Henrich Managed Ethernet Switches
User's Manual

Second Edition, April 2013

www.henrich-inc.com

Information Coding:M008120424
Version: V1.1
Product version: all
Product Name: Managed Industrial Ethernet Switches on DIN Rail and Rack.
Applicable to: Technical Support

Attention:

This document will be updated on regular bases due to version upgrades or other requirements.

Unless otherwise agreed on, this document is only to be used as a guide and not for warranty purposes.

Definition of signs:

⚠ **Danger:** It is of high potential danger. If not avoided; it will cause death or serious injury.

⚠ **Warning:** It is moderate and low level of danger. If not avoided, it will cause minor or moderate injury.

⚠ **Attention:** Potential risk exists, if neglected it is possible that the equipment will be damaged, data will be lost, equipment performance can be reduced or unpredictable results may occur.

🔑 **Tip:** It can provide you with solutions and minimize the amount of time spent on troubleshooting.

📖 **Appendix:** Additional information that can provide you with further details.

Table of Contents

T

1

Chapter One Preface

The managed switch products are designed and developed for industrial communication, to ensure reliability, stability and real time of industrial Ethernet environment, and functions well in severe rugged environments. It supports redundancy power input and a wide temperature range of DC and AC power input to meet the requirements of complex power in an industrial environment. The level of protection is IP30, which can meet the requirements of Industrial Level 4 of electromagnetic environment, provides DIN rail or 19’ chassis installation and supports a wide temperature range of (-40℃-85℃), it’s a high-end industrial Ethernet communication solution applied in severe rugged environments.

Our managed switches integrate the function of plug-and-play management, and all ports support auto-negotiation, 10/100Mbps half-duplex and full duplex, flow control, Auto-MDIX, etc. It is convenient and quick to deploy and manage switches using serial ports, Web Management, GUI SNMP. Senior management functions include a series of common senior functions: Ring redundancy, STP/RSTP, VLAN, Trunking, Quality of Service, IGMP Snooping, Rate Control, Port Mirroring, Static MAC Address Transmit List, SNMP (Simple Network Management Protocol), Diagnostic Function, Email /Replay Breakdown Warning and Software On-line Upgrading, etc.

Private Ring technology is designed and developed for industry, (opto/electrical)100 M and1 GB port are used to assemble ring, provides functions of self-recovery after Ethernet disconnects , the interval is less than 15 seconds, enjoy independent intellectual property rights, possess leading technology in the field.

Before you operate any of our switches, please read this user manual carefully.

2

Chapter Two Feature

Industrial Internet Performance:

- Provides 2, 4 Gigabit RJ45/SFP Combo Ports
- Link redundancy self-restoring technology based on ring technology
- Built in Web server, remote management and configuration through a browser Trunking
- Real-time Broadcast Storm Detection and Control
- On-line Firmware Update
- Support IGMP snooping and GMRP, multicast flow
- Maximum 6 100Base-FX optical interface, Support different transmission distance and different types of fiber optic interfaces
- Store and forward mode, back bandwidth is 8.8Gbps
- 10/100/1000M, full-half duplex MDI/MDIX self-adjust mode
- Full duplex flow control and half duplex backpressure flow control
- Port VLAN and IEEE802.1Q VLAN
- Support QoS IEEE802.1p and TOS/DiffServe with four priority queues, improve communication quality
- Support SNMP V1/V2/V3, different levels of Internet Management
- Redundant dual power input, meet the requirements of high reliability
- Function well in the environment of strong electromagnetic interference
- Support REMON, effective remote data monitoring and predictive capacity
- 8K MAC addresses with automatic learning and aging 4K-entry Multicast Address table
- LLDP Link Layer Discovery Protocol

Industrial Application Design

- Redundant dual power input design
- DIN rail or Wall-mounting or cabinet 19’’
- Passive cooling (without FAN)
- Support both AC and DC power input and power LED indicator
- Bandwidth Management to prevent unpredictable network problems
- System set parameter backup and restore
- User friendly graphical interface, instantly recover factory
- Port mirroring is for on-line diagnostics
- Support POE af/at standard: max 8 ports
- Effective Network Diagnostic Tool
- Work temperature:-40C~85C
- Automatic Warning Device based on E-mail and Relay
- Classic IP30 protection
- Work huimidity:5%~95%
- Console port with RS-232 or RJ-45
- Switch power off can still work 30s
- Integrated Digital Signal Input
- Fast recovery by changing port connections
- Network Real Time Synchronization
- Limit Accessible IP, manage switches in network

Remote Management Settings

- Set and manage by Web page, console program and Windows Application Program
- Support standard SNMP protocol

3

Chapter Three Packing List

The packing list of our products is as follows:

If any of the following items are missing or damaged, please feel free to contact your sales agent or our Customer Care Centre, who will be happy to assist you with a solution or a replacement.

Before you operate any of the product families, please be sure to read this user manual carefully

Item	Quantity
Managed Switch	1
User Manual	1
Quick Start	1
RS232 serial cable	1
Link plate (selected accessory, excluded in standard layout)	1

4

Chapter Four Performance & Specification

The managed switches that we have provided you with can complete the Ethernet information exchange only when the following steps are followed.

This information can offer you the requirements for a successful network information exchange.

Description

Certification: CE, FCC, EN55022, EN55024, Class B, CFR47, P15, Class A

Standard: IEEE802.3, 802.3u, 802.3x, 802.1D, 802.1w, 802.1Q, 802.3ad LACP

Protocol: IGMP Snooping , GMRP , SNMPv1/v2c/v3 , DHCP Client , HTTP , HTTPS , NTP ClientInterface: RJ45 10/100Mbps, RS232 DB9 port, 4-foot power input connector (AC and DC), 2-foot relay Warning Input connector

Serial No. of Din-rail: TS-35

5

How to Set Managed Series of Switch

The managed switch products can be accessed, set, and managed through the Web. The web can be sued to set or change the IP address for the switches using Hyper Terminal on the connected PC.

5.1 Setting up the IP address for a managed switches through Hyper Terminal

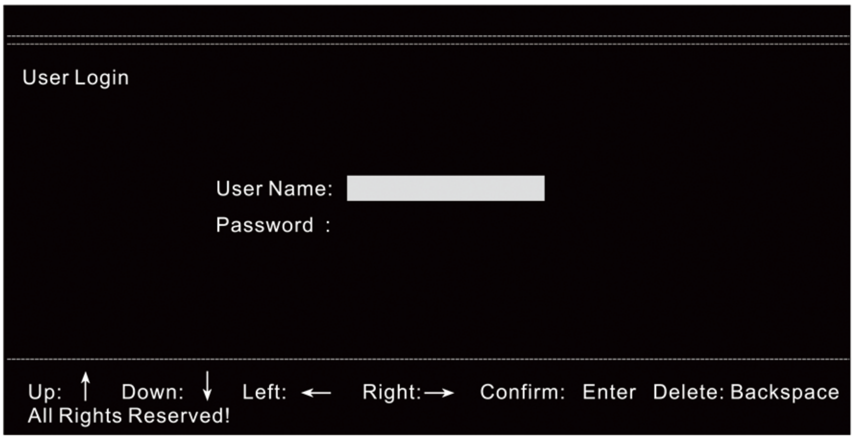
Firstly, please make sure the managed switches are connected via a serial cable through the PC's serial ports.

Next, open Hyper Terminal from the computer: **Start → programs → Accessories → Communication → HyperTerminal**. Once you have opened Hyper Terminal, you need to create a new connection, select the communication port to the switch, and use the following parameter:

Baud Rate: 115200 Data Bits: 8 Parity: None Stop Bits: 1 Flow Control: None

5.1.1 User Name and Password

When HyperTerminal finish setting, you can see the page display as below :



```
User Login

                User Name:
                Password  :

Up: ↑   Down: ↓   Left: ←    Right:→    Confirm:  Enter  Delete: Backspace
All Rights Reserved!
```

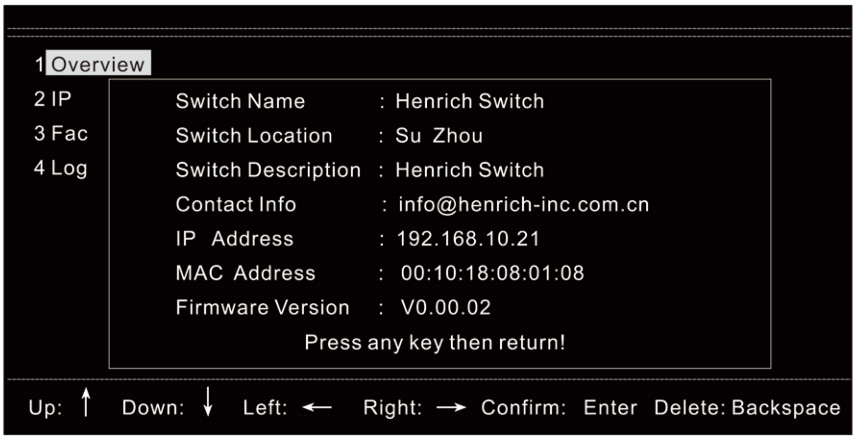
Enter User Name and Password, the default User Name and Password as "**admin**", then press "**Enter**", go into Console Program.

5.1.2 Console Menu

Console menu includes the following:

1. Overview	View basic information
2. IP setting (support IP address)	Obtain an address automatically (DHCP) or use affixed IP address
3. Factory default (restore factory default)	Restore factory default
4. Logout	Logout

Shift “↑” arrow or “↓” arrow or press “**Enter**” to go into sub-function modules.

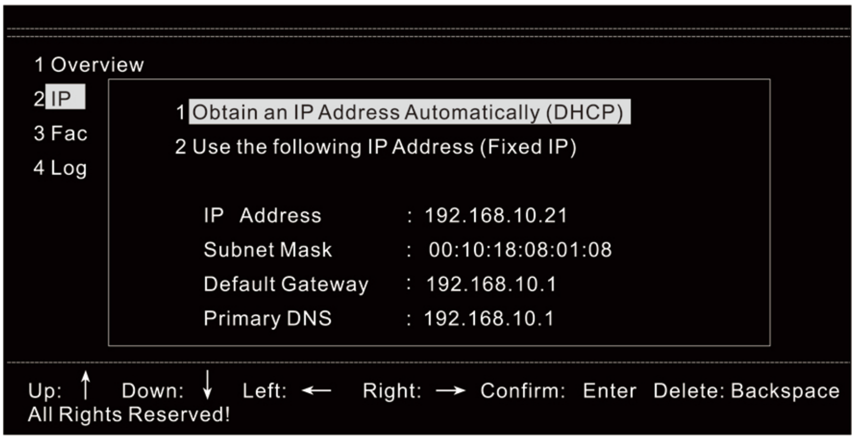


```
1 Overview
2 IP        Switch Name        : Henrich Switch
3 Fac       Switch Location    : Su  Zhou
4 Log       Switch Description : Henrich Switch
            Contact Info       : info@henrich-inc.com.cn
            IP  Address        : 192.168.10.21
            MAC  Address       :  00:10:18:08:01:08
            Firmware Version   :  V0.00.02
                       Press any key then return!

Up: ↑   Down: ↓   Left: ←   Right: →   Confirm:  Enter   Delete: Backspace
```

5.1.3 Overview

In “**Overview**”, you can see some basic information in this sub-option, Switch Name, for example: Switch Location, Switch Description, Contact Information, IP Address, MAC Address, Firmware Version, etc. Details are in the following page:



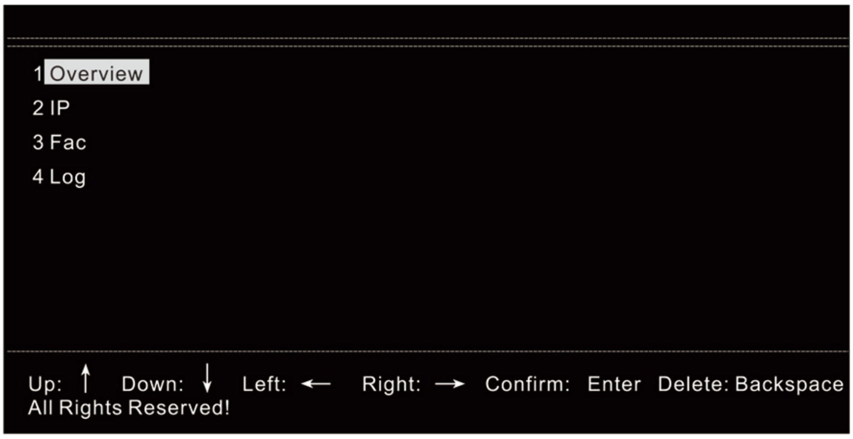
```
1 Overview
2 IP
3 Fac       1 Obtain an IP Address Automatically (DHCP)
4 Log       2 Use the following IP Address (Fixed IP)

                IP  Address       :  192.168.10.21
                Subnet Mask       :   00:10:18:08:01:08
                Default Gateway   :  192.168.10.1
                Primary DNS       :  192.168.10.1

Up: ↑   Down: ↓   Left: ←   Right: →   Confirm:  Enter   Delete: Backspace
All Rights Reserved!
```

5.1.4 Settings

When setting the IP Address through the Console Program, select “**IP settings**”, the following page prompts. This page allows to set a new IP address. When selecting “**Obtain an IP address automatically (DHCP)**”, the switch obtains an IP Address automatically through DHCP. When selecting “**Use the following IP Address (fixed IP), IP address, Sub-net Mask, Default Gateway, DNS can be edited to get a fixed address**”. When IP Address is set, you can access the Web page through this IP address.



```
1 Overview
2 IP
3 Fac
4 Log

Up: ↑   Down: ↓   Left: ←   Right: →   Confirm: Enter   Delete: Backspace
All Rights Reserved!
```

5.1.5 Restore Factory Default

This function will restore all configuration parameters to factory default.

5.1.6 Logout Console Program

This function will exit the management series switch from console program.

5.2 How to setup the IP address of Switches by changing the IP address of the PC

To access the series of switches through the Web, the IP for switch and the PC must be in the same domain network.

Please refer to the following steps.

Start → Control Panel → Network Connection → Local Network → Property → Internet Protocol (TCP/IP)

The default IP address for managed switches is 192.168.118.100. Set the IP address of the PC to 192.168.118.X (X can be any value from 2 to 254 except 100).

After changing the IP address of the PC, use the default IP address of 192.168.118.100, to access the switches through Web and set the related items.

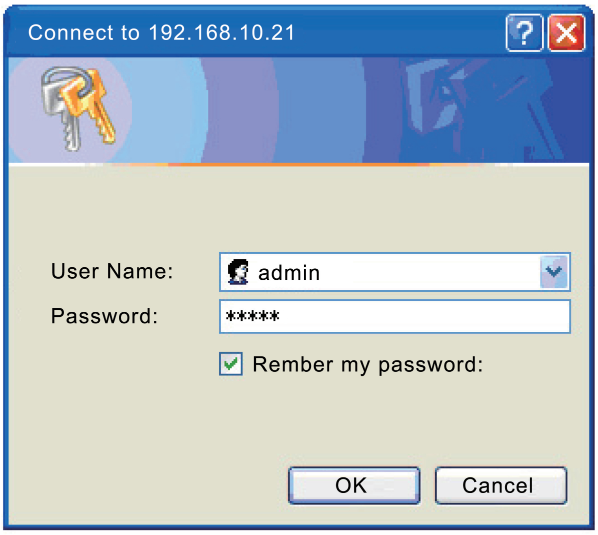
6

Web Management Function

The Webserver is an effective way to access and set up your managed switch products. You can manage, monitor, edit and set up your managed switch products through the Web page conveniently. Users can use the Internet or other browser to access the serials of the managed switches. If you wish to do so, please open a browser and enter in the address bar the switch IP address, for example: **http://192.168.118.100** once you have done so, please press "**Enter**".

6.1 How to login to the Webserver

Once you have completed the above the following window will appear and you are to type in your User Name and Password. Please note that the default IP address is "**admin**". Please be sure of your User Name and Password as the switches will only accept 3 tries and after your third try, you will receive a display error with the following "**401 Unauthorized**". Input correct User Name and Password login to Webserver and we recommend you to change User Name and Password. If you encounter more problems, please feel free t



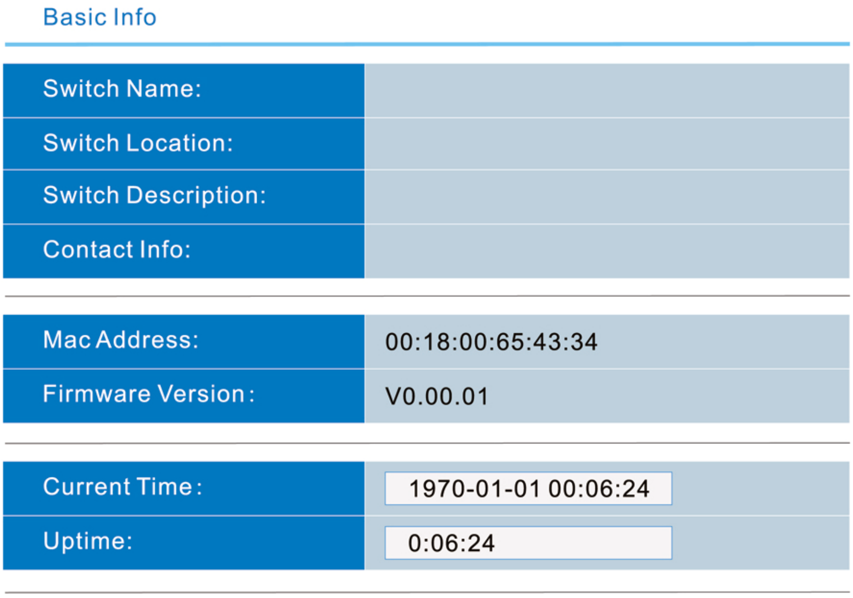
Connect to 192.168.10.21

User Name: admin

Password: *****

☑ Rember my password:

6.2 Basic Information



Basic Info

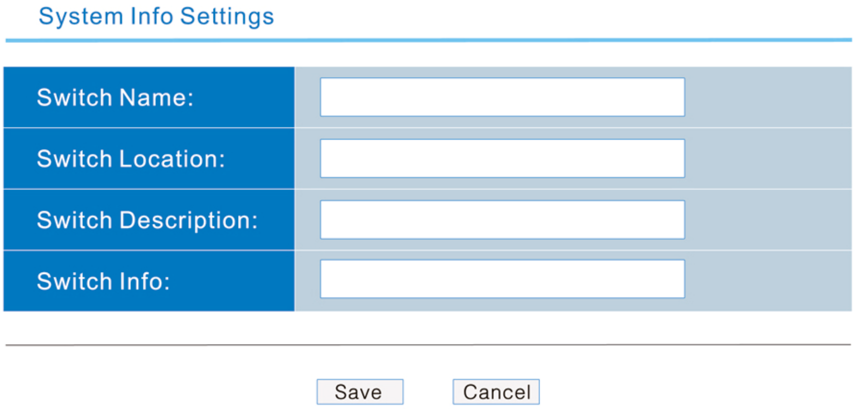
Switch Name:	
Switch Location:	
Switch Description:	
Contact Info:	
Mac Address:	00:18:00:65:43:34
Firmware Version :	V0.00.01
Current Time :	1970-01-01 00:06:24
Uptime:	0:06:24

- Switch Name: Please setup a different name for each switch to distinguish the difference between them
- Switch Location: Describe the location of switches installed; the maximum length is 64 bytes
- Switch Description: Describe the summary of switches which can be searched through SNMP
- Contact Info: Display contact info for a technical support representative that can be contacted immediately if any issues occur.
- MAC Address: MAC Address of Network Nodes
- Firmware Version: The current firmware of the switch at the time of installation.
- Current Time: Current local time and date
- Up Time: The running time is counting from switches "power-on, when they are reset or Power-off and restart, time will count from zero".

6.3 Basic Info Setting

The basic info setting includes: **System Info Setting, User Name and Password setting, switches accessible IP Address setting, port setting, switches IP Address setting, time setting**. Through convenient Web management, it's easy to find related setting page, this manual will introduce how to operate managed serials of switches one by one.

6.3.1 System Info



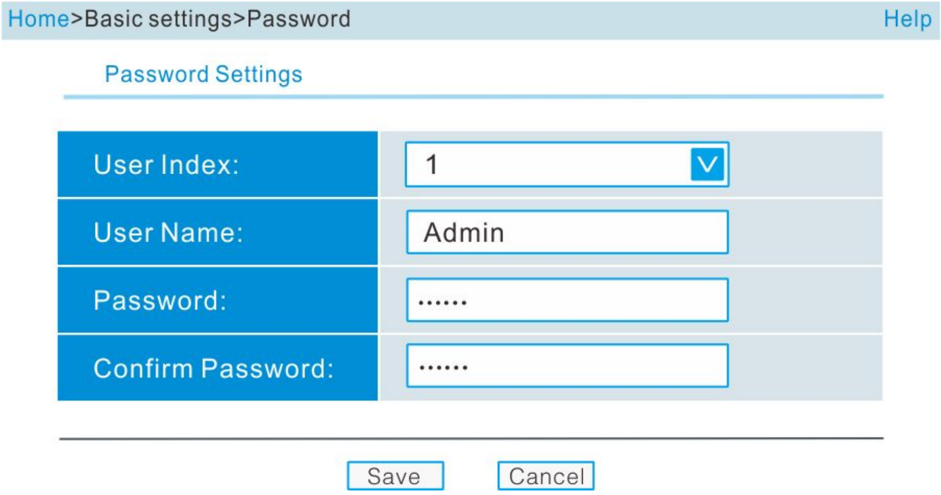
System Info Settings

Switch Name:	
Switch Location:	
Switch Description:	
Switch Info:	

- Switch Name: Give a different name for each switch to distinguish each one, support Chines input, switch name allows a maximum length of 64 bytes.
- Switch Location: Describe the location of switches installed; support Chines input, the maximum length is 64bytes.
- Switch Description: Describe the summary of switches which can be searched through SNMP. The maximum length is 64bytes.
- Contact Info: Display contact info for technical support so that users can contact hem immediately if any issue occurs. The maximum length is 64bytes.
- After finishing inputting info, click on "**Save**" to save info.

6.3.2 User Name and Password

Webserver of Managed serials of switches provides 3 different sets of User Name and Password to manage managed serials of switches. User Name and Password can be added, deleted, and modified through modifying User Index. If user name and password are empty, delete the user name and password this index represents. When the switches leave the factory the default User Name and Password is set as “**admin**”. As a rule, User Name and Password must be legal, User Name and Password can be empty, and whose maximum length is 32 bytes. If the current User Name and Password is changed and different from the original one, when you access again, Web page will prompt you to re-enter User Name and Password.



Home>Basic settings>Password

Password Settings

User Index:	1
User Name:	Admin
Password:	······
Confirm Password:	······

- User Index: Represent a group of users. There are three user indexes in the drop-down list box
- User Name: User Name (maximum length is 32 bytes).
- Password: User Password (maximum length is 32 bytes)
- Confirm Password: Confirm the password to prevent password from inputting incorrectly

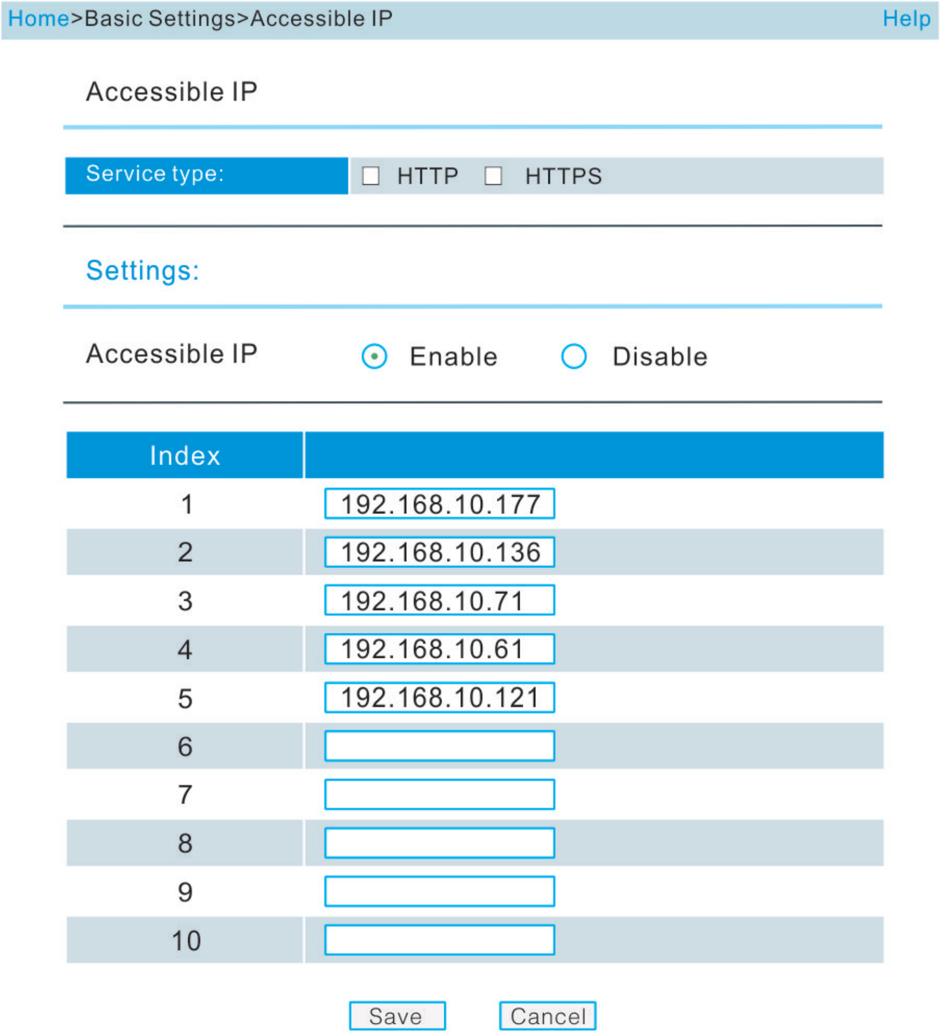
6.3.3 Accessible IP settings

Service type is a connection way from user’s PC to the switches.

Hyper Text Transfer Protocol (HTTP) is a communication protocol used to transfer information in worldwide Web (www). It’s a request response protocol between client and server. When the server receives the request, it will reply according to corresponding request, for example HTTP1.1 200 OK, the response may be a message, a file, an error message and other related information.

HTTPS is a safe HTTP connection. In the establishment of access connection, it’s similar to HTTP, for example: http://url , while the difference is that HTTPS use https://url to establish a more secure access connection. HTTPS use default port t 443, Encryption and authentication layer is used between HTTP and TCP protocol to establish a more secure mechanism. HTTPS is originally designed and developed by Netscape Communications Corporation, later used in WAN, mainly in some of the industry and institution with higher communication security requirements.

From a security perspective, it is recommended to use HTTPS to access HTTPS use https://url to access while HTTP use http://url . Next, have a look at the following page:



Accessible IP

Service type: □ HTTP □ HTTPS

Settings:

Accessible IP ◉ Enable ○ Disable

Index	
1	192.168.10.177
2	192.168.10.136
3	192.168.10.71
4	192.168.10.61
5	192.168.10.121
6	
7	
8	
9	
10	

Access Control proves an advance communication filtering function. The filter function is used as an integral part of the firewall. A firewall is usually a network device to control access to network resources. Firewall should be connected to entry port of the LAN. When this function is enabled, only the computer whose IP Address is assigned can access to the switches.

6.3.4 Port Setting

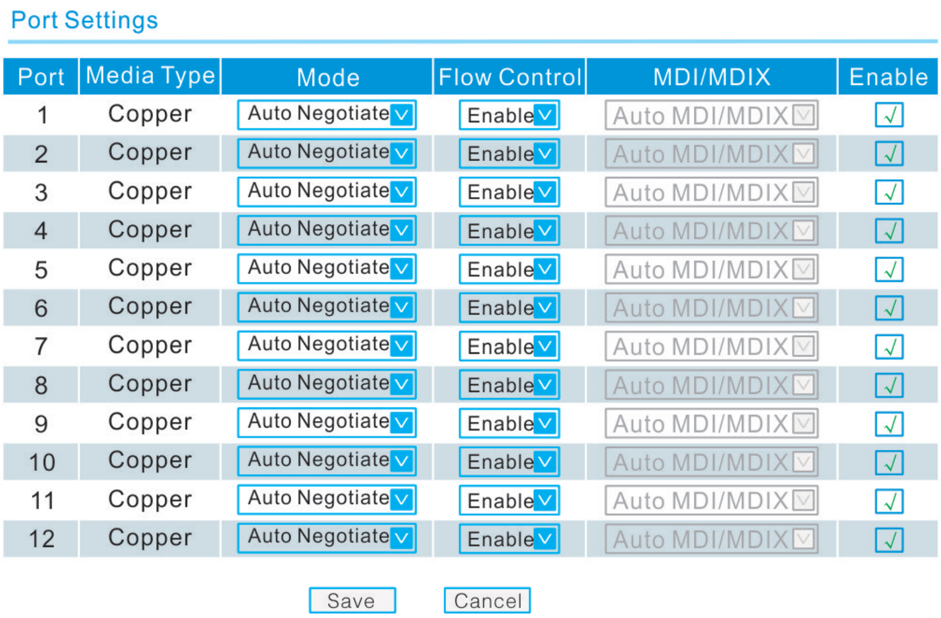
- Media Type: The media type of each communication port, for example, copper or optical port
- Mode: Include Auto-negotiation, 100Mbps full-duplex, 100Mbps half-duplex, 10Mbps full-duplex, 10Mbps half –duplex
- Auto-negotiate: Allow communication port to use IEEE 802.3u Protocol and connected devices to negotiate, the negotiation result will choose the best rate to communicate.
- 100M-Full, 100M-Half, 10M-Full, 10M-Half: Fixed communication rate and duplex modes options
- Flow Control: In computer networks, flow control is used to handle the data transfer rate between the two transmission nodes. When the data flow is blocked, the flow control mechanism is quite obvious which can be enabled or disabled
- MDI/MDIX: MDI (Medium Dependent Interface), MDIX ("X" means cross-line), it's a connection mode from Ethernet port to Router, HUB and Switches. This series of switches only use Auto-MDI/MDIX, with auto-flip function.

For port settings, please see the following form:

Item	Description	Default
Media Type	Media port type, copper or optical	Copper
Mode	Transmission mode between 2 nodes	Auto Negotiate
Flow Control	Data Transmission Management	Enable
MDI/MDIX	Connection type for media interface	Auto MDI/MDIX
Enable	Enable port settings	Enable

Webserver of managed serials switches provide Web page as below to set port. Each item option can select parameters from pull-down list.

All settings parameters will be enabled after clicking '**Save**".

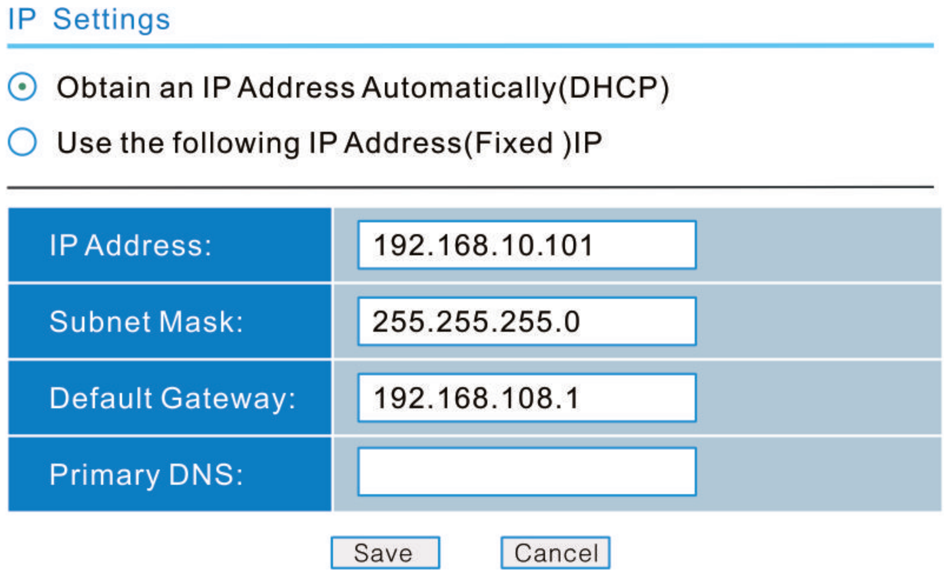


Port Settings

Port	Media Type	Mode	Flow Control	MDI/MDIX	Enable
1	Copper	Auto Negotiate	Enable	Auto MDI/MDIX	☑
2	Copper	Auto Negotiate	Enable	Auto MDI/MDIX	☑
3	Copper	Auto Negotiate	Enable	Auto MDI/MDIX	☑
4	Copper	Auto Negotiate	Enable	Auto MDI/MDIX	☑
5	Copper	Auto Negotiate	Enable	Auto MDI/MDIX	☑
6	Copper	Auto Negotiate	Enable	Auto MDI/MDIX	☑
7	Copper	Auto Negotiate	Enable	Auto MDI/MDIX	☑
8	Copper	Auto Negotiate	Enable	Auto MDI/MDIX	☑
9	Copper	Auto Negotiate	Enable	Auto MDI/MDIX	☑
10	Copper	Auto Negotiate	Enable	Auto MDI/MDIX	☑
11	Copper	Auto Negotiate	Enable	Auto MDI/MDIX	☑
12	Copper	Auto Negotiate	Enable	Auto MDI/MDIX	☑

6.3.5 IP Settings

This function will assign a managed IP Address for the switches. There are two options that can be used to set Ethernet managed switch: automatic assign (DHCP) and Fixed (Static) IP Address. Managed series of switches default fixed IP address when they leave the factor. Automatically assign (DHCP): Switches automatically obtain IP Address, Sub-net Mask, Gateway and DNS Address from DHCP Server in network.



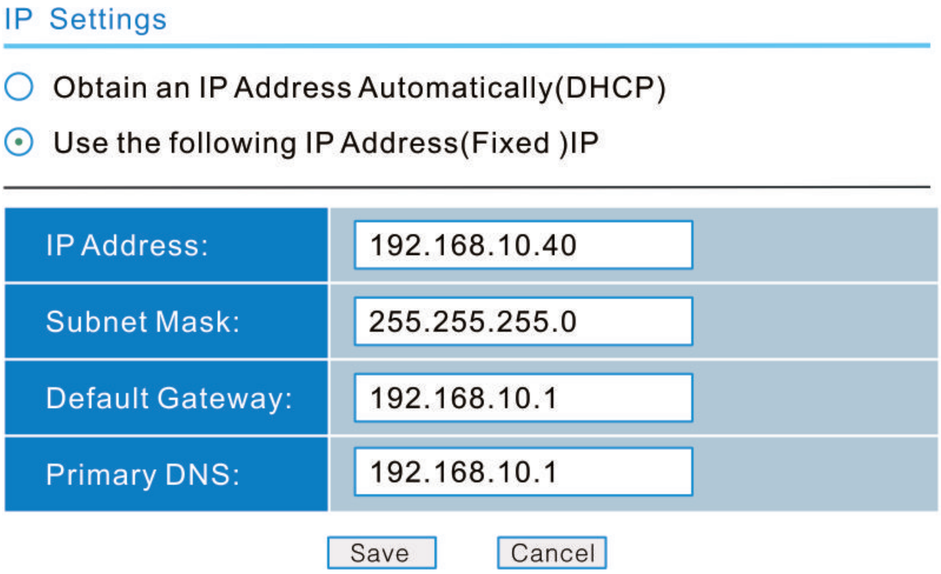
IP Settings

● Obtain an IP Address Automatically(DHCP)

○ Use the following IP Address(Fixed)IP

IP Address:	192.168.10.101
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.108.1
Primary DNS:	

Assign a IP Address: Can set a IP Address, DSun-net Mask, Gateway and DNS Address.



IP Settings

○ Obtain an IP Address Automatically(DHCP)

● Use the following IP Address(Fixed)IP

IP Address:	192.168.10.40
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.10.1
Primary DNS:	192.168.10.1

The form as below is parameters default set by IP:

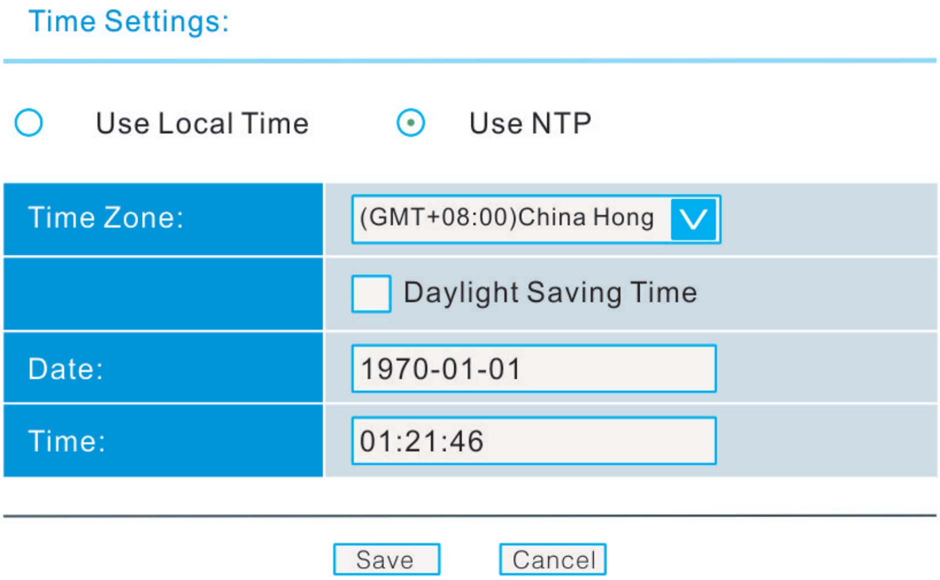
Item	Description	Default
DHCP/Fixed IP	Obtain an IP address automatically or assign a fixed IP	Assign fixed IP Address
IP Address	Only IP Address is network	192.168.118.100
Subnet Mask	Space range sub-net logical address use	255.255.255.0
Default Gateway	Network Node, reach a entry port of network	192.168.118.1
DNS	Domain Name System, IP Address for Domain Server	Name Empty

Assign or specify an IP Address for managed serials of switches through Web page or Console System. If you want to use E-mail Warning and NTP, it’s recommended to input DNS IP Address here. The witches can also obtain an IP Address through DHCP Server.

The settings below will not be enabled until you click “**Save**”.

6.3.6 Time Settings

In this section, we will tell you how to set Time Zone, Date and Time. The switches provide the following two options: Use Local Time and NTP (Network Time Protocol). Local time uses the switches internal clock while NTP (Network Time Protocol) is a Network Time Synchronization Protocol. NTP use UDP Protocol and 1234 Port, the use of which can be used to resist unstable network response time to set time.



Time Settings:

○ Use Local Time ● Use NTP

Time Zone:	(GMT+08:00)China Hong
	□ Daylight Saving Time
Date:	1970-01-01
Time:	01:21:46

If the switch you use currently has access to the Internet, it's recommended to use NTP to obtain accurate network time.

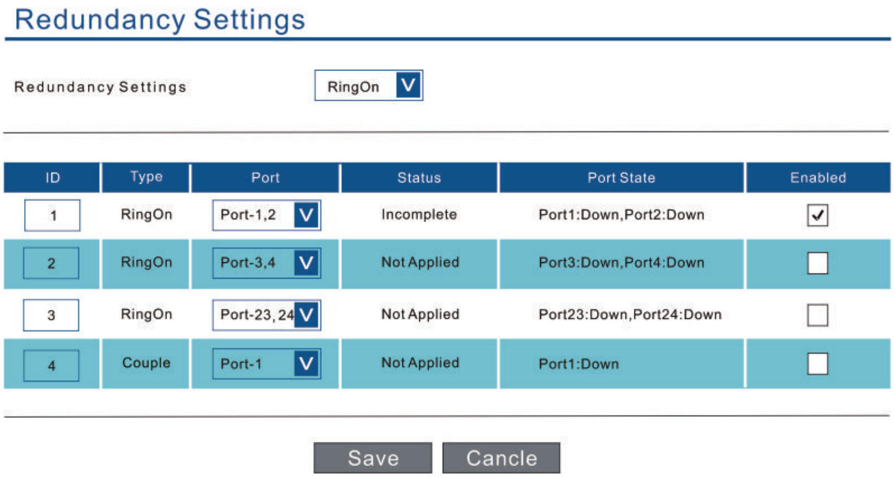
Item	Description	Default
Local Time/NTP	Two way to set switch time	Local Time
Time Zone	Time zone	GMT+8
Daylight Saving Time	Daylight Saving time	Disable
Data	The date format must be yyyy-mm-dd	1970-01-01
Time	The time format must be hh:mm:ss	00:00:00

6.4 Advanced Function Settings

Advanced function settings includes link redundancy function based on private Ring ON, VLAN, Truncking, QoS, IGMP, Snooping, Broadcast Storm Control, Bandwidth Management, Port Mirroring, Static Forwarding List.

6.4.1 Advanced Function Setting

Settings through advanced function includes: Link redundancy based on private ring, VLAN, Trunking, OoS, IGMP Snooping, Broadcast Storm Control , Bandwidth Management, Port Mirroring, Static Forwarding Table, etc.   Next, specify each function .



Redundancy Settings

Redundancy Settings: RingOn

ID	Type	Port	Status	Port State	Enabled
1	RingOn	Port-1,2	Incomplete	Port1:Down,Port2:Down	☑
2	RingOn	Port-3,4	Not Applied	Port3:Down,Port4:Down	□
3	RingOn	Port-23, 24	Not Applied	Port23:Down,Port24:Down	□
4	Couple	Port-1	Not Applied	Port1:Down	□

In Redundancy Setting, you can select from Disable, RingON, and RSTP.

- Disable: No RingOn Protection (Default Value)
- RingOn: Apply dedicated RingOn Protection
- RSTP: Apply RSTP RingOn Protection

Ring On™:

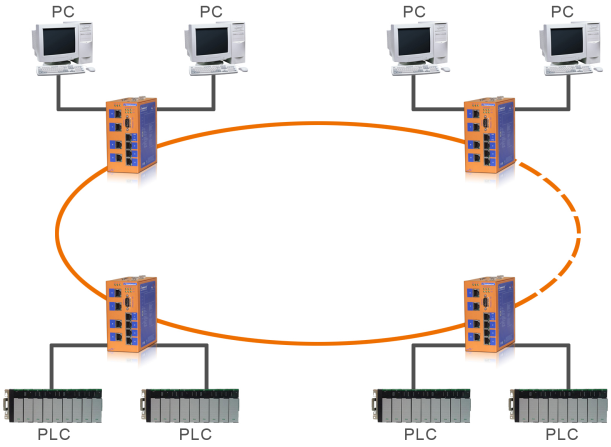
Ring On™ provides the mechanism of restoring automatically and re-connecting for Ethernet, when network interrupts or fails, it has link redundancy and self-recovery function, Ring On™ technology is developed by us and dedicatedly designed and developed for highly reliable Industrial Control Network Application.

Ring On™ technology is in multi-ring network of 500 switches, self-recovery time after disconnecting is less than 15ms. These serials of switches assign part of ports as Ring On™ and connect with other switches. When network disrupts, Relay for Malfunction

Warning enables back-up links to restore network communication rapidly. The following is to compare self-recovery redundancy time, for your reference.

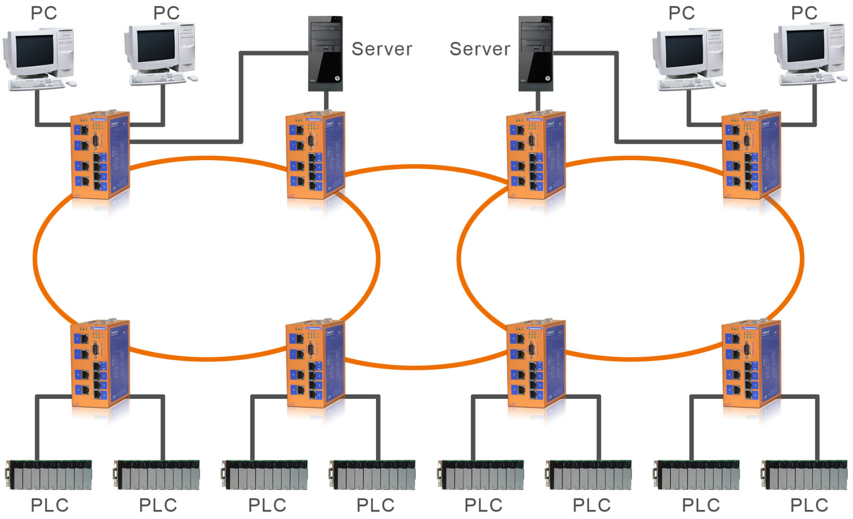
Redundancy Technology	**RingOn**	**RSTP**	**STP**
Restore Time	15ms	Up to 50ms	Up to 30s

Typically, RingOn^{TM} technology requires three or more of the switches to form a ring, the figure as below are a most typical application case:

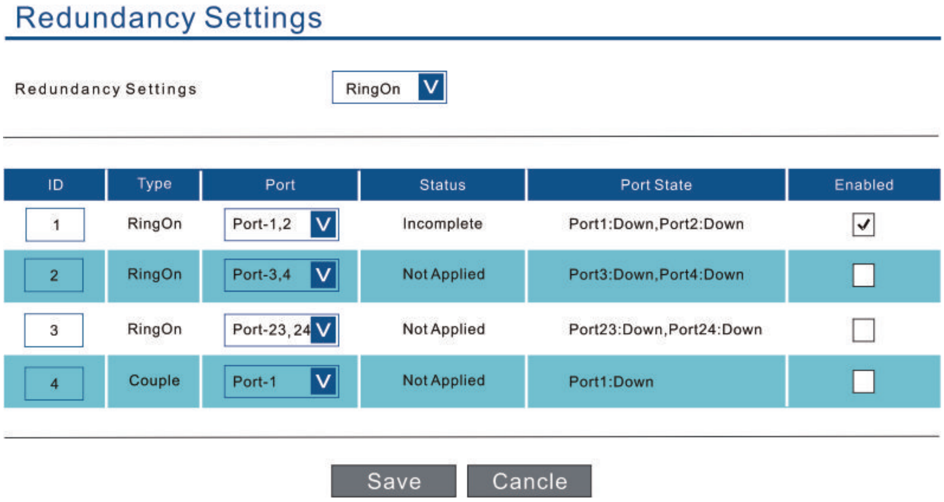


RingOn can build 2 types of ring: single loop and dual loop. Single loop is a basic unit, and one loop consists of 2 ports of this serial of switches. Dual loop is used to connect two or more rings, dual loop use 2 cables to connect 4 switches to form loop.

The figure below is a typical dual loop case



RingOn technology allows the same network to have one or more rings at the same time, but you must set unique ID for each ring, please refer to the screen shot on how to set and use RingOn:



Redundancy Settings

Redundancy Settings: RingOn

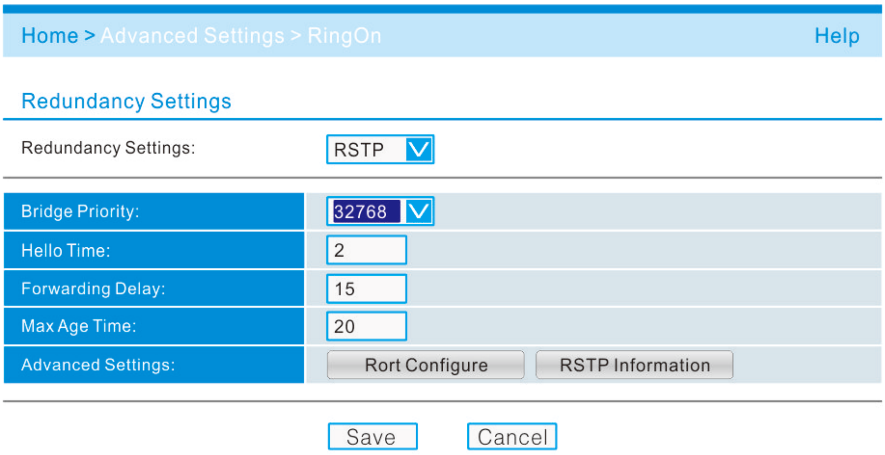
ID	Type	Port	Status	Port State	Enabled
1	RingOn	Port-1,2	Incomplete	Port1:Down,Port2:Down	☑
2	RingOn	Port-3,4	Not Applied	Port3:Down,Port4:Down	□
3	RingOn	Port-23, 24	Not Applied	Port23:Down,Port24:Down	□
4	Couple	Port-1	Not Applied	Port1:Down	□

Redundancy Settings: can select RingOn after setting, save setting parameters, then RingOn will be enabled. To set RingOn function and related parameters, please refer to the following forms.

Item	Description	Default
Ring ID	Mark different ring, each one must select independent ID	1/2/3/4
Ring Type	Ring type to connect switches (RingOn Couple)	Single
Ring Port	Assign different ports for different ring type	1, 2, 3, 4, 23, 24
Networks status	Incomplete: not complete connecting Complete: RingOn finish connecting Not available: RingOn disabled	Not Available
Port status	Fwd: Forward down: not connected block: hold up	Down
RingOn Enable	User RingOn technology	Disable

RSTP Protocol RingOn Protection

Through standard RSTP Protocol RingOn Protection, when network connections disconnects, Relay for Malfunction Warning will be enabled while back-up link is enabled to recover network communication.

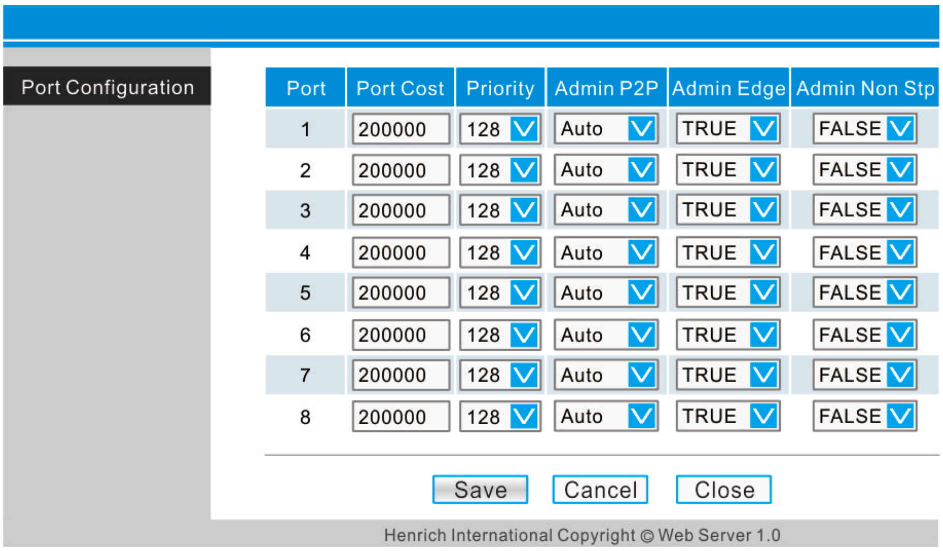


Redundancy Settings

Redundancy Settings:	RSTP
Bridge Priority:	32768
Hello Time:	2
Forwarding Delay:	15
Max Age Time:	20

Item	Description	Default
Bridge Priority	Bridge Priority	32768
Hello Time	Time span (1~10s) to send Hello Packet	2s
Forwarding Delay	Forward delay time (4~30s)	15s
Max Age Time	Maximum survival time (6~40s)	20s
Advanced settings	Advanced settings [port configure] [RSTP information]	

Port configure

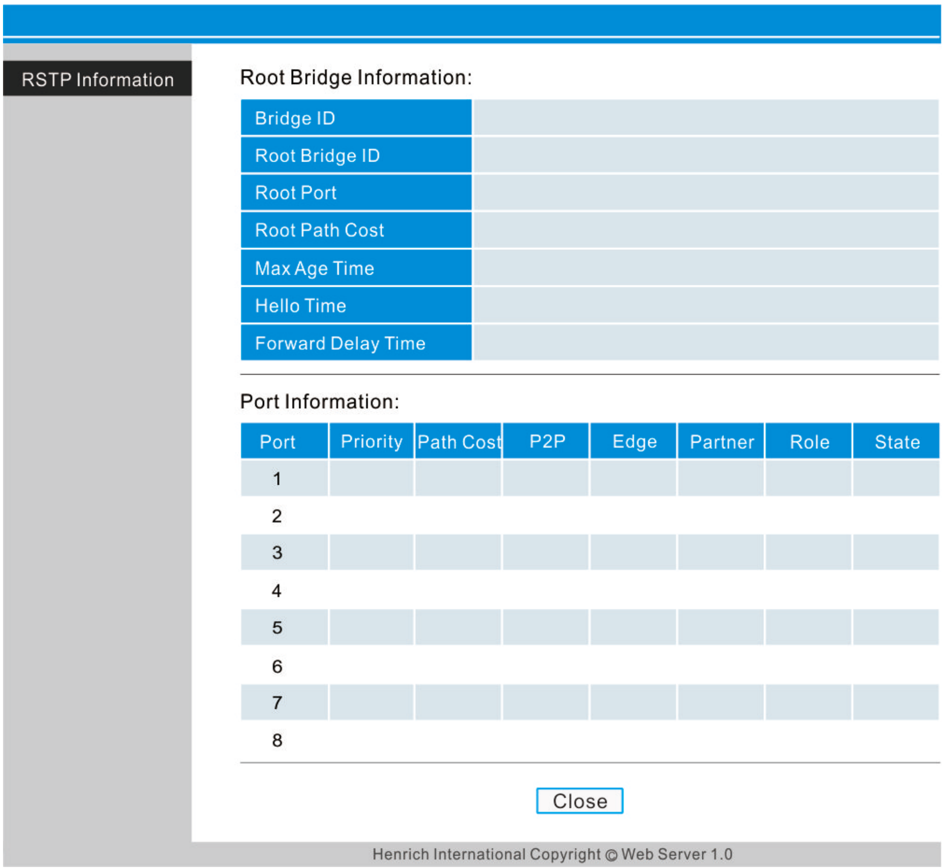


Port	Port Cost	Priority	Admin P2P	Admin Edge	Admin Non Stp
1	200000	128	Auto	TRUE	FALSE
2	200000	128	Auto	TRUE	FALSE
3	200000	128	Auto	TRUE	FALSE
4	200000	128	Auto	TRUE	FALSE
5	200000	128	Auto	TRUE	FALSE
6	200000	128	Auto	TRUE	FALSE
7	200000	128	Auto	TRUE	FALSE
8	200000	128	Auto	TRUE	FALSE

Henrich International Copyright © Web Server 1.0

Item	Description	Default
Port Cost	Port cost	20000
Priority	Port Priority	128
Admin P2P	Port's Point-to Point connection	Auto
Admin Edge	Port lies in the edge of RSTP Protocol	Yes (True)
Admin Non Stp	The port doesn't add RSTP calculation	Add (False)

RSTP Information: Display root bridge and port information for current RSTP



Root Bridge Information:

Bridge ID	
Root Bridge ID	
Root Port	
Root Path Cost	
Max Age Time	
Hello Time	
Forward Delay Time	

Port Information:

Port	Priority	Path Cost	P2P	Edge	Partner	Role	State
1							
2							
3							
4							
5							
6							
7							
8							

Henrich International Copyright © Web Server 1.0

6.4.2 VLAN

What's VLAN?

A Virtual, commonly known as a VLAN, is used to create independent logical networks within a physical network. Several VLANs may co-exist within such a network. VLAN can effectively reduce the scope of Broadcast, and it's convenient to manage network through logical network segment (for example, company's department) that cannot conduct data exchange and is separated. As a matter of fact, if you add a router between different virtual network segments, they can conduct data exchange through router.

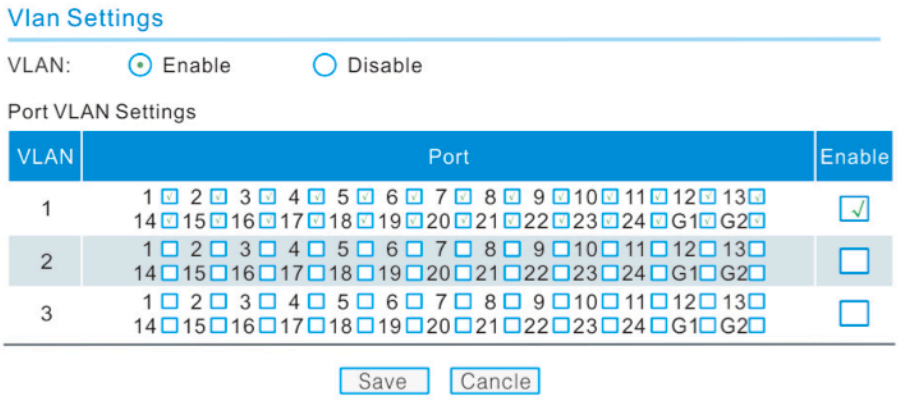
Managed serials of switches support VLAN and IEEE802.1Q VLAN, but the two cannot use at the same time. VLAN can effectively suppress the occurrence of broadcast storm. Next, this manual will show you how to use VLAN.

In VLAN option, you can select port VLAN and IEEE 802.1Q VLAN from VLAN ways (can only select one).

Item	Description	Default
VLAN	VLAN type, based on port or 802.1Q, selected	Port VLAN

Port VLAN

Port VLAN divides a switch's ports into different VLAN domain. Data exchange is not allowed between different VLAN domain, data exchange is allowed only between ports of the VLAN domain to guarantee the security of data exchange. Provide 26-port VLAN, one port can belongs to all VLAN, and can be added to different VLAN domain.



Vlan Settings

VLAN: ● Enable ○ Disable

Port VLAN Settings

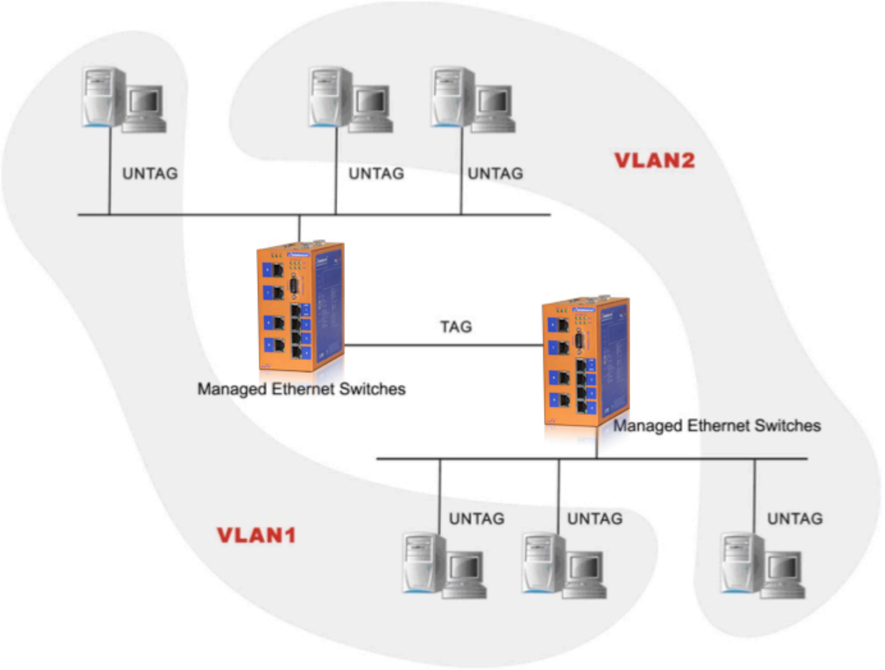
VLAN	Port	Enable
1	1 ☑ 2 ☑ 3 ☑ 4 ☑ 5 ☑ 6 ☑ 7 ☑ 8 ☑ 9 ☑ 10 ☑ 11 ☑ 12 ☑ 13 ☑ 14 ☑ 15 ☑ 16 ☑ 17 ☑ 18 ☑ 19 ☑ 20 ☑ 21 ☑ 22 ☑ 23 ☑ 24 ☑ G1 ☑ G2 ☑	☑
2	1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7 □ 8 □ 9 □ 10 □ 11 □ 12 □ 13 □ 14 □ 15 □ 16 □ 17 □ 18 □ 19 □ 20 □ 21 □ 22 □ 23 □ 24 □ G1 □ G2 □	□
3	1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7 □ 8 □ 9 □ 10 □ 11 □ 12 □ 13 □ 14 □ 15 □ 16 □ 17 □ 18 □ 19 □ 20 □ 21 □ 22 □ 23 □ 24 □ G1 □ G2 □	□

Check box is used to divide the port VLAN and enable VLAN, click “**Save**” to save settings and enable port VLAN function.

Item	Description	Default
VLAN	VLAN No.	
Port	Port No.	All ports in VLAN1
Enable	Enable VLAN	Enable

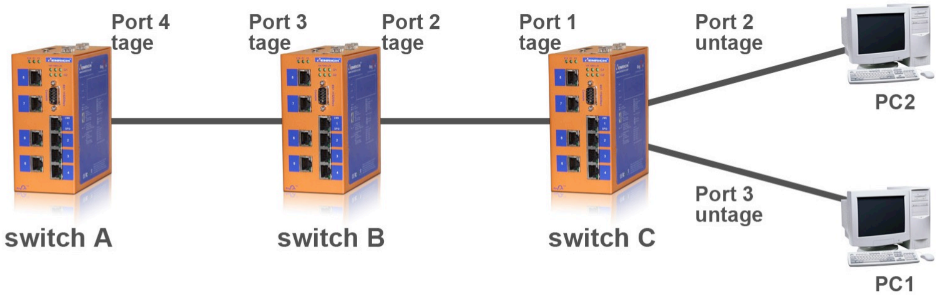
IEEE802.1Q VLAN

Managed switches also support IEEE 802.1Q VLAN. Virtual local area network can be divided across multiple switches through IEEE 802.1Q Protocol. The switches support standard IEEE 802.1Q Protocol, and are compatible with other switches which support IEEE 802.1Q Protocol. The switches can connect and identify 802.1Q tag or not 802.1Q tag device. Use the switches to set IEEE802.1Q VLAN are very convenient. The figure as below gives a basic 802.1Q VLAN case, which helps you learn furthermore about IEEE802.1Q VLAN.



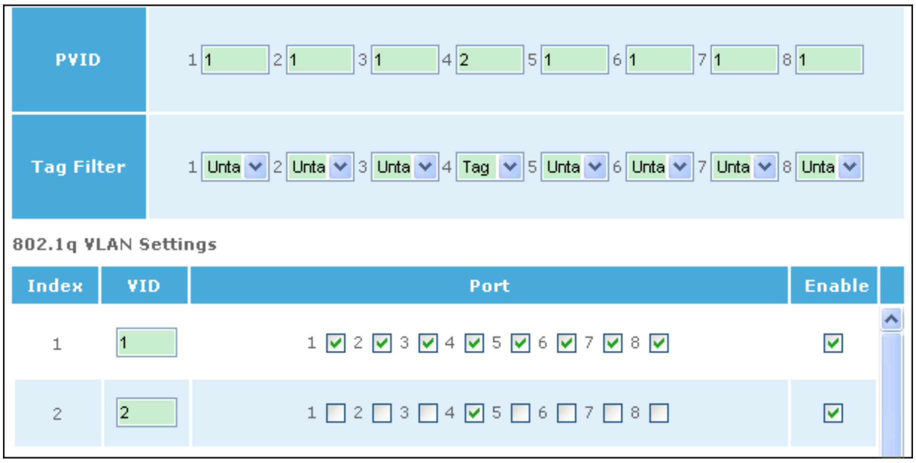
Importing Ethernet data packets will add 802.1Q tag when setting 802.1Q VLAN. PVID is the defaulted 802.1Q tag value to set up each port Vlan. Ethernet data packet will be added with the 802.1Q tag. Tag filter is to configure if each Ethernet data packet will be tagged with 802.1Q or not. If the set-up is tagged, then the data packet will have the 802.1Q mark; If the setup is untagged, then the data packet will not have 802.1Q mark. This series of switches when connected with other branded switches that support 802.1Q, or with the same branded switch, should be configured Tagged. Otherwise, they should be marked Untagged ,Majority of PCs or networking equipment do not receive Ethernet packets tagged with 802.1Q. Tagged port(s) can add more than one VLAN, while untagged port(s) can only add to one VLAN. The PVID value for each port is the VLAN ID for this port. However, as the tagged port(s) ports support more than one VLAN, the configurations are different from one application to the other.

Below is an example:



PC2 in VLAN2, PC1 in VLAN 1. The scenario: for switch B, the port 3 PVID=2; for switch C, the port 1 PVID=1 and the port 2 PVID=2, and port 3 PVID = 1, then PC1 can only visit switch B. PC2 can only visit switch A..

Switch A :

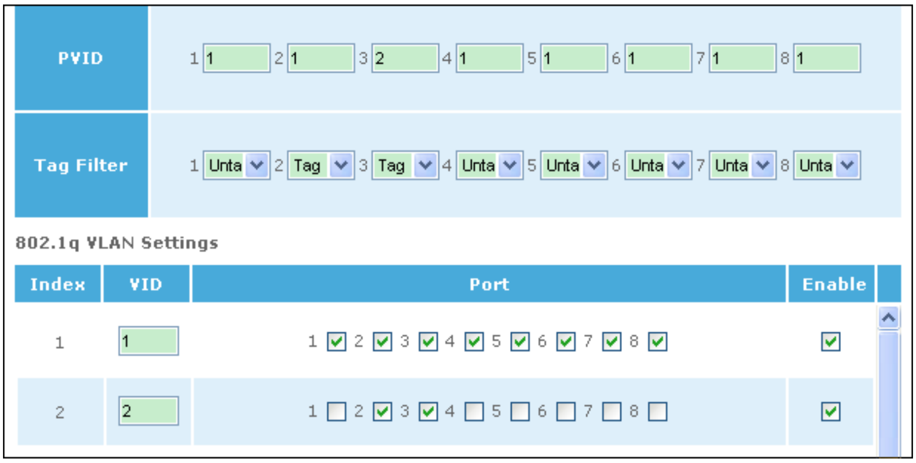


	1	2	3	4	5	6	7	8
PVID	1	1	1	2	1	1	1	1
Tag Filter	Unta	Unta	Unta	Tag	Unta	Unta	Unta	Unta

802.1q VLAN Settings

Index	VID	Port	Enable
1	1	1 ☑ 2 ☑ 3 ☑ 4 ☑ 5 ☑ 6 ☑ 7 ☑ 8 ☑	☑
2	2	1 □ 2 □ 3 □ 4 ☑ 5 □ 6 □ 7 □ 8 □	☑

Switch B :

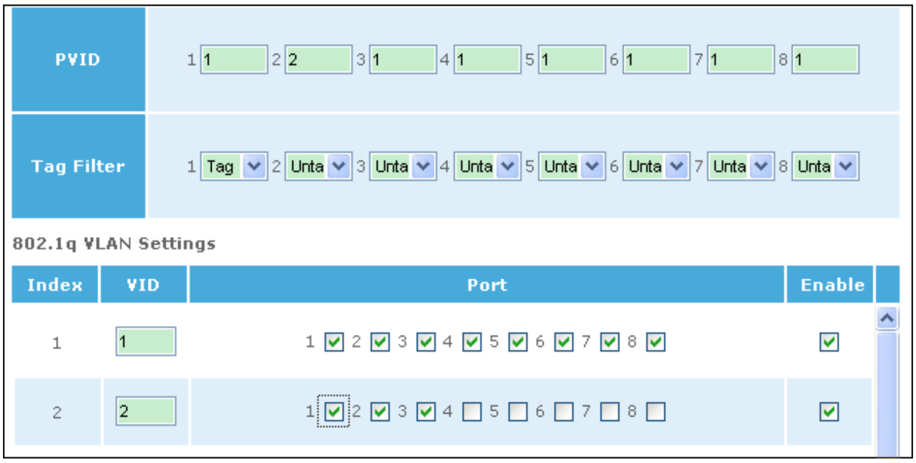


PVID	1 1	2 1	3 2	4 1	5 1	6 1	7 1	8 1
Tag Filter	1 Unta	2 Tag	3 Tag	4 Unta	5 Unta	6 Unta	7 Unta	8 Unta

802.1q VLAN Settings

Index	VID	Port	Enable
1	1	1 ☑ 2 ☑ 3 ☑ 4 ☑ 5 ☑ 6 ☑ 7 ☑ 8 ☑	☑
2	2	1 □ 2 ☑ 3 ☑ 4 □ 5 □ 6 □ 7 □ 8 □	☑

Switch C :



PVID	1 1	2 2	3 1	4 1	5 1	6 1	7 1	8 1
Tag Filter	1 Tag	2 Unta	3 Unta	4 Unta	5 Unta	6 Unta	7 Unta	8 Unta

802.1q VLAN Settings

Index	VID	Port	Enable
1	1	1 ☑ 2 ☑ 3 ☑ 4 ☑ 5 ☑ 6 ☑ 7 ☑ 8 ☑	☑
2	2	1 ☑ 2 ☑ 3 ☑ 4 □ 5 □ 6 □ 7 □ 8 □	☑

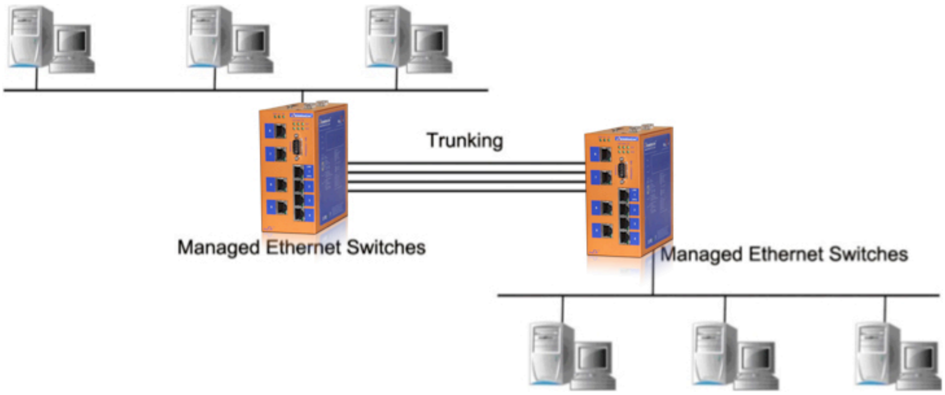
The screenshot as below is Web page to set IEEE 802.1Q VLAN of Switch A:

On the above web page, PVID, TAG FILTER and the ENABLE box have to be configured. The ENABLE box is used to separate the VLANs and activate the VLAN grouping. At the end, click SAVE button to save the settings and activate the functionalities of 802.1Q VLAN.

Item	Description	Default
VLAN	VLAN No.	
Port	Port No.	All ports in VLAN1
Enable	Enable VLAN	Enable

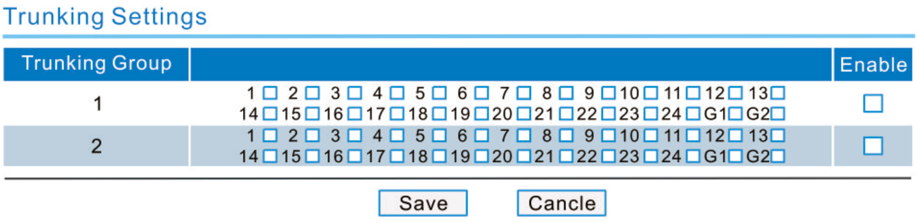
6.4.3 Trunking

Trunking, sometimes called Link Aggregation, is a way to parallel Switch ports using a few cables to improve the bandwidth and generate link redundancy. Trunks are a very useful function in building redundancy network. Managed series of switches provide Trunking function, which allows two or more ports to be a group of Trunking as a single logical link in order to improve the bandwidth and link redundancy; when a physical connection cannot communicate or fails, other link in Trunking group will take over and maintain communications, in this case fast recovery mechanism is set up. The following is a case to use Trunking:



The figure above builds a computer network between one Trunking between two switches, Trunking setting need to be done in the Web page below. Managed series of switches provide two groups of Trunking function, other ports expect Port 1 can be added to Trunking group (Port 1 cannot be used as Trunking).

Besides, one port cannot exist in two Trunking group. Click **"Checking Box"** to add ports to Trunking Group, ports with "√" belong to members of one Trunking Group. Ports without marking "√" don't belong to Trunking Group. When using Trunking, you must enable firstly, then connect physically. Port 1 cannot set in Trunking Group.



Trunking Settings

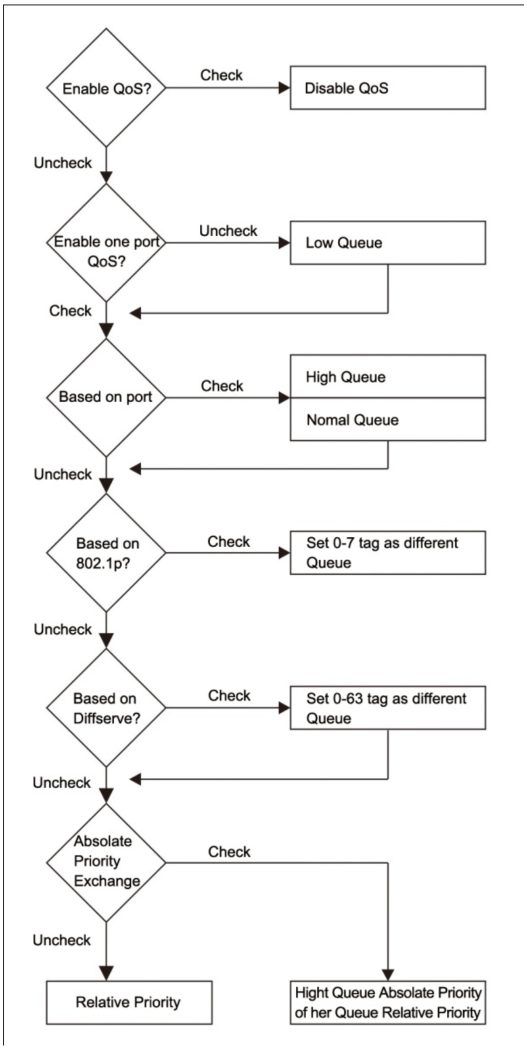
Trunking Group		Enable
1	1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7 □ 8 □ 9 □10 □11 □12 □13 □ 14 □15 □16 □17 □18 □19 □20 □21 □22 □23 □24 □G1 □G2 □	□
2	1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7 □ 8 □ 9 □10 □11 □12 □13 □ 14 □15 □16 □17 □18 □19 □20 □21 □22 □23 □24 □G1 □G2 □	□

Advantages:

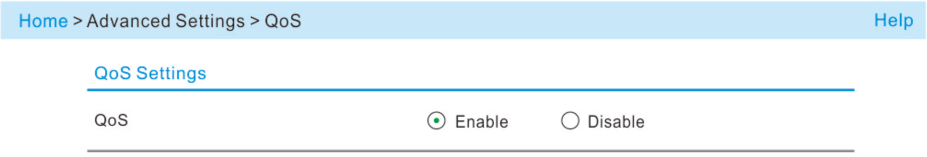
- Improve bandwidth between two switches
- Provide link redundancy back-up and fast self-recovery after disconnecting

6.4.4 QoS

Quality of Service provides 4 different levels (high, middle, normal and low), data packed with high priority stays for a short time, support, low latency for Delay-sensitive traffic. According to settings, for 802.1q Priority Tag and Diffserve Priority Tag, switches can classify data packet into one corresponding level. QoS full line-rate manipulation mechanism can select from Relative Priority and Absolute Priority. Relative priority dispatch carry out rotary exchange based on an advantage. Absolute priority dispatch gives priority to high priority level exchanging, and rotary exchange with other levels (middle, normal, low) based on an advantage.



Enable QoS function



Home > Advanced Settings > QoS

Help

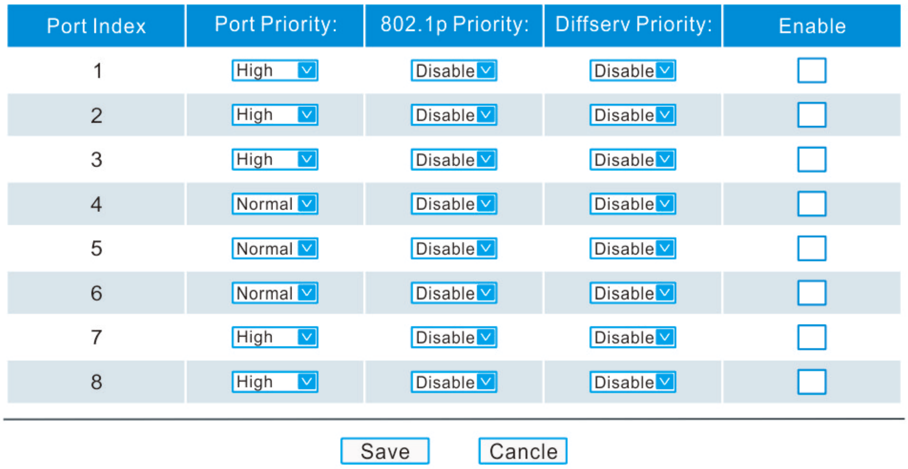
QoS Settings

QoS ● Enable ○ Disable

Select Enable, enable QoS function.

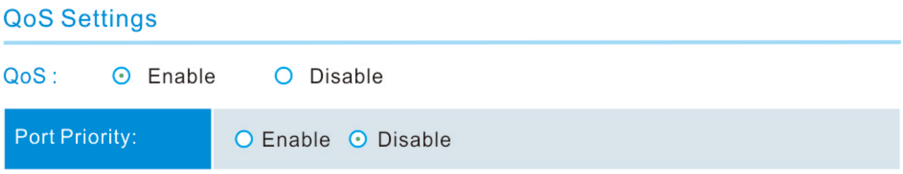
Select port for QoS

Select port you need, mark "√" in Enable Column.



Port Index	Port Priority:	802.1p Priority:	Diffserv Priority:	Enable
1	High	Disable	Disable	□
2	High	Disable	Disable	□
3	High	Disable	Disable	□
4	Normal	Disable	Disable	□
5	Normal	Disable	Disable	□
6	Normal	Disable	Disable	□
7	High	Disable	Disable	□
8	High	Disable	Disable	□

Priority based on port

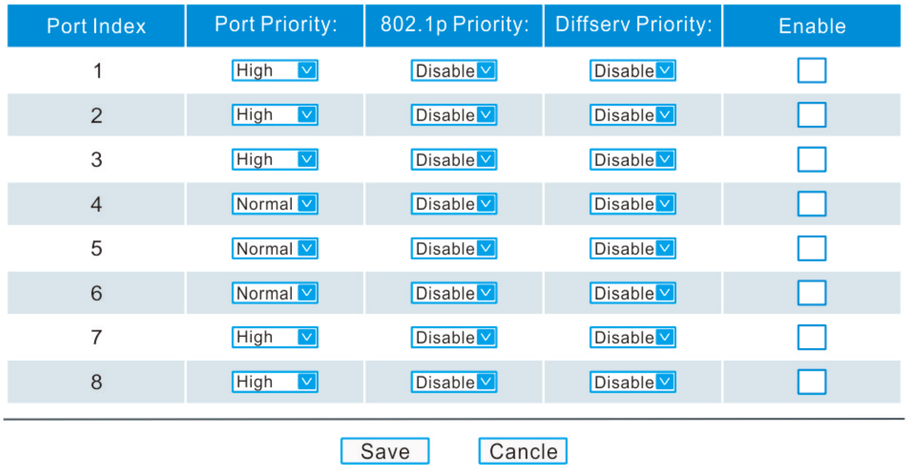


QoS Settings

QoS : ● Enable ○ Disable

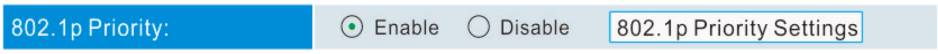
Port Priority: ○ Enable ● Disable

Select **Enable**, enable priority function based on port. There are only **high** and **normal** levels.



Port Index	Port Priority:	802.1p Priority:	Diffserv Priority:	Enable
1	High	Disable	Disable	□
2	High	Disable	Disable	□
3	High	Disable	Disable	□
4	Normal	Disable	Disable	□
5	Normal	Disable	Disable	□
6	Normal	Disable	Disable	□
7	High	Disable	Disable	□
8	High	Disable	Disable	□

Priority based on 802.1p

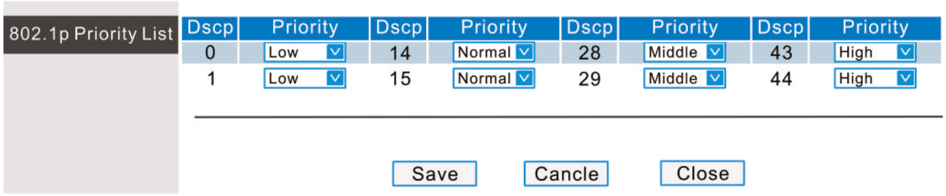


802.1p Priority: ● Enable ○ Disable

Select **Enable**, enable priority function based on **802.1p**.

Click 802.1p priority setting; classify tag from 0 to 7 into different levels.

About IEEE802.1p priority, there are 8 classified levels available, in IEEE802.1Q tags; there are 3 user priority levels.

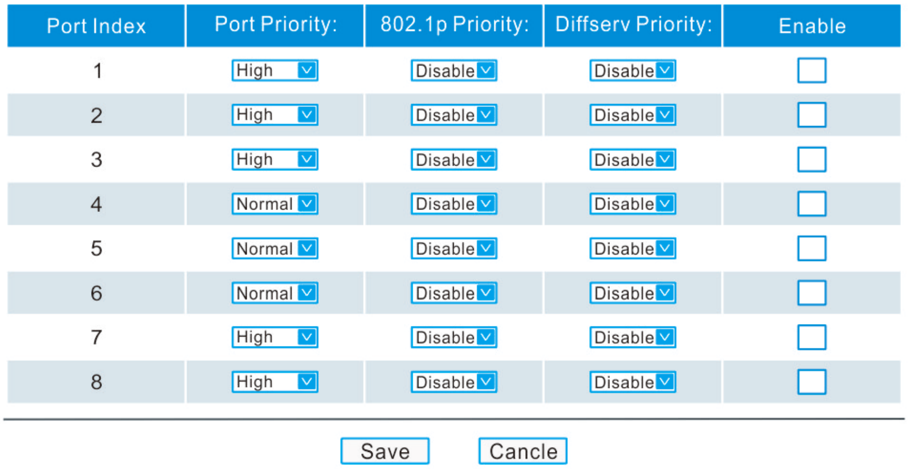


802.1p Priority List

Dscp	Priority	Dscp	Priority	Dscp	Priority	Dscp	Priority
0	Low	14	Normal	28	Middle	43	High
1	Low	15	Normal	29	Middle	44	High

About 802.1p priority, the switches parameters default settings are listed below:

Tag Value	Default	Tag Value	Default
0	Low	4	Middle
1	Low	5	Middle
2	Normal	6	High
3	Normal	7	High



Port Index	Port Priority:	802.1p Priority:	Diffserv Priority:	Enable
1	High	Disable	Disable	□
2	High	Disable	Disable	□
3	High	Disable	Disable	□
4	Normal	Disable	Disable	□
5	Normal	Disable	Disable	□
6	Normal	Disable	Disable	□
7	High	Disable	Disable	□
8	High	Disable	Disable	□

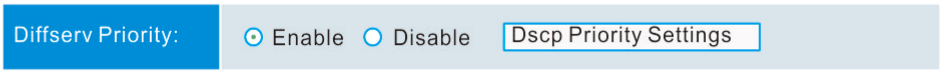
Priority based on DiffServ QoS

DiffServ, also known as differentiated service, is a computer Network System which is assigned to be simple gradable, roughly divided, in modern IP Network, it is used to manage network communication and provide guarantee for quality of service. For example, Diffserv can used to provide shorter responding time to make sure key network data such as audio and video pass successfully, provide simple and best communication guarantee for non-critical data communication such as Web communications or file transfer.

For value of DSCP based on IP information header, the switches can classify service level of communication data. The switch support DSCP IP v4 and IPv6.If enabling DSCP Priority, the switch divides the communication volume level according to DSCP Value.

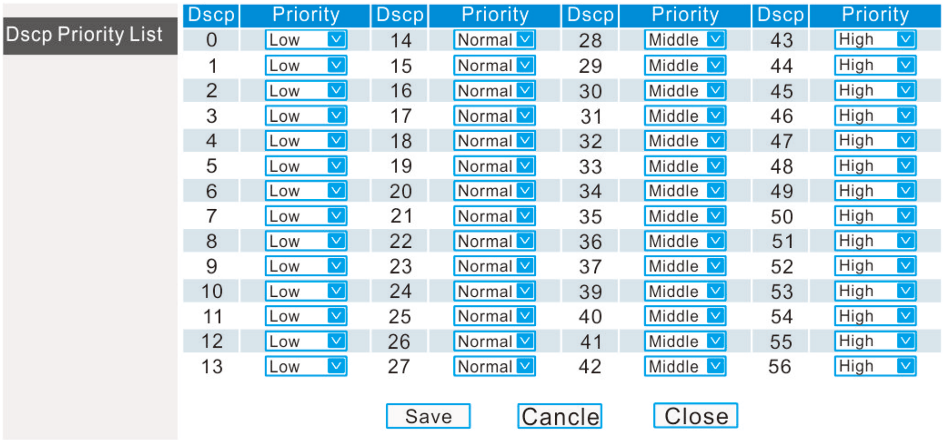
DiffServ is a 3-layer representation scheme for DSCP domain in IP header to store priority level. DSCP is a high intelligent method as to differentiate the priority for different types of communication volume. DSCP maps 64 values to user to define service level, allow establishing more operation control in network communications.

Select **“Enable”**, enable Priority based on DiffServ



Diffserv Priority: ● Enable ○ Disable

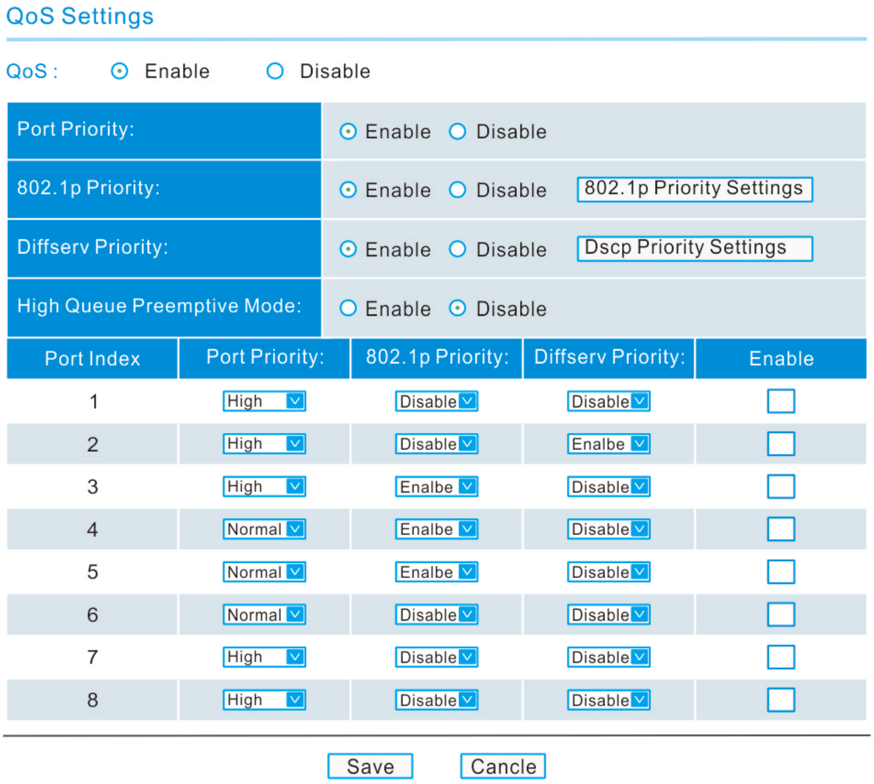
Add DiffServ priority setting; classify tag form to 63 into different queue.



Dscp Priority List

Dscp	Priority	Dscp	Priority	Dscp	Priority	Dscp	Priority
0	Low	14	Normal	28	Middle	43	High
1	Low	15	Normal	29	Middle	44	High
2	Low	16	Normal	30	Middle	45	High
3	Low	17	Normal	31	Middle	46	High
4	Low	18	Normal	32	Middle	47	High
5	Low	19	Normal	33	Middle	48	High
6	Low	20	Normal	34	Middle	49	High
7	Low	21	Normal	35	Middle	50	High
8	Low	22	Normal	36	Middle	51	High
9	Low	23	Normal	37	Middle	52	High
10	Low	24	Normal	39	Middle	53	High
11	Low	25	Normal	40	Middle	54	High
12	Low	26	Normal	41	Middle	55	High
13	Low	27	Normal	42	Middle	56	High

Select DSCP Mode for each port



QoS Settings

QoS : ● Enable ○ Disable

Port Priority:	● Enable ○ Disable
802.1p Priority:	● Enable ○ Disable 802.1p Priority Settings
Diffserv Priority:	● Enable ○ Disable Dscp Priority Settings
High Queue Preemptive Mode:	○ Enable ● Disable

Port Index	Port Priority:	802.1p Priority:	Diffserv Priority:	Enable
1	High	Disable	Disable	□
2	High	Disable	Enalbe	□
3	High	Enalbe	Disable	□
4	Normal	Enalbe	Disable	□
5	Normal	Enalbe	Disable	□
6	Normal	Disable	Disable	□
7	High	Disable	Disable	□
8	High	Disable	Disable	□

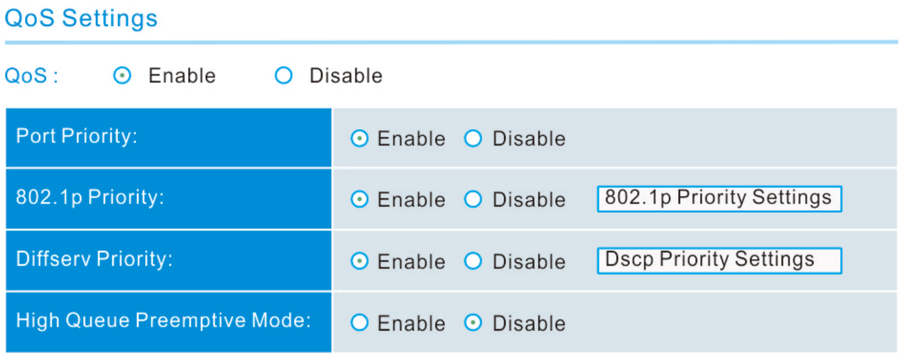
Advantages of DiffServ based on IEEE802.1D:

Assign a variety of network service levels for selected applications and service through setting switches

Store DSCP value in IP header, priority level of data frame can pass through the whole internet DSCP downward is compatible with IPv4 TOS, allowing device using three-layer TOS Priority Programs to operate.

Select Absolute Priority

Select Enable, enable absolute priority exchange; if selecting Disable, Relative Priority will be enabled. Relative Priority Dispatch is based on favorable way of rotary exchange, Absolute Priority Dispatch gives priority to High Priority level for exchange, for other levels, while for others (middle, normal, low) based on favorable way of rotary exchange select port with 802.1p mode

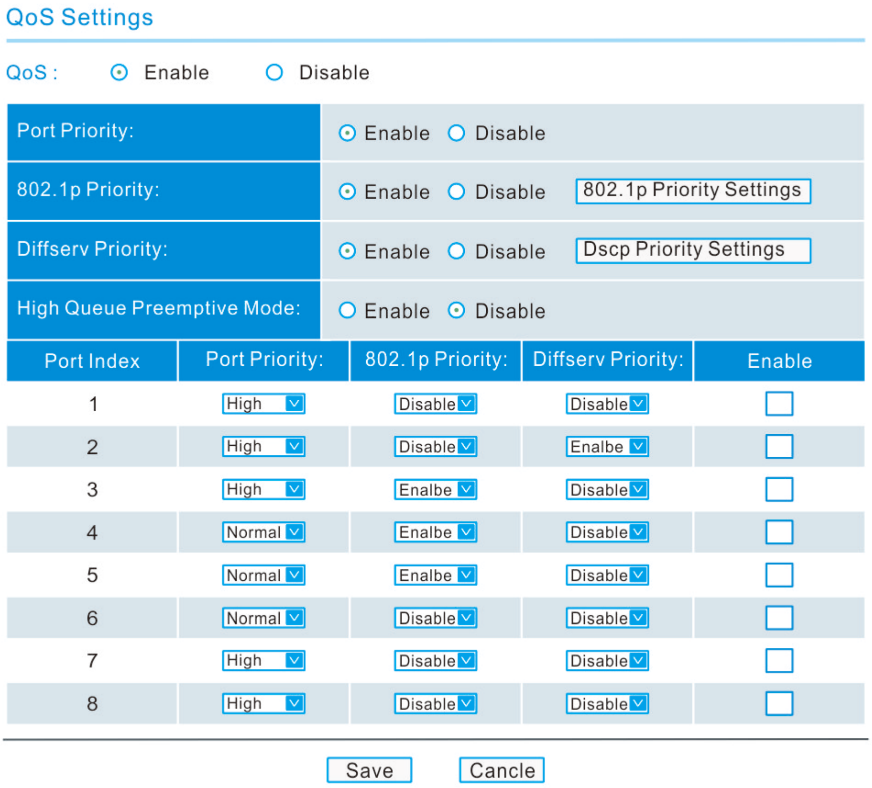


QoS Settings

QoS : ● Enable ○ Disable

Port Priority:	● Enable ○ Disable	
802.1p Priority:	● Enable ○ Disable	802.1p Priority Settings
Diffserv Priority:	● Enable ○ Disable	Dscp Priority Settings
High Queue Preemptive Mode:	○ Enable ● Disable	

Brief Introduction of Interface Parameters



QoS Settings

QoS : ⊙ Enable ○ Disable

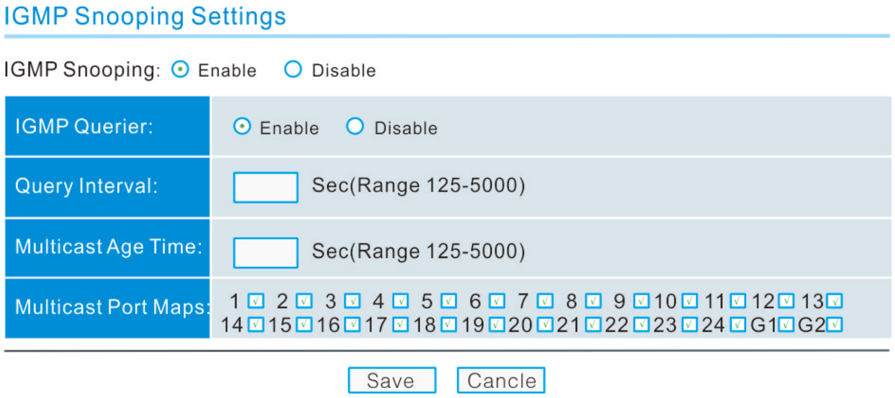
Port Priority:	⊙ Enable ○ Disable
802.1p Priority:	⊙ Enable ○ Disable 802.1p Priority Settings
Diffserv Priority:	⊙ Enable ○ Disable Dscp Priority Settings
High Queue Preemptive Mode:	○ Enable ⊙ Disable

Port Index	Port Priority:	802.1p Priority:	Diffserv Priority:	Enable
1	High	Disable	Disable	□
2	High	Disable	Enalbe	□
3	High	Enalbe	Disable	□
4	Normal	Enalbe	Disable	□
5	Normal	Enalbe	Disable	□
6	Normal	Disable	Disable	□
7	High	Disable	Disable	□
8	High	Disable	Disable	□

Item	Description	Default
QoS Enable	Enable QoS	Disable
Port-based QoS Enable	Enable Port QoS	Enable this group
802.1p QoS Enable	Enable 802.1p QoS	Disable
802.1p QoS Settings	Set 802.1p Priority	---
Diffserv QoS Enable	Enable DiffServ QoS	Disable
Diffserv QoS Settings	Set DiffServ Priority	---
Port Priority	Set Priority for Port	High

6.4.5 IGMP Snooping

Managed switches provide Internet Multi-cast Management Protocol function to snoop data packet of IGMP so as to obtain multicast group information of switch port.



IGMP Snooping Settings

IGMP Snooping: ● Enable ○ Disable

IGMP Querier:	● Enable ○ Disable
Query Interval:	Sec(Range 125-5000)
Multicast Age Time:	Sec(Range 125-5000)
Multicast Port Maps:	1 ☑ 2 ☑ 3 ☑ 4 ☑ 5 ☑ 6 ☑ 7 ☑ 8 ☑ 9 ☑ 10 ☑ 11 ☑ 12 ☑ 13 ☑ 14 ☑ 15 ☑ 16 ☑ 17 ☑ 18 ☑ 19 ☑ 20 ☑ 21 ☑ 22 ☑ 23 ☑ 24 ☑ G1 ☑ G2 ☑

IGMP snooping can work with GMRP, when device of network change connection port. Send GMRP notice to prevent multi-cast information from missing. Query Packet for IGMP is used to query existing multi-cast group, Query interval is according to Query Interval in web page above .If MAC address have not refreshed within aging time, switches will delete multi-cast group , and not send leaving message when deleting.

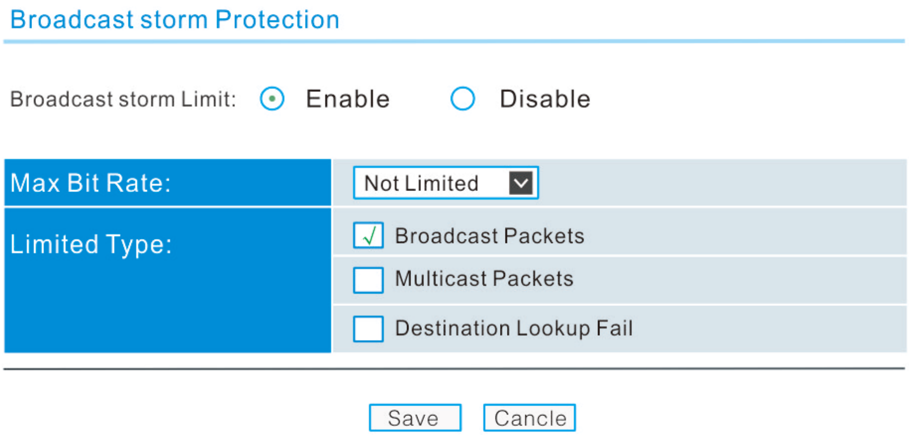
Item	Description	Default
IGMP Snooping Enable	Enable IGMP Snooping	Disable
IGMP Query Enable	Enable IGMP Query Setting	Enable
IGMP Query Interval	Query interval for Switch	125(as protocol's standard
Multicast Age Time	Aging time for switch's	300
IGMP Port Maps	Snoop port selection	All ports

6.4.6 Broadcast Storm Control

The cause for Broadcast Storm is diverse, for example, a redundancy or wrong connection to form Broadcast and multi-cast packet and send to other ports through switches, the ports receiving broadcast and multi-cast packet will continue to broadcast circularly and form broadcast storm.

In some conditions, Broadcast Storm control prevent malicious attach, for example, DOS(Danial of Service) attach, DOS send ICMP request to a broadcast address via a server, resulting in other servers to respond to this address, broadcast storm come into being due to DOS attach. If enabling Broadcast Storm, prevent the attach to some extent.

- Enable Broadcast Storm: Broadcast Storm Limit select "Enable"
- Select Broadcast Max Bit Rate: Select Broadcast Max Bit Rate (64k-90M) from Drop-down List Menu
- Select Limited Type: Select Limited Type, broadcast Packets, Multicast Packets, Desti



Broadcast storm Protection

Broadcast storm Limit: ● Enable ○ Disable

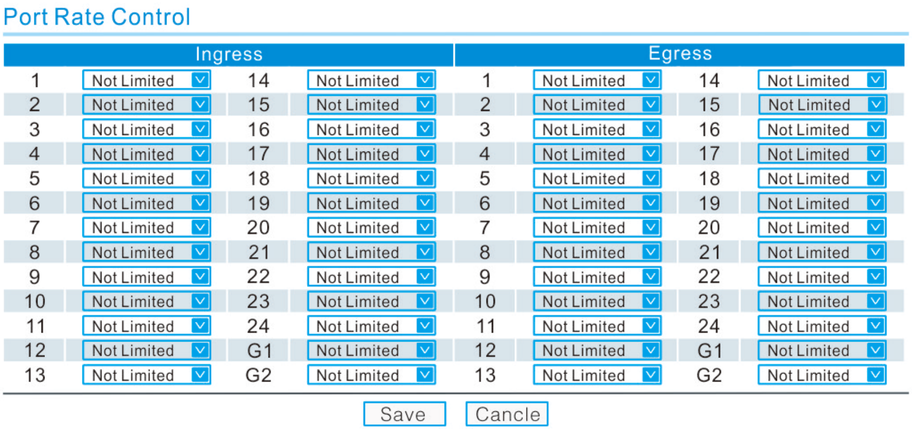
Max Bit Rate:	Not Limited
Limited Type:	☑ Broadcast Packets □ Multicast Packets □ Destination Lookup Fail

Item	Description	Default
Broadcast Storm Enable	Enable Broadcast Strom Protection	Disable
Max Bit Rate	Max Bit Rate can be selected from: Not limited, 64K., 128K, 256K, 512K, 1M,, 2M, 3M, 4M, 5M, 6M、7M, 8M, 9M, 10M, 20M, 30M, 40M,	Not limited
Little Type	Broadcast packet, multi-cast packet, MAC Address, Destination Lookup Fail	

Note: Destination Lookup Failure is also called DLF Message; when MAC Address List cannot find matched entries, the message is not broadcast or multi-cast message, and then the message is called DLF Message, the way that switches deal with the message is the same as dealing with broadcast message, just diffuse the message form VLAN of port.

6.4.7 Port Rate Control

The switches provide Port Control Rate Limit, including Ingress and Egress Rate Limit. Through Web page, users can limit or cancel communication flow of each port. Users can select a fixed rate from Drop-down menu, with the range of 6Kbps ~ 100Mbps.

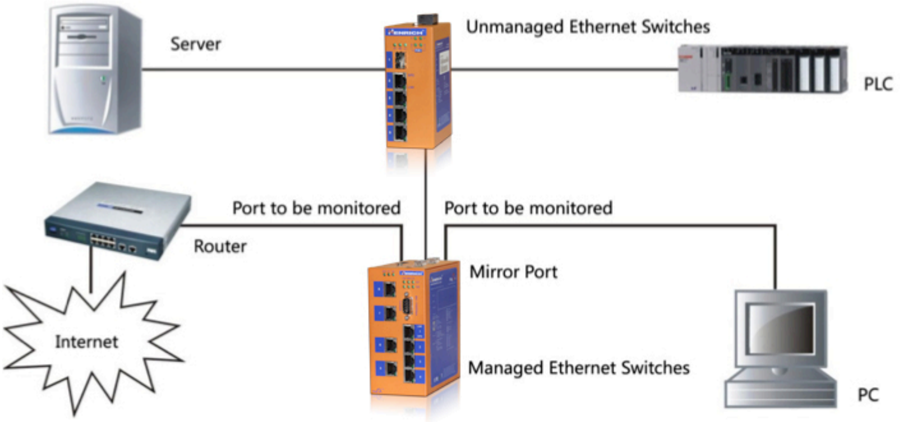


Port Rate Control

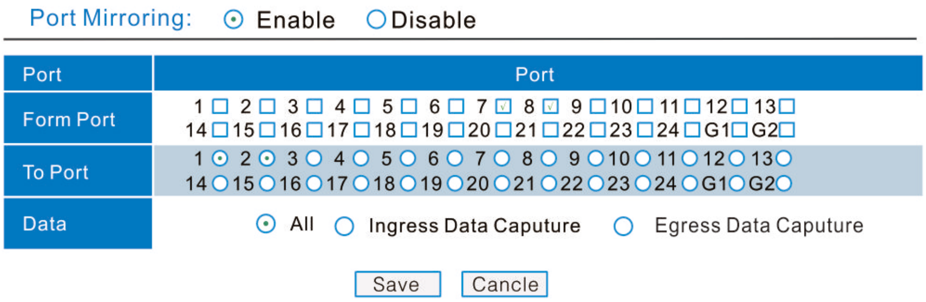
Ingress				Egress			
1	Not Limited	14	Not Limited	1	Not Limited	14	Not Limited
2	Not Limited	15	Not Limited	2	Not Limited	15	Not Limited
3	Not Limited	16	Not Limited	3	Not Limited	16	Not Limited
4	Not Limited	17	Not Limited	4	Not Limited	17	Not Limited
5	Not Limited	18	Not Limited	5	Not Limited	18	Not Limited
6	Not Limited	19	Not Limited	6	Not Limited	19	Not Limited
7	Not Limited	20	Not Limited	7	Not Limited	20	Not Limited
8	Not Limited	21	Not Limited	8	Not Limited	21	Not Limited
9	Not Limited	22	Not Limited	9	Not Limited	22	Not Limited
10	Not Limited	23	Not Limited	10	Not Limited	23	Not Limited
11	Not Limited	24	Not Limited	11	Not Limited	24	Not Limited
12	Not Limited	G1	Not Limited	12	Not Limited	G1	Not Limited
13	Not Limited	G2	Not Limited	13	Not Limited	G2	Not Limited

6.4.8 Port Mirroring

Port Mirroring is just to send data copy of one or more ports to the assigned por. Network Communication and Data Packet can be monitored and viewed by taking advantage of Port Mirroring through an assigned port. The switches provide Port Mirroring, which can be used for network fault diagnosis, debugging and analyzing. The following is schematic drawing for Port Mirroring:



Port Mirroring for managed series of switches provides many mirroring rules; user can capture Form Port, to port and all data. Some actions of Port Mirroring can be done through Web page of switch. The screenshot below is detailed setting for Web page Port Mirroring:



Port Mirroring: ● Enable ○ Disable

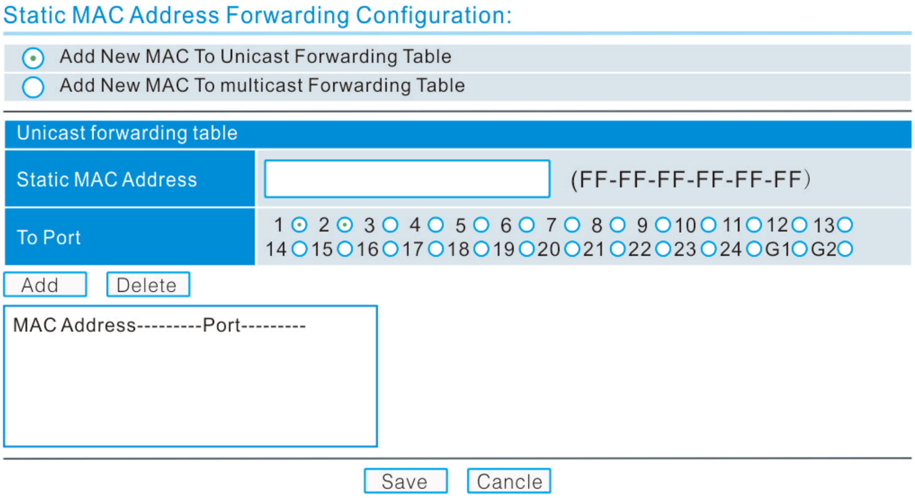
Port	Port
Form Port	1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7 ☑ 8 ☑ 9 □ 10 □ 11 □ 12 □ 13 □ 14 □ 15 □ 16 □ 17 □ 18 □ 19 □ 20 □ 21 □ 22 □ 23 □ 24 □ G1 □ G2 □
To Port	1 ● 2 ● 3 ○ 4 ○ 5 ○ 6 ○ 7 ○ 8 ○ 9 ○ 10 ○ 11 ○ 12 ○ 13 ○ 14 ○ 15 ○ 16 ○ 17 ○ 18 ○ 19 ○ 20 ○ 21 ○ 22 ○ 23 ○ 24 ○ G1 ○ G2 ○
Data	● All ○ Ingress Data Caputure ○ Egress Data Caputure

In Mirroring, Mirroring Port is **"To Port"**, Mirrored Port is **"From Port"**. As Capturing Port, Mirroring Port can only select; while as source port, Mirrored Port can select more. Relative to the switches, data inflowing from Mirrored Port is Ingress Data Capture; data out flowing into Mirrored Port is Egress Data Capture.

6.4.9 Static MAC Address Forwarding Table

Managed series of switches provide Static MAC Address Forwarding function. The aim is forward data packet including static MAC address to assigned ports. Forwarding Address Table built in switch chips can not only Learning function but support ten static unicast MAC address and ten multicast MAC addresses. Static MAC Address performs forwarding function, but it is not dominated by aging treatment, normal and high priority can be applied for message processing.

In the following Web page, you can select a unicast or multicast MAC address settings through radio button “**Add New Static MAC Address To Unicast Forwarding Table**” or “**Add New Static MAC Address To Multicast Forwarding Table**”. The button “**Add**” and “**Delete**” are used to add and delete Static MAC Address. Static MAC Address Domain is a valid input from users, if MAC address input is not valid, Web page will prompt warning message. Port domain is used to select Static MAC Address Forwarding Port, if it is Unicast Static MAC Address, it can assign one forwarding port, if it is Multicast Static MAC Static Address, and it can assign one or more forwarding port. After editing Static MAC Address Table, click “**Save**” to finish Updating Static MAC Address, click “**Cancel**” to quit updating, then go back to the page that originally set and save.



Static MAC Address Forwarding Configuration:

● Add New MAC To Unicast Forwarding Table
○ Add New MAC To multicast Forwarding Table

Unicast forwarding table

Static MAC Address	(FF-FF-FF-FF-FF-FF)
To Port	1 ● 2 ● 3 ○ 4 ○ 5 ○ 6 ○ 7 ○ 8 ○ 9 ○ 10 ○ 11 ○ 12 ○ 13 ○ 14 ○ 15 ○ 16 ○ 17 ○ 18 ○ 19 ○ 20 ○ 21 ○ 22 ○ 23 ○ 24 ○ G1 ○ G2 ○

MAC Address---------Port---------

Note:

01005E00006C 0180C2000010 0180C200000X 0180C200002X

6. 5 Management Function

In this chapter, we will introduce management function of switches. The functions make it easy for switch management and provide much more useful information for users. The functions include SNMP (Simple Network Management Protocol）, Diagnosis, Email Warning, Relay Warning, etc.

6. 5.1 SNMP

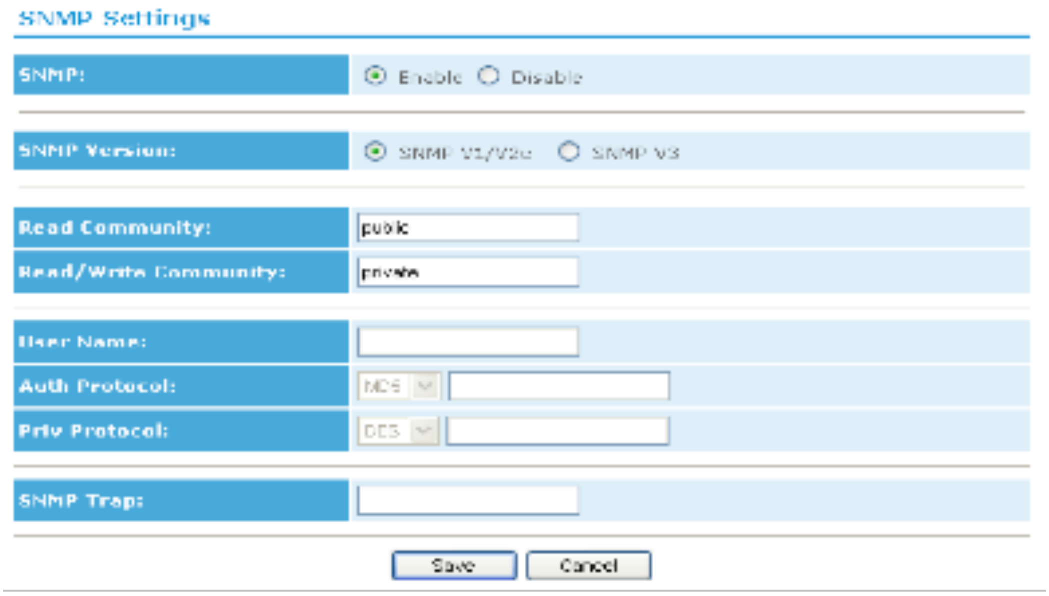
Simple Network Management Protocol (SNMP), defined by Internet Engineering Task Force, is a part of Internet protocol. Concerning the condition of one network device, using SNMP monitors network device through network management. SNMP Protocols consists of a series of standard network management, Application Layer Protocol, Database, Data Objects. SNMP Protocol can display management parameter, such as system description setting through management system forms. The setting description can be looked up and set through management application that supports SNMP.

Managed series of switches support SNMP V1/V2c/V3. SNMP V1 and V2c match certification through public string, which means to use public or private string. SNMP server allows read-only or read-and-write way to access all objects.

Based on TCP/IP Protocol, SNMP usually uses UDP port 161（SNMP）and 162（SNMP-traps）, SNMP Protocol Agent is in network device .Use MIBs (information specific to the device) as device interface, and the device can be monitored and controlled through agent When a trap event occurs, message is transferred by SNMP Trap, a trap receivers available can receive the trap message.

Managed series of switches support two types of trap: cold start and hot start.　If you enter IP address in the column of Trap To (IP), then click “Save” button, trap receiver can receive trap message.　If failing to trap message, please check network setting and connection.

The screenshot below is SNMP setting page:



SNMP Settings

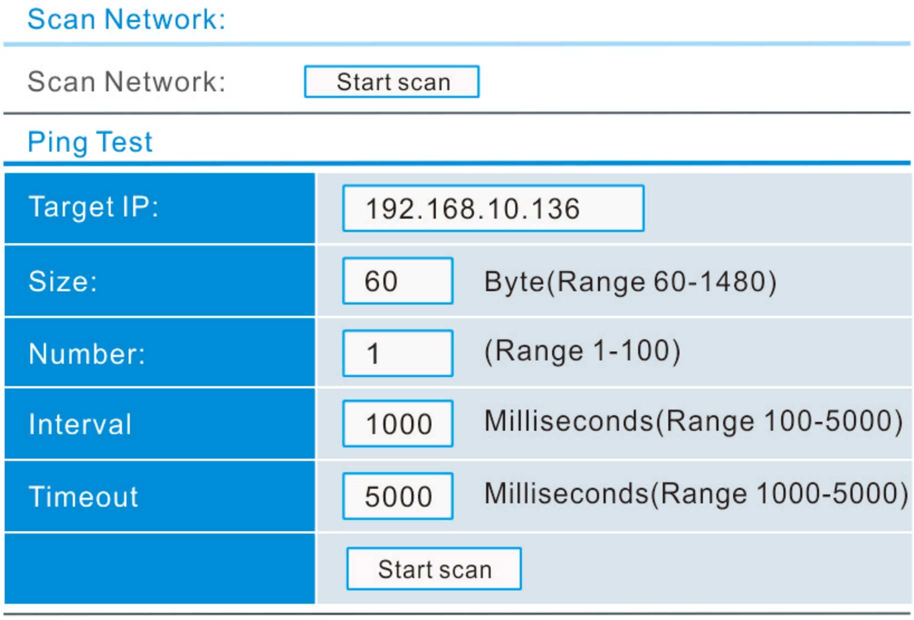
SNMP:	● Enable ○ Disable
SNMP Version:	● SNMP V1/V2c ○ SNMP V3
Read Community:	public
Read/Write Community:	private
User Name:	
Auth Protocol:	MD5
Priv Protocol:	DES
SNMP Trap:	

The table below provides some explanation for SNMP function project, for more information, please refer to the appendix in this manual.

Item	Description	Default
SNMP Enable	Enable SNMP	Disable
SNMP Version	V1/V2c V3	V1/V2c
Read Community	Match certification through public string, access to it in read-only (V1/V2c)	Public
Read/Write Community	Match certification through public string, access to it in read-Write way (V1/V2c)	Private
User Name	User security name (V3)	Blank
Auth Protocol	Authentication algorithm MD5/SHA (V3)	Blank
Priv Protocol	encryption algorithm DES/AES (V3)	Blank
SNMP Trap	IP Address of Trap receiver	Blank

6. 5.2 Diagnosis Function

Managed series of switches support diagnosis function, which is network fault analyzing, network testing and trouble shooting.



Scan Network:

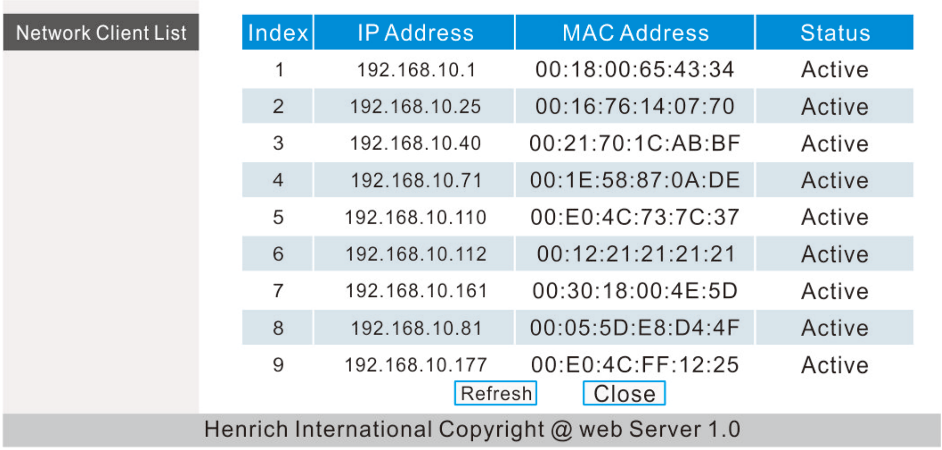
Scan Network: Start scan

Ping Test

Target IP:	192.168.10.136
Size:	60 Byte(Range 60-1480)
Number:	1 (Range 1-100)
Interval	1000 Milliseconds(Range 100-5000)
Timeout	5000 Milliseconds(Range 1000-5000)
	Start scan

Diagnosis function provides two tools, Net Scan and Ping. Net Scan look up all network devices, Net scan function is a simple and useful tool; just click **"Start Scan"**, scan function can be completed.

The screenshot below is a scan result:



Network Client List

Index	IP Address	MAC Address	Status
1	192.168.10.1	00:18:00:65:43:34	Active
2	192.168.10.25	00:16:76:14:07:70	Active
3	192.168.10.40	00:21:70:1C:AB:BF	Active
4	192.168.10.71	00:1E:58:87:0A:DE	Active
5	192.168.10.110	00:E0:4C:73:7C:37	Active
6	192.168.10.112	00:12:21:21:21:21	Active
7	192.168.10.161	00:30:18:00:4E:5D	Active
8	192.168.10.81	00:05:5D:E8:D4:4F	Active
9	192.168.10.177	00:E0:4C:FF:12:25	Active

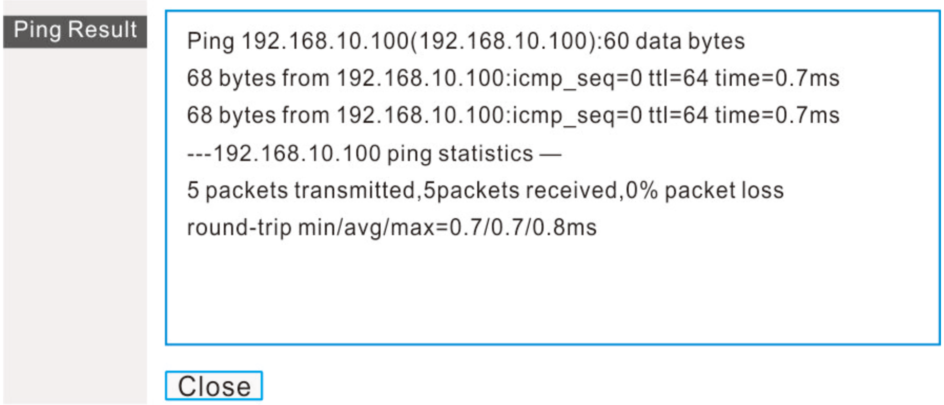
Henrich International Copyright @ web Server 1.0

Ping function provides simple ping command a simple and powerful tool for network problem diagnosis for users.

The most unique of this function is to enter a ping command though Web page, the switches themselves trigger a ping

Command and enter the result in Web page. In this way, users can expediently control the switches to send ping command and output the result.

Use ping function, enter target IP address, other items are default; click **"Start Test"**, output result is just as below:



```
Ping 192.168.10.100(192.168.10.100):60 data bytes
68 bytes from 192.168.10.100:icmp_seq=0 ttl=64 time=0.7ms
68 bytes from 192.168.10.100:icmp_seq=0 ttl=64 time=0.7ms
---192.168.10.100 ping statistics —
5 packets transmitted,5packets received,0% packet loss
round-trip min/avg/max=0.7/0.7/0.8ms
```

Items settings for Ping function

Item	Description	Default
Target IP	Ping's IP Address	Blank
Size	Length of Ping Packet	60
Number	The number of Ping Packet sent	1
Interval	The Interval of Ping sent	1000
Timeout	Ping Timeout	5000

6. 5.3 Email Warning

When the following events occur, Email Warning function will send warning message via E-mail immediately:

- ☆ Connection Status
- ☆ Broadcast Storm occur
- ☆ Ring Net Status Change
- ☆ Power State Change

The message below will be sent every 12 hours via E-mail:

☆ NTP Time

☆ Ring Net Status Change

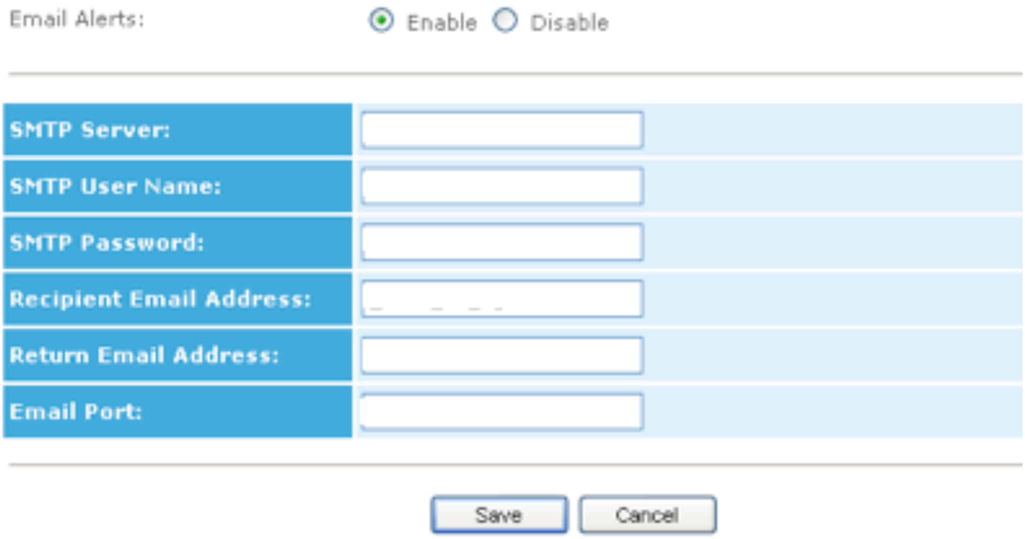
☆ Broadcast Storm Information

☆ Power Information

☆ Connection Status Change

☆ Login Information Synchronization

☆ System Action and Operation Record



Email Alerts: ● Enable ○ Disable

SMTP Server:	
SMTP User Name:	
SMTP Password:	
Recipient Email Address:	
Return Email Address:	
Email Port:	

If click “**Save**”, an E-mail will be sent immediately. The parameters in table below are for your reference.

Item	Description	Default
Email Alerts	Enable/disable Email Warning Function	Disable
SMTP Server	SMTP Servers Name or IP Address	Blank
SMTP User	SMTP Server User Name	Blank
SMTP Password	SMTP Server User Password	Blank
Recipient Email Address	Receive Email Address	Blank
Return Email Address	Send Email Address	Blank
Email Port	SMTP Port	25

6. 5.4 Relay Warning

Managed series of switch has relay output to send warning signal. When one or more events occur, relay will export an electric signal through setting. Usually, when the following event occurs, relay will send warning signal:

☆ Connection Status Change ☆ Ring Net Change

☆ Broadcast Storm Occur ☆ Power Status Change

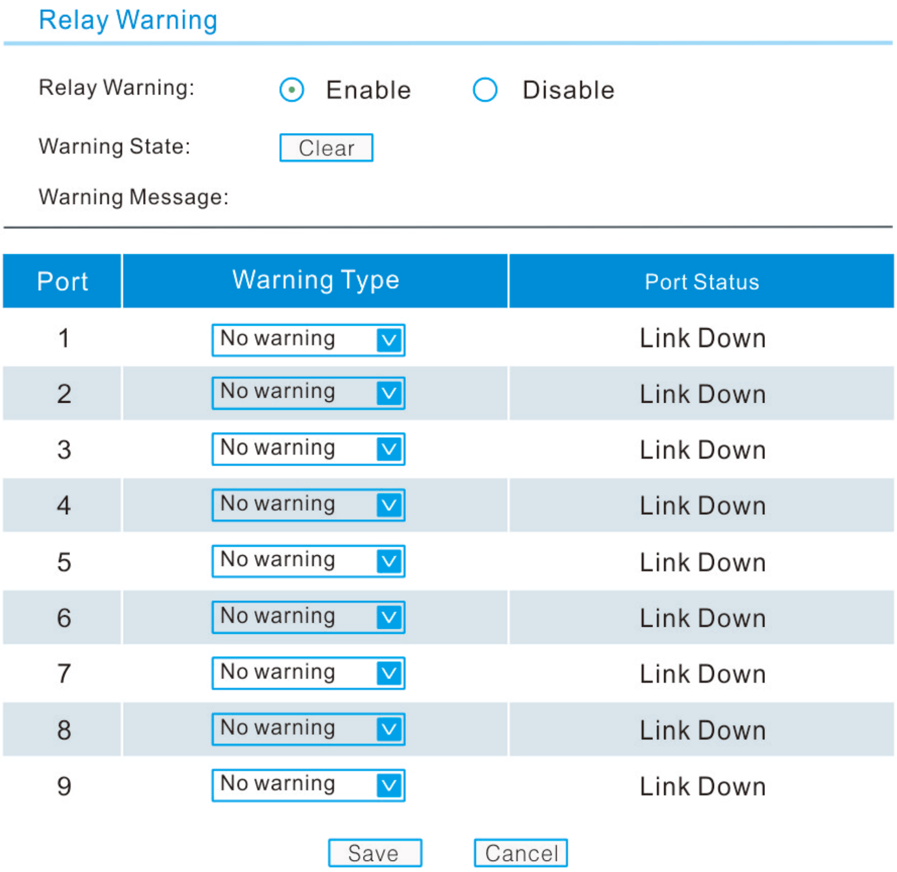
The following 2 steps are on how to set Realy Warning:

² ☆ Set Warning Type of Relay (Warning Type

In Drop-down column of Web page below, select Warning Type for Connection Status

² ☆ Enable settings

Click radio button **"Enable"**, then click **"Save"** to enable Relay Warning Function.



Relay Warning

Relay Warning: ● Enable ○ Disable

Warning State: Clear

Warning Message:

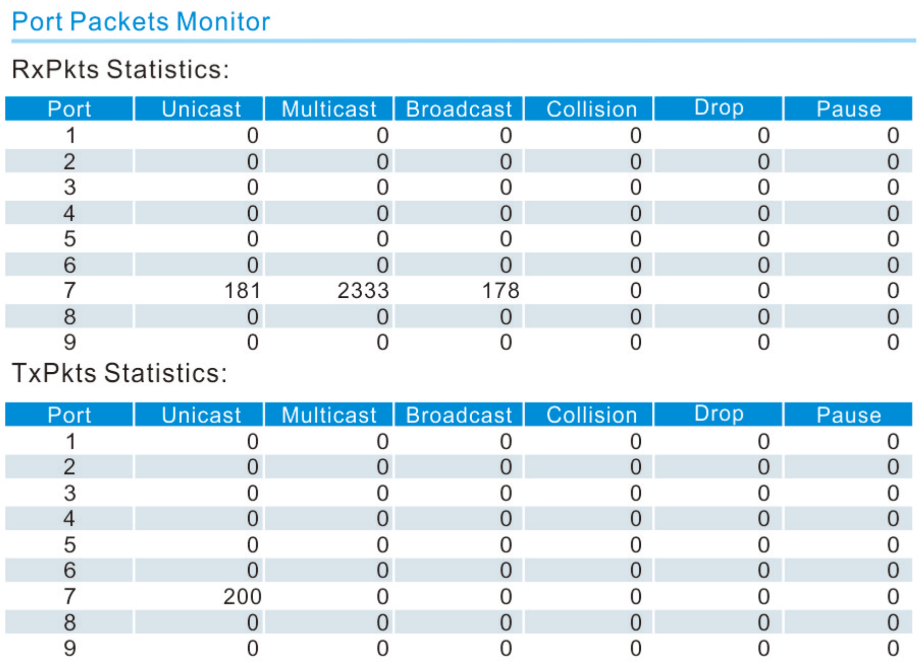
Port	Warning Type	Port Status
1	No warning	Link Down
2	No warning	Link Down
3	No warning	Link Down
4	No warning	Link Down
5	No warning	Link Down
6	No warning	Link Down
7	No warning	Link Down
8	No warning	Link Down
9	No warning	Link Down

6.6 Performance Monitoring

This chapter will describe how to view performance parameters for managed series of switches, the use of which can provide professional data for users to analyze and monitor the switches performance.

6.6.1 Information Packet Statics

Managed series of switches conduct each port monitoring, and send all network data packets and display them in Web page. The statics start Statistics Package as soon as switches power on, when switch soft reset and power down and reset, the data will zero. When opening the page as below, the page will be refreshed ever 30 seconds .Please refer to the page below for detailed data display:



Port Packets Monitor

RxPkts Statistics:

Port	Unicast	Multicast	Broadcast	Collision	Drop	Pause
1	0	0	0	0	0	0
2	0	0	0	0	0	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	181	2333	178	0	0	0
8	0	0	0	0	0	0
9	0	0	0	0	0	0

TxPkts Statistics:

Port	Unicast	Multicast	Broadcast	Collision	Drop	Pause
1	0	0	0	0	0	0
2	0	0	0	0	0	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	200	0	0	0	0	0
8	0	0	0	0	0	0
9	0	0	0	0	0	0

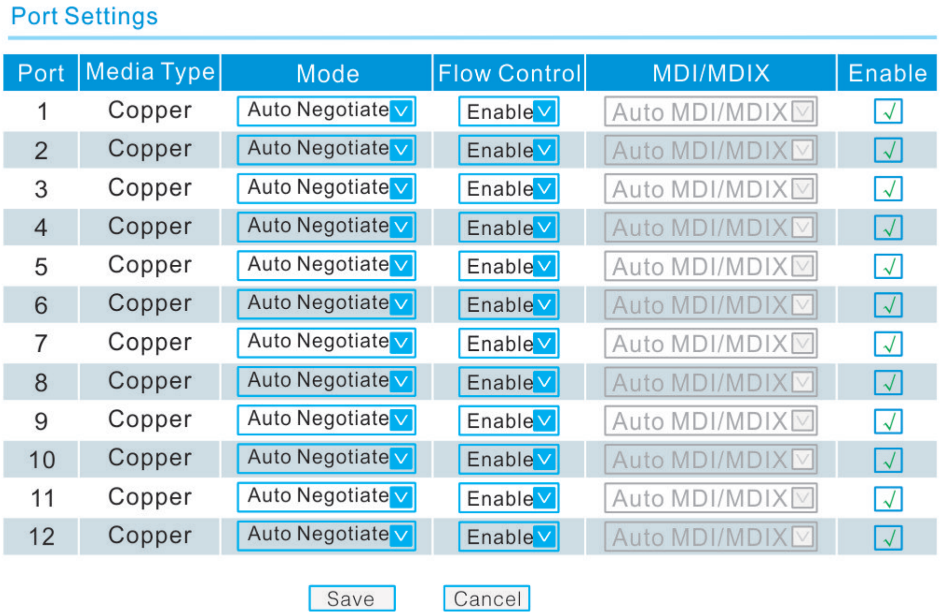
If click **“Save”**, an E-mail will be sent immediately. The parameters in table below are for your reference.

Item	Description	Default
Error	Rx（Receive）	The number of data packets received by mistake, such as data has bad FCS or the length is more than1537
Drop	Rx（Receive）	When MAC address safe control is enabled. The number of data packets that are thrown away for safety
Pause	Rx（Receive）	The number of data packets one port receives pause frames
Unicast	Tx（Send） Rx（Receive）	The number of one certain data packet received and sent by each port , such as the number of unicast, multicast and broadcast data packets received
Multicast	Tx（Send） Rx（Receive）	The number of one certain data packet received and sent by each port, such as the number of unicast, multicast and broadcast data packets received
Broadcast	Tx（Send） Rx（Receive）	The number of one certain data packet received and sent by each port, such as the number of unicast, multicast and broadcast data packets received
Collisions	Tx（Send）	The number of times collision occurs to one port when transmit data
Drop	Tx（Send）	Data packet is thrown away as resource is short or MAC Layer transmission issue, called Drop. When it occurs for one time, the value will be added 1.
Pause	Tx（Send）	The number of pause frame one port send

6.6.2 MAC Address List

In computer network, media access control address (MAC Address), hardware address and adapter address are only ID mark attached to most network adapter. For example, two different computers network cards have two different MAC address. One computer has a number of network cards, such as Ethernet Card, wireless network card, which will have different MAC addresses. The MAC address is sole, don’t modify, even though you can modify, it’s better not to.

Managed series of switches provide 8K MAC Address List for automatic learning and aging treatment. In the following Web page, you can view all MAC address.



Port Settings

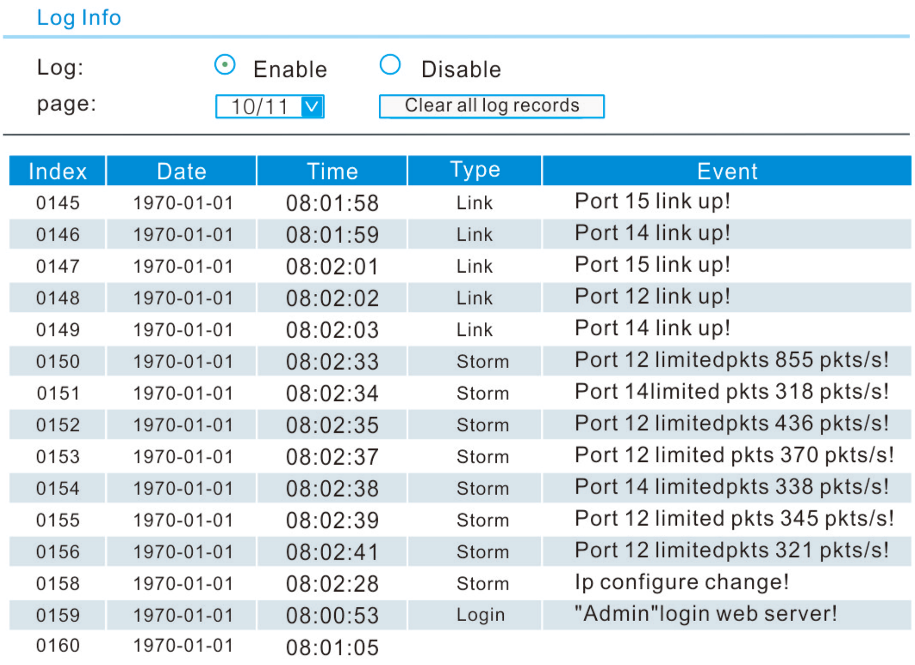
Port	Media Type	Mode	Flow Control	MDI/MDIX	Enable
1	Copper	Auto Negotiate	Enable	Auto MDI/MDIX	✓
2	Copper	Auto Negotiate	Enable	Auto MDI/MDIX	✓
3	Copper	Auto Negotiate	Enable	Auto MDI/MDIX	✓
4	Copper	Auto Negotiate	Enable	Auto MDI/MDIX	✓
5	Copper	Auto Negotiate	Enable	Auto MDI/MDIX	✓
6	Copper	Auto Negotiate	Enable	Auto MDI/MDIX	✓
7	Copper	Auto Negotiate	Enable	Auto MDI/MDIX	✓
8	Copper	Auto Negotiate	Enable	Auto MDI/MDIX	✓
9	Copper	Auto Negotiate	Enable	Auto MDI/MDIX	✓
10	Copper	Auto Negotiate	Enable	Auto MDI/MDIX	✓
11	Copper	Auto Negotiate	Enable	Auto MDI/MDIX	✓
12	Copper	Auto Negotiate	Enable	Auto MDI/MDIX	✓

Web display page, MAC Address List can assign types of sorts, select from **“Auto”**, **“Port”** and **“MAC”**, three types of sorts. MAC Address and related forwarding port will display in this table. If Status column display **“Static”**, suggesting MAC address is static, static address do aging treatment. If using static multicast MAC address or IGMP Snooping, multicast address can be found in this MAC Address List.

6.6.3 Log

Managed series of switches provide Log function, which can be easily enable and disable. Factory default is disabling the function. When enabling the function, if the following event occurs, it will be recorded in event list of switches.

☆ System Reboot	☆ Port Link Down / Link UP
☆ Power Status Change	☆ Login Information
☆ Broadcast Storm Occurs	☆ System Action and Operation Record
☆ Ring Net Status Change	☆ NTP Time Synchronization



Log Info

Log: ● Enable ○ Disable

page: 10/11 Clear all log records

Index	Date	Time	Type	Event
0145	1970-01-01	08:01:58	Link	Port 15 link up!
0146	1970-01-01	08:01:59	Link	Port 14 link up!
0147	1970-01-01	08:02:01	Link	Port 15 link up!
0148	1970-01-01	08:02:02	Link	Port 12 link up!
0149	1970-01-01	08:02:03	Link	Port 14 link up!
0150	1970-01-01	08:02:33	Storm	Port 12 limitedpkts 855 pkts/s!
0151	1970-01-01	08:02:34	Storm	Port 14limited pkts 318 pkts/s!
0152	1970-01-01	08:02:35	Storm	Port 12 limitedpkts 436 pkts/s!
0153	1970-01-01	08:02:37	Storm	Port 12 limited pkts 370 pkts/s!
0154	1970-01-01	08:02:38	Storm	Port 14 limitedpkts 338 pkts/s!
0155	1970-01-01	08:02:39	Storm	Port 12 limited pkts 345 pkts/s!
0156	1970-01-01	08:02:41	Storm	Port 12 limitedpkts 321 pkts/s!
0158	1970-01-01	08:02:28	Storm	Ip configure change!
0159	1970-01-01	08:00:53	Login	"Admin"login web server!
0160	1970-01-01	08:01:05		

Just as the page above display, each page of Log information has 16 event records. View more log record by switching to different pages. If Log function is disabled, drop-down list box will become grey, event log will not be added. Log function save all record in nonvolatile Flash chips, which can save 2000 record at most, when more than 2000, old records will be deleted, new ones will be added.

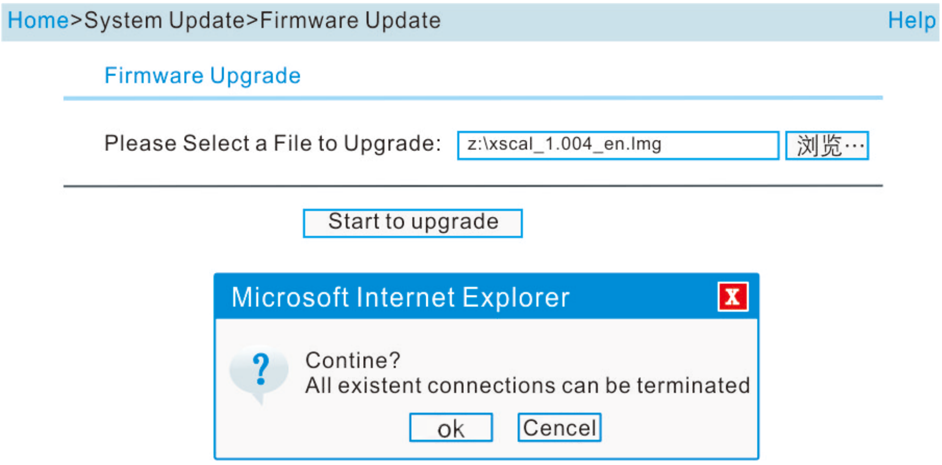
6.7 System Update and Back-up

In this chapter, such functions as Firmware Upgrade (Update), parameter backup and restoring for switch setting, factory default

6.7.1 Firmware Update

Latest firmware will be obtained from our company's system WEB, upgrade switch following the steps below:

- Click **"Browse"**, open Firmware File (*.img) .
- Click **"Start to upgrade"**, message box will prompts, if clicking **"OK"** in it, start to upgrade, if clicking **"Cancel"**, Quit upgrading Firmware upgrading will last for a period of time till switches restart.
- When you see **"Overview"** Web page, it suggests firmware upgrading is completed, you can see updated version information in **"Overview"** page:



Home>System Update>Firmware Update

Firmware Upgrade

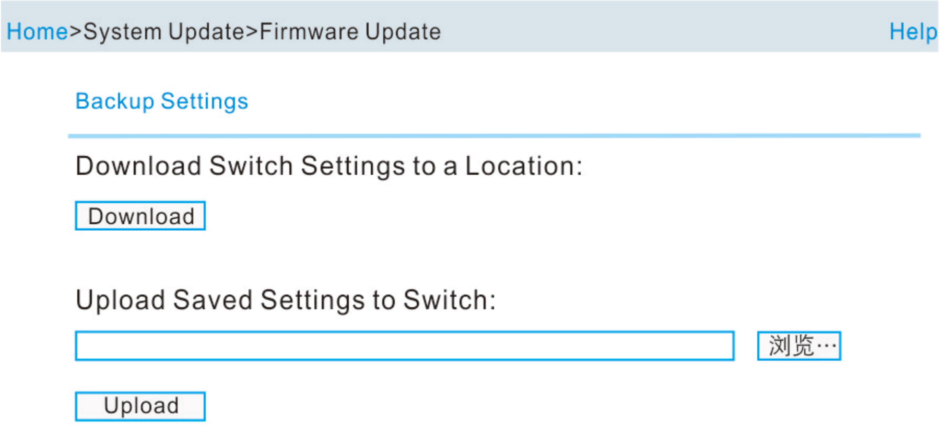
Please Select a File to Upgrade: z:\xscal_1.004_en.Img

Microsoft Internet Explorer

Contine?
All existent connections can be terminated

6.7.2 Setting Parameter Backup

Setting information for managed series of switches can be saved in one PC or restore data setting from one PC if backup setting parameters to PC, click “Download”, a saving dialogue box prompts , select a proper file and save setting parameters in PC. Please refer to the screenshot below:



Home>System Update>Firmware Update Help

Backup Settings

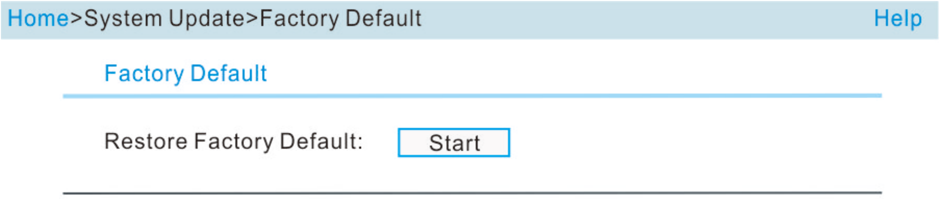
Download Switch Settings to a Location:

Upload Saved Settings to Switch:

Restore original setting information from PC in switch, click **“Browse”**, open a setting file （*.cfg）, then click **“Upload”**, restore parameters to the original setting. After finish recovering, switches need to reboot.

6.7.3 Restore

To restore factory default can restore factory default quickly. Click **“Start”** in Web page, select **“OK”** in confirmation information box prompted, and factory default can be restored. After finishing restoring, switches need to reboot.



Home>System Update>Factory Default Help

Factory Default

Restore Factory Default:

7

Maintenance and Service

From the date of product shipment, we are happy to provide you with a one-year guarantee. According to product specification, within the guarantee period, if the products are faulty or if the function operation fails, we will repair or replace the item at no extra cost.

Please note that this commitment will not apply if the damage is caused by improper use, accidents, natural disaster, invalid operation or incorrect installation.

To ensure the consumer benefits from the use of our managed switches, you can get further support through the following ways:

7.1 Internet Service

You can get more information from our Technical Support Team.

7.2 Call to Technical support

Users can call our Technical Support team, where a professional engineer will be happy to assist you with your questions.

7.3 Product Repairing and Replacing

Our service team will be able to confirm if you require a replacement or a repair, and once you have this information you are to contact your sales rep for further assistance.

8

Appendix

8.1 SNMP Performance Parameters

Managed series of switches provide SNMP Agent to manage switch device, the switches support the following RFCs:

RFC 1157-SNMP protocol
RFC 1215-Traps for SNMP
RFC 1213-MIB-2
RFC 1573-IF-MIB
RFC 1643-Interface MIB
MIB groups:
system Group
sysDescr
sysObjectID
sysUpTime
sysContact
sysName
sysLocation
sysServices
sysORLastChange
sysORID
sysORDescr
sysORUpTime
Interfaces Group
ifNumber
ifIndex
ifDescr
ifType
ifMtu
ifSpeed
ifPhysAddress
ifAdminStatus
ifOperStatus
ifLastChang
ifInOctets
ifInUcastPkts
ifInNUcastPkts
ifInDiscards
ifInErrors
ifInUnknownProtos
ifOutOctets
ifOutUcastPkts
ifOutNUcastPkts
ifOutDiscards
ifOutErrors
ifOutQlen
ifSpecific
At Group
atIfInde
atPhysAddress
atNetAddress
IP Group
ipForwarding
ipDefaultTTL
ipInReceives
ipInHdrErrors
ipInAddrErrors
ipForwDatagrams
ipInUnknownProtos
ipInDiscards
ipInDelivers
ipOutRequest
ipOutDiscards
ipOutNoRoutes
ipReasmTimeout
ipReasmReqds
ipReasmOKs
ipReasmFails
ipFragOKs
ipFragFails
ipFragCreates
ipAdEntAddr
ipAdEntIfIndex
ipAdEntNetMask
ipAdEntBcastAddr
ipAdEntReasmMaxSize
ipRouteDest
ipRouteIfIndex
ipRouteMetric
ipRouteNextHop
ipRouteType
ipRouteProto
ipRouteAge
ipRouteMask
ipRouteMetric
ipRouteInfo
ipNetToMediaIfIndex
ipNetToMediaPhysAddress
ipNetToMediaNetAddress
ipNetToMediaType
ipRoutingDiscards
TCP Group
tcpRtoAlgorithm
tcpRtoMin
tcpRtoMax
tcpMaxConn
tcpActiveOpens
tcpPassiveOpens

tcpAttemptFails
tcpEstabResets
tcpCurrEstab
tcpInSegs
tcpOutSegs
tcpRetransSegs
tcpConnState
tcpConnLocalAddress
tcpConnLocalPort
tcpConnRemAddress
tcpConnRemPort
tcpInErrs
tcpOutRsts
ICMP Group
icmpInMsgs
icmpInErrors
icmpInDestUnreachs
icmpInTimeExcds
icmpInParmProbs
icmpInSrcQuenchs
icmpInRedirects
icmpInEchos
icmpInEchoReps
icmpInEchoReps
icmpInTimestamps
icmpInTimestampReps
icmpInAddrMasks
icmpInAddrMaskReps
icmpOutMsgs
icmpOutErrors
icmpOutDestUnreachs
icmpOutTimeExcds
icmpOutParmProbs
icmpOutSrcQuenchs
icmpOutRedirects
icmpOutEchos
icmpOutEchoReps
icmpOutTimestamps
icmpOutTimestampReps
icmpOutAddrMasks
icmpOutAddrMaskReps

UDP Group
udpInDatagrams
udpNoPorts
udpInErrors
udpOutDatagrams
udpLocalAddress
udpLocalPort
SNMP Group
snmpInPkts
snmpOutPkts
snmpInBadCommunityNames
snmpInBadCommunityUses
snmpInASNParseErrs
snmpInTooBigs
snmpInNoSuchNames
snmpInBadValues
snmpInReadOnlys
snmpInGenErrs
snmpInTotalReqVars
snmpInTotalSetVars
snmpInGetNexts
snmpInGetRequests
snmpInResponses
snmpInTraps
snmpOutTooBigs
snmpOutNoSuchNames
snmpOutBadValues
snmpOutGenErrs
snmpOutGetRequests
snmpOutGetNexts
snmpOutSetRequests
snmpOutGetResponses
snmpOutTraps
snmpEableAuthenTraps
snmpSilentDrops
snmpProxyDrops