



## **TGRS-T120-M12X**

### **EN50155 12-port managed router switch**

## **User Manual**

**Version 1.0**

**May, 2020**

[www.oringnet.com](http://www.oringnet.com)

## Table of Content

<b>Getting Started .....</b>	<b>5</b>
1.1 About the TGRS-T120-M12X Series.....	5
1.2 Software Features .....	5
1.3 Hardware Specifications .....	6
<b>Hardware Overview .....</b>	<b>7</b>
2.1 Front Panel.....	7
2.2 Front Panel LED.....	8
<b>Hardware Installation.....</b>	<b>9</b>
3.1 Wall-mount Installation.....	9
3.2 Wiring .....	10
3.2.1 Grounding .....	10
3.2.2 Fault Relay.....	11
3.2.3 Power Input .....	11
3.3 Connection.....	11
3.3.1 Cables .....	11
3.3.2 O-Ring/O-Chain.....	13
<b>Redundancy .....</b>	<b>17</b>
4.1 O-Ring (Pending) .....	17
4.1.1 Introduction .....	17
4.1.2 Configurations .....	17
4.2 O-Chain (Pending).....	19
4.2.1 Introduction .....	19
4.2.2 Configurations .....	19
4.3 Bypass .....	20
4.3.1 Introduction .....	20
4.3.2 Bypass & Ring Topology .....	21
<b>Management via Web Browser.....</b>	<b>24</b>
5.1 Basic Settings .....	25
5.1.1 System Setting.....	26
5.1.2 WAN IP Settings .....	27
5.2 Admin & Password .....	28
5.2.1 LAN IP Setting .....	28

5.2.2	Time Configuration .....	30
5.2.3	LLDP .....	31
5.2.4	Backup/Restore Configurations.....	32
5.2.5	Firmware Update .....	32
5.3	Routing Protocol .....	32
5.3.1	NAPT Settings.....	33
5.3.2	Port Forwarding .....	33
5.3.3	DMZ .....	34
5.3.4	Static NAT (1:1 NAT) .....	35
5.3.5	Static Routing .....	36
5.3.6	Routing Security Group .....	37
5.3.7	Routing Table .....	38
5.3.8	IGMP Proxy .....	39
5.3.9	Multicast Routing Table.....	39
5.3.10	VRRP Setting .....	40
5.3.11	VRRP State .....	42
5.4	ETBN Protocol .....	42
5.4.1	TTDP Setting.....	42
5.4.2	TTDP Topology .....	44
5.4.3	Dynamic Setting .....	44
5.4.4	R-NAT .....	44
5.4.5	LAN IP .....	46
5.4.6	WAN IP .....	47
5.5	Backbone Switch .....	48
5.5.1	Port Setting .....	48
5.5.1.1	Port Control .....	48
5.5.1.2	Port Status .....	48
5.5.1.3	Port Trunk .....	49
5.5.1.3.1	Port Trunk - Setting .....	50
5.5.2	Vlan.....	50
5.5.2.1	Vlan Setting.....	50
5.6	Consist Switch .....	51
5.6.1	Redundancy .....	51
5.6.1.1	RSTP .....	51
5.6.1.1.1	Bridge Setting.....	51
5.6.1.2	MSTP.....	54
5.6.1.2.1	Bridge Setting.....	55

5.6.1.2.2 Bridge Port .....	56
5.6.1.2.3 Instance Setting .....	57
5.6.1.2.4 Instance port.....	58
5.6.1.3 Multicast .....	59
5.6.1.3.1 IGMP Snooping .....	59
5.6.1.3.2 Static Multicast Filtering .....	60
5.6.1.4 Port Setting .....	60
5.6.1.4.1 Port Control .....	61
5.6.1.4.2 Port Status .....	61
5.6.1.4.3 Port Alias.....	62
5.6.1.4.4 Egress.....	62
5.6.1.4.5 Ingress.....	63
5.6.1.4.6 Port Trunk .....	63
5.6.1.5 VLAN .....	65
5.6.1.5.1 802.1Q VLAN .....	65
5.6.1.5.2 Port Based VLAN .....	66
5.6.1.6 Traffic Prioritization.....	67
5.6.1.6.1 QoS Policy .....	68
5.6.1.6.2 Port-based Priority .....	69
5.6.1.6.3 COS/802.1p.....	69
5.6.1.6.4 TOS/DSCP.....	71
5.7 DHCP Server.....	71
5.7.1 Basic Setting.....	71
5.7.2 Client List and Static IP .....	72
5.7.3 Port and IP Binding.....	73
5.8 SNMP .....	74
5.8.1 Agent Setting .....	74
5.8.2 Trap Setting .....	75
5.8.3 SNMPv3 Setting .....	76
5.8.3.1 SNMPv3 User Configuration .....	76
5.8.3.2 SNMPv3 Group Configuration .....	77
5.8.3.3 SNMPv3 View.....	78
5.8.3.4 SNMPv3 Access Configuration .....	78
5.9 Security .....	79
5.9.1 Management Security.....	79
5.9.2 NAPT Only .....	80
5.9.3 Static MAC Address .....	81

5.10	Warming .....	82
5.10.1	Fault Relay Alarm .....	82
5.10.2	SYSLOG Setting.....	83
5.10.3	SMTP Setting.....	83
5.10.4	Event Selection .....	85
5.11	System Monitor and Diag.....	86
5.11.1	System Event Log .....	86
5.11.2	Ping Watchdog.....	86
5.11.3	CPU Loading Average .....	87
5.11.4	Temperature Monitor .....	87
5.11.5	Cable Diagnostics .....	87
5.12	System Reboot .....	88
5.13	Logout.....	89
<b>Command Line Management.....</b>		<b>90</b>
<b>Technology.....</b>		<b>97</b>

# Getting Started

## 1.1 About the TGRS-T120-M12X Series

ORing's Transporter™ series managed Router switches are designed for industrial applications such as rolling stock, vehicle, and railway. The TGRS-T120-M12X-BP2-WV, which is compliant with the EN50155 standard, is a managed Gigabit Redundant Ring Ethernet switch with 12x10/100/1000Base-T(X) ports which is specifically designed for the toughest and fully compliant with EN50155 requirement. The switch support IEC 61375-2-5 TTDP (Train Topology Discovery Protocol) and IEC 61375-2-3 TRDP (Train Real-Time Data Protocol) for railway application, improving the operational efficiency and minimize configuration errors. It is specifically designed for the toughest industrial environments. TGRS-T120-M12X-BP2-WV EN50155 Ethernet switch uses M12 connectors to ensure tight, robust connections, and guarantee reliable operation against environmental disturbances, such as vibration and shock. TGRS-T120-M12X-BP2-WV EN50155 provides a wide power input range from 24 to 110VDC. TGRS-T120-M12X-BP2-WV includes 2 sets of bypass ports that protect the network from failures and Network maintenance by ensuring network integrity during power loss. And support wide operating temperature from -25°C to 70°C. TGRS-T120-M12X-BP2-WV can also be managed centralized and convenient by Open-Vision, as well as the Web-based interface, Telnet and console (CLI) configuration. Therefore, the router switch is one of the most reliable choice for highly-managed and railway application.

## 1.2 Software Features

- Leading EN50155 compliant Ethernet switch for rolling stock application
- Support TTDP (IEC 61375-2-5) protocol
- Support TRDP (IEC 61375-2-3) protocol
- Easy network setup with network address translation (NAT)
- R-NAT (Railway Network Address Translation) for train IP management
- Provided HTTPS/SSH protocol to enhance network security
- Supports SMTP client
- Supports QoS management
- IGMP v2/v3 (IGMP snooping support) for filtering multicast traffic
- Supports SNMP v1/v2c/v3 & RMON & 802.1Q VLAN Network Management
- Supports 10K Bytes Jumbo Frame
- Multiple notification for warning of unexpected event
- Web-based, Telnet, Console (CLI), and Windows utility (Open-Vision) configuration

- Support LLDP Protocol
- Rigid IP-30 housing design
- Wall mounting enabled
- Wide range power input from 24-110VDC

## 1.3 Hardware Specifications

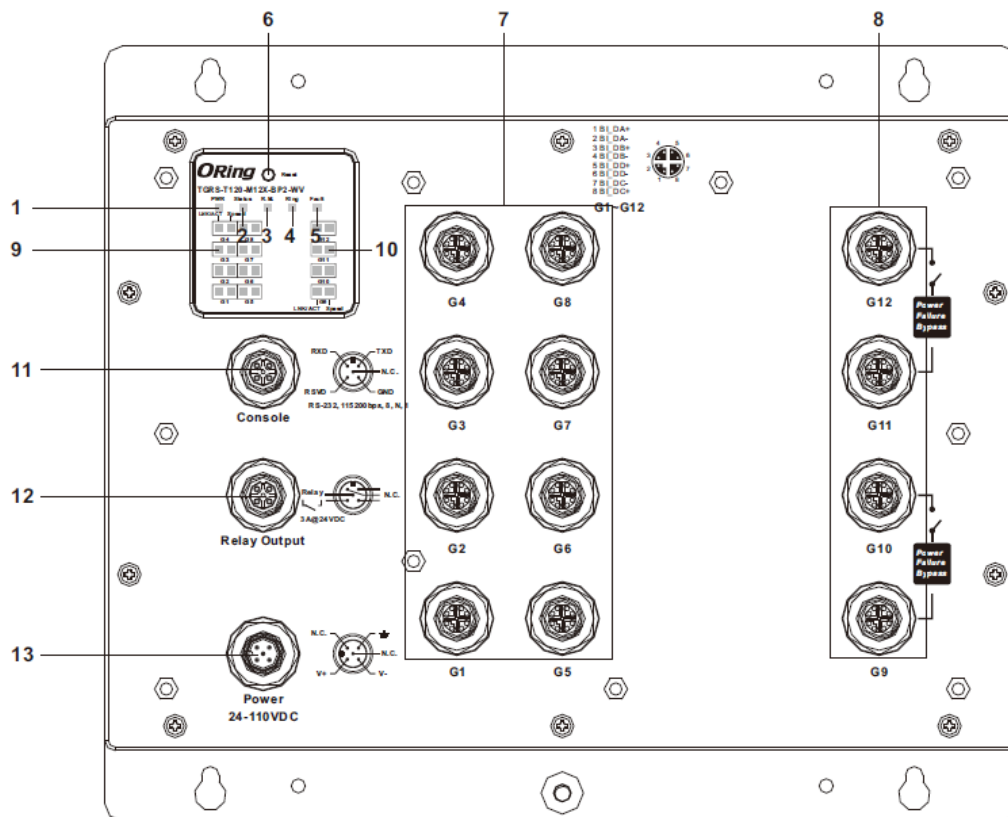
- LAN x 8 (8-pin M12 female X-Coding connector in G1 ~ G8 ports)
- WAN x 4 (8-pin M12 female X-Coding connector in G9 ~ G12 ports)
- 1 x console port
- 2 sets of bypass ports in WAN Ports
- Operating temperature: -25 to 70°C
- Storage temperature: -40 to 85°C
- Operating humidity: 5% to 95%, non-condensing
- Casing: IP-30
- Wall-mount installation
- Wide-range power input form 24 ~ 110VDC

# Hardware Overview

## 2.1 Front Panel

The device provides the following ports on the front panel. All connectors are in M12 type to ensure tight, robust connections, as well as reliable operation against environmental disturbances, such as vibration and shock.

Port	Description
Power connector	1 x power connector (5-pin A-Coding, male type)
ports	LAN x 8 (8-pin X-Coding, female type) WAN x 4 (8-pin X-Coding, female type)
Console	1 x console port (5-pin A-coding, female type)
Relay output	1 x relay output (5-pin A-coding, female type)
Reset button	1 x reset button





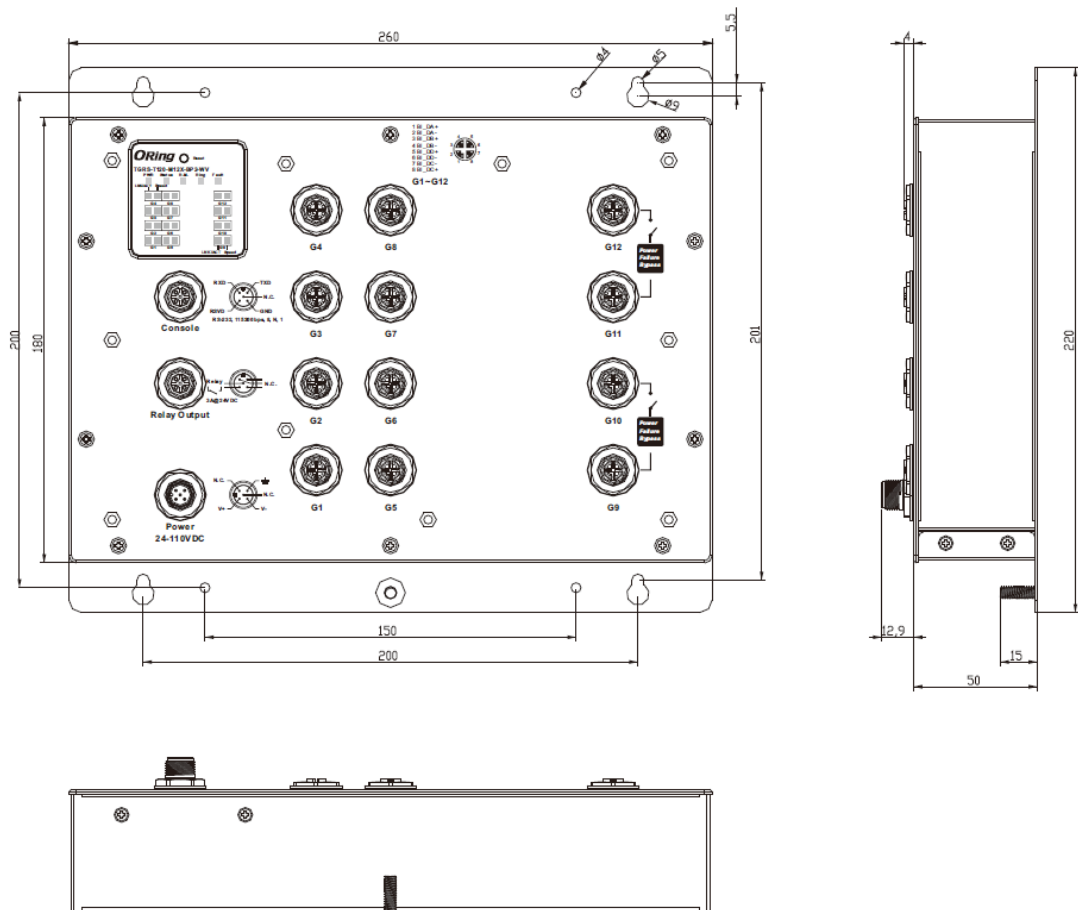
1. Power status LED
2. System status LED
3. R.M. status LED
4. Ring status LED
5. Fault LED
6. Reset button
7. Ethernet LAN ports
8. Ethernet WAN ports with bypass
9. Link/ACT LED for Gigabit ports
10. Speed LED for Gigabit ports
11. Console port
12. Relay output
13. Power connector

## 2.2 Front Panel LED

LED	Color	Status	Description
PWR	Green	On	DC power module activated
Status	Green	On	System work
R.M (Pending)	Green	On	Device operating in Ring Master mode
Ring (Pending)	Green	On	Ring enabled
		Blinking	Ring structure is broken
Fault	Amber	On	Errors occur (i.e. power failure or port malfunctioning)
10/100/1000Base-T(X) LAN Port (G1 ~ G8)			
LNK/ACT	Green	On	Port is linked
		Blinking	Transmitting data
Speed	Green	On	Port is running at 1000Mbps
		OFF	Port is running at 10/100Mbps
10/100/1000Base-T(X) WAN Port (G9 ~ G12)			
LNK/ACT	Green	On	Port is linked
		Blinking	Transmitting data
Speed	Green	On	Port is running at 1000Mbps
		OFF	Port is running at 10/100Mbps

# Hardware Installation

## 3.1 Wall-mount Installation



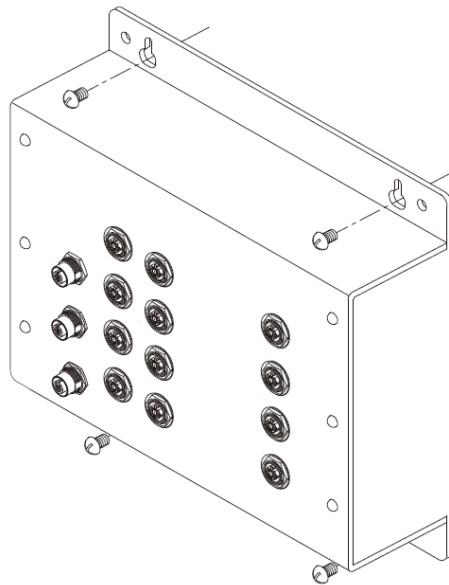
Wall-mount Measurement (Unit = mm)

Follow the steps below to mount the switch to the wall.

Step 1: Hold the switch upright against the wall

Step 2: Insert two screws through the screw holes located at the top and bottom of the unit and fasten the screw to the wall with a screwdriver.

Step 3: Slide the switch downwards and tighten the screws for added stability.



Instead of screwing the screws in all the way, it is advised to leave a space of about 2mm to allow room for sliding the switch between the wall and the screws.

## 3.2 Wiring

---



### **WARNING**

Do not disconnect modules or wires unless power has been switched off or the area is known to be non-hazardous. The devices may only be connected to the supply voltage shown on the type plate.

---



### **ATTENTION**

1. Be sure to disconnect the power cord before installing and/or wiring your switches.
  2. Calculate the maximum possible current in each power wire and common wire. Observe all electrical codes dictating the maximum current allowable for each wire size.
  3. If the current goes above the maximum ratings, the wiring could overheat, causing serious damage to your equipment.
  4. Use separate paths to route wiring for power and devices. If power wiring and device wiring paths must cross, make sure the wires are perpendicular at the intersection point.
  5. Do not run signal or communications wiring and power wiring through the same wire conduit. To avoid interference, wires with different signal characteristics should be routed separately.
  6. You can use the type of signal transmitted through a wire to determine which wires should be kept separate. The rule of thumb is that wiring sharing similar electrical characteristics can be bundled together.
  7. You should separate input wiring from output wiring.
  8. It is advised to label the wiring to all devices in the system.
- 

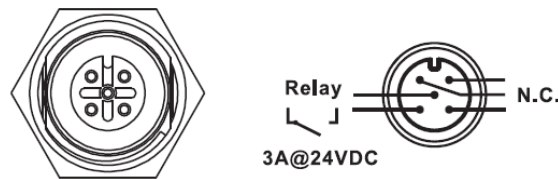
### 3.2.1 Grounding

Grounding and wire routing help limit the effects of noise due to electromagnetic interference (EMI).

Run the ground connection on the power connector to the grounding surface prior to connecting devices.

### 3.2.2 Fault Relay

The switch uses the M12 A-coded 5-pin Female connector on the front panel for relay output. Use a cable with an M12 A-coded 5-pin female connector to connect the relay contacts from the switch. The relay contacts will detect user-configured events and form an open circuit when an event is triggered.

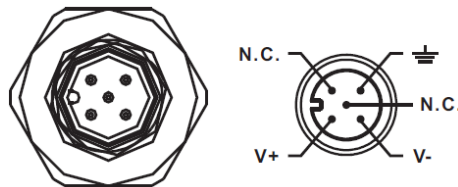


### 3.2.3 Power Input

The switch provides one set of power supply on a M12 5-pin A-code male connector to enable power input.

**Step 1:** Insert a power cable to the power connector on the device.

**Step 2:** Rotate the outer ring of the cable connector until a snug fit is achieved. Make sure the connection is tight.



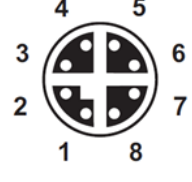
## 3.3 Connection

### 3.3.1 Cables

#### 10/100/1000BASE-T(X) PIN ASSIGNMENTS

The device provides Ethernet ports in M12 connector type. According to the link type, the switch uses CAT 3, 4, 5, 5e UTP cables to connect to any other network devices (PCs, servers, switches, routers, or hubs). Please refer to the following table for cable specifications.

## 8-Pin Gigabit Port Definition

 <b>X-Coding M12</b>	10/100/1000Base-T(X) M12 port	
	Pin No.	Description
	#1	BI_DA+
	#2	BI_DA-
	#3	BI_DB+
	#4	BI_DB-
	#5	BI_DD+
	#6	BI_DD-
	#7	BI_DC-
	#8	BI_DC+

Cable Types and Specifications:

Cable	Type	Max. Length	Connector
10BASE-T	Cat. 3, 4, 5 100-ohm	UTP 100 m (328 ft)	M12 X-coding connector
100BASE-TX	Cat. 5 100-ohm UTP	UTP 100 m (328 ft)	M12 X-coding connector
1000BASE-T	Cat. 5/Cat. 5e 100-ohm UTP	UTP 100 m (328ft)	M12 X-coding connector

Below is the pin assignment for the Ethernet ports.

10/100/1000Base-T(X) M12 port

Pin Number	Assignment
#1	BI_DA+
#2	BI_DA-
#3	BI_DB+
#4	BI_DB-
#5	BI_DD+
#6	BI_DD-
#7	BI_DC-
#8	BI_DC+

The device supports auto MDI/MDI-X operation. You can use a cable to connect the switch to a PC. The table below shows the 10/100Base-T(X) MDI and MDI-X port pin outs.

10/100 Base-T(X) MDI/MDI-X Pin Assignments:

Pin Number	MDI port	MDI-X port
1	TD+(transmit)	RD+(receive)
2	TD-(transmit)	RD-(receive)
3	RD+(receive)	TD+(transmit)
4	Not used	Not used
5	Not used	Not used
6	RD-(receive)	TD-(transmit)
7	Not used	Not used
8	Not used	Not used

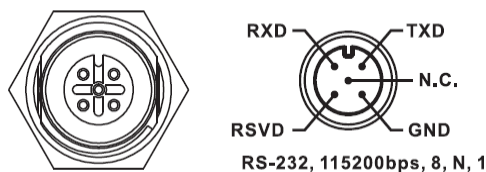
1000Base-T MDI/MDI-X Pin Assignments:

Pin Number	MDI port	MDI-X port
1	BI_DA+	BI_DB+
2	BI_DA-	BI_DB-
3	BI_DB+	BI_DA+
4	BI_DB-	BI_DA-
5	BI_DD+	BI_DC+
6	BI_DD-	BI_DC-
7	BI_DC-	BI_DD-
8	BI_DC+	BI_DD+

**Note:** “+” and “-” signs represent the polarity of the wires that make up each wire pair.

### Console port wiring

The switch has one RS-232 (M12 5pin female) console port, located on the front panel. Use a M12-to-DB9 console cable to connect the console port to your PC's COM port.

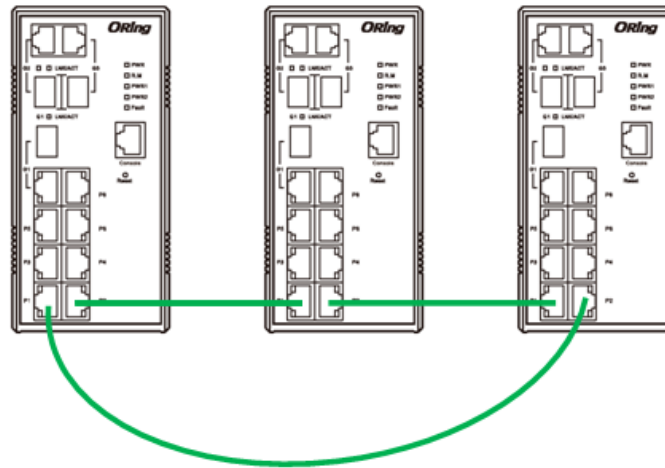


## 3.3.2 O-Ring/O-Chain

### O-Ring

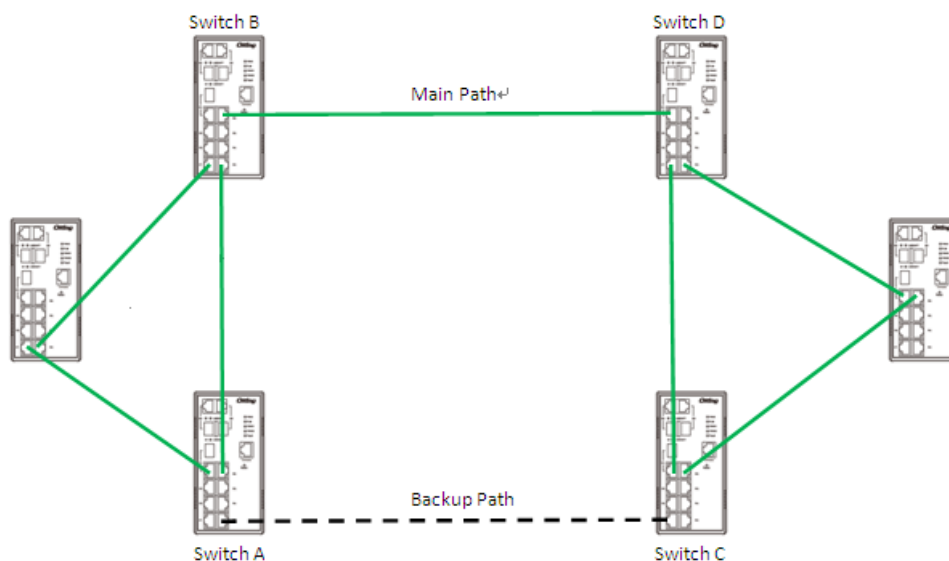
You can connect three or more switches to form a ring topology to gain network redundancy capabilities through the following steps.

1. Connect each switch to form a daisy chain using an Ethernet cable.
2. Set one of the connected switches to be the master and make sure the port setting of each connected switch on the management page corresponds to the physical ports connected. For information about the port setting, please refer to [4.1.2 Configurations](#).
3. Connect the last switch to the first switch to form a ring topology.



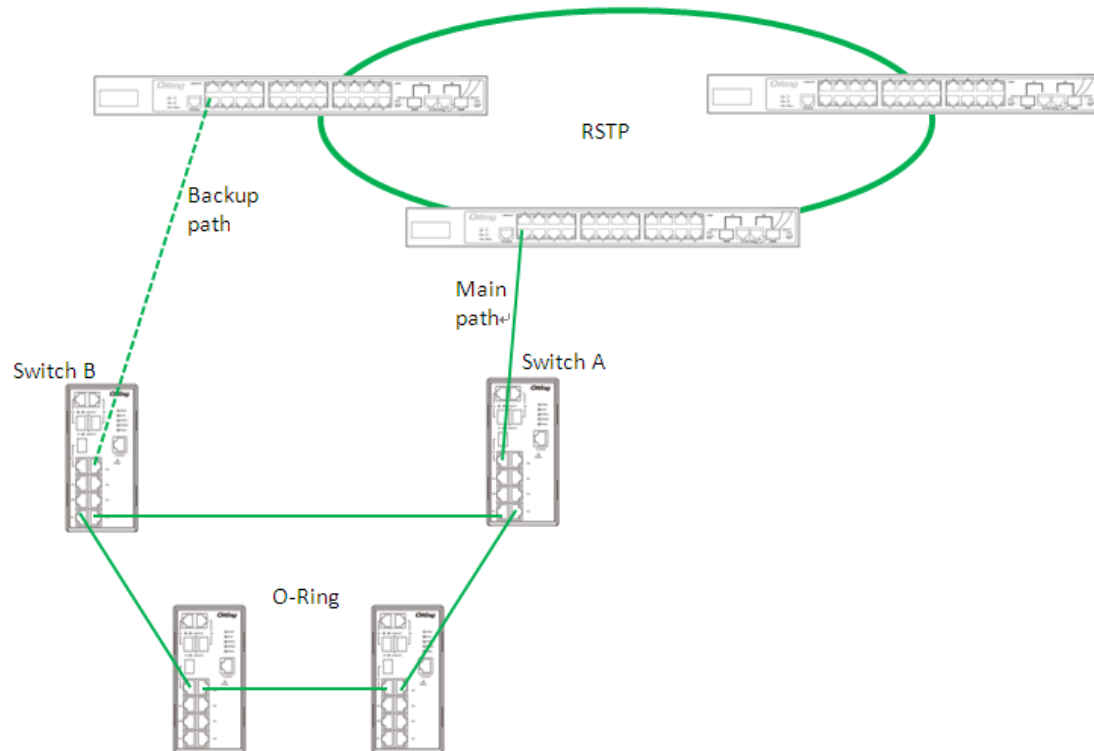
## Coupling Ring

If you already have two O-Ring topologies and would like to connect the rings, you can form them into a coupling ring. All you need to do is select two switches from each ring to be connected, for example, switch A and B from Ring 1 and switch C and D from ring 2. Decide which port on each switch to be used as the coupling port and then link them together, for example, port 1 of switch A to port 2 of switch C and port 1 of switch B to port 2 of switch D. Then, enable Coupling Ring option by checking the checkbox on the management page and select the coupling ring in correspondence to the connected port. For more information on port setting, please refer to [4.1.2 Configurations](#). Once the setting is completed, one of the connections will act as the main path while the other will act as the backup path.



## Dual Homing

If you want to connect your ring topology to a RSTP network environment, you can use dual homing. Choose two switches (Switch A & B) from the ring for connecting to the switches in the RSTP network (core switches). The connection of one of the switches (Switch A or B) will act as the primary path, while the other will act as the backup path that is activated when the primary path connection fails.

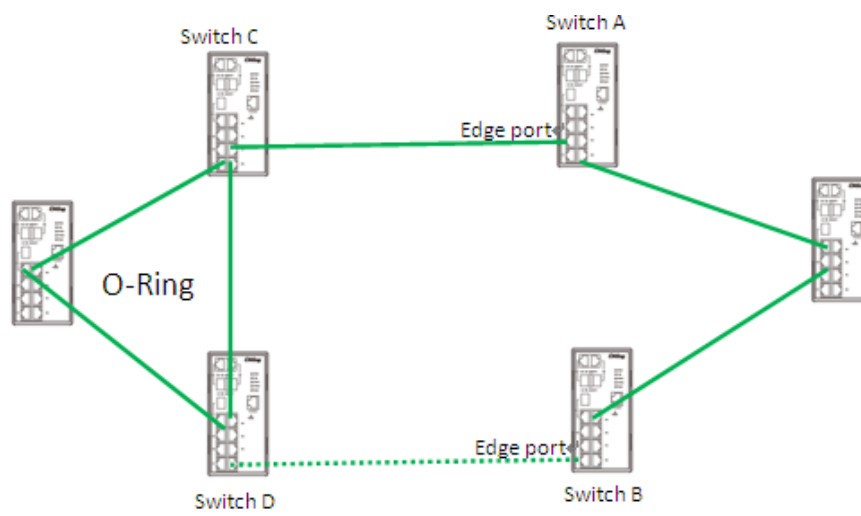


## O-Chain

When connecting multiple O-Rings to meet your expansion demand, you can create an O-Chain topology through the following steps.

1. Select two switches from the chain (Switch A & B) that you want to connect to the O-Ring and connect them to the switches in the ring (Switch C & D).
2. In correspondence to the port connected to the ring, configure an edge port for both of the connected switches in the chain by checking the box in the management page (see 4.2 Configurations).
3. Once the setting is completed, one of the connections will act as the main path, and the other as the backup path.





# Redundancy

Redundancy for minimized system downtime is one of the most important concerns for industrial networking devices. Hence, ORing has developed proprietary redundancy technologies including O-Ring and O-Chain featuring faster recovery time than existing redundancy technologies widely used in commercial applications, such as RSTP, and MSTP. ORing's proprietary redundancy technologies not only support different networking topologies, but also assure the reliability of the network.

**NOTE.** The O-Ring & O-Chain function is currently not included in the software function, and efforts are being made to integrate it.

## 4.1 O-Ring (Pending)

### 4.1.1 Introduction

O-Ring is ORing's proprietary redundant ring technology, with recovery time of less than 30 milliseconds (in full-duplex Gigabit operation) or 10 milliseconds (in full-duplex Fast Ethernet operation) and up to 250 nodes. The ring protocols identify one switch as the master of the network, and then automatically block packets from traveling through any of the network's redundant loops. In the event that one branch of the ring gets disconnected from the rest of the network, the protocol automatically readjusts the ring so that the part of the network that was disconnected can reestablish contact with the rest of the network. The O-Ring redundant ring technology can protect mission-critical applications from network interruptions or temporary malfunction with its fast recover technology.



### 4.1.2 Configurations

O-Ring supports three ring topologies: **Ring Master**, **Coupling Ring**, and **Dual Homing**. You can configure the settings in the interface below.

### O-Ring Configuration

<input checked="" type="checkbox"/> <b>O-Ring</b>		
<b>Ring Master</b>	Disable ▼	This switch is Not a Ring Master.
<b>1st Ring Port</b>	Port 1 ▼	LinkDown
<b>2nd Ring Port</b>	Port 2 ▼	LinkDown
<input type="checkbox"/> <b>Coupling Ring</b>		
<b>Coupling Port</b>	Port 3 ▼	LinkDown
<input type="checkbox"/> <b>Dual Homing</b>		
<b>Homing Port</b>	Port 4 ▼	LinkDown

Label	Description
Redundant Ring	Check to enable O-Ring topology.
Ring Master	Only one ring master is allowed in a ring. However, if more than one switches are set to enable <b>Ring Master</b> , the switch with the lowest MAC address will be the active ring master and the others will be backup masters.
1 <sup>st</sup> Ring Port	The primary port when the switch is ring master
2 <sup>nd</sup> Ring Port	The backup port when the switch is ring master
Coupling Ring	Check to enable <b>Coupling Ring</b> . <b>Coupling Ring</b> can divide a big ring into two smaller rings to avoid network topology changes affecting all switches. It is a good method for connecting two rings.
Coupling Port	Ports for connecting multiple rings. A coupling ring needs four switches to build an active and a backup link.  Links formed by the coupling ports will run in active/backup mode.
Dual Homing	Check to enable <b>Dual Homing</b> . When <b>Dual Homing</b> is enabled, the ring will be connected to normal switches through two RSTP links (ex: backbone Switch). The two links work in active/backup mode, and connect each ring to the normal switches in RSTP mode.
Apply	Click to apply the configurations.

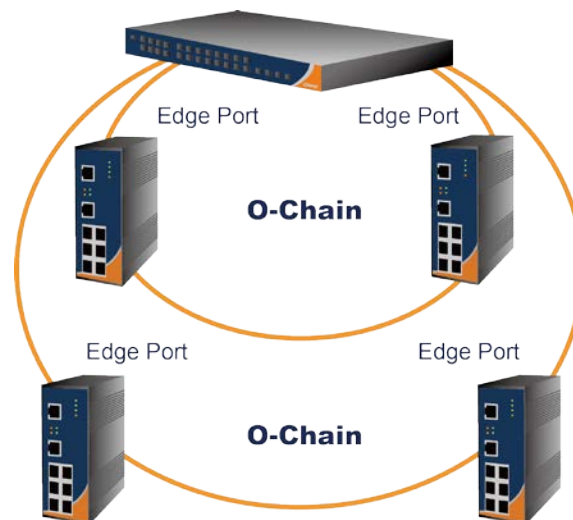
**Note:** due to heavy computing loading, setting one switch as ring master and coupling ring at the same time is not recommended.

## 4.2 O-Chain (Pending)

### 4.2.1 Introduction

O-Chain is ORing's revolutionary network redundancy technology which enhances network redundancy for any backbone networks, providing ease-of-use and maximum fault-recovery swiftness, flexibility, compatibility, and cost-effectiveness in a set of network redundancy topologies. The self-healing Ethernet technology designed for distributed and complex industrial networks enables the network to recover in less than 30 milliseconds (in full-duplex Gigabit operation) or 10 milliseconds (in full-duplex Fast Ethernet operation) for up to 250 switches if at any time a segment of the chain fails.

O-Chain allows multiple redundant rings of different redundancy protocols to join and function together as a large and the most robust network topologies. It can create multiple redundant networks beyond the limitations of current redundant ring technologies.



### 4.2.2 Configurations

O-Chain is very easy to configure and manage. Only one edge port of the edge switch needs to be defined. Other switches beside them just need to have O-Chain enabled.

**O-Chain**

☒ **Enable**

	Uplink Port	Edge Port	State
1st	Port.01	<input type="checkbox"/>	Linkdown
2nd	Port.02	<input type="checkbox"/>	Forwarding

Label	Description
Enable	Check to enable O-Chain function
1 <sup>st</sup> Ring Port	The first port connecting to the ring
2 <sup>nd</sup> Ring Port	The second port connecting to the ring
Edge Port	An O-Chain topology must begin with edge ports. The ports with a smaller switch MAC address will serve as the backup link and RM LED will light up.

## 4.3 Bypass

### 4.3.1 Introduction

Bypass provides reliable and uninterrupted connections of inline network devices when any of the devices encounter hardware failure such as power outage. Figure 1 shows the topology consisting of switches without bypass function. When any of the devices breaks down, the network will lose connection.

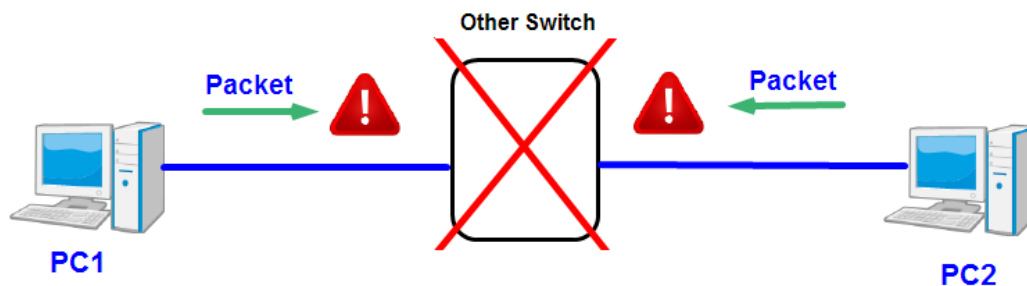


Figure 1

Figure 2 shows the topology consisting of switches with bypass functions. When one of the devices is unavailable, the network traffic will bypass the inactive device and continue to flow to other active devices, ensuring consistent connections.

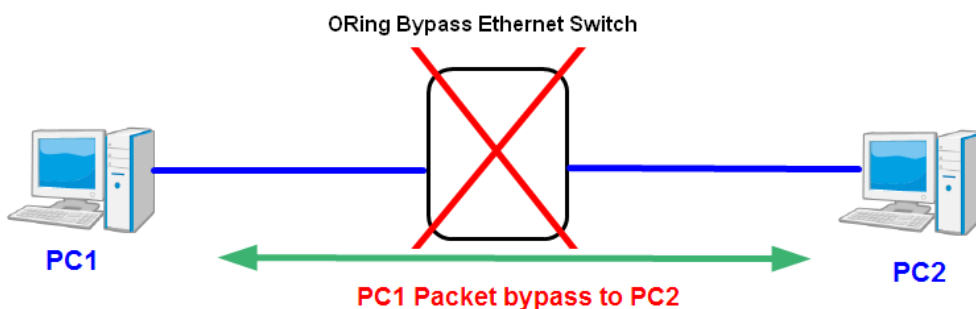
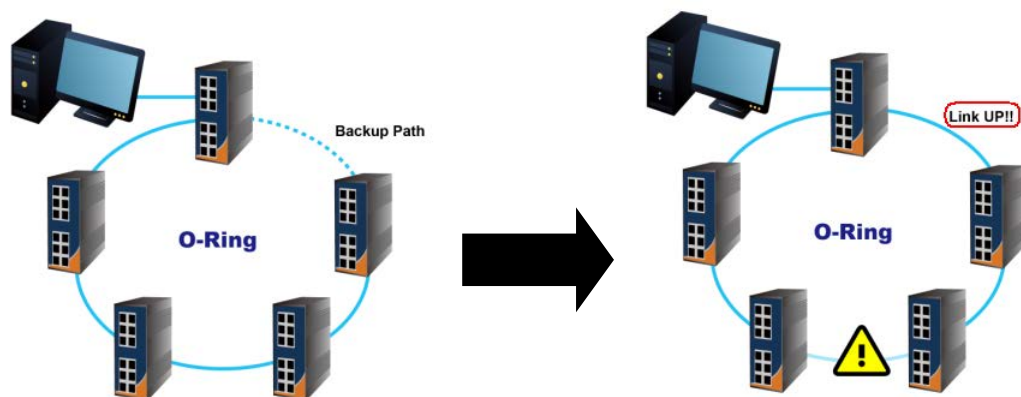


Figure 2

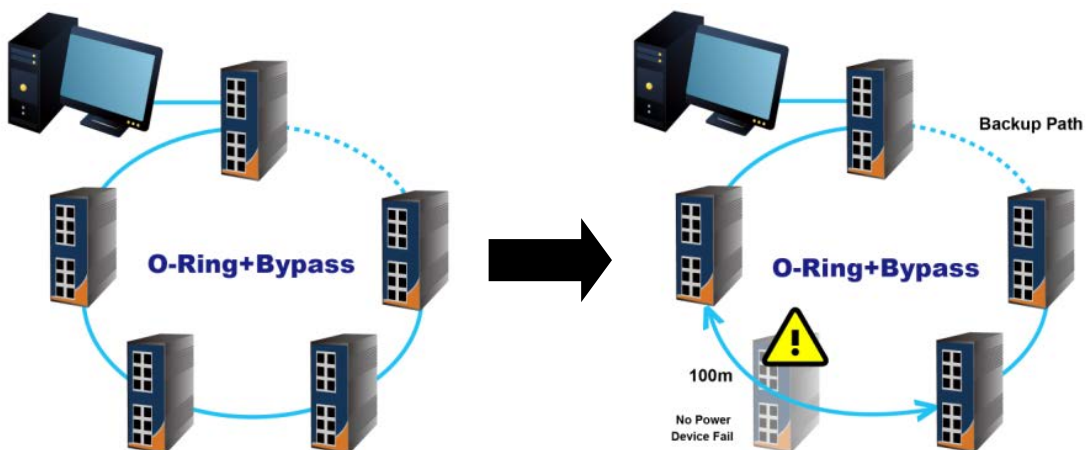
### 4.3.2 Bypass & Ring Topology

Bypass provides redundancy during device failure and O-Ring provides redundancy when links are broken. Together the two will provide users with dual protection when links and devices are broken.

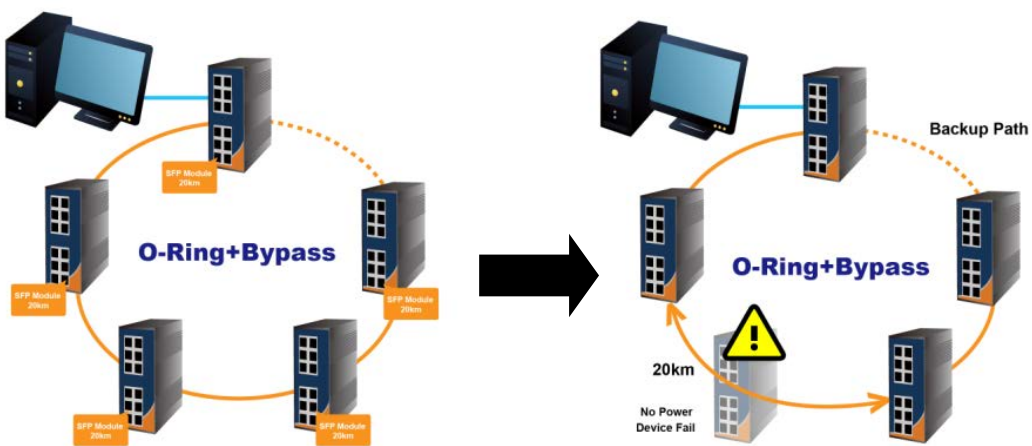
In a ring topology where switches are not bypass-enabled, the backup link will be activated immediately when one of the links is down, thereby ensuring uninterrupted data transmission. However, if any inline device fails, the network will be disconnected (see below).



By using bypass-enabled switches in a ring topology, data will continue to flow to the next active switch through the same route when one or more inline devices fail. Data will bypass the inactive switches during transmission as if they do not exist. In this case, the backup path will remain inactive and the ring topology will remain unchanged (see below).

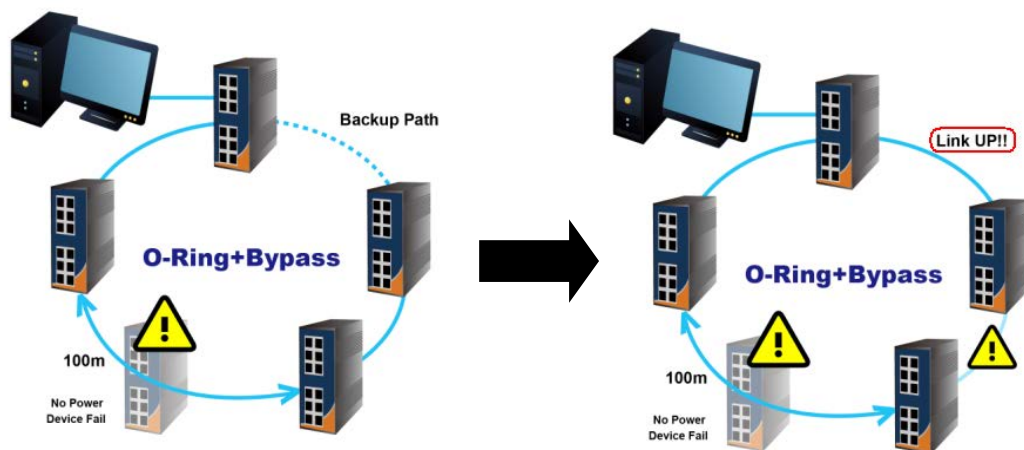


Ethernet Networks

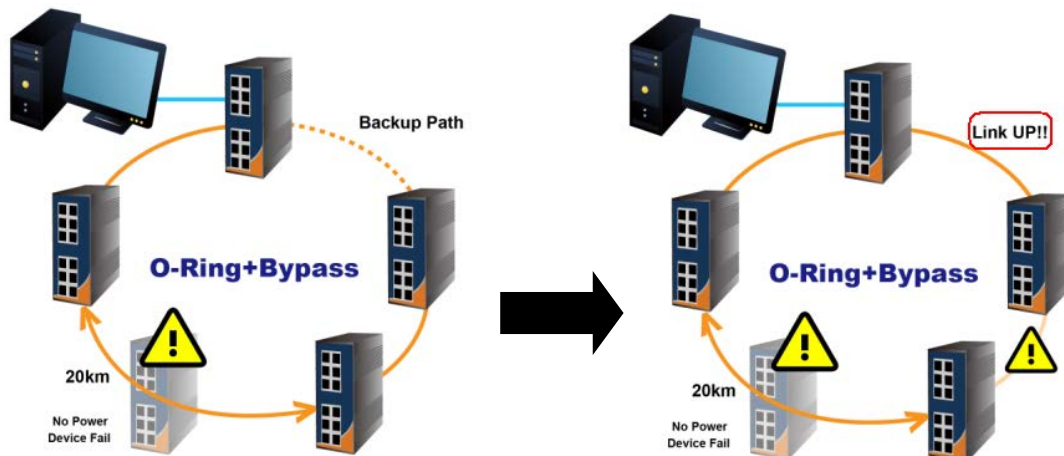


Fiber Networks

When a link between two switches fails following the breakdown of the switch, the backup link will be activated. Data will then be transmitted via the backup path (see below).



Ethernet Networks



Fiber Networks

**Note:** The maximum cable length for copper ports is 100 meters and 20km for fiber ports. When data bypasses the inactive switch(s) to another active switch, the distance between the two active switches must be within the maximum length, otherwise transmission will fail.

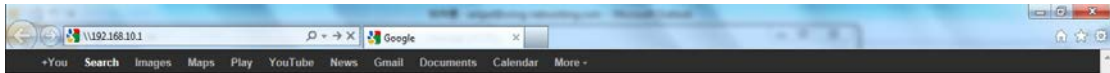


# Management via Web Browser

Follow the steps below to manage your switch via a Web browser

## System Login

1. Launch an Internet Explorer.
2. Type `http://` and the IP address of the switch. Press **Enter**.



3. A login screen appears.
4. Type in the username and password. The default username and password are **admin**.
5. Press **Enter** or click **OK**, the management page appears.

A screenshot of the login screen for the switch management page. The screen is divided into two main sections. The top section is titled 'Login' and contains a 'Logged Out' status, 'Enter User Name:' and 'Enter Password:' labels, two input fields, and a 'Login' button. The bottom section is titled 'Current Date & Time' and displays '04/14/20 1:07 PM BST'.

Note: you can use the following default values:

IP Address: **10.0.0.1**

Subnet Mask: **255.255.192.0**

User Name: **admin**

Password: **admin**

After logging in, you will see the information of the switch as below.

Information	
System Name:	TGRS-T120-M12X
System Description:	EN50155 12-port managed Giga router switch with 12x10/100/1000 Base-T(X), M12 connector
System Location:	-
System Contact:	-
System OID:	1.3.6.1.4.1.25972.100.6.0.348
<hr/>	
Model Name:	TGRS-T120-M12X
Loader Version:	L1.02
Kernel Version:	K28.13
Firmware Version:	V1.00
<hr/>	
Uptime:	0 days, 0 hours, 1 minutes
Current Date & Time:	03/26/20 6:50 AM UTC
<hr/>	
LAN DHCP Client:	Disabled
LAN IP Address:	10.0.0.1
LAN Netmask:	255.255.192.0
LAN MAC Address:	00:1E:94:FF:FF:DA
LAN Gateway IP:	-
LAN DNS Server(s):	-
<hr/>	
WAN DHCP Client:	Disabled
WAN IP Address:	10.128.0.1
WAN Netmask:	255.255.192.0
WAN MAC Address:	00:1E:94:FF:FF:DB
WAN Gateway IP:	-
WAN DNS Server(s):	-
<hr/>	

On the left side of the management interface shows links to various settings. Clicking on the links will bring you to individual configuration pages.

## 5.1 Basic Settings

The Basic Settings page allows you to configure the basic functions of the switch.

### 5.1.1 System Setting

This page shows the general information of the switch.

**System Setting**

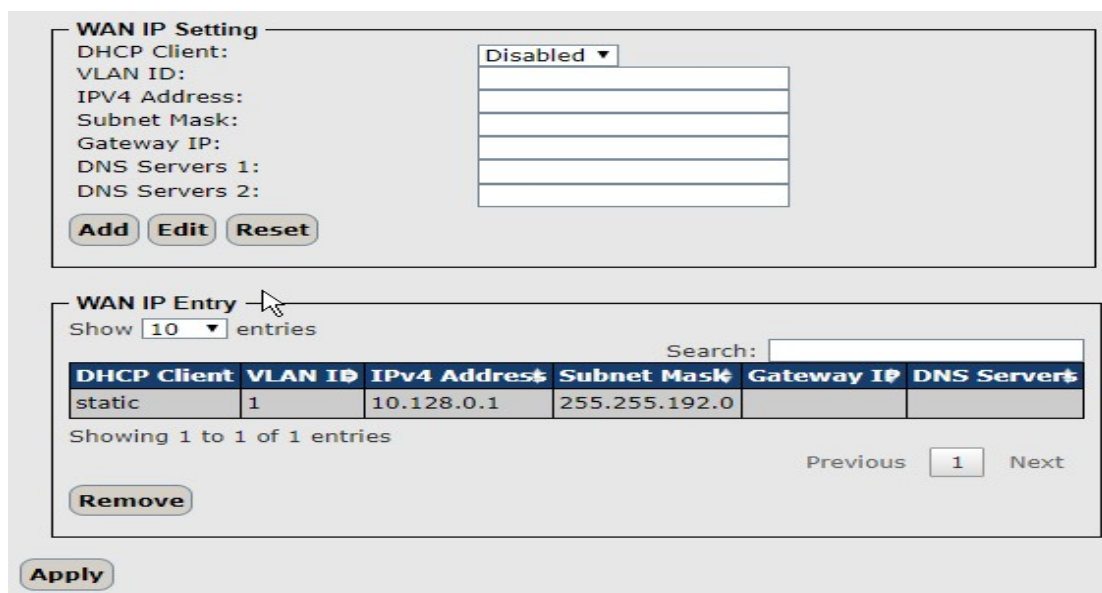
System Name: TGRS-T120-M12X  
System Description: EN50155 12-port managed Giga router swit  
System Location:   
System Contact:   
System OID: 1.3.6.1.4.1.25972.100.6.0.348  
Loader Version: L1.02  
Kernel Version: K28.13  
Firmware Version: V1.00  
MAC Address: 00:1E:94:FF:FF:DA

Save changes
Reset

Label	Description
System Name	An administratively assigned name for the managed node. By convention, this is the node's fully-qualified domain name. A domain name is a text string consisting of alphabets (A-Z, a-z), digits (0-9), and minus sign (-). Space is not allowed to be part of the name. The first character must be an alpha character. And the first or last character must not be a minus sign. The allowed string length is 0 to 255.
System Description	Description of the device
System Location	The physical location of the node (e.g., telephone closet, 3rd floor). The allowed string length is 0 to 255, and only ASCII characters from 32 to 126 are allowed.
System Contact	The textual identification of the contact person for this managed node, together with information on how to contact this person. The allowed string length is 0 to 255, and only ASCII characters from 32 to 126 are allowed.
Save changes	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

### 5.1.2 WAN IP Settings

This page allows you to configure WAN IP Setting for the switch. You can specify configure the settings manually by disabling DHCP Client. After inputting the values, click **Add/Edit** and the new values will be applied, which will be displayed under **Current**.



Label	Description
DHCP Client	Enable the DHCP client by checking this box. If DHCP fails or the configured IP address is zero, DHCP will retry. If DHCP retry fails, DHCP will stop trying and the configured IP settings will be used.
IPv4 Address	Assigns the IP address of the network in use. If DHCP client function is enabled, you do not need to assign the IP address. The network DHCP server will assign an IP address to the switch and it will be displayed in this column. The default IP is <b>10.128.0.1</b> .
Subnet Mask	Assigns the subnet mask of the IP address. If DHCP client function is enabled, you do not need to assign the subnet mask 255.255.192.0.
Gateway IP	Assigns the network gateway for the switch. The default gateway is <b>empty</b> .
VLAN ID	Provides the managed VLAN ID. The allowed range is 1 through 4094.
DNS Server	Enter the IP address of the DNS server in dotted decimal notation.
Add	Set IP to Add
Edit/Reset	Clicking WAN IP entry , Edit 、 Reset or Remove
Reset	Click to undo any changes made locally and revert to previously saved values

## 5.2 Admin & Password

This page allows you to configure the system password required to access the web pages or log in from CLI.

**Account**

User Name:

Password:

Confirm Password:

Permission Level: Admin ▼

**Add User** **Delete User**

**User List**

Username	Permission
admin	Admin

Label	Description
User Name	Input New user Name.
Password	Input New password.
Confirm Password	Re-type the new password.
Permission Level	Set New User Permission
Add User/Delete User	Add New User/Delete User
Save Changes	Click to save changes.

### 5.2.1 LAN IP Setting

This page allows you to configure LAN IP Setting for the switch. You can specify configure the settings manually by disabling DHCP Client. After inputting the values, click **Add/Edit** and the new values will be applied, which will be displayed under **Current**.

### LAN IP Setting

DHCP Client: Disabled ▾  
VLAN ID:   
IPv4 Address:   
Subnet Mask:   
Gateway IP:   
DNS Servers 1:   
DNS Servers 2:

Add Edit Reset

### LAN IP Entry

Show 10 ▾ entries

Search:

DHCP Client	VLAN ID	IPv4 Address	Subnet Mask	Gateway IP	DNS Server
static	1	10.0.0.1	255.255.192.0		

Showing 1 to 1 of 1 entries

Previous 1 Next

Remove

Apply

Label	Description
DHCP Client	Enable the DHCP client by checking this box. If DHCP fails or the configured IP address is zero, DHCP will retry. If DHCP retry fails, DHCP will stop trying and the configured IP settings will be used.
IPv4 Address	Assigns the IP address of the network in use. If DHCP client function is enabled, you do not need to assign the IP address. The network DHCP server will assign an IP address to the switch and it will be displayed in this column. The default IP is <b>10.0.0.1</b> .
Subnet Mask	Assigns the subnet mask of the IP address. If DHCP client function is enabled, you do not need to assign the subnet mask 255.255.192.0.
Gateway IP	Assigns the network gateway for the switch. The default gateway is <b>empty</b> .
VLAN ID	Provides the managed VLAN ID. The allowed range is 1 through 4094.
DNS Server	Enter the IP address of the DNS server in dotted decimal notation.
Add	Set IP to Add
Edit/Reset	Clicking LAN IP entry , Edit 、 Reset or Remove
Reset	Click to undo any changes made locally and revert to previously saved values

## 5.2.2 Time Configuration

Time

Current Date & Time: 03/27/20 3:17 AM UTC

Time Zone:  
UTC+00:00 England

Date Format:  
mm/dd/yy

Time Format:  
12 hour

NTP/SNTP Client Setting:  
Disabled

NTP Client IP :

SNTP Client IP :

NTP Server Setting:  
Disabled

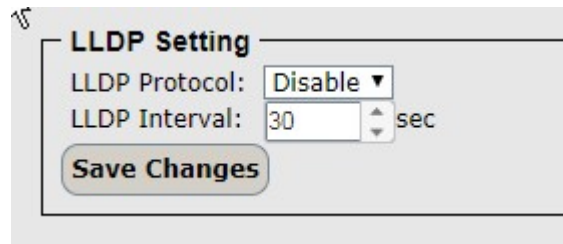
Save Changes Reset

Label	Description
Time Zone:	Select an appropriate time zone from the drop-down list according to the location of the device.
Data Format:	Specifies the year, month and day of the system clock (YYYY/MM/DD). Year: 2006-2015. Month: Jan-Dec. Day:1-31(28)
Time Format:	Specifies 12 hour / 24 hour
NTP/SNTP Client Setting:	Specifies NTP /SNTP Client enable
NTP Client IP:	Assign the NTP Client ip address
SNTP client IP	Assign the SNTP Client ip address
NTP Server Setting:	NTP server Disable/Enable (Default: Disable)

### 5.2.3 LLDP

#### LLDP Configurations

LLDP (Link Layer Discovery Protocol) provides a method for networked devices to receive and/or transmit their information to other connected devices on the network that are also using the protocols, and to store the information that is learned about other devices. This page allows you to examine and configure current LLDP settings.

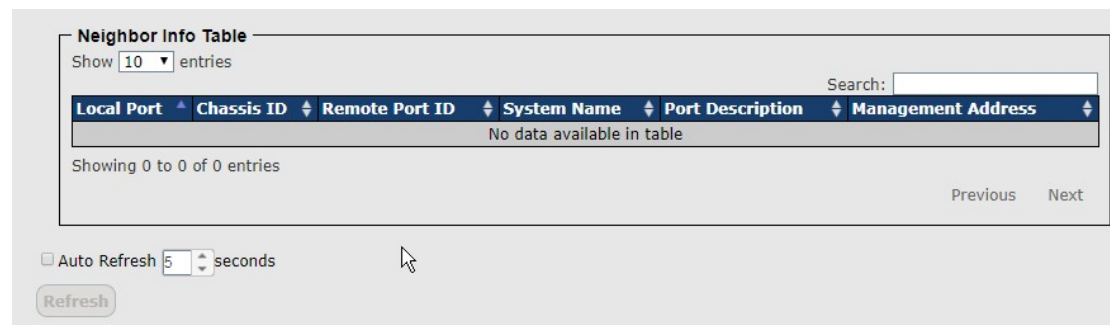


The LLDP Setting configuration interface shows two main options: 'LLDP Protocol' set to 'Disable' and 'LLDP Interval' set to '30' seconds. A 'Save Changes' button is located at the bottom of the configuration area.

Label	Description
LLDP Protocol	Enables or disables LLDP function.
LLDP Interval	The interval of resending LLDP ( 30 seconds by default)

#### LLDP Neighbor Information

This page provides a status overview for all LLDP neighbors. The following table contains information for each port on which an LLDP neighbor is detected. The columns include the following information:



The Neighbor Info Table interface displays a table with columns: Local Port, Chassis ID, Remote Port ID, System Name, Port Description, and Management Address. The table currently shows 'No data available in table'. Below the table, there is a search bar, a 'Show 10 entries' dropdown, and a 'Refresh' button. The 'Auto Refresh' checkbox is checked, set to 5 seconds.

Label	Description
Local Port	The port that you use to transmits and receives LLDP frames.
Chassis ID	The identification number of the neighbor sending out the LLDP frames.
Remote Port ID	The identification of the neighbor port
System Name	The name advertised by the neighbor.
Port Description	The description of the port advertised by the neighbor.
Management Address	The neighbor's address which can be used to help network management. This may contain the neighbor's IP address.
Refresh	Click to refresh the page immediately
Auto-refresh	Check to enable an automatic refresh of the page at regular intervals



## 5.2.4 Backup/Restore Configurations

You can save/view or load switch configurations.

### Backup Current Configuration

Get Backup Now

### Restore Old Configuration

Select Old Configuration File: 選擇檔案 未選擇任何檔案

Restore Configuration Now

Label	Description
Get Backup Now	Click to back up the configurations.
Restore Configuration Now	Click to restore the configurations.

## 5.2.5 Firmware Update

This page allows you to update the firmware of the switch, choose the firmware file form your PC.

### Upgrade Firmware

By default upgrading your firmware will completely erase your current configuration. It is strongly recommended that you back up your current configuration before performing an upgrade.

You can attempt to preserve your old settings by ticking Attempt to Preserve Settings below. Be aware that this can potentially lead to problems if the new version is significantly newer than the old version, but for small, incremental differences this will likely work. It is always best to keep a backup just in case.

Current Loader Version: L1.02

Current Kernel Version: K28.13

Current Firmware Version: V1.00

Select Firmware File: 選擇檔案 未選擇任何檔案

☐ Attempt to Preserve Settings

Upgrade Now

## 5.3 Routing Protocol

The switch provides routing functions. You can configure static and dynamic.

### 5.3.1 NAPT Settings

This page allows you to set up NAPT settings for the switch. A public port must be defined for the virtual server on your router in order to redirect traffic to an internal LAN IP address and LAN port. Any PC used as a virtual server must have a static or reserved IP address.

**NAPT Setting**

Group Name:  
LAN VID:  
WAN VID:

Add

**NAPT Interface Entry**

Show  entries

Search:

Group Name	LAN VID	WAN VID
No data available in table		

Showing 0 to 0 of 0 entries

Previous Next

Remove

*Note:*  
If you delete NAPT setting, also delete all firewall setting.(You must be input new setting again.)

Apply

Label	Description
Group Name	Specify the Group Name.
LAN VID	Specify the LAN VID.
WAN VID	Specify the WAN VID

### 5.3.2 Port Forwarding

When NAPT functions are activated, the port forwarding is translated into a single network address and its TCP/UDP ports.

**Port Forwarding**

Description:   
NAPT Group Name:   
Protocol:   
External Port (or Range):   
Local Port (or Range):   
Local IP:   

Add Edit

**Port Forwarding Entry**

Show  entries

Search:

Description	NAPT Group Name	Protocol	External Port	Local Port	Local IP
No data available in table					

Showing 0 to 0 of 0 entries

Previous Next

Remove

Apply

Label	Description
Description	Defined forwarding port for identify.
NAPT Group Name	Choose Group Name.
Protocol	Choose Protocol
External Port (or Range)	WAN port number
Local Port (or Range)	LAN port number
Local IP	LAN IP address

### 5.3.3 DMZ

DMZ (Demilitarized Zone) allows a computer to be exposed to the Internet without passing through the security settings and therefore is unsecured. This feature is useful for special purposes such as gaming. To use this function, you need to set an internal computer as the DMZ host by entering its IP address. Adding a client to the DMZ may expose your local network to a variety of security risks, so use this function carefully.

**DMZ**  
Description:   
NAPT Group Name:   
DMZ IP:   
Add Edit

**DMZ Entry**  
Show  entries  
Search:   

Description	NAPT Group Name	DMZ IP
No data available in table		
<input type="text" value="Filter Description"/>	<input type="text" value="Filter NAPT Group Name"/>	<input type="text" value="Filter DMZ IP"/>

Showing 0 to 0 of 0 entries  
Previous Next  
Remove

Apply

Label	Description
Description	Defined the for identify.
NAPT Group Name	Choose Group Name.
DMZ IP	Specify IP address

### 5.3.4 Static NAT (1:1 NAT)

Static Network Address Translation (NAT) allows the user to configure one-to-one translations of the inside local addresses to the outside global addresses. It allows both IP addresses and port number translations from the inside to the outside traffic and the outside to the inside traffic.

**Static NAT Setting**

Group Name:
LAN VID:
Local IP/Subnet(Range):
WAN VID:
External IP/Subnet(Range):

Add

**Static NAT Interface Entry**

Show 

10

 entries

Search:

Group Name	LAN VID	Local IP/Subnet	WAN VID	External IP/Subnet
No data available in table				

Showing 0 to 0 of 0 entries

PreviousNext

Remove

Apply

Label	Description
Group Name	Defined for the Group Name
LAN VID	Defined for the LAN VID
Local IP/Subnet (Range)	The IP address (LAN) of the computer that will provide virtual server / The subnet mask of the LAN
WAN VID	Defined for the WAN VID
External IP /Subnet (Range)	The IP address (WAN) of the computer that will provide virtual server / The subnet mask of the WAN

### 5.3.5 Static Routing

The router will operate in static routing mode, which means routers forward packets using either route information from route table entries that you manually configure or the route information that is calculated using dynamic routing algorithms.

### Static Routing Setting

Destination/Subnet(Range):  
Gateway:  
Metric:  
Interface:  
Vlan ID:

LAN

Add Edit

### Static Route Entry

Show 10 entries

Search:

Destination	Gateway	Metric	Interface
No data available in table			
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Showing 0 to 0 of 0 entries

First Previous Next Last

Remove Remove All

Label	Description
Destination/Subnet (Range)	Destination IP address/Subnet.
Gateway	Gateway IP address.
Metric	The range is 0-255
Interface	Choose WAN/LAN
VLAN ID	Defined for the LAN VID

### 5.3.6 Routing Security Group

The relay statistics shows the information of relayed packets of the switch.

### Default Forward

Default Forward:

Enable

Apply

### Allow Setting

Group Name:

Interface: ---choose--- Add

Choose data:

Add Group Edit Group

**Note:**

Tag vlan 1 can't join vlan routing when used vlan trunk port.

### Allow Setting Entry

Show 10 entries

Search:

Group Name	Network
No data available in table	
<input type="text" value="Filter Group Name"/>	<input type="text" value="Filter Network"/>

Showing 0 to 0 of 0 entries

Remove

Previous Next

Apply

Label	Description
Default Forward	Routing Disable /Enable
Group Name	Defined for the Group Name
Interface	Choose Interface add

### 5.3.7 Routing Table

Show all routing information, will be displayed in Current Routing Table.

### Routing Table

Show 10 entries

Search:

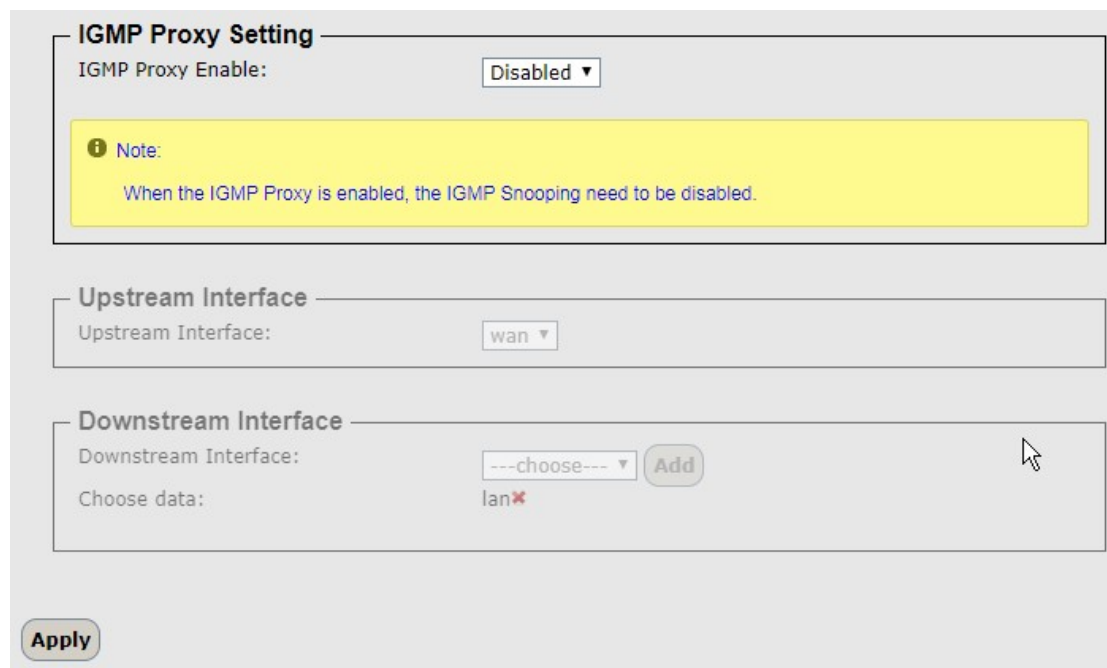
Destination	Gateway	Subnet Mask	Metric	Interface
10.0.0.0	0.0.0.0	255.255.192.0	0	lan
10.128.0.0	0.0.0.0	255.255.192.0	0	wan
<input type="text" value="Filter Destination"/>	<input type="text" value="Filter Gateway"/>	<input type="text" value="Filter Subnet Mask"/>	<input type="text" value="Filter Metric"/>	<input type="text" value="Filter Interface"/>

Showing 1 to 2 of 2 entries

First Previous 1 Next Last

### 5.3.8 IGMP Proxy

IGMP Proxy is used to learn proxy group information and forwards multicast traffic based on this information.



**IGMP Proxy Setting**

IGMP Proxy Enable: Disabled ▼

**Note:**  
When the IGMP Proxy is enabled, the IGMP Snooping need to be disabled.

**Upstream Interface**

Upstream Interface: wan ▼

**Downstream Interface**

Downstream Interface: ---choose--- ▼ Add

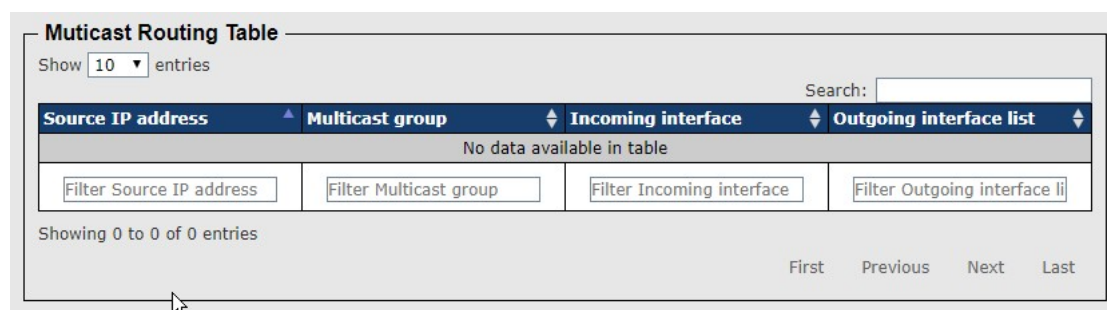
Choose data: lan ✖

Apply

Label	Description
IGMP Proxy Enable	Enable /Disable the function
Upstream Interface	Specify Interface WAN or LAN
Downstream Interface	Specify Interface WAN or LAN

### 5.3.9 Multicast Routing Table

Show all multicast routing information, including source ip address 、 multicast group 、 incoming interface 、 outgoing interface list.



**Muticast Routing Table**

Show 10 ▼ entries

Search:

Source IP address ▲	Multicast group ◆	Incoming interface ◆	Outgoing interface list ◆
No data available in table			
<input type="text" value="Filter Source IP address"/>	<input type="text" value="Filter Multicast group"/>	<input type="text" value="Filter Incoming interface"/>	<input type="text" value="Filter Outgoing interface li"/>

Showing 0 to 0 of 0 entries

First Previous Next Last



### 5.3.10 VRRP Setting

A VRRP (Virtual Router Redundancy Protocol) is a computer networking protocol aimed to eliminate the single point of failure by automatically assigning available IP routers to participating hosts. Using a virtual router ID (VRID) address and virtual router IP (VRIP) address to represent itself, a virtual router consists of two or more physical routers, including one master router and one or more backup routers. All routers in the virtual router group share the same VRID and VRIP. The master router provides primary routing and the backup routers monitor the status of the master router and become active if the master router fails.

**VRRP Global Setting**
  
VRRP Enable: Enabled ▼

**Virtual IP Address Group**
  
Virtual IP Address Group Name: 
  
Virtual IP Interface: ---choose--- ▼
  
Virtual IP/Mask: 
  
Add Edit

**VIP Group Entry**
  
Show 10 ▼ entries
  
Search: 
  

Virtual IP Group Name ▲	Virtual IP Interface ▲	Virtual IP/Mask ▲
No data available in table		

  
Showing 0 to 0 of 0 entries
  
Remove
Previous Next

### VRRP

Instance Name:

Virtual IP Group:

Choose data:

VRRP Interface:

Priority:  (1~254)

Virtual Router ID:  (1~255)

Preemption:

Preempt Delay(sec):  (10~300)

Advertisement Interval(sec):  (1~30)

### VRRP Entry

Show  entries

Search:

IName	VIP Group	Interface	Priority	VRID	Preemption	PDelay	ADV Interval
No data available in table							

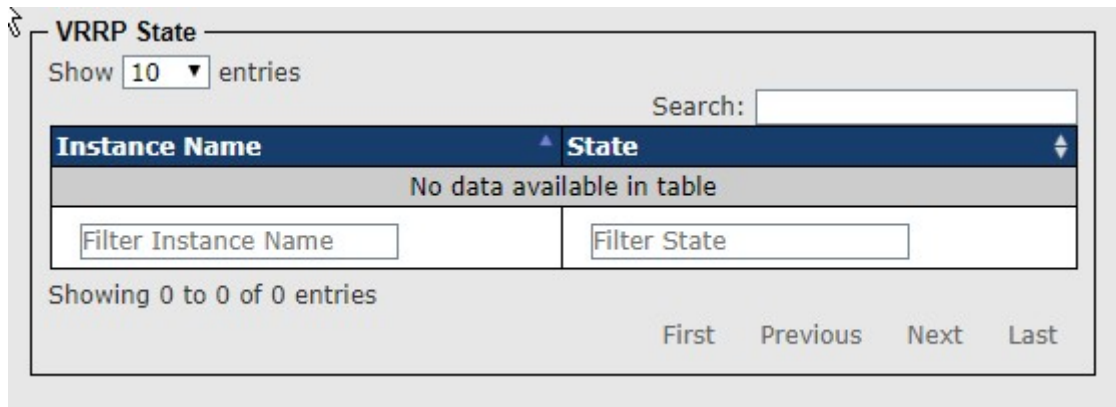
Showing 0 to 0 of 0 entries

Label	Description
VRRP Enable	Enable or Disable VRRP function
Virtual IP Address Group Name	Specify Virtual IP Group Name
Virtual IP Interface	Specify WAN or LAN
Virtual IP/Mask	An IP address associated with the VRID from which other hosts can obtain network service. The VRIP is managed by the VRRP instances belonging to a VRID
Instance Name	Create a VRRP instance
Virtual IP Group	Choose Virtual IP Group
VRRP Interface	Choose WAN or LAN
Priority	The priority value used by the VRRP router when selecting the master virtual router. (Range 1-254)
Virtual Router ID	A VRID consists of one master router and one or more backup routers. The master router is the router that owns the IP

	address you associate with the VRID. Configure the VRID on the router that owns the default gateway interface. The other router in the VRID does not own the IP address associated with VRID but provides the backup path if the Master router becomes unavailable (Range1~255).
Preemption	VRRP can be configured to preempt the existing router. This means that if a new VRRP router is added to the network with priority higher than the existing routers, then the new router will become the master. If preemption is disabled, then the new router will not become a master. This router will become master only when the current master is down, that is, only when it does not receive any advertisement packets from the current master. By default, preempt mode is Disable.
Preempt Delay(sec)	Specify delay time (Range 10.-300)
Advertisement Interval(sec)	Specify interval Time (Range 1-30)

### 5.3.11 VRRP State

Show VRRP Master / Backup Status.



**VRRP State**

Show  entries

Search:

Instance Name	State
No data available in table	

Filter Instance Name  Filter State

Showing 0 to 0 of 0 entries

First Previous Next Last

## 5.4 ETBN Protocol

Designed specifically for the backbone network to support NAT and routing functions.

### 5.4.1 TTDP Setting

Auto assign ip for device. (TTDP setting > Save changes > Rebuild>Inaugurate)

### TTDP Setting

TTDP Enabled: Enabled

Reverse: False

Interface1: G9

Interface2: G10

cstUUID: 2E03CC96-7DF2-11EA-A395-6D2CBE8696BE

Save changes
Inaugurate
Rebuild
UUID generator

### TTDP INFO

IP Address: 10.128.0.1

MAC: 00:1E:94:FF:FF:F1

Stable: False

### TTDP Entry

Show 25 entries

Search:

Number	MAC	CSTUUID
1	001E94FFFFF1	2E03CC96-7DF2-11EA-A395-6D2CBE8696BB

Showing 1 to 1 of 1 entries

Previous 1 Next

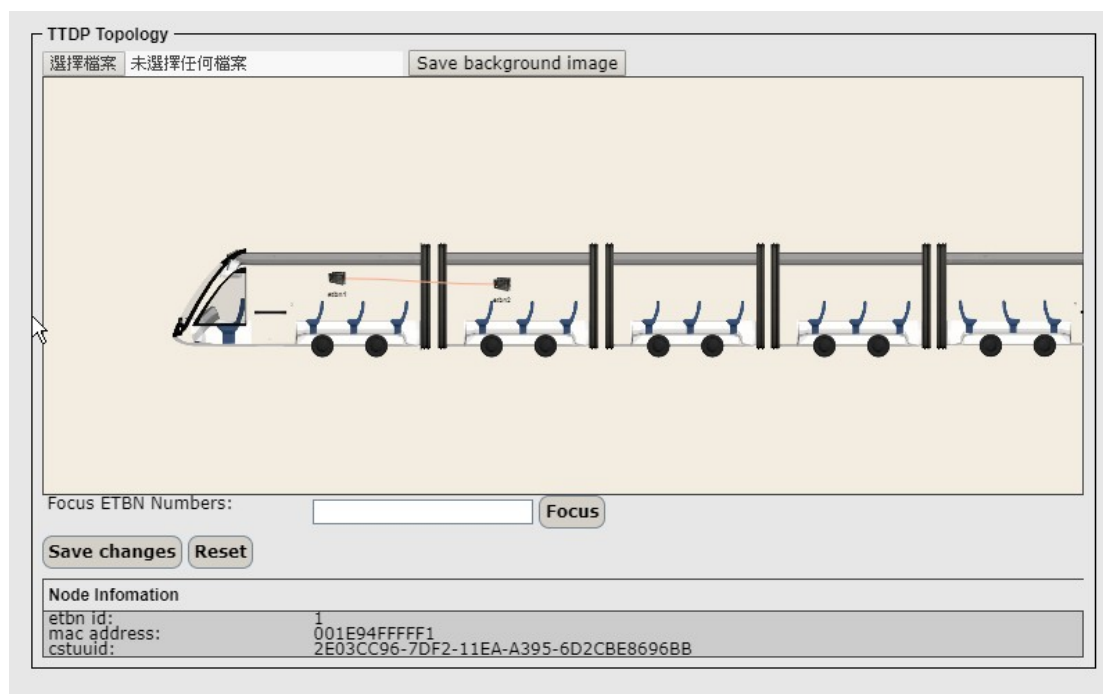
☒ Auto Refresh 5 seconds

Refresh

Label	Description
TTDP Enable	TTDP function Enable or Disable.
Reverse	IP performs forward or reverse function selection
Interface1	Select the port to connect (G9~G12).
Interface2	Select the port to connect (G9~G12).
Save changes	Click to save changes.
Inaugurate	When the Stable status in TTDP INFO is True, it means that TTDP topology learning is completed. At this time, press this button and TTDP will allocate the IP of this machine according to the ETBN ID against the entry in the Dynamic Setting set earlier.
Rebuild	When the train sequence changes, you need to press this button to learn the topology again.
UUID generator	Generate a new UUID.

## 5.4.2 TTDP Topology

View TTDP Topology.



Label	Description
File selection	Choose your own train map
Save background image	Background image save
Focus	Move to a specific ETBN
Save changes	Click to save changes

## 5.4.3 Dynamic Setting

Multiple virtual IP addresses correspond to multiple real IP addresses, but at the same time, a real IP address corresponds to only one virtual IP address.

The maximum number of simultaneous connections is equal to the number of real addresses in the storage area.

Dynamic NAT uses a connection track to communicate with the Internet.

## 5.4.4 R-NAT

R-NAT uses NAT technology for railways. The IP setting needs to be set according to R-NAT rules, which also simplifies the management difficulties. R-NAT must send packets on different network segments from its own Additional routing table.

R-NAT Mode:

Mode:

Disabled ▾

Automatic Setting:

Auto Mode:

Disabled ▾

ETBN Numbers:

16

Backbone(VLAN) Numbers:

1 ▾

R-NAT Setting

ETBN ID:
LAN VID:
Local IP/Subnet:
WAN VID:
External IP/Subnet:

Add

R-NAT Interface Entry

Show

10 ▾

entries

Search:

Number ID	Local IP/Subnet	LAN VID	External IP/Subnet	WAN VID
No data available in table				

Showing 0 to 0 of 0 entries

Previous Next

Remove

Remove All

Apply

Label	Description
R-NAT Mode	Disable or Enable
Auto Mode	Disable or Enable
ETBN Numbers	Automatically generate RNAT entry
Backbone (VLAN)Numbers	Automatically generate RNAT entry
R-NAT Setting	R-NAT Automatic info
R-NAT interface Entry	Number ID corresponds to which car

## 5.4.5 LAN IP

This page allows you to configure the Dynamic LAN IP.

**Dynamic LAN IP Mode:**  
Mode: Disabled ▼

**Automatic Setting:**  
Auto Mode: Disabled ▼  
ETBN Numbers: 16  
Backbone(VLAN) Numbers: 1 ▼

**Dynamic LAN IP Setting**  
ETBN ID:   
LAN IP/Subnet:   
LAN VID:   
Add

**Dynamic LAN IP Entry**  
Show 10 ▼ entries  
Search:   

Number ID ▲	LAN IP/Subnet ◆	LAN VID ◆
No data available in table		

Showing 0 to 0 of 0 entries  
Previous Next  
Remove Remove All

Apply

Label	Description
Mode	Disable or Enable
Auto Mode	Disable or Enable
ETBN Numbers	自動產生 RNAT entry
Backbone (VLAN)Numbers	自動產生 RNAT entry
LAN IP/ Subnet	LAN IP address/Subnet mask
LAN VID	LAN VLAN identifier

## 5.4.6 WAN IP

This page allows you to configure the Dynamic WAN IP.

**Dynamic WAN IP Mode:**  
Mode: Disabled ▾

**Automatic Setting:**  
Auto Mode: Disabled ▾  
ETBN Numbers: 16  
Backbone(VLAN) Numbers: 1 ▾

**Dynamic WAN IP Setting**  
ETBN ID:   
WAN IP/Subnet:   
WAN VID:   
Add

**Dynamic WAN IP Entry**  
Show 10 ▾ entries  
Search:   

Number ID	WAN IP/Subnet	WAN VID
No data available in table		

Showing 0 to 0 of 0 entries  
Remove Remove All  
Previous Next  
Apply

Label	Description
Mode	Disable or Enable
Auto Mode	Disable or Enable
ETBN Numbers	Automatically generate RNAT entry
Backbone (VLAN)Numbers	Automatically generate RNAT entry
WAN IP/ Subnet	WAN IP address/Subnet mask
WAN VID	WAN VLAN identifier



## 5.5 Backbone Switch

### 5.5.1 Port Setting

Port Setting allows you to manage individual ports of the switch, including speed/duplex, flow control, and security.

#### 5.5.1.1 Port Control

This page shows current port configurations. Ports can also be configured here.

**Port Control**

Port No.	State	Speed/Duplex	Flow Control	Security
G9	Enable ▼	AutoNegotiation ▼	Disable ▼	Disable ▼
G10	Enable ▼	AutoNegotiation ▼	Disable ▼	Disable ▼
G11	Enable ▼	AutoNegotiation ▼	Disable ▼	Disable ▼
G12	Enable ▼	AutoNegotiation ▼	Disable ▼	Disable ▼

Save Changes

Label	Description
Port NO.	The number of the port to be configured.
State	Enables or disables the port.
Speed/Duplex	Available values include <b>auto-negotiation</b> , <b>1000-full</b> , <b>1000-half</b> , <b>100-full</b> , <b>100-half</b> , <b>10-full</b> , or <b>10-half</b>
Flow Control	Supports symmetric mode to avoid packet loss when congestion occurs
Security	Enabling port security will disable MAC address learning in this port. Thus, only the frames with MAC addresses in the port security list will be forwarded, otherwise will be discarded.
Save Changes	Click to save changes

#### 5.5.1.2 Port Status

This page shows the status of each port in terms of its state, speed/duplex, flow control, security and learning limit.

**Port Status**

Port No.	Type	Link	State	Speed/Duplex	Flow Control	Security	Learning Limit
G9	1000TX	Down	Forwarding	N/A	Disable	Disable	Disable
G10	1000TX	Down	Forwarding	N/A	Disable	Disable	Disable
G11	1000TX	Down	Forwarding	N/A	Disable	Disable	Disable
G12	1000TX	Down	Forwarding	N/A	Disable	Disable	Disable

Refresh

Label	Description
Refresh	Click to refresh the page.

### 5.5.1.3 Port Trunk

A port trunk is a group of ports that have been grouped together to function as one logical path. This method provides an economical way for you to increase the bandwidth between the switch and another networking device. In addition, it is useful when a single physical link between the devices is insufficient to handle the traffic load. This page allows you to configure the aggregation hash mode and the aggregation group.

**Port Trunk - Setting**

Port No.	Group ID	Type
G9	none ▼	Static ▼
G10	none ▼	Static ▼
G11	none ▼	Static ▼
G12	none ▼	Static ▼

**802.3ad LACP Work Ports**

Group ID	Work Ports
Trunk.1	max ▼
Trunk.2	max ▼

Save Changes

Label	Description
Group ID	Indicates the ID of each aggregation group. <b>None</b> means no aggregation. Only one group ID is valid per port.
Type	The switch supports two types of link aggregation; static and 802.3ad LACP. Static trunks are manually configured, while, LACP-configured ports will automatically negotiate a trunk with LACP-configured ports on another device.
Work Port	The total number of active ports in a dynamic trunk group. The default value of works ports is <b>Max</b> . In a dynamic trunk group, if the number of work ports is lower than the number of members of the trunk group, the exceed ports are standby/redundant ports and can be aggregated if working ports fail. If it is a static trunk group, the number of work ports must equal the total number of group member ports.
Save Changes	Click to save changes

### 5.5.1.3.1 Port Trunk - Setting

Label	Description
Group ID	Indicates the ID of each aggregation group. <b>None</b> means no aggregation. Only one group ID is valid per port.
Trunk Member	Lists members of a specific trunk group.
Type	Indicates the type of the port trunk

## 5.5.2 Vlan

### IEEE 802.1Q

A VLAN (Virtual LAN) is a logical LAN based on a physical LAN with links that does not consist of a physical (wired or wireless) connection between two computing devices but is implemented using methods of network virtualization. A VLAN can be created by partitioning a physical LAN into multiple logical LANs using a VLAN ID. You can assign switch ports to a VLAN and add new VLANs in this page.

### 5.5.2.1 Vlan Setting

**VLAN Mode Setting**

Operation Mode: 802.1Q ▼

**Port Setting**

Port No.	Link Type	PVID	Untagged VID	Tagged VIDs
G9	Access ▼	1	1	
G10	Access ▼	1	1	
G11	Access ▼	1	1	
G12	Access ▼	1	1	

Label	Description
VLAN Operation Mode	Available options include <b>Disable</b> and <b>802.1Q</b>
Link type	<p>Three link types are available:</p> <p><b>Access Link:</b> An access link connects a VLAN-unaware device to the port of a VLAN-aware bridge. All frames on access links must be implicitly tagged (untagged).</p> <p><b>Trunk Link:</b> All the devices connected to a trunk link, including workstations, must be VLAN-aware. All frames on a trunk link must have a special header attached.</p> <p><b>Hybrid Link:</b> The combination of Access Link and Trunk Link. This is a link where both VLAN-aware and VLAN-unaware devices are attached. It can have both tagged and untagged frames, but all the frames for a</p>

	specific VLAN must be either tagged or untagged. <b>Hybrid (QinQ) Link:</b> Allows one more VLAN tag in an original VLAN frame.
Untagged VID	Set the port default VLAN ID for untagged devices that connect to the port. The range is 1 to 4094.
Tagged VIDs	Set the tagged VIDs to carry different VLAN frames to another switch.
Save Changes	Click to save changes

## 5.6 Consist Switch

### 5.6.1 Redundancy

Redundancy for minimized system downtime is one of the most important concerns for industrial networking devices. Hence, ORing has developed proprietary redundancy technologies including O-Ring and O-Chain featuring faster recovery time than existing redundancy technologies widely used in commercial applications, such as STP, RSTP, and MSTP. ORing's proprietary redundancy technologies not only support different networking topologies, but also assure the reliability of the network

#### 5.6.1.1 RSTP

**RSTP Setting**

RSTP Mode: Disable ▾

Label	Description
RSTP mode	Enables or disables RSTP mode.

##### 5.6.1.1.1 Bridge Setting

**Bridge Setting**

<b>Priority (0-61440):</b>	<input type="text" value="32768"/>
<b>Max Age Time (6-40):</b>	<input type="text" value="20"/>
<b>Hello Time (1-10):</b>	<input type="text" value="2"/>
<b>Forward Delay Time (4-30):</b>	<input type="text" value="15"/>

Label	Description
Priority (0-61440)	A value used to identify the root bridge. The bridge with the lowest priority is selected as the root. If more than one bridges have the same priority, the one with the lowest MAC address will be selected. If the value changes, you must reboot the switch. The value must be a multiple of 4096 according to the protocol standard rule
Max Age Time (6-40)	The number of seconds a bridge waits without receiving STP

	configuration messages before attempting a reconfiguration. The valid value is between 6 and 40.
<b>Hello Time (1-10)</b>	The time interval a switch sends out the BPDU packet to check RSTP current status. The time is measured in seconds and the valid value is between 1 and 10.
<b>Forwarding Delay Time (4-30)</b>	The time of a port waits before changing from RSTP learning and listening states to forwarding state. The valid value is between 4 and 30.

**NOTE:** the calculation of the MAX Age, Hello Time, and Forward Delay Time is as follows:

$$2 \times (\text{Forward Delay Time value} - 1) \geq \text{Max Age value} \geq 2 \times (\text{Hello Time value} + 1)$$

**Port Setting**

Port	Enable	Priority (0-240)	Path Cost (0:Auto,1-200000000)	P2P	Edge
G1	Enable ▼	128 ▲▼	0:Auto	Auto ▼	True ▼
G2	Enable ▼	128 ▲▼	0:Auto	Auto ▼	True ▼
G3	Enable ▼	128 ▲▼	0:Auto	Auto ▼	True ▼
G4	Enable ▼	128 ▲▼	0:Auto	Auto ▼	True ▼
G5	Enable ▼	128 ▲▼	0:Auto	Auto ▼	True ▼
G6	Enable ▼	128 ▲▼	0:Auto	Auto ▼	True ▼
G7	Enable ▼	128 ▲▼	0:Auto	Auto ▼	True ▼
G8	Enable ▼	128 ▲▼	0:Auto	Auto ▼	True ▼

Save Changes

Label	Description
<b>Port No.</b>	The number of ports you want to configure.
<b>Enable</b>	Enable/Disable RSTP function of the port.
<b>Path Cost (1-200000000)</b>	The path cost incurred by the port. The path cost is used when establishing an active topology for the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. The range of valid values is 1 to 200000000.
<b>Priority (0-240)</b>	Decide which port should be blocked by priority in the LAN. The valid value is between 0 and 240, and must be a multiple of 16.
<b>Admin P2P</b>	Configures whether the port connects to a point-to-point LAN rather than a shared medium. This can be configured automatically or set to true or false manually. True means P2P enabling. False means P2P disabling. Transiting to forwarding state is faster for point-to-point LANs than for shared media.

Admin Edge	Specify whether this port is an edge port or a non-edge port. An edge port is not connected to any other bridge. Only edge ports and point-to-point links can rapidly transition to forwarding state. To configure the port as an edge port, set the port to True.
Admin Non STP	The port includes the STP mathematic calculation. True is not including STP mathematic calculation, false is including the STP mathematic calculation.
Save Changes	Click to save changes.

The following pages show the information of the root bridge, including its port status.

Root Bridge Information	
Bridge ID	00:1E:94:FF:FF:F0
Root Priority	32768
Root Port	N/A
Root Path Cost	0
Max Age Time	20
Hello Time	2
Forward Delay Time	15

Port Information							
Port	Enable	Priority	Path Cost	OperP2P	OperEdge	Role	State
G1	Enable	128	200000000	no	yes	Disabled	discarding
G2	Enable	128	20000	yes	yes	Designated	forwarding
G3	Enable	128	200000000	no	yes	Disabled	discarding
G4	Enable	128	200000000	no	yes	Disabled	discarding
G5	Enable	128	20000	yes	yes	Designated	forwarding
G6	Enable	128	200000000	no	yes	Disabled	discarding
G7	Enable	128	200000000	no	yes	Disabled	discarding
G8	Enable	128	200000000	no	yes	Disabled	discarding

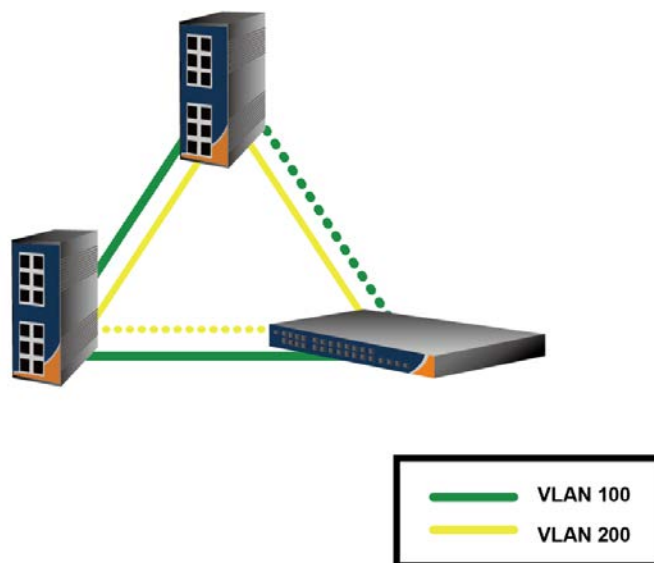
Refresh

Label	Description
Enable	Enable/Disable RSTP function of the port.
Port Priority (0-240)	Decide which port should be blocked by priority in the LAN. The valid value is between 0 and 240, and must be a multiple of 16
Path Cost (1-200000000)	The path cost incurred by the port. The path cost is used when establishing an active topology for the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. The range of valid values is 1 to 200000000.
Oper P2P	Configures the port connects to a point-to-point LAN rather than a

	shared medium. This can be configured automatically or set to true or false manually. True means P2P enabling. False means P2P disabling. Transiting to forwarding state is faster for point-to-point LANs than for shared media.
<b>Oper Edge</b>	A flag indicating whether the port is connected directly to edge devices or not (no bridges attached). Transiting to the forwarding state is faster for edge ports (oper Edge set to true) than other ports.
<b>Role</b>	When enabled, the port will not be selected as root port for CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an alternate port after the root port has been selected. If set, spanning trees will lose connectivity. It can be set by a network administrator to prevent bridges outside a core region of the network from influencing the active spanning tree topology because those bridges are not under the full control of the administrator. This feature is also known as Root Guard.
<b>State</b>	Determines the STP state of the port
<b>Refresh</b>	Click to refresh the page.

### 5.6.1.2 MSTP

Since the recovery time of STP and RSTP takes seconds, which is unacceptable in industrial applications, MSTP was developed. The technology supports multiple spanning trees within a network by grouping and mapping multiple VLANs into different spanning-tree instances, known as MSTIs, to form individual MST regions. Each switch is assigned to an MST region. Hence, each MST region consists of one or more MSTP switches with the same VLANs, at least one MST instance, and the same MST region name. Therefore, switches can use different paths in the network to effectively balance loads.



### 5.6.1.2.1 Bridge Setting

**MSTP Setting**

MSTP Enable: Disable ▾  
Force Version: STP ▾  
Configuration Name: TGRS-T120-M12X  
Revision Level (0-65535): 100  
Priority (0-61440): 4096  
Max Age Time (6-40): 10  
Hello Time (1-10): 4  
Forward Delay Time (4-30): 15  
Max Hops (1-40): 20

Save Changes

Label	Description
MSTP Enable	Enables or disables MSTP function.
Force Version	Forces a VLAN bridge that supports RSTP to operate in an STP-compatible manner.
Configuration Name	The name which identifies the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configurations in order to share spanning trees for MSTIs (intra-region). The name should not exceed 32 characters.
Revision Level (0-65535)	Revision of the MSTI configuration named above. This must be an integer between 0 and 65535.
Priority (0-61440)	A value used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root. If the value changes, you must reboot the switch. The value must be a multiple of 4096 according to the protocol standard rule.
Max Age Time (6-40)	The number of seconds a bridge waits without receiving Spanning-tree Protocol configuration messages before attempting a reconfiguration. The valid value is between 6 through 40.
Hello Time (1-10)	The time interval a switch sends out the BPDU packet to check RSTP current status. The time is measured in seconds and the valid value is between 1 through 10.
Forwarding Delay Time (4-30)	The time of a port waits before changing from RSTP learning and listening states to forwarding state. The valid value is between 4 through 30.
Max Hops (1-40)	An additional parameter for those specified for RSTP. A single value applies to all STP within an MST region (the CIST and all MSTIs) for which the bridge is the regional root.



Save Changes

Click to save changes.

### 5.6.1.2.2 Bridge Port

MSTP Ports

Port	Priority (0-240)	Path Cost (0:Auto,1-200000000)		P2P		Edge		Admin Non Stp
		Admin	Oper	Admin	Oper	Admin	Oper	
G1	128	0:Auto	200000000	False	False	False	True	False
G2	128	0:Auto	20000	True	True	False	True	False
G3	128	0:Auto	200000000	True	False	False	True	False
G4	128	0:Auto	200000000	True	False	False	True	False
G5	128	0:Auto	20000	True	True	False	True	False
G6	128	0:Auto	200000000	True	False	False	True	False
G7	128	0:Auto	200000000	True	False	False	True	False
G8	128	0:Auto	200000000	True	False	False	True	False

Save Changes

Label	Description
Port No.	The number of ports you want to configure
Priority (0-240)	Decide which port should be blocked by priority in the LAN. The valid value is between 0 and 240, and must be a multiple of 16.
Path Cost (1-200000000)	The path cost incurred by the port. The path cost is used when establishing an active topology for the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. The range of valid values is 1 to 200000000.
P2P	Configures whether the port connects to a point-to-point LAN rather than a shared medium. This can be configured automatically or set to true or false manually. True means P2P enabling. False means P2P disabling. Transiting to forwarding state is faster for point-to-point LANs than for shared media.
Edge	Specify whether this port is an edge port or a non-edge port. An edge port is not connected to any other bridge. Only edge ports and point-to-point links can rapidly transition to forwarding state. To configure the port as an edge port, set the port to True.
Admin Non STP	The port includes the STP mathematic calculation. True is not including STP mathematic calculation, false is including the STP mathematic calculation.

Save Changes

Click to save changes.

### 5.6.1.2.3 Instance Setting

MSTI Mapping

Instance	State	VLANs	Priority (0-61440)	Regional Root Bridge ID	Path Cost	Root Port
1	Disable ▼	1-4094	32768 ▲▼	0	0	0
2	Disable ▼	1-4094	32768 ▲▼	0	0	0
3	Disable ▼	1-4094	32768 ▲▼	0	0	0
4	Disable ▼	1-4094	32768 ▲▼	0	0	0
5	Disable ▼	1-4094	32768 ▲▼	0	0	0
6	Disable ▼	1-4094	32768 ▲▼	0	0	0
7	Disable ▼	1-4094	32768 ▲▼	0	0	0
8	Disable ▼	1-4094	32768 ▲▼	0	0	0
9	Disable ▼	1-4094	32768 ▲▼	0	0	0
10	Disable ▼	1-4094	32768 ▲▼	0	0	0
11	Disable ▼	1-4094	32768 ▲▼	0	0	0
12	Disable ▼	1-4094	32768 ▲▼	0	0	0
13	Disable ▼	1-4094	32768 ▲▼	0	0	0
14	Disable ▼	1-4094	32768 ▲▼	0	0	0
15	Disable ▼	1-4094	32768 ▲▼	0	0	0

Save Changes

Label	Description
Instance	Set the instance from 1 to 15
State	Enables or disables the instance
VLANs	The VLAN which is mapped to the MSTI. A VLAN can only be mapped to one MSTI. An unused MSTI will be left empty (ex. without any mapped VLANs).
Priority (0-61440)	A value used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root. If the value changes, you must reboot the switch. The value must be a multiple of 4096 according to the protocol standard
Regional Root Bridge ID	The Bridge ID of this Bridge instance.
Path Cost	Path Cost. For the Root Bridge it is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.
Root Port	The switch port currently assigned the <i>root</i> port role.
Save Changes	Click to save changes.

### 5.6.1.2.4 Instance port

#### Port Priority

This page allows you to change the configurations of current MSTI bridge instance priority.

**MSTI Priorities**

Instance: CIST ▼

Port No.	Priority (0-240)	Path Cost (0:Auto,1-200000000)		State	Role
		Admin	Oper		
G1	<span>128 ▼</span>	<span>0:Auto</span>	200000000	discarding	Disabled
G2	<span>128 ▼</span>	<span>0:Auto</span>	20000	forwarding	Designated
G3	<span>128 ▼</span>	<span>0:Auto</span>	200000000	discarding	Disabled
G4	<span>128 ▼</span>	<span>0:Auto</span>	200000000	discarding	Disabled
G5	<span>128 ▼</span>	<span>0:Auto</span>	20000	forwarding	Designated
G6	<span>128 ▼</span>	<span>0:Auto</span>	200000000	discarding	Disabled
G7	<span>128 ▼</span>	<span>0:Auto</span>	200000000	discarding	Disabled
G8	<span>128 ▼</span>	<span>0:Auto</span>	200000000	discarding	Disabled

Save Changes

Label	Description
Instance	The bridge instances. CIST is the default instance, which is always active.
Port	The port number which you want to configure.
Priority (0-240)	Decides the priority of ports to be blocked in the LAN. The valid value is between 0 and 240, and must be a multiple of 16
Path Cost (1-200000000)	The path cost incurred by the port. The path cost is used when establishing an active topology for the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. The range of valid values is 1 to 200000000.
State	Determines the STP state of the port
Role	When enabled, the port will not be selected as root port for CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an alternate port after the root port has been selected. If set, spanning trees will lose connectivity. It can be set by a network administrator to prevent bridges outside a core region of the network from influencing the active spanning tree topology because those bridges are not under the full control of the administrator. This feature is also known as Root Guard.

Save Changes

Click to save changes.

### 5.6.1.3 Multicast

#### 5.6.1.3.1 IGMP Snooping

IGMP (Internet Group Management Protocol) snooping monitors the IGMP traffic between hosts and multicast routers. The switch uses what IGMP snooping learns to forward multicast traffic only to interfaces that are connected to interested receivers. This conserves bandwidth by allowing the switch to send multicast traffic to only those interfaces that are connected to hosts that want to receive the traffic, instead of flooding the traffic to all interfaces in the VLAN. This page allows you to set up IGMP snooping configurations.

#### IGMP Snooping

IGMP Snooping	Disable ▼
IGMP Query Mode	Disable ▼
IGMP Unregister Stream	Blocking ▼

Save Changes

**Note:**

When the IGMP Snooping is enabled ,the IGMP Proxy need to be disabled.

#### IGMP Snooping Table

IP Address	VLAN ID	Member Port
------------	---------	-------------

Label	Description
IGMP Snooping	Check to enable global IGMP snooping
IGMP Query Mode	Configures the switch to be the IGMP querier. Only one IGMP querier is allowed in an IGMP application. <b>Auto</b> will select the switch with the lowest IP address as the querier.
IGMP Unregister Stream	Unregistered IPMCv4 traffic flooding/Blocking.
Save Changes	Click to save changes.
IGMP Snooping Table	Shows a list of current IP multicast

### 5.6.1.3.2 Static Multicast Filtering

Static multicast filtering provides a method for users to configure multicast group memberships manually. The function enables end devices to receive multicast traffic only if they register to join specific multicast groups. With static multicast filtering, network devices only forward multicast traffic to the ports connected to registered end devices. The function allows you to control the multicast traffic precisely.

**Filtering Setting**

IP Address

Ports

G1 ▾

Add

Delete

**Multicast Filtering List**

IP Address	Member Ports
Label	Description
IP Address	Assigns a multicast group IP address in the range of 224.0.0.0 ~ 239.255.255.255
Ports	Check the box next to the port number to include them as member ports in the specific multicast group.
Add	Click to add the ports to the IP multicast list.
Delete	Deletes an entry from the table.

### 5.6.1.4 Port Setting

Port Setting allows you to manage individual ports of the switch, including speed/duplex, flow control, and security.

### 5.6.1.4.1 Port Control

**Port Control**

Port No.	State	Speed/Duplex	Flow Control	Security
G1	Enable ▾	AutoNegotiation ▾	Disable ▾	Disable ▾
G2	Enable ▾	AutoNegotiation ▾	Disable ▾	Disable ▾
G3	Enable ▾	AutoNegotiation ▾	Disable ▾	Disable ▾
G4	Enable ▾	AutoNegotiation ▾	Disable ▾	Disable ▾
G5	Enable ▾	AutoNegotiation ▾	Disable ▾	Disable ▾
G6	Enable ▾	AutoNegotiation ▾	Disable ▾	Disable ▾
G7	Enable ▾	AutoNegotiation ▾	Disable ▾	Disable ▾
G8	Enable ▾	AutoNegotiation ▾	Disable ▾	Disable ▾

Save Changes

Label	Description
Port NO.	The number of the port to be configured.
State	Enables or disables the port.
Speed/Duplex	Available values include <b>auto-negotiation</b> , <b>1000-full</b> , <b>1000-half</b> , <b>100-full</b> , <b>100-half</b> , <b>10-full</b> , or <b>10-half</b> .
Flow Control	Supports symmetric mode to avoid packet loss when congestion occurs.
Security	Enabling port security will disable MAC address learning in this port. Thus, only the frames with MAC addresses in the port security list will be forwarded, otherwise will be discarded.
Save Changes	Click to save changes.

### 5.6.1.4.2 Port Status

This page shows the status of each port in terms of its state, speed/duplex and flow control

**Port Status**

Port No.	Type	Link	State	Speed/Duplex	Flow Control
G1	1000TX	Down	Enable	N/A	Disable
G2	1000TX	Up	Enable	1000 Full	Disable
G3	1000TX	Down	Enable	N/A	Disable
G4	1000TX	Down	Enable	N/A	Disable
G5	1000TX	Up	Enable	1000 Full	Disable
G6	1000TX	Down	Enable	N/A	Disable
G7	1000TX	Down	Enable	N/A	Disable
G8	1000TX	Down	Enable	N/A	Disable

Refresh

Label	Description
Refresh	Click to refresh the page.

#### 5.6.1.4.3 Port Alias

This page provides alias IP address configuration. Some devices might have more than one IP addresses.

You could specify other IP addresses here.

**Port Alias**

Port No.	Alias
G1	<input type="text"/>
G2	<input type="text"/>
G3	<input type="text"/>
G4	<input type="text"/>
G5	<input type="text"/>
G6	<input type="text"/>
G7	<input type="text"/>
G8	<input type="text"/>

Save Changes

#### 5.6.1.4.4 Egress

**Egress Setting**

Port No.	Egress	Type
G1	<input type="text" value="0"/>	fps ▼
G2	<input type="text" value="0"/>	fps ▼
G3	<input type="text" value="0"/>	fps ▼
G4	<input type="text" value="0"/>	fps ▼
G5	<input type="text" value="0"/>	fps ▼
G6	<input type="text" value="0"/>	fps ▼
G7	<input type="text" value="0"/>	fps ▼
G8	<input type="text" value="0"/>	fps ▼

Save Changes

Label	Description
Port No.	The number of ports you want to configure.
Egress	The transmission rate for outgoing traffic.
Type	Controls the unit of measure for the storm control rate as fps or kbps. The default value is "fps".
Save Changes	Click to save changes.

### 5.6.1.4.5 Ingress

**Ingress Setting**

Port No.	Ingress Limit Frame Type	Ingress	Burst Size
G1	All	0 kbps	2000 Byte
G2	All	0 kbps	2000 Byte
G3	All	0 kbps	2000 Byte
G4	All	0 kbps	2000 Byte
G5	All	0 kbps	2000 Byte
G6	All	0 kbps	2000 Byte
G7	All	0 kbps	2000 Byte
G8	All	0 kbps	2000 Byte

Save Changes

Label	Description
<b>Ingress Limit Frame Type</b>	Valid values include <b>All</b> , <b>Broadcast only</b> , <b>Broadcast/Multicast</b> and <b>Broadcast/Multicast/Flooded Unicast</b> .
<b>Ingress</b>	The transmission rate for incoming traffic.
<b>Burst Size</b>	The default value is 2000 Byte.
<b>Save Changes</b>	Click to save changes.

### 5.6.1.4.6 Port Trunk

A port trunk is a group of ports that have been grouped together to function as one logical path. This method provides an economical way for you to increase the bandwidth between the switch and another networking device. In addition, it is useful when a single physical link between the devices is insufficient to handle the traffic load. This page allows you to configure the aggregation hash mode and the aggregation group.



Port Trunk - Setting

Port No.	Group ID	Type
G1	none ▼	Static ▼
G2	none ▼	Static ▼
G3	none ▼	Static ▼
G4	none ▼	Static ▼
G5	none ▼	Static ▼
G6	none ▼	Static ▼
G7	none ▼	Static ▼
G8	none ▼	Static ▼

802.3ad LACP Work Ports

Group ID	Work Ports
Trunk.1	max ▼
Trunk.2	max ▼
Trunk.3	max ▼
Trunk.4	max ▼

Save Changes

Label	Description
Group ID	Indicates the ID of each aggregation group. <b>None</b> means no aggregation. Only one group ID is valid per port.
Type	The switch supports two types of link aggregation; static and 802.3ad LACP. Static trunks are manually configured, while LACP-configured ports will automatically negotiate a trunk with LACP-configured ports on another device.
Work Port	The total number of active ports in a dynamic trunk group. The default value of works ports is <b>Max</b> . In a dynamic trunk group, if the number of work ports is lower than the number of members of the trunk group, the exceed ports are standby/redundant ports and can be aggregated if working ports fail. If it is a static trunk group, the number of work ports must equal the total number of group member ports.
Save Changes	Click to save changes.

**Port Trunk - Status**

Group ID	Trunk Member	Type
Trunk.1	N/A	Static
Trunk.2	N/A	Static
Trunk.3	N/A	Static
Trunk.4	N/A	Static

Refresh

Label	Description
Group ID	Indicates the ID of each aggregation group. <b>None</b> means no aggregation. Only one group ID is valid per port.
Trunk Member	Lists members of a specific trunk group.
Type	Indicates the type of the port trunk
Refresh	Click to refresh the page.

### 5.6.1.5 VLAN

#### 5.6.1.5.1 802.1Q VLAN

##### IEEE 802.1Q

A VLAN (Virtual LAN) is a logical LAN based on a physical LAN with links that does not consist of a physical (wired or wireless) connection between two computing devices but is implemented using methods of network virtualization. A VLAN can be created by partitioning a physical LAN into multiple logical LANs using a VLAN ID. You can assign switch ports to a VLAN and add new VLANs in this page.

**VLAN Mode Setting**

Operation Mode: 802.1Q ▼

**Port Setting**

Port No.	Link Type	PVID	Untagged VID	Tagged VIDs
G1	Access ▼	1	1	
G2	Access ▼	1	1	
G3	Access ▼	1	1	
G4	Access ▼	1	1	
G5	Access ▼	1	1	
G6	Access ▼	1	1	
G7	Access ▼	1	1	
G8	Access ▼	1	1	

Note: Use the comma to separate the multiple tagged VIDs.  
E.g., 2-4,6 means joining the Tagged VLAN 2, 3, 4 and 6.

Save Changes

Label	Description
VLAN Operation Mode	Available options include <b>Disable</b> and <b>802.1Q</b>
Link type	<p>Three link types are available:</p> <p><b>Access Link:</b> An access link connects a VLAN-unaware device to the port of a VLAN-aware bridge. All frames on access links must be implicitly tagged (untagged).</p> <p><b>Trunk Link:</b> All the devices connected to a trunk link, including workstations, must be VLAN-aware. All frames on a trunk link must have a special header attached.</p> <p><b>Hybrid Link:</b> The combination of Access Link and Trunk Link. This is a link where both VLAN-aware and VLAN-unaware devices are attached. It can have both tagged and untagged frames, but all the frames for a specific VLAN must be either tagged or untagged.</p> <p><b>Hybrid (QinQ) Link:</b> Allows one more VLAN tag in an original VLAN frame.</p>
Untagged VID	Set the port default VLAN ID for untagged devices that connect to the port. The range is 1 to 4094.
Tagged VIDs	Set the tagged VIDs to carry different VLAN frames to another switch.
Save Changes	Click to save changes.

### 5.6.1.5.2 Port Based VLAN

Packets can only be sent to members in the same VLAN group. All unselected ports will be treated as belonging to another single VLAN. If port-based VLAN is enabled, the VLAN-tagging is ignored.

**VLAN Mode Setting**  
Operation Mode: Port Based ▼

**Port Based VLAN Setting**  
Group Name :   
Vlan ID :   

Port Name	Enable
G1	<input type="checkbox"/>
G2	<input type="checkbox"/>
G3	<input type="checkbox"/>
G4	<input type="checkbox"/>
G5	<input type="checkbox"/>
G6	<input type="checkbox"/>
G7	<input type="checkbox"/>
G8	<input type="checkbox"/>

Add Edit

**Port Based Vlan Table**  
Show 10 ▼ entries  

Search:

Vlan ID ▲	Group Name ▼	Ports ▼
No data available in table		

Showing 0 to 0 of 0 entries  

First Previous Next Last

Remove

Apply

Label	Description
VLAN Operation Mode	Available options include <b>Disable</b> and <b>Port Base</b> .
Group Name	The name of the VLAN that you want to change settings.
VLAN ID	The number of the VLAN
Add	Click to start adding a VLAN
Edit	Edits existing VLANs
Remove	Deletes existing VLANs
Apply	Click to apply the configurations

### 5.6.1.6 Traffic Prioritization

With traffic prioritization schemes, the switch can transmit data based on its importance, thereby ensuring mission-critical applications, such as VoIP and video teleconferencing, have sufficient bandwidth for transmission when the network is congested.

QoS (Quality of Service) is a method to achieve efficient bandwidth utilization between devices by

prioritizing frames according to individual requirements and transmit the frames based on their importance. Frames in higher priority queues receive a bigger slice of bandwidth than those in a lower priority queue.

### 5.6.1.6.1 QoS Policy

Policing is a traffic regulation mechanism for limiting the rate of traffic streams, thereby controlling the maximum rate of traffic sent or received on an interface. When the traffic rate exceeds the configured maximum rate, policing drops or remarks the excess traffic. This page allows you to configure QoS policies for the switch.

**QoS Mode**

Disable

**QoS Policy**

☒ Use an 33,25,17,12,6,3,2,1 weighted fair queuing scheme
 ☐ Use a strict priority scheme

Save Changes

Label	Description
QOS Mode	<p>Available modes include:</p> <p><b>Disable:</b> disables the mode</p> <p><b>Port-base:</b> the output priority is determined by ingress port.</p> <p><b>COS only:</b> the output priority is determined by COS only.</p> <p><b>TOS only:</b> the output priority is determined by TOS only.</p> <p><b>COS first:</b> the output priority is determined by COS and TOS, but COS first.</p> <p><b>TOS first:</b> the output priority is determined by COS and TOS, but TOS first.</p>
QOS policy	<p><b>Using the 32,25,17,12,6,3,2,1 weight fair queue scheme:</b> the output queues will use a 32:25:17:12:6:3:2:1 ratio to transmit packets from the highest to lowest queue. For example: 32 high queue packets, 12 middle queue packets, 2 low queue packets, and the one lowest queue packets are transmitted in one turn.</p> <p><b>Use the strict priority scheme:</b> when traffic arrives at the device, traffic on the highest priority queue will be transmitted first, followed by traffic on lower priorities. If there is always some content in the highest priority queue, then the other packets in the rest of queues will not be sent until the highest priority queue is empty.</p>
Save Changes	Click to save changes.

### 5.6.1.6.2 Port-based Priority

**Port-based Priority**

Port No.	Priority
G1	7 ▼
G2	7 ▼
G3	7 ▼
G4	7 ▼
G5	7 ▼
G6	7 ▼
G7	7 ▼
G8	7 ▼

Save Changes

Label	Description
Priority	Assigns a port to a priority queue. Eight priority queues are available
Save Changes	Click to save changes.

### 5.6.1.6.3 COS/802.1p

COS (Class of Service), also known as 802.1p, is a parameter for differentiating the types of payloads contained in the packet to be transmitted. CoS operates only on 802.1Q VLAN Ethernet at Layer 2, while other QoS mechanisms operate at the Layer 3 or use a local QoS tagging system that does not modify the actual packet. COS supports up to 7 priorities and 8 priority queues. When an ingress packet has no VLAN tag, the default priority value will be used.

### COS Priority Setting

COS	Priority
0	0 ▼
1	1 ▼
2	2 ▼
3	3 ▼
4	4 ▼
5	5 ▼
6	6 ▼
7	7 ▼

### COS Port Default Setting

Port No.	COS
G1	0 ▼
G2	0 ▼
G3	0 ▼
G4	0 ▼
G5	0 ▼
G6	0 ▼
G7	0 ▼
G8	0 ▼

Save Changes

Label	Description
Priority	Assigns a port to a priority queue. Eight priority queues are available
Save Changes	Click to save changes.

### 5.6.1.6.4 TOS/DSCP

TOS (Type of Service) is a field in the IP header of a packet. It is used by Differentiated Services and is called the DSCP (Differentiated Services Code Point). The output priority of a packet can be determined by this field and the supported priority value ranges from 0 to 63. DSCP supports eight priority queues.

TOS/DSCP

DSCP	0	1	2	3	4	5	6	7
Priority	0 ▼	0 ▼	0 ▼	0 ▼	0 ▼	0 ▼	0 ▼	0 ▼
DSCP	8	9	10	11	12	13	14	15
Priority	1 ▼	1 ▼	1 ▼	1 ▼	1 ▼	1 ▼	1 ▼	1 ▼
DSCP	16	17	18	19	20	21	22	23
Priority	2 ▼	2 ▼	2 ▼	2 ▼	2 ▼	2 ▼	2 ▼	2 ▼
DSCP	24	25	26	27	28	29	30	31
Priority	3 ▼	3 ▼	3 ▼	3 ▼	3 ▼	3 ▼	3 ▼	3 ▼
DSCP	32	33	34	35	36	37	38	39
Priority	4 ▼	4 ▼	4 ▼	4 ▼	4 ▼	4 ▼	4 ▼	4 ▼
DSCP	40	41	42	43	44	45	46	47
Priority	5 ▼	5 ▼	5 ▼	5 ▼	5 ▼	5 ▼	5 ▼	5 ▼
DSCP	48	49	50	51	52	53	54	55
Priority	6 ▼	6 ▼	6 ▼	6 ▼	6 ▼	6 ▼	6 ▼	6 ▼
DSCP	56	57	58	59	60	61	62	63
Priority	7 ▼	7 ▼	7 ▼	7 ▼	7 ▼	7 ▼	7 ▼	7 ▼

Save Changes

Label	Description
Priority	Assigns a port to a priority queue. Eight priority queues are available
Save Changes	Click to save changes.

## 5.7 DHCP Server

The switch provides DHCP server functions. By enabling DHCP, the switch will become a DHCP server and dynamically assigns IP addresses and related IP information to network clients.

### 5.7.1 Basic Setting

This page allows you to set up DHCP settings for the switch. You can check the **Enabled** checkbox to activate the function. Once the box is checked, you will be able to input information in each column.



**DHCP Server**

Delete	Enabled	Vlan	Start IP Address	End IP Address	Lease Time
default	<input checked="" type="checkbox"/>	lan	10.0.0.100	10.0.0.109	1 (hours)

Add

Save

Label	Description
DHCP Server	Enables or disables DHCP server function. When enabled, the switch will become the DHCP server on your local network.
Start IP Address	The beginning of the dynamic IP address range. The lowest IP address in the range is considered the start IP address. For example, if the range is from 10.0.0.100 to 10.0.0.109, 10.0.0.100 will be the start IP address.
End IP Address	The end of the dynamic IP address range. The highest IP address in the range is considered the end IP address. For example, if the range is from 10.0.0.100 to 10.0.0.109, 10.0.0.109 will be the end IP address
Lease Time (hours)	The length of time that the client may use the IP address it has been assigned. The time is measured in hours.
Save Changes	Click to save changes.

## 5.7.2 Client List and Static IP

When DHCP server functions are activated, the switch will collect DHCP client information and display it in the following table.

**Client IP Entry**

Show  entries

Search:

Name	Vlan	IP	MAC
No data available in table			

Showing 0 to 0 of 0 entries

Previous Next

Refresh

### Static IP Setting

Name:   
VLAN ID:   
IP Address:   
MAC Address:

Add Edit Reset

### Static IP Entry

Show  entries

Search:

Name	Vlan	IP	MAC
No data available in table			

Showing 0 to 0 of 0 entries

Previous Next

Remove

Apply

Label	Description
Name	The Name of client.
VLAN ID	Indicates the ID of this particular VLAN.
IP Address	The IP address of client
MAC Address	The MAC Address of client.

### 5.7.3 Port and IP Binding

You can assign a specific IP address within the dynamic IP range to a specific port. When a device is connected to the port and requests for dynamic IP assigning, the switch will assign the IP address that has previously been assigned to the connected device.

### Port and IP Binding

Port No.	VLAN	IP
G1	lan ▼	<input type="text"/>
G2	lan ▼	<input type="text"/>
G3	lan ▼	<input type="text"/>
G4	lan ▼	<input type="text"/>
G5	lan ▼	<input type="text"/>
G6	lan ▼	<input type="text"/>
G7	lan ▼	<input type="text"/>
G8	lan ▼	<input type="text"/>

Save Changes

## 5.8 SNMP

SNMP (Simple Network Management Protocol) is a protocol for managing devices on IP networks. It is mainly used network management systems to monitor the operational status of networked devices. In an event-triggered situation, traps and notifications will be sent to administrators.

### 5.8.1 Agent Setting

An SNMP agent will receive and process requests, send responses to the manager, and send traps when an event occurs. The following page allows you to configure the SNMP agent for the switch.

**Agent Mode Setting**

SNMP Agent Version:

SNMPV1/V2c ▼

**SNMP V1/V2c Community**

Community String	Privilege
public	Read only ▼
private	Read and Write ▼
	Read only ▼
	Read only ▼

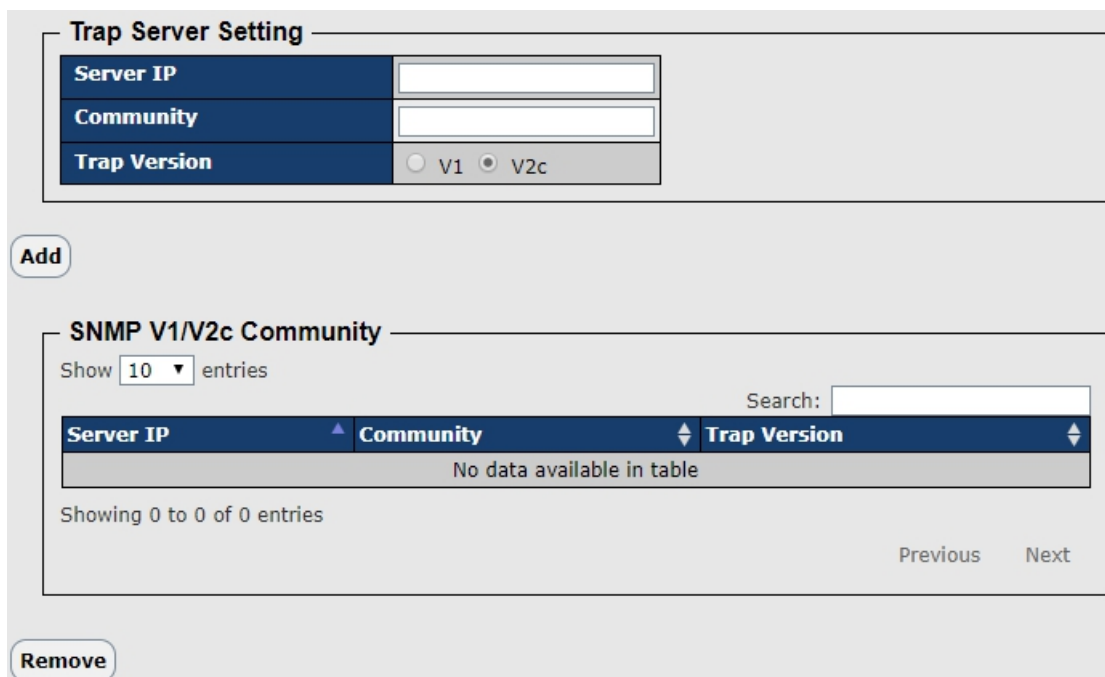
Save Changes

Label	Description
SNMP Agent Version	The column shows the version of the SNMP agent used by the switch. Three SNMP versions are supported, including <b>SNMP V1</b> , <b>SNMP V2c</b> , and <b>SNMP V3</b> . SNMP V1/SNMP V2c agents use a community string to authenticate the SNMP management station and SNMP agent. SNMP V3 requires MD5 or DES authentication which will encrypt data for higher data security.
Community String	The default community string that provides monitoring or read capability is often <b>public</b> . The default management or write community string is often <b>private</b> . Do not leave the community string to public on any of your SNMP agents. Since anyone with SNMP manager software installed on his/her PC can make changes to your SNMP agents, this will expose your SNMP agent to any SNMP management station.
Privilege	Choose the appropriate access level from the dropdown list. <b>Read Only:</b> The community string can only read the values of MIB objects. <b>Write Only:</b> The community string can read and write the values of MIB objects. <b>Read and Write:</b> The community string can read and write the values of

	MIB objects and send MIB object values for a trap and inform messages.
Save Changes	Click to save changes.

## 5.8.2 Trap Setting

SNMP traps are event reports sent to a list of managers configured to receive event notifications when an error occurs. SNMP traps provide the value of one or more instances of management information. A trap manager is a management station that receives traps. If no trap manager is defined, no traps will be issued. You can create a trap manager by entering the IP address of the station and a community string.



Label	Description
Server IP	The IP address of the server to receive traps
Community	The community string for authentication
Trap Version	The trap version. V1 and V2c are supported.
Add	Click to add the trap sever to the trap server profile.
SNMP V1/V2c Community	Shows a list of trap servers, including their community strings and trap versions.
Remove	Click to remove a trap server from the profile

### 5.8.3 SNMPv3 Setting

Unlike SNMP v1 and v2 which uses community strings for authentication, SNMP v3 uses username/password authentication, along with an encryption key. Therefore, SNMPv3 provides greater security features for authentication, privacy, and access control. The switch supports SNMP v3 which can be configured in the following page.



The screenshot shows the 'SNMPv3 User Configuration' window. It includes a label 'SNMP Engine ID:' and a table with columns: 'Delete', 'User Name', 'Security Level', 'Authentication Protocol', 'Authentication Password', 'Privacy Protocol', and 'Privacy Password'. There is an 'Add' button below the table.

#### 5.8.3.1 SNMPv3 User Configuration

Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Engine ID	An octet string identifying the engine ID that this entry should belong to. The string must contain an even number between 10 and 64 hexadecimal digits, but all-zeros and all-'F's are not allowed. The SNMPv3 architecture uses User-based Security Model (USM) for message security and View-based Access Control Model (VACM) for access control. For the USM entry, the <b>usmUserEngineID</b> and <b>usmUserName</b> are the entry keys. In a simple agent, usmUserEngineID is always that agent's own snmpEngineID value. The value can also take the value of the snmpEngineID of a remote SNMP engine with which this user can communicate. In other words, if user engine ID is the same as system engine ID, then it is local user; otherwise it's remote user.
User Name	A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and only ASCII characters from 33 to 126 are allowed.
Security Level	Indicates the security model that this entry should belong to. Possible security models include: <b>NoAuth, NoPriv</b> : no authentication and none privacy <b>Auth, NoPriv</b> : Authentication and no privacy <b>Auth, Priv</b> : Authentication and privacy The value of security level cannot be modified if the entry already exists, which means the value must be set correctly at the time of entry creation.
Authentication Protocol	Indicates the authentication protocol that this entry should belong to. Possible authentication protocols include: <b>None</b> : no authentication protocol <b>MD5</b> : an optional flag to indicate that this user is using MD5 authentication

	<p>protocol</p> <p><b>SHA:</b> an optional flag to indicate that this user is using SHA authentication protocol</p> <p>The value of security level cannot be modified if the entry already exists, which means the value must be set correctly at the time of entry creation.</p>
<b>Authentication Password</b>	<p>A string identifying the authentication pass phrase. For MD5 authentication protocol, the allowed string length is 8 to 32. For SHA authentication protocol, the allowed string length is 8 to 40. Only ASCII characters from 33 to 126 are allowed.</p>
<b>Privacy Protocol</b>	<p>Indicates the privacy protocol that this entry should belong to. Possible privacy protocols include:</p> <p><b>None:</b> no privacy protocol</p> <p><b>DES:</b> an optional flag to indicate that this user is using DES authentication protocol</p>
<b>Privacy Password</b>	<p>A string identifying the privacy pass phrase. The allowed string length is 8 to 32, and only ASCII characters from 33 to 126 are allowed.</p>

### 5.8.3.2 SNMPv3 Group Configuration

An SNMP group is an access control policy for you to add users. Each SNMP group is configured with a security model, and is associated with an SNMP view. A user within an SNMP group should match the security model of the SNMP group. These parameters specify what type of authentication and privacy a user within an SNMP group uses. Each SNMP group name and security model pair must be unique. This page allows you to configure the SNMPv3 group table. The entry index keys are **Security Model** and **Security Name**.

SNMPv3 Group Configuration

Delete Security Model Security Name Group Name

Add

Label	Description
<b>Delete</b>	Check to delete the entry. It will be deleted during the next save.
<b>Security Model</b>	<p>Indicates the security model that this entry should belong to. Possible security models included:</p> <p><b>v1:</b> Reserved for SNMPv1.</p> <p><b>v2c:</b> Reserved for SNMPv2c.</p> <p><b>usm:</b> User-based Security Model (USM).</p>
<b>Security Name</b>	A string identifying the security name that this entry should belong to. The allowed string length is 1 to 32, and only ASCII characters from 33 to 126 are allowed.

Group Name	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and only ASCII characters from 33 to 126 are allowed.
------------	---

### 5.8.3.3 SNMPv3 View

The SNMP v3 View table specifies the MIB object access requirements for each View Name. You can specify specific areas of the MIB that can be accessed or denied based on the entries or create and delete entries in the View table in this page. The entry index keys are **View Name** and **OID Subtree**.

**SNMPv3 View Configuration**

Delete View Name View Type OID Subtree

Add

Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
View Name	A string identifying the view name that this entry should belong to. The allowed string length is 1 to 32, and only ASCII characters from 33 to 126 are allowed.
View Type	<p>Indicates the view type that this entry should belong to. Possible view types include:</p> <p><b>Included:</b> an optional flag to indicate that this view subtree should be included.</p> <p><b>Excluded:</b> An optional flag to indicate that this view subtree should be excluded.</p> <p>Generally, if an entry's view type is <b>Excluded</b>, it should exist another entry whose view type is <b>Included</b>, and its OID subtree oversteps the <b>Excluded</b> entry.</p>
OID Subtree	The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is digital number or asterisk (*).

### 5.8.3.4 SNMPv3 Access Configuration

This page allows you to configure SNMPv3 access table. The entry index keys are **Group Name**, **Security Model**, and **Security Level**.

**SNMPv3 Access Configuration**

Delete Group Name Security Model Security Level Read View Name Write View Name

Add

Save configure

Label	Description
<b>Delete</b>	Check to delete the entry. It will be deleted during the next save.
<b>Group Name</b>	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and only ASCII characters from 33 to 126 are allowed.
<b>Security Model</b>	Indicates the security model that this entry should belong to. Possible security models include: <b>any</b> : Accepted any security model (v1 v2c usm). <b>v1</b> : Reserved for SNMPv1. <b>v2c</b> : Reserved for SNMPv2c. <b>usm</b> : User-based Security Model (USM).
<b>Security Level</b>	Indicates the security model that this entry should belong to. Possible security models include: <b>NoAuth, NoPriv</b> : no authentication and no privacy <b>Auth, NoPriv</b> : Authentication and no privacy <b>Auth, Priv</b> : Authentication and privacy
<b>Read View Name</b>	The name of the MIB view defining the MIB objects for which this request may request the current values. The allowed string length is 1 to 32, and only ASCII characters from 33 to 126 are allowed.
<b>Write View Name</b>	The name of the MIB view defining the MIB objects for which this request may potentially SET new values. The allowed string length is 1 to 32, and only ASCII characters from 33 to 126 are allowed.
<b>Save Changes</b>	Click to save changes.

## 5.9 Security

### 5.9.1 Management Security

By setting up a secure IP list, only IP addresses in the list can manage the switch according to the management mode you have specified (WEB, HTTPS, SSH, SNMP, ICMP , etc.).



**Interface Setting**

Interface:
lan

**Management Security**

Mode:
Disable

Management Security	Enable
Enable HTTP(Web) Management	<input type="checkbox"/>
Enable HTTPS Management	<input type="checkbox"/>
Enable SSH Management	<input type="checkbox"/>
Enable SNMP Management	<input type="checkbox"/>
Enable ICMP(Ping) Management	<input type="checkbox"/>

Modify

Secure IP

Add

**Note:**

When the NAT service is turned on, the Interface-Security will be invalid.

Save Changes

Label	Description
Mode	Indicates IP security mode. Enables or disables IP security functions.
Enable WEB Management	Check to enable WEB management
Enable HTTPS Management	Check to enable HTTPS management
Enable SSH Management	Check to enable SSH management
Enable SNMP Management	Check to enable SNMP management
Enable ICMP Management	Check to enable ICMP management
Secure IP	Management Security can restrict remote management to some specific IP addresses. Only these secure IP addresses can manage this switch remotely.

### 5.9.2 NAPT Only

By setting up a NAPT interface or IP address,Only interface or IP addresses in the list can manage the switch according to the management mode you have specified

**NAPT Interface Setting**

Interface: Choose Interface ▼

**Management Security**

Lan	
Management Security	Enable
Enable HTTP(Web) Management	<input type="checkbox"/>
Enable HTTPS Management	<input type="checkbox"/>
Enable SSH Management	<input type="checkbox"/>
Enable SNMP Management	<input type="checkbox"/>
Enable ICMP(Ping) Management	<input type="checkbox"/>

Wan	
Management Security	Enable
Enable HTTP(Web) Management	<input type="checkbox"/>
Enable HTTPS Management	<input type="checkbox"/>
Enable SSH Management	<input type="checkbox"/>
Enable SNMP Management	<input type="checkbox"/>
Enable ICMP(Ping) Management	<input type="checkbox"/>

Lan	
Modify	Secure IP
<input type="button" value="Add"/>	<input type="text"/>

Wan	
Modify	Secure IP
<input type="button" value="Add"/>	<input type="text"/>

**Note:**

When the Interface-Security or other Nat services are turned on, the NAPT-Security will be invalid.

Label	Description
Interface	Choose NAPT interface.
Enable WEB Management	Check to enable WEB management
Enable HTTPS Management	Check to enable HTTPS management
Enable SSH Management	Check to enable SSH management
Enable SNMP Management	Check to enable SNMP management
Enable ICMP Management	Check to enable ICMP management
LAN Secure IP	Management Security can restrict remote management to some specific IP addresses. Only these LAN secure IP addresses can manage this switch remotely.
WAN Secure IP	Management Security can restrict remote management to some specific IP addresses. Only these WAN secure IP addresses can manage this switch remotely.

### 5.9.3 Static MAC Address

You can use static MAC addresses to provide port security for the switch. With this method, only the frames with the MAC addresses in this list will be forwarded, otherwise will be discarded.

### Static Mac Setting

Mac Address:

Port No:

G1 ▼

Add

Remove

### Static Mac Address Table

Show 

20 ▼

 entries

Search:

Type ▲	Mac Address	Port No. ▼
No data available in table		

Showing 0 to 0 of 0 entries

Previous

Next

Flush Table

Label	Description
MAC Address	Enter a MAC address for a specific port.
Port NO.	Select a switch port
Add	Add the MAC address and port information.
Remove	Deletes an entry
Flush Table	Click to refresh the page.

## 5.10 Warming

The switch supports several alerting methods, including fault relay, SYSLOG and e-mail. These methods enable you to monitor switch status remotely. When an event occurs, the system will send an alert to your appointed servers.

### 5.10.1 Fault Relay Alarm

When any selected fault event is happened, the Fault LED in switch panel will light up and the electric relay will signal at the same time.

### Fault Relay Alarm

Consist Switch Port Link Down/Broken

☐ G1
 ☐ G2

☐ G3
 ☐ G4

☐ G5
 ☐ G6

☐ G7
 ☐ G8

Backbone Switch Port Link Down/Broken

☐ G9
 ☐ G10

☐ G11
 ☐ G12

Save Changes

### 5.10.2 SYSLOG Setting

SYSLOG is a protocol that allows a device to send event notification messages across IP networks to event message collectors. It permits separation of the software that generates messages from the system that stores them and the software that reports and analyzes them. As Syslog messages are UDP-based, the sender and receiver will not be aware of it if the packet is lost due to network disconnection and no UDP packet will be resent.

### SYSLOG Setting

Mode: Disable ▾

Server IP Address: 0.0.0.0

Save Changes

Label	Description
Syslog Mode	<b>Enable:</b> enables SYSLOG <b>Disable:</b> disables SYSLOG
Save Changes	Click to save changes.

### 5.10.3 SMTP Setting

SMTP (Simple Mail Transfer Protocol) is a protocol for transmitting e-mails across the Internet. By setting up SMTP alert, the device will send a notification e-mail when a user-defined event occurs.

**SMTP Setting**

Mode:

SMTP Server Address:

Sender E-mail Address:

Mail Subject:

SSL/TLS:

Authentication:

Username:

Password:

Confirm Password:

Recipient E-mail Address 1:

Recipient E-mail Address 2:

Recipient E-mail Address 3:

Recipient E-mail Address 4:

Recipient E-mail Address 5:

Recipient E-mail Address 6:

Save Changes

Label	Description
E-mail Alert	Enables or disables transmission of system warnings by e-mail
SMTP Server Address	The IP address of the SMTP server to receive the notification e-mail
Mail Subject	Subject of the mail
SSL/TLS	Enables or disables security.
Sender	The email account to send the alert
Authentication	<ul style="list-style-type: none"> <li>■ <b>Username:</b> the authentication username</li> <li>■ <b>Password:</b> the authentication password</li> <li>■ <b>Confirm Password:</b> re-enter password</li> </ul>
Recipient E-mail Address	The recipient's e-mail address. A mail allows for 6 recipients.
Save Changes	Click to save changes.

### 5.10.4 Event Selection

The device supports both SYSLOG and SMTP alerts. Check the corresponding box to enable the system event warning method you want. Please note that the checkboxes will gray out if SYSLOG or SMTP is disabled.

**Event Selection**

Event	SYSLOG	SMTP
System Restart	<input type="checkbox"/>	<input type="checkbox"/>
SNMP Authentication Failure	<input type="checkbox"/>	<input type="checkbox"/>
O-Ring Topology Change	<input type="checkbox"/>	<input type="checkbox"/>

Consist Switch Port

Port No.	SYSLOG	SMTP
G1	Disable ▼	Disable ▼
G2	Disable ▼	Disable ▼
G3	Disable ▼	Disable ▼
G4	Disable ▼	Disable ▼
G5	Disable ▼	Disable ▼
G6	Disable ▼	Disable ▼
G7	Disable ▼	Disable ▼
G8	Disable ▼	Disable ▼

Backbone Switch Port

Port No.	SYSLOG	SMTP
G9	Disable ▼	Disable ▼
G10	Disable ▼	Disable ▼
G11	Disable ▼	Disable ▼
G12	Disable ▼	Disable ▼

Save Changes

Label	Description
<b>System Restart</b>	Sends alerts when you restart the device using the power button on your PC.
<b>Authentication Failure</b>	Sends alerts when SNMP authentication fails
<b>O-Ring topology change</b>	Sends alerts when O-Ring topology changes
<b>Port Event</b>	<p>Sends alerts when the port meets a specified condition. Available options include:</p> <ul style="list-style-type: none"> <li>■ <b>Disable</b>: disables alert function</li> <li>■ <b>Link Up</b>: sends alerts when port is connected</li> </ul>

	<ul style="list-style-type: none"> <li>■ <b>Link Down:</b> sends alerts when port is not connected</li> <li>■ <b>Link Up &amp; Link Down:</b> sends alerts when port is connected and disconnected</li> </ul>
Save Changes	Click to save changes.

## 5.11 System Monitor and Diag

### 5.11.1 System Event Log

If a system log is enabled, the system event log will be shown in this table.

#### System Event Log

Show  entries

Search:

Date Time	Message Text
No data available in table	

Filter Time  Filter Text

Showing 0 to 0 of 0 entries

Previous Next

Refresh Clear

Label	Description
Clear	Clear log
Refresh	Click to refresh the page

### 5.11.2 Ping Watchdog

Specify ping IP address, set ping Interval 、Startup Delay 、. Failure ping count, choose action (reboot/Run custom script) after failure ping count.

#### Ping Watchdog

☐ Enable Ping Watchdog

IP Address To Ping:  IP Address

Ping Interval:  1 - 59 minutes

Startup Delay:  1 - 999 seconds

Failure ping count:  1 - 10

Action:

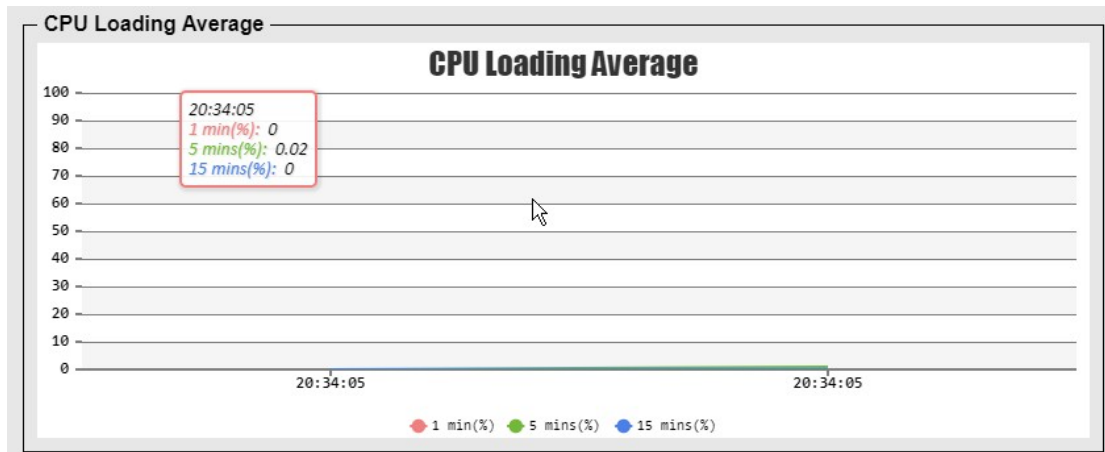
Save Changes Reset

Label	Description
IP Address To Ping	Specify destination IP address
Ping Interval	Set interval time

Startup Delay	Set delay time
Failures ping count	Ping loss count
Action	Select after failure ping Reboot/Run custom script

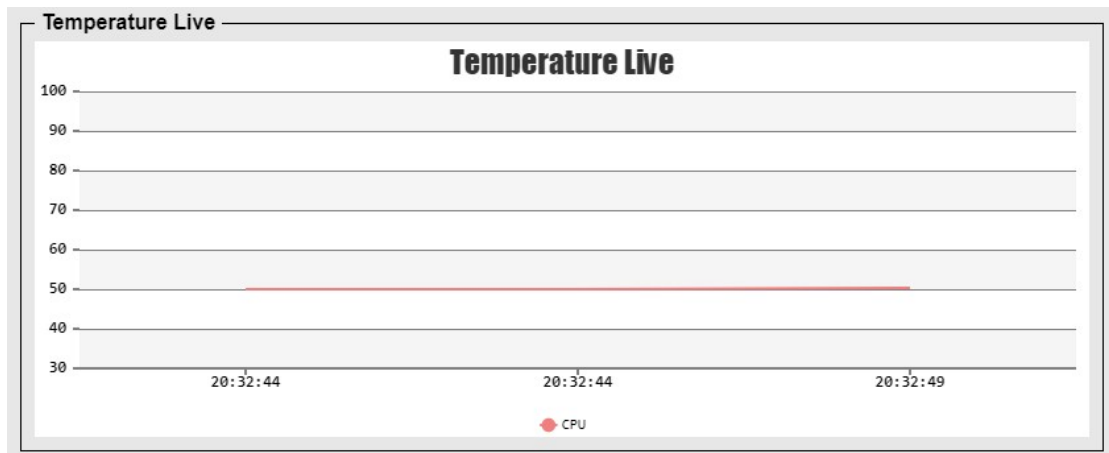
### 5.11.3 CPU Loading Average

View the CPU loading average



### 5.11.4 Temperature Monitor

View the CPU temperature



### 5.11.5 Cable Diagnostics

You can perform cable diagnostics for all ports or selected ports to diagnose any cable faults (short, open etc.) and feedback a distance to the fault. Simply select the port from the drop-down list and click **Start** to run the diagnostics. This will take approximately 5 seconds. If all ports are selected, this can take approximately 15 seconds. When completed, the page refreshes automatically, and you can view



the cable diagnostics results in the cable status table. Note that VeriPHY diagnostics is only accurate for cables 7 - 140 meters long. 10 and 100 Mbps ports will be disconnected while running VeriPHY diagnostics. Therefore, running VeriPHY on a 10 or 100 Mbps management port will cause the switch to stop responding until VeriPHY is completed.

**Cable Diagnostics**

Port No.	Result	Length(meter)	Date	Diagnostics
G1	no testing	0	none	diagnostic <input type="checkbox"/>
G2	no testing	0	none	diagnostic <input type="checkbox"/>
G3	no testing	0	none	diagnostic <input type="checkbox"/>
G4	no testing	0	none	diagnostic <input type="checkbox"/>
G5	no testing	0	none	diagnostic <input type="checkbox"/>
G6	no testing	0	none	diagnostic <input type="checkbox"/>
G7	no testing	0	none	diagnostic <input type="checkbox"/>
G8	no testing	0	none	diagnostic <input type="checkbox"/>
G9	no testing	0	none	diagnostic <input type="checkbox"/>
G10	no testing	0	none	diagnostic <input type="checkbox"/>
G11	no testing	0	none	diagnostic <input type="checkbox"/>
G12	no testing	0	none	diagnostic <input type="checkbox"/>

Select Diagnostics

Label	Description
Result	Cable connect status.
Length	Cable Length.
Date	Diagnostic Date
Diagnostic	Choose single port
Select Diagnostics	Choose multiple port

## 5.12 System Reboot

You can reset the stack switch on this page. After reset, the system will boot normally as if you have powered on the devices.

**Reboot**

- ☒ Image Bank 0: Kernel Version :K28.14 Firmware Version :V1.00
- ☐ Image Bank 1: Kernel Version :K28.13 Firmware Version :V1.00

Reboot Now

Save Changes

Reset

## 5.13 Logout

You can logout the system.

# Command Line Management

Besides Web-based management, the device also supports CLI management. You can use console or telnet to manage the switch by CLI.

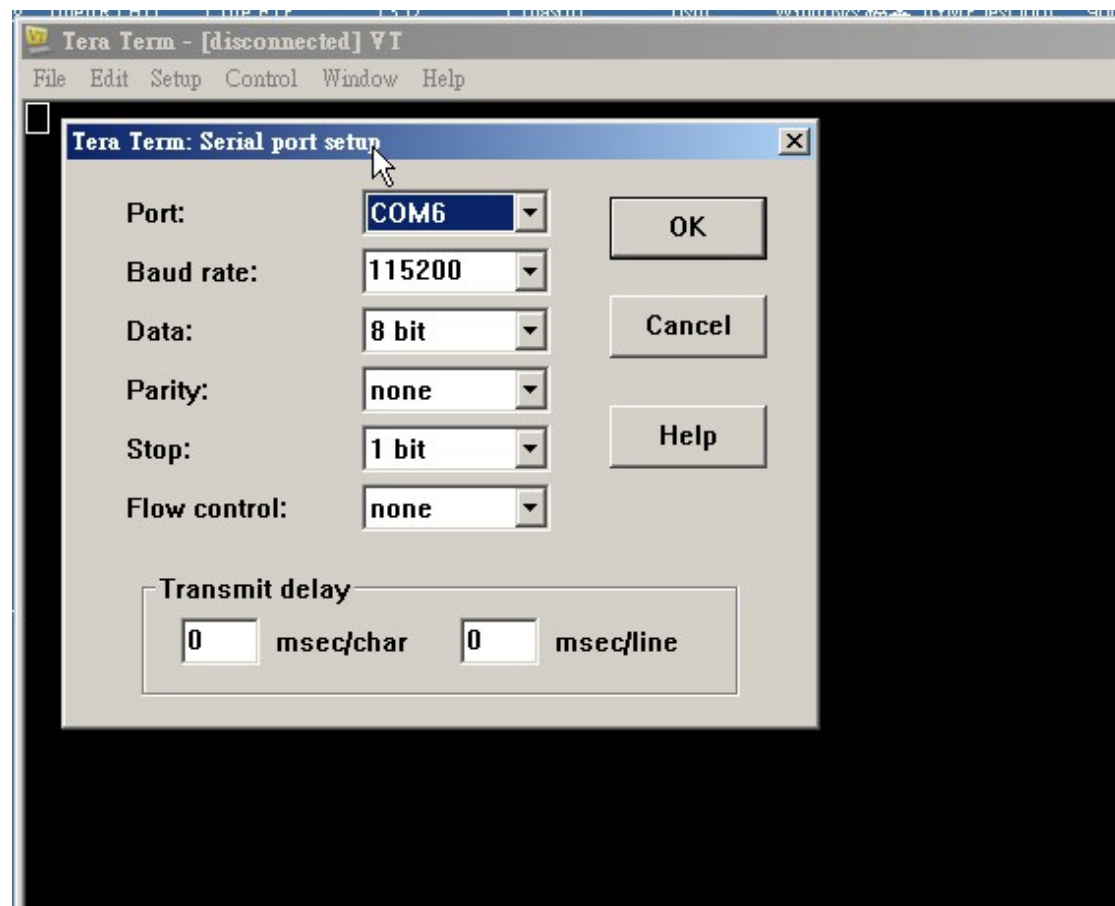
## CLI Management by Serial Console (115200, 8, none, 1, none)

Follow the steps below to access the console via M12-DB9 serial cable.

### Step 1: Install Tera Term



### Step 2. Input a "port" and "Baud rate" for the new connection.



Step 3. Input UserName and password: Default are admin



### Commander Groups



## System

System>	Name [name]
	Description [description]
	Location [location]
	Contact [contact]

## IGMP

IGMP>	Snooping 1:Enable 0:Disable
	Query 1:Enable 0:Disable
	Stream 1:Flooding 0:Blocking
	Filtering add [port][ip]
	Filtering delete [port][ip]

## admin

admin>	Adduser
	Deluser
	User-list

## Port

Port>	control[port] [item] [set]
	alias [port] [content]
	egress [port] [value] [speedtype]
	ingress [port] [value] [frame_type]
	trunk [port] [id] [trunk_type]
	lacp [id] [lacp_port]

## time

time>	timezone [utc]
	dateformat [dateformat]
	timeformat [timeformat]
	ntp_sntp_client
	ntp_server [enable_server]
	reset
	show

## rstp

rstp>	mode [enable_rstp_mode]
	setting
	port [port] [option] [input]
	reset
	restart
	show

## mstp

mstp setting>	mstp setting
	mstp port [port] [option] [input]
	mstp instance-setting [instance] [option] [input]
	mstp restart
	mstp reset
	mstp show
	mstp instance-port [instance] [port] [option] [input]

## lan\_ip

lan_ip>	configuration
	apply
	ip_setting

## wan\_ip

Wan_ip>	configuration
	wan_ip apply
	wan_ip ip_setting

## priority

priority>	priority qosmode [mode]
	priority qospolicy [policy]
	priority portbased [port] [port_based]
	priority cospri [cos] [port_based]
	priority cosport [port] [cos]
	priority tosdscp [dscp] [priority]

## warning

warning>	poweralarm [power] [alarm]
	linkalarm [port] [alarm]
	syslog [mode] [ip]
	smtp
	event [set] [select] [event]
	portevent [port] [select] [event]

## DHCP

dhcp>	configuration
	server [state]
	range [start] [end] [leasetime]
	static_ip_add [host] [mac] [ip]
	static_ip_del [ip]
	static_ip_edit [ip] [option] [input]
	restart

## VLAN

VLAN>	restart
	disable
	port_based
	8021q
	show

## LLDP

LLDP>	Setting [option] [protocol_num] [interval_num]
	show

## Security

Security >	configuration
	management[mode] [web] [telnet] [snmp]
	secure_ip_add [num] [ip]
	secure_ip_del [num]

## SNMP

Snm>	mode [version]
	community [option] [name] [privilege]
	trap_snmpv1v2 [option] [ip] [community] [version]
	trap_snmpv3 [option] [ip] [community]
	show

## Monitor

Monitor>	monitor portCounter
----------	---------------------

## Static MacAddress

staticMacaddress>	add [portNum] [mac]
	del [mac]
	show

## etbn ttdp setting

etbn ttdp_setting>	enable
	disable
	inaugurate
	rebuild
	show

## etbn dynamic\_setting rnat

etbn dynamic_setting rnat >	disable
	enable [etbn_auto_manual] [etbn_num] [etbn_bb_vlan_num]
	remove [etbn_remove]
	apply
	show

## etbn dynamic\_setting wan

etbn dynamic_setting wan >	disable
	enable [etbn_auto_manual] [etbn_num] [etbn_bb_vlan_num]
	wan remove [etbn_remove]
	wan apply
	wan show



### etbn dynamic\_setting lan

etbn dynamic_setting lan >	disable
	enable [etbn_auto_manual] [etbn_num] [etbn_bb_vlan_num]
	remove [etbn_remove]
	apply
	show

### etbn dynamic\_setting wan

etbn dynamic_setting wan>	wan disable
	wan enable [etbn_auto_manual] [etbn_num]
	[etbn_bb_vlan_num]
	wan remove [etbn_remove]
	wan apply
	wan show

### etbn dynamic\_setting lan

etbn dynamic_setting lan>	disable
	enable [etbn_auto_manual] [etbn_num]
	[etbn_bb_vlan_num]
	remove [etbn_remove]
	apply
	show

# Technology

ORing Switch Model	TGRS-T120-M12X-BP2-WV
Physical Ports	
10/100/1000Base-T(X) Ports in M12 Auto MDI/MDIX	LAN (G1 ~ G8) – 8 (8-pin female X-coding)
	WAN (G9 ~ G12) – 4 (8-pin female X-coding)
Technology	
Ethernet Standards	IEEE 802.3 for 10Base-T IEEE 802.3u for 100Base-TX IEEE 802.3ab for 1000Base-T IEEE 802.3x for Flow control IEEE 802.3ad for LACP (Link Aggregation Control Protocol) IEEE 802.1p for COS (Class of Service) IEEE 802.1Q for VLAN Tagging IEEE 802.1w for RSTP (Rapid Spanning Tree Protocol) IEEE 802.1s for MSTP (Multiple Spanning Tree Protocol) IEEE 802.1AB for LLDP (Link Layer Discovery Protocol)
MAC Table	2K (WAN port), 16K (LAN port)
Packet Buffer Size	1MB share
Priority Queues	8
Processing	Store-and-Forward
Switch Properties	Switching latency: 0.9 us Switching bandwidth: 24Gbps Throughput (packet per second): 17.857Mpps@64Bytes packet Max. Number of Available VLANs: 256 VLAN ID Range: VID 1 to 4095 IGMP multicast groups: 128 for each VLAN Port rate limiting: User Define
Jumbo Frame	Up to 10K Bytes
L3 Function	Static Routing, VRRP
Security Features	Enable/disable ports, MAC based port security Port based network access control (802.1x) VLAN (802.1Q) to segregate and secure network traffic Radius centralized password management SNMPv3 encrypted authentication and access security Https / SSH enhance network security Web and CLI authentication
Software Features	IEC 61375-2-5 TTDP (Train Topology Discovery Protocol) IEC 61375-2-3 TRDP (Train Real-Time Data Protocol) RSTP/MSTP (IEEE 802.1D/w/s) NAT: N-1 NAT, 1-1 NAT TOS/Diffserv supported Quality of Service (802.1p) for real-time traffic VLAN (802.1Q) with VLAN tagging IGMP Snooping QoS management Port configuration, status, statistics, monitoring, security DHCP Server/Client SMTP Client
Network Redundancy	O-Ring (Pending) O-Chain (Pending) MRP**NOTE MSTP (RSTP/STP compatible)
RS-232 Serial Console Port	RS-232 in M12 connector (5 pin female A-coding) with console cable. 115200bps, 8, N, 1 (support backup unit)
LED Indicators	
Power Indicator (PWR)	Green: Power LED x 1

System Indicator (Status)	Green: System on
Ring Master Indicator (R.M.)	Green: Indicates that the system is operating in O-Ring Master mode <b>(Pending)</b>
O-Ring Indicator (Ring)	Green: Indicates that the system operating in O-Ring mode <b>(Pending)</b> Green Blinking: Indicates that the Ring is broken.
Fault Indicator (Fault)	Amber: Indicate unexpected event occurred
10/100/1000Base-T(X) M12 Port Indicator	Green for Link/Act indicator: Green for link-up, Off for link-down, Blinking for Act. Green for speed indicator: Green for 1000Mbps, Off for 10/100Mbps
<b>Fault Contact</b>	
Relay	Relay output to carry capacity of 3A at 24VDC on M12 connector (5-pin female A-coding)
<b>Reset Function</b>	
Reset Button	< 5 sec: System reboot, > 5 sec: Factory default
<b>Power</b>	
Redundant Input Power	24~110 (16.8~137.5) VDC on M12 5-pin A-coding Male connector
Power Consumption (Typ.)	≤17Watts, 24VDC/0.69A (17W), 36VDC/0.45A (16W), 72VDC/0.21A (15W), 110VDC/0.13A (15W)
Overload Current Protection	Present
Reverse Polarity Protection	Present
<b>Physical Characteristic</b>	
Enclosure	IP-30
Dimension (W x D x H)	260 (W) x 50 (D) x 220 (H)mm 10.24 (W) x 1.97 (D) x 8.66 (H) inch
Weight (g)	1.865 Kg
<b>Environmental</b>	
Storage Temperature	-40 to 85°C (-40 to 185°F)
Operating Temperature	-25 to 70°C (-13 to 158°F)
Operating Humidity	5% to 95% Non-condensing
<b>Regulatory Approvals</b>	
EMC	CE EMC (EN 55024, EN 55032), FCC Part 15 B, EN 50155(EN 50121-1, EN 50121-3-2)
EMI	EN 55032, CISPR32, EN 61000-3-2, EN 61000-3-3, FCC Part 15 B class A
EMS	EN 55024 (IEC/EN 61000-4-2 (ESD: Contact 6KV, Air 8KV), IEC/EN 61000-4-3 (RS 80MHz to 1GHz: 20V/m, 1.4-2GHz:10V/m 1kHz 80% AM), IEC/EN 61000-4-4 (EFT Power 2KV, Single 2KV), IEC/EN 61000-4-5 (Surge: Power 2KV, RJ45 2KV), IEC/EN 61000-4-6 (CS 150K-80MHz: 10Vrms 1kHz 80% AM), IEC/EN 61000-4-8(PFME), IEC/EN 61000-4-11 (DIP))
Shock	IEC60068-2-27
Free Fall	IEC60068-2-31
Vibration	IEC60068-2-6
Safety	EN 60950-1 (LVD)
Other	EN 50155 (IEC 61373) compliant
MTBF	155,786hrs
Warranty	5 years