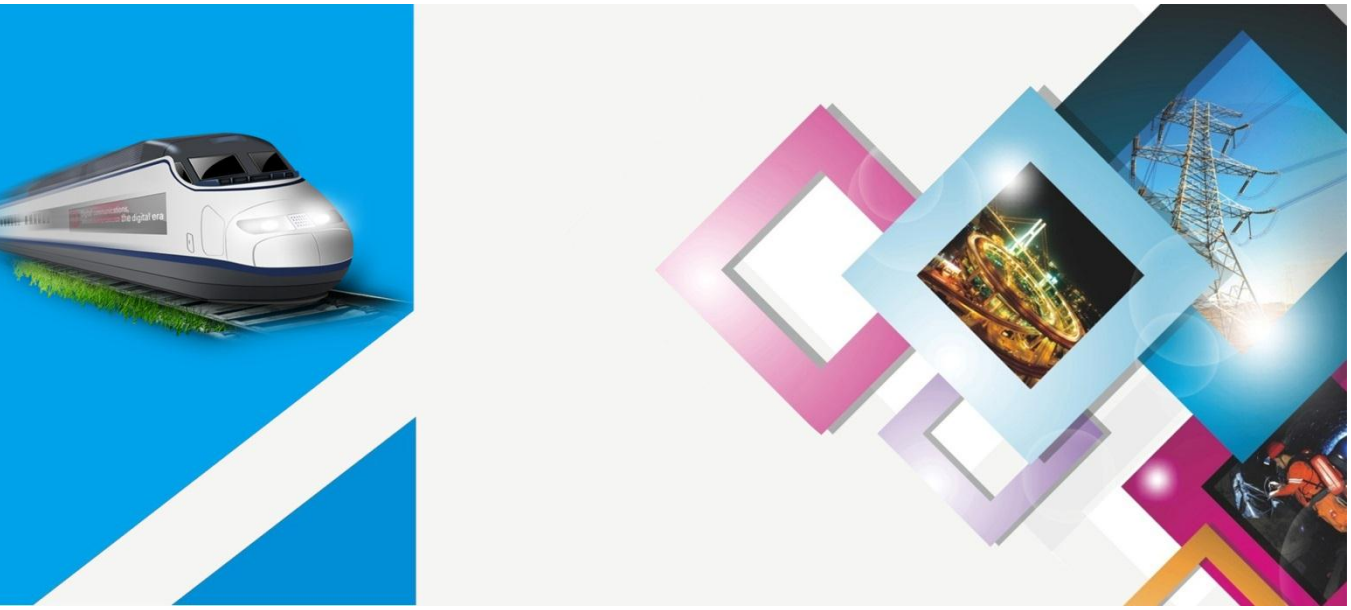
3onedata
Make network communication more reliable



MES600 Series

Managed Industrial Ethernet Switch

User Manual

Version: 02

Issue Date: 2018-08-16

Trademark statement

3onedata, 3onedata® and 3One data® are the registered trademark owned by 3onedata Co., Ltd. And other trademarks mentioned in this manual belong to their corresponding companies.

Notes

Purchased product, service or features should be constrained by 3ondedata commercial contracts and clauses. The whole or part product, service or features described in this document may beyond purchasing or using range. 3onedata won't make any statement or warranty for this document content unless any other appointment exists.

Due to product version upgrading or other reason, this document content will be upgraded periodically. Unless other appointment exists, this document only for usage guide, all statement, information and suggestion in this document won't constitute any warranty.

3onedata
Make network communication more reliable

3onedata Co., Ltd.

Headquarter address:	3/B, Zone 1, Baiwangxin High Technology Industrial Park, Song Bai Road, Nanshan District, Shenzhen, 518108, China
Technology support:	tech-support@3onedata.com
Service hotline:	+86-400-880-4496
E-mail:	sales@3onedata.com
Fax:	+86-0755-26703485
Website:	http://www.3onedata.com

Preface

Managed Industrial Ethernet Switch User Manual has introduced this series of switches:

- Product feature
- Network management method
- Network management relative principle overview

Readers

This manual mainly suits for engineers as follows:

- Network administrator responsible for network configuration and maintenance
- On-site technical support and maintenance staff
- Hardware engineer

Text Format Convention

Format	Description
“”	Words with "" represent the interface words. e.g.: "The port number".
>	Multi-level path is separated by ">". Such as opening the local connection path description: Open "Control Panel> Network Connection> Local Area Connection".
Light Blue Font	Represent the words click to achieve hyperlink. Font color as: "Light blue".
About This Chapter	The "About This Chapter" section provides links to each section and corresponding principles / operating chapters in this chapter.

Icon Convention

Format	Description

Format	Description
 Notice	Reminder the announcements in the operation, improper operation may result in data loss or equipment damage.
 Warning	Pay attention to the notes on the mark, improper operation may cause personal injury.
 Note	Make a necessary supplementary instruction for operation description.
 Key	Configuration, operation, or tips for device usage.
 Tips	Pay attention to the operation or information to ensure success device configuration or normal working.

Revision Record

Version NO.	Revision Date	Revision Description
01	2018-04-11	Product release
02	2018-08-16	Delete Gigabit product function

Content

1 Log in the Web Interface

1.1 WEB Browsing System Requirements

While using managed industrial Ethernet switches, the system should meet the following conditions.

Hardware and Software	System Requirements
CPU	Above Pentium 586
Memory	Above 128MB
Resolution	Above 1024x768
Color	Above 256 color
Browser	Above Internet Explorer 6.0
Operating System	Windows XP Windows 7

1.2 Setting IP Address of PC

The switch default management as follows:

IP Setting	Default Value
IP Address	192.168.1.254
Subnet Mask	255.255.255.0

While configuring the switch via Web:

- Before remote configuration, please make sure the route between computer and

switch is reachable.

- Before local configuration, please make sure the computer IP address is on the same subnet as the one of switch.

Notes:
While first configuring the switch, if it is a local configuration mode, please make sure that the network segment of current PC is 1.

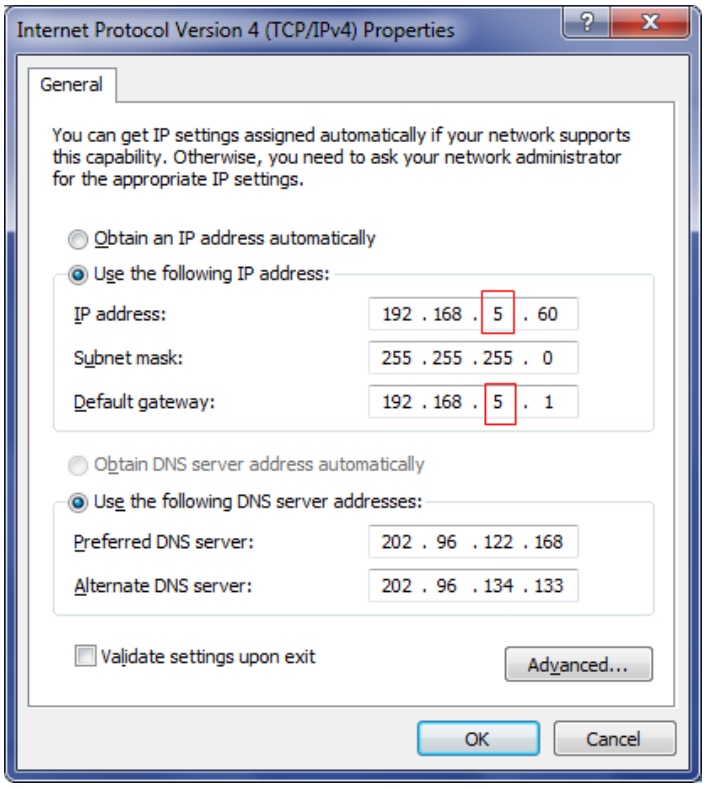
E.g.: Assume that the IP address of the current PC is 192.168.5.60, change the network segment "5" of the IP address to "1".

Operation Steps

Amendment steps as follows:

Step 1 Open "Control Panel > Network Connection> Local Area Connection> Properties> Internet Protocol Version 4 (TCP / IPv4)> Properties".

Step 2 Change the selected "5" in red frame of the picture below to "1".



Step 3 Click “OK”, IP address modifies successfully.

Step 4 End.

Notice
In windows system, if user adopts the advanced configuration function of IP address and accesses the switch device via setting IP dummy address, the following managed functions can't be achieved: IEEE 802.1x polling.

1.3 Log in the Web Configuration Interface

Operation Steps

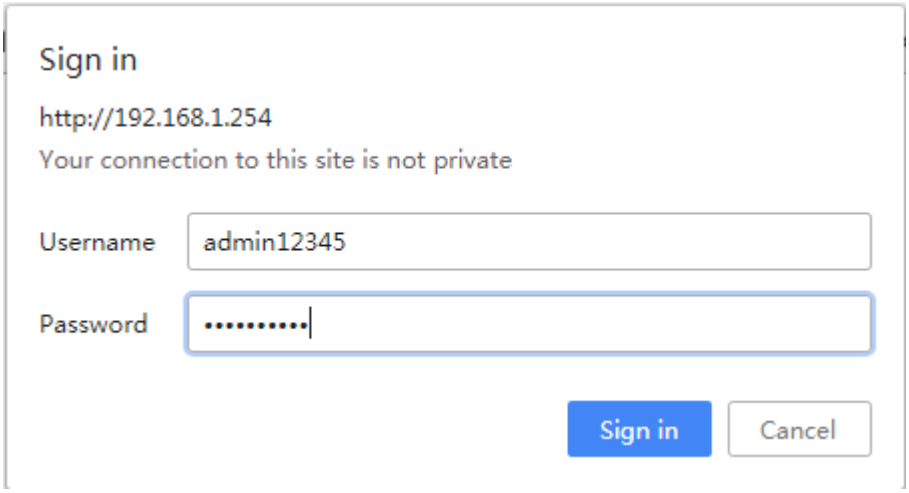
Login in the web configuration interface as follows:

Step 1 Run the computer browser.

Step 2 On the browser's address bar, type in the switch addresses "http://192.168.1.254 ".

Step 3 Click the “Enter” key.

Step 4 Pop-up a window as the figure below, enter the user name and password on the login window.



Notes:

- The default username and password are “admin12345”, please strictly distinguish capital and small letter while entering.
- Default username and password have the administrator privileges.
- WebServer will provide 3 times opportunities to enter username and password. If enter the error information for 3 times, the browser will display a "Access denied" to reject access message. Refresh the page and try again.

Step 5 Click "OK".

Step 6 End.

After login in successfully, user can configure relative parameters and information according to demands.

Notes:

After login in the device, modify the switch IP address for usage convenience.

2 System status

Enter the correct user name and password that the normal switch WEB interface display information about the state of the system, including: the main menu, equipment information, port information, the upper right corner of display is the current time, as shown in figure:

2.1 Device information

Equipment information mainly display basic information, Switch include: equipment type, equipment name, description of the equipment, equipment, hardware version number, firmware version, the Switch of MAC address, contact method.

2.2 Port information

Switch a total of 8 ports, ports can confirm whether the port with the equipment complies with the information bar. Equipment at work, via the port status of the port

information in the status view, for example in the figure below you can see port 4 is LINK and port connection status as FULL, speed is 100M and port type for the TX(RJ45).

- LINK: Indicates that the port is in a connected state;
- LOS: Indicates that the port is not connected;
- FULL: Indicates that the port State is full duplex;
- HALF: Indicates that the port State is half-duplex (if the ports are not connected, the port status is HALF);

Port Information

Port	Connection	Duplex	Speed	Type
1	LOS	HALF	10M	TX
2	LOS	HALF	10M	TX
3	LOS	HALF	10M	TX
4	LINK	FULL	100M	TX
5	LOS	FULL	100M	FX
6	LOS	FULL	100M	FX
7	LOS	FULL	100M	FX
8	LOS	FULL	100M	FX

3 Serial device server

Note

This section applies only to the device with serial port.

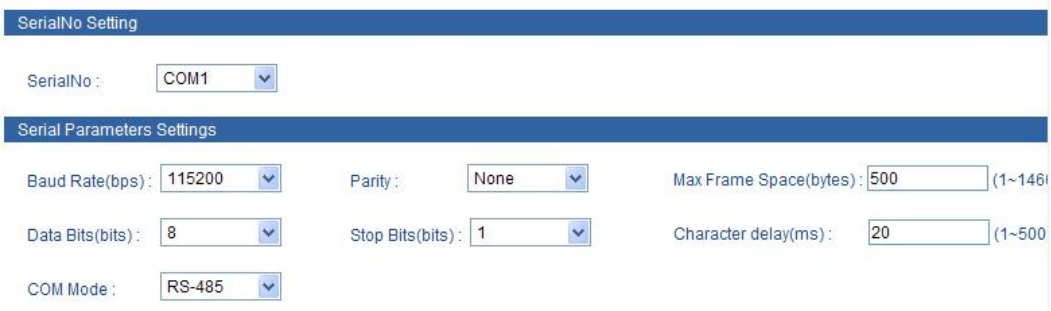
Server configuration includes the serial port configuration and mode of operation of the configuration parameters

3.1.1 Configure serial port parameter

Serial port configuration menu	Optional data	Description
Serial port working mode	RS-232 full duplex/RS-422 full duplex/RS-485 half duplex	Serial work mode
Baud rate（bps）	300-115200（10pcs band rate optional）	Baud rate choice
Parity	None,Even,Odd,Mark,Space	Checkout choice
Data bits（bits）	5,6,7,8	The parameter of serial
Stop bits (bits)	1,1.5,2	The last of the data package
Max frame space(bytes)	1-1460	The length of frame from serial data to Ethernet data.
Character delay（ms）	1-500	The time space from serial

		data to Ethernet data

Enter into switch WEB interface, knock [Serial Server/COM settings], Please choice necessary configuration in drop down list, the serial configuration interface is as follows:



Configuration option: [Baud rate], [Parity], [Data Bits], [Stop Bits], [Max Frame Space], [Character Delay] and [COM mode], the explaining is as follows:

[Baud rate]

It is a parameter to check the communication speed. It shows to transfer how many bits in 1 second.

For example, 300 baud rate means have 300 bits transferred in 1 second.

[Parity]

Parity bits: It is a simple method to checkout fault in serial communication,

have 4 types: Even, Odd, Mark, Space

[Data Bits]

It is a parameter to check the actual data bits in communication.

When PC send a Packet, actual data is not 8 bits, the standard is 5, 6, 7, 8.

[Stop Bits]

The last bit of the single Packet. Typical value is 1, 1.5 and 2 bit.

When data bits is 5, stop bit 1.5 and 1 option. When data bits is 6, 7, 8, stop bit 1 and 2 option.

[Max frame space]

The frame length that serial interface data convert into Ethernet data, within the range of setting time,
it forward when data is equal to or longer than the setting frames.
Available setting value ranged from1 to 1024.

[Character Delay]

The wait time when serial interface send data do not 1 data frames. If up to this time and do not have
data, then send automatic. Can configure 1-500.

[COM mode]

Web interface default work mode.

3.1.2 Configure working mode

Working mode configuration menu：

Configuration menu	Data option		Description
Sessions	1-4		
Working mode	Based mode	TCP Client TCP Server UDP TcpAuto	Choice serial port working mode, default is not open
	Advanced mode	Tcp Server	
		UDP	
Local port	1-65535		COM1 default is 30000，COM4 default is 30003, between them, add step by step
Target address	Default is192.168.0.254		
Target port	1-65535		COM1 default is 31000，COM4 default is 31003, between them, add step by step
Connect mode	Connect immediately/data		Default is connect

	trigger	immediately
AT	0-65535 s	Default is 0
Disconnect Timeout	0-65535 s	Default is 300
RealCom	Open/Close	Default is Close

[Sessions**]**

Each serial port of serial device servers can support 1-4 sessions. It means serial port of serial device server send the received data to Ethernet through socket. More than one of the sessions means serial port of serial device server sends the received data to Ethernet through more than one socket. sessions enable to use by checking the corresponding box.

Based mode

- TCP client

  As TCP Client side, serial device server will connect forwardly to TCP/IP network equipment, such as PC. It need to setup to tell serial device server to connect which network address and TCP port number when conditions is matched. After creating socket, serial device server will sent the data received from each serial port through socket On the contrary, the data received from socket will be sent to the corresponding serial port.

  TCP Client setting option: [Target address], [Target port], [Connect mode] And [AT]

  The explanation of these setting is as follows

  [Local port]

  The configuration is the same TCP server, default is 0~65535.

  [Target address]

  The IP address or domain name address that device will connect, both of them can correspond the host computer address on the Internet

  [Target port]

  The port that device will be connected, default is 1~65535.

  [Connect mode]

Connection mode has 2 types: Immediately and Data trigger

Immediately: When Switch have power supply, it will connect immediately, if connection cut off, it will connect immediately.

Data trigger: Once Switch receive the data, it will connect immediately.

[AT]

SWITCH send the AT package accord the setting time, if no response continue 3 times, will be cut off.

If set “0”, meaning this function closed, the range is 0-65535 second, default is 0 second.

[Disconnect Timeout]

Setting the vacancy time for connection cut off automatic; if there do not have data transfer, the connection will cut off. If set “0”, means do not care how much time vacancy, SWITCH do not cut off voluntary. The range is 1-65535s. Default is 300s

The figure below is the configuration interface of TCP Client Mode. Session 1 is setting to local address available for router.”192.168.2.168”，the “Destination Port” connected to serial port is host computer 192.168.2.168” 31000 port, Connection mode is Immediately, Disconnect Timeout time is 300 seconds, please pay attention to pure TCP Client, TCP Server, UDP or TCPAuto mode. Please close RealCom. Session 3 is setting to Internet address available for router ”www.test.com”（the choice this time is DNS）the “Destination Port” connected to serial port is host computer ”www.test.com” 31002 port， Connection mode is Immediately, Disconnect Timeou time is 300 seconds, click “Apply’, setting successful.

- TCP server

  TCP Server, Passive connect, one pivotal parameter is [Local port], have relationship with other setting, need combine setting

  [Local port]

  Switch provided TCP port can be connect by other TCP/IP node, the TCP port have the relationship with the Switch's relevant serial interface. The figure as follows is TCP Server setting interface, Session 1 set local port is 30000, external TCP port connect Switch through this port. Connection keep-alive time is 300 second。 Click "Apply", setting successful.

- UDP

  Under the UDP work mode. SWITCH is server and also client, the relevant setting is "Local port", "Target address" and "Target port". It can support point to point and multicast UDP, setting method is the same as TCP.

- TCP Auto

  In this Mode, serial device server can act as server or client. Before setting this Mode, please ensure related parameters are correct when you turn on the server mode, client mode is automatically disconnected.

- RealCom

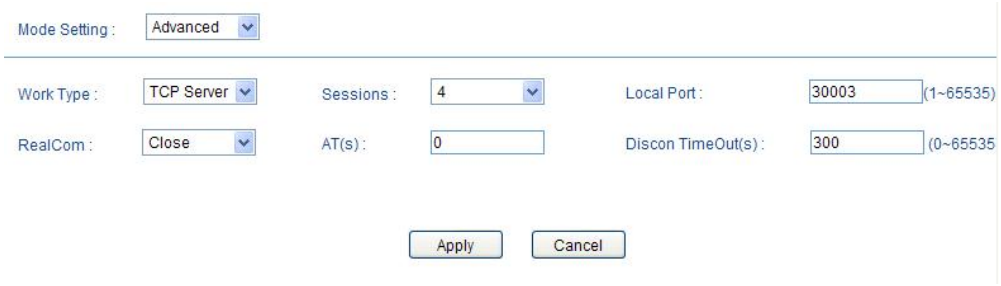
  RealCom support TCP Server and TcpAuto, can choice open and close function in RealCom.

  When device open the RealCOM function, can cooperate with VSP Management Software create virtual COM port to communication, now, device's work mode is server, the virtual COM port is client, how to create the Virtual COM port, please the VSP Management Software user manual.

Advanced mode

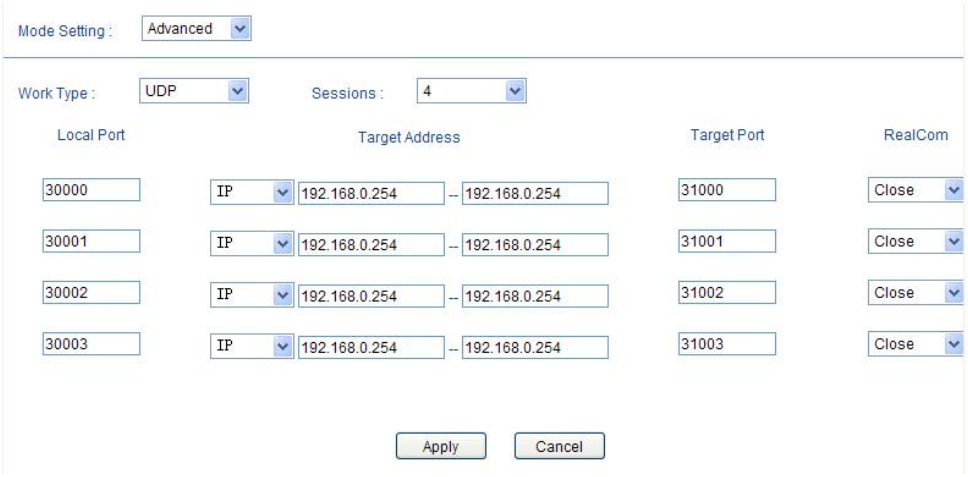
- TCP server

  Under this mode, series is server, SWITCH can choice 0-4 channel connection at the same time, configuration mode is the same based mode.



- UDP

  Under this mode, Target address is a address pool, all of the address in pool can connect with NP30XT series, can choice 0-4 channel connect at the same time.

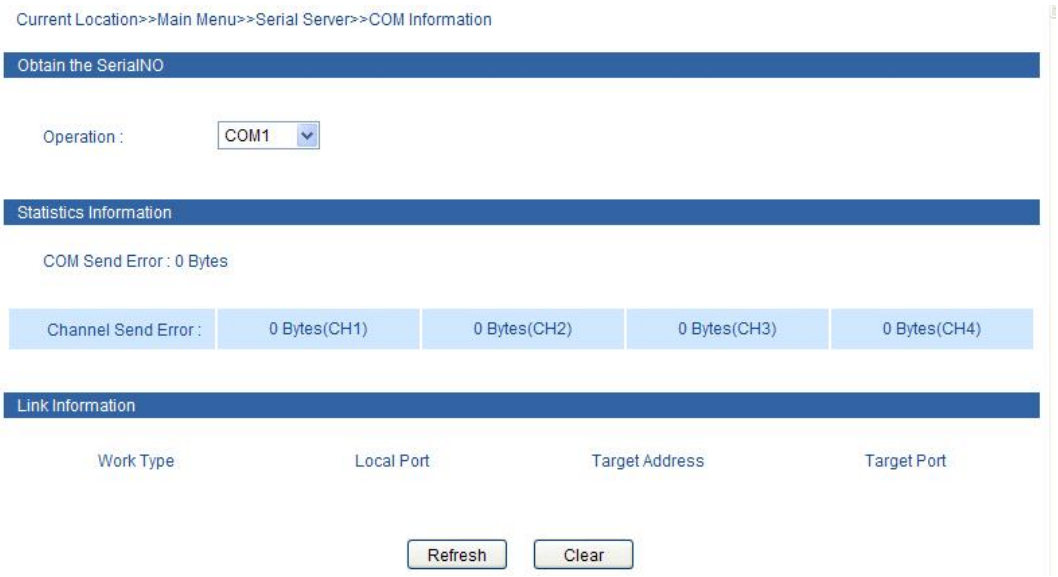


Notes:

- Address pool just support Type A and type B address
- Start address and end address must in the network segment.
- Start address value must less than or equal to end address.

3.1.3 Serial port information

It main function of serial port information: Display incorrect data statistics and connection information that send by serial port.



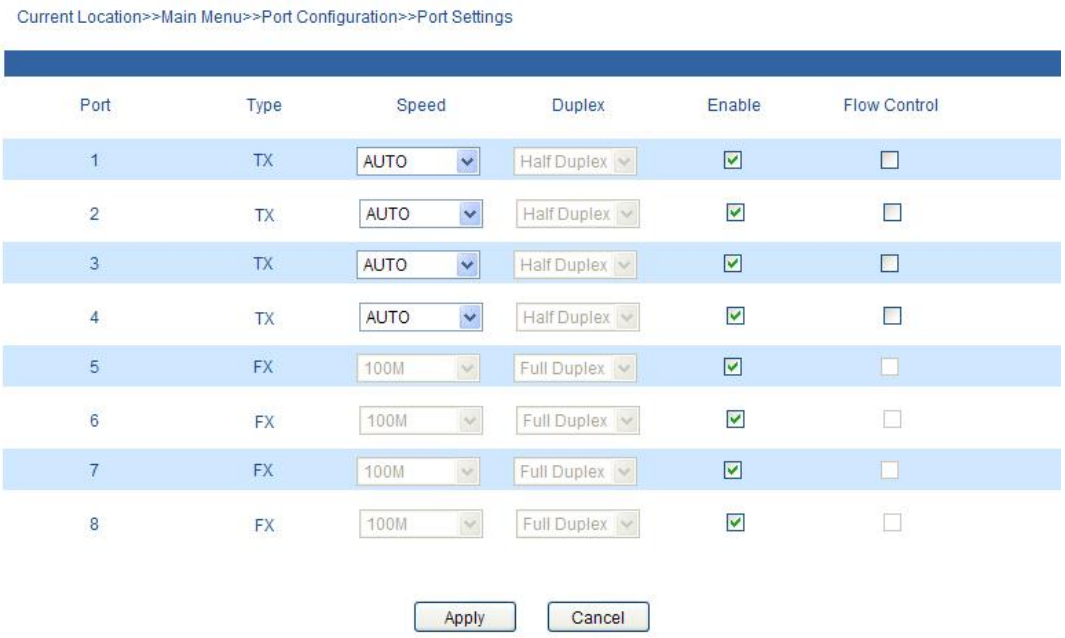
4 Port configuration

4.1 Port settings

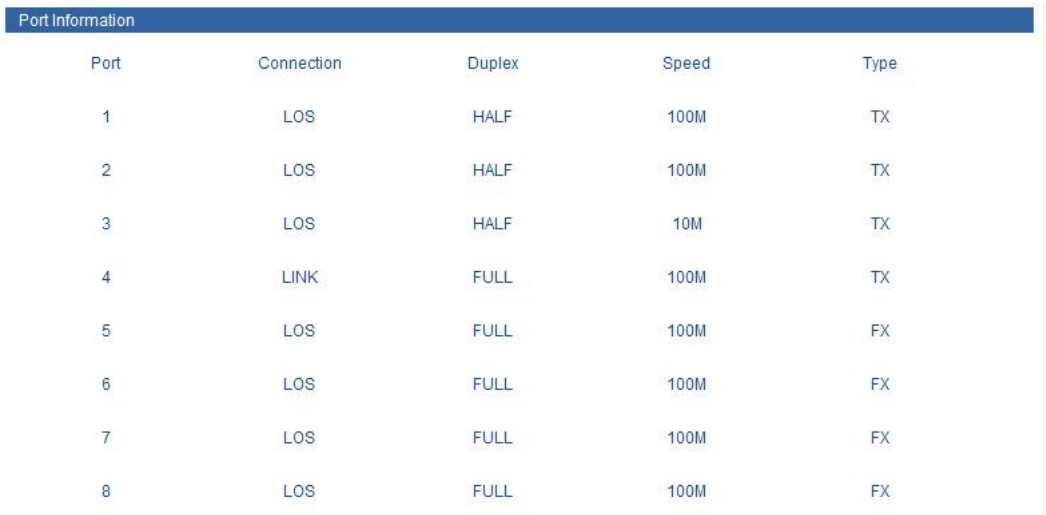
The port configuration interface mainly includes port type (Electric port or optical port), setup speed mode and duplex mode, flow control. Only when the port is enabled for the port speed, duplex, flow control will work. Select auto-negotiation, speed, and duplex auto-negotiation.

Configuration Items	Description
Port	Port name, corresponding to mark in panel.
Type	Display port type (TX or FX).
Speed	Display configurable speed of port or auto-negotiation mode.
Duplex	Auto-negotiation（AUTO）,full duplex（FULL）, half duplex（HALF）optional, default mode is auto-negotiation mode.
Enable	Configurable port enables or disable. Selecting square frame is for enable the corresponding port. It can not transmit data if any port disable. The default is “Enable”.
Flow Control	Whether selecting flow control to the port. Only can selecting flow control when the port enable. The default is off.

Port setting interface, as shown in Figure.



This feature is consistent with the port status of the port information, for example: set port 1 and port 2 is for the hundreds of megabytes rate half double work, use network cable connect port 1 and port 2, by port information for a query, you can view the status of port 1 and port 2. Port settings and restarts the device when you are finished. View port information column of the port State, rate, whether or not in accordance with reality.



Notes:

- When one end is auto-negotiation, and the other end to force rate setting, according to the Ethernet standard consultation rate for corresponding obligatory rate for half-duplex mode
- Port flow control auto-negotiation mode can be set only when other modes cannot be set

- Optical port rate mode, duplex mode, flow control may not be installed. It defaults to full duplex, flow control closed. This feature is consistent with the port status of the port information.

4.2 Bandwidth management

4.2.1 Bandwidth Management

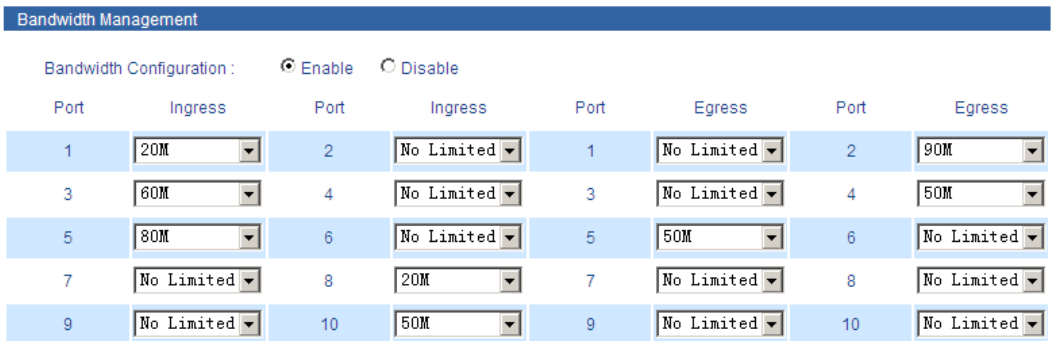
Bandwidth management mainly refers to limit the data's egress and ingress bandwidth to save the network sources.

Click [port setting/bandwidth management] and enter into the following interface.

Egress Bandwidth and Ingress Bandwidth Configuration:

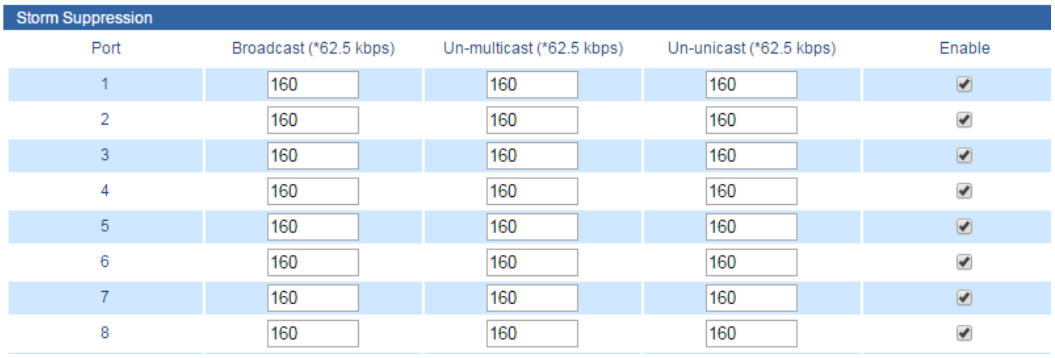
"----" stands for no limitation for the speed, the others are corresponding speed.

As shown in following figure, the forcible egress rate of Port 5 is 50Mbps. Only need to select 50Mbps in egress rate setting of Port 5. The bandwidth of Port 5 as receiver is still 80Mbps, but the forcible egress bandwidth of Port 5 is 50Mbps.



4.3 Storm Suppression

Broadcast storm is the accumulation of broadcast and multicast traffic on a computer network. Extreme amounts of broadcast traffic constitute a broadcast storm. A broadcast storm can consume sufficient network resources so as to render the network unable to transport normal traffic.



Storm Suppression

Port	Broadcast (*62.5 kbps)	Un-multicast (*62.5 kbps)	Un-unicast (*62.5 kbps)	Enable
1	160	160	160	☑
2	160	160	160	☑
3	160	160	160	☑
4	160	160	160	☑
5	160	160	160	☑
6	160	160	160	☑
7	160	160	160	☑
8	160	160	160	☑

There are many reasons to cause broadcast storm. For example: a redundant or incorrect connect among switches.

If enable storm suppression, it can stop the attack. Our device can detect 3 kinds of broadcast messages according to the type of broadcast storm.

Broadcast packets: data frame of the destination address of FF-FF-FF-FF-FF-FF

Multicast packets: destination address is XX-XX-XX-XX-XX-XX data frames, second x is odd numbers such as 1, 3, 5, 7, 9, b, d, and f, x represents any digit.

Unicast: unicast is the term used to describe communication where a piece of information is sent from one point to another point. In this case there is just one sender, and one receiver.

Destination lookup failure frame: the MAC address of this data frame doesn't exist in inside index. It needs to transmit to all the ports, including unicast and multicast flow.

Notes:

- The maximum length of Ethernet data frames is 1518 bytes, and each 64Kb of data communication includes about 6 Ethernet data frames with 1518-byte.
- The minimum length of Ethernet data frames is 64 bytes. Each 64 Kb of data communication includes about 128 Ethernet data frames with 64-byte.
- In the network the broadcast packets are more than 800packet/s, the network delay is obvious.
- The recommended setting is 3% based on the above theory.
- Please be caution to use MAC control frame and destination lookup failure frame, disabling IGMP Snooping will have impact on the transmission of the multicast.

5 L2 Features

5.1 VLAN

5.1.1 VLAN

Based on port VLAN

Port VLAN provides a solution that can divide the ports of switch into different virtual private domain. The data cannot be exchanged in the different private domain, so it's more secure to maintenance.

About port VLAN，different VLAN with different identity. Use the same ID identity will lead to internal members of the group be replaced, the new ID identity will create a new forwarding rule; all ports must belong to one or more VLAN.

1. Add Item

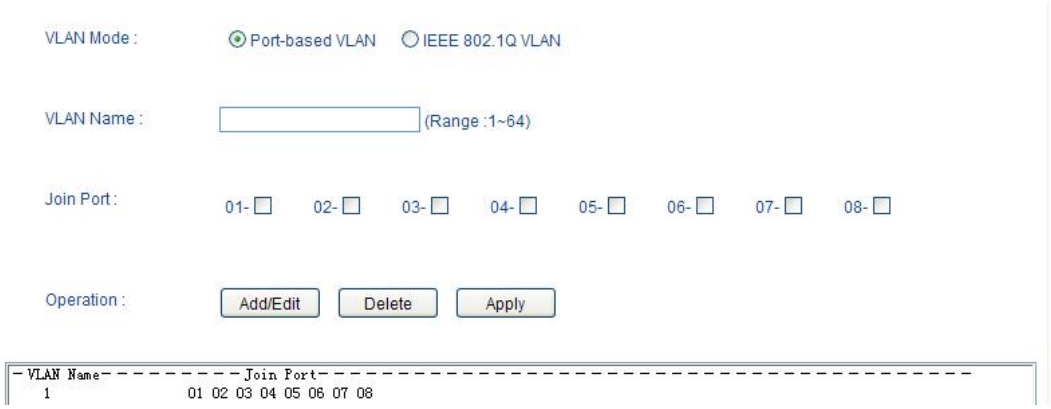
Group name can use any valid characteristic in port based VLAN. The same group name means you need to modify the members of the group. A new group name means the new transmission rule is built. The transmission item is not more than 32 in port based VLAN. It just changed the inside exchange rule, cannot achieve across switch.

Step 1 Choice “VLAN Group”, like as “3”, means VLAN1,

Step 2 Choice VLAN member, like as choice port 2 and port 3

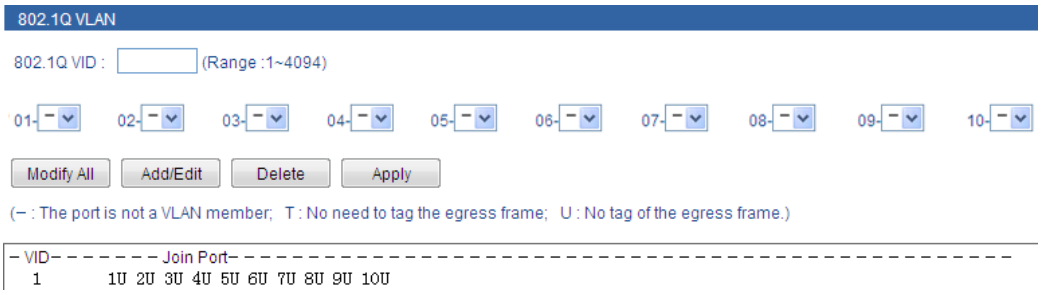
Step 3 Choice “Add/Edit”

Step 4 Choice “Apply”, then port 2 and port 3 were divided in VLAN3, they are in same VLAN, can transfer and receive data for each other.



Based on IEEE 802.1Q VLAN

Main function of IEEE 802.1Q VLAN is the VLAN tag. The tag including VLAN information can insert in the Ethernet frame. The device transmits the data according its transmission rules. VLAN tag protocol in the data frame is 2 byte; the number is 0x8100.



1. Add Item

Step 1 File in VLAN item in 802.1Q VID (Range: 1-4094);

Step 2 Choice port and add into VLAN table, if do not choice the port, it displayed "-" on right side, "U" means the port will be added in VLAN table and no tag of the egress frame. "T" means the port will be added in VLAN table and no need tag the egress frame

Step 3 The default setting of the port is PVID, change the VLAN group member's port PVID the same as VID (For special application, and PVID and VID can be different)

Step 4 Choice"Add/Edit" Button, the VLAN item will be added in VLAN table, Will be replace directly if there have same VLAN before configuration.

Step 5 Choice "Apply"

2. Delete Item

Delete the item in the table

3. VLAN configuration：

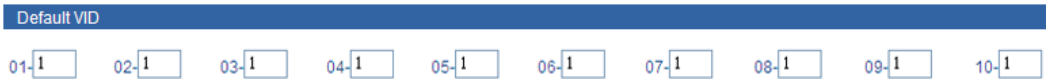
VLAN identification replace configuration:

Manage VLAN ID：

There must have members in VLAN, can access switch regularly through VLAN group members.

For example: If configure VLAN to VLAN2, it must have members (Like as port 2 and port3), then port 2 and port 3 can access switch regularly.

Port VID：The default configuration of port VID



- Keeping the same VID
  If data did not have VLAN mark, created VLAN mark with default priority and port VID and add to data frame, priority did not change. If data have VLAN mark, the data frame did not change, priority did not change.
- Replace identification VID with default VID
  If data did not have VLAN mark, created VLAN mark with default priority and port VID and add to data frame, if data have VLAN mark, VLAN mark's VID will be replace by default port VID

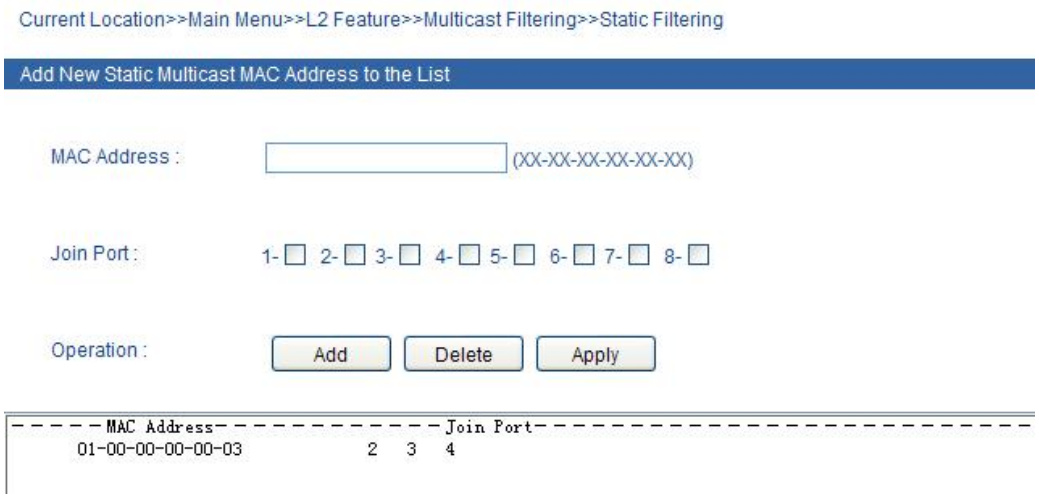
For example: Set port 2 and port 3 into VLAN2, PVID is 2, port 4 and port 5 into VLAN 3, PVID is 3, Choice" Keep VID and priority", then port 2 and port 3 can communication, port 4 and port 5 can communicate, port 2 and port 3 cannot communicate with port 4 and port 5.

5.2 Static filtering

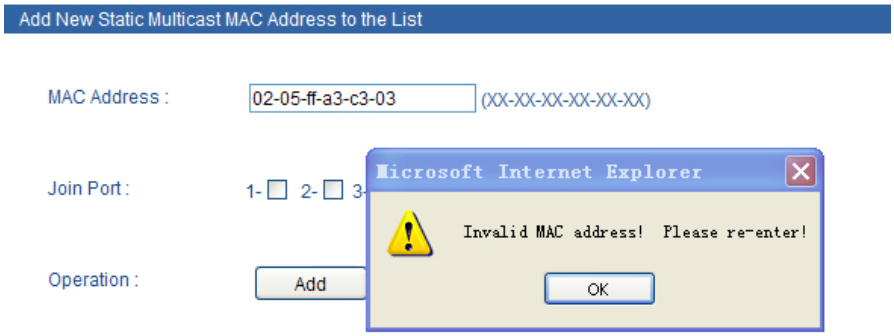
Devices to provide static MAC address forwarding. Static address table in a multicast MAC address corresponding to a port, if set, all data sent to this address will be forwarded to that port only, but the others could not receive data. Static address is the MAC address does not age once it has been added, this address tables before being deleted remains in effect, and not be restricted by maximum aging time. Switch supports up to 15 static multicast filtering.

Button [Add/Edit], [Delete] were used for add/delete static Multicast MAC address. Join port is used to choice the transmit port of static MAC address, can point to 1 or more transmit port. Knock [Add], [Delete], static MAC address will be updated. For example, add MAC address “01-00-00-00-00-03” member is port 2，3，4. Multicast MAC address is 1 of highest byte’s low byte.

Configuration	Description
MAC Address	Valid multicast address, a multicast MAC address is high byte low for 1
Join Port	Select desired configuration port
Add	The configured static multicast address entries added to the list
Delete	Selected multicast address is a static entry in the list, click <Delete>, delete this entry



All none multicast address did not allow adding in this table and the format must according to XX-XX-XX-XX-XX-XX, did not have space or other illegal character, otherwise, will be display warning information.



6 QoS

6.1 QoS Classification

QoS provides four internal queues, each queue supports four different levels of traffic, shorter persistence time of high-priority data packets in the switch, supports lower latency for certain delay-sensitive traffic. According to port ID, MAC address, 802.1p priority tags, DiONetServ and IP TOS, equipment can be abale to put the packets to an appropriate level.

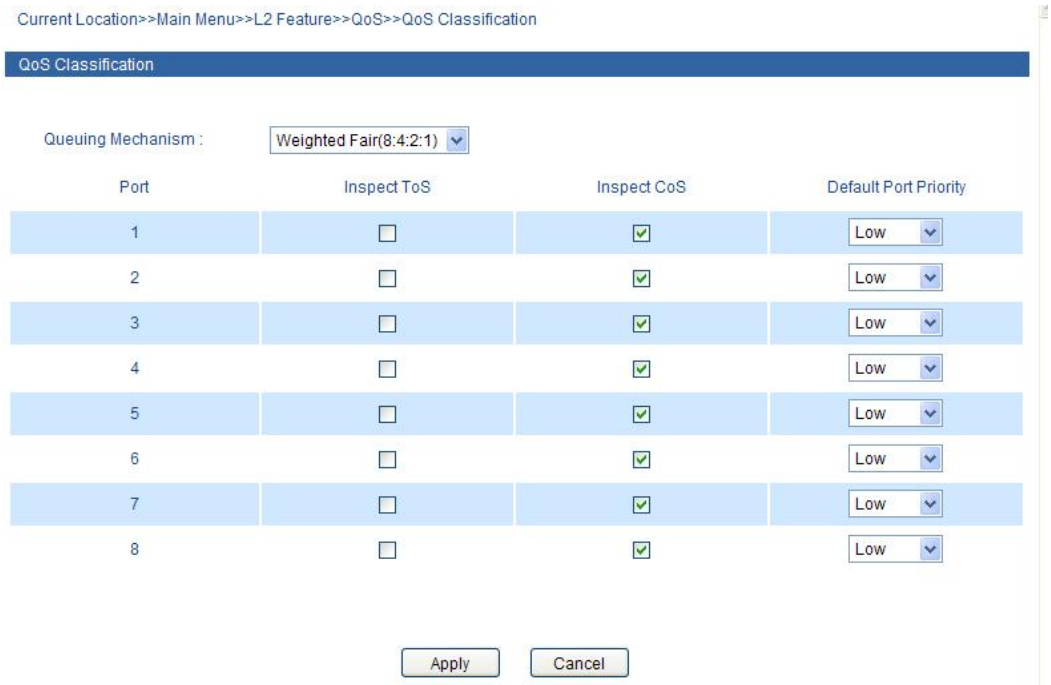
Users can select the QOS priority queue mechanism, the queue mechanism in two ways: weighted Fair mode and strict mode.

Weighted Fair refers to this port sends message according to queue priority High, Medium, Normal and low in proportion of 8:4:2:1 when some ports traffic is heavy. If sending speed is less than bandwidth, the message of each priority queues can send normally; if the port keeps sending in full speed, then the rest of the message of each priority queues will be discarded.

Strict priority: it refers to QoS deals with the message from high priority to low priority. If the low priority queues is full but the message of high priority queues don't finish, the message of low priority queues will be discarded; but if the speed of high priority queue does not reach the port's wire speed, then message of lower priority can send one by one, and the data may be lost because of shortage of bandwidth. The ports always finish all messages of high priority queues first then allow the message of lower priority queues

Default priority is based on port priority, default priority is different from COS and TOS, it did not have relationship with data package, it had relationship with switch port's priority. If the port's priority is higher, the data packet will be transferred at first.

When open port priority, must open inspect COS. The example is as figure below: open inspect port, 1, 2, 3, 4 COS, divide port 1, 2, 3, 4 in different priority, COS value corresponding priority no need to set up. Port 1, 2, 3, 4, port 1, the priority is the highest. When these 4 port's receive data must transfer from other port, because the limited of bandwidth, will be transferred according to priority queue mechanism (If use strict mode, then port 1's data must be transferred over at first. If use Weighted Fair 8:4:2:1, the 4 port will be transferred according 8: 4: 2: 1 ratio)



6.2 CoS

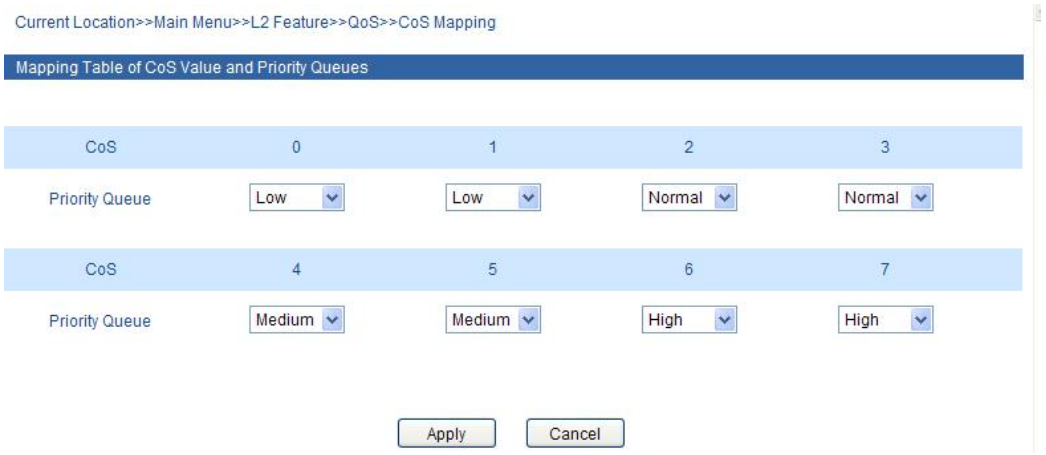
IEEE P802.1p is the name of a task group active during 1995–98 responsible for adding traffic class expediting and dynamic multicast filtering to the IEEE 802.1D standard. Essentially, they provided a mechanism for implementing Quality of Service (QoS) at the media access control (MAC) level. The group's work with the new priority classes and Generic Attribute Registration Protocol (GARP) was not published separately but was incorporated into a major revision of the standard, IEEE 802.1D-1998. It also required a short amendment extending the frame size of the Ethernet standard by four bytes which was published as IEEE 802.3ac in 1998.

The QoS technique developed by the working group, also known as class of service (CoS), is a 3-bit field called the Priority Code Point (PCP) within an Ethernet frame

header when using VLAN tagged frames as defined by IEEE 802.1Q. It specifies a priority value of between 0 and 7 inclusive that can be used by QoS disciplines to differentiate traffic. Although this technique is commonly referred to as *IEEE 802.1p*, there is no standard or amendment by that name published by the IEEE. Rather the technique is incorporated into IEEE 802.1Q standard which specifies the tag inserted into an Ethernet frame.

802.1P defined 8 priorities（0-7）, corresponding 4 priority (High, Medium, Normal, Low)

Default priority mark 0 and 1 is low queue, 2 and 3 is normal queue, 4 and 5 is Medium, 6 and 7 is High.



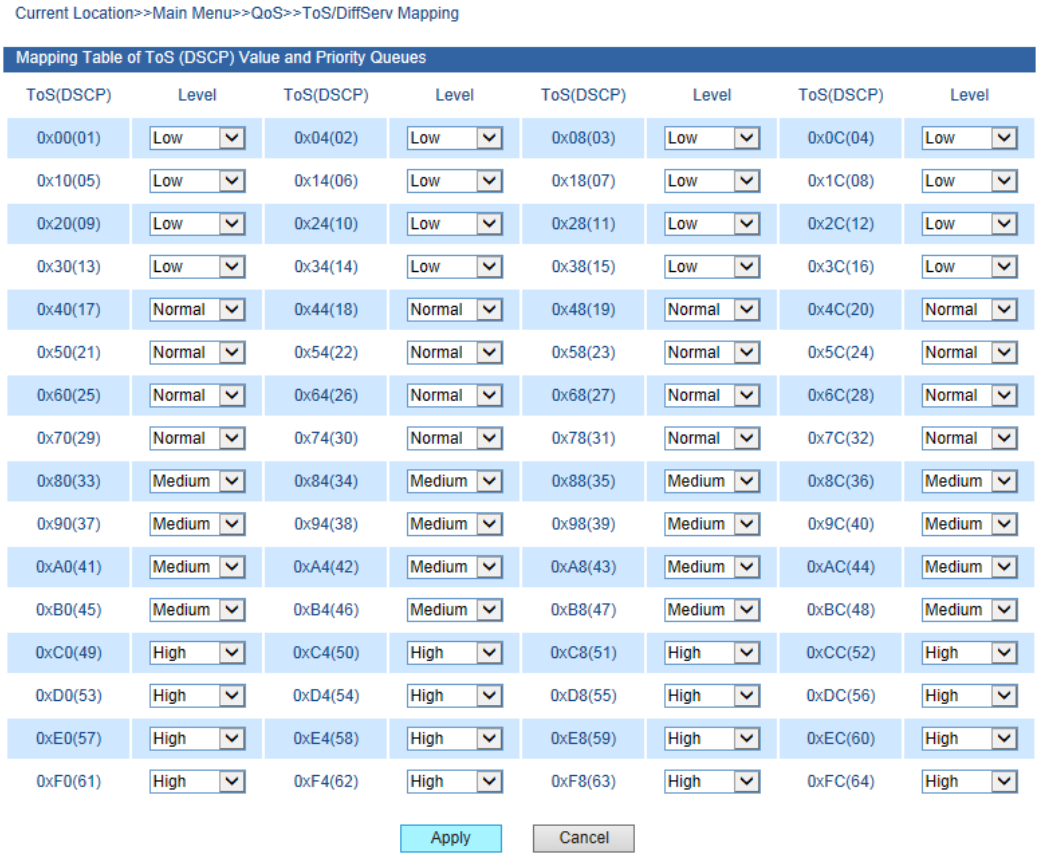
6.3 Tos

DiffServ architecture provides each transport packets in the network are classified into different categories, classified information is contained in the IP packet header, DiffServ architecture using the first 6 bits of IP packet header TOS(Type of Service) to carry the packets' classified information. This definition is only for the lower 6 bits, one number does not exceed 63. This definition supports both IPv4 (ToS field) and IPv6 (Traffic Class field). DSCP has 64 priority values (0-63), the lowest priority 0 and the highest priority 63. In fact, the DSCP field is a superset of the IP precedence field, DSCP field definition is backward-compatible with IP precedence field.

So far, the defined DSCP with default DSCP, the value is 0; class selector DSCP defined as the backward-compatible with IP precedence, the value(8,16,24,32,40,48,56); Expedited Forwarding (EF), generally used for low latency service, the recommended value is 46 (101110); identified by forwarding (AF)

defines four service levels, each service level has 3 down process, so spent 12 DSCP values ((10,12,14), (18,20,22), (26,28,30), (34,36,38)).

The priority value of the device (1-16) is defined as the lowest priority, as the first queue. Priority value (17-32) is defined as the second queue, the priority value (33-48) is defined as the third queue, the priority value (49-64 is defined as the fastest queue, the highest priority.



7 Redundancy

7.1 Rapid Ring

7.1.1 SwRing

SwRing™ technology provides auto-recovery and re-connection mechanism for broken network. When network is broken, it has link redundancy and self-recovery capability and self-recovery time is less than 20ms. SW-Ring is the patented technology of 3onedata Co.,Ltd. designed for industrial control network requiring high reliability.

SwRing™ technology support maximum 250 pieces switches, in which the **SwRing**™ its self-recovery time is <20ms.

Each port of Switch can be Ring Port to connect other switches. When network is broken, relay for failure alarm will be activated. Redundant organization of **SwRing**™ enable backup link to recover network instantly.

Self-developed patented technology for SW-Ring network can realize the intelligent redundancy for industrial Ethernet switch, which can make you easily and conveniently establish redundant Ethernet, and can facilitate the quick recovery of any network section of automatic system disconnected from the network. Switch supports maximum 4 ring groups. Each group set up 2 ports as Ring Port and a port cannot belong to several rings.

Hello_time setting is time interval of sending detecting packet to network at regular time. The unit is ms. Its main purpose is to detect network connection. It sends a detecting packet to next door devices by CPU. If they receive it, then reply a confirm

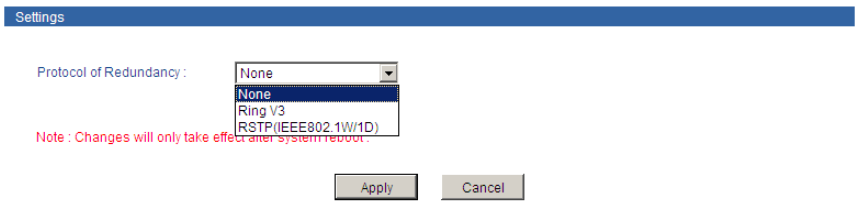
packet to ensure network connection is active. If this setting will influence self-recovery time, we suggest advanced users can use it.

Basic interface of Rapid Ring as shown in figure below:

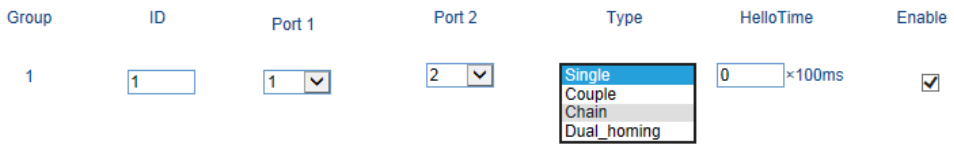
Initial interface display redundancy protocol is none, can configure it through [Settings]. Ring V3 support Single ring, coupling ring, chain ring and Dual_homing.

Method to enable Ring V3

Step 1 Enable Ring V3，Select Ring V3 in [Settings] drop-down menu, figure as shown below



Step 2 After select Ring V3, Configuration interface is as figure below, we can see Ring V3 support 4 different ring group: Single, Coupling, Chain and Dual_homing.



Step 3 Enable Ring Group 1 (or Group 2), and enter into Network ID (support 0-255 number only). Select Ring Port between Port 7 and Port 8.

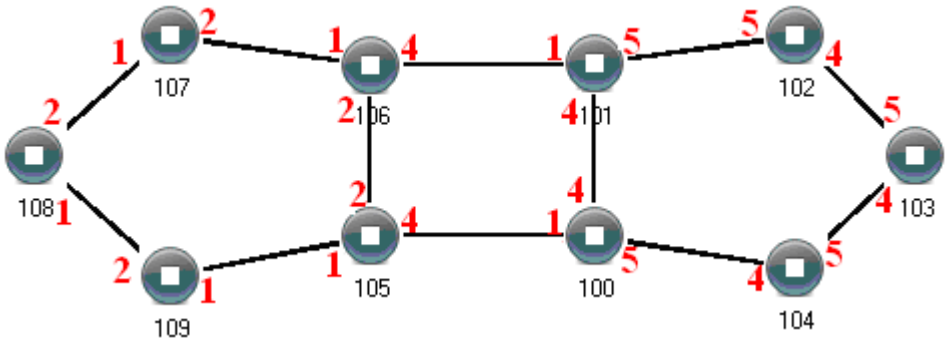
"Chain" refers to strengthen user's capability of making any type of redundant topological structure with flexibility by taking an advanced software technology. In fact, Chain is to cascade several switches already set up to Ring and both sides of chain access to network.

"Dual Homing" refers to a fact that two Rings connect the same switch. This type of configuration is ideal choice for centralized management of several Rings.

Method to enable Chain and Dual Homing is similar to that to enable Single Ring and Coupling Ring. It only needs to select corresponding items in [Type].

1. Method to enable Ring V3 coupling ring

The architecture of coupling ring as figure below:

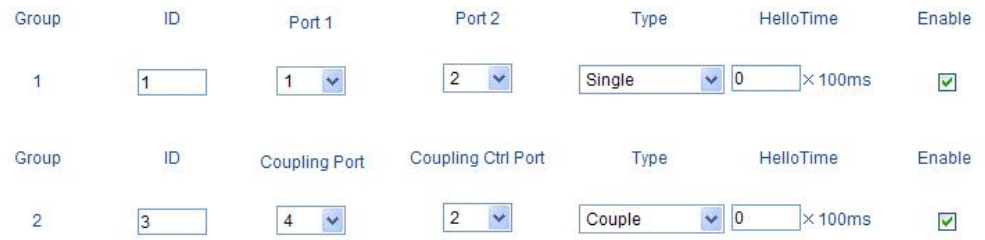


Operation method:

Step 1 Select Ring V3, enable ring group 1 and 2. (Hello_time can be disable, if enable, time of sending Hello packet could not be very fast, it will influence CPU operate speed);

Step 2 Set 105, 106 device's ring port as port 1 and port 2 in ring group 1, network ID: 1, type: single ring.

Step 3 Set ring port as port 4 in ring group 2, Coupling ctrl port: 2, network ID: 3, type: coupling ring, figure as shown below.



Step 4 Set 100, 101 device's ring port as port 4 and port 5 in ring group 1, network ID: 2, type: single ring.

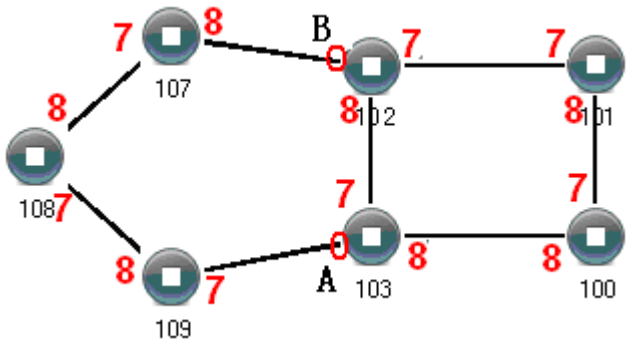
Step 5 Set ring port as port 1 in ring group 2, Coupling ctrl port: 4, network ID: 3, type: coupling ring, figure as shown below.

Step 6 Set 107, 108, 109 device's ring port as port 1 and port 2 in ring group 1, network ID: 1, type: single ring. Set 102, 103, 104 device's ring port as port 4 and port 5 in group 1, network ID: 2, type: single ring.

Step 7 Connect 100-104 devices' port 4 and port 5 with network cable. Connect 105-109 devices' port 1 and port 2 with network cable, Connect 101 device's port 1 to 106 device's port 4 with network cable, Connect 100 device's port 1 to 105 device's port 4 with network cable.

2. Method to enable Ring V3 Chain ring

The structure of Chain ring as figure below



Operating method:

Step 1 Enable Ring Group 1: Hello time can be disable too, if it enable, time of sending Hello packet could not be very fast, or it will influence CPU dealing speed.

Step 2 Set up Port 7 and 8 of Device 100, 101, 102 and 103 to be Ring Port in Ring Group 1, Network ID is1, Ring Type is Single; as shown in figure. Set up Port 7 and 8 of Device 107, 108 and 109 to be Ring Ports in Ring Group 2, Network ID is 2. Ring Type is Chain; as shown in figure below.

Step 3 Use a wire to connect Port 7 and 8 of Device 107-109 in turn to make a chain. Use a wire to connect Port 7 and 8 of Device 100-103 in turn to make a Single Ring, Then use a wire to connect Port 8 of Device 107 and Port 7 of Device 109 to normal port of Device 102 and 103. Chain is finished.

Notes:

- Port can not be trunking setting when it is already Ring port.
- In the same single ring, identity must be consistent; otherwise it will not build a ring and can not communicate.
- All ring ports in the VLAN settings must be TRUNK tagged VLAN member, otherwise can not communicate.
- To form tangent ring or other complex rings, should pay attention to the ring identity whether is it consistent, different single ring identification must be different.

7.1.2 RSTP

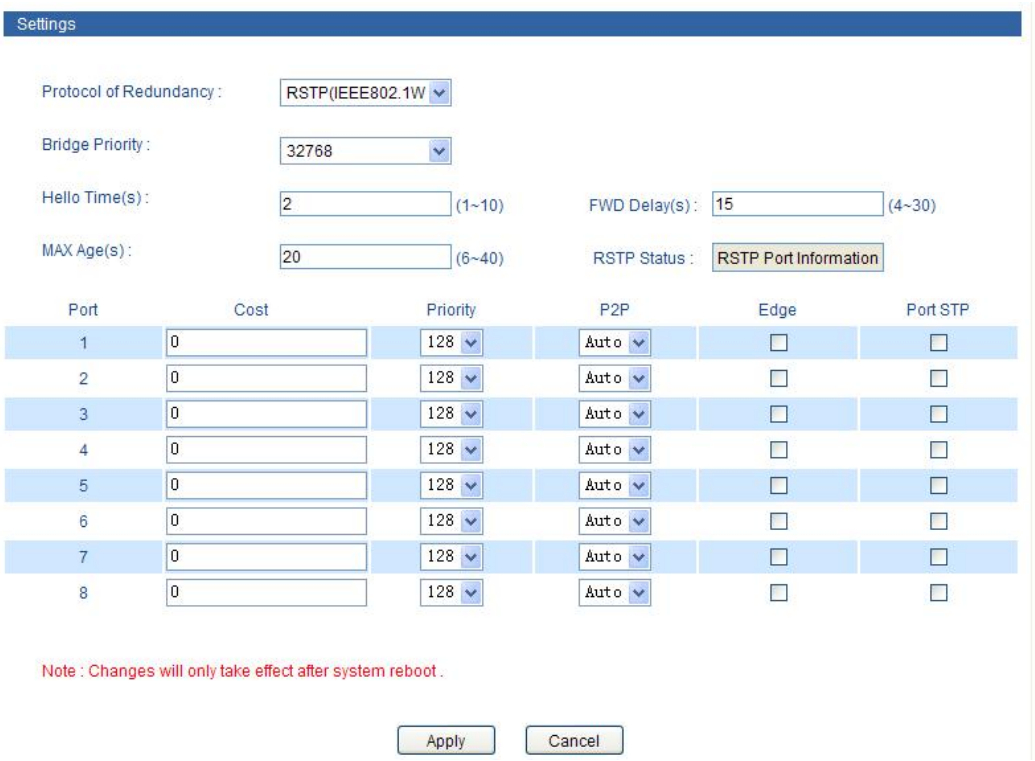
The first spanning tree protocol was invented in 1985 at the Digital Equipment Corporation by Radia Perlman. In 1990, the IEEE published the first standard for the protocol as 802.1D, based on the algorithm designed by Perlman. Subsequent versions were published in 1998 and 2004, incorporating various extensions.

Although the purpose of a standard is to promote interworking of equipment from different vendors, different implementations of a standard are not guaranteed to work,

due for example to differences in default timer settings. The IEEE encourages vendors to provide a "Protocol Implementation Conformance Statement", declaring which capabilities and options have been implemented, to help users determine whether different implementations will interwork correctly.

Also, the original Perlman-inspired Spanning Tree Protocol, called DEC STP, is not a standard and differs from the IEEE version in message format as well as timer settings. Some bridges implement both the IEEE and the DEC versions of the Spanning Tree Protocol, but their interworking can create issues for the network administrator, as illustrated by the problem discussed in an on-line Cisco document.

In 2001, the IEEE introduced Rapid Spanning Tree Protocol (RSTP) as 802.1w. RSTP provides significantly faster spanning tree convergence after a topology change, introducing new convergence behaviors and bridge port roles to do this. RSTP was designed to be backwards-compatible with standard STP.While STP can take 30 to 50 seconds to respond to a topology change, RSTP is typically able to respond to changes within 3 × Hello times (default: 3 times 2 seconds) or within a few milliseconds of a physical link failure. The so-called Hello time is an important and configurable time interval that is used by RSTP for several purposes; its default value is 2 seconds. Standard IEEE 802.1D-2004 incorporates RSTP and obsoletes the original STP standard Select RSTP function in rapid ring network interface as follows:



Rapid Spanning Tree of concepts:

- **Switch priority**：As the bridge priority，the bridge priority and bridge MAC address combine bridge ID，the smallest ID bridge will become the root bridge on the network.
- **Polling interval**：how often send BPDU packet at one time.
- **Forwarding delay**：the port state of switch remain a forward delay time over the listening and learning.
- **The maximum aging time**：After one switch receive a packet from other switches , how long the packet is valid
- **The port concepts of RSTP:**
- **Port path overhead**：port link cost compared with port priority and port ID .
- **Port priority**：port priority among the net bridge compared with port priority and port ID.
- **Point to point network connection**：directly connect with switches port each other ,the port is P2P,which adopted negotiation mechanism,RSTP can achieve port state rapid conversion RSTP.
- **Directly connect terminal**：connect the edge of network switch with terminal devices with **configuration Edge port**，which can achieve port state rapid conversion without the processing Discarding，Learning，Forwarding.
- **Don't join RST structure**：don't participate in RSTP running.

RSTP switch port states:

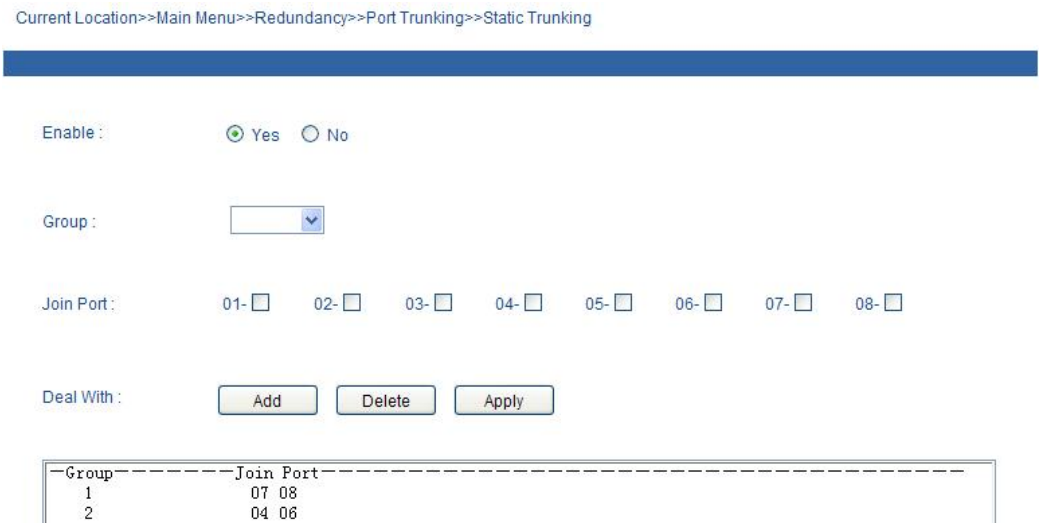
- **Blocking**- A port that would cause a switching loop if it were active. No user data is sent or received over a blocking port, but it may go into forwarding mode if the other links in use fail and the spanning tree algorithm determines the port may transition to the forwarding state. BPDU data is still received in blocking state. Prevents the use of looped paths.
- **Listening**- The switch processes BPDUs and awaits possible new information that would cause it to return to the blocking state. It does not populate the MAC address table and it does not forward frames.
- **Learning**- While the port does not yet forward frames it does learn source addresses from frames received and adds them to the filtering database (switching database). It populates the MAC Address table, but does not forward frames.
- **Forwarding**- A port receiving and sending data, normal operation. RSTP still monitors incoming BPDUs that would indicate it should return to the blocking state to prevent a loop.

The example of Configuration: The priority of network bridge is "32768"，If there did not have network ID less than itself, itself is root network bridge. There did not have same network ID in network. Every 2 seconds, the network bridge will transmit BPDU

message to all appoint port. If did not receive BPDU message more than 20 seconds, it realized port invalid, will calculate the status of network bridge again. Each status exchange for each other if need to transmit, need to wait 15 seconds

7.2 Port Trunking

In telecommunications, trunking is a method for a system to provide network access to many clients by sharing a set of lines or frequencies instead of providing them individually. This is analogous to the structure of a tree with one trunk and many branches. Trunking, is set by the configuration software, the two or more physical ports get together into a logical path to increase the bandwidth between the switch and the network node. Trunking is a packaging technology, it is a peer to peer link, both ends of the link are switches, it can be a switch and a router, and also can be a host, switch or router. Based on port trunking function that allows between two or more ports between switches, switches and routers, hosts the switch or router connected in parallel to provide for the simultaneous transmission of higher bandwidth and greater throughput, significantly entire network capacity. Trunking is more economical to increase the bandwidth between the switch and network device, such as servers, routers, workstations, or other switches. Trunking function is to integrate more than one physical port (typically 2-4) to a logical channel.



Device supported 2 trunking group, operate method: choice apply, choice the port need to trunking the port list, Choice setting, available after reboot. If the port already

set to Ring port, it cannot set to trunking port. Each trunking group at least have 2 port member, at more 4. 1 port cannot exist in 2 trunking group.

Notes:

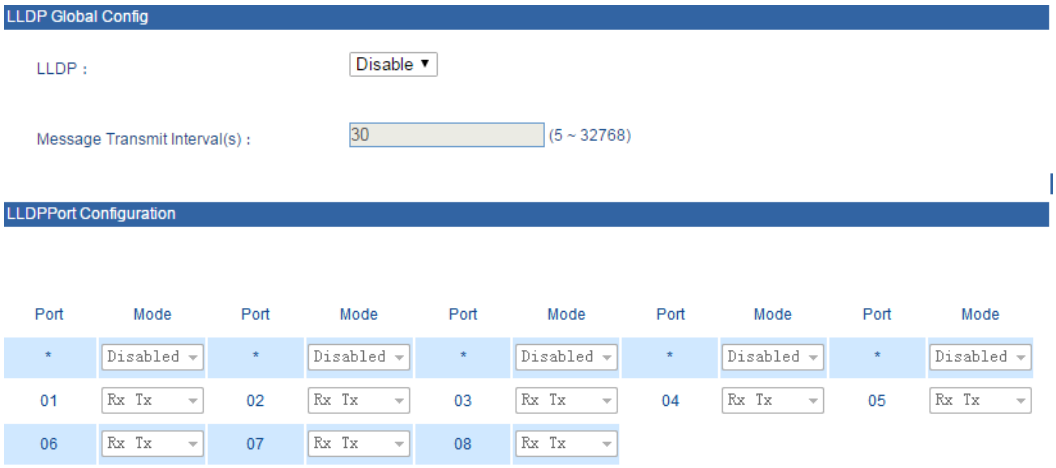
- The trunking groups require all the attributes can be the same, including speed, duplex, STP state etc.
- If you do not confirm the STP state, please disable RSTP function, or close others, leaving only one STP channel.
- Port 1 as the system reserved, cannot be used as trunking.
- The ports of having been set to the port aggregation that cannot be set to ring ports.

8 LLDP

8.1 Parameter Configuration

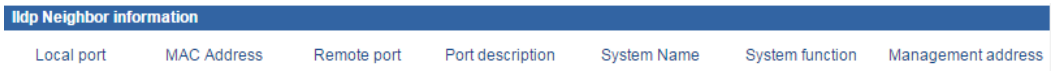
LLDP is a second layer topology discovery protocol, the basic principle is: network equipment to the adjacent equipment issued its notice of state information, and each port of all equipment are stored with their own information, if a local device state changes, also can with its directly connected neighbor devices to send updated information to that neighbor devices will be the information stored in the standard SNMP-MIB library. Network management system can query from the SNMP-MIB Library of the current second layer connection. It should be noted that LLDP is only a remote device status information discovery protocol, it can't complete the network device configuration and port control and other functions.

Configuration item	meaning
Disable	The switch will not send the LLDP message, and will reduce the LLDP message received from the neighbor.
Enable	The switch will send the LLDP message, which will analyze the LLDP message received from the neighbor.
TX interval	The switch status is not changed, the device periodically to the neighbor nodes to send LLDP packets, the interval time is called to send LLDP message interval.
RX	Switch will not send out the LLDP information, but the information from the vicinity of the unit LLDP analysis.
TX	Will reduce the LLDP information received from the neighbors, but will send LLDP information.



8.2 Neighbor Information

LLDP management address is the address of the network management system identification and management. Management address can clearly identify a device, it is conducive to the network topology, network management, network management. The management address is encapsulated in the Management Address TLV field of the LLDP message and is sent to the neighbor node.



9 Access Control

9.1 User Password

Enterprise usually required two different people to monitor device and manage system/network. The authority need to separate. Monitor person was in charge of monitor work, system/network person was in charge of system/work management. The switch provided classification management: Administrator authority and Observer authority. Observer just had authority to check the status of switch. Administrator had the authority to configure the parameters of the switch.

Index

User index indicates which group of users. There are three user indexes in drop-down list.

Access level:

- administrator: have the right to check and configure all settings
- observer: have the right to check all settings merely

Login name

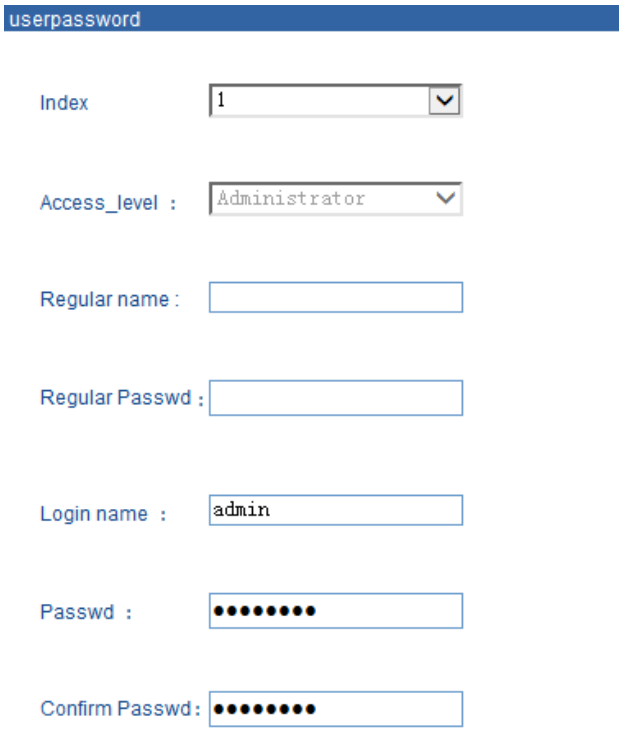
The identity of visitor with the letter combination is no more than 16 bytes

Password:

Visitor use password, user authority allows the letter combination no more than 16 bytes

Confirm password

Make sure the last time input password is correct.

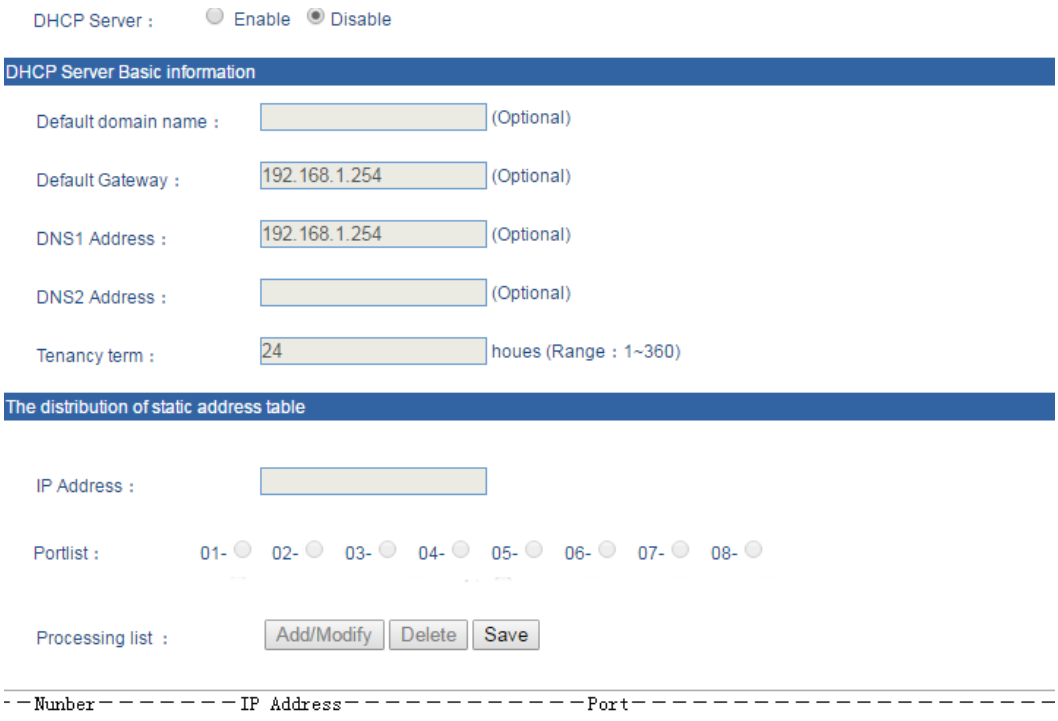


Notes:

- User must remember user name and password after modified. If forget it, please use DIP switch to make default factory. The default user name and password: admin12345.
- Set same user mane, the front settings of user name/password will be available.

9.2 DHCP Server

The DHCP Server function is enabled, is to use this equipment as a DHCP server, by setting the static address table realization, this equipment is able to assign IP addresses to other devices connected to this equipment. For example: If the device is a turn on DHCP Server functionality, 2 sets the static address table: 192.168.1.19 corresponds to port 1; 192.168.1.20 port 2. Unit b opens automatically obtain an IP address feature, if the device is connected to a port 1 device-b, device b to automatically obtain IP addresses 192.168.1.19; if the device is connected to port 2 and an equipment b equipment b able to automatically obtain an IP address 192.168.1.20.



Fill out basic information about the DHCP Server, the DHCP client can automatically access to the information.

- **Default domain name:** DHCP client can automatically access to the domain name;
- **Default gateway:** DHCP client can automatically access to the gateway;
- **DNS address:** DHCP clients to automatically obtain DNS address;
- **Lease:** DHCP clients to automatically obtain the address to a valid time. Range from 1-360 hours

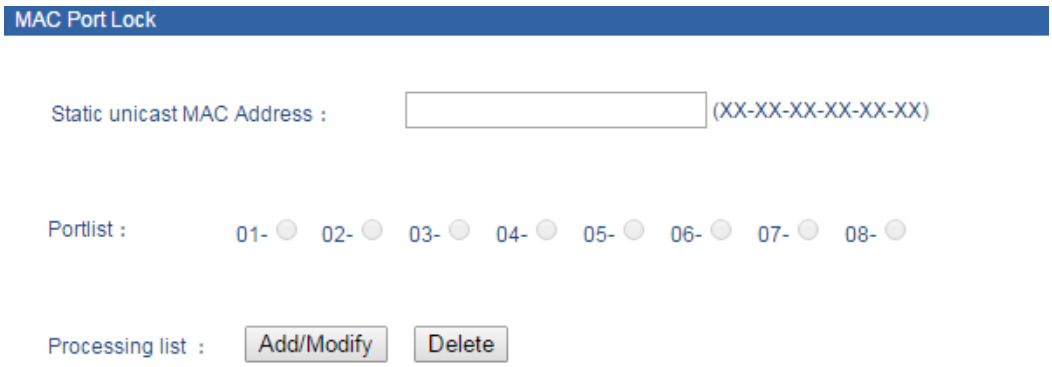
9.3 MAC port lock

Static MAC address table

Static MAC address is different from dynamic MAC address. Once the static address is added, the address will remain in effect before deleting it, cannot be limited by the maximum aging time. Static address list records the static address of ports. In the static address list, one MAC address corresponds to one port, if try to configuration, all data sent to this address will only be forwarded to the port. And also become he MAC address binding.

Static MAC address list is designed to limit the movement of the computer, any computer's MAC and port binding, this computer inserts to the other port cannot

communicate with another computer, over this interface can still communicate with other computers. Port security is designed to protect the port and the corresponding port security, the port will forward the data when the specified MAC make a connection with this port, it is assumed that to set port security and with one MAC binding, then this PC can communicate with other ports, but other computers connected to this port cannot communicate. Button [Add/Edit] and [Delete] for adding, removing the static MAC address. Static MAC address requests a valid input from the user, will display warning messages if you enter an invalid MAC address. Port field is used to select a static MAC address forwarding ports; you can specify one or more forward ports. Click [Add/Edit] and [Delete] will trigger the static MAC address forwarding table updates.



Notes:

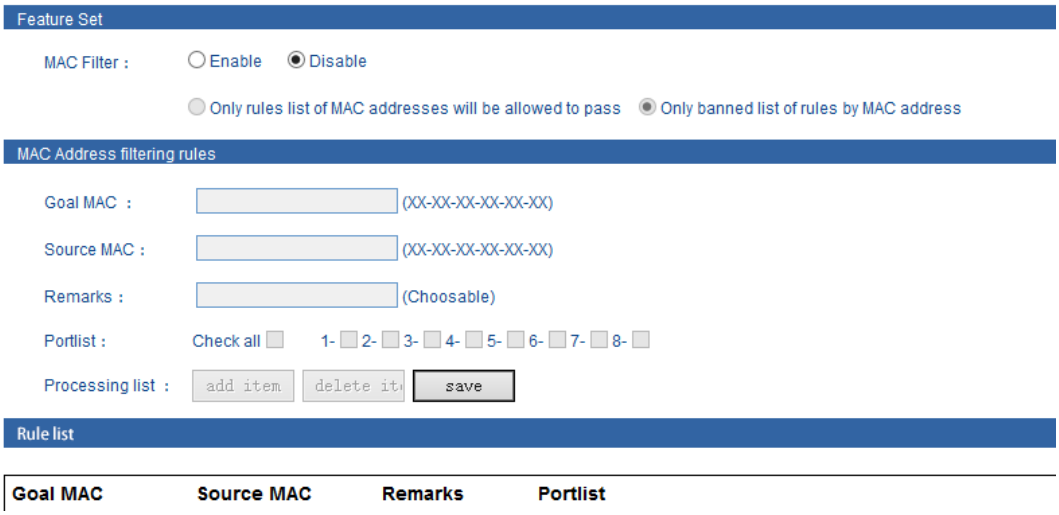
- This function is a security mechanism, be careful to confirm the setting, otherwise be used with caution.
- Do not use a multicast address as the input address.
- Do not enter the reserved MAC address, such as the device's MAC address.

9.4 Safety management

Security management can filter the MAC, set the port to allow or prohibit a specific MAC address.

MAC filtering

MAC address filtering interface includes enabling or disabling MAC address filtering, MAC address filtering rule setting and rule list view, as shown in Figure.



10 Remote monitoring

10.1 SNMP management

- Introduction of SNMP

  SNMP (Simple Network Management Protocol) is an internet-standard protocol for managing devices on IP networks. It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

- Work Mechanism of SNMP

  SNMP includes 2 parts: NMS and Agent:

  NMS: Network Management Station. Software runs on the manager. The common management platforms are "Quid View", "Sun Net Manager" and "IBM Net View". Agent is the software of the server running in the network device. NMS can send "Get Request", "Get Next Request" and "Set Request" message to Agent. After Agent gets those messages, it will read or write according to the message type to create Response message and send the Response message back to NMS. Agent will also send Trap message to NMS when the device is abnormal.

- SNMP Version

  Currently SNMP Agent of the device supports SNMP V3 and it is also compatible with SNMP V1and SNMP V2C. It is authenticated by user name and password in SNMP V3.

  SNMP V1 and SNMP V2C adopt authentication of Community Name. The SNMP message of the community name which is not authenticated will be discarded. SNMP community name defines the relationship of SNMP NMS and SNMP Agent. User can choose the following one or more features related to community name.

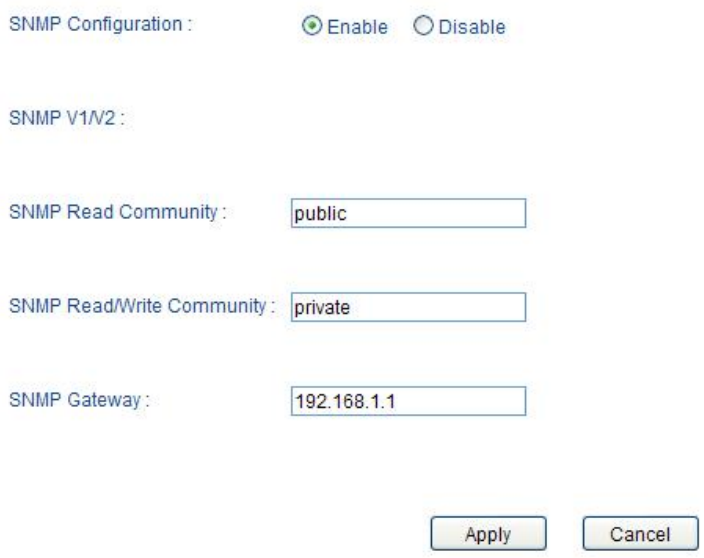
- Defines MIB view of community name.
- Setup visit privilege of MIB objective is Write or Read. Community name with Read privilege can check the device information only. Community name with Write privilege can configure the device.
- Setup appointed basic visit control list of the community name.

Switch supports SNMP V1/V2c. Both SNMP V1 and V2c use public character strings for match authentication.

SNMP usually uses UDP Port 161(SNMP) and 162 (SNMP-traps) based on TCP/IP protocol. SNMP protocol agent is existed in network device. MIB (information specific to the device) is uses as device connector. These network devices can be monitored or controlled through the agent. When trap event happens, a message is transmitted by SNMP Trap, an available trap receiver can get this trap information.

SNMP supports 3 kinds of basic operating in total:

- **Get:** Manager can use this to get some variable value of Agent.
- **Set:** Manager can use this to set up some variable value of Agent.
- **Trap:** Agent uses this to send an alarm to manager.



Read Community

Use a character string to name a SNMP community. This community only has Get privilege.

Read/Write Community

Use a character string to name a SNMP community. This community has Get and Set privilege.

SNMP TRAP Gateway

IP address of the receiver of the alarm information sent Agent

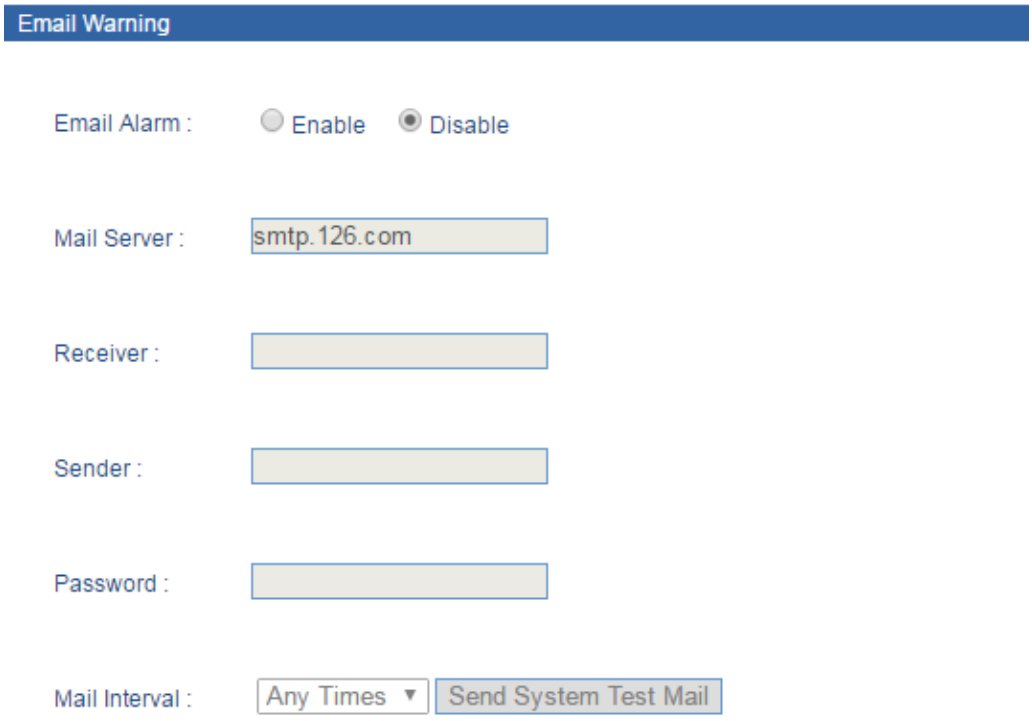
Notes:

The device supports warm start of Trap. If existed IP address in Trap gateway, click "Apply", the Trap receiver can get the trap information. If the trap receiver cannot get trap information, please check network setting and connecting. Please pay attention to the privilege of Read and Write in SNMP Explorer.

10.2 Email Warning

Please make sure the switch can access internet regularly if use Email Warning. The gateway of the switch and local area network must identical.

Email warning function will send the warn information immediately by Email if these things happen: NTP information, connection statue changed, login information, broadcast storm information, operating record, and other system log.



Mail server

Please provide the host IP of POP3 mail delivery service or the host name to our device

Sender

E-mail account is used to login to e-mail server.

Password

E-mail password.

Receiver

Recipient to solve the problem of abnormal events hoping to find a contact e-mail address

Mail Interval

Regularly send log interval time

10.3 Relay alarm

Warning had 2 types: Power alarm, port alarm. Main function: once the devices were in unusual status, can inform administrator in time and repair the status of device quickly, can avoid more lose

Relay warning input type: Close/Open. Once select close, the light will be bright when alarms have. Relay will be in open status.

Power alarm

Switch provided dual DC power supply (AC power supply did not have alarm), if one power supply had problem, another will support power supply immediately, dual power supply hot back-up. Select to enable power alarm, If power supply was in unusual status, device will send alarm signal, inform power supply work unusual.

Port Alarm

Alarm when port disconnects. Enable port alarm, if port was in unusual status (Connect or disconnect), device will output a signal, inform the device work unusual.

Note:

In default status, the type of relay output is open, the alarm light is OFF, and have no alarm, relay alway open.

When the device have alarm, the light is ON, relay close.

11 Port Statistics

The function of traffic Statistics is to calculate the data packets in a fixed time, included transmit and receive data packets.

Operate method: Start to calculate after select clear

11.1 RX frame statistics

Current Location>>Main Menu>>Port Statistics>>Rx Frame

Rx Frame Statistics

Port	Unicast	Multicast	Broadcast	Drop	Pause	UnderSize	OverSize	Fragments	Jabber	SysbolErr
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	0	0	0	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

Unicast

Numbers of the unicast data packets received by the port

Multicast

Numbers of the multicast data packets received by the port

Broadcast

Numbers of the broadcast data packets received by the port

Drop

Number of discarded normal data packets because of safety control

Pause

Ethernet control frames of protocol 0x8808 received by the port, in full duplex mode; this data packet is used to control frequency of data sending.

Undersize

Number of data packets (including FCS) less than 64 bytes

Oversize

Number of data packets (including FCS) more than 1518 or 1522 bytes (Enable VLAN)

Fragments

Number of incorrect or incomplete FCS data packets (including FCS) less than 64 bytes

Jabber

Number of incorrect or incomplete FCS data packets (including FCS) more than 1522 bytes

SysbolErr

Number of data packets which is incorrect, incomplete or including invalid characters (including FCS) between 64 bytes and 1518/1522 bytes (Enable VLAN)

11.2 TX frame statistics

Current Location>>Main Menu>>Port Statistics>>Tx Frame

Port	Unicast	Multicast	Broadcast	Drop	Pause	Collision	Multiple Collision	LateCollision	Conflict Discard	Res Busy Discarded
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	0	0	0	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

Unicast

Numbers of the unicast data packets sent by the port

Multicast

Numbers of the multicast data packets sent by the port

Broadcast

Numbers of the broadcast data packets sent by the port

Drop

Number of discarded normal packets because of lack of resources or not meeting analytic conditions (excluding discarded packets because of conflict)

Pause

Ethernet control frames of protocol 0x8808 sent by the port, in full duplex mode, this data packet is used to control frequency of data sending

Collision

Number of conflicts encountered in the port while sending data

Multiple Collision

Number of successful output packets (collision more than 1 time)

Late Collision

Numbers of packets less than 64 bytes when a conflict is detected.

Conflict Discard

Numbers of discarded packets caused by conflict happening more than 16 times.

Res Busy Discarded

Number of discarded packets out of stack queue because of lack of resources (large amounts of low priority data after enabling QoS)

11.3 Traffic Statistics

Traffic Statistics

Port	Tx	Rx	Unicast	Multicast	Broadcast	Error
1	0	0	0	0	0	0
2	3571352	8244712	7857	33256	18490	0
3	0	0	0	0	0	0
4	0	0	0	0	0	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

Tx

Number of bytes of all data packets sent by the port

Rx

Number of bytes of all data packets received by the port

Unicast

Number of unicast data packets sent and received by the port

Multicast

Number of multicast data packets sent and received by the port

Broadcast

Number of broadcast data packets sent and received by the port

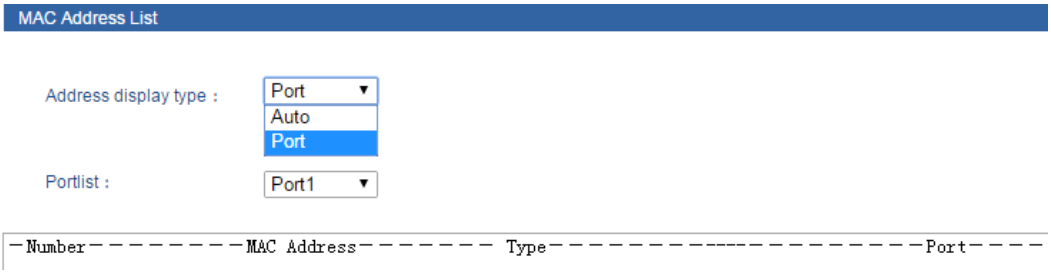
Error

Number of error packets because of some reasons sent and received by the port

11.4 MAC address table

MAC（Media Access Control）address is the network device hardware identification, the switch to forward packets based on MAC addresses. The MAC address is unique, which ensures correct packet forwarding. Each switch maintains a MAC address table. In this table, MAC addresses and switches port one-to-one correspondence. When the switches received a data frame, according to the MAC address table to determine

the filter or forward the data frame corresponding to the switch port. MAC address table is the basis and premise of the switch to achieve fast forwarding.



MAC address classify into three types in device address MAC address list:

- Dynamic MAC address
  Dynamic MAC address of the switches in the network through the data frame to learn, when the arrival of aging time will be deleted. When the device is connected to the switch port to change the MAC address table and port corresponding relationship will change accordingly. Dynamic MAC address of the switch is powered restart will disappear, the need to re-learn.
- Static certification (solidify) MAC address
  Static authentication MAC address by configuring IEEE 802.1x authentication, the switch will not be aging. Regardless of the device is connected to the switch port happen to the MAC address table MAC address and port corresponding relationship always will not change, the relationship is completely controlled by the IEEE 802.1X authentication server. Static MAC address after the switch is powered restart will disappear.
- Permanent static MAC addresses
  permanent MAC address generated through configuration will not be aging, regardless of the device is connected switches of the change of the port, the MAC address table of MAC address and port of corresponding relation is always does not change, permanent MAC address does not disappear after the switch is restart

MAC address table can specify the sort type, can choose "auto" and "MAC" two sort types, MAC address and related forwarding port will be showed in this table. if the status bar displays "certification"，shows MAC address static certification that is not aging treatment, if displays “static” means that MAC address is a permanent static address that is not aging treatment.

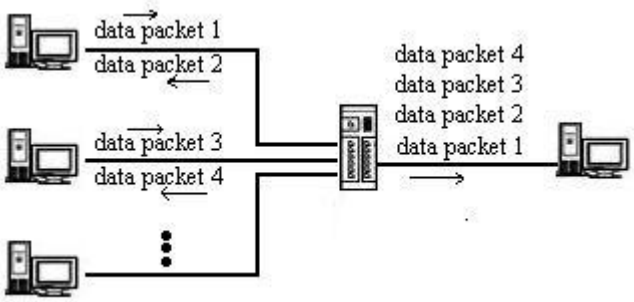
Notes:

- The address of the device index according to switch's address, so all MAC address displayed VLAN value is 0.
- Permanent static address configured in the previous static MAC address port list, need to modify the corresponding item when port changed.
- Multicast address list displays the IGMP snooping item, in the address list here all unicast address.
- MAC address aging time is 300 seconds, the port is disconnected our parent program to clear all the corresponding port items.

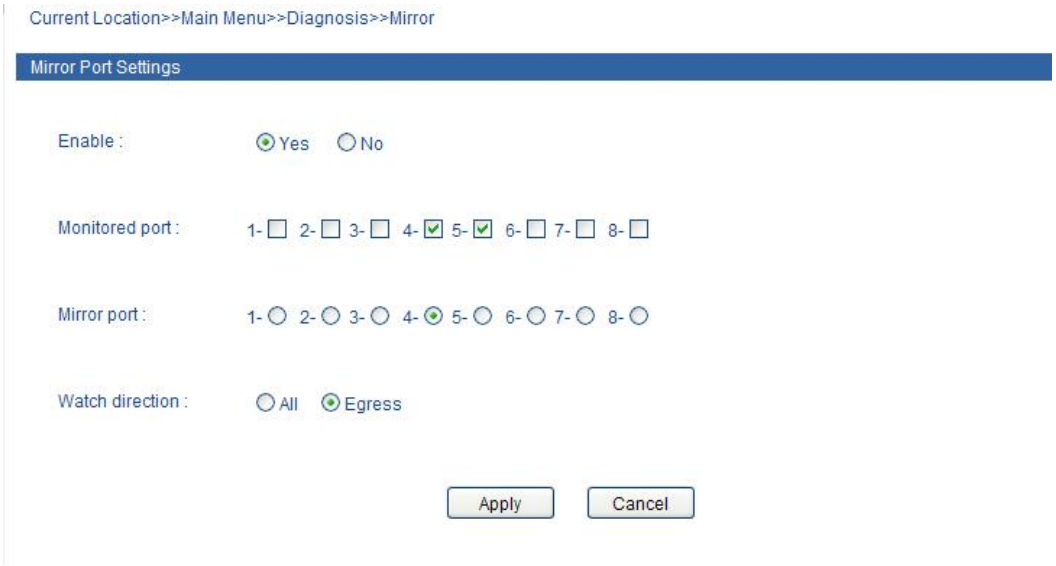
12 Network Diagnosis

12.1 Port mirroring

Port mirroring refers to copy data from the port which need to be monitored to appointed monitoring port for analysis and monitoring. Ethernet switch supports many-for-one mirror which means messages from several ports can be copied to a monitored port. User can appoint the direction of monitored message, such as only monitoring of transmitted messages of appointed port. The device configures port mirroring function through port mirroring group. Each group includes a monitored port and a group of mirror ports. Total bandwidth of mirroring is not more than that of monitored port. It is good to monitor and manage its internal network data when using port mirroring in a company. It is also good to locate the failure when network is cut up.



Example as figure below: Port 4 collects all of the data from port 4 and port 5



Note:

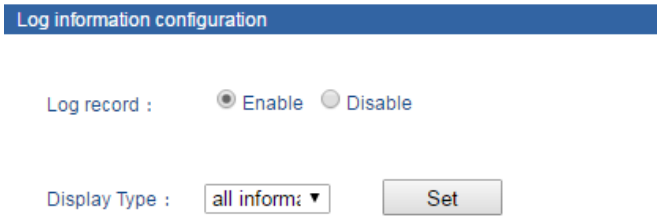
- This function is not often used. Otherwise other port-based higher management function like RSTP,IGMP SNOOPING
- Port mirroring function can only deal with the normal FCS packets. It cannot deal with error data frames.

13 Basic settings

13.1 Log information

The device provides system log for user's reference of troubles. When enabling this function, the following events will be recorded:

The all information, boot information, handing information, linkage information.



13.2 SNTP

NTP (Network Time Protocol) is a protocol and software implementation for synchronizing the clocks of computer systems over packet-switched data network. It provides coordinated universal time including scheduled adjustments. No information about time zones or daylight saving time is transmitted; this information is outside its scope and it must be obtained separately.

Local Time

To configure the time by hand to undated the time of the device

Enable NTP

To update the time of the device by using NTP protocol

Time Zone

Standard time zones could be defined by geometrically subdividing the Earth's spheroid into 24 lines. The local time in neighboring zones would differ by one hour. And the variation in the position of the sun from one end of the zone to the other (east vs. west) would be at most 1/24 of the sky. Most of the 25 nautical time zones (specifically UTC−11 to UTC+11) are indeed defined this way, and are 15° of longitude wide. An hourly zone in the central Pacific Ocean is split into two 7.5°-wide zones (UTC±12) by the 180th meridian, part of which coincide with the International Date Line.

NTP Server

It provides host name or IP address of NTP timing.

System Time

Device time

PC Time

Visitor's own PC, display and switch itself does not matter.

Notes:

- NTP server can be empty, the device using the own server update, but must use the correct DNS and gateway.
- NTP server must have a valid host name or a valid IP address.
- Only the Administrators have permission to manually configure the device time.
- Time zones must be configured; either uses the "local time" or "NTP time.
- The configuration of the NTP server or PC can cause the display is not normal, you can change the time display format to adjust the display.

13.3 Device address

Device address

Device configuration support two modes, DHCP and static IP address, can get the device's IP address via client when the DHCP function is running, if you need NTP that need to connect internet, please enter the available and correct gateway and DNS address.

IP Address

IP address is a address of 32 bits length which is assigned to the device on the internet. The IP address consists of two fields: the network number field (net-id) and the Host ID field (host-id). For can conveniently manage IP address, IP addresses are divided into five categories.

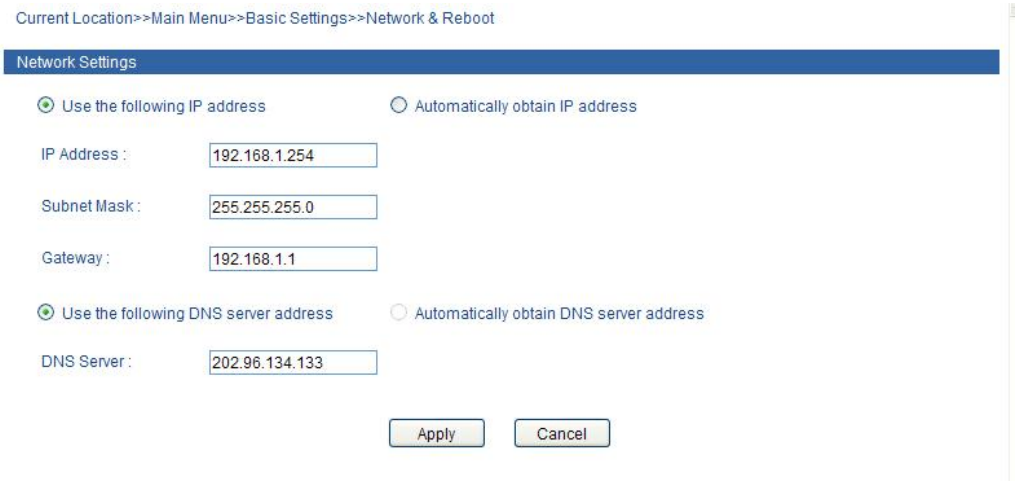
Subnet Mask

Mask is corresponding 32 bits number of IP address. Some are 1, the others are 0. These 1 and 0 can be combined arbitrary in principle, but the first continuous bits are 1 when designing subnet mask. IP address can be divided into 2 parts by subnet mask: subnet address and host address. 1 in IP address and subnet corresponds to subnet address, other bits are host address. A type of address corresponding mask is 255.0.0.0; mask of B type address is 255.255.0.0; mask of C type address is 255.255.255.0.

Default Gateway

Default gateway in the host PC is generally called default route. Default route refer to a kind of router that destination address of IP data packet will choose when it

don't find other existing route. All data packets of destination address which don't exist in the list of router will choose default route.



Device reboot

Can reboot the switch remote. Knock [Basic settings & Logout] menu, Enter into reboot interface, figure as shown below.

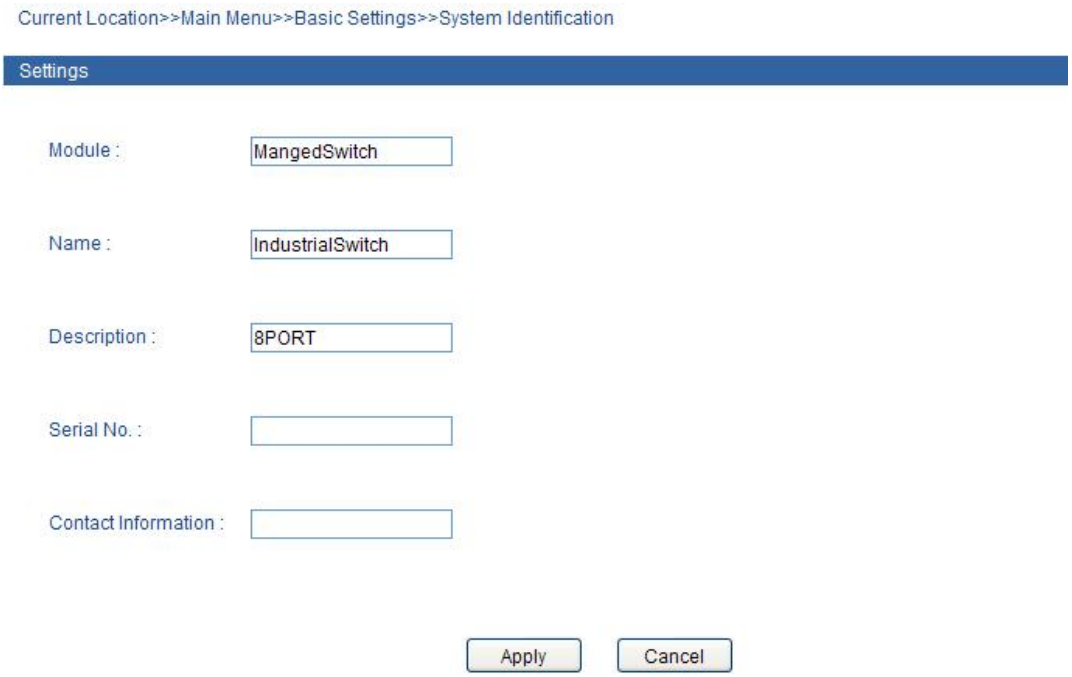
Knock<OK> button, after confirmation, device will be logout. After 20 seconds, know menu bar and back to WEB manged login interface.

Notes:

Before reboot, please save all configurations. Otherwise, all configuration will be lost.

13.4 System identification

In System Identification interface we can see Model, Name, Description, Serial NO., and Contact Information. We can modify these above items by this function. It will take effect after system reboot. Figure below is initial device settings of Switch.



Name

To give a name to each device, length is not more than 16 bytes.

Description

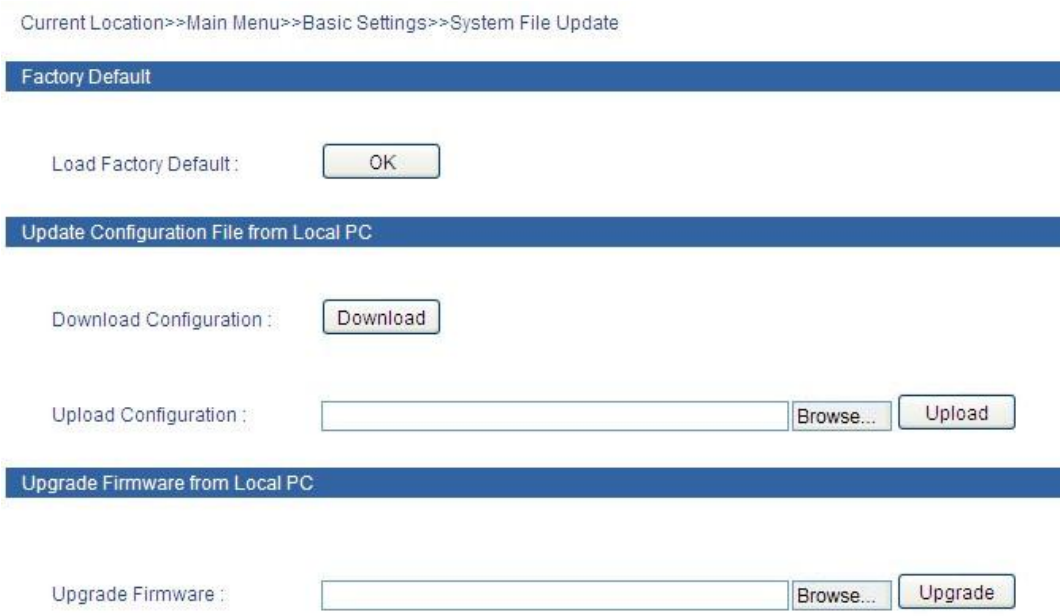
A brief description to a device, the length is not more than 16 bytes.

Serial No.

Display Installation Location of the device, the length is not more than 30 bytes.

13.5 System File Upgrade

The menu included 4 functions: Factory default, Download Configuration, upload configuration, upgrade firmware.



1. Factory Default

If you know the IP address of the device, user name and password:

Step 1 Use IE to login Web interface.

Step 2 Click "System Management"

Step 3 Click "System File Update"

Step 4 Choose "Factory Default"

Step 5 Click "OK"

Notice:

the IP address will be "192.168.1.254".

Open a new interface, input "192.168.1.254" to make a new configuration.

2. Download Configuration

If you know the IP address of the device, user name and password:

Step 1 Use IE to login Web interface.

Step 2 Click "System Management"

Step 3 Click "System File Update"

Step 4 Choose "Download Configuration"

Step 5 Click "Download"

Step 6 Choose the name of the file and the place to save.

3. Upload Configuration

If you know the IP address of the device, user name and password:

Step 1 Use IE to login Web interface.

Step 2 Click "System Management"

Step 3 Click "System File Update"

Step 4 Choose "Upload Configuration"

Step 5 Click "Upload"

4. Upgrade Firmware

If you know the IP address of the device, user name and password:

Step 1 Use IE to login Web interface.

Step 2 Click "System Management"

Step 3 Click "System File Update"

Step 4 Choose "Upgrade Firmware"

Step 5 Click "Browse" and find the place of uploading the file.

Step 6 Click "Upgrade"

A suggestion" interruption of power is not allowed during uploading", confirm it.

Notes:

- Load factory default will result in all status be in factory default settings, the IP could be static IP address "192.168.1.254".
- Upload the configuration file, in the new configuration if static IP is not in the same network segment, the website will not be opened.
- Use dynamic IP settings, but there is no DHCP server on the network segment, that will result in the relevant part of the IP will not be updated in the new configuration when upload configuration.

13.6 System logout

Knock<OK> button, after confirmation, device will be logout. After 20 seconds, know menu bar and back to WEB manged login interface.

14 FAQ

14.1 Sign in Problems

1. **Why the webpage display abnormally when browsing the configuration via WEB?**
   Before access the WEB, please eliminate IE cache buffer and cookies. Otherwise, the webpage will display abnormally.

2. **How about forget the login password?**
   For forgetting the login password, the password can be initialized by restoring factory setting, specific method is adopt BlueEyes_Ⅱ software to search and use restore factory setting function to initialize the password.

3. **Is configuring via WEB browser same to configuring via BlueEyes_Ⅱ software?**
   Both configurations are the same, without conflict.

14.2 Configuration Problem

1. **How to configure the device restore default setting via DIP switch?**
   Turn the DIP switch 2 to ON position, and restore default setting after power on again.

2. **Why the bandwidth can't be increased after configure Trunking (port aggregation) function?**

Check whether the port attributes set to Trunking are consistent, such as rate, duplex mode, VLAN and other attributes.

3. **What's the difference between RING V2 and RING V3?**
   RING V2 and RING V3 are our company's ring patents. RING V2 only supports single ring and coupling ring. RING V3 supports single ring, coupling ring, chain and Dual_homing, and Hello_Time can be set to detect port connection status.

4. **How to deal with the problem that part of switch ports are impassable?**
   When some ports on the switch are impassable, it may be network cable, network adapter and switch port faults. User can locate the faults via following tests:
   - Connected computer and switch ports keep invariant, change other network cable;
   - Connected network cable and switch port keep invariant, change other computers;
   - Connected network cable and computer keep invariant, change other switch port;
   - If the switch port faults are confirmed, please contact supplier for maintenance.

5. **How about the order of port self-adaption state detection?**
   The port self-adaption state detection is conducted according to following order: 1000Mbps full duplex, 100Mbps full duplex, 100Mbps half-duplex, 10Mbps full duplex, 10Mbps half-duplex, detect in order from high to low, connect automatically in supported highest speed.

14.3 Alarm Problem

1. **When the device alarms, except BlueEyes_II software nether alarm information display area will display alarm information, is there any other way to notify technical staffs?**
   When the device alarms, monitoring host computer buzzer will continue to emit alarm sounds.

14.4 Indicator Problem

1. **Power indicator isn't bright, what's the reason?**

   Possible reasons include:

   - Not connected to the power socket; troubleshooting, connected to the power socket.
   - Power supply or indicators faults; troubleshooting, change the power supply or device test.
   - Power supply voltage can't meet the device requirements; troubleshooting, configure the power supply voltage according to the device manual.

2. **Link/Act indicator isn't bright, what's the reason?**

   Possible reasons include:

   - The network cable portion of Ethernet copper port is disconnected or bad contact; troubleshooting, connect the network cable again.
   - Ethernet terminal device or network card works abnormally; troubleshooting, eliminate the terminal device fault.
   - Not connected to the power socket; troubleshooting, connected to the power socket.
   - Interface rate doesn't match the pattern; troubleshooting, examine whether the device transmission speed matches the duplex mode.

3. **Ethernet copper port and fiber port indicator are connected normally, but can't transmit data, what's the reason?**

   When the system is power on or network configuration changes, the device and switch configuration in the network will need some time. Troubleshooting, after the device and switch configuration are completed, Ethernet data can be transmitted; if it's impassable, power off the system, and power on again.

4. **The switch halts after communicate for a period time, and returns to normal after reboot, what's the reason?**

   Reasons may include:

   - Surrounding environment disturbs the product; troubleshooting, product grounding adopts shielding line or shields the interference source.

- Site wiring is not normative; Troubleshooting, optical fiber, network cable, optical cable cannot be arranged with power line and high-voltage line.
- Network cable is disturbed by static electricity or surge; Troubleshooting, change the shielded cable or install a lightning protector.
- High and low temperature influence; troubleshooting, check the device temperature usage range.

15 Maintenance and Service

Since the date of product delivery, our company provides five-year product warranty. According to our company's product specification, during the warranty period, if the product exists any failure or functional operation fails, our company will be free to repair or replace the product. However, the commitments above do not cover damage caused by improper usage, accident, natural disaster, incorrect operation or improper installation.

In order to ensure that consumers benefit from our company's managed switch products, consumers can get help and solutions in the following ways:

- Internet service;
- Call technical support office;
- Product repair or replacement;

15.1 Internet Service

More useful information and tips are available via our company website. Website: http://www.3onedata.com

15.2 Service Hotline

Users using our company products can call technical support office. Our company has professional technical engineers to answer the questions and help solve the products or usage problems ASAP. Free service hotline: **+86-400-880-4496**

15.3 Product Repair or Replacement

As for the product repair, replacement or return, customers should firstly confirm with the company technical staff, and then contact the company salesmen and solve the problem. According to the company's handling procedure, customers should negotiate with our company's technical staff and salesmen to complete the product maintenance, replacement or return.

3onedata
Make network communication more reliable

3onedata Co., Ltd.

Headquarter address: 3/B, Zone 1, Baiwangxin High Technology Industrial Park, Song Bai Road, Nanshan District, Shenzhen

Technology support: tech-support@3onedata.com

Service hotline: +86-400-880-4496

Official Website: http://www.3onedata.com