



Hardened Managed 8-port 10/100/1000BASE-T +16-port 100/1000BASE SFP +4-port 1G/10G SFP+ Layer 3 Switch

EG97000 Series User's Guide - GUI

FastFind Links

[Introduction](#)

[Installing the Switch](#)

All Rights Reserved

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

Disclaimer of Liability

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

All other trademarks are property of their respective owners.

Warranty

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

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

Products Supported by this Manual:

EG97000 Series

Preface

Audience

This guide is designed for the person who installs, configures, deploys, and maintains the Ethernet network. This document assumes the reader has moderate hardware, computer, and networking skills.

Document Revision Level

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

Revision	Document Version	Date	Description
A	Version 1	10/08/2018	
A	Version 2	04/28/2020	Added note to duplex/speed configuration
A	Version 3	10/29/2020	Added console port pin definitions

Changes in this Revision




This is second 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.
	Tip	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
100/1000BASE-TX Ports	12
1 Gbps SFP+ Slots	12
1/10 Gbps SFP+ Slots	12
Connecting Power	12
Terminal Block.....	12
Relay Output Alarm	13
Initial Configuration.....	13
Copy Configuration to USB.....	13
Alternate (Backup) Firmware	13
2 Web Management Interface	14
About the Web-based graphical user interface (GUI)	14
Default IP Address	14
Login Process and Default Credentials.....	14
Navigating the GUI	16
3 System Menu	18
System Information	18
System Name.....	19
System Password.....	19
IP Address.....	19

IPV6 Address	20
System Time	21
Management Interface.....	22
Configuration	22
Saving Switch Configuration	22
Firmware Upgrade.....	23
Reboot	24
User Account.....	24
Command Privilege	25
4 Diagnostics Commands	27
System Utilization.....	27
System Log	29
RMON Statistics.....	30
Remote Log Setting.....	30
Alarm Setting.....	31
Port Mirroring	34
Email Alert.....	35
5 Port Commands	36
Port Configuration	36
Port Status	37
Flow Control.....	38
Rate Control.....	39
6 Switching	40
MAC Table	40
Static MAC Entry	41
Storm Control.....	41
Storm Detect	42
Trunking	43
LACP Trunking.....	43
GVRP	44
GMRP	45

VLAN Translation	46
7 IGMP	47
IGMP Configuration	47
IGMP Snooping	49
8 STP	50
Spanning Tree Protocol (STP)	50
Rapid Spanning Tree protocol (RSTP)	50
Multiple Spanning Tree Protocol (MSTP)	50
Global Configuration	50
RSTP Port Setting	51
MSTP Properties	52
MSTP Instance Setting	52
MSTP Port Setting	53
Advanced Setting	54
9 VLAN	56
VLAN Setting	56
Port Setting	56
Private VLAN	57
MAC/Subnet/Protocol Based VLAN	58
10 QOS	60
Global Configuration	60
Interface	61
DSCP	62
11 ACL	63
ACL Information	63
ACL Configuration	63
IP ACL	66
Port ACL Setting	66
12 DHCP	67
DHCP Server	67
DHCPv6 Server	68

DHCP Relay	69
DHCP Snooping	70
13 NTP	71
NTP Configuration	71
Daylight Saving Time Setting	72
14 SNMP	73
SNMP General Setting	73
SNMP v1/v2	75
SNMP v3	76
15 802.1X	77
Radius Configuration	77
Port Authentication	78
16 LLDP	79
LLDP General Settings	79
LLDP Port Settings	79
LLDP Statistics	80
LLDP Neighbors	81
17 Routing	82
Static Route	82
Route Table	83
Route Map	84
Proxy ARP	85
VRRP	86
18 RIP	88
RIP General Setting	88
RIP Port Setting	89
RIP Route	90
RIP Network	90
RIP Neighbor	91
RIP Passive	91
RIP Redistribute	92

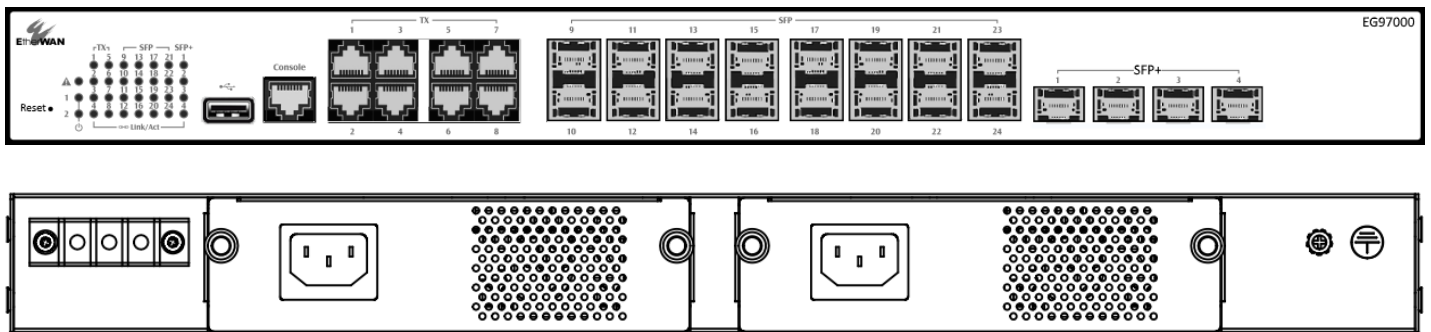
19 RIPng	93
RIPng General Setting.....	93
RIPng Port Setting.....	93
RIPng Route.....	94
RIPng Neighbor.....	94
RIPng Passive.....	94
RIPng Redistribute	95
20 OSPF	96
OSPF General Setting.....	96
OSPF Advanced Setting.....	99
OSPF Area Configuration	103
OSPF Interface Configuration.....	107
OSPF Interface Configuration With Address.....	109
21 OSPFv3.....	111
OSPFv3 General Setting	111
OSPFv3 Advanced Setting	112
OSPFv3 Area Configuration	115
OSPFv3 Interface Configuration.....	118
22 PIM (Protocol Independent Multicast).....	120
Global Configuration.....	120
Interface Configuration	121
PIM-SM RP Configuration	122
PIM-SM SSM Configuration.....	123
PIM-SM Neighbor Table	124
23 AAA (Authentication, Authorization, and Accounting).....	125
TACACS Plus.....	125
24 Contact Information.....	126

1 Introduction

EtherWAN's EG97000 is a gigabit Layer 3 switch designed for high bandwidth uplink or interconnection. With full wire speed switching capability, the EG97000 provides IP routing and switching across VLANs and subnetworks with no compromise in performance. The EG97000 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 Layer 3 features, the EG97000 supports a full set 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 EG97000 supports out-band management via a dedicated RJ-45 Management port.

The EG97000 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 EG97000 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.



Unpacking and Installation

Unpacking

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

- EG97000 Ethernet switch
- 2 Mounting brackets
- 12 Mounting screws
- 1 Console cable
- 1 AC Power Cord (optional)
- Quick install 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

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

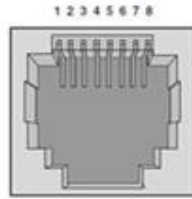
The EG97000 has the following ports:

- 8 x 10/100/1000 Mbps RJ-45 copper ports
- 16 x 100/1000 SFP slots
- 4 x 1/10G SFP+ slots
- 1 x RJ-45 Management port
- 1 x USB port

Console Port

Interface is RJ-45. Pin definitions are as follows:

RJ-45



Pin	Signal	Function
1	3.3V	Connected 0 ohm to RTS signal
2	3.3V/NC	Connected 0 ohm for Backup (NC)
3	TxD	Transmit Data from Switch
4	GND	Ground
5	GND	Ground
6	RxD	Receive Data to Switch
7	NC	Not Connected
8	NC	Not Connected

(Pin 8 of RTS with 3.3vdc for EB-232 dongle device).

10/100/1000BASE-TX Ports

Ports 1 to 8 are gigabit copper ports and can be connected to routers, other switches, or end devices. Use category 5 or higher STP cable.

100 Mbps / 1 Gbps SFP Slots

Ports 9 – 24 are dual-rate gigabit SFP slots, for connection with stackable switches to form multiple fiber interconnections. Use appropriate SFP transceivers.

1/10 Gbps SFP+ Slots

The dual-rate 10G SFP+ ports 1 – 4 are for uplink connection to core networks. 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 EG97000 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 the 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 normally open and normally closed. Relay output current is 30VDC / 0.6A.



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

Initial Configuration

Connect to the switch using the enclosed Ethernet cable to connect a serial port on a PC to the RJ-45 Management port located on the front panel next to the USB port. You can also use regular Ethernet cable to connect the RJ-45 port on the PC to any of the TX ports 1 - 8. The IP address of VLAN 1 is 192.168.1.10.

Configuration via CLI

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

The default login name is “root,” no password.

Configuration via Web Browser

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

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

Copy Configuration to USB

The USB port can be used to save the running switch configuration to a (FAT32) USB storage device. Plug the device into the USB port, and use the “Save Configuration” command in the web interface, or “write config-file usb://FILENAME” in the CLI. You can later load the configuration from the USB drive by navigating to System --> Configuration in the GUI, or using install config-file usb://FILENAME in the CLI.

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

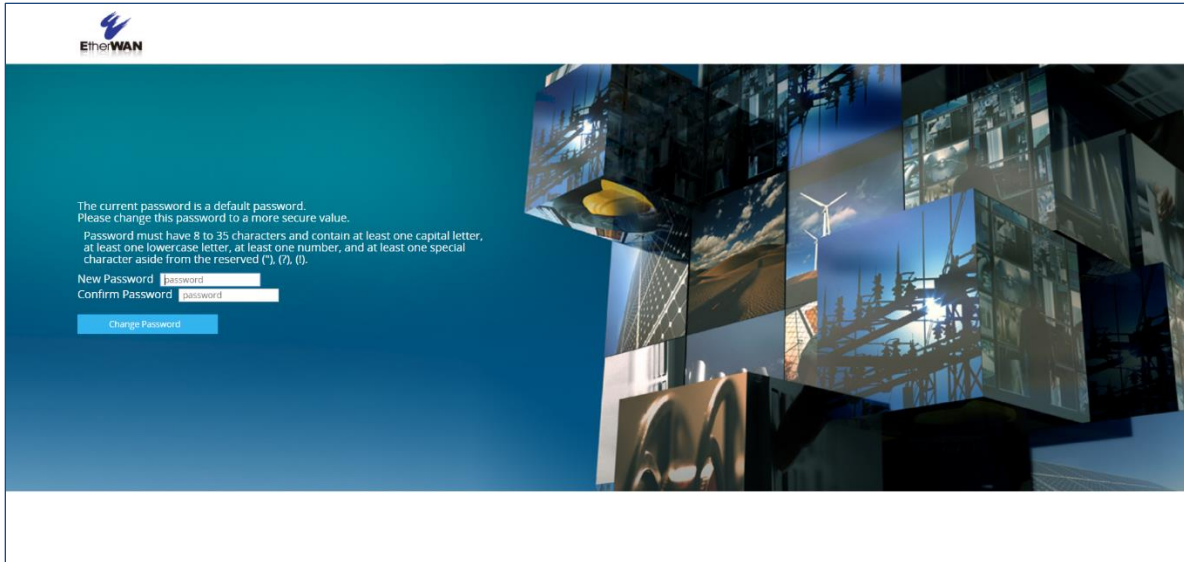
Default IP Address

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



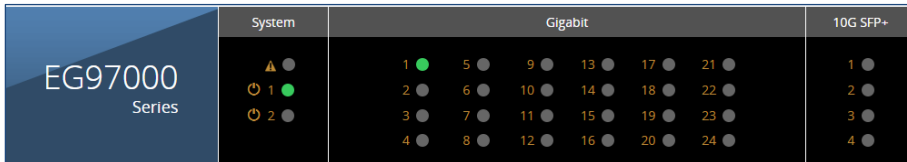
Note: Starting from firmware 3.00.4.5, when logging into the GUI or the CLI for the first time, the switch will prompt you to change the default password to a new one. The new password must meet the following complexity requirements:

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

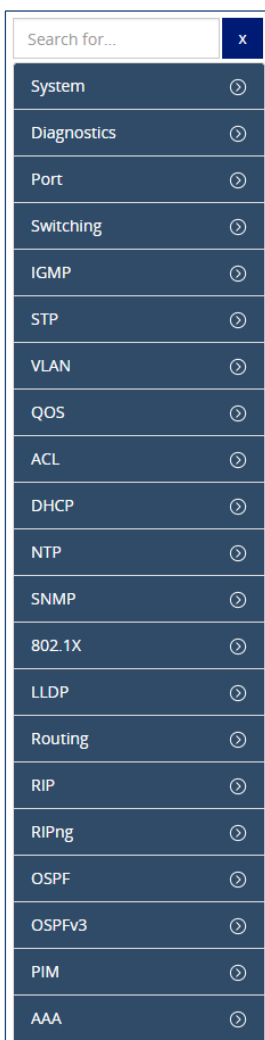
User account will be locked after 10 (configurable) password attempts and will stay locked for 5 minutes.

Navigating the GUI

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



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.



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:

System Information

System Information

System Information	
System Name	EG97000
System Time	Tue Nov 13 14:05:41 UTC 2018
System Uptime	4 days, 20:55
Firmware Version	3.00.0.2 10/26/18 19:11:05
Management IP	192.168.2.10
CPU Utilization	70%

The second panel shows the active and alternate firmware versions.

Firmware Information

Firmware Information	
Active Version	3.00.0.2 10/26/18 19:11:05
Alternate Version	3.00.0.2 10/26/18 19:11:05

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

MAC Address

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.

System Name

System Name

System Name

System Name	EG97000_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 Password


Change Password

New Password	<input type="password"/>	Show
Confirm Password	<input type="password"/>	Show


IP Address

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



IP Address

Static IP 



Edit	VLAN ID	IP Address
<input type="checkbox"/>	1	192.168.1.10/24

DHCP Client 

Edit	Interface	Request	IP Address	Subnet Mask	Default Gateway	DNS Server
<input type="checkbox"/>	Disable					

Default Gateway  

Edit	Default Gateway IP

DNS Server  

Edit	Server IP

IPV6 Address

On this screen, you can add IPV6 addresses to an interface, static IPV6 addresses, and DHCPV6 Client information.

IPv6 Address

▼ Add IPv6 Address

Add IPv6 Address	
Interface	vlan1.1 ▼
IPv6 Address/Prefix	2001:0db8:85a3:0000:c

Apply

▼ Static IPv6 Address

Edit	Interface	IPv6 Address
<input type="checkbox"/>	lo	
<input type="checkbox"/>		::1/128
<input type="checkbox"/>	vlan1.1	
<input type="checkbox"/>		2001:db8:85a3::8a2e:370:7334/64
<input type="checkbox"/>	vlan1.2	
<input type="checkbox"/>		2001:620:40b:555::210/64

▼ DHCPv6 Client

Edit	Interface	Request	IPv6 Address
<input type="checkbox"/>	Disable		

System Time

This page is for manual setting of the system time. Click the edit icon, and enter the time and date data in the corresponding fields. Click “Apply” when finished. To configure a network time server, refer to chapter on [NTP](#).

System Time

▼ System Time

System Time	
Year	2017
Month	05
Day	05
Hour	13
Minute	22
Second	52

Management Interface

Enable / disable access to switch management through http, https, 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.

Management Interface

Management Interface

Management Interface	
WEB Agent	http
Telnet	Disabled
SSH	Disabled



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

Configuration

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

Configuration

Auto Save Configuration

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

Save/Load Configuration File	
Action	<input checked="" type="radio"/> Save <input type="radio"/> Load
via	<input checked="" type="radio"/> TFTP <input type="radio"/> USB
Filename	<input type="text"/>
TFTP Server IP	<input type="text"/>
Path (Optional)	<input type="text"/>
Port (Optional)	<input type="text"/>

Apply

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.

Firmware Upgrade

Via TFTP Server

Via TFTP Server	
Filename	<input type="text" value="eg97000.tar.xz"/>
TFTP Server IP	<input type="text"/>

Apply

Via web

Please select image to upgrade:

No file chosen

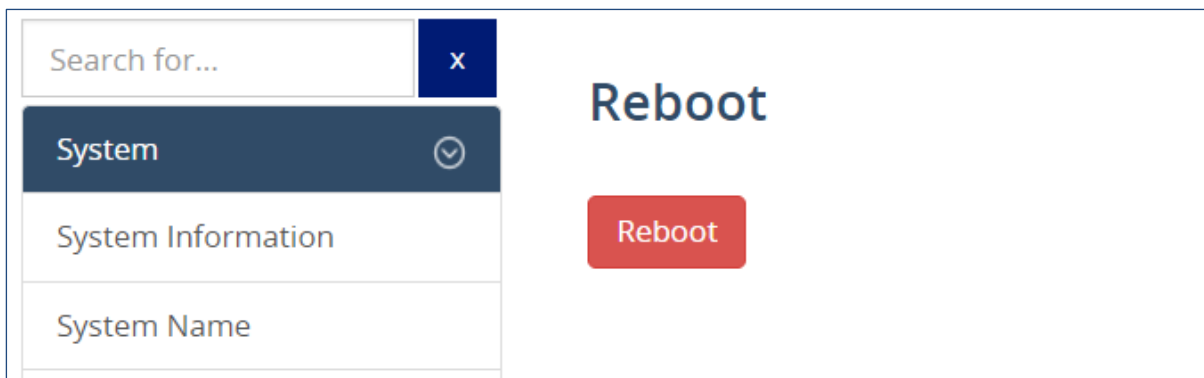
To upgrade the switch firmware:

1. Log in to the switch and navigate to System → Firmware Upgrade.

2. Enter the filename and TFTP server address and click apply, OR select the file manually with the **Choose File** button.
3. It will take several minutes to install the new firmware.
4. Click the **Reboot** button when you see the message “Firmware upgrade successful.” (Do not power off the switch or the firmware upgrade will fail)
5. Wait 90 seconds (60 seconds for switch reboot, and 30 seconds for system verification) and re-log in to the switch. Check the System Information screen to ensure that the firmware upgrade has been successful.

Reboot

Reboot the switch.



User Account

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

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

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

User Account

▼ Login Mode ✎ ↺

Login Mode	
Mode	<div style="border: 1px solid #ccc; padding: 2px;"> Single-user ▼ <div style="background-color: #fff; border: 1px solid #ccc; padding: 2px; margin-top: 2px;"> Single-user Multi-user TACACS </div> </div>

✔ Apply
Cancel

▼ User Account + ↺

Edit	User Name	Privilege Level

Command Privilege

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

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

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

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

Command Privilege

▼ Command Privilege




Edit	Command Group	Technician	Operator
<input type="checkbox"/>	System-Name&Password	Hide	Hide
<input type="checkbox"/>	IP-Address	Read-only	Read-only
<input type="checkbox"/>	Management-Interface	Read-only	Read-only
<input type="checkbox"/>	Save-Configuration	Hide	Hide
<input type="checkbox"/>	Firmware-Upgrade	Hide	Hide
<input type="checkbox"/>	Reboot	Hide	Hide
<input type="checkbox"/>	Remote-Log	Read-only	Read-only
<input type="checkbox"/>	User-Account	Read-only	Read-only
<input type="checkbox"/>	Command-Privilege	Read-only	Read-only
<input type="checkbox"/>	Alarm-Setting	Read-only	Read-only
<input type="checkbox"/>	Email-Alert	Read-only	Read-only
<input type="checkbox"/>	Port-Mirroring	Read-only	Read-only
<input type="checkbox"/>	Configuration	Read-only	Read-only
<input type="checkbox"/>	Flow-Control	Read-only	Read-only
<input type="checkbox"/>	Rate-Control	Read-only	Read-only

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.

System Utilization

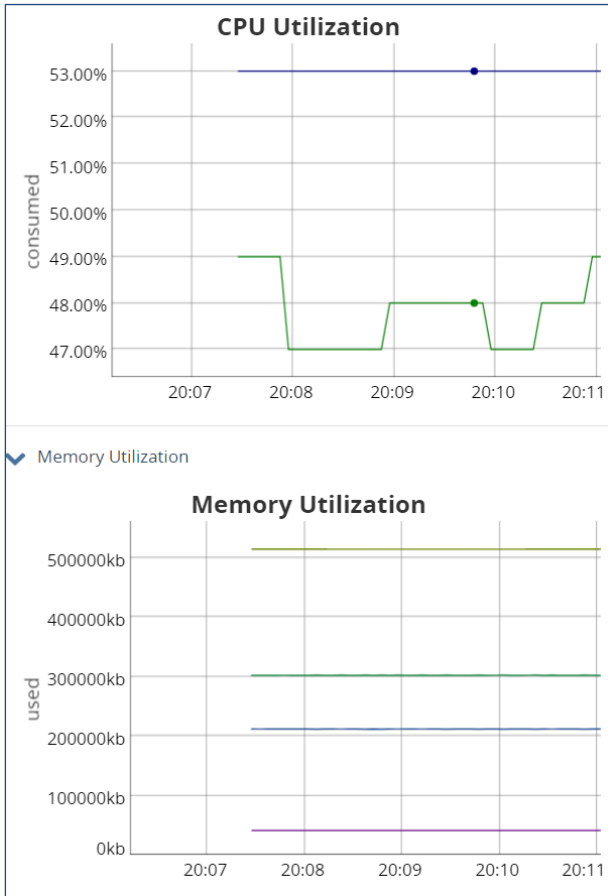
▼ CPU Utilization 

CPU Utilization	
Current utilization	49%
Max utilization	53%

▼ Memory Utilization 


Memory Utilization	
Total	513664
Used	211640
Free	302024
Cached	41052

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



System Log

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

System Log				
System Log 				
Index	Date	Time	Severity	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.

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 Log Setting

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

Remote Log Setting

Remote Logging ✎ ↻

Remote Logging	
Status	Enabled

Log Server IP List + ↻

Edit	Log Server IP
<input type="checkbox"/>	192.168.1.75

Alarm Setting

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


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, and either power input (if dual power inputs are used).

Alarm Setting

Basic SFP SFP RX SFP TX

Alarm Trigger Link 

Edit	Port	Enabled	Status
<input checked="" type="checkbox"/>	ge1	No ▾	Link-down
<input type="checkbox"/>	ge2	No	Link-down
<input type="checkbox"/>	ge3	No	Link-down
<input type="checkbox"/>	ge4	No	Link-down
<input type="checkbox"/>	ge5	No	Link-down
<input type="checkbox"/>	ge6	No	Link-down
<input type="checkbox"/>	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 voltage.


Alarm Setting

Basic


SFP

SFP RX

SFP TX

Alarm Trigger SFP Vcc Major 

Edit	PORT	Enabled	Status
<input type="checkbox"/>	ge9	No	Vcc:SFP Module none detect (Major)
<input type="checkbox"/>	ge10	No	Vcc:SFP Module none detect (Major)
<input type="checkbox"/>	ge11	No	Vcc:SFP Module none detect (Major)
<input type="checkbox"/>	ge12	No	Vcc:SFP Module none detect (Major)
<input type="checkbox"/>	ge13	No	Vcc:SFP Module none detect (Major)
<input type="checkbox"/>	ge14	No	Vcc:SFP Module none detect (Major)
<input type="checkbox"/>	ge15	No	Vcc:SFP Module none detect (Major)
<input type="checkbox"/>	ge16	No	Vcc:SFP Module none detect (Major)
<input type="checkbox"/>	ge17	No	Vcc:SFP Module none detect (Major)

Alarm Trigger SFP Vcc Minor 

Edit	PORT	Enabled	Status
<input type="checkbox"/>	ge9	No	Vcc:SFP Module none detect (Minor)
<input type="checkbox"/>	ge10	No	Vcc:SFP Module none detect (Minor)
<input type="checkbox"/>	ge11	No	Vcc:SFP Module none detect (Minor)
<input type="checkbox"/>	ge12	No	Vcc:SFP Module none detect (Minor)
<input type="checkbox"/>	ge13	No	Vcc:SFP Module none detect (Minor)
<input type="checkbox"/>	ge14	No	Vcc:SFP Module none detect (Minor)
<input type="checkbox"/>	ge15	No	Vcc:SFP Module none detect (Minor)
<input type="checkbox"/>	ge16	No	Vcc:SFP Module none detect (Minor)
<input type="checkbox"/>	ge17	No	Vcc:SFP Module none detect (Minor)

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


Alarm Setting

Basic

SFP


SFP RX

SFP TX

Alarm Trigger SFP RX-Power Major 

Edit	PORT	Enabled	Status
<input type="checkbox"/>	ge9	No	Rx Power:SFP Module none detect (Major)
<input type="checkbox"/>	ge10	No	Rx Power:SFP Module none detect (Major)
<input type="checkbox"/>	ge11	No	Rx Power:SFP Module none detect (Major)
<input type="checkbox"/>	ge12	No	Rx Power:SFP Module none detect (Major)
<input type="checkbox"/>	ge13	No	Rx Power:SFP Module none detect (Major)
<input type="checkbox"/>	ge14	No	Rx Power:SFP Module none detect (Major)
<input type="checkbox"/>	ge15	No	Rx Power:SFP Module none detect (Major)
<input type="checkbox"/>	ge16	No	Rx Power:SFP Module none detect (Major)
<input type="checkbox"/>	ge17	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 Trigger SFP TX-Bias Major 

Edit	PORT	Enabled	Status
<input type="checkbox"/>	ge9	No	Tx Bias:SFP Module none detect (Major)
<input type="checkbox"/>	ge10	No	Tx Bias:SFP Module none detect (Major)
<input type="checkbox"/>	ge11	No	Tx Bias:SFP Module none detect (Major)
<input type="checkbox"/>	ge12	No	Tx Bias:SFP Module none detect (Major)
<input type="checkbox"/>	ge13	No	Tx Bias:SFP Module none detect (Major)
<input type="checkbox"/>	ge14	No	Tx Bias:SFP Module none detect (Major)
<input type="checkbox"/>	ge15	No	Tx Bias:SFP Module none detect (Major)
<input type="checkbox"/>	ge16	No	Tx Bias:SFP Module none detect (Major)
<input type="checkbox"/>	ge17	No	Tx Bias:SFP Module none detect (Major)
<input type="checkbox"/>	ge18	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	To	Mode
ge1 ▼	ge1 ▼	both ▼

Apply Cancel

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

Port Mirroring

▼ Port Mirroring

Edit	From	To	Mode
<input type="checkbox"/>	xe2	ge3	both
<input type="checkbox"/>	ge1	ge2	transmit
<input type="checkbox"/>	ge7	ge8	receive

Email Alert

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

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

To configure mail server and recipient email addresses:

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

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

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

Email Alert

▼ Mail Server

Mail Server	
SMTP Status	Disable
SMTP Server	
Email Address	
Password	
SSL Status	Disable
Delete Server configuration	<input type="button" value="Delete"/>

▼ Mail Recipients

Edit	Recipients Mail Address (Max number: 5)
------	-----------------------------------------

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

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

Edit	Port	Port Type	IP Address	Link Status	Shutdown	Port Description	Duplex/Speed
<input type="checkbox"/>	ge1	Routed port	10.10.10.10/24	Down	No		Auto
<input type="checkbox"/>	ge2	Switch port		Down	No		Auto
<input type="checkbox"/>	ge3	Routed port		Down	No		Auto
<input type="checkbox"/>	ge4	Switch port		Down	No		Auto
<input checked="" type="checkbox"/>	ge5	Switch port ▼	<input type="text"/>	Down	No ▼	<input type="text"/>	Auto ▼
<input type="checkbox"/>	ge6	Switch port		Down	No		Auto
<input type="checkbox"/>	ge7	Switch port		Down	No	Mirrored to ge8	Auto
<input type="checkbox"/>	ge8	Switch port		Down	No		Auto
<input type="checkbox"/>	ge9	Switch port		Down	No		Auto
<input type="checkbox"/>	ge10	Routed port		Down	No		Auto
<input type="checkbox"/>	ge11	Routed port		Down	No		Auto
<input type="checkbox"/>	ge12	Switch port		Down	No		Auto
<input type="checkbox"/>	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 


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 is 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."

Flow Control

▼ Port Flow Control 


Edit	Port	Send Admin	Send Operation	Receive Admin	Receive Operation
<input checked="" type="checkbox"/>	ge1	on ▼	on	on ▼	on
<input type="checkbox"/>	ge2	on	on	on	on
<input type="checkbox"/>	ge3	on	on	on	on
<input type="checkbox"/>	ge4	on	on	on	on
<input type="checkbox"/>	ge5	on	on	on	on
<input type="checkbox"/>	ge6	on	on	on	on
<input type="checkbox"/>	ge7	on	on	on	on
<input type="checkbox"/>	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.

Rate Control

▼ Port 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
<input checked="" type="checkbox"/>	ge1	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
<input type="checkbox"/>	ge2	0	0	0	0
<input type="checkbox"/>	ge3	0	0	0	0
<input type="checkbox"/>	ge4	0	0	0	0
<input type="checkbox"/>	ge6	0	0	0	0
<input type="checkbox"/>	ge7	0	0	0	0



Apply Cancel

6 Switching


MAC Table

The MAC Table page contains a panel for setting the Ageing Time, one for clearing Dynamic, Multicast, 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  

Ageing Time	
Ageing Time (10-1000000)	300

Clear MAC 

Clear MAC	
Clear Dynamic MAC	<input type="button" value="Clear"/>
Clear Multicast MAC	<input type="button" value="Clear"/>
Clear Static MAC	<input type="button" value="Clear"/>

MAC Table 

Index	VLAN	MAC Address	Type	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**.

Static MAC Entry

Static MAC Entry Forward + ↺

Edit	Index	Port	MAC Address (Ex: 0000.1111.2222)	VLAN
<input type="checkbox"/>	1	ge1	0090.4ce3.a80d	1

Static MAC Entry Discard + ↺

Edit	Index	Port	MAC Address (Ex: 0000.1111.2222)	VLAN
------	-------	------	----------------------------------	------

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

Storm Control

Storm Control (Threshold Level:0.01-100 Packet-per-second: 0-8388608)

Edit	Port	Broadcast Threshold Level	Multicast Threshold Level	DLF Threshold Level	Broadcast Packet-per-second	Multicast Packet-per-second	DLF Packet-per-second
<input type="checkbox"/>	ge1	100.00	100.00	100.00	0	0	0
<input checked="" type="checkbox"/>	ge2	<input type="text" value="100.00"/>	<input type="text" value="100.00"/>	<input type="text" value="100.00"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
<input type="checkbox"/>	ge3	100.00	100.00	100.00	0	0	0
<input type="checkbox"/>	ge4	100.00	100.00	100.00	0	0	0
<input type="checkbox"/>	ge5	100.00	100.00	100.00	0	0	0
<input type="checkbox"/>	ge6	100.00	100.00	100.00	0	0	0
<input type="checkbox"/>	ge7	100.00	100.00	100.00	0	0	0
<input type="checkbox"/>	ge8	100.00	100.00	100.00	0	0	0
<input type="checkbox"/>	ge9	100.00	100.00	100.00	0	0	0

Apply Cancel

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

Configuration

Storm-Detect Configuration Enabled Disabled

Interval (2..65535 sec), Default: 10

Errdisable-recovery time (0..65535 sec), 0: no recovery

Apply Cancel

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

By Utilization: Percentage of port's maximum speed

By Broadcast / Multicast+Broadcast: Type of packet to be monitored

Packets Per Second: Threshold for Storm Detect activation

Storm Detect Per Port

Edit	Port	State / Recovery time remains	By Utilization(%) (0-100) 0: not limited	By Broadcast / Multicast+Broadcast	Packets Per Second (0-100000) 0: not limited	
<input checked="" type="checkbox"/>	ge1		<input type="text" value="0"/>	bc	<input type="text" value="0"/>	<input checked="" type="checkbox"/> Apply <input type="checkbox"/> Cancel
<input type="checkbox"/>	ge2		0	bc	0	
<input type="checkbox"/>	ge3		0	bc	0	
<input type="checkbox"/>	ge4		0	bc	0	
<input type="checkbox"/>	ge5		0	bc	0	

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 Trunk

Port	Member
<input type="checkbox"/>	ge1 <input type="checkbox"/> ge2 <input type="checkbox"/> ge3 <input type="checkbox"/> ge4 <input type="checkbox"/> ge5 <input type="checkbox"/> ge6 <input type="checkbox"/> ge7 <input type="checkbox"/> ge8 <input type="checkbox"/> ge9 <input type="checkbox"/> ge10 <input type="checkbox"/> ge11 <input type="checkbox"/> ge12 <input type="checkbox"/> ge13 <input type="checkbox"/> ge14 <input type="checkbox"/> ge15 <input type="checkbox"/> ge16 <input type="checkbox"/> ge17 <input type="checkbox"/> ge18 <input type="checkbox"/> ge19 <input type="checkbox"/> ge20 <input type="checkbox"/> ge21 <input type="checkbox"/> ge22 <input type="checkbox"/> ge23 <input type="checkbox"/> ge24 <input type="checkbox"/> xe1 <input type="checkbox"/> xe2 <input type="checkbox"/> xe3 <input type="checkbox"/> xe4

Apply Cancel



LACP Trunking

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


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

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

LACP Trunking

▼ LACP Configuration  

LACP Configuration	
LACP System Priority (1-65535, default:32768)	32768

▼ Port Status 



Edit	Port	Trunk Port	LACP Mode	LACP Port Priority (Set 0 for None)	LACP Timeout	LACP Sync	
<input checked="" type="checkbox"/>	ge1	po1	active ▼	<input type="text"/>	long ▼	No link	<input type="checkbox"/> Apply <input type="checkbox"/> Delete <input type="checkbox"/> Cancel
<input type="checkbox"/>	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.

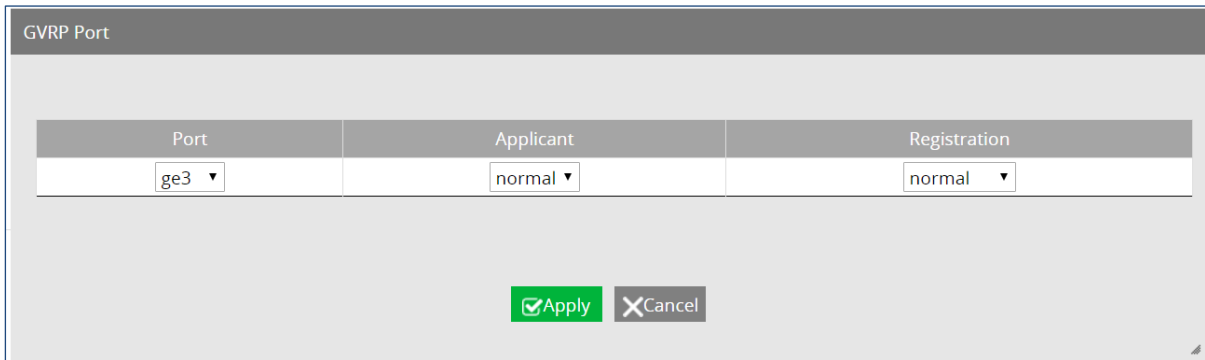
GVRP

▼ GVRP  

GVRP	
GVRP	Disabled
Dynamic VLAN Creation	Disabled

▼ GVRP Port  

Edit	Port	Applicant	Registration
------	------	-----------	--------------



Port	Applicant	Registration
ge3	normal	normal

Add GVRP Port

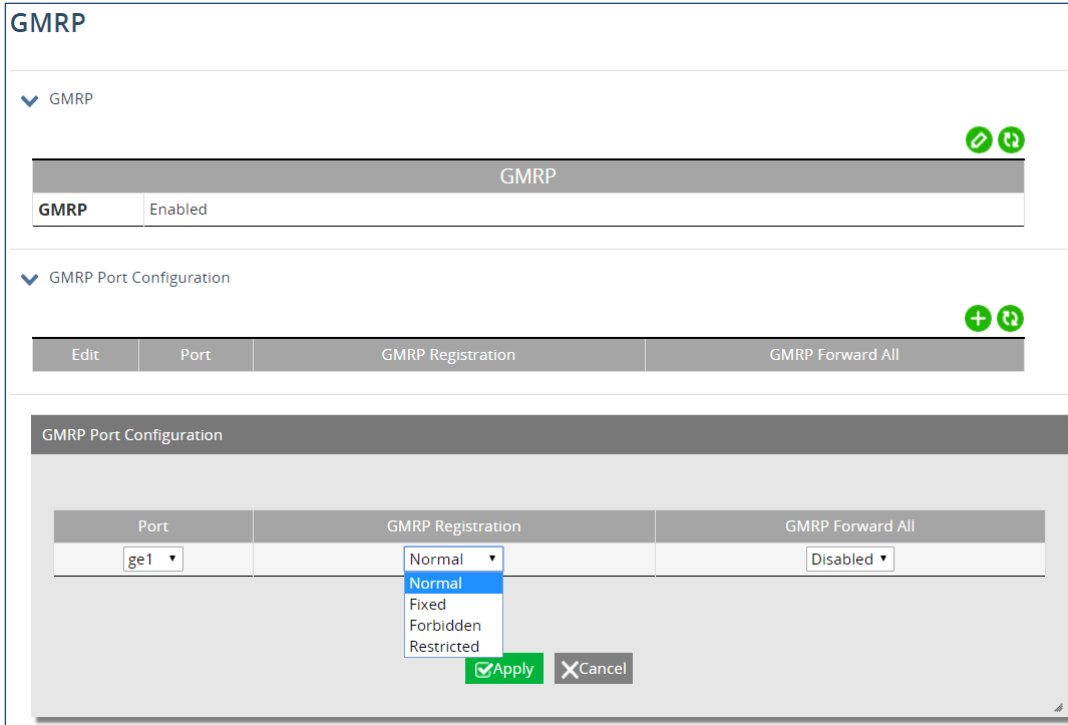
GMRP

The settings in the GMRP feature controls how the switch automates the process of multicast packet forwarding, both within a single switch as well 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 the local switch.

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

- Normal
- Fixed
- Forbidden
- Restricted

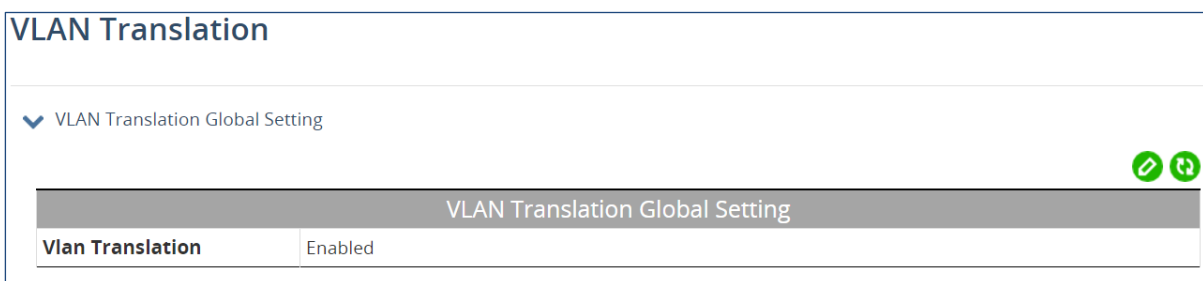
GMRP Forward All can be enabled or disabled when configuring GMRP ports.



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**.



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.”

VLAN Translation			
Port	Ingress/Egress	Translate from	Translate to
ge3 ▾	ingress ▾	<input type="text"/>	<input type="text"/>

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 ✎ ↻	
IGMP Global Setting	
IP Multicast Routing Status	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
IGMP Limit	<input type="text" value="64001"/>
<input checked="" type="button" value="Apply"/> <input type="button" value="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.



IGMP Interface Summary

Port



IGMP Interface Summary 

IGMP Interface Summary	
IGMP Status	Disabled
IGMP Version	3
ProxyService	Disabled
MRoute Proxy	Disabled
Immediate Leave	
IGMP Limit (1~2097152, set to 0 to disable)	0
AccessGroup (1~99, set to 0 to disable)	

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

IGMP Join Group  

Edit	Index	Group Address	Interface	Up Time	Expires	Last Reporter
------	-------	---------------	-----------	---------	---------	---------------

IGMP Clear Group  

IGMP Clear Group	
Clear IGMP Local-Memberships On Interface	
Clear IGMP Local-Memberships	<input type="button" value="CLEAR ALL"/>

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**.


IGMP Snooping

IGMP Snooping  

IGMP Snooping	
IGMP Snooping Mode	Enabled

IGMP Snooping Setting (by VLAN) 

Edit	VLAN ID	IGMP Snooping Status	IGMP Snooping Querier	IGMP Version	Fast Leave	IGMPv1/v2 Report suppression	IGMPv3 Report suppression
<input type="checkbox"/>	1	Enabled	Disabled	3	Disabled	Enabled	Disabled

Forward Ports 

Edit	Forward Mode	Forward Ports
<input type="checkbox"/>	passive-forward	none
<input type="checkbox"/>	force-forward	none

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

Setting

Setting	
Spanning Tree Protocol	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Bridge Priority (0..61440)	<input type="text" value="32768"/>
Hello Time (1..10 sec)	<input type="text" value="2"/>
Max Age (6..40 sec)	<input type="text" value="20"/>
Forward Delay (4..30 sec)	<input type="text" value="15"/>
STP Version	<input type="text" value="RSTP"/>

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.

RSTP Port Setting

▼ RSTP Port Configuration

Edit	Port	Port Status (Role/State)	Priority (Granularity 16)	Admin. Path Cost	Conf. Link Type	Curr. Link Type	Conf. Edge Port	Curr. Edge Port	
<input checked="" type="checkbox"/>	ge1	Disabled / Discarding	<input type="text" value="128"/>	<input type="text" value="20000"/>	<input type="text" value="point-to-point"/>	point-to-point	<input type="text" value="Enabled"/>	Enabled	<input checked="" type="button" value="Apply"/> <input type="button" value="Cancel"/>
<input type="checkbox"/>	ge2	Disabled / Discarding	128	20000	point-to-point	point-to-point	Enabled	Enabled	
<input type="checkbox"/>	ge3	Disabled / Discarding	128	20000	point-to-point	point-to-point	Enabled	Enabled	
<input type="checkbox"/>	ge4	Disabled / Discarding	128	20000	point-to-point	point-to-point	Enabled	Enabled	
<input type="checkbox"/>	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 Properties

Setting

Setting	
Region Name	Default
Revision Level	0
Max Hops	20
Digest	0xAC36177F50283CD4B83821D8AB26DE62
CIST Root ID	800000904ce3a800
CIST Reg Root ID	800000904ce3a800
CIST Bridge ID	800000904ce3a800

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).

MSTP Instance Setting

▼ VLAN Instance Configuration

Edit	VLAN ID	Instance ID (1-63, 0 to delete)
<input type="checkbox"/>	300	1

▼ MSTP Instance Setting

Edit	Instance ID	Bridge Priority (0-61440)	Root ID	Root Port	Root Path Cost	Bridge ID
<input type="checkbox"/>	1	32768	8001000000000000	0	0	8001000000000000

MSTP Port Setting

You can adjust the location of the blocking port in a MSTP network by modifying the **Port Priority** and the **Path Cost** of the ports on the switch. Modifying the **Port Priority** adjusts the blocking port between two switches. Modify the **Port Cost** adjusts the location of the blocking port in a MSTP loop.

First assign ports to an MSTP instance by clicking the check box next to the instance ID, and then the check boxes next to the ports you want to add.

MSTP Port Setting

▼ Port Instance Configuration

Edit	Instance ID	Member
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/> ge1 <input type="checkbox"/> ge2 <input type="checkbox"/> ge3 <input type="checkbox"/> ge4 <input type="checkbox"/> ge5 <input type="checkbox"/> ge6 <input type="checkbox"/> ge7 <input type="checkbox"/> ge8 <input type="checkbox"/> ge9 <input type="checkbox"/> ge10 <input type="checkbox"/> ge11 <input type="checkbox"/> ge12 <input type="checkbox"/> ge13 <input type="checkbox"/> ge14 <input type="checkbox"/> ge15 <input type="checkbox"/> ge16 <input type="checkbox"/> ge17 <input type="checkbox"/> ge18 <input type="checkbox"/> ge19 <input type="checkbox"/> ge20 <input type="checkbox"/> ge21 <input type="checkbox"/> ge22 <input type="checkbox"/> ge23 <input type="checkbox"/> ge24 <input type="checkbox"/> xe1 <input type="checkbox"/> xe2 <input type="checkbox"/> xe3 <input type="checkbox"/> xe4

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.”

MSTP Port Setting

Port Instance Configuration

Edit	Instance ID	Member
<input type="checkbox"/>	1	ge1

MSTP Port Setting

Edit	Instance ID	Port	Port State	Role	Priority	Path Cost	Designated Bridge ID	Designated Port ID	Designated Root ID	Designated Path Cost
<input type="checkbox"/>	1	ge1	Discarding	Disabled	128	20000	800100904ce3a800	838f	000000904ce3a800	0

Advanced Setting

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

- **Bridge bpduguard configuration** - When the BPDU Guard feature is set for a bridge, all portfast-enabled ports of the bridge that have **bpduguard** 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 **bpduguard**.

Advanced Setting

Advanced Bridge Configuration

Advanced Bridge Configuration	
Bridge BPDU-guard configuration	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Error disable timeout configuration	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Interval (10..1000000 sec), Default: 300	<input type="text" value="300"/>

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.

Advanced Per Port Configuration



Edit	Port	Portfast Configuration	BPDU-guard Configuration	
<input checked="" type="checkbox"/>	ge1	Disabled ▾	Default ▾	<input checked="" type="checkbox"/> Apply <input type="checkbox"/> Cancel
<input type="checkbox"/>	ge2	Disabled	Default	
<input type="checkbox"/>	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.

VLAN Setting

▼ VLAN Setting + ↺

Edit	VLAN ID	VLAN Name
<input type="checkbox"/>	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.

▼ VLAN Port

VLAN ID

▼ VLAN Port

Edit	Port	VLAN Member	Tagged / Untagged		
<input checked="" type="checkbox"/>	ge1	<input type="radio"/> Yes <input checked="" type="radio"/> No		Tagged ▼ Tagged Untagged	<input checked="" type="checkbox"/> Apply <input type="checkbox"/> Cancel
<input type="checkbox"/>	ge2	No		Tagged	
<input type="checkbox"/>	ge3	No		Tagged	
<input type="checkbox"/>	ge4	No		Tagged	
<input type="checkbox"/>	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	
<input checked="" type="checkbox"/>	ge1	access ▼ access	<input type="text" value="1"/>	<input type="text" value="0"/>	<input checked="" type="checkbox"/> Apply <input type="checkbox"/> Cancel
<input type="checkbox"/>	ge2	trunk	1	0	
<input type="checkbox"/>	ge3	hybrid 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 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 [VLAN Setting](#) 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
<input type="text"/>	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
<input type="text"/>	<input type="text"/>

In the third panel, configure port status in a private VLAN. Click the add icon, then 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 [VLAN Setting](#) screen.

VLAN Private Port Mode

Switchport	Private VLAN Mode
ge1 ▾	host ▾

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 applying to a protocol, you must also specify the type of packet encapsulation: **ethv2**, **snapllc**, or **nosnapllc**.

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

MAC/Subnet/Protocol Based VLAN

MAC-Based VLAN

Edit	Rule	MAC Address (in HHHH.HHHH.HHHH format)	VLAN Identifier
<input type="checkbox"/>	1	9465.9cfe.9709	500

Subnet-Based VLAN

Edit	Rule	IPv4 address (in A.B.C.D/E format)	VLAN Identifier
<input type="checkbox"/>	2	10.10.10.10/24	600

Protocol-Based VLAN

Edit	Rule	Ethernet Protocol	Ethernet Decimal (0-65535)	Packet Encapsulation	VLAN Identifier
<input type="checkbox"/>	3	decnaremoteconsole - DEC DNA Remote Console		ethv2	500

VLAN Classifier Group

Edit	Group (1-16)	Rules
<input type="checkbox"/>	10	1



VLAN Classifier Port Setting

Edit	Port	Group (1-16)	VLAN
<input type="checkbox"/>	ge5	10	500

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), **wrr** (weighted deficit round robin), or **wrr** (weighted round robin).


Global Configuration

▼ QoS  

QoS	
QoS	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Trust	<input type="checkbox"/> cos <input type="checkbox"/> dscp
Policy	<input type="radio"/> strict <input type="radio"/> wdrd <input checked="" type="radio"/> wrr

✔ Apply
Cancel

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

▼ Weighted Round Robin 

Edit	Queue	Weight (1-20)
<input type="checkbox"/>	0	1
<input type="checkbox"/>	1	1
<input type="checkbox"/>	2	2
<input type="checkbox"/>	3	2
<input type="checkbox"/>	4	4
<input type="checkbox"/>	5	4
<input type="checkbox"/>	6	8
<input type="checkbox"/>	7	8

802.1p Priority ↻

Edit	VLAN Priority	Queue
<input type="checkbox"/>	0	0
<input type="checkbox"/>	1	1
<input type="checkbox"/>	2	2
<input type="checkbox"/>	3	3
<input type="checkbox"/>	4	4
<input type="checkbox"/>	5	5
<input type="checkbox"/>	6	6
<input type="checkbox"/>	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 ▾	<input type="text"/>	<input type="text"/>

Interface

QOS Interface Tail-Drop Threshold

port ▾

QOS Interface Tail-Drop Threshold +

Edit	Tail-Drop Queue	Tail-Drop Min Threshold Percentages	Tail-Drop Max Threshold Percentages
<input type="checkbox"/>	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.

DSCP

▼ DSCP ↻

Edit	DSCP Priority	Queue	
<input checked="" type="checkbox"/>	0	0	<input type="checkbox"/> Apply <input type="checkbox"/> Cancel
<input type="checkbox"/>	1	1	
<input type="checkbox"/>	2	2	
<input type="checkbox"/>	3	3	
<input type="checkbox"/>	4	4	
<input type="checkbox"/>	5	5	
<input type="checkbox"/>		6	
<input type="checkbox"/>		7	
<input type="checkbox"/>		↓	

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

IP Access List

Edit	Index	IP Access List (1-99/1300-1999)	Action	IP address (A.B.C.D)	Mask (A.B.C.D)
<input type="checkbox"/>	1	10	permit	10.10.10.10	0.0.0.0

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

IP Access List (Extended)

Edit	Index	IP Access List (100-199/2000-2699)	Action	Protocol	IANA Assigned Protocol Number	Source Address	Source Wildcard Bits	Destination Address	Destination Wildcard Bits
<input type="checkbox"/>	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

access-group

Edit	Applied Class Name	Access Group Number (1-199, 1300-2699)
<input type="checkbox"/>	Sample_name	10

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

Policy-map Match ACL + ↺

Edit	Policy Map	Class Map Matched
<input type="checkbox"/>	Sample_policy	
<input type="checkbox"/>	Sample_policy	Sample_name

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

ACL Port Attach ↺



Edit	Port	ACL Attached
<input type="checkbox"/>	ge1	None
<input checked="" type="checkbox"/>	ge2	<div style="border: 1px solid #ccc; padding: 2px;"> None ▾ None Sample_policy none </div>
<input type="checkbox"/>	ge3	
<input type="checkbox"/>	ge4	None

Apply
 Cancel


IP ACL

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

IP ACL

▼ Add Access List  

Add Access List	
Type	Standard
Number	
Action	Permit
Source Type	Address
Source Address	
Source Mask	



▼ Access List 

Edit	Number	Action	Rules
<input type="checkbox"/>	99	permit	0.0.0.11 255.255.255.0

Port ACL Setting

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

Port ACL Setting

▼ Port ACL Setting  

Edit	Interface	Access List	Direction
------	-----------	-------------	-----------

12 DHCP


DHCP Server

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

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


Global DHCP Server	
Global Status	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Restart DHCP Server	<button>Restart</button>

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 

Edit	Interface	Status	Start IP	END IP	Subnet Mask	Gateway	Primary DNS	Secondary DNS	Lease Time
<input type="checkbox"/>	vlan1.1	Disabled							86400
<input type="checkbox"/>	vlan1.500	Disabled							86400
<input type="checkbox"/>	vlan1.600	Disabled							86400

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



▼ DHCP Binding Table 

Mac Address	IP Address	Host Name	Expires in
-------------	------------	-----------	------------

DHCPv6 Server


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

DHCPv6 Server

▼ Global DHCPv6 Server  

Global DHCPv6 Server	
Global Status	Disabled
Restart DHCPv6 Server	<input type="button" value="Restart"/>

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

▼ DHCPv6 Server setting 

Edit	Interface	Status	Start IP	END IP	Prefix Length	Primary DNS	Secondary DNS	Lease Time
<input type="checkbox"/>	vlan1.1	Disabled						86400
<input checked="" type="checkbox"/>	vlan1.2	Disabled ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	86400

DHCP Relay

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

DHCP Relay

▼ DHCP Relay Server List + ↺

Edit	DHCP Relay Server IP (A.B.C.D)
------	--------------------------------



▼ Global DHCP Relay ✎ ↺

Global DHCP Relay	
Enabled Ports	
Option 82	Disabled
Global Status	Disabled
Restart DHCP Relay	<input type="button" value="Restart"/>



DHCP Snooping

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

DHCP Snooping

▼ DHCP Snooping Setting  

DHCP Snooping Setting	
DHCP Snooping Status	Disabled
Trusted Interfaces	
Clear Binding Table	

▼ DHCP Snooping Binding  

Mac Address	IP Address	Lease Time	Binding Type	Vlan	Port
-------------	------------	------------	--------------	------	------

NTP Configuration

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

NTP Configuration

▼ NTP Setting ✎ ↻

NTP Setting	
NTP Status	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Sync Time	<input type="button" value="Sync"/>

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 + ↻

Edit	Server IP
<input type="checkbox"/>	192.168.1.2
<input type="checkbox"/>	10.10.10.10

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 Setting

Daylight Saving Time Setting

DST Mode:

Daylight Saving Time Setting

Daylight Saving Time Setting

Daylight Saving Time Setting	
Current DST Mode	disable
Disable DST setting	<input type="button" value="Disable"/>

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

Daylight Saving Time Setting

DST Mode:


Daylight Saving Time Setting

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	
Date	
Hour	
Minute	
DST End Month	
Date	
Hour	
Minute	

Daylight Saving Time Setting

DST Mode

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	

14 SNMP

SNMP General Setting

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

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

1. Set the SNMP Status to **enable**.
2. Enter a short description (up to 256 characters) into the **Description** field.

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



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

6. Enter an IP address for the NMS host(s) that should be receiving traps from this switch, into the fields next to any of the 5 **Trap Host IP Address** fields.
7. Enable or disable the **Link Down Trap**. This will allow or stop the switch from sending a trap to the identified trap community groups when any port on the switch moves from the link up state to the link down state.
8. Enable or disable the **Link Up Trap**. This will allow or stop the switch from sending a trap to the identified trap community groups when any port on the switch moves from the link down state to the link up state.
9. Enable or disable the **MAC Notification Trap**. This will allow or stop the switch from sending a trap to the identified trap community groups anytime there is a change in the MAC table on certain selected ports of the switch.
10. Set the interval between the MAC notification traps that you want the switch to send by entering the interval (in number of seconds from 1 to 65535) into the entry field next to **MAC Notification Interval (1 to 65535 seconds)**.
11. Set the size of the MAC notification history table by entering the total number of records (from 1 to 500) that the switch will keep for user to review at any one time into the entry field next to **MAC Notification History Size (1 to 500)**.
12. Select which ports on the switch for which traps should be sent when there is a new MAC address added to the MAC table for the port, by checking the corresponding check boxes for these ports in the **MAC Notification Added** section.
13. Select which ports on the switch for which traps should be sent when there is a MAC address being removed from the MAC table for the port, by checking the corresponding check boxes for these ports in the **MAC Notification Removed** section.
14. Click the “Apply” button when finished.
15. Save the configuration.

SNMP General Setting

SNMP General Setting



SNMP General Setting	
SNMP Status	Enable
Description	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 an NMS to change the status of a data item in the switch.

SNMP v1/v2

SNMP V1/V2c Setting

SNMP V1/V2c Setting	
Get Community Name	public
Set Community Name	

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.”

SNMP v3

SNMP V3 Add User

SNMP Version

SNMP V3 Add User

SNMP V3 Add User	
User Name	
Access Mode	Read Only

SNMP V3 Setting

Edit	User Name	Access Mode	Security Level	Authentication Type	Authentication Password	Privacy Pass Phrase
------	-----------	-------------	----------------	---------------------	-------------------------	---------------------

Radius Configuration

By default, the 802.1X function is globally disabled on the 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.”

Radius Configuration

▼ Radius Server Global Setting ✎ ⌂

Radius Server Global Setting

Radius Status Enabled Disabled

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>

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 Authentication

802.1x Port Setting 

Edit	Port	Authentication State	Port Enabled	Port Control	Port Status	Periodic Reauthentication	Reauthentication Period(default: 3600)
<input type="checkbox"/>	ge1	Disable					
<input type="checkbox"/>	ge2	Disable					
<input checked="" type="checkbox"/>	ge3	Enable ▾	false	force-authorized ▾	Authorized	Enable ▾	<input type="text" value="2147483647"/>

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.

LLDP General Settings

LLDP General Settings

LLDP General Settings


LLDP Status	Disabled ▾
Holdtime Multiplier (2-10)	<input type="text" value="4"/>
Tx Interval (5-32768 sec)	<input type="text" value="30"/>
Global TLV	<input type="checkbox"/> All <input type="checkbox"/> Port Description <input type="checkbox"/> System Name <input type="checkbox"/> System Description <input type="checkbox"/> System Capabilities <input type="checkbox"/> Management Address <input type="checkbox"/> Port VLAN ID <input type="checkbox"/> MAC/PHY Configuration/Status <input type="checkbox"/> Port And Protocol VLAN ID <input type="checkbox"/> VLAN Name <input type="checkbox"/> Protocol Identity <input type="checkbox"/> Link Aggregation <input type="checkbox"/> Maximum Frame Size

LLDP Port Settings

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

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

LLDP Port Settings


LLDP Port Setting 

Edit	Port	Link Status	Transmit	Receive	Notify
<input type="checkbox"/>	ge1	down	Disabled	Disabled	Disabled
<input type="checkbox"/>	ge2	down	Disabled	Disabled	Disabled
<input type="checkbox"/>	ge3	down	Disabled	Disabled	Disabled
<input type="checkbox"/>	ge4	down	Disabled	Disabled	Disabled
<input type="checkbox"/>	ge5	down	Disabled	Disabled	Disabled
<input type="checkbox"/>	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**.

LLDP Statistics

LLDP Device Statistics 

LLDP Device Statistics	
Last Update	6 Days 15:35:28
Total Inserts	5
Total Deletes	2
Total Drops	0
Total Ageouts	2


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

LLDP Statistics 

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

LLDP Neighbors

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

LLDP Neighbors 

LLDP Neighbors

Index	Port	System Name	Chassis ID	Port ID	IP Address	TTL
1	ge1	none	30:65:ec:91:98:20	30:65:ec:91:98:20	0.0.0.0	3439

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 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)
<input type="checkbox"/>	12.12.12.0	--	--	24	13.12.13.12	ge10			

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

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

Prefix Length – Length of IPv6 prefix

Gateway Type – Address or interface

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

Distance – From 1 to 255, Administrative Distance

▼ IPv6 Static Routing + ↺

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

Route Table

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

Route Table

▼ Route ↺

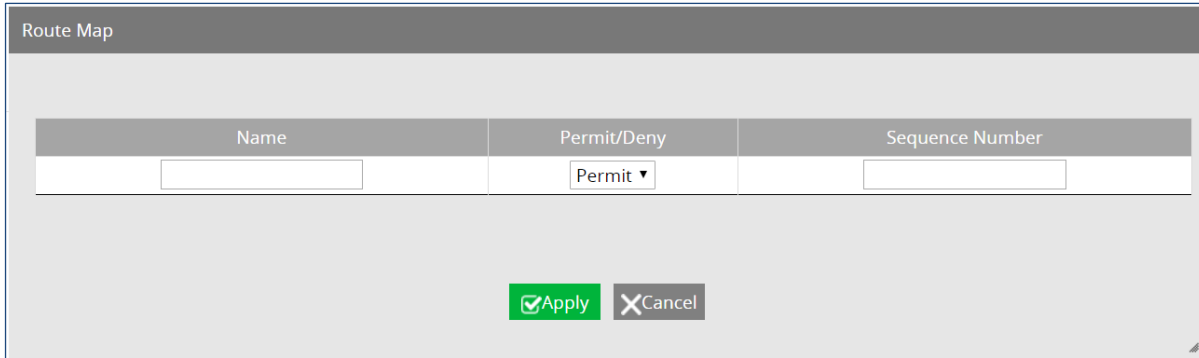
Type	Route default	Subtype	Route
Connect			127.0.0.0/8 is directly connected, lo
Connect			192.168.1.0/24 is directly connected, vlan1.1
Connect			192.168.2.0/24 is directly connected, eth0

▼ IPv6 Route ↺

Type	Route default	Subtype	IPv6 Route
Connect			::1/128 via ::, lo, 45w3d13h
Connect			2001:db8:85a3::/64 via ::, vlan1.1, 05:09:15
Connect			fe80::/64 via ::, vlan1.1, 05:09:15

Route Map

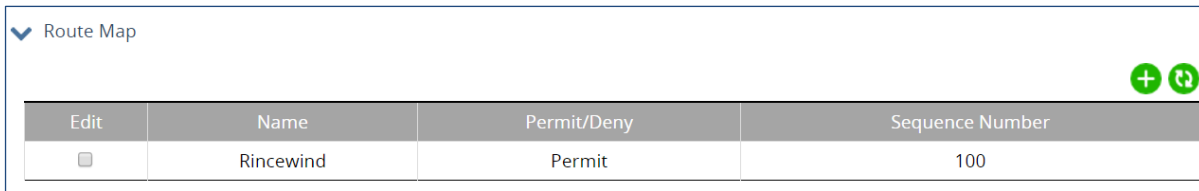
Route Maps can be used for both redistribution and policy routing. To create a route map, click the add icon. Enter the **name** of the route map, the type (**Permit** or **Deny**), and the sequence number (Sequence to insert to or delete from an existing route-map entry. Then click “Apply.”



The dialog box titled "Route Map" contains a table with three columns: "Name", "Permit/Deny", and "Sequence Number". The "Permit/Deny" column has a dropdown menu currently set to "Permit". Below the table are two buttons: a green "Apply" button with a checkmark and a grey "Cancel" button with an 'X'.

Name	Permit/Deny	Sequence Number
<input type="text"/>	Permit ▾	<input type="text"/>

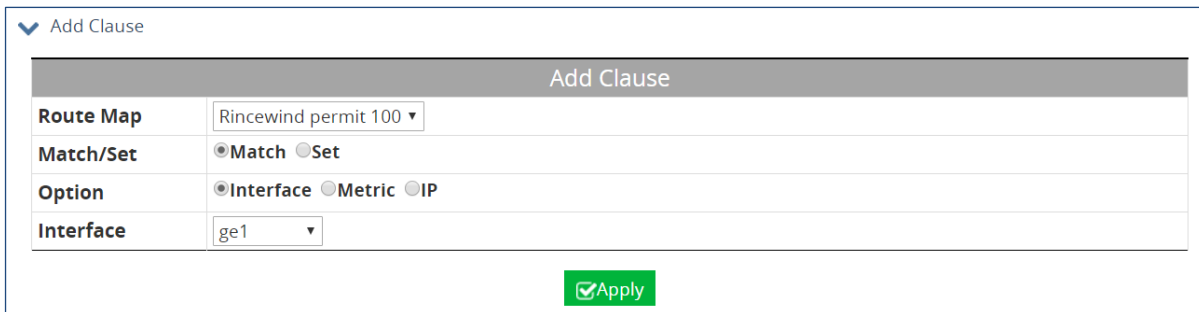
Existing route maps can be deleted by clicking the corresponding check box and clicking “Delete.”



The "Route Map" list view shows a table with columns: "Edit", "Name", "Permit/Deny", and "Sequence Number". There is a check box in the "Edit" column and a green plus icon in the top right corner.

Edit	Name	Permit/Deny	Sequence Number
<input type="checkbox"/>	Rincewind	Permit	100

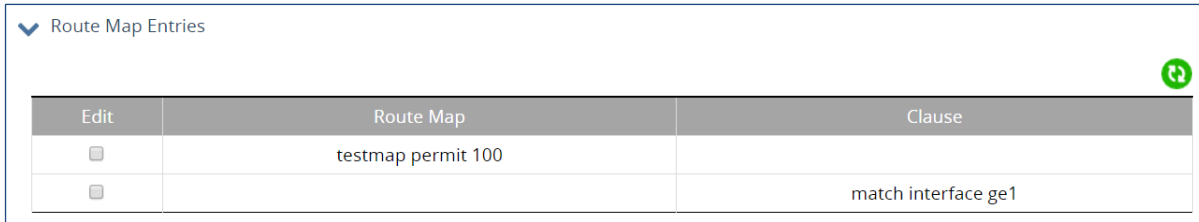
Add match Clauses in the second panel. These are the conditions that must be met in order for a route map to redistribute from one routing protocol to another.



The "Add Clause" dialog box has a title bar "Add Clause" and a table with the following fields:

Route Map	Rincewind permit 100 ▾
Match/Set	<input checked="" type="radio"/> Match <input type="radio"/> Set
Option	<input checked="" type="radio"/> Interface <input type="radio"/> Metric <input type="radio"/> IP
Interface	ge1 ▾

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



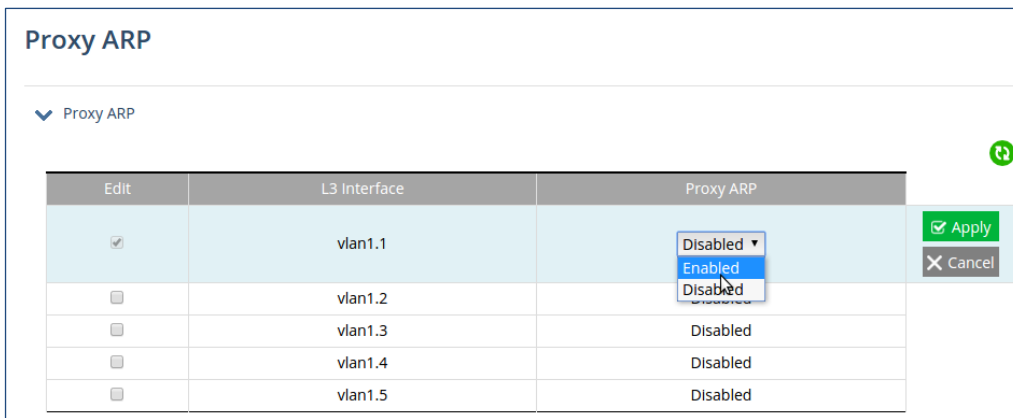
The screenshot shows a web interface panel titled "Route Map Entries" with a refresh icon in the top right. It contains a table with three columns: "Edit", "Route Map", and "Clause".

Edit	Route Map	Clause
<input type="checkbox"/>	testmap permit 100	
<input type="checkbox"/>		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."



The screenshot shows a web interface panel titled "Proxy ARP" with a refresh icon in the top right. It contains a table with three columns: "Edit", "L3 Interface", and "Proxy ARP".

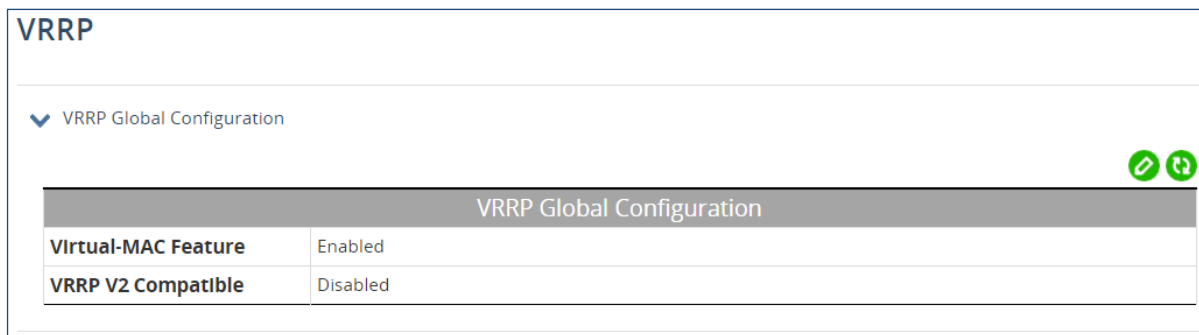
Edit	L3 Interface	Proxy ARP
<input checked="" type="checkbox"/>	vlan1.1	Disabled
<input type="checkbox"/>	vlan1.2	Disabled
<input type="checkbox"/>	vlan1.3	Disabled
<input type="checkbox"/>	vlan1.4	Disabled
<input type="checkbox"/>	vlan1.5	Disabled

Below the table, there are two buttons: "Apply" (with a checkmark icon) and "Cancel" (with an X icon).

VRRP

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



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



To configure VRRP:

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

- Set the priority. If you are configuring the master router, set this value to 255. For other VRRP routers, use a value from 1 - 254. If the master router fails, the router with the highest priority will become the new master.
- Set the **Switch Back Delay** for the timer for the master VRRP router.
- Enter the virtual IP address for the VRRP session.
- Set the status to enable.
- Click the “Apply” button.


▼ Add VRRP  

Add VRRP

IP Version	<input type="radio"/> IPv4 <input type="radio"/> IPv6
VRID	<input type="text" value="1..255"/>
Interface	<input type="text" value="vlan1.1"/>
Accept Mode	<input type="text" value="True"/>
Advertisement Interval (csec, only in multiple of 5)	<input type="text" value="5..4095"/>
Circuit Interface	<input type="text" value="ge1"/>
Circuit Failover Priority	<input type="text" value="1..253"/>
Preempt	<input type="text" value="True"/>
Configured Priority	<input type="text" value="1..255"/>
Switch Back Delay (ms)	<input type="text" value="1..500000"/>
Virtual IP	<input type="text"/>
Status	<input type="text" value="Enable"/>

Apply

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

▼ VRRP Table 

Edit	VRID	Interface	Virtual IP Address	Priority	Advertisement Interval	Accept Mode	Preempt Mode	Circuit Failover Interface	Circuit Failover Priority	Circuit Failover Status	Operation
<input type="checkbox"/>	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”.

RIP General Setting

Route RIP

Route RIP	
Route RIP	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Version	<input type="text" value="2"/>
Default-Information	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Default Matrix (1~16) Default:1	<input type="text" value="1"/>
Distance	<input type="text" value="120"/>
Routing Table Update Timer (5~2147483647) Default:30s	<input type="text" value="30"/>
Routing Information Timeout Timer (5~2147483647) Default:180s	<input type="text" value="180"/>
Garbage Collection Timer (5~2147483647) Default:120s	<input type="text" value="120"/>

RIP Port Setting

In order for a port to be displayed on this screen, the interface must first be added on the [RIP Network by Interface](#) 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.”

RIP Port Setting

▼ Edit Interface ↻

Edit	Edit Interface	Link Status	Line Protocol	Receive Version	Receive Packet	Send Version	Send Packet	Split Horizon	Authentication Mode	Authentication Key
<input checked="" type="checkbox"/>	ge10	down	down	1 ▼	Enable ▼	1 ▼	Enable ▼	Poison Reverse ▼	Disable ▼	

Apply
 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 Subnet + ↺

Edit	Subnet Address	Prefix Length
<input type="checkbox"/>	10.10.10.10	24

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
<input type="checkbox"/>	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.

RIP Neighbor

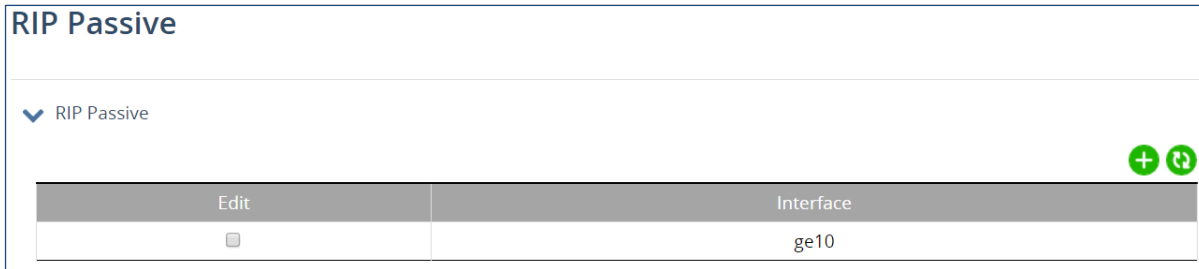
▼ RIP Neighbor + ↺

Edit	Neighbor Address
<input type="checkbox"/>	10.10.10.11

RIP Passive

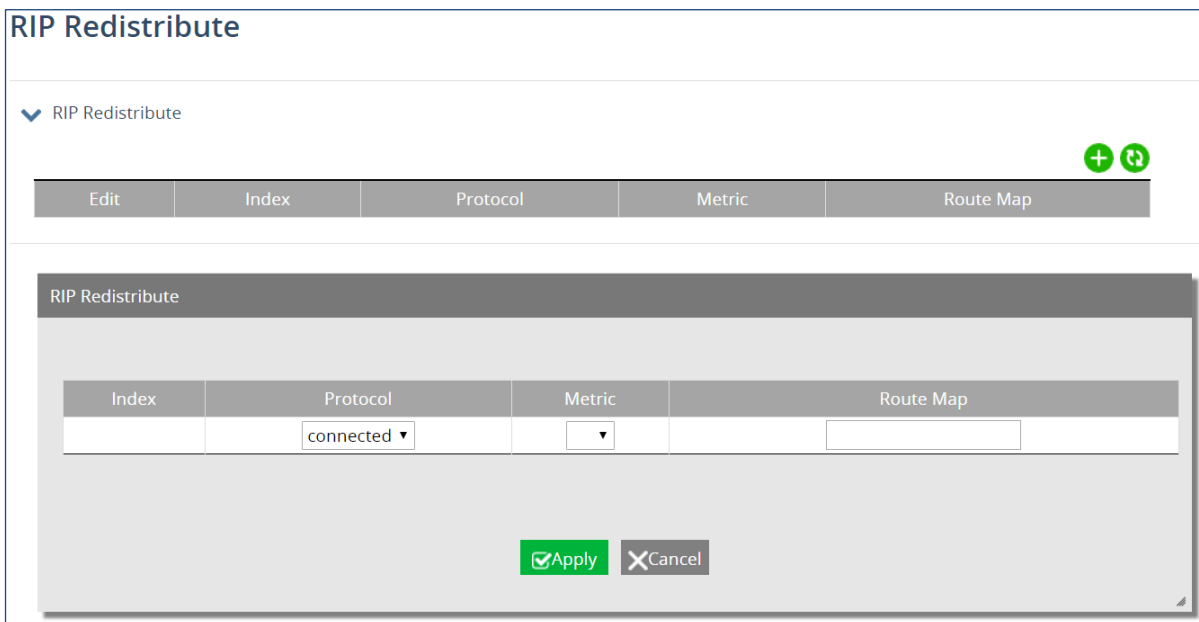
On the RIP Passive screen, you can select an interface to be “passive,” that is, to prevent the RIP routing process from sending multicast/broadcast updates on that interface. Click the add icon, select

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 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 [route map](#) that has been previously defined, and the desired metric, then click the “Apply” button.



RIPng General Setting

Routing Information Protocol next generation (RIPng) is intended for IP version 6 (IPv6)-based networks. Configure the general settings in the same manner as RIP general settings.

RIPng General Setting

▼ Router RIPng  



Router RIPng	
Router RIPng	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Default-Information	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Default-Metric (Default:1)	<input type="text" value="1"/>
Routing Table Update Timer (Default:30s)	<input type="text" value="30"/>
Routing Information Timeout Timer (Default:180s)	<input type="text" value="180"/>
Garbage Collection Timer (Default:120s)	<input type="text" value="120"/>

Apply

RIPng Port Setting

Click the edit icon and enter values for the Interface, Link Status, Line Protocol, RIPng Status, and Split Horizon fields.


RIPng Port Setting

▼ Edit Interface  

Edit	Edit Interface	Link Status	Line Protocol	RIPng Status	Split Horizon
------	----------------	-------------	---------------	--------------	---------------



RIPng Route

The RIP route table is a read-only page that shows existing RIP routes.

RIPng Route						
▼ RIPng Route 						
Code	Network	Next Hop	Interface	Metric	Tag	Time

RIPng Neighbor

Use this screen to screen to add/delete RIPng neighbor IP addresses.

RIPng Neighbor		
▼ RIPng Neighbor  		
Edit	Neighbor Address (IPv6 link-local address)	Interface name

RIPng Passive

On the RIPng Passive screen, you can select an interface to be “passive,” that is, to prevent the RIPng routing process from sending multicast/broadcast updates on that interface.

RIPng Passive	
▼ RIPng Passive  	
Edit	Interface

RIPng Redistribute

To add an item to the redistribute list, select the protocol (**connected** or **static**), a [route map](#) that has been previously defined, and the desired metric, then click the “Apply” button.

RIPng Redistribute

RIPng Redistribute

Index	Protocol	Metric	Route Map
	connected ▾	▾	▾

Apply Cancel

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 OSPF enabled device then calculates best routes and adds them to the routing table.

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

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

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

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

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

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

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

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

OSPF Network

Edit	Network Number (I.I.I.I)	Network Mask Type	Subnet Mask (A.B.C.D)	Prefix Length	Area ID	Instance ID
	<input type="text"/>	Subnet Mask ▾	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Apply Cancel

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

OSPF Timers

Timers


Link State Advertisement (LSA)

Link State Advertisement (LSA)	
LSA Minimum Delay	1000
Reset To Default	<input type="button" value="Reset"/>


OSPF Advanced Setting

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

OSPF Advanced Setting

OSPF Distribute Filter List 



Process ID

OSPF Distribute Filter List 

Edit	Access-list Name	Filter Direction	Route Type	OSPF Process ID
<input type="checkbox"/>	Test	in		

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

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

OSPF Neighbor Router  

Edit	OSPF Neighbor Router	Cost (1~65535)	Dead Router Poll Interval (0~2147483647)	Priority (0~255)
	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Apply Cancel

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

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

Apply Cancel

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

OSPF Default Information

Status
Disabled

The fifth panel is used to set OSPF Routes Administrative Distance. The administrative distance rates the trustworthiness of a routing information source. A higher distance value means a lower trust rating.

OSPF Routes Administrative Distance

OSPF Routes Administrative Distance	
External Routes	<input type="text" value="0"/>
Inter-Area Routes	<input type="text" value="0"/>
Intra-Area Routes	<input type="text" value="0"/>
Disable OSPF Distance	<input type="button" value="Disable"/>

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.”

OSPF Distance Value

Edit	Index	Distance Value	IP Source Prefix (A.B.C.D/M)	Access List Name
OSPF Distance Value				
	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

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

OSPF Overflow Control	
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) ▼

Apply
 Cancel

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.”

Passive Interface

Edit	Passive Interface	Interface Address (A.B.C.D)
	eth0 ▼	

Apply
 Cancel

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)
	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Apply Cancel

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

OSPF Redistribute

Index	Routing Protocol	OSPF Process ID (1~65535)	OSPF Metric Value (1~16777214)	OSPF Metric Type	Route Map Entries	Tag Value (0~4294967295)
	ospf	<input type="text"/>	<input type="text"/>	1	<input type="text"/>	<input type="text"/>

Apply Cancel

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

OSPF Area Config	
OSPF Area ID (0~4294967295)	<input type="text"/>
Authentication	<input type="text"/>
Set Summary-Default Cost (1~16777215)	<input type="text"/>
Name of Filter Access List	<input type="text"/>
Filter networks between OSPF areas	<input type="text"/>
Multi-Area-Adjacency Interface	<input type="text"/>
Multi-Area-Adjacency Neighbor IP	<input type="text"/>
Shortcutting Mode	<input type="text"/>
Configure OSPF Area As Stub	<input type="text"/>

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.

OSPF Area Virtual Link

OSPF Area Virtual Link	
OSPF Area ID (0~4294967295)	<input type="text"/>
Virtual Link IP Address	<input type="text"/>
Authentication	Enable ▾
Authentication Key (8 chars)	<input type="text"/>
Dead Interval (1~65535, 0 to disable)	<input type="text"/>
Hello Interval (1~65535, 0 to disable)	<input type="text"/>
Message Digest Key (1~255)	<input type="text"/>
Message Digest Keyword (16 chars)	<input type="text"/>
Retransmit Interval (1~3600, 0 to disable)	<input type="text"/>
Transmit Delay (1~3600, 0 to disable)	<input type="text"/>

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

OSPF Area Nssa

OSPF Area ID (0~4294967295)	<input type="text"/>
Specify a NSSA area	<input type="radio"/> Enabled <input type="radio"/> Disabled
NSSA Default Information Originate	<input type="radio"/> Enabled <input type="radio"/> Disabled
NSSA OSPF Default Metric	<input type="text"/>
NSSA OSPF Metric Type For Default Routes (default:2)	1 ▾
No Redistribution Into This NSSA area	<input type="radio"/> Enabled <input type="radio"/> Disabled
Do Not Send Summary LSA Into NSSA	<input type="radio"/> Enabled <input type="radio"/> Disabled
NSSA Stability Interval	<input type="text"/>
NSSA-ABR Translator role	Always ▾

Apply

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.

OSPF Area Routes Matching Range (Border Routers Only)

OSPF Area Routes Matching Range (Border Routers Only)

OSPF Area ID (0~4294967295)	<input type="text"/>
Area Range Prefix (A.B.C.D)	<input type="text"/>
PrefixType	Subnet Mask ▾
Area Range Subnet Mask (A.B.C.D)	<input type="text"/>
Advertise (default enable)	<input type="text"/>

Apply

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

Edit	Index	Area	Status
<input checked="" type="button" value="Refresh"/>			

OSPF Interface Configuration

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

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

Click “Apply” when finished.

OSPF Interface Configuration

▼ OSPF Interface Summary

Port

▼ 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.

▼ Interface Message Digest Key

Port

▼ Interface Message Digest Key

Edit	Key ID (1~255)	OSPF password (key)
<input type="checkbox"/>	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.

OSPF Interface Configuration With Address

▼ OSPF Interface Summary

Port

▼ OSPF Interface Summary 

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.

▼ Interface OSPF Statistics

port

▼ Interface OSPF Statistics


Edit	Index	Interface Address	Statics
------	-------	-------------------	---------

OSPFv3 General Setting


OSPFv3 supports both IPv4 and IPv6 addresses.

To enable and configure OSPFv3, add a new OSPFv3 process in the first panel, and in the second panel enter values for the following fields:

1. **Auto Cost. (1~4294967)** The auto-cost reference bandwidth, which controls how OSPF calculates the default metric for the interface.
2. **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.
3. **Maximum number allowed to process DD concurrently** (1~65535) Limits the number of Database Descriptors (DD) that can be processed concurrently.
4. **Maximum number of OSPF area** (Excluding Backbone Area, 1~4294967294)
5. **OSPF ABR type** (Cisco, IBM, shortcut, standard) OSPF Area Border Router (ABR) type.
6. **OSPFv3 router-id in IPv4 address format.** (A.B.C.D) format.
7. **Extension to OSPF Multi Instance Support.** (enable/disable)
8. **Passive Interface (Global Control).** (enable/disable)
9. **Shutdown OSPF Process.** (enable/disable)
10. Click "Apply" when finished.


OSPFv3 General Setting 

Process ID


OSPFv3 General Setting 

OSPFv3 General Setting	
Auto Cost (1-4294967)	100
Default Metric (1~16777214, 0 to disable)	0
Maximum number allowed to process DD concurrently (1~65535)	64
OSPF ABR type	Cisco
OSPFv3 router-Id In IPv4 address format (A.B.C.D)	
Extension To OSPF Multi Instance Support	Disabled
Passive Interface (Global Control)	Disabled
Shutdown OSPF Process	Disabled

The final panel is for setting OSPFv3 SPF (Shortest path first) maximum and minimum delay timers.

OSPF Timers 

Process ID

SPF Timers 

SPF Timers	
SPF Maximum Delay (ms)	50000
SPF Minimum Delay (ms)	500
Reset To Default	<input type="button" value="Reset"/>

OSPFv3 Advanced Setting

The top panel is for applying filters to networks in routing updates, redistributing other routing protocols into the OSPFv3 routing table. Click the add icon, and enter the name of the access list and filter direction.

OSPFv3 Advanced Setting

OSPFv3 Distribute Filter List ↺

Process ID

OSPFv3 Distribute Filter List +

Edit	Access-list Name	Filter Direction	Route Type	OSPF Process ID
------	------------------	------------------	------------	-----------------

The second panel is OSPFv3 default information. Use this command to enable the creation of a default external route into an OSPF routing domain.

OSPFv3 Default Information ↺

Process ID

OSPFv3 Default Information ✎

OSPFv3 Default Information	
Status	Disabled

The third panel is used to set the distance for OSPFv3 routes.

OSPFv3 Routes Administrative Distance ↺

Process ID

OSPFv3 Routes Administrative Distance ✎

OSPFv3 Routes Administrative Distance	
External Routes	<input type="text" value="0"/>
Inter-Area Routes	<input type="text" value="0"/> Range : 1..255
Intra-Area Routes	<input type="text" value="0"/>
Disable OSPFv3 Distance	<input type="button" value="Disable"/>

In the fourth, fifth, and sixth panels, set the OSPFv3 Distance value, Passive Interface, and summary Address.

▼ OSPFv3 Distance Value ↻

Process ID

▼ OSPFv3 Distance Value ✎

OSPFv3 Distance Value	
Distance Value	110

▼ OSPFv3 Passive Interface ↻

Process ID

▼ OSPFv3 Passive Interface +

Edit	Passive Interface

▼ OSPFv3 Summary Address ↻

Process ID

▼ OSPFv3 Summary Address +

Edit	Index	IPv6 summary prefix (X::X:X/M)	Action	Tag Value (0~4294967295)

The final panel is of OSPFv3 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.

OSPFv3 Redistribute

Process ID

OSPFv3 Redistribute

Edit	Index	Routing Protocol	OSPFv3 Process ID (1~65535 WORD)	OSPFv3 Metric Value (1~16777214)	OSPFv3 Metric Type	Route Map Entries	Tag Value (0~4294967295)

OSPFv3 Redistribute

Index	Routing Protocol	OSPFv3 Process ID (1~65535 WORD)	OSPFv3 Metric Value (1~16777214)	OSPFv3 Metric Type	Route Map Entries	Tag Value (0~4294967295)
	ospf		0..16777214	1		0..4294967295

OSPFv3 Area Configuration

The OSPFv3 Area Configuration screen is comprised of five panels, the first of which is OSPFv3 Area Config, used for defining areas and authentication. To add an area, click the edit icon and enter values for the following fields:

1. OSPFv3 Area ID
2. Set Summary-Default Cost
3. Configure OSPFv3 Area As Stub

Click "Apply" when finished

OSPFv3 Area Config

Process ID

OSPFv3 Area Config

OSPFv3 Area Config	
OSPFv3 Area ID (0~4294967295)	<input type="text" value="0.4294967295"/>
Set Summary-Default Cost (1~16777215)	<input type="text" value="1..16777215"/>
Configure OSPFv3 Area As Stub	<input type="text"/>

All OSPFv3 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. OSPFv3 Area ID
2. Virtual Link IP Address
3. Dead Interval
4. Hello Interval
5. Retransmit Interval
6. Transmit Delay

Click “Apply” when finished.

OSPFv3 Area Virtual Link

Process ID

OSPFv3 Area Virtual Link

OSPFv3 Area Virtual Link	
OSPFv3 Area ID (0~4294967295)	<input type="text"/>
Virtual Link IP Address	<input type="text"/>
Dead Interval (seconds) (1~65535, 0 to disable)	<input type="text"/>
Hello Interval (seconds) (1~65535, 0 to disable)	<input type="text"/>
Retransmit Interval (seconds) (5~65535, 0 to disable)	<input type="text"/>
Transmit Delay (seconds) (1~3600, 0 to disable)	<input type="text"/>

The third panel is for creating OSPFv3 NSSA Areas. An NSSA (Not So Stubby Area) (NSSA) is an OSPFv3 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).

OSPFv3 Area Nssa

Process ID 2000

OSPFv3 Area Nssa

OSPFv3 Area Nssa	
OSPFv3 Area ID (0~4294967295)	
Specify a NSSA area	
NSSA Default Information Originate	
NSSA OSPFv3 Default Metric	
NSSA OSPFv3 Metric Type For Default Routes (default:2)	1
No Redistribution Into This NSSA area	
Do Not Send Summary LSA Into NSSA	
NSSA Stability Interval	
NSSA-ABR Translator role	Always

The OSPFv3 Area Routes Matching Range panel allows OSPFv3 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.

Summarize routes matching address/mask (border routers only)

Process ID 2000

Summarize routes matching address/mask (border routers only)

Summarize routes matching address/mask (border routers only)	
OSPFv3 Area ID (0~4294967295)	
Area range for IPv6 prefix (X::X::X/M)	
Advertise (default enable)	

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

OSPFv3 Area Status

Process ID: 2000

OSPFv3 Area Status

Edit	Index	Area	Status
------	-------	------	--------

OSPFv3 Interface Configuration

OSPFv3 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. Interface Cost
- 2.
3. Interval After Which A Neighbor Is Declared Dead
4. Flood Reduction
5. Time Between HELLO Packets
6. Network Type
7. Router Priority
8. Time Between Retransmitting Lost Link State Advertisements
9. Link State Transmit Delay

Click “Apply” when finished.

OSPFv3 Interface Configuration

OSPFv3 Interface Summary



Port

OSPFv3 Interface Summary



OSPFv3 Interface Summary	
Interface Cost (1~65535)	10
Interval After Which A Neighbor Is Declared Dead (1~65535)	40
Time Between HELLO Packets (1~65535)	10
Network Type	Disabled
Router Priority (1~255)	1
Time Between Retransmitting Lost Link State Advertisements (1~65535)	5
Link State Transmit Delay (1~65535)	1

22 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

Global Configuration



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 Configuration

Interface Configuration





Edit	Port	PIM Mode	Passive mode	IP Address	Hello message interval (default:30)	Hello message holdtime (default:105)	Border of PIM domain	Exclude Gen-id	Peering Filter (1~199/1300~2699)	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.

PIM-SM RP Configuration

▼ RP General Config  

RP 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.

▼ Anycast Rendezvous-Point  

Edit	Anycast RP address (A.B.C.D)	Anycast member RP address (A.B.C.D)

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.

▼ Candidate bootstrap router (candidate BSR) + ↺

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) + ↺

Edit	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.

▼ PIMv2 RP-candidate ↺

Edit	RP-Candidate	Interface Name

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



PIM SSM Configurations

Configure Source Specific multicast



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 Table

▼ PIM Neighbor Information

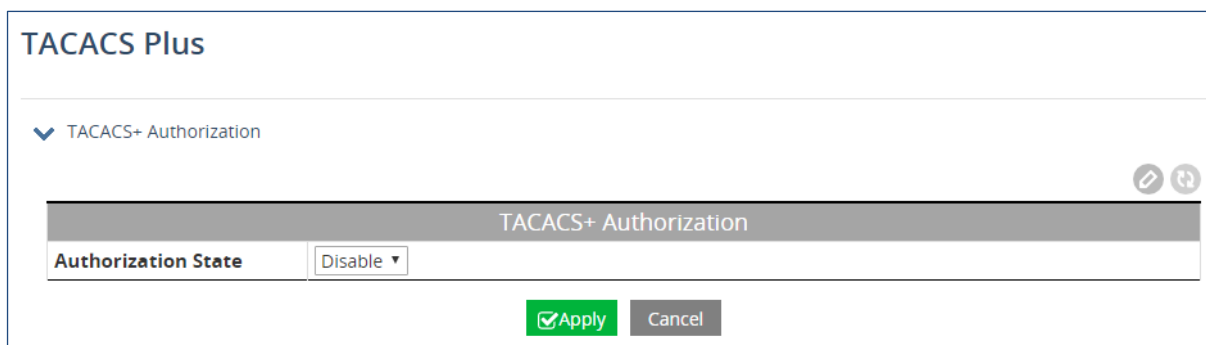


Neighbor Address	Interface	Uptime/Expires	Ver	DR Priority	DR Mode
------------------	-----------	----------------	-----	-------------	---------

23 AAA (Authentication, Authorization, and Accounting)

TACACS Plus

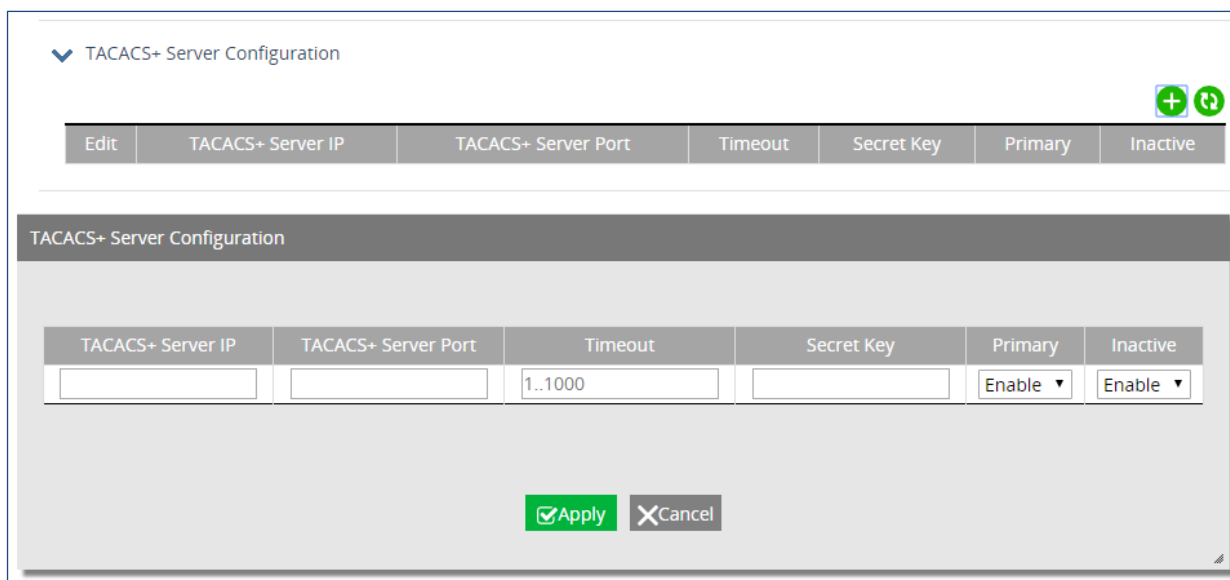
EG97000 series switches support the Tacacs+ protocol IEEE 802.1X protocol to provide port based security against unauthorized access. Enable Tacacs+ by clicking the edit button in the top panel and setting the Authorization State to Enable. Then click Apply.



The screenshot shows the 'TACACS Plus' configuration page. Under the 'TACACS+ Authorization' section, there is a table with one row. The 'Authorization State' column has a dropdown menu currently set to 'Disable'. Below the table are 'Apply' and 'Cancel' buttons.

TACACS+ Authorization	
Authorization State	Disable ▾

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



The screenshot shows the 'TACACS+ Server Configuration' panel. It features a table with columns for 'TACACS+ Server IP', 'TACACS+ Server Port', 'Timeout', 'Secret Key', 'Primary', and 'Inactive'. The 'Timeout' column has a value of '1..1000'. The 'Primary' and 'Inactive' columns have dropdown menus set to 'Enable'. Below the table are 'Apply' and 'Cancel' buttons.

TACACS+ Server IP	TACACS+ Server Port	Timeout	Secret Key	Primary	Inactive
		1..1000		Enable ▾	Enable ▾

24 Contact Information

EtherWAN System, Inc.

www.etherwan.com

USA Office

2301 E. Winston Road

Anaheim, CA 9280

Tel: +1-714-779-3800

Email: info@etherwan.com

Pacific Rim Office

8F., No.2, Alley 6, Lane 235, Baoqiao Rd.

Xindian District, New Taipei City 231

Taiwan

Tel: +886 -2- 6629-8986

Email: info@etherwan.com.tw

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

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

Copyright 2023. All Rights Reserved.

All trademarks and registered trademarks are the property of their respective owners

EG97000 Layer 3 Hardened Managed Ethernet Switch

February 14, 2023