

**KYLAND**



## **WEB Management User Manual for SICOM L2 Industrial Ethernet Switches**

May 2010

Publisher: Beijing **KYLAND** Technology Co., Ltd.

Address: Chongxin Creative Building, Shixing East Street 18#,  
Shijingshan District, Beijing, China (100089)

Website: [www.kyland.cn](http://www.kyland.cn)

Tel: +86 -10-88798888

Fax: +86 -10-88796678

E-mail: [sales@kyland.cn](mailto:sales@kyland.cn)

Version: V1, May, 2009

No.: 27030041-10

# **WEB Management User Manual for SICOM L2 Industrial Ethernet Switches**

**Copyright © 2010 Beijing Kyland Technology Co., LTD.**

**All rights reserved.**

No part of this documentation may be excerpted, reproduced, translated, annotated or duplicated, in any form or by any means without the prior written permission of KYLAND Corporation.

# Content

<b>Chapter 1 Service Functions .....</b>	<b>8</b>
<b>Chapter 2 WEB Management Software .....</b>	<b>12</b>
2.1 Device Management.....	12
2.2 Device Status Display .....	14
2.2.1 Basic Information .....	14
2.2.2 Port Status .....	15
2.2.3 Port Statistics.....	16
2.2.4 Device Operating Information.....	17
2.3 Basic Configurations .....	18
2.3.1 Configuring IP Address .....	18
2.3.2 Configuring Device Info .....	19
2.3.3 Configuring Port.....	20
2.3.4 Change Password .....	21
2.3.5 Software Version .....	22
2.3.6 Software Update.....	23
2.3.7 Upload & Download Configuration.....	25
2.4 Advanced Configurations .....	27
2.4.1 Port Rate.....	27
2.4.2 VLAN.....	28
2.4.3 Port Mirroring .....	32
2.4.4 Port Trunk.....	33
2.4.5 Link Status Check .....	37
2.4.6 Static FDB Multicast.....	38

2.4.7 IGMP-snooping .....	40
2.4.8 ACL Configuration .....	42
2.4.9 ARP Configuration .....	45
2.4.10 SNMP Configuration .....	45
2.4.11 RSTP Configuration .....	46
2.4.12 RSTP Transparent Transmission .....	47
2.4.13 DT-Ring Configuration .....	49
2.4.14 QoS Configuration .....	54
2.4.15 MAC Aging Time .....	59
2.4.16 Alarm .....	59
2.4.17 RMON Configuration .....	62
2.4.18 Log Query .....	66
2.4.19 Unicast Address Configuration and Query .....	68
2.5 Device Management .....	70
2.5.1 Reboot .....	70
2.5.2 Logout .....	71
2.6 Save configuration .....	72
2.7 Load default .....	73
<b>Chapter 3 FTP Application for Switch Software Update .....</b>	<b>74</b>
3.1 WFTPD Software Configuration .....	74
3.2 Software Upgrade .....	76

## Chapter 1 Service Functions

The SICOM series layer 2 industrial Ethernet switches contains SICOM3000, SICOM3000BA, SICOM3004, SICOM3005, SICOM3006, SICOM3008J, SICOM3016, SICOM3024, SICOM3024P, SICOM3024SM, SICOM4000, SICOM8000 etc, which have the following common service functions:

### 1. LED Indicator

The LEDs (front panel) indicate the port status correctly including transmission rate, link status and system status.

### 2. Layer-2 Switching

Switches work in two ways: Cut-Through and Store-and-Forward. In Cut-Through, a data packet is immediately relayed further after detecting the target address; in Store-and-Forward, a data packet is first read-in completely and checked for errors before the switch relays the same. SICOM series employ Store-and-Forward that is a switching mode widely used.

### 3. VLAN

VLAN will divide one network into multiple logical subnets. Data packets cannot be transmitted between different VLANs so as to control the broadcast domain and segment flow and improve the reliability, security and manageability. IEEE802.1q VLAN tag is supported. It can be divided into up to 4094 VLANs based on ports. The VLAN division can be realized via WEB or console. Transparent transmission is supported for VLAN tag frames.

### 4. QoS

IEEE 802.1p is the most popular priority solution in the LAN environment. 802.1p, IP TOS and DSCP are all supported by SICOM series. In the case that none of the three priority solutions is supported by the terminal devices and different priorities needs to be assigned to different ports, QoS can be applied to configure the priority based on port. This function is effective on the received packets without priority fields. Each port of the SICOM series supports 4 priority queues with ID number of 0, 1, 2, and 3, which has the priorities of lowest->low->high->highest. QoS can be realized by configuring schedule and policy. There are three schedule policies supported by Kyland: port priority based, 802.1p based and IP TOS/DIFF based. These three policies are available for the different ports of the devices but mutually exclusive for one port.

### 5. Port Trunking

For SICOM series, multiple physical ports can be aggregated into one logic port, which has the same rate, duplex and VLAN ID. Port trunking can be configured in one single switch, the trunk group quantity differs according to different chips, and normally it is 2 or 4. Max 4 ports can be configured for each trunk group. This can reduce network traffic.

## 6. Port Mirroring

The data of one port can be mapped to another port for user to real-time monitor the communication.

## 7. Configure Port Working Modes

SICOM series is able to configure the working mode of all ports through management: adaptive, 10M/half-duplex, 100M/half-duplex, 10M/full-duplex, 100M/full-duplex and flow control etc

## 8. Configure Port Traffic Flow

You can configure the TX and RX rate of all ports via the management software of SICOM3024P. For port of 100Mbps, it can be set as 128K、256K、512K、1M、2M、10M、50M、100M. For Gigabit port, it can be set as 100M、500M、1000M.

For SICOM series, the port rate, port service, and broadcast of all ports can be controlled via the management, they are all actually rate limitation of traffic flow. Max 26 ports' rate can be restricted simultaneously, and the range of limited rate is from min 64Kbps to max 100000Kbps for 100Mbps port and 1000000Kbps for 1000Mbps port.

There are two groups for the rate limitation: group1 and group2, group1 is used to limit the rate especially for the service frames (defaults: unicast and multicast), and group2 is used to for other frames (defaults: broadcast, reserved multicast, unknown unicast and unknown multicast). Separate limitation is supported for service frames and broadcasting frames, which are limited in whole. The transmitted frames can also be limited in whole.

## 9. Static Multicast

It is more simple, reliable, less delayed, and no need for protocol to add the static multicast table, compared with dynamic multicast. The multicasting frames can be forwarded by configuring the static multicast forwarding table. The user can manually configure the multicast as needed. The static multicast can not be used together with IGMP simultaneously.

## 10. IGMP Snooping

IGMP Snooping (Internet Group Multicast Protocol Snooping) is employed to effectively restrict the spread of multicast data in layer 2 network. And it is mainly used for layer 2 devices with the

purpose of monitoring and analyzing IGMP messages. The mapping relation is established between port and multicast MAC, and based on this relation, the multicast data are forwarded. When the multicast data are received, the switch will know which port should receive the arriving multicast data and which port the data should be forwarded to.

### **11. DT-Ring**

DT-Ring is the proprietary communication protocol of Kyland. Via ring port status detection and less protocol messages, DT-Ring decides on the ring and port status to ensure a redundant ring network but no loop. This protocol can realize the fast and reliable Ethernet redundancy so as to better meet the requirements of the industrial communication.

### **12. DT-Ring+**

DT-Ring+ is the proprietary communication protocol of Kyland. This protocol realizes the redundancy and backup for two rings and meets higher requirements for the industrial communications.

### **13. RSTP**

RSTP and STP offer network redundancy protection for the switch network. RSTP can realize all the functions of STP, and additionally reduce the delay from block to forward, reconfiguring the network ASAP.

### **14. ACL**

ACL (Access Control Lists) is a data packets filtering mechanism to permit or deny specified data packets into/out of the network, by which the switch can control the network access and ensure the network security effectively. Based on specified messages, the user can set up a group of rules, which describe how to handle the appropriate packets: permit or deny. The user can apply the rules to the port ingress or egress, in this way, the traffic flow must be transmitted out of or into the switch according to the ACL rules.

### **15. Alarm**

Alarm is significant when it is used for real-time transmission of device alarm output. This function contains port alarm and ring alarm. Through management software, all the alarm functions can be set as enabled or disabled. The alarm information is available from management interface

### **16. SNMP**

SNMP (Simple Network Management Protocol) offers frame structure for low level

network management. SNMP protocol is used so widely that many kinds of networking devices, software and system employ it. It is easy to realize, open and free, and can be used to control various devices

### **17. RMON**

RMON is a standard monitoring regulation to exchange the network monitoring data between network monitor and console system. It offers more selections for network operator to use the suitable console and network monitor for special requirements. It is also the expansion to SNMP functions and is especially useful for monitoring and managing LAN. The purpose of developing RMON is to provide statistic result of information flow and analyze network parameters so as to work out a comprehensive diagnoses, plan and regulation.

With RMON function, the user can operate among multiple manufacturers for SNMP management and monitoring agent. What's more, it can offer a standard for a group of MIB to collect the network statistics which is unavailable via SNMP. RMON realizes previous network diagnoses by using powerful alarm group, it allows that a domain value is set for critical parameters so as to automatically send alarm signal to manager control center.

## Chapter 2 WEB Management Software

### 2.1 Device Management

Log in to Web Interface

Connecting the switch with a computer, enter the IP address like “192.168.0.2” in the IE browser, a window will appear as Figure 2-1, the default user name and password are “admin” and “123”. Click “OK” to enter into the main interface.

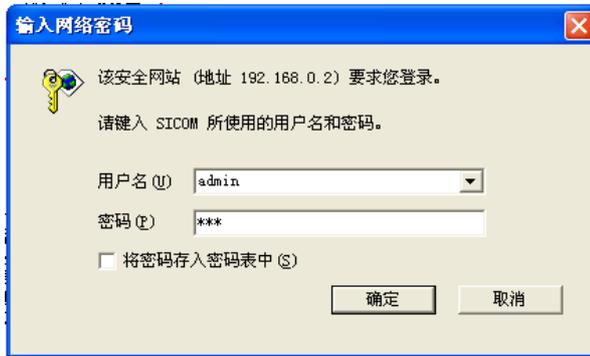


Figure 2-1 Login

The main page is as Figure 2-2

At the left of the page is the management tree menu including device state, basic configuration, advanced configuration, device management, save all changes. Restore default settings and so on. , each menu may include some submenu.

There are two function buttons: collapse and expand

Click on the expand button to display the main menu and all sub-menus.

Click on the collapse button to display main menu and collapse all the sub-menus.

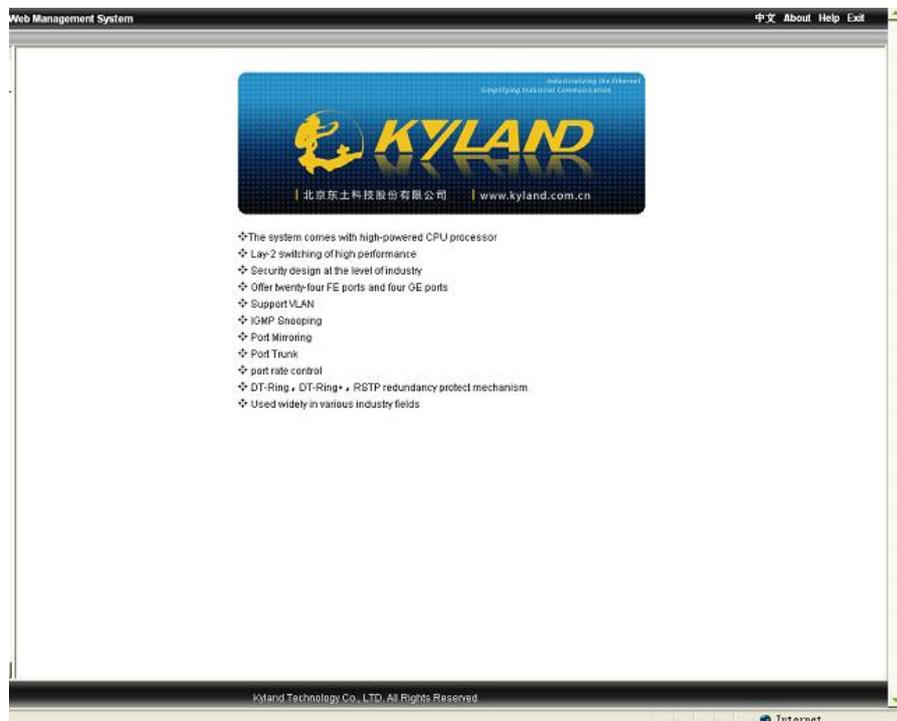


Figure2-2 Main Interface

## 2.2 Device Status Display

The menu of device status includes three submenus: Basic Information; Port status Port Traffic Flow.

### 2.2.1 Basic Information

Click “Basic info” and enter the interface as shown in Figure 2-3, which displays MAC address, IP address, software version etc.

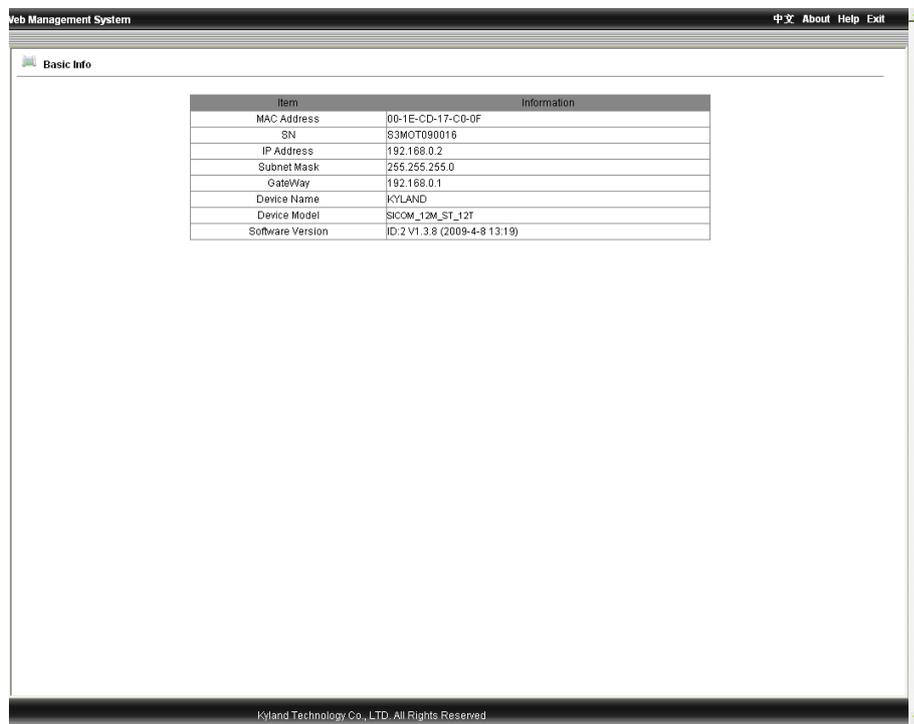


Figure 2-3 Basic Info

### 2.2.2 Port Status

Click “Port Status” and enter the page as shown in Figure 2-4, which displays the link state, port speed, full/half duplex and flow control state etc.

Port ID	State	Link	Bytes Sent	Packets Sent	Bytes Received	Packets Received	CRC Error	Packets < 64 bytes
FE1	Enable	Down	0	0	0	0	0	0
FE2	Enable	Down	0	0	0	0	0	0
FE3	Enable	Down	0	0	0	0	0	0
FE4	Enable	Down	0	0	0	0	0	0
FE5	Enable	Down	0	0	0	0	0	0
FE6	Enable	Down	0	0	0	0	0	0
FE7	Enable	Down	0	0	0	0	0	0
FE8	Enable	Down	0	0	0	0	0	0
FE9	Enable	Down	0	0	0	0	0	0
FE10	Enable	Down	0	0	0	0	0	0
FE11	Enable	Down	0	0	0	0	0	0
FE12	Enable	Down	0	0	0	0	0	0
FE13	Enable	Up	1643697	3565	394500	2624	0	0
FE14	Enable	Down	0	0	0	0	0	0
FE15	Enable	Down	0	0	0	0	0	0
FE16	Enable	Down	0	0	0	0	0	0
FE17	Enable	Down	0	0	0	0	0	0
FE18	Enable	Down	0	0	0	0	0	0
FE19	Enable	Down	0	0	0	0	0	0
FE20	Enable	Down	0	0	0	0	0	0
FE21	Enable	Down	0	0	0	0	0	0
FE22	Enable	Down	0	0	0	0	0	0
FE23	Enable	Down	0	0	0	0	0	0
FE24	Enable	Down	0	0	0	0	0	0
GE1	Enable	Down	0	0	0	0	0	0
GE2	Enable	Down	0	0	0	0	0	0
GE3	Enable	Down	0	0	0	0	0	0
GE4	Enable	Down	0	0	0	0	0	0

Reset

Kyland Technology Co., LTD. All Rights Reserved

Figure 2-4 Port Status

### 2.2.3 Port Statistics

Click “Port Statistics” and enter the page as shown in Figure 2-5 which displays the port flow statistics of each port.

Port ID	State	Link	Bytes Sent	Packets Sent	Bytes Received	Packets Received	CRC Error	Packets < 64 bytes
FE1	Enable	Down	0	0	0	0	0	0
FE2	Enable	Down	0	0	0	0	0	0
FE3	Enable	Down	0	0	0	0	0	0
FE4	Enable	Down	0	0	0	0	0	0
FE5	Enable	Down	0	0	0	0	0	0
FE6	Enable	Down	0	0	0	0	0	0
FE7	Enable	Down	0	0	0	0	0	0
FE8	Enable	Down	0	0	0	0	0	0
FE9	Enable	Down	0	0	0	0	0	0
FE10	Enable	Down	0	0	0	0	0	0
FE11	Enable	Down	0	0	0	0	0	0
FE12	Enable	Down	0	0	0	0	0	0
FE13	Enable	Up	1643697	3565	394500	2624	0	0
FE14	Enable	Down	0	0	0	0	0	0
FE15	Enable	Down	0	0	0	0	0	0
FE16	Enable	Down	0	0	0	0	0	0
FE17	Enable	Down	0	0	0	0	0	0
FE18	Enable	Down	0	0	0	0	0	0
FE19	Enable	Down	0	0	0	0	0	0
FE20	Enable	Down	0	0	0	0	0	0
FE21	Enable	Down	0	0	0	0	0	0
FE22	Enable	Down	0	0	0	0	0	0
FE23	Enable	Down	0	0	0	0	0	0
FE24	Enable	Down	0	0	0	0	0	0
GE1	Enable	Down	0	0	0	0	0	0
GE2	Enable	Down	0	0	0	0	0	0
GE3	Enable	Down	0	0	0	0	0	0
GE4	Enable	Down	0	0	0	0	0	0

Reset

Kyland Technology Co., LTD. All Rights Reserved

Figure 2-5 Port Statistics

### 2.2.4 Device Operating Information

Click “Device Operating Information”, and enter the page as Fig2-6 which displays the device operating time, CPU, device temperature and system time etc.

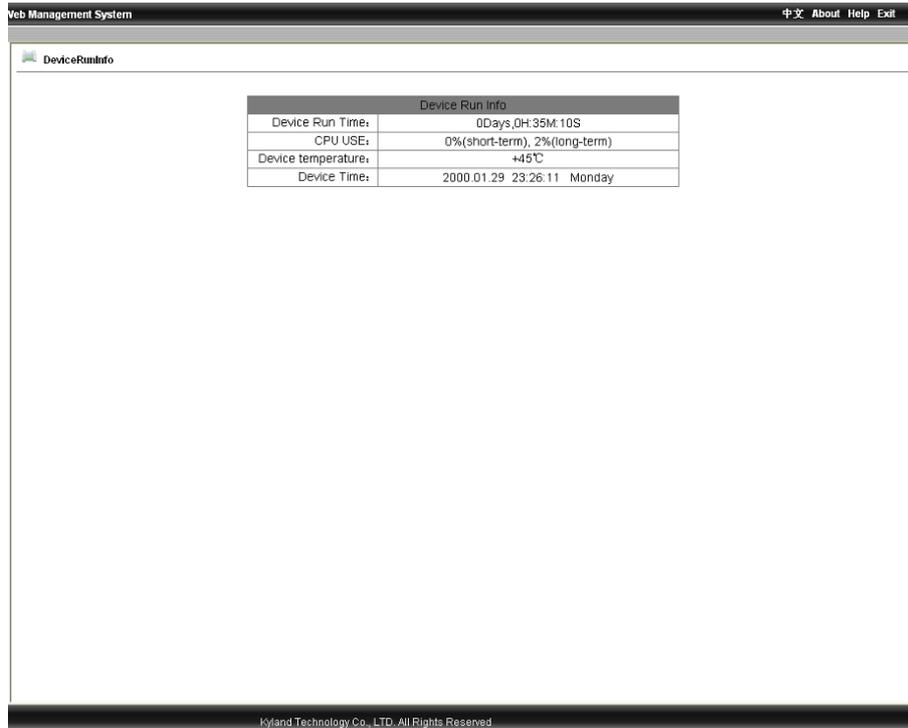


Figure2-6 Device Operating Information

In the menu of “Device”, there are functions to configure IP address, device name, port, to change password, query software version and upgrade software etc.

## 2.3 Basic Configurations

In the menu of “Device”, there are functions to configure IP address, device basic information, port, to change password, query software version and upgrade software, set uploading/downloading etc.

### 2.3.1 Configuring IP Address

Click the “IP address” in the left menu and enter the page (as Figure 2-7), where the user can modify IP address, subnet mask and gateway with click on “Apply” button. To make the modification take effect, the device needs to be reset.

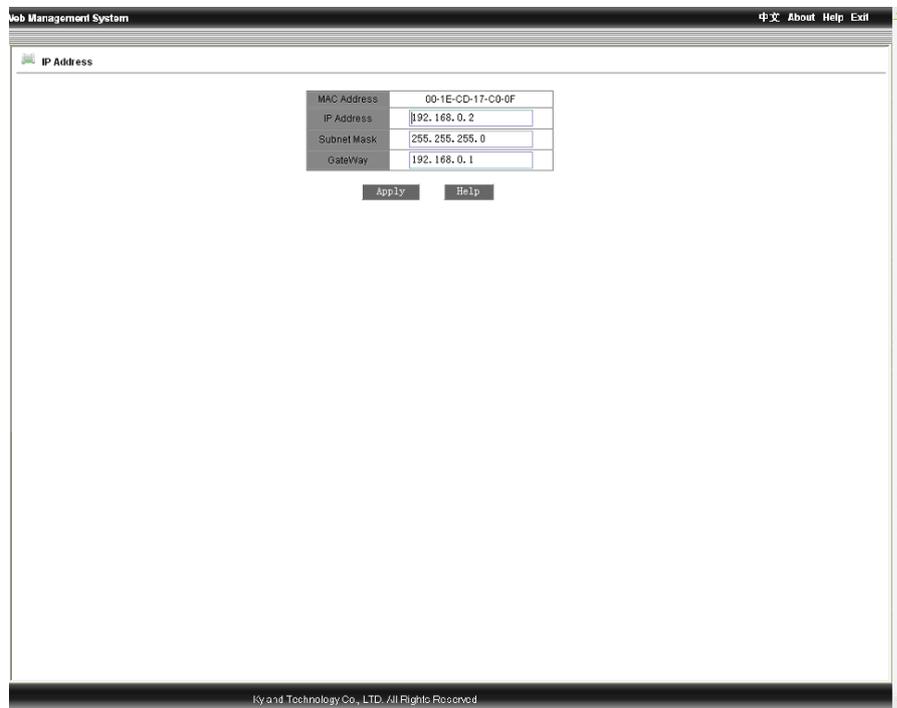


Figure2-7 Configuring IP Address

### 2.3.2 Configuring Device Info

Click the “Device Info” in the left menu and enter the page (as Figure 2-8), enter the project name, device name, system time and click “Apply” button.

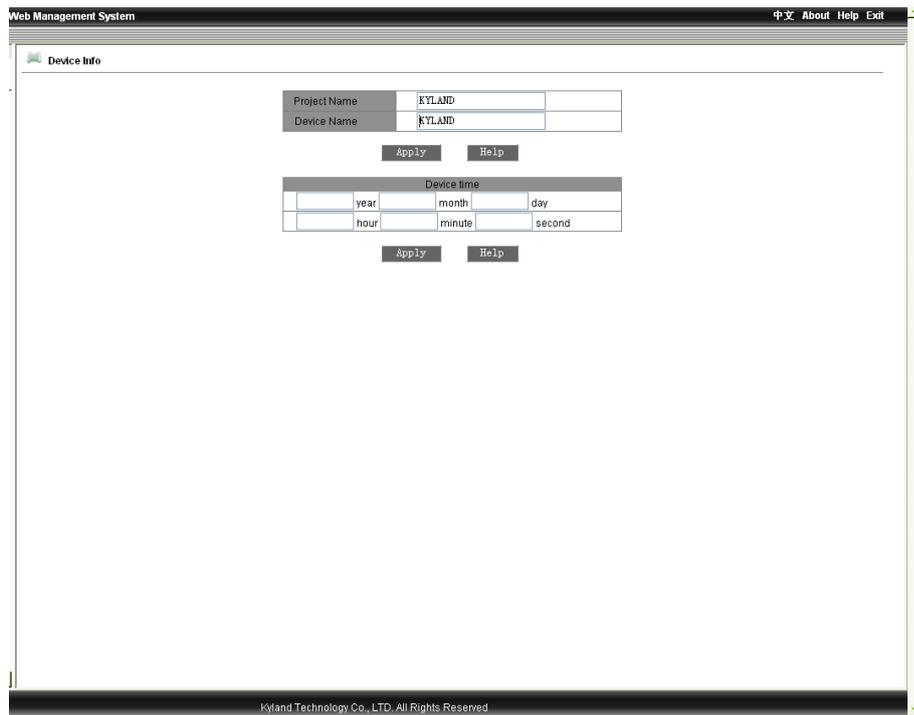


Figure 2-8 Device Info

### 2.3.3 Configuring Port

Click the “Port Configuration” in the left menu and enter the page (as Figure 2-9), where the user can configure port administration status (enable/disable), operation status(enable/disable), auto-negotiation (enable/disable), port speed (10/100M), duplex (full/half), flow control (open/close), reset (reset/no reset). After configuration, click “Apply” to make it take effect. For FX port, the auto-negotiation is disabled; port is forced to be 100M and full-duplex.

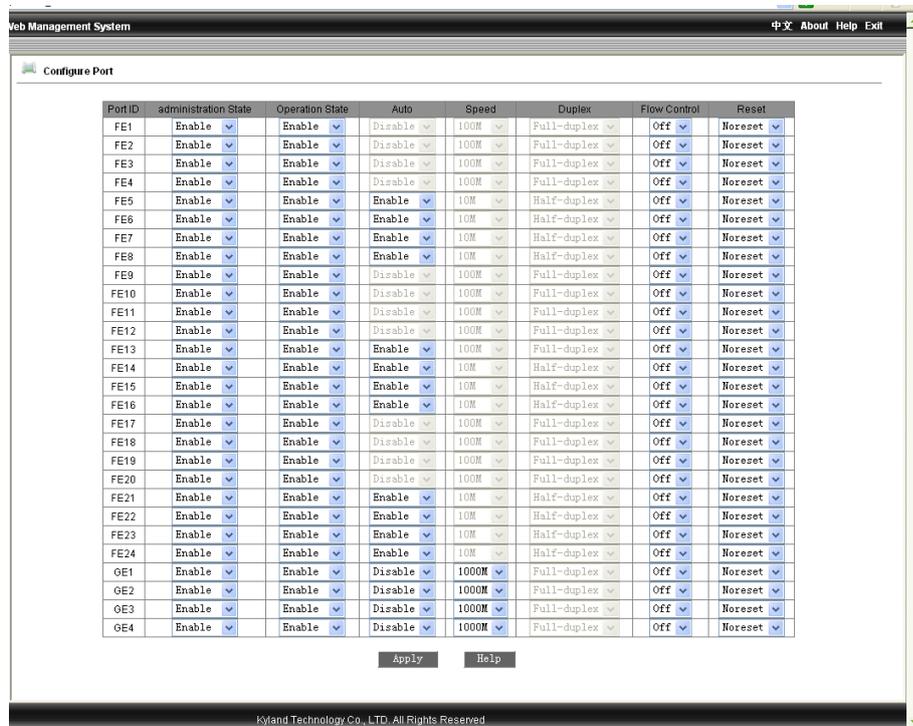


Figure 2-9 Port Configurations

### 2.3.4 Change Password

Click the “Change Password” in the left menu and enter the page (as Figure 2-10), enter old password and new password, click “Apply” to take effect.

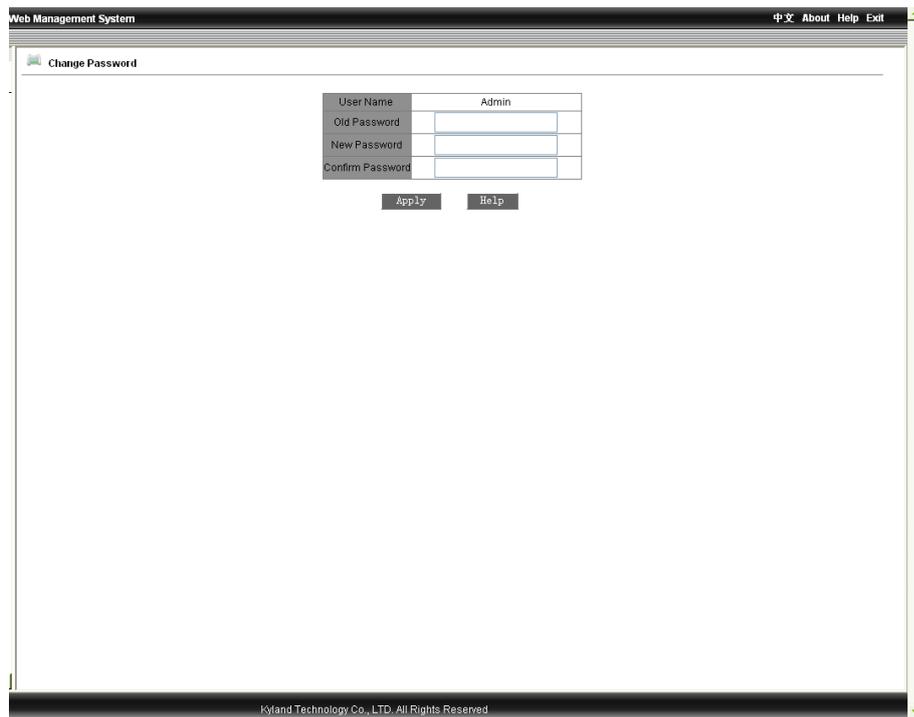


Figure 2-10 Change the password

### 2.3.5 Software Version

Click the “Software Version” in the left menu and enter the page (as Figure 2-11), which displays two versions: one is startup and another is not closed. This function is for the purpose of upgrading software.

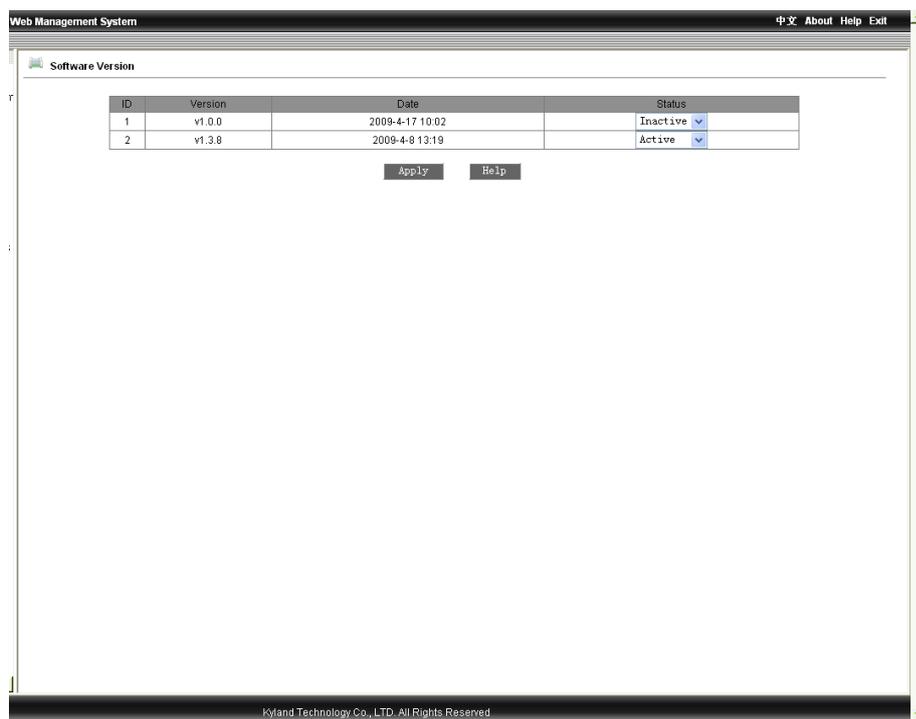


Figure 2-11 Software Version

### 2.3.6 Software Update

Click the “Software Update” in the left menu and enter the page (as Figure 2-12). For detailed upgrading instructions, please refer to the Appendix D.

Enter the main WEB page, and click “upgrading bar” of basic configuration in navigation bar to enter into the upgrading page as shown in the following Figure:

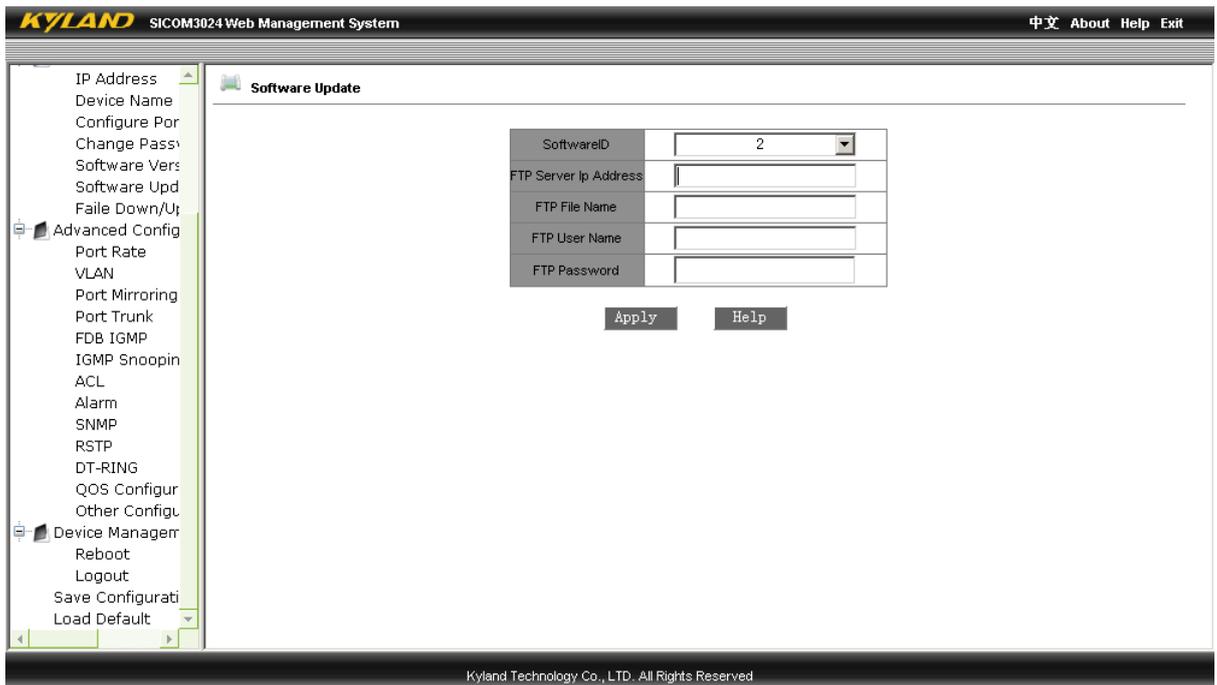


Figure2-12 Software Update

Set IP address, user name, password and software name of the FTP server, click “Apply” button and record upgraded software ID. The FTP address must be in the same network segment with the switch IP address.

Wait for upgrading and see the successful message.

Click “Software Version” in navigation bar, set the software ID as startup version and click “OK” as shown in the Figure 2-11 of software version.

Click “reset” in the navigation bar and click “rest.”

Wait for 30 seconds to start up network management system. Click “Device Basic Info”, check software version to confirm if it is upgraded successfully.



Figure 2-12-2 Reset

### 2.3.7 Upload & Download Configuration

Click and select the “Upload & Download” in the left menu and enter the page (as Figure 2-13 and 2-14), where enter the server IP address and the uploaded/downloaded file name, username, password,, click “Apply” to finish. Please refer to the software update details.

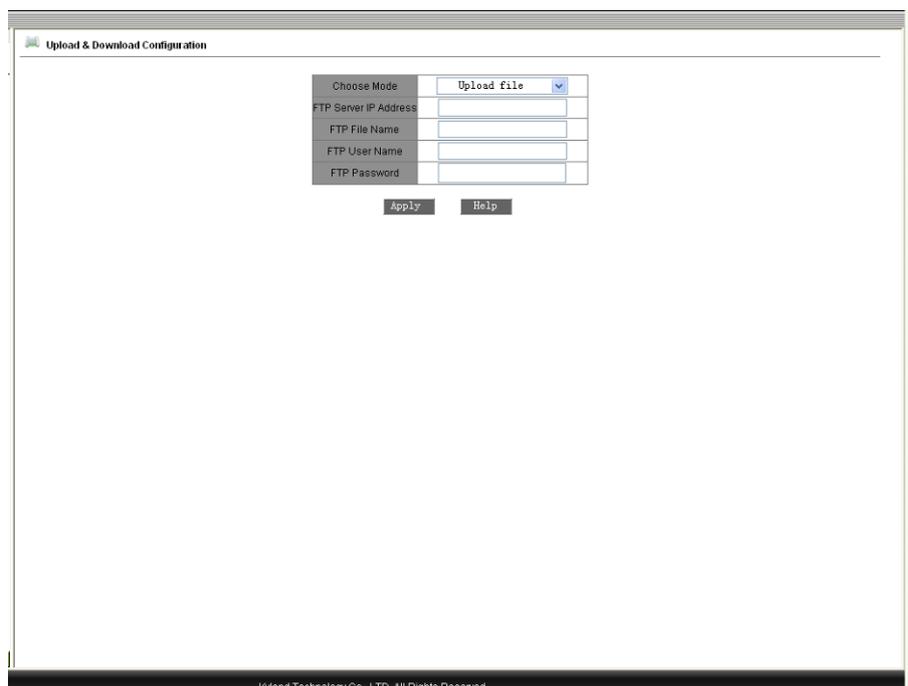


Figure 2-13 Upload

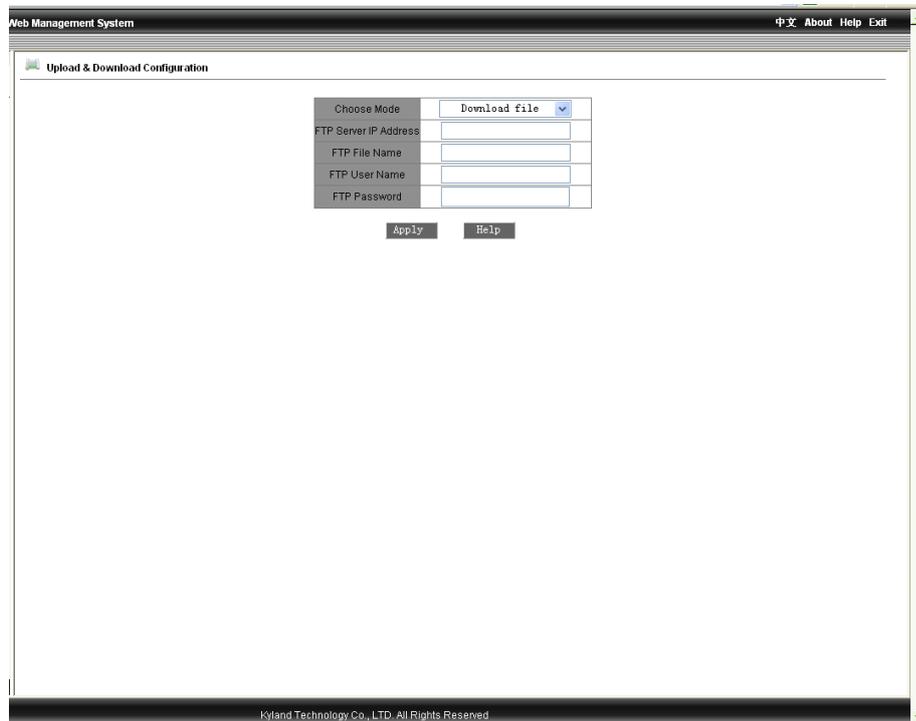


Figure 2-14 Download

## 2.4 Advanced Configurations

The advanced configurations contains port rate, VLAN, port mirroring, port trunk, link check, static multicast, IGMP snooping, ACL, ARP, SNMP, RSTP, RSTP transparent transmission, DT-Ring, QoS, MAC aging time, alarm, RMON, log query(only for SICOM3024P, SICOM3024PT), unicast query and configuration etc.

### 2.4.1 Port Rate

Click the “Port Rate” in the left menu and enter the page (as Figure 2-15), select packet type (defaults are: unicast and multicast for service packets; broadcast, reserved multicast, unknown unicast and unknown multicast for broadcast packets) from the restricted packets table. From this page, the user can configure the service restriction, broadcast restriction and transmission rate for each port. The restriction range is 64K~ 100000Kbps for fast Ethernet port and 64K~1000000Kbps for Gigabit port. When it is 0, the restriction is disabled. After all settings are finished, click on the “Apply” button.

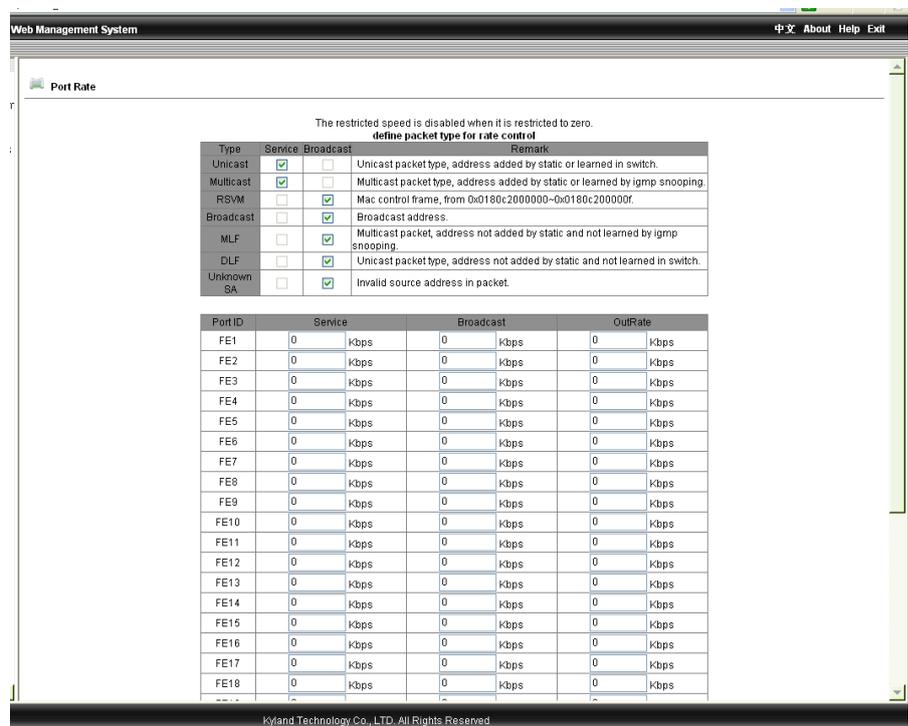


Figure 2-15 Port Rate

### 2.4.2 VLAN

Click the “Configure VLAN” in the left menu and enter the page (as Figure 2-16) and select transparent enable or disable for the VLAN mode, click “Add” to enter into the page as Figure 2-17. Enter VLAN name, ID (VLAN1 is the default), select VLAN member, tag or untagged, click “Apply” to finish configuration. In the case of Untagged, the user can configure the priorities from 0 to 7 for port, and in the case of tagged, the user can set PVLAN enable/disable for the port. The operation can be done according to the instructions.

---

 **Note: in the default state, VLAN ID is “1”; the range of ID no. is from 2 to 4093.**

#### **Instructions:**

All the ports of uplink domain must be added to the shared domain VLAN in untagged mode;

All the ports of isolated domain must be added to the shared domain VLAN in tagged mode;

All the ports of isolated domain must be added to the isolated domain VLAN in untagged mode;

All the ports of uplink domain must be added to the isolated domain VLAN in the tagged mode;

Add all uplink port domain and isolated domain VLAN to the PVLAN.

---

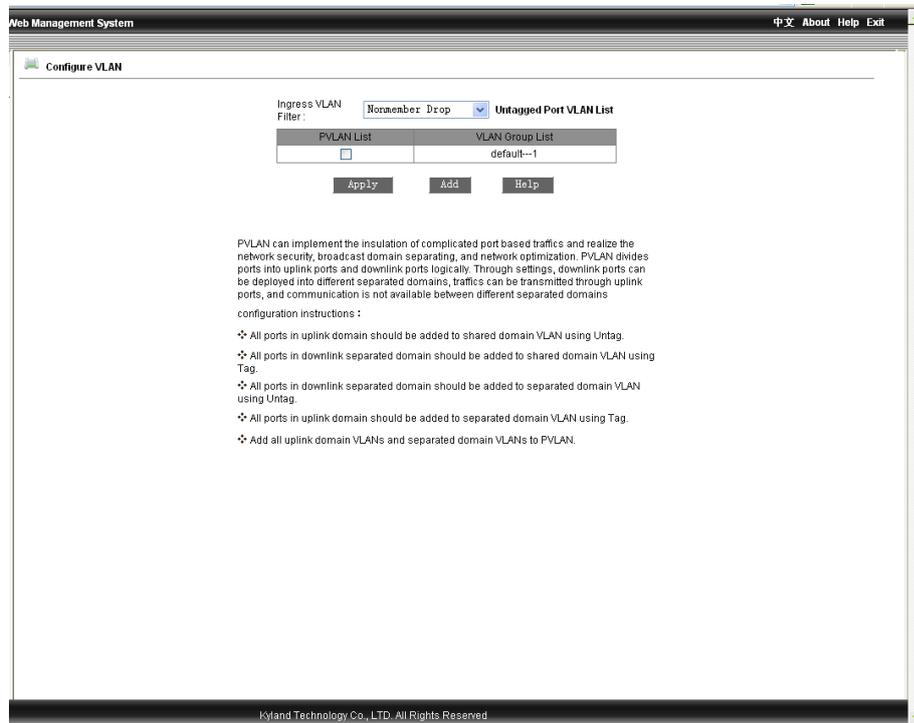
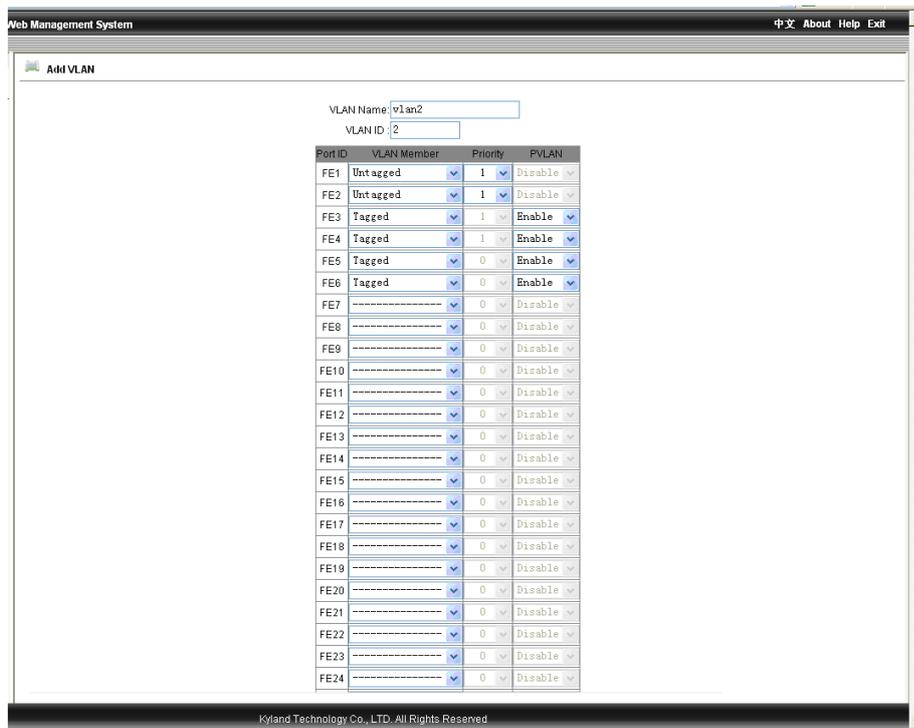
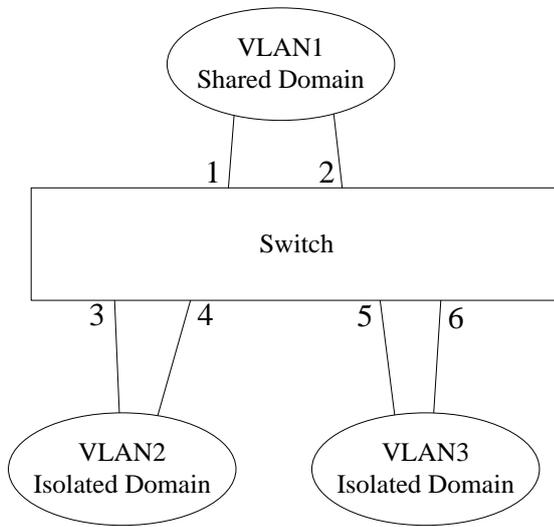


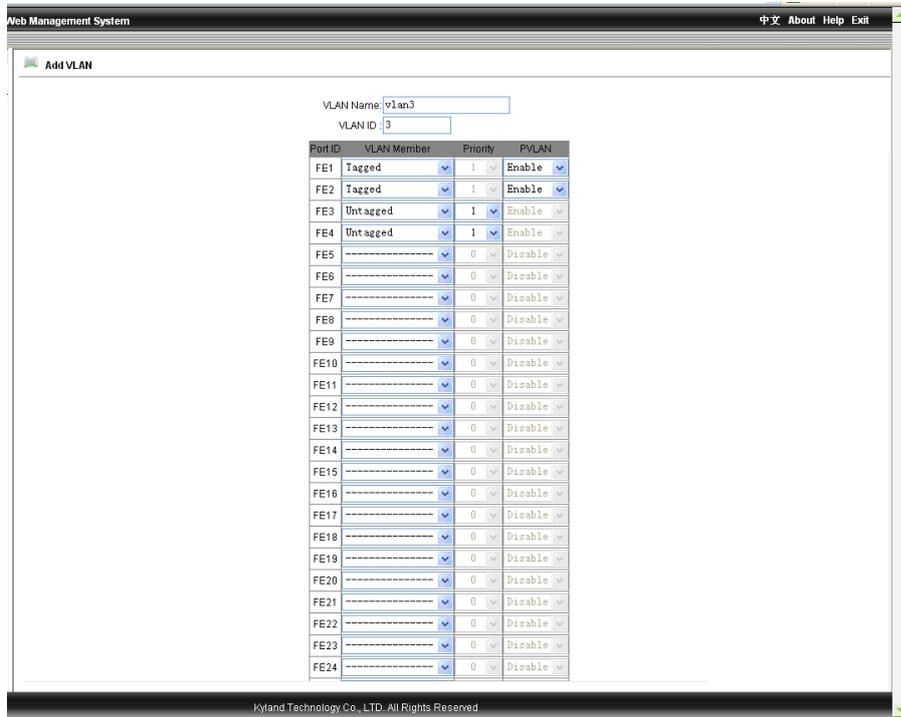
Figure 2-16 Add VLAN

EX: define FE1/FE2 as uplink ports, FE3/FE4 and FE5/FE6 as isolated ports.

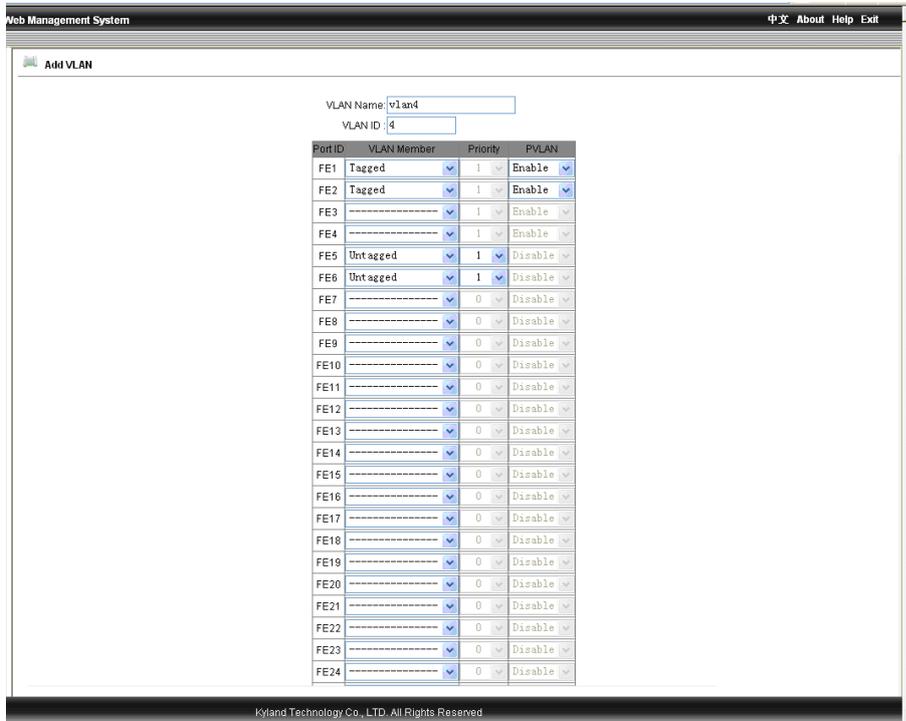
The uplink ports FE1/FE2 can set into shared domain, FE3/FE4 and FE5/FE6 can be set into different isolated domains; Add all uplink port domain VLAN and isolated VLAN to the PVLAN. FE3/FE4 and FE5/FE6 can communicate with FE1/FE2. FE3/F4 can not communicate with FE5/FE6.



(a) Configure VLAN of shared domain (FE1/FE2)



(b) Configure VLAN of isolated domain (FE3/FE4)



(c) Configure VLAN of isolated domain (FE5 /FE6)

Figure 2-17 VLAN Configuration

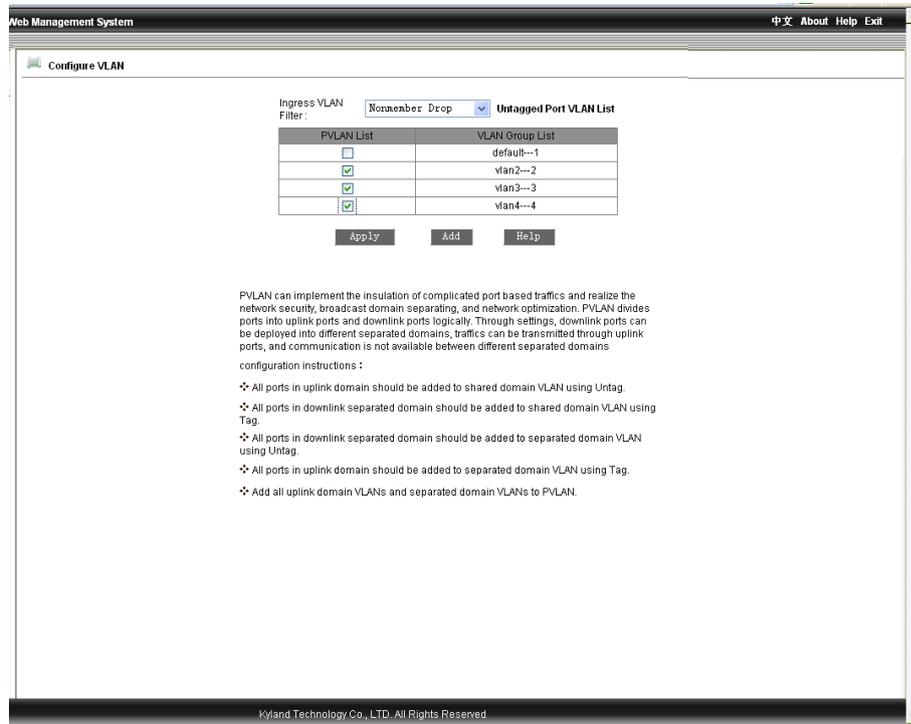


Figure 2-18 VLAN Configuration Finished

(Add all uplink port VLAN and isolated VLAN to PVLAN)

### 2.4.3 Port Mirroring

Click the “Port Mirroring” in the left menu and enter the page (as Figure 2-19), select mirroring port from range of port1~port48、G0、G1 and mirrored port from the range of TX、RX、TX&RX, click “Apply” to finish configuration.

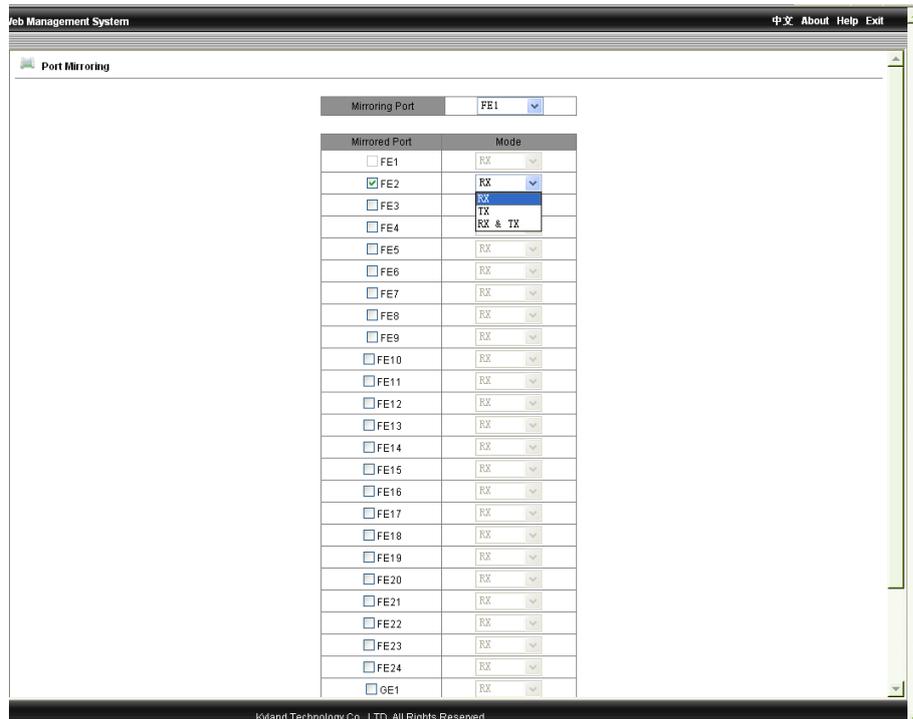


Figure 2-19 Port Mirroring

### 2.4.4 Port Trunk

Click the “Port Trunk” in the left menu and enter the page (as Figure 2-20), six trunk groups are supported and max 4 ports can be added to the each group. Click , , to add or delete aggregated port. Click “Apply” to finish configuration.

 **Note:**

Port trunk means multiple physical ports are used as one logical forwarding port, which will not only widen the network bandwidth but also offers backup function to the link. Only the ports in the same VLAN can be aggregated and the configurations of all ports in the same trunk group should be accordant.

The ports of 1-4 of switch S1 are aggregated into one trunk, whose bandwidth is the sum of the bandwidth of the 4 ports. At S1, if there are frames to go through trunk to S2, the port trunk of S1 will calculate the frames allocation according to the minimum value of the source MAC

---

address and target MAC address, and decide which port of the trunk transmit the frames. In the case that one port of the trunk fails in connection, the frames, which should have been transmitted by the port, will be assigned to the other ports in the trunk according to the calculation. The algorithm depends on the switch's hardware.

---

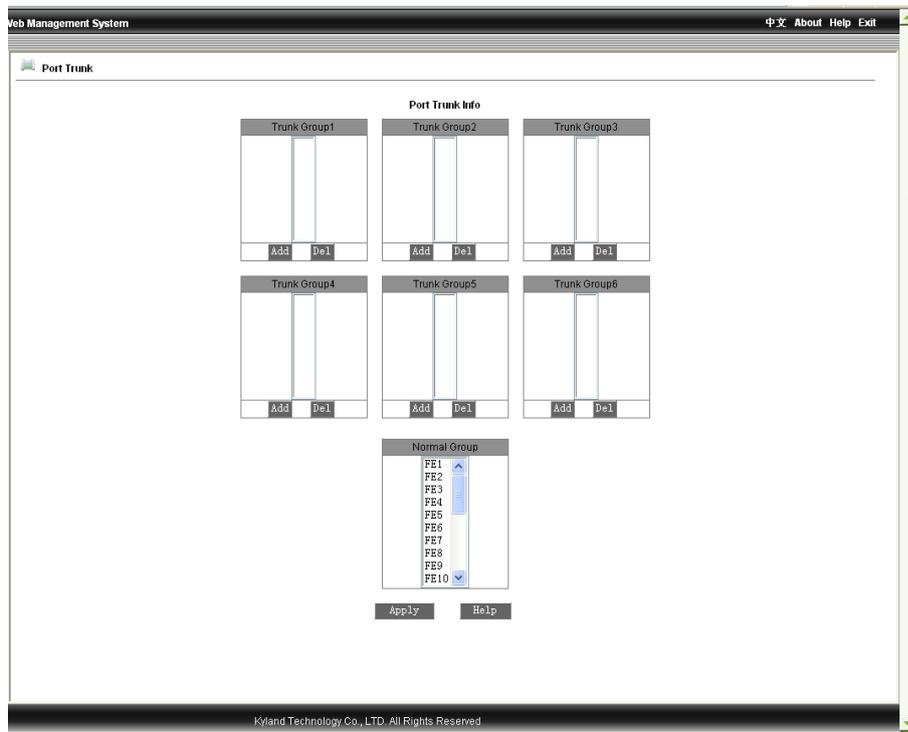
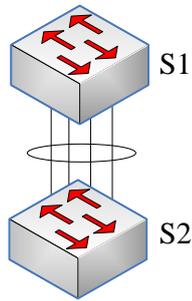


Figure 2-20 Port Trunk Configuration

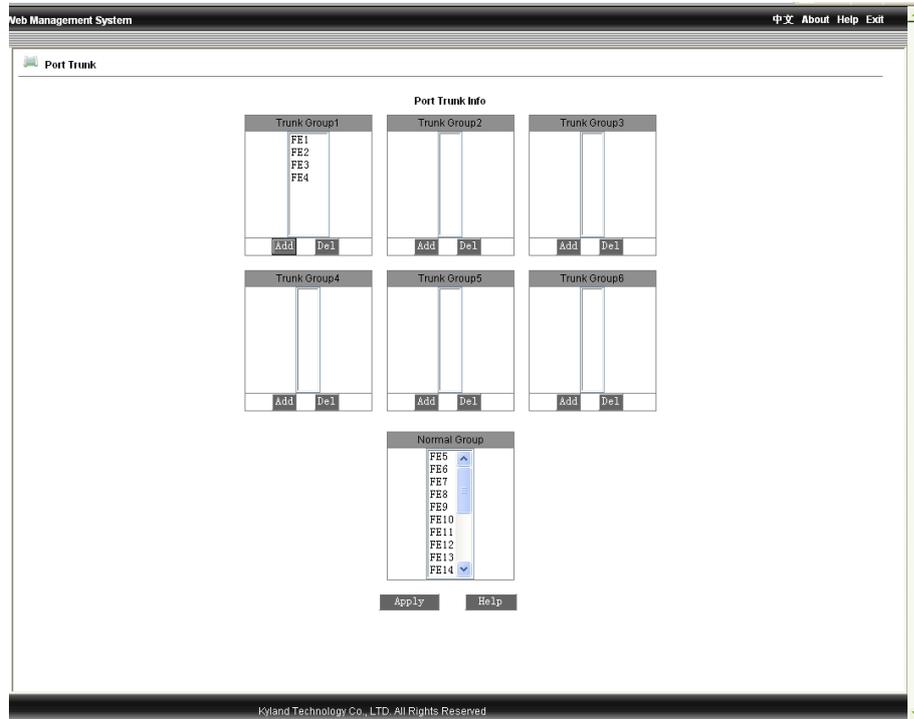


Figure 2-21 Port Trunk Configuration Graphic

### 2.4.5 Link Status Check

Click the “Link Check” in the left menu and enter the page (as Figure 2-22), after configuring “RSTP”, “STP” or “DT-ring”, where the user can configure the link check as “disable” or “enable”, click “Apply” to finish. Click again the “Port Trunk” in the left menu to view the link status as Figure 2-23.

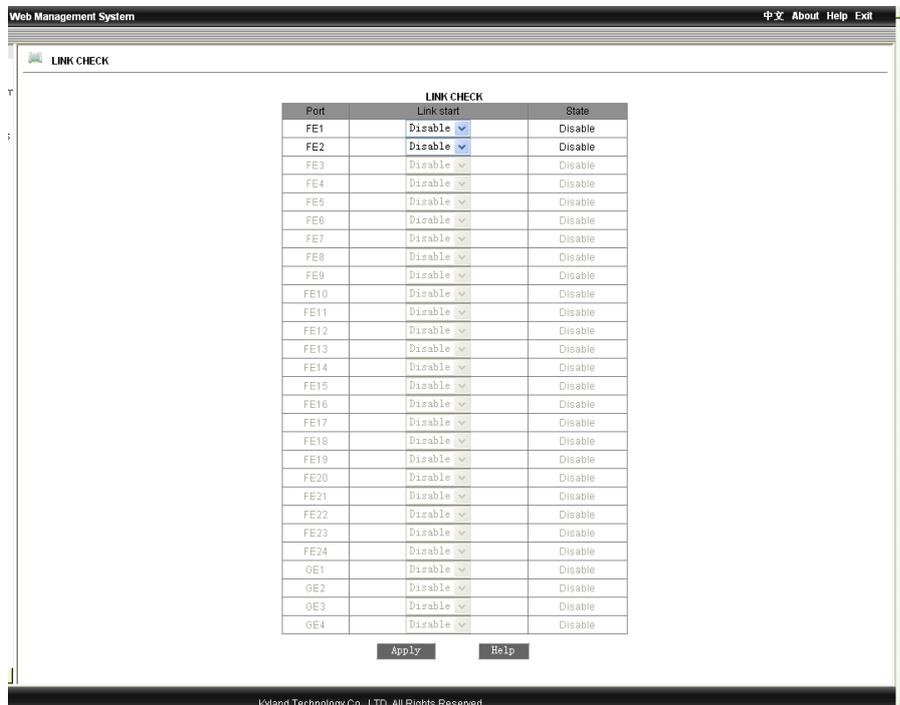


Figure 2-22 Link Status Configuration

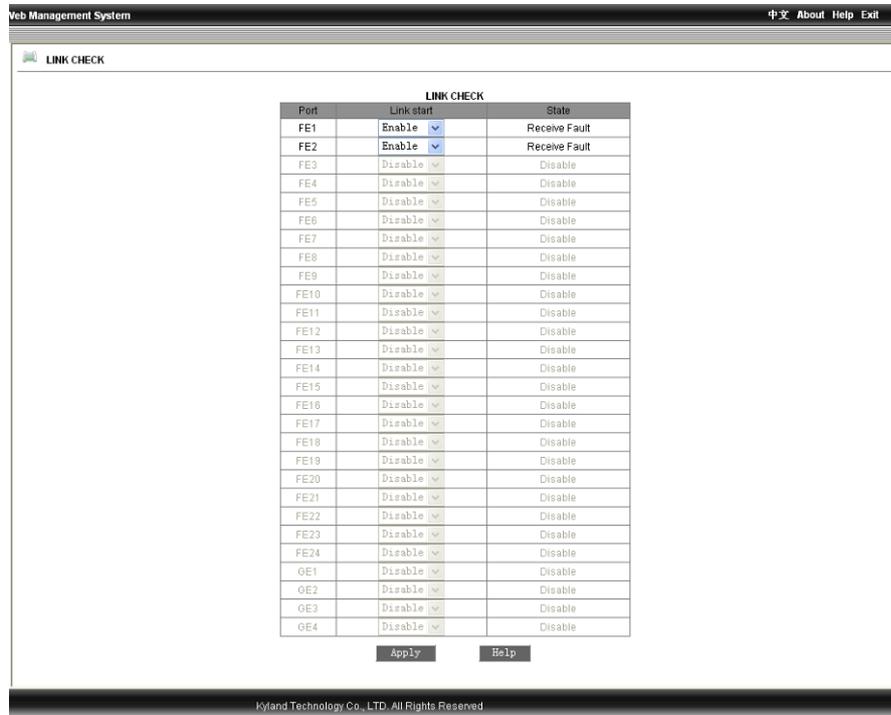


Figure 2-23 View Link Status Check

### 2.4.6 Static FDB Multicast

Click the “Static FDB Multicast” in the left menu and enter the page (as Figure 2-24), where the user can select multicast filtering mode: unknown dropped or unknown transmit, FDB multicast is enabled, click “Apply” to finish. Add static MAC address, VLAN id and select port from the page as Figure 2-25, and click “Apply” to finish. After the configurations, click the “Static FDB Multicast” in the left menu and enter the page as Figure 2-26, to configure static multicast address, just select the item no. in the table and click “Modify” to reset the port table. To delete the address, click “Delete”.



Attention: “IGMP Snooping” must be disabled before enable static multicast.

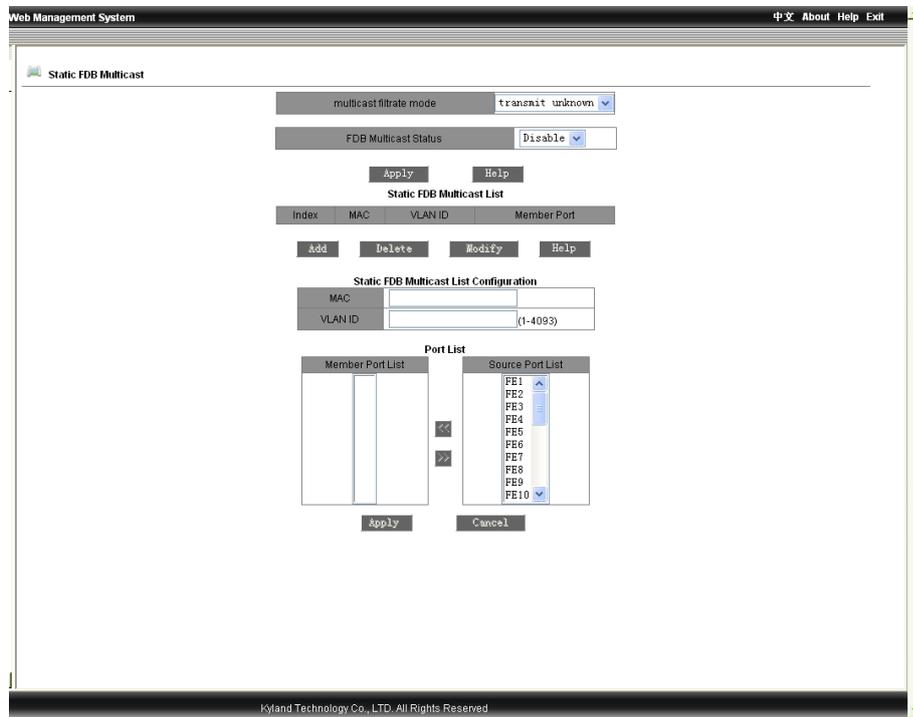


Figure 2-24 Static FDB Multicast

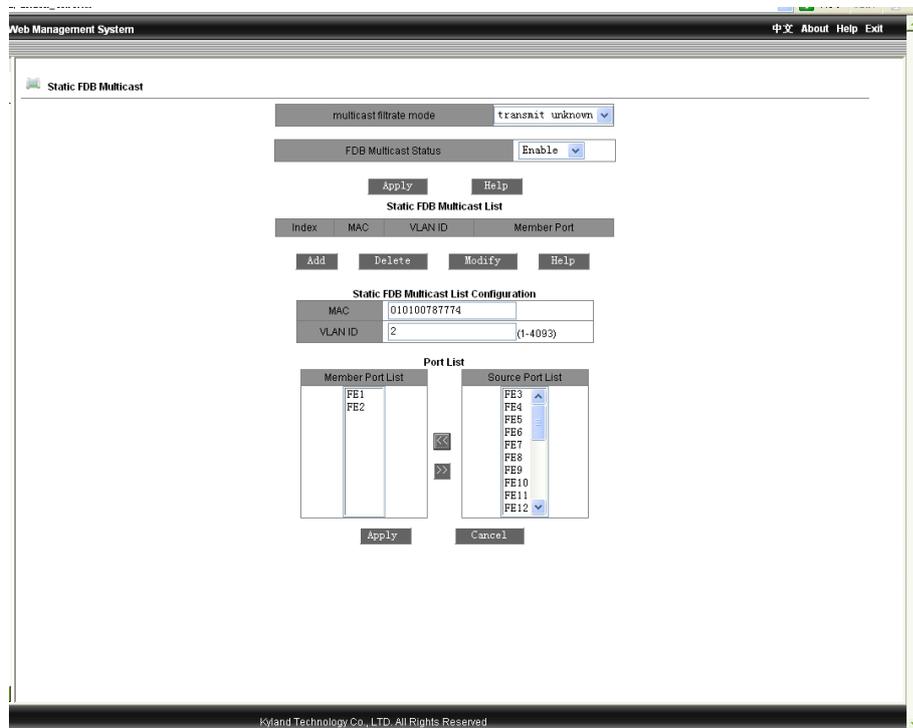


Figure 2-25 Static FDB Multicast Graphic

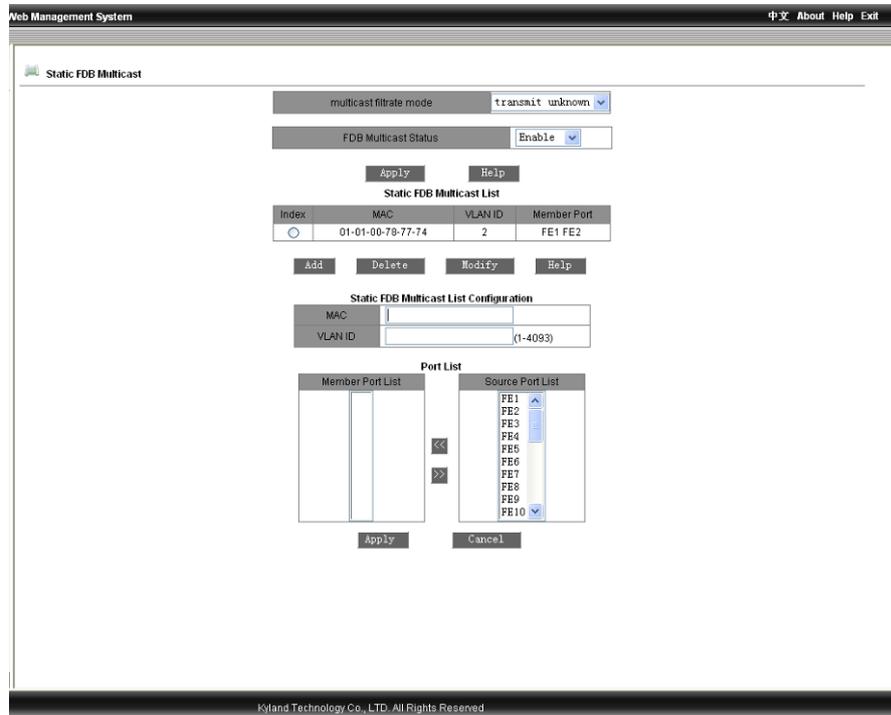


Figure 2-26 Successful Configuration of Static Multicast

### 2.4.7 IGMP-snooping

Click the “IGMP-SNOOPING” in the left menu and enter the page (as Figure 2-27), enable IGMP-SNOOPING and auto query, click “Apply” to finish configuration. Click again the “IGMP-SNOOPING” in the left menu to display the configuration results.



Attention: Disable the static FDB multicast before enable IGMP Snooping. Max 256 multicast addresses are supported, note this range during operation.



Figure 2-27 IGMP-SNOOPING

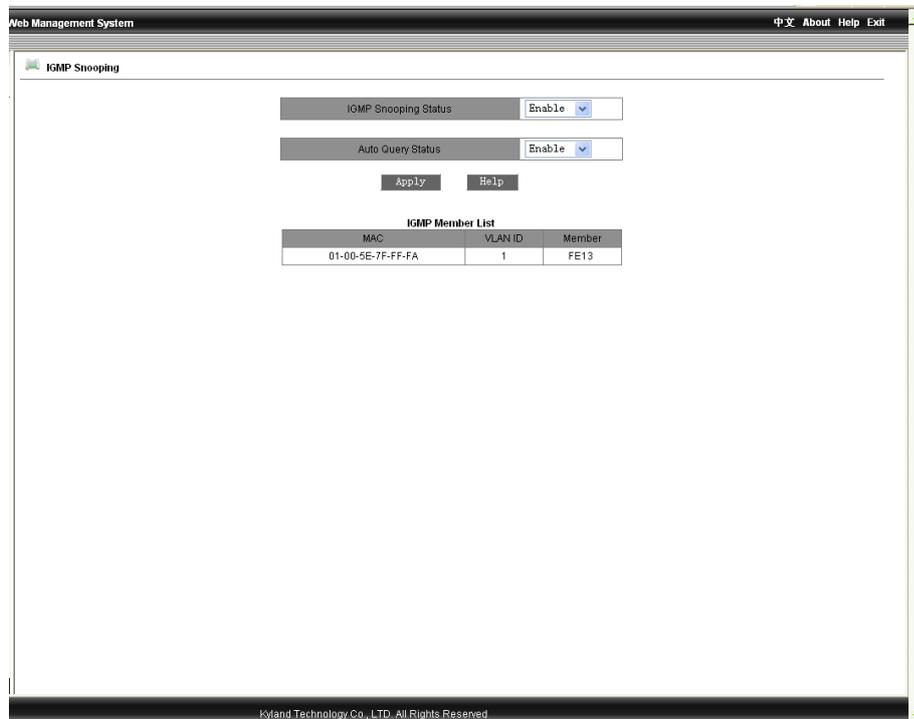


Figure 2-28 Successful Configuration

### 2.4.8 ACL Configuration

Click the “ACL Configuration” in the left menu and enter the page (as Figure 2-29), click port to enter the page as Figure 2-30, select enable/disable to click “Apply” to finish. Click “Add” to enter the page as Figure2-31, select the group no. and item no.(0-512), action(“deny/change port/add port), control port (all ports//FE1~FE24,GE1~GE4), source MAC, destination MAC, Ethernet Type, and VLAN, click “Apply” to finish.

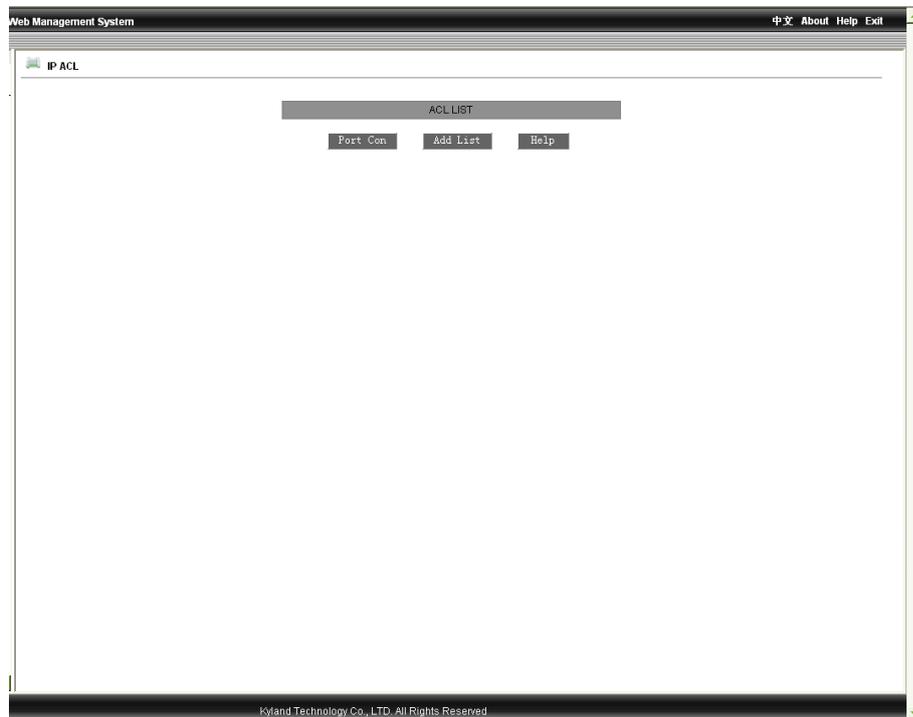


Figure 2-29 IP ACL

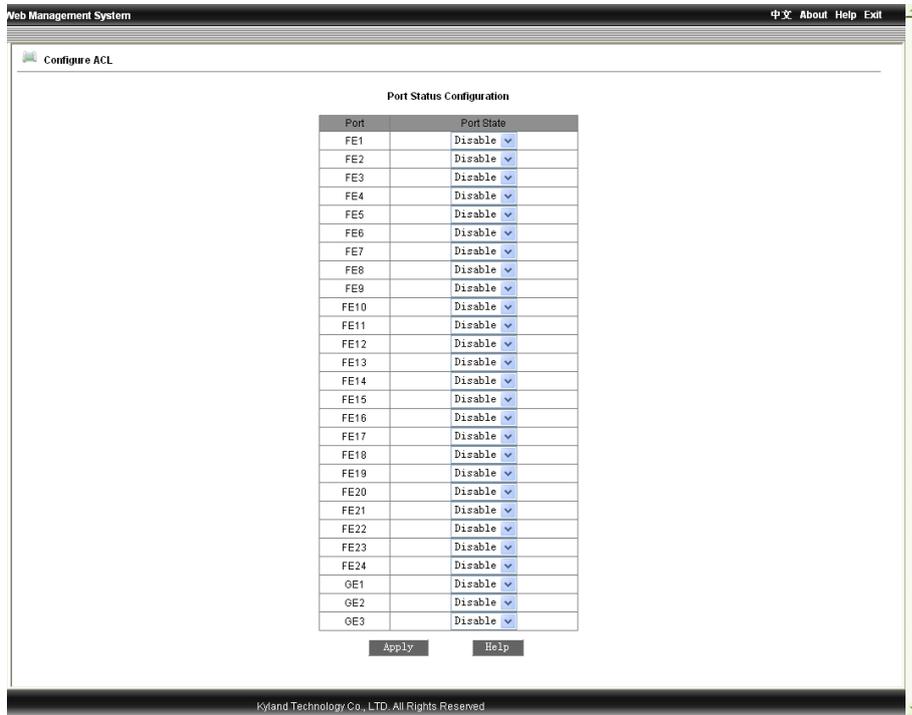


Figure 2-30 Port Configuration

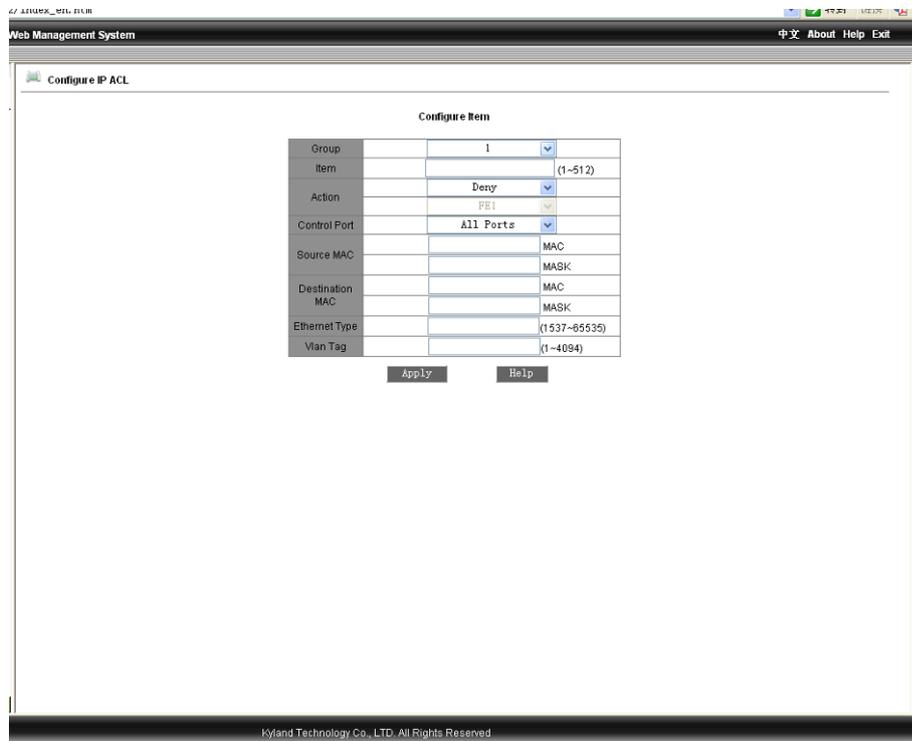


Figure 2-31 Protocol Configuration



### 2.4.9 ARP Configuration

Click the “ARP” in the left menu and enter the page (as Figure 2-32), configure the ARP aging time and click “Apply” to finish. Then configure the ARP address including IP, MAC, and click the “Apply” to finish. Select item no. in the list and click “Delete” to delete the ARP address.

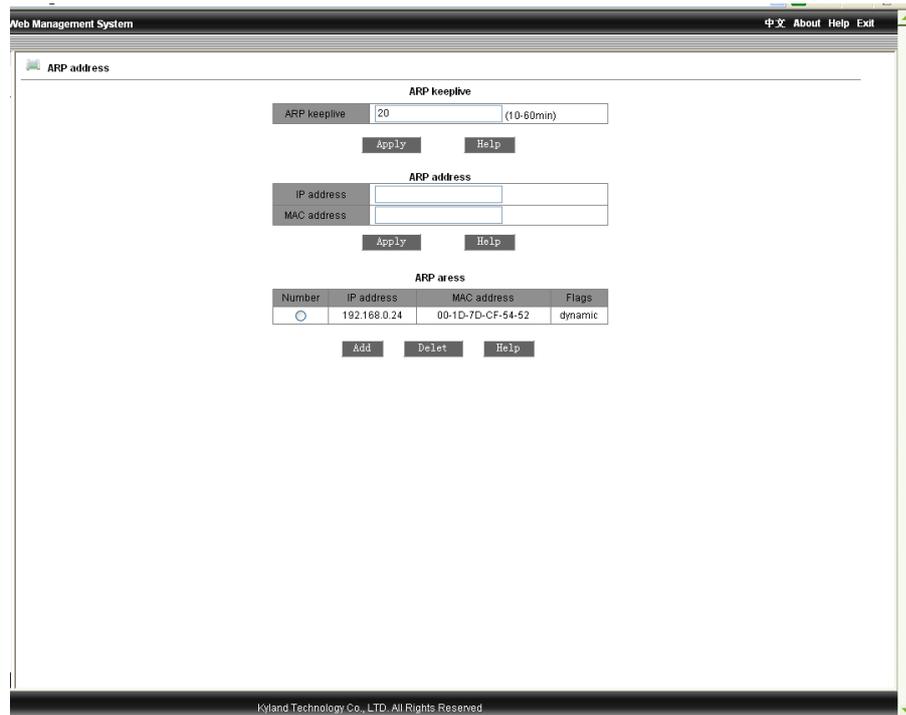


Figure 2-32 ARP Configuration

### 2.4.10 SNMP Configuration

Click the “SNMP” in the left menu and enter the page (as Figure 2-33), enable SNMP, set read-only and read-write group name, select trap server IP address, select trap port no, click “Apply” to finish. The device will accept the frames which match with the group name of read-only and read-write. The device will send the trap frames to the IP address in the trap IP address list. Only on the trap port can the administration station receive the trap frames.



Figure 2-33 SNMP Configuration

### 2.4.11 RSTP Configuration

Click the “RSTP” in the left menu and enter the page (as Figure 2-34), select RSTP or STP to configure. Set Spanning Tree Priority(range: 0-65535,default: 32768,step size: 4096),Hello Time(range: 1-10, default: 2),Max Age Time (range: 6-40, default: 20),Forward Delay Time (range: 4-30,default: 15),Message-age inc(default or compulsion),click “Apply” to finish. Additionally, the protocol status, priority and path cost of each port can be configured too.

-----

 Attention:

The DT-Ring contains port-based ring and VLAN-based ring. The former can be used together with RSTP simultaneously and the latter can not.

-----

The device’s bridge priority and MAC address compose the bridge ID, by which RSTP decided on the root bridge and root port. The less priority level, the more priority, the device with the lowest bridge ID will be chosen as the root bridge. The bridge priority is set as the lowest but can

be forced to be the root bridge. In the cast of the same priorities, the one with lowest MAC address is the root bridge.

Forward Delay Time, Max Age Time, Hello Time should accord with the rules:  $2 \times (\text{Bridge\_Forward\_Delay} - 1.0 \text{ seconds}) \geq \text{Bridge\_Max\_Age}$   $\text{Bridge\_Max\_Age} \geq 2 \times (\text{Bridge\_Hello\_Time} + 1.0 \text{ seconds})$ .

The port path cost is the path expenses of the port link, and used to calculate the shortest path, which depends on link bandwidth. The more bandwidth, the less link cost. The forwarding path from current device to root port can be changed by changing port link cost.

The port priority and port no. compose the port ID, which is used for the root port selection calculation. The smaller the port ID is, the more priority it has.

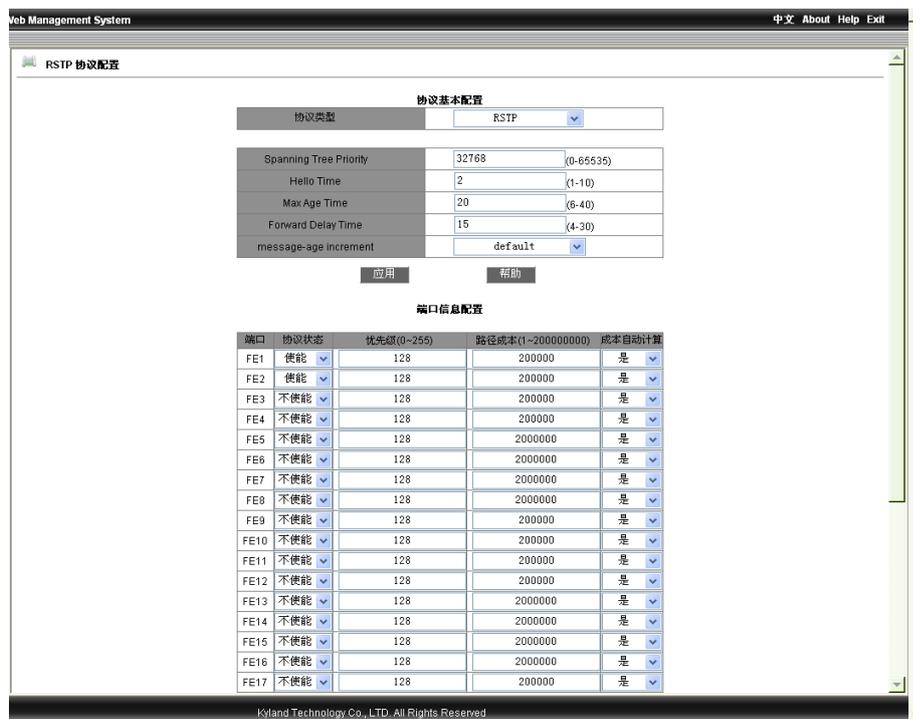


Figure 2-34 RSTP Configuration

### 2.4.12 RSTP Transparent Transmission

Click the “RSTP Transparent Transmission” in the left menu and enter the page (as Figure 2-35), set it as enable or disable. The port, whose RSTP or STP has been set, can not set with enabled RSTP transparent transmission.



Attention:

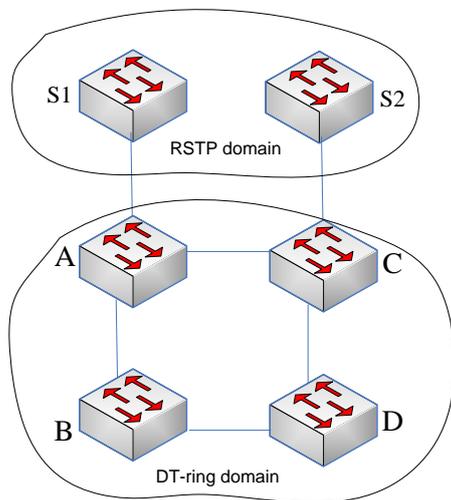
RSTP transparent transmission is actually the process that the switch forwards the received RSTP frames to the port set as transparent mode. In the network of RSTP, the switch is considered as transparent link.

RSTP is a redundant protection protocol for Ethernet link and has been the IEEE standard. DT-Ring is incompatible with RSTP and other redundant protocols.

The highlight of RSTP transparent transmission is that the switch can reserve its own redundancy protocol so as to ensure the link reconfiguration time to meet the industrial requirements.

In the ring, the RSTP frames are transmitted transparently, so the ring of the switches can be considered as a transparent link, in this way, both reconfiguration speed and compatibility can be ensured.

The configurations of RSTP domain is RSTP protocol and the one of DT-Ring domain is DT-Ring protocol; The RSTP is enabled in the ring port and the RSTP transparent transmission is set in the switch port connected to the RSTP domain.



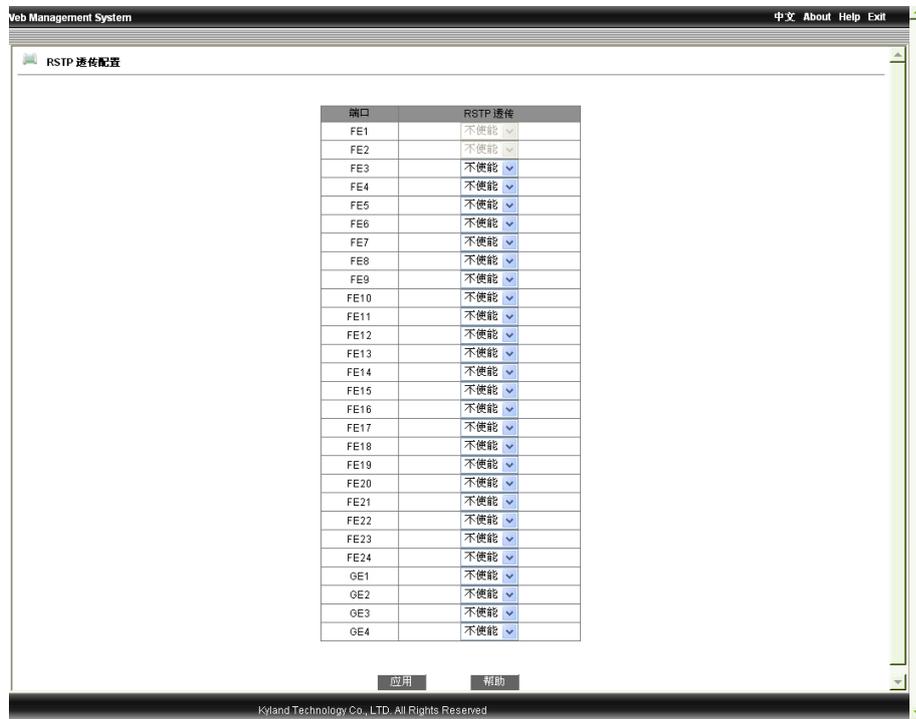


Figure 2-35 RSTP Transparent Transmission

### 2.4.13 DT-Ring Configuration

Click the “DT-RING” in the left menu and enter the page (as Figure 2-36), the redundant ring can be configured based on port or VLAN. Select enable or disable for check loop status, click “Apply” to finish. Click “Add” to enter the page as Figure 3-37. Enter ID No.(ID=1 to 32), domain name, set station type(master/slave), select ring port(GE1~GE4、FE1~FE24), select enable/disable for DT-Ring+ and backup port, click “Apply” to finish. As Figure2-39, click each ring domain name in the DT-Ring list to view the ring status.

**⚠ Attention:**

The redundant ring supports for DT-Ring, DT-Ring+ and DT-VLAN.

Multiple domains can be set in one switch so as to meet the requirements for tangent rings.

In one ring, each switch needs to be configured with identical domain ID, and identical domain name for easier maintenance.

Only one station in one ring.

One VLAN must be in only one DT-Ring domain.

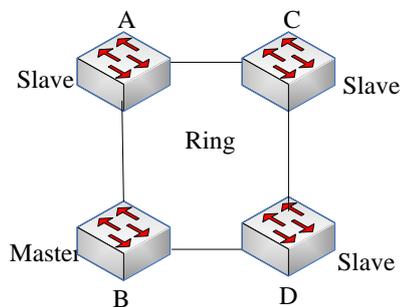
When the DT-VLAN is set in one switch, t, the DT-Ring based on port can not be set.

Check ring status: check the ring port and ring ID. It is based on port VLAN. Only the port, whose ring check function is enabled, can check the ring automatically. The ring check function is defaulted to be disabled. If the system find loop, the port will be down to remove the loop.

In case of closed ring, one ring port of master station is blocked and another is for forwarding. If the ring is opening or blocked, the blocked port will be for forwarding in 50ms.

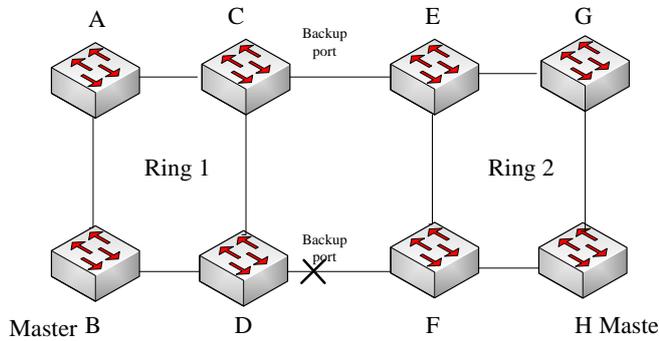
The configurations of the switches connected in the DT-Ring+: there are only two backup ports between two rings.

The DT-Ring topology is as following Figure. In the ring, one switch is set as master station and the others are slavery station.



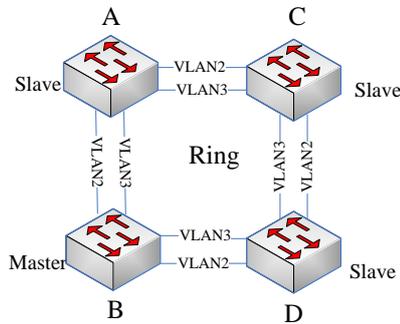
DT-Ring offers backup for two rings based on DT-Ring. It determines the status of the ring and port according to the backup switch's ID to ensure that loop won't be formed.

The topology is as following figure:



DT-VLAN is the expansion of DT-Ring. The latter offers redundancy based on port and supports only one redundant ring in a redundant link. The former offers link redundancy based on different VLAN groups in one link. In one redundant physical link, multiple redundant rings can be set based on VLAN group to control the VLAN forwarding status on the ring port and realize the fast reconfiguration.

The topology is as following figure:



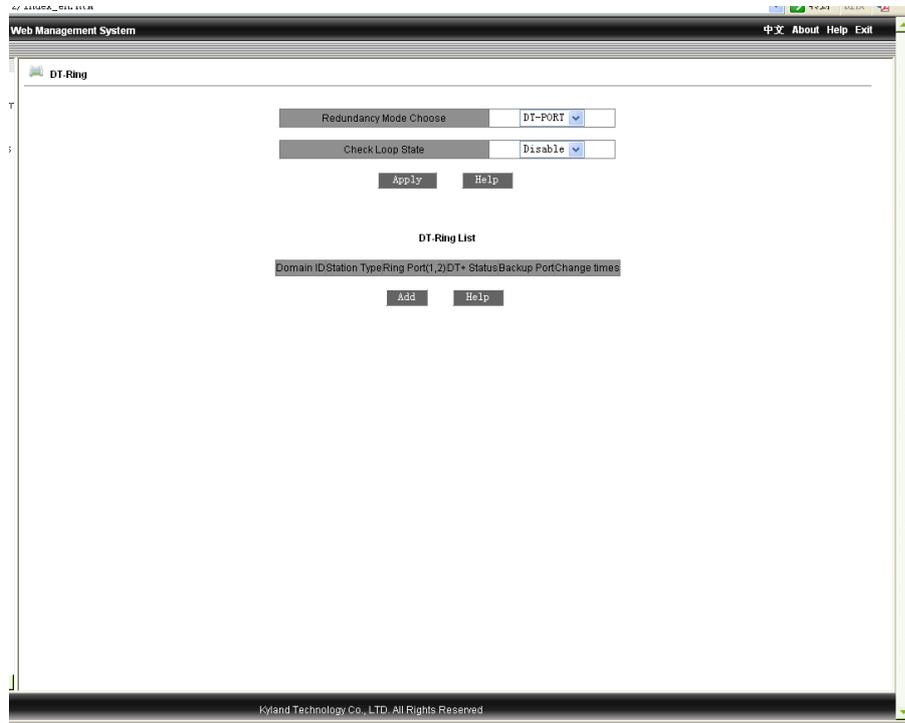


Figure 2-36 Ring Configuration

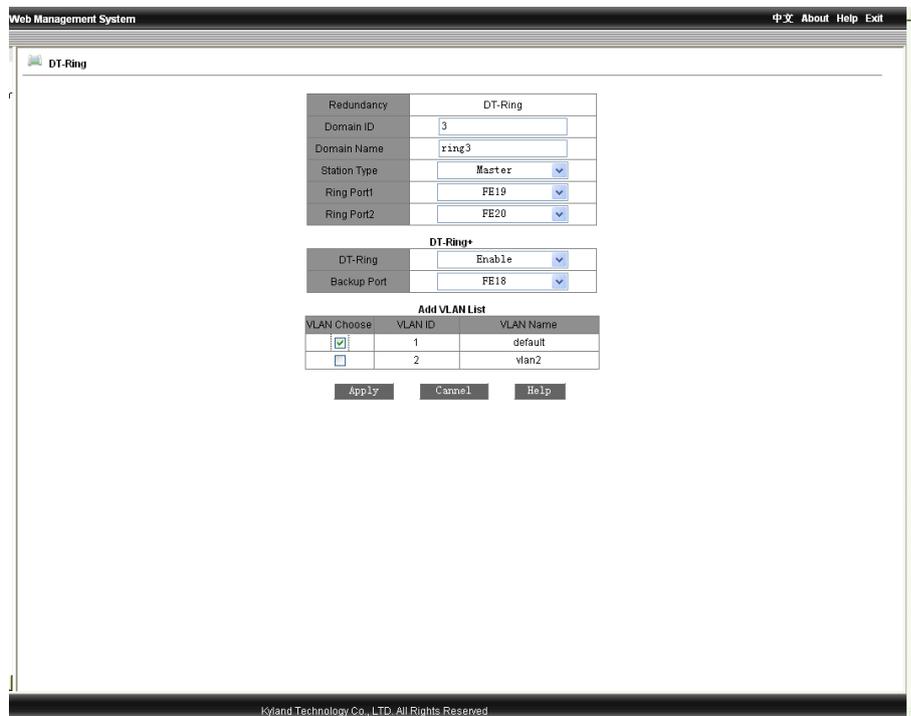


Figure 2-37 Ring Based on VLAN

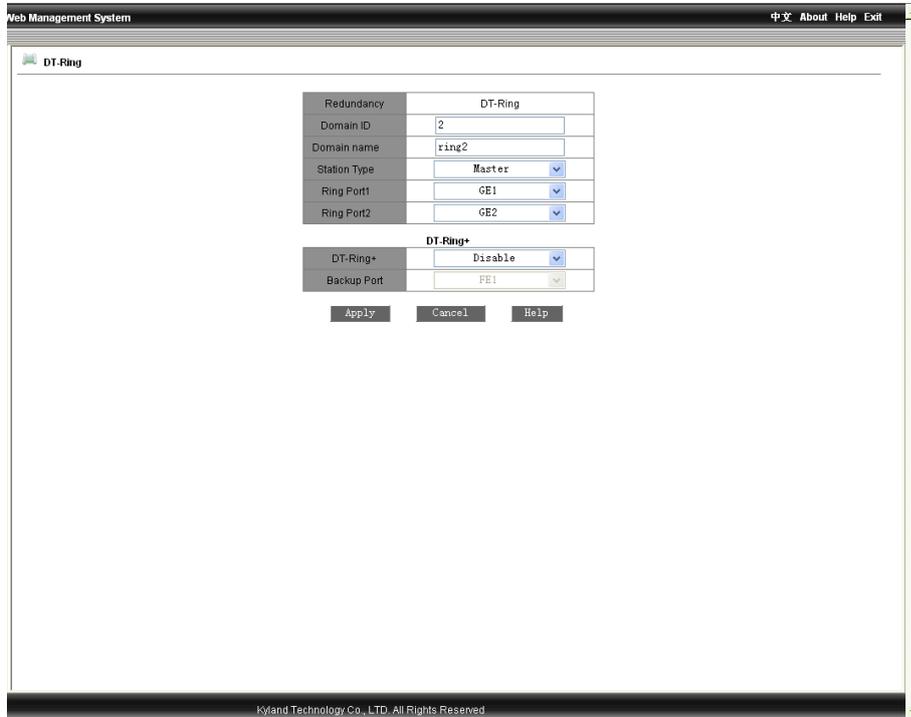


Figure 2-38 Ring Based on Port

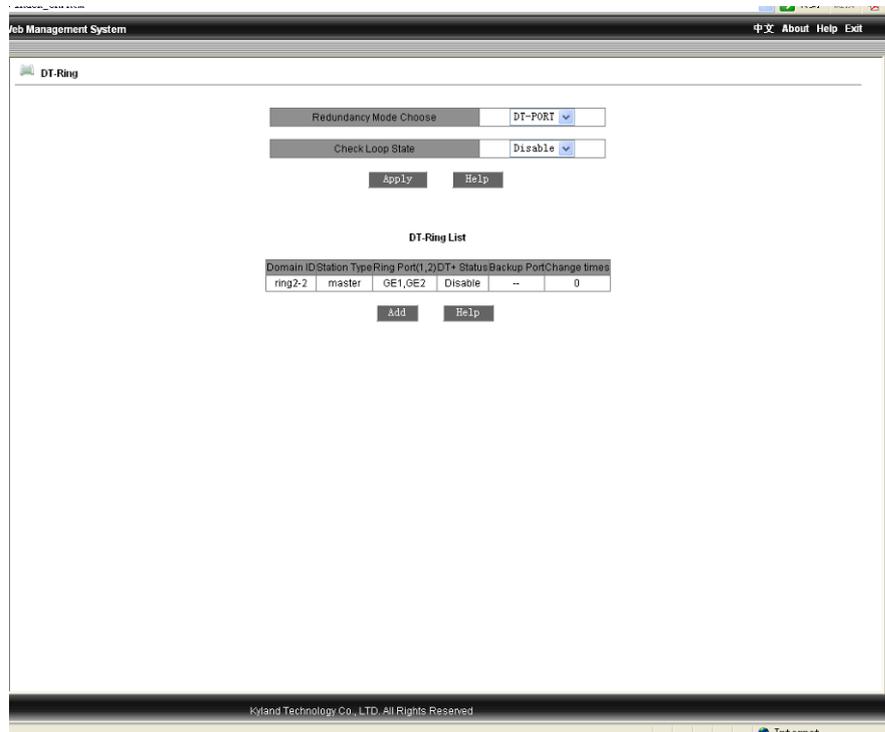


Figure 2-39 Finishing DT-Ring configuration

### 2.4.14 QoS Configuration

Click the “QoS Configuration” in the left menu and enter the page (as Figure 2-40), enable the QoS scheduling mode: weight (WRR) and preemption mode. Select “disable” will disable the function. The weight ratio is supported and can be set as 8:4:2:1(HIGHEST, SECHIGH, SECLow, LOWEST). The priority can be based on 802.1P, IP TOS, DSCP or port. Click “Apply” to finish.

---

 **Attention:**

The priority based on port can map only two queues: high and low.

The other three priorities support for 4 queues with the ID no.: 1,1,2,3 corresponding to the priority of lowest-low-high-highest.

QoS is realized via different queue scheduling modes of WRR and preemption as well as different scheduling policies.

Three scheduling policies are supported: port-based, 802.1P-based and IP TOS/DIFF-based, all of

which can be enabled in different port of the device. But they are exclusive in one port.

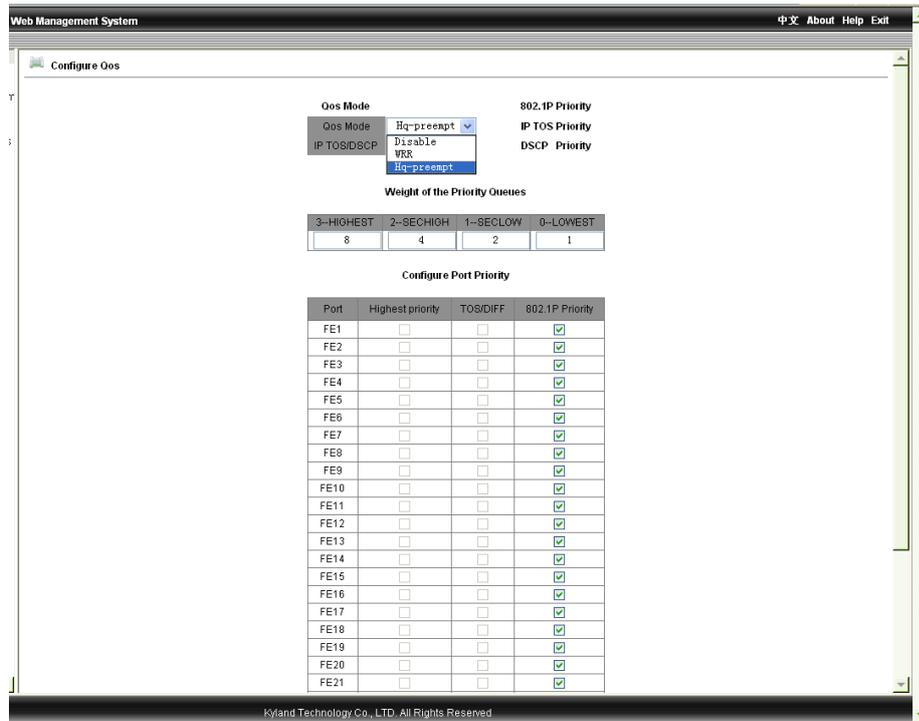


Figure 2-40 QoS Configuration

Click “802.1P Priority” the page as Figure 2-41: there are 8 priority levels, select the level and click “Apply” to finish.

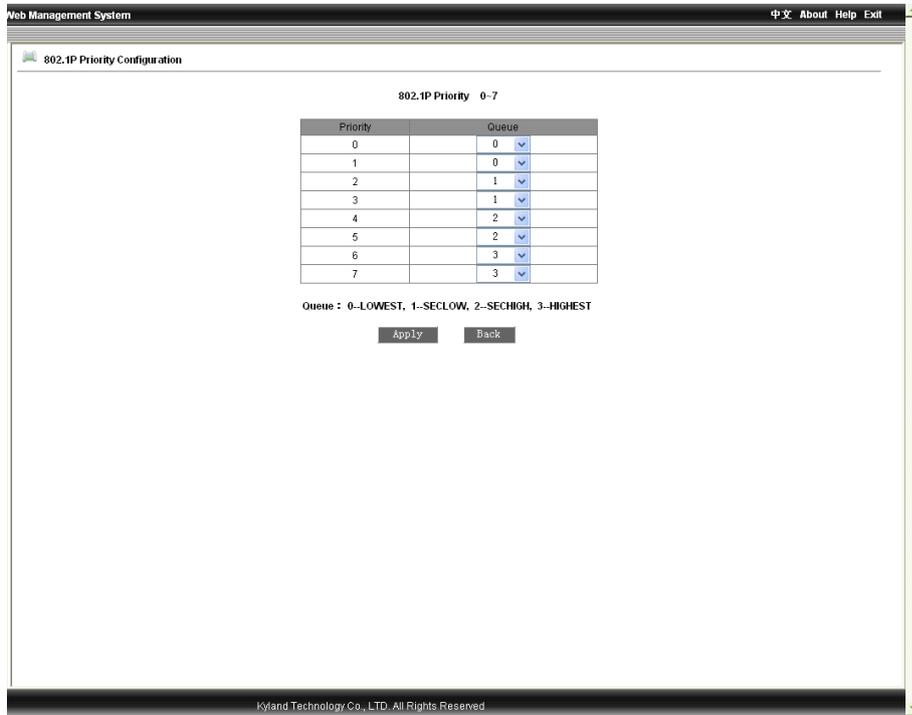


Figure 2-41 802.1P Priority

Click “IPTOS Priority” the page as Figure 2-42: there are 8 priority levels, select the level and click “Apply” to finish.

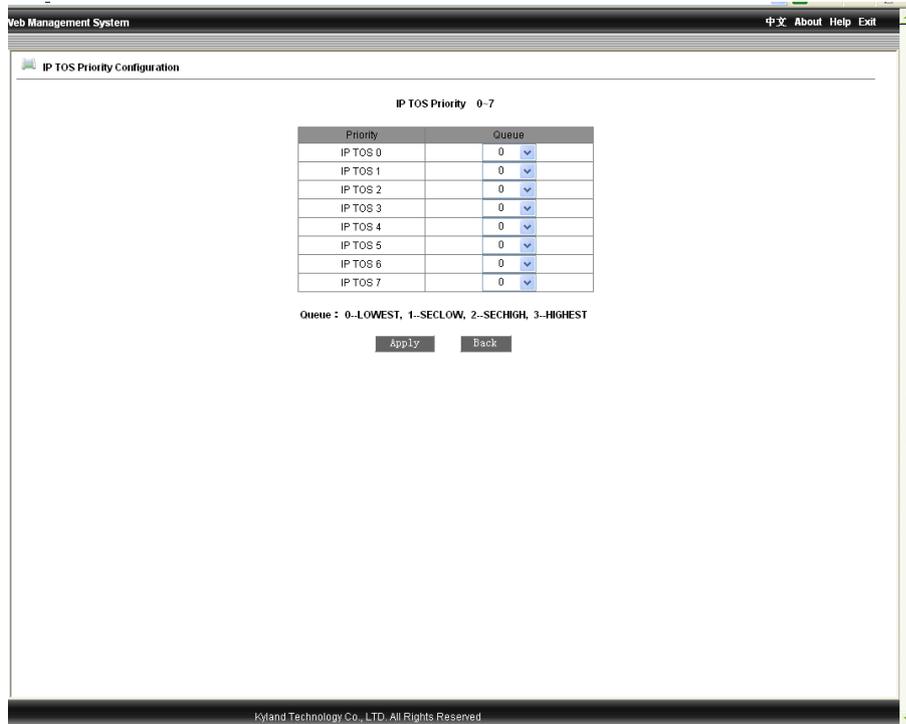


Figure 2-42 IPTOS Priority

Click “DSCP Priority” the page as Figure 2-43: there are 64 priority levels, select the level and click “Apply” to finish.

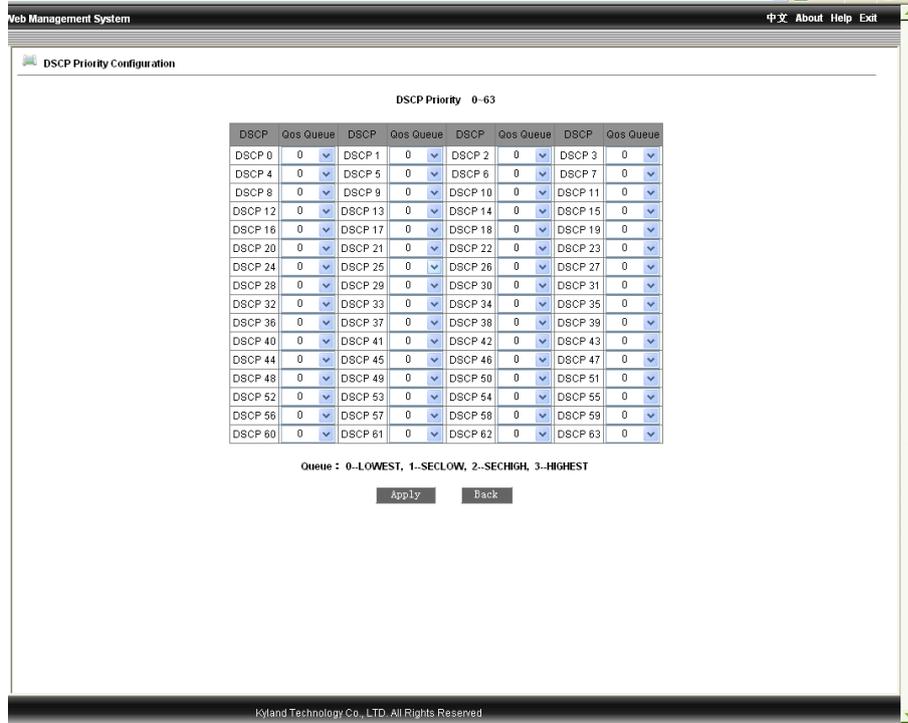


Figure 2-43 DSCP Priority

### 2.4.15 MAC Aging Time

Click the “MAC Aging Time” to enter the page as Figure 2-44: select the MAC aging time (range: 15-3600 sec) and click “Apply” to finish. The default time is 300s.

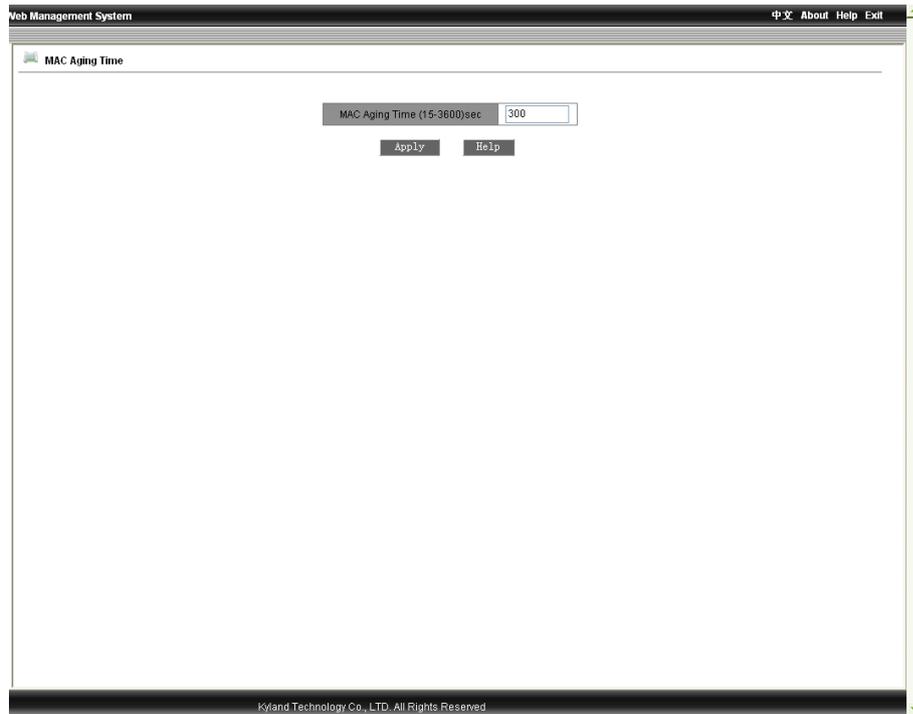


Figure 2-44 MAC Aging Time

### 2.4.16 Alarm

Alarm functions contain alarm vision and alarm configuration.

#### Alarm Vision

Click “Alarm Vision” in the left menu and enter the page as Figure 2-45 to display the enabled alarm information for power, temperature, IP conflict, MAC conflict, port status and ring status. If the port connection is normal, the alarm status will be shown as “Link Up”, and if abnormal, as “Link Down”. DT-Ring is shown as “Ring open ” for alarm and “Ring Close” for reconfiguration status.

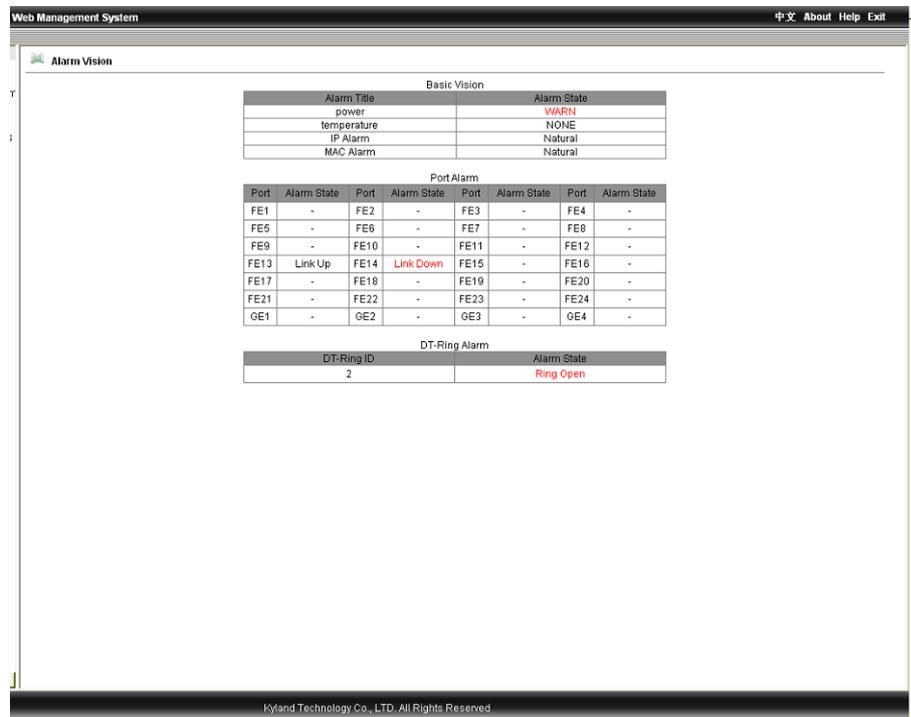


Figure 2-45 Alarm Vision

### Alarm Setting

Click the “Alarm Setting” in the left menu and enter the page as Figure 2-46 to configure the alarm for power, temperature, port, and ring etc. Select the inspection time from 180 to 600s for IP and MAC conflict. The default time is 300s. Enable the alarm for temperature and set the threshold value, click “Apply” to finish.



The alarm function for IP and MAC conflict is default enabled.

-----

To test the throughout of all the ports, the inspection function for IP and MAC conflict shall be disabled.

Click the “√” of “Alarm Enable” to disable as follows:

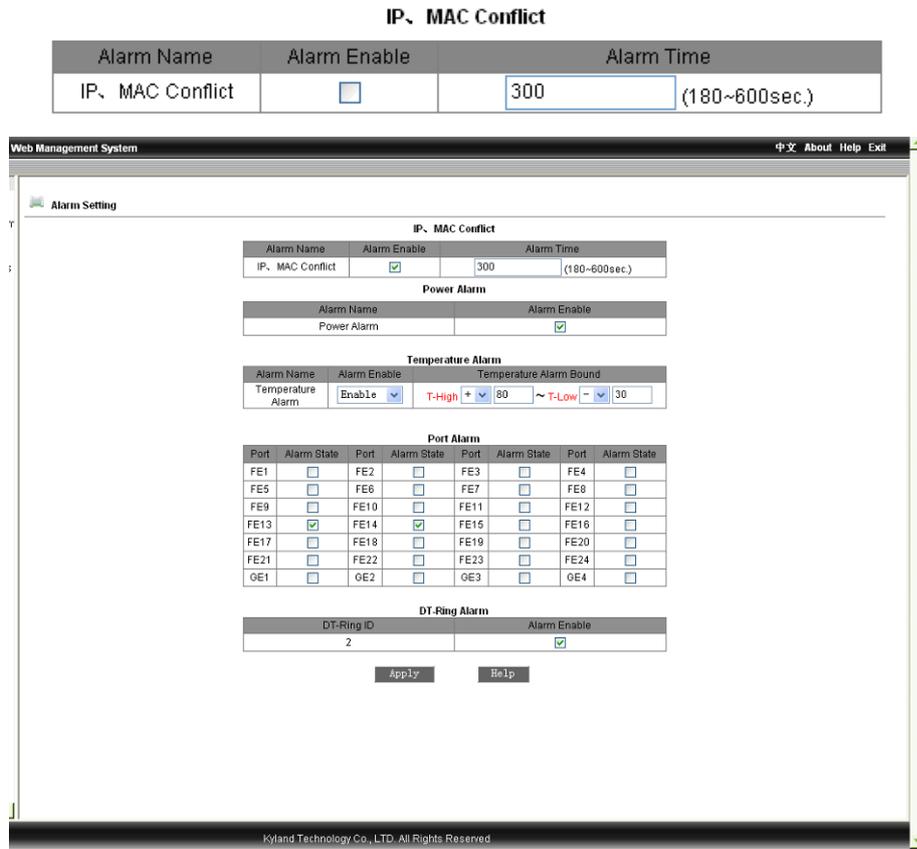


Figure 2-46 Alarm Configuration

### 2.4.17 RMON Configuration

RMON configuration contains RMON statistics, RMON history, RMON alarm and RMON event.

#### RMON Statistics

Click the “RMON Statistics” in the left menu and enter the page as Figure 2-47 to configure the RMON statistics. Fill in index no.(range: 1-65535), owner name (range: 1-32), select port (range: ifindex1-26), click “Apply ” to finish.

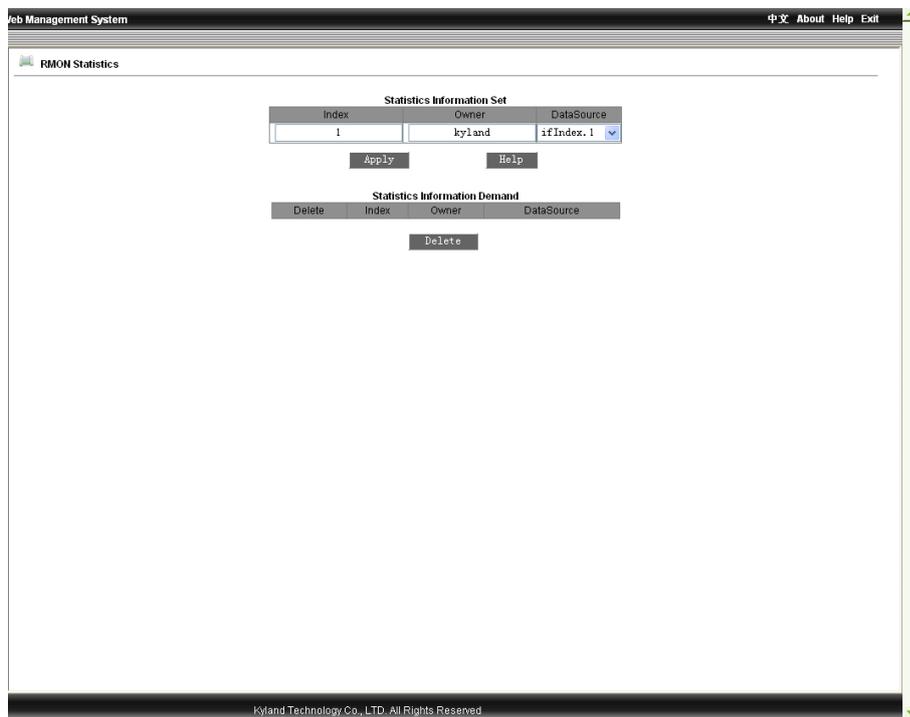


Figure 2-47 RMON Statistics

### RMON History

Click the “RMON History” in the left menu and enter the page as Figure 2-48 to configure the RMON history. Fill in index no. (Range: 1-65535), owner name (range: 1-32), select port (range: ifindex1-26), sampling no. (Range: 1-65535), sampling interval (range: 1-3600, default:1800), click “Apply ” to finish.



Figure 2-48 RMON History

### RMON Alarm

Click the “RMON Alarm” in the left menu and enter the page as Figure 2-49 to configure the RMON alarm. Select the alarm node from the MIB node list and double click, and the OID will fill in automatically. Fill in index no.(range: 1-65535), owner name (range: 1-32), select port (range: ifindex1-26), sampling type (Absolute/Delta), alarm type (Rising Alarm/Falling Alarm/Rise or Fall Alarm), sampling interval (range: 1-65535), Rising threshold value (1-65535), falling threshold value(1-65535), rising event index(1-65535) and falling event index (1-65535), click “Apply ” to finish.

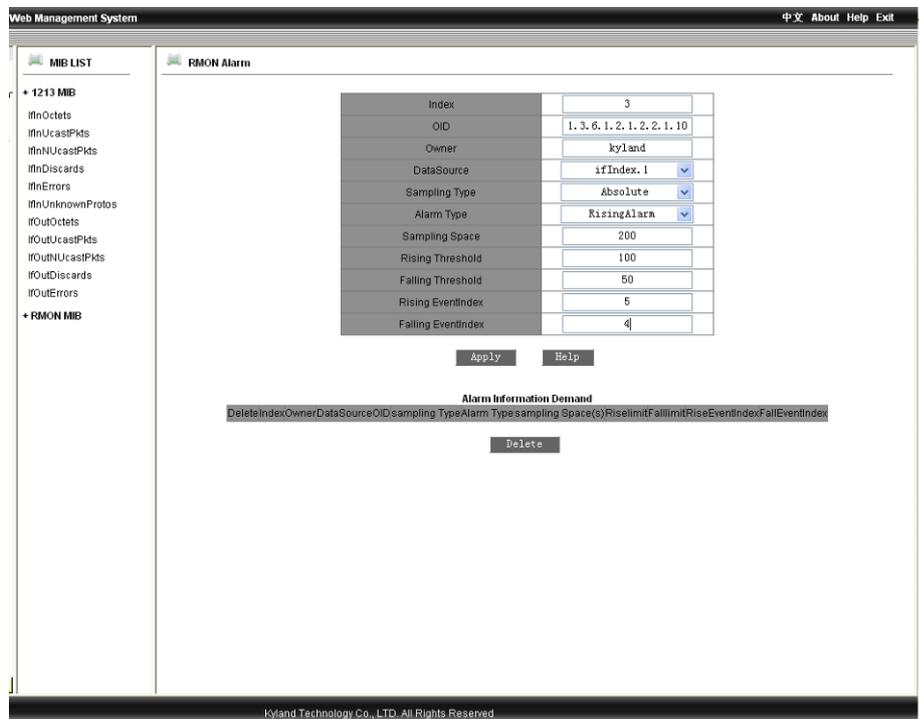


Figure 2-49 RMON Alarm

**RMON Event**

Click the “RMON Event” in the left menu and enter the page as Figure 2-50 to configure the RMON event. Fill in index no.(range: 1-65535), owner name (range: 1-32), event type (LOG/SNMP-Trap/Log and Trap), event description(range: 1-127), event community(event trap receiving community: 1-127), click “Apply ” to finish.

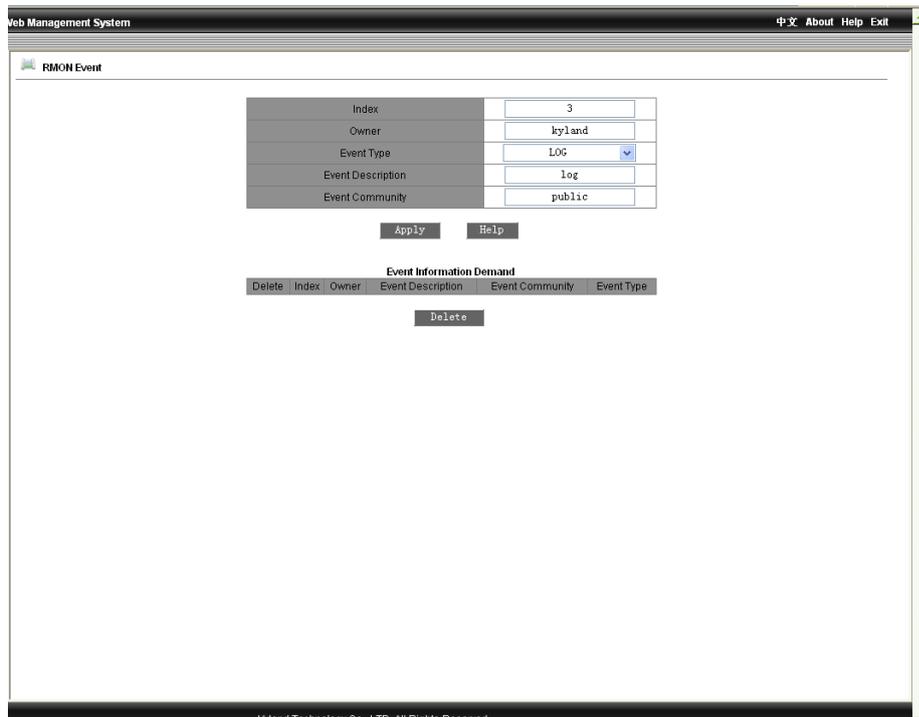


Figure 2-50 RMON Event

### 2.4.18 Log Query

This function contains: enable log and operate log.

#### Enable Log

Click “Enable Log” to enter the page as Figure 2-51 to enable the log operation, click “Apply” to finish.

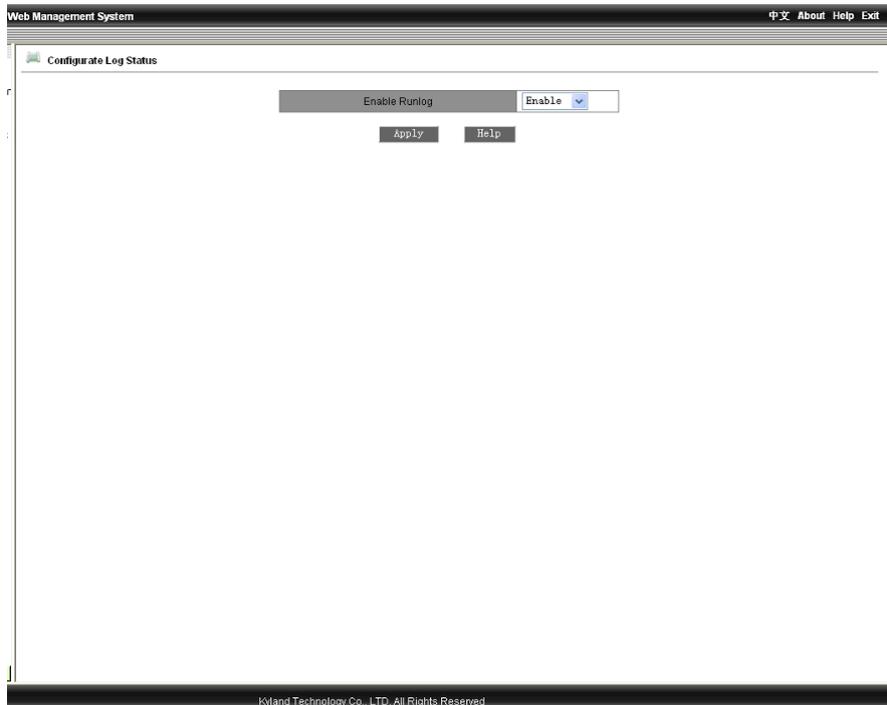


Figure 2-51 Enable Log

### Operate Log

Click the “Run Log” in the left menu to enter the page as Figure 2-52 TO query log, display serial no, log type, time, and log description.

Index	LogType	Time	Description
8690	PowerAlarm	SUN JAN 30 00:30:53 2000	Power alarm: entity id:2 state:Power down
8689	Broadcast	SAT JAN 15 01:41:10 2000	broadcast storm attack
8688	Broadcast	SAT JAN 15 01:41:00 2000	broadcast storm attack
8687	Broadcast	SAT JAN 15 01:39:58 2000	broadcast storm attack
8686	Broadcast	SAT JAN 15 01:39:47 2000	broadcast storm attack
8685	Broadcast	SAT JAN 15 01:39:36 2000	broadcast storm attack
8684	Broadcast	SAT JAN 15 01:39:25 2000	broadcast storm attack
8683	Broadcast	SAT JAN 15 01:39:14 2000	broadcast storm attack
8682	Broadcast	SAT JAN 15 01:39:03 2000	broadcast storm attack
8681	Broadcast	SAT JAN 15 01:38:52 2000	broadcast storm attack
8680	Broadcast	SAT JAN 15 01:38:41 2000	broadcast storm attack
8679	Broadcast	SAT JAN 15 01:38:30 2000	broadcast storm attack
8678	Broadcast	SAT JAN 15 01:38:20 2000	broadcast storm attack
8677	Broadcast	SAT JAN 15 01:35:12 2000	broadcast storm attack
8676	Broadcast	TUE JAN 04 06:52:28 2000	broadcast storm attack
8675	Broadcast	TUE JAN 04 06:52:17 2000	broadcast storm attack
8674	Broadcast	TUE JAN 04 06:52:06 2000	broadcast storm attack
8673	Broadcast	TUE JAN 04 06:51:55 2000	broadcast storm attack
8672	Broadcast	TUE JAN 04 06:51:44 2000	broadcast storm attack
8671	Broadcast	TUE JAN 04 06:51:33 2000	broadcast storm attack
8670	Broadcast	TUE JAN 04 06:51:22 2000	broadcast storm attack
8669	Broadcast	TUE JAN 04 06:51:11 2000	broadcast storm attack
8668	Broadcast	TUE JAN 04 06:51:00 2000	broadcast storm attack
8667	Broadcast	TUE JAN 04 06:50:49 2000	broadcast storm attack
8666	Broadcast	TUE JAN 04 06:50:38 2000	broadcast storm attack
8665	Broadcast	TUE JAN 04 06:50:27 2000	broadcast storm attack
8664	Broadcast	TUE JAN 04 06:50:16 2000	broadcast storm attack
8663	Broadcast	TUE JAN 04 06:50:06 2000	broadcast storm attack
8662	SoftWare Restart	TUE JAN 04 06:49:19 2000	software system reboot
8661	Broadcast	TUE JAN 04 06:49:15 2000	broadcast storm attack

Figure 2-52 Operate Log

### 2.4.19 Unicast Address Configuration and Query

This function contains static unicast address configuration and dynamic unicast address query.

#### Static Unicast Address Configuration

Click “static unicast address configuration” in the left menu and enter the page as Figure 2-53, select member port, configure MAC address and VLAN ID(1-4093), click the “Apply” to finish. In the address list, select serial number and click “Add” “Delete” and “Modify” to configure the address list.

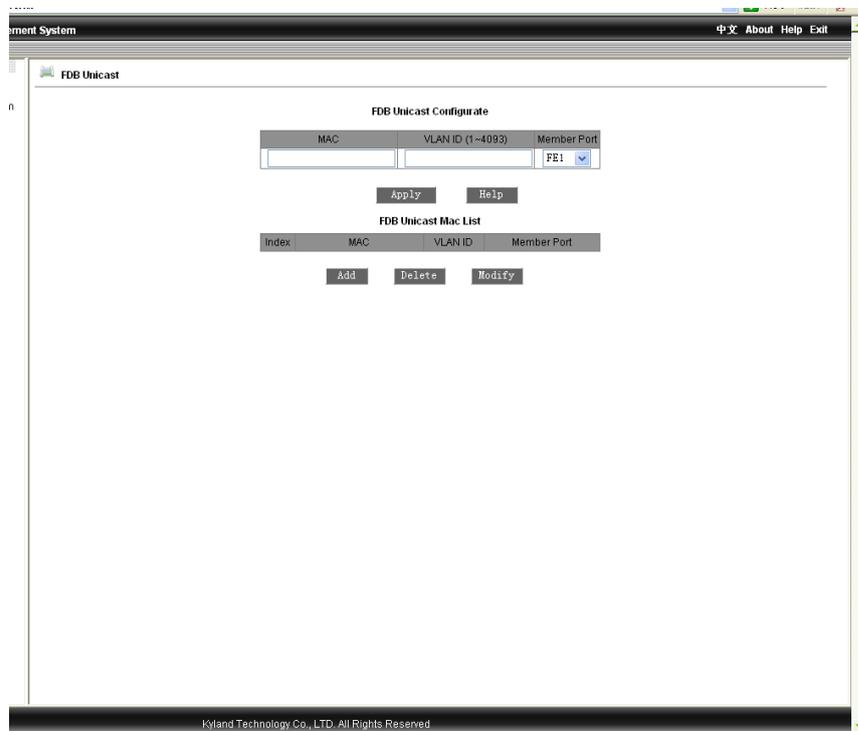


Figure 2-53 Static Unicast Address Configuration

**Dynamic Unicast Address Query**

Click the “Dynamic Unicast Address Query” to enter the page as Figure 2-54 to view the address list, display the terminal devices’ MAC addresses, set up switch port no. and port VLAN ID.

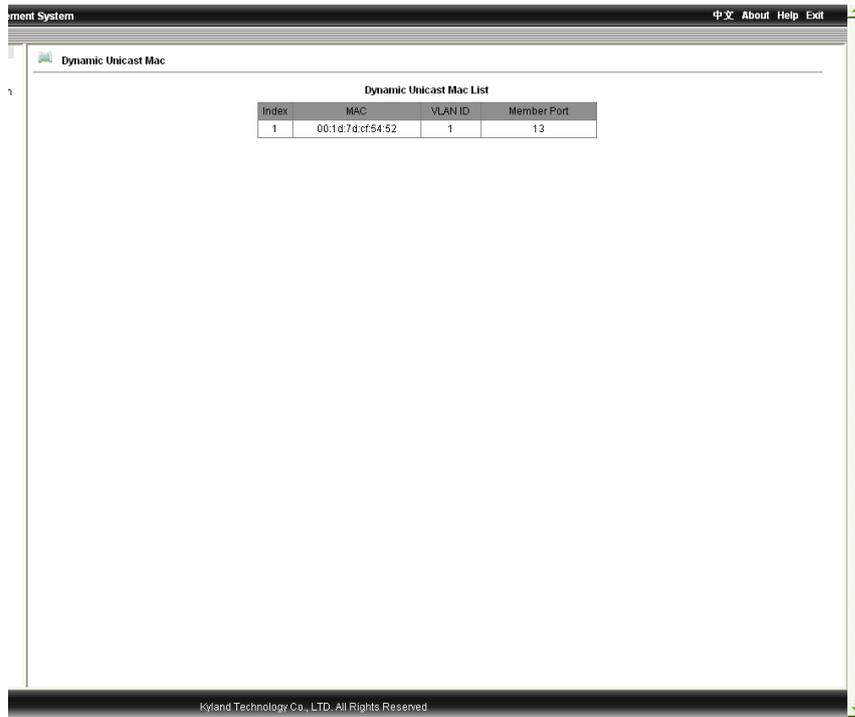


Figure 2-54 Dynamic Unicast Address Query

## 2.5 Device Management

Device management contains “Reboot” and “Logout”.

### 2.5.1 Reboot

Click the “Reboot” in the left menu to enter the page as Figure 2-55 and click “Reboot” button to restart the device.



Figure 2-55 Reboot

### 2.5.2 Logout

Click the “Logout” in the left menu to enter the page as Figure 2-56 and click the “Logout” button to logout.

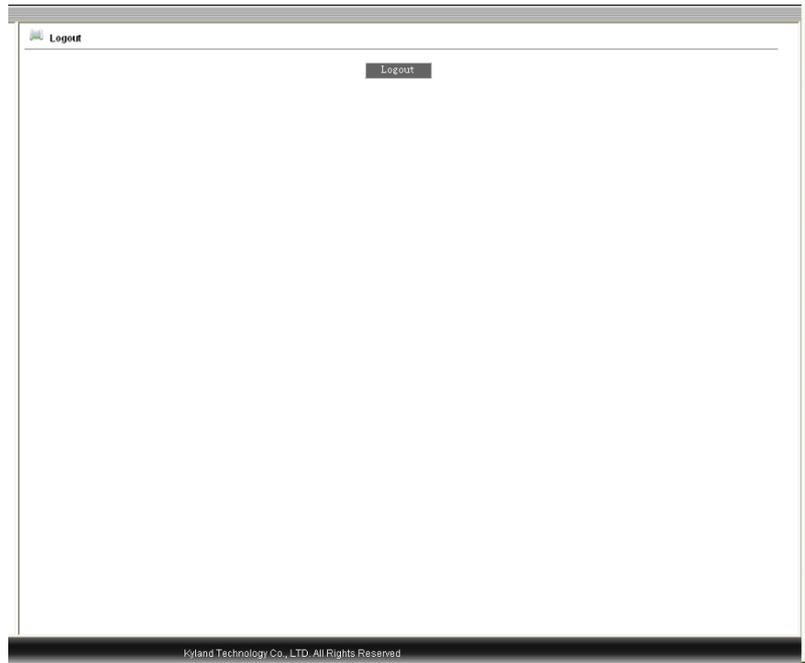


Figure 2-56 Logout

## 2.6 Save configuration

Click the “Save Configuration” in the left menu to enter the page as Figure 2-57, and click the “Save” button to save all configuration.

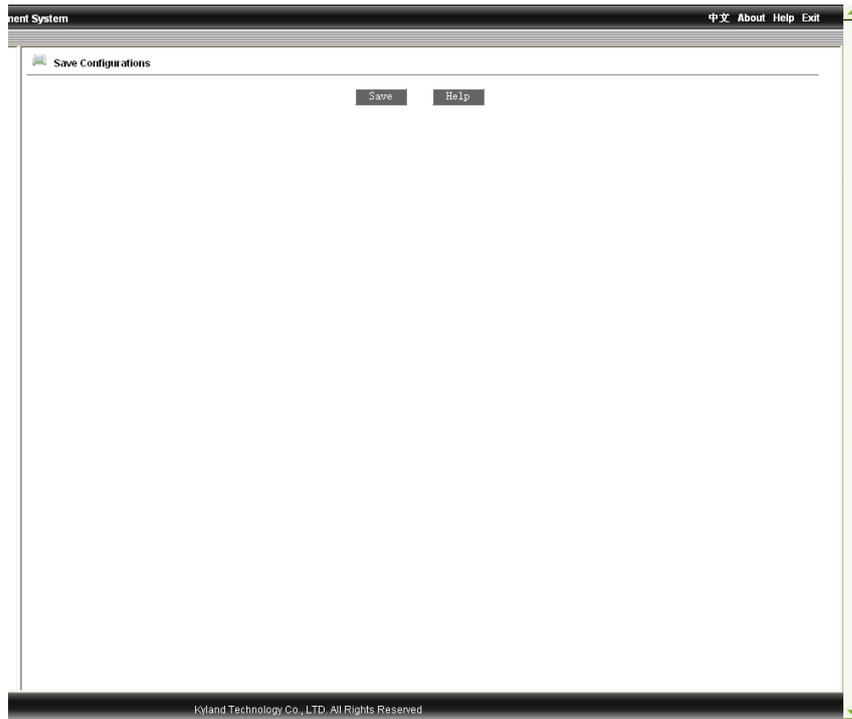


Figure 2-57 Save the configuration

## 2.7 Load default

Click the “ Load Default” in the left menu to enter the page as Figure 2-58 and click the “Load Default” to restore the default configuration.

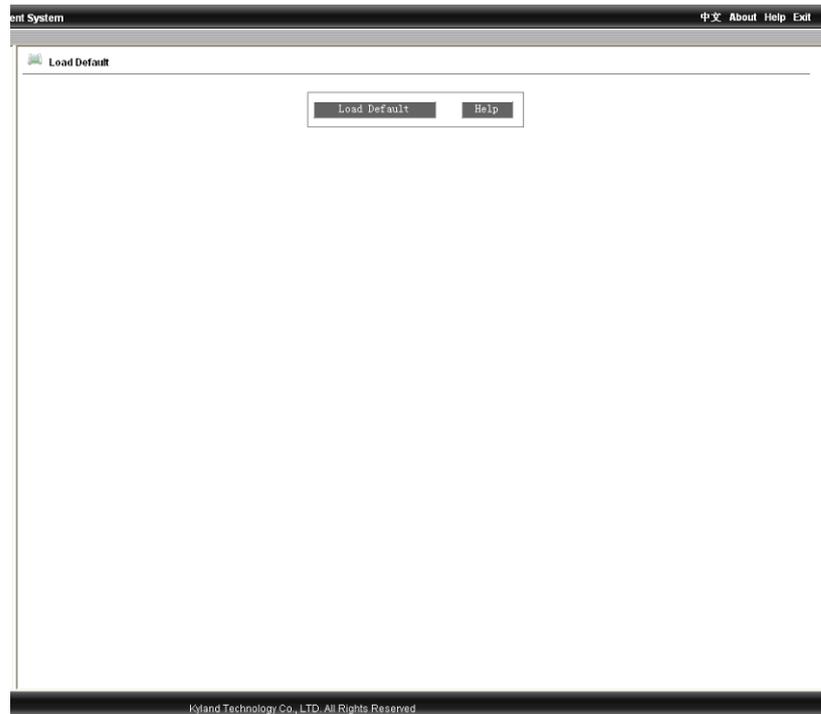


Figure 2-58 Load Default

## Chapter 3 FTP Application for Switch Software Update

You can use web management to upgrade software through switch by FTP protocol (Switch as Ftp client; PC as Ftp server). Before update, you need to setup the Ftp server; FTP server is a often used software which can be downloaded on the internet. Here is the step for FTP server configuration.

### 3.1 WFTPD Software Configuration

1. Install WFTPD in PC. Startup WFTPD as shown in figure 3-1:

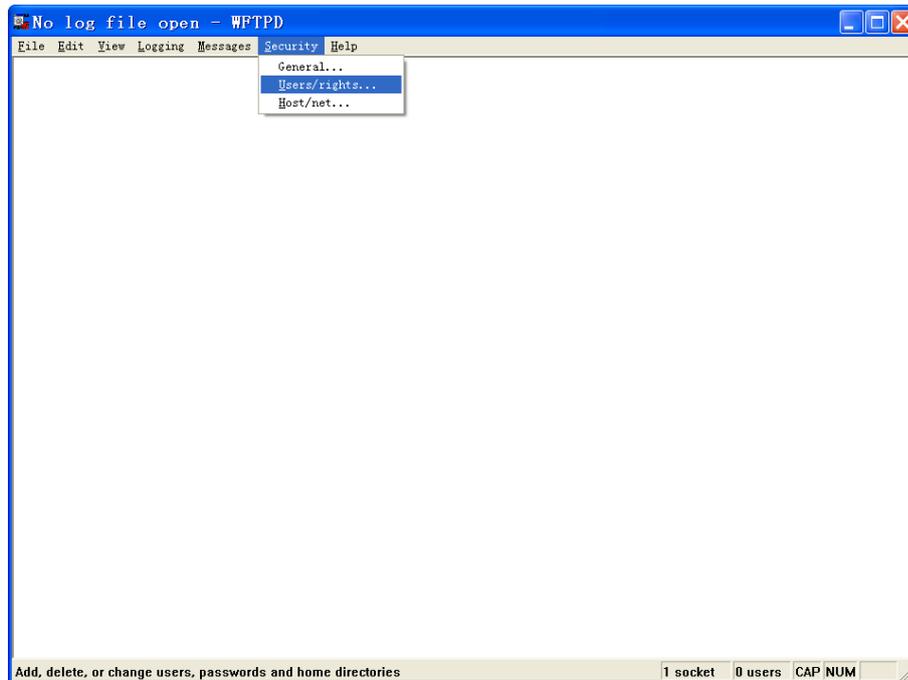


Figure 3-1 starts up WFTPD software

2. Click the “Security” button in the Figure 3-1 and click the “Users/rights” in the pull down menu to open the window “User/Rights Security Dialog” as Figure 3-2 and click the button “New User”.



Figure 3-2 WFTPD user name and password configuration

3. Type your user name in New User window; here is “test”, click OK, as Figure D-3



Figure 3-3 WFTPD username configuration

4. In Change Password window, enter the password in New Password and Verify area, here is ”test”, click OK.



Figure 3-4 WFTPD password configuration

5. Set main path in “home directory”; here is E:\



Figure 3-5 Configuration of user information

Click “Done” to finish FTP server configuration. If it is used to upload/download, we can stop here and go back to the web management interface as Figure 2-13 and 2-14. If it is upgrade, please continue the following steps.

Please copy the software to home directory of FTP server, here is under E:\

FTP server setup is finished now.

### 3.2 Software Upgrade

For the successful setup, our devices support two software versions: Host and Backup. The Host version is the one we currently used which is not allowed to be updated for the purpose of protecting software. We use WEB management software to upgrade it, the steps are as follows:

1. Enter WEB management page, select the “software update” to set Update, as Figure 3-6:

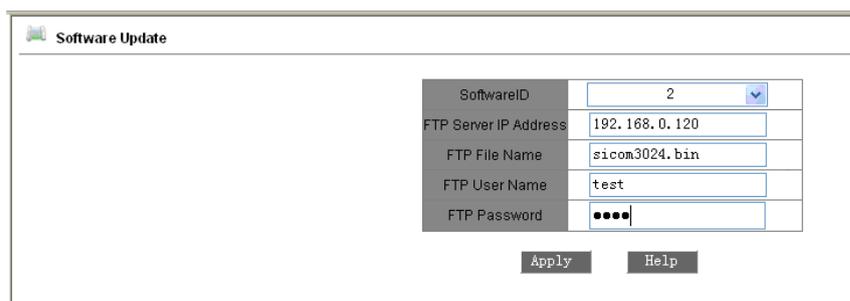


Figure 3-6 Software Update

2. Set FTP server IP address, user name, password, Update software name, click Apply button, and record the update software ID;
3. Wait for upgrade software, Update successful;
4. Click on navigation bar to check version; set updated software ID as startup version; as Figure3-7:

ID	Version	Date	Status
1	v1.0.0	2009-4-17 10:02	Inactive
2	v1.3.8	2009-4-8 13:19	Active

Figure 3-7 Software Version Enquiry

Click Reboot under equipment management in navigation bar; as Figure 3-8:



Figure 3-8 reboot

Wait for 30 seconds, start Web management system; click on navigation bar to check equipment basic information; software version; sure about the update successfully. As Figure 3-9:

Item	Information
MAC Address	00-1E-CD-17-C0-0F
SN	S3MOT090016
IP Address	192.168.0.2
Subnet Mask	255.255.255.0
GateWay	192.168.0.1
Device Name	KYLAND
Device Model	SICOM3024P_12M_ST_12T
Software Version	ID:2 V1.3.8 (2009-4-8 13:19)

Figure 3-9 Basic information

Update is finished.