

# VigorSwitch G2280

24 Ports + 4 Combo UTP/SFP Ports L2 Managed Gigabit Switch



Your reliable networking solutions partner

# User's Guide

# VigorSwitch G2280 24 Ports + 4 Combo UTP/SFP Ports L2 Managed Gigabit Switch User's Guide

Version: 1.0 Firmware Version: V2.2.1 (For future update, please visit DrayTek web site) Date: March 27, 2018

#### 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 tore-store 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.

## Table of Contents

Part I Introduction	1
I-1 Introduction	
I-1-1 Key Features	
I-1-2 Specifications	
I-1-3 Packing List	
I-1-4 LED Indicators and Connectors	
I-2 Installation	
I-2-1 Typical Applications	
I-2-2 Installing Network Cables	
I-2-3 Configuring the Management Agent of Sw	tch 10
I-2-4 Managing VigorSwitch G2280 through Eth	ernet Port 10
I-2-5 IP Address Assignment	
I-3 Accessing Web Page of VigorSwitch	
I-4 Dashboard	
I-5 Status	
I-5-1 Port Bandwidth Utilization	
I-5-2 LLDP Statistics	
I-5-3 GVRP Statistics	
I-5-4 MLD Snooping Statistics	
Part II Switch LAN	
Part II Switch LAN	
II-1 General Setup	
II-1 General Setup II-1-1 IP Address	
II-1 General Setup II-1-1 IP Address II-1-2 IPv6 Address	
II-1 General Setup II-1-1 IP Address II-1-2 IPv6 Address II-1-3 Management VLAN	
II-1 General Setup II-1-1 IP Address II-1-2 IPv6 Address	20 20 20 21 22 23
II-1 General Setup II-1-1 IP Address II-1-2 IPv6 Address II-1-3 Management VLAN II-2 Port Setting II-3 Mirror	20 20 21 22 23 25
II-1 General Setup II-1-1 IP Address II-1-2 IPv6 Address II-1-3 Management VLAN II-2 Port Setting II-3 Mirror II-3 Mirror	20 20 21 22 23 25 26
<ul> <li>II-1 General Setup</li> <li>II-1-1 IP Address</li> <li>II-1-2 IPv6 Address</li> <li>II-1-3 Management VLAN</li> <li>II-2 Port Setting</li> <li>II-3 Mirror</li> <li>II-3 Mirror</li> <li>II-4 Link Aggregation</li> <li>II-4-1 LAG Setting</li> </ul>	20 20 21 22 23 25 26 26
<ul> <li>II-1 General Setup</li> <li>II-1-1 IP Address</li> <li>II-1-2 IPv6 Address</li> <li>II-1-3 Management VLAN</li> <li>II-2 Port Setting</li> <li>II-3 Mirror</li> <li>II-4 Link Aggregation</li> <li>II-4-1 LAG Setting</li> <li>II-4-2 LAG Management</li> </ul>	20 20 21 22 23 25 26
<ul> <li>II-1 General Setup</li> <li>II-1-1 IP Address</li> <li>II-1-2 IPv6 Address</li> <li>II-1-3 Management VLAN</li> <li>II-2 Port Setting</li> <li>II-3 Mirror</li> <li>II-4 Link Aggregation</li> <li>II-4-1 LAG Setting</li> <li>II-4-2 LAG Management</li> <li>II-4-3 LAG Port Setting</li> </ul>	20 20 21 22 23 25 26 26 27
<ul> <li>II-1 General Setup</li> <li>II-1-1 IP Address</li> <li>II-1-2 IPv6 Address</li> <li>II-1-3 Management VLAN</li> <li>II-2 Port Setting</li> <li>II-3 Mirror</li> <li>II-3 Mirror</li> <li>II-4 Link Aggregation</li> <li>II-4-1 LAG Setting</li> <li>II-4-2 LAG Management</li> <li>II-4-3 LAG Port Setting</li> <li>II-4-4 LACP Setting</li> </ul>	20 20 21 22 23 23 25 26 26 27 28
<ul> <li>II-1 General Setup</li> <li>II-1-1 IP Address</li> <li>II-1-2 IPv6 Address</li> <li>II-1-3 Management VLAN</li> <li>II-2 Port Setting</li> <li>II-3 Mirror</li> <li>II-3 Mirror</li> <li>II-4 Link Aggregation</li> <li>II-4-1 LAG Setting</li> <li>II-4-2 LAG Management</li> <li>II-4-3 LAG Port Setting</li> <li>II-4-4 LACP Setting</li> </ul>	20 20 21 22 23 23 25 26 26 27 28 29 30
<ul> <li>II-1 General Setup</li> <li>II-1-1 IP Address</li> <li>II-1-2 IPv6 Address</li> <li>II-1-3 Management VLAN</li> <li>II-2 Port Setting</li> <li>II-3 Mirror</li> <li>II-3 Mirror</li> <li>II-4 Link Aggregation</li> <li>II-4-1 LAG Setting</li> <li>II-4-2 LAG Management</li> <li>II-4-3 LAG Port Setting</li> <li>II-4-5 LACP Setting</li> <li>II-5 VLAN Management</li> </ul>	20 20 21 22 23 23 25 26 26 27 28 29 30
<ul> <li>II-1 General Setup</li> <li>II-1-1 IP Address</li> <li>II-1-2 IPv6 Address</li> <li>II-1-3 Management VLAN</li> <li>II-2 Port Setting</li> <li>II-3 Mirror</li> <li>II-3 Mirror</li> <li>II-4 Link Aggregation</li> <li>II-4-1 LAG Setting</li> <li>II-4-2 LAG Management</li> <li>II-4-3 LAG Port Setting</li> <li>II-4-4 LACP Setting</li> <li>II-4-5 LACP Port Setting</li> <li>II-5 VLAN Management</li> <li>II-5-1 Create VLAN</li> </ul>	20 20 21 22 23 23 25 26 26 26 27 28 29 30 31
<ul> <li>II-1 General Setup</li> <li>II-1-1 IP Address</li> <li>II-1-2 IPv6 Address</li> <li>II-1-3 Management VLAN</li> <li>II-2 Port Setting</li> <li>II-3 Mirror</li> <li>II-3 Mirror</li> <li>II-4 Link Aggregation</li> <li>II-4-1 LAG Setting</li> <li>II-4-2 LAG Management</li> <li>II-4-2 LAG Port Setting</li> <li>II-4-3 LAG Port Setting</li> <li>II-4-5 LACP Setting</li> <li>II-5 VLAN Management</li> <li>II-5-1 Create VLAN</li> <li>II-5-2 Interface Settings</li> </ul>	20 20 21 22 23 23 25 26 26 26 26 27 28 29 30 31 31
<ul> <li>II-1 General Setup</li></ul>	20 20 21 22 23 23 25 26 26 26 27 28 29 30 31 31 31

II-5-4 MAC VLAN	37
II-5-4-1 MAC Group	
I-5-4-3 Group Binding	
II-5-5 Protocol VLAN	39
II-5-5-1 Protocol Group	
II-5-5-2 Group Binding	
II-5-6 Surveillance VLAN	42
II-5-6-1 Property	
II-5-6-1 Surveillance OUI	
II-5-7 GVRP	45
II-5-7-1 Property	
II-5-7-2 Membership	
II-6 EEE	47
II-7 Multicast	48
II-7-1 Properties	48
II-7-2 IGMP Snooping	
II-7-2-1 IGMP Setting	
II-7-2-2 IGMP Querier Setting	
II-7-2-3 IGMP Static Group	
II-7-2-4 IGMP Group Table	
II-7-2-5 IGMP Router Table	
II-7-2-6 Forward AII II-7-2-7 Throttling	
II-7-2-8 Filtering Profile	
II-7-2-9 Filtering Binding	
II-7-3 MVR	61
II-7-3-1 Property	61
II-7-3-2 Port Setting	
II-7-3-3 Group Address	
II-7-4 MLD Snooping	64
II-7-4-1 MLD Setting	
II-7-4-2 MLD Static Group	
II-7-4-3 MLD Group Table II-7-4-4 MLD Router Table	
II-7-4-5 Forward AII	
II-7-4-6 Throttling	
II-7-4-7 Filtering Profile	
II-7-4-8 Filtering Binding	
II-8 Jumbo Frame	75
II-9 STP	76
II-9-1 Properties	
II-9-2 Port Setting	77
II-9-3 Bridge Setting	
II-9-4 Port Advanced Setting	
II-9-5 Statistics	
II-9-6 MST Instance	
II-9-7 MST Port Setting	
II-10 MAC Address Table	
II-10-1 Static MAC Setting	85

	II-10-2 Dynamic Address Setting	86
	II-10-3 Dynamic Learned	86
	II-11 Blocked Port Recover	88
Part II	II Security	89
	III-1 RADIUS	90
	III-2 TACACS+	
	III-3 Management Access Authentication	
	III-3-1 Method Profile	
	III-3-2 Application Authentication	
	III-4 Management Access Control	
	III-4-1 Management Access Control Profile (ACL)	
	III-4-2 Management Access Control Entries (ACE)	
	III-5 802.1X/MAC Authentication	
	III-5-1 Properties	
	III-5-1-1 Global Settings III-5-1-2 Port Authentication Setting	
	III-5-2 Port Control/Settings	100
	III-5-3 MAC-Based Local Account	102
	III-5-4 Authenticated Hosts	103
	III-6 Port Security	104
	III-7 Protected Ports	106
	III-8 Storm Control	107
	III-8-1 Properties	107
	III-8-2 Port Setting	108
	III-9 DoS	110
	III-9-1 Properties	110
	III-9-2 DoS Port Setting	112
	III-10 Dynamic ARP Inspection	113
	III-10-1 Properties	
	III-10-1-1 Global Property Settings III-10-1-2 Per Port Property Settings	113 114
	III-10-2 Statistics	115
	III-11 DHCP Snooping	116
	III-11-1 Properties III-11-1-1 Global Property Settings III-11-1-2 Per Port Property Settings	116
	III-11-2 Statistics	
	III-11-2 Statistics	
	III-11-3-1 Global Option82 Property Settings III-11-3-2 Per Port Option82 Property Settings	118
	III-11-4 Option82 Circuit ID	120
	III-12 IP Source Guard	121

III-12-1 Port Settings	121
III-12-2 IMPV Binding	122
III-12-3 Save Database	123
Part IV ACL Configuration	
IV-1 Create ACL	
IV-1-1 MAC	
IV-1-2 IPv4	127
IV-1-3 IPv6	127
IV-2 Create ACE	129
IV-2-1 MAC	129
IV-2-2 IPv4	130
IV-2-3 IPv6	132
IV-3 ACL Binding	
Part V QoS Configuration	135
V-1 General	
V-1-1 Properties	
V-1-1-1 QoS General Setting	
V-1-1-2 Trust Ports	
V-1-2 Port Settings	
V-1-3 Queue Settings V-1-4 CoS Mapping	
V-1-4 COS Mapping	
V-1-5 DSCP Mapping	
V-2 Bandwidth	
V-2-1 Ingress Rate Limit	
V-2-2 Egress Shaping Rate	
V-2-3 Egress Shaping Per Queue	
Part VI System Maintenance	
VI-1 LLDP	
VI-1-1 Properties	
VI-1-2 LLDP Port Setting	
VI-1-3 LLDP Local Device	
VI-1-4 MED Network Policy	
VI-1-5 LLDP MED Port Settings	
VI-1-6 LLDP Remote Device	
VI-1-7 LLDP Overloading	154
VI-2 SNMP	155
VI-2-1 View	156
VI-2-2 Group	157
VI-2-3 Community	158

VI-2-4 User	
VI-2-5 Engine ID	
VI-2-5-1 Local Engine ID	
VI-2-5-2 Remote Engine ID	
VI-2-6 Trap Event	
VI-2-7 Notification	
VI-3 Access Manager	
VI-4 Time and Date	
VI-4-1 System Time Zone	
VI-4-2 Time	
VI-5 Backup Manager	
VI-6 Upgrade Manager	
VI-7 Firmware Information	
VI-8 Account Manager	
VI-9 Factory Default	
VI-10 Reboot Switch	175
Part VII Diagnostics	
VII-1 Cable Diagnostics	
VII-2 Ping Test	
VII-3 SysLog	
VII-3-1 SysLog Explorer	
VII-3-2 SysLog Settings	
VII-3-2-1 SysLog Service	
VII-3-2-2 Local SysLog VII-3-2-3 Remote SysLog	
VII-5-2-5 Remote SysLog	
Appendix: Reference	
A-1 What's the Ethernet	
A-2 Media Access Control (MAC)	
A-3 Flow Control	
Index	105

# Part I Introduction

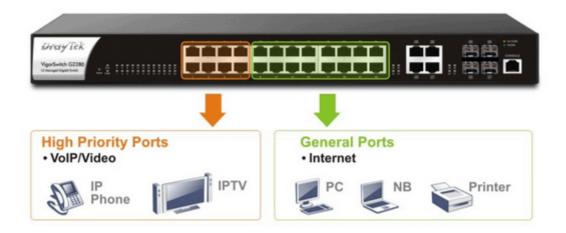
VigorSwitch G2280 User's Guide

## **I-1 Introduction**

VigorSwitch G2280, 24 Ports + 4 Combo UTP/SFP Ports 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 fully complies with all IEEE 802.3z and 1000Base-SX/LX standards.



### 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 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.

#### **Power Saving**

The Power saving using the IEEE 802.3az, Energy-Efficient Ethernet to detect the client idle and cable length automatically and provides the different power. It could efficient to save the switch power and reduce the power consumption.

## I-1-2 Specifications

The VigorSwitch G2280, 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

- ✤ 24 10/100/1000Mbps Auto-negotiation Gigabit Ethernet ports
- Jumbo frame support 9KB
- ✤ 4 UTP/SFP Combo Ethernet Ports
- 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

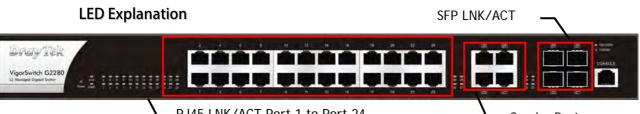
Before you start installing the switch, verify that the package contains the following:

- $\div$ VigorSwitch G2280
- \* AC Power Cord
- \* **Quick Start Guide**
- Rubber feet  $\dot{\mathbf{v}}$
- \* 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.





Combo Port

LED	Color	Explanation
	On (Green)	The switch finishes system booting and the system is ready.
SYS	Blinking (Green)	The switch is powered on and starts system booting.
	Off	The power is off or the system is not ready / malfunctioning.
PWR	On (Green)	The device is powered on and running normally.
FVVK	Off	The device is not ready or is failed.
RJ 45	On (Green)	The device is connected with 1000Mbps.
LNK/ACT Port 1 ~ 24	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.
Combo for	On (Green)	The device is connected with 1000Mbps.
Port 25 ~ 28	On (Amber)	The device is connected with 10/100Mbps.

(RJ 45 LNK/ACT)	Blinking	The system is sending or receiving data through the port.
	Off	The port is disconnected or the link is failed.
SFP LNK/ACT	On (Green)	The device is connected with 1000Mbps.
	On (Amber)	The device is connected with 10/100Mpps.
	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
RJ 45 LNK/ACT Port 1 ~ 24	Port 1 to Port 24 can be used for Ethernet connection.
SFP LNK/ACT Port 25 ~ 28	Port 25 to Port 28 are used for fiber connection.
Console	Used to perform telnet command control.
	Power inlet for AC input (100~240V/AC, 50/60Hz).

# **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:

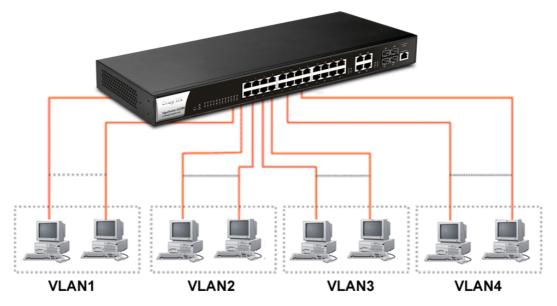
#### Case 1: All switch ports are in the same local area network.

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.

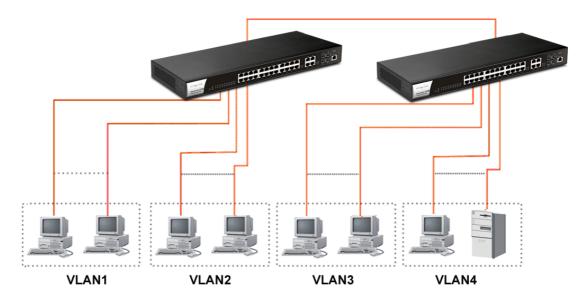
Here VLAN area is defined by what VLAN you are using. The switch supports both port-based VLAN and tag-based VLAN. They are different in practical deployment, especially in physical location. The following diagram shows how it works and what the difference they are.



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

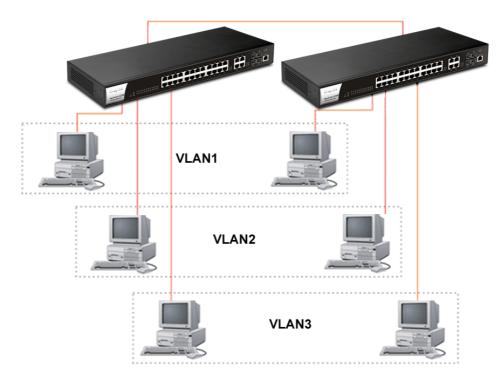
- The same VLAN members could not be in different switches.
- Every VLAN members could not access VLAN members each other.
- The switch manager has to assign different names for each VLAN groups at one switch.

#### 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.

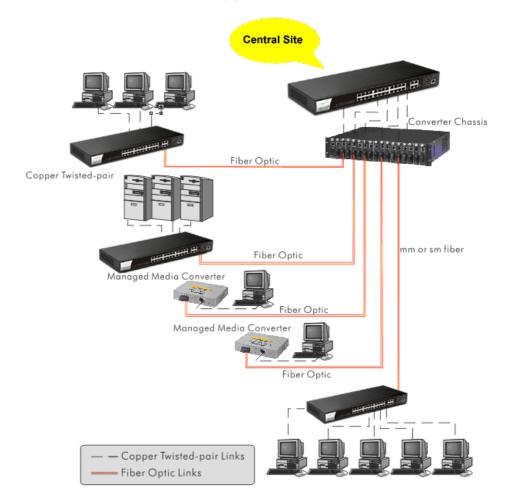
#### Case 6: Rack-mount Installation

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

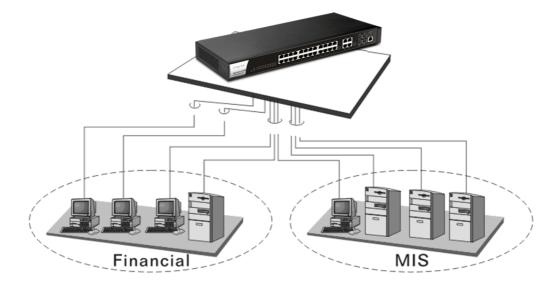
Procedures to Rack-mount the switch:

- 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.

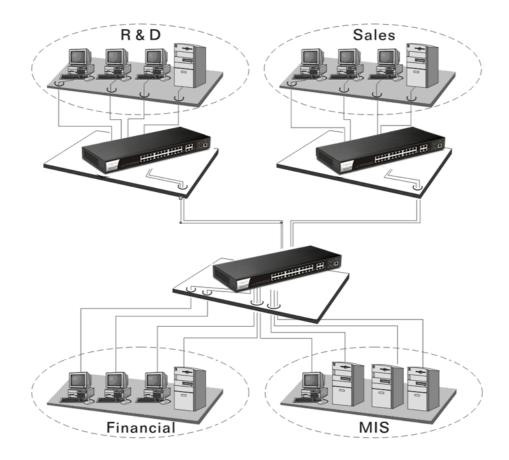
#### Case 7: Central Site/Remote site application is used in carrier or ISP



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	10 Mbps	Category 3,4,5 UTP/STP
10/100/1000 Mbps copper	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 G2280 through the Ethernet Port.

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

VigorSwitch, for example: IPAddress: 192.168.1.224 Subnet Mask: 255.255.255.0 Default Gateway: 192.168.1.254



Assign a reasonable IP Address, for example: IP Address: 192.168.1.100 Subnet Mask: 255.255.255.0 Default Gateway: 192.168.1.254



## I-2-4 Managing VigorSwitch G2280 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.



32 bits

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.

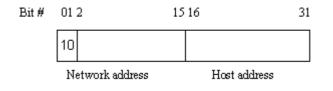
#### Class A:

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.

Bit #	01	78		31
	0			
	Network a	ldress	Host address	

#### 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.

Bit # 01 2 3 23 24 31

110	Netv	vork address	Host address
	110		

#### 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

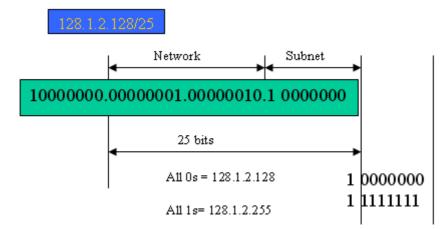
Please refer to RFC 1597 and RFC 1466 for more information.

#### 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.

<b>Dray</b> Tek	VigorSwitch G2280
Login	
User	admin
Password	
	Login

3. Now, the Main Screen will appear.

ray Tek						VigorSv	witch GZ
Auto Lugout : Dif	<b>-</b>	Admin					Ð
Diarhbowia			D	wihoura			
Status	- O Lunders						
Switch LAN	- O Londona						_
ecurity	-	Tela /		TTTT			
CL	- Vigorjavi						
5							
stem Maintenance	-						
agnostico		Device Information	11 I	System	n Information	_	
	Model	VigarSwitch (\$2280	CPU 0%	Memory 0%	Cache 0%		
	Famevare	221	Usage	Memory	Cached		
	Lowder	10.0					
	Revision	534					
	Elicitd Date	2017-11-15 11:36:27					
	System Time	This Jan 6 10 13 12 2000					
	System Up Time						
	ay about the range						
	-			ection Status			



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.

Auto Logout :	3 min	×	I
Dashboard			I
Status		-	ľ
Switch LAN		-	
Security			

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

				Dashboard				
Coading								
	is gada Swith				11 20 22 24 11 20 20 24 10 10 10 10 10 10 10 10 10 10 10 10 10 1			
	Device Informatio	ı			System Infor	mation		
Model	VigorSwitch	G2280	CPU 0%	Memory	0%	Cache 0%		
Firmware	2.2.1		Usage		Memory	Cached		
Loader	1.0.0							
Revision	534							
Build Date	2017-11-15	1:36:27						
System Time	Thu Jan 6 10	):13:12 2000						
System Up Time								
			C	onnection Status				
IPv4	IPv6							
ystem Name	Location	Contact	MAC	Protocol	IP	Gateway	DNS	Modify
2280	Default	Default	00:1D:AA:0C:C	Static	192.168.1.224	192.168.1.254		3

# I-5 Status

## I-5-1 Port Bandwidth Utilization

This page offers the traffic statistics inlcuding data information and data of interframe gap for each port (GE1 to GE28). In which, data of interframe gap can be displayed or hidden by choose Enable / Disable for IFG.

Auto Logout : Off 🛛 👻	Admin 10.22,40	D)
Dashboard	Castor > Part Bandwath Unixition > Part Bendwath Unixitian	
	Port Bandwath Utilization	
LLDP Statistics	uuto Refrente: 2 Bec - IFG: Enable -	
GVRP Statistics		
MLD Snooping Statistics	Gbps 100Mbps 10Mbps Unit Duwn	
Switch LAN	IX IX	
Security -	01 - 01 -	
ACL -	91. 63	
005 -	81- 41-	
System Maintenance -	95 - 95 -	
Diagnostics -	08- 92-	
	* * * * * * * * * * * * * * * * * * * *	100
	es. es.	
	91 64 - 74	

## I-5-2 LLDP Statistics

This page offers the statistics of LLDP packets (in, out and error) of each port (GE1 to GE28).

Auto Logout : Off	-			dmin						102400 🕞	
Dashboard		O tinita	• LLZIP Distriction -	LLL P. Shinkiten							
5940a		LLDP Sink									
Port Bandwidth Utilization		LEDF-GUIN	11122								-
						LLDP Global Statist	leş.				
GVRP Statistics		-	-								
MLD Snooping Statistics		Retresh	Clear All								
Switch LAN	*	Insertions							o		-
Security	*	Deletions							0		
ACL	1	Drops							0		
005	~										
System Maintenance		Age Outs							0		
Diagnostics	-					LLDP Port Statistic	s.				
		Port	TX Frames Total	RX Frames	RX Fr Disca			RX TLVs Discarded	 RX TLVs Unrecognized	RX Ageouts Total	
		GEI	ö	ū	à	à		ñ.	ō.	D	
		GEØ	1/3	¢	в	a		E.	0	0	
		GES	0	D.	٥	0.		ō	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.

DrayTek								Vigor	Switch G228	
Auto Logout : 🕞 Tam	*		andmin						G	
Dashboard		O Status	- GVRP Statistics + Statistics							
Shalos	-	-								
Port Bandwidth Utilization		Statistics					 			
LLDP Statistics			Port:		GE1, GE2, GE3, GE4, GE5, GE6, GE	E7, GE8, GE9, GE10		÷		
GVRP Statistics			Statistics:		Transmit, Receive, Error					
MLD Snooping Statistics					10 sec					
Switch LAN			Refresh Rate:		10 sec					
Security		8			Tx Statistic	4			7	
ACL					La Statistic					
QuS	~	Port	Join empty	Empty	Leave Empty	Join In	Leave In	Leave Al	Lf.	
System Maintenance	2	GE1	D	n	ņ	0	D	D		
Diagnostics	1	GEP	0	0	0	0.	D.	0		
		GE3	0	σ	0	0	0	0		
		GE4	Q	ū	a	D	0	0		
		GES	0	.0	D	ú	ń	0		
		GE6	0	u u	U	0	0	0		
		GE7	D	xi -	ŭ	D	D	Ď.		

## I-5-4 MLD Snooping Statistics

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

DrayTek			Vigor Switch G2280
Auto Logaut : 3 min	-	Admin	03.28 19 🕞
Dashboard		Statut > MLD Snooping Statiates > Statistics	
	-	Stillatics	
Port Bandwidth Ublization	1.0		
LLDP Statistics		@Rehesh OClear All	
GVRP Statistics	_	Rx Statistics	
MLD Scooplog Statistics			
Switch LAN		Rx Total	٥
Security		Rx Valid	0
ACL.		Rx invalid	ŭ
Dos		Rx Other	0
System Maintenance	*	Rx Leave	Ø
Diagnostics		Rx Report	0
		Rx General Query	0
		Rx Special Group Query	۵
		Rx Source-specific Group Query	۵
		Tx Statistics	
		Tx Leave	U

# Part II Switch LAN

VigorSwitch G2280 User's Guide

## 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.

Pray Tek			Vigor Switch G
Auto Engout : 3 min 💌			03.30.0) 🕞
Dashboard 🖸	General Setup > 11/ Address > 12 Addres	0	
Status -			
Swith LAN	Address		
General Setup	Mode:	⊙ Static ○ DHCP	
P Alidress	IP Address:	152 168 1.224	
PV6 Address	Subnet Mask:	266 265 255 0	
Management's LAIV	Gateway:	192.168.1.254	
fort Setting			
firror	<b>DNS Server 1:</b>		
Ink Aggregation	DNS Server 2:		
LAN Management	Andy		
EE	Contract		
Autocast			
umbo Frame			
TP			
AC Address Table			
locked Port Recover			

Item	Description
Mode	Select the mode of network connection. Static- Use static IPv4 address.
	DHCP - Use DHCP provisioned IP address and Gateway if feasible.
IP Address	It is available when <b>Static</b> is selected as <b>Mode</b> . 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> . 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> . 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> . 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> . 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.

DrayTek					Vigors	wilch G	2280
Auto Loguvt : 3 min 🦉					03.90.48	₽	
Dashboard Status Switch (JAN) General Setup	Convert Billor: >196 Address > 196 Address  P.6 Address  Auto Configuration:	© Enable 🔿 Disable					
P Address P Address Poin Address Management VLAV Port Setting Manor Link Aggregation VLAV Management EEE Multicust Jumbo Frame. STP MAC Address Table Blocked Port Recover	IPv6 Address: Link Local Address: Gateway: DHCPv6 Client: (Agg)	fe0:21d saff fsOcred08	4 	U Et			

Item	Description
Auto Configuration	Enable - Check it to let switch automatically configure IPv6 address.
IPv6 Address	It is available when Auto Configuration is set as Disable. 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 Auto Configuration is set as Disable. 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 Auto Configuration is set as Disable.

	If static mode is enabled, enter primary DNS server address in this field.
DNS Server 2	It is available when Auto Configuration is set as Disable. If static mode is enabled, enter secondary DNS server address in this field.
DHCPv6 Client	It is available when Auto Configuration is set as Enable. 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.

Auto Logout : 3 min 🖌	Admin		យរាស 🕒
Dashboard	O General Setup > Management VLAU = Mana	germed VLAN Setting	
Status	Management VLAN Setting		
SWICH LAN	Management VD4A Setting		
General Setop	Management VLAN:	default(1) -	
IP Address	Autor	default(1)	
IPV6 Address	CHEEL,		
Managaran VEAN			
Port Setting			
Mirtor			
Link Aggregation			
VLAN Management			
EEE			
Multicast			
Jumbo Frame			
STP			
MAC Address Table			
Blocked Port Recover			

Item	Description
Management VLAN	Select the VLAN ID as management VLAN. You can create additional VLAN profiles by Switch LAN>>VLAN management>> Create VLAN.
Apply	Apply the settings to the switch.

# **II-2 Port Setting**

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

Auto Luguota 3 mm	-												10:10:59	B
Dashboard		Siviteh LAN	> Port Setting +	Port 5	iethog;									-
Status	14	Concession of the local division of the loca												
Switch IDM		Post Setting						_			_			
General Setup			Ports:				Nellong - le lieg							
Fort-Setting			Enable State:			100	Enable 🔿 Disable							
Mirror			Speed:			Ĩ	Auto							
Link Aggregation														
VLAN Management			Duplex:				Auto							
EEE			Flow Control:			۲	Enable 🔿 Disable							
Multicast									Appig					
Jumbo Frame														
STP		Port	Description	11	Enable State	10	Link Status	0	Speed	Duplex	11	FlowCtrl Config	FlowCtri Status	Modify
MAC Address Table		GE1			Enabled		Down		Auto	Autu		Enabled	Disabled	0
Blocked Port Recover		GE2			Enabled		Up		Auto(1000M)	Auto(Full)		Enabled	Enabled	00
Security		GE3			Enabled		Down		Aute	Auto		Enabled	Disabled	0
ACL		GE4			Enabled		Down		Autri	Auto		Enabled	Disabled	0
0.05		GE5			Enabled		Down		Auto	Auto		Enabled	Disabled	0
						_	-			-				-

Item	Description
Ports	Use the drop down list to selelct one or more LAN port(s).
Enable State	Enable -Click it to enable the port.
	Disable - Click it to disable the port.
Speed	Port speed capabilities:
	• Auto: Auto speed with all capabilities.
	• Auto-10M: Auto speed with 10M ability only.
	• Auto-100M: Auto speed with 100M ability only.
	• Auto-1000M: Auto speed with 1000M ability only.
	• Auto-10/100M: Auto speed with 10/100M ability.
	• 10M: Force speed with 10M ability.
	• 100M: Force speed with 100M ability.
	• <b>1000M</b> : Force speed with 1000M ability.
	Selecting Auto (auto-negotiation) allows one port to negotiat with a peer port automatically to obtain the connection spee and duplex mode that both ends support. When auto-negotiation is turned on, a port on the switch negotiate 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.
	For SFP fiber module, you might need to manually configure the speed to match fiber module speed.

	<ul> <li>Port duplex capabilities:</li> <li>Auto: Auto duplex with all capabilities.</li> <li>Half: Auto speed with 10/100M ability only.</li> <li>Full: Auto speed with 10/100/1000M ability only.</li> </ul>					
Flow Control	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. Enable - Click it to enable such function. Disable - Click it to disable such function.					
Apply	Apply the settings to the switch.					
Modify	It is used to manually enter the description, state, speed, duplex, flow control for the port.					
	Description					
	Enable State					
	Enable					
	Speed					
	e S					
	ed					
	ed Auto					
	Flow Control					
	ed Enable -					
	ed Enable					
	ed Disable Out Outour					

# **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 convinent for system administrator to monitor / understand the traffic operation.

Auto Logout : 3 mm	-		Admin					10.25 16	₽	
Dashboard		② Exists LAN ⇒ Mini	u > Marin							
Status		Minur								
		10010								
General Setup		Sessi	ion ID:	î.						
Port Setting		Moni	tor Session State:	Disable						
			nation Port:	GE1						
Link Aggregation		Desti	nation Port:	GET			1. •			
VLAN Management		Allov	Allow Operation as Normal Port		Disable					
EEE		Sniff	Ports(RX):	Hitthing and	icted.					
Multicast		Sniff	Parts(TX):	Techniq activities				24		
Jumbo Frame					Apply					
STP					Carlos Sector					
MAC Address Table		Session ID	Destination Port		Allow ingress	Sniff Ports(RX)		Sniff Ports(TX)		
Blocked Port Recover		1	N/A		N/A	N/A		N/A.		
Security	-	2	N/A		N/A	N/A.		N/A.		
AGL	$(\mathbf{r})$	à	N/A		NVA.	16/4		N/A.		
005		a	N/A		ntin.	104		NPA.		

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

Available s	ettings 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	Enable - Enable specified mirror session. Disable - Disable specified mirror session.
Destination Port	Specify the port where you wish to observe the mirrored packets.
Allow Operation as Normal Port	<ul><li>Enable - The destination port is able to function as a port connecting to network, communicating with other network devices.</li><li>Disable - 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.

Auto Logout : 3 mili			18 <b>22</b> 🕞
Dashboard O	Link Apgrogation > LAG Setting > LAG Setting	(	
Status -	AG Setting		
swith LAN	Load Balance Algorithm:		
General Setup	1 0ad Balance Algorithm:	IP/Mac Address	*
Part Setting	Apply	Mac Address	
Mixtor		IP/Mac Address	
Link Aggregation			
LAG Samo			
LAG Management			
LAG Port Setting			
LACP Setting			
LACP Fort Silling			
VLAN Management			
EEE			
Multiciest			
Jumbo Frame			
STP			

Item	Description
Load Balance Algorithm	Select your Load balance algorithm.
	MAC address - Aggregated group will balance the traffic based on different MAC addresses. Therefore, the packets from different MAC addresses will be sent to different links.
	<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.
Apply	Apply the settings to the switch.

## II-4-2 LAG Management

There are eight LAG profiles allowed to group different physical ports (GE1 to GE28). The system will assign certain port(s) as Active Member and Standby Member according to the GE selections.

Auto Logout : 3 min	*					03-37-06
Dashboard	O Link Aqui	egition > LAG Management >	LAG Management			
Status	-					
Switch 1,429	LAG Manage	iment				
General Setup	LAG	Description	Port Type	Link Status	Active Member	Standby Member D Modify
Port Setting	LAGT		-	Not Present		0
Mirror	LAG2		-	Not Present		0
Link Aggregation	LAGS		-	Not Present		0
LAG Setting	LAG4		-	Not Present		0
	LAGS		-	Not Present		0
LAG Port Setting	LAGE		~	Not Present		0
UACP Setting	LAG7		-	Not Present		0
LACP Port Setting	LAGE		-	Not Present		0
VLAN Management EEE Multicast Jumbo Frame STP						

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.					
	Image: Static - The static aggregated port sends packets over active member without detecting or negotiating with remote aggregated port.         Image: ACCP- 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 LAG8), including data speed and enabling/disabling the flow control.

Auto Logout : Cff	*	Adalin							
Dashboard	O Link Aggingation > LAS Po	O Link Aggregation > LAG Port Setting > LAG Point Setting							
Status	Concession of the local division of the loca								
Seerch Lefter	LAG Part Setting								
General Setup	LAG:			- Nathing substore					
Port Setting	Enable:			Enable					
Mirror									
Link Aggregation	Speed:		Auto					1	
	Flow Control:		Dinable	Dinable				•	
LAG Management				Ap	uply -				
DAU Post Setting									
LACP Setting	LAG Description	Port Type	Enable State	Link Status	Speed	Duplex	Flow Control	Flow Control	Modity
LACP Part Setting	LAGI		Enable	Down	Auto(Ail)	Auto	Enable	Disable	0
VLAN Management	LAG2	~	Enable	Down	Auto(All)	Auto	Enable	Disable	0
EEE	LAGS	-	Enable	Down	AULO(AII)	Auto	Enable	Disable	0
Multicast	LAG4	-	Enable	Down	Auto(Ali)	Auto	Enable	Disable	0
Jumbo Frame	LAG5	-	Enable	LIOWT	Auto(All)	Auto	Enable	Disable	0
STP	LAGÊ		Enable	Down	Auto(All)	Auto	Enable	Disable	0

Item	Description			
LAG	Use the drop down list to select one or more LAG profiles.			
Enable	Enable -Click it to enable the profile. Disable - Click it to disable the profile.			
Speed	<ul> <li>Port speed capabilities:</li> <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-100M: Auto speed with 100M 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>100M: Force speed with 100M ability.</li> <li>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 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.</li> </ul>			
Flow Control	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. Enable - Click it to enable such function. Disable - Click it to disable such function.
АррІу	Apply the settings to the switch.
Modify	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.

Aino Logout : Orr 🚿	- Million		ouri a 🕞
Dashboard	LINGP Sattling		
Status	LACP:	⊙Enable ⊖Disable	
Guildin LAM	System Priority:		(1.65535)
General Setup	System Privay.	32768	(1 65635)
Port Setting	ADDN		
Mirror			
Link Aggregation			
LAG Setting			
LAG Management			
LAR Port Setting			
LACP Port Setting			
VLAN Management			
EEE			
Multicant			
Jumbo Frame			
STP			
MAC Address Table			
Security -			
ACL -			
QuS -			
-			and a second
Auto Logout : Off	Admin		4394427 <b>E</b> 9
Dashboard	C Link Applegation > LACP Setting, + LACP 5	Setting	
Status.	LACP Sutting		
Swanh LMI		Charles Laboration	
General Setup	LACP:	💿 Enable 🔘 Disable	
Port Setting	System Priority:	10760	5 (1-65535)
Mirror			
Link Aggregation	Apply		
LAU Setting			
LAG Management			
LAG Port Setting			
LACP Series			
LACP Pert Setting			
VLAN Management			
EEE			
Multicast			
Jumbo Frame STP			

Item	Description
LACP	Enable - Click it to enable such function. Disable - Click it to disable the function.
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 Vigorwitch 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.
ApplyApply the settings to the switch.	

## II-4-5 LACP Port Setting

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

Auto Logout : Of	Admin .			03:45:46		
Dashboard	O Link Appregiation -> LACP Port	Batting > LACP Port Sett	na			
Status	· DESCRIPTION OF					
Summ 1.442	LACR Part Setting					
General Setup	Ports:		thathing unterlied.		2	
Part Setting	Priority:		10		8	(1-65535)
Marton			1			
Link Aggregation	Timeout:		Long	1.00	•	
LAG Selling				Anply		
LAU Management						
LAG Port Setting	Port	Priority		Timeout	Modity	
LACP Setting	GE1	i i		Long	0	
LACP Poly Billing	GE2	- 1 -		Long	0	
VLAN Management	GE3	j.		Long	0	
EEE	GE4	= 1 =		Long	0	
Multicast	GE5	- <b>f</b> -		Long	0	
Jumbo Frame	GE6	= <b>1</b> =		Long	0	
STP	GE7	-1-		Long	0	

Item	Description
Ports	Use the drop down list to specify LAN Port.
Priority	Enter a port priority number for the port.
Timeout	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.
	Long - LACP PDU will be sent every 30 seconds. If port member is not seen over 90 seconds, it will cause port member timeout.
	Short - LACP PDU will be sent per second. If port member is not seen over 3 seconds, it will cause port member timeout.
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

Aato Logout : Off 👻	Ar	nan -			07/20:45	G
Port Setting Mirror Link Aggregation	VLAR Management > Create for     Create VLAN	m = Covele YLAN				
VUAN Munagemant Cravite Vien Interface Settings Value VLAN MAC VLAN	Action: VLAN ID: VLAN Name:	S Add O Delete	ada Acoly			
Philocol VLAN Surveillance VLAN GVRph EEE Multicast Jumbo Frame STP	VLAN ID	Uctouit	VLAN Type Default	ii Medity		
MAC Address Table Blocked Port Recover						

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

Item	Descript	Description		
Action	Add - Cre	Select which action to perform, add VLANs or delete VLANs. Add - Create a new VLAN profile. Delete - Delete an existed VLAN profile.		
VLAN ID	want to a multiple	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	name. Le	e prefix you wish to eave it empty for u cking Apply, you w	ising default "VLAN	
	VLAN ID	IE VLAN Name	VLAN Type	Modify
	x	petault	Deraut	0
	2	markeling0002	State	00
	3	inarketing0003	Stabo	00
Apply	Apply the	Apply the settings to the switch.		
Modify	🧷 - Mo	Modify the name of the selected VLAN ID.		

Арру
Edit name of VLAN 4067
diHDMIVLAN4067
OK Cancel
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.

Auto Logout : Off 🛛 👻	Q	
Dachboard	VLA/I Management > Intarluce/Sattangs = Interlace Settings	
Status -	Interface Settings	_
Synthe LAN	Port Select: #021emp avaulatin -	
General Setup	Port Select:	
Port Setting	Interface VLAN Mode:	
Mirror.	PVID: 1 (1 - 4034)	
Link Aggregiation	Accepted Type: 🛞 All 🔿 Tag Only 🔿 Untag Only	
MLAN Management	Ingress Filtering: 🛞 Enabled 🔿 Disabled	
Create Vian	Tagged VLAN: Ferning structures	
Interluce Settings	Untagged VLAN: Polition autocles	
More VLAN	Forbidden VLAN: Mothway annalko -	
MAC VLAN		
Protocal VLAN	Aavy	
Surveillance VLAN		
	Port Interface VLA PVID Tagged VLAN Untagged VL Forbidden V Accept Fram Ingress Filte Uplink TPID	Mod
EEE	GE1 Trunk I - I - ALL Enabled Disabled 0x8100	0
Multicent	OE2 Trunk 1 - 1 - ALL Enabled Disabled Bx8100	0 .

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.
	Hybrid - Support all functions as defined in IEEE 802.1Q specification.
	Access - Accept only untagged frames and join an untagged VLAN.
	<b>Trunk</b> - An untagged member of one VLAN at most, and is a tagged member of zero or more VLANs.
PVID	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. For port under Access Mode, VLAN ID provided as PVID would automatically be selected as the untagged VLAN.	
Accepted Type	Specify the acceptable-frame-type of the specified interfaces. It's only available with Hybrid mode. All - Accept frames regardless it's tagged with 802.1q or not. Tag Only - Accept frames only with 802.1q tagged. Untag Only - Accept frames untagged.	
Ingress Filtering	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. Enabled - Click it to enable the function. Disabled - Click it to disable the function.	
Tagged VLAN	Specify the VLAN profile tagged in the VLAN.	
Untagged VLAN	Specify the VLAN profile untagged in the VLAN.	
Forbidden VLAN	Specify the VLAN profile forbidden in the VLAN.	
Apply	Apply the settings to the switch.	
Modify	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 priorioty 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.

Auto Logoot : Of 🖉 👻	Admin			(0.97.26 🕞
Dashboard	Properties Telephony OUI Setting Part Sutting			
Status -	Voice VLAN State:	OEnabled  ODisabled		_
General Setup	Voice VLAN Id: Remark CoSi802.1p:	_HDM(_VL4/4007(4007)		Enable
Port Setting Mirror	Remark Value:	6		
Link Aggregation	Aging Time:	1440:	¢	(30-65536 min)
VLAN Management Ureste Vian Ureste Settings Yotos VLAN MAC VLAN Surveitance VLAN Surveitance VLAN EEE Metteand Jumiti Frame BTP Mic Address Table	(Apply)			

Item	Description
Voice VLAN State	Enabled - Click it to enable Voice VLAN. Disabled - Click it to disable Voice VLAN.
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. 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). Default is 1440 minutes. A voice VLAN entry will be age out after this time if without any packet pass through.
АррІу	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.

Auto Logoot : 🛛 🖓 🛸	Admin		10.38.29 🕒
Pashbóard tálus	Properties Telephany OUI Getting Por	Setting	
etan 1299	OUI Address:	រាករាំក កង់	
ieneral Setup	Description:		
Port Setting	1.	800	
unk Aggregation	OUI Address	Description	Edit
/LAN Management	00.E0.BB	зсом	Ø 👩
Create Vian	00.03.68	Cisca	Ø 😑
Interface Settinos	00:E0:75	veriter	Ø 👩
	00 D0:1E	Pingtel	00
MAC VLAM	00:01:E3	Siemens	20
	00.60.09	NEC#Philips	20
Blime Lance VLAN	06.0F.E2	HOC	00
EE	00.09.EE	locaya	Ø 👩
dubcast Jumbo Frame aTP			
MAC Address Table			

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.				
Modify	<ul> <li>Additional content of the selected OUI entry.</li> </ul>				

## II-5-3-3 Port Setting

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

Auto Logout : Off. 🚿	a strange of the second	Admin		10:4408
Dashboard Status	Properties Telephony	OUI Setting Part Setting		
Clarken Laya.	- Port:	Modulin	l Pronegori	1
General Setup	State:	CEnabled	Disabled	
Port Setting	Cos Mode:	O All S	rc	
Mirror			Apply	
Link Aggregation				
VLAN Management	Port	11 State	Cos Mode	Edit
Create Vian	GE1	disable	srt	0
Interface Sollings	GE2	distable	SHE	0
	GE3	disable	src	0
MAG VEAN	GE4	disable	372	0
	965	disable	Sr£	0
Surveillance VLAN	GE6	disable	src	0
GVRP.	GE7	desable	ste	0
EEE	GEB	disable	srt	0
Multicast	069	disable	SIC	0
Jumbo Frame	9610	disable	STL	0
STP	0É11	disable	stc	0
MAC Address Table	GE12	detably	stu	0
WWW CMMIRSO, Japie	GE13	disable.	sn	0

Item	Description
Port	Use the drop down list to specify one or more LAN ports.
State	Enabled - Click it to enable the port settings for Voice LAN. Disabled - Click it to disable the port settings for Voice LAN.
Cos Mode	If Remark CoS/802.1p is enabled in Voice VLAN>>Properties, settings in this page shall be applied. Otherwise, this option will not take effect.
	All - 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.
	Src (Source) - 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.
Apply	Apply the settings to the switch.
Edit	Click the icon under Edit for one entry to modify port settings (State, Cos Mode) for voice VLAN.
	y OUI Setting Port Setting
	Edit port GE1
	State:
	Enabled
	Cos Mode:
	See Edit
	OK Cancel

## 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.

Auto Loonata 100 😒			Beni							64:52:57	Ð
Dashboard	MAC-Group	Group Binding									
Status -	_										
		Group ID:							6	(1-2147483)	647)
General Setup		MAC Address:		100.000	nais ciman						
Port Setting		Maskc							12	(9 - 48)	
Miltor						Add					
Link Aggregation						_					
VLAN Management	Group ID			MAC Address				AT Mask		LT Edit	
Greate Vian						No cata available in	table				
- interface Setting i											
Volce VLAN											
NAC VERY											
Preliscel VLAH											
Serveillance VLAN											
1870											
EEE											
Multicast											
Jumbo Frame											
STP											
MAC Address Table											

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. 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.
Edit	Click the icon under Edit for one entry to modify settings for group ID.

### I-5-4-3 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.

Auto Logout : 01 🕅	BOIL				anata Di
Dashboard MAC Group	Oroup Binding				
Status -					
SWITE LAN	Ports:	067, 063, 064, 066, 067			
General Getup	Group ID:	requiring anneared		-	
Port Getting	VI.AN.				(1 - 4094)
Mirran			Ants		
Link Aggregation					
VLIVI Management Port	Graup		VLAN		Edit
Create vian		No data en	allable in table		
Interface Settings					
Valen VLAN					
MIND VILLARE					
Finiscol VLAN					
Surviulance VLAN					
OVRP					
18E					
lutineard					
lumbo Frame					
TTP					
MAC Address Table					

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

Auto Logout : Off 🛛 💌	Admin			07:43:45 🕞
Dashboard	Protocol Group Group Binding			
Status -				
Switch LAN	Group ID:		\$	(1 - 8)
General Setup	Frame Type:	Ethernet_II	-	
Port Setting	Protocol Value:	0x		(0×600 - 0×FFFE)
Mirror				(,
Link Aggregation		Add		
VLAN Management			- /	
	Group ID	Frame Type	Protocol Value	LE Edit
Interface Settings	1	IEEE802.3_LLC_Other	0x0601	<b>1</b>
Voice VLAN	3	Ethernet_II	0x0600	<i>(</i> )
MAC VLAN				
Protocol VLAN				
Surveillance VLAN				
GVRP				
EEE				
Multicast				

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.			
	Ethernet_II IEEE802.3_LLC_Other RFC_1042			
	Ethernet_II - Packet will be mapped based on Ethernet version 2. IEEE802.3_LLC_Other -Packet will be mapped based on 802.3 packet with LLC other header. RFC_1042 - Packet will be mapped based on RFC 1042.			
Protocol Value	Input a value (ranging from 0x600 ~0xFFFE). 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.			

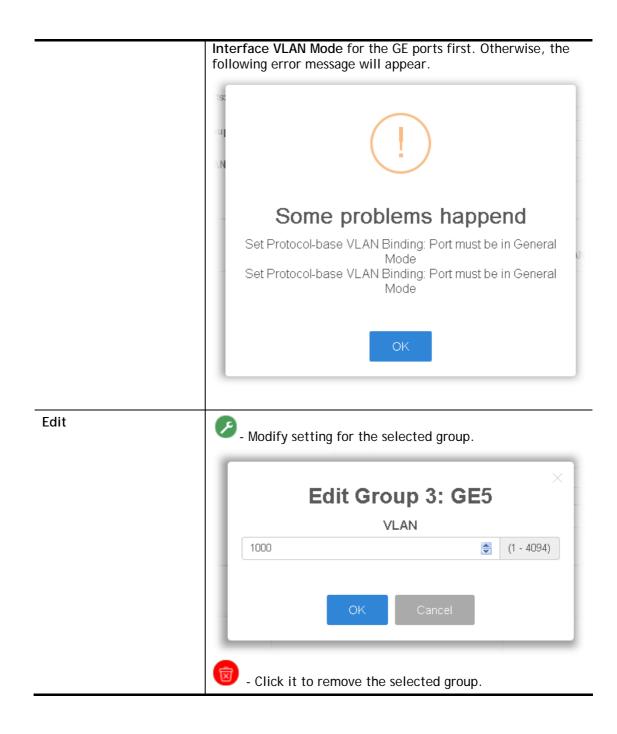
am	Edit	Group 1	×
oto	Fra	ame Type	
	IEEE802.3_LLC_Other		-
	Prof	tocol Value	
	(0x600 - 0xFFFE) 0x	0601	
	OK	Cancel	

## 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.

Auto Logout : 3 min 🖉					10:50:41
Dashboard	VLAN Management - Protocol V	CAN = Group Elinding			
Status -					
Switch (247	Protocol Group Group Binding				
General Setup	Ports:	Fample	ng pelysted.	-	
Print Setting	Group ID;	1		7	
Mirror					
Link Aggregation	VLAN:			\$	(1 4094)
VLAN Management			Add		
Croate Vlan					
Interlace Softings	Port	Group ID	VLAN	Edit	
Voice VLAN	GB5	3	1000	00	
NIAG-VILAN	GEB	\$	1000	00	
Protocol VLAN					
Soveillance VLAN					
GVRP					
ECE					
Molticast					

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



## 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.

Adda Lagoul : 🛛 🖉	La constante de la constante d				
Dashboard	Property Sur	veillance OUI			
Status	-				
EWITE LINE		state:	CEnabled Obisabled		
General Setup	- V	/LAN ID:	HDMIVLAN4067(4067)		
Port Setting		CoS/802.1p Remarking:	6		- Enable
Mirror		Aging Time:	1440		(30-65536 sec)
Link Aggregation			Appl	2	
VLAN Management					
Creale Vian	Port	State	Mode	17 DoS Policy	() Edit
Indentives: Settings	GE1	Disantes	Auto	Video Packet	0
VOICE VEAN	QE2	Disables	Auto	Video Packet	0
	0E3	Disables	Avito .	Video Packét	0
	064	Disables	Auto	Video Packet	0
	GES	Disables	Auto	Video Parket	0
	OE8	Disables	Auto	Video Packet	0
EEE	9E7	Disables	Auto	Video Packet	0
Molticiest	0E8	Disables	Auto	Video Packet	9
Jumbo Frame	0E9	Disaples	Auto	Videa Packet	0
STP	DE10	Disablen	Auto	Video Pacioji	0
MAC Address Table	OEIT	Disables	Auto	Video Packet	0

Item	Description
State	Enabled - Click it to enable the port settings for such VLAN. Disabled - Click it to disable the port settings for such VLAN.
VLAN ID	Choose a VLAN profile (created in Switch LAN>>VLAN Management>>Create Vlan) 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. Enable - If enabled, qualified packets will be remarked by this value.
Aging Time	Unit is second. Select value of aging time (30~65536 seconds). 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	Iclick it to modify port setting status.

> Surveillance VLAN -> Property
Edit port GE1
Edit port OET
State:
Disabled
Mode:
1 Auto -
QoS Policy:
Video Packet -
OK Cancel
State -Set it to enable surveillance VLAN function of interface. Mode -Select port surveillance VLAN mode.
<ul> <li>Auto: Surveillance VLAN auto detect packets that match OUI table and add received port into surveillance VLAN ID tagged member.</li> <li>Manual: User need add interface to VLAN ID tagged member manually.</li> </ul>
QoS Policy - Select port QoS Policy mode.
<ul> <li>Video Packet: QoS attributes are applied to packets with OUI in the source MAC address.</li> </ul>
• 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.

Auto Longut : Off 🛛 🕅	Born		05-27-34 🕞
Dashboard	Property Surveillance OV/		
Status	-		
See. 1.01	Oth Address:	110 Monto	
General Setup	Description:		
Port Setting		Add	
Mirror			
Link Aggregation	OUI Address	Description	Edit
VLAN Management		766 düta available in table	
Interface Settings			
MAC VLAN			
Protocol VIJAN			
OVAP			
EEE			
Muticast			
Jumbo Frame			
STP			
MAC Anniese Table			

Available settings a	e explained a	s 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	<ul> <li>Modify OUI setting for surveillance VLAN.</li> <li>Click it to remove the selected OUI entry.</li> </ul>

## 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.

tuto Logoist : Off 🛛 😹					05:37:39 🕞
Pashboard	Property M	embership			
Status	*				
with LATI		State:	OEnabled ODisabled		
General Betop		Timeout:	Join 20 ms		
ord Setting			Leave 60 ms		
litter			Leave All 1000 ms		
Link Aggregation			Appl	W)	
/LAN Management					
Create viso	Port	State	VLAN Creation	Registration	Edit
Interface Settings	OEt	Disables	Enabled	Normal	0
Voice VLAN	GEZ	Disables	Enabled	Nomial	0
MAC VLAN	QE3	Disables	Enabled	Nomial	0
Protocol VLAN	064	Disables	Enabled	Normal	0
Surveillance VI AN	0E5	Disables	Enabled	Normal	0
	GE6	Disphies	Enabled	Normal	0
EE	GET	Durabiyy	Enabled	Normal	0
	GEE	Disables	Enabled	Normal	0
fulticest	GE9	Disables	Enabled	Normal	0
umbo Frame	GE10	Disables	Enabled	Normai	0
ΠP	GE11	Disables	Enabled	Nomial	0
MC Address Table	and a second	1. Deciminant			

Item	Description		
State	Enabled - Click it to enable the port settings for such VLAN. Disabled - Click it to disable the port settings for such VLAN.		
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		
	State - Select Enabled or Disabled for such port.		

VI AN Creation Calact Enchlad on Dischlad
VLAN Creation -Select Enabled or Disabled.
Mode - There are three modes to be specified.
<ul> <li>Normal - Default setting. All packets can pass through the selected GE port.</li> </ul>
• Fixed - The selected GE port only sends static VLAN information to neighboring device and allows static VLAN packet to pass through.
<ul> <li>Forbidden - The selected GE port only allows default VLAN packet to pass through.</li> </ul>

## II-5-7-2 Membership

This page display information about membership for GVRP.

Auto Logout : 🛛 🖉		Admin		00-13:21 🕞
Dashboard	Property	lenjuentip.		
Status				
s - d li (Al)	VLAN	Member	Dynamic Member	Type
General Setup			No dată available în tâble	
Port Sotting				
Mirror				
Lick Aggrogation				
VLAN Management				
Create-Vlan				
Interface Settings				
MAG VLAN				
Professed VI. NV				
Sumiliance VLAN				
EEE				
Mollicad				

# II-6 EEE

Auto Logout : 01	<b>*</b>	Admin		17/28 A) 🕞
Dashboard	Switch LAN > EEE :	Emmy Efficient Ethomot Situp		
Status	*			
	Energy Efficient Ethernet	Switch		
General Setup	Port	Hapling	an ju en mel	
Port Setting	Enab	le: O Enable	Disable	
Mirror			Apply	
Link Aggregation				
VLAN Management	Port	Enable	Status	Modify
626	GE1	Disable	Disable	0
Multicast	.GE2	Disable	Disable	0
Jumbo Frame	GED	Disable	Disable	0
STP	GE4	Disable	Disable	0
MAC Address Table	GE5	Oisable	Disable	0
Blocked Port Recover	GEE	Disable	Disable	0
lecurity	GE7	Disable	Disable	0
NGL	GE8	Disable	Disable	0
005	GE9	Disable	Disable	0

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	Enable -Click it to enable the EEE function. Disable - Click it to disable the EEE function.
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.

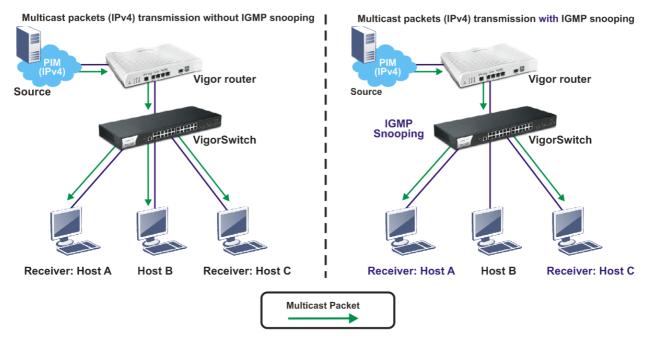
Auto Lognul : 📝	<b>M</b> .			thisas 🕞
Dashboard	Prop	entres		
Status		Unknown Multicast Action:	Obrop @Flood OForward to Router Port	
Switch Links	1	IPv1 Forward Method	@Dst. MAC & VID () Dst. IP & VID	
Oeneral Setup		IPv6 Forward Method	⊙Dst. MAC & VIDDst. IP & VID	
Port Setting				
Mirror		Apply		
Link Aggregation				
VLAN Management				
EEE				
Multicast				
Propertie				
IGMP Shaaping				
MVR				
NLD Sneeping				
Jumbo Frame				
STP				
MAC Address Table				
lecurity	-			
ICL.				
205				

Item	Description
Unknown Multicast Action	Select an action for switch to handle with unknown multicast packet.
	Drop- Drop the unknown multicast data.
	Flood- Flood the unknown multicast data.
	Forward to Router port- Forward the unknown multicast data to router port.
IPv4 Forward Method	Set the IPv4 multicast forward method.
	Dst. MAC & VID- Forward using destination multicast MAC address and VLAN IDs.
	<b>Dst. IP &amp; VID-</b> Forward using destination multicast IP address and VLAN ID.
IPv6 Forward Method	Set the IPv6 multicast forward method.
	Dst. MAC & VID- Forward using destination multicast MAC address and VLAN IDs.
	Dst. IP & VID- Forward using destination multicast IPv6 address

	and VLAN ID.
Apply	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.

Auto Logout : 🛛 🖉								09.26:10	
Dashboard	O Materiard	I ISMR Smith	ing + 69MR Sitting						
Status -	(Constanting of the local division of the lo		STREET, STREET	Supervised Super-			Service (Incompany)	(Conservation)	
Swinch LAN	IGMP Setting	and the second value of th	amin Satling IGMP	Static Group IGMP	Group Table IGMP	Router Table Forw	ard All Throttling	Filtuning Profile	
General Setup	Filtering Bindd	ng							_
Port Setting					Global Setting				
Mirror	1.1	IGMP Snoo	ning States	O Fre	ble O Disable				
Link Aggregation			ping Version:		© v3 (BISS)				
VLAN Management			ping Report Suppressio		ble O Disable				
EEE		Parer Shoo	hurd webour authresse		Apply				
Mülticast									_
Properties	-		_		VLAN Setting				
	Entry No.	VLAN ID	IGMP Snoopi	Router Ports	Query Robus	Query Interv	Query Max R	Last Member	14
MVR	1		Disabled	Enabled	2	125	10	2	1
MLD Shooping	8								
Jumbo Frame									
STP									
MAC Address Table									
Blocked Part Recover									

Item	Description
IGMP Snooping State	Enable - Click it to set enabling IGMP function.

	Disable - Click it to disable IGMP function.					
IGMP Snooping Version	Set the IGMP snooping version.					
	v2 - Only support process IGMP v2 packet.					
	v3 (BISS) - Support v3 basic and v2.					
IGMP Snoopign 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	Click it to modify IGMP settings for selected profile. However, if IGMP Snooping State is not set as Enable, such option will be disabled.					
	Edit VLAN ID 1					
	IGMP Snooping State					
	Disable -					
	Router Ports Auto Learn					
	Enable •					
	Query Robustness (Operational: 2)					
	2 (1-7, default 2)					
	Query Interval (Operational: 125)					
	125 Sec (30-18000, default 125)					
	Query Response Interval (Operational: 10)					
	10 \$ Sec (5-20, default 10)					
	Last Member Query Counter (Operational: 2)					
	2 Sec (1-7, default 2)					
	Last Member Query Interval (Operational: 1)					
	1 Sec (1-25, default 1)					
	Immediate Leave:					
	Enable -					
	ec OK Cancel					
	IGMP Snooping State -Choose Enable to enable IGMP snooping function. Router Ports Auto Learn - Set the enabling status of IGMP					
	<ul><li>router port learning. Choose Enable to learn router port by IGMP query.</li><li>Query Robustness - Set a number which allows tuning for the set of the set of</li></ul>					
	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 quering 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.

Auto Lougut 1 Off 🛛 🖄		Admin						11:22:41	Ð	
Dashboard	IOMP Setting	IOMP Querier Setting IOMP 9	tatic Group Table	IOMP Router Table	Forward All Throttling	Fittering Profile	Fatering Binding			
Status -	Contraction of the local division of the loc		Statements in the second second		Support Statement					-
eneri per		VLAN ID:	evenue a elected				- 0			
General Setup		Querier State:	O Emable O Disable							
Part Setting		Querier Version:	⊙v2: ⊖v3 (BISS)							
Mirnor				Apply						
Link Appregiation	· · · · ·									
VI.AN Management	VLAN ID	Ouerier State	Quarier Sta	tus	Querier Version		0 Querie	IP.		
EEE	1	Disabled	Disabled		-		-			
Mutteast	4087	Disabled	Disabled		-		-			
Properties	4058	Disabled	Disabled							
	4069	Disabled	Disabled		0-0		-			
MV77	4070	Dissbied	Disabled		-		1			
MLE Shooping	4071	Disabled	Disabled				1.000			
Jumbo Frame	4073	Disabled	Disabled		3		~			
STP	#073	Disabled	Disabled		-		-			
MAC Address Table	4074	Disabled	Disabled		-		-			
	4075	Disabled	Disabled		-		1			
ter or of	4078	Disabled	Disabied		-		~			
766	4(177	Disabled	Disabled		-					
205 -	4070	Disabled	Disabled		-					

Item	Description	
VLAN ID	Use the drop down list to specify a VLAN profile as IGMP Snooping querier.	
Querier State	Enable - Click Enable to set the enabling status of IGMP Querier on the chosen VLAN profile. Disable - Click it to disable the function.	
Querier Version	Set the query version of IGMP Querier Election on the chosen VLANs. v2 - Querier version 2. v3 - Querier version 3. Note: For maximum compatibility, it is suggested to use querier version lower than IGMP snooping version, for there is possibile network mixed with IGMP v2/v3 client and v2 query message is widerly 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.

Auto Logout ; Of	Admin 09.00.38 🕞
Dashboard	O Multicart > IGMP Sonophing = IGMP Salur Group
Status -	IGMP Setting IGMP Querer Setting IGMP State Group I GMP Group Table IGMP Router Table Forward All Throttling Filtering Profile Filtering Binding
Switch LAN	IGMP Setting IGMP Querier Setting IGMP State Group IGMP Group Table IGMP Router Table Forward All Throttling Filtering Profile Filtering Binding
General Setup	VLAN ID: Faithing proceded
Port Setting	Group IP Address:
Mirror	Member Ports: Dotting released
Link Aggregation	
VLAN Management	(App)
EEE	
Multicast	VLAN ID Group IP Address Member Ports Modify
Properties	No riata available in table
IGMP Strangeron	
MTV7Y	
MLD Sheeping	
Jambo Frame	
SIP	
MAC Address Table	
Blocked Pod Recover	

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.
	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.

Anto Logout : 🖓						na	29:30 CH
Dashboard	O Multicant > 1	GMP Shooping + IGMP Group Table					
Status.	and the second second		Contraction of the	GMP Router Table	Second Second		and the second
Sweeting	IGMP Setting	IGMP Quener Setting IGMP Static Group	IGMP Group Table	GMP Roder Table	Forward All Triro	ttling Filtering Profile	Filtering Einding
General Setup	VLAN ID	Group IP Address	Member Ports	1.012	Type	Life(sec.)	1
Port Setting			No data avai	able in table			
Metter							
Link Aggregation							
VLAN Management							
EEE.							
Multicast							
Properties							
MVR							
MLD Snooping							
Jumbo Frame							
STP.							
MAC Address Table							
Flocked Port Recover							

Item	Description
VLAN ID Display the VLAN of this multicast group belongs t	
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.
Туре	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.

Auto Logout : 📝 🕅 🛒		Admiri					09 30-28 🕞
Dashboard	O Material > ISM	P Souchag = IGMP Router Te	ble				
Status -	-	SCHOOL STREET,		Concernation of the			Constanting of the
Iwites Law	IGMP Setting	GMP Querier Setting IGM	IP Static Group IGMP Group Table	IGMP Router Table	Forward All The	ottling Filtening Profile	Filtering Binding
General Setup	VLA	N ID:	Thisting selected				
Port Setting	Type	e:	💿 Static 🔿 Forbidden				
Mirror		nber Ports.	Nillform colucted				
Link Aggregation				-			
VLAN Management				Ad			
EEE	and the second		Static Port	Forbidden Por			Edit
Multicast	VLAN ID	Port			τ Εχριγγ	Time(sec.)	Edit
Properties			140 da	a available in table			
MVR							
Jumbo Frame	· · · · · ·						
STP							
MAC Address Table							
Placked Port Recover							

Item	Description
VLAN ID	Use the drop down list to specify a VLAN profile (created in Switch LAN>>VLAN Management>>Create VIan) that the MLD querier belongs to.
Туре	Static - Specify LAN Port (GE/LAG) to send out query to remote host.Forbidden - 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.

Auto Lopout : 🛛 🖉		Donts						0548.93 🕞
Dashboard	(GMP Setting	IGMP Quener Selling	IGMP State Group	IGMP Group Table	KIMP Router Table	Forward All The	ottling Filtering Profile	Filtering Binding
Status	-							
ÈMINTI LAN		Available VLAN:		Parcenge (witholder)				1
General Setup		Static Ports:		mattering waterbed				7
Port Setting		Forbidden Ports:		Nothing polacted				4
Mirror					Add			
Link Aggrégation								
VLAN Management	VLAN	Ú.	Static Port		E Forbidd	en Port		D Edit
333	- 1		061-065		GE11-GE	10		00
Multicest	4067		0E1-965		GE11-GE	15		00
Frapetties	4060		061-055		0611-06	15		00
	4069		061-065		GE11-GE	15		00
	4076		QE1-GE5		GE11-GE	15		00
MLD Shooping	4071		0E1-GE5		GE11-GE	15		00
Jumbo Frame	4072		081-085		0E11-0E	15		00
STP	4073		061-065		OE11-OE			00
MAC Address Table								
Blocked Ford Recover	4074		0E1-0E5		GE11-GE			00
Security	4075		QE1-0E5		QE11 QE			e 😳 😡
AÓL	4076		0E1-0E5		GE11-GE	15		Ø.0

Item	Description
Available VLAN	To display all of the available VLAN, the State must be set as Enabled in MLD Setting first.
	Use the drop down list to specify a VLAN profile (created in Switch LAN>>VLAN Management>>Create Vlan) that multicast packets will be forwarded to.
Static Ports	Use the drop down list to specify LAN Port (GE/LAG). 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). 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	<ul> <li>Click it to modify port setting (static port and forbidden port).</li> <li>Click it to remove the selected entry.</li> </ul>

### 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 <u>can join</u>. 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.

Anto Logout 2 Ori 🔍		Honi						066501	Ð
Dashboard	(GMP Setting	IGMP Querier Setting	IGMP Static Group	IGMP Group Table	IGMP Router Table	Forward All Throttling	Filtering Profile Filterin	g Binding	
Status -							The second second		
www.enilari		Ports:		Nerros searcad			-		
General Setup		Max Group:		256			\$	(0 - 256)	
PortSetting		Exceed Action:		Deny OReplace					
Mirrór					Apply				
Link Aggregation									
VLAN Management	Port	dif (M	ax Group		Exceed Ar	tion		Edit	
EEE	OEI	2	56		Detty			0	
Multicast	GE2	.2	56		Deny			0	
Properties	OE3	2	58		Dény			0	
	GE4	2	56		Dony			0	
MVH	OE5		56		Deny			0	
MLD Snaping	OE6	2	50		Deny			0	
Jumbo Frame	0E1	2	56		Empy				
8TP	0E6	3			Deny			0	
MAC Address Table	OEA	2			Deny			0	
Blocked Port Recover.	0E10	2			Deiny			0	
Security -	OE11	2			Dieny			0	
2.16.2.171.2280/#ab-bals7	0617	2	SR		Denv			0	

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. Deny - It is default setting. The IGMP join report (for multicast service) received by such interface will be discarded. Replace - When it is selected, a new group with IGMP report received will replace the existing group.
АррІу	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.

Auto Logout : 🛛 🕬	<b>×</b>	Admin			usw.si 🕞
Dashboard	O Multicast is IGMP Snr	ioping is Filtening Pimilia	1.1.1.1.1.1.1		The second s
Status	IGMP Setting IGMP	Quesier Setting IGMP Static I	Group IGMP Group Table IGMP F	Router Table Forward All Th	Filtering Profile Filtering Binding
	ISMP Setting	Commit Serung	HOMP CHINE HANN	Tooser Inoine Forward Ad	nonaniti i i i inaniti i i inaniti paraniti
General Setup	Profile ID		Friter Profile (D		¢ (1 - 120)
Port Setting	Start Add	1855	254.0 0.1		
Mirror	End Addr				
Link Aggregation			224.0.0.2		
VLAN Management	Action:		Allow O Deny		
EEE			Add		
Multipast					
Properties	Profile ID	Start Address	End Address	Action	Edit
	1	224.0.0 1	224.0.0.2	Allow	00
MVR	2	224 0.0 10	224 0 0 20	Allow	C 🔘
MLD Snooping					
Jumbo Framo					
STP					
MAC Address Table					

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> <li>Deny - It is default setting. The forwarding request of multicast traffic will be discarded.</li> <li>Allow - 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).

Ec	it Profile 1
	Start Address:
224.0.0.1	
	End Address:
224.0.0.2	
	Action:
Allow	•

### 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.

Anto Logout 🗧 🞯 🖉	1.1	Boot						00:02/15	B
Dashboard Status -		GMP Querier Setting	IGMP Static Group	IOMP Group Table	IGMP Router Table	Forward All Throttl	ing Filtering Profile	Fillening Binding	_
Ganters (Jack	Po	rts:		Annual services					
General Setup	Pre	ofile ID:		Long to Long A				Enable	
Port Setting Million					(Apply)				
Link Aggregation	Port		11.1	tofile ID				dit	
VLAN Management	OE1							0	
EEE	OE2							D	
Multicast	0E3							D	
Properties	0E4			-				2	
	055			-				D	
MVR	066		-	-				D	
MLD Snacping	OE7			-				0	
Jumbo Frame	OE8		-	-				0	
BTP	OE9			-				B	
MAC Address Table	GETO			-				B	
Blocked Port Recover.	GE11							B	
Security -	OE12		2	-				Ð	
2 16 2 171 2200 995 6459	0613			-				2	

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.
	<b>Enable -</b> Check this box first to make profile ID selection be available for choosing.
АррІу	Apply the settings to the switch.
Edit	Click it to modify port setting (enabling / disabling filter function and choosing a profile for such interface).

	Edit Port GE1	>
	Filter:	
Enable		-
	Profile:	
1		•
	OK Cancel	

### 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.

Auto Logout : 🔐 👻	Admin		2342-18 🕞
Dashboard Status -	Mutchad > MVR > Property Property Port Setting Group Address		
General Setup		Property Settings	
Port Setting Mittor Link Aggregation VLAN Management EEE	State: VLAH ID: Mude: Group Start:	© Enabled ○ Disabled defacil(1) - © Competible ○ Dynamic DO.070	
Multicast	Group Count:	1 🖉	(1.128)
Properties IGNP Shapping MYP	Query Time:	a Chaire	(1-10 sec)
MLD Seneping		Operational Group	
uumbo Frame STP MAC Address Table	Maximum Current	126 a	

Item	Description
State	Enabled - Click it to enable the MVR function. Disabled - Click it to disable the MVR function.
VLAN ID	Choose one VLAN profile (defined in VLAN Management>>Create VLAN) from the drop down list as multicast source VLAN which will receive multicast data. The default is VLAN 1. Note: Each VLAN ID shall be configured with group address and member port (defined in MVR>>Group Address page).
Mode	There are two modes offered for MVR operation. <b>Comaptible -</b> Multicast data received by MVR hosts (multicast server) will be forwarded to all MVR receiver ports. <b>Dynamic -</b> Multicast data received by MVR hosts (multicast server) on Vigor switch will be forwarded from those MVR

	data and client ports grouped under MVR server.
Group Start	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.
Group Count	Select a number to configure a contiguous series of MVR group addresses (the range for count is 1 to 128; the default is 1).
Query Time	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.
Apply	Apply the settings to the switch.
Operation Group	Display group information for MVR.

### 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.

kata Logout : 🔐 👷	1. Sec. 1.			00-10-35 🕞
Dashboard	Property Pog Selling	Group Addrase		
Status				
Sheeka I Alama	Ports:		Frathing selected	
General Setup	Role:		⊙Nose ⊜Receiver ⊜Source	
Port Setting	Immediat	e Leave:	CEnabled Obsabled	
Mirror			Aboty.	
Link Aggregation	-			
VLAN Management	Port	Bale	13 Immodiate Leave	Eda
EEE	OE1	None	Disabled	0
Multicast	0E2	None	Disabled	0
Properties	OE)	None	Disabled	0
IOMP Shooping	OE4	None	Disabled	0
	GE5	None	Disabled	0
MLD Smidping	OE6	None	Disabled	0
Jumbo Frame	OE7	None	Disabled	0
STP	GE8	Mone	Disabled	0
MAC Address Table	OE9	None	Desabled	0
Blocked Port Recover	0E10	None	Disabled	0
Security	0E11	None	Disabled	0
	OE12	None	Denabled	0

Item	Description
Ports	Use the drop down list to select LAN Port (GE/LAG). Later, each port can be set as Recevier or Source port respectively. If you do not satisfy with the port setting, simply click the Edit button to make the modification.
Role	None - Noting will be happed to the selected LAN port in MVR operation.
	<b>Receiver</b> - The selected port will be treated as destination port which will receive multicast data from the multicast server.
	<b>Source -</b> The selected port will be treated as source port which will send multicast data to the receiver port.
Immediate Leave	<b>Enabled</b> - Enable the function fo immediate leave. When the port (with the role of receiver) receives the leave message, it will be removed from multicast group to speed up leave latency.

	Disabled - Disable the function of immediate leave.
Apply	Apply the settings to the switch.
Edit	Click it to modify port setting (role and immediate leave).

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

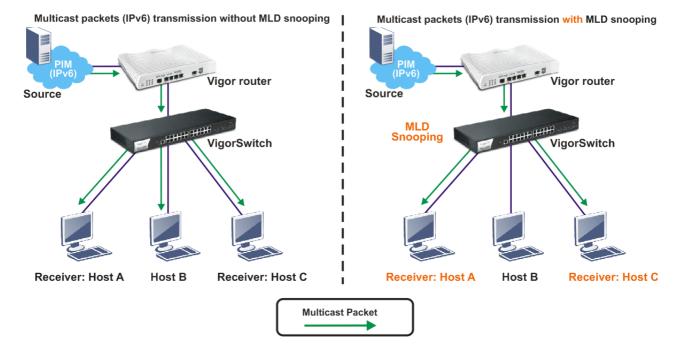
This page allows the network administrator to configure IP address and specify port member for VLAN selected in MVR>>Property page.

Auto Logost : 07 🔗		Эрил				on to M
Dashboard	Property	Port Sritting Group Address				
Status						
		VLAN ID:	1			
General Setup		Group Address:	1			(0.0.0.0 - 0.0.0.0)
Port.Setting		Member:	hitemay assessed.			-1
Mirror			Addr			
Link Aggregation						
VLAN Menagement	VLAN	Group Address	Member	Туре	Life (Sec.)	Eat
EEE			No data availat	ble in Tuble		
Multicast	1					
Properties						
IONP Shooping						
MLD Bhooping						
Jumbo Frame	1					
STP						
MAC Address Table						
Blocked Port Recover						
Security	-					
ACL						

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

kato Logout : Off 🛛 🖳										
kashiboard Natus -	MLD Setting	MLD Static Group	MLD Group Table	MLD Router Tabl			Filtering Profile Filter	ing Binding		_
witth LAN					Prop	serty Settings				
General Setup		State:		Ofnabled ()	Disabled					
Port Setting		Version:		OMLOVI OM	LDv2					
Mirróz		Report Suppression:		CEnabled GI	Disabled					
ink Aggregation						Aprily				
AAN Manugement						_				
tee					V1	AN Belling				
Multicast	1	MLD Snooping	Router Port	Query	Query	Query Max	Last Member	Last Member		
Properties	VLAN ID	Operational Status	Auto Learn	Robustness		Response Interval	Query Counter	Ouery Interval	Immediate Leave	Edit
IGMP Shapping	1	Disabled	Enabled	2	125	10	2	1	Disables	0
MVP	4067	Disabled	Enabled	\$	125	10	2	24	Disables	0
NLD Sharding	4068	Disabled	Enabled	2	125	10		-1	Disables	0
umbo Frame	4069	Disabled.	Empbled	1	125	10	2	1	Disables	0
TP	4070	Disabled	Enabled	2	125	10	2	4	Disables	0
AAC Address Table	4071	Disabled	Enabled	2	126	10.	2	1	Disables	0
locked Port Recover	4072	Disabled	Enabled	2	125	10	2	1	Disables	0
	407.2	Dicabled	Enabled	2	125	10	2	-1	Disables	0
ecurity -	4074	Treaters	Enabled	2	125	10		4	Elicables	0

Item	Description
State	Enabled - Click it to enable the MLD snooping function.

	<b>Disabled</b> - Click it to disable the MLD snooping function.
Version	VigorSwitch supports two versions of MLD snooping. MLDv1 - When it is selected, VigorSwitch will detect packet controlled by MLDv1 and <i>bridge</i> the traffic to IPv6 destination defined with multicast address(es).
	MLDv2 - When it is selected, VigorSwitch will detect packet controlled by MLDv1 and <i>forward</i> the traffic to destination defined with multicast address(es).
Report Suppression	<ul><li>Enabled - Click it to allow the switch to handle MLD reports between router and host, suppressing bandwidth used by ML</li><li>Disabled - Click it to disable the function.</li></ul>
Apply	Click it to display the result based on the settings configured above.
Edit	Click it to modify the settings for the selected VLAN IE (GE/LAG port).
	Edit VLAN ID 1
	MLD Snooping State
	Disable
	Router Ports Auto Learn
	Enable
	Query Robustness (Operational: 2)
	2 (1-7, default 2)
	Query Interval (Operational: 125)
	125 🗘 Sec (30-18000, default 125)
	Query Response Interval (Operational: 10)
	on 10 🗘 Sec (5-20, default 10)
	Last Member Query Counter (Operational: 2)
	2 Sec (1-7, default 2)
	Last Member Query Interval (Operational: 1)
	1 Sec (1-25, default 1)
	Immediate Leave:
	Disable
	OK Cancel
	MLD Snooping State - Enable/disable the MLD snooping function for the selected port. Router Ports Auto Learn -Set the enabling status of IGMP router port learning. Choose Enable to learn router port by

<b>Query Robustness</b> - Set a number which allows tuning for the expected packet loss on a subnet.
<b>Query Interval</b> - 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 quering 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.

Auto Logaut : 🔐 👷		Во	ng.							06/20:23	ē
Dashboard	MLD Setting	MLD Status Group	MLD Oroup Table	MLD Route Table	Forward All	Throtting	Filaning Profile	Filaning Biniting			
Status -	-	and the second s									
CHARLEN (		VLAN ID:		mindling satisfield	σ				- 1		
General Setup		Group IP Address:									
PortSetting		Member Ports:		Ardiney	α.						
Mirror					0	non					
Link Appregation											
VLAN Management	VLAN ID		Group IP Address			E Mer	mber Ports		L(	Modify	
EEE					No data ava	allable in table					
Multicast											
Properties											
IOMP Shooping											
MVR											
10.25 Encoderes											
Jumbo Frame											
STP											
MAC Address Table											
Blocked Port Recover											
Security -											
ACL -											

Item	Description
VLAN ID	Use the drop down list to specify a VLAN profile (created in Switch LAN>>VLAN Management>>Create VIan) as MLD Static Group.
	However, if State in MLD Setting is not set as Enabled, such option will be disabled and no ID can be selected.
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. Specify the IPv6 multicast address you wish to assign for the static group (defined in VLAN ID).
Member Ports	Use the drop down list to specify interaces (GE/LAG) for receiving the packets from group IP address.
Add	Click it to display the result based on the settings configured above.

#### 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.

Auto Logical : 🛛 🐨 🖉		Both					00:31.41	Ð
Dashboard	MLD Setting	MLD Static Group	Imup Table MLD Rou	er Table Fotward All The	rottling Filtering Profile	Filtering Binding		
Status -		And a state of the	a second	and a subscription of the				
ientruga -	VLAN ID	Group IP As	dress	Member Ports		Type	1.nn(sec.)	
Öeneral Setup				No data availab				
Polt Setting								
Mirrot								
Link Augrepation								
VLAN Management								
EEE								
Multicast								
Properties								
(QM≢ Sneeping								
MOR								
MLTI Prooping								
Jumbo Frame								
STP								
MAC Address Table								
Blocked Port Recover								
Security -								
ACL ·								

Item	Description
VLAN ID	Display the name of VLAN configured in MLD Static Group.
Group IP Address	Display the IP adderss defined in MLD Static Group.
Member Ports	Display all of the interfaces defined in MLD Static Group.
Туре	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).

Auto Lopout : 🛛 😁 🛛 😿		Rot	1997 - C. 1997 -							66.33.35	Θ
Dashboard	MLD Setting	MLD Static Group	MLD Group Table	MLD Router Table	Forward All	Throttling	Filtering Proteia	Filtening Binding			
Status -	-				-						
Renario UAN.		VI. AN ID:		matring united	d				+		
General Setup		Type:		Static OForbid	idèci						
Port Betting		Member Ports:		beaming polocia	n.						
Mirror						Ada					
Link Aggregation	1.5										
VLAN Management	VLAN ID	Port	Static	Port	Forbidde	n Port		Expiry Time(sec.)		- 0	Edit
EEE					No data av	allable in table	9				
Muticant											
Properties											
10MP Shooping											
MVR											
Multi Onuciump											
Jumbo Frame											
<b>STP</b>											
MAC Address Table											
Blocked Port Recover											
Security -											
3 16 23 77 2280468-6664											

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.
Туре	<ul> <li>Static - Specify LAN Port (GE/LAG) to send out query to remote host.</li> <li>Forbidden - 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.
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 it to modify the settings for the selected entry.

Static Port: GE1, GE2, GE3
GE1, GE2, GE3
Forbidden Port:
Nothing selected

#### 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.

Auto Logoul : Cit 📧		Bón	5							06.8691	G
Dashboard	MLD Setting	MLD Static Group	MLD Group Table	MLD Router Table	Forward All	Throttling	Filtering Profile	Filtering Binding	1		
Status -											
Theise LAN		Available VLAN:		faithing palatette	a,						
General Setup		Static Ports:		(date-o) - etc. to	a						
Port Setting		Forbidden Ports:		Nothing colects	α						
Mirror						Add					
Link Aggregation					_						
VLAN Management	VLAN		Static Port			Forbidden Pa	ort			T) East	
EEE					Nó data av	vailable in table					
Muticast											
Properties											
IGMP Shooping											
MVR											
Jumbo Frame											
9TP											
MAG-Address Table											
Blocked Port Recover											
Security -											
121 16 9 191 9200 mile-612-6											

Item	Description
Available VLAN	To display all of the available VLAN, the State must be set as Enabled in MLD Setting first.
	Use the drop down list to specify a VLAN profile (created in Switch LAN>>VLAN Management>>Create VIan) that multicast packets will be forwarded to.
Static Ports	Use the drop down list to specify LAN Port (GE/LAG).
	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).
	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	<ul> <li>Click it to modify port setting (static port and forbidden port).</li> <li>Click it to remove the selected entry.</li> </ul>

#### 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 <u>can join</u>. 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.

Auto Logout : 🛛 👷								
Dashboard Status -	MLD Setting	MLD Static Group	MLD Group Table	MLD Router Table	Forward All Throming	Filtering Profile Filtering Binding	-	
Swien LAN	1	Ports:		Nettong addresses				
General Setup		Max Group:		258			2	(0 - 256)
Port Setting		Exceed Action:		Deny      Replace				
Mirror					Apply			
Link Aggregation								
VLAN Management	Port	10	Max Group		Exceed Act	lition		LI Edit
EEE	GE1		256		Deny			0
Multicast	GE2		256		Сних			0
Fréderties	GE3		256		Deny			0
IOMP Shooping	QE4		256		Deny			0
	OE5		256		Dieny			00
MLD Drokolna	OEB		256		Deny			0
Jumbo Friame	GE7		/58		Deny			0
STP	0E8		266		Dony			0
MAC Address Table	OE9		256		Denv			0
Blocked Port Recover	OE10		256		Deny			0
lecuity -	OE11		256		Dietty			0
21621912200965-6666	GET2		25ñ		Deny			0

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	VigorSwitch will perform the action defined below when the number of MLD join report for the specified interface exceeds value defined in Max Group.
	<b>Deny</b> - It is default setting. The MLD join report (for multicast service) received by such interface will be discarded.
	<b>Replace -</b> When it is selected, a new group with MLD report received will replace the existing group.
АррІу	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 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 traffic. It has nothing to do with the general MLD query.

Auto Logout : 🛛 🖉		Admin			053639 🕒
Dashboard	Multicast > MLD Snoo	ang = Filtering Profile			
Status -	Entering Franks	and the second second	Description of the second		The second second
Swatch GAN	MLD Setting MLD St.	MLD Group Table	MLD Router Table Forward All	Throttling Filtening Profile	Filtering Binding
General Setup	Profile ID:		Port Public ID		= (1 - 120)
Port Setting	Start Addre	55:	8F02:1		
vlirror	End Addres				
ink Aggregation	End Addres	a.	FF02:2		
/LAN Management	Action:	۲	Allow O Deny		
566	A		bnA		
Multicard	1.5.5				
Properties	Profile ID	Start Address	End Address	Action	Edit
IGMP Shocoing	2	102.1	1102_2	Allow	Ø 📵
MVR					
lumbo Frame					
STP-					

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> <li>Deny - It is default setting. The forwarding request of multicast traffic will be discarded.</li> <li>Allow - 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	I 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.

Aato Logaat : 🛯 🖉 🖉	Boni		06.41.09 🕞
Dashboard	MLD Setting MLD Static Group	MLD Group Table MLD Router Table. Forward All Throttling	Filtering Profile Filtening Binding
Status	-		
	Ports:	Nothing a elector.	7
Géneral Sétup	Profile ID:		Enable
Port Setting		Appy	
Link Aggregation	Port	11 Profile ID	Eat
VLAN Management	0E1	***	0
EEE	0E2		0
Multicast	061	~	0
Properties	054	-	0
IOMP Shooping	GE5	Profile ID	0
MVR	OEQ	-	0
	067		0
Jumbo Frame	OES		0
STP	080		0
MAC Address Table	0.610		0
Blocked Port Recover	OEIT	-	0
Security	- GE12		0
	QE13	~	0

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.
	Enable - Check this box first to make profile ID selection be available for choosing.
АррІу	Apply the settings to the switch.
Edit	Click it to modify port setting (enabling / disabling filter function and choosing a profile for such interface).

	Edit Port GE1	>
	Filter:	
Enable		-
	Profile:	
1		•
	OK Cancel	

# II-8 Jumbo Frame

Auto Logout : 08	~	Admini			00.08.28
Dashboard	0 =	wich LAN in Jonda Prama in Jumba Prama Sittin	a.		
Status	-	Concerning and the second s			
Switch LAVE	Jume	e Frame Setting			
General Setup		Jumbu Frame (Bytes):	1626	2	(1526-9216)
Port Setting		(Dame)			
Mirror		(Addiy.)			
Link Aggregation					
VEAN Management					
EEE					
Multicant					
STP					
MAC Address Table					
Blocked Port Recover					
Security	÷				
ACL	-				
DoS					

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

Item	Description
Jumbo Frame (Bytes)	Enter Jumbo frame size. The valid range is 1526 bytes - 9216 bytes.
АррІу	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.

Zuto Logout : Off	Admin	ar ta an
Dashboard	Switch LAN - STP - Properties	
Status	Properties Fort Setting Endge Setting Fort Advanced Softing Statistics MST Instance MST	Port Setting
General Setup Port Setting Minor Link Aggregation VLAN Management	STP Made: © Disabled © STP © NSTP © MSTP BPDU Handling: © Filtering PathCost Method: © Short @ Long	
EEE Multicast Jumbo Frame		
MAC Address Table Blocked Port Receiver		
Security ACL	*	
0.oS		

Item	Description
STP Mode	Set the operating mode of Spanning Tree (STP). Disabled - Disable the STP operation. STP - Enable the Spanning Tree (STP) operation. RSTP - Enable the Rapid Spanning Tree (RSTP) operation. MSTP - Enable the Multiple Spanning Tree Protocol (MSTP) operation.
BPDU Handling	Specify the BPDU forward method when the STP is disabled. Filtering - Filter the BPDU when STP is disabled. Flooding - Flood the BPDU when STP is disabled.

PathCost Method	Specify the path cost method. Long - Specifies that the default port path costs are within the range: 1~200,000,000. Short - Specifies that the default port path costs are within the range: 1~65,535.
АррІу	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.

Auto Logout : Off	1	Admin		08 10 50 🕞
Dashboard		O thetch LAN + BTP + Port Setting		
Status.		Properties Port Setting Bridge Setting	Port Advanced Setting Statistics MST Instance MST Port Setting	
	-1	Properties Port Solling Bridge Setting	Port Advanced Setting Statistics MST Instance MST Port Sulling	
General Setup		Ports:	Nations assessed	
Part Satting		Path Cost @ - Auto):	3	
Merror		Priority:	128	1
Link Aggregation				
VLAN Management		Edge Port:	O Yes 💿 No	
EEE		P2P Option:	· ③ Auto ○ Yes ○ No	
Multicast		BPDU Filter:	Tes .	
Jumbo Frame		BPDU Guard:	🗇 Yes	
SIR			App <sup>2</sup> y	
MAC Address Table				
Blocked Port Recover		Ports:	patients protection	
Security			Mignate	
ACL	÷			
QoS		Port II Admin Enable II Path Cost	Priority Edge Port P2P Option BPDU Filter	BPDU Guard Edit

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	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. Yes - Enable the function. No - Disable the function.
P2P Option	<ul> <li>Auto - VigorSwitch determines the STP of link type for this port automatically.</li> <li>Yes - It means the STP of link type on this port is full-duplex and directly connect to another switch or host.</li> <li>No - It means the STP of link type on this port is "not"</li> </ul>

	full-duplex and "does not" directly connect to another switch or host.						
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.						
АррІу	Apply the settings to the switch. 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 Migrate.						
Migrate	Click it to force the port(s) specified above to send one RSTP BPDU (Rapid Spanning Tree Protocol Bridge Protocol Data Unit).						
Admin Enable	YES - Such port is managed by VigorSwitch.						
Edit	Click it to modify the settings for the selected GE port.           Edit Port GE1						
	Path Cost (0 = Auto)						
	0						
	Priority						
	128 *						
	Edge Port						
	No ·						
	P2P Option						
	Auto -						
	BPDU Filter: TYes						
	BPDU Guard:  Yes						
	th OK Cancel D						

## 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.

Auto Logout : 💴	*	Admin				08:32.4/ E
Dashboard		O Switch (LAV) > STP > Budge Setting		the second s		
Status			Contractor of French	A Description of the second second		
Smith LAN		Properties Port Setting Bindge Setting	Port Advanced Setting Statistics	MST Instance MST Part Setting		
General Setup		Priority:	32768			
Port Setting		Forward Delay:	15			(4-30)
Merce		Max Age:				(6.40)
Link Aggregation			20		2	(6-40)
VLAN Management		Tx Hold Count:	3		2	(1-10)
EEE		Bello Time:	2		2	(1-10)
Multicast.				Apply		
Jumbo Frame						
		Bridge Identifier		32768/ 0/00 1D AA 0C CD 08		
MAC Address Table		Designated Root Bridge		0/ 0/00 00 00 00 00 00		
Blocked Port Recover		Root Path Cost		0		
Security		Designated Bridge		0/ 0/00:00 00:00:00:00		
ACL		Rost Port		0/0		
QoS	-	Max Hops		20		

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 10 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.

Auto Logout : Off	-			Admin							5.27 D	
Dashboard		O the	th LAN > STP > I	fort Advanced Set	ing.							
Status.		all succession of			In the second		Correspondent (	and the second second				
Switch LAN	-	Properti	Port Settin	g Bridge Sett	Port Advanced	Sutting Statistics	MST Instance	MST Port Setting				_
General Setup			Indentitier	Path Cost				Edge Port	P2P Option			
Part Setting		Port	(Priority/ID)	Conf/Oper	Designated	Root Path Cost	Designated	Conf/Oper	Conf/Oper	Port Role	Port State	Ec
Meror		GE1	128./ 1	0/20000	0/00/00/00/00	n	0 / 00 00 00 00 0	No / No	Auto / No	Disated	Disabled	G
Link Aggregation		GE2	128/2	0/20000	0/00.00.00.00.0	0	0/00/00/00/00.0	No 7 No	Auto / Yes	Disabed	Forwarding	4
VLAN Management		GE3	128/3	0720000	0/00:00:00:00.0	Ø	07000000000	No / No	Auto / No	Disabed	Disabled	G
EEE		GE4	128/4	0/20000	0/00/00/00/00/0	0	0/00/00/00/00/0	No / No	Auto / No	Disabed	Disabled	G
Multicast		GE5	128/5	0/20000	0/00:00:00:00:0	0	0 / 00,00,00,00 0	No / No	Auto / No	Disabed	Disabled	6
Jumbo Frame		GE5	12876	0/20000	0 / 00 00 00 00 0	0	0 / 00 00 00 00 0	No / No	Auto / No.	Disabed	Disabled	G
		GE7	128/7	0/20000	0/00.00.00.00.0	0	0/00/00/00/00.0	No / No	Auto / No	Disabled	Clisabled	4
MAC Address Table		GEB	12878	0/20000	0.00.00.00.00.0	0	0/00/00/00/00/0	No / No	Auto / No	Disabed	Disabled	6
Blocked Port Recover		GE9	1287.9	0/20000	5/00/00/00/00.	0	0/00/00/00/00/0	No / No	Auto / No	Disabed	Disabled	6
Security		GE10	128/10	0/20000	0/00/00/00/00.0	0	0700.00.00.00.0.	NO/NO	Auto 7 No	Desabed	Disabled	G
VCL.		GETI	1287.11	0/20000	0.00.00.00.00.0	0	0 / 00 00 00 00 0	No / No	Auto / No.	Disabed	Disabled	4
DoS		GE12	128/12	8/20000	0 / 00 00 00:00 0	0	0/00.00.00.00.0	No / No	Auto / No	Disabed	Disabled	G

Item	Description
Port	Display the interface number for GE and LAG.
Indentifier(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.

Designated 🚦	Designated 👔 Root Path Cost 👔	Path Cost Conf/Oper 🎼	Indentifier (Priority/ID) 🂵
×		0 / 20000	128 / 1
1	Edit Port GE1	0 / 20000	/2
	Priority	0 / 20000	3
· ·	28	0 / 20000	
		0 / 200000	
	OK Cancel	0 / 20000	6
		0 / 20000	7

## II-9-5 Statistics

This page displays STP statistics.

Auto Logours Off	2		Admin				G#
Dashboard		Switch LAM = STP = Stat	outigate				
Status	-	Properties Port Setting	Bridge Setting Port Advanced	Setting Statistics MST	Instance MST Port Setting		
	10	Properties Port Setting	Bridge Setting Port Advanced	Setting Statistics MS1	MSI Port Setting		
General Setup		Port	Configure BPDUs Rx.	TCN BPDUS RX.	Configure BPDUs Tx.	TCN BPDUS TX.	11.
Port Setting		GET	0	a	ú.	0	
Minor		GE2	0.	Ø	Ø.	o	
Link Aggregation		GE3	0	σ	0	0	
VLAN Management		GE4	0.	0	Ū	D	
BEE		GE5	0	0	a	0	
Multicast		GER	á	α	a	a	
Jumbo Frame		GE7	0	0	a	0	
STP.		GEB	0	α	à	0	
MAC Address Table		GE9	0	0	a.	0	
Blocked Port Recover		GE10	0	0.	0	0	
Security	+	GE11	D	α	0	0	
AGL	-	GE12	0	0	0	0	
DoS		GE13	0	ä	α	Ð	

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.

Auto Logout : Off	(								0.37 (i) 🕞
Deshboard		O Switch	LAN STP MAT	Instance					
Statun	1	Courses.	Port Setting	Dur Dur Dur	Advanced Setting	Statistics M	ST Instance MST Port S	2.00	
		Properties	Prun Setting.	Bridge Setting Per	t Advanced Setting	stationes	IST MILLINCE MIST POR S	Setting	
General Setup		MSTI	Priority	Bridge Identifi	Designated R	Root Port	Root Path Cost	Remaining Hop VLAN	Edit
Port Setting		0	32766	32768-00 1D AA 0	0-00 00 00 00 00 00	NGA.	0	0 1-4094	
Mirror		1	32768	32768-00 1D AA.0	0-00 00 00 00 00 00	N/A	0	.0	0
Link Aggrégation		2	32768	32768-00.1D:AA.0.	0-00:00:00:00:00:00	M/A.	Q.	0	0
VLAN Management		3	32768	32766-00 1D AA 0	0-00 00 00 00 00 00	NJ/A.	a	٥	0
EEE		4	32768	32758-00 1D AA.0	0-00-00-00-00-00-00	N/A	0	U	0
Muhicast		5	32768	32768-00 1D AA 0	0-00-00-00-00-00	N/A	U	0	0
Jumbo Frame		6	32768	32768-00 1D AA-0	0-00 00 00 00 00 00 00	N/A	0	0	0
517		7	32768	32768-00:10 AA:0	0-00 00 00 00 00 00	M/A	0	0	0
MAC Address Table		8	32768	32768-00 1D AA.0	0-00 00 00 00 00 00	11/A.	a	0	0
Blocked Port Recover		9	32768	32765-00 10 AA 0	0-00 00 00 00 00 00	M/A.	0	U	0
Security		10	32765	32766-00 1D AA.0	0-00 00 00 00 00 00	NIGA.	a	ō	0
ACL		11	32768	32758-00 1D AA.0	0.00 00 00 00 00 00 0	N/A	0	0	0
OoS		12	32768	32768-00 10 AA 0	0-00 00 00 00 00 00	NIA	0	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.			
	Edit MSTI 1			
	VLAN P.			
	2 0 (1 - 4094, set 0 to cancel)			
	2 Priority			
	2 32768 (0 - 61440, default 32768)			
	2 Bridge Identifiter			
	32768-00:1D:AA:11:22:44			
	Designated Root Bridge			
	0-00:00:00:00:00			
	2 Root Port			
	2 Root Path Cost			
	2 0			
	2 Remaining Hop			
	2			
	2 2 OK Cancel			
	VLAN - Enter the ID (1-4094) of the VLAN which should be			
	associated with this MSTI.			

<b>Priority</b> - The switch priority for this MST instance. A lower number gives the switch higher chance to be chosen as the root bridge.
Bridge Identifiter - Display the priority of MSTI instance number + MAC address of the switch.
<b>Designated Root Bridge -</b> 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.
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.

Auto Logout : Oll	*											и 🕒
Dashboard		O Swe	ch LAN > STP	MST Puri Se	Ating							
Status			-						Access of the second	and the second se		
		Properti	es Port Set	ting Bridg	e Setting Pa	art Advanced Setti	ing Stati	atics MS	IT Instance MST Pr	in Setting		
General Setup			MSTI:			3						-
Port Setting												
Minter												
Link Aggregation		Port	Path Cost	Priority	Port Role	Port State	Mode	Type	Designated	Designated P	Designated	Remaining Hop
VEAN Management		GE1	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00	128-1	20000	20
EEE		GE2	20000	128	Disabled	Forwarding	R5TP	Boundary	0-00.00.00.00.00	128-2	20000	20
Multicast		GES	20000	128	Elisabled	Disabled	RSTP	Boundary	0-60-00-00-00-00	128-3	20000	20
Jumbo Frame		GE4	20000	128	Disatifed	Disabled	RSTP	Boundary	0-00 00 00 00 00	128-4	20000	20
		GES	30000	128	Disapled	Disabled	RSTP	Boundary	0-00-00-00-00	128.5	20000	20
MAC Address Table		GEG	20000	128	Disablert	Disabled	RSTP	Boundary	0-00 00 00 00 00	128-6	20000	20
Blocked Port Recover		GE7	20000	128	Disabled	Disabled	RSTP	Boundary	00 00 00 00 00 00	128-7	20000	20
Security		GES	20000	128	Disabled	Disabled	RSTP	Boundary	0-00.00.00.00.00	128-8	20000	20
ACL	-	GE9	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00	128-9	20000	20-
Zoo	-	GE10	20000	125	Disabled	Disabled	RSTP	Boundary	0-00.00.00.00.00	128-10	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.

	Nicebied	DOT		D	X
		Edit Po	rt GE1	Í	C
		MS	TI		
	D				C
		Path	Cost		
			(1 - 200	00000,0 = A(10)	
		Prio	rity		1
	128				] -
					-
		ок	Cancel		
1	Disabled	RSTR	,	Boundary	- N
MSTI	- Display t	he selected	MST insta	ance.	
alue	e will be us	ed as the fo	rwarding	ne port. A port port by spanr ne bandwidth	ning tree.
owe forwa	r priority v arding port	vill have high	ner chanc i tree. Us	e path cost, p e to be used a se the drop do	as the

# 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.

Auto Logout : Of 🛛 🔐					09.41:40 🕞
Dashboard	O MAC Addmini Table - Statio	MAC Setting (> Statis MAC	(		
Status -	Static MAC				
SWITTLA	State HLAC				
General Setup	MAC Address:		COLUMN D COLUMN		
Part Setting	VLAN:		default		1.4
Mirron	Port:		GE1.		141
Link Aggregation					
VLAN Management			(bbA)		
EEE					
Mollicast	No.	MAC Address	VLAN	Port	Delete
Jumbo Frame	1	DE 1D AA BOICE 08	default(1)	CFU	
STP					
MAC Address Table					
Static MAC Setting					
Dynamic Address Satting					
Dynamit Learned					
Blocked Port Recover					

Item	Description			
MAC Address	nter 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.

Auto Logout : Off	-Admin		19-45-40	G
Dashboard C	MAC Address Table > Dynamic Address	Setting > Dynamic Address Setting		
Status	and the second se			
sweets LAN	lynamic Address Setting			
General Setup	Aging Time:	300	<b>5</b> (5 32767)	
Part Setting	Autory			
Mettor	eanit			
Link Aggregation				
VLAN Management				
EEE				
Multicast				
Jumbo Frame				
StP				
MAC Address Table				
Static MAC Setting				
Dynamia: Address: Satting				
Dynamic Learnin				
Blocked Port Recover				
Recurity				

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.

Auto Logout : Off 🛛 👻					
Dashboard	MAC Andress Table = 0	ynamic Learned -> Dynamic Learn	00		
Status	and the second se				
Swath LAN	Dynamic Learned				
General Setup	MAC Address	VLAN	Type	Port	11.5
Port Setting	D0.08 54 74 60 7D	idefault(1)	Dynamic	GE8	Add to Static
Mirror	00 1D AA 00.00 00	default(1)	Dynamic	GE28	Add to Static
Link Aggregation	01:00:00 AA 01:00	default(1)	Dynamic	GE28	Add to Static
EEE	00:10:AA:01:05:44	default(1)	Dynamic	GEB	Add to Static
Molticast	00 1D:AA:01:05:54	default(1)	Dynamic	GE8	Add to Static
Jumbo Frame	00 1D AA 01 05 73	default(1)	Dynamic	GE16	Add to Static
STP	00 10 AA 01 05 77	default(1)	Dynamic	GE16	Add to Static
MAC Address Table	00 10 AA 06 C1 57	default(1)	Dynamic	GE24	Add to Static
Static MAC Setting Dynamic Address Setting	00-1D:AA-0D:08:80	default(1)	Dynamic	GE24	Add to Static
	00.1D.AA.80.30.3C	peraut(1)	Dynamic	GE16	Add to Static
Blocked Port Recover	00 1D AA C3.32 70	default(1)	Dynamic	GE24	Add to Static
Security	00 50 40 00 00 00	data data	Dunamin	GE12	(and a second se

Item	Description
MAC Address	Display the MAC address that will be forwarded.

VLAN	Display the VLAN group to which the MAC address belongs.
Туре	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.

Auto Logout : 🛛 🖉	Tom			ផលនា 🕞
Dashibpard	Sweich LAN > Blocked Prel Renover > Blocked	Port Bincom		
Status	Blocked Port Recover			
Similar (200)				
General Setup	Recovery Interval:	300	Sec (30 - 06400)	
Port Setting	BPDII Guard:	Enable		
Meror	Self Loop:	🖂 Enable		
Link Aggregation	Broadcast Flood:	🖂 Enable		
VLAN Management	Unknown Multicast Flood:	Enable		
EEE	Unicasi Flood:	Enable		
Molticast	ACL:	🖾 Enable		
Jumbo Frame	Port Security:	🗖 Enable		
STP	DHCP Rate Limit:	📋 Enable		
MAC Address Table	ARP Rate Limit:	🗇 Enable		
Blocked Port Recover	Apply			
Security	- 7490			
ACL	-			

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.
АррІу	Apply the settings to the switch.

# Part III Security

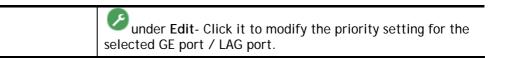
VigorSwitch G2280 User's Guide

# **III-1 RADIUS**

Auto Logout : Off 🛛 👻	Autori				10.06.14	E)
Dashboard	Security RADIUS RADIUS					
Status -	RADIUS					
Switch LAN -	india2					
lationy -		Use Default Para	meters			
Rubhus						
ACACS+	Retries:	3	8	(F 10, xwtaut 3)		
Management Access Authentication	Timeout for Reply:	3	2	neo (1 - 30, default.it)		
Anagement Access Control	Key String:					
02 1X/MAC Authentication		Aroh				
ort Security		Add RADIUS 5				-
ratected Parts		Add NADIUS 5	erver			
Storm Control	Address Type:	⊖ Hostname ⊚ IPv4				
65	Server Address:	O hosename @ irva				
ynamic ARP Inspection						
HCP Snooping	Server Port:	1012	\$	() - 65535, default 1612)		
P Source Guard	Priority:		5	(0 - 65536)		
CL -	Retry:	🖉 lise Default				

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

Item	Description
Use Default Parameters	Retries - The retry time before this server being considered not-reachable.
	<b>Timeout for Reply</b> - Set the time (in seconds) before this server being considered lost connection.
	Key String - Enter the string used to encrypt and authenticate with RADIUS server.
	Apply - Save the settings.
Add RADIUS Server	Address Type - Specify whether switch uses a hostname to resolve address by DNS to connect to server, or directly connect using IPv4 address.
	Sever Address - Enter the server's address corresponding with address type given.
	Server Port - Enter the port number used by RADIUS server.
	<b>Priorty</b> - Specify the priority that switch uses this server. The higher number, the lower priority. Switch will start with server with lowest priority.
	Retry - Set the time before this server being considered not-reachable
	<b>Timeout</b> - Set the time (in seconds) before this server being considered lost connection.
	Key String - Enter the key string used for encrypting and authenticating with server. Unless Key String is specified here, the default string will be used.
	<b>Usage</b> -Specify whether you would like to use this server for switch login authentication or 802.1x access port authentication, or both.
	Add - Click it to add a new RADIUS server and display in this page.



# III-2 TACACS+

Auto Logout : Or 🔗	Admin				norm Be
Statua	Security -> Tricales+ -> Tacales+ Dadis+				
Secury -		Use Default Paramet	tira		
RADIUS TACADS+	Timeout:	5		ner (1 - 70, debolt 5)	
Management Access Authentication Management Access Control 802 10/MAC Authentication	Key String:	(Apply)			
Port Sieconty		Add TACACS I Set	vet		
Protected Ports Storm Control DeS	Address Type: Server Address:	🔘 Hostname 🍥 IPv4			
Dynamic ARP Inspection	Server Port:	49	2	(T - 85535, detault 49)	
DHCP Snooping	Priority:		*	(0 - 65535)	
IP Source Guard	Timeout:	🕑 Use Default			
ACL -		5		Hets (T = 3D, debiult 5)	

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

Item	Description
Use Default Parameters	Timeout -Set the time (in seconds) before this server being considered lost connection.
	Key String - Enter the string used to encrypt and authenticate with TACACS+ server.
	Apply - Save the settings.
Add TACACS+ Server	Address Type - Specify whether switch use a hostname to resolve address by DNS to connect to server, or directly connect using IPv4 address.
	Sever Address - Enter the server's address corresponding with address type given.
	Server Port - Enter the port number used by TACACS+ server.
	<b>Priorty</b> - Specify the priority that switch uses this server. The higher number, the lower priority. Switch will start with server with lowest priority.
	Timeout -Set the time (in seconds) before this server being considered lost connection.
	Key String - Enter the key string used for encrypting and authenticating with server. Unless Key String is specified here, the default string will be used.
	Add - Click it to add a new RADIUS server and display in this page.
	Under Edit- Click it to modify the priority setting for the selected GE port / LAG port.

# **III-3 Management Access Authentication**

#### III-3-1 Method Profile

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

Auto Logout : 💷 🖉	Admin				12.09.36	Ð
Dashboard	Shearing > Management Actions Automotivation > N	Millinad Profile				
Status -	Method Prolife Application Authentication					
Switch LAN ~	Mendus Prome Approcation Autoretarication					
Jermy -			Method Profile			-1
RADIUS						
TACACS+	Name:					
Management August Automoticatie	Optional Methods:		Selected Methods:			
Menagement Access Control	None	32				
802.1X/MAC Authentication	Local RADIUS					
Port Security	TACACS+	<				
Protected Ports						
Starm Control						
DoS			(144)			
Dynamic ARP Impedian						_
DHCP Snooping IP Source Guard	Profile Name	Selected Method		Edit		
ACL -	default	Local		0		
AUL						A

Item	Description		
Method Profile	Name - Enter a name for creating a method.		
	<b>Optional Methods</b> - Available methods include Local, RADIUS and TACACS+.		
	Selected Methods - The method listed in this field will be applied for such method profile.		
	Add - Click it to add a method from Optional Method onto Selected Method.		
Øunder Edit	Click it to modify the optional methods/selected methods for the selected profile.		

Edit Profile: default
Optional Methods: Selected Methods:
None RADIUS TACACS+
OK Cancel

## III-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.

Auto Logout : 🖓 🔤	Tom				12)/18	G)
Dashboard	Strendy > Management Agency Arthrophy	silinon is Application Addamtical	ion .			
Status -	Method Profile Application Authentication					
Switch LAN -	Method Proble Application Authentication					-
Se wonty			Application Authentication			
RADIUS						
TACACS+	Application:	Console		×		
Management Access Automotication	Selected Profile:	defaolt				
Management Access Control			Apply			
B02 1X/MAC Authentication						
Port Seconty	Application		Selected Profile			
Protected Ports	Console		detaurt			
Storm Control	Teinet		perault			
DaS	SSH		detault			
Dynamic ARP Inspection	нттр		cetaut			
DHCP Snooping	HTTPS		default			
IP Source Guard						

Item	Description
Application	There are five methods to be configured with different profile respectively.
	Console/Telnet/SSH/HTTP/HTTPS
Selected Profile	Specify one of customized method profiles to apply to any management service, for management access control.
Apply	Save the settings.

# **III-4 Management Access Control**

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

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

Auto Logout : 🛛 👻		Admin					e	
Diashboard	Security > Management	Security = Management Access Control = Management Access Control Producted						
Status *	Management Access Cont		t Access Control Entries (ACE)					
Switch LAN -	- martine	and the second and the second second	Construction Commentary					
Depting			Management Acc	vus Control Profile(ACL)				
RÁDIUS								
TACACS+	ACL Nam	e:						
Management Access Authentication				Held				
Management Ascess Central								
802.1X/MAC Authentication	ACL Profile Name	State	Rule	Activate	Deactivate	Delete		
Port Security	ACL_Carrie 1	Inactive		9	Descurate	C		
Protected Porta	Bot Camer	Transarye:	n					
Storm Control								
DoS								
Dynamic ARP Inspection								
DHCP Shooping								
IP Source Guard								
ACL -								

Available settings are explained as follows:

Item	Description
ACL Name	Enter a name to create a profile for ACL. 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	<ul> <li>Click it to activate / deactivate such entry.</li> <li>To configure detailed settings for the selected ACL profile, do not click Activate for that profile.</li> </ul>
Delete	Click the icon under Delete to remove the selected entry.

#### III-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.

Auto Logout : Off 👻	Admin				10:13:37		
Dashboard	Security > Management Accurs Canital > Management Accurs Control Entries (ACE)						
Status -	Management Access Control Profile(ACL)	regement Access Control Entries (ACE)					
Switch LAN -							
Recordy		Management Access Control Ent	ies (ACE)		- 1		
RADIUS							
TACACS+	ACI Profile Name:	ACL_Carrie1					
Management Access Authentication	Priority:	8		[1 - 65535]			
Munagement Access Control	Service:	II.					
802 1X/MAC Authentication	Action:	Deny		-			
Port Security	ACTION:	Linuy					
Protected Pons	Ports:	Divisito organisation banda		×.			
Storm Control	IP Versions:	⊙ All ◯ IPv4 ◯ IPv6					
DoS	IPv4:		- F	36/36/36(36			
Dynamic ARP Inspection	IPv6:		1	- CB - 5			
DHCP Snooping		Add					
IP Source Guard							
ACL -	ACL Profile N Priority Ser	vice Action Ports	IP Version	IP Address	Netmask Edit		

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. Deny - Incoming / outgoing data which meets ACE rules will be			
	blocked. <b>Permit</b> - Incoming / outgoing data which meets ACE rule is allowed to pass through.			
Ports	Select the ports to which the ACL should be applied.			
IP Versions	<ul> <li>Specify the IP address/subnet to which the ACL should be applied.</li> <li>All - All the IP address should be applied.</li> </ul>			
	• IPv4 - Specify the IPv4 address /subnet.			
	IPv6 -Specify the IPv6 address /subnet.			
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	Iclick it to modify the settings for the selected entry.			

Edit ACI	Edit ACE with ACL profile=sdf						
a	and Priority=1						
Service:	All						
Action:	Deny -						
Ports:	GE1 ·						
IP Versions:		- 1					
IPv4:	1						
IPv6:	1	*					
	OK Cancel	- 1					
		_					

# III-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.

## **III-5-1** Properties

#### III-5-1-1 Global Settings

VigorSwitch G2280 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.

Auto Logoul : Cof 🛛 🔟			010256 Br
Dashboard	Global Settinge Port Authentication Setting		
Status -			
Switch LAN	it.	Global Settings	
Seconds			
RADIUS	Authentication Types:	Notreing = elected	
TAOACB+	Guest VLAN:	Enable	
Management Access Authentics	Selected VID:	1	-
Management Access Control	MAC Based User ID Format	1000000000	- 4
802 INMAC Authentication		Approx	
Probattion			
Port Cantrolegistings			
MAC Baken Local Account			
Autoenticated Hosts			
PortSecurity			
Protected Ports			
Storm Control			
Des			
Dynamic ABP Inspection			
DHCP Snooping			
IP Source Guard			
ACL ·			

Item	Description			
Global Settings	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 - Click it to save the settings.			
Apply	Save and activate the settings configured above.			

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

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

Anto Logout : 🖉 🗶			08.085	• •
Dashboard	I Settings Part Authentication Setting			
Statue -				
Switch LAN -		Per Port Mode: Bettings		
Decemp -				
RUDIUS	Apply Settings to Ports:	Similar (recht)	2	
TACACS+	Authentication Types Enabled:	ruh i uni dalan bia		
Management Access Authentics	Host Mode:	Multiper Authentication	-	
Monagement Access Control	Available Authentication Types:	Selected Authentication Types: (In O	rder)	
802 TXMAC Aumentication	MAC-based	54 (COULD COULD )		
Properties	and crasses			
Park Controllisings				
MAC-Based Local Account	2	-		
Apprendicated Hesta	Available Methods:	Selected Methods: (In Order)		
Port Becunty	Free State	PASTING T		
Protected Ports	Loćal	PASING		
Storm Control				
Deg				
Dynamic ARP Inspection				
DHCP Snooping	Guest VLAN	Enable		
IP Source Guard	RADIUS VLAN Assignment:	State	•	
ACL -		Apph		

Item	Description
Apply Settings to Ports	Select physical port(s) for applying settings. 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> <li>Multiple Authentication - Each host are authenticated individually.</li> <li>Multiple Hosts - 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>Single Host - 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 Enable to enable Guest VLAN on this port for those didn't authenticated successfully.
RADIUS VLAN Assignment	Disable - Switch will ignore the VLAN assignment from the RADIUS server and keep the original VLAN of the host. Static - Switch will use the VLAN assignment from the RADIUS server if it receives the information. If there is not VLAN information, it will keep the original VLAN of the host.

	<b>Reject</b> - Switch will reject the host if it does not receive the VLAN information from RADIUS server.
Apply	The modification made above can be applied on to the selected GE port immediately.

## III-5-2 Port Control/Settings

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

Auto Logout : 🔐 🕺											01 (13:12)
Dashboard	Port Co	nVol/Sellings									
Státun	_										
Bwitch LAN -						Port Con	trol/Séttings	£			
leculty:											
RADIUS		Ports:			blahring privating						
TAGAG8+		Port Cor	strok		Disabled						
Management Access Authentics		Periodic	Reauthentication:		Enable						
Management Access Control		Max Hos	sts:		256				(1+256)	default 256)	
802.1XMAC Authentication	Reauthentication Period:				2600 🛫 Sec (200- 4294867294, default 2600)					efault 3800)	
Propertien		inactive	Timeout:		60 🗸 Sor (00 - 85538, dutaut 60)				dutault 60)		
Prod control/comps	Quet Period:				60 Sei (40 - 55335, default 80)					detault att	
MAD-Bissed Local Account	Resend EAP Period(002, 1X Parameter):		ameteric	30 Sec (30 - 55535, deteuit 30)							
Automocaled Hosts											
Port Security		Supplica	ant Timeout(802.1X Pa	rameter):	30 Sec (10-65635, detaurt 30)					(detwurt:30)	
Protected Ports		Server	Imeout(802.1X Param	eter):	70 🦉 Sec (30 65535, detault 30)					(distault 30)	
Storm Control		Max EAU	P Requests(802.1X Par	ameter);	2				5 pr-4	ti, itetauri ()	
Dog						0	uply .				
Dynamic ARP Inspection						-	-				
DHCP Snooping	Port	Port Control	Reauthenticat	Max Hosts	Reauthenticati	Inactive	Quiet	Resend EAP	P.,. Supplicant Tim	Server Tim	wou Max EAP Regu
IP Source Guard	0E1	Desanled	Disabled	258	3600	60	60	30	30	30	2
ACL -	GE2	Distabled	Disabled	356	3600	éa	60	30	30	30	3

Item	Description			
Ports	Select the ports to modify the port control settings.			
Port Control	Specify if you wish this account to be allowed (Authorized) or blocked (Unauthorized) or determined by VigorSwtich (Auto).			
	<ul> <li>Disabled - Disable any authentication requirement for port access. All clients are allowed to access the network.</li> </ul>			
	• Force Authorized- Port will be considered authorized. All clients are allowed to access the network.			
	• Force Unauthorized - Port will be considered un-authorized. All clients are NOT allowed to access the network.			
	• Auto - Port will be considered authorized or unauthorized based on the authentication results of the host.			
Periodic Reauthentication	Enable - The hosts via the selected GE port will be re-authenticated periodically.			
Max Hosts	If Multiple Authentication mode is selected as Host Mode (802.1X/MAC Authenticaion>>Properties>>Port Authentication Setting), the total number of hosts cannot exceed the maximum numer of hosts configured here.			

Reauthentication Period	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.
Inactivate Timeout	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 Authenticaion>>Properties>>Port Authentication Setting), the packet is counted on the authorized host only and not all packets on the port.
Quiet Period	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. Later, after the time period set in this field, the host wll be allowed to perform authentication again.
Resend EAP Period (802.1X Parameter)	Set the period for host to re-send EAP (Ethernet Automatic Protection) requests. Default value is 30 (seconds).
Supplicant Timeout(802.1X Parameter)	Set a period of time for the maximum number of EAP requests will be sent. If a response from the host is not received by VigorSwitch after the defined period (supplicant timeout), the authentication process will be started again.
Server Timeout (802.1X Parameter)	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.
MAX EAP Request (802.1X Parameter)	Set the maximum time interval for EAP request sent out.
АррІу	The modification made above can be applied on to the selected GE port immediately.

## III-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.

Auto Logovit : Der 😒		Tom				urreat	D)
Dashboard	MAC-Dissed Local	Account					
Status -							
Switch LAN -			W	NC-Based Local Account Bettings			
TORNER .							
RADIUS		MAC Address:	90-00-00-00-00-00-02				
TADACE+		Port Control:	⊙Force Authorized ○Force	ce Unauthorized			
Management Access Autoentics		VLAN	User Defines	Ť	(1-#294)		
Management Access Control		Reauthentication Period:	User Defined	3600	Gec (200-4204957294)		
807 1X9MAC Authentication		inactive Timeout:	User Defined	60	Sep (00 - 055 35)		
Propertion				Add			
PortControlSettings				-			
WAC-BASES LINK Account	MAC Address	Port Control	U. VLAN	Readhentication Period	isoche Timeoul		Edit
Authenticated Holits				No data available in table			
Pari Secunty							
Protected Ports							
Storm Control							
DaS							
Ovmamic ARP Inspection							
DHCH Snooping							
IP Source Quard							
ACL -							

Item	Description
MAC Address	Enter the MAC address of the host.
Port Control	Specify a control type for the host. Force Authorized - Click it to forcefully authenticate the host specified above. Force Unauthorized - The host specified above will not be authenticated by VigorSwitch.
VLAN	User Defined - Check it to specify which VLAN will be assigned by the host of this account.
Reauthentication Period	<b>User Defined</b> - Check it to specify the time this account required to be authenticated again after authentication taken place.
Inactive Timeout	<b>User Defined</b> - 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. Click it to modify the settings for the selected entry.

## III-5-4 Authenticated Hosts

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

with Ecopout : 🗠 😹	Tan erzza G	
bashboard	Authoritic site it Hosta	
Status :		
Switch LAN -	Authenticated Hosts	
10.00	Session ID    Pert    MAC Address Current Type Status Operational V., Operational S., Operational L Operational O., Authorized V., Authorized R., Authorized R.,	zed in
RADIUS	No. data available in table	
ACACS+		
lanagumeni Access Authordus s		
Aanagement Access Control		
02.1WMAC Authentication		
Properties		
Rod ContraiSemoge		
MAC Based Local Account		
Autoenanie ( voor		
Port Security		
Probectied Ports		
Storm Control		
908		
Synamic ARP Inspection		
DHCP Shooping		
P Bourse Gward		
CL -		

# **III-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, releated action will be performed once detecting that the number of MAC address exceeds the limit.

Auto Logout : Off 👻		Admin			10.03/42	B
Dashboard	Security > Port Se	canty = Post Security				
Status -	Port Security					
Switch LAN -	a car de chiny					
Security			Part Security	-		
RADIUS						
TACACS+	Stat	a:	Enabled      Disabled			
Management Access Authentication	Part	s:	Nuttiony subsched.			
Management Access Control	Part	State:	O Enabled () Disabled			
802/1X/MAC Authenticution	MAC	Address:	1			(0 - 255)
Rock Sinclim's	Activ	on:	⊖ Forward ⊕ Discard ⊖ S	hutdown		
Protected Ports			-Au			
Starm Control						
DeS						
Dynamic ARP Inspection	Port	State	MAC Address	L <sup>®</sup> Action	Modify	
DHCP Snooping	GE1	Disable	1	Discard		
IP Source Goard	GE2	Disable	1	Discard		
ACL -	GEB	Disable	1	Discard		
	GE4	Disable	1	Discord		

Item	Description
State	Enable or disable port security function on the switch. Enabled - Enable the port security function. Disabled - Disable the port security function.
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. Enabled - The selected port applies the port security settings. Disabled - The selected port does not apply the port security settings.
MAC Address	Enter the maximum number of MAC addresses that the port is allowed to learn.
Action	<ul> <li>Select an action to perform when there is an unknown MAC address on the port.</li> <li>Forward- Forward a packet whose source MAC is unknown to the switch.</li> <li>Discard- Discard a packet whose source MAC is unknown to the switch.</li> <li>Shutdown- Shutdown this port when a packet with unknown source MAC is received.</li> </ul>
Арріу	The modification made above can be applied on to the selected GE/LAG port immediately.
Edit	I click it to modify the settings for the selected entry.

at	Edit Port GE14			
at	Port State			
at	◯Enabled ⊙Disabled			
	MAC Address			
1		(0 - 255)		
at	Action			
a	⊖Forward ⊙Discard ⊝Shutdown			
at at at	OK Cancel			

# **III-7 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.

Auto Logout : 🛛 🖉	Adaba		18:24:00
Dashboard	Security > Protected Parts > Protected Parts		
Status -	Protected Prote		
Switch LAN -	FUTURE FORE		
energy		Protected Parts Settings	
RADIUS			
TACACS+	Port List	1 halling states ( 40	
Management Access Authentication	Protected	🔿 Enable 🕤 Disable	
Management Access Control		Apply	
802 100MAC Authentication			
Port Security		Protected Ports Status	
Protected Ports	Port	Protected	0
Storm Centrol	GE1	Disable	
DdS	GE2	Disable	
Dynamic ARP Inspection	GE8	Disable	
DHCP Snooping	G84	Disable	
IP Source Guard	GE5	Disable	
ACL +	GE6	Disable	

Item	Description
Protected Ports Settings	<b>Port List</b> - Use the drop down list to select the port(s) (GE1 to GE28) for applying the settings configured in this page.
	Protected - Click Enable to activate the protected port function.
	<b>Apply</b> - The modification made above can be applied on to the selected GE port immediately.
Protected Port Status	Display current status for each GE port.

# **III-8 Storm Control**

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

## **III-8-1** Properties

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

Auto Logoitt: Off 😽	Admin	10.98 17 🕞
Dashboard	Starm Control + Properties	
Status -	and the second se	
Switch LAN -	Repeties	
Sweeney -	Storm Control Mode: 💿 Packet/sec 💿 Kbits/sec	
RADIUS	Preamble & Inter Frame Gap: (i) Excluded () Included	
TACACS+	Apply	
Management Access Authentication		
Management Access Control		
802 TX/MAC Authentication		
Port Security		
Protected Ports		
Starm Centrol		
Propertier:		
Post Sitting		
DoS-		
Dynamic ARP Inspection		
DHCP Snooping		

Item	Description
Storm Control Mode	Select the mode of storm control.
	Packet/sec - Storm control rate will be calculated by packet-based.
	Kbits/sec - Storm control rate will be calculated by octet-based.
Preamble & Inter Frame Gap	Select the rate calculation with/without preamble & IFG (20 bytes).
	<b>Excluded</b> - Exclude preamble & IFG (20 bytes) when count ingress storm control rate.
	Included - Include preamble & IFG (20 bytes) when count ingress storm control rate.
Apply	Apply the settings to the switch.

## III-8-2 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.

Auto Logout : Of 🛛 🖉		Admin					in so si 🕞
Deshboard	Starm Control	* Port Sieting * Port Set	Ϋ́				
Statua -	Purt Settings						
Switch LAN -	Contraction of the						
Sector ty				Port Settings			
RADIUS							
TACACS+		Ports:		blaming salarrad			-
Management Access Authentication		Storm Control:		C Enable  Disable			
Management Access Control		Limiting Rate:		Diroadcast	10000	. (H	Opes, 15 (000000)
802 19/MAC Authentication				Dinknown Multicast	10000	08	(bpv, 16-1000000)
Port Siecunty							
Protected Ports				DUnknown Unicast	10000	0	(bps, 15-1000000)
Starm Control		Action:		Drop      Shutdown			
Propedies				Auply			
Pog Sming							
DoS	Rot	Stars Castral	Brandsart land	Unknow Multicas	Unknowl Unisset	Artist	Made
Dynamic ARP Inspection	Port	Storm Control	Broadcast (pps)			and a second second	Modify
DHCP Snooping	GE1	Disable	Disable	Disable	Disable	Drep	0
	GE2	Disable	Disable	Disable	Driable	Drop	0

Item	Description
Ports	Use the drop down list to select the port profile (GE1 to GE28).
Storm Control	<b>Disable</b> - Disable the storm control configuration for the selected port profile.
	<b>Enable</b> - Enable the storm control configuration for the selected port profile.
Limiting Rate	Check the box(es) to enable strom control rate limited for Broadcast, Unknown Multicast and/or Unknow Unicast packet.
	<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.
	Unknown Multicast - 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.
	Unknown Unicast - 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.
Action	Select the state of setting.
	Drop - Packets exceed storm control rate will be dropped. Shutdown - Port exceeds storm control rate will be shutdown.
Apply	Apply the settings to the switch.
Modify	Iclick it to modify the settings for the selected entry.

	Edit Port GE1
	Storm Control
Disable	
	Limiting Rate
	Broadcast
10000	(Kbps, 16-1000
	Unknown Multicast
10000	(Kbps, 16-1000
	Unknown Unicast
10000	(Kbps, 16-1000
	Action
Drop	

# III-9 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.

#### **III-9-1** Properties

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

Auto Logout : Of 🦉						10.33:28
Dashboard O Drid	- Proparties - Presenting					
Status -						
Switch LAN -	ties .					
Secondy		Global Setting	15			
RADIUS						
TACACS	Dst MAC = Src MAC	Enabled O Disabled				
Management Access Authentication	LAND	🖲 Enabled 🔘 Disabled				
Management Access Control	UDP Blat	() Enabled () Disabled				
B02 1X/MAC Authentication	TCP Blat	🛞 Enabled 🔿 Disabled				
Port Security	Ping of Death					
Protected Ports	IPv6 Min Fragments	⊙ Enabled ⊖ Disabled	1240	Bytes (0-65535)		
Storm Control	ICMP Fragments	③ Enabled ① Disabled				
DoS	IPv4 Ping Max Size	S Enabled O Disabled				
Propining	IPv6 Ping Max Size	S Enabled O Disabled				
DoS Pop Setting	Ping Max Size Setting	512	Bytes (0.65535)			
Dynamic ARP Inspection	Smurf Attack	© Enabled () Disabled	Netmask Length: 0		(0.32)	
DHCP Shooping	TCP Min Hdr Size	© Enabled () Disabled	20	Bytes (0.31)		

Item	Description
Dst MAC=Src MAC	Drop the packets if the destination MAC address is equal to the source MAC address. Disabled - Disable the item function. Enabled - Enable the item function.
LAND	Drop the packets if the source IP address is equal to the destination IP address. Disabled - Disable the item function. Enabled - Enable the item function.
UDP Blat	Drop the packets if the UDP source port equals to the UDP destination port. Disabled - Disable the item function. Enabled - Enable the item function.
TCP Blat	Drop the packages if the TCP source port is equal to the TCP destination port. Disabled - Disable the item function. Enabled - Enable the item function.
Ping of Death	Avoid ping of death attack.

	Ping packets that length are larger than 65535 bytes.
	Disabled - Disable the item function.
	Enabled - Enable the item function.
IPv6 Min Fragments	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.
	Disabled - Disable the item function.
	Enabled - Enable the item function.
ICMP Fragments	Drop the fragmented ICMP packets.
	<b>Disabled</b> - Disable the item function.
	Enabled - Enable the item function.
IPv4 Ping Max Size	Determine the IPv4 PING packet with the length.
	Disabled - Disable the item function.
	Enabled - Enable the item function
IPv6 Ping Max Size	Determine the IPv6 PING packet with the length.
J. J	<b>Disabled</b> - Disable the item function.
	Enabled - Enable the item function.
Ping Max Size Setting	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.
Smurf Attack	Avoid smurf attack. The length range of the netmask is from 0 to 323 bytes, and default length is 0 byte.
	Disabled - Disable the item function.
	Enabled - Enable the item function.
TCP Min Hdr Size	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.
	<b>Disabled</b> - Disable the item function.
	Enabled - Enable the item function.
TCP-SYN (SPORT<1024)	Drop SYN packets with sport less than 1024.
	Disabled - Disable the item function.
	Enabled - Enable the item function.
Null Scan Attack	Drop the packets with NULL scan.
	Disabled - Disable the item function.
	Enabled - Enable the item function.
X-mas Scan Attack	Drop the packets if the sequence number is zero, and the FIN, URG and PSH bits are set.
	Disabled - Disable the item function.
	Enabled - Enable the item function.
TCP SYN-FIN Attack	Drop the packets with SYN and FIN bits set.
	<b>Disabled</b> - Disable the item function.
	Enabled - Enable the item function
TCP SYN-RST Attack	Drop the packets with SYN and RST bits set
TCP SYN-RST Attack	Drop the packets with SYN and RST bits set. Disabled - Disable the item function.
TCP SYN-RST Attack	Drop the packets with SYN and RST bits set. Disabled - Disable the item function. Enabled - Enable the item function.
TCP SYN-RST Attack TCP Fragment (Offset=1)	Disabled - Disable the item function.

	Disabled - Disable the item function. Enabled - Enable the item function.
Apply	Apply the settings to the switch.

## III-9-2 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.

Auto Logent : Off 🛛 👻				10 34 42 🕞
Dashboard	O Dos + Dos Pon Setting + Prit Settinds			
Status				
Switch LAN -	Port Settings			
Diversity -		Port Setting		
RADIUS				
TACACS+	Ports:	Nutting subrand		
Management Access Authentication	DoS Protection:	@ Enabled () Disabled		
Management Access Control		Apply		
602 1X/MAC Authentication				
Port Security	Port	DoB Protection	Modity	
Protected Ports	GEI	Disableti		
Starm Control			0	
DeS	GE2	Disabled	0	
Properties	GES	Disabled	0	
Dr.S Port Sutting	GE4	Disabled	0	
	GE6	Disabled	0	
Dynamic ARP Inspection	GEE	Disabled	0	
DHCP Snooping	GE7	Disabled	0	

Item	Description
Ports	Use the drop down list to select the port profile (GE1 to GE28) or profiles.
DoS Protection	<b>Disabled</b> - Disable the function of DoS Protection. <b>Enabled</b> - Enable the function of DoS Protection.
Apply	Apply the settings to the switch.
Modify	Click it to modify settings.

# **III-10 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.

#### **III-10-1** Properties

#### III-10-1-1 Global Property Settings

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

Auto Lognot 1 3 mm 🖉	Admin		03.40 BB
Deshboard Status - Switch LAN -	Global Property Settings Per Per	Property Settings	
RADIUS TADACS+	State: VLANs:	Enshie forthurg palaeroof	
Management Access Authenticator Management Access Centrol 802 IVMAC Authentication Part Security Protected Ports		Ages	
Storm Control DoS Dynamic ARP Inspection			
Properties Statistics DHCP Smooping IP Source Guard			

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. Only the GE port /LAG group within the selected VLAN will apply DAI function.
Apply	Apply the settings to the switch.

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

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

Auto Lonout : 🛛 🖉		A	umin						05:42 12	Br
Dashboard Status -	Global P	roperty Settings	er Rott Pre	perty Settings	_					
Switch LAN -					P	er Part Property Settings				
Sectory RADIUS		Ports:		Denter	4 months)					
TACACS+ Management Access Authentication Management Access Control		Trust: Source MAC DestinationM		🗌 Enable 📑 Enable s: 📄 Enable						
802 TXMAC Authentication Part Security Protected Ports		IP Address; Rate Limit:		Enable		Allow Zero ()	 50, daharilii 4, D ia Anin	miati		
Stern Centrel DoS	Port	Trust		ource MAC Address		Destination MAC Address	 IP Address		Rate Limit	- ú
Dynamic ARP Inspection	GET	DISABLED	I	SABLED		DISABLED	DISABLED		Unimited	
Frequenties	G82	DISABLED	1	SABLED		DISABLED	DISABLED		Unimited	
Statutice	GE3	DISABLED	1	SABLED		DISABLED	DISABLED		Unlimited	
DHCP Snaoping	GE4	DISABLED	1	SABLED		DISABLED	DISABLED		Unimited	
IP Source Guard	GE5	DISABLED	5	SABLED		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 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	Enable - Check it to enable the function of IP address validation mechanism for the selected port(s). Allow Zero - The IP address of "0.0.0.0" can be applied to the			
	Allow Zero - The in address of 0.0.0.0 can be applied to the			

selected port(s) if it is enabled.

Apply the settings to the switch.

for the selected port(s).

Available settings are explained as follows:

Rate Limit

Apply

Use the drop down list to choose a rate limitation value (0~50)

## III-10-2 Statistics

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

Auto Lognot - 🛛 🖉			Aam				0250.04 🕞
Dashboard	Statistics						
Status -	and the second s						
Switch LAN *	K.			Stati	sticar		1
Security	Rafresh	Clear All					
RADIUS	Connessi	O creation					
TACACS+							
Management Access Authentication	Port	Forward	Source MAC Failure	Destination MAC Fail	Source IP Validation	Destination IP Validat	IP-MAC Mismatch Fal 1
Management Access Control	GEI	ũ	D	0	. <b>р</b>	٥	<u>n</u>
802.1X/MAC Authentication	GE2	0	0	0	0	0	0
Port Security	GES	0	D.	0	0	<u>n</u>	0
Protected Ports	GE4	0	0	0	,a	α	0
Storm Control	GE5	0	0	Ð	0	0	a
DeS	DE6	σ	Û	n	D	D	0
Dynamic ARP Inspection	G87	a	D .	Q	U	ø	0
	GEB	0	0	Q	n	Q	0
Pippentes	GE9	0	D	0	۵	٥	0
Statemen	CE10	ü	0	ġ	D.	ũ	ú
HCP Snooping	GE11	0	0	n	0	D	ů.
IP Source Guard	GE12	0	0	0	0	ŋ	a

# **III-11 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.

#### **III-11-1** Properties

#### III-11-1 Global Property Settings

This page allows a user to configure global property settings for the fuction 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.

Auto Logour : Ott 😐		Jam	m:550) 🕞
Dashboard	Global Property Settings	Per Purt Property Settings	
Status -	No. of the local division of the local divis		
Switch LAN -		Global Property Settings.	N.
EXTURITY			
RADIUS	State:	☑ Enable	
TACACS+	VLANs:	Nintharey a election	
Management Access Authentication		Apple	
Management Access Control			
802 1X/MAC Authentication			
Port Security			
Protected Ports			
Storm Control			
DeS			
Dynamic ARP Inspection			
DHCP Snooping			
Properties			
Statistics			
Optim/62 Property			

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. Only the GE/LAG port within the selected VLAN will apply DHCP Snooping function.
Apply	Apply the settings to the switch.

#### III-11-1-2 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.

Auto Logout : 🕬 👾		Tom			02:66:03	Ð
Dashboard Status -	Global Property	Settings Per Port Property Sets	ngs Per Port Property S	Note that the		
Switch LAN -	-		Per Port Property 3	settings.		
RADIUS		Ports:	flatting assisted			
TACACS+		Trust:	🗀 Enable			
Management Access Authentication		Verify Chadde:	🗇 Enable			
Management Access Control		Rate Limit:	a	pps (0-300); default 0. D is Unlimited)		
902 1X/MAC Authentication			Papely			
Pon Security						
Protected Ports	Port	Trust	Verify Chaddr	Rate Limit		
Storm Control	GEI	DISABLED	DISABLED	Unimited		
DeS	GE2	DISABLED	DISABLED	Unitmited		
Dynamic ARP Inspection	GE3	DISABLED	DISABLED	Unlimited		
DHCP Snaoping	GE4	DISABLED	DISABLED	Unimited		
Hvaniniai	GEŞ	DISABLED	DISABLED	Unimited		
Statistics	GE6	DISABLED	DISABLED	Unlimited		
Option82 Property	GE7	DIBABLED	DISABLED	Unlimited		

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	Enable - 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.

## III-11-2 Statistics

This page displays all statistics recorded by DHCP snooping function.

Auto Logout : 🛛 🛛 🛃							e
Dashboard	Stabutes						
Status -	Concession of the local division of the loca						
Switch LAN -				Babsten			
Easting	Prese	Clear All					
RADIUS	WHenesh	CIER MI					
TACACS+							
Management Access Authentication	Port	Forward	Chaddr Check Drop	Untrust Port Drop	Untrust Port Drop with Opti	Invalid Drop	- 11
Management Access Control	GET	0	0	0	D	a	
BU2 1X/MAC Authentication	GE2	0	O	0	0	a	
Port Security	CES	0	û	Ó	0	0	
Protected Ports	GE4	D.	a.	d	0	ū	
Storm Control	GE5	0	α	0.	0	a .	
DeS	GEB	Ø	D.	0	D	a.	
Dynamic ARP Inspection	GE7	0	0.	0	0	ŭ	
DHCP Snooping	DE8	D	Ш	0	0	0	
	GE9	ø	σ	0	D	0	
Properties	GEIO	0	α	0	0	σ	
Slidentics	GEII	Q	Π	0	D	Q	
Option82 Property	GE12	0	P.	0	0	0	

### III-11-3 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.

#### III-11-3-1 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.

Auto Lugout : 👘 📃	Tan		02(20 D7 🕞
Dashboard	Global Option82 Property Settings	Per Port Option82 Property Settings	
Stetus -			
Switch LAN -		Glippal Option82 Property Settings	
Sectory			
RADIUS	Remote ID:	E User Defined	
TACACS+		00-1d ar 11-22-44 (Switch Mac in Byte Order)	
Management Access Authenbication		Apply	
Management Access Control			
802 IX/MAC Authentication			
Port Security			
Protected Parts			
Storm Control			
Do5			
Dynamic ARP Inspection			
DHCP Snooping			
Properties			
Statutos			
OptionEC Program			

Item	Description
Remote ID	The string specified here is used to identify the remote host.

	User Defined - Check it and manually enter ASCII text string in the entry box.
Apply	Apply the settings to the switch.

#### III-11-3-2 Per Port Option82 Property Settings

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

Auto Logovi : 🕅 🚽	Tom			164611 E <del>)</del>
Dashboard	O DHCP Snooping = Option52 Property	Per Port Option82 Property Settings		
Status -	Global Option®2 Property Settings	Port.Ophor82 Property Settings		
Secondy -		Per Port Option82 Property Set	ttings	
RADIUS				
TACACS+	Ports:	Wateria sensited	-	
Management Access Authentication	State:	[] Enable		
Management Access Control	Allow Untrust:	⊖Keep ⊛ Drop ⊙ Replace		
802 1X/MAC Authentication		Apply		
Port Security				
Protected Ports	Port	State	Allow Untrust	
Storm Control	GE1	DISABLED	Orop	
DéS	GE2	DISABLED	Drop	
Dynamic ARP Inspection	GE3	DISABLED	Drop	
DHCP Sneeping	GE4	DISABLED	Drop	
Properties	CE5	DISABLED	Drop	
Statestics	GE6	DISABLED	Drop	

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	Enable - 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. Keep - Packets are allowed to pass through. Drop - Packets are blocked and discarded.
	Replace - Packets will be replaced.
Apply	Apply the settings to the switch.

## III-11-4 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).

Auto Logout : Dif	8		Admin			14:15:07 D
DoS Dynamic ARP Inspection		Option®2 Circuit ID				
DHCP Snooping				Option82 Gircuit ID Table	-	
Properties Statubics Option82 Property		Port: VLAN:		GB1	(1 - 4094)	
		Circuit IB:				
IP Source Guard						
ACL	1			Add		
QoS	-					
System Maintenance	•	Port II VLAN	U VLAN	Circuit ID		Edit
Diagnostics				No dața available in table		

ltem	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.
VLAN	Choose a number as VLAN ID which is easy to be identified for a packet containing with it. 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	<ul> <li>click it to modify the circuit ID value for the selected entry.</li> <li>click it to remove the selected entry.</li> </ul>

# III-12 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.

## III-12-1 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.

Auto Logout : 🖓 🚿		Admin			D4:16:27 🕞
Dashboard	Port Settin	DAK			
Status -	- out occurs				
Switch LAN -				Port Settings	
Secon					
RADIUS		Ports:	Ave have as	larba 4	· · · ·
TACACS+		State:	🗇 Enable		
Management Access Authentication		Verify Source:	⊙ IP ⊖ IP.8	AAC	
Management Access Control		Max Entry:	σ	C (0 - 50	, default 0. 0 in Unimonid)
802.1%MAC Authentication				Apply	
Port Security					
Protected Ports	Port	State	Verity Source	Current Entry	Max Entry
Storm Control	GE1	DISABLED	P	ō	Unimited
DoS	GE?	DISABLED	IP	a	Unlimited
Dynamic ARP Inspection	GE3	DISABLED	P	0	Unimited
DHOP Snooping	GE4	DISABLED	IP	Ø	Unlimited
IP Source Guard	C/E6	DISABLED	P	0	Unimited
Port Settings	GE6	DISABLED	P	0	Unlimited
IMPV Binding	GE7	DISABLED	18	0	Unlimited

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. IP - Only the packet with specified IP address will be verified. IP-MAC - Only the packet with specified IP address and MAC address will be verified.
Max Entry	Define the number (0~50) for the port. The default is 0 (no limit).
Apply	Apply the settings to the switch.

## III-12-2 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.

Auto Logout : Off 😒	Jam	03/10/22	B)
Dashboard	IMPV Binting		
Status ·			_
Switch LAN -	N 1 1	IR-MAC-Pon-VLAN Binding Table	
EXTUDIV			
RADIUS	Ports:	(GE)	
TACACS+	VLAN:	2 (1 4034)	
Management Access Authentication	Binding:	⊙ IP MAC Port-VLAN ○ IP Port-VLAN	
Management Access Control	MAC Address:	(0.0.0000000	
802 1X/MAC Authentication	IPv4 Address		
Port Security		/ Constraint	
Protected Ports		Arm	
Storm Control			
DoS	Port VLAN MAC Address	IP Address II Subnet Mask II Binding II Type II Lease Time	Edit
Dynamic ARP Inspection	GE1 1 11/22/33:44:55.66	192 168 1.101 255 255 255 IP-MAC-Port-VLAN Static N/A	00
DHCP Snooping			
IP Source Guard			
Port Saturda			
MIR* Einding			

Item	Description
Ports	Use the drop down list to select the port (GE1 to GE28, LAG1 to LAG8) 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. It is optional setting.
Binding	Select the binding type for such feature. IP-MAC-Port-VLAN – 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. IP-Port-VLAN – 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.
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	I click it to modify the settings for the selected entry.

	Edit	×
Ports:	GE1 -	
VLAN:	1 (1 - 4094)	
Binding:	○ IP-MAC-Port-VLAN	VLAN
IPv4 Address:	192.168.1.86 / 255.255.26	55.255
	OK Cancel	

## III-12-3 Save Database

This page allows the network administrator to configure the DHCP Snooping database.

Auto Logout : 08		Autimip			04:17:55	Ð
DeS		Save Databana				
Dynamic ARP Inspection DHCP Snooping			Sine Databa	ар		
IP Source Guard		Туре:	👁 Nove 🔿 Flash 🔿 TFTP			
Part Sottings MPV Binding		Filename:				
Sure Deljačna		Address Type:	Hostname IPv4			
ACL	*	Server Address: Write Delay:				
QoS System Maintenance	-1	Timeout:	000	<ul> <li>Sec (15 – 86400, default 300)</li> <li>Sec (0. 86400, default 300)</li> </ul>		
Diagnostics	-		Apply			

Item	Description
Туре	None - Do not save the database. Flash - Save the database to flash memory. TFTP - Save the database to a TFTP server.
Filename	Enter a filename if TFTP is used.
Address Type	Specify the address type if TFTP is used. Hostname - Use hostname as server address. IPv4 - Use IPv4 address.

Server Address	Enter an IP address or hostname of TFTP sever if TFTP is used.		
Write Delay	Set a value from 15 to 86400. After the database is changed, the transfer work will be delayed for the value set. The default value is 300 (seconds).		
Timeout	Set a value from 0 to 86400. Stop the transfer process if it is not finished after waiting for the set value. Set a value. The default value is 300 (seconds).		
Apply	Apply the settings to the switch.		

# Part IV ACL Configuration

VigorSwitch G2280 User's Guide

# **IV-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.

#### **IV-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.

Auto Lugout : DE	н	-ar	0				04.1824 🕑
Dashboard		MAC IPvd IPv6					
Stutus		States States					
Switch LAN	-	ACL Profile Name		AGL_MAC_Came			
Security					A46		
Conste ACC		No.	MAC ACL Name			Action	0
Create ACE		1	ACL_MAC_Came			0	
ACL Binding							
QeB							
System Maintenance							
Diagnostics							

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.

#### IV-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.

Auto Logour: Off 🖉		Admin					04/21/02	B
Dashboard		MAC IPHE IPHE						
Status		Cintral Contral						
Switch LAN	+	ACL Profile Name:		ACL PL1				
Security	-				DBA			
Contra ACI		No.	IPv4 ACL Name			Action		
Create ACE		1	ACL_IP4_1			0		
ACL Binding								
QoS	+							
System Maintenance	-							
Dregnostica								

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.

#### IV-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.

Auto Logour : Off 🧟		Admin				04:35:29	D)
Dashboard	MAC	Pv4 IPv6					
Status							
Switch LAN		ACL Profile Name:	ACL_IP6_CT				
Security -				Add			
Cristin ACL	No.	IPv6 ACL Na	ne		Action		304
Create ACE	1	ACL_IP6_C1			0		
ACL Binding							
QoS ·							
System Maintenance							
Diagnostics							

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.

# **IV-2 Create ACE**

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

#### IV-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.

Auto Logour :	2	Admin					94,36,31	B	
Dashboard		MAD IPV4 IPv6							
Stablis	-								
Witch LAN		ACL Profile Name:	ACL_MAC_Canna •						
lecurity		Sequence:	1 (1 - 2147483647)						
	-	Action:	Permit -						
Creste ACL		Source MAC:	@Any						
CHERRACE				1	EFFETERE EL 101				
ACL Binding		Destination MAC:	2 Any						
103	-			1	*********				
ystem Maintenance		Ethertype:	Plany						
Diagnosoco			(0x600-0xFFFF)						
		VLAN:	(wood-arrer)						
		VLAN.							
			- (1-4094)						
		802.tp:	(2) Any						
			167	1					
			Add	_					_
		No. I Name Sequence A	ction Source MAC Mask Destuna	tion MAC Mask	Ethertype	VLAN	802.1p	Modify	
		option design of	Series align despedances		0.802	337	Rap1077		

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	<ul> <li>Select the action applied to the packet matched this ACE.</li> <li>Permit or deny the packets into switch core, or shutdown the port for stopping further transmission.</li> <li>Permit</li> <li>Deny</li> <li>Shutdown</li> </ul>				
Source MAC / Destination MACSpecify the source and the destination MAC address for filtering.Any - All packets will be filtered. Or, enter the IP address to filter the packets coming filter					

	address.					
Ethertype	Specify ethernet type for filtering.					
	Select Any.					
	Or, enter the value with the format of "0x600 ~ 0xFFF".					
VLAN	Specify VLAN profile for filtering.					
	Select Any.					
	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 Any, 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.					
	click it to remove the selected entry.					

#### IV-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.

Alto Logost : Of	2	MAC INA	IPv6										
Dashboard		AC	1. Profile Name:			ACL_IP4_1							
Status Switch LAN		Se	quence:			11	1 - 2147483847)						
Security		Ac	tion:			Permit							
4(1)		Pro	ilocol:			Any							
Create ACL		So	arce IP:			@Any							
STRUCT ADE						0.8.3.0		1	3535181				
ACL Binding		De	stination IP:			@Any							
800	1					0.0 10		1 L .	2421201				
System Maintenance		Se	Nice:			Any							
Diagnostics		50	urce Port:			Ani							
		De	stination Port:			Attir							
		ici	MP Typie:			Atry.							
		101	dP code:			Any							
						0.255							
							Add						
		Source IP.Mask	Destination I	DSCP	IPP	Source Port	Source Port	Destination P	Destination P.,	TCP Plag	ICMP type	ICMP code	Modity 7
		AnjóAnji	AnglAny	Any	Αεγγ				4	*	4	-	00
		47()(47)(	-lungbarry	-Anii	$ hf  ^2$	Hay	Any:	(40)/	Am	Hung	Alle	Athr	

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. Permit Deny Shutdown
Protocol	Specify the protocol for filtering.
	<ul> <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</li> </ul>
	example, 0 means "Echo Reply"; 254 means "RFC3692-style Experiment 2".
Source IP / Destination IP	Specify the source and the destination IPv4 address for filtering.
	Any - All packets will be filtered. Or, enter the IP address to filter the packets coming from that address.
Service	Any - All packets will be filtered. 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.
	<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.
Source Port / Destination Port	Specify the source and destination port number for filtering the packets.
	Any - All packets will be filtered. Single - Only the packets passing through the number defined here will be filtered.
	Range - Only the packets passing through the port range defined here will be filtered.
ІСМР Туре	Any - All packets will be filtered. Select - Choose one of the type (e.g., Destination Unreachable Echo Reply, MLD Query) from the drop down list.
	<b>Define</b> - Specify a type number (0 - 255) for ICMP code. For example, 0 means "Echo Reply"; 254 means "RFC3692-style Experiment 2".
ICMP code	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. Any - All packets will be filtered. Or, enter 0 to 255 based on the ICMP type specifed.
Add	Click it to create a new binding profile.
Modify	I click it to modify the settings for the selected entry.
	click it to remove the selected entry.

#### IV-2-3 IPv6

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

Hatus	-	ACL Profile Name:	ACL_IP6_C					
witch LAN	- 4	Sequence:	1	2 11 - 21474835471				
acunity		Action:	Permit					
		Protocol	Ann					
réaté ACL		Source IP:	1 Any					
reate Atte	- 3				ī	10000		
CL Binding		Destination IP:	I Any					
98			6		1			
rstern Maintenance		Service	ANV					
iagnostics								
		Source Port:	Atin	×.				
		Destination Port:	Any					
		ICMP Type:	.AtlV	•				
		ICMP code:	Any					
			1.359					
				And				
				_				

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. • Permit
	<ul> <li>Deny</li> </ul>
	<ul> <li>Shutdown</li> </ul>
Protocol	Specify the protocol for filtering. Any - All packets will be filtered.
	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.
	Define - Specify a type number (0 - 255) for ICMP code. For example, 0 means "Echo Reply"; 254 means "RFC3692-style Experiment 2".
Source IP / Destination IP	Specify the source and the destination IPv6 address for filtering.
	Any - All packets will be filtered.
	Or, enter the IPv6 address to filter the packets coming from that address.
Service	Any - All packets will be filtered.

	<ul> <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>
Source Port / Destination Port	Specify the source and destination port number for filtering the packets. Any - All packets will be filtered.
	<ul><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>
ІСМР Туре	Any - All packets will be filtered. Select - Choose one of the type (e.g., Destination Unreachable Echo Reply, MLD Query) from the drop down list. Define - Specify a type number (0 - 255) for ICMP code. For example, 0 means "Echo Reply"; 254 means "RFC3692-style Experiment 2".
ICMP code	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. Any - All packets will be filtered. Or, enter 0 to 255 based on the ICMP type specifed.
Add	Click it to create a new binding profile.
Modify	<ul> <li>Click it to modify the settings for the selected profile.</li> <li>Click it to remove the selected entry.</li> </ul>

# **IV-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.

Auto Logout : Óff	-		Admin			nei) (I 🕞
Dashboard		ACL Binding				
Status	-					
Switch LAN		3	Ports:	Mattery sale mes		
Security	~		AC ACL:	Swart MAC ATL		
Mil.	-		Pvi ACL:	Transis (Proj. ac.)		
Create ACL			Pv6 ACL:	Stand (PuB-W-1		
Creste ACE				- apty		
ACI Elimitary						
QoS		Port	MAC ACL	IPv4 ACL	IPv6 ACL	
		GEI		ACL_IP4_1		
System Maintenance		GE2				
Diagnostics		GE3				
		GE4				
		GES				
		GE5				
		GE7				
		GEB				
		GE9				
		GE10				

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 V QoS Configuration

VigorSwitch G2280 User's Guide

## V-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.

#### **V-1-1** Properties

#### V-1-1-1 QoS General Setting

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

Auto Logout : 06	14	Admin	04 43 35
Dashboard		QdS Blobal Setting Trust Ports	
Status	- 1	The second second second	
Switch LAN	-	QoS Mode:	🗇 Basic 💿 Disable
Security	-	Ingress Trust Mode:	③ CoSt802.1p □ DSCP □ CoSt802.1p-DSCP ○ IP Precedence
ACL		Apple	
245	-	- PRRY	
General			
Propurties	3		
Port Settings			
Queue Settings			
CIAS Mapping			
DSCP Mapping			
IP Preundunch Mapping			
Bandwidth			
System Maintenance			
Diagnostico			

Item	Description
QoS Mode	Disable -Disable the function of QoS mode. Basic - Enable the function of QoS mode.
Ingress Trust Mode	<ul> <li>Select the QoS operation mode.</li> <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.

#### V-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.

Auto Logout : 🛛 🕅 🖉	Ab		04/44/26 🕞
Dashboard	QoS Global Setting	d	
tatus -	The second se		
witch LAN	-	Trust Ports	
acurity -			
ci	Ports:	Finition growthing	
05	Trust:	🕑 Enable 🔘 Disable	
Seneral		(ADDA)	
Properties			
Port Settings			
	Port	Trust	2.0
CeS Mapping	GE1	Enable	
DSCP Mapping	GE2	Enáble	
P Procedence Migping	GE3	Enable	
Bandwidth	G64	Enable	
	GE5	Enable	
ystem Maintenance	GE6	Enable	
agnostice -	GE7	Enable	
	GEB	Enable	
	GE9	Enable	

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. Enable - Traffic will follow trust mode in general setting. Disable - No QoS service for this port.
АррІу	Apply the settings to the switch.

# V-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.

Auto Logout : Off 🛛 👻		Admin			14/45/26 🕞
Dashboard Status	Port Setting			_	
	1		Port Settin	ge	
Security		Parts:	Mathing patronial		1
ACL 005		Ingress Default CoS:	a		-
General		Egress Remarking			
Propedies		- Remark CoS:	🔘 Enable 🛞 Disable		
		Remark DSCP / IP Precedence:	O DSCP O IP Preced	ence 🕒 Disable	
Gueue Settingu CoS Mapping DSCP Mapping			Apply		
P Procedence Mipping	GE1	ingress Default CoS	Disable	Remark DSCP / IP Precedence	Modify
Bandwidth	GE2	D	Disable	Disable	0
System Maintenance	GE3	D	Disable	Disable	0
Diagnostice	GE4	D	Disable	Disable	0
	GE5	D	Disable	Disable	0
	GE6	0	Disable	Disable	0

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).
Engress Remarking	
Remark CoS	<b>Disable</b> - Disable CoS remarking function for outgoing packets. <b>Enable</b> - Egress traffic will be marked with CoS value according to the Queue to CoS mapping table.
Remark DSCP/IP Precedence	<ul> <li>Disable - Disable DSCP/IP Precedence remarking function for outgoing packets.</li> <li>DSCP - Egress traffic will be marked with DSCP value according to the Queue to DSCP mapping table.</li> <li>IP Precedence - 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.

#### V-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.

Dashboard	Queue Settings				
Status -					
Switch LAN -			Queue Settings		
Security -					
ACL -	Queue	Schedule	Weight	% of WRR Bandwidth	
onS -	1	Strict Prianty      WRR	0		
General	2	() Strict Priority () WRR	p		
Properties	3	Strict Priority O WRR	o		
Port Settings	4	Strict Priority O WRR	U	3	
	ś	Strict Priority O WRR	0		
CoS Mapping	6	Strict Priority O WRR	D		
DSCP Mapping	7	Strict Priority O WRR	o	1	
P Procedonce Mapping Bandwidth	8	Strict Priority O WRR	Ū.		
System Maintenance *			Apply		
Diagnostics -					

Item	Description
Queue	There are eight queue ID numbers allowed to be configured.
Schedule	Strict Priority - Click it to set queue to strict priority type. WRR - Click it to set queue to Weight round robin type.
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.

# V-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.

Auto Logour : 🛛 😨	Adminy		(14/47/4) 🕞
Dashboard	Mapping		
Status -			
Switch LAN -		CoS to Gunue Mapping (for Ingress)	
Security -	Class of Service	Queue	
ACL -	0	2	3
0%		1	+
General	2	3	-
Firoperties	3	4	
Port Sktimp	4	5	· · · ·
	5	8	-
Cueue Gettings	6	7	
1.65 Minpung	7	8	÷
DSCF Mapping			
IP Precadence Mapping		Oueue to CoS Mapping (or Egress Remarking)	
Bandwidth	Quene	Class of Service	
	1	1	4
System Maintenance	2	Ω.	-
Diagnostics -	3	2	-
		3	4
	5	4	-

Item	Description	
CoS to Queue Mapping (for Ingress) - Settings for incoming packets.		
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.	
Queue to CoS Mapping (fo	r Egress Remarking) - Settings for outgoing packets.	
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).	
АррІу	Apply the settings to the switch.	

## V-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.

Auto Logout : Cifi 🖉		- Admin		na na na 🕞
Dashboard	DSCP Mapping			
Status	-			
Switch LAN			DSCP to Queue Mapping (lot Ingress)	
Security	- DSCP		Queue	
ACL	- Richma	g pullecting .	1	
	1 m			
General		Qu	aue to DSCP Mapping (for Egress Remarking)	
Properties	Queue		DSCP	
Port Settings	1		0	-
	2		8	
	3		16	*
CoS Mapping	4		24	•
DSCP Massimi	5		32	÷
IP Freendance Mapping	6		40.	+
Bandwidth	1		40	•
System Maintenance	. 8		56	-
Diagnostics	-		(Apply)	
	DSCP	J. Mappin	a to Oueue	

Item	Description	
DSCP to Queue Mapping (for Ingress) - Settings for the incoming packets.		
DSCP	Display the DSCP value (0 to 7).	
Queue	Define the queue ID (level 1 to 8) for different DSCP values.	
Queue to DSCP Mapping (for Egress Remarking) - Settings for outgoing packets.		
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.	

## V-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.

Auto Logout : 💴 🧟			uranu C+
Dashboard	cedence Mapping		
Statue			
Switch LAN -		IP Precedence to Deans Mapping (for Ingress)	
Security -	IP Precedence.	Queue	
ACL -	<u>0</u> .	10	
26 I	1	2	-
General	2	3	-1
Piopetties	.à	4.	-
Fort Sylton	4	6	
	5	6	
Official Soft or a	6	7	· (*
COS Marpino	7	â	
DSCP Mapping			
d'Altrogolingi Majanta	and the second	Queue to IP Precedence Mapping (for Egress Remarking)	
Bandwidth	Queue	IP Precedence	
	1	0	
System Mautenance	2	1	+
Diagnostics -	3	2	÷.
	4	1	
	5	4	-

Item	Description	
IP Precedence to Queue Mapping (for Ingress) - Settings for the incoming packets.		
IP Precedence	Display the IP Precedence value (0 to 7).	
Queue	Define the queue ID (level 1 to 8) for different IP Precedence values.	
Queue to IP Precedence M	apping (for Egress Remarking) - Settings for outgoing packets.	
Queue	Dueue         Display the queue ID (level 1 to 8) for different IP Precedend values.	
IP Precedence	Define the IP Precedence value (0 to 7).	
Apply	Apply the settings to the switch.	

# V-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.

Auto Logout : Of	2					₽
Dashboard		logress Rate Lund				
Status						_
Switch LAN				Ingress Rate Limit:		
Security	-					
ACL		Ports:		Nothing selected	1	
465		State:		🔿 Enable 💿 Disable		
General		Rate (Kbps):			(16-1000000, multiple at 16)	
Bandwidth				Apply		
Egress Silaping Rate	P	Port	Rate Limit (Kbps)		Modify	
Egress Shaping Per Que	nie (	3E1	off		0	
System Maintenance		5E2	. 017.		0	
Diagnostics		9E3	off		0	
	0	3E4	att		0	
	c	3E5	off		0	
	G	966	off.		0	
	c	SE7	1017		0	
	c	3EB	off		0	

Item	Description
Ingress Rate Limit	
Ports	Use the drop down list to select the port profile (GE1 to GE28) or profiles.
State	Disable - Disable ingress bandwidth control. Enable - Enable ingress bandwidth control.
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.

# V-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.

Auro Logout : 🛛 🕅 🖉	Admin		04-52-25 🕞
Dashboard	Egress Shaping Rate		
Status -			
Switch LAN -		Egress Shaping Rate	4
Security -			
ACL -	Ports:	Menhong salarated	*
Gw5	State:	🔿 Enable 🛞 Disable	
General	CIR (Kbps):		(16-1000000, methods of 16)
Bandwidth		Apply	
ingress Rate Limit			
Egreet Stating Rate	Port	CIR (Kbps)	Modify
Egress Shaping Per Queue	GE1	10	0
System Maintenance -	GEZ	off	0
or agrostics *	GE3	aff	0
	GE4	aft	0
	GE5	10	0
	GE6	oft	0
	GE7	off	0
	GE8	oft	D

Item	Description
Egress Shapping Rate	
Ports	Use the drop down list to select the port profile (GE1 to GE28) or profiles.
State	Disable - Disable egress bandwidth control. Enable - Enable egress bandwidth control.
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.

## V-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.

Auto Logout : Off 🦉		Admin	0455290 (	Ð	
Dashboard		Egress Shiping Per Queue			
Status	-				1
Switch LAN	-		Egress Shaping Per Queue		
Security	•				
ACL		Port	0E1 -		
ÚrS		Queue:	- Select Queue ID -		
General		State:	🖒 Enable 🛞 Disable		
Bandwidth		CIR (Kbps):	(16-1000000, multiple of 16)		
Ingress Ride Limit			Apple		
Egress Shaping Rate					
System Maintenance		Queue Information of Port GE1			
Diagnostics	•	Queue ID	CIR (Kbps)	11	
		r.	off		
		2	orr		
		3	off		
		4	off		
		5	on,		

Item	Description
Egress Shapping Per Queu	e
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	Disable - Disable egress bandwidth control. Enable - Enable egress bandwidth control.
CIR (Kbps)	Enter the rate value,<16-1000000>,unit:16 Kbps.
Apply	Apply the settings to the switch.

This page is left blank.

# Part VI System Maintenance

VigorSwitch G2280 User's Guide

# VI-1 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.

#### **VI-1-1** Properties

Auto Logout : Off  🗟	Admin			05.12.22
ashboard	LIP Global Setting			
tatus -	LLDP State:	③ Enable 〇 Disable		
witch LAN +	Transmission Interval:		đ	(5.32767)
ecurity -		30		
cL -	Holdtime Multiplier:	-4.	ş	(2-10)
05	Reinitialization Delay:	7	8	(1-10)
yaton Mandonace	Transmit Delay:	2	*	(1.8191)
LDP	LLDP-MED Fast Start Repeat Count:	3	1	(1-10)
Proportion	(TTT)			
LDP Port Setting	Apply			
LEDP Local Device				
LLOP MED Network Policy				
LLDP MED Port Settings				
LLDP Remote Device				
LLDP Overlanding				
NMP				
ccuso Manager				
Time and Date				

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

Item	Description
LLDP State	Enable - Enable LLDP protocol on this switch. Disable - Disable LLDP protocol on this switch.
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. The default is 3. Available range is from 1 to 10.
АррІу	Apply the settings to the switch.

# VI-1-2 LLDP Port Setting

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

Auto Lognat : 🛛 🖉		./Asimm			05 13 38 🕒
Dashboard	LLDP Port St	atting			
Status	and the second s				
Switch LAN -		Ports:	Fourthorny applied too.		
Security		State:	Disable		+
ACL ·		Optional TLVs:	kenterny contraction.		
0oS -		VLAN:	Nottong contextory		21
$\operatorname{Sychon} \tilde{R} = \operatorname{her} \varphi_{n+1}$					
LLDP			(#pply)		
Propatilus:	Port	State	Selected Optional TLVs	Selected VLAN	Modiny
	GE1	TX8PX	System Name, Port Description, 802 3 MAC		0
LLDP Local Dence	GE2	TREFX	System Name, Port Description, 802.3 MAC-		0
LLDP MED Nationals Pally	GE3	TX8PX	System Name, Port Description, 802.3 MAC-	PHY	0
LLDP MED Port Settings	GE4	TXSRX	System Name, Port Description, 802 3 MAC-	PHY	0
LLDP Remote Danice	GE5	TSERX	System Name, Port Description, 802 3 MAC-	PHY	0
SNMP	QE6	TX8RX	System Name, Port Description, 802.3 MAC-	РНУ	0
Access Manager	ĠE7	TX8RX	System Name, Port Description, 802.3 MAC-	PHV	0
Time and Date	GE8	TX8RX	System Name, Port Description, 802,3 MAC-	PHY	0
LIVE AND MADE	200	*1/2/min	Game Bren Distriction and State	et pr	-

Item	Description
Ports	Use the drop down list to select the port (GE1 to GE28) or ports for device check.
State	<ul> <li>Disable - Disable the transmission of LLDP PDUs.</li> <li>TX&amp;RX - Transmit and receive LLDP PDUs both.</li> <li>TX Only - Transmit LLDP PDUs only.</li> <li>RX Only - Receive LLDP PDUs only.</li> </ul>
Optional TLVs	<ul> <li>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.</li> <li>The type and length are fixed in size (typically 1-4 bytes), and the value field is of variable size.</li> <li>Select the LLDP optional TLVs to be carried (multiple selection is allowed).</li> <li>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.</li> </ul>
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.

# VI-1-3 LLDP Local Device

uto Logout : 🛛 Off 👘 🔮	Aur	tin)		05:14:33
Deshbawd	LLDP Local Device			
Status -	and the second se			
Switch LAN -	-		Emire Summary	
Security	Name		Value	
ACL -	Chassis ID Subtype		MAC Address	
005 -	Chassis ID		09/10:AA:00:00	
Spilon Manimore a	System Name		G2280	
LLOP	System Description		24/Poit 10/100/1000BaseT+	4-Port 100M/1000M Combo SFP L2 Switch
Purporties	Capabilities Supported		Bridge	
LLDP Part Selling	Capabilities Enabled		Bridge	
LLDP Cocol Device	Port ID Subtyp≷		Interface name	
LLDP MED Network Policy			Port Detwils	
LLDP MED Pml Selong	Port	LLDP State		Detail
LLDP Remote Dawce	GEI	TX8RX		0
LLDP Querto a min	GE2	TXERS		0
SHARE	GE3	TX8RX		0
Access Manager	G64	TX880		0
Time and Date	955	TYPEY		

This page displays information for LLDP Local Device.

Item	Description
Device Summary	Display a summary of the LLDP information for this switch. Chassis ID Subtype - Display the type of chassis ID, such as the MAC address.
	<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.
	System Name - Display model name of switch.
	System Description - Display description of switch.
	Capabilities Supported - Display the primary functions of the device, such as Bridge, WLAN AP, or Router.
	Capabilities Enabled - Primary enabled functions of the device.
	<b>Port ID Subtype -</b> Display the type of the port identifier that is shown.
Port Details	Display detailed information of the selected GE port.
	Detail - 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 GE28).

## VI-1-4 MED Network Policy

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

Auto Logout : Dif	8		sidmin									05 (6)	π G	
Dashboard		MED Network P	Policy											
Status		_						_					_	_
Switch LAN	-					ME	D Network Pol	ey .						
Security	-													
ACL	-	P	alicy ID:		1						4			
QoS	-	E	hable Policy:	ΘI	Enable 🔘 Disat	ale								
System Maintanance	-	A	oplication		Voice Signaling						•			
LLDP		v	AN:							2 (	1-4095)			
Properties		v	LAN Tag:	01	Untag 🔘 Tag									
LLBP-Port Serring			riority:		0.									
LLDP Local Device			SCP:		a									
	e []	0.	SCP.	12			-							
LLDF MED Part Settings							Apply							
LLDP Remote Onvice														
LLDP Overloading		Policy ID	Policy Enabled	30 A	pplication	-11	VLAN ID		Tagged/Untagged	II.	Priority	10	DSCP	11
SNMP		1.	Disabled	U	ntinown		U		Untagged		0		a	
Accuss Managar		2	Disabled	Ur	nkinown		0		Untagged		ġ		σ	
Time and Date		3	Disabled	Ur	nknown		σ		Untagged		0		α	

Item	Description
Policy ID	Choose a number for configuring the policy profile. Available selections include 1 to 32.
Enable Policy	Enable - Click it to enable such function.
Application	There are several applications which can be used for MED network.
	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. Untag - Packets will be sent out without any tag. Tag - Packets will be sent out with a number tagged.
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.

## VI-1-5 LLDP MED Port Settings

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

Anto Logout : 00	1	Admin		06 IF 10 🕞
Dashboard		Part Control/Seltings		
Status	-			
Switch LAN		P	Port Control/Settings	
Security				
ACL		Ports:	marting selected	
QoS		State:	2 Enable	
System Mantenance	1	Available Optional TLV:	Selected Optional TLV:	
LLOP		Location	55 Balgari Pa	
Properties		fervient or y		
LLDP Fort Setting			13	
LLDP Local Dency		-	<b>CC</b>	
LLDP MED Network Policy		Selected Network Policies:	Matter predection	
LLDP Remote Davide		Location TLV Settings:		
LLDP Overlauding		Coordinate	(15 pairs of here	adecimal characters)
SNMP		Civic	邱一160 pairs of hexa	adecimal characters)
Access Manager		-ECS ELIN	(10 - 25 pairs of heat	adecimal characters)
Time and Date			Apply	

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. 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.
	<b>Coordinate</b> -Enter the coordinate location in 16 pairs of hexadecimal characters.
	<b>Civic</b> - Enter the civic address in 6 ~ 160 pairs of hexadecimal characters.
	ECS ELIN - Enter the ECS (Emergency Call Service) ELIN (Emergency Location Identification Number) in 10 ~ 25 pairs of hexadecimal characters.
Apply	Apply the settings to the switch.

# VI-1-6 LLDP Remote Device

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

Anto Logout : Dff	R	Vedmen.	06:16:09	₿.
Dashboard		LLDP Remote Dence		
Status			_	-
Switch LAN		Local Port Chassis ID Subtype Chassis ID Port ID Subtype II Port ID System Name II Time to Live	Details	Delete
Security	÷	No data avutable (n table		
ACL	$\sim$			
005	+			
Syatem Masala				
LLDP				
Properties				
LLOR For Setting				
LLDP MED Network Proce	n.			
LLDP Gvetossting				
SNMP				
Access Manager				
Time and Date				

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.

# VI-1-7 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.

Auto Logout : Off	1			(Hanvr					05 19 01 🕞
Dashboard		LLDP Pr	ut Setting						
Status		-							
Switch LAN		Port	Total(Bytes)	Left to Send(Bytes)	Status	Mandatory TLVs	B02.3 TLVs	Optional TLVs	B02.1 TLVs
Security	3	GE1	68	1420	Not overloading	21(Transmitted)	11(Transmilled)	e(Transmitted)	e(Transmilled)
ACL	-	GE2	68	3420	Not Overloading	21(Transmitted)	11(Transmitted)	9(Transmitted)	R(Transmitted)
QuaS	G.	GE3	68	1420	Not Overloading	21(Transmitted)	11(Transmitted)	9(Transmitted)	B(Transmitted)
Systematic		GE4	68	1420	Not Overloading	21(Transmitted)	11(Transmitted)	9(Transmitted)	B(Transmitted)
LLOP-		GE5	68	1420	Not Overloading	21(Transmitted)	11(Transmitted)	9(Transmitted)	B(Transmitted)
Properties		GEE	60	1420	Not Overloading	21(Transmitted)	11(Transmitted)	9(Transmitted)	fl(Transmitted)
LLDP Part Setting		GE7	68	1420	Not Overloading	21(Transmitted)	) ( ( ransmitted)	9(Transmitted)	8(Transmitted)
LLDP Local Device		GEB	60	1420	Not Overloading	21(Transmitted)	I f(Transmitted)	9/Transmitted)	.B(Transmitted)
LLDP MED Network Pr	dia.yo	GE9	68	1420	Not Overloading	23(Transmitted)	Ti(Transmitted)	9(Transmitted)	B(Transmitted)
LLDP MED Put Satur		GE10	69	1419	Not Overloading	22(Transmitted)	11(Transmitted)	9(Transmitted)	B(Transmitted)
LLDP Renate Dev. e		GE11	69	1419	Not Overloading	22(Transmitted)	11(Transmitted)	9(Transmitted)	B(Transmitted)
LLDP Speltfaaling		GE12	69	1419	Not Overloading	22(Transmitted)	TT(Transmitted)	9(Transmitted)	8(Transmitted)
SNMP	_	GE13	69	1419	Not Overloading	22(Transmitted)	FI(Transmitted)	9(Transmitted)	B(Transmitted)
Access Manager		GE14	69	1419	Not Overloading	22(Transmitted)	11(Transmitted)	9(Transmitted)	B(Transmitted)
Time and Date		GE15	69	1419	Not Overloading	22(Transmitted)	11(Transmitted)	9(Transmitted)	B(Transmitted)
Time and Date		OE16	69	1419	Not Chardonaina	22/Transmitten)	11(Leansmitted)	(iransmitted)	P(Transmitted)

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.

# VI-2 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.

## VI-2-1 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.

Anto Lagout : 🛛 🖉	-dher	16:2001 <b>G</b> r
Dashboard	New	
Status -		
Switch LAN	SNMP View	
Security +		_
ACL	View Name:	
0eS -	OID Subtree:	
System Mana	Type: © Included © Excluded	
LLDP		
SNMP		
	View OID Subtree Type	Delete
	al I Included	
Engine fo		
Trup Event		
Notification .		
Access Manager		
Time and Date		

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.
Туре	Determine to include or exclude the selected MIBs.
АррІу	Apply the settings to the switch.

## VI-2-2 Group

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

Auto Logout 2 08 💌	amio		nisis 🕞
Dashboard	Group		
Status	-		
Switch LAN	-	SNMP Group	
Security	+ 11 A A A A A A A A A A A A A A A A A A		
ACL	- Group Name:		
QoS	- Version:	© SNMPV1 © SNMPV2 © SNMPV3	
System Manlessore	Security Level:	No Security Authentication Authentication and Privacy	
LLDP	Read View	- Enabled all	1.1
SNMP	Write View	C Enable ali	4-C
	Notify View	🗇 Enable 🔐	
	100	400	
Gipermania			
	2.412.1.12.1		
Engine IL)	Group Name Version	Security Level View (Read) View (Write) View (Notity)	Le Edit
		No data available in table	
Nitrication			
Access Manager			
Time and Date			

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.
	No Security - No authentication and no encryption.
	Authentication - Requires authentication but no encryption.
	Authentication and Privacy -Requires authentication and encryption.
Read View	Enabled - Users of this group have the right to read the selected MIB view.
	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	Enabled - Users of this group have the right to write the selected MIB view.
	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	Enabled - Users of this group have the right to send notification for the selected MIB view.
	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.

# VI-2-3 Community

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

Auto Logout : Dif	8	Admin				ustans 🕒
Dashboard		SHMP Community				
Status	~					
Switch LAN		Community Name:	Entre Dour	amondy filame		
Security	-	Тура:	🛞 Basic 🔘	Advanced		
ACL	7	Views	-ail.			
QoS		Access Right	Read Only	C Read & Write		
System Managements		Group:				
LLDP				Add		
SNMP						
View		Community Name	Group	View	Access Right	Edit
նուր		public		aii	Read & Write	0
Trop Event						
Notific diam						
Access Manager						
Time and Date						

Item	Description
Community Name	Enter a name as community name. The maximum length of the text is limited to 23 characters.
Туре	<ul> <li>Basic - View and access right can be specified for such SNMP community profile.</li> <li>Advanced - Specify one of the SNMP groups for such SNMP community profile.</li> </ul>
View	Simply specify one of the view profiles (created in SNMP>>View) from the drop down list.
Access Right	Read Only - It allows unidirectional access to node-specific information. Read & Write - It allows bidirectional access to node-specific information.
Group	Specify the SNMP group configured by user (SNMP>>Group) to define the object available to the community.
Add	Click it to add a new community.
Edit	Click the icon under Edit to remove the selectd community strings.

# VI-2-4 User

This page allows a user to configure SNMP user profile.

Auto Logout : Of 🛛 🗟	- diman	08.00(19) 🕞
Dashboard	User	
Status	*	
Switch LAN	Style User	
Security		
ACL	User Name:	
005	Group: 122	1 -
Secon Municipaese	Security Level No Security Authentication Authentication and Privacy	
LLDP	Autheniication Method:	
SNMP	Method: None MDS SHA	
	Password:	
	Privacy:	
Community	Method: None DES	
	Password:	
Enon O		
Tise Envil		
Nothealten		
Access Manager	User    Group    Security Level Authentication Method    Privacy Method	Edit
Time and Date	User_1_came 122 NoAutr Kone None	Ø 🙆

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. No Security - No authentication.
	Authentication - Authentication without encryption will be performed for packets.
	Authentication and Privacy - Authentication with encryption will be performed for packets.
Authentication Method	It is available when Authentication or Authentication and Privacy is selected as security level.
	Method - At present, available methods include None, MD5 and SHA.
	Password - Enter a password for the selected method.
Privacy	It is available when Authentication or Authentication and <b>Privacy</b> is selected as security level.
	Method -At present, available methods include DES and None. Password - Enter a password for the selected method.
Add	Click it to add a new user profile.
Edit	I click it to modify the settings for the selected profile.
	click it to remove the selected entry.

Edit SNMP User=Carrie_FI	× oor
Group: TEST2	•
Security Level: <ul> <li>No Auth </li> <li>Auth &amp; Press</li> </ul>	ivacy
Authentication Method:	
Method   None  MD5  SHA	
Password:	
n Privacy:	
Method: <ul> <li>None  <ul> <li>DES</li> </ul> </li> </ul>	
Password:	
20	
OK Cancel	

# VI-2-5 Engine ID

#### VI-2-5-1 Local Engine ID

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

Auto Lognut : 00	-8	Almin		08.26.01	Ð
Dashboard		Local Engine ID Remote Engine ID			
Status	-	The second second second	and the second		_
Switch LAN	-		Local Engine (D)		-
Security	3	4-5.55	347 T 2 37 T		
ACL.		Engine ID:	User Defined 80005x9202001daa2cca06 (D - 84 Introductional connautors)		
QoS	-		Apply		
	-				
LLDP					
SNMP	1				
View					
Viser					
Trap Event					
Notineation					
Access Manager					
Time and Date					

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".
	<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.

#### VI-2-5-2 Remote Engine ID

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

Auto Logout : 06	10	Admin		(8:29:51	Ð
Dashboard		Local Engine ID Remote Engine ID			
Status					_
Switch LAN	-		SNMP Uker		
Security					
ACL		Address Type:	⊗ Hostname © IPv4 © IPv6		
QoS	-	Server Address:			
System Mandanents	-	Engine ID:	(1U =64' heradetimal characters)		
LLDP			Add		
SNMP	1				
Varw		Server Address	Engine ID Edit		
Group		172.163.9	B0006a9203001daa112244		
Community					
	_				
Trup Event					
Notification					
Access Manager					
Time and Date					

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. The engine ID is range10 to 64 hexadecimal characters, and the hexadecimal number must be divided by 2.
Add	Click it to create a new profile.
Edit	<ul> <li>Click it to modify the settings for the selected server profile.</li> <li>Click it to remove the selected entry.</li> <li>Click it to remove the selected entry.</li> <li>Click it to remove the selected entry.</li> </ul>
	IP=172.16.8.2
	Engine ID: 80006a9203001daa1 (10-64 pairs of hex char)
	OK Cancel

# VI-2-6 Trap Event

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

			08.31.33
Tran	Ewel		
Ratus -			
Switch LAN		Trap Event	
Security	Link Up / Down: Cold Start:	9 Enable 9 Enable 9 Enable 9 Enable	
Conninay Liger Engine ID Yaşı Elwent Notific Julia Kocas Manager			

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

# VI-2-7 Notification

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

Auto Logout : 08	2			18:35 (9	D+
Dashboard		Nitification			
Status		discussion of the local discus	NotAcations		1
Switch LAN					
Security	-	Address Type:	🔿 Hostname 🛞 IPv4 🔿 IPv6		
ACL	7	Server Address:			
005	. *	Version:	© SNMPv1 © SNMPv2 © SNMPv3		
System Mantenance		Type:	🛞 Trap 🛛 Inform		
LLDP		Community/user	public -		
SNMP		Security Level:	No Security Authentication Authentication and Privacy		
Strath		Server Port:	P Use Default (67) [1 - 65535, default (62)		
Community		Timeout	Use Default 15 sec (1 - 300, default 15)		
		Retry:	- Use Default (1 - 255; default 3)		
			Add		
Trap Everat					
Visible store					
Access Manager		Index Server Address Server Por	and the second se		
Time and Date		u 192,168 1,52 162	SIMPV1 Traps public NoAuth		00

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).
Туре	Specify Notification Type. <b>Trap</b> -Send SNMP traps to the host. <b>Inform</b> - Send SNMP informs to the host. If it is used, Timeout and Retry also shall be defined.
Community/user	Use the drop down list to choose one of the community profiles.
Security Level	<ul> <li>Specify SNMP security level for SNMP notification packet. It is available when SNMPv3 is selected.</li> <li>No Security - No authentication.</li> <li>Authentication - Authentication without encryption will be performed for packets.</li> <li>Authentication and Privacy - Authentication with encryption will be performed for packets.</li> </ul>
Server Port	Specify the UDP port number for the recipient's server. Use Default - If it is checked, the default number (162) will be used automaticallty.
Timeout	Specify the SNMP informs timeout. It is available when Inform is selected as Type. Use Default - If it is checked, the default number (15) will be used automaticallty.
Retry	Specify the SNMP informs retry count. It is available when

	Inform is selected as Type. Use Default - If it is checked, the default number (3) will be			
	used automaticality.			
Add	Click it to create a new notification profile.			
Edit	<ul> <li>Click it to modify the settings for the selected server profile.</li> <li>Click it to remove the selected entry.</li> </ul>			
	Edit Notification Entry for Server IP=192.168.1.1			
	Version: ○ SNMPv1 ⊙ SNMPv2 ○ SNMPv3 Type: ⊙ Trap ○ Inform			
	Community/user			
	Security Level: <ul> <li>No Security  </li></ul> <li>Auth  </li> <li>Privacy</li>			
	Server Port:  ☑ Use Default 162 (1-65535)			
	Timeout: Vse Default sec (1-300)			
	Retry: Use Default (1-255)			
	OK Cancel			

# VI-3 Access Manager

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

Auto Logout : Dif	2	Adren		in com 🕞
Dashboard		Accest		
Status	-			
Switch LAN			Access Settings	
Security				
ACL	-	HTIP Service:	Enabled O Disabled	
QoS		HTTPS Service:	④ Enabled	
Evaluary Magazantan	-	Telnet Service:	Enabled      Disabled	
LLDP		SSH Service:	Enabled () Disabled	
SNMP			Apply	
Access Manager				
Time and Date				
Backup Manager				
Upgrade Manager				
Firmware Information				
Account Manager				
Factory Default				
Rebool Switch				
Diagnostics				

j <del></del>	
Item	Description
HTTP Service	HTTP is the acronym of HyperText Transfer Protocol.
	Enabled -Click it to enable HTTP service.
HTTPS Service	HTTPS is the acronym of Hypertext Transfer Protocol over Secure Socket Layer.
	Enabled - Click it to enable HTTPS service.
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.
	Disabled - Click it for not accessing telnet service.
	Enabled - Click it to access telnet service.
SSH Service	Enabled - Enable SSH service.
Apply	Apply the settings to the switch.

# VI-4 Time and Date

# VI-4-1 System Time Zone

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

Auto Logour : 3 min 3	8	Admin		09 50.52 🕞
Deshboard		System Time Zone Time		
Status	~			
Switch LAN	-		System Time Zone Setting	
Security	-	Time Zone:	Today Tree Tree	
AGL.	-	Daylight Saving Time:	Drawble	
QueS	1		Apply	
LLDP			System Time Zona Informations	
SNMP		Terror and the second s		
		Current Date/Time	09:50.47 (UTC+8) Jan. 8 2000	
Access Manager	_	Time zone	UTC+6	
Time and Date		Daylight Saying Time	Elisabled	
Backup Manager				
Upgrade Manager				
Firmware Information				
Account Manager				
Factory Default				
Reboot Switch				
Diagnostics	1			

Item	Description				
System Time Zone Setting	System Time Zone Setting				
Time Zone	Use the drop down menu to select a time zone that VigorSwitch is located.				
Daylight Saving Time	<ul> <li>Select the mode of daylight saving time.</li> <li>Disable -Disable daylight saving time.</li> <li>Recurring - Using recurring mode of daylight saving time.</li> <li>Non-Recurring - Using non-recurring mode of daylight saving time.</li> <li>USA -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>European - Using daylight saving time in the Europe that starts on the last Sunday.</li> </ul>				
Daylight Saving Time Offset	It is available when <b>Recurring</b> is selected as Daylight Saving Time. Specify the adjust offset of daylight saving time.				
Recurring From / To	It is available when <b>Recurring</b> is selected as Daylight Saving Time. From - Specify the starting time of recurring daylight saving time. To - Specify the ending time of recurring daylight saving time.				
Non-recurring From / To	It is available when <b>Non-Recurring</b> is selected as Daylight Saving Time.				

	<ul><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.

# VI-4-2 Time

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

Aute Logout : 3 min	8	Admin	· 编辑 (1)
Dashboard		System Time Zone	
Status	-	Manual Time:	Year Month Day Hours Minutes Seconds
witch LAN	-	indiana time.	2000 - Jav - 8 - 9 - 66 - 4 -
Security	-		
CL		Enable SNTP:	🛞 Enable 🔿 Disable
Roll		SNTP/NTP Server Address:	pool nto org (X.X.X.X er Hostname)
yatam Mantonairgo		Server Port:	123 (1 - 65535   Default : 123 )
LDP			
SNMP-		Apply	
Access Manager			
Time and Date	1		
Backup Manager			
Ipgrade Manager			
firmware Information			
Account Manager			
actory Default			
Reboot Switch			
isignentics	1		

Item	Description
Manual Time	Specify static time (year, month, day, hours, miniutes and seconds) manually.
Enable SNTP	Enable - Click it to enable SNTP time server. Disable - Click to disable the time server.
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.

# VI-5 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.

Anto Logont : 3 mm	10				09.67.67 🕞
Dashboard	Back	up Minager			
Status		Backup Method:	TFTP	a	
Switch LAN	+		(F)P	8	
Secunty		Server IP:	Erza: Seven IP		(IPv4 or IPv6 Address)
ACL		Backup Type:	Configuration		
205			Apply		
System Maintenature	3				
LLDP					
SNMP					
Access Manager					
Time and Date					
Backen Miniager					
Upgrade Manager					
Firmware Information					
Account Manager					
Factory Default					
Reboot Switch					
Diagnostics	÷				

Item	Description
Backup Method	Select Backup method. TFTP - Using TFTP to backup firmware. HTTP - Using WEB browser to ubackup firmware.
Server IP	It is available when TFTP is selected as Backup Method. 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.

# VI-6 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.

Auto Logout : 01	۲	Autor		10:36:50 🕞
Dashbuwd		Upgrade Manager		
Status	4	Ilpgrade Method:	भाष	
Switch LAN				
Security		File/Path:	【 <u>增厚復亮</u> 】未道理當兩	
ACL		Upgrade Type:	@ Image 🔘 Configuration	
QoS	4		Apply	
System Mandanana e	1			
U.DP				
SNMP				
Access Manager				
Time and Date				
Backup Manager				
Operator Manager				
Firmware Information				
Account Manager				
Factory Default				
Reboot Switch				
Diagnostics	~			

Item	Description		
Upgrade Method	Select Upgrade method: TFTP - Using TFTP to upgrade firmware. HTTP - Using WEB browser to upgrade firmware.		
Server IP	It is available when TFTP is selected as Upgrade Method. Enter the IPv4/IPv6 address for the TFTP server.		
File Name	It is available when TFTP is selected as Upgrade Method. Enter the firmware image or configuration file name on the TFTP server.		
File/Path	It is available when HTTP is selected as Upgrade Method. Choose the firmware file located in your computer.		
Upgrade Type	It is available when TFTP is selected as Upgrade Method. Image - Click it to upgrade the firmware image. Configuration - Click ito to upgrade the configurations for VigorSwitch.		
АррІу	Apply the settings to the switch.		

# **VI-7 Firmware Information**

Auto Logout : Of 🦉		Admin			10:36:42 E	B+
Dashboard	Emware Informa	1017				
Status	-					
Switch LAN	-	Active Image:	Firmware T			
Security	-			apply		
ACL		Fermine 1 Militation				
00S						
	Mode	Active	Version	Build Time	Size (MB)	
LLDF	Backup	1	10.2	2017-08-29 09:44:57	6276667	
SNMP		Firmware 2 Inform won				
Access Manager	Mede	Active	Version	Build Time	Size (MB)	
Time and Date	Active	v	221	2017-11-15 11:37 11	6814428	
Backup Manager						
Upgrade Manager						
Account Manager						
Factory Default						
Reboot Switch						
Disensetics without(0)	4					

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

Item	Description		
Active Image	There are two versions of firmware. Simply choose the one you want as primary firmware.		
АррІу	Apply the settings to the switch.		
Firmware 1 Information	rmation Mode - Display the mode (Active or Backup) of the firmware.		
Firmware 2 Information	Active -Display the status (in use or not) of the firmware.		
	Version - Display the switch version.		
	Build Time - Display the built time of the firmware.		
	Size (MB) - Display the size of the firmware.		

# VI-8 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.

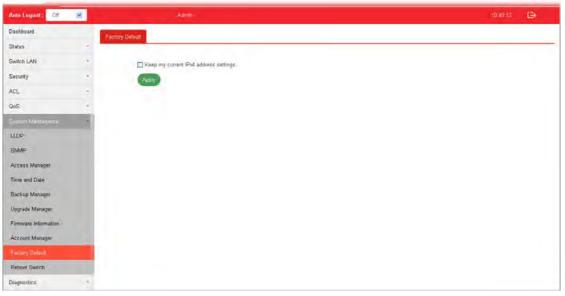
Anto Logout : Co	*	(edman			103854 <b>G</b> e
Dashboard		Local User Information			
Status	-	No. of Concession, Name			
Switch LAN	-			Account	
Security		User Name:	Enter Usi	ay Nama	
ACL		Password:	Exter Pa	land f	
OoS	•	Retype Password:			
			Enter Tu	11 m 2	
LLDP		Privilege Level:	Admin		
SNMP				Apply	
Access Manager		1		Local Users	
fime and Date			6 6 T.	1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1	
Backup Manager		User Name	Password Type	Privilege Type	Modify
Upgrade Manager		admin	Encrypted	admin	0
Firmware Information		user_carrie	Encrypted	admin	Ø 📵
Account Manager					
Factory Default					
Reboot Switch					
Diagnostics	+				

Item	Description	
User Name	Enter a username for new account.	
	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.	
	Admin - Allow to change switch settings.	
	User - See switch settings only. Not allow to change it.	
Apply	Apply the settings to the switch.	
Delete	Remove the selected account.	
Edit	<ul> <li>Click it to modify the settings for the selected user profile.</li> <li>Click it to remove the selected entry.</li> </ul>	

	Edit User: user_carrie	×
rd: :	Retype Password:	
	PrivilegeType:	•
	OK Cancel	1

## **VI-9 Factory Default**

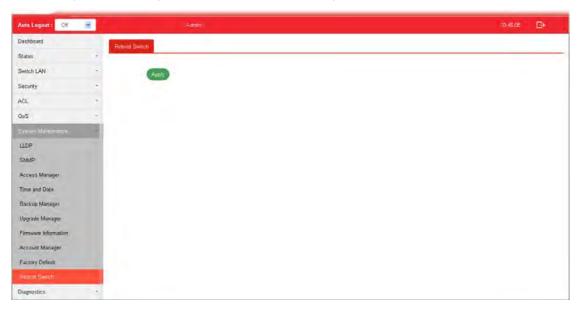
Click Apply to return to factory default settings for VigorSwitch.



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

## VI-10 Reboot Switch

Click Apply to reboot VigorSwitch with current settings.



This page is left blank.

# Part VII Diagnostics

VigorSwitch G2280 User's Guide

# **VII-1 Cable Diagnostics**

Auto Logout : 06		Admin		10.47.45 🕞
Dashboard	Copper	Tied		
Status				
Switch LAN			Copper Test	
Security	-			
ACL		Ports	GE1, GE2, GE3, GE4, GE5, G66, GE7, GE8, GE9, GE10, GE11, GE1	12, GE13, GE14, GE15, GE16 *
OoS	-		🖸 Slan	
System Maintenance				
มีแลการเมิงแ	Port		Result	ile ii
Subje Diagonation	GET		FAIL	S
Ping Test	GE2		PASS	
SysLog	GE3		FAIL	
	GE4		FAIL	
	GES		FAIL	
	GEB		FAIL	
	GE7		FAIL	
	GEB		FAIL	
	GEB		FAIL	
	GE10		FAIL	

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

Item	Description
Port	Use the drop down list to select the port (GE1 to GE28) or ports for performing cable diagnostics.
Start	Perform the copper test action.

# VII-2 Ping Test

Auto Logaut : 💴 🖉	8	Admos		10:50:55	
Dashboard		Pieg Teal			
Status	-				
Switch LAN	- 1		Ping Test		
Security	-				
ACL	-	Protocol	iPv4:	-	
Cos	-	Host:	192.168.1.224	(RF)4 widdress or hostname)	
System Maintenance		Count:	4	(i-5)	
Dragment is (	- 5	Interval (sec):		2 (1 - 5)	
Cable Disgnostics			CSter CSton		
Dag 1ed	(		Contraction State		
SysLug		P195 194.108.1.274 (194.108.1.274); 16 dat 54 gyrs from 103.106.1.3231 time period of 64 gyrs from 109.106.1.3241 time period to 65 gyrs from 195.106.1.3241 time period to 64 kyrss from 103.106.1.3241 time period to 64 kyrss from 103.106.1.3241 time period to 195.108.1.3242 ping statistics 4 packetd teammatted, 4 packets reprived, round-time packets reprived, so (Process is finished)	1464 time0.0 ms 1464 time0.0 ms 1464 time0.0 ms 1464 time0.0 ms		

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

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.
	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.

# VII-3 SysLog

### VII-3-1 SysLog Explorer

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

Auto Logout : 🛛 💭	8				006150 🕞
Dashboard		SysLog Explorer			
Status	-				
Switch LAN				SysLog Filter	
Security	-				
ACL	-		Source:	Vilatile Memory	O
QoS	1.0		Severity:	SILMINE production	
System Maintenance	-		Category:	Magning: web-man	
ó usudar				View	
Cable Diagnostics					
Piog Ten		Source		Volatile Memory	
SysLog		Seventy		emerg, alert, crit, error, warning, notice, into,	10000
		Category			HCP_SNOOPING, GVRP, IGMP_SNOOPING, IPSG
SysLog Selling		Total Entries		ig	ner_anocrina, over, ionir_anocarino, irac
		and proved			
				SysLog Message	
		OReferen Ocka			
		Constant October			

ltem	Description
Source	Volatile Memory - Explore the logs contained in volatile memory (also known as RAM). Non-Volatile Memory - Explore the logs contained in non-volatile memory (also known as Flash).
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. 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.

### VII-3-2 SysLog Settings

#### VII-3-2-1 SysLog Service

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

Auto Logoot : 0/	*	Admm		105429 D
Dashboard		Systog Sinnet Local Systog Remote Sys	Log	
Status	-	Personal Per		
Switch LAN	-	SysLog Service:	💿 Enable 🔘 Disable	
Security		Apply		
ACL	-			
0oS				
System Maintenance				
	-			
Cable Diagnostics				
Ping Teul				
SysLog				
Systing Explorer				
System Settings				

Item	Description
SysLog Service	Enable - Click it to activate function of syslog. Disable - Click it to inactivate the function.
Apply	Apply the settings to the switch.

### VII-3-2-2 Local SysLog

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

Daskbald   Status   Status   Security   ACL   Code   Security   ACL   System Mantenance   System Mantenance   Code Diagnostick.   Ping Twit   Source   Sou		Overlage Contrast			
Status St	States		Remote SysLon		
Act Security					
ACL Source: Filterry without of Annoly Constraints of Annoly Const	Switch LAN	-		Local SysLeg Settings	
Act Severity: Interior Severity: Interior Severity Provide Status Severity Pro	Security	-			
Auguster Maierenance - Auguster -	ICL.	- Source:	0.0nt	and addeded	
Cable Diagnostica. Ping Text Status    Severity    Delete	045	- Severity:	larne	nğ	
Cable Diagnostics. Ping Test Source II Status II Severity II Delete	System Maintenance			(Heady)	
Ping Text Source Status Severity Delete	waged the second	F			
Pring rest	Cable Diagnostics				
SysLog Volabile Memory enabled emerg, alert, crit, error, warring, notice.	Ping Test	Source	Status	Severity	Delete
	SysLog	Volable Memory	enabled	emerg, alert, crit, error, warning, notice	0
SyitagEgalawa					
SynLing Dettings					

Item	Description
Source	<b>Volatile Memory</b> - Select the volatile memory for saving local log. Volatile memory does not hold the log after reboot or power off.
	Non-Volatile Memory - Select the non-volatile memory for saving.
	If you want to modify Volatile Memory / Non-Volatile Memory, select Volatile Memory / Non-Volatile Memory in this field. Then, use the drop down list of severity to specify type of log message. After clicking Apply, the Volatile Memory / Non-Volatile Memory will be modified with new configured severity level.
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.

#### VII-3-2-3 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.

Auto Logout : Dif	×	Antor			1059-30 🕞
Dashboard		SysLog Service Local SysLog Remote	SysLog		
Status	*				
Switch LAN		10-	Remote SysLog Settings		
Security					
ACL	+	Server Address:	Sprev Server, Addressa		
QoS		Server Port:	514	(1 - 65536)	
System Maintenance		Severity:	emerg	×	
	-	Facility:	local0		
Cable Diagnostics			Approx		
Ping Test	-		Apprix		
System		5.7.50			
SysLog Explorer		Server IP(Port)	Status Seventy	Facility	Delete
Systing Settings			No data available in table	e.	
191.100 [ 224961-6181					

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.

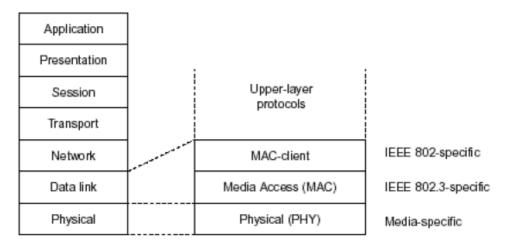
This page is left blank.

# **Appendix: Reference**

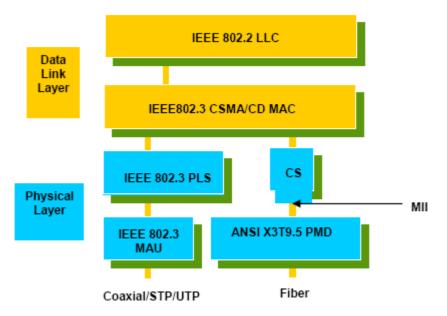
This chapter will tell you the basic concept of features to manage this switch and how they work.

## 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.

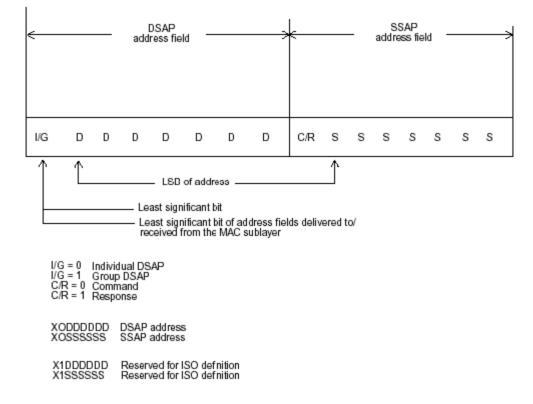
Logical link control supports the interface between the Ethernet MAC and upper layers in the protocol stack, usually Network layer, which is nothing to do with the nature of the LAN. So it can operate over other different LAN technology such as Token Ring, FDDI and so on. Likewise, for the interface 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			Control	Information
	8 bits	8	bits	8 or 16 bits	M*8 bits
SS/	AP address = Destination service access point address AP address = Source service access point address ntrol = Control field [16 bits for formats tha sequence numbering, and 8 bits for do rot (see 5.2)]		point address field formats that include		
Info	rmation	=	Informa	tion field	
*		=	Multiplic	cation	
М		=	An integ (Upper access	er value equal bound of M is a control method	to or greater than 0. function of the medium ology 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.



## 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 numb	er

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.

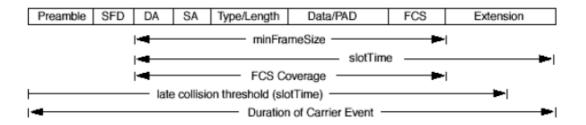
As the transmission of a MAC frame with the half-duplex operation exists only in the same collision domain, the carrier signal needs to spend time to travel to reach the targeted device. For two most-distant devices in the same collision domain, when one sends the frame first, and the second sends the 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.

416 bytes for 1000Base-X 520 bytes for 1000Base-T								•
Preamble	SFD	DA	SA	Length/type	Data	Pad	FCS	Extension*
								•
				64 bytes				-

Parameter value/LAN	10Base	100Base	1000Base
Max. collision domain DTE to DTE	100 meters	100 meters for UTP 412 meters for	100 meters for UTP 316 meters for
		fiber	fiber
Max. collision domain with repeater	2500 meters	205 meters	200 meters
Slot time	512 bit times	512 bit times	512 bit times
Interframe Gap	9.6us	0.96us	0.096us
AttemptLimit	16	16	16
BackoffLimit	10	10	10
JamSize	32 bits	32 bits	32 bits
MaxFrameSize	1518	1518	1518
MinFrameSize	64	64	64
BurstLimit	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.

$$0 \le r < 2^k$$

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.

Pre	SFD	DA	SA	VLAN type ID	Tag control information	Length/ type	Data	Pad	FCS	Ext
-----	-----	----	----	-----------------	----------------------------	-----------------	------	-----	-----	-----

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.

Bits 15-13	User Priority 7-0, 0 is lowest priority
Bit 12	CFI (Canonical Format Indicator)
	1: RIF field is present in the tag header
	0: No RIF field is present
Bits 11-0	VID (VLAN Identifier)
	0x000: Null VID. No VID is present and only user priority is present.
	0x001: Default VID
	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

	А		L
Account Manager, 171, 172		License Agreement, 23	
	В	License Information, 25, 26, 31, 47,	48, 75, 76, 85
Deslaur Managan 160	D	Limiting Rate, 108	
Backup Manager, 169 Bandwidth, 143			Р
Balluwidul, 145	0	Preamble, 107	-
	С	Properties, 110	
CoS Mapping, 140		Properties, 110	0
	D		Q
Dashboard, 16, 17		QoS Configuration, 125, 135	
Diagnostics, 177			S
DoS, 110		Security, 89	
DoS Port Setting, 112		SNMP, 155	
DoS Protection, 112		SNMP Community, 158, 159, 161	
	E	Storm Control, 108	
		Storm Control, 90, 92, 93, 95, 98, 10	04, 106, 107
Egress Shaping Per Queue, 145		Storm Control, 113	
Egress Shaping Rate, 144	_	Storm Control, 116	
	F	Storm Control, 121	
Factory Default, 174		Stric Priority Queue, 139	
	G	System Configuration, 19	
General, 126, 129, 134, 136		System Maintenance, 147	
General Setup, 20			IJ
, , , , , , , , , , , , , , , , , , ,	Ι	Upgrade Manager, 170	C
	1	Opgrade Manager, 170	
Ingress Rate Limit, 143			W
Installation for VigorAPM, 6		Weight, 139	
		WRR Bandwidth, 139	