Lantech

8 10/100TX plus 1 10/100/1000T + 1 MINI GBIC Managed Switch

MODEL:LES2208

User Manual

Notice

This manual contents are based on the below table listing software kernel version, hardware version, and firmware version. If your switch functions have any different from the manual contents description, please contact the local sale dealer for more information.

Firmware Version	V1.08
Kernel Version	V1.23
Hardware Version	---------

FCC Warning

This Equipment has been tested and found to comply with the limits for a Class-A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

CE Mark Warning

This is a Class-A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Content

Introduction

The 8 10/100TX plus 1 10/100/1000T + 1 MINI GBIC Managed Switch is a multi-port switch that can be used to build high-performance switched workgroup networks. This switch is a store-and-forward device that offers low latency for high-speed networking. The switch is targeted at workgroup, department or backbone computing environment.

The 8 10/100TX plus 1 10/100/1000T + 1 MINI GBIC Managed Switch features a "store-and-forward "switching scheme. This allows the switch to auto-learn and store source address in an 8K-entry MAC address table.

The 8 10/100TX plus 1 10/100/1000T + 1 MINI GBIC Managed Switch has 8x auto-sensing 10/100Base-TX RJ-45 ports and 1 Giga copper port and 1 Mini GBIC slot for higher connection speed.

Features

- Confirm to IEEE802.3 10BASE-T, 802.3u 100BASE-TX, 802.3z Gigabit fiber and IEEE 802.3ab 1000Base-T
- 8-port 10/100TX plus 1 Mini GBIC socket and 1 10/100/1000T port
- 5.6Gbps switch bandwidth
- Support IEEE802.3x Flow control
  - ➢ Flow control with full duplex
  - ➢ Backpressure with half duplex
- Support 802.1p COS with per port 4 queues
- Support IGMP snooping and Query mode with Multi-Media application
- Support Port mirror and bandwidth control
- Support GVRP function
- Support TFTP firmware update
- Support Web/SNMP/Telnet/CLI management

- Support Per port band width control
- Support Management IP address security
- Support System Event log
- Support Port Based VLAN /802.1Q VLAN
- Support IEEE802.3ad Port trunk with LACP
- Support Spanning tree protocol
  - STP / Rapid STP
- QoS method:
  - Port based / Tag based
  - IPv4 ToS/ Ipv4, IPv6 DiffServe
- Support IEEE 802.1x user authentication
- Support Broadcast storm filter
- Support DHCP Client and Server
- Support SNTP and SMTP
- Support MAC address security
- Support SNMP Trap
- Configuration up-load and down-load

Software Feature

Management	SNMP v1 SNMP v2c SNMP v3 Telnet Console (CLI) and Web management
SNMP Trap	Up to 3 Trap stations Cold start, Port link up, Port link down, Authentication Failure, Private Trap for power status, X-ring topology change

RFC standard	RFC2233 MIBII RFC 1157 SNMP MIB RFC 1493 Bridge MIB RFC 2674 VLAN MIB RFC 2665 Ethernet like MIB RFC1215 Trap MIB RFC 2819 RMON MIB Private MIB RFC2030 SNTP RFC 2821 SMTP RFC 1757 RMON1 MIB RFC 1215 Trap
Port Trunk	IEEE802.3ad with LACP function Up to 3 trunk groups Maximum group member up to 4 ports
Spanning Tree	IEEE802.1d Spanning tree IEEE802.1w Rapid spanning tree
VLAN	Port Based VLAN IEEE 802.1Q Tag VLAN (256 entries)/ VLAN ID (Up to 4K, VLAN ID can be assigned from 1 to 4096.) GVRP (256 Groups) Double Tag VLAN (Q in Q)*
Class of Service	Per port supports 4 queues Weight round ratio (WRR): High: Mid-High: Mid-Low: Low (8:4:2:1)

Quality of service	Port based Tag based IPv4 Type of service IPv6 Different service
IGMP	IGMP v1 and v2 compliance 256 IGMP groups query mode
Port Mirror	3 mirroring types: "RX, TX and Both packet" Maximum of port mirror entries is up to 8.
Port Security	ingress and egress MAC address filter Static source MAC address lock
Bandwidth Control	Support ingress packet filter and egress packet limit The egress rate control supports all of packet type and the limit rates are 100K~250Mbps Ingress filter packet type combination rules are Broadcast/Multicast/Unknown Unicast packet, Broadcast/Multicast packet, Broadcast packet only and all of packet. The packet filter rate can be set from 100k to 250Mbps
SNMP IP security	10 IP address accounts for system management security for Web, SNMP, Telnet management security to prevent intruder
User Authentication	IEEE802.1x User-Authentication and can report to RADIUS server. ■ Reject ■ Accept ■ Authorize

	■ Disable
DHCP	DHCP Client DHCP Server
Software Upgrade	TFTP firmware upgrade
Packet filter	Broadcast storm packet filter
Port security	Support 100 entries of MAC address for static MAC and another 100 for MAC filter
System log	Support System log record and remote system log server
SNTP	Support SNTP to synchronize system clock in Internet
SMTP	Support SMTP Server and 6 e-mail accounts for receiving event alert
Configuration upload and download	Support text format configuration file for system quick installation

* Future release

Package Contents

Unpack the contents of the 8 10/100TX plus 1 10/100/1000T + 1 MINI GBIC Managed Switch and verify them against the checklist below:

■ 8 10/100TX plus 1 10/100/1000T + 1 MINI GBIC Managed Switch

■ Four Rubber Pads

■ RS-232 cable

■ Power Cord

■ User Manual

**8 10/100TX + 1 10/100/1000T
+ 1 Mini-GBIC Managed Switch**

Four Rubber Pads

RS-232 cable
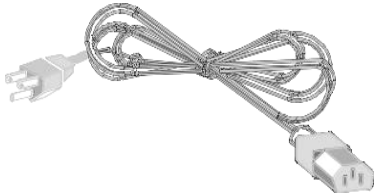
Power Cord

User Manual

Compare the contents of your 8 10/100TX plus 1 10/100/1000T + 1 MINI GBIC Managed Switch package with the standard checklist above. If any item is missing or damaged, please contact the local dealer for exchanging.

Hardware Description

This section mainly describes the hardware of the 8 10/100TX plus 1 10/100/1000T + 1 MINI GBIC Managed Switch and gives a physical and functional overview on the certain switch.

Physical Dimension

8 10/100TX plus 1 10/100/1000T + 1 MINI GBIC Managed Switch's physical dimensions is **217mm(W) x 140mm(D) x 43mm(H)**.

Front Panel

The front panel of the 8 10/100TX plus 1 10/100/1000T + 1 MINI GBIC Managed Switch consists of 8x 10/100Base-TX RJ-45 ports (Auto MDI/MDIX), 1 Giga port and 1 Mini GBIC module (module is optional). The LED Indicators are also located on the front panel of the switch.
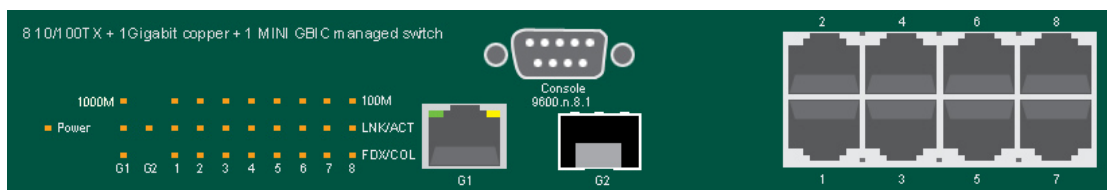
The Front panel of the 8 10/100TX plus 1 10/100/1000T + 1 MINI GBIC Managed Switch

■ **RJ-45 Ports (Auto MDI/MDIX):** 8x 10/100 N-way auto-sensing for 10Base-T or 100Base-TX connections.

In general, **MDI** means connecting to another Hub or Switch while **MDIX** means connecting to a workstation or PC. Therefore, **Auto MDI/MDIX** would allow connecting to another switch or workstation without changing non-crossover or

7

crossover cabling.
- **1 Giga port:** 1x 10/100/1000TX N-Way auto-sensing for 10/100/1000 connection.
- **1 Mini GBIC port:** one optional mini GBIC module port

LED Indicators

The LED Indicators display real-time information of systematic operation status. The following table provides descriptions of LED status and their meaning.
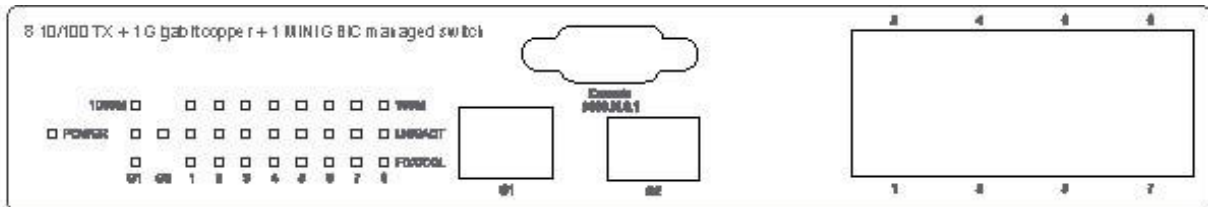
LED indicators

LED	Status	Description
Power	Green	Power On
	OFF	Power is not connected
100M	Green	In 100Mbps connection speed
	Blink	In 10Mbps connection speed
	OFF	No device attached
LNK/ACT	Green	The port is connecting with the device
	Blink	The port is receiving or transmitting data
	OFF	No device attached.

8

FDX/COL	Orange	The port is operating in Full-duplex mode
	Blinks	Collision of packets occurs
	OFF	In half-duplex mode
1000M (G1 port)	Green	In 1000Mbps connection speed
	Orange	In 100Mbps connection speed
	OFF	No device attached
LNK/ACT (G1 port)	Green	The port is connecting with the device
	Blink	The port is receiving or transmitting data
	OFF	No device attached
FDX/COL (G1 port)	Orange	The port is operating in Full-duplex mode
	Blink	Collision of Packets occurs in the port
	OFF	In half-duplex mode
LNK/ACT (G2 port)	Green	The port is connecting with the device
	Blink	The port is receiving or transmitting data

Rear Panel

The 3-pronged power plug is located at the rear panel of the 8 10/100TX plus 1 10/100/1000T + 1 MINI GBIC Managed Switch as shown in figure. The switch will work with AC in the voltage range of AC 100-240V and Frequency of 50-60Hz.
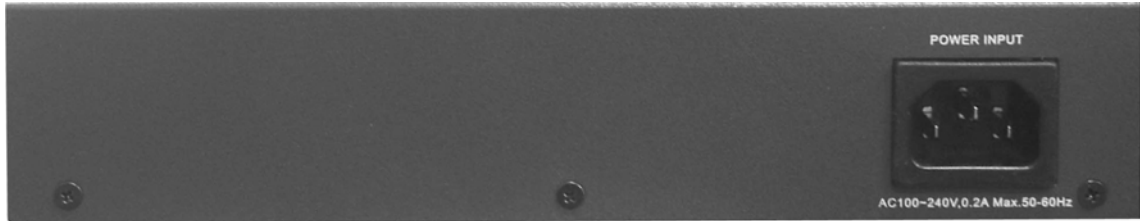
The Rear Panel of the 8 10/100TX plus 1 10/100/1000T + 1 MINI GBIC Managed Switch

Desktop Installation

Set the switch on a sufficiently large flat space with a power outlet nearby. The surface where you put the switch should be clean, smooth, level and sturdy. Make sure there is enough clearance around the switch to allow attachment of cables, power cord and allow air circulation.

Attaching Rubber Pads

A.   Make sure mounting surface on the bottom of the switch is grease and dust free.
B.   Remove adhesive backing from your Rubber Pads.
C.   Apply the Rubber Pads to each corner on the bottom of the switch. These footpads can prevent the switch from shock/vibration.

Power On

Connect the power cord to the power socket on the rear panel of the switch. The other side of power cord connects to the power outlet. The internal power supply of the switch works with voltage range of AC in the 100-240VAC and Frequency of 50~60Hz. Check the power indicator on the front panel to see if power is properly supplied.

Network Application

This section provides a few samples of network topology in which the switch is used. In general, the 8 10/100TX plus 1 10/100/1000T + 1 MINI GBIC Managed Switch is designed as a segment switch which with its large address table (8k MAC address) and high performance, it is ideal for interconnecting networking segments.

PC, workstations, and servers can communicate each other by directly connecting with 8 10/100TX plus 1 10/100/1000T + 1 MINI GBIC Managed Switch. The switch automatically learns nodes address, which are subsequently used to filter and forward all traffic based on the destination address.

By using Uplink port, the switch can connect with another switch or hub to interconnect other small-switched workgroups to form a larger switched network. Meanwhile, user can also use fiber ports to connect switches.

Small Workgroup

The 8 10/100TX plus 1 10/100/1000T + 1 MINI GBIC Managed Switch can be used as a standalone switch to which personal computers, server, printer server, are directly connect to form a small workgroup.

8 10/100TX plus 1 Gigabit copper
& MINI GBIC Managed Switch

PC   Laser Printer   Scanner
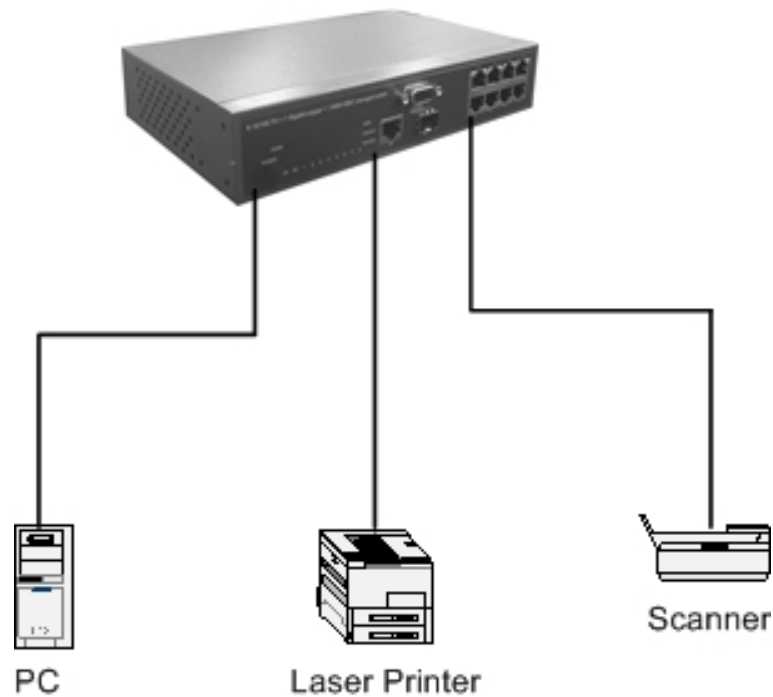
Small Workgroup application

Segment Bridge

For enterprise networks where large data broadcasts are constantly processed, this switch is an ideal solution for department users to connect to the corporate backbone.

In the illustration below, two Ethernet switches with PCs, print server, and local server attached, are both connect to the switch. All the devices in this network can communicate with each other through the switch. Connecting servers to the switch allow other users to access the data on server.

Core Switch

8 10/100TX plus 1 Gigabit copper
& MINI GBIC Managed Switch

8 10/100TX plus 1 Gigabit copper
& MINI GBIC Managed Switch

PC   Laser Printer   Scanner   Server   Laser Printer   PC
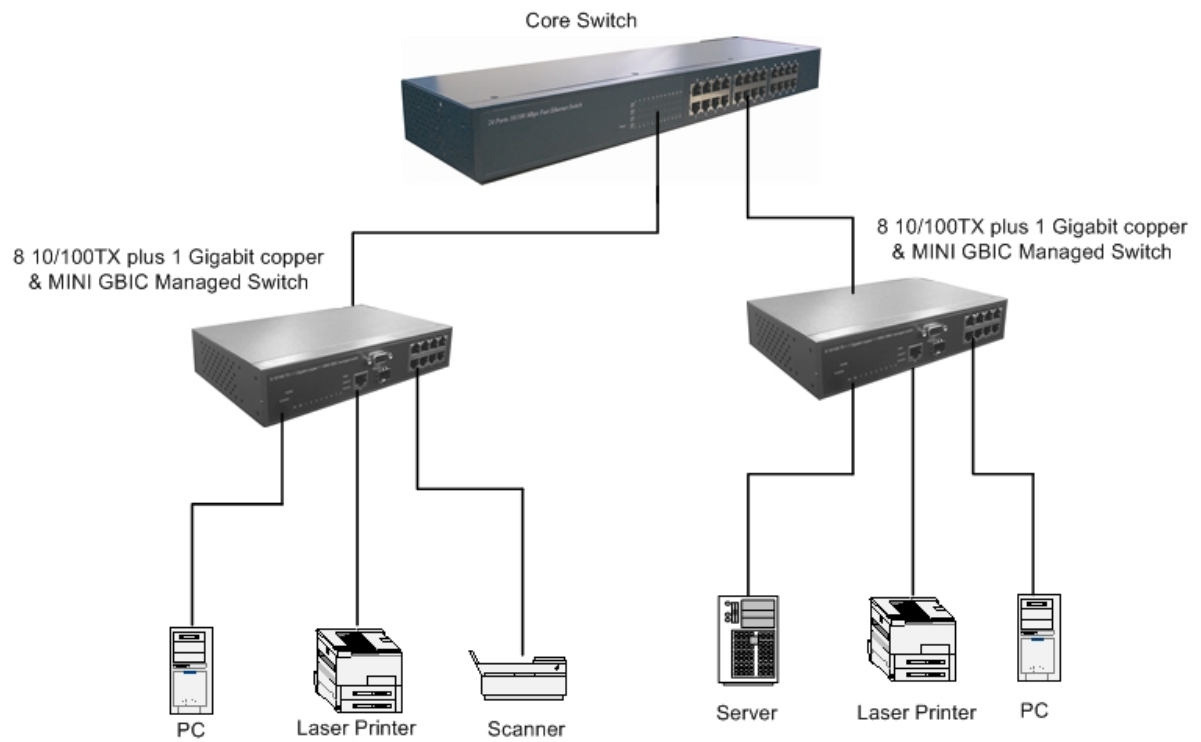
Segment Bridge application

Console Management

Login in the Console Interface

When the connection between switch and PC is ready, and then turn on the PC and run a terminal emulation program or **Hyper Terminal** and configure its **communication parameters** to match the following default characteristics of the console port:

Baud Rate: 9600 bps

Data Bits: 8

Parity: none

Stop Bit: 1

Flow control: None
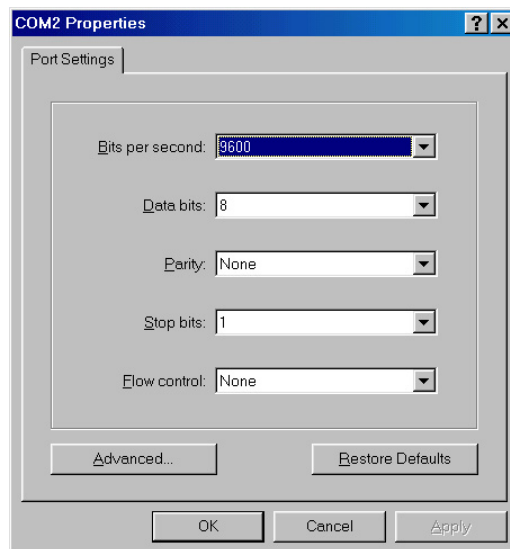
The settings of communication parameters

After finished the parameter settings, click "**OK**". When the blank screen shows up, press Enter key to bring out the login prompt. Key in the "**root**"(default value) for the both User name and Password (use **Enter** key to switch), then press Enter key and the console management appears right after. Please see below figure for login screen.

```
                    Welcome to the
        FE-8F2GBTM SNMP Managed Ethernet Switch




                    User Name :
                    Password  :
```

Console login screen

CLI Management

The system supports console management – CLI command. After you login to the system, you will see a command prompt. To enter CLI management interface, enter "**enable**" command. The following table lists the CLI commands and description.

```
switch>enable
switch#_
```
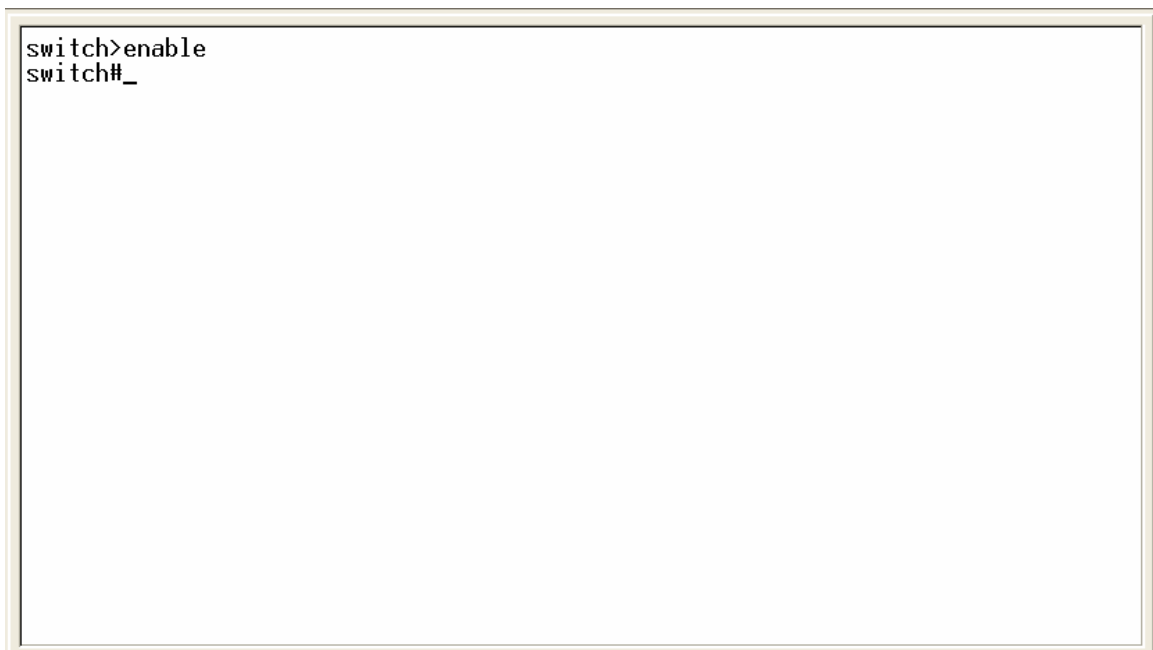
Commands Level

Modes	Access Method	Prompt	Exit Method	About This Mode1
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 • Perform basic tests. • Display system information.
Privileged EXEC	Enter the enable command while in user EXEC mode.	switch#	Enter disable to exit.	The privileged command is advance mode Privileged this mode to • Display advance function status • Save configures
Global Configuration	Enter the configure command while in privileged EXEC mode.	switch (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	switch (vlan)#	To exit to user EXEC	Use this mode to configure

			To exit to global configuration mode, enter exit. To exist to privileged EXEC mode, or end.	
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.

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

Commands Set List

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**
write memory	P	Save user configuration into permanent memory (flash rom)	switch#**write memory**

system name	G	Configure system name	switch(config)#**system name xxx**
[System Name]			
system location	G	Set switch system location string	switch(config)#**system location xxx**
[System Location]			
system description	G	Set switch system description string	switch(config)#**system description xxx**
[System Description]			
system contact	G	Set switch system contact window string	switch(config)#**system contact xxx**
[System Contact]			
show system-info	E	Show system information	switch>**show system-info**
ip address	G	Configure the IP address of switch	switch(config)#**ip address 192.168.1.1 255.255.255.0 192.168.1.254**
[Ip-address]			
[Subnet-mask]			
[Gateway]			
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	G	Changes a login username. (maximum 10 words)	switch(config)#**admin username xxxxxx**
[Username]			
admin password	G	Specifies a password (maximum 10 words)	switch(config)#**admin password xxxxxx**
[Password]			
show admin	P	Show administrator information	switch#**show admin**
dhcpserver enable	G	Enable DHCP Server	switch(config)#**dhcpserver enable**
Dhcpserver disable	G	Disable DHCP Server	switch(config)#**no dhcpserver**

dhcpserver lowip [Low IP]	G	Configure low IP address for IP pool	switch(config)#**dhcpserver lowip 192.168.1.100**
dhcpserver highip [High IP]	G	Configure high IP address for IP pool	switch(config)#**dhcpserver highip 192.168.1.200**
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)#**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	G	Set the IP security list	switch(config)#**security ip 1**

[Index(1..10)] [IP Address]			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**

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**
no flowcontrol	I	Disable flow control of	switch(config-if)#**no flowcontrol**

		interface	
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	switch(config)#**interface fastEthernet 2** switch(config-if)#**bandwidth in 100**

		limit.	
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** (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** (config-if)#**show interface status**
show interface accounting	I	show interface statistic counter	switch(config)#**interface fastEthernet 2** (config-if)#**show interface accounting**

no accounting	I	Clear interface accounting information	switch(config)#**interface fastEthernet 2** switch(config-if)#**no accounting**

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 [Group ID] [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	switch(config)#**aggregator group 1 2-4 nolacp** or switch(config)#**aggregator group 1 3,1,2 nolacp**

Netstar Commands	Level	Description	Example
		range(ex.1-4) or a port list separate by a comma(ex.2, 3, 6)	
show aggregator	P	Show the information of trunk group	switch#**show aggregator 1** or switch#**show aggregator 2** or switch#**show aggregator 3**
no aggregator lacp [GroupID]	G	Disable the LACP function of trunk group	switch(config)#**no aggreator lacp 1**
no aggregator group [GroupID]	G	Remove a trunk group	switch(config)#**no aggreator group 2**

VLAN Commands Set

Netstar Commands	Level	Description	Example
vlan database	P	Enter VLAN configure mode	switch#**vlan database**
Vlanmode [portbase| 802.1q	gvrp]	V	To set switch VLAN mode.	switch(vlan)#**vlanmode portbase** or switch(vlan)#**vlanmode 802.1q** or switch(vlan)#**vlanmode gvrp**
no vlan	V	No VLAN	Switch(vlan)#**no vlan**
Ported based VLAN configuration			
vlan port-based grpname [Group Name] **grpid** [GroupID] **port**	V	Add new port based VALN	switch(vlan)#**vlan port-based grpname test grpid 2 port 2-4** or switch(vlan)#**vlan port-based grpname test grpid 2 port 2,3,4**

[PortNumbers]			
show vlan [GroupID] or **show vlan**	V	Show VLAN information	switch(vlan)#**show vlan 23**
no vlan group [GroupID]	V	Delete port base group ID	switch(vlan)#**no vlan group 2**
IEEE 802.1Q VLAN			
vlan 8021q name [GroupName] **vid** [VID]	V	Change the name of VLAN group, if the group didn't exist, this command can't be applied.	switch(vlan)#**vlan 8021q name test vid 22**
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 trunk [PortNumber] **access-link untag** [UntaggedVID]	V	Assign a access link for VLAN by trunk group	switch(vlan)#**vlan 8021q trunk 3 access-link untag 33**
vlan 8021q trunk [PortNumber] **trunk-link tag** [TaggedVID List]	V	Assign a trunk link for VLAN by trunk group	switch(vlan)#**vlan 8021q trunk 3 trunk-link tag 2,3,6,99** or

			switch(vlan)#**vlan 8021q trunk 3 trunk-link tag 3-20**
vlan 8021q trunk [PortNumber] **hybrid-link untag** [UntaggedVID] **tag** [TaggedVID List]	V	Assign a hybrid link for VLAN by trunk group	switch(vlan)#**vlan 8021q trunk 3 hybrid-link untag 4 tag 3,6,8** or switch(vlan)#**vlan 8021q trunk 3 hybrid-link untag 5 tag 6-8**
show vlan [GroupID] or **show vlan**	V	Show VLAN information	switch(vlan)#**show vlan 23**
no vlan group [GroupID]	V	Delete port base group ID	switch(vlan)#**no vlan group 2**

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	switch(config)#**spanning-tree max-age 15**

		this interval, it recomputed the Spanning Tree Protocol (STP) topology.	
spanning-tree hello-time [seconds]	**G**	Use the spanning-tree hello-time global configuration command to specify the interval between hello bridge protocol data units (BPDUs).	switch(config)#**spanning-tree hello-time 3**
spanning-tree forward-time [seconds]	**G**	Use the spanning-tree forward-time global configuration command to set the forwarding-time for the specified spanning-tree instances. The forwarding time determines how long each of the listening and learning states last before the port begins forwarding.	switch(config)#**spanning-tree forward-time 20**
stp-path-cost [1~200000000]	**I**	Use the spanning-tree cost interface configuration command to set the path cost for Spanning Tree	switch(config)#**interface fastEthernet 2** switch(config-if)#**stp-path-cost 20**

		Protocol (STP) calculations. In the event of a loop, spanning tree considers the path cost when selecting an interface to place into the forwarding state.	
stp-path-priority **[Port Priority]**	**I**	Use the spanning-tree port-priority interface configuration command to configure a port priority that is used when two switches tie for position as the root switch.	switch(config)#**interface fastEthernet 2** switch(config-if)#**stp-path-priority 128**
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**	Displays a summary of the spanning-tree	switch>**show spanning-tree**

Netstar Commands	Level	Description	Example
		states.	
no spanning-tree	G	Disable spanning-tree.	switch(config)#**no spanning-tree**

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 0 middle**
qos priority tos [Priority][lowest|low|middle|high]	G	Configure TOS Priority	switch(config)#**qos priority tos 3 high**
show qos	P	Displays the information of QoS configuration	Switch#**show qos**
no qos	G	Disable QoS function	switch(config)#**no qos**

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	P	Displays the details of	switch#**show igmp configuration**

Netstar Commands	Level	Description	Example
configuration		an 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**

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	G	Remove an entry of MAC address table	switch(config)#**no mac-address-table filter hwaddr**

		(filter)	**000012348678**
no mac-address-table	**G**	Remove dynamic entry of MAC address table	switch(config)#**no mac-address-table**

SNMP Commands Set

Netstar Commands	Level	Description	Example
snmp system-name [System Name]	**G**	Set SNMP agent system name	switch(config)#**snmp system-name l2switch**
snmp system-location [System Location]	**G**	Set SNMP agent system location	switch(config)#**snmp system-location lab**
snmp system-contact [System Contact]	**G**	Set SNMP agent system contact	switch(config)#**snmp system-contact where**
snmp agent-mode [v1v2c|v3|v1v2cv3]	**G**	Select the agent mode of SNMP	switch(config)#**snmp agent-mode v1v2cv3**
snmp community-strings [Community] **right** [RO/RW]	**G**	Add SNMP community string.	switch(config)#**snmp community-strings public right rw**
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**
snmpv3 context-name [Context Name]	**G**	Configure the context name	switch(config)#**snmpv3 context-name Test**
snmpv3 user [User Name] **group**	**G**	Configure the userprofile for SNMPV3 agent.	switch(config)#**snmpv3 user test01 group G1 password AuthPW PrivPW**

[Group Name] **password** [Authentication Password] [Privacy Password]		Privacy password could be empty.	
snmpv3 access context-name [Context Name] **group** [Group Name] **security-level** [NoAuthNoPriv|AuthNoPriv|AuthPriv] **match-rule** [Exact|Prifix] **views** [Read View Name] [Write View Name] [Notify View Name]	G	Configure the access table of SNMPV3 agent	switch(config)#**snmpv3 access context-name Test group G1 security-level AuthPriv match-rule Exact views V1 V1 V1**
snmpv3 mibview view [View Name] **type** [Excluded|Included] **sub-oid** [OID]	G	Configure the mibview table of SNMPV3 agent	switch(config)#**snmpv3 mibview view V1 type Excluded sub-oid 1.3.6.1**
show snmp	P	Show SNMP configuration	switch#**show snmp**
no snmp community-strings [Community]	G	Remove the specified community.	switch(config)#**no snmp community-strings public**
no snmp-server host [Host-address]	G	Remove the SNMP server host.	switch(config)#**no snmp-server 192.168.1.50**

Netstar Commands	Level	Description	Example
no snmpv3 user **[User Name]**	**G**	Remove specified user of SNMPv3 agent.	switch(config)#**no snmpv3 user Test**
no snmpv3 access **context-name** [Context Name] **group** [Group Name] **security-level** [NoAuthNoPriv|AuthNoPriv|AuthPriv] **match-rule** [Exact|Prifix] **views** [Read View Name] [Write View Name] [Notify View Name]	**G**	Remove specified access table of SNMPv3 agent.	switch(config)#**no snmpv3 access context-name Test group G1 security-level AuthPr iv match-rule Exact views V1 V1 V1**
no snmpv3 mibview **view** [View Name] **type** [Excluded|Included] **sub-oid** [OID]	**G**	Remove specified mibview table of SNMPV3 agent.	switch(config)#**no snmpv3 mibview view V1 type Excluded sub-oid 1.3.6.1**

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	switch#**show monitor**

		information	
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**

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 radiousip **[IP address]**	**G**	Use the 802.1x system radious IP global configuration command to change the radious server IP.	switch(config)# **8021x system radiousip 192.168.1.1**
8021x system serverport **[port ID]**	**G**	Use the 802.1x system server port global configuration command to change the radious server port	switch(config)# **8021x system serverport 1815**
8021x system accountport **[port ID]**	**G**	Use the 802.1x system account port global configuration command to change	switch(config)# **8021x system accountport 1816**

		the accounting port	
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**

Netstar Commands	Level	Description	Defaults Example
8021x misc maxrequest [number]	G	Use the 802.1x misc max request global configuration command to set the MAX requests.	switch(config)# **8021x misc maxrequest 3**
8021x misc reauthperiod [sec.]	G	Use the 802.1x misc reauth period global configuration command to set the reauth period.	switch(config)# **8021x misc reauthperiod 3000**
8021x portstate [disable | reject | accept | authorize]	I	Use the 802.1x port state interface configuration command to set the state of the selected port.	switch(config)#**interface fastethernet 3** switch(config-if)#**8021x portstate accept**
show 8021x	E	Displays 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**

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	switch(config)#**restore**

		TFTP server and need to specify the IP of TFTP server and the file name of image.	**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**

SystemLog, SMTP and Event 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	Displays 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 X-ring-topology-change [Systemlog|SMTP|Both]	G	Set X-ring topology changed event type	switch(config)#**event X-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 X-ring-topology-change	G	Disable X-ring topology changed event type	switch(config)#**no event X-ring-topology-change**
no event systemlog	I	Disable port event for system log	switch(config)#**interface fastethernet 3** switch(config-if)#**no event systemlog**

| no event smpt | I | Disable port event for SMTP | switch(config)#**interface fastethernet 3** switch(config-if)#**no event smtp** |
| show systemlog | P | Show system log client & server information | switch#**show systemlog** |

SNTP Commands Set

Netstar Commands	Level	Description	Example
sntp enable	G	Enable SNTP function	switch(config)#**sntp enable**
sntp daylight	G	Enable daylight saving time, if SNTP function is inactive, this command can't be applied.	switch(config)#**sntp daylight**
sntp daylight-period [Start time] [End time]	G	Set period of daylight saving time, if SNTP function is inactive, this command can't be applied. Parameter format: [yyyymmdd-hh:mm]	switch(config)# **sntp daylight-period 20060101-01:01 20060202-01-01**
sntp daylight-offset [Minute]	G	Set offset of daylight saving time, if SNTP function is inactive, this command can't be applied.	switch(config)#**sntp daylight-offset 3**
sntp ip [IP]	G	Set SNTP server IP, if SNTP function is inactive, this command can't be applied.	switch(config)#**sntp ip 192.169.1.1**
sntp timezone [Timezone]	G	Set timezone index, use "show sntp	switch(config)#**sntp timezone 22**

		timzezone" command to get more information of index number	
show sntp	P	Show SNTP information	switch#**show sntp**
show sntp timezone	P	Show index number of time zone list	switch#**show sntp timezone**
no sntp	G	Disable SNTP function	switch(config)#**no sntp**
no sntp daylight	G	Disable daylight saving time	switch(config)#**no sntp daylight**

X-ring Commands Set

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

no Xring master	G	Disable ring master	switch(config)# **no Xring master**
no Xring couplering	G	Disable couple ring	switch(config)# **no Xring couplering**
no Xring dualhoming	G	Disable dual homing	switch(config)# **no Xring dualhoming**

Web-Based Management

This section introduces the configuration and functions of the Web-Based management.

About Web-based Management

On the CPU board of the switch, there is an embedded HTML web site residing in flash memory, which offers advanced management features and allow users to manage the switch from anywhere on the network through a standard browser such as Microsoft Internet Explorer.

The Web-Based Management supports Internet Explorer 6.0. And, it is applied with Java Applets for reducing network bandwidth consumption, enhance access speed and present an easy viewing screen.

Preparing for Web Management

Before use web management, user can use console to login the switch checking the default IP of the switch. Please refer to **Console Management** Chapter for console login. If user need change IP address in first time, user can use console mode to modify it. The default value is as below:

    IP Address: **192.168.16.1**
    Subnet Mask: **255.255.255.0**
    Default Gateway: **192.168.16.254**
    User Name: **root**   Password: **root**

System Login

- Launch the Internet Explorer.
- Key in "http://" + "IP Address" of the Switch, and then press "**Enter**"
- Login screen will appear right after
- Key in the user name and password. The default user name and password is "**root**"

■ Click "**Enter**" or" **OK**", then the home screen of the Web-based management appears right after
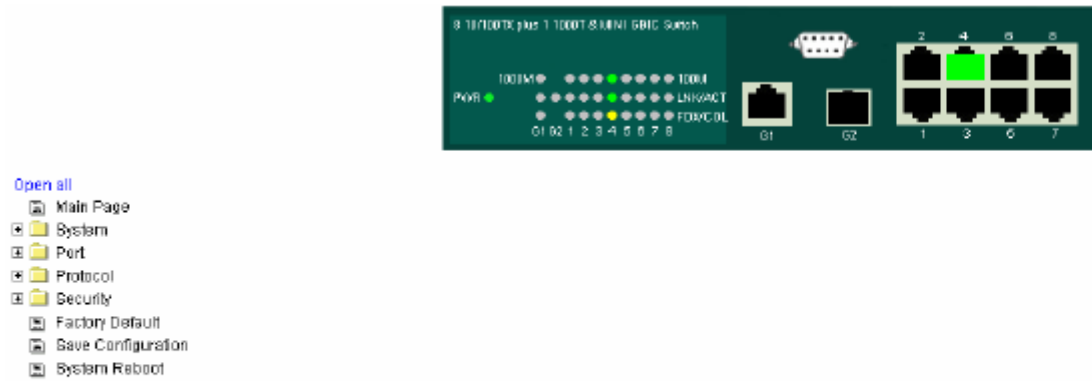
Welcome to the

FE-8F2GBTM SNMP Managed Ethernet Switch

Main interface

System Information

Assign the system name and location and view the system information

■ **System Name:** Assign the system name of the switch (The maximum length is 64 bytes)

■ **System Description:** Displays the description of switch(Read only cannot be modified)

■ **System Location:** Assign the switch physical location(The maximum length is 64 bytes)

■ **Firmware Version:** Displays the switch's firmware version

■ **Kernel Version:** Displays the kernel software version

■ **MAC Address:** Displays the unique hardware address assigned by manufacturer (default)

■ And than, click Apply

System Information

System Name	FE-8F2GBTM
System Description	FE-8F2GBTM SNMP Managed Ethernet Switch
System Location	
System Contact	

[Apply] [Help]

Firmware Version	v1.08
Kernel Version	v1.23
MAC Address	001122334466

System Information interface

IP Configuration

User can configure the IP Settings and DHCP client function

- ■ **DHCP:** To disable or enable the DHCP client function
- ■ **IP Address:** Assign the switch IP address. The default IP is 192.168.16.1
- ■ **Subnet Mask:** Assign the switch IP subnet mask
- ■ **Gateway:** Assign the switch gateway. The default value is 192.168.16.254
- ■ **DNS1:** Short for Domain Name Server an Internet service that translates domain name into IP addresses. Because domain name are alphabetic, they're easier to remember. The Internet is based on IP address. Every time you use a domain name , therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name **www.net.com** might translate to **192.168.1.1**
- ■ **DNS2:** The backup for DNS1. When the DNS1 cannot function, the DNS2 can replace DNS1 immediately
- ■ And than, click Apply
- ■ Reboot the switch after reset the IP address

IP Configuration

DHCP Client : Disable ☑

IP Address	192.168.16.1
Subnet Mask	255.255.255.0
Gateway	192.168.16.254
DNS1	0.0.0.0
DNS2	0.0.0.0

Apply Help

IP Configuration interface

DHCP Configuration

It short for Dynamic Host Configuration Protocol that is a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses. Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address.

DHCP Server Configuration

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

■ **DHCP Server:** To enable or Disable the DHCP Server function. Enable – the switch will be the DHCP server on your local network

■ **Low IP Address:** The dynamic IP range. Low IP address is the beginning of the

dynamic IP range. For example: dynamic IP range is from 192.168.1.100 ~ 192.168.1.200. 192.168.1.100 will be the Low IP address

- **High IP Address:** The dynamic IP range. High IP address is the end of the dynamic IP range. For example: dynamic IP range is from 192.168.1.100 ~ 192.168.1.200. 192.168.1.200 will be the High IP address

- **Subnet Mask:** The dynamic IP assign range subnet mask

- **Gateway:** The gateway in your network

- **DNS:** Domain Name Server IP Address in your network

- **Lease Time (sec):** It is the time period that system will reset the dynamic IP assignment to ensure the dynamic IP will not been occupied for a long time or the server doesn't know that the dynamic IP is idle

DHCP Server - System Configuration

| System Configuration | Client Entries | Port and IP Binding |

DHCP Server : Disable

Low IP Address	192.168.16.100
High IP Address	192.168.16.200
Subnet Mask	255.255.255.0
Gateway	192.168.16.254
DNS	0.0.0.0
Lease Time (sec)	86400

Apply Help

DHCP Server Configuration interface

DHCP Client Entries

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

DHCP Server - Client Entries

System Configuration	**Client Entries**	Port and IP Binding

IP addr	Client ID	Type	Status	Lease

DHCP Client Entries interface

Port and IP Bindings

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

DHCP Server - Port and IP Binding

System Configuration	Client Entries	**Port and IP Binding**

Port	IP
Port.01	0.0.0.0
Port.02	0.0.0.0
Port.03	0.0.0.0
Port.04	0.0.0.0
Port.05	0.0.0.0
Port.06	0.0.0.0
Port.07	0.0.0.0
Port.08	0.0.0.0
G1	0.0.0.0
G2	0.0.0.0

Apply   Help

Port and IP Bindings interface

TFTP - Update Firmware

It provides the functions to allow you to update the switch firmware. Before updating, make sure the TFTP server is ready and the firmware image is on the TFTP server.

■ **TFTP Server IP Address:** Key in the TFTP server IP

■ **Firmware File Name:** The name of firmware image

■ And then, click Apply

TFTP - Update Firmware

| Update Firmware | Restore Configuration | Backup Configuration |

| TFTP Server IP Address | 192.168.16.2 |
| Firmware File Name | image.bin |

Apply   Help

Update Firmware interface

TFTP - Restore Configuration

Restore EEPROM value from TFTP server

■ **TFTP Server IP Address:** Key in the TFTP server IP

■ **Restore File Name:** Key in the restore file image name

■ And then, click Apply

TFTP - Restore Configuration

| Update Firmware | **Restore Configuration** | Backup Configuration |

| TFTP Server IP Address | 192.168.16.2 |
| Restore File Name | data.bin |

Apply   Help

Restore Configuration interface

TFTP - Backup Configuration

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

■ **TFTP Server IP Address:** Key in the TFTP server IP

■ **Backup File Name:** Key in the file image name

■ And then, click Apply

TFTP - Backup Configuration

| Update Firmware | Restore Configuration | **Backup Configuration** |

| TFTP Server IP Address | 192.168.16.2 |
| Backup File Name | data.bin |

Apply   Help

Backup Configuration interface

System Event Log – Syslog Configuration

Configuring the system event mode that want to be collected and system log server IP.

1. **Syslog Client Mode:** select the system log mode – client only, server only, or both S/C.

2. **Syslog Server IP Address:** assigned the system log server IP.

3. Click Reload to refresh the events log.

4. Click Clear to clear all current events log.

5. After configuring, Click Apply .

System Event Log - Syslog Configuration

Syslog Configuration interface

System Event Log - SMTP Configuration

You can set up the mail server IP, mail account, account password, and forwarded email account for receiving the event alert.

1. **Email Alert:** enable or disable the email alert function.
2. **SMTP Server IP:** set up the mail server IP address (when **Email Alert** enabled, this function will then be available)..
3. **Authentication:** mark the check box to enable and configure the email account and password for authentication (when **Email Alert** enabled, this function will then be available)..
4. **Mail Account:** set up the email account, e.g. johnadmin@123.com, to receive the alert. It must be an existing email account on the mail server, which you had set up

in **SMTP Server IP Address** column.

5. **Password:** The email account password.

6. **Confirm Password:** reconfirm the password.

7. **Rcpt e-mail Address 1 ~ 6:** you can assign up to 6 e-mail accounts also to receive the alert.

8. Click Apply .

SMTP Configuration interface

System Event Log - Event Configuration

You can select the system log events and SMTP events. When selected events occur, the system will send out the log information. Also, per port log and SMTP events can be selected. After configure, Click Apply .

- **System event selection:** 4 selections – Device cold start, Device warm start, SNMP Authentication Failure, and X-ring topology change. Mark the checkbox to select the event. When selected events occur, the system will issue the logs.
  - ➢ **Device cold start:** when the device executes cold start action, the system will issue a log event.
  - ➢ **Device warm start:** when the device executes warm start, the system will issue a log event.
  - ➢ **Authentication Failure:** when the SNMP authentication fails, the system will issue a log event.
  - ➢ **X-ring topology change:** when the X-ring topology has changed, the system will issue a log event.

System Event Log - Event Configuration

| Syslog Configuration | SMTP Configuration | **Event Configuration** |

System event selection

Event Type	Syslog	SMTP
Device cold start	☐	☐
Device warm start	☐	☐
Authentication Failure	☐	☐
X-Ring topology change	☐	☐

Port event selection

Port	Syslog	SMTP
Port.01	Disable	Disable
Port.02	Disable	Disable
Port.03	Disable	Disable
Port.04	Disable	Disable
Port.05	Disable	Disable
Port.06	Disable	Disable
Port.07	Disable	Disable
Port.08	Disable	Disable
G1	Disable	Disable
G2	Disable	Disable

Apply   Help

■ **Port event selection:** select the per port events and per port SMTP events. It has 3 selections – Link UP, Link Down, and Link UP & Link Down. Disable means no event is selected.

> ➢ **Link UP:** the system will issue a log message when port connection is up only.
> ➢ **Link Down:** the system will issue a log message when port connection is down only.
> ➢ **Link UP & Link Down:** the system will issue a log message when port connection is up and down.

SNTP Configuration

You can configure the SNTP (Simple Network Time Protocol) settings. The SNTP allows you to synchronize switch clocks in the Internet.

1. **SNTP Client:** enable or disable SNTP function to get the time from the SNTP server.
2. **Daylight Saving Time:** enable or disable daylight saving time function. When daylight saving time is enabling, you need to configure the daylight saving time period..
3. **UTC Timezone:** set the switch location time zone. The following table lists the different location time zone for your reference.

Local Time Zone	Conversion from UTC	Time at 12:00 UTC
November Time Zone	- 1 hour	11am
Oscar Time Zone	-2 hours	10 am
ADT - Atlantic Daylight	-3 hours	9 am
AST - Atlantic Standard EDT - Eastern Daylight	-4 hours	8 am

EST - Eastern Standard CDT - Central Daylight	-5 hours	7 am
CST - Central Standard MDT - Mountain Daylight	-6 hours	6 am
MST - Mountain Standard PDT - Pacific Daylight	-7 hours	5 am
PST - Pacific Standard ADT - Alaskan Daylight	-8 hours	4 am
ALA - Alaskan Standard	-9 hours	3 am
HAW - Hawaiian Standard	-10 hours	2 am
Nome, Alaska	-11 hours	1 am
CET - Central European FWT - French Winter MET - Middle European MEWT - Middle European Winter SWT - Swedish Winter	+1 hour	1 pm
EET - Eastern European, USSR Zone 1	+2 hours	2 pm
BT - Baghdad, USSR Zone 2	+3 hours	3 pm
ZP4 - USSR Zone 3	+4 hours	4 pm
ZP5 - USSR Zone 4	+5 hours	5 pm
ZP6 - USSR Zone 5	+6 hours	6 pm
WAST - West Australian	+7 hours	7 pm

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

4. **SNTP Sever URL:** set the SNTP server IP address.
5. **Daylight Saving Period:** set up the Daylight Saving beginning time and Daylight Saving ending time. Both will be different in every year.
6. **Daylight Saving Offset (mins):** set up the offset time.
7. **Switch Timer:** display the switch current time.
8. Click Apply .

SNTP Configuration

SNTP Client : Disable ▾

Daylight Saving Time : Disable ▾

UTC Timezone	(GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London ▾
SNTP Server URL	0.0.0.0
Switch Timer	
Daylight Saving Period	20040101 00:00 20040101 00:00
Daylight Saving Offset(mins)	0

[Apply] [Help]

SNTP Configuration interface

IP Security

IP security function allows user to assign 10 specific IP addresses that have permission to access the switch through the web browser for the securing switch management.

- **IP Security Mode:** when this option is in **Enable** mode, the **Enable HTTP Server** and **Enable Telnet Server** check boxes will then be available.
- **Enable HTTP Server:** when this check box is checked, the IP addresses among Security IP1 ~ IP10 will be allowed to access via HTTP service.
- **Enable Telnet Server:** when checked, the IP addresses among Security IP1 ~ IP10 will be allowed to access via telnet service.
- **Security IP 1 ~ 10:** Assign up to 10 specific IP address. Only these 10 IP address can access and manage the switch through the Web browser
- And then, click Apply button to apply the configuration

[NOTE] Remember to execute the "Save Configuration" action, otherwise the new configuration will lose when switch power off.

IP Security interface

User Authentication

Change web management login user name and password for the management security issue

1. **User name:** Key in the new user name(The default is "root")

2. **Password:** Key in the new password(The default is "root")

3. **Confirm password:** Re-type the new password

4. And then, click [Apply]

User Authentication

User Name :	root
New Password :	••••
Confirm Password :	••••

Apply Help

User Authentication interface

Port Statistics

The following information provides the current port statistic information.

■ **Port:** The port number.

■ **Type:** Displays the current speed of connection to the port.

■ **Link:** The status of linking—'**Up**' or '**Down**'.

■ **State:** It's set by Port Control. When the state is disabled, the port will not transmit or receive any packet.

■ **Tx Good Packet:** The counts of transmitting good packets via this port.

■ **Tx Bad Packet:** The counts of transmitting bad packets (including undersize [less than 64 octets], oversize, CRC Align errors, fragments and jabbers packets) via this port.

■ **Rx Good Packet:** The counts of receiving good packets via this port.

■ **Rx Bad Packet:** The counts of receiving good packets (including undersize [less than 64 octets], oversize, CRC error, fragments and jabbers) via this port.

■ **Tx Abort Packet:** The aborted packet while transmitting.

■ **Packet Collision:** The counts of collision packet.

■ **Packet Dropped:** The counts of dropped packet.

■ **Rx Bcast Packet:** The counts of broadcast packet.

■ **Rx Mcast Packet:** The counts of multicast packet.

■ Click Clear button to clean all counts.

Port Statistics

Port	Type	Link	State	Tx Good Packet	Tx Bad Packet	Rx Good Packet	Rx Bad Packet	Tx Abort Packet	Packet Collision	Packet Dropped	RX Bcast Packet	RX Mcast Packet
Port.01	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.02	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.03	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.04	100TX	Up	Enable	13575	0	84102	0	0	0	0	53324	13505
Port.05	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.06	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.07	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.08	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
G1	1000TX	Down	Enable	0	0	0	0	0	0	0	0	0
G2	mGBIC	Down	Enable	0	0	0	0	0	0	0	0	0

Clear   Help

Port Statistics interface

Port Control

In Port control, you can view every port status that depended on user setting and the negotiation result.

1. **Port:** select the port that you want to configure.

2. **State:** Current port status. The port can be set to disable or enable mode. If the port setting is disable then will not receive or transmit any packet.

3. **Negotiation:** set auto negotiation status of port.

4. **Speed:** set the port link speed.

5. **Duplex:** set full-duplex or half-duplex mode of the port.

6. **Flow Control:** set flow control function is **Symmetric** or **Asymmetric** in Full Duplex mode. The default value is **Disable**.

7. **Security:** When its state is "**On**", means this port accepts only one MAC address.

8. Click Apply .

Port Control

Port	Group ID	Type	Link	State	Negotiation	Speed Duplex Config	Actual	Flow Control Config	Actual	Security
Port.01	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Symmetric	N/A	OFF
Port.02	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Symmetric	N/A	OFF
Port.03	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Symmetric	N/A	OFF
Port.04	N/A	100TX	Up	Enable	Auto	100 Full	100 Full	Symmetric	ON	OFF
Port.05	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Symmetric	N/A	OFF
Port.06	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Symmetric	N/A	OFF
Port.07	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Symmetric	N/A	OFF
Port.08	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Symmetric	N/A	OFF
G1	N/A	1000TX	Down	Enable	Auto	1G Full	N/A	Symmetric	N/A	OFF
G2	N/A	mGBIC	Down	Enable	Auto	1G Full	N/A	Symmetric	N/A	OFF

Port Control interface

Port Trunk

The Link Aggregation Control Protocol (LACP) provides a standardized means for exchanging information between Partner Systems on a link to allow their Link Aggregation Control instances to reach agreement on the identity of the Link Aggregation Group to which the link belongs, move the link to that Link Aggregation Group, and enable its transmission and reception functions in an orderly manner. Link aggregation lets you group up to seven consecutive ports into two dedicated connections. This feature can expand bandwidth to a device on the network. **LACP operation requires full-duplex mode,** more detail information refers to IEEE 802.3ad.

Aggregator setting

1. **System Priority:** a value used to identify the active LACP. The switch with the lowest value has the highest priority and is selected as the active LACP.

2. **Group ID:** There are three trunk groups to provide configure. Choose the "**Group ID**" and click `Select` .

3. **LACP:** If enable, the group is LACP static trunk group. If disable, the group is local static trunk group. All ports support LACP dynamic trunk group. If connecting to the device that also supports LACP, the LACP dynamic trunk group will be created automatically.

4. **Work ports:** allow max four ports can be aggregated at the same time. With LACP static trunk group, the exceed ports are standby and can be aggregated if work ports fail. If it is local static trunk group, the number of ports must be the same as the group member ports.

5. Select the ports to join the trunk group. Allow max four ports can be aggregated at the same time. Click `Add` button to add the port. To remove unwanted ports, select the port and click `Remove` button.

6. If LACP enable, you can configure LACP Active/Passive status in each ports on State Activity page.

7. Click `Apply` .

8. Use `Delete` button to delete Trunk Group. Select the Group ID and click `Delete` button.

Port Trunk - Aggregator Setting

Port Trunk—Aggregator Setting interface

Aggregator Information

When you have setup the LACP aggregator, you will see the related information here.

Port Trunk - Aggregator Information

Port Trunk – Aggregator Information interface

State Activity

When you had setup the LACP aggregator, you can configure port state activity. You can mark or un-mark the port. When you mark the port and click Apply button the port state activity will change to **Active**. Opposite is **Passive**.

- **Active:** The port automatically sends LACP protocol packets.
- **Passive:** The port does not automatically send LACP protocol packets, and responds only if it receives LACP protocol packets from the opposite device.

[NOTE]

1. A link having either two active LACP ports or one active port can perform dynamic LACP trunk.
2. A link has two passive LACP ports will not perform dynamic LACP trunk because both ports are waiting for an LACP protocol packet from the opposite device.
3. If you are active LACP's actor, after you have selected trunk port, the active status will be created automatically.

Port Trunk - State Activity

| Aggregator Setting | Aggregator Information | State Activity |

Port	LACP State Activity	Port	LACP State Activity
1	☑ Active	2	N/A
3	N/A	4	N/A
5	N/A	6	N/A
7	N/A	8	N/A
9	N/A	10	N/A

Apply   Help

Port Trunk – State Activity interface

Port Mirroring

The Port mirroring is a method for monitor traffic in switched networks. Traffic through ports can be monitored by one specific port. That means traffic goes in or out monitored (source) ports will be duplicated into mirror (destination) port.

■ **Destination Port:** There is only one port can be selected to be destination (mirror) port for monitoring both RX and TX traffic which come from source port. Or, use one of two ports for monitoring RX traffic only and the other one for TX traffic only. User can connect mirror port to LAN analyzer or Netxray

■ **Source Port:** The ports that user wants to monitor. All monitored port traffic will be copied to mirror (destination) port. User can select multiple source ports by checking the **RX** or **TX** check boxes to be monitored.

■ And then, click Apply button.

Port Mirroring

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

Apply Help

Port Trunk – Port Mirroring interface

Rate Limiting

You can set up every port's bandwidth rate and frame limitation type.

■ **Ingress Limit Frame type:** select the frame type that wants to filter. The frame types have 4 options for selecting: **All, Broadcast/Multicast/Flooded Unicast, Broadcast/Multicast** and **Broadcast only**.

Broadcast/Multicast/Flooded Unicast, Broadcast/Multicast and **Bbroadcast only** types are only for ingress frames. The egress rate only supports **All** type.

Rate Limiting

	Ingress Limit Frame Type	Ingress	Egress
Port.01	All	0 kbps	0 kbps
Port.02	All Broadcast/Multicast/Flooded Unicast	0 kbps	0 kbps
Port.03	Broadcast/Multicast Broadcast only	0 kbps	0 kbps
Port.04	All	0 kbps	0 kbps
Port.05	All	0 kbps	0 kbps
Port.06	All	0 kbps	0 kbps
Port.07	All	0 kbps	0 kbps
Port.08	All	0 kbps	0 kbps
G1	All	0 kbps	0 kbps
G2	All	0 kbps	0 kbps

Rate Range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports, and zero means no limit.

[Apply] [Help]

Rate Limiting interface

■ All the ports support port ingress and egress rate control. For example, assume port 1 is 10Mbps, users can set it's effective egress rate is 1Mbps, ingress rate is 500Kbps. The switch performs the ingress rate by packet counter to meet the specified rate

➢ **Ingress:** Enter the port effective ingress rate(The default value is "0")

➢ **Egress:** Enter the port effective egress rate(The default value is "0")

■ And then, click [Apply] to apply the settings

VLAN configuration

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

The industrial switch supports port-based and 802.1Q (tagged-based) VLAN. The default configuration of VLAN operation mode is "**Disable**".

VLAN Configuration

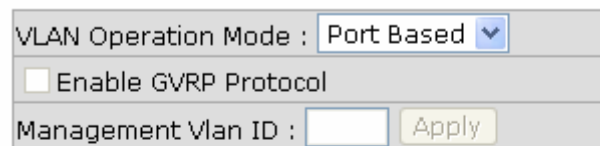|	
VLAN Operation Mode :	Disable
☐ Enable GVRP Protocol	
Management Vlan ID :	Apply

VLAN NOT ENABLE

VLAN Configuration interface

VLAN configuration - Port-based VLAN

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

In order for an end station to send packets to different VLAN groups, it itself has to be either capable of tagging packets it sends with VLAN tags or attached to a VLAN-aware bridge that is capable of classifying and tagging the packet with different VLAN ID based on not only default PVID but also other information about the packet, such as the protocol.

VLAN Configuration

VLAN Operation Mode : Port Based ∨
☐ Enable GVRP Protocol
Management Vlan ID : ☐ Apply

[Add] [Edit] [Delete] [Help]

VLAN – Port Based interface

- ■ Click Add to add a new VLAN group(The maximum VLAN group is up to 64 VLAN groups)
- ■ Entering the VLAN name, group ID and grouping the members of VLAN group
- ■ And then, click Apply

VLAN Configuration

VLAN Operation Mode : Port Based ▼
☐ Enable GVRP Protocol
Management Vlan ID : [____] [Apply]

| Group Name | [_____] |
| VLAN ID | 1 |

Port.01
Port.02
Port.03
Port.04
Port.05
Port.06
G1
G2
Trunk.1

[Add]

[Remove]

[Apply] [Help]

VLAN—Port Based Add interface

■ You will see the VLAN displays.

■ Use [Delete] button to delete unwanted VLAN.

■ Use [Edit] button to modify existing VLAN group.

[NOTE] Remember to execute the "Save Configuration" action, otherwise the new configuration will lose when switch power off.

802.1Q VLAN

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

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

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

VLAN Configuration

VLAN Operation Mode : 802.1Q
☐ Enable GVRP Protocol
Management Vlan ID : 0   Apply

802.1Q Configuration	Group Configuration

Port	Link Type	Untagged Vid	Tagged Vid
Port.01	Access Link	1	

Apply   Help

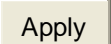| Port	Link Type	Untagged Vid	Tagged Vid
Port.01	Access Link	1	
Port.02	Access Link	1	
Port.03	Access Link	1	
Port.04	Access Link	1	
Port.05	Access Link	1	
Port.06	Access Link	1	
G1	Access Link	1	
G2	Access Link	1	
Trunk.1	Access Link	1	

802.1q VLAN interface

802.1Q Configuration

1. **Enable GVRP Protocol:** check the check box to enable GVRP protocol.
2. Select the port that wants to configure.
3. **Link Type**: there are 3 types of link type.
   - ■ **Access Link:** single switch only, allow user to group ports by setting the same VID.
   - ■ **Trunk Link:** extended application of **Access Link**, allow user to group ports by setting the same VID with 2 or more switches.
   - ■ **Hybrid Link:** Both **Access Link** and **Trunk Link** are available.
4. **Untagged VID:** assign the untagged frame VID.
5. **Tagged VID:** assign the tagged frame VID.
6. Click Apply
7. You can see each port setting in the below table on the screen.

Group Configuration

Edit the existing VLAN Group.

1. Select the VLAN group in the table list.
2. Click Apply

VLAN Configuration

VLAN Operation Mode : 802.1Q
☐ Enable GVRP Protocol
Management Vlan ID : 0   Apply

802.1Q Configuration   **Group Configuration**

Default___1

Edit Delete

Group Configuration interface

3. You can Change the VLAN group name and VLAN ID.

4. Click Apply .

VLAN Configuration

VLAN Operation Mode : 802.1Q
☐ Enable GVRP Protocol
Management Vlan ID : 0   Apply

802.1Q Configuration   **Group Configuration**

Group Name	Default
VLAN ID	1

Apply

Group Configuration interface

Rapid Spanning Tree

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

RSTP - System Configuration

- User can view spanning tree information about the Root Bridge
- User can modify RSTP state. After modification, click Apply button

  - ➢ **RSTP mode:** user must enable or disable RSTP function before configure the related parameters

  - ➢ **Priority (0-61440):** a value used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root. If the value changes, user must reboot the switch. The value must be multiple of 4096 according to the protocol standard rule

  - ➢ **Max Age (6-40):** the number of seconds a bridge waits without receiving Spanning-tree Protocol configuration messages before attempting a reconfiguration. Enter a value between 6 through 40

  - ➢ **Hello Time (1-10):** the time that controls switch sends out the BPDU packet to check RSTP current status. Enter a value between 1 through 10

  - ➢ **Forward Delay Time (4-30):** the number of seconds a port waits before changing from its Rapid Spanning-Tree Protocol learning and listening states to the forwarding state. Enter a value between 4 through 30

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

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

RSTP - System Configuration

System Configuration	Port Configuration

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

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

[Apply] [Help]

Root Bridge Information

Bridge ID	N/A
Root Priority	N/A
Root Port	N/A
Root Path Cost	N/A
Max Age	N/A
Hello Time	N/A
Forward Delay	N/A

RSTP System Configuration interface

RSTP - Port Configuration

You can configure path cost and priority of every port.

1. Select the port in Port column.
1. **Path Cost:** The cost of the path to the other bridge from this transmitting bridge at the specified port. Enter a number 1 through 200000000.
2. **Priority:** Decide which port should be blocked by priority in LAN. Enter a number 0 through 240. The value of priority must be the multiple of 16.
3. **P2P:** Some of the rapid state transactions that are possible within RSTP are dependent upon whether the port concerned can only be connected to exactly one other bridge (i.e. it is served by a point-to-point LAN segment), or can be connected to two or more bridges (i.e. it is served by a shared medium LAN segment). This

function allows the P2P status of the link to be manipulated administratively. True is P2P enabling. False is P2P disabling.

4. **Edge:** The port directly connected to end stations cannot create bridging loop in the network. To configure the port as an edge port, set the port to "**True**" status.

5. **Non Stp:** The port includes the STP mathematic calculation. **True** is not including STP mathematic calculation. **False** is including the STP mathematic calculation.

6. Click Apply .

RSTP - Port Configuration

| System Configuration | Port Configuration |

Port	Path Cost (1-200000000)	Priority (0-240)	Admin P2P	Admin Edge	Admin Non Stp
Port.01 Port.02 Port.03 Port.04 Port.05	200000	128	Auto	true	false

priority must be a multiple of 16

Apply Help

RSTP Port Status

Port	Path Cost	Port Priority	Oper P2P	Oper Edge	Stp Neighbor	State	Role
Port.01	200000	128	True	True	False	Disabled	Disabled
Port.02	200000	128	True	True	False	Disabled	Disabled
Port.03	200000	128	True	True	False	Disabled	Disabled
Port.04	200000	128	True	False	True	Forwarding	Root
Port.05	200000	128	True	True	False	Disabled	Disabled
Port.06	200000	128	True	True	False	Disabled	Disabled
Port.07	200000	128	True	True	False	Disabled	Disabled
Port.08	200000	128	True	True	False	Disabled	Disabled
G1	20000	128	True	True	False	Disabled	Disabled
G2	20000	128	True	True	False	Disabled	Disabled

RSTP Port Configuration interface

SNMP Configuration

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

by receiving traps or change notices from network devices implementing SNMP.

System Configuration

■ **Community Strings**

You can define new community string set and remove unwanted community string.
1. **String:** fill the name of string.
2. **RO:** Read only. Enables requests accompanied by this string to display MIB-object information.
3. **RW:** Read write. Enables requests accompanied by this string to display MIB-object information and to set MIB objects.
1. Click Add .
2. To remove the community string, select the community string that you have defined and click Remove . You cannot remove the default community string set.

■ **Agent Mode:** Select the SNMP version that you want to use it. And then click Change to switch to the selected SNMP version mode.

SNMP - System Configuration

| System Configuration | Trap Configuration | SNMPv3 Configuration |

Community Strings

Current Strings : **New Community String :** [Add]

[Remove]

```
public__RO
private__RW
```

String : [_____]

○ RO ○ RW

Agent Mode

Current Mode:
SNMP v1/v2c only

○ SNMP V1/V2C only
○ SNMP V3 only
○ SNMP V1/V2C/V3

[Change]

SNMP System Configuration interface

Trap Configuration

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

1. **IP Address:** enter the IP address of trap manager.
2. **Community:** enter the community string.
3. **Trap Version:** select the SNMP trap version type – v1 or v2.
4. Click [Add] .
5. To remove the community string, select the community string that you have defined and click [Remove] . You cannot remove the default community string set.

SNMP - Trap Configuration

| System Configuration | **Trap Configuration** | SNMPv3 Configuration |

Trap Managers

Current Managers :	New Manager :	
Remove		Add
(none)	IP Address :	
	Community :	
	Trap version: ⦿ v1 ◯ v2c	

Trap Managers interface

SNMPV3 Configuration

Configure the SNMP V3 function.

Context Table

Configure SNMP v3 context table. Assign the context name of context table. Click Add

to add context name. Click Remove to remove unwanted context name.

User Profile

Configure SNMP v3 user table..

- ■ **User ID:** set up the user name.
- ■ **Authentication Password:** set up the authentication password.
- ■ **Privacy Password:** set up the private password.
- ■ Click Add to add context name.
- ■ Click Remove to remove unwanted context name.

SNMP - SNMPv3 Configuration

| System Configuration | Trap Configuration | **SNMPv3 Configuration** |

Context Table

| Context Name : | [   ] | Apply |

User Table

Current User Profiles : Remove

(none)

New User Profile : Add

User ID:	[ ]
Authentication Password:	[ ]
Privacy Password:	[ ]

Group Table

Current Group content : Remove

(none)

New Group Table: Add

| Security Name (User ID): | [   ] |
| Group Name: | [   ] |

Access Table

Current Access Tables : Remove

(none)

New Access Table : Add

Context Prefix:	[ ]
Group Name:	[ ]
Security Level:	○ NoAuthNoPriv. ○ AuthNoPriv. ○ AuthPriv.
Context Match Rule	○ Exact ○ Prefix
Read View Name:	[ ]
Write View Name:	[ ]
Notify View Name:	[ ]

MIBView Table

Current MIBTables : Remove

(none)

New MIBView Table : Add

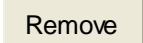| View Name: | [   ] |
| SubOid-Tree: | [   ] |
| Type: | ○ Excluded   ○ Included |

Help

Note:
Any modification of SNMPv3 tables might cause MIB accessing rejection. Please take notice of the causality between the tables before you modify these tables.
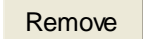
SNMP V3 configuration interface

Group Table

Configure SNMP v3 group table.

- **Security Name (User ID):** assign the user name that you have set up in user table.
- **Group Name:** set up the group name.
- Click Add to add context name.
- Click Remove to remove unwanted context name.

Access Table

Configure SNMP v3 access table.

- **Context Prefix:** set up the context name.
- **Group Name:** set up the group.
- **Security Level:** select the access level.
- **Context Match Rule:** select the context match rule.
- **Read View Name:** set up the read view.
- **Write View Name:** set up the write view.
- **Notify View Name:** set up the notify view.
- Click Add to add context name.
- Click Remove to remove unwanted context name.

MIBview Table

Configure MIB view table.

- **ViewName:** set up the name.
- **Sub-Oid Tree:** fill the Sub OID.
- **Type:** select the type – exclude or included.

- Click Add to add context name.

- Click Remove to remove unwanted context name.

QoS Configuration

You can configure Qos policy and priority setting, per port priority setting, COS and TOS setting.

QoS Policy and Priority Type

- **Qos Policy:** select the Qos policy rule.
  - ➢ **Using the 8,4,2,1 weight fair queue scheme:** The switch will follow 8:4:2:1 rate to process priority queue from High to lowest queue. For example: the system will process 80 % high queue traffic, 40 % middle queue traffic, 20 % low queue traffic, and 10 % lowest queue traffic at the same time. And the traffic in the Low Priority queue are not transmitted until all High, Medium, and Normal traffic are serviced.
  - ➢ **Use the strict priority scheme:** Always higher queue will be process first, except higher queue is empty.
- **Priority Type:** there are 5 priority type selections available. Disable means no priority type is selected.
- **Port-base:** the port priority will follow the **Port-base** that you have assigned – High, middle, low, or lowest.
  - ➢ **COS only:** the port priority will only follow the **COS priority** that you have assigned.
  - ➢ **TOS only:** the port priority will only follow the **TOS priority** that you have assigned.
  - ➢ **COS first:** the port priority will follow the COS priority first, and then other

priority rule.

➢ **TOS first:** the port priority will follow the TOS priority first, and the other priority rule.

■ Click Apply .

QoS Configuration interface

Port Base Priority

Configure per port priority level.

- **Port 1 ~ Port 8 & G1~G2:** each port has 4 priority levels – High, Middle, Low, and Lowest.
- Click Apply .

COS Configuration

Set up the COS priority level.

- **COS priority:** Set up the COS priority level 0~7 –High, Middle, Low, Lowest.
- Click Apply .

TOS Configuration

Set up the TOS priority.

- **TOS priority:** the system provides 0~63 TOS priority level. Each level has 4 types of priority – high, middle, low, and lowest. The default value is "Lowest" priority for each level. When the IP packet is received, the system will check the TOS level value in the IP packet that has received. For example, user set the TOS level 25 is high. The port 1 is following the TOS priority policy only. When the port 1 packet received, the system will check the TOS value of the received IP packet. If the TOS value of received IP packet is 25(priority = high), and then the packet priority will have highest priority.
- Click Apply .

IGMP Configuration

The Internet Group Management Protocol (IGMP) is an internal protocol of the Internet Protocol (IP) suite. IP manages multicast traffic by using switches, routers, and hosts that support IGMP. Enabling IGMP allows the ports to detect IGMP queries and report packets and manage IP multicast traffic through the switch. IGMP have three fundamental types of message as follows:

Message	Description
Query	A message sent from the querier (IGMP router or switch) asking for a response from each host belonging to the multicast group.
Report	A message sent by a host to the querier to indicate that the host wants to be or is a member of a given group indicated in the report message.
Leave Group	A message sent by a host to the querier to indicate that the host has quit being a member of a specific multicast group.

The switch support IP multicast, you can enable IGMP protocol on web management's switch setting advanced page, then display the IGMP snooping information. IP multicast addresses range from 224.0.0.0 through 239.255.255.255.

- **IGMP Protocol:** enable or disable the IGMP protocol.
- **IGMP Query:** enable or disable the IGMP query function. The IGMP query information will be display in IGMP status section.
- Click Apply .

IGMP Configuration

IP Address	VLAN ID	Member Port
239.255.255.250	1	***4******

IGMP Protocol: Enable

IGMP Query : Auto

Apply Help

IGMP Configuration interface

X-Ring

X-Ring provides a faster redundant recovery than Spanning Tree topology. The action is similar to STP or RSTP, but the algorithms not the same.

In the X-Ring topology, every switch should enable X-Ring function and assign two member ports in the ring. Only one switch in the X-Ring group would be set as a backup switch that would be blocked, called backup port, and another port is called working port. Other switches are called working switches and their two member ports are called working ports. When the failure of network connection occurs, the backup port will automatically become a working port to recovery the failure.

The switch supports the function and interface for setting the switch as the ring master or slave mode. The ring master can negotiate and place command to other switches in the X-Ring group. If there are 2 or more switches in master mode, then software will select the switch with lowest MAC address number as the ring master. The X-Ring master ring mode will be enabled by the X-Ring configuration interface. Also, user can identify the switch as the ring master from the R.M. LED panel of the LED panel on the switch.

The system also supports the coupling ring that can connect 2 or more X-Ring group for

the redundant backup function and dual homing function that prevent connection lose between X-Ring group and upper level/core switch.

- **Enable X-Ring:** To enable the X-Ring function. Marking the check box to enable the X-Ring function.
- **Enable Ring Master:** Mark the check box for enabling this machine to be a ring master.
- **1st & 2nd Ring Ports:** Pull down the selection menu to assign two ports as the member ports. **1st Ring Port** is the working port and **2nd Ring Port** is the backup port. When **1st Ring Port** fails, the system will automatically upgrade the **2nd Ring Port** to be the working port.
- **Enable Coupling Ring:** To enable the coupling ring function. Marking the check box to enable the coupling ring function.
- **Coupling port:** Assign the member port.
- **Control port:** Set the switch as the master switch in the coupling ring.
- **Enable Dual Homing:** Set up one of port on the switch to be the Dual Homing port. In an X-Ring group, maximum Dual Homing port is one. Dual Homing only work when the X-Ring function enable.
- And then, click Apply to apply the configuration.

X-Ring Interface

[NOTE]

1. When the X-Ring function enable, user must disable the RSTP. The X-Ring function and RSTP function cannot exist at the same time.

2. Remember to execute the "Save Configuration" action, otherwise the new configuration will lose when switch power off.

■ Security

In this section, you can configure 802.1x and MAC address table.

802.1X/Radius Configuration

802.1x is an IEEE authentication specification that allows a client to connect to a wireless access point or wired switch but prevents the client from gaining access to the Internet until it provides authority, like a user name and password that are verified by a separate server.

System Configuration

After enabling the IEEE 802.1X function, you can configure the parameters of this function.

1. **IEEE 802.1x Protocol:** .enable or disable 802.1x protocol.
2. **Radius Server IP:** set the Radius Server IP address.
3. **Server Port:** set the UDP destination port for authentication requests to the specified Radius Server.
4. **Accounting Port:** set the UDP destination port for accounting requests to the specified Radius Server.
5. **Shared Key:** set an encryption key for using during authentication sessions with the specified radius server. This key must match the encryption key used on the Radius

Server.

6. **NAS, Identifier:** set the identifier for the radius client.

7. Click Apply .

802.1x/Radius - System Configuration

| System Configuration | Port Configuration | Misc Configuration |

802.1x Protocol	Disable
Radius Server IP	0.0.0.0
Server Port	1812
Accounting Port	1813
Shared Key	12345678
NAS, Identifier	NAS_L2_SWITCH

Apply   Help

802.1x System Configuration interface

802.1x Per Port Configuration

You can configure 802.1x authentication state for each port. The State provides Disable, Accept, Reject and Authorize. Use "**Space**" key change the state value.

■ **Reject:** the specified port is required to be held in the unauthorized state.

■ **Accept:** the specified port is required to be held in the Authorized state.

■ **Authorized:** the specified port is set to the Authorized or Unauthorized state in accordance with the outcome of an authentication exchange between the Supplicant and the authentication server.

■ **Disable:** The specified port is required to be held in the Authorized state

■ Click Apply .

802.1x/Radius - Port Configuration

| System Configuration | **Port Configuration** | Misc Configuration |

Port	State
Port.01 Port.02 Port.03 Port.04 Port.05	Authorize

[Apply] [Help]

Port Authorization

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

802.1x Per Port Setting interface

Misc Configuration

1. **Quiet Period:** set the period during which the port doesn't try to acquire a supplicant.
2. **TX Period:** set the period the port wait for retransmit next EAPOL PDU during an authentication session.
3. **Supplicant Timeout:** set the period of time the switch waits for a supplicant response to an EAP request.
4. **Server Timeout:** set the period of time the switch waits for a server response to an authentication request.
5. **Max Requests:** set the number of authentication that must time-out before authentication fails and the authentication session ends.
6. **Reauth period:** set the period of time after which clients connected must be re-authenticated.

7. Click Apply .

802.1x/Radius - Misc Configuration

System Configuration	Port Configuration	**Misc Configuration**

Quiet Period	60
Tx Period	30
Supplicant Timeout	30
Server Timeout	30
Max Requests	2
Reauth Period	3600

Apply   Help

802.1x Misc Configuration interface

MAC Address Table

Use the MAC address table to ensure the port security.

Static MAC Address

You can add a static MAC address; it remains in the switch's address table, regardless of whether the device is physically connected to the switch. This saves the switch from having to re-learn a device's MAC address when the disconnected or powered-off device is active on the network again. You can add / modify / delete a static MAC address.

■ **Add the Static MAC Address**

You can add static MAC address in switch MAC table.

1. **MAC Address:** Enter the MAC address of the port that should permanently forward traffic, regardless of the device network activity.

2. **Port No.:** pull down the selection menu to select the port number.

3. Click Add .

4. If you want to delete the MAC address from filtering table, select the MAC address and click Delete .

MAC Address Table - Static MAC Addresses

Static MAC Addresses	MAC Filtering	All Mac Addresses

MAC Address		Port

MAC Address	
Port No.	Port.01 ∨

[Add] [Delete] [Help]

Static MAC Addresses interface

MAC Filtering

By filtering MAC address, the switch can easily filter pre-configure MAC address and reduce the un-safety. You can add and delete filtering MAC address.

MAC Address Table - MAC Filtering

Static MAC Addresses	**MAC Filtering**	All Mac Addresses

MAC Address

MAC Address [   ]

[Add] [Delete] [Help]
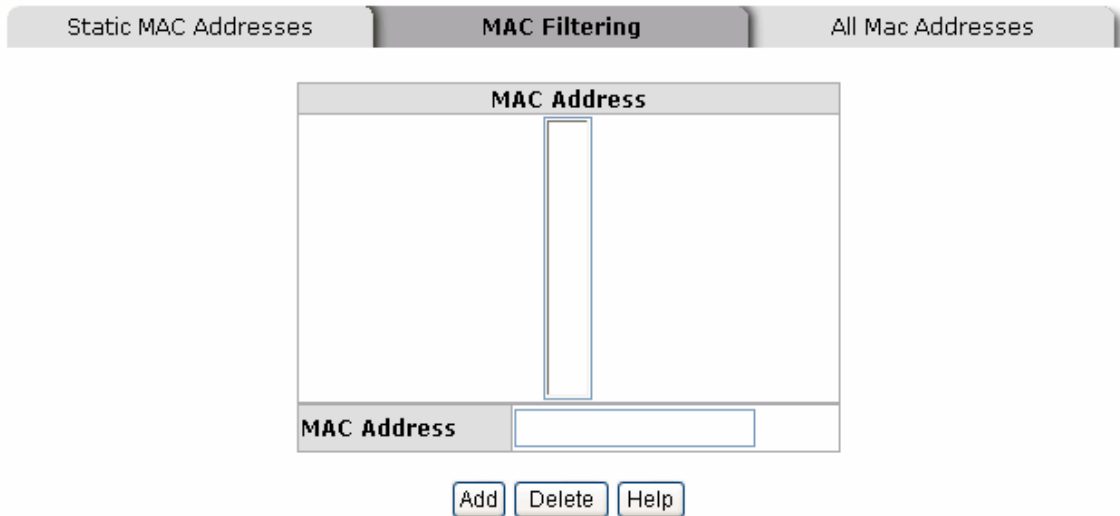
MAC Filtering interface

1. **MAC Address:** Enter the MAC address that you want to filter.

2. Click [Add] .

3. If you want to delete the MAC address from filtering table, select the MAC address and click [Delete] .

All MAC Addresses

You can view the port that connected device's MAC address and related devices' MAC address.

1. Select the port.

2. The selected port of static MAC address information will display.

3. Click [Clear MAC Table] to clear the current port static MAC address information on screen.

MAC Address Table - All Mac Addresses

Static MAC Addresses	MAC Filtering	**All Mac Addresses**

Port No: Port.01

Current MAC Address

Dynamic Address Count: 0
Static Address Count: 0

Clear MAC Table

All MAC Address interface

Factory Default

Reset switch to default configuration. Click Reset to reset all configurations to the default value.

Factory Default

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

Reset Help

Factory Default interface

Save Configuration

Save all configurations that you have made in the system. To ensure the all configuration

will be saved. Click [Save] to save the all configuration to the flash memory.

Save Configuration

[Save] [Help]

Save Configuration interface

System Reboot

Reboot the switch in software reset. Click [Reboot] to reboot the system.

System Reboot

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

[Reboot]

System Reboot interface

Troubleshooting

This section is intended to help solve the most common problems on the 8 10/100TX plus 1 10/100/1000T + 1 MINI GBIC Managed Switch.

Incorrect connections

The switch port can automatically detect straight or crossover cable when you link switch with other Ethernet device. For the RJ-45 connector should use correct UTP or STP cable, 10/100Mbps port use 2-pairs twisted cable and Gigabit 1000T port use 4 pairs twisted cable. If the RJ-45 connector is not correct pin on right position then the link will fail. For fiber connection, please notice that fiber cable mode and fiber module should be match.

■ Faulty or loose cables

Look for loose or obviously faulty connections. If they appear to be OK, make sure the connections are snug. If that does not correct the problem, try a different cable.

■ Non-standard cables

Non-standard and miss-wired cables may cause numerous network collisions and other network problem, and can seriously impair network performance. A category 5-cable tester is a recommended tool for every 100Base-T network installation.

RJ-45 ports: use unshielded twisted-pair (UTP) or shield twisted-pair (STP) cable for RJ-45 connections: 100Ω Category 3, 4 or 5 cable for 10Mbps connections or 100Ω Category 5 cable for 100Mbps connections. Also be sure that the length of any twisted-pair connection does not exceed 100 meters (328 feet). Gigabit port should use Cat-5 or cat-5e cable for 1000Mbps connections. The length does not exceed 100

meters.

■ **Improper Network Topologies**

It is important to make sure that you have a valid network topology. Common topology faults include excessive cable length and too many repeaters (hubs) between end nodes. In addition, you should make sure that your network topology contains no data path loops. Between any two ends nodes, there should be only one active cabling path at any time. Data path loops will cause broadcast storms that will severely impact your network performance.

Diagnosing LED Indicators

The switch can be easily monitored through panel indicators to assist in identifying problems, which describes common problems user may encounter and where user can find possible solutions.

If the power indicator does not light on when the power cord is plugged in, you may have a problem with power outlet, or power cord. However, if the Switch powers off after running for a while check for loose power connections, power losses or surges at power outlet. If the problem still cannot be resolved, please contact the local dealer for assistance.

Technical Specification

This section provides the specifications of 8 10/100TX plus 1 10/100/1000T + 1 MINI GBIC Managed Switch.

Standard	IEEE 802.3 10Base-T Ethernet IEEE 802.3u 100Base-TX IEEE802.3ab 1000Base-T IEEE802.3z Gigabit fiber IEEE802.3x Flow Control and Back Pressure IEEE802.3ad Port trunk with LACP IEEE802.1d Spanning Tree/ IEEE802.1w Rapid Spanning Tree IEEE802.1p Class of Service IEEE802.1Q VLAN Tag IEEE 802.1x User Authentication (Radius)
LED Indicators	System Power (Green) 10/100TX Port: Link/Activity (Green), Full-duplex/Collision (Yellow), 100Mbps(Green) Gigabit copper port: 1000/100Mbps (Green/Yellow), Link/Activity (Green), Full Duplex/Collision (Yellow) Mini GBIC: Link/Activity (Green)

Connector	10/100TX: 8 x ports RJ-45 with Auto MDI/MDI-X function 10/100/1000T: 1 x ports RJ-45 with Auto MDI/MDI-X function Gigabit fiber: 1 x Mini-GBIC RS-232 DB-9 Female connector for switch management
Switch architecture	Store and forward switch architecture System throughput up to 8.3Mpps
Back-plane	5.6Gbps
MAC address	8K MAC address table with Auto learning function
DRAM	32Mbytes
Packet Buffer	1Mbits for packet buffer
Power Supply	100~240VAC, 50/60Hz
Power Consumption	10.8 Watts(Maximum)
Ventilation	Fan free design
Operating environment	0℃~45℃, 5%~95%RH
Storage environment	-40℃~70℃, 95% RH

Dimensions	217mm(W) x 140mm(D) x 43mm(H)
EMI	FCC Class A, CE
Safety	UL cUL CE/EN60950-1

Appendix

Console Port Pin Assignments

The DB-9 serial port on the switch is used to connect to the switch for out-of-band console configuration. The console menu-driven configuration program can be accessed from a terminal or a PC running a terminal emulation program. The pin assignments used to connect to the serial port are provided in the following tables.
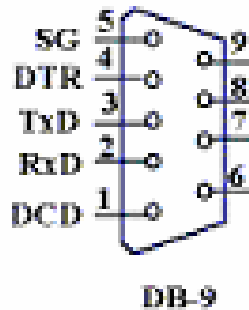
DB-9 Console Port Pin Numbers

■ **DB-9 Port Pin Assignments**

EIA Circuit	CCITT Signal	Description	Switch's DB9 DTE Pin #	PC DB9 DTE Pin #
BB	104	RxD (Received Data)	2	2
BA	103	TxD (Transmitted Data)	3	3
AB	102	SGND (Signal Ground)	5	5

■ **Console Port to 9-Pin DTE Port on PC**

Switch's 9-Pin Serial Port	CCITT Signal PC's 9-Pin	DTE Port
2 RXD	<---------RXD ------------	3 TxD
3 TXD	-----------TXD ---------->	2 RxD
5 SGND	-----------SGND ----------	5 SGND

Cables

The RJ-45 ports on the switch support automatic MDI/MDI-X operation, so you can use standard straight-through twisted-pair cables to connect to any other network device (PCs, servers, switches, routers, or hubs). Please refer to the following table for cable specifications.

■ **Cable Types and Specifications**

Cable	Type	Max. Length	Connector
10BASE-T	Cat. 3, 4, 5100-ohm	UTP 100 m (328 ft)	RJ-45
100BASE-TX	Cat. 5 100-ohm UTP	100 m (328 ft)	RJ-45
100BASE-FX	50/125 or 62.5/125 micron core multimode fiber (MMF)	2 km (1.24 miles)	SC or ST

Cable specification table

100BASE-TX/10BASE-T Pin Assignments

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

■ **RJ-45 Pin Assignments**

Pin Number	Assignment
1	Tx+
2	Tx-
3	Rx+
6	Rx-

[NOTE] "+" and "-" signs represent the polarity of the wires that make up each wire pair.

All ports on this switch support automatic MDI/MDI-X operation, you can use straight-through cables for all network connections to PCs or servers, or to other switches or hubs. In straight-through cable, pins 1, 2, 3, and 6, at one end of the cable, are connected straight through to pins 1, 2, 3 and 6 at the other end of the cable. The table below shows the 10BASE-T/ 100BASE-TX MDI and MDI-X port pin outs.

Pin MDI-X	Signal Name	MDI Signal Name
1	Receive Data plus (RD+)	Transmit Data plus (TD+)
2	Receive Data minus (RD-)	Transmit Data minus (TD-)
3	Transmit Data plus (TD+)	Receive Data plus (RD+)
6	Transmit Data minus (TD-)	Receive Data minus (RD-)