

USER'S MANUAL

Industrial Ethernet Managed Switch

Ver. 1.0, Apr. 2007



Industrial managed Switches

ESW-8xxx Series User's Manual

The software described in this manual is furnished under a license agreement and may be used only in accordance with the terms of that agreement.

Copyright Notice

Copyright © 2006 Industrial-managed Networking Co., Ltd.
All rights reserved.
Reproduction without permission is prohibited.

Trademarks

Industrial-managed is a registered trademark of the Industrial-managed Group.
All other trademarks or registered marks in this manual belong to their respective manufacturers.

Disclaimer

Information in this document is subject to change without notice and does not represent a commitment on the part of Industrial-managed. Industrial-managed provides this document "as is," without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose. Industrial-managed reserves the right to make improvements and/or changes to this manual, or to the products and/or the programs described in this manual, at any time. Information provided in this manual is intended to be accurate and reliable. However, Industrial-managed assumes no responsibility for its use, or for any infringements on the rights of third parties that may result from its use. This product might include unintentional technical or typographical errors. Changes are periodically made to the information herein to correct such errors, and these changes are incorporated into new editions of the publication.

Table of Contents

1	INTRODUCTION	4
1.1	Inside the Future of Industrial Ethernet Technology	4
1.2	Sunix Switch	4
1.3	Package Checklist	4
1.4	Optional Accessories	4
1.5	Features.....	4
1.6	Hardware Installation	5
2	FEATURED FUNCTIONS	8
3	GETTING START	9
3.1	Configuration by Web Browser	9
3.1.1	Basic Setting.....	10
3.1.2	DHCP Server	15
3.1.3	Port Configuration.....	19
3.1.4	Port Trunk.....	22
3.1.5	Redundancy	23
3.1.6	802.1Q VLAN	30
3.1.7	Traffic Prioritization	33
3.1.8	IGMP Snooping	36
3.1.9	SNMP Configuration	38
3.1.10	Security	41
3.1.11	Warning.....	46
3.1.12	Monitor and Diag	51
3.1.13	Front Panel.....	53
3.1.14	Save Configuration	54
3.2	Configuration by RS-232 Serial Console (9600,8,none,1,none).....	54
3.2.1	Commands Level	57
3.2.2	Commands Set List.....	59
3.2.2.1	System Commands Set.....	59
3.2.2.2	Port Commands Set.....	60
3.2.2.3	Trunk Commands Set.....	61
3.2.2.4	VLAN Commands Set	62
3.2.2.5	Spanning Tree Commands Set.....	62
3.2.2.6	QOS Commands Set	63
3.2.2.7	IGMP Commands Set	63
3.2.2.8	Mac / Filter Table Commands Set.....	64
3.2.2.9	SNMP Commands Set	64
3.2.2.10	Port Mirroring Commands Set.....	64
3.2.2.11	802.1x Commands Set.....	65
3.2.2.12	TFTP Commands Set.....	66
3.2.2.13	SystemLog, SMTP and Event Commands Set.....	66
3.2.2.14	Sntp Commands Set.....	67
3.2.2.15	Elite Ring Commands Set.....	67
3.3	Configuration by Telnet Console	67
3.4	Configuration by Sunix Commander	68
3.4.1	Starting Sunix Commander.....	69
3.4.2	Discovery Function	70
3.4.3	Switch Setting.....	73
3.4.4	Status Monitor.....	80
3.4.5	Syslog Events	82
3.4.6	Group IP Setting Wizard.....	84
3.4.7	Group Firmware Update Wizard	86
4	MIB GROUPS	88
4.1	Tree structure of Sunix MIB.....	88
4.2	Sunix Private MIB	89
	APPENDIX A	94
	APPENDIX B	96

1. Introduction

Welcome to Sunix ESW Switch Series, the intelligent Ethernet Device Switch specially designed for connecting Ethernet-enabled devices in industrial field applications.

The following topics are covered:

- **Inside the Future of Industrial Ethernet Technology**
- **Sunix Switch**
- **Package Checklist**
- **Optional Accessories**
- **Features**

1.1. Inside the Future of Industrial Ethernet Technology

The trend in industrial communications and automation applications

As the world's network and information technology becomes more mature, the trend is to use Ethernet as the major communications interface in many industrial communications and automation applications. In fact, a whole new industry has sprung up to provide Ethernet products that comply with the requirements of demanding industrial applications.

Industrial vs. Commercial

Users have found that when moving Ethernet from the comfortable office environment to the harsh and less predictable industrial environment, the commercial Ethernet equipment available in today's market simply cannot meet the high reliability requirements demanded by industrial applications. This means that a more robust type of network equipment, commonly referred to as *industrial* Ethernet equipment, is required for these applications.

Informative vs. Passive

Since industrial Ethernet devices are often located at the endpoints of a system, such devices cannot always know what's happening elsewhere on the network. This means that industrial Ethernet communication equipment that connects these devices must take responsibility for providing system maintainers with real-time alarm messages.

1.2. Sunix Switch

Sunix Switch comes with a suite of useful maintenance and monitoring functions, and is designed to provide smooth and reliable operation in harsh industrial environments. You will find that Sunix Switch establishes a new industrial Ethernet benchmark. It is excellent for keeping automation systems running continuously, is ideal for sending status reports to help prevent system damage and losses, is a great tool for mastering your industrial Ethernet networks, and is well-suited for use with industrial device control networks.

1.3. Package Checklist

Sunix Switch Series is shipped with the following items:

- ◎ Management Industrial Ethernet Switch
- ◎ Accessories
 - SUNIX Din Rail Accessory Package × 1
 - Wall Mountable Accessory Package × 1
 - Fiber Lid × 2 (For ESW-80XX-G Series Model)
- ◎ CD Driver
- ◎ Quick Installation Guide (This Document)
- ◎ User Manual (In CD)

NOTE Notify your sales representative if any of the above items is missing or damaged.

1.4. Optional Accessories

- ◎ RJ45 to DB9 Console port cable

1.5. Features

Advanced Industrial Networking Capability

- ◎ Sunix Elite Ring with Redundant Self-Healing Ethernet Ring Capability (recovery time < 10 ms at full load)
- ◎ IGMP Snooping for filtering multicast traffic from industrial Ethernet Protocols
- ◎ Supports IEEE 802.1Q VLAN and GVRP protocol to ease network planning

- ◎ Supports QoS—IEEE 802.1p/1Q and TOS/DiffServ to increase determinism
- ◎ Port Trunking to quadruple bandwidth or provide redundant path

Designed for Industrial Applications

- ◎ Long-haul transmission distance of 40 km or 80 km
- ◎ -40 to 75°C operating temperature range (for “T” models)
- ◎ Redundant, dual DC power inputs
- ◎ Rugged high-strength case
- ◎ DIN-Rail or panel mounting ability
- ◎ Rate limiting to prevent unpredictable network status
- ◎ Lock port for authorized MAC address access only
- ◎ Port mirroring for online debugging
- ◎ Automatic warning by exception through email
- ◎ Digital inputs to integrate a sensor and alarm with an IP network
- ◎ Automatic recovery of connected device IP addresses

Useful Utility and Remote Configuration

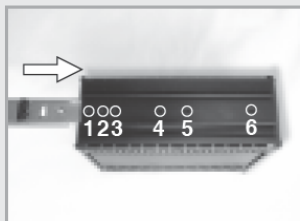
- ◎ Configurable by web browser, Telnet/serial console, Windows utility

1.6. Hardware Installation

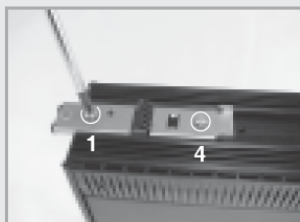
◆ DIN-Rail



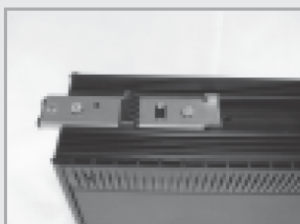
► Package contents : 3 screws and 1 DIN-Rail bracket.



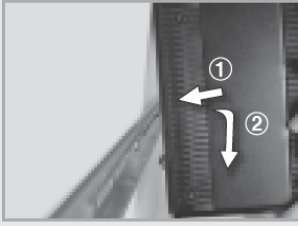
Step 1: Insert the DIN-Rail bracket into the Switch's back channel.



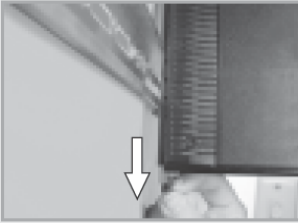
Step 2: Screwing the DIN-Rail bracket to 1 and 4 holes.



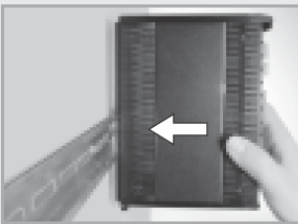
Step 3: Screwing complete.



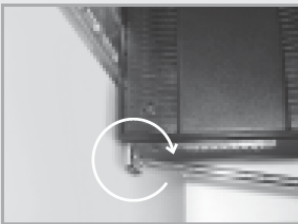
Step 4: DIN-Rail bracket hooked into the above of Aluminum track.



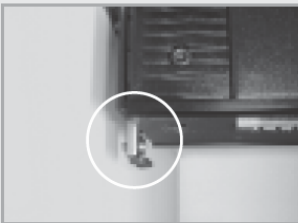
Step 5: Pull the below of DIN-Rail bracket black hanger.



Step 6: Push the Switch into the Aluminum track.

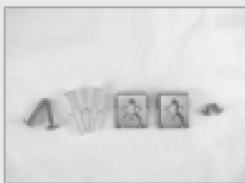


Step 7: Lock in the below of DIN-Rail bracket black hanger.

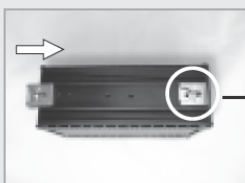


Step 8: DIN-Rail Hardware Install complete.

◆ Wall Hanging

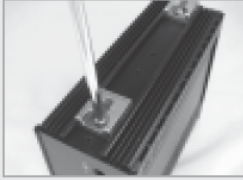


▶ Short screw X 2, lead screw X 2, plastic tap X 2, Wall-Mounting bracket X 2.



Step 1: Insert the Wall-Mounting bracket into the Switch's back channel.





Step 2: Picked the fixed hole, and screwing the Wall-Mounting to be fixed.

2. Featured Functions

- Basic Setting
- DHCP Server
- Port Configuration
- Port Trunk
- Redundancy
- 802.1Q VLAN
- Traffic Prioritization
- IGMP Snooping
- SNMP Configuration
- Security
- Warning
- Monitor and Diag
- Front Panel
- Save Configuration
- Special Utility ~ Sunix Commander Utility

3. Getting Start

This chapter explains how to access Sunix Switch for the first time. There are three ways to access the switch: serial console, Telnet console, and web browser. The serial console connection method, which requires using a short serial cable to connect Sunix Switch to a PC's COM port, can be used if you do not know Sunix Switch's IP address. The Telnet console and web browser connection methods can be used to access Sunix Switch over an Ethernet LAN, or over the Internet.

The following topics are covered:

- Configuration by RS-232 Serial Console (9600, 8, none, 1, none)
- Configuration by Telnet Console
- Configuration by Web Browser
- Configuration by Sunix Commander

3.1. Configuration by Web Browser

ESW Switch's web browser interface provides a convenient way to modify the switch's configuration and access the built-in monitoring and network administration functions. You may use either Internet Explorer or Netscape to access ESW.

NOTE To use ESW's management and monitoring functions from a PC host connected to the same LAN as ESW, you must make sure that the PC host and ESW are on the same logical subnetwork.

NOTE If ESW is configured for other VLAN settings, you must make sure your PC host is on the management VLAN.

NOTE Before accessing ESW Switch's web browser interface, first connect one of ESW Switch's RJ45 Ethernet ports to your Ethernet LAN, or directly to your PC's Ethernet NIC. You can establish a connection with either a straight-through or cross-over Ethernet cable. If you have difficulty connecting, refer to the Auto MDI/MDI-X Connection section from the Hardware installation Guide for more information about the different types of Ethernet cables and ports.

NOTE ESW Switch's default IP is 192.168.1.1

Follow the steps below to access ESW Switch's web browser interface.

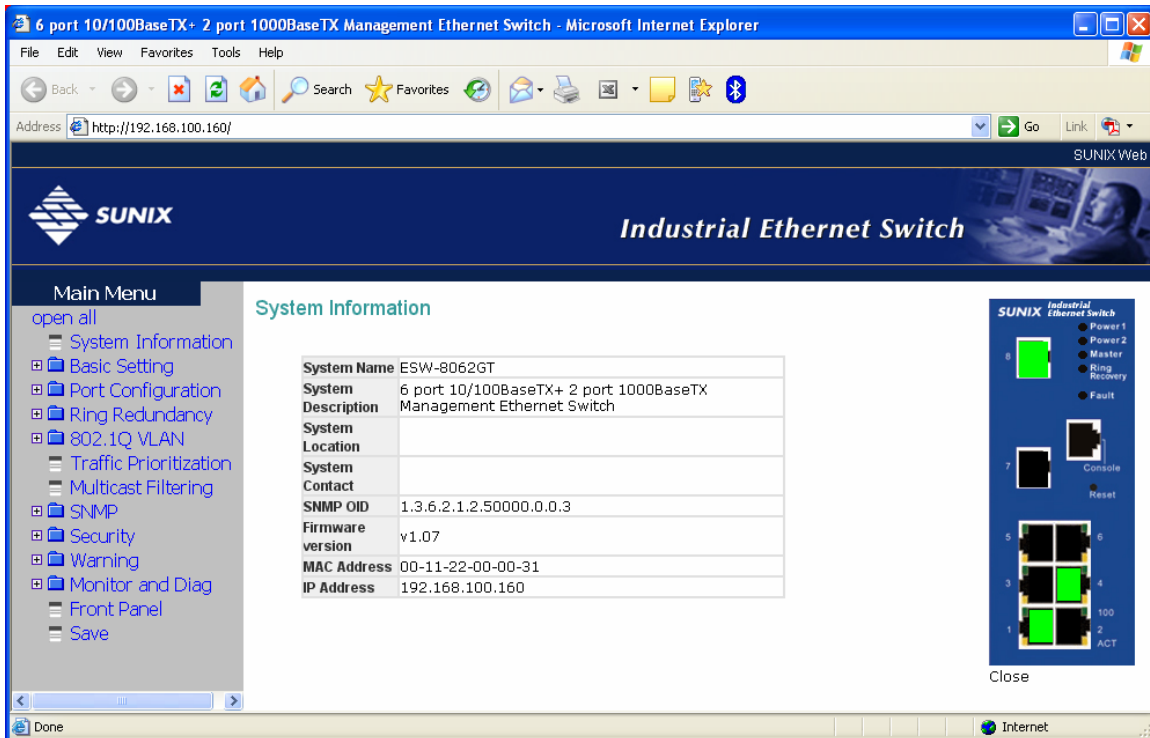
(1) Open Internet Explorer and type ESW Switch's IP address in the **Address** field. Press **Enter** to establish the connection.



(2) The web login page will open. Enter the **Username (admin)** and **Password (admin)**, and then press **Enter** to continue.



(3) You may need to wait a few moments for the web page to be downloaded to your computer. Use the menu tree on the left side of the window to open the function pages to access each of ESW Switch's functions.



3.1.1. Basic Setting

The Basic Settings group includes the most commonly used settings required by administrators to maintain and control Sunix Switch.

Switch Setting

The system identification items are displayed at the top of the web page, and will be included in alarm emails. Setting system identification items makes it easier to identify the different switches connected to your network. The system identification items are displayed at the top of the web page, and will be included in alarm emails.

Switch Setting

System Name	ESW-8062GT
System Description	6 port 10/100BaseTX+ 2 port 1000BaseTX Management Ethernet
System Location	!!
System Contact	!!
System OID	1.3.6.2.1.2.50000.0.0.3
Firmware Version	v1.07
Kernel Version	v2.02
Device MAC	00-11-22-00-00-31
<input type="button" value="Apply"/> <input type="button" value="Help"/>	

System Name

Setting	Descriptions	Factory Default
The maximum length is 64 bytes	This option is useful for specifying the role or application of different Sunix units.E.G., Factory Switch 1.	ESW-8062GT

System Description

Setting	Descriptions	Factory Default
The maximum length is 64 bytes	Use this space to record a more detailed description of the switch	6 Port 10/100BaseTX+2 port 1000BaseTX Management Ethernet

System Location

Setting	Descriptions	Factory Default
The maximum length is 64 bytes	To specify the location of different Sunix units. E.G., production line 1.	None

System Contact

Setting	Descriptions	Factory Default
The maximum length is 64 bytes	Use this space to record contact information of the person responsible for maintaining this switch	None

System OID

Setting	Descriptions	Factory Default
None	Display the SNMP Object ID of enterprise private MIB	None

Firmware Version

Setting	Descriptions	Factory Default
None	Display firmware release version	None

Kernel Version

Setting	Descriptions	Factory Default
None	Display system kernel version	None

Device MAC

Setting	Descriptions	Factory Default
None	Display the unique Ethernet hardware address.	None

IP Configuration

The **IP configuration** allows users to modify the usual TCP/IP network parameters. An explanation of each configuration item is given below.

IP Configuration

DHCP Client : ▾

IP Address	<input type="text" value="192.168.100.160"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="192.168.100.254"/>
DNS1	<input type="text" value="0.0.0.0"/>
DNS2	<input type="text" value="0.0.0.0"/>
<input type="button" value="Apply"/> <input type="button" value="Help"/>	

NOTE Sunix Switch's default IP Address is **192.168.1.1**

DHCP Client

Setting	Descriptions	Factory Default
Disable	Set up Sunix Switch IP address manually.	Disable
Enable	If DHCP client is enabled, the following table will show the IP setting assigned by DHCP server.	

IP Address

Setting	Descriptions	Factory Default
IP Address	Identifies the Switch on a TCP/IP network	192.168.1.1

Subnet Mask

Setting	Descriptions	Factory Default
Subnet Mask	Identifies the type of network of Switch connect to (e.g., 255.255.0.0 for a Class B network, or 255.255.255.0 for a Class C network)	255.255.255.0

Gateway

Setting	Descriptions	Factory Default
Gateway	The IP address of the router that's connects the LAN to an outside network	192.168.1.254

DNS1

Setting	Descriptions	Factory Default
1st DNS Server's IP Address	The IP address of the 1st DNS Server used by your network.	0.0.0.0

DNS2

Setting	Descriptions	Factory Default
2nd DNS Server's IP Address	The IP address of the 2nd DNS Server used by your network.	0.0.0.0

Admin Password

You can change login user name and password of web, console and telnet management for security.

Admin Password

User Name :	<input type="text" value="admin"/>
New Password :	<input type="password" value="••••"/>
Confirm Password :	<input type="password" value="••••"/>
<input type="button" value="Apply"/> <input type="button" value="Help"/>	

NOTE Sunix Switch's default User name and Password is **admin**

User Name

Setting	Descriptions	Factory Default
The maximum length is 10 bytes	Allows the user to modify all switch configurations	admin

New Password

Setting	Descriptions	Factory Default
The maximum length is 10 bytes	Type new password when changing the password	admin

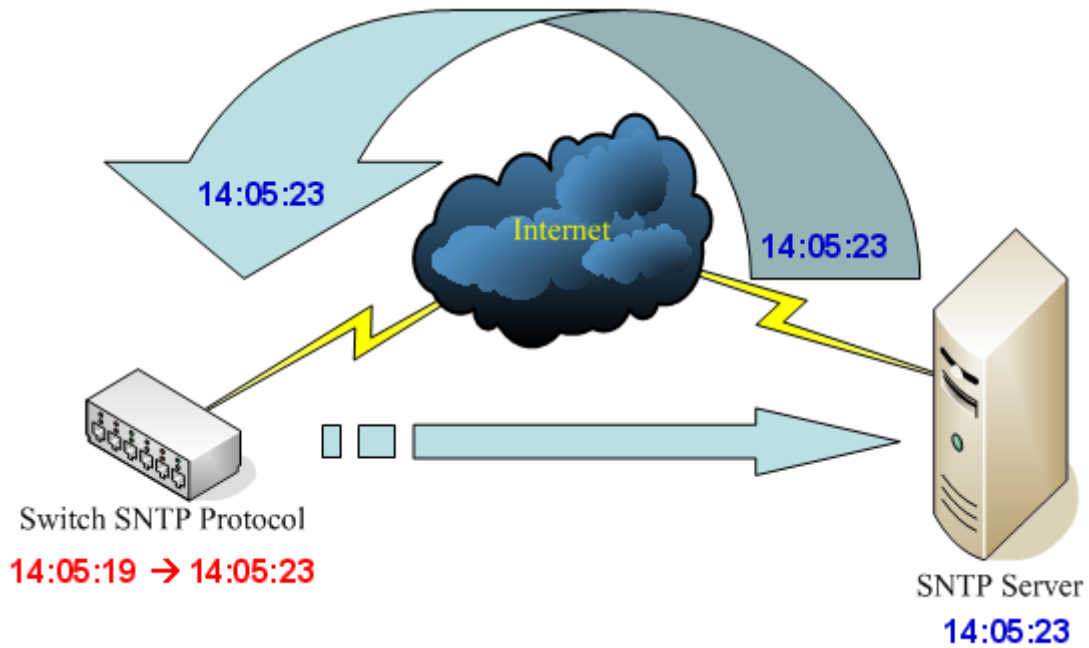
Confirm Password

Setting	Descriptions	Factory Default
The maximum length is 10 bytes	If you type a new password in the Password field, you will be required to retype the password in the Confirm password field before updating the new password.	admin

Time(SNTP)

SNTP is simple network time protocol used to synchronize the system clock to SNTP server. Sunix Switch has a time calibration function based on information from an SNTP server.

NOTE Sunix does not have a real time clock. The user must update the **Current Time** with a SNTP server.



SNTP Configuration

SNTP Client : ▾

Daylight Saving Time : ▾

UTC Timezone	(GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London ▾
SNTP Server IP Address	<input type="text" value="0.0.0.0"/>
Current System Time	<input type="text"/>
Daylight Saving Period	2006 ▾ / Jan ▾ / 1 ▾ 00 ▾ ~ 2006 ▾ / Jan ▾ / 1 ▾ 00 ▾
Daylight Saving Offset	<input type="text" value="0"/> (hours)
<input type="button" value="Apply"/> <input type="button" value="Help"/>	

NOTE Changing the time zone will automatically correct the current time. You should **configure the time zone before setting the time.**

SNTP Client

Setting	Descriptions	Factory Default
Disable	Disable SNTP client	Disable
Enable	Enable SNTP client	

Daylight Saving Time

Setting	Descriptions	Factory Default
Disable	Disable daylight saving time	Disable
Enable	Enable daylight saving time	

UTC Timezone

Setting	Descriptions	Factory Default
User selectable time zone	The time zone setting allows conversion from GMT(Greenwich Mean Time) to local time	(GMT)Greenwich Mean Time: Dublin, EdinBurgh, Lisbon, London

SNTP Server IP Address

Setting	Descriptions	Factory Default
Time Server IP	The SNTP server IP address	0.0.0.0

Currnet System Time

Setting	Descriptions	Factory Default
None	Current system time after synchronized.	None

Daylight Saving Period

Setting	Descriptions	Factory Default
YYYYMMDD HH:mm	The beginning and end of daylight saving time.	20060101 00:00 20060101 00:00

Daylight Saving Offset

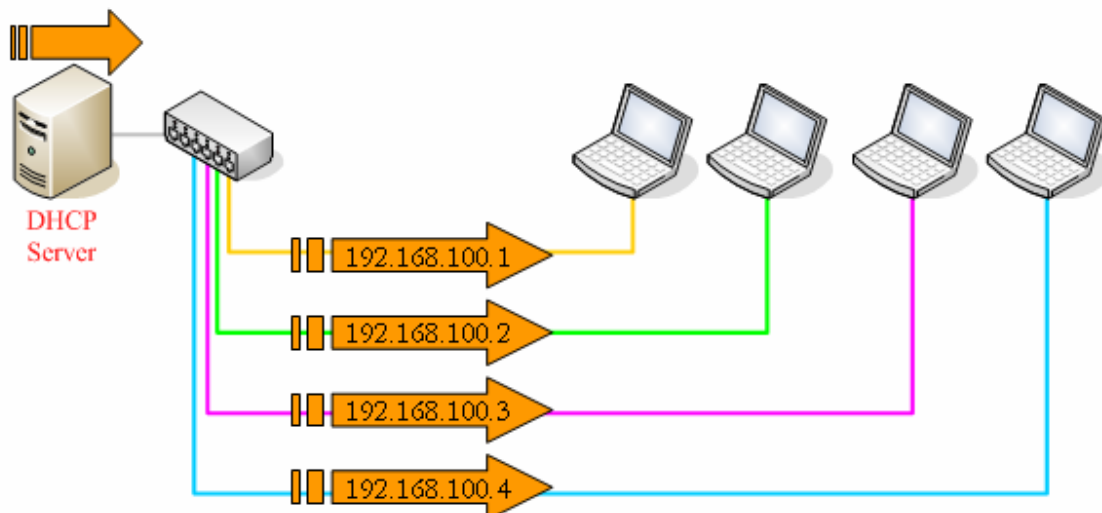
Setting	Descriptions	Factory Default
0~720	Turn system clock forward certain minute. A negative number means to turn clock backward	0

3.1.2. DHCP Server

DHCP server can automatically assign an IP address to DHCP client.

Configuration

Setting the range of IP address, subnet mask, gateway, DNS and release time of DHCP server



DHCP Server - Configuration

DHCP Server : ▾

Start IP Address	<input type="text" value="192.168.1.2"/>
End IP Address	<input type="text" value="192.168.1.200"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="0.0.0.0"/>
DNS	<input type="text" value="0.0.0.0"/>
Lease Time (day)	<input type="text" value="7"/>

DHCP Server

Setting	Descriptions	Factory Default
Disable	Disable DHCP server	Disable
Enable	Enable DHCP server	

Start IP Address

Setting	Descriptions	Factory Default
IP address	The start IP address of IP pool	192.168.1.2

End IP Address

Setting	Descriptions	Factory Default
IP address	The end IP address of IP pool	192.168.1.200

Subnet Mask

Setting	Descriptions	Factory Default
Net mask	The subnet mask	255.255.255.0

Gateway

Setting	Descriptions	Factory Default
Gateway IP address	The IP address of gateway	0.0.0.0

DNS

Setting	Descriptions	Factory Default
DNS IP address	The IP address of domain name server	0.0.0.0

Lease Time (Day)

Setting	Descriptions	Factory Default
	The client will reclaim an IP address after lease time	7

Client List

When Enable DHCP Server function, this page will display the table of DHCP client.

DHCP Server - Client List

IP Address	MAC Address	Type	Status	Lease(secs)
------------	-------------	------	--------	-------------

IP Binding

An IP address can be bound to a port. Thus a DHCP client will always get the binding IP address of source port. Keep "0.0.0.0" to disable binding

DHCP Server - IP Binding

Port No.	IP Address
Port.01	<input type="text" value="0.0.0.0"/>
Port.02	<input type="text" value="0.0.0.0"/>
Port.03	<input type="text" value="0.0.0.0"/>
Port.04	<input type="text" value="0.0.0.0"/>
Port.05	<input type="text" value="0.0.0.0"/>
Port.06	<input type="text" value="0.0.0.0"/>
G1	<input type="text" value="0.0.0.0"/>
G2	<input type="text" value="0.0.0.0"/>

IP Address		
Setting	Descriptions	Factory Default
IP address	IP address can be bound to a port and the DHCP client will always get the binding IP address of source port	0.0.0.0

Backup & Restore

Sunix Switch supports upload your configuration file to a remote TFTP server to backup or allow other Sunix Switches to use the same configuration at a later time. And it also can download user configuration data of switch from TFTP server to restore to system.

Backup & Restore

Backup Configuration

TFTP Server IP Address	<input type="text" value="0.0.0.0"/>
Backup File Name	<input type="text" value="backup.bin"/>

Restore Configuration

TFTP Server IP Address	<input type="text" value="0.0.0.0"/>
Restore File Name	<input type="text" value="backup.bin"/>

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

NOTE It's not commend to use different switch model configuration file to restore system.

TFTP Server IP Address

Setting	Descriptions	Factory Default
IP address	Assign TFTP server IP address	0.0.0.0

Restore File Name

Setting	Descriptions	Factory Default
The maximum length is 40 bytes	Assign backup file name for downloading	backup.bin

Backup File Name

Setting	Descriptions	Factory Default
The maximum length is 40 bytes	Assign backup file name for uploading	backup.bin

Upgrade Firmware

It can download firmware image file of switch from TFTP server to upgrade to system

Firmware Upgrade

TFTP Server IP	<input type="text" value="0.0.0.0"/>
Firmware File Name	<input type="text" value="firmware.bin"/>

TFTP Server IP

Setting	Descriptions	Factory Default
IP address	Assign backup file name for downloading	0.0.0.0

Firmware File Name

Setting	Descriptions	Factory Default
The maximum length is 40 bytes	Assign backup file name for downloading	firmware.bin

Reset to Default

The Reset to Default function is included to give users a quick way of restoring Sunix Switch's configuration settings to their factory default values. This function can be accessed from either the Console utility or Web Browser interface.

NOTE After activating the Reset to Default function, you will need to use the default network settings to re-establish a web-browser or Telnet connection with your Sunix Switch.

Reset to Default

- Keep current IP address setting?
- Keep current username & password?

Setting	Descriptions	Factory Default
Keep current IP address setting ?	Marked the field, it will keep current IP address setting after reset factory default values	marked
Keep current username & password ?	Marked the field, it will keep current username and password after reset factory default values	marked

System Reboot

Restart switch device and it will reloaded configuration that have saved in flash

System Reboot

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

3.1.3. Port Configuration

Port configuration are included to give the user control over Port Access, Port Transmission Speed, Flow Control, Port Security, Ingress rate limit and port trunk setting

Port Control

Port control are included to give the user control over Port State, Speed/Duplex, Flow Control, and Security

Port Control

Port No.	State	Speed/Duplex	Flow Control	Security
Port.01	Enable <input type="button" value="v"/>	AutoNegotiation <input type="button" value="v"/>	Disable <input type="button" value="v"/>	Disable <input type="button" value="v"/>
Port.02	Enable <input type="button" value="v"/>	AutoNegotiation <input type="button" value="v"/>	Disable <input type="button" value="v"/>	Disable <input type="button" value="v"/>
Port.03	Enable <input type="button" value="v"/>	AutoNegotiation <input type="button" value="v"/>	Disable <input type="button" value="v"/>	Disable <input type="button" value="v"/>
Port.04	Enable <input type="button" value="v"/>	AutoNegotiation <input type="button" value="v"/>	Disable <input type="button" value="v"/>	Disable <input type="button" value="v"/>
Port.05	Enable <input type="button" value="v"/>	AutoNegotiation <input type="button" value="v"/>	Disable <input type="button" value="v"/>	Disable <input type="button" value="v"/>
Port.06	Enable <input type="button" value="v"/>	AutoNegotiation <input type="button" value="v"/>	Disable <input type="button" value="v"/>	Disable <input type="button" value="v"/>
G1	Enable <input type="button" value="v"/>	AutoNegotiation <input type="button" value="v"/>	Disable <input type="button" value="v"/>	Disable <input type="button" value="v"/>
G2	Enable <input type="button" value="v"/>	AutoNegotiation <input type="button" value="v"/>	Disable <input type="button" value="v"/>	Disable <input type="button" value="v"/>

State

Setting	Descriptions	Factory Default
Disable	Disable port transmission	Enable
Enable	Enable port transmission	

Speed/Duplex

Setting	Descriptions	Factory Default
AutoNegotiation	Set the port speed/duplex to autonegotiation	AutoNegotiation
100 Full	Set the port speed/duplex to 100 Full	
100 Half	Set the port speed/duplex to 100 Half	
10 Full	Set the port speed/duplex to 10 Full	
10 Half	Set the port speed/duplex to 10 Half	

Flow Control

Setting	Descriptions	Factory Default
Disable	It will disable flow control ability	Disable
Symmetric	The 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	The flow control ability is always active on this port whether the linked partner port enabled or not.	

Security

Setting	Descriptions	Factory Default
Disable	Disable security function	Disable
Enable	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.	

Port Status

Display the current status of port control

Port Status

Port No.	Type	Link	State	Speed/Duplex	Flow Control
Port.01	100TX	UP	Enable	100 Full	Disable
Port.02	100TX	UP	Enable	100 Full	Disable
Port.03	100TX	UP	Enable	100 Full	Disable
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
G1	1000TX	UP	Enable	100 Full	Disable
G2	1000TX	UP	Enable	100 Full	Disable

Rate Limit

A single device should not be allowed to occupy unlimited bandwidth, especially when the device malfunctions. For example, broadcast storms could be caused by an incorrect topology or malfunctioning device. The Sunix series not only

prevents broadcast storms, but can also configure the ingress/egress rate of unicast/multicast/broadcast packets, giving administrators full control of the limited bandwidth, and preventing unpredictable faults before they occur.

NOTE The 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

	Ingress Limit Frame Type	Ingress	Egress
Port.01	Broadcast only	8192 kbps	0 kbps
Port.02	Broadcast only	8192 kbps	0 kbps
Port.03	Broadcast only	8192 kbps	0 kbps
Port.04	Broadcast only	8192 kbps	0 kbps
Port.05	Broadcast only	8192 kbps	0 kbps
Port.06	Broadcast only	8192 kbps	0 kbps
G1	Broadcast only	8192 kbps	0 kbps
G2	Broadcast only	8192 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.

Ingress Limit Frame Type

Setting	Descriptions	Factory Default
All	Selecting this option prohibits all traffic of broadcast, multicast, unicast packets that exceed the rate set in the following "Rate" field.	Broadcast only
Broadcast/Multicast/Flooded Unicast	Selecting this option prohibits all traffic of broadcast, multicast, and flooded unicast (new unicast addresses not learned by the switch) packets that exceed the rate set in the following "Rate" field.	
Broadcast/Multicast	Selecting this option prohibits all traffic of broadcast and multicast packets that exceed the rate set in the following "Rate" field.	
Broadcast only	Selecting this option prohibits all traffic of broadcast packets that exceed the rate set in the following "Rate" field.	

NOTE This setting is only against ingress rate limit but egress not.

Ingress

Setting	Descriptions	Factory Default
The 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	The value of ingress rate limit. The unit of rate is kbps, and 1 Mbps is equal to 1024 kbps	8192

Egress

Setting	Descriptions	Factory Default
---------	--------------	-----------------

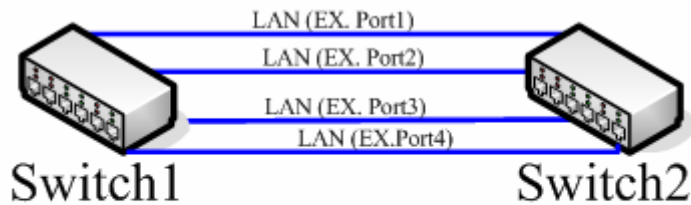
The rate range is from 100 kbps to 102400 kbps (i.e. 100Mbps) for mega-ports, or 256000 kbps (i.e. 250Mbps) for giga-ports. Zero means no limit	The value of egress rate limit. The unit of rate is kbps, and 1 Mbps is equal to 1024 kbps	0
---	--	---

3.1.4. Port Trunk

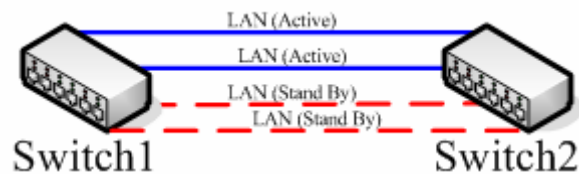
Port Trunking allows devices to communicate by aggregating up to four links in parallel, with a maximum of 4 ports for each link. This means that users can connect one Sunix Switch to another Sunix Switch by port trunking to double, triple, or quadruple the bandwidth of the connection.

Setting

The Port Trunking Settings page is used to configure ports to Trunking Group.



4 Ports set to Trunk function
 Speed = 100MB x 4 = 400MB
 (Half duplex)



2 ports set to Trunk function
 2 ports set to 802.3ad LACP function
 (2 Ports = Active line, 2 Ports = Stand By line)
 Speed = 100MB x 2 = 200MB (Half duplex)

Port Trunk - Setting

Port No.	Group ID	Type
Port.01	None <input type="button" value="v"/>	Static <input type="button" value="v"/>
Port.02	None <input type="button" value="v"/>	Static <input type="button" value="v"/>
Port.03	None <input type="button" value="v"/>	Static <input type="button" value="v"/>
Port.04	None <input type="button" value="v"/>	Static <input type="button" value="v"/>
Port.05	None <input type="button" value="v"/>	Static <input type="button" value="v"/>
Port.06	None <input type="button" value="v"/>	Static <input type="button" value="v"/>
G1	None <input type="button" value="v"/>	Static <input type="button" value="v"/>
G2	None <input type="button" value="v"/>	Static <input type="button" value="v"/>

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

Group ID

Setting	Descriptions	Factory Default
None	This port does not belong to any of the trunking groups	None
Trunk 1	This port belongs to trunking group 1	
Trunk 2	This port belongs to trunking group 2	
Trunk 3	This port belongs to trunking group 3	
Trunk 4	This port belongs to trunking group 4	

Type

Setting	Descriptions	Factory Default
Static	Join to a static trunk group directly	Static
802.3ad LACP	Join to a trunk group by determining with IEEE 802.3ad LACP dynamically	

Status

Display the table of port trunk status

Port Trunk - Status

Group ID	Trunk Member	Type
Trunk 1		Static
Trunk 2		Static
Trunk 3		Static
Trunk 4		Static

3.1.5. Redundancy

Setting up Redundancy on your network helps protect critical links against failure, protects against network loops, and keeps network downtime at a minimum.

The Redundancy function allows the user to set up **redundant loops** in the network to provide a backup data transmission route in the event that a cable is inadvertently disconnected or damaged. This is a particularly important

feature for industrial applications, since it could take several minutes to locate the disconnected or severed cable. Sunix Switch supports two different protocols to support this communication redundancy function—**ELite Ring** and **Rapid Spanning Tree Protocol (IEEE-802.1W)**.

NOTE Network redundancy protocol should be configured well-done for all switches in redundant network before actually connecting any backup/redundant path in order to prevent the inadvertent generation of traffic loops.

	Elite Ring	STP	RSTP
Topology	Ring	Ring, Mesh	Ring, Mesh
Recovery Time	< 10 ms	Up to 30 sec.	Up to 5 sec

Elite Ring


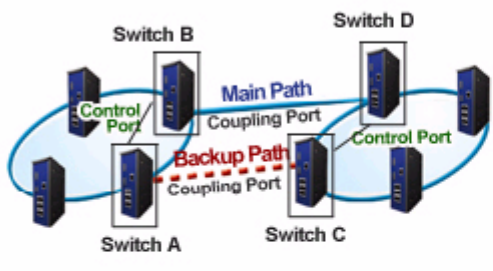
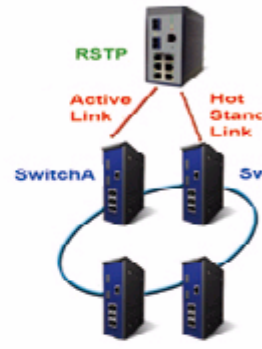
Elite Ring Protocol is a very fast network redundancy protocol that provides link fail-over protection with very fast self-healing recovery.

Elite Ring

Elite Ring

Coupling Ring

Dual Homing

Ring Master	Coupling Port	Homing Port
1st Ring Port	Control Port	
2nd RingPort		

Elite Ring

Setting	Descriptions	Factory Default
Unmarked	Disable Elite Ring	Unable to config (RSTP Mode is enable) or Unmarked
Marked	Enable Elite Ring	

Ring Master

Setting	Descriptions	Factory Default
Disable	Not Ring Master	Disable
Enable	Set as Ring Master	

NOTE There should be one and only one Ring Master in a ring. However if there are two or more switches which set Ring Master to enable, the switch with the lowest MAC address will be the actual Ring Master and others will be Backup Masters

1st Ring Port

Setting	Descriptions	Factory Default
Port.01	Select any port of the switch to be one of the redundant ports	Port.01
Port.02		
Port.03		
Port.04		
Port.05		
Port.06		
G1		
G2		

2nd Ring port

Setting	Descriptions	Factory Default
Port.01	Select any port of the switch to be one of the redundant ports	Port.02
Port.02		
Port.03		
Port.04		
Port.05		
Port.06		
G1		
G2		

Coupling Ring

Setting	Descriptions	Factory Default
Unmarked	Disable Coupling Ring	Unable to config (RSTP Mode is enable) or Unmarked
Marked	Enable Coupling Ring	

NOTE Only two switches can enable Coupling Ring in a ring. More or less is invalid

Coupling Port

Setting	Descriptions	Factory Default
Port.01	Link to Coupling Port of the switch in another ring	Port.03
Port.02		

Port.03		
Port.04		
Port.05		
Port.06		
G1		
G2		

Control Port

Setting	Descriptions	Factory Default
Port.01	Link to Control Port of the switch in the same ring.	Port.04
Port.02		
Port.03		
Port.04		
Port.05		
Port.06		
G1		
G2		

Dual Homing

Setting	Descriptions	Factory Default
Unmarked	Disable Dual Homing	Unable to config (RSTP Mode is enable) or Unmarked
Marked	Enable Dual Homing	

NOTE Only two switches can enable Dual Homing in a ring. More or less is invalid

Homing Port

Setting	Descriptions	Factory Default
Port.01	Link to a RSTP Mode switch	Port.05
Port.02		
Port.03		
Port.04		
Port.05		
Port.06		
G1		
G2		

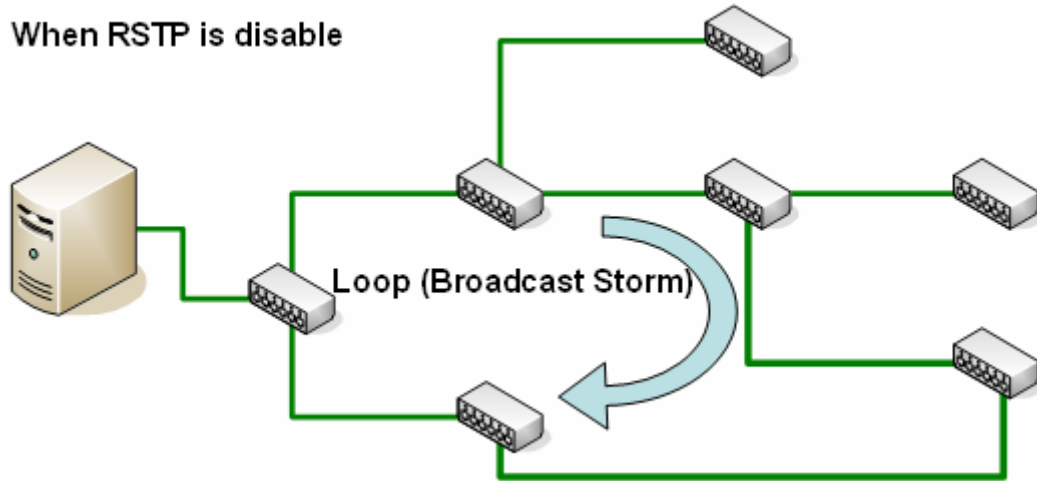
RSTP

The Rapid Spanning Tree Algorithm 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. Please refer to IEEE 802.1W.

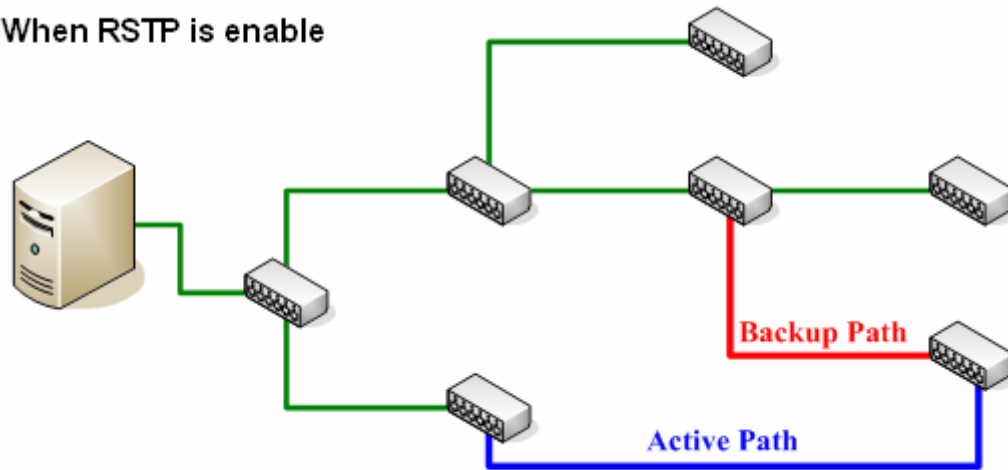
RSTP Setting

The RSTP Settings page is used to configure Rapid Spanning Tree

When RSTP is disable



When RSTP is enable



RSTP Setting

RSTP Mode	Disable ▾				
Bridge Configuration					
Priority (0-61440)	<input type="text" value="8192"/>				
Max Age Time (6-40)	<input type="text" value="20"/>				
Hello Time (1-10)	<input type="text" value="2"/>				
Forward Delay Time (4-30)	<input type="text" value="15"/>				
Port Configuration					
Port	Path Cost (1-200000000)	Priority (0-240)	Admin P2P	Admin Edge	Admin Non STP
1	<input type="text" value="200000"/>	<input type="text" value="128"/>	Auto ▾	True ▾	False ▾
2	<input type="text" value="200000"/>	<input type="text" value="128"/>	Auto ▾	True ▾	False ▾
3	<input type="text" value="200000"/>	<input type="text" value="128"/>	Auto ▾	True ▾	False ▾
4	<input type="text" value="200000"/>	<input type="text" value="128"/>	Auto ▾	True ▾	False ▾
5	<input type="text" value="200000"/>	<input type="text" value="128"/>	Auto ▾	True ▾	False ▾
6	<input type="text" value="200000"/>	<input type="text" value="128"/>	Auto ▾	True ▾	False ▾
7	<input type="text" value="20000"/>	<input type="text" value="128"/>	Auto ▾	True ▾	False ▾
8	<input type="text" value="20000"/>	<input type="text" value="128"/>	Auto ▾	True ▾	False ▾
<input type="button" value="Apply"/> <input type="button" value="Help"/>					

RSTP Mode

Setting	Descriptions	Factory Default
Disable	Disable RSTP	Enable
Enable	Enable RSTP	

***** Bridge Configuration*****

Priority

Setting	Descriptions	Factory Default
The valid value is 0 ~ 61440 in steps of 4096	A value used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root.	32768

NOTE If bridge priority is changed, the RSTP MUST be restarted.

Max Age Time

Setting	Descriptions	Factory Default
The valid value is 6 ~ 40	The number of seconds a bridge waits without receiving BPDUs before attempting a reconfiguration	20

Hello Time

Setting	Descriptions	Factory Default
The valid value is 1 ~ 10	The number of seconds between the transmission of BPDUs	2

Forward Delay Time

Setting	Descriptions	Factory Default
The valid value is 4 ~ 30	The number of seconds a port waits before changing from its protocol learning and listening states to the forwarding state	15

***** Port Configuration *****

Path Cost

Setting	Descriptions	Factory Default
The valid value is 1 ~ 200000000	The cost of the path to the other bridge from this transmitting bridge at the specified port	200000 for mega-ports and 20000 for giga-ports

Priority

Setting	Descriptions	Factory Default
The valid value is 0 ~ 240 in steps of 16	Decide which port should be blocked by priority	128

Admin P2P

Setting	Descriptions	Factory Default
True	Some of the rapid state transactions that are possible within RSTP are dependent upon whether the Port concerned can only be connected to exactly one other Bridge (i.e., it is served by a point-to-point LAN segment), or can be connected to two or more Bridges (i.e., it is served by a shared medium LAN segment).	Auto
False		
Auto		

Admin Edge

Setting	Descriptions	Factory Default
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.	True
False		

Admin Non STP

Setting	Descriptions	Factory Default
True	If true, this port will not participate in RSTP	False
False		

RSTP Information

Display RSTP root bridge information and port information. The **Port Information** indicates the current Rapid Spanning Tree status of this port. "Forwarding" for normal transmission, "Blocking" to block transmission.

RSTP Information

Root Bridge Information

Bridge ID	00200001F4BB8170
Root Priority	8192
Root Port	7
Root Path Cost	20001
Max Age Time	20
Hello Time	2
Forward Delay Time	15

Port Information

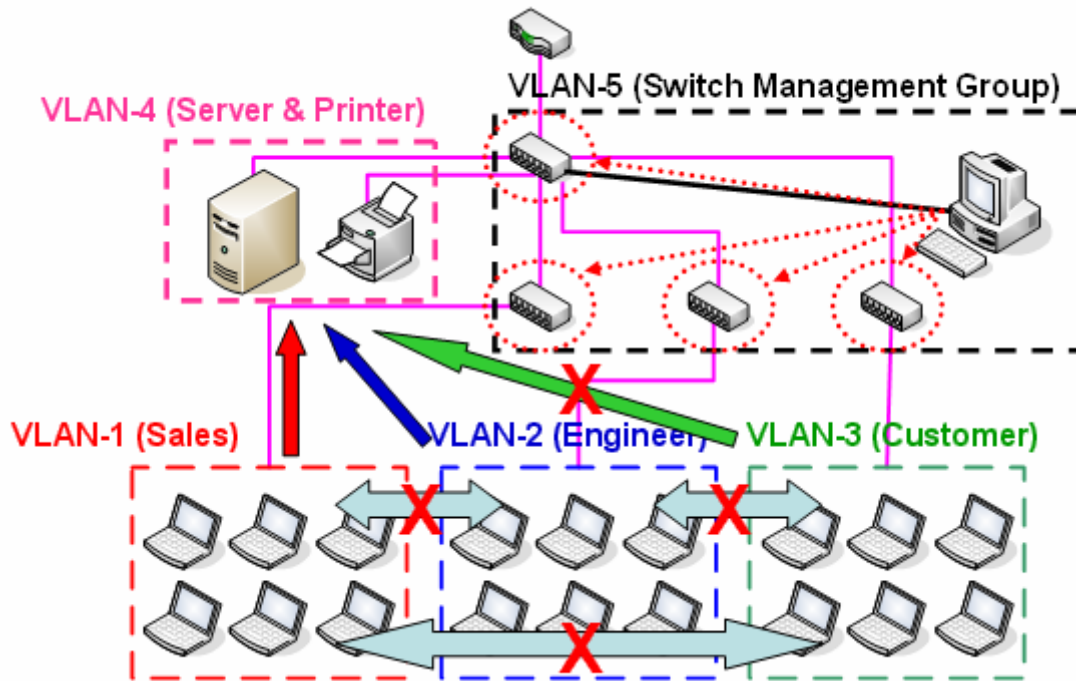
Port	Path Cost	Port Priority	OperP2P	OperEdge	STP Neighbor	State	Role
Port.01	200000	128	True	True	False	Forwarding	Designated
Port.02	200000	128	True	True	False	Forwarding	Designated
Port.03	200000	128	True	True	False	Forwarding	Designated
Port.04	200000	128	True	True	False	Disabled	Disabled
Port.05	200000	128	True	True	False	Disabled	Disabled
Port.06	200000	128	True	True	False	Disabled	Disabled
G1	20000	128	True	False	False	Forwarding	Root
G2	20000	128	True	True	False	Forwarding	Designated

3.1.6. 802.1Q VLAN

Setting up Virtual LANs (VLANs) on your Sunix switch increases the efficiency of your network by dividing the LAN into logical segments, as opposed to physical segments.

VLAN Configuration

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-compliant VLAN pruning and dynamic VLAN creation on 802.1Q trunk ports. Please refer to IEEE 802.1Q.



802.1Q VLAN

GVRP Mode :

Management Vlan ID :

VLAN Configuration

Port No.	Link Type	Untagged VID	Tagged VIDs
Port.01	Access	1	
Port.02	Access	1	
Port.03	Access	1	
Port.04	Access	1	
Port.05	Access	1	
Port.06	Access	1	
G1	Access	1	
G2	Access	1	

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

GVRP Mode

Setting	Descriptions	Factory Default
Disable	Disable GVRP Mode	Disable
Enable	Enable GVRP Mode	

Link Type

Setting	Descriptions	Factory Default
Access	The access link only supports an untagged VID.	Access
1QTrunk	The 1Q trunk link only supports multiple tagged VIDs.	
Hybrid	The hybrid link supports an untagged VID and multiple tagged VIDs.	

Untagged VID

Setting	Descriptions	Factory Default
support 1~4094	Set the port default VLAN ID for untagged devices that connect to the port	1

Tagged VIDs

Setting	Descriptions	Factory Default
support 1~4094 and multiple VIDs.	Use the comma to separate the multiple tagged VIDs. E.g., 2,3,4 means joining the Tagged VLAN 2,3 and 4	None

NOTE The ports with the same VID means in the same VLAN group.

VLAN Table

In this table, you can review the created VLAN groups, Joined Access Ports, and Trunk Ports.

VLAN Table

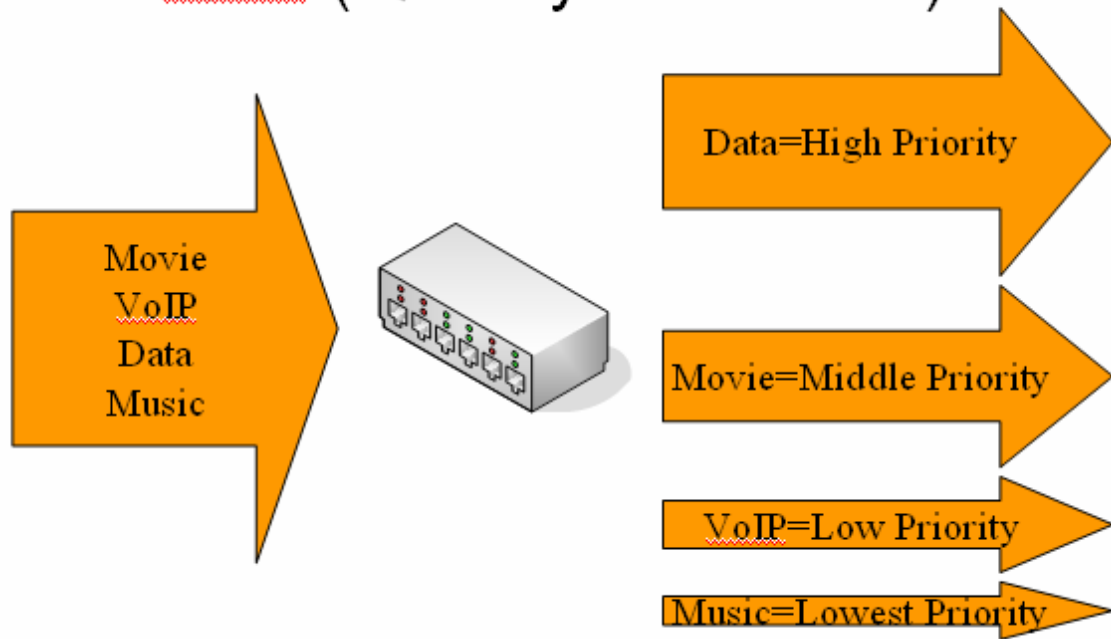
VLAN Table

VLAN ID	Untagged Ports	Tagged Ports
1	1,2,3,4,5,6,7,8	

3.1.7. Traffic Prioritization

Sunix switch's traffic prioritization capability provides Quality of Service (QoS) to your network by making data delivery more reliable. You can prioritize traffic on your network to ensure that high priority data is transmitted with minimum delay. Traffic can be controlled by a set of rules to obtain the required Quality of Service for your network. The rules define different types of traffic and specify how each type should be treated as it passes through the switch. Sunix switch can inspect both IEEE 802.1p/1Q layer 2 CoS tags, and even layer 3 TOS information to provide consistent classification of the entire network. Sunix switch's QoS capability improves the performance and determinism of industrial networks for mission critical applications.

QoS (Quality of service)



Traffic Prioritization

Qos Policy :

- Use an 8,4,2,1 weighted fair queuing scheme
 Use a strict priority scheme

Priority Type : Port-based

Port-based Priority :

Port.01	Port.02	Port.03	Port.04	Port.05	Port.06	G1	G2
Lowest	High	High	High	High	High	High	High

COS/802.1p :

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

COS Port Default :

Port.01	Port.02	Port.03	Port.04	Port.05	Port.06	G1	G2
0	0	0	0	0	0	0	0

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

Qos Policy

Setting	Descriptions	Factory Default
Use an 8,4,2,1 weighted fair queuing scheme	The output queues will follow 8:4:2:1 ratio to transmit packets from the highest to lowest queue. For example: 8 high queue packets, 4 middle queue packets, 2 low queue packets, and the one lowest queue packets are transmitted in one turn.	Use an 8,4,2,1 weighted fair queuing scheme
Use a strict priority scheme	Always the packets in higher queue will be transmitted first until higher queue is empty.	

Priority Type

Setting	Descriptions	Factory Default
Disable	Disable traffic prioritization function	Disable
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	

Port-based Priority

Setting	Descriptions	Factory Default
High	The output priority of a packet is determined by port number	Port.01~08 all Lowest
Middle		
Low		
Lowest		

COS/802.1p

Setting	Descriptions	Factory Default
High	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.	0 => Low
Middle		1 => Lowest
Low		2 => Lowest
Lowest		3 => Low 4 => Middle 5 => Middle 6 => High 7 => High

COS Port Default

Setting	Descriptions	Factory Default
0~7	When an ingress packet has not VLAN tag, a default priority value is considered and determined by ingress port	Port.01~08 all 0

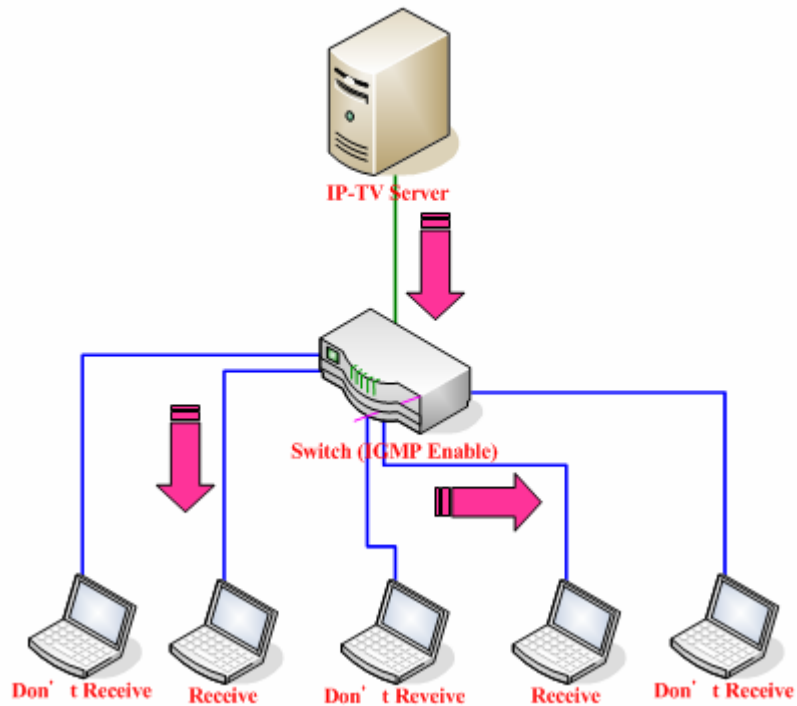
TOS/DSCP

Setting	Descriptions	Factory Default
High	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.	0~7 => Lowest 8~15 => Lowest 16~23 => Low 24~31 => Low 32~39 => Middle 40~47 => Middle 48~55 => High 56~63 => High

3.1.8. Multicast Filtering (IGMP Snooping)

Internet Group Management Protocol (IGMP) is used by IP hosts to register their dynamic multicast group membership. IGMP has 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.

IGMP



Multicast Filtering

IGMP Snooping :

IGMP Query Mode:

IGMP Snooping Table

IP Address	VLAN ID	Member Port
239.255.255.250	1	1*****

IGMP Snooping

Setting	Descriptions	Factory Default
Disable	Disable IGMP snooping	Disable
Enable	Enable IGMP snooping	

IGMP Query Mode

Setting	Descriptions	Factory Default
Disable	Not to be a IGMP querier	Disable
Enable	To be a IGMP querier	
Auto	Querier is the one with lower IP address.	

NOTE There should exist one and only one IGMP querier in an IGMP application

IGMP Snooping Table

Setting	Descriptions	Factory Default
IP Address	Show current IP multicast list, include the ip address, vlan id and member port	None
VLAN ID		
Member Port		

3.1.9. SNMP Configuration

Sunix switch supports three SNMP protocols. The available protocols are SNMP V1, SNMP V2c, and SNMP V3.

Agent Setting

SNMP V1 and SNMP V2c use a community string match for authentication, which means SNMP servers access all objects with read-only or read/write permissions using the community string public/private (default value). SNMP V3 requires an authentication level of MD5 or DES to encrypt data to enhance data security.

SNMP Configuration

SNMP Agent Version

SNMPV1/V2c

SNMP V1/V2c Community

Community String	Privilege
public	Read Only <input type="button" value="v"/>
private	Read and Write <input type="button" value="v"/>
	Read Only <input type="button" value="v"/>
	Read Only <input type="button" value="v"/>

SNMPv3 User

User Name	<input type="text"/>
Auth Password	<input type="text"/>
Privacy Password	<input type="text"/>

Current SNMPv3 User Profile

User Name	Auth. Password	Priv. Password

SNMP Agent Version

Setting	Descriptions	Factory Default
SNMPV1/V2c	Select SNMP protocol versions V1, V2c to manage the switch	SNMPV1/V2c
SNMPV3	Select only SNMP protocol version V3 to manage the switch	

NOTE When SNMP V3 agent is selected, you can: (1)Input SNMPv3 user name only. (2)Input SNMPv3 user name and Auth Password. (3)Input SNMPv3 user name, Auth Password and Privacy Password, which can be different with Auth Password.

***** SNMP V1/V2C Community*****

Community String

Setting	Descriptions	Factory Default
Each Community String is maximum 32 characters	SNMP Community should be set for SNMP V1/V2c. Four sets of "Community String/Privilege" are supported. Keep empty to remove this Community string.	public private

Privilege

Setting	Descriptions	Factory Default
Read Only	Uses a community string match for authentication. (e.g., community string = public , privilege = Read Only , this means that the SNMP agent access all objects with read-only permissions using the community string Public)	Read Only Read and Write Read Only
Read and Write	Use a community string match for authentication. (e.g., community string = private , privilege = Read and Write , this means that SNMP servers access all objects with read/write permissions using the community string Private .)	Read Only

***** SNMPv3 User *****

User Name

Setting	Descriptions	Factory Default
There are maximum 8 sets of SNMPv3 User and maximum 16 characters in user name, and password	If SNMP V3 agent is selected, the SNMPv3 user profile should be set for authentication. The User Name is necessary	None

Auth Password

Setting	Descriptions	Factory Default
There are maximum 8 sets of SNMPv3 User and maximum 16 characters in user name, and password	The Auth Password is encrypted by MD5	None

Privacy Password

Setting	Descriptions	Factory Default
There are maximum 8 sets of SNMPv3 User and maximum 16 characters in user name, and password	The Privacy Password which is encrypted by DES	None

NOTE To remove a current user profile: (1) Input SNMPv3 user name you want to remove. (2) Click "Remove" button.

*****Current SNMPv3 User Profile*****

Setting	Descriptions	Factory Default
None	Show all SNMPv3 user profiles	None

SNMP Traps

Sunix Switch comes with built-in SNMP (Simple Network Management Protocol) agent software that supports cold/warm start trap, line up/down trap.

SNMP Traps

Trap Server Setting

Server IP	<input type="text"/>
Community	<input type="text"/>
Trap Version	<input checked="" type="radio"/> V1 <input type="radio"/> V2c
<input type="button" value="Add"/>	

Trap Server Profile

Server IP	Community	Trap Version
192.168.100.150:	SNMPTEST	v2
<input type="button" value="Remove"/>		
<input type="button" value="Help"/>		

***** Trap Server Setting *****

Server IP

Setting	Descriptions	Factory Default
IP address	Enter the IP address of the Trap Server used by your network	None

Community

Setting	Descriptions	Factory Default
The maximum length is 32 bytes	Use a community string match for authentication	None

Trap Version

Setting	Descriptions	Factory Default
V1	Trap Version supports V1 and V2c	V1
V2c		

***** Trap Server Profile *****

Setting	Descriptions	Factory Default
---------	--------------	-----------------

None	Show all SNMP Trap setting	None
------	----------------------------	------

3.1.10. Security

Port Security

Port security 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.

Port Security

MAC Address

Port No.

Port Security List

MAC Address	Port

MAC Address

Setting	Descriptions	Factory Default
MAC address	Assign MAC addresses	None

Port No.

Setting	Descriptions	Factory Default
Port.01~08	Assign port number	None

NOTE 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 "Add" button.

To delete a static MAC address

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

Port Security List

Setting	Descriptions	Factory Default
None	Display current port security list	None

IP Security

IP security can enable/disable remote management from WEB or Telnet or SNMP. Additionally, IP security can restrict remote management to some specific IP addresses. Only these secure IP addresses can manage this switch remotely.

IP Security

IP Security Mode: ▼

- Enable WEB Management
- Enable Telnet Management
- Enable SNMP Management

Secure IP List

Secure IP1	<input type="text" value="0.0.0.0"/>
Secure IP2	<input type="text" value="0.0.0.0"/>
Secure IP3	<input type="text" value="0.0.0.0"/>
Secure IP4	<input type="text" value="0.0.0.0"/>
Secure IP5	<input type="text" value="0.0.0.0"/>
Secure IP6	<input type="text" value="0.0.0.0"/>
Secure IP7	<input type="text" value="0.0.0.0"/>
Secure IP8	<input type="text" value="0.0.0.0"/>
Secure IP9	<input type="text" value="0.0.0.0"/>
Secure IP10	<input type="text" value="0.0.0.0"/>

IP Security Mode

Setting	Descriptions	Factory Default
Disable	Disable IP security	Disable
Enable	Enable IP security	

Enable WEB Management

Setting	Descriptions	Factory Default
Unmarked	Disable remote management from WEB.	Unmarked
Marked	Enable remote management from WEB.	

Enable Telnet Management

Setting	Descriptions	Factory Default
Unmarked	Disable remote management from Telnet.	Unmarked
Marked	Enable remote management from Telnet	

Enable SNMP Mangement

Setting	Descriptions	Factory Default
Unmarked	Disable remote management from SNMP	Unmarked
Marked	Enable remote management from SNMP	

Secure IP List

Setting	Descriptions	Factory Default
---------	--------------	-----------------

IP address	Assign secure IP addresses	0.0.0.0
------------	----------------------------	---------

MAC Filter

MAC Filter 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 received any frame.

MAC Filter

MAC Address

MAC Blacklist

MAC Address
<input type="text"/>

Mac Address

Setting	Descriptions	Factory Default
MAC address	Assign MAC addresses	None

NOTE To add a MAC address filter

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

To delete a filter MAC address

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

MAC Blacklist

Setting	Descriptions	Factory Default
None	Display current MAC Blacklist	None

802.1x

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. Please refer to IEEE 802.1X - Port Based Network Access Control.

Radius Server Setting

Config 802.1x Radius Server

802.1x - Radius Server Setting

Radius Server Setting

802.1x Protocol	Disable ▾
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

***** Radius Server Setting *****

802.1x Protocol

Setting	Descriptions	Factory Default
Disable	Disable 802.1x protocol	Disable
Enable	Enable 802.1x protocol	

Radius Server IP

Setting	Descriptions	Factory Default
IP address	The IP address of the authentication server.	192.168.16.3

Server Port

Setting	Descriptions	Factory Default
0~65535	The UDP port number used by the authentication server to authenticate	1812

Accounting Port

Setting	Descriptions	Factory Default
0~65535	The UDP port number used by the authentication server to retrieve accounting information	1813

Shared Key

Setting	Descriptions	Factory Default
The maximum length is 30 bytes	A key shared between this switch and authentication server	12345678

NAS, Identifier

Setting	Descriptions	Factory Default
The maximum length is 30 bytes	A string used to identify this switch	NAS_L2_SWITCH

***** **Advanced Setting** *****

Quiet Period

Setting	Descriptions	Factory Default
0~65535	Period of time during which it will not attempt to acquire a supplicant	60

TX Period

Setting	Descriptions	Factory Default
0~65535	The period of time to transmit an EAPOL PDU	30

Supplicant Timeout

Setting	Descriptions	Factory Default
1~300	The timeout conditions in the exchanges between the supplicant and authentication server	30

Server Timeout

Setting	Descriptions	Factory Default
1~300	The timeout conditions in the exchanges between the authenticator and authentication server	30

Max Requests

Setting	Descriptions	Factory Default
1~10	The number of reauthentication attempts that are permitted before the specific port becomes unauthorized	2

Re-Auth Period

Setting	Descriptions	Factory Default
1~99999	A nonzero number of seconds between periodic reauthentication of the supplications	3600

Port Authorize Configuration

Config 802.1x port authorize mode

802.1x - Port Authorize Configuration

Port	Port Authorize Mode
Port.01	Disable <input type="button" value="v"/>
Port.02	Disable <input type="button" value="v"/>
Port.03	Disable <input type="button" value="v"/>
Port.04	Disable <input type="button" value="v"/>
Port.05	Disable <input type="button" value="v"/>
Port.06	Disable <input type="button" value="v"/>
G1	Disable <input type="button" value="v"/>
G2	Disable <input type="button" value="v"/>

Port Authorize Mode

Setting	Descriptions	Factory Default
Reject	Force this port to be unauthorized	Accept
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	

Port Authorize State

Display current 802.1x port authorize state

802.1x - Port Authorize State

Port	Port Authorize State
Port.01	Disable
Port.02	Disable
Port.03	Disable
Port.04	Disable
Port.05	Disable
Port.06	Disable
G1	Disable
G2	Disable

3.1.11. Warning

Since industrial Ethernet devices are often located at the endpoints of a system, these devices will not always know what is happening elsewhere on the network. This means that an industrial Ethernet switch that connects to these devices must provide system maintainers with real-time alarm messages. Even when control engineers are out of the control room for an extended period of time, they can still be informed of the status of devices almost instantaneously when exceptions occur.

Fault Relay Setting

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

Fault Relay Setting

Power Failure

PWR 1 PWR 2

Port Link Down/Broken

Port 1 Port 2
 Port 3 Port 4
 Port 5 Port 6
 Port 7 Port 8

Power Failure

Setting	Descriptions	Factory Default
PWR 1~2	Fault alarm when any selected power failure. (This switch support dual powers)	All unmarked

Port Link Down/Broken

Setting	Descriptions	Factory Default
Port 1~8	Fault alarm when any selected port link down/broken.	All unmarked

Event & Email Warning

Sunix Switch supports different approaches to warn engineers automatically, such as email and syslog.

Event Configuration

There are two warning ways supported by system, that is SYSLOG and SMTP. Check corresponding box will enable specific system event warning to SYSLOG or SMTP.

NOTE The checkbox can not be checked when SYSLOG or SMTP is disabled.

Warning - Event Configuration

System Event Selection

Event Type	System Log	SMTP
Device cold start	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Power status	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Authentication Failure	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Super ring topology change	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Port Event Selection

Port No.	System Log	SMTP
Port.01	Link Up & Link Down <input type="button" value="v"/>	Disable <input type="button" value="v"/>
Port.02	Link Up & Link Down <input type="button" value="v"/>	Disable <input type="button" value="v"/>
Port.03	Link Up & Link Down <input type="button" value="v"/>	Disable <input type="button" value="v"/>
Port.04	Link Up & Link Down <input type="button" value="v"/>	Disable <input type="button" value="v"/>
Port.05	Link Up & Link Down <input type="button" value="v"/>	Disable <input type="button" value="v"/>
Port.06	Link Up & Link Down <input type="button" value="v"/>	Disable <input type="button" value="v"/>
G1	Link Up & Link Down <input type="button" value="v"/>	Disable <input type="button" value="v"/>
G2	Link Up & Link Down <input type="button" value="v"/>	Disable <input type="button" value="v"/>

NOTE Before config system event, it have to enable **SYSLOG Mode** or **E-mail Alert** first

***** System Event Selection*****

Device Cold Start

Setting	Descriptions	Factory Default
System Log	Alert when system restart	All unmarked
SMTP	Alert when system restart	

Power Status

Setting	Descriptions	Factory Default
System Log	Alert when power up or down	All unmarked
SMTP	Alert when power up or down	

Authentication Failure

Setting	Descriptions	Factory Default
System Log	Alert when SNMP authentication failure	All unmarked
SMTP	Alert when SNMP authentication failure	

Elite Ring Topology Change

Setting	Descriptions	Factory Default
System Log	Alert when Elite Ring topology change	All unmarked
SMTP	Alert when Elite Ring topology change	

***** Port Event Selection *****

Setting	Descriptions	Factory Default
Disable	Not alert anything	All Disable
Link up	Alert when port link up	
Link Down	Alert when port link down	
Link Up & Link Down	Alert when port link up or link down	

SysLog Configuration

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

Warning - SysLog Configuration

SYSLOG Mode	Client Only <input type="button" value="v"/>
SYSLOG Server IP Address	<input type="text" value="0.0.0.0"/>
<input type="button" value="Apply"/> <input type="button" value="Help"/>	

SYSLOG Mode

Setting	Descriptions	Factory Default
Disable	Disable SYSLOG	Disable
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

Setting	Descriptions	Factory Default
IP address	The remote SYSLOG Server IP address	0.0.0.0

SMTP Configuration

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

Warning - SMTP Configuration

E-mail Alert :

SMTP Configuration

SMTP Server IP Address :	<input type="text" value="0.0.0.0"/>
SMTP Sender E-mail :	<input type="text"/>
SMTP Mail Subject :	<input type="text" value="Automated Email Alert"/>
<input checked="" type="checkbox"/> Authentication	
Username :	<input type="text"/>
Password :	<input type="text"/>
Confirm Password :	<input type="text"/>
Rcpt e-mail Address 1 :	<input type="text"/>
Rcpt e-mail Address 2 :	<input type="text"/>
Rcpt e-mail Address 3 :	<input type="text"/>
Rcpt e-mail Address 4 :	<input type="text"/>
Rcpt e-mail Address 5 :	<input type="text"/>
Rcpt e-mail Address 6 :	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Help"/>	

E-mail Alert

Setting	Descriptions	Factory Default
Disable	Disable transmission system warning events by e-mail.	Disable
Enable	Enable transmission system warning events by e-mail.	

SMTP Server IP Address

Setting	Descriptions	Factory Default
IP address	The SMTP server IP address	0.0.0.0

SMTP Sender E-Mail

Setting	Descriptions	Factory Default
E-mail address	The sender's E-mail address of the mail.	None

SMTP Mail Subject

Setting	Descriptions	Factory Default
The maximum length is 31 bytes	The Subject of the mail.	Automated Email Alert

Authentication

Setting	Descriptions	Factory Default
---------	--------------	-----------------

Unmarked	Checked if the SMTP server needs authentication. If marked the field, it will need to config 3 option: Username: the authentication username. Password: the authentication password. Confirm Password: re-enter password	Unmarked
Marked		

Recipient E-mail Address

Setting	Descriptions	Factory Default
E-mail address	The recipient's E-mail address. It supports 6 recipients for a mail	None

3.1.12. Monitor and Diag

Sunix Switch provides several important tools for administrators to diagnose network systems.

MAC Address Table

Refer to IEEE 802.1D Section 7.9. The MAC Address Table, that is Filtering Database, supports queries by the Forwarding Process, as to whether a frame received by a given port with a given destination MAC address is to be forwarded through a given potential transmission port. This page shows all MAC addresses mapping to a selected port in table.

MAC Address Table

Port No :

Current MAC Address

0013028FE44F	DYNAMIC
0090CCB89A3A	DYNAMIC
01005E7FFFA	DYNAMIC

Dynamic Address Count : 3
 Static Address Count : 0

Port No

Setting	Descriptions	Factory Default
Port.01~08	Display all MAC addresses mapping to a selected port in table	Port.01

Clear MAC Table

Setting	Descriptions	Factory Default
None	The " Clear MAC Table " button is to clear all MAC addresses in table.	None

Port Statistic

This page shows several statistics counters for all ports.

- 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 detected by this port.

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	Up	Enable	10862029	0	695208	0	0	0
Port.02	100TX	Up	Enable	10662566	0	90058	0	0	0
Port.03	100TX	Up	Enable	10765923	0	100606	0	0	0
Port.04	100TX	Down	Enable	7048	0	1874	0	0	0
Port.05	100TX	Down	Enable	92640	0	1237	0	0	0
Port.06	100TX	Down	Enable	17516	0	4092	0	0	0
G1	1000TX	Up	Enable	1140916	0	12489506	0	0	0
G2	1000TX	Up	Enable	8196650	0	766639	23	0	0

Clear

Setting	Descriptions	Factory Default
None	The "Clear" button is to reset all counters to zero for all ports	None

Port Mirror

Port mirror supports TX (egress) only monitoring, RX (ingress) only monitoring or TX and 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 ingresses 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 Mirror

Port	Destination Port		Source Port	
	RX	TX	RX	TX
Port.01	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.02	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.03	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.04	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.05	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port.06	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
G1	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>
G2	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

Event Log

1: Jan 1 00:33:32 : Clear System Log Table!
2: Jan 1 00:54:58 : G2 : Link Down!
3: Jan 1 51:21:15 : G2 : Link Up!
4: Jan 1 51:21:44 : G2 : Link Down!
5: Jan 1 51:21:45 : G2 : Link Up!
6: Jan 1 56:26:29 : G2 : Link Down!
7: Jan 1 56:26:31 : G2 : Link Up!
8: Jan 1 56:27:26 : G2 : Link Down!
9: Jan 1 56:27:32 : G2 : Link Up!
10: Jan 1 56:28:11 : G2 : Link Down!
11: Jan 1 56:28:12 : G2 : Link Up!
12: Jan 1 01:33:07 : G2 : Link Down!
13: Jan 1 15:25:53 : G2 : Link Up!
14: Jan 1 15:26:25 : G2 : Link Down!
15: Jan 1 15:26:27 : G2 : Link Up!
16: Jan 1 17:35:55 : Port.04: Link Up!
17: Jan 1 17:36:29 : Port.02: Link Down!
18: Jan 1 17:36:31 : Port.02: Link Up!
19: Jan 1 17:48:04 : Port.04: Link Down!
20: Jan 1 17:48:19 : Port.04: Link Up!

Page.1

Reload

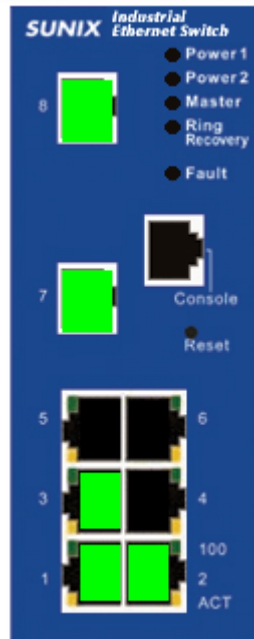
Setting	Descriptions	Factory Default
None	The " Reload " button is to get the newest event logs and refresh this page	None

Clear

Setting	Descriptions	Factory Default
None	The " Clear " button is to clear all logs in system.	None

3.1.13. Front Panel

Display front panel



Close

Close

Setting	Descriptions	Factory Default
None	The "Close" button is to close front panel.	None

3.1.14. Save Configuration

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

Save Configuration



Save

Setting	Descriptions	Factory Default
None	The "Save" button is to save current configuration of switch.	None

3.2. Configuration by RS-232 Serial Console (9600, 8, none, 1, none)

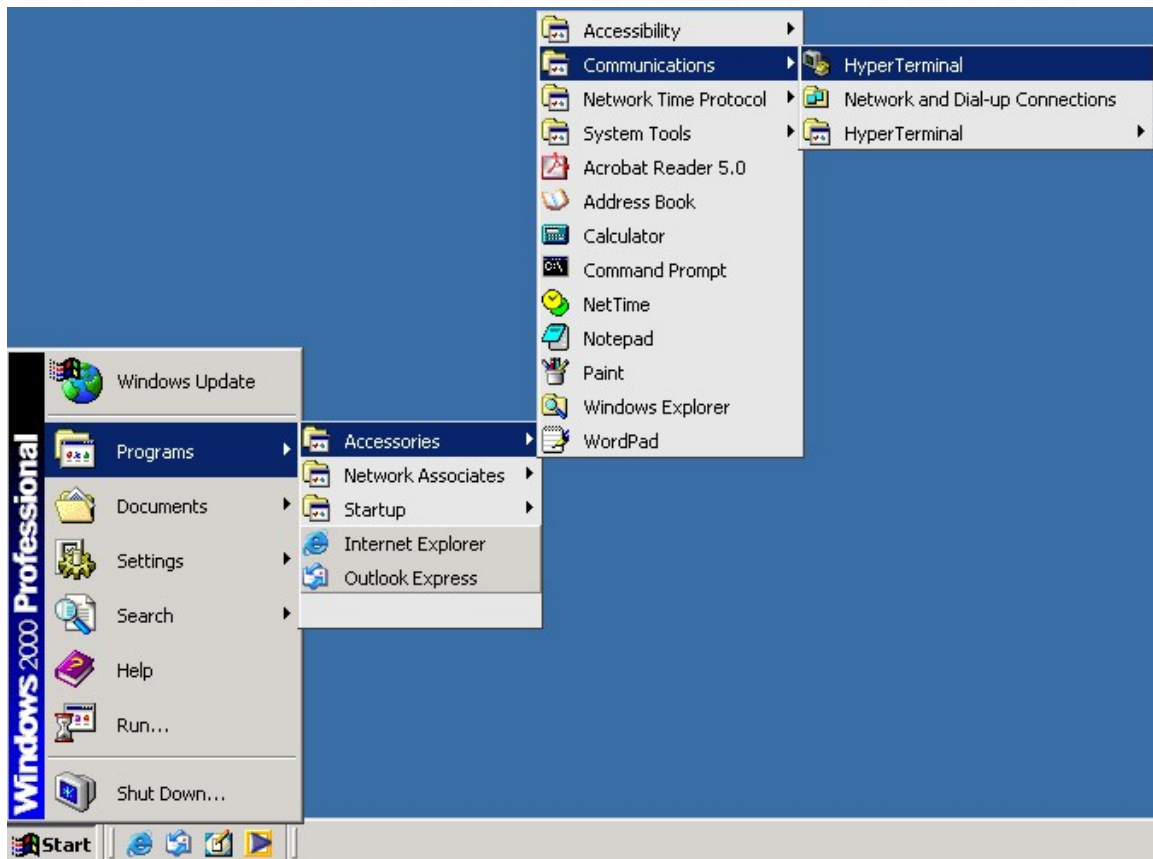
NOTE Connection Caution

1. Before Config by RS-232 serial console, use an RJ45 to DB9-F cable to connect Sunix Switch's RS-232 Console port to your PC's COM port (generally COM1 or COM2, depending on how your system is set up).
2. You cannot connect to Sunix Switch simultaneously by serial console and by Telnet.
3. You can connect to Sunix Switch simultaneously by web browser and serial console, or by web browser and by Telnet.
4. Recommendation—when connecting to Sunix Switch by web browser, do NOT simultaneously connect by either serial console or via Telnet.

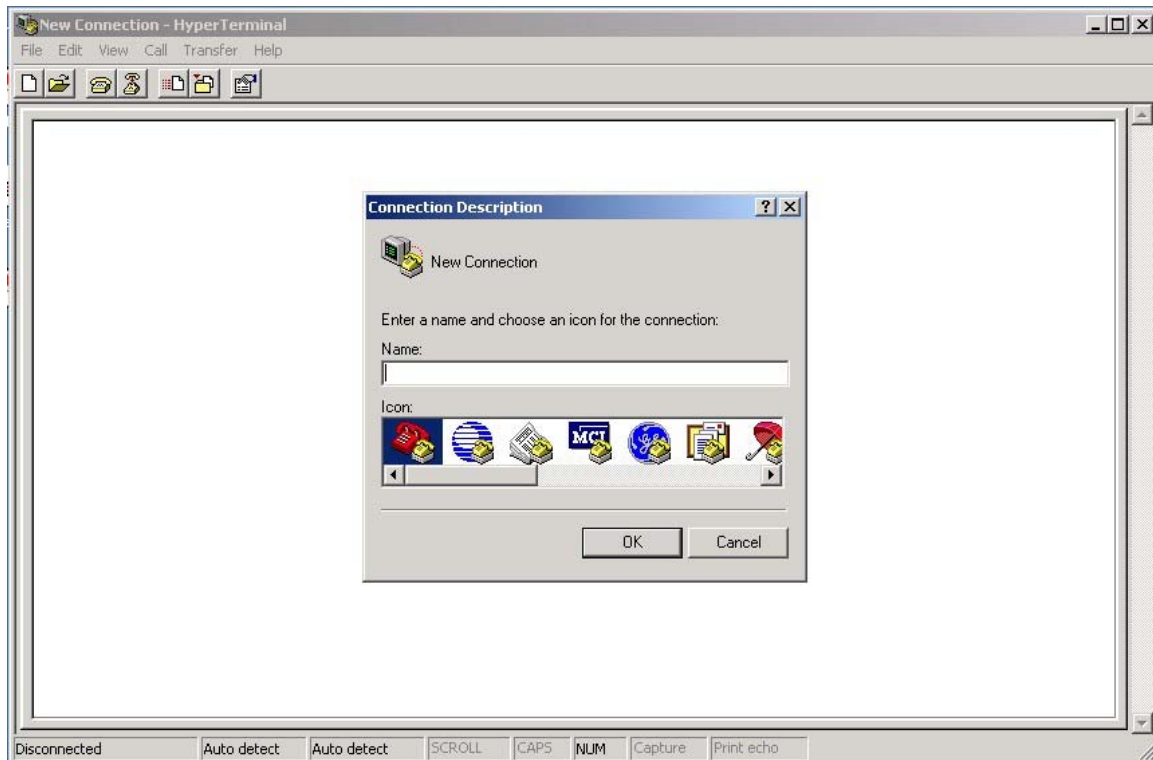
By following this advice, you can maintain better control over how your Sunix Switch is managed.

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

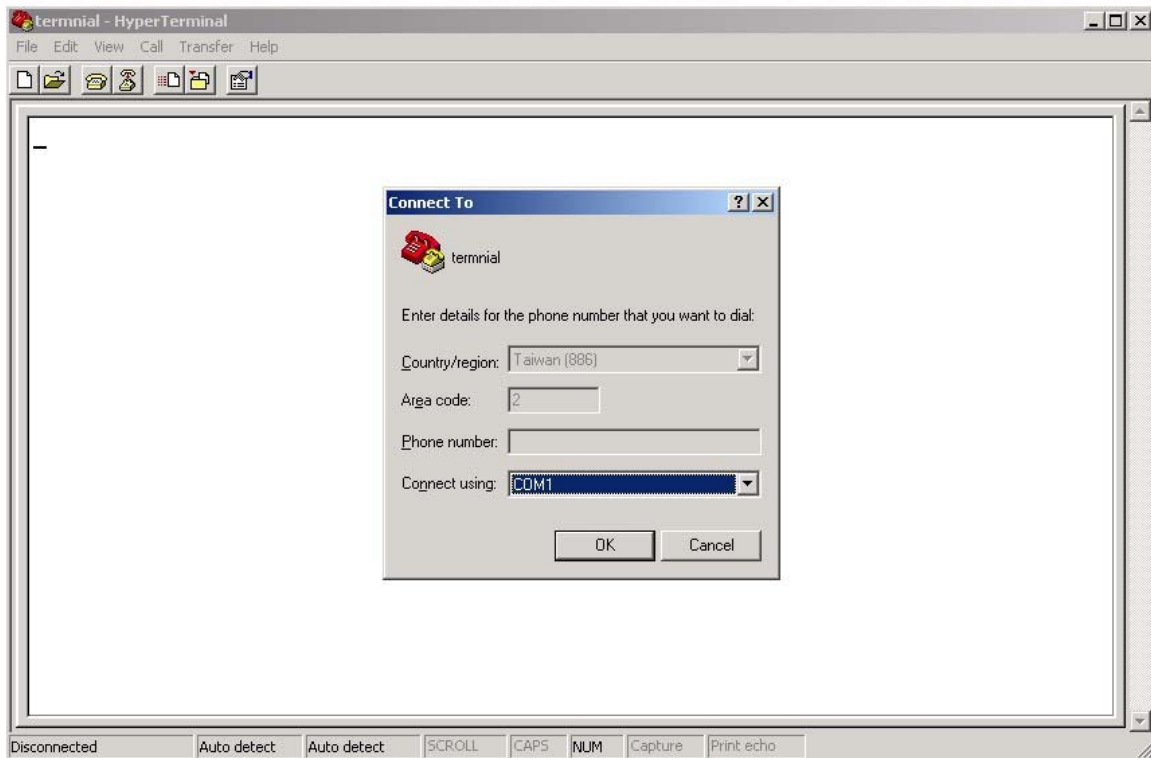
- (1) From the Windows desktop, click on Start -> Programs -> Accessories -> Communications -> Hyper Terminal



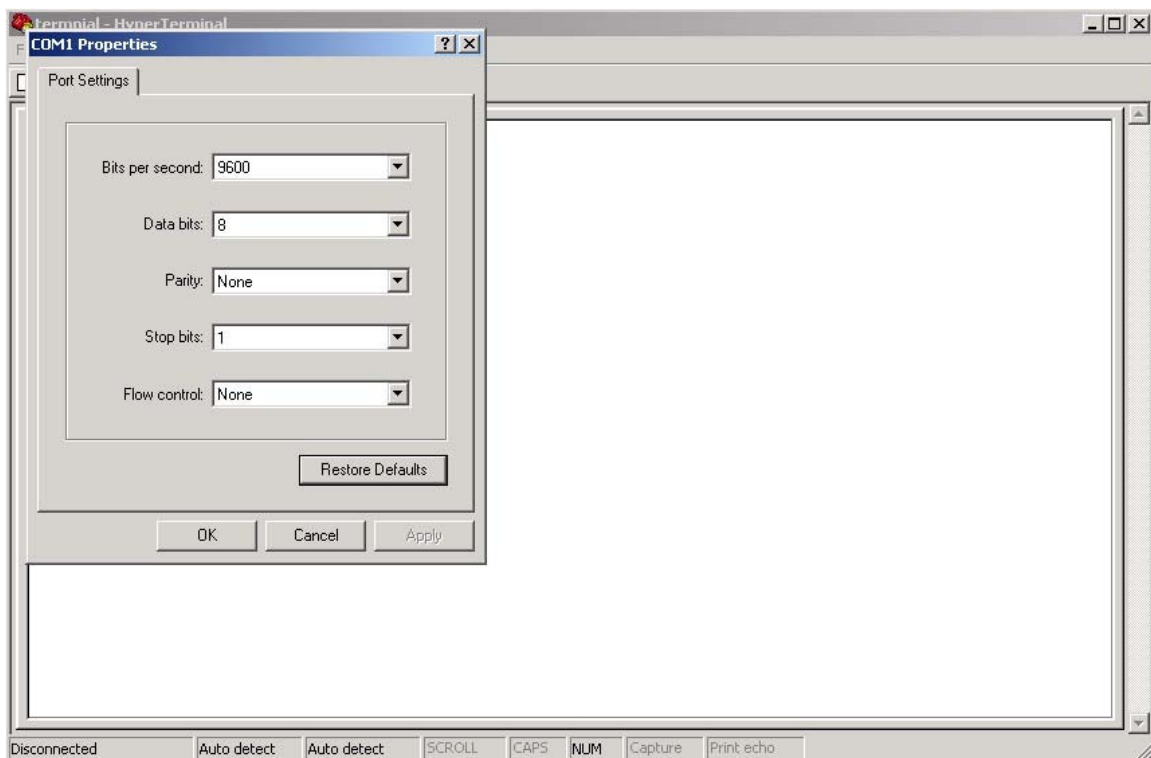
(2) Input a name for new connection



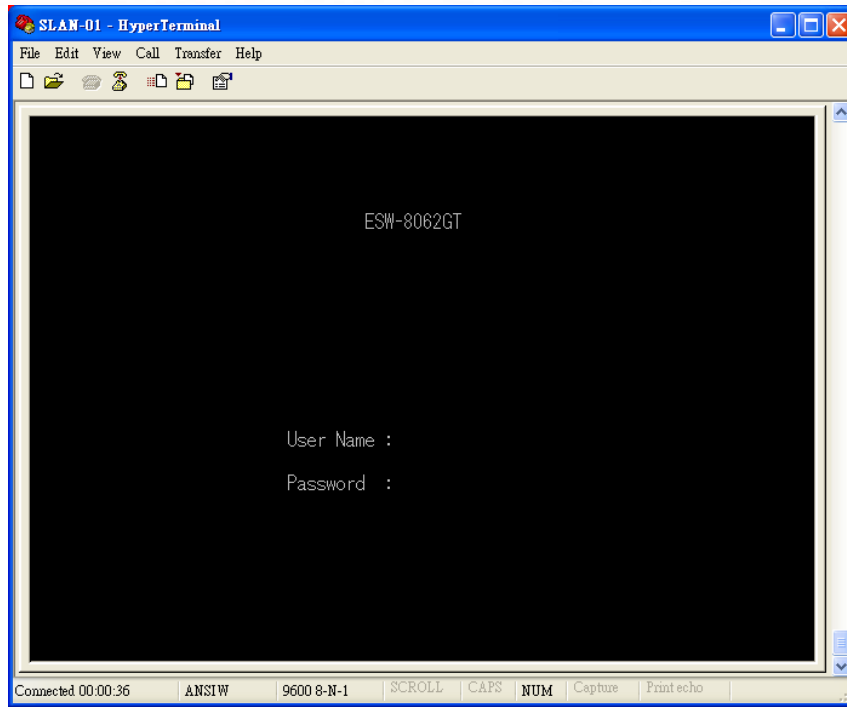
(3) Select connet using COM port number



- (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



- (5) The Console login screen will appear. Use the keyboard enter the Console Username (**admin**) and Password (**admin**), and then press Enter.



3.2.1. Commands Level

1. User EXEC Level

```
switch>_
```

2. Privileged EXEC Level

```
switch>en
switch#
```

3. Global configuration Level

```
switch>en
switch#configure
switch(config)#
```

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 user level are a subset of those available at the privileged level. Use this mode to <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • 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 exist to privileged EXEC mode, or end .	Use this mode to configure parameters for the switch and Ethernet ports.

3.2.2 Commands Set List

User EXEC **E**
 Privileged EXEC **P**
 Global configuration **G**
 VLAN database **V**
 Interface configuration **I**

3.2.2.1 System Commands Set

Netstar Commands	Level	Description	Example
show config	E	Show switch configuration	switch>show config
show terminal	P	Show console information	switch#show terminal
menu	E	Enter MENU mode	switch>menu
write memory	P	Save user 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 clients
show dhcpserver ip-binding	P	Show IP-Binding information of DHCP server	switch#show dhcpserver ip-binding
no dhcpserver	G	Disable DHCP server function	switch(config)#no dhcpserver
security enable	G	Enable IP security function	switch(config)#security enable
security http	G	Enable IP security of HTTP server	switch(config)#security http
security telnet	G	Enable IP security of telnet server	switch(config)#security telnet
security ip [Index(1..10)] [IP Address]	G	Set the IP security list	switch(config)#security ip 1 192.168.1.55
show security	P	Show the information of 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

3.2.2.2. Port Commands Set

Netstar Commands	Level	Description	Example
interface fastEthernet [Portid]	G	Choose the port for modification.	switch(config)#interface fastEthernet 2
duplex [full half]	I	Use the duplex configuration command to specify the duplex mode of operation for Fast Ethernet.	switch(config)#interface fastEthernet 2 switch(config-if)#duplex full
speed [10 100 1000 auto]	I	Use the speed configuration command to specify the speed mode of operation for Fast Ethernet., the speed can't be set to 1000 if the port isn't a giga port..	switch(config)#interface fastEthernet 2 switch(config-if)#speed 100
flowcontrol mode [Symmetric Asymmetric]	I	Use the flowcontrol configuration command on Ethernet ports to control traffic rates during congestion.	switch(config)#interface fastEthernet 2 switch(config-if)#flowcontrol mode Asymmetric
no flowcontrol	I	Disable flow control of interface	switch(config-if)#no flowcontrol
security enable	I	Enable security of interface	switch(config)#interface fastEthernet 2 switch(config-if)#security enable
no security	I	Disable security of interface	switch(config)#interface fastEthernet 2 switch(config-if)#no security
bandwidth type all	I	Set interface ingress limit frame type to "accept all frame"	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type all
bandwidth type broadcast-multicast-flooded-unicast	I	Set interface ingress limit frame type to "accept broadcast, multicast, and flooded unicast frame"	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type broadcast-multicast-flooded-unicast
bandwidth type broadcast-multicast	I	Set interface ingress limit frame type to "accept broadcast and multicast frame"	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type broadcast-multicast

bandwidth type broadcast-only	I	Set interface ingress limit frame type to "only accept broadcast frame"	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type broadcast-only
bandwidth in [Value]	I	Set interface input bandwidth. Rate Range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports, and zero means no limit.	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth in 100
bandwidth out [Value]		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

3.2.2.3. Trunk Commands Set

Netstar Commands	Level	Description	Example
aggregator priority [1~65535]	G	Set port group system priority	switch(config)#aggregator priority 22
aggregator activityport [Port Numbers]	G	Set activity port	switch(config)#aggregator activityport 2
aggregator group [GroupID] [Port-list] lACP workp [Workport]	G	Assign a trunk group with LACP active. [GroupID] :1~3 [Port-list]:Member port list, This parameter could be a port range(ex.1-4) or a port list separate by a comma(ex.2, 3, 6) [Workport]: The 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] :1~3 [Port-list]:Member port list, This parameter could be a port range(ex.1-4) or a port list separate by a comma(ex.2, 3, 6)	switch(config)#aggregator group 1 2-4 nolACP or switch(config)#aggregator group 1 3,1,2 nolACP
show aggregator	P	Show the information of trunk group	switch#show aggregator
no aggregator lACP [GroupID]	G	Disable the LACP function of trunk group	switch(config)#no aggregator lACP 1

no aggregator group [GroupID]	G	Remove a trunk group	switch(config)#no aggregator group 2
---	---	----------------------	--------------------------------------

3.2.2.4. VLAN Commands Set

Netstar 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 8021q 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 8021q port 3 access-link untag 33
vlan 8021q port [PortNumber] trunk-link tag [TaggedVID List]	V	Assign a trunk link for VLAN by port, if the port belong to a trunk group, this command can't be applied.	switch(vlan)#vlan 8021q port 3 trunk-link tag 2,3,6,99 or switch(vlan)#vlan 8021q port 3 trunk-link tag 3-20
vlan 8021q port [PortNumber] hybrid-link untag [UntaggedVID] tag [TaggedVID List]	V	Assign a hybrid link for VLAN by port, if the port belong to a trunk group, this command can't be applied.	switch(vlan)# vlan 8021q port 3 hybrid-link untag 4 tag 3,6,8 or switch(vlan)# vlan 8021q port 3 hybrid-link untag 5 tag 6-8
vlan 8021q aggregator [TrunkID] access-link untag [UntaggedVID]	V	Assign a access link for VLAN by trunk group	switch(vlan)#vlan 8021q aggregator 3 access-link untag 33
vlan 8021q aggregator [TrunkID] trunk-link tag [TaggedVID List]	V	Assign a trunk link for VLAN by trunk group	switch(vlan)#vlan 8021q aggregator 3 trunk-link tag 2,3,6,99 or switch(vlan)#vlan 8021q aggregator 3 trunk-link tag 3-20
vlan 8021q aggregator [PortNumber] hybrid-link untag [UntaggedVID] tag [TaggedVID List]	V	Assign a hybrid link for VLAN by trunk group	switch(vlan)# vlan 8021q aggregator 3 hybrid-link untag 4 tag 3,6,8 or switch(vlan)# vlan 8021q aggregator 3 hybrid-link untag 5 tag 6-8
show vlan [VID] or show vlan	V	Show VLAN information	switch(vlan)#show vlan 23

3.2.2.5. Spanning Tree Commands Set

Netstar Commands	Level	Description	Example
spanning-tree enable	G	Enable spanning tree	switch(config)#spanning-tree enable
spanning-tree priority [0~61440]	G	Configure spanning tree priority parameter	switch(config)#spanning-tree priority 32767
spanning-tree max-age [seconds]	G	Use the spanning-tree max-age global configuration command to change the interval between messages the spanning tree receives from the root switch. If a switch does not receive a bridge protocol data unit (BPDU) message from the root switch within this interval, it recomputed the Spanning Tree Protocol (STP) topology.	switch(config)# spanning-tree max-age 15

spanning-tree hello-time [seconds]	G	Use the spanning-tree hello-time global configuration command to specify the interval between hello bridge protocol data units (BPDUs).	switch(config)#spanning-tree hello-time 3
spanning-tree forward-time [seconds]	G	Use the spanning-tree forward-time global configuration command to set the forwarding-time for the specified spanning-tree instances. The forwarding time 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 [1~200000000]	I	Use the spanning-tree cost interface configuration command to set the path cost for Spanning Tree Protocol (STP) calculations. In the event of a loop, spanning tree considers the path cost when selecting an interface to place into the forwarding state.	switch(config)#interface fastEthernet 2 switch(config-if)#stp-path-cost 20
stp-path-priority [Port Priority]	I	Use the spanning-tree port-priority interface configuration command to configure a port priority that is used when two switches tie for position as the root switch.	switch(config)#interface fastEthernet 2 switch(config-if)# stp-path-priority 127
stp-admin-p2p [Auto True False]	I	Admin P2P of STP priority on this interface.	switch(config)#interface fastEthernet 2 switch(config-if)# stp-admin-p2p Auto
stp-admin-edge [True False]	I	Admin Edge of STP priority on this interface.	switch(config)#interface fastEthernet 2 switch(config-if)# stp-admin-edge True
stp-admin-non-stp [True False]	I	Admin NonSTP of STP priority on this interface.	switch(config)#interface fastEthernet 2 switch(config-if)# stp-admin-non-stp False
Show spanning-tree	E	Display a summary of the spanning-tree states.	switch>show spanning-tree
no spanning-tree	G	Disable spanning-tree.	switch(config)#no spanning-tree

3.2.2.6. QoS Commands Set

Netstar 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

3.2.2.7. IGMP Commands Set

Netstar 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

3.2.2.8. Mac / Filter Table Commands Set

Netstar 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

3.2.2.9. SNMP Commands Set

Netstar Commands	Level	Description	Example
snmp agent-mode [v1 v2c v3]	G	Select the agent mode of SNMP	switch(config)#snmp agent-mode v1v2c
snmp-server host [IP address] community [Community-string] trap-version [v1 v2c]	G	Configure SNMP server host information and community string	switch(config)#snmp-server host 192.168.1.50 community public trap-version v1 (remove) Switch(config)# no snmp-server host 192.168.1.50
snmp community-strings [Community-string] right [RO RW]	G	Configure the community string right	switch(config)#snmp community-strings public right RO or switch(config)#snmp community-strings public right RW
snmp snmpv3-user [User Name] password [Authentication Password] [Privacy Password]	G	Configure the userprofile for SNMPV3 agent. Privacy password could be empty.	switch(config)#snmp snmpv3-user test01 password AuthPW PrivPW
show snmp	P	Show SNMP configuration	switch#show snmp
show snmp-server	P	Show specified trap server information	switch#show snmp-server
no snmp community-strings [Community]	G	Remove the specified community.	switch(config)#no snmp community-strings public
no snmp snmpv3-user [User Name] password [Authentication Password] [Privacy Password]	G	Remove specified user of SNMPv3 agent. Privacy password could be empty.	switch(config)# no snmp snmpv3-user test01 password AuthPW PrivPW
no snmp-server host [Host-address]	G	Remove the SNMP server host.	switch(config)#no snmp-server 192.168.1.50

3.2.2.10. Port Mirroring Commands Set

Netstar 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

3.2.2.11. 802.1x Commands Set

Netstar 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	switch(config)#interface fastethernet 3 switch(config-if)#8021x portstate accept

		selected port.	
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

3.2.2.12. TFTP Commands Set

Netstar 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

3.2.2.13. SystemLog, SMTP and Even Commands Set

Netstar 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 super-ring-topology-change [Systemlog SMTP Both]	G	Set super ring topology changed event type	switch(config)#event super-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 super-ring-topology-change	G	Disable super ring topology changed event type	switch(config)#no event super-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 smpt
show systemlog	P	Show system log client & server information	switch#show systemlog

3.2.2.14. SNTP Commands Set

Netstar Commands	Level	Description	Example
<code>sntp enable</code>	G	Enable SNTP function	switch(config)#sntp enable
<code>sntp daylight</code>	G	Enable daylight saving time, if SNTP function is inactive, this command can't be applied.	switch(config)#sntp daylight
<code>sntp daylight-period</code> [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
<code>sntp daylight-offset</code> [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
<code>sntp ip</code> [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
<code>sntp timezone</code> [Timezone]	G	Set timezone index, use "show sntp timzezone" command to get more information of index number	switch(config)#sntp timezone 22
<code>show sntp</code>	P	Show SNTP information	switch#show sntp
<code>show sntp timezone</code>	P	Show index number of time zone list	switch#show sntp timezone
<code>no sntp</code>	G	Disable SNTP function	switch(config)#no sntp
<code>no sntp daylight</code>	G	Disable daylight saving time	switch(config)#no sntp daylight

3.2.2.15. Elite Ring Commands Set

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

3.3. Configuration by Telnet Console

You may use Telnet to access Sunix Switch's console over a network. To be able to access Sunix Switch's functions over the network (by Telnet or Web Browser) from a PC host that is connected to the same LAN as Switch, you need to make sure that the PC host and Sunix Switch are on the same logical subnetwork. To do this, check your PC host's IP address and netmask. By default, Sunix ESW's IP address is 192.168.1.1 and ESW's netmask is 255.255.255.0 (for a Class C network). If you do not change these values, and your PC host's netmask is 255.255.255.0, then its IP address must have the form 192.168.1.xxx.

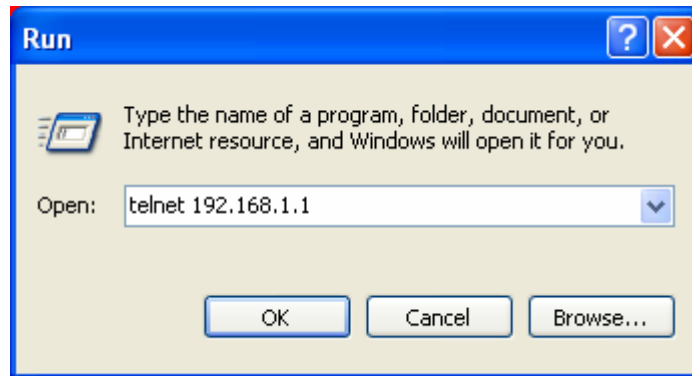
NOTE To use ESW's management and monitoring functions from a PC host connected to the same LAN as ESW, you must make sure that the PC host and ESW are on the same logical subnetwork.

NOTE Before accessing the console via Telnet, first connect one of ESW Switch's RJ45 Ethernet ports to your Ethernet LAN, or directly to your PC's Ethernet NIC. You can establish a connection with either a straight-through or cross-over Ethernet cable. If you have difficulty connecting, refer to the Auto MDI/MDI-X Connection section from the Hardware installation Guide for more information about the different types of Ethernet cables and ports.

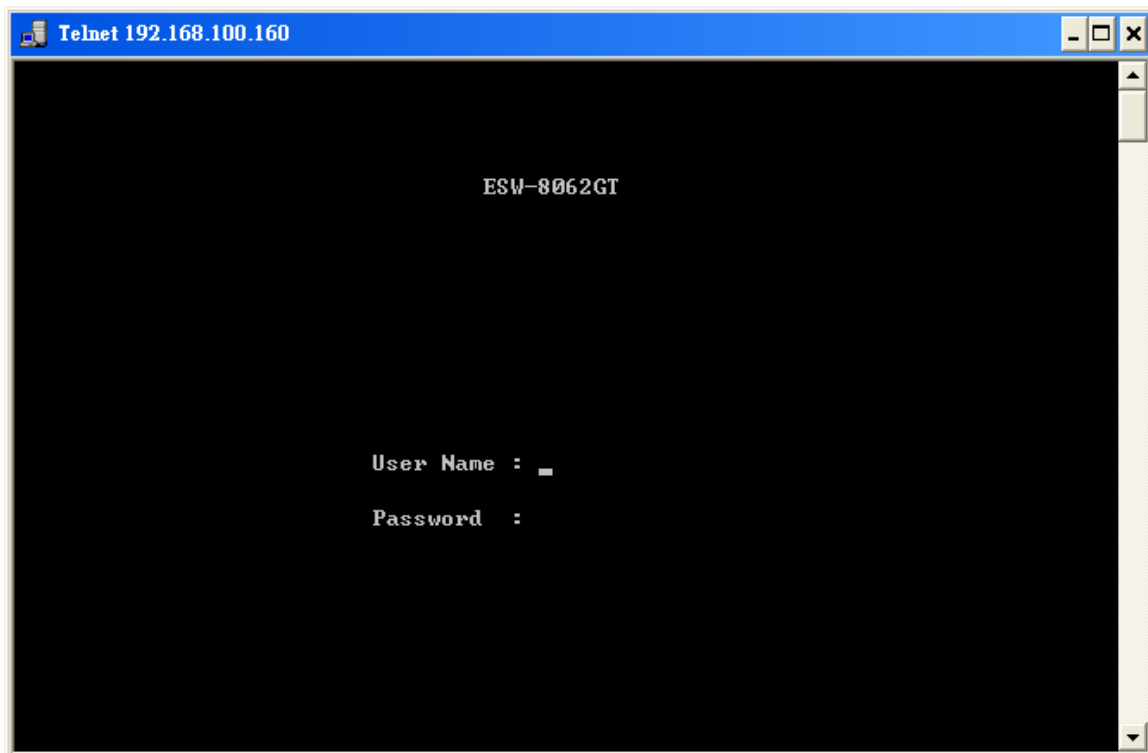
NOTE ESW Switch's default IP is 192.168.1.1

Follow the steps below to access the console via Telnet.

(1) Telnet to ESW Switch's IP address from the Windows **Run** window (or from the MS-DOS prompt).



(2) The Console login screen will appear. Use the keyboard enter the Console Username and Password that is the same as the Web Browser password), and then press Enter.



NOTE The Telnet Console looks and operates in precisely the same manner as the RS-232 Console.

3.4. Configuration by Sunix Commander

Sunix Commander is a comprehensive Windows-based GUI that is used to configure and maintain multiple Sunix Switches. A suite of useful utilities is available to help you locate Sunix Switches attached to the same LAN as the PC host (regardless of whether or not you know the IP addresses of the switches), connect to a Sunix Switch whose IP address is known, modify the network configurations of one or multiple Sunix Switches, and update the firmware of one or more Sunix Switches. Sunix Commander is designed to provide you with instantaneous control of *all* of your Sunix Switches,

regardless of location. You may download the Sunix Commander software from Industrial-managed's website free of charge. (**Sunix Commander Utility only support Sunix Switch**)

The following topics are covered:

- Starting Sunix Commander
- Discovery Function
- Switch setting
- IP Configuration
- Backup & Restore
- Upgrade Firmware
- Group IP Setting Wizard
- Group Firmware Update Wizard

NOTE To use Sunix Commander from a PC host connected to the same LAN as ESW, you must make sure that the PC host and ESW switch are on the same logical subnetwork.

NOTE If ESW switch is configured for other VLAN settings, you must make sure your PC host is on the management VLAN.

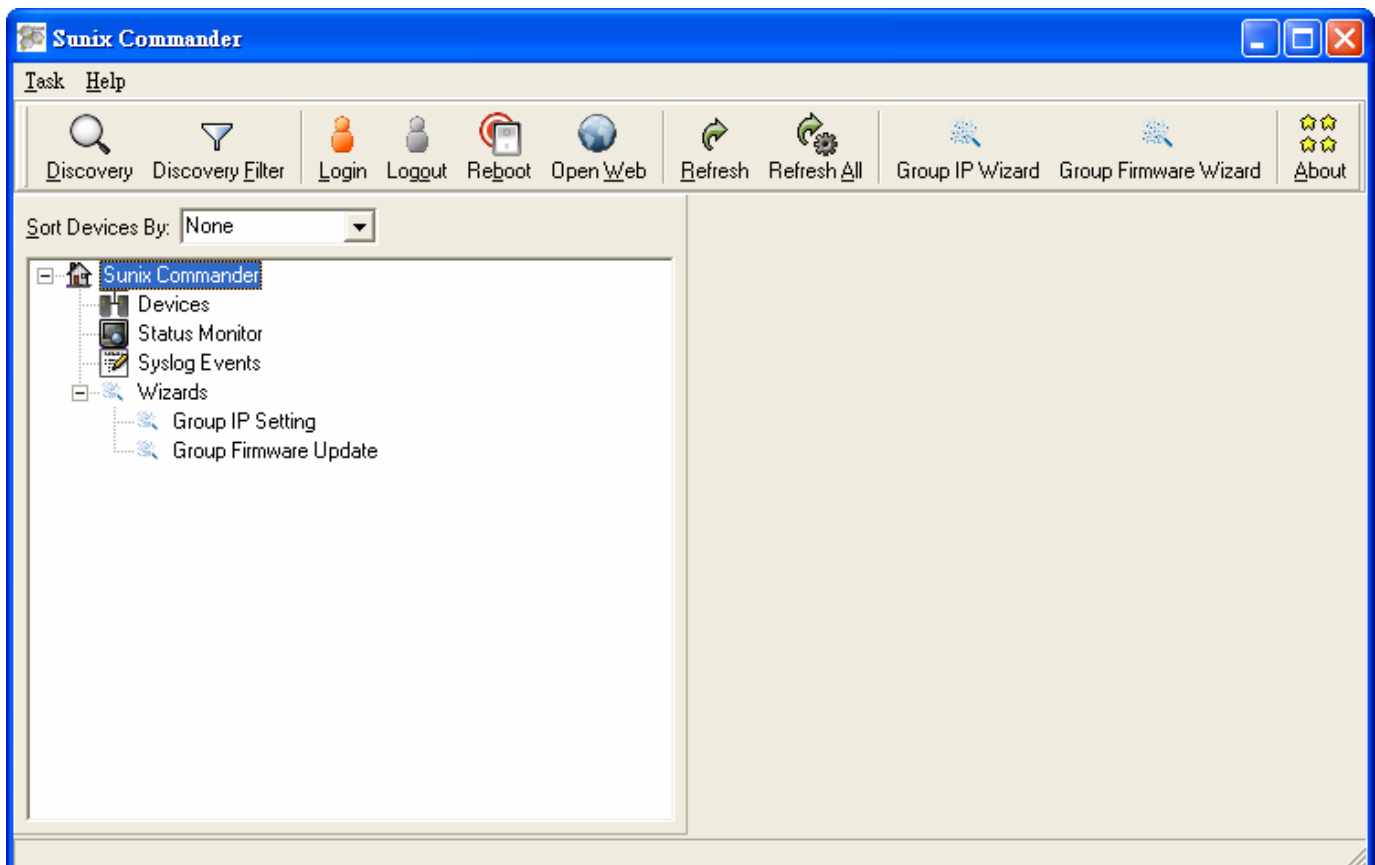
NOTE Before accessing ESW Switch by using Sunix Commander, first connect one of ESW Switch's RJ45 Ethernet ports to your Ethernet LAN, or directly to your PC's Ethernet NIC. You can establish a connection with either a straight-through or cross-over Ethernet cable. If you have difficulty connecting, refer to the Auto MDI/MDI-X Connection section from the Hardware installation Guide for more information about the different types of Ethernet cables and ports.

NOTE Sunix Commander Utility only support Sunix switch.

NOTE 任何設定改變後都必須執行 "Save To Flash" 來儲存設定, 否則一旦關掉電源後, 將回復到之前的設定值
You have to execute "Save To Flash" when you change any settings, or else back to previous setting when turn off power.

Follow the steps below to access ESW Switch by using Sunix Commander.

3.4.1. Starting Sunix Commander



NOTE If there have multi devices, and their IP address are all the same, it must config their IP address first and make

their IP address are different.(By using Basic -> IP configuration)

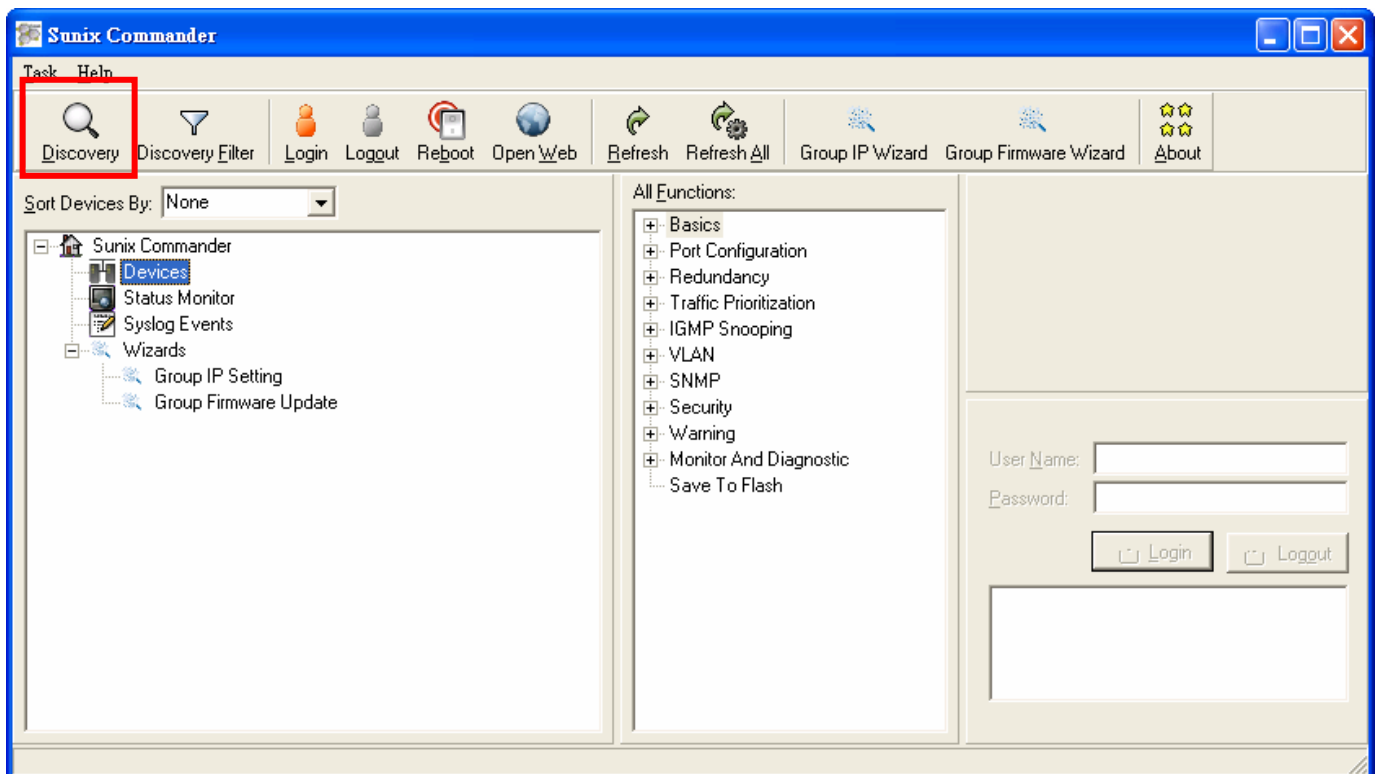
NOTE When all IP address of devices are different, **first**, we must **Login** to device **then** start to config switch setting, backup configuration, restore configuration, upgrade firmware, reboot device, or save configuration.

3.4.2. Discovery Function

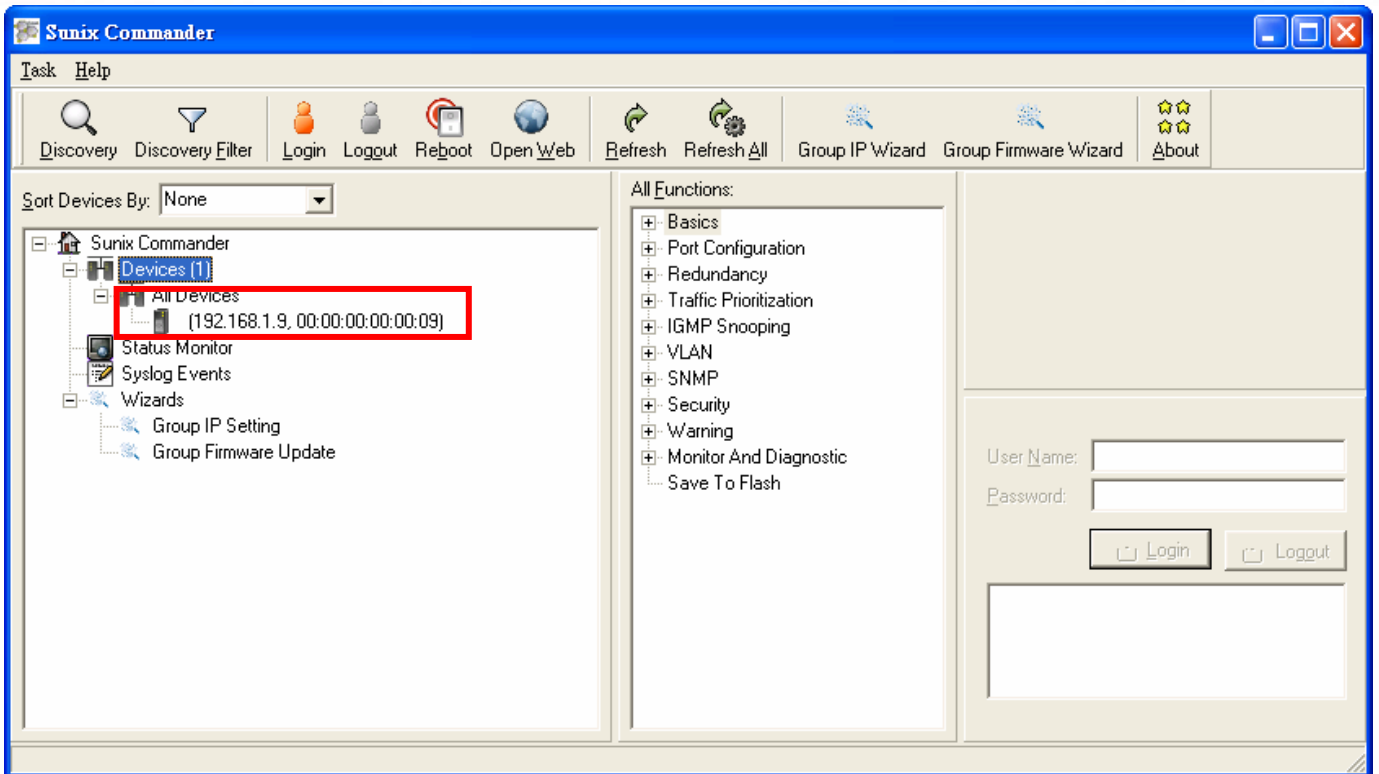
Discovery

The discovery function is one of function in the windows utility programme. You can start it under Task item menu or press right-button of mouse. The discovery function can find all Sunix devices in Ethernet, even if devices' IP are assigned in different subnet with your computer. After discovery function success, the programme will list on "All devices" list in the detected Sunix devices in the left part of programme window. You can select one or mutli-select devices in the list, and operate or setting them by the following functions.

(1) Click "Discovery" icon



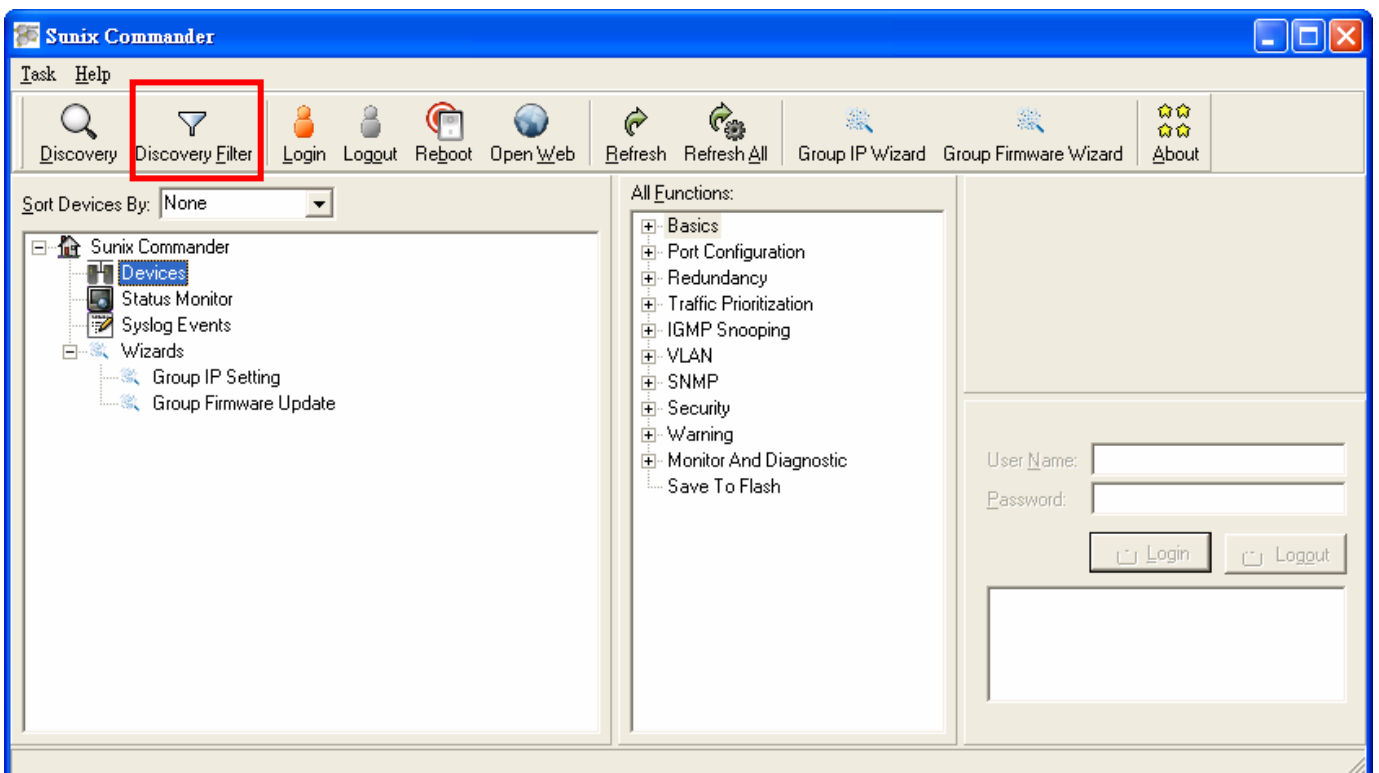
(2) Sunix Commander will search and list all items. (For example: search one switch and IP address 192.168.1.9)



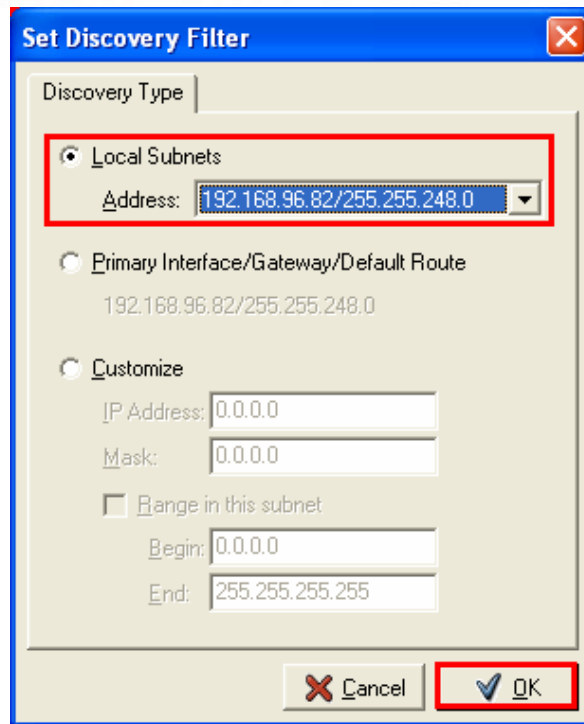
Discovery Filter

What differences between “Discovery Filter” and “Discovery”? “Discovery” could search all Sunix Switches on LANs, but “Discovery Filter” could restrict the searching conditions to find out the matching one.

- (1) Click “Discovery Filter” icon.



- (2) The setting windows appeared.



Set Discovery Filter

Discovery Type

Local Subnets
Address: 192.168.96.82/255.255.248.0

Primary Interface/Gateway/Default Route
192.168.96.82/255.255.248.0

Customize
IP Address: 0.0.0.0
Mask: 0.0.0.0
 Range in this subnet
Begin: 0.0.0.0
End: 255.255.255.255

Cancel OK

Local Subnets

Setting	Descriptions	Factory Default
None	Using current setting parameters of PC (IP Address & Subnet Mask) to search switches which located in the same subnet.	Decide for system's setting

Primary Interface/Gateway/Default Route

Setting	Descriptions	Factory Default
None	Setting final IP Address that distributed by system.	Decide for system's setting

Customize

Setting	Descriptions	Factory Default
None	Importing IP Address to search all Switches in the same subnet.	None

IP Address

Setting	Descriptions	Factory Default
None	Importing IP Address to search all Switches in the same subnet.	0.0.0.0

Mask

Setting	Descriptions	Factory Default
None	Importing Subnet Mask to search all Switches in the same subnet.	0.0.0.0

Range in this subnet

Setting	Descriptions	Factory Default
Mark	Import IP Address to search all Switches.	Unmark
Unmark	Do not import IP Address to search all Switches.	

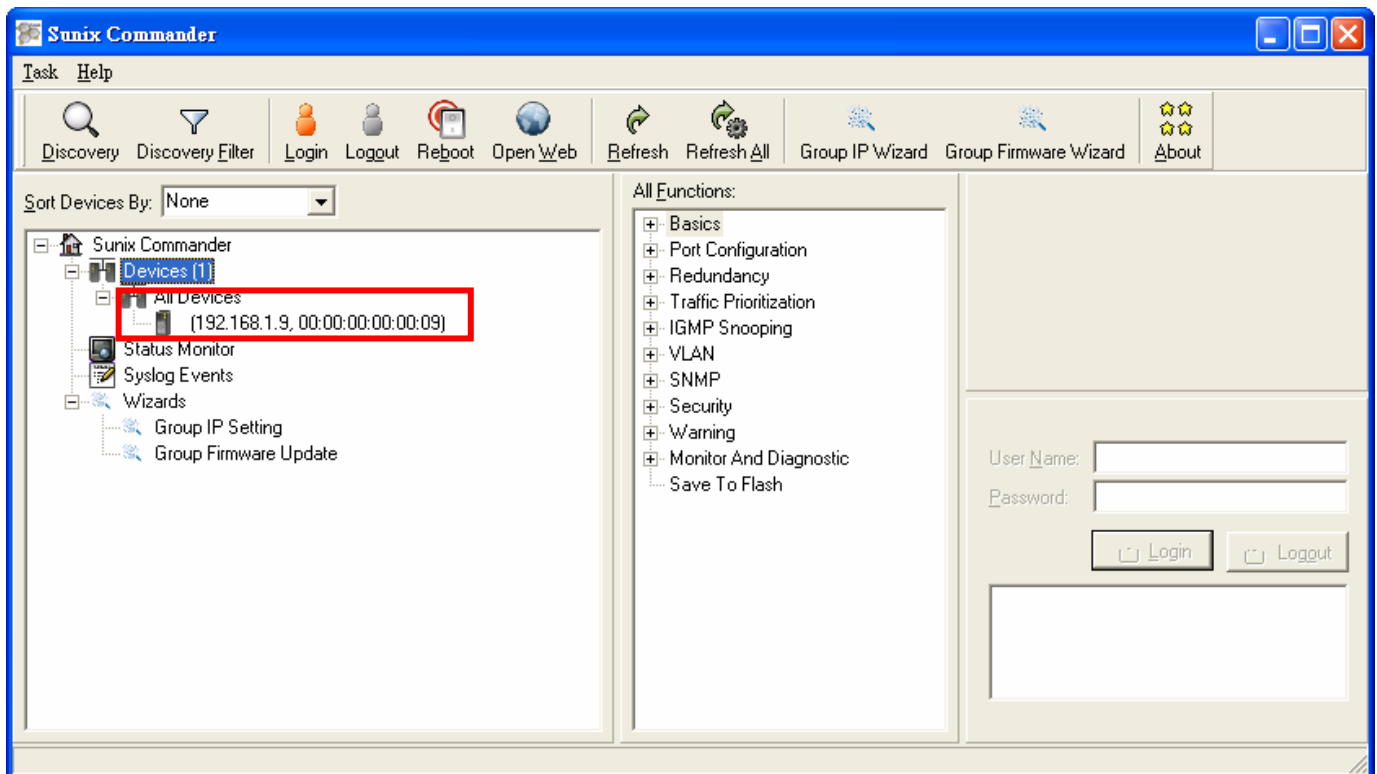
Begin

Setting	Descriptions	Factory Default
None	Searching initial IP Address	0.0.0.0

End

Setting	Descriptions	Factory Default
None	Searching final IP Address	0.0.0.0

(3) Sunix Commander will search and list all items. (For example: search one switch and IP address 192.168.1.9)



3.4.3. Switch Setting

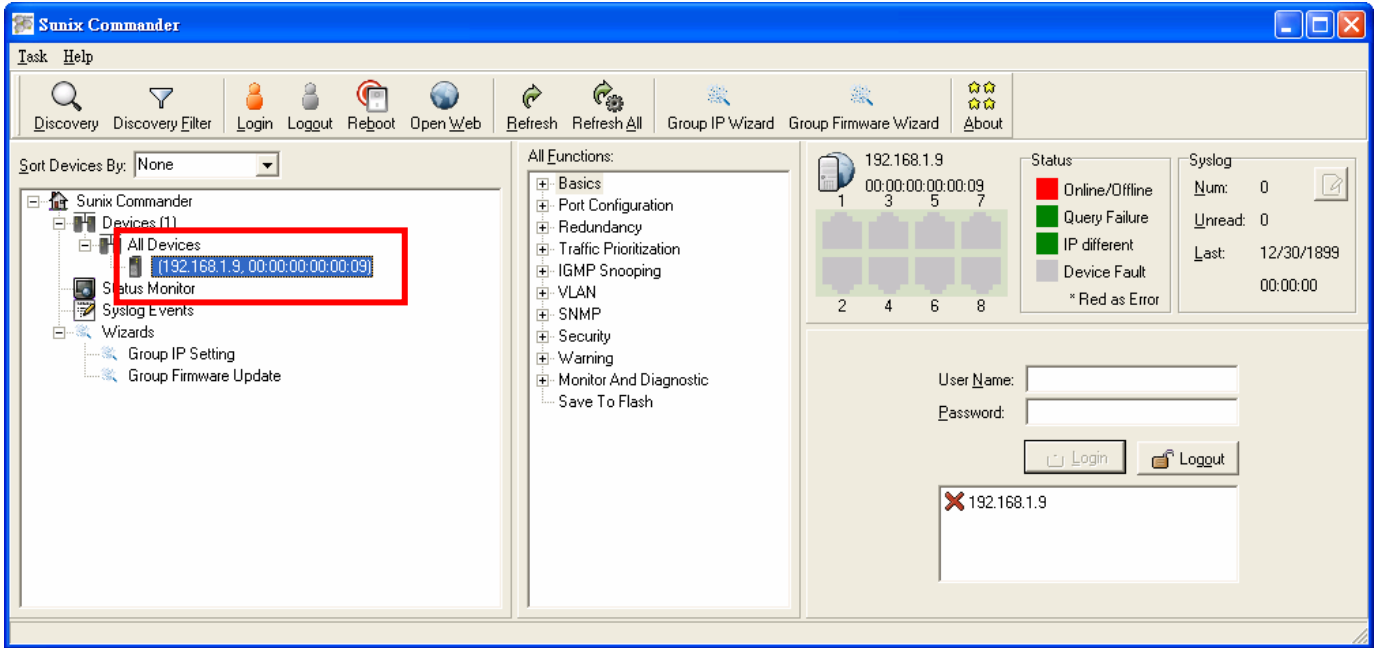
The page includes some basic setting configuration of Sunix switches

Basics

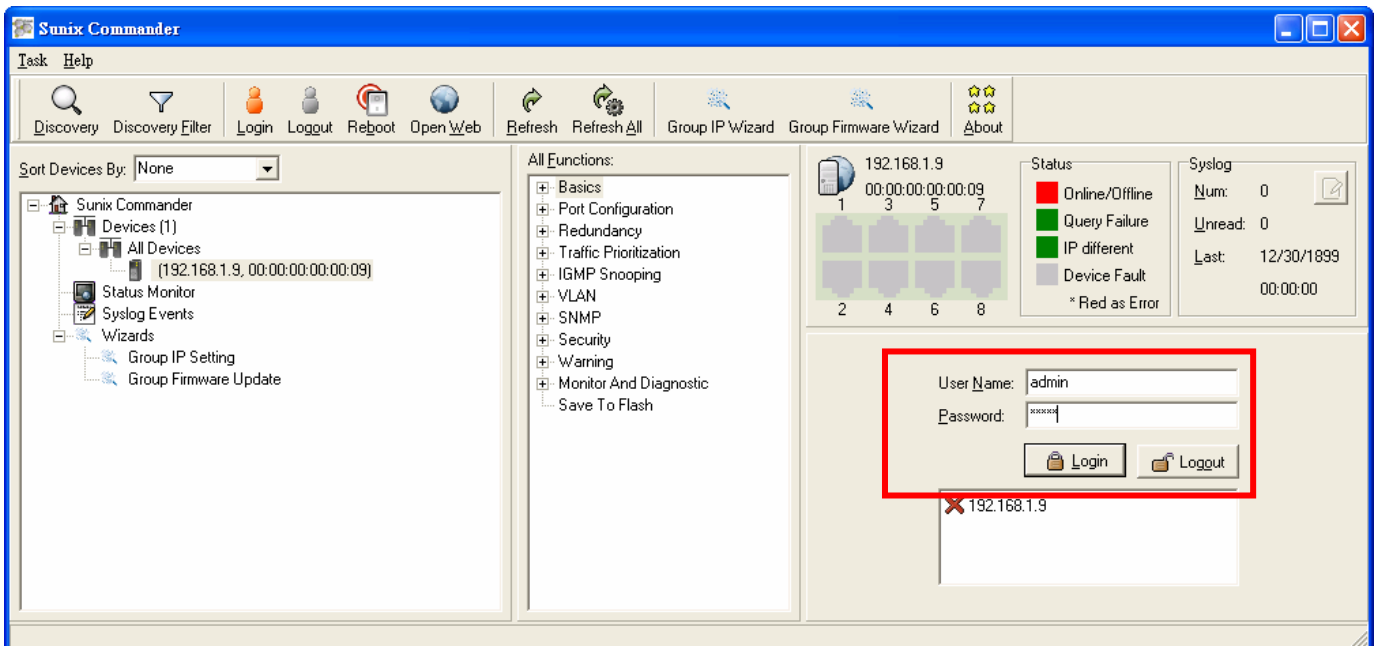
Login Switch to change setting

Using "Supervisor" status to log in Switch, and then start to change related settings of Switch.

(1) Select Switch that would be modify (as well as using "Ctrl" or "Shift" key to copy that)

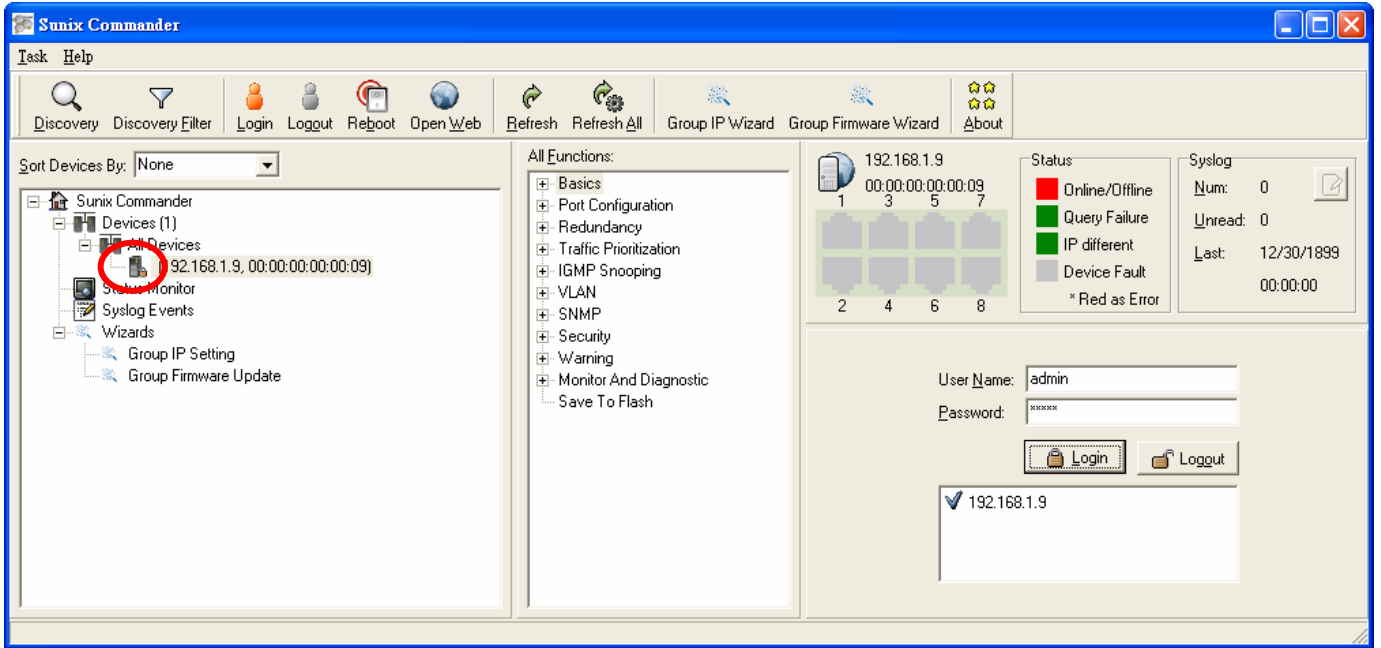


(2) Insert Supervisor's password, and then click "Login" button.

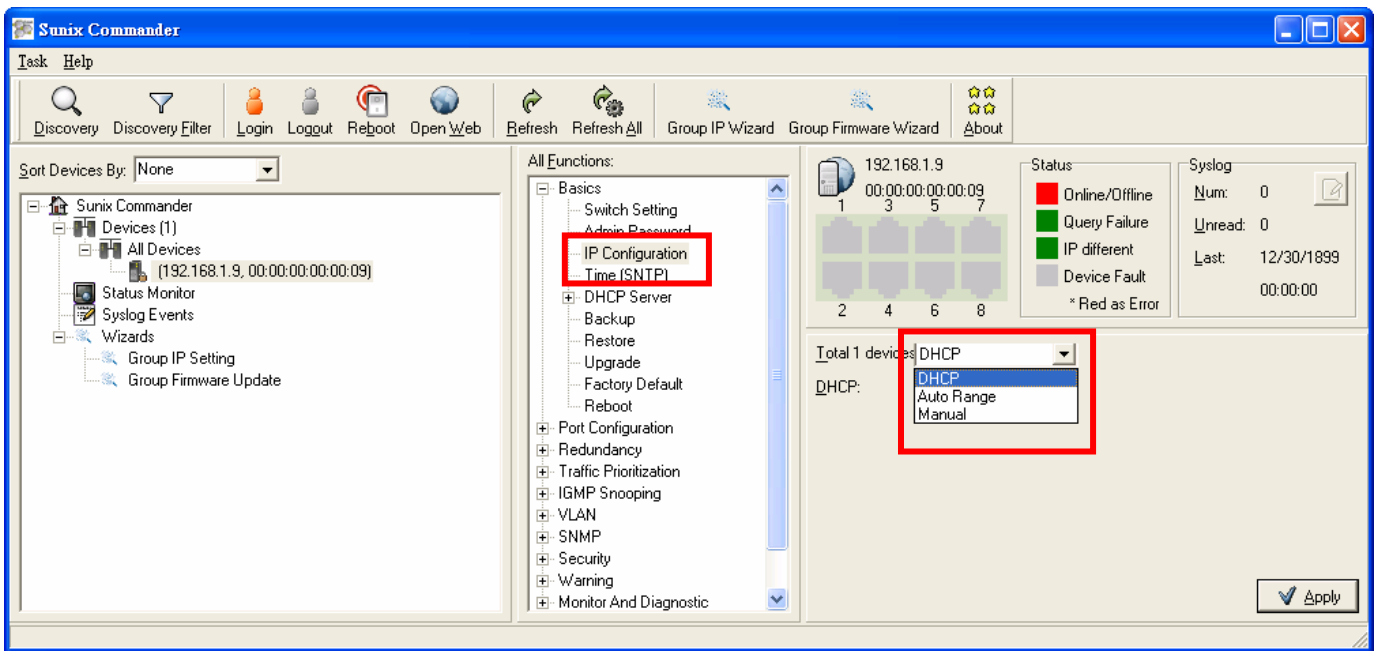


Note Default User Name : admin
 Default Password : admin

(3) After log in successful, there will be a small icon appeared, that's mean this switch be blocked and could start to modify settings.



IP Configuration



***** DHCP *****

Setting	Descriptions	Factory Default
None.	DHCP Server distribute Switch's IP Address	None

***** Auto Range *****

Setting	Descriptions	Factory Default
None	Manager restricts IP Address and distribute to Switches automatically.	None

IP Begin

Setting	Descriptions	Factory Default
None	Searching initial IP Address	0.0.0.0

IP End

Setting	Descriptions	Factory Default
None.	Searching final IP Address	0.0.0.0

Netmask

Setting	Descriptions	Factory Default
None	Setting Switch's Net mask Address	0.0.0.0

Gateway

Setting	Descriptions	Factory Default
None	Setting Switch's Gateway Address	0.0.0.0

DNS Server1

Setting	Descriptions	Factory Default
None.	Setting Switch's first "Domain Name Server Address"	0.0.0.0

DNS Server2

Setting	Descriptions	Factory Default
None	Setting Switch second "Domain Name Server Address"	0.0.0.0

***** Manual *****

Setting	Descriptions	Factory Default
None	Distribute IP Address to Switches by definition	None

DHCP

Setting	Descriptions	Factory Default
Mark	Distribute IP Address to Switches automatically by DHCP Server	Mark
Unmark	Distribute IP Address to Switches by definition	

IP Addr

Setting	Descriptions	Factory Default
None	Import IP Address to modify switch's IP Address	0.0.0.0

Netmask

Setting	Descriptions	Factory Default
None.	Import Net mask Address to modify switch's Net mask Address	0.0.0.0

Gateway

Setting	Descriptions	Factory Default
None	Import Gateway Address to modify Switch's Gateway Address	0.0.0.0

DNS Server1

Setting	Descriptions	Factory Default
None.	Setting Switch's first "Domain Name Server Address"	0.0.0.0

DNS Server2

Setting	Descriptions	Factory Default
None	Setting Switch's second "Domain Name Server Address"	0.0.0.0

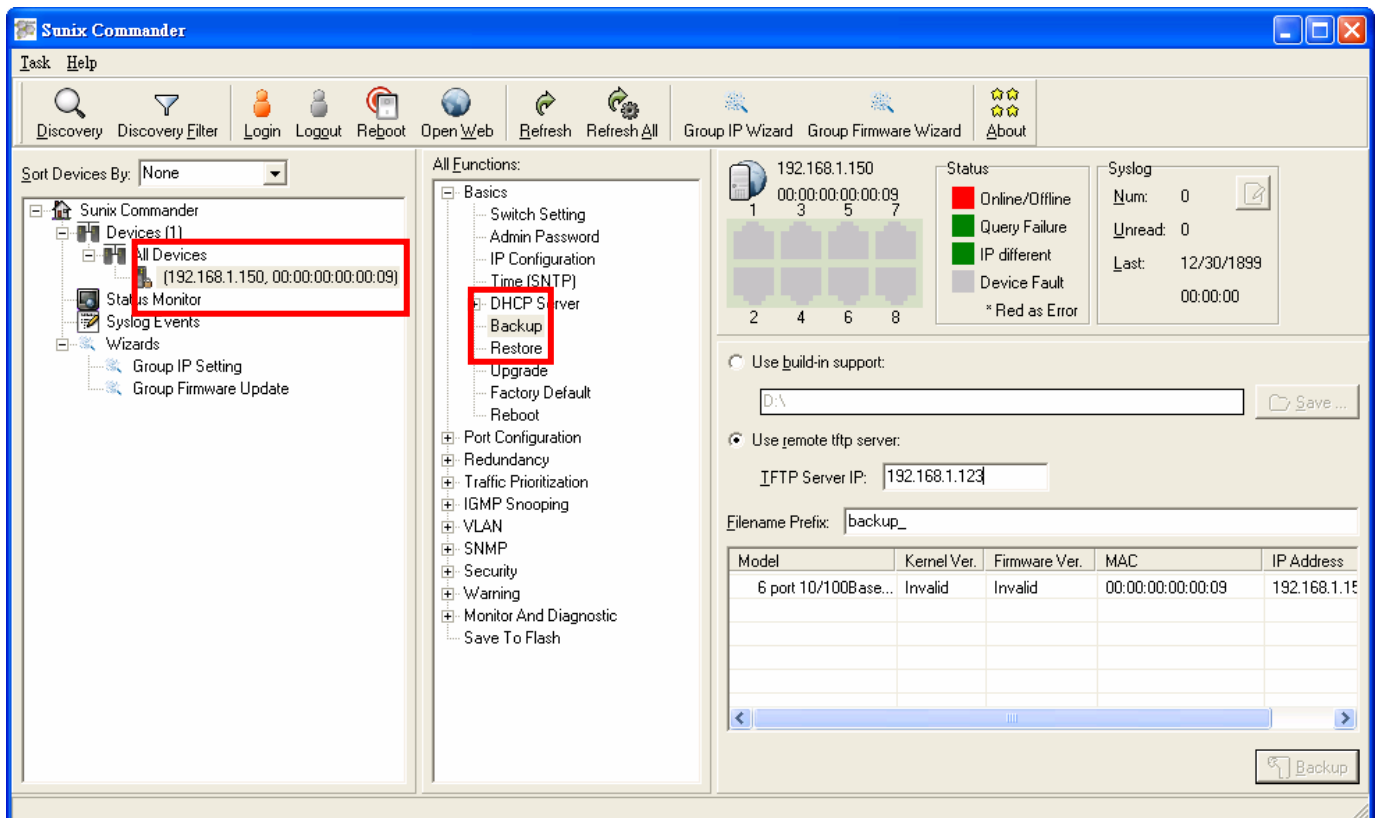
NOTE Click "set" button after finish settings, and then click "Apply" button to finish setting.

NOTE Must execute "Save To Flash" when change any settings, or else system will back to previous when turn off power.

Backup

Sunix Switches allow users backup and file all settings, and using backup file to recover all settings. This function could save setting time and all switches have the same settings at the same time

Select switch that would like to backup settings, click "Backup" item.



Use build-in support

Setting	Descriptions	Factory Default
None	Select backup file's location.	None

Use remote tftp server

Setting	Descriptions	Factory Default
None.	Backup settings to TFTP Server	None

TFTP Server IP

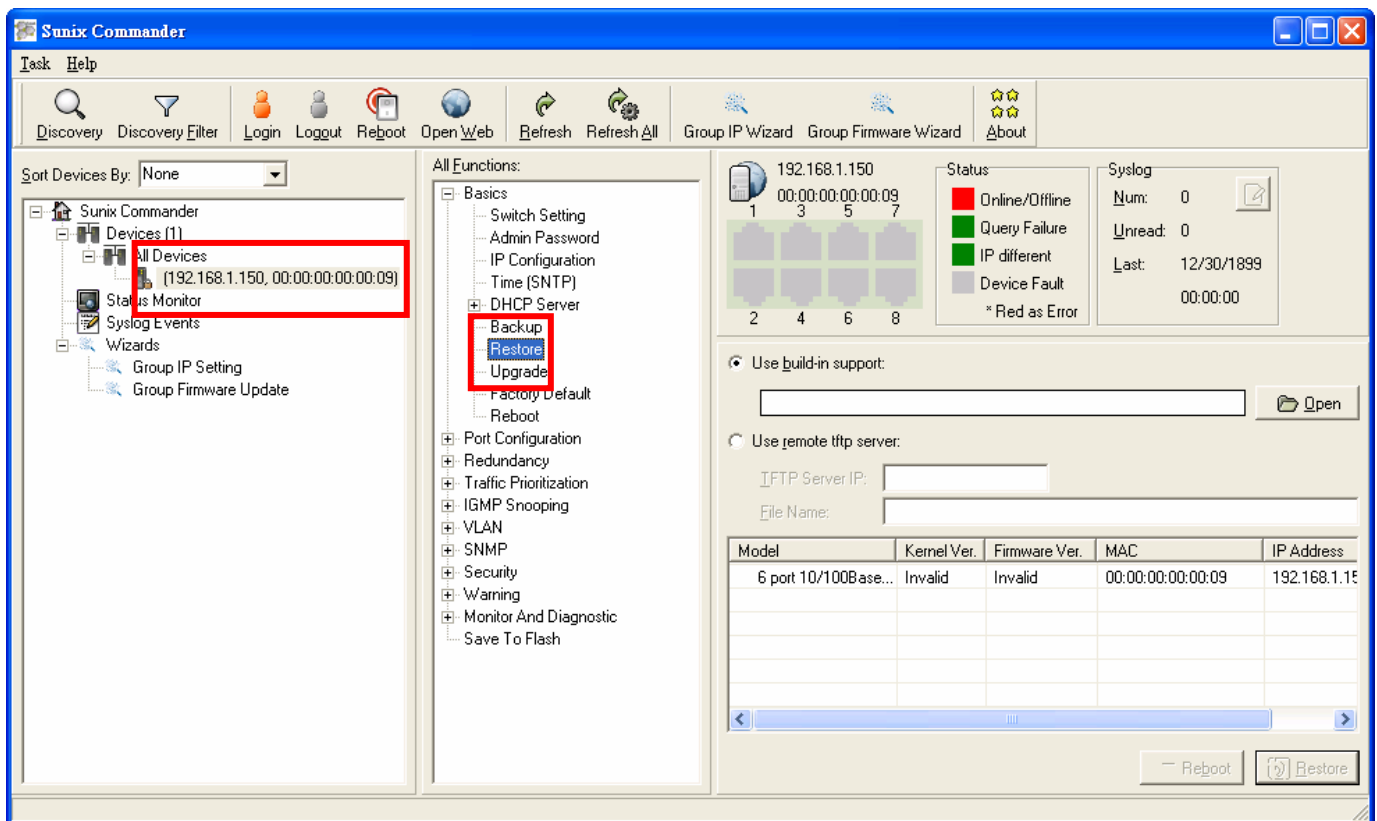
Setting	Descriptions	Factory Default
None	Setting TFTP Server's IP Address	None

Filename Prefix

Setting	Descriptions	Factory Default
None	You could change the name of backup file.	Backup_

Restore

Sunix Switches allow users use previous backup file to recover all settings, also import backup files to all Switches.
 Select Switch and click "Restore" item.



Use build-in support

Setting	Descriptions	Factory Default

None	Select backup file's location	None
------	-------------------------------	------

Use remote tftp server

Setting	Descriptions	Factory Default
None.	Using TFTP Server's backup file to recover settings	None

TFTP Server IP

Setting	Descriptions	Factory Default
None	Setting TFTP Server's IP Address	None

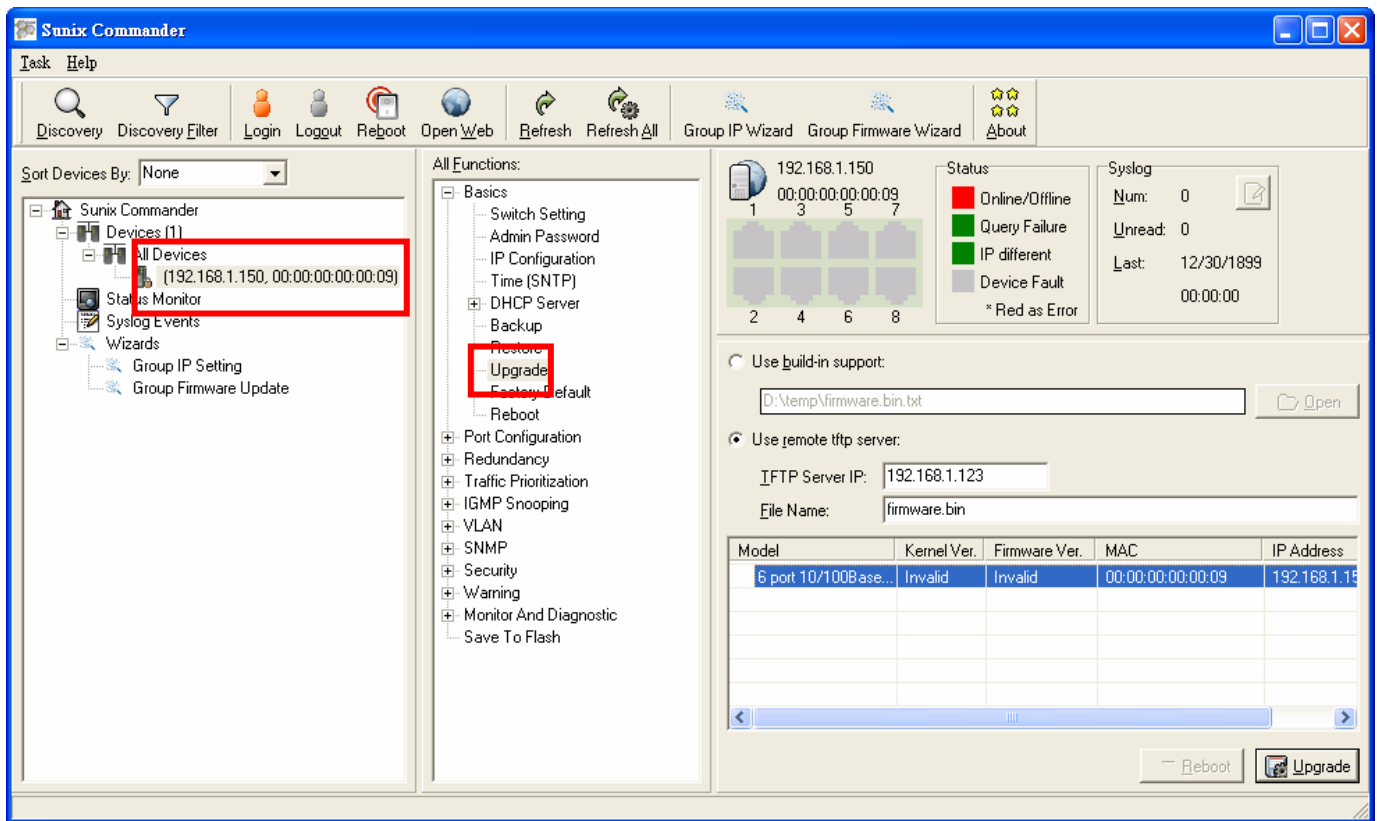
File Name

Setting	Descriptions	Factory Default
None	Must key in backup file's name manually, both file name and sub file name have to exactly.	None

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

Upgrade

Sunix Switch could upgrade Firmware, not only upgrades alone, but also could upgrade several Switches firmware in the same time. This function could save time to upgrade Switches, and leave no one in the same time. Select Switch and click "Restore" item.



Use build-in support

Setting	Descriptions	Factory Default
None	Select location that save new version Firmware.	None

Use remote tftp server

Setting	Descriptions	Factory Default
None.	Using TFTP Server's Firmware to upgrade Switch	None

TFTP Server IP

Setting	Descriptions	Factory Default
None	Setting TFTP Server's IP Address	None

File Name

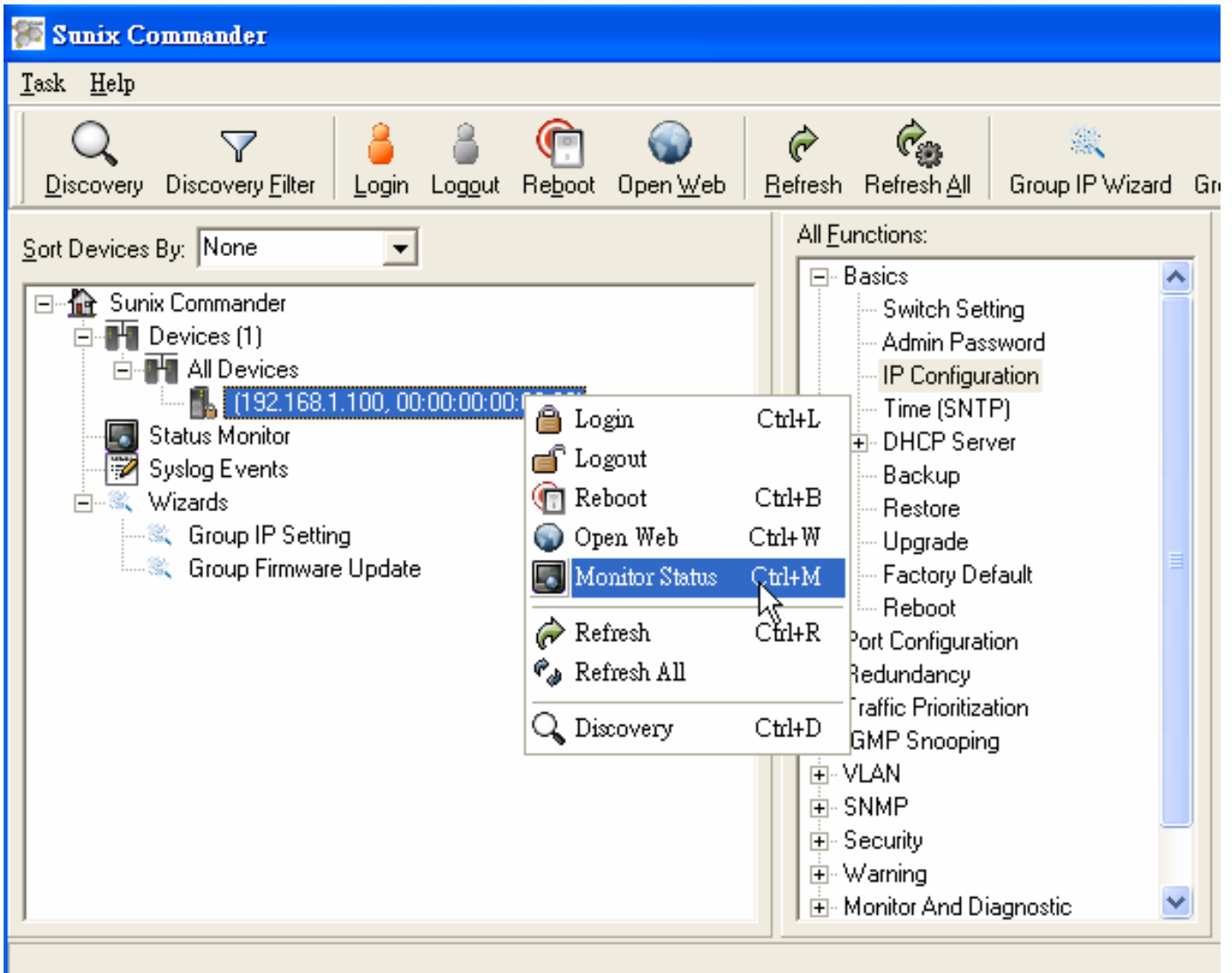
Setting	Descriptions	Factory Default
None	Must key in backup file's name manually, both file name and sub file name have to exactly.	None

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

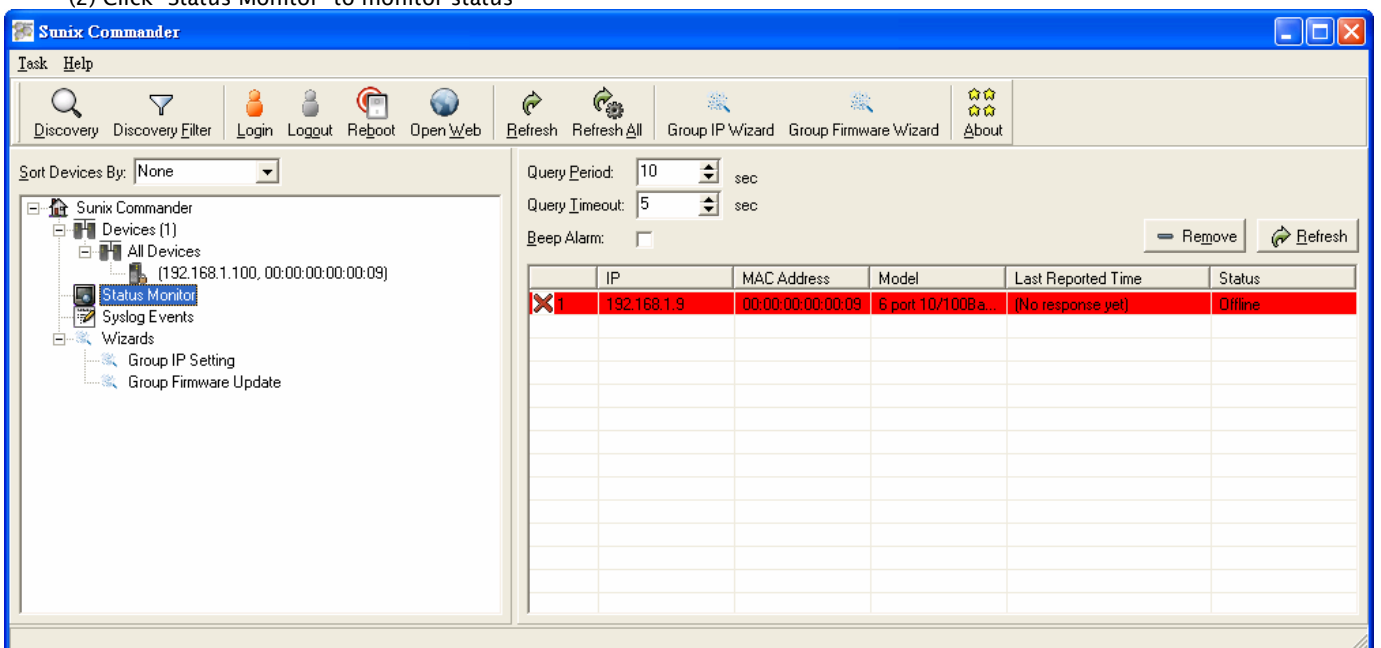
3.4.4. Status Monitor

Managers monitor all Switches status easily. We could monitor Switch and check it is alive or not.

- (1) Select Switch (repeat also be allowed), then click right button of mouse and select "Monitor Status" to monitor Switches.



(2) Click "Status Monitor" to monitor status



Query Period

Setting	Descriptions	Factory Default
The number range is 5 ~ 86400 sec.	Setting Switch's status to renew the interval time	10

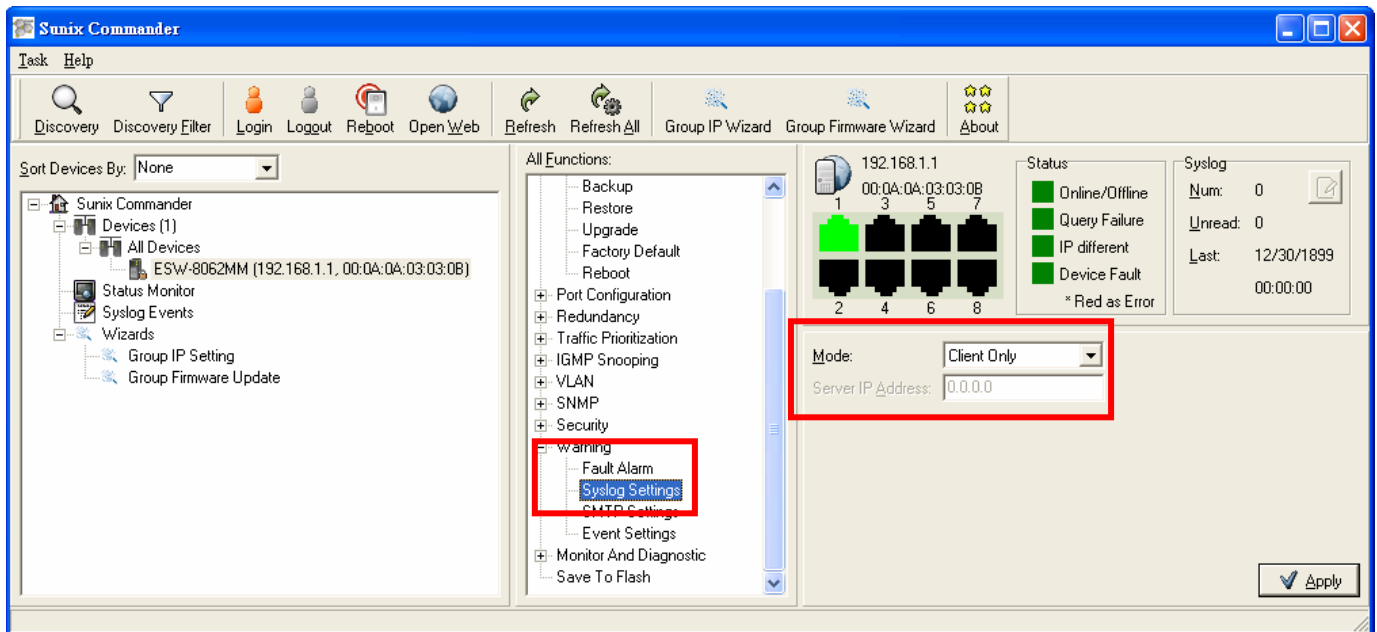
Query Timeout

Setting	Descriptions	Factory Default
The number range is 1 ~ 86399 sec.	Setting "time to fail" that un-receive reply when renew Switches.	5

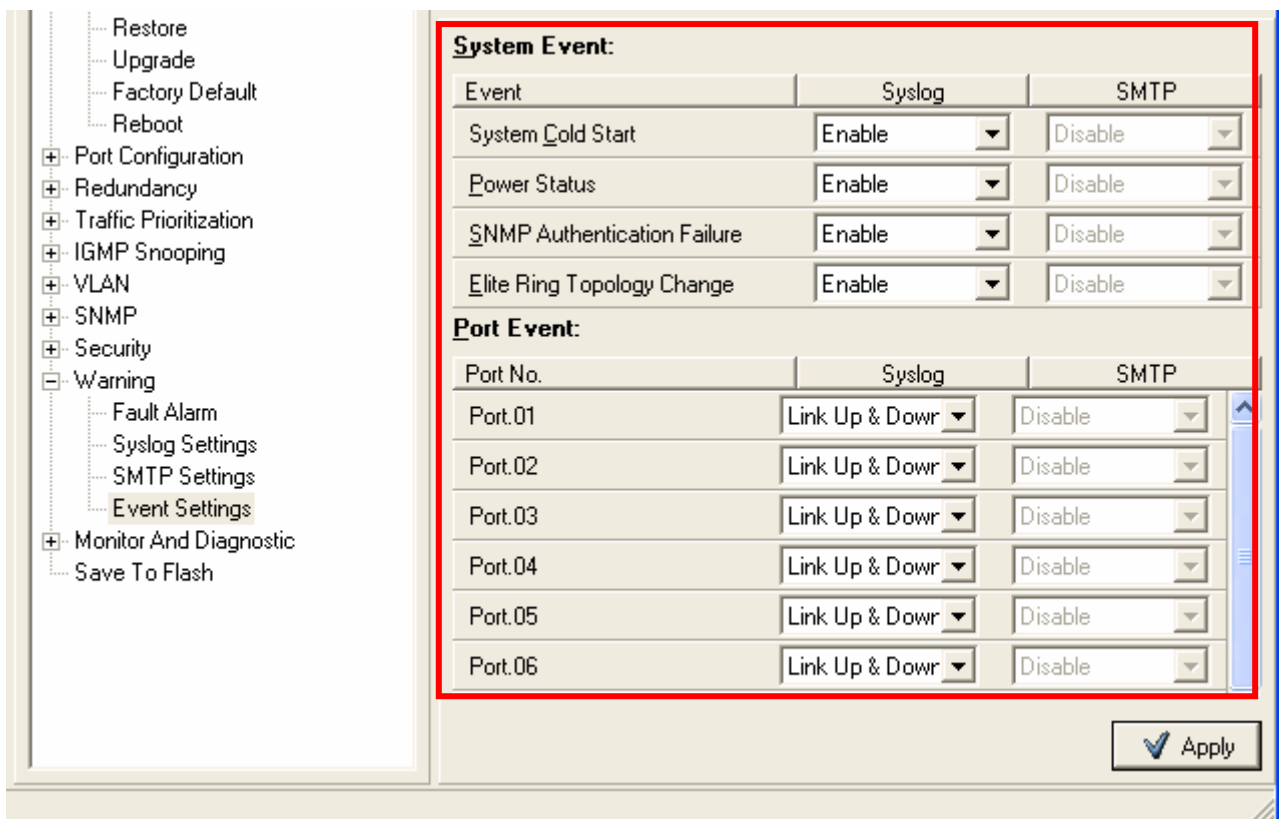
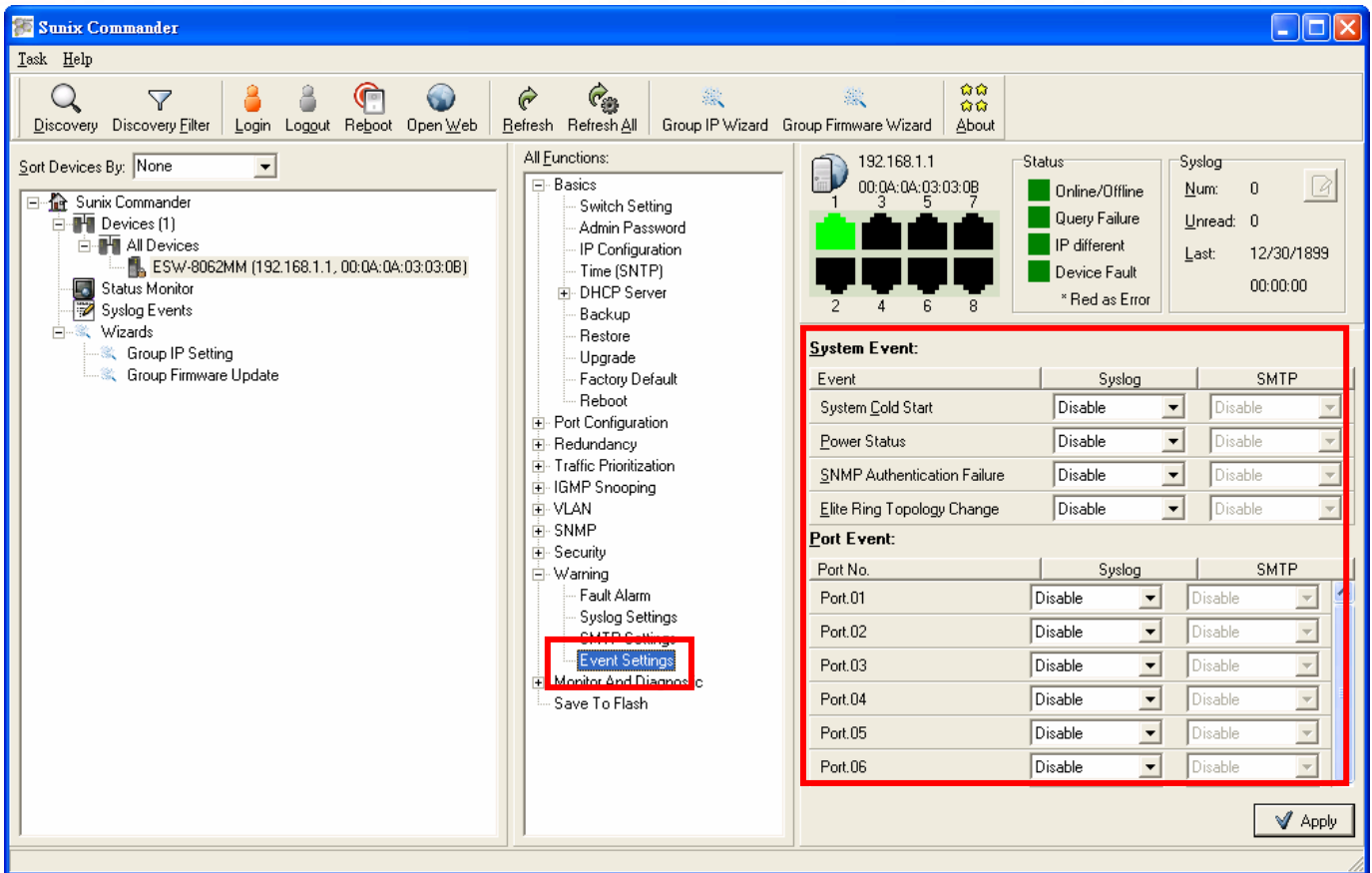
3.4.5. Syslog Events

Managers could monitor Switch's status, and understand what happens of Switches. This function helps managers understand all records and status of Switches to control Switches.

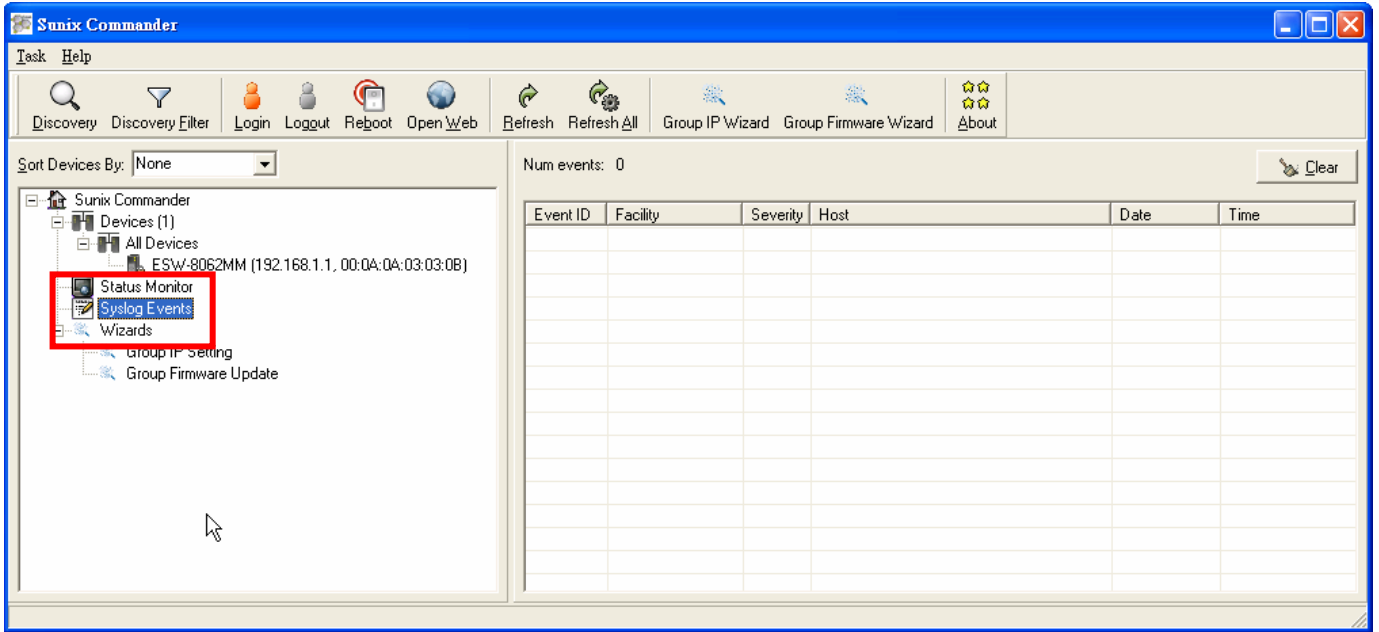
- (1) First, go to "Warning \ Syslog Settings" to enable "Syslog Event"



- (2) Go to "Warning \ Event Settings" to select System Event that would be monitored.



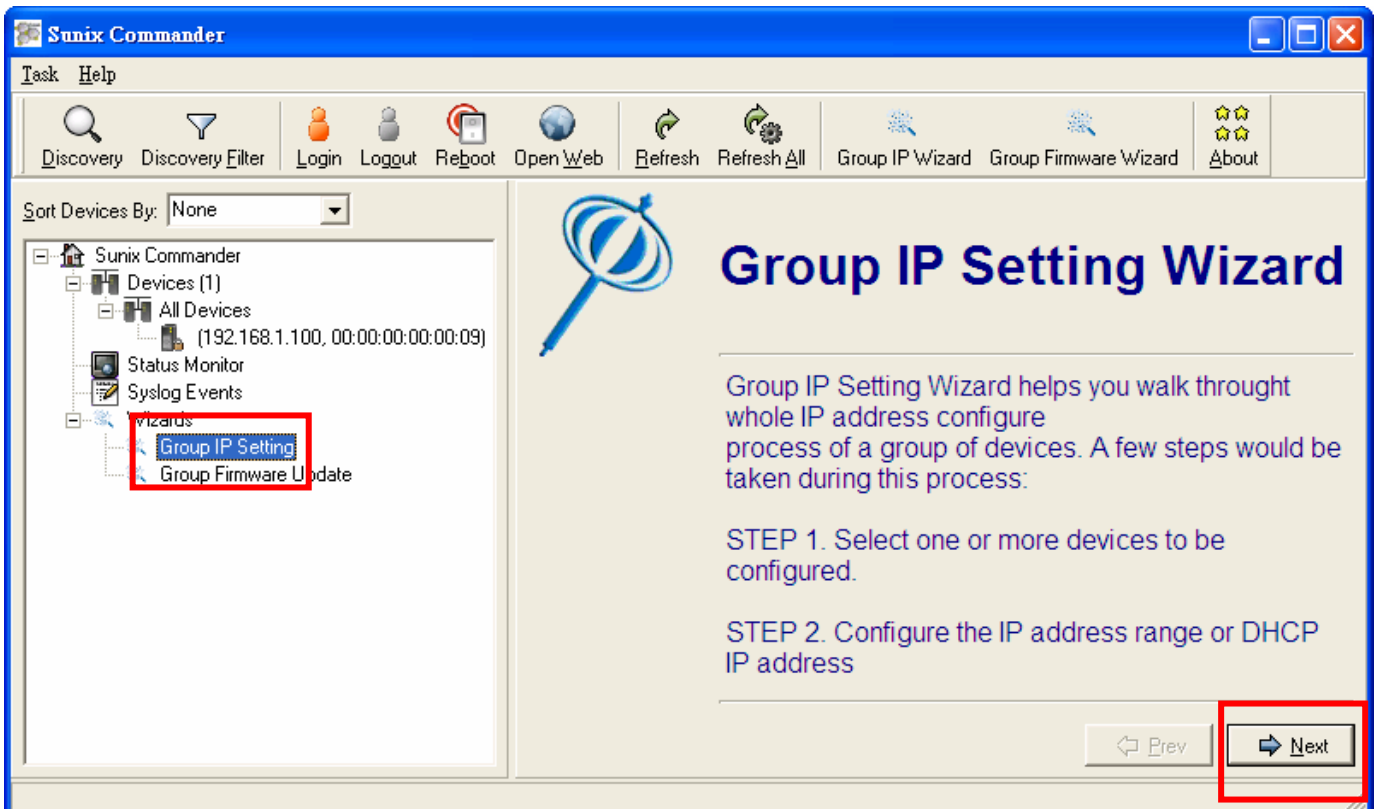
(3) Select "Syslog Events" and start to monitor Switch's events.



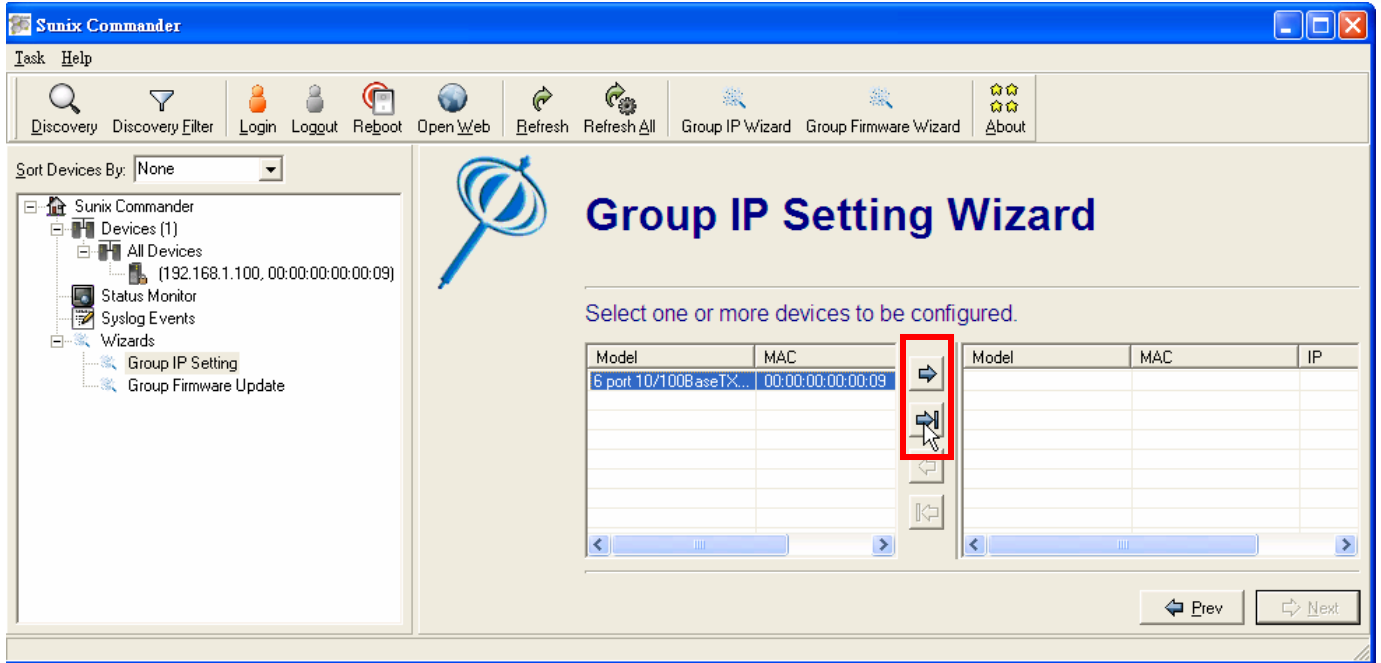
3.4.6. Group IP Setting Wizard

IP Address Setting Wizard, managers could set all IP Address of Switches once. Managers just follow the procedure to setup IP Address step by step.

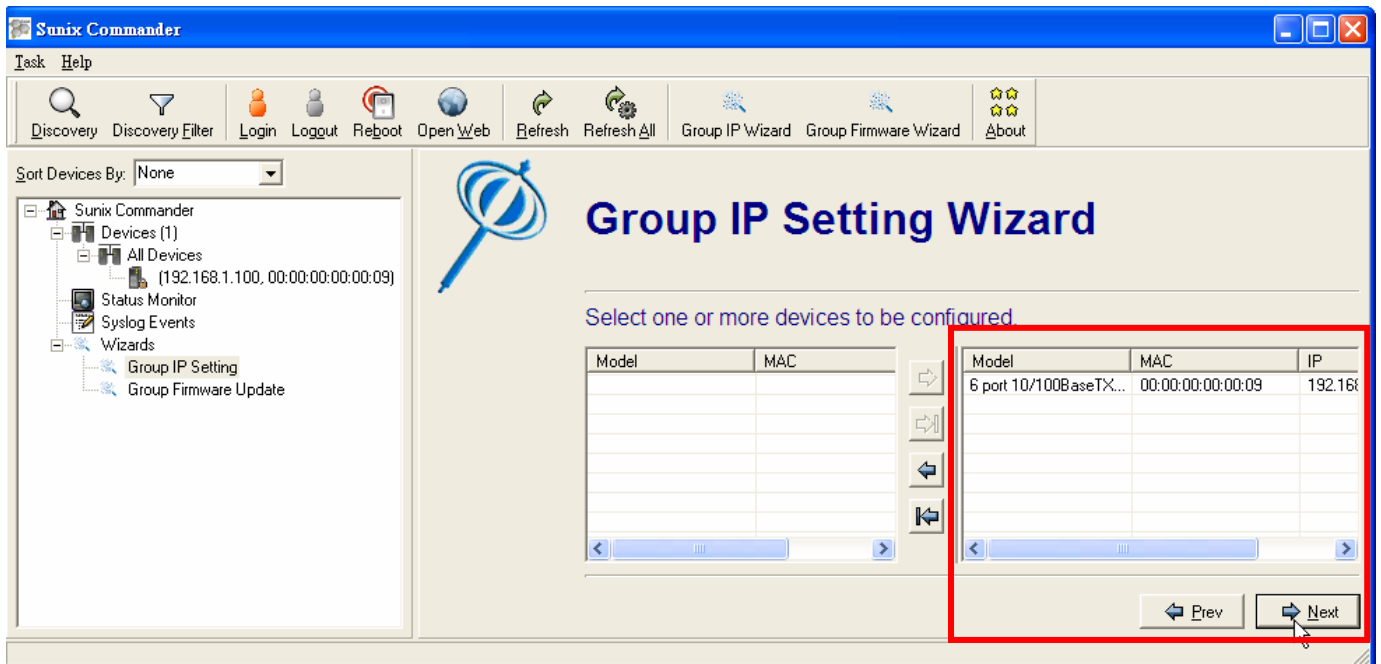
- (1) Select "Group IP Setting" and click "Next" button.



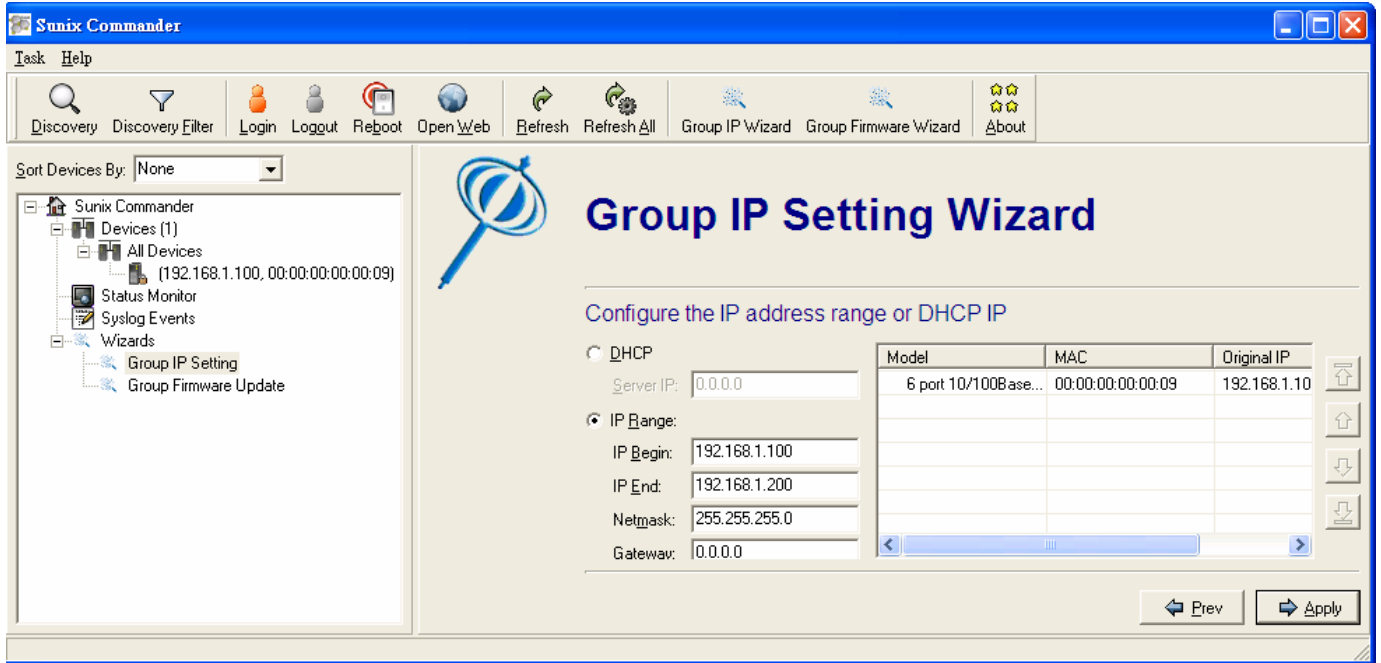
- (2) Click  and add one Switch to right field. Click  button add all Switches to right field.



- (3) List Switches that would be modified IP Address to the right field, Click "Next" button.



- (4) Select "DHCP" or "IP Range" to distribute IP Address, Click "Apply" button and then finish all.

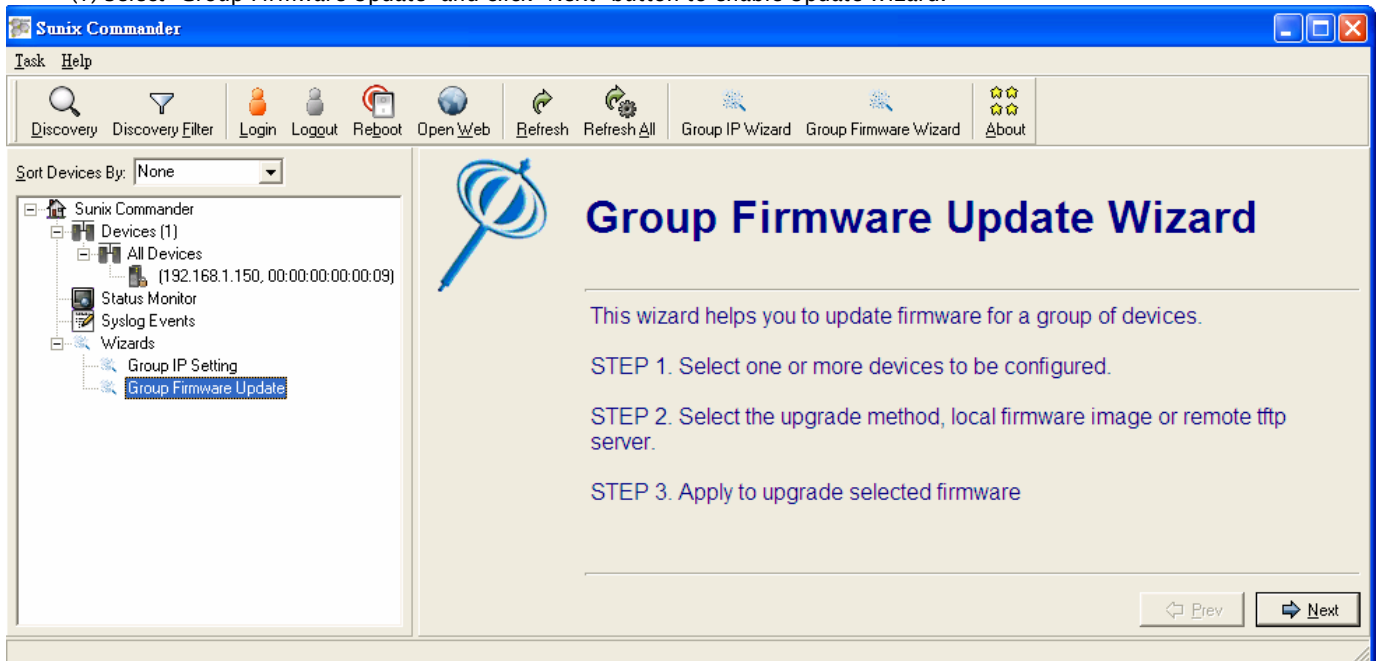




NOTE Must execute "Save to Flash" to save all when change any settings, or else system will back to previous setting when turn off the power.

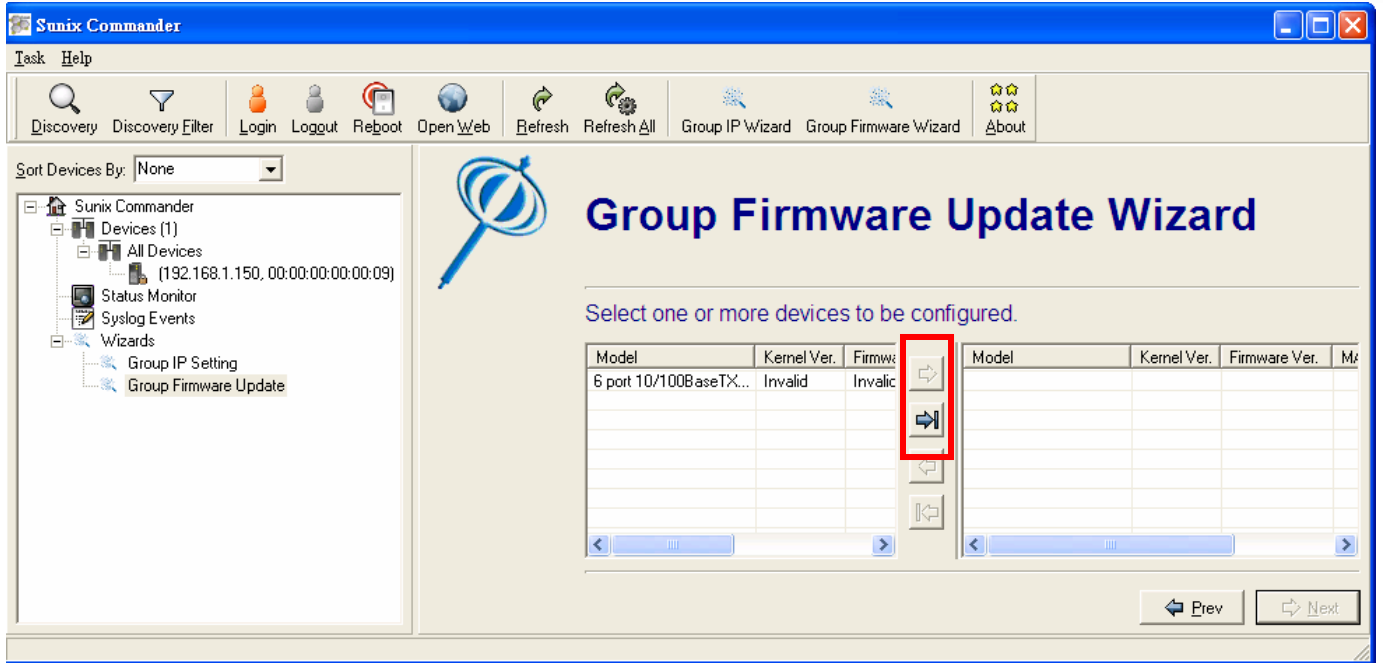
3.4.7. Group Firmware Update Wizard

Upgrade Firmware Wizard, Managers could upgrade all Switches Firmware once and simultaneously.

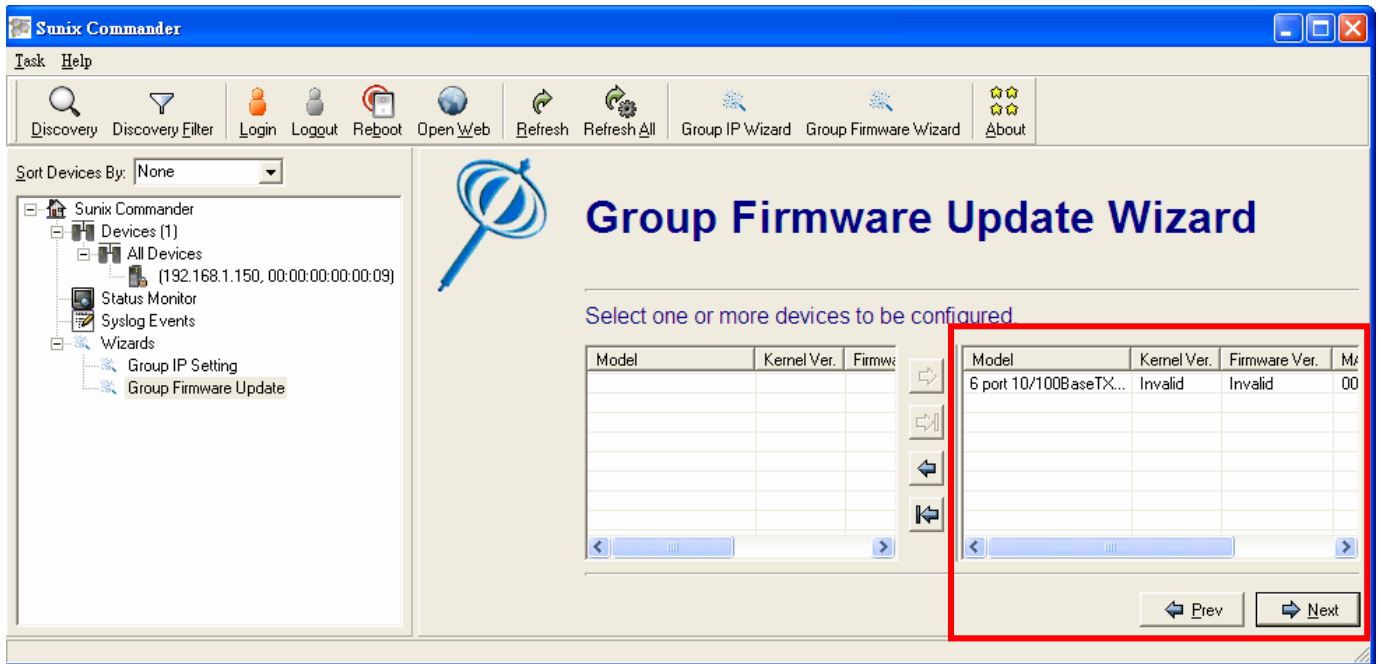
(1) Select "Group Firmware Update" and click "Next" button to enable Update Wizard.



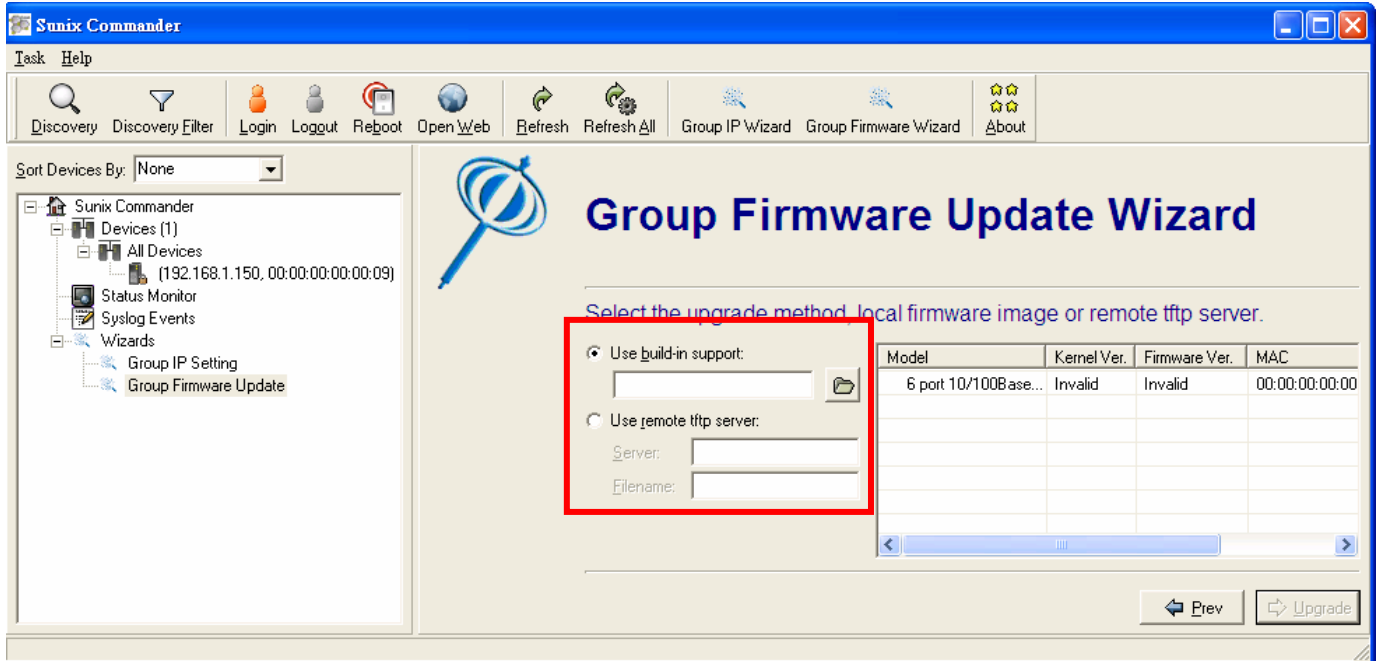
(3) Click  add one switch to right field, click  add all Switches to right field.



(3) List Switches that would be update Firmware to the right field, Click “Next” button.



(4) Select “Use build-in support” or TFTP Server (Use remote TFTP Server to upgrade Firmware), and click “Upgrade” button



4. MIB Groups

Sunix Switch comes with built-in SNMP (Simple Network Management Protocol) agent software that supports cold/warm start trap, line up/down trap, and Rfc 1757 RMON, RFC 1493 Bridge MIB, RFC 1213 MIB II, RFC 1643—Ethernet-like MIB and RFC 2674—P-BRIDGE-MIB, QBRIDGE-MIB, VLAN Bridge MIB

The following topics are covered in this chapter:

- Tree structure of the Sunix MIB
- Sunix Private MIB

4.1. Tree structure of Sunix MIB

The Management Information Base (MIB) is designed in the form of an abstract tree structure. The branching points are the **object classes**. The "leaves" of the MIB are called **generic object classes**. Wherever necessary for unambiguous identification, the generic object classes are **instantiated**, i.e. the abstract structure is imaged on the reality, by specifying the port or the source address. Values (integers, time ticks, counters or octet strings) are assigned to these instances; these values can be read and, in some cases, modified. The **object description** or the **object ID** (OID) identifies the object class. The **subidentifier** (SID) is used for instantiation.

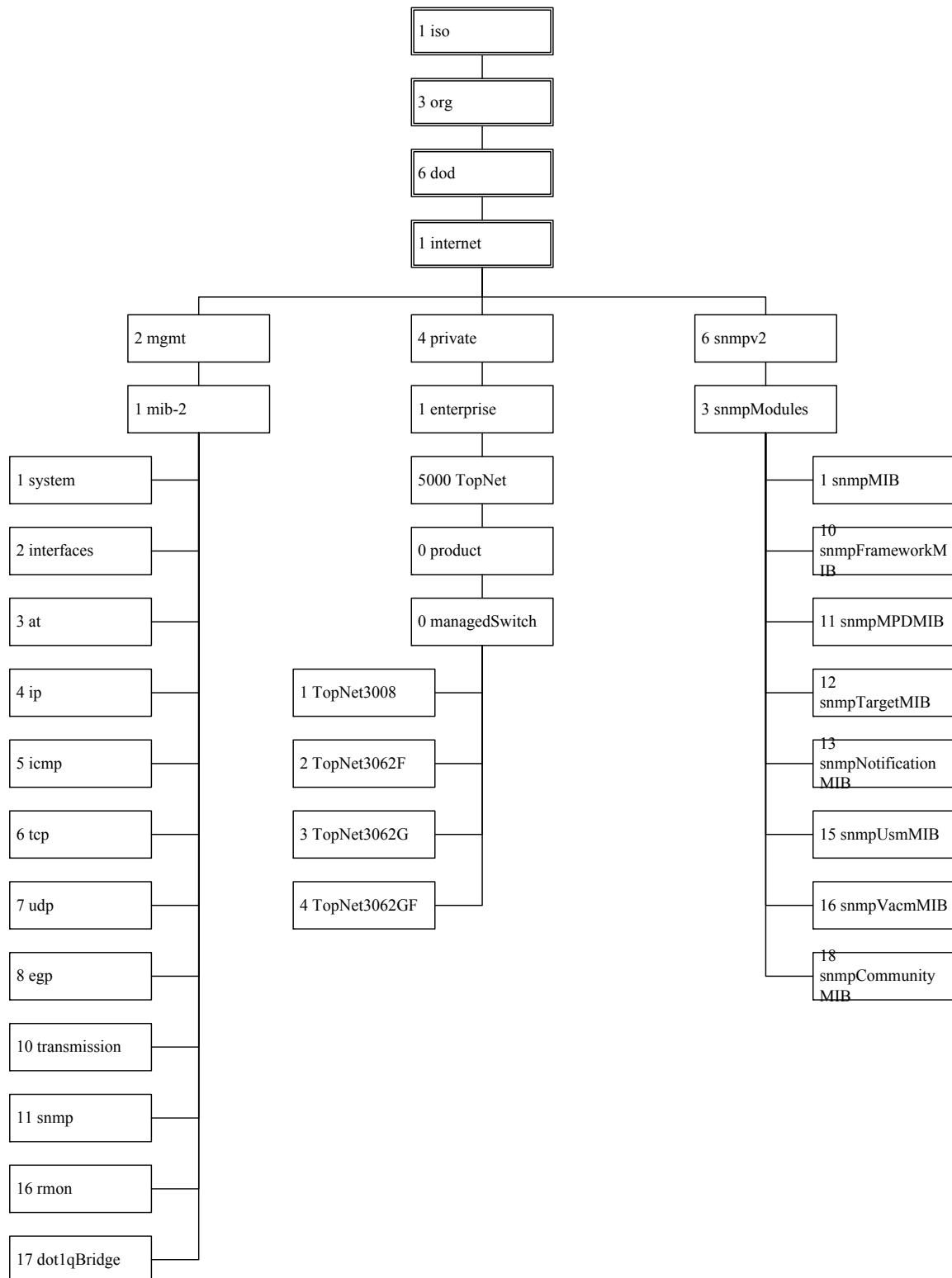
Example:

The generic object class

tportCtrlEntry (OID = 1.3.6.1.4.1.5000.0.0.3.3.1.1.1)

is the description of the abstract information "An entry in the table, containing information about configuration in one switch port of the switch". However, it is not possible to read any information from this, as the system does not know which port control is meant. Specification of the subidentifier (3) images this abstract information onto reality (instantiates it), which means that it refers to disable (or enable) control of this port. A value is assigned to this instance and can then be read. The instance "get 1.3.6.1.4.1.5000.0.0.3.3.1.1.3", for example, returns the response "1", which means that the port is enable

The following is the tree structure of the Sunix MIB



4.2. Sunix Private MIB

The private MIB is for configuring the device-specific properties of the Sunix switch. The groups below are implemented in the Sunix from the private MIB hmConfiguration (OID = 1.3.6.1.4.1.5000.0.0.1(ESW-8062-TX) or 2(ESW-8062-GT) or 3(ESW-8062-SS) or 4(ESW-8062-GS) or 5(ESW-8062-MM) or 6(ESW-8062-GM))

©contact(OID = 1.3.6.1.4.1.5000.0.0.x.1)

- ◎basicSetting(OID = 1.3.6.1.4.1.5000.0.0.x.2)
- ◎portConfiguration(OID = 1.3.6.1.4.1.5000.0.0.x.3)
- ◎ringRedundancy(OID = 1.3.6.1.4.1.5000.0.0.x.4)
- ◎ieee8021qVlan(OID = 1.3.6.1.4.1.5000.0.0.x.5)
- ◎trafficPrioritization(OID = 1.3.6.1.4.1.5000.0.0.x.6)
- ◎multicastFiltering(OID = 1.3.6.1.4.1.5000.0.0.x.7)
- ◎snmp(OID = 1.3.6.1.4.1.5000.0.0.x.8)
- ◎security(OID = 1.3.6.1.4.1.5000.0.0.x.9)
- ◎warning(OID = 1.3.6.1.4.1.5000.0.0.x.10)
- ◎monitorandDiag(OID = 1.3.6.1.4.1.5000.0.0.x.11)
- ◎save(OID = 1.3.6.1.4.1.5000.0.0.x.12)
- ◎specificTrap(OID = 1.3.6.1.4.1.5000.0.0.x.13)

(3)ESW-8062-GT

- |--(1)contact
 - | |--(1)systemName
 - | |--(2)systemLocation
 - | |--(3)systemContact
 - | |--(4)systemDescr
 - | |--(5)systemFwVer
 - | |--(6)systemMacAddress
- |--(2)basicSetting
 - | |--(1)switchSetting
 - | | |--(1)switchSettingSystemName
 - | | |--(2)switchSettingSystemLocation
 - | | |--(3)switchSettingSystemContact
 - | |--(2)adminPassword
 - | | |--(1)adminPasswordUserName
 - | | |--(2)adminPassword_Password
 - | |--(3)ipConfiguration
 - | | |--(1)ipConfigurationTable
 - | | | |--(1)ipConfigurationEntry
 - | | | | |--(1)ipConfigurationIndex
 - | | | | |--(2)ipConfigurationDHCPStatus
 - | | | | |--(3)ipConfigurationAddress
 - | | | | |--(4)ipConfigurationSubMask
 - | | | | |--(5)ipConfigurationGateway
 - | | | | |--(6)ipConfigurationDNS1
 - | | | | |--(7)ipConfigurationDNS2
 - | |--(4)sntp
 - | | |--(1)sntpClientStatus
 - | | |--(2)sntpDaylightSavingTime
 - | | |--(3)sntpUTCTimezone
 - | | |--(4)sntpServerIP
 - | | |--(5)sntpSwitchTimer
 - | | |--(6)sntpDaylightSavingPeriodStart
 - | | |--(7)sntpDaylightSavingPeriodEND
 - | | |--(8)sntpDaylightSavingOffset
 - | |--(5)dhcpServer
 - | | |--(1)dhcpServerCfgTable
 - | | | |--(1)dhcpServerCfgEntry
 - | | | | |--(1)dhcpServerCfgIndex
 - | | | | |--(2)dhcpServerCfgStatus
 - | | | | |--(3)dhcpServerCfgLowIPAddr
 - | | | | |--(4)dhcpServerCfgHighIPAddr
 - | | | | |--(5)dhcpServerCfgSubMask
 - | | | | |--(6)dhcpServerCfgGateway
 - | | | | |--(7)dhcpServerCfgDNS
 - | | | | |--(8)dhcpServerCfgLeaseTime
 - | | |--(2)dhcpServerClientInfoTable
 - | | | |--(1)dhcpServerClientInfoEntry
 - | | | | |--(1)dhcpServerClientInfoIndex
 - | | | | |--(2)dhcpServerClientInfoIPAddr
 - | | | | |--(3)dhcpServerClientInfoID
 - | | | | |--(4)dhcpServerClientInfoType
 - | | | | |--(5)dhcpServerClientInfoStatus
 - | | | | |--(6)dhcpServerClientInfoLease
 - | | |--(3)dhcpServerIPBindingTable
 - | | | |--(1)dhcpServerIPBindingEntry
 - | | | | |--(1)dhcpServerIPBindingPortNum
 - | | | | |--(2)dhcpServerIPBindingAddr
 - | |--(6)backupAndRestore
 - | | |--(1)backupServerIP
 - | | |--(2)backupAgentBoardFwFileName
 - | | |--(3)backupStatus
 - | | |--(4)restoreServerIP
 - | | |--(5)restoreAgentBoardFwFileName

```
| | |--(6)restoreStatus
| |--(7)tftpUpgrade
| | |--(1)tftpDownloadServerIP
| | |--(2)tftpDownloadAgentBoardFwFileName
| | |--(3)tftpDownloadStatus
|--(8)factoryDefault
| | |--(1)factoryDefaultAction
|--(9)systemReboot
| | |--(1)systemRebootAction
|--(10)switchCurrentPortNameListTable
| | |--(1)switchCurrentPortNameListEntry
| | | |--(1)swCurrentPortNameListIndex
| | | |--(2)swCurrentPortNameListPortName
| | | |--(3)swCurrentPortNameListPortNumber
|--(3)portConfiguration
| |--(1)portControl
| | |--(1)portCtrlTable
| | | |--(1)portCtrlEntry
| | | | |--(1)portCtrlIndex
| | | | |--(2)portCtrlPortName
| | | | |--(3)portCtrlPortStatus
| | | | |--(4)portCtrlNegotiation
| | | | |--(5)portCtrlSpeed
| | | | |--(6)portCtrlDuplex
| | | | |--(7)portCtrlFlowControl
|--(2)rateLimiting
| | |--(1)rateLimitingTable
| | | |--(1)rateLimitingEntry
| | | | |--(1)rateLimitingPortNum
| | | | |--(2)rateLimitingPortType
| | | | |--(3)rateLimitingIngressRate
| | | | |--(4)rateLimitingEgressRate
|--(3)PortTrunk
| |--(1)aggregatorSetting
| | |--(1)portTrunkSyspri
| | |--(2)portTrunkAggregatorTable
| | | |--(1)portTrunkAggregatorEntry
| | | | |--(1)portTrunkAggregatorIndex
| | | | |--(2)portTrunkAggregatorGroupName
| | | | |--(3)portTrunkAggregatorMemberPorts
| | | | |--(4)portTrunkAggregatorLACPStatus
| | | | |--(5)portTrunkAggregatorWorkPorts
|--(2)aggregatorStatus
| | |--(1)portTrunkAggregatorInfoTable
| | | |--(1)portTrunkAggregatorInfoEntry
| | | | |--(1)portTrunkAggregatorInfoIndex
| | | | |--(2)portTrunkAggregatorInfoGroupName
| | | | |--(3)portTrunkAggregatorInfoDescription
|--(3)stateActivity
| | |--(1)portTrunkLACPStateActTable
| | | |--(1)portTrunkLACPStateEntry
| | | | |--(1)portTrunkLACPStateActPortNum
| | | | |--(2)portTrunkLACPStateActStatus
|--(4)ringRedundancy
|--(1)superRing
| | |--(1)superRingStatus
| | |--(2)superRingRingMasterStatus
| | |--(3)superRingRingPort1
| | |--(4)superRingRingPort2
| | |--(5)superRingCoupleRingStatus
| | |--(6)superRingCouplingPort
| | |--(7)superRingControlPort
| | |--(8)superRingDualHomingStatus
| | |--(9)superRingHomingPort
| | |--(10)superRingLeagcyModeStatus
|--(2)rstp
| | |--(1)rstpStatus
| | |--(2)rstpPriority
| | |--(3)rstpMaxAge
| | |--(4)rstpHelloTime
| | |--(5)rstpForwardDelayTime
| | |--(6)rstpPerPortCfgTable
| | | |--(1)rstpPerPortCfgEntry
| | | | |--(1)rstpPerPortCfgPortNum
| | | | |--(2)rstpPerPortCfgPathCost
| | | | |--(3)rstpPerPortCfgPriority
| | | | |--(4)rstpPerPortCfgAdminP2P
| | | | |--(5)rstpPerPortCfgAdminEdge
| | | | |--(6)rstpPerPortCfgAdminNonStp
```

```
--(3)bridgeInformation
  |--(1)rstpRootBridgeInfomationTable
  |   |--(1)rstpRootBridgeInfomationEntry
  |       |--(1)rstpRootBridgeInfomationIndex
  |       |--(2)rstpRootBridgeInfomationBridgeID
  |       |--(3)rstpRootBridgeInfomationRootPriority
  |       |--(4)rstpRootBridgeInfomationRootPort
  |       |--(5)rstpRootBridgeInfomationRootPathCost
  |       |--(6)rstpRootBridgeInfomationMaxAge
  |       |--(7)rstpRootBridgeInfomationHelloTime
  |       |--(8)rstpRootBridgeInfomationForwardDelay
  |--(2)rstpPerPortInfoTable
  |   |--(1)rstpPerPortInfoEntry
  |       |--(1)rstpPerPortInfoPortNum
  |       |--(2)rstpPerPortInfoPathCost
  |       |--(3)rstpPerPortInfoPriority
  |       |--(4)rstpPerPortInfoAdminP2P
  |       |--(5)rstpPerPortInfoAdminEdge
  |       |--(6)rstpPerPortInfoStpNeighbor
  |       |--(7)rstpPerPortInfoState
  |       |--(8)rstpPerPortInfoRole
--(5)ieee8021qVlan
  |--(1)vlanOperationMode
  |--(2)vlanGVRP
  |--(3)vlanIEEE8021QTable
  |   |--(1)vlanIEEE8021QEntry
  |       |--(1)vlanIEEE8021QIndex
  |       |--(2)vlanIEEE8021QPortName
  |       |--(3)vlanIEEE8021QLinkType
  |       |--(4)vlanIEEE8021QUntaggedVid
  |       |--(5)vlanIEEE8021QTaggedVids
  |--(4)vlanIEEE8021QGroupTable
  |   |--(1)vlanIEEE8021QGroupEntry
  |       |--(1)vlanIEEE8021QGroupVid
  |       |--(2)vlanIEEE8021QGroupName
  |       |--(3)vlanIEEE8021QGroupStatus
--(6)trafficPrioritization
  |--(1)qosPolicy
  |--(2)qosPriorityType
  |--(3)qosPortBasedPriorityTable
  |   |--(1)qosPortBasedPriorityEntry
  |       |--(1)qosPortBasedPriorityPortNum
  |       |--(2)qosPortBasedPriority
  |--(4)qosCOSTable
  |   |--(1)qosCOSEntry
  |       |--(1)qosCOSPRIORITY
  |       |--(2)qosCOS
  |--(5)qosCOSPortDefaultTable
  |   |--(1)qosCOSPortDefaultEntry
  |       |--(1)qosCOSPort
  |       |--(2)qosCOSPortDefault
  |--(6)qosTOSTable
  |   |--(1)qosTOSEntry
  |       |--(1)qosTOSPRIORITY
  |       |--(2)qosTOS
--(7)multicastFiltering
  |--(1)igmpStatus
  |--(2)igmpQuery
  |--(3)igmpEntriesTable
  |   |--(1)igmpEntriesEntry
  |       |--(1)igmpEntriesEntryIndex
  |       |--(2)igmpEntriesEntryIPAddr
  |       |--(3)igmpEntriesEntryVID
  |       |--(4)igmpEntriesEntryMembers
--(8)snmp
  |--(1)snmpAgentMode
  |--(2)snmpSystemName
  |--(3)snmpSystemLocation
  |--(4)snmpSystemContact
  |--(5)snmpCommunityStringTable
  |   |--(1)snmpCommunityStringEntry
  |       |--(1)snmpCommunityStringIndex
  |       |--(2)snmpCommunityStringName
  |       |--(3)snmpCommunityStringAttribute
  |       |--(4)snmpCommunityStringStatus
  |--(6)snmpTrapServerTable
  |   |--(1)snmpTrapServerEntry
  |       |--(1)snmpTrapServerIndex
  |       |--(2)snmpTrapServerIPAddr
```

```
|      |--(3)snmpTrapServerTrapComm
|      |--(4)snmpTrapServerTrapVer
|      |--(5)snmpTrapServerStatus
|--(9)security
| |--(1)portSecurityMgt
| | |--(1)portSecurityTable
| | | |--(1)portSecurityEntry
| | | | |--(1)portSecurityIndex
| | | | |--(2)portSecurityPortName
| | | | |--(3)portSecurityAddr
| | | | |--(4)portSecurityStatus
|--(2)ipSecurityMgt
| |--(1)ipSecurityStatus
| |--(2)ipSecurityHTTPServerStatus
| |--(3)ipSecurityTelnetServerStatus
| |--(4)ipSecuritySNMPServerStatus
| |--(5)ipSecuritySecurityIP1
| |--(6)ipSecuritySecurityIP2
| |--(7)ipSecuritySecurityIP3
| |--(8)ipSecuritySecurityIP4
| |--(9)ipSecuritySecurityIP5
| |--(10)ipSecuritySecurityIP6
| |--(11)ipSecuritySecurityIP7
| |--(12)ipSecuritySecurityIP8
| |--(13)ipSecuritySecurityIP9
| |--(14)ipSecuritySecurityIP10
|--(3)macFiltering
| |--(1)macFilteringTable
| | |--(1)macFilteringEntry
| | | |--(1)macFilterIndex
| | | |--(2)macFilterAddr
| | | |--(3)macFilterStatus
|--(4)ieee8021x
| |--(1)radiusServerSetting
| | |--(1)radius8021xProtocolStatus
| | |--(2)radiusServerIP
| | |--(3)radiusServerPort
| | |--(4)radiusAccountingPort
| | |--(5)radiusShareKey
| | |--(6)radiusNASIdentifier
| | |--(7)radiusMiscQuietPeriod
| | |--(8)radiusMiscTxPeriod
| | |--(9)radiusMiscSupplicantTimeout
| | |--(10)radiusMiscServerTimeout
| | |--(11)radiusMiscReAuthMax
| | |--(12)radiusMiscReauthPeriod
|--(2)portAuthConfiguration
| |--(1)radiusPerPortCfgTable
| | |--(1)radiusPerPortCfgEntry
| | | |--(1)radiusPerPortCfgIndex
| | | |--(2)radiusPerPortCfgPortName
| | | |--(3)radiusPerPortCfgState
|--(10)warning
| |--(1)eventAndEmailWarning
| | |--(1)eventSelection
| | | |--(1)systemEventsTable
| | | | |--(1)systemEventsEntry
| | | | | |--(1)eventSystemEventIndex
| | | | | |--(2)eventDeviceColdStartEvent
| | | | | |--(3)eventDeviceWarmStartEvent
| | | | | |--(4)eventAuthenticationFailureEvent
| | | | | |--(5)eventSuperRingTopologyChangeEvent
| | |--(2)portEventsTable
| | | |--(1)portEventsEntry
| | | | |--(1)eventPortNumber
| | | | |--(2)eventPortEventLog
| | | | |--(3)eventPortEventSMTP
|--(2)sysLogConfiguration
| |--(1)syslogStatus
| |--(2)eventServerAddr
|--(3)smtpConfiguration
| |--(1)eventEmailAlertStatus
| |--(2)eventEmailAlertAddr
| |--(3)eventEmailAlertAuthentication
| |--(4)eventEmailAlertAccount
| |--(5)eventEmailAlertPassword
| |--(6)emailAlertRcptTable
| | |--(1)emailAlertRcptEntry
| | | |--(1)eventEmailAlertRcptIndex
```

```
|      |--(2)eventEmailAlertRcptEmailAddr
|--(11)monitorandDiag
|  |--(1)macAddressTable
|  |  |--(1)macAddrTable
|  |  |  |--(1)macAddrEntry
|  |  |  |  |--(1)macAddressIndex
|  |  |  |  |--(2)macAddressPortName
|  |  |  |  |--(3)macAddressAddr
|  |  |  |  |--(4)macAddressType
|  |  |--(2)portSecurityClearMACTable
|--(2)PortStatistic
|  |--(1)switchPortStatTable
|  |  |--(1)switchPortStatEntry
|  |  |  |--(1)swPortStatIndex
|  |  |  |--(2)swPortStatType
|  |  |  |--(3)swPortStatLink
|  |  |  |--(4)swPortStatState
|  |  |  |--(5)swPortStatTXGoodPkt
|  |  |  |--(6)swPortStatTXBadPkt
|  |  |  |--(7)swPortStatRXGoodPkt
|  |  |  |--(8)swPortStatRXbadPkt
|  |  |  |--(9)swPortStatTXAbortPkt
|  |  |  |--(10)swPortStatPacketCollision
|--(3)portmirroring
|  |--(1)swPortMirrorDestinationPortTX
|  |--(2)swPortMirrorDestinationPortRX
|  |--(3)switchPortMirrorSourceTable
|  |  |--(1)switchPortMirrorSourceEntry
|  |  |  |--(1)swPortMirrorPortNum
|  |  |  |--(2)swPortMirrorSourcePort
|--(4)eventLog
|  |--(1)eventLogTable
|  |  |--(1)eventLogEntry
|  |  |  |--(1)eventLogIndex
|  |  |  |--(2)eventLogDescription
|--(12)save
|  |--(1)saveCfgMgtAction
|--(13)specificTrap
|  |--(1)trapPowerStatus
|  |--(2)trapTopologyChange
```

Appendix A

Specification

Technology

Standards
IEEE802.3, 802.3u, 802.3x, 802.1D, 802.1W, 802.1Q, 802.1p

Protocols

IGMP V1/V2/V3 device, GVRP, SNMP V1/V2C/V3, DHCP Server/Client, BootP, TFTP, SNTP, SMTP, RARP

MIB

MIB-II, Ethernet-Like MIB, P-BRIDGE MIB, Q-BRIDGE MIB, Bridge MIB, RSTP MIB

Forwarding and Filtering Rate

148800 pps

Processing Type

Store and Forward

Flow Control

IEEE802.3x flow control, back pressure flow control

Address Table Size

8K uni-cast addresses

Interface

RJ45 Ports

10/100BaseT(X) auto negotiation speed, F/H duplex mode, and auto MDI/MDI-X connection

Fiber Ports
100BaseFX ports (SC/ST connector)

Console
RS-232 (RJ45)

LED Indicators
Power, Fault, 10/100M, Ring Master, and Ring Coupler

Alarm Contact
One relay outputs with current carrying capacity of 1A @ 24 VDC

Power
Input Voltage
12 to 48 VDC, redundant inputs

Input Current (@24V)
0.29A:
0.43A:

Connection
Two removable 7-pin terminal blocks

Overload Current Protection
Present, can withstand 1.6A

Reverse Polarity Protection
Present

Mechanical
Casing
IP30 protection, aluminum case

Dimensions
56.5 x 110 x 150 mm (D x W x H)

Installation
DIN-Rail, Wall Mounting

Casing
IP30 protection, metal case

Environment
Operating Temperature
Standard 0 to 60°C / Extend -40 to 80°C

Storage Temperature
-40 to 85°C

Ambient Relative Humidity
5% to 95% (non-condensing)

Regulatory Approvals
Safety
UL60950 (E212360), UL 508, CAN/CSA C22.2 No. 60950

Hazardous Location
UL/cUL Class I, Division 2

EMI
CE/FCC Part 15, CISPR (EN55022) class A

Shock
IEC60068-2-27

Freefall
IEC60068-2-32

Vibration
IEC60068-2-6

MTBF
830,000 hours

WARRANTY
5 years

Appendix B

Service Information

This appendix shows you how to contact Industrial-managed for information about this and other products, and how to report problems. In this appendix, we cover the following topics.

- **Industrial-managed Internet Services**
- **Problem Report Form**
- **Product Return Procedure**

Industrial-managed Internet Services

Customer satisfaction is our number one concern, and to ensure that customers receive the full benefit of our products, Industrial-managed Internet Services has been set up to provide technical support, driver updates, product information, and user's manual updates.

The following services are provided

E-mail for technical support.....info@sunix-ncci.com.tw

World Wide Web (WWW) Site for product information:<http://www.sunix-ncci.com.tw>

Problem Report Form

Sunix Series

Customer name:

Company:

Tel:

Fax:

Email:

Date:

1. Industrial-managed Product:

ESW-8062-TX ESW-8062-GT ESW-8062-SS ESW-8062-GS ESW-8062-MM ESW-8062-GM

2. Serial Number: _____

Problem Description:

Please describe the symptoms of the problem as clearly as possible, including any error messages you see. A clearly written description of the problem will allow us to reproduce the symptoms, and expedite the repair of your product.

Product Return Procedure

For product repair, exchange, or refund, the customer must:

- Ⓒ Provide evidence of original purchase.
- Ⓒ Obtain a Product Return Agreement(PRA) from the sales representative or dealer.
- Ⓒ Fill out the Problem Report Form. Include as much detail as possible for a shorter product repair time.
- Ⓒ Carefully pack the product in an anti-static package, and send it, pre-paid, to the dealer. The PRA should be visible on the outside of the package, and include a description of the problem, along with the return address and telephone number of a technical contact.