

# DrayTek

## VigorSwitch G2500

L2 Managed Gigabit Switch

DrayTek



*Your reliable networking solutions partner*

# User's Guide

**V1.1**

# **VigorSwitch G2500**

## ***L2 Managed Gigabit Switch***

### **User's Guide**

Version: 1.1

Firmware Version: V2.4.3

(For future update, please visit DrayTek web site)

Date: September 5, 2019

## Copyrights

© All rights reserved. This publication contains information that is protected by copyright. No part may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language without written permission from the copyright holders.

## Trademarks

The following trademarks are used in this document:

- Microsoft is a registered trademark of Microsoft Corp.
- Windows, Windows 95, 98, Me, NT, 2000, XP, Vista, 7, 8, 10 and Explorer are trademarks of Microsoft Corp.
- Apple and Mac OS are registered trademarks of Apple Inc.
- Other products may be trademarks or registered trademarks of their respective manufacturers.

## Caution

Circuit devices are sensitive to static electricity, which can damage their delicate electronics. Dry weather conditions or walking across a carpeted floor may cause you to acquire a static electrical charge.

To protect your device, always:

- Touch the metal chassis of your computer to ground the static electrical charge before you pick up the circuit device.
- Pick up the device by holding it on the left and right edges only.

## Warranty

We warrant to the original end user (purchaser) that the device will be free from any defects in workmanship or materials for a period of one (1) year from the date of purchase from the dealer. Please keep your purchase receipt in a safe place as it serves as proof of date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, we will, at our discretion, repair or replace the defective products or components, without charge for either parts or labor, to whatever extent we deem necessary to restore the product to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be offered solely at our discretion. This warranty will not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions. The warranty does not cover the bundled or licensed software of other vendors. Defects which do not significantly affect the usability of the product will not be covered by the warranty. We reserve the right to revise the manual and online documentation and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

## Be a Registered Owner

Web registration is preferred. You can register your Vigor router via <http://www.DrayTek.com>.

## Firmware & Tools Updates

Due to the continuous evolution of DrayTek technology, all routers will be regularly upgraded. Please consult the DrayTek web site for more information on newest firmware, tools and documents.

More update, please visit [www.draytek.com](http://www.draytek.com).

## Table of Contents

|   |           |
|---|-----------|
| <b>Part I Introduction</b> .....                            | <b>1</b>  |
| I-1 Introduction .....                                      | 2         |
| I-1-1 Key Features .....                                    | 2         |
| I-1-2 Specifications .....                                  | 3         |
| I-1-3 Packing List .....                                    | 4         |
| I-1-4 LED Indicators and Connectors .....                   | 4         |
| I-2 Installation .....                                      | 6         |
| I-2-1 Typical Applications.....                             | 6         |
| I-2-2 Installing Network Cables.....                        | 10        |
| I-2-3 Configuring the Management Agent of Switch.....       | 10        |
| I-2-4 Managing VigorSwitch G2500 through Ethernet Port..... | 10        |
| I-2-5 IP Address Assignment .....                           | 11        |
| I-3 Accessing Web Page of VigorSwitch .....                 | 14        |
| I-4 Dashboard.....  | 15        |
| I-5 Status .....  | 16        |
| I-5-1 Port Bandwidth Utilization .....                      | 16        |
| I-5-2 LLDP Statistics .....                                 | 16        |
| I-5-3 GVRP Statistics .....                                 | 17        |
| I-5-4 MLD Snooping Statistics .....                         | 17        |
| I-5-5 Hardware Monitor .....                                | 18        |
| <b>Part II Switch LAN</b> .....                             | <b>19</b> |
| II-1 General Setup .....                                    | 20        |
| II-1-1 IP Address .....                                     | 20        |
| II-1-2 IPv6 Address .....                                   | 21        |
| II-1-3 Management VLAN .....                                | 22        |
| II-2 Port Setting .....                                     | 23        |
| II-2-1 General Setting.....                                 | 23        |
| II-2-2 Protected Ports.....                                 | 25        |
| II-3 Mirror.....  | 26        |
| II-4 Link Aggregation .....                                 | 27        |
| II-4-1 LAG Setting .....                                    | 27        |
| II-4-2 LAG Management .....                                 | 28        |
| II-4-3 LAG Port Setting.....                                | 29        |
| II-4-4 LACP Setting .....                                   | 31        |
| II-4-5 LACP Port Setting .....                              | 32        |
| II-5 VLAN Management.....                                   | 33        |
| II-5-1 Create VLAN .....                                    | 33        |
| II-5-2 Interface Settings.....                              | 34        |

|                                      |    |
|--------------------------------------|----|
| II-5-3 Voice VLAN .....              | 36 |
| II-5-3-1 Properties .....            | 36 |
| II-5-3-2 Telephony OUI Setting ..... | 37 |
| II-5-3-3 Port Setting .....          | 38 |
| II-5-4 MAC VLAN .....                | 39 |
| II-5-4-1 MAC Group .....             | 39 |
| II-5-4-2 Group Binding .....         | 40 |
| II-5-5 Protocol VLAN .....           | 41 |
| II-5-5-1 Protocol Group .....        | 41 |
| II-5-5-2 Group Binding .....         | 42 |
| II-5-6 Surveillance VLAN.....        | 44 |
| II-5-6-1 Property .....              | 44 |
| II-5-6-1 Surveillance OUI.....       | 46 |
| II-5-7 GVRP .....                    | 47 |
| II-5-7-1 Property .....              | 47 |
| II-5-7-2 Membership .....            | 48 |
| II-6 EEE .....                       | 49 |
| II-7 Multicast .....                 | 50 |
| II-7-1 Properties .....              | 50 |
| II-7-2 IGMP Snooping .....           | 52 |
| II-7-2-1 IGMP Setting .....          | 52 |
| II-7-2-2 IGMP Querier Setting .....  | 54 |
| II-7-2-3 IGMP Static Group .....     | 55 |
| II-7-2-4 IGMP Group Table.....       | 56 |
| II-7-2-5 IGMP Router Table.....      | 57 |
| II-7-2-6 Forward All .....           | 58 |
| II-7-2-7 Throttling .....            | 59 |
| II-7-2-8 Filtering Profile .....     | 60 |
| II-7-2-9 Filtering Binding .....     | 61 |
| II-7-3 MVR.....                      | 63 |
| II-7-3-1 Property .....              | 63 |
| II-7-3-2 Port Setting .....          | 64 |
| II-7-3-3 Group Address .....         | 65 |
| II-7-4 MLD Snooping.....             | 66 |
| II-7-4-1 MLD Setting .....           | 66 |
| II-7-4-2 MLD Static Group .....      | 68 |
| II-7-4-3 MLD Group Table.....        | 70 |
| II-7-4-4 MLD Router Table.....       | 71 |
| II-7-4-5 Forward All .....           | 72 |
| II-7-4-6 Throttling .....            | 73 |
| II-7-4-7 Filtering Profile .....     | 74 |
| II-7-4-8 Filtering Binding .....     | 75 |
| II-8 Jumbo Frame .....               | 77 |
| II-9 STP .....                       | 78 |
| II-9-1 Properties .....              | 78 |
| II-9-2 Port Setting .....            | 79 |
| II-9-3 Bridge Setting .....          | 81 |
| II-9-4 Port Advanced Setting.....    | 82 |
| II-9-5 Statistics .....              | 83 |
| II-9-6 MST Instance .....            | 84 |

|  |            |
|--|------------|
| II-9-7 MST Port Setting .....                        | 85         |
| II-10 MAC Address Table.....                         | 87         |
| II-10-1 Static MAC Setting .....                     | 87         |
| II-10-2 Dynamic Address Setting .....                | 88         |
| II-10-3 Dynamic Learned .....                        | 88         |
| II-11 Blocked Port Recover.....                      | 90         |
| <b>Part III ONVIF Surveillance.....</b>              | <b>91</b>  |
| III-1 Discovery .....                                | 92         |
| III-2 Topology .....                                 | 93         |
| III-2-1 Status .....                                 | 93         |
| III-2-2 Throughput Threshold .....                   | 97         |
| III-3 Video .....                                    | 99         |
| III-4 Device Maintenance .....                       | 100        |
| III-4-1 General.....                                 | 100        |
| III-4-2 Network .....                                | 102        |
| III-4-3 Security.....                                | 103        |
| <b>Part IV Security .....</b>                        | <b>105</b> |
| IV-1 RADIUS .....                                    | 106        |
| IV-2 TACACS+.....                                    | 108        |
| IV-3 Management Access Authentication.....           | 109        |
| IV-3-1 Method Profile .....                          | 109        |
| IV-3-2 Application Authentication.....               | 110        |
| IV-4 Management Access Control.....                  | 111        |
| IV-4-1 Management Access Control Profile (ACL) ..... | 111        |
| IV-4-2 Management Access Control Entries (ACE).....  | 112        |
| IV-5 802.1X/MAC Authentication.....                  | 114        |
| IV-5-1 Properties.....                               | 114        |
| <i>IV-5-1-1 Global Settings .....</i>                | <i>114</i> |
| <i>IV-5-1-2 Port Authentication Setting.....</i>     | <i>115</i> |
| IV-5-2 Port Control/Settings .....                   | 116        |
| IV -5-3 MAC-Based Local Account .....                | 118        |
| IV-5-4 Authenticated Hosts .....                     | 119        |
| IV-6 Port Security .....                             | 120        |
| IV-7 Storm Control.....                              | 122        |
| IV-7-1 Properties.....                               | 122        |
| IV-7-2 Port Setting .....                            | 123        |
| IV-8 DoS.....  | 124        |
| IV-8-1 Properties.....                               | 124        |
| IV-8-2 DoS Port Setting .....                        | 126        |
| IV-9 Dynamic ARP Inspection .....                    | 127        |

|  |            |
|--|------------|
| IV-9-1 Properties.....                             | 127        |
| IV-9-1-1 Global Property Settings.....             | 127        |
| IV-9-1-2 Per Port Property Settings.....           | 128        |
| IV-9-2 Statistics.....                             | 129        |
| IV-10 DHCP Snooping.....                           | 130        |
| IV-10-1 Properties.....                            | 130        |
| IV-10-1-1 Global Property Settings.....            | 130        |
| IV-10-1-2 Per Port Property Settings.....          | 131        |
| IV-10-2 Statistics.....                            | 132        |
| IV-10-3 Option82 Property.....                     | 132        |
| IV-10-3-1 Global Option82 Property Settings.....   | 132        |
| IV-10-3-2 Per Port Option82 Property Settings..... | 133        |
| IV-10-4 Option82 Circuit ID.....                   | 134        |
| IV-11 IP Source Guard.....                         | 135        |
| IV-11-1 Port Settings.....                         | 135        |
| IV-11-2 IMPV Binding.....                          | 136        |
| IV-12 IP Conflict Prevention.....                  | 138        |
| IV-13 Loop Protection.....                         | 142        |
| <b>Part V ACL Configuration.....</b>               | <b>143</b> |
| V-1 Create ACL.....                                | 144        |
| V-1-1 MAC.....                                     | 144        |
| V-1-2 IPv4.....                                    | 145        |
| V-1-3 IPv6.....                                    | 146        |
| V-2 Create ACE.....                                | 147        |
| V-2-1 MAC.....                                     | 147        |
| V-2-2 IPv4.....                                    | 148        |
| V-2-3 IPv6.....                                    | 150        |
| V-3 ACL Binding.....                               | 152        |
| <b>Part VI QoS Configuration.....</b>              | <b>153</b> |
| VI-1 General.....                                  | 154        |
| VI-1-1 Properties.....                             | 154        |
| VI-1-1-1 QoS General Setting.....                  | 154        |
| VI-1-1-2 Trust Ports.....                          | 155        |
| VI-1-2 Port Settings.....                          | 156        |
| VI-1-3 Queue Settings.....                         | 157        |
| VI-1-4 CoS Mapping.....                            | 158        |
| VI-1-5 DSCP Mapping.....                           | 159        |
| VI-1-6 IP Precedence Mapping.....                  | 160        |
| VI-2 Bandwidth.....                                | 161        |
| V-2-1 Ingress Rate Limit.....                      | 161        |
| VI-2-2 Egress Shaping Rate.....                    | 162        |
| VI-2-3 Egress Shaping Per Queue.....               | 163        |

|  |                |
|--|----------------|
| <b>Part VII System Maintenance .....</b> | <b>165</b>     |
| VII-1 TR-069 .....                       | 166            |
| VII-2 OpenVPN.....                       | 168            |
| VII-3 Webhook.....                       | 169            |
| VII-4 LLDP .....                         | 170            |
| VII-4-1 Properties.....                  | 170            |
| VII-4-2 LLDP Port Setting .....          | 171            |
| VII-4-3 LLDP Local Device.....           | 173            |
| VII-4-4 MED Network Policy .....         | 174            |
| VII-4-5 LLDP MED Port Settings .....     | 175            |
| VII-4-6 LLDP Remote Device.....          | 176            |
| VII-4-7 LLDP Overloading.....            | 177            |
| VII-5 SNMP .....                         | 178            |
| VII-5-1 View .....                       | 179            |
| VII-5-2 Group .....                      | 180            |
| VII-5-3 Community .....                  | 182            |
| VII-5-4 User.....                        | 183            |
| VII-5-5 Engine ID .....                  | 185            |
| <i>VII-5-5-1 Local Engine ID.....</i>    | <i>185</i>     |
| <i>VII-5-5-2 Remote Engine ID.....</i>   | <i>186</i>     |
| VII-5-6 Trap Event.....                  | 187            |
| VII-5-7 Notification .....               | 188            |
| VII-6 Access Manager .....               | 190            |
| VII-7 Time and Date .....                | 191            |
| VII-7-1 System Time Zone .....           | 191            |
| VII-7-2 Time .....                       | 192            |
| VII-8 Backup Manager.....                | 193            |
| VII-9 Upgrade Manager.....               | 194            |
| VII-10 Firmware Information.....         | 195            |
| VII-11 Account Manager .....             | 196            |
| VII-12 Factory Default .....             | 198            |
| VII-13 Reboot Switch.....                | 199            |
| <br><b>Part VIII Diagnostics .....</b>   | <br><b>201</b> |
| VIII-1 Device Check.....                 | 202            |
| VIII-2 Cable Diagnostics.....            | 203            |
| VIII-3 Ping Test .....                   | 204            |
| VIII-4 SysLog.....                       | 205            |
| VIII-4-1 SysLog Explorer.....            | 205            |
| VIII-4-2 SysLog Settings .....           | 206            |
| <i>VIII-4-2-1 SysLog Service.....</i>    | <i>206</i>     |
| <i>VIII-4-2-2 Local SysLog .....</i>     | <i>207</i>     |



|   |            |
|---|------------|
| VIII-4-2-3 Remote SysLog .....              | 208        |
| VIII-4-2-4 SysLog Mail .....                | 209        |
| <b>Part IX Mail Alert .....</b>             | <b>211</b> |
| IX-1 Alert Setting .....                    | 212        |
| <b>Part X Telnet Commands.....</b>          | <b>215</b> |
| X-1 Accessing Telnet of VigorSwitch .....   | 216        |
| X-2 Available Commands .....                | 218        |
| X-2-1 Clear Configuration .....             | 218        |
| X-2-2 Clock Configuration.....              | 227        |
| X-2-3 Configure Configuration .....         | 228        |
| X-2-4 Copy Configuration .....              | 312        |
| X-2-5 Delete Configuration .....            | 314        |
| X-2-6 Disable Configuration.....            | 315        |
| X-2-7 End Configuration .....               | 315        |
| X-2-8 Exit Configuration.....               | 316        |
| X-2-9 Ping Configuration.....               | 316        |
| X-2-10 Reboot Configuration .....           | 317        |
| X-2-11 Renew Configuration.....             | 317        |
| X-2-12 Restore-defaults Configuration ..... | 317        |
| X-2-13 Save Configuration.....              | 318        |
| X-2-14 Show Configuration.....              | 318        |
| X-2-15 SSL Configuration .....              | 319        |
| X-2-16 Terminal Configuration.....          | 319        |
| X-2-17 Traceroute Configuration .....       | 320        |
| X-2-18 UDLD Configuration .....             | 320        |
| <b>Appendix: Reference .....</b>            | <b>323</b> |
| A-1 What's the Ethernet .....               | 323        |
| A-2 Media Access Control (MAC) .....        | 326        |
| A-3 Flow Control.....                       | 330        |
| <b>Index .....</b>                          | <b>333</b> |



# Part I Introduction

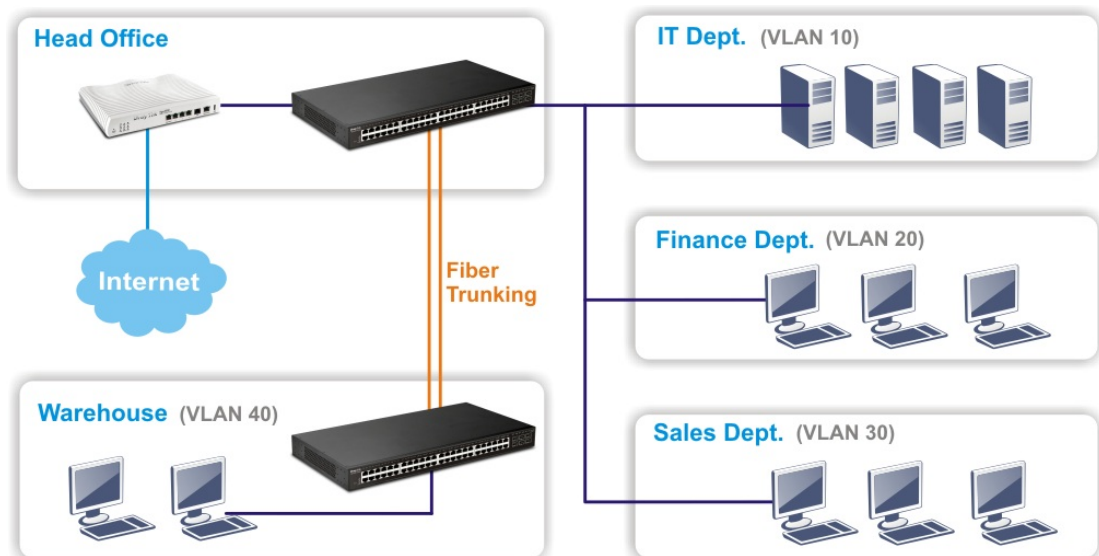
---

## I-1 Introduction

VigorSwitch G2500, L2 Managed Gigabit Switch, is a standard switch that meets all IEEE 802.3/u/x/z Gigabit, Fast Ethernet specifications. The switch has 24 10/100/1000Mbps TP ports. It supports telnet, http, https, SSH and SNMP interface for switch management. The network administrator can login the switch to monitor, configure and control each port's activity. In addition, the switch implements the QoS (Quality of Service), VLAN, and Trunking. It is suitable for office application.

Vigor switch supports IEEE 802.3az, Energy-Efficient Ethernet, and provides power saving feature. It can efficiently save the switch power with auto detect the client idle and cable length to provide different power.

1000Mbps SFP Fiber port could be used in 1000Base-X/100Base-FX interface applications.



---

### I-1-1 Key Features

Below shows key features of this device:

#### QoS

The switch offers powerful QoS function. This function supports 802.1p VLAN tag priority and DSCP on Layer 3 of network framework.

#### VLAN

Support Port-based VLAN and IEEE802.1Q Tag VLAN. Support 24 active VLANs and VLAN ID 1~4094.

#### Port Trunking

Allows one or more links to be aggregated together to form a Link Aggregation Group by the static setting.

---

## I-1-2 Specifications

The VigorSwitch G2500, a standalone off-the-shelf switch, provides the comprehensive features listed below for users to perform system network administration and efficiently and securely serve your network.

### Hardware

- ❖ 44 10/100/1000Mbps Auto-negotiation Gigabit Ethernet TP ports
- ❖ 4 TP/SFP Combo Ethernet Ports
- ❖ 2 SFP Ports
- ❖ Jumbo frame support 9KB
- ❖ Programmable classifier for QoS (Layer 2/Layer 3)
- ❖ 8K MAC address and support VLAN ID(1~4094)
- ❖ Per-port shaping, policing, and Broadcast Storm Control
- ❖ Power Saving with IEEE 802.3az, Energy-Efficient Ethernet
- ❖ Full-duplex flow control (IEEE802.3x) and half-duplex backpressure
- ❖ Extensive front-panel diagnostic LEDs; Power, System
- ❖ Hardware reset button for resetting configuration to factory default by pressing over 5 seconds

### Management

- ❖ Supports per port traffic monitoring counters
- ❖ Supports a snapshot of the system Information when you login
- ❖ Supports port mirror function
- ❖ Supports the static trunk function
- ❖ Supports 802.1Q VLAN
- ❖ Supports user management and limits three users to login
- ❖ Maximal packet length can be up to 9600 bytes for jumbo frame application
- ❖ Supports Broadcasting Suppression to avoid network suspended or crashed
- ❖ Supports to send the trap event while monitored events happened
- ❖ Supports default configuration which can be restored to overwrite the current configuration which is working on via Web UI and Reset button of the switch
- ❖ Supports on-line plug/unplug SFP modules
- ❖ Supports Quality of Service (QoS) for real time applications based on the information taken from Layer 2 to Layer 3
- ❖ Built-in web-based management and CLI management, providing a more convenient UI for the user

## I-1-3 Packing List

Before you start installing the switch, verify that the package contains the following:

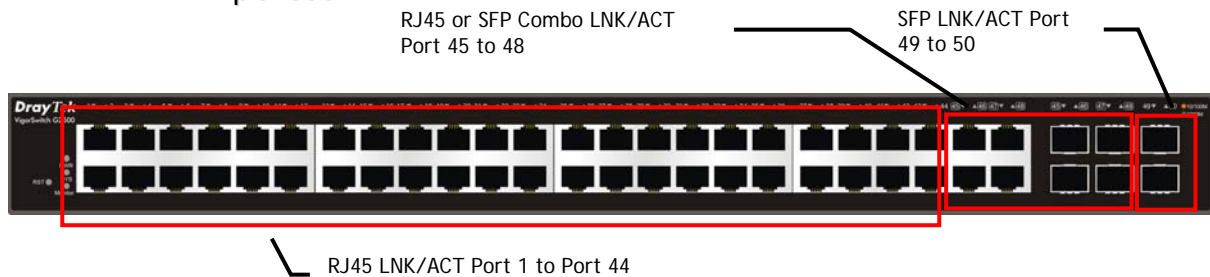
- ❖ VigorSwitch G2500
- ❖ AC Power Cord
- ❖ Quick Start Guide
- ❖ Rubber feet
- ❖ Rack mount kit

Please notify your sales representative immediately if any of the aforementioned items is missing or damaged.

## I-1-4 LED Indicators and Connectors

Before you use the Vigor device, please get acquainted with the LED indicators and connectors first. There are 8 Ethernet ports and SFP ports on the front panel of the switch. LED display area, locating on the front panel, contains an ACT, Power LED and ports working status of the switch.


### LED Explanation



| LED         | Color            | Explanation  |
|-------------|------------------|--|
| PWR         | On (Green)       | The device is powered on and running normally.                   |
|             | Off              | The device is not ready or is failed.                            |
| SYS         | On (Green)       | The switch finishes system booting and the system is ready.      |
|             | Blinking (Green) | The switch is powered on and starts system booting.              |
|             | Off              | The power is off or the system is not ready / malfunctioning.    |
| Monitor     | On (Red)         | An alert for system failure due to overheating or wrong voltage. |
|             | Off              | The device is in normal condition and running normally.          |
| Port 1 ~ 44 | On (Green)       | The device is connected with 1000Mbps.                           |
|             | On (Amber)       | The device is connected with 10/100Mbps.                         |
|             | Blinking         | The system is sending or receiving data through                  |

|                               |            |   |
|-------------------------------|------------|---|
|                               |            | the port.   |
|                               | Off        | The port is disconnected or the link is failed.           |
| Port 45 ~ 48<br>(RJ45 or SFP) | On (Green) | The device is connected with 1000Mbps.                    |
|                               | On (Amber) | The device is connected with 10/100Mbps.                  |
|                               | Blinking   | The system is sending or receiving data through the port. |
|                               | Off        | The port is disconnected or the link is failed.           |
| Port 49 ~ 50<br>(SFP)         | On (Green) | The device is connected with 1000Mbps.                    |
|                               | On (Amber) | The device is connected with 10/100Mbps.                  |
|                               | Blinking   | The system is sending or receiving data through the port. |
|                               | Off        | The port is disconnected or the link is failed.           |

### Connector Explanation

| Interface   | Description  |
|---|--|
| Port 1 ~ 44 (RJ45)  | Port 1 to Port 44 can be used for Ethernet connection.               |
| Port 45 ~ 48 (RJ45 or SFP)  | Port 45 to Port 48 are used either for Ethernet or fiber connection. |
| Port 49 ~ 50 (SFP)  | Port 49 to Port 50 are used for fiber connection.                    |
| Console   | Used to perform telnet command control.                              |
|  | Power inlet for AC input (100~240V/AC, 50/60Hz).                     |

#### Note:

##### Power Output -

- IEEE 802.3af Max. 15.4W Output Supported
- IEEE 802.3at Max. 30W Output Supported

---

## I-2 Installation

---

### I-2-1 Typical Applications

The VigorSwitch implements 24 Gigabit Ethernet TP ports with auto MDIX and four slots for the removable module supporting comprehensive fiber types of connection, including LC and BiDi-LC SFP modules. The switch is suitable for the following applications:

**Case 1: All switch ports are in the same local area network.**

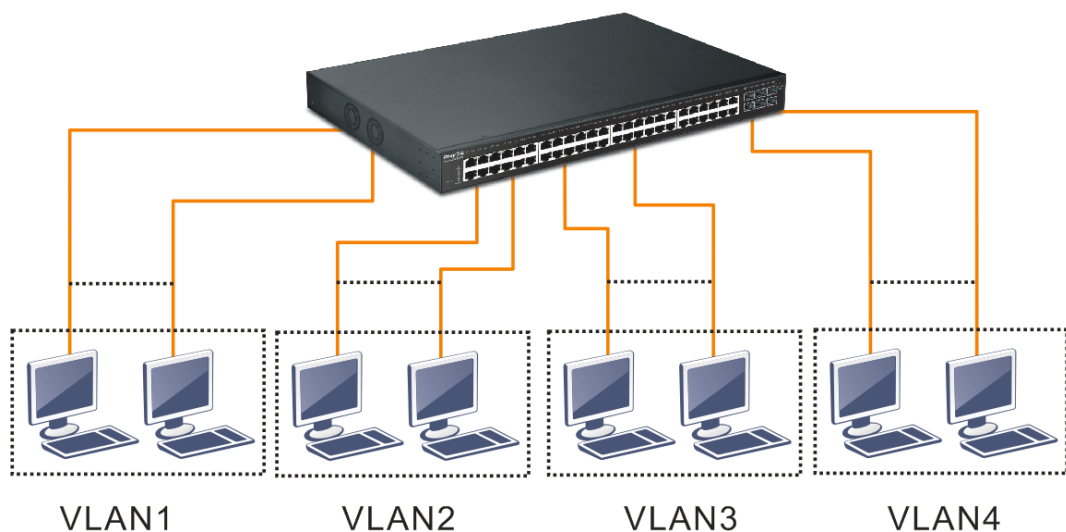
Every port can access each other. (\*The switch image is sample only.)



If VLAN is enabled and configured, each node in the network that can communicate each other directly is bounded in the same VLAN area.

Here VLAN area is defined by what VLAN you are using. The switch supports both port-based VLAN and tag-based VLAN. They are different in practical deployment, especially in physical location. The following diagram shows how it works and what the difference they are.

**Case 2: Port-based VLAN -1** (\*The switch image is sample only.)

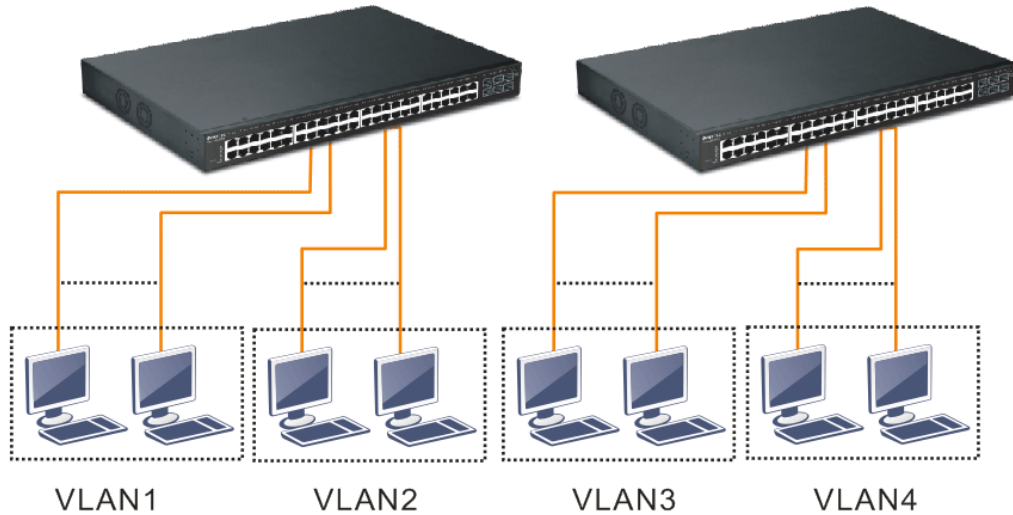


- ❖ The same VLAN members could not be in different switches.



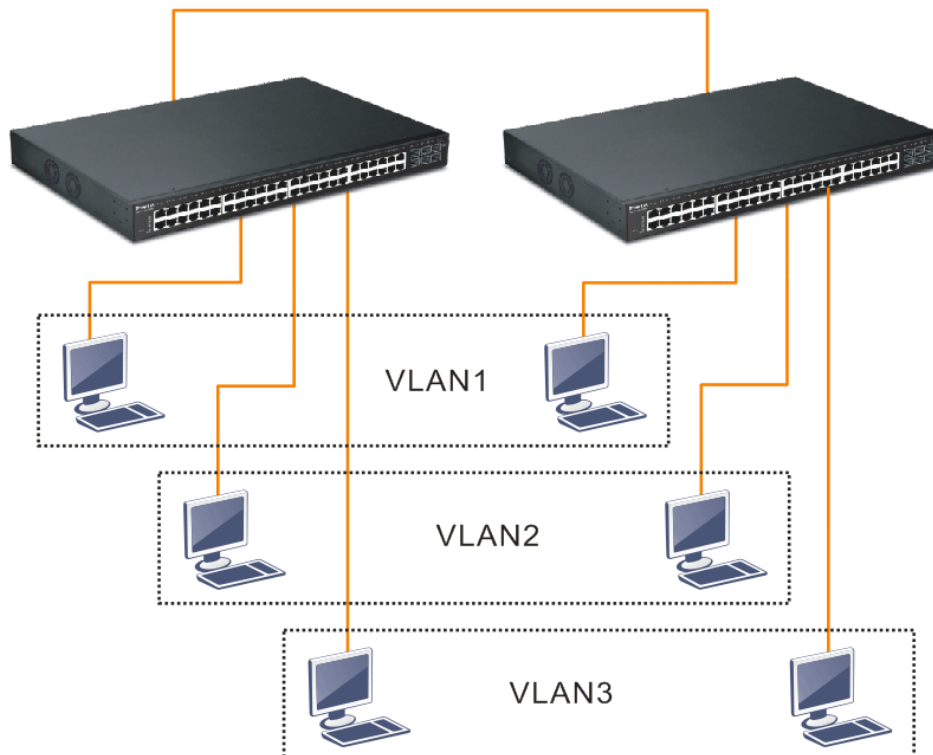
- ❖ Every VLAN members could not access VLAN members each other.
- ❖ The switch manager has to assign different names for each VLAN groups at one switch.

### Case 3: Port-based VLAN - 2



- ❖ VLAN1 members could not access VLAN2, VLAN3 and VLAN4 members.
- ❖ VLAN2 members could not access VLAN1 and VLAN3 members, but they could access VLAN4 members.
- ❖ VLAN3 members could not access VLAN1, VLAN2 and VLAN4.
- ❖ VLAN4 members could not access VLAN1 and VLAN3 members, but they could access VLAN2 members.

### Case 4: The same VLAN members can be at different switches with the same VID



### Case 5: Desktop Installation

1. Install the switch on a level surface that can support the weight of the unit and the relevant components.
2. Plug the switch with the female end of the provided power cord and plug the male end to the power outlet.

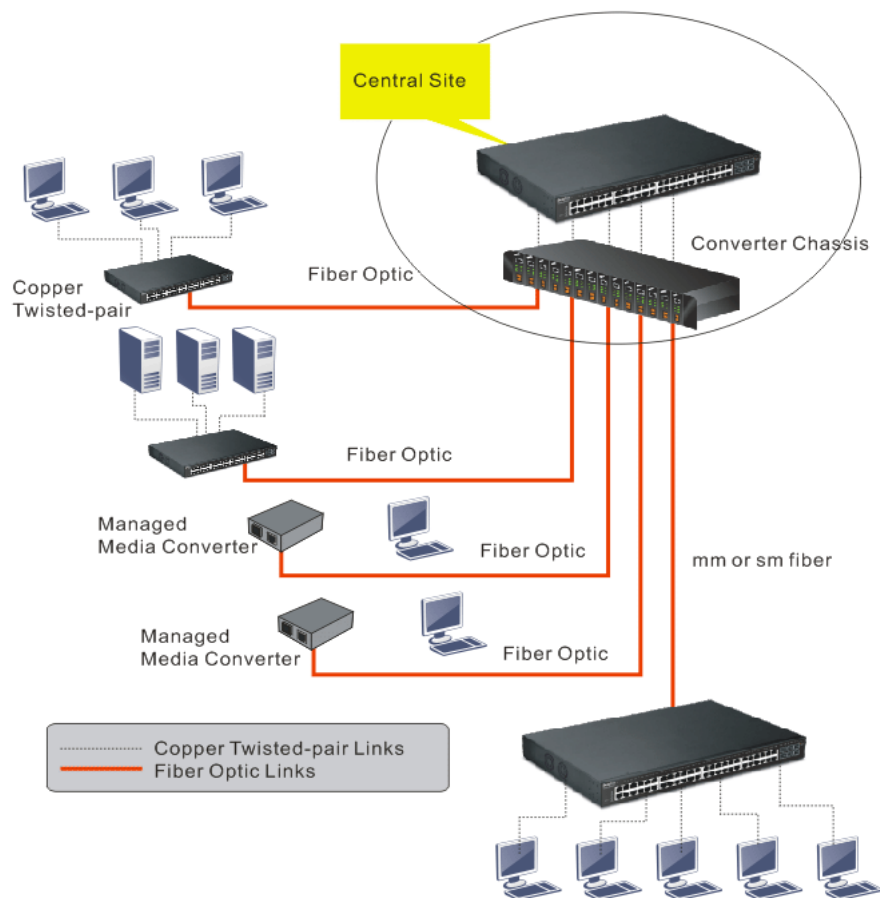
### Case 6: Rack-mount Installation

The switch may be standalone, or mounted in a rack. Rack mounting facilitates to an orderly installation when you are going to install series of networking devices.

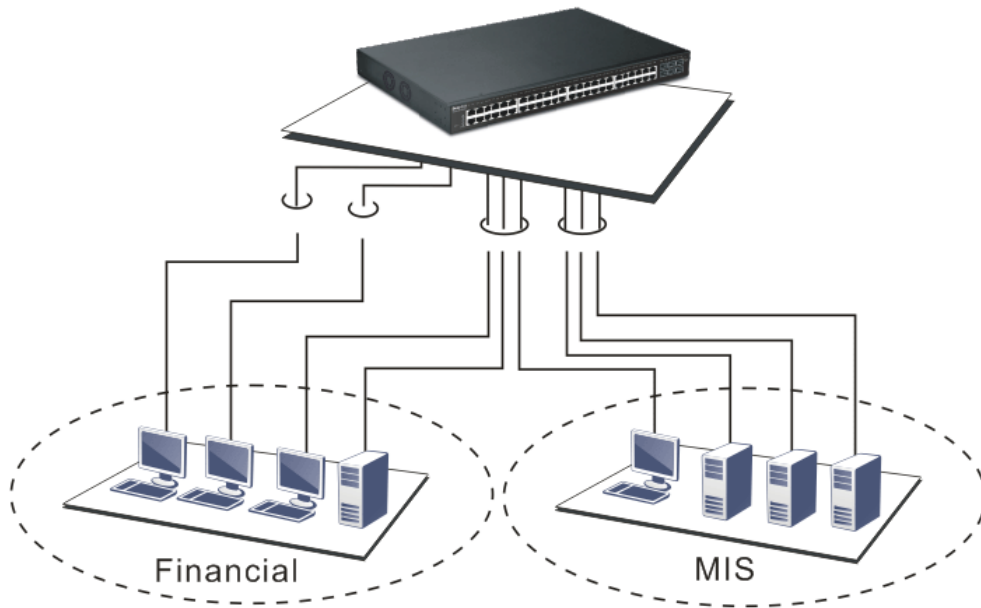
Procedures to Rack-mount the switch:

1. Disconnect all the cables from the switch before continuing.
2. Place the unit the right way up on a hard, flat surface with the front facing you.
3. Locate a mounting bracket over the mounting holes on one side of the unit.
4. Insert the screws and fully tighten with a suitable screwdriver.
5. Repeat the two previous steps for the other side of the unit.
6. Insert the unit into the rack and secure with suitable screws.
7. Reconnect all the cables.

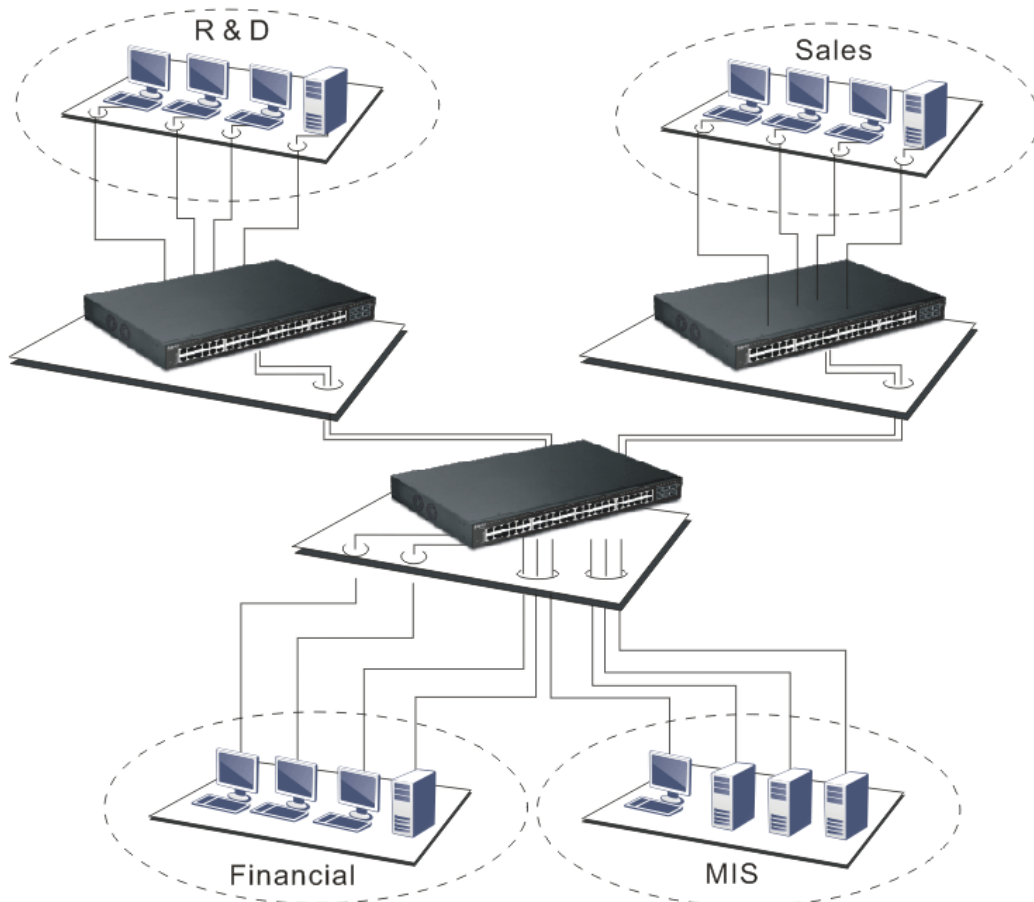
### Case 7: Central Site/Remote site application is used in carrier or ISP



Case 8: Peer-to-peer application is used in two remote offices



Case 9: Office network



---

## I-2-2 Installing Network Cables

Crossover or straight-through cable: All the ports on the switch support Auto-MDI/MDI-X functionality. Both straight-through or crossover cables can be used as the media to connect the switch with PCs as well as other devices like switches, hubs or router.

Category 3, 4, 5 or 5e, 6 UTP/STP cable: To make a valid connection and obtain the optimal performance, an appropriate cable that corresponds to different transmitting/receiving speed is required. To choose a suitable cable, please refer to the following table.

| Media                   | Speed     | Wiring                 |
|-------------------------|-----------|------------------------|
| 10/100/1000 Mbps copper | 10 Mbps   | Category 3,4,5 UTP/STP |
|                         | 100Mbps   | Category 5 UTP/STP     |
|                         | 1000 Mbps | Category 5e, 6 UTP/STP |

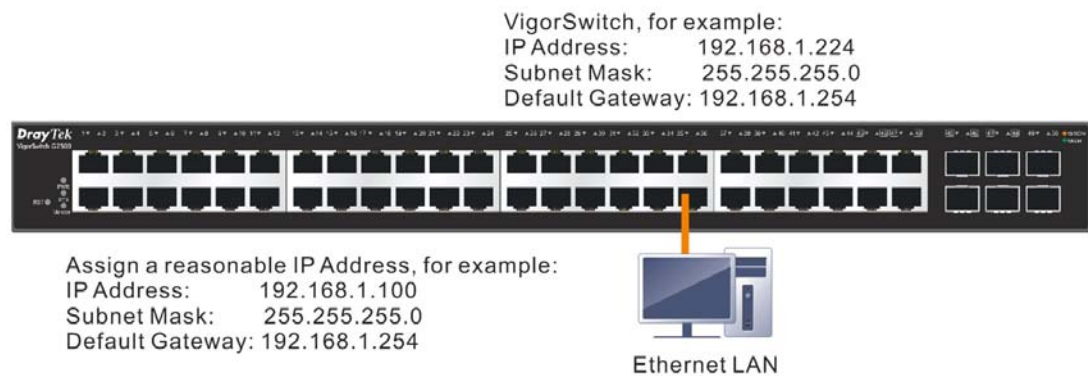
---

## I-2-3 Configuring the Management Agent of Switch

Users can monitor and configure the switch through the following procedures.

Configuring the Management Agent of VigorSwitch G2500 through the Ethernet Port.

There are several ways to configure and monitor the switch through Ethernet port, includes Web-UI and SNMP.



---

## I-2-4 Managing VigorSwitch G2500 through Ethernet Port

Before start using the switch, the IP address setting of the switch should be done, then perform the following steps:

1. Set up a physical path between the configured the switch and a PC by a qualified UTP Cat. 5e cable with RJ-45 connector.

**Note:** If PC directly connects to the switch, you have to setup the same subnet mask between them. But, subnet mask may be different for the PC in the remote site. Please refer to the above figure about the Web Smart Switch default IP address information.

2. After configuring correct IP address on your PC, open your web browser and access switch's IP address.

Default system account is "admin", with password "admin" in default. Switch IP address is "192.168.1.224" by default with DHCP client enabled.

---

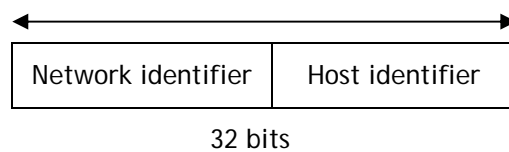
## I-2-5 IP Address Assignment

For IP address configuration, there are three parameters needed to be filled in. They are IP address, Subnet Mask, Default Gateway and DNS.

### *IP address:*

The address of the network device in the network is used for internetworking communication. Its address structure looks is shown below. It is "classful" because it is split into predefined address classes or categories.

Each class has its own network range between the network identifier and host identifier in the 32 bits address. Each IP address comprises two parts: network identifier (address) and host identifier (address). The former indicates the network where the addressed host resides, and the latter indicates the individual host in the network which the address of host refers to. And the host identifier must be unique in the same LAN. Here the term of IP address we used is version 4, known as IPv4.



With the classful addressing, it divides IP address into three classes, class A, class B and class C. The rest of IP addresses are for multicast and broadcast. The bit length of the network prefix is the same as that of the subnet mask and is denoted as IP address/X, for example, 192.168.1.0/24. Each class has its address range described below.

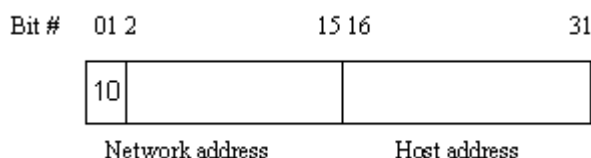
### *Class A:*

Address is less than 126.255.255.255. There are a total of 126 networks can be defined because the address 0.0.0.0 is reserved for default route and 127.0.0.0/8 is reserved for loopback function.



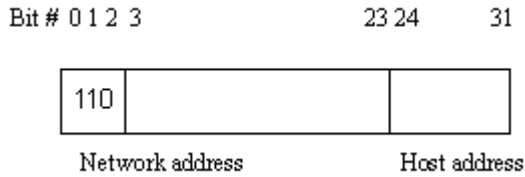
### *Class B:*

IP address range between 128.0.0.0 and 191.255.255.255. Each class B network has a 16-bit network prefix followed 16-bit host address. There are 16,384 ( $2^{14}$ )/16 networks able to be defined with a maximum of 65534 ( $2^{16} - 2$ ) hosts per network.



### *Class C:*

IP address range between 192.0.0.0 and 223.255.255.255. Each class C network has a 24-bit network prefix followed 8-bit host address. There are 2,097,152 ( $2^{21}$ )/24 networks able to be defined with a maximum of 254 ( $2^8 - 2$ ) hosts per network.



**Class D and E:**

Class D is a class with first 4 MSB (Most significance bit) set to 1-1-1-0 and is used for IP Multicast. See also RFC 1112. Class E is a class with first 4 MSB set to 1-1-1-1 and is used for IP broadcast.

According to IANA (Internet Assigned Numbers Authority), there are three specific IP address blocks reserved and able to be used for extending internal network. We call it Private IP address and list below:

|         |                                 |
|---------|---------------------------------|
| Class A | 10.0.0.0 --- 10.255.255.255     |
| Class B | 172.16.0.0 --- 172.31.255.255   |
| Class C | 192.168.0.0 --- 192.168.255.255 |

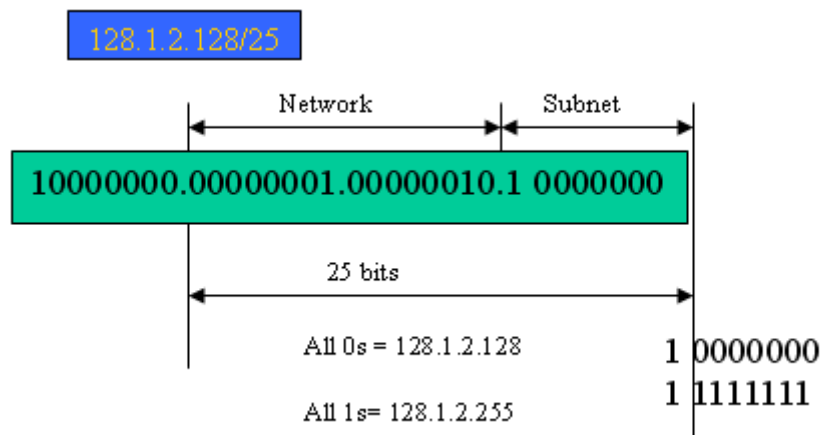
Please refer to RFC 1597 and RFC 1466 for more information.

**Subnet mask:**

It means the sub-division of a class-based network or a CIDR block. The subnet is used to determine how to split an IP address to the network prefix and the host address in bitwise basis. It is designed to utilize IP address more efficiently and ease to manage IP network.

For a class B network, 128.1.2.3, it may have a subnet mask 255.255.0.0 in default, in which the first two bytes is with all 1s. This means more than 60 thousands of nodes in flat IP address will be at the same network. It's too large to manage practically. Now if we divide it into smaller network by extending network prefix from 16 bits to, say 24 bits, that's using its third byte to subnet this class B network. Now it has a subnet mask 255.255.255.0, in which each bit of the first three bytes is 1. It's now clear that the first two bytes is used to identify the class B network, the third byte is used to identify the subnet within this class B network and, of course, the last byte is the host number.

Not all IP address is available in the sub-netted network. Two special addresses are reserved. They are the addresses with all zero's and all one's host number. For example, an IP address 128.1.2.128, what IP address reserved will be looked like? All 0s mean the network itself, and all 1s mean IP broadcast.



In this diagram, you can see the subnet mask with 25-bit long, 255.255.255.128, contains 126 members in the sub-netted network. Another is that the length of network prefix equals the number of the bit with 1s in that subnet mask. With this, you can easily count the number of IP addresses matched. The following table shows the result.

| Prefix Length | No. of IP matched | No. of Addressable IP |
|---------------|-------------------|-----------------------|
| /32           | 1                 | -                     |
| /31           | 2                 | -                     |
| /30           | 4                 | 2                     |
| /29           | 8                 | 6                     |
| /28           | 16                | 14                    |
| /27           | 32                | 30                    |
| /26           | 64                | 62                    |
| /25           | 128               | 126                   |
| /24           | 256               | 254                   |
| /23           | 512               | 510                   |
| /22           | 1024              | 1022                  |
| /21           | 2048              | 2046                  |
| /20           | 4096              | 4094                  |
| /19           | 8192              | 8190                  |
| /18           | 16384             | 16382                 |
| /17           | 32768             | 32766                 |
| /16           | 65536             | 65534                 |

According to the scheme above, a subnet mask 255.255.255.0 will partition a network with the class C. It means there will have a maximum of 254 effective nodes existed in this sub-netted network and is considered a physical network in an autonomous network. So it owns a network IP address which may looks like 168.1.2.0.

With the subnet mask, a bigger network can be cut into small pieces of network. If we want to have more than two independent networks in a worknet, a partition to the network must be performed. In this case, subnet mask must be applied.

For different network applications, the subnet mask may look like 255.255.255.240. This means it is a small network accommodating a maximum of 15 nodes in the network.

For assigning an IP address to the switch, you just have to check what the IP address of the network will be connected with the switch. Use the same network address and append your host address to it.

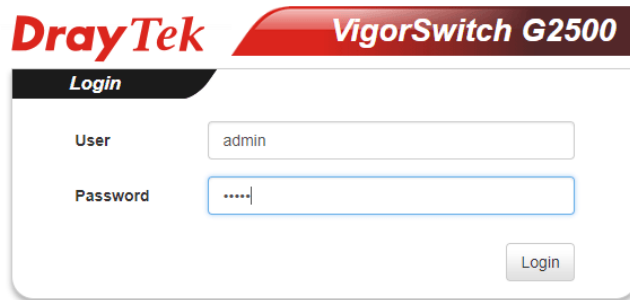
- ❖ First, IP Address: as shown above, enter "192.168.1.224", for instance. For sure, an IP address such as 192.168.1.x must be set on your PC.
- ❖ Second, Subnet Mask: as shown above, enter "255.255.255.0". Choose a subnet mask suitable for your network.

**Note:** The DHCP Setting is enabled in default. Therefore, if a DHCP server presented on network connected to the switch, check before accessing your switch is essential.

---

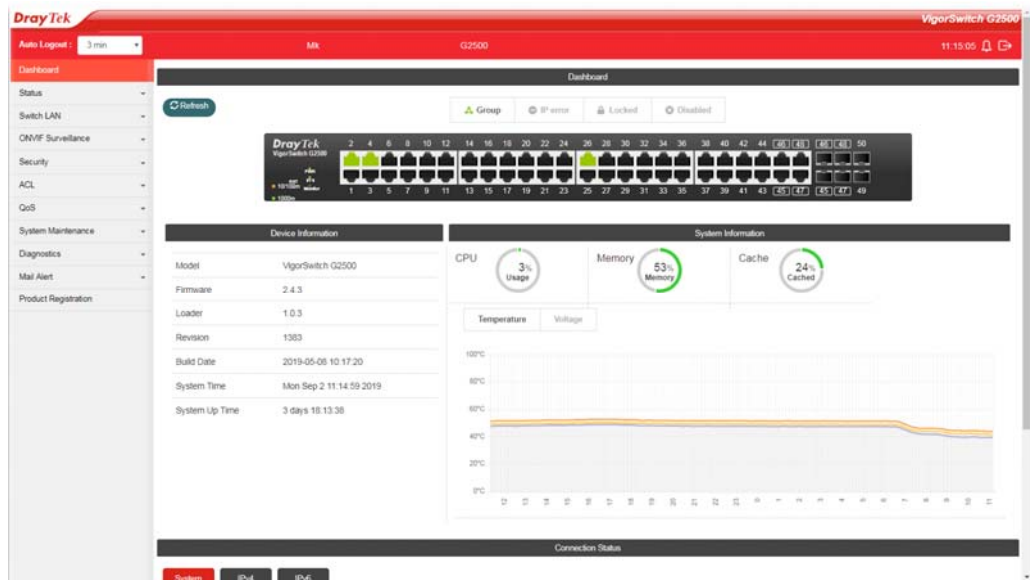
## I-3 Accessing Web Page of VigorSwitch

1. Open any browser (e.g., Firefox) and type "192.168.1.224" as URL.
2. Please type "admin/admin" as the Username/Password and click Login.



The image shows the login page for the VigorSwitch G2500. At the top left is the DrayTek logo, and at the top right is the device name "VigorSwitch G2500". Below this is a "Login" header. There are two input fields: "User" with the text "admin" and "Password" with masked characters ".....". A "Login" button is located at the bottom right of the form.

3. Now, the Main Screen will appear.



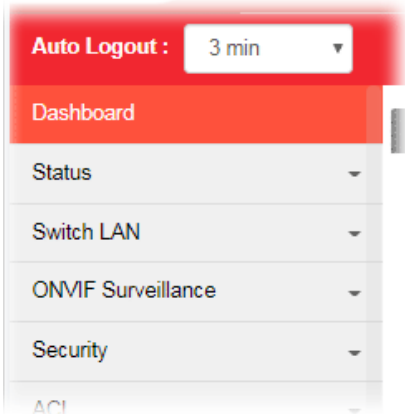
### Info

The DHCP Setting is enabled in default. Therefore, if a DHCP server presented on network connected to VigorSwitch, checking before accessing VigorSwitch is essential.

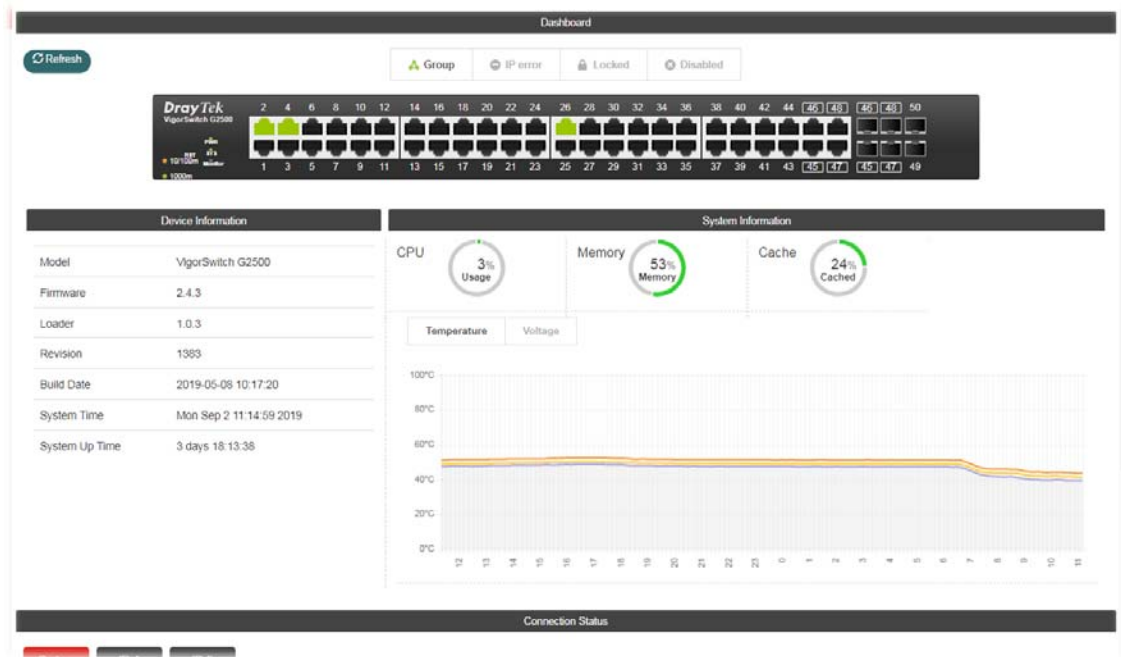


## I-4 Dashboard

Click Dashboard from the main menu on the left side of the main page.



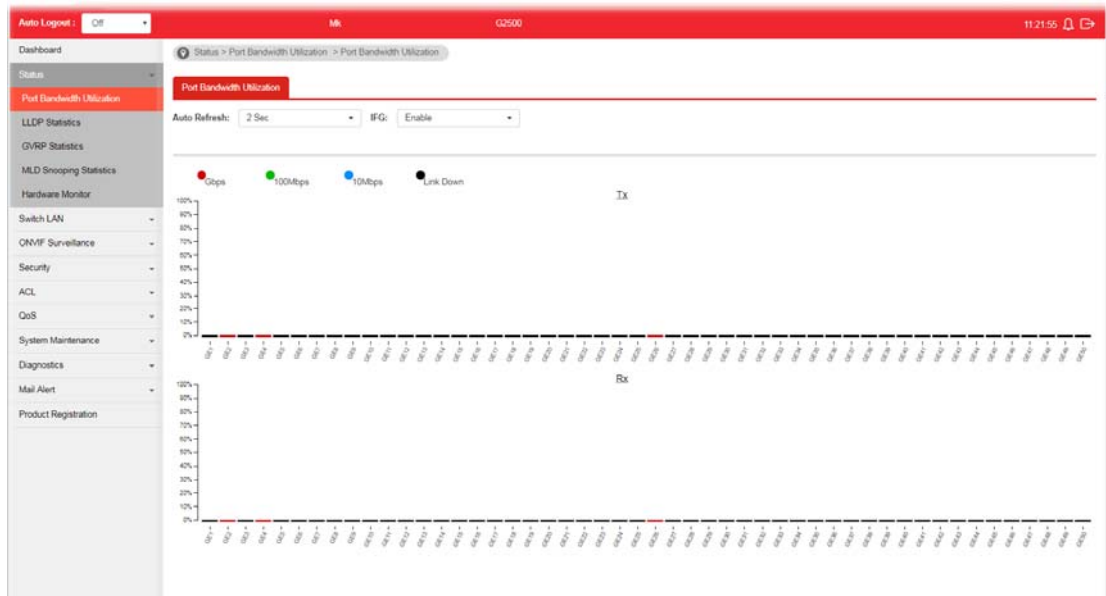
A web page with default selections will be displayed on the screen. Refer to the following figure:



# I-5 Status

## I-5-1 Port Bandwidth Utilization

This page offers the traffic statistics including data information and data of interframe gap for each port (GE1 to GE50). In which, data of interframe gap can be displayed or hidden by choose Enable / Disable for IFG.



## I-5-2 LLDP Statistics

This page offers the statistics of LLDP packets (in, out and error) of each port (GE1 to GE50).

The screenshot displays the 'LLDP Statistics' page. At the top, there is a navigation bar with 'Auto Logout: Off', 'Mk', 'G2500', and the time '11:23:12'. A sidebar on the left contains various menu items. The main content area shows 'LLDP Statistics' with 'Refresh' and 'Clear All' buttons. Below this, there are two sections: 'LLDP Global Statistics' and 'LLDP Port Statistics'. The 'LLDP Global Statistics' section shows a table with the following data:

|            |   |
|------------|---|
| Insertions | 3 |
| Deletions  | 0 |
| Drops      | 0 |
| Age Outs   | 0 |

The 'LLDP Port Statistics' section is a table with the following columns: Port, TX Frames Total, RX Frames Total, RX Frames Discarded, RX Frames Errors, RX TLVs Discarded, RX TLVs Unrecognized, and RX Ageouts Total. The data for each port is as follows:

| Port | TX Frames Total | RX Frames Total | RX Frames Discarded | RX Frames Errors | RX TLVs Discarded | RX TLVs Unrecognized | RX Ageouts Total |
|------|-----------------|-----------------|---------------------|------------------|-------------------|----------------------|------------------|
| GE1  | 0               | 0               | 0                   | 0                | 0                 | 0                    | 0                |
| GE2  | 10843           | 10843           | 0                   | 0                | 0                 | 0                    | 0                |
| GE3  | 0               | 0               | 0                   | 0                | 0                 | 0                    | 0                |
| GE4  | 10843           | 10530           | 0                   | 0                | 0                 | 0                    | 0                |
| GE5  | 0               | 0               | 0                   | 0                | 0                 | 0                    | 0                |
| GE6  | 0               | 0               | 0                   | 0                | 0                 | 0                    | 0                |
| GE7  | 0               | 0               | 0                   | 0                | 0                 | 0                    | 0                |
| GE8  | 0               | 0               | 0                   | 0                | 0                 | 0                    | 0                |
| GE9  | 0               | 0               | 0                   | 0                | 0                 | 0                    | 0                |

## I-5-3 GVRP Statistics

GVRP (Generic Attribute Registration Protocol) is used automatically for exchanging information for VLAN membership between switches. This page counts the GVRP information received on each port.

The screenshot shows the GVRP Statistics page with the following configuration and data:

- Port:** Nothing selected
- Statistics:** Transmit, Receive, Error
- Refresh Rate:** 10 sec

**Tx Statistics**

| Port                       | Join empty | Empty | Leave Empty | Join In | Leave In | Leave All |
|----------------------------|------------|-------|-------------|---------|----------|-----------|
| No data available in table |            |       |             |         |          |           |

**Rx Statistics**

| Port                       | Join empty | Empty | Leave Empty | Join In | Leave In | Leave All |
|----------------------------|------------|-------|-------------|---------|----------|-----------|
| No data available in table |            |       |             |         |          |           |

**Error Statistics**

| Port                       | Invalid Protocol ID | Invalid Attribute Type | Invalid Attribute Value | Invalid Attribute Length | Invalid Event |
|----------------------------|---------------------|------------------------|-------------------------|--------------------------|---------------|
| No data available in table |                     |                        |                         |                          |               |

## I-5-4 MLD Snooping Statistics

This page counts the MLD messages received or transmitted on the network.

The screenshot shows the MLD Snooping Statistics page with the following data:

**Rx Statistics**

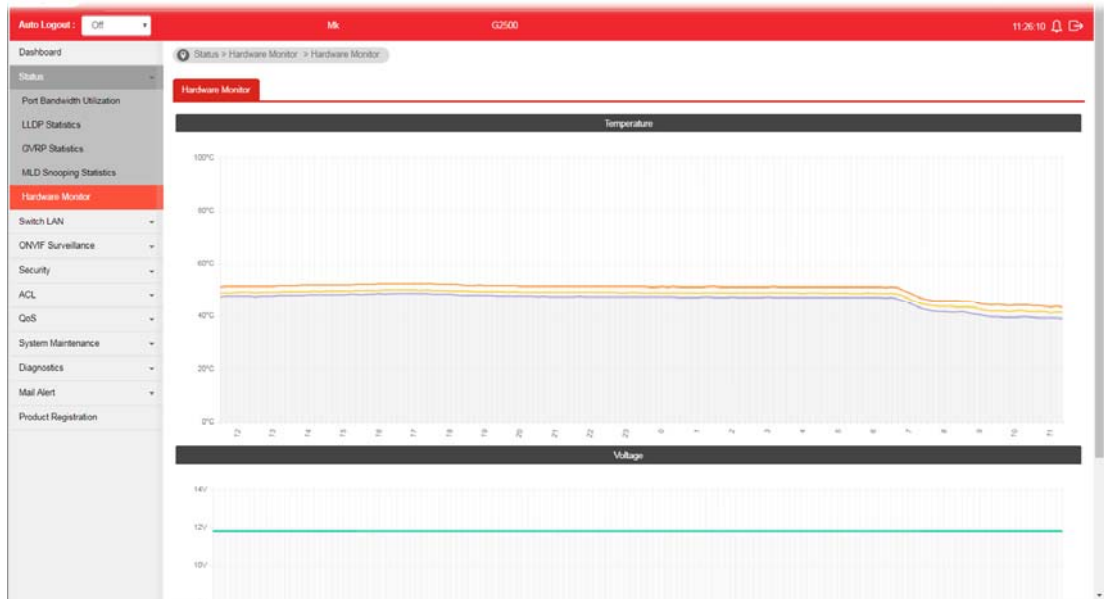
|                                |   |
|--------------------------------|---|
| Rx Total                       | 0 |
| Rx Valid                       | 0 |
| Rx Invalid                     | 0 |
| Rx Other                       | 0 |
| Rx Leave                       | 0 |
| Rx Report                      | 0 |
| Rx General Query               | 0 |
| Rx Special Group Query         | 0 |
| Rx Source-specific Group Query | 0 |

**Tx Statistics**

|                                |   |
|--------------------------------|---|
| Tx Leave                       | 0 |
| Tx Report                      | 0 |
| Tx General Query               | 0 |
| Tx Special Group Query         | 0 |
| Tx Source-specific Group Query | 0 |

## I-5-5 Hardware Monitor

This page displays the temperature change and voltage of VigorSwitch.



# Part II Switch LAN

## II-1 General Setup

General setup is used to configure settings for the switch network interface and offers how the switch connects to a remote server to get services.

### II-1-1 IP Address

Use the IP Address screen to configure the switch IP address and the default gateway device. The gateway field specifies the IP address of the gateway (next hop) for outgoing traffic.

The switch needs an IP address for it to be managed over the network. The factory default IP address is 192.168.1.224. The subnet mask specifies the network number portion of an IP address. The factory default subnet mask is 255.255.255.0.



#### Info

If VigorSwitch has connected to Vigor router, it will use the IP address obtained from the DHCP server on Vigor router. Thus, the user must type the assigned IP as URL for accessing into the web user interface of VigorSwitch. If not, 192.168.1.224 shall be the default IP.

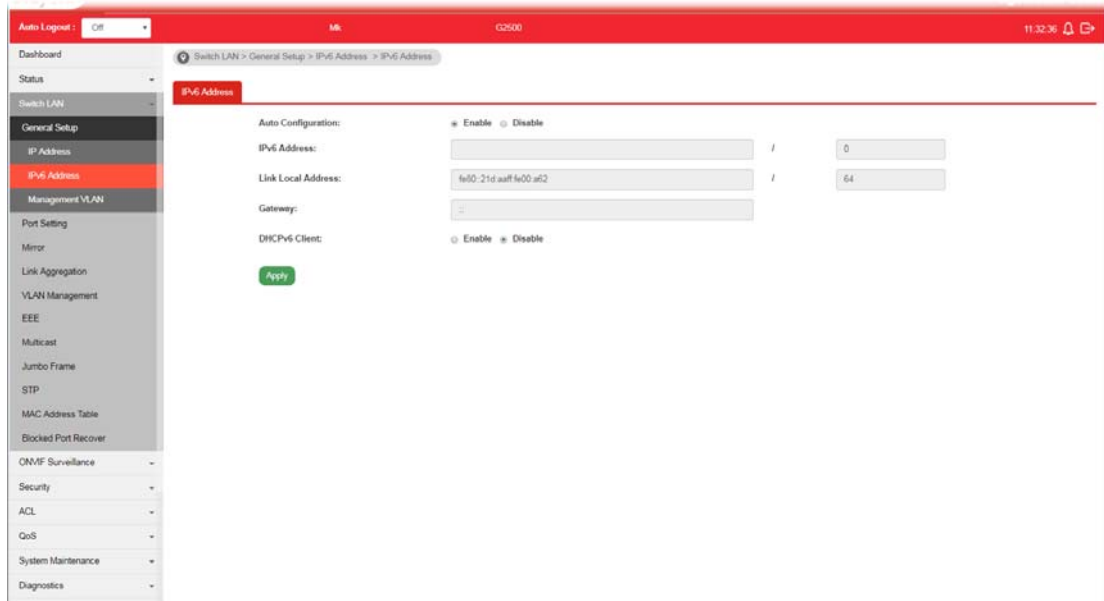
Available settings are explained as follows:

| Item        | Description   |
|-------------|---|
| Mode        | Select the mode of network connection. <ul style="list-style-type: none"><li>● <b>Static</b>- Use static IPv4 address.</li><li>● <b>DHCP</b> - Use DHCP provisioned IP address and Gateway if feasible.</li></ul>       |
| IP Address  | It is available when <b>Static</b> is selected as <b>Mode</b> .<br>Enter the IP address of your switch in dotted decimal notation for example 192.168.1.224. If static mode is enabled, enter IP address in this field. |
| Subnet Mask | It is available when <b>Static</b> is selected as <b>Mode</b> .<br>Enter the IP subnet mask of your switch in dotted decimal  |

|              |  |
|--------------|--|
|              | notation for example 255.255.255.0. If static mode is enabled, enter subnet mask in this field.  |
| Gateway      | It is available when <b>Static</b> is selected as <b>Mode</b> .<br>Enter the IP address of the gateway in dotted decimal notation. If static mode is enabled, enter gateway address in this field. |
| DNS Server 1 | It is available when <b>Static</b> is selected as <b>Mode</b> .<br>If static mode is enabled, enter primary DNS server address in this field.  |
| DNS Server 2 | It is available when <b>Static</b> is selected as <b>Mode</b> .<br>If static mode is enabled, enter secondary DNS server address in this field.  |
| Apply        | Apply the settings to the switch.  |

## II-1-2 IPv6 Address

Use the IPv6 Address screen to configure the switch IPv6 address and the default gateway device. The gateway field specifies the IPv6 address of the gateway (next hop) for outgoing traffic.



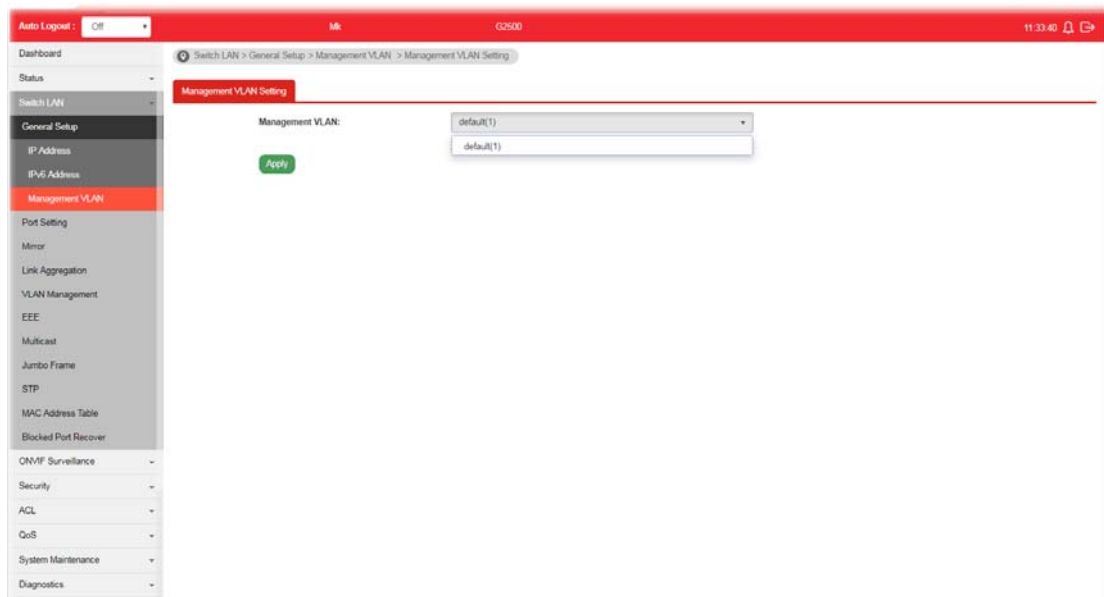
Available settings are explained as follows:

| Item               | Description   |
|--------------------|---|
| Auto Configuration | <b>Enable</b> - Check it to let switch automatically configure IPv6 address.  |
| IPv6 Address       | It is available when <b>Auto Configuration</b> is set as <b>Disable</b> .<br>Enter the IPv6 address of your switch. If auto configuration mode is disabled, enter IPv6 address in this field. |
| Link Local Address | Display link local address.   |
| Gateway            | It is available when <b>Auto Configuration</b> is set as <b>Disable</b> .<br>Enter the IPv6 address of the router as your default IPv6  |

|               |  |
|---------------|--|
|               | gateway to access IPv6 Internet or other IPv6 network.   |
| DNS Server 1  | It is available when <b>Auto Configuration</b> is set as <b>Disable</b> .<br>If static mode is enabled, enter primary DNS server address in this field.  |
| DNS Server 2  | It is available when <b>Auto Configuration</b> is set as <b>Disable</b> .<br>If static mode is enabled, enter secondary DNS server address in this field.  |
| DHCPv6 Client | It is available when <b>Auto Configuration</b> is set as <b>Enable</b> .<br>Enable this feature if there is a DHCPv6 server on your network for assigning IPv6 Address, instead of using Router Advertisement. |
| Apply         | Apply the settings to the switch.  |

## II-1-3 Management VLAN

This page allows the network administrator to change the VLAN ID of management access. Management access protocols such as http, https, SNMP and etc., are only accessible from the VLAN specified as management VLAN.



Available settings are explained as follows:

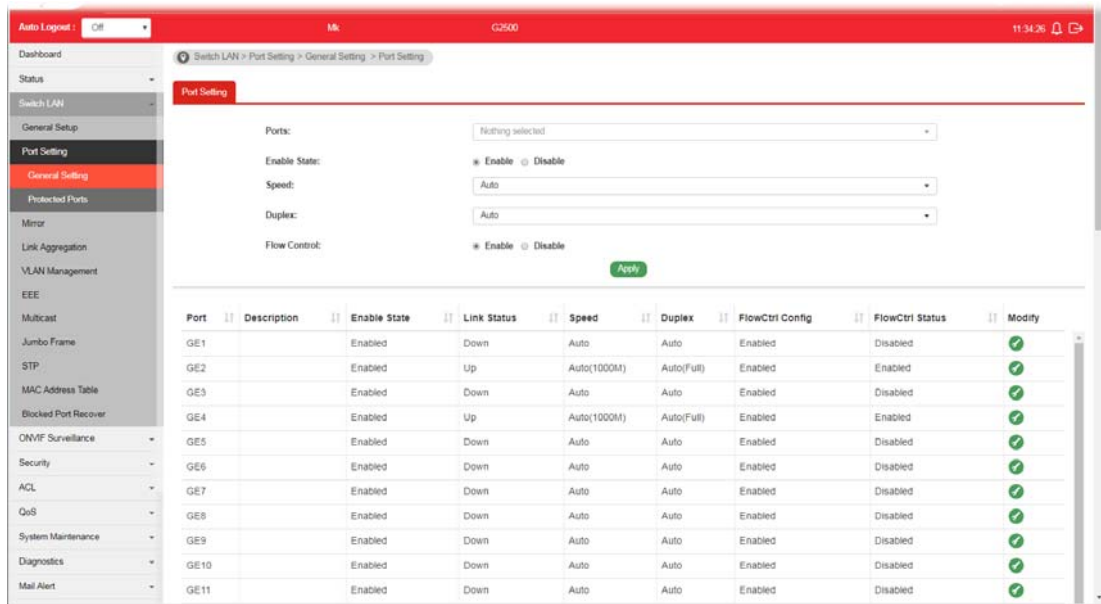
| Item            | Description  |
|-----------------|--|
| Management VLAN | Select the VLAN ID as management VLAN. You can create additional VLAN profiles by <b>Switch LAN&gt;&gt;VLAN management&gt;&gt; Create VLAN</b> . |
| Apply           | Apply the settings to the switch.  |



## II-2 Port Setting

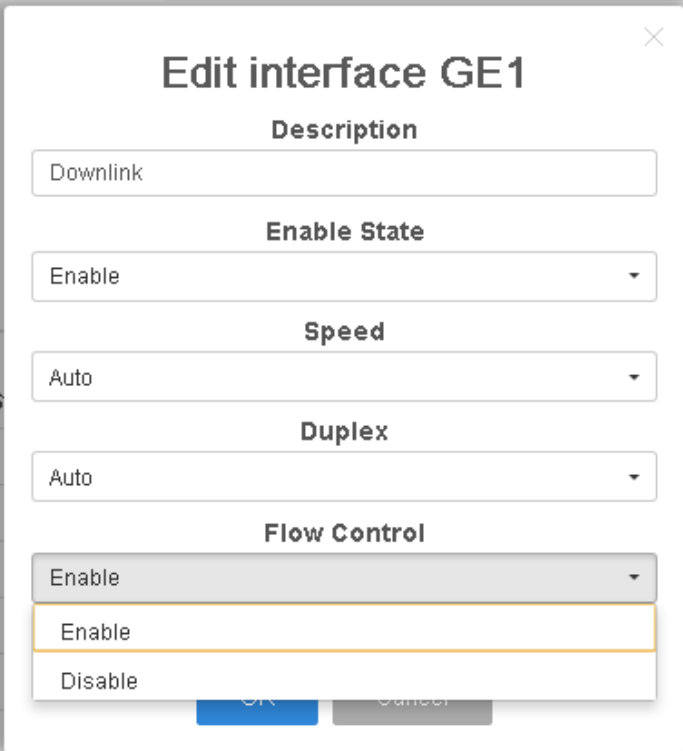
### II-2-1 General Setting

Port Setting is used to configure settings for the switch ports, trunk, Layer 2 protocols and other switch features.



Available settings are explained as follows:

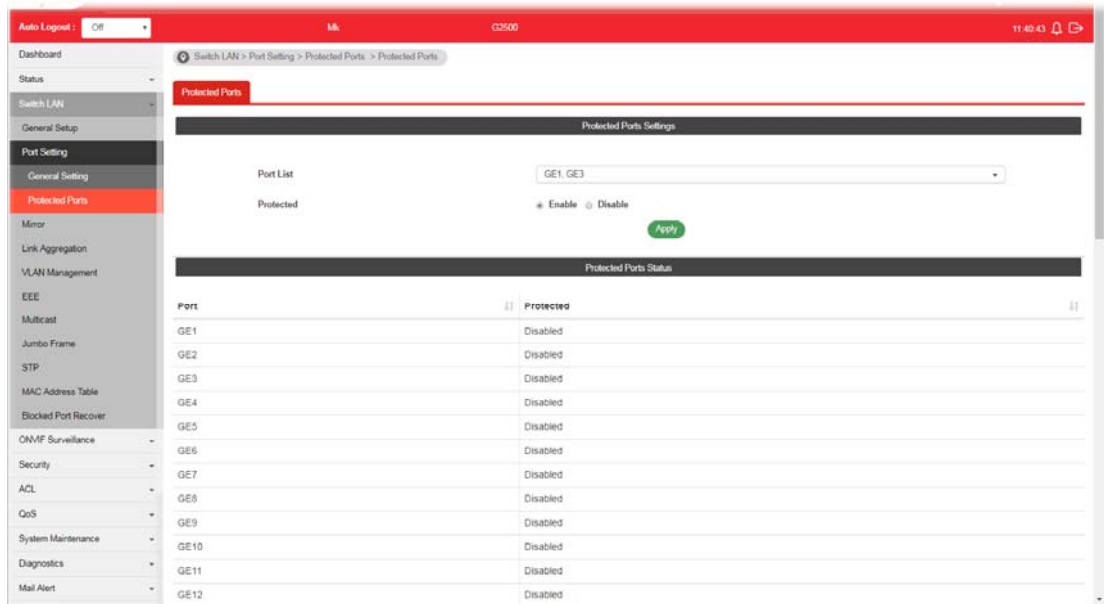
| Item         | Description  |
|--------------|--|
| Ports        | Use the drop down list to select one or more LAN port(s).  |
| Enable State | <p><b>Enable</b> - Click it to enable the port.</p> <p><b>Disable</b> - Click it to disable the port.</p>  |
| Speed        | <p>Port speed capabilities:</p> <ul style="list-style-type: none"> <li>● <b>Auto</b>: Auto speed with all capabilities.</li> <li>● <b>Auto-10M</b>: Auto speed with 10M ability only.</li> <li>● <b>Auto-100M</b>: Auto speed with 100M ability only.</li> <li>● <b>Auto-1000M</b>: Auto speed with 1000M ability only.</li> <li>● <b>Auto-10/100M</b>: Auto speed with 10/100M ability.</li> <li>● <b>10M</b>: Force speed with 10M ability.</li> <li>● <b>100M</b>: Force speed with 100M ability.</li> <li>● <b>1000M</b>: Force speed with 1000M ability.</li> </ul> <p>Selecting Auto (auto-negotiation) allows one port to negotiate with a peer port automatically to obtain the connection speed and duplex mode that both ends support. When auto-negotiation is turned on, a port on the switch negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer port does not support auto-negotiation or turns off this feature, the switch determines the connection speed by detecting the signal on the cable and using half duplex mode. When the switch's auto-negotiation is turned off, a port uses the pre-configured</p> |

|              |  |
|--------------|--|
|              | <p>speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer port are the same in order to connect.</p> <p>For SFP fiber module, you might need to manually configure the speed to match fiber module speed.</p>   |
| Duplex       | <p>Port duplex capabilities:</p> <ul style="list-style-type: none"> <li>● <b>Auto:</b> Auto duplex with all capabilities.</li> <li>● <b>Half:</b> Auto speed with 10/100M ability only.</li> <li>● <b>Full:</b> Auto speed with 10/100/1000M ability only.</li> </ul>  |
| Flow Control | <p>A concentration of traffic on a port decreases port bandwidth and overflows buffer memory causing packet discards and frame losses. Flow Control is used to regulate transmission of signals to match the bandwidth of the receiving port. The switch uses IEEE802.3x flow control in full duplex mode and backpressure flow control in half duplex mode. IEEE802.3x flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill. Back Pressure flow control is typically used in half duplex mode to send a "collision" signal to the sending port (mimicking a state of packet collision) causing the sending port to temporarily stop sending signals and resend later.</p> <ul style="list-style-type: none"> <li>● <b>Enable</b> - Click it to enable such function.</li> <li>● <b>Disable</b> - Click it to disable such function.</li> </ul> |
| Apply        | Apply the settings to the switch.  |
| Modify       | <p>It is used to manually enter the description, state, speed, duplex, flow control for the port.</p>    |

## II-2-2 Protected Ports

This page allows the network administrator to configure protected port setting to prevent the selected ports from communication with each other. Protected port is only allowed to communicate with unprotected port.

For example, GE1 and GE3 are selected in Port List and Enable is clicked as Protected, then users behind GE1 and GE3 are separated and can not communicate with each other.



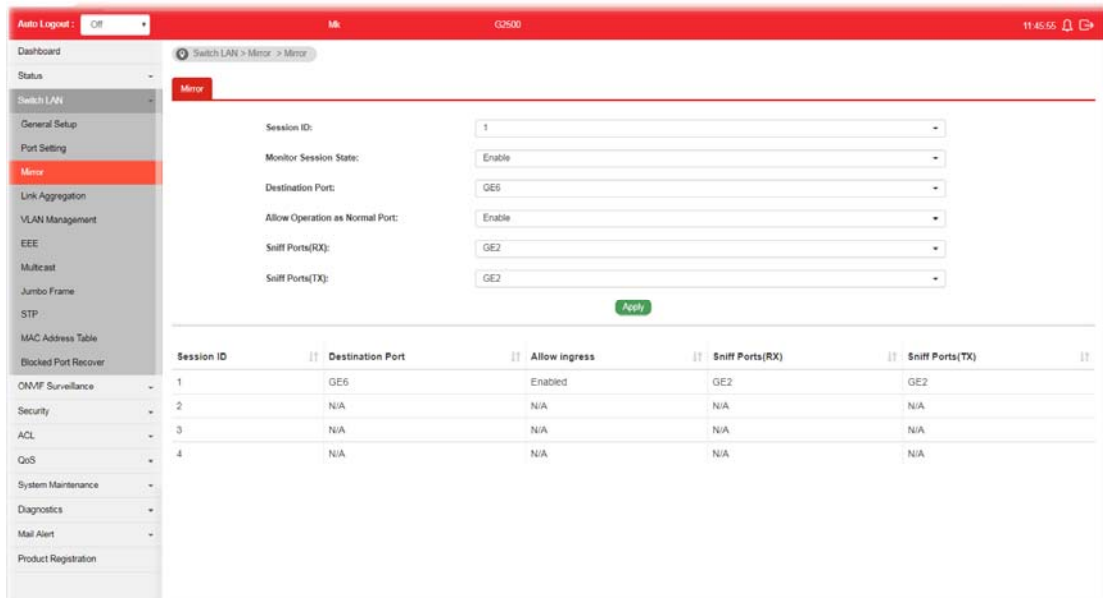
Available settings are explained as follows:

| Item                     | Description  |
|--------------------------|--|
| Protected Ports Settings | <ul style="list-style-type: none"> <li>● <b>Port List</b> - Use the drop down list to select the port(s) (GE1 to GE50) for applying the settings configured in this page.</li> <li>● <b>Protected</b> - Click <b>Enable</b> to activate the protected port function.</li> <li>● <b>Apply</b> - The modification made above can be applied on to the selected GE port immediately.</li> </ul> |
| Protected Port Status    | Display current status for each GE port.   |

## II-3 Mirror

This section provides ability to mirror packets coming in or going out on any port to a destination port. Through the packet duplication in the destination port, this feature is convenient for system administrator to monitor / understand the traffic operation.

Session ID 1 to 4 can be enabled simultaneously and operate independently.



Available settings are explained as follows:

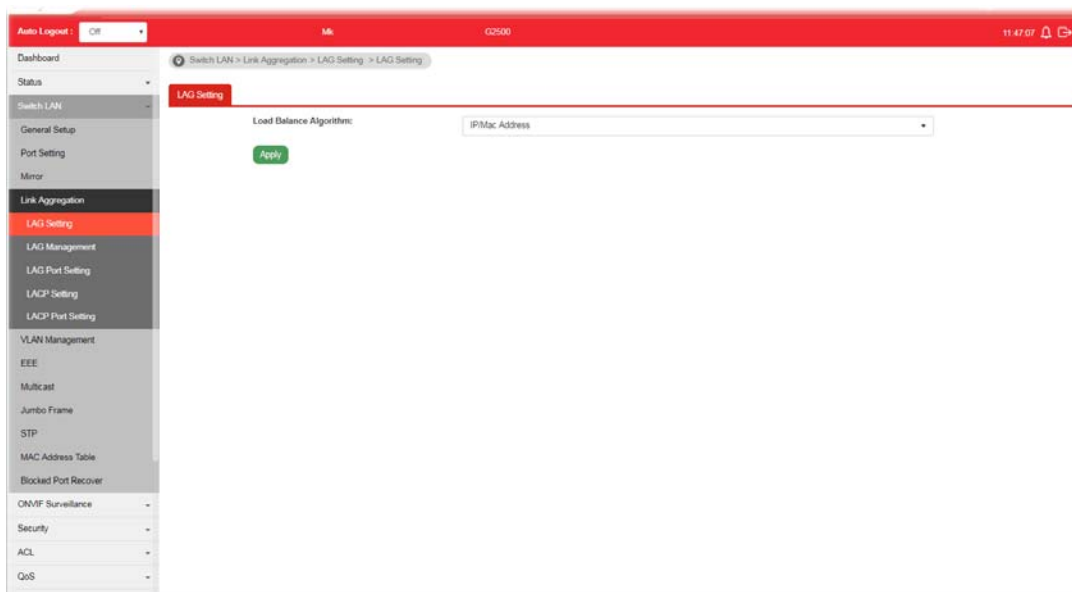
| Item                           | Description  |
|--------------------------------|--|
| Session ID                     | Select the session ID (profile 1 to 4) of mirror operation you wish to configure.  |
| Monitor Session State          | <ul style="list-style-type: none"> <li>● <b>Enable</b> - Enable specified mirror session.</li> <li>● <b>Disable</b> - Disable specified mirror session.</li> </ul>   |
| Destination Port               | Specify the port where you wish to observe the mirrored packets.   |
| Allow Operation as Normal Port | <ul style="list-style-type: none"> <li>● <b>Enable</b> - The destination port is able to function as a port connecting to network, communicating with other network devices.</li> <li>● <b>Disable</b> - Only observe the mirrored packets.</li> </ul> |
| Sniff Ports (RX) / (TX)        | Select the port(s) which you wish to mirror the traffic, Rx for mirror the packets into the port, Tx for mirror the packets going out from the port.   |
| Apply                          | Apply the settings to the switch.  |

## II-4 Link Aggregation

LAG means Link Aggregation Group which groups some physical ports together to make a single high-bandwidth data path. Thus it can implement traffic load sharing among the member ports in a group to enhance the connection reliability.

### II-4-1 LAG Setting

This page allows to configure Load Balance Algorithm for Link Aggregation.



Available settings are explained as follows:

| Item                   | Description   |
|------------------------|---|
| Load Balance Algorithm | Select your Load balance algorithm. <ul style="list-style-type: none"><li>● <b>MAC address</b> - Aggregated group will balance the traffic based on different MAC addresses. Therefore, the packets from different MAC addresses will be sent to different links.</li><li>● <b>IP/Mac Address</b> - Aggregated group will balance the traffic based on MAC addresses and IP addresses. Therefore, the packets from same MAC addresses but different IP addresses will be sent to different links.</li></ul> |
| Apply                  | Apply the settings to the switch.   |

## II-4-2 LAG Management

There are eight LAG profiles allowed to group different physical ports. The system will assign certain port(s) as Active Member and Standby Member according to the GE selections.

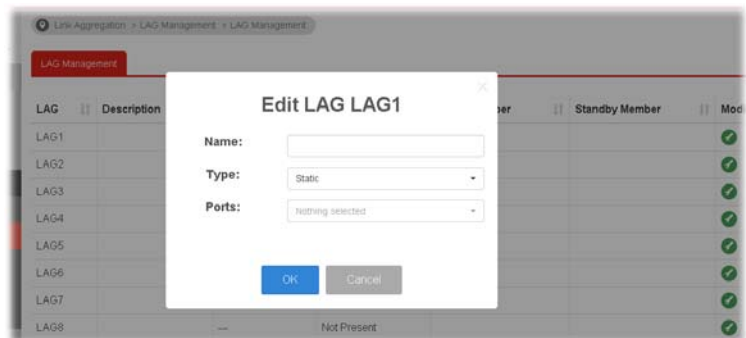
| LAG   | Description | Port Type | Link Status | Active Member | Standby Member | Modify |
|-------|-------------|-----------|-------------|---------------|----------------|--------|
| LAG1  | test1       | ---       | Not Present |               |                | ✓      |
| LAG2  |             | ---       | Not Present |               |                | ✓      |
| LAG3  |             | ---       | Not Present |               |                | ✓      |
| LAG4  |             | ---       | Not Present |               |                | ✓      |
| LAG5  |             | ---       | Not Present |               |                | ✓      |
| LAG6  |             | ---       | Not Present |               |                | ✓      |
| LAG7  |             | ---       | Not Present |               |                | ✓      |
| LAG8  |             | ---       | Not Present |               |                | ✓      |
| LAG9  |             | ---       | Not Present |               |                | ✓      |
| LAG10 |             | ---       | Not Present |               |                | ✓      |
| LAG11 |             | ---       | Not Present |               |                | ✓      |
| LAG12 |             | ---       | Not Present |               |                | ✓      |
| LAG13 |             | ---       | Not Present |               |                | ✓      |
| LAG14 |             | ---       | Not Present |               |                | ✓      |
| LAG15 |             | ---       | Not Present |               |                | ✓      |
| LAG16 |             | ---       | Not Present |               |                | ✓      |

Available settings are explained as follows:

| Item           | Description  |
|----------------|--|
| Description    | Display the port description.                          |
| Port Type      | Display the type of the LAG.                           |
| Link Status    | Display LAG port link status.                          |
| Active Member  | Display active member ports of the LAG.                |
| Standby Member | Display inactive or candidate member ports of the LAG. |

### Modify

It is used to edit the name, type and port number for each link aggregation profile.



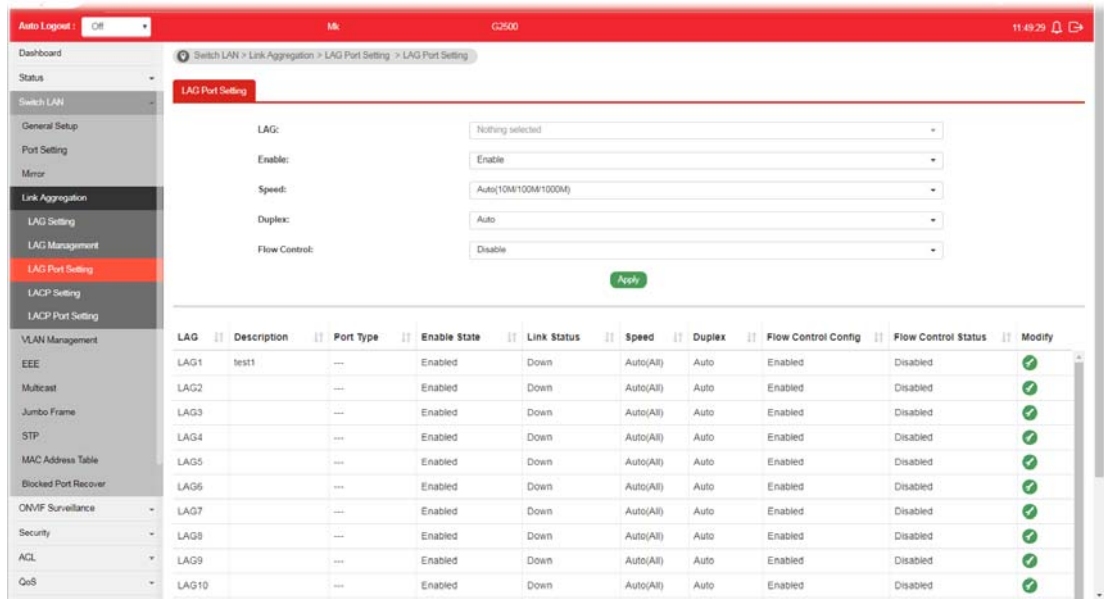
**Name-** Enter a string as LAG name.

**Type -** Use the drop down menu to specify the type for LAG.

- **Static-** The static aggregated port sends packets over active member without detecting or negotiating with remote aggregated port.
- **LACP-** The LACP aggregated ports place member into active only after negotiated with remote aggregated port for best reliability.

## II-4-3 LAG Port Setting

This page defines port setting for each LAG profile (LAG1 to LAG16), including data speed and enabling/disabling the flow control.



Available settings are explained as follows:

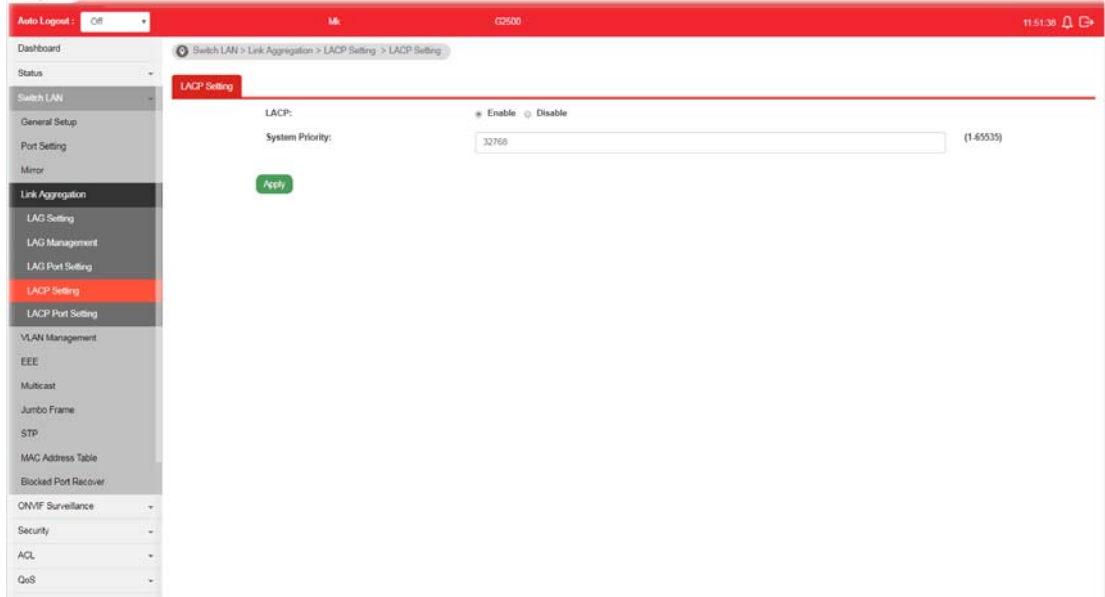
| Item   | Description   |
|--------|---|
| LAG    | Use the drop down list to select one or more LAG profiles.  |
| Enable | <ul style="list-style-type: none"> <li>● Enable -Click it to enable the profile.</li> <li>● Disable - Click it to disable the profile.</li> </ul>   |
| Speed  | <p>Port speed capabilities:</p> <ul style="list-style-type: none"> <li>● Auto: Auto speed with all capabilities.</li> <li>● Auto-10M: Auto speed with 10M ability only.</li> <li>● Auto-100M: Auto speed with 100M ability only.</li> <li>● Auto-1000M: Auto speed with 1000M ability only.</li> <li>● Auto-10/100M: Auto speed with 10/100M ability.</li> <li>● 10M: Force speed with 10M ability.</li> <li>● 100M: Force speed with 100M ability.</li> <li>● 1000M: Force speed with 1000M ability.</li> <li>● 10G: Force speed with 10G ability.</li> </ul> <p>Selecting Auto (auto-negotiation) allows one port to negotiate with a peer port automatically to obtain the connection speed and duplex mode that both ends support. When auto-negotiation is turned on, a port on the switch negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer port does not support auto-negotiation or turns off this feature, the switch determines the connection speed by detecting the signal on the cable and using half duplex mode. When the switch's auto-negotiation is turned off, a port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer port are the same in order to connect.</p> <p>For SFP fiber module, you might need to manually configure</p> |

|                     |  |
|---------------------|--|
|                     | the speed to match fiber module speed.   |
| <b>Duplex</b>       | <p>Port duplex capabilities:</p> <ul style="list-style-type: none"> <li>● <b>Auto:</b> Auto duplex with all capabilities.</li> <li>● <b>Half:</b> Auto speed with 10/100M ability only.</li> <li>● <b>Full:</b> Auto speed with 10/100/1000M /10G ability only.</li> </ul>   |
| <b>Flow Control</b> | <p>A concentration of traffic on a port decreases port bandwidth and overflows buffer memory causing packet discards and frame losses. Flow Control is used to regulate transmission of signals to match the bandwidth of the receiving port. The switch uses IEEE802.3x flow control in full duplex mode and backpressure flow control in half duplex mode. IEEE802.3x flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill. Back Pressure flow control is typically used in half duplex mode to send a "collision" signal to the sending port (mimicking a state of packet collision) causing the sending port to temporarily stop sending signals and resend later.</p> <ul style="list-style-type: none"> <li>● <b>Enable</b> - Click it to enable such function.</li> <li>● <b>Disable</b> - Click it to disable such function.</li> </ul> |
| <b>Apply</b>        | Apply the settings to the switch.  |
| <b>Modify</b>       | It is used to edit status, speed, and flow control for the LAG.  |



## II-4-4 LACP Setting

This page allows the network administrator to enable or disable the LACP function.

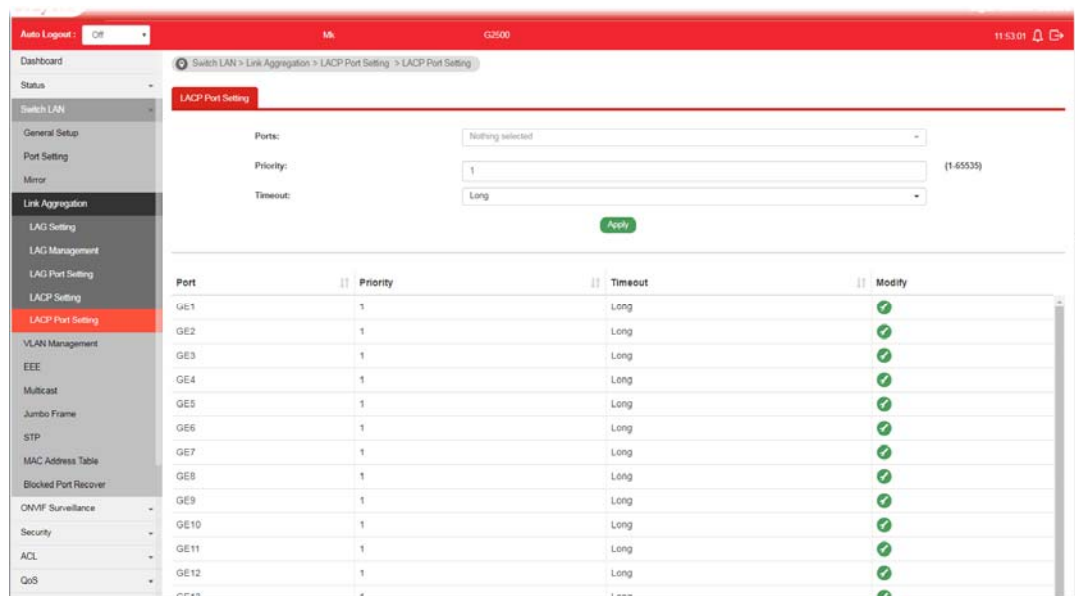


Available settings are explained as follows:

| Item            | Description  |
|-----------------|--|
| LACP            | <ul style="list-style-type: none"><li>● <b>Enable</b> - Click it to enable such function.</li><li>● <b>Disable</b> - Click it to disable the function.</li></ul>   |
| System Priority | The priority is used to determine which switch (local or remote) on the LAG connection is able to decide LACP activities. The lower the number is, the higher the priority for VigorSwitch will be. Therefore, the switch with the highest system priority (e.g., 1) can make decisions about which ports actively participate in LAG at a given time. |
| Apply           | Apply the settings to the switch.  |

## II-4-5 LACP Port Setting

This section provides few detailed configuration regarding to Ports under LACP protocol.



Available settings are explained as follows:

| Item     | Description   |
|----------|---|
| Ports    | Use the drop down list to specify LAN Port.   |
| Priority | Enter a port priority number for the port.  |
| Timeout  | <p>The timeout option decides how local switch of LAG connection determines connection to be lost. Switch would also notify the remote switch about this setting value, so that remote switch can send LACP PDU in correct timing.</p> <ul style="list-style-type: none"> <li>● <b>Long</b> - LACP PDU will be sent every 30 seconds. If port member is not seen over 90 seconds, it will cause port member timeout.</li> <li>● <b>Short</b> - LACP PDU will be sent per second. If port member is not seen over 3 seconds, it will cause port member timeout.</li> </ul> |
| Apply    | Apply the settings to the switch.   |
| Modify   | It is used to edit settings (priority and timeout) for LACP port.   |

## II-5 VLAN Management

A virtual local area network, virtual LAN or VLAN, is a group of hosts with a common set of requirements that communicate as if they were attached to the same broadcast domain, regardless of their physical location. A VLAN has the same attributes as a physical local area network (LAN), but it allows for end stations to be grouped together even if they are not located on the same network switch. VLAN membership can be configured through software instead of physically relocating devices or connections.

### II-5-1 Create VLAN

This page allows a user to add, edit or delete VLAN settings.

Available settings are explained as follows:

| Item      | Description   |           |   |           |        |   |         |         |                                      |   |               |        |   |   |               |        |   |
|-----------|---|-----------|---|-----------|--------|---|---------|---------|--------------------------------------|---|---------------|--------|---|---|---------------|--------|---|
| Action    | Select which action to perform, add VLANs or delete VLANs. <ul style="list-style-type: none"> <li>● Add - Create a new VLAN profile.</li> <li>● Delete - Delete an existed VLAN profile.</li> </ul>   |           |   |           |        |   |         |         |                                      |   |               |        |   |   |               |        |   |
| VLAN ID   | Enter the number as VLAN ID to be created or deleted. If you want to create / delete multiple VLAN profiles, simply enter multiple VLAN ID separated by comma, and/or range of VLAN ID using hyphen.  |           |   |           |        |   |         |         |                                      |   |               |        |   |   |               |        |   |
| VLAN Name | Enter the prefix you wish to add followed by VLAN ID as VLAN name. Leave it empty for using default "VLAN".<br>After clicking Apply, you will see: <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <table border="1"> <thead> <tr> <th>VLAN ID</th> <th>VLAN Name</th> <th>VLAN Type</th> <th>Modify</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>default</td> <td>Default</td> <td><span style="color: green;">✔</span></td> </tr> <tr> <td>2</td> <td>marketing0002</td> <td>Static</td> <td><span style="color: green;">✔</span> <span style="color: red;">✘</span></td> </tr> <tr> <td>3</td> <td>marketing0003</td> <td>Static</td> <td><span style="color: green;">✔</span> <span style="color: red;">✘</span></td> </tr> </tbody> </table> </div> | VLAN ID   | VLAN Name   | VLAN Type | Modify | 1 | default | Default | <span style="color: green;">✔</span> | 2 | marketing0002 | Static | <span style="color: green;">✔</span> <span style="color: red;">✘</span> | 3 | marketing0003 | Static | <span style="color: green;">✔</span> <span style="color: red;">✘</span> |
| VLAN ID   | VLAN Name   | VLAN Type | Modify  |           |        |   |         |         |                                      |   |               |        |   |   |               |        |   |
| 1         | default   | Default   | <span style="color: green;">✔</span>                                    |           |        |   |         |         |                                      |   |               |        |   |   |               |        |   |
| 2         | marketing0002   | Static    | <span style="color: green;">✔</span> <span style="color: red;">✘</span> |           |        |   |         |         |                                      |   |               |        |   |   |               |        |   |
| 3         | marketing0003   | Static    | <span style="color: green;">✔</span> <span style="color: red;">✘</span> |           |        |   |         |         |                                      |   |               |        |   |   |               |        |   |
| Apply     | Apply the settings to the switch.   |           |   |           |        |   |         |         |                                      |   |               |        |   |   |               |        |   |

## Modify



- Modify the name of the selected VLAN ID.

- New Name - Type a name for such VLAN profile.
- OK - Apply the settings to the switch.
- Cancel - Close the page and return to previous page.



- Delete the selected VALN ID.


## II-5-2 Interface Settings

This page allows a user to configure interface setting related to VLAN.

| Port | Interface VLAN | PVID | Tagged VLAN | Untagged VLAN | Forbidden VLAN | Accept Frame T... | Ingress Filtering | Uplink   | TPID   | Modify |
|------|----------------|------|-------------|---------------|----------------|-------------------|-------------------|----------|--------|--------|
| GE1  | Trunk          | 1    | ---         | 1             | ---            | ALL               | Enabled           | Disabled | 0x8100 | ✓      |
| GE2  | Trunk          | 1    | ---         | 1             | ---            | ALL               | Enabled           | Disabled | 0x8100 | ✓      |
| GE3  | Trunk          | 1    | ---         | 1             | ---            | ALL               | Enabled           | Disabled | 0x8100 | ✓      |
| GE4  | Trunk          | 1    | ---         | 1             | ---            | ALL               | Enabled           | Disabled | 0x8100 | ✓      |
| GE5  | Trunk          | 1    | ---         | 1             | ---            | ALL               | Enabled           | Disabled | 0x8100 | ✓      |
| GE6  | Trunk          | 1    | ---         | 1             | ---            | ALL               | Enabled           | Disabled | 0x8100 | ✓      |
| GE7  | Trunk          | 1    | ---         | 1             | ---            | ALL               | Enabled           | Disabled | 0x8100 | ✓      |

Available settings are explained as follows:

| Item                | Description  |
|---------------------|--|
| Port Select         | Select LAN ports to configure VLAN Settings.   |
| Interface VLAN Mode | Select the VLAN mode of the interface. <ul style="list-style-type: none"><li>● Hybrid - Support all functions as defined in IEEE 802.1Q specification.</li><li>● Access - Accept only untagged frames and join an untagged VLAN.</li></ul> |

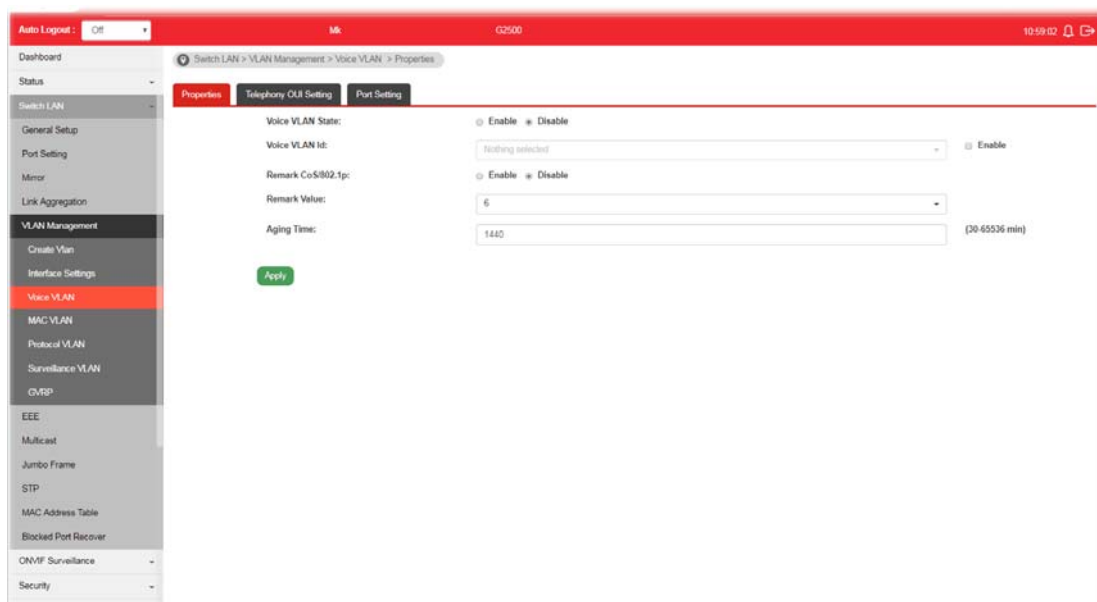
|                          |  |
|--------------------------|--|
|                          | <ul style="list-style-type: none"> <li>● <b>Trunk</b> - An untagged member of one VLAN at most, and is a tagged member of zero or more VLANs.</li> </ul>   |
| <b>PVID</b>              | <p>A PVID (Port VLAN ID) is a tag that adds to incoming untagged frames received on a port so that the frames are forwarded to the VLAN group that the tag defines.</p> <p>For port under <b>Access Mode</b>, VLAN ID provided as PVID would automatically be selected as the untagged VLAN.</p>   |
| <b>Accepted Type</b>     | <p>Specify the acceptable-frame-type of the specified interfaces. It's only available with Hybrid mode.</p> <ul style="list-style-type: none"> <li>● <b>All</b> - Accept frames regardless it's tagged with 802.1q or not.</li> <li>● <b>Tag Only</b> - Accept frames only with 802.1q tagged.</li> <li>● <b>Untag Only</b> - Accept frames untagged.</li> </ul> |
| <b>Ingress Filtering</b> | <p>Enable the ingress filtering to filter out any packets not belong to any VLAN members of this port. It is enabled automatically while operating in Access and Trunk mode.</p> <ul style="list-style-type: none"> <li>● <b>Enabled</b> - Click it to enable the function.</li> <li>● <b>Disabled</b> - Click it to disable the function.</li> </ul>            |
| <b>Tagged VLAN</b>       | Specify the VLAN profile tagged in the VLAN.   |
| <b>Untagged VLAN</b>     | Specify the VLAN profile untagged in the VLAN.   |
| <b>Forbidden VLAN</b>    | Specify the VLAN profile forbidden in the VLAN.  |
| <b>Apply</b>             | Apply the settings to the switch.  |
| <b>Modify</b>            |  - It is used to edit settings for the selected port.   |

## II-5-3 Voice VLAN

With such feature, a VLAN will be created temporarily and when the specified OUI device delivers protocol packets related to "VoIP", VigorSwitch will guide these packets into the specified Voice LAN with specified priority tag to speed up the packet transmission. Such voice VLAN is only active inside VigorSwitch for packet transmission. After these packets leave VigorSwitch, the Voice VLAN tag will be removed immediately.

### II-5-3-1 Properties

This page allows a user to configure global and per interface setting of voice VLAN.



Available settings are explained as follows:


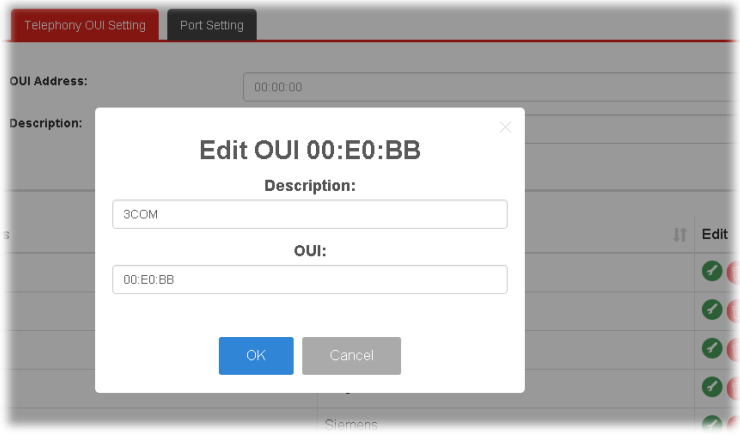

| Item              | Description   |
|-------------------|---|
| Voice VLAN State  | <ul style="list-style-type: none"><li>● Enabled - Click it to enable Voice VLAN.</li><li>● Disabled - Click it to disable Voice VLAN.</li></ul>                       |
| Voice VLAN Id     | Check the box of Enable first and then select Voice VLAN ID profile.  |
| Remark CoS/802.1p | Click Enabled / Disabled to enable or disable 1p remarking. If enabled, qualified packets will be remarked by this value.   |
| Remark Value      | Specify the number of packets to be remarked.<br>Specify the CoS/802.1p number you wish ingress VoIP packets be tagged with, so that QoS can prioritize it correctly. |
| Aging Time        | Select value of aging time (30~65536 min).<br>Default is 1440 minutes. A voice VLAN entry will be age out after this time if without any packet pass through.         |
| Apply             | Apply the settings to the switch.   |

## II-5-3-2 Telephony OUI Setting

This page allows a user to add, edit or delete OUI MAC addresses. Default has 8 pre-defined OUI MAC.

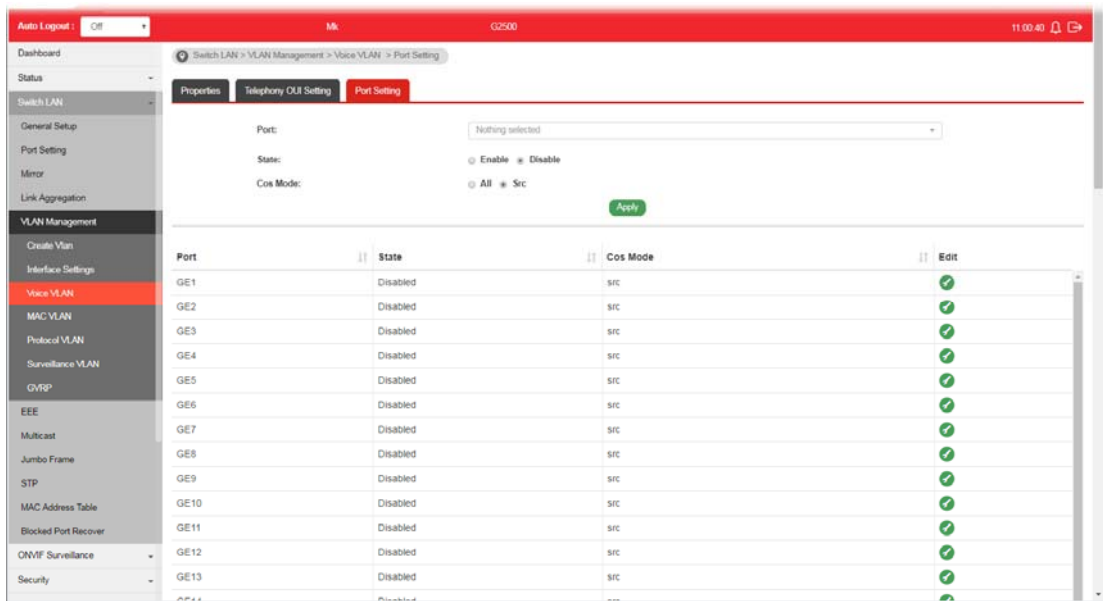
| OUI Address | Description | Edit |
|-------------|-------------|------|
| 00:E0:BB    | 3COM        | ✓ ✗  |
| 00:03:5B    | Cisco       | ✓ ✗  |
| 00:E0:75    | Vertel      | ✓ ✗  |
| 00:D0:1E    | Pingtel     | ✓ ✗  |
| 00:01:E3    | Siemens     | ✓ ✗  |
| 00:60:B9    | NEC/Philips | ✓ ✗  |
| 00:0F:E2    | H3C         | ✓ ✗  |
| 00:09:6E    | Avaya       | ✓ ✗  |

Available settings are explained as follows:

| Item        | Description  |
|-------------|--|
| OUI Address | Type OUI address.  |
| Description | Enter a description of the specified MAC address to the voice VLAN OUI table.  |
| Add         | Click it to create a new voice OUI based on the settings configured above.   |
| Edit        |  - Modify OUI setting for voice VLAN.<br><br> - Click it to remove the selected OUI entry. |

## II-5-3-3 Port Setting

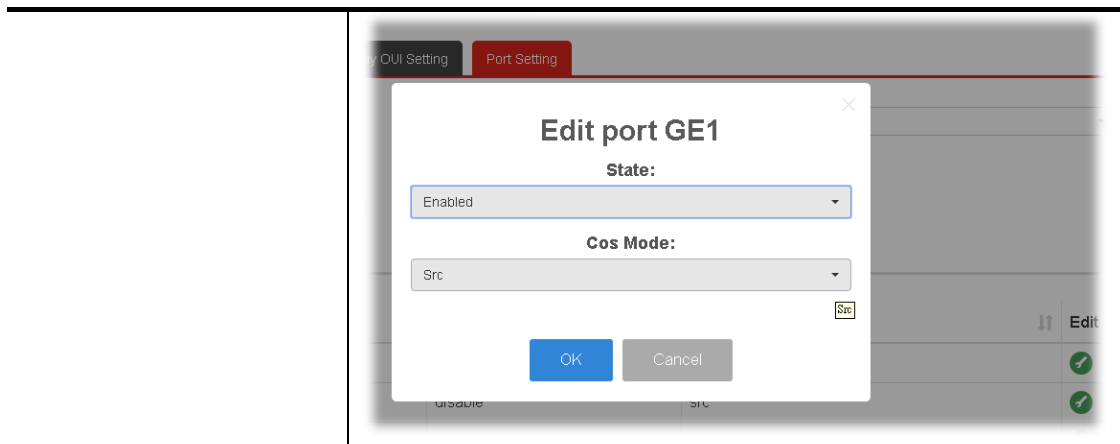
This page allows a user to specify LAN port(s) as Voice LAN port.



Available settings are explained as follows:

| Item     | Description   |
|----------|---|
| Port     | Use the drop down list to specify one or more LAN ports.  |
| State    | <ul style="list-style-type: none"> <li>● <b>Enabled</b> - Click it to enable the port settings for Voice LAN.</li> <li>● <b>Disabled</b> - Click it to disable the port settings for Voice LAN.</li> </ul>  |
| Cos Mode | <p>If Remark CoS/802.1p is enabled in Voice VLAN&gt;&gt;Properties, settings in this page shall be applied. Otherwise, this option will not take effect.</p> <ul style="list-style-type: none"> <li>● <b>All</b> - Once this port is identified as Voice VLAN by frame with matched OUI, remark CoS/802.1p shall tag for all ingress frame regardless of remarked frame matched with pre-configured OUI or not.</li> <li>● <b>Src (Source)</b> - Once this port is identified as Voice VLAN by frame with matched OUI, remark CoS/802.1p shall tag for only the matched ingress frame with pre-configured OUI.</li> </ul> |
| Apply    | Apply the settings to the switch.   |
| Edit     | Click the icon under <b>Edit</b> for one entry to modify port settings (State, Cos Mode) for voice VLAN.  |

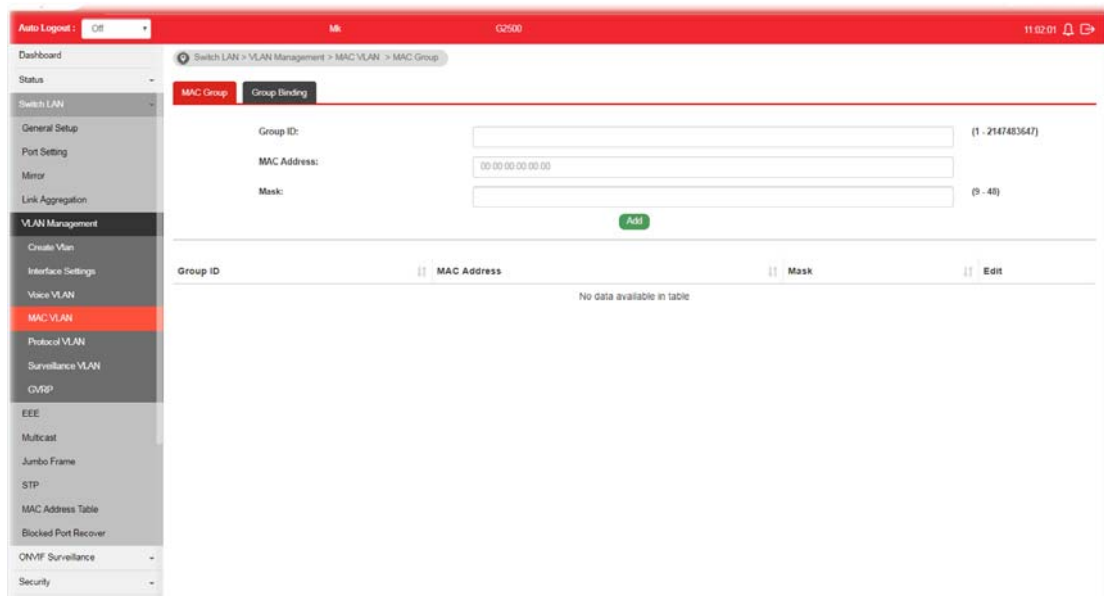




## II-5-4 MAC VLAN

### II-5-4-1 MAC Group

The MAC VLAN allows you to statically assign a VLAN ID to a host with specific MAC address(es). VigorSwitch allows you configure multiple groups with configured MAC address and mask to be active on ports and to be bound with VLAN ID. This page allows the network administrator to define groups with specific MAC addresses for later binding with VLAN and Port.



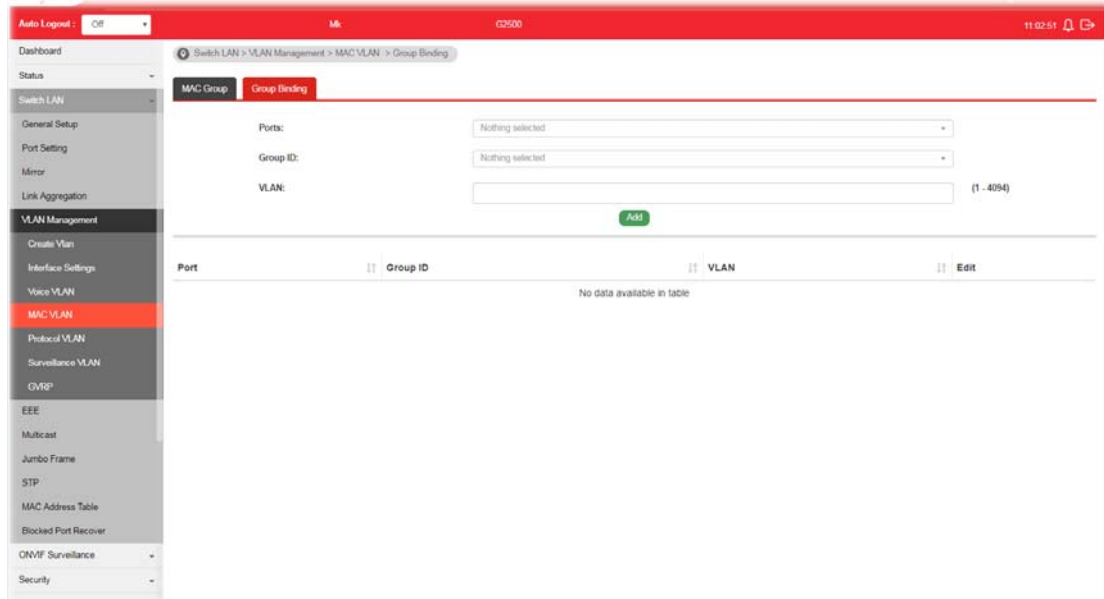
Available settings are explained as follows:

| Item        | Description  |
|-------------|--|
| Group ID    | It is a number for identification later, while chosen to be bound with VLAN/Port.  |
| MAC Address | Enter the MAC address you wish to be classified in this group  |
| Mask        | The mask is the length of matching prefix you wish to have on MAC address.<br>For example, configure mask in 10. It means a host with beginning of the 10-digit of MAC address will be checked, and classified into this group if matched. |
| Add         | Click it to create a new MAC group profile based on the  |

|             |   |
|-------------|---|
|             | settings configured above.  |
| <b>Edit</b> | Click the icon under <b>Edit</b> for one entry to modify settings for group ID. |

## II-5-4-2 Group Binding

The MAC VLAN allows you to statically assign a VLAN ID to a host with specific MAC address(es). VigorSwitch allows you to configure multiple groups with configured MAC address and mask to be active on ports and to be bound with VLAN ID. This page allows the network administrator to bind the group of specified MAC addresses with VLAN and Port.



Available settings are explained as follows:

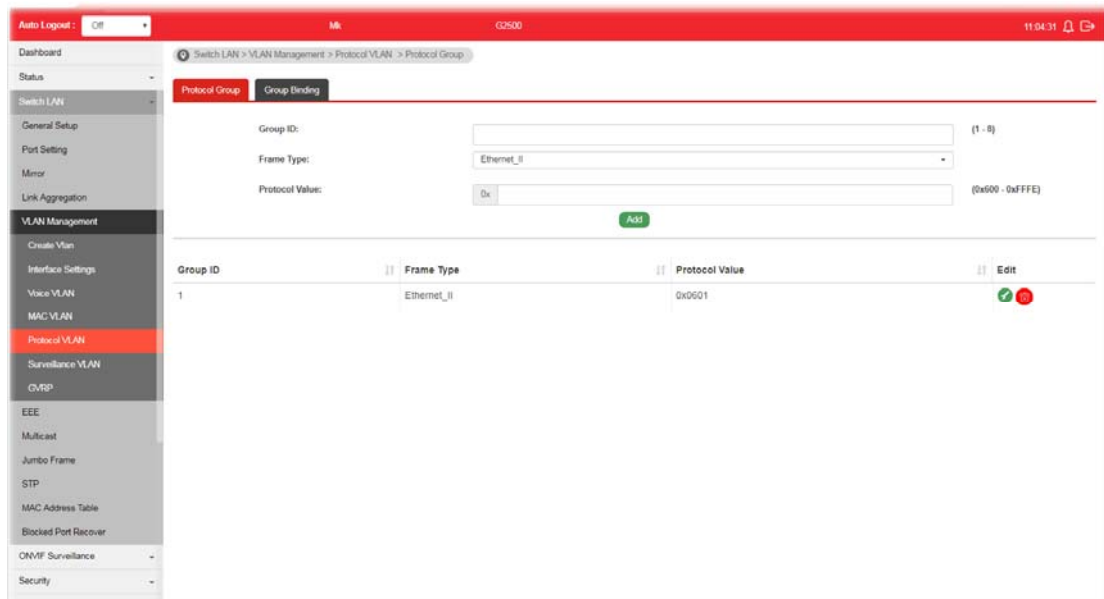
| Item            | Description   |
|-----------------|---|
| <b>Ports</b>    | Select the ports you wish to be bound with specified MAC address group.   |
| <b>Group ID</b> | Choose the group ID you have created in earlier section, which specified a group of host by MAC address and its mask. |
| <b>VLAN</b>     | Enter the VLAN ID that you wish to be bound with.   |
| <b>Add</b>      | Click it to create a new MAC group binding profile based on the settings configured above.                            |
| <b>Edit</b>     | Click the icon under <b>Edit</b> for one entry to modify settings for selected port profile.                          |

## II-5-5 Protocol VLAN

VigorSwitch offers protocol VLANs which allows Network Administrator to filter out untagged traffic of certain protocol and then assign them a specific VLAN ID.

### II-5-5-1 Protocol Group

Up to eight protocol groups can be defined, each of them can have a unique filtering criteria such as frame type and protocol value.



Available settings are explained as follows:

| Item           | Description  |
|----------------|--|
| Group ID       | It is a number for identification while bounding with VLAN/Port.   |
| Frame Type     | Use the drop-down list to specify the frame type which you would like to filter. <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <input type="text" value="Ethernet_II"/> <ul style="list-style-type: none"> <li style="border: 1px solid #ccc; padding: 2px;">Ethernet_II</li> <li>IEEE802.3_LL_C_Other</li> <li>RFC_1042</li> </ul> </div> <ul style="list-style-type: none"> <li>● Ethernet_II - Packet will be mapped based on Ethernet version 2.</li> <li>● IEEE802.3_LL_C_Other -Packet will be mapped based on 802.3 packet with LLC other header.</li> <li>● RFC_1042 - Packet will be mapped based on RFC 1042.</li> </ul> |
| Protocol Value | Input a value (ranging from 0x600 ~0xFFFF). Packets match with such value will be classified into this group.  |
| Add            | Click it to create a new protocol group profile based on the settings configured above.  |

**Edit**

- Modify setting for selected group.

### Edit Group 1

Frame Type

IEEE802.3\_LL\_C\_Other

Protocol Value

(0x600 - 0xFFFE) 0x 0601

OK

Cancel

- Click it to remove the group.

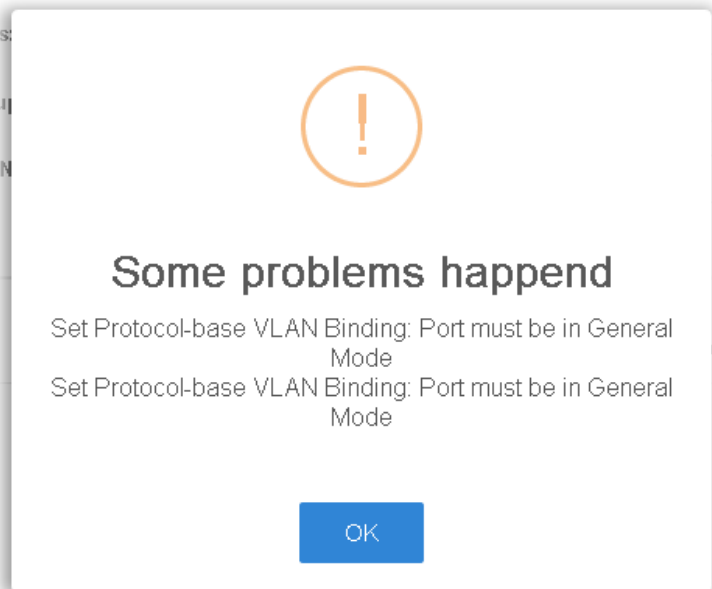
### II-5-5-2 Group Binding

This page is for setting up the ports and protocol group that we would like to filter, and the VLAN ID we would like to assign.

Available settings are explained as follows:

| Item     | Description   |
|----------|---|
| Ports    | Use the drop-down list to select one or more ports for applying protocol-based VLAN. Note that protocol-based VLAN can only be applied to the ports of which Interface VLAN Mode (at VLAN Management >> Interface Settings) is set to "Hybrid". |
| Group ID | Select the protocol group defined in Protocol Group setup.  |
| VLAN     | Use drop down list to choose a value as VLAN number.  |
| Add      | Add the above settings to the switch.   |

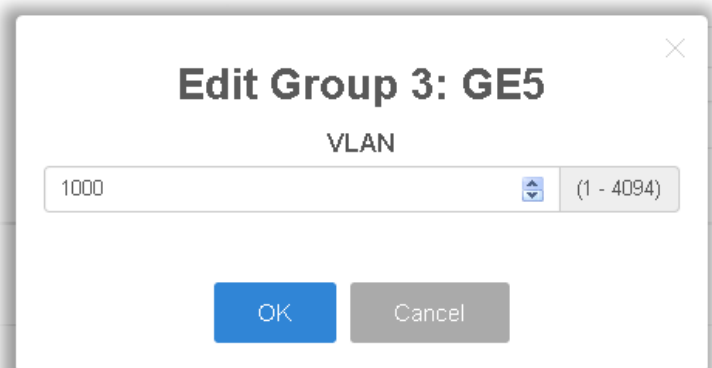
Before using Add, open **Switch LAN>>VLAN Management>>Interface Settings** to specify **Hybrid as Interface VLAN Mode** for the GE ports first. Otherwise, the following error message will appear.



**Edit**



- Modify setting for the selected group.



- Click it to remove the selected group.


## II-5-6 Surveillance VLAN

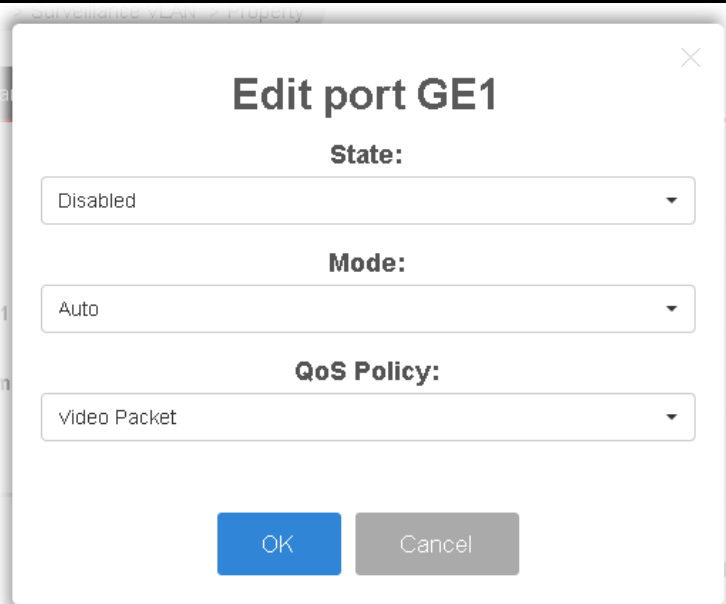
Surveillance VLAN can be configured for VigorSwitch to identify the packets coming from an IP camera automatically and assign those traffics to a specific VLAN ID and CoS/802.1p value, this helps you to prioritize those traffics and improve video quality.

### II-5-6-1 Property

This page is for setting up the VLAN to which the video traffic should be assigned and to enable/disable Surveillance VLAN on each port.

Available settings are explained as follows:

| Item                 | Description   |
|----------------------|---|
| State                | <ul style="list-style-type: none"> <li>● <b>Enabled</b> - Click it to enable the port settings for such VLAN.</li> <li>● <b>Disabled</b> - Click it to disable the port settings for such VLAN.</li> </ul>  |
| VLAN ID              | Choose a VLAN profile (created in <b>Switch LAN&gt;&gt;VLAN Management&gt;&gt;Create Vlan</b> ) as Surveillance VLAN.   |
| CoS/802.1p Remarking | Specify the CoS/802.1p number you wish ingress packets be tagged with, so that QoS can prioritize it correctly. <ul style="list-style-type: none"> <li>● <b>Enable</b> - If enabled, qualified packets will be remarked by this value.</li> </ul> |
| Aging Time           | Unit is second.<br>Select value of aging time (30~65536 seconds).<br>Default is 1440 seconds. VLAN entry will be aged out after this time if no packet passes through.  |
| Apply                | Apply the settings to the switch.   |
| Edit                 |  - Click it to modify port setting status.   |



**Edit port GE1**

**State:**  
 Disabled

**Mode:**  
 Auto

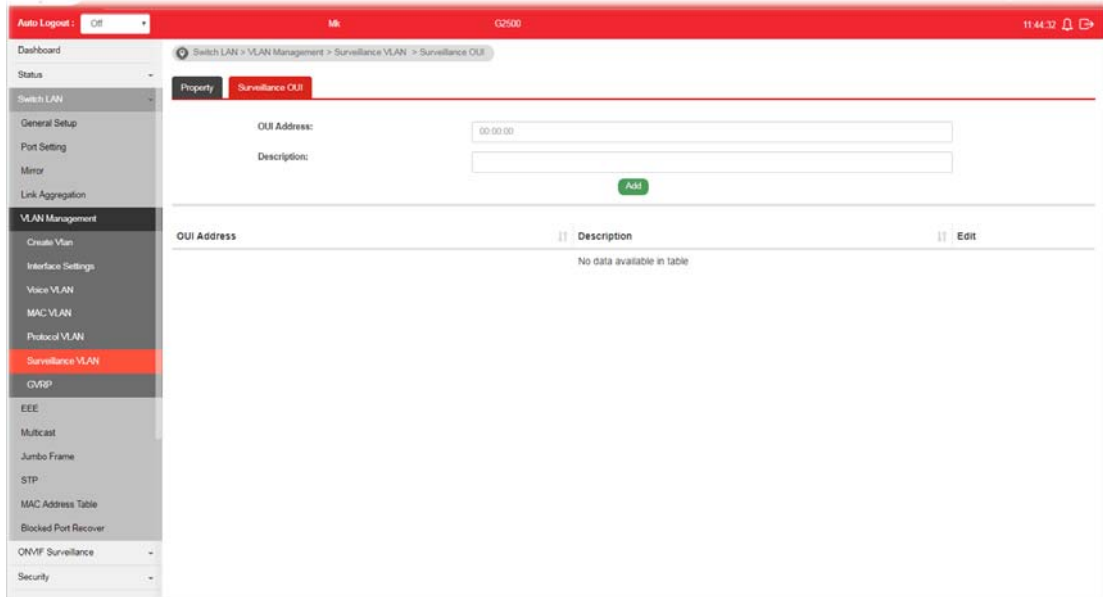
**QoS Policy:**  
 Video Packet

OK Cancel



- **State** -Set it to enable surveillance VLAN function of interface.
- **Mode** -Select port surveillance VLAN mode.
  - ◆ **Auto:** Surveillance VLAN auto detect packets that match OUI table and add received port into surveillance VLAN ID tagged member.
  - ◆ **Manual:** User need add interface to VLAN ID tagged member manually.
- **QoS Policy** - Select port QoS Policy mode.
  - ◆ **Video Packet:** QoS attributes are applied to packets with OUI in the source MAC address.
  - ◆ **All:** QoS attributes are applied to packets that are classified to the Surveillance VLAN.
- **OK** - Apply the settings to the switch.
- **Cancel** - Abandon the changes and return to previous page.

## II-5-6-1 Surveillance OUI

Filtering Surveillance traffic is based on the OUI of the IP cameras. Users can add, edit, and delete OUI on this page.



Available settings are explained as follows:

| Item        | Description   |
|-------------|---|
| OUI Address | Enter OUI MAC address of monitored IP camera. It can't be edited in edit dialog.  |
| Description | Enter a description of the specified MAC address to the surveillance VLAN OUI table.  |
| Add         | Click it to create a new voice OUI based on the settings configured above.  |
| Edit        |  - Modify OUI setting for surveillance VLAN.<br> - Click it to remove the selected OUI entry. |

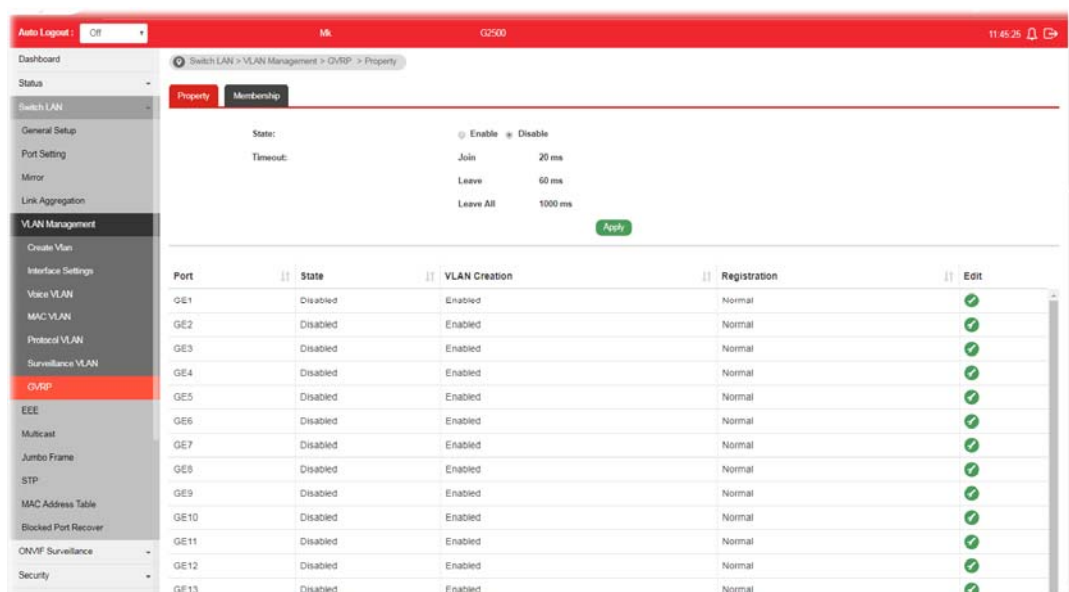


## II-5-7 GVRP


### II-5-7-1 Property

This page allows the network administrator to configure registration mode (e.g., Normal, Fixed or Forbidden) of GVRP (GARP VLAN Registration Protocol) for each GE port.

Such function can eliminate unnecessary network traffic and prevent any attempt to transmit information to unregistered users.



Available settings are explained as follows:

| Item    | Description   |
|---------|---|
| State   | <ul style="list-style-type: none"><li>● <b>Enabled</b> - Click it to enable the port settings for such VLAN.</li><li>● <b>Disabled</b> - Click it to disable the port settings for such VLAN.</li></ul> |
| Timeout | Display the current time status for GVRP.   |
| Apply   | Apply the settings to the switch.   |
| Edit    |  - Click it to modify settings for the selected port.  |

**Edit port GE1**

**State:**  
 Disabled

**VLAN Creation:**  
 Enabled

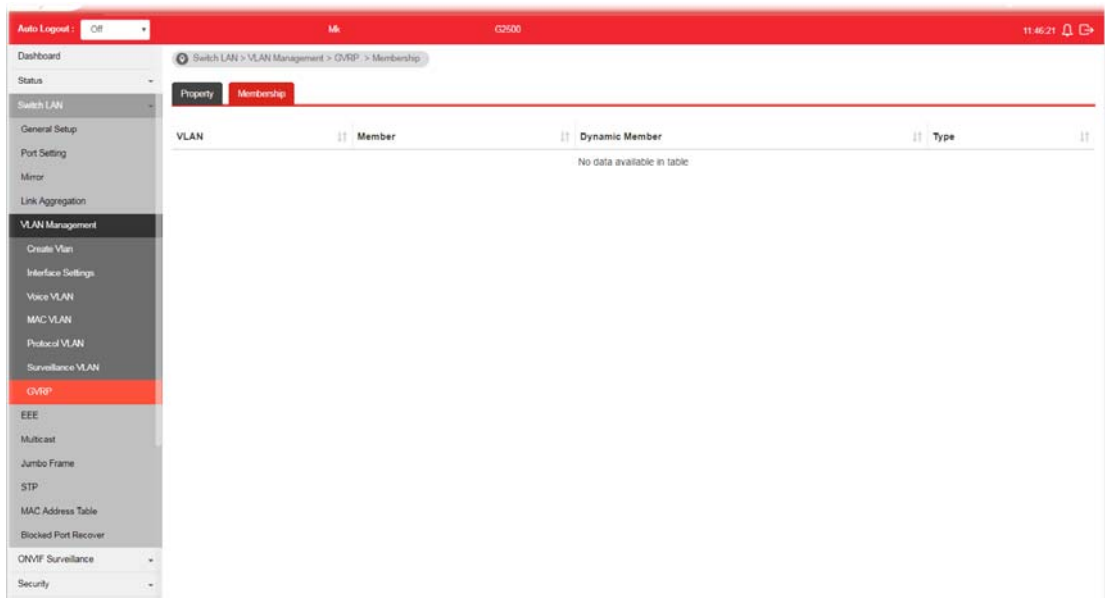
**Mode:**  
 Normal

OK Cancel

- **State** - Select Enabled or Disabled for such port.
- **VLAN Creation** -Select Enabled or Disabled.
- **Mode** - There are three modes to be specified.
  - ◆ Normal - Default setting. All packets can pass through the selected GE port.
  - ◆ Fixed - The selected GE port only sends static VLAN information to neighboring device and allows static VLAN packet to pass through.
  - ◆ Forbidden - The selected GE port only allows default VLAN packet to pass through.

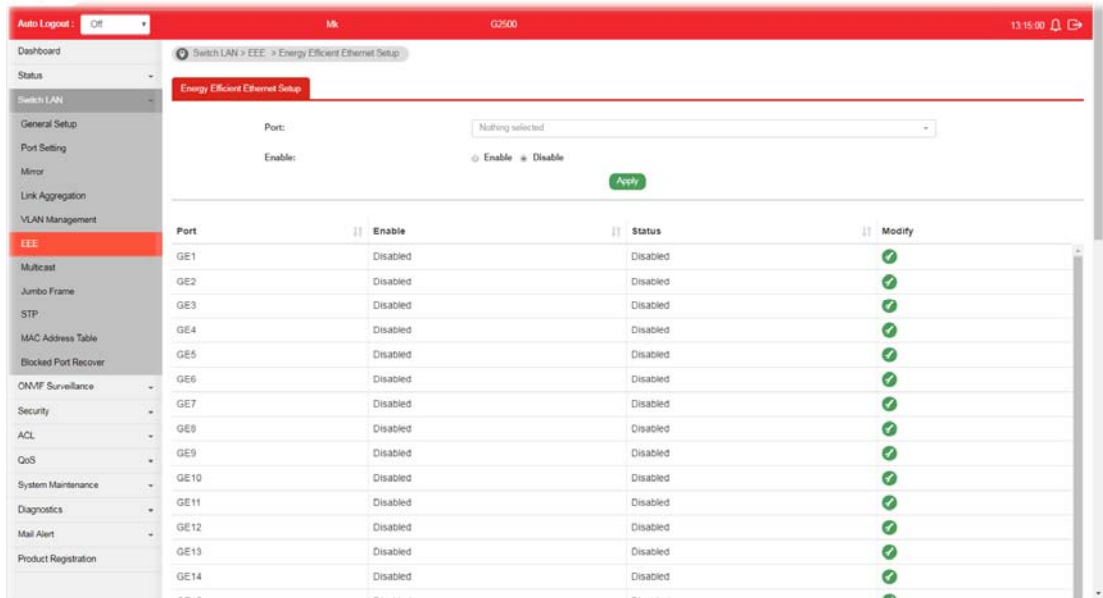
## II-5-7-2 Membership

This page display information about membership for GVRP.




## II-6 EEE

This page allows a user to enable or disable port EEE (Energy Efficient Ethernet) function.



Available settings are explained as follows:

| Item   | Description  |
|--------|--|
| Port   | Select one or multiple ports to configure (GE1 to GE28).   |
| Enable | <ul style="list-style-type: none"> <li>● <b>Enable</b> - Click it to enable the EEE function.</li> <li>● <b>Disable</b> - Click it to disable the EEE function.</li> </ul> |
| Apply  | Apply the settings to the switch.  |
| Modify |  - Click it to modify port setting status.  |

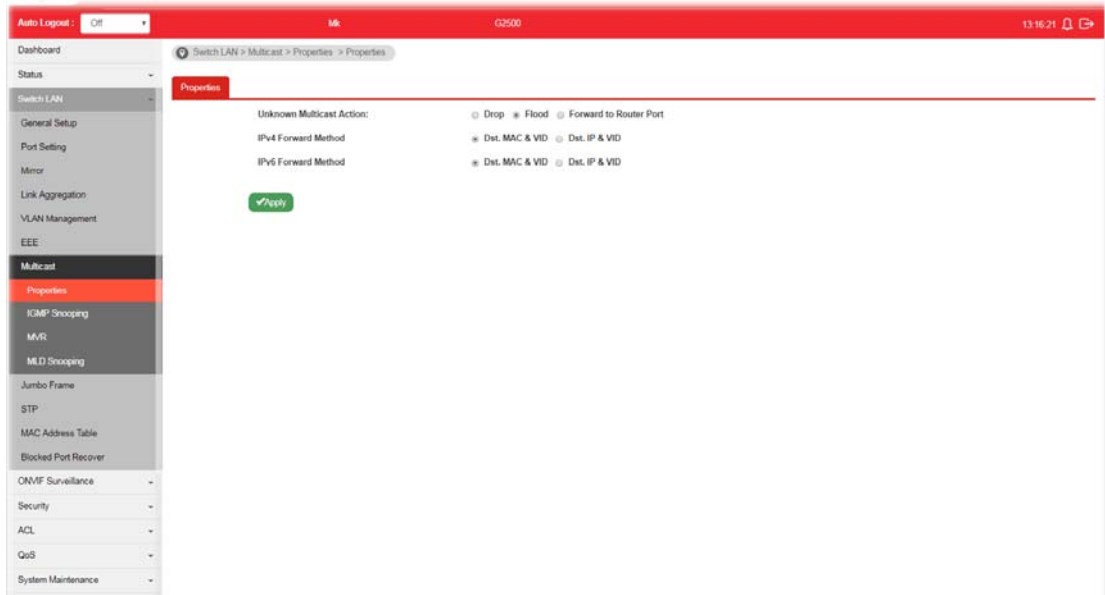
## II-7 Multicast

IP multicast is a technique for one-to-many communication over an IP infrastructure in a network.

To avoid the incoming data broadcasting to all GE ports, multicast is useful to transfer the data/message to specified GE ports for IGMP snooping. When VigorSwitch receives a message “subscribed” by the client, it must decide to transfer the data to specified GE ports according to the location of the client (subscribed member).

### II-7-1 Properties

For the multicast packets, This page allows the network administrator to choose actions for processing the unknown multicast packets and for handling known packets with MAC address, IP address and VLAN ID.



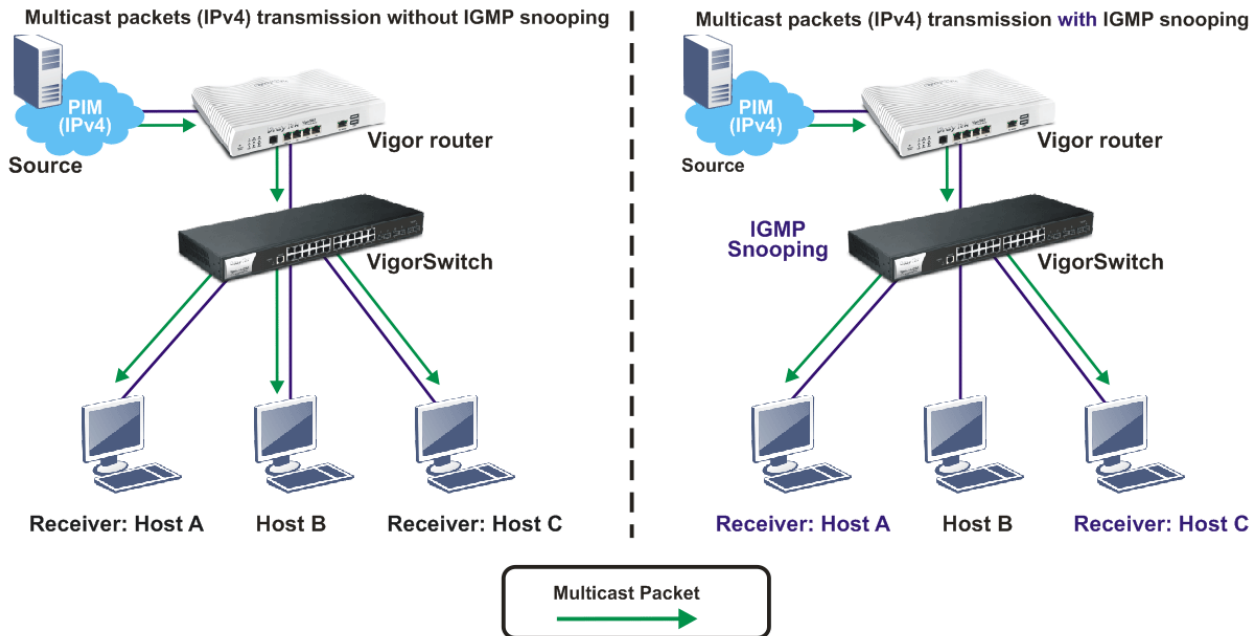
Available settings are explained as follows:

| Item                     | Description  |
|--------------------------|--|
| Unknown Multicast Action | Select an action for switch to handle with unknown multicast packet. <ul style="list-style-type: none"><li>● <b>Drop</b>: Drop the unknown multicast data.</li><li>● <b>Flood</b>: Flood the unknown multicast data.</li><li>● <b>Forward to Router port</b>: Forward the unknown multicast data to router port.</li></ul> |
| IPv4 Forward Method      | Set the IPv4 multicast forward method. <ul style="list-style-type: none"><li>● <b>Dst. MAC &amp; VID</b>: Forward using destination multicast MAC address and VLAN IDs.</li><li>● <b>Dst. IP &amp; VID</b>: Forward using destination multicast IP address and VLAN ID.</li></ul>  |
| IPv6 Forward Method      | Set the IPv6 multicast forward method. <ul style="list-style-type: none"><li>● <b>Dst. MAC &amp; VID</b>: Forward using destination multicast MAC address and VLAN IDs.</li></ul>  |

|              |  |
|--------------|--|
|              | <ul style="list-style-type: none"><li>● Dst. IP &amp; VID: Forward using destination multicast IPv6 address and VLAN ID.</li></ul> |
| <b>Apply</b> | Apply the settings to the switch.  |

## II-7-2 IGMP Snooping

IGMP snooping is the process of listening to Internet Group Management Protocol (IGMP) network traffic. The feature allows a network switch to listen in on the IGMP conversation between hosts and routers. By listening to these conversations the switch maintains a map of which links need which IP multicast streams. Multicasts may be filtered from the links which do not need them and thus controls which ports receive specific multicast traffic.




### II-7-2-1 IGMP Setting

This page allows the network administrator to enable/disable IGMP function, select snooping version, and enable/disable snooping report suppression.

| Entry No. | VLAN ID | IGMP Snooping | Router Ports | Query Robustness | Query Interval | Query Max Response | Last Member Query | Last Member Interval | Immediate Leave |
|-----------|---------|---------------|--------------|------------------|----------------|--------------------|-------------------|----------------------|-----------------|
| 1         | 1       | Disabled      | Enabled      | 2                | 125            | 10                 | 2                 | 1                    | Disabled        |

Available settings are explained as follows:

| Item | Description |
|------|-------------|
|------|-------------|

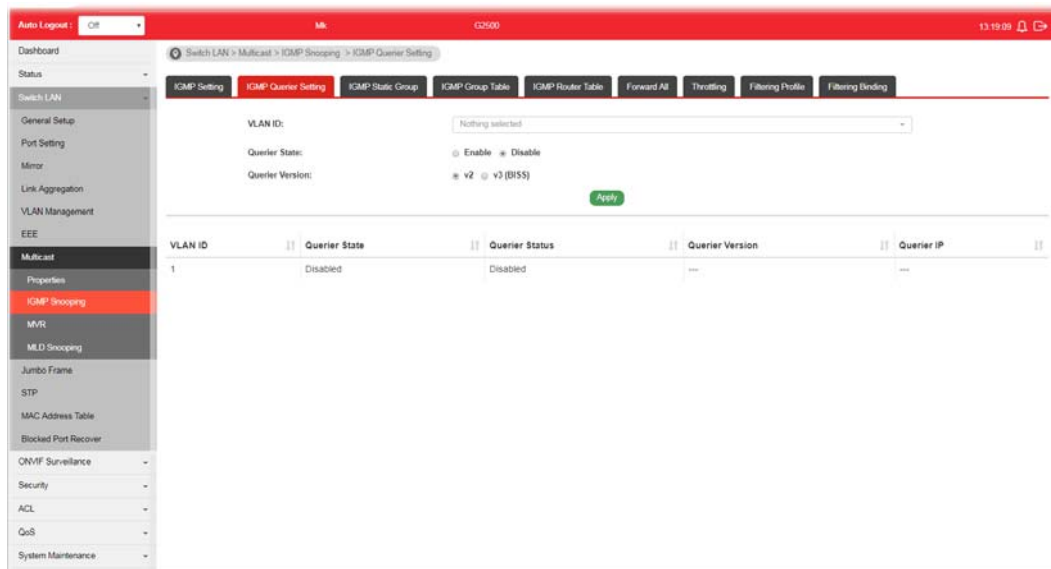
|                                  |  |
|----------------------------------|--|
| IGMP Snooping State              | <ul style="list-style-type: none"> <li>● <b>Enable</b> - Click it to set enabling IGMP function.</li> <li>● <b>Disable</b> - Click it to disable IGMP function.</li> </ul>   |
| IGMP Snooping Version            | Set the IGMP snooping version. <ul style="list-style-type: none"> <li>● <b>v2</b> - Only support process IGMP v2 packet.</li> <li>● <b>v3 (BISS)</b> - Support v3 basic and v2.</li> </ul>   |
| IGMP Snooping Report Suppression | Click <b>Enable</b> to allow the switch to handle IGMP reports between router and host, suppressing bandwidth used by IGMP.  |
| Apply                            | Apply the settings to the switch.  |
| Modify                           | <div data-bbox="683 577 730 633" style="display: inline-block; vertical-align: middle;">  </div> - Click it to modify IGMP settings for selected profile. However, if <b>IGMP Snooping State</b> is not set as <b>Enable</b> , such option will be disabled.<br><br><div data-bbox="695 719 1417 1832" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <div style="text-align: right; font-size: 20px; color: #ccc;">×</div> <h3 style="text-align: center; margin: 0;">Edit VLAN ID 1</h3> <p style="text-align: center; margin: 5px 0;"><b>IGMP Snooping State</b></p> <div style="margin-bottom: 10px;"> <input type="text" value="Disable"/> </div> <p style="text-align: center; margin: 5px 0;"><b>Router Ports Auto Learn</b></p> <div style="margin-bottom: 10px;"> <input type="text" value="Enable"/> </div> <p style="text-align: center; margin: 5px 0;"><b>Query Robustness (Operational: 2)</b></p> <div style="margin-bottom: 10px;"> <input type="text" value="2"/> <span style="float: right;">(1-7, default 2)</span> </div> <p style="text-align: center; margin: 5px 0;"><b>Query Interval (Operational: 125)</b></p> <div style="margin-bottom: 10px;"> <input type="text" value="125"/> <span style="float: right;">Sec (30-18000, default 125)</span> </div> <p style="text-align: center; margin: 5px 0;"><b>Query Response Interval (Operational: 10)</b></p> <div style="margin-bottom: 10px;"> <input type="text" value="10"/> <span style="float: right;">Sec (5-20, default 10)</span> </div> <p style="text-align: center; margin: 5px 0;"><b>Last Member Query Counter (Operational: 2)</b></p> <div style="margin-bottom: 10px;"> <input type="text" value="2"/> <span style="float: right;">Sec (1-7, default 2)</span> </div> <p style="text-align: center; margin: 5px 0;"><b>Last Member Query Interval (Operational: 1)</b></p> <div style="margin-bottom: 10px;"> <input type="text" value="1"/> <span style="float: right;">Sec (1-25, default 1)</span> </div> <p style="text-align: center; margin: 5px 0;"><b>Immediate Leave:</b></p> <div style="margin-bottom: 10px;"> <input type="text" value="Enable"/> </div> <div style="text-align: center; margin-top: 10px;"> <input type="button" value="OK"/> <input type="button" value="Cancel"/> </div> </div><br><ul style="list-style-type: none"> <li>● <b>IGMP Snooping State</b> -Choose <b>Enable</b> to enable IGMP snooping function.</li> <li>● <b>Router Ports Auto Learn</b> - Set the enabling status of IGMP router port learning. Choose <b>Enable</b> to learn router port by IGMP query.</li> <li>● <b>Query Robustness</b> - Set a number which allows tuning for</li> </ul> |

the expected packet loss on a subnet.

- **Query Interval** - Set the interval of querier send general query.
- **Query Response Interval** - It specifies the maximum allowed time before sending a responding report in units of 1/10 second.
- **Last Member Query Counter** - After querying for specified times (defined here) and still not receiving any response from the subscribed member, VigorSwitch will stop transmitting data to the related GE port(s).
- **Last Member Query Interval** - The maximum time interval between counting each member query message with no responses from any subscribed member.
- **Immediate Leave** - Leave the multicast group immediately on the port & VLAN where leave message is sent from, regardless there is still a subscribed member or not. Click Enable to enable Fastleave function.
- **OK** - Apply the settings to the switch.
- **Cancel** - Close the page and return to previous page.

## II-7-2-2 IGMP Querier Setting

This page allows a user to configure querier settings on specific VLAN of IGMP Snooping.



Available settings are explained as follows:

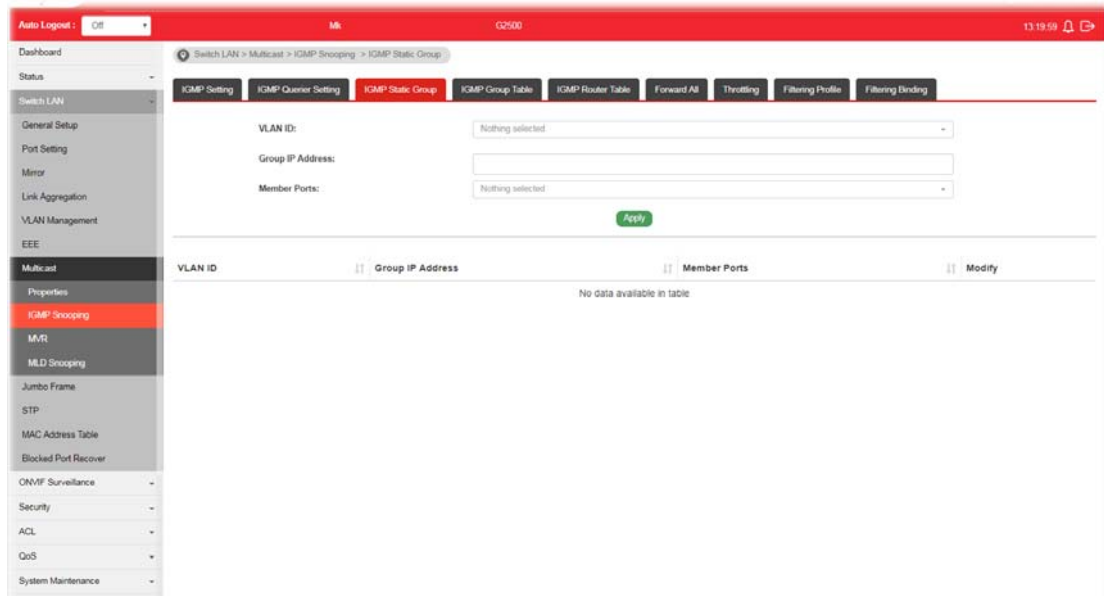
| Item            | Description   |
|-----------------|---|
| VLAN ID         | Use the drop down list to specify a VLAN profile as IGMP Snooping querier.  |
| Querier State   | <ul style="list-style-type: none"> <li>● <b>Enable</b> - Click <b>Enable</b> to set the enabling status of IGMP Querier on the chosen VLAN profile.</li> <li>● <b>Disable</b> - Click it to disable the function.</li> </ul>  |
| Querier Version | <p>Set the query version of IGMP Querier Election on the chosen VLANs.</p> <ul style="list-style-type: none"> <li>● <b>v2</b> - Querier version 2.</li> <li>● <b>v3</b> - Querier version 3.</li> </ul> <p><b>Note:</b> For maximum compatibility, it is suggested to use</p> |




|       |   |
|-------|---|
|       | querier version lower than IGMP snooping version, for there is possible network mixed with IGMP v2/v3 client and v2 query message is widely understandable for those clients. |
| Apply | Apply the settings to the switch.   |

### II-7-2-3 IGMP Static Group

The IGMP static group is allowed to assign a VLAN/port as a specific IPv4 multicast member. Every IPv4 multicast stream that belongs to the specified group IP address will be forwarded to the specified port/VLAN member.

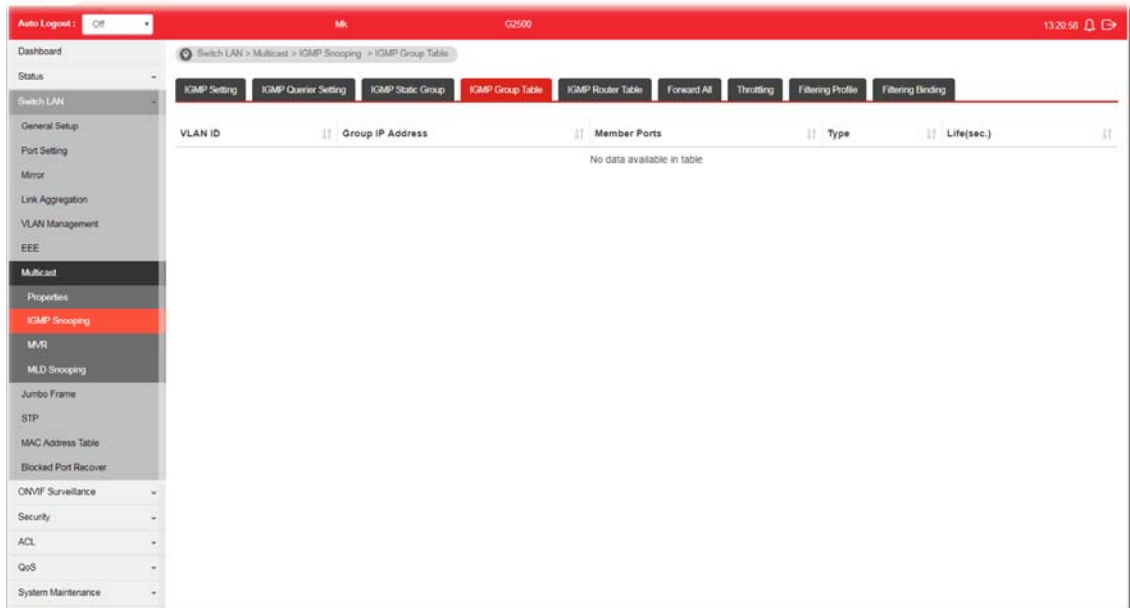


Available settings are explained as follows:

| Item             | Description   |
|------------------|---|
| VLAN ID          | Use the drop down list to specify a VLAN profile as IGMP Static Group.  |
| Group IP Address | It is an identifier for the group member. Packets sent to such address will be transferred to all interfaces defined in Member Ports.<br>Specify the IPv4 multicast address you wish to assign for the static group (defined in VLAN ID). |
| Member Ports     | Specify the port(s) that static group with given IPv4 multicast address shall include.  |
| Apply            | Apply the settings to the switch.   |
| Modify           |  - Click it to modify settings.  |

## II-7-2-4 IGMP Group Table

This page shows currently known and dynamically learned by IGMP snooping or shows the assigned IPv4 multicast address group in operation.

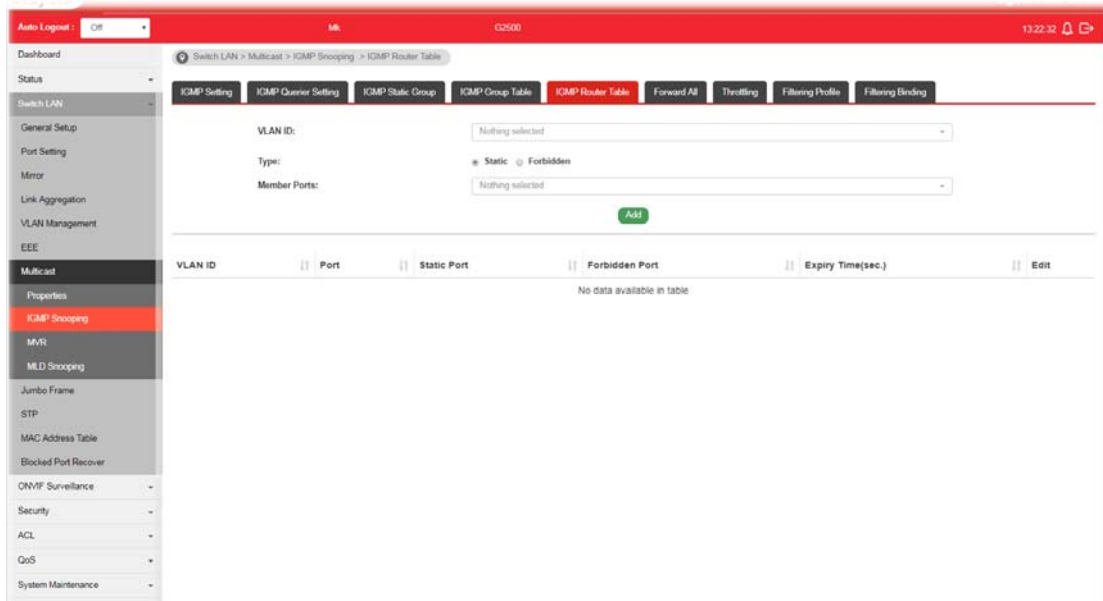


Available settings are explained as follows:

| Item             | Description   |
|------------------|---|
| VLAN ID          | Display the VLAN of this multicast group belongs to.                                    |
| Group IP Address | Display the multicast address of this multicast group.                                  |
| Member Ports     | Display the port(s) where subscribing member of this multicast group belongs to.        |
| Type             | Display if it is dynamically learned or statically assigned.                            |
| Life(sec.)       | Display the life time of this multicast member left if no membership report sent again. |

## II-7-2-5 IGMP Router Table

This page shows the IGMP querier router known to this switch.

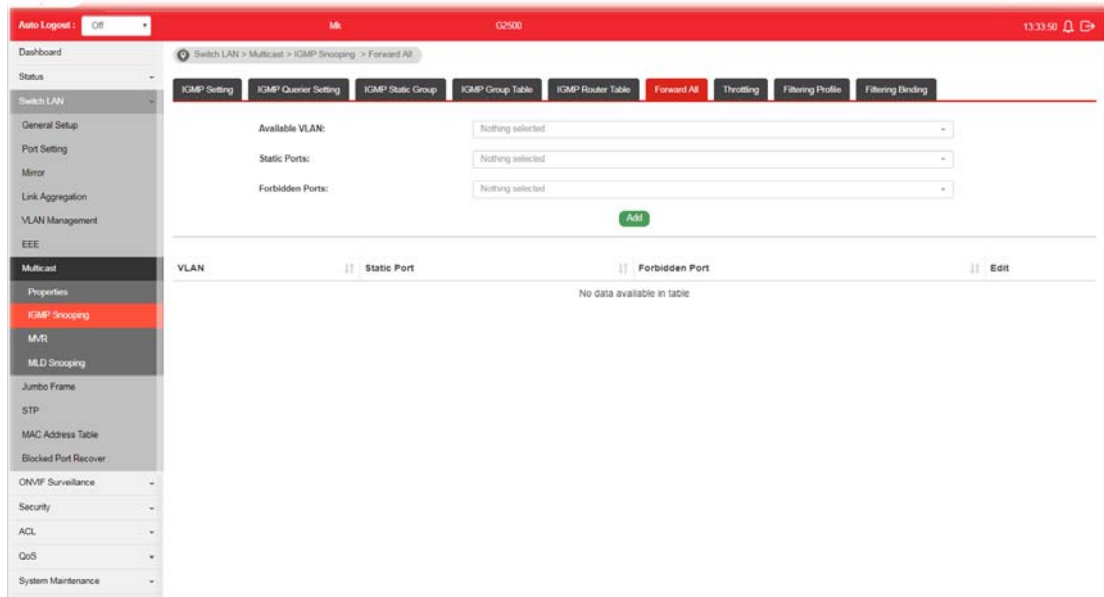


Available settings are explained as follows:



| Item               | Description  |
|--------------------|--|
| VLAN ID            | Use the drop down list to specify a VLAN profile (created in <b>Switch LAN&gt;&gt;VLAN Management&gt;&gt;Create Vlan</b> ) that the MLD querier belongs to.      |
| Type               | <b>Static</b> - Specify LAN Port (GE/LAG) to send out query to remote host.<br><b>Forbidden</b> - Use the drop down list to specify forbidden LAN Port (GE/LAG). |
| Member Ports       | Use the drop down list to choose the uplink ports where querier router exists.   |
| Add                | Click it to display the result based on the settings configured above.   |
| Port               | Display the static port member specified in Member Ports.  |
| Expire Time (sec.) | Display the time before querier is considered no longer existed.   |
| Edit               | Click the icon under Edit to modify the settings for the selected VLAN profile.  |

## II-7-2-6 Forward All

This page is allowed to determine which port(s) would like to receive the data (multicast packets) that forwarded by VigorSwitch.



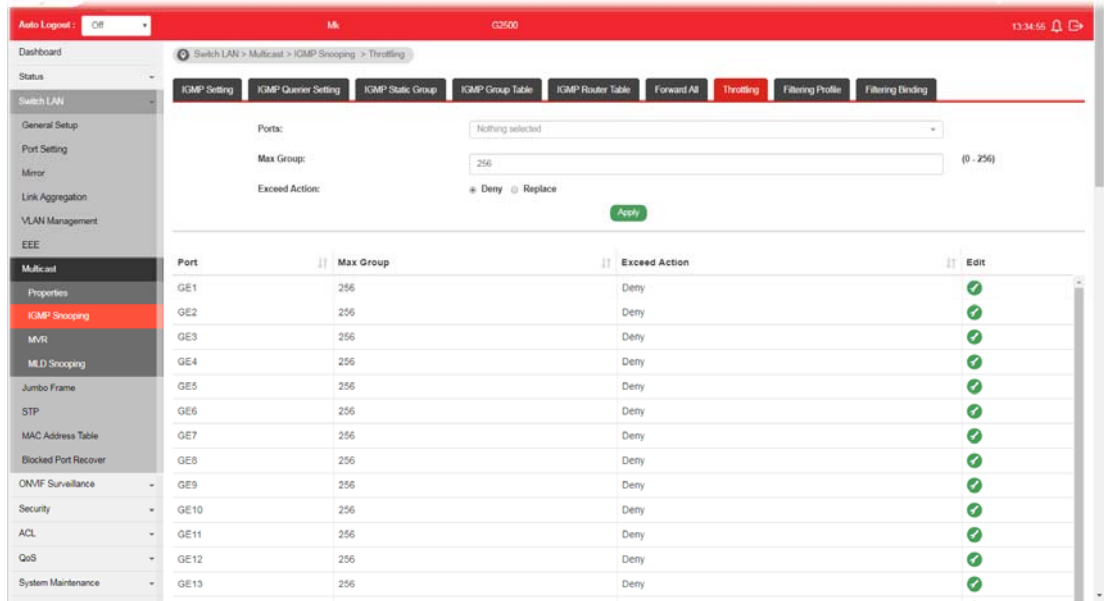
Available settings are explained as follows:

| Item            | Description   |
|-----------------|---|
| Available VLAN  | To display all of the available VLAN, the State must be set as <b>Enabled</b> in MLD Setting first.<br>Use the drop down list to specify a VLAN profile (created in <b>Switch LAN&gt;&gt;VLAN Management&gt;&gt;Create Vlan</b> ) that multicast packets will be forwarded to.          |
| Static Ports    | Use the drop down list to specify LAN Port (GE/LAG).<br>Later, the multicast packets will be delivered to the network device connected by these ports.  |
| Forbidden Ports | Use the drop down list to specify forbidden LAN Port (GE/LAG).<br>Later, the multicast packets will not be delivered to the network device connected by these ports.  |
| Add             | Click it to display the result based on the settings configured above.  |
| Edit            |  - Click it to modify port setting (static port and forbidden port).<br> - Click it to remove the selected entry. |


## II-7-2-7 Throttling

The administrator can configure the user on a switch port (GE/LAG port) belonging to which multicast group and restrict the number of multicast group that the user on the switch can join. Then the administrator is able to control the network service (e.g, IP/TV service) that the user can enjoy.

The Throttling page is used for configuring the maximum number (0~255) of IGMP group that a user on a switch port can join. After defined the maximum number, each switch port interface can be set to deny the IGMP join report or set to replace randomly selected multicast interface with received IGMP join report.



Available settings are explained as follows:

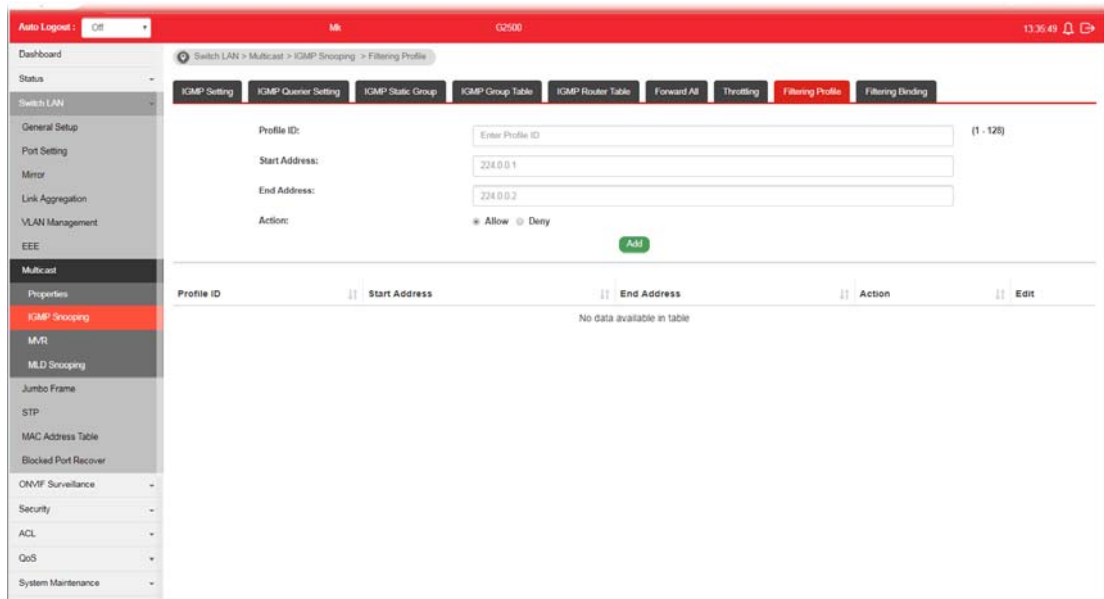
| Item          | Description   |
|---------------|---|
| Ports         | Use the drop down list to specify LAN Port (GE/LAG).  |
| Max Group     | Define the maximum number of IGMP group profile that a user on the switch can join. If "0" is selected, then such interface (port) can join all of the IGMP group profiles (defined in Filtering Profile).  |
| Exceed Action | VigorSwitch will perform the action defined below when the number of IGMP join report for the specified interface exceeds value defined in Max Group. <ul style="list-style-type: none"> <li>● Deny - It is default setting. The IGMP join report (for multicast service) received by such interface will be discarded.</li> <li>● Replace - When it is selected, a new group with IGMP report received will replace the existing group.</li> </ul> |
| Apply         | Apply the settings to the switch.   |
| Edit          |  - Click it to modify port setting (max group and exceed action).  |

## II-7-2-8 Filtering Profile


The administrator can configure the user on a switch port (GE/LAG port) belonging to which multicast group and restrict the number of multicast group that the user on the switch can join. Then the administrator is able to control the network service (e.g, IP/TV service) that the user can enjoy.

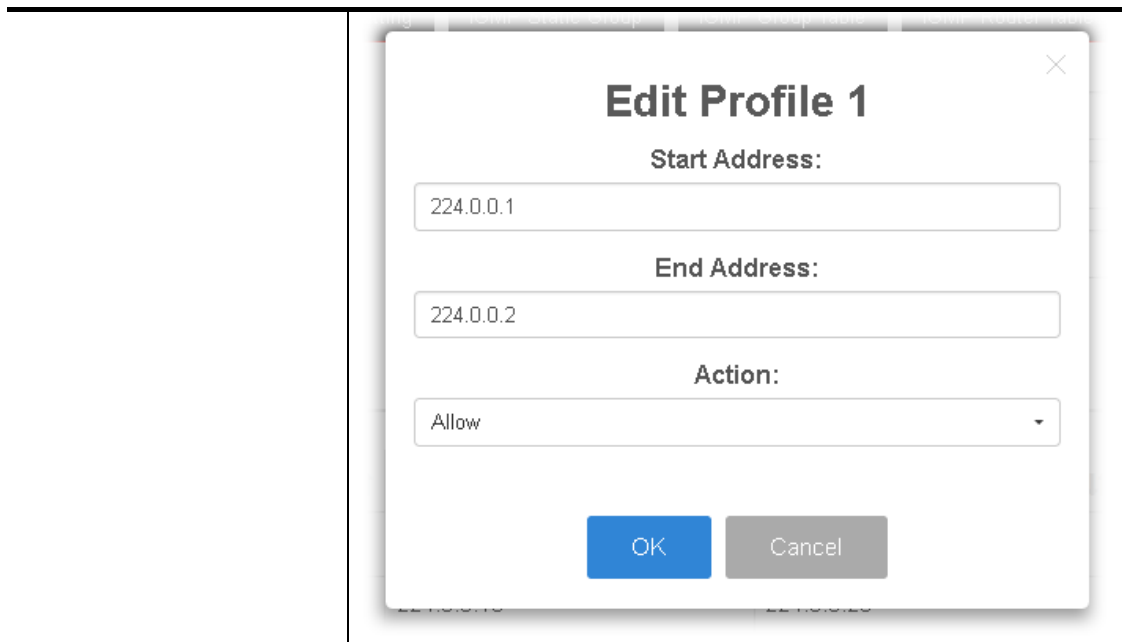
The filtering profile page allows to configure up to 128 IP-group (for multicast servie) profiles (starting and ending point within an IP range shall be specified). Each IP group profile can be set for permission of / denial of network service respectively.

In addition, such filtering profile is only effective for controlling the query for multicast. It has nothing to do with the general IGMP query.



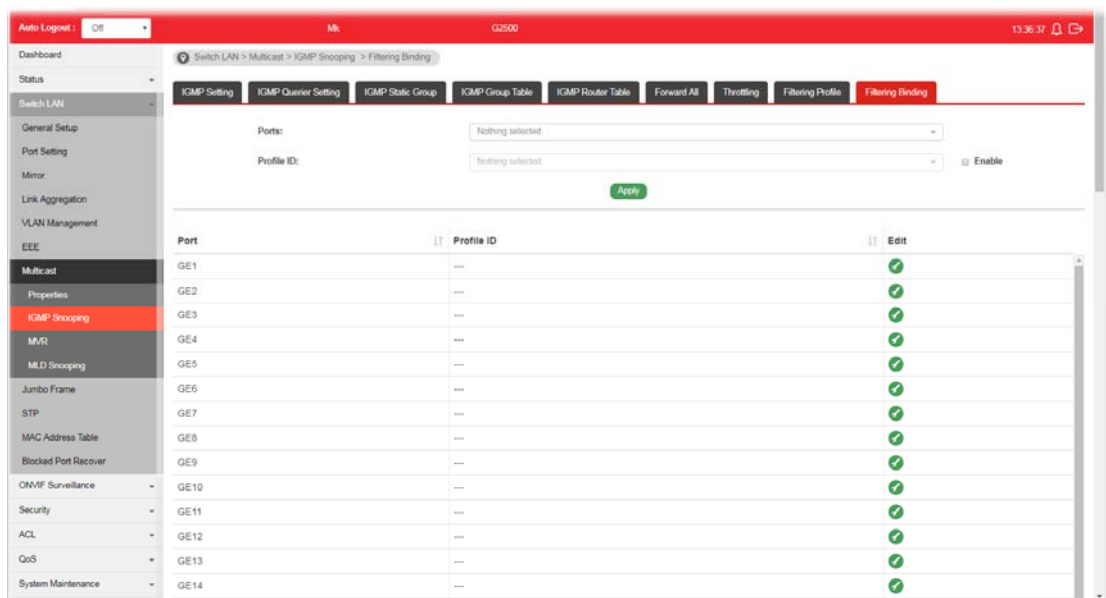
Available settings are explained as follows:

| Item          | Description   |
|---------------|---|
| Profile ID    | Use the drop down list to select one filtering profile (1~128) for IGMP snooping.   |
| Start Address | Enter an IP address as the starting point for the IP range.   |
| End Address   | Enter an IP address as the ending point for the IP range.   |
| Action        | <ul style="list-style-type: none"> <li>● <b>Deny</b> - It is default setting. The forwarding request of multicast traffic will be discarded.</li> <li>● <b>Allow</b> - When it is selected, the request for multicast traffic will be forwarded to the multicast group normally.</li> </ul> |
| Add           | Click it to display the result based on the settings configured above.  |
| Edit          |  - Click it to modify port setting (max group and exceed action).  |




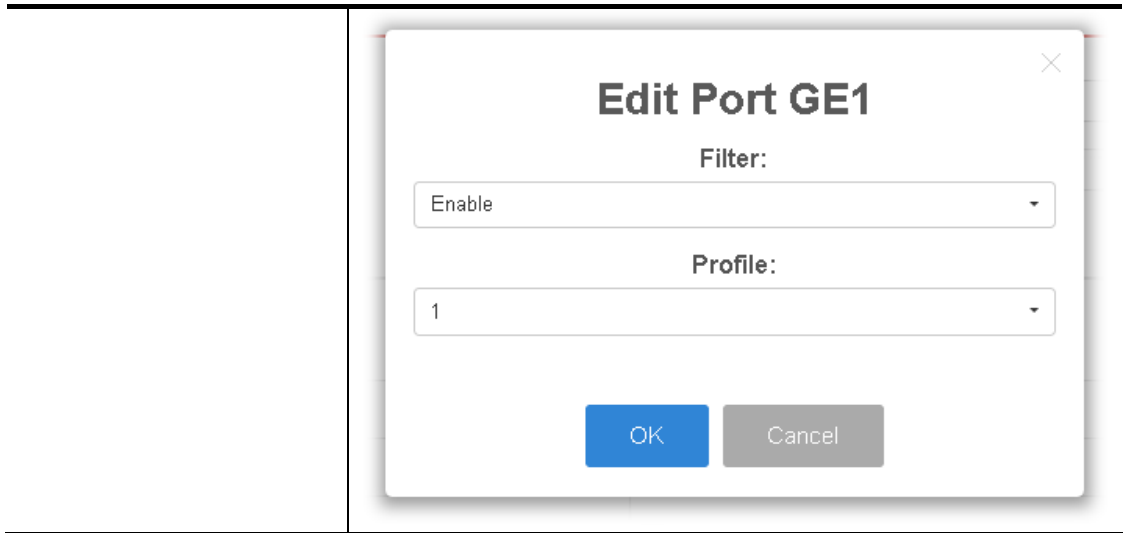
### II-7-2-9 Filtering Binding

This page allows the network administrator to select a filtering profile for LAN/GE port to process multicast traffic.



Available settings are explained as follows:

| Item       | Description  |
|------------|--|
| Ports      | Use the drop down list to specify LAN Port (GE/LAG).   |
| Profile ID | Use the drop down list to choose the filtering profile for the select port/interface. <ul style="list-style-type: none"> <li>● <b>Enable</b> - Check this box first to make profile ID selection be available for choosing.</li> </ul> |
| Apply      | Apply the settings to the switch.  |
| Edit       |  - Click it to modify port setting (enabling / disabling filter function and choosing a profile for such interface).                                |





## II-7-3 MVR

Multicast VLAN Registration (MVR) can route packets received in a multicast source VLAN to one or more destination VLANs. LAN users are in the destination VLANs and the multicast server is in the source VLAN.

MVR can continuously send multicast stream for traffic in the multicast VLAN, but isolate the streams from the source VLANs for bandwidth and security reasons.

In general, MVR is able to:

- Identify the MVR IP multicast streams and their associated IP multicast group.
- Intercept the IGMP messages

### II-7-3-1 Property

This page allows the network administrator to configure general settings for MVR, such as enabling function, selecting VLAN ID (as source VLAN) and specify IP address(es) for receiver/LAN users.

The screenshot displays the 'MVR Property' configuration page. The left sidebar shows a navigation menu with 'MVR' highlighted. The main content area is divided into 'Property Settings' and 'Operational Group'. Under 'Property Settings', there are fields for State (radio buttons for Enable and Disable), VLAN ID (a dropdown menu showing 'default(1)'), Mode (radio buttons for Compatible and Dynamic), Group Start (text input '0.0.0.0'), Group Count (text input '1' with '(1-128)' next to it), and Query Time (text input '1' with '(1-10 sec)' next to it). An 'Apply' button is located below these fields. The 'Operational Group' section shows a table with 'Maximum' set to 128 and 'Current' set to 0.

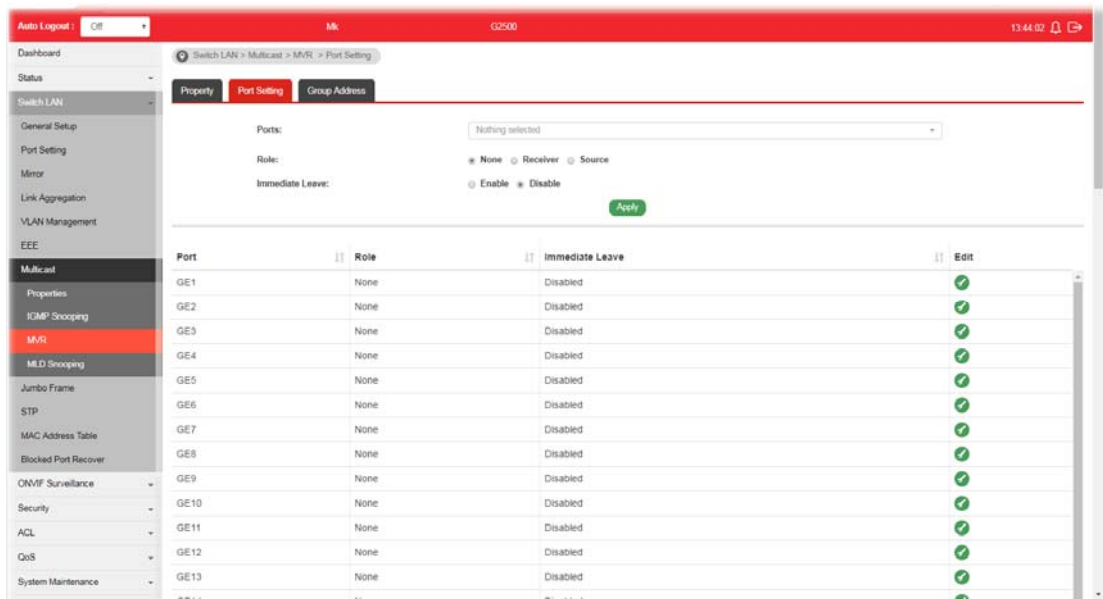
Available settings are explained as follows:

| Item    | Description   |
|---------|---|
| State   | <ul style="list-style-type: none"><li>● <b>Enabled</b> - Click it to enable the MVR function.</li><li>● <b>Disabled</b> - Click it to disable the MVR function.</li></ul>   |
| VLAN ID | <p>Choose one VLAN profile from the drop down list as multicast source VLAN which will receive multicast data. All source ports must belong to this VLAN. The default is VLAN 1.</p> <p>Note: Each VLAN ID shall be configured with group address and member port (defined in MVR&gt;&gt;Group Address page).</p>                                     |
| Mode    | <p>There are two modes offered for MVR operation.</p> <ul style="list-style-type: none"><li>● <b>Comaptible</b> - Multicast data received by MVR hosts (multicast server) will be forwarded to all MVR receiver ports.</li><li>● <b>Dynamic</b> - Multicast data received by MVR hosts (multicast server) on Vigor switch will be forwarded</li></ul> |

|                        |   |
|------------------------|---|
|                        | from those MVR data and client ports grouped under MVR server.  |
| <b>Group Start</b>     | Enter an IP address. Any multicast data sent to this IP address will be sent to all source ports on Vigor switch; and all receiver ports will accept /receive data from that multicast address. |
| <b>Group Count</b>     | Select a number to configure a contiguous series of MVR group addresses (the range for count is 1 to 128; the default is 1).  |
| <b>Query Time</b>      | Use the drop down list to define the maximum time (1 - 10 seconds) to wait for IGMP report members on a receiver port before the port is removed from multicast group.                          |
| <b>Apply</b>           | Apply the settings to the switch.   |
| <b>Operation Group</b> | Display group information for MVR operation.  |


### II-7-3-2 Port Setting

It is necessary to specify destination port and source port (GE/LAG) for Vigor system to perform MVR operation.



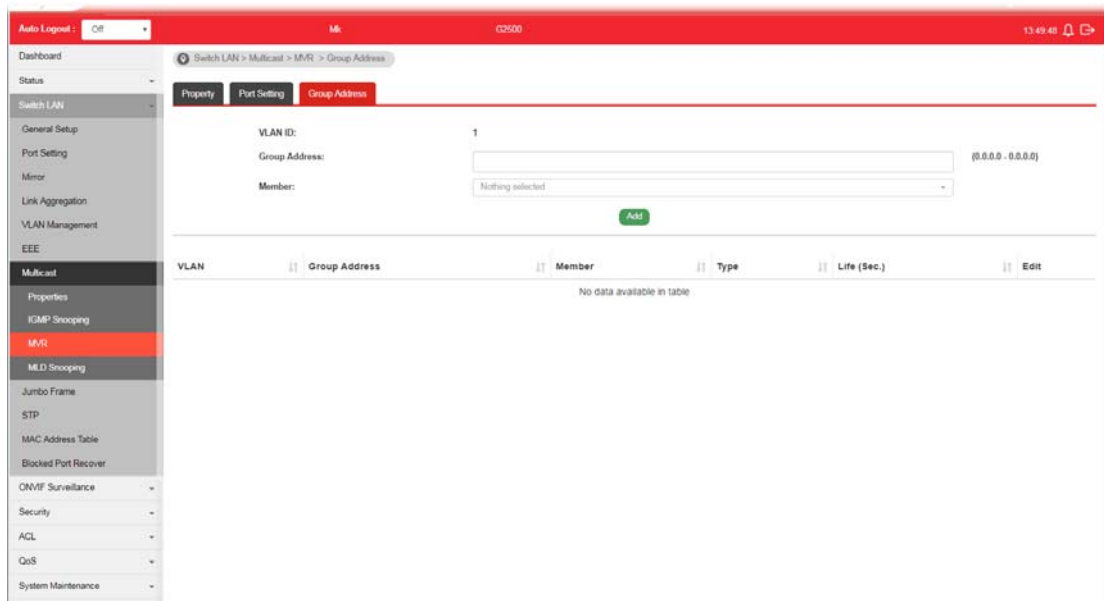
Available settings are explained as follows:

| Item                   | Description  |
|------------------------|--|
| <b>Ports</b>           | Use the drop down list to select LAN Port (GE/LAG). Later, each port can be set as Receiver or Source port respectively. If you do not satisfy with the port setting, simply click the Edit button to make the modification.   |
| <b>Role</b>            | <ul style="list-style-type: none"> <li>● <b>None</b> - Nothing will be happened to the selected LAN port in MVR operation.</li> <li>● <b>Receiver</b> - The selected port will be treated as destination port which will receive multicast data from the multicast server.</li> <li>● <b>Source</b> - The selected port will be treated as source port which will send multicast data to the receiver port.</li> </ul> |
| <b>Immediate Leave</b> | <ul style="list-style-type: none"> <li>● <b>Enabled</b> - Enable the function fo immediate leave. When</li> </ul>  |


|              |   |
|--------------|---|
|              | <p>the port (with the role of receiver) receives the leave message, it will be removed from multicast group to speed up leave latency.</p> <ul style="list-style-type: none"> <li>● <b>Disabled</b> - Disable the function of immediate leave.</li> </ul> |
| <b>Apply</b> | Apply the settings to the switch.   |
| <b>Edit</b>  |  - Click it to modify port setting (role and immediate leave).   |

### II-7-3-3 Group Address

This page allows the network administrator to configure IP address and specify port member for VLAN selected in MVR>>Property page.

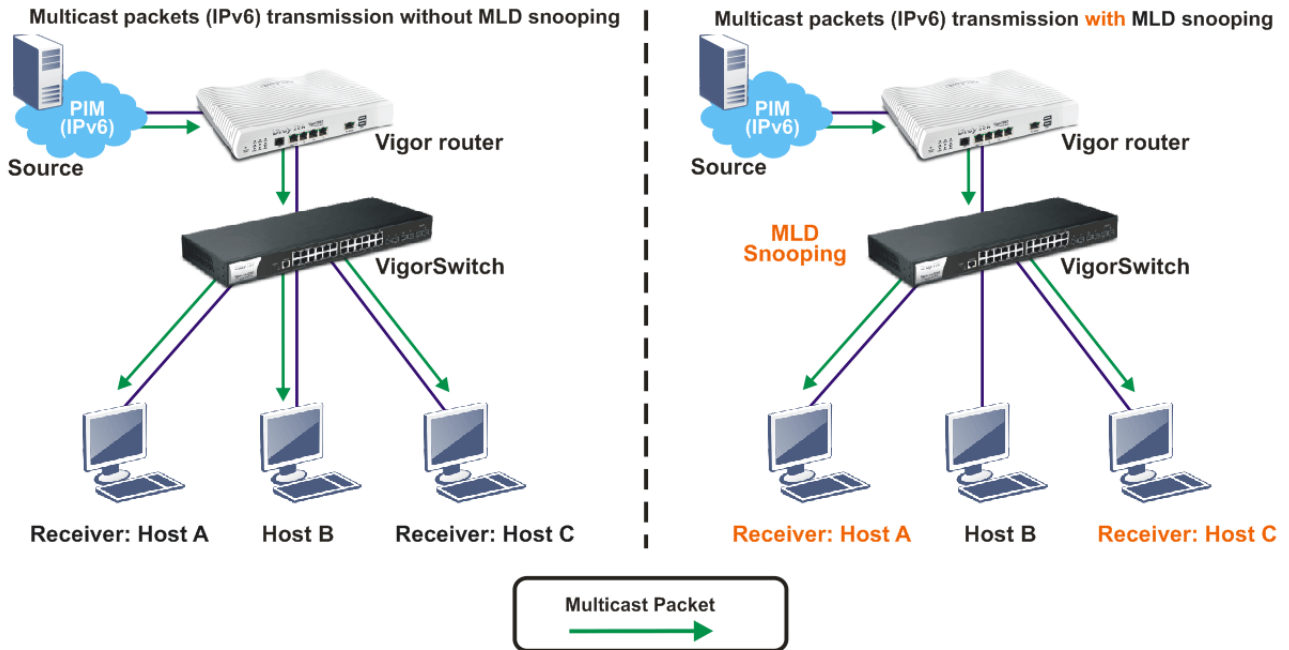


Available settings are explained as follows:

| Item                 | Description  |
|----------------------|--|
| <b>VLAN ID</b>       | Display the ID number of the VLAN.   |
| <b>Group Address</b> | Define a range of IP address(es) with the format of "xxx.xxx.xxx.xxx - xxx.xxx.xxx.xxx".                               |
| <b>Member</b>        | Choose GE/LAG port to be grouped under the selected VLAN.  |
| <b>Add</b>           | Click it to display the result based on the settings configured above.   |
| <b>Edit</b>          |  - Click it to modify the settings. |

## II-7-4 MLD Snooping

MLD snooping does the same thing as IGMP snooping. The difference is that IGMP snooping acts on IPv4 packets; MLD snooping acts on IPv6 packets. MLD snooping is the process of listening to Multicast Listener Discovery network traffic. It can examine IPv6 packets and forward these packets to designate location via VLAN port members.




### II-7-4-1 MLD Setting

This page allows the network administrator to enable/disable MLD Snooping function, select snooping version, and enable/disable snooping report suppression.

| VLAN ID | MLD Snooping Operational Status | Router Port Auto Learn | Query Robustness | Query Interval | Query Max Response Interval | Last Member Query Counter | Last Member Query Interval | Immediate Leave | Edit |
|---------|---------------------------------|------------------------|------------------|----------------|-----------------------------|---------------------------|----------------------------|-----------------|------|
| 1       | Disabled                        | Enabled                | 2                | 125            | 10                          | 2                         | 1                          | Disabled        | ✓    |

Available settings are explained as follows:

| Item | Description |
|------|-------------|
|------|-------------|

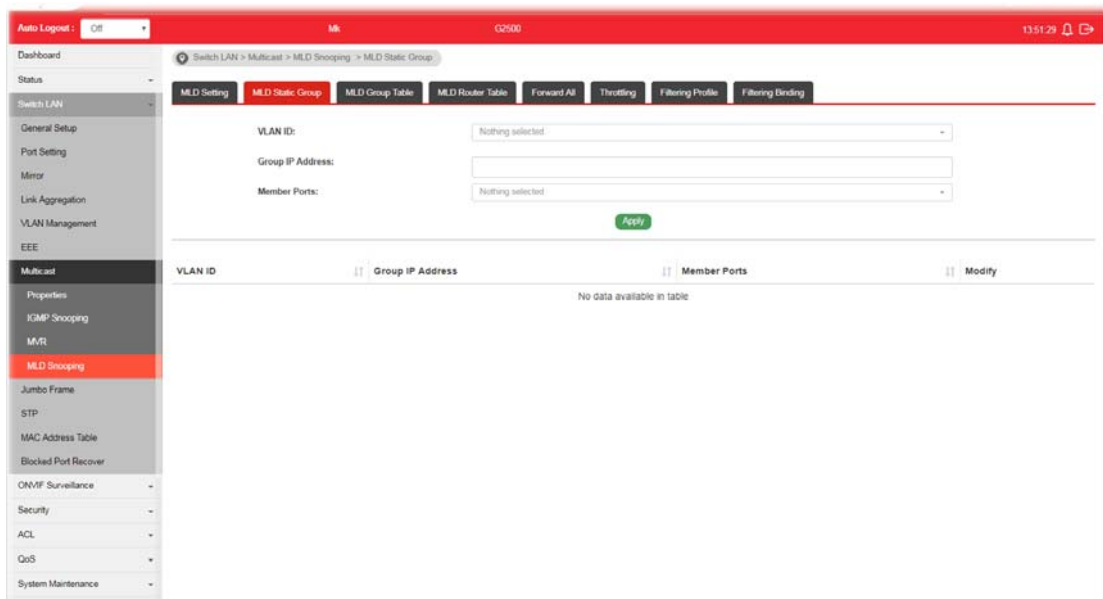
|                    |  |
|--------------------|--|
| State              | <ul style="list-style-type: none"> <li>● <b>Enabled</b> - Click it to enable the MLD snooping function.</li> <li>● <b>Disabled</b> - Click it to disable the MLD snooping function.</li> </ul>   |
| Version            | <p>VigorSwitch supports two versions of MLD snooping.</p> <ul style="list-style-type: none"> <li>● <b>MLDv1</b> - When it is selected, VigorSwitch will detect packets controlled by MLDv1 and <i>bridge</i> the traffic to IPv6 destination defined with multicast address(es).</li> <li>● <b>MLDv2</b> - When it is selected, VigorSwitch will detect packets controlled by MLDv1 and <i>forward</i> the traffic to destination defined with multicast address(es).</li> </ul>   |
| Report Suppression | <ul style="list-style-type: none"> <li>● <b>Enabled</b> - Click it to allow the switch to handle MLD reports between router and host, suppressing bandwidth used by MLD.</li> <li>● <b>Disabled</b> - Click it to disable the function.</li> </ul>   |
| Apply              | Click it to display the result based on the settings configured above.   |
| Edit               | <p> - Click it to modify the settings for the selected VLAN ID (GE/LAG port).</p> <div data-bbox="683 884 1412 1960" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <div style="text-align: center;"><b>Edit VLAN ID 1</b></div> <div style="text-align: center;"><b>MLD Snooping State</b></div> <div style="margin-bottom: 10px;"><input type="text" value="Disable"/></div> <div style="text-align: center;"><b>Router Ports Auto Learn</b></div> <div style="margin-bottom: 10px;"><input type="text" value="Enable"/></div> <div style="text-align: center;"><b>Query Robustness (Operational: 2)</b></div> <div style="margin-bottom: 10px;"><input type="text" value="2"/> (1-7, default 2)</div> <div style="text-align: center;"><b>Query Interval (Operational: 125)</b></div> <div style="margin-bottom: 10px;"><input type="text" value="125"/> Sec (30-18000, default 125)</div> <div style="text-align: center;"><b>Query Response Interval (Operational: 10)</b></div> <div style="margin-bottom: 10px;"><input type="text" value="10"/> Sec (5-20, default 10)</div> <div style="text-align: center;"><b>Last Member Query Counter (Operational: 2)</b></div> <div style="margin-bottom: 10px;"><input type="text" value="2"/> Sec (1-7, default 2)</div> <div style="text-align: center;"><b>Last Member Query Interval (Operational: 1)</b></div> <div style="margin-bottom: 10px;"><input type="text" value="1"/> Sec (1-25, default 1)</div> <div style="text-align: center;"><b>Immediate Leave:</b></div> <div style="margin-bottom: 10px;"><input type="text" value="Disable"/></div> <div style="display: flex; justify-content: center; gap: 20px;"> <input type="button" value="OK"/> <input type="button" value="Cancel"/> </div> </div> <ul style="list-style-type: none"> <li>● <b>MLD Snooping State</b> - Enable/disable the MLD snooping function for the selected port.</li> <li>● <b>Router Ports Auto Learn</b> -Set the enabling status of IGMP</li> </ul> |

router port learning. Choose **Enable** to learn router port by MLD query.

- **Query Robustness** - Set a number which allows tuning for the expected packet loss on a subnet.
- **Query Interval** - Specify the time interval for VigorSwitch to send out general MLD query to the host (responsible for responding). Later, based on the response, VigorSwitch can forward the traffic through ports in VLAN.
- **Query Response Interval** - Specify the time interval for VigorSwitch to receive the query response from the host. If time is up and no response received, the packets will be blocked and discarded.
- **Last Member Query Counter** - After querying for specified times (defined here) and still not receiving any response from the subscribed member, VigorSwitch will stop transmitting data to the related GE port(s).
- **Last Member Query Interval** - The maximum time interval between counting each member query message with no responses from any subscribed member.
- **Immediate Leave** - Click **Enable** to enable the function of immediate leave. When the GE/LAG port receives the leave message, it will be removed from multicast group to speed up leave latency.
- **OK** - Apply the settings to the switch.
- **Cancel** - Close the page and return to previous page.

## II-7-4-2 MLD Static Group

The MLD static group is allowed to assign a VLAN/port as a specific IPv6 multicast member. Every IPv6 multicast stream that belongs to the specified group IP address will be forwarded to the specified port/VLAN member.



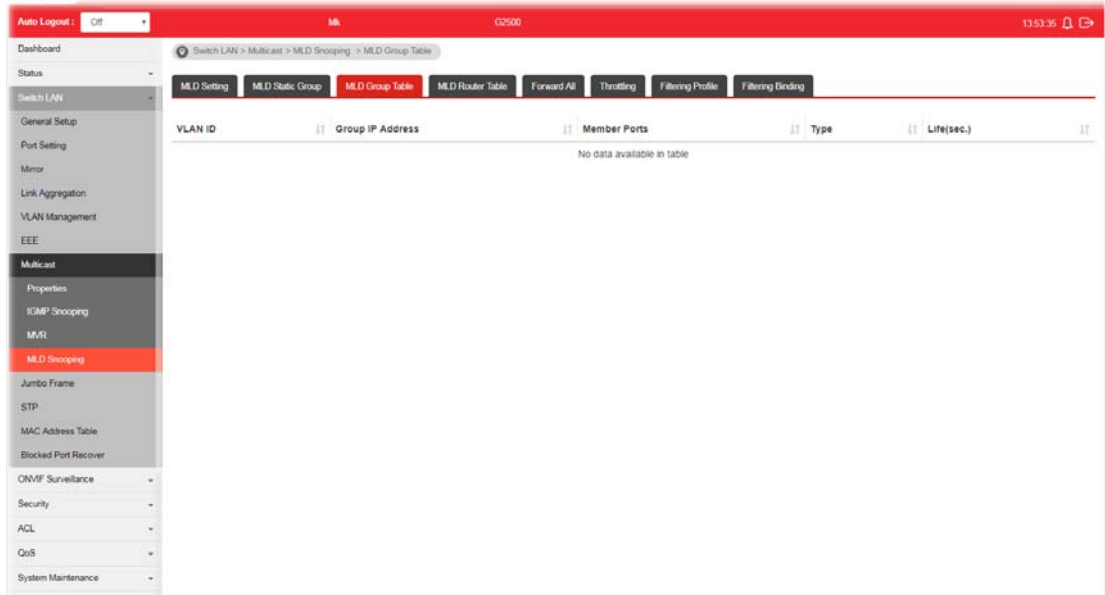
Available settings are explained as follows:

| Item    | Description   |
|---------|---|
| VLAN ID | Use the drop down list to specify a VLAN profile (created in Switch LAN>>VLAN Management>>Create Vlan) as MLD |

|                         |  |
|-------------------------|--|
|                         | <p>Static Group.</p> <p>However, if <b>State in MLD Setting</b> is not set as <b>Enabled</b>, such option will be disabled and no ID can be selected.</p>  |
| <b>Group IP Address</b> | <p>It is an identifier for the group member. Packets sent to such address will be transferred to all interfaces defined in Member Ports.</p> <p>Specify the IPv6 multicast address you wish to assign for the static group (defined in VLAN ID).</p> |
| <b>Member Ports</b>     | <p>Use the drop down list to specify interaces (GE/LAG) for receiving the packets from group IP address.</p>   |
| <b>Apply</b>            | <p>Click it to display the result based on the settings configured above.</p>  |

## II-7-4-3 MLD Group Table

This page shows currently known and dynamically learned by MLD snooping or shows the assigned IP6 multicast address group in operation.



Available settings are explained as follows:


| Item             | Description   |
|------------------|---|
| VLAN ID          | Display the name of VLAN configured in MLD Static Group.                                |
| Group IP Address | Display the IP address defined in MLD Static Group.                                     |
| Member Ports     | Display all of the interfaces defined in MLD Static Group.                              |
| Type             | Display if it is dynamically learned or statically assigned.                            |
| Life(sec.)       | Display the life time of this multicast member left if no membership report sent again. |

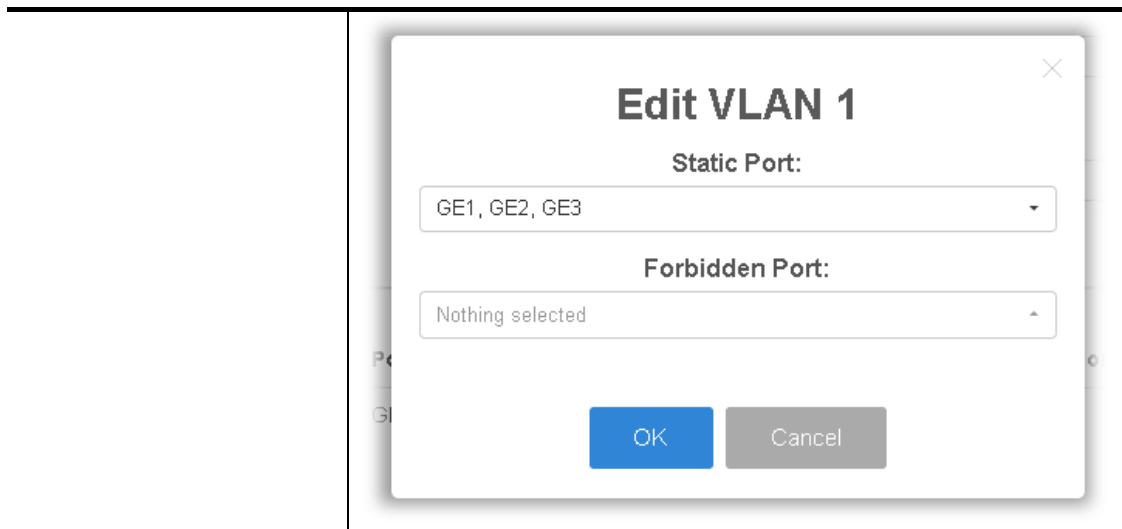


## II-7-4-4 MLD Router Table

This page is allowed to configure VLAN profile by specifying static/forbidden ports for the router (MLD querier).

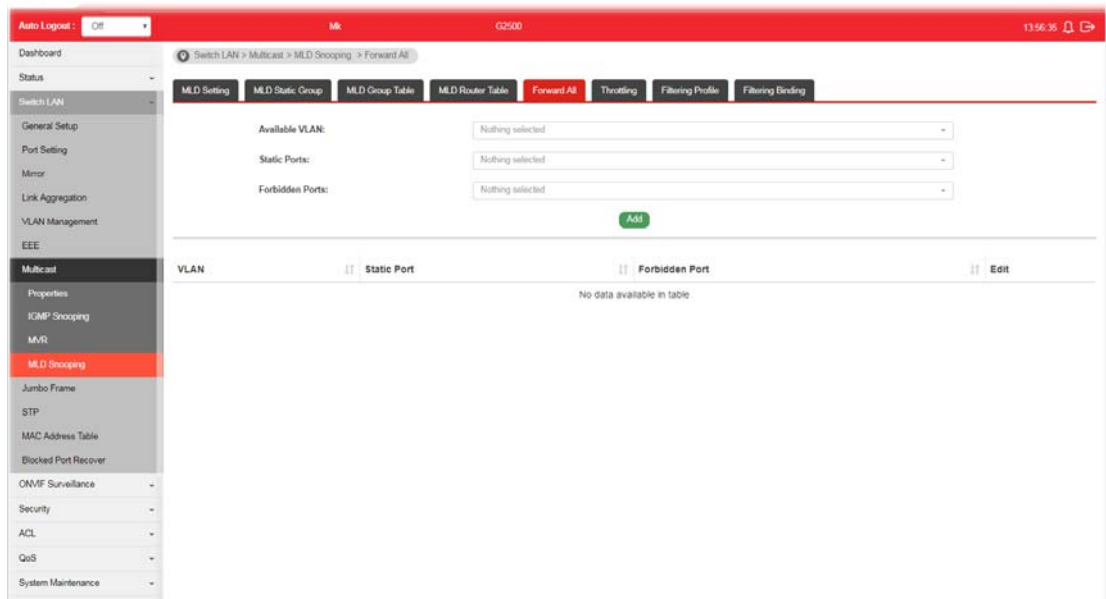
Available settings are explained as follows:

| Item                         | Description  |
|------------------------------|--|
| VLAN ID                      | Use the drop down list to specify a VLAN profile (created in Switch LAN>>VLAN Management>>Create Vlan) that the MLD querier belongs to.  |
| Type                         | <ul style="list-style-type: none"> <li>● <b>Static</b> - Specify LAN Port (GE/LAG) to send out query to remote host.</li> <li>● <b>Forbidden</b> - Use the drop down list to specify forbidden LAN Port (GE/LAG).</li> </ul> |
| Member Ports                 | Use the drop down list to choose the uplink ports where querier router exists.   |
| Add                          | Click it to display the result based on the settings configured above.   |
| Static Port / Forbidden Port | Display the static port / forbidden port member specified in Member Ports.   |
| Expire Time (sec.)           | Display the time before querier is considered no longer existed.   |
| Edit                         |  - Click it to modify the settings for the selected entry.  |





### II-7-4-5 Forward All

This page is allowed to determine which port(s) would like to receive the data (multicast packets) that forwarded by VigorSwitch.



Available settings are explained as follows:

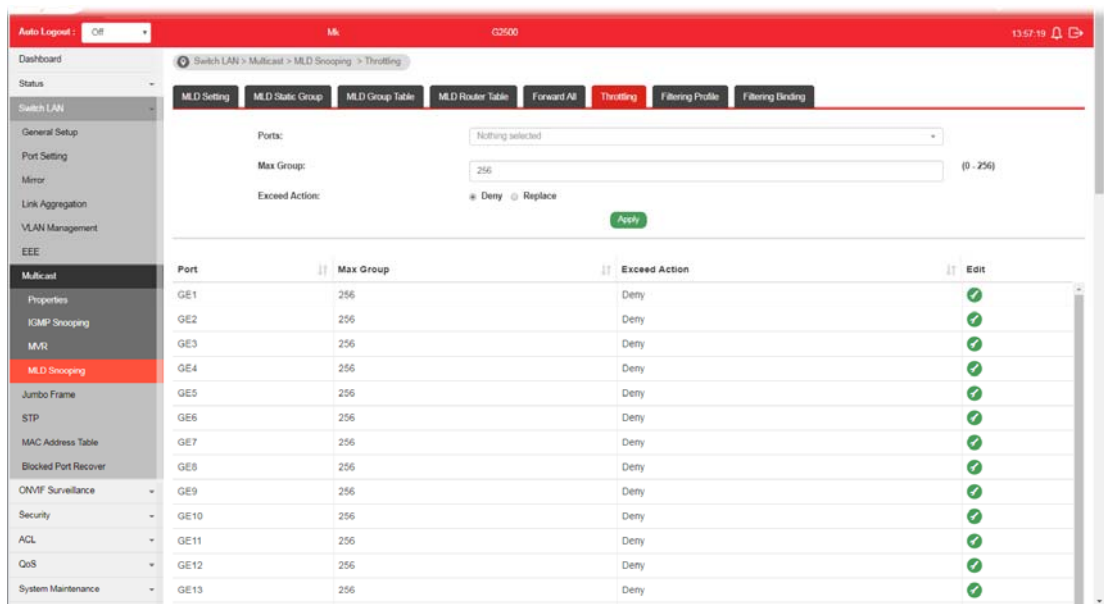
| Item            | Description   |
|-----------------|---|
| Available VLAN  | To display all of the available VLAN, the State must be set as <b>Enabled</b> in <b>MLD Setting</b> first.<br>Use the drop down list to specify a VLAN profile (created in <b>Switch LAN&gt;&gt;VLAN Management&gt;&gt;Create Vlan</b> ) that multicast packets will be forwarded to. |
| Static Ports    | Use the drop down list to specify LAN Port (GE/LAG).<br>Later, the multicast packets will be delivered to the network device connected by these ports.  |
| Forbidden Ports | Use the drop down list to specify forbidden LAN Port (GE/LAG).<br>Later, the multicast packets will not be delivered to the network device connected by these ports.  |

|      |   |
|------|---|
| Add  | Click it to display the result based on the settings configured above.  |
| Edit |  - Click it to modify port setting (static port and forbidden port).<br> - Click it to remove the selected entry. |

## II-7-4-6 Throttling


The administrator can configure the user on a switch port (GE/LAG port) belonging to which multicast group and restrict the number of multicast group that the user on the switch can join. Then the administrator is able to control the network service (e.g, IP/TV service) that the user can enjoy.

The Throttling page is used for configuring the maximum number (0~255) of MLD group that a user on a switch port can join. After defined the maximum number, each switch port interface can be set to deny the MLD join report or set to replace randomly selected multicast interface with received MLD join report.



Available settings are explained as follows:

| Item          | Description   |
|---------------|---|
| Ports         | Use the drop down list to specify LAN Port (GE/LAG) for applying throttling feature.  |
| Max Group     | Define the maximum number of MLD group profile that a user on the switch can join. If "0" is selected, then such interface (port) can join all of the MLD group profiles (defined in Filtering Profile).  |
| Exceed Action | <p>VigorSwitch will perform the action defined below when the number of MLD join report for the specified interface exceeds value defined in Max Group.</p> <ul style="list-style-type: none"> <li>● <b>Deny</b> - It is default setting. The MLD join report (for multicast service) received by such interface will be discarded.</li> <li>● <b>Replace</b> - When it is selected, a new group with MLD report received will replace the existing group.</li> </ul> |

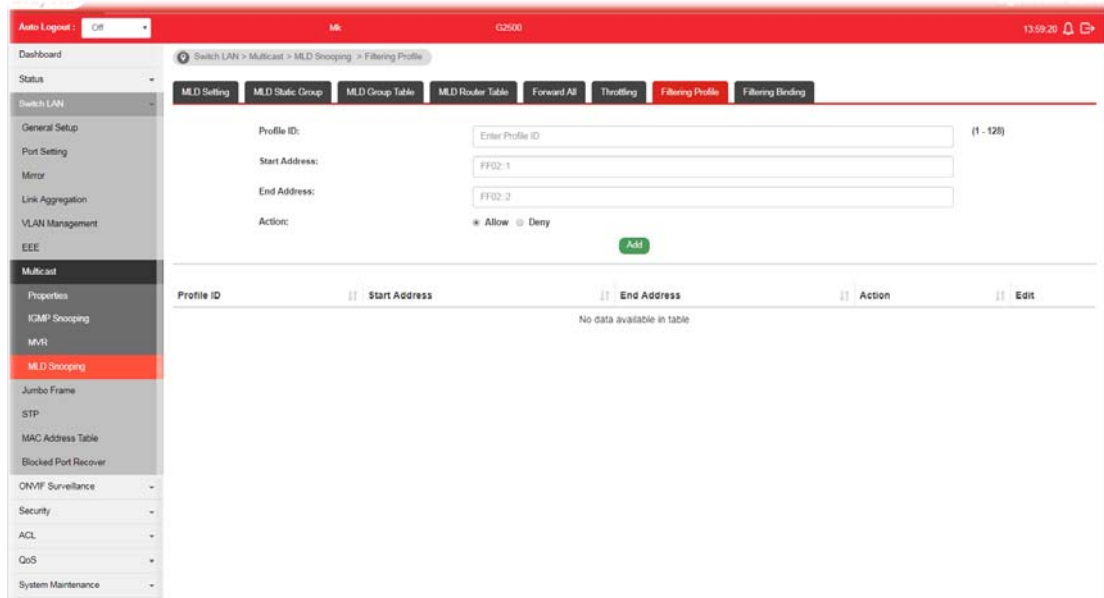
|       |   |
|-------|---|
| Apply | Apply the settings to the switch.   |
| Edit  |  - Click it to modify the settings for the selected entry. |

## II-7-4-7 Filtering Profile


The administrator can configure the user on a switch port (GE/LAG port) belonging to which multicast group and restrict the number of multicast group that the user on the switch can join. Then the administrator is able to control the network service (e.g., IP/TV service) that the user can enjoy.

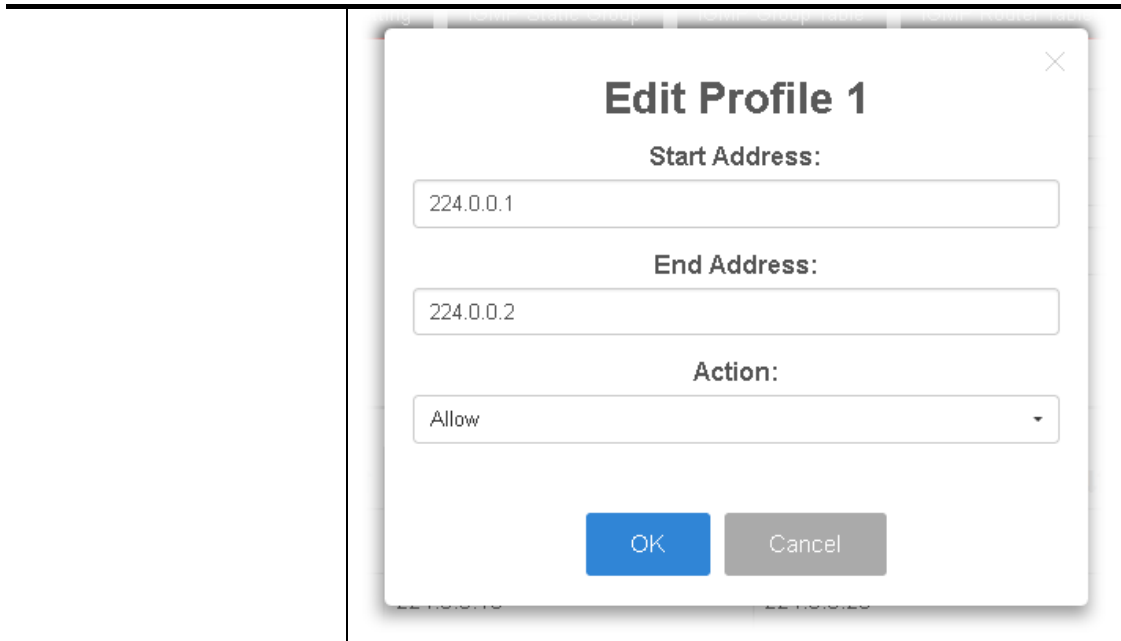
The filtering profile page allows to configure up to 128 IP-group (for multicast service) profiles (starting and ending point within an IP range shall be specified). Each IP group profile can be set for permission of / denial of network service respectively.

In addition, such filtering profile is only effective for controlling the query for multicast traffic. It has nothing to do with the general MLD query.



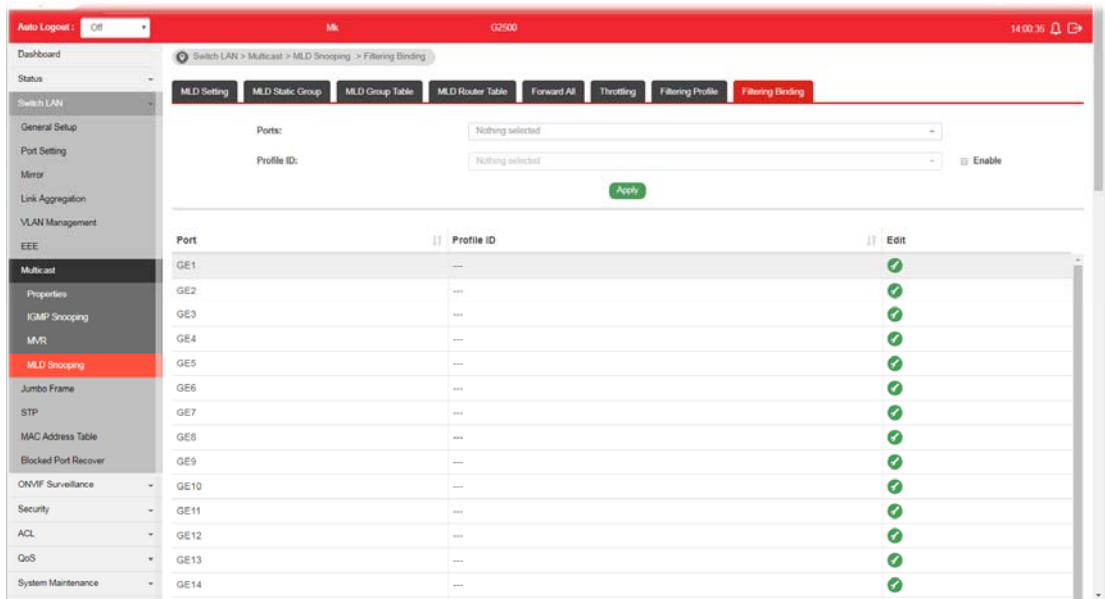
Available settings are explained as follows:

| Item          | Description   |
|---------------|---|
| Profile ID    | Use the drop down list to select one filtering profile (1~128) for MLD snooping.  |
| Start Address | Enter an IP address as the starting point for the IP range.   |
| End Address   | Enter an IP address as the ending point for the IP range.   |
| Action        | <ul style="list-style-type: none"> <li>● <b>Deny</b> - It is default setting. The forwarding request of multicast traffic will be discarded.</li> <li>● <b>Allow</b> - When it is selected, the request for multicast traffic will be forwarded to the multicast group normally.</li> </ul> |
| Add           | Click it to display the result based on the settings configured above.  |
| Edit          |  - Click it to modify the settings for the selected entry.   |




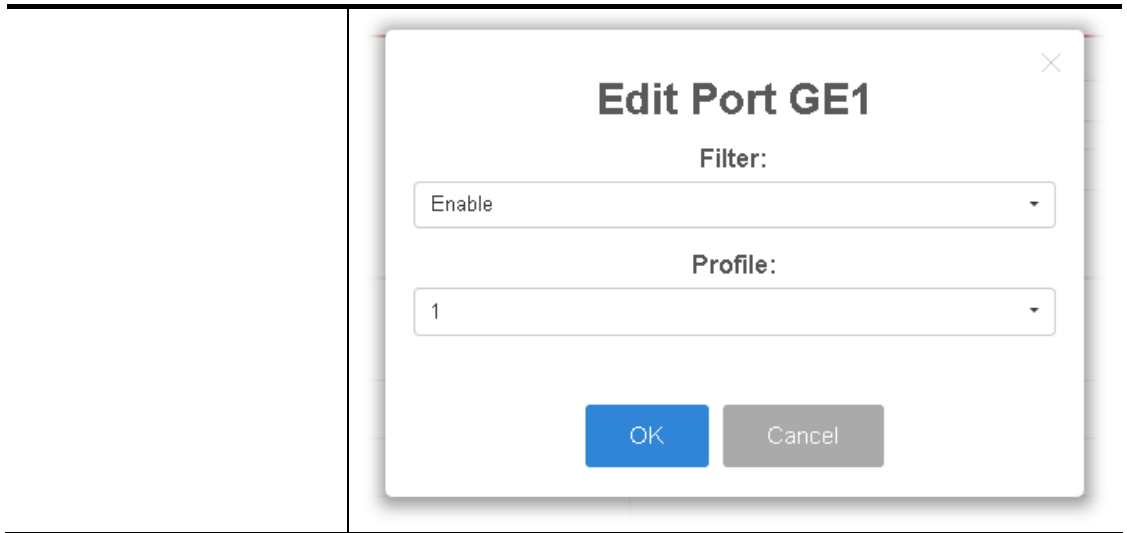
### II-7-4-8 Filtering Binding

This page allows the network administrator to select a filtering profile for LAN/GE port to process multicast traffic.



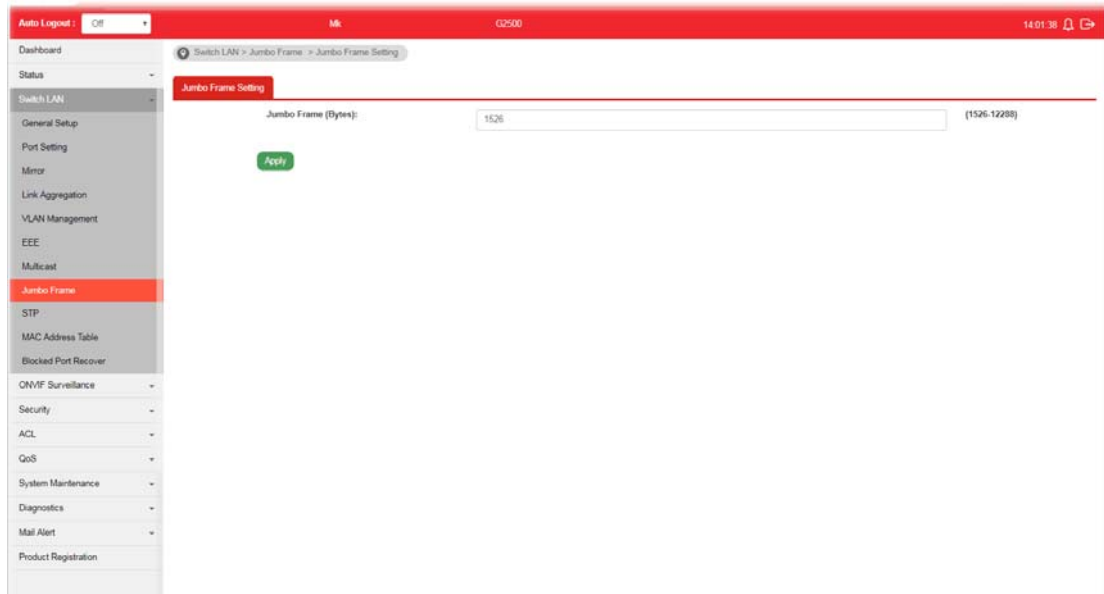
Available settings are explained as follows:

| Item       | Description  |
|------------|--|
| Ports      | Use the drop down list to specify LAN Port (GE/LAG).   |
| Profile ID | Use the drop down list to choose the filtering profile for the select port/interface. <ul style="list-style-type: none"> <li>● <b>Enable</b> - Check this box first to make profile ID selection be available for choosing.</li> </ul> |
| Apply      | Apply the settings to the switch.  |
| Edit       |  - Click it to modify port setting (enabling / disabling filter function and choosing a profile for such interface).                                |



## II-8 Jumbo Frame

This page allows a user to configure switch port jumbo frame settings.



Available settings are explained as follows:

| Item                | Description   |
|---------------------|---|
| Jumbo Frame (Bytes) | Enter Jumbo frame size. The valid range is 1526 bytes - 9216 bytes. |
| Apply               | Apply the settings to the switch.                                   |

## II-9 STP

The Spanning Tree Protocol (STP) is a network protocol that ensures a loop-free topology for any bridged Ethernet local area network.

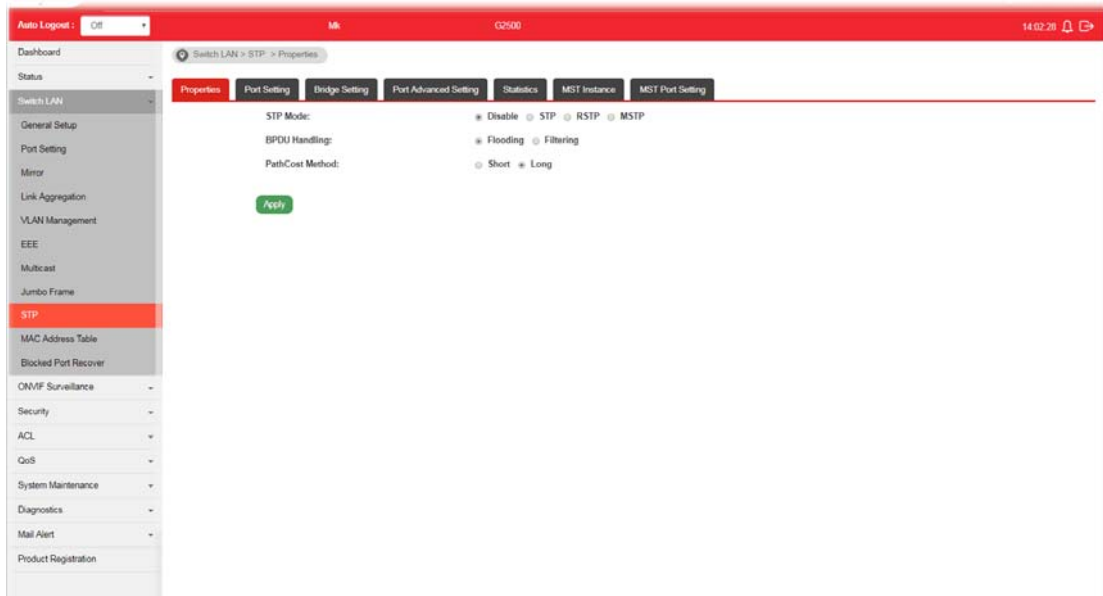
Bridge Protocol Data Units (BPDUs) are frames that contain information about the Spanning Tree Protocol (STP). Switches send BPDUs using a unique MAC address from its origin port and a multicast address as destination MAC (01:80:C2:00:00:00, or 01:00:0C:CC:CC:CD for Per VLAN Spanning Tree).

For STP algorithms to function, the switches need to share information about themselves and their connections. What they share are bridge protocol data units (BPDUs).

BPDUs are sent out as multicast frames to which only other layer 2 switches or bridges are listening. If any loops (multiple possible paths between switches) are found in the network topology, the switches will co-operate to disable a port or ports to ensure that there are no loops; that is, from one device to any other device in the layer 2 network, only one path can be taken.

### II-9-1 Properties

This page allows a user to configure and display Spanning Tree Protocol (STP) property configuration.



Available settings are explained as follows:

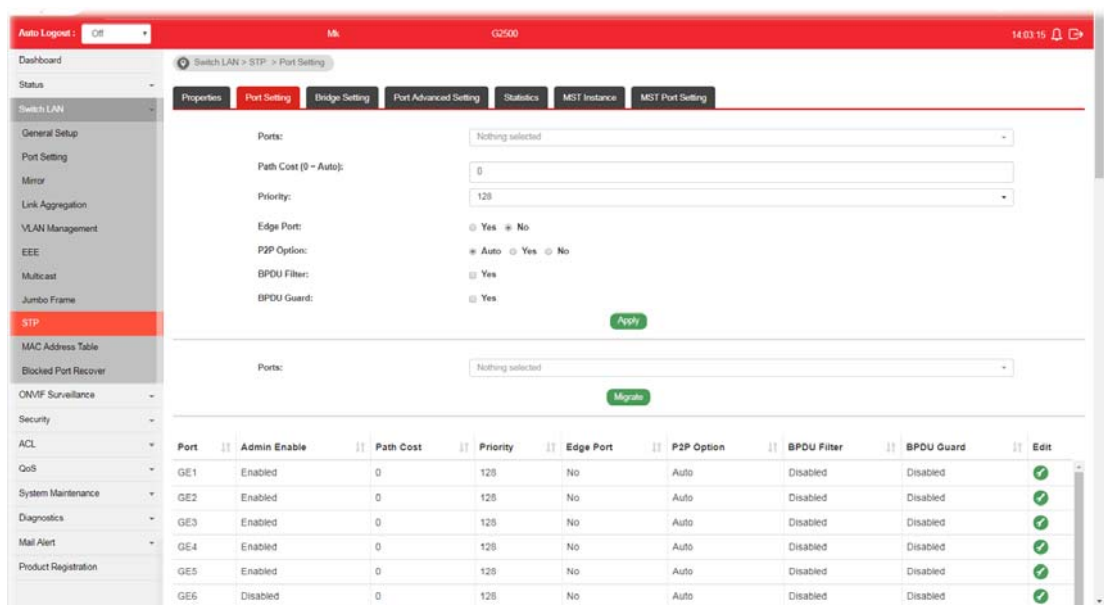
| Item          | Description  |
|---------------|--|
| STP Mode      | Set the operating mode of Spanning Tree (STP). <ul style="list-style-type: none"><li>● Disabled - Disable the STP operation.</li><li>● STP - Enable the Spanning Tree (STP) operation.</li><li>● RSTP - Enable the Rapid Spanning Tree (RSTP) operation.</li><li>● MSTP - Enable the Multiple Spanning Tree Protocol (MSTP) operation.</li></ul> |
| BPDU Handling | <ul style="list-style-type: none"><li>● Specify the BPDU forward method when the STP is disabled.</li></ul>  |



|                 |   |
|-----------------|---|
|                 | <ul style="list-style-type: none"> <li>● <b>Filtering</b> - Filter the BPDU when STP is disabled.</li> <li>● <b>Flooding</b> - Flood the BPDU when STP is disabled.</li> </ul>  |
| PathCost Method | <ul style="list-style-type: none"> <li>● Specify the path cost method.</li> <li>● <b>Long</b> - Specifies that the default port path costs are within the range: 1~200,000,000.</li> <li>● <b>Short</b> - Specifies that the default port path costs are within the range: 1~65,535.</li> </ul> |
| Apply           | Apply the settings to the switch.   |

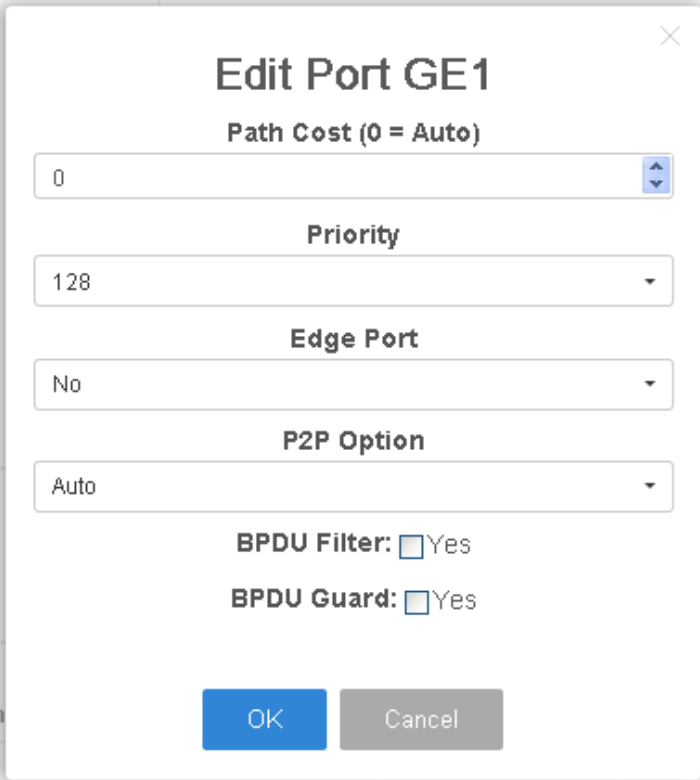
## II-9-2 Port Setting

This page allows the user to configure and display Spanning Tree Protocol (STP) port settings.



Available settings are explained as follows:

| Item               | Description   |
|--------------------|---|
| Ports              | Use the drop down to specify the interface ID or the list of interface IDs.   |
| Path Cost (0=Auto) | Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended to assign this value according to the speed of the bridge. The slower the media, the higher the cost. Entering 0 means the switch will automatically assign a value.   |
| Priority           | Specify a priority value for the switch. The smaller the priority value, the higher the priority and greater chance of becoming the root.   |
| Edge Port          | <p>In the edge mode, the interface would be put into the Forwarding state immediately upon link up. If the edge mode is enabled for the interface and there are BPDUs received on the interface, the loop might be occurred in the short time before the STP state change.</p> <ul style="list-style-type: none"> <li>● <b>Yes</b> - Enable the function.</li> <li>● <b>No</b> - Disable the function.</li> </ul> |

|             |  |
|-------------|--|
| P2P Option  | <ul style="list-style-type: none"> <li>● <b>Auto</b> - VigorSwitch determines the STP of link type for this port automatically.</li> <li>● <b>Yes</b> - It means the STP of link type on this port is full-duplex and directly connect to another switch or host.</li> <li>● <b>No</b> - It means the STP of link type on this port is "not" full-duplex and "does not" directly connect to another switch or host.</li> </ul> |
| BPDU Filter | Yes - Drop all BPDU packets and no BPDU will be sent.  |
| BPDU Guard  | Yes - BPDU Guard further protects your switch by turning this port into error state and shutdown if any BPDU received from this port. Check it to enable such function.  |
| Apply       | Apply the settings to the switch.<br>After clicking it, the settings configured above will be shown on the table below.  |
| Ports       | Use the drop down to specify the interface(s) for applying the function of <b>Migrate</b> .  |
| Migrate     | Click it to force the port(s) specified above to send one RSTP BPDU (Rapid Spanning Tree Protocol Bridge Protocol Data Unit).  |
| Edit        | Click it to modify the settings for the selected GE port.<br>  |

## II-9-3 Bridge Setting

This page allows the network administrator to configure required information to negotiate with other VigorSwitch for determining the bridge switch.

Available settings are explained as follows:

| Item          | Description   |
|---------------|---|
| Priority      | Specify the bridge priority. The valid range is from 0 to 61440, and the value should be the multiple of 4096. It ensures the probability that the switch is selected as the root bridge, and the lower value has the higher priority for the switch to be selected as the root bridge of the topology. |
| Forward Delay | Specify the STP forward delay time, which is the amount of time that a port remains in the Listening and Learning states before it enters the Forwarding state. Its valid range is from 4 to 30 seconds.  |
| Max Age       | Specify the time interval in seconds for a switch to wait the configuration messages, without attempting to redefine its own configuration.   |
| Tx Hold Count | Specify the tx-hold-count used to limit the maximum numbers of packets transmission per second. The valid range is from 1 to 10.  |
| Hello Time    | Specify the STP hello time in second to broadcast its hello message to other bridge by Designated Ports. Its valid range is from 1 to 10 seconds.   |
| Apply         | Apply the settings to the switch.   |

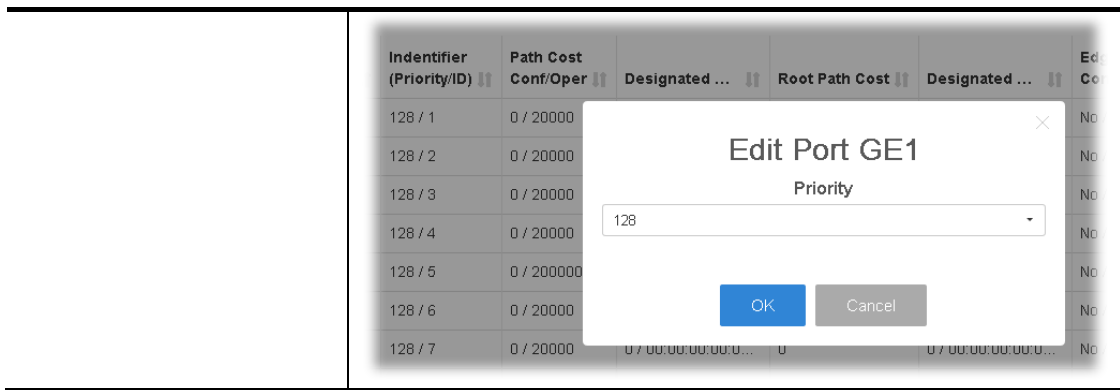
## II-9-4 Port Advanced Setting

This page allows user to edit general setting of STP CIST port and browser CIST port status.

| Port | Identifier (Priority/ID) | Path Cost Conf/Oper | Designated Root Bridge | Root Path Cost | Designated Bridge     | Edge Port Conf/Oper | P2P Option Conf/Oper | Port Role | Port State | Edit |
|------|--------------------------|---------------------|------------------------|----------------|-----------------------|---------------------|----------------------|-----------|------------|------|
| GE1  | 128 / 1                  | 0 / 20000           | 0 / 00:00:00:00:00:00  | 0              | 0 / 00:00:00:00:00:00 | No / No             | Auto / No            | Disabled  | Disabled   | ✓    |
| GE2  | 128 / 2                  | 0 / 20000           | 0 / 00:00:00:00:00:00  | 0              | 0 / 00:00:00:00:00:00 | No / No             | Auto / Yes           | Disabled  | Forwarding | ✓    |
| GE3  | 128 / 3                  | 0 / 20000           | 0 / 00:00:00:00:00:00  | 0              | 0 / 00:00:00:00:00:00 | No / No             | Auto / No            | Disabled  | Disabled   | ✓    |
| GE4  | 128 / 4                  | 0 / 20000           | 0 / 00:00:00:00:00:00  | 0              | 0 / 00:00:00:00:00:00 | No / No             | Auto / Yes           | Disabled  | Forwarding | ✓    |
| GE5  | 128 / 5                  | 0 / 20000           | 0 / 00:00:00:00:00:00  | 0              | 0 / 00:00:00:00:00:00 | No / No             | Auto / No            | Disabled  | Disabled   | ✓    |
| GE6  | 128 / 6                  | 0 / 20000           | 0 / 00:00:00:00:00:00  | 0              | 0 / 00:00:00:00:00:00 | No / No             | Auto / No            | Disabled  | Disabled   | ✓    |
| GE7  | 128 / 7                  | 0 / 20000           | 0 / 00:00:00:00:00:00  | 0              | 0 / 00:00:00:00:00:00 | No / No             | Auto / No            | Disabled  | Disabled   | ✓    |
| GE8  | 128 / 8                  | 0 / 20000           | 0 / 00:00:00:00:00:00  | 0              | 0 / 00:00:00:00:00:00 | No / No             | Auto / No            | Disabled  | Disabled   | ✓    |
| GE9  | 128 / 9                  | 0 / 20000           | 0 / 00:00:00:00:00:00  | 0              | 0 / 00:00:00:00:00:00 | No / No             | Auto / No            | Disabled  | Disabled   | ✓    |
| GE10 | 128 / 10                 | 0 / 20000           | 0 / 00:00:00:00:00:00  | 0              | 0 / 00:00:00:00:00:00 | No / No             | Auto / No            | Disabled  | Disabled   | ✓    |
| GE11 | 128 / 11                 | 0 / 20000           | 0 / 00:00:00:00:00:00  | 0              | 0 / 00:00:00:00:00:00 | No / No             | Auto / No            | Disabled  | Disabled   | ✓    |
| GE12 | 128 / 12                 | 0 / 20000           | 0 / 00:00:00:00:00:00  | 0              | 0 / 00:00:00:00:00:00 | No / No             | Auto / No            | Disabled  | Disabled   | ✓    |
| GE13 | 128 / 13                 | 0 / 20000           | 0 / 00:00:00:00:00:00  | 0              | 0 / 00:00:00:00:00:00 | No / No             | Auto / No            | Disabled  | Disabled   | ✓    |
| GE14 | 128 / 14                 | 0 / 20000           | 0 / 00:00:00:00:00:00  | 0              | 0 / 00:00:00:00:00:00 | No / No             | Auto / No            | Disabled  | Disabled   | ✓    |
| GE15 | 128 / 15                 | 0 / 20000           | 0 / 00:00:00:00:00:00  | 0              | 0 / 00:00:00:00:00:00 | No / No             | Auto / No            | Disabled  | Disabled   | ✓    |
| GE16 | 128 / 16                 | 0 / 20000           | 0 / 00:00:00:00:00:00  | 0              | 0 / 00:00:00:00:00:00 | No / No             | Auto / No            | Disabled  | Disabled   | ✓    |
| GE17 | 128 / 17                 | 0 / 20000           | 0 / 00:00:00:00:00:00  | 0              | 0 / 00:00:00:00:00:00 | No / No             | Auto / No            | Disabled  | Disabled   | ✓    |
| GE18 | 128 / 18                 | 0 / 20000           | 0 / 00:00:00:00:00:00  | 0              | 0 / 00:00:00:00:00:00 | No / No             | Auto / No            | Disabled  | Disabled   | ✓    |

Available settings are explained as follows:

| Item                    | Description  |
|-------------------------|--|
| Port                    | Display the interface number for GE and LAG.   |
| Identifier(Priority/ID) | Display the spanning tree port identifier.   |
| Path Cost Conf/Oper     | Display current path cost of given port.   |
| Designated Root Bridge  | Display the identifier of designated root bridge.  |
| Root Path Cost          | Display the operational root path cost.  |
| Designated Bridge       | Display the identifier of next bridge on this port.  |
| Edge Port Conf/Oper     | Display if this port is configured as Edge of STP network, for speed up link up.   |
| P2P MAC Conf/Oper       | Display if this port is configured as point to point link to another switch or host.   |
| Port Role               | Display current port role on the specified port. The possible values will be: "Disabled", "Root", "Designated", "Alternative", and "Backup". |
| Port State              | Display current port state on the specified port. The possible values will be: "Disabled", "Discarding", "Learning", and "Forwarding".       |
| Edit                    | Click it to modify the priority setting for the selected GE port / LAG port.   |



## II-9-5 Statistics

This page displays STP statistics.

| Port | Configure BPDUs Rx. | TCN BPDUs Rx. | Configure BPDUs Tx. | TCN BPDUs Tx. |
|------|---------------------|---------------|---------------------|---------------|
| GE1  | 0                   | 0             | 0                   | 0             |
| GE2  | 0                   | 0             | 0                   | 0             |
| GE3  | 0                   | 0             | 0                   | 0             |
| GE4  | 0                   | 0             | 0                   | 0             |
| GE5  | 0                   | 0             | 0                   | 0             |
| GE6  | 0                   | 0             | 0                   | 0             |
| GE7  | 0                   | 0             | 0                   | 0             |
| GE8  | 0                   | 0             | 0                   | 0             |
| GE9  | 0                   | 0             | 0                   | 0             |
| GE10 | 0                   | 0             | 0                   | 0             |
| GE11 | 0                   | 0             | 0                   | 0             |
| GE12 | 0                   | 0             | 0                   | 0             |
| GE13 | 0                   | 0             | 0                   | 0             |
| GE14 | 0                   | 0             | 0                   | 0             |
| GE15 | 0                   | 0             | 0                   | 0             |
| GE16 | 0                   | 0             | 0                   | 0             |
| GE17 | 0                   | 0             | 0                   | 0             |
| GE18 | 0                   | 0             | 0                   | 0             |
| GE19 | 0                   | 0             | 0                   | 0             |

Available settings are explained as follows:


| Item                | Description  |
|---------------------|--|
| Port                | Display the port number (GE / LAG).                |
| Configure BPDUs Rx. | Display the counts of the received CONFIG BPDU.    |
| TCN BPDUs Rx.       | Display the counts of the received TCN BPDU.       |
| Configure BPDUs Tx. | Display the counts of the transmitted CONFIG BPDU. |
| TCN BPDUs Rx        | Display the counts of the transmitted TCN BPDU.    |

## II-9-6 MST Instance

MSTP allows traffic of different VLAN to be mapped into different MST Instances. VigorSwitch supports up to 16 independent MST instances (0~15) with which the VLAN can be associated.

| MSTI | Priority | Bridge Identifier       | Designated Root Brid... | Root Port | Root Path Cost | Remaining Hop | VLAN   | Edit |
|------|----------|-------------------------|-------------------------|-----------|----------------|---------------|--------|------|
| 0    | 32768    | 32768-00:1D:AA:00:0A:62 | 0-00:00:00:00:00:00     | N/A       | 0              | 0             | 1-4094 |      |
| 1    | 32768    | 32768-00:1D:AA:00:0A:62 | 0-00:00:00:00:00:00     | N/A       | 0              | 0             |        | ✓    |
| 2    | 32768    | 32768-00:1D:AA:00:0A:62 | 0-00:00:00:00:00:00     | N/A       | 0              | 0             |        | ✓    |
| 3    | 32768    | 32768-00:1D:AA:00:0A:62 | 0-00:00:00:00:00:00     | N/A       | 0              | 0             |        | ✓    |
| 4    | 32768    | 32768-00:1D:AA:00:0A:62 | 0-00:00:00:00:00:00     | N/A       | 0              | 0             |        | ✓    |
| 5    | 32768    | 32768-00:1D:AA:00:0A:62 | 0-00:00:00:00:00:00     | N/A       | 0              | 0             |        | ✓    |
| 6    | 32768    | 32768-00:1D:AA:00:0A:62 | 0-00:00:00:00:00:00     | N/A       | 0              | 0             |        | ✓    |
| 7    | 32768    | 32768-00:1D:AA:00:0A:62 | 0-00:00:00:00:00:00     | N/A       | 0              | 0             |        | ✓    |
| 8    | 32768    | 32768-00:1D:AA:00:0A:62 | 0-00:00:00:00:00:00     | N/A       | 0              | 0             |        | ✓    |
| 9    | 32768    | 32768-00:1D:AA:00:0A:62 | 0-00:00:00:00:00:00     | N/A       | 0              | 0             |        | ✓    |
| 10   | 32768    | 32768-00:1D:AA:00:0A:62 | 0-00:00:00:00:00:00     | N/A       | 0              | 0             |        | ✓    |
| 11   | 32768    | 32768-00:1D:AA:00:0A:62 | 0-00:00:00:00:00:00     | N/A       | 0              | 0             |        | ✓    |
| 12   | 32768    | 32768-00:1D:AA:00:0A:62 | 0-00:00:00:00:00:00     | N/A       | 0              | 0             |        | ✓    |
| 13   | 32768    | 32768-00:1D:AA:00:0A:62 | 0-00:00:00:00:00:00     | N/A       | 0              | 0             |        | ✓    |
| 14   | 32768    | 32768-00:1D:AA:00:0A:62 | 0-00:00:00:00:00:00     | N/A       | 0              | 0             |        | ✓    |
| 15   | 32768    | 32768-00:1D:AA:00:0A:62 | 0-00:00:00:00:00:00     | N/A       | 0              | 0             |        | ✓    |

Available settings are explained as follows:

| Item | Description   |
|------|---|
| MSTI | Display the index number of MST Instance. Each MSTI can have one or multiple VLANs.   |
| Edit |  - Click it to modify the priority setting for the selected GE port / LAG port. <div data-bbox="694 1332 1204 2049" style="border: 1px solid gray; padding: 10px; margin-top: 10px;"> <p style="text-align: center;"><b>Edit MSTI 1</b></p> <p style="text-align: center;"><b>VLAN</b></p> <p>0 (1 - 4094, set 0 to cancel)</p> <p style="text-align: center;"><b>Priority</b></p> <p>32768 (0 - 61440, default 32768)</p> <p style="text-align: center;"><b>Bridge Identifier</b></p> <p>32768-00:1D:AA:11:22:44</p> <p style="text-align: center;"><b>Designated Root Bridge</b></p> <p>0-00:00:00:00:00:00</p> <p style="text-align: center;"><b>Root Port</b></p> <p></p> <p style="text-align: center;"><b>Root Path Cost</b></p> <p>0</p> <p style="text-align: center;"><b>Remaining Hop</b></p> <p>0</p> <p style="text-align: center;">OK Cancel</p> </div> |


- VLAN - Enter the ID (1-4094) of the VLAN which should be associated with this MSTI.
- Priority - The switch priority for this MST instance. A lower number gives the switch higher chance to be chosen as the root bridge.
- Bridge Identifier - Display the priority of MSTI instance number + MAC address of the switch.
- Designated Root Bridge - Display the Bridge Identifier of the root bridge.
- Root Port - Display the port toward the root.
- Root Path Cost - Display the path cost toward the root.
- Remaining Hop - Display the remaining hop count in BPDU.
- VLAN - Display the range of VLAN ID numbers.
- OK - Save the modifications.

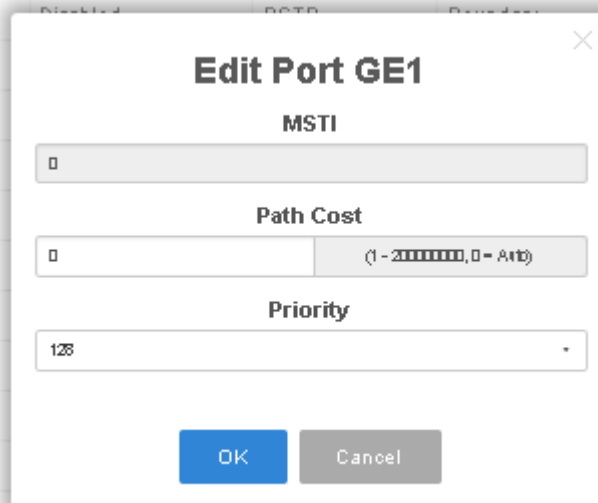
## II-9-7 MST Port Setting

MST Port Settings is used to configure the GE port / LAG group settings for each MST instance. The table displays the MST parameters for each port.

| Port | Path Cost | Priority | Port Role | Port State | Mode | Type     | Designated Bridge   | Designated Port ID | Designated Cost | Remaining Hop | Edit |
|------|-----------|----------|-----------|------------|------|----------|---------------------|--------------------|-----------------|---------------|------|
| GE1  | 20000     | 128      | Disabled  | Disabled   | RSTP | Boundary | 0-00:00:00:00:00:00 | 128-1              | 20000           | 20            | ✓    |
| GE2  | 20000     | 128      | Disabled  | Forwarding | RSTP | Boundary | 0-00:00:00:00:00:00 | 128-2              | 20000           | 20            | ✓    |
| GE3  | 20000     | 128      | Disabled  | Disabled   | RSTP | Boundary | 0-00:00:00:00:00:00 | 128-3              | 20000           | 20            | ✓    |
| GE4  | 20000     | 128      | Disabled  | Forwarding | RSTP | Boundary | 0-00:00:00:00:00:00 | 128-4              | 20000           | 20            | ✓    |
| GE5  | 20000     | 128      | Disabled  | Disabled   | RSTP | Boundary | 0-00:00:00:00:00:00 | 128-5              | 20000           | 20            | ✓    |
| GE6  | 20000     | 128      | Disabled  | Disabled   | RSTP | Boundary | 0-00:00:00:00:00:00 | 128-6              | 20000           | 20            | ✓    |
| GE7  | 20000     | 128      | Disabled  | Disabled   | RSTP | Boundary | 0-00:00:00:00:00:00 | 128-7              | 20000           | 20            | ✓    |
| GE8  | 20000     | 128      | Disabled  | Disabled   | RSTP | Boundary | 0-00:00:00:00:00:00 | 128-8              | 20000           | 20            | ✓    |
| GE9  | 20000     | 128      | Disabled  | Disabled   | RSTP | Boundary | 0-00:00:00:00:00:00 | 128-9              | 20000           | 20            | ✓    |
| GE10 | 20000     | 128      | Disabled  | Disabled   | RSTP | Boundary | 0-00:00:00:00:00:00 | 128-10             | 20000           | 20            | ✓    |
| GE11 | 20000     | 128      | Disabled  | Disabled   | RSTP | Boundary | 0-00:00:00:00:00:00 | 128-11             | 20000           | 20            | ✓    |
| GE12 | 20000     | 128      | Disabled  | Disabled   | RSTP | Boundary | 0-00:00:00:00:00:00 | 128-12             | 20000           | 20            | ✓    |
| GE13 | 20000     | 128      | Disabled  | Disabled   | RSTP | Boundary | 0-00:00:00:00:00:00 | 128-13             | 20000           | 20            | ✓    |
| GE14 | 20000     | 128      | Disabled  | Disabled   | RSTP | Boundary | 0-00:00:00:00:00:00 | 128-14             | 20000           | 20            | ✓    |
| GE15 | 20000     | 128      | Disabled  | Disabled   | RSTP | Boundary | 0-00:00:00:00:00:00 | 128-15             | 20000           | 20            | ✓    |
| GE16 | 20000     | 128      | Disabled  | Disabled   | RSTP | Boundary | 0-00:00:00:00:00:00 | 128-16             | 20000           | 20            | ✓    |

Available settings are explained as follows:

| Item | Description   |
|------|---|
| MSTI | Select one of the MST instances.  |
| Edit |  - Click it to modify the path cost and priority setting for the port. |



- **MSTI** - Display the selected MST instance.
- **Path Cost** - Set path cost value for the port. A port with lowest value will be used as the forwarding port by spanning tree. Default value was set according to the bandwidth of the port.
- **Priority** - Among the ports with same path cost, port with lower priority will have higher chance to be used as the forwarding port by spanning tree. Use the drop down list to choose desired priority value.



## II-10 MAC Address Table

This section allows user to view the dynamic MAC address entries in the MAC table, change related setting, and assign MAC address into MAC table.

### II-10-1 Static MAC Setting

This section allows user to manually assign MAC address into MAC table. The configuration result will be displayed on the table listed on the lower side of this web page.

The screenshot displays the 'Static MAC' configuration page. At the top, there's a navigation breadcrumb: 'Switch LAN > MAC Address Table > Static MAC Setting > Static MAC'. The main content area has three input fields: 'MAC Address' with the value '00:00:00:00:00:00', 'VLAN' with a dropdown set to 'default', and 'Port' with a dropdown set to 'GE1'. A green 'Add' button is positioned below these fields. Below the form is a table with the following data:

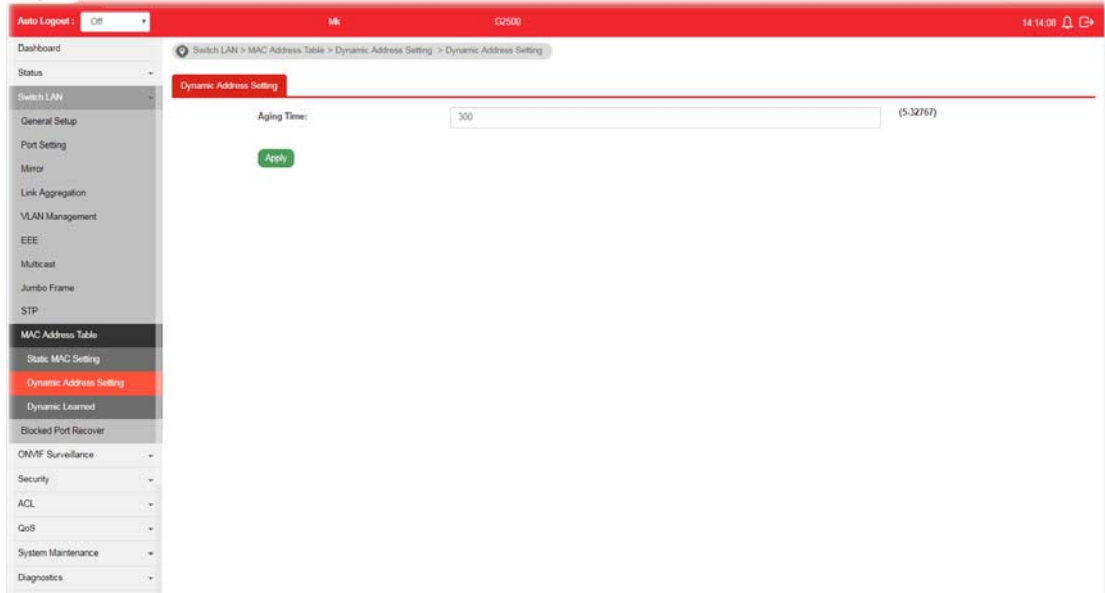
| No. | MAC Address       | VLAN       | Port | Delete |
|-----|-------------------|------------|------|--------|
| 1   | 00:1D:AA:00:0A:62 | default(1) | CPU  |        |

Available settings are explained as follows:

| Item        | Description   |
|-------------|---|
| MAC Address | Enter the MAC address that will be forwarded.   |
| VLAN        | This is the VLAN group to which the MAC address belongs.                                      |
| Port        | Select the port where received frame of matched destination MAC address will be forwarded to. |
| Add         | Click it to add any port into the static MAC table.   |
| Delete      | Click it to remove the selected port from the static MAC table.                               |

## II-10-2 Dynamic Address Setting

This page allows a user to configure aging time for dynamic MAC address.

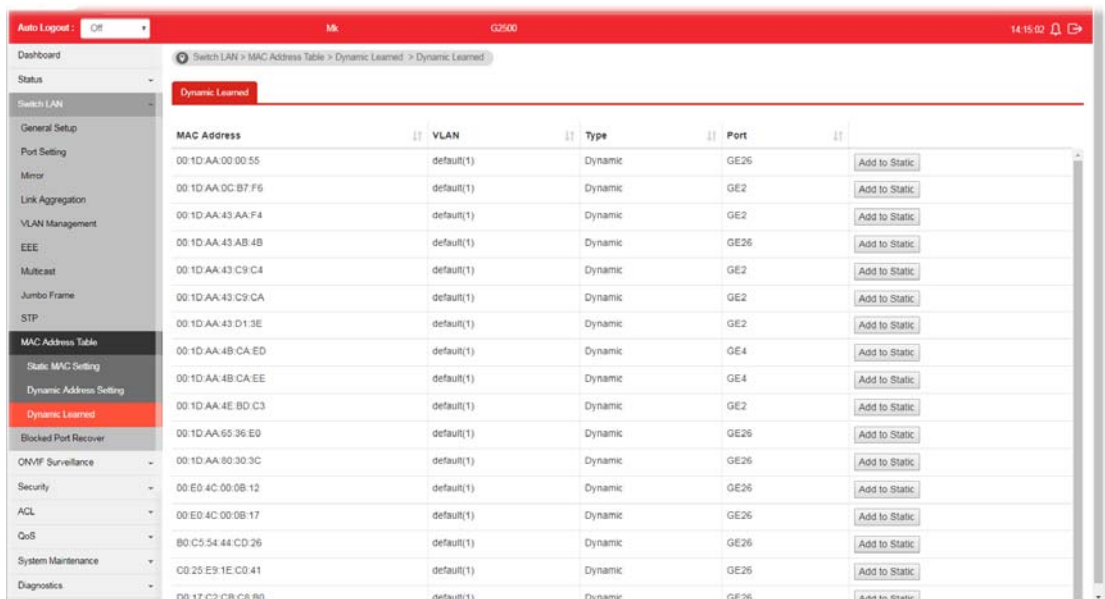


Available settings are explained as follows:

| Item       | Description  |
|------------|--|
| Aging Time | Enter the Dynamic MAC address aging out value (5-32767 seconds). |
| Apply      | Apply the settings to the switch.                                |

## II-10-3 Dynamic Learned

This page displays the MAC address and port number automatically learned by VigorSwitch.

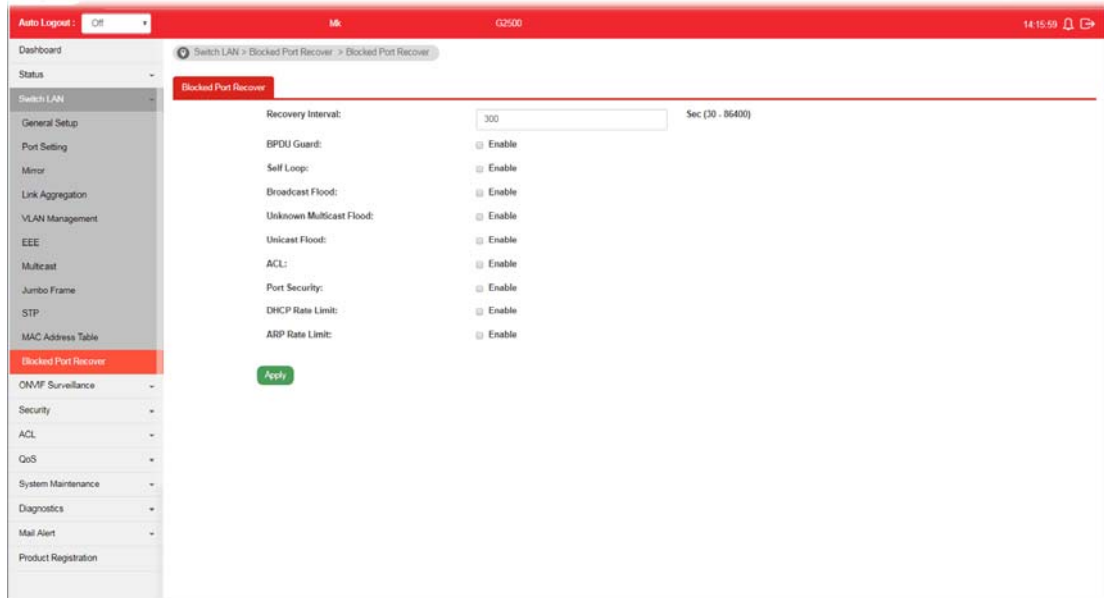


Available settings are explained as follows:

| Item          | Description   |
|---------------|---|
| MAC Address   | Display the MAC address that will be forwarded.   |
| VLAN          | Display the VLAN group to which the MAC address belongs.  |
| Type          | Display whether the MAC address is <b>Dynamic</b> (learned by the Switch) or <b>Static Unicast</b> (manually entered in the <b>Static MAC Forwarding</b> screen). |
| Port          | Display the port to which this MAC address belongs.   |
| Add to Static | Click this button to add any port into the static MAC table.  |

## II-11 Blocked Port Recover

This page is used for configuring settings to recover the port which is being blocked by the following functions after a defined period of time.



Available settings are explained as follows:

| Item                    | Description   |
|-------------------------|---|
| Recovery Interval       | The port being blocked will be able to receive and send traffic after the time period configured here.      |
| BPDU Guard              | Enable - Recover the port being blocked by BPDU Guard after the time set in Recovery Interval.              |
| Self Loop               | Enable - Recover the port being blocked by self loop Guard after the time set in Recovery Interval.         |
| Broadcast Flood         | Enable - Recover the port being blocked by broadcast flood after the time set in Recovery Interval.         |
| Unknown Multicast Flood | Enable - Recover the port being blocked by unknown multicast flood after the time set in Recovery Interval. |
| Unicast Flood           | Enable - Recover the port being blocked by unicast flood after the time set in Recovery Interval.           |
| ACL                     | Enable - Recover the port being blocked by ACL after the time set in Recovery Interval.                     |
| Port Security           | Enable - Recover the port being blocked by port security after the time set in Recovery Interval.           |
| DHCP Rate Limit         | Enable - Recover the port being blocked by DHCP rate limit after the time set in Recovery Interval.         |
| ARP Rate Limit          | Enable - Recover the port being blocked by ARP rate limit after the time set in Recovery Interval.          |
| Apply                   | Apply the settings to the switch.   |

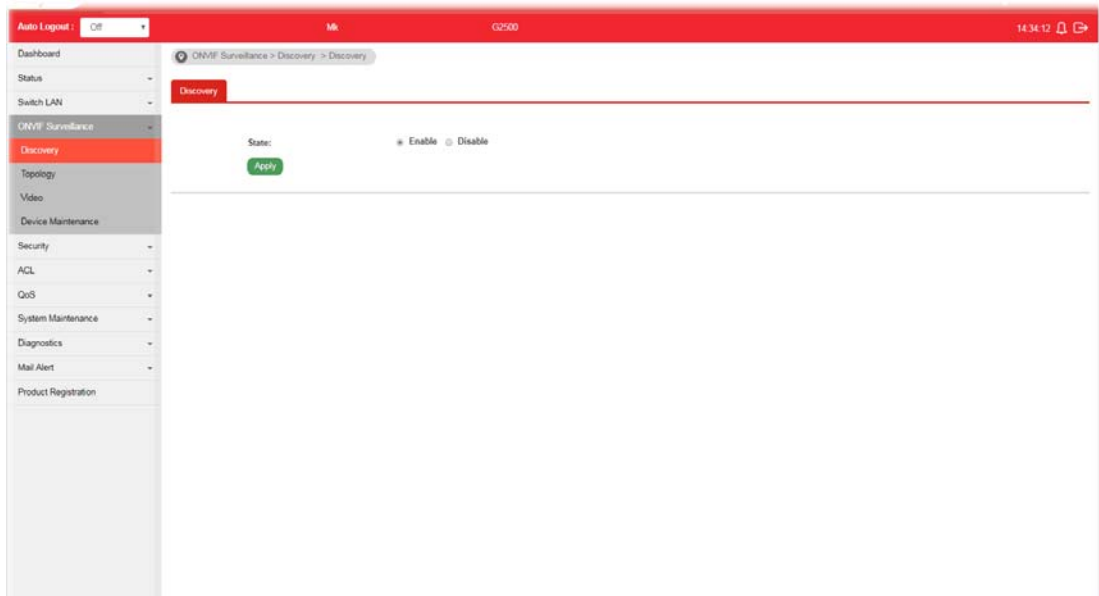
# Part III ONVIF Surveillance

## III-1 Discovery

ONVIF (Open Network Video Interface Forum), an International standard for current surveillance system industry, focuses on security products based on network IP address.

With this feature, VigorSwitch can:

- Integrate the ONVIF device and surveillance network
- Centralize management of IP video products
- Offer real-time video monitoring
- Offer remote IP video products maintenance



Available settings are explained as follows:

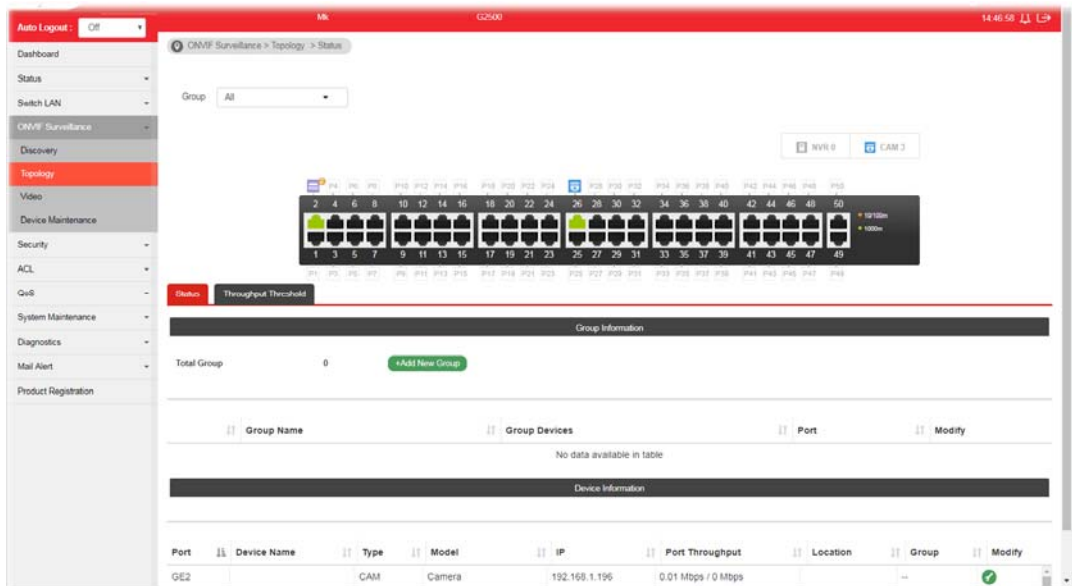
| Item  | Description  |
|-------|--|
| State | <b>Enable</b> - If enabled, VigorSwitch will automatically detect ONVIF devices, recognize third party IP cameras and NVR and integrate ONVIF device(s) to form surveillance network.<br><b>Disable</b> - Disable the function of Discovery. |
| Apply | Apply the settings to the switch.  |

## III-2 Topology

ONVIF devices can be centralized and managed remotely via VigorSwitch. With a hierarchy view, the administrator can manage several ONVIF devices and check abnormal traffic detected by Vigor system.

### III-2-1 Status

The status (including port enabled, traffic, downlink, etc.) of the IP cameras and NVRs (Network Video Recorders) can be seen on this page.



Available settings are explained as follows:

| Item                     | Description   |
|--------------------------|---|
| Group                    | Specify a group for displaying group information and device information under the selected group.<br>Or, choose the default setting, All, to display information for all groups.  |
| NVR                      | Display the number of NVR device(s) connected to VigorSwitch. The panel sketch on the screen will display which LAN port that the NVR device connected.   |
| CAM                      | Display the number of IP camera(s) connected to VigorSwitch. The panel sketch on the screen will display which LAN port that the IP camera connected.   |
| <b>Group Information</b> |   |
| Total Group              | Display the total number of groups.   |
| +Add New Group           | A group can contain one (IP camera or NVR, as group leader) to several devices (IP cameras as group devices).<br>Click the button to create a new group for managing multiple devices.<br>Step (1) - The first page allows you to configure general settings for a new group. |

- **Group Name** - Enter the name of a group.
- **All IPC Group** - Check it to group all IP cameras within the group. However, if you want to specify an NVR device as the group leader, do NOT check this box.  
Available selections of devices (IP cameras or NVR devices) will vary according to the configuration of All IPC Group. If "All IPC Group" is disabled, the system will detect the NVR devices and list them on the field of NVR. If "All IPC Group" is enabled, the system will detect the IP cameras and list them on the field of Group Leader.
- **NVR/Group Leader** - Select an IP device. For the video from IP camera will be recorded on an NVR device, it is suggested to assign an NVR as the group leader.
- **Group Device** - This field lists all devices (IP cameras) not included by other group. Simply select one IP device to multiple devices for managed by this group.
- **Next** - Click it to access into next page.

Step (2) - The second page allows you to configure throughput threshold for the group port. It is helpful for the system administrator to make the corresponding process if encountered abnormal situation.



- **Apply to All Member Ports** - Check the box to apply the throughput threshold setting to all member ports.
- **GE# Ingress Threshold Alert** - Click **Enable** to set the ingress limit value. When the incoming traffic (packet) of the GE port reaches the limit, the Vigor System will send an alert email to the system administrator.
  - **GE# Ingress Rate** - If enabling the ingress threshold alert, enter the ingress rate as a threshold to send mail alert.
- **GE# Egress Threshold Alert** - Click **Enable** to set the egress limit value. When the outgoing traffic (packet) of the GE port reaches the limit, the Vigor System will send an alert email to the system administrator.
  - **GE# Egress Rate** - If enabling the egress threshold alert, enter the egress rate as a threshold to send mail alert.
- **OK** - Save the configuration and exit the box.
- **Cancel** - Exit the box without saving the configuration.

Device Information

Modify

Click it to modify the settings of the selected IP device.

✕

### Edit Device - Camera

**Online**

**Port**

**Device Name**

**Group**

---

**Auth Username**

**Auth Password**

**Location**

Set Location

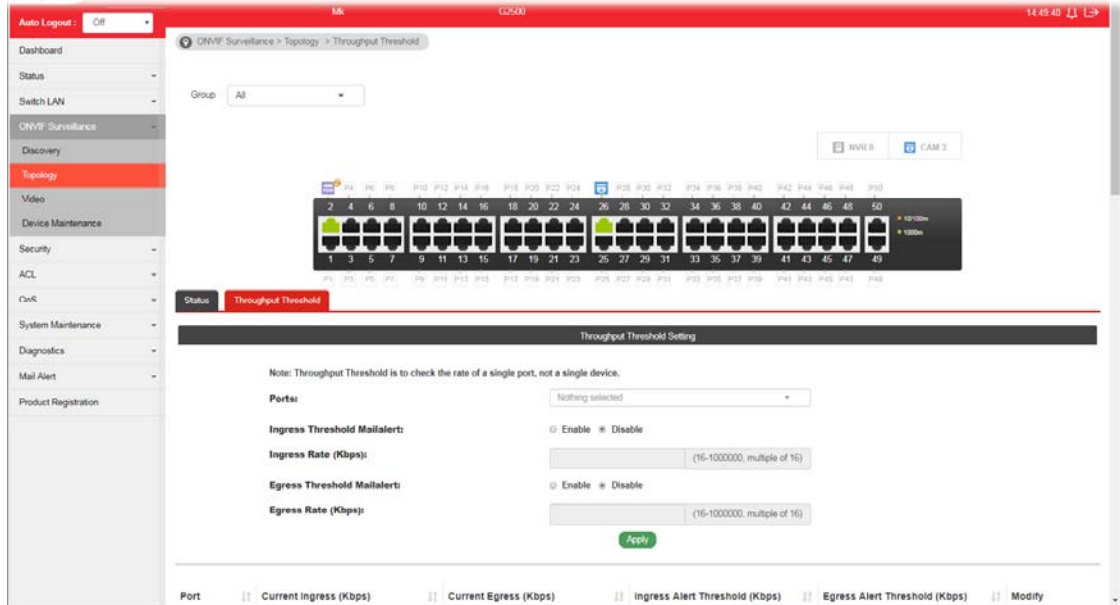
Settings may not take effect immediately

Reboot!

OK Cancel

## III-2-2 Throughput Threshold

This page is used for set throughput threshold for **multiple** ONVIF devices managed by VigorSwitch.



Available settings are explained as follows:

| Item                        | Description  |
|-----------------------------|--|
| Ports                       | Specify one to several GE ports which will be limited by the threshold configured here.  |
| Ingress Threshold Mailalert | <p><b>Enable</b> - When the ingress rate reaches the threshold configured here, Vigor system will send alert mail to specified mail address.</p> <p><b>Disable</b> - No mail alert will be sent out.</p> |
| Ingress Rate (Kbps)         | Enter a value as the threshold of ingress packets.   |
| Egress Threshold Mailalert  | <p><b>Enable</b> - When the egress rate reaches the threshold configured here, Vigor system will send alert mail to specified mail address.</p> <p><b>Disable</b> - No mail alert will be sent out.</p>  |
| Egress Rate (Kbps)          | Enter a value as the threshold of egress packets.  |
| Apply                       | Save the settings or changes to the switch.  |
| Modify                      | Click it to modify the settings for the selected GE port / LAG port.   |

✕

### Edit Port GE1

**Ingress Threshold Alert**

Enable  Disable

**Egress Threshold Alert**

Enable  Disable

**Ingress Rate (Kbps)**

16(16-1000000, multiple of 16)

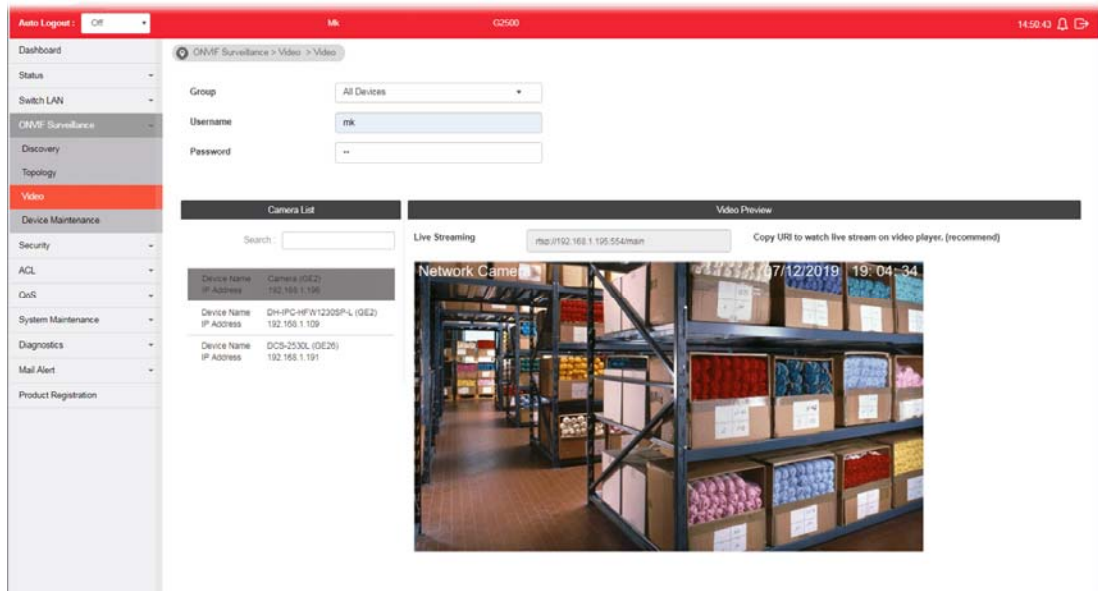
**Egress Rate (Kbps)**

16(16-1000000, multiple of 16)

OK Cancel

## III-3 Video

This page can offer a real-time video of specified IP camera for monitoring and control environments.



Available settings are explained as follows:

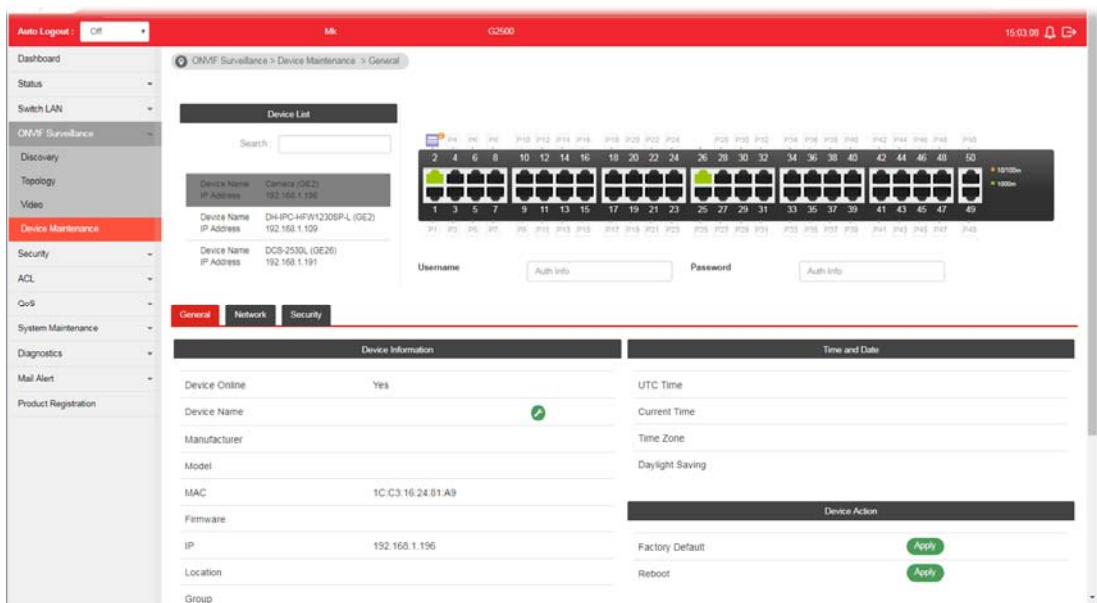
| Item          | Description   |
|---------------|---|
| Group         | Specify a group which contains the IP camera you want to check.   |
| Username      | Enter the username of the IP camera.  |
| Password      | Enter the password of the IP camera.  |
| Camera List   | <b>Search</b> - Enter the device name of the IP camera for searching and displaying on this field.  |
| Video Preview | After authenticated with correct username and password, the video of the specified IP camera (supported by VigorSwitch) will be shown immediately.<br><b>Live Streaming</b> - Display the streaming URI of the IP camera. |

## III-4 Device Maintenance


The system administrator can remotely configure time setting and reboot the devices (IP cameras or NVRs) managed by VigorSwitch.

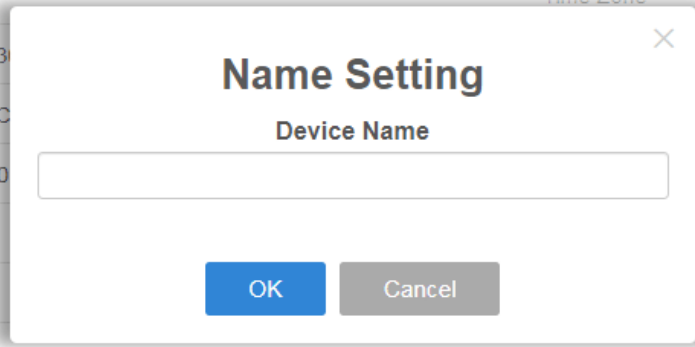

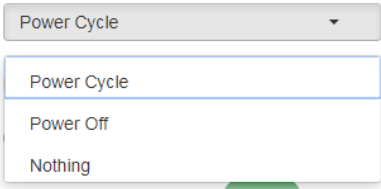
### III-4-1 General

This page displays the information (e.g., device online, device name, etc.), time and date and the device action for a selected IP device (e.g., IP camera). Meanwhile, this page allows configuring settings for ping check of IP camera or NVR.



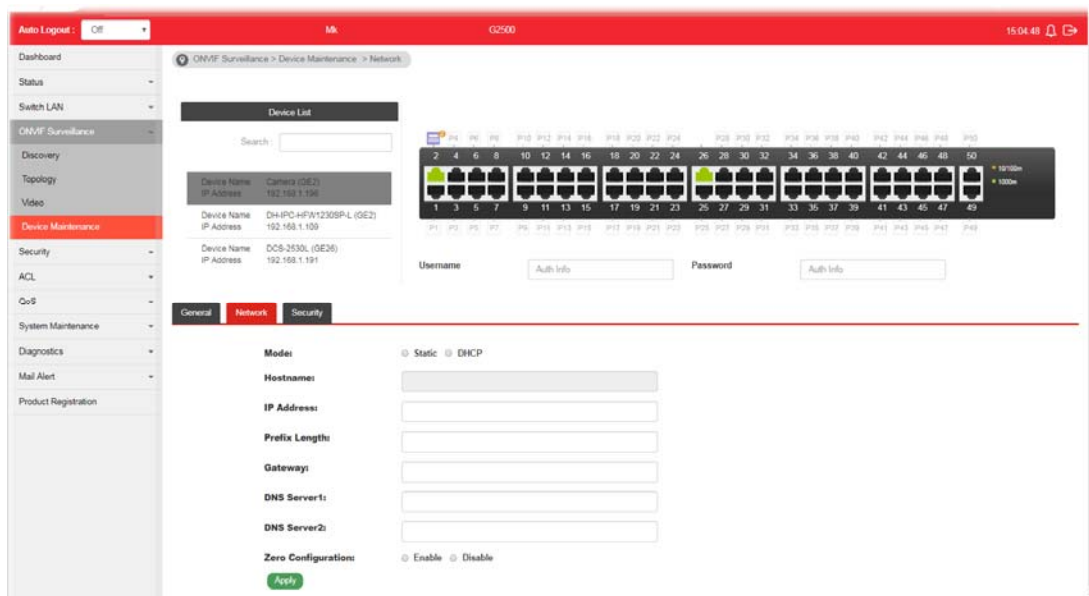
Available settings are explained as follows:

| Item               | Description  |
|--------------------|--|
| Device List        | <p><b>Search</b> - Enter a string to search the IP device you want.</p> <p><b>Username / Password</b> - Enter the username / password of the IP-based device.</p> <p>After entering the correct username and password of the IP camera, click the mouse on the device name under the Device List. Later, general information related to the IP device will be shown below.</p> |
| Device Information | <p>Display the information related to the selected device.</p> <p> - Click it to modify the device name.</p>  |

|   |  |
|---|--|
|   |  <p>The image shows a 'Name Setting' dialog box with a title bar, a close button (X), a label 'Device Name', an empty text input field, and 'OK' and 'Cancel' buttons.</p>   |
| Time and Date   | <p>Display the time and date information related to the selected device.</p> <p> - Click it to modify the time setting for the device.</p>  |
| Device Action   | <p>Display the action performed by IP-based device.</p> <p><b>Factory Default</b> - Click the <b>Apply</b> button to rest the factory default to the IP device.</p> <p><b>Reboot</b> - Click the <b>Apply</b> button to reboot the IP device immediately.</p>  |
| Device Ping Check -- Configure settings for ping check of IP camera or NVR. |  |
| Port  | Display the port number of the IP device   |
| Enable  | <p><b>Enable</b> - Click it to enable the device ping check function.</p> <p><b>Disable</b> - Click it to disable the function.</p>  |
| Ping IP Address   | <p><b>Add Device</b> - Click it to add an IP address of the device to be pinged by VigorSwitch. Up to 16 IP address(es) can be added and displayed in this field one by one (with the format of x.x.x.x, x.x.x.x, x.x.x.x...)</p> <p><b>Del Device</b> - Click it to remove the selected IP address.</p>   |
| Interval Time (sec)   | Set a time interval (15, 30, 60, 120) for ping action.   |
| Retry Time  | Choose 1, 3, or 5 for Vigor system to retry the ping action.   |
| Failure Action  | <p>Configure the power behavior for each LAN port.</p> <p><b>Power Cycle</b> - Once the device is offline, VigorSwitch will power off the device and then power on the device again.</p> <p><b>Power Off</b> - When the device is offline, power off the device immediately.</p> <p><b>Nothing</b> - When the device is offline, no action will be</p>  <p>The image shows a dropdown menu for 'Failure Action' with options: Power Cycle, Power Off, and Nothing. An 'Apply' button is visible below the menu.</p> <p><b>Note:</b> When a PoE hub connecting to LAN port of VigorSwitch, the power behavior (on/off) to the PoE hub also will apply to all the devices connecting to the PoE hub.</p> |
| Mail Alert  | <b>Enable</b> - When the device is offline, Vigor system will send an alert mail to notify the receiptant.   |
| Apply   | Save the settings or changes to the switch.  |

## III-4-2 Network

This page displays the network settings of the specified device (IP CAM or NVR).



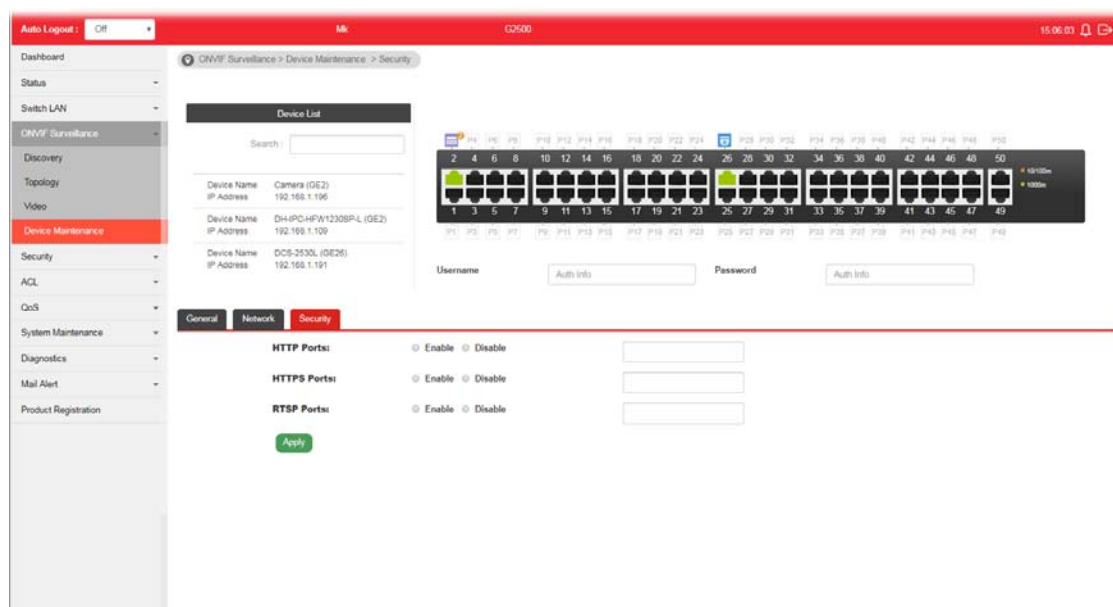
Available settings are explained as follows:

| Item               | Description   |
|--------------------|---|
| Device List        | <p><b>Search</b> - Enter a string to search the device you want.</p> <p><b>Username / Password</b> - Enter the username / password of the IP-based device. Later, current network settings related to this device will be shown on the screen.</p>  |
| Mode               | <p>Change the connection mode for this device.</p> <p><b>Static</b> - When it is selected, you have to enter value for network setting manually for the IP device.</p> <ul style="list-style-type: none"> <li>● <b>IP Address</b> - Enter an IPv4 address for the IP device.</li> <li>● <b>Prefix Length</b> - Specify the subnet mask for the IP address.</li> <li>● <b>Gateway</b> - Enter the IPv4 address for the gateway.</li> <li>● <b>DNS Server1/2</b> - Enter the IP address for primary / secondary DNS server.</li> </ul> <p><b>DHCP</b> - When it is selected, the IP device will be assigned with the settings by the network's DHCP server automatically to access the Internet.</p> <ul style="list-style-type: none"> <li>● <b>Hostname</b> - Display the hostname of the DHCP server.</li> </ul> |
| Zero Configuration | <p><b>Enable</b> - The network settings for the IP device will be configured automatically.</p> <p><b>Disable</b> - The network settings for the IP devcie must be configured manually.</p>   |
| Apply              | Save the settings or changes to the switch.   |



### III-4-3 Security

This page displays the security settings of the specified IP device (IP CAM or NVR).



Available settings are explained as follows:

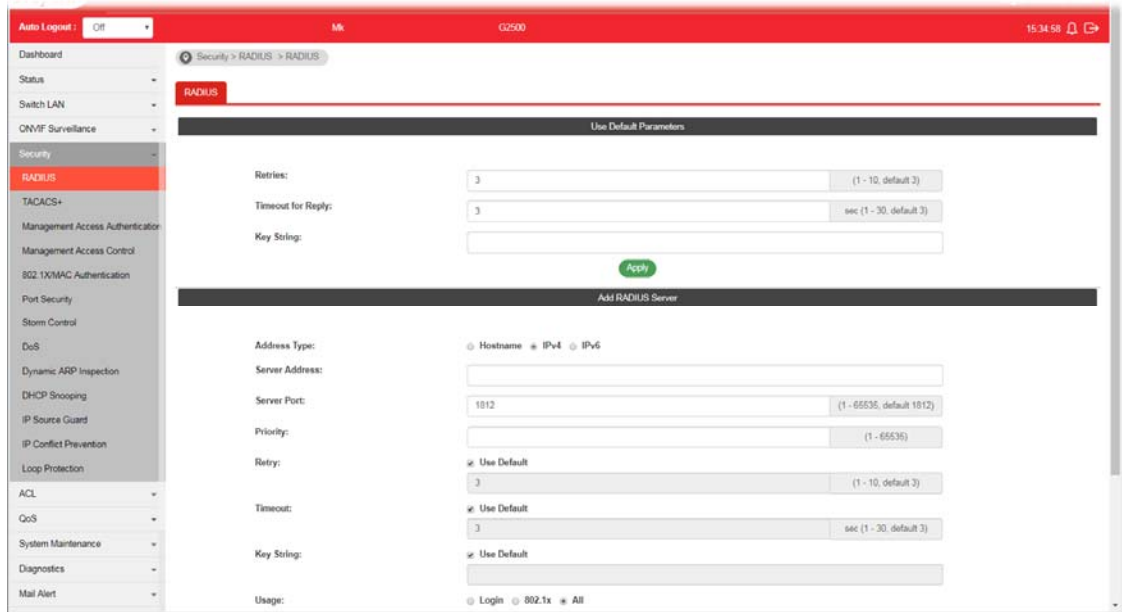
| Item        | Description   |
|-------------|---|
| Device List | <b>Search</b> - Enter a string to search the device you want.<br><b>Username / Password</b> - Enter the username / password of the IP-based device. Later, current network settings related to this device will be shown on the screen. |
| HTTP Ports  | Current HTTP port number of the IP device is shown in this field.<br><b>Enable</b> - Click it to enable the HTTP port configuration and enter a port value if required.<br><b>Disable</b> - Disable the HTTP port configuration.        |
| HTTPS Ports | Current HTTPS port number of the IP device is shown in this field.<br><b>Enable</b> - Click it to enable the HTTPS port configuration and enter a port value if required.<br><b>Disable</b> - Disable the HTTPS port configuration.     |
| RTSP Ports  | Current RTSP port number of the IP device is shown in this field.<br><b>Enable</b> - Click it to enable the RTSP port configuration and enter a port value if required.<br><b>Disable</b> - Disable the RTSP port configuration.        |
| Apply       | Save the settings or changes to the switch.   |

This page is left blank.

# Part IV Security


# IV-1 RADIUS

This page allows the network administrator to add and configure multiple RADIUS servers.



Available settings are explained as follows:


| Item                   | Description  |
|------------------------|--|
| Use Default Parameters | <ul style="list-style-type: none"> <li>● <b>Retries</b> - The retry time before this server being considered not-reachable.</li> <li>● <b>Timeout for Reply</b> - Set the time (in seconds) before this server being considered lost connection.</li> <li>● <b>Key String</b> - Enter the string used to encrypt and authenticate with RADIUS server.</li> <li>● <b>Apply</b> - Save the settings.</li> </ul>  |
| Add RADIUS Server      | <ul style="list-style-type: none"> <li>● <b>Address Type</b> - Specify whether switch uses a hostname to resolve address by DNS to connect to server, or directly connect using IPv4 address.</li> <li>● <b>Sever Address</b> - Enter the server’s address corresponding with address type given.</li> <li>● <b>Server Port</b> - Enter the port number used by RADIUS server.</li> <li>● <b>Priority</b> - Specify the priority that switch uses this server. The higher number, the lower priority. Switch will start with server with lowest priority.</li> <li>● <b>Retry</b> - Set the time before this server being considered not-reachable</li> <li>● <b>Timeout</b> - Set the time (in seconds) before this server being considered lost connection.</li> <li>● <b>Key String</b> - Enter the key string used for encrypting and authenticating with server. Unless Key String is specified here, the default string will be used.</li> <li>● <b>Usage</b> -Specify whether you would like to use this server for switch login authentication or 802.1x access port authentication, or both.</li> </ul> |

- 
- **Add** - Click it to add a new RADIUS server and display in this page.
-  **Edit** - Click it to modify the priority setting for the selected GE port / LAG port.
-

## IV-2 TACACS+

This page allows the network administrator to add and configure multiple TACACS+ server.

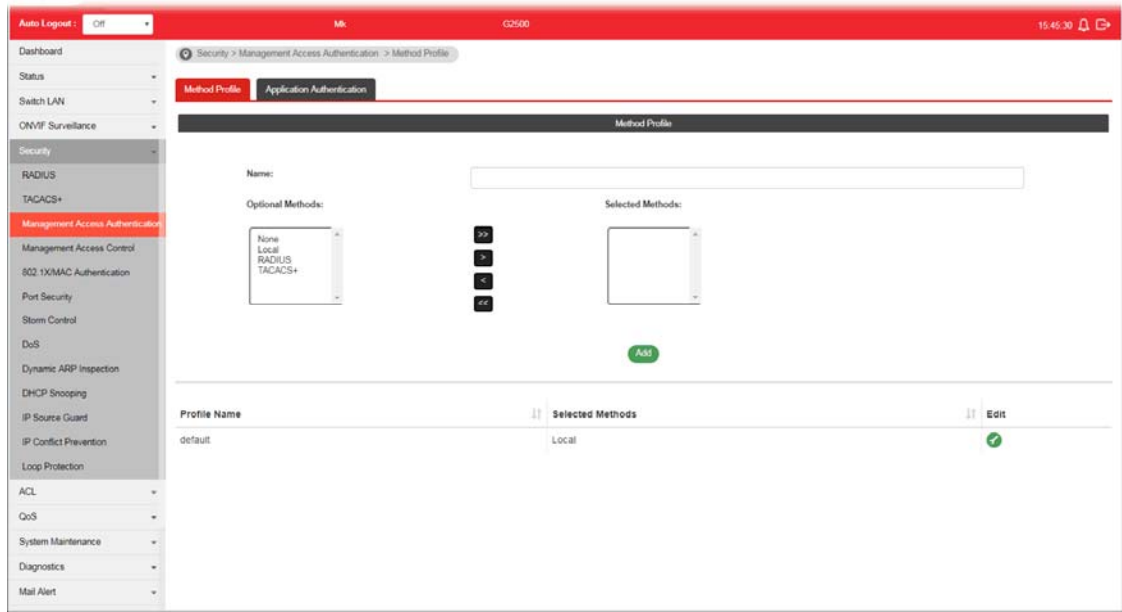
Available settings are explained as follows:

| Item                   | Description   |
|------------------------|---|
| Use Default Parameters | <ul style="list-style-type: none"> <li>● <b>Timeout</b> -Set the time (in seconds) before this server being considered lost connection.</li> <li>● <b>Key String</b> - Enter the string used to encrypt and authenticate with TACACS+ server.</li> <li>● <b>Apply</b> - Save the settings.</li> </ul>   |
| Add TACACS+ Server     | <ul style="list-style-type: none"> <li>● <b>Address Type</b> - Specify whether switch use a hostname to resolve address by DNS to connect to server, or directly connect using IPv4 address.</li> <li>● <b>Sever Address</b> - Enter the server's address corresponding with address type given.</li> <li>● <b>Server Port</b> - Enter the port number used by TACACS+ server.</li> <li>● <b>Priority</b> - Specify the priority that switch uses this server. The higher number, the lower priority. Switch will start with server with lowest priority.</li> <li>● <b>Timeout</b> -Set the time (in seconds) before this server being considered lost connection.</li> <li>● <b>Key String</b> - Enter the key string used for encrypting and authenticating with server. Unless Key String is specified here, the default string will be used.</li> <li>● <b>Add</b> - Click it to add a new RADIUS server and display in this page.</li> <li>●  under <b>Edit</b>- Click it to modify the priority setting for the selected GE port / LAG port.</li> </ul> |


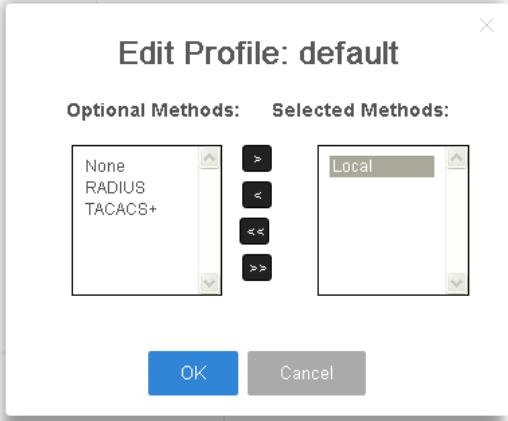
# IV-3 Management Access Authentication

## IV-3-1 Method Profile

This page allows a user to create method list for applying on management service.

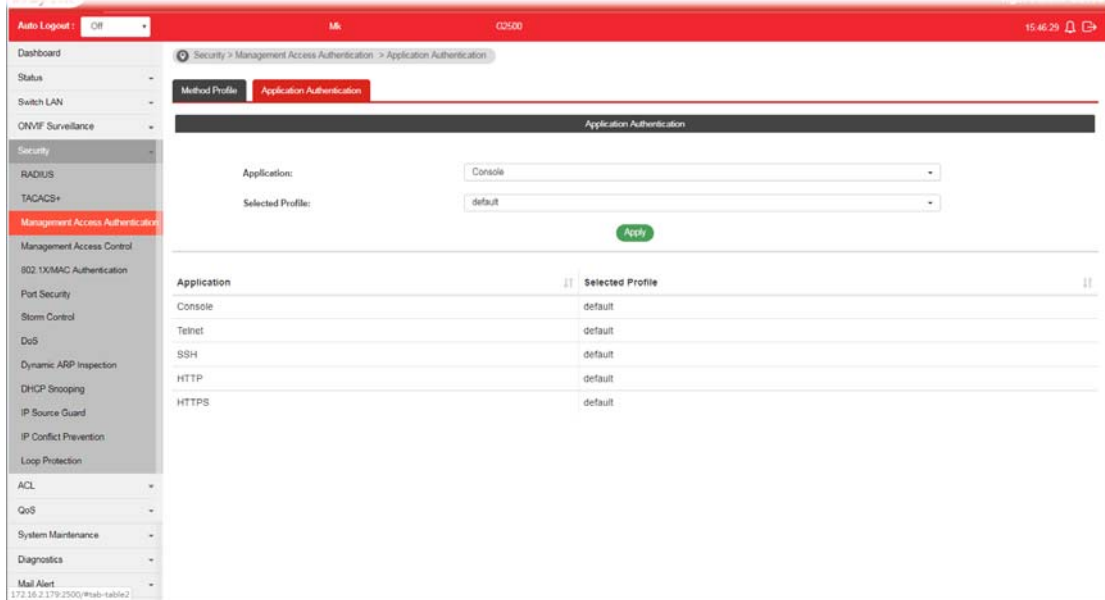


Available settings are explained as follows:

| Item   | Description   |
|--|---|
| Method Profile   | <ul style="list-style-type: none"> <li>● <b>Name</b> - Enter a name for creating a method.</li> <li>● <b>Optional Methods</b> - Available methods include Local, RADIUS and TACACS+.</li> <li>● <b>Selected Methods</b> - The method listed in this field will be applied for such method profile.</li> <li>● <b>Add</b> - Click it to add a method from Optional Method onto Selected Method.</li> </ul> |
|  under Edit | <p>Click it to modify the optional methods/selected methods for the selected profile.</p>   |

## IV-3-2 Application Authentication

This page allows the network administrator to select the customized Method List to apply to any management service, for management access control.



Available settings are explained as follows:

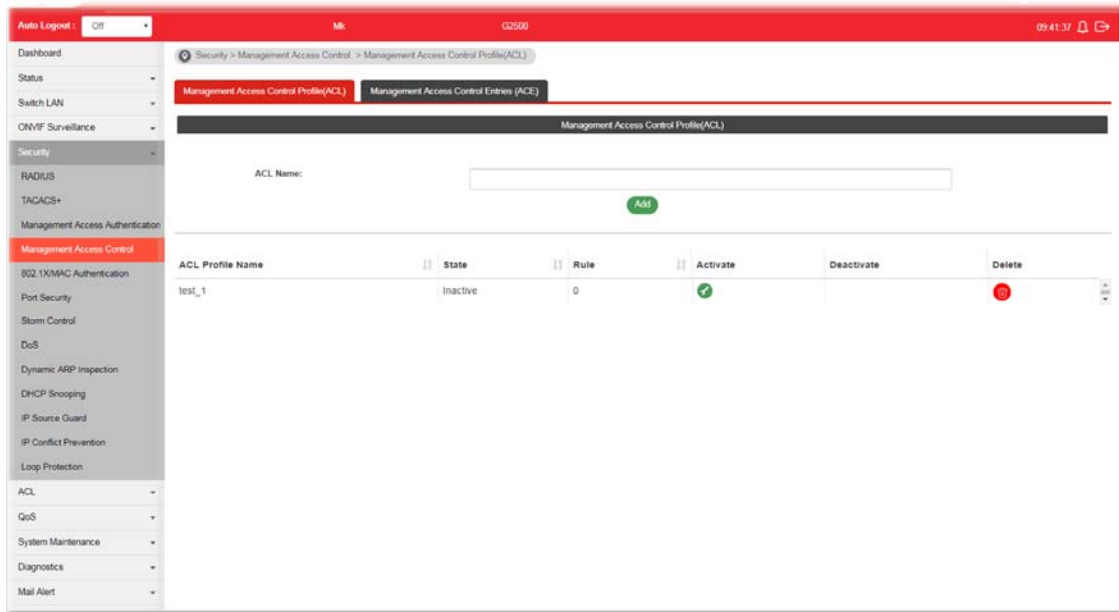
| Item             | Description  |
|------------------|--|
| Application      | There are five methods to be configured with different profile respectively. <ul style="list-style-type: none"> <li>● Console/Telnet/SSH/HTTP/HTTPS</li> </ul> |
| Selected Profile | Specify one of customized method profiles to apply to any management service, for management access control.   |
| Apply            | Save the settings.   |




## IV-4 Management Access Control

### IV-4-1 Management Access Control Profile (ACL)

This page allows a user to add, edit, and delete Management Access Control profiles.



Available settings are explained as follows:

| Item                  | Description   |
|-----------------------|---|
| ACL Name              | Enter a name to create a profile for ACL.<br>Once a profile is created, it will be displayed on this page.  |
| Add                   | Click it to create a new ACL profile after entering the ACL name.   |
| ACL Profile Name      | Display the name of the ACL profile.  |
| State                 | Display if such ACL profile is active or inactive.  |
| Rule                  | Display the number of ACE used by this ACL profile.   |
| Activate / Deactivate |  - Click it to activate / deactivate such entry.<br>To configure detailed settings for the selected ACL profile, do not click Activate for that profile. |
| Delete                | Click the icon under Delete to remove the selected entry.   |

## IV-4-2 Management Access Control Entries (ACE)

This page allows a user to add, edit, or remove Access Control Entries (ACE) of the Management Access Control profiles. However, only the ACE of inactive profiles can be modified, and before configuring ACE, at least one ACL profile should be created.

Available settings are explained as follows:

| Item             | Description   |
|------------------|---|
| ACL Profile Name | Use the drop-down list to select the inactive ACL profile you would like to modify.   |
| Priority         | Specify a priority number (1 to 65535) for such rule. The lower the number, the higher the priority.  |
| Service          | Choose the service type you would like to control the access.   |
| Action           | Select the action to be taken on the traffic of selected service type. <ul style="list-style-type: none"> <li>● Deny - Incoming / outgoing data which meets ACE rules will be blocked.</li> <li>● Permit - Incoming / outgoing data which meets ACE rule is allowed to pass through.</li> </ul> |
| Ports            | Select the ports to which the ACL should be applied.  |
| IP Versions      | Specify the IP address/subnet to which the ACL should be applied. <ul style="list-style-type: none"> <li>● All - All the IP address should be applied.</li> <li>● IPv4 - Specify the IPv4 address /subnet.</li> <li>● IPv6 -Specify the IPv6 address /subnet.</li> </ul>                        |
| IPv4             | Enter the IPv4 address/subnet to which the ACE rule should apply.   |
| IPv6             | Enter the IPv6 address/subnet to which the ACE rule should apply.   |
| Add              | Click it to create an ACE rule profile. Then, such ACE rule profile will be shown on the table below.   |

Edit



- click it to modify the settings for the selected entry.

✕

### Edit ACE with ACL profile=sdf and Priority=1

Service:

Action:

Ports:

IP Versions:  All  IPv4  IPv6

IPv4:  /

IPv6:  /



- click it to remove the selected entry.

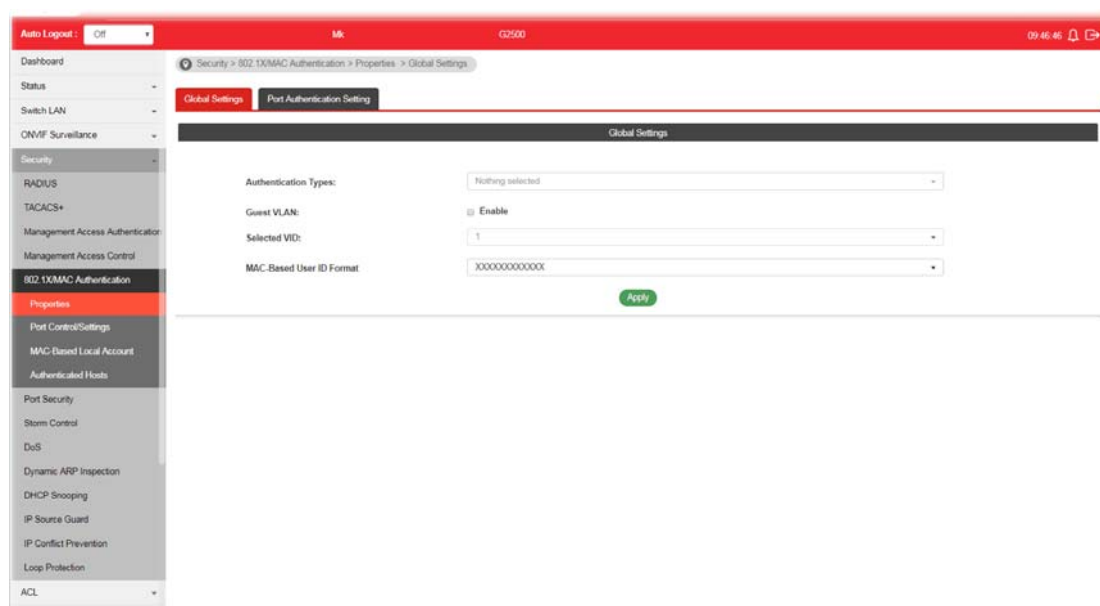
## IV-5 802.1X/MAC Authentication

The authentication manager allows you to configure securely access from any host connected to physical ports. You may apply multiple ways of authentication to each port.

### IV-5-1 Properties

#### IV-5-1-1 Global Settings

VigorSwitch G2500 supports 802.1x and MAC-based authentication methods. In Global Settings page, you can specify authentication type, enable Guest VLAN function, specify a VID and select format for MAC address entry.

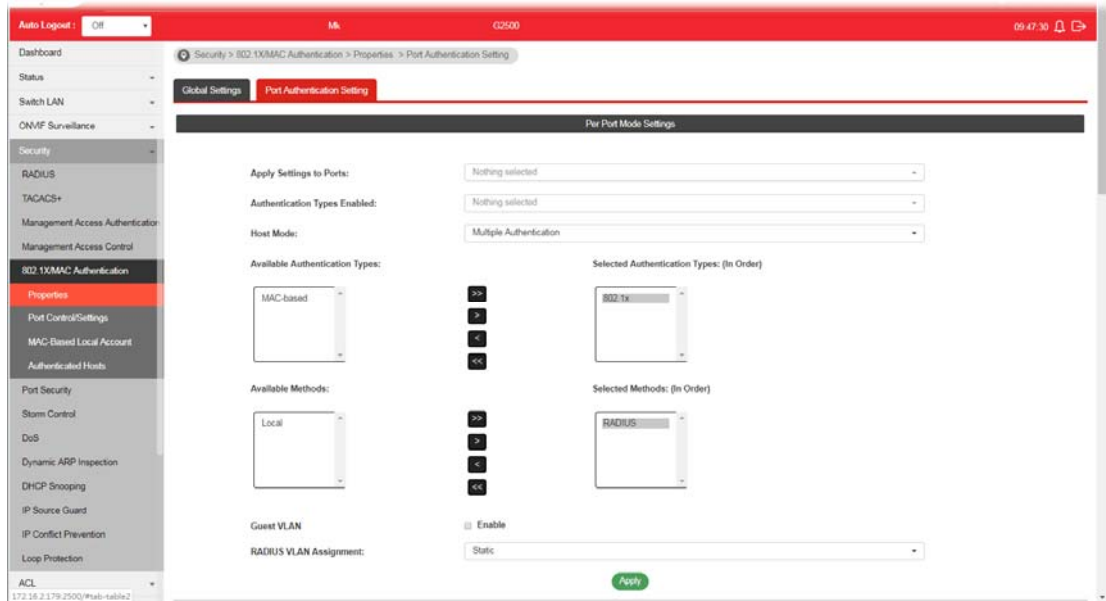


Available settings are explained as follows:

| Item                     | Description   |
|--------------------------|---|
| Authentication Types     | Use the drop down list to specify which type (802.1x, MAC-based) will be used for authentication. Choose to enable 802.1x or MAC-based authenticate method for host connecting to Ethernet port. You may configure which type to be used per port, but enabling any per port without enabling here will not be effective. |
| Guest VLAN               | Check to enable a Guest VLAN for those have not successfully authenticated with any given methods. Choose one of the VLAN ID as a Guest VLAN.   |
| Selected VID             | If Guest VLAN is enabled, use the drop down list to specify one VID number.   |
| MAC-Based User ID Format | Specify how the MAC-based user ID should be expressed in EAP message between AAA server and switch.   |
| Apply                    | Save and activate the settings configured above.  |

## IV-5-1-2 Port Authentication Setting

This page allows the network administrator to configure detailed authentication settings for each port.



Available settings are explained as follows:

| Item                           | Description   |
|--------------------------------|---|
| Apply Settings to Ports        | Select physical port(s) for applying settings.<br>Note that port authentication will not be effective if none of them were enabled.   |
| Authentication Types Enabled   | Select 802.1x and/or MAC-based authenticate method for host connecting to this port.  |
| Host Mode                      | <ul style="list-style-type: none"> <li>● <b>Multiple Authentication</b> - Each host are authenticated individually.</li> <li>● <b>Multiple Hosts</b> - Authentication is done on port basis, only one authenticated host is required; other hosts connected to this port can access freely as authenticated host.</li> <li>● <b>Single Host</b> - Only one host can be authenticated, and access the port.</li> </ul> |
| Available Authentication Types | Display available authentication types of AAA server (or local) you wish to have on this port.  |
| Selected Authentication Types  | Specify the order of authentication type you wish to have on this port.   |
| Available Methods              | Display available methods of AAA server (or local) you wish to have on this port.   |
| Selected Methods               | Specify the order of authentication methods you wish to have on this port.  |
| Guest VLAN                     | Check <b>Enable</b> to enable Guest VLAN on this port for those didn't authenticated successfully.  |
| RADIUS VLAN Assignment         | <ul style="list-style-type: none"> <li>● <b>Disable</b> - Switch will ignore the VLAN assignment from the RADIUS server and keep the original VLAN of the host.</li> <li>● <b>Static</b> - Switch will use the VLAN assignment from the</li> </ul>  |

|              |  |
|--------------|--|
|              | <p>RADIUS server if it receives the information. If there is not VLAN information, it will keep the original VLAN of the host.</p> <ul style="list-style-type: none"> <li>● <b>Reject</b> - Switch will reject the host if it does not receive the VLAN information from RADIUS server.</li> </ul> |
| <b>Apply</b> | The modification made above can be applied on to the selected GE port immediately.   |

## IV-5-2 Port Control/Settings

This page allows the network administrator to controls port setting, based on 802.1X, for ethernet port authentication.

| Port | Port Control | Reauthenticat... | Max Hosts | Reauthenticat... | Inactive | Quiet | Resend EAP ... | Supplicant TL... | Server Timeo... | Max EAP Req... |
|------|--------------|------------------|-----------|------------------|----------|-------|----------------|------------------|-----------------|----------------|
| GE1  | Disabled     | Disabled         | 256       | 3600             | 60       | 60    | 30             | 30               | 30              | 2              |
| GE2  | Disabled     | Disabled         | 256       | 3600             | 60       | 60    | 30             | 30               | 30              | 2              |

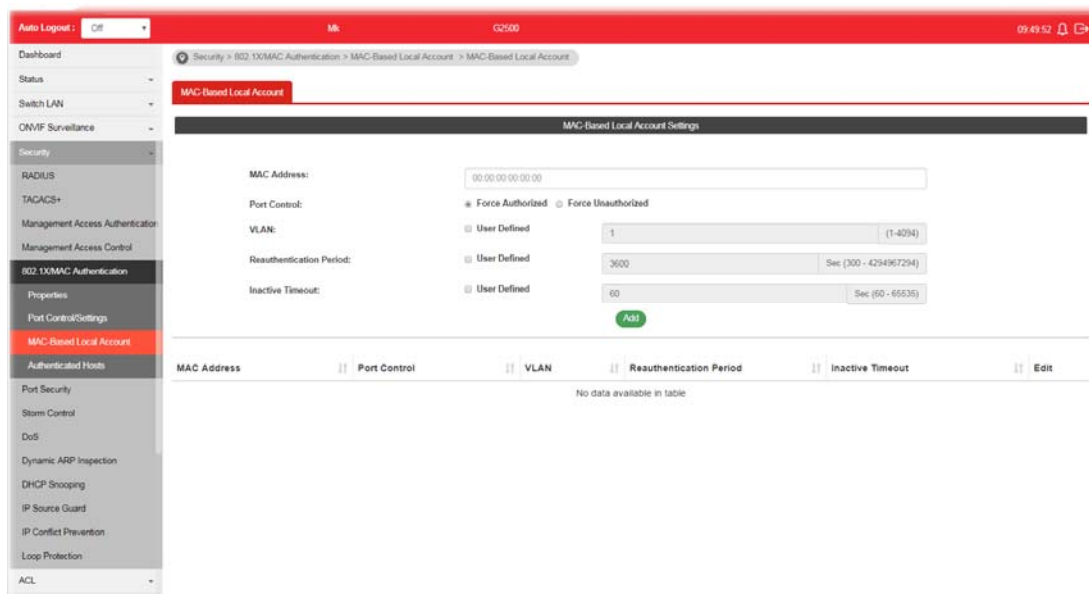
Available settings are explained as follows:

| Item                             | Description   |
|----------------------------------|---|
| <b>Ports</b>                     | Select the ports to modify the port control settings.   |
| <b>Port Control</b>              | <p>Specify if you wish this account to be allowed (Authorized) or blocked (Unauthorized) or determined by VigorSwitch (Auto).</p> <ul style="list-style-type: none"> <li>● <b>Disabled</b> - Disable any authentication requirement for port access. All clients are allowed to access the network.</li> <li>● <b>Force Authorized</b>- Port will be considered authorized. All clients are allowed to access the network.</li> <li>● <b>Force Unauthorized</b> - Port will be considered un-authorized. All clients are NOT allowed to access the network.</li> <li>● <b>Auto</b> - Port will be considered authorized or unauthorized based on the authentication results of the host.</li> </ul> |
| <b>Periodic Reauthentication</b> | <b>Enable</b> - The hosts via the selected GE port will be re-authenticated periodically.   |


|   |  |
|---|--|
| <b>Max Hosts</b>                            | If Multiple Authentication mode is selected as Host Mode (802.1X/MAC Authentication>>Properties>>Port Authentication Setting), the total number of hosts cannot exceed the maximum number of hosts configured here.  |
| <b>Reauthentication Period</b>              | Enter a time period. When the time is up, the host shall return to initial state and prepare to pass authentication procedure again. Default is 3600 seconds.  |
| <b>Inactivate Timeout</b>                   | When there is no packet coming from the authenticated host, the system will start the inactive timer. After inactive timeout, the host will be unauthorized and corresponding session will be deleted. In Multiple Hosts mode (configured in 802.1X/MAC Authentication>>Properties>>Port Authentication Setting), the packet is counted on the authorized host only and not all packets on the port. |
| <b>Quiet Period</b>                         | When a GE port is disabled just because authentication fails several times, the host connected to that port will be blocked for a period of time configured in quiet period.<br>Later, after the time period set in this field, the host will be allowed to perform authentication again.  |
| <b>Resend EAP Period (802.1X Parameter)</b> | Set the period for host to re-send EAP (Ethernet Automatic Protection) requests.<br>Default value is 30 (seconds).   |
| <b>Supplicant Timeout(802.1X Parameter)</b> | Set a period of time for the maximum number of EAP requests will be sent.<br>If a response from the host is not received by VigorSwitch after the defined period (supplicant timeout), the authentication process will be started again.   |
| <b>Server Timeout (802.1X Parameter)</b>    | Set a period of time for the server. The EAP requests shall be resent to the supplicant within the time; otherwise, the time setting will lapse and the requests won't be sent out.  |
| <b>Max EAP Request (802.1X Parameter)</b>   | Set the maximum time interval for EAP request sent out.  |
| <b>Apply</b>                                | The modification made above can be applied on to the selected GE port immediately.   |

## IV -5-3 MAC-Based Local Account

This page allows the network administrator to create profiles by entering MAC address of the hosts to be authenticated.



Available settings are explained as follows:

| Item                    | Description  |
|-------------------------|--|
| MAC Address             | Enter the MAC address of the host.   |
| Port Control            | Specify a control type for the host. <ul style="list-style-type: none"> <li>● Force Authorized - Click it to forcefully authenticate the host specified above.</li> <li>● Force Unauthorized - The host specified above will not be authenticated by VigorSwitch.</li> </ul> |
| VLAN                    | User Defined - Check it to specify which VLAN will be assigned by the host of this account.  |
| Reauthentication Period | User Defined - Check it to specify the time this account required to be authenticated again after authentication taken place.  |
| Inactive Timeout        | User Defined - Check it to specify the time of inactive this account becoming log-off.   |
| Add                     | Click it to create a new account.  |
| Edit                    | It is available when there is one profile existed. <ul style="list-style-type: none"> <li> - Click it to modify the settings for the selected entry.</li> </ul>                           |



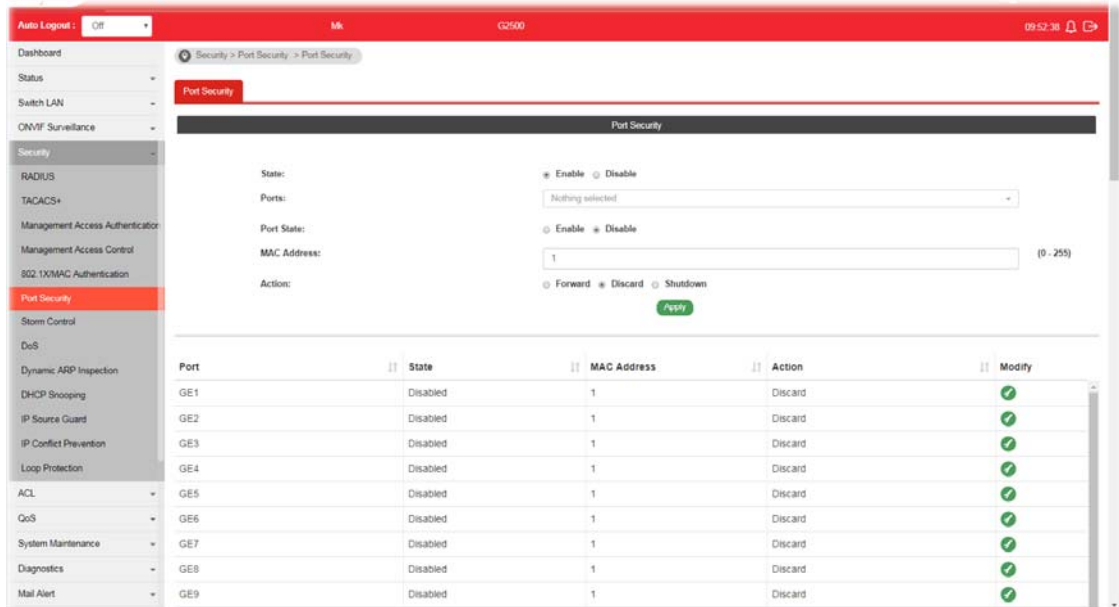
## IV-5-4 Authenticated Hosts

This page displays information related to the host authenticated by VigorSwitch.

The screenshot shows the VigorSwitch web interface. The top navigation bar is red and contains 'Auto Logout: Off', 'Mk', 'G2500', and a clock showing '09:59:43'. The left sidebar is a grey menu with various security options. The main content area has a red header 'Authenticated Hosts' and a breadcrumb trail: 'Security > 802.1X/MAC Authentication > Authenticated Hosts > Authenticated Hosts'. Below this is a table with the following columns: 'Session ID', 'Port', 'MAC Address', 'Current Type', 'Status', 'Operational V...', 'Operational S...', 'Operational L...', 'Operational ...', 'Authorized V...', and 'Authorized R...'. The table is currently empty, displaying the message 'No data available in table'.

## IV-6 Port Security

This page allows the network administrator to configure security settings for each port interface (GE port /LAG group). When port security is enabled for each interface, related action will be performed once detecting that the number of MAC address exceeds the limit.



Available settings are explained as follows:

| Item        | Description  |
|-------------|--|
| State       | Enable or disable port security function on the switch. <ul style="list-style-type: none"> <li>● <b>Enabled</b> - Enable the port security function.</li> <li>● <b>Disabled</b> - Disable the port security function.</li> </ul>   |
| Ports       | Select the port(s) you would like to configure the port security settings.   |
| Port State  | Enable or disable port security function on the ports selected above. <ul style="list-style-type: none"> <li>● <b>Enabled</b> - The selected port applies the port security settings.</li> <li>● <b>Disabled</b> - The selected port does not apply the port security settings.</li> </ul>   |
| MAC Address | Enter the maximum number of MAC addresses that the port is allowed to learn.   |
| Action      | Select an action to perform when there is an unknown MAC address on the port. <ul style="list-style-type: none"> <li>● <b>Forward</b>- Forward a packet whose source MAC is unknown to the switch.</li> <li>● <b>Discard</b>- Discard a packet whose source MAC is unknown to the switch.</li> <li>● <b>Shutdown</b>- Shutdown this port when a packet with unknown source MAC is received.</li> </ul> |
| Apply       | The modification made above can be applied on to the selected GE/LAG port immediately.   |

Edit



- click it to modify the settings for the selected entry.

### Edit Port GE1

**Port State**

Enabled  Disabled

**MAC Address**

1 (0 - 255)

**Action**

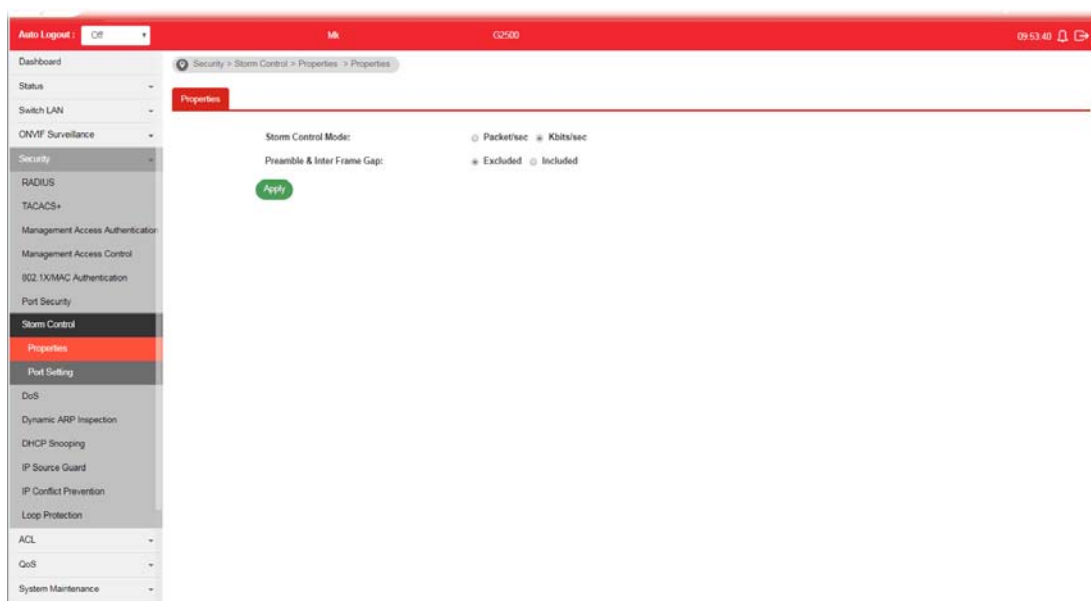
Forward  Discard  Shutdown

## IV-7 Storm Control

Storm Control helps to suppress possible broadcast, unknown multicast or unknown unicast storm by applying a rate limit on those packets.

### IV-7-1 Properties

This page allows a user to configure general settings for Storm Control.

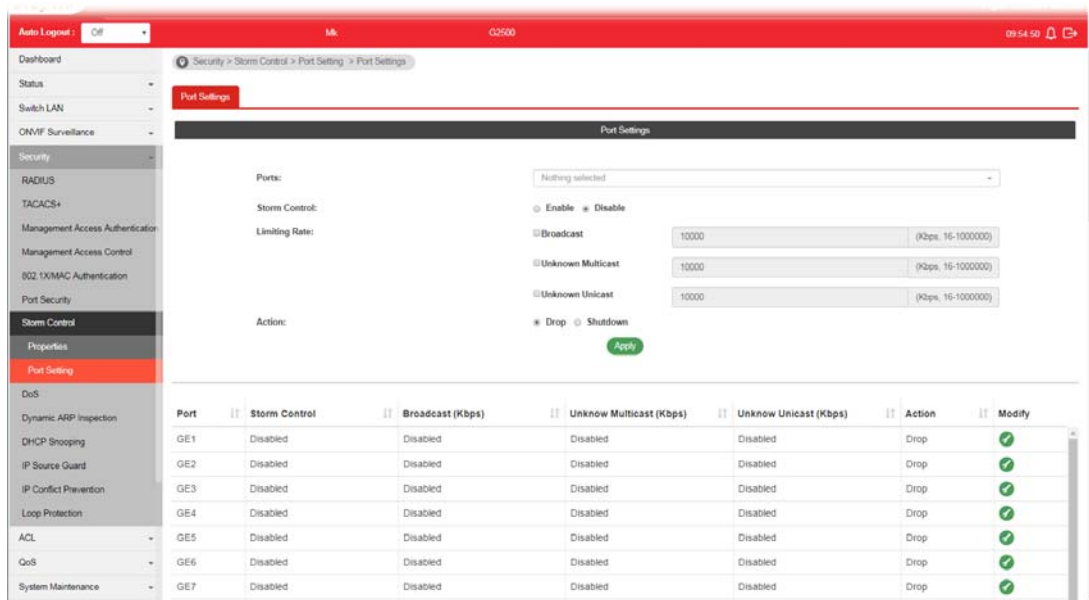


Available settings are explained as follows:

| Item                       | Description   |
|----------------------------|---|
| Storm Control Mode         | Select the mode of storm control. <ul style="list-style-type: none"><li>● <b>Packet/sec</b> - Storm control rate will be calculated by packet-based.</li><li>● <b>Kbits/sec</b> - Storm control rate will be calculated by octet-based.</li></ul>   |
| Preamble & Inter Frame Gap | Select the rate calculation with/without preamble & IFG (20 bytes). <ul style="list-style-type: none"><li>● <b>Excluded</b> - Exclude preamble &amp; IFG (20 bytes) when count ingress storm control rate.</li><li>● <b>Included</b> - Include preamble &amp; IFG (20 bytes) when count ingress storm control rate.</li></ul> |
| Apply                      | Apply the settings to the switch.   |

## IV-7-2 Port Setting

This page allows the network administrator to configure port settings for Storm Control. The configuration result for each port will be displayed on the table listed on the lower side of this web page.



Available settings are explained as follows:

| Item          | Description   |
|---------------|---|
| Ports         | Use the drop down list to select the port profile (GE1 to GE28).  |
| Storm Control | <ul style="list-style-type: none"> <li>● <b>Disable</b> - Disable the storm control configuration for the selected port profile.</li> <li>● <b>Enable</b> - Enable the storm control configuration for the selected port profile.</li> </ul>  |
| Limiting Rate | <p>Check the box(es) to enable storm control rate limited for Broadcast, Unknown Multicast and/or Unknow Unicast packet.</p> <ul style="list-style-type: none"> <li>● <b>Broadcast</b> - Specify the storm control rate for Broadcast packet. Value of storm control rate, Unit: Kbps (Kbits per-second). The range is from 16 to 1000000.</li> <li>● <b>Unknown Multicast</b> - Specify the storm control rate for unknown multicast packet. Value of storm control rate, Unit: Kbps (Kbits per-second). The range is from 16 to 1000000.</li> <li>● <b>Unknown Unicast</b> - Specify the storm control rate for unknown multicast packet. Value of storm control rate, Unit: Kbps (Kbits per-second). The range is from 16 to 1000000.</li> </ul> |
| Action        | <p>Select the state of setting.</p> <ul style="list-style-type: none"> <li>● <b>Drop</b> - Packets exceed storm control rate will be dropped.</li> <li>● <b>Shutdown</b> - Port exceeds storm control rate will be shutdown.</li> </ul>   |
| Apply         | Apply the settings to the switch.   |

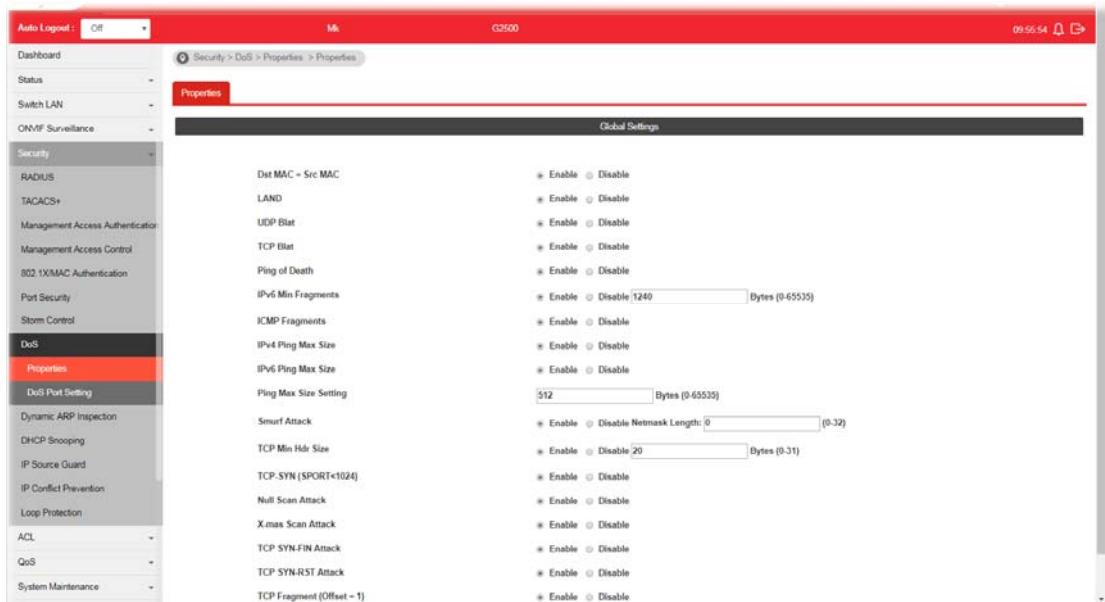
## IV-8 DoS

A Denial of Service (DoS) attack is a hacker attempt to make a device unavailable to its users. DoS attacks saturate the device with external communication requests, so that it cannot respond to legitimate traffic. These attacks usually lead to a device CPU overload.

The DoS protection feature is a set of predefined rules that protect the network from malicious attacks. The DoS Security Suite Setting enables activating the security suite.

### IV-8-1 Properties

This page allows a user to configure DoS setting to enable/disable DoS function for global setting.



Available settings are explained as follows:

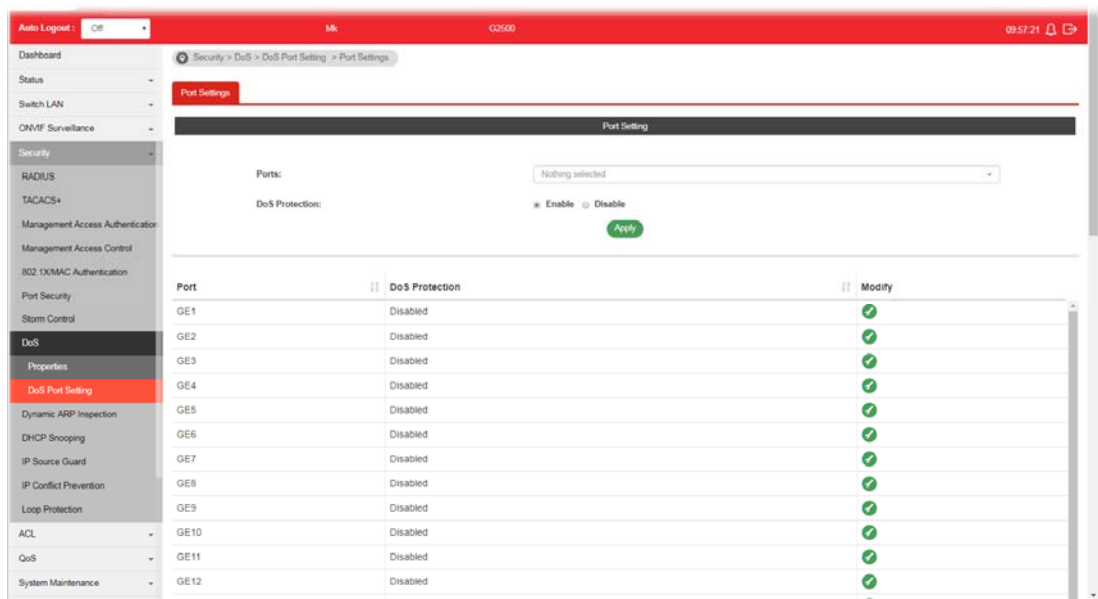
| Item            | Description  |
|-----------------|--|
| Dst MAC=Src MAC | Drop the packets if the destination MAC address is equal to the source MAC address. <ul style="list-style-type: none"> <li>● Disabled - Disable the item function.</li> <li>● Enabled - Enable the item function.</li> </ul> |
| LAND            | Drop the packets if the source IP address is equal to the destination IP address. <ul style="list-style-type: none"> <li>● Disabled - Disable the item function.</li> <li>● Enabled - Enable the item function.</li> </ul>   |
| UDP Blat        | Drop the packets if the UDP source port equals to the UDP destination port. <ul style="list-style-type: none"> <li>● Disabled - Disable the item function.</li> <li>● Enabled - Enable the item function.</li> </ul>         |
| TCP Blat        | Drop the packages if the TCP source port is equal to the TCP destination port. <ul style="list-style-type: none"> <li>● Disabled - Disable the item function.</li> </ul>   |

|                                |   |
|--------------------------------|---|
|                                | <ul style="list-style-type: none"> <li>● <b>Enabled</b> - Enable the item function.</li> </ul>  |
| <b>Ping of Death</b>           | <p>Avoid ping of death attack.<br/>Ping packets that length are larger than 65535 bytes.</p> <ul style="list-style-type: none"> <li>● <b>Disabled</b> - Disable the item function.</li> <li>● <b>Enabled</b> - Enable the item function.</li> </ul>   |
| <b>IPv6 Min Fragments</b>      | <p>Check the minimum size of IPv6 fragments, and drop the packets smaller than the minimum size. The valid range is from 0 to 65535 bytes, and default value is 1240 bytes.</p> <ul style="list-style-type: none"> <li>● <b>Disabled</b> - Disable the item function.</li> <li>● <b>Enabled</b> - Enable the item function.</li> </ul>      |
| <b>ICMP Fragments</b>          | <p>Drop the fragmented ICMP packets.</p> <ul style="list-style-type: none"> <li>● <b>Disabled</b> - Disable the item function.</li> <li>● <b>Enabled</b> - Enable the item function.</li> </ul>   |
| <b>IPv4 Ping Max Size</b>      | <p>Determine the IPv4 PING packet with the length.</p> <ul style="list-style-type: none"> <li>● <b>Disabled</b> - Disable the item function.</li> <li>● <b>Enabled</b> - Enable the item function.-</li> </ul>  |
| <b>IPv6 Ping Max Size</b>      | <p>Determine the IPv6 PING packet with the length.</p> <ul style="list-style-type: none"> <li>● <b>Disabled</b> - Disable the item function.</li> <li>● <b>Enabled</b> - Enable the item function.</li> </ul>   |
| <b>Ping Max Size Setting</b>   | <p>Determine the IPv4/IPv6 PING packet with the length. Specify the maximum size of the ICMPv4/ICMPv6 ping packets. The valid range is from 0 to 65535 bytes, and the default value is 512 bytes.</p>   |
| <b>Smurf Attack</b>            | <p>Avoid smurf attack. The length range of the netmask is from 0 to 323 bytes, and default length is 0 byte.</p> <ul style="list-style-type: none"> <li>● <b>Disabled</b> - Disable the item function.</li> <li>● <b>Enabled</b> - Enable the item function.</li> </ul>   |
| <b>TCP Min Hdr Size</b>        | <p>Check the minimum TCP header and drops the TCP packets with the header smaller than the minimum size. The length range is from 0 to 31 bytes, and default length is 20 bytes.</p> <ul style="list-style-type: none"> <li>● <b>Disabled</b> - Disable the item function.</li> <li>● <b>Enabled</b> - Enable the item function.</li> </ul> |
| <b>TCP-SYN (SPORT&lt;1024)</b> | <p>Drop SYN packets with sport less than 1024.</p> <ul style="list-style-type: none"> <li>● <b>Disabled</b> - Disable the item function.</li> <li>● <b>Enabled</b> - Enable the item function.</li> </ul>   |
| <b>Null Scan Attack</b>        | <p>Drop the packets with NULL scan.</p> <ul style="list-style-type: none"> <li>● <b>Disabled</b> - Disable the item function.</li> <li>● <b>Enabled</b> - Enable the item function.</li> </ul>  |
| <b>X-mas Scan Attack</b>       | <p>Drop the packets if the sequence number is zero, and the FIN, URG and PSH bits are set.</p> <ul style="list-style-type: none"> <li>● <b>Disabled</b> - Disable the item function.</li> <li>● <b>Enabled</b> - Enable the item function.</li> </ul>   |
| <b>TCP SYN-FIN Attack</b>      | <p>Drop the packets with SYN and FIN bits set.</p> <ul style="list-style-type: none"> <li>● <b>Disabled</b> - Disable the item function.</li> <li>● <b>Enabled</b> - Enable the item function.-</li> </ul>  |
| <b>TCP SYN-RST Attack</b>      | <p>Drop the packets with SYN and RST bits set.</p> <ul style="list-style-type: none"> <li>● <b>Disabled</b> - Disable the item function.</li> </ul>   |


|                         |  |
|-------------------------|--|
|                         | <ul style="list-style-type: none"> <li>● <b>Enabled</b> - Enable the item function.</li> </ul>   |
| TCP Fragment (Offset=1) | Drop the fragmented ICMP packets. <ul style="list-style-type: none"> <li>● <b>Disabled</b> - Disable the item function.</li> <li>● <b>Enabled</b> - Enable the item function.</li> </ul> |
| Apply                   | Apply the settings to the switch.  |

## IV-8-2 DoS Port Setting

This page allows a user to configure and display the state of DoS protection for interfaces. The configuration result for each port will be displayed on the table listed on the lower side of this web page.



Available settings are explained as follows:

| Item           | Description  |
|----------------|--|
| Port           | Use the drop down list to select the port profile (GE1 to GE28) or profiles.   |
| DoS Protection | <ul style="list-style-type: none"> <li>● <b>Disabled</b> - Disable the function of DoS Protection.</li> <li>● <b>Enabled</b> - Enable the function of DoS Protection.</li> </ul> |
| Apply          | Apply the settings to the switch.  |
| Modify         |  - Click it to modify settings.   |



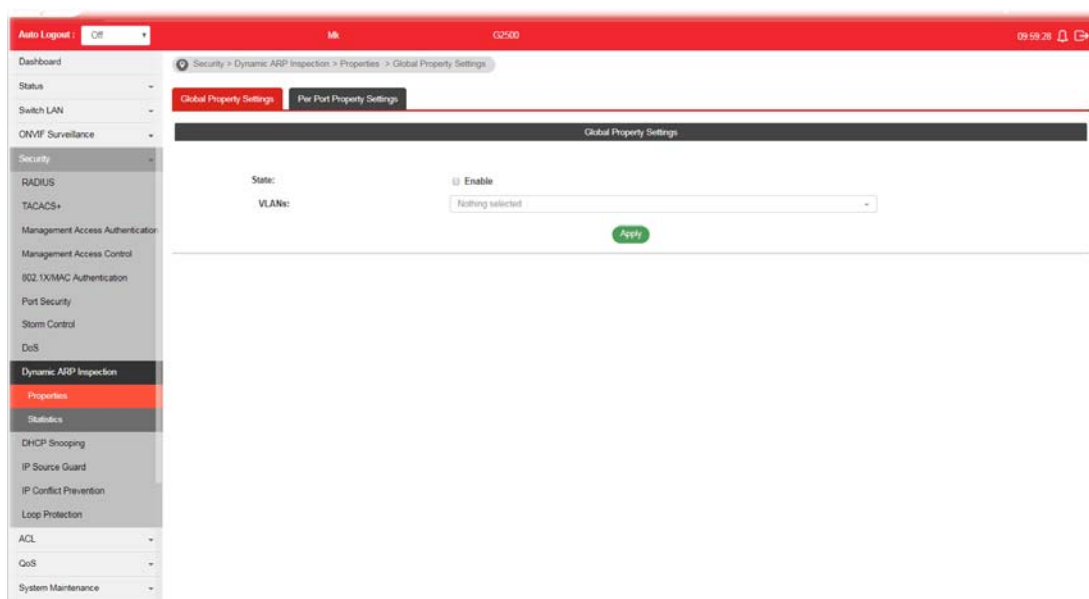
## IV-9 Dynamic ARP Inspection

Dynamic ARP inspection (DAI) can prevent ARP spoofing attacks by validating ARP packet in a network. It can intercept, record, and discard ARP packets with invalid IP-to-MAC address bindings; and then protect the network against malicious attacks.

### IV-9-1 Properties

#### IV-9-1-1 Global Property Settings

This page allows a user to configure global property settings for the function of Dynamic ARP Inspection.

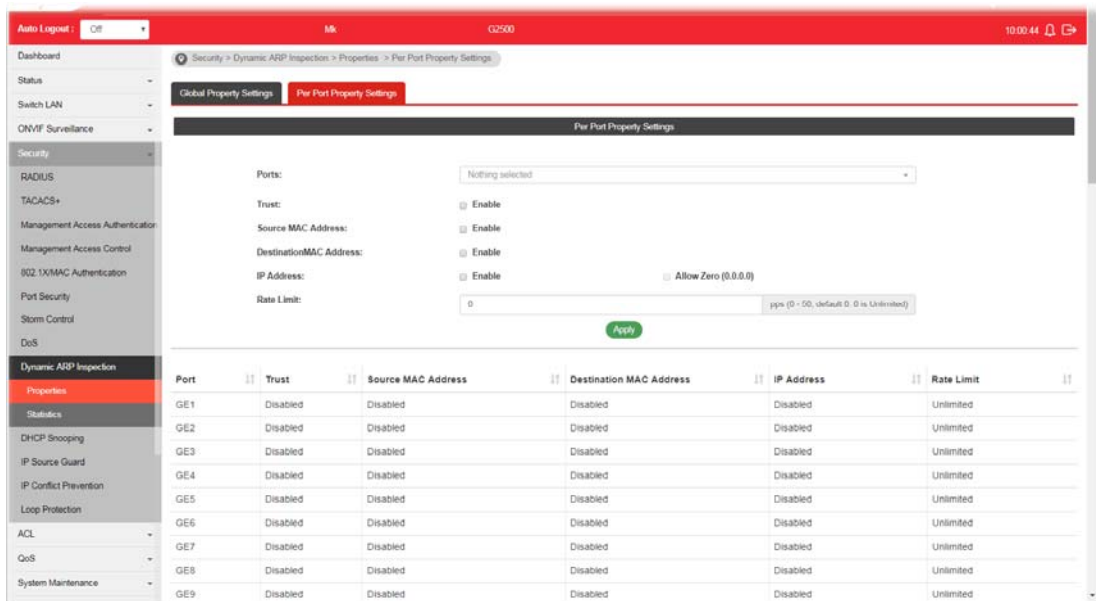


Available settings are explained as follows:

| Item  | Description   |
|-------|---|
| State | Enable - Check the box to enable global property settings.  |
| VLANs | Select VLAN profile(s) to apply the function of Dynamic ARP Inspection.<br>Only the GE/LAG port within the selected VLAN will apply DAI function. |
| Apply | Apply the settings to the switch.   |

## IV-9-1-2 Per Port Property Settings

This page allows a user to configure detailed settings of DAI for each port (GE/LAG).



Available settings are explained as follows:

| Item                    | Description  |
|-------------------------|--|
| Ports                   | Use the drop down list to select the port (GE1 to GE28, LAG1 to LAG8) or ports for applying DAI function.  |
| Trust                   | <b>Enable</b> - Enable the function of DAI for the port(s) selected above.   |
| Source MAC Address      | <b>Enable</b> - Check it to enable the function of source MAC address validation mechanism for the selected port(s).   |
| Destination MAC Address | <b>Enable</b> - Check it to enable the function of destination MAC address validation mechanism for the selected port(s).  |
| IP Address              | <ul style="list-style-type: none"> <li><b>Enable</b> - Check it to enable the function of IP address validation mechanism for the selected port(s).</li> <li><b>Allow Zero</b> - The IP address of "0.0.0.0" can be applied to the selected port(s) if it is enabled.</li> </ul> |
| Rate Limit              | Use the drop down list to choose a rate limitation value (0-50) for the selected port(s).  |
| Apply                   | Apply the settings to the switch.  |

## IV-9-2 Statistics

This page displays all statistics recorded by Dynamic ARP Inspection function.

The screenshot shows the web interface for a VigorSwitch G2500. The top navigation bar is red and contains the text "Auto Logout: 00", "M", "G2500", and "10:01:20". The left sidebar is a grey menu with various security and management options. The main content area is titled "Security > Dynamic ARP Inspection > Statistics > Statistics" and features a red "Statistics" header. Below the header are "Loading" and "Clear All" buttons. The main data is presented in a table with the following columns: Port, Forward, Source MAC Failure, Destination MAC Failure, Source IP Validation Failure, Destination IP Validation Failure, and IP-MAC Mismatch Failure. The table lists 15 ports (GE1 through GE15) with all values set to 0.

| Port | Forward | Source MAC Failure | Destination MAC Failure | Source IP Validation Failure | Destination IP Validation Failure | IP-MAC Mismatch Failure |
|------|---------|--------------------|-------------------------|------------------------------|-----------------------------------|-------------------------|
| GE1  | 0       | 0                  | 0                       | 0                            | 0                                 | 0                       |
| GE2  | 0       | 0                  | 0                       | 0                            | 0                                 | 0                       |
| GE3  | 0       | 0                  | 0                       | 0                            | 0                                 | 0                       |
| GE4  | 0       | 0                  | 0                       | 0                            | 0                                 | 0                       |
| GE5  | 0       | 0                  | 0                       | 0                            | 0                                 | 0                       |
| GE6  | 0       | 0                  | 0                       | 0                            | 0                                 | 0                       |
| GE7  | 0       | 0                  | 0                       | 0                            | 0                                 | 0                       |
| GE8  | 0       | 0                  | 0                       | 0                            | 0                                 | 0                       |
| GE9  | 0       | 0                  | 0                       | 0                            | 0                                 | 0                       |
| GE10 | 0       | 0                  | 0                       | 0                            | 0                                 | 0                       |
| GE11 | 0       | 0                  | 0                       | 0                            | 0                                 | 0                       |
| GE12 | 0       | 0                  | 0                       | 0                            | 0                                 | 0                       |
| GE13 | 0       | 0                  | 0                       | 0                            | 0                                 | 0                       |
| GE14 | 0       | 0                  | 0                       | 0                            | 0                                 | 0                       |
| GE15 | 0       | 0                  | 0                       | 0                            | 0                                 | 0                       |

## IV-10 DHCP Snooping

DHCP snooping is able to validate DHCP messages obtained from untrusted sources and filter out invalid message.

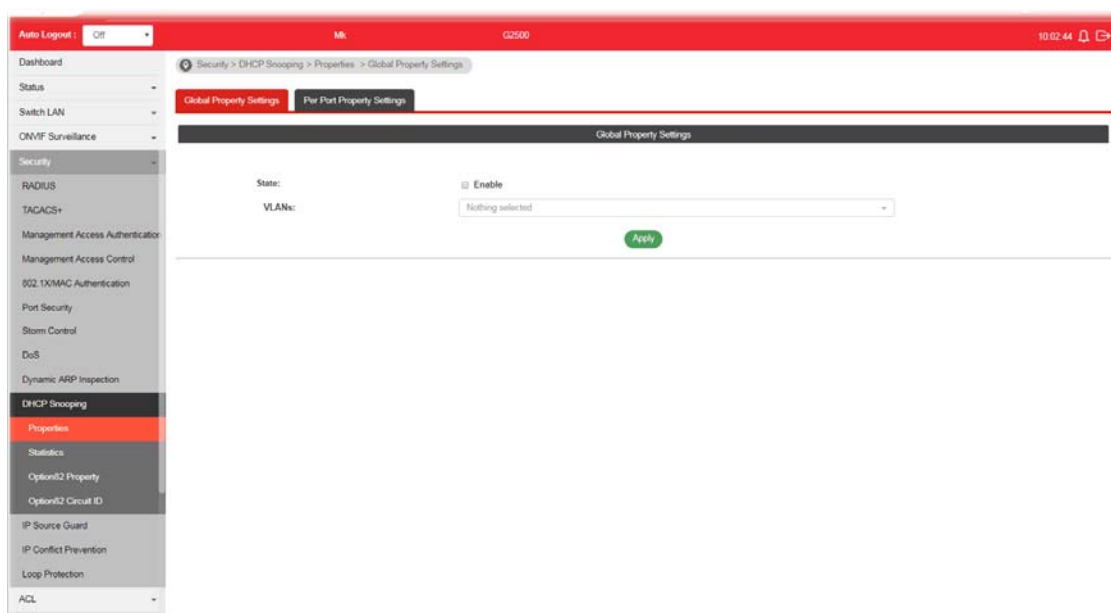
For DHCP snooping to function properly, it is suggested to connect DHCP servers to VigorSwitch through trusted interfaces; because untrusted DHCP messages will be forwarded to trusted interfaces only.

### IV-10-1 Properties

#### IV-10-1-1 Global Property Settings

This page allows a user to configure global property settings for the function of DHCP snooping Inspection.

In default, DHCP snooping is inactive on all VLANs. You can enable such feature on a single VLAN or a range of VLANs.



Available settings are explained as follows:

| Item  | Description   |
|-------|---|
| State | Enable - Check the box to enable global property settings.  |
| VLANs | Select VLAN profile(s) to apply the function of DHCP Snooping Inspection.<br>Only the GE/LAG port within the selected VLAN will apply DHCP Snooping function. |
| Apply | Apply the settings to the switch.   |

## IV-10-1-2 Per Port Property Settings

This page allows a user to configure detailed settings of DHCP Snooping for each port (GE/LAG).

Any device that is not in the service provider network will be regarded as an untrusted source (such as a customer switch). Host ports are untrusted sources. In VigorSwitch, you can assign a source as trusted device by configuring the trust state of its connecting port.

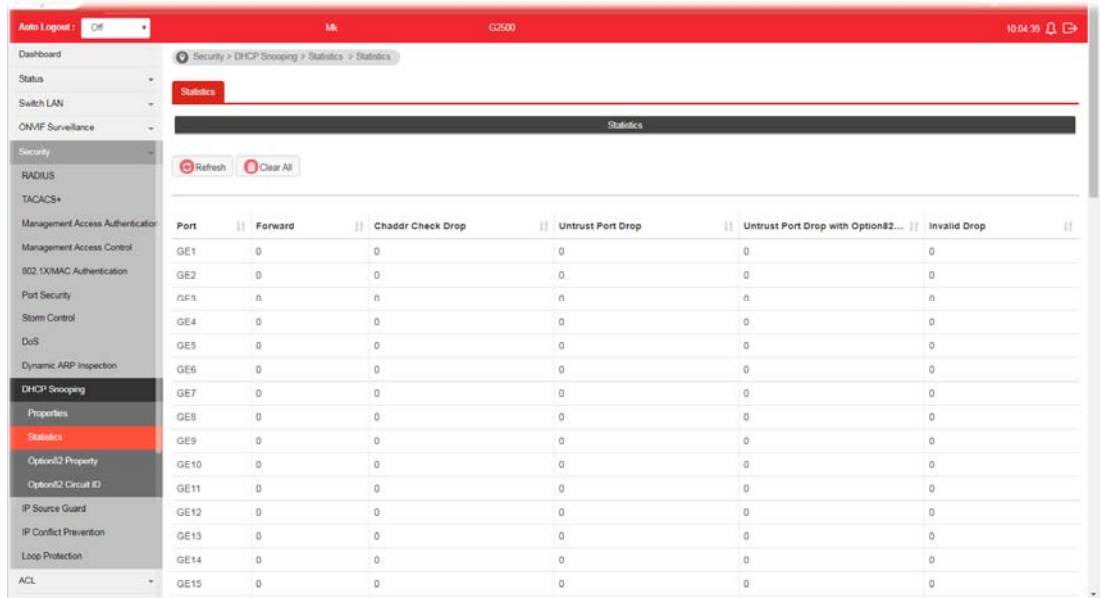
| Port | Trust    | Verify Chaddr | Rate Limit |
|------|----------|---------------|------------|
| GE1  | Disabled | Disabled      | Unlimited  |
| GE2  | Disabled | Disabled      | Unlimited  |
| GE3  | Disabled | Disabled      | Unlimited  |
| GE4  | Disabled | Disabled      | Unlimited  |
| GE5  | Disabled | Disabled      | Unlimited  |
| GE6  | Disabled | Disabled      | Unlimited  |
| GE7  | Disabled | Disabled      | Unlimited  |
| GE8  | Disabled | Disabled      | Unlimited  |
| GE9  | Disabled | Disabled      | Unlimited  |
| GE10 | Disabled | Disabled      | Unlimited  |
| GE11 | Disabled | Disabled      | Unlimited  |

Available settings are explained as follows:

| Item          | Description  |
|---------------|--|
| Ports         | Use the drop down list to select the port (GE1 to GE28, LAG1 to LAG8) or ports for applying DHCP snooping function.  |
| Trust         | <b>Enable</b> - Check it to make the port(s) selected above as trusted interface.  |
| Verify Chaddr | <b>Enable</b> - Check it to enable chaddr (client hardware address) validation of GE/LAG port. All DHCP packets will be checked if the client hardware MAC address is the same as source MAC in Ethernet header or not. Default is disabled. |
| Rate Limit    | Input rate limitation (0~300) of DHCP packets. The unit is "pps". "0" means unlimited. Default is unlimited.   |
| Apply         | Apply the settings to the switch.  |

## IV-10-2 Statistics

This page displays all statistics recorded by DHCP snooping function.



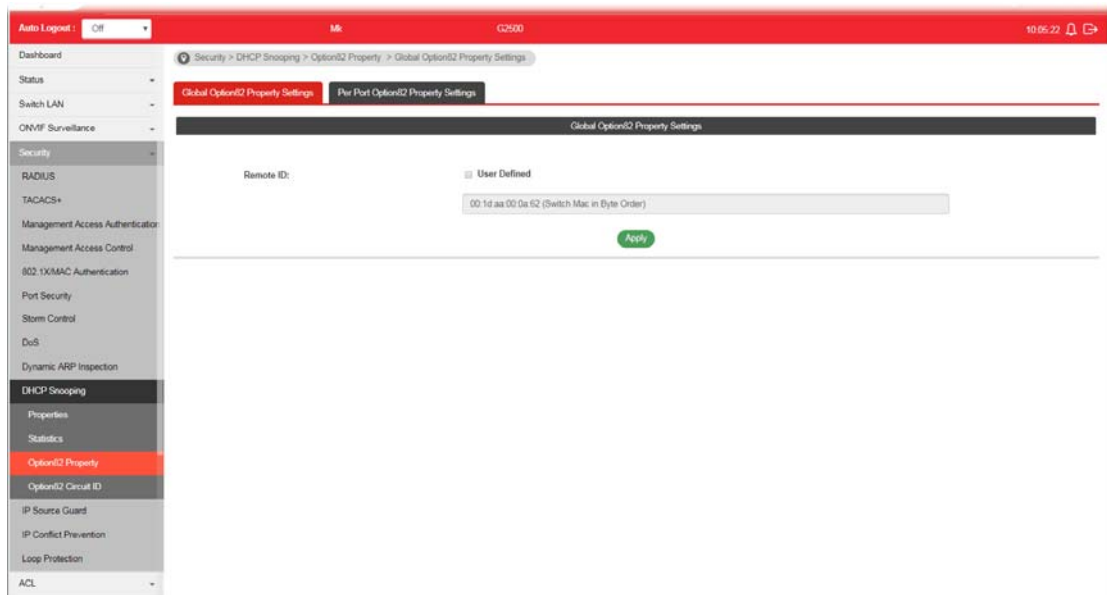
| Port | Forward | Chaddr Check Drop | Untrust Port Drop | Untrust Port Drop with Option82... | Invalid Drop |
|------|---------|-------------------|-------------------|------------------------------------|--------------|
| GE1  | 0       | 0                 | 0                 | 0                                  | 0            |
| GE2  | 0       | 0                 | 0                 | 0                                  | 0            |
| GE3  | 0       | 0                 | 0                 | 0                                  | 0            |
| GE4  | 0       | 0                 | 0                 | 0                                  | 0            |
| GE5  | 0       | 0                 | 0                 | 0                                  | 0            |
| GE6  | 0       | 0                 | 0                 | 0                                  | 0            |
| GE7  | 0       | 0                 | 0                 | 0                                  | 0            |
| GE8  | 0       | 0                 | 0                 | 0                                  | 0            |
| GE9  | 0       | 0                 | 0                 | 0                                  | 0            |
| GE10 | 0       | 0                 | 0                 | 0                                  | 0            |
| GE11 | 0       | 0                 | 0                 | 0                                  | 0            |
| GE12 | 0       | 0                 | 0                 | 0                                  | 0            |
| GE13 | 0       | 0                 | 0                 | 0                                  | 0            |
| GE14 | 0       | 0                 | 0                 | 0                                  | 0            |
| GE15 | 0       | 0                 | 0                 | 0                                  | 0            |

## IV-10-3 Option82 Property

You can use information settings including Remote ID and Circuit ID for Option82 Property, also known as the DHCP relay agent, to protect VigorSwitch against spoofing attacks.

### IV-10-3-1 Global Option82 Property Settings

This page allows a user to set string as remote ID for DHCP option82. For example, use a switch-configured hostname or specify an ASCII text string as remote ID.



Global Option82 Property Settings

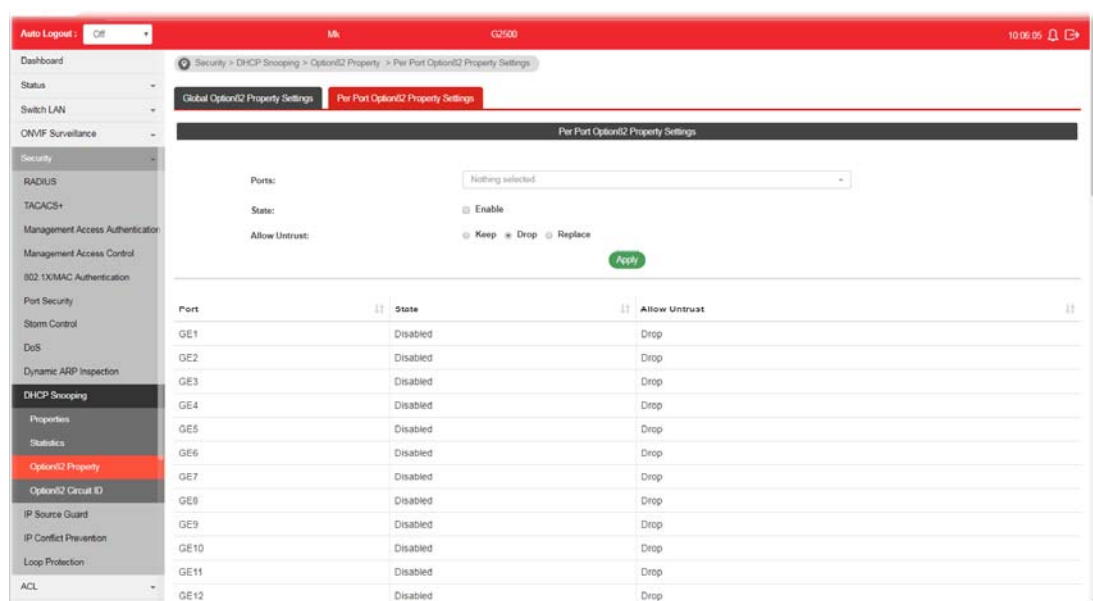
Remote ID:

Available settings are explained as follows:

| Item      | Description   |
|-----------|---|
| Remote ID | The string specified here is used to identify the remote host.<br><b>User Defined</b> - Check it and manually enter ASCII text string in the entry box. |
| Apply     | Apply the settings to the switch.   |

### IV-10-3-2 Per Port Option82 Property Settings

This page allows a user to configure detailed settings of DHCP Snooping, Option82 for each port (GE/LAG).



Available settings are explained as follows:

| Item          | Description   |
|---------------|---|
| Ports         | Use the drop down list to select the port (GE1 to GE28, LAG1 to LAG8) or ports for applying DHCP snooping, Option82 Property function.  |
| State         | <b>Enable</b> - Check it to make the port(s) selected above apply the settings configured in this page.   |
| Allow Untrust | Untrusted packets detected by VigorSwitch will be performed by the action determined here. <ul style="list-style-type: none"> <li>● <b>Keep</b> - Packets are allowed to pass through.</li> <li>● <b>Drop</b> - Packets are blocked and discarded.</li> <li>● <b>Replace</b> - Packets will be replaced.</li> </ul> |
| Apply         | Apply the settings to the switch.   |

## IV-10-4 Option82 Circuit ID

This page allows a user to set string as circuit ID for DHCP option82 setting. Circuit ID shall be combined with VLAN name (or VLAN ID number) and interface name (GE/LAG port).



The screenshot shows the configuration page for Option82 Circuit ID. The sidebar on the left includes sections like Security, DHCP Snooping, and Option82 Property. The main content area has a form with the following fields:

- Port:** A dropdown menu currently showing 'GE1'.
- VLAN:** A text input field with a placeholder 'Keep empty to set without VLAN' and a range indicator '(1 - 4094)'.
- Circuit ID:** An empty text input field.

Below the form is a table with the following structure:

| Port                       | VLAN | Circuit ID | Edit |
|----------------------------|------|------------|------|
| No data available in table |      |            |      |

Available settings are explained as follows:

| Item       | Description   |
|------------|---|
| Port       | Use the drop down list to select the port (GE1 to GE28, LAG1 to LAG8) or ports for applying DHCP snooping, Option82 Property function.  |
| VLAN       | Choose a number as VLAN ID which is easy to be identified for a packet containing with it.<br>It is optional setting.   |
| Circuit ID | Enter ASCII text string in the entry box. Later, any packet passes through the specified interface (GE/LAG port) will be inserted with such information.  |
| Add        | Click it to create a profile.   |
| Edit       |  - click it to modify the circuit ID value for the selected entry.<br> - click it to remove the selected entry. |

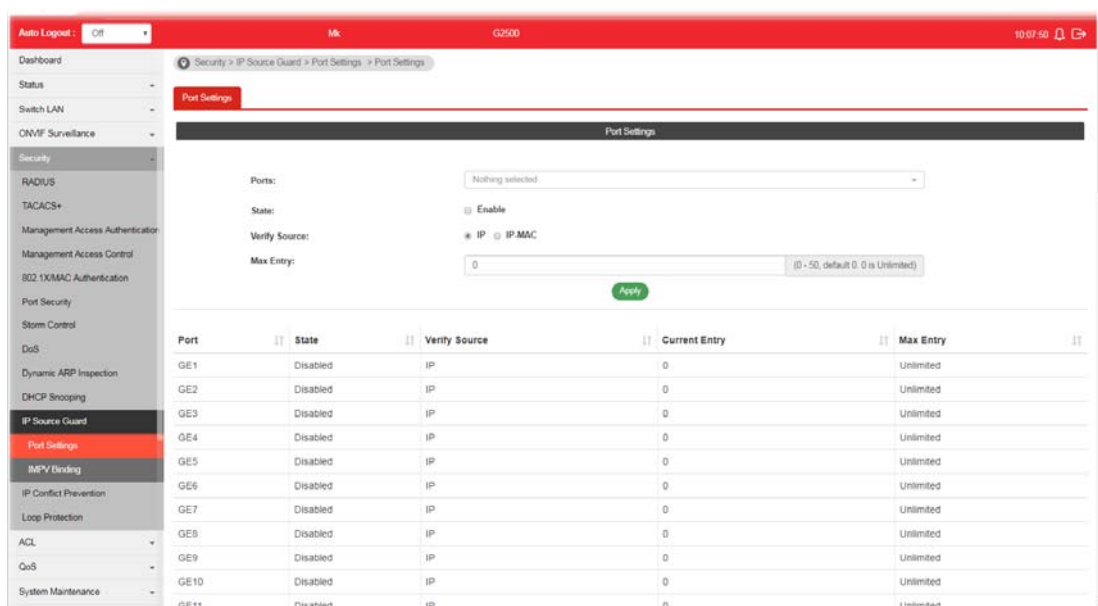


## IV-11 IP Source Guard

By using the source IP address filtering function, IP source guard can prevent a malicious host from feigning a legal host with its IP address and performing malicious attack.

### IV-11-1 Port Settings

IP source guard is a port-based feature. Therefore, it is necessary to configure detailed settings for each GE/LAG port interface separately.




Available settings are explained as follows:

| Item          | Description   |
|---------------|---|
| Ports         | Use the drop down list to select the port (GE1 to GE28, LAG1 to LAG8) or ports for applying IP source guard function.   |
| State         | <b>Enable</b> - Check it to make the port(s) selected above apply the settings configured in this page.   |
| Verify Source | Specify the type of source IP for the packet coming from. <ul style="list-style-type: none"><li>● <b>IP</b> - Only the packet with specified IP address will be verified.</li><li>● <b>IP-MAC</b> - Only the packet with specified IP address and MAC address will be verified.</li></ul> |
| Max Entry     | Define the number (0-50) for the port.<br>The default is 0 (no limit).  |
| Apply         | Apply the settings to the switch.   |

## IV-11-2 IMPV Binding

This page allows the network administrator to set the filtering conditions (binding type, MAC address, IPv4 address) for packets through the specified LAN port.

Available settings are explained as follows:

| Item         | Description   |
|--------------|---|
| Ports        | Use the drop down list to select the port (GE1 to GE50, LAG1 to LAG16) or ports for applying IMPV Binding function.   |
| VLAN         | Choose a number as VLAN ID which is easy to be identified for a packet containing with it.<br>It is optional setting.   |
| Binding      | Select the binding type for such feature. <ul style="list-style-type: none"> <li>● <b>IP-MAC-Port-VLAN</b> - Packets will be allowed to pass through the port interface if they meet the conditions specified by IP address, MAC address, Port setting and VLAN ID setting.</li> <li>● <b>IP-Port-VLAN</b> - Packets will be allowed to pass through the port interface if they meet the conditions specified by IP address, Port setting and VLAN ID setting.</li> </ul> |
| MAC Address  | Enter the MAC address of the device connecting to the port interface selected above.  |
| IPv4 Address | Enter the IP address with mask address of the device connecting to the port interface selected above.   |
| Add          | Click it to create a new binding profile.   |
| Edit         |  - Click it to modify the settings for the selected entry.   |

**Edit** ✕

**Ports:**

**VLAN:**  (1 - 4094)

**Binding:**  IP-MAC-Port-VLAN  IP-Port-VLAN

**MAC Address:**

**IPv4 Address:**  /

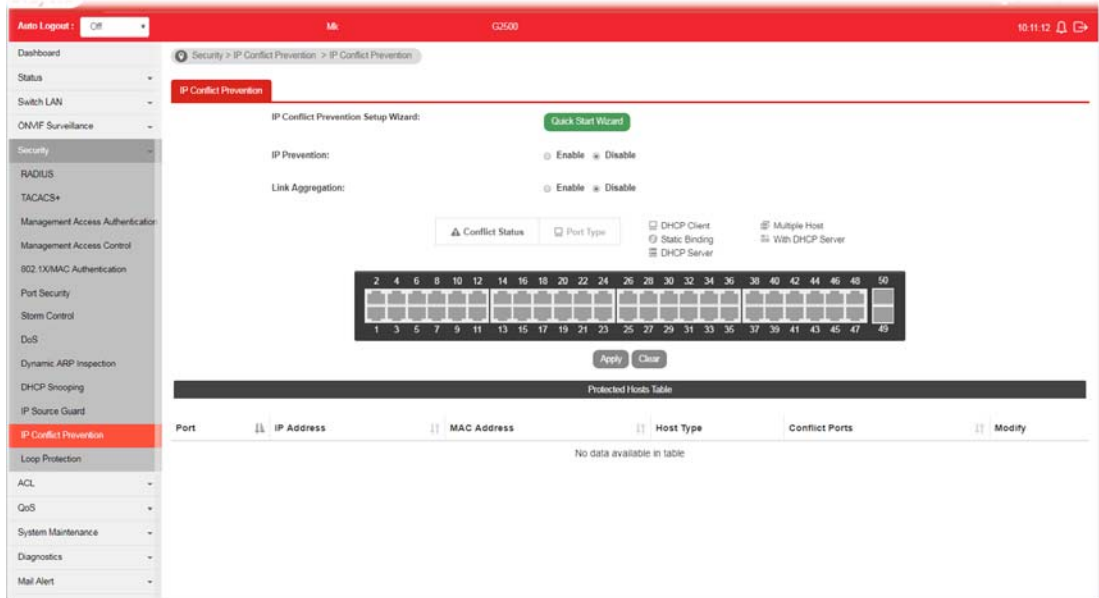


- click it to remove the selected entry.

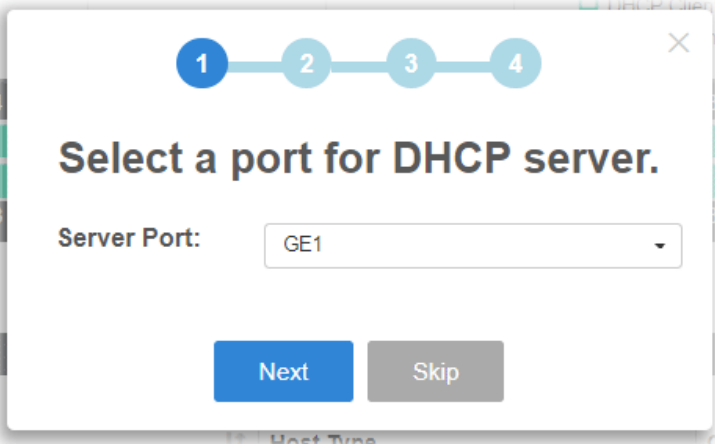
## IV-12 IP Conflict Prevention

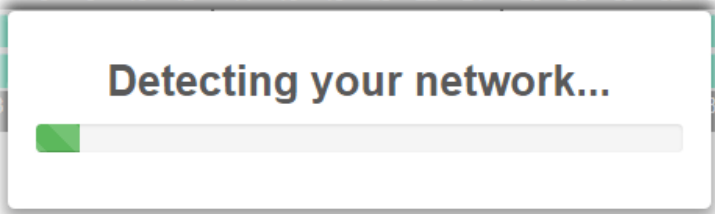
A user can configure IP addresses for network devices manually. However, it might result in conflict between different devices due to using the same IP address, and cause the devices not working correctly.

This page allows you to prevent IP conflict by binding the port with the specified IP address.

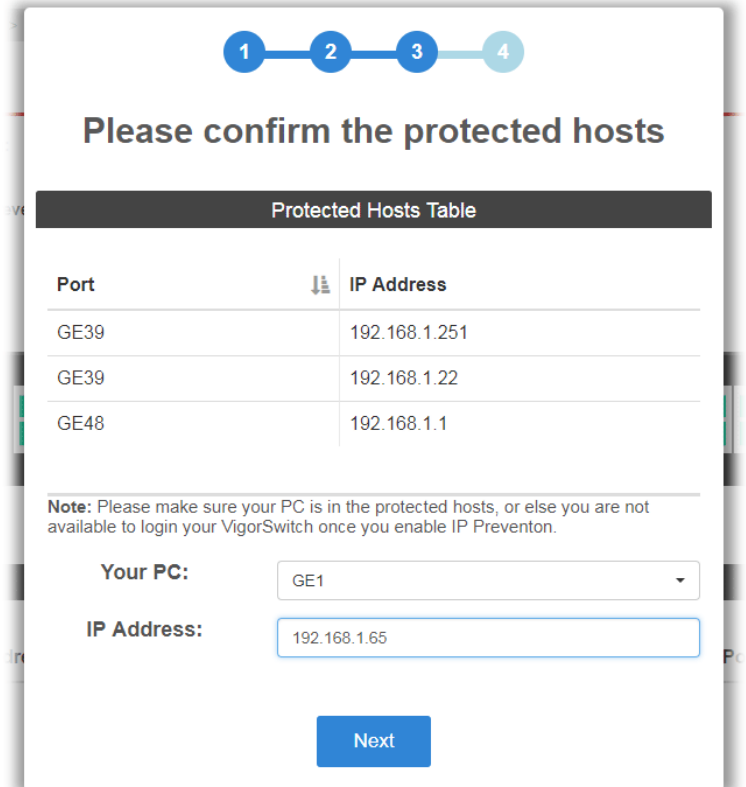


Available settings are explained as follows:

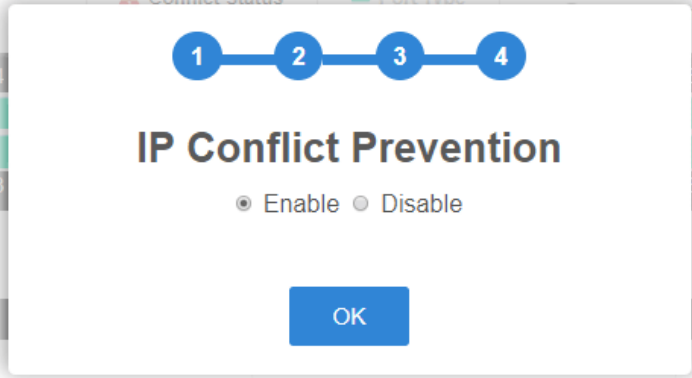

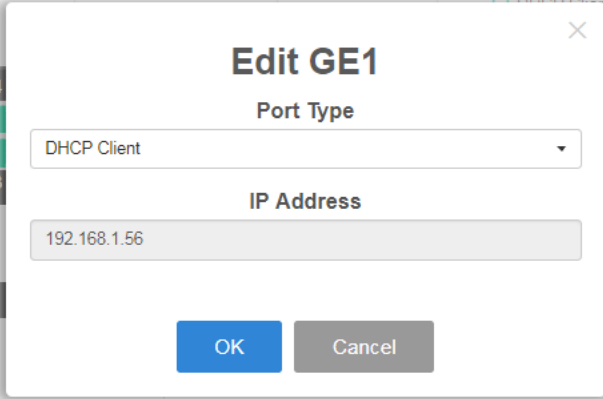
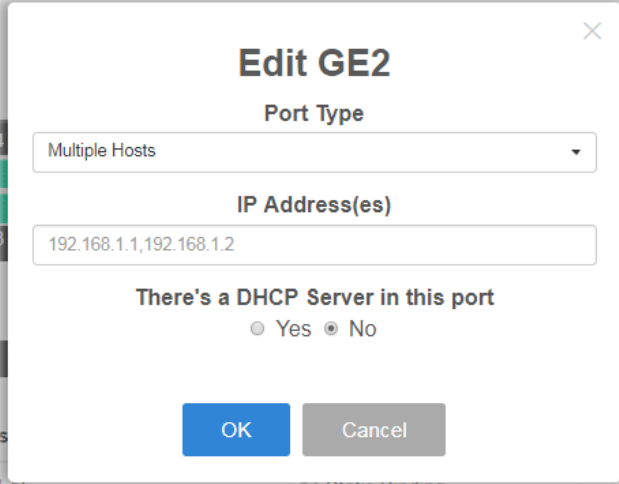
| Item                                | Description   |
|-------------------------------------|---|
| IP Conflict Prevention Setup Wizard | <p>Quick Start Wizard - The system will guide to bind server port with an IP address step by step.</p> <p>Step 1</p>  <p>Step 2</p> |



Step 3



Step 4

|                  |   |
|------------------|---|
|                  |  <p>After clicking OK, the IP address specified for the GE port will be unavailable for other network devices.</p>  |
| IP Prevention    | <p><b>Enable</b> - Click it to activate the function of IP prevention.<br/> <b>Disable</b> - Click it to deactivate the function of IP prevention.</p>  |
| Link Aggregation | <p><b>Enable</b> - Click it to activate the function of link aggregation.<br/> <b>Disable</b> - Click it to deactivate the function of link aggregation.</p>  |
| Apply            | <p>Apply the settings to the switch.</p>  |
| Clear            | <p>Remove all settings of IP source guard DHCP snooping and dynamic ARP inspection.</p>   |
| Modify           |  - Click it to modify the settings for the selected entry.<br><br> |

---

**Port Type** - There are four selections - DHCP Client, Static Binding, Multiple Hosts and DHCP Server. Each type will bring out different IP address(es) settings.

**OK** - Click it to save the settings.

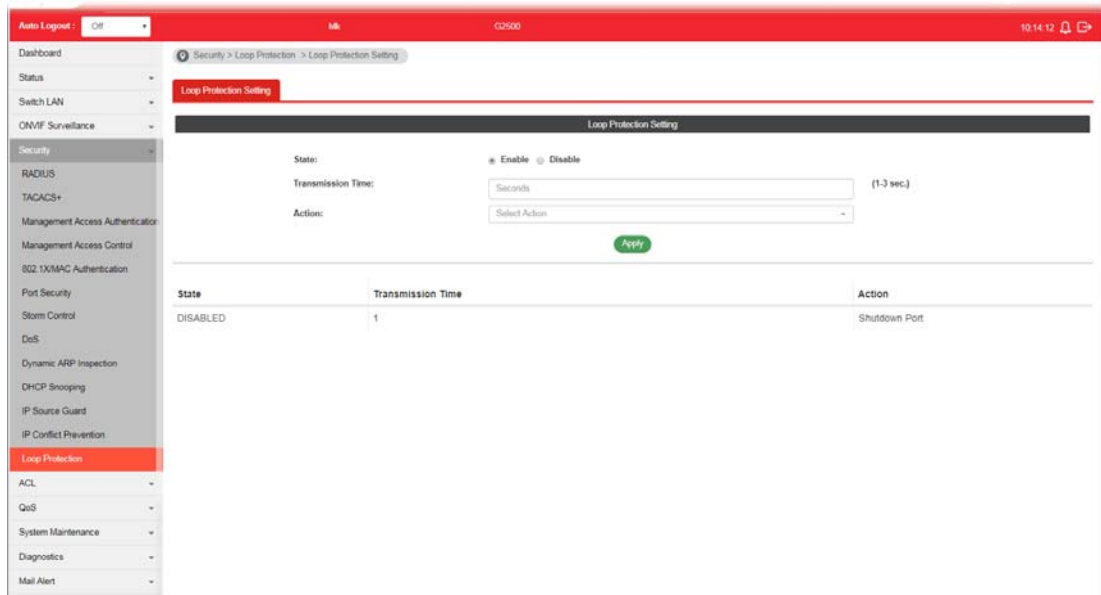


- Click it to remove the selected entry.

---

## IV-13 Loop Protection

Loop event might be caused due to wrong hardware connection. VigorSwitch will periodically send packets out to check if they loopback or not. This page allows you to set conditions and perform an action when VigorSwitch detects the looped packet.



Available settings are explained as follows:

| Item              | Description  |
|-------------------|--|
| State             | <ul style="list-style-type: none"> <li>● <b>Enable</b> - VigorSwitch detects the loop event of GE ports/LAG ports automatically.</li> <li>● <b>Disable</b> - VigorSwitch will not detect the loop event.</li> </ul>  |
| Transmission Time | When the loop event occurred, VigorSwitch will perform the action after a period of time.  |
| Action            | <p>When the switch detects loop situation occurred to a port; it will perform the action selected in this field.</p> <div data-bbox="691 1503 1361 1641" style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p>Select Action</p> <ul style="list-style-type: none"> <li>Log</li> <li>Shutdown Port</li> <li>Shutdown Port and Log</li> </ul> </div> <ul style="list-style-type: none"> <li>● <b>Log</b> - The switch will record such event as a log.</li> <li>● <b>Shutdown Port</b> - The switch will shut down the port.</li> <li>● <b>Shutdown Port and Log</b> - The switch will shut down the port and record the event as a log. The system administrator will view the content from system log.</li> </ul> |
| Apply             | Apply the settings to the switch.  |



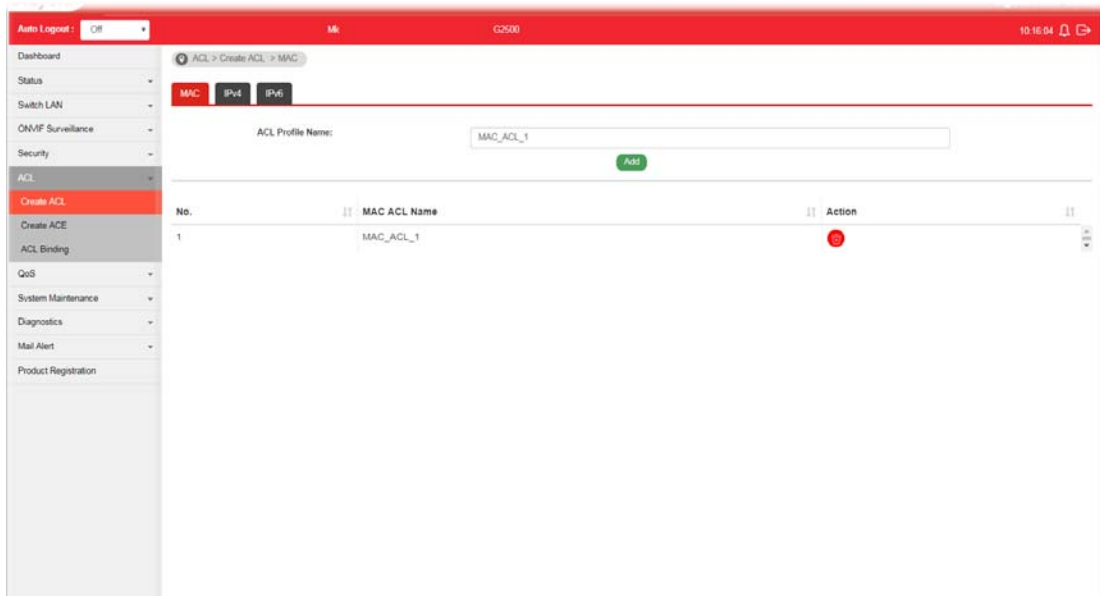
# Part V ACL Configuration

## V-1 Create ACL


An Access Control List (ACL) is a sequential list of permit or deny conditions that apply to IP addresses, MAC addresses, or other more specific criteria. This switch tests ingress packets against the conditions in an ACL one by one. A packet will be accepted as soon as it matches a permit rule, or dropped as soon as it matches a deny rule. If no rules match, the frame is accepted.

### V-1-1 MAC

The function is used to show the Access Control List (ACL) based on Layer 2 filtering, the MAC layer. The ACL is composed by many Access Control Element (ACE) rules. You can create a new ACL here; then add multiple ACEs.

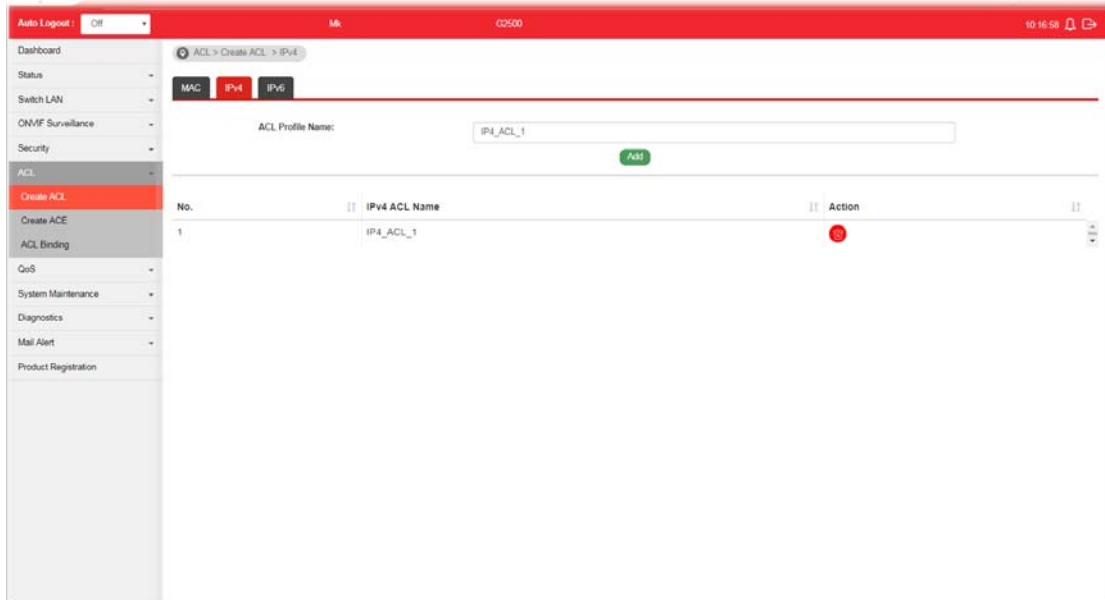


Available settings are explained as follows:


| Item             | Description  |
|------------------|--|
| ACL Profile Name | Enter a name for creating a new ACL profile.   |
| Add              | Add a new ACL entry using given ACL name.  |
| Action           |  - click it to remove the selected entry. |

## V-1-2 IPv4

The function is used to show the Access Control List (ACL) based on Layer 2 to Layer 4 filtering, the IPv4. The ACL is composed by many Access Control Element (ACE) rules. You may create a new ACL here; then add multiple ACEs.

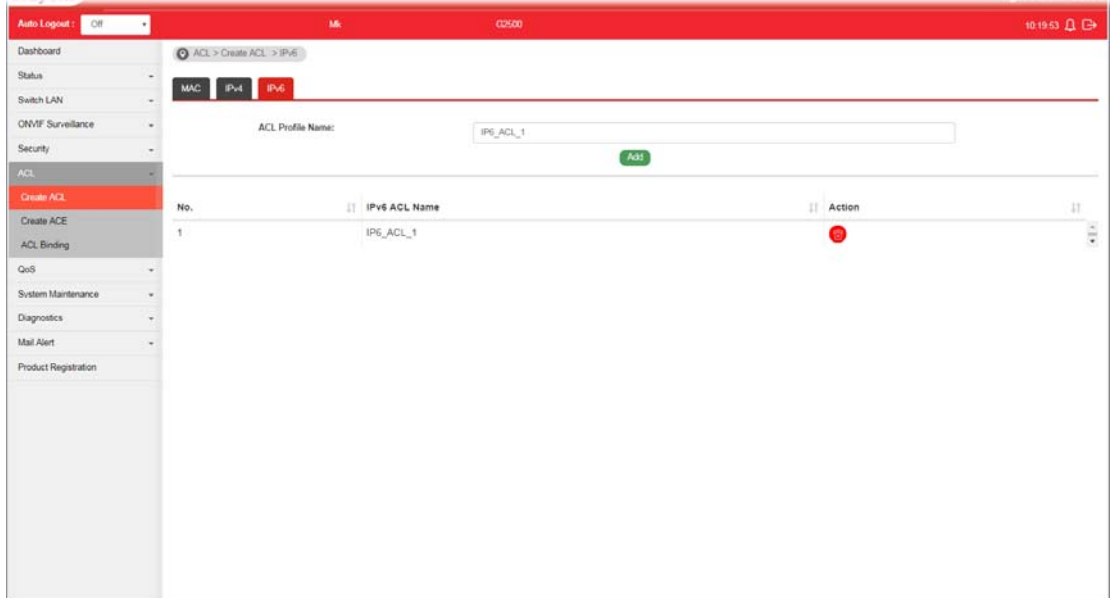


Available settings are explained as follows:


| Item             | Description  |
|------------------|--|
| ACL Profile Name | Enter a name for creating a new ACL profile.   |
| Add              | Add a new ACL entry using given ACL name.  |
| Action           |  - click it to remove the selected entry. |

## V-1-3 IPv6

The function is used to show the Access Control List (ACL) based on Layer 2 to Layer 4 filtering, the IPv6. The ACL is composed by many Access Control Element (ACE) rules. You may create a new ACL here; then add multiple ACEs.



Available settings are explained as follows:

| Item             | Description  |
|------------------|--|
| ACL Profile Name | Enter a name for creating a new ACL profile.   |
| Add              | Add a new ACL entry using given ACL name.  |
| Action           |  - click it to remove the selected entry. |

## V-2 Create ACE

Since ACL based on MAC, IPv4 and/or IPv6 has been created on the section of IV-1, now you can add multiple ACE rules for each ACL.

### V-2-1 MAC



This page shows ACE based on MAC address. You may choose ACL, permit, and deny particular packet or frame, even shutdown the port.

You may provide filtering/matching criteria for one or more of packet characteristic (such as Source/Destination MAC, Ethertype, VLAN, 802.1p) for this ACE to identify the packet.

| No.     | Name      | Sequence | Action | Source MAC/Mask | Destination MAC/Mask | Ethertype | VLAN | 802.1p  | Modify  |
|---------|-----------|----------|--------|-----------------|----------------------|-----------|------|---------|---|
| 1       | MAC_ACL_1 | 1        | Permit | Any/Any         | Any/Any              | Any       | Any  | Any/Any | <span style="color: green;">+</span> <span style="color: red;">-</span> |
| Default | deny all  | -        | Deny   | Any/Any         | Any/Any              | Any       | Any  | Any/Any |   |

Available settings are explained as follows:

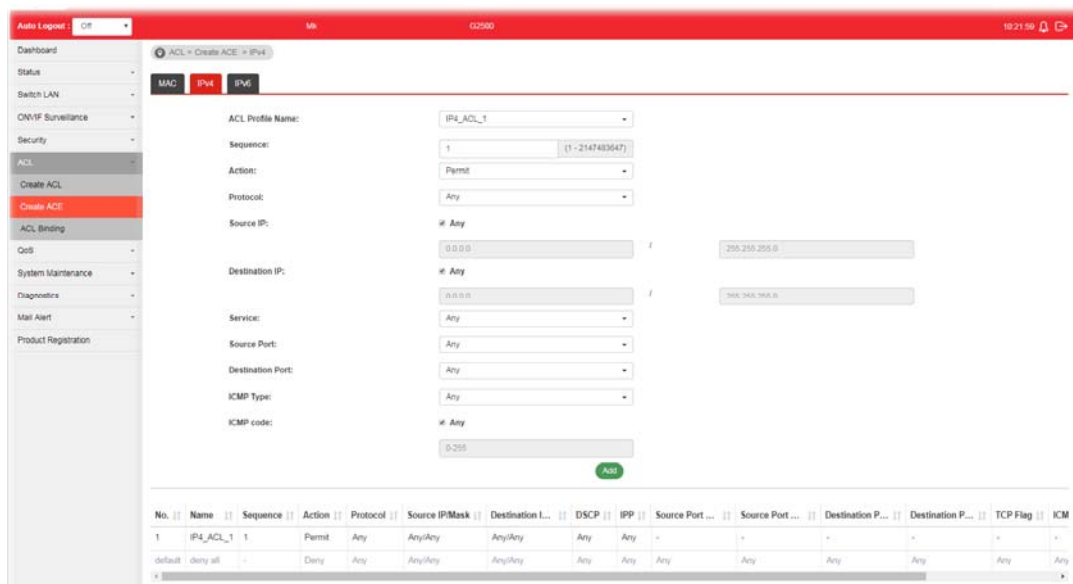
| Item                         | Description  |
|------------------------------|--|
| ACL Profile Name             | Use the drop down list to selected one of the user defined ACL profiles.   |
| Sequence                     | Assign a sequence number to this ACE. The sequence is used to identify which one of ACEs in an ACL is firstly used to match ingress packets. The switch port bound with an ACL use the contained ACE rules, start with the one with lower sequence number to match the packet first. |
| Action                       | Select the action applied to the packet matched this ACE. Permit or deny the packets into switch core, or shutdown the port for stopping further transmission. <ul style="list-style-type: none"> <li>● Permit</li> <li>● Deny</li> <li>● Shutdown</li> </ul>                        |
| Source MAC / Destination MAC | Specify the source and the destination MAC address for filtering.<br>Any - All packets will be filtered.   |

|           |   |
|-----------|---|
|           | Or, enter the IP address to filter the packets coming from that address.  |
| Ethertype | Specify ethernet type for filtering.<br>Select <b>Any</b> .<br>Or, enter the value with the format of "0x600 ~ 0xFFFF".   |
| VLAN      | Specify VLAN profile for filtering.<br>Select <b>Any</b> .<br>Or, enter a VLAN number. The packets coming from the VLAN specified here will be filtered by Vigor device.  |
| 802.1p    | Specify the 802.1p priority value for filtering. Select <b>Any</b> , or a number from 0 to 7.   |
| Add       | Click it to create a new ACE rule.  |
| Modify    |  - click it to modify the settings for the selected entry.<br> - click it to remove the selected entry. |

## V-2-2 IPv4


This page shows ACE based on IPv4 address. You may choose ACL, permit, and deny particular packet or frame, even shutdown the port.

You may provide filtering/matching criteria for one or more of following packet characteristic (such as Protocol over the IP layer, Source/Destination IPv4 address, Type of Service, Source/Destination port number, TCP flags, ICMP Type, if chosen protocol contains ICMP), for this ACE to identify the packet.



Available settings are explained as follows:

| Item             | Description   |
|------------------|---|
| ACL Profile Name | Use the drop down list to selected one of the user defined ACL profiles.  |
| Sequence         | Assign a sequence number to this ACE. The sequence is used to identify which one of ACEs in an ACL is firstly used to match |

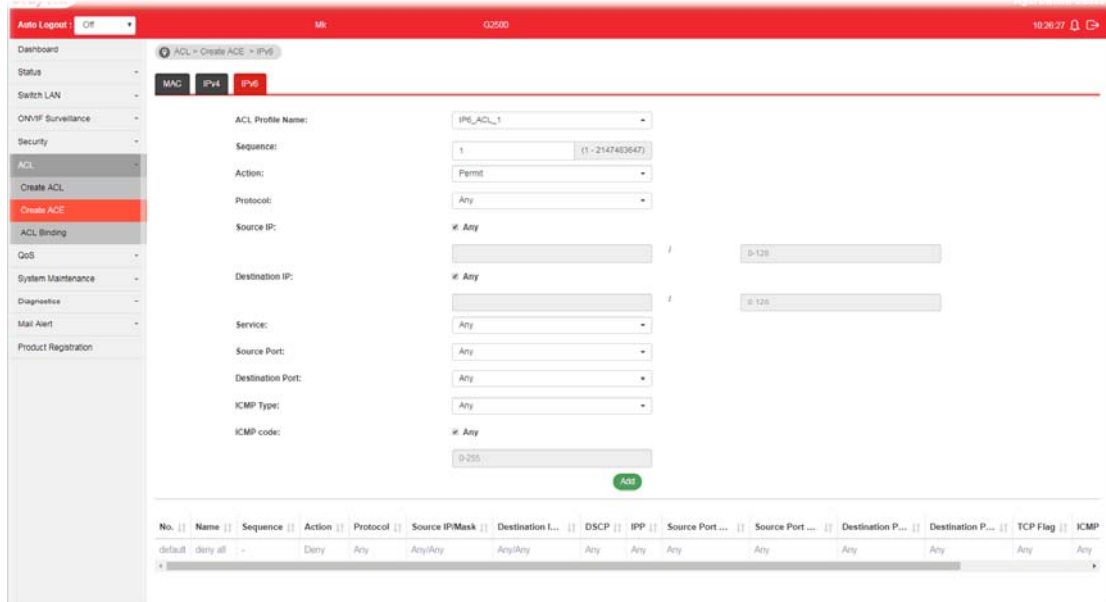
|                                       |  |
|---------------------------------------|--|
|                                       | ingress packets. The switch port bound with an ACL use the contained ACE rules, start with the one with lower sequence number to match the packet first.   |
| <b>Action</b>                         | Select the action applied to the packet matched this ACE. Permit or deny the packets into switch core, or shutdown the port for stopping further transmission. <ul style="list-style-type: none"> <li>● Permit</li> <li>● Deny</li> <li>● Shutdown</li> </ul>  |
| <b>Protocol</b>                       | Specify the protocol for filtering. <ul style="list-style-type: none"> <li>● Any - All packets will be filtered.</li> <li>● Select - Choose one of the protocol (e.g., ICMP, IP in IP, TCP, EGP, IGP...) from the drop down list. Packets passing through the selected protocol will be filtered.</li> <li>● Define - Specify a type number (0 - 255) for ICMP code. For example, 0 means "Echo Reply"; 254 means "RFC3692-style Experiment 2".</li> </ul> |
| <b>Source IP / Destination IP</b>     | Specify the source and the destination IPv4 address for filtering. <p>Any - All packets will be filtered.</p> <p>Or, enter the IP address to filter the packets coming from that address.</p>  |
| <b>Service</b>                        | <ul style="list-style-type: none"> <li>● Any - All packets will be filtered.</li> <li>● DSCP - All IP traffic is mapped to queues based on the DSCP field in the IP header. If traffic is not IP traffic, it is mapped to the lowest priority queue.</li> <li>● IP Precedence - All IP traffic is mapped to queues based on the IP Precedence field in the IP header. If traffic is not IP traffic, it is mapped to the lowest priority queue.</li> </ul>  |
| <b>Source Port / Destination Port</b> | Specify the source and destination port number for filtering the packets. <ul style="list-style-type: none"> <li>● Any - All packets will be filtered.</li> <li>● Single - Only the packets passing through the number defined here will be filtered.</li> <li>● Range - Only the packets passing through the port range defined here will be filtered.</li> </ul>   |
| <b>ICMP Type</b>                      | <ul style="list-style-type: none"> <li>● Any - All packets will be filtered.</li> <li>● Select - Choose one of the type (e.g., Destination Unreachable Echo Reply, MLD Query...) from the drop down list.</li> <li>● Define - Specify a type number (0 - 255) for ICMP code. For example, 0 means "Echo Reply"; 254 means "RFC3692-style Experiment 2".</li> </ul>   |
| <b>ICMP code</b>                      | Each ICMP type can be defined with different codes. For example, if you define ICMP Type as "3", then the available codes for Type 3 will be 0-15. <p>Any - All packets will be filtered.</p> <p>Or, enter 0 to 255 based on the ICMP type specified.</p>  |
| <b>Add</b>                            | Click it to create a new binding profile.  |
| <b>Modify</b>                         |  - click it to modify the settings for the selected entry.  |



- click it to remove the selected entry.

## V-2-3 IPv6



This page allows the network administrator to create ACE based on IPv6 address.



Available settings are explained as follows:

| Item                       | Description   |
|----------------------------|---|
| ACL Profile Name           | Use the drop down list to selected one of the user defined ACL profiles.  |
| Sequence                   | Assign a sequence number to this ACE. The sequence is used to identify which one of ACEs in an ACL is firstly used to match ingress packets. The switch port bound with an ACL use the contained ACE rules, start with the one with lower sequence number to match the packet first.  |
| Action                     | Select the action applied to the packet matched this ACE. Permit or deny the packets into switch core, or shutdown the port for stopping further transmission. <ul style="list-style-type: none"> <li>● Permit</li> <li>● Deny</li> <li>● Shutdown</li> </ul>   |
| Protocol                   | Specify the protocol for filtering. <ul style="list-style-type: none"> <li>● Any - All packets will be filtered.</li> <li>● Select - Choose one of the protocol (e.g., ICMP, TCP, EGP...) from the drop down list. Packets passing through the selected protocol will be filtered.</li> <li>● Define - Specify a type number (0 - 255) for ICMP code. For example, 0 means "Echo Reply"; 254 means "RFC3692-style Experiment 2".</li> </ul> |
| Source IP / Destination IP | Specify the source and the destination IPv6 address for filtering.  |

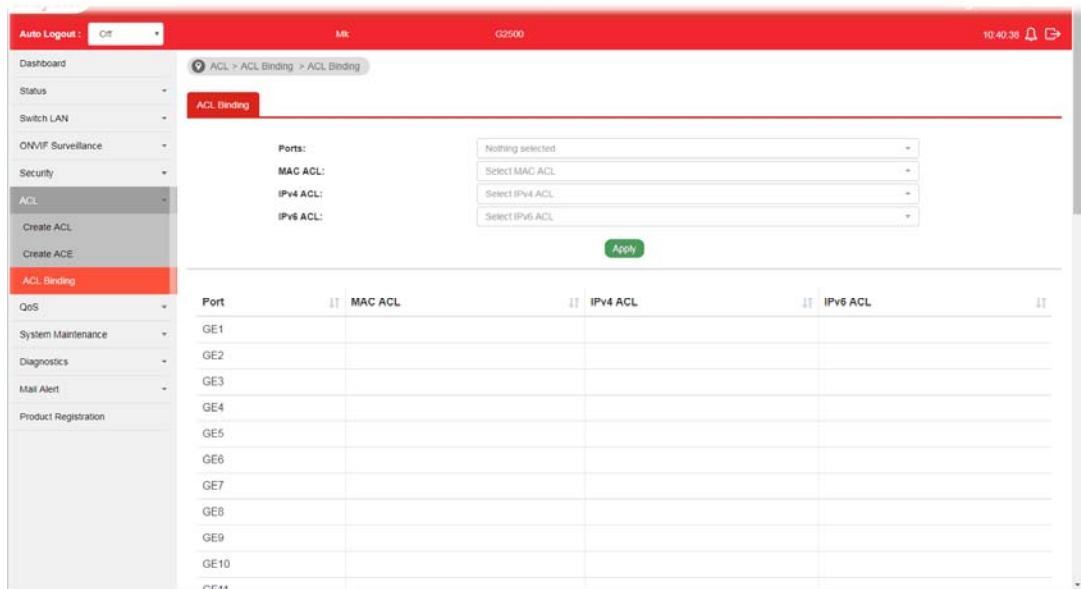


|                                |  |
|--------------------------------|--|
|                                | <p><b>Any</b> - All packets will be filtered.</p> <p>Or, enter the IPv6 address to filter the packets coming from that address.</p>  |
| Service                        | <ul style="list-style-type: none"> <li>● <b>Any</b> - All packets will be filtered.</li> <li>● <b>DSCP</b> - All IP traffic is mapped to queues based on the DSCP field in the IP header. If traffic is not IP traffic, it is mapped to the lowest priority queue.</li> <li>● <b>IP Precedence</b> - All IP traffic is mapped to queues based on the IP Precedence field in the IP header. If traffic is not IP traffic, it is mapped to the lowest priority queue.</li> </ul> |
| Source Port / Destination Port | <p>Specify the source and destination port number for filtering the packets.</p> <ul style="list-style-type: none"> <li>● <b>Any</b> - All packets will be filtered.</li> <li>● <b>Single</b> - Only the packets passing through the number defined here will be filtered.</li> <li>● <b>Range</b> - Only the packets passing through the port range defined here will be filtered.</li> </ul>   |
| ICMP Type                      | <ul style="list-style-type: none"> <li>● <b>Any</b> - All packets will be filtered.</li> <li>● <b>Select</b> - Choose one of the type (e.g., Destination Unreachable Echo Reply, MLD Query...) from the drop down list.</li> <li>● <b>Define</b> - Specify a type number (0 - 255) for ICMP code. For example, 0 means "Echo Reply"; 254 means "RFC3692-style Experiment 2".</li> </ul>  |
| ICMP code                      | <p>Each ICMP type can be defined with different codes. For example, if you define ICMP Type as "3", then the available codes for Type 3 will be 0-15.</p> <p><b>Any</b> - All packets will be filtered.</p> <p>Or, enter 0 to 255 based on the ICMP type specified.</p>  |
| Add                            | Click it to create a new binding profile.  |
| Modify                         | <p> - Click it to modify the settings for the selected profile.</p> <p> - Click it to remove the selected entry.</p>   |

## V-3 ACL Binding

This section allows you to bind Access Control Lists created in previous section to an interface (physical port or aggregation).

A physical port can only be bound with one of the IPv4 and IPv6 ACL, not both.



Available settings are explained as follows:

| Item                          | Description  |
|-------------------------------|--|
| Ports                         | Use the drop down list to select the port profiles (GE1 to GE28) for binding ACL.                                    |
| MAC ACL / IPv4 ACL / IPv6 ACL | Select ACLs (MAC, IPv4, and/or IPv6) to be bound on this interface (port), so Switch may filter packets by using it. |
| Apply                         | Apply the settings to the switch.  |

# Part VI QoS Configuration

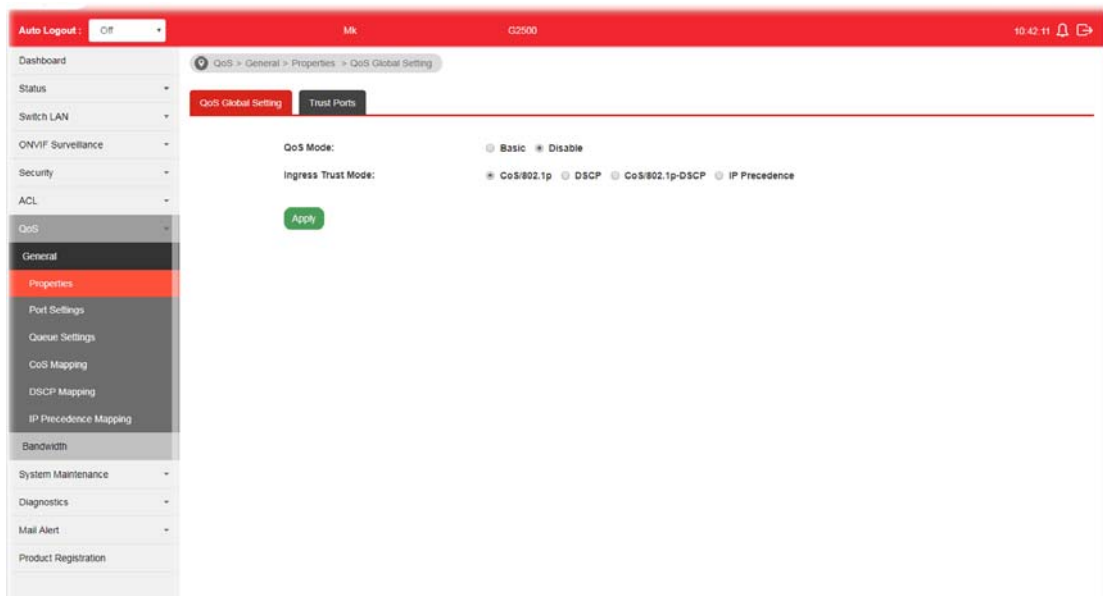
## VI-1 General

QoS (Quality of Service) functions to provide different quality of service for various network applications and requirements and optimize the bandwidth resource distribution so as to provide a network service experience of a better quality.

### VI-1-1 Properties

#### VI-1-1-1 QoS General Setting

This page allows the network administrator to specify Ingress Trust Mode for basic QoS mode.



Available settings are explained as follows:

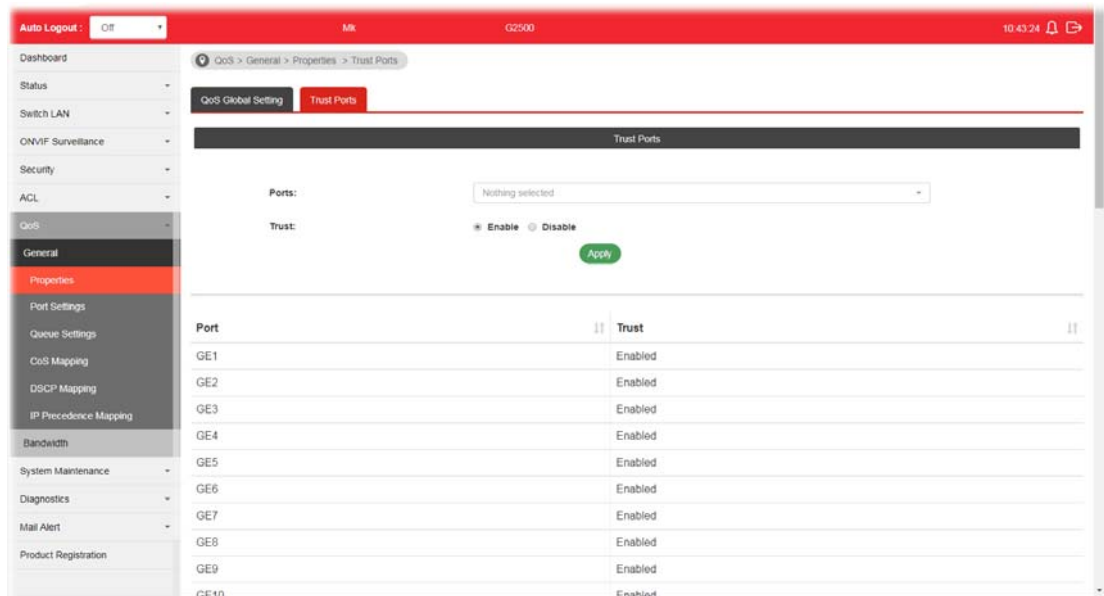
| Item               | Description  |
|--------------------|--|
| QoS Mode           | Disable -Disable the function of QoS mode.<br>Basic - Enable the function of QoS mode.   |
| Ingress Trust Mode | Select the QoS operation mode. <ul style="list-style-type: none"><li>● CoS/802.1p -Traffic is mapped to queues based on the CoS field in the VLAN tag, or based on the per-port default CoS value if there is no VLAN tag on the incoming packet.</li><li>● DSCP - All IP traffic is mapped to queues based on the DSCP field in the IP header. If traffic is not IP traffic, it is mapped to the lowest priority queue.</li><li>● CoS/802.1p-DSCP - All IP traffic is mapped to queues based on the DSCP field in the IP header. If traffic is not IP but has VLAN tag, mapped to queues based on the CoS value in the VLAN tag.</li><li>● IP Precedence - All IP traffic is mapped to queues based on the DSCP field in the IP header. If traffic is not IP but has VLAN tag, mapped to queues based on the CoS value in the VLAN tag.</li></ul> |

Apply

Apply the settings to the switch.

## VI-1-1-2 Trust Ports

This page allows the network administrator to enable the trust mode of basic QoS on each port. Port that is trust disabled will be sent with lowest priority queue. The configuration result for each port will be displayed on the table listed on the lower side of this web page.



Available settings are explained as follows:

| Item  | Description  |
|-------|--|
| Ports | Use the drop down list to select the port profile (GE1 to GE28) or profiles.   |
| Trust | Click Enable to make traffic follow the trust mode in general setting. <ul style="list-style-type: none"><li>● Enable - Traffic will follow trust mode in general setting.</li><li>● Disable - No QoS service for this port.</li></ul> |
| Apply | Apply the settings to the switch.  |

## VI-1-2 Port Settings

This page allows the network administrator to configure port settings for QoS. The configuration result for each port will be displayed on the table listed on the lower side of this web page.

| Port | Ingress Default CoS | Remark CoS | Remark DSCP / IP Precedence | Modify |
|------|---------------------|------------|-----------------------------|--------|
| GE1  | 0                   | Disabled   | Disabled                    |        |
| GE2  | 0                   | Disabled   | Disabled                    |        |
| GE3  | 0                   | Disabled   | Disabled                    |        |
| GE4  | 0                   | Disabled   | Disabled                    |        |
| GE5  | 0                   | Disabled   | Disabled                    |        |
| GE6  | 0                   | Disabled   | Disabled                    |        |

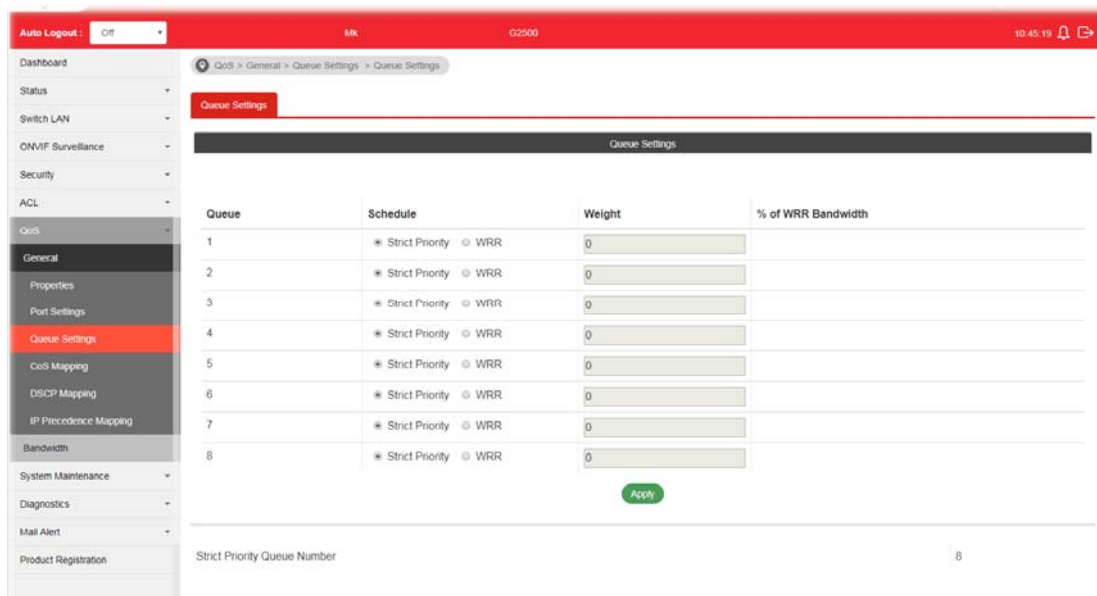
Available settings are explained as follows:

| Item                      | Description   |
|---------------------------|---|
| Ports                     | Use the drop down list to select the port profile (GE1 to GE28) or profiles.  |
| Ingress Default CoS       | Specify the default CoS priority value for those ingress frames without given trust QoS tag (802.1q/DSCP/IP Precedence, depending on configuration).  |
| <b>Egress Remarking</b>   |   |
| Remark CoS                | <ul style="list-style-type: none"> <li>● <b>Disable</b> - Disable CoS remarking function for outgoing packets.</li> <li>● <b>Enable</b> - Egress traffic will be marked with CoS value according to the Queue to CoS mapping table.</li> </ul>  |
| Remark DSCP/IP Precedence | <ul style="list-style-type: none"> <li>● <b>Disable</b> - Disable DSCP/IP Precedence remarking function for outgoing packets.</li> <li>● <b>DSCP</b> - Egress traffic will be marked with DSCP value according to the Queue to DSCP mapping table.</li> <li>● <b>IP Precedence</b> - Egress traffic will be marked with IP Precedence value according to the Queue to IP Precedence mapping table.</li> </ul> |
| Apply                     | Apply the settings to the switch.   |
| Modify                    | - Click it to modify the settings for the selected port profile.  |

## VI-1-3 Queue Settings

VigorSwitch supports multiple queues for each interface. The higher numbered queue represents the higher priority. The following lists the types of supported priority queue:

- Strict Priority (SP) - Egress traffic from the higher priority queue will be transmitted first, lower priority queue shall wait until all traffic in SP queue is transmitted.
- Weighted Round Robin (WRR) - The number of packets sent from the queue is proportional to the weight of the queue.



Available settings are explained as follows:

| Item                         | Description   |
|------------------------------|---|
| Queue                        | There are eight queue ID numbers allowed to be configured.  |
| Schedule                     | <ul style="list-style-type: none"> <li>● <b>Strict Priority</b> - Click it to set queue to strict priority type.</li> <li>● <b>WRR</b> - Click it to set queue to Weight round robin type.</li> </ul> |
| Weight                       | If the queue type is WRR, set the queue weight for the queue.   |
| % of WRR Bandwidth           | Display the percentage of traffic which can be sent by current queue compared to total WRR queues.  |
| Apply                        | Apply the settings to the switch.   |
| Strict Priority Queue Number | Display the number of queues using Strict Priority method.  |

## VI-1-4 CoS Mapping

This section allows user to configure how ingress frames with CoS/802.1p tag map to QoS queues, and QoS queues to CoS/802.1p on egress frames.

Actual effectiveness is based on how QoS is configured in previous QoS section. This page provides settings for user to configure mapping only.

Available settings are explained as follows:

| Item  | Description  |
|---|--|
| <b>CoS to Queue Mapping (for Ingress) - Settings for incoming packets.</b>          |  |
| Class of Service  | Display the class of service value (0 to 7).                               |
| Queue   | Define the queue ID (level 1 to 8) for different class of service values.  |
| <b>Queue to CoS Mapping (for Egress Remarking) - Settings for outgoing packets.</b> |  |
| Queue   | Display the queue ID (level 1 to 8) for different class of service values. |
| Class of Service  | Define the class of service value (0 to 7).                                |
| Apply   | Apply the settings to the switch.  |



## VI-1-5 DSCP Mapping

This section allows user to configure how ingress packets with DSCP tag map to QoS queues, and QoS queues to DSCP on egress packets.

Actual effectiveness is based on how QoS is configured in previous QoS section. This page provides settings for user to configure mapping only.

Available settings are explained as follows:

| Item   | Description  |
|--|--|
| <b>DSCP to Queue Mapping (for Ingress) - Settings for the incoming packets.</b>      |  |
| DSCP   | Display the DSCP value (0 to 7).                               |
| Queue  | Define the queue ID (level 1 to 8) for different DSCP values.  |
| <b>Queue to DSCP Mapping (for Egress Remarking) - Settings for outgoing packets.</b> |  |
| Queue  | Display the queue ID (level 1 to 8) for different DSCP values. |
| DSCP   | Define the DSCP value (0 to 7).                                |
| Apply  | Apply the settings to the switch.                              |

## VI-1-6 IP Precedence Mapping

This section allows user to configure how ingress packets with IP Precedence tag map to QoS queues, and QoS queues to IP Precedence on egress packets.

Actual effectiveness is based on how QoS is configured in previous QoS section. This page provides settings for user to configure mapping only.

The screenshot shows the configuration page for IP Precedence Mapping. The interface includes a sidebar with navigation options like Dashboard, Status, Switch LAN, ONVIF Surveillance, Security, ACL, QoS, General, Properties, Port Settings, Queue Settings, CoS Mapping, DISCP Mapping, IP Precedence Mapping, Bandwidth, System Maintenance, Diagnostics, Mail Alert, and Product Registration. The main content area is titled 'IP Precedence Mapping' and contains two tables:

| IP Precedence to Queue Mapping (for Ingress) |       |
|--|-------|
| IP Precedence                                | Queue |
| 0  | 1     |
| 1  | 2     |
| 2  | 3     |
| 3  | 4     |
| 4  | 5     |
| 5  | 6     |
| 6  | 7     |
| 7  | 8     |

| Queue to IP Precedence Mapping (for Egress Remarking) |               |
|---|---------------|
| Queue   | IP Precedence |
| 1   | 0             |
| 2   | 1             |
| 3   | 2             |
| 4   | 3             |
| 5   | 4             |
| 6   | 5             |

Available settings are explained as follows:

| Item  | Description   |
|---|---|
| <b>IP Precedence to Queue Mapping (for Ingress) - Settings for the incoming packets.</b>      |   |
| IP Precedence   | Display the IP Precedence value (0 to 7).                               |
| Queue   | Define the queue ID (level 1 to 8) for different IP Precedence values.  |
| <b>Queue to IP Precedence Mapping (for Egress Remarking) - Settings for outgoing packets.</b> |   |
| Queue   | Display the queue ID (level 1 to 8) for different IP Precedence values. |
| IP Precedence   | Define the IP Precedence value (0 to 7).                                |
| Apply   | Apply the settings to the switch.                                       |

## VI-2 Bandwidth

Use the bandwidth setting pages to define values that determine how much traffic the switch can receive and send on specific port or queue.


### V-2-1 Ingress Rate Limit

This page allows a user to configure ingress port rate limit. The ingress rate limit is the number of bits per second that can be received from the ingress interface. Excess bandwidth above this limit is discarded. The configuration result for each port will be displayed on the table listed on the lower side of this web page.

The screenshot shows the 'Ingress Rate Limit' configuration page. On the left is a navigation menu with 'Bandwidth' > 'Ingress Rate Limit' selected. The main area contains configuration fields: 'Ports' (a dropdown menu currently showing 'Nothing selected'), 'State' (radio buttons for 'Enable' and 'Disable'), and 'Rate (Kbps)' (a text input field with a range of 16-1000000 and a note 'multiple of 16'). An 'Apply' button is below these fields. At the bottom is a table with columns 'Port', 'Rate Limit (Kbps)', and 'Modify'.

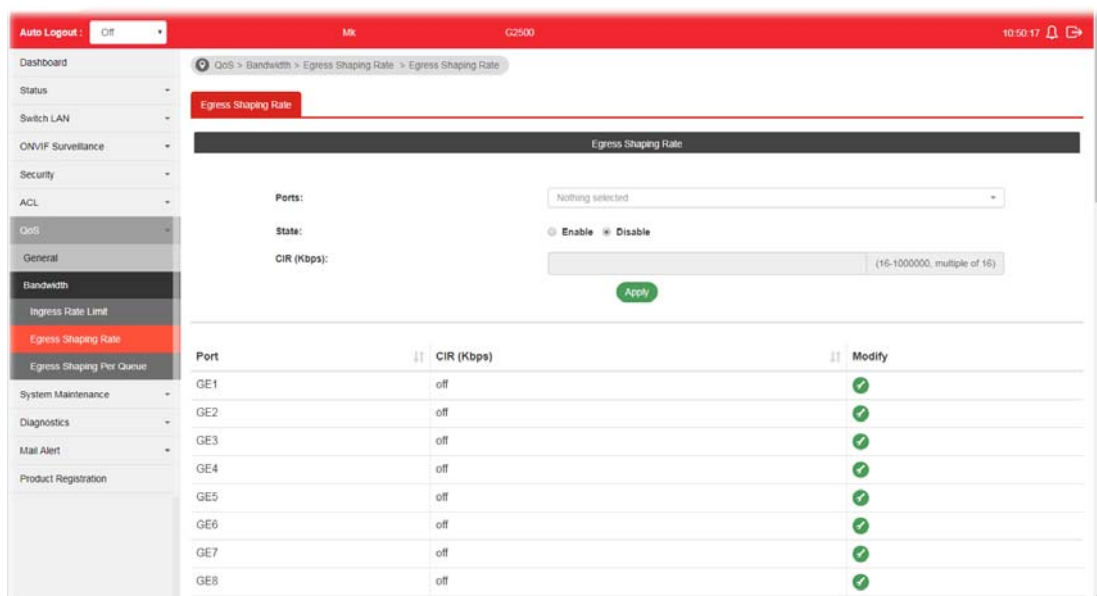
| Port | Rate Limit (Kbps) | Modify |
|------|-------------------|--------|
| GE1  | off               | ✓      |
| GE2  | off               | ✓      |
| GE3  | off               | ✓      |
| GE4  | off               | ✓      |
| GE5  | off               | ✓      |
| GE6  | off               | ✓      |
| GE7  | off               | ✓      |
| GE8  | off               | ✓      |

Available settings are explained as follows:


| Item                      | Description  |
|---------------------------|--|
| <b>Ingress Rate Limit</b> |  |
| Ports                     | Use the drop down list to select the port profile (GE1 to GE28) or profiles.   |
| State                     | <ul style="list-style-type: none"> <li>● <b>Disable</b> - Disable ingress bandwidth control.</li> <li>● <b>Enable</b> - Enable ingress bandwidth control.</li> </ul> |
| Rate (Kbps)               | Enter the rate value, <16-1000000>, unit: 16 Kbps.   |
| Apply                     | Apply the settings to the switch.  |
| Modify                    |  - Click it to modify the settings for the selected port profile.                 |

## VI-2-2 Egress Shaping Rate

This page allows a user to configure egress port rate limit. The egress rate limit is the number of bits per second that can be received from the egress interface. Excess bandwidth above this limit is discarded.



Available settings are explained as follows:

| Item                        | Description  |
|-----------------------------|--|
| <b>Egress Shapping Rate</b> |  |
| Ports                       | Use the drop down list to select the port profile (GE1 to GE28) or profiles.   |
| State                       | <ul style="list-style-type: none"> <li>● <b>Disable</b> - Disable egress bandwidth control.</li> <li>● <b>Enable</b> - Enable egress bandwidth control.</li> </ul> |
| CIR (Kbps)                  | Enter the rate value,<16-1000000>,unit:16 Kbps.  |
| Apply                       | Apply the settings to the switch.  |
| Modify                      |  - Click it to modify the settings for the selected port profile.               |

## VI-2-3 Egress Shaping Per Queue

This page allows user to configure the maximum egress bandwidth not only by port but also by specific QoS queues. The configuration result for each port will be displayed on the table listed on the lower side of this web page.

Available settings are explained as follows:

| Item                             | Description  |
|----------------------------------|--|
| <b>Egress Shapping Per Queue</b> |  |
| Port                             | Use the drop down list to select the port profile (GE1 to GE28) or profiles.   |
| Queue                            | Use the drop down list to select queue number (1 to 8) for the selected GE port.   |
| State                            | <ul style="list-style-type: none"> <li>● Disable - Disable egress bandwidth control.</li> <li>● Enable - Enable egress bandwidth control.</li> </ul> |
| CIR (Kbps)                       | Enter the rate value,<16-1000000>,unit:16 Kbps.  |
| Apply                            | Apply the settings to the switch.  |

This page is left blank.

# Part VII System Maintenance

## VII-1 TR-069

This page allows a user to configure TR-069 settings for connecting to VigorACS 2.

The screenshot shows the 'TR-069 Setting' page in the VigorSwitch G2500 web interface. The page is titled 'TR-069 Setting' and is part of the 'System Maintenance' menu. It is divided into three main sections: 'ACS Settings', 'CPE Settings', and 'Periodic Inform Settings'.  
**ACS Settings:** This section allows users to enable or disable TR-069. It includes a 'URL' field with a 'Wizard' button, a 'Username' field, a 'Password' field, and a 'Last Inform' status showing 'Successfully, 2019-09-04 10:50:49'. A 'Test Inform' button is labeled 'Test With Inform'.  
**CPE Settings:** This section allows users to configure the CPE client. It includes a 'CPE Client' dropdown (set to HTTP), a 'URL' field, a 'Port' field (set to 8069), a 'Username' field (set to vigor), and a 'Password' field.  
**Periodic Inform Settings:** This section is currently empty.

Available settings are explained as follows:

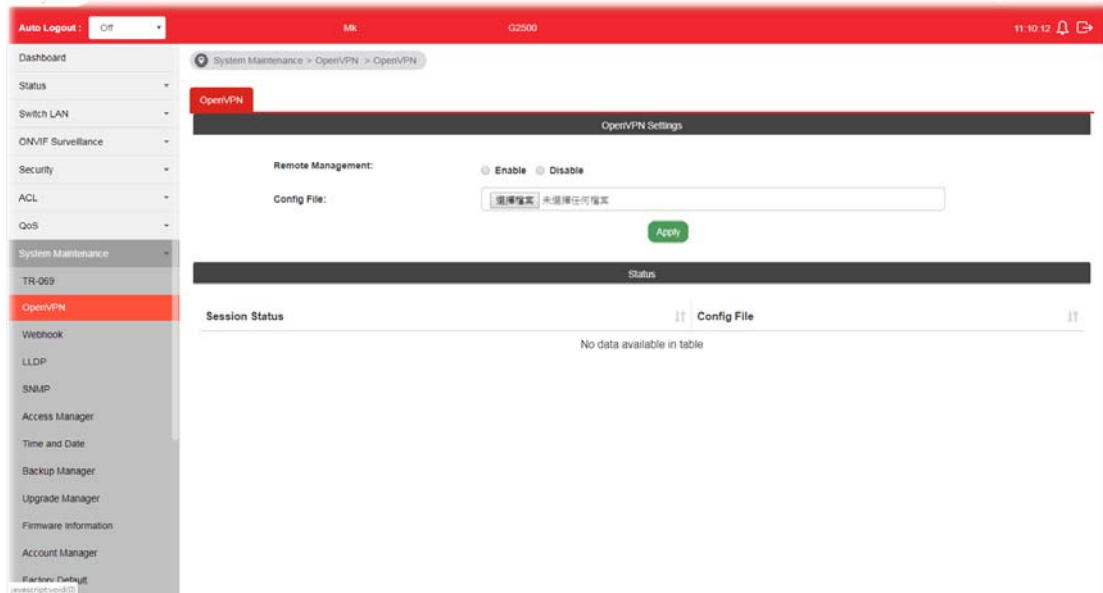
| Item         | Description   |
|--------------|---|
| ACS Settings | <ul style="list-style-type: none"> <li>● <b>TR-069</b> - Click <b>Enable</b> to activate the settings on this page.</li> <li>● <b>URL</b> - The URL must be entered according to the ACS (Auto Configuration Server) you want to link.</li> <li>● <b>Wizard</b> - Click it to enter the IP address of VigorACS server, port number and the handler.</li> <li>● <b>Username</b> - The string of username must be entered according to the VigorACS (Auto Configuration Server) you want to link.</li> <li>● <b>Password</b> - The password must be entered according to the VigorACS (Auto Configuration Server) you want to link.</li> <li>● <b>Last Inform</b> - Display the time that VigorACS server makes a response while receiving Inform message from CPE last time.</li> <li>● <b>Test Inform</b> - Click <b>Test With Inform</b> to send a message to test if such CPE is able to communicate with VigorACS server.</li> </ul> |
| CPE Settings | <ul style="list-style-type: none"> <li>● <b>CPE Client</b> - Choose HTTP or HTTPS for connecting with VigorACS.</li> <li>● <b>URL</b> - Display the URL of VigorSwitch.</li> <li>● <b>Port</b> - Type the username and password that VigorACS can use to access into this switch.</li> <li>● <b>Username</b> - Enter the username that VigorACS can use to access into this switch.</li> <li>● <b>Password</b> - Enter the password that VigorACS can use to access into this switch.</li> </ul>  |



|                          |  |
|--------------------------|--|
| Periodic Inform Settings | <ul style="list-style-type: none"> <li>● <b>Periodic Inform Settings</b> - Click <b>Enable</b> to configure the interval time.</li> <li>● <b>Interval Time</b> - Set the interval time for the switch to send notification to CPE.</li> </ul>  |
| STUN Settings            | <ul style="list-style-type: none"> <li>● <b>STUN Settings</b> - Click <b>Enable</b> to configure STUN settings.</li> <li>● <b>Server Address</b> - Enter the IP address of the STUN server.</li> <li>● <b>Server Port</b> - Enter the port number of the STUN server.</li> <li>● <b>Minimum Keep Alive Period</b> - If STUN is enabled, the switch must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the minimum period. The default setting is "60 seconds".</li> <li>● <b>Maximum Keep Alive Period</b> - If STUN is enabled, the switch must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the maximum period. A value of "-1" indicates that no maximum period is specified.</li> </ul> |
| Health Check             | <p>Vigor system will check the health status of LAN ports including link up /down or speed change.</p> <ul style="list-style-type: none"> <li>● <b>Port Link Up/Down</b> - Select LAN port(s) to do the health check of port link.</li> <li>● <b>Link Speed Change</b> - Select LAN port(s) to do the health check of speed change.</li> </ul>   |
| Apply                    | Apply the settings to the switch.  |
| Clear                    | Discard current settings.  |

## VII-2 OpenVPN

Devices connecting to VigorSwitch can transmit data to remote end via OpenVPN to ensure the information security.

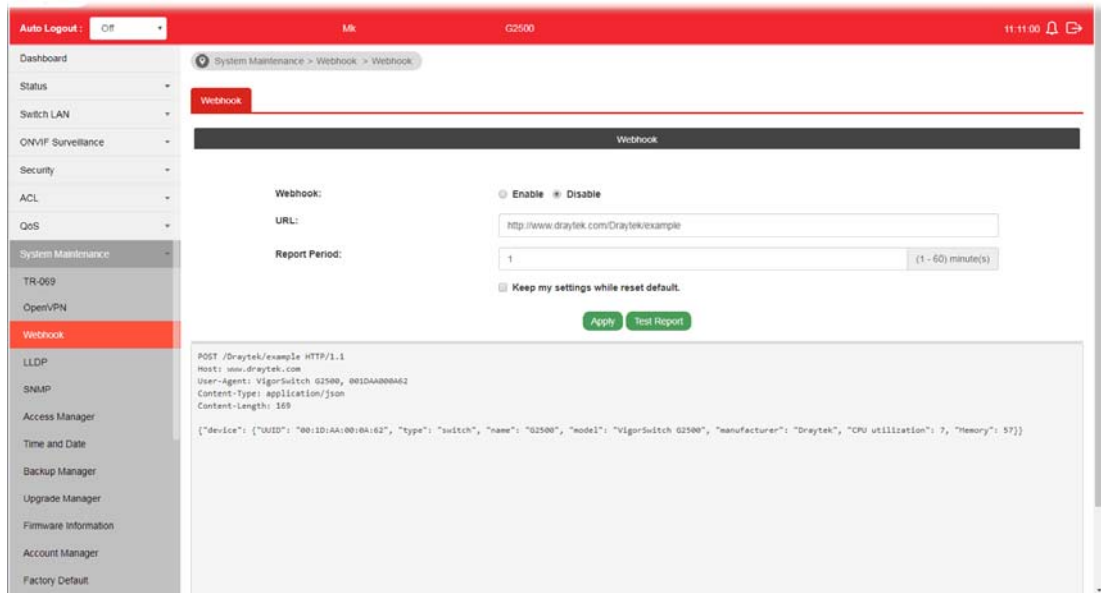


Available settings are explained as follows:

| Item              | Description  |
|-------------------|--|
| Remote Management | <b>Enable</b> - Click it to enable OpenVPN tunnel between VigorSwitch with the remote end.<br><b>Disable</b> - Click it to disable OpenVPN tunnel. |
| Config File       | As a VPN client, please import the OpenVPN config file coming from OpenVPN server.   |
| Apply             | Save and apply the settings to the switch.   |
| Status            | Display current OpenVPN status (Disabled, Connecting or Success) and configuration file used.  |

## VII-3 Webhook

Without getting any request, VigorSwitch will send the data (if available) that a user concerned to the specified URL (provided by remote client) automatically.



Available settings are explained as follows:

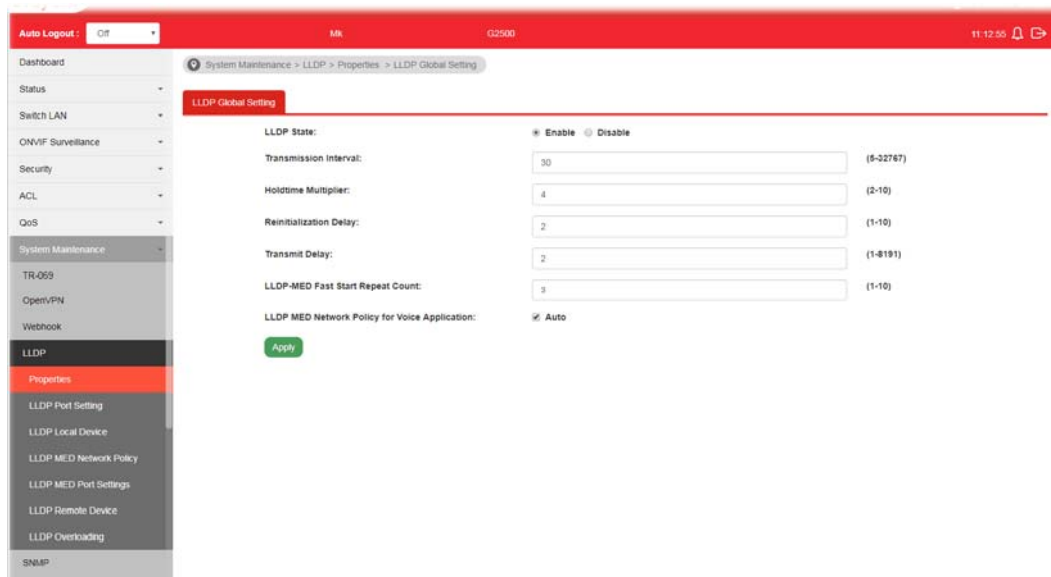
| Item          | Description   |
|---------------|---|
| Webhook       | <b>Enable</b> - Click it to enable the webhook service. The data will be transmitted to the specified URL.<br><b>Disable</b> -Click it to disable the webhook service.                                  |
| URL           | Specify the destination to receive the real-time data by entering the URL.<br>Please get the URL from the client who wants to obtain the newest and available data automatically from the Vigor switch. |
| Report Period | Set the transmission interval (unit is minute).<br><b>Keep my settings while rest default</b> - Check the box to keep the webhook configuration when resetting VigorSwitch with default settings.       |
| Apply         | Apply the settings to the switch.   |
| Test Report   | Vigor system will send a test report to the remote address.   |

## VII-4 LLDP

LLDP is a one-way protocol; there are no request/response sequences. Information is advertised by stations implementing the transmit function, and is received and processed by stations implementing the receive function. The LLDP category contains LLDP and LLDP-MED pages.

### VII-4-1 Properties

This page allows a user to set general settings for LLDP.



Available settings are explained as follows:


| Item  | Description   |
|---|---|
| LLDP State                                    | <ul style="list-style-type: none"><li>● Enable - Enable LLDP protocol on this switch.</li><li>● Disable - Disable LLDP protocol on this switch.</li></ul> |
| Transmission Interval                         | Select the interval at which frames are transmitted. The default is 30 seconds, and the valid range is 5-32768seconds.                                    |
| Holdtime Multiplier                           | Select the multiplier on the transmit interval to assign to TTL (range 2-10, default = 4).  |
| Reinitialization Delay                        | Select the delay before a re-initialization (range 1-10 seconds, default = 2).  |
| Transmit Delay                                | Select the delay after an LLDP frame is sent (range 1-8192 seconds, default = 3).   |
| LLDP-MED Fast Start Repeat Count              | Select the number of LLDP packets that will be sent during LLDP-MED Fast Start period.<br>The default is 3. Available range is from 1 to 10.              |
| LLDP MED Network Policy for Voice Application | The default is Auto.  |
| Apply   | Apply the settings to the switch.   |

## VII-4-2 LLDP Port Setting

This page allows a user to select specified port or all ports to configure LLDP state.

| Port | State | Selected Optional TLVs                       | Selected VLAN | Modify |
|------|-------|--|---------------|--------|
| GE1  | TX&RX | System Name, Port Description, 802.3 MAC-PHY |               | ✓      |
| GE2  | TX&RX | System Name, Port Description, 802.3 MAC-PHY |               | ✓      |
| GE3  | TX&RX | System Name, Port Description, 802.3 MAC-PHY |               | ✓      |
| GE4  | TX&RX | System Name, Port Description, 802.3 MAC-PHY |               | ✓      |
| GE5  | TX&RX | System Name, Port Description, 802.3 MAC-PHY |               | ✓      |
| GE6  | TX&RX | System Name, Port Description, 802.3 MAC-PHY |               | ✓      |
| GE7  | TX&RX | System Name, Port Description, 802.3 MAC-PHY |               | ✓      |
| GE8  | TX&RX | System Name, Port Description, 802.3 MAC-PHY |               | ✓      |
| GE9  | TX&RX | System Name, Port Description, 802.3 MAC-PHY |               | ✓      |

Available settings are explained as follows:

| Item          | Description   |
|---------------|---|
| Ports         | Use the drop down list to select the port (GE1 to GE50) or ports for device check.  |
| State         | <ul style="list-style-type: none"> <li>● <b>Disable</b> - Disable the transmission of LLDP PDUs.</li> <li>● <b>TX&amp;RX</b> - Transmit and receive LLDP PDUs both.</li> <li>● <b>TX Only</b> - Transmit LLDP PDUs only.</li> <li>● <b>RX Only</b> - Receive LLDP PDUs only.</li> </ul>   |
| Optional TLVs | <p>Within data communication protocols, optional information may be encoded as a type-length-value or TLV element inside a protocol. TLV is also known as tag-length value.</p> <p>The type and length are fixed in size (typically 1-4 bytes), and the value field is of variable size.</p> <p>Select the LLDP optional TLVs to be carried (multiple selection is allowed).</p> <p>Available items include System Name, Port Description, System Description, System Capability, 802.3 MAC-PHY, 802.3 Link Aggregation, 802.3 Maximum Frame Size, Management Address and 802.1 PVID.</p> |
| VLAN          | Select the VLAN ID number to be performed (multiple selections are allowed).  |
| Apply         | Apply the settings to the switch.   |
| Modify        |  - Click it to modify the settings for the selected port profile.  |

---

✕

### Edit Port GE1

**State**

TX&RX▼

**Optional TLVs**

System Name, Port Description, 802.3 MAC-PHY▼

**VLAN**

Nothing selected▼

OK Cancel

---

## VII-4-3 LLDP Local Device

This page displays information for LLDP Local Device.

The screenshot shows the LLDP Local Device configuration page. The left sidebar contains navigation options like Dashboard, Status, Switch LAN, ONMP Surveillance, Security, ACL, QoS, System Maintenance, TR-069, OpenVPN, Webhook, LLDP, Properties, LLDP Port Setting, LLDP Local Device (selected), LLDP MED Network Policy, LLDP MED Port Settings, LLDP Remote Device, and LLDP Overloading. The main content area is titled 'LLDP Local Device' and contains two sections: 'Device Summary' and 'Port Details'.

| Name                   | Value  |
|------------------------|--|
| Chassis ID Subtype     | MAC Address  |
| Chassis ID             | 00-1D-AA-00-0A-62  |
| System Name            | G2500  |
| System Description     | 44-Port 10/100/1000BaseT + 4-Port 100M/1000M Combo SFP + 2-Port 100M/1000M ... |
| Capabilities Supported | Bridge   |
| Capabilities Enabled   | Bridge   |
| Port ID Subtype        | Interface name   |

| Port | LLDP State | Detail |
|------|------------|--------|
| GE1  | TX&RX      |        |
| GE2  | TX&RX      |        |
| GE3  | TX&RX      |        |
| GE4  | TX&RX      |        |
| GE5  | TX&RX      |        |

Available settings are explained as follows:

| Item           | Description  |
|----------------|--|
| Device Summary | <p>Display a summary of the LLDP information for this switch.</p> <ul style="list-style-type: none"> <li>● <b>Chassis ID Subtype</b> - Display the type of chassis ID, such as the MAC address.</li> <li>● <b>Chassis ID</b> - Display Identifier of chassis. Where the chassis ID subtype is a MAC address, the MAC address of the switch is displayed.</li> <li>● <b>System Name</b> - Display model name of switch.</li> <li>● <b>System Description</b> - Display description of switch.</li> <li>● <b>Capabilities Supported</b> - Display the primary functions of the device, such as Bridge, WLAN AP, or Router.</li> <li>● <b>Capabilities Enabled</b> - Primary enabled functions of the device.</li> <li>● <b>Port ID Subtype</b> - Display the type of the port identifier that is shown.</li> </ul> |
| Port Details   | <p>Display detailed information of the selected GE port.</p> <p> <b>Detail</b> - Click the button under it to review the detailed information contained in TLVs sent out from each interface, containing MAC/PHY, 802.3, 802.3 Link Aggregation, 802.1 VLAN and Protocol for each LAN port (GE1 to GE50).</p>  |

## VII-4-4 MED Network Policy

This page allows the network administrator to set MED (Media Endpoint Discovery) network policy.

| Policy ID | Policy Enabled | Application | VLAN ID | Tagged/Untagged | Priority | DSCP |
|-----------|----------------|-------------|---------|-----------------|----------|------|
| 1         | Disabled       | Unknown     | 0       | Untagged        | 0        | 0    |
| 2         | Disabled       | Unknown     | 0       | Untagged        | 0        | 0    |
| 3         | Disabled       | Unknown     | 0       | Untagged        | 0        | 0    |
| 4         | Disabled       | Unknown     | 0       | Untagged        | 0        | 0    |

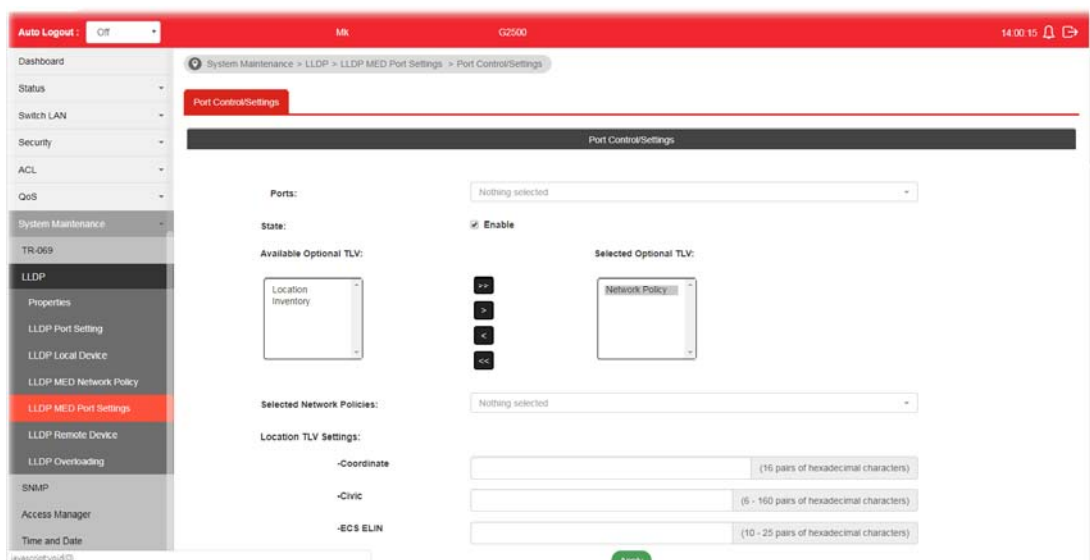
Available settings are explained as follows:

| Item          | Description  |
|---------------|--|
| Policy ID     | Choose a number for configuring the policy profile.<br>Available selections include 1 to 32.   |
| Enable Policy | <b>Enable</b> - Click it to enable such function.  |
| Application   | There are several applications which can be used for MED network.<br>Selections include Voice Signaling, Guest Voice, Guest Voice Signaling, Softphone Voice, Video Conferencing, Stream Video and Video Signaling.                        |
| VLAN          | Set a VLAN ID (ranging from 1 to 4095) for such profile.   |
| VLAN Tag      | Specify if the outgoing packets will be tagged or not. <ul style="list-style-type: none"> <li>● <b>Untag</b> - Packets will be sent out without any tag.</li> <li>● <b>Tag</b> - Packets will be sent out with a number tagged.</li> </ul> |
| Priority      | Set Layer2 priority (range from 0 to 7).   |
| DSCP          | Set DSCP value (range form 0 to 63).   |
| Apply         | Apply the settings to the switch.  |



## VII-4-5 LLDP MED Port Settings

This page allows the network administrator to configure TLV (Type / Length / Value) settings for each port.



Available settings are explained as follows:

| Item                      | Description  |
|---------------------------|--|
| Ports                     | Choose the port(s) for configuring TLV settings.   |
| State                     | Enable - Click it to enable LLDP MED on the selected port.   |
| Available Optional TLV    | Available TLV items will be shown in this field.<br>Choose the one(s) you want and click the >> arrow to transfer the selection(s) to the field of "Selected Optional TLV".  |
| Selected Optional TLV     | Display the selected TLV items.  |
| Selected Network Policies | Select network policy profiles (created in LLDP>>LLDP MED Network Policy) for applying onto the selected port.   |
| Location TLV Settings     | Define the location, civic address and ECS ELIN for LLDP protocol. <ul style="list-style-type: none"> <li>● <b>Coordinate</b> -Enter the coordinate location in 16 pairs of hexadecimal characters.</li> <li>● <b>Civic</b> - Enter the civic address in 6 ~ 160 pairs of hexadecimal characters.</li> <li>● <b>ECS ELIN</b> - Enter the ECS (Emergency Call Service) ELIN (Emergency Location Identification Number) in 10 ~ 25 pairs of hexadecimal characters.</li> </ul> |
| Apply                     | Apply the settings to the switch.  |

## VII-4-6 LLDP Remote Device

This page allows the network administrator to view the information sent from neighboring devices by LLDP protocol.

| Local Port | Chassis ID Subtype | Chassis ID        | Port ID Subtype  | Port ID | System Name | Time to Live | Details | Delete |
|------------|--------------------|-------------------|------------------|---------|-------------|--------------|---------|--------|
| GE2        | MAC address        | 00 1D AA 43 C9... | Locally assigned | g6      | G2280x      | 109          | ✓       | ✗      |
| GE4        | MAC address        | 00 1D AA 4B C...  | Locally assigned | g1      | G2500       | 119          | ✓       | ✗      |
| GE26       | MAC address        | 00 E0 4C 00 0B... | Locally assigned | g5      |             | 118          | ✓       | ✗      |

Available settings are explained as follows:

| Item               | Description   |
|--------------------|---|
| Local Port         | Display the number of the local port to which the neighbor is connected.                            |
| Chassis ID Subtype | Display the type of chassis ID (for example, MAC address).  |
| Chassis ID         | Display the identifier of the 802 LAN neighboring device's chassis.                                 |
| Port ID Subtype    | Display the type of port identifier.  |
| Port ID            | Display the number of port identifier.  |
| System Name        | Display the name of the switch.   |
| Time to Live       | Display the time interval in seconds after which the information for remote device will be deleted. |
| Details            | Display detailed information contained in TLVs sent out from neighboring devices.                   |
| Delete             | Click it to remove information of the selected port.  |

## VII-4-7 LLDP Overloading

This page allows user to review current size, overall size of LLDP packet and whether it is to exceed maximum allowed size of single LLDP packet.

| Port | Total(Bytes) | Left to Send(Bytes) | Status          | Mandatory TLVs  | 802.3 TLVs      | Optional TLVs  | 802.1 TLVs     |
|------|--------------|---------------------|-----------------|-----------------|-----------------|----------------|----------------|
| GE1  | 68           | 1420                | Not Overloading | 21(Transmitted) | 11(Transmitted) | 9(Transmitted) | 8(Transmitted) |
| GE2  | 68           | 1420                | Not Overloading | 21(Transmitted) | 11(Transmitted) | 9(Transmitted) | 8(Transmitted) |
| GE3  | 68           | 1420                | Not Overloading | 21(Transmitted) | 11(Transmitted) | 9(Transmitted) | 8(Transmitted) |
| GE4  | 68           | 1420                | Not Overloading | 21(Transmitted) | 11(Transmitted) | 9(Transmitted) | 8(Transmitted) |
| GE5  | 68           | 1420                | Not Overloading | 21(Transmitted) | 11(Transmitted) | 9(Transmitted) | 8(Transmitted) |
| GE6  | 68           | 1420                | Not Overloading | 21(Transmitted) | 11(Transmitted) | 9(Transmitted) | 8(Transmitted) |
| GE7  | 68           | 1420                | Not Overloading | 21(Transmitted) | 11(Transmitted) | 9(Transmitted) | 8(Transmitted) |
| GE8  | 68           | 1420                | Not Overloading | 21(Transmitted) | 11(Transmitted) | 9(Transmitted) | 8(Transmitted) |
| GE9  | 68           | 1420                | Not Overloading | 21(Transmitted) | 11(Transmitted) | 9(Transmitted) | 8(Transmitted) |
| GE10 | 69           | 1419                | Not Overloading | 22(Transmitted) | 11(Transmitted) | 9(Transmitted) | 8(Transmitted) |
| GE11 | 69           | 1419                | Not Overloading | 22(Transmitted) | 11(Transmitted) | 9(Transmitted) | 8(Transmitted) |
| GE12 | 69           | 1419                | Not Overloading | 22(Transmitted) | 11(Transmitted) | 9(Transmitted) | 8(Transmitted) |
| GE13 | 69           | 1419                | Not Overloading | 22(Transmitted) | 11(Transmitted) | 9(Transmitted) | 8(Transmitted) |
| GE14 | 69           | 1419                | Not Overloading | 22(Transmitted) | 11(Transmitted) | 9(Transmitted) | 8(Transmitted) |
| GE15 | 69           | 1419                | Not Overloading | 22(Transmitted) | 11(Transmitted) | 9(Transmitted) | 8(Transmitted) |
| GE16 | 69           | 1419                | Not Overloading | 22(Transmitted) | 11(Transmitted) | 9(Transmitted) | 8(Transmitted) |

Available settings are explained as follows:

| Item                | Description  |
|---------------------|--|
| Port                | Display the name of the port.  |
| Total(Bytes)        | Display the total number of bytes of LLDP information in each packet.                            |
| Left to Send(Bytes) | Display the total number of available bytes left for additional LLDP information in each packet. |
| Status              | Display if LLDP TLVs has overloaded the PDU maximum size or not.                                 |
| Mandatory TLVs      | Display how many bytes used by mandatory TLVs.   |
| 802.3 TLVs          | Display how many bytes used by 802.3 TLVs.   |
| Optional TLVs       | Displays how many bytes used by optional TLVs.   |
| 802.1 TLVs          | Displays how many bytes used by 802.1 TLVs.  |

---

## VII-5 SNMP

Simple Network Management Protocol (SNMP) is an "Internet-standard protocol for managing devices on IP networks". Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks and more.

SNMP is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

SNMP is a component of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF). It consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects.

An SNMP-managed network consists of three key components:

- Managed device
- Agent - software which runs on managed devices
- Network management station (NMS) - software which runs on the manager

A managed device is a network node that implements an SNMP interface that allows unidirectional (read-only) or bidirectional (read and write) access to node-specific information. Managed devices exchange node-specific information with the NMSs. Sometimes called network elements, the managed devices can be any type of device, including, but not limited to, routers, access servers, switches, bridges, hubs, IP telephones, IP video cameras, computer hosts, and printers.

An agent is a network-management software module that resides on a managed device. An agent has local knowledge of management information and translates that information to or from an SNMP-specific form.

A network management station (NMS) executes applications that monitor and control managed devices. NMSs provide the bulk of the processing and memory resources required for network management. One or more NMSs may exist on any managed network.

## VII-5-1 View

This page allows the network administrator to create MIB views (Management information base) and then include or exclude OID (Object Identifier) in a view.

The screenshot shows the 'SNMP View' configuration page. The breadcrumb trail is 'System Maintenance > SNMP > View > View'. The main content area has the following fields:

- View Name:** [Text input field]
- OID Subtree:** [Text input field]
- Type:**  Included  Excluded

A green 'Add' button is located below the form. Below the form is a table with the following columns: View, OID Subtree, Type, and Delete.

| View | OID Subtree | Type     | Delete |
|------|-------------|----------|--------|
| all  | 1           | Included |        |


Available settings are explained as follows:

| Item        | Description   |
|-------------|---|
| View Name   | Enter a name of the MIB view.                                     |
| OID Subtree | Enter an OID string to be included or excluded from the MIB view. |
| Type        | Determine to include or exclude the selected MIBs.                |
| Apply       | Apply the settings to the switch.                                 |

## VII-5-2 Group

This page allows the network administrator to group SNMP users and assign different authorization and access privileges.

Available settings are explained as follows:

| Item           | Description  |
|----------------|--|
| Group Name     | Enter a name for the group.  |
| Version        | Specify SNMP version.  |
| Security Level | Specify SNMP security level for the group. It is available when SNMPv3 is selected. <ul style="list-style-type: none"> <li>● <b>No Security</b> - No authentication and no encryption.</li> <li>● <b>Authentication</b> - Requires authentication but no encryption.</li> <li>● <b>Authentication and Privacy</b> - Requires authentication and encryption.</li> </ul> |
| Read View      | <b>Enabled</b> - Users of this group have the right to read the selected MIB view.<br>Use the drop down list to select one of the views. The default is "all", which means the group user can read all MIB views.  |
| Write View     | <b>Enabled</b> - Users of this group have the right to write the selected MIB view.<br>Use the drop down list to select one of the views. The default is "all", which means the group user can write all MIB views.  |
| Notify View    | <b>Enabled</b> - Users of this group have the right to send notification for the selected MIB view.<br>Use the drop down list to select one of the views. The default is "all", which means the group user have the right to send notification for all MIB views.  |
| Add            | Click it to create a new group profile.  |
| Edit           |  - Click it to modify the settings for the selected group.  |



- click it to remove the selected group.

---

## VII-5-3 Community

This page allows a user to add/remove multiple communities of SNMP.

Available settings are explained as follows:

| Item           | Description   |
|----------------|---|
| Community Name | Enter a name as community name. The maximum length of the text is limited to 23 characters.   |
| Type           | <ul style="list-style-type: none"> <li>● <b>Basic</b> - View and access right can be specified for such SNMP community profile.</li> <li>● <b>Advanced</b> - Specify one of the SNMP groups for such SNMP community profile.</li> </ul> |
| View           | Simply specify one of the view profiles (created in <b>SNMP&gt;&gt;View</b> ) from the drop down list.  |
| Access Right   | <ul style="list-style-type: none"> <li>● <b>Read Only</b> - It allows unidirectional access to node-specific information.</li> <li>● <b>Read &amp; Write</b> - It allows bidirectional access to node-specific information.</li> </ul>  |
| Group          | Specify the SNMP group configured by user ( <b>SNMP&gt;&gt;Group</b> ) to define the object available to the community.   |
| Add            | Click it to add a new community.  |
| Delete         | Click the icon to remove the selected community strings.  |



## VII-5-4 User


This page allows a user to configure SNMP user profile.

The screenshot shows the 'SNMP User' configuration page. The left sidebar contains a navigation menu with 'User' highlighted. The main content area has the following fields:

- User Name:** A text input field.
- Group:** A dropdown menu with 'test\_name' selected.
- Security Level:** Radio buttons for 'No Security', 'Authentication', and 'Authentication and Privacy'. 'No Security' is selected.
- Authentication Method:** Radio buttons for 'None', 'MD5', and 'SHA'. 'None' is selected. Below it is a password input field.
- Privacy:** Radio buttons for 'None' and 'DES'. 'None' is selected. Below it is a password input field.

At the bottom, there is a table with columns: User, Group, Security Level, Authentication Method, Privacy Method, and Edit. The table is currently empty, with the message 'No data available in table' below it.

Available settings are explained as follows:

| Item                  | Description  |
|-----------------------|--|
| User Name             | Enter a name for creating new SNMP user.   |
| Group                 | Choose one of the SNMP group from the drop down list. Then, this user profile will be grouped under the selected SNMP group.   |
| Security Level        | Specify SNMP security level for the group. It is available when SNMPv3 is selected. <ul style="list-style-type: none"> <li>● <b>No Security</b> - No authentication.</li> <li>● <b>Authentication</b> - Authentication without encryption will be performed for packets.</li> <li>● <b>Authentication and Privacy</b> - Authentication with encryption will be performed for packets.</li> </ul> |
| Authentication Method | It is available when <b>Authentication</b> or <b>Authentication and Privacy</b> is selected as security level. <ul style="list-style-type: none"> <li>● <b>Method</b> - At present, available methods include None, MD5 and SHA.</li> <li>● <b>Password</b> - Enter a password for the selected method.</li> </ul>   |
| Privacy               | It is available when <b>Authentication</b> or <b>Authentication and Privacy</b> is selected as security level. <ul style="list-style-type: none"> <li>● <b>Method</b> -At present, available methods include DES and None.</li> <li>● <b>Password</b> - Enter a password for the selected method.</li> </ul>   |
| Add                   | Click it to add a new user profile.  |
| Edit                  |  - click it to modify the settings for the selected profile.  |



- click it to remove the selected entry.

### Edit SNMP User=carrie

Group:

Security Level:  No Auth  Auth  Auth & Privacy

Authentication Method:

Method  None  MD5  SHA

Password:

Privacy:

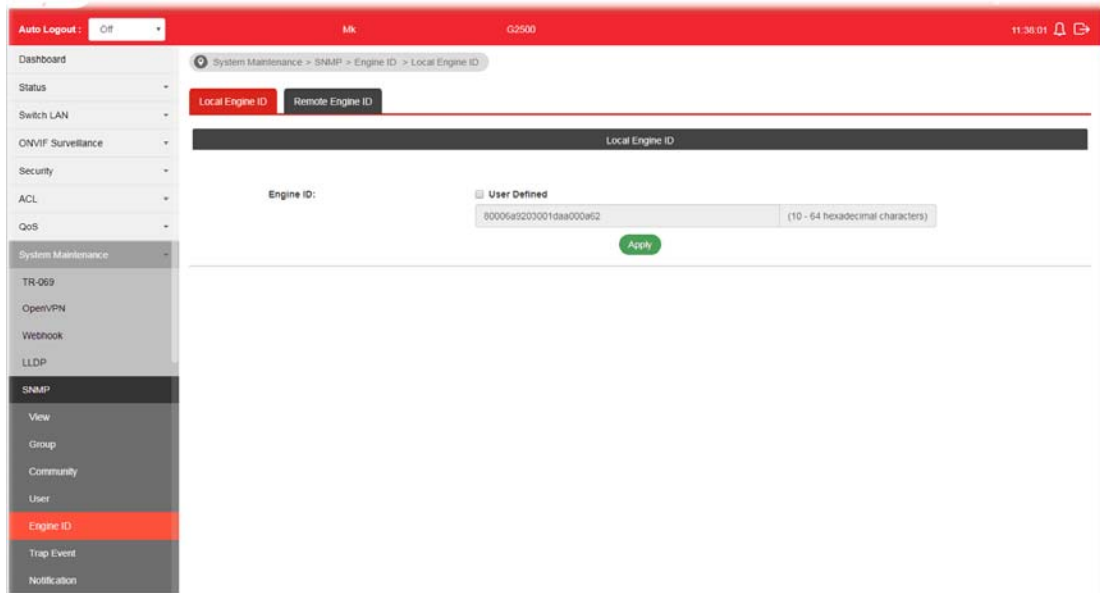
Method:  None  DES

Password:

## VII-5-5 Engine ID

### VII-5-5-1 Local Engine ID

This page allows a user to configure and display SNMP local engine ID.





Available settings are explained as follows:

| Item      | Description   |
|-----------|---|
| Engine ID | The user defined engine ID is range 10 to 64 hexadecimal characters, and the hexadecimal number must be divided by "2".<br><b>User Defined</b> - If it is checked, the local engine ID will be configured manually. If not, the default Engine ID which is made up of MAC and Enterprise ID will be used instead. |
| Apply     | Apply the settings to the switch.   |

## VII-5-5-2 Remote Engine ID

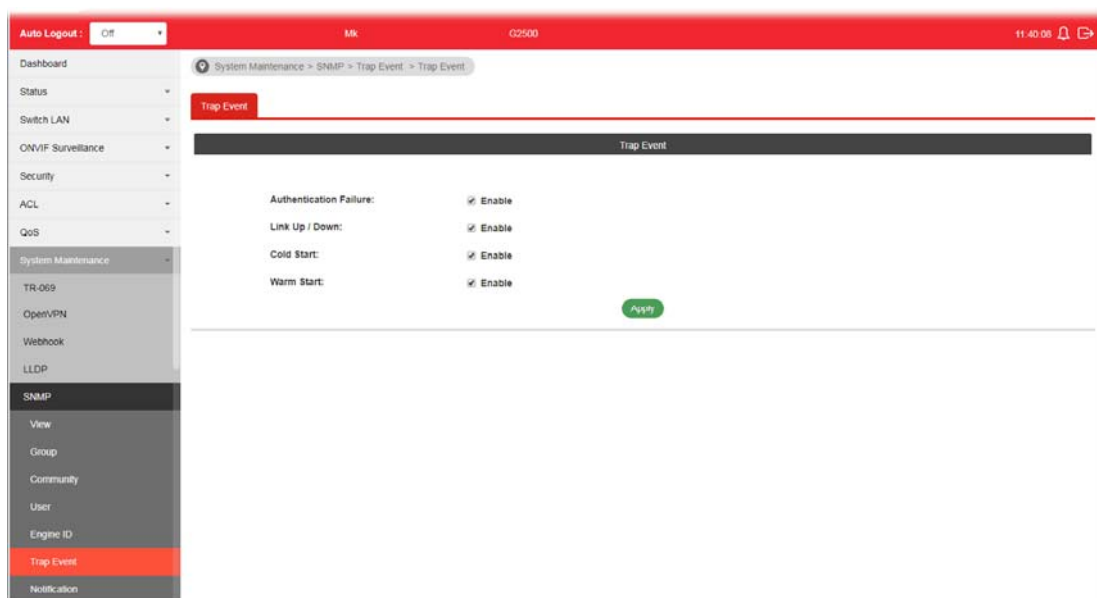
This page allows a user to configure and display SNMP remote engine ID.

Available settings are explained as follows:

| Item           | Description  |
|----------------|--|
| Address Type   | Specify the address type for entering hostname or IPv4/IPv6 address.   |
| Server Address | Enter the IP address or the host name of the SNMP server.  |
| Engine ID      | Specify the engine ID for remote SNMP server.<br>The engine ID is range 10 to 64 hexadecimal characters, and the hexadecimal number must be divided by 2.  |
| Add            | Click it to create a new profile.  |
| Edit           |  - click it to modify the settings for the selected server profile.<br> - click it to remove the selected entry. <div style="border: 1px solid gray; padding: 10px; margin-top: 10px;"> <p style="text-align: center;"><b>Edit SNMP Engine ID for</b></p> <p style="text-align: center;"><b>IP=172.16.8.2</b></p> <p>Engine ID: <input type="text" value="80006a9203001daa1"/> (10-64 pairs of hex char)</p> <p style="text-align: center;"> <input type="button" value="OK"/> <input type="button" value="Cancel"/> </p> </div> |

## VII-5-6 Trap Event

This page allows a user to add or delete SNMP trap receiver IP address and community name.



Available settings are explained as follows:

| Item                   | Description   |
|------------------------|---|
| Authentication Failure | Enable - VigorSwitch will reboot when encountering authentication failure (including community not match or user password not match). |
| Link Up / Down         | Enable - VigorSwitch will reboot while encountering port link up or down trap.  |
| Cold Start             | Enable - VigorSwitch will reboot while encountering user trap.  |
| Warm Start             | Enable - VigorSwitch will reboot while encountering power down trap.  |
| Apply                  | Apply the settings to the switch.   |

## VII-5-7 Notification

This page allows a user to configure a host to receive SNMPv1/v2/ve notification.



The screenshot shows the 'Notification' configuration page in the VigorSwitch G2500 web interface. The page has a red header with 'Auto Logout: Off', 'MR', 'G2500', and '11:41:13'. The left sidebar menu includes 'Dashboard', 'Status', 'Switch LAN', 'ONVIF Surveillance', 'Security', 'ACL', 'QoS', 'System Maintenance', 'TR-069', 'OpenVPN', 'Webhook', 'LLDP', 'SNMP', 'View', 'Group', 'Community', 'User', 'Engine ID', 'Trap Event', and 'Notification'. The main configuration area has the following fields:

- Address Type:** Radio buttons for Hostname, IPv4, and IPv6.
- Server Address:** A text input field.
- Version:** Radio buttons for SNMPv1, SNMPv2, and SNMPv3.
- Type:** Radio buttons for Trap and Inform.
- Community/user:** A dropdown menu with 'public' selected.
- Security Level:** Radio buttons for No Security, Authentication, and Authentication and Privacy.
- Server Port:** A text input field with '162' and a note '(1 - 65535, default 162)'. A 'Use Default' checkbox is checked.
- Timeout:** A text input field with '15' and a note 'sec (1 - 300, default 15)'. A 'Use Default' checkbox is checked.
- Retry:** A text input field with '3' and a note '(1 - 255, default 3)'. A 'Use Default' checkbox is checked.

Below the form is a table with the following columns: Index, Server Address, Server Port, Timeout, Retry, Version, Type, Communication/U..., Security Level, and Edit. The table currently shows 'No data available in table'.

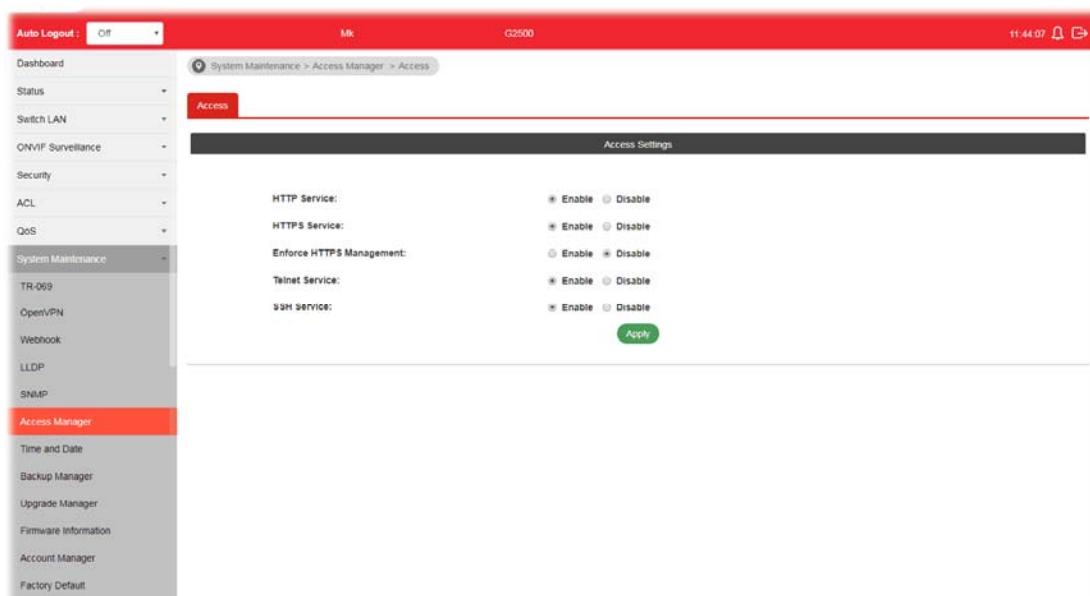
Available settings are explained as follows:

| Item           | Description   |
|----------------|---|
| Address Type   | Choose IPv4/IPv6/Hostname to specify IP address or the hostname of the SNMP trap recipients.  |
| Server Address | Enter the IP address of SNMP server based on the address type selected above.   |
| Version        | Specify SNMP notification version (SNMPv1/v2/v3).   |
| Type           | Specify Notification Type. <ul style="list-style-type: none"> <li>● <b>Trap</b> -Send SNMP traps to the host.</li> <li>● <b>Inform</b> - Send SNMP informs to the host. If it is used, Timeout and Retry also shall be defined.</li> </ul>  |
| Community/user | Use the drop down list to choose one of the community profiles.   |
| Security Level | Specify SNMP security level for SNMP notification packet. It is available when SNMPv3 is selected. <ul style="list-style-type: none"> <li>● <b>No Security</b> - No authentication.</li> <li>● <b>Authentication</b> - Authentication without encryption will be performed for packets.</li> <li>● <b>Authentication and Privacy</b> - Authentication with encryption will be performed for packets.</li> </ul> |
| Server Port    | Specify the UDP port number for the recipient's server.<br><b>Use Default</b> - If it is checked, the default number (162) will be used automatically.  |
| Timeout        | Specify the SNMP informs timeout. It is available when Inform is selected as Type.<br><b>Use Default</b> - If it is checked, the default number (15) will be used automatically.  |

|       |  |
|-------|--|
| Retry | <p>Specify the SNMP informs retry count. It is available when <b>Inform</b> is selected as Type.</p> <p><b>Use Default</b> - If it is checked, the default number (3) will be used automatically.</p>  |
| Add   | Click it to create a new notification profile.   |
| Edit  | <p> - Click it to modify the settings for the selected server profile.</p> <p> - Click it to remove the selected entry.</p> <div data-bbox="699 584 1410 1413" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <div style="text-align: right; font-size: 20px;">×</div> <h3 style="text-align: center;">Edit Notification Entry for<br/>Server IP=172.16.3.98</h3> <p>Version:     <input checked="" type="radio"/> SNMPv1   <input type="radio"/> SNMPv2   <input type="radio"/> SNMPv3</p> <p>Type:                   <input checked="" type="radio"/> Trap   <input type="radio"/> Inform</p> <p>Community/user   <input type="text" value="public"/></p> <p>Security Level:   <input checked="" type="radio"/> No Security   <input type="radio"/> Auth   <input type="radio"/> Privacy</p> <p>Server Port:   <input checked="" type="checkbox"/> Use Default   <input type="text" value="162"/>   <input type="text" value="(1-65535)"/></p> <p>Timeout:       <input checked="" type="checkbox"/> Use Default   <input type="text"/>   <input type="text" value="sec (1-300)"/></p> <p>Retry:          <input checked="" type="checkbox"/> Use Default   <input type="text"/>   <input type="text" value="(1-255)"/></p> <p style="text-align: center;"> <input type="button" value="OK"/>   <input type="button" value="Cancel"/> </p> </div> |

## VII-6 Access Manager

This page allows the network administrator to control availability of management services such as HTTP, HTTPS, Telnet and SSH.



Available settings are explained as follows:

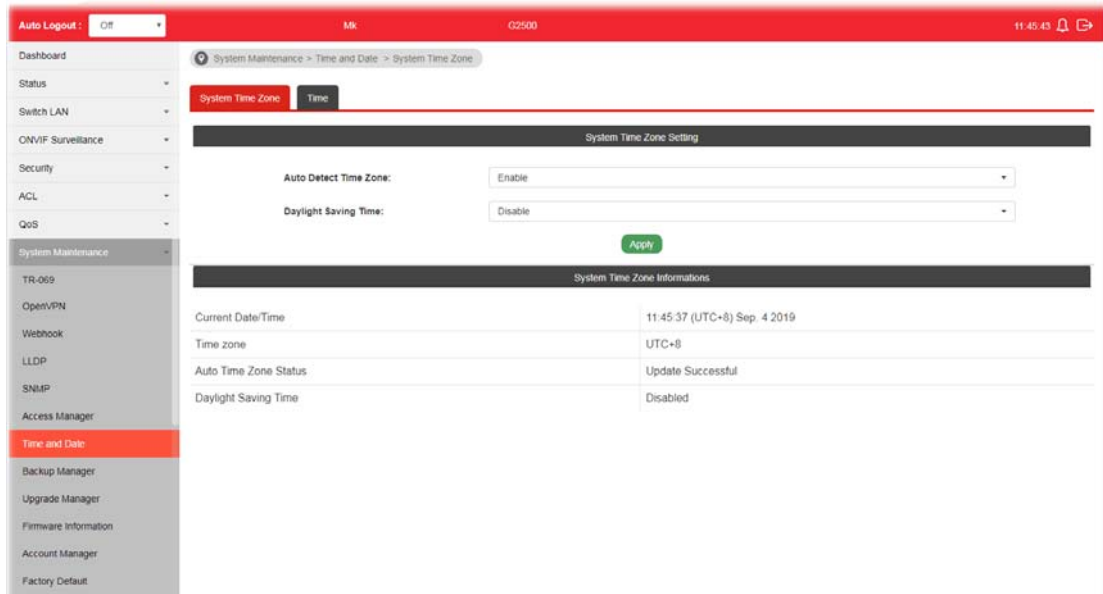
| Item                     | Description   |
|--------------------------|---|
| HTTP Service             | HTTP is the acronym of HyperText Transfer Protocol.<br><b>Enabled</b> -Click it to enable HTTP service.   |
| HTTPS Service            | HTTPS is the acronym of Hypertext Transfer Protocol over Secure Socket Layer.<br><b>Enabled</b> - Click it to enable HTTPS service.   |
| Enforce HTTPS Management | <b>Enabled</b> - Users will be forced to access into the web user interface of VigorSwitch by HTTPS protocol.   |
| Telnet Service           | Telnet is the TCP/IP standard protocol for remote terminal service. TELNET allows a user at one site to interact with a remote timesharing system at another site as if the user's keyboard and display connected directly to the remote machine. <ul style="list-style-type: none"> <li>● <b>Disabled</b> - Click it for not accessing telnet service.</li> <li>● <b>Enabled</b> - Click it to access telnet service.</li> </ul> |
| SSH Service              | <b>Enabled</b> - Enable SSH service.  |
| Apply                    | Apply the settings to the switch.   |



## VII-7 Time and Date

### VII-7-1 System Time Zone

This page allows a user to specify where the time of VigorSwitch should be inquired from.



Available settings are explained as follows:

| Item                               | Description   |
|------------------------------------|---|
| <b>System Time Zone Setting</b>    |   |
| <b>Auto Detect Time Zone</b>       | Select <b>Enable</b> to make Vigor router detect the time zone that VigorSwitch is located automatically.   |
| <b>Daylight Saving Time</b>        | Select the mode of daylight saving time. <ul style="list-style-type: none"> <li>● <b>Disable</b> -Disable daylight saving time.</li> <li>● <b>Recurring</b> - Using recurring mode of daylight saving time.</li> <li>● <b>Non-Recurring</b> - Using non-recurring mode of daylight saving time.</li> <li>● <b>USA</b> -Using daylight saving time in the United States that starts on the second Sunday of March and ends on the first Sunday of November.</li> <li>● <b>European</b> - Using daylight saving time in the Europe that starts on the last Sunday.</li> </ul> |
| <b>Daylight Saving Time Offset</b> | It is available when <b>Recurring</b> is selected as Daylight Saving Time.<br>Specify the adjust offset of daylight saving time.  |
| <b>Recurring From / To</b>         | It is available when <b>Recurring</b> is selected as Daylight Saving Time. <ul style="list-style-type: none"> <li>● <b>From</b> - Specify the starting time of recurring daylight saving time.</li> <li>● <b>To</b> - Specify the ending time of recurring daylight saving time.</li> </ul>   |

|                               |  |
|-------------------------------|--|
| Non-recurring From / To       | It is available when Non-Recurring is selected as Daylight Saving Time. <ul style="list-style-type: none"> <li>● From - Specify the starting time of non-recurring daylight saving time.</li> <li>● To - Specify the ending time of recurring daylight saving time.</li> </ul> |
| Apply                         | Apply the settings to the switch.  |
| System Time Zone Informations | Display the status of system time zone.  |

## VII-7-2 Time

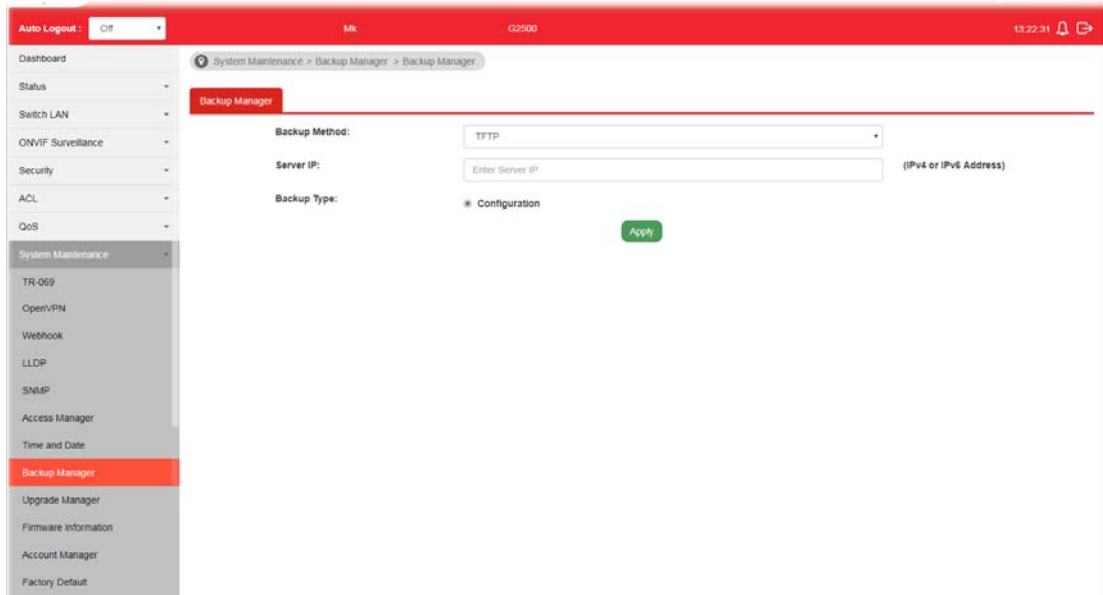
This page allows a user to specify time and activate SNTP server manually.

Available settings are explained as follows:

| Item                    | Description  |
|-------------------------|--|
| Manual Time             | Specify static time (year, month, day, hours, minutes and seconds) manually.   |
| Enable SNTP             | <ul style="list-style-type: none"> <li>● Enable - Click it to enable SNTP time server.</li> <li>● Disable - Click to disable the time server.</li> </ul> |
| SNTP/NTP Server Address | Enter the web site of the time server or the IP address of the server.   |
| Server Port             | Enter the port number use by the time server.  |
| Apply                   | Apply the settings to the switch.  |

## VII-8 Backup Manager

Backup Manager allows a user to backup the firmware image or configuration file on the switch to remote TFTP server or host file system through HTTP protocol.

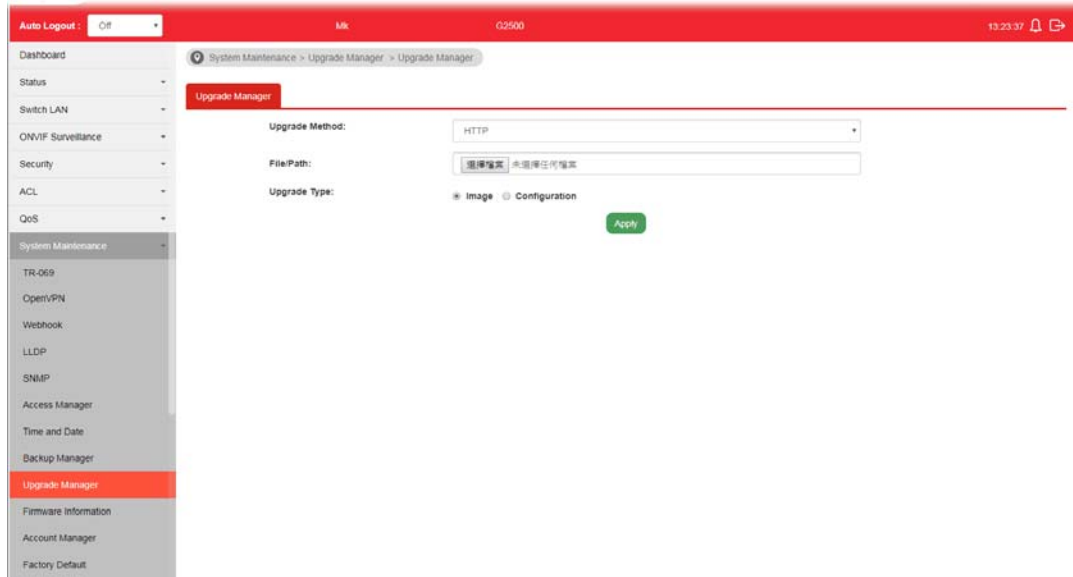


Available settings are explained as follows:

| Item          | Description   |
|---------------|---|
| Backup Method | Select Backup method. <ul style="list-style-type: none"><li>● TFTP - Using TFTP to backup firmware.</li><li>● HTTP - Using WEB browser to ubackup firmware.</li></ul> |
| Server IP     | It is available when TFTP is selected as Backup Method.<br>Enter the IPv4/IPv6 address for the TFTP server.   |
| Backup Type   | <b>Configuration</b> - Make a backup copy for the configurations for VigorSwitch.   |
| Apply         | Apply the settings to the switch.   |

## VII-9 Upgrade Manager

Backup Manager allows a user to upgrade the firmware image or configuration file on the switch to remote TFTP server or host file system through HTTP protocol.



Available settings are explained as follows:

| Item           | Description   |
|----------------|---|
| Upgrade Method | Select Upgrade method: <ul style="list-style-type: none"> <li>● TFTP - Using TFTP to upgrade firmware.</li> <li>● HTTP - Using WEB browser to upgrade firmware.</li> </ul>  |
| Server IP      | It is available when TFTP is selected as Upgrade Method.<br>Enter the IPv4/IPv6 address for the TFTP server.  |
| File Name      | It is available when TFTP is selected as Upgrade Method.<br>Enter the firmware image or configuration file name on the TFTP server.   |
| File/Path      | It is available when HTTP is selected as Upgrade Method.<br>Choose the firmware file located in your computer.  |
| Upgrade Type   | It is available when TFTP is selected as Upgrade Method. <ul style="list-style-type: none"> <li>● Image - Click it to upgrade the firmware image.</li> <li>● Configuration - Click it to upgrade the configurations for VigorSwitch.</li> </ul> |
| Apply          | Apply the settings to the switch.   |

## VII-10 Firmware Information

This page allows a user to choose the active firmware and backup firmware.



Available settings are explained as follows:

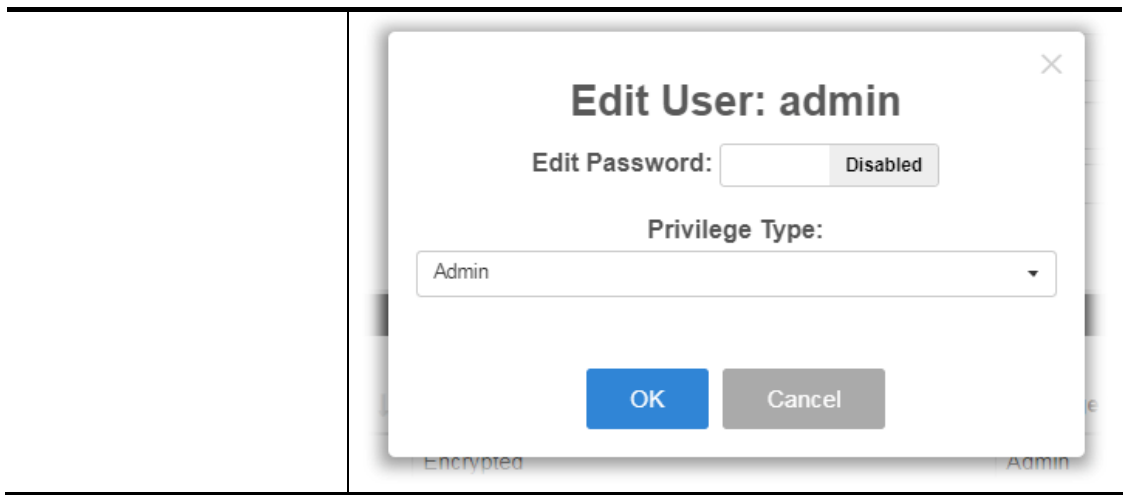
| Item   | Description  |
|--|--|
| Active Image                                     | There are two versions of firmware. Simply choose the one you want as primary firmware.  |
| Apply  | Apply the settings to the switch.  |
| Firmware 1 Information<br>Firmware 2 Information | <ul style="list-style-type: none"> <li>● <b>Mode</b> - Display the mode (Active or Backup) of the firmware.</li> <li>● <b>Active</b> - Display the status (in use or not) of the firmware.</li> <li>● <b>Version</b> - Display the switch version.</li> <li>● <b>Build Time</b> - Display the built time of the firmware.</li> <li>● <b>Size (MB)</b> - Display the size of the firmware.</li> </ul> |

## VII-11 Account Manager

This page allows a user to add or delete local user on switch database for authentication. The configuration result for each port will be displayed on the table listed on the lower side of this web page.

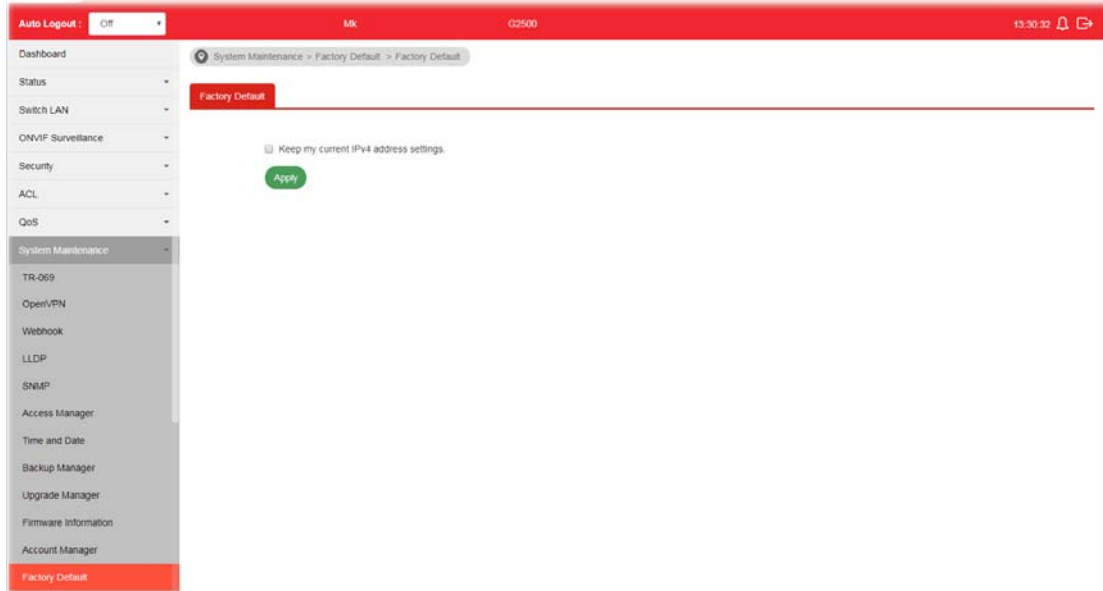
Available settings are explained as follows:

| Item            | Description  |
|-----------------|--|
| User Name       | Enter a username for new account.<br>If you want to modify an existed user account, simply enter the same string in this field. Then, modify the password and choose privilege level. After clicking <b>Apply</b> , the existed user name will be modified with different values.    |
| Password        | Enter a password for new account.  |
| Retype Password | Retype password to make sure the password is exactly you typed before in "Password" field.   |
| Privilege Level | Use the drop down list to select privilege level (Admin/User) for new account. <ul style="list-style-type: none"> <li>● <b>Admin</b> - Allow to change switch settings.</li> <li>● <b>User</b> - See switch settings only. Not allow to change it.</li> </ul>                        |
| Apply           | Apply the settings to the switch.  |
| Edit            |  - Click it to modify the settings for the selected user profile.<br> - Click it to remove the selected entry. |



## VII-12 Factory Default

Click **Apply** to return to factory default settings for VigorSwitch.

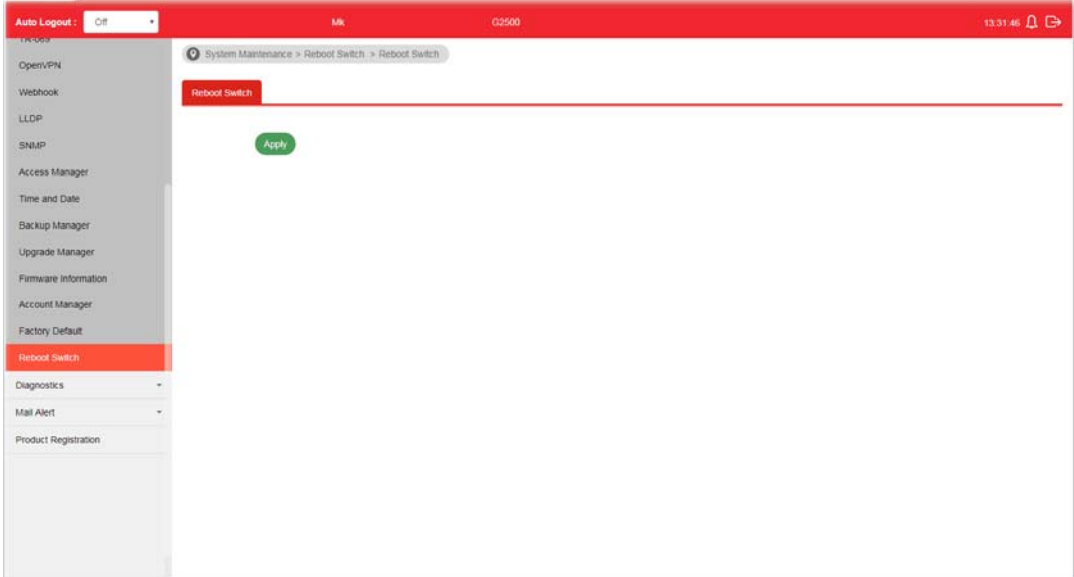


If **Keep my current IPv4 address settings** is checked, after clicking **Apply**, the original configuration for IP address will be kept.



# VII-13 Reboot Switch

Click Apply to reboot VigorSwitch with current settings.



This page is left blank.

# Part VIII Diagnostics

## VIII-1 Device Check

After finished copper test, the results will be shown on the lower side of this web page.

This page is used to configure device check of PoE PD devices. It can be applied to PoE PD devices connected directly, check ping echo status, and forcibly reboot the device when meeting the preset health condition.

The configuration result for each port will be displayed on the table listed on the lower side of this web page.

The screenshot shows the 'Device Check' configuration page. The settings for the selected port (GE1) are as follows:

- Port: GE1
- Enable:  Enable  Disable
- Ping IP Address: 0.0.0.0 (IPv4, up to 16 IP addresses)
- Interval Time (sec.): 15
- Retry Time: 1
- Mail Alert:  Enable  Disable

Below the settings is a table showing the configuration for all ports:

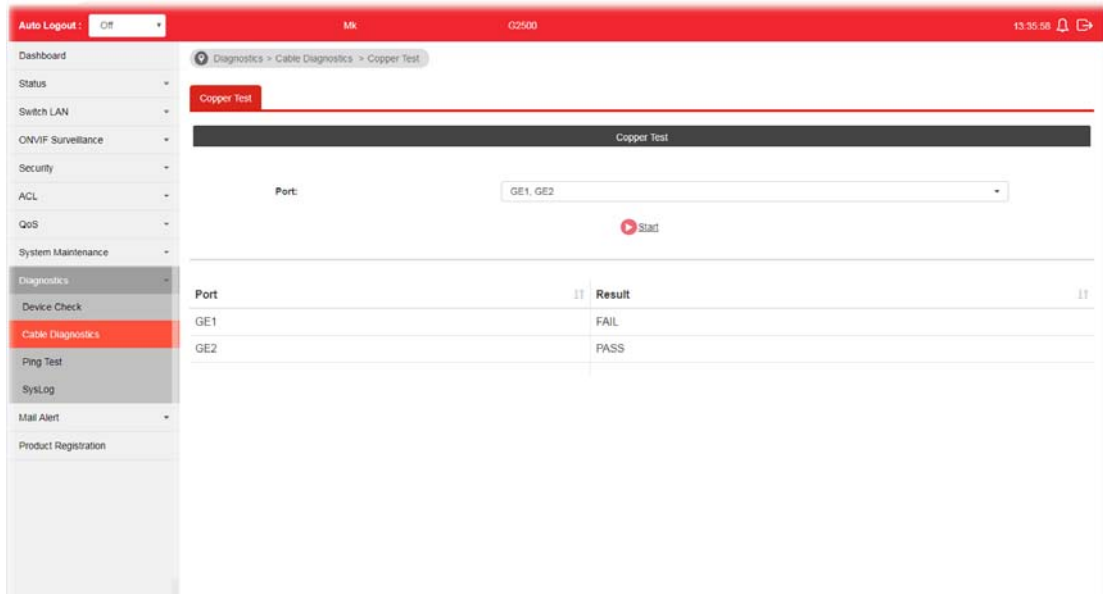
| Port | Enable   | Ping IP Addr | Interval Times (s) | Retry Time | Mail Alert |
|------|----------|--------------|--------------------|------------|------------|
| GE1  | Disabled | 0.0.0.0      | 15                 | 1          | Disabled   |
| GE2  | Disabled | 0.0.0.0      | 15                 | 1          | Disabled   |
| GE3  | Disabled | 0.0.0.0      | 15                 | 1          | Disabled   |
| GE4  | Disabled | 0.0.0.0      | 15                 | 1          | Disabled   |
| GE5  | Disabled | 0.0.0.0      | 15                 | 1          | Disabled   |

Available settings are explained as follows:

| Item                 | Description  |
|----------------------|--|
| Port                 | Use the drop down list to select the port (GE1 to GE50) or ports for device check.   |
| Enable               | <b>Disable</b> - No PoE function for the selected GE port.<br><b>Enable</b> - PoE function will be enabled for the selected GE port.   |
| Ping IP Address      | Enter the IP address of the PoE device for check.  |
| Interval Time (sec.) | The ping check will be performed every 10, 30, 60 or 120 seconds for the selected port.  |
| Retry Time           | The system will perform the ping check the selected port (PoE device) for 1, 3 or 5 times.   |
| Mail Alert           | <ul style="list-style-type: none"> <li>● <b>Enable</b> - Click it to enable the mail alert function.</li> <li>● <b>Disable</b> - Click it to disable the mail alert function.</li> </ul> |
| Apply                | Save the settings or changes to the switch.  |

## VIII-2 Cable Diagnostics

After finished copper test, the results will be shown on the lower side of this web page.

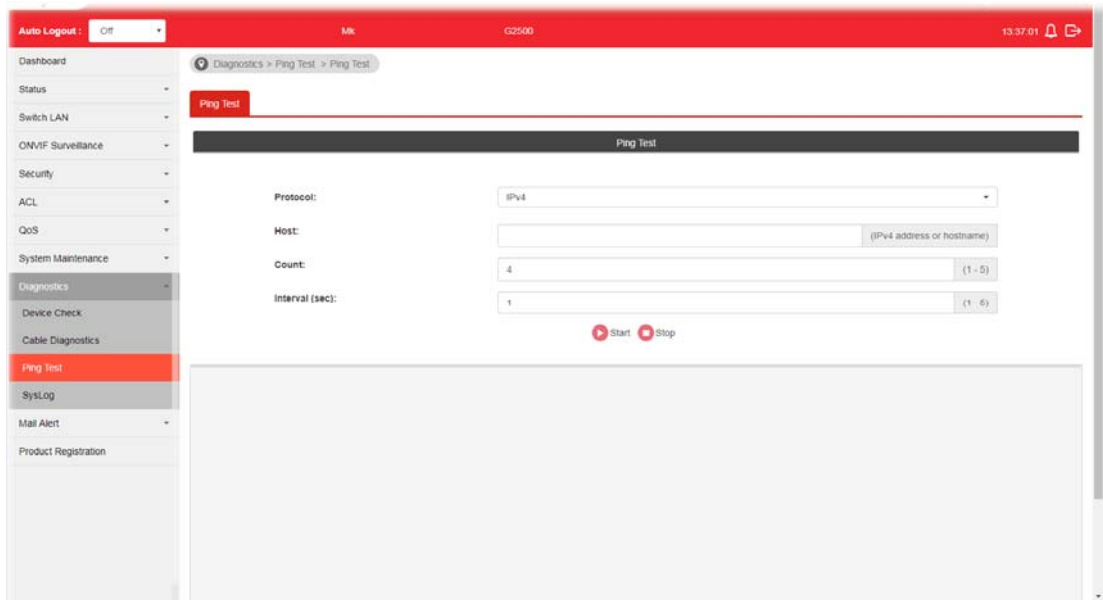


Available settings are explained as follows:

| Item  | Description  |
|-------|--|
| Port  | Use the drop down list to select the port (GE1 to GE50) or ports for performing cable diagnostics. |
| Start | Perform the copper test action.  |

## VIII-3 Ping Test

After finished the ping test, the results will be shown on the lower side of this web page.



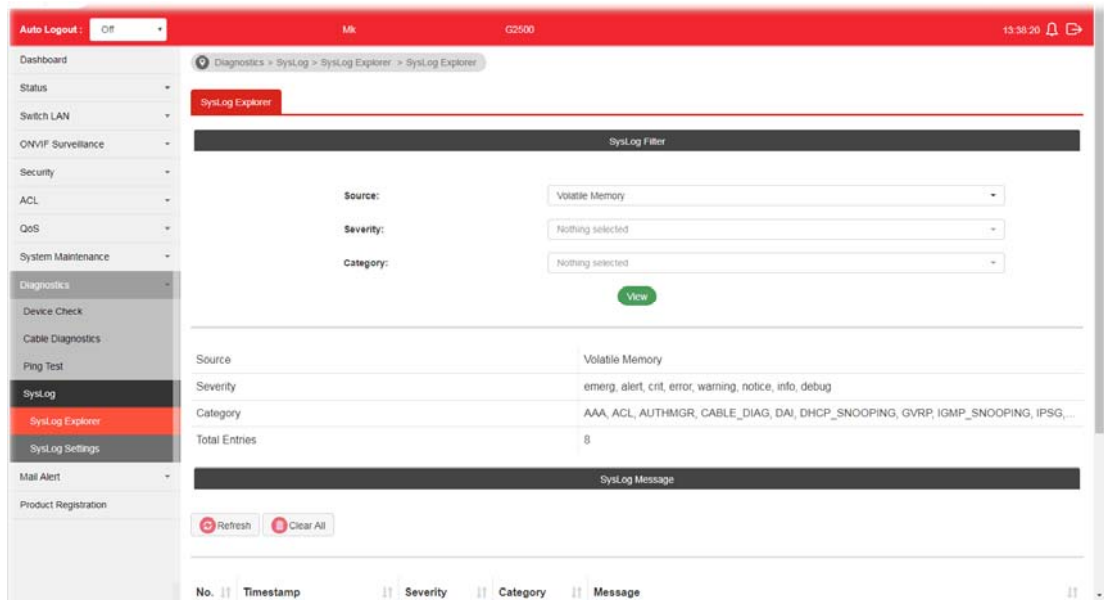
Available settings are explained as follows:

| Item          | Description   |
|---------------|---|
| Protocol      | Choose IPv4/IPv6 to specify IP address for sending ping to check if network path is ok.   |
| Host          | Enter the IP address of SNMP server based on the protocol selected above.   |
| Count         | It means how many times to send ping request packet.<br>Enter a number between 1 and 5 as the count and the default configuration is 4. |
| Interval(sec) | Define the interval to perform ping action. For example, "1" means the ping action will be performed per second.                        |
| Start         | Perform ping action.  |
| Stop          | Terminate ping action.  |

## VIII-4 SysLog

### VIII-4-1 SysLog Explorer

After clicking View, the results will be shown on the lower side of this web page.



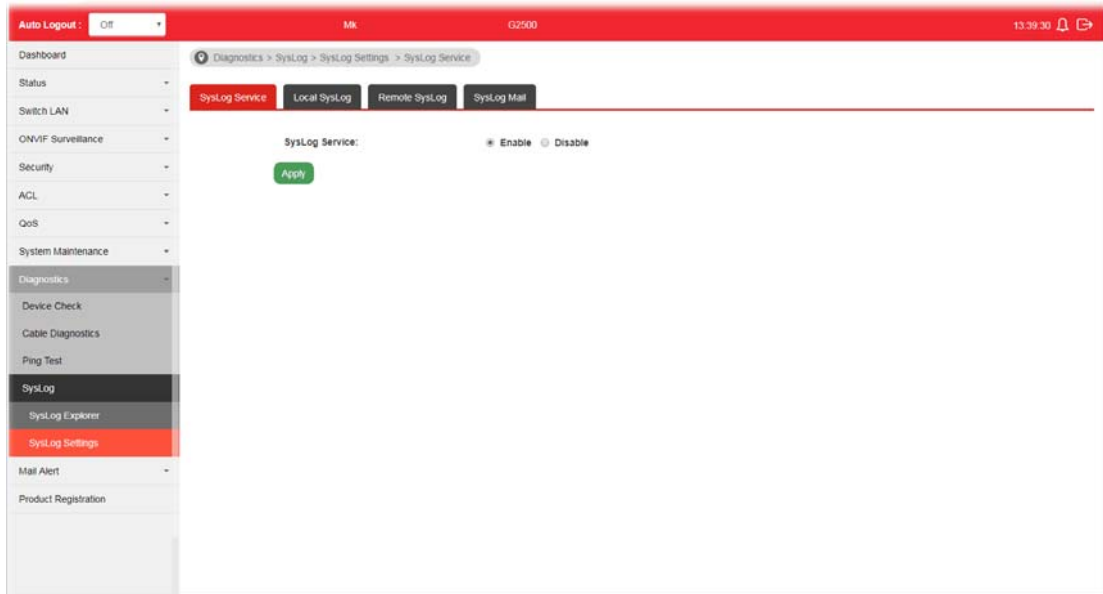
Available settings are explained as follows:

| Item      | Description   |
|-----------|---|
| Source    | <ul style="list-style-type: none"> <li>● <b>Volatile Memory</b> - Explore the logs contained in volatile memory (also known as RAM).</li> <li>● <b>Non-Volatile Memory</b> - Explore the logs contained in non-volatile memory (also known as Flash).</li> </ul>  |
| Severity  | Select severity (emerg, alert, crit, error, warning, notice, info and debug) of log messages which you wish to filter out for review.   |
| Category  | Select the categories (related features) of logs you wish to review.<br>Category contains AAA, ACL, AUTHMGR, CABLE_DIAG, DAI, DHCP_SNOOPING, GVRP, IGMP_SNOOPING, IPSG, L2, LLDP, Mac-based VLAN, Mirror, MLD_SNOOPING, Platform, PM, Port, PORT_SECURITY, QoS, Rate, SNMP, STP, Security suite, System, Surveillance VLAN, Trunk, UDLD and VLAN. |
| View      | Click it to display logs based on the settings configured above.  |
| Refresh   | Click it to refresh the log.  |
| Clear All | Clear it to remove all logs displayed in this page.   |

## VIII-4-2 SysLog Settings

### VIII-4-2-1 SysLog Service

This page allows user to enable system logging into local syslog and specific remote syslog server for storage.



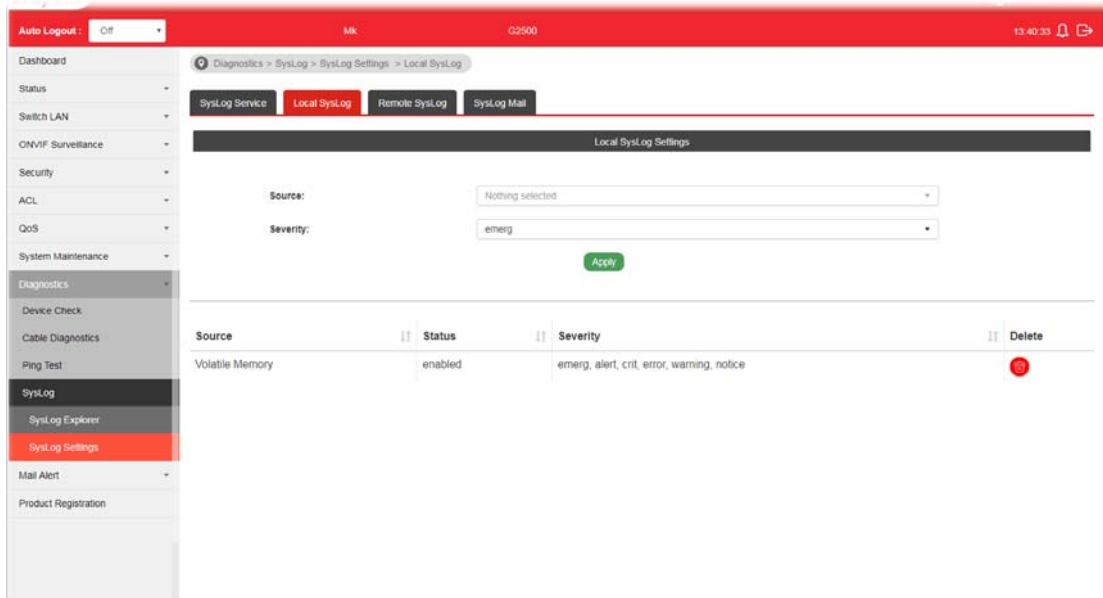
Available settings are explained as follows:

| Item           | Description  |
|----------------|--|
| SysLog Service | <ul style="list-style-type: none"><li>● Enable - Click it to activate function of syslog.</li><li>● Disable - Click it to inactivate the function.</li></ul> |
| Apply          | Apply the settings to the switch.  |



## VIII-4-2-2 Local SysLog

This page allows user to enable logging into volatile memory or non-volatile memory.

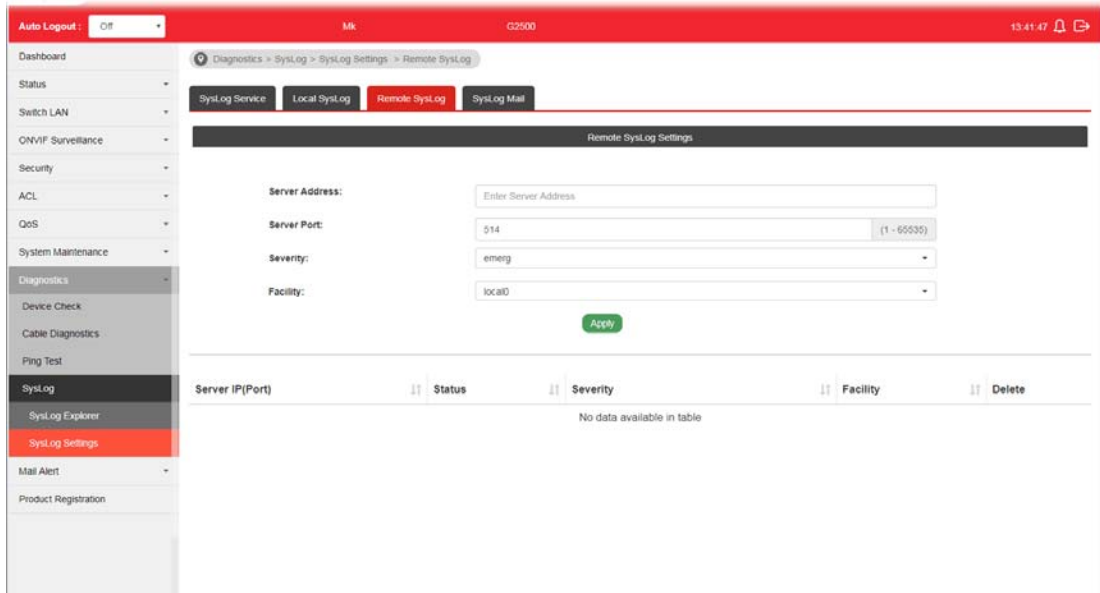


Available settings are explained as follows:

| Item     | Description   |
|----------|---|
| Source   | <ul style="list-style-type: none"> <li>● <b>Volatile Memory</b> - Select the volatile memory for saving local log. Volatile memory does not hold the log after reboot or power off.</li> <li>● <b>Non-Volatile Memory</b> - Select the non-volatile memory for saving.</li> </ul> <p>If you want to modify <b>Volatile Memory / Non-Volatile Memory</b>, select <b>Volatile Memory / Non-Volatile Memory</b> in this field. Then, use the drop down list of severity to specify type of log message. After clicking <b>Apply</b>, the <b>Volatile Memory / Non-Volatile Memory</b> will be modified with new configured severity level.</p> |
| Severity | Select severity (emerg, alert, crit, error, warning, notice, info and debug) of log messages which will be stored.  |
| Apply    | Apply the settings to the switch.   |
| Delete   | Remove all logs displayed in this page.   |

### VIII-4-2-3 Remote SysLog

This page allows user to enable system logging into specific remote syslog server for storage. After clicking **Apply**, the results will be shown on the lower side of this web page.

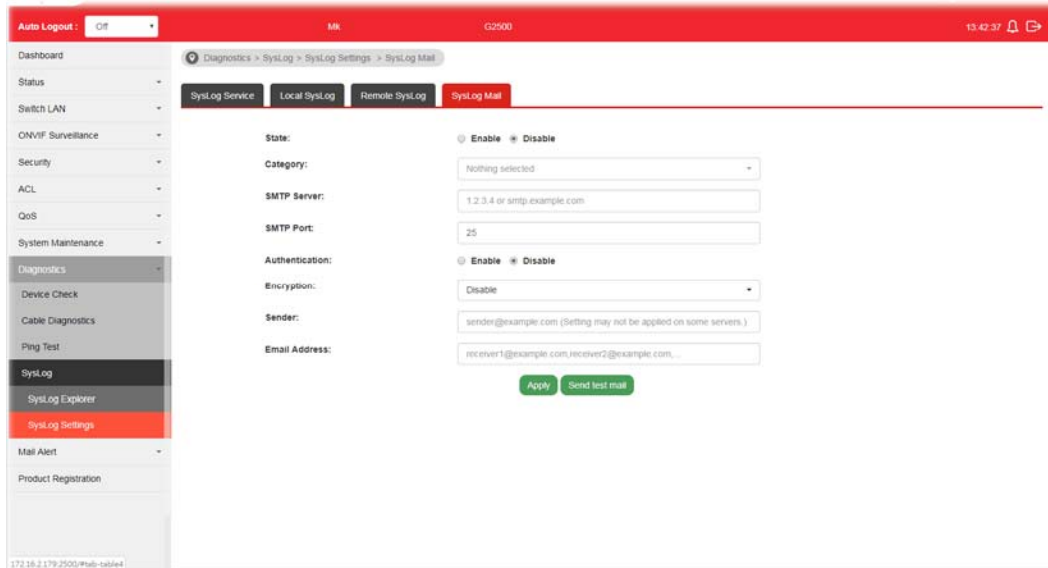


Available settings are explained as follows:

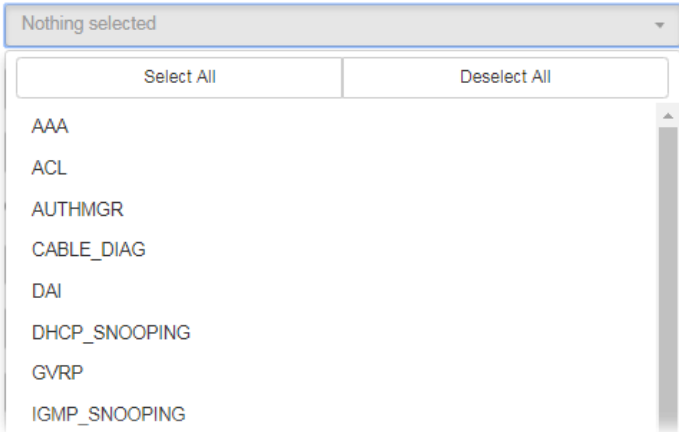
| Item           | Description  |
|----------------|--|
| Server Address | Enter the IP address of Syslog server.   |
| Server Port    | Specify the port that syslog should be sent to.  |
| Severity       | Select severity (emerg, alert, crit, error, warning, notice, info and debug) of log messages which will be stored.   |
| Facility       | One device supports multiple facilities (represented with facility ID, local0 to local7) of remote Syslog server. For each facility ID contains different syslog server configuration, please choose a facility ID for such Syslog server. |
| Apply          | Apply the settings to the switch.  |
| Delete         | Remove specific remote syslog entry.   |

## VIII-4-2-4 SysLog Mail

This page allows user to enable system logging into specific remote syslog server for storage. After clicking **Apply**, the results will be shown on the lower side of this web page.



Available settings are explained as follows:

| Item           | Description  |
|----------------|--|
| State          | <p><b>Enable</b> - Enable the function of Syslog Mail.</p> <p><b>Disable</b> - Disable the function of Syslog Mail.</p>  |
| Category       | <p>Vigor sytem will send the e-mail related to the selected feature(s) to the recipient.</p>   |
| SMTP Server    | Enter IP address or URL of the SMTP server.  |
| SMTP Port      | Enter the port number for the SMTP server.   |
| Authentication | <p><b>Enable</b> - Click it to enable authentication mechanism.</p> <ul style="list-style-type: none"> <li>● <b>User Name</b> - Enter a user name for authentication.</li> <li>● <b>Password</b> - Enter a password for authentication.</li> </ul>                                   |
| Encryption     | <p>After enabling Authentication, choose one of the encryption servers for data encryption.</p> <ul style="list-style-type: none"> <li>● <b>StartTLS</b> - The mail will be encrypted with StartTLS.</li> <li>● <b>SSL/TLS</b> - The mail will be encrypted with SSL/TLS.</li> </ul> |

|                       |   |
|-----------------------|---|
|                       | <ul style="list-style-type: none"><li>● <b>Disable</b> - The mail sent out will not be encrypted.</li></ul> |
| <b>Sender</b>         | Enter the email address which will send the syslog mail out.  |
| <b>Email Address</b>  | Enter the email address which will receive the syslog mail.   |
| <b>Apply</b>          | Apply the settings to the switch.   |
| <b>Send test mail</b> | After clicking this button, VigorSwitch system will send a test mail to the recipient.                      |

# Part IX Mail Alert

## IX-1 Alert Setting

This page allows a user to configure settings for VigorSwitch to send alert mail when encountering certain situation.

Available settings are explained as follows:

| Item                   | Description  |
|------------------------|--|
| State                  | <ul style="list-style-type: none"> <li>● <b>Enable</b> - Click it to enable the mail alert function.</li> <li>● <b>Disable</b> - Click it to disable the mail alert function.</li> </ul>   |
| SMTP Server            | Enter IP address or URL of the SMTP server.  |
| SMTP Port              | Enter the port number for the SMTP server.   |
| Authentication         | <b>Enable</b> - Click it to enable authentication mechanism. <ul style="list-style-type: none"> <li>● <b>User Name</b> - Enter a user name for authentication.</li> <li>● <b>Password</b> - Enter a password for authentication.</li> </ul>  |
| Encryption             | After enabling Authentication, choose one of the encryption servers for data encryption. <ul style="list-style-type: none"> <li>● <b>StartTLS</b> - The mail will be encrypted with StartTLS.</li> <li>● <b>SSL/TLS</b> - The mail will be encrypted with SSL/TLS.</li> <li>● <b>Disable</b> - The mail sent out will not be encrypted.</li> </ul> |
| Sender                 | Enter the email address which will send the alert mail out.  |
| Receiver               | Enter the email address which will receive the alert mail.   |
| Min. Transmit Interval | Set a time interval for VigorSwitch system to send an alert out from the specified sender.   |
| Alert Type             | Specify the condition(s) for VigorSwitch system to send an alert out. <ul style="list-style-type: none"> <li>● Port Link Status</li> <li>● Port Link Speed</li> <li>● System Restarted</li> <li>● IP Conflict</li> </ul>   |

|                       |  |
|-----------------------|--|
|                       | <ul style="list-style-type: none"><li>● Hardware Monitor</li><li>● Device Check</li><li>● ONVIF Throughput Threshold</li></ul> |
| <b>Apply</b>          | Apply the settings to the switch.  |
| <b>Send test mail</b> | After clicking this button, VigorSwitch system will send a test mail to the recipient.   |

This page is left blank.



# Part X Telnet Commands

---

## X-1 Accessing Telnet of VigorSwitch

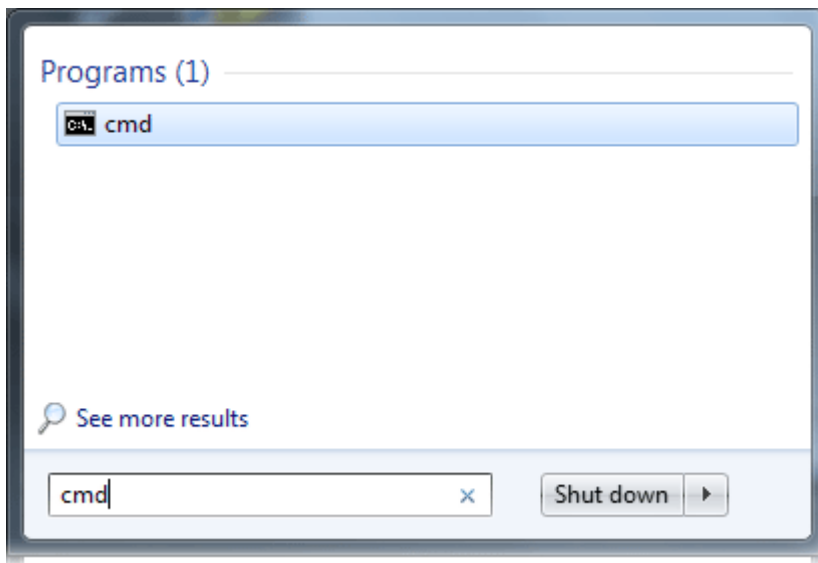
This chapter also gives you a general description for accessing telnet and describes the firmware versions for the routers explained in this manual.



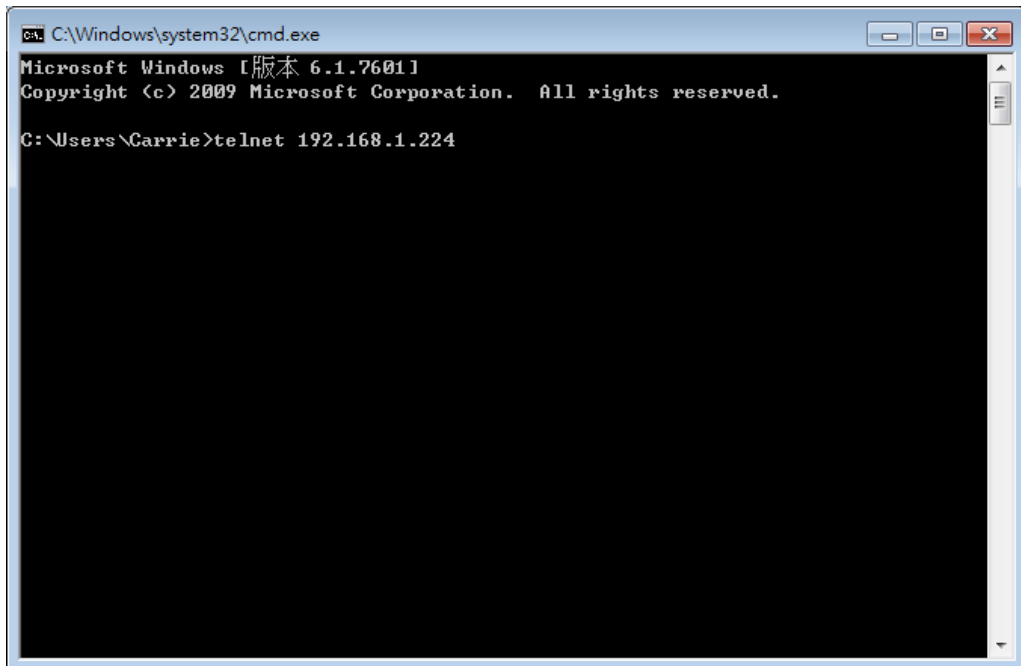
Info

For Windows 7 user, please make sure the Windows Features of Telnet Client has been turned on under Control Panel>>Programs.

Type cmd and press Enter. The Telnet terminal will be open later.



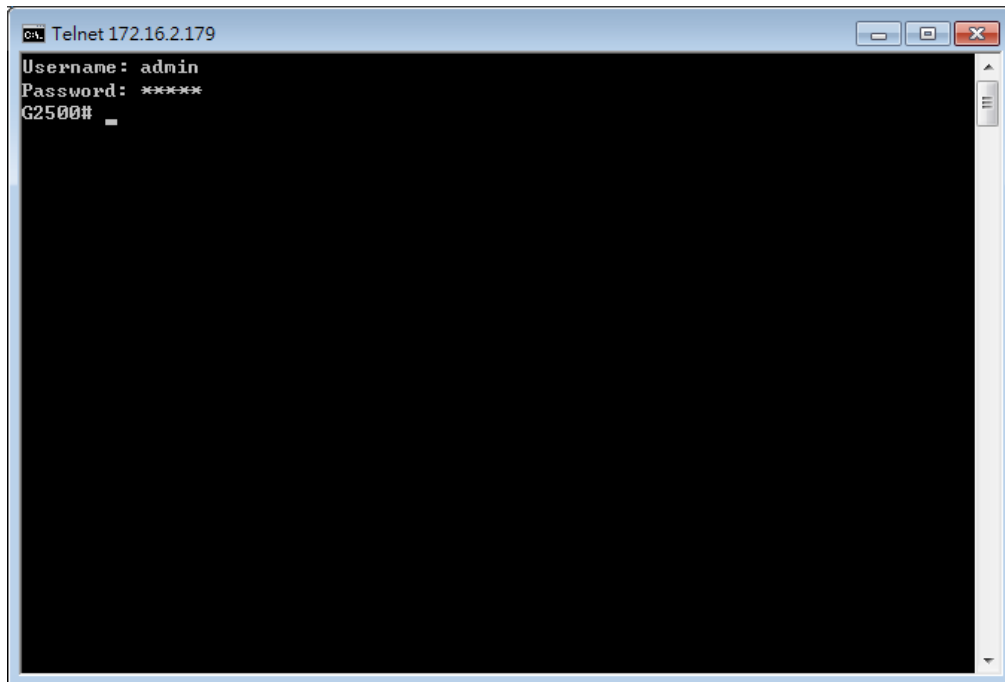
In the following window, type Telnet 192.168.1.224 as below and press Enter. Note that the IP address in the example is the default address of the router. If you have changed the default, enter the current IP address of the router.



Next, enter admin/admin for Account/Password.

For users using previous Windows system (e.g., XP), simply click **Start >> Run** and type **Telnet 192.168.1.224** in the Open box.

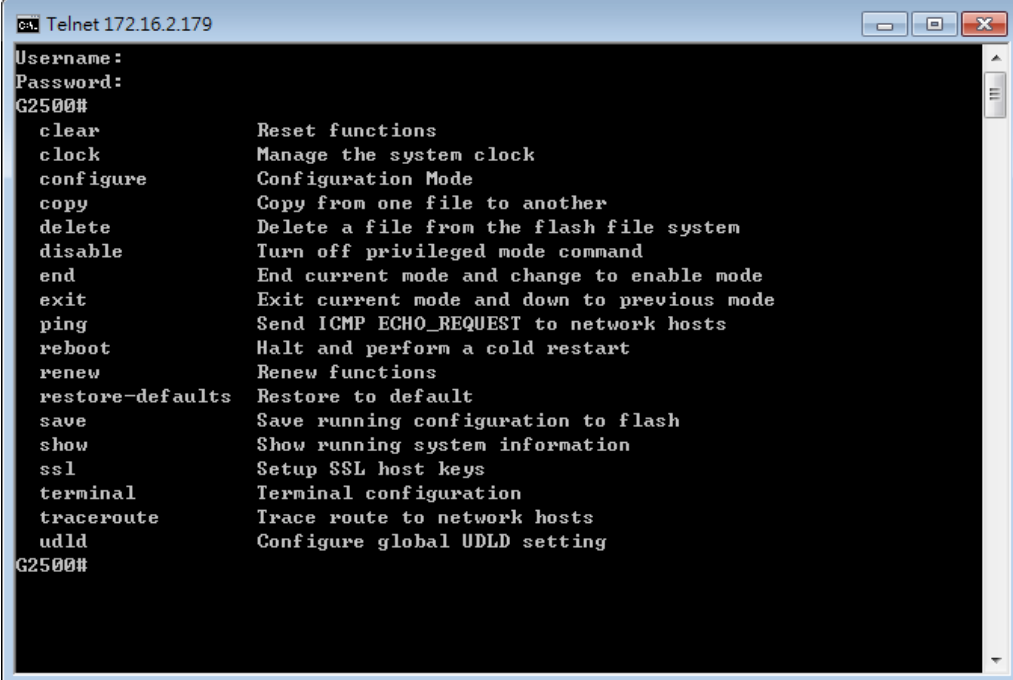
Next, enter **admin/admin** for Account/Password.



---

## X-2 Available Commands

Enter ? to get a list of available commands.



```
ca: Telnet 172.16.2.179
Username:
Password:
G2500#
clear          Reset functions
clock         Manage the system clock
configure     Configuration Mode
copy         Copy from one file to another
delete       Delete a file from the flash file system
disable      Turn off privileged mode command
end          End current mode and change to enable mode
exit        Exit current mode and down to previous mode
ping        Send ICMP ECHO_REQUEST to network hosts
reboot      Halt and perform a cold restart
renew       Renew functions
restore-defaults Restore to default
save        Save running configuration to flash
show        Show running system information
ssl         Setup SSL host keys
terminal    Terminal configuration
traceroute  Trace route to network hosts
udld        Configure global UDLN setting
G2500#
```

The available commands contain - clear, clock, configure, copy, delete, disable, end, exit, ping, reboot, renew, restore-defaults, save, show, ssl, terminal, traceroute and udld. Each command will be explained as follows.

Note: You can also enter ? to check if there are subcommands under current command.

---

### X-2-1 Clear Configuration

This command allows resetting the functions of ARP, interface, IP, IPv6, LACP, Line, LLDP, Logging, MAC, and Spanning Tree.

#### Telnet Command: clear arp

Use this command to clear entries in the ARP cache.

#### Syntax Items

clear arp

#### Description

| Syntax Items     | Description  |
|------------------|--|
| <i>clear arp</i> | <A.B.C.D> - Enter the IP address of the device (e.g., 192.168.1.224).<br><br>Related Syntax: <ul style="list-style-type: none"><li>● # clear arp</li><li>● # clear arp &lt;A.B.C.D&gt;</li></ul> |

#### Example

```
G2500# clear arp 192.168.1.224
G2500#
```

## Telnet Command: clear authentication

Use this command to clear authentication sessions based on LAN port, MAC address, or authentication type for 802.1x/MAC authentication.

### Syntax Items

clear authentication sessions

clear authentication sessions interfaces gigabitethernet

clear authentication sessions mac

clear authentication sessions session-id

clear authentication sessions type

### Description

| Syntax Items  | Description  |
|---|--|
| <i>clear authentication sessions</i>                            | Clear all of the sessions related to authentication.<br><b>Related Syntax:</b><br><ul style="list-style-type: none"> <li>● # clear authentication sessions</li> </ul>  |
| <i>clear authentication sessions interfaces gigabitethernet</i> | Clear the sessions of a specific interface.<br><1-50> - Enter the number of LAN port.<br><b>Related Syntax:</b><br><ul style="list-style-type: none"> <li>● # clear authentication sessions interfaces gigabitethernet &lt;1-50&gt;</li> </ul>   |
| <i>clear authentication sessions mac</i>                        | Clear the sessions with the MAC address set here.<br><A:B:C:D:E:F> - Enter the MAC address of the device that you want to clear the authentication information.<br><b>Related Syntax:</b><br><ul style="list-style-type: none"> <li>● # clear authentication sessions mac &lt;A:B:C:D:E:F&gt;</li> </ul>                                       |
| <i>clear authentication sessions session-id</i>                 | Clear the sessions with the string set here.<br><WORD> - Enter a string of a session that you want to clear.<br><b>Related Syntax:</b><br><ul style="list-style-type: none"> <li>● # clear authentication sessions session-id &lt;WORD&gt;</li> </ul>  |
| <i>clear authentication sessions type</i>                       | Clear the sessions with authentication type selected here.<br><dot1x> - Use 802.1x authentication.<br><mac> - Use mac-based authentication.<br><web> - Use web-based authentication.<br><b>Related Syntax:</b><br><ul style="list-style-type: none"> <li>● # clear authentication sessions type &lt;dot1x&gt;&lt;mac&gt;&lt;web&gt;</li> </ul> |

### Example

```
G2500# clear authentication sessions
No Auth Manager sessions currently exist
G2500# clear authentication sessions mac 48:5B:39:2F:A8:66
G2500# clear authentication sessions interfaces GigabitEthernet 2
G2500# clear authentication sessions session-id 0000000B002AFBE8
```

## Telnet Command: clear gvrp

Use this command to clear statistics or port error statistics for all interfaces or a specific interface (LAN or LAG).

### Syntax Items

clear gvrp error-statistics

clear gvrp statistics

### Description

| Syntax Items                       | Description  |
|------------------------------------|--|
| <i>clear gvrp error-statistics</i> | <p>Specify a LAN/LAG interface for clearing error statistics for GVRP.</p> <p>&lt;1-50&gt; - Enter the number (1 to 50) of LAN port.</p> <p>&lt;1-8&gt; - Enter the number (1 to 8) of LAG interface (IEEE 802.3 Link Aggregation Interface) that you want to clear the GVRP setting.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"><li>● # clear gvrp error-statistics interfaces GigabitEthernet &lt;1-50&gt;</li><li>● # clear gvrp error-statistics interfaces LAG &lt;1-8&gt;</li></ul> |
| <i>clear gvrp statistics</i>       | <p>Specify a LAN/LAG interface for clearing statistics for GVRP.</p> <p>&lt;1-50&gt; - Specify an interface for clearing statistics for GVRP.</p> <p>&lt;1-8&gt; - Specify LAG interface for clearing statistics for GVRP.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"><li>● # clear statistics interfaces GigabitEthernet &lt;1-50&gt;</li><li>● # clear statistics interfaces LAG &lt;1- 8&gt;</li></ul>   |

### Example

```
G2500# clear gvrp error-statistics interfaces GigabitEthernet 2
G2500#
G2500# clear gvrp error-statistics interfaces LAG 2
G2500#
```

## Telnet Command: clear interfaces

Use this command to clear statistics counters for all interfaces or a specific interface (LAN or LAG).

### Syntax Items

clear interfaces GigabitEthernet

clear interfaces LAG

### Description

| Syntax Items                            | Description  |
|---|--|
| <i>clear interfaces GigabitEthernet</i> | Specify a LAN interface for clearing statistics counters on that port.<br><1-50> - Enter the number (1 to 25) of LAN port.<br><br>Related Syntax: <ul style="list-style-type: none"><li>● # clear interfaces gigabitEthernet &lt;1-50&gt; counters</li></ul>                               |
| <i>clear interfaces LAG</i>             | Specify a LAG interface for clearing statistics counters on that port.<br><1-8> - Enter the number (1 to 8) of LAG interface (IEEE 802.3 Link Aggregation Interface).<br><br>Related Syntax: <ul style="list-style-type: none"><li>● # clear interfaces LAG &lt;1-8&gt; counters</li></ul> |

### Example

```
G2500# clear interfaces gigabitEthernet 3 counters
G2500# clear interfaces
G2500# clear interfaces lag 2 counters
G2500#
```

## Telnet Command: clear ip

Use this command to clear ARP inspection information, DHCP snooping database agent, and IGMP snooping groups (dynamic or static) information for all interfaces or a specific interface (LAN or LAG) with IP address.

### Syntax Items

clear ip arp

clear ip dhcp

clear ip igmp

### Description

| Syntax Items         | Description  |
|----------------------|--|
| <i>clear ip igmp</i> | snooping groups dynamic - Clear dynamic snooping groups of IGMP server.<br>snooping groups static - Clear static snooping groups of IGMP server.<br>snooping statistics - Clear snooping statistics for IGMP server.<br><br>Related Syntax: <ul style="list-style-type: none"><li>● # clear ip igmp snooping groups dynamic</li><li>● # clear ip igmp snooping groups static</li><li>● # clear ip igmp snooping statistics</li></ul> |

|                      |  |
|----------------------|--|
| <i>clear ip dhcp</i> | <p>snooping database statistics - Clear snooping database statistics for DHCP server.</p> <p>snooping interfaces GigabitEthernet / LAG- Specify a LAN / LAG interface for clearing DHCP snooping information.</p> <p>&lt;1-50&gt; - Enter the number (1 to 50) of LAN port.</p> <p>&lt;1-8&gt; - Specify a LAG interface for clearing DHCP snooping information.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● # clear ip dhcp snooping database statistics</li> <li>● # clear ip dhcp snooping interfaces GigabitEthernet &lt;1-50&gt; statistics</li> <li>● # clear ip dhcp snooping interfaces LAG &lt;1-8&gt; statistics</li> </ul> |
| <i>clear ip igmp</i> | <p>snooping groups dynamic - Clear dynamic snooping groups of IGMP server.</p> <p>snooping groups static - Clear static snooping groups of IGMP server.</p> <p>snooping statistics - Clear snooping statistics for IGMP server.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● # clear ip igmp snooping groups dynamic</li> <li>● # clear ip igmp snooping groups static</li> <li>● # clear ip igmp snooping statistics</li> </ul>   |

### Example

```
G2500# clear ip igmp snooping groups dynamic
G2500#
```

## Telnet Command: clear ipv6

Use this command to clear MLD snooping configuration for dynamic / static group(s) with IPv6 address.

### Syntax Items

`clear ipv6 mld`

### Description

| Syntax Items          | Description   |
|-----------------------|---|
| <i>clear ipv6 mld</i> | <p>snooping groups dynamic - Clear dynamic snooping groups of MLD.</p> <p>snooping groups static - Clear static snooping groups of MLD.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● # clear ipv6 mld snooping groups dynamic</li> <li>● # clear ipv6 mld snooping groups static</li> </ul> |

### Example

```
G2500# clear ipv6
G2500# clear ipv6 mld snooping groups dynamic
G2500# clear ipv6 mld snooping groups dynamic?
<cr>
G2500# clear ipv6 mld snooping groups static
```



## Telnet Command: clear lacp

Use this command to clear LACP configuration for specified LAG interface or all LAG interfaces.

### Syntax Items

`clear lacp <1-8> counters`

`clear lacp counters`

### Description

| Syntax Items                        | Description  |
|-------------------------------------|--|
| <code>clear lacp &lt;1-8&gt;</code> | <1-8> - Enter the number (1 to 8) of LAG interface (IEEE 802.3 Link Aggregation Interface).<br><br>Related Syntax: <ul style="list-style-type: none"><li>● # clear lacp &lt;1-8&gt; counters</li></ul> |
| <code>clear lacp counters</code>    | Clear LACP configuration for all LAG interfaces.<br><br>Related Syntax: <ul style="list-style-type: none"><li>● # clear lacp counters</li></ul>  |

### Example

```
G2500# clear lacp 1 counters
No interfaces configured in the channel group
G2500#
```

## Telnet Command: clear line

Use this command to clear line settings including SSH (Secure Shell) configuration and telnet daemon configuration.

### Syntax Items

`clear line ssh`

`clear line telnet`

### Description

| Syntax Items                   | Description  |
|--------------------------------|--|
| <code>clear line ssh</code>    | Clear SSH configuration for line connection.<br><br>Related Syntax: <ul style="list-style-type: none"><li>● # clear line ssh</li></ul>           |
| <code>clear line telnet</code> | Clear SSH Telnet configuration for line connection.<br><br>Related Syntax: <ul style="list-style-type: none"><li>● # clear line telnet</li></ul> |

### Example

```
G2500# clear line ssh
G2500# clear line telnet
```

## Telnet Command: clear lldp

Use this command to clear LLDP statistics or reset LLDP information.

### Syntax Items

clear lldp global  
clear lldp interfaces

### Description

| Syntax Items                 | Description  |
|------------------------------|--|
| <i>clear lldp global</i>     | Clear all of the statistics related to LLDP.<br><b>Related Syntax:</b> <ul style="list-style-type: none"><li>● # clear lldp global statistics</li></ul>  |
| <i>clear lldp interfaces</i> | Specify a LAN / LAG interface for clearing LLDP information.<br><1-50> - Enter the number (1 to 50) of LAN port.<br><1-8> - Enter the number (1 to 8) of LAG interface (IEEE 802.3 Link Aggregation Interface).<br><b>Related Syntax:</b> <ul style="list-style-type: none"><li>● # clear lldp interfaces GigabitEthernet &lt;1-50&gt; statistics</li><li>● # clear lldp interfaces LAG &lt;1-8&gt; statistics</li></ul> |

### Example

```
G2500# clear lldp global statistics
G2500#
G2500# clear lldp interfaces LAG 1 statistics
G2500# clear lldp interfaces gigabitethernet 1 statistics
G2500#
```

## Telnet Command: clear logging

Use this command to clear log messages from the internal logging buffer and flash.

### Syntax Items

clear logging buffered  
clear logging file

### Description

| Syntax Items                  | Description   |
|-------------------------------|---|
| <i>clear logging buffered</i> | Clear the log stored in RAM.<br><b>Related Syntax:</b> <ul style="list-style-type: none"><li>● # clear logging buffered</li></ul> |
| <i>clear logging file</i>     | Clear the log stored in flash.<br><b>Related Syntax:</b> <ul style="list-style-type: none"><li>● # clear logging file</li></ul>   |

## Example

```
G2500# clear logging buffered
G2500# clear logging file
G2500#
```

## Telnet Command: clear mac

Use this command to clear MAC configuration related to VLAN, LAG, and LAN port.

### Syntax Items

clear mac

### Description

| Syntax Items                   | Description   |
|--------------------------------|---|
| <i>clear mac address-table</i> | <1-50> - Enter the number (1 to 50) of LAN port.<br><1-8>- Enter the number (1 to 8) of LAG interface (IEEE 802.3 Link Aggregation Interface).<br><1-4094> - Specify a VLAN ID by entering its number.<br><br><b>Related Syntax:</b> <ul style="list-style-type: none"><li>● # clear mac address-table dynamic interfaces GigabitEthernet &lt;1-50&gt;</li><li>● # clear mac address-table dynamic interfaces LAG &lt;1-8&gt;</li><li>● # clear mac address-table dynamic vlan &lt;1-4094&gt;</li></ul> |

## Example

```
G2500# clear mac address-table dynamic vlan 2038
G2500# clear mac address-table dynamic interfaces gigabitethernet 3
G2500#
```

## Telnet Command: clear mvr

Use this command to clear information for all members (including dynamic, static) of MVR.

### Syntax Items

clear mvr members

### Description

| Syntax Items             | Description  |
|--------------------------|--|
| <i>clear mvr members</i> | Clear information for dynamic / static members.<br><br><b>Related Syntax:</b> <ul style="list-style-type: none"><li>● # clear mvr members dynamic</li><li>● # clear mvr members static</li></ul> |

## Example

```
G2500# clear mvr members dynamic
G2500# clear mvr members static
G2500#
```

## Telnet Command: clear spanning-tree

Use this command to clear running system information.

### Syntax Items

clear spanning-tree

### Description

| Syntax Items                          | Description  |
|---------------------------------------|--|
| <i>clear spanning-tree interfaces</i> | <p>Specify a LAN interface for clearing its running information.</p> <p>&lt;1-50&gt;- Enter the number (1 to 50) of LAN port.</p> <p>&lt;1-8&gt;- Enter the number (1 to 8) of LAG interface (IEEE 802.3 Link Aggregation Interface).</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"><li>● # clear spanning-tree interfaces GigabitEthernet &lt;1-50&gt; statistics</li><li>● # clear spanning-tree interfaces LAG &lt;1-8&gt; statistics</li></ul> |

### Example

```
G2500# clear spanning-tree interfaces GigabitEthernet
      <1-50> GigabitEthernet device number
G2500# clear spanning-tree interfaces gigabitethernet 3 statistics
G2500# clear spanning-tree interfaces LAG 1 statistics
G2500#
```

---

## X-2-2 Clock Configuration

This command allows managing the system clock.

### Telnet Command: clock set

Use this command to configure the system clock manually.

### Syntax Items

clock set

### Description

| Syntax Items     | Description   |
|------------------|---|
| <i>clock set</i> | <p>Set current by entering hours, minutes, seconds, month, date and year with the format listed below:</p> <p>&lt;HH:MM:SS&gt; - Hour, minute, second (e.g., 08:10:30).</p> <p>&lt;Jan&gt; - January.</p> <p>&lt;feb&gt; - February</p> <p>&lt;mar&gt; - March</p> <p>&lt;apr&gt; - April</p> <p>&lt;may&gt; - May</p> <p>&lt;jun&gt; - June</p> <p>&lt;jul&gt; - July</p> <p>&lt;aug&gt; - August</p> <p>&lt;sep&gt; - September</p> <p>&lt;oct&gt; - October</p> <p>&lt;nov&gt; - November</p> <p>&lt;dec&gt; - December</p> <p>&lt;1-31&gt; - Date 1 to 31.</p> <p>&lt;2000-2035&gt; - Year of 2000 to 2035.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"><li>● # clock set HH:MM:SS<br/>jan/feb/mar/apr/may/jun/jul/aug/sep/oct/nov/dec &lt;1-31&gt;<br/>&lt;2000-2035&gt;</li></ul> |

### Example

```
G2500# clock set 12:10:30 jan 1 2019
2019-01-01 12:10:30 UTC+8
```

---

## X-2-3 Configure Configuration

This command allows configuring the settings related to VigorSwitch.

Available sub-commands under Configure include:

*aaa, authentication, boot, clock, custom, dos, dot1x, do, dray\_surveillance, enable, end, errdisable, exit, gvrp, hostname, interface, ip, ipv6, jumbo-frame, lacp, lag, line, lldp, logging, logmail, loop-protection, mac, mailalert, management, management-vlan, mirror, mvr, no, openvpn, poe, port-security, qos, radius, schedule, snmp, sntp, spanning-tree, start-up, storm-control, surveillance-vlan, system, tacacs, tr069, udd, username, vlan, voice-vlan, webhook*

Before configuration, you have to enter "configure" to access into next phase.

To return to previous phase, enter "exit"

### Example

```
G2500# configure
G2500(config)#
G2500(config)# exit
G2500#
```

### Telnet Command: aaa

Use this command to add a login authentication list to authenticate with local, tacacs+, radius, and none service.

### Syntax Items

aaa authentication enable

aaa authentication login

### Description

| Syntax Items                     | Description   |
|----------------------------------|---|
| <i>aaa authentication enable</i> | <p>Enable authentication is used only on CLI for a user trying to switch from User EXEC (&gt;) mode to Privileged EXEC (#) mode.</p> <p>enable - Enable the authentication list.</p> <p>&lt;LISTNAME&gt; - Enter a string as the list name for authentication type. Default value is "default".</p> <p>&lt;none, enable, tacacs+, radius&gt; - Specify the authentication method by entering none, enable, tacacs+ or radius.</p> <ul style="list-style-type: none"><li>● None: Do nothing and just make user be authenticated.</li><li>● Enable: Use local password to authenticate.</li><li>● Tacacs+: Use remote Tacas+ server to authenticate.</li><li>● Radius: Use remote Radius server to authenticate.</li></ul> <p>default - It is used to configure default enable authentication.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"><li>● &lt;config&gt;#aaa authentication enable &lt;LISTNAME&gt; &lt;none, enable, tacacs+, radius&gt;</li><li>● &lt;config&gt;#aaa authentication enable default &lt;none, enable, tacacs+, radius&gt;</li></ul> |
| <i>aaa authentication login</i>  | <p>Login authentication is used when a user tries to login into the switch.</p> <p>&lt;LISTNAME&gt; - Enter a string as the list name for authentication type. Default value is "default".</p>  |

|  |   |
|--|---|
|  | <p>&lt;none, enable, tacacs+, radius&gt; -Specify the authentication method by entering none, enable, tacacs+ or radius.</p> <p>default - It is used to configure default login authentication.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;#aaa authentication login &lt;LISTNAME&gt; &lt;none, enable, tacacs+, radius&gt;</li> <li>● &lt;config&gt;#aaa authentication login default &lt;none, enable, tacacs+, radius&gt;</li> </ul> |
|--|---|

## Example

```
G2500# configure
G2500(config)#
G2500(config)# aaa authentication enable LISTNAME enable
G2500(config)#
G2500(config)# exit
G2500# show aaa authentication enable lists
  Enable List Name   Authentication Method List
-----
                default           enable
                LISTNAME           enable
G2500#
```

## Telnet Command: authentication

Use this command to enable the global setting of 802.1x/MAC/WEB authentication network access control (default is disabled for all).

### Syntax Items

authentication dot1x

authentication guest-vlan

authentication mac

authentication web

### Description

| Syntax Items                     | Description   |
|----------------------------------|---|
| <i>authentication dot1x</i>      | <p>Enable 802.1x authentication by entering the word, dot1x after authentication.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# authentication dot1x</li> </ul>  |
| <i>authentication guest-vlan</i> | <p>Configure the guest VLAN.</p> <p>&lt;1-4094&gt; - Specify a guest VLAN ID by entering its number.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# authentication guest-vlan &lt;1-4094&gt;</li> </ul>   |
| <i>authentication mac</i>        | <p>Enable MAC authentication by entering the word, mac after authentication.</p> <p>mac local - Local database for MAC-Based authentication. It can add local MAC authentication hosts in database.</p> <p>&lt;A:B:C:D:E:F&gt; - Enter the MAC address to be added for authentication.</p> <p>control auth - Set a local entry control mode, auth (the host will be set to authorized) or unauth (the host will be set to unauthorized).</p> <p>vlan &lt;1-4094&gt; - Specify a VLAN ID by entering its number</p> <p>reauth-period &lt;300-4294967294&gt; - Set a time to initiate automatic</p> |

|                                  |   |
|----------------------------------|---|
|                                  | <p>re-authentication.</p> <p>inactive-timeout &lt;60-65535&gt;- Set the inactive timeout for MAC authentication host. After the time interval, if there is no activity from the client, then it will be unauthorized by Vigor system.</p> <p>control unauth - Set a local entry control mode as "unauth" to let the host set as unauthorized.</p> <p>radius mac-case &lt;lower / upper&gt; - Set RADIUS user ID with lower case or upper case.</p> <p>radius mac-delimiter &lt;colon/dot/hyphen/none&gt; - Select RADIUS user ID delimiter. In which,</p> <p style="padding-left: 40px;">colon: XX:XX:XX:XX:XX:XX</p> <p style="padding-left: 40px;">dot: XX.XX.XX.XX.XX.XX</p> <p style="padding-left: 40px;">hyphen: XX-XX-XX-XX-XX-XX</p> <p style="padding-left: 40px;">none: XXXXXXXXXXXX</p> <p>gap &lt;2/4/6&gt; - Select delimiter gap.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;#authentication mac</li> <li>● &lt;config&gt;#authentication mac local &lt;A:B:C:D:E:F&gt; control auth inactive-timeout &lt;60-65535&gt;</li> <li>● &lt;config&gt;#authentication mac local &lt;A:B:C:D:E:F&gt; control auth reauth-period &lt;300-4294967294&gt;</li> <li>● &lt;config&gt;#authentication mac local &lt;A:B:C:D:E:F&gt; control auth vlan &lt;1-4094&gt;</li> <li>● &lt;config&gt;#authentication mac local &lt;A:B:C:D:E:F&gt; control auth vlan&lt;1-4094&gt; reauth-period &lt;300-4294967294&gt;</li> <li>● &lt;config&gt;#authentication mac local &lt;A:B:C:D:E:F&gt; control auth vlan&lt;1-4094&gt; reauth-period &lt;300-4294967294&gt; inactive-timeout &lt;60-65535&gt;</li> <li>● &lt;config&gt;#authentication mac local &lt;A:B:C:D:E:F&gt; control unauth</li> <li>● &lt;config&gt;#authentication mac radius mac-case &lt;lower / upper&gt;</li> <li>● &lt;config&gt;#authentication mac radius mac-delimiter &lt;colon/dot/hyphen/none&gt;</li> <li>● &lt;config&gt;#authentication mac radius mac-delimiter &lt;colon/dot/hyphen/none&gt; gap &lt;2/4/6&gt;</li> </ul> |
| <p><i>authentication web</i></p> | <p>Web - Enable web authentication by entering the word "web" after "authentication".</p> <p>username &lt;WORD&gt; - Specify a username.</p> <p>password &lt;string&gt; - Set a password.</p> <p>vlan &lt;1-4094&gt; - Specify a VLAN ID by entering its number.</p> <p>reauth-period &lt;30-4294967294&gt; - Set a time to initiate automatic re-authentication.</p> <p>inactive-timeout &lt;60-65535&gt;- Set the inactive timeout for MAC authentication host. After the time interval, if there is no activity from the client, then it will be unauthorized by Vigor system.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;#authentication web</li> <li>● &lt;config&gt;#authentication web local username &lt;WORD&gt; password &lt;string&gt; inactive-timeout &lt;60-65535&gt;</li> <li>● &lt;config&gt;#authentication web local username &lt;WORD&gt; password &lt;string&gt; reauth-period &lt;300-4294967294&gt;</li> <li>● &lt;config&gt;#authentication web local username &lt;WORD&gt; password &lt;string&gt; reauth-period &lt;300-4294967294&gt; inactive-timeout &lt;60-65535&gt;</li> <li>● &lt;config&gt;#authentication web local username &lt;WORD&gt;</li> </ul>   |



---

password <string> vlan<1-4094>

- <config>#authentication web local username <WORD>  
password <string> vlan<1-4094> reauth-period  
<30-4294967294> inactive-timeout <60-65535>
- 

## Example

```
G2500# configure
G2500(config)# authentication dot1x
G2500(config)# vlan 3
G2500(config-vlan)# exit
G2500(config)# authentication guest-vlan 3
G2500(config)#
G2500(config)# exit
G2500# show authentication
Authentication dot1x state      : enabled
Authentication mac state      : disabled
Authentication web state      : disabled
Guest VLAN                     : enabled (3)
Mac-auth Radius User ID Format : XXXXXXXXXXXXXXX
Mac-auth Local Entry          :
Web-auth Local Entry          :
Interface Configurations
Interface GigabitEthernet1
  Admin Control                : disable
  Host Mode                    : multi-auth
  Type dot1x State             : disabled
  Type mac State               : disabled
  Type web State               : disabled
  Type Order                   : dot1x
  MAC/WEB Method Order        : radius
  Guest VLAN                   : disabled
  Reauthentication             : disabled
  Max Hosts                    : 256
  VLAN Assign Mode             : static
--More--
.....
G2500# configure
G2500(config)# authentication mac local 00:11:22:33:00:01 control auth vlan
3 reauth-period 500 inactive-timeout 300
G2500(config)#
G2500(config)# authentication mac local 00:11:22:33:00:01 control unauth
G2500(config)#
G2500(config)# authentication web local username user_1 password 1234tw vlan
3 reauth-period 600 inactive-timeout 700
G2500(config)#
```

## Telnet Command: boot

Use this command to have a backup image in the flash partition. Select the active firmware image, and another firmware image will become a backup one.

### Syntax Items

boot system

### Description

| Syntax Items       | Description  |
|--------------------|--|
| <i>boot system</i> | Boot the system from flash image partition 0 / 1.<br><b>Related Syntax:</b> <ul style="list-style-type: none"> <li>● &lt;config&gt;# boot system image0</li> <li>● &lt;config&gt;# boot system image1</li> </ul> |

## Example

```

G2500# configure
G2500(config)#
G2500(config)# boot system image0
Select "image0" Success
G2500(config)# exit
G2500#
G2500# show boot
Image Version      Date                Status      File Name
-----
0      1.0.2      2017-08-29 09:44:57  Not active*  2280_r442_220RC1.all
1      2.3.2      2018-05-16 09:14:31  Active      p2280_r734_230RC4.all

"*" designates that the image was selected for the next boot

G2500#

```

## Telnet Command: clock

Use this command to configure time zone, summer-time and external time source for the system clock.

### Syntax Items

clock auto timezone  
clock source local  
clock source sntp  
clock summer-time  
clock timezone

### Description

| Syntax Items               | Description   |
|----------------------------|---|
| <i>clock auto timezone</i> | VigorSwitch sets the time zone automatically.   |
| <i>clock source local</i>  | Configure an external time source for the system clock.<br>"local" means to use static time. It is the default setting.<br><b>Related Syntax:</b> <ul style="list-style-type: none"><li>● &lt;config&gt;# clock source local</li></ul>  |
| <i>clock source sntp</i>   | Configure an external time source for the system clock. "sntp" means to use SNTP time.<br><b>Related Syntax:</b> <ul style="list-style-type: none"><li>● &lt;config&gt;# clock source sntp</li></ul>  |
| <i>clock summer-time</i>   | Configure the system to automatically switch to summer time (daylight saving time).<br>ACRONYM - Specify the acronym name of time zone. The acronym of the time zone will be displayed when summer time is in effect. If unspecified, the time zone acronym will be used in default. (1-4 chars)<br><jan/feb/mar/apr/may/jun/jul/aug/sep/oct/nov/dec> - Indicate January, February, March, April, May, June, July, August, September, October, November, December.<br><1-31> means date 1 to 31.<br><2000-2037> - means year of 2000 to 2035.<br><HH:MM> - means hours and minutes.<br>recurring - Summer time should start and end on the corresponding specified days every year.<br><1-1440>- Set the number of minutes to add during the summer time. The default number is 60.<br>eu - The summer time is based on the European Union rules. (Start point - last Sunday in March, End point - last Sunday in October)<br>usa - The summer time is based on the United States rules. (Start point - second Sunday in March, End point - first Sunday in November)<br>first - The first week of the month.<br>last - The last week of the month.<br><sun/mon/tue/wed/thu/fri/sat> - Indicate Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday.<br><jan/feb/mar/apr/may/jun/jul/aug/sep/oct/nov/dec> - Indicate January, February, March, April, May, June, July, August, September, October, November, December.<br><first/last>- Specify the first week or the last week of the month.<br><1-5> - Specify the number of the week in the month.<br>Note that the first group of month, date, hour and minute is used for configuring starting time, and the second group is used for |

|  |   |
|--|---|
|  | <p>configuring ending time.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# clock summer-time ACRONYM date<br/>&lt;jan/feb/mar/apr/may/jun/jul/aug/sep/oct/nov/dec&gt;<br/>&lt;1-31&gt; &lt;2000-2037&gt; &lt;HH:MM&gt;<br/>&lt;jan/feb/mar/apr/may/jun/jul/aug/sep/oct/nov/dec&gt;&lt;1-31&gt;<br/>&gt;&lt;2000-2037&gt; &lt;HH:MM&gt;</li> <li>● &lt;config&gt;# clock summer-time ACRONYM recurring eu &lt;1-1440&gt;</li> <li>● &lt;config&gt;# clock summer-time ACRONYM recurring usa<br/>&lt;1-1440&gt;</li> <li>● &lt;config&gt;# clock summer-time ACRONYM recurring first<br/>&lt;sun/mon/tue/wed/thu/fri/sat&gt;&lt; jan / feb / mar / apr / may<br/>/ jun/jul/aug/sep/oct/nov/dec&gt; &lt;HH:MM&gt; &lt;first/last&gt;<br/>&lt;sun/mon/tue/wed/thu/fri/sat&gt;&lt; jan /feb /mar /apr/may/<br/>jun/jul/aug/sep/oct/nov/dec&gt; &lt;HH:MM&gt; &lt;1-14400&gt;</li> <li>● &lt;config&gt;# clock summer-time ACRONYM recurring last<br/>&lt;sun/mon/tue/wed/thu/fri/sat&gt;&lt; jan /feb /mar /apr /may<br/>/jun/jul/aug/sep/oct/nov/dec&gt; &lt;HH:MM&gt;<br/>&lt;first/last&gt;&lt;sun/mon/tue/wed/thu/fri/sat&gt;&lt; jan /feb /mar<br/>/apr/may/ jun/jul/aug/sep/oct/nov/dec&gt; &lt;HH:MM&gt;<br/>&lt;1-14400&gt;</li> <li>● &lt;config&gt;# clock summer-time ACRONYM recurring &lt;1-5&gt;<br/>&lt;sun/mon/tue/wed/thu/fri/sat&gt;&lt; jan /feb /mar /apr /may<br/>/jun/jul/aug/sep/oct/nov/dec&gt; &lt;HH:MM&gt; &lt;1-5&gt;<br/>&lt;sun/mon/tue/wed/thu/fri/sat&gt;&lt; jan /feb /mar /apr<br/>/may/jun/jul/aug/sep/oct/nov/dec&gt; &lt;HH:MM&gt; &lt;1-14400&gt;</li> </ul> |
| <p><i>clock timezone ACRONYM<br/>&lt;-12-13&gt; minutes &lt;0-59&gt;</i></p> | <p>Set the time zone for display purposes.</p> <p>ACRONYM - Specify the acronym name of time zone. The acronym of the time zone will be displayed when summer time is in effect. If unspecified, the time zone acronym will be used in default. (1-4 chars)</p> <p>&lt;-12-13&gt; - Specify the hour offset (from -12 to +13) of time zone.</p> <p>minutes &lt;0-59&gt; - Specify the minute difference from UTC.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# clock timezone ACRONYM &lt;-12-13&gt; minutes &lt;0-59&gt;</li> </ul>  |

## Example

```
G2500# configure
G2500(config)# clock source sntp
G2500(config)# exit
G2500# show clock detail
2019-01-05 06:51:23 UTC+8
Time source is sntp
Time zone:
Acronym is
Offset is UTC+8
G2500# configure
G2500(config)# clock summer-time tw date jan 30 2019 23:30 feb 1 2019 20:50
G2500(config)# exit
G2500# show clock detail
2019-01-05 07:13:49 UTC+8
Time source is sntp

Time zone:
Acronym is ACRONYM
Offset is UTC-10:08

Summertime:
```

```

Acronym is tw
Starting and ending on a specific date.
Begins at 1 30 19 23:30
Ends at 2 1 19 20:50
Offset is 60 minutes.
G2500# configure
G2500(config)# clock summer-time ACRONYM recurring eu 1200
G2500(config)# clock summer-time ACRONYM recurring first mon jan 10:10 first
sun feb 10:10 1000
G2500(config)# exit
G2500# show clock detail
2019-01-05 11:37:18 UTC+8
Time source is sntp
Time zone:
Acronym is
Offset is UTC+8
Summertime:
Acronym is ACRONYM
Recurring every year.
Begins at 1 1 1 10:10
Ends at 1 0 2 10:10
Offset is 1000 minutes.

```

## Telnet Command: custom

Use this command to enable the module settings.

### Syntax Items

custom enable

### Description

| Syntax Items         | Description   |
|----------------------|---|
| <i>custom enable</i> | Enable the module settings.<br>Related Syntax:<br>● <config># custom enable |

### Example

```

G2500# configure
G2500(config)# custom enable
G2500(config)#

```

## Telnet Command: dos

Use this command to enable specific Denial of Service (DoS) protection.

### Syntax Items

```

dos daeqsa-deny
dos icmp-frag-pkts-deny
dos icmp-ping-max-length
dos icmpv4-ping-max-check
dos icmpv6-ping-max-check
dos ipv6-min-frag-size-check
dos ipv6-min-frag-size-length
dos land-deny
dos nullscan-deny

```

dos pod-deney  
 dos smurf-deney  
 dos smurf-netmask  
 dos syn-sport1024-deney  
 dos synfin-deney  
 dos synrst-deney  
 dos tcp-frag-off-min-check  
 dos tcpblat-deney  
 dos tcphdr-min-check  
 dos tcphdr-min-length  
 dos udpblat-deney  
 dos xma-deney

## Description

| Syntax Items                                      | Description  |
|---|--|
| <i>dos daeqsa-deney</i>                           | Drop the packets if the destination MAC address equals to the source MAC address.<br><b>Related Syntax:</b><br>● <config># dos daeqsa-deney  |
| <i>dos icmp-frag-pkts-deney</i>                   | Drop the fragmented ICMP packets.<br><b>Related Syntax:</b><br>● <config># dos icmp-frag-pkts-deney  |
| <i>dos icmp-ping-max-length</i>                   | Set the maximum packet size for ICMPv4/ICMPv6 ping operation.<br><0-65535> - Specify a packet number.<br><b>Related Syntax:</b><br>● <config># dos icmp-ping-max-length <0-65535>  |
| <i>dos icmpv4-ping-max-check</i>                  | Check ICMPv4 ping maximum packets size and drop the packets larger than the maximum packet size defined by the command, <i>dos icmp-ping-max-length</i> .<br><b>Related Syntax:</b><br>● <config># dos icmpv4-ping-max-check |
| <i>dos icmpv6-ping-max-check</i>                  | Check ICMPv6 ping maximum packets size and drop the packets larger than the maximum packet size defined by the command, <i>icmp-ping-max-length</i> .<br><b>Related Syntax:</b><br>● <config># dos icmpv6-ping-max-check     |
| <i>dos ipv6-min-frag-size-check</i>               | Check minimum size of IPv6 fragments.<br><b>Related Syntax:</b><br>● <config># dos ipv6-min-frag-size-check  |
| <i>dos ipv6-min-frag-size-length</i><br><0-65535> | Set the minimum packet size of IPv6 fragmented packets.<br><0-65535> - Specify a packet number.<br><b>Related Syntax:</b><br>● <config># dos ipv6-min-frag-size-length <0-65535>   |
| <i>dos land-deney</i>                             | Drop the packets if the source IP address equals to destination IP address.<br><b>Related Syntax:</b><br>● <config># dos land-deney  |
| <i>dos nullscan-deney</i>                         | Drop the packets if attacked by NULL Scan.<br><b>Related Syntax:</b><br>● <config># dos nullscan-deney   |
| <i>dos pod-deney</i>                              | Drop the packets if attacked by Ping of Death.<br><b>Related Syntax:</b>   |

|                                   |  |
|-----------------------------------|--|
|                                   | <ul style="list-style-type: none"> <li>● &lt;config&gt;# dos pod-deny</li> </ul>   |
| <i>dos smurf-deny</i>             | <p>Drop the packets if encountered Smurf attack.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# dos smurf-deny</li> </ul>  |
| <i>dos smurf-netmask</i>          | <p>Set the smurf attack size.</p> <p>&lt;0-32&gt; - Enter a number as smurf attacks size.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# dos smurf-netmask &lt;0-32&gt;</li> </ul>             |
| <i>dos syn-sport11024-deny</i>    | <p>Drop SYN packets with sport less than 1024.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# dos syn-sport11024-deny</li> </ul>   |
| <i>dos synfin-deny</i>            | <p>Drop the packets with SYN and FIN bits set.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# dos synfin-deny</li> </ul>   |
| <i>dos synrst-deny</i>            | <p>Drop the packets with SYNC and RST bits set.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# dos synrst-deny</li> </ul>  |
| <i>dos tcp-frag-off-min-check</i> | <p>Drop the TCP fragmented packet with offset equals to the minimum packet size.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# dos tcp-frag-off-min-check</li> </ul>                          |
| <i>dos tcpblat-deny</i>           | <p>Drop the packets if the source TCP port equals to destination TCP port.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# dos tcpblat-deny</li> </ul>  |
| <i>dos tcphdr-min-check</i>       | <p>Check the minimum TCP header and drop the TCP packets with the header smaller than the minimum size defined.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# dos tcphdr-min-check</li> </ul> |
| <i>dos tcphdr-min-length</i>      | <p>Set the minimum size of TCP header.</p> <p>&lt;0-65535&gt; - Specify a packet number.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# dos tcphdr-min-length &lt;0-65535&gt;</li> </ul>       |
| <i>dos udpblat-deny</i>           | <p>Drop the packets if the source UDP port equals to destination UDP port.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# dos udpblat-deny</li> </ul>  |
| <i>dos xma-deny</i>               | <p>Drop the packets if the sequence number is zero and the FIN, URG and PSH bits are set already.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# dos xma-deny</li> </ul>                       |

## Example

```
G2500# configure
G2500(config)#
G2500(config)# dos icmp-ping-max-length 25252
G2500(config)# dos icmpv4-ping-max-check
G2500(config)#
```

## Telnet Command: dray\_surveillance

Use this command to enable / disable the ONVIF.

### Syntax Items

dray\_surveillance add

dray\_surveillance direct-add

dray\_surveillance set

### Description

| Syntax Items                        | Description  |
|-------------------------------------|--|
| <i>dray_surveillance add</i>        | Add an IP device for surveillance.<br>WORD <36-36> - Enter the UUID string of the IP camera or IP-based device.<br><b>Related Syntax:</b> <ul style="list-style-type: none"><li>● &lt;config&gt;# dray_surveillance add device uuid WORD &lt;36-36&gt;</li><li>● &lt;config&gt;# dray_surveillance add group uuid WORD &lt;36-36&gt;</li></ul> |
| <i>dray_surveillance direct-add</i> | WORD <36-36> - Enter the UUID string of the IP camera or IP-based device.<br><b>Related Syntax:</b> <ul style="list-style-type: none"><li>● &lt;config&gt;# dray_surveillance direct-add device uuid WORD &lt;36-36&gt;</li></ul>  |
| <i>dray_surveillance set</i>        | WORD <36-36> - Enter the UUID string of the IP camera or IP-based device.<br><b>Related Syntax:</b> <ul style="list-style-type: none"><li>● &lt;config&gt;# dray_surveillance set device uuid WORD &lt;36-36&gt;</li><li>● &lt;config&gt;# dray_surveillance set group uuid WORD &lt;36-36&gt;</li></ul>                                       |

### Example

```
G2500# configure
G2500(config)#
G2500(config)# dray_surveillance
G2500(config)#
G2500(config)# dray_surveillance add device uuid
53d7762a-c52b-4bb9-8000-305501e0f35f
G2500(config)#
```

## Telnet Command: do

Use this command to execute a command immediately.

### Syntax Items

do SEQUENCE

### Description

| Syntax Items    | Description  |
|-----------------|--|
| <i>SEQUENCE</i> | Enter the command that you want to execute immediately.<br><b>Related Syntax: (for example)</b> <ul style="list-style-type: none"><li>● &lt;config&gt;# do show info</li></ul> |



## Example

```
G2500(config)# do show info
System Name       : P2280x
System Location   : Default
System Contact    : Default
MAC Address       : 00:1D:AA:43:D1:3E
IP Address        : 192.168.1.238
Subnet Mask       : 255.255.255.0
Loader Version    : 1.0.4
Loader Date       : Apr 18 2019 - 16:31:58
Firmware Version  : 2.5.0
Firmware Date     : May 22 2019 - 18:09:18
Firmware Revision : 1421
System Object ID  : 1.3.6.1.4.1.7367
System Up Time    : 0 days, 5 hours, 33 mins, 8 secs
PoE SW Version    : 211
G2500(config)#
```

## Telnet Command: enable

Use this command to configure local password with encrypted string or not.

### Syntax Items

enable password  
enable privilege  
enable secret

### Description

| Syntax Items            | Description  |
|-------------------------|--|
| <i>enable password</i>  | Edit the password for each privilege level for activating authentication.<br><1-15> - Enter a number for specifying a privilege level. Default value is 15.<br><b>Related Syntax:</b> <ul style="list-style-type: none"><li>● &lt;config&gt;# enable password &lt;1-15&gt;</li></ul>   |
| <i>enable privilege</i> | Edit the privilege level of the password for local user.<br><1-15> - Enter a number for specifying a privilege level. Default value is 15.<br><string> - Enter a new string as the password.<br><b>Related Syntax:</b> <ul style="list-style-type: none"><li>● &lt;config&gt;# enable privilege &lt;1-15&gt; password &lt;string&gt; (This password will <b>NOT</b> be encrypted.)</li><li>● &lt;config&gt;# enable privilege &lt;1-15&gt; secret &lt;string&gt; (This password will <b>BE</b> encrypted.)</li><li>● &lt;config&gt;# enable privilege &lt;1-15&gt; secret encrypted &lt;string&gt; (This password is copied from another configuration file. So, enter an <b>existed</b> and <b>encrypted</b> password.)</li></ul> |
| <i>enable secret</i>    | <PASSWORD> - Enter a new string as the encrypted password.<br><b>Related Syntax:</b> <ul style="list-style-type: none"><li>● &lt;config&gt;# enable secret PASSWORD</li><li>● &lt;config&gt;# enable secret encrypted PASSWORD</li></ul>   |

## Example

```
G2500# configure
G2500(config)# enable secret encrypted testtest
G2500(config)# exit
G2500# show running-config
G2500# ...
enable privilege 2 secret "OTE5ZTY4MmNhYzgyNWQ0MzBhNTgwZTg0MmZmMGJiYzQ="
enable secret "testtest"
vlan 2
  name "test0002"
vlan 3
  name "test0003"
vlan 5
  name "test_carrie"
voice-vlan oui-table 00:E0:BB "3COM"
voice-vlan oui-table 00:03:6B "Cisco"
voice-vlan oui-table 00:E0:75 "Veritel"
.....
```

## Telnet Command: end

Use this command to end current mode.

### Syntax Items

end

## Example

```
G2500# configure
G2500(config)#end
G2500#
```

## Telnet Command: errdisable

Use this command to enable the auto recovery timer for port error.

### Syntax Items

errdisable recovery cause  
errdisable recovery interval

### Description

| Syntax Items                        | Description   |
|-------------------------------------|---|
| <i>errdisable recovery cause</i>    | Enable the auto recovery timer for port error disabled from ACL, all, ARP rate limit, STP BPDU guard, broadcast flooding, DHCP rate limit, port security, STP self-loop, unicast flooding, or unknown multicast flooding causes.<br><b>Related Syntax:</b> <ul style="list-style-type: none"><li>● &lt;config&gt;# errdisable recovery cause &lt; acl /all /arp-inspection /bpduguard /broadcast-flood /dhcp-rate-limit /psecure-violation /selfloop /unicast-flood /unknown-multicast-flood &gt;</li></ul> |
| <i>errdisable recovery interval</i> | Set the recovery time of the error disabled port.<br><30-86400> - The default value is 300 seconds.<br><b>Related Syntax:</b>   |

- <config># errdisable recovery interval <30-86400>

## Example

```
G2500# configure
G2500(config)#
G2500(config)# errdisable recovery interval 600
G2500(config)#
```

## Telnet Command: exit

Use this command to exit current mode and return to previous mode/phase.

## Syntax Items

exit

## Example

```
G2500# configure
G2500(config)#
G2500(config)# exit
G2500#
```

## Telnet Command: gvrp

Use this command to enable the GVRP configuration. In default, the GVRP is disabled.

## Syntax Items

gvrp

## Example

```
G2500# configure
G2500(config)# gvrp
G2500(config)#
G2500(config)# exit
G2500# show gvrp
          GVRP      Status
-----
GVRP                : Enabled
Join time            : 200 ms
Leave time            : 600 ms
LeaveAll time         : 10000 ms
G2500#
```

## Telnet Command: hostname

Use this command to modify the network name of VigorSwitch.

## Syntax Items

hostname

## Description

| Syntax Items    | Description   |
|-----------------|---|
| <i>hostname</i> | <word> - Enter a string as the network name for VigorSwitch.<br>Related Syntax: |

- <config># hostname <word>

## Example

```
G2500# configure
G2500(config)# hostname Switch_3F
Switch_3F(config)#
```

## Telnet Command: interface

Use this command to configure interface settings.

Before configuring, you have to access into next phase. See the following example:

```
G2500# configure
G2500(config)#
G2500(config)# interface GigabitEthernet 3
G2500(config-if)#
```

Or

```
G2500# configure
G2500(config)#
G2500(config)# interface range LAG 3
P2500(config-if-range)#
```

## Syntax Items

interface GigabitEthernet  
interface LAG  
interface range

## Description

| Syntax Items                     | Description   |
|----------------------------------|---|
| <i>interface GigabitEthernet</i> | <1-50> - Specify the number of Ethernet LAN port.<br><b>Related Syntax:</b><br>● <config># interface GigabitEthernet <1-50>   |
| <i>interface LAG</i>             | <1-8> - Specify the number of LAG interface.<br><b>Related Syntax:</b><br>● <config># interface LAG <1-8>   |
| <i>Interface range</i>           | Specify an interface ranges for configuring detailed settings.<br><b>Related Syntax:</b><br>● <config># interface range GigabitEthernet <1-50><br>● <config># interface range LAG <1-8> |

## Example

```
G2500# configure
G2500(config)# interface LAG 1
P2280x(config-if)#
```

Under (config-if)#, available sub-commands for LAN or LAG will be different. Below shows the items under Ethernet LAN:

<config-if># authentication

```

<config-if># back-pressure
<config-if># custom
<config-if># description
<config-if># device-check
<config-if># dos
<config-if># dot1x
<config-if># do
<config-if># dray_surveillance
<config-if># duplex
<config-if># eee
<config-if># end
<config-if># exit
<config-if># flowcontrol
<config-if># gvrp
<config-if># ip
<config-if># ipv6
<config-if># lacp
<config-if># lag
<config-if># lldp
<config-if># mac
<config-if># mvr
<config-if># no
<config-if># poe
<config-if># port-security
<config-if># power
<config-if># protected
<config-if># qos
<config-if># rate-limit
<config-if># shutdown
<config-if># spanning-tree
<config-if># speed
<config-if># storm-control
<config-if># surveillance-vlan
<config-if># switchport
<config-if># udd
<config-if># vlan
<config-if># voice-vlan

```

## Description

| Syntax Items          | Description   |
|-----------------------|---|
| <i>authentication</i> | <p>Apply Auth Manager Port Configuration Commands to the specified interface (Ethernet port/LAG port).</p> <p>dot1x - Execute the 802.1x authentication.</p> <p>guest-vlan - Authenticate the guest VLAN configuration.</p> <p>host-mode &lt;multi-auth / multi-host / single-host&gt; - Set the host mode for authentication on this port.</p> <p>max-hosts &lt;1-256&gt; - Set the maximum number of authenticated hoss allowed on this port.</p> <p>method &lt;local/radius&gt; - Set authentication method by using local or RADIUS server.</p> <p>order &lt;dot1x / mac /web&gt; - Add an authentication type to the order list.</p> <p>port-control &lt;auto / force-auth / force-unauth&gt; - Set the port state of this port as AUTO, Authorized or Unauthorized.</p> <p>radius-attributes vlan reject - If the Radius server authorizes the supplicant, but does not provide a supplicant VLAN, the supplicant will be rejected. If the parameter is omitted, the option is applied by default.</p> <p>radius-attributes vlan static - If the Radius server authorizes the</p> |

|                      |   |
|----------------------|---|
|                      | <p>supplicant but does not provide a supplicant VLAN, the supplicant will be accepted.</p> <p>reauth - Enable/Disable Reauthentication for this port</p> <p>timer &lt;inactive&gt; &lt;60-65535&gt; - Set the time value for authentication. After the time interval, if there is no activity from the client, it will be unauthorized.</p> <p>timer quiet &lt;0-65535&gt; - Set the time value to wait failed authentication exchange.</p> <p>timer reauth &lt;300-4294967294&gt; - Set the time value. After the time interval, an automatic re-authentication should be initiated.</p> <p>web - Execute the web-based authentication.</p> <p>web max-login-attempts &lt;3-10&gt; - Set a maximum number of login attempts on the port.</p> <p>web max-login-attempts infinite - No limit for login attempts.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config-if&gt;# authentication dot1x</li> <li>● &lt;config-if&gt;# authentication guest-vlan</li> <li>● &lt;config-if&gt;# authentication host-mode &lt;multi-auth / multi-host / single-host&gt;</li> <li>● &lt;config-if&gt;# authentication mac</li> <li>● &lt;config-if&gt;# authentication max-hosts &lt;1-256&gt;</li> <li>● &lt;config-if&gt;# authentication method &lt;local/radius&gt;</li> <li>● &lt;config-if&gt;# authentication order &lt;dot1x / mac / web&gt;</li> <li>● &lt;config-if&gt;# authentication port-control &lt;auto / force-auth / force-unauth&gt;</li> <li>● &lt;config-if&gt;# authentication radius-attributes vlan reject</li> <li>● &lt;config-if&gt;# authentication radius-attributes vlan static</li> <li>● &lt;config-if&gt;# authentication reauth</li> <li>● &lt;config-if&gt;# authentication timer inactive &lt;60-65535&gt;</li> <li>● &lt;config-if&gt;# authentication timer quiet &lt;0-65535&gt;</li> <li>● &lt;config-if&gt;# authentication timer reauth &lt;300-4294967294&gt;</li> <li>● &lt;config-if&gt;# authentication web</li> <li>● &lt;config-if&gt;# authentication web max-login-attempts &lt;3-10&gt;</li> <li>● &lt;config-if&gt;# authentication web max-login-attempts infinite</li> </ul> |
| <i>back-pressure</i> | <p>Enable back-pressure for the specified interface (Ethernet port/LAG port).</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config-if&gt;# back-pressure</li> </ul>  |
| <i>custom</i>        | <p>&lt;enable&gt; - Enable the custom module configuration for the specified interface (Ethernet port/LAG port).</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config-if&gt;# custom enable</li> </ul>   |
| <i>description</i>   | <p>Write a description for the specified interface (Ethernet port/LAG port).</p> <p>&lt;WORD&gt; - Enter a description (up to 32 characters).</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config-if&gt;# descripton &lt;WORD&gt;</li> </ul>  |
| <i>device-check</i>  | <p>Perform a device check the specified interface (Ethernet port/LAG port).</p> <p>ip-address&lt;A.B.C.D&gt; - Enter the IP address of the device.</p> <p>interval &lt;120/15/30/60&gt;- Check the device interval by entering the time value. Unit is second.</p> <p>retry &lt;1/3/5&gt; - Enter the retry time during a checking period.</p> <p>Failure-action &lt;nothing/powercycle/poweroff&gt; - Set the power</p>  |

|                          |  |
|--------------------------|--|
|                          | <p>cycle.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config-if&gt;# device-check ip-address &lt;A.D.C.D&gt; interval &lt;120/15/30/60&gt; retry &lt;1/3/5&gt; failure-action &lt;nothing/powercycle/poweroff&gt;</li> </ul>  |
| <i>dos</i>               | Apply DoS to the specified interface (Ethernet port/LAG port).   |
| <i>dot1x</i>             | <p>It is available for GigabitEthernet port only.</p> <p>guest-vlan - Set guest VLAN configuration.</p> <p>max-req &lt;1-10&gt;- Set the maximum request retries. Default is 2.</p> <p>Port-control &lt;auto/force-auth/force-unauth&gt;- Set the port control value (auto, authorized or unauthorized)</p> <p>reauth - Enable/disable the reauthentication for this port.</p> <p>timeout &lt;quiet-period / reauth-period / server-timeout /supp-timeout /tx-period&gt;- Set timeout value for this port.</p> <p>&lt;0-65535&gt; - Set a value as quiet period (default is 60-second).</p> <p>&lt;300-4294967294&gt; - Set a value as re-authentication period. (default is 3600-second).</p> <p>&lt;1-65535&gt; - Set a value to wait for a packet retransmission to the authentication server.</p> <p>supp-timeout &lt;1-65535&gt; - Set a vale as supplicant timeout period.</p> <p>tx-period &lt;1-65535&gt; - Set a value to wait for a response to an EAP-request / identity before resending the request.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config-if&gt;# dot1x guest-vlan</li> <li>● &lt;config-if&gt;# dot1x max-req &lt;1-10&gt;</li> <li>● &lt;config-if&gt;# dot1x port-control &lt;auto /force-auth /force-unauth &gt;</li> <li>● &lt;config-if&gt;# dot1x reauth</li> <li>● &lt;config-if&gt;# dot1x timeout quiet-period &lt;0-65535&gt;</li> <li>● &lt;config-if&gt;# dot1x timeout reauth-period &lt;300-4294967294&gt;</li> <li>● &lt;config-if&gt;# dot1x timeout server-timeout &lt;1-65535&gt;</li> <li>● &lt;config-if&gt;# dot1x timeout supp-timeout &lt;1-65535&gt;</li> <li>● &lt;config-if&gt;# dot1x timeout tx-period &lt;1-65535&gt;</li> </ul> |
| <i>do</i>                | Run execution commands in current mode.  |
| <i>dray_surveillance</i> | <p>Use this command to set the ONVIF throughput alert threshold.</p> <p>&lt;16-1000000&gt; - Specify a number as the alert threshold for egress /ingress throughput.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config-if&gt;#dray_surveillance set threshold alert egress &lt;16-1000000&gt;</li> <li>● &lt;config-if&gt;#dray_surveillance set threshold alert ingress &lt;16-1000000&gt;</li> </ul>   |
| <i>duplex</i>            | <p>Apply the duplex configuration to the specified interface (Ethernet port/LAG port).</p> <p>&lt;Auto&gt; - Auto duplex configuration.</p> <p>&lt;Full&gt;- Force full duplex operation.</p> <p>&lt;Half&gt; - Force half-duplex operation.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config-if&gt;# duplex &lt;auto/full/half&gt;</li> </ul>  |
| <i>eee</i>               | Apply the EEE configuration to the specified interface (Ethernet port).  |
| <i>end</i>               | End current mode, change to enable mode and return to previous phase.  |

|                    |   |
|--------------------|---|
| <i>exit</i>        | Exit from current mode.   |
| <i>flowcontrol</i> | <p>Configure flow-control mode to the specified interface (Ethernet port/LAG port).</p> <p>&lt;Auto&gt; - Enable AUTO flow-control configuration.</p> <p>&lt;Off&gt; - Disable the force flow-control.</p> <p>&lt;On&gt; - Enable the force flow-control.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config-if&gt;# flowcontrol &lt;auto/off/on&gt;</li> </ul>  |
| <i>gvrp</i>        | <p>Apply the GVRP configuration to the specified interface (Ethernet port/LAG port).</p> <p>registration-mode &lt;fixed / forbidden / normal&gt;- Set registration mode for GVRP. When registration-mode is fixed or forbidden, it will remove the dynamic port from VLAN.</p> <p>vlan-creation-forbid - Do not remove dynamic port from VLAN.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config-if&gt;# gvrp registration-mode &lt;fixed / forbidden / normal&gt;</li> <li>● &lt;config-if&gt;# gvrp vlan-creation-forbid</li> </ul>   |
| <i>ip</i>          | <p>Apply IP configuration to the specified interface (Ethernet port/LAG port).</p> <p>acl &lt;NAME&gt; - Specify an ACL for packets. Enter the name of the ACL.</p> <p>arp inspection rate-limit &lt;1-50&gt; - ARP inspection is to enable Dynamic ARP Inspection function. Set the rate limitation (1 - 50) on the interface. VigorSwitch will drop ARP packets after receives more than configured rate of packets per second.</p> <p>arp inspection trust - Use it to set trusted interface.</p> <p>arp inspection validate dst-mac - It means the switch will drop ARP reply packets if arp-target-mac and ethernet-dst-mac are not matched.</p> <p>arp inspection validate ip allow-zeros - The "allow-zeros" means the switch will not drop all zero IP address.</p> <p>arp inspection validate src-mac - It means the switch will drop ARP requests and reply packets if arp-sender-mac and ethernet-source-mac are not matched.</p> <p>conflict prevention bind-ip &lt;A.B.C.D&gt; -</p> <p>conflict prevention port-type DHCP-Client -</p> <p>conflict prevention port-type DHCP-Client has-server -</p> <p>conflict prevention port-type DHCP-Server -</p> <p>conflict prevention port-type DHCP-Server has-server -</p> <p>conflict prevention port-type Multiple-Hosts -</p> <p>conflict prevention port-type Multiple-Hosts has-server -</p> <p>conflict prevention port-type Static-Binding -</p> <p>conflict prevention port-type Static-Binding has-server -</p> <p>dhcp snooping option - Use it to enable the function of inserting option82 content into the packet.</p> <p>dhcp snooping option action &lt;drop / keep / replace&gt; - Use it to set the action (drop, keep or replace) when receiving packets with option82 content.</p> <p>dhcp snooping option circuit-id &lt;STRING&gt; - Use it to set user-defined circuit-id string (1 to 63 characters).</p> <p>dhcp snooping rate-limit &lt;1-300&gt; - Use it to set rate limitation on the interface.</p> <p>dhcp snooping trust - Use it to set trusted interface.</p> <p>dhcp snooping verify mac-address - Use it to verify MAC address function on the interface.</p> <p>dhcp snooping vlan &lt;1-4094&gt; option circuit-id &lt;STRING&gt; - Set</p> |



|                    |   |
|--------------------|---|
|                    | <p>user-defined circuit-id string for specified VLAN ID.</p> <p>igmp filter &lt;1-128&gt; - Use it to bind a profile for a port. Specify a profile ID.</p> <p>igmp max-groups &lt;0-256&gt; - Use it to limit port learning max group number (0-256).</p> <p>igmp max-groups action &lt;deny/replace&gt; - Use it to set the action (deny or replace) when the number of groups reach the limitation.</p> <p>source binding max-entry &lt;1-50&gt; -</p> <p>source binding max-entry no-limit -</p> <p>source verify mac-and-ip - Use it to enable IP source guard function.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config-if&gt;# ip acl &lt;NAME&gt;</li> <li>● &lt;config-if&gt;# ip arp inspection rate-limit &lt;1-50&gt;</li> <li>● &lt;config-if&gt;# ip arp inspection trust</li> <li>● &lt;config-if&gt;# ip arp inspection validate dst-mac</li> <li>● &lt;config-if&gt;# ip arp inspection validate ip allow-zeros</li> <li>● &lt;config-if&gt;# ip arp inspection validate src-mac</li> <li>● &lt;config-if&gt;# ip conflict prevention bind-ip &lt;A.B.C.D&gt;</li> <li>● &lt;config-if&gt;# ip conflict prevention port-type DHCP-Client has-server</li> <li>● &lt;config-if&gt;# ip conflict prevention port-type DHCP-Server has-server</li> <li>● &lt;config-if&gt;# ip conflict prevention port-type DHCP-Server has-server</li> <li>● &lt;config-if&gt;# ip conflict prevention port-type Multiple-Hosts has-server</li> <li>● &lt;config-if&gt;# ip conflict prevention port-type Multiple-Hosts has-server</li> <li>● &lt;config-if&gt;# ip conflict prevention port-type Static-Binding has-server</li> <li>● &lt;config-if&gt;# ip conflict prevention port-type Static-Binding has-server</li> <li>● &lt;config-if&gt;# ip dhcp snooping option</li> <li>● &lt;config-if&gt;# ip dhcp snooping option action &lt;drop / keep / replace&gt;</li> <li>● &lt;config-if&gt;# ip dhcp snooping option circuit-id &lt;STRING&gt;</li> <li>● &lt;config-if&gt;# ip dhcp snooping rate-limit &lt;1-300&gt;</li> <li>● &lt;config-if&gt;# ip dhcp snooping trust</li> <li>● &lt;config-if&gt;# ip dhcp snooping verify mac-address</li> <li>● &lt;config-if&gt;# ip dhcp snooping vlan &lt;1-4094&gt; option circuit-id &lt;STRING&gt;</li> <li>● &lt;config-if&gt;# ip igmp filter &lt;1-128&gt;</li> <li>● &lt;config-if&gt;# ip igmp max-groups &lt;0-256&gt;</li> <li>● &lt;config-if&gt;# ip igmp max-groups action &lt;deny/replace&gt;</li> <li>● &lt;config-if&gt;# ip source binding max-entry &lt;1-50&gt;</li> <li>● &lt;config-if&gt;# ip source binding max-entry no-limit</li> <li>● &lt;config-if&gt;# ip source verify mac-and-ip</li> </ul> |
| <p><i>ipv6</i></p> | <p>Apply IPV6 configuration to the specified interface (Ethernet port/LAG port).</p> <p>acl &lt;NAME&gt; - Specify the ACL name for packets</p> <p>mld &lt;filter&gt; - Set IPv6 filter for MLD configuration.</p> <p>mld max-groups - Specify the number for maximum group.</p> <p>&lt;0-256&gt; - MLD snooping group number.</p> <p>action &lt;deny /replace&gt; - Define the action to be performed when exceeding the maximum group.</p>  |

|             |  |
|-------------|--|
|             | <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config-if&gt;# ipv6 acl &lt;NAME&gt;</li> <li>● &lt;config-if&gt;# ipv6 mld filter</li> <li>● &lt;config-if&gt;# ipv6 mld max-groups &lt;0-256&gt;</li> <li>● &lt;config-if&gt;# ipv6 mld max-groups action &lt;deny / replace&gt;</li> </ul>   |
| <i>lacp</i> | <p>Apply LACP Configuration to the specified interface (Ethernet port/LAG port).</p> <p>&lt;1-65535&gt; - Set a number for IEEE 802.3 link aggregation port priority.</p> <p>&lt;long/short&gt; - Set long or short timeout value.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config-if&gt;# lacp port-priority &lt;1-65535&gt;</li> <li>● &lt;config-if&gt;# lacp timeout &lt;long/short&gt;</li> </ul>   |
| <i>lag</i>  | <p>Apply Link Aggregation Group Configuration the specified interface (Ethernet port/LAG port).</p> <p>&lt;1-8&gt; - Specify LAG number.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config-if&gt;# lag &lt;1-8&gt;</li> </ul>  |
| <i>lldp</i> | <p>med location - Configure the LLDP MED location data. The "coordinate", "civic-address", "ecs-elin" locations are independent, so at most three location TLVs could be sent if their data are not empty.</p> <p>med network-policy add / remove - Configure the LLDP MED network policy table. Add /remove a network policy entry that can be bind to ports.</p> <p>med tlv-select - Configure LLDP MED TLVs selection. Available optional TLVs are network-policy, location, inventory and poe-pse.</p> <p>tlv-select - Select LLDP TLVs to send.</p> <p>&lt;civic-address&gt; - The location is specified as civic address.</p> <p>    &lt;ADDR&gt; - Range from 6 to 160 hexadecimal bytes.</p> <p>&lt;Coordinate&gt; - The location is specified as coordinates.</p> <p>    &lt;ADDR&gt; - 16 hexadecimal bytes exactly.</p> <p>&lt;ecs-elin&gt; - The location is specified as ECS ELIN.</p> <p>    &lt;ADDR&gt; - 10 to 25 hexadecimal bytes.</p> <p>&lt;IDX_LIST&gt; - Range from 1 to 32.</p> <p>&lt;TLV&gt; - LLDP optional TLV, pick from: port-desc, sys-name, sys-desc, sys-cap, mac-phy, lag, max-frame-size, management-addr.</p> <p>pvid &lt;disable/enable&gt; - Enable or disable the TX optional-TLV 802.1 PVID.</p> <p>vlan-name &lt;add/remove&gt; &lt;2-4094&gt; - Add/remove a selected VLAN. Enter the VLAN ID number.</p> <p>&lt;rx&gt; - Enable LLDP reception on interface.</p> <p>&lt;tx&gt; - Enable LLDP transmission on interface.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config-if&gt;# lldp med location &lt;civic-address/coordinate/ecs-elin&gt; &lt;ADDR&gt;</li> <li>● &lt;config-if&gt;# lldp med network-policy add &lt;IDX_LIST&gt;</li> <li>● &lt;config-if&gt;# lldp med network-policy remove &lt;IDX_LIST&gt;</li> <li>● &lt;config-if&gt;# lldp med tlv-select &lt;network-policy/location/inventory/poe-pse&gt; &lt;network-policy/location/inventory/poe-pse&gt; &lt;network-policy/location/inventory/poe-pse&gt;</li> <li>● &lt;config-if&gt;# lldp tlv-select &lt;TLV/pvid/vlan-name&gt;</li> <li>● &lt;config-if&gt;# lldp tlv-select pvid &lt;disable/enable&gt;</li> </ul> |

|                      |  |
|----------------------|--|
|                      | <ul style="list-style-type: none"> <li>● &lt;config-if&gt;# lldp tlv-select vlan-name &lt;add/remove&gt; &lt;2-4094&gt;</li> <li>● &lt;config-if&gt;# lldp &lt;rx/tx&gt;</li> </ul>  |
| <i>mac</i>           | <p>Specify an access control list for packets.<br/>Before configuring, you have to create an ACL based on MAC address.<br/>For example,</p> <pre>&lt;config&gt;# mac acl CA_ACL &lt;config-mac-acl&gt;# &lt;NAME&gt; - Enter a name for ACL.</pre> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config-if&gt;# mac acl &lt;NAME&gt;</li> </ul>   |
| <i>mvr</i>           | <p>Make MVR configuration.<br/>immediate - Enable MVR function.<br/>type &lt;receiver/source&gt; - Specify MVR port type as receiver or source.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config-if&gt;# mvr immediate</li> <li>● &lt;config-if&gt;# mvr type &lt;receiver/source&gt;</li> </ul>  |
| <i>no</i>            | <p>Negate command. Such command can disable current setting of command executed and return to the factory setting of that command.<br/>Example:</p> <pre>&lt;config-if&gt; # no mvr The operation will make mvr setting is default. Continue? [yes/no]:yes &lt;config-if&gt; #</pre> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config-if&gt;# no &lt;command&gt;</li> </ul>   |
| <i>poe</i>           | <p>Enable or disable the PoE port.</p>   |
| <i>port-security</i> | <p>port-security - Enable the port security functionality. Default is disabled.<br/>address-limit &lt;1-256&gt;- Enter the number as limitation for MAC address.<br/>action &lt;discard / forward / shutdown&gt; - Speicfy an action to be performed.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config-if&gt;# port-security</li> <li>● &lt;config-if&gt;# port-security addresss-limit &lt;1-256&gt; action &lt;discard / forward / shutdown&gt;</li> </ul>  |
| <i>power</i>         | <p>Configure the inline power for the PoE device.<br/>inline auto - Turn on the PoE device discovery protocol and apply the power to the devcie.<br/>inline never - Turn off the PoE device power.<br/>power-limit &lt;15.4w/30w/MW&gt; - Set the power limit for the PoE device.<br/>priority &lt;1-3/critical/high/low&gt; - Set the priority of power application for the PoE device.<br/>schedule-index - Specify the index number of the schedule profile.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config-if&gt;# power inline auto</li> <li>● &lt;config-if&gt;# power inline never</li> <li>● &lt;config-if&gt;# power power-limit &lt;15.4w/30w/MW&gt;</li> <li>● &lt;config-if&gt;# power priority &lt;1-3/critical/high/low&gt;</li> <li>● &lt;config-if&gt;# power schedule-index</li> </ul> |

|                      |   |
|----------------------|---|
| <i>protected</i>     | <p>Configure an interface to be a protected port.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config-if&gt;#protected</li> </ul>   |
| <i>qos</i>           | <p>cos - Configure the default CoS value for an Ethernet port.</p> <p>&lt;0-7&gt; - Specify a CoS value for the selected interface. Default value is 0.</p> <p>remark - Configure remarking state of each port.</p> <p>trust - Configure each port to trust state while the system is in "basic" mode. There are four trust types for a device to judge the appropriate queue of the packets.</p> <p>&lt;cos&gt; - Enable cos remarking.</p> <p>&lt;dscp&gt; - Enable DSCP remarking.</p> <p>&lt;cos-dscp&gt; - Enable cos and DSCP remarking.</p> <p>&lt;precedence&gt; - Enable IP precedence remarking.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config-if&gt;#qos cos &lt;0-7&gt;</li> <li>● &lt;config-if&gt;#qos remark &lt;cos/dscp/precedence&gt;</li> <li>● &lt;config-if&gt;#qos trust &lt;cos/cos-dscp/ dscp/precedence&gt;</li> </ul> |
| <i>rate-limit</i>    | <p>It is effective for Ethernet port only.</p> <p>egress - Configure the egress port shaper.</p> <p>ingress - Configure the ingress port shaper.</p> <p>egress queue - Configure queue for egress port shaper.</p> <p>&lt;0-1000000&gt; - Enter a number as the average traffic rate in Kbps. It must be a multiple of 16.</p> <p>&lt;16-1000000&gt; - Enter a number as the average traffic rate in Kbps. It must be a multiple of 16.</p> <p>&lt;1-8&gt; - Specify a nubmer as queue ID.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config-if&gt;# rate-limit egress &lt;0-1000000&gt;</li> <li>● &lt;config-if&gt;# rate-limit egress queue &lt;1-8&gt; &lt;16-1000000&gt;</li> <li>● &lt;config-if&gt;# rate-limit ingress &lt;16-1000000&gt;</li> </ul>  |
| <i>shutdown</i>      | <p>Disable the selected interface.</p> <p>Example:</p> <pre>(config)# interface gigabitethernet 3 (config-if)# shutdown (config-if)# exit (config)# exit # show interface Gigabitethernet 3 GigabitEthernet3 is down</pre> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config-if&gt;# shutdown</li> </ul>  |
| <i>spanning-tree</i> | <p>Configure spanning-tree settings.</p> <p>bpdu-filter - Set the BPDU-Filter for specified port.</p> <p>bpdu-guard - Set the BPDU-Guard for specified port.</p> <p>edge - Set the edge-port for specified port.</p> <p>cost - Change an interface's spanning tree path cost.</p> <p>link-type - Specify a link type for spanning tree protocol use.</p> <p>mcheck - Set the mcheck for specified port to migrate.</p> <p>mst - Set spanning-tree parameters of instance.</p> <p>port-priority- Set the priority for specified instance.</p> <p>&lt;0-200000000&gt; - Specify a value of internal path cost (0 means Auto).</p> <p>&lt;point-to-point&gt; - The selected port will be treated as</p>  |

|                          |  |
|--------------------------|--|
|                          | <p>point-to-point.</p> <p>&lt;shared&gt; - The selected port will be treated as shared.</p> <p>&lt;0-15&gt; - Specify an instance ID.</p> <p>&lt;0-240&gt; - Specify a priority number for the selected port.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config-if&gt;# spanning-tree &lt;bpdu-filter /bpdu-guard/ edge&gt;</li> <li>● &lt;config-if&gt;# spanning-tree cost &lt;0-200000000&gt;</li> <li>● &lt;config-if&gt;# spanning-tree link-type &lt;point-to-point/shared&gt;</li> <li>● &lt;config-if&gt;#spanning-tree mcheck</li> <li>● &lt;config-if&gt;#spanning-tree mst &lt;0-15&gt; cost &lt;0-200000000&gt;</li> <li>● &lt;config-if&gt;# spanning-tree port-priority &lt;0-240&gt;</li> </ul>   |
| <i>speed</i>             | <p>Configure speed operation.</p> <p>&lt;10/100/1000&gt; - Force 10/100/1000 Mbps operation.</p> <p>&lt;auto&gt; - Enable Auto speed configuration.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config-if&gt;# speed&lt;10/100/1000&gt;</li> <li>● &lt;config-if&gt;# speed auto</li> </ul>   |
| <i>storm-control</i>     | <p>action - Select an action for storm control after exceeding the threshold.</p> <p>broadcast level - Enable the storm control type of broadcast for the selected port.</p> <p>unknown-multicast level - Enable the storm control type of unknown-multicast for the selected port.</p> <p>unknown-unicast level- Enable the storm control type of unknown-unicast for the selected port.</p> <p>&lt;drop&gt; - Drop packets after exceeding storm control threshold.</p> <p>&lt;shutdown&gt; - Disable the port after exceeding storm control threshold.</p> <p>&lt;1-1000000&gt; - Specify the rate value.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config-if&gt;# storm-control action &lt;drop/shutdown&gt;</li> <li>● &lt;config-if&gt;# storm-control broadcast level &lt;1-1000000&gt;</li> <li>● &lt;config-if&gt;# storm-control unknown-multicast level &lt;1-1000000&gt;</li> <li>● &lt;config-if&gt;# storm-control unknown-unicast level &lt;1-1000000&gt;</li> </ul> |
| <i>surveillance-vlan</i> | <p>cos - Set surveillance VLAN configuration.</p> <p>mode - Set surveillance member port join mode.</p> <p>&lt;all&gt; - QoS attributes are applied to all packets that are classified to the Surveillance VLAN.</p> <p>&lt;src&gt; - QoS attributes are applied only on packets from IP phones.</p> <p>&lt;auto&gt; - Make surveillance member port join voice VLAN automatically.</p> <p>&lt;manual&gt; - The administrator manually makes surveillance member port join voice VLAN.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config-if&gt;# surveillance-vlan cos &lt;all/src&gt;</li> <li>● &lt;config-if&gt;# surveillance-vlan mode &lt;auto/manual&gt;</li> </ul>   |
| <i>switchport</i>        | <p>Set switching mode characteristics.</p> <p>access vlan -Use it to set a native VLAN on the interface.</p> <p>default-vlan tagged - Use it to make the selected port interface to become the default VLAN tagged member.</p> <p>forbidden default-vlan - Use it to forbid the default-vlan on the interface.</p>   |

|             |  |
|-------------|--|
|             | <p>forbidden vlan - Use it to forbid a vlan on the interface.</p> <p>hybrid acceptable-frame-type - Use it to choose which type of frame will be accepted.</p> <p>hybrid allowed - Use it to allow a VLAN set on the interface.</p> <p>hybrid ingress-filtering - Use it to enable VLAN ingress filter.</p> <p>hybrid pvid - Use it to set PVID of the interface.</p> <p>mode access - Use it to configure the selected port as the role of access. Only untagged frames will be accepted.</p> <p>mode hybrid - Use it to configure the selected port as the role of hybrid. Support all functions defined in IEEE 802.1Q specification.</p> <p>mode trunk uplink - Use it to configure the selected port as the role of trunk. It can recognize double tagging on the interface.</p> <p>trunk allowed - Use it to allow a VLAN on the interface.</p> <p>trunk native - Use it to set a native VLAN on the interface.</p> <p>tunnel vlan - Use it to set a Dot1q tunnel VLAN on the interface.</p> <p>vlan tpid - Use it to set TPID on the interface.</p> <p>&lt;1-4094&gt; - Specify a VLAN ID.</p> <p>&lt;add/remove&gt; - Add or remove the allowed VLAN list.</p> <p>&lt;all/tagged-only/untagged-only&gt; - Specify an option for accepting all frames, only tagged frames or only untagged frames.</p> <p>&lt;1-4094/all&gt; - Specify a VLAN ID or all VLAN IDs.</p> <p>&lt; 0x8100 / 0x88A8 / 0x9100 / 0x9200&gt; - Specify one tag-protocol-id.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config-if&gt;# switchport access vlan &lt;1-4094&gt;</li> <li>● &lt;config-if&gt;# switchport default-vlan tagged</li> <li>● &lt;config-if&gt;# switchport forbidden default-vlan</li> <li>● &lt;config-if&gt;# switchport forbidden vlan &lt;add/remove&gt; &lt;1-4094&gt;</li> <li>● &lt;config-if&gt;# switchport hybrid acceptable-frame-type &lt;all/tagged-only/untagged-only&gt;</li> <li>● &lt;config-if&gt;# switchport hybrid allowed vlan add &lt;1-4094&gt;</li> <li>● &lt;config-if&gt;# switchport hybrid allowed vlan add &lt;1-4094&gt; &lt;tagged/ untagged&gt;</li> <li>● &lt;config-if&gt;# switchport hybrid allowed vlan remove &lt;1-4094&gt;</li> <li>● &lt;config-if&gt;# switchport hybrid ingress-filtering</li> <li>● &lt;config-if&gt;# switchport hybrid pvid &lt;1-4094&gt;</li> <li>● &lt;config-if&gt;# switchport mode &lt;access/hybrid&gt;</li> <li>● &lt;config-if&gt;# switchport mode trunk uplink</li> <li>● &lt;config-if&gt;# switchport trunk allowed vlan &lt;add /remove&gt; &lt;1-4094/all&gt;</li> <li>● &lt;config-if&gt;# switchport trunk native &lt;1-4094&gt;</li> <li>● &lt;config-if&gt;# switchport tunnel vlan &lt;1-4094&gt;</li> <li>● &lt;config-if&gt;# switchport vlan tpid &lt; 0x8100/0x88A8 / 0x9100 / 0x9200&gt;</li> </ul> |
| <i>udld</i> | <p>Configure UDLD enabled or disabled and ignore global UDLD setting.</p> <p>aggressive - Enable UDLD protocol on such interface.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config-if&gt;# udld</li> <li>● &lt;config-if&gt;# udld aggressive</li> </ul>  |
| <i>vlan</i> | <p>mac-vlan group - Set a MAC-based VLAN configuration.</p> <p>protocol-vlan group - Set a protocol-based VLAN configuration.</p> <p>&lt;1-2147483647&gt; - Specify a group ID to map.</p> <p>&lt;1-4094&gt; - Specify a VLAN ID.</p> <p><b>Related Syntax:</b></p>  |

|                   |   |
|-------------------|---|
|                   | <ul style="list-style-type: none"> <li>● &lt;config-if&gt;# vlan mac-vlan group &lt;1-2147483647&gt; vlan &lt;1-4094&gt;</li> <li>● &lt;config-if&gt;# vlan protocol-vlan group&lt;1-2147483647&gt; vlan &lt;1-4094&gt;</li> </ul>  |
| <i>voice-vlan</i> | <p>cos - Set voice VLAN configuration as COS mode.<br/> mode - Set voice member port join mode.<br/> &lt;all&gt; - QoS attributes are applied on all packets that are classified to the Voice VLAN.<br/> &lt;src&gt; - QoS attributes are applied only on packets from IP phones.<br/> &lt;auto&gt; - Make voice member port join voice VLAN automatically.<br/> &lt;manual&gt; - The administrator manually makes voice member port join voice VLAN.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config-if&gt;# voice-vlan cos &lt;all/src&gt;</li> <li>● &lt;config-if&gt;# voice-vlan mode &lt;auto/manual&gt;</li> </ul> |

## Example

```
G2500# configure
G2500(config)# interface LAG 1
G2500(config-if)# speed 100
G2500(config-if)# backpressure
G2500(config-if)# lldp med location ecs-elin 112233445566778899AA
G2500(config-if)# vlan mac-vlan group 35 vlan 1000
G2500(config-if)#
```

## Telnet Command: ip

Use this command to create an IPv4 access list (ACL) which performs classification on layer 3 fields and enters ip-access configuration mode.

### Syntax Items

```
ip acl
ip arp
ip conflict
ip dhcp
ip igmp
ip source
```

### Description

| Syntax Items  | Description  |
|---------------|--|
| <i>ip acl</i> | <p>acl &lt;NAME&gt; - Set the name of the access list (ACL) based on IPv4.<br/> To configure detailed settings, enter the name of ACL to access into next level.<br/> &lt;config&gt;#ip acl &lt;NAME&gt;<br/> Then, available sub-command includes:<br/> &lt;config-ip-acl&gt;#deny<br/> &lt;config-ip-acl&gt;#do<br/> &lt;config-ip-acl&gt;#end<br/> &lt;config-ip-acl&gt;#exit<br/> &lt;config-ip-acl&gt;#permit<br/> &lt;config-ip-acl&gt;#sequence<br/> &lt;config-ip-acl&gt;#show</p> |

Use the “deny” command to create deny rules for the IPv4 access list.  
 <0-255/egp/hmp/icmp/igp/ipinip/ipv6 /ipv6:frag /ipv6:icmp /ipv6:rout / ip / I2tp /ospf /pim / rdp / rsvp /tcp /udp > - Specify the IP protocol number or enter the name of the protocol.  
 <A.B.C.D>/<A.B.C.D> <A.B.C.D>/<A.B.C.D> - Specify the source and destination IPv4 addresses and subnet masks.  
 dscp <0-63> - Set the DSCP filtering by specifying a value for DSCP.  
 precedence <0-7> - Set the cos value and the cos mask for a packet.  
 shutdown - Disable the Ethernet interface.  
 any - Any IP address (as source or destination).

**Related Syntax:**

- <config-ip-acl >#deny <0-255> <A.B.C.D>/<A.B.C.D> <A.B.C.D>/<A.B.C.D> dscp <0-63>
- <config-ip-acl >#deny <0-255> <A.B.C.D>/<A.B.C.D> <A.B.C.D>/<A.B.C.D> dscp <0-63> shutdown
- <config-ip-acl >#deny <0-255> <A.B.C.D>/<A.B.C.D> <A.B.C.D>/<A.B.C.D> precedence <0-7>
- <config-ip-acl >#deny <0-255> <A.B.C.D>/<A.B.C.D> <A.B.C.D>/<A.B.C.D> precedence <0-7> shutdown
- <config-ip-acl >#deny <0-255> any <A.B.C.D>/<A.B.C.D> dscp <0-63>
- <config-ip-acl >#deny <0-255> any <A.B.C.D>/<A.B.C.D> dscp <0-63> shutdown
- <config-ip-acl >#deny <0-255> any <A.B.C.D>/<A.B.C.D> precedence <0-7>
- <config-ip-acl >#deny <0-255> any <A.B.C.D>/<A.B.C.D> precedence <0-7> shutdown
- <config-ip-acl >#deny <0-255> any any dscp <0-7>
- <config-ip-acl >#deny <0-255> any any dscp <0-7> shutdown
- <config-ip-acl >#deny <0-255> any any precedence <0-7>
- <config-ip-acl >#deny <0-255> any any precedence <0-7> shutdown

Use the “do” command to run execution command in current mode.  
 <SEQUENCE> -

**Related Syntax:**

- <config-ip-acl>#do <SEQUENCE>

Use the “end” command to finish current mode. Any changes in current mode will be saved.

**Related Syntax:**

- <config-ip-acl>#end

Use the “exit” command to close the current CLI session or return to the previous mode without saving the settings.

**Related Syntax:**

- <config-ip-acl>#exit

Use the “no sequence” command to delete any entry in management ACL.

<1-2147483647>- Specify an index number of the ACL.

**Related Syntax:**

- <config-ip-acl>#no sequence <1-2147483647>

Use the “permit” command to create permit rules which bypass the packets meet the rule.

<0-255/egp/hmp/icmp/igp/ipinip/ipv6 /ipv6:frag /ipv6:icmp /ipv6:rout / ip / I2tp /ospf /pim / rdp / rsvp /tcp /udp > - Specify the IP protocol number or enter the name of the protocol.

<A.B.C.D>/<A.B.C.D> <A.B.C.D>/<A.B.C.D> - Specify the source and



|                    |  |
|--------------------|--|
|                    | <p>destination IPv4 addresses and subnet masks.</p> <p>dscp &lt;0-63&gt; - Set the DSCP filtering by specifying a value for DSCP.</p> <p>precedence &lt;0-7&gt; - Set the cos value and the cos mask for a packet.</p> <p>Shutdown - Disable the Ethernet interface.</p> <p>any - Any IP address (as source or destination).</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config-ip-acl &gt;#permit &lt;0-255&gt; &lt;A.B.C.D&gt;/&lt;A.B.C.D&gt; &lt;A.B.C.D&gt;/&lt;A.B.C.D&gt; dscp &lt;0-63&gt;</li> <li>● &lt;config-ip-acl &gt;#permit &lt;0-255&gt; &lt;A.B.C.D&gt;/&lt;A.B.C.D&gt; &lt;A.B.C.D&gt;/&lt;A.B.C.D&gt; dscp &lt;0-63&gt; shutdown</li> <li>● &lt;config-ip-acl &gt;#permit &lt;0-255&gt; &lt;A.B.C.D&gt;/&lt;A.B.C.D&gt; &lt;A.B.C.D&gt;/&lt;A.B.C.D&gt; precedence &lt;0-7&gt;</li> <li>● &lt;config-ip-acl &gt;#permit &lt;0-255&gt; &lt;A.B.C.D&gt;/&lt;A.B.C.D&gt; &lt;A.B.C.D&gt;/&lt;A.B.C.D&gt; precedence &lt;0-7&gt; shutdown</li> <li>● &lt;config-ip-acl &gt;#permit &lt;0-255&gt; any &lt;A.B.C.D&gt;/&lt;A.B.C.D&gt; dscp &lt;0-63&gt;</li> <li>● &lt;config-ip-acl &gt;#permit &lt;0-255&gt; any &lt;A.B.C.D&gt;/&lt;A.B.C.D&gt; dscp &lt;0-63&gt; shutdown</li> <li>● &lt;config-ip-acl &gt;#permit &lt;0-255&gt; any &lt;A.B.C.D&gt;/&lt;A.B.C.D&gt; precedence &lt;0-7&gt;</li> <li>● &lt;config-ip-acl &gt;#permit &lt;0-255&gt; any &lt;A.B.C.D&gt;/&lt;A.B.C.D&gt; precedence &lt;0-7&gt; shutdown</li> <li>● &lt;config-ip-acl &gt;#permit &lt;0-255&gt; any any dscp &lt;0-7&gt;</li> <li>● &lt;config-ip-acl &gt;#permit &lt;0-255&gt; any any dscp &lt;0-7&gt; shutdown</li> <li>● &lt;config-ip-acl &gt;#permit &lt;0-255&gt; any any precedence &lt;0-7&gt;</li> <li>● &lt;config-ip-acl &gt;#permit &lt;0-255&gt; any any precedence &lt;0-7&gt; shutdown</li> </ul> <p>Use the "sequence" command to deny or permit the ACL.</p> <p>&lt;1-2147483647&gt; - Enter the sequence of ACL entry. The sequence represents the priority of the ACE in the ACL.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config-ip-acl &gt;#sequence &lt;1-2147483647&gt; deny</li> <li>● &lt;config-ip-acl &gt;#sequence &lt;1-2147483647&gt; permit</li> </ul> <p>Use the "show acl" command to list current status of the selected ACL.</p> |
| <i>ip arp</i>      | <p>Use this command to enable the function of dynamic ARP inspection.</p> <p>vlan &lt;1-4094&gt; - Specify the VLAN ID number.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;#ip arp inspection</li> <li>● &lt;config&gt;#ip arp inspection vlan &lt;1-4094&gt;</li> </ul>  |
| <i>ip conflict</i> | <p>Use this command to do IP conflict prevention.</p> <p>lag - Enable/disable the function.</p> <p>&lt;A.B.C.D&gt; - Specify the IPv4 addresses.</p> <p>&lt;1-50&gt; - Specify a physical port.</p> <p>&lt;1-8&gt; - Specify a LAG port.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;#ip conflict lag</li> <li>● &lt;config&gt;#ip conflict prevention</li> <li>● &lt;config&gt;#ip conflict prevention clear</li> <li>● &lt;config&gt;#ip conflict prevention server-ip &lt;A.B.C.D&gt; interface GigabitEthernet &lt;1-50&gt;</li> <li>● &lt;config&gt;#ip conflict prevention server-ip &lt;A.B.C.D&gt; interface LAG &lt;1-8&gt;</li> </ul>   |
| <i>ip dhcp</i>     | <p>Use this command to enable DHCP client to get IP address from remote DHCP server.</p>   |

|                  |  |
|------------------|--|
|                  | <p>database &lt;flash/tftp/timeout/write-delay&gt; - Write the database to FLASH or remote TFTP server. Set timeout interval for abortion. Set delay timer for writing to URL.</p> <p>&lt;A.B.C.D&gt; - Specify the IPv4 addresses.</p> <p>&lt;HOSTNAME&gt; - Enter the name of the host.</p> <p>&lt;NAME&gt; - Set a name for the backup file.</p> <p>&lt;0-86400&gt; - Enter a value. Unit is second.</p> <p>&lt;15-86400&gt; - Enter a value. Unit is second.</p> <p>option - Configure DHCP-Option82 settings by specifying remote ID number.</p> <p>&lt;STRING&gt; - Enter a string (from 1 to 63 characters) for the DHCP option.</p> <p>vlan - Configure VLAN settings.</p> <p>&lt;1-4094&gt; - Specify the VLAN ID number.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;#ip dhcp snooping</li> <li>● &lt;config&gt;#ip dhcp snooping database</li> <li>● &lt;config&gt;#ip dhcp snooping database flash</li> <li>● &lt;config&gt;#ip dhcp snooping database tftp &lt;A.B.C.D&gt;</li> <li>● &lt;config&gt;#ip dhcp snooping database tftp &lt;HOSTNAME&gt;&lt;NAME&gt;</li> <li>● &lt;config&gt;#ip dhcp snooping database timeout &lt;0-86400&gt;</li> <li>● &lt;config&gt;#ip dhcp snooping database write-delay &lt;15-86400&gt;</li> <li>● &lt;config&gt;#ip dhcp snooping option remote-id &lt;STRING&gt;</li> <li>● &lt;config&gt;#ip dhcp snooping vlan &lt;1-4094&gt;</li> </ul> |
| <i>ip igmp</i>   | <p>Use this command to set IGMP profile and enable IGMP snooping function.</p> <p>Profile - Set IGMP profile.</p> <p>&lt;1-128&gt; - Enter the index number of IGMP profile to access into next phase for configuring detailed settings.</p> <p>&lt;A.B.C.D&gt;&lt;A.B.C.D&gt; - Specify the source and destination IPv4 addresses</p> <p>action &lt;deny/permit&gt; - Speicfy the rule (deny/permit) for the IGMP profile.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;#ip igmp profile &lt;1-128&gt; <ul style="list-style-type: none"> <li>&lt;config-igmp-profile&gt;# do</li> <li>&lt;config-igmp-profile&gt;# end</li> <li>&lt;config-igmp-profile&gt;# exit</li> <li>&lt;config-igmp-profile&gt;# profile range ip &lt;A.B.C.D&gt;&lt;A.B.C.D&gt;</li> <li>&lt;config-igmp-profile&gt;# profile range ip &lt;A.B.C.D&gt;&lt;A.B.C.D&gt; action &lt;deny/permit&gt;</li> <li>&lt;config-igmp-profile&gt;# profile range ip &lt;A.B.C.D&gt; action &lt;deny/permit&gt;</li> <li>&lt;config-igmp-profile&gt;# show</li> </ul> </li> <li>● &lt;config&gt;#ip igmp snooping</li> </ul>  |
| <i>ip source</i> | <p>Use this command to create a static IP source binding entry.</p> <p>&lt;A:B:C:D:E:F&gt; - Enter the MAC address for the binding entry.</p> <p>vlan &lt;1-4094&gt; - Specify the VLAN ID number.</p> <p>&lt;A.B.C.D&gt;&lt;A.B.C.D&gt; - Specify the source and destination IPv4 addresses.</p> <p>&lt;1-50&gt; - Specify a physical port.</p> <p>&lt;1-8&gt; - Specify a LAG port.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;#ip source binding &lt;A:B:C:D:E:F&gt; vlan &lt;1-4094&gt;</li> </ul>   |

|  |   |
|--|---|
|  | <p>&lt;A.B.C.D&gt; &lt;A.B.C.D&gt; interface GigabitEthernet &lt;1-50&gt;</p> <ul style="list-style-type: none"> <li>● &lt;config&gt;#ip source binding &lt;A:B:C:D:E:F&gt; vlan &lt;1-4094&gt;<br/>&lt;A.B.C.D&gt; &lt;A.B.C.D&gt; interface LAG &lt;1-8&gt;</li> <li>● &lt;config&gt;#ip source binding vlan &lt;1-4094&gt; &lt;A.B.C.D&gt; &lt;A.B.C.D&gt; interface GigabitEthernet &lt;1-50&gt;</li> <li>● &lt;config&gt;#ip source binding vlan &lt;1-4094&gt; &lt;A.B.C.D&gt; &lt;A.B.C.D&gt; interface LAG &lt;1-8&gt;</li> </ul> |
|--|---|

## Example

```
G2500# configure
G2500(config)# ip acl market_1
G2280(config-ip-acl)#
G2280(config-ip-acl)# deny 20 192.168.2.55/255.255.255.0 192.168.2.85/255
G2500(config)# ip dhcp snooping database tftp draytek carrie_backup
```

## Telnet Command: ipv6

Use this command to create an IPv6 access list (ACL).

### Syntax Items

ipv6

ipv6 acl

ipv6 mld

### Description

| Syntax Items    | Description   |
|-----------------|---|
| <i>ipv6 acl</i> | <p>&lt;NAME&gt; - Set the name of the access list (ACL) based on IPv6.<br/>To configure detailed settings, enter the name of ACL to access into next level.<br/>&lt;config&gt;#ipv6 acl &lt;NAME&gt;<br/>Then, available sub-command includes:<br/>&lt;config-ipv6-acl&gt;#deny<br/>&lt;config-ipv6-acl&gt;#do<br/>&lt;config-ipv6-acl&gt;#end<br/>&lt;config-ipv6-acl&gt;#exit<br/>&lt;config-ipv6-acl&gt;#no<br/>&lt;config-ipv6-acl&gt;#permit<br/>&lt;config-ipv6-acl&gt;#sequence<br/>&lt;config-ipv6-acl&gt;#show</p> <hr/> <p>Use the "deny" command to create deny rules for the IPv4 access list.<br/>&lt;0-255/icmp/ipv6/tcp /udp &gt; - Specify the IP protocol number or enter the name of the protocol.<br/>&lt;0-255/any&gt; - Specify ICMPv6 number.<br/>&lt;X:X::X:X&gt;/&lt;0-128&gt; &lt;X:X::X:X&gt;/&lt;0-128&gt; - Specify the source/destination IPv6 addresses and subnet masks.<br/>dscp &lt;0-63&gt; - Set the DSCP filtering by specifying a value for DSCP.<br/>precedence &lt;0-7&gt; - Set the cos value and the cos mask for a packet.<br/>shutdown - Disable the Ethernet interface.<br/>any - Any IP address (as source or destination).<br/>&lt;0-65535 / PORT_RANGE / any / daytime / discard / domain / drip</p> |

/ echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> <X::X:X>/<0-128> <0-65535 / PORT\_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> - Set TCP port.

match-all <TCP\_FLAG> - Set TCP flags. List of TCP flags that should occur. If a flag should be set, it is prefixed by "+". If a flag should be unset, it is prefixed by "-". Available options are +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn and -fin. To define more than 1 flag - enter additional flags one after another without a space (example +syn-ack).

<0-65535/ PORT\_RANGE / any / bootpc / bootps / discard / domain / echo / nameserver / netbios-ns / ntp / rip / snmp / snmptrap / sunrpc / syslog / tacacs-ds / talk / tftp / time / who> <X::X:X>/<0-128> <0-65535/ PORT\_RANGE / any / bootpc / bootps / discard / domain / echo / nameserver / netbios-ns / ntp / rip / snmp / snmptrap / sunrpc / syslog / tacacs-ds / talk / tftp / time / who> - Set UDP port.

#### Related Syntax:

- <config-ipv6-acl >#deny <0-255> <X::X:X>/<0-128> <X::X:X>/<0-128>
- <config-ipv6-acl >#deny <0-255> <X::X:X>/<0-128> <X::X:X>/<0-128> dscp <0-63>
- <config-ipv6-acl >#deny <0-255> <X::X:X>/<0-128> <X::X:X>/<0-128> dscp <0-63> shutdown
- <config-ipv6-acl >#deny <0-255> <X::X:X>/<0-128> <X::X:X>/<0-128> precedence <0-7>
- <config-ipv6-acl >#deny <0-255> <X::X:X>/<0-128> <X::X:X>/<0-128> precedence <0-7> shutdown
- <config-ipv6-acl >#deny <0-255> <X::X:X>/<0-128> <X::X:X>/<0-128> shutdown
- <config-ipv6-acl >#deny <0-255> <X::X:X>/<0-128> any dscp <0-63>
- <config-ipv6-acl >#deny <0-255> <X::X:X>/<0-128> any dscp <0-63> shutdown
- <config-ipv6-acl >#deny <0-255> <X::X:X>/<0-128> any precedence <0-7>
- <config-ipv6-acl >#deny <0-255> <X::X:X>/<0-128> any precedence <0-7> shutdown
- <config-ipv6-acl >#deny <0-255> <X::X:X>/<0-128> any shutdown
- <config-ipv6-acl >deny icmp <X::X:X>/<0-128> <X::X:X>/<0-128> <0-255 / any / destination-unreachable / echo-reply / echo-request / nd-na / nd-ns / packet-too-big/ parameter-problem/ router-advertisement / router-solicitation / time-exceeded> <0-255/any> dscp <0-63>
- <config-ipv6-acl >#deny icmp <X::X:X>/<0-128> <X::X:X>/<0-128><0-255 / any / destination-unreachable / echo-reply / echo-request / nd-na / nd-ns / packet-too-big/ parameter-problem/ router-advertisement / router-solicitation / time-exceeded> <0-255/any> dscp <0-63> shutdown
- <config-ipv6-acl >#deny icmp <X::X:X>/<0-128> <X::X:X>/<0-128><0-255 / any / destination-unreachable / echo-reply / echo-request / nd-na / nd-ns / packet-too-big/ parameter-problem/ router-advertisement / router-solicitation / time-exceeded> <0-255/any> precedence <0-7>
- <config-ipv6-acl >#deny icmp <X::X:X>/<0-128> <X::X:X>/<0-128><0-255 / any / destination-unreachable / echo-reply / echo-request / nd-na / nd-ns / packet-too-big/ parameter-problem/ router-advertisement / router-solicitation / time-exceeded> <0-255/any> precedence

---

<0-7> shutdown

- <config-ipv6-acl >#deny icmp <X::X:X>/<0-128>  
<X::X:X>/<0-128><0-255 / any / destination-unreachable /  
echo-reply / echo-request / nd-na / nd-ns / packet-too-big/  
parameter-problem/ router-advertisement /  
router-solicitation / time-exceeded> <0-255/any> shutdown
  - <config-ipv6-acl >#deny icmp <X::X:X>/<0-128> any <0-255  
/ any / destination-unreachable / echo-reply / echo-request /  
nd-na / nd-ns / packet-too-big/ parameter-problem/  
router-advertisement / router-solicitation / time-exceeded>  
<0-255 /any> dscp <0-63>
  - <config-ipv6-acl >#deny icmp <X::X:X>/<0-128> any <0-255  
/ any / destination-unreachable / echo-reply / echo-request /  
nd-na / nd-ns / packet-too-big/ parameter-problem/  
router-advertisement / router-solicitation / time-exceeded>  
<0-255 /any> dscp <0-63> shutdown
  - <config-ipv6-acl >#deny icmp <X::X:X>/<0-128> any <0-255  
/ any / destination-unreachable / echo-reply / echo-request /  
nd-na / nd-ns / packet-too-big/ parameter-problem/  
router-advertisement / router-solicitation / time-exceeded>  
<0-255 /any> precedence <0-7>
  - <config-ipv6-acl >#deny icmp <X::X:X>/<0-128> any <0-255  
/ any / destination-unreachable / echo-reply / echo-request /  
nd-na / nd-ns / packet-too-big/ parameter-problem/  
router-advertisement / router-solicitation / time-exceeded>  
<0-255 /any> precedence <0-7> shutdown
  - <config-ipv6-acl >#deny icmp <X::X:X>/<0-128> any <0-255  
/ any / destination-unreachable / echo-reply / echo-request /  
nd-na / nd-ns / packet-too-big/ parameter-problem/  
router-advertisement / router-solicitation / time-exceeded>  
<0-255 /any> shutdown
  - <config-ipv6-acl >#deny ipv6 <X::X:X>/<0-128>  
<X::X:X>/<0-128>
  - <config-ipv6-acl >#deny ipv6 <X::X:X>/<0-128>  
<X::X:X>/<0-128> dscp <0-63>
  - <config-ipv6-acl >#deny ipv6 <X::X:X>/<0-128>  
<X::X:X>/<0-128> dscp <0-63> shutdown
  - <config-ipv6-acl >#deny ipv6 <X::X:X>/<0-128>  
<X::X:X>/<0-128> precedence <0-7>
  - <config-ipv6-acl >#deny ipv6 <X::X:X>/<0-128>  
<X::X:X>/<0-128> precedence <0-7> shutdown
  - <config-ipv6-acl >#deny ipv6 <X::X:X>/<0-128>  
<X::X:X>/<0-128> shutdown
  - <config-ipv6-acl >#deny ipv6 <X::X:X>/<0-128> any dscp  
<0-63>
  - <config-ipv6-acl >#deny ipv6 <X::X:X>/<0-128> any dscp  
<0-63> shutdown
  - <config-ipv6-acl >#deny ipv6 <X::X:X>/<0-128> any  
precedence <0-7>
  - <config-ipv6-acl >#deny ipv6 <X::X:X>/<0-128> any  
precedence <0-7>shutdown
  - <config-ipv6-acl >#deny ipv6 <X::X:X>/<0-128> any shutdown
  - <config-ipv6-acl >#deny ipv6 any <X::X:X>/<0-128>
  - <config-ipv6-acl >#deny ipv6 any <X::X:X>/<0-128> dscp  
<0-63>
  - <config-ipv6-acl >#deny ipv6 any <X::X:X>/<0-128> dscp  
<0-63> shutdown
  - <config-ipv6-acl >#deny ipv6 any <X::X:X>/<0-128>  
precedence <0-7>
  - <config-ipv6-acl >#deny ipv6 any <X::X:X>/<0-128>  
precedence <0-7> shutdown
  - <config-ipv6-acl >#deny ipv6 any <X::X:X>/<0-128> shutdown
  - <config-ipv6-acl >#deny ipv6 any any
-



```

syslog / tacacs-ds / talk / telnet / time / whois / www>
match-all <TCP_FLAG> precedence <0-7> shutdown

```

- <config-ipv6-acl >#deny tcp <X::X:X>/<0-128> <0-65535 / PORT\_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> <X::X:X>/<0-128> <0-65535 / PORT\_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> match-all <TCP\_FLAG> shutdown
- <config-ipv6-acl >#deny tcp <X::X:X>/<0-128> <0-65535 / PORT\_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> <X::X:X>/<0-128> <0-65535 / PORT\_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> precedence <0-7>
- <config-ipv6-acl >#deny tcp <X::X:X>/<0-128> <0-65535 / PORT\_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> <X::X:X>/<0-128> <0-65535 / PORT\_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> precedence <0-7> shutdown
- <config-ipv6-acl >#deny tcp <X::X:X>/<0-128> <0-65535 / PORT\_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> <X::X:X>/<0-128> <0-65535 / PORT\_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> shutdown
- <config-ipv6-acl >#deny udp <X::X:X>/<0-128> <0-65535/ PORT\_RANGE / any / bootpc / bootps / discard / domain / echo / nameserver / netbios-ns / ntp / rip / snmp / snmptrap / sunrpc / syslog / tacacs-ds / talk / tftp / time / who> <X::X:X>/<0-128> <0-65535/ PORT\_RANGE / any / bootpc / bootps / discard / domain / echo / nameserver / netbios-ns / ntp / rip / snmp / snmptrap / sunrpc / syslog / tacacs-ds / talk / tftp / time / who>
- <config-ipv6-acl >#deny udp <X::X:X>/<0-128> <0-65535/ PORT\_RANGE / any / bootpc / bootps / discard / domain / echo / nameserver / netbios-ns / ntp / rip / snmp / snmptrap / sunrpc / syslog / tacacs-ds / talk / tftp / time / who> <X::X:X>/<0-128> <0-65535/ PORT\_RANGE / any / bootpc / bootps / discard / domain / echo / nameserver / netbios-ns / ntp / rip / snmp / snmptrap / sunrpc / syslog / tacacs-ds / talk / tftp / time / who> dscp <0-63>
- <config-ipv6-acl >#deny udp <X::X:X>/<0-128> <0-65535/ PORT\_RANGE / any / bootpc / bootps / discard / domain / echo / nameserver / netbios-ns / ntp / rip / snmp / snmptrap / sunrpc / syslog / tacacs-ds / talk / tftp / time / who> <X::X:X>/<0-128> <0-65535/ PORT\_RANGE / any / bootpc / bootps / discard / domain / echo / nameserver / netbios-ns / ntp / rip / snmp / snmptrap / sunrpc / syslog / tacacs-ds / talk / tftp / time / who> dscp <0-63> shutdown
- <config-ipv6-acl >#deny udp <X::X:X>/<0-128> <0-65535/ PORT\_RANGE / any / bootpc / bootps / discard / domain / echo / nameserver / netbios-ns / ntp / rip / snmp / snmptrap / sunrpc / syslog / tacacs-ds / talk / tftp / time / who>

|  |  |
|--|--|
|  | <p>&lt;X:X::X:X&gt;/&lt;0-128&gt; &lt;0-65535/ PORT_RANGE / any / bootpc / bootps / discard / domain / echo / nameserver / netbios-ns / ntp / rip / snmp / snmptrap / sunrpc / syslog / tacacs-ds / talk / tftp / time / who&gt; dscp &lt;0-63&gt; precedence &lt;0-7&gt;</p> <ul style="list-style-type: none"> <li>● &lt;config-ipv6-acl &gt;#deny udp &lt;X:X::X:X&gt;/&lt;0-128&gt; &lt;0-65535/ PORT_RANGE / any / bootpc / bootps / discard / domain / echo / nameserver / netbios-ns / ntp / rip / snmp / snmptrap / sunrpc / syslog / tacacs-ds / talk / tftp / time / who&gt; &lt;X:X::X:X&gt;/&lt;0-128&gt; &lt;0-65535/ PORT_RANGE / any / bootpc / bootps / discard / domain / echo / nameserver / netbios-ns / ntp / rip / snmp / snmptrap / sunrpc / syslog / tacacs-ds / talk / tftp / time / who&gt; dscp &lt;0-63&gt; precedence &lt;0-7&gt; shutdown</li> <li>● &lt;config-ipv6-acl &gt;#deny udp &lt;X:X::X:X&gt;/&lt;0-128&gt; &lt;0-65535&gt; any</li> </ul>  |
|  | <p>Use the “do” command to run execution command in current mode.<br/>&lt;SEQUENCE&gt; -</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config-ipv6-acl&gt;#do &lt;SEQUENCE&gt;</li> </ul>   |
|  | <p>Use the “end” command to finish current mode. Any changes in current mode will be saved.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config-ipv6-acl&gt;#end</li> </ul>  |
|  | <p>Use the “exit” command to close the current CLI session or return to the previous mode without saving the settings.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config-ipv6-acl&gt;#exit</li> </ul>  |
|  | <p>Use the “no sequence” command to delete any entry in management ACL.<br/>&lt;1-2147483647&gt;- Specify an index number of the ACL.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config-ip-acl&gt;#no sequence &lt;1-2147483647&gt;</li> </ul>   |
|  | <p>Use the “permit” command to create permit rules which bypass the packets meet the rule.</p> <p>&lt;0-255/icmp/ipv6/tcp /udp &gt; - Specify the IP protocol number or enter the name of the protocol.</p> <p>&lt;0-255/any&gt; - Specify ICMPv6 number.</p> <p>&lt;X:X::X:X&gt;/&lt;0-128&gt; &lt;X:X::X:X&gt;/&lt;0-128&gt; - Specify the source/destination IPv6 addresses and subnet masks.</p> <p>dscp &lt;0-63&gt; - Set the DSCP filtering by specifying a value for DSCP.</p> <p>precedence &lt;0-7&gt; - Set the cos value and the cos mask for a packet.</p> <p>shutdown - Disable the Ethernet interface.</p> <p>any - Any IP address (as source or destination).</p> <p>&lt;0-65535 / PORT_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www&gt; &lt;X:X::X:X&gt;/&lt;0-128&gt; &lt;0-65535 / PORT_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www&gt; - Set TCP port.</p> <p>match-all &lt;TCP_FLAG&gt; - Set TCP flags. List of TCP flags that should occur. If a flag should be set, it is prefixed by "+". If a flag should be unset, it is prefixed by "-". Available options are +urg, +ack, +psh, +rst, +syn, +fin, -urg, -ack, -psh, -rst, -syn and -fin. To define more than 1 flag - enter additional flags one after another without a space (example +syn-ack).</p> <p>&lt;0-65535/ PORT_RANGE / any / bootpc / bootps / discard / domain / echo / nameserver / netbios-ns / ntp / rip / snmp / snmptrap / sunrpc / syslog / tacacs-ds / talk / tftp / time / who&gt; &lt;X:X::X:X&gt;/&lt;0-128&gt; &lt;0-65535/ PORT_RANGE / any / bootpc /</p> |



---

bootps / discard / domain / echo / nameserver / netbios-ns / ntp / rip / snmp / snmptrap / sunrpc / syslog / tacacs-ds / talk / tftp / time / who> - Set UDP port.

**Related Syntax:**

- <config-ipv6-acl >#permit <0-255> <X::X:X>/<0-128> <X::X:X>/<0-128>
  - <config-ipv6-acl ># permit <0-255> <X::X:X>/<0-128> <X::X:X>/<0-128> dscp <0-63>
  - <config-ipv6-acl ># permit <0-255> <X::X:X>/<0-128> <X::X:X>/<0-128> dscp <0-63> shutdown
  - <config-ipv6-acl ># permit <0-255> <X::X:X>/<0-128> <X::X:X>/<0-128> precedence <0-7>
  - <config-ipv6-acl ># permit <0-255> <X::X:X>/<0-128> <X::X:X>/<0-128> precedence <0-7> shutdown
  - <config-ipv6-acl ># permit <0-255> <X::X:X>/<0-128> <X::X:X>/<0-128> shutdown
  - <config-ipv6-acl ># permit <0-255> <X::X:X>/<0-128> any dscp <0-63>
  - <config-ipv6-acl ># permit <0-255> <X::X:X>/<0-128> any dscp <0-63> shutdown
  - <config-ipv6-acl ># permit <0-255> <X::X:X>/<0-128> any precedence <0-7>
  - <config-ipv6-acl ># permit <0-255> <X::X:X>/<0-128> any precedence <0-7>shutdown
  - <config-ipv6-acl ># permit <0-255> <X::X:X>/<0-128> any shutdown
  - <config-ipv6-acl > permit icmp <X::X:X>/<0-128> <X::X:X>/<0-128> <0-255 / any / destination-unreachable / echo-reply / echo-request / nd-na / nd-ns / packet-too-big/ parameter-problem/ router-advertisement / router-solicitation / time-exceeded> <0-255/any> dscp <0-63>
  - <config-ipv6-acl ># permit icmp <X::X:X>/<0-128> <X::X:X>/<0-128><0-255 / any / destination-unreachable / echo-reply / echo-request / nd-na / nd-ns / packet-too-big/ parameter-problem/ router-advertisement / router-solicitation / time-exceeded> <0-255/any> dscp <0-63> shutdown
  - <config-ipv6-acl ># permit icmp <X::X:X>/<0-128> <X::X:X>/<0-128><0-255 / any / destination-unreachable / echo-reply / echo-request / nd-na / nd-ns / packet-too-big/ parameter-problem/ router-advertisement / router-solicitation / time-exceeded> <0-255/any> precedence <0-7>
  - <config-ipv6-acl ># permit icmp <X::X:X>/<0-128> <X::X:X>/<0-128><0-255 / any / destination-unreachable / echo-reply / echo-request / nd-na / nd-ns / packet-too-big/ parameter-problem/ router-advertisement / router-solicitation / time-exceeded> <0-255/any> precedence <0-7> shutdown
  - <config-ipv6-acl ># permit icmp <X::X:X>/<0-128> <X::X:X>/<0-128><0-255 / any / destination-unreachable / echo-reply / echo-request / nd-na / nd-ns / packet-too-big/ parameter-problem/ router-advertisement / router-solicitation / time-exceeded> <0-255/any> shutdown
  - <config-ipv6-acl ># permit icmp <X::X:X>/<0-128> any <0-255 / any / destination-unreachable / echo-reply / echo-request / nd-na / nd-ns / packet-too-big/ parameter-problem/ router-advertisement / router-solicitation / time-exceeded> <0-255 /any> dscp <0-63>
  - <config-ipv6-acl ># permit icmp <X::X:X>/<0-128> any <0-255 / any / destination-unreachable / echo-reply / echo-request / nd-na / nd-ns / packet-too-big/ parameter-problem/ router-advertisement / router-solicitation / time-exceeded> <0-255 /any> dscp <0-63>
-

---

shutdown

- <config-ipv6-acl ># permit icmp <X::X:X>/<0-128> any <0-255 / any / destination-unreachable / echo-reply / echo-request / nd-na / nd-ns / packet-too-big/ parameter-problem/ router-advertisement / router-solicitation / time-exceeded> <0-255 /any> precedence <0-7>
  - <config-ipv6-acl ># permit icmp <X::X:X>/<0-128> any <0-255 / any / destination-unreachable / echo-reply / echo-request / nd-na / nd-ns / packet-too-big/ parameter-problem/ router-advertisement / router-solicitation / time-exceeded> <0-255 /any> precedence <0-7> shutdown
  - <config-ipv6-acl ># permit icmp <X::X:X>/<0-128> any <0-255 / any / destination-unreachable / echo-reply / echo-request / nd-na / nd-ns / packet-too-big/ parameter-problem/ router-advertisement / router-solicitation / time-exceeded> <0-255 /any> shutdown
  - <config-ipv6-acl ># permit ipv6 <X::X:X>/<0-128> <X::X:X>/<0-128>
  - <config-ipv6-acl ># permit ipv6 <X::X:X>/<0-128> <X::X:X>/<0-128> dscp <0-63>
  - <config-ipv6-acl ># permit ipv6 <X::X:X>/<0-128> <X::X:X>/<0-128> dscp <0-63> shutdown
  - <config-ipv6-acl ># permit ipv6 <X::X:X>/<0-128> <X::X:X>/<0-128> precedence <0-7>
  - <config-ipv6-acl ># permit ipv6 <X::X:X>/<0-128> <X::X:X>/<0-128> precedence <0-7> shutdown
  - <config-ipv6-acl ># permit ipv6 <X::X:X>/<0-128> <X::X:X>/<0-128> shutdown
  - <config-ipv6-acl ># permit ipv6 <X::X:X>/<0-128> any dscp <0-63>
  - <config-ipv6-acl ># permit ipv6 <X::X:X>/<0-128> any dscp <0-63> shutdown
  - <config-ipv6-acl ># permit ipv6 <X::X:X>/<0-128> any precedence <0-7>
  - <config-ipv6-acl ># permit ipv6 <X::X:X>/<0-128> any precedence <0-7>shutdown
  - <config-ipv6-acl ># permit ipv6 <X::X:X>/<0-128> any shutdown
  - <config-ipv6-acl ># permit ipv6 any <X::X:X>/<0-128>
  - <config-ipv6-acl ># permit ipv6 any <X::X:X>/<0-128> dscp <0-63>
  - <config-ipv6-acl ># permit ipv6 any <X::X:X>/<0-128> dscp <0-63> shutdown
  - <config-ipv6-acl ># permit ipv6 any <X::X:X>/<0-128> precedence <0-7>
  - <config-ipv6-acl ># permit ipv6 any <X::X:X>/<0-128> precedence <0-7> shutdown
  - <config-ipv6-acl ># permit ipv6 any <X::X:X>/<0-128> shutdown
  - <config-ipv6-acl ># permit ipv6 any any
  - <config-ipv6-acl ># permit ipv6 any any dscp <0-63>
  - <config-ipv6-acl ># permit ipv6 any any dscp <0-63> shutdown
  - <config-ipv6-acl ># permit ipv6 any any precedence <0-7>
  - <config-ipv6-acl ># permit ipv6 any any precedence <0-7> shutdown
  - <config-ipv6-acl ># permit ipv6 any any shutdown
  - <config-ipv6-acl ># permit tcp <X::X:X>/<0-128> <0-65535 / PORT\_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> <X::X:X>/<0-128> <0-65535 / PORT\_RANGE / any /
-



- <config-ipv6-acl ># permit tcp <X:X::X>/<0-128> <0-65535 / PORT\_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> <X:X::X>/<0-128> <0-65535 / PORT\_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> precedence <0-7>
- <config-ipv6-acl ># permit tcp <X:X::X>/<0-128> <0-65535 / PORT\_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> <X:X::X>/<0-128> <0-65535 / PORT\_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> precedence <0-7> shutdown
- <config-ipv6-acl ># permit tcp <X:X::X>/<0-128> <0-65535 / PORT\_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> <X:X::X>/<0-128> <0-65535 / PORT\_RANGE / any / daytime / discard / domain / drip / echo / ftp / ftp-data / hostname / klogin / kshell / pop2 / pop3 / smtp / sunrpc / syslog / tacacs-ds / talk / telnet / time / whois / www> shutdown
- <config-ipv6-acl ># permit udp <X:X::X>/<0-128> <0-65535/ PORT\_RANGE / any / bootpc / bootps / discard / domain / echo / nameserver / netbios-ns / ntp / rip / snmp / snmptrap / sunrpc / syslog / tacacs-ds / talk / tftp / time / who> <X:X::X>/<0-128> <0-65535/ PORT\_RANGE / any / bootpc / bootps / discard / domain / echo / nameserver / netbios-ns / ntp / rip / snmp / snmptrap / sunrpc / syslog / tacacs-ds / talk / tftp / time / who>
- <config-ipv6-acl ># permit udp <X:X::X>/<0-128> <0-65535/ PORT\_RANGE / any / bootpc / bootps / discard / domain / echo / nameserver / netbios-ns / ntp / rip / snmp / snmptrap / sunrpc / syslog / tacacs-ds / talk / tftp / time / who> <X:X::X>/<0-128> <0-65535/ PORT\_RANGE / any / bootpc / bootps / discard / domain / echo / nameserver / netbios-ns / ntp / rip / snmp / snmptrap / sunrpc / syslog / tacacs-ds / talk / tftp / time / who> dscp <0-63>
- <config-ipv6-acl ># permit udp <X:X::X>/<0-128> <0-65535/ PORT\_RANGE / any / bootpc / bootps / discard / domain / echo / nameserver / netbios-ns / ntp / rip / snmp / snmptrap / sunrpc / syslog / tacacs-ds / talk / tftp / time / who> <X:X::X>/<0-128> <0-65535/ PORT\_RANGE / any / bootpc / bootps / discard / domain / echo / nameserver / netbios-ns / ntp / rip / snmp / snmptrap / sunrpc / syslog / tacacs-ds / talk / tftp / time / who> dscp <0-63> shutdown
- <config-ipv6-acl ># permit udp <X:X::X>/<0-128> <0-65535/ PORT\_RANGE / any / bootpc / bootps / discard / domain / echo / nameserver / netbios-ns / ntp / rip / snmp / snmptrap / sunrpc / syslog / tacacs-ds / talk / tftp / time / who> <X:X::X>/<0-128> <0-65535/ PORT\_RANGE / any / bootpc / bootps / discard / domain / echo / nameserver / netbios-ns / ntp / rip / snmp / snmptrap / sunrpc / syslog / tacacs-ds / talk / tftp / time / who> dscp <0-63> precedence <0-7>
- <config-ipv6-acl ># permit udp <X:X::X>/<0-128> <0-65535/ PORT\_RANGE / any / bootpc / bootps / discard / domain / echo / nameserver / netbios-ns / ntp / rip / snmp / snmptrap / sunrpc / syslog / tacacs-ds / talk / tftp / time / who> <X:X::X>/<0-128> <0-65535/ PORT\_RANGE / any / bootpc / bootps / discard / domain / echo / nameserver / netbios-ns / ntp / rip / snmp / snmptrap / sunrpc / syslog / tacacs-ds / talk

|                        |  |
|------------------------|--|
|                        | <p>/ tftp / time / who&gt; dscp &lt;0-63&gt; precedence &lt;0-7&gt; shutdown</p> <ul style="list-style-type: none"> <li>● &lt;config-ipv6-acl &gt;# permit udp &lt;X::X:X&gt;/&lt;0-128&gt; &lt;0-65535&gt; any</li> </ul> <p>Use the “sequence” command to deny or permit the ACL.<br/> &lt;1-2147483647&gt; - Enter the sequence of ACL entry. The sequence represents the priority of the ACE in the ACL.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config-ipv6-acl &gt;#sequence &lt;1-2147483647&gt; deny</li> <li>● &lt;config-ipv6-acl &gt;#sequence &lt;1-2147483647&gt; permit</li> </ul> <p>Use the “show acl” command to list current status of the selected ACL.</p>  |
| <p><i>ipv6 mld</i></p> | <p>Use this command to set MLD configuration.</p> <p>profile &lt;1-128&gt; - Use it to enter profile configuration.</p> <p>snooping - Use it to enable MLD snooping function.</p> <p>forward-method &lt;dip/mac&gt; -</p> <p>report-suppression - Use it to enable MLD snooping report-suppression function.</p> <p>unknown-multicast action &lt;drop/flood/router-port&gt; - Use it to set unknown multicast action.</p> <p>version &lt;1/2&gt; - Use it to change MLD support version.</p> <p>vlan &lt;1-4094&gt; - Use it to enable MLD on VLAN. Specify a VLAN ID for configuration.</p> <p>forbidden-port GigabitEthernet &lt;1-50&gt; - Specify a physical port.</p> <p>forbidden-port LAG &lt;1-8&gt; - Specify a LAG port.</p> <p>forbidden-router-port GigabitEthernet &lt;1-50&gt; - Use it to add static forbidden router port. Specify a physical port.</p> <p>forbidden-router-port LAG &lt;1-8&gt; - Use it to add static forbidden router port. Specify a LAG port.</p> <p>immediate-leave - Use it to enable fastleave function.</p> <p>last-member-query-count &lt;1-7&gt; - Use it to change how many query packets will send. Specify the last member query count. Default is 2.</p> <p>last-member-query-interval &lt;1-25&gt; - Use it to set interval between each query packet. Specify the last member query interval. Default is 1.</p> <p>query-interval &lt;30-18000&gt; - Use it to set interval between each query. Specify the query interval. Default is 125.</p> <p>response-time &lt;5-20&gt; - Use it to set response time. Specify a time value. Default is 10.</p> <p>robustness-variable &lt;1-7&gt; - Specify a robustness-variable value. Default is 2.</p> <p>router learn pim-dvmrp - Use it to enable learning router port by rouing protocol packets (DVMRP).</p> <p>static-group &lt;X::X:X&gt; interfaces gigabitethernet &lt;1-50&gt; - Use it to add a static group. Specify a physical port.</p> <p>static-group &lt;X::X:X&gt; interfaces LAG &lt;1-8&gt; - Use it to add a static group. Specify a LAG port.</p> <p>static-port gigabitethernet &lt;1-50&gt;- Use it to add static forwarding port. Specify a physical port.</p> <p>static-port LAG &lt;1-8&gt;- Use it to add static forwarding port. Specify a LAG port.</p> <p>static-router-port GigabitEthernet &lt;1-50&gt; - Use it to add static router port. All query packets wil forward to the specified port. Specify a physical port.</p> <p>static-router-port LAG &lt;1-8&gt; - Use it to add static router port. All query packets wil forward to the specified port. Specify a LAG port.</p> <p><b>Related Syntax:</b></p> |

- <config>#ipv6 mld profile <1-128>  
     <config-mld-profile># do  
     <config-mld-profile># end  
     <config-mld-profile># exit  
     <config-mld-profile># profile range ipv6 <X:X::X:X>  
     action <deny/permit>  
     <config-mld-profile># profile range ipv6 <X:X::X:X>  
     <X:X::X:X>  
     <config-mld-profile># profile range ipv6 <X:X::X:X>  
     <X:X::X:X> action <deny/permit>  
     <config-mld-profile># show
- <config>#ipv6 mld snooping
- <config>#ipv6 mld snooping forward-method <dip/mac>
- <config>#ipv6 mld snooping report-suppression
- <config>#ipv6 mld snooping unknown-multicast action  
     <drop/flood/router-port>
- <config>#ipv6 mld snooping version <1/2>
- <config>#ipv6 mld snooping vlan <1-4094>
- <config>#ipv6 mld snooping vlan <1-4094> forbidden-port  
     GigabitEthernet <1-50>
- <config>#ipv6 mld snooping vlan <1-4094> forbidden-port LAG  
     <1-8>
- <config>#ipv6 mld snooping vlan <1-4094>  
     forbidden-router-port GigabitEthernet <1-50>
- <config>#ipv6 mld snooping vlan <1-4094>  
     forbidden-router-port LAG <1-8>
- <config>#ipv6 mld snooping vlan <1-4094> immediate-leave
- <config>#ipv6 mld snooping vlan <1-4094>  
     last-member-query-count <1-7>
- <config>#ipv6 mld snooping vlan <1-4094>  
     last-member-query-interval <1-25>
- <config>#ipv6 mld snooping vlan <1-4094> query-interval  
     <30-18000>
- <config>#ipv6 mld snooping vlan <1-4094> response-time  
     <5-20>
- <config>#ipv6 mld snooping vlan <1-4094> robustness-variable  
     <1-7>
- <config>#ipv6 mld snooping vlan <1-4094> router learn  
     pim-dvmrp
- <config>#ipv6 mld snooping vlan <1-4094> static-group  
     <X:X::X:X> interfaces gigabitethernet <1-50>
- <config>#ipv6 mld snooping vlan <1-4094> static-group  
     <X:X::X:X> interfaces LAG <1-8>
- <config>#ipv6 mld snooping vlan <1-4094> static-port  
     gigabitethernet <1-50>
- <config>#ipv6 mld snooping vlan <1-4094> static-port LAG  
     <1-8>
- <config>#ipv6 mld snooping vlan <1-4094> static-router-port  
     GigabitEthernet <1-50>
- <config>#ipv6 mld snooping vlan <1-4094> static-router-port  
     LAG <1-8>

## Example

```
G2500# configure
G2500(config)#
```

```
G2500(config)# ipv6 mld snooping vlan 33
G2500(config)# ipv6 acl CA_v6
G2500(config-ipv6-acl)# deny 3 00:50::32:ff/24 00:50::78:aa/32
```

## Telnet Command: jumbo-frame

Use this command to modify the maximum frame size of jumbo frame.

### Syntax Items

jumbo-frame

### Description

| Syntax Items       | Description  |
|--------------------|--|
| <i>jumbo-frame</i> | <p>Enable the function of jumbo frame.<br/>Set the maximum frame size.<br/>&lt;1518-12288&gt; - The default value is 1522.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# jumbo-frame</li> <li>● &lt;config&gt;# jumbo-frame &lt;1518-12288&gt;</li> </ul> |

### Example

```
G2500# configure
G2500(config)#
G2500(config)# jumbo-frame 8000
G2500(config)#
```

## Telnet Command: lacp

Use this command to set the system priority of the switch.

### Syntax Items

lacp

lacp system-priority

### Description

| Syntax Items                | Description   |
|-----------------------------|---|
| <i>lacp</i>                 | Enable the function.  |
| <i>lacp system-priority</i> | <p>It is used for selecting a master switch between two devices. Lower system priority has higher priority. The device with higher priority value can determine which port is able to join LAG.<br/>&lt;1-65535&gt; - Specify the system priority value.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# lacp</li> <li>● &lt;config&gt;# lacp system-priority &lt;1-65535&gt;</li> </ul> |

### Example

```
G2500# configure
G2500(config)#
G2500(config)# lacp system-priority 1000
G2500(config)#
```

## Telnet Command: lag

LAG port can transmit packets to all ports for balancing the traffic loading. Use this command to change the load balance algorithm to src-dst-mac or src-dst-mac-ip as the Load Balance policy.

### Syntax Items

lag load-balance

### Description

| Syntax Items            | Description   |
|-------------------------|---|
| <i>lag load-balance</i> | LAG load balancing is based on source and destination MAC address and/or IP address.<br><b>Related Syntax:</b> <ul style="list-style-type: none"><li>● &lt;config&gt;# lag load-balance src-dst-mac</li><li>● &lt;config&gt;# lag load-balance src-dst-mac-ip</li></ul> |

### Example

```
G2500# configure
G2500(config)#
```

## Telnet Command: line

Use this command to select line configuration mode.

### Syntax Items

line console

line ssh

line telnet

### Description

| Syntax Items              | Description  |
|---------------------------|--|
| <i>console/ssh/telnet</i> | Select console configuration mode.<br>To configure <i>detailed settings</i> , access into next level.<br><config>#line <console/ssh/telnet><br>console - Select the console line to configure. Then, available sub-commands are:<br><config-line>#do<br><config-line>#exec-timeout<br><config-line>#exit<br><config-line>#history<br><config-line>#no<br><config-line>#password-thresh<br><config-line>#silent-time<br><br>Select SSH line to configure. Then, available sub-commands are:<br><config-line>#do<br><config-line>#end<br><config-line>#exec-timeout<br><config-line>#exit<br><config-line>#password-thresh |



|                         |  |
|-------------------------|--|
|                         | <p>&lt;config-line&gt;#silent-time</p> <hr/> <p>telnet - Select telnet line to configure. Then, available sub-commands are:</p> <p>&lt;config-line&gt;#do<br/>         &lt;config-line&gt;#end<br/>         &lt;config-line&gt;#exec-timeout<br/>         &lt;config-line&gt;#exit<br/>         &lt;config-line&gt;#password-thresh<br/>         &lt;config-line&gt;#silent-time</p> |
| <i>#do</i>              | <p>Use the “do” command to run execution command in current mode.<br/>         &lt;SEQUENCE&gt; -</p> <p><b>Related Syntax:</b><br/>         &lt;config-line&gt;#do &lt;SEQUENCE&gt;</p>   |
| <i>#exec-timeout</i>    | <p>Use the “exec-timeout” to set the session timeout configuration.<br/>         &lt;0-65535&gt; - Enter the number.</p> <p><b>Related Syntax:</b><br/>         &lt;config-line&gt;#exec-timeout &lt;0-65535&gt;</p>   |
| <i>#exit</i>            | <p>Use the “exit” command to close the current CLI session or return to the previous mode without saving the settings.</p> <p><b>Related Syntax:</b><br/>         &lt;config-line&gt;#exit</p>   |
| <i>#history</i>         | <p>Use the “history” command to specify the index number of history.<br/>         &lt;1-256&gt; - Enter a number.</p> <p><b>Related Syntax:</b><br/>         &lt;config-line&gt;#history &lt;1-256&gt;</p>   |
| <i>#no</i>              | <p>Use the “no” command to negate line command.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config-line&gt;#no enable</li> <li>● &lt;config-line&gt;#no history</li> <li>● &lt;config-line&gt;#no login</li> </ul>  |
| <i>#password-thresh</i> | <p>Use the “password-thresh” command to set the login password intrusion threshold.<br/>         &lt;0-120&gt; - Set a number of allowed password attempts. 0 means no threshold.</p> <p><b>Related Syntax:</b><br/>         &lt;config-line&gt;#password-thresh &lt;0-120&gt;</p>   |
| <i>#silent-time</i>     | <p>Use the “silent-time” command to set fail silent time.<br/>         &lt;0-65535&gt; - Set the time to disable the console response.</p> <p><b>Related Syntax:</b><br/>         &lt;config-line&gt;#silent-time &lt;0-65535&gt;</p>  |

## Example

```
G2500# configure
G2500(config)#
G2500(config)# line telnet
P2280x(config-line)#
```

## Telnet Command: Ildp

Use this command to set LLDP function.

### Syntax Items

Ildp  
Ildp holdtime-multiplier  
Ildp Ildpdu  
Ildp med  
Ildp reinit-delay  
Ildp tx-delay  
Ildp tx-interval

### Description

| Syntax Items                    | Description  |
|---------------------------------|--|
| <i>Ildp</i>                     | Enable the function of LLDP.   |
| <i>Ildp holdtime-multiplier</i> | Set the multiplier used for calculating the LLDP discovery packet hold time.<br><2-10> - Set the LLDP hold time multiplier.<br><b>Related Syntax:</b> <ul style="list-style-type: none"><li>● &lt;config&gt;# Ildp holdtime-multiplier &lt;2-10&gt;</li></ul>  |
| <i>Ildp Ildpdu</i>              | bridging - The LLDP packets will be bridging when LLDP is disabled.<br>filtering - The LLDP packets will be filtered and deleted when LLDP is disabled.<br>flooding - The LLDP packets will be flooded and forwarded to all interfaces when LLDP is disabled.<br><b>Related Syntax:</b> <ul style="list-style-type: none"><li>● &lt;config&gt;# Ildp Ildpdu bridging</li><li>● &lt;config&gt;# Ildp Ildpdu filtering</li><li>● &lt;config&gt;# Ildp Ildpdu flooding</li></ul>  |
| <i>Ildp med</i>                 | med fast-start-repeat-count - Set the LLDP PDU fast start TX repeat count.<br>med network-policy - Set the LLDP MED network policy table.<br>med network-poicy voice auto - Enable the network policy voice auto mode.<br><1-10> - Set the fast start repeat count.<br><1-32> - Specify the index number of the policy.<br>app <guest-voice/ gust-voice-signaling / softphone-voice / streaming-video / video-conferencing / video-signaling / voice / voice-signaling> - Configure the application type for the policy.<br>vlan <1-4094> - Specify the VLAN ID.<br>vlan-type <tag/untag> - Set the VLAN tag status.<br>priority <0-7> - Specify the L2 priority.<br>dscp <0-63> - Specify the DSCP value.<br><b>Related Syntax:</b> <ul style="list-style-type: none"><li>● &lt;config&gt;# Ildp med fast-start-repeat-count &lt;1-10&gt;</li><li>● &lt;config&gt;# Ildp med network-policy &lt;1-32&gt; app&lt; guest-voice/ gust-voice-signaling / softphone-voice / streaming-video / video-conferencing / video-signaling / voice / voice-signaling &gt; vlan &lt;1-4094&gt; vlan-type &lt;tag/untag&gt; priority &lt;0-7&gt; dscp &lt;0-63&gt;</li><li>● &lt;config&gt;# Ildp med network-poicy voice auto</li></ul> |

|                         |  |
|-------------------------|--|
| <i>lldp rinit-delay</i> | Set the LLDP re-initial delay to avoid LLDP generating too many PDU.<br><1-10> - Specify a number for LLDP server to initialize.<br><b>Related Syntax:</b><br>● <config># lldp rinit-delay <1-10>  |
| <i>lldp tx-delay</i>    | Set the delay time between the successful LLDP frame transmissions.<br><1-8191> - Enter the number of delay time.<br>Note that both tx-interval and tx-delay will affect the LLDP PDU TX time.<br><b>Related Syntax:</b><br>● <config># lldp tx-delay <1-8191> |
| <i>lldp tx-interval</i> | Set the LLDP TX interval.<br><5-32767> - Enter the interval in unit of second.<br><b>Related Syntax:</b><br>● <config># lldp tx-interval <5-32767>   |

### Example

```
G2500# configure
G2500(config)#
G2500(config)# lldp med network-policy 30 app guest-voice vlan 30 vlan-type
untag priority 3 dscp
G2500(config)#
```

## Telnet Command: logging

Use this command to set logging service on VigorSwitch.

### Syntax Items

logging

logging buffered

logging console

logging file

logging host

### Description

| Syntax Items            | Description   |
|-------------------------|---|
| <i>logging</i>          | Enable the logging service.   |
| <i>logging buffered</i> | Store the log message in the RAM.   |
| <i>logging console</i>  | Specify the logging level.<br><0-7> - Specify the logging level by entering a number (from EMEGR-DEBUG).<br><b>Related Syntax:</b><br>● <config># logging console<br>● <config># logging console severity <0-7> |
| <i>logging file</i>     | Store the log message in the flash.<br><0-7> - Specify the logging level by entering a number (from EMEGR-DEBUG).<br><b>Related Syntax:</b>   |

|                     |  |
|---------------------|--|
|                     | <ul style="list-style-type: none"> <li>● &lt;config&gt;# logging <i>file severity</i> &lt;0-7&gt;</li> </ul>   |
| <i>logging host</i> | <p>Define the logging server.</p> <p>host &lt;A.B.C.D&gt; - Enter an IP address of the remote (or local) server.</p> <p>facility &lt;local0-local7&gt; - Specify the facility parameter for the syslog message.</p> <p>port &lt;1-65535&gt; - Enter a number for the remote server. Default is 514.</p> <p>severity &lt;0-7&gt; - Specify the logging level by entering a number (from EMEGR-DEBUG).</p> <p>&lt;HOSTNAME&gt; - Define a name as the host.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;#logging host &lt;A.B.C.D&gt; facility &lt;local0-local7&gt;</li> <li>● &lt;config&gt;#logging host &lt;A.B.C.D&gt; port &lt;1-65535&gt;</li> <li>● &lt;config&gt;#logging host &lt;A.B.C.D&gt; port &lt;1-65535&gt; facility &lt;local0-local7&gt;</li> <li>● &lt;config&gt;#logging host &lt;A.B.C.D&gt; port &lt;1-65535&gt; severity &lt;0-7&gt; facility &lt;local0-local7&gt;</li> <li>● &lt;config&gt;#logging host &lt;A.B.C.D&gt; severity &lt;0-7&gt; facility &lt;local0-local7&gt;</li> <li>● &lt;config&gt;#logging host &lt;HOSTNAME&gt; facility &lt;local0-local7&gt;</li> <li>● &lt;config&gt;#logging host &lt;HOSTNAME&gt; port &lt;1-65535&gt;</li> <li>● &lt;config&gt;#logging host &lt;HOSTNAME&gt; port &lt;1-65535&gt; facility &lt;local0-local7&gt;</li> <li>● &lt;config&gt;#logging host &lt;HOSTNAME&gt; port &lt;1-65535&gt; severity &lt;0-7&gt; facility &lt;local0-local7&gt;</li> <li>● &lt;config&gt;#logging host &lt;HOSTNAME&gt; severity &lt;0-7&gt; facility &lt;local0-local7&gt;</li> <li>● &lt;config&gt;#logging host &lt;X:X::X:X&gt; facility &lt;local0-local7&gt;</li> <li>● &lt;config&gt;#logging host &lt;X:X::X:X&gt; port &lt;1-65535&gt;</li> <li>● &lt;config&gt;#logging host &lt;X:X::X:X&gt; port &lt;1-65535&gt; facility &lt;local0-local7&gt;</li> <li>● &lt;config&gt;#logging host &lt;X:X::X:X&gt; port &lt;1-65535&gt; severity &lt;0-7&gt; facility &lt;local0-local7&gt;</li> </ul> |

### Example

```
G2500# configure
G2500(config)#
G2500(config)# logging host aa:00::1a:FF facility local1
```

### Telnet Command: logmail

Use this command to configure log mail.

#### Syntax Items

logmail active  
logmail auth  
logmail category  
logmail encry  
logmail password  
logmail port  
logmail receiver  
logmail sender  
logmail server  
logmail username

## Description

| Syntax Items            | Description   |
|-------------------------|---|
| <i>logmail active</i>   | <disable/enable> - Enable or disable the function of log mail.<br><b>Related Syntax:</b><br>● <config># logmail active <disable/enable>   |
| <i>logmail auth</i>     | <disable/enable> - Enable or disable the function of SMTP server authentication.<br><b>Related Syntax:</b><br>● <config># logmail auth <disable/enable>   |
| <i>logmail category</i> | <AAA, ACL, AUTHMGR, CABLE_DIAG, DAI, DHCP_SNOOPING, GVRP, IGMP_SNOOPING, IPSP, L2, LLDP, Mac-based, Mirror, MLD_SNOOPING, Platform, PM, POE, Port, PORT_SECURITY, QoS, Rate, SNMP, STP, Security, System, Surveillance, Trunk, UDLD, VLAN, CLEAR> - Specify one type for the logmail.<br><b>Related Syntax:</b><br>● <config># logmail category <AAA, ACL, AUTHMGR, CABLE_DIAG, DAI, DHCP_SNOOPING, GVRP, IGMP_SNOOPING, IPSP, L2, LLDP, Mac-based, Mirror, MLD_SNOOPING, Platform, PM, POE, Port, PORT_SECURITY, QoS, Rate, SNMP, STP, Security, System, Surveillance, Trunk, UDLD, VLAN, CLEAR> |
| <i>logmail encry</i>    | <disable/sslTls/starttls> - Specify the encryption type for mail alert.<br><b>Related Syntax:</b><br>● <config># logmail encry <disable/ sslTls/starttls>   |
| <i>logmail password</i> | <PASSWORD> - Enter the password for SMTP server authentication.<br><b>Related Syntax:</b><br>● <config># logmail password <PASSWORD>  |
| <i>logmail port</i>     | <0-65535>- Enter a port number.<br><b>Related Syntax:</b><br>● <config># logmail port <0-65535>   |
| <i>logmail receiver</i> | Specify an address for receiving the alert mail.<br><ADDRESS> - Enter the email address of the receiver.<br><b>Related Syntax:</b><br>● <config># logmail receiver <ADDRESS>  |
| <i>logmail sender</i>   | Specify an address which sends out the alert mail.<br><ADDRESS> - Enter the email address of the sender.<br><b>Related Syntax:</b><br>● <config># logmail   |
| <i>logmail server</i>   | Set the IP address of the server.<br><ADDRESS> - Enter the IP address of the SMTP server.<br><b>Related Syntax:</b><br>● <config># logmail server <ADDRESS>   |
| <i>logmail username</i> | <NAME> - Enter the username authenticated by STMP server.<br><b>Related Syntax:</b><br>● <config># logmail username <NAME>  |

## Example

```
G2500# configure
G2500(config)#
G2500(config)# logmail receiver carrie_ni@draytek.com
G2500(config)#
```

## Telnet Command: loop-protection

Use this command to set loop-protection.

### Syntax Items

loop-protection action  
loop-protection periodicTime  
loop-protection state

### Description

| Syntax Items                        | Description  |
|-------------------------------------|--|
| <i>loop-protection action</i>       | Specify an action to be taken when the loop is happened.<br><all/log/shutdown> - Specify one action to be executed.<br><b>Related Syntax:</b> <ul style="list-style-type: none"><li>● &lt;config&gt;# loop-protection action &lt;all/log/shutdown&gt;</li></ul>            |
| <i>loop-protection periodicTime</i> | Send the loop protection packets to the network hosts.<br><1-3> - Enter the number of the packet.<br><b>Related Syntax:</b><br><config># <b>Related Syntax:</b> <ul style="list-style-type: none"><li>● &lt;config&gt;# loop-protection periodicTime &lt;1-3&gt;</li></ul> |
| <i>loop-protection state</i>        | <enable/disable> - Enable or disable the function of loop protection.<br><b>Related Syntax:</b> <ul style="list-style-type: none"><li>● &lt;config&gt;# loop-protection state &lt;enable/disable&gt;</li></ul>   |

### Example

```
G2500# configure
G2500(config)#
G2500(config)# loop-protection state enable
G2500(config)#
```

## Telnet Command: mac

Use this command to create a MAC access list.

### Syntax Items

mac acl  
mac address-table

### Description

| Syntax Items   | Description  |
|----------------|--|
| <i>mac acl</i> | <NAME> - Set the name of the access list (ACL).<br>To configure detailed settings, enter the name of ACL to access into next level.<br><config>#mac acl <NAME><br>Then, available sub-commands are:<br><config-mac-acl>#deny<br><config-mac-acl>#do<br><config-mac-acl>#end<br><config-mac-acl>#exit |

---

<config-mac-acl>#permit  
<config-mac-acl>#sequence

---

Use the "deny" command to add deny rules for the MAC access list:

<A:B:C:D:E:F>/<A:B:C:D:E:F>><A:B:C:D:E:F>/<A:B:C:D:E:F> - Specify the source and destination MAC addresses and subnet masks.

cos <0-7><0-7> - Set the cos value and the cos mask for a packet.

<0x0600-0xFFFF> - Set the EtherType of the packet.

Shutdown - Disable the Ethernet interface.

vlan <1-4094> - Specify the VLAN ID of the packet.

any - Any MAC address.

**Related Syntax:**

- <config-mac-acl >#deny <A:B:C:D:E:F>/<A:B:C:D:E:F> ><A:B:C:D:E:F>/<A:B:C:D:E:F> cos <0-7><0-7>
  - <config-mac-acl >#deny <A:B:C:D:E:F>/<A:B:C:D:E:F> ><A:B:C:D:E:F>/<A:B:C:D:E:F> cos <0-7><0-7> ethtype <0x0600-0xFFFF>
  - <config-mac-acl >#deny <A:B:C:D:E:F>/<A:B:C:D:E:F> ><A:B:C:D:E:F>/<A:B:C:D:E:F> cos <0-7><0-7> ethtype <0x0600-0xFFFF> shutdown
  - <config-mac-acl >#deny <A:B:C:D:E:F>/<A:B:C:D:E:F> ><A:B:C:D:E:F>/<A:B:C:D:E:F> cos <0-7><0-7> shutdown
  - <config-mac-acl >#deny <A:B:C:D:E:F>/<A:B:C:D:E:F> ><A:B:C:D:E:F>/<A:B:C:D:E:F> ethtype <0x0600-0xFFFF>
  - <config-mac-acl ># deny <A:B:C:D:E:F>/<A:B:C:D:E:F> ><A:B:C:D:E:F>/<A:B:C:D:E:F> ethtype <0x0600-0xFFFF> shutdown
  - <config-mac-acl ># deny <A:B:C:D:E:F>/<A:B:C:D:E:F> ><A:B:C:D:E:F>/<A:B:C:D:E:F> shutdown
  - <config-mac-acl >#deny any <A:B:C:D:E:F>/<A:B:C:D:E:F> ><A:B:C:D:E:F>/<A:B:C:D:E:F> cos <0-7><0-7>
  - <config-mac-acl >#deny any <A:B:C:D:E:F>/<A:B:C:D:E:F> ><A:B:C:D:E:F>/<A:B:C:D:E:F> cos <0-7><0-7> ethtype <0x0600-0xFFFF>
  - <config-mac-acl >#deny any <A:B:C:D:E:F>/<A:B:C:D:E:F> ><A:B:C:D:E:F>/<A:B:C:D:E:F> cos <0-7><0-7> ethtype <0x0600-0xFFFF> shutdown
  - <config-mac-acl >#deny any <A:B:C:D:E:F>/<A:B:C:D:E:F> ><A:B:C:D:E:F>/<A:B:C:D:E:F> cos <0-7><0-7> shutdown
  - <config-mac-acl >#deny any any cos <0-7><0-7>
  - <config-mac-acl >#deny any any cos <0-7><0-7> ethtype <0x0600-0xFFFF>
  - <config-mac-acl >#deny any any cos <0-7><0-7> ethtype <0x0600-0xFFFF> shutdown
  - <config-mac-acl >#deny any any cos <0-7><0-7> shutdown
  - <config-mac-acl >#deny any any ethtype <0x0600-0xFFFF>
  - <config-mac-acl >#deny any any ethtype <0x0600-0xFFFF> shutdown
  - <config-mac-acl >#deny any any shutdown
  - <config-mac-acl >#deny any any vlan <1-4094>
  - <config-mac-acl >#deny any any vlan <1-4094> cos <0-7><0-7>
  - <config-mac-acl >#deny any any vlan <1-4094> cos <0-7><0-7> ethtype <0x0600-0xFFFF>
  - <config-mac-acl >#deny any any vlan <1-4094> cos <0-7><0-7> ethtype <0x0600-0xFFFF> shutdown
  - <config-mac-acl >#deny any any vlan <1-4094> ethtype <0x0600-0xFFFF>
  - <config-mac-acl >#deny any any vlan <1-4094> ethtype <0x0600-0xFFFF> shutdown
  - <config-mac-acl >#deny any any vlan <1-4094> shutdown
-

|  |  |
|--|--|
|  | <p>Use the “do” command to run execution command in current mode.<br/>&lt;SEQUENCE&gt; -</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config-mac-acl&gt;#do &lt;SEQUENCE&gt;</li> </ul>  |
|  | <p>Use the “end” command to finish current mode. Any changes in current mode will be saved.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config-mac-acl&gt;#end</li> </ul>   |
|  | <p>Use the “exit” command to close the current CLI session or return to the previous mode without saving the settings.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config-mac-acl&gt;#exit</li> </ul>   |
|  | <p>Use the “no sequence” command to delete any entry in management ACL.</p> <p>&lt;1-65535&gt;- Specify an index number of the ACL.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config-mac-acl&gt;#no sequence &lt;1-65535&gt;</li> </ul>   |
|  | <p>Use the “permit” command to add permit rules which bypass the packets meet the rule.</p> <p>&lt;A:B:C:D:E:F&gt;/&lt;A:B:C:D:E:F &gt;- Specify the source and destination MAC addresses and subnet masks.</p> <p>cos &lt;0-7&gt;&lt;0-7&gt; - Set the cos value and the cos mask for a packet.</p> <p>&lt;0x0600-0xFFFF&gt; - Set the EtherType of the packet.</p> <p>Shutdown - Disable the Ethernet interface.</p> <p>vlan &lt;1-4094&gt; - Specify the VLAN ID of the packet.</p> <p>any - Any MAC address.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config-mac-acl &gt;#permit &lt;A:B:C:D:E:F&gt;/&lt;A:B:C:D:E:F&gt; cos &lt;0-7&gt;&lt;0-7&gt;</li> <li>● &lt;config-mac-acl &gt;#permit &lt;A:B:C:D:E:F&gt;/&lt;A:B:C:D:E:F&gt; cos &lt;0-7&gt;&lt;0-7&gt; ethtype &lt;0x0600-0xFFFF&gt;</li> <li>● &lt;config-mac-acl &gt;#permit &lt;A:B:C:D:E:F&gt;/&lt;A:B:C:D:E:F&gt; ethtype &lt;0x0600-0xFFFF&gt;</li> <li>● &lt;config-mac-acl &gt;#permit &lt;A:B:C:D:E:F&gt;/&lt;A:B:C:D:E:F&gt; vlan &lt;1-4094&gt;</li> <li>● &lt;config-mac-acl &gt;#permit &lt;A:B:C:D:E:F&gt;/&lt;A:B:C:D:E:F&gt; vlan &lt;1-4094&gt;cos &lt;0-7&gt;&lt;0-7&gt;</li> <li>● &lt;config-mac-acl &gt;#permit &lt;A:B:C:D:E:F&gt;/&lt;A:B:C:D:E:F&gt; vlan &lt;1-4094&gt;cos &lt;0-7&gt;&lt;0-7&gt; ethtype &lt;0x0600-0xFFFF&gt;</li> <li>● &lt;config-mac-acl &gt;#permit &lt;A:B:C:D:E:F&gt;/&lt;A:B:C:D:E:F&gt; vlan &lt;1-4094&gt;ethtype &lt;0x0600-0xFFFF&gt;</li> <li>● &lt;config-mac-acl &gt;#permit any &lt;A:B:C:D:E:F&gt;/&lt;A:B:C:D:E:F&gt; cos &lt;0-7&gt;&lt;0-7&gt;</li> <li>● &lt;config-mac-acl &gt;#permit any &lt;A:B:C:D:E:F&gt;/&lt;A:B:C:D:E:F&gt; cos &lt;0-7&gt;&lt;0-7&gt;ethtype &lt;0x0600-0xFFFF&gt;</li> <li>● &lt;config-mac-acl &gt;#permit any &lt;A:B:C:D:E:F&gt;/&lt;A:B:C:D:E:F&gt; ethtype &lt;0x0600-0xFFFF&gt;</li> <li>● &lt;config-mac-acl &gt;#permit any &lt;A:B:C:D:E:F&gt;/&lt;A:B:C:D:E:F&gt; vlan &lt;1-4094&gt;</li> <li>● &lt;config-mac-acl &gt;#permit any &lt;A:B:C:D:E:F&gt;/&lt;A:B:C:D:E:F&gt; vlan &lt;1-4094&gt; cos &lt;0-7&gt;&lt;0-7&gt;</li> <li>● &lt;config-mac-acl &gt;#permit any &lt;A:B:C:D:E:F&gt;/&lt;A:B:C:D:E:F&gt; vlan &lt;1-4094&gt; cos &lt;0-7&gt;&lt;0-7&gt;ethtype &lt;0x0600-0xFFFF&gt;</li> <li>● &lt;config-mac-acl &gt;#permit any &lt;A:B:C:D:E:F&gt;/&lt;A:B:C:D:E:F&gt; vlan &lt;1-4094&gt; ethtype &lt;0x0600-0xFFFF&gt;</li> </ul> |
|  | <p>Use the “sequence” command to deny or permit the ACL.</p>   |



<1-2147483647> - Enter the sequence index ACE. The sequence represents the priority of the ACE in the ACL.  
 <A:B:C:D:E:F>/<A:B:C:D:E:F >- Specify the source and destination MAC addresses and subnet masks.  
 cos <0-7><0-7> - Set the cos value and the cos mask for a packet.  
 <0x0600-0xFFFF> - Set the EtherType of the packet.  
 shutdown - Disable the Ethernet interface.  
 vlan <1-4094> - Specify the VLAN ID of the packet.  
 any - Any MAC address.

**Related Syntax:**

- <config-mac-acl >#sequence <1-2147483647>deny <A:B:C:D:E:F>/<A:B:C:D:E:F ><A:B:C:D:E:F>/<A:B:C:D:E:F> cos <0-7><0-7>
- <config-mac-acl >#sequence <1-2147483647>deny <A:B:C:D:E:F>/<A:B:C:D:E:F ><A:B:C:D:E:F>/<A:B:C:D:E:F> cos <0-7><0-7> ethtype <0x0600-0xFFFF>
- <config-mac-acl >#sequence <1-2147483647>deny <A:B:C:D:E:F>/<A:B:C:D:E:F ><A:B:C:D:E:F>/<A:B:C:D:E:F> cos <0-7><0-7> ethtype <0x0600-0xFFFF> shutdown
- <config-mac-acl >#sequence <1-2147483647>deny <A:B:C:D:E:F>/<A:B:C:D:E:F ><A:B:C:D:E:F>/<A:B:C:D:E:F> cos <0-7><0-7> shutdown
- <config-mac-acl >#sequence <1-2147483647>deny <A:B:C:D:E:F>/<A:B:C:D:E:F ><A:B:C:D:E:F>/<A:B:C:D:E:F> ethtype <0x0600-0xFFFF>
- <config-mac-acl >#sequence <1-2147483647>deny <A:B:C:D:E:F>/<A:B:C:D:E:F ><A:B:C:D:E:F>/<A:B:C:D:E:F> ethtype <0x0600-0xFFFF> shutdown
- <config-mac-acl >#sequence <1-2147483647>deny <A:B:C:D:E:F>/<A:B:C:D:E:F ><A:B:C:D:E:F>/<A:B:C:D:E:F> shutdown
- <config-mac-acl >#sequence <1-2147483647>deny any <A:B:C:D:E:F>/<A:B:C:D:E:F ><A:B:C:D:E:F>/<A:B:C:D:E:F> cos <0-7><0-7>
- <config-mac-acl >#sequence <1-2147483647>deny any <A:B:C:D:E:F>/<A:B:C:D:E:F ><A:B:C:D:E:F>/<A:B:C:D:E:F> cos <0-7><0-7> ethtype <0x0600-0xFFFF>
- <config-mac-acl >#sequence <1-2147483647>deny any <A:B:C:D:E:F>/<A:B:C:D:E:F ><A:B:C:D:E:F>/<A:B:C:D:E:F> cos <0-7><0-7> ethtype <0x0600-0xFFFF> shutdown
- <config-mac-acl >#sequence <1-2147483647>deny any <A:B:C:D:E:F>/<A:B:C:D:E:F ><A:B:C:D:E:F>/<A:B:C:D:E:F> cos <0-7><0-7> shutdown
- <config-mac-acl >#sequence <1-2147483647>deny any any cos <0-7><0-7>
- <config-mac-acl >#sequence <1-2147483647>deny any any cos <0-7><0-7> ethtype <0x0600-0xFFFF>
- <config-mac-acl >#sequence <1-2147483647>deny any any cos <0-7><0-7> ethtype <0x0600-0xFFFF> shutdown
- <config-mac-acl >#sequence <1-2147483647>deny any any cos <0-7><0-7> shutdown
- <config-mac-acl >#sequence <1-2147483647>deny any any ethtype <0x0600-0xFFFF>
- <config-mac-acl >#sequence <1-2147483647>deny any any ethtype <0x0600-0xFFFF> shutdown
- <config-mac-acl >#sequence <1-2147483647>deny any any shutdown
- <config-mac-acl >#sequence <1-2147483647>deny any any vlan <1-4094>
- <config-mac-acl >#sequence <1-2147483647>deny any any vlan <1-4094> cos <0-7><0-7>
- <config-mac-acl >#sequence <1-2147483647>deny any any

|  |   |
|--|---|
|  | <pre> vlan &lt;1-4094&gt; cos &lt;0-7&gt;&lt;0-7&gt; ethtype &lt;0x0600-0xFFFF&gt; ● &lt;config-mac-acl &gt;#sequence &lt;1-2147483647&gt;deny any any vlan &lt;1-4094&gt; cos &lt;0-7&gt;&lt;0-7&gt; ethtype &lt;0x0600-0xFFFF&gt; shutdown ● &lt;config-mac-acl &gt;#sequence &lt;1-2147483647&gt;deny any any vlan &lt;1-4094&gt; ethtype &lt;0x0600-0xFFFF&gt; ● &lt;config-mac-acl &gt;#sequence &lt;1-2147483647&gt;deny any any vlan &lt;1-4094&gt; ethtype &lt;0x0600-0xFFFF&gt; shutdown ● &lt;config-mac-acl &gt;#sequence &lt;1-2147483647&gt;deny any any vlan &lt;1-4094&gt; shutdown ● &lt;config-mac-acl &gt;#sequence &lt;1-2147483647&gt;permit &lt;A:B:C:D:E:F&gt;/&lt;A:B:C:D:E:F&gt; &lt;A:B:C:D:E:F&gt;/&lt;A:B:C:D:E:F&gt; cos &lt;0-7&gt;&lt;0-7&gt; ● &lt;config-mac-acl &gt;#sequence &lt;1-2147483647&gt;permit &lt;A:B:C:D:E:F&gt;/&lt;A:B:C:D:E:F&gt; &lt;A:B:C:D:E:F&gt;/&lt;A:B:C:D:E:F&gt; cos &lt;0-7&gt;&lt;0-7&gt; ethtype &lt;0x0600-0xFFFF&gt; ● &lt;config-mac-acl &gt;#sequence &lt;1-2147483647&gt;permit &lt;A:B:C:D:E:F&gt;/&lt;A:B:C:D:E:F&gt; &lt;A:B:C:D:E:F&gt;/&lt;A:B:C:D:E:F&gt; ethtype &lt;0x0600-0xFFFF&gt; ● &lt;config-mac-acl &gt;#sequence &lt;1-2147483647&gt;permit &lt;A:B:C:D:E:F&gt;/&lt;A:B:C:D:E:F&gt; &lt;A:B:C:D:E:F&gt;/&lt;A:B:C:D:E:F&gt; vlan &lt;1-4094&gt; ● &lt;config-mac-acl &gt;#sequence &lt;1-2147483647&gt;permit &lt;A:B:C:D:E:F&gt;/&lt;A:B:C:D:E:F&gt; &lt;A:B:C:D:E:F&gt;/&lt;A:B:C:D:E:F&gt; vlan &lt;1-4094&gt; cos &lt;0-7&gt;&lt;0-7&gt; ● &lt;config-mac-acl &gt;#sequence &lt;1-2147483647&gt;permit &lt;A:B:C:D:E:F&gt;/&lt;A:B:C:D:E:F&gt; &lt;A:B:C:D:E:F&gt;/&lt;A:B:C:D:E:F&gt; vlan &lt;1-4094&gt; cos &lt;0-7&gt;&lt;0-7&gt; ethtype &lt;0x0600-0xFFFF&gt; ● &lt;config-mac-acl &gt;#sequence &lt;1-2147483647&gt;permit &lt;A:B:C:D:E:F&gt;/&lt;A:B:C:D:E:F&gt; &lt;A:B:C:D:E:F&gt;/&lt;A:B:C:D:E:F&gt; vlan &lt;1-4094&gt; ethtype &lt;0x0600-0xFFFF&gt; ● &lt;config-mac-acl &gt;#sequence &lt;1-2147483647&gt;permit any &lt;A:B:C:D:E:F&gt;/&lt;A:B:C:D:E:F&gt; cos &lt;0-7&gt;&lt;0-7&gt; ● &lt;config-mac-acl &gt;#sequence &lt;1-2147483647&gt;permit any &lt;A:B:C:D:E:F&gt;/&lt;A:B:C:D:E:F&gt; cos &lt;0-7&gt;&lt;0-7&gt; ethtype &lt;0x0600-0xFFFF&gt; ● &lt;config-mac-acl &gt;#sequence &lt;1-2147483647&gt;permit any &lt;A:B:C:D:E:F&gt;/&lt;A:B:C:D:E:F&gt; vlan &lt;1-4094&gt; ● &lt;config-mac-acl &gt;#sequence &lt;1-2147483647&gt;permit any &lt;A:B:C:D:E:F&gt;/&lt;A:B:C:D:E:F&gt; vlan &lt;1-4094&gt; cos &lt;0-7&gt;&lt;0-7&gt; ● &lt;config-mac-acl &gt;#sequence &lt;1-2147483647&gt;permit any &lt;A:B:C:D:E:F&gt;/&lt;A:B:C:D:E:F&gt; vlan &lt;1-4094&gt; cos &lt;0-7&gt;&lt;0-7&gt; ethtype &lt;0x0600-0xFFFF&gt; ● &lt;config-mac-acl &gt;#sequence &lt;1-2147483647&gt;permit any &lt;A:B:C:D:E:F&gt;/&lt;A:B:C:D:E:F&gt; vlan &lt;1-4094&gt; ethtype &lt;0x0600-0xFFFF&gt; ● &lt;config-mac-acl &gt;#sequence &lt;1-2147483647&gt;permit any any cos &lt;0-7&gt;&lt;0-7&gt; ● &lt;config-mac-acl &gt;#sequence &lt;1-2147483647&gt;permit any any cos &lt;0-7&gt;&lt;0-7&gt; ethtype &lt;0x0600-0xFFFF&gt; ● &lt;config-mac-acl &gt;#sequence &lt;1-2147483647&gt;permit any any ethtype &lt;0x0600-0xFFFF&gt; ● &lt;config-mac-acl &gt;#sequence &lt;1-2147483647&gt;permit any any vlan &lt;1-4094&gt; ● &lt;config-mac-acl &gt;#sequence &lt;1-2147483647&gt;permit any any vlan &lt;1-4094&gt; cos &lt;0-7&gt;&lt;0-7&gt; ● &lt;config-mac-acl &gt;#sequence &lt;1-2147483647&gt;permit any any vlan &lt;1-4094&gt; cos &lt;0-7&gt;&lt;0-7&gt; ethtype &lt;0x0600-0xFFFF&gt; ● &lt;config-mac-acl &gt;#sequence &lt;1-2147483647&gt;permit any any vlan &lt;1-4094&gt; ethtype &lt;0x0600-0xFFFF&gt; </pre> |
| <pre> mac address-table aging-time &lt;10-630&gt; </pre> | <pre> Set the aging time for an entry remains in the MAC address table. address-table static - Add a static address to the MAC address table to drop the packets with the specified source or destination MAC </pre>  |

|  |  |
|--|--|
|  | <p>address.</p> <p>&lt;10-630&gt; - Unit is second. Default is 300.</p> <p>static &lt;A:B:C:D:E:F&gt; - Enter the MAC address.</p> <p>vlan &lt;1-4094&gt; - Specify the VLAN ID of the packet.</p> <p>gigabitEthernet &lt;1-50&gt; - Specify a physical port.</p> <p>LAG &lt;1-8&gt; - Specify a LAG port.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# mac address-table aging-time &lt;10-630&gt;</li> <li>● &lt;config&gt;# mac address-table static &lt;A:B:C:D:E:F&gt; vlan &lt;1-4094&gt; drop</li> <li>● &lt;config&gt;# mac address-table static &lt;A:B:C:D:E:F&gt; vlan &lt;1-4094&gt; interfaces GigabitEthernet &lt;1-50&gt;</li> <li>● &lt;config&gt;# mac address-table static &lt;A:B:C:D:E:F&gt; vlan &lt;1-4094&gt; interfaces LAG &lt;1-8&gt;</li> </ul> |
|--|--|

## Example

```
G2500# configure
G2500(config)# mac acl test_CA
G2500(config-mac-acl)# deny 00:50:00:7f:12:11/00:00:00:00:10:20
00:50:00:aa:bb:cc/00:00:00:00:12:00 cos 3 2 ethtype 0x0600
G2500(config-mac-acl)# deny any 00:50:00:7f:12:11/00:00:00:00:10:20 cos 5 6
ethtype 0x0600
G2500(config-mac-acl)# deny any
G2500(config)# mac address-table static 00:50:07:12:ff:aa vlan 300 drop
```

## Telnet Command: mail alert

Use this command to configure mail alert for various conditions.

### Syntax Items

mailalert active  
 mailalert auth  
 mailalert devicecheck  
 mailalert encry  
 mailalert hwmon  
 mailalert interval  
 mailalert ipconfilict  
 mailalert password  
 mailalert poestatus  
 mailalert port  
 mailalert portlink  
 mailalert portspeed  
 mailalert receiver  
 mailalert sender  
 mailalert server  
 mailalert sysrestart  
 mailalert throughputcheck  
 mailalert username

### Description

| Syntax Items            | Description  |
|-------------------------|--|
| <i>mailalert active</i> | <disable/enable> - Enable or disable the function of mail alert.<br><b>Related Syntax:</b> <ul style="list-style-type: none"> <li>● &lt;config&gt;# mailalert active &lt;disable/enable&gt;</li> </ul> |
| <i>mailalert auth</i>   | <disable/enable> - Enable or disable the function of SMTP server   |

|                              |   |
|------------------------------|---|
|                              | <p>authentication.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# mailalert auth &lt;disable/enable&gt;</li> </ul>  |
| <i>mailalert devicecheck</i> | <p>&lt;disable/enable&gt; - Enable or disable the function of sending a mail alert when encountering a device check error.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# mailalert devicecheck &lt;disable/enable&gt;</li> </ul> |
| <i>mailalert encry</i>       | <p>Specify the encryption type for mail alert.</p> <p>&lt;disable/sslts/starttls&gt; -</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# mailalert encry &lt;disable/sslts/starttls&gt;</li> </ul>                                   |
| <i>mailalert hwmon</i>       | <p>Send a mail alert when hardware monitor error.</p> <p>&lt;disable/enable&gt; - Enable or disable the function.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# mailalert hwmon &lt;disable/enable&gt;</li> </ul>                |
| <i>mailalert interval</i>    | <p>Set the transmission interval for the mail alert.</p> <p>&lt;1-60&gt; - Unit is second.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# mailalert interval &lt;1-60&gt;</li> </ul>  |
| <i>mailalert ipconflict</i>  | <p>&lt;disable/enable&gt; - Enable or disable the function of sending a mail alert if encountering the IP conflict.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# mailalert ipconflict &lt;disable/enable&gt;</li> </ul>         |
| <i>mailalert password</i>    | <p>&lt;PASSWORD&gt; - Enter the password for SMTP server authentication.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# mailalert password &lt;PASSWORD&gt;</li> </ul>  |
| <i>mailalert poestatus</i>   | <p>&lt;disable/enable&gt; - Enable or disable the function of sending a mail alert when PoE status is changed.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# mailalert poestatus &lt;disable/enable&gt;</li> </ul>               |
| <i>mailalert port</i>        | <p>&lt;0-65535&gt;- Enter a port number.</p> <p><b>Related Syntax:</b></p> <p>&lt;config&gt;# mailalert port &lt;0-65535&gt;</p>  |
| <i>mailalert portlink</i>    | <p>&lt;disable/enable&gt; - Enable or disable the function of sending an alert when the port link status changes.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# mailalert portlink &lt;disable/enable&gt;</li> </ul>             |
| <i>mailalert portspeed</i>   | <p>&lt;disable/enable&gt; - Enable or disable the function of sending an alert when the port link speed changes.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# mailalert portspeed &lt;disable/enable&gt;</li> </ul>             |
| <i>mailalert receiver</i>    | <p>Specify an address for receiving the alert mail.</p> <p>&lt;ADDRESS&gt; - Enter the email address of the receiver.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# mailalert receiver &lt;ADDRESS&gt;</li> </ul>                |
| <i>mailalert sender</i>      | <p>Specify an address which sends out the alert mail.</p> <p>&lt;ADDRESS&gt; - Enter the email address of the sender.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# mailalert sender &lt;ADDRESS&gt;</li> </ul>                  |
| <i>mailalert server</i>      | <p>Set the IP address of the server.</p>  |

|                                  |   |
|----------------------------------|---|
|                                  | <p>&lt;ADDRESS&gt; - Enter the IP address of the SMTP server.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# mailalert server &lt;ADDRESS&gt;</li> </ul>  |
| <i>mailalert sysrestart</i>      | <p>&lt;disable/enable&gt; - Enable or disable the function of sending a mail alert when the system restarts.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# mailalert sysrestart &lt;disable/enable&gt;</li> </ul>                    |
| <i>mailalert throughputcheck</i> | <p>&lt;disable/enable&gt; - Enable or disable the function of sending a mail alert when reaching the throughput threshold.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# mailalert throughputcheck &lt;disable/enable&gt;</li> </ul> |
| <i>mailalert username</i>        | <p>&lt;NAME&gt; - Enter the username authenticated by STMP server.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# mailalert username &lt;NAME&gt;</li> </ul>  |

## Example

```
G2500# configure
G2500(config)#
G2500(config)# mailalert receiver carrie_ni@draytek.com
```

## Telnet Command: management

Use this command to create a management access list and set configuration mode.

### Syntax Items

management access-list  
management access-class

### Description

| Syntax Items                  | Description  |
|-------------------------------|--|
| <i>management access-list</i> | <p>&lt;NAME&gt; - Enter the name of the access list.</p> <p>To configure detailed settings, enter the name of ACL to access into next level.</p> <p>&lt;config&gt;#management access-list &lt;NAME&gt;</p> <p>Then, available sub-commands are:</p> <p>&lt;config-macl&gt;#deny<br/>&lt;config-macl&gt;#do<br/>&lt;config-macl&gt;#end<br/>&lt;config-macl&gt;#exit<br/>&lt;config-macl&gt;#permit<br/>&lt;config-macl&gt;#sequence</p> <hr/> <p>Use the "deny" command to add deny rules for the management access list:</p> <p>GigabitEthernet &lt;1-50&gt; - Specify a physical port.<br/>LAG &lt;1-8&gt; - Specify a LAG port.<br/>service &lt;all/http/https/snmp/ssh/telnet&gt; - Specify the servcie type.<br/>ip &lt;A.B.C.D&gt;/&lt;A.B.C.D&gt; - Specify the source IP address with mask for the packets.<br/>ipv6 &lt;X::X::X::X&gt;/&lt;0-128&gt; - Specify the source IPv6 address and prefix length of the packet.</p> <p><b>Related Syntax:</b></p> |

- <config-macl>#deny interfaces GigabitEthernet <1-50> service <all/http/https/snmp/ssh/telnet>
- <config-macl>#deny interfaces LAG <1-8> service <all/http/https/snmp/ssh/telnet>
- <config-macl>#deny ip <A.B.C.D>/<A.B.C.D> interfaces GigabitEthernet <1-50> service <all/http/https/snmp/ssh/telnet>
- <config-macl>#deny ip <A.B.C.D>/<A.B.C.D> interfaces LAG <1-8> service <all/http/https/snmp/ssh/telnet>
- <config-macl>#deny ipv6 <X::X:X>/<0-128> interfaces GigabitEthernet <1-50> service <all/http/https/snmp/ssh/telnet>
- <config-macl>#deny ipv6 <X::X:X>/<0-128> interfaces LAG <1-8> service <all/http/https/snmp/ssh/telnet>

Use the “do” command to run execution command in current mode.  
<SEQUENCE> -

**Related Syntax:**

- <config-macl>#do <SEQUENCE>

Use the “end” command to finish current mode. Any changes in current mode will be saved.

**Related Syntax:**

- <config-macl>#end

Use the “exit” command to close the current CLI session or return to the previous mode without saving the settings.

**Related Syntax:**

- <config-macl>#exit

Use the “no sequence” command to delete any entry in management ACL.

<1-65535>- Specify an index number of the ACL.

**Related Syntax:**

- <config-macl>#no sequence <1-65535>

Use the “permit” command to add permit rules which bypass the packets meet the rule.

GigabitEthernet <1-50> - Specify a physical port.

LAG <1-8> - Specify a LAG port.

service <all/http/https/snmp/ssh/telnet> - Specify the service type.

ip <A.B.C.D>/<A.B.C.D> - Specify the source IP address with mask for the packets.

ipv6 <X::X:X>/<0-128> - Specify the source IPv6 address and prefix length of the packet.

**Related Syntax:**

- <config-macl>#permit interfaces GigabitEthernet <1-50> service <all/http/https/snmp/ssh/telnet>
- <config-macl>#permit interfaces LAG <1-8> service <all/http/https/snmp/ssh/telnet>
- <config-macl>#permit ip <A.B.C.D>/<A.B.C.D> interfaces GigabitEthernet <1-50> service <all/http/https/snmp/ssh/telnet>
- <config-macl>#permit ip <A.B.C.D>/<A.B.C.D> interfaces LAG <1-8> service <all/http/https/snmp/ssh/telnet>
- <config-macl>#permit ipv6 <X::X:X>/<0-128> interfaces GigabitEthernet <1-50> service <all/http/https/snmp/ssh/telnet>
- <config-macl>#permit ipv6 <X::X:X>/<0-128> interfaces

|                                       |   |
|---------------------------------------|---|
|                                       | <p>LAG &lt;1-8&gt; service &lt;all/http/https/snmp/ssh/telnet&gt;</p> <p>Use the “sequence” command to deny or permit the ACL.<br/>         &lt;1-65535&gt;- Specify an index number of the ACL.<br/>         GigabitEthernet &lt;1-50&gt; - Specify a physical port.<br/>         LAG &lt;1-8&gt; - Specify a LAG port.<br/>         service &lt;all/http/https/snmp/ssh/telnet&gt; - Specify the service type.<br/>         ip &lt;A.B.C.D&gt;/&lt;A.B.C.D&gt; - Specify the source IP address with mask for the packets.<br/>         ipv6 &lt;X:X::X:X&gt;/&lt;0-128&gt; - Specify the source IPv6 address and prefix length of the packet.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config-macl&gt;#sequence &lt;1-65535&gt;deny interfaces GigabitEthernet &lt;1-50&gt; service &lt;all/http/https/snmp/ssh/telnet&gt;</li> <li>● &lt;config-macl&gt;#sequence &lt;1-65535&gt;deny interfaces LAG &lt;1-8&gt; service &lt;all/http/https/snmp/ssh/telnet&gt;</li> <li>● &lt;config-macl&gt;#sequence &lt;1-65535&gt;deny ip &lt;A.B.C.D&gt;/&lt;A.B.C.D&gt; interfaces GigabitEthernet &lt;1-50&gt; service &lt;all/http/https/snmp/ssh/telnet&gt;</li> <li>● &lt;config-macl&gt;#sequence &lt;1-65535&gt;deny ip &lt;A.B.C.D&gt;/&lt;A.B.C.D&gt; interfaces LAG &lt;1-8&gt; service &lt;all/http/https/snmp/ssh/telnet&gt;</li> <li>● &lt;config-macl&gt;#sequence &lt;1-65535&gt;deny ipv6 &lt;X:X::X:X&gt;/&lt;0-128&gt; interfaces GigabitEthernet &lt;1-50&gt; service &lt;all/http/https/snmp/ssh/telnet&gt;</li> <li>● &lt;config-macl&gt;#sequence &lt;1-65535&gt;deny ipv6 &lt;X:X::X:X&gt;/&lt;0-128&gt; interfaces LAG &lt;1-8&gt; service &lt;all/http/https/snmp/ssh/telnet&gt;</li> <li>● &lt;config-macl&gt;#sequence &lt;1-65535&gt; permit interfaces GigabitEthernet &lt;1-50&gt; service &lt;all/http/https/snmp/ssh/telnet&gt;</li> <li>● &lt;config-macl&gt;#sequence &lt;1-65535&gt; permit interfaces LAG &lt;1-8&gt; service &lt;all/http/https/snmp/ssh/telnet&gt;</li> <li>● &lt;config-macl&gt;#sequence &lt;1-65535&gt; permit ip &lt;A.B.C.D&gt;/&lt;A.B.C.D&gt; interfaces GigabitEthernet &lt;1-50&gt; service &lt;all/http/https/snmp/ssh/telnet&gt;</li> <li>● &lt;config-macl&gt;#sequence &lt;1-65535&gt; permit ip &lt;A.B.C.D&gt;/&lt;A.B.C.D&gt; interfaces LAG &lt;1-8&gt; service &lt;all/http/https/snmp/ssh/telnet&gt;</li> <li>● &lt;config-macl&gt;#sequence &lt;1-65535&gt; permit ipv6 &lt;X:X::X:X&gt;/&lt;0-128&gt; interfaces GigabitEthernet &lt;1-50&gt; service &lt;all/http/https/snmp/ssh/telnet&gt;</li> <li>● &lt;config-macl&gt;#sequence &lt;1-65535&gt; permit &lt;X:X::X:X&gt;/&lt;0-128&gt; interfaces LAG &lt;1-8&gt; service &lt;all/http/https/snmp/ssh/telnet&gt;</li> </ul> |
| <p><i>management access-class</i></p> | <p>Specify an ACL as active access-list.<br/>         &lt;NAME&gt; - Enter the name of the access list.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# management access-class &lt;NAME&gt;</li> </ul>  |

## Example

```
P2500 # configure
G2500(config)#
G2500(config)# management access-list CA_ACL
P2500(config-macl)# deny ip 192.168.2.56/255.255.255.0 interfaces
gigabitethernet 3 service telnet
```

```
P2500(config-macl)#
P2500(config-macl)# deny ipv6 00:50::7f:3b/24
```

## Telnet Command: management-vlan

Use this command to set VLAN ID for management VLAN.

### Syntax Items

management-vlan vlan

### Description

| Syntax Items                | Description   |
|-----------------------------|---|
| <i>management-vlan vlan</i> | Set the management VLAN ID.<br><1-4094>- Specify the VLAN ID number of management VLAN.<br><b>Related Syntax:</b> <ul style="list-style-type: none"> <li>● &lt;config&gt;# management-vlan vlan &lt;1-4094&gt;</li> </ul> |

### Example

```
G2500# configure
G2500(config)#
G2500(config)# management-vlan vlan 200
VLAN 200: VLAN does not exist
G2500(config)#
```

## Telnet Command: mirror

Use this command to set the source / destination interface of a port mirror session.

### Syntax Items

mirror session

### Description

| Syntax Items          | Description  |
|-----------------------|--|
| <i>mirror session</i> | Set the destination interface of a port mirror session.<br><1-4> - Specify the mirror session ID number.<br>GigabitEthernet <1-50> - Specify a physical port.<br>allow-ingress - Enable the ingress traffic forwarding.<br><both/rx/tx> - Specify the mirror direction, TX only, RX only or TX and RX.<br><b>Related Syntax:</b> <ul style="list-style-type: none"> <li>● &lt;config&gt;# mirror session &lt;1-4&gt; destination interface GigabitEthernet &lt;1-50&gt; allow-ingress</li> <li>● &lt;config&gt;# mirror session &lt;1-4&gt; source interfaces GigabitEthernet &lt;1-50&gt; &lt;both/rx/tx&gt;</li> </ul> |

### Example

```
G2500# configure
G2500(config)#
G2500(config)# mirror session 3 destination interface GigabitEthernet 3 allow
G2500(config)#
G2500(config)# mirror session 3 source interfaces LAG 3 both
```



```
G2500(config)#
```

## Telnet Command: mvr

Use this command to enable MVR function and configure related settings.

### Syntax Items

```
mvr
mvr group
mvr mode
mvr query-time
mvr vlan
```

### Description

| Syntax Items          | Description   |
|-----------------------|---|
| <i>mvr</i>            | Enable MVR function.<br><b>Related Syntax:</b> <ul style="list-style-type: none"><li>● &lt;config&gt;# mvr</li></ul>  |
| <i>mvr group</i>      | Set MVR group address.<br><A.B.C.D> - Enter an IP address.<br><1-128> - Specify a number for contiguous series of IPv4 multicast address.<br><b>Related Syntax:</b> <ul style="list-style-type: none"><li>● &lt;config&gt;# mvr group &lt;A.B.C.D&gt;&lt;1-128&gt;</li></ul>  |
| <i>mvr mode</i>       | Set MVR mode as compatible or dynamic.<br><compatible> - The switch does not support IGMP dynamic joins on the source ports.<br><dynamic> - The switch supports MVR membership on the source ports.<br><b>Related Syntax:</b> <ul style="list-style-type: none"><li>● &lt;config&gt;# mvr mode &lt;compatible/dynamic&gt;</li></ul> |
| <i>mvr query-time</i> | Set query response time for MVR.<br><1-10> - Specify the response time (second).<br><b>Related Syntax:</b> <ul style="list-style-type: none"><li>● &lt;config&gt;# mvr query-time &lt;1-10&gt;</li></ul>  |
| <i>mvr vlan</i>       | Set a VLAN ID for MVR.<br><1-4094> - Specify the existed static VLAN ID.<br><b>Related Syntax:</b> <ul style="list-style-type: none"><li>● &lt;config&gt;# mvr vlan &lt;1-4094&gt;</li></ul>  |

### Example

```
G2500# configure
G2500(config)#
G2500(config)# mvr group 192.168.2.33
The operation will delete the MVR VLAN groups include static MVR groups.Continue
? [yes/no]:y
Input Parameter Error
G2500(config)#
```

## Telnet Command: no

Use this command to disable specific command.

### Syntax Items

no <command>

### Example

```
G2500# configure
G2500(config)#
G2500(config)# no port-security
G2500(config)#
```

## Telnet Command: openvpn

Use this command to enable/disable the OpenVPN tunnel.

### Syntax Items

openvpn enable

openvpn disable

openvpn filename

### Description

| Syntax Items    | Description  |
|-----------------|--|
| <i>enable</i>   | Enable the OpenVPN tunnel.   |
| <i>disable</i>  | Disable the OpenVPN tunnel.  |
| <i>filename</i> | <NAME> - Define a name for OpenVPN configuration.<br>Related Syntax: <ul style="list-style-type: none"><li>● &lt;config&gt;# openvpn filename &lt;NAME&gt;</li></ul> |

### Example

```
G2500# configure
G2500(config)#
G2500(config)#
```

## Telnet Command: port-security

Use this command to enable the function of port security.

### Syntax Items

port-security

### Example

```
G2500# configure
G2500(config)#
G2500(config)# port-security
G2500(config)#
```

## Telnet Command: qos

Use this command to configure QoS settings.

### Syntax Items

qos  
qos map  
qos queue  
qos trust

### Description

| Syntax Items     | Description   |
|------------------|---|
| <i>qos</i>       | Enable the quality of service based on basic trust type to assign the queue for packets.<br><b>Related Syntax:</b> <ul style="list-style-type: none"><li>● &lt;config&gt;# qos</li></ul>  |
| <i>qos map</i>   | map cos-queue - Set the CoS to queue map.<br>map dscp-queue - Set the DSCP to queue map.<br>map precedence-queue - Set the IP Precedence to queue map.<br>map queue-cos - Modify the queue to CoS map.<br>map queue-dscp - Modify the queue to DSCP map.<br>map queue-precedence - Modify the queue to IP precedence map.<br><1-8> - Specify the queue number for the following CoS values mapped.<br><1-8> - Specify the queue number to which the DSCP value shall correspond.<br><1-8> - Specify the queue number to which the IP precedence value shall correspond.<br><0-7> - Enter the cos value to which the queue ID shall correspond.<br><0-7> - Enter the DSCP value to which the queue ID shall correspond.<br><0-7> - Enter the IP precedence value to which the queue ID shall correspond.<br><b>Related Syntax:</b> <ul style="list-style-type: none"><li>● &lt;config&gt;# qos map cos-queue SEQUENCE to &lt;1-8&gt;</li><li>● &lt;config&gt;# qos map dscp-queue SEQUENCE to &lt;1-8&gt;</li><li>● &lt;config&gt;# qos map precedence-queue SEQUENCE to &lt;1-8&gt;</li><li>● &lt;config&gt;# qos map queue-cos SEQUENCE to &lt;0-7&gt;</li><li>● &lt;config&gt;# qos map queue-dscp SEQUENCE to &lt;0-7&gt;</li><li>● &lt;config&gt;# qos map queue-precedence SEQUENCE to &lt;0-7&gt;</li></ul> |
| <i>qos queue</i> | queue strict-priority-num - Set the number of strict priority queue.<br>queue weight SEQUENCE - Set the number of non-strict priority queue.<br><0-8> - Specify the queue number.<br><weight1-weight8> <1-127> - Specify a number (1-127) representing queue weight value.<br><b>Related Syntax:</b> <ul style="list-style-type: none"><li>● &lt;config&gt;# qos queue strict-priority-num &lt;0-8&gt;</li><li>● &lt;config&gt;# qos queue weight SEQUENCE &lt;weight1 - weight8&gt; &lt;1-127&gt;</li></ul>  |
| <i>qos trust</i> | Set the trust type, cos, for the device to judge the appropriate queue of the packets.  |

|  |   |
|--|---|
|  | <b>Related Syntax:</b> <ul style="list-style-type: none"> <li>● &lt;config&gt;# qos trust &lt;cos/cos-dscp/ dscp/ip-precedence&gt;</li> </ul> |
|--|---|

## Example

```
G2500# configure
G2500(config)#
G2500(config)# qos map cos-queue SEQUENCE to 3
G2500(config)#
```

## Telnet Command: radius

Use this command to configure settings for RADIUS server.

### Syntax Items

radius default-config

radius host

### Description

| Syntax Items                 | Description   |
|------------------------------|---|
| <i>radius default-config</i> | <p>Key &lt;RADIUSKEY&gt; - Specify key string for RADIUS server.</p> <p>Retransmit &lt;1-10&gt; - Specify the retransmit times (from 1 to 10) for RADIUS server.</p> <p>Timeout &lt;1-30&gt; - Specify the time out value (from 1 to 30) for RADIUS server.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# radius default-config key &lt;RADIUSKEY&gt;</li> <li>● &lt;config&gt;# radius default-config key &lt;RADIUSKEY&gt; retransmit &lt;1-10&gt;</li> <li>● &lt;config&gt;# radius default-config key &lt;RADIUSKEY&gt; retransmit &lt;1-10&gt; timeout &lt;1-30&gt;</li> <li>● &lt;config&gt;# radius default-config retransmit &lt;1-10&gt;</li> <li>● &lt;config&gt;# radius default-config retransmit &lt;1-10&gt; timeout &lt;1-30&gt;</li> <li>● &lt;config&gt;# radius default-config timeout &lt;1-30&gt;</li> </ul>   |
| <i>radius host</i>           | <p>host &lt;HOSTNAME&gt; - Specify a domain name or IP address for RADIUS server host.</p> <p>auth-port &lt;0-65535&gt; - Speicfy a UDP port number for RADIUS server.</p> <p>key &lt;RADIUSKEY&gt; - Specify key string for RADIUS server.</p> <p>priority &lt;0-65535&gt; - Specify the priority for RADIUS server.</p> <p>retransmit &lt;1-10&gt; - Specify the retransmit times (from 1 to 10) for RADIUS server.</p> <p>timeout &lt;1-30&gt; - Specify the time out value (from 1 to 30) for RADIUS server.</p> <p>type &lt;802.1x / all / login&gt; - Choose the usage type for 802.1X authentication, or login, or both 802.1X authentication and login of RADIUS type.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# radius host &lt;HOSTNAME&gt; auth-port &lt;0-65535&gt;</li> <li>● &lt;config&gt;# radius host &lt;HOSTNAME&gt; auth-port &lt;0-65535&gt; key &lt;RADIUSKEY&gt;</li> <li>● &lt;config&gt;# radius host &lt;HOSTNAME&gt; auth-port &lt;0-65535&gt; key &lt;RADIUSKEY&gt; priority &lt;0-65535&gt;</li> <li>● &lt;config&gt;# radius host &lt;HOSTNAME&gt; auth-port &lt;0-65535&gt; key &lt;RADIUSKEY&gt; priority &lt;0-65535&gt; retransmit &lt;1-10&gt;</li> <li>● &lt;config&gt;# radius host &lt;HOSTNAME&gt; auth-port &lt;0-65535&gt; key &lt;RADIUSKEY&gt; priority &lt;0-65535&gt; retransmit &lt;1-10&gt; timeout &lt;1-30&gt; type &lt;802.1x / all / login&gt;</li> </ul> |

- <config># radius host <HOSTNAME> key <RADIUSKEY>
- <config># radius host <HOSTNAME> key <RADIUSKEY> priority <0-65535>
- <config># radius host <HOSTNAME> key <RADIUSKEY> priority <0-65535> retransmit <1-10>
- <config># radius host <HOSTNAME> key <RADIUSKEY> priority <0-65535> retransmit <1-10> timeout <1-30>
- <config># radius host <HOSTNAME> key <RADIUSKEY> priority <0-65535> retransmit <1-10> timeout <1-30> type <802.1x / all / login>
- <config># radius host <HOSTNAME> priority <0-65535>
- <config># radius host <HOSTNAME> priority <0-65535> retransmit <1-10>
- <config># radius host <HOSTNAME> priority <0-65535> retransmit <1-10> timeout <1-30>
- <config># radius host <HOSTNAME> priority <0-65535> retransmit <1-10> timeout <1-30> type <802.1x / all / login>
- <config># radius host <HOSTNAME> retransmit <1-10>
- <config># radius host <HOSTNAME> retransmit <1-10> timeout <1-30>
- <config># radius host <HOSTNAME> retransmit <1-10> timeout <1-30> type <802.1x / all / login>
- <config># radius host <HOSTNAME> timeout <1-30>
- <config># radius host <HOSTNAME> timeout <1-30> type <802.1x / all / login>
- <config># radius host <HOSTNAME> type <802.1x / all / login>

## Example

```
G2500# configure
G2500(config)#
G2500(config)# radius default-config key 123456789 retransmit 3 timeout 10
G2500(config)# radius host radius auth-port 3000
```

## Telnet Command: schedule

Use this command to set schedule.

## Syntax Items

schedule index

## Description

| Syntax Items          | Description  |
|-----------------------|--|
| <i>schedule index</i> | <p>Specify an index number for configuring detailed settings of a schedule profile.</p> <p>&lt;1-15&gt; - Enter a number to select a schedule profile.</p> <p>&lt;DESCRIPTION&gt; - Give a brief description for such profile.</p> <p>cycle-days - The action applied with the schedule will take place every few days.</p> <p>monthly-date - The action applied with the schedule will take place in specified day within a month.</p> <p>once - The action applied with the schedule will take place for one time.</p> <p>weekdays - The action applied with the schedule will take place on a certain day within a week.</p> <p>&lt;1-31&gt; - Enter a number to make action repeat.</p> <p>&lt;apr / aug / dec / feb /jan / jul / jun /jul / mar / may / nov / oct / sep &gt; - Represent month of April, August, December, February, January, July, June, March, May, November, October, and September.</p> |

|  |   |
|--|---|
|  | <p>&lt;sun /mon /tue /wed / thu / fri / sat&gt; - Represent Sunday, Monday, Tuesday, Wednesday, Thursday, Friday and Saturday.</p> <p>&lt;1-31&gt; - Enter a number as the start date within a month.</p> <p>&lt;2000-2035&gt; - Enter the number as the year of start date.</p> <p>&lt;HH:MM&gt; - Enter the hours and the minutes.</p> <p>&lt;on/off&gt; - Enable (on) or disable (off) the action applied with such profile.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# schedule index &lt;1-15&gt; description &lt;DESCRIPTION&gt;</li> <li>● &lt;config&gt;# schedule index &lt;1-15&gt; how-often cycle-days &lt;1-31&gt; start-date &lt;apr / aug / dec / feb /jan / jul / jun / mar / may / nov / oct / sep &gt; &lt;1-31&gt; &lt;2000-2035&gt; start-time &lt;HH:MM&gt; duration &lt;HH:MM&gt; action &lt;on/off&gt;</li> <li>● &lt;config&gt;# schedule index &lt;1-15&gt; how-often monthly-date &lt;1-31&gt; start-date &lt;apr / aug / dec / feb /jan / jul / jun / mar / may / nov / oct / sep &gt; &lt;1-31&gt; &lt;2000-2035&gt; start-time &lt;HH:MM&gt; duration &lt;HH:MM&gt; action &lt;on/off&gt;</li> <li>● &lt;config&gt;# schedule index &lt;1-15&gt; how-often once start-date&lt;apr / aug / dec / feb /jan / jul / jun / mar / may / nov / oct / sep &gt; &lt;1-31&gt; &lt;2000-2035&gt; start-time &lt;HH:MM&gt; duration &lt;HH:MM&gt; action &lt;on/off&gt;</li> <li>● &lt;config&gt;# schedule index &lt;1-15&gt; how-often weekdays &lt;sun /mon /tue /wed / thu / fri / sat&gt; start-date &lt;apr / aug / dec / feb /jan / jul / jun / mar / may / nov / oct / sep &gt; &lt;1-31&gt; &lt;2000-2035&gt; start-time &lt;HH:MM&gt; duration &lt;HH:MM&gt; action &lt;on/off&gt;</li> </ul> |
|--|---|

## Example

```
G2500# configure
G2500(config)#
G2500(config)# schedule index 1 how-often cycle-days 3 start-date jan 1 2019
start-time 08:01 duration 17:30 action on
G2500(config)# schedule index 2 how-often weekdays sun start-date may 11 2019
start-time 02:10 duration 12:10 action on
G2500(config)#
```

## Telnet Command: snmp

Use this command to define SNMP community.

### Syntax Items

```
snmp community
snmp engineid
snmp group
snmp host
snmp trap
snmp user
snmp view
```

### Description

| Syntax Items          | Description  |
|-----------------------|--|
| <i>snmp community</i> | <p>snmp community - Set community name for SNMP v1 and v2, and access group name.</p> <p>Available parameters for SNMP community:</p> <p>&lt;NAME&gt; after community - Enter a string (maximum length: 20 characters) as community name.</p> <p>&lt;NAME&gt; after group - Enter a string (maximum length: 30</p> |

|                      |  |
|----------------------|--|
|                      | <p>characters) as access group.</p> <p>ro - Set the community as read only.</p> <p>rw - Set the community as read and write.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# snmp community &lt;NAME&gt; group &lt;NAME&gt;</li> <li>● &lt;config&gt;# snmp community &lt;NAME&gt; ro</li> <li>● &lt;config&gt;# snmp community &lt;NAME&gt; rw</li> <li>● &lt;config&gt;# snmp community &lt;NAME&gt; view &lt;NAME&gt; ro</li> <li>● &lt;config&gt;# snmp community &lt;NAME&gt; view &lt;NAME&gt; rw</li> </ul>  |
| <i>snmp engineid</i> | <p>snmp engineid - Set the remote host for SNMP engine.</p> <p>default - Reset to default setting of engine ID for SNMP server.</p> <p>&lt;ENGINEID&gt; - Such number must be 10 ~ 64 hexadecimal.</p> <p>&lt;A.B.C.D&gt; - Enter the IP address of the remote SNMP server.</p> <p>&lt;HOSTNAME&gt; - Enter the host name of the remote SNMP server.</p> <p>&lt;X:X::X:X&gt; - Enter the IPv6 address for remote SNMP server.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# snmp engineid &lt;ENGINEID&gt;</li> <li>● &lt;config&gt;# snmp engineid default</li> <li>● &lt;config&gt;# snmp engineid remote &lt;A.B.C.D&gt; &lt;ENGINEID&gt;</li> <li>● &lt;config&gt;# snmp engineid remote &lt;HOSTNAME&gt; &lt;ENGINEID&gt;</li> <li>● &lt;config&gt;# snmp engineid remote &lt;X:X::X:X&gt;&lt;ENGINEID&gt;</li> </ul>  |
| <i>snmp group</i>    | <p>snmp group - Set the SNMP group.</p> <p>&lt;NAME&gt; - Specify the name of SNMP group.</p> <p>version &lt;1/2c/3&gt; - Specify the version of SNMP service.</p> <p>&lt;auth/noauth/priv&gt; - Specify the packet authentication mode. "auth" means to perform packet authentication without encryption. It is applicable for SNMPv3 only. "noauth" means no packet authentication performed. "priv" means to perform packet authentication with encryption and also it is applicable for SNMPv3 only.</p> <p>read-view &lt;NAME&gt; - Set the view name to enable agent configuration.</p> <p>notify-view &lt;NAME&gt; - Set the view name to send only trap included in SNMP view for notification.</p> <p>write-view &lt;NAME&gt; - Set the view name to enable viewing.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# snmp group &lt;NAME&gt; version &lt;1/2c/3&gt;<br/>  &lt;auth/noauth/priv&gt; read-view &lt;NAME&gt;</li> <li>● &lt;config&gt;# snmp group &lt;NAME&gt; version &lt;1/2c/3&gt;<br/>  &lt;auth/noauth/priv&gt; read-view &lt;NAME&gt; notify-view &lt;NAME&gt;</li> <li>● &lt;config&gt;# snmp group &lt;NAME&gt; version &lt;1/2c/3&gt;<br/>  &lt;auth/noauth/priv&gt; read-view &lt;NAME&gt; notify-view &lt;NAME&gt;<br/>  write-view &lt;NAME&gt;</li> </ul> |
| <i>snmp host</i>     | <p>snmp host - Set a host to receive SNMP notifications.</p> <p>&lt;A.B.C.D&gt; - Enter the IPv4/IPv6 address or host name of the receipt.</p> <p>version &lt;1/2c/3&gt; - Specify the version of SNMP service.</p> <p>&lt;NAME&gt; - Set the community name sent with the notification.</p> <p>udp-port &lt;1-65535&gt; - Set the UDP port number.</p> <p>timeout &lt;1-300&gt; - Set the timeout of V2c informs.</p> <p>retries &lt;1-255&gt; - Enter the retry counter of V2c informs.</p> <p><b>Related Syntax:</b></p> <p>Set a host to receive SNMP notifications.</p>   |

- <config># snmp host <A.B.C.D> <NAME> retries <1-255>
- <config># snmp host <A.B.C.D> <NAME> timeout <1-300> retries <1-255>
- <config># snmp host <A.B.C.D> <NAME> udp-port <1-65535> retries <1-255>
- <config># snmp host <A.B.C.D> <NAME> udp-port <1-65535> timeout <1-300>

Set a host to receive SNMP notifications. Notification type is informs.

- <config># snmp host <A.B.C.D> informs <NAME> retries <1-255>
- <config># snmp host <A.B.C.D> informs <NAME> timeout <1-300>
- <config># snmp host <A.B.C.D> informs <NAME> timeout <1-300> retries <1-255>
- <config># snmp host <A.B.C.D> informs <NAME> udp-port <1-65535>
- <config># snmp host <A.B.C.D> informs <NAME> udp-port <1-65535> retries <1-255>
- <config># snmp host <A.B.C.D> informs <NAME> udp-port <1-65535> timeout <1-300>
- <config># snmp host <A.B.C.D> informs <NAME> udp-port <1-65535> timeout <1-300> retries <1-255>
- <config># snmp host <A.B.C.D> informs version <1/2c/3>
- <config># snmp host <A.B.C.D> informs version <1/2c/3><NAME> retries <1-255>
- <config># snmp host <A.B.C.D> informs version <1/2c/3><NAME> timeout <1-300>
- <config># snmp host <A.B.C.D> informs version <1/2c/3><NAME> timeout <1-300> retries <1-255>
- <config># snmp host <A.B.C.D> informs version <1/2c/3><NAME> udp-port <1-65535>
- <config># snmp host <A.B.C.D> informs version <1/2c/3><NAME> udp-port <1-65535> retries <1-255>
- <config># snmp host <A.B.C.D> informs version <1/2c/3><NAME> udp-port <1-65535> timeout <1-300>
- <config># snmp host <A.B.C.D> informs version <1/2c/3><NAME> udp-port <1-65535> timeout <1-300> retries <1-255>

Set a host to receive SNMP notifications. Notification type is traps.

- <config># snmp host <A.B.C.D> traps <NAME>
- <config># snmp host <A.B.C.D> traps <NAME> retries <1-255>
- <config># snmp host <A.B.C.D> traps <NAME> timeout <1-300>
- <config># snmp host <A.B.C.D> traps <NAME> timeout <1-300> retries <1-255>
- <config># snmp host <A.B.C.D> traps version <1/2c/3><NAME> retries <1-255>
- <config># snmp host <A.B.C.D> traps version <1/2c/3><NAME> timeout <1-300> retries <1-255>
- <config># snmp host <A.B.C.D> traps version <1/2c/3><NAME> udp-port <1-65535>
- <config># snmp host <A.B.C.D> traps version <1/2c/3><NAME> udp-port <1-65535> retries <1-255>
- <config># snmp host <A.B.C.D> traps version <1/2c/3><NAME> udp-port <1-65535> timeout <1-300>
- <config># snmp host <A.B.C.D> traps version <1/2c/3><NAME> udp-port <1-65535> timeout <1-300> retries <1-255>
- <config># snmp host <A.B.C.D> version <1/2c/3><NAME>



|  |  |
|--|--|
|  | <p>retries &lt;1-255&gt;</p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# snmp host &lt;A.B.C.D&gt; version &lt;1/2c/3&gt;&lt;NAME&gt; timeout &lt;1-300&gt;</li> <li>● &lt;config&gt;# snmp host &lt;A.B.C.D&gt; version &lt;1/2c/3&gt;&lt;NAME&gt; timeout &lt;1-300&gt; retries &lt;1-255&gt;</li> <li>● &lt;config&gt;# snmp host &lt;A.B.C.D&gt; version &lt;1/2c/3&gt;&lt;NAME&gt; udp-port &lt;1-65535&gt;</li> <li>● &lt;config&gt;# snmp host &lt;A.B.C.D&gt; version &lt;1/2c/3&gt;&lt;NAME&gt; udp-port &lt;1-65535&gt; retries &lt;1-255&gt;</li> <li>● &lt;config&gt;# snmp host &lt;A.B.C.D&gt; version &lt;1/2c/3&gt;&lt;NAME&gt; udp-port &lt;1-65535&gt; timeout &lt;1-300&gt;</li> <li>● &lt;config&gt;#snmp host &lt;A.B.C.D&gt; version &lt;1/2c/3&gt;&lt;NAME&gt; udp-port &lt;1-65535&gt; timeout &lt;1-300&gt; retries &lt;1-255&gt;</li> </ul>   |
|  | <ul style="list-style-type: none"> <li>● &lt;config&gt;# snmp host HOSTNAME &lt;NAME&gt;</li> <li>● &lt;config&gt;# snmp host HOSTNAME &lt;NAME&gt; retries &lt;1-255&gt;</li> <li>● &lt;config&gt;# snmp host HOSTNAME &lt;NAME&gt; timeout &lt;1-300&gt;</li> <li>● &lt;config&gt;# snmp host HOSTNAME &lt;NAME&gt; timeout &lt;1-300&gt; retries &lt;1-255&gt;</li> <li>● &lt;config&gt;# snmp host HOSTNAME &lt;NAME&gt; udp-port &lt;1-65535&gt;</li> <li>● &lt;config&gt;# snmp host HOSTNAME &lt;NAME&gt; udp-port &lt;1-65535&gt; retries &lt;1-255&gt;</li> <li>● &lt;config&gt;# snmp host HOSTNAME &lt;NAME&gt; udp-port &lt;1-65535&gt; timeout &lt;1-300&gt;</li> <li>● &lt;config&gt;# snmp host HOSTNAME &lt;NAME&gt; udp-port &lt;1-65535&gt; timeout &lt;1-300&gt; retries &lt;1-255&gt;</li> </ul>   |
|  | <ul style="list-style-type: none"> <li>● &lt;config&gt;# snmp host HOSTNAME informs &lt;NAME&gt;</li> <li>● &lt;config&gt;# snmp host HOSTNAME informs &lt;NAME&gt; retries &lt;1-255&gt;</li> <li>● &lt;config&gt;# snmp host HOSTNAME informs &lt;NAME&gt; timeout &lt;1-300&gt;</li> <li>● &lt;config&gt;# snmp host HOSTNAME informs &lt;NAME&gt; retries &lt;1-255&gt; timeout &lt;1-300&gt; retries &lt;1-255&gt;</li> <li>● &lt;config&gt;# snmp host HOSTNAME informs &lt;NAME&gt; udp-port &lt;1-65535&gt;</li> <li>● &lt;config&gt;# snmp host HOSTNAME informs &lt;NAME&gt; udp-port &lt;1-65535&gt; retries &lt;1-255&gt;</li> <li>● &lt;config&gt;# snmp host HOSTNAME informs &lt;NAME&gt; udp-port &lt;1-65535&gt; timeout &lt;1-300&gt;</li> <li>● &lt;config&gt;# snmp host HOSTNAME informs &lt;NAME&gt; udp-port &lt;1-65535&gt; timeout &lt;1-300&gt; retries &lt;1-255&gt;</li> </ul>   |
|  | <ul style="list-style-type: none"> <li>● &lt;config&gt;# snmp host HOSTNAME traps &lt;NAME&gt;</li> <li>● &lt;config&gt;# snmp host HOSTNAME traps &lt;NAME&gt; retries &lt;1-255&gt;</li> <li>● &lt;config&gt;# snmp host HOSTNAME traps &lt;NAME&gt; timeout &lt;1-300&gt;</li> <li>● &lt;config&gt;# snmp host HOSTNAME traps &lt;NAME&gt; timeout &lt;1-300&gt; retries &lt;1-255&gt;</li> <li>● &lt;config&gt;# snmp host HOSTNAME traps &lt;NAME&gt; udp-port &lt;1-65535&gt;</li> <li>● &lt;config&gt;# snmp host HOSTNAME traps &lt;NAME&gt; udp-port &lt;1-65535&gt; retries &lt;1-255&gt;</li> <li>● &lt;config&gt;# snmp host HOSTNAME traps &lt;NAME&gt; udp-port &lt;1-65535&gt; timeout &lt;1-300&gt;</li> <li>● &lt;config&gt;# snmp host HOSTNAME traps &lt;NAME&gt; udp-port &lt;1-65535&gt; timeout &lt;1-300&gt; retries &lt;1-255&gt;</li> <li>● &lt;config&gt;# snmp host HOSTNAME traps version &lt;1/2c/3&gt; &lt;NAME&gt; retries &lt;1-255&gt;</li> <li>● &lt;config&gt;# snmp host HOSTNAME traps version &lt;1/2c/3&gt; &lt;NAME&gt; timeout &lt;1-300&gt;</li> <li>● &lt;config&gt;# snmp host HOSTNAME traps version &lt;1/2c/3&gt; &lt;NAME&gt; timeout &lt;1-300&gt; retries &lt;1-255&gt;</li> </ul> |



|                  |  |
|------------------|--|
|                  | <ul style="list-style-type: none"> <li>● &lt;config&gt;# snmp host &lt;X:X::X:X&gt; traps &lt;NAME&gt; udp-port &lt;1-65535&gt; timeout &lt;1-300&gt;</li> <li>● &lt;config&gt;# snmp host &lt;X:X::X:X&gt; traps &lt;NAME&gt; udp-port &lt;1-65535&gt; timeout &lt;1-300&gt; retries &lt;1-255&gt;</li> <li>● &lt;config&gt;# snmp host &lt;X:X::X:X&gt; version &lt;1/2c/3&gt; &lt;NAME&gt;</li> <li>● &lt;config&gt;# snmp host &lt;X:X::X:X&gt; version &lt;1/2c/3&gt; &lt;NAME&gt; retries &lt;1-255&gt;</li> <li>● &lt;config&gt;# snmp host &lt;X:X::X:X&gt; version &lt;1/2c/3&gt; &lt;NAME&gt; timeout &lt;1-300&gt;</li> <li>● &lt;config&gt;# snmp host &lt;X:X::X:X&gt; version &lt;1/2c/3&gt; &lt;NAME&gt; timeout &lt;1-300&gt; retries &lt;1-255&gt;</li> <li>● &lt;config&gt;# snmp host &lt;X:X::X:X&gt; version &lt;1/2c/3&gt; &lt;NAME&gt; udp-port &lt;1-65535&gt;</li> <li>● &lt;config&gt;# snmp host &lt;X:X::X:X&gt; version &lt;1/2c/3&gt; &lt;NAME&gt; udp-port &lt;1-65535&gt; retries &lt;1-255&gt;</li> <li>● &lt;config&gt;# snmp host &lt;X:X::X:X&gt; version &lt;1/2c/3&gt; &lt;NAME&gt; udp-port &lt;1-65535&gt; timeout &lt;1-300&gt;</li> <li>● &lt;config&gt;# snmp host &lt;X:X::X:X&gt; version &lt;1/2c/3&gt; &lt;NAME&gt; udp-port &lt;1-65535&gt; timeout &lt;1-300&gt; retries &lt;1-255&gt;</li> </ul> |
| <i>snmp trap</i> | <p>snmp trap - Send the SNMP traps.</p> <p>auth - Enable the SNMP authentication failure trap.</p> <p>cold-start - Enable the SNMP cold startup failure trap.</p> <p>linkUpDown - Enable the SNMP link up and down failure trap.</p> <p>wort-security - Enable the SNMP port security trap.</p> <p>Warm-start - Enable the SNMP warm startup failure trap.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# snmp trap &lt;auth / cold-start / linkUpDown / port-security / warm-start&gt;</li> </ul>   |
| <i>snmp user</i> | <p>snmp user - Set SNMP user account.</p> <p>&lt;username&gt; - Specify a name of SNMP user.</p> <p>&lt;groupName&gt; - Sepcify a name of SNMP group.</p> <p>auth &lt;md5/sha&gt; - Specify the authentication mode, md5 or sha.</p> <p>&lt;AUTHPASSWD&gt; - Enter the password for the md5/sha mode.</p> <p>Pri &lt;PRIVPASSWD&gt; - Enter a password as a privacy key.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# snmp user &lt;username&gt; &lt;groupName&gt;</li> <li>● &lt;config&gt;# snmp user &lt;username&gt; &lt;groupName&gt; auth &lt;md5/sha&gt; &lt;AUTHPASSWD&gt;</li> <li>● &lt;config&gt;# snmp user &lt;username&gt; &lt;groupName&gt; auth &lt;md5/sha&gt; &lt;AUTHPASSWD&gt; priv &lt;PRIVPASSWD&gt;</li> </ul>  |
| <i>snmp view</i> | <p>snmp view - Set the SNMP view.</p> <p>&lt;NAME&gt; - Enter the SNMP view name.</p> <p>Subtree &lt;OID&gt; - Specify the ASN.1 subtree object identifier (OID).</p> <p>oid-mask &lt;mask/all&gt; - Speicfy the OID mask, or use all for all masks.</p> <p>viewtype &lt;excluded/included&gt; - Let the selected MIBs include or exclude in the SNMP view.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# snmp view &lt;NAME&gt; subtree &lt;OID&gt; oid-mask &lt;mask&gt; viewtype &lt;excluded/included&gt;</li> </ul>  |

## Example

```
G2500# configure
G2500(config)#
```

```
G2500(config)# snmp engineid remote 192.168.2.38 00036D001188
G2500(config)# snmp engineid remote 00:50::16:88 00036D002288
G2500(config)# snmp host 192.168.2.89 CAR_community udp-port 1500 timeout 200
G2500(config)# snmp host 192.168.2.88 informs version 2c CAR_community
udp-port 3000 timeout 180 retries 35
G2500(config)# snmp host 192.168.2.88 traps version 2c CAR_traps udp-port 6500
timeout 60 retries 2
G2500(config)# snmp host 192.168.2.88 version 2c CAR_version udp-port 3000
timeout 60 retries 2
G2500(config)# snmp host HOSTNAME CAR_host udp-port 3000 timeout 60 retries
G2500(config)# snmp host HOSTNAME informs HA_informs udp-port 3000 timeout 60
retries 2
G2500(config)# snmp host HOSTNAME version 2c HT_verstion udp-port 3000 timeout
60 retries 2
G2500(config)# snmp user CA_user_1 CA_group_1 auth md5 CA12345678 priv
PR12345678
G2500(config)# snmp view CAR_community subtree 10 oid-mask 9 viewtype included
G2500(config)#
```

## Telnet Command: sntp

Use this command to configure settings for remote SNMP server.

### Syntax Items

snmp host

### Description

| Syntax Items     | Description  |
|------------------|--|
| <i>snmp host</i> | <p>Set the remote SNMP server by specifying IP address or hostname.<br/>           &lt;HOSTNAME&gt; - Enter the IP address or hostname of SNMP server.<br/>           &lt;1-65535&gt; - Specify the port number for the SNMP server.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# snmp host &lt;HOSTNAME&gt;</li> <li>● &lt;config&gt;# snmp host &lt;HOSTNAME&gt;&gt; port &lt;1-65535&gt;</li> </ul> |

### Example

```
G2500# configure
G2500(config)#
G2500(config)# snmp host KEY1245 port 3000
G2500(config)#
```

## Telnet Command: spanning-tree

Use this command to configure settings for spanning-tree.

### Syntax Items

spanning-tree  
spanning-tree bpdu  
spanning-tree forward-delay  
spanning-tree hello-time  
spanning-tree max-hops  
spanning-tree maximum-age  
spanning-tree mode

spanning-tree mst  
spanning-tree pathcost  
spanning-tree priority  
spanning-tree tx-hold-count

## Description

| Syntax Items                       | Description  |
|------------------------------------|--|
| <i>spanning-tree</i>               | Enable the function of spanning-tree.<br><br><b>Related Syntax:</b><br><ul style="list-style-type: none"> <li>● &lt;config&gt;# spanning-tree</li> </ul>   |
| <i>spanning-tree bpdu</i>          | Filter/flood the BPDU packets.<br><filtering> - Packets will be filtered when STP is disabled on specified interface.<br><flooding> - Packets will be flooded to all interfaces with STP disabled and flooding mode.<br><br><b>Related Syntax:</b><br><ul style="list-style-type: none"> <li>● &lt;config&gt;# spanning-tree bpdu&lt;filtering/flooding&gt;</li> </ul> |
| <i>spanning-tree forward-delay</i> | Set the STP forward delay time.<br><4-30> - Default value is 15 (seconds).<br><br><b>Related Syntax:</b><br><ul style="list-style-type: none"> <li>● &lt;config&gt;# spanning-tree forward-delay &lt;4-30&gt;</li> </ul>   |
| <i>spanning-tree hello-time</i>    | Set the hello time interval to broadcast the message to other bridges.<br><1-10> - Default value is 2 (seconds).<br><br><b>Related Syntax:</b><br><ul style="list-style-type: none"> <li>● &lt;config&gt;# spanning-tree hello-time &lt;1-10&gt;</li> </ul>  |
| <i>spanning-tree max-hops</i>      | Set the number of hops for BPDI packets to be forwarded in the MSTP region.<br><1-40> - Default value is 20 (seconds).<br><br><b>Related Syntax:</b><br><ul style="list-style-type: none"> <li>● &lt;config&gt;# spanning-tree max-hops &lt;1-40&gt;</li> </ul>  |
| <i>spanning-tree maximum-age</i>   | Set the time interval for VigorSwitch to wait without receiving the configuration message.<br><6-40> - Default value is 20 (seconds).<br><br><b>Related Syntax:</b><br><ul style="list-style-type: none"> <li>● &lt;config&gt;# spanning-tree maximum-age &lt;6-40&gt;</li> </ul>  |
| <i>spanning-tree mode</i>          | <mstp/rstp/stp> - Specify the operation mode for spanning tree, such as multiple spanning tree (MSTP), rapid spanning tree (RSTP) or spanning tree (STP).<br><br><b>Related Syntax:</b><br><ul style="list-style-type: none"> <li>● &lt;config&gt;# spanning-tree mode &lt;mstp/rstp/stp&gt;</li> </ul>  |
| <i>spanning-tree mst</i>           | <i>spanning-tree mst</i> - Configure port priority settings for MST.<br><0-15> - Specify the instance ID.<br><0-61440> - Set the priority for the specified instance ID.<br><br><b>Related Syntax:</b><br><ul style="list-style-type: none"> <li>● &lt;config&gt;# spanning-tree mst &lt;0-15&gt; priority &lt;0-61440&gt;</li> </ul>                                  |
|                                    | spanning-tree mst configuration - Access into the MSTP configuration mode. To configure detailed settings, access into next  |

|                                    |  |
|------------------------------------|--|
|                                    | <p>level.</p> <p>&lt;config&gt;# spanning-tree mst configuration</p> <p>&lt;config-mst&gt;#</p> <p>Then, available sub-commands are:</p> <p>&lt;config-mst&gt;#do</p> <p>&lt;config-mst&gt;# end</p> <p>&lt;config-mst&gt;# exit</p> <p>&lt;config-mst&gt;# instance</p> <p>&lt;config-mst&gt;# name</p> <p>&lt;config-mst&gt;# no</p> <p>&lt;config-mst&gt;# revision</p> <p>do &lt;SEQUENCE&gt; - Enter the action to be performed.</p> <p>end - End current mode.</p> <p>exit - Exit from current mode.</p> <p>instance &lt;0-15&gt; vlan &lt;1-4094&gt; - Specify the instance ID number and VLAN ID number.</p> <p>name &lt;NAME&gt; - Set a name of MST configuration.</p> <p>no - Set to default setting.</p> <p>revision &lt;0-65535&gt; - Set revision level.</p> |
| <i>spanning-tree pathcost</i>      | <p>Set the path-cost method for spanning tree.</p> <p>&lt;long/short&gt; - Long means the path cost ranging from 1 to 200000000; short means the path cost ranging from 1 to 65535.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# spanning-tree pathcost method &lt;long/short&gt;</li> </ul>   |
| <i>spanning-tree priority</i>      | <p>Set the priority for the specified instance ID.</p> <p>&lt;0-61440&gt; - The number must be multiple of 4096.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# spanning-tree priority &lt;0-61440&gt;</li> </ul>  |
| <i>spanning-tree tx-hold-count</i> | <p>Set the maximum number of packets transmission per second.</p> <p>&lt;1-10&gt; - Valid range is from 1 to 10.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# spanning-tree tx-hold-count &lt;1-10&gt;</li> </ul>  |

## Example

```
G2500# configure
G2500(config)#
G2500(config)# spanning-tree forward-delay 20
G2500(config)#
G2500(config)# spanning-tree maximum-age 38
G2500(config)#
G2500(config)# spanning-tree tx-hold-count 3
G2500(config)#
```

## Telnet Command: start-up

Use this command to restart ICP status after rebooting VigorSwitch.

### Syntax Items

start-up icp

### Description

| Syntax Items        | Description  |
|---------------------|--|
| <i>start-up icp</i> | <b>Related Syntax:</b> <ul style="list-style-type: none"> <li>● &lt;config&gt;# start-up icp enable</li> </ul> |

### Example

```
G2500# configure
G2500(config)#
G2500(config)# start-up icp enable
G2500(config)#
```

## Telnet Command: storm-control

Use this command to configure settings for Storm Control.

### Syntax Items

```
storm-control ifg exclude
storm-control ifg include
storm-control unit bps
storm-control unit pps
```

### Description

| Syntax Items                     | Description  |
|----------------------------------|--|
| <i>storm-control ifg exclude</i> | Exclude the preamble and IFG (inter frame gap) into the calculating.<br><br><b>Related Syntax:</b> <ul style="list-style-type: none"> <li>● &lt;config&gt;# storm-control ifg exclude</li> </ul>   |
| <i>storm-control ifg include</i> | Include the preamble and IFG (inter frame gap) into the calculating.<br><br><b>Related Syntax:</b> <ul style="list-style-type: none"> <li>● &lt;config&gt;# storm-control ifg include</li> </ul>   |
| <i>storm-control unit bps</i>    | Change the unit of calculating method for storm-control.<br>bps - Calculate the storm control rate by octet-based.<br><br><b>Related Syntax:</b> <ul style="list-style-type: none"> <li>● &lt;config&gt;# storm-control unit bps</li> </ul>  |
| <i>storm-control unit pps</i>    | Change the unit of calculating method for storm-control.<br>pps - Calculate the storm control rate by packet-based.<br><br><b>Related Syntax:</b> <ul style="list-style-type: none"> <li>● &lt;config&gt;# storm-control unit pps</li> </ul> |

### Example

```
G2500# configure
G2500(config)#
G2500(config)# storm-control ifg exclude
G2500(config)#
G2500(config)# storm-control unit bps
G2500(config)#
```

## Telnet Command: surveillance-vlan

Use this command to configure settings for surveillance-VLAN.

## Syntax Items

surveillance-vlan  
surveillance-vlan aging-time  
surveillance-vlan cos  
surveillance-vlan oui-table  
surveillance-vlan vlan

## Description

| Syntax Items                        | Description  |
|-------------------------------------|--|
| <i>surveillance-vlan</i>            | Enable the function of surveillance VLAN on VigorSwitch.<br><b>Related Syntax:</b> <ul style="list-style-type: none"><li>● &lt;config&gt;# surveillance-vlan</li></ul>   |
| <i>surveillance-vlan aging-time</i> | Set the aging time for surveillance VLAN.<br><30-65536> - Enter a value as aging time.<br><b>Related Syntax:</b> <ul style="list-style-type: none"><li>● &lt;config&gt;# surveillance-vlan aging-time &lt;30-65536&gt;</li></ul>   |
| <i>surveillance-vlan cos</i>        | Set the class of service (0~7) for surveillance VLAN.<br><0-7>- Enter a number.<br><b>Related Syntax:</b> <ul style="list-style-type: none"><li>● &lt;config&gt;# surveillance-vlan cos &lt;0-7&gt; remark</li></ul>   |
| <i>surveillance-vlan oui-table</i>  | Enable OUI surveillance VLAN configuration for specified interface.<br><A:B:C> - Enter the OUI address (e.g., 00:50:12).<br><DESCRIPTION> - Enter a string to briefly explain the surveillance VLAN.<br><b>Related Syntax:</b> <ul style="list-style-type: none"><li>● &lt;config&gt;# surveillance-vlan oui-table &lt;A:B:C&gt; &lt;DESCRIPTION&gt;</li></ul> |
| <i>surveillance-vlan vlan</i>       | Specify a VLAN profile as surveillance VLAN.<br><2-4094> - Specify the surveillance VLAN ID.<br><b>Related Syntax:</b> <ul style="list-style-type: none"><li>● &lt;config&gt;# surveillance-vlan vlan &lt;2-4094&gt;</li></ul>   |

## Example

```
G2500# configure
G2500(config)#
G2500(config)#
G2500(config)# surveillance-vlan aging-time 60
G2500(config)#
G2500(config)# surveillance-vlan oui-table 00:50:12 fortestonly
G2500(config)#
```

## Telnet Command: system

Use this command to modify the contact information of VigorSwitch.

## Syntax Items

system contact  
system location  
system name



## Description

| Syntax Items           | Description  |
|------------------------|--|
| <i>system contact</i>  | <p>&lt;CONTACT&gt; - Enter a string (maximum length: 256 characters).</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# system contact &lt;CONTACT&gt;</li> </ul>   |
| <i>system location</i> | <p>&lt;LOCATION&gt; - Specify the location of the host.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# system location &lt;LOCATION&gt;</li> </ul>               |
| <i>system name</i>     | <p>&lt;NAME&gt; - Change the name of the system. The default name is "P1280".</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# system name &lt;NAME&gt;</li> </ul> |

## Example

```
G2500# configure
G2500(config)#
G2500(config)# system contact callMIS
G2500(config)#
G2500(config)# system location DrayTek
G2500(config)# system name UPDATEFRIM
UPDATEFRIM(config)#
```

## Telnet Command: tacacs

Use this command to configure TACACS+ server.

### Syntax Items

tacacs default-config

tacacs host

### Description

| Syntax Items                 | Description  |
|------------------------------|--|
| <i>tacacs default-config</i> | <p>Set the default parameters for the TACACS+ server.</p> <p>Modify the default parameters of server key and timeout setting for the TACACS+ server.</p> <p>&lt;TACPLUSKEY&gt; - Enter a string as the TACACS+ server key.</p> <p>&lt;1-30&gt; - Enter a value as the TACACS+ server timeout.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# tacacs default-config</li> <li>● &lt;config&gt;# tacacs default-config key &lt;TACPLUSKEY&gt;</li> <li>● &lt;config&gt;# tacacs default-config key &lt;TACPLUSKEY&gt; timeout &lt;1-30&gt;</li> </ul> |
| <i>tacacs host</i>           | <p>Set host name for the TACACS+ server or set host name, server key and priority for the TACACS+ server.</p> <p>&lt;HOSTNAME&gt; - Enter the host name of the TACACS+ server.</p> <p>&lt;TACPLUSKEY&gt; - Enter a string as the TACACS+ server key.</p> <p>&lt;0-65535&gt; - Enter a value as server priority in server group.</p> <p>&lt;1-30&gt; - Enter a timeout setting.</p> <p><b>Related Syntax:</b></p>   |

- <config># tacacs host <HOSTNAME>
- <config># tacacs host <HOSTNAME> key <TACPLUSKEY>
- <config># tacacs host <HOSTNAME> key <TACPLUSKEY> priority <0-65535>
- <config># tacacs host <HOSTNAME> key <TACPLUSKEY> priority <0-65535> timeout <1-30>

## Example

```
G2500# configure
G2500(config)#
G2500(config)# tacacs default-config key tce00056 timeout 25
G2500(config)#
G2500(config)# tacacs host carrie02 key TA012345 priority 3000 timeout 10
G2500(config)#
```

## Telnet Command: tr069

Use this command to configure parameter settings of TR-069.

### Syntax Items

tr069 acsPwd  
tr069 acsUsername  
tr069 acsurl  
tr069 cpeEnable  
tr069 cpePwd  
tr069 cpeUsername  
tr069 cpeport  
tr069 healthlinkstatus  
tr069 healthpoewarning  
tr069 healthspeedstatus  
tr069 periodicInfo  
tr069 periodicTime Time  
tr069 ssl  
tr069 stun  
tr069 stunMAXkeepalive  
tr069 stunMINkeepalive  
tr069 stunaddr  
tr069 stunport

### Description

| Syntax Items             | Description   |
|--------------------------|---|
| <i>tr069 acsPwd</i>      | <PASSWORD> - Enter the password used for registering to VigorACS server.<br><br>Related Syntax:<br>● <config># tr069 acsPwd<PASSWORD> |
| <i>tr069 acsUsername</i> | <NAME> - Enter the username used for registering to VigorACS server.<br><br>Related Syntax:<br>● <config># tr069 acsUsername<NAME>    |
| <i>tr069 acsurl</i>      | <ADDRESS> - Enter the URL for VigorACS server.<br><br>Related Syntax:<br>● <config># tr069 acsurl <ADDRESS>                           |
| <i>tr069 cpeEnable</i>   | <disable/enable> - Enter Enable for VigorACS controlling such CPE   |

|                                |  |
|--------------------------------|--|
|                                | <p>through the Internet.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# tr069 cpeEnable &lt;disable/enable&gt;</li> </ul>  |
| <i>tr069 cpePwd</i>            | <p>&lt;PASSWORD&gt; - Enter the password that VigorACS server can use it to authenticate and control the CPE device.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# tr069 cpePwd &lt;PASSWORD&gt;</li> </ul>   |
| <i>tr069 cpeUsername</i>       | <p>&lt;NAME&gt; - Enter the username that VigorACS server can use it to authenticate and control the CPE device.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# tr069 cpeUsername &lt;NAME&gt;</li> </ul>  |
| <i>tr069 cpeport</i>           | <p>&lt;0-65535&gt; - Enter the port number for CPE.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# tr069 cpeport &lt;0-65535&gt;</li> </ul>  |
| <i>tr069 healthlinkstatus</i>  | <p>Perform the health check for the link status of specified interface(s).</p> <p>&lt;PORTLIST&gt; - Specify the interface, such as GE1, GE3-GE5 and so on.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# tr069 healthlinkstatus &lt;PORTLIST&gt;</li> </ul>    |
| <i>tr069 healthpoewarning</i>  | <p>Perform the health check for PoE port warning status.</p> <p>&lt;PORTLIST&gt; - Specify the interface, such as GE1, GE3-GE5 and so on.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# tr069 healthpoewarning &lt;PORTLIST&gt;</li> </ul>                      |
| <i>tr069 healthspeedstatus</i> | <p>Perform the health check for link speed status of specified interface(s).</p> <p>&lt;PORTLIST&gt; - Specify the interface, such as GE1, GE3-GE5 and so on.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# tr069 healthspeedstatus &lt;PORTLIST&gt;</li> </ul> |
| <i>tr069 periodicInfo</i>      | <p>&lt;disable/enable&gt; - Enter Enable to activate periodic information setting.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# tr069 periodicInfo &lt;disable/enable&gt;</li> </ul>   |
| <i>tr069 periodicTime TIME</i> | <p>Update the CPE information to VigorACS server.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# tr069 periodicTime TIME</li> </ul>  |
| <i>tr069 ssl</i>               | <p>&lt;disable/enable&gt; - Enter Enable to enable CPE management protocol with SSL.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# tr069 ssl &lt;disable/enable&gt;</li> </ul>  |
| <i>tr069 stun</i>              | <p>&lt;disable/enable&gt; - Enter Enable to enable CPE management protocol with STUN server.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# tr069 stun &lt;disable/enable&gt;</li> </ul>   |
| <i>tr069 stunMAXkeepalive</i>  | <p>Set the maximum time period for CPE to send the binding request to</p>  |

|                               |   |
|-------------------------------|---|
|                               | <p>VigorACS server.<br/>&lt;0-65535&gt; - Enter a number.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# tr069 stunMAXkeepalive &lt;0-65535&gt;</li> </ul>  |
| <i>tr069 stunMINkeepalive</i> | <p>Set the minimum time period for CPE to send the binding request to VigorACS server.<br/>&lt;0-65535&gt; - Enter a number.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# tr069 stunMINkeepalive &lt;0-65535&gt;</li> </ul> |
| <i>tr069 stunaddr</i>         | <p>&lt;ADDRESS&gt; - Enter the URL/IP address of STUN server.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# tr069 stunaddr &lt;ADDRESS&gt;</li> </ul>  |
| <i>tr069 stunport</i>         | <p>&lt;0-65535&gt; - Set the port number for STUN server.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# tr069 stunport &lt;0-65535&gt;</li> </ul>  |

### Example

```
G2500# configure
G2500(config)#
G2500(config)# tr069 stunaddr 192.168.3.99
G2500(config)#
```

### Telnet Command: uddl

Use this command to set the time interval of UniDirectional Link Detection (UDLD) sent message.

### Syntax Items

uddl

### Description

| Syntax Items             | Description   |
|--------------------------|---|
| <i>uddl message time</i> | <p>&lt;1-90&gt; - Specify a time interval for sending message.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# uddl message time &lt;1-90&gt;</li> </ul> |

### Example

```
G2500# configure
G2500(config)# uddl message time 35
G2500(config)#
```

### Telnet Command: username

Use this command to add a new user account or edit an existing user account.

### Syntax Items

username

### Description

| Syntax Items    | Description  |
|-----------------|--|
| <i>username</i> | <p>privilege - Set a user account with the privilege of admin, user or customized level.</p> <p>secret - Set a user account with unencrypted password.</p> <p>secret encrypted - Set a user account with encrypted password.</p> <p>&lt;WORD&gt; - Enter the name (0-32 characters) of the local user profile.</p> <p>&lt;admin/ user&gt; - Specify the privilege level to be admin (privilege 15) / user (privilege 1).</p> <p>&lt;PASSWORD&gt; - Enter a string as the password for the local user.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# username &lt;WORD&gt; privilege &lt;admin/user&gt; secret &lt;PASSWORD&gt;</li> <li>● &lt;config&gt;# username &lt;WORD&gt; secret &lt;PASSWORD&gt;</li> <li>● &lt;config&gt;# username &lt;WORD&gt; secret encrypted &lt;PASSWORD&gt;</li> </ul> |

### Example

```
G2500# configure
G2500(config)#
G2500(config)# username carrie_1 privilege admin secret md123456
G2500(config)#
G2500(config)# username carrie_1 secret encrypted ca123456
Old password: *****
G2500(config)#
```

### Telnet Command: vlan

Use this command to configure detailed settings for VLAN profile.

Before configuring, you have to access into next phase. See the following example:

```
G2500# configure
G2500(config)#
G2500(config)# vlan 3
G2500(config-vlan)#
```

### Syntax Items

vlan vlan-list  
vlan mac-vlan group  
vlan protocol-vlan group

### Description

| Syntax Items | Description  |
|--------------|--|
| <i>vlan</i>  | <p>Specify the index number of VLAN profile. To configure detailed settings, access into next level.</p> <p>&lt;vlan-list&gt; - The available range is 1 to 4094.</p> <p>&lt;config&gt;# vlan 33</p> <p>&lt;config-vlan&gt;#</p> <p>Then, available sub-commands are:</p> <p>&lt;config-vlan&gt;#do</p> <p>&lt;config-vlan&gt;#end</p> <p>&lt;config-vlan&gt;#exit</p> <p>&lt;config-vlan&gt;#name</p> |

|                                 |   |
|---------------------------------|---|
|                                 | <p>Use the “do” command to run execution command in current mode.<br/>&lt;SEQUENCE&gt; -</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config-vlan&gt;#do &lt;SEQUENCE&gt;</li> </ul>  |
|                                 | <p>Use the “end” command to finish current mode. Any changes in current mode will be saved.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config-vlan&gt;#end</li> </ul>   |
|                                 | <p>Use the “exit” command to close the current CLI session or return to the previous mode without saving the settings.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config-macl&gt;#exit</li> </ul>   |
|                                 | <p>Use the “name” command to add a VLAN profile.<br/>&lt;string&gt; - Enter the name of the VLAN profile.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config-vlan&gt;#name &lt;string&gt;</li> </ul>   |
| <i>vlan mac-vlan group</i>      | <p>Create a MAC-vlan group.<br/>&lt;1-2147483647&gt; - Specify a group ID.<br/>&lt;A:B:C:D:E:F&gt; - Enter the MAC address to be mapped.<br/>&lt;9-48&gt; - Enter a number representing the subnet mask.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# vlan mac-vlan group &lt;1-2147483647&gt; &lt;A:B:C:D:E:F&gt; mask &lt;9-48&gt;</li> </ul>   |
| <i>vlan protocol-vlan group</i> | <p>Create a protocol VLAN group with specified protocol type and value.<br/>&lt;1-8&gt; - Enter a number to specify a VLAN group.<br/>&lt;Ethernet_ii/ 11c_other/snap_1042&gt; - Specify a frame type by entering Ethernet_ii, 11c_other or snap_1042.<br/>&lt;value&gt; - Enter a value (0x0600-0xFFFE).</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"> <li>● &lt;config&gt;# vlan protocol-vlan group &lt;1-8&gt; frame-type &lt;Ethernet_ii/ 11c_other/snap_1042&gt; protocol-value &lt;value&gt;</li> </ul> |

## Example

```
G2500# configure
G2500(config)# vlan 3
G2500(config-vlan)#
G2500(config-vlan)# name vlan_friends
G2500(config-vlan)#
...
G2500(config)# vlan mac-vlan group 33 00:50:17:22:12:ff mask 10
G2500(config)# vlan group 1 frame-type ethernet_ii protocol-value 0x0600
G2500(config)#
```

## Telnet Command: voice-vlan

Use this command to enable voice VLAN and configure settings for voice VLAN.

### Syntax Items

voice-vlan aging-time  
voice-vlan cos  
voice-vlan oui-table

## voice-vlan vlan

### Description

| Syntax Items                 | Description  |
|------------------------------|--|
| <i>voice-vlan aging-time</i> | Set the voice VLAN aging timeout interval.<br><30-65536> - The unit is minute. Default is 1440 (minutes).<br><string> - Enter the name of the VLAN profile.<br><b>Related Syntax:</b> <ul style="list-style-type: none"><li>● &lt;config&gt;# voice-vlan aging-time &lt;30-65536&gt;</li></ul>   |
| <i>voice-vlan cos</i>        | Set the voice VLAN cos value and remark function.<br>Specify the class of service for voice VLAN.<br><0-7> - CoS value. Default is 6. Remark is disabled.<br>remark - L2 user priority is remarked with the CoS value.<br><b>Related Syntax:</b> <ul style="list-style-type: none"><li>● &lt;config&gt;# voice-vlan cos &lt;0-7&gt; remark</li></ul>                   |
| <i>voice-vlan oui-table</i>  | Add or remove the selected OUI to/from the OUI table. In default, there are 8 OUI addresses.<br><A:B:C> - Enter the OUI address.<br><DESCRIPTION> - Enter a brief description for the specified MAC address to the voice VLAN OUI table.<br><b>Related Syntax:</b> <ul style="list-style-type: none"><li>● &lt;config&gt;# voice-vlan cos &lt;0-7&gt; remark</li></ul> |
| <i>voice-vlan vlan</i>       | Set the VLAN identifier of the voice VLAN.<br><2-4094> - Enter the number of VLAN ID.<br><b>Related Syntax:</b> <ul style="list-style-type: none"><li>● &lt;config&gt;# voice-vlan vlan &lt;2-4094&gt;</li></ul>   |

### Example

```
G2500# configure
G2500(config)# voice-vlan aging-time 1000
G2500(config)#
G2500(config)# voice-vlan oui-table 22:30:ff test_01
G2500(config)#
G2500(config)# voice-vlan oui-table 00:01:E2 STAMP
G2500(config)# exit
G2500# show voice-vlan interfaces gigabitEthernet 1
Voice VLAN Aging      : 1000 minutes
Voice VLAN CoS        : 6
Voice VLAN lp Remark  : disabled
```

```
OUI table
  OUI MAC | Description
-----+-----
  00:E0:BB | 3COM
  00:03:6B | Cisco
  00:E0:75 | Veritel
  00:D0:1E | Pingtel
  00:01:E3 | Siemens
  00:60:B9 | NEC/Philips
  00:0F:E2 | H3C
  00:09:6E | Avaya
  22:30:FF | test_01
  00:01:E2 | STAMP
```

```
Port | State | Port Mode | Cos Mode
-----+-----+-----+-----
```

|        |          |      |     |
|--------|----------|------|-----|
| g11    | Disabled | Auto | Src |
| G2500# |          |      |     |



## Telnet Command: webhook

Use this command to enable or disable the webhook service.

### Syntax Items

webhook active

webhook host

webhook interval

webhook keep

### Description

| Syntax Items            | Description   |
|-------------------------|---|
| <i>webhook active</i>   | <p>&lt;enable/disable&gt; - Enable or disable the webhook application.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"><li>● &lt;config&gt;# webhook active &lt;enable/disable&gt;</li></ul>  |
| <i>webhook host</i>     | <p>Specify the destination (URL, domain name, IP address) to receive the data transferred by VigorSwitch.</p> <p>ip &lt;ADDRESS&gt; - Enter the IP address of the destination.</p> <p>path &lt;PATH&gt; - Enter the path string (part of the composition of the URL) of the destination.</p> <p>port &lt;number&gt; - Enter a port number.</p> <p>service &lt;http/https&gt; - Specify the protocol (http or https) of the destination.</p> <p>url &lt;domain name&gt; - Enter the domain name (e.g., draytek.com) of the destination. Note that it is not necessary to enter this information if IP address has been set first.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"><li>● &lt;config&gt;# webhook host ip &lt;ADDRESS&gt;</li><li>● &lt;config&gt;# webhook host path &lt;PATH&gt;</li><li>● &lt;config&gt;# webhook host port &lt;number&gt;</li><li>● &lt;config&gt;# webhook host service &lt;http/https&gt;</li><li>● &lt;config&gt;# webhook host url &lt;domain name&gt;</li></ul> |
| <i>webhook interval</i> | <p>&lt;1-60&gt; - Set the transmission interval (unit is minute).</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"><li>● &lt;config&gt;# webhook interval &lt;1-60&gt;</li></ul>   |
| <i>webhook keep</i>     | <p>settings &lt;enable/disable&gt; - Enable or disable the function of keep webhook settings.</p> <p><b>Related Syntax:</b></p> <ul style="list-style-type: none"><li>● &lt;config&gt;# webhook keep settings &lt;enable/disable&gt;</li></ul>  |

### Example

```
G2500# configure
G2500(config)# webhook host service https
G2500(config)# webhook host url www.demo.com
G2500(config)# webhook host path Draytek/demo
G2500(config)# webhook host port 443
G2500(config)# webhook interval 2
```

---

## X-2-4 Copy Configuration

Use this command to upgrade firmware image, configuration file, syslog file, language file and security certificate.

### Syntax Items

copy flash://

copy tftp://

copy backup-config

copy running-config

copy startup-config

### Description

| Syntax Items               | Description  |
|----------------------------|--|
| <i>copy flash://</i>       | <b>Related Syntax:</b> <ul style="list-style-type: none"><li>● # copy flash:// flash://</li><li>● # copy flash:// tftp://</li></ul>  |
| <i>copy running-config</i> | startup-config - Copy the running configuration file to startup configuration.<br>tftp://- Copy the running configuration file to remote TFTP server with a filename.<br><IP address> - Enter the IP address of TFTP sever.<br><filename> - Create a name to save the configuration file.<br><b>Related Syntax:</b> <ul style="list-style-type: none"><li>● # copy running-config backup-config</li><li>● # copy running-config startup-config</li><li>● # copy running-config tftp://</li></ul>     |
| <i>copy startup-config</i> | running-config - Copy the startup configuration file to the running configuration.<br>tftp://- Copy the startup configuration file to remote TFTP server with a filename.<br><IP address> - Enter the IP address of TFTP sever.<br><filename> - Create a name to save the configuration file.<br><b>Related Syntax:</b> <ul style="list-style-type: none"><li>● # copy startup-config backup-config</li><li>● # copy startup-config running-config</li><li>● # copy startup-config tftp://</li></ul> |
| <i>copy tftp://</i>        | Backup-config - Get the backup configuration from specified TFTP server.<br>running-config - Get the running configuration from specified TFTP server.<br>startup-config - Get the startup configuration from specified TFTP server.<br><b>Related Syntax:</b> <ul style="list-style-type: none"><li>● # copy tftp:// backup-config</li><li>● # copy tftp:// flash://</li><li>● # copy tftp:// running-config</li><li>● # copy tftp:// startup-config</li></ul>                                      |

- 
- # copy tftp:// tftp://
- 

## Example

```
G2500# copy running-config tftp://172.16.3.8/test_carrie.cfg
Uploading file. Please wait...
Save configuration done.
G2500# copy startup-config tftp://172.16.3.8/test_da.cfg
Uploading file. Please wait...
Save configuration done.
G2500#
```

---

## X-2-5 Delete Configuration

Use this command to delete a file from the FLASH file system or restore the factory default settings of VigorSwitch.

### Syntax Items

delete backup-config

delete flash:// startup-config

delete startup-config

delete system

### Description

| Syntax Items                         | Description   |
|--------------------------------------|---|
| <i>delete backup-config</i>          | Delete the backup configuration file in FLASH file system.<br><b>Related Syntax:</b> <ul style="list-style-type: none"><li>● # delete backup-config</li></ul>   |
| <i>delete flash://startup-config</i> | Delete the startup configuration file in FLASH file system.<br><b>Related Syntax:</b> <ul style="list-style-type: none"><li>● # delete flash://startup-config</li></ul>                               |
| <i>delete startup-config</i>         | Restore the factory default settings of VigorSwitch.<br><b>Related Syntax:</b> <ul style="list-style-type: none"><li>● # delete startup-config</li></ul>  |
| <i>delete system</i>                 | Delete the firmware image0/image1 stored in FLASH file system.<br><image0/image1> -<br><b>Related Syntax:</b> <ul style="list-style-type: none"><li>● # delete system &lt;image0/image1&gt;</li></ul> |

### Example

```
G2500# delet flash://startup-config
Delete flash://startup-config [y/n] y
Do you want to reload the system to take effect? [y/n] y
...
```

---

## X-2-6 Disable Configuration

All commands used will be divided into EXEC mode and Privileged EXEC mode. This command is to turn off privileged mode command.

Default privilege level is 15 if no privilege level is specified on enable command.

Default privilege level is 1 if no privilege level is specified on disable command.

### Syntax Items

disable

### Description

| Syntax Items | Description   |
|--------------|---|
| disable      | <1-14> - Enter a number to specify the privilege level.<br><br>Related Syntax: <ul style="list-style-type: none"><li>● # disable &lt;1-14&gt;</li></ul> |

### Example

```
G2500# disable ?
  <1-14> Privilege level
  <cr>
G2500# disable 3
G2500#
```

---

## X-2-7 End Configuration

Use this command to end current mode.

### Syntax Items

end

### Example

```
G2500(config)# interface GigabitEthernet 3
P2280x(config-if)# end
G2500#
```

---

## X-2-8 Exit Configuration

Use this command to close current CLI session or return to previous mode.

### Syntax Items

exit

### Example

```
G2500(config)# interface GigabitEthernet 3
P2280x(config-if)# exit
G2500(config)#
```

---

## X-2-9 Ping Configuration

Use this command to send ICMP ECHO\_REQUEST to network hosts.

### Syntax Items

ping

### Description

| Syntax Items | Description   |
|--------------|---|
| <i>ping</i>  | <HOSTNAME> - Enter an IPv4/IPv6 address or a domain name to ping.<br>count <1-999999999> - Specify the number of repetitions of ping operation.<br><br>Related Syntax:<br><ul style="list-style-type: none"><li>● # ping &lt;HOSTNAME&gt; count &lt;1-999999999&gt;</li></ul> |

### Example

```
G2500# ping 192.168.1.11 count 3
PING 192.168.1.11 (192.168.1.11): 56 data bytes
64 bytes from 192.168.1.11: icmp_seq=0 ttl=64 time=0.0 ms
64 bytes from 192.168.1.11: icmp_seq=1 ttl=64 time=0.0 ms
64 bytes from 192.168.1.11: icmp_seq=2 ttl=64 time=0.0 ms

--- 192.168.1.11 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
G2500#
```

---

## X-2-10 Reboot Configuration

Use this command to perform a cold restart of VigorSwitch.

### Syntax Items

reboot

### Example

```
G2500# reboot
G2500#
```

---

## X-2-11 Renew Configuration

Use this command to renew DHCP Snooping database from backup file.

### Syntax Items

renew ip dhcp snooping database

### Example

```
G2500# renew ip dhcp snooping database
G2500#
```

---

## X-2-12 Restore-defaults Configuration

Use this command to restore the factory default settings for the system or for the selected port.

### Syntax Items

restore-defaults

### Description

| Syntax Items            | Description  |
|-------------------------|--|
| <i>restore-defaults</i> | <1-50> - Enter the number (1 to 50) of LAN port.<br><1-8> - Enter the number of LAG port.<br><br>Related Syntax: <ul style="list-style-type: none"><li>● # restore-defaults</li><li>● # restore-defaults interfaces GigabitEthernet &lt;1-50&gt;</li><li>● # restore-defaults interfaces LAG &lt;1-8&gt;</li></ul> |

### Example

```
G2500# restore-defaults interfaces gigabitethernet 3
Interface gi3: restore factory defaults.
G2500#
G2500# restore-default
System: restore factory defaults. Do you want to reboot now? (y/n)y
```

---

## X-2-13 Save Configuration

Use this command to save configuration and activate the settings.

Note that this command has the same effect as "copy running-config startup-config".

### Syntax Items

save

### Example

```
G2500# save
Success
G2500#
```

---

## X-2-14 Show Configuration

After finished the command setting, use this command to display the configuration for all commands.

### Syntax Items

show <command>

### Example

```
G2500# show acl utilization
Type: sys                usage: 256
Type: IPSPG              usage: 128
Type: Auth               usage: 128
G2500#
G2500#
G2500# show arp
Address      HWtype  HWaddress      Flags Mask    Iface
192.168.1.55 ether   00:1D:AA:F0:26:08  C           eth0
192.168.1.10 ether   00:05:5D:E4:D8:EE  C           eth0
G2500# show voice-vlan interfaces gigabitethernet 3
Voice VLAN Aging      : 1440 minutes
Voice VLAN CoS        : 6
Voice VLAN lp Remark: disabled

OUI table
  OUI MAC  | Description
  -----+-----
  00:E0:BB  | 3COM
  00:03:6B  | Cisco
  00:E0:75  | Veritel
  00:D0:1E  | Pingtel
  00:01:E3  | Siemens
  00:60:B9  | NEC/Philips
```



```

00:0F:E2 | H3C
00:09:6E | Avaya

Port | State | Port Mode | Cos Mode
-----+-----+-----+-----
gi3 | Disabled | Auto | Src
G2500#

```

---

## X-2-15 SSL Configuration

Use this command to generate security certificate files such as RSA, DSA.

After entering the command of SSL, follow the onscreen questions to give the required information.

### Syntax Items

ssl

### Example

```

G2500# ssl
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to '/mnt/ssh/ssl_key.pem_tmp'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:tw
State or Province Name (full name) [Some-State]:hs
Locality Name (eg, city) []:hschu
Organization Name (eg, company) [Internet Widgits Pty Ltd]:draytek
Organizational Unit Name (eg, section) []:marketing
Common Name (e.g. server FQDN or YOUR name) []:draytek
Email Address []:carrie_ni@draytek.com
G2500#

```

---

## X-2-16 Terminal Configuration

Use this command to set the maximum line number that the terminal is able to print.

### Syntax Items

terminal

### Syntax Description

| Syntax Items    | Description   |
|-----------------|---|
| <i>terminal</i> | <0-24> - Enter the length value. 0 means no limit.<br><br>Related Syntax:<br><ul style="list-style-type: none"> <li>● # terminal length &lt;0-24&gt;</li> </ul> |

### Example

```
G2500# terminal length 15
G2500# show running-config
.....
```

## X-2-17 Traceroute Configuration

Use this command to execute network trace route diagnostic.

### Syntax Items

traceroute

### Syntax Description

| Syntax Items | Description  |
|--------------|--|
| traceroute   | <HOSTNAME>- Enter the IP address or the hostname of the device for VigorSwitch to perform traceroute diagnostic.<br><br>Related Syntax:<br><ul style="list-style-type: none"> <li>● # traceroute &lt;HOSTNAME&gt;</li> </ul> |

### Example

```
G2500# traceroute 192.168.1.224
traceroute to 192.168.1.224 (192.168.1.224), 30 hops max, 40 byte packets
 1 192.168.1.224 (192.168.1.224) 0 ms 0 ms 0 ms
G2500#
```

## X-2-18 UDLD Configuration

Use this command to reset all interfaces disabled by the UniDirectional Link Detection (UDLD) and make data traffic begin passing through the interfaces again.

### Syntax Items

udld

### Syntax Description

| Syntax Items | Description   |
|--------------|---|
| udld         | Enter the IP address or the hostname of the device for VigorSwitch to perform traceroute diagnostic.<br><br>Related Syntax:<br><ul style="list-style-type: none"> <li>● # udld reset</li> </ul> |

## Example

```
G2500# udlld reset
```

```
G2500#
```

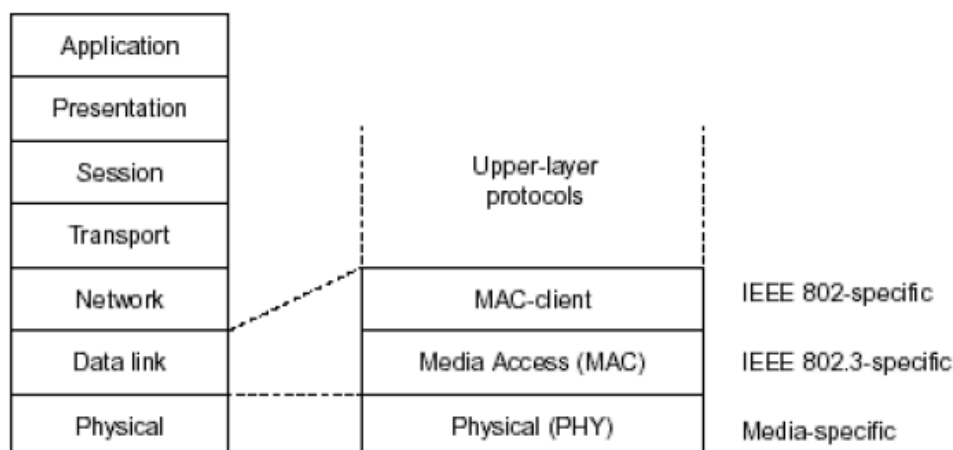
This page is left blank.

# Appendix: Reference

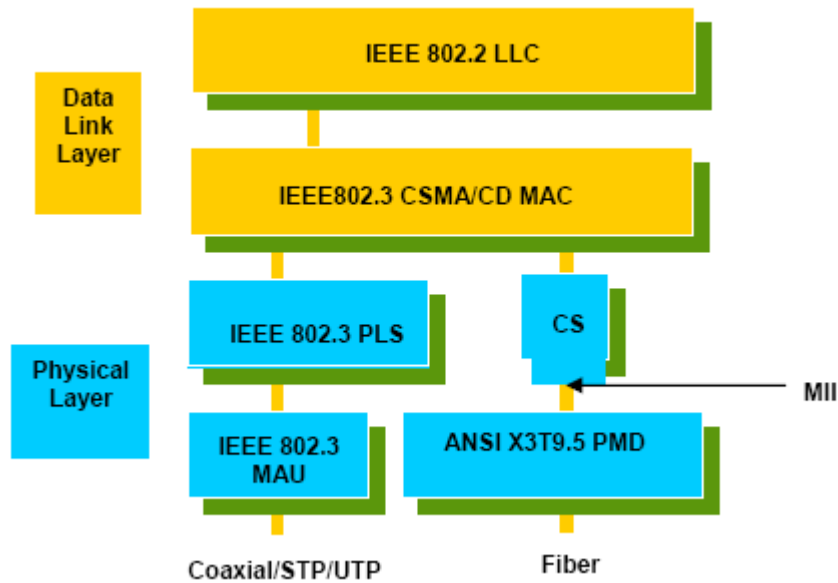
This chapter will tell you the basic concept of features to manage this switch and how they work.

## A-1 What's the Ethernet

Ethernet originated and was implemented at Xerox in Palo Alto, CA in 1973 and was successfully commercialized by Digital Equipment Corporation (DEC), Intel and Xerox (DIX) in 1980. In 1992, Grand Junction Networks unveiled a new high speed Ethernet with the same characteristic of the original Ethernet but operated at 100Mbps, called Fast Ethernet now. This means Fast Ethernet inherits the same frame format, CSMA/CD, software interface. In 1998, Gigabit Ethernet was rolled out and provided 1000Mbps. Now 10G/s Ethernet is under approving. Although these Ethernet have different speed, they still use the same basic functions. So they are compatible in software and can connect each other almost without limitation. The transmission media may be the only problem.



In the above figure, we can see that Ethernet locates at the Data Link layer and Physical layer and comprises three portions, including logical link control (LLC), media access control (MAC), and physical layer. The first two comprises Data link layer, which performs splitting data into frame for transmitting, receiving acknowledge frame, error checking and re-transmitting when not received correctly as well as provides an error-free channel upward to network layer.



This above diagram shows the Ethernet architecture, LLC sub-layer and MAC sub-layer, which are responded to the Data Link layer, and transceivers, which are responded to the Physical layer in OSI model. In this section, we are mainly describing the MAC sub-layer.

### Logical Link Control (LLC)

Data link layer is composed of both the sub-layers of MAC and MAC-client. Here MAC client may be logical link control or bridge relay entity.

Logical link control supports the interface between the Ethernet MAC and upper layers in the protocol stack, usually Network layer, which is nothing to do with the nature of the LAN. So it can operate over other different LAN technology such as Token Ring, FDDI and so on. Likewise, for the interface to the MAC layer, LLC defines the services with the interface independent of the medium access technology and with some of the nature of the medium itself.

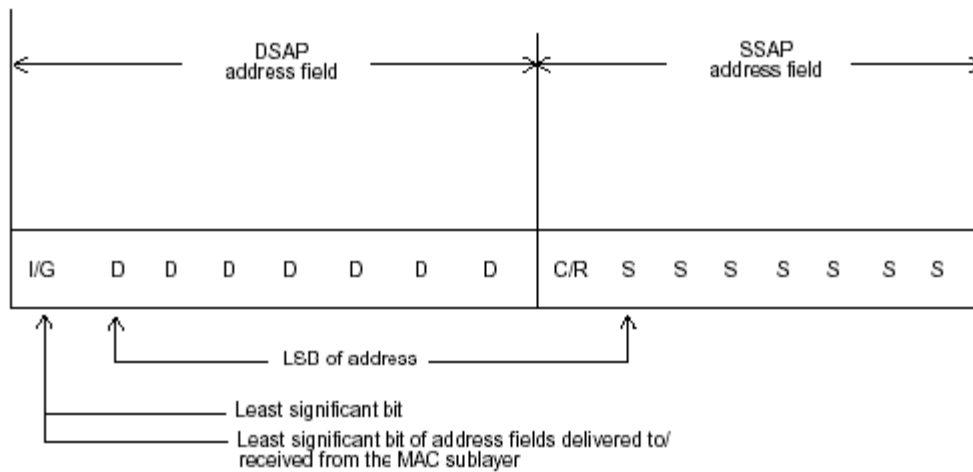
| DSAP address | SSAP address | Control      | Information |
|--------------|--------------|--------------|-------------|
| 8 bits       | 8 bits       | 8 or 16 bits | M*8 bits    |

- DSAP address = Destination service access point address field
- SSAP address = Source service access point address field
- Control = Control field [16 bits for formats that include sequence numbering, and 8 bits for formats that do not (see 5.2)]
- Information = Information field
- \* = Multiplication
- M = An integer value equal to or greater than 0. (Upper bound of M is a function of the medium access control methodology used.)

The table above is the format of LLC PDU. It comprises four fields, DSAP, SSAP, Control and Information. The DSAP address field identifies the one or more service access points, in which the I/G bit indicates it is individual or group address. If all bit of DSAP is 1s, it's a global address. The SSAP address field identifies the specific services indicated by C/R bit (command or response). The DSAP and SSAP pair with some reserved values indicates some well-known services listed in the table below.

|        |                             |
|--------|-----------------------------|
| 0xAAAA | SNAP                        |
| 0xE0E0 | Novell IPX                  |
| 0xF0F0 | NetBios                     |
| 0xFEFE | IOS network layer PDU       |
| 0xFFFF | Novell IPX 802.3 RAW packet |
| 0x4242 | STP BPDU                    |
| 0x0606 | IP                          |
| 0x9898 | ARP                         |

LLC type 1 connectionless service, LLC type 2 connection-oriented service and LLC type 3 acknowledge connectionless service are three types of LLC frame for all classes of service. In Fig 3-2, it shows the format of Service Access Point (SAP). Please refer to IEEE802.2 for more details.



I/G = 0 Individual DSAP  
I/G = 1 Group DSAP  
C/R = 0 Command  
C/R = 1 Response

XODDDDDD DSAP address  
XOSSSSSS SSAP address

X1DDDDDD Reserved for ISO definition  
X1SSSSSS Reserved for ISO definition

---

## A-2 Media Access Control (MAC)

### MAC Addressing

Because LAN is composed of many nodes, for the data exchanged among these nodes, each node must have its own unique address to identify who should send the data or should receive the data. In OSI model, each layer provides its own mean to identify the unique address in some form, for example, IP address in network layer.

The MAC is belonged to Data Link Layer (Layer 2), the address is defined to be a 48-bit long and locally unique address. Since this type of address is applied only to the Ethernet LAN media access control (MAC), they are referred to as MAC addresses.

The first three bytes are Organizational Unique Identifier (OUI) code assigned by IEEE. The last three bytes are the serial number assigned by the vendor of the network device. All these six bytes are stored in a non-volatile memory in the device. Their format is as the following table and normally written in the form as aa-bb-cc-dd-ee-ff, a 12 hexadecimal digits separated by hyphens, in which the aa-bb-cc is the OUI code and the dd-ee-ff is the serial number assigned by manufacturer.

|                      |                      |                      |                      |                      |                      |       |
|----------------------|----------------------|----------------------|----------------------|----------------------|----------------------|-------|
| Bit 47               |                      |                      |                      |                      |                      | Bit 0 |
| 1 <sup>st</sup> byte | 2 <sup>nd</sup> byte | 3 <sup>rd</sup> byte | 4 <sup>th</sup> byte | 5 <sup>th</sup> byte | 6 <sup>th</sup> byte |       |
|                      | OUI code             |                      |                      | Serial number        |                      |       |

The first bit of the first byte in the Destination address (DA) determines the address to be a Unicast (0) or Multicast frame (1), known as I/G bit indicating individual (0) or group (1). So the 48-bit address space is divided into two portions, Unicast and Multicast. The second bit is for global-unique (0) or locally-unique address. The former is assigned by the device manufacturer, and the later is usually assigned by the administrator. In practice, global-unique addresses are always applied.

A unicast address is identified with a single network interface. With this nature of MAC address, a frame transmitted can exactly be received by the target an interface the destination MAC points to.

A multicast address is identified with a group of network devices or network interfaces. In Ethernet, a many-to-many connectivity in the LANs is provided. It provides a mean to send a frame to many network devices at a time. When all bit of DA is 1s, it is a broadcast, which means all network device except the sender itself can receive the frame and response.

### Ethernet Frame Format

There are two major forms of Ethernet frame, type encapsulation and length encapsulation, both of which are categorized as four frame formats 802.3/802.2 SNAP, 802.3/802.2, Ethernet II and Netware 802.3 RAW. We will introduce the basic Ethernet frame format defined by the IEEE 802.3 standard required for all MAC implementations. It contains seven fields explained below.

|     |     |    |    |             |      |                |     |
|-----|-----|----|----|-------------|------|----------------|-----|
| PRE | SFD | DA | SA | Type/Length | Data | Pad bit if any | FCS |
| 7   | 7   | 6  | 6  | 2           |      | 46-1500        | 4   |

**Preamble (PRE)** - The PRE is 7-byte long with alternating pattern of ones and zeros used to tell the receiving node that a frame is coming, and to synchronize the physical receiver with the incoming bit stream. The preamble pattern is:

10101010 10101010 10101010 10101010 10101010 10101010 10101010



**Start-of-frame delimiter (SFD)** - The SFD is one-byte long with alternating pattern of ones and zeros, ending with two consecutive 1-bits. It immediately follows the preamble and uses the last two consecutive 1s bit to indicate that the next bit is the start of the data packet and the left-most bit in the left-most byte of the destination address. The SFD pattern is 10101011.

**Destination address (DA)** - The DA field is used to identify which network device(s) should receive the packet. It is a unique address. Please see the section of MAC addressing.

**Source addresses (SA)** - The SA field indicates the source node. The SA is always an individual address and the left-most bit in the SA field is always 0.

**Length/Type** - This field indicates either the number of the data bytes contained in the data field of the frame, or the Ethernet type of data. If the value of first two bytes is less than or equal to 1500 in decimal, the number of bytes in the data field is equal to the Length/Type value, i.e. this field acts as Length indicator at this moment. When this field acts as Length, the frame has optional fields for 802.3/802.2 SNAP encapsulation, 802.3/802.2 encapsulation and Netware 802.3 RAW encapsulation. Each of them has different fields following the Length field.

If the Length/Type value is greater than 1500, it means the Length/Type acts as Type. Different type value means the frames with different protocols running over Ethernet being sent or received.

For example,

|        |              |
|--------|--------------|
| 0x0800 | IP datagram  |
| 0x0806 | ARP          |
| 0x0835 | RARP         |
| 0x8137 | IPX datagram |
| 0x86DD | IPv6         |

**Data** - Less than or equal to 1500 bytes and greater or equal to 46 bytes. If data is less than 46 bytes, the MAC will automatically extend the padding bits and have the payload be equal to 46 bytes. The length of data field must equal the value of the Length field when the Length/Type acts as Length.

**Frame check sequence (FCS)** - This field contains a 32-bit cyclic redundancy check (CRC) value, and is a check sum computed with DA, SA, through the end of the data field with the following polynomial.

$$G(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$$

It is created by the sending MAC and recalculated by the receiving MAC to check if the packet is damaged or not.

### How does a MAC work?

The MAC sub-layer has two primary jobs to do:

1. Receiving and transmitting data. When receiving data, it parses frame to detect error; when transmitting data, it performs frame assembly.
2. Performing Media access control. It prepares the initiation jobs for a frame transmission and makes recovery from transmission failure.

### Frame transmission

As Ethernet adopted Carrier Sense Multiple Access with Collision Detect (CSMA/CD), it detects if there is any carrier signal from another network device running over the physical medium when a frame is ready for transmission. This is referred to as sensing carrier, also "Listen". If

there is signal on the medium, the MAC defers the traffic to avoid a transmission collision and waits for a random period of time, called backoff time, then sends the traffic again.

After the frame is assembled, when transmitting the frame, the preamble (PRE) bytes are inserted and sent first, then the next, Start of frame Delimiter (SFD), DA, SA and through the data field and FCS field in turn. The followings summarize what a MAC does before transmitting a frame.

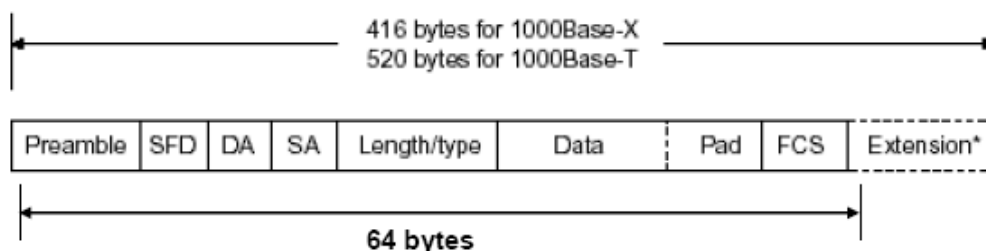
1. MAC will assemble the frame. First, the preamble and Start-of-Frame delimiter will be put in the fields of PRE and SFD, followed DA, SA, tag ID if tagged VLAN is applied, Ethertype or the value of the data length, and payload data field, and finally put the FCS data in order into the responded fields.
2. Listen if there is any traffic running over the medium. If yes, wait.
3. If the medium is quiet, and no longer senses any carrier, the MAC waits for a period of time, i.e. inter-frame gap time to have the MAC ready with enough time and then start transmitting the frame.
4. During the transmission, MAC keeps monitoring the status of the medium. If no collision happens until the end of the frame, it transmits successfully. If there is a collision happened, the MAC will send the patterned jamming bit to guarantee the collision event propagated to all involved network devices, then wait for a random period of time, i.e. backoff time. When backoff time expires, the MAC goes back to the beginning state and attempts to transmit again. After a collision happens, MAC increases the transmission attempts. If the count of the transmission attempt reaches 16 times, the frame in MAC's queue will be discarded.

Ethernet MAC transmits frames in half-duplex and full-duplex ways. In halfduplex operation mode, the MAC can either transmit or receive frame at a moment, but cannot do both jobs at the same time.

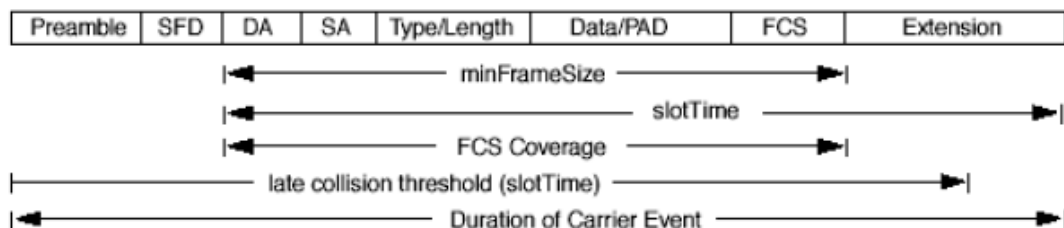
As the transmission of a MAC frame with the half-duplex operation exists only in the same collision domain, the carrier signal needs to spend time to travel to reach the targeted device. For two most-distant devices in the same collision domain, when one sends the frame first, and the second sends the frame, in worstcase, just before the frame from the first device arrives. The collision happens and will be detected by the second device immediately. Because of the medium delay, this corrupted signal needs to spend some time to propagate back to the first device. The maximum time to detect a collision is approximately twice the signal propagation time between the two most-distant devices. This maximum time is traded-off by the collision recovery time and the diameter of the LAN.

In the original 802.3 specification, Ethernet operates in half duplex only. Under this condition, when in 10Mbps LAN, it's 2500 meters, in 100Mbps LAN, it's approximately 200 meters and in 1000Mbps, 200 meters. According to the theory, it should be 20 meters. But it's not practical, so the LAN diameter is kept by using to increase the minimum frame size with a variable-length non-data extension bit field which is removed at the receiving MAC. The following tables are the frame format suitable for 10M, 100M and 1000M Ethernet, and some parameter values that shall be applied to all of these three types of Ethernet.

Actually, the practice Gigabit Ethernet chips do not feature this so far. They all have their chips supported full-duplex mode only, as well as all network vendors' devices. So this criterion should not exist at the present time and in the future. The switch's Gigabit module supports only full-duplex mode.



| Parameter value/LAN                        | 10Base         | 100Base                                    | 1000Base                                   |
|--|----------------|--|--|
| <b>Max. collision domain DTE to DTE</b>    | 100 meters     | 100 meters for UTP<br>412 meters for fiber | 100 meters for UTP<br>316 meters for fiber |
| <b>Max. collision domain with repeater</b> | 2500 meters    | 205 meters                                 | 200 meters                                 |
| <b>Slot time</b>                           | 512 bit times  | 512 bit times                              | 512 bit times                              |
| <b>Interframe Gap</b>                      | 9.6us          | 0.96us                                     | 0.096us                                    |
| <b>AttemptLimit</b>                        | 16             | 16   | 16   |
| <b>BackoffLimit</b>                        | 10             | 10   | 10   |
| <b>JamSize</b>                             | 32 bits        | 32 bits                                    | 32 bits                                    |
| <b>MaxFrameSize</b>                        | 1518           | 1518                                       | 1518                                       |
| <b>MinFrameSize</b>                        | 64             | 64   | 64   |
| <b>BurstLimit</b>                          | Not applicable | Not applicable                             | 65536 bits                                 |



In full-duplex operation mode, both transmitting and receiving frames are processed simultaneously. This doubles the total bandwidth. Full duplex is much easier than half duplex because it does not involve media contention, collision, retransmission schedule, padding bits for short frame. The rest functions follow the specification of IEEE802.3. For example, it must meet the requirement of minimum inter-frame gap between successive frames and frame format the same as that in the half-duplex operation.

Because no collision will happen in full-duplex operation, for sure, there is no mechanism to tell all the involved devices. What will it be if receiving device is busy and a frame is coming at the same time? Can it use "backpressure" to tell the source device? A function flow control is introduced in the full-duplex operation.

---

## A-3 Flow Control

Flow control is a mechanism to tell the source device stopping sending frame for a specified period of time designated by target device until the PAUSE time expires. This is accomplished by sending a PAUSE frame from target device to source device. When the target is not busy and the PAUSE time is expired, it will send another PAUSE frame with zero time-to-wait to source device. After the source device receives the PAUSE frame, it will again transmit frames immediately. PAUSE frame is identical in the form of the MAC frame with a pause-time value and with a special destination MAC address 01-80-C2-00-00-01. As per the specification, PAUSE operation can not be used to inhibit the transmission of MAC control frame.

Normally, in 10Mbps and 100Mbps Ethernet, only symmetric flow control is supported. However, some switches (e.g. 24-Port GbE Web Smart Switch) support not only symmetric but asymmetric flow controls for the special application. In Gigabit Ethernet, both symmetric flow control and asymmetric flow control are supported. Asymmetric flow control only allows transmitting PAUSE frame in one way from one side, the other side is not but receipt-and-discard the flow control information. Symmetric flow control allows both two ports to transmit PASUE frames each other simultaneously.

### Inter-frame Gap time

After the end of a transmission, if a network node is ready to transmit data out and if there is no carrier signal on the medium at that time, the device will wait for a period of time known as an inter-frame gap time to have the medium clear and stabilized as well as to have the jobs ready, such as adjusting buffer counter, updating counter and so on, in the receiver site. Once the inter-frame gap time expires after the de-assertion of carrier sense, the MAC transmits data. In IEEE802.3 specification, this is 96-bit time or more.

### Collision

Collision happens only in half-duplex operation. When two or more network nodes transmit frames at approximately the same time, a collision always occurs and interferes with each other. This results the carrier signal distorted and undiscriminated. MAC can afford detecting, through the physical layer, the distortion of the carrier signal. When a collision is detected during a frame transmission, the transmission will not stop immediately but, instead, continues transmitting until the rest bits specified by jamSize are completely transmitted. This guarantees the duration of collision is enough to have all involved devices able to detect the collision. This is referred to as Jamming. After jamming pattern is sent, MAC stops transmitting the rest data queued in the buffer and waits for a random period of time, known as backoff time with the following formula. When backoff time expires, the device goes back to the state of attempting to transmit frame. The backoff time is determined by the formula below. When the times of collision is increased, the backoff time is getting long until the collision times excess 16. If this happens, the frame will be discarded and backoff time will also be reset.

$$0 \leq r < 2^k$$

where

$$k = \min(n, 10)$$

### Frame Reception

In essence, the frame reception is the same in both operations of half duplex and full duplex, except that full-duplex operation uses two buffers to transmit and receive the frame independently. The receiving node always "listens" if there is traffic running over the medium when it is not receiving a frame. When a frame destined for the target device comes,

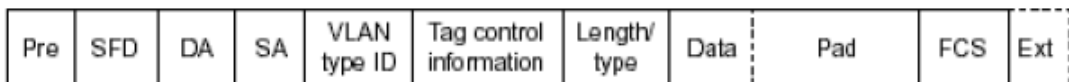
the receiver of the target device begins receiving the bit stream, and looks for the PRE (Preamble) pattern and Start-of-Frame Delimiter (SFD) that indicates the next bit is the starting point of the MAC frame until all bit of the frame is received.

For a received frame, the MAC will check:

1. If it is less than one slotTime in length, i.e. short packet, and if yes, it will be discarded by MAC because, by definition, the valid frame must be longer than the slotTime. If the length of the frame is less than one slotTime, it means there may be a collision happened somewhere or an interface malfunctioned in the LAN. When detecting the case, the MAC drops the packet and goes back to the ready state.
2. If the DA of the received frame exactly matches the physical address that the receiving MAC owns or the multicast address designated to recognize. If not, discards it and the MAC passes the frame to its client and goes back to the ready state.
3. If the frame is too long. If yes, throws it away and reports frame Too Long.
4. If the FCS of the received frame is valid. If not, for 10M and 100M Ethernet, discards the frame. For Gigabit Ethernet or higher speed Ethernet, MAC has to check one more field, i.e. extra bit field, if FCS is invalid. If there is any extra bits existed, which must meet the specification of IEEE802.3. When both FCS and extra bits are valid, the received frame will be accepted, otherwise discards the received frame and reports frameCheckError if no extra bits appended or alignmentError if extra bits appended.
5. If the length/type is valid. If not, discards the packet and reports lengthError.
6. If all five procedures above are ok, then the MAC treats the frame as good and de-assembles the frame.

#### What if a VLAN tagging is applied?

VLAN tagging is a 4-byte long data immediately following the MAC source address. When tagged VLAN is applied, the Ethernet frame structure will have a little change shown as follows.



Only two fields, VLAN ID and Tag control information are different in comparison with the basic Ethernet frame. The rest fields are the same.

The first two bytes is VLAN type ID with the value of 0x8100 indicating the received frame is tagged VLAN and the next two bytes are Tag Control Information (TCI) used to provide user priority and VLAN ID, which are explained respectively in the following table.

|                   |   |
|-------------------|---|
| <b>Bits 15-13</b> | User Priority 7-0, 0 is lowest priority   |
| <b>Bit 12</b>     | CFI (Canonical Format Indicator)<br><br>1: RIF field is present in the tag header<br><br>0: No RIF field is present                                 |
| <b>Bits 11-0</b>  | VID (VLAN Identifier)<br><br>0x000: Null VID. No VID is present and only user priority is present.<br><br>0x001: Default VID<br><br>0xFFF: Reserved |

**Note:** RIF is used in Token Ring network to provide source routing and comprises two fields, Routing Control and Route Descriptor.

When MAC parses the received frame and finds a reserved special value 0x8100 at the location of the Length/Type field of the normal non-VLAN frame, it will interpret the received frame as a tagged VLAN frame. If this happens in a switch, the MAC will forward it, according to its priority and egress rule, to all the ports that is associated with that VID. If it happens in a network interface card, MAC will deprive of the tag header and process it in the same way as a basic normal frame. For a VLAN-enabled LAN, all involved devices must be equipped with VLAN optional function.

At operating speeds above 100 Mbps, the slotTime employed at slower speeds is inadequate to accommodate network topologies of the desired physical extent. Carrier Extension provides a means by which the slotTime can be increased to a sufficient value for the desired topologies, without increasing the minFrameSize parameter, as this would have deleterious effects. Nondata bits, referred to as extension bits, are appended to frames that are less than slotTime bits in length so that the resulting transmission is at least one slotTime in duration. Carrier Extension can be performed only if the underlying physical layer is capable of sending and receiving symbols that are readily distinguished from data symbols, as is the case in most physical layers that use a block encoding/decoding scheme.

The maximum length of the extension is equal to the quantity (slotTime - minFrameSize). The MAC continues to monitor the medium for collisions while it is transmitting extension bits, and it will treat any collision that occurs after the threshold (slotTime) as a late collision.

# Index

- A**
- Account Manager, 179, 180
- B**
- Backup Manager, 177
  - Bandwidth, 147
- C**
- CoS Mapping, 144
- D**
- Dashboard, 15, 16
  - Diagnostics, 184, 193
  - DoS, 110
  - DoS Port Setting, 112
  - DoS Protection, 112
- E**
- Egress Shaping Per Queue, 149
  - Egress Shaping Rate, 148
- F**
- Factory Default, 182
- G**
- General, 130, 133, 138, 140
  - General Setup, 19
- I**
- Ingress Rate Limit, 147
  - Installation for VigorAPM, 6
- L**
- License Agreement, 22
  - License Information, 25, 26, 32, 48, 49, 76, 77, 86
  - Limiting Rate, 109
- P**
- Preamble, 108
  - Properties, 110
- Q**
- QoS Configuration, 129, 139
- S**
- Security, 91
  - SNMP, 162
  - SNMP Community, 166, 167, 169
  - Storm Control, 109
  - Storm Control, 92, 94, 95, 97, 100, 106, 108
  - Storm Control, 113
  - Storm Control, 116
  - Storm Control, 121
  - Stric Priority Queue, 143
  - System Configuration, 18
  - System Maintenance, 151
- U**
- Upgrade Manager, 178
- W**
- Weight, 143
  - WRR Bandwidth, 143