



16+8 Industrial Managed Ethernet Fiber Switch

User Guide

 RLH Industries, Inc.

Copyright © 2014 RLH Industries, Inc. All rights reserved.

No part of this document may be copied or distributed without permission.

The RLH logo may not be used for commercial purposes without the prior written consent of RLH and may constitute trademark infringement.

Other company and product names mentioned herein are trademarks of their respective companies. Mention of third-party products is for informational purposes only and constitutes neither an endorsement nor a recommendation. RLH assumes no responsibility regarding the performance or use of these products.

The information contained in this document is the property of RLH Industries, Inc. and may not be reproduced or disseminated to third parties without the express written permission of RLH.

Every effort has been made to ensure that the information in this manual is accurate. RLH is not responsible for printing or clerical errors. Because we are constantly seeking ways to improve our products, specifications and information contained in this document are subject to change without notice.

RLH Industries, Inc.
936 North Main Street
Orange, CA 92867

Ph. 714 532-1672
email: info@fiberopticlink.com
www.fiberopticlink.com

Contents

1. Important Information

Intended Audience	6
Conventions	6
General Safety Practices	6

2. Introduction

Product Description	7
Standard Features	7
Application Diagram	8
Front Panel	8
Front Panel Components	8
Front Panel LEDs	9
Rear Panel	9
Rear Panel Components	9
Power Input	9
Download Program Port	10
Communication Ports	10
10Base-T /100Base-TX Ethernet ports	10
100Base-FX fiber port	11

3. Before Installing

Observe Special Handling Requirements	12
Be careful when handling electronic components	12
Guidelines for handling terminated fiber cable	12
Prepare for Installation	13
Check for shipping damage	13
Verify system contents	13
Verify matching optical module and fiber modes	13
Site Requirements	14
Site selection	14
Required power sources	14

4. Quick Start Guide

Easy Installation	15
Install the Switch	15
Connect power	15
Connect fiber cables	15
Connect ethernet cables	15

5. Configuring the System

Managing with Hyper Terminal	16
Modification of IP Address	17
Web Management	18
Network Setting	18
Startup and Log in	19
System Status	20
System Status	21
Port Configuration	23
Broadcast Storm Suppression	26
L2 Features	27
VLAN	27
Port based VLAN	28
IEEE 802.1Q VLAN	28
IGMP Snooping	30
Qos	32
QOS Classification	32
Default Priority	32
COS	33
DSCP	33
Redundancy	34
Single Ring Configuration of Ring V2	37
Coupling Ring Configuration of Ring V2	38
Ring V3 Coupling	40
Ring V3 Chain Configuration	41
Access Control	42
Access Profile	43
Static Unicast FWD	44
Static MAC Address	44

Port Statistics	46
Rx Frame Statistics	46
Tx Frame Statistics	47
Traffic Statistics	48
MAC Address	48
Diagnosis	50
Port Mirroring	50
Diagnosis	51
System	52
Device IP	52
IP Address	52
Subnet Mask	52
Default Gateway	53
DNS Address	53
System File Update	53
Logout Exit from the WEB interface.	55
Default Settings	57

6. Specifications

General Specifications	58
-------------------------------	-----------

7. Troubleshooting

First Step: Isolate the problem	59
Common Issues	59

8. Ordering Information

Part Number and Configurations	60
---------------------------------------	-----------

9. Support

Technical Support	61
Contact Information	61

1. Important Information

Intended Audience

This manual is intended for use by knowledgeable telco/network installation, operation and repair personnel. Every effort has been made to ensure the accuracy of the information in this manual is accurate. However, due to constant product improvement, specifications and information contained in this document are subject to change without notice.

Conventions

Symbols for notes, attention, and caution are used throughout this manual to provide readers with additional information, advice when special attention is needed, and caution to prevent injury or equipment damage.



Notes: Helpful information to assist in installation or operation.



Attention: information essential to installation or operation.



Caution: Important information that may result in equipment damage or injury if ignored.

General Safety Practices

The equipment discussed in this manual may require tools designed for the purpose being described. RLH recommends that installation and service personnel be familiar with the correct handling and use of any equipment used, and follow all safety precautions including the use of protective personal equipment as required.

Caution - Severe Shock Hazard

- Never install during a lightning storm or where unsafe high voltages are present.
- Active T1 lines carry high DC voltages up to 56V. Use caution when handling T1 wiring.

Laser Safety

- Radiation emitted by laser devices is dangerous to human eyes.
- Avoid eye exposure to direct or indirect radiation.
- Do not operate without fiber cable attached or dust caps installed.

2. Introduction

Product Description

The RLH Managed Ethernet Switch is a smart managed switch that offers 16 10/100Base-T(x) RJ-45 TCP ports together with 8 100Base-FX fiber connectors. The optical interfaces may be dual fiber single mode or multimode, or bi-directional single fiber, and have a transmission up to 120Km/74 miles.

The switch can be managed through its imbedded Web Interface, with simplified settings accessible through the console port, and also supports external alarm functions for alarm input monitor purposes. It supports Port based VLAN and IEEE802.1Q VLAN, VLAN groups and VLAN IDs can be created. It also supports Broadcast storm control, Port bandwidth control, QOS, etc.

The switch may be used to establish SW-Ring for accomplishing redundancy for an Ethernet ring network topology. The intelligent redundancy system has a short self-recovery time for automatic recovery of the network section.

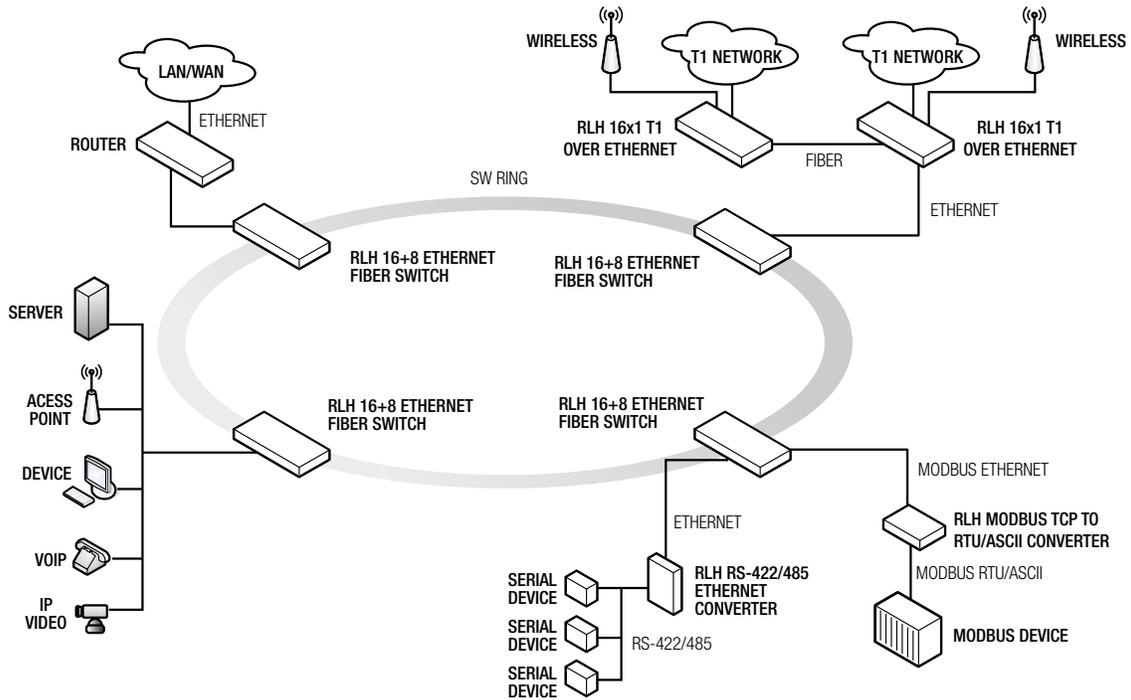
The RLH Managed Ethernet Switch uses only 1RU and comes complete with EIA19" rack ears for rack mount applications, or it may be used on a desktop or shelf. The fiber optic ports allow for Ethernet network extension over long distances, and fiber optic cable provides electrical isolation between devices. It is ideal for institutional use, medium/small enterprises and intelligent community networks that need to accommodate various services such as video, VOIP and high speed data over fiber.

The RLH 16+8 Ethernet Switch comes complete with an internal 115/220VAC power supply, and is covered by a 5 year warranty.

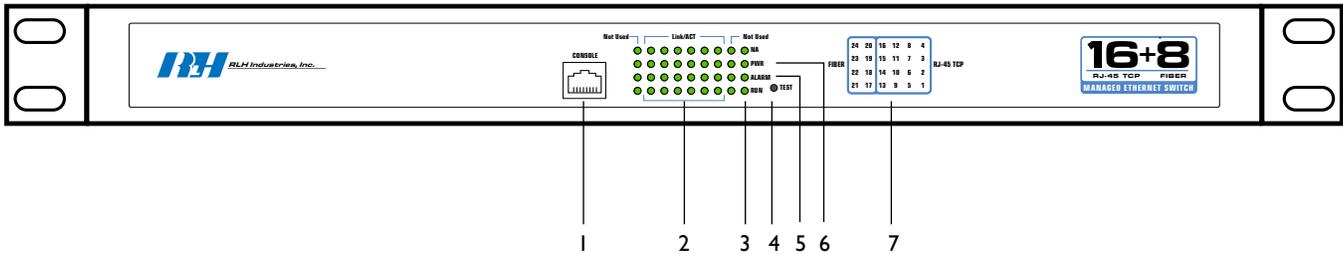
Standard Features

16 port 10/100M TCP ports & 8 100Base FX fiber ports.	Port mirroring for online debugging and monitoring network status.
IEEE 802.3, IEEE 802.3u, IEEE 802.3ad, IEEE 802.3z, IEEE 802.1w, IEEE 802.1D, IEEE 802.1x compliant.	Supports port trunk function and 3 groups of trunking links, port mirroring, port priority, TOS priority.
Supports IEEE 802.3x flow control for full-duplex mode and collision-based back-pressure for half-duplex mode.	Supports SW-Ring technology SW-Ring patented technology (self-recovery time <20ms).
RJ-45 ports are auto MDI/MDIX, auto negotiating.	Supports 8K MAC addressing.
IEEE802.1P QoS, WRR and DSCP.	IGMP snooping for filter multicast.
Supports IP address setting and dynamic learning (DHCP).	Built-in power supply, 115/220VAC.
No fan, low consumption design.	19" 1RU rack mount steel enclosure, Industrial grade 4 design.
-40°F to +167°F (-40°C to +75°C) operating temp.	Rugged with high strength shell with IP30 protection.

Application Diagram



Front Panel



Front Panel Components

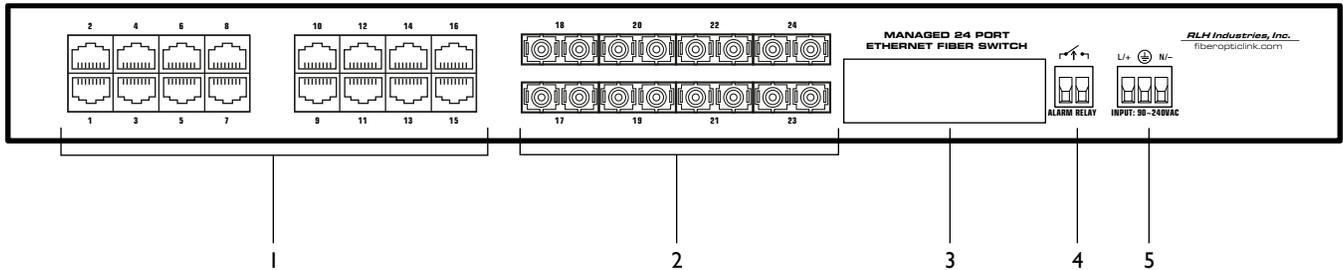
Item	Description
1	Console Port
2	Link/ACT LED indicators
3	RUN LED
4	Test Button
5	ALARM LED
6	PWR LED
7	Link/ACT LED port identifier table

Front Panel LEDs

LED	Color	State	State
PWR	GRN	ON	Power is working normally
		OFF	Power is not connected or not operating normally
RUN	GRN	Blinking	System is operating normally
		OFF	System is not connected or operating normally
ALARM	GRN	ON	Alarm condition is detected and alarm relay is closed
		OFF	No alarm condition present and alarm relay is open
Link/ACT	GRN	ON	Network connection of the port is valid
		Blinking	Activity is detected and data is being transmitted
		OFF	Network connection of the port is not valid

Note: The alarm condition is set through the management software.

Rear Panel

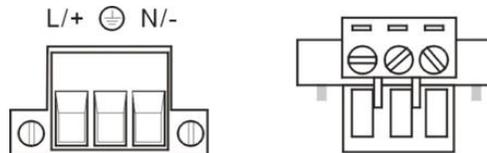


Rear Panel Components

Item	Description
1	100BaseT(X) Ethernet Ports
2	100Base-FX Fiber Optic Ports
3	Model number and MAC address
4	Alarm terminal block (Normally open)
5	Power terminal block

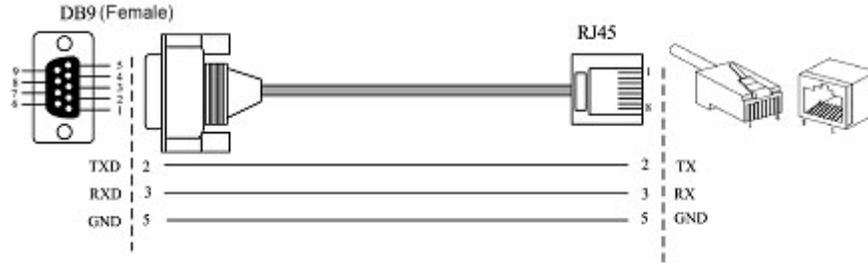
Power Input

A 3 position terminal block on back panel is used for 100-240VAC/DC.



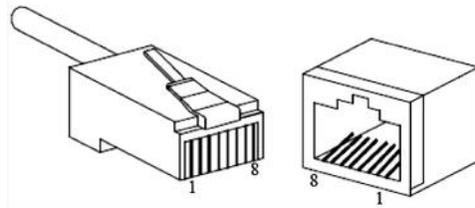
Download Program Port

The RLH fiber switch has 1 download program port (RJ45 type) designated CONSOLE on the front panel, It manages the system with PC through RJ45-DB9F adapter.



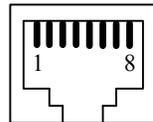
Communication Ports

The switch has 16 10/100BaseT(X) Ethernet ports and 8 100M fiber ports. The pinout of the RJ45 ports connect to UTP or STP. The cable length may not be more than 100m. 100Mbps Ethernet connector takes 100Ω of UTP 5, 10Mbps Ethernet connector takes 100Ω of UTP 3, 4, 5.



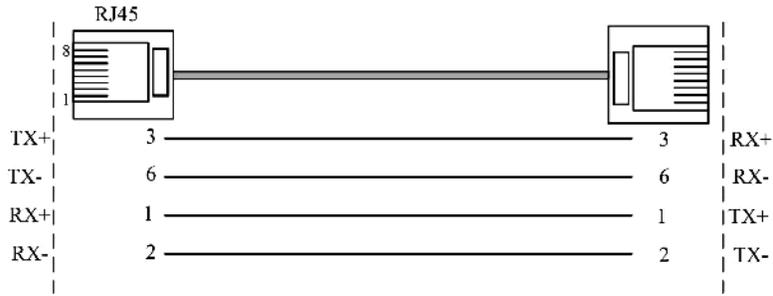
10Base-T /100Base-TX Ethernet ports

The RJ45 ports support auto MDI/MDI-X connections. It can connect directly to PCs, Servers, Converters and HUBs. Corresponding connection of Pin 1,2,3,6 is like this: 1→3, 2→6, 3→1, 6→2. The Pin-out definition is displayed as below.

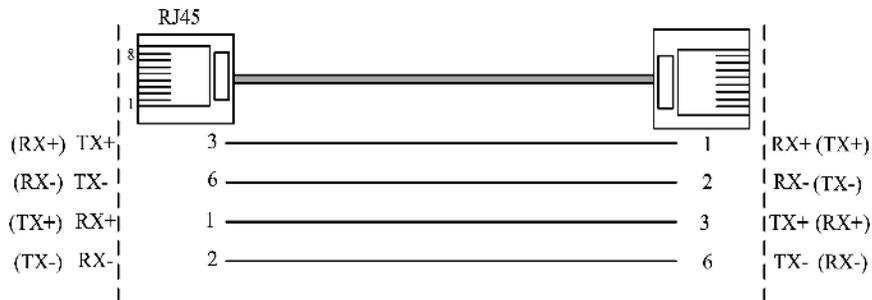


PIN	MDI	MDI-X
1	TX+	RX+
2	TX-	RX-
3	RX+	TX+
6	RX-	TX-
4, 5, 7, 8	—	—

MDI (straight-through cable):



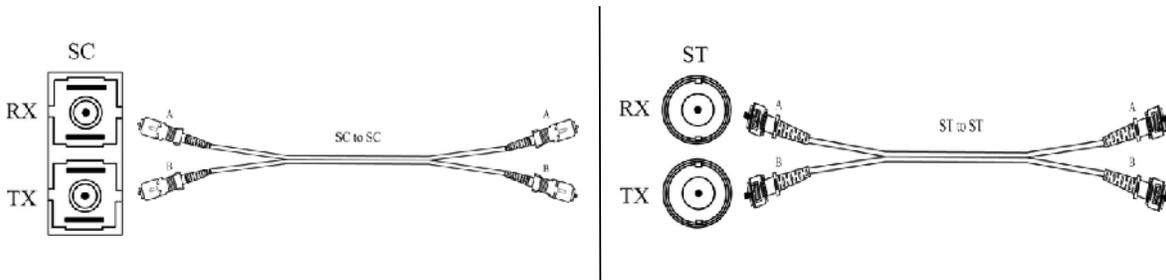
MDI-X (Cross over cable):



100Base-FX fiber port

100Base-FX port works with full-duplex, SM or MM SC/ST. The fiber port may contain single fiber bidirectional connectors, or dual fiber connectors. Dual fiber connectors must be used in pairs. The TX (transmitting) port connects to the remote switch's RX (receive) port; RX (receiving) port connects to the remote switch's TX (transmitting) port.

We advise to label the two sides of the cable with the same letter (A-to-A and B-to-B, shown as below, or A1-to-A2 and B1-to-B2, etc.).



3. Before Installing

Observe Special Handling Requirements

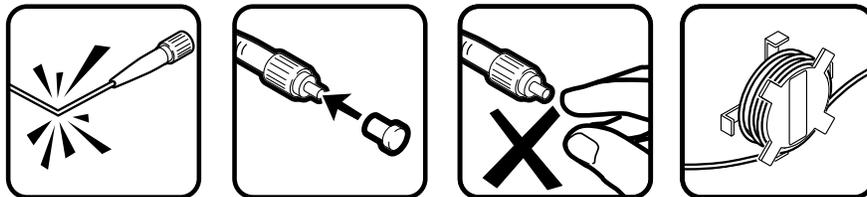
Be careful when handling electronic components



- This product contains static sensitive components.
- Handle the modules by their faceplates only, do not touch the circuit boards or components.
- Follow proper electrostatic discharge procedures.

This contains components that may be damaged by static electricity. When transporting modules, carry it in an ESD safe container such as the antistatic bag provided with the module. Before installing or replacing modules, discharge yourself of static electricity by physical bodily contact with earth ground. When handling modules, hold by the faceplate only and avoid touching circuitry. Failure to follow ESD precautions may cause serious damage to the modules and prevent proper operation.

Guidelines for handling terminated fiber cable



- Do not bend fiber cable sharply. Use gradual and smooth bends to avoid damaging glass fiber.
- Keep dust caps on fiber optic connectors at all times when disconnected.
- Do not remove dust caps from unused fiber.
- Keep fiber ends and fiber connectors clean and free from dust, dirt and debris. Contamination will cause signal loss.
- Do not touch fiber ends.
- Store excess fiber on housing spools or fiber spools at site

Prepare for Installation

Check for shipping damage

Carefully unpack and inspect the unit and accessories. Contact RLH immediately if any components are damaged or missing. Electronic components, fiber optic cable, and accessories have special handling requirements to prevent damage and enhance system reliability.

If the switch will be relocated in the future, save the cartons and protective packaging material.

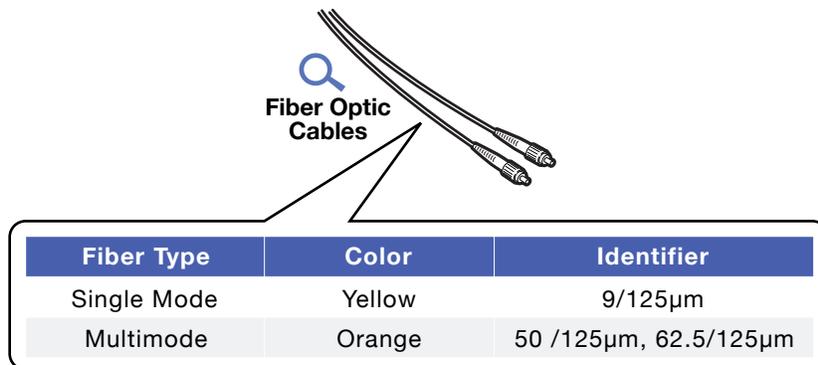
Verify system contents

The following items are shipped with your RLH Fiber Switch (as applicable)

- User manual
- AC power converter and cord
- Serial cable adapter for use with the console port
- Rack mount ears and attaching hardware
- Rubber feet for table or self mount applications

Verify matching optical module and fiber modes

Fiber mode and optical module mode must be the same. Test the fiber cables before installation.



Site Requirements

Site selection

Locate the switch to allow easy access to the equipment. Leave at enough clearance in the front and rear to gain access to the fiber, ethernet alarm and power connections. Typical application environments

Route the fiber optic cable to the installation area before installing the switch.

Required power sources

You will need an acceptable power source. The RLH Fiber Switch accepts 90 ~ 280VAC (50/60Hz).

The F.C.C. requires telecommunication equipment to withstand electrical surge that may result from lightning strikes. This equipment has been tested and found to comply with the F.C.C. requirement. Users should follow the precautions below to insure the safety and minimize the risk of damage to the equipment

Make sure that the AC power outlet is properly grounded. Proper grounding should include a minimum of a grounded rod buried outside the building at least 8 feet (2.44 meters) deep.

4. Quick Start Guide

Easy Installation

Before starting

- Review the safety information in section [1. Important Information](#)
- Familiarize yourself with the fiber switch as described in section [2. Introduction](#)
- Know how to handle fiber optic cable, have a suitable installation environment with the correct power, as described in section [3. Before Installing](#)

Install the Switch

The switch is pre-configured at the factory for general application, and will operate without any setup. For additional configuration instructions please refer to [5. Configuring the System](#).

- Mount the switch in a 19" equipment rack, on a shelf or table

Connect power

Remove power from AC mains supply. Connect the AC power cord to the terminals on the switch and plug into 110/240VAC, 50/60Hz mains outlet.

- Alternately, wire AC mains power directly from AC power source to the power terminals.

Connect fiber cables

- The fiber cable(s) must be the correct type of cable, with the correct connectors and suitable length.
- Attach the connector(s) carefully using care to avoid bending the fiber cable too sharply and damaging the fiber.
- Do not touch fiber connector ends which could cause contamination and lower signal performance.



Radiation emitted by laser devices is dangerous to human eyes. Avoid eye exposure to direct or indirect radiation. **Do not operate without fiber cable attached or dust caps installed.**

Connect ethernet cables

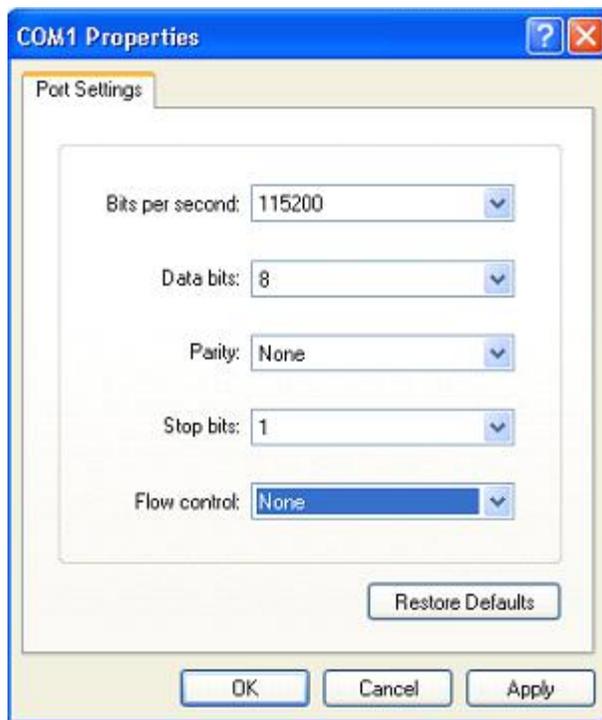
- Attach ethernet cables to the RJ-45 ethernet ports labeled 1 through 16 on the rear panel of the switch. Start the system

5. Configuring the System

Managing with Hyper Terminal

Connect the switch to a PC running Windows®, then open Hyper Terminal: Start->Program->Attachment->Communication.

Make a new connection when opening Hyper Terminal. The communication port needs to connect the PC to the switch. It must use the following configuration parameters: Bits per second: 115200, Data bits: 8, Parity: None, Stop bits: 1, Flow control: None.



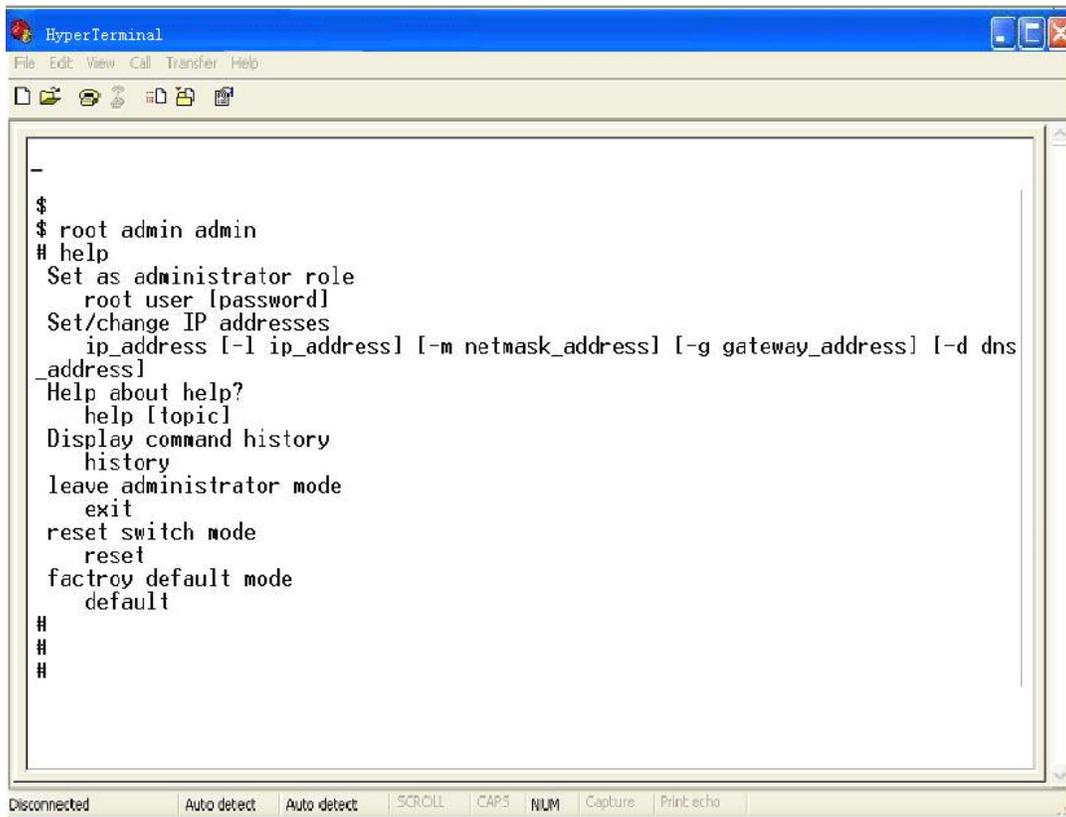
Connection Screen

Connection Notes

- If the computer doesn't have a serial port, you can use a USB to serial converter and the settings are the same.
- Name of serial device can be chosen according to properties of hardware device.
- After Hyper Terminal is connecting, if there is no response with pressing "Enter" continuously, please make sure the cable is connected. Status indicator of CPU is blinking means the device can work normally. PING the managed address in Hyper Terminal, if the switch is not connecting to the PC, please contact our engineers.

Modification of IP Address

When Hyper Terminal is finished, you can see the following screen:



```
HyperTerminal
File Edit View Call Transfer Help
-
$
$ root admin admin
# help
Set as administrator role
  root user [password]
Set/change IP addresses
  ip_address [-l ip_address] [-m netmask_address] [-g gateway_address] [-d dns
address]
Help about help?
  help [topic]
Display command history
  history
leave administrator mode
  exit
reset switch mode
  reset
factory default mode
  default
#
#
#
```

Terminal Window

\$\$ means user enters into restricted privileges mode;

means user enters into manager mode;

The two modes use command root and command exit to switch mode. The default password of the switch is "admin: admin". Command root uses "root user [password]". Command "exit" is to exit manager mode.

If you don't know IP address of the device, please input "ip_address" to show the IP address of the device.

Command of "ip_address" without parameter don't need manager privilege. Command of "ip_address" with parameter need manager privilege to configure IP address, subnet mask, default gateway and DNS server. The format of the command is as follows:

ip_address [-l ip_address] [-m net mask_address] [-g gateway_address] [-d dns]

Input the command "ip_address -l 192.168.1.10" in manager mode to modify the IP address to 192.168.1.10. The default subnet mask is "225.255.255.0".

Web Management

The RLH-ESMXXX-XX-X series switch supports Web management.

It is very intuitive to manage and maintain the equipment through Web interface. Before configuring the switch, please ensure necessary software installed your computer and reasonable configuration of the network.

The lowest requirement for user's computer is as below:

- Install operating system (Windows XP/2000,etc)
- Install Ethernet card
- Install Web explorer (IE6.0 or higher version)
- Install and start TCP/IP protocol

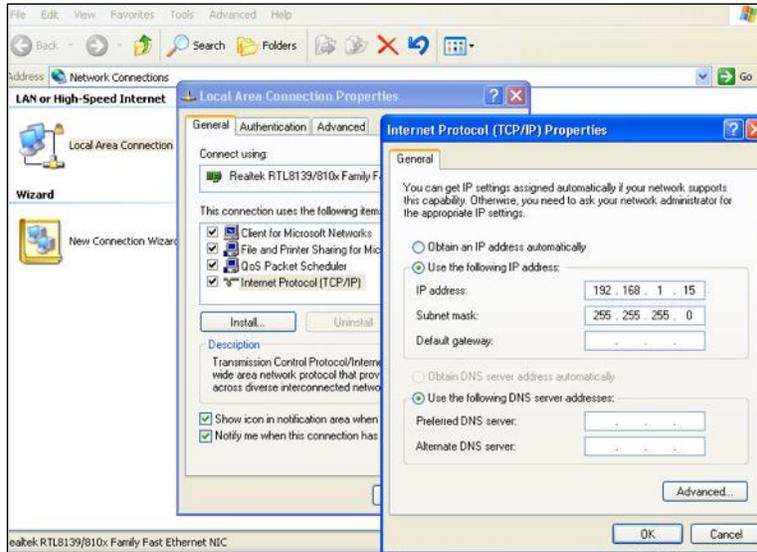
Network Setting

The switch's default address is: **192.168.1.254**, subnet mask is: **255.255.255.0**. When entering into the Web interface through internet explorer, the IP address of switch and PC must be in the same Local Area Network.

You can modify PC's or the switch's IP address to make sure that they are in the same Local Area Network. Operating process can follow method 1 or method 2 as below,

Method 1: Modify PC's IP address

- Set DIP switch 1 to ON. Restart the power of the switch and set DIP switch 1 to OFF. Restore the device to default settings. (The device's IP address is probably changed, this step can restore devices' IP address to default address.)
- Click Start->Control panel->network connections->Local area Connection->Properties->Internet protocol (TCP/IP)Setting PC's IP address: 192.168.1.X (X is less than 254, from 2 to 253).
- Click "OK", IP address modifies successfully. The Windows operation interface is shown below:



TCP/IP Properties Screen

Startup and Log in

Open IE, input `http://192.168.1.254` in the address field, click “Enter” as shown below:



Input correct user name and password, then enter successfully (default user name is “admin”, password is “admin”). If user name or password input incorrectly in 3 times continuously, you must login again.

Note: User name and password are case-sensitive.

System Status

Menu Introduction

Menu Bar consists of 8 parts: system status, port configuration, L2 Feature, Qos, Redundancy, Monitor, Port Statistics, Diagnosis and basic settings.

Main Menu	Tag	Function
System Status	Overview	Show device information and port information such as software version, IP address, etc.
Port Configuration	Port settings	Display and configure each port's basic information of switch, like link status, speed mode, flow control status, etc.
	Bandwidth management	Set up the maximum speed rate of data
	Storm suppression	Set up type of flow of the port storm suppression
	VLAN	Display the list of 802.1Q VLAN, and configure and manage 802.1Q VLAN.
	IGMP Snooping	Display the list of based on port VLAN, configure and manage based on port VLAN.
	Static Multicast FWD	Set up MAC address of static multicast and corresponding port.
QoS	Qos Classification	Set up QOS queue mode, implement of QOS and default port priority.
	Cos	Set up the meaning of COS value.
	DSCP	Set up DSCP priority.
Redundancy	Port Trunking	Setup trunking group of the port
	Rapid Ring	It possess redundant communication in industrial network.
Access Control	Login Settings	Setup user names and passwords with different privilege
	Access profile	Set up login mode and accessible IP
	Static Unicast FWD	Set up static unicast address and its corresponding port
Port statistics	Rx frame statistics	Status of the recieved frames
	Tx frame statistics	Status of the transmitted frames
	Traffic statistics	Show total number of the transmitted and received messages
	MAC address table	List of MAC address
Diagnosis	Mirror	Setup mirror port and monitored port
	Diagnosis	Setup PING some host address
System	Device IP	Device IP, gateway and DNS, etc.
	System update file	Software update, achieve, save or restore the configuration of switch.
	Logout	Exit from the WEB interface

Web Overtime Handling

If user doesn't operate the Web interface for a long time, The system will cancel this login (but configuration change made in this login will be saved in Web configuration interface). If the user wants to do any operating

on Web configuration interface again, the system will remind user and return to the login dialog box. Users need to log in again if operating is needed.

System Status

Device Information mainly display the basic information of RLH-XXXXXX-XX-X series switch including: Name, Serial No., Description, Contact Information, MAC address, Hardware Version and Firmware Version, as shown in below:

Device Information			
Name :	Industrial Switch	Serial No. :	1
Description :	24 PORT	Contact Information :	
MAC Address :	00:22:6F:7A:00:02	Hardware Ver :	V1.0.1
Firmware Ver :	V2.1.0 build 20120209-t6		

Configuration Items	Meaning
Name	Network mark of the device. It is convenient for management tools to judge.
Serial No.	Serial number of the device. It is convenient for device management.
Description	Description of the product features.
Contact Information	Contact information of the operator for device maintenance.
MAC address	Hardware address of the device. It is an unique address which is made up of hexadecimal number with 48 bits (6 bytes) in length.
Hardware Version	Current hardware version.
Firmware Version	Current firmware version.
Current Time	Current time of the device.

Among them, Model, Hardware Version, Firmware Version and MAC address can't be changed. Name, Description, Serial No. and Contact Information can be changed or customized if necessary. Please refer to chapter about Device Information if change is necessary.

Current time can be seen in the following figure:



We can also see each port status in the Port Information area.

Port Information				
Port	Connection	Duplex	Speed	Type
1	LOS	HALF	10M	TX
2	LOS	HALF	10M	TX
3	LOS	HALF	10M	TX
4	LOS	HALF	10M	TX
5	LOS	HALF	10M	TX
6	LOS	HALF	10M	TX
7	LOS	HALF	10M	TX
8	LOS	HALF	10M	TX
9	LOS	HALF	10M	TX
10	LOS	HALF	10M	TX
11	LOS	HALF	10M	TX
12	LOS	HALF	10M	TX
13	LOS	HALF	10M	TX
14	LOS	HALF	10M	TX
15	LINK	FULL	100M	TX
16	LOS	HALF	10M	TX
17	LOS	HALF	10M	TX
18	LOS	HALF	10M	TX
19	LOS	HALF	10M	TX
20	LOS	HALF	10M	TX
21	LOS	HALF	10M	TX
22	LOS	HALF	10M	TX
23	LOS	HALF	10M	TX
24	LOS	HALF	10M	TX

Port Information Screen

- Connection: LINK or LOS
- Port Status: FULL (Full duplex) or HALF (Half duplex)
- Speed: 10M or 100M
- Port Type: Tx or Fx

Port Configuration

Main function of port settings:

- Forcibly set up speed mode and duplex mode of each port
- Enable or disable each port
- Each port is allowed flow control or not.

Port	Type	Speed	Duplex	Enable	Flow Control	MDI/MDIX
1	TX	AUTO	Full Duplex	<input checked="" type="checkbox"/>	<input type="checkbox"/>	AUTO
2	TX	AUTO	Full Duplex	<input checked="" type="checkbox"/>	<input type="checkbox"/>	AUTO
3	TX	AUTO	Full Duplex	<input checked="" type="checkbox"/>	<input type="checkbox"/>	AUTO
4	TX	AUTO	Full Duplex	<input checked="" type="checkbox"/>	<input type="checkbox"/>	AUTO
5	TX	AUTO	Full Duplex	<input checked="" type="checkbox"/>	<input type="checkbox"/>	AUTO
6	TX	AUTO	Full Duplex	<input checked="" type="checkbox"/>	<input type="checkbox"/>	AUTO
7	TX	AUTO	Full Duplex	<input checked="" type="checkbox"/>	<input type="checkbox"/>	AUTO
8	TX	AUTO	Full Duplex	<input checked="" type="checkbox"/>	<input type="checkbox"/>	AUTO
9	TX	AUTO	Full Duplex	<input checked="" type="checkbox"/>	<input type="checkbox"/>	AUTO
10	TX	AUTO	Full Duplex	<input checked="" type="checkbox"/>	<input type="checkbox"/>	AUTO
11	TX	AUTO	Full Duplex	<input checked="" type="checkbox"/>	<input type="checkbox"/>	AUTO
12	TX	AUTO	Full Duplex	<input checked="" type="checkbox"/>	<input type="checkbox"/>	AUTO
13	TX	AUTO	Full Duplex	<input checked="" type="checkbox"/>	<input type="checkbox"/>	AUTO
14	TX	AUTO	Full Duplex	<input checked="" type="checkbox"/>	<input type="checkbox"/>	AUTO
15	TX	AUTO	Full Duplex	<input checked="" type="checkbox"/>	<input type="checkbox"/>	AUTO
16	TX	AUTO	Full Duplex	<input checked="" type="checkbox"/>	<input type="checkbox"/>	AUTO
17	TX	AUTO	Full Duplex	<input checked="" type="checkbox"/>	<input type="checkbox"/>	AUTO
18	TX	AUTO	Full Duplex	<input checked="" type="checkbox"/>	<input type="checkbox"/>	AUTO
19	TX	AUTO	Full Duplex	<input checked="" type="checkbox"/>	<input type="checkbox"/>	AUTO
20	TX	AUTO	Full Duplex	<input checked="" type="checkbox"/>	<input type="checkbox"/>	AUTO
21	TX	AUTO	Full Duplex	<input checked="" type="checkbox"/>	<input type="checkbox"/>	AUTO
22	TX	AUTO	Full Duplex	<input checked="" type="checkbox"/>	<input type="checkbox"/>	AUTO
23	TX	AUTO	Full Duplex	<input checked="" type="checkbox"/>	<input type="checkbox"/>	AUTO
24	TX	AUTO	Full Duplex	<input checked="" type="checkbox"/>	<input type="checkbox"/>	AUTO

Port Configuration Screen

This interface displays basic information of each port. The meaning of information is shown as below:

Configuration Items	Meaning
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 enable 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 state is off.

Port Setting Notes

Port Speed

Port speed shows the connecting speed of the port. It includes 3 kinds of speed: 10M, 100M and auto-negotiation.

10M uses 10base-T standard and UTP cable for connection. When the port is in 10M speed, Link/Act indicator will blink continuously while data transmitting and status indicator of 10M/100Mbps will stay OFF.

100M uses 100Base-TX standard and UTP/STP cable for connection. When the port is in 100M speed, Link/Act indicator will blink continuously while data transmitting. 100M fiber port uses 100Base-FX standard and single/multi-mode fiber for connection. Main fiber of 100Base-FX standard includes: 62.5nm multi-mode fiber and 50nm multi-mode fiber.

Auto-negotiation includes 2 kinds of speed according the capability of the other end: 10M and 100M.

Port Enable

This item provides a device to enable/disable the port. When choosing disable, the device would cut off power supply of this port. Even if other device is connected to this port, all status indicators of this port are OFF. Only enable this port, all settings about this port will be valid. This item provides a kind of safety mechanism to protect the port from illegal use. It is not allowed to disable all the ports.

Duplex Mode

Full duplex of the switch means switch can transmit and receive data at the same time. Half duplex of the switch means switch can transmit or receive data in a certain time. Generally the speed will choose auto-

negotiation so that the port can automatically judge the connection type of the device connected to it and automatically adjust the connection type to ensure the maximum compatibility.

Flow Control

Flow control is used to prevent the frames from discard while port is blocked. This method is to send back the blocking signal to its original address while sending or receiving buffer area start to overflow. It limits the abnormal flows into a certain range. Flow control can be effective in preventing large amounts of data in the network instant impact on the network to ensure the efficient and stable user network running.

There are two types of flow control:

1. In the half duplex mode, flow control is through back pressure. It is to send a jamming signal to the transmission source to reduce transmission speed.
2. In the full duplex mode, flow control generally follow IEEE 802.3x standard. Switch sends "pause" to information source to pause its sending information.

Polarity (MDI/MDIX auto-negotiation)

MDI-II (Medium Dependent Interface- II mode), is a kind of standard built by IEEE for RJ-45 UTP cable of fast Ethernet 100BASE-T. II stands for parallel configuration. MDI-X(Media Dependent Interface-x mode). MDI- II is a kind of standard built by IEEE for RJ-45 UTP cable of fast Ethernet 100BASE-T. X stands for crossover configuration.

Bandwidth Management

The device provides port based speed limitation, including ingress and egress limitation. User can limits communication flow of each port and quits the flow limitation of the port. User can choose a settled speed, the range is: 64Kbps ~ 100Mbps. The type of port limitation includes all unicast, multicast and broadcast. When the port speed reaches the appointed speed, the device will enable or disable flow to limit the transmitting speed or receiving speed by flow control or discard the message.

Bandwidth Configuration : Enable Disable

Port	Ingress	Port	Ingress	Port	Egress	Port	Egress
1	9M	2	No Limited	1	No Limited	2	9M
3	No Limited	4	No Limited	3	No Limited	4	No Limited
5	No Limited	6	No Limited	5	No Limited	6	No Limited
7	No Limited	8	No Limited	7	No Limited	8	No Limited
9	No Limited	10	No Limited	9	No Limited	10	No Limited
11	No Limited	12	No Limited	11	No Limited	12	No Limited
13	No Limited	14	No Limited	13	No Limited	14	No Limited
15	No Limited	16	No Limited	15	No Limited	16	No Limited
17	No Limited	18	No Limited	17	No Limited	18	No Limited
19	No Limited	20	No Limited	19	No Limited	20	No Limited
21	No Limited	22	No Limited	21	No Limited	22	No Limited
23	No Limited	24	No Limited	23	No Limited	24	No Limited

The device provides both ingress and egress speed limitation. The ingress speed refers to the actual speed from PC and other devices to the switch. The egress speed refers to the actual speed from the switch to other devices. If ingress and egress speed of the connecting port between two devices are limited at the same time, the actual speed will be the smaller value.

For example, the screen above shows Port 1 limits the ingress speed only, the maximum speed of this port is 9M. Port 2 limits egress speed only, and the maximum speed of this port is 9M.

Settings Notes

- Please enable flow control when using port speed limitation.
- When using speed limitation, it will not discard the packet unless the flow control is disabled.
- Port speed limitation needs cables with high quality, otherwise it will cause a lot of conflict packets and incomplete packets.

Broadcast Storm Suppression

Broadcast Storm

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 : Enable Disable

Max Rate : 3% 5% 10% 20% 30%

Type : Broadcast, Multicast and Flood
 Only Broadcast

Apply Cancel

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

If storm suppression is enabled, it can stop the attack. Our device can detect 2 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
- Destination lookup failure frame: the MAC address of this data frame doesn't exist in the index. It needs to transmit to all the ports, including unicast and multicast flow.

Maximum Speed

There are 5 levels: 3%, 5%, 10%, 20%, 30%. The base is 100Mbps.

Alarm Type

Email alarm: when the switch enables Email settings, the switch will send an email to the customer immediately when broadcast happens.



Settings 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 cautious to use MAC control frame and destination lookup failure frame, disabling IGMP SNOOPING will have impact on the transmission of the multicast.

L2 Features

VLAN

VLAN (Virtual Local Area Network) is a kind of new data exchange technology for logically dividing LAN into many segments and making many virtual work groups. This technology mainly allows that switch can limit broadcast when LAN interconnects. This technology can divide a LAN into several logical LAN—VLAN.

Each VLAN is a broadcast domain and hosts in VLAN can communicate just like in the same LAN. But it can not interconnect between VLAN. Then broadcast message is limited in the VLAN.

Port based VLAN

A port based VLAN determines the membership of a data frame by examining the configuration of the port that receive the transmission or reading a portion of the data frame's tag header. A four--byte field in the header is used to identify the VLAN. This VLAN identification indicates what VLAN the frame belongs to. If the frame has no tag header, the switch checks the VLAN setting of the port that receive the frame. If the switch has been configured for port based VLAN support, it assigns the port's VLAN identification to the new frame.

1. AddItem

Group name can be 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.

VLAN Mode : Port-based VLAN IEEE 802.1Q VLAN

VLAN Name : (Range :1~4094)

Join Port : 01- 02- 03- 04- 05- 06- 07- 08- 09- 10- 11- 12-
 13- 14- 15- 16- 17- 18- 19- 20- 21- 22- 23- 24-

Operation :

VLAN Name	Join Port
1	01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24

2. Delete Item

It refers to delete the existing transmission items. The example above shows that all ports are in the same VLAN. Each port can intercommunicate with others. We can modify the default configuration to add VLAN item. The ports in the group can intercommunicate with each other, but the port outside the group cannot intercommunication with the port inside.

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.

802.1Q VLAN

802.1Q VID : (Range :1~4094)

01-	02-	03-	04-	05-	06-	07-	08-	09-	10-	11-	12-
13-	14-	15-	16-	17-	18-	19-	20-	21-	22-	23-	24-

(- : Not FWD M : FWD and reserve vlan tag U : FWD but remove vlan tag) Modify All Add/Edit Delete Apply

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

1. Add Item

Group name can be number only in IEEE 802.1Q VLAN. It is TPID in VLAN ID. 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 64 in IEEE 802.1Q VLAN.

2. Delete Item

It refers to delete the existing transmission items. The example above shows that all ports are in the same VLAN. Each port can intercommunicate with others. We can delete the default configuration and use the different VID to add some items (VID value range is: 1~4094). The ports in the group can intercommunicate with each other, but the port outside the group cannot intercommunication with the port inside.

3. VLAN Configuration

VLAN Tag Replace Configuration:

Vlan Tag Replace

Vlan Frame Control : No need change VID and Priority Replace VID into default VID Replace both Priority and VID

Port VID: Default VID Configuration

Default VID

01-	02-	03-	04-	05-	06-	07-	08-	09-	10-	11-	12-
13-	14-	15-	16-	17-	18-	19-	20-	21-	22-	23-	24-

Priority: Default Priority Setting

Default Priority

01-	02-	03-	04-	05-	06-	07-	08-	09-	10-	11-	12-
13-	14-	15-	16-	17-	18-	19-	20-	21-	22-	23-	24-

- Keep the same VID and priority
If the data has no VLAN ID, please use the default priority and port VID to create a VLAN ID and insert it into the data frame, otherwise the data frame keeps the same.
- Default VID replace the VID of the ingress packets
If the data has no VLAN tag, please use the default priority and port VID to create a VLAN tag and insert it into the data frame, otherwise the default VID will replace the VID of the ingress packets.
- Use the default VID and priority to create a new VID

IGMP Snooping

IP host applies to join (or leave) multicast group to the neighboring router through IGMP (Internet Group Management Protocol) protocol. IGMP Snooping is multicast constraining mechanism. It manages and controls multicast group by snooping and analysis of the IGMP messages between the host and the multicast device.

Work process of IGMP Snooping: the switch snoops messages between the host computer and the router and tracks multicast information and the port applied for. When the switch snoops IGMP Report message sent from the host computer to the router, the switch would add this port to multicast forwarding list; when the switch snoops IGMP Leave message sent by the host computer, the router will send Group-Specific Query message of this port. If other hosts need this multicast, then they rely on IGMP Report message. If the router doesn't get any reply from the hosts, the switch would delete this port from the multicast forwarding list. The router will send IGMP Query message regularly, the switch will delete the port from the multicast forwarding list if it doesn't get the IGMP Report message from the host.

- IGMP Snooping: Enable or disable IGMP snooping function
- IGMP Query: Enable or disable IGMP query function
- IGMP Query Interval: after enabling IGMP Query, the interval to check existing multicast members.
- MAX Age: the maximum existing time of the members

IGMP Snooping : Enable Disable

IGMP Query : Enable Disable

IGMP Query Interval : S (Range :60~1000)

MAX Age : S (Range :120~5000)

NO	MAC Address	Type	Join Port
1	01-00-5E-7F-FF-FA	Dynamic	15

IGMP Notes

- It must set up 802.1Q VLAN first before enabling IGMP Snooping.
- It had better not to have many IGMP query to save the resources. If you are not sure of the forwarding relationship of the unknown multicast group, please choose all the ports.

Static Multicast FWD

The device provides the function of static MAC address forwarding. The destination address includes the data packets with static MAC address which will be transferred to the appointed port. Embedded forwarding address list in the switch chip can learn and support 4,000 MAC addresses and 256 multicast forwarding ports list.

Static Multicast MAC Address : (XX-XX-XX-XX-XX-XX)

Join Port : 01- 02- 03- 04- 05- 06- 07- 08- 09- 10- 11- 12-
 13- 14- 15- 16- 17- 18- 19- 20- 21- 22- 23- 24-

Operation :

No	MAC Address	Join Port
1	01-22-6F-01-02-03	02 03 04

Bottoms [Add] and [Delete] are used to add and delete static MAC address. Static MAC Address asks the user to input a valid address. If it is not valid, a warning ejects. Join port is used to choose MAC address forwarding port. You can appoint one or more forwarding ports. Click [Add] and [Delete] to update static MAC address forwarding.

IGMP Notes

1. This function has great impact on forwarding multicast, unless you can make sure the address is no problem, otherwise, please use it with caution.
2. The following multicast addresses are reserved for the device or protocol, please don't use them: 0180C20000xx, 01005E0000xx.
3. IGMP dynamic learning will not update the multicast address, static multicast forwarding is a kind of safety mechanism.

QoS

QoS Classification

QoS can provide 4 internal queues and each queue supports 4 different levels of traffic. The data packets with high priority stay a short time in the ethernet switch. Some traffic which is sensitive to delay will supports very short latent period. According to port ID, MAC address, 802.1p priority tag, DiONetServ and IP TOS, the device can classify data packets to its corresponding classification.

Current Location>>Main Menu>>QoS>>QoS Classification

QoS Classification

Queuing Mechanism : **Weighted Fair(8:4:2:1)** ▼

Port	Inspect DSCP	Inspect Cos	Default Port Priority
1	<input type="checkbox"/>	<input type="checkbox"/>	Low ▼
2	<input type="checkbox"/>	<input type="checkbox"/>	Low ▼
3	<input type="checkbox"/>	<input type="checkbox"/>	Low ▼
4	<input type="checkbox"/>	<input type="checkbox"/>	Low ▼
5	<input type="checkbox"/>	<input type="checkbox"/>	Low ▼
6	<input type="checkbox"/>	<input type="checkbox"/>	Low ▼
7	<input type="checkbox"/>	<input type="checkbox"/>	Low ▼
8	<input type="checkbox"/>	<input type="checkbox"/>	Low ▼
9	<input type="checkbox"/>	<input type="checkbox"/>	Low ▼
10	<input type="checkbox"/>	<input type="checkbox"/>	Low ▼
11	<input type="checkbox"/>	<input type="checkbox"/>	Low ▼
12	<input type="checkbox"/>	<input type="checkbox"/>	Low ▼
13	<input type="checkbox"/>	<input type="checkbox"/>	Low ▼
14	<input type="checkbox"/>	<input type="checkbox"/>	Low ▼
15	<input type="checkbox"/>	<input type="checkbox"/>	Low ▼

User can choose QOS priority queue mechanism. The mechanism includes 2 kinds: Weighted Fair(8:4:2:1) and Strict.

Weighted Fair(8:4:2:1): when 4 100M data with different priority seize 1 100M port to transmit the data, it will transmit data as the proportion of 8:4:2:1. Data with High priority will take 8/15, Medium priority will take 4/15, Normal priority will take 2/15 and Low priority will take 1/15.

Strict: when 4 100M data with different priority seize 1 100M port to transmit the data, data with high priority will be transmitted at first, data with Medium, Normal and Low will be transmitted later according to their priority.

Default Priority

Default priority is also the port based priority. Default priority is quite different from COS and TOS, it has nothing to do with data packets but port priority of the switch. When port priority is high, the data packets transmitted from this port will faster than other ports.

COS

Priority tag in 802.1P includes 8 kinds (0-7). The corresponding priority includes 4 kinds (High, Medium, Normal, Low).

Cos	0	1	2	3
Priority Queue	Low	Low	Normal	Normal
Cos	4	5	6	7
Priority Queue	Medium	Medium	High	High

In device's default settings, data with priority tag 0 and 1 will be in queue Low, data with 2 and 3 will be in queue Normal, data with 4 and 5 will be in queue Medium and data with 6 and 7 will be in queue High.

DSCP

DiffServ system need every transmitting message with different classification in the network. Classification information is comprised in the head of IP message. former 6 bits of TOS is used to comprise the classification information.

Now the defined DSCP we have here includes: default DSCP, the value is 0; class selector DSCP, the value is (8,16,24,32,40,48,56); expedited forwarding(EF), has the characteristics of low delay, The recommended DSCP for expedited forwarding is 46(101110);assured forwarding(AF), The AF behavior group defines four separate AF classes with Class 4 having the highest priority. Within each class, packets are given a drop precedence (high, medium or low). The combination of classes and drop precedence yields 12 separate DSCP encodings,((10,12,14), (18, 20, 22), (26, 28, 30), (34, 36, 38)).

The device defines value (0-15) as Low priority queuing, the first queuing, value (16-31) as Normal priority queuing, the second queuing, value(32-47) as Medium priority queuing, the third queuing and the value(48-63) as High priority queuing.

Mapping Table of ToS(DSCP)Value and Priority Queues

ToS(DSCP)	Level	ToS(DSCP)	Level	ToS(DSCP)	Level	ToS(DSCP)	Level
0x00(01)	Low	0x04(02)	Low	0x08(03)	Low	0x0C(04)	Low
0x10(05)	Low	0x14(06)	Low	0x18(07)	Low	0x1C(08)	Low
0x20(09)	Low	0x24(10)	Low	0x28(11)	Low	0x2C(12)	Low
0x30(13)	Low	0x34(14)	Low	0x38(15)	Low	0x3C(16)	Low
0x40(17)	Normal	0x44(18)	Normal	0x48(19)	Normal	0x4C(20)	Normal
0x50(21)	Normal	0x54(22)	Normal	0x58(23)	Normal	0x5C(24)	Normal
0x60(25)	Normal	0x64(26)	Normal	0x68(27)	Normal	0x6C(28)	Normal
0x70(29)	Normal	0x74(30)	Normal	0x78(31)	Normal	0x7C(32)	Normal
0x80(33)	Medium	0x84(34)	Medium	0x88(35)	Medium	0x8C(36)	Medium
0x90(37)	Medium	0x94(38)	Medium	0x98(39)	Medium	0x9C(40)	Medium
0xA0(41)	Medium	0xA4(42)	Medium	0xA8(43)	Medium	0xAC(44)	Medium
0xB0(45)	Medium	0xB4(46)	Medium	0xB8(47)	Medium	0xBC(48)	Medium
0xC0(49)	High	0xC4(50)	High	0xC8(51)	High	0xCC(52)	High
0xD0(53)	High	0xD4(54)	High	0xD8(55)	High	0xDC(56)	High
0xE0(57)	High	0xE4(58)	High	0xE8(59)	High	0xEC(60)	High
0xF0(61)	High	0xF4(62)	High	0xF8(63)	High	0xFC(64)	High

 **Note**

1. If the default priority is High, then other QoS property will not be checked and put into High priority queuing
2. DSCP is lower than default priority, if there is no settings about DSCP, 802.1P will be checked, or the queuing will be based on DSCP settings.
3. The above 3 kinds of priority can be used both independently and together.

Redundancy

Port Trunking

Main features of TRUNK is to bind several physical ports (general number is 2-4) to make a logical channel. After binding several physical links, bandwidth of entire network improves a lot so that data can be transmitted through several physical links, which also make many redundant links. When one or more links are cut off by failure or other reason, the rest of them can continue to work well.

Trunking : Enable Disable

Trunking Group :

Join Port : 01- 02- 03- 04- 05- 06- 07- 08- 09- 10- 11- 12-
13- 14- 15- 16- 17- 18- 19- 20- 21- 22- 23- 24-

Operation :

Group	Join Port
1	02 03
2	04 05

The device supports 2 Trunking groups. Each group support 2-4 port trunking.



Trunking Notes

1. The action of Trunking member is the same, so configuration sub-items of each member (port properties, VLAN properties) are the same in a group.
2. If you don't confirm RSTP status, please disable RSTP, or close the others, leaving one RSTP channel.
3. Port 1 as a system reservation cannot be used as Trunking port. 4. Trunking port cannot be Ring port any more.

Rapid Ring

It is very important to possess redundant communication in industrial network. Redundancy can protect important link from failure. With it network will auto-recover and runs normally when it is broken.

Redundant communication allows redundant ring enable backup data link when the wire is broken up or destroyed. It is very important feature for industrial application for it will take great loss maybe if it takes a long time to locate the broken or destroyed wires.

RLH-ESMXXXX-XX-X series switch supports redundant communication with SW-Ring technology. SW-Ring technology provides auto-recovery and reconnection mechanism for broken network. When network is broken, it has link redundancy and self-recovery capability and self-recovery time is less than 20ms. RLH-ESMXXXX-XX-X series supports maximum 2 ring groups. Each group set up 2 ports as Ring Port and a port cannot belong to several rings.

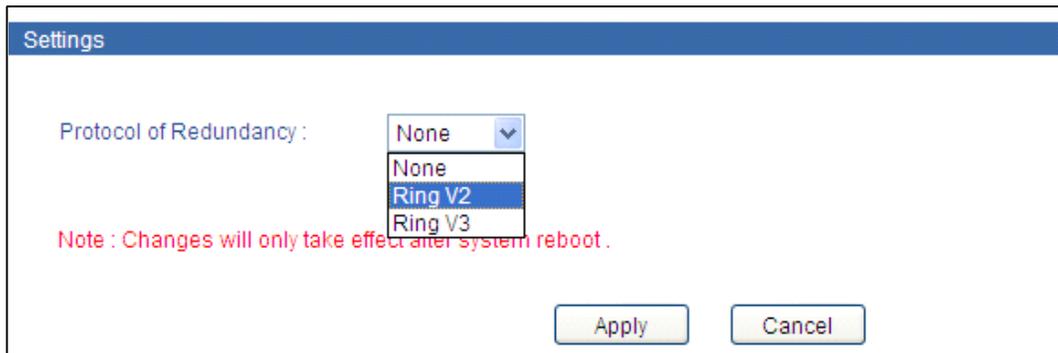
Hello_time setting is time interval of sending detecting packet to network at regular time. The unit is ms. Its main purpose is to detect network connection. It sends a detecting packet to next door devices by CPU. If they receive it, then reply a confirm packet to ensure network connection is active. If this setting will influence self-recovery time, we suggest advanced users can use it.

Basic interface of Rapid Ring as shown in the following figure:



Basic interface shows Protocol of Redundancy is None. Ring can be set by Protocol of Redundancy configuration if it is needed. As shown in the figure below, in [Settings] area there are 2 kinds in corresponding drop-down menu of Protocol of Redundancy: **Ring V2** and **Ring V3**.

1. Method to enable Ring V2: Configuration interface of Ring V2 is shown in following figure.



2. Ring V2 supports 4 Ring groups available for sing ring and coupling ring. As shown in the following figure.

Protocol of Redundancy : Ring V2

Group	ID	Port 1	Port 2	Type	Hello Time	Enable
1	1	1	2	Single	0 × 100ms	<input checked="" type="checkbox"/>
2	2	7		Couple	0 × 100ms	<input checked="" type="checkbox"/>
3	3	12	13	Single	0 × 100ms	<input checked="" type="checkbox"/>
4	4	23		Couple	0 × 100ms	<input checked="" type="checkbox"/>

Note : Changes will only take effect after system reboot.

Apply Cancel

3. Click Apply and it will take effect after system reboot.

Single Ring Configuration of Ring V2

1. Enable Ring V2. Choose Ring V2 in [Settings] area, as shown in figure 6-25.

Settings

Protocol of Redundancy :
 None
 Ring V2
 Ring V3

Note : Changes will only take effect after system reboot.

Apply Cancel

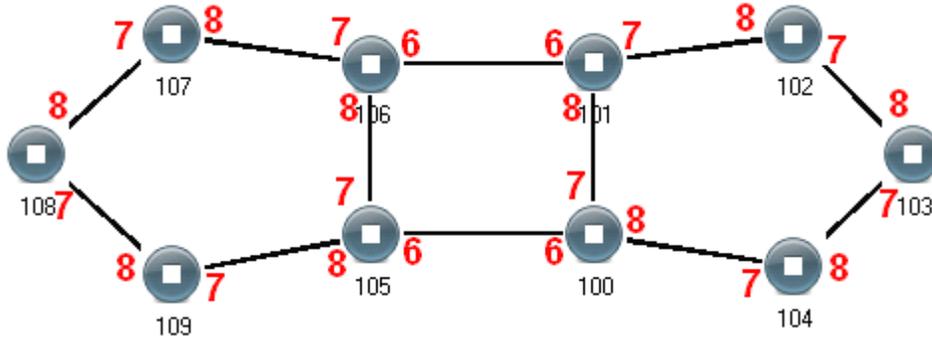
2. Enable Group 1 (or Group 2), input ID (0-255 numbers only) choose Port 1 and 2 to be Ring Ports, as shown in figure below.

Protocol of Redundancy : Ring V2

Group	ID	Port 1	Port 2	Type	Hello Time	Enable
1	1	1	2	Single	0 × 100ms	<input checked="" type="checkbox"/>

Coupling Ring Configuration of Ring V2

Basic structure of coupling ring is shown in the following figure.



Operating Method

1. Select Ring V2 in Settings area and enable Ring Group 1 and 2;(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.);
2. Set up Port 7 and 8 of Device 105, 106 to be Ring Ports in Ring Group 1, Network ID is 1, Ring Type is Single; Set up Port 6 of device to be Ring Port in Ring Group 2, Network ID is 3, Ring Type is Couple, as shown in the following figure.

Protocol of Redundancy : Ring V2						
Group	ID	Port 1	Port 2	Type	Hello Time	Enable
1	1	7	8	Single	0 × 100ms	<input checked="" type="checkbox"/>
2	3	6		Couple	0 × 100ms	<input checked="" type="checkbox"/>

3. Set up Port 7 and 8 of Device 100, 101 to be Ring Ports in Ring Group 1, Network ID is 2, Ring Type is Single; Set up Port 6 of device to be Ring Port in Ring Group 2, Network ID is 3, Ring Type is Couple, as shown in the following figure.

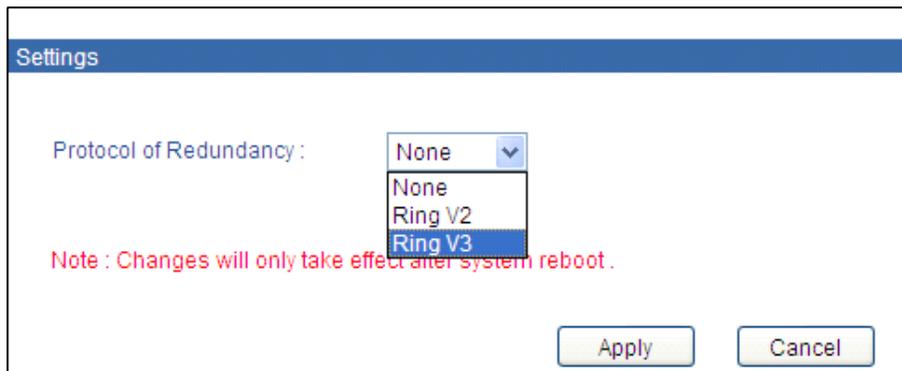
Protocol of Redundancy : Ring V2						
Group	ID	Port 1	Port 2	Type	Hello Time	Enable
1	2	7	8	Single	0 × 100ms	<input checked="" type="checkbox"/>
2	3	6		Couple	0 × 100ms	<input checked="" type="checkbox"/>

4. Set up Port 7 and 8 of Device 107, 108, 109 to be Ring Ports in Ring Group 1 , Network ID is 1, Ring Type is Single; Set up Port 7 and 8 of Device 102, 103, 104 to be Ring Ports in Ring Group 1, Network ID is 2, Ring Type is Single.

5. Use wire to connect Port 7 and 8 of Device100-104 in turn to make a Single Ring. Use a wire to connect Port 7 and 8 of Device 105-109 in turn to make another Single Ring. Then use a wire to connect Port 6 of Device 106 and Port 6 of Device 101, Port 6 of Device 105 and Port 6 of Device 100. The coupling Ring is completed as shown in figure 6-27.

Method to enable Ring V3

1. Enable Ring V3. Choose Ring V3 in [settings] area as shown below.



2. As shown in the figure, Ring V3 supports 4 Ring groups. It supports single ring, coupling ring, chain and Dual_homing .



3. Enable Ring 1 (or other Groups), input network ID (0-255 numbers only), choose ring port in Group 1. The Single Ring configuration of Ring V3 is similar to that of Ring V2, so the following page mainly talks about Couple, Chain and Dual homing .

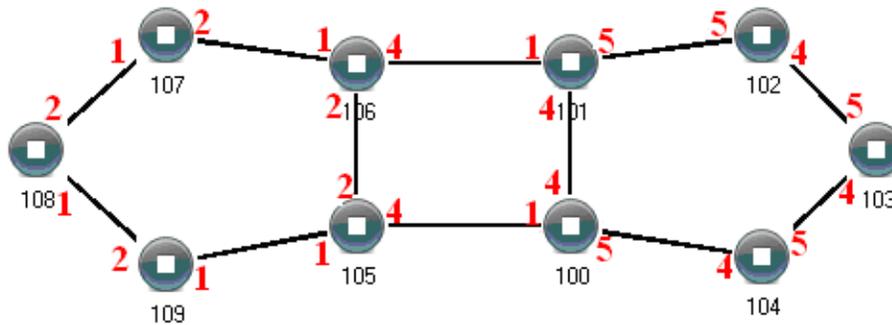
“Chain” refers to strengthen user’s capability of making any type of redundant topological structure with flexibility by taking an advanced software technology. In fact, Chain is to cascade several switches already set up to Ring and both sides of chain access to network.

“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].

Ring V3 Coupling

Ring Configuration Basic structure of Coupling Ring is shown below. 2 ports connecting Device105 and 106 are called Control Ports. The control ports of Device 101 and 100 is the same as Device105 and 106.



Operating Method:

1. Enable Ring Group 1 and Ring Group 2; (Hello_time can be disable too, if enabled, time of sending Hello packet could not be very fast, or it will influence CPU dealing speed.);
2. Set up Port 1 and 2 of Device 105, 106 to be Ring Ports in Ring Group 1, Network ID is 1, Ring Type Single; Set up Port 4 of device to be Coupling Port in Ring Group 2, Coupling Control Port is 2, Network ID is 3.
3. Ring Type is Couple. As shown below.

Protocol of Redundancy : Ring V3						
Group	ID	Port 1	Port 2	Type	Hello Time	Enable
1	<input type="text" value="1"/>	1	2	Single	<input type="text" value="0"/> × 100ms	<input checked="" type="checkbox"/>
Group	ID	Coupling Port	Coupling Ctrl Port	Type	Hello Time	Enable
2	<input type="text" value="3"/>	4	2	Couple	<input type="text" value="0"/> × 100ms	<input checked="" type="checkbox"/>

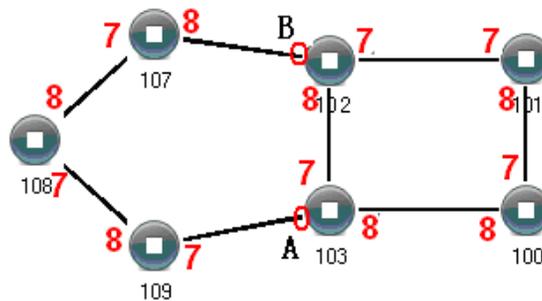
- Set up Port 4 and 5 of Device 100, 101 to be Ring Ports in Ring Group 1, Network ID is 2, Ring Type is Single; Set up Port 1 of device to be Coupling Port in Ring Group 2 , Coupling Control Port is Port 4, Network ID is 3, Ring type is Couple, as shown in figure 6-36.

Group	ID	Port 1	Port 2	Type	Hello Time	Enable
1	2	4	5	Single	0 × 100ms	<input checked="" type="checkbox"/>
Group	ID	Coupling Port	Coupling Ctrl Port	Type	Hello Time	Enable
2	3	1	4	Couple	0 × 100ms	<input checked="" type="checkbox"/>

- Set up Port 1 and 2 of Device 107, 108, 109 to be Ring Ports in Ring Group 1, Network ID is 1, Ring Type is Single; Set up Port 4 and 5 of Device 102, 103, 104 to be Ring Port in Ring Group 1, Network ID is 2, Ring Type is Single.
- Use a wire to connect Port 4 and 5 of Device 100-104 in turn to make a Single Ring. Use a wire to connect Port 1 and 2 of Device 105-109 in turn to make a Single Ring. Then use a wire to connect Port 4 of Device 106 to Port 1 of Device 101, Port 4 of Device 105 to Port 1 of Device 100. The Coupling Ring is completed.

Ring V3 Chain Configuration

Basic structure of Chain is shown below.



Operating method:

- Enable Ring Group 1: (Hello time can be disabled too, if it is enabled, the time of sending Hello packet could not be very fast, or it will influence CPU dealing speed.);
- Set up Port 7 and 8 of Device 100, 101, 102 and 103 to be Ring Port in Ring Group 1, Network ID is 1, Ring Type is Single; as shown in the following figure.

Protocol of Redundancy : Ring V3						
Group	ID	Port 1	Port 2	Type	Hello Time	Enable
1	1	7	8	Single	0 × 100ms	<input checked="" type="checkbox"/>

- 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 below

Protocol of Redundancy :		Ring V3				
Group	ID	Port 1	Port 2	Type	Hello Time	Enable
1	2	7	8	Single	0 × 100ms	<input checked="" type="checkbox"/>

- 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. The chain is now complete.



Note

- The trunking port cannot be set into Rapid Ring Port, and one port cannot belong to several rings.
- The network ID must be same in the single ring.
- All ring ports must be tagged as a VLAN member in VLAN settings, otherwise they will not work properly.

Access Control

Password

The company may use the manager to monitor the device, and the switch manager to manage both the system or network. Their privileges must be different. The former manager is in charge of monitoring the device only. The latter one is in charge of system or network. This type of switch provides managements with different privileges: observer privilege and administrator privilege. Observer can check the switch status only, and the administrator can configure the parameters of the switch.

- Index** It refers to which groups of users.
- Access Level Administrator:** privilege to check and configure the switch. Observer: privilege to check the settings only.
- Login Name** It allowed the combination of letters which is less than 16 bytes.
- Password** It allowed the combination of letters which is less than 16 bytes.
- Confirm Password** Confirm the password is right.

Index :	1	▼
Access Level :	Administrator	▼
Login Name :	admin	
Password :	••••••	
Confirm Password :	••••••	
	Apply	Cancel

Index :	2	▼
Access Level :	Observer	▼
Login Name :		
Password :		
Confirm Password :		
	Apply	Cancel

Note: If you forget the login name and password, please contact our technical support.

Access Profile

Web Server Transfer Protocol

- **HTTP**
HTTP (Hyper Text Transfer Protocol) is an application protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the WorldWide Web.
- **HTTPS**
HTTPS (Hyper Text Transfer protocol Secure) is a combination of HTTP with SSL/TLS protocol. It provides encrypted communication and secure identification of a network web server.

Current Location>>Main Menu>>Access Control>>Access Profile

Transport Protocol

HTTP HTTPS

IP Address Login Control

Enable Disable

Index	Allow access to the IP address list	Index	Allow access to the IP address list
1	<input type="text"/>	2	<input type="text"/>
3	<input type="text"/>	4	<input type="text"/>
5	<input type="text"/>	6	<input type="text"/>
7	<input type="text"/>	8	<input type="text"/>
9	<input type="text"/>	10	<input type="text"/>
11	<input type="text"/>	12	<input type="text"/>
13	<input type="text"/>	14	<input type="text"/>
15	<input type="text"/>	16	<input type="text"/>
17	<input type="text"/>	18	<input type="text"/>
19	<input type="text"/>	20	<input type="text"/>

 **Note**

1. It must enable at least one protocol in HTTP and HTTPS.
2. Some explorer cannot display normally when it use HTTPS at the first time. It will display normally after afresh.
3. The IP address must be valid. At least one address and the IP address are in the same network segment. Otherwise the device is invalid.

Static Unicast FWD

Static MAC Address

The static MAC address is different from general dynamic MAC address obtained by learning. Once a static MAC address is entered in, the address is valid until it is deleted and beyond the maximum age. The static address list records the static address of the ports. Each MAC address corresponds to one port.

The static MAC address aims to limit the moving of the computer. Once the MAC address of the computer is bound with one port, this computer cannot communicate with others when it connects the other port. But other computers can communicate with others when they connect this port. It is used to keep the port safe.

Button **[add]** and **[delete]** are used to add and delete MAC address. Static MAC Address asks the user to input a valid address, if the MAC address is invalid, the warning information ejects. **Static Unicast Address** is used to choose the transfer port of static MAC address. It can appoint one or more transfer ports. Click **[add]** and **[delete]** to update the static MAC address.

Static Unicast Address : (XX-XX-XX-XX-XX)

Join Port: 01- 02- 03- 04- 05- 06- 07- 08- 09- 10- 11- 12-
 13- 14- 15- 16- 17- 18- 19- 20- 21- 22- 23- 24-

Operation :

Index	MAC Address	Join Port
1	00-22-6F-01-02-03	01

 **Note**

1. This is a safety mechanism, please use it with caution.
2. Please don't use multicast address as input address
3. Please don't input the reserved MAC address, like the MAC address of the computer.

Port Statistics

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

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

Sysbol Err

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

Tx Frame Statistics

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

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

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

Conflict Discard

Number 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)

Traffic Statistics

Current Location>>Main Menu>>Port Statistics >>Traffic Statistics						
Port	Tx	Rx	Unicast	Multicast	Broadcast	Error
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

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

MAC Address

MAC (Media Access Control) is a unique identifier assigned to network interfaces for communications on physical network segment. The switch transmits the messages according to MAC address. Each switch maintains a MAC address list. In this list, each MAC address corresponds to one port of the switch. When switch receives some data frames, it is decided by MAC address to filter these frames or transmit to the corresponding ports of the switch.

MAC Address List					
Address Mode :		Auto			
Join Port :		Port 1			
Index	MAC Address	Type	VLAN	Port	
1	00-05-F4-00-20-57	Dynamic	0	15	
2	00-1E-8C-81-6E-62	Dynamic	0	15	
3	00-1E-8C-81-6E-88	Dynamic	0	15	
4	00-1F-C6-1C-BA-93	Dynamic	0	15	
5	00-1F-C6-E2-AE-AE	Dynamic	0	15	
6	00-21-5E-46-0A-82	Dynamic	0	15	
7	00-21-5E-46-0A-83	Dynamic	0	15	
8	00-22-6F-01-00-03	Dynamic	0	15	
9	00-22-6F-01-00-12	Dynamic	0	15	
10	00-22-6F-01-02-03	Static	0	1	
11	00-22-6F-7A-00-02	Static	0	MII	
12	00-22-6F-FF-00-24	Dynamic	0	15	
13	00-25-86-8D-68-BC	Dynamic	0	15	
14	00-26-18-3D-6C-1E	Dynamic	0	15	
15	00-26-18-67-8A-DB	Dynamic	0	15	
16	00-AF-6F-11-11-11	Dynamic	0	15	
17	14-DA-E9-68-72-FC	Dynamic	0	15	
18	48-5B-39-A7-72-CE	Dynamic	0	15	
19	54-04-A6-6D-FE-43	Dynamic	0	15	
20	54-04-A6-6D-FE-59	Dynamic	0	15	
21	54-04-A6-A3-DE-7D	Dynamic	0	15	
22	84-2B-2B-04-B2-25	Dynamic	0	15	
23	84-2B-2B-04-B2-27	Dynamic	0	15	
24	90-E6-BA-C2-DC-A9	Dynamic	0	15	

MAC address includes 3 kinds:

1. Dynamic MAC address

Dynamic MAC address is created by data frames learning in the network. It will be deleted when it is beyond maximum age. When the port of the switch connected to the device has changed, the corresponding MAC address in the MAC address table also change. Dynamic MAC address will disappear when the switch restarts.

2. Static MAC address (Solidified)

Static MAC address is generated by configuration of IEEE 802.1x. It is beyond maximum age. Whatever changes the ports of the switch make, the relationship of the MAC address and corresponding port will never change. The relationship is controlled by IEEE 802.1X authentication server. Static MAC address will disappear when the switch re-start.

3. Permanent Static MAC address

Permanent MAC address is generated by configuration. It is beyond maximum age. Whatever changes the ports of the switch make, the relationship of the MAC address and corresponding port will never change. Permanent MAC address will disappear when the switch re-start.

MAC address table can appoint type of the order. You can choose "auto" and "MAC". In this table, MAC address and its corresponding port will be displayed. If the status shows "Authentication", it means the MAC address is static authentication and the MAC address is beyond maximum age. If the status shows "static", it means the MAC address is permanent static MAC address and it is beyond the maximum age.



- Permanent static address can be configurable in the former static MAC address table.
- Multicast addresses are displayed in IGMP Snooping list, here are unicast addresses.
- Maximum age of MAC address is 300s.

Diagnosis

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.

Enable :	<input checked="" type="radio"/> Yes	<input type="radio"/> No										
Monitored port :	01- <input checked="" type="checkbox"/>	02- <input checked="" type="checkbox"/>	03- <input type="checkbox"/>	04- <input type="checkbox"/>	05- <input type="checkbox"/>	06- <input type="checkbox"/>	07- <input type="checkbox"/>	08- <input type="checkbox"/>	09- <input type="checkbox"/>	10- <input type="checkbox"/>	11- <input type="checkbox"/>	12- <input type="checkbox"/>
	13- <input type="checkbox"/>	14- <input type="checkbox"/>	15- <input type="checkbox"/>	16- <input type="checkbox"/>	17- <input type="checkbox"/>	18- <input type="checkbox"/>	19- <input type="checkbox"/>	20- <input type="checkbox"/>	21- <input type="checkbox"/>	22- <input type="checkbox"/>	23- <input type="checkbox"/>	24- <input type="checkbox"/>
Mirror port :	01- <input type="radio"/>	02- <input type="radio"/>	03- <input checked="" type="radio"/>	04- <input type="radio"/>	05- <input type="radio"/>	06- <input type="radio"/>	07- <input type="radio"/>	08- <input type="radio"/>	09- <input type="radio"/>	10- <input type="radio"/>	11- <input type="radio"/>	12- <input type="radio"/>
	13- <input type="radio"/>	14- <input type="radio"/>	15- <input type="radio"/>	16- <input type="radio"/>	17- <input type="radio"/>	18- <input type="radio"/>	19- <input type="radio"/>	20- <input type="radio"/>	21- <input type="radio"/>	22- <input type="radio"/>	23- <input type="radio"/>	24- <input type="radio"/>
Watch direction :	<input checked="" type="radio"/> All	<input type="radio"/> Ingress	<input type="radio"/> Egress									
		<input type="button" value="Apply"/>		<input type="button" value="Cancel"/>								

Mirror Port

It defines a group of ports which are needed to be monitored. The device collects data from these ports.

Monitored Port

It defines a group of ports which are used to monitor other ports. The device outputs the data through these ports.

Watch direction

This parameter indicates the direction of the data. It includes 3 kinds of choices: "All", "Ingress" and "Egress".



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.

Diagnosis

PING (Packet Internet Grope), is a computer network administration utility used to test the reachability of a host on an Internet Protocol network and to measure the round-trip time for messages sent from the originating host to a destination computer. Ping operates by sending Internet Control Message Protocol echo request packets to the target host and waiting for an ICMP response. In the process it measures the time from transmission to reception and records any packet loss.

Host Address:	<input type="text" value="192.168.1.14"/>	(IP or Domain)
Message Size:	<input type="text" value="60"/>	Bytes(Range : 60~1480)
Message Number:	<input type="text" value="1"/>	Bytes(Range : 1~100)
Message Interval:	<input type="text" value="1000"/>	Ms (Range : 100~5000)
Response Timeout:	<input type="text" value="5000"/>	Ms (Range :1000~5000)
Diagnosis:	<input type="button" value="Apply"/>	

Host Address

Appointed computer need to ping, it can be an IP address or a domain.

Message Size

Echo data packet including data in "message length"

Message Number

Number of appointed echo data packet

Message Interval

Appointed message sending interval, the unit is ms.

Response Timeout

Timeout interval, the unit is ms.

Diagnosis

Start to send ping message.

**Note**

- "Diagnosis" is only to collect information of the device, not solving the faults.
- The domain of "Host Address" doesn't support unlimited expansion, only not more than 3 levels domain like "mail.sina.com"
- "Request timeout" indicates the other network card is not working properly or some problems of lines.
- If the message "unknown host name" appears when Ping the domain, it means DNS configuration is wrong.
- If the message "Request timeout" appears when Ping domain, it means the gateway setting is wrong.

System

Device IP

Device address supports 2 modes, DHCP and static IP address. When enabling DHCP, you can get the IP address of the device by Hyper Terminal. If you need to use NTP, please input valid gateway and DNS address.

IP Address

IP address is a dispatched 32 bites address of the device in Internet. IP address includes 2 parts: Net-ID and Host-ID. The default IP address of the device is 192.168.1.254 .

Subnet Mask

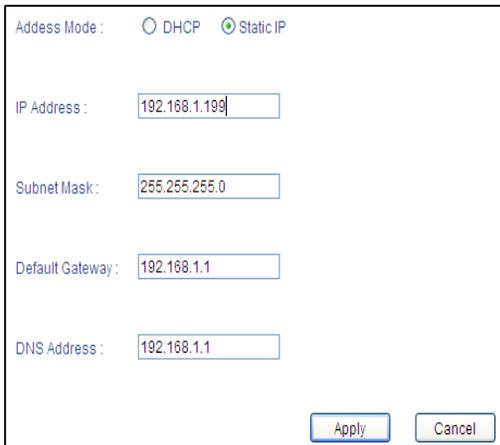
Mask is corresponding 32 bits number of IP address. Some are 1, the others are 0. These 1 and 0 can be combined arbitrary in principle, but the first continuous bits are 1 when designing subnet mask. IP address can be divided into 2 parts by subnet mask: subnet address and host address. 1 in IP address 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.

DNS Address

DNS is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities.



The screenshot shows a network configuration dialog box with the following fields and values:

- Address Mode: DHCP Static IP
- IP Address: 192.168.1.199
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.1.1
- DNS Address: 192.168.1.1

Buttons: Apply, Cancel

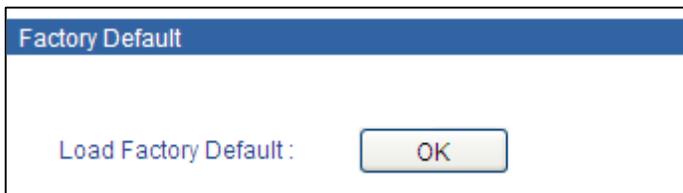


Note

- The IP address range is 92.168.x.x, 162.[16-31].x.x, or 10.x.x.x NTP and EMAIL will use DNS service. If you need to use these two functions, please input the right DNS address.

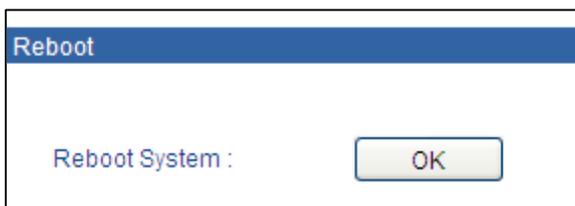
System File Update

This function includes 5 kinds: Factory Defaults, Reboot, Download Configuration, Upload Configuration and upgrade Firmware.



The screenshot shows a dialog box titled "Factory Default" with the following text and button:

Load Factory Default :



The screenshot shows a dialog box titled "Reboot" with the following text and button:

Reboot System :

Update Configuration File From Local PC

Download Configuration :

Upload Configuration :

Upgrade Firmware From Local PC

Upgrade Firmware :

1. Factory Default

If you know the IP address of the device, user name and password: Use IE to login Web interface. Click "System Management" Click "System File Update"

Choose "Factory Default" 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. Reboot

Click "OK", the device reboot. Before reboot, please save all configuration, otherwise the unsaved configuration would be lost after reboot.

3. Download Configuration

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

- Use IE to login Web interface.
- Click "System Management"
- Click "System File Update"
- Choose "Download Configuration"
- Click "Download"
- Choose the name of the file and the place to save.

4. Upload Configuration

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

- Use IE to login Web interface.
- Click "System Management"
- Click "System File Update"
- Choose "Upload Configuration"
- Click "Upload"

5. Upgrade Firmware

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

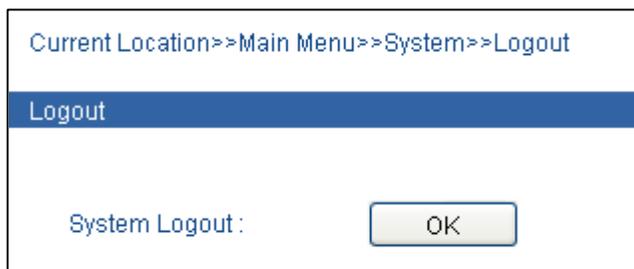
- Use IE to login Web interface.
- Click "System Management"
- Click "System File Update"
- Choose "Upgrade Firmware"
- Click "Browse" and find the place of uploading the file.
- Click "Upgrade" A suggestion" interruption of power is not allowed during uploading", confirm it.



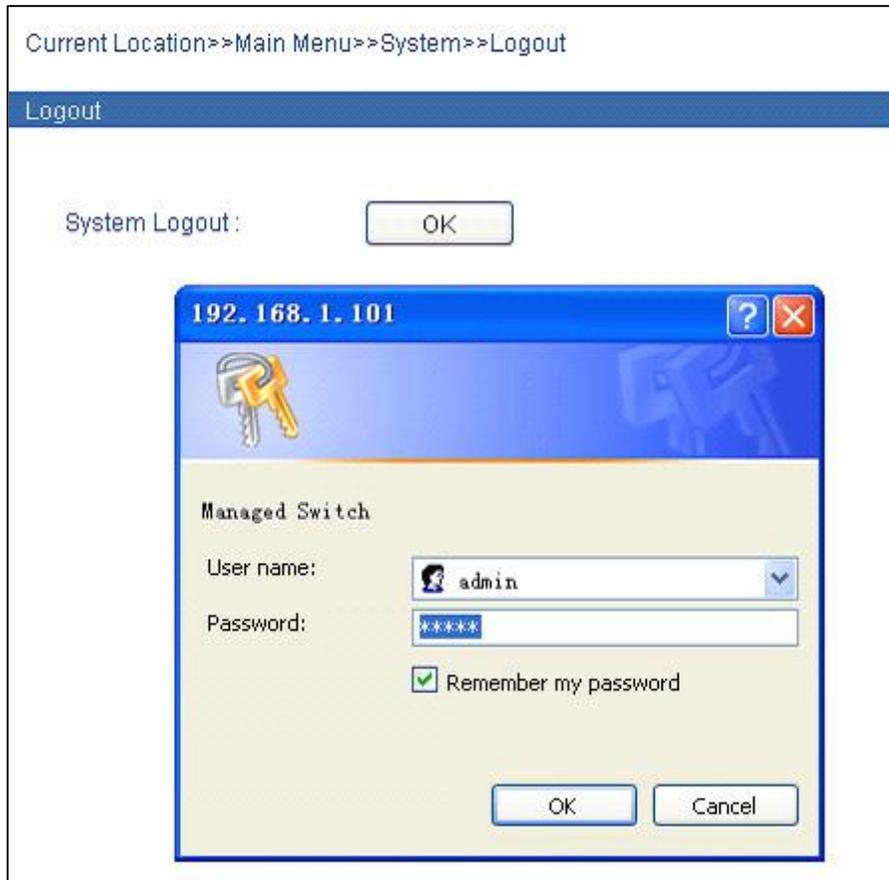
Note

- Factory Default setting restores all status to default status, the default IP address is "192.168.1.254".

Logout Exit from the WEB interface.



Click "OK" and you will see the picture below.



Click "Cancel" you will logout the interface.

You will see a message stating that "access is unauthorized".

Default Settings

Main Menu	Subitem	Rules of Web Interface	Default Settings
System Status	Overview	Name	RLH-XXXXXXX-XX-X
		Type	RLH-XXXXXXX-XX-X
		Description	
		Serial No.	2009122800001
		Contact Information	
Port Configuration	Port Settings	Port enable	Enable
		Speed	Auto-negotiation
		Flow control	Enable
	Bandwidth Management	Egress bandwidth	Disable
		Ingress bandwidth	Disable
Storm Suppression		Disable	
L2 Features	QoS	Qos Classification	Disable
		Cos	Disable
		DSCP	Disable
	VLAN	802.1Q VLAN	Disable
		Port-based VLAN	Enable
	IGMP Snooping		Disable
Static Multicast FWD		Disable	
Redundancy	Port Trunking		Disable
	Rapid Ring	SWRING II	Disable
		SWRING III	Disable
Access Control	Login Settings		Disable
	Access Profile		Disable
	Static Unicast FWD		Disable
Port statistics	Rx frame statistics		
	Tx frame statistics		
	Traffic Statistics		
Diagnosis	Port Mirroring		Disable
	Diagnosis		
System	Device IP	IP	192.168.1.254
		Subnet mask	255.255.255.0
		Default gateway	192.168.1.1

6. Specifications

General Specifications

Standards	IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3z, IEEE 802.1Q, IEEE 802.1D, IEEE 802.1x compliant				
Ports	16 10/100M TCP ports				
	8 100 FX 1x9 optical ports				
MAC address	8K				
Switching mode	Store & forward architecture and performs forwarding and filtering at non-blocking full wire speed				
VLAN	IEEE 802.1Q Port-based VLAN				
QOS	Supports IEEE802.1P QoS, supports WRR				
Flow Control Mode	IEEE 802.3x flow control for full-duplex mode and collision-based back-pressure for half-duplex mode				
LED Indicators	Link/Act for each port				
	Power ON				
	SYS	ON/OFF	System operation status		
Port Management	Imbedded Web Management/ console port				
Fiber Type / Connector / Distance (See Note 1)	Single Fiber, Bi-directional	Multimode	SC	2km / 1.2 miles	
		Single-mode	ST, SC	20km / 12.4 miles 60km / 36 miles	
	Dual Fiber	Multimode	ST, SC	2km / 1.2 miles	
		Single-mode	ST, SC	20km / 12.4 miles 60km / 36 miles 120km / 74 miles	
Fiber	Multimode	62.5/125, 50/125 μm			
	Single-mode	9/125 μm			
Dimensions	W 17.4" x D 8." x H 1.75" / 441.6mm x 206.9mm x 44.6mm EIA 19" Rack Mountable, 1RU rack height				
Power	90~264VAC/1.2A max, 50/60Hz, 35W				
Temperature	Operating	-40°F to +167°F (-40°C to +75°C)			
	Storage	-45°F to +185°F (-45°C to +85°C)			
Humidity	10%~95% non-condensing				
Warranty	Limited 5 years	Visit www.fiberopticklink.com for warranty details			

Note:

1. Refer to ordering information for available connector/fiber type/distance configurations.

7. Troubleshooting

First Step: Isolate the problem

Following the installation procedure will greatly speed any troubleshooting. It is designed to get the system up and running quickly during installation.

Isolating the source of trouble is essential to determining the steps needed to fix the problem. Most installation problems can be easily fixed in the field once the problem is properly identified.

Common Issues

Most problems encountered during installation and testing can be attributed to these 5 issues:

- **Problems with the incoming signal**
- **Problems providing correct power to the system**
- **Problems with the copper connections wiring**
- **Problems with the fiber optic cable or connectors**
- **Problems with configuration**

RLH Ethernet switch systems are built to the highest standards and fully tested before leaving the factory.

Isolating and ruling out common issues with the installation will help determine if there is a problem with the unit itself.

If trouble is encountered, verify all copper and fiber connections and settings. Refer to the LED Indicators on the front panel. They show availability of power, modes of operation, and data being received by the fiber and TP ports.

Reset and test in the factory default mode. If trouble persists, replace the unit and retest. If technical assistance is required, contact RLH Industries, Inc. technical support department:

800-877-1672 (6 am to 6 pm- PST), or call our 24/7 Technical/Customer Service: Toll Free 1-855-RLH-24X7 (1-855-754-2497)

8. Ordering Information

Part Number and Configurations

Each unit is identified by the part number.

Optics	Side	Distance	Wavelength	Fiber	Part Number
Multimode ST	-	2 km/1.2 mi	1310nm	62.5 μm	RLH-ESM1608-04-1
Multimode SC	-	2 km/1.2 mi	1310nm	62.5 μm	RLH-ESM1608-03-1
Bi-Directional Multimode SC	A	2 km/1.2 mi	Tx 1310nm / Rx 1550nm	62.5 μm	RLH-ESM1608-01-1
	B	2 km/1.2 mi	Tx 1550nm / Rx 1310nm	62.5 μm	RLH-ESM1608-02-1
Single-mode ST	-	20km/12.4mi.	1310nm	8~9 μm	RLH-ESM1608-50-1
	-	60km / 37mi.	1310nm	8~9 μm	RLH-ESM1608-51-1
	-	120km / 74 mi.	1550nm	8~9 μm	RLH-ESM1608-55-1
Single-mode SC	-	20km/12.4mi.	1310nm	8~9 μm	RLH-ESM1608-40-1
	-	60km / 37mi.	1310nm	8~9 μm	RLH-ESM1608-41-1
	-	120km / 74 mi.	1550nm	8~9 μm	RLH-ESM1608-45-1
Bi-Directional Single-mode SC	A	20km/12.4mi.	Tx 1310nm / Rx 1550nm	8~9 μm	RLH-ESM1608-10-1
	B	20km/12.4mi.	Tx 1550nm / Rx 1310nm	8~9 μm	RLH-ESM1608-11-1
	A	60km / 37mi.	Tx 1310nm / Rx 1550nm	8~9 μm	RLH-ESM1608-14-1
	B	60km / 37mi.	Tx 1550nm / Rx 1310nm	8~9 μm	RLH-ESM1608-15-1

- ▶ Bidirectional single fiber models require an **A** unit and **B** unit for a complete system.
- ▶ Bidirectional optic wavelength may be special ordered. Contact factory for availability.
- ▶ Please contact your RLH sales representative for pricing and delivery information.

9. Support

Technical Support

Email:	support@fiberopticlink.com
24/7 technical support:	Toll Free 1-855-RLH-24X7
	Toll Free 1-855-754-2497

Contact Information

Corporate Headquarters:	RLH Industries, Inc. 936 N. Main Street Orange, CA 92867 USA
Phone:	(714) 532-1672 Toll Free 1-800-877-1672 Toll Free 1-866-DO-FIBER
Fax:	(714) 532-1885
Email:	info@fiberopticlink.com
Web site:	www.fiberopticlink.com



RLH Industries, Inc.
936 N. Main Street, Orange, CA 92867 USA
T: (714) 532-1672
F: (714) 532-1885

Please contact your RLH sales representative
for pricing and delivery information.

Specifications subject to change without notice.