



# Hardened Managed 24-port 10/100/1000BASE-T

(8-port combo SFP) and 4-port 10G SFP+ Layer 3 Switch

**FastFind Links** 

Introduction

Installing the Switch

**Connecting to the Management Interface** 

**User's Guide - GUI** 

#### 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.

All other trademarks are property of their respective owners.

#### Warranty

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

#### www.etherwan.com

#### Products Supported by this Manual:

EG99000



# 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 Internet skills.

#### **Document Revision Level**

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

Revision	Document Version	Date	Description
A	Version 1	12/11/2018	

## 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	
Note         Notes emphasize or supplement important points of the main text.		Notes emphasize or supplement important points of the main text.	
Ŷ	Тір	Tips provide helpful information, guidelines, or suggestions for performing tasks more effectively.	
	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	iii
Changes in this Revision	iii
Document Conventions	iv
Safety and Warnings	iv
Contents	v
1 Introduction	10
Unpacking and Installation	11
Unpacking	11
Installing the Switch	11
Connecting to the Data Ports	11
1 Gbps Combo/SFP Ports	11
SPF+ Slots	11
Connecting Power	12
Terminal Block	12
Relay Output Alarm	
Connecting to the Management Interface	12
Alternate (Backup) Firmware	12
2 Web Management Interface	
About the Web-based graphical user interface (GUI)	
Default IP Address	
Login Process and Default Credentials	
Navigating the GUI	15
3 System Menu	
System Information	17
System Name	
System Password	
IP Address	18
System Time	19
Management Interface	

	Configuration	20
	Saving Switch Configuration	20
	Firmware Upgrade	21
	Reboot	22
4 Dia	ignostics Commands	23
	System Utilization	23
	System Log	25
	RMON Statistics	26
	Remote Logging	26
	Alarm Setting	
	Port Mirroring	
5 Poi	rt Commands	32
	Port Configuration	
	Port Status	
	Flow Control	34
	Rate Control	35
6 Sw	itching	36
	MAC Table	
	Static MAC Entry	
	Storm Control	
	Storm Detect	
	Trunking	
	LACP Trunking	
	GVRP	40
	VLAN Translation	41
7 IGN	ИР	42
	IGMP Configuration	42
	IGMP Snooping	
	GMRP	
8 STI	P	
	Spanning Tree Protocol (STP)	

Rapid Spanning Tree protocol (RSTP)	46
Multiple Spanning Tree Protocol (MSTP)	46
Global Configuration	
RSTP Port Setting	47
MSTP Properties	
MSTP Instance Setting	
MSTP Port Setting	49
Advanced Setting	50
9 VLAN	52
VLAN Setting	52
Port Setting	52
Private VLAN	53
MAC/Subnet/Protocol Based VLAN	54
10 QOS	56
Global Configuration	56
Interface	57
DSCP	58
11 ACL	59
ACL Information	59
ACL Configuration	59
12 DHCP	
DHCP Server	61
13 NTP	-
NTP Configuration	
Daylight Saving Time Setting 14 8021.X	
Radius Configuration	
Port Authentication	
15 LLDP	68
LLDP General Settings	68
LLDP Port Settings	68

	LLDP Statistics	69
	LLDP Neighbors	70
16 Ro	outing	71
	Static Route	71
	Route Table	71
	Route Map	72
	Proxy ARP	73
	VRRP	73
17 RI	Ρ	76
	RIP General Setting	76
	RIP Port Setting	76
	RIP Route	77
	RIP Network	77
	RIP Neighbor	78
	RIP Passive	78
	RIP Redistribute	79
18 SN	IMP	80
	SNMP General Setting	80
	SNMP v1/v2	81
	SNMP v3	82
19 08	SPF	83
	OSPF General Setting	83
	OSPF Advanced Setting	85
	OSPF Area Configuration	90
	OSPF Interface Configuration	94
	OSPF Interface Configuration With Address	95
20 PI	M (Protocol Independent Multicast)	97
	Global Configuration	97
	Interface Configuration	
		08
	PIM-SM RP Configuration	90

PIM-SM Neighbor Table	. 100
Contact Information	. 101



## **1** Introduction

ac b 2 SS 7 SS

EtherWAN's EG99000 is a gigabit Layer 3 switch designed for high bandwidth uplink or interconnection. With full wire speed switching capability, the EG99000 provides IP routing and switching across VLANs and subnetworks with no compromise in performance. The EG99000 supports comprehensive internetwork IP routings including static route, RIP v1 & v2, and OSPF v2 for IPv4. All these routing protocols can operate simultaneously with redistributions to each other and route control tools, including IP prefix-list and route-map.

In addition to supporting Layer 3 features, the EG99000 supports full sets of EtherWAN Layer 2 features such as port security, IGMP snooping, port-based VLAN, GARP protocols, link aggregation, access control lists and STP/RSTP/MSTP. Besides in-band management via web browser, Telnet, SSH and SNMP, the EG99000 supports out-band management via an RJ-45 port and an RS-232 console interface.

The EG99000 Series provides high reliability and nonstop operation in harsh environments where temperatures range from -40° to 75°C (-40° to 167°F), as well as in areas with high electromagnetic interference (EMI). The EG99000 is also equipped with sophisticated network and system failure recovery features including VRRP, and dual redundant power supplies to minimize the chance of network or system downtime. This makes it an ideal choice for both industrial and mission critical applications where sustained connectivity is crucial. The switch is shipped ready for use.



000000000000000000

6900000000000000

 $\oplus$ 

0

0



0

090000000000000000

Mgmt

0



## Unpacking and Installation

### Unpacking

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

- One EG99000 switch
- One CD containing this user's guide
- One quick start guide

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 is bracket-mount. Use the enclosed screws and brackets to mount the switch in an open or enclosed rack.

- 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).
- Be sure there is adequate airflow.

### **Connecting to the Data Ports**

The EG99000 has the following ports:

- 24 x 10/100/1000 Mbps copper ports
- 8 x Gigabit combo ports (RJ-45 & SPF)
- 4 x 1/10G SPF+ slots
- 1 x RJ-45 Management port
- 1 x USB port

#### 1 Gbps Combo/SFP Ports

Ports 17 – 24 are combo ports, and have two physical interfaces for each port. These ports can be used as either 10/100/1000BASE-TX on the left section or 1000BASE-FX on the right section. These ports operate in "either/or" fashion, i.e., connecting to fiber port 17 will render copper port 17 inoperable.

#### SPF+ Slots

SPF transceivers can be installed directly into right-side ports 17 - 24 and SPF+ ports 1 - 4. Ensure that the same type of transceiver is used at both ends of the link and that the correct type of fiber cable is used.

## **Connecting Power**

### **Terminal Block**

If your EG99000 comes with AC power cables, connect the cables into the power modules at the back of the switch. If your switch comes with a DC or AC terminal block (no cable), then connect the switch to a suitable power supply using 12 to 24 AWG wire. Redundant power supply is supported. However, only one power input is required to operate the switch. Input voltage is 48 VDC or 100 – 240 VAC, depending on model.

### **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 normal open and normal closed. Relay output current is 30VDC / 1A.

## **Connecting to the Management Interface**

**Serial -** Connect to the switch console by connecting the DB-9 cable to the console port of the switch and to the serial port of the computer running a terminal emulation application (such as HyperTerminal or Putty).

Configuration settings of the terminal-emulation program: Baud rate: 115,200bps, Data bits: 8, Parity: none, Stop bit: 1, Flow control: none.

**TCP/IP** - Connect to the switch via the RJ-45 Management port located on the rear panel below the serial port, or via one of the Ethernet ports on the front panel. Use a terminal emulation program and connect to IP address **192.168.2.10**. You can also connect to the switch through any of the RJ-45 ports on the front panel, IP address is **192.168.1.10** (VLAN1.1).

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

### 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.

## 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.

Note: Supported browsers are Chrome, Internet Explorer version 11, and Microsoft Edge

### **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

## **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.



On the left 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 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	Ø
VLAN	$\odot$
QOS	Ø
ACL	$\odot$
DHCP	$\odot$
NTP	Ø
802.1X	Ø
LLDP	Ø
Routing	Ø
RIP	Ø
SNMP	⊘
OSPF	Ø
РІМ	Ø

#### 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:

S	/stem Informati	on	
	<ul> <li>System Information</li> </ul>		•
			<u> </u>
		System Information	
	System Name	EG99000	
	System Time	Fri May 05 10:58:39 UTC 2017	
	System Uptime	2:12	
	Firmware Version	3.04.1 05/15/17 12:40:12	
	Management IP	192.168.2.10	
	CPU Utilization	45%	

The second panel shows the active and alternate firmware versions.

✔ Firmware Information		
		0
	Firmware Information	
Active Version	3.04.1 05/15/17 12:40:12	
Alternate Version	3.03.2.1 03/09/17 15:15:19	

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

✓ MAC Address	Ø
Interface	MAC Address
eth0	0090.4ce3.a800
ge1	0090.4ce3.a802
ge2	0090.4ce3.a803
ge3	0090.4ce3.a804
ge4	0090.4ce3.a805
ge5	0090.4ce3.a806
ge6	0090.4ce3.a807
ge7	0090.4ce3.a808

## **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.

/stem Name	2	
<ul> <li>System Informatio</li> </ul>	n	0 0
	System Information	
System Name	EG99000_Test-switch-for-documentation	

### **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 Passwor	ď	
		Change Password
New Password		Show
Confirm Password		Show
Cancel	<u>,</u>	

## **IP Address**

The two panels on this page allow for the changing of the IP address of VLAN 1, and for the creation of default gateways.

Address			
Static IP			
Edit	VLAN ID	IP Address	
	1	192.168.1.50/24	
Default Gateway			
Default Gateway			¢
Default Gateway Edit		Default Gateway IP	0
-		Default Gateway IP 10.10.10.10	0
Edit			•
Edit		10.10.10.10	•

## **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 chapter on <u>NTP</u>.

/stem T	me	
<ul> <li>System Tin</li> </ul>	ie	
		Ø@
	System Time	
Year	2017	
Month	05	
Day	05	
Hour	13	
Minute	22	
	52	

## **Management Interface**

Enable / disable access to switch management through http, Telnet, and SSH on this page. Note that if you disable http you will lose access to the GUI, and need to use another management method to access the switch to save changes.

M	anagemei	it Interface	
~	Management Ir	terface	Ø 🛛
I		Managen	nent Interface
	WEB Agent	http	
	Telnet	Disabled	
	SSH	Disabled	

## 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		
<ul> <li>Auto Save Configuration</li> </ul>		
		0 📀
	Auto Save Configuration	
Auto Save	Disabled	
Interval (5~65535 sec)		

### **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 a .TGZ or .IMG format.

Fi	irmware Upgrade		
	Via TFTP Server		
			Via TFTP Server
	Filename	eg99000.tar.xz	
	TFTP Server IP		
			<b>⊘</b> Apply
	<ul> <li>Via web</li> </ul>		
	Please select ima	ge to upgrade:	
	Choose File No file	chosen	Upload file

## Reboot

Reboot the switch.

Search for	x
System	⊘
System Information	
System Name	

## **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.

Stern o	tilization		
CPU Utiliza	ition		
			(
		CPU Utilization	
Current uti	ilization	49%	
Max utiliza	ition	53%	
e Memory Lit	tilization		
Memory Ut	tilization		
		Memory Utilization	
Memory Ut     Total	tilization 513664	Memory Utilization	
		Memory Utilization	(
Total	513664	Memory Utilization	

Below these 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 L	og				
					<b>()</b>	
	Index	Date			Log	
	1	2017-05-05	00:00:25	NOTICE	Link down on Port ge14	
	2	2017-05-05	00:00:25	NOTICE	Link down on Port ge6	
	3	2017-05-05	00:00:25	NOTICE	Link down on Port ge8	
	4	2017-05-05	00:00:25	NOTICE	Link down on Port ge7	
	5	2017-05-05	00:00:25	NOTICE	Link down on Port ge5	
	6	2017-05-05	00:00:25	NOTICE	Link down on Port ge2	
	7	2017-05-05	00:00:25	NOTICE	Link down on Port ge4	
	8	2017-05-05	00:00:25	NOTICE	Link down on Port ge3	
	9	2017-05-05	00:00:25	NOTICE	Link down on Port ge1	
	10	2017-05-05	00:00:25	NOTICE	Link down on Port ge16	

## **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.

RMON Statistics	
rt ge11 🔻	
Port RMON Statistics	
	Port RMON Statistics
Drop Events	0
Multicast Packets Received	474
Broadcast Packets Received	10153
Undersize Packets Received	0
Fragments Packets	0
64-byte Packets Received	9492
65 to 127-byte Packets Received	1000
128 to 255-byte Packets Received	59
256 to 511-byte Packets Received	0
512 to 1023-byte Packets Received	110
1.0 to Maximum Packets Received	0
Oversize Packets Received	0
Jabber Packets	0
Bytes Received	802045
Packets Received	474
Collisions	0
CRC/Alignment Errors Received	0
TX No Errors	435
RX No Errors	10661

## **Remote Logging**

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.

emote l	Log Setting		
🗸 Remote Lo	ogging		
			00
		Remote Logging	
Status	Enabled		
<ul> <li>Log Server</li> </ul>	r IP List		• •
	Edit	Log Server IP	
		192.168.1.75	

## **Alarm Setting**

Alarms can be set for a variety of general switch conditions including link down, redundant power failure, and overheating. When equipped with a DDI compatible SFP module, major and minor alarms can also be set for SFP temperature, 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 DDI 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, either power input (if dual power inputs are used), and system temperature.

Alarm S	etting		
Basic	SFP	SFP RX	SFP TX

Alarm Trigger Lir	nk			
				6
Edit	Port	Enabled	Status	
1	ge1	No T	Link-down	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	

#### 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 temperature and voltage.

Alarm S	etting		
Basic	SFP	SFP RX	SFP TX

Edit	PORT	Enabled	
	ge17	No	Temper:SFP Module none detect (Major)
	ge18	No	Temper:SFP Module none detect (Major)
	ge19	No	Temper:SFP Module none detect (Major)
	ge20	No	Temper:SFP Module none detect (Major)
	ge21	No	Temper:SFP Module none detect (Major)
	ge22	No	Temper:SFP Module none detect (Major)
	ge23	No	Temper:SFP Module none detect (Major)
	ge24	Yes	Temper:SFP Module none detect (Major)
	xe1	No	Temper:SFP Module none detect (Major)
	xe2	No	Temper:SFP Module none detect (Major)
	xe3	No	Temper:SFP Module none detect (Major)

ge17 No Vcc:SFP Module none detect (Major)					
ge17       No       Vcc:SFP Module none detect (Major)         ge18       No       Vcc:SFP Module none detect (Major)         ge19       No       Vcc:SFP Module none detect (Major)         ge20       No       Vcc:SFP Module none detect (Major)         ge21       No       Vcc:SFP Module none detect (Major)	Edit	PORT	Enabled	Status	
ge19     No     Vcc:SFP Module none detect (Major)       ge20     No     Vcc:SFP Module none detect (Major)       ge21     No     Vcc:SFP Module none detect (Major)	1	ge17	No 🔻	Vcc:SFP Module none detect (Major)	Canc
ge20     No     Vcc:SFP Module none detect (Major)       ge21     No     Vcc:SFP Module none detect (Major)		ge18	No	Vcc:SFP Module none detect (Major)	
ge21 No Vcc:SFP Module none detect (Major)		ge19	No	Vcc:SFP Module none detect (Major)	
		ge20	No	Vcc:SFP Module none detect (Major)	
ge22 No Vcc:SFP Module none detect (Major)		ge21	No	Vcc:SFP Module none detect (Major)	
		ge22	No	Vcc:SFP Module none detect (Major)	
ge23 No Vcc:SFP Module none detect (Major)		ge23	No	Vcc:SFP Module none detect (Major)	
		xe1	No	Vcc:SFP Module none detect (Major)	

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).



Edit	PORT	Enabled	
	ge17	No	Rx Power:SFP Module none detect (Major)
	ge18	No	Rx Power:SFP Module none detect (Major)
	ge19	No	Rx Power:SFP Module none detect (Major)
	ge20	No	Rx Power:SFP Module none detect (Major)
	ge21	No	Rx Power:SFP Module none detect (Major)
	ge22	No	Rx Power:SFP Module none detect (Major)
	ge23	No	Rx Power:SFP Module none detect (Major)
	ge24	No	Rx Power:SFP Module none detect (Major)

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 Trig	gger SFP TX-Bias	Major	
Edit	PORT	Enabled	Status
	ge17	No	Tx Bias:SFP Module none detect (Major)
	ge18	No	Tx Bias:SFP Module none detect (Major)
	ge19	No	Tx Bias:SFP Module none detect (Major)
	ge20	No	Tx Bias:SFP Module none detect (Major)
	ge21	No	Tx Bias:SFP Module none detect (Major)
	ge22	No	Tx Bias:SFP Module none detect (Major)
	ge23	No	Tx Bias:SFP Module none detect (Major)
	ge24	No	Tx Bias:SFP Module none detect (Major)
	xe1	No	Tx Bias:SFP Module none detect (Major)

## **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 <b>v</b>
	Cancel	

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

Port N	/lirroring			
♥ Port	Mirroring			00
	Edit	From	То	Mode
		xe2	ge3	both
		ge1	ge2	transmit
		ge7	ge8	receive

## **5 Port Commands**

## **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.

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

- Port Type- Routed port or Switch port
- **IP address** For routed ports only, aaa.bbb.ccc.ddd/mm format
- Link Status Operational State of the Port's Link (Read-Only)
- Shutdown Shutdown state
- Port Description User-supplied description, 80 characters maximum
- **Duplex / Speed** Options are Auto, 100M/FD, 100M/HD, 10M/FD, and 10M/HD.

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

dit	Port	Port Type	IP Address	Link Status	Shutdown	Port Description	Duplex/Speed	
	ge1	Routed port	10.10.10.10/24	Down	No		Auto	
	ge2	Switch port		Down	No		Auto	
	ge3	Routed port		Down	No		Auto	
	ge4	Switch port		Down	No		Auto	
s.	ge5	Switch port		Down	No 🔻		Auto 🔻	Canc
	ge6	Switch port		Down	No		Auto	
	ge7	Switch port		Down	No	Mirrored to ge8	Auto	
	ge8	Switch port		Down	No		Auto	
	ge9	Switch port		Down	No		Auto	
	ge10	Routed port		Down	No		Auto	
	ge11	Routed port		Down	No		Auto	
	ge12	Switch port		Down	No		Auto	
	ge13	Switch port		Running	No		Auto	

## **Port Status**

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

Port Status	5					
Port	Link Status	Port Description	Port Type	IP Address	Speed	Duplex
ge1	Down		Router port		1g	auto
ge2	Down		Switch port		1g	auto
ge3	Down		Router port		1g	auto
ge4	Down		Switch port		1g	half
ge5	Down		Switch port		1g	half
ge6	Down		Switch port		1g	half
ge7	Down	Mirrored to ge8	Switch port		100m	half
ge8	Down		Switch port		1g	half
ge9	Down		Switch port		1g	half
ge10	Down		Router port		1g	auto
ge11	Down		Router port		1g	auto
ge12	Down		Switch port		1g	half
ge13	Running		Switch port		1g	full

## **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."

low C	ontro	I				
✓ Port F	low Contro	l				
Edit	Port	Send Admin	Send Operation	Receive Admin	Receive Operation	•
¢.	ge1	on 🔻	on	on <b>T</b>	on	<ul><li>☑ Apply</li><li>X Cancel</li></ul>
	ge2	on	on	on	on	
	ge3	on	on	on	on	
	ge4	on	on	on	on	
	ge5	on	on	on	on	
	ge6	on	on	on	on	
	ge7	on	on	on	on	
	ge8	on	on	on	on	

## **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.

ate	Con	trol				
V Por	rt Rate (	Control				
Edit	Port	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	6
V	ge1	0	0	0	0	☑ Apply Cancel
	ge2	0	0	0	0	
	ge3	0	0	0	0	
	ge4	0	0	0	0	
	ge6	0	0	0	0	
	ge7	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		
		00
	Ageing Time	
Ageing Time (10-1000000)	300	
		6)
Clear Dynamic MAC	Clear MAC	
Clear Dynamic MAC Clear Multicast MAC		

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**.

	C Entry			
tatic MAC	Entry Forward			
				<b>()</b>
Edit	Index	Port	MAC Address (Ex: 0000.1111.2222)	VLAN
	1	ge1	0090.4ce3.a80d	1
	Edit		Edit Index Port	Edit Index Port MAC Address (Ex: 0000.1111.2222)

# **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

torm Control								
• Sto	rm Cor	itrol						
Edit	Port	Broadcast Threshold Level	Multicast Threshold Level	DLF Threshold Level	Broadcast Packet-per- second	Multicast Packet-per- second	DLF Packet-per-second	6
	ge1	0.00	0.00	0.00	0	0	0	
¥	ge2	0.00	0.00	0.00	0	0	0	Cancel
	ge3	0.00	0.00	0.00	0	0	0	
	ge4	0.00	0.00	0.00	0	0	0	
	ge6	0.00	0.00	0.00	0	0	0	
	ge7	0.00	0.00	0.00	0	0	0	
	ge8	0.00	0.00	0.00	0	0	0	
	ge9	0.00	0.00	0.00	0	0	0	
	ge10	0.00	0.00	0.00	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	
Confi	guration
Storm-Detect Configuration	○Enabled  ●Disabled
Interval (265535 sec), Default: 10	10
Errdisable-recovery time (065535 sec), 0: no recovery	0

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

# 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 Tr	unk
Port	Member
	ge1 ge2 ge3 ge4 ge5 ge6 ge7 ge8 ge9 ge10 ge11 ge12 ge13 ge14 ge15 ge16 ge17
	ge18 ge19 ge20 ge21 ge22 ge23 ge24 xe1 xe2 xe3 xe4
	Cancel Cancel
	4

# 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.

AC	P.	Trur	nking						
<ul> <li>L</li> </ul>	_ACP	Config	guration						
									00
					LA	CP Configuration			
LA	ACP	Syster	n Priority (1-6	55535, default:	32768)	32768			
E	dit	Port	Trunk Port	LACP Mode		Priority (Set 0 for None)	LACP Timeout	LACP Sync	
		ge1	ро1	active •				No link	Apply     Delete     Cancel
		ge2	po1	active		-	long	No link	

## **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.

	Ø Q
GVRP	
sabled	
sabled	
	GVRP isabled sabled

GVRP Port		
Port	Applicant	Registration
ge3 ▼	normal <b>v</b>	normal 🔻
	Cancel	
		Å

#### Add GVRP Port

### **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	n	
VLAN Translation Globa	Setting	
		00
	VLAN Translation Global Setting	5
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."

V	LAN Translation			
	Port	Ingress/Egress	Translate from	Translate to
	ge3 ▼	ingress ▼		
			<b>⊘</b> Apply <b>X</b> Cancel	
				Å

# 7 IGMP

# **IGMP** Configuration

IGMP (Internet Group Management Protocol) was designed to manage IP multicast applications. There are three versions of IGMP, and all versions are backwards compatible:

IGMP version 1 sends queries to 224.0.0.1, while membership reports are sent to the group's multicast address.

IGMP version 2 accelerates the leaving of a group, and makes other adjustments to timeouts. Leave-group messages are sent to 224.0.0.2. It also introduces a group-specific query, which is sent to the multicast address of the group.

IGMP version 3 introduces source-specific multicasts. Membership reports are sent to 224.0.0.22

To enable IGMP globally on the switch, click the edit icon in the top panel, and select the radio button next to **enabled**. Enter a number for the **IGMP Limit**, which is the maximum number of group membership states (range is 1-2097152).

IGMP Configuration	
✔ IGMP Global Setting	
	0 🕥
	IGMP Global Setting
IP Multicast Routing Status	Enabled     Disabled
IGMP Limit	64001
	<b>⊘</b> Apply Cancel

To enable IGMP on an interface, select the interface from the drop-down menu in the second panel, then click the edit icon. Select the radio button next to **enabled**, and then select the IGMP version to be run. Enable **ProxyService** and/or **MRoute Proxy** if needed. Then set the **Immediate Leave**, **IGMP Limit**, and **Accessgroup** parameters.

t ge1 🔻	
<ul> <li>IGMP Interface Summary</li> </ul>	
Fight intenace summary	
	IGMP Interface Summary
IGMP Status	Disabled
IGMP Version	3
ProxyService	Disabled
MRoute Proxy	Disabled
Immediate Leave	

In the bottom panel, you can add IGMP Join Groups, and clear selected or all IGMP Local Memberships.

in Group					
					<b>(</b> )
Index	Group Address	Interface	Up Time	Expires	Last Reporter
ear Group		IGMP Clear G	roup		0 0
MP Local-Men	nberships On Interface				
MP Local-Men	nberships	CLEAR ALL			
	Index ear Group MP Local-Men	Index Group Address	Index Group Address Interface ear Group IGMP Clear G MP Local-Memberships On Interface	Index Group Address Interface Up Time ear Group IGMP Clear Group MP Local-Memberships On Interface	Index Group Address Interface Up Time Expires ear Group IGMP Clear Group MP Local-Memberships On Interface

# **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**.

IGN	MP Snoopi	ng					
							Ø 🛛
			IGN	1P Snooping			
IGM	P Snoopi	ng Mode En	abled				
• IGN	in shoopi	0,					
• IGN	in shoopi						
_		IGMP Snooping Stat	us IGMP Snooping Querier	IGMP Version	Fast Leave	IGMPv1/v2 Report suppression	IGMPv3 Report suppress
_			us IGMP Snooping Querier Disabled	IGMP Version	Fast Leave Disabled	IGMPv1/v2 Report suppression Enabled	IGMPv3 Report suppress Disabled
Edit	VLAN ID	IGMP Snooping Stat Enabled					
Edit	VLAN ID 1	IGMP Snooping Stat Enabled					Disabled
Edit	VLAN ID 1 ward Port	IGMP Snooping Stat Enabled	Disabled			Enabled	Disabled

### 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 ports to these groups to the local switch.

To enable GMRP, click the edit icon and select enabled. Once GMRP is enabled, you can configure GMRP on a port. Click the add icon in the lower panel, and use the drop-down menu to select a port. Set the GMRP Registration: **normal**, **fixed**, **forbidden**, or **restricted**. Set GMRP Forward All field to **enable** or **disable**. Then click "Apply."

GMRP			
✔ GMRP			
			0 🛛
		GMRP	
GMRP	Disabled	I	
✓ GMRP Por	t Configurati	ion	Ø
		GMRP Port Configuration	
Error Mes	sage	% GMRP is not enabled globally!	

GMR	GMRP Port Configuration							
	Port	GMRP Registration	GMRP Forward All					
	ge1 ▼	normal 🔻	disable 🔻					
	Cancel							
			ĥ					

# 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

		00
	Setting	
Spanning Tree Protocol	●Enabled ○Disabled	
Bridge Priority (061440)	32768	
Hello Time (110 sec)	2	
Max Age (640 sec)	20	
Forward Delay (430 sec)	15	
STP Version	RSTP V	

### **RSTP Port Setting**

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.
- **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.

STP	Ροι	rt Setting							
RST	TP Port	Configuration							C
Edit	Port	Port Status (Role/State)	Priority (Granularity 16)	Admin. Path Cost	Conf. Link Type	Curr. Link Type	Conf. Edge Port	Curr. Edge Port	
¢.	ge1	Disabled / Discarding	128	20000	point-to-point ▼	point-to- point	Enabled 🔻	Enabled	Cancel
	ge2	Disabled / Discarding	128	20000	point-to-point	point-to- point	Enabled	Enabled	
	ge3	Disabled / Discarding	128	20000	point-to-point	point-to- point	Enabled	Enabled	
	ge4	Disabled / Discarding	128	20000	point-to-point	point-to- point	Enabled	Enabled	
	ge5	Disabled / Discarding	128	20000	point-to-point	point-to- point	Enabled	Enabled	

#### **MSTP Properties**

In order 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."

MSTP Propertie	S	
✓ Setting		
		0 🖉
		Setting
Region Name	Default	
<b>Revision Level</b>	0	
Max Hops	20	
Digest	0xAC36177F50283CD4B	383821D8AB26DE62
CIST Root ID	800000904ce3a800	
CIST Reg Root ID	800000904ce3a800	
CIST Bridge ID	800000904ce3a800	
		<b>⊘</b> Apply Cancel

### **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).

ISTP Instance Setting								
VLAN	V Instance Conf	iguration						
						e		
E		VLAN ID		nctance ID (1-6	53, 0 to delete)			
		300		1				
MSTI	P Instance Setti	ng				G		
Edit	Instance ID	Bridge Priority (0-614	10) Root ID	Root Port	Root Path Cost	Bridge ID		

# **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.

N	STI	P Port	Setting	
	_	rt Instance	Configuration	Ø
	Edit	ID		
	¢.	1		Apply     Cancel

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."

ISTP Port Setting										
Port I	Instance Co	onfigu	ration							
										0
						1			ge1	
• MCTE	Port Settir	2.5								
	T OIL Setti	ig								e
Edit Ir	nstance ID	Port	Port State	Role	Priority	Path Cost	Designated Bridge ID	Designated Port ID	Designated Root ID	

# **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 re-enable 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**.

Advanced Setting	
✓ Advanced Bridge Configuration	
	D 🛇
	Advanced Bridge Configuration
Bridge BPDU-guard configuration	Enabled  Disabled
Error disable timeout configuration	○Enabled  ●Disabled
Interval (101000000 sec), Default: 300	300
	<b>⊘</b> Apply Cancel

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.

~	Advance	ed Per Port C	onfiguration		0
	Edit	Port	Portfast Configuration	BPDU-guard Configuration	
	V	ge1	Disabled <b>•</b>	Default 🔻	Cancel
		ge2	Disabled	Default	
		ge3	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.

V	VLAN Setting						
`	<ul> <li>VLAN Setting</li> </ul>		<b>C</b>				
	Edit	VLAN ID	VLAN Name				
		500	TestVLAN				

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.

VLA	▼ VLAN Port VLAN ID 500 ▼							
Ĭ	VLAN Port     Edit	Port	VLAN Member	Tagged / Untagged				
	<b>X</b>	ge1	⊖Yes ●No	Tagged ▼ Tagged	<ul><li>☑ Apply</li><li>X Cancel</li></ul>			
		ge2	No	Untagged				
		ge3	No	Tagged				
		ge4	No	Tagged				
		ge5	No	Tagged				

## **Port Setting**

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

Port Setting							
VLAN Port Setting							
Edit	Port	Mode	PVID	User Priority	0		
<b>X</b>	ge1	access ▼ access	1	0 •	Cancel		
	ge2	trunk hybrid	1	0			
	ge3	access	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 community isolated
☑ Apply	Cancel

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	XCancel			

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	
	<b>⊘</b> Apply <b>X</b> Cancel	

### 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.

					e
Edit	Rule	MAC Address (in HHHH.I	HHHH.HHHH format)	VLAN I	dentifier
	1	9465.9cfe	.9709	5	500
Edit	Rule	IPv4 address (in A.B	.C.D/E format)	VLAN Ide	ntifier
	2	10.10.10.1	0/24	600	)
	Based VLAN				

			e	
Edit	Edit Group (1-16)		Rules	
		10	1	
AN Classifier Deat	C-ttine			
LAN Classifier Port	Setting		0	
LAN Classifier Port : Edit	Setting Port	Group (1-16)	+ VLAN	

# 10 QOS

# **Global Configuration**

To enable QoS, 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).

Global Configuration					
V QoS					
		0			
	QoS				
QoS	Enabled     Isabled				
Trust	Cos dscp				
Policy	●strict ●wdrr ●wrr				
	Cancel Cancel				

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

Veighted Round Robin					
Edit	Queue	Weight (1~20)			
	0	1			
	1	1			
	2	2			
	3	2			
	4	4			
	5	4			
	6	8			
	7	8			

.1p Priority				
Edit	VLAN Priority	Queue		
	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 •				
_					
		<b>⊘</b> Apply <b>X</b> Cancel			
			Å		

Interfac	e					
✔ QOS Interface Tail-Drop Threshold						
port ge1	•					
V QOS I	nterface Tail-Drop Thres	hold				
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.

DSC	CP			
<b>v</b> D	DSCP			
	Edit	DSCP Priority	Queue	0
	1	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** Configuration

In order 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.

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)
		10	permit	10.10.10.10	0.0.0.0

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

V IP Access List (Extended)									
									<b>()</b>
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.

🗸 Classmap	Match ACL		
match acce	ss-group ▼		
V access	group		
			Đ
Edit	Applied Class Name	Access Group Number (1-199, 1300-2699)	
	Sample_name	10	

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

V 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.

~	<ul> <li>ACL Port Attach</li> </ul>			
	Edit	Port	ACL Attached	
		ge1	None	
	Ø	ge2	None   None	Cancel
		ge3	Sample_policy	
		ge4	None	

# **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			
	<ul> <li>Global DHCP Server</li> </ul>			
				0
		Global D	HCP Server	
	Global Status	●Enabled ●Disabled		
	Restart DHCP Server	Restart		
		<b>⊘</b> 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.

✓ DHCP Server setting								
								6
	Interface		Start IP	END IP	Subnet Mask	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 has been allocated to which DHCP clients.

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

# **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.

N	TP Config	uration		
~	<ul> <li>NTP Setting</li> </ul>			
				<b>6</b>
			NTP Setting	
	NTP Status	●Enabled ●Disabled		
	Sync Time	Sync		
			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		
		<b>()</b>
Edit	Server IP	
	192.168.1.2	
	10.10.10	

# 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	Daylight Saving Time Setting				
<ul> <li>✓ Daylight Saving Time Setting</li> <li>DST Mode disable ▼</li> </ul>					
✓ Daylig date ne Setting weekday					
weekday	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.

<b>V</b> D	aylight Saving Time Setting	
DST	Mode date 🔻	
~	Daylight Saving Time Setting	
		Ø
		Daylight Saving Time Setting
	Current DST Mode	disable
	DST Timezone Name (3-6 chars)	
	DST Offset (1-480 mins)	
	DST Start Month	
	Date	
	Hour	
	Minute	
	DST End Month	
	Date	
	Hour	
	Minute	

✓ Daylight Saving Time Setting

DST Mode weekday 🔻

✤ Daylight Saving Time Setting

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						

0

# **Radius Configuration**

By default, the 802.1X function is globally disabled on the EtherWAN switch. If you want to use the 802.1X port based 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."

Ra	adius Config	guration		
~	<ul> <li>Radius Server Glob</li> </ul>	oal Setting		
			Radius Server Global Setting	
	Radius Status	●Enabled ●Disabled		
			☑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.

Radius Configuration				
Radius Server IP	Radius Server Port (default:1812)	Secret Key	Timeout <1-1000>	Retransmit <1-100>
		Apply XCancel		
				li li

## **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.

Port	Auth	nentication						
✔ 80	)2.1x Por	t Setting						
Edi	t Por	t Authentication State	Port Enabled	Port Control	Port Status	Periodic Reauthentication	Reauthentication Period(default: 3600)	œ
	ge1	Disable						
	ge2	Disable						
\$	geB	Enable 🔻	false	force-authorized •	Authorized	Enable 🔻	2147483647	Cancel

# 15 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.

şs
0
LLDP General Settings
Disabled <b>v</b>
4
30
All       Port Description       System Name       System Description       System Capabilities         Management Address       Port VLAN ID       MAC/PHY Configuration/Status         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	LDP Port Settings										
🗸 LLDI	P Port S	etting									
						0					
E	dit	Port	Link Status	Transmit	Receive	Notify					
(		ge1	down	Disabled	Disabled	Disabled					
0		ge2	down	Disabled	Disabled	Disabled					
0		ge3	down	Disabled	Disabled	Disabled					
(		ge4	down	Disabled	Disabled	Disabled					
0		ge5	down	Disabled	Disabled	Disabled					
0		ge6	down	Disabled	Disabled	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.

DP Statistics		
<ul> <li>LLDP Device Statisti</li> </ul>	:5	
		•
		LLDP Device Statistics
Last Update	0	
Total Inserts	0	
Total Deletes	0	
Total Drops	0	
Total Ageouts	0	

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

Port	Tx Total		Discards		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).

LLDP Nei	ghbors				
✓ LLDP Neig	hbors				0
Port	System Name	Chassis ID	Port ID	IP Address	ΠL

# **16 Routing**

## **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.

Static l	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			727707273)

# Route Table

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

Route Table							
✔ Route Table							
Destination	Gateway	Genmask	Flags	Metric	Ref	Use	lface
192.168. <mark>1</mark> .0	0.0.0.0	255.255.255.0	U	0	0	0	vlan1.1
192.168.2.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0

# **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	
		li li

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

•	🗸 Route Map			
				<b>• •</b>
	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	
Route Map	Rincewind permit 100 🔻	
Match/Set	Match      Set	
Option	●Interface      ●Metric      □IP	
Interface	ge1 v	

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

oxy ARP			
Proxy ARP			
Ø	vlan1.1	Disabled ▼ Enabled	Can
	vlan1.2	Disabred	
	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.

To configure VRRP:

• Click the edit icon.

- 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.

RRP		
Add VRRP		
		00
	Add VRRP	
VRID (1-255)		
Interface	V	
Accept Mode	True 🔻	
Advertisement Interval (1-10)		
Circuit Interface	ge1 v	
Circuit Failover Priority (1-253)		
Preempt	True 🔻	
Configured Priority (1-255)		
Switch Back Delay (1-500000)		
Virtual IP		
Status	Enable •	

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

~	VRRP Table											
												•
E	dit	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

### **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".

IP General Setting	
✓ Route RIP	
Route RIP	
Route RIP	○Enabled ●Disabled
Version	2
Default-Information	○Enabled ●Disabled
Default Matrix (1~16) Default:1	1
Distance	120
Routing Table Update Timer (5~2147483647) Default:30s	30
Routing Information Timeout Timer (5~2147483647) Default:180s	180
Garbage Collection Timer (5~2147483647) Default:120s	120

### **RIP Port Setting**

In order for a port to be displayed on this screen, the interface must first be added on the <u>RIP</u> <u>Network by 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.
- 8. If the Authentication Mode is MD5 or Simple Password, set the Authentication Key (1 16 characters).
- 9. Click "Apply."

IP P	ort Set	tting									
🗸 Edit	t Interface										
Edit	Edit Interface	Link Status	Line Protocol	Receive Version	Receive Packet	Send Version	Send Packet	Split Horizon	Authentication Mode	Authentication Key	G
¥.	ge10	down	down	1 •	Enable 🔻	1 •	Enable 🔻	Poison Reverse <b>v</b>	Disable •		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."

RIP Network		
✓ RIP Network by Sub	net	
		0
Edit	Subnet Address	Prefix Length

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

RIP Network by Interface							
	• •						
Edit	Port						
	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.

R	IP Neighbor		
`	<ul> <li>RIP Neighbor</li> </ul>		80
	<b>E</b> 11		
	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.

RIP Passive	
✓ RIP Passive	
	<b>⊕</b> (
Edit	Interface

### **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 Redistribu	ute					
✓ RIP Redistribute						
						• •
Edit	Index	Protoc	ol	Metric	Route Ma	ар
RIP Redistribute						
Index	Proto	ocol	Metric		Route Map	
	connec	ted 🔻	•			
				Cancel		
						4

# 18 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.
- 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		00
12	NMP General Setting	
SNMP Status	Enable	
Discription	24 GbE + 4 10GbE 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	
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		

### 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 a NMS to change the status of a data item in the switch.

NMP 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 user name. Set the Access mode to **Read Only** or **Read/Write**. Then click "Apply."

SN	MP v3					
~	SNMP V3 Add User					
SN	NMP Version SNMP	v3 No-Auth	v			
	SNMP V3 Add Us	ser				
						0
				SNMP V3 Add Us	er	
	User Name					
	Access Mode	Read Only				
~	SNMP V3 Setting					
						Θ
I	dit User Name	Access Mode	Security Level	Authentication Type	Authentication Password	Privacy Pass Phrase

# **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 224.0.0.6 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 OSFP 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, click the edit icon in the first panel, and 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	
OSPF General Setting	0
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	Mask (A.B.C.I	)) Prefix Lengtl	h 🛛 Area ID	Instance ID
OSPF Network							
Network Number (i.i.i.i)	Network Mask Type Subnet Mask 🔻	Subnet Mask	(A.B.C.D)	Prefix Length	Area ID		nstance ID
Subnet Mask							

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						
Tir	mers Link State Advertisement (LSA) 🔻						
	Link State Advertisement (L	LSA)					
			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 to be applied next to the filter type.

#### OSPF Advanced Setting

V OSPF Distribute Filter List

	00
OSPF D	Distribute Filter List
Incoming Routing Updates Access List	None
Outgoing Connected Routing Updates Access List	None
Outgoing Kernel Routing Updates Access List	None
Outgoing OSPF Routing Updates Access List	None
Outgoing RIP Routing Updates Access List	None
Outgoing Static Routing Updates Access List	None

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 Ne	eighbor Router			
				<b>()</b>
Edit	OSPF Neighbor Router	Cost (1~65535)	Dead Router Poll Interval (0~214748364	7) Priority (0~255)
OSPF Neighb	or Router			
OSPF Ne	eighbor Router	Cost (1~65535)	Dead Router Poll Interval (0~2147483647)	Priority (0~255)
		_		
			Apply 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.

✓ OSPF Stub Host IP		<b>G</b> (B)
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)
	☑Apply XCancel	
		4

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.

<ul> <li>OSPF Routes Administrative</li> </ul>	Jistance	
	OSPF Routes Administrative Distance	
External Routes	0	
Inter-Area Routes	0	
Intra-Area Routes	0	
Disable OSPF Distance	Disable	
	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	tance Value	2		
				<b>+</b> (2)
Edit	Index	Distance Value	IP Source Prefix (A.B.C.D/M)	Access List Name
OSPF Distand	ce Value			
Index		Distance Value	IP Source Prefix (A.B.C.D/M)	Access List Name
			Cancel	
				li li

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 Con	itrol
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)
<b>⊘</b> Apply Cancel	Soft(Gives Warning) 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 Interface	2			00
Edit	Passive Interface		Interface Address (A.B.C.D)	
Passive Interface				
	Passive Interface		Interface Address (A.B.C.D)	
	eth0 🔻			
		€Ар	oly XCancel	

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)		
			<b>•</b>			
		Cano XCano	el			
				4		

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 (OSPF, connected, kernel, RIP, static route). Enter the OSPF Process ID, Metric Value, and Metric Type. Finally, specify the route map reference and the tag value. Click "Apply when finished.

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 •		

### **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

OSPF Area Configuration	
✓ OSPF Area Config	
	0
	OSPF Area Config
OSPF Area ID (0~4294967295)	
Authentication	<b></b>
Set Summary-Default Cost (1~16777215)	
Name of Filter Access List	
Filter networks between OSPF areas	<b>v</b>
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 Filter networks sent from this area by prefix-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 is 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.

(2) (2)
rea Virtual Link
Ψ

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).

OSPF	Area Nssa
DSPF 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 🔻

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.

		Ø
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)	<b>v</b>	

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					
				G		
	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	
V OSPF Interface Summary	
Port ge1 •	
✓ OSPF Interface Summary	
•	
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.

✔ Int	Interface Message Digest Key						
Port	Port ge15 V						
~	✓ 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.

OS	PF Interface Configuration With Address						
-	<ul> <li>✓ OSPF Interface Summary</li> <li>Port ge1 ▼</li> </ul>						
	<ul> <li>OSPF Interface Summary</li> </ul>	0					
	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.

🗸 Int	✓ Interface OSPF Statistics						
port	port ge1 🔻						
~	✓ Interface OSPF Statistics						
	Edit         Index         Interface Address         Statics						

# **20 PIM (Protocol Independent Multicast)**

### **Global Configuration**

Protocol Independent Multicast (PIM) is a family of multicast routing protocols (MRP). There are two PIM modes: Sparse (PIM-SM) and Dense (PIM-DM).

PIM works with any unicast routing protocol to get route information to a Rendezvous Point (RP) and source. PIM neighbors are established through the exchange of Hello messages. A Designated Router (DR) is chosen in the subnet connected to the receivers. The DR sends periodic Join/Prune messages toward a group-specific RP for each group where there are active members.

To configure PIM globally, click the edit icon and enter values for the following fields:

- 1. Register accept filter at RP
- 2. Join/Prune timer
- 3. Rate limit for PIM Registers
- 4. Source address for PIM Register (A.B.C.D or Interface)
- 5. Register Suppression for PIM Registers
- 6. Source-tree switching threshold

Click "Apply" when finished.

Global Configuration	
V Global Configuration	
	00
Global Configuration	
Register accept filter at RP <100~199, 2000~2699>	
Join/Prune timer <1-65535>	
Rate limit for PIM Registers <1-65535>	
Source address for PIM Register (A.B.C.D or Interface)	
Register Suppression for PIM Registers <1-65535>	
Source-tree switching threshold <1~99, 1300~1999>	

### **Interface Configuration**

To configure PIM on an interface, click the add icon and enter values for the following fields:

- 1. Port
- 2. PIM Mode
- 3. Passive mode

- 4. IP Address
- 5. Hello message interval (default:30)
- 6. Hello message holdtime (default:105)
- 7. Border of PIM domain
- 8. Exclude Gen-id
- 9. Peering Filter (1~199/1300~2699)
- 10. State-Refresh interval (default:60)
- 11. Enable unicast BSM

Interface (	Configu	ratior	1				
✓ Interface Cor	nfiguration						<b>(</b> )
Edit Port	IM Passive ode mode		Hello message interval (default:30)	Hello message holdtime (default:105)	Exclude Gen-id	State-Refresh interval (default:60)	Enable unicast BSM

### **PIM-SM RP Configuration**

A Rendezvous Point (RP) is where sources and receivers of multicast data meet. Sources send traffic to the RP, which is then forwarded to receivers along a shared distribution tree. When the first hop router of the receiver learns about the source, it creates a source-based distribution tree by sending a join message to the source.

The first panel on this screen is RP General Configuration (sparse mode). To configure a PIM Sparse Mode RP, click the edit icon, and enable/disable the RP Ignore Priority and Enable RP Reachability Check for PIM registers fields. Then set the KeepAliveTimer at RP value. Click "Apply" when finished.

M-SM RP Configuration		
RP General Config		
		00
RI	P General Config	
RP Ignore Priority	Disable	
Enable RP reachability check for PIM Registers	Enable	
KAT for (S,G) at RP from PIM Registers <1-65535>		

The second panel is Anycast Rendezvous-Point. Use it to set the Anycast RP address and Anycast Member RP address.

Edit Anycast RP address (A.B.C.D) Anycast member RP address (A.B.C.D)			Rendevzous-Point	✓ Anycast Ren
Edit Anycast RP address (A.B.C.D) Anycast member RP address (A.B.C.D)	€0			
		Anycast member RP address (A.B.C.D)	Anycast RP address (A.B.C.D)	Edit

The third panel is Candidate Bootstrap Router (Candidate BSR). Routers learn RP information from the BSR. Click the add icon, and enter the Interface name, The Hash Mask length, and the Priority value for candidate BSR. Click "Apply" when finished.

•	🗸 Can	didate bootstrap rou	uter (candidate BSR)	
				<b>O</b>
	Edit	Interface name	Hash Mask length for RP selection <0-32>	Priority value for candidate bootstrap router <0-255>

The fourth panel is for configuring the RP. Enter the IP address of the RP, the access list number or name, and enable/disable the switch's ability to override dynamically learned RP mappings.

~	PIM RP-address (Rendezvous Point)		
			<b>O</b>
Ec	lit IP address of Rendezvous-point (A.B.C.D)	ZebOS access-list number/name	Overrides dynamically learned RP mappings

The fifth and final panel is a read only panel that shows existing RPs and interfaces.

0
me
Nai

### **PIM-SM SSM Configuration**

PIM Source-Specific Multicast (PIM-SSM) builds trees that are rooted in a single source. Configure a source specific multicast by clicking the edit icon, and selecting a source from the drop-down list. Click "Apply" when finished.

PIM-SM SSM Configuration	
✓ PIM SSM Configurations	
	0
PIM SSM Configurations	
Configure Source Specific multicast	
<b>⊘</b> Apply Cancel	

## **PIM-SM Neighbor Table**

This is a read-only table that shows the current information for all PIM-SM neighbors.

PIM-SM Neighbor Tabl	le				
<ul> <li>PIM Neighbor Information</li> </ul>					0
Neighbor Address	Interface	Uptime/Expires	Ver	DR Priority	DR Mode



### **Contact Information**

### EtherWAN System, Inc.

www.etherwan.com

m Office
ley 6, Lane 235, Baoqiao Rd.
ict, New Taipei City 231
6629-8986
etherwan.com.tw
r

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 2018. All Rights Reserved. All trademarks and registered trademarks are the property of their respective owners EG99000 Layer 3 Hardened Managed Ethernet Switch December 11, 2018