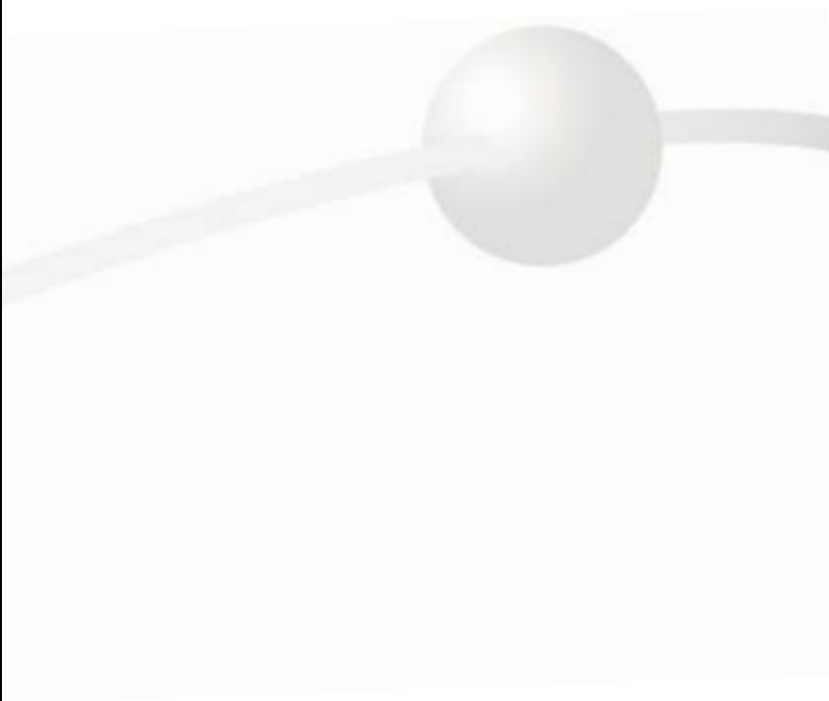


Management Switch

Enable-IT 8824 Managed Fast Gigabit Switch

Users Manual



FCC COMPLIANCE STATEMENT

This equipment has been tested and found to comply with the limits of a Class A computing devices, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference. 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.

If you suspect this product is causing interference, turn your computer on and off while your radio or TV is showing interference. If the interference disappears then when you turn the computer off and reappears when you turn the computer on, something in the computer is causing interference.

You can try to correct the interference by one or more of the following measures:

1. Reorient/relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Connect the equipment into an outlet on a circuit difference from that to which the receiver is connected.
4. Ensure that all expansion slots (on the back or side of the computer) are covered. Also ensure that all metal retaining brackets are tightly attached to the computer.

Content

Chapter1 Introduction

1. Introduction	6
2. Features & Specifications	8
3. Package Contents.....	10
4. Hardware Description	11

Chapter 2 Web Management Function

1. Web Management Overview.....	13
2. Port Status	15
3. Port Statistics	17
4. Administrator	18
4.1 IP Address	18
4.2 Switch Settings	19
4.3 Console Port Information.....	22
4.4 Port Controls	23
4.5 Trunking	25
4.6 Filter Database	28
4.7 VLAN configuration	31
4.8 Spanning Tree.....	36
4.9 Port Sniffer	38
4.10 SNMP	39
4.11 Security Manager	41

4.12	802.1X Configuration	42
4.13	TFTP Update Firmware	45
4.14	Configuration Backup	46
4.15	Reset System	47
4.16	Reboot	48

Chapter 3 Console-Menu Line

1. Main Menu	50
2. Switch Static Configuration.....	51
2.1 Port Configuration.....	52
2.2 Trunk Configuration.....	54
2.3 VLAN Configuration	55
2.4 Misc Configuration	61
2.5 Administration Configuration	65
2.6 Port Mirroring Configuration	68
2.7 Priority Configuration.....	69
2.8 MAC Address Configuration	70
3. Protocol Related Configuration	72
3.1 STP	72
3.2 SNMP	75
3.3 GVRP	80
3.4 IGMP.....	81
3.5 LACP.....	83
3.6 802.1X.....	86
4. Status and Counters	89

4.1 Port Status.....	90
4.2 Port Counters	91
4.3 System Information	92
5. Reboot Switch	93
5.1 Default.....	93
5.2 Restart	93
6. TFTP Update Firmware.....	94
6.1 TFTP Update Firmware	94
6.2 Update Configure File	95
6.3 Upload Configure File	97

Chapter 1 Introduction

1. Introduction

Congratulations on your purchase of this Fast/Gigabit Ethernet Management Switch. This high performance management switch provides Ethernet ports to segment network traffics, extend Ethernet connection distance, and convert data packets between different transmission speeds.

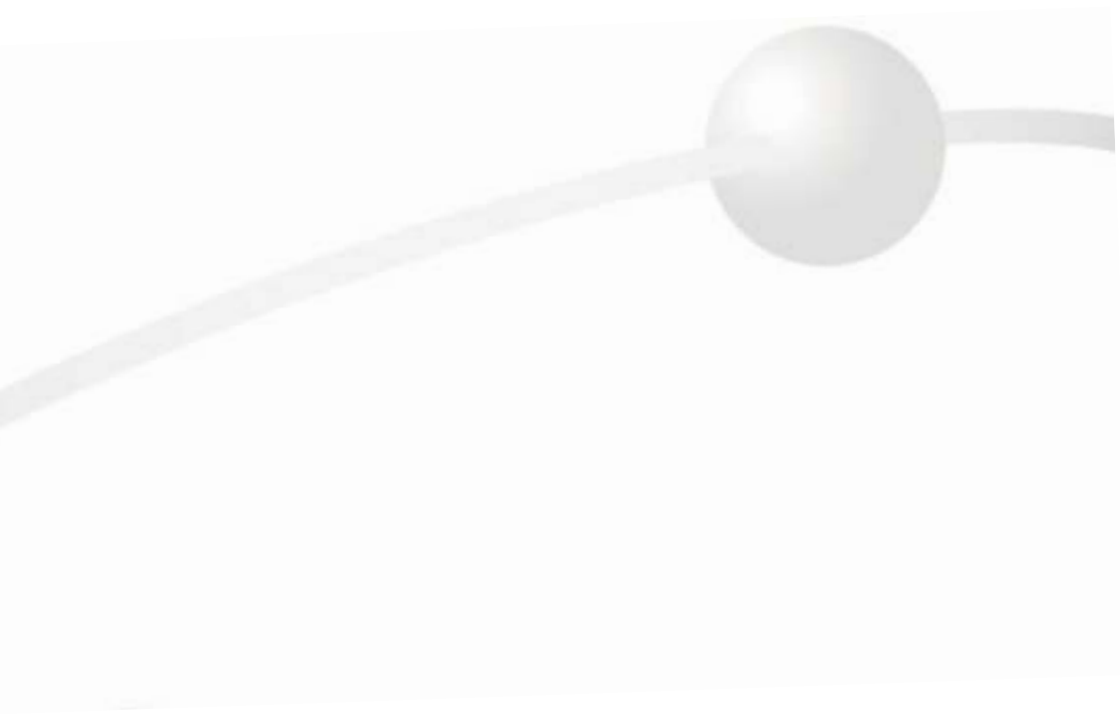
This switch utilizes stored-and-forward switching architecture that filters and forwards data after the complete data packet is received and examined to be free of errors. With one set of status LEDs for each individual port, the switch operation status can be easily monitored.

All the Fast Ethernet ports support both **Full and Half duplex mode** which are able to provide up to 200Mbps(2000Mbps for Gigabit Ports) of bandwidth to the connected devices, with **auto-negotiation** providing the capability to connect to **100/10Mbps**(1000/100/10Mbps for Gigabit ports) network devices. It also supports backpressure and **IEEE 802.3x advanced flow control** capabilities that can reduce congestion and prevent packet loss.

And it offers advance features:

- **SNMP/Web-based Management:** Provides a web browser to manage and monitor the switch.
- **Bandwidth Control:** Input and output rate control.
- **VLAN:** Port-based and Tag-based VLAN allow you to set virtual LANs within your network
- **Trunking:** Reduce the bottleneck between switches
- **QoS:** Two priority queues per port allow you to define which port has higher priority.
- **802.1X:** This switch supports port-based authentication protocol, IEEE 802.1X.

In addition, all the ports support the **MDI/MDI-X** auto-detect function. That is to say, you can connect any device (including PC, Switch, Hub) to a port of this switch using a regular cable. The RJ-45 port will auto-detect and auto-switch to the correct MDI/MDI-X mode (do not need to use a specific uplink port or cross-over cable).



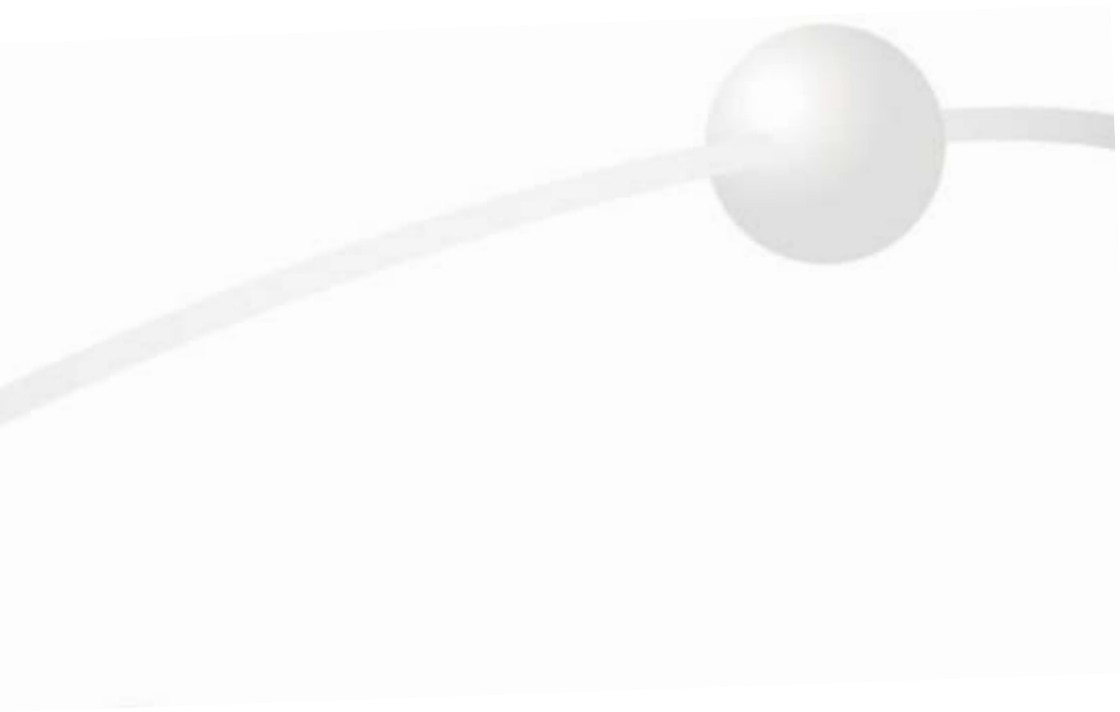
2. Features & Specifications

Features

- Complies with the IEEE802.3 Ethernet, IEEE802.3u Fast Ethernet (IEEE802.3z, IEEE802.3ab for Gigabit switch)
- Provides Store-and-Forward architecture and full wire speed filtering and forwarding rates
- 10/100Mbps Ports support full/half duplex modes and auto-negotiation
- Provides two Fast Ethernet Modules option (Fast/Gigabit Ethernet Management Switch):
 - ◆ 100/10Mbps UTP connector (RJ-45)
 - ◆ 100Mbps Fiber SC/ST connector (multi/single mode)
- Provides two Gigabit Ethernet Modules option (Gigabit Ethernet Management Switch only):
 - ◆ 1000/100/10Mbps UTP connector (RJ-45)
 - ◆ 1000Mbps Fiber SC connector (multi/single mode)
- Supports flow control: back pressure for half-duplex mode, IEEE 802.3x for full-duplex mode
- Supports SNMP, Web-based, Telnet and Console Management
- MIB: MIB

Specifications

- **Standards:** IEEE802.3, IEEE802.3u, IEEE802.3z, IEEE802.3ab, IEEE802.1Q, IEEE802.1p
- **10/100Mbps Ports:** RJ-45



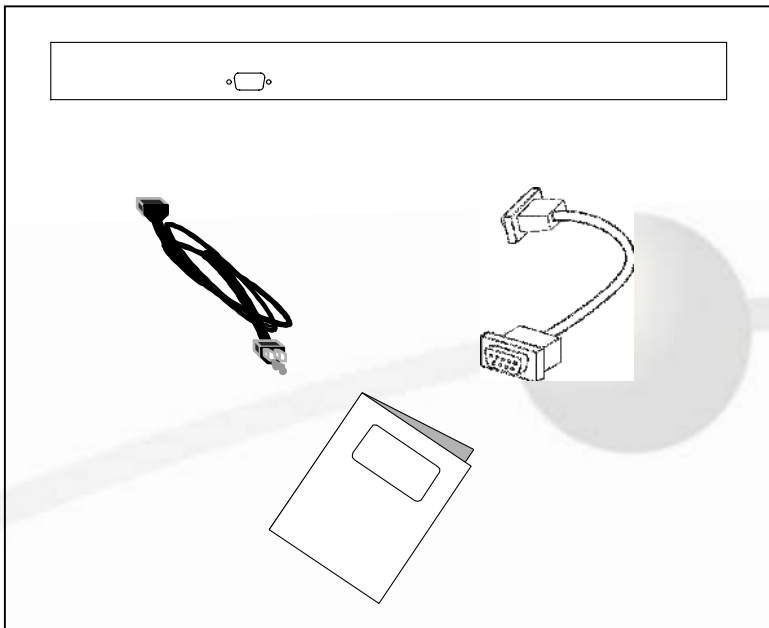
3. Package Contents

Packing list

Check the contents of your package for following parts:

- One Fast/Gigabit Ethernet Management Switch
- One User's manual
- One Power cord
- One RS-232 Cable

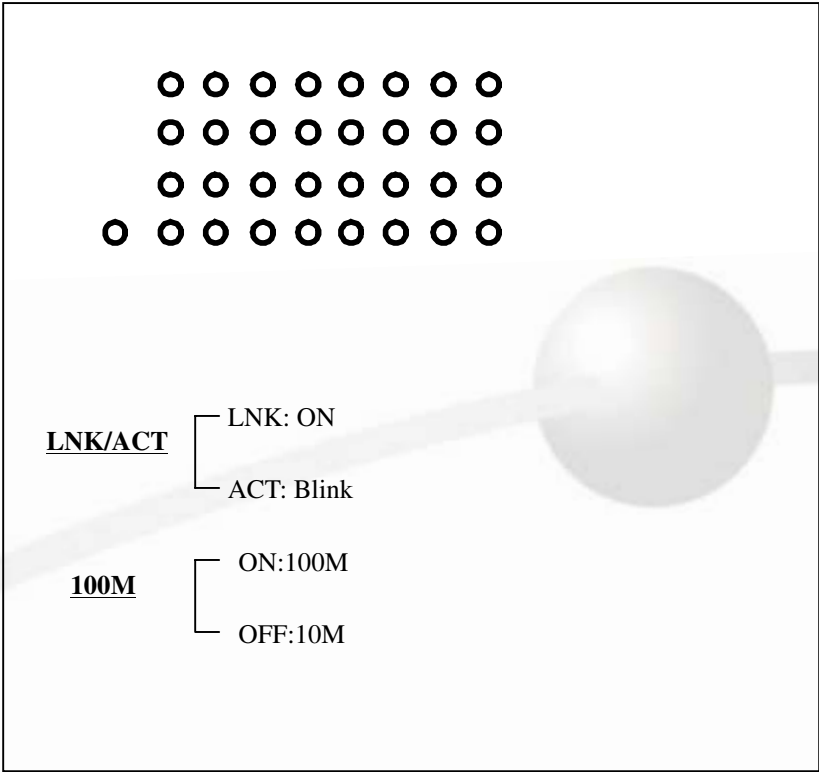
If any of the items are missing or damaged, please contact your local dealer.



4. Hardware Description

This section describes the hardware features of this Fast/Gigabit Ethernet Management Switch. For easier management and control of the switch, familiarize yourself with its display indicators and ports. All LEDs are located on the front panel of the switch. They serve the purpose of monitoring the operation and performance of the switch at a glance.

- LED indicators



Operating Environment

This management switch must be installed and operated within the limits of the specified operating temperature and humidity (see previous section on Specifications). Do not place objects on top of the unit or obstruct any vents at the sides of the unit. Do not position the unit near any heating source such as heaters, radiators, or direct exposure to sun. Do not expose the unit to water and or moisture. If necessary, use a dehumidifier to reduce humidity.

Connecting to network devices

1. All ports of this switch support the Auto-MDI/MDI-X function. That is to say, you can connect any device (including PC, Switch, Hub) to a port of this switch using a regular cable. The RJ-45 port will auto-detect and auto-switch to the correct MDI/MDI-X mode. (do not need to connect to a specific uplink port or cross-over cable)
2. Connect one end of the network cable to the RJ-45 port on the front panel, and connect the other end of the network cable to the RJ-45 port on the network device. Follow the same procedure to connect all the RJ-45 ports of the switch. Maximum length, using UTP cable, between the switch and connected device is 100 meters (300ft). Once the network cable is connected to both ends and the attached network device is powered on, the LNK/ACT LED should be lit.
3. Make sure the wiring is correct. You need to use Category 3/4/5 cable for 10Mbps operation or Category 5 cable for 100Mbps connections.

Connecting the power

Plug the power cable into the internal three-pronged power plug. Connect it to an electrical outlet then turn on the switch.

Chapter 2 Web Management Function

1. Web Management Overview

This switch provides a web browser to manage and monitor. The default values are as follows:

IP Address: 192.168.223.100
Subnet Mask: 255.255.248.0
Default Gateway: 192.168.223.254
User Name: admin
Password: 123

You can browse <http://192.168.223.100>, type user name and password as below.



Enter Network Password

Please type your user name and password.

Site: 192.168.223.100

Realm: index.htm

User Name: admin

Password: 123

☐ Save this password in your password list

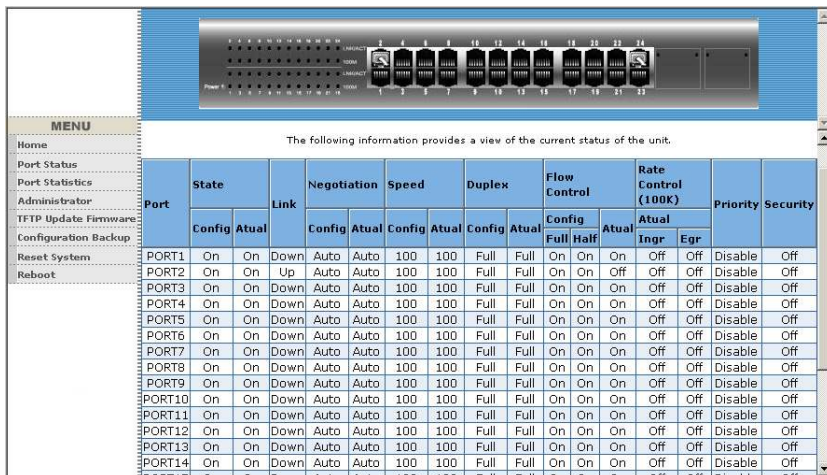
OK Cancel

After type in the correct username and password, you can see the homepage as follows:



2. Port Status

Click the port status icon on the menu column you will see the port status page. In this page, you can see the status of each port that depended on user's settings and the negotiation results.



The following information provides a view of the current status of the unit.

Port	State		Link	Negotiation		Speed		Duplex		Flow Control			Rate Control (100K)			Priority	Security
	Config	Actual		Config	Actual	Config	Actual	Config	Actual	Config	Full	Half	Actual	Ingr	Egr		
PORT1	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	
PORT2	On	On	Up	Auto	Auto	100	100	Full	Full	On	On	Off	Off	Off	Disable	Off	
PORT3	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	
PORT4	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	
PORT5	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	
PORT6	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	
PORT7	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	
PORT8	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	
PORT9	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	
PORT10	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	
PORT11	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	
PORT12	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	
PORT13	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	
PORT14	On	On	Down	Auto	Auto	100	100	Full	Full	On	On	On	Off	Off	Disable	Off	

1. State: Displays the status of each port (“on” means enable and “off” means disable). “Unlink” will be treated as “off”.

2. Link Status: “Down” and “Up” means “No Link” and “Link” respectively.

3. Negotiation: Displays the auto negotiation modes: auto, force and nway-force.

4. Speed status: Displays the speed of each port:

Port 1- 24 are 10/100Mbps

Port 25-26 are 10/100/1000Mbps(Gigabit Ethernet Switch)
10/100Mbps(Fast Ethernet Switch)

5. Duplex status: Displays the port is full-duplex mode or half-duplex mode.

6. Flow Control:

Full: Displays the flow control status is enable or disable in full duplex mode.

Half: Displays the backpressure is enable or disable in half duplex mode.

7. Rate Control: Displays the rate control settings.

Ingr: Displays the port's effective ingress rate of user settings.

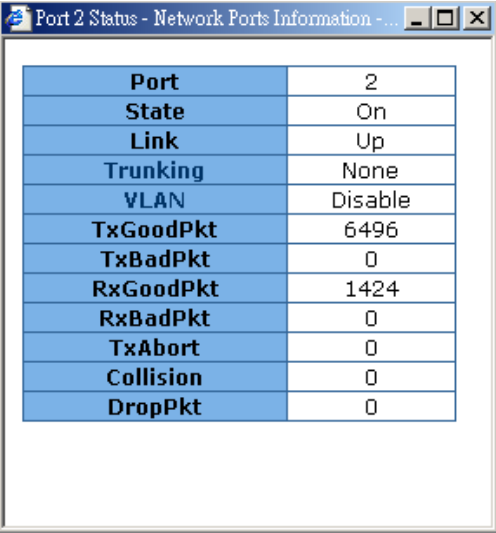
Egr: Displays the port's effective egress rate of user settings.

8. Port Security: Shows the port security is enabled or disabled.

9. Config: Displays the state of user's settings.

10. Atual: Displays the negotiation results.

You can see a single port counter by clicking on each port as following.



Port	2
State	On
Link	Up
Trunking	None
VLAN	Disable
TxGoodPkt	6496
TxBadPkt	0
RxGoodPkt	1424
RxBadPkt	0
TxAbort	0
Collision	0
DropPkt	0

3. Port Statistics

The following information provides a view of the current status of the switch. Press “Reset” button to clean all count.

MENU

Home

Port Status

Port Statistics

Administrator

TFTP Update Firmware

Configuration Backup

Reset System

Reboot

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24

Power 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24

Port Statistics

The following information provides a view of the current status of the unit.

Port	State	Link	TxGoodPkt	TxBadPkt	RxGoodPkt	RxBadPkt	TxAbort	Collision	DropPkt
PORT1	On	Down	0	0	0	0	0	0	0
PORT2	On	Up	8	0	4	0	0	0	0
PORT3	On	Down	0	0	0	0	0	0	0
PORT4	On	Down	0	0	0	0	0	0	0
PORT5	On	Down	0	0	0	0	0	0	0
PORT6	On	Down	0	0	0	0	0	0	0
PORT7	On	Down	0	0	0	0	0	0	0
PORT8	On	Down	0	0	0	0	0	0	0
PORT9	On	Down	0	0	0	0	0	0	0

Reset

4. Administrator

This management switch provides advance features, which offers you more flexibility in setting up your network. The following sections explain how to set up the IP address, Switch settings, Console port information, Port controls, Trunk configuration, Filter database, VLAN configuration, Spanning tree, Port Sniffer, SNMP management, Security Manager, TFTP Update Firmware, Configuration Backup, Reset system and Reboot etc.

4-1 IP Address

You can configure the IP Settings and fill in the new values, than click “Apply” button. You must restart the switch then use new IP address to browse this web management.

MENU

- Home
- Port Status
- Port Statistics
- Administrator
 - IP Address
 - Switch Settings
 - Console Port Info
 - Port Controls
 - Trunking
 - Filter Database
 - VLAN Configuration
 - Spanning Tree
 - Port Sniffer
 - SNMP
 - Security Manager
 - 802.1x Configuration
- TFTP Update Firmware
- Configuration Backup
- Reset System
- Reboot

Set IP Addresses

DHCP:

IP Address	<input type="text" value="192.168.223.100"/>
Subnet_Mask	<input type="text" value="255.255.240.0"/>
Gateway	<input type="text" value="192.168.223.254"/>

4.2 Switch Settings

4.2.1 Basic

Description: Displays the name of this management switch.

MAC Address: The unique hardware address is assigned by manufacturer (default).

Firmware Version: Displays the switch's firmware version.

ASIC Version: Displays the switch's Hardware version.

PCBA version: Displays the switch's PCBA version.

Serial number: The serial number is assigned by manufacturer.

Switch Settings

Basic	Module Info	Advanced												
<table><tr><td>Description</td><td>Intelligent 24+2 Switch</td></tr><tr><td>MAC Address</td><td>004063809988</td></tr><tr><td>Firmware version</td><td>v2.3</td></tr><tr><td>ASIC version</td><td>A07.00</td></tr><tr><td>PCBA version</td><td>v01.00</td></tr><tr><td>Serial number</td><td></td></tr></table>			Description	Intelligent 24+2 Switch	MAC Address	004063809988	Firmware version	v2.3	ASIC version	A07.00	PCBA version	v01.00	Serial number	
Description	Intelligent 24+2 Switch													
MAC Address	004063809988													
Firmware version	v2.3													
ASIC version	A07.00													
PCBA version	v01.00													
Serial number														

4.2.2 Module Info

Displays the module card informations.

Switch Settings

Basic	Module Info	Advanced									
<table><tr><th></th><th>TYPE</th><th>DESCRIPTION</th></tr><tr><td>Module1</td><td>NC</td><td>N/A</td></tr><tr><td>Module2</td><td>NC</td><td>N/A</td></tr></table>				TYPE	DESCRIPTION	Module1	NC	N/A	Module2	NC	N/A
	TYPE	DESCRIPTION									
Module1	NC	N/A									
Module2	NC	N/A									

Note:

The module type will be 100/10Mbps for Fast Ethernet Management Switch (1000/100/10Mbps for Gigabit Switch).

4.2.3 Advanced

Miscellaneous Settings:

MAC Address Age-out Time: Type the number of seconds that an inactive MAC address remains in the switch's address table. The valid range is 300~765 seconds. Default is 300 seconds.

Max bridge transit delay bound control: Limit the packets queuing time in switch. If enable, the packets queued exceed the time will be dropped. This valid value are 1sec, 2 sec, 4 sec and off. Default is 1 second.

Broadcast Storm Filter Mode: To configure broadcast storm control, enable it and set the upper threshold for individual ports. The threshold is the percentage of the port's total bandwidth used by broadcast traffic. When broadcast traffic for a port rises above the threshold you set, broadcast storm control becomes active. The valid threshold value are 5%, 10%, 15%, 20%, 25% and off.

Switch Settings



Basic

Module Info

Advanced

Enter the settings, then click Submit to apply the changes on this page.

☒ MAC Table Address Entry

Age-Out Time: seconds (300~765, must multiple of 3)

Max bridge transmit delay bound control:

☐ Enable Low Queue Delay Bound ----- Max Delay Time: (1~255, 2ms/unit)

Broadcast Storm Filter Mode:

Priority Queue Service settings:

First Come First Service: The sequence of packets sent is depend on arrive order.

All High before Low: The high priority packets sent before low priority packets.

WRR: Weighted Round Robin. Select the preference given to packets in the switch's high-priority queue. These options represent the number of high priority packets sent before one low priority packet is sent. For example, 2 High : 1 Low means

that the switch sends 2 high priority packets before sending 1 low priority packet.

Qos Policy: High Priority Levels, 0~7 priority levels, can map to high or low queue.

Collisions Retry Forever: Enable it or just disable this function.

802.1X Protocol: IEEE 802.1X is port-based authentication protocol. You can enable it to control users' access to the internet.

Priority Queue Service:

802.1p Priority
☒ First Come First Service
☐ All High before Low
☐ WRR ----- High weight: Low weight:

Qos Policy: High Priority Levels
☐ Level0 ☐ Level1 ☐ Level2 ☐ Level3 ☒ Level4 ☒ Level5 ☒ Level6 ☒ Level7

Collisions Retry Forever : ▼

802.1x Protocol : ▼

4.3 Console Port Information

Console is a standard UART interface to communicate with Serial Port. You can use windows HyperTerminal program to link the switch. Connect To->Configure

Bits per second: 9600

Data bits: 8

Parity: none

Stop Bits: 1

Flow control: none

Console Information



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

Help

4.4 Port Controls

Port Controls

Port	State	Negotiation	Speed	Duplex	Flow Control		Rate Control (100K)		Priority	Security
					Full	Half	Ingress	Egress		
PORT1										
PORT2	Enable	Auto	100	Full	Enable	Enable	0	0	Disable	<input type="checkbox"/>
PORT3										
PORT4										

Apply

You can change the status of each port in this page.

1.State: You can enable or disable this port.

2.Auto Negotiation: You can set auto negotiation mode as Auto, Nway (specify the speed/duplex on this port and enable auto-negotiation) or Force of each port.

3.Speed: You can set 100 or 10Mbps speed on Port1~Port24. And set 1000/100/10Mbps on Port25~Port26 (Gigabit Ethernet switch) or 100/10Mbps on Port25~Port26 (Fast Ethernet switch).

4.Duplex: You can set each port as full-duplex or half-duplex mode.

5.Flow control:

Full: You can set flow control function is enable or disable in full duplex mode.

Half: You can set backpressure is enable or disable in half duplex mode.

6.Rate Control: This switch, port1 ~ port 24, supports by-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. This switch will perform flow control or backpressure to confine the ingress rate to meet the specified rate.

Ingress: Type the port effective ingress rate. The valid range is 0 ~ 1000. The unit is 100K

0: disable rate control

1 ~ 1000: valid rate value

Egress: Type the port effective egress rate. The valid range is 0~1000. The unit is 100K.

0: disable rate control

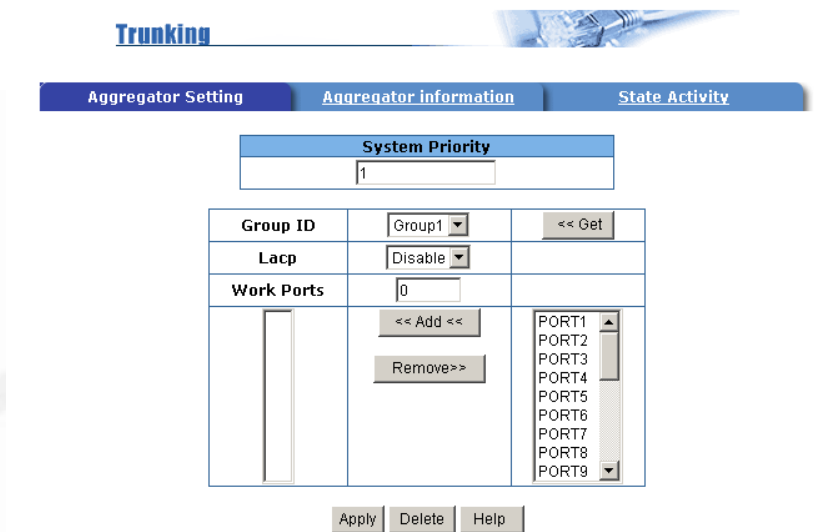
1 ~ 1000: valid rate value.

7.Port Security: A port in security mode will be “locked” without permission of address learning. Only the incoming packets with SMAC already existing in the address table can be forwarded normally. You can disable the port from learning any new MAC addresses then use the static MAC addresses screen to define a list of MAC addresses that can use the secure port. Enter the settings, then click Apply button to changes on this page.

4.5 Trunking

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. In conclusion, Link aggregation lets you group up to eight consecutive ports into a single dedicated connection. 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.

4.5.1 Aggregator setting



The image shows a network configuration interface for trunking. At the top, there is a blue header bar with three tabs: "Aggregator Setting", "Aggregator information", and "State Activity". The "Aggregator Setting" tab is selected. Below the tabs, there is a "System Priority" section with a text box containing the value "1". Below this, there is a table with three columns. The first column is "Group ID" with a dropdown menu showing "Group1". The second column is "Lacp" with a dropdown menu showing "Disable". The third column is "Work Ports" with a text box containing "0". Below the table, there are buttons for "<< Add <<", "Remove>>", and a list of ports from PORT1 to PORT9. At the bottom, there are buttons for "Apply", "Delete", and "Help".

System Priority		
1		

Group ID	Lacp	Work Ports
Group1	Disable	0

<< Add << Remove>>

PORT1
PORT2
PORT3
PORT4
PORT5
PORT6
PORT7
PORT8
PORT9

Apply Delete Help

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.

1.Group ID: There are seven trunk groups to provided configure. Choose the "group id" and click "Get".

2.LACP: If enable, the group is LACP static trunking group. If

disable, the group is local static trunking group.

All ports support LACP dynamic trunking group. If connecting to the device that also supports LACP, the LACP dynamic trunking group will be created automatically.

3. Work ports: Allow max four ports can be aggregated at the same time. If LACP static trunking group, the exceed ports is standby and able to aggregate if work ports fail. If local static trunking group, the number must be as same as the group member ports.

4 Select the ports to join the trunking group. Allow max four ports can be aggregated at the same time.

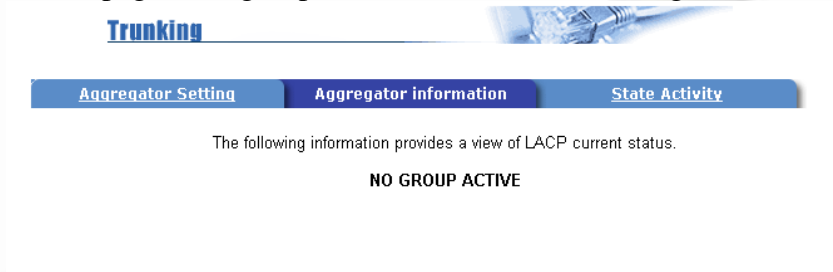
5. If LACP enable, you can configure LACP Active/Passive status in each ports on State Activity page.

6. Click Apply.

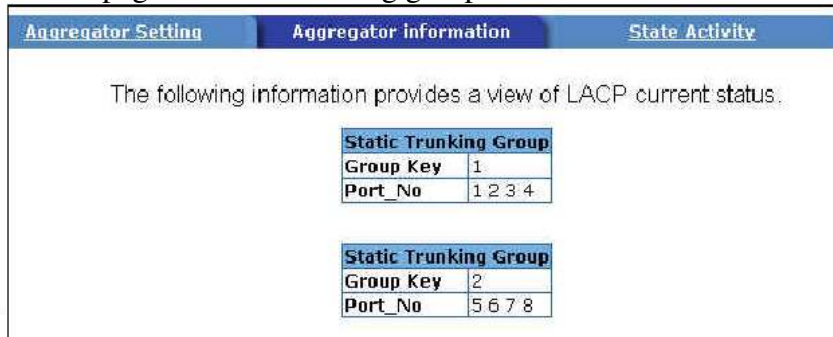
4.5.2 Aggregator Information

When you are setting LACP aggregator, you can see relation information here.

1. This page is no group active. LACP don't working.



2. This page is Static Trunking group.



4.5.3 State Activity

Active (selected): The port automatically sends LACP protocol packets.

Passive (not selected): The port does not automatically sends LACP protocol packets, and responds only if it receives LACP protocol packets from the opposite device.

- 1. A link having either two active LACP ports or one active port can perform dynamic LACP trunking. A link has two passive LACP ports will not perform dynamic LACP trunking because both ports are waiting for LACP protocol packets from the opposite device.
- 2. If you are active LACP actor, when you select trunking port, the active status will be created automatically.

Trunking



Aggregator Setting

Aggregator information

State Activity

Port	LACP State Activity	Port	LACP State Activity
1	<input checked="" type="checkbox"/> Active	2	<input checked="" type="checkbox"/> Active
3	<input checked="" type="checkbox"/> Active	4	<input checked="" type="checkbox"/> Active
5	N/A	6	N/A
7	N/A	8	N/A
9	N/A	10	N/A
11	N/A	12	N/A
13	N/A	14	N/A
15	N/A	16	N/A
17	N/A	18	N/A
19	N/A	20	N/A
21	N/A	22	N/A
23	N/A	24	N/A
25	N/A	26	N/A

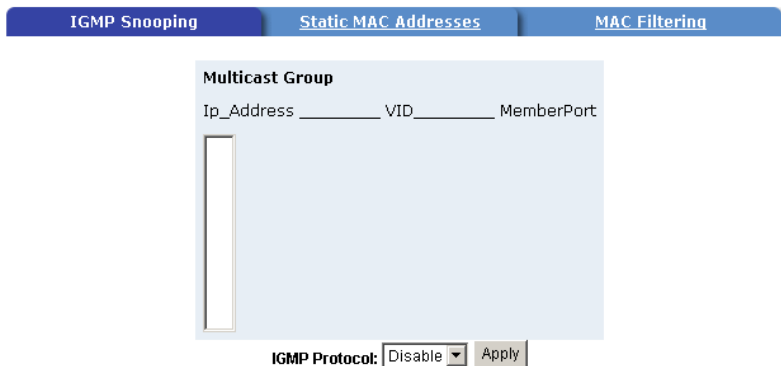
Apply

Help

4.6 Filter Database

4.6.1 IGMP Snooping

Forwarding and Filtering



IGMP Snooping Static MAC Addresses MAC Filtering

Multicast Group

Ip_Address _____ VID _____ MemberPort

IGMP Protocol: Disable ▾ Apply

This switch supports IP multicast, you can enable IGMP protocol on web management's switch settings advanced page, then display the IGMP snooping information in this page, you can view difference multicast group ,VID and member port here, IP multicast addresses range from 224.0.0.0 through 239.255.255.255.

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.

4.6.2 Static MAC Address

When you add a static MAC address, it remains in the switch's address table, regardless of whether the device is physically connected to the switch or not. 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.



Static addresses currently defined on the switch are listed below.
Click Add to add a new static entry to the address table.

MAC Address _____ PORT _____ VID _____

Mac Address

Port num

Vlan ID

Steps to add Static MAC Address:

1. From the main menu, click administrator->Filter Database ->Static MAC Address.
2. In the MAC address box, enter the MAC address to and from which the port should permanently forward traffic, regardless of the device's network activity.
4. In the Port Number box, enter a port number.
5. If tag-based (IEEE 802.1Q) VLANs are set up on the switch, static addresses are associated with individual VLANs. Type the VID (tag-based VLANs) to associate with the MAC address.
6. Click add.

Mac Address

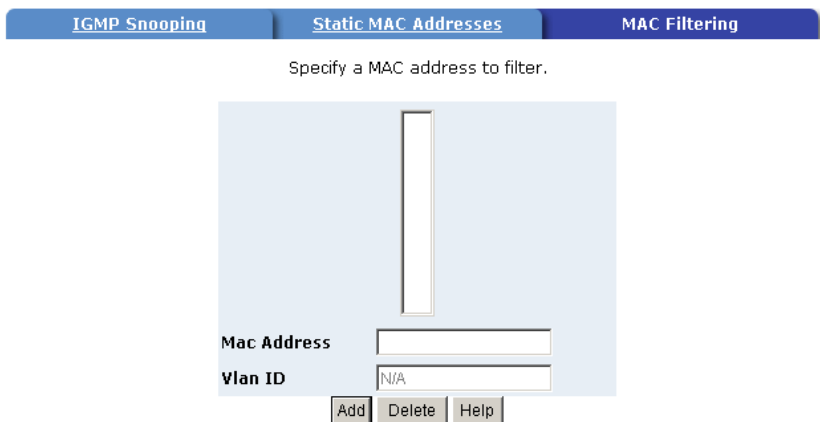
Port num

Vlan ID

4.6.3 MAC Filtering

MAC address filtering allows the switch to drop unwanted traffic. Traffic is filtered based on the destination addresses.

Forwarding and Filtering



Specify a MAC address to filter.

Mac Address

Vlan ID N/A

Add Delete Help

Steps to specify a MAC address to filter:

1. In the MAC Address box, enter the MAC address that wants to filter.
2. If tag-based (802.1Q) VLAN are set up on the switch, in the VLAN ID box, type the VID to associate with the MAC address.
3. Click the Add.
4. Choose the MAC address that you want to delete and then click the Delete can delete it.

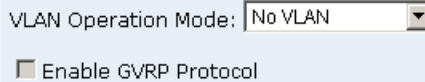
4.7 VLAN Configuration

A Virtual LAN (VLAN) is a logical network group that limits the broadcast domain. It allows you to isolate network traffic so only members of the VLAN receive traffic from the same VLAN members. 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 plug into the same switch physically.

This switch supports both port-based and 802.1Q (tagged-based) VLAN in web management page.

In the default configuration, VLAN support is disabled.

VLAN Configuration



VLAN Operation Mode:

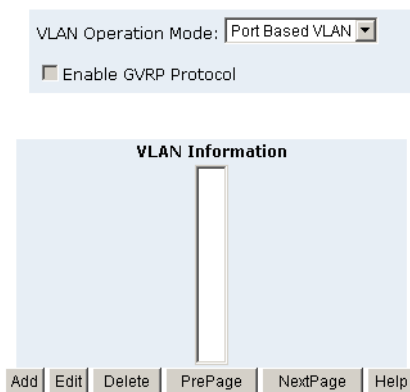
☐ Enable GVRP Protocol

VLAN NOT ENABLE

NOTE: You have to reboot the switch for valid value every time you change the VLAN mode.

4.7.1 Port-based VLAN

VLAN Configuration



The image shows a web-based configuration interface for VLANs. At the top, there is a section titled 'VLAN Configuration' with a background image of a network cable. Below this, there is a 'VLAN Operation Mode' dropdown menu set to 'Port Based VLAN'. Below the dropdown is a checkbox labeled 'Enable GVRP Protocol' which is currently unchecked. In the center, there is a large light blue box titled 'VLAN Information' containing a vertical list box. At the bottom of the interface, there is a row of buttons: 'Add', 'Edit', 'Delete', 'PrePage', 'NextPage', and 'Help'.

Steps to create a new VLAN group based on port-based VLAN:

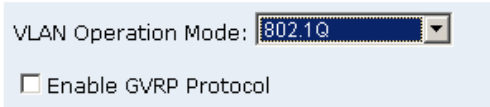
1. Click Add to create a new VLAN group.
2. Enter the VLAN name, group ID and select the members for the new VLAN.
3. Click Apply.
4. If there are many groups that over the limit of one page, you can click the “NextPage” to view other VLAN groups.

NOTE: If the trunk group exists, you can see it (ex: TRK1, TRK2...) in select menu of ports, and you can configure it as the member of the VLAN or not.

4.7.2 802.1Q VLAN

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

VLAN Configuration



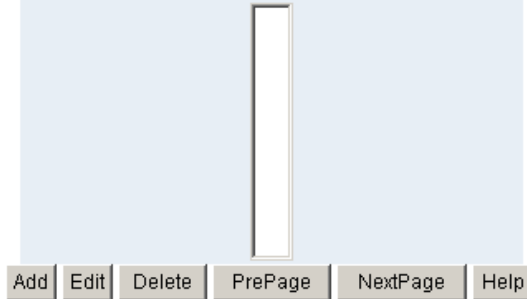
VLAN Operation Mode: 802.1Q

☐ Enable GVRP Protocol

Basic

Port VID

VLAN Information



VID

Add Edit Delete PrePage NextPage Help

GVRP (GARP [Generic Attribute Registration Protocol] VLAN Registration Protocol) 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, then it will automatically add that device to the existing VLAN.

- Basic

Create a VLAN and add tagged member ports to it.

1. From the main menu, click administrator-> VLAN configuration, click Add then you will see the page as follow.

The screenshot shows the 'Basic' configuration tab for a new VLAN. The 'VLAN Name' field is empty. The 'VID' field contains the number '1'. The 'Protocol Vlan' dropdown menu is set to 'NONE'. A list of ports (PORT1 through PORT12) is shown on the left, with an 'Add >>' button to its right. Below the port list is a '<< Remove' button. At the bottom of the form are 'Next' and 'Help' buttons.

2. Type a name for the new VLAN.
3. Type a VID (between 2-4094). The default is 1.
4. Choose the protocol type.
5. From the Available ports box, select ports to add to the VLAN and click “Add >>”. If the trunk group exists, you can see it here (ex: TRK1,TRK2...), and you can configure it as the member of the VLAN or not.
6. Click Next. Then you can view the page as follow.

The screenshot shows the 'Tag Member' configuration tab. The 'VLAN Name' is 'v1' and the 'VLAN ID' is '2'. Below this is a table for configuring member ports:

Tag Member	
PORT1	Tag
PORT2	Tag
PORT3	Tag

An 'Apply' button is located at the bottom of the form.

7. Use this page to set the outgoing frames as VLAN-Tagged frames or no. Then click Apply.
 Tag: outgoing frames with VLAN-Tagged.
 Untag: outgoing frames without VLAN-Tagged.

- Port VID

Configure port VID settings

From the main Tag-based (IEEE 802.1Q) VLAN page, click Port VID Settings.

Basic		Port VID	
Assign a Port VLAN ID (1~255) for untagged traffic on each port, then click Submit to apply the changes on this page.			
Ingress Filtering Rule 1 (Forward only packets with VID matching this port's configured VID)			
Ingress Filtering Rule 2 (Drop Untagged Frame)			
NO	PVID	Ingress Filtering 1	Ingress Filtering 2
PORT1	1	Enable	Disable
PORT2			
PORT3			
PORT4			
<input type="button" value="Apply"/> <input type="button" value="Default"/> <input type="button" value="Help"/>			

Port VID (PVID)

Set the port VLAN ID that will be assigned to untagged traffic on a given port. This feature is useful for accommodating devices that you want to participate in the VLAN but that don't support tagging. Each port of this switch allows user to set one PVID, the range is 1~255, default PVID is 1. The PVID must be the same as the VLAN ID the port belongs to, or the untagged traffic will be dropped.

Ingress Filtering

Ingress filtering lets frames belonging to a specific VLAN to be forwarded if the port belongs to that VLAN. This switch have two ingress filtering rule as follows:

Ingress Filtering Rule 1: Forward only packets with VID matching this port's configured VID.

Ingress Filtering Rule 2: Drop Untagged Frame.

4.8 Spanning Tree

The Spanning-Tree Protocol (STP) is a standardized method (IEEE 802.1D) for avoiding loops in switched networks. When STP enabled, ensure that only one path at a time is active between any two nodes on the network.

You can enable Spanning-Tree Protocol on web management's switch setting advanced item by selecting enable Spanning-Tree protocol. We are recommended that you enable STP on all switches ensures a single active path on the network.

1.You can view spanning tree information about the Root Bridge, such as following screen.

Root Bridge Information

Priority	32768
Mac Address	004063809988
Root_Path_Cost	0
Root Port	0
Max Age	20
Hello Time	2
Forward Delay	15

2.You can view spanning tree status about the switch, such as following screen.

STP Port Status

PortNum	PathCost	Priority	PortState
PORT1	10	128	FORWARDING
PORT2	10	128	FORWARDING
PORT3	10	128	FORWARDING
PORT4	10	128	FORWARDING
PORT5	10	128	FORWARDING
PORT6	10	128	FORWARDING
PORT7	10	128	FORWARDING
PORT8	10	128	FORWARDING
PORT9	10	128	FORWARDING
PORT10	10	128	FORWARDING

3. You can set new value for STP parameter, then click Apply button to modify.

Configure Spanning Tree Parameters

STP State	<input checked="" type="checkbox"/>
Priority (0-65535)	<input type="text" value="32768"/>
Max Age (6-40)	<input type="text" value="20"/>
Hello Time (1-10)	<input type="text" value="2"/>
Forward_Delay_Time(4-30)	<input type="text" value="15"/>

Apply

Parameter	Description
Priority	You can change priority value, A value used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root. Enter a number 1 through 65535.
Max Age	You can change Max Age value, The number of seconds a bridge waits without receiving Spanning-Tree Protocol configuration messages before attempting a reconfiguration. Enter a number 6 through 40.
Hello Time	You can change Hello time value, the number of seconds between the transmission of Spanning-Tree Protocol configuration messages. Enter a number 1 through 10.
Forward Delay Time	You can change forward delay time, The number of seconds a port waits before changing from its Spanning-Tree Protocol learning and listening states to the forwarding state. Enter a number 4 through 30.

4. The following parameter can be configured on each port, click Apply button to modify.

Configure Spanning Tree Port Parameters

Port Number	Path Cost (1 - 65535; Default 10)	Priority (0 - 255; Default 128)
<div> <div>PORT1</div> <div>PORT2</div> <div>PORT3</div> <div>PORT4</div> <div>PORT5</div> </div>	<input type="text" value="10"/>	<input type="text" value="128"/>

Apply

Help

Parameter	Description
Port Priority	You can make it more or less likely to become the root port, the range is 0-255,default setting is 128 the lowest number has the highest priority.
Path Cost	Specifies the path cost of the port that switch uses to determine which port are the forwarding ports the lowest number is forwarding ports, the range is 1-65535 and default value base on IEEE802.1D 10Mb/s = 50-600 100Mb/s = 10-60 1000Mb/s = 3-10

4.9 Port Sniffer

The Port Sniffer is a method for monitor traffic in switched networks. Traffic through ports can be monitored by one specific port. That is, traffic goes in or out monitored ports will be duplicated into sniffer port.

1.Roving Analysis State: Press **Space** key to set sniffer mode as Disable, Rx, Tx or Both.

2.Analysis Port: It means sniffer port which can be used to see all monitored port traffic. You can connect analysis port to Lan analysier or netxray.

3.Monitored Port: The ports you want to monitor. All monitor ports' traffic will be copied to analysis port. You can select max 25 monitor ports in the switch. You can choose which port want to be monitored in only one sniffer mode.

Port Sniffer

Roving Analysis State:		DISABLE ▾	
Analysis Port:		None	
		DISABLE	
		RX	
		TX	
		BOTH	
Port	Monitor	Port	Monitor
PORT1	<input type="checkbox"/>	PORT2	<input type="checkbox"/>
PORT3	<input type="checkbox"/>	PORT4	<input type="checkbox"/>
PORT5	<input type="checkbox"/>	PORT6	<input type="checkbox"/>
PORT7	<input type="checkbox"/>	PORT8	<input type="checkbox"/>
PORT9	<input type="checkbox"/>	PORT10	<input type="checkbox"/>
PORT11	<input type="checkbox"/>	PORT12	<input type="checkbox"/>
PORT13	<input type="checkbox"/>	PORT14	<input type="checkbox"/>
PORT15	<input type="checkbox"/>	PORT16	<input type="checkbox"/>
PORT17	<input type="checkbox"/>	PORT18	<input type="checkbox"/>
PORT19	<input type="checkbox"/>	PORT20	<input type="checkbox"/>
PORT21	<input type="checkbox"/>	PORT22	<input type="checkbox"/>
PORT23	<input type="checkbox"/>	PORT24	<input type="checkbox"/>

Apply Default Help

4.10 SNMP

Any Network Management running the simple Network Management Protocol (SNMP) can management the switch, provided the Management Information Base (MIB) is installed correctly on the management station. The SNMP is a Protocol that governs the transfer of information between management and agent. This switch supports SNMP V1.

1. Use this page to define management stations as trap managers and to enter SNMP community strings. You can also define a name, location, and contact person for the switch. Fill in the system options data then click Apply to update the changes on this page.

Name: Enter a name to be used for the switch.

Location: Enter the location of the switch.

Contact: Enter the name of a person or organization.

SNMP Management



System Options

Name :

Location :

Contact :

Apply

Help

2. Community strings serve as passwords and can be entered as one of the following:

RO: Read only. Enables requests accompanied by this string to display MIB-object information.

RW: Read write. Enables requests accompanied by this string to display MIB-object information and to set MIB objects.

Community Strings

Current Strings : <div style="border: 1px solid black; padding: 5px; min-height: 100px;">public__RO private__RW</div>	New Community String : String : <input style="width: 150px;" type="text"/> <div style="display: flex; justify-content: flex-end; align-items: center;"><input checked="" type="radio"/> RO <input type="radio"/> RW</div>
	<div style="display: flex; justify-content: center; gap: 10px;"><div style="border: 1px solid black; padding: 2px 10px;"><< Add <<</div><div style="border: 1px solid black; padding: 2px 10px;">Remove</div></div>

Trap Managers

Current Managers : <div style="border: 1px solid black; padding: 5px; min-height: 100px;">(none)</div>	New Manager : IP Address : <input style="width: 150px;" type="text"/> Community : <input style="width: 150px;" type="text"/>
	<div style="display: flex; justify-content: center; gap: 10px;"><div style="border: 1px solid black; padding: 2px 10px;"><< Add <<</div><div style="border: 1px solid black; padding: 2px 10px;">Remove</div></div>

3. Trap Manager

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 are issued. Create a trap manager by entering the IP address of the station and a community string.

4.11 Security Manager

Use this page you can change web management user name and password.

1. User name: Type the new user name.
2. Password: Type the new password.
3. Reconfirm password: Retype the new password.
4. Click Apply.

Security Manager



User Name:	<input type="text" value="admin"/>
Assign/Change password:	<input type="password" value="***"/>
Reconfirm pssword:	<input type="password" value="***"/>
	<input type="button" value="Apply"/>

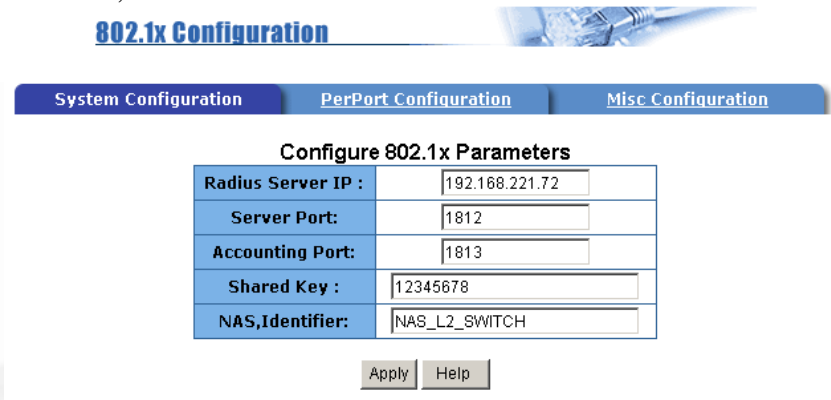
4.12 802.1X Configuration

If you enable the IEEE 802.1X function, you can configure the parameters of this function.

- System Configuration

1. Radius Server IP: Set the Radius Server IP address
2. Server Port: Set the UDP destination port for authentication requests to the specified Radius Server.
3. Accounting Port: Set the UDP destination port for accounting requests to the specified Radius Server.
4. Shared Key: Set an encryption key for use during authentication sessions with the specified radius server. This key must match the encryption key used on the Radius Server.
5. NAS, Identifier: Set the identifier for the radius client.

802.1x Configuration

The image shows a screenshot of a network configuration window titled "802.1x Configuration". At the top, there are three tabs: "System Configuration" (which is selected), "PerPort Configuration", and "Misc Configuration". Below the tabs, the main title is "Configure 802.1x Parameters". There is a table with five rows, each representing a configuration parameter. The first row is "Radius Server IP :" with a value of "192.168.221.72". The second row is "Server Port:" with a value of "1812". The third row is "Accounting Port:" with a value of "1813". The fourth row is "Shared Key :" with a value of "12345678". The fifth row is "NAS,Identifier:" with a value of "NAS_L2_SWITCH". At the bottom of the window, there are two buttons: "Apply" and "Help".

Configure 802.1x Parameters	
Radius Server IP :	192.168.221.72
Server Port:	1812
Accounting Port:	1813
Shared Key :	12345678
NAS,Identifier:	NAS_L2_SWITCH

Apply Help

- **Perport Configuration:**
There are four types for each port:

Fu, Force unauthorized: The specified port is required to be held in the Unauthorized state.

Fa, Force authorized: The specified port is required to be held in the Authorized state.

Au, Auto: 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.

No, None: The specified port is required to be held in the Authorized state.



Configure 802.1x Per Port State

Port Number	Port State
<div style="border: 1px solid black; padding: 2px;"> PORT1 ▲ PORT2 PORT3 PORT4 PORT5 ▼ </div>	<div style="border: 1px solid black; padding: 2px;"> Au ▼ Fu Fa Au No </div>
<div style="display: inline-block; margin-right: 10px;">Apply</div> <div style="display: inline-block;">Help</div>	

Port Status

PortNum	State
PORT1	No
PORT2	No
PORT3	No
PORT4	No
PORT5	No
PORT6	No
PORT7	No
PORT8	No
PORT9	No
PORT10	No
PORT11	No

● 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 waits to 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 attempts 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.

System Configuration

PerPort Configuration

Misc Configuration

Configure 802.1x misc configuration

Quiet period:	<input type="text" value="60"/>
Tx period:	<input type="text" value="30"/>
Supplicant timeout:	<input type="text" value="30"/>
Server timeout:	<input type="text" value="30"/>
Max requests:	<input type="text" value="2"/>
Reauth period:	<input type="text" value="3600"/>

Apply

Help

4.13 TFTP Update Firmware

The following menu options provide some system control functions to allow a user to update firmware and remote boot switch system:

1. Install TFTP Turbo98 and execution.
2. Copy firmware update version image.bin to TFTP Turbo98 directory.
3. In web management select administrator—TFTP update firmware.
4. Download new image.bin file then in web management press <update firmware>.
5. After update finished, press <reboot> to restart switch.

TFTP Download New Image



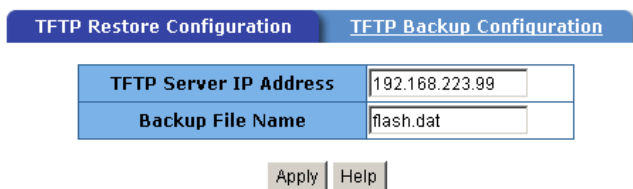
TFTP Server IP Address	<input type="text" value="192.168.223.99"/>
Firmware File Name	<input type="text" value="image.bin"/>

4.14 Configuration Backup

4.14.1 TFTP Restore Configuration

Use this page to set tftp server address. You can restore EEPROM value from here, but you must put back image in tftp server, switch will download back flash image.

TFTP Configuration



The image shows a web interface for TFTP configuration. It has two tabs: 'TFTP Restore Configuration' (selected) and 'TFTP Backup Configuration'. Below the tabs is a table with two rows: 'TFTP Server IP Address' with the value '192.168.223.99' and 'Backup File Name' with the value 'flash.dat'. At the bottom are 'Apply' and 'Help' buttons.

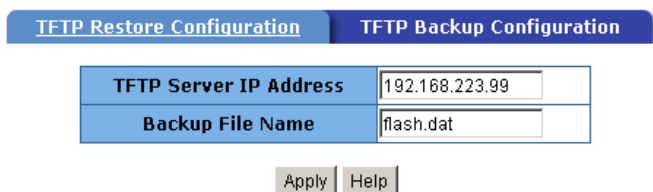
TFTP Restore Configuration		TFTP Backup Configuration
TFTP Server IP Address	192.168.223.99	
Backup File Name	flash.dat	

Apply Help

4.14.2 TFTP Backup Configuration

Use this page to set tftp server IP address. You can save current EEPROM value from here, then go to the TFTP restore configuration page to restore the eeprom value.

TFTP Configuration



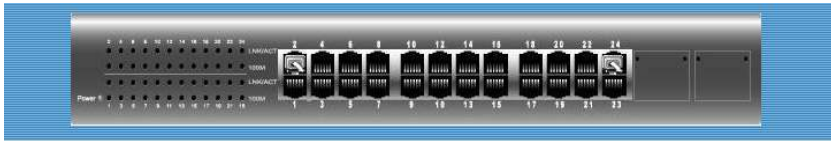
The image shows a web interface for TFTP configuration. It has two tabs: 'TFTP Restore Configuration' and 'TFTP Backup Configuration' (selected). Below the tabs is a table with two rows: 'TFTP Server IP Address' with the value '192.168.223.99' and 'Backup File Name' with the value 'flash.dat'. At the bottom are 'Apply' and 'Help' buttons.

TFTP Restore Configuration	TFTP Backup Configuration
TFTP Server IP Address	192.168.223.99
Backup File Name	flash.dat

Apply Help

4.15 Reset System

Reset the Switch to default configuration, default value as below



Reset System

Reset Switch to Default Configuration

reset

4.16 Reboot

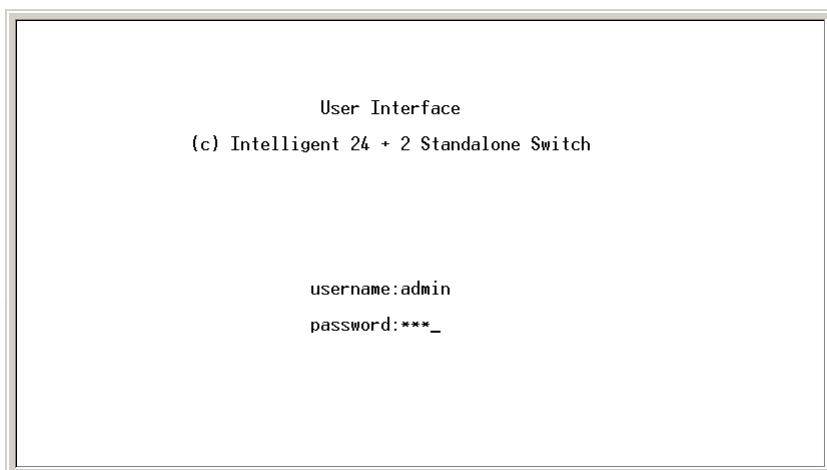
Reboot the system in software reset.



Chapter 3 Console-Menu Line

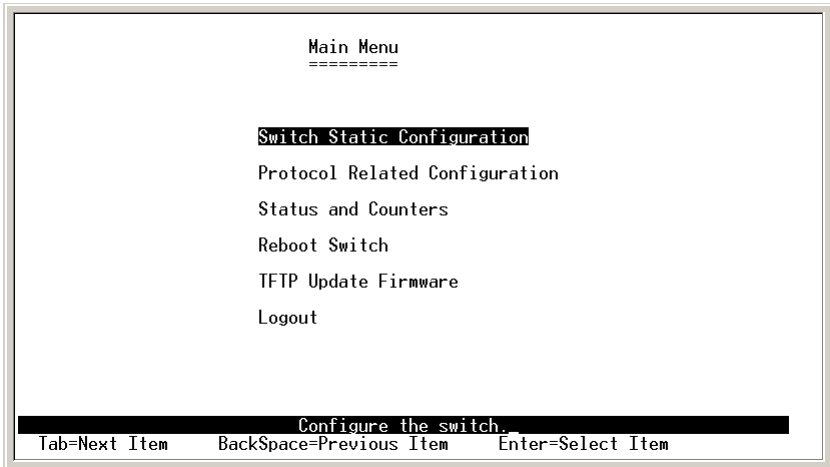
This switch also provides a serial interface to manage and monitor, you can follow the Console Port Information provided by web to use windows HyperTerminal program to link the switch.

You can type user name and password to login. The default user name is “admin” with password “123 ”.



1. Main Menu

There are six items for selected as follows:



Switch Static Configuration: Configure the switch.

Protocol Related Configuration: Configure the protocol function.

Status and Counters: Show the status of the switch.

Reboot Switch: Restart the system or reset switch to default configuration.

TFTP Update Firmware: Use tftp to download image.

Logout: Exit the menu line program.

<Control Key>

The control keys as follow provided in all menus:

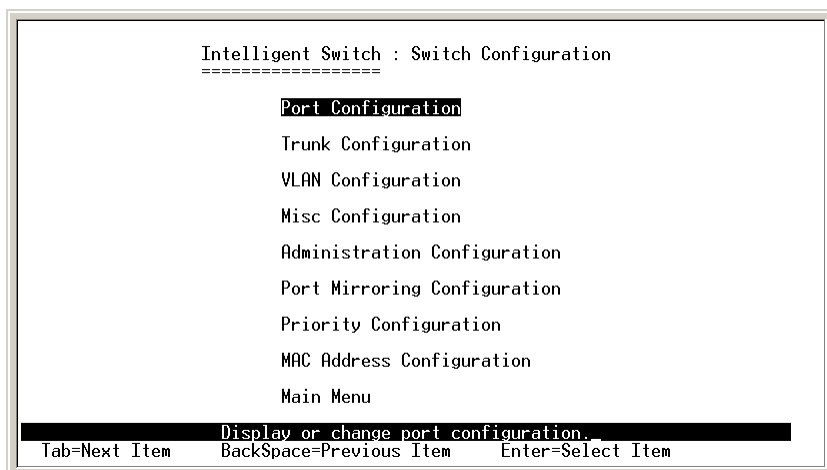
Tab: Move the vernier to next item.

Backspace: Move the vernier to previous item.

Enter: Select item.

Space: Toggle selected item to next configure.

2. Switch Static Configuration



You can press the key of **Tab** or **Backspace** to choose item, and press **Enter** key to select item. The action menu line as follow provided in later configure page.

Actions->

<Quit>: Exit the page of port configuration and return to previous menu.

<Edit>: Configure all items. Finished configure press **Ctrl+A** to go back action menu line.

<Save>: Save all configure value.

<Previous Page>: Return to previous page to configure.

<Next page>: Go to next page to configure.

2.1 Port Configuration

This page can change the status of each port. Press <Space> key to change configuration of each item.

Intelligent Switch : Port Configuration									
=====									
Port	Type	InRate (100K)	OutRate (100K)	Enable	Auto	Spd/Dpx		FlowControl	
								Full	Half
PORT1	100Tx	0	0	Yes	AUTO	100	Full	0n	0n
PORT2	100Tx	0	0	Yes	AUTO	100	Full	0n	0n
PORT3	100Tx	0	0	Yes	AUTO	100	Full	0n	0n
PORT4	100Tx	0	0	Yes	AUTO	100	Full	0n	0n
PORT5	100Tx	0	0	Yes	AUTO	100	Full	0n	0n
PORT6	100Tx	0	0	Yes	AUTO	100	Full	0n	0n
PORT7	100Tx	0	0	Yes	AUTO	100	Full	0n	0n
PORT8	100Tx	0	0	Yes	AUTO	100	Full	0n	0n

actions->	<Quit>	<Edit>	<Save>	<Previous Page>	<Next Page>
Select the Action menu.					
Tab=Next Item BackSpace=Previous Item Quit=Previous menu Enter=Select Item					

- InRate(100K/unit):** You can set input rate control, per unit is 100K. The valid range is 0~1000.
0: disable rate control.
1~1000: valid rate value.
- OutRate(100K/unit):** You can set output rate control, per unit is 100K. The valid range is 0~1000.
0: disable rate control.
1~1000: valid rate value.
- Enable:** You can disable or enable this port control. “Yes” means the port is enabled, “No” means the port is disabled.
- Auto:** You can set auto-negotiation mode as Auto, Nway_Force or Force of each port.
- Spd/Dpx:** You can set 100/10Mbps speed on port 1~port24; 1000/100/10Mbps speed on port25~port26 (Gigabit Switch), 100/10Mbps speed on port25~port26 (Fast Ethernet Switch) and set full-duplex or half-duplex mode.
- Flow Control:**
Full: Displays the flow control status is enable/disable in full

duplex mode.

Half: Displays the backpressure is enable/disable in half duplex mode.

NOTE:

1. Pressing <Save> only can save one page configuration.
2. If the static trunk group exists, you can see it (ex: TRK1, TRK2...) after port 26, and you can configure all of the items as above.

2.2 Trunk Configuration

This page can create max to seven trunk groups. You can arbitrarily select up to four ports from port 1~port 24/port25 ~ port26 to build a trunking group.

1. Select **<Edit>** on actions menu.
 2. Press **<Space>** key to configure the member port of the trunk group. Besides, you have to set “Static” or “LACP” for the corresponding trunk group of TRK1~TRK7 item.
 “Static” – the normal trunk.
 “LACP” – this trunk group have link aggregation control protocol.
 3. Press **Ctrl+A** to go back action menu line.
 4. Select **<Save>** to save all configure value.
 5. If the item of TRK1~TRK7 is set “Disable”, it means the trunk group is deleted.
 6. All ports in the same static trunk group will be treated as single port. So when you setting VLAN members and Port configuration they will be toggled on or off simultaneously.
- NOTE:** If VLAN group exists, all of the members of static trunk group **must** be in same VLAN group.

Intelligent Switch : Trunk Configuration																										
	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	M1	M2
1	v	v	v	v	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
3	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
4	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
5	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
6	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
7	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	

TRK1	LACP
TRK2	Disable
TRK3	Disable
TRK4	Disable
TRK5	Disable
TRK6	Disable
TRK7	Disable

actions->	<Edit>	<Save>	<Quit>
Select the action menu.			
Tab=Next Item	BackSpace=Previous Item	Quit=Previous menu	Enter=Select Item

2.3 VLAN Configuration

```
Intelligent Switch : VLAN Configuration
=====

VLAN Configure

Create a VLAN Group
Edit/Delete a VLAN Group
Group Sorted Mode
Previous Menu

Configure the VLAN pvid and ingress.egress Rule.
Tab=Next Item BackSpace=Previous Item Quit=Previous menu Enter=Select Item
```

2.3.1 VLAN Configure

This page can set VLAN mode as port-based VLAN, 802.1Q VLAN or just disable the VLAN function.

NOTE: You have to restart the switch for valid value every time you change the VLAN mode.

```
Intelligent Switch : VLAN Support Configuraton
=====

VLAN Mode : PortBased

actions-> <Quit> <Edit> <Save> <Previous Page> <Next Page>
Select the Action menu.
Tab=Next Item BackSpace=Previous Item Space=Toggle Ctrl+A=Action menu
```

If set 802.1Q VLAN, you can set PVID, ingress filtering 1 and ingress filtering 2 in this page too.

```

Intelligent Switch : VLAN Support Configuraton
=====
VLAN Mode : 802.1Q

Port      PVID      IngressFilter1      IngressFilter2
-----
PORT1     1          Drop                Forward
PORT2     1          Drop                Forward
PORT3     1          Drop                Forward
PORT4     1          Drop                Forward
PORT5     1          Drop                Forward
PORT6     1          Drop                Forward
PORT7     1          Drop                Forward
PORT8     1          Drop                Forward

actions->   <Quit>      <Edit>      <Save>      <Previous Page>   <Next Page>
Select the Action menu.
Tab=Next Item BackSpace=Previous Item Space=toggle Ctrl+A=Action menu

```

1.PVID (Port VID : 1~255): Type the PVID.

2.NonMember Pkt: It matches that Ingress Filtering Rule 1 on web management. It will forward only packets with VID matching this port's configured VID. Press **Space** key to choose forward or drop the frame that VID not matching this port's configured VID.

3.UnTagged Pkt: It matches that Ingress Filtering Rule 2 on web management. It will drop untagged frames. Press **Space** key to choose drop or forward the untagged frames.

2.3.2 Create a VLAN Group

- Create Port-based VLAN and add member/nonmember ports to it

1. Select **<Edit>**.

2. **VLAN Name:** Type a name for the new VLAN.

3. **Grp ID:** Type the VLAN group ID. The group ID range is 1~26.

4. **Member:** Press **Space** key to choose VLAN member.

There are two types to select:

a. Member: the port is a member port.

b. NO: the port is NOT a member port.

5. Press **Ctrl+A** go back action menu line.

6. Select **<Save>** to save all configure value.

NOTE: If the trunk group exists, you can see it (ex: TRK1, TRK2...) after port26, and you can configure it is the member of the VLAN or not.

Add an VLAN Group

VLAN Name: [vlan2

1

Grp ID: [2

1(1~4094)

Port	Member
PORT1	Member
PORT2	Member
PORT3	No
PORT4	No
PORT5	No
PORT6	No
PORT7	No
PORT8	No

actions->

<Quit>

<Edit>

<Save>

<Previous Page>

<Next Page>

Select the Action menu.

Tab=Next Item BackSpace=Previous Item Space=Toggle Ctrl+A=Action menu

- Create 802.1Q VLAN and add tagged /untagged member ports to it

1. Select **<Edit>**.

2. **VLAN Name:** Type a name for the new VLAN.

3. **VLAN ID:** Type a VID (between 2~4094). The default is 1.
There are 256 VLAN groups to configure.

3. **Protocol VLAN:** Press **Space** key to choose protocol types.

4. **Member:** Press **Space** key to choose VLAN members. There are three types to select:

UnTagged: this port is the member port of this VLAN group and outgoing frames are NO VLAN-Tagged frames.

Tagged: this port is the member port of this VLAN group and outgoing frames are VLAN-Tagged frames.

NO: The port is NOT member of this VLAN group.

5. Press **Ctrl+A** go back action menu line.

6. Select **<Save>** to save all configure value.

NOTE: If the trunk group exists, you can see it (ex: TRK1, TRK2...) after port26, and you can configure it as the member of the VLAN or not.

Add an VLAN Group

VLAN Name: [vlan2] 1 VLAN ID: [2] 1(1~4094)

Protocol VLAN : None

Port	Member
PORT1	UnTagged
PORT2	Tagged
PORT3	UnTagged
PORT4	No
PORT5	No
PORT6	No
PORT7	No
PORT8	No

actions-> <Quit> <Edit> <Save> <Previous Page> <Next Page>

Select the Action menu.

Tab=Next Item BackSpace=Previous Item Space=Toggle Ctrl+A=Action menu

2.3.3 Edit / Delete a VLAN Group

In this page, you can edit or delete a VLAN group.

1. Press **<Edit>** or **<Delete>** item.
2. Choose the VLAN group that you want to edit or delete and then press enter.
3. You can modify the protocol VLAN item and the member port as tagged or un-tagged and remove some member ports from this VLAN group.
4. After edit VLAN, press **<Save>** key to save all configures value.

NOTE:

1. Press **<Enter>** once will complete deletion on delete mode.
2. The VLAN Name and VLAN ID cannot be modified.
3. The default VLAN can't be deleted.

NAME: _____	VID: _____	NAME: _____	VID: _____
DEFAULT	1		
vlan2	2		

actions-> **<Quit>** **<Edit>** **<Delete>** **<Previous Page>** **<Next Page>**
Edit/Delete a VLAN Group.
Tab=Next Item BackSpace=Previous Item Quit=Previous menu Enter=Select Item

Edit an VLAN Group

VLAN Name: [vlan2] 1 VLAN ID: [2] 1(1~4094)

Protocol VLAN : None

Port	Member
PORT1	UnTagged
PORT2	Tagged
PORT3	UnTagged
PORT4	No
PORT5	No
PORT6	No
PORT7	No
PORT8	No

actions-> **<Quit>** **<Edit>** **<Save>** **<Previous Page>** **<Next Page>**
Select the Action menu.
Tab=Next Item BackSpace=Previous Item Quit=Previous menu Enter=Select Item

2.3.4 Groups Sorted Mode

In this page, you can select VLAN groups sorted mode as (1) sorted by name (2) sorted by VID.
In the *Edit/Delete a VLAN group* page will display the result.

Intelligent Switch : Group Sorted Selection
=====

Group Sorted :Sorted_By_Name

actions-> <Edit> <Save> <Quit>
Select the action menu.
Tab=Next Item BackSpace=Previous Item Quit=Previous menu Enter=Select Item

In the *Edit/Delete a VLAN Group* page, the result of sorted by name.

NAME:	VID:	NAME:	VID:
-----	-----	-----	-----
DEFAULT	1		
A1	56		
B1	33		
Vlan2	23		

In the *Edit/Delete a VLAN Group* page, the result of sorted by VID.

NAME:	VID:	NAME:	VID:
-----	-----	-----	-----
DEFAULT	1		
Vlan2	23		
B1	33		
A1	56		

2.4 Misc Configuration

```
Intelligent Switch : Misc Configuration
=====

MAC Age Interval
Broadcast Storm Filtering
Max bridge transmit delay bound
Port Security
Collisions Retry Forever
Previous Menu

Configure the MAC aging time.
Tab=Next Item BackSpace=Previous Item Enter=Select Item
```

2.4.1 MAC Age Interval

Type the number of seconds that an inactive MAC address remains in the switch's address table. The valid range is 300~765 seconds. Default is 300 seconds.

```
Intelligent Switch : MAC Aging Time
=====

MAC Age Interval (sec) [300] : 300
(disable:0,valid value:300~765)

actions-> <Edit> <Save> <Quit>
Select the action menu.
Tab=Next Item BackSpace=Previous Item Quit=Previous menu Enter=Select Item
```

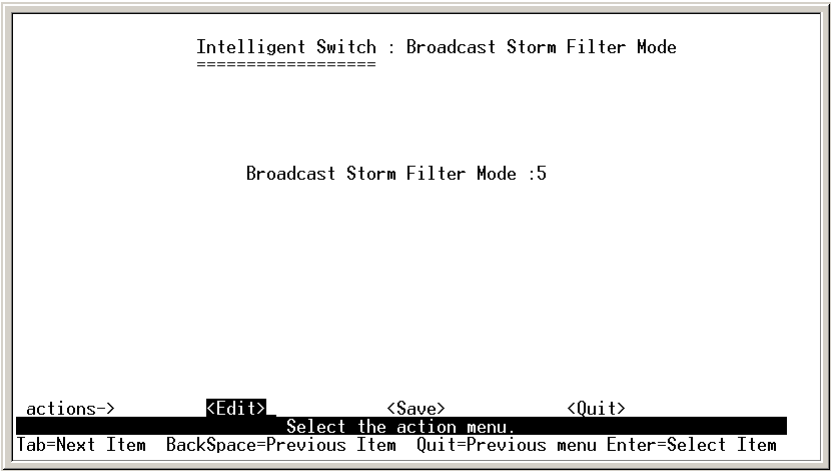
2.4.2 Broadcast Storm Filtering

In this page you can configure broadcast storm settings.

1.Press **<Edit>** to configure the broadcast storm filter mode.

2.Press **Space** key to choose the threshold value.

The valid threshold value are 5%,10%,15%,20%,25% and NO.



2.4.3 Max bridge transmit delay bound

1.Max bridge transmit delay bound: Limit the packets queuing time in switch. If enable, the packets queued exceed will be drop. Press **Space** key to set the time. This valid value are 1sec, 2sec, 4sec and off. Default is off.

2.Low Queue Delay Bound: Limit the low priority packets queuing time in switch. If enable, the low priority packet stays in switch exceed Low Queue Max Delay Time, it will be sent. Press **Space** key to enable or disable this function.

3.Low Queue Max Delay Time: To set the time that low priority packets queuing in switch. Default Max Delay Time is 255ms. The valid range is 1~255 ms.

NOTE: Make sure of “Max bridge transit delay bound control” is enabled before enable Low Queue Delay Bound, because Low Queue Delay Bound must be work under “Max bridge transit delay bound control” is enabled situation.



2.4.4 Port Security

A port in security mode will be “locked” without permission of address learning. Only the incoming packets with SMAC already existing in the address table can be forwarded normally. You can disable the port from learning any new MAC addresses, then use the static MAC addresses screen to define a list of MAC addresses that can use the secure port.

Intelligent Switch : Port Security

=====

Port	Enable Security (disable for MAC Learning)
PORT1	enabled
PORT2	Disabled
PORT3	Disabled
PORT4	Disabled
PORT5	Disabled
PORT6	Disabled
PORT7	Disabled
PORT8	Disabled

actions-> **<Quit>** <Edit> <Save> <Previous Page> <Nex

Tab=Next Item BackSpace=Previous Item Quit=Previous menu Enter=Select Item

1. Select **<Edit>**.
2. Press **Space** key to choose enable / disable item.
3. Press **Ctrl+A** to go back action menu line.
4. Select **<Save>** to save all configure value.
4. You can press **<Next Page>** to configure port9 ~ port26 and press **<Previous Page>** to return to last page.

2.5 Administration Configuration

Intelligent Switch : Device Configuration
=====

Change Username

Change Password

Device Information

IP Configuration

Previous Menu

Configure the username.

Tab=Next Item BackSpace=Previous Item Enter=Select Item

2.5.1 Change Username

You can change web management user name in this page. Type the new user name, then press **<Save>** item.

Intelligent Switch : UserName Configuration
=====

UserName : admin

actions->

<Edit>

<Save>

<Quit>

Select the action menu.

Tab=Next Item BackSpace=Previous Item Quit=Previous menu Enter=Select Item

2.5.2 Change Password

In this page you can change web management login password.

```
Intelligent Switch : Password Configuration
=====

Old Password:***
new password:***
enter again :***

Entering new password.
Esc=Previous menu
```

2.5.3 Device Information

This page provide user to configure the device information.

```
Intelligent Switch : Device Information
=====

Name      : Intelligent 24+2 Switch
Description : Intelligent 24+2 Switch
Location   :
Content    : 24 + 1 PORTS

actions->      [Edit]      <Save>      <Quit>
Select the action menu.
Tab=Next Item BackSpace=Previous Item Quit=Previous menu Enter=Select Item
```

2.5.4 IP Configuration

You can configure the IP setting and fill in the new value.

Intelligent Switch : IP Configuration
=====

DHCP : Disabled

IP Address : 192.168.233.100

Subnet Mask : 255.255.255.0

Gateway : 192.168.233.254

actions-> <Edit> <Save> <Quit>

Select the action menu.

Tab=Next Item BackSpace=Previous Item Quit=Previous menu Enter=Select Item

2.6 Port Mirroring Configuration

The port mirroring is a method for monitor traffic in switched networks. Traffic through ports can be monitored by one specific port. That is, traffic goes in or out monitored ports will be duplicated into monitoring port.

Press **Space** key to change configure of each item.

1.Select **<Edit>**.

2.**Sniffer Mode:** Press **Space** key to set sniffer mode: Disable\Rx\Tx\Both.

3.**Monitoring Port:** It means sniffer port can be used to see all monitor port traffic. Press **Space** key to choose it.

4.**Monitored Port:** The ports you want to monitor. All monitor port traffic will be copied to sinffer port. You can select max 25 monitor ports in the switch. You can choose which port want to be monitored in only one sniffer mode.

Press **Space** key to choose member port,

“V” – is the member,

“—” – not the member.

5.Press **Ctrl+A** go back action menu line

6.Select **<Save>** to save all configure value.

7.On the action menu line you can press **<Next Page>** to configure port9 ~ port26, press **<Previous Page>** return to last page.

NOTE: Only have one sniffer mode in this switch at the same time.

```

Intelligent Switch : Port Sniffer
=====
Sniffer Mode: Rx
Monitoring Port : PORT1
Monitored Port :

Port      member
-----
PORT1     -
PORT2     -
PORT3     v
PORT4     -
PORT5     0
PORT6     -
PORT7     -
PORT8     -

actions->  <Quit>    <Edit>    <Save>    <Previous Page>    <Next Page>
                Select the Action menu.
Tab=Next Item BackSpace=Previous Item Space=Toggle Ctrl+A=Action menu
```

2.7 Priority Configuration

There are 0~7 priority levels can map to high or low queue.

1. Select **<Edit>**.
2. Press **Space** key to select the priority level mapping to high or low queue.
3. **High/Low Queue Service Ration H:L** : You can select the ratio of high priority packets and low priority packets.
4. Press **Ctrl+A** go back action menu line.
5. Select **<Save>** to save all configure value.

```
Intelligent Switch : Port Priority
=====

Port          Priority
-----
PORT1         Low
PORT2         Low
PORT3         High
PORT4         High
PORT5         Disable
PORT6         Disable
PORT7         Disable
PORT8         Disable

actions->      <Quit>      <Edit>      <Save>      <Previous Page>      <Next Page>
Select the Action menu.
Tab=Next Item  BackSpace=Previous Item  Quit=Previous menu  Enter=Select Item
```

2.8 MAC Address Configuration

```
Intelligent Switch : MAC Address Configuration
=====

Static MAC Address

Filtering MAC Address

Previous Menu

Configure the MAC address.
Tab=Next Item      BackSpace=Previous Item      Enter=Select Item
```

2.8.1 Static MAC Address

When you 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.

In this page you can add/modify/delete a static MAC address.

```
Intelligent Switch : Static MAC Address Configuration
=====

Mac Address  Port num  Vlan ID          Mac Address  Port num  Vlan ID
-----

actions->  <Quit>  <Add>  <Edit>  <Delete>  <Previous Page>  <Next Page>
Add/Edit/Delete a Mac.
Tab=Next Item  BackSpace=Previous Item  Quit=Previous menu  Enter=Select Item
```

2.8.2 Filtering MAC Address

MAC address filtering allows the switch to drop unwanted traffic. Traffic is filtered based on the destination addresses. In this page you can add/modify/delete the filtering MAC address.

```

Intelligent Switch : Filter MAC Address Configuration
=====
Mac Address      Vlan ID
-----
Mac Address      Vlan ID
-----

actions-> <Quit> <Add> <Edit> <Delete> <Previous Page> <Next Page>
          AddItem Quit=Previous menu Enter=Select Item

```

3. Protocol Related Configuration

```
Intelligent Switch : The Protocol Related configuration
=====

STP

SNMP

GVRP

IGMP

LACP

802.1X

Previous Menu

Configure the Spanning Tree Protocol.
Tab=Next Item      BackSpace=Previous Item      Enter=Select Item
```

3.1 STP

```
Intelligent Switch : Spanning Tree Protocol
=====

STP Enable

System Configuration

Perport Configuration

Previous Menu

Enabled or disabled the Spanning Tree Protocol.
Tab=Next Item      BackSpace=Previous Item      Enter=Select Item
```


3.1.1 STP Enable

You can enable or disable Spanning Tree function in this page. Press **Space** key to select enable or disable.

```
Intelligent Switch : STP Enabled/Disabled Configuration
=====

STP : Enabled

actions->          <Edit>          <Save> u Enter=Select Item
Configure STP enabled/disabled.
Tab=Next Item BackSpace=Previous Item Space=Toggle Ctrl+A=Action menu
```

3.1.2 System Configuration

```
Intelligent Switch : STP System Configuration
=====

Root Bridge Information          Configure Spanning Tree Parameters
-----
Priority       : 32768           Priority (0-65535) : 32768
Mac Address   : 004063809988    Max Age (6-40)     : 20
Root_Path_Cost : 0              Hello Time (1-10)  : 2
Root Port     : Root            Forward_Delay_Time(4-30) : 15
Max Age       : 20
Hello Time    : 2
Forward Delay : 15

actions->          <Edit>          <Save>          <Quit>
Select the action menu.
Tab=Next Item BackSpace=Previous Item Quit=Previous menu Enter=Select Item
```

1. You can view spanning tree information about the Root Bridge on the left.
2. On the right, you can set new values for STP parameters.

3.1.3 Perport Configuration

Intelligent Switch : STP Port Configuration =====			
Port	PortState	PathCost	Priority
PORT1	Forwarding	10	128
PORT2	Forwarding	10	128
PORT3	Forwarding	10	128
PORT4	Forwarding	10	128
PORT5	Forwarding	10	128
PORT6	Forwarding	10	128
PORT7	Forwarding	10	128
PORT8	Forwarding	10	128
actions-> <Quit> <Edit> <Save> <Previous Page> <Next Page>			
Select the Action menu.			
Tab=Next Item BackSpace=Previous Item Quit=Previous menu Enter=Select Item			

- 1.**PortState:** Display spanning tree status about the switch for per port as forwarding or blocking.
- 2.Select **<Edit>**.
- 3.**PathCost:** Specifies the path cost of the port that switch uses to determine which port are the forwarding ports.
- 4.**Priority:** This means port priority. You can make it more or less likely to become the root port.
- 5.Press **Ctrl+A** go back action menu line.
- 6.Select **<Save>** to save all configure value.
- 7.On the action menu line you can press **<Next Page>** to configure port9 ~ port26, press **<Previous Page>** to return to last page.

3.2 SNMP

Use this page to define management stations as trap managers and to enter SNMP community strings. You can also define a name, location, and contact person for the switch.

Intelligent Switch : SNMP Configuration
=====

System Options

Community Strings

Trap Managers

Previous Menu

Configure the system information.

Tab=Next Item BackSpace=Previous Item Enter=Select Item

3.2.1 System Options

Intelligent Switch : System Options Configuration
=====

System Name :

System Contact :

System Location :

actions-> <Edit> <Save> <Quit>

Select the action menu.

Tab=Next Item BackSpace=Previous Item Quit=Previous menu Enter=Select Item

1. Press <Edit>.
2. **System Name:** Type a name to be used for the switch.
3. **System Contact:** Type the name of contact person or organization.
4. **System Location:** Type the location of the switch.
5. Press **Ctrl+A** go back action menu line.
6. Press <Save> to save configure value.

3.2.2 Community Strings

Use this page to add/edit/delete SNMP community strings.

1.Community Name: The name of current strings.

2.Write Access: Enable the rights is read only or read write.

- **Restricted:** Read only, enables requests accompanied by this string to display MIB-object information.
- **Unrestricted:** Read write, enables requests accompanied by this string to display MIB-object information and to set MIB objects.

Intelligent Switch : SNMP Community Configuration	
Community Name	Write Access
public	Restricted
private	Unrestricted

actions-> **<Add>** **<Edit>** **<Delete>** **<Quit>**

Add/Edit/Delete community strings.

Tab=Next Item BackSpace=Previous Item CTRL+A=Action menu Enter=Select Item

3.2.3 Trap Managers

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 are issued. Create a trap manager by entering the IP address of the station and a community string.

```
Intelligent Switch : Trap Managers Configuration
=====

IP _____ Community Name _____

actions->      <Add>      <Edit>      <Delete>      <Quit>
Add/Edit/Delete trap managers.
Tab=Next Item BackSpace=Previous Item Quit=Previous menu Enter=Select Item
```

● Add the trap manager

1. Press <Add> -> <Edit> to add the trap manager.
2. **IP:** Type the IP address.
3. **Community Name:** Type the community name.
4. Press **Ctrl+A** go to actions line, then press <Save> key to save all configure.

```
Intelligent Switch : Add SNMP Trap Manager
=====

IP :192.168.223.100
Community Name :public_

actions->      <Edit>      <Save>      <Quit>
Select the action menu.
Tab=Next Item BackSpace=Previous Item CTRL+A=Action menu Enter=Select Item
```

● Edit trap manager

1. Press **<Edit>** key to choose the item that you want to modify.
2. Press **<Edit>** key.
3. **IP:** Type the new IP address.
4. **Community Name:** Type the community name.
5. Press **Ctrl+A** go to actions line, press **<Save>** key to save all configure.

```

Intelligent Switch : Add SNMP Trap Manager
=====

IP :192.168.223.100
Community Name :trap

actions->      <Edit>      <Save>      <Quit>
Select the action menu.
Tab=Next Item BackSpace=Previous Item CTRL+A=Action menu Enter=Select Item

```

● Delete trap manager

1. Press **<Delete>** key.
2. Choose the trap manager that you want to delete and then press enter.
3. Press **<Enter>** once will complete deletion on delete mode.

```

Intelligent Switch : Trap Managers Configuration
=====

IP      Community Name
-----
192.168.223.100      comma

actions->      <Add>      <Edit>      <Delete>      <Save>      <Quit>
Add/Edit/Delete trap managers.
Tab=Next Item BackSpace=Previous Item Quit=Previous menu Enter=Select Item

```

3.3 GVRP

In this page you can enable/disable the GVRP (GARP VLAN Registration Protocol) support.

1. Select **<Edit>**.
2. Press **Space** key to choose Enabled / Disabled.
3. Press **Ctrl+A** go back action menu line.
4. Select **<Save>** to save configure value.

```
Intelligent Switch : GVRP Configuration
=====

GVRP : Enabled _

actions->          <Edit>          <Save>          <Quit>
Select the action menu.
Tab=Next Item  BackSpace=Previous Item  Space=Toggle  Ctrl+A=Action menu
```


3.4 IGMP

In this page you can enable / disable the IGMP support.

1. Select **<Edit>**.
2. Press **Space** key to choose Enabled / Disabled.
3. Press **Ctrl+A** go back action menu line.
4. Select **<Save>** to save configure value.

```
Intelligent Switch : IGMP Configuration
=====

IGMP : Enabled

actions->      <Edit>      <Save>      <Quit>
Select the action menu.
Tab=Next Item BackSpace=Previous Item Space=Toggle Ctrl+A=Action menu
```

3.5 LACP

In this page you can configure and view all the LACP status.

Intelligent Switch : LACP Configuration
=====

Working Ports Setting

State Activity

LACP Status

Previous Menu

LACP setting.

Tab=Next Item BackSpace=Previous Item Enter=Select Item

3.5.1 Working Port Setting

This page can set the actually work ports in trunk group.

1. Select **<Edit>**.

2. **Group:** Display the trunk group ID.

3. **LACP:** Display the trunk group's LACP status.

4. **LACP Work Port Num:** The max number of ports can be aggregated at the same time. If LACP static trunking group, the exceed ports is standby and able to aggregate if work ports fail.

NOTE: Before set this page, you have to set trunk group on the page of *Trunk Configuration* first.

Intelligent Switch : LACP Group Configuration
=====

Group

LACP Work Port Num

actions->

<Edit>

<Save>

<Quit>

Select the action menu.

Tab=Next Item BackSpace=Previous Item Quit=Previous menu Enter=Select Item

1. Select **<Edit>**.

2. Press **Space** key to choose the item.

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.

3. Press **Ctrl+A** go back action menu line.

4. Select **<Save>** to save configure value.

If user set LACP mode in the trunk group, all of the member ports of this trunk group will set "Active" automatic.

```

Intelligent Switch : LACP Port State Active Configuration
=====
Port          State Activity          Port          State Activity
-----

```

3.5.3 LACP Status

When you set trunking groups you can see relation information here.

Intelligent Switch : LACP Group Status
=====

Static Trunking Group

Group Key : 1

Port_No : 1 2 3 4

actions-> <Quit> <Previous Page> <Next Page>
Select the action menu.
Tab=Next Item BackSpace=Previous Item Quit=Previous menu Enter=Select Item

<Quit>: Exit this page and return to previous menu.

<Previous Page>: Return to previous page to view.

<Next page>: Go to next page to view.

3.6 802.1X Configuration



3.6.1 Enable 802.1X function

Press **Space** key to enable or disable the 802.1x function.



3.6.2 System Configuration

If you enable the IEEE 802.1X function, you can configure the parameters of this function.

1. Radius Server IP: Set the Radius Server IP address
2. Shared Key: Set an encryption key for use during authentication sessions with the specified radius server. This key must match the encryption key used on the Radius Server.
3. NAS, Identifier: Set the identifier for the radius client.
4. Server Port: Set the UDP destination port for authentication requests to the specified Radius Server.
5. Accounting Port: Set the UDP destination port for accounting requests to the specified Radius Server.

There are four types for each port:

Fu, Force unauthorized: The specified port is required to be held in the Unauthorized state.

Fa, Force authorized: The specified port is required to be held in the Authorized state.

Au, Auto: 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.

No, None: The specified port is required to be held in the Authorized state.

```
Intelligent Switch : 802.1x System Configuration
=====

Radius Server IP : 192.168.221.72
Shared Key : 12345678
NAS,Identifier: NAS_L2_SWITCH
Server Port: 1812
Accounting Port: 1813

(Force Unauth=Fu, Force Auth=Fa, Auto=Au, None=No):
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 M1 M2
Au Fu Fa No No No No No No No No No No No No No No No No No No No

actions->      <Edit>          <Save>          <Quit>
Select the action menu.
Tab=Next Item  BackSpace=Previous Item  Quit=Previous menu Enter=Select Item
```

3.6.3 Misc Configuration

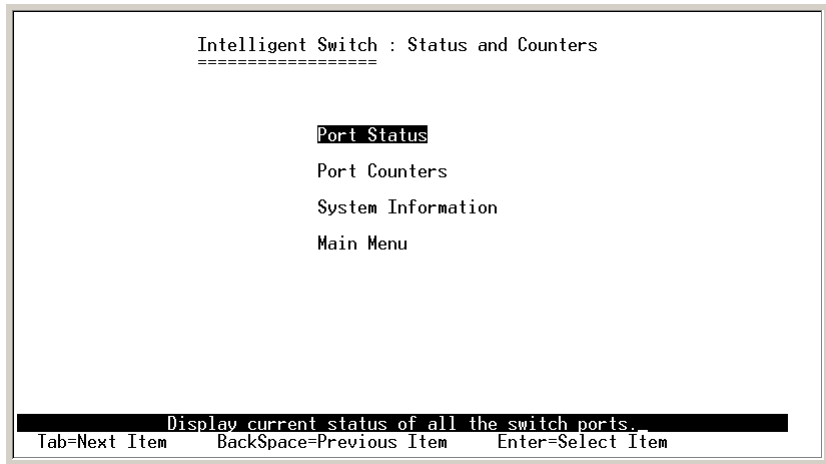
1. Quiet period: Set the period during which the port doesn't try to acquire a supplicant.
2. Tx period: Set the period the port waits to retransmit next EAPOL PDU during an authentication session.
3. Supplicant timeout: Set the period of time the switch waits for a supplicant response to an EAP request.
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 attempts 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

```
Intelligent Switch : 802.1x Misc Configuration
=====

Quiet-period <0..65535,default=60>      : 60
Tx-period <0..65535,default=30>          : 30
Supplicant-timeout <1..300,default=30>    : 30
Server-timeout <1..300,default=30>        : 30
ReAuthMax <1..10,default=2>               : 2
Reauth-period <1..9999999,default=3600>   :36

actions->      <Edit>      <Save>      <Quit>
Select the action menu.
Tab=Next Item BackSpace=Previous Item Quit=Previous menu Enter=Select Item
```

4. Status and Counters



You can press the key of **Tab** or **Backspace** to choose each item, and press **Enter** key to select the item.

4.1 Port Status

This page displays the status of each port.

Link Status: “Down” and “Up” means “No Link” and “Link” respectively.

InRate: Displays the input rate control (100K/unit) setting values.

OutRate: Displays the output rate control (100K/unit) setting values.

Enabled: Displays the port is enabled or disable depended on user settings. Enable will be displayed as “Yes”, disable will be displayed as “No”. If the port is unlink it will be treated as “No”.

Auto: Displays the port is link on which Nway mode: Auto , Nway_Force , Force.

Spd/Dpx: Displays the port speed and duplex.

Flow Control: In auto / Nway force mode, displays the flow control status is enable or disable after negotiation.

In force mode, displays the flow control status is enable or disable depending on user settings.

Intelligent Switch : Port Status							
=====							
Port	Link Status	InRate (100K)	OutRate (100K)	Enable	Auto	Spd/Dpx	Flow Control
PORT5	Down	0	0	Yes	AUTO	10 Half	Off
PORT6	Down	0	0	Yes	AUTO	10 Half	Off
PORT7	Down	0	0	Yes	AUTO	10 Half	Off
PORT8	Down	0	0	Yes	AUTO	10 Half	Off
PORT9	Down	0	0	Yes	AUTO	10 Half	Off
PORT10	Down	0	0	Yes	AUTO	10 Half	Off
PORT11	Down	0	0	Yes	AUTO	10 Half	Off
PORT12	Down	0	0	Yes	AUTO	10 Half	Off

actions-> <Quit> <Previous Page> <Next Page>
Select the action menu.
Tab=Next Item BackSpace=Previous Item Quit=Previous menu Enter=Select Item_

4.2 Port Counters

The following information provides a view of the current status of the unit.

<Quit>: Exit the page of port status, and return to previous menu.

<Reset All>: Set all count to 0.

<Previous Page>: Display previous page.

<Next page>: Display next page.

Intelligent Switch : Port Counters							
=====							
Port	TxGoodPkt	TxBadPkt	RxGoodPkt	RxBadPkt	TxAbort	Collision	DropPkt

PORT5	0	0	0	0	0	0	0
PORT6	0	0	0	0	0	0	0
PORT7	0	0	0	0	0	0	0
PORT8	0	0	0	0	0	0	0
PORT9	0	0	0	0	0	0	0
PORT10	0	0	0	0	0	0	0
PORT11	0	0	0	0	0	0	0
PORT12	0	0	0	0	0	0	0
actions-> <Quit> <Reset All> <Previous Page> <Next Page>							
Configure the action menu.							
Tab=Next Item BackSpace=Previous Item Quit=Previous menu Enter=Select Item							

4.3 System Information

MAC Address: The unique hardware address assigned by manufacturer.

Firmware Version: Display the switch's firmware version.

Hardware Version: Display the switch's Hardware version.

Default config value version: Display write to default eeprom value tale version.

Module1 information: Display the information saved in eeprom of module1.

Module2 information: Display the information saved in eeprom of module2.

```
Intelligent Switch : System Information
=====

MAC Address           : 004063809988
Firmware version      : 2.3
ASIC version          : A7.0
PCBA version          : 1.0
Serial number         :
Module 1 Type         : NC
Module 1 information  : N/A
Module 2 Type         : NC
Module 2 information  : N/A

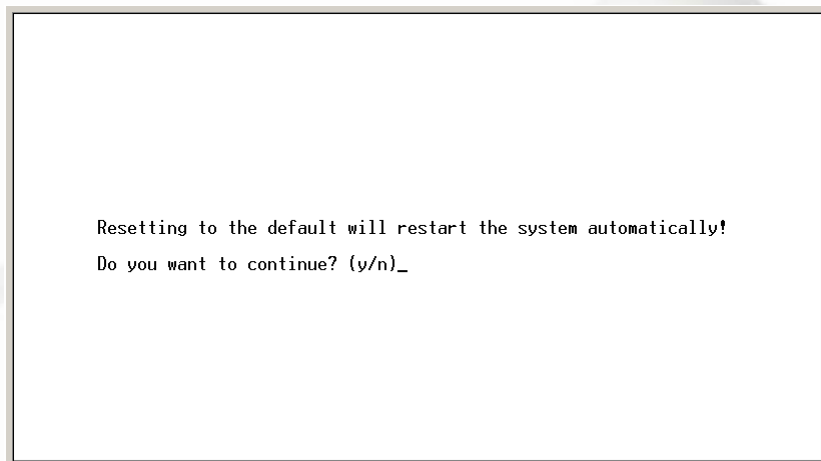
Display the switch system.
Esc=Previous menu
```

5. Reboot Switch



5.1 Default

Reset switch to default configuration.

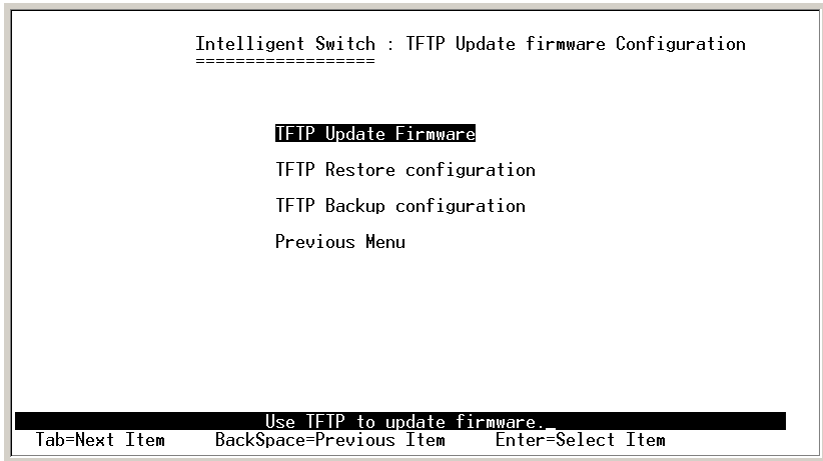


5.2 Restart

Reboot the switch in software reset.

6. TFTP Update Firmware

This page provides you to update firmware or restore EEPROM value or upload current EEPROM values.



6.1 TFTP Update Firmware

This page provides you use TFTP to update firmware.

1. Start the TFTP server, and copy firmware update version image file to TFTP server.
2. Press **<Edit>** on this page.
3. **TFTP Server:** Type the IP of TFTP server.
4. **Remote File Name:** Type the image file name.
5. Press **Ctrl+A** to go back action line.
6. Press **<Save>** key, it will start to download the image file.
7. When save successfully, the image file download finished too.
8. Restart the switch.

Intelligent Switch : TFTP Update Firmware	
=====	
TFTP Server	: 192.168.223.99
Remote File Name	: image.bin
actions-> <Edit> <Save> <Quit>	
Select the action menu.	
Tab=Next Item BackSpace=Previous Item Quit=Previous menu Enter=Select Item	

6.2 Update Configure File

In this page you can restore EEPROM values, save image file before, from TFTP server.

1. Start the TFTP server.
2. Press <Edit> on this page.
3. **TFTP Server:** Type the IP of TFTP server.
4. **Remote File Name:** Type the image file name.
5. Press **Ctrl+A** go to action line.
6. Press <Save> key, it will start to download the image file.
7. When save successfully, the image file download finished too.
8. Restart switch.

Intelligent Switch : Restore Configuration File
=====

TFTP Server : 192.168.223.99

Remote File Name : data.dat

actions-> <Edit> <Save> <Quit>

Select the action menu.

Tab=Next Item BackSpace=Previous Item Quit=Previous menu Enter=Select Item

6.3 Upload Configure File

In this page you can save current EEPROM values to image file. Then go to the update configure page to restore the EEPROM values.

1. Start the TFTP server.
2. Press **<Edit>** on this page.
3. **TFTP Server:** Type the IP of TFTP server.
4. **Remote File Name:** Type the image file name.
5. Press **Ctrl+A** go to action line.
6. Press **<Save>** key, it will start to upload the image file.
7. When save successfully, the image file upload finished too.
8. Restart switch.

Intelligent Switch : Backup Configuration File
=====

TFTP Server : 192.168.223.99
Remote File Name : data.dat

actions-> **<Edit>** **<Quit>**
Select the action menu.
Tab=Next Item BackSpace=Previous Item Quit=Previous menu Enter=Select Item

Troubleshooting

1. Power LED is not lit

Check if the power cord is properly connected to the power outlet and the switch. Make sure the power switch at the rear panel is turned ON.

2. Link LED is not lit when connected to the network device

- (1) Make sure the power switch of the network device is turned on
- (2) Check if the network cable is properly connected to the switch and the network device
- (3) Make sure the UTP cables comply with EIA/TIA 568 and Category 5 specification

3. Collision LED flashes constantly

- (1) Remove all the network cables; connect the cables back one by one to isolate the source of the collision.
- (2) Check the network cable, inferior cable quality will result in excessive collisions and packet errors.

[!] Contact your dealer if problems persist.