Figure 63



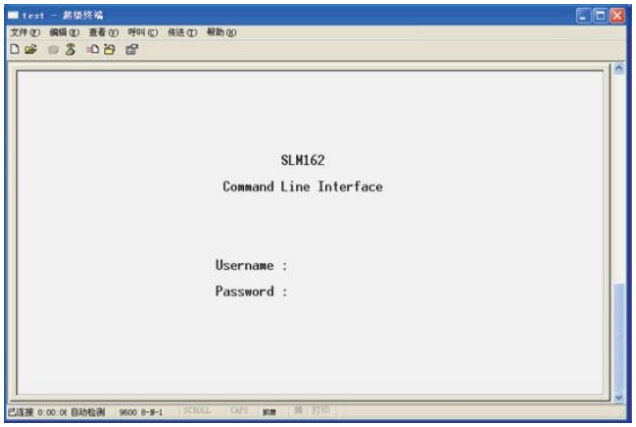
Step 4 The COM port properties setting, 9600 for Bits per second, 8 for Data bits, None for Parity, 1 for Stop bits and none for Flow control.

Figure 64



Step 5. The Console login screen will appear. Use the keyboard to enter the Username and Password (The same with the password for Web Browser), then press “Enter”.

Figure 65 SLM162 User’s Manual–November 2013



6.1.2 Commands Level

Modes	Access Method	Prompt	Exit Method	About This Model
User EXEC	Begin a session with your switch.	switch>	Enter logout or quit.	The user command 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 Privileged this mode to • Display advance function status • save configures
Global configuration	Enter the configure command while in privileged EXEC mode.	switch (coswitch (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 E XEC 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 exist privileged EXEC mode or end.	Use this mode to configure parameters for the switch and Ethernet ports.

6.1.3 Symbol of Command Level.

Mode	Symbol of Command Level
User EXEC	e
Global configuration	c
VLAN database	VLAN database

6.2 Commands Set List—System Commands Set

Commands	Level	Description	Example
show config	E	Show switch configuration	switch>show config
show system-info	P	Show system information	Switch>show system-info
write memory	P	Save y our 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	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	switch(config)# dhcpserver lowip 192.168.1.1
dhcpserver highip [High IP]	G	Configure high IP address for IP	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

Commands	Level	Description	Example
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 dhcpser ver configuration	P	Show configuration of DHCP	switch#show dhcpser ver configuration
show dhcpser ver clients	P	Show client entries of DHCP server	switch#show dhcpser ver clinets
show dhcpserver ip-binding	P	Show IP-Binding information of DHCP	switch#show dhcpserver ip-binding
no dhcpserver	G	Disable DHCP server functionDisable 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 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

6.3 Commands Set List—Port Commands

SLM162Commands	Level	Description	Example
interface fast Ethernet [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

SLM162Commands	Level	Description	Example
speed [10|100|1000|auto]	I	Use the speed configuration command to specify the speed mode of operation for Fast Ethernet., the speed can't be set to 1000 if the port isn't a giga port.	switch(config)#interface fastEthernet 2 switch(config-if)#speed 100
Flow control mode [Symmetric| Asymmetric]	I	Use the flow control configuration command on Ethernet ports to control traffic rates during	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	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type all
bandwidth type broadcast-multicast-flooded-unicast	I	Set interface ingress limit frame type to "accept broadcast , multicast , and flooded unicast frame"	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type broadcast-multicast-flooded-unicast
bandwidth type broadcast-multicast	I	Set interface ingress limit frame type to "accept broadcast and multicast frame"	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type broadcast-multicast
bandwidth type broadcast -only	I	Set interface ingress limit frame type to "only accept broadcast frame"	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type broadcast-only
bandwidth in [Value]	I	Set interface input bandwidth. Rate Range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports, and zero means no limit.	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth in 100

SLM162Commands	Level	Description	Example
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 Commands Set List—Trunk command set

SLM162Commands	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 activity port 2

SLM162Commands	Level	Description	Example
aggregator group [GroupID] [Port-list] lacp workp [Workport]	G	Assign a trunk group with LACP active. [GroupID] :1to3 [P or t -list]: Member por t 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 [P or t -list]: Member por t list, This parameter could be a port range(ex.1-4) or a port list separate by a comma (ex.2, 3, 6)	switch(config)#aggregator group 1 2-4 nolacp or switch(config)#aggreator group 1 3,1,2 nolacp
show aggregator	P	Show the information of trunk group	switch#show aggregator
no aggregator lacp [GroupID]	G	Disable the L ACP function of trunk group	switch(config)#no aggreator lacp 1
no aggregator groups [GroupID]	G	Remove a trunk group	switch(config)#no aggreator group 2

6.5 Commands Set List—VLAN command set

SLM162Command	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

SLM162Command	Level	Description	Example
vlan 8021q port [PortNumber] trunk-link tag [TaggedVID List]	V	Assign a trunk link for VL AN 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 Commands Set List—Spanning Tree command set

SLM162Commands	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

SLM162Commands	Level	Description	Example
spanning-tree max-age [seconds]	G	Use the spanning-tree max-age global configuration command to change the interval between messages the spanning tree receives from the root switch. If a switch does not receive a bridge protocol data unit (BPDU) message from the root switch within this interval, it recomputed the Spanning Tree Protocol (STP) topology.	switch(config)# spanning- tree max-age 15
spanning-tree hello-time [seconds]	G	Use the spanning-tree hello-time global configuration command to specify the interval between hello bridge protocol data units (BPDUs).	switch(config)#spanning- tree hello-time 3
spanning - tree forward-time [seconds]	G	Use the spanning-tree forward - time global configuration command to set the forwarding-time for the specified spanning-tree instances. The forwarding time 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 Protocol (STP) calculations. In the event of a loop, spanning tree considers the path cost when selecting an interface to place into the forwarding state.	switch(config)#interface fastEthernet 2 switch(config-if)#stp-path-cost 20
stp-path-priority [Port Priority]	I	Use the spanning-tree por t-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

SLM162Commands	Level	Description	Example
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 Commands Set List—QoS command set

SLM162Commands	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) # q o s 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 Commands Set List—IGMP command set

SLM162Comma	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 Commands Set List—MAC/Filter Table command set

SLM162Comma	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- addr ess-table static hw addr 000012345678
mac-address- table filter hwaddr [MAC]	G	Configure MAC addr ess table(filter)	switch(config)#mac-addr ess- 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 MA C addr ess table of interface (static)	switch(config)#interface fastEthernet 2 switch(config-if)#no mac- addr ess-table static hw addr 000012345678
no mac-address-table filter hwaddr [MAC]	G	Remove an entry of MA C 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 Commands Set List—SNMP command set

SLM162Comma	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 user profile for SNMP V3 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 ser ver 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 SNMP v3 agent . Privacy password could be empty.	switch(config)# no snmp snmpv3-user test01 password AuthP W PrivPW

no snmp-server host [Host-address]	G	Remove the SNMP server host .	switch(config)#no snmp-server 192.168.10.50

6.11 Commands Set List—Port Mirroring command set

SLM162Comma	Level	Description	Example
monitor rx	G	Set RX destination por t of monitor function	switch(config)#monitor rx
monitor tx	G	Set TX destination por t 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 Commands Set List—802.1x command set

SLM162Comma	Level	Description	Example
8021x enable	G	Use the 802.1x global configuration command to enable 802.1x protocols.	switch(config)# 8021x enable
8021x system radiousip [IP address]	G	Use the 802.1x system radious IP global configuration command to change the radious server IP.	switch(config)# 8021x system radiousip 192.168.1.1
8021x system serverport [port ID]	G	Use the 802.1x system server port global configuration command to change the radious 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

SLM162Comma	Level	Description	Example
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 suppor timeout [sec.]	G	Use the 802.1x misc supp timeout global configuration command to set the supplicant timeout .	switch(config)# 8021x misc supportimeout 20
8021x miscser ver timeout [sec.]	G	Use the 802.1x misc ser ver timeout global configuration command to set the ser ver timeout .	switch(config)#8021x misc servertimeout 20
8021x miscmaxrequest [number]	G	Use the 802.1x misc max request global configuration command to set the MAX requests.	switch(config)# 8021x misc maxrequest 3
8021x miscreauthperiod [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 inter face 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
show 8021x	G	Disable 802.1x function	switch(config)#no 8021x

6.13 Commands Set List—TFTP command set

SLM162Comma	Level	Description	Defaults Example
backup flash:backup_cfg	G	Save configuration to TF TP 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 TF TP 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 TF TP and need to specify the IP of TFTP server and the file name of image.	switch(config)#upgrade lash:upgrade_fw

6.14 Commands Set List—SYSLOG, SMTP, EVENT command set

SLM162Commands	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 function	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
smtp rcptemail [Index] [Email address]	G	Configure Rcpt e-mail Address	switch(config)#smtp rcptemail
show smtp	P	Show the information of SMTP	switch#show smtp

SLM162Commands	Level	Description	Example
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 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
show systemlog	P	Show system log client & server information	switch#show systemlog

6.15 Commands Set List—SNTP command set

SLM162Comma	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 f unction 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 f unction is inactive, this command can't be applied.	switch(config)#sntp daylight -offset 3
sntp ip [IP]	G	Set SNTP ser ver IP, if SNTP f u nction 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

6.16 Commands Set List—Redundant Ring command set

SLM162Comma	Level	Description	Example
ring enable	G	Enable	switch(config)# ring enable
ring master	G	Enable ring master	switch(config)# ring master
ring couple-ring	G	Enable couple ring	switch(config)# ring coupe-ring
ring dual-homing	G	Enable dual homing	switch(config)# ring dual-homing
ring port [1st Ring Port] [2nd Ring Port]	G	Configure 1st/2nd Ring Port	switch(config)# ring port 9 10
ring coupling-port [Coupling Port]	G	Configure Coupling Port	switch(config)# ring coupling-port
ring homing-port [Dual Homing Port]	G	Configure Dual Homing Port	switch(config)# ring homing-port 3

SLM162Comma	Level	Description	Example
show Ring	P	Show the ring information	switch#show ring
no ring	G	Disable Redundant Ring	switch(config)#no ring
no ring master	G	Disable ring master	switch(config)# no ring master
no ring couple ring	G	Disable couple ring	switch(config)# no ring couple ring
no ring dual-homing	G	Disable dual homing	switch(config)# no ring dual-homing

Chapter 7: Technical Specifications

Emerson Switch Model	**SLM162**
Physical Ports	
10/100 Base-T(X) Ports in RJ45 Auto MDI/MDIX	16
100/1000Base-X SFP Ports	2
Technology	
Ethernet Standards	IEEE 802.3 for 10Base-T IEEE 802.3u for 100Base-TX and 100Base-FX IEEE 802.3z for 1000Base-X IEEE 802.3x for Flow control IEEE 802.3ad for LACP (Link Aggregation Control Protocol) IEEE 802.1D for STP (Spanning Tree Protocol) IEEE 802.1p for COS (Class of Service) IEEE 802.1Q for VLAN Tagging IEEE 802.1w for RSTP (Rapid Spanning Tree Protocol) IEEE 802.1x for Authentication IEEE 802.1AB for LLDP (Link Layer Discovery Protocol)
MAC Table	8192 MAC addresses
Priority Queues	4
Processing	Store-and-Forward
Switch Properties	Switching latency: 7 us Switching bandwidth: 7.2Gbps 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

Emerson Switch Model	**SLM162**
Software Features	STP/RSTP (IEEE 802.1D/w) Redundant Ring (Redundant Ring) with recovery time less than 10ms over 250 units TOS/Diffserv supported Quality of Service (802.1p) for real-time traffic VLAN (802.1Q) with VLAN tagging and GVRP supported IGMP Snooping for multicast filtering Port configuration, status, statistics, monitoring, security SNTP for synchronizing of clocks over network DHCP Server / Client support Port Trunk support
Network Redundancy	Redundant Ring STP RSTP
Warning / Monitoring System	Relay output for fault event alarming Syslog server / client to record and view events Include SMTP for event warning notification via email Event selection support
RS-232 Serial Console Port	RS-232 in RJ45 connector with console cable. 9600bps, 8, N, 1
LED Indicators	
Power Iindicator	Green : Power LED x 3
R.M. Indicator	Green : Indicate system operated in Redundant RingMaster
Redundant RingIndicator	Green : Indicate system operated in Redundant Ringmode
Fault Indicator	Amber : Indicate unexpected event occurred
10/100Base-T(X) RJ45 P o r t Indicator	Green for port Link/Act . Amber for Duplex/Collision
100/1000Base-X SFP P o r t Indicator	Green for port Link/Act
Fault Contact	
Relay	Relay output to carry capacity of 1A at 24VDC
Power	
Redundant Input Power	Triple DC inputs. 12~48VDC on 6-pin terminal block,
Power Consumption (Typ.)	12 Watts
Overload Current Protection	Present
Reverse Polarity Protection	Present on terminal block
Physical Characteristic	
Enclosure	IP-30
Dimension (W x D x H)	96.4(W)x108.5(D)x154(H) mm (3.8x4.27x6.06 inch.)

Emerson Switch Model	**SLM162**
Weight (g)	1220g
Environmental	
Storage Temperature	-40 to 85°C (-40 to 185oF)
Operating Temperature	-40 to 70°C (-40 to 158oF)
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
Warranty	5 years

Technical Support & Contact Information

Home link: http://www.Emerson.com/Industrial-Automation-Controls

Knowledge Base: https://www.emerson.com/Industrial-Automation-Controls/support

Note: If the product is purchased through an Authorized Channel Partner, please contact the seller directly for any support.

Emerson reserves the right to modify or improve the designs or specifications of the products mentioned in this manual at any time without notice. Emerson does not assume responsibility for the selection, use or maintenance of any product. Responsibility for proper selection, use and maintenance of any Emerson product remains solely with the purchaser.

EMERSON