MISCOM7028G Series
Industrial Management Gigabit Ethernet Switch

User Manual

All logos appearing in this manual are the intellectual property of the respective company.
Please read carefully before using this instruction. Only agree this contract that can use product in the instruction.

On these pages we have provided general technical data for the application of our products. For specific industry standards and further guidance. If you need more information or you want to use these information ,please contact our customer service.
All statements and technical information are based on results obtained under typical conditions. It is the responsibility of the recipient to verify with us that the information is appropriate for the specific use intended by the recipient.

Notice:

As technology developing，maybe there are some differences between some part of the data sheet and actual product. More information about our products can be found our website.Or you can contact our sales person directly.

Usage Safety

Although the product has good functions in the theory range, it still need to avoid any destroy by human causes.

- Please read carefully and keeping this instruction for reference.
- Please keep equipment from water or wet place.
- Don’t put anything around the power line and keeping the power line alone.
- To avoid fire, don’t confuse the power line and keep them uncovered.
- Please usually check power control whether connect with other equipment well.
- Please keep optical fiber ports and slots clean. When working, don’t watch the fiber section directly.
- Please keep equipment clean. If necessary, it can be cleaned by soft cotton.
- Please do not maintain equipment by yourself except that the instruction has mentioned.

Once appearing any things as following, please shut down the power and contact our company.

- Water split
- Equipment destroyed or crust broken.
- Working abnormal or some function of equipment changed.
- Equipment gets some smell or smoke or noise.

CHAPTER 1 Introduction

1.1 Product description

The MISCOM7028G series is a layer 2 all gigabit ports industrial ethernet switch which is developed for the high speed industry ethernet communications .It makes industrial communication more fluent, more stable and more fast.

This switch can support both hot plugging and complicated web managed style. All the copper ports support auto-negotiation, 10/100Mbps full duplex and half duplex, Auto-MDI/MDI-X functions. It supports various management method,include the command line interface(CLI) through the hyper terminal,the telnet management system and the SNMP management software.It also supports the network monitoring protocol of LLDP and SNTPv4.

This switch can supply high-grade management function including MSTP, IGMP Snooping,VLAN,GVRP,QoS, VPN , Trunk, rate control, Broadcast storm suppression, mirror port configuration, Static MAC address transfer, diagnostic function, Email/Relay, fault alarm relay.

This switch is a standard 19 inch 1U rack mounting device.

This switch provides total 28 gigabit ethernet communication ports,include 8 Gigabit Combo ports,4 Gigabit SFP fiber ports and 16 Gigabit RJ45 copper ports. All the ports support 802.1Q VLAN, 64 Kbps minimum step speed limit, 4K VLAN, 512 layer 2 multicast, and L2's Ipv4 and Ipv6 message forwarding across the wire.

1.2 Product characteristic

1.2.1 Industrial Network Performance

- Support total 28 gigabit ports for difference network mode
- 8 gigabit Combo ports can be used as a SFP port or a RJ45 copper port
- 16 gigabit copper ports 10/100/1000M adaptive, full / half duplex, MDI / MDIX adaptive mode
- Less than 50ms fast redundancy fiber ring network technology enhance the reliability of system communication
- Support VLAN based on IEEE802.1Q, number 4094
- Support for EAPS, MSTP and other redundant protocols
- Support the improved QoS strategy and various queue scheduling algorithms
- Support SNMP, PMON, Telnet and other network management protocols
- Support the command line interfaces(CLI) to access switches through super terminals
- Support hardware ACL function and provide ACL hardware filtering based on L2-L7 level data.
- Support IGMP Snooping detection function
- Support for broadcast storm suppression
- Supporting full duplex and half duplex mode traffic control
- Support power alarm, port alarm, ring alarm function
- FTP/TFTP based online software upgrade can facilitate user's equipment management and update
- It has the function of graphical network configuration, management and maintenance. It can monitor the running state and performance of the network remotely and provide network fault.Monitoring, diagnosis, location and alarm capability

1.2.2 Industrial power design

- Different industrial power range for customer option:
  24DC(18-36VDC),48DC(36-72VDC) or 220AC/DC(85-264VAC/110-370VDC)
  single power or dual redundancy power
  power consumption<27W

1.2.3 Strong appearance design

- Aluminum chassis heat dissipation surface design, no fan efficient heat dissipation, can make the system work reliably in -40℃~85℃ environment
- High-strength enclosed aluminum enclosures, IP40 protection rating, enable the system to work reliably in harsh and dangerous industrial environments

1.3 Packing List

Item	QTY
MISCOM7028G Industrial Ethernet switch	1pcs
User manual(CD with manage software)	1pcs
Console cable	1pcs

1.4 Performance Specifications

IEEE Standards: IEEE802.3-10BaseT, IEEE802.3u-100BaseTX, IEEE802.3x-Flow Control, IEEE802.3z-1000BaseLX, IEEE802.3ab-1000BaseTX, IEEE802.1D-Spanning Tree Protocol, IEEE802.1w-Rapid Spanning Tree Protocol, IEEE802.1Q -VLAN Tagging, IEEE802.1p -Class of Service,IEEE802.1X-Port Based Network Access Control
Exchange method: store and forward
Backplane bandwidth: 56Gbps
Packet forwarding rate: 41.664 Mbps
MAC Address: 16K
Transmission distance: 100m for twisted pair, 20 km for single mode fiber
Physical size (width * height * depth): 482.6MM * 44mm * 315mm
Installation mode: standard 19 '1U rack type
Case protection: IP40
Weight: 4kg
EMC standard:
IEC61000-4-2 ESD:±8 KV Contact discharge,±15 KV Air discharge
IEC61000-4-3 RS:10V/m(80-1000MHz)
IEC61000-4-4 EFT: Power port ±4 KV,Data port ±2 KV
IEC61000-4-5 Surge:±2 KV(Differential mode),±4 KV(common mode)
IEC61000-4-6 CS:3 V(10kHz~150 kHz),10V(150kHz~80 MHz)
IEC61000-4-8 Power frequency magnetic field:100A/m
IEC61000-4-10 Damped oscillating magnetic field:10A/m
EN55022：EN55022 Class A

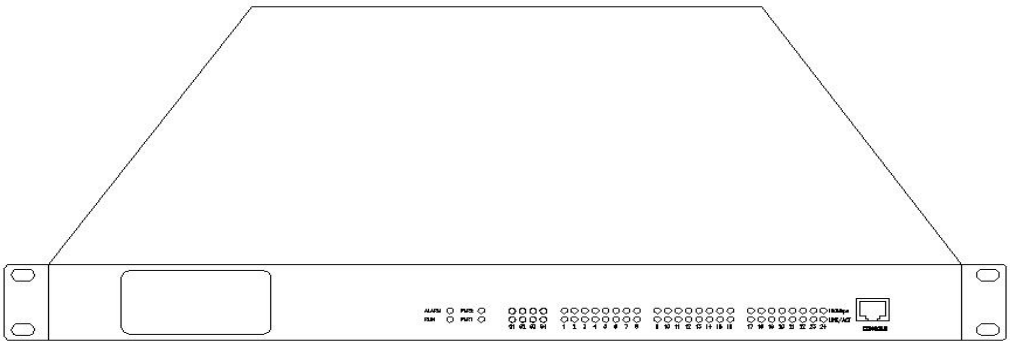
Chapter 2 Hardware function

2.1 Main hardware

2.1.1 Panel layout

The MISCOM7028G casing designed for industrial applications, IP40 protection, rugged high-strength metal case.

Physical size (width * height * depth): 482.6MM * 44mm * 315mm



The indicatior lights of the front panel shows the working status of the switch:

PWR1 PWR2	ALARM		RUN	LINK/ACT		1000Mbps	
Red on	Gree n off	Green blinking	Green blinking	Green on	Green blinking	Green on	Green off
Power work	No alarm	Alarm	System work	Link construct	Data transmitting	1000Mbps Link rate	10/100Mbps Link rate

The indicatior lights of the communication ports:

RJ45（1-24）			SFP（17-28）		
Green			Green		
on	blinking	off	on	blinking	off
Port connected	Port active	Port unconnected	Port connected	Port active	Port unconnected

Gigabit fiber SFP interfaces

This product has two full-duplex 1000Base-LX single mode / multimode fiber interface, the port number for the G1 and G2, using hot-swappable SFP during the optical interface using LC connectors. Optical interface to be used in pairs (TX and RX as a pair), TX mouth to light the originator, the remote switch connected to another optical interface of the light receiving end RX; RX ports for the light receiving end, to connect with a remote switch with an optical interface light originator TX. The use of two redundant 1000Base-LX optical interface fiber optic redundant ring network can be formed in the system failure redundant ring switching time less than 20ms, can effectively improve network reliability.

SFP optical module shown in the figure :

Hot-swappable SFP modules as follows:

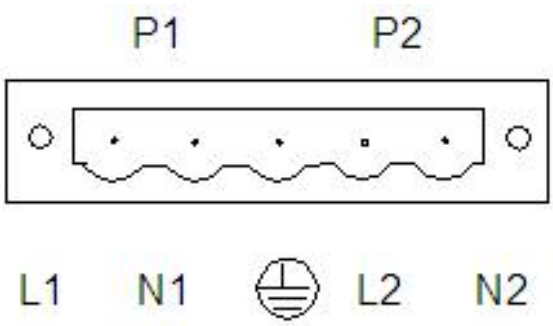
Hot-plug procedure:
1, SFP during the observation of a finger end of the PCB.
2, the finger end into the SFP metal shielding cage, hear a click sound indicates that the device has been inserted in place, then the SFP plug handle, into the interface parallel to the normal position, you can use.
Hot drawing steps:
1, first unplug the SFP's plug handle perpendicular to the interface, this time the device should be shielded with SPF cage mount hook disengaged.
2, parallel to pull the SFP module.

Ethernet RJ45 port

This product has multiple RJ45 10Base-T/100Base-TX Ethernet ports. Each RJ45 port with auto-negotiation, auto MDI / MDI-X connection. Internet can be used straight line / cross-over cable to connect the switch to terminal equipment, servers, hubs or other switches. Each port supports IEEE802.3x adaptive, so the optimum transmission mode (half or full duplex) and data rate (10Mbps or 100Mbps) can be automatically selected (the connected devices must also support this feature). If the device is connected to these ports do not support adaptive, then the port will send the correct speed, but will default to half duplex transmission mode.

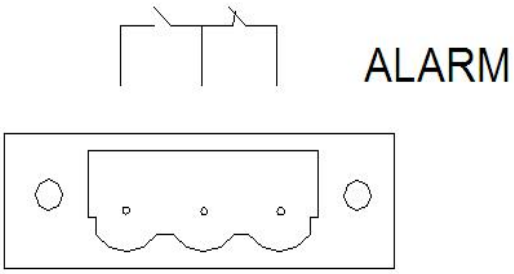
Power input terminals

The power of this product standard configuration is: dual redundancy AD220V power, using 5.08mm space terminal connect the power input.
Max power: ＜27W
Input voltage range: AC85—265V (frequency:47-63HZ) or DC110—370V.



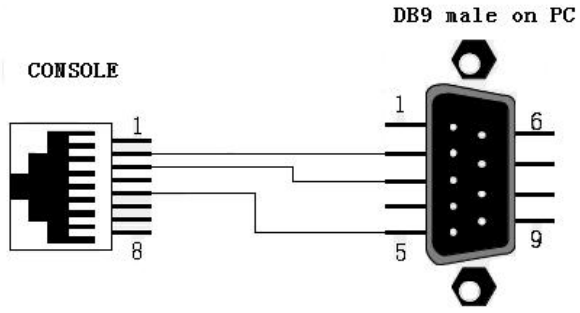
Alarm relay

This switch has a 3-ways 5.08mm terminal block for alarm relay on the front panel.It’s a normally open relay(left side) and a normally closed relay(right side),the block in the middle is shared used.
When the switch works well, the normally open relay is closed,and the normally closed relay is off.When the device power off(single power or dual power off),the port link down,or cause network storm, the normally open relay is off,and the normally closed relay is closed. Recommended load capacity of the relay switch is 1A (24VDC).



Serial network management interface (CONSOLE)

Network management port is a RJ45 interface, please use our serial extension cable to the PC's serial port. Interface communication standard 3-wire RS-232.
Serial communication parameters are as follows:



Baud Rate: 115200bps, Data bits: 8 , Parity: none, stop bit: 1 Flow Control: none

Grounding

There is a Grounding screw on the back panel of the switch. One end of the grounding wire is fixed on the grounding hole of the cabinet by a grounding screw. The other end of the grounding wire reliably connects to the earth..

2.2 Hardware Installation

2.2.1 Installation notice

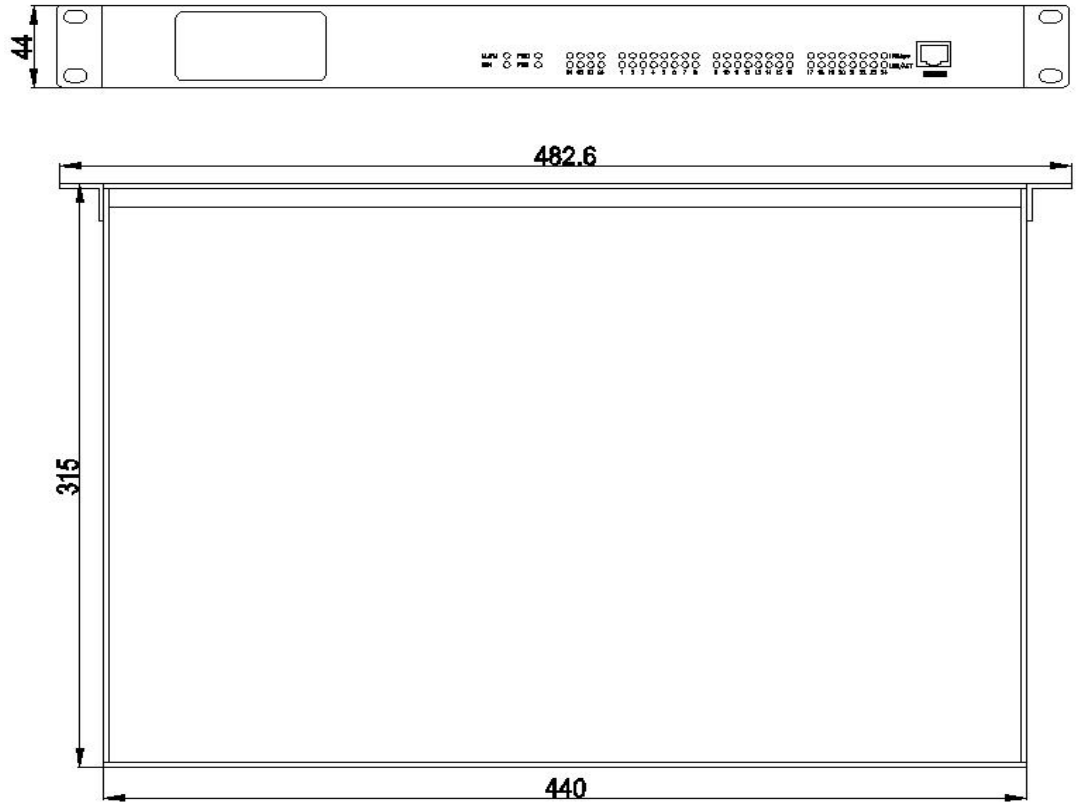
The Industrial Ethernet switch is standard 19 inch rack mounting installation.Please make sure a suitable work environment, including power requirements, enough space, connect equipment and other equipment status. Please confirm the following installation requirements:

- Power supply: Standard redundant AC/DC220V power supply.Other special power type please refer to the power stick and label on the switch.
- Environmental requirements: Temperature -40 ℃ ~ 85 ℃, relative humidity 0 ~ 95% (no condensation).
- Grounding resistance requirement: <.Ω5
- Configuration requirements under the contract, check the cable is in place, fiber optic connectors is appropriate.
- Avoid direct sunlight and away λ from heat sources or areas with strong electromagnetic interference.
- Standard 19 inch 1U installation. Check for suitable cables and connectors.

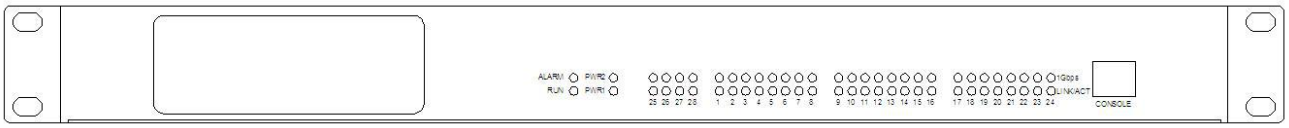
Attention：

- Before installing or connecting Ethernet switch please make ensure that disconnect the power line. Do not exceed Max. current. If exceeds the maximum current, make the wire overheat, causing serious damage to the equipment.
- Separate the power cable and other cables, if the two paths must cross, must ensure that the intersection of these lines are vertical.
- Grounding and cabling can effectively suppress the noise caused by electromagnetic interference. Before connect the switch with equipment please connect GND first. Connected to the grounding screw from the ground surface

2.2.2 Rack installation



The front panel of the switch:



Before installation, please make sure the below 2 items:

- If enough space to install this ethernet switch.
- If suitable working power for the ethernet switch.

2.2.3 Cable connection

After install Ethernet switch , please correct install cable. Cable installation please following behind notice:

Equipment port connection

This product provides RJ45 port for copper ethernet connection, use the crossover cable direct connect with terminal equipment , use cross wire connect network equipment .

2.2.4 Fiber connection

This product provides single mode or multimode LC fiber connection port.

Attention：

This switch uses lasers to transmit signals over fiber cable. Laser Class 1 laser/LED products can cause serious damage on the eyes harmless. When the equipment is power on, please do not stare directly into the laser beam.

Connection optic cable , please use following steps:

- When use fiber cable port, port cover; When it finish work, please put the plastic cover to protect the fiber optic head, keep clean.
- Check the fiber optic cable head whether it clean or not. If it not clean, will effect port and communication quality.
- One fiber optic head connect with Ethernet switch optic port, the other fiber head connect with another equipment fiber optic interface equipment.
- After connection, please check switch the front interface's LNK/ACT LED lights. If lights on,

connection is available.

2.2.5 Cable Layout

- Laying of cable should as following conditions:
  Before laying cable please checking weather suitable for project.
- Before laying cable laying please checking quantity, route to, location an other related , construction design weather suitable. Separate users cable and power supply cables.
- Please check the cable do not broken or other connector.
- Fiber optic cable should be straight in the aisles neatly inside, turning uniform, smooth and straight.
- cable in the channel, it should be straight, not close to channel, blocking the other inlet and outlet holes in the cable channel out of the corner site or cable should be binding and fixed.
- Do not mix cable, power cable, GND cable. Do not overlap.
- If cable is too long, it must be structured cable support rail site on the middle, do not pressure the cable.
- It is necessary to prevent the cable too tie and turns should be minimized, turning radius should be suitable. Banding should be appropriately tight, not too tight.
- Cable should be the appropriate identity, easy to maintain.

Attention:

Laying cable, it is necessary to prevent the cable tie and turns should be minimized, and the turning radius is not too small, the turning radius is too small will lead to a serious loss of optical signal link. The quality of communication.

2.3 Testing guide

2.3.1 Self-examination

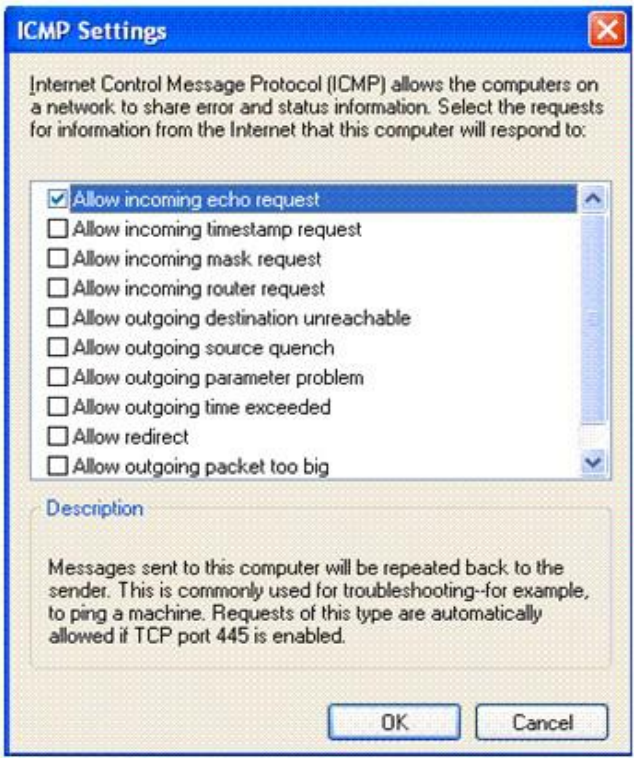
When connection equipment, the front panel power supply indicator light will blinking once, it means working well. After a while Power supply indicator light is on. Run indicator light (system status LED) will blink interval 1s.

2.3.2 Copper port testing

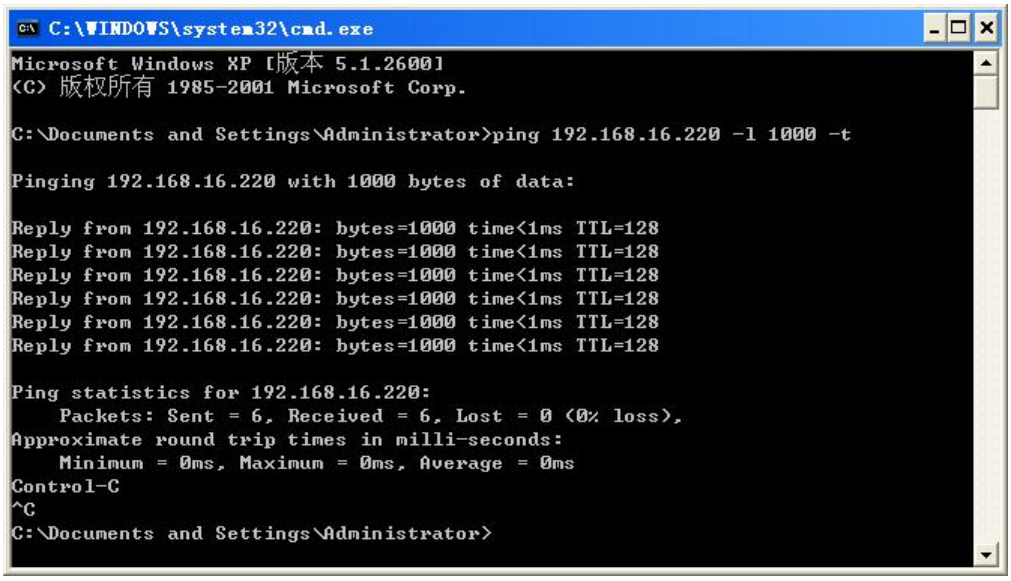
As picture show, the power port by any two straight lines and two test networked computers connected to the network port, send a Ping command to each other, both sides were able to correctly Ping to each other without loss. That tested the hardware working properly the two power ports

PING command example:

Testing computer1 IP address as: 192.168.0.10, testing computer2 IP address is 192.168.0.11, please make sure the two computer's local connection ICMP first option" allow incoming echo request" have been chose, as below picture show:



Please click testing1 start---run, input cmd or command (win2000/XP system use cmd, win98/95 system command), pop up control window, send ping192.168.0.11—1 1000-t,(-1 means sending data packet bits,-t means sending data packet instantly) command, with same method testing computer2, running ping 192.168.0.11---1 1000 –t. If the testing computer 1 return to reply from 192.168.0.11: bytes=1000 times<10ms TTL = 128, running over 10mins, use CTL+C command count packet loss rate as 0, that means device working normal, as below picture show:

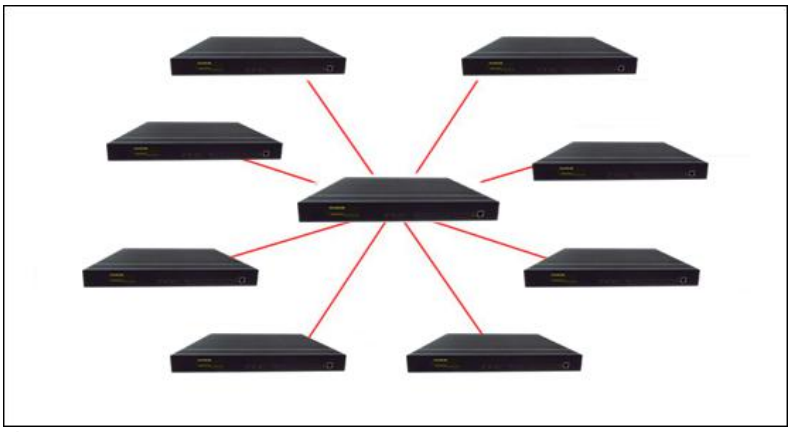


2.3.3 Fiber optic port testing

Composed of two devices as shown in the optical chain network. Each device port by any one power line and testing of computer networking directly connected to each other and send the Ping command, both to each other and do not correctly Ping packet loss. While the corresponding optical port Link / Act LED should be lit. Two optical ports that the hardware is tested working properly. Another way to test using the same optical port.

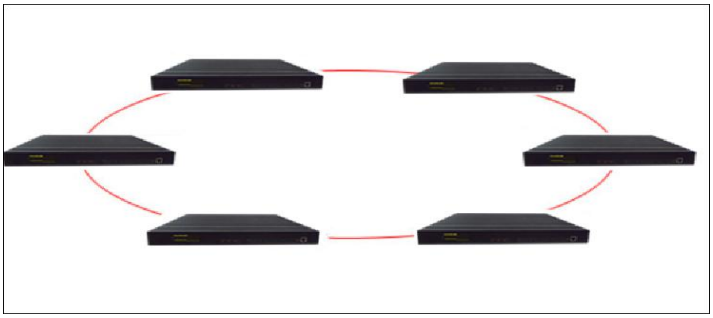
2.4 Network construction

2.4.1 star ring network

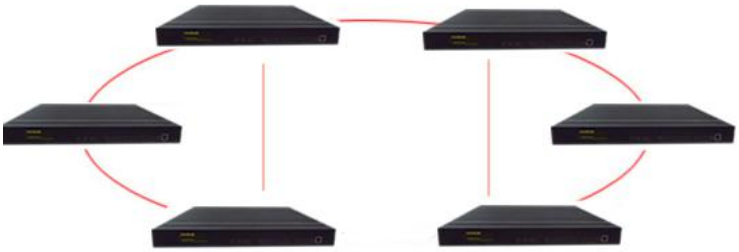


2.4.2 Line network

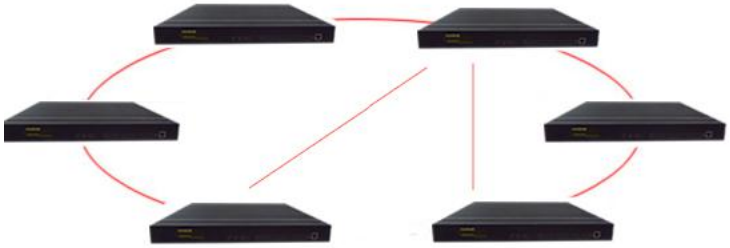
2.4.3 single ring network



2.4.4 Single loop coupling



2.4.5 Tangent ring coupling



Chapter 3 Serial Port configure Specification

This managed Ethernet switch, can visit, configure and manage by in-build web page. Before detail operate, must make sure customer web managed PC in the same network segment with visited Ethernet switch. The Ethernet switch default IP address is 192.168.16.253,
User can visit console port through windows HT Hyper Terminal, or through Ethernet connect visit web manage set Ethernet switch IP address.

3.1 Though Hyper Terminal set up Managed Serials Ethernet Switch IP Address

This ethernet switch console port connect with PC serial port by a professional serial wire ., then open Hyper Terminal by PC , Windows user can do as that : beginning ---->program---->attachment ---->communication then find Hyper Terminal. Open the Hyper Terminal you need create a new link , then you must choose the communicate port that connect with Ethernet switch , use bellow data :

Braud rate：9600， **Data Number** ：8， **Proofreader Number** ：none， **Stop Number** ：1，**fluid control**：none

3.1.1 User Name & Password

After Hyper Terminal set up well , click enter ,you will see below picture as（3.1.1）

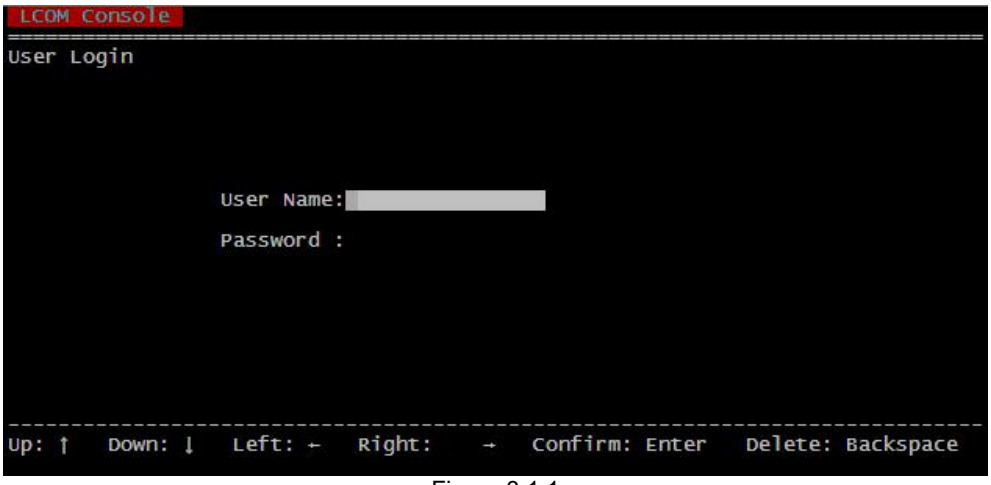


Figure 3.1.1

User name and password , default user name and pass word : admin, every line over please click enter , login success please enter control program .

3.1.2 Control menu

Control menu including : 1 basic info , 2 IP set up, 3 revert default ,4 go back windows. choose "↑"or "↓", click enter then choose sub-function module .

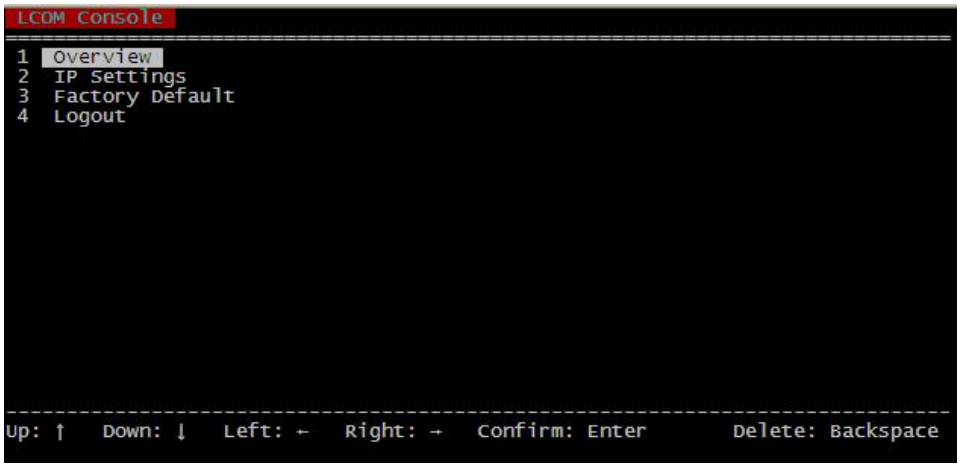


Figure 3.1.2

- Overview: check the system basic data
- IP setting : can use DHCP auto-allocate a static IP address , also can assign a IP address.
- Revert Factory Default
- Logout: go back to login windows

3.1.3 Overview

We can see Ethernet switch system info in overview sub-key, such as : Ethernet switch name , description, MAC address, Firmware Version . detail as below （3.1.3）:

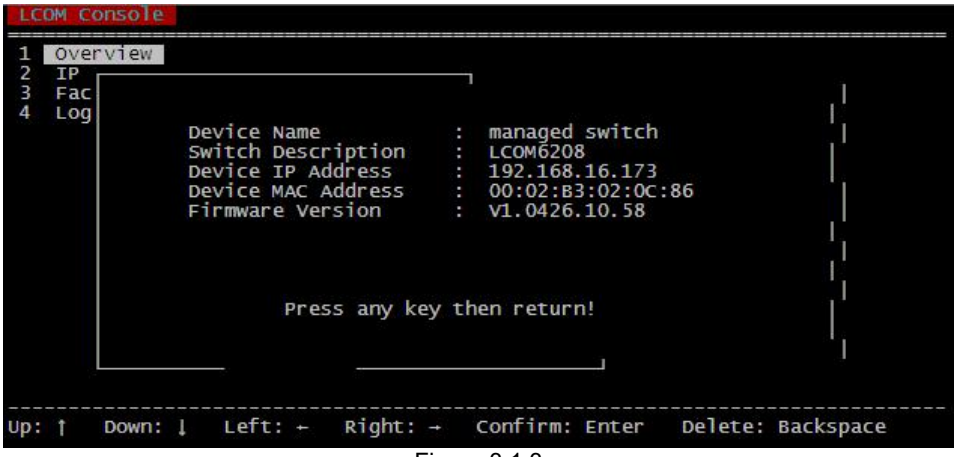
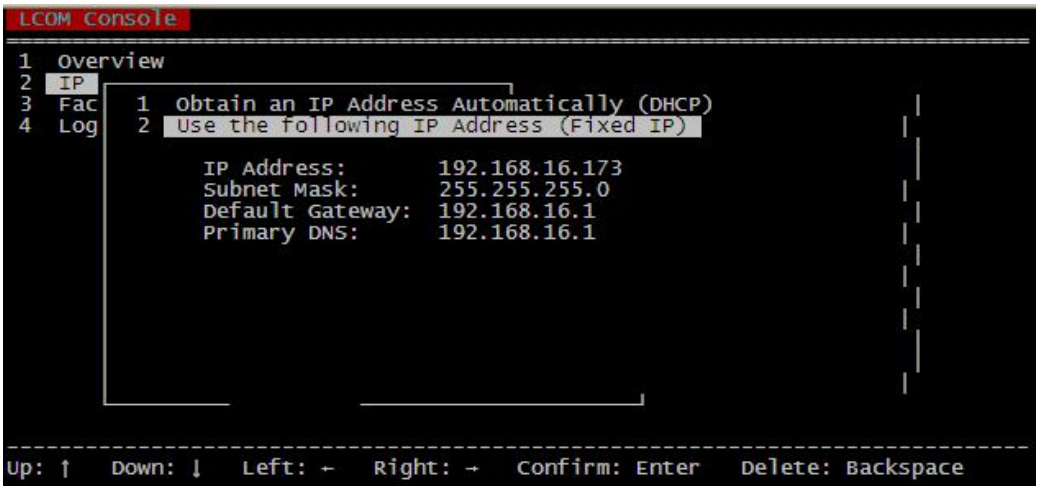


Figure 3.1.3

- Device Name：equipment name, user can through web management modify .
- Device Description：:equipment description , different model that term is different , user can not modify.
- Device IP Address: equipment IP address , user can modify .
- Device MAC Address：equipment MAC address, user can not modify.
- Click any key go back control menu ..

3.1.4 IP Settings

Through control program setting IP address , choose “IP Settings” as Figure below :



Can setting a new IP address . choose “Obtain an IP Address Automatically (DHCP)”, that series Ethernet switch can through DHCP , then use DHCP server auto-assign a IP address, when choose” Use the following IP Address (Fixed IP)”, can edit IP address （IP Address）.（Sub net Mask）.（Default Gateway）,DNS server four terms to setting a fixed network parameter.
After IP address ,

3.1.5 Factory Default

That function will revert all data specification to Factory Default.

Attention:

Revert successful , we suggest user cut off power of ethernet switch then turn on again , that can clean ram catalogue content . revert to factory default , please attention that IP address is : 192.168.16.253 , user need modify your network parameter, then you can visit Webmaster .

3.1.6 Logout Control Program

This managed Ethernet switch control program. To avoid modifying Ethernet switch core function by mistake, logout from control program, just go back to its login windows.

Chapter 4 WEB Managed Function

Illustration

All the function bellow, configuration based on final subject.

This managed Ethernet switch have inbuilt Web server, make convenient for visiting and configurating Ethernet switch . User can use IE.Firefox and other browser **(attention: system upgrading must used IE browser, other browsers will make mistake)** visiting that series Ethernet switch.
Through Web visiting that series Ethernet switch. Ethernet switch and PC must in same segment. Modify PC and IP address, make sure that it in the same LAN, Windows user please consult below steps:
Start----control----network & Internet connect---network connection----Ethernet adapter----nature---- Internet protocol（TCP/IP）
This managed series Ethernet switch default IP : 192.168.16.253. Setting PC IP : 192.168.16.X（X not including 253 ， can any number of 2---254）。
After modify PC and IP address, can use default IP address : 192.168.16.253, through Web visiting that series Ethernet switch and other configuration operation.
That handbook choose the switch model to illustrate , same series' different models just have difference in optic port and RJ-45 port.

4.1 WEB Login WEB

Open browser, searching that series Ethernet switch default IP address in the Address Field

Click enter , will popup a forms, Prompting login name and password.

4.1.2

Default user name and password all "admin". If user name or password input not right , that managed series Ethernet switch's Web Serve will offer three chances to input user name and password, if three times all wrong , browser will show "401 Unauthorized" mistake information. Input right user name and password, if identified okay , soon go to Web server windows, as

picture below:

Attention:

1.	That user can use IE.Firefox.google that browser visiting Web server, different browser Show pages may different , if effect the normal usage, please change to IE.Firefox.google
2	That Ethernet switch have using IE.Firefox.google that browser to do testing, all can normal use, we suggest when upgrading core program use IE browser, avoiding other browsers have problem .

4.2 System State

4.2.1 Equipment Information

- **Equipment name:** can modify by user
- **Equipment No:** describe Ethernet switch manufacturer settled number
- **Equipment description:** a brief introduction of Ethernet switch .
- **MAC Address:** that Ethernet switch managed system MAC address.
- **Hardware version :** current hardware version
- **Software version :** Current Firmware Version
- **Current Time :** When Ethernet switch turn on , the is 1970 Linux time, user can modify , if start ntp. When Ethernet switch connect with internet , time can auto—Synchronous with server clock.
- MT: from Ethernet switch turn on , timing begin . when Ethernet switch reset or cut off And restart, time will begin from 0.

4.2.2 Equipment State

Equipment in state , black lace bar represent system memory and CPU utilization rate。If you want to see the figure change , need refresh that page.
Memory utilization: Ethernet switch inside CPU have extended SDRAM，memory utilization also reflect used how much SDRAM.

Figure4.2.2

4.2.3 Port Information

When port connect well , the port background show black , connect not well or not connect, the background is white . when the port have latest connect , must refresh the page by hand ,then you can see .

Figure4.2.3

4.2.4 Menu & additional function

The webpage menu as below: system state, port setting, two-layer, link back up, visiting control, remote monitor , ports statistics, network diagnosis , system management .

Figure 4.2.4

Features	status	Function
System status	Equipment information	Equipment information， such as： name, number, software version, IP address, etc.
	Equipment status	Equipment status, such as: CPU utilization
	Port information	such as: number, port type, etc.
Port setting	Port setting	switch ports basic information, such as: speed mode, flow control status
	Bandwidth management	the rate of switch port management
	Broadcast storm suppression	set the type of inhibition of the storm
Lay 2 status	QoS	set 802.1p, port priority, DSCP priority, etc.
	VLAN	802.1Q VLAN and Port VLAN display a list of VLAN can be configured and managed, in the advanced settings there 802.1Q VLAN VLAN TRUNK
	IGMP Snooping	IGMP MAC address and set the corresponding port
	static multicast	Set the static multicast MAC address and its corresponding static multicast ports
Link backup	Fast ring network	Set fast ring network port and ring type
	port aggregation	port aggregation group
	Rapid Spanning Tree	Rapid Spanning Tree settings for more information
User management	user password	user privileges and passwords
	User management	modify the system's firewall to restrict access to the client IP address
	Port authentication	achieve the separate with business and certification
	Authentication database	stored on the database user name and password to add or delete
	MAC port locking	set MAC address with a port binding
Alarm monitoring	SNMP	SNMP alarm monitoring to manage the switching equipment
	Email log	E-mail to the user to specify the mailbox to send system log
Port Statistics	frame receive statistics	frame statistics of various statistics, such as unicast, multicast, etc.
	frame sent statistics	frame statistics of various statistics, such as unicast, multicast, etc.
	Total frame statistics	frame statistics of various statistics, such as unicast, multicast, etc.
	MAC address	MAC address table shows the situation
Network Diagnostics	port mirroring	set port mirror port and collection
	Network Diagnostics	analyzes network problems, network testing, or problem solving
System configuration settings	Time setting	system management time
	Address setting	IP address set
	System information	System information equipment model, CPU, and other related parameters or view
	Log information	display log information and management
	Document management	switch software update, acquire, preserve or restore the configuration of the switch

Every page right corner have logout link , at any time user can click logout , as below picture:

Figure 4.2.5

Click login again then you will enter identification windows.

The top right of the menu is the access to this; Lading IP address: 192.168.16.119 MAC address: 00:24:21:3E:AE:BC that is current PC(which visiting the Ethernet switch web server) ‘s IP address and MAC address.4.3 Port Setting

Port setting have three sub-menu: port setting , broadband management, broadcast-suppression

4.3.1 Port Setting

Port setting as below page :

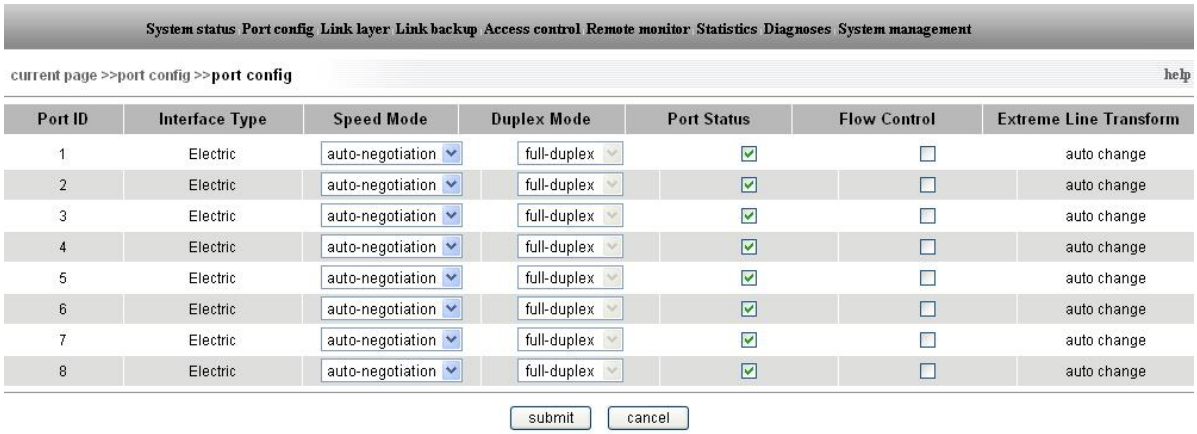


Figure 4.3.1

Picture （4.3.1）port setting is default setting , every setting as below :

Port ID : show the Ethernet switch’s all ports , as picture have 8 ports .

Interface Type : that show every communication port style , such as : RJ45 port or optic connector , above picture RJ-45 port and optic port have , have no related with connector.

Baud rate Mode :including auto—negotiation,10 M ,100M rate three kinds. Auto—negotiation is default , 10 M ,100M rate is force style.

Duplex mode: have 2 choice, full duplex and half duplex, just start using at enforcement rate(when auto-negotiation , its invalid)

Port status : If choose that port will use, if not choose , that port will forbid.

Flow control: flow control is used to manage data transferring of two node points, two node points must all support flow control is valid , If network equipment do not support flow control

Extreme line transform: MDI（Medium Dependent Interface）, MDIX(“X” cross line), that is the way Ethernet port connect to router, HUB , Ethernet switch . That series just use Auto-MDI/MDIX,have

auto –turn over function, that choice user can not change .

explanation

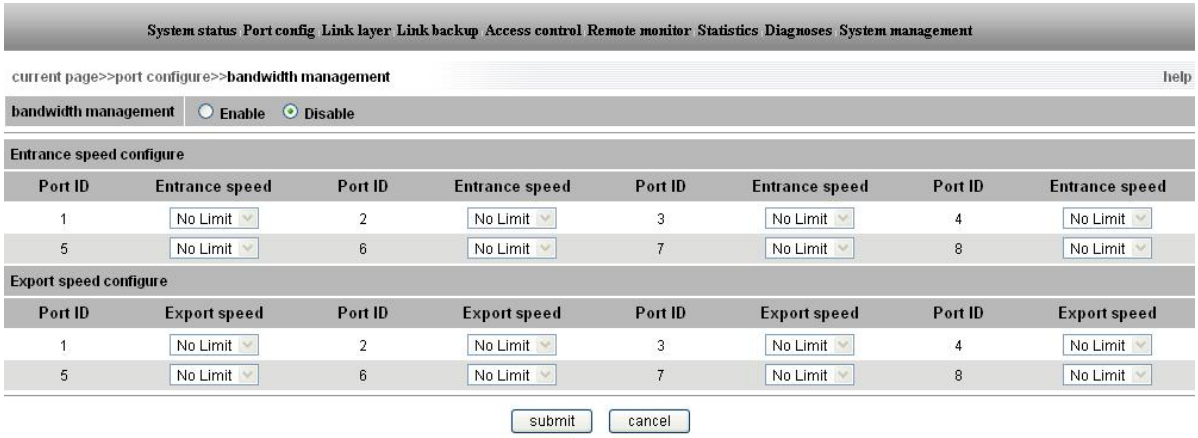
This management Ethernet switch supply Web page setting , all configuration parameters will submit to Ethernet switch after you click setting up. If you not click set up before exit the page , all modify that user make will cancel. Click “cancel” will not submit user modify.

Attention:

1. Auto-negotiation mode are all RJ-45 port default mode , when RJ-45 ports are all auto-negotiation mode , the connected equipment should also use auto-negotiation Mode, otherwise auto-negotiation failed the Ethernet switch ports will default half-duplex mode , lead to communication problem .
2. flow control is used to manage data transferring of two node points, two node points must all support flow control is valid , If network equipment do not support flow control , we suggest close that function.
3. Flow control can be started or forbid , default as forbid . Using flow control will generate many pause ifybc, if quantity too large , may cause pause ifybc storm ,so please choose flow control function carefully .

4.3.2 Band Width Management

That equipment supply port speed limited, including entrance and exist speed limited. User should choose a fixed speed, it scope in : 64Kbps ~ 100Mbps， the minist grain is 64Kbps. Port limited style including all single cast packet, multicast packet and broadcast packet. That equipment supply bi-directional speed limited. Entrance speed is PC and other equipment flow to Ethernet switch actual speed . exist speed is Ethernet switch flow to usage equipment actual speed. If limited two equipment entrance speed and exist speed , actual speed will be minimum figure.



4.3.2

Attention

1. When port arrived to appointed speed rate, Ethernet switch not limited speed at once, that Because entrance and exist all have 128k data slow down area, when that slow down area running out , it will turn speed limited.
2. When use port speed limited , if connected equipment all start flow control , the speed between equipment will be a steady curved line .Ethernet switch according if/not start flow

control to decided if/not throw away the excess flow message;

3. When use port speed limited, if both used flow control, should not happen packet loss problem . Packet loss will reflect as speed transferring sometimes fast sometimes low ;

3、 Port speed limited have high requirement of net network cable quality, otherwise will have a lot of impact packet and uncompleted packet.

4.3.3 Storm Control

When host system response a cyclic message grouping, or try to response a no response system will cause broadcast storm.

We use RSTP or **Mwring** Cisco prevent circuit generate, here we talked broadcast prevent is main to those network congestion. If start broadcast storm prevent function, can prevent that kind of attack. According broadcast storm style, our equipment can test four kinds of broadcast message.

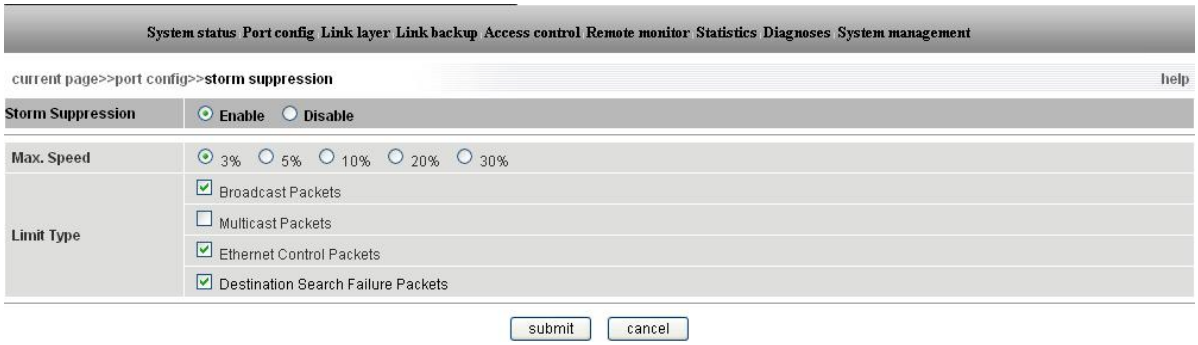
1.broadcast packet: Aim address is FF-FF-FF-FF-FF-FF data frames.

2,multi board packet : MAC address' highest byte 's low byte is odd data frames.

3. MAC FC Frame Control : when Ethernet length or type field 0x8808, that means this data frames is MAC FC Frame Control.

4. Destination checking fail frame: that data frames MAC address do not in equipment index table , need transmit to all ports.

Broadcast storm configuration as below （4.3.3）:



4.3.3

Max Speed Rate : all have 5 choices, 3%，5%，10%，20%，30%, 100M port basic speed rate is 100Mbps.

all configuration parameters will submit to Ethernet switch after you click setting up. If you not click set up before exit the page , all modify that user make will cancel. Click "cancel" will not submit user modify.

Attention:

1. Ethernet data frame extreme length is 1518B Byte, each 64Kb data communication traffic including 128pcs 64B Byte Ethernet data frame; in network broadcast packet more than 800pc/s , time delay obvious , and networks' broadcast flow usually 64B Byte Ethernet data frame; we suggest you setting as 3%.

2. Broadcast-suppression and broadband management are basic on same logic,broadcast-suppression is corresponding speed limit, and the suppression percentage also effect by slow down area. Speed rate change is a up-and-down curve line .

3. Destination address is multicast address but multicast list do not record destination checking fail packet.

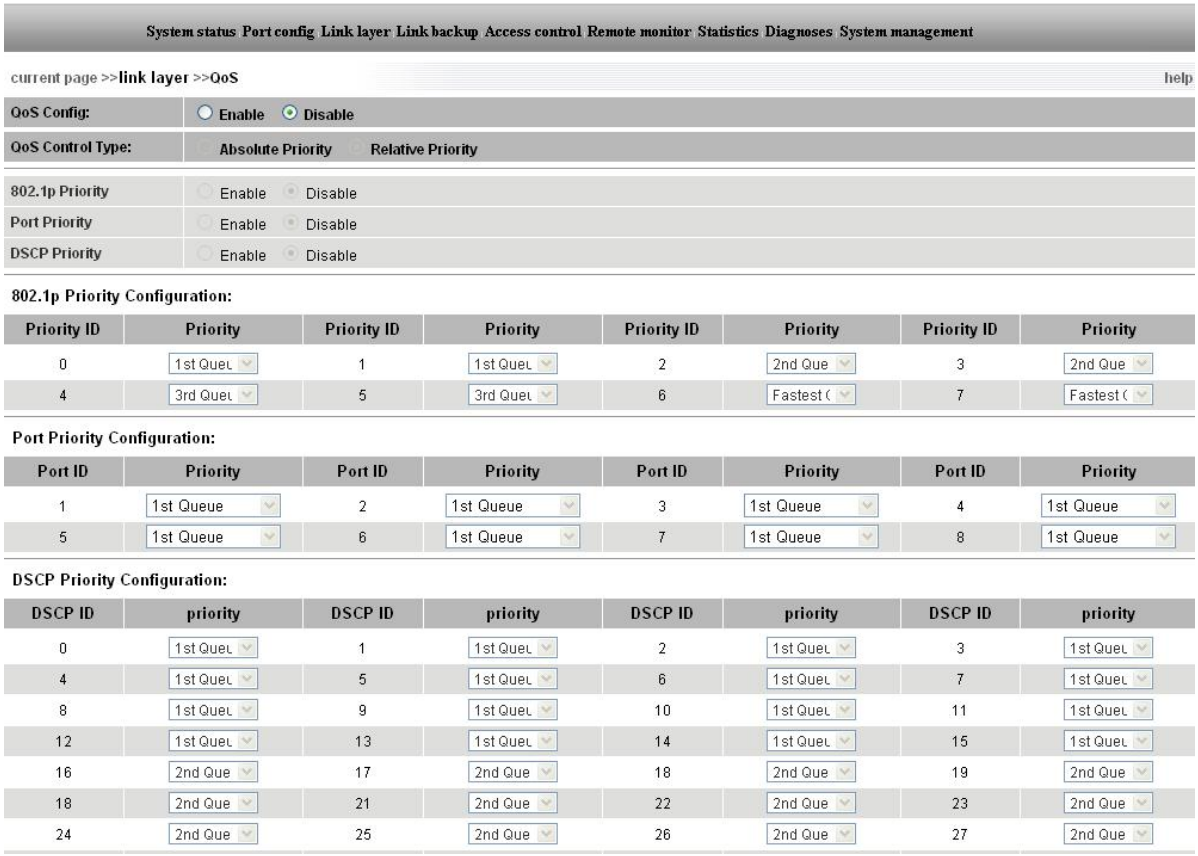
MAC control frame and destination checking fail frame please careful use , in doule ring network all around port use flow function, you had better start MAC control frame storm suppression

4.4 Layer Two Property

Layer two property setting including : QoS，VLAN，IGMP intercept, static broadcast list .

4.4.1 QoS（priority）

QoS（Quality of Service）is quality function, that will realize by switch chip' 4 interior priority line. Deal with different priority data packet, each port most 4 queues, QoS setting page as below（4.4.1）



4.4.1

When QoS forbidden , all choices are forbidden, if you want to setting QoS must first choose start, as below :

Then you choose absolute priority. relative priority when you choose absolute priority, Ethernet switch will frist deal with high priority queue data packet , then deal with low priority data packet, four queues transmit percentage from high to low

8：4：2：1，as below picture ：

QoS Control Type:	Absolute Priority	Relative Priority

Priority setting : 802.1P priority , port priority and DSCP priority, can start several kinds, ports priority have priority in those three priority setting ,as below picture:

802.1p Priority	Enable	Disable
Port Priority	Enable	Disable
DSCP Priority	Enable	Disable

As the port priority just can use ethernet switch 4 priority queues' maximum and minimum,
If one port use high priority queue, then all data packet enter from that port, will go to Ethernet switch highest priority queue , not IEEE 802.1P and DSCP priority setting condition, that mean Port priority have absolutely priority right to other two priority setting .

802.1P is IEEE802.1Q （VLAN Label technology ）standard expanding protocol, they work together. Generally it supply a QoS operation system at layer 2 （Media Access Control）. VLAN Label have two parts : VLAN ID（12bit）and priority（3bit）。IEEE802.1Q VLAN standard have no definition and use priority character, and 802.1P definite that character, so IEEE802.1P priority grade have 8(3 bits), IEEE802.1Q label have 3 pcs as user priority .

802.1p Priority Configuration:

Priority ID	Priority	Priority ID	Priority	Priority ID	Priority	Priority ID	Priority
0	1st Quel	1	1st Quel	2	2nd Que	3	2nd Que
4	3rd Quel	5	3rd Quel	6	Fastest (	7	Fastest (

Priority 0 is Default Value, and should start as not setting other priority value. Equipment default setting priority grade 0 and priority grade 1 map to the first queue, that is priority lowest queue. Priority 2 and priority 3 map to the second queue, priority 4 and priority 5 map to the third queue, priority 6 and priority 7 map to priority highest queue.

DSCP Priority Configuration:

DSCP ID	priority	DSCP ID	priority	DSCP ID	priority	DSCP ID	priority
0	1st Quel	1	1st Quel	2	1st Quel	3	1st Quel
4	1st Quel	5	1st Quel	6	1st Quel	7	1st Quel
8	1st Quel	9	1st Quel	10	1st Quel	11	1st Quel
12	1st Quel	13	1st Quel	14	1st Quel	15	1st Quel
16	2nd Que	17	2nd Que	18	2nd Que	19	2nd Que
18	2nd Que	21	2nd Que	22	2nd Que	23	2nd Que
24	2nd Que	25	2nd Que	26	2nd Que	27	2nd Que
28	2nd Que	29	2nd Que	30	2nd Que	31	2nd Que
32	3rd Quel	33	3rd Quel	34	3rd Quel	35	3rd Quel
36	3rd Quel	37	3rd Quel	38	3rd Quel	39	3rd Quel
40	3rd Quel	41	3rd Quel	42	3rd Quel	43	3rd Quel
44	3rd Quel	45	3rd Quel	46	3rd Quel	47	3rd Quel
48	Fastest (	49	Fastest (	50	Fastest (	51	Fastest (
52	Fastest (	53	Fastest (	54	Fastest (	55	Fastest (
56	Fastest (	57	Fastest (	58	Fastest (	59	Fastest (
60	Fastest (	61	Fastest (	62	Fastest (	63	Fastest (

Attention:

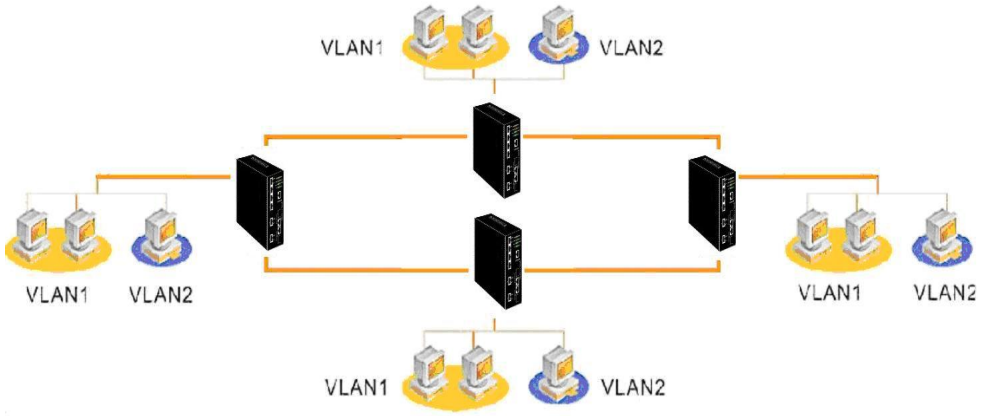
1. Ethernet switch inside just have 4 transmit priority queue, 802.1P and DSCP each have 8 and 64 priority grade, finally need realize by Ethernet switch, so the default setting802.1P and DSCP those priority grade will be same transmit queue, all packet in the same transmit queue have same priority grade in hardware, and in software they can setting as different priority grade .
2. The absolutely priority is first deal with the highest priority data, then deal with lower queue data, at last will deal with the lowest queue data; Relatively priority means deal with the highest queue data while process lower priority grade data, 4 queues transmit percentage from high to low : 8：4：2：1；
3. Three priority grade start at same time, priority grade from high to low\ is :port>DSCP>802.1P
4. Port priority just have two kinds, the highest and lowest; port priority grade will be highest in three priority grade cases, no matter how 802.1and DSCP setting , if port priority settled as lowest, then 802.1P and DSCP still can change its priority grade ;
5. 802.1P is extending of 802.1Q , priority identification will in VLAN Tag , so just valid for 802.1Q and VLAN packet.
6. DSCP priority identification in IP, so just valid for IP data packet; IP data frame priority can through the whole internet . DSCP down and IPv4 TOS compatible, admit and use three layer TOS priority grade case equipment to operate.

4.4.2 VLAN

VLAN means Virtual Local Area Network technology, VLAN also an effective method in net management, can suppress broadcast storm happen .
It support port VLAN and IEEE 802.1Q VLAN, but can not use same time , default start is basic on port VLAN.

Port based VLAN

Port VLAN supply a solve case that can divide Ethernet switch ports to different Virtual Local Area Network. In different Virtual Local Area, do not allow data exchange , so each Virtual Local Area data maintenance is more safe. About port VLAN, can consult below picture:



It support VLAN setting at each port, VLAN as a filter, intercept all none Virtual Local Area Network information. In default condition , start VLAN , have addition a default NAT, then put all Port in VLAN , as picture :

User can according ourselves requirement , through below Web page, setting port VLAN, right corner advanced setting bottom just work at 802.1Q VLAN, that is gray color, is forbidden state:

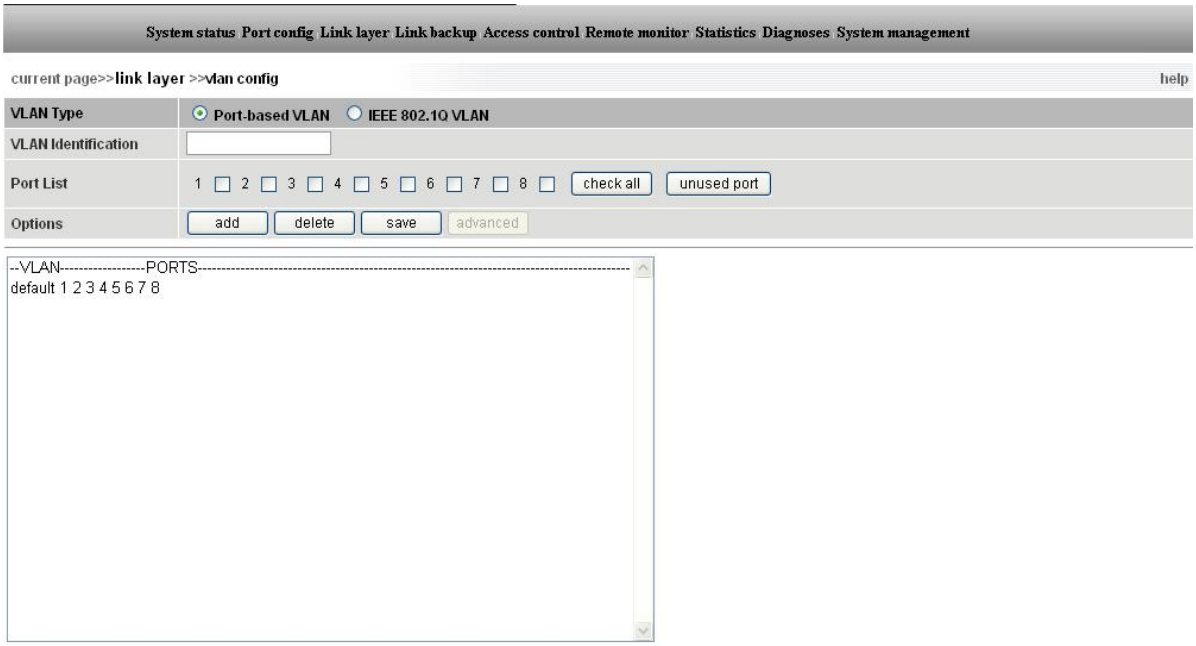


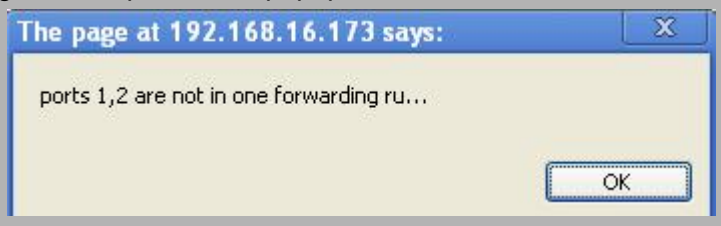
Figure 4.4.4

Step as below :

1. should add your VLAN, first delete default choice, click “delete choice”
2. Input need added VLAN name in the blank frame, must be figure or letter combination, as group 1;
3. choose add VLAN port from port list, right have two bottom “ choose not use port “ and “all choose “ can help user choose needed port more convenient.
4. choose port , then click” add “ then can add VLAN to that list.
5. use the same method to add new VLAN groups.
6. when add finished , if have left port do not add to any VLAN , need add those ports to a new VLAN.
7. Input VLAN name in frame, click”choose unset port” choose all unused ports, then add to list.

Attention

1. Should delete default choice first first .
2. All ports must add to a group of VLAN, such as port 1,2 do not add to any VLAN, then chick “save setting “, below picture will popup:

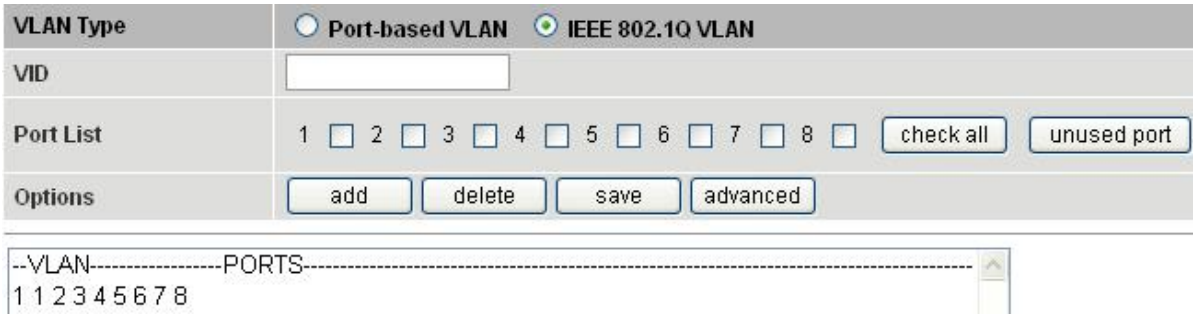


3. One port can add to several group of VLAN, that port can communicate with other ports in

its VLAN .

802.1Q VLAN

It also support IEEE 802.1Q VLAN。VLAN can divided through several Ethernet switch by IEEE802.1Q
protocol standard. That Ethernet switch support standard IEEE802.1Q protocol, compatible with other support IEEE802.1Q protocol standard Ethernet switch, also support 802.1Q label modify, can connect 802.1Q recognized label and 802.1Q non-recognized label equipment . Use that series Ethernet switch setting IEEE802.1Q VLAN very convenient . IEEE 802.1Q VLAN can setting the Web page as below :



4.4.5

802.1Q VLAN's VLAN add method as port VLAN , one point need stress is VID value must in 1~4094 figures. Default list already have a VID is 1 choice, all ports in VLAN:

Setting as below :

1. Need add itself VLAN, first delete default "VID is 1" that choice, choose 1 then click "delete"

2, Input you want to added VID in VID frame, must be integer , scope is1~4094；

3. Choose those ports that will add to VLAN, on the right have two buttons"choose not used port" and "all choose" could help user more convenient to choose.

4, choose port , then click "add " ,will add to VLAN list.

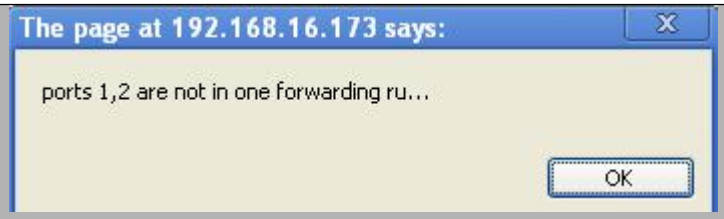
5, use the same method add new VLAN;

6, When add finished, if some ports do not add to any VLAN, need add those ports to a new VLAN;

7, Input need added VID in VID frame, click " choose no used port" , then add to the list.

Attention:

1. First delete the option which VID default as 1.
2, All ports must choose a VIAN to add , such as port 1,2 do not add to any VLAN, please click "save setting up", will popup as picture as below:



3 a port just can add to one 802.1Q vlan.

In the above VLAN setting Web page , when choose IEEE802.1Q VLAN , “advanced setting “ button been started, in port VLAN is forbidden, click “ advanced setting”, pop up （4.4.6） As picture.

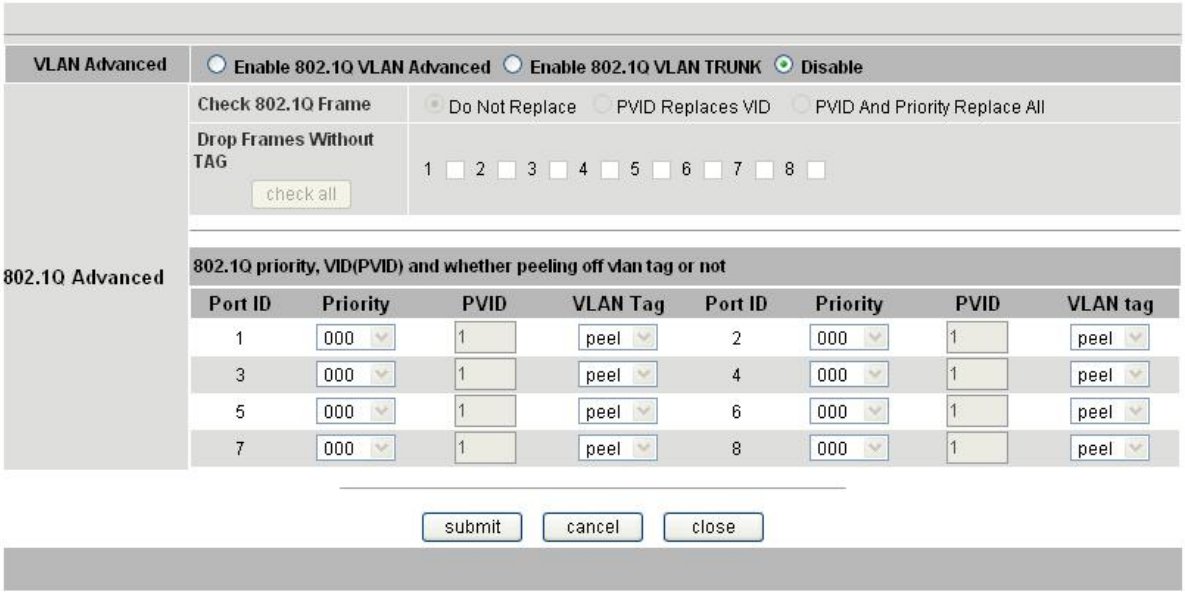
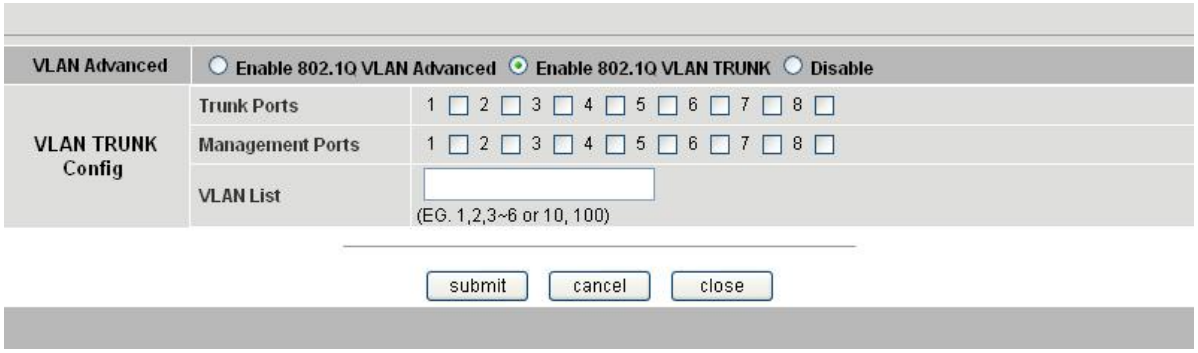


Figure4.4.6

Advance setting default is forbidden , the below option that gray color are in forbidden sate,click “start “ can setting , user can setting through that page , could do more subtle operation for the VLAN function, below will define how to do setting :

Enable 802.1Q VLAN TRUNK：start 802.1QVLAN TRUNK :

Vlan trunk function is make several ehternet switch connect network , then dived VLAN. The WEB page as below :



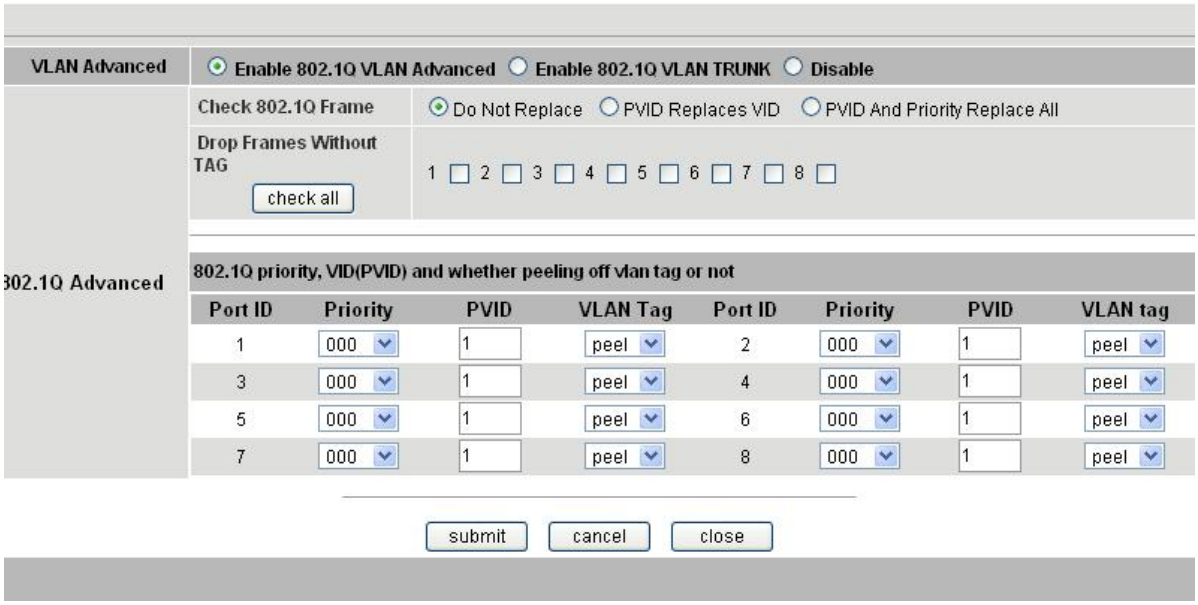
4.4.7

Trunk port list: which is assign to trunk;

Manage port list: just need one net setting, could manage the Ethernet switch in the net.

VLAN List : could list need used trunk port ‘s VLAN ID .

start use 802.1Q VLAN advanced rule



4.4.8

802.1Q frame checking:

VID that is add VLAN ‘s group id , scope is 1~4094; PVID is port vid, same with below “port VID”, user could setting PVID below; also can setting up priority. Replace function means some port use the below settled up PVID or priority replace the VLAN Tag receive from port. If not replace no need operate that function.

Discard no TAG frame: Assign some port receive no VLAN Tag data packet(not VLAN data packet), discard that data packet. That function user had better carefully use .

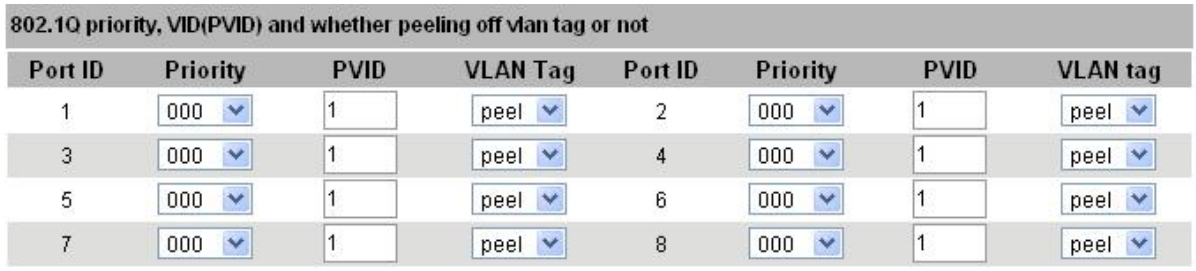


Figure4.4.9

Priority: setting port default priority part, all 3, so all have 8 priority choices, setting purpose is used to replace.

Port VID: As above said PVID, setting port default VID, setting purpose just used to replace.

VLAN tab: means VLAN packet transmit from that port, strip or reserve the VLAN Tag . usually strip function

Attention

1. Modify VLAN setting need delete default VLAN group, for it including all ports;
2. IEEE 802.1Q VLAN packet process :data enter into port---check if need attach or replace VLAN tab---check transmit list need transmit or discard---check if need discard VLAN

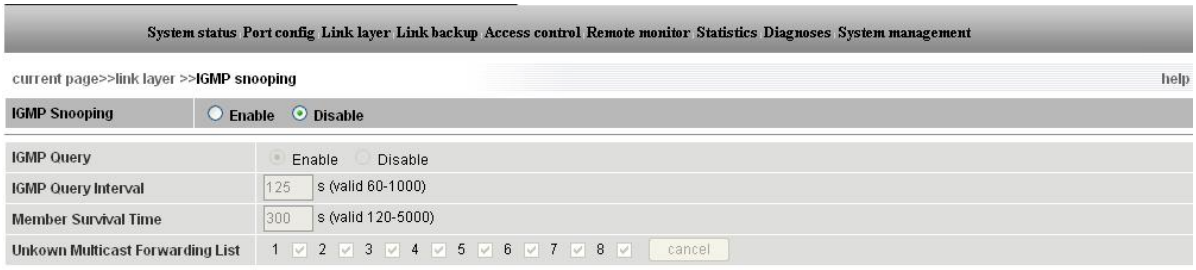
tab---data go from port

3. IEEE 802.1Q VLAN have a VLAN tab add and discard process compare port VLAN , about that kind of VLAN, just admit port is up-connect-port, or terminal port.

4 If start 802.1Q vlan, PVID will auto-update till consistent with vlan VID, as picture（4.4.8）

4.4.3 IGMP Snooping

It support internet multicast management protocol, Ethernet switch could auto-intercept IGMP data packet,
Auto-inquiry multicast members, and maintenance a multicast transmit list according multicast information trends.



4.4.10

IGMP Snooping function default as forbidden , use IGMP function need choose “start “ option, setting parameter as below :
IGMP Inquiry: choose if start multicast member inquiry function, IGMP query
Used to inquiry existing multicast, inquiry interval time , user can set by themselves. When multicast member received that inquiry query will answer a report, Ethernet switch received member’s report will update multicast list, count that member’s living time again , if inquiry several times , still not received the member’s report, Ethernet switch will delete multicast group member after them exceed member’s living time.
That Function could let Ethernet switch as IGMP ruler , when network do not have router or router do not support multicast , if network already have other IGMP inquiry equipment, could forbid that inquiry function, do not start that option will not check multicast members period, could reduce network load.
That function default as start

IGMP inquiry Interval : That choice will start after “IGMP Inquiry “ that option choose,
Time interval scope as: 60~1000s, default value is :125s. This time is software count , will have some errors.
Group member living time: Multicast group member living time, when member add into multicast group or received that member’s report (count living time again), If time exceed , that member will delete from this multicast group. Time setting scope is 120~5000s, default as 300s.
Member can add several multicast group, each multicast group will count time individually,
Unknown multicast group transmit list: when Ethernet switch received a destination address as multicast address data packet,
When start IGMP Snooping function, Ethernet switch will maintain a multicast transmit list , as below picture:

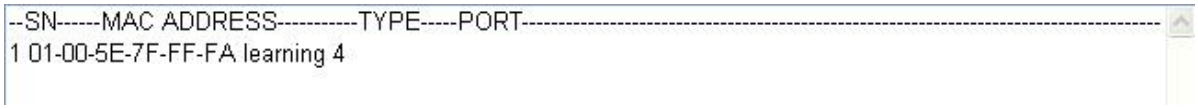


Figure4.4.11

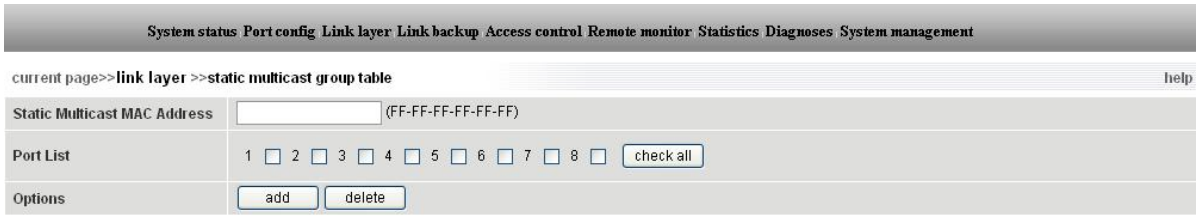
The option 2 is maintenance multicast address transmit option,

Attention

1.	If PC is one network port with IP address, Windows system always use the lowest IP address reply, that may have problem.
2.	Network had better not come several IGMP inquiry , or may waste resource.
3.	If not sure unknown multicast group transmit relationship, please choose all the ports.

4.4.4 Static multicast list

That Ethernet switch supply add/delete MAC multicast address transmit function by hand ,as below picture:



Picture 4.4.12

That statics multicast list and before

IGMP Snooping dynamic multicast list using the same multicast list, in-built Ethernet switch chip transfer address , not only keep learning function, and also support max 4k multicast MAC address and 256 multicast transfer ports, the difference is IGMP Snooping according IGMP protocol dynamic add/delete multicast list, and start ageing timing , delete outdated multicast group , and statics multicast list supply user add/delete multicast list, that list in multicast defined as statics , static MAC address transfer function, destination address including statics MAC address data packet will transfer to the appointed port. Specification

Statics multicast MAC address: input need added MAC multicast address, format is (FF-FF-FF-FF-FF-FF), multicast address the first three Byte are 16 binary 01-00-5E。

Port List: Choose destination address as multicast MAC address default transmit port, need transmit to which port , you can label it.

Figure4.4.13

Disposal List: That used to operate multicast list, push “add” & “delete” used to add/ modify/ delete static MAC address. Already existed static multicast list will show in the below format, when user open the Web page or operate add&delete will renew update the form , as below picture have add a multicast static transfer address（01-00-5E-00-02-01）.

ATTENTION:

1.add and delete operation will valid immediately, and do not need “save” as other page.
2.do not input unicast address as input address ;

3.please do not input saved multicast MAC address, such as : 01-00-5E-00-00-XX(save multicast management MAC address), 01-80-C2-XX-XX-XX(saved bridging Ethernet Management MAC address)

link Backup

Link Backup function setting : Mwring, Trunk port , RSTP.

4.5.1 Mwring

Mwring let Ethernet switch connect with redundancy link , when one link off , the other link can soon renew.

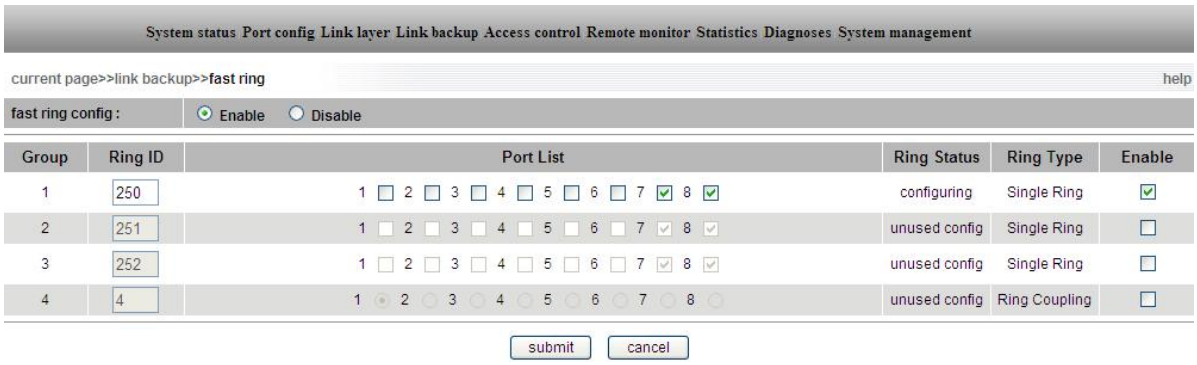
Mwring could let network self-healing time less than 20ms in a multi-ring network. Mwring technology admit user appoint some Ethernet switch ports as double ring redundancy port, connect with other Ethernet switches. When one way network off, Miring will use link backup, quick self-healing network communication. Below form is based on redundancy self-healing time compare, just for reference :

Form 4.2

Redundancy technology	**Mwring**	RSTP	STP
Self-healing time	<20ms	>5s	>30s

Usually , Miring technology need three or over three that series Ethernet switch connect a ring . Miring technology could construct two kinds of ring : monocycle ring , double-ring . monocycle ring is a basic unit, a monocycle ring usually use Ethernet switch ‘s two ports connect, as above picture show. Double ring is used to connect two or multi monocycle ring, double ring use two network wires separately connect four Ethernet switch as ring , as picture （4.5.1）:

Miring technology admit one network exist one or more ring , but each ring must have its own ID, that ID is share for all Ethernet switch in the ring . as picture （4.5.2）show :



Group: Each Ethernet Switch most support four groups of ring network , three monocycle ring, and a double ring . we suggest if use one monocycle ring is okay , then had better not start other network ring .

Ring status: above we said about ring ID, scale is integer from 1~254, each ring must have it own ID, all ethernet switch in this ring share the ID, that is Network Identification.

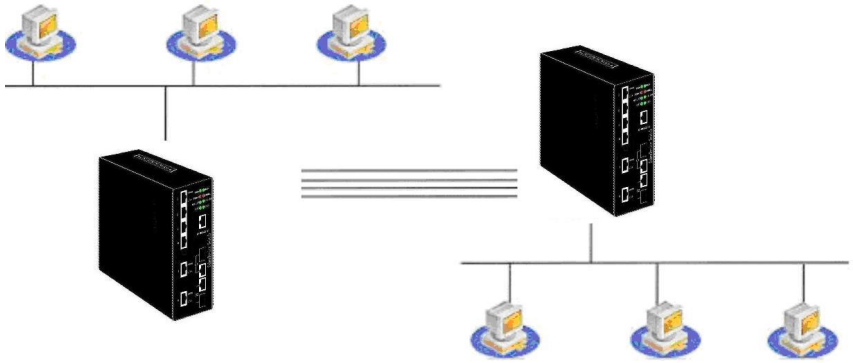
Ring type: choose access ring as which ports , access monocycle ring need 2 ports, coupler between rings just need 1 port,ports not in ring please not choose.

ATTENTION

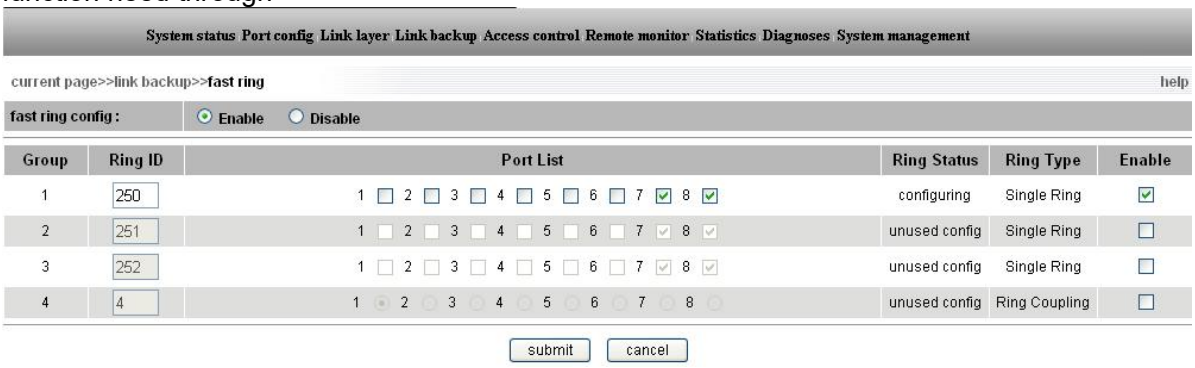
1 Miring is our company's private protocol , just can used in our companies same series Ethernet switc, can not compatible with other company's Ethernet switch.
2 Miring and RSTP could not use same time, when user use Miring, RSTP will close automatically, when use RSTP, Miring will close.
3 Self-healing time is <20ms (this time is test in a 4 Ethernet switches connect monocycle ring.)
Self-healing time closely connect with Ethernet switch quantity and its ring complication.
4 suggest user do not start too many ring network , if monocycle ring is okay , do not start double ring.
5 Attention, when start Miring, those ring network connect ports do not start TRUNK function, port mirroring,bandwidth
6 Now set the first group as default open, ring network construction ports default as 7,8 ports, ID is 250, when construct ring network , do remember not connect to the wrong ports, otherwise may create broadcast storm .

4.5.2 TRUNK

TRUNK main function is binding 2-4 ports as 1 logic channel , which not only update whole network bandwidth , and also data can transmit through those bind multichannel , have redundancy function. Below is a Trunk application picture(4.5.3):



Above is two ethernet switch build through Trunk construct a computer network, two sets of Ethernet switch use four ports connect , to update bandwidth and realize link redundancy .
It support Trunk function, it admit two groups of Trunk, each group including 2-4 ports as unit logic link, use to update bandwidth and link redundancy , when one connection can not communication or have problem , then supply a quick self-healing system. Allocate Trunk function need through



Trunk Group: That Ethernet Switch most support two groups of Trunk. .
Port List: choose ports allocate to each trunk group, each trunk group could allocate 2-4 100M ports, except port 1, others could add to Trunk group(port 1 could not use as Trunk). one port could not exist in two Trunk group same time . If port need add to Trunk , you can choose it

Super fetch : choose if super fetch the Trunk group, if need please choose √.

ATTENTION:

1 That Ethernet group most support three groups Trunk, 1,2 group each could consist of 2-4 100M ports.

2 port 1 could not use as Trunk, that means port 1 could not support Trunk function, could not add to any Trunk group.

3 one port could not exist in two Trunk groups same time , default setting as close.

4 use Trunk , must super fetch it , then connect.

5 Bandwidth update is decided by idt pci-e forwarding mechanism , not decided by ports quantity .

6 Trunk self-healing time very short , 100M braud rate do not lost package.

4.5.3 Rapid Spanning Tree Protocol (RSTP)

STP protocol to address this shortcoming, the century and the beginning of the IEEE 802.1w standard introduced as a supplement to the 802.1D standard. Standards in the IEEE 802.1w Rapid Spanning Tree Protocol defined in the RSTP (Rapid Spanning Tree Protocol). STP RSTP protocol based on the agreement made three important improvements, making the convergence rate is much faster (less than 1 second fastest).

The first improvement: the root port and designated port is set to replace the use of fast switching ports (Alternate Port) and backup port (Backup Port) two roles, when the root port / port failure specified circumstances, replace the port / port for backup will enter the forwarding state without delay. Image above all bridges are running RSTP protocol, SW1 is the root bridge, if SW3 is the root port the port2, port 1 will be able to identify this topology, a replacement of the root port port, enter the blocked state. When port 1 case where the link failure, port 2 will be able to immediately enter the forwarding state, twice the Forward Delay time without having to wait.

The second improvement: in only two switch ports connected point to point link, specify the port just once shook hands with the downstream bridge can enter the forwarding state without delay. If more than three bridges connecting the shared link, the downstream bridge upstream of the specified port will not respond to requests issued by shaking hands, twice the Forward Delay can only wait for time to enter the forwarding state.

The third improvement: rather than directly connected terminals connected to the other bridge port is defined as the edge of the port (Edge Port). Edge of the port into the forwarding state directly, without any delay. Because the bridge can not know whether the port is directly connected with the terminal, you need to manually configure.

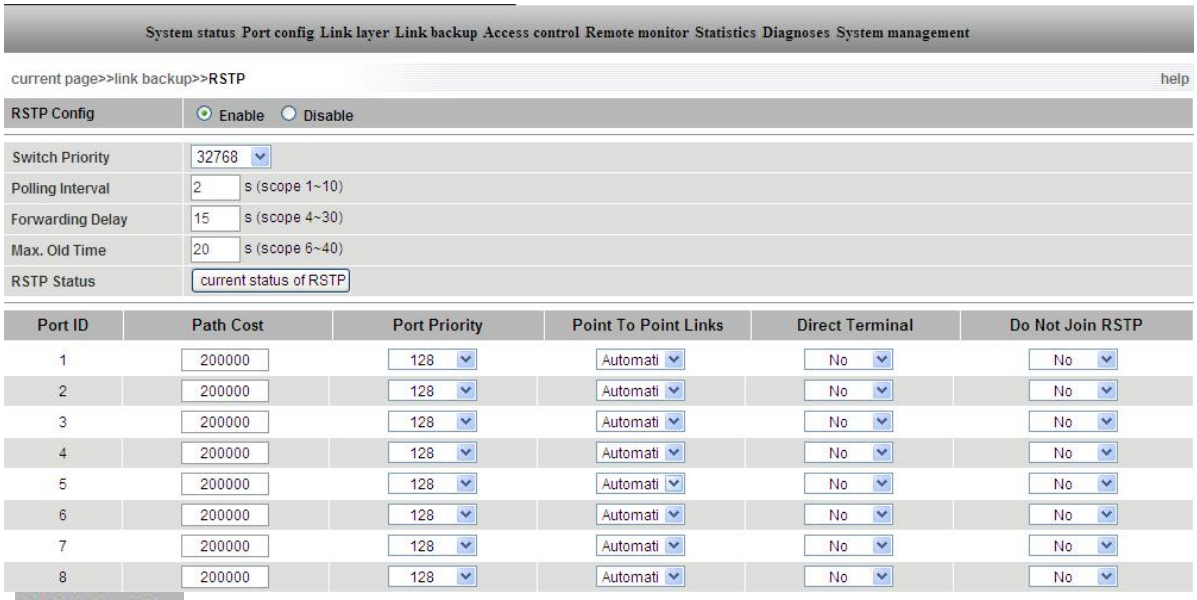
Visible, RSTP protocol relative to the STP protocol is indeed improved a lot. To support these improvements, BPDU made some changes to the format, but is still backward compatible with STP RSTP protocol agreement to the hybrid network.

(STP) Brief Introduction

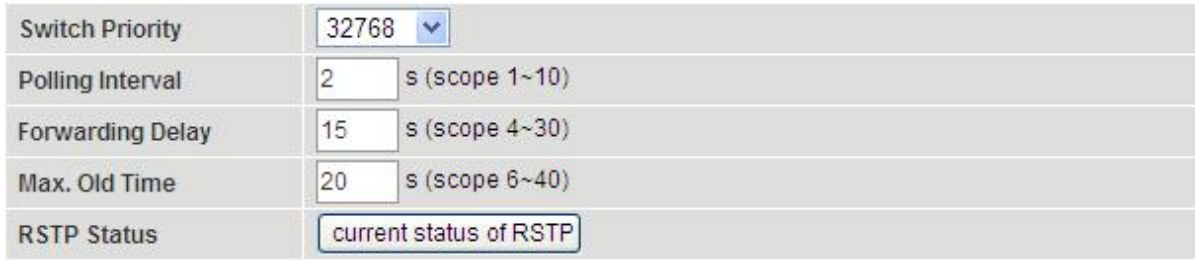
STP is a two layer management protocol, selectivity block network redundancy link to ease network 2 layer , and have link spare function.

（RSTP） for configuration instructions

Click RSTP menu, then will pop below allocation interface:



RSTP Config: Enable / Disable Fast Spanning Tree feature is disabled by default, Rapid Spanning Tree and Rapid Ring feature can not be enabled, such as the opening of the RSTP, it will automatically shut down quickly ring the same token ring network is enabled fast, it will automatically Disabling RSTP. When enabled, when the RSTP, RSTP will first disable all the ports, such as the convergence of business, will enable and block certain ports, during which the Web server will lose the response, when the convergence of the end, the network tree generation, you can re-use Web server.



Switch Priority: setting Ethernet switch (bridge) priority, Ethernet switch priority and Ethernet switch MAC address composed as bridge ID, which Ethernet switch bridge ID is minimal , its will as network's root bridge. The minimal the figure, it more possible as root bridge, default figure as 32768.

Polling Interval :setting Ethernet switch how many time send BPDU data package once, if interval time is short will speed up self –healing , but also will Increase the network load, the figure set too big, will make the RSTP self-healing time longer. Default value is 2, value scale is 1~10 integer ,unit as second..

Forwarding Delay :Ethernet switch port status in listening and learning , maintain a forward delay time, unit as second. Default is 15, figure scale is 4~30 integer.

Max. Old Time : Maximum aging time: one Ethernet switch receive a BPDU data package from other Ethernet switch, this data package valid time ,default figure is 20, default unit is second, figure scale is integer from 6~40.

Time setting figure need below formula: 2*（forward delay-1）>= Maximum aging time
RSTP status information: click RSTP current status button And check RSTP status information, as below picture:

RSTP Status : Click current status of RSTP to find the RSTP status information, as shown in Figure (4.5.8) as follows:

RSTP Status

Root Device Information:

This Switch ID	8000-0002b3020c86
Root Switch ID	8000-0002b3020c86
Root Switch Port	NULL
Root Port Path Cost	0

Switch Information List:

Port	Priority	Cost	P-to-P	Edge Ports	Connected Network	Port Role	Forwarding Status
1	128	200000	Y	N	Rapid	Unknown	Disabled
2	128	200000	Y	N	Rapid	Unknown	Disabled
3	128	200000	Y	N	Rapid	Unknown	Disabled
4	128	200000	Y	N	Rapid	Designated	Forwarding
5	128	200000	Y	N	Rapid	Unknown	Disabled
6	128	200000	Y	N	Rapid	Unknown	Disabled
7	128	200000	Y	N	Rapid	Unknown	Disabled
8	128	200000	Y	N	Rapid	Unknown	Disabled

close

Figure 4.5.8

That page show current network root bridge is root Ethernet switch MAC address 00-02-b3-02-02-02 not local address, local Ethernet switch port is 2, so port 2 as forward state , additionally 3 ports are designated port, also in forward state, but port 6 is blocked, that means port 6 redundant link. That page information show RSTP current state, RSTP always in motion detected， negotiation process, each time the page update , you will see the newest state , so each time update , you get information is different.

Forwarding Status: port operation state have four kinds :

Disabled: That means port do not connect .

Discarding :in that state could receive BPDU data package, if this period not receive BPDU then change to learning state, when link just connect to ports will in discarding state.

Learning : Learning state, a time to receive data packets, connectivity is turned on immediately after the switch stays in the blocked state max age = 20s time to determine the switch port it is possible to become a root port or designated port, send and receive BPDU packets during to complete the election of the root of spanning tree, construction, completion port status whereabouts decision. If the decision is the root port or designated port, then to stay forward delay (= 15s) time, and continue to the port can not be calculated to determine the root port or designated port, this time with learning MAC addresses. If it is the root port or designated goods to the forwarding state after conversion, if not, then switch to the blocking state.

Forwarding : Forwarding state, the port can now send and receive normal packets.

To speed up the healing process RSTP to reduce network load, the user can configure the port the following pages more information:

Port ID	Path Cost	Port Priority	Point To Point Links	Direct Terminal	Do Not Join RSTP
1	200000	128	Automati	No	No
2	200000	128	Automati	No	No
3	200000	128	Automati	No	No
4	200000	128	Automati	No	No
5	200000	128	Automati	No	No
6	200000	128	Automati	No	No
7	200000	128	Automati	No	No
8	200000	128	Automati	No	No

Figure 4.5.9

Path Cost ::Port path cost: port link cost and port priority forming ID use to compare, link cost is decided by physical link, user could according physical to modify the figure .default 100M port link cost as 200000.

Port Priority: Port Priority: ports priority and port link cost forming port ID as compare , that value smaller priority higher, default is 128.

Point To Point Links: Point to point network connection: Ethernet switch port and Ethernet switch port just have direct connection, that port is port to port connection. RSTP according to point to point link negotiation

Direct Terminal: Directly connection terminal: network remote Ethernet switch usually connect with terminal equipment , such as PC ,station. If allocate these ports(which connect with terminal equipment) as Edge ports, could realize port state quick swift, no need Discarding，Learning，Forwarding swift process, could realize port state quick swift.

Do Not Join RSTP: Not attend STP structure: That designated port not attend STP protocol operation , that could reduce port quantity, reduce RSTP operation complication, then reduce RSTP self-healing time

1 RSTP protocol according with 802.1w standard, our company's Ethernet switch RSTP protocol could compatible with other companies network equipment which also support standard RSTP protocol.

2 RSTP and rapid ring function can not open the same time , if start RSTP, will automatically close rapid ring, also if start rapid ring ,will automatically forbid RSTP.

3 when start RSTP, RSTP will first forbid all ports, after network tree generate , could use Web server again .

4 when link change , RSTP will have a self-healing time , may cause Web server can not visit , after Self-healing finish, can visit again.

5 After RSTP start, each Ethernet switch will send inquiry package from each port according different time interval , so this will add network load.

6 Max aging time and transfer delay need meet below term ; 2*（transfer delay-1）≥ Max aging time.in order to reduce network computer complicated ,reduce self—healing time, sugges user setting port information, reduce port quantity; reduce transfer delay, max aging time speed

4.6 Visit Control

Visit control function setting : user password, login control, port identification, authentication data base, MAC port lock.

4.6.1User Password

Ethernet switch Web server offer three groups of different user name and password, each group could choose two grade, to protect Web server visit, just know user name and password could login Web server, could manage Ethernet switch.. through change user index, user name and password could add , delete and modify. If user name and password is blank, And system delete this index represented user name and password. That series Ethernet switch when delivery, default user name and password ”admin”, visit grade is manager.

User name and password must fit for logic character, consist of English letter(distinguish capitalization) and figure consist of , user name can not blank, but password can blank, user name and password max length is 32bits. If current login user name or password modified and different as before , when you visit again, will let you input user name and password again.

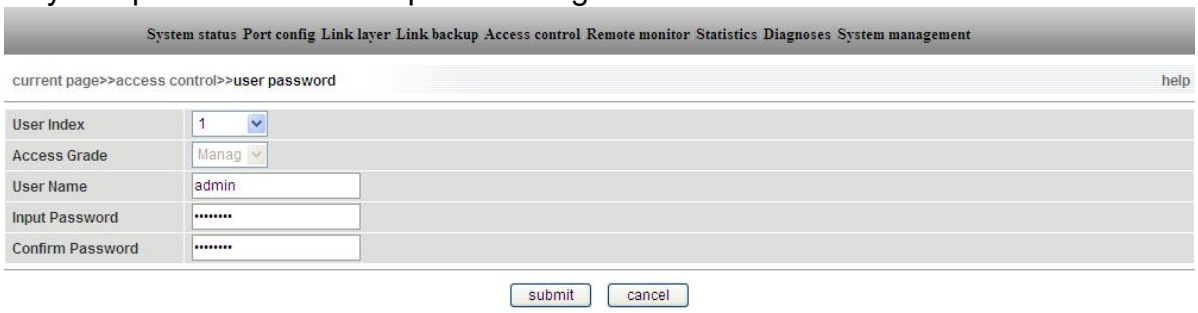


Figure 4.6.1

User Index :User Index: user name and password index is figure 1~3, total 3 groups.

Access Grade :Visiting Grade: have two grades, as administrator and observer, administrator have right to check and modify , observer just have check right. the first jut can set as administrator mdoe.

User Name: set that group user name , user name could consist of English letter(distinguish capitalization) and figure consist of , user name cannot as blank , max length is 32bits.

User Name : User Name: set that group user name , user name could consist of English letter(distinguish capitalization) and figure consist of , user name cannot as blank , max length is 32bits.

Input Password : Input password: setting this group user password, password could consist of English letter(distinguish capitalization) and password can be blank, max length is 32bits.

Confirm Password : Confirm password : input password again, make sure the password not input wrong .

1 The first group just can set as administrator mode, that make sure at least one group is administrator mode.
2 user name and password could consist of English letter and figure, suggest user not use Chinese , in order to keep safety, suggest administrator first time login , please modify default the first group user name and password.

3 when user login enter into Web server, if server not work in 5 min , this login will invalid The operation Web page will ask user login again, this is to prevent others will make mistake operation when administer not in. That time is computer time, not very accurate .

4 user could click page right corner “exist” to logout Web server, then active again.

4.6.2 Login Control

Login Control function through modify system firewall to restrict visit customers IP address, then restrict Web server visiting , Web allocation as below :

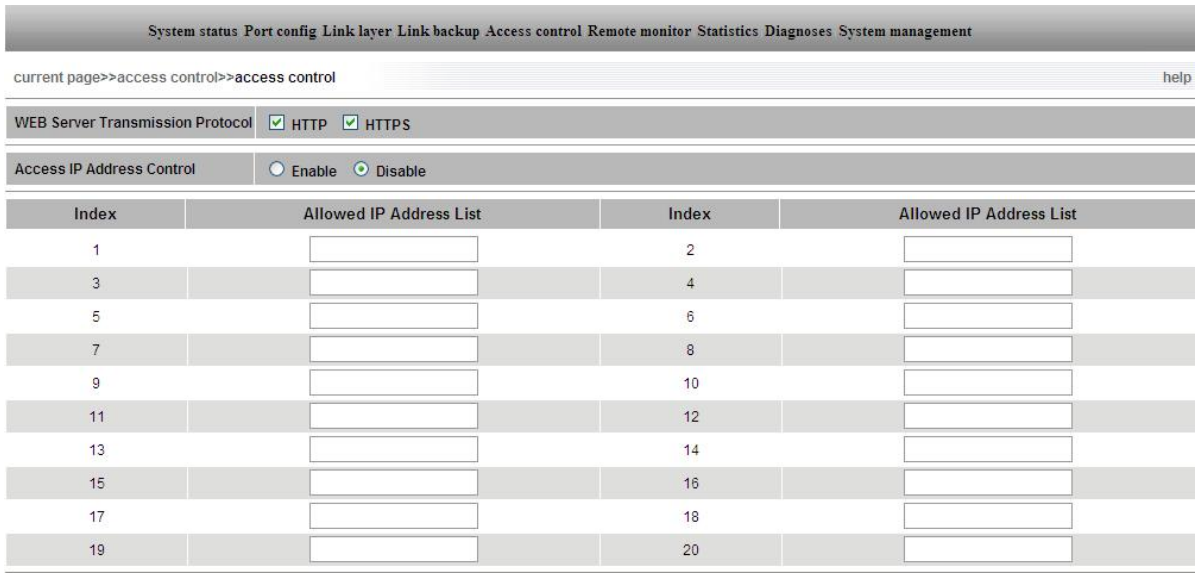


Figure 4.6.2

WEB Server Transmission Protocol: WEB server transmission protocol: this option use to start WEB server support transmit protocol, default as support http and https two kinds , suggest user not modify this option.

HTTP: HTTP（Hyper Text Transfer Protocol）, used to transmit WWW data , more detail information please refer RFC2616. User input http://192.168.16.253, then visit Web server.

HTTPS:HTTP（Hyper Text Transfer Protocol）, used to transmit WWW data , more detail information please refer RFC2616. User input http://192.168.16.253, then visit Web server.
HTTPS: HTTPS is HTTP protocol safety version,
User input https://192.168.16.253, then click enter , could through https protocol visit Web server, may pop below warning :

Figure 4.6.3

Click “yes” can continue, when login first time , home page will show not normal, that because web page

Script operation not normal, freshen several time , then will show normal.

Access IP Address Control :Access IP Address Control: through modify system firewall, Ethernet switch offer advance communication filter function .when start this function , just designated IP address computer could visit this equipment, other not list IP address computer will forbid.

Allowed IP Address List: Allowed enter into IP address list: input network equipment IP address in the frame , all admit 20pcs records, user could use several terms , user at least setting one pc IP address list , and this address list could not as Ethernet Switch itself address, otherwise Web server will not visit.

1 HTTP.HTTPS must use at list one kind of visiting protocol；
2 Some browser use HTTPS , when first open home page will not totally show, that is network script not working normal ；
3 Visit IP address must be a legal IP address, at least should have one address in the same segment, otherwise equipment will judge as setting invalid.
4 Address list admit entered IP address, so at least setting one adder, otherwise this Web server can not visit;
5 Could not use Ethernet switch itself address input, for if you just admit this address , will make mistake , and will cause can not visit Web server.

4.6.3 Port Authentication

IEEE 802.1X authentication architecture adopted the "control port" and "control port" of the logic function, which allows the separation of business and certification. User authentication, traffic and certification flow to achieve separation, the follow-up data packet processing has no special requirements, the business can be very flexible, especially in carrying out the business aspects of broadband multicast has a great advantage, all businesses are not subject to certification way limits.

802.1X structure of three main components:

1. Applicants supplicant: want authenticated users or customers.

2. Authentication server : a typical example of the RADIUS server.

3. Authentication system authenticator: on the connection between devices such as wireless access points, switches and so on.

Our equipment can play a certification system and the authentication server roles, you can also use an external authentication server, while supporting the external billing system. Port authentication page shown in Figure (4.6.4) as follows:

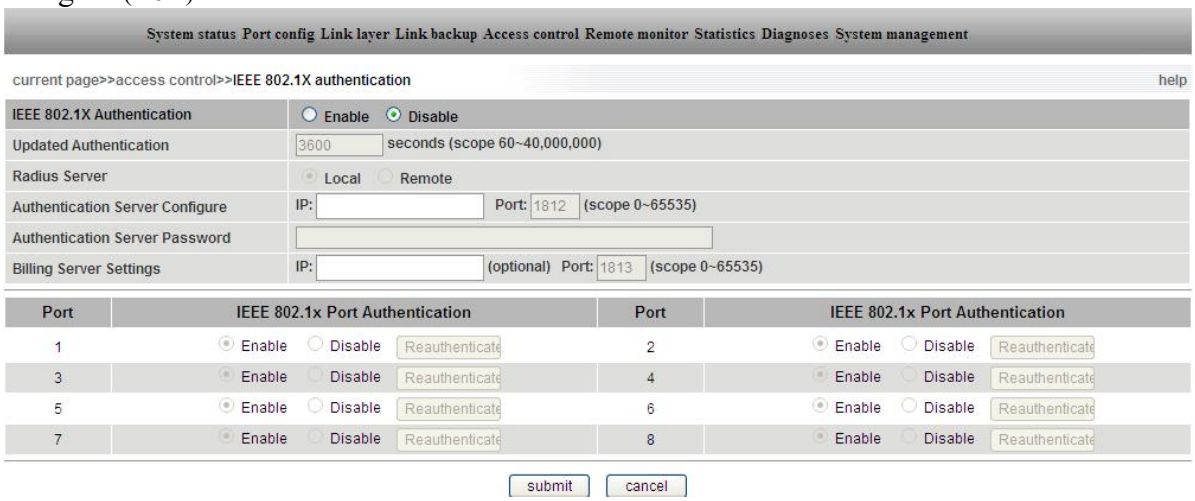


Figure 4.6.4

Updated Authentication: 802.1X re-authentication cycle time, more than this time, the last successful authentication failure, to be re-certified, used to enhance the security of authentication. The setting range is 60 to 40 million seconds, default is 3600 seconds, that is to be re-certified every time 1 hour

Radius Server: RADIUS server: have Local and Remote two options.

Local Is the use of the switch as a RADIUS authentication server, the switch built-in Radius server, the applicant will only use the switch inside the Radius database user and password, the following three are disabled;

Remote Is used to switch an external Radius server local port on the switch for authentication, external Radius authentication server refers to non-switch built-in Radius server, the switch built-in Radius server can not serve as a remote authentication server, the other switch. Enable this option, the following three have been enabled, billing server, optional to fill in, the rest is required.

Authentication Server Configure: This option in the selection of After the server will be, fill in the remote server's IP and port, set the IP address must be accessible to the device, the default port is 1812.

Authentication Server Password: This option in the selection of After the server will be, fill in the switch to access the remote authentication server share the password string.

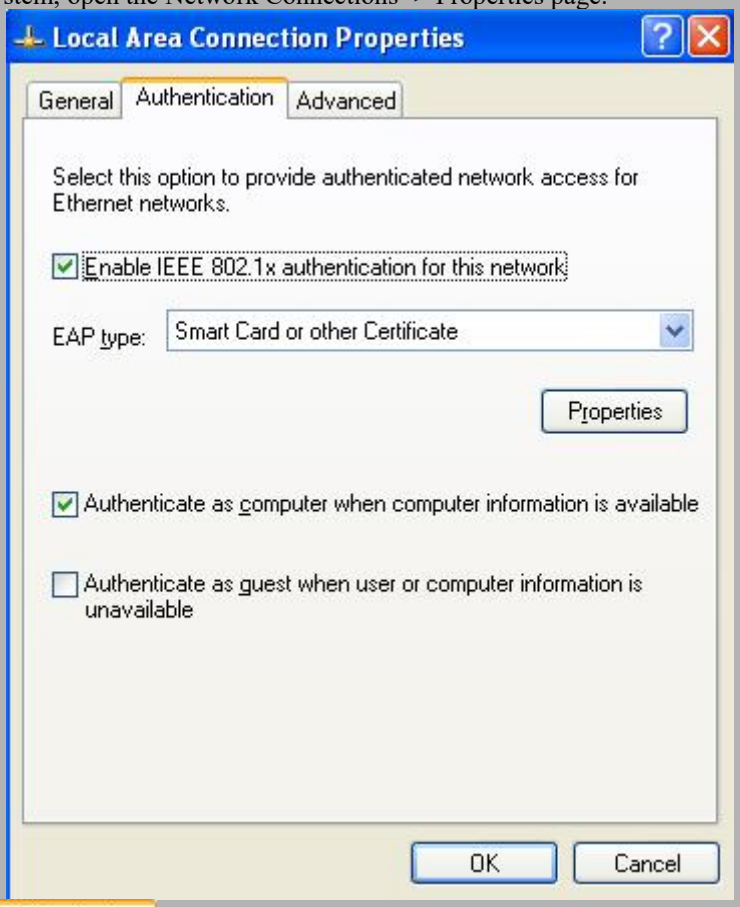
Billing Server Settings: This option in the selection of After the server will be able, for the optional settings, billing server, billing function is implemented, set IP address must be accessible to the device, the default port is 1813, accounting server configuration errors can cause the applicant Through authentication, accounting server does not need to set.

Port	IEEE 802.1x Port Authentication	Port	IEEE 802.1x Port Authentication
1	Enable Disable Reauthenticate	2	Enable Disable Reauthenticate
3	Enable Disable Reauthenticate	4	Enable Disable Reauthenticate
5	Enable Disable Reauthenticate	6	Enable Disable Reauthenticate
7	Enable Disable Reauthenticate	8	Enable Disable Reauthenticate

Figure 4.6.5

Part of the picture above to set a Yes / No enable the corresponding port 802.1X authentication, if enabled, the port before the adoption of the certification in a "failure" state, the certification will be passed forward into the normal state. Click Reauthenticate Button to make the last authentication failure, need to re-authenticate the port.

1 In the windows system, open the Network Connections -> Properties page:



If you do not find Authentication Tab, select "Control Panel" → "Administrative Tools" → "Componen Services" → "service", enable the "Wireless Zero Configuration" and "Wired AutoConfig" service. In Optio

to use MD5-question, otherwise do not support. shown in the diagram;

2. If you enable 802.1X authentication, and set the authentication database user name and password, in the windows system, a network connection, an authentication dialog will appear as follows: Enter the user name and password set can be certified

3 If the user access to Web server uses the switch port authentication is enabled, when the authentication is started, the user can not access normal Web server, to be certified to re-access the Web server, this is a normal phenomenon, not a fault behavior;

4 All uplink port, the second line port and billing server port must be forced through certification, the "forbidden to" certification, or can not use the remote server, unless the internal authentication server;

5 Billing errors also cause the server to set the applicant can not authentication, accounting server if there is

no need to set;
6 Use a remote server, make sure the administrator can access the remote server device, the "device address" in the gateway settings are correct, If you use a domain name, DNS must be set correctly;
7 The built-in authentication server of the switch, the switch can not be used as a remote authentication server to another;
8 If the authentication database, without any user name and password, then all ports automatically certified.

4.6.4 RADIUS Database

RADIUS is a remote user dial-up authentication system (RADIUS: Remote Authentication Dial In User Service), the network access server (Network Access Server) and share transfer between authentication server authentication, authorization and configuration information of the agreement. RADIUS uses UDP as its transport protocol. In addition RADIUS network access server is also responsible for sending and sharing of billing information between the billing server.

RADIUS authentication database as 802.1X authentication, authorization part, save for multiple authentication user name and password, the user can use this page to save the database user name and password to additions and deletions. Any applicant found the user name and password database matching rules, the device authentication system that is licensed to the applicant. RADIUS authentication database configuration page as follows:

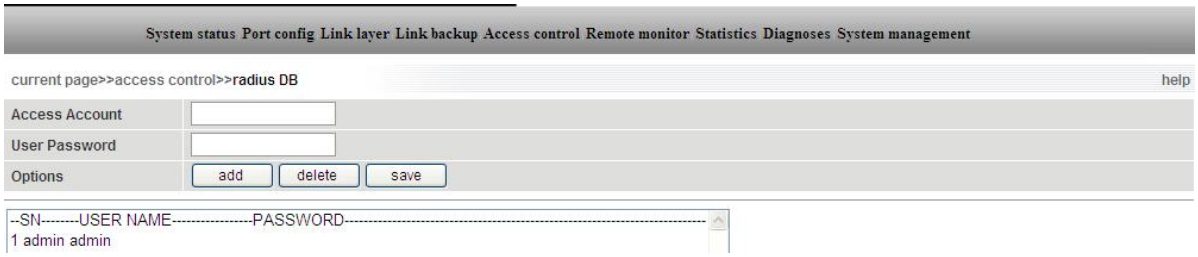


Figure 4.6.6

Access Account : Set new authentication user name, by a less than 16 bytes of numbers, letters (case sensitive) component.

User Password : The new password is not greater than a 16-byte numbers and letters (case sensitive) component.

Options : Click add And delete The box in the following table is used to add and delete user names and passwords, all the additions and deletions have to click save Button to submit to the switch, and will trigger a database update and the start 802.1X authentication. After clicking save Button to exit this page before, all changes have been revoked.

ATTENTION:

1. click " add " and " delete ", additions and deletions will show changed in table box but not save, just click " save " button those change will submit to Ethernet switch , and will trigger a database update and restart the 802.1X authentication.

2 Please login using the 802.1X standard tools such as windows comes with tools such as the 802.1X login H3C tool users have a custom field byte, this device could not land;
3 The total number of user groups is not more than 128;
4 Local Radius Authentication is not enabled, the contents of the database is actually invalid;
5 If the authentication database, without any user name and password, then all ports automatically certified.

4.6.5 MAC Port Locking

MAC port locking refers to the forwarding address of the switch manually add a static MAC address and the address and a port binding, all data sent to this address will only be forwarded to the port, also known as MAC address tied set.

Static MAC addresses are different from the dynamic MAC address learning, aging dynamic addresses for more than the maximum is deleted after, after over maximum aging time dynamic address will be deleted, once static address be added , the address will not limited by maximum aging time, if we not delete it , will always exist. A static MAC address corresponds to a port, that is called a static address and port binding , binding aimed at limiting movement of the computer, any computer MAC and port binding ,this computer swift to another non-locking port can not communicate, and other computer swift to this binding port can communicate. For the MAC address binding is, therefore, limits the computer, and this protect ports, which limits the port. The function of the configuration page as follows:

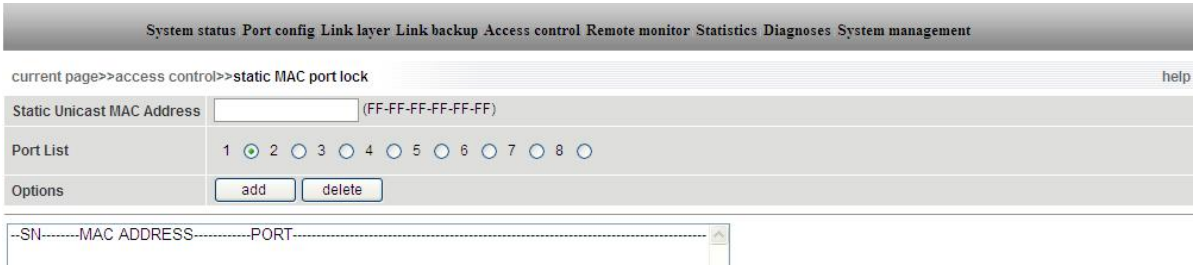


Figure 4.6.7

MAC port locking configuration page similar to the multicast table, methods of operation are the same, only difference is former is one to one relationship , that means one MAC address just corresponds to one port , but later one is one to many relationship.

Static Unicast MAC Address: Fill in this box to add a static unicast MAC address in the format Unicast address of the beginning of the 16 hex 00;

Port List: Select this unicast MAC address binding packets forwarding ports to which port to forward, it will be elected to, where only allowed to select a port.

Options: This column table for unicast operation, button add And delete Used to add / modify and delete static MAC address. Existing static address entries will be displayed in the table below the box, every time a user opens the Web page, or add and delete operations executive will update the table frame;

1 add And delete Operation will take effect immediately, rather than the other pages to be "saved" a similar operation;
2, this feature is a security mechanism, so be careful to confirm the setting, or use it with caution;
3, do not use multicast addresses as input addresses;
4, please do not enter the reserved MAC address, such as the machine's MAC address.

4.7 Monitoring Alarm

Monitor alarm settings: SNMP Configuration, Email log.

4.7.1 SNMP

Simple Network Management Protocol (SNMP) defined by the Internet Engineering Task Force, is part of Internet protocols. Concerned about the conditions of a particular network devices , using SNMP network management system to monitor network devices. SNMP protocol is consist of a series of standard network management protocol, application layer protocol, database, data objects. SNMP protocol through the management system windows, display management figure , such as the system description allocation. These allocation description can be supported by an SNMP management application to query or set. SNMP protocol is based on TCP / IP protocol, SNMP is commonly used UDP port 161 (SNMP) and 162 (SNMP-Trap), SNMP protocol agent (SNMP Agent) exist in the network equipment, the use of standard MIBs (information specific to the device) as equipment interface, through a proxy, the network equipment can be monitored or controlled. When a Trap event occurs, SNMP Trap message is transmitted, this time, one of the available Trap receiver can receive this Tap message. SNMP Settings page as follows:

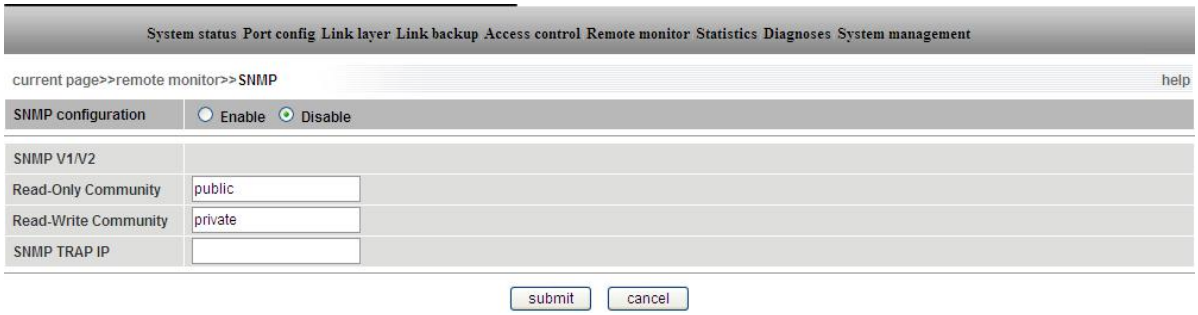


Figure 4.7.1

it support SNMP V1/V2C. SNMP V1 and V2C all used public string matching certificate, which means that the string used public or private, SNMP server allows read-only or read-write access to all objects. SNMPV1, SNMPV2C by community name authentication. SNMP community (Community) named by a string, called the community name (Community Name). SNMP community name used to define the SNMP manager and SNMP Agent relationship. Groups were played the role similar to the password, you can restrict access to SNMP manager on the Ethernet switch SNMP Agent.

Read-Only Community : Enable or disable SNMP, the default is disabled.

Read-Write Community : Use a string to name the SNMP community name, the group permissions only Get operation, the default is public.

SNMP TRAP IP : Use a string to name the SNMP community name, the group has operations and Set Get permission to operate, the default is private.

Network Management Photoelectric support SNMP V1/V2C. Use SNMP V1 and V2C certified public string matching, which means that the string used public or private, SNMP server allows read-only or read-write access to all objects. SNMPV1, SNMPV2C by community name authentication. SNMP community (Community) named by a string, called the community name (Community Name).SNMP community name used to define the SNMP manager and SNMP Agent relationship. Groups were played the role similar to the password, you can restrict access to SNMP manager on the Ethernet switch SNMP Agent.

ATTENTION:

1, the switch SNMP does not support the SNMP Trap function of SNMP, SNMP Trap using UDP port 162 , the switch use private 7051 port send up crew Trap packets;

2, the switch SNMP Agent RMON support a part of standard MIB-2 and RMON and can only use the get operation; also support the company private MIBs, this part o the MIBs can use get and set operation, after simple allocation of switch, However, a private MIBS just have part function of Web network management , we suggest users not to use;
3, in the SNMP browser, please note that read and write permissions issue, if you can not read and write properly, please check with the group name

SNMP Performance parameters
It supply SNMP agent to manage Ethernet Switch, this series Ethernet switch support below RFCS:
RFC 1157 – SNMP protocol
RFC 1213 – MIB-2
RFC 1573 – IF-MIB
RFC 1643 – Interface MIB
RFC 2819 – RMON

4.7.2 Email Log

The function of the form by e-mail to the user specified mailbox periodically to send the system log, as shown in Figure (4.7.2) as follows:

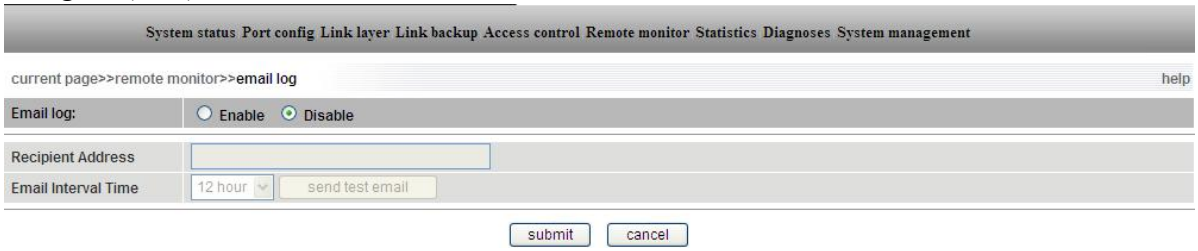


Figure 4.7.2

Email log: : Enable or disable this feature, the default is disabled.

Recipient Address : Enter the message you want to receive e-mail address for this log, can be Sohu, Sina and any other mailbox can send and receive mail properly, you need to set the mailbox to avoid log messages mistaken for spam to be deleted; log the sender address is always To: maiweso@sohu.com , this address will not change, the user could then set up mail filtering.

Email Interval Time : Refers to the time between sending the log messages, default is 12 hours, range 1 to 24 hours, in hours, this time for the software to calculate time, not very precise.

When the parameters are set, the user can click send test email Send a test message button, wait a minute, if you receive the following message, then the test is successful, the mail system is working properly:

Receiver Address: Enter the e-mail to receive this log, can be Sohu, Sina and any other mailbox can send and receive mail properly, you need to set the mailbox to avoid log messages mistaken for spam to be deleted; log the sender address is always : maiweso@sohu.com, this address will not change, the user could then set up mail filtering.
E-mail interval time: Mean time between sending the log messages, default is 12 hours, range 1 to 24 hours, in hours, this time for the software to calculate time, not very accurately.

When the parameters are set, the user can click “send system testing mail “on the button to send a test message, wait a minute, if you receive the following message, then the test is successful, the mail system is working properly:

Dear user:

Thank you for using Email logging System! If you read this mail it means this system will work well for you! This system can provide periodic email logging supports, and email to you all the system logs include network storm and other events message.

Of course, you can also customize this system. Please contact us. We are looking forward to hearing from you.

please don't reply to this mail directly.

Sincerely

Figure 4.7.3

ATTENTION:

1 Users can not receive messages if required to check the mail settings so that the log message is mistaken for junk mail and deleted;

2, just click Button send test email , set the value that is stored send test email submit can be understood as Equal Plus send a test message.

4.8 Port Statistics

Port Statistics feature set: receive frame statistics, sending the frame statistics, the total traffic statistics, MAC address table.

4.8.1 Receive Frame Statistics

Each port of the switch automatically monitor all network packets statistics, and display the Web page statistics. These statistics are from the power switch since the cumulative network data packets, soft reset or power off when the switch restarts, these data will have been set to zero.

System status Port config Link layer Link backup Access control Remote monitor Statistics Diagnoses System management

current page>>port statistics>>receive frame statistics help

Port	Unicast	Multicast	Broadcast	Discarded	Pause	Ultrashort	Ultralong	Wrong Ultrashort	Wrong Ultralong	Wrong Normal
1	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0
4	1191827	549	1047	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0

Figure 4.8.1

unicast packet: Port receive address as unicast address package number .

Multicast packet: Port received address as multicast address package number.

Broadcast Packet: Port receive address as broadcast address package number

Dropped packet: Port receiving is normal , but dropped packages for security reason.

Pause frame: Port received protocol 0x8808 Ethernet control frame, in full duplex mode, the packet is used to control the frequency of the port to send data.

ultrashort frames: Port received, including FCS, including the 64-byte packet length is less than

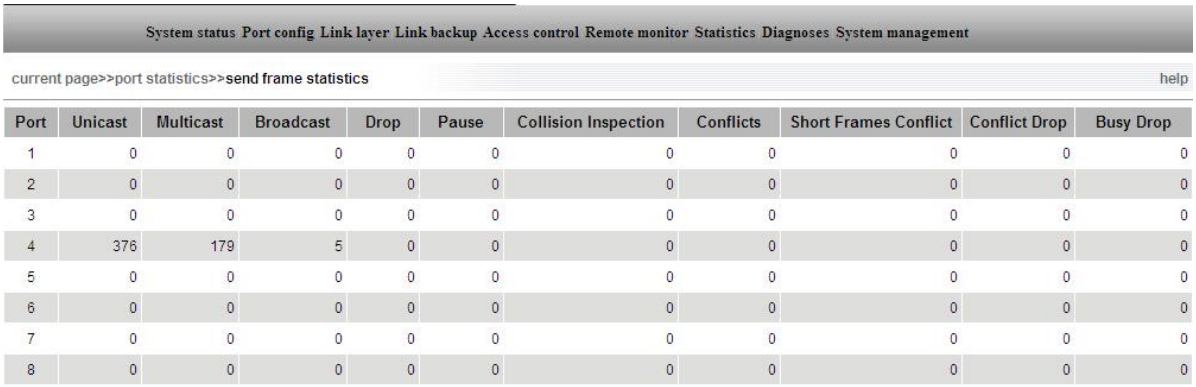
the number.

ultralong frames: Port received, including FCS, including more than 1518 or 1522 (open VLAN) the number of bytes of packets.
wrong ultrashort frame : port, including FCS received less than 64 bytes, including the length of the FCS is incorrect or incomplete the number of characters in the package.

wrong ultralong frame : received port, including FCS, including the length of more than 1522 FCS is incorrect or incomplete the number of characters in the package.

wrong normal frame: received port, including FCS, including the length of 64 to 1518 or 1522 (on VLAN), and between the FCS is incorrect or incomplete characters, and invalid characters are detected number of packets.

4.8.2 Send Frame Statistics



Port	Unicast	Multicast	Broadcast	Drop	Pause	Collision Inspection	Conflicts	Short Frames Conflict	Conflict Drop	Busy Drop
1	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0
4	376	179	5	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0

Figure 4.8.2

Unicast packet : port sending address is unicast address package number.

Multicast packet : port sending address is multicast address package number

Broadcast Packet : port sending address is broadcast address data package number.

Dropped packet: Port sending is normal , but dropped packages for security reason.

Pause frame: Port send protocol 0x8808 Ethernet control frame, in full duplex mode, the packet is used to control the frequency of the port to send data.

Conflict Test: Port sending data conflicts encountered times.

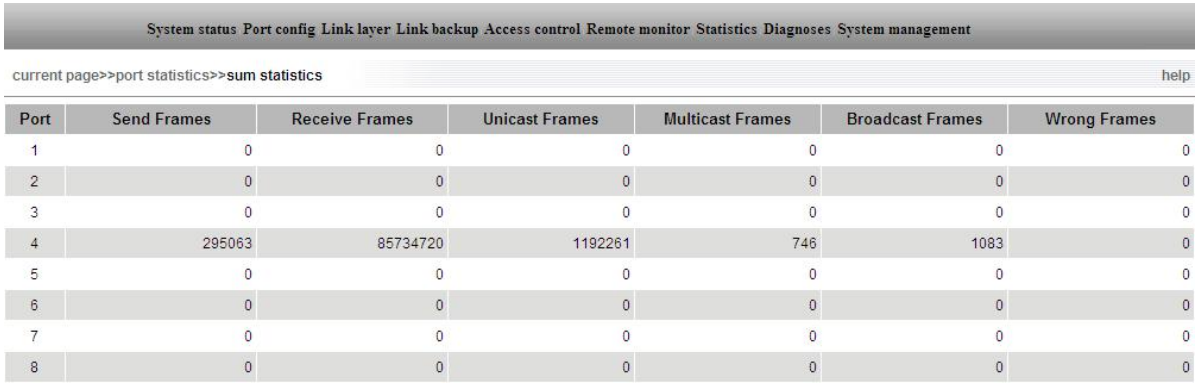
Times of conflict: sending data encountered conflicts times more than 1 times but still the data packets successfully transmitted out of the number.

Short Frame Conflict: less than 64 bytes in the transmission conflict detected while the number of packets.

Discard conflict: the conflict caused more than 16 times the number of packets dropped.

Resource busy discarded: the queue in the stack dropped due to lack of resources (after the opening of a large number of lower priority QoS data) the number of packets.

4.8.3 General traffic statistics



Port	Send Frames	Receive Frames	Unicast Frames	Multicast Frames	Broadcast Frames	Wrong Frames
1	0	0	0	0	0	0
2	0	0	0	0	0	0
3	0	0	0	0	0	0
4	295063	85734720	1192261	746	1083	0
5	0	0	0	0	0	0
6	0	0	0	0	0	0
7	0	0	0	0	0	0
8	0	0	0	0	0	0

Figure 4.8.3

sending bytes : port to send all packets of the total number of bytes.
receive total bytes : Port receives all packets the total number of bytes.
unicast packets total number : port address for sending and receiving unicast address the number of packets.
multicast packets total number : port address for sending and receiving data packets multicast address number.
broadcast packets total number : port to send and receive multicast address broadcast address is the number of packets.
error packets total number : port address to send and receive the error due to various reasons the number of packets.

4.8.4 MAC address table

MAC (Media Access Control) address is a network device hardware ID, the switch packets based on MAC address forwarding. MAC address is unique, which guarantees the right to forward packets. Each switch maintains a MAC address table. In this table, MAC address and switch port-one correspondence. When the switch receives the data frame, according to MAC address table to determine the filtering of the data frame is forwarded to the appropriate switch port. Is the switch MAC address table for fast forwarding the basis and premise.

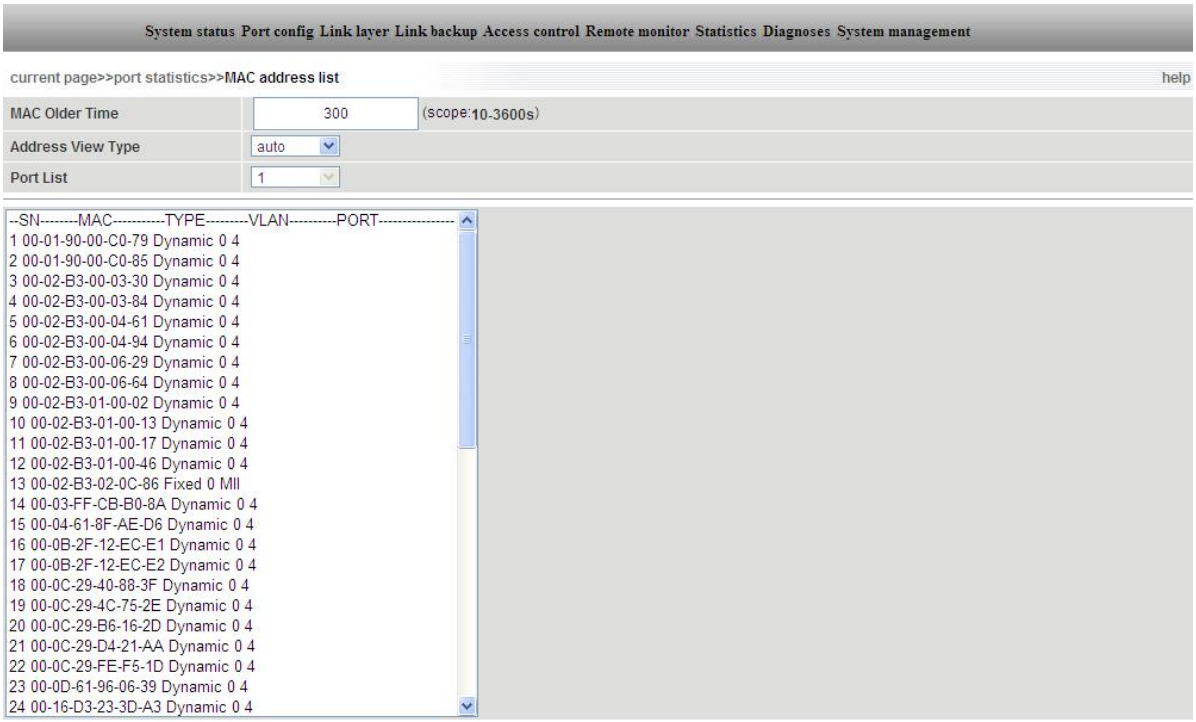


Figure 4.8.4

Address View Type: Address Display Type: Specifies the type of MAC address table sorting, you can choose "automatic" and "port " two kinds of sort types, select "Automatic" will list all ports MAC addresses, select the "port " will only correspond to the appropriate port MAC address listed.

Port List:: choose the MAC address of the corresponding port need display . this option just can use when “address display type “ option as ”port” , choose “automatic “ will show all port’s MAC address.

Address View Type :MAC address of the switch are divided into three types:

1, Dynamic MAC address

Such address in the MAC address table as "dynamic", the dynamic MAC address is the switch learn through the frame, when the aging time comes will be deleted. When the device connected switch ports changed, MAC address table corresponded port relations will change accordingly. Dynamic MAC address will disappear after power-on reset, need to learn again.

2, the static authentication (curing) MAC address

Such address in the MAC address table as "cure", the static authentication MAC address generated through configuration IEEE 802.1X authentication, will not be aged out. No matter the device connected switch port have what change, MAC address and port relationship will not change, the relationship entirely controlled by the IEEE 802.1X authentication server. Static MAC address will disappear after power-on reset.

3, permanent static MAC address

Such address in the MAC address list as "static", the permanent MAC address is configured to generate, and will not be aged out. No matter how the device connected switch port , the MAC address and port relationship will not changed.

MAC address of the permanent organs of power in the exchange will not disappear after reboot.

ATTENTION:

1 The device address according switch MAC address calculate index, so all of the display VLAN MAC values are 0;
2 permanent static MAC address in front of static table configured through above static MAC address , when ports change need to modify the corresponding table;
3 multicast address table will show in IGMP Snooping multicast table ,there address table are al unicast;
4, MAC address of the default aging time is 300 seconds (5 minutes), and network managemen through the WEB to set the time on talent

4.9 Network Diagnostics

Network Diagnostics feature set: port mirroring, network ping diagnosis.

4.9.1 Port Mirroring

Managed series Ethernet switch port mirroring function provides multiple image rule, the user can capture the exist, entrance all data. Through that series switches Web page, mirroring can be related to action.

Port mirroring is copying the monitored ports to the specified monitoring port, data analysis and monitoring. Ethernet switches support multi-to-one mirror. User can specify the direction of the Monitored packets, such as only monitoring messages sent by the specified port. This equipment uses the port mirroring group mode to configure port mirroring. The device use port mirroring group to configuration port mirror function. Each group contain a monitoring ports, and a group of monitored ports., that function configuration page as below:

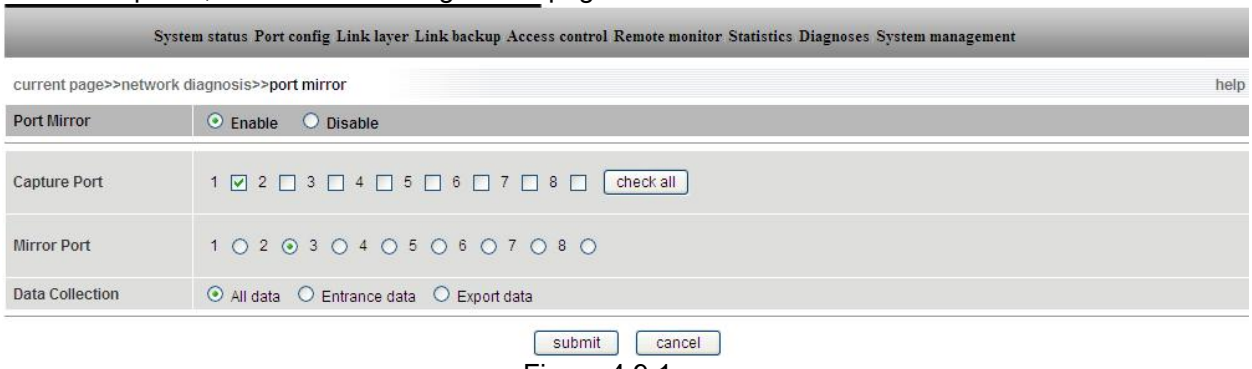


Figure 4.9.1

Port Mirror: Enables or disables port mirroring feature, the default is disabled.

Capture Port: Refers to the mirror port, or port the data is collected, the concept confusing, from the mirror means to understand the function of sending and receiving data will be copied to the port, you can set a number.

Mirror Port: Refers to the port to collect data from the mirror means understanding the functional copy of the data collected by the port, can only choose one, that is, while there is only a mirror port.

Data Collection: Refers to the direction of data collection options, import or export data, it can be

all the data in and out of the concept is defined for the capture port instead of the angle from the mirror port to describe.

ATTENTION:

1 This function must be turned off during normal use, or the senior management of al port-based features are not available. Such as RSTP, IGMP Snooping;
2 mirroring function is deal with FCS normal package , can not handle wrong data frame;
3 Data collection options, in or out data, it can be all the data in and out of the concept is defined for the capture port instead of the angle from the mirror port to describe.

4.9.2 Network Diagnostics

It provide diagnostic function, that is network fault analysis , network testing , or problem-solving, configuration page as follows.

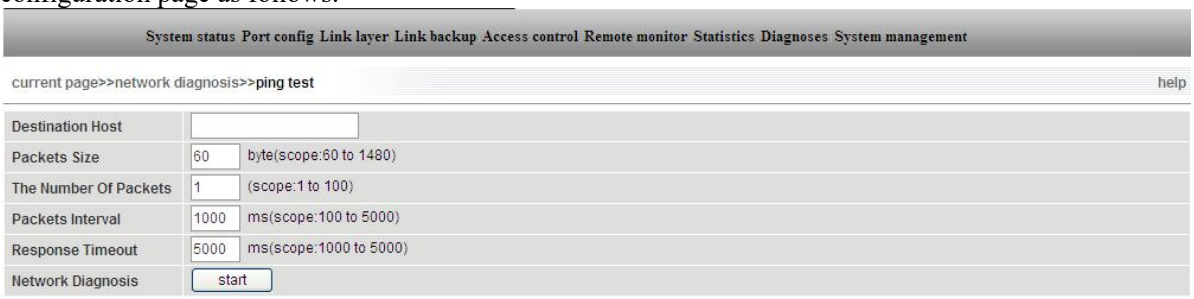


Figure 4.9.2

Ping functions using simple ping command, give the user a simple and powerful diagnostic tool for network problems. The most unique feature of the Web page is by entering a ping command through the Web page, ping send from the switch itself and the resulting output to the Web page. In this way, users can easily control the switch to send out ping command and output.
Ping function of each set are as follows:

Setting Project	Description State	Default
Destination host	Ping the IP address	Blank
Packet size	Ping packet length	60
The number of packets	Number of packets sent Ping	1
Packet interval	Ping packets sent at intervals	1000
Response timeout	Ping overflow time	5000

ATTENTION:

1 Network using the ping diagnostic function, you should ensure that the destination host loca connection windows firewall settings in the first ICMP "Allow incoming echo request" is checked, otherwis the destination host can not be ping-pass;
2 "Destination host" the domain name does not support unlimited expansion, only supports the following three domain names, such as "mail.sina.com";
3 The All "Request timeout" prompt, then the other network card is not working properly or faulty network line;
4, Ping domain If there is "unknown host name" message, then the DNS configuration error;
5, Ping domain If there is "Request timeout" prompt, it shows the gateway settings are wrong.

1 Before use ping network diagnostic , make sure the destination host windows firewall loca connection ICMP setting first option “allow incoming echo request” is checked, otherwise the destination host can not be ping—pass;
2 “destination host” the domain name does not support unlimited expansion, only supports the follow three domain names, such as “mail.sina.com”;

3 appears all the “request timeout “prompt, then the other network card is not working properly or faulty network line;
4 Ping domain if there is “unknown host name “ prompt message, then the DNS configuration error;
5 Ping domain if there is “request timeout” message, it shows the gateway setting are wrong ;

4.10 System Management

System management settings: time allocation, set the address, system information, log information, document management.

4.10.1 Time Configuration

Through time configuration to set Ethernet switch system time . This switch does not have backup battery to save the system time value, when the power outage, the system time will lost, after power-on reset, the switch system time is linux time , January 1, 1970, so when each power Restart the switch must simultaneously look after the switch time. Time configuration page as follows:

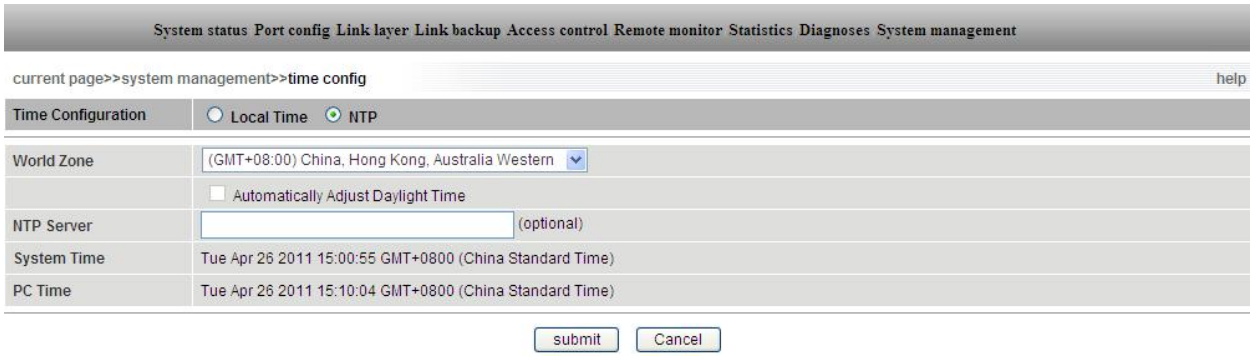


Figure 4.10.1

Time Configuration : This switch provides two different time configuration options: Local Time And NTP .

Time Configuration: This switch provides two configuration options at different times: local time and use NTP.

Local Time (Local time) is the time set by user, usually is the PC time visit this page, when the user selects the item and click "Settings", will appear ”update time to Ethernet switch” in the bottom button, and click will access the PC after time to update to the switch.

Use NTP : NTP Is the switch automatically synchronization Internet time server NTP (The Network Time Protocol) is a network time synchronization protocol, using the UDP protocol and port 123, NTP protocol can resist the instability of the network response time, to improve the accuracy of calibration time.

NTP Server: could supply NTP time server host name or IP address, can be blank.

System time : The device itself is the current system time, after the power is "January 1, 1970 0:00:10 Thursday", you can manually update the local time to switch or automatically using NTP updates.

PC Time : Visit the Web server PC 's system time, when ”local time” selected, will appear ”update time to Ethernet “ button, click to the switch will update this time.

1. NTP ,NTP server could be empty, Ethernet switch be able to access the internet , using public internet NTP server;
2. Update time need user choose Local Time , and click “setting” then pop up ,when user swift to “use NTP”, must click ”setting”, then will disappear.
3. only the “administrator” have right to manually configure the device ;
4. Time zone and daylight saving time must be configured, either using the "local time" o "NTP time";
5 NTP server or the time the visitor's PC configuration may cause the display is not normal you can change the "Show time" to adjust the display format.

4.10.2 Setting Address

This function will assign an IP address to the series of switches. IP addresses are usually allocated in two ways: automatically assigned (DHCP) or assign a IP address. The switch factory default IP address using a fixed, IP address 192.168.16.253. Configuration page as shown in Figure (4.10.2) below:

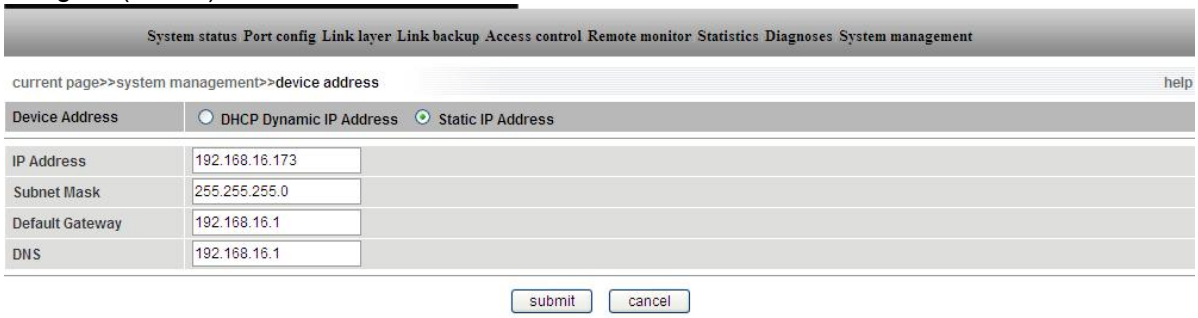


Figure 4.10.2

DHCP Dynamic IP Address : Use the DHCP protocol, from a DHCP server dynamically assign IP addresses, you need a DHCP server in the network, suggest user not use, because the Web server needs to access the switch's IP address clear that, while the dynamic allocation of IP addresses can not be determined before, and each restart may assign a new IP address.

Static IP Address : Manually set a fixed static IP address, and suggest users use this option to manually set a fixed IP address, easy to use Web network management, set the IP address can not have conflict.

IP Address : IP address is assigned to a device connected to the Internet, a 32-bit length of the address. IP address consists of two fields: the network number field (net-id) and the host number field (host-id). IP addresses by the Defense Data Network Network Information Center (NIC) for distribution. In order to facilitate the management of IP addresses, IP addresses are divided into five categories: where A, B, C class address unicast (unicast) address; D class address for multicast (multicast) address; E class addresses are reserved addresses, for future special purpose. Currently a large number of IP addresses in use are A, B, C three types of addresses.

Subnet Mask :Mask is an IP address corresponding to the 32-bit numbers, some of these numbers is 1, others 0. IP address mask can be divided into two parts: subnet address and host address. IP address and mask bits for a subnet address part corresponding to the other bits are the host address. A class A address corresponding to the mask as 255.0.0.0; B type the address mask is 255.255.0.0; C class address mask of 255.255.255.0.

Default Gateway : Host in the default gateway is often called the default route. Default route (Default route), is the IP packet destination address found in the presence of other routes, the route chosen by the router. Destined for the router's routing table for all packets will use the default route. This route will generally go to another router connected, and this router also process the data packets, if know how

to route the packet, the packet will be forwarded to the known route; Otherwise, the packet will be forwarded to the default route to reach the other router.
DNS Address: DNS stands for Domain Name Server, the role is to facilitate our memory of the domain name resolves to the IP address of Internet can be identified. If we need access to a host device name, you need to take advantage of this server resolve IP addresses.
Whenever a user changes address settings will be submitted to the click of a button switches, and switch into a wait for a page:

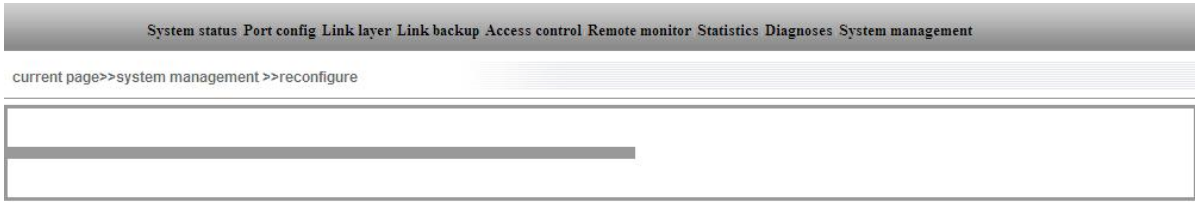


Figure 4.10.3

When the screen after the progress bar, the switch is using the new IP address and restart the Web server.

1 We can set the IP address range should be 192.168.xx, 172. [16-31]. Xx or 10.xxx;
2, NTP will use the DNS and Email services, if the application of these two services, be sure to fill in the correct DNS address.

4.10.3 System Information

Through this page users can find information about the switch of the system, set the switch's name:

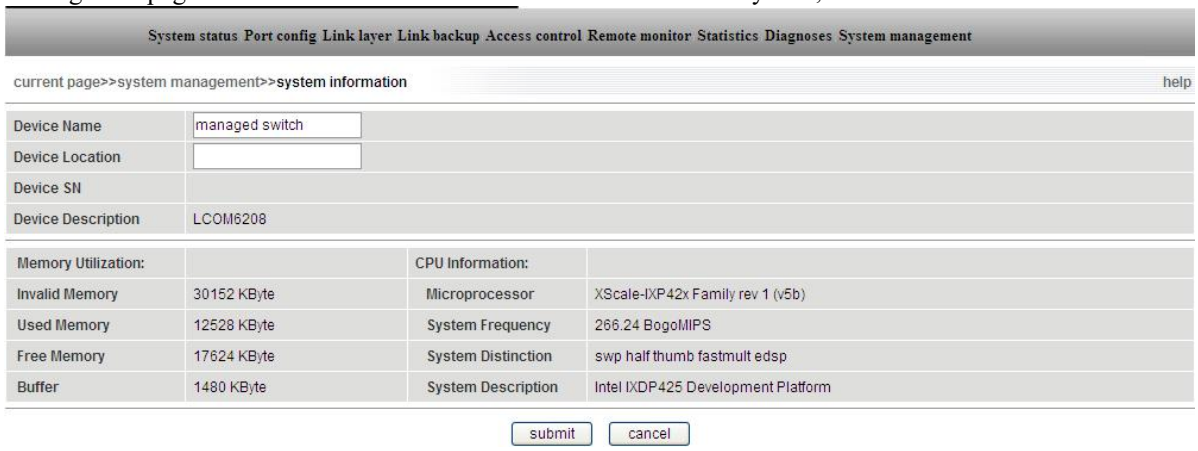


Figure 4.10.4

Equipment Name: To mark each Ethernet switch in the network , send each switch a different name , to distinguish , and to support Chinese input, switch name maximum is 16bytes.
Equipment Serial Number: describe the switch serial number, factory-set by the manufacturer, the user can not modify.
Equipment Description: The switch model,, decided by hardware, users can not modify, this message use could through a SNMP customer software or CD-ROM search tools provided stool.
Memory usage : This section describes the switch system memory RAM usage.
CPU Information : This section describes the main CPU switching system basic information.

4.10.4 log information

Logging equipment in order for users to set the reference may encounter problems. When this

feature is enabled, the switch will record the relevant events took place, and save information to log file, logging all of the records stored in the SDRAM can store up to 2,000 records, when more than 2000 records, old records will automatically be deleted, the new record is added. The following events will be saved to a log file:
System restart
Port Link Down / UP
Login Information
Broadcast storm occurs
Actions and operational records system
NTP time synchronization information
Some other system information
This page as shown below:

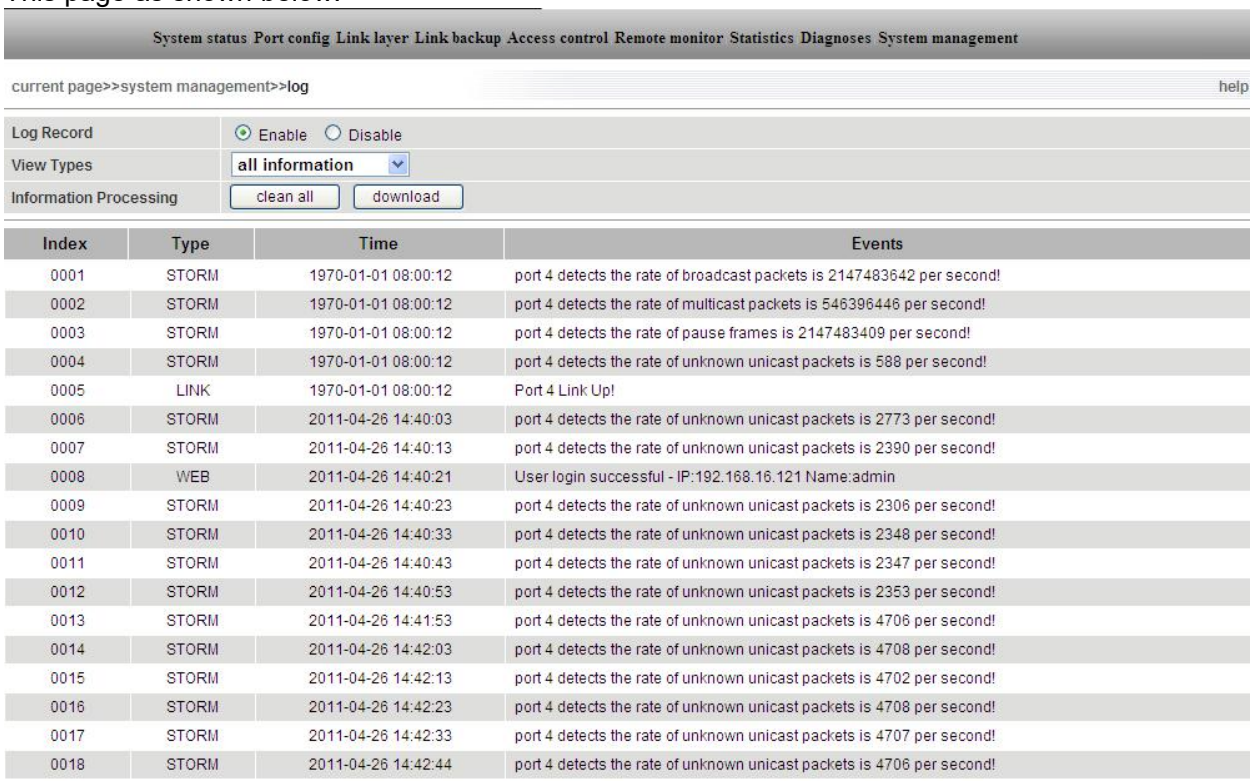


Figure 4.10.5

Log Record : Enable or disable logging record function, default as enable , logging I disable and does not delete the log contents, but not add a new log information.

View Types : Certain types of information displayed, you can "all information", "Operational Information", "Connection Information" to switch

clean all : Click this button to clear out all log information

download : Click this button to log information from the Web server to download and save to visit the PC, the file name is syslog.cfg, please download a browser, Web server, the switch does not support multi-threaded download Thunder and other tools.

4.10.5 Document Management

This face of some unconventional switch system operation, the user is careful to use, improper operation may damage the switch. Only the "administrator" to perform these operations.
Management page as shown below:

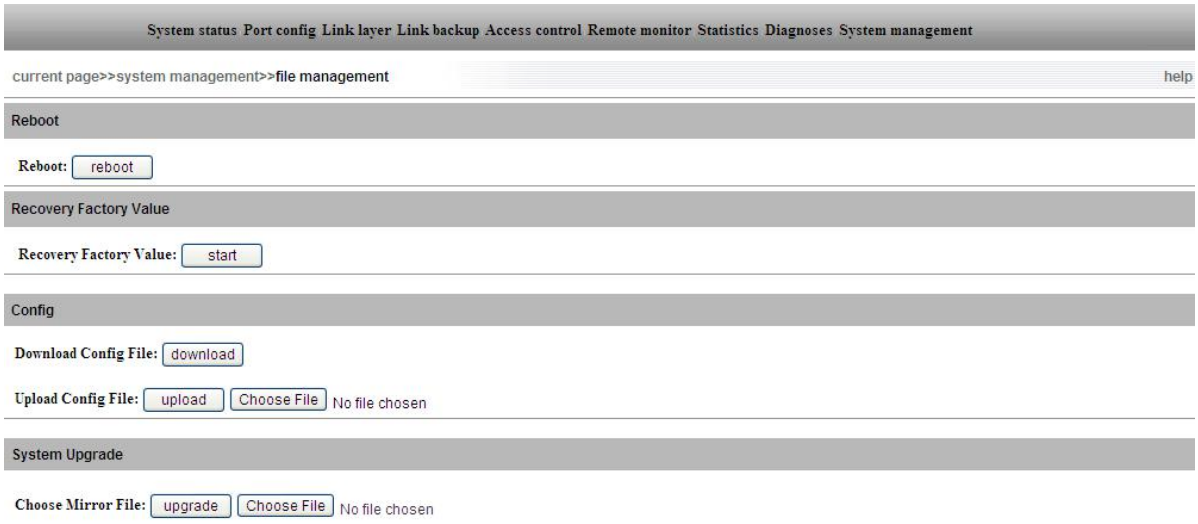


Figure 4.10.6

Reboot: This operation is used to restart a switch,before the switch successfully complete restart, this switch does not work, can not forward any data packets, which is different from the power-on reset to restart the hardware reset, but software reset switch , like windows operation system "hot start." The greatest advantage of this feature is to provide a remote reboot switch, users can remotely access to the switch as long as can be remotely reboot. Click the reboot, waiting for pages to go to a reboot:

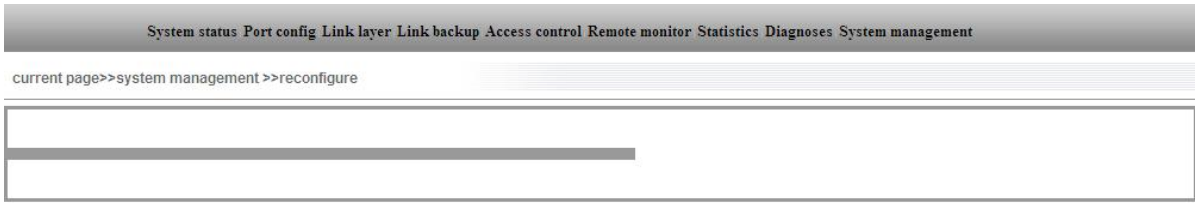


Figure 4.10.7

When the screen after the progress bar, the switch that is software reset is complete.

Recovery Factory Value: :Recovery Factory value : This operation is used to switch restored to factory settings, and automatically restart the switch, when the success of the switch before the restart, the switch does not work, can not forward any packets. Once this feature is set when the user error parameter causes the switch is not working properly, you can restore the factory default configuration values. Factory default IP address is: 192.168.16.253, restore factory settings when successful, users need to use this IP address to access Web server. Click the button start, go to a wait for a page

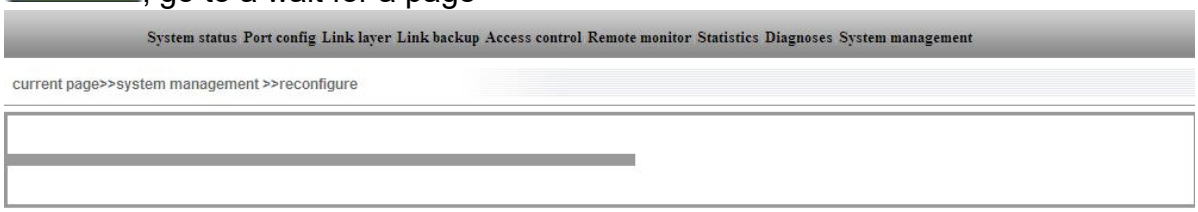


Figure 4.10.8

When the progress bar finish, the switch is completed to restore the factory settings and reboot.

Configuration file: The operation of this switch allows the user to save all the current configuration to a file, you can use this configuration file to backup and restore switches' all the configuration . This function let users easily use a configuration file quickly configure multiple

switches. Click the download button, you can access this configuration file downloaded to PC, the file name is: Switch cfg. cfg, the switches do not support multi-threaded downloading tool Thunder, etc., please use the browser to download. To upload a configuration file, you must first click ”browse” to select a file, please note that you must not select a non-switch configuration file, upload the wrong file may result in damage to the switch, click upload button to go to a wait for a page:

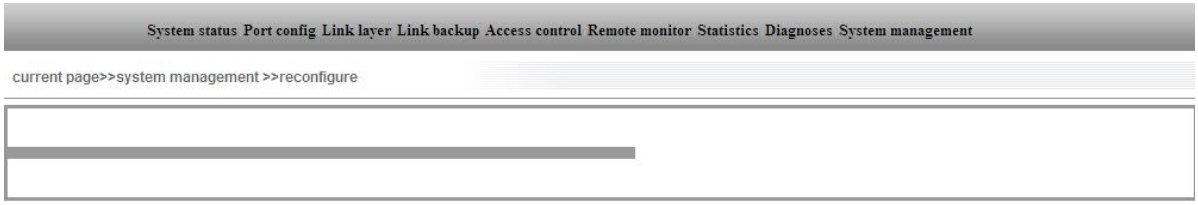


Figure 4.10.9

When the progress bar is completed, the switch is configured with the new settings and restart the switch. This operation can not be power, or it may damage the switch

System Upgrade: This operation is used to upgrade switch kernel, users can e-mail or our web site get the Ethernet switch upgrades program, please note the device model and version to match, use the upgrade program does not match the switch may cause permanent damage. Users get the upgrade process and click the ”browse” button to select the upgrade process, and then click the button “begin upgrade ”is transferred to the waiting page:

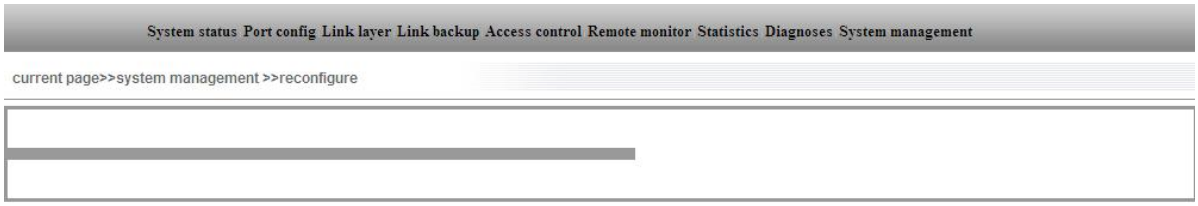


Figure 4.10.10

When the screen after the progress bar, the switch or upgrade is completed, the switch will automatically resume after the upgrade the factory settings, and reboot. Please note that the upgrade process can not power off, or it may damage the switch.

1, restore factory default settings will result in all the states in the newly set up state o the factory, the set of IP is static IP address "192.168.16.253", users need to use the IP address to access the Web server;
2, upload the configuration file operation, must not select a non-switch configuration file, upload the wrong file may result in damage to the switch;
3, upload a configuration file that can not cut operation, the switch may be damaged;
4, upload the configuration file, the new static IP configuration, if not in the same network segment will cause the page can not refresh, because it could not re-log Web server;
5, upload the configuration file, the new configuration using dynamic IP settings, bu there is no DHCP server segment, will result in the relevant part of the IP will not be updated;
6, upgrade, note the matching device type and version, use the upgrade program does not match the switch may cause permanent damage;
7, the upgrade process does not allow power outages, power outages may cause permanent damage to the switch, upgrade the power to immediately send the products of the Company to seek possible solutions.

ATTENTION:

If the setting disorder, may consider the switch to restore the factory settings, you can re-set. Remember to restore the factory settings of the IP is: 192.168.16.253, the best to modify the switch's IP, so as to avoid conflict of use.

Chapter 5 maintenance and service

Since the date of product shipment, it provide five years of product warranty. Optoelectronic Technology Co., Ltd. based in Wuhan Marvell product specification, in the warranty period, if there is any failure or functional product fails, it will repair or replace free of charge for users of the product. However, these commitments do not cover improper use, accidents, natural disasters, improper operation or improper installation caused the damage.
To ensure that consumers benefit of products, through the following ways to get help and problem solving:

- Internet services.
- Call the technical support office.
- Product repair or replacement.

5.1 INTERNET Service

Through the website of Wuhan Technical Support section, you can get more useful information and tips.

5.2 Technical Support Phone Services

By using the product user manual, you can connect with our technical support office, we have professional technical engineers to answer your questions, help you the first time resolve your product or issue.

5.3 The product repair or replacement

Product repair, replacement or refund, should first connect with our technical staff to confirm, and then sales staff to contact and get the problem handled. Above shall technical staff and sales staff through consultations, to complete the product maintenance, replacement or return.