



Hardened L2/L3 Managed PoE++ Ethernet Switch

EX78900G Series User's Guide - GUI **FastFind Links**

Introduction

Installing the Switch

All Rights Reserved

Dissemination or reproduction of this document, or its contents, is not authorized except where expressly permitted. Violators are liable for damages. All rights reserved, for the purposes of patent application or trademark registration.

Disclaimer of Liability

The information contained in this document is subject to change without notice. EtherWAN is not liable for any errors or omissions contained herein or for resulting damage in connection with the information provided in this manual.

Warranty

For details on the EtherWAN warranty replacement policy, please visit our web site at:

https://www.etherwan.com/us/support/warranty-policy

Products Supported by this Manual:

EX78900G Series



Preface

Audience

This guide is designed for the person who installs, configures, deploys, and maintains the Ethernet network. This document assumes the reader has moderate hardware, computer, and networking skills. To be more familiar with networking technologies, please visit our free online training resources, EtherWAN Academy (academy.etherwan.com). You can also directly contact your sales representative in your respective region. For alternative ways to reach us, use <u>info@etherwan.com</u> for US customers; for other countries, <u>info@etherwan.com.tw</u>

Document Revision Level

This section provides a history of the revision changes to this document.

Revision	Document Version	Date	Description
А	Version 1	2024/06/20	Initial version

Changes in this Revision

This is first version of this document.

Document Conventions

This guide uses the following conventions to draw your attention to certain information.

Safety and Warnings

This guide uses the following symbols to draw your attention to certain information.

Symbol	Meaning	Description
6	Note	Notes emphasize or supplement important points of the main text.
Ŷ	Тір	Tips provide helpful information, guidelines, or suggestions for performing tasks more effectively.
<u>.</u>	Warning	Warnings indicate that failure to take a specified action could result in damage to the device, or could result in serious bodily injury.

Contents

Preface	3
Changes in this Revision	3
Document Conventions	4
Safety and Warnings	4
Contents	5
1 Introduction	10
Unpacking and Installation	11
Unpacking	11
Installing the Switch	11
Connecting to the Data Ports	11
Console Port	12
Connecting Power	12
Terminal Block	12
Relay Output Alarm	12
Initial Configuration	13
Reset Button	14
Copy Configuration to USB	14
Alternate (Backup) Firmware	14
2 Web Management Interface	16
About the Web-based graphical user interface (GUI)	16
Default IP Address	16
Login Process and Default Credentials	16
Navigating the GUI	18
3 System Menu	20
System Information	20
System Name	21
- System Password	21
IP Address	22
IPV6 Address	23

	System Time	. 24
	Management Interface	.24
	Configuration	.25
	Saving Switch Configuration	.25
	Firmware Upgrade	.26
	Reboot	.27
	User Account	.27
	Command Privilege	. 28
4 Dia	gnostics Commands	. 30
	System Utilization	. 30
	System Log	. 31
	RMON Statistics	. 32
	Remote Log Setting	. 33
	Alarm Setting	. 33
	Port Mirroring	. 38
	Email Alert	. 38
5 Por	rt Commands	. 40
5 Por	t Commands	40
5 Por	rt Commands Port Configuration Port Status	40 . 40 . 41
5 Por	rt Commands Port Configuration Port Status Flow Control	40 40 41 42
5 Por	rt Commands Port Configuration Port Status Flow Control Rate Control	. 40 40 41 42 43
5 Por 6 Swi	rt Commands Port Configuration Port Status Flow Control Rate Control	. 40 40 41 42 43 . 44
5 Por 6 Swi	rt Commands Port Configuration Port Status Flow Control Rate Control itching MAC Table	. 40 40 41 42 43 44 44
5 Por 6 Swi	rt Commands Port Configuration Port Status Flow Control Rate Control itching MAC Table Static MAC Entry	. 40 40 41 42 43 44 44
5 Por	Port Configuration	. 40 40 41 42 43 43 44 45 45
5 Por	Port Configuration	. 40 41 42 43 43 44 45 45 46
5 Por	rt Commands Port Configuration Port Status Flow Control Rate Control itching MAC Table Static MAC Entry Storm Control Storm Detect Trunking	. 40 41 42 43 43 44 45 45 45 46 47
5 Por	rt Commands Port Configuration Port Status Flow Control Rate Control itching MAC Table Static MAC Entry Storm Control Storm Detect Trunking LACP Trunking	. 40 40 41 42 43 43 44 45 45 45 46 47 47
5 Por	rt Commands Port Configuration Port Status Flow Control Rate Control MAC Table Static MAC Entry Storm Control Storm Detect Trunking LACP Trunking GVRP	. 40 40 41 42 43 43 44 45 45 45 46 47 47 48
5 Por	t Commands Port Configuration Port Status Flow Control Rate Control MAC Table MAC Table Static MAC Entry Storm Control Storm Detect Trunking LACP Trunking GVRP GMRP	. 40 40 41 42 43 43 44 45 45 45 46 47 47 48 49
5 Por	t Commands Port Configuration Port Status Flow Control Rate Control itching MAC Table Static MAC Entry Storm Control Storm Detect Trunking LACP Trunking GVRP GMRP VLAN Translation	. 40 40 41 42 43 43 44 45 45 45 45 46 47 47 48 49 50

PoE Scheduling	53
PoE Watchdog	55
7 IGMP	56
IGMP Snooping	56
8 STP	57
Spanning Tree Protocol (STP)	57
Rapid Spanning Tree protocol (RSTP)	57
Multiple Spanning Tree Protocol (MSTP)	57
Global Configuration	57
RSTP Port Setting	
MSTP Properties	
MSTP Instance Setting	60
MSTP Port Setting	60
Advanced Setting	61
9 VLAN	63
VLAN Setting	63
Port Setting	63
Private VLAN	64
MAC/Subnet/Protocol Based VLAN	65
10 QOS	67
Global Configuration	67
Interface	
DSCP	
11 ACL	70
ACL Information	70
ACL Configuration	70
IP ACL	73
Port ACL Setting	74
12 DHCP	75
DHCP Server	75
DHCPv6 Server	
DHCP Relay	77

DHCP Snooping	78
13 NTP	
NTP Configuration	
Daylight Saving Time Setting	
14 SNMP	
SNMP General Setting	
SNMP v1/v2	
SNMP v3	
15 802.1X	
Radius Configuration	
Port Authentication	
16 LLDP	
LI DP General Settings	89
LI DP Port Settings	
LIDP Statistics	90
LLDP Neighbors	
17 Routing	
ARP Table	92
Static Route	
Route Table	93
Route Map.	
Proxy ARP	
VRRP	
18 RIP	
RIP General Setting	99
RIP Port Setting	100
BIP Route	
RIP Network	
RIP Neighbor	
RIP Passive	
RIP Redistribute	

19 OSPF	104
OSPF General Setting	
OSPF Advanced Setting	
OSPF Area Configuration	111
OSPF Interface Configuration	114
OSPF Interface Configuration with Address	116
20 AAA (Authentication, Authorization, and Accounting)	118
TACACS Plus	118
21 ERPS (Ethernet Ring Protection Switching)	119
Acronyms	119
ERPS Sample Configuration – Network Topology	126
ERPS Configuration	127
22 Contact Information	132



1 Introduction

The EX78900G series represents EtherWAN's latest advancement in 2.5G Ethernet switch technology, featuring comprehensive Layer 2 and Layer 3 management functionalities. This 2.5G managed PoE switch, compactly DIN-rail mounted, supports up to 8 gigabit PoE ports, providing a maximum of 90W of PoE power. It adheres to the IEEE 802.3.bt protocol while maintaining compatibility with IEEE 802.3af and IEEE 802.3at standards, allowing for versatile PoE power delivery ranging from 15W, 30W, 60W to 90W per Ethernet port.

Additionally, the switch integrates up to 4 tri-rate 2.5G SFP uplink ports, providing adaptability with triple-speed options of 100Mbps, 1000Mbps, and 2500Mbps for flexible connectivity expansion. The EX78900G series is designed to offer networks in urban infrastructure, transportation, security, and other critical sectors the trifecta of flexibility, speed, and reliability.

Unpacking and Installation

Unpacking

Unpack the items and confirm that no items are missing or damaged. Your package should include:

- EX78900G Ethernet switch with RJ-45/SFP/USB dust covers installed
- 1 RJ-45 Console cable

If any item is damaged or missing, notify your authorized EtherWAN representative. Keep the carton, including the original packing material, in case you need to store the product or return it.

Installing the Switch

- Installation: Din-rail mount.
- Select a power source within 6 feet (1.8 meters).
- Choose a dry area with ambient temperature between -40 and 75°C (-40 and 167°F).
- Keep away from heat sources, sunlight, warm air exhausts, hot-air vents, and heaters.
- Be sure there is adequate airflow.

Connecting to the Data Ports

The EX78900G has the following ports:

- 8 x 1G RJ-45 ports
- 2 or 4 x 100/1G/2.5G tri-rate SFP ports
- 1 x RJ-45 console port
- 1 x USB port

Console Port

The console port uses an RJ-45 interface cable. Pin definitions are as follows:



Pin	Signal	Function
1	NC	Not Connected
2	NC	Not Connected
3	TxD	Transmit Data from Switch
4	GND	Ground
5	GND	Ground
6	RxD	Receive Data to Switch
7	NC	Not Connected
8	NC	Not Connected

Connecting Power

Terminal Block

The switch provides two power inputs on a terminal block. The terminal block has 5 terminal posts, consisting of a primary and secondary source, negative, and a single ground. Redundant power supply is supported. via the secondary source pins. However, only one power input is required to operate the switch. Input voltage is 46-57VDC. (54-57VDC to use IEEE 802.3bt devices).

Relay Output Alarm

The switch provides one dry contact for signaling of a user-defined power or port failure. The alarm relay default is "open" and forms a closed circuit when the event occurs. The relay output can be connected to an alarm signaling device, and supports both normally open and normally closed. Relay output current is 48VDC / 0.5A.

NOTE: The initial normal state of the relay is open, and if the switch loses *all* power, then this state will come into effect. This is important to remember when using the relay to indicate a power failure. The relay will close in an alarm state when there is redundant power input and an alarmed input fails.

Initial Configuration

Serial (RJ45): Connect to the switch using the enclosed console cable via the serial port (or USB to serial adapter) on the PC to the RJ-45 Management port located on the front panel above to the USB port.

Ethernet: Connect to any ethernet port on the switch using a CAT5e or better Ethernet cable with the other end connected to the Ethernet port on your PC. You will need to set the IP address on the PC to a 192.168.1.0/24 address to connect.

For more information on setting up the connection, please refere to the EtherWAN Academy course, *"Managed Switch Basics"* and *"Introduction to EtherWAN Switches."*

Configuration via CLI

If using a terminal-emulation program such as Putty, configuration settings are: Baud rate: 115,200bps, Data bits: 8, Parity: none, Stop bit: 1, Flow control: none.

The default login name is "root," no password.

Configuration via Web Browser

Log in to the switch by launching a web browser and entering 192.168.1.10 in the address bar.

Enter the default login ID: root (no password) and click "Login." The system information screen will display.



- **NOTE**: When logging into the GUI or the CLI for the first time, the switch will prompt you to change the default password to a new one. The new password must meet the following complexity requirements:
- Minimum 8 characters and maximum 35 characters in password length without leading or trailing blanks.
- The password must contain characters from the following categories:
 - 1. Uppercase English letters, (A to Z)
 - 2. Lowercase English letters, (a to z)
 - 3. Numbers, (0 to 9)
 - 4. Non-alphanumeric characters (e.g. @, #, \$), but not including (", ?, !)

User account will be locked after 10 (configurable) password attempts and will stay locked for 5 minutes.

The current password is	a default password.
Please change this pass	word to a more secure value.
Password must have 8	to 35 characters and contain at least one capital letter,
at least one lowercase	letter, at least one number, and at least one special
character aside from t	ne reserved ("), (?), (!).
New Password password	

Reset Button

The switch has a physical reset button, to either just reboot the switch, or reset everything to the factory default configuration.

- To reboot the switch, press and hold the reset button for less than 10 seconds.
- To reset the switch to the factory default configuration, press and hold the reset button for more than 10 seconds.

Copy Configuration to USB

The USB port can be used to upgrade firmware from a FAT32 formatted USB flash drive. Plug the USB device into the USB port, and navigate to **System** \rightarrow **Configuration** in the WebGUI, and type the firmware's <filename>. Or you can use "install image usb <filename>" command in the CLI.

Via USB 🗸	drive
	Via USB drive
Filename	
	Apply

Alternate (Backup) Firmware

Under certain circumstances, such as when there is a loss of power during an upgrade, the firmware build on the switch can become unstable. There are two firmware images stored on the switch: Active and Alternate. If the Active firmware image becomes unstable, the switch

will automatically boot from the Alternate image on the next boot. Navigating System \rightarrow System Information to check Firmware Information.

✓ Firmware Inf	mation	
	Firmware Information	
Active Versio	6.00.1.5 03/08/24 18:13:18	
Alternate Ve	Alternate Version 6.00.0.4 09/01/23 15:48:41	

2 Web Management Interface

About the Web-based graphical user interface (GUI)

The web interface allows for remote monitoring, configuration, and control of the switch through any standard web browser. All switch features that can be configured through the Command Line Interface can also be configured through the GUI.

Default IP Address

The switch's default IP address is **192.168.1.10**. The management computer must be set up so that it is on the same network as the switch. For example, the IP address of the management computer can be set to 192.168.1.100 with a subnet mask of 255.255.255.0. DHCP is disabled by default.

Login Process and Default Credentials

Once a compatible IP address has been assigned to the management computer, the user is ready to log in to the switch. To log in, type the URL http://192.168.1.10/ into the address field of the browser and hit return. (See figure below)

- The Default Login is **root** (case sensitive)
- There is no password by default
- Enter the login name and click the Login button



Login Screen



NOTE: When logging into the GUI or the CLI for the first time, the switch will prompt you to change the default password to a new one. The new password must meet the following complexity requirements:

- Minimum 8 characters and maximum 35 characters in password length without • leading or trailing blanks.
- The password must contain characters from the following categories: •
 - 1. Uppercase English letters, (A to Z)
 - 2. Lowercase English letters, (a to z)
 - 3. Numbers, (0 to 9)
 - 4. Non-alphanumeric characters (e.g. @,#,\$), but not including (", ?, !)

User account will be locked after 10 (configurable) password attempts and will stay locked for 5 minutes.

Navigating the GUI

At the top of every page of the web interface is a panel containing a graphic that shows status of power & ports on the switch, and an alarm indicator.

	System	Gigabit
EX78900G _{Series}	▲ ● ① 1 ● ② 2 ●	$1 \bullet 5 \bullet 9 \bullet$ $2 \bullet 6 \bullet 10 \bullet$ $3 \bullet 7 \bullet 11 \bullet$ $4 \bullet 8 \bullet 12 \bullet$

On the left side of the page is the navigation panel. Each section can be expanded and collapsed to view or hide the page headings within. At the top of the navigation panel is a search box, which can be used to quickly find a specific page in the GUI. Note that the search box works best with specific terms like "MSTP." Generic search terms like "Setting" will yield many results, and it may be difficult to quickly identify the specific setting page needed.

Search for	x
System	\odot
Diagnostics	\odot
Port	\odot
Switching	\odot
IGMP	\odot
STP	\odot
VLAN	\odot
QOS	\odot
ACL	\odot
DHCP	\odot
NTP	\odot
SNMP	\odot
802.1X	\odot
LLDP	\odot
Routing	\odot
RIP	\odot
RIPng	\odot
OSPF	\odot
OSPFv3	\odot
PIM	\odot
AAA	\odot

Icons

The GUI uses a few simple icons to for viewing and editing switch configuration data.



Refresh the panel



Edit data in panel



Add a new entry to the panel (Example: Add a new static route)

3 System Menu

System Information

When you log into the switch GUI, you will be taken to the system information page. This is a read-only page with three panels. The first panel shows basic system info:

ystem Information		
 System Information 		
	•	
	System Information	
System Name	switch	
System Time	Sun Jan 01 21:15:13 UTC 2017	
System Uptime	8 min	
System MAC	00e0.b311.3361	
Serial Number	G231100117	
Firmware Version	6.00.1.5 03/08/24 18:13:18	
Management IP	192.168.1.10	
CPU Utilization	16%	

The second panel shows the active and alternate firmware versions.

 Firmware Information 		
		Ø
	Firmware Information	
Active Version	6.00.1.5 03/08/24 18:13:18	
Alternate Version	6.00.0.4 09/01/23 15:48:41	

The third panel shows the MAC address of each port on the switch.

MAC Address	
	0
Interface	MAC Address
ge1	00e0.b311.3367
ge2	00e0.b311.3368
ge3	00e0.b311.3369
ge4	00e0.b311.336a
ge5	00e0.b311.336b

System Name

To change the system name, click the edit icon and enter a name in the field shown. The name may not contain spaces. Maximum length is 64 characters.

System Name		
✓ System Name		
		Ø Ø
	<u>c</u>	iystem Name
System Name	switch	

System Password

By default, there is no password assigned to the switch. To set a password, enter it into both fields and click "Apply."

System Password		
	Change Password	
New Password	Show	
Confirm Password	Show	
Cancel	3101	

IP Address

The two panels on this page allow for the changing of the IP address of VLAN 1, configuration of DHCP client information, and for the creation of default gateways. Enter/delete DNS Server addresses at the bottom of this screen.

 ✓ Static IP ✓ LAN ID IP Address Edit 1 192.168.1.10/24 Io IP ✓ Io IP ✓ Io IP ✓ OIP ✓ Apply Cancel ✓ DHCP Client ✓ DHCP Client ✓ Interface IP Address Subnet Mask Default Gateway DNS Server Edit
VLAN ID IP Address Edit 1 192.168.1.10/24 - Image: Instant of the second s
VLAN ID IP Address Edit 1 192.168.1.10/24 □
1 192.168.1.10/24 ✓ lo IP
 ✓ Io IP Io ip address Edit 127.0.0.1/8 □ ✓ Apply Cancel ✓ DHCP Client ✓ DHCP Client ✓ Interface Request IP Address Subnet Mask Default Gateway DNS Server Edit
Io ip address Edit 127.0.0.1/8 □ ✓ DHCP Client ✓ DHCP Client Interface Request IP Address Subnet Mask Default Gateway DNS Server Edit
Io ip address Edit 127.0.0.1/8 □ ✓ Apply Cancel
127.0.0.1/8 □ ✓ Apply Cancel ✓ DHCP Client ✓ Interface Request IP Address Subnet Mask Default Gateway DNS Server Edit
✓ Apply Cancel ✓ DHCP Client ✓ Interface Request IP Address Subnet Mask Default Gateway DNS Server Edit
✓ DHCP Client Interface Request IP Address Subnet Mask Default Gateway DNS Server Edit
Interface Request IP Address Subnet Mask Default Gateway DNS Server Edit
Disable
✓ Default Gateway
Default Gateway IP Edit
V DNS Server
Ø ⊘ ⊕
Server IP Edit

IPv6 Address

On this screen, you can add IPV6 addresses to an interface, static IPV6 addresses, and DHCPv6 Client information.

IPv6 Addres	S			
✓ Add IPv6 Addres	SS			
			Add IPv6 Address	
Interface		vlan1.1 🔻		
IPv6 Address/P	refix	2001:0db8:85a3:0	000:0	
			Apply	
✓ Static IPv6 Addr	ess			
				Θ
Edit	Interfa	ce	IPv	6 Address
	lo			
				::1/128
	vlan1.	1		
			2001:db8:85a	3::8a2e:370:7334/64
	vlan1.	2		
			2001:620	:40b:555::210/64
✔ DHCPv6 Client				
				0
Edit		Interface	Request	IPv6 Address
		Disable		

System Time

This page is for manual setting of the system time. Click the edit icon, and enter the time and date data in the corresponding fields. Click "Apply" when finished. To configure a network time server, refer to the <u>NTP</u> chapter.

System T	ime	
✓ System Tin	ne	•••
		<u> </u>
	System Time	
Year	2017	
Month	05	
Day	05	
Hour	13	
Minute	22	
Second	52	

Management Interface

Enable / disable access to switch management through http, Telnet, and SSH on this page. Note that if you disable http without enabling https you will lose access to the GUI and need to use another management method to access the switch to save changes.

Management Interface		
 Management Interface 		
		00
	Management Interface	
WEB Agent	HTTP	
Consecutive Login Failure Checking	Disabled	
	Note: HTTPS can encrypt data and ensure data transmission security.	
Update HTTPS Key	Generate	
	Note: Please reload the page after generating new keys.	
Telnet	Enabled	
SSH	Disabled	

Warning! Enabling HTTP may lead to potential security vulnerabilities. Therefore, it is suggested to only enable HTTPS.

Configuration

This page is comprised of three panels. The first is for setting auto-save interval of the switch configuration. Auto-save is disabled by default.

onfiguration		
 Auto Save Configuration 		0 0
	Auto Save Configuration	
Auto Save	Disabled	

Saving Switch Configuration

The second panel is for saving the current switch configuration, and resetting the switch configuration to factory default. A confirmation message will display if the second option is chosen.

✓ Configuration		
	Configuration	
Save Configuration	Apply	
Restore Default	Apply	

Load a switch configuration from, or save a configuration to, a TFTP server or USB flash drive using the third panel. Path and port fields are optional.

	Save/Load Configuration File
Action	●Save ◎Load
via	®TFTP ◎USB
Filename	
TFTP Server IP	
Path (Optional)	
Port (Optional)	

Firmware Upgrade

Firmware can be upgraded from either a TFTP server or from any drive that is accessible to the web browser. The firmware file for the switch should be in ".XZ" format and is downloadable from the product page on <u>www.etherwan.com</u>.

Firmware Upgra	ade		
✓ Via TFTP Server			
		Vi	a TFTP Server
Filename			
TFTP Server IP			
			☑Apply
✓ Via SFTP Server			
		Vi	a SFTP Server
Username			
Password			
Filename			
SFTP Server IP			
			☑Apply
✓ Via USB drive			
		١	/ia USB drive
Filename			
			☑Apply
✔ Via web			
Please select new f	firmware file:		
選擇檔案 未選擇任何	檔案	Upload file	

To upgrade the switch firmware:

- 1. Log in to the switch and navigate to System \rightarrow Firmware Upgrade.
- 2. Upgrade Methods:
 - a. TFTP: Enter the filename and TFTP server address and click "Apply"
 - b. SFTP: Enter the username, password, filename and SFTP Server IP and click "Apply"
 - c. Web: Select the fiile manually with the **Choose File** button and click "Upload File"

- 3. It will take several minutes to install the new firmware.
- 4. Click the **Reboot** button when you see the message "Firmware upgrade successful." (Do not power off the switch or the firmware upgrade will fail)
- 5. Wait 90 seconds (60 seconds for switch reboot, and 30 seconds for system verification) and re-log in to the switch. Check the System Information screen to ensure that the firmware upgrade has been successful.

Reboot

Reboot the switch.

Reboot		
Reboot		

User Account

From the User Account page, multiple users can be setup with different access privileges to the switch. There are three modes that can be set using the drop-down menu, Single-User, Multi-User, RADIUS or TACACS+.

New user accounts can be added and deleted in the bottom section. Usernames can only contain alphanumeric characters.

Passwords must have 8 to 35 characters and contain at least one capital letter, at least one lowercase letter, at least one number, and at least one special character aside from the reserved ("), (?), (!).

User Acc	count		
🗸 Login Mo	ode		
			00
		Login Mode	
Mode	Single-user 🗸		
	Single-user Multi-user RADIUS TACACS+	⊘ Apply Cancel	
VUser Acco	ount		● Ø Ð
	User Name	Privilege Level	Edit

Command Privilege

There are 3 different Privilege levels on the EtherWAN Managed Switch.

- Admin Has access to all configuration and administration of the switch.
- **Technician** Configurable by Admin By default no configuration ability is given.
- **Operator** Configurable by Admin By default no configuration ability is given.

The User Privilege Configuration page allows specific configuration and/or administration levels to be assigned or removed from the Technician and Operator user roles. The privilege levels are: **Show**, **Hidden**, **Read-Only**, and **Read-Write**.

NOTE: For each function, an Operator's privilege cannot be higher than a Technician's.

Command Privilege

✓ Command Privilege

Command Group	Technician	Operator	Edit
System-Name&Password	Hide	Hide	
IP-Address	Read-only	Read-only	
Management-Interface	Read-only	Read-only	
Save-Configuration	Hide	Hide	
Firmware-Upgrade	Hide	Hide	
Reboot	Hide	Hide	
User-Account	Read-only	Read-only	
Command-Privilege	Read-only	Read-only	
Utilization	Read-write	Read-write	
RMON-Statistics	Read-only	Read-only	
Remote-Log	Read-only	Read-only	
Alarm-Setting	Read-only	Read-only	
Port-Mirroring	Read-only	Read-only	
Email-Alert	Read-only	Read-only	
Configuration	Read-only	Read-only	
Flow-Control	Read-only	Read-only	
Rate-Control	Read-only	Read-only	
Static-MAC-Entry	Read-only	Read-only	
Port-Trunking	Read-only	Read-only	
LACP-Trunking	Read-only	Read-only	
GVRP	Read-only	Read-only	
GMRP	Read-only	Read-only	
VLAN-Translation	Read-only	Read-only	
IGMP	Read-only	Read-only	
IGMP-Snooping	Read-only	Read-only	
STP	Read-only	Read-only	
VLAN	Read-only	Read-only	
QOS	Read-only	Read-only	
ACL	Read-only	Read-only	
DHCP	Read-only	Read-only	
NTP	Read-only	Read-only	
SNMP	Read-only	Read-only	
802.1X	Read-only	Read-only	
LLDP	Read-only	Read-only	
Static-Route	Read-only	Read-only	
Route-Map	Read-only	Read-only	
Proxy-ARP	Read-only	Read-only	
VRRP	Read-only	Read-only	
RIP	Read-only	Read-only	
OSPF	Read-only	Read-only	
PIM	Read-only	Read-only	
TACACS-Plus	Read-only	Read-only	
Configure-terminal	Read-write	Read-only	

00

4 Diagnostics Commands

System Utilization

The System Utilization page is a read-only page for viewing the current CPU and memory utilization levels. The first panel shows utilizations as a percentage, and the second panel shows the total memory, amount used, amount free, and amount cached.

	tilization		
CPU Utiliza	ition		
		CPU Utilization	
Current ut	ilization	%	
Max utiliza	tion	7%	
• Memory U	tilization		
Memory U	tilization	Memory Utilization	
 Memory U Total 	tilization 1029716	Memory Utilization	
 Memory U Total Used 	tilization 1029716 377152	Memory Utilization	
Memory U Total Used Free	tilization 1029716 377152 652564	Memory Utilization	

Below there are real-time graphs of CPU and memory usage. Mouse over any point on these graphs to see detailed information.





System Log

The System Log shows the data and time of system events, such as port links going up or down.

Sy	System Log		
	 System Log 		
		0	
	Index	Log	
	1	<13>Jan 1 21:06:33 switch EW: Link down on Port ge5	
	2	exec: No such file or directory	
	3	<13>Jan 1 21:06:33 switch EW: Link down on Port ge7	
	4	exec: No such file or directory	
	5	<13>Jan 1 21:06:33 switch EW: Link down on Port ge8	
	6	exec: No such file or directory	
	7	<13>Jan 1 21:06:33 switch EW: Link down on Port ge6	
	8	exec: No such file or directory	
	9	<13>Jan 1 21:06:33 switch EW: Link down on Port ge1	
	10	exec: No such file or directory	
	11	<13>Jan 1 21:06:33 switch EW: Link down on Port ge3	

RMON Statistics

RMON Statistics gives a detailed listing of the types and quantity of packets that a particular port has seen since the last reboot of the switch.

RM	ON Statistics	
~	RMON Statistics	
Ро	rt ge1 🗸	U
	Port RMON Statistics	
		Port RMON Statistics
	Drop Events	0
	Multicast Packets Received	178
	Broadcast Packets Received	31
	Undersize Packets Received	0
	Fragments Packets	0
	64-byte Packets Received	902
	65 to 127-byte Packets Received	429
	128 to 255-byte Packets Received	165
	256 to 511-byte Packets Received	32
	512 to 1023-byte Packets Received	627
	1.0 to Maximum Packets Received	0
	Oversize Packets Received	0
	Jabber Packets	0
	Bytes Received	513311
	Packets Received	2155
	Collisions	0
	CRC/Alignment Errors Received	0
	TX No Errors	4491
	RX No Errors	2155
	Clear Counters	Clear

Remote Log Setting

Remote Logging to a Syslog server allows administrators to log important system and debugging information. The Remote Logging configuration page allows reporting to a Syslog server to be enabled or disabled as well as management of a list of Syslog servers to report to. Enable or disable remote logging in the top panel, and use the bottom panel to add, edit, or delete log server IP addresses.

Remote	Log Setting		
✔ Remote L	ogging		00
		Remote Logging	
Status	Enabled		
✓ Log Serve	r IP List		
			0 🕀
	Edit	Log Server IP	
		192.168.1.75	

Alarm Setting

1

Alarms can be set for a variety of general switch conditions including link down and redundant power failure. When equipped with a DDM (Digital Diagnostics Monitoring) compatible SFP module, major and minor alarms can also be set for SFP voltage, power, and TX bias. By default, alarms are sent to the system log, and displayed on the top panel of the web interface. Alarms can also be sent as SNMP traps to an SNMP server. External alarm devices can be configured using the <u>relay output alarm</u>.

NOTE: To configure specific threshold values for DDM SFP alarms, you must use the command line interface (CLI).

The Alarm Setting page is divided into four sections, accessible by tabs at the top of the page.

In the first section, **Basic** alarms can be set for failure on any port, and either power input (if dual power inputs are used).

Alarm Setting				
Basic	SFP	SFP RX	SFP TX	

Port	Enabled	Status	Edit
ge1	No 🛩	Link-up	Cancel
ge2	No	Link-down	
ge3	No	Link-down	
ge4	No	Link-down	
ge5	No	Link-down	
ge6	No	Link-down	
ge7	No	Link-down	
ge8	No	Link-down	
ge9	No	Link-down	
ge10	No	Link-down	
ge11	No	Link-down	
ge12	No	Link-down	
rm Trigger Power			
Power	Enabled	Status	Edit
Dowor1	No	Un	

To set a link-down alarm check the box next to a port, and click "Apply"

Panels on the second tab panels allow for setting of major and minor alarms for SFP voltage.



✓ Alarm Trigger SFP Temperature Major

PORT	Enabled	Status	Edit
ge9	No	Temper:SFP Module none detect (Major)	
ge10	No	Temper:SFP Module none detect (Major)	
ge11	No	Temper:SFP Module none detect (Major)	
ge12	No	Temper:SFP Module none detect (Major)	

00

✔ Alarm Trigger SFP Temperature Minor

			00
PORT	Enabled	Status	Edit
ge9	No	Temper:SFP Module none detect (Minor)	
ge10	No	Temper:SFP Module none detect (Minor)	
ge11	No	Temper:SFP Module none detect (Minor)	
ge12	No	Temper:SFP Module none detect (Minor)	

✓ Alarm Trigger SFP Vcc Major

			00
PORT	Enabled	Status	Edit
ge9	No	Vcc:SFP Module none detect (Major)	
ge10	No	Vcc:SFP Module none detect (Major)	
ge11	No	Vcc:SFP Module none detect (Major)	
ge12	No	Vcc:SFP Module none detect (Major)	

✔ Alarm Trigger SFP Vcc Minor

PORT	Enabled	Status	Edit
ge9	No	Vcc:SFP Module none detect (Minor)	
ge10	No	Vcc:SFP Module none detect (Minor)	
ge11	No	Vcc:SFP Module none detect (Minor)	
ge12	No	Vcc:SFP Module none detect (Minor)	

On the third tab are panels to set major and minor alarms for RX power. This is the optical power ratio received in decibels (dB).



✓ Alarm Trigger SFP RX-Power Major

			00
PORT	Enabled	Status	Edit
ge9	No	Rx Power:SFP Module none detect (Major)	
ge10	No	Rx Power:SFP Module none detect (Major)	
ge11	No	Rx Power:SFP Module none detect (Major)	
ge12	No	Rx Power:SFP Module none detect (Major)	

✓ Alarm Trigger SFP RX-Power Minor

Edit

ge9	No	Rx Power:SFP Module none detect (Minor)	
ge10	No	Rx Power:SFP Module none detect (Minor)	
ge11	No	Rx Power:SFP Module none detect (Minor)	
ge12	No	Rx Power:SFP Module none detect (Minor)	
The fourth tab contains panels for setting major and minor alarms for TX Bias and TX Power. TX Bias is the transmit bias power signal, in milliamperes (mA). TX Power is the transmit power signal, in decibels (dB).

Alarm Setting								
Basic	SFP	SFP RX	SFP TX					

✓ Alarm Trigger SFP TX-Bias Major

			00
PORT	Enabled	Status	Edit
ge9	No	Tx Bias:SFP Module none detect (Major)	
ge10	No	Tx Bias:SFP Module none detect (Major)	
ge11	No	Tx Bias:SFP Module none detect (Major)	
ge12	No	Tx Bias:SFP Module none detect (Major)	

✓ Alarm Trigger SFP TX-Bias Minor

PORT	Enabled	Status	Edit
ge9	No	Tx Bias:SFP Module none detect (Minor)	
ge10	No	Tx Bias:SFP Module none detect (Minor)	
ge11	No	Tx Bias:SFP Module none detect (Minor)	
ge12	No	Tx Bias:SFP Module none detect (Minor)	

00

✓ Alarm Trigger SFP TX-Power Major

_			00
PORT	Enabled	Status	Edit
ge9	No	Tx Power:SFP Module none detect (Major)	
ge10	No	Tx Power:SFP Module none detect (Major)	
ge11	No	Tx Power:SFP Module none detect (Major)	
ge12	No	Tx Power:SFP Module none detect (Major)	

✓ Alarm Trigger SFP TX-Power Minor

			00
PORT	Enabled	Status	Edit
ge9	No	Tx Power:SFP Module none detect (Minor)	
ge10	No	Tx Power:SFP Module none detect (Minor)	
ge11	No	Tx Power:SFP Module none detect (Minor)	
ge12	No	Tx Power:SFP Module none detect (Minor)	

Port Mirroring

To configure port mirroring, click the add icon, and enter the **From** and **To** ports. Select the desired mode: transmit (mirror transmits traffic), receive (mirror receives traffic), or both (traffic is mirrored in both directions).

Port mirroring can only be configured on interfaces of the same type, e.g., only a switchport interface can mirror a switchport interface. Issuing a switchport command on a port where mirroring is enabled will remove port mirroring on that interface.

Port Mirroring		
From	То	Mode
ge1 🔻	ge1 🔻	both 🔻
	Cancel	
		4

Existing mirrors can be viewed and deleted from the initial page.

Po	Port Mirroring								
~	 Port Mirroring 								
				⊕ ⊘ ⊕					
	From	То	Mode	Edit					
	ge1	ge3	both						
	ge12	ge9	receive						

Email Alert

The switch can send email alerts to up to three recipients when an environmental alarm is triggered.

To enable email notifications, click the edit button and set the SMTP Status to enable.

To configure mail server and recipient email addresses:

- 1. Enter the name of the SMTP server to be used in the corresponding field, and the server port.
- 2. Enter the email address of the sending account.
- 3. Enter the password for the email account being used, and select Enable or disable for SSL (Secure Sockets Layer) Status.
- 4. Click the Update button.

NOTE: If SSL is disabled, port 25 will be used to send email. If SSL is enabled, port 465 will be used.

You can view, add, and delete email recipients in the fields at the bottom of the page. Only one email address can be added at a time.

Email Alert		
✔ Mail Server		00
	Mail Server	
SMTP Status	Disable	
SMTP Server		
Email Address		
Password		
SSL Status	Disable	
Delete Server configuration	Delete	
V Mail Recipients		
•		0
Edit	Recipients Mail Address (Max number: 5)	

Port Configuration

Port configuration contains features as flow control, port speed, and duplex settings. These settings can be very useful when the switch is connected to a latency-critical device such as a VOIP phone, IP camera, or video multiplexor. The ability to alter port settings can make the difference between a poorly responding device and one that functions without loss of data or clarity.

rt (Configu	ration							
GE F	Port Configur	ation							
									0
	Port Type	IP Address	Link Status	Shutdown	Port Description	Speed/Duplex	Mtu		
e1	Switch port		Down	No		Auto	12288	Disable	
e2	Switch port		Down	No		Auto	12288	Disable	
e3	Switch port		Down	No		Auto	12288	Disable	
e4	Switch port		Running	No		Auto	12288	Disable	
e5	Switch port		Down	No		Auto	12288	Disable	
e6	Switch port		Down	No		Auto	12288	Disable	
e7	Switch port		Down	No		Auto	12288	Disable	
e8	Switch port		Down	No		Auto	12288	Disable	
GE S Port	SFP Port Con Port Type	figuration IP Address	Link Status	Shutdown	Port Description	Speed/Duplex	Mtu		C Q
ge9	Switch port		Down	No		Auto	12288		
, e10	Switch port		Down	No		100M/FD	12288		
e11	Switch port		Down	No		Auto	12288		
- 1 2	Switch port		Down	No		250014/50	40000		

The **Configuration** page shows (see figure below):

- 1. Port Type Routed port or Switch port
- 2. IP address For routed ports only, aaa.bbb.ccc.ddd/mm format
- 3. Link Status Operational State of the Port's Link (Read-Only)
- 4. Shutdown Shutdown state
- 5. Port Description User-supplied description, 80 characters maximum

- 6. Duplex / Speed Click on the drop-down box under Speed/Duplex and select the desired port speed / duplex settings for that port.
 - For 10/100/1000 TX ports Have five options: Auto, 100M/FD, 100M/HD, 10M/FD, 10M/HD.
 - For 100/1000/2500 SFP ports Have three options: Auto, 100M/FD, 2500M/FD. Note that the default seting is Auto, and it is running at a fixed speed 1000M.

NOTE: It is recommended to manually select the speed required instead of using the Auto option.

7. EEE (Energy-Efficient Ethernet) – EEE reduces the switch's power consumption during periods of low activity. EEE is disabled by default.

Click the check box to modify the settings for a port and click "Apply" when finished.

Port Status

1

This is a read-only page that lists the settings described in the previous section.

t Sta	atus							a
ort	Link Status	Port Description	Port Type	IP Address	Speed	Duplex	Mtu	EEE
ge1	Down		Switch port		1G		12288	Disable
ge2	Down		Switch port		1G		12288	Disable
ge3	Down		Switch port		1G		12288	Disable
ge4	Running		Switch port		1G	Full	12288	Disable
ge5	Down		Switch port		1G		12288	Disable
ge6	Down		Switch port		1G		12288	Disable
ge7	Down		Switch port		1G		12288	Disable
ge8	Down		Switch port		1G		12288	Disable
ge9	Down		Switch port		1G		12288	Disable
ge10	Down		Switch port		100M		12288	Disable
ge11	Down		Switch port		1G		12288	Disable
ge12	Down		Switch port		2.5G		12288	Disable

SFP Port	Connector		Mode		Link Length (m)	Temperature (C)		Tx Bias (mA)	Tx Pow (dbm)	Rx Pow (dbm)
ge9	NONE	NONE	NONE	NONE	NONE	None	None	None	None	None
ge10	LC	100BASE-FX	MMF	1310	2000	37.391	3.284	13.250	-15.258	-40.000
ge11	LC	1000BASE-SX	MMF	850	550	51.109	3.215	3.968	-6.164	-40.000
ge12	LC	2.5GBASE-X	OM4	850	500	47.484	3.326	5.612	-3.215	-40.000

Flow Control

Flow Control

Flow control allows switches of different speeds to communicate. When enabled, the lower speed switch can request that the higher speed switch refrains from sending packets. Transmissions are temporarily halted to prevent overflows. Flow control in enabled by default on all ports.

When enabling or editing flow control on a port, click the check box next to the port, then set the **Send Admin** and **Receive Admin** fields to **on** or **off**, enabling or disabling the port's ability to send and receive flow control administrative requests. Then click "Apply."

✓ Port F	✓ Port Flow Control									
					00					
Port	Send Admin	Send Operation	Receive Admin	Receive Operation	Edit					
ge1	off	off	off	off						
ge2	off	off	off	off						
ge3	off	off	off	off						
ge4	off	off	off	off						
ge5	off	off	off	off						
ge6	off	off	off	off						
ge7	off	off	off	off						
ge8	off	off	off	off						
ge9	off	off	off	off						
ge10	off	off	off	off						
ge11	off	off	off	off						
ge12	off	off	off	off						

Rate Control

Rate control forces a port to drop packets when an ingress / egress rate limit has been exceeded. Click on the check box next to a port, and enter the limits for **Ingress Rate in Kbps**, **Ingress Burst Size in Kbits**, **Egress Rate in Kbps**, and **Egress Burst Size in Kbits**. Then click "Apply."

To disable Rate Control on a port, set all values to zero.

Rat	e Control				
v	Port Rate Control				
					0 📀
Po	ort Ingress Rate in Kbps (1- 1000000), 0 to disable	Ingress Burst Size in Kbits (2-1048576), 0 to disable	Egress Rate in Kbps (1- 1000000), 0 to disable	Egress Burst Size in Kbits (2-1048576), 0 to disable	Edit
g	e1 0	0	0	0	
g	2 0	0	0	0	
g	93 0	0	0	0	
g	94 0	0	0	0	
g	95 0	0	0	0	
g	96 0	0	0	0	
g	27 0	0	0	0	
g	8 0	0	0	0	
g	9 0	0	0	0	
ge	10 0	0	0	0	
ge	11 0	0	0	0	
ge	12 0	0	0	0	

6 Switching

MAC Table

The MAC Table page contains a panel for setting the Ageing Time, one for clearing Dynamic, Mulitcast, and Static MAC addresses, and a read-only panel for viewing the current MAC Table. Change the Ageing time (the time that a networked device's MAC address will live in the switch's memory before being removed) by clicking the edit icon, and entering the desired Ageing Time in seconds. Then click "Apply."

MAC Table			
✓ Ageing Time			
			0 0
		Ageing Time	
Ageing Time (10-1000000)	300		
		Clear MAC	•
Clear Dynamic MAC	Clear		
Clear Multicast MAC	Clear		
Clear Static MAC	Clear		

MAC Table				
Index	VLAN	MAC Address	Туре	Ports
1	1	00e0.b33f.208e	dynamic	ge11
2	1	00e0.b33f.209d	dynamic	ge11
3	1	3065.ec91.9820	dynamic	ge13

Static MAC Entry

Static MAC Entry Forward allows you to specify a MAC address on a particular port and VLAN rather than adjusting the ageing time for the entire switch. Alternatively, you can prevent a MAC address from ever being registered with a switch by using **Static MAC Entry Discard**.

St	atic M	AC En	try		
~	Static MA	C Entry Fo	rward		
					() ()
1	Index	Port	MAC Address (Ex: 0000.1111.2222)	VLAN	Edit
	1	ge1	00e0.b33f.208e	1	
~	Static MA	C Entry Di	scard		0 0
Ī	Index		MAC Address (Ex: 0000.1111.2222)	VLAN	Edit

Storm Control

Set the rising threshold level for broadcast, multicast, or destination lookup failure traffic. The storm control action occurs when traffic utilization reaches the set level. Storm control blocks the forwarding of unnecessary flooded traffic.

To enable Storm Control on a port, select it by clicking the check box on the left. Then enter values for:

Broadcast Threshold Level: Broadcast rate limiting, based on percentage of the maximum speed (in packets per second) of the interface

Multicast Threshold Level: Multicast rate limiting, based on percentage of the maximum speed (in packets per second) of the interface

DLF Threshold Level: Destination lookup failure, based on percentage of the maximum speed (pps) of the interface

Broadcast Packet-per-second: Broadcast rate limiting, based on total number of packets **Multicast Packet-per-second**: Multicast rate limiting, based on total number of packets **DLF Packet-per-second**: Destination lookup failure, based on total number of packets

Sto	orm	n Control						
~	Stor	m Control (Thresh	old Level:0.01~100) Packet-per-sec	ond: 0~8388608)			00
	Port	Broadcast Threshold Level	Multicast Threshold Level	DLF Threshold Level	Broadcast Packet-per- second	Multicast Packet-per- second	DLF Packet- per-second	Edit
	ge1	100.00	100.00	100.00	0	0	0	
	ge2	100.00	100.00	100.00	0	0	0	
	ge3	100.00	100.00	100.00	0	0	0	
	ge4	100.00	100.00	100.00	0	0	0	

Storm Detect

Storm Detect can disable a port that is receiving excessive Broadcast and/or Multicast packets. The switch can be configured to take action based on percentage of bandwidth utilization or number of packets per second.

To enable Storm Detect globally, click the edit icon and then **Enable**. Then set the Storm Detect **interval** to a value between 2 and 65535 seconds. Set the **errdisable-recovery time** to value between 0 and 65535 seconds.

Storm Detect	
✓ Configuration	
	0
Config	guration
Storm-Detect Configuration	○Enabled ●Disabled
Interval (265535 sec), Default: 10	10
Errdisable-recovery time (065535 sec), 0: no recovery	0
⊘ Apply	Cancel

Configure the Storm Detect parameters for each port by clicking on the check box and entering values for:

By Utilization: Percentage of port's maximum speed By Broadcast / Multicast+Broadcast: Type of packet to be monitored Packets Per Second: Threshold for Storm Detect activation ✓ Storm Detect Per Port

Port	State / Recovery time remains	By Utilization(%) (0-100) 0: not limited	By Broadcast / Multicast+Broadcast	Packets Per Second (0- 100000) 0: not limited	Edit
ge1		0	bc	0	
ge2		0	bc	0	
ge3		0	bc	0	
ge4		0	bc	0	
ge5		0	bc	0	

00

Trunking

The switch supports Static Channel Trunking for up to 12 trunks. To add a trunk, click the add icon in either the **Static Trunk** or **LACP Trunk** section, and then select the ports to be added. Then click "Apply."

Static Ti	unk
Port	Member
	□ge1 □ge2 □ge3 □ge4 □ge5 □ge6 □ge7 □ge8 □ge9 □ge10 □ge11 □ge12
	A

LACP Trunking

The Link Aggregation Control Protocol (LACP) provides a method to control the bundling of several physical ports together to form a single logical channel. LACP allows a device to negotiate an automatic bundling of links by sending LACP packets to the peer (directly connected device that also implements LACP). This means that both sides of the LACP channel must be configured for LACP which implies both devices must support it.

The LACP system priority is used with the MAC address of the switch to create a system ID and to negotiate with other switches. A higher number means a lower priority.

LACP port priority is set on each LACP port. The port priority is used with the port number to create the port identifier. The port priority determines which ports will be put in standby mode when aggregation for all ports is impossible.

LACP Trunking		
✔ LACP Configuration		
		0 📀
L	_ACP Configuration	
LACP System Priority (1-65535, default:32768)	32768	
Port Status Port Trunk Port LACP Mode LACP Port Priority (Set 0 feedback)	or None) LACP Timeout LACP Sync	Ø 🕑

GVRP

GVRP is used to dynamically create VLANs on a switch. Any IEEE 802.1Q compliant switch must implement this protocol.

To enable GVRP, click the edit icon and then the radio button next to **GVRP** and/or **Dynamic VLAN Creation**. Then add a GVRP port by clicking the add icon, and selecting the desired port, **normal** or **active** status for the Applicant, and **normal**, **fixed**, or **forbidden** for Registration.

GVRP			
✔ GVRP			0
		GVRP	
GVRP	Disabled		
Dynamic VLAN Creation	Disabled		
✓ GVRP Port			€
Edit Po	rt	Applicant	Registration

G	VRP Port		
	Port	Applicant	Registration
	ge1 🛩	Normal 🗸	Normal 🗸
-			
		Apply Cancel	

Add GVRP Port

GMRP

The settings in the GMRP feature controls how the switch automates the process of multicast packet forwarding, both within a single switch as wells as between switches in a bridged network. With the GMRP feature enabled, when the switch receives any GMRP multicast group registration requests from either a multicast client or a neighbor switch, the switch will register these multicast groups on these ports and will only transmit the multicast packets that belong to these groups to these ports. The switch will also automatically propagate these multicast group registrations onto the neighbor switches to allow the neighbor switches to forward the multicast packets that belong to these groups to these groups to these groups to the belong to the neighbor switches to allow the neighbor switches to forward the multicast packets that belong to these groups to the belong to

The ports on the EtherWAN switch can be configured with the GMRP feature in five modes:

- Normal
- Fixed
- Forbidden
- Restricted

GMRP Forward All can be enabled or disabled when configuring GMRP ports.

iMRP			
GMRP			
			00
		GMRP	
GMRP	Enabled		
GMRP Port C	Configuration		
Edit	Port	GMRP Registration	GMRP Forward All
GMRP Port Co	onfiguration		
100	Port	GMRP Registration	GMRP Forward All
g	e1 🔻	Normal 🔻	Disabled 🔻
		Normal Fixed Forbidden	
		Restricted Cancel	

VLAN Translation

In VLAN translation, a VLAN tag is removed from an Ethernet frame and rewritten to a different VLAN. This effectively "translates" the frame from one VLAN ID to another. This can be very useful when merging two networks in which the same VLAN is used by both.

To enable VLAN translation, click the edit icon and then click the radio button next to enable.

VLAN Translatio	1						
VLAN Translation Global Setting							
		00					
VLAN Translation Global Setting							
Vlan Translation	Enabled						

To add a new translation entry, click the add icon. Select the port, and whether the translation is to take effect on packet **ingress** or **egress**. Then enter the corresponding VLAN IDs in the **Translate from** and **Translate to** fields. Then click "Apply."

VI	AN Translation			
	Port	Ingress/Egress	Translate from	Translate to
	ge1 🗸	ingress 🗸	23999	23999
			⊘ Apply X Cancel	
				h

ΡοΕ

The PoE page provides access to PoE System Setting information and PoE Port configuration. The System Setting information:

- 1. Main Supply Voltage
- 2. System Temperature
- 3. Power Consumption Actual wattage supplied to attached PoE device(s)
- 4. System Power Budget The maximum and default values

P	PoE											
-	✓ PoE System Setting											
			Ð									
		PoE System Setting										
	Main Supply Voltage	48.00 (V)										
	System Temperature	40 (C)										
	Power Consumption	2.00 (W)										
	System Power Budget	480 (W)										
	Firmware Version	3.5.5										

The PoE Port Configuration section provides the following configurable settings and information:

V Pol	V PoE Port Configuration													
Port	Enable Mode	Extend Mode	Force Power	Fixed Power Limit	Power Priority	Power Down Alarm (W)	Status	PD Class	Current (mA)	Consumption (W)	Edit			
ge1	Enable	Disable	Disable	30W	High	Disable	Searching	N/A	0	0				
ge2	Enable	Disable	Disable	30W	High	Disable	Delivering Power	3	44.00	2.10				
ge3	Enable 🗸	Disable 🗸	Disable 🗸	30W 🗸	High 🗸	Disable 🗸	Searching	N/A	0	0	G Apply X Cancel			
ge4	Enable	Disable	Disable	30W	High	Disable	Searching	N/A	0	0				

- 1. **Enable Mode** Set the PoE Enable Mode by selecting one of the following settings in the drop-down box under PoE Mode
 - Enable Enable PoE on a specific port
 - Disable Disable PoE on a specific port
 - Scheduling Schedule time of day that PoE will be enabled per port
- 2. **Extend Mode** This allows the port to deliver PoE power up to 250 meters at a speed of 10Mbps.

NOTE: It is suggested to pre-test the function before deployment. The maximum available transmission distance of PoE depends on the negotiation result of PD and PSE. Some PDs using EtherWAN PoE/PSE switches may only support a standard distance of 100 meters. Contact EtherWAN if assistance is needed. The input power voltage from the switch must be at least 57 volts to make PoE Extend Mode work.

6

1

NOTE: If PoE extend mode is enabled, **EEE** and **auto-negotiation** of the port will be disabled, instead, the port will be set at full duplex. Only 10Mbps speed is available if this feature is enabled.

- 3. **Force Power** If enable Force Power on a specific port, the port will supply power to the connected PD without any detection or negotiation.
- Fixed Power Limit Provides a fixed maximum Wattage to the attached PoE (PD) device. Use the Drop-Down box to set 15W (2 pairs), 15W, 30W (2 pairs), 30W, 60W, 60W Pre-BT, or 90W.



NOTE. PoE port's fixed power setting restrictions:

(1). Total PoE power budget for the entire system:

- 480 Watts for EX78924G & EX78922G within an operating temperature range of -40 to 70°C
- 400 Watts for EX78924G & EX78922G within an operating temperature range of -40 to 75°C
- 240 Watts for EX78912G within an operating temperature range of -40 to 75°C

(2). The 4 or 8 PoE ports can be divided into 2 or 4 groups. The maximum PoE output is 120W for each group, and the maximum PoE output per port is 90W.

- Group 1 comprises of Port 1 and Port 2
- Group 2 comprises of Port 3 and Port 4
- Group 3 comprises of Port 5 and Port 6
- Group 4 comprises of Port 7 and Port 8
- 5. **Power Priority** Use the Drop-Down box in the Power Priority column to set the priority to Critical, High, or Low.
- 6. **Power Down Alarm** If enabled, the Power Down Alarm will trigger the switch relay when a loss of PoE power on a port occurs.
- 7. Status Informational only. Provides the status of the PoE port.
- 8. **PD Class** Informational only. Provides the PoE Classification of the PoE (PD) device attached to the PoE port in accordance with 802.3bt standards.
- Current (mA) Informational only. Shows the current draw from the attached PoE (PD) device.
- 10. **Consumption (W)** Informational only. Shows the power consumption of the attached PoE (PD) device.

PoE Scheduling

PoE Scheduling allows PoE ports to have their power up time scheduled by the hour of the day and day of the week. For a port to follow a schedule defined here, the port must be set to Scheduling on the PoE page (see PoE Port Configuration section).

PoE Scheduling												
✓ PoE Per Port Scheduling												
port ge1 🗸												
✓ PoE Per Port Scheduling												
								Ø				
Time	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Edit				
<00:00>												
<01:00>												
<02:00>												
<03:00>												
<04:00>												
<05:00>												
<06:00>												
<07:00>												
<08:00>												
<09:00>												
<10:00>												

Each PoE port on the switch can be scheduled to power up and down automatically. To configure a port:

- 1. Select the port from the drop-down list
- 2. Select the hour(s) of the day for each day of the week
- 3. Click on the Apply button.

~	PoE Per P	ort Scheduli	ng										
Ī	Time	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Edit				
	<00:00>	- 🗸	- •	- 🗸	- 🗸	- 🗸	- 🗸	- 🗸	Apply X Cancel				
	<01:00>	- Yes											
	<02:00>	No											
	<03:00>												

PoE Watchdog

PoE Watchdog is a management feature to help system administrators monitor and manage critical PoE powered devices. PoE Watchdog is only supported on PoE enabled ports. Once enabled, the switch will continuously ping a user specified IP address across the port. If the switch does not receive a reply within a specified interval, it can automatically power down or power cycle the powered device.

V PoE	PoE Watchdog Config												
								00					
Port	Enable Watchdog	Target Address(IP)	Ping Interval (Default 300s)	Failure Count (Default 3)	No Response Action	Startup Delay(Default 300s)	Current Status	Edit					
ge1	Disable		300	3	NoAction	300	NoAction						
ge2	Enable 🗸		300	2	NoAction ~	300	NoAction	Cancel					
ge3	Disable		300	3	NoAction	300	NoAction						
ge4	Disable		300	3	NoAction	300	NoAction						
ge5	Disable		300	3	NoAction	300	NoAction						
ge6	Disable		300	3	NoAction	300	NoAction						
ge7	Disable		300	3	NoAction	300	NoAction						
ge8	Disable		300	3	NoAction	300	NoAction						

- 1. **Enable Watchdog** Set the PoE Watchdog by selecting one of the following settings in the drop-down box.
 - Enable Enable PoE Watchdog on a specific port.
 - Disable Disable PoE Watchdog on a specific port.
- 2. Target Address (IP) Set the IP address to which the device is connected.
- 3. Ping Interval (Default 300s) Set the ping interval.
- 4. Failure Count (Default 3) Set the failure count.
- 5. **No Response Action** Set the response action when switch does not receive a reply from the specified IP address across the port.
 - No Action
 - Power Cycle To reboot the PD.
 - Power Off To power off the PD.
- The StartUp Delay (Default 300s) is the initial time delay before the system sends out the first ICMP echo request on the port (Range: 30 - 600 sec).

IGMP Snooping

A switch running IGMP snooping will dynamically determine which hosts connected to a particular VLAN in the switch should receive specific multicasts. The switch "snoops" (listens in on) IGMP messages and other multicast transmissions. The switch then determines which ports are associated with each multicast transmission.

Enable IGMP snooping by clicking the edit icon in the first panel, and selecting **enabled**. Then click "Apply."

To configure IGMP settings for a specific VLAN, click the check box next to the VLAD ID. Then set the parameters for **IGMP Snooping Status**, **IGMP Snooping Querier**, **IGMP Version** (1 -3), **Fast Leave**, **IGMPv1/v2 Report suppression**, and **IGMPv3 Report suppression**.

In the bottom panel, select which ports will take a **passive-forward** role, and which ones will be **force-forward**.

IG	MP S	Snooping	5								
~	IGMP	Snooping								•••	
I					IG	/P Snooning					
	IGMP S	Snooping Mod	e Enable	d							
	IGMP	Snooning Settir	ag (by VLAN)								
•	IGIMI	Shooping Setti	IG (Dy VD ((V)								00
	VLAN ID	IGMP Snooping Config	IGMP Snooping Querier	IGMP Version	Fast Leave	IGMPv1/v2 Report suppression	Query Interval	Max Response Time		Edit	
	1	Enabled	Disabled	3	Disabled	Enabled	125	10			
~	Forwa	ard Ports								Ø (ł)	
Ī		Forwa	rd Mode			Forward Ports			Edit		
		passive	e-forward			none					
		force-	forward			all					

8 STP

The Spanning Tree algorithm works by designating a single switch (The Root Bridge) in the network, as the root or the parent to all the switches. All the switches in the network will use the same algorithm to form unique paths all the way back to the Root Bridge. Some switches establish a blocking point (a port on a switch) somewhere along the path to prevent a loop. There are 3 versions of the Spanning Tree protocol, STP, RSTP, MSTP, and they are all backwards compatible with each other.

Spanning Tree Protocol (STP)

This is the original Spanning Tree protocol, and it has been superseded by both the RSTP and MSTP protocol. It is based on a network with a maximum diameter of no more than **17 switches**. It uses timers to synchronize any changes in the network topology, and this could take minutes. It is not recommended that you use this version of the Spanning Tree protocol.

Rapid Spanning Tree protocol (RSTP)

The RSTP protocol is the new enhanced version of the original STP protocol. It uses an enhanced negotiation mechanism to directly synchronize any topology changes between switches; it no longer uses timers as in the original STP protocol, which results in a faster re-convergence time. The maximum allowed network diameter for the RSTP protocol is **40 switches**.

Multiple Spanning Tree Protocol (MSTP)

The MSTP protocol extends the RSTP protocol by simultaneously running multiple instances of the Spanning Tree Protocol and mapping different VLANs to each instance, thus providing load balance across multiple switches. The MSTP protocol accomplishes this by creating new extended sections within the RSTP protocol, called Regions. Each region runs its own instance of the Spanning Tree Protocol. Within each Region, the MSTP protocol can accommodate a network diameter of up to 40 switches. There can be a maximum of 40 Regions in a single MSTP network.

Global Configuration

Spanning Tree Protocol is enabled by default. To enable/disable STP, click the edit icon in the lower panel of the page, and click the corresponding radio button. The set values for the following fields:

- **Bridge Priority** Bridge Priority is used to set the Root and backup Root Bridge. Default is 32768. Range is 0 to 61440.
- **Hello Time** The rate at which BPDUs (Bridge Protocol Data Units) are sent. Default is 2 seconds. Range is 1 to 10 seconds.

- Max Age Hop count limit for BPDU packets. Range is 6 to 40. Default is 20.
- Forward Delay Range is 4 to 30 seconds. Default is 15 seconds.
- STP Version Select from MSTP, RSTP, or STP compatible

Status		
	Status	
Bridge ID	800100e0b3113361	
Designated Root	800100e0b3113361	
Reg Root ID		
Root Port		
Root Path Cost	0	
Current Max Age (sec)	20	
Current Hello Time (sec)	2	
Current Forward Delay (sec)	15	
Topology Change Count	1	
Time Since Last Topology Change	Sun Jan 1 23:08:01 2017	
Setting		

RSTP Port Setting

Hello Time (1..10 sec) Max Age (6..40 sec)

STP Version

Forward Delay (4..30 sec)

Configure individual port RSTP settings on this page. Click the checkbox next to the desired ports, and set the following parameters:

- **Port Priority** Port Priority range is between 0 and 240 in multiples of 16.
- Admin Path Cost range is between 1 and 200,000,000.

2

20

15

RSTP

- **Conf. Link Type** This is the spanning tree link type. Choose **auto (**link type is set based on the interface's duplex setting**)**, **point-to-point**, or **shared**.
- Conf. Edge Port Select enable to make the interface an edge port.

RSTP	Port Setti	ng											
✓ RST	✓ RSTP Port Configuration Ø (3)												
Port	Port Status (Role/State)	Priority (Granularity 16)	Admin. Path Cost	Conf. Link Type	Curr. Link Type	Conf. Edge Port	Curr. Edge Port	Edit					
ge1	Designated / Forwarding	128	20000	point-to-point 🗸	point-to- point	Disabled 🗸	Disabled	Apply X Cancel					
ge2	Disabled / Discarding	128	20000	point-to-point	point-to- point	Disabled	Disabled						
ge3	Disabled / Discarding	128	20000	point-to-point	point-to- point	Disabled	Disabled						
ge4	Disabled / Discarding	128	20000	point-to-point	point-to- point	Disabled	Disabled						
ge5	Disabled / Discarding	128	20000	point-to-point	point-to- point	Disabled	Disabled						

MSTP Properties

To form a MSTP Region, the switches that will be connected together to form the MSTP Region must have the same values for these parameters:

- Region name
- Revision level
- Configuration Digest

The first two parameters can be configured directly on the MSTP Properties screen. **Configuration Digest** will be automatically calculated by the switch based on the VLAN to **MSTI (Multiple Spanning Tree Instance)** mapping. The VLAN to **MSTI** instance mapping must be the same for all the switches within the same **MSTP Region**.

Click the edit icon, and enter the **Region Name**, **Revision Level**, and **Max Hops**. Then click "Apply."

ISTP Propertie	es	
 Setting 		
		Setting
Region Name	Default	
Revision Level	0	
Max Hops	20	
Digest	0xAC36177F50283CD	4B83821D8AB26DE62
CIST Root ID	800000904ce3a800	
CIST Reg Root ID	800000904ce3a800	
CIST Bridge ID	800000904ce3a800	

MSTP Instance Setting

Select the **VLAN** that you want to map to an MSTP instance by clicking the corresponding check box next to the VLAN ID. Then enter the instance ID and click "Apply."

Configure the MSTP instance by clicking the check box next to the Instance ID and entering the Bridge Priority (range is 0 to 61440).

Μ	MSTP Instance Setting												
~	VLAN Instance Configuration												
								0					
		Edit	dit VLAN ID Inctance ID (1-63, 0 to delete)										
			300	1									
~	MST	P Instance Se	tting										
								0					
	Edit	Instance ID	Bridge Priority (0-61	440)	Root ID	Root Port	Root Path Cost	Bridge ID					
		1	32768		8001000000000000	0	0	8001000000000000					

MSTP Port Setting

You can adjust the location of the blocking port in a MSTP network by modifying the **Port Priority** and the **Path Cost** of the ports on the switch. Modifying the **Port Priority** adjusts the blocking port between two switches. Modify the **Port Cost** adjusts the location of the blocking port in a MSTP loop. First assign ports to an MSTP instance by clicking the check box next to the instance ID, and then the check boxes next to the ports you want to add.



To modify the **Port Priority** and the **Path Cost**, click the check box next to the corresponding MSTP instance in the bottom panel, and enter values in those fields. Then click "Apply."

M	STF	Port S	etti	ng							
~	Por	t Instance Co	onfigu	ration							
											0
		Edit				Inst	ance ID		1	Member	
							1			ge1	
~	MS	TP Port Settir	ng								
											0
	Edit	Instance ID	Port	Port State	Role	Priority	Path Cost	Designated Bridge ID	Designated Port ID	Designated Root ID	Designated Path Cost
		1	ge1	Discarding	Disabled	128	20000	800100904ce3a800	838f	000000904ce3a800	0

Advanced Setting

The top panel of the Advanced Setting page contains three settings which determine how the switch handles BPDU packets.

- **Bridge bpdu-guard configuration -** When the BPDU Guard feature is set for a bridge, all portfast-enabled ports of the bridge that have **bpdu-guard** set to default shut down the port on receiving a BPDU. In this case, the BPDU is not processed.
- Error disable timeout configuration Enabling this allows a Disabled port to reenable itself automatically after the specified Interval.
- Interval Default is 300 seconds. This is the length of time a port will remain disabled after shutting down due to the **bpdu-guard**.

dvanced Setting	
 Advanced Bridge Configuration 	
	Advanced Bridge Configuration
Bridge BPDU-guard configuration	Enabled Isabled
Error disable timeout configuration	Enabled Isabled
Interval (101000000 sec), Default: 300	300

In the Advanced Power Port configuration panel, you can enable **Portfast**, which sets a port as an edge-port to enable rapid transitions and enable disable **BPDU-Guard Configuration**. When set to default, the port will use the Advanced Bridge Configuration settings. Enable or Disable to override the Bridge BPDU-Guard settings.

🗸 Adv	anced Per Port Configuration		
			00
Po	Portfast Configuration	BPDU-guard Configuration	Edit
ge	Disabled 🗸	Default 🗸	Cancel
ge	Disabled	Default	

VLAN Setting

VLANS are created and modified in the VLAN Setting panel. Click the add icon, and then enter the VLAN ID and the VLAN name. The VLAN name should not be more than 32 characters and cannot include spaces. If you do not specify a VLAN name, the system will create one. Click "Apply" when finished.

VI	AN Setting			
~	VLAN Setting			• • •
	VLAN ID	VLAN Name	State	Edit
	1	default	Enable	

After a VLAN has been created, use the VLAN Port panel to attach specific ports to the VLAN, and to set as Tagged or Untagged. Click "Apply" when finished.

~	VLAN Port		
VL	AN ID 1 🗸		Θ
	VLAN Port		
	Port	VLAN Member	Tagged / Untagged
	ge1	✓Yes	Tagged 🗸
	ge2	□Yes	Tagged
	ge3	□Yes	Untagged V
	ge4	□Yes	Untagged 🗸

Port Setting

Configure the port type (access, trunk, or hybrid), PVID, and User Priority for each switch port.

Po	ort Set	ting			
~	VLAN Po	ort Setting			
					00
	Port	Mode	PVID	User Priority	Edit
	ge1	hybrid 🗸	1	0 🗸	Generation Apply X Cancel
	ge2	access trunk	1	0	
	ge3	hybrid	1	0	
	ge4	hybrid	1	0	
	ge5	hybrid	1	0	

Private VLAN

In private VLANs, a primary VLAN is broken into secondary VLANs, classified as either **community** or **isolated**. Hosts in an isolated secondary VLAN can't communicate with anything except the **promiscuous** port, which is usually a gateway. In private VLANs, a primary VLAN is broken into secondary VLANs, classified as either **community** or **isolated**. Hosts in an isolated secondary VLANs, classified as either **community** or **isolated**. Hosts in an isolated secondary VLANs, classified as either **community** or **isolated**. Hosts in an isolated secondary VLAN can't communicate with anything except the **promiscuous** port, which is usually a gateway or uplink. Hosts within the same community can communicate with other members of that community VLAN.

The first panel of the Private VLAN screen is Private VLAN Setting, where VLANs are added and set as primary, community, or isolated. Note that the VLANS added here must have been already created on the <u>VLAN Setting</u> screen. To add a private VLAN, click the add icon, and enter the VLAN ID. Then select the **VLAN Type**, and click "Apply."

VLAN Private Setting	
PVID	VLAN Type
	primary 🔻
	primary
	isolated
Cancel XCancel	
	A

Private VLAN associations are set up in the second panel. Click the add icon, and enter the VLAN ID of the primary and secondary VLANs. Then click "Apply."

VLAN Private Association					
Primary Vlan	Secondary Vlan				
⊘ Apply	Cancel				

In the third panel, configure port status in a private VLAN. Click the add icon, then the select the port using the drop-down menu. Set the port as either **host** or **promiscuous**. Then click "Apply." Note that ports still must be made a member of the secondary VLAN on the <u>VLAN</u> <u>Setting</u> screen.

VLAN Private Port Mode				
Switchport	Private VLAN Mode			
ge1 ▼	host			
	Cancel			
	ĥ			

MAC/Subnet/Protocol Based VLAN

In port based VLANs, a port is mapped directly to a VLAN. Instead of a port, you can also map MAC addresses, IPv4 addresses, or an Ethernet protocol to a specific VLAN. Each mapping must have its own rule number. When aping to a protocol, you must also specify the type of packet encapsulation: **ethv2**, **snaplic**, or **nosnaplic**.

Multiple rules can be grouped into a single **VLAN Classifier Group**, which can be created in the third panel. In the fourth panel, a VLAN Classifier Group can be assigned to a port.

MAC/Su	lbnet/Pr	otocol Based VLAN			
✓ MAC-Bas	sed VLAN				
Edit	Rule	MAC Address (in HHHH.	HHHH.HHHH format)	VLAI	H ldentifier
	1	9465.9cfe	.9709		500
✔ Subnet-I	Based VLAN				+ 0
✓ Subnet-I Edit	Based VLAN Rule	IPv4 address (in A.B	.C.D/E format)	VLAN IG	entifier
Subnet-l	Based VLAN Rule 2	IPv4 address (in A.B 10.10.10.1	.C.D/E format) 0/24	VLAN Id 6	entifier
 Subnet- Edit Protocol 	Based VLAN Rule 2 I-Based VLAN	IPv4 address (in A.B 10.10.10.1	.C.D/E format) 0/24	VLAN Id 6	 •••••••••••••••••••••••••••••
 Subnet-l Edit Protocol Edit Rule 	Based VLAN Rule 2 I-Based VLAN	IPv4 address (in A.B 10.10.10.1	.C.D/E format) 0/24 Ethernet Decimal (0-65535)	VLAN Id 6 Packet Encapsulation	et Q dentifier 00 tet Q vLAN Identifier

~	VLAN Classifier Grou	р		
				()
	Edit		Group (1-16)	Rules
			10	1
~	VLAN Classifier Port	Setting		• •
	Edit	Port	Group (1-16)	VLAN
		ge5	10	500

10 QOS

Global Configuration

To enable QoS (Quality of Service), click the edit icon on the first panel and select the radio button next to **enabled**. Then select either **cos** (Class of Service) or **dscp** (Diffserv Code Point). Choose a queuing policy: **strict** (strict priority), **wdrr** (weighted deficit round robin), or **wrr** (weighted round robin).

obal C	onfiguration	
QoS		
		00
	QoS	
QoS	○Enabled	
Trust	□cos □dscp	
D. I'	Ostrict Owdrr Owr	

Enter the weight and the 802.1p priority for each queue in the second and third panels.

Veighted Round Robin						
		00				
Queue	Weight (1~63)	Edit				
0	1					
1	1					
2	2					
3	2					
4	4					
5	4					
6	8					
7	8					

✓ 802.1p Priority							
		00					
VLAN Priority	Queue	Edit					
0	0						
1	1						
2	2						
3	3						
4	4						
5	5						
6	6						
7	7						

Interface

Tail drop is a queue management algorithm that determines when the switch needs to drop packets. When the queue is filled to its maximum capacity, the newly arriving packets are dropped until the queue has enough room to accept incoming traffic. Note that the minimum threshold cannot exceed the maximum threshold.

QOS Interface Tail-Drop Threshold								
Tail-Drop Queue	Tail-Drop Min Threshold Percentages	Tail-Drop Max Threshold Percentages						
0 •								
	⊘ Apply ★Cancel							
	Cubbi							
		Å.						

Inte	erfac	e		
~ ()OS Inte	rface Tail-Drop Threshol	ld	
por	t ge1	•		
~	QOS I	nterface Tail-Drop Thres	hold	
				0
	Edit	Tail-Drop Queue	Tail-Drop Min Threshold Percentages	Tail-Drop Max Threshold Percentages
		1	50	75

DSCP

The DSCP screen lets you choose DSCP priorities, which are by default assigned to the lowest-priority queue, 0. For each DSCP priority, you can change the value of the queue to between 0 and 7.

D	SCP			
`	DSCP			
				0
	Edit	DSCP Priority	Queue	
	Ø	0	0 •	Cancel
		1	1	
		2	3	
		3	4	
		4	6	
		5	7	

ACL Information

The ACL Information screen is a read-only page for viewing which ACL Policy Maps are applied to which ports. Just select the port to be viewed with the drop-down menu.

ACL Informatio	n	
ACL Interface Summa	ary	Ø
ye1 ye2 ge3		
ge4	Error Message	
ge5 ge6 ge7	No Access Control Lists Attached	
ge8		
ge9		
ge10		
ge11		
gerz		

ACL Configuration

To enable ACL on the switch, QoS must first be enabled.

- 1. Create and configure an ACL Access List first.
- 2. Next, you will need to create and configure an ACL Class Map,
- 3. Associate the previously created ACL Access Lists to this ACL Class Map.
- 4. Next, create and configure an ACL Policy Map
- 5. Associate all the appropriate and necessary ACL Classes into this ACL Policy Map.
- 6. Then apply this ACL Policy Map (and all the Access Lists that it contains) to a specific port.



Create a standard IP Access List in the first panel by clicking the add icon and entering the required parameters.

A	ACL Configuration								
V IP Access List									
Edit Index IP Access List (1-99/1300-1999) Action IP address (A.B.C.D) Mask (A.B.C.D)									
		1	10	permit	10.10.10.10	0.0.0.0			
				· · · · · · · · · · · · · · · · · · ·					

In the second panel, Extended IP ACLs are created in the same way.

✓ IP Access List (Extended)									
									()
Edit	Index	IP Access List (100-199/2000- 2699)	Action	Protocol	IANA Assigned Protocol Number	Source Address	Source Wildcard Bits	Destination Address	Destination Wildcard Bits
	1	2000	deny	any		11.11.11.11	255.0.0.0	12.12.12.12	255.0.0.0

In third panel, Class Maps are created and assigned an Access List.

~ (lassmap N	1atch ACL		
ma	tch acces	s-group ▼		
	 access-g 	roup		
				Đ
	Edit	Applied Class Name	Access Group Number (1-199, 1300-2699)	
		Sample_name	10	

In the fourth panel, ACL Policy Maps are created and assigned one or more Class Maps.

1	Policy-map Match ACL						
			• •				
	Edit	Policy Map	Class Map Matched				
		Sample_policy					
		Sample_policy	Sample_name				

In the fifth and final panel, existing ACL policies can be applied to ports.

ACL Port Attach			
			0
Edit	Port	ACL Attached	
	ge1	None	
Ø	ge2	None None	Cancel
	ge3	Sample_policy	
	ge4	None	
IP ACL

IP Access Control Lists (ACLs) allow/deny packets based on Protocol Type, Source Type, Source Address, Destination Type, and/or Destination Address. Defined IP Acess Lists can be viewed in the second panel.

P ACL				
Add Access List				
				0
		Add Ac	cess List	
Туре	Standard			
Number				
Action	Permit			
Source Type	Address			
Source Address				
Source Mask				
Access List				(
Edit	Number	Action	Rules	

Vlan Access Map, Vlan Map Entries, and Vlan Filter can be viewed in the lower panel.

			0 🛛
		Vlan Access Map	
Access-Map Name			
Sequence Number			
Statistics per-entry	Disable		
Match/Action	Match		
List Type			
List Number			
Vlan Map Entries			0 0
Vlan Map Entries Vlan Vlar	n Map	Clause	Ø 🚱 Edit
Vlan Map Entries Vlan Vlan Filter	n Map	Clause	Ø 3 Edit

Port ACL Setting

The section allows for configuration of ACL parameters for individual switch ports. Click the Add icon, and then enter the interface, access list, and direction (inbound or outbound). Then click Apply.

Port ACL Setting					
~	✓ Port ACL Setting				
	Edit	Interface	Access List	Direction	

12 DHCP

DHCP Server

The EtherWAN switch can function as a DHCP server for a single VLAN (it can be any VLAN) on the switch. When functioning as a DHCP server, the EtherWAN switch can be configured with a range of IP addresses, default gateway and DNS servers, which will allow the switch to use the dynamic configuration function of the DHCP protocol to provide any TCP/IP device that is a DHCP client, to dynamically obtain an IP address, default router, and DNS servers. The EtherWAN DHCP server can also be configured with a lease period that the DHCP clients are allowed the use of their assigned IP address. In this simple implementation, both the DHCP Client and the DHCP Server must be on the same network (same VLAN).

To enable DHCP, click the edit icon on the first panel, and click the radio button next to **enabled**. Then click "Apply."

D	HCP Server		
`	Global DHCP Server		
			0
		Global DHCP Server	
	Global Status	●Enabled ○Disabled	
	Restart DHCP Server	Restart	
		⊘ Apply Cancel	

In the second panel, select the VLAN for which you want to configure DHCP, and enter the start IP, end IP, Subnet mask, Gateway, Primary & Secondary DNS, and Lease Time.

1	✓ DHCP Server setting									
										0
	Edit	Interface	Status	Start IP	END IP	Subnet Mask	Gateway	Primary DNS	Secondary DNS	Lease Time
		vlan1.1	Disabled							86400
		vlan1.500	Disabled							86400
		vlan1.600	Disabled							86400

The DHCP Binding table at the bottom is a read-only table that displays which IP addresses have been allocated to which DHCP clients.

✔ DHCP Binding Table			
			0
Mac Address	IP Address	Host Name	Expires in

DHCPv6 Server

To configure the switch as a DHCPv6 server, set the global status to enabled.

D	HCPv6 Server		
~	 Global DHCPv6 Server 		0 🛛
		Global DHCPv6 Server	
	Global Status	Disabled	
	Restart DHCPv6 Server	Restart	

In the second panel, enter the starting and ending IP addresses, the prefix length, primary and secondary DNS, and the lease time.

✓ DHCPv6 Server setting							0			
	Edit	Interface	Status	Start IP	END IP	Prefix Length	Primary DNS	Secondary DNS	Lease Time	
		vlan1.1	Disabled						86400	
	*	vlan1.2	Disabled •						86400	Cancel

The third panel is the DHCPv6 Binding Table.

✔ DHCPv6 Binding 1	Fable			Ø
IPv6 Addre	ess Binding State	Preferred Life	e Max Life	Expires

DHCP Relay

DHCP relays pass a client's requests to the DHCP server, even when the server is on a different VLAN. To configure a DHCP relay, first enter the IP address of a DHCP relay server. Then select the ports and enable Option 82 (for added security) and Global Status if desired.

DHCP Relay		
V DHCP Relay Server List		
_		()
Edit	DHCP Relay Server IP (A.B.C.D)
V Global DHCP Relay		
		0 📀
	Global DHCP Relay	
Enabled Ports		
Option 82	Disabled	
Global Status	Disabled	
Restart DHCP Relay	Restart	

DHCP Snooping

DHCP snooping allows for the drooping of undesired DHCP traffic. It is most commonly used to prevent unauthorized DHCP servers from offering IP addresses to DHCP clients. Set the DHCP Snooping Status to enabled and check the box next to trusted interfaces. You can also clear the binding table for static, dynamic, or all entries.

DHCP Snooping					
✔ DHCP Snooping Setting					
					<u>Ø</u> Q
	C	HCP Snooping Settin	g		
DHCP Snooping Status	Disabled				
Trusted Interfaces					
Clear Binding Table					
✓ DHCP Snooping Binding					•0
Mac Address	IP Address	Lease Time	Binding Type	Vlan	Port

13 NTP

NTP Configuration

To enable Network Time Protocol (NTP), click the edit icon on the first panel, and click the radio button next to **enabled**. Then click "Apply." Use the "Sync" button to force the switch to synchronize the system time with the server.

NTP Configuration					
✓ NTP Setting					
		Ð			
	NTP Setting				
NTP Status	○Enabled				
Sync Time	Sync				
Time Zone & Offset	●UTC -0 ○Predefined ○Custom				
	Cancel				

Add NTP servers in the second panel by clicking the add icon, entering the IP address of the NTP server, and then clicking "Apply." You can see a list of all current NTP servers in this panel.

✓ NTP Server List			
			000
	Server IP	Кеу	Edit
 NTP Authentication Key 			
			000
Key ID	HMAC	Key Value	Edit

Daylight Saving Time Setting

There are two ways to set daylight saving on the switch: Weekday Mode and Date Mode. To enable daylight saving time, select the desired mode.

Daylight Saving Time	Setting
✓ Daylight Saving Time Setting DST Mode disable ▼	
✓ Daylig date ne Setting	
weekddy	Daylight Saving Time Setting
Current DST Mode	disable
Disable DST setting	Disable

The only difference between the two modes is the method by which the starting and ending dates are entered.

V Da	aylight Saving Time Setting	
	Davlight Saving Time Setting	
Ť	Daylight Saving Hine Setting	Ø
		Daylight Saving Time Setting
	Current DST Mode	disable
I	DST Timezone Name (3-6 chars)	
I	DST Offset (1-480 mins)	
I	DST Start Month	
I	Date	
I	Hour	
I	Minute	
I	DST End Month	
I	Date	
I	Hour	
	Minute	

✓ Daylight Saving Time Setting

DST Mode weekday 🔻

✤ Daylight Saving Time Setting

		0
	Daylight Saving Time Setting	
Current DST Mode	disable	
DST Timezone Name (3-6 chars)		
DST Offset (1-480 mins)		
DST Start Month		
Week		
Day		
Hour		
Minute		
DST End Month		
Week		
Day		
Hour		
Minute		

14 SNMP

SNMP General Setting

SNMP is a TCP/IP application layer network management protocol that allows any TCP/IP device to be managed across a TCP/IP network. It is based on the client-server paradigm. The server (called a SNMP Agent) runs a process on the managed device that listens for a client's NMS (Network Management Station) polling requests to fetch or set a data item on the managed device. The SNMP Agent can also send alert messages (called Traps) to an NMS automatically, based on the occurrence of certain events on the device that the Agent resides.

To configure SNMP general settings, click the edit icon, and enter values for the following fields:

- 1. Set the SNMP Status to enable.
- 2. Enter a short description (up to 256 characters) into the **Description** field.
- 3. Enter a name into the entry field next to Location.
- 4. Enter a name (up to 256 characters) into the entry field next to **Contact**.
- 5. Enter a trap community name (up to 256 characters) into any of the fields next to Trap Community Name 1 5. Community names identify the SNMP Trap community group that the traps on this switch should be sending to. The identical Trap community names should also be set on the NMS hosts that will be receiving the traps. Each name defined corresponds with the Trap host IP address fields with the same number below.

Warning! Use of the default Community settings may lead to potential security vulnerabilities. Therefore, it is suggested to set your own Community Name or leave the Community Name blank.

- 6. Enter an IP address for the NMS host(s) that should be receiving traps from this switch, into the fields next to any of the 5 **Trap Host IP Address** fields.
- **7.** Enable or disable the **Link Down Trap**. This will allow or stop the switch from sending a trap to the identified trap community groups when any port on the switch moves from the link up state to the link down state.
- 8. Enable or disable the Link Up Trap. This will allow or stop the switch from sending a trap to the identified trap community groups when any port on the switch moves from the link down state to the link up state.

- **9.** Enable or disable the **MAC Notification Trap**. This will allow or stop the switch from sending a trap to the identified trap community groups anytime there is a change in the MAC table on certain selected ports of the switch.
- 10. Set the interval between the MAC notification traps that you want the switch to send by entering the interval (in number of seconds from 1 to 65535) into the entry field next to MAC Notification Interval (1 to 65535 seconds).
- 11. Set the size of the MAC notification history table by entering the total number of records (from 1 to 500) that the switch will keep for user to review at any one time into the entry field next to MAC Notification History Size (1 to 500).
- **12.** Select which ports on the switch for which traps should be sent when there is a new MAC address added to the MAC table for the port, by checking the corresponding check boxes for these ports in the **MAC Notification Added** section.
- **13.** Select which ports on the switch for which traps should be sent when there is a MAC address being removed from the MAC table for the port, by checking the corresponding check boxes for these ports in the **MAC Notification Removed** section.
- **14.** Click the "Apply" button when finished.
- **15.** Save the configuration.

SNMP General Setting

✓ SNMP General Setting

SNM	P General Setting
SNMP Status	Enable
Description	12 GbE Managed Switch
Location	
Contact	
Trap Community Name 1	
Trap Community Name 2	
Trap Community Name 3	
Trap Community Name 4	
Trap Community Name 5	
Trap Host 1 IP Address	
Trap Host 2 IP Address	
Trap Host 3 IP Address	
Trap Host 4 IP Address	
Trap Host 5 IP Address	
Link Down Trap	Disabled
Link Up Trap	Disabled
PoE Interface Down Trap	Disabled
PoE Interface Up Trap	Disabled
PoE OverLoad Trap	Disabled
PoE Watchdog Trap	Disabled
Power Down Trap	Disabled
Power Up Trap	Disabled
MAC Notification Trap	Disabled
MAC Notification Interval (1 to 65535 seconds)	1
MAC Notification History Size (1 to 500)	1
MAC Notification Added	
MAC Notification Removed	

00

SNMP v1/v2

Click the edit icon and enter the SNMP community name into the **Get Community Name** field. This will allow the NMS to poll status information from the switch (read only). Then enter the SNMP community name, into the **Set Community Name** field. This will allow an NMS to change the status of a data item in the switch.

SNMP v1/v2		
✓ SNMP V1/V2c Setting		
		00
	SNMP V1/V2c Setting	
Get Community Name	public	

SNMP v3

The top panel of this screen is SNMP v3 Add User. To add a user, click the edit icon, and then enter the username. Set the Access mode to **Read Only** or **Read/Write**. Then click "Apply."

SNMP v3					
V SNMP V3 Add Use	er				
SNMP Version SNM	IPv3 No-Auth	•			
🗸 SNMP V3 Add	User				
					Ø
			SNMP V3 Add Us	er	
User Name					
Access Mode	Read Only				
 SNMP V3 Setting 					Ø
Edit User Name	Access Mode	Security Level	Authentication Type	Authentication Password	Privacy Pass Phrase

In the first panel, select SNMP Version from the drop-down menu.

NMP Version	SNMPv3 No-Auth	
	SNMPv3 No-Auth	
SINIVIP V3	SNMPv3 Auth-MD5	
	SNMPv3 Auth-SHA	
	SNMPv3 Priv-AES-128 Auth-MD5	
	SNMPv3 Priv-AES-192 Auth-MD5	SNMP V3 Add User
	SNMPv3 Priv-AES-256 Auth-MD5	
User Nam	SNMPv3 Priv-AES-128 Auth-SHA	
Access Mo	SNMPv3 Priv-AES-192 Auth-SHA	
Access MU	SNMPv3 Priv-AFS-256 Auth-SHA	

15 802.1X

Radius Configuration

By default, the 802.1X function is globally disabled on the switch. If you want to use the 802.1X portbased security on a port, you must enable it globally on the switch first, and then enable it on a per port basis.

To enable Radius globally, click the edit icon on the first panel, and click the radio button next to **enabled**. Then click "Apply."

R	adius Config	guration		
`	Radius Server Glo	bal Setting		
				0
			Radius Server Global Setting	
	Radius Status	Enabled Isabled		
			⊘ Apply Cancel	

To add a Radius server, click the add icon in the second panel. Enter the **Radius Server IP address**, **Radius Server Port**, **Secret Key**, **Timeout**, and **Retransmit** values.

Rad	ius Configuration				
	Radius Server IP	Radius Server Port (default:1812)	Secret Key	Timeout <1-1000>	Retransmit <1-100>
		€Ap	ply XCancel		
					ĥ

Port Authentication

Click the check box next to the port for which you want to configure Radius and set the Authentication state to **enable**. Set the Port control feature to **auto** (enables 802.1X authentication, port starts in unauthorized state), **force-authorized** (disables 802.1X authentication, port transitions to the authorized state without authentication), or **force-unauthorized** (port stays in unauthorized state and ignores authentication attempts).

Enable **Periodic Reauthentication** if needed. If Periodic Reauthentication is enabled, enter a value for the interval (in seconds) between reauthorization attempts. Click "Apply" when finished.

P	ort	Authe	ntication						
`	802	.1x Port Se	etting						
									0
		ge1	Disable						
		ge2	Disable						
	1	ge3	Enable 🔻	false	force-authorized 🔻	Authorized	Enable 🔻	2147483647	Cancel

16 LLDP

The Link Layer Discovery Protocol (LLDP) allows network devices to advertise their identity, capabilities, and neighbors on a local network.

LLDP General Settings

To enable LLDP, click the edit icon on the first panel, and select **enabled** from the drop-down menu. Enter a value for the **Holdtime Multiplier**, which is used to compute the actual time-to-live (TTL) value used in an LLDP frame. Then enter the **TX Interval**, which adjusts the time that LLDP information is transmitted by the switch. Finally, select items that will be advertised in the **Global TLV** (Time – Length – Value) by clicking in the corresponding check boxes. Click "Apply" when finished.

LDP General Setting	5
 LLDP General Settings 	
	8
	LLDP General Settings
LLDP Status	Disabled •
Holdtime Mutiplier (2-10)	4
Tx Interval (5-32768 sec)	30
	All Port Description System Name System Description System Capabilities
	Management Address Port VLAN ID MAC/PHY Configuration/Status
Global ILV	■Port And Protocol VLAN ID ■VLAN Name ■Protocol Identity ■Link Aggregation
	Maximum Frame Size

LLDP Port Settings

LLDP Ports Settings allows the individual ports on the switch to be configured for LLDP independently of one another. Each port can be configured to transmit LLDP information, receive LLDP information, and notify (via SNMP or Syslog) if there are changes in the LLDP information received from neighboring devices.

Click the check box next to the port for which LLDP is to be configured. Select enabled or disabled for the **Transmit**, **Receive**, and **Notify** fields.

LLDP Port Settings							
~	LLDP Port	Setting				0 0	
Ī	Port	Link Status	Transmit	Receive	Notify	Edit	
	ge1	up	Enabled	Enabled	Disabled		
	ge2	down	Enabled	Enabled	Disabled		
	ge3	down	Enabled	Enabled	Disabled		
	ge4	down	Enabled	Enabled	Disabled		
	ge5	down	Enabled	Enabled	Disabled		
	ge6	down	Enabled	Enabled	Disabled		

LLDP Statistics

The top panel of the LLDP Statistics screen is LLDP Device Statistics, a read-only panel that shows total values for Last Update, Total Inserts, Total Deletes, Total Drops, and Total Ageouts.

LDP Statistic	S	
 LLDP Device Statis 	tics	
		0
	LLDP Device Statistics	
Last Update	6 Days 15:35:28	
Total Inserts	5	
Total Deletes	2	
Total Drops	0	

The second panel shows LLDP statistics per port, including **Tx Total**, **Rx Total**, **Discards**, **Errors**, **Ageout**, **TLV Discards**, and **TLV Unknowns**.

V	LLDP Statistics								
								0	
	Port	Tx Total	Rx Total	Discards	Errors	Ageout	TLV Discards	TLV Unknowns	
	ge1	0	0	0	0	0	0	0	
	ge2	0	0	0	0	0	0	0	
	ge3	0	0	0	0	0	0	0	
	ge4	0	0	0	0	0	0	0	
	ge5	0	0	0	0	0	0	0	
	ge6	0	0	0	0	0	0	0	

LLDP Neighbors

LLDP Neighbors is a read-only page (see Figure 108) that will display all the LLDP capable devices detected by the switch. The following information about connected LLDP-enabled devices is displayed in a tabular format. The columns displayed are: **Port**, **Chassis ID**, **Port ID**, **IP Address**, and **TTL** (Time to Live).

LL	LDP Neighbors									
~	V LLDP Neighbors									
							0			
	Index	Port	System Name	Chassis ID	Port ID	IP Address	ΠL			
	1	ge1	none	30:65:ec:91:98:20	30:65:ec:91:98:20	0.0.0	3439			
		· · · ·								

17 Routing

ARP Table

A	ARP Table							
~	ARP Table			۵				
	IP Address	MAC Address	Interface	State				
	192.168.1.25	8c8c.aa75.ae78	vlan1.1	REACHABLE				

Static Route

Static routes are created by specifying the next hop to which the switch forwards data for a specific subnet. Configured static routes will be added to the routing table database and stored in the switch.

To add a new static route, click the add icon, and then enter values for the following fields:

IP destination prefix (A.B.C.D) — Subnet IP destination prefix
Prefix Type — Mask or Length, corresponding field type below appears based on selection.
Prefix Mask— A.B.C.D format, if Prefix Type is Mask
Prefix Length — 0 - 32
Gateway Address — A.B.C.D format
Gateway Interface — Gateway nexthop interface name
Distance — 1 - 255, Administrative Distance
Description — Description of the static route
Tag — Range is 1-4294967295, Tag used as a "match" value to control redistribution via route maps

Click "Apply" when finished. Existing routes can be edited by clicking the checkbox next to the IP destination prefix on the left.

St	Static Route									
	✓ Static Routing									
	Edit	IP destination prefix(A.B.C.D)	Prefix Type	Prefix Mask (A.B.C.D)	Prefix Length	Gateway Address(A.B.C.D)	Gateway Interface	Distance	Description	Tag (1- 4294967295)
		12.12.12.0			24	13.12.13.12	ge10			

To add an IPv6 route, enter values for these fields:

IPv6 destination prefix – (X:X::X:X) format

Prefix Length – Length of IPv6 prefix

Gateway Type – Address or interface

Gateway Address - (A.B.C.D) format

Distance - From 1 to 255, Administrative Distance

V IPv6 Static Routing								
					• •			
Edit	IPv6 destination prefix(X:X::X:X)	Prefix Length	Gateway Address(A.B.C.D)	Gateway Interface	Distance			

Route Table

The routing table is a read-only screen that shows existing routes.

oute Table							
oute							
Туре	Route default	Subtype	Route				
Connect		51	127.0.0.0/8 is directly connected, lo				
Connect			192.168.1.0/24 is directly connected, vlan1.1				
Connect			192.168.2.0/24 is directly connected, eth0				
Pv6 Route							
Туре	Route default	Subtype	IPv6 Route				
Type Connect	Route default	Subtype	IPv6 Route ::1/128 via ::, lo, 45w3d13h				
Type Connect Connect	Route default	Subtype	IPv6 Route ::1/128 via ::, lo, 45w3d13h 2001:db8:85a3::/64 via ::, vlan1.1, 05:09:15				

Route Map

Route Maps can be used for both redistribution and policy routing. To create a route map, click the add icon. Enter the **name** of the route map, the type (**Permit** or **Deny**), and the sequence number (Sequence to insert to or delete from an existing route-map entry. Then click "Apply."

Route Map		
Name	Permit/Deny	Sequence Number
	Permit 🔻	
	Cancel	
		h

Existing route maps can be deleted by clicking the corresponding check box and clicking "Delete."

✓ Route Map								
			• •	Ð				
Edit	Name	Permit/Deny	Sequence Number					
	Rincewind	Permit	100					

Add match Clauses in the second panel. These are the conditions that must be met in order for a route map to redistribute from one routing protocol to another.

~	Add Clause	
		Add Clause
	Route Map	Rincewind permit 100 •
	Match/Set	Match Set
	Option	●Interface ●Metric ●IP
	Interface	ge1 v
		✓Apply

The Route Map Entries panel is a read-only panel that shows configured Route Maps.

•	✔ Route Map Entries							
			0					
	Edit	Route Map	Clause					
		testmap permit 100						
			match interface ge1					

Proxy ARP

Proxy ARP allows the switch to answer ARP queries for a network address that is not on that network. The ARP Proxy is aware of the location of the traffic's destination and offers its own MAC address as the (seemingly) final destination. The "captured" traffic is then typically routed by the Proxy to the intended destination via another interface or via a tunnel. To enable Proxy ARP, select an interface or VLAN by clicking the check box at the left. Select enable, and then click "Apply."

Pr	oxy ARP			
~	Proxy ARP			
1	- 10			•
- 1		L3 Interface	Proxy ARP	
	Ø	vlan1.1	Disabled v Enabled	Cancel
		vlan1.2	Disabked	
		vlan1.3	Disabled	
		vlan1.4	Disabled	
		vlan1.5	Disabled	

VRRP

VRRP (Virtual Router Redundancy Protocol) is a distance-vector routing protocol that uses hop count as a routing metric. VRRP eliminates the risk of a single point of failure inherent in a static default routing environment. It specifies an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN. One of the major advantages of VRRP is that it makes default path available without requiring configuration of dynamic routing on every end-host.

The virtual-MAC Feature allows the backup device to use the MAC address of the primary device.

VRRP		
VRRP Global Configuration		
		00
	VRRP Global Configuration	
Virtual-MAC Feature	Enabled	
VRRP V2 Compatible	Disabled	

To configure VRRP:

- Click the edit icon.
- Select the IP version (IPv4 or IPv6)
- Enter a Virtual Router Identifier (VRID), from 1 255.
- Select the physical interface or VLAN that will be used for virtual routing.
- Set **Accept Mode** to true or false. Accept Mode allows the switch to respond to pings (ICMP EchoRequests) sent to the VRRP virtual IP address.
- Set the Advertisement Interval (the rate at which the Master router sends advertisement packets to all members of the VRRP group) in seconds. Range is from 1 – 10. These packets indicate that the master router is still operational.
- Select the circuit interface to be used for circuit failover.
- Set the **Circuit Failover Priority**. This is the value by which the virtual router decrements its priority value during a circuit failover event. Configure this value to be greater than the difference of priorities between the master and backup routers.
- Set the **Preempt Mode** to True or False. If true, this specifies that the router with the highest priority will function as a backup to the Master router when master is unavailable.
- Set the priority. If you are configuring the master router, set this value to 255. For other VRRP routers, use a value from 1 254. If the master router fails, the router with the highest priority will become the new master.
- Set the **Switch Back Delay** for the timer for the master VRRP router.
- Enter the virtual IP address for the VRRP session.
- Set the status to enable.
- Click the "Apply" button.

V Add VRRP	
	🖉 🖸
	Add VRRP
IP Version	○IPv4 ○IPv6
VRID	1255
Interface	vlan1.1 T
Accept Mode	True 🔻
Advertisement Interval (csec, only in multiple of 5)	54095
Circuit Interface	ge1 🔻
Circuit Failover Priority	1253
Preempt	True 🔻
Configured Priority	1255
Switch Back Delay (ms)	1500000
Virtual IP	
Status	Enable 🔻
⊙ ⁄	Apply Cancel

Details of existing instances of VRRP can be viewed in the VRRP table at the bottom of the screen.

VRRP Table											
											0
Edit	VRID	Interface	Virtual IP Address	Priority	Advertisement Interval	Accept Mode	Preempt Mode	Circuit Failover Interface	Circuit Failover Priority	Circuit Failover Status	Operation
	100	ge10	unset		1	FALSE	TRUE	unset	unset	unset	Disable

18 RIP

RIP General Setting

The Routing Information Protocol (RIP) is a distance-vector routing protocol that uses hop count as a routing metric. RIP prevents routing loops by setting a limit on the number of hops allowed in a path from source to destination.

To enable and configure RIP on the managed switch:

- Click the edit icon.
- Set the Router RIP field to **Enable**.
- Choose RIP version 1 or 2.
- Enable/disable **Default Information** to distribute default routes.
- Set the **Default Matrix** value in the range of 1 to 16.
- Set the Distance from 1 to 255 (Default value is 120)
- Set the timings for the **Routing Table Update Timer**, the **Routing Information Timeout Timer**, and the **Garbage Collection Timer** (Default values are 30, 180, and 120 seconds respectively).
- Click "Apply".

RIP General Setting

	Router RIP
Router RIP	Enabled ODisabled
Version	○1
Default-Information	○Enabled
Default-Metric (Default:1)	1
Distance	120
Routing Table Update Timer (Default:30s)	30
Routing Information Timeout Timer (Default:180s)	180
Garbage Collection Timer (Default:120s)	120

RIP Port Setting

For a port to be displayed on this screen, the interface must first be added on the <u>RIP Network by</u> <u>Interface</u> panel. To configure RIP port settings:

- 1. Select the interface by clicking the corresponding check box.
- 2. Set the RIP receive version (1, 2, or both)
- 3. Set Receive packets to enable or disable.
- 4. Set the Send Version to 1 or 2.
- 5. Set Send Packet to Enable or Disable.
- 6. For the Split Horizon Field, select enable, disable, or poison reverse.
- 7. Set the Authentication Mode to disable, MD5, or simple password.
- If the Authentication Mode is MD5 or Simple Password, set the Authentication Key (1 16 characters).
- 9. Click "Apply."

RIP Port Setting												
~	 Edit 	Interface										Ø
	Edit	Edit Interface	Link Status	Line Protocol	Receive Version	Receive Packet	Send Version	Send Packet	Split Horizon	Authentication Mode	Authentication Key	-
	Ø	ge10	down	down	1 •	Enable 🔻	1 •	Enable 🔻	Poison Reverse v	Disable •		☑ ApplyX Cancel

RIP Route

The RIP route table is a read-only page that shows existing RIP routes. The Routing Table fields are:

- Route Code (R)ip, (K)ernel, (C)onnected, (S)tatic
- **Network** IP address of destination network
- Next Hop Next closest router or Layer 3 switch towards destination
- Metric Number of hops
- From IP address of source router
- I/F Interface

• **Time** – Duration of time since last update

RIP Network

On the RIP Network screen, you can add or delete subnet addresses and interfaces to be advertised by RIP. To add a subnet, click the add icon in the top panel, and enter the subnet address and prefix length. Then click "Apply."

R	RIP Network								
~	✓ RIP Network by Subnet								
			• • •						
	Edit	Subnet Address	Prefix Length						
		10.10.10	24						

To add an interface, click the add icon, select the interface from the drop-down list, and then click "Apply."

G	✓ RIP Network by Interface						
		• •					
Edit Port	Edit	Port					
ge10		ge10					

RIP Neighbor

The RIP Neighbor screen is used to add/delete RIP neighbor IP addresses. To add a neighbor, click the add icon and then add the IP address of the neighboring router or Layer 3 switch, and click "Apply." Select existing neighbors from the list and click "Delete" to remove them.

RI	9 Neighbor		
~	RIP Neighbor		0
	Edit	Neighbor Address	
		10.10.10.11	

RIP Passive

On the RIP Passive screen, you can select an interface to be "passive," that is, to prevent the RIP routing process from sending multicast/broadcast updates on that interface. Click the add icon, select the desired interface from the drop-down menu, then click "Apply" to make that interface passive. You can select and delete passive interfaces from the Passive Interface List by clicking the check box next to the interface and then clicking "Delete." Doing so will return that interface to sending multicast/broadcast updates normally.

RI	P Passive		
~	RIP Passive		•
		U	0
		Interface	
		ge10	

RIP Redistribute

Redistribution is using a routing protocol to advertise routes that have been learned by another routing protocol, static routes, or directly connected routes. To add an item to the redistribute list, select the protocol (**connected** or **static**), a <u>route map</u> that has been previously defined, and the desired metric, then click the "Apply" button.

RIP Redistrib	ute						
✓ RIP Redistribute						•	
Edit	Index	Protoc	ol	Metric	Ro	ute Map	
RIP Redistribute							
Index	Prote	ocol cted T	Metric		Route Map		-1
			☑Apply	Cancel			
							4

19 OSPF

OSPF General Setting

OSPF (Open Shortest Path First) is a link state routing protocol. It is a classless protocol with support for VLSM and CIDR, manual route summarization, incremental updates, and equal cost load balancing. OSPF uses only the interface cost as its metric. The administrative distance default value is 110. OSPF uses multicast addresses 224.0.0.5 and 224.0.06 for routing updates.

Devices running OSPF establish neighbor relationships, and then exchange routes. Instead of exchanging routing tables, devices exchange information about known network topologies. Each OSPF enabled device then calculates best routes and adds them to the routing table.

The following fields must be the same on both OSPF-enabled devices in order for them to become neighbors:

- subnet
- area id
- hello and dead interval timers
- authentication
- area stub flag
- MTU

To enable and configure OSPF, add a new OSPF process in the first panel, and in the second panel enter values for the following fields:

- 1. Auto Cost. (1~4294967) The auto-cost reference bandwidth, which controls how OSPF calculates the default metric for the interface.
- 2. Opaque LSA Capability. (enable/disable)
- 3. **RFC 1583 Compatibility**. (enable/disable) Setting this to enable will make the instance compatible with OSPFv2.
- 4. **Default Metric**. (1-16777214) A default metric facilitates redistributing routes with incompatible metrics. If the metrics do not convert, the default metric provides an alternative.

- 5. **OSPF Database Summary Optimization**. (enable/disable) When enabled, the database exchange process is optimized by removing the LSA from the database summary list for the neighbor, if the LSA instance in database summary list is the same as or less recent than the listed LSA in the database description packet received from the neighbor.
- 6. Log Adjacency Changes. (Log Adjacency Changes/Log Adjacency Changes-Detail)
- 7. **Maximum number allowed to process DD concurrently** (1~65535) Limits the number of Database Descriptors (DD) that can be processed concurrently.
- 8. Maximum number of OSPF area (Excluding Backbone Area, 1~4294967294)
- 9. **OSPF ABR type** (Cisco, IBM, shortcut, standard) OSPF Area Border Router (ABR) type.
- 10. **Flood reduction**. (enable/disable) When enabled, flood reduction reduces unnecessary refreshing and flooding of already known and unchanged information.
- 11. Router-ID For The OSPF Process (A.B.C.D)
- 12. Extension to OSPF Multi Instance Support. (enable/disable)
- 13. Passive Interface (Global Control). (enable/disable)
- 14. Shutdown OSPF Process. (enable/disable)
- 15. Click "Apply" when finished.

OSPF General Setting					
✓ OSPF General Setting					
	0 📀				
OSPF General Setting					
Auto Cost (1~4294967)	100				
Opaque LSA Capability	Enabled				
rfc1583 Capatible	Disabled				
Default Metric (1~16777214, 0 to disable)	0				
OSPF Database Summary Optimization					
Log AdJacency Changes					
Maximum number allowed to process DD concurrently (1~65535)	64				
Maximum number of ospf area (Excluding Backbone Area, 1~4294967294)	0				
OSPF ABR type	cisco				
Flood Reduction	Disabled				
Router-ID For The OSPF Process					
Extension To OSPF Multi Instance Support	Disabled				
Passive Interface (Global Control)					
Shutdown OSPF Process					

The second panel is OSPF Network. Use this panel to enable OSPF routing with a specified area ID (and optionally an instance ID) on interfaces with IP addresses that match the specified network address.

To add an OSPF network, click the add icon and enter the IPv4 network address. Select subnet mask or prefix length, and enter the value for the corresponding field that displays. Enter an **Area ID** from 0 -4294967295, and an Instance ID from 1 - 255 (if running multiple instances of OSPF).

✓ OSPF Network							
							()
Edit Network Number	(i.i.i.i) Networ	k Mask Type	Subnet M	Mask (A.B.C.D)) Prefix Len	gth 🛛 Area ID	Instance ID
OSPF Network	_	_		_	_	_	
Network Number (i.i.i.i)	Network Mask Type	Subnet Mask (/	A.B.C.D)	Prefix Length	Area ID		Instance ID
	Subnet Mask 🔻						
☑Apply XCancel							
							4

The final panel is for setting OSPF Timers, including Link State Advertisements (LSA), SPF Timers, and LSA Throttle Timers. Use the drop-down menu to select the timer type, and then click the edit icon in the panel displayed below.

OSPF Timers		
Timers Link State Advertiseme	it (LSA) 🔻	
✔ Link State Advertisement	SA)	
		0
	Link State Advertisement (LSA)	
LSA Minimum Delay	1000	
Reset To Default	Reset	

OSPF Advanced Setting

The top panel is for applying filters to networks in routing updates, redistributing other routing protocols into the OSPF routing table. Click the edit icon, and enter the name of the access list to be applied next to the filter type.

OSPF Advanced Setting						
✓ OSPF Distribute Filter List						
Process ID 100 V						
✓ OSPF Distribute Filter List						
				•		
Edit	Access-list Name	Filter Direction	Route Type	OSPF Process ID		
	Test	in				

The second panel is OSPF neighbor, used to configure OSPF routers interconnecting to NBMA (Non-Broadcast Multi-Access) networks. Include one neighbor entry for each known non-broadcast network neighbor. Configure the neighbor address on the primary address of the interface.

To add a neighbor router, click the add icon and enter the IP address of the neighbor in A.B.C.D format. Then enter the Cost (the Link-state metric to this neighbor), the Dead Router Poll Interval (the rate at which routers send hello packets when neighboring router is inactive, in seconds), and the priority.

V OSPF Neighbor Router					
			+ ()		
Edit OSPF Neighbor Router	Cost (1~65535)	Dead Router Poll Interval (0~214748364	7) Priority (0~255)		
OSPF Neighbor Router					
OSPE Neighbor Router	Cost (1~65535)	Dead Router Poll Interval (0~2147483647)	Priority (0~255)		
Cancel					
			4		

The third panel is OSPF Stub Host IP. Click the add icon, then enter the Stub Host IP address, the OSPF Area ID (0-4294967295 or A.B.C.D Format), and the Cost of host (0-65535). Click "Apply" when finished.

V OSPF Stub Host IP					
		0 0			
Edit OSPF Stub Host IP	OSPF Area ID (0-4294967295 or A.B.C.D Format)	Cost of host (0-65535)			
OSPF Stub Host IP					
OSPF Stub Host IP	OSPF Area ID (0-4294967295 or A.B.C.D Format)	Cost of host (0-65535)			
_					

The fourth panel is OSPF Default Information. Use (enable) it to create a default external route into an OSPF routing domain.

•	✓ OSPF Default Information						
				00			
			OSPF Default Information				
	Status	Disabled					

The fifth panel is used to set OSPF Routes Administrative Distance. The administrative distance rates the trustworthiness of a routing information source. A higher distance value means a lower trust rating.
 OSPF Routes Administrative 	stance	0
	OSPF Routes Administrative	Distance
External Routes	0	
Inter-Area Routes	0	
Intra-Area Routes	0	
Disable OSPF Distance	Disable	
	⊘ Apply Cancel	

In the OSPF Distance panel, set administrative distances for access lists or next hop IP addresses. Click the add icon, and enter the distance value, the IP source prefix, and the access list name. Then click "Apply."

V OSPF Dis	stance Value				
			O O		
Edit	Index Distance Value	IP Source Prefix (A.B.C.D/M)	Access List Name		
OSPF Distance	ce Value				
Index	Distance Value	IP Source Prefix (A B C D/M)	Access List Name		
	· · · · · · · · · · · · · · · · · · ·				
	Cancel				
			ĥ		

The OSPF Overflow Control Panel contains the settings for the maximum number of LSAs that can be supported by the OSPF instance.

✔ OSPF Overflow Control	
	0
OSPF Overflow Cont	trol
External Link States Maximum Number of LSAs (0~2147483647)	0
External Link States Recover Time (0~65535, 0 not recover)	0
Maximum number of LSAs (0~4294967294)	
Exceed Action	Soft(Gives Warning)
	Soft(Gives Warning)
⊘ Apply Cancel	Hard(Shutdown Instance)

The seventh panel, OSPF Passive interface is used to suppress sending Hello packets on an interface. Click the add icon, and then enter the interface and the interface IP address. Then click "Apply."

V Passive Interfac	e			
				()
Edit	Passive Interface		Interface Address (A.B.C.D)	
Passive Interface				
-	Dessius laterface		Interface Address (A.D.C.D)	_
_	Passive Interface		Interface Address (A.B.C.D)	_
-	eth0 •			
		Cancel		
				h

The OSPF Summary Address panel is used to summarize or suppress external routes with the specified address range. An address range is a pairing of a starting address and a mask that is almost the same as IP network number. Click the add icon, and enter the IP prefix, the Prefix Mask, the action (**not advertise** or **tag**), and the tag value. Then click "Apply."

OSPF Summary Address				
Index	IP Prefix	Prefix Mask	Action	Tag Value (0~4294967295)
			•	
⊘ Apply X Cancel				
✓Apply ★Cancel				

The final panel is OSPF Redistribute, for redistributing routes from a routing protocol, static route, and kernel route into an OSPF routing table. Click the add icon, and select the routing protocol (OSPFv3, connected, kernel, RIP, static route). Enter the OSPFv3 Process ID, Metric Value, and Metric Type. Finally, specify the route map reference and the tag value. Click "Apply when finished.

OSPF Re	distribute					
Index	Routing Protocol	OSPF Process ID (1~65535)	OSPF Metric Value (1~16777214)	OSPF Metric Type	Route Map Entries	Tag Value (0~4294967295)
	ospf 🔻			1 🔻		
	Cancel					
_						4

OSPF Area Configuration

The OSPF Area Configuration screen is comprised of five panels, the first of which is OSPF Area Config, used for defining areas and authentication. To add an area, click the edit icon and enter values for the following fields:

- 1. OSPF Area ID
- 2. Authentication
- 3. Set Summary-Default Cost
- 4. Name of Filter Access List
- 5. Filter networks between OSPF areas
- 6. Multi-Area-Adjacency Interface

- 7. Multi-Area-Adjacency Neighbor IP
- 8. Shortcutting Mode
- 9. Configure OSPF Area As Stub

Click "Apply" when finished.

OSPE Area Config		
Shi Aica com ₆		0
	OSPF Area Config	
OSPF Area ID (0~4294967295)		
Authentication	v	
Set Summary-Default Cost (1~16777215)		
Name of Filter Access List		
Filter networks between OSPF areas	v	
Multi-Area-Adjacency Interface	Filter networks sent to this area by access list	
Multi-Area-Adjacency Neighbor IP	Filter networks sent to this area by prefix-list	
Shortcutting Mode	Filter networks sent from this area by access-list	
Configure OSPF Area As Stub		

All OSPF areas must be connected to the backbone area 0. If this is not physically possible, a Virtual Link can be used. A virtual link connects through another area that is connected to area 0. To create an OSPF Area Virtual Link, click the add icon in the second panel and enter values for the following fields:

- 1. OSPF Area ID
- 2. Virtual Link IP Address
- 3. Authentication
- 4. Authentication Key (8 chars)
- 5. Dead Interval
- 6. Hello Interval
- 7. Message Digest Key
- 8. Message Digest Keyword
- 9. Retransmit Interval
- 10. Transmit Delay

Click "Apply" when finished.

V OSPF Area virtual Link		
	OSPF Area Virtual Link	00
OSPF Area ID (0~4294967295)		
Virtual Link IP Address		
Authentication	Enable •	
Authentication Key (8 chars)		
Dead Interval (1~65535, 0 to disable)		
Hello Interval (1~65535, 0 to disable)		
Message Digest Key (1~255)		
Message Digest Keyword (16 chars)		
Retransmit Interval (1~3600, 0 to disable)		
Transmit Delay (1~3600, 0 to disable)		

The third panel is for creating OSPF NSSA Areas. An NSSA (Not So Stubby Area) (NSSA) is an OSPF stub area that can also import external route information. External routes from other areas are not flooded into an NSSA, but route information from the NSSA is translated and flooded into other areas (like the backbone).

V OSPF Area Nssa			
	0 📀		
OSPF Ar	rea Nssa		
OSPF Area ID (0~4294967295)			
Specify a NSSA area	©Enabled ©Disabled		
NSSA Default Information Originate	©Enabled ©Disabled		
NSSA OSPF Default Metric			
NSSA OSPF Metric Type For Default Routes (default:2)	1 •		
No Redistribution Into This NSSA area	©Enabled ©Disabled		
Do Not Send Summary LSA Into NSSA	©Enabled ©Disabled		
NSSA Stability Interval			
NSSA-ABR Translator role	Always •		
⊘ Apply	Cancel		

The OSPF Area Routes Matching Range panel allows OSPF routes to be summarized at an area boundary. A single summary route is then advertised to other areas by the Area Border Routers (ABRs). Routing information is condensed at area boundaries and outside the area.

		0
OSPF Are	a Routes Matching Range (Border Routers Only)	
OSPF Area ID (0~4294967295)		
Area Range Prefix (A.B.C.D)		
PrefixType	Subnet Mask 🔻	
Area Range Subnet Mask (A.B.C.D)		
Advertise (default enable)	T	

The final panel is OSPF Area Status. It is read only, and displays the current Index, Area and Status of created OSPF areas.

✓ OSPF Area Status				
			0	
Edit	Index	Area	Status	

OSPF Interface Configuration

OSPF must be enabled on at least one interface in order to be activated on a network. Select the port from the drop-down menu in the upper left and then click the edit icon. Enter values for the following fields in the OSPF Interface Summary panel.

- 1. Authentication
- 2. Authentication Password (Key)
- 3. Interface Cost
- 4. Filter OSPF LSA During Synchronization And Flooding
- 5. Interval After Which A Neighbor Is Declared Dead
- 6. Flood Reduction

- 7. Time Between HELLO Packets
- 8. OSPF Interface MTU
- 9. Ignores the MTU in DBD packets
- 10. Network Type
- 11. Router Priority
- 12. Time Between Retransmitting Lost Link State Advertisements
- 13. Link State Transmit Delay
- 14. Disable OSPF

Click "Apply" when finished.

OSPF Interface Configuration	
✓ OSPF Interface Summary	
Port ge1 •	
✓ OSPF Interface Summary	
	0
OSPF Interface Summary	
Authentication	Disabled
Authentication Password (Key)	
Interface Cost (1~65535)	10
Filter OSPF LSA During Synchronization And Flooding	Disabled
Interval After Which A Neighbor Is Declared Dead (1~65535)	40
Flood Reduction	Disabled
Time Between HELLO Packets (1~65535)	10
OSPF Interface MTU (576~65535)	1500
Ignores the MTU in DBD packets	Disabled
Network Type	Disabled
Router Priority (1~255)	1
Time Between Retransmitting Lost Link State Advertisements (1~65535)	5
Link State Transmit Delay (1~3600)	1
Disable OSPF	Disabled

The second panel on this screen is for configuring the Interface Message Digest Key, which allows for uninterrupted transitions between passwords. This is helpful for administrators who want to change the OSPF password without disrupting communication. Click the add icon and enter the key and the OSPF password. Click "Apply" when done.

Port ge15 ▼ ✓ Interface Message Digest Key	
✓ Interface Message Digest Key	
Edit Key ID (1~255) OSPF password (key)	
1 1	

OSPF Interface Configuration with Address

The OSPF Interface Summary panel on this screen is similar to the one in the OSPF Interface Configuration screen, except that the OSPF area is restricted to an IP address. Select the port from the drop-down menu in the upper left and then click the edit icon. Enter values for the following fields:

- 1. Address of Interface
- 2. Authentication
- 3. Authentication Password (Key)
- 4. Interface Cost
- 5. Filter OSPF LSA During Synchronization and Flooding
- 6. Interval After Which A Neighbor Is Declared Dead
- 7. Time Between HELLO Packets
- 8. Ignores the MTU in DBD packets
- 9. Router Priority
- 10. Time Between Retransmitting Lost Link State Advertisements
- 11. Link State Transmit Delay

Click "Apply" when finished.

SP	F Interface Configuration With Address	
 O 	SPF Interface Summary	
Port	t ge1 ▼	
~	OSPF Interface Summary	
I	OSPF Interface Summary	
	Address of Interface	
	Authentication	
	Authentication Password (Key)	
	Interface Cost (1~65535)	
	Filter OSPF LSA During Synchronization And Flooding	
	Interval After Which A Neighbor Is Declared Dead (1~65535)	
	Time Between HELLO Packets (1~65535)	
	Ignores the MTU in DBD packets	
	Router Priority (1~255)	
	Time Between Retransmitting Lost Link State Advertisements (1~65535)	
	Link State Transmit Delay (1~3600)	

The Interface OSPF Statistics panel is a read-only panel that shows the index, interface address, and statistics for the selected port.

🗸 In	nterface OSPF Stat	istics										
port	port ge1 🔻											
~	Interface OSPF S	itatistics										
	Edit	Index	Interface Address	Statics								

20 AAA (Authentication, Authorization, and Accounting)

TACACS Plus

This switch supports the Tacacs+ protocol IEEE 802.1X protocol to provide port based security against unauthorized access. Enable Tacacs+ by clicking the edit button in the top panel and setting the Authorization State to Enable. Then click Apply.

TACACS Plus			
✓ TACACS+ Authorization			
			0
		TACACS+ Authorization	
Authorization State	Disable 🔻		
		Cancel	

The next panel allows for the configuration of the switch to connect to a TACACS+ server. Setting a TACACS+ server to "primary" means that it will be the first server contacted when the switch tries to create a TACACS+ session. Only one server can be set to primary. Setting a TACACS+ server to "inactive" will disable it. A maximum of 3 servers can be added to a switch.

✓ TACACS+ Server Con	figuration						
							⊕⊘ ⊕
TACACS+ Server IP	TACACS+ Server Port	Timeout	Secret Key	Primary	Inactive	Edit	
TACACS+ Server Configu	iration						
TACACS+ Server II	P TACACS+ Server	Port	Timeo	ut	Secret Kev	Primary	Inactive
		1	1000			Enable 🗸	Enable 🗸
			☑ Apply	X Cancel			
							ĥ

21 ERPS (Ethernet Ring Protection Switching)

ERPS (Ethernet ring protection switching) is a protocol defined by the International Telecommunication Union (ITU) in its G.8032 recommendation. This document describes how ERPS can offer rapid detection and recovery if a link or node fails and also instructs the user on how to configure it. ERPS prevents loops on a per-VLAN basis with networks that are wired in a simple ring topology. ERPS (G.8032) Version 2 provides enhancements in support of multiple ring and ladder topologies, and EtherWAN is compliant with G.8032 Version 2, February 2012 edition.

Acronyms

The following acronyms are used in the discussion about Ethernet ring protection switching (ERPS):

- 1. **Node**: The L2 switch equipment added to the ERPS ring is called a node. Each node cannot be added to more than two ports in the same ERPS ring. The nodes are divided into RPL Owner, Neighbor, and Ring Node.
- 2. **Ring Protection Link (RPL)**: which is the link designated by mechanism that is blocked during idle state to prevent loop on an ERPS ring. In ERPS, port roles include RPL Owner, Neighbor, and Ring ports. The RPL Owner Node and the RPL Neighbor Node are responsible for blocking traffic over the RPL in normal conditions.
- 3. **RPL Owner Node**: RPL is controlled by the RPL Owner, which is one of the terminating nodes of this link. Usually, the RPL is blocked, and traffic cannot pass through it. Therefore, no loop will be formed within the ring. When a failure in a ring is detected, the RPL will become unblocked, and traffic can then pass through it. By this way, a single-point failure in the ring can be overcame and traffic can keep being forwarded in the ring.
- 4. **RPL Neighbor Node**: An ERPS ring has only one RPL Neighbor port configured by the user, and it must be a port connected to the RPL Owner port. If the network is normal, it will block together with the RPL Owner port to prevent loops in the ERPS ring. The node with the RPL neighbor port becomes the RPL neighbor node.



- 5. **Ring Node**: The common port The ports except RPL owner and neighbor port are ring node ports. If the node has only the common port, it will become the ring node.
- 6. **ERP Instance** (or **ERPS Instance**): ERP Instance (or ERPS Instance): An EPR instance is formed by the same instance ID, control VLAN, and interconnected switches.
- 7. **Major-Ring**: The topology of an ERPS network consists of one or several rings. Its ring members can be categorized into two types: the major ring and the sub-ring. An ERPS topology must include at least one major ring. The major ring is a closed circle formed by nodes. Each of the nodes has exactly two links that connect it to its neighbor node. One of the links in the closed circle should be configured as the RPL. Normally the RPL is blocked to prevent the traffic in the ring from looping.



8. **Sub-Ring**: A sub-ring is not a closed circle but a list of nodes with two terminating nodes. These two terminating nodes connect to either the major ring or another sub-ring. There is also a RPL, which is the sub-ring, and normally it is blocked to avoid traffic looping.



(Different forms of Main-Ring and Sub-Ring)

- Interconnected Node: There could be many nodes that connect to different rings. Each node cannot be added to more than two ports in the same ERPS ring. These nodes are divided into three categories: RPL Owner, Neighbor, and Ring Node. The nodes across different rings are called "interconnected nodes.
- 10. **Ring Automatic Protection Switching (R-APS)** protocol message: The protocol uses R-APS messages to communicate and coordinate the behavior among all ring nodes.
- 11. Link Failure:



11.1. The ring nodes adjacent to the failed link block the ring ports on the failed link.



11.2. The ring nodes adjacent to the failed link send R-APS (SF) message (SF: Signal Fail)

- 11.3. The R-APS (SF) messages are forwarded along the logical topology to the RPL owner and the RPL neighbor.
- 11.4. The RPL owner and the RPL neighbor unblock the RPL ports.



11.5. The ring nodes adjacent to the failed link continue sending R-APS (SF) messages periodically.

12. Link Recovery:



- 12.1. The ring nodes adjacent to the recovered link send an R-APS (NR) message (NR: No Request).
- 12.2. The R-APS (NR) messages are forwarded along the logical topology to the RPL owner.



- 12.3. The RPL owner blocks its PRL port.
- 12.4. The RPL owner sends an R-APS (NR, RB) message (NR: No Request, RB: RPL Blocked).



- 12.5. The R-APS (NR, RB) messages are forwarded along the logical topology to the ring nodes adjacent to the recovered link.
- 12.6. The ring nodes adjacent to the recovered link unblock the ports on the recovered link and stop sending R-APS (NR) messages.



12.7. The RPL owner continues to send R-APS (NR, RB) messages periodically.

13. **Control Channel**: The control channel is the transmission VLAN of the ERPS protocol, and the protocol packet will carry a corresponding VLAN tag.

- 14. Virtual Channel: A sub-ring can either have or not have a virtual channel on the interconnected node. In a sub-ring, there are two modes for transmitting the sub-ring's R-APS packets: the virtual-channel mode and the non-virtual-channel mode. R-APS packets cannot pass through the RPL of the sub-ring because the RPL is blocked. To transmit the R-APS from one side of the RPL to another, a tunnel in the major ring will be adopted. When R-APS packets arrive at the sub-ring's terminating node, they will be passed into this tunnel. By this way, R-APS packets can travel in the main ring and then arrive at another terminating node in the same sub-ring. Such a tunnel is called the Virtual Channel. In non-virtual-channel mode, there is no tunnel for the sub-ring. In this case, the G.8032 protocol will allow the R-APS packets belonging to the sub-ring to pass through the sub-ring's RPL to reach nodes on the other side of this RPL. Hence, every node in the sub-ring can receive the R-APS packets. Note that only the R-APS packets are allowed to pass through the sub-ring's RPL.
- 15. **Revertive Mode**: When the link fails, the RPL link is in the release protection state, and the RPL link is re-protected after the faulty link is restored to prevent loops.
- 16. **Non-revertive Mode**: After the fault is rectified, the faulty node remains faulty (without entering forwarding) and the RPL link remains in the release protection state.
- 17. Forced Switch: This is a management-triggered state. When an administrator needs to shut down a port that is participating in a ring, this management entity will come into action. When a Forced Switch object is issued on the port, the port goes down and the APS PDU gets propagated around the ring, indicating the status. When the clear management object is set on the port, this forced switch is revoked.
- 18. **Manual Switch**: Similar to the Forced Switch, the Manual Switch is also management-triggered. The difference is that it has a lower priority compared to forced switching.

ERPS Sample Configuration – Network Topology

Five switches are connected into one Major-Ring + Sub-Ring. (Shown as below)



ERPS Configuration

Go to the switch Web GUI Interface, from the left items list, the user can find ERPS option and go to ERPS Setting page. In this page the user can configure the ERPS function for the switch, see the figure shown below:

ERPS Configuration								
✓ Physical Ring Configuration					40 0			
Physical Ring	East Interface	West Interface		Edit				
✓ ERPS RAPS-Ring-Mac Mode					00			
	ERPS RA	PS-Ring-Mac Mode						
Mode Enabled								
✓ Profile Configuration						+ ØØ		
Profile Wait to Restore Time (unit: n	nins) Hold Off Time (unit	: 100ms) Guard time (unit: 10)ms) Revertive		Edit			
✓ ERP Instance Setting								
ERPS Instance Physical Subring RPL Name Ring Interface Role	Neighbor/Owner Profil Interface Name	e RAPS Data Vlan Channel ID(2~4094, Ring Vlan ID) ID	Virtual Level Channel Vlan ID	Attached to Instance Pro	TCN- pogation		Edit	<u>000</u>
		☑ Apply	Cancel	Name				
✓ ERP Instance Status Current ERP Instance					6	Ð		
✓ ERP Instance Status						2		
	EF	RP Instance Status				í		
Instance Name								
G8032 State								
Physical Ring								
Role								
East Link								
West Link								
TCN Propagation								
Attached								
AttachedTo								
VirtualID								
Data Vlan ID								
Raps Dest Mac Address								

There are five selections that can be made, which are Physical Ring Configuration, ERPS RAPS-Ring-Mac Mode, Profile Configuration, ERP Instance Setting, and ERP Instance Status.

Physical Ring Configuration		
Physical Ring	East Interface	West Interface
	ge1 🗸	ge1 🗸
☑A	Apply XCancel	
		ß

Choose Physical Ring Configuration, the user can Set Physical Ring Name, designed West Interface Port, and designed East Interface Port of the switch, see the figure below.

In ERPS RAPS-Ring-Mac Mode, the user can determine if RAPS Control MAC is set to "01" or the userdefined ring-id (ERPS RAPS-Ring-Mac Mode is enabled the user-defined ring-id by default); for example, If the ERPS ring is created with a user-defined ring-id, then its Control MAC address is set to 01:19:A7:00:00:ring-id (control-mac), while if the ERPS ring is created with control MAC set to "01", then its Control MAC address is always 01:19:A7:00:00:01. For detailed information, please refer to the document of ITU-T G.8032 (2010) and ITU-T G.8032 (2012).

V ERPS RAF	2S-Ring-Mac Mode	
		0 0
	ERPS RAPS-Ring-Mac Mode	
Mode	●Enabled ○Disabled	
	Apply Cancel	

Once the user has determined the RAPS Control MAC Mode is enabled or disabled, if the user want to modify the RAPS Control MAC Mode again, make sure the ERPS instance has to be completely removed in advance.

In Profile Configuration, the user can set a different profile name, wait to restore time, , Hold Off Time, and Grand Time for the designed profile. Also, setting up if the profile is worked in revertive mode or non-revertive mode, is shown in the figure below.

file Configuration				
e Wait to Restore Time (unit: n	nins) Hold Off Time (unit: 100ms)	Guard time (unit: 10ms) Re	vertive	Edit
Profile Configuration				
Drofilo	Wait to Postoro Timo (unit: mine)	Hold Off Time (unit: 100ms)	Cuard time (unit: 10mc)	Dovortivo
	112	0100	1200	Enable 🗸
	€Ap			

The original Physical Ring setting or Profile Configuration can also be removed once the configuration is not available to use anymore.

Choose ERP Instance setting, the user can set ERPS Instance ID, Physical Ring, RAPS Channel Vlan ID, Ring ID, and choose the appropriate Profile Name, RPL Role, and ERPS level for this Instance, see the figure below.

ERF	Instance Setting													
I	ERPS Instance Name	Physical Ring	Subring Block Interface	RPL Role	Neight	or/Owner erface	Profile Name	RAPS Channel Vian ID	Data Vlan ID(2~4094,)	Ring ID	Level	Virtual Channel Vian ID	Attached to Instance Name	TCN- Propogation
		none 🗸	none 🗸	none	 none 	~	none 🗸	24094	24094,	1255	07	none 🗸	none 🗸	enable 🗸
Cancel														

✓ Physical Ring Configuration														
	⊕⊘⊕													
Р	hysical Rir	ng	E	East Interface		West	t Interfa	ace			E	dit		
	R1			ge1			ge3				(
Profile Configuration Profile Wait to Postora Time (mins) Hold Off Time (mc) Cuard time (mc) Powertive Edit														
P1	Walt to F	1		0		1		Ena	ble		(
✓ ERP Instance Setting													400	
ERPS Instance Name	Physical Ring	Subring Block Interface	RPL Role	Neighbor/Owner Interface		RAPS Channel Vlan ID	Data Vlan ID	Ring ID		Virtual Channel Vlan ID	Attached to Instance Name	TCN- Propogation		Edit
INST_1	R1	east- interface	owner	west-interface	P1	2		none	none	none	none	enable		

The user can still add or delete a new ERPS Instance ID by clicking on the "+" button and setting a new ERPS Instance ID and other information related to the desired Instance setting, see the figure below.

•	✓ ERP Instance Setting														
														000	
	ERPS Instance Name	Physical Ring	Subrii Blocl Interfa	ng RPL k Role	Neighbor/Owne Interface		RAPS Channe Vlan ID	Data I Vlan D ID	Ring ID		Virtual Channe Vlan ID	Attached to Instance Name	TCN- Propogation	Edit	
	INST_1	R1	east interfa	owner	west-interface	P1	2		none	none	none	none	enable		
E	ERP Instance Setting														
	ERPS Instance Name			Physical Ring	Subring Block Interface	RPL I	RPL Role		Neighbor/Owne Interface		Profile Name	RAPS Channel Vlan ID		Data Vlan ID	
				none 🗸	none 🗸	none	~	none		~	none 🗸	24094			1.
													Apply	X Cancel	

Select a different ERPS Instance from ERPS Instance Status, and then the user can check the different ERPS Instance status, see the figure below.

Current ERP Instance 12 🗸						
✓ ERP Instance Status						
	ERP Instance Status					
Instance Name	12					
G8032 State	G8032_ST_INIT					
Physical Ring	R1					
Role	-					
East Link	-					
West Link	-					
TCN Propagation	Enabled					
Attached	-					
AttachedTo	-					
VirtualID						
Data Vlan ID						
Raps Dest Mac Address	01:19:A7:00:01					

22 Contact Information

EtherWAN System, Inc.

www.etherwan.com

USA Office	Pacific Rim Office
5 Jenner	8F., No.2, Alley 6, Lane 235, Baoqiao Rd.
Irvine, CA 92618	Xindian District, New Taipei City 231
Tel: +1-714-779-3800	Taiwan
Email: info@etherwan.com	Tel: +886-2-6629-8986
	Email: info@etherwan.com.tw

EtherWAN has made a good faith effort to ensure the accuracy of the information in this document and disclaims the implied warranties of merchantability and fitness for a particular purpose, and makes no express warranties, except as may be stated in its written agreement with and for its customers.

EtherWAN shall not be held liable to anyone for any indirect, special or consequential damages due to omissions or errors. The information and specifications in this document are subject to change without notice.

Copyright© 2024. All Rights Reserved. All trademarks and registered trademarks are the property of their respective owners EX78900G Hardened Managed PoE++ Ethernet Switch June 20, 2024