

# VigorSwitch P2121

PoE L2 Managed Gigabit Switch



Your reliable networking solutions partner

# User's Guide

# VigorSwitch P2121 PoE L2 Managed Gigabit Switch User's Guide

Version: 1.0 Firmware Version: V2.3.2 (For future update, please visit DrayTek web site) Date: September 10, 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	2
I-1-1 Key Features	3
I-1-2 Specifications	3
I-1-3 Packing List	5
I-1-4 LED Indicators and Connectors	5
I-2 Installation	7
I-2-1 Network Connection	7
I-2-2 Rack-Mounted Installation	8
I-2-3 Connection via Console Cable	9
I-2-4 Typical Applications	12
I-2-5 Installing Network Cables	16
I-2-6 Configuring the Management Agent of Switch	16
I-2-7 Managing VigorSwitch P2121 through Ethernet Port	16
I-2-8 IP Address Assignment	17
I-3 Accessing Web Page of VigorSwitch	21
I-4 Dashboard	22
I-5 Status	23
I-5-1 Port Bandwidth Utilization	23
I-5-2 LLDP Statistics	23
I-5-3 GVRP Statistics	24
I-5-4 MLD Snooping Statistics	24
Part II Switch LAN	25
II-1 General Setup	26
II-1-1 IP Address	26
II-1-2 IPv6 Address	27
II-1-3 Management VLAN	28
II-2 Port Setting	29
II-3 Mirror	31
II-4 Link Aggregation	32
II-4-1 LAG Setting	32
II-4-2 LAG Management	33
II-4-3 LAG Port Setting	34
II-4-4 LACP Setting	35
II-4-5 LACP Port Setting	36
II-5 VLA Management	37
II-5-1 Create VLAN	37
II-5-2 Interface Settings	

II-5-3 Voice VLAN	40
II-5-3-1 Properties	
II-5-3-2 Telephony OUI Setting	
II-5-3-3 Port Setting	
II-5-4 MAC VLAN	
II-5-4-1 MAC Group	
I-5-4-3 Group Binding	
II-5-5 Protocol VLAN	45
II-5-5-1 Protocol Group	
II-5-5-2 Group Binding	
II-5-6 Surveillance VLAN	
II-5-6-1 Property	
II-5-6-1 Surveillance OUI	
II-5-7 GVRP	
II-5-7-1 Property	
II-5-7-2 Membership	
II-6 EEE	53
II-7 Multicast	54
II-7-1 Properties	54
II-7-2 IGMP Snooping	55
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 All	
II-7-2-7 Throttling	
II-7-2-8 Filtering Profile	63
II-7-2-9 Filtering Binding	64
II-7-3 MVR	66
II-7-3-1 Property	
II-7-3-2 Port Setting	
II-7-3-3 Group Address	
II-7-4 MLD Snooping	
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	
II-9 STP	
II-9-1 Properties	81
II-9-2 Port Setting	82
II-9-3 Bridge Setting	84
II-9-4 Port Advanced Setting	
II-9-5 Statistics	
II-9-6 MST Instance	

	II-9-7 MST Port Setting	88
	II-10 MAC Address Table	
	II-10-1 Static MAC Setting	
	II-10-2 Dynamic Address Setting	
	II-10-3 Dynamic Learned	
	II-11 Blocked Port Recover	
Part	III Security	95
	III-1 RADIUS	
	III-2 TACACS+	
	III-3 Management Access Authentication	
	III-3-1 Method Profile	
	III-3-2 Application Authentication	100
	III-4 Management Access Control	101
	III-4-1 Management Access Control Profile (ACL)	101
	III-4-2 Management Access Control Entries (ACE)	102
	III-5 802.1X/MAC Authentication	104
	III-5-1 Properties	104
	III-5-1-1 Global Settings III-5-1-2 Port Authentication Setting	
	III-5-2 Port Control/Settings	106
	III-5-3 MAC-Based Local Account	108
	III-5-4 Authenticated Hosts	109
	III-6 Port Security	110
	III-7 Protected Ports	112
	III-8 Storm Control	113
	III-8-1 Properties	113
	III-8-2 Port Setting	114
	III-9 DoS	115
	III-9-1 Properties	115
	III-9-2 DoS Port Setting	117
	III-10 Dynamic ARP Inspection	118
	III-10-1 Properties	118
	III-10-1-1 Global Property Settings III-10-1-2 Per Port Property Settings	
	III-10-2 Statistics	120
	III-11 DHCP Snooping	121
	III-11-1 Properties	121
	III-11-1-1 Global Property Settings III-11-1-2 Per Port Property Settings	
	III-11-2 Statistics	123
	III-11-3 Option82 Property III-11-3-1 Global Option82 Property Settings	

	III-11-3-2 Per Port Option82 Property Settings	124
	III-11-4 Option82 Circuit ID	125
	III-12 IP Source Guard	
	III-12-1 Port Settings	126
	III-12-2 IMPV Binding	
	III-12-3 Save Database	
Part	IV ACL Configuration	
	IV-1 Create ACL	
	IV-1-1 MAC	
	IV-1-2 IPv4	
	IV-1-3 IPv6	
	IV-2 Create ACE	
	IV-2-1 MAC	
	IV-2-2 IPv4	
	IV-2-3 IPv6	
	IV-3 ACL Binding	
_		
Part	V QoS Configuration	
	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-1-5 DSCP Mapping	
	V-1-6 IP Precedence Mapping	
	V-2 Bandwidth	
	V-2-1 Ingress Rate Limit	
	V-2-2 Egress Shaping Rate	
	V-2-3 Egress Shaping Per Queue	153
Part	VI PoE Configuration	
	VI-1 Properties	
	VI-2 Status	
	VI-3 Device Check	
	VI-4 Schedule	
	VI-4-1 Schedule Profile	
	VI-4-2 Port Scheduling	
	, and the second s	
Part	VII System Maintenance	
	VII-1 TR-069	

VII-2 LLDP	·······	164
VII-2-1 Properties		164
VII-2-2 LLDP Port Setting		165
VII-2-3 LLDP Local Device		166
VII-2-4 MED Network Policy		167
VII-2-5 LLDP MED Port Setti	ngs	168
VII-2-6 LLDP Remote Device		169
VII-2-7 LLDP Overloading		170
VII-3 SNMP	······································	171
VII-3-1 View		172
VII-3-2 Group	······································	173
VII-3-3 Community		174
VII-3-4 User		175
5		
	ID ine ID	
-		
VII-4 Access Manager		182
VII-5 Time and Date		183
VII-5-1 System Time Zone		183
VII-5-2 Time		184
VII-6 Backup Manager		185
VII-7 Upgrade Manager		186
VII-8 Firmware Information		187
VII-9 Account Manager		188
VII-10 Factory Default		190
VII-11 Reboot Switch		191
Part VIII Diagnostics	1	193
VIII-1 Cable Diagnostics		194
VIII-2 Ping Test		195
VIII-3 SysLog		196
VIII-3-1 SysLog Explorer		196
VIII-3-2 SysLog Settings		197
	ice	
	g Log	
Appendix: Reference	2	201
A-1 What's the Ethernet		201
A-2 Media Access Control (MAC)		204
A-3 Flow Control		208

# Part I Introduction

VigorSwitch P2121User's Guide

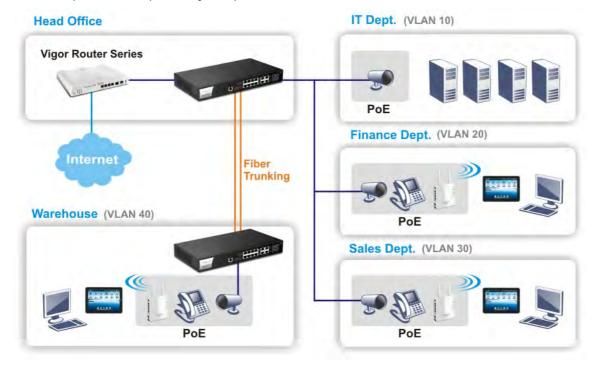
# **I-1 Introduction**

VigorSwitch P2121, 8 Ports + 4 Combo UTP/SFP Ports PoE L2 Managed Gigabit Switch, is a standard switch that meets all IEEE 802.3/u/x/z Gigabit, Fast Ethernet specifications. The switch has 8 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 12 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 P2121, 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

- ✤ 8 10/100/1000Mbps Auto-negotiation Gigabit Ethernet TP ports with PoE+
- 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, PoE fail and PoE/link activity
- 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 802.10 VLAN
- Supports user management and limits three users to login
- Maximal packet length can be up to 9600 bytes for jumbo frame application
- Supports Broadcasting Suppression to avoid network suspended or crashed
- Supports to send the trap event while monitored events happened
- Supports default configuration which can be restored to overwrite the current configuration which is working on via Web UI and Reset button of the switch
- Supports on-line plug/unplug SFP modules
- Supports Quality of Service (QoS) for real time applications based on the information taken from Layer 2 to Layer 3
- Built-in web-based management and CLI management, providing a more convenient UI for the user

## I-1-3 Packing List

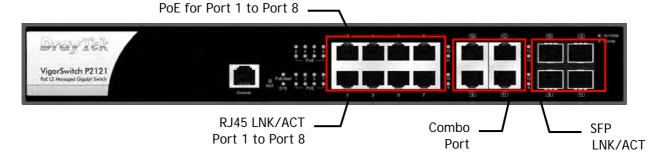
Before you start installing the switch, verify that the package contains the following:

- VigorSwitch P2121
- AC Power Cord
- Quick Start Guide
- Rubber feet
- Rack mount kit
- Console Cable

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

## I-1-4 LED Indicators and Connectors

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



LED	Status	Explanation
PoE/Alert	On (Green)	Devices connected over the PoE maximum power budget.
	Blinking (Green)	More than 80% of maximum power budget is supplied for PoE device(s).
	Off	Devices connected within the PoE maximum power budget.
	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 malfunctioning.		The power is off or the system is not ready / malfunctioning.
	On (Green)	The port is supplied with PoE power.
PoE 1~8	Off	No PoE power is supplied on the port.
RJ 45	On (Green)	The device is connected with 1000Mbps.
LNK/ACT	On (Amber)	The device is connected with 10/100Mbps.

Port 1 ~ 8	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 9 ~ 12	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 10/100Mbps.
	Blinking	The system is sending or receiving data through the port.
	Off	The port is disconnected or the link is failed.

#### **Connector Explanation**

Interface	Description
Console	Used to perform telnet command control.
RST	<ul> <li>Factory reset button.</li> <li>Press it to reboot the system. (&lt;5 seconds) The PoE/Alert and SYS LEDs will blink too.</li> <li>Press it to reset the system with factory default settings. (5~20 seconds)</li> <li>The PoE/Alert and SYS LEDs will be off if RST button is pressed between 5 seconds and 10 seconds.</li> </ul>
RJ 45 LNK/ACT Port 1 ~ 8 PoE for Port 1 ~ 8	Port 1 to Port 8 can be used for Ethernet connection and PoE connection, depending on the device connected.
SFP LNK/ACT Port 9 ~ 12	Port 9 to Port 12 are used for fiber connection.
-	Power inlet for AC input (100~240V/AC, 50/60Hz).

Note:

Power Output -

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

PoE Power Budget--

• 140 Watts

# **I-2 Installation**

# I-2-1 Network Connection

- Use a Cat. 5e twisted-pair cable to connect a PoE device to the port (1~8) of this switch.
- The switch will supply power to PoE Device over the twisted-pair cable.
- Please note that Power Device must comply with IEEE 802.3af/at.
- Other PCs, servers and network devices can be connected to the switch using a standard 'straight through' twisted pair cable.



# I-2-2 Rack-Mounted Installation

The switch can be installed easily by using rack mount kit.

1. Attach the brackets to the chassis of a 19- or a 23-inch rack. The second bracket attaches the other side of the chassis as above procedure.



2. After the bracket installation, the VigorSwitch's chassis can be installed in a rack by using four screws for each side of the rack.

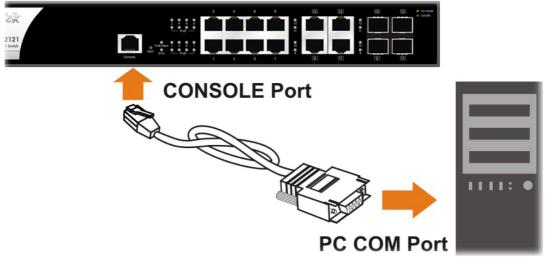


## I-2-3 Connection via Console Cable

You can perform debugging, configuration and firmware upgrade, through the console connection.

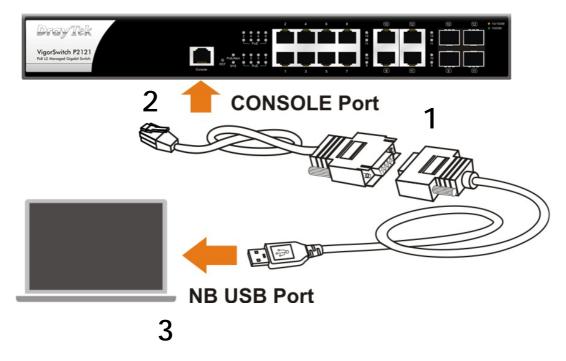
To connect VigorSwitch to a PC via console cable, please

- 1. Connect the RJ45 connector of console cable to the console port on Vigor device.
- 2. Connect the DB9 connector of the console cable to the RS232 port on the PC.



To connect VigorSwitch to a notebook, please

- 1. Connect the DB9 connector of the console cable to the DB9 connector of USB to RS232 cable first.
- 2. Connect the RJ45 connector of console cable into the Console Port of the switch.
- 3. Connect the USB connector to the USB port of the notebook.



#### **Console Port Configuration**

- 1. Open Hyper Terminal on the PC.
- 2. Open the following dialog to configure COM1 Properties as

Baud rate:115200Data bits:8Stop bits:1Parity:NoneFlow control:None

System Prope	erties <b>?X</b>
General Ne	twork Identification   Hardware   User Profiles   Advanced
	vigor 3300 - HyperTerminal COM1 Properties
	Port Settings
-	Bits per second: 57600
	Data bits: 8
	Parity: None
	Stop bits: 1
	Flow control: None
	Restore Defaults
	OK Cancel Apply

Or, you can make configuration via PuTTY utility.

- 1. Make sure the PuTTY utility has been installed on your PC. Execute PuTTY.
- 2. Configure the settings as the following figures. The default settings of the console port are:

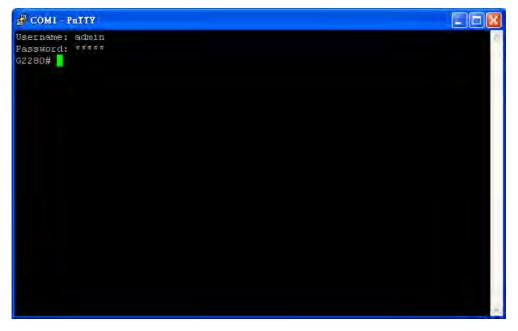
Baud rate:115200Data bits:8Stop bits:1Parity:NoneFlow control:None

🕵 PuTTY Configuration		? 🗙
Category:		
<ul> <li>Session</li> <li>Logging</li> <li>Terminal</li> <li>Keyboard</li> <li>Bell</li> <li>Features</li> <li>Window</li> <li>Appearance</li> <li>Behaviour</li> <li>Translation</li> <li>Selection</li> <li>Colours</li> <li>Connection</li> <li>Data</li> <li>Proxy</li> <li>Telnet</li> <li>Rlogin</li> <li>SSH</li> <li>Serial</li> </ul>	Options controlling loc Select a serial line Serial line to connect to Configure the serial line Speed (baud) Data bits Stop bits Parity Elow control	COM1
<u>A</u> bout <u>H</u> elp		n <u>C</u> ancel
Pully Configuration     Category:     Session     Logging     Termina	Basic options for your F Specify the destination you want Serial line	
Category:	Basic options for your F Specify the destination you want Serial line COM1 Connection type: Raw I elnet Rlogin Load, save or delete a stored set Saved Sessions Default Settings Close window on egit:	to connect to Speed 115200

3. Click Open. The default login is:

Username: admin

Password: admin



# I-2-4 Typical Applications

The VigorSwitch implements 8 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:

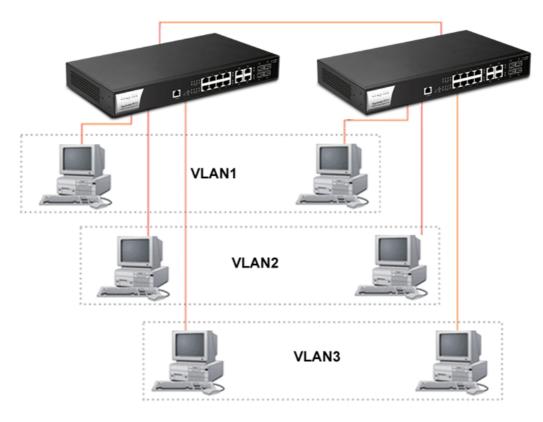
#### Case 1: All switch ports are in the same local area network.

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

#### **Case 3: 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.

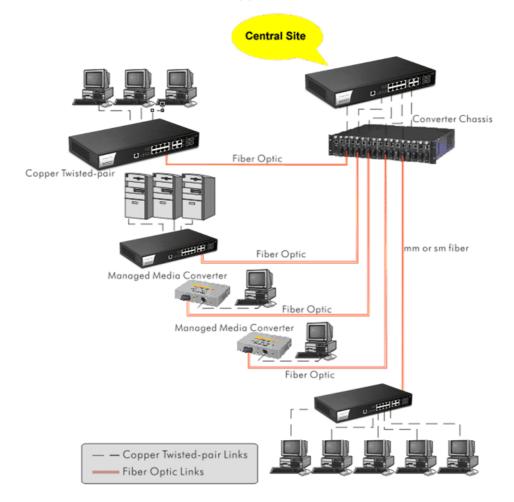
#### **Case 4: Rack-mount Installation**

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.

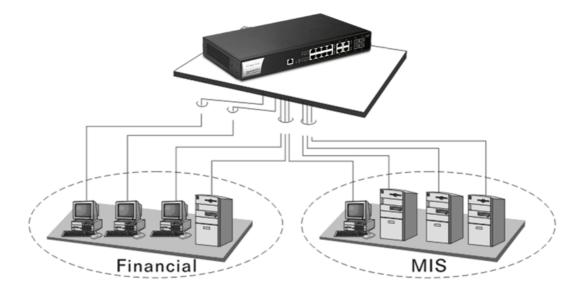
Procedures to Rack-mount the switch:

- 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.

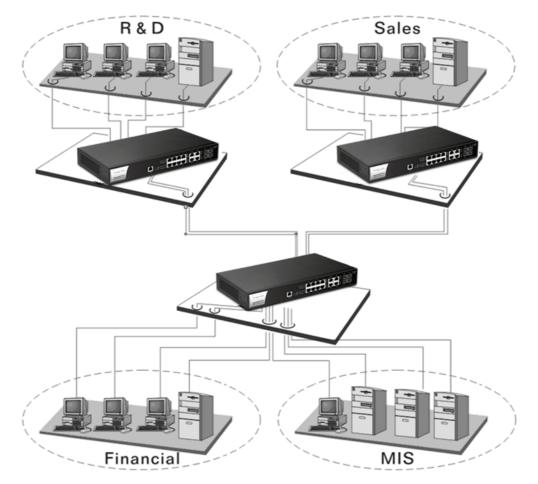
#### Case 5: Central Site/Remote site application is used in carrier or ISP



Case 6: Peer-to-peer application is used in two remote offices



### Case 7: Office network



## I-2-5 Installing Network Cables

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

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

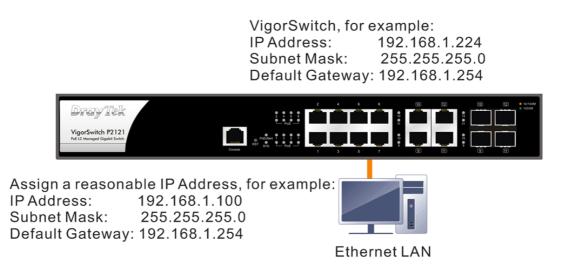
Media	Speed	Wiring
10/100/1000 Mbps copper	10 Mbps	Category 3,4,5 UTP/STP
	100Mbps	Category 5 UTP/STP
	1000 Mbps	Category 5e, 6 UTP/STP

## I-2-6 Configuring the Management Agent of Switch

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

Configuring the Management Agent of VigorSwitch P2121 through the Ethernet Port.

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



# I-2-7 Managing VigorSwitch P2121 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-2-8 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.

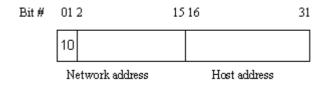
#### Class A:

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 addre	ss	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 addres:	s
	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

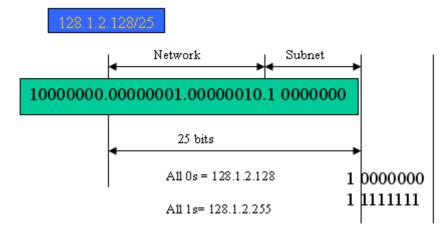
Please refer to RFC 1597 and RFC 1466 for more information.

#### 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.

e <b>k V</b> igor	Switch P2121
admin	
•••••	
	Login
	Login
	admin

3. Now, the Main Screen will appear.

-									04,18	50 🕞
				Da	shboard					
-	Contractor	1.1.1				1.2.1			1.1	
	29 Hebesti	DrawTe	. /	-	2.4	6 8 10	12	10/100		
-				Dell'Mart	***			= 1000M		
-		P2121			1 3 3	5 7 9	1			
-										
-	Da	vice Information			_	System	Information			
	Model	VigorSwitch P2121	CPU	(115)	Memor	48	Cache	21%	POE	0.0% Usage
	Firmware	232		Deage		Memory		Cached		Ocade
	Laader	1.0.3	PoE	Consuming						
	Revision	886	F00%							
	Build Date	2018-05-28 19:09.43								
	System Time	Sat Jan 8 64 18 26 2000								
	System Up Time	6 days 20 18 26	27%							
				8	8	14	8	8	-	9
		Model Firmware Loader Remsinn Build Date System Time	Device Information           Model         VigorSwitch P2121           Firmware         2.3.2           Lader         1.0.3           Renstinn         886           Build Date         2018/05/28 19:09:43           System Time         Sai Jan B 04:18:26 2000	DrayTek           Wigerswitch #7777           Proce Information           Model         Vigorswitch P2121           Firmware         2.3.2           Lander         10.3           Remsion         866           Bund Date         2016/05/28 19:09:43           System Time         Sal Jan 8:04 16:25 2000           System Up Time         6 days 20:10:28	Extrements       Processing       Register         VigorSwitck #3737       Register       Register         VigorSwitck #7372       Register       Register         Model       VigorSwitch P2121       CPU       115         Fermenic       2.3.2       PoE Consuming       PoE Consuming         Remain       888       10%       10%         Build Date       2018.05.28 19.09.43       0%       10%         System Time       Sai Jan 80 64.16 35.2000       37%       30%         System Up Time       6 days 20.10.26       0%       10%	Dray Tek Ways winks #2222     Refailer     Part of the system of the system       Device Information     Provide Information     Provide Information       Model     VigorSwitch P2121     CPU     111       Fermiore     2.3.2     CPU     111       Lander     1.0.3     PoE Consuming       Build Date     2018/05/28 19:09:43     075       System Time     Sai Jan 8/04 16:25 2000     105       System Up Time     6 days 20:10:26     05	Extrements         Decry Teck         Vegersburkte P2222         Peerde Information         System         Model         VigorSburtch P2121         Fermano         2.3.2         Lander       10.3         Remaino       886         Build Date       2018/05/28 19:09:43         System Time       Sau Jan 8:04:18:25:200         System Up Time       6 days 20:10:26	Chrony Tele         Politiket         Politiket	Consuming         Consuming           Remain         88           Build Date         2018/05/28 19.09.43           System Time         Sail Jan 80.41 10.25 2000           System Up Time         6 days 20.10.26	Constraint       Constraint

0

Info

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

# I-4 Dashboard

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

Auto Logout :	3 min	×	
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					
C Refresh			witch P2121	PoE/Alert	4 6 8 10 12 3 5 7 9 11	100 100	Y100M DOM		
	Device Information	I			System	Information			
Model	VigorSwitch	P2121	CPU 1	9%	mory 48%	Cache 21	% Pol	0.0%	
Firmware	2.3.2		Usa	ge	Memory	Cache	d	Usage	
Loader	1.0.3		PoE Consun	ning					
Revision	886		100%						
Build Date	2018-05-28 1	9:09:43	80%						
System Time	Sat Jan 8 04	30:08 2000	40%						
System Up Time	6 days 20:30	:20	20%						
				3:40	8	4100	4: 10	4:20	
				Connection Sta	itus				
IPv4 IPv	6								
rstem Name	Location	Contact	MAC	Protocol	IP	Gateway	DNS	Modify	

# 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 GE12). In which, data of interframe gap can be displayed or hidden by choose **Enable / Disable** for IFG.

										Vigoi	Switch P21
										0420342	G
Status *	Port Bandwidth Utilizat	ion > Poir Eandw	idth Utilization								
Tree Brownie	the Distance of Contract										
-				_							
Auto Refresh:	2 Sec	• IFG: E	nable	-							
_											
Gbps	TODMbps	TOMbps	Link Down								
					Is						
AD 1											
70 H - 50 T											
401-											
30%											
10 x -											
- ro	i je	-100	3	le .	į	-100	į	1	80-	- tig	-Sa
					Rx						2
4012 -											
603											
	Pod Escound Auto Refresh: • Copic • C	Status > Port Backwith Unised      Port Backwith Unised      Anto Refrest: 2.5ec      Claps     Tothogs     Set     Set	Port Bendwitth Utilization           Auto Refrest:         2 Sec.         IFG:         E           • Gbps:         • 000Mbps:         • t0Mbps:         • t0Mbps:           • 000Mbps:         • t0Mbps:         • t0Mbps:         • t0Mbps:           • 000Mbps:         • 000Mbps:         • 000Mbps:         • 000Mbps:           • 000Mbp:         • 000Mbps:         • 000Mbps:         • 000Mbps:           • 000Mbps:         • 000Mbps:<	Status > Por Bandwidth Witzanion > Por Bandwidth Utilization Por Bandwidth Utilization Anna Refredi: 2.5ec • IFG: Enable  Cope • 100Mogo • 10Mogo • Link Dover  Status	Statur > Pon Bacowith Ukization > Part Bandwidh Ukization      Pon Bacowith Ukization      Anto Refresh: 2.5sc • IFG: Enable      Objes 100Mbgs 10Mbgs Link Down      status      sta	Statu - Port Bandwith Uhization - Part Eundwith Uhization      Port Bandwith Uhization      Anto Refrest: 2.5sc • IFG: Enable      Objec • 100Mege • 10Mege • Link Down      Statu      Statu	Status - Pen Bacdwidth Whitzation - Pen Eandwidth Ultization  Prof Bacdwidth Whitzation  Anto Refrest: 2.5ac • IFG: Enable -  Cobpe • 100Mbgs • 10Mbps • Lok Down  Set	Statu - Por Bardwith Unization - Por Eandwith Unization   Por Bardwith Unization   Por Bardwith Unization   Anto Refresh: 2.5e: • IFG: Enable   Objec   Objec </td <td>Status &gt; Port Bandwith Witzation &gt; Port Bandwith Unization  Port Bandwith Unization  Anna Refresh: 2.5ec • IFG: Enable -  Chps • 100Mbps • Inh Down  Status -  Status</td> <td>Statu - Prin Backwath Uhization - Pein Bandwidh Uhization  Point Backwath Uhization  Anto Refresh: 2.5x. + IFG: Enable  Objes  ODMoge  ItMope  Lak Down  Iz</td> <td>Um         000000000000000000000000000000000000</td>	Status > Port Bandwith Witzation > Port Bandwith Unization  Port Bandwith Unization  Anna Refresh: 2.5ec • IFG: Enable -  Chps • 100Mbps • Inh Down  Status -  Status	Statu - Prin Backwath Uhization - Pein Bandwidh Uhization  Point Backwath Uhization  Anto Refresh: 2.5x. + IFG: Enable  Objes  ODMoge  ItMope  Lak Down  Iz	Um         000000000000000000000000000000000000

# I-5-2 LLDP Statistics

This page offers the statistics of LLDP packets (in, out and error) of each port (GE1 to GE12).

Auto Logoni : 3 mm	2								045143 🕑	
Dashboard		O Statio = 1	LOP Statute	P.Statistic:						
		LLDP Standie								
Port Bandwidth Utilization		there shared								_
UDP Intinici					L	LDFI Global Statistics				
GVRP Statistics		-	-							
MLD Snooping Statistics		Refresh	Clear All							
Switch LAN	-	Insertions						45		
Security	-	Deletions						43		
ACL		Drops						0		
QoS										
PoE		Age Outs						0		
System Maintenance	+	24.4				LLDP Port Statistics				
Diagnostics		Port	TX Frames	RX Frames Total	RX Frames Discarded	RX Frames Errors	RX TLVs Discarded	RX TLVs Unrecognized	RX Ageouts	
		GE1	402	-402	0	0	D	u	u	
		GE2	3	0	0	0	D	D	0	
		GEB	298	0.96	n	0	10	n	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.

Auto Logout : 3 min									
Dashbeard		O Statos	= GVRP Statistica + Statistica						
		Statistics							
Port Bandwidth Utilization		- HEALINGS							
LLDP Statistics Port:			- 1	3E1, GE2, GE3; GE4, GE5, GE6, GE	7, GEB, GE9, GE10, GE11	GE12, LAG1, LAG2, LAG3, L	AG4, -		
GARR Searce Statistics				15	frankmit, Receive, Errov				
MLD Snooping Statistics			Refresh Rate:		i0 sec				
Switch LAN	-		nenesi nate:		lo sec				
Security		-			Ty Statisti				
ACL	-	-			TX Source	<i>b</i>			
QoS	10	Port	Join empty	Empty	Leave Empty	Join In	Leave in	Leave All	
PoE		GE1	Ø	0	ū	D	D	0	
System Maintenance		GE2	0	0	0	a	0	0	
Diagnostics		GE3	Ð	a.	ū	ø	Ū	ä	
		GE4	α	- a	-10	ø	п	0	
		GES	0	0.	0	0	0	0	
		G66	0	0	.0	u	0	0	
		GE7	0	a.	Ū	a	U	0	

# I-5-4 MLD Snooping Statistics

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

Auto Logout : 3 min	2			000,400 De
Dashboard		Statur + MLD Synophy Statetics + Statistics		
	3	Stationer		
Port Bandwidth Utilizatio	n			
LLDP Statistics		Refresh     OClear All		
GVRP Statistics		8-	Rx Statutica	
MLD Streeping Sciencies	(C) (			
Switch LAN		Rx Total		0
Security		RX Valid		a
ACL		Rx Invalid		α
QoS		Rx Other		ö
PoE		RxLeave		۵
System Maintenance		Rx Report		ū.
Diagnostica		Rx General Query		Û.
		Rx Special Group Query		п
		Rx Source-specific Group Query		ñ
			Tx Statistics	2
		TxLeave		0.

# Part II Switch LAN

VigorSwitch P2121User's Guide

# II-1 General Setup

() Info

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.

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.

Auto Logout : Cm	8			0854/30 🕞
Dashboard	IP.Ad	diesai		
Status	-		Conf. D. John	
WICH LAN	4	Mode:	Static: ○DHCP	
General Setup		IP Address;	192,160,1,22#	
In Address		Subnet Mask:	255.255.255.0	
(Pvő Adaress		Gateway	192.169.1.1	
Management VILAN		DNS Server 1:		
Port Setting		DNS Server 2:		
Mittor				
Link Aggregation		APEN		
VLAN Management				
EEE				
Multicast				
Jumbo Frame				
STP				
MAC Address Table				
Security	+			
ICL.				
QuS				
Ъ				
System Maintenance				

Available settings are explained as follows:

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.

Auto Logout : Off 🛛 🖌	Tom				10:39:31	Ð
Dashboard		iress				
Status -						
Switch LAN -	IPv6 Address					
General Setup	Auto Configuration:	🔿 Enable 💿 Disable				
IP Address	IPv6 Address:	2001:b031:7008:ff00:21d:aaff:fe11:3366	1	64		
IPv6 Address	Link Local Address:	fe8D::21d:aaff:fe11:2244	/	64		
Management VLAN	Gateway:	2001:b031:7008:ft00:21d:aaff:fe11:2260				
Port Setting	DNS Server 1:	2001::7008:ff00:21d:aaff:fe11:2258				
Mirror						
Link Aggregation	DNS Server 2:	2001::7008:ff00:21d:aaff:fe11:2259				
VLAN Management	Apply					
EEE						
Multicast						
Jumbo Frame						
STP						
MAC Address Table						
Blocked Port Recover						
Security -						

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.
АррІу	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 🖉	User		06/1261	G
Dashboard	O General Sidop + Management VLAV + Manage	ament VLAN Sotting		
Status -	Management VLAN Setting			
5x-101-x40			 	
General Setup	Management VLAN:	default(1)		
IP Addpess	Apply	dafault[1]		
IP√F Ad∱ress	and the second sec			
Management VLAN				
Port Setting				
Mirror				
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 Logout : 3 min	2		Vie	e.					061456	Ð
Dashboard Status		Purt Setting	WV ⇒ Port Satting ⇒ Pr	n Setting						
General Setup			Ports:		Motory (Windows				+	
Unit Satura Murice Link Aggregation VLAN Management EEE Multi-cast			Enable State: Speed: Duplex: Flow Control:		<ul> <li>Enable C Dis</li> <li>Auto</li> <li>Auto</li> <li>Enable C Dis</li> </ul>		ol e co		4	
Jumbs, Frame		Port	Description	Enable State	Link Status	Speed	Duplex	FlowCtrl Config	FlowCtrl Status	Modify
MAC Address Table		GE1		Enabled	Down	Auto	Auto	Enabled	Disabled	0
Blocked Port Recover		GE2		Enabled	Down	Auto	Auto	Enabled	Disabled	0
Security	,	GES		Enabled	Diawn	Auto	Auto	Enabled	Disabled	0
ACL .	-	GE4		Enabled	Down	Auto	Auto	Enabled	Disabled	0
QoS	-	GES		Enabled	Dawn	Auto	Auto	Enabled	Disabled	0
	_	086		Encolor	Dawn	Aite	Auto	Eponios	Glephind	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.
	• 1000M: Force speed with 1000M ability.
	Selecting Auto (auto-negotiation) allows one port to negotiate with a peer port automatically to obtain the connection speed and duplex mode that both ends support. When auto-negotiation is turned on, a port on the switch negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer port does not support auto-negotiation or turns off this feature, the switch determines the connection speed by detecting the signal on the cable and using half duplex mode. When the switch's auto-negotiation is turned off, a port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer port are the same in order to connect.
	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 Outout				

# **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.

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

Auto Logout : Simin		Date			00.00.00	G
Dashboard	O Switch LAM + Marri	e = Darm				
Status -	Manur					
Switch Left	harron					
General Setup	Ses	sion ID:	1			
Port Setting	Mor	itor Session State:	Disable			
Munt	Deat	lination Port:	GE1			
Link Aggregation						
VLAN Management	Allo	w Operation as Normal Port:	Disable	-		
EEE:	Snif	f Pons(RX):	forma autochol			
Multicast	Solf	( Ports(TX):	Notriceg annotated			
Jumbo Frame			Augur			
STP			Charles Car			
MAC Address Table	Session ID	Destination Port	Allow ingress	Sniff Ports(RX)	Sniff Ports(TX)	
Blocked Port Recover		N/A	N/A	N/A	N/A	
Security -	2	N/A	N/A	104	N/A	
ACL ~	3	N/A.	N/A	16A	N/A	
QoS -		N/A	N/A	tUA.	N/A	

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 Logous : 5 min 🖉				Ð
Dashboard	O Las Aggregation = LAS Betting > LAG Setting			
Status -	LAG Setting			
Swith Left	and the second se			
General Setup	Load Balance Algorithm:	IP/Mac Address	-	
Fort Setting	Apply	Mac Address		
Minor		FVMuz Address		
Link Aggregation				
LAG Settom				
LAG-Misnagement				
LACP Setting				
LACP Port Setting				
VLAN Management				
EEE				
Multicast				
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. IP/Mac Address - 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.

Dashboard	O Link Anore	sation > LAG Management = LA	5 Management				
Status	-						
Serich LAVI	LAG Manager	sent -					
General Setup	LAG	Description	Port Type	Link Status	Active Member	Standby Member	Modify
Port Setting	LAG1		-	Not Present			0
Mierte	LAG2		-	Not Present			0
Link Aggregation	LAGE		-	Not Present			0
LAG Setting	LAG4		-	Not Present			0
	LAGS		-	Not Present			0
LAG Port Setting	LAGE		-	Not Present			0
	LAG7		-	Not Present			0
LACP Port Setting	LAGE			Not Present			0
VEAN Management							
CCE							
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.					
	<ul> <li>Name- Enter a string as LAG name.</li> <li>Type - Use the drop down menu to specify the type for LAG.</li> <li>Static- The static aggregated port sends packets over active member without detecting or negotiating with remote aggregated port.</li> <li>LACP- The LACP aggregated ports place member into active only after negotiated with remote aggregated port for best reliability.</li> </ul>					

# 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.

luta Logout : 3 min	<b>2</b>							05/20(14	C)
lashboard	🕑 Link Aggrégistión 🕫 LAG	Pod Selling > LAG Pod S	etting						
lates	LAG Part Setting								
instals (249)	UNG Port Softing								
Jeneral Setup	LAG:			me0					
Port Setting	Enable:		Enable						
Mirror	Sec. 4		Auto						
Jnk Aggregation		Speed:						7.1	
	Flow Cont	xel:	Disable					• 1	
LAG Management				( A66					
	LAG Description	Port Type	Enable State	Link Status	Speed	Duplex	Flow Control	Flow Control	Modify
LACP Part Setting	LAGY	-	Enabled	Down	Auto(All)	Auto	Enabled	Disabled	0
/LAN Management	LAG2		Enabled	Down	Auto(All)	Auto	Enabled	Disabled	0
EEE	LAGE	-	Enabled	Down	Auto(All)	Auto	Enabled	Disabled	0
Aulticast	LA54	-	Enabled	Down	Auto(All)	Auto	Enabled	Disabled	00
umbo Frame	LAGS	140	Enabled	Down	Auto(All)	Auto	Enabled	Disabled	0
STP	LAGE	-	Enaberd	Down	ALED[AE]	Auto	Enabled	Osabled	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	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.
	• <b>100M:</b> Force speed with 100M ability.
	• <b>1000M:</b> Force speed with 1000M ability.
	<ul> <li>Selecting Auto (auto-negotiation) allows one port to negotiat 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 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.</li> <li>For SFP fiber module, you might need to manually configure the speed to match fiber module speed.</li> </ul>
Flow Control	A concentration of traffic on a port decreases port bandwidtl 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 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.

Auto Logout : 3 min 😁				minia 🕞
Dashboard	Curk Aggregation + LACP Setting + LACP Setting	0		
Status	LACP Setting			
Switch LAN				
General Setup	LACP:	Enable Olisable     Disable		
Port Setting	System Priority:	32768	5	(1-65535)
Mirror				
Link Aggregation	(Abbit)			
LAG Prin Setting				
	11 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1			
LACP Poin 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.
Apply	Apply the settings to the switch.

# II-4-5 LACP Port Setting

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

Auto Logout : 3 min	e Ubr					06-22-23 🕑
Dashboard	C Link Aggiégithten > LACP Plan Ex	tting > LACP Part Setting	R			
Status	* Berneral					
Smitch LAN	LACP Port Setting					
General Setup	Ports:		National solected			
Port Setting	Priority:		Ŧ		2	(1-65535)
Mimar	Timeout		Long			
Link Aggregation	Imeout		Long	-		
				Apply		
LAS Management						
LAG Port Setting	Port	Priority		Timeout	1 Modity	
LACP Selling	GB1	1		Long	0	
LACP Port Enloy	GE2	а.		Long	0	
VLAN Management	GES	1		Long	0	
EEE	064	1		Long	0	
Multicast	GES	3		Long	0	
Jumbo Frame	GE6	3		Long	0	
SIP	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.				
	Edit Port GE1				
	Priority				
	1				
	Timeout				
Long					
	OK Cancel				

# **II-5 VLA 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

Anto Logout : 🗦 min 🔗	Unin				(6412) D
Dashboard	O VILAN Management + Canada Vian	> Create VLAM			
Status -	(Transmission)				
Switch LAFI	Create VLAN				
General Setup	Action:	e	Add 🗇 Defete		
Port Setting	VLAN ID:		1000000000		
Mirror	VLAN Name:				
Link Aggregation	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		(Arthy)		
VLAN Management			Theory .		
	122				
Interface Settings	VLAN ID	11 VLAN Name	VLAN Type	Modify	
Voice VLAN	1	refaut	Defaut	0	
MAČ VLAN					
Protocel VLAN					
Summance VLMI					
GVRP					
EEE					
Multicast					

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

ltem	Descript	ion					
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	11 VLAN Name	VLAN Type	Modity			
	τ	petauit	Deraut	0			
	2	markeling0002	State	00			
	3	marketing0003	Stabic	00			
Apply	Apply the settings to the switch.						
Modify	🧷 - Mo	Modify the name of the selected VLAN ID.					

Apply
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.
Oelete the selected VALN ID.

# II-5-2 Interface Settings

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

Auto Logout : 3 min 🦉									2074		C#
Dashboard	O VLA	O VLAN Managamant → Interlativ Settings → Interlativ Settings									
Status	-	Settings									
augus Late	Interface	caranin'n									
General Setup		Port Select:			toth-g-plori-d				- 1		
Port Setting		Interface VLA	Mode:		Hybrid () Access ()	Trunk () Tunnel					
Murta		PVID:			1				= 1	4094)	
Link Aggregation											
VLAN Management		Accepted Type			All □ Tag Only □	Unitag Only					
Craute Vian		Ingress Filterin	2		Enable O Disable						
Interlace Seiberg.		Tagged VLAN:			Nillion estected						
Voice VLAIV		Untagged VLA	N:		1 Mattering a standard				1-1		
		Forbidden VL/	MN:		Talling policited						
Protocol VLAN						( supply					
Summinice VLAN											
				-						-	
EEE-	Port		PVID	Tagged VLAN	Untagged VLAN	Porbidaen VL					Modify
Multicast	GEI	Trunk	1	-	1	- (144)	ALL	Enabled	Disabled	0x8100	0
	GE2	Trunk	1	ine.	1	÷	ALL	Enabled	Disabled	0x8100	0

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 woul 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.				
	Interface VLAN Mode: <ul> <li>Hybrid Access Trunk Tunnel</li> </ul> <li>PVID <ol> <li>Accepted Type</li> <li>All Tag Only Untag Only</li> </ol> </li> <li>Ingress Filtering <ul> <li>Enable Disable</li> </ul> </li>				
	Tagged VLAN				
	Nothing selected - Untagged VLAN Nothing selected -				
	Forbidden VLAN				
	Nothing selected -				
	Uplink TPID:				
	OK Cancel				

### 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 Logout : 📑 min 💌	theory			15.4622 🕞
Dashbeard	VLNI Management > Voide VLAN > Properties			
Status -	Properties Felephany OUI Setting Pod Setting			
Search LAN				
General Setup	Voice VLAN State:	🖸 Enable 💿 Disable		Carlos and
Port Setting	Voice VLAN Id:			Enable
Mirror	Remark CoS/802.1p:	🔿 Enable 💿 Disable		
Link Aggregation	Remark Value:	3		
VLAN Management	Aging Time:	1440	2	(30 65536 min)
Create Vian				
Interface Sottings	ADDIV			
Store weak				
MAC YEAN				
Protocoli VLAN				
Summance VLAN				
GVRP				
EEE				
Multicast				

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 Legout : 3 mm	- User			06/45/16
Dashboard	O VLAN Management & Voice VLAN = Talapho	ny OULSetting		
Status	Properties Talephony CUI Satting Port	Dation		
	Propentes Telephony Coll Sectory Pron	Setting		
General Setup	OUI Address:	101.00700		
Port Setting	Description:			
Meror				
Link Aggregation		_		
VLAN Management	OUI Address	Description	Edit	
	00:60.88	SCOM	00	
Interface Settings	00 03 65	Cisco	00	
MAC-VEAN	00-E0.75	Vientei	00	
Protocol VLAN	00:00:16	Pingtet	00	
Surveillance VLAN	00:01:E3	Siemens		
	the second s		00	
EEE	00:60.89	NEC/Philips	00	
Multicant	00:0F:E2	H3C	00	
	D0:09 6E	Avaya	Ø 📵	

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>• Modify OUI setting for voice VLAN.</li> <li>• Wodify OUI setting for voice VLAN.</li> <li>• Edit OUI 00:E0:BB</li> <li>• OUI:</li> <li></li></ul>				

# II-5-3-3 Port Setting

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

Auto Logout : 3 min	Yuar Quar			06:47/24	D)
Dashboard	O VLAN Managament - Vinca VLAN	a Port Setting			
Status	·				
Sector ( 1994	Properties Telephony OUI Setting	Port Setting			
General Setup	Port	Hater g 3032	186		
Part Setting	State:	C Enable @	Disable		
Maror	Cos Mode:	() All () Sirc			
Link Aggregation	Corner.	Ginn Quin	Appily		
VLAN Management			and a second sec		
Create Vian	Port	State	Cos Mode	Edit	
Interface Security	GE1	Disabled	src	0	
	GE2	Disabled	SIC	0	
	GED	Disabled	HTC .	0	
Protectl VLAN	GE4	Disabled	Brc	0	
Servellance VLAN	GES	Deabled	arc-	0	
OVRP	GE6		arc		
EEE		Disabled		0	
Multicast	G67	Disabled	SEC	0	
	GEB	Disabled	555	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.
	<b>Src (Source)</b> - Once this port is identified as Voice VLAN by frame with matched OUI, remark CoS/802.1p shall tag for only the matched ingress frame with pre-configured OUI.
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.
	VOUI Setting Port Setting
	Edit port GE1
	State:
	Enabled
	Cos Mode:
	Src
	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 Logout : 3 min 🖉					uc 50/28 🕞
Dashboard	VLAN Miningement > MAC VLAN > MAC 6	iouti			
Slatus -	MAC Group Binding				
Sect Left	MARY Brough				
General Setup	Group ID:			4	(1 - 2147483647)
Fort Setting	MAC Address:	0.0 (01 (01 (02 (02 (02 (02			
Mince	Mask:				(9 - 48)
Link Aggregation	and an		-	2	for each
VUAN Management			(Add)		
Create Vian	South Street Str	and the second second		Edit	
hiterace Setting:	C 1 4 (2)	MAC Address	Mask		
Valce VLAN	20	00.00.07.69.24.53	a	S 🙆	
GVBP					
EEE					
Multicast					

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. Edit Group 20: 00:00:07:69:2A:33/9 MAC Address 00:00:07:69:2A:33 Mask 3 (9-48) OK Cancel		
	OK Cancel		

#### 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 : 3 min	2)					ue 60:50
Dashboard	VLAN Managament = MAC VLA	A Croup Brydwy				
Status	·					
Switch 1744	MAC Greup Briding					
General Setup	Ports:		Wathing gloster			
Port Setting	Group ID:		20			
Maror	VLAN:					(1 -4094)
Unik Aggrugistion	VLAN:		-		2	(1-4004)
VLAN Management			Add			
Sreate Mim						
inderface Securing	Port	Group ID		VLAN	Edit	
Valcé VEAN	(ce)	20		1	00	
	GE2	200		X	00	
Protocol VLAN						
Surveillance VLAN						
OVRP						
EEE						
Multicast						

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.  Edit Group 20: GE2 VLAN 1 (1 - 4094) OK Cancel		

### 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 Logaut : 3 min	User					17:01:01 🕞
Dashboard	O VLAN Management = Protocol VLAN	~ Phptocal Group				
Status	Protacol Group Binding					
	Printing Childy Children					
General Setup	Group ID:					(1 - 0)
Port Setting	Framo Type:	Ethomet_I			14.1	
Mirroi	Protocol Value:	01				(0x600 -0xFFFE)
Link Aggregation	Toucor value.	0.	-			(0,000 - 0,0111 - 0)
VLAN Management			EEA .			
Craule Vien	1000	and the second second				
Marlace Beilings	Group ID	Frame Type	11	Protocol Value	Edit	
	3	Ethemet_8		0x0600	00	
MACVEAN						
Suverlance VLAN						
EEE						
Multicant						

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 -		
	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.		
Edit	Modify setting for selected group.		

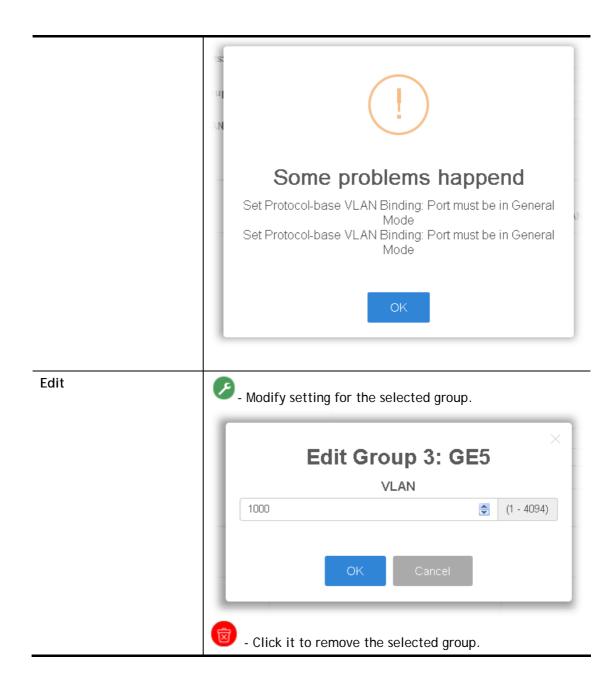
am oto		Group 1 ame Type	
	Pro	tocol Value	
	(0x600 - 0xFFFE) 0x	0601	<b>/</b> a
	OK - Click it to remove the	Cancel	

#### 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 : 👌 min 🖉	Ad					10:00:41
Dashboard	O VLAN Management + Protocol	VLAN = Group Brinding				
Status -	Protocol Group Group Bindin					
Swith Link 4	Protocol Group Group Bindin					
General Setup	Parts:		Tailing words.d			
Port Setting	Group ID:		1			
Mirror	VLAN:					(1 -4094)
Link Aggregation	VLAN:				g	(1 -4094)
VUAN Management			,Aidd	1		
Greate Vien						
Interface Settings	Port	Group ID	11	VLAN	Edit .	
Voice VLAN	GES	3		1000	Ø 🔞	
MAC VILAN	GEB	3		1000	00	
Sune Hance VLAN						
EEE						
Multicast						

Item	Description			
Ports	Use the drop-down list to select one or more ports for applying protocol-based VLAN. Note that protocol-based VLAN can only be applied to the ports of which Interface VLAN Mode (at VLAN Management >> Interface Settings) is set to "Hybrid".			
Group ID	Select the protocol group defined in Protocol Group setup.			
VLAN	Use drop down list to choose a value as VLAN number.			
Add	Add the above settings to the switch. Before using Add, open Switch LAN>>VLAN Management>>Interface Settings to specify Hybrid as Interface VLAN Mode for the GE ports first. Otherwise, the following error message will appear.			



## 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.

Auto Logoot : Of	•				mum 🕒
Dashboard	O VLAN Managemen	ot = Suovillance VLAN > Property			
Status	-				
Samete LAN	Property Surveil	lance QUI			
General Setup	Sta	te:	🔿 Enable 💿 Disable		
Port Setting	VL	NN ID:	Mitting analasid		
Mirror	CoS	5/002.1p Remarking:	6		- Enable
Link Aggregation					
VLAN Management	Agi	ng Time:	1440		2 (30.65536 sec)
			Activ		
Interface Settings					
	Port	State	Mode	QoS Policy	Edit
	GE1	Disabled	Auto	Video Packet	0
	GE2	Disabled	Auto	Video Packet	0
	GES	Disabled	Auto	Video Packet	0
GVRP	GE4	Disabled	Auto	Video Packet	0
EEE	GE5	Disabled	Auto	Video Packet	0
Muticast	GE6	Disabled.	Auto	Vitteo Packet	0
	0.63	Disease.	14142	Lizza Parilia	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	P - Click it to modify port setting status.

> surveillance vLAN > Property ()
×
Edit port GE1
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> </ul>
<ul> <li>Manual: User need add interface to VLAN ID tagged member manually.</li> </ul>
QoS Policy - Select port QoS Policy mode.
• Video Packet: QoS attributes are applied to packets with OUI in the source MAC address.
<ul> <li>All: QoS attributes are applied to packets that are classified to the Surveillance VLAN.</li> </ul>
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 Logout : Of	~	Unit			(0) (2;56 🕞
Dashboard	0	VLAN Managament + Somethings VLAN +	Serverlance (30)		
Status	-	perty Surveillance OUT			
		peny currentarce our			
General Setup		OUI Address:	10100-001		
Port Setting		Description:			
Martir			Add		
Unk Aggregation					
VLAN Management	OUI	Address	Description	IT Edit	
			No data available		
Protect VLAN					
GYRP					
EEE					
Multicast					

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.

Auto Logoui : OF	~						G
Dashboard	O VEAR Managem	ont & GVRP @ Property					
Status	-	bership					
protects (2009)	Property Mem	bership					
General Setup	St	ate:	O Enable @	Disable			
Port Setting	n	meout	Join	20 ms			
Mirror			Leave	60 ms			
Link Aggregation			Leave All	1000 ms			
VLAN Management				(Approx			
Greate Vian							
Interface Settings	Port	State		VLAN Creation	Registration	Edit	
	OE1	Disabled		Enabled	Normal	0	
MAD YLAN	GE2	Disabled		Enabled	Normal	0	
Protocol VLAN	GES	Disabled		Enabled	Normal	0	
Schellance YLAN	GE4	Desabled		Enabled	Normal	0	
OVER	GES	Disabled		Enabled	Normal	0	
EEE	GEG	Disabled		Enabled	Normal	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.			
Timeout	Display the current time status for GVRP.			
Apply	Apply the settings to the switch.			
Edit	Click it to modify settings for the selected port.			
	Edit port GE1			
	State:			
	Disabled -			
	VLAN Creation:			
	Enabled			
	Mode:			
	Normal			
	OK Cancel			
	State - Select Enabled or Disabled for such port.			
	VLAN Creation -Select Enabled or Disabled.			

Mode - There are three modes to be specified.
<ul> <li>Normal - Default setting. All packets can pass through the selected GE port.</li> </ul>
<ul> <li>Fixed - The selected GE port only sends static VLAN information to neighboring device and allows static VLAN packet to pass through.</li> </ul>
<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 : 🔐 🔮		Unar			09.16.20 🕞
Danhboard	O VIAN Management -> GVRP	> Momberature			
Status ·	Property Membership				
semh Levi -	-roberty memocically				
General Setup	VLAN	Member	Dynamic Member	Type	11.U
Port Setting			No data available in table		
Mirror					
Link Aggregation					
VLAN Management					
	20.00				
Interface Sattings					
MAC VLAN					
Protocol VLAN					
EEE					
Muticant					

# II-6 EEE

Auto Logout : Off	~					09.17.25	€.
Dashboard	O Switch	LAN > BEE > Energy Efficient B	barnet Setup	5			
Status		and the second second second					
Switch LAN	Energy E	flicient Ethernet Setup					-
General Setup		Port		Notiveg zelezież			
Port Setting		Enable:		🔿 Enable 💿 Disable			
Mirror				Appl			
Link Aggregation							
VLAN Management	Port	10	Enable	11	Status	Modify	
BBE	GET		Disabled		Disabled	0	
Multicast	GE2		Disabled		Disabled	0	
Jumbo Frame	GE3		Disabled		Disabled	0	
STP	GE4		Disabled		Disabled	0	
MAC Address Table	GE5		Disabled		Disabled	0	
Blocked Port Recover	GE6		Disabled		Disabled	0	
Security	GE7		Disabled		Disabled	0	
AGL	GE8		Disabled		Disabled	0	
QoS	- GEN		Disabled		Disabled	0	

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

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.				
АррІу	Apply the settings to the switch.				
Modify	Click it to modify port setting status.  Edit Port GE1				
	Enable				
	Disable -				
	Enable				
	Disable OK Cancel				
	Disabled Disabled				

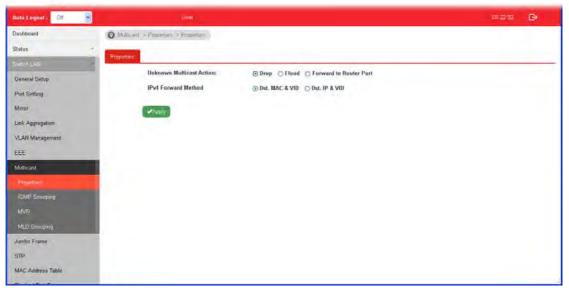
# **II-7 Multicast**

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

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

## **II-7-1** Properties

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

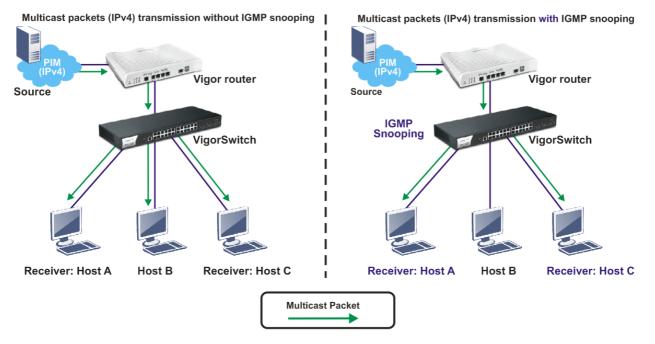


Available settings are explained as follows:

Item	Description
Unknown Multicast Action	Select an action for switch to handle with unknown multicast packet.
	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.
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 Materiad	I ISMP Smith	ng = 63MP Solling						
Status -	IBMP Sitting	IGMP Qu	enin Sotling IGME	Static Group IGM	P Group Table IGM	P Router Table Forv	ard All Throttling	Filturing Profile	
Switch LAN	Filtenng Bindir	ng l							
General Setup			_		Global Setting			_	
Port Setting	_								
Mirror	1.0	IGMP Snoop	ning State:	💿 En	able 🔿 Disable				
Link Aggregation		IGMP Snoot	alog Version:	(E) V2	© v3 (8155)				
VLAN Management		IGMP Snoop	ning Report Suppressi	ion: () En	able O Disable				
EEE					Apply				
Mülticast					VLAN Setting				
Properties									
	Entry No.	VLAN ID	IGMP Snoopi	Router Ports	Query Robus	Query Interv	Query Max R	Last Member	La
MVR			Disabled	Enabled	2	125	10	2	1
MLD Shooping									
Jumbo Frame									
STP									
MAC Address Table									
Blocked Part Recover									

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

t the ICMP speeping version					
Set the IGMP snooping version.					
2 - Only support process IGMP					
3 (BISS) - Support v3 basic and	v2.				
Click <b>Enable</b> to allow the switch to handle IGMP reports between router and host, suppressing bandwidth used by IGMP.					
oply the settings to the switch					
Click it to modify IGMP set owever, if IGMP Snooping Stat otion will be disabled.					
Edit VLA	AN ID 1				
IGMP Snoo	ping State				
Disable	•				
Router Ports	Auto Learn				
Enable	•				
Query Robustness	s (Operational: 2)				
2	(1-7, default 2)				
Querv Interval (O	perational: 125)				
125	Sec (30-18000, default 125)				
Query Response Inter	val (Operational: 10)				
10	Sec (5-20, default 10)				
Last Member Quenc Co	unter (Operational: 2)				
	Sec (1-7, default 2)				
	erval (Operational: 1)				
	Sec (1-25, default 1)				
	e Leave:				
Enable	•				
	etween router and host, suppro MP. oply the settings to the switch Click it to modify IGMP set owever, if IGMP Snooping Stat otion will be disabled. Edit VL/ IGMP Snoo Disable Router Ports Enable Query Robustness 2 Query Interval (O 125				

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.
<b>Immediate Leave -</b> 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 Louisut : 10f. 🖄		Admin			11/22/41	Ð
Deshboard	IGMP Setting	IGMP Quesier Setting	tatic Group IGMP Group Table IGMP Route	rTable Forward All Throthing Filt	ering Profile Filtering Dinding	
Status -	and the second second		States and a second second	Station in the second second second		
and Letter and		VLANID:	#184mig celected		1	
General Setap		Querier State:	Otriabile Orisable			
Port Setting		Querier Version:	⊙v2 ⊜v3 (BISS)			
Mirror				Apple		
Link Appregiation	T					
VLAN Management	VLAN ID	Querier State	Querier Status	Querier Version	Ouerier IP	
EEE	1	Disabled	Disabled	-	-	
Muticast	4067	Disabled	Disabled	-	14 C	
Proparties	4058	Disabled	Disabled			
	4069	Disabled	Disabled	(-)	-	
MVR	4070	Dissbied	Disabled	~		
MLE) Shooping	4071	Disabled	Drsabled	-	( and	
Jumbo Frame	4073	Disabled	Disabled		8	
STP	#073	Disabled	Disabled			
MAC Address Table	4074	Disabled	Disabled	-	-	
Recurity -	4075	Disabled	Disabled	-		
4CL -	4078	Disabled	Disabjed	-		
	4077	Disstred	Disabled	~	246	
Q6S -	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	Walmin 09:08:36 🕞	
Dashboard	O Multicart is IGMP Stooping in IGMP Stoop	
Status	IGMP Setting IGMP Querrer Setting IGMP State Group IGMP Group Table IGMP Roder Table Forward All Threating Frittening Profile Filtering Binding	
Switch LAN	Journ particity Town Section S	-
General Setup	VLAN ID: Faithing smeched -	
Port Setting	Group IP Address:	
Mirror	Member Ports: Diffing universed	
Link Aggregation		
VLAN Management	(Appy)	
EEE	ing a later second and a second	
Mutrcast	VLAN ID Group IP Address. Member Ports Modify	
Properties	No data available in table	
IGMR Stangard		
MV7/		
MLD Streeping		
Jumbo Frame		
SIP		
MAC Address Table		
Blocked Pod Recover		1

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.
АррІу	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.

Auto Logout: 01							29:30 CH
Dashboard	O Mubicant >	IGMP Shooping + IGMP Group Table					
Status.	·		Concernment of the	Table of the sector	STREET, STREET	none in the second second	Construction of the local division of the
Swarn Little	IGMP Setting	IGMP Quenur Setting IGMP Static Group	IGMP Group Table	IGMP Router Table	Forward All	Throttling Filtering Profile	Filtering Binding
General Setup	VLAN ID	Group IP Address	Member Ports	100	Type	Life(sec.)	
Port Setting			No data av	allable in table			
Mirror							
Link Aggregation							
VEAN Management							
EEE							
Multicast							
Properties							
MVR							
MLD Snooping							
Jumbo Frame							
SIP							
MAC Address Table							
Plocked Port Recover							

Item	Description
VLAN ID	Display the VLAN of this multicast group belongs to.
Group IP Address	Display the multicast address of this multicast group.
Member Ports	Display the port(s) where subscribing member of this multicast group belongs to.
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.

Anto Logout : 🛛 🕜 💮		Admin					09 30-28 🕞
Dashboard	O Material > ISA	MP Sevening = IGMP Rout	ar Table			-	
Status -							-
Inter Laty -	IGMP Setting	IGMP Querier Setting	IGMP Static Group IGMP Group	Table IGMP Router Table	Forward All	Throttling Filtening Profile	Filtering Binding
General Setup	VL	AN ID:	Thisting selected				
Port Sulting	Tvi	·e:	⊚ Static ⊙ Ferbidder				
Mirror		mber Ports:	Nulling Johnston				
Link Aggregation				Add			
VLAN Management				(Heat)			
EEE	VLAN ID	Port	Static Port	Forbidden P		iry Time(sec.)	Edit
Multicast	VLANID	Port		rorbidden Pr	ort Exp	iry Time(sec.)	ear
Properties			14	olara available in cibio			
MVR							
MLD Shooping							
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 : 🛛 🐨 🚿		Bonts						05:48:33 🕞
Dashboard Status	(GMP Setting	IONP Querier Selling	IOMP Static Group	IOMP Group Table	IOMP Router Table	Forward All Throthing	Filtering Profile Filter	ing Binding
INNEED LANN		Available VLAN:		Parceng (which				
General Setup		Static Ports:		mattering whether			7	
Port Setting		Forbidden Ports:		turning patiented			-	
Mitror					Add			
VLAN Management	VLAN	Ú.	Static Port		Forbidde	m Port		Ear
EEE	1		061-065		GE11-GE	10		00
Multicest	4067		0E1-965		GE11-GE	15		00
Propeties	4060		061-055		0611-06	15		00
	4069		061-065		GE11-GE	5		00
	4070		0Ê1-0E5		GE11-GE	15		00
MLD Shooping Jumbo Frame	4071		0E1-0E5		OE11-OE	15		00
Jumbo Frame	4072		081-085		QE11-GE	15		00
MAC Address Table	4073		061-065		OEITOE	15		00
Blocked Port Recover	4074		0E1-0E5		GE11-GE	6		00
lecunty	4075		QE1 QE5		OE11 OE	15		00
ICL .	4076		GEI-GE5		GE11-GE	15		00

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.

Auto Logout : 🛛 🦉		Bans						05:53:01. 🕞	
Dashboard	IGMP Butting	IGMP Quener Setting	IGMP Static Group	IGNP Group Table	IGMP Router Table	Forward All Throla	Fillering Profile	Fillering Binding	
Status -	and the second division of the				1		and a second second second second		
Switch (LAN)		Ports:		eletrong satisfies					
Seneral Setup		Max Group:		256				(0 25	56)
Point Setting		Exceed Action:		Deny OReplace					
Mirror					Apply				
Link Aggregation									
VLAN Management	Port		Group		Exceed Ac	tion		U Ed	
EEE	0E1	GE1 258			Deny			6	
Multicaist	082	0E2 256			Denv			0	2
Properties	0E3	0E3 250			Deny			6	1
	OE4	256			Deny			0	2
MVR.	065	256			Deay			6	
MLD Shooping	DEE	256			Deny			0	
Jumbo Frame	0E7	256			Deny			0	2
STP	GES	256			Deny			6	1
MAC Address Table	GE9	256			Denv			6	
Blocked Port Recover	OE10	256			Deny			0	
Becurity -	GETT	250			Dieth			0	A
216.217/0200844-6457	0F17	250			Dietry			6	)

Description						
Use the drop down list to specify LAN Port (GE/LAG).						
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).						
VigorSwitch will perform the action defined below when the number of IGMP join report for the specified interface exceeds value defined in Max Group.						
<b>Deny</b> - It is default setting. The IGMP join report (for multicast service) received by such interface will be discarded.						
<b>Replace -</b> When it is selected, a new group with IGMP report received will replace the existing group.						
Apply the settings to the switch.						
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.st 🕞
Dashboard	O Multicart is IGMP 5	innoping S Filtrang Profile			
Status	·				
Shanch Calif	IGMP Setting IGN	P Queener Setting IGMP Static	Group IGMP Group Table IGMP F	Router Table Forward All Th	Watting Filtening Profile Filtening Binding
General Setup	Profile	ID;	Fritar Profile (D		g (1 · 120)
Port Setting	Start A	tdress:	224.9.0.1		
Mircor	End Ad				
Link Aggregation	End Ad	dress:	228.0.0.2		
VLAN Management	Action:		Allow O Deny		
PEE			Add		
Multipast					
Properties	Profile ID	Start Address	End Address	Action	Edit
	1	224.0.0 1	224.0.0.2	Aliqw	S ()
MVR	2	224.0.0.10	224 0 0 20	Allow	00
MLD Snooping					
Jumbo Frame					
SIP					
MAC Address Table					

Available settings are explained as follows:
----------------------------------------------

Item	Description
Profile ID	Use the drop down list to select one filtering profile (1~128) for IGMP snooping.
Start Address	Enter an IP address as the starting point for the IP range.
End Address	Enter an IP address as the ending point for the IP range.
Action	<ul> <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).

	Edit 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 : 🖓 🕮	6. ····	Hoot						00.0235	B
Dashboard Status -	(GMP Setting )G	MP Querier Setting	IGMP Static Group	IGMP Group Table	IGMP Router Table	Forward All Throttle	ng Filtering Profile	Filtering Binding	
Galler ( Arts	Por	IS:		Long services					
General Setup	Pro	file ID:		Longs ( Longs				Enable	
PortSelling Mirror					(Apply)				
Link Aggregation	Port		11.14	trofile ID			11 (1	dit	
VLAN Management	GE1			-				9	
EEE	OE2			-				0	
Multicast	OE3							0	
Properties	OE4		-	-				D	
	065			-				D	
MVR	0E6		-	-					
MLD Snacping	087							0	
Jumbo Frame	OE8			-				0	
8TP	GE9			-				D	
MAC Address Table	GEID							0	
Blocked Port Recover.	GE11							Ø	
Security -	GE12		2	-				Ð	
72 16 2 171 2280/Pail-64169	0E13			-				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:
Ena	ble -
	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 desination 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		23.42.48 D
Dashboard Status - Dwitte Left	Muticiaal > MVR > Property Port Setting Group Address		
Géneral Setup	N.	Property Settings	
Port Setting Mitror Unk Aggregation VLAN Management EEE	State: VLAN ID: Mode: Group Start:	© Enabled _> Disabled defacil(1) © Competible (> Dynamic D0.000	
Multicast	Group Count:	1	(1-128)
Properties IGNP Snuoping MVR	Query Time:	1 (Angle)	(1-10 sec)
MLD Streeping		Operational Group	
uumbo Frame STP MAC Address Table	Maximum Current	126 a	

Item	Description
State	Enabled - Click it to enable the MVR function.
	<b>Disabled</b> - Click it to disable the MVR function.
VLAN ID	Choose one VLAN profile from the drop down list as multicast source VLAN which will receive multicast data. All source ports must belong to this VLAN. The default is VLAN 1.
	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.
	Comaptible - 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 operation.

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

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

Auto Logout : Off. 🔤	lest -			09.29.04 🕞
Dashboard	Multicast > MVR	> Pod Setting		
Status	Property Port Se	Group Address		
	Property Port Se	Group Address		
General Setup	Ports:		Plathing methodox	17
Port Setting	Role:		Nane      Receiver      Source	
Mirror		fiate Leave:	O Enable O Disable	
Link Aggnegition			Apply	
VLAN Management				
EEE	Port	Role	immediate Leave	Edit
Multicast	GE1	None	Disabled.	0
Properties	GE2	None	Disabled	0
IGMP Snonping	GES	None	Disabled	0
	GE4	None	Disabled	0
MLD Shonping	GE6	None	Disabled	0
Jambo Frame	GE6	None	Disabled	0
STP	GE7	None	Disabled	0
MAC Address Table	GES	None	Disabled	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	<ul> <li>None - Noting will be happed to the selected LAN port in MVR operation.</li> <li>Receiver - The selected port will be treated as destination port which will receive multicast data from the multicast server.</li> <li>Source - The selected port will be treated as source port which will send multicast data to the receiver port.</li> </ul>
Immediate Leave	Enabled - 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).
	Edit port GE1
	None -
	Disable -
	OK Cancel

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

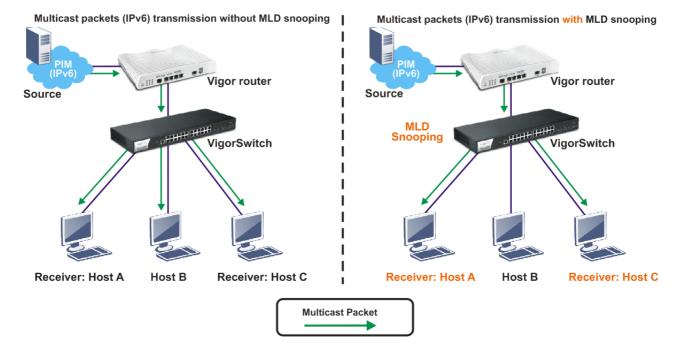
This page allows the network administrator to configure IP address and specify port member for VLAN selected in MVR>>Property page.

Auto Logout : Off.				08 90 07 🕞
Dashboard	Mullicard > MVR > Group Address			
Status	Property Fort Setting Group Address			
Sance Lift	Holouny Hou Second Report Manager			
General Setup	VLAN ID:			
Port Setting	Group Address:			(0.0.0.0 - 0.0.0.0)
Mittor	Member:	sentence - succing		
Link Aggragatian		Add		
VLAN Management				
EEE	VLAN Group Address	Member Type	Life (Sec.)	Edit
Multicast	and star and star	No data available in table	cire (dear)	Lan.
Propertien		The sets at the set of the set		
IGMP Snooping				
MLD Shuaping				
Jumbo Frame				
STP				
MAC Address Table				

ltem	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.

Auto Logout C Od 🔤		User						09.3	142 🕞
Dashboard	O Multicard	⇒M∐(Snacpmj = ML	D Setting						
Status	MLD Setting	-	MLD Group Ta	ble MLD Route	Second Res	orward Ali Throttling	( marine and )	Photo	
Switch Linki	MLD Siding	MLD Static Group	MLD Group Ia	ple MLLO Houth	r table P	orward Ali Throttling	Filtering Profile	Filtering Binding	
Deneral Setup					Property	Settings			1
Port Setting		State:		O Enable (0)	-				
Mirror				- C					
Link Aggregation		Version:		⊙ MLDv1 ○ M					
VLAN Management		Report Suppression:		⊙Enable ⊚I					
EEE					Ap	iply 1			
Multicast					VLAN	Søtting			
Propertons									
IGMP Snooping	VLAN ID	MLD Snooping Operational	Router Port Auto Learn	Ouery Robustness	Ouery	Ouery Max Response Int	Last Member Query Counter	Last Member Ouery Interval	Immediate Le
	1	Disabled	Enabled	2	125	10	2	1	Disabled
	*							_	-
Jumbo Frame									
STP									

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 packets 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 packe controlled by MLDv1 and <i>forward</i> the traffic to destination defined with multicast address(es).			
Report Suppression	Enabled - Click it to allow the switch to handle MLD reports between router and host, suppressing bandwidth used by MLD. Disabled - Click it to disable the function.			
АррІу	Click it to display the result based on the settings configure above.			
Edit	Click it to modify the settings for the selected VLAN I (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 MLD query.			

Query Robustness - 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.

Anto Logout : 🛛 🖓	User		09:32:52 🕞
Dashboard	O Multicell + MLD Seaturing > MLD Shalic Group		
Status -	MLD Setting MLD Static Group MLD Group	up Table MLD Router Table Forward All Throtting	Filtering Profile Filtering Eindeng
General Setup	VLAN ID:	Mathing palacting	1.0
Port Setting	Group IP Address:		
Million Link Aggrégation	Member Ports:	Watering and octave	
VLAN Management		Apply	
EEE Multicaut	VLAN ID Gro	up IP Address Member Ports	Modify
Properties KGMP Shooping MVR		No data available in table	
Mill Shaping			
Jumbo Frame STP MAC Address Table			

ltem	Description
VLAN ID	Use the drop down list to specify a VLAN profile (created in Switch LAN>>VLAN Management>>Create Vlan) as MLD Static Group.
	However, if <b>State</b> in <b>MLD Setting</b> is not set as <b>Enabled</b> , 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
Member Ports	static group (defined in VLAN ID). 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.

o Logout : Off 🛛 👻		L) park			(13) 33) 45	Gt
ihboard	O Meticart > ML	D Snooping = MLD Group Table				
tus 😔			(Constanting (Constanting)	Concern 1 Concernance	Distance in the local distance in the	
(0) LAN	MLD Setting	MLD Static Group MLD Group Table	MLD Router Table Forward All	Threttling Filtening Profile	Filtering Binding	
neral Setup	VLAN ID	Group IP Address	Member Ports	Туре	Life(sec.)	
Sotting			No data available in tabl			
ar.						
Aggregation						
N Management						
-						
agast						
ирентира.						
MP Seneping						
bo Frame						
C Address Table						

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 Logout = 🖉 🦉		1899.42 🕞
Dashboard	O Muticalit > MLD Scooping > MLD River To	bos
Status -	MLD Setting MLD Static Group MLD	Smup Table MLD Router Table Forward All Throttling Filtering Proble Filtering Binding
Switch LAD	MED Surling MED Statue Group MED 6	kunda mena warra kannak kana kanama wa Lukarnuki Lumasuk kunina kunauki enalani
General Setup	VLAN ID:	Hötting keletiné -
Port Setting	Туре:	⊚ Static ○ Forhidden
Mirror	Member Ports:	Wathing aniesped
Link Aggregation		Put
VLAN Management		-
EEE	VLAN ID Port	Static Port Forbidden Port Expiry Time(sec.) Edit
Multicast	in the second second	No data available in table
Pepperlies		
GMP Shooping		
MVR		
Ma_D Scopping		
Jumbo Frame		
STP		
MAC Address Table		

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	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 it to modify the settings for the selected entry.

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

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

Auto Logoul : 🛛 🖓	User		094121 Ge
Dashboard	Multicard + MLD Shooping + Farward AV	0	
Status	MLD Setting MLD Static Group M	LD Group Table MLD Router Table Perward All Throttling	Filtering Ptotile Filtering Binding
20010-1201	and the second s	House and the second se	Contraction of the second
General Setup	Available VLAN:	Fighting Antiscied	
Port Setting	Static Ports:	Platfing selected	1.4
Mirror	Forbidden Ports:	Ploting selected	
Link Aggregation		Add	
VLAN Management			
EEE Multicast	VLAN	Static Port Forbidden Port	Edit
Properties IGMP Securpting MVR		No data available in table	
Jumbo Frame STP MAC Address Table			

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-7-4-6 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 : 🖓 🔹	User				18.42:11 🕞
Dashboard	Multicaul > MLD Snooping > The	ittivg			
Status	MLD Setting MLD Static Group	MLD Group Table MLD Route	r Table Forward All Thinttling Fil	tenng Profile Filtenng Bind	
	MLD Setting MLD Static Group	MLD Group Table MLD Rouse	er Table Forward All Throttling Fil	tenng Profile Filtenng Bind	ang
General Setup	Ports:	Nationy polocia	1		
Port Setting	Max Group:	256			(0 - 256)
Mirtor	Exceed Action:				
Link Aggregation	Exceed Action:	② Deny 〇 Rep			
VLAN Management			Apply		
EEE	Port	Max Group	Exceed Action	Edit	
Multicarit					
Properties.	GEI	256	Deny	0	
IGMP Sneeping	GE2	256	Deny	0	
	GE3	256	Deny	0	
	GE4	256-	Deny	0	
Jumbo Frame	GE5	255	Deny	0	
STP	GEE	256	Deny	0	
MAC Address Table	GE7	256	Deny.	0	
	GEB	256	Dem	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.
Apply	Apply the settings to the switch.
Edit	Click it to modify the settings for the selected entry.

#### II-7-4-7 Filtering Profile

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

The filtering profile page allows to configure up to 128 IP-group (for multicast 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			05.35.30 🕞
Dashboard	Multicest > MLD Snoope	ig = Filtering Profile			
Status -	Environment Environment	Contraction of the	Description of Francisco	In the second second second	The second s
Souton Whi	MLD Setting MLD State	s Group MLD Group Table	MLD Router Table Forward All	Throttling Filtening Profile	Filtering Binding
General Setup	Profile ID:		Port Public ID		= (1 - 128)
Port Setting	Start Addres		PED2-1		
vlirror	End Address				
Link Aggregation	End Address.		FF02:3		
LAN Management	Action:	© #	ullow 🔿 Deny		
BEB-			bnA		
Multicast					
Properties	Profile ID	Start Address	End Address	Action	Edit
IGMP Shocoing	2	m02.1	mp2_2	Allow	00
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	Click it to modify the settings for the selected entry.

анту томп отале отвер томп отвер тавле томп router тавле Х
Edit Profile 1
Start Address:
224.0.0.1
End Address:
224.0.0.2
Action:
Allow
OK Cancel

#### 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.

Auto Logout : Olf	- Dank			09/43/37
Dashboard	Mullicaet. > MLD Swooping + Filtering	Emiling		
Status	MLD Setting MLD Static Group			-
Senten LAN	MLD Setting MLD Static Group	MLD Group Table MLD Router Table Forward All	Throttling Filtering Profile Filtering	g Blinding
General Setup	Ports:	Mathing saletted		4.1
Port Setting	Profile ID:	timeg search		Enable
Mirror				
Link Aggregation		Apply		
VLAN Management	Port	Profile ID	Edit	
EEE		In Prome in		
Multicast	GE1		0	
Properties	GE2	-	0	
IGMP Suparion	GE3	-	0	
MVR	GE4	_	0	
MLD Staeping	GE5	-	0	
Jumbo Frame	GEG	-	0	
STP	GE7		0	
MAC Address Table	GE8	-	0	
	GE9		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.
	<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	
	Sancer	

# II-8 Jumbo Frame

Auto Logout : Off	-	User		09.44.36
Dashboard	0 Sw	ch LAN > Jumbo Frame > Jumbo Frame Satting		
Status	1			
	Juma	Frame Satting		Tanada
General Setup		Jumbo Frame (Bytes): 1526	*	(1526-9216)
Port Setting		Analy		
Mirror		a started		
Link Aggregation				
VLAN Management				
EEE				
Multicast				
oumpolitimme :				
STP				
MAC Address Table				
Blocked Port Recover				
Security				
AČL				
QoS				

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.
Apply	Apply the settings to the switch.

# II-9 STP

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

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

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

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

#### **II-9-1** Properties

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

Auto Logout : 🖂	Admin		00.38 DE 🕞
Dashboard	Switch LAN = STP = Properties		
Status Swatch (LAN)	Properties Port Setting Bridge Setting STP Mode:	Port Advanced Setting Statistics MST Instance MST Port Setting	
General Setup Port Setting Metor	S 1P Mone: BPDU Handling: PathCost Method:	© Disabled © STP © RSTP © MSTP © Flooding © Filtering © Shorr © Long	
Link Aggregation VLAN Management	Arela		
EEE Multicast Jumbo Franké			
err MAC Address Table			
Blocked Port Recover Security			
ACL	3		
QoS			

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.
Apply	Apply the settings to the switch.

## II-9-2 Port Setting

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

Auto Logout : Of	~		-Adm	ie .					09,39,15	G
Dashboard		O Switch LAN 7	STP Pon Smi	ng.						
Status	-	Properties	or Setting	indge Setting	Port Advanced Setting	Statistics M	ST Instance MST P	art Setting		
		Properties	or deting	noge outling	Polit Mehaniced Septite	Citatiotico m	al meaner mai e	on Sering		_
General Setup		Po	orts:		Photonog solu	ctoo!				
Port Setting		Pa	ath Cost (0 - Auto	):	n				×	
Mirror		P.	lority:		128					
Link Aggregation										
VLAN Management			lge Part:		© Yes ⊚ No					
EEE			2P Option:		Auto      Yes	O No				
Multicast			POU Filter:		T Yes					
Jumbo Frame		BF	PDU Guard:		TYes .	-				
SIP	_1					Apply				
MAC Address Table			nrts:		Biothing bold					
Blocked Port Recover		Pa	ins.		moturili som					
Security	2					Migrate				
ACL										
005		Port Adi	min Enable	Path Cost	Priority	Edge Port	P2P Option	BPDU Filter	BPDU Guard	Edit
R-E		GE1 Em	aple	U	128	NQ	Auto	Disable	Disable	8

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)		
	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 : Off	*	Admin		0340.33 🕒	
Dashboard		Switch LAN ~ STP - Endge Setting			
Status		Properties Port Setting Bridge Setting	Port Advanced Setting Statistics MST Instance MST Port	Patrice 1	
	2	Properties Pront Setting Broge Setting	Port Advanced Setting Statistics MIST Instance MIST Port	Seming	
General Setup		Priority:	32769		
Port Setting		Forward Delay:	15	(4.30)	
Minor		Max Age:			
Link Aggregation			33	(6.40)	
VLAN Management		Tx Hold Count:	В.	(1-10)	
EEE		Hello Time:	2	(1-10)	
Multicast			+anty ]		
Jumbo Frame					
		Bridge Identifier	32768/ 0/00 1D/AA 11 22 44		
MAC Address Table		Designated Root Endge	D/ 0/00, 00: 00: 00: 00: 00:		
Blocked Port Recover		Root Path Cost	U		
Secunty		Designated Bridge	0/ 0/00 00 00 00 00	0/ 0/00 00 00 00 00 00	
ACL		Root Port	0/0		
0.65	~	Max Hops	20		
N/E		Distanti di Linea			

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.
АррІу	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 : CE	1			User						114	ag na 🖸 🕞	
Dashboard		O SWID	th LAN STP S	Port Advanced Self	ting .							
Status	-	Desert	es Port Settin	g Bridge Sett	Pert Advanced	Setting Stylestics	MST instance	MST Port Setting				
		Préperts	es Port-Settin	ng bridge oen	ng ron Advanced	owing orwines	INO1 Instancy	mot non cetting				_
General Setup			Indentifier	Path Cost				Edge Port	P2P Option			
Port Setting		Port	(Priority1D)	Cont/Oper	Designated	Root Path Cost	Designated	Conf/Oper	Conf/Oper	Port Role	Port State	Edi
Mirror		GEL	12871	0 / 20000	0 / 00:00:00:00:0	0	0/00:00:00:00:0	NO / NO	Auto / No	Disabed	Disabled	0
Link Aggregation		GE2	128/2	0 / 20000	G / 00:00:00:00 U _	<u>p</u>	0 / 00:00:00:00 0	No / No	Auto / No	Disabed	Disabled	0
VLAN Management		GE3	128/3	0720000	0/00:00:00:00:0	D	0/00/00/00/00/0	No / No	Auto / No	Disabéd	Disabled	0
EEE		GE4	12874	0/20000	0 / 00 00 00 00 0	0	0 / 00 00 00 00 0	No / No	Auto / No	Disabed	Disabled	0
Multicast		GES	128/5	0/20000	0/00:00:00:00:0	0	0/00:00:00:00:0	No / No	Auto / No	Disabed	Disabled	0
Jumbo Frame		GEG	12876	0720060	0 / 00 00:00 00 0	0	0/00/00/00/00	No / No	Auto / No	Disabed	Disabled	0
STF		GE7	128/7	0/20000	G / CO-DO-OD-DU U _	0	0 / 00:00:00 00 0	No / No	Auto / No	Disabed	Disabled	0
MAC Address Table		GE8	128/8	0/20000	0 / 00 00 00 00 0	0	0 / 00,00 00 D0 D.	Na / Na	Auto / No	Disabed	Disabled	0
Blocked Port Recover		GE9	128/9	0/20000	0/00/00/00/00/0	0	0/00/00/00/00/0	No / No	Auto / No	Disabed	Disabled	0
Security	-	GE10	128710	0/20000	0/00.00.00.00.0	Q	0/00/00 00 00/0	ND / NO	Auto / Yes	Disabed	Forwarding	0
ACL	-	GE11	128711	0720000	0 / 00 00:00 00 0	0	0/00/00/00/00	No / No	Auto / No	Disabed	Disabled	0
QoS	-	GE12	128712	0 / 20000	0/00/00/00/00/0	.0.	0/00/00/00/00/0	No./ No	Auto / Yes	Disabed	Forwarding	0

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 Logoot : CE	*					09.60.00 🕒
Dashboard		O Switch LAA STP Stat	er fun n			
Status	-	Constant Property in	Concernent Francisco	Statistics MST In		
S-HON LAN	2	Properties Port Setting	Bridge Setting Port Advenced S	Setting Statistics MST In	stance MST Part Setting	
General Setup		Port	Configure BPDUs Rx.	TCN BPDUs Rx.	Configure BPDUs Tx.	TCN BPDUs Tx.
Port Setting		GE1	0	D.	D	ň
Mirror		GE2	0	ō.	a	D
Link Aggregation		GE3	ø	D	a	D
VLAN Management		GE4	0	D	Q	D
EEE		GE5	0	0	0	0
Multicast		GE6	0	0	0	ġ.
Jumbo Frame		GE7	0	0	0	Q
		GEB	ø	0	a	<u>a</u>
MAC Address Table		GE9	0	o	a	D
Blocked Post Recover		GE10	0	Ø	0	D
Security	-	GE11	0	0	0	á.
ACL		GE12	0	0	.u	D
QoS	-	LAG1	0	0	n .	0

Available settings are explained as follows:

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

## II-9-6 MST Instance

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

Auto Lagout ; 🕬 🔮								553 <b>D</b>
Dashboard	0 :	with LAN > STP > MS	1 Wetance					
Status	-			Conception of the		Tinstance MST Port Se		
Seattle LAN	Prop	erties Port Setting	Bridge Setting Por	t Advanced Setting S	tatistics MS	Tinstance MST Port Se	tting	
General Setup	MST	Priority	Bridge identifi	Designated R	Root Port	Root Path Cost	Remaining Hop VLAN	Edit
Port Setting	0	32768	32768-00 1D AA B	0-00-00-00-00-00	NIGA.	0	0 1-4094	
Metor		32768	32768-00 1D AA 8	0-00 00 00 00 00 00	N/A	0	0	0
Link Aggregation	2	32768	32768-00 1D AA B	0-00-00-00-00-00-00	N/A	0	ń	0
VLAN Management	. 9	32768	32768-00 1D AA B.	0-00-00-00-00-00	R/A	0	D	0
EEE	4	32760	32768-00 1D AA B	0-00 00 00 00 00 00	N/A.	0	D	0
Multicast	5	32768	32766-00 1D AA B	0-00:00:00:00:00:00	N/A.	0	0	0
Jumbo Frame	6	32768	32768-00.1D:AA B	0-00-00-00-00-00-00	N/A.	0.	D	0
SUB	7	32768	32768-00 1D AA B	0-00-00-00-00-00-00	NIGA.	0	0	0
MAC Address Table	8	32768	32768-00 1D AA B	0-00 00 00 00 00 00	N/A.	D	Ú.	0
Blocked Port Recover	g	32766	32768-00 1D AA B	0-00 00 00 00 00 00	N/A	0	0	0
Security	10	32768	32768-00 1D AA 5	0-00-00-00-00-00	N/A	0	0	
ACL	- 11	32768	32758-00 1D AA B	0-00-00-00-00-00-00	NICA	0	D	00
QoS	- 12	32768	32766-00 1D AA B	0-00-00-00-00-00	N/A.	0	D	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 GI port / LAG port.							
	Edit MSTI 1							
	VLAN							
	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							
	Root Port							
	2 Root Path Cost							
	2 0							
	2 Remaining Hop							
	2 0							
	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 : OP	2											10107140 🕞	
Dashboard		O Sut	M.LAN. > GTP :	METPUTEN	ticy								
Status	- 81	and the second		-		ort Advanced Sett				or Setting			
Switch Levi	-	Properti	Port-Set	ing bindg	a Setting Pr	ort Advanced Sett	ng Stat	istics Ma	ST Instance MST P	of satting			_
General Setup			MSTE			I							
Port Setting													
Mirror													
Link Aggregation		Port	Path Cost	Priority	Port Role	Port State	Mode	Туре	Designated	Designated P	Designated	Remaining Hop	Edit
VLAN Management		GET	20000	128	Disabled	Disabled	RSTP	Boundary	0-00.00.00.00.00	128-1	20000	20	0
EEE.		OE2	20000	128	Disabled	Disasled	RSTP	Boundary	0-00-00-00-00-00	128-2	20000	20	0
Multicast		GES	20000	128	Disabled	Dissoled	RSTP	Boundary	0.00.00.00.00.00	128-3	20000	20	0
Jumbo Frame		GE4	20000	128	Disabled	Disablea	RSTP	Boundary	0-00-00-00-00-00	128/4	20000	20	0
		GE5	20000	128	Disabled	Disabled	RSTE	Boundary	0-00 00:00 00 00	128-5	20000	29	0
MAC Address Table		GE6	20000	128	Detabled	Disabled	RSTP	Ebundary	0.00.00.00.00.00	128-6	20000	20.	0
Ellocked Port Recover		GE7	20000	128	Disabled	Disabled	RSTP	Boundary	0-00 00 00 00 00	128-7	20000	20	0
Secunty	-	GEB	20000	128	Disabled	Disabled	RSTP	Boundary	0-00-00-00-00-00	128-8	20000	20	0
ACL.	-	GE9	20000	128	Disabled	Disabled	RSTP	Boundary	0-00 Dia DO 00 00	128-9	20000	20.	0
DoS		GE10	20080	128	Disabled	Forwarding	RSTP	Boundary	0-00:00:00:00:00	128-10	20000	20	0

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.

Di-		DOTO			
		Edit Po	rt GE1		· •
		MS	ті		C
		Path (	Cost		
			(1 - 2000	0000,0 = A(10)	0
		Prior	rity		
12	8			•	
		ок	Cancel		
Dis	sabled	RSTP		Boundary	
MSTI -	Display th	e selected	MST insta	nce.	
lue w	vill be use	d as the for	warding	e port. A port port by spann ie bandwidth (	ing tree.
ower p prwarc	oriority wi	II have high	er chance tree. Use	e path cost, po e to be used a e the drop dov	is 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 : Off 🛛 👻									
Dashboard	MAC Address Table > Static MAC Setting > Static MAC								
Status -	Static MAC								
Switch LAN	Static MAC								
General Setup	MAC Address:			00:00					
Port Setting	VLAN:	default				•			
Mirror	Port:	GE1				•			
Link Aggregation	Fuit		GET	_					
VLAN Management				Add					
EEE									
Multicast	No. It	MAC Address	11	VLAN		Port I	Delete		
Jumbo Frame	1	00:1D:AA:BB:C1:D	1	default(1)		CPU			
STP									
MAC Address Table									
Static MAC Setting									
Dynamic Address Setting									
Dynamic Learned									
Blocked Port Recover									

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

# II-10-2 Dynamic Address Setting

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

Auto Logout : Off	~					Ð
Dashboard		MAC Address Table > Dynamic > Dynamic > Dynamic > Dynamic > Dynamic > Dynam	ress Setting > Dynamic Address Setting			
Status	*	Domania Address Dettion				
	Ŧ	Dynamic Address Setting				
General Setup		Aging Time:	300	٥	(5-32767)	
Port Setting		Apply				
Mirror						
Link Aggregation						
VLAN Management						
EEE						
Multicast						
Jumbo Frame						
STP						
MAC Address Table						
Dynamic Learned						
Blocked Port Recover						

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 : 🛛 🗧 🧧					10:11:02 🕞
Dashboard	MAC Address Table :	> Dynamic Learned -> Dynami	c Learned		
Status -	C-COLUMN TWO IS				
Switch LAU	Dynamic Learned				
General Setup	MAC Address	VLAN	Туре	Port	Ú.
Port Setting	00-10-AA-01-05-74	default(1)	Dynamic	GE12	Add to Static
Mirror Link Aggregation	00 1D-AA 0C 87 F6	default(1)	Dynamic	GÈ10	Add to Static
VLAN Management	00 1D-AA-0C-88 05	default(1)	Dynamic	GE10	Add to Static
EEE	00 1D AA 11 22 5E	default(1)	Dynamic	GE12	Add to Static
Multicarst	00 1D AA 80 30 3C	default(1)	Dynamic	GE12	Add to Static
Jumbo Frame	00:10 AA 9F 55 DC	default(1)	Dynamic	GE12	Add to Static
STP	00:10 AA:E6:00:00	default(1)	Dynamic	GE12	Add to Static
MAC Address Table	00:1F:D0:1C:FE:79	default(1)	Dynamic	GE10	Add to Static
Static MAC Setting Oynamic Address Setting	00:50:7F:F1:06:7A	default(1)	Dynamic	GE10	Add to Static
	00:E0:4C:00:00:00	default(1)	Dynamic	GE10	Add to Static
Blocked Port Recover	08.00.27 18,88.2A	default(1)	Dynamic	GEIO	Add to Static
and the second se					

Item	Description	
MAC Address	Display the MAC address that will be forwarded.	
VLAN	)isplay 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 : 🛛 🖉				14 07 23 🕞
Dashboard	Switch LAN > Blocked Pen Recover > Blocked R	Park Hingann		
Status -	Concernments of			
SHIMUM	Blocked Part Recover		in the second	
General Setup	Recovery Interval:	300	Sec (30 - 06400)	
Port Setting	BPDII Guard:	Enable		
Mirror	Self Loop:	🖂 Enable		
Link Aggregation	Broadcast Flood:	Enable		
VLAN Management	Unknown Multicast Flood:	Enable		
EEE	Unicast Flood:	Enable		
Molticast	ACL:	Enable		
Jumbo Frame	Port Security:	🗖 Enable		
STP	DHCP Rate Limit:	Enable		
MAC Address Table	ARP Rate Limit:	🗇 Enable		
Ellocked Port Fracover	Apply			
Security -	CANO.			
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.
Apply	Apply the settings to the switch.

This page is left blank.

# Part III Security

VigorSwitch P2121 User's Guide

# **III-1 RADIUS**

o Logue 🗤 💌				
RADI	AR			
hua 🗠 👘		Use Default Parameters		
ICR LAN				
umi-	Retries:	a	👙 (1 - 10, default 3)	
aa l	Timeout for Reply:	. th	📚 sec (1 - 30, defauls 3)	
109+	Key String:			
agement Access Auther		Haply		
agement Access Contro		Add RADIUS Genrer		
187MAC Autoentication				
Security	Address Type:	OHostname @#v4		
cted Ports	Server Address:			
n Control	Server Port:	1419	11 85535, datau(11812)	
	Priority:		(0-65536)	
amic ARP Inspection	Retry:	Dise Default		
P Snooping		7	(1 = 10, dafault 3)	
ourre Guard	Timeouti	Wise Default		
		14	sec (1 - 30, détaut 3)	
	Key String:	Use Default		
	Usage:	OLogin ⊖802.1x ⊙All		
m Maintenance		()		
ostiću -				
Surver	Address Ser	ver Port Priority Retry	Timeout Usage	

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

Available settings are e	explained as	follows:
--------------------------	--------------	----------

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.

under Edit- Click it to modify the priority setting for the selected GE port / LAG port.

		*	(1 - 65535, default 18
Priority:	1	٢	(0 - 65535)
Retry:	Use Defa	ult	
	3	4 >	sec (1 - 10, default 3
Timeout:	🔽 Use Defa	ult	
	З	\$	sec (1 - 30, default 3
Key String:	☑ Use Defa	ult	
Usage:	(	) Login () 80	)2.1x ⊚ All

# III-2 TACACS+

Auto Logout : 🔄 min 🚿	Tom		22343:17 🕞
Dashboard	TALACS+		
Status -			
Switch LAN -		Use Default Parameters	
terior 1			
RADIUS	Teneout:	5	🗧 sec (1 - 30, detaut 5)
Тирицан	Key String:		
Management Access Authentica		Apply	
Management Access Control		Add TACACS • Server	
S02 1X/MAC Authentication			
Parl Security	Address Type:	CHostname @IPv4	
Protected Ports	Server Address:		
Storm Control	Server Port:	-19	C (1 - 85535, detault 40)
DoB	Priority:		(0 - 55535)
Dynamic ARP Inspection	Timeout:	🖅 Use Defasil	
DHCP Snooping	Harabar.	2 El Ana Ana ana	4.66. (1 - 30, default.6)
IP Source Guard	Key String:	Ouse Default	
AOL -		T	
QoS -		(Ada)	
PoE -			
System Maintenance -	Server Address	Server Port II Priority	Timeout
Disonostics -		No data available en table	

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 : Off 🛛 👻			10:15:08 🕞				
Dashboard	Security > Management Access Authentication > Method Profile						
Status *	Method Profile Application Authentication						
Switch LAN *	Application Addientication						
Security		Method Profile					
RADIUS							
TACACS+	Name:						
Management Access Authentication	Optional Methods:	Selected Methods:					
Management Access Control	None	A					
802.1X/MAC Authentication	Local RADIUS						
Port Security	TACACS+						
Protected Ports	~	···					
Storm Control							
DoS		Add					
Dynamic ARP Inspection							
DHCP Snooping							
IP Source Guard	Profile Name	Selected Methods	Edit				
ACL -	default	Local	0				
ACL -			-				

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.

Anto Logout : 🔍 🖌	Tom			14:2010	e 🕞
Dashboard	Security > Management Access Authenlic	ation - Application Authenricale	חק		-
Status -	Method Profile Application Authentication				
Switch LAN -	Milling Prose				
Sendty -			Application Authentication		
RADIUS					
TACACS+	Application:	Console		÷.	
Management Access Authenticatio	Selected Profile:	default			
Management Access Control			Apple		
B02 1X/MAC Authentication					
Port Security	Application		Selected Profile		4
Protected Ports	Console		default		
Storm Control	Telnet		default		
DoS	SSH		default		
Dynamic ARP inspection	HTTP		default		
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 : Off	8					004E45 🕞
Dashboard Status	Management Acress Control Pro	Management Access Control 3	intries (ACE)	_		
Switch LAN			Management Access	i Control Profile(ACL)		
Shann	1					
RADIUS	ACL Name:					
TACACS+			68	a		
Management Access Ad	Inentics					
Management Access to	ACL Profile Name	State	Rute	Activitie	Deactivate	Delete
802.1XMAC Authenticab	ion AOL_Came_1	Insutre	0	0		٠
Port Security						
Protected Ports						
Storm Control						
Dos						
Dynamic ARP Inspection	n -					
DHCP Snooping						
IP Bource Guard						
ACL	-					
800						
PoE	-					
System Maintenance	-					
Diagnostics						

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 🛛 👻	📀 Security > Manage	ment Access Cor	itrol > Manag	gemen	t Access Contr	ol Entries (ACE;	1						
Dashboard	Management Access (	Control Profile(ACL	Mana	aemen	it Access Contr	ol Entries (ACE							
Status *	<b>,</b>	,	, <u> </u>	~									
Switch LAN -	Management Access Control Entries (ACE)												
Security													
RADIUS	ACL Pro	file Name:		ACL	_1_Carrie						-		
TACACS+	Priority:			1					\$	(1 - 65	(535)		
Management Access Authentication	Service:			All							-		
Management Access Control	Action:			Den	Y						•		
802.1X/MAC Authentication	Ports:				ning selected								
Port Security	Pons:			Notr	ning selected						÷		
Protected Ports	IP Versio	ins:		<ul> <li>All</li> </ul>	OIPv4 O	IPv6							
Storm Control	IPv4:							/	255.25	5.255.2	255		
DoS	IPv6:							/	128				
Dynamic ARP Inspection						Add							
DHCP Snooping													
IP Source Guard	ACL Profile N 灯	Priority 👫	Service	II	Action 📗	Ports 👫	IP Version	II	IP Address	11	IP Netmask	11	Edit
ACL -	ACL_1_Carrie(In	1	ALL		Deny	GE1-GE3	All						

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.
	Permit - 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	Specify the IP address/subnet to which the ACL should be applied.
	• All - All the IP address should be applied.
	<ul> <li>IPv4 - Specify the IPv4 address /subnet.</li> </ul>
	• 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 AC	E with ACL profile=sdf
	and Priority=1
Service:	All
Action:	Deny
Ports:	GE1 ·
IP Versions:	
IPv4:	
IPv6:	I

# 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 P2121 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 Logout : Off 🗸				G				
Dashboard	802.1X/MAC Authentication > Properties > Global Settings							
Status -								
Switch LAN -	Global Settings Port Authentication Setting							
Security		Global Settings						
RADIUS								
TACACS+	Authentication Types:	Nothing selected *						
Management Access Authentication	Guest VLAN:	🗌 Enable						
Management Access Control	Selected VID:	1						
802.1X/MAC Authentication	MAC-Based User ID Format	×00000000000 -						
Properties		Apply						
Port Control/Settings		Adda 1						
MAC-Based Local Account								
Authenticated Hosts								
Port Security								
Protected Ports								
Storm Control								
DoS								

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.

Dashboard	Global Settings Post Automatication Setting			
Status -				
Switch LAN -		Per Port Mode Settings		
Generity.				
RADIUS	Apply Settings to Ports:	56-30-31	1	
TACACS	Authentication Types Enabled:	Fourthern a		
Management Access Authendes	Host Mode:	Multiple Authentication		
Management Access Control	Available Authentication Types:	Selected Authimliciation Type	s: (In Dritler)	
S02 1XMMC Autoestication	MAC-based	Sk Denned		
Propersies	MAC-Based	and a second sec		
Port CantrovSecting		0		
MAC-Balled Lot at Account	_			
Autoenticated Fronts	Available Methods:	Selected Methods: (In Order)		
Port Security		and Party and Pa		
Protected Ports	Locar	en la companya de la comp		
Starm Control		ā		
DoB				
Dynamic ARP inspection				
DHCP Snooping	Guest VLAN	Enable		
IP Source Ouard	RADIUS VLAN Assignment:	Static		
ACL .		( Apply )		

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	Multiple Authentication - Each host are authenticated individually. 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.
	Single Host - Only one host can be authenticated, and access the port.
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.
	Reject - 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 : Off 🛛 👻						Ð
Dashboard	802.1X/MAC Authentication > Port Control/Settings	s > Port Control/Settings				
Status -	Port Control/Settings					
Switch LAN +	Port Control/Settings					 
Security -		Port Control/Settings				
RADIUS						
TACACS+	Ports:	Nothing selected			*	
Management Access Authentication	Port Control:	Disabled			•	
Management Access Control	Periodic Reauthentication:	🗌 Enable				
802.1X/MAC Authentication	Max Hosts:	256		*	(1-256, default 256)	
Properties Port Control/Settings	Reauthentication Period:	3600	Sec (300	- 42949	967294, default 3600)	
MAC-Based Local Account	Inactive Timeout:	30	*	Sec (6	0 - 65535, default 60)	
Authenticated Hosts	Quiet Period:	30	*	Sec (6	0 - 65535, default 60)	
Port Security	Resend EAP Period(802.1X Parameter	30	•	Sec (3	0 - 65535, default 30)	
Protected Ports Storm Control	Supplicant Timeout(802.1X Parameter	30	*	Sec (3	0 - 65535, default 30)	
DoS	Server Timeout(802.1X Parameter):	30	*	Sec (3	0 - 65535, default 30)	
Dynamic ARP Inspection	Max EAP Requests(802.1X Parameter)	2		*	(1 - 10, default 2)	

Item	Description		
Ports	Select the ports to modify the port control settings.		
Port Control	Specify if you wish this account to be allowed (Authorized) o blocked (Unauthorized) or determined by VigorSwtich (Auto)		
	• <b>Disabled</b> - Disable any authentication requirement for port access. All clients are allowed to access the network.		
	• 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.
Apply	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 Logout : Off 🛛 👻			10:37:38 🕞
Dashboard	0 802.1X/MAC Authentication > MAC-Based Local A	Account > MAC-Based Loc	cal Account
Status -	MAC-Based Local Account		
Switch LAN -	WAC-based Local Account		
Security -		MAC-Based	d Local Account Settings
RADIUS			
TACACS+	MAC Address:	00:00:00:00:00:00	
Management Access Authentication	Port Control:	💿 Force Authorized (	) Force Unauthorized
Management Access Control	VLAN:	🔲 User Defined	1 (1-4094)
802.1X/MAC Authentication	Reauthentication Period:	🔲 User Defined	3600 Sec (300 - 4294967294)
Properties	Inactive Timeout:	User Defined	
Port Control/Settings	inacuve Timeout:	_ oser benneu	60 🔅 Sec (60 - 65535)
MAC-Based Local Account			Add
Authenticated Hosts			
Port Security	MAC Address II Port Control	IT VLAN	It Reauthentication P It Inactive Timeout It Edit
Protected Ports		No data	a available in table
Storm Control			
DoS			
Dynamic ARP Inspection			

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	User Defined - Check it to specify the time of inactive this account becoming log-off.	
Add	Click it to create a new account.	
Edit	It is available when there is one profile existed.	
	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.

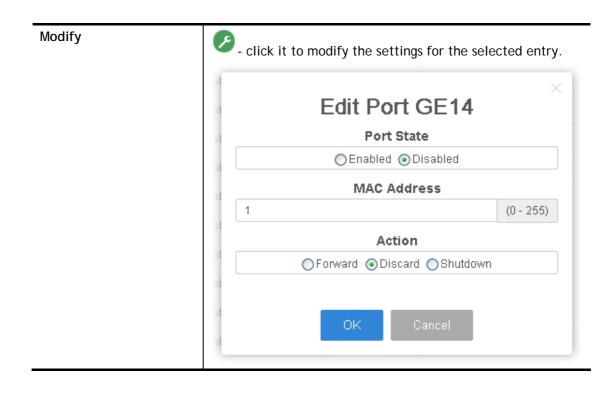
Auto Logout : Off 💦 👻	User 10.38-19 🕞
Dashboard	🕐 1922 19/MAC Authentication -> Authenticated Hostie -> Authenticated Hostie
Status -	Authenvirosted Hosts
Switch LAN -	Authemicated Hosts
Securit)	Autombicated Hosto
RADIUS	Session ID Port MAC Address Current Type Status Operational Operational Operational I Operational
TACACS+	No data available in table
Management Access Authenticatio	
Management Access Control	
802 IX/MAC Authentication	
Properties	
Port Control/Settings	
MAC-Based Local Account	
Pad Security	
Protected Ports	
Storm Control	
DeS	
Dynamic ARP Inspection	

# **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 Lugaut : 🛛 a min 🛛 👻		üser.			(03:39-))	Ð
Dashboard	Security > Pon	security > Pon Security				
Status -	Providencial Strength					
Switch LAN	Port Security					
Beconty			Port Security			
RADIUS						
TACACS+	Stat	te:	🛞 Enable 🔿 Disable			
Management Access Authenticatio	Por	ts:	in a training make the o		-	
Management Access Control	Por	t State:	🔿 Enable 💿 Disable			
802.1X/MAC Authentication	MAC Address		1 2			(0 - 255)
Port Security	Acti	00:	O Forward (2) Discard	C Shutdown	-	
Protected Ports			(App)			
Storm Control						
DuS						
Dynamic ARP Inspection	Port	State	MAC Address	Action	Modify	
DHCP Shooping	GE1	Disabled	ň.:	Discard		
IP Source Goard	GE2	Disabled	A	Discard		
ACL -	GES	Disabled	#5	Discard		
0.05 -	GE4	Disabled	1	Discard		

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.
	<b>Disabled</b> - 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	Select an action to perform when there is an unknown MAC address on the port.
	<b>Forward</b> - Forward a packet whose source MAC is unknown to the switch.
	<b>Discard</b> - Discard a packet whose source MAC is unknown to the switch.
	<b>Shutdown</b> - Shutdown this port when a packet with unknown source MAC is received.
Apply	The modification made above can be applied on to the selected GE/LAG port immediately.



# **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 Looput : 💷 🚿			ay as the 🕞
Dashboard	Protected Points		
Status +			
Switch LAN +	1 Constanting	Protected Perts Settings	
=000liM			
RADAIS	Port List	Matthing anomalia	3+
TAGACS+	Protected	OEnable @Disable	
Management Access Authentics		Hanty	
Management Access Control			
802 1X0MAC Authantication		Protected Ports Blasus	
Port Recurity	Port	Protected	
Pronkalia Porte	0E1	Depable	
Starm Control	062	Disable	
Dog	9E3	Disable	
Dynamic ARP Inspection	OE4	Disable	
DHCP Brooping	0E5	Distable	
P Source Ocard	066	Disable	
KCL -	0E7	Desable	
- 205	OES	Delhabié	
PoE -	OES	Disable	
System Maintenance -	OE10	Disable	
Diagnostics =	0E11	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 Lagout : 3 min 🤎		05-42:36 🕞
Dashboard	💽 Stomi Control -> Properties -> Properties	
Status -		
Switch LAN -	Propèrties	
Secondy	Storm Control Mode: O Packet/sec   Kbits/sec	
RADIUS	Preamble & Inter Frame Gap: <ul> <li>Excluded</li> <li>Included</li> </ul>	
TACAOS+	Apply	
Management Access Authentication	-	
Management Access Control		
802.1X/MAC Authentication		
Port Security		
Protected Ports		
Storm Control		
Proportion		
Fort Selling		
DeS		
Dynamic ARP Inspection		
DHCP Snooping		
IP Source Guard		

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 Legest : 3 min 👻		User				1	19 44 20 🕞
Dashboard	O Stami	Control > Port Setting > Por	t Settingé				-
Status -	No. Since						
Switch LAN -	Port Settin	g*					
Secula				Port Sellings			
RADIUS							
TACACS+		Ports:		othing selected			
Management Access Authentication		Storm Control:		O Enable 💿 Disable			
Management Access Control		Limiting Rate:		Bruadcast	10000	(Khps; 18-111	0000
802.1X/MAC Authentication				Unknown Multicast	10000	(Hops, 16-100	
Port Security							
Protected Ports				Onknown Unicast	10000	(Abps, 16-100	00000)
Storm Control		Action:		Orop O Shutdown			
Properties				Apply			
Part Sinting							
HeS	Port	Storm Control	Broadcast (pps)	Unknow Multica	Unknow Unicas	Action	Modify
Dynamic ARP Inspection							
DHCP Snaoping	GE1	Disabled	Disabled	Disabled	Disabled	Drop	0
IP Source Guard	GE2	Disabled	Disabled	Disabled	Disabled	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.
	Enable - 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.
	<b>Unknown Multicast</b> - Specify the storm control rate for unknown multicast packet. Value of storm control rate, Unit: Kbps (Kbits per-second). The range is from 16 to 1000000.
	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.

# 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 : 08	~					100 SA 33 🕞
Protected Ports Storm Control	0	oS i Properties i Protoctica				
DoS	Prop	etter				
			Global Settings			
DaS Port Sitting						
Dynamic ARP Impection		Dst MAC - Src MAC	S Enabled Disabled			
DHCFI Snooping		LAND	© Enabled () Disabled			
IP Source Guard		UDP Blat	⊙ Enabled ⊖ Disabled			
ACL	-	TCP Blat	💮 Enabled 🔘 Disabled			
DoS	-	Ping of Death	Enabled O Disabled			
PoE	-	IPv6 Min Fragments	Enabled O Disabled	1240	Bytes (0-65535)	
System Maintenance		ICMP Fragments	Enabled      Disabled			
Diagnostics	10	IPv4 Ping Max Size	Enabled      Disabled			
		IPv6 Ping Max Size	@ Enabled () Disabled			
		Ping Max Size Setting	512	Bytes (0.65535)		
		Smud Attack	③ Enabled ⑤ Disabled	Netmask Length: 0		(0-32)
		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.
5	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.
	Disabled - 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.
-	Disabled - 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. <b>Enabled</b> - 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.
	Disabled - Disable the item function.
	Enabled - Enable the item function
TCP SYN-RST Attack	Drop the packets with SYN and RST bits set.
I OF JIN-KJI ALLOUK	<b>Disabled</b> - Disable the item function.
	Enabled - Enable the item function.

TCP Fragment (Offset=1)	Drop the fragmented ICMP packets. Disabled - Disable the item function. Enabled - Enable the item function.
АррІу	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 Logout : 3 min 🖌	User			03:46:42 🕞
Dashboard	O DoS > DoS Port Setting > Port Settings			
Status -	Port Settings			
Switch LAN -	Port Settings			
Security -		Port Setting		
RADIUS				
TACACS+	Ports:	Nothing selected		-
Management Access Authentication	DoS Protection:	💿 Enable i 🔘 Disable		
Management Access Control		Apply		
802.1X/MAC Authentication				
Port Security	Port It	DoS Protection	If Modify	
Protected Ports	GE1	Disabled		
Storm Control	GE2	Disabled	0	
DoS	GE3	Disabled	0	
Properties	GE4	Disabled	0	
DoS Port Setting	GE5	Disabled	0	
Dynamic ARP Inspection				
DHCP Snooping	GE6	Disabled	0	
IP Source Guard	GE7	Disabled	<b>Ø</b>	

Item	Description
Port	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.

Aista Lagoost : Of 📧	Tem			62:44:02 E+
Dashboard	Oldhal Property Settings Per Port Property Settings			
Status -				
Switch LAN -			Olobal Property Settings	
CLOSER	1.000	-		
RADIUS	Statir:	Enable		
TACACS+	VLANS:	Consell Property		
Management Access Authentics			(Apple)	
Management Access Control				
802.19/MAC Authentication				
Port Security				
Protected Ports				
Storm Control				
Doð				
Dynamic ARP Inspection				
Properties				
Abellie				
DHCP Sepaping				
IP Bourde Gulard				
ACL -				
0o8 +				
PoE +				

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/LAG port 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 Logout : 3 mite 👻		User					G•
Dashboard	O Dynam	n. ARP Inspontion -> Proportion ->	Per Part Property Solump	(			
Status -	(Internet						
Switch LAN -	Global Pro	perty Settings Per Port Prope	ny Settings				_
Summer -			P	er Port Property Settings			-1
RADIUS							
TACACS+		Puris:	Mattinu sa asjari				
Management Access Authentication		Trust:	🗇 Enable				
Management Access Control		Source MAC Address:	🗇 Enable				
602.1X/MAC Authentication		DestinationMAC Address:	Enable				
Part Security		IP Address:	Enable	Allow Zero (	(0.0.0.0		
Protected Ports		Rate Limit:	10	🗢 pps. (1	50, detault 0 0 in 100medend)	1	
Storm Control				Apply			
DoS							
Dynamic ARP Inspection	Port	Trust	Source MAC A	dd Destination MAC	IP Address	Rate Limit	
Proportion	GE1	Disabled	Disabled	Disabled	Disabled	Unlimited	
Statedies	GE2	Disabled	Disabled	Disabled	Disabled	Unlimited	
DHCP Snooping	GES	Disabled	Disabled	Disabled	Disabled	Unlimited	
IP Source Guard	GE4	Disabled	Disabled	Disabled	Disabled	Unlimited	

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	Enable - Check it to enable the function of source MAC address validation mechanism for the selected port(s).
Destination MAC Address	Enable - Check it to enable the function of destination MAC address validation mechanism for the selected port(s).
IP Address	<ul> <li>Enable - Check it to enable the function of IP address validation mechanism for the selected port(s).</li> <li>Allow Zero - The IP address of "0.0.0.0" can be applied to the selected port(s) if it is enabled.</li> </ul>
Rate Limit	Use the drop down list to choose a rate limitation value (0~50) for the selected port(s).
Apply	Apply the settings to the switch.

# III-10-2 Statistics

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

Anin Longoui : 3 mm 💌		0161							
Dashboard	O Dynami	ARP Importun	Statistics + Statistics						
Status -	(Property)	1000							
Switch LAN -	Statietics								
Simular -				Statistics					
RADIUS	-								
TACACS+	Refresh	O Clear All							
Management Access Authenticatio	à								
Management Access Control	Port	Forward	Source MAC Fa	Destination MA	Source IP Valid	Destination IP	IP-MAC Mismat		
602 1X/MAC Authentication	GEI	0.	0.	٥	0	0	0		
Port Security	GE2	a	ű.	a	п	0	n.		
Protected Ports	GE3	a.	a.	0	п	0	n		
Storm Control	GE4	a	a.	a	n	0	n.		
DoS	GE5	0.	0	٥	Ø	0	0		
Dynamic ARP Inspection	GE6	0	0	0	Ø	0	Ŭ.		
Proporties	GE7	0	0.	٥	ũ	0	Ŭ.		
	GE8	0	0.	٥	ũ	0	0		
DHCP Snooping	GE9	0	a.	0	O	0	0		
IP Source Guard	GE10	0	ā	0	0	0	D		

# **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.

-	User		03:54-11 🕞
	O DHCP Shamping > Properties > P	Solial Property Solition:	
	Contractor of the second		
	Global Property Settings Per Por	ti Property Settings	
1		Global Property Settings	1
	State:	🗇 Enable	
	VLANs:	[Initiary association	-
		Apply	
+			
-			
-			
		OHCP Strangarty - Properties - C Global Property Settings Per Por State:	DHCP Shamperg > Properties: > Global Property Settings     Global Property Settings     Global Property Settings     State:      Lable     VLANs:      Natting subscene

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 : 3 min	•							03:54:54	Ð
DoS		O DHCP Snooping > Properties > Per F	Port Propert	y Settings					
Dynamic ARP Inspection									
DHCP Snooping		Global Property Settings Per Port Po	roperty Sett	ings					
Properties				Per Port Pro	perty Settings				
		Ports:		Nothing selected			*		
		Trust:		🔲 Enable					
IP Source Guard		Verify Chaddr:		🔲 Enable					
ACL	-	Rate Limit:		0	*	pps (0 - 300, default 0. 0 is	Unlimited)		
QoS	•				ply	ppe (e coci, construction			
PoE	•				Vid				
System Maintenance	•	Port	Trust	It	Verify Cha	ldr It	Rate Lim	it	11
Diagnostics	*	GE1	Disabled		Disabled		Unlimited		
		GE2	Disabled		Disabled		Unlimited		
		GE3	Disabled		Disabled		Unlimited		
		GE4	Disabled		Disabled		Unlimited		
		GE5	Disabled		Disabled		Unlimited		
		GE6	Disabled		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 : 3 min 👻						03:56:20 🕞
Storm Control	O DHCP Snooping	> Statistics > Statistics				
DoS	Statistics					
Dynamic ARP Inspection						
DHCP Snooping			S	tatistics		
Properties	@Refresh ()	Clear All				
	Port 1		Chaddr Check Drop 🕼		Untrust Port Drop 1	
IP Source Guard	GE1	0	0	0	0	0
ACL -	GE2	0	0	0	0	0
QoS -	GE3	0	0	0	0	0
PoE -	GE4	0	0	0	0	0
	GE5	0	0	0	0	0
System Maintenance *	GE6	0	0	0	0	0
Diagnostics -	GE7	0	0	0	0	0
	GE8	0	0	0	0	0
	GE9	0	0	0	0	0
	GE10	0	0	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 Logout : 3 min	*	Dum		10.57.04 🕞
Storm Control	0	DHCP Structure > Option82 Property	$n_T > 3  ext{stabal}$ Optor 82 Property Settinga	
DoS		label Option82 Property Settings	Per Pod OptionR2 Property Settings	
Dynamic ARP Inspection				
DHCP Snooping			Global Option82 Property Settings	
Properties. Statistims		Remote ID:	🔲 User Defined	
Option82 Propeny			00.1d/aa.bb/c1.d1 (Switch Mac in Byte Dider)	
Option82 Circuit ID			Apply	
IP Source Guard	-			
ACL	12			
Gos	- 12			
PaE				
System Maintenance				
Diagnostics	- 9			

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 Logout : 3 min	▼ User			03:57:45 🕞				
Storm Control	O DHCP Snooping > Option82 Pr	O DHCP Snooping > Option82 Property > Per Port Option82 Property Settings						
DoS	Global Option82 Property Settings	Per Port Option82 Property Settings						
Dynamic ARP Inspection		Per Port Option82 Pr	operty Settings					
DHCP Snooping	_							
Properties Statistics	Ports:	Nothing selected	*					
	State:	🗌 Enable						
Option82 Circuit ID	Allow Untrust:	🔿 Keep 💿 Drop 🔿 Replace						
IP Source Guard		Apply						
ACL QoS	_ Port	Lt State	Allow Untrust	It				
PoE	GE1	Disabled	Drop					
System Maintenance	GE2	Disabled	Drop					
Diagnostics	- GE3	Disabled	Drop					
	GE4	Disabled	Drop					
	GE5 GE6	Disabled	Drop					
	GE7	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.
АррІу	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 : 🛛 3 min 🛛 👻													
Storm Control	ODHCP Snooping > Option82 Circ	DHCP Snooping > Option82 Circuit ID > Option82 Circuit ID											
DoS	Option82 Circuit ID												
Dynamic ARP Inspection			o /										
DHCP Snooping			Option82 Circuit	t ID Table									
	Port:		GE1	•									
	VLAN:		Keep empty to set without VLAN	\$ (1 - 4094)									
	Circuit ID:												
IP Source Guard													
ACL -			Add										
QoS -													
PoE -	Port	IT VLAN	11	Circuit ID	L) Edit								
System Maintenance -			No data availab	le in table									
Diagnostics -													

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.
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 : 3 min 👻								04:00:48	G
DYNAMIC ARP Inspection DHCP Snooping	IP Source Guard > Port S	lettings > Port Setting	S						
IP Source Guard	Port Settings								
				Port Settings					
IMP∨ Binding				T on Gennige					
Save Database	Ports:		Nothing sel	ected			÷		
ACL -									
QoS -	State:		🗌 Enable						
PoE -	Verify Source:								
System Maintenance	Max Entry:		0 (0 - 50, default 0. 0 is Unlimited)						
Diagnostics -				Apply					
	Port	t State	II	Verify Source	1J	Current Entry	IJ	Max Entry	1J
	GE1	Disabled		IP		0		Unlimited	
	GE2	Disabled		IP		0		Unlimited	
	GE3	Disabled		IP		0		Unlimited	
	GE4	Disabled		IP		0		Unlimited	
	GE5	Disabled		IP		0		Unlimited	
	GE6	Disabled		IP		Π		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 : 3 min 💌												04:03		Ð
Dynamic ARP inspection DHCP Snooping	O IP Sou	P Source Guard > IMPV Binding > IMPV Binding												
IP Source Guard	IMP∨ Bind	PV Binding												
Port Settings		IP-MAC-Port-VLAN Binding Table												
Save Database		Ports:			GE1							•		
ACL -														
QoS -	VLAN:				1 - 4094)					094)				
PoE -		Binding:			O IP-MAC-Port-VLAN     O IP-Port-VLAN									
System Maintenance -		MAC Addre	ess:		00:00:00:00:00									
Diagnostics -		IPv4 Addre	ss:		/ 255.255.255									
					Add									
	Port 📗	VLAN	II	MAC Address 🕼	IP Address	11	Subnet Mask	11	Binding 💵	Туре	lt	Lease Time	11	Edit
	GE1	1		00:00:7E:51:20:9A	192.168.1.82		255.255.255.25	5	IP-MAC-Port-V	Static		N/A		Ø 🔞

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.
	<b>IP-MAC-Port-VLAN</b> – Packets will be allowed to pass through the port interface if they meet the conditions specified by IP address, MAC address, Port setting and VLAN ID setting.
	<b>IP-Port-VLAN</b> – Packets will be allowed to pass through the port interface if they meet the conditions specified by IP address, Port setting and VLAN ID setting.
MAC Address	Enter the MAC address of the device connecting to the port interface selected above.
IPv4 Address	Enter the IP address with mask address of the device connecting to the port interface selected above.
Add	Click it to create a new binding profile.
Edit	Click it to modify the settings for the selected entry.

í		Edit
	Ports:	GE1 -
	VLAN:	1 🔅 (1 - 4094)
	Binding:	● IP-MAC-Port-VLAN ○ IP-Port-VLAN
	MAC Address:	00:00:7E:51:20:9A
	IPv4 Address:	192.168.1.82 <i>I</i> 255.255.255
		OK Cancel
	MAC Address 11	IP Address If Subnet Mask If Bir
(E	- click it to rer	move the selected entry.

# III-12-3 Save Database

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

Anin Logoui ; 3 min						84:05:40	⇔
Dynamic Axi- inspection DHCP Snooping		O IP Source Guard - Siner Uniations - S	ions Dabatime				
IP Source Guard		Save Database					
Port Sithings			Save	Database			
MPV Binding							
		Туре:	None O Flash O TFTT	P.			
ACL	-	Filename:					
0oS	-	Address Type:	- Hostname IPv4				
PoE		Server Address:					
System Maintenance		Write Delay:	301		Stor: (15 - 196403), dotaid( 303)		
Diagnostics							
		Timeout:	300	2	Sec (0 - 86400, default 300)		
				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.

This page is left blank.

# Part IV ACL Configuration

VigorSwitch P2121 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 Logoni : 3 min	-					84:08:16	Ġ:
Dashboard		O ADL - Coole ADL - MAC					_
Status		MAC IPv4 IPv6					
Switch LAN	-	MAC IPv6					
Security	-	ACL Profile Name:	ACL_1_carrie				
	-			Ade			
Small MG(				-			
Create ACE		No.	 MAC ACL Name		Action		- 11
ACL Binding		t	ACL_1_came		0		
QoS					1.24		
PoE	•						
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 Logout : 3 min 💌				04:09:36	€
Dashboard	O ACL > Create ACL > IPv4				
Status -					
Switch LAN -	MAC IPv4 IPv6				
Security -	ACL Profile Name:	ACL_1_4			
ACL -		Add			
Create ACL					
Create ACE	No. It	IPv4 ACL Name	It Action		II
ACL Binding	1	ACL_1_4			
QoS *					
PoE *					
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-1-3 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 Engout : 3 min	User			041100 De
Dashboard	Alt - Limite Alt - Heb			
Status Switch LAN	MAC IPvd IPvB			
Security	- ACL Profile Name:	ACL_1_6		
		Patr		
Create ACE	No.	IPv6 ACL Name	Action	91D
ACL Binding	1	ACL_1_6	0	
PoE	-			
System Maintenance Diagnostics	-			
rundino sur s				

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 Logoul : 08	~	ALL - Drepts ALL + MAC							
Dashboard		MAD IPv4 IPv6							_
Status Switch LAN	-	ACL Profile Names	ALL_1_carrie						
Security	-	Sequence:	1 21474836473						
M2	-	Action:	Perrol: -						
Create AGL		Source MAC:	[] Any						
GIBNERGE.			00/00/00/00/00	2	mounting				
ACL binding		<b>Restination MAC:</b>	Any						
QnS	-		46, pro monos ras cas		កាកកាត	1			
PoE System Maintenance		Ethertype:	[☑] Any						
Diagnostics	1		(0x8x3)-0xFFFF)						
		VLAIE	[2] Any						
			(antia.r)						
		602.1p:	Aby						
				1	(a)				
			Ada						
		No. Name Sequence	Action Source MAC/ Desti	nation	Ethertype	VLAN	802.1p	Modify	П
		1 ACL_1_come 1	Permit Any/Any Any/A	any	Any	Any	Any/Any	00	

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 MAC	Specify 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 from tha 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.
	Edit ACE ACL_1_carrie
	Sequence: 1
	Action: Permit -
	Source MAC: Any
	00:00:00:00:00:00 / FF:FF:FF:FF:00
	Destination MAC: Any
	00:00:00:00:00 / FF:FF:FF:FF:00
	Ethertype: 🔽 Any
	(0×600-0×FFF)
	VLAN: Any
	(1-4094)
	802.1p: 🛛 🖓 Any
	0-7
	OK Cancel
	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.

Auto Lognut : Off	8			Tón							04:19:45	G
Dashboard		MAC	4 IP-6									1.00
Status												
Switch LAN	-		ACL Prot	file Name	¥	ACL_IP4_MAC_CAR	RIE -					
Security			Sequenc	:0:		1. 0	(1 - 2147,483647)					
	-		Action:			Permè						
Create A/CL			Protocol			Any						
Criste ACE			Source I			P Any						
ACL Binding			Source I	P.2				1				
QoS						0.0 0.0		261.0	5.258 F			
PoE			Destinati	on IP:		🗹 Any						
System Maintenance	1							1 200 0	6,266.0			
Diagnostics			Service:			i#ny.						
			Source P	Port		Any						
			Destinati	on Port:		Any	÷.					
			ICMP Typ	pe:		Any						
			ICMP con	de:		2 Any						
						1355						
							Ana					
		nation I	DSCP	IPP II	Source Port	Source Port	Destination P	Destination P	TCP Flag	ICMP type	ICMP code	Modify
		ΠY.	Any	Any			-					00
		100	am	my.	an	any	any	-2/11/	Any		DV	

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> <li>Shutdown</li> </ul>
Protocol	Specify the protocol for filtering.
FIOLOCOI	Any – All packets will be filtered.
	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.
	<b>Define</b> - 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 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.
	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.
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

Auto Logout : Off	-			Ten	0						04/26/22	Ð
Dashboard		MAC IP	id IPi6									
Status												
Switch LAN			ACL Pro	file Name		ACL_P6_MAD	CARRIE +					
Security			Sequen	ce:		1	(1 - 2147483647)					
			Action:			Permit						
Create ACL			Protocol			Any						
ACL Binding			Source I	IP:		🖸 Any						
QoS								1	01.0			
PoE			Destinat	ion IP:		P Any						
System Maintenance	-							1	1121			
Diagnostics			Services			Any						
			Source I	Port		Any	-					
			Destinat	ion Port		Αηγ						
			ICMP Ty	da:		Απγ	•					
			ICMP co	de:		🖻 Any						
						0.265						
							Add					
		nation I	DSCP	IPP	Source Port	Source Port	Destination P	Destinatio	m P    TCP F	ag ICMP type	ICMP code	Modify
		.ñy	Any	Any		-		÷	1.5			00
		σų		NIX	Any	1 Mil	14/0	All	1.01	No.	- 444	-

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

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>
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	<ul> <li>Any - All packets will be filtered.</li> <li>DSCP - All IP traffic is mapped to queues based on the DSCP field in the IP header. If traffic is not IP traffic, it is mapped to the lowest priority queue.</li> <li>IP Precedence - All IP traffic is mapped to queues based on the IP Precedence field in the IP header. If traffic is not IP traffic, it is mapped to the lowest priority queue.</li> </ul>
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.
	<b>Select</b> - 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	Click it to modify the settings for the selected profile.
	Click it to remove the selected entry.

## **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 Logour : DH	~	Litter					Ð
Dashbowd		💽 ±CL + ±Cl Binding + ±CL Binding					
Stubus	4	ACL Bridha					
Switch LAN		WCC DI MITH					 
Security	+	Ports:		Usering websited			
40		MAC ACL:		Simpl MAC ACL		-	
Create ACL		IPe-I ACL:		Saect Py ( ARL		*	
Create ACE		IP46 ACL:		South this ald			
40 Andre					(Azal)		
GeS	-						
PoE		Port	MAC A	a	II IPvt ACL	IPv6 ACL	0
System Maintenance	-	GE1					
Diagnostics		GE2					
		GE3					
		GE4					
		GE5					
		GE6					
		GE7					
		GEB					
		GE9					
		GE10					
		GEN					

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.

This page is left blank.

# Part V QoS Configuration

VigorSwitch P2121 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 : Dil	*			G
Dashboard		General > Properties > OoS Clobal Setting		
Status	- 2	(Freedom and a second		
Switch LAN		OoS Global Setting Trial Ports		 
Security		QoS Mode:	🔿 Basic 💿 Disable	
ACL	- 4	Ingress Trust Mode:	⊙ CoS/802.1p ○ DSCP ○ CoS/802.1p.DSCP ○ IP Precedence	
	÷	_		
General		Apply		
Penperlan				
Port Settings				
Queue Settings				
CoS Mapping				
DSCP Mupping				
IP Precedence Mapping				
Bandwidth				
PoE	-			
System Maintenance	-			
Diagnostics	-			

Item	Description
QoS Mode	<b>Disable</b> -Disable the function of QoS mode. <b>Basic</b> - Enable the function of QoS mode.
Ingress Trust Mode	Select the QoS operation mode. 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. 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. 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. 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.
АррІу	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 : 04 👻	User		04:30:37 CF
Dashtroard	O General > Proportie > Trust P	ons.	
Status			
Switch LAN	QoS Global Setting Trust Port		
Security	-	Trust Ports	
ACL			
2 d D	Ports:	Nothing sweeting	~
General	Trust:	) Enable 🗇 Disable	
Properties		Apply	
Port Settings			
Quatar Settings			
CoS Mapping	Port	11 Trust	u.
OSCP Mapping	GET	Enabled	
IF Procedence Mapping	GE2	Enabled	
Bandwidth	GES	Enabled	
PoE	GE4	Enabled	
System Maintenance	GE5	Enabled	
Diagnostics	GE6	Enabled	
	GE7	Enabled	

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 Logost : Off	-		Liser -			04(31) 19 🕞
Dashboard		General > F	tod Settinge - Port Settings			
Status		Port Settings				
Switch LAN	*	In the second second				
Security	-			Port Settings		-
ACL						
GaS			Ports:	Mathing selected		F
General			ngress Default CoS:	a		1
			gress Remarking			
			- Remark CoS:	🔿 Enable 🛞 Disable		
			Remark DSCP / IP Precedence:	O DSCP O IP Precede	ence 🛞 Disable	
GoS Mappoor				Apply		
DSCF Mapping						
IP Precedence Mapping		Port	Ingress Default CoS	Remark Co5	Remark DSCP / IP Prec	Modify
Bandwidth		GE1	0	Disabled	Disabled	Ø
PoE		GE2	ů.	Disabled	Disabled	0
System Maintenance						
Diagnostics	-	GE3	u.	Disabled	Disableri	0
		GE4	0	Disabled	Disabled	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>	
АррІу	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	🕑 General > Gueue Sett	ngs > Queue Settings		
Status	Quaue Settings			
Switch LAN	- Gueve Settings			
Security	-	0	Queve Settings	
ACL	-			
005	Oueue	Schedule	Weight	% of WRR Bandwidth
Germal	1	Strict Priority OWRR	n	=
Propurties. Port Settings	2	Strict Priority O WRR	0	12
Queue Settings	а		D.	12
CoS Mapping	4	Strict Priority O WRR	0	-
DSCP Mapping	5	Strict Priority     O WRR	0	1
IP Precedence Mapping	6	Strict Priority D WRR	0	1
Bandwidth	7	Strict Priority O WRR	c	
PoE System Maintenance	. 8	Strict Priority O WRR	0	1
Diagnostics			Apply	

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 Logout : Off	4			04 14 10 🕞
Dashbuard		🕑 General > GoS Mapping > Gos Mapping		
Status		and the second se		
Switch LAN	. +	CoS Mapping		
Security	4		CoS to Queue Mapping (for Ingress)	
ACL	-	Class of Service	Queur	
Job	- 5	0	2	-
General		-	Ũ.	
Proportion		2	3	
Port Settings		з	4	
Oueue Settings		4	5	
		5	6	
DSCP Mupping		6	7	
IP Precedence Mapping		1	8	
Bandwidth			Quaue to CoS Mapping (for Egress Remarking)	
PoE		Queue	Class of Service	
System Maintenance	- 7	x	1	÷.
Diagnostics	1	2	0	
and the second s		3	2	T
		1		

Item	Description			
CoS to Queue Mapping (fo	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.         Values.				
Class of Service Define the class of service value (0 to 7).				
Apply	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 :	2	Uşer			04/36/12 🕞
Dashboard		Ganeral > DSCP Mapping > DSCP Mapping			
Status		The second se			
Switch LAN		DSCP Mapping			
Security				DSCP to Queue Mapping (for Ingress)	
ACL	÷.,	DSCP		Queue	
	5	Failing selected		1	
General	- 1	1 Tenuguit perceptor	_	-1	
Properties			Que	no to DSCP Mapping (for Egness Romarking)	10
Port Setting		Queue		DSCP	
Ouaue Settings		1		ū	
CoS Mapping		2		8	
		3		1lx	÷
IP Precedence Mapping		4		24	
Bandwidth		5		32 40	
PoE		6		40	
System Maintenance		8		56	
Diagnostics				(Apoly)	

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 value		
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 Lognat : Dit	-	Uper		04/06/04 🕞
Dashtioard	0	Seneral > IP Proceedom is Mapping = IP Proce	alamas Magning	
Status	-	Contract Name		
Switch LAN		mandence Mapping		
Security			IP Precedence to Queue Mapping (for Ingens)	-
ACL		IP Precedence	Queue	
MS		0	1	
General		1	2	
Propution		2	3	÷1
Port Setlings		3	4	•
Queue Settings		4	6	÷
CoS Mapping		5	6	
DSCP Mapping		6	7	+
		7	8	
Procedence Mapping	_		Queue to IP Precedence Mapping (for Egress Remarking	
Bandwidth				4
PoE		Oueve	IP Precedence	
System Maintenance	8	1	à	•
Diagnostics	-	.2	1	•
		3	2	•]
				1.0

Available settings are	explained as follows:
------------------------	-----------------------

Item	Description
IP Precedence to Queue N	lapping (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 N	apping (for Egress Remarking) - Settings for outgoing packets.
Queue	Display the queue ID (level 1 to 8) for different IP Precedence values.
IP Precedence	Define the IP Precedence value (0 to 7).
АррІу	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 : On					05.32-13 EF
Dashboard		Ingrase Rate Limit			
Status		Can be address of the second			
Switch LAN	-	A COLORADO		logress Rate Limit	
Security					
ACL	-	Ports:		Minning syningles	
0a5	3	State:		🔿 Enable 🛞 Disable	
General		Rate (Kbps):			(16-t000000), multiple of 16)
Elandwidth				Apply	
Egress Shaping Rate		Port	Rate Limit (Kbps)		Modify
Egress Shaping Per Que	ue	GEI	800		0
PoE	1	GE2	48		0
System Maintenance	÷	GER	64		0
Diagnostics	*	GE4	96		0
		GE5	128		0
		GE6	.144		ø
		GE7	608		0
		GEA	608		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.

Auto Logaut : Off	*			16 17 <i>0</i> 0	₽	
Dashboard		Bandwidth > Egress Sheeing Pate > I	Egrees Shaping Pate		-	
Status		Egress Shaping Rate				
Switch LAN	-	Câlese chebilă kate				
Security			Egress Shaping	Rate		
ACL	÷.					
	-	Ports:	Nothing selected			
General		State:	🔿 Enable 📀 Disabl	le		
Bandwidth		CIR (Kbps): (16-100000, malipio of 1				
ingress Rate Limit			Anoly			
Egress Shaping Rite						
Egress Shaping Per Que	Je	Port	CIR (Kbps)	Modity		
PoE	*	GEI				
System Maintenance			aff	0		
Diagnostics	+	GE2	aff	0		
		GE3	off	0		
		GE4	aff	ø		
		GE5	uff	0		
		GER	-mr	0		

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			15.18.06	₿			
Dashboard	O Ba	ndwidlin > Egress Shaping Par Queue +)	Eprese Skaping Par Ouece				
Status	-	s Shaping Per Queue					
Switch LAN	-	s onaping ner oleve					
Security	-		Egress Shaping Per Queue				
ACL	*						
	1	Port	GE1 -				
General		Queue:	- Select Queue ID -				
Bandwidth	1	State:	🔿 Enable 💿 Disable				
Ingress Rate Limir		CIR (Kbps):	(15 100000), multiple of 16)				
Egress Shaping Rote			Арриу				
Egross Shaping Per Quaue							
PoE	+						
System Maintenance	- Queue I	Information of Port GE1					
Diagnostics	Oueue	a ID	CIR (Kbps)	1.0			
	1		pπ				
	2		70				
	3		DT .				

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 PoE Configuration

VigorSwitch P2121 User's Guide

## **VI-1** Properties

This page allows a user to configure general settings for PoE and configure priority of each port for supplying PoE power. While maximum power budget is reached, power will be served starting with critical priority.

If the priority setting for all GE ports is configured as the same value (e.g., High); then, GE1 will have the highest priority to obtain PoE power in actual operation.

Auto Logout : Off	~				37:32:33	Ð
Dashboard		PoE > Properties > Properties				
Status		Properties				
Switch LAN	+	ropentes				-
Security	-		Properties			
ACL						
GoS		PoE Mode:	@ Auto 🔿 Manual 🔿 Disable			
	-					
Properties		Ports:	Nelwry sewaled			
Status		Enable:	Enoble			
Device Check			Low			
Schedule	_	Priority:		*		
System Maintenance	-					
Diagnostics	-		Apply			

Item	Description
PoE Mode	Disable - Disable the PoE function.
	Auto - Provides plug and play PoE function. PoE schedule and Power Limit are disabled in this mode.
	Manual - Before using PoE>>Schedule, set Manual as PoE mode.
Ports	Use the drop down list to select the port (GE1 to GE24) or ports for applying PoE configuration.
Enable	Enable - Make the selected ports be applied with PoE mode. Disable - Make the selected ports be not applied with PoE mode.
Priority	Select Priority for PoE device.
	Low -Set PoE device to low priority connection.
	High -Set PoE device to high priority connection.
	Critical - Set PoE device to highest priority connection.
Power Limit	This setting is available when Manual is selected as PoE Mode.
	Enter the value as the maximum limit of power given to each physical port.
Apply	Apply the settings to the switch.

## VI-2 Status

This page displays the current PoE status (configured in Properties, Device Check and Schedule) for each PoE port.

Auto Engout: DI	-								07 09 00 🕞
Dashboard		O POE	> Status - Status						
Status	$\overline{\sigma}$	Land							
Switch LAN	1	Status							
Security		GRet	mesh						
ACL	+	1							
QoS									
PoE		PoE Mod					Au	0	
Properties		Power Budget(VV) 120.0							
Siarus		Consuming Power(W) 0.0							
Device Check		Remaining Power(W) 120.0							
Schedule		SW Version 260							
System Maintenance									
Diagnostics	3	Port	Enable	Status	PD Class	Priority	Power Used (W)	Power Limit (W)	Power Cycle
		GE1	Enabled	No PD		Low	0	AT (30)	Apiply
		GE7	Enabled	No PD		Low	a	A7 (30)	Apoly
		GES	Enabled	No PD	-	Low	o	AT (30)	Apply
		GE4	Enabled	No PD		LOW	0	AT (30)	Appty

Item	Description
Refresh	Click it to refresh the status page.
PoE Mode	Display the PoE Mode (Manual, Auto or Disable) selected for the LAN port.
Power Budget(W)	Display the maximum power this switch can supply over PoE.
Consuming Power(W)	Display current power being consumed by all devices over PoE.
Remaining Power(W)	Display remaining power that can be supplied to additional devices over PoE.
Power Cycle	<b>Apply</b> - If PoE device connects to VigorSwitch, such button will be avaible for you to manually perform the <b>cold boot</b> for the PoE device by cycling the power supply.

## **VI-3 Device Check**

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

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

Auto Logout : Off	*		Davi						07 16 4B	÷
Dashboard		O Pat :	Desice Check + Desic	e Cherk						
Status	~	Direntari Ch								
Switch LAN		Linvian Ch								
Security.						Device Check	Ú.			
ACL										
QoS	•		Port:		GET			÷		
PNE	1		Enable:		C Fnable	② Disable				
Properties			Ping IP Address:		onnn			()PV4)		
Status			Interval Time (sec.	):	aut.			40		
Dreeve Lifnesh			Retry Time:		1.					
Schedule					100					
System Maintenance	- 4		Failure Action:		Power Cyc	le				
Diagnostics						Apply				
		Port	Enable	Ping	P Addr	Interval Times (s)	Retry Time	Failure Action	Failure Log	1.0
		GET	Disabled	0.0.0.	3	10	1	Power Cycle		
		GE2	Disablect	0.0.0.	0	10	4	Power Cycle		

Item	Description
Port	Use the drop down list to select the port (GE1 to GE24) or ports for device check.
Enable	<b>Disable</b> - No PoE function for the selected GE port. <b>Enable</b> - PoE function will be enabled for the selected GE port.
Ping IP Address	Enter the IP address of the PoE device for check.
Interval Time (sec.)	The ping check will be performed every 10, 30, 60 or 120 seconds for the selected port (PoE device).
Retry Time	The system will perform the ping check the selected port (PoE device) for 1, 3 or 5 times.
Failure Action	Specify the action performed for PoE device when there is no number of retry time of echo from given IP address.
	<b>Power Cycle</b> - Forcely reboot the device by cycling the power given to PoE device.
	Power Off - The PoE divice will be powered off.
	Nothing - Log this event only, no action is taken on PoE device.
Apply	Apply the settings to the switch.

## **VI-4 Schedule**

### VI-4-1 Schedule Profile

This page allows the network administrator to configure maximum 15 PoE schedule rules.

Auto Logout : 08 S		Tom							16/68/54	Gr
Dashboard		Schedule Profile Port Scheduling								
Status	-									
Switch LAN	4		3	ichedule Pr	ofile					
Security	3	Constanting of								
ACL.	-	Schedule Index:	0							
DoS	-	Enable:	🗇 Enable 🛞 Disable							
70E		Description:								
Properties		Start Date:	2000/01/01					×St		
Status		Start Time:	0	-	4	0		14		
Device Check		Duration Time:	0		:	0				
icheann)		Action:	Power On							
ystem Maintenance										
hiegnostics	-	How Often:	③ Once							
			🔿 Weekitays	Sun	Mon 3	Tue Wed	Thu S	Fri Sat		
			C Monthly, on date	1				-		
			Cycle duration: (days)	1						
			Ahr	6						

Available settings are expl	lained as follows:
-----------------------------	--------------------

Item	Description
Schedule Index	Use the drop down list (1 to 15) to choose one schedule profile.
Enable	<b>Disable</b> - The selected schedule profile will not take action but be saved for future use.
	Enable - The selected schedule profile will take action as configured.
Description	Enter a brief comment for such schedule.
Start Date	Specify the starting date of the schedule by choosing from a drop down calendar.
Start Time	Specify the starting time of the schedule by using the drop down list to specify the starting time (hours and minutes).
Duration Time	Define the time duration (hours and minutes).
Action	Specify which action should perform during the period of the schedule.
	Power On - PoE connection is always on.
	Power Off - PoE connection is always down.
How Often	Specify how often the schedule will be applied.
	Once - The schedule will be applied just once.
	Weekdays - Specify which days in one week should perform the schedule.
	Monthly, on date - Specify the day in a month as the starting point.
	Cycle duration (days) - The period of cycle duration is

	between 1 day and 31 days. For example, 7 means the whole cycle is 7 days; 20 means the whole cycle is 20 days. When the time is up, the PoE device will be turned on of off automatically.
Apply	Apply the settings to the switch.

### VI-4-2 Port Scheduling

This page allows the network administrator to specify the PoE port for applying the schedule. The configuration result for each port will be displayed on the table listed on the lower side of this web page.

Auto Lugout : 00 3		Tom			06,01.4	8 <b>G</b>
Dashboard	Sche	dule Profile Port Scheduling				
Status	-					
Switch LAN				Port Schudaling		1
Security						
NCL	-	Ports:	Southing bit	ikizi (d. 1	-+	
2oS	-	Schedule Index:	Nonie			
∿u±				Apply		
Properties						
Status						
Davice Check	Port		- 0	Schedule		
Spreadule	GE1			None		
System Maintenance	- GE2			None		
hagnostics	GE3			Npne		
	GE4			Novie		
	GES			None		
	GE6			None		
	GE7			None		
	GE8			None		
	GFR			Mona		

Item	Description
Ports	Select the port or ports for applying the schedule.
Schedule Index	Use the drop down list to choose the schedule profile (from 1 to 15). After clicking <b>Apply</b> , the selected port(s) will be applied with the specified schedule.
Apply	Apply the settings to the switch.

## Part VII System Maintenance

VigorSwitch P2121 User's Guide

## VII-1 TR-069

This device supports TR-069 standard. It is very convenient for an administrator to manage a TR-069 device (e.g., such switch) through an Auto Configuration Server, e.g., VigorACS.

Dashboard		System Manfamania - 19 (59) = 19 (59)	Sinting		
Status		TR-069 Softing			
Switch LAN	*	(House Solding			_
Security	•		ACS Settings		
ACL	-	TR-069:	🖸 Enable 🔿 Disable		
QoS		URL:	Entar OFL	Witzund	
PoE	- 1	Username:	Entre Usur Idamie		
	1		Sources of the second second		
		Password:	Enter Paeswora		
LLDP		Last Inform:	🔹 (N4)		
SNMP		Test Inform:	Test With Inform		
Access Manager			CPE Settings		
Time and Date		CPE Client:	ourn ourne		
Backop Manager		and the second second	© HITPS		
Upgrade Manager		URL:	https://192.168.1.222/80E9/cwm/CRN.html		
Firmware Information		Port:	8069	0 - 65535	
Account Manager		Username:	vigor		
Factory Default		Password:	Comme		8

Description
TR-069 - Click Enable to activate the settings on this page.
URL/Username/Password - Such data must be typed according to the ACS (Auto Configuration Server) you want to link. Please refer to Auto Configuration Server user's manual for detailed information.
Wizard - Click it to enter the IP address of VigorACS server, port number and the handler.
Last Inform - Display the time that VigorACS server made a response while receiving Inform message from switch last time.
Test Inform -Click Test With Inform to send a message based on the event code selection to test if such switch is able to communicate with VigorACS SI server.
The field lists the authentication information coming from VigorACS server.
<b>CPE Client</b> - Specify a protocol (HTTP/HTTPS)for authentication.
<b>Port</b> - Sometimes, port conflict might be occurred. To solve such problem, you might change port number for switch. The default number is 8069.
<b>Username / Password -</b> Type the username and password that VigorACS can use to access into such switch.
Periodic Inform Settings - The default setting is Disable. If enabled, please set interval time or schedule time for the Vigor switch to send notification to CPE. Or click Disable to close the mechanism of notification. Interval Time - Enter a value.

STUN Settings	STUN Settings -The default is Disable. If you click Enable, please type the relational settings listed below. Server Address - Enter the IP address of the STUN server.
	Server Port - Enter the port number of the STUN server.
	Minimum Keep Alive Period - If STUN is enabled, Vigor switch must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the minimum period. The default setting is "60 seconds".
	Maximum Keep Alive Period - If STUN is enabled, Vigor switch must send binding request to the server for the purpose of maintaining the binding in the Gateway. Please type a number as the maximum period. A value of "-1" indicates that no maximum period is specified. The default setting is "0 second".
АррІу	Apply the settings to the switch.
Clear	Remove current configuration.

## VII-2 LLDP

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

### **VII-2-1** Properties

ogout : Off 🛛 👻			04:04:49
nboard	LLDP > Properties > LLDP Global Setting		
tus	LLDP Global Setting		
vitch LAN	LLDP State:		
curity		Senable Obisable	(C 00707)
L	Transmission Interval:	30 🔹	(5-32767)
s	Holdtime Multiplier:	4	(2-10)
E	Reinitialization Delay:	2	(1-10)
	Transmit Delay:	2	(1-8191)
R-069	LLDP-MED Fast Start Repeat Count:	3	(1-10)
_DP	LLDP MED Network Policy for Voice Application:	✓ Auto	
		¥ 640	
LLDP Port Setting	Apply		
NMP			

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.
LLDP MED Network Policy for Voice Application	Auto - After checking the box, Vigor switch will create an LLDP MED network policy for voice application (e.g, voice signaling, guest voice, softphone voice and etc.,) based on the voice VLAN, automatically.

### VII-2-2 LLDP Port Setting

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

Auto Logout : 🖉 🦉				04 10 28 🕞
Dashboard	O LLOP > LLD	P Port Setting + LLDP Port Settie	ng	
Status				
Switch LAN	LLOP Port Setti	ng		
Security	· •	orts:	Vidpling selected	
ACL		itate:	Detable	(41)
005		optional TLVs:	Mathing converted	
PoE				
		LAN:	(fothing selected	0
TR-069			Арру	
LLOP				
Properties	Port	State	Selected Optional TLVs Selected VLAN	Modify
	GE1	TX&RX	System Name, Port Descripti	0
LI DP Local Dovero	GE2	TX8RX	System Name, Port Descripti	0
LLDP MED Notwork Policy	GE3	TX8RX	System Name, Port Descripti	0
LLDP MED Fort Sollings	GE4	TX&RX	System Name, Port Descripti	0
LLDP Remote Device	GES	TX&RX	System Name, Port Descript	0
LLDP Overlanding	GE6	TX&RX	System Name, Port Descripti	0
SNMP	GE7	TXERX	System Name, Port Descripti	0

Available settings are explained as follows:

Item	Description
Ports	Use the drop down list to select the port (GE1 to GE28) or ports for device check.
State	Disable - Disable the transmission of LLDP PDUs. TX&RX - Transmit and receive LLDP PDUs both. TX Only - Transmit LLDP PDUs only. RX Only - Receive LLDP PDUs only.
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.

### VII-2-3 LLDP Local Device

Amo Logom : 🛛 Off 👘 💌			14 12 56 🕞	þ.
Dashboard	O LLDP -> LLDP Local Device -> LLDP L	ocal Device		
Status -	LLDP Logal Dower			
Switch LAN -	TIDe Logic Dower			_
Security		Device Summary		
ACL -	Name	Value		
QoS -		MAC Ad		
PoE -	Chassis ID		A:08:01:01	
	System Name	P2121		
TR-069	System Description		0/100/1000BaseT + 4-Port 100M/1000M Combo SFP L2 Switch	
LLDP	Capabilities Supported	Bridge		
Properties.	Capabilities Enabled	Bridge		
LLDP Port Setting	Port ID Subtype	Interfaci	2 name	
		Port Details		
LLDP MED Network Policy	1 m m			
LLDP MED Port Settings	Port	LLDP State	Detail	
LLDP Remote Device	GEI	TXSRX	0	
LDP Overlanding	GE2	TXSRX	0	
SNMP	GEB	TX&RX	0	

This page displays information for LLDP Local Device.

Item	Description				
Device Summary	Display a summary of the LLDP information for this switch.				
	<b>Chassis ID Subtype -</b> 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).				

### VII-2-4 MED Network Policy

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

Auto Logout : 05	-	User					04/16:32	€
Dashboard	O LIDP > LIDP M	El/Notwark Palicy > ME	D Network Policy					
Status	- MED Network Policy							
Switch LAN	- Meter Network Poscy							
Security				MED Network Pr	alicy			
ACL								
QoS	- Policy II	):	1					
PoE	- Enable i	Policy:	💿 Enable 🔘	Disable				
	Applicat	lon:	Voice Signali	ig				
TR-069	VLAN:					(1-4094)		
LLOP	VLAN TO		⊚ Untag ⊙1	au .		- 1 - 1 - 1 - 1		
Propertues	Priority:			-9				
LLDP Part Setting			-					
LLDP Local Device	DSCP:		0	-				
				Apply				
LLDP MED Port Settings								
LLDP Remote Device	Policy ID	Policy Enabled	Application	VLAN ID	Tagged/Untag	Priority	DSCP	17
LLDP Overlauding	ŕ.	Disabled	Unknown	0	Untanged	U	Q	
SNMP	1	Disabled	Unknown	0	Untanged	0	0	

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.

### VII-2-5 LLDP MED Port Settings

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

Auto Lagout : Off 🛛 💌	User		04:26:23
Dashboard	ILTP = 110P MED Port Settings = Port Contro	u/Satton	
Status	Pint Control/Soltings		
Switch LAN	Con compactoring		
Security	<u>k</u>	Part Control/Settings	
ACL			
QoS	Ports:	Nothing selected: -	
PeE	State:	✓ Enable	
System Monororo	Available Optional TLV:	Selected Optional TLV:	
18-069	Locaten	>> Notwork Policy	
LLOP	Inventory		
Ploperties		6	
LLDP Port Setting		ec	
(10P Local Dovice		1 million and 1	
LLDP MED Midwark Policy	Selected Network Policies:	Mathing Islation	
	Location TLV Settings:		
LLDP Remote Device	Coordinate	(16 pairs of hexadecimal characters)	
LLDP Overloading	Civic	(E - 150 pairs of hexadecimal characters)	
SNMP	JCS FUN	and the second	~

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. Coordinate -Enter the coordinate location in 16 pairs of hexadecimal characters. Civic - 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.

### VII-2-6 LLDP Remote Device

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

Auto Logout : DI	14			Uper											Gŧ
Dashboard		O LLOP >L	LDP	Remote Device = L	LDP	Remote Device									
Status		LLDP Remote	i.												
Switch LAN		LEDI- Hemon	e Dev	ce	-			_			_		_		
Security		Local Port	iii.	Chassis ID S	n	Chassis ID	Port ID Subtype	Port	0	System Name	10	Time to Live	.0	Details	Delete
ACL		GE12		MAC address		00 10 AA 11 2	Locally assigned	gi76		P2280		98		0	0
205															-
PoE															
System Multitlevatics	1														
TR-069															
LLDP															
Properties															
LLDP Port Setting															
LLDP Local Device															
LLDP MED Nelwork Polic	y.														
LLDP MED Port Settings															
LLDP Overloading															
SNMP															

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

### VII-2-7 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	~								04/28/21
Dashboard		O LLDP	> LLDP Overloading	> LLOP Port Setting					
Status		Concession in the							
Switch LAN	-	LLDP Per	Setting		_				
Security	-	Port	Total(Bytes)	Left to Send(	Status	Mandatory TLVs	802.3 TLVs	Optional TLVs	802.1 TLVs
ACL		GE1	68	1420	Not Overloading	21(Transmitted)	11(Transmitted)	9(Transmitted)	8(Transmitted)
QoS		GE2	68	1420	Not Overloading	21(Transmitted)	11(Transmitted)	9(Transmitted)	B(Transmitted)
PoE		GES	68	1420	Not Overloading	21(Transmitted)	11(Transmitted)	9(Transmitted)	6(Transmitted)
	3	GE4	68	1420	Not Overloading	21(Transmitted)	11(Transmitted)	9(Transmitted)	8(Transmitted)
TR-069		GE5	68	1420	Not Overloading	21(Transmitted)	11(Transmitted)	9(Transmitted)	8(Transmitted)
LLDP		GE6	68	1420	Not Overloading	21(Transmitted)	11(Transmitted)	9(Transmitted)	8(Transmitted)
Properties		GE7	68	1420	Not Overloading	21(Transmitted)	11(Transmitted)	9(Transmitted)	8(Transmitted)
LLDP Port Setting		GE8	68	1420	Not Overloading	21(Transmitted)	11(Transmitted)	9(Transmitted)	8(Transmitted)
LLDP Local Davice		GE9	68	1420	Not Overloading	21(Transmitted)	11(Transmitted)	9(Transmitted)	8(Transmitted)
LLDP MED Network Polic	Y.	GE10	69	1419	Not Overloading	27( transmitted)	11(Transmitted)	9(Transmitted)	8(Transmitted)
LLDP MED Part Settings		GE11	69	1419	Not Overloading	22(Transmitted)	11(Transmitted)	9(Transmitted)	B(Transmitted)
LLDP Remote Dovice		GE12	69	1419	Not Overloading	22(Transmitted)	11(Transmitted)	9(Transmitted)	B(Transmitted)
LLDP Overloading									
SNMP									

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

# VII-3 SNMP

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

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

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

An SNMP-managed network consists of three key components:

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

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

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

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

### VII-3-1 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.

Auro Logout : Off 🔗	User			14-29:00 Eb	
TR-069	STRUP > Varw > Varw				
LIDP	Manw				_
SNMP			SNMP View		
Minut	-	_	onthic states		
	and the second second				
Continuinity	View Name:				
	OID Subtree:				
Engine (D	Type:	⊙ Included ○ Ex	cluded		
Trup Evont			add		
Notification					
Access Manager					
Time and Date	View	OID Subtree	Туре	1 Delete	
Backup Manager	ali	Y	Included		
Upgrade Manager					
Firmware Information					
Account Manager					
Factory Default					
Reboot Switch					

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.
Apply	Apply the settings to the switch.

### VII-3-2 Group

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

Auto Logout : Dt. 🔗	User	04	4 30:23	Ð
TR-069	SURVE > Laurup > Group			
SNMP	Group	SIMP Group		_
Voor Farannoody User Engine ICS Fagit Event	Group Name: Version: Security Level: Road View	© SNMPv1 © SNMPv2 © SNMPv3 • No Security Authentication Authentication and Privacy © Enabled all		
Rotification Access Manager Time and Date Backup Manager	Write View Notify View	Enable •== Enable •== (Antr)	4	
Upgrade Manager Firmwere Information Account Manager Factory Default Reboot Switch	Group Name Version	Security Level View (Read) View (Write) View (Notify) No data available in table	(H)	Edit

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	P - Click it to modify the settings for the selected group.



click it to remove the selected group.

## VII-3-3 Community

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

Auto Logoot : 06 🛛 👻				04:32:00
TR-069	$\bigodot SNMe \Rightarrow Commandy \Rightarrow SNMe Commandy$			
LLDP	SNMP Community			
SNMP				
Vinv	Community Name:	Enjor Lanerriendy Manie		
Smap	Туре:	🛞 Basic 📋 Advanced		
	View:	all		1.0
	Access Right:	Read Only		
Engine (D	Group:	Littung sources		
Trap Errol		And		
Notrication				
Access Manager	Community Name Group	View	Access Right	Delete
Time and Date	public	au	Read & Write	0
Backup Manager	Personal Providence		11000 0 11000	
Upgrade Manager				
Firmware Information				
Account Manager				
Factory Default				
Reboot Switch				

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.

#### VII-3-4 User

This page allows a user to configure SNMP user profile.

Auto Logout : Off 🛛 💌			04-35-42 🕞
TR-069	SHAP > Unit > Group		
LLDP	Group		
SNMP			
		SNMP Groun	
Formunity	Group Name:		
	Version:	© SNMPv1 © SNMPv2 ○ SNMPv3	
	Security Level:	- No Security Authentication Authentication and Privacy	
Trap Even	Read View	- Enabled Sil	÷.
Notification	Write View	Enable 👘	+
Access Manager	Notify View	Enable all	100
Time and Date	houry view		
Backup Manager		40	
Upgrade Manage			101 A 34 3
Firmware information	Group Name Version	Security Level View (Read) View (Write) View	(Notify) Edit
Account Manager		No dats available in table	
Factory Default			
Reboat Switch			

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.
Version	Choose one of the SNMP versions.
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.
Read View/Write View / Notify View	Read View - The default setting is Enabled. Use the drop down list to specify a user account.
Add	Click it to add a new user profile.
Edit	- click it to modify the settings for the selected profile.
	click it to remove the selected entry.

sion: OSNMPv1 OSNMPv2 OS	⊙ SNMPv3
rity Level: 🔿 No Auth 🔿 Auth 💿 Auth	th & Privacy
ew:	
Read all -	
✓ Write all -	
Notify all -	

## VII-3-5 Engine ID

#### VII-3-5-1 Local Engine ID

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

Auto Logout : 🛛 🖉				04:42:30	G
Dashboard	SNME > Empror D > Local Engine II.				
Status -	Local Engine ID Remote Engine ID				
Switch LAN -	Remote Engine ID				
Security -		Local Engine ID			
ACL -					
QoS -	Engine ID:	🐷 User Defined			
PoE -		80006 x9203001 d x x000000	(10 - 64 hexadecimal characters)		
System Maintenança	5	Apply			
TR-069					
LLOP					
SNMP					
View					
Gmup					
Community					
Mary					
Trop Exam					
Netrinalium				_	

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.
АррІу	Apply the settings to the switch.

#### VII-3-5-2 Remote Engine ID

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

Auto Logoul : Dil	3	Ťim		16:30:23 🕞
Dashboard		Local Engine ID Remote Engine ID		
Status	*		1010	
Switch LAN			SHMP Unor	
Security				
ACL		Address Type:	Hostname C IPv4 C IPv6	
QoS		Server Address:		
PoE		Engine ID:	(10 - 64 nézadécima) characters)	
System Managemente	4		(Add)	
LLDP				
SNMP		Server Address	Engine ID Edit	
		172.16.8.2	B0006a9203001dua112244	
			•	
disar.				
Trap 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> </ul> Edit SNMP Engine ID for <ul> <li>IP=172.16.8.2</li> </ul> Engine ID: <ul> <li>80006a9203001daa1</li> <li>(10-64 pairs of hex char)</li> </ul>			

### VII-3-6 Trap Event

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

Auto Logout : 0f	~				114 47 38 🕒
Dashboard	0	SNMP + Trap Event + Trap Event			
Status					
Switch LAN	+	p Event			
Security	- 1			Trap Event	
ACL	-				
QoS	-	Authentication Failure:	Enable Enable		
PaE	-	Link Up / Down:	🔄 Enable		
System Manderone (	-	Cold Start:	🔄 Enable		
18-069		Warm Start:	🔄 Enable		
LLDP				Apply	
SNMP					
Vany					
Community					
Engine 10					
Trop Berni					
Nethinalian					

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.

### VII-3-7 Notification

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

Auto Lugout : 🖓 💡	User					04:40147	Ge
TR-069	SNMP = Notification = Notification						
LLOP	Mitlification						
SNMP			Notification	ik.			
Yiew							
Յուսը	Address Type:	🔿 Hostname 🔅	IPv1 O IPv6				
Community	Server Address:						
Úter	Version:	⊚ SNMPv1 ⊖ S	NMPv2 O SNMP	-2			
Engran ID				v.			
Trap Event	Type:	Trap Information	m				
Neblication	Community/user	public					
Access Manager	Security Level:	- No Security	Authentication	Authentication and	Privacy		
Time and Date	Server Port:	Use Default	162		(1-65535, default 162)		
Backup Manager	Timeout:	Use Default	15		séc (1 - 300, default 15)		
Upgrade Manager	Retry:	Use Default	з		(1 + 255, default 3)		
Firmware Information			Aild		1. ment control of		
Account Manager			Cond.				
Factory Default							
Report Switch	Index Server Addre Server	ort Timeout	Retry V	ersion Type	Commnuicati S	acuirty Level	Edit

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	<ul> <li>Specify Notification Type.</li> <li>Trap -Send SNMP traps to the host.</li> <li>Inform - Send SNMP informs to the host. If it is used, Timeout and Retry also shall be defined.</li> </ul>
Community/user	Use the drop down list to choose one of the community profiles.
Security Level	Specify SNMP security level for SNMP notification packet. It is available when SNMPv3 is selected. No Security - No authentication. Authentication - Authentication without encryption will be performed for packets. Authentication and Privacy - Authentication with encryption will be performed for packets.
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 automaticallty.			
Add	Click it to create a new notification profile.			
Edit	Click it to modify the settings for the selected server profile.			
	😨 - Click it to remove the selected entry.			
	Edit Notification Entry for			
	Server IP=192.168.1.1			
	Version: O SNMPv1 O SNMPv2 O SNMPv3			
	Type: <ul> <li>Trap O Inform</li> </ul>			
	Community/user _			
	Security Level: <ul> <li>No Security  </li></ul> <li>Auth  </li> <li>Privacy</li>			
	Server Port: Vise Default 162 (1-65535)			
	Timeout: Use Default sec (1-300)			
	Retry: Use Default (1-255)			
	OK Cancel			

# VII-4 Access Manager

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

Auto Logout : 🛛 🖓	*			04/61/14 🕞
Dashboard		O System Montenance + Access Menager + Ac	2007	
Status	-	Access		
Switch LAN	-	ACCESS		
Security			Access Settings	
ACL	-			
065		HTTP Service:	💿 Enable 🔘 Disable	
PoE		IITTPS Service:	⊗ Enable ⊖ Disable	
System Ministerio		Telnet Service:	③ Enable 〇 Disable	
18-069		SSII Service:	Enable      Disable	
LLDP			Apply: )	
SNMP				
Webess Manager				
Time and Date				
Backup Manager				
Upgrado Monager				
Firmware Information				
Account Manager				
Factory Default				

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. <b>Disabled</b> - Click it for not accessing telnet service. <b>Enabled</b> - Click it to access telnet service.
SSH Service	Enabled - Enable SSH service.
АррІу	Apply the settings to the switch.

# VII-5 Time and Date

### VII-5-1 System Time Zone

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

Auto Logout : Off			04/64/02 🕞
Dashboard	O System Mentenance > Time and Date > System	ern Time Zone	
Status -	System Time Zone Time		
Switch LAN -	System time zone		
Security -		System Time Zone Setting	
ACL -	Time Zone:	Select Time Zone	~
0o5 -	Daylight Saving Time:	Disable	348
PoE		(Apply)	. 12 2000
System Managemen		5.9443 ·	
TR 069		System Time Zone Informations	14
LLDP	Current Date/Time	04:53:54 (UTC+8) Jan. 12 2000	
SNMP	Time zone	uTC+8	
Access Manager	Dayiight Saving Time	Disabled	
Time and Date			
Backup Manager			
Upgrade Manager			
Firmware Information			
Account Manager			
Factory Default			

Item	Description
System Time Zone Setting	
Time Zone	Use the drop down menu to select a time zone that VigorSwitch is located.
Daylight Saving Time	Select the mode of daylight saving time. Disable -Disable daylight saving time.
	Recurring - Using recurring mode of daylight saving time.
	Non-Recurring - Using non-recurring mode of daylight saving time.
	<b>USA</b> -Using daylight saving time in the United States that starts on the second Sunday of March and ends on the first Sunday of November.
	<b>European</b> - Using daylight saving time in the Europe that starts on the last Sunday.
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 Non-Recurring is selected as Daylight

	Saving Time.
	From - Specify the starting time of non-recurring daylight saving time.
	To - Specify the ending time of recurring daylight saving time.
АррІу	Apply the settings to the switch.
System Time Zone Informations	Display the status of system time zone.

## VII-5-2 Time

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

Auto Engout : 00	~	Usar		04:55:32 <b>G</b> +
Dashboard		O System Maintenance + Time and Date + Time		
Status		System Time Zone		
Switch LAN	-	Party and a second s	11 . 11 . 11 . 11	
Security	-	Manual Time:	and the second sec	Minutes Seconds
ACL	-		algor ison is	23 AV
QoS	-	Enable SNTP:	⊙ Enable ○ Disable	
PaE	- 2	SNTP/NTP Server Address:	peol.ntp.org (X.X.	.X.X or Hostname)
System Maintenante		Server Part:	123 2 (1-6	65535   Default : 123 )
TR-069				
LLDP		Apply		
SNMP				
Access Manager				
Time and pate				
Backup Manager				
Upgrade Manager				
Fornware Information				
Account Manager				
Factory Default				

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.

# VII-6 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.

Aato Logant : 200	-	User			04.58,06 G+
Dashboard		System Muniterance > Backup Manage	• - Harkup Manapot		
Status		Constant and the second second			
Switch LAN		Backup Managac			
Security	-	Backup Method:	TFTP	*	
ACL	-	Server IP:	Bolin Suran (6)		(IPv4 or IPv6 Address)
QoS	-	Backup Type:	Configuration		
PoE	.÷		Apply		
System Moleconce	1				
TR-069					
LLDP					
SNMP					
Access Manager					
Time and Date					
Boolarge Manager					
Upgrade Manager					
Firmware Information					
Account Manager					
Factory Default					

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.
АррІу	Apply the settings to the switch.

# VII-7 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 : Of	*			Ö4:59.19	Ð
Dashboard		🔘 Syciem Mantenance - Upgrade Menore	r - Uppratie Maaager		
Status		Upgrade Manager			
Switch LAN	-	and the second se			
Security		Upgrade Method:	нгр		
ACL		File/Path:	<b>谢贤</b> 未递择框架。		
QoS		Upgrade Type:	(a) Image (Configuration)		
PoE			Apply		
	- 1				
18-069					
LLDP-					
SNMP					
Access Manager					
Time and Date					
Backup Manager					
Upglade Nanagér					
Firmware Information					
Account Manager					
Factory Default					

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.

# **VII-8 Firmware Information**

Auto Engout - Citi		User			050053 🕞
Dashboard	O System	Maintenance - Firmware Information - Fir	mware information)		
Status	-	The second s			
Switch LAN	Firmware I	normation			
Security.		Active Image:	Firmware 1		
CL			Apply		
loS	1.0		Firmware 1 Infom	-	_
PoE			r innware 1 mjorn	nation	
VETOM MERNENDALE	Mode	Active	Version	Build Time	Size (MB)
TR-069	Attive	v.	232	2018-05-28 19 10:25	6778867
LLOP	1		Firmware 2 inform	nation	
SNMP	64				
Access Manager	Mode	Active	Version	Build Time	Size (MB)
Time and Date	Backup		2.3.2	2018-05-28 (9)10:25	6770067
Backup Manager					
Upgrade Manager					
Account Manager					
Factory Default					

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.
Apply	Apply the settings to the switch.
Firmware 1 Information Firmware 2 Information	<ul> <li>Mode - Display the mode (Active or Backup) of the firmware.</li> <li>Active -Display the status (in use or not) of the firmware.</li> <li>Version - Display the switch version.</li> <li>Build Time - Display the built time of the firmware.</li> <li>Size (MB) - Display the size of the firmware.</li> </ul>

# VII-9 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.

Auto Logoni : Dit 🖉	User			0503	6 🕞
QuS	. System Mantenance > Account Ma	naget a Local Caer Information			
PeE	Local User Information				
System Maintenance					_
TR-069	-		Account		
UDPI	User Name:	Entra Aver Na	mē		
SNMP	Password:	The second second			
Ancess Manager		Enter Prospens			
Time and Date	Retype Password:	Enter Flassen	rd		
Backup Mariager	Privilege Lovel:	Admin		4	
Upgrade Manager			avpauly		
Firmware Information			Local Usiero		
Armuni Manane		10 T.		11.12	
Factory Detaolt	User Name	Password Type	Privilege Type	Modify	
Reboot Switch	admin	Encrypted	Admin	0	
Diagnostics	user	Encrypted	Admin	00	

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.
АррІу	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: aki	×
: :	Password:	
	Retype Password:	
	PrivilegeType:	
	Admin	•
	OK Cancel	
	EINTYDICU au	

# **VII-10 Factory Default**

Click Apply to return to factory default settings for VigorSwitch.



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

# **VII-11 Reboot Switch**

Auto Logout : C#	Man -	06/06/53
Dashboard	System Mantenance > Rebitol Setch > Reback Setch	
Status	Contraction of the local division of the loc	
Switch LAN	Reboot Switch	
Security	- Change	
ACL		
QeS	*	
PoE		
System Maintenance -		
TR-069		
UDP		
SNMP		
Access Manager		
Time and Date		
Backup Manager		
Upgrade Manager		
Firmware Information		
Account Manager		
Factory Default		

Click Apply to reboot VigorSwitch with current settings.

This page is left blank.

# Part VIII Diagnostics

VigorSwitch P2121 User's Guide

# **VIII-1 Cable Diagnostics**

Auto Logoui : 08	-			05:07:00
Dashboard	O Hay	numbers - « Galder Disagramities - »	Chypner Reyl	
Status	-			
Switch LAN	Copper	1961		
Security	-		Copper Test	24
ACL	-			
QoS	-	Port:	GE1, GE2, GE3, GE4, GE5, GE6, GE7, GE8, GE9, GE10, GE11, GE12	-
PoE	-		C Start	
System Maintenance				
Diagnostice	Port		Result	
Cible Disgnation	GET		FAIL	
Ping Test	GE2		FAIL	
Systog	GE3		FAIL	
	GE4		FAIL	
	GE5		FAIL	
	Port		FAIL	
	GEB		FAIL	
	GEO		PASS	
			PAR .	

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.

# VIII-2 Ping Test

Auto Logoul : 08	-				⊜
Dashboard		O Diagnostics - Ping Test - Ping Test			
Status	-	Prog Total			
Switch LAN		Pariti rea			_
Security	-		Ping Test		
ACL	-				
QoS	-	Protocol:	iPy4	<u>)</u>	
PoE	-	Host:	192.160.1.1	(IPv/I eddress or hostname)	
System Maintenance	-	Count:	4	📮 (1 – b).	
	-	Interval (sec):	1	S (1-5)	
Cable Diagnostics			Start OStop		
Ring Test			Garan Garab		
SysLog		PINC 192.168.1.1 (192.168.1.1): SG data 64 bytes from 192.100.1.1: stmp peart 0 64 bytes from 192.168.1.1: stmp peart 0 64 bytes from 192.168.1.1: stmp peart 0 64 bytes from 192.168.1.1: stmp peard 0 192.160.1.1 ping statistics 4 packets remultired, 4 packets rearing cound-trip min/way/mas - 0.0/2.5/10.0 m [Process is finished]	Liez5 time+0.0 mi Liez5 time+0.0 mi Liez55 time+0.0 mi Liez55 time+0.0 mi rd, 0\ putter lina		

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.		

# VIII-3 SysLog

### VIII-3-1 SysLog Explorer

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

Auto Logout : 🛛 🖉	1	User		05:10:53			
Dashboard		System > System Explorer > System Explorer	0				
Status	-	SysLog Explorer					
Switch LAN	-	charob extroner					
Security			SysLog Filter				
ACL							
QoS		Source:	Volatio Memory				
PoE		Severity:	Netmingselactae	<u>i</u>			
System Maintenance	+	Category:	Nothing equated	14			
			(Vine)				
Cable Diagnostics							
Ping Test							
SysLog		Source	Volable Memory				
	1	Seventy	emerg, alert, cnt, error, warning, notice, info, d	lebug			
SysLog Settings		Category	AAA, ACL, AUTHMGR, CABLE_DIAG, DAI, DH	CP_SNDOPING, GVRP, IGMP_SNOOPING,			
		Total Entries	115				
			SysLog Message				
		BRafresh Clear All	ech O Clear All				

Item	Description
Source	<ul> <li>Volatile Memory - Explore the logs contained in volatile memory (also known as RAM).</li> <li>Non-Volatile Memory - Explore the logs contained in non-volatile memory (also known as Flash).</li> </ul>
Severity	Select severity (emerg, alert, crit, error, warning, notice, info and debug) of log messages which you wish to filter out for review.
Category	Select the categories (related features) of logs you wish to review. Category contains AAA, ACL, AUTHMGR, CABLE_DIAG, DAI, DHCP_SNOOPING, GVRP, IGMP_SNOOPING, IPSG, L2, LLDP, Mac-based VLAN, Mirror, MLD_SNOOPING, Platform, PM, Port, PORT_SECURITY, QoS, Rate, SNMP, STP, Security suite, System, Surveillance VLAN, Trunk, UDLD and VLAN.
View	Click it to display logs based on the settings configured above.
Refresh	Click it to refresh the log.
Clear All	Clear it to remove all logs displayed in this page.

### VIII-3-2 SysLog Settings

#### VIII-3-2-1 SysLog Service

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

Auto Logout : Of	-	User		15-16-19 🕞
Dashboard		🕑 Systog > Systog Settings > Systog Setin	e )	
Status		Contraction of Contraction of Contraction	SysLog	
Switch LAN		SysLog Service Local SysLog Remote	2 Aaroğ	
Security	7	SysLog Service:	🕑 Enable 🔘 Disable	
ACL		Apply		
QoS				
PoE				
System Maintenance	4			
Cable Diagnostics				
Ping Test				
SysLog				
SysLog Explorer				
SkeLog 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.

#### VIII-3-2-2 Local SysLog

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

Auto Logout : Off.		User						05:19:27	₽
Dashboard		System > System Bettings > Los	sal SynLog						
Status	-	Synton Service Count Syntage	Remain Syste						
Switch LAN		SAlaroli Slawija	Hamilto Synco						
Security				Lincal Syst	Log Settings				
ACL									
QoS	-	Source:		Multury enjoyiest					
PoE		Severity:		emerg					
System Maintenance	2			Apply					
Cable Diagnostics									
Ping Test		Source	Status		Severity	11	Delete		
SysLog		Volatile Memory	enabled		emerg, aiert, crit, error, warning, not	ice	0		
Sys.Log Explorer									
Siva Log Settings									
	-								

Item	Description	
Source	Volatile Memory - 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.	

#### VIII-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 : Off	v		Own			05,22,00
Dashboard		😧 SysLeg = SysLog Se	lings + Demote SysLog			
Status		Environmental Inc.				
Switch LAN		SysLog Service Loc	al SysLog Remote S	À 2170Ĥ		
Security				Remote SysLog S	lettings	
ACL						
QoS	-	Server Ad	dress:	172,15-0.0		
PoE	+	Server Po	re:	514		(1 - 65535)
System Maintenance		Severity:		emerg		4
Duquéntici	7	Facility:		local0		
Cable Diagnostics		, senig				
Ping Test				Apply		
SysLog						
SynLog Explorer		Server IP(Port)	Status	Severity	Facility	Delete
SynLog Setting)		172,16,8.8(514)	enabled	emerg	local0	0

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.			

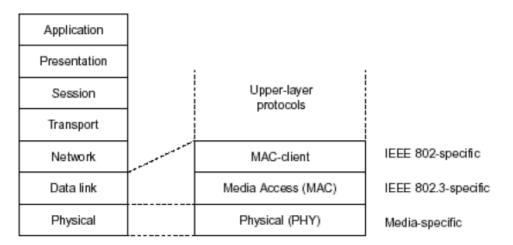
This page is left blank.

# **Appendix: Reference**

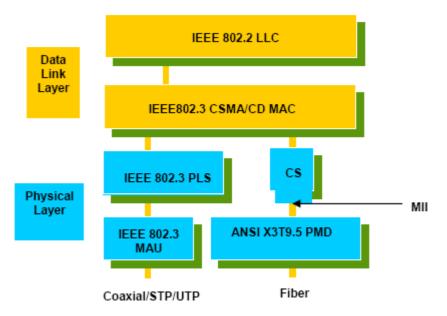
This chapter will tell you the basic concept of features to manage this switch and how they work.

## 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.

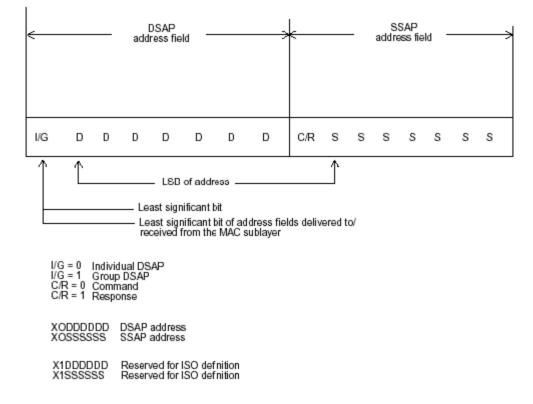
Logical link control supports the interface between the Ethernet MAC and upper layers in the protocol stack, usually Network layer, which is nothing to do with the nature of the LAN. So it can operate over other different LAN technology such as Token Ring, FDDI and so on. Likewise, for the interface 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		SAP dress	Control	Information		
	8 bits	8	bits	8 or 16 bits	M*8 bits		
SS/	AP address AP address htrol	= =	Source Control sequent	service access field [16 bits for	ess point address field point address field formats that include and 8 bits for formats tha		
Info	rmation	=	Information field				
*		=	Multiplication				
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 gueue 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.

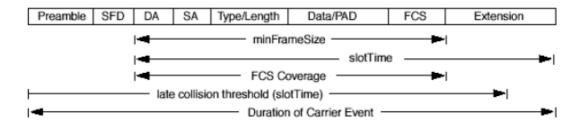
As the transmission of a MAC frame with the half-duplex operation exists only in the same collision domain, the carrier signal needs to spend time to travel to reach the targeted device. For two most-distant devices in the same collision domain, when one sends the frame first, and the second sends the 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*
4				64 bytes				•

Parameter value/LAN	10Base	100Base	1000Base	
Max. collision domain DTE to DTE	domain DTE to		100 meters for UTP	
		412 meters for fiber	316 meters for 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	License Information, 31, 32, 37, 53,	54, 80, 81, 90
Account Manager, 184, 185		Limiting Rate, 113	
1	В		Р
Deslaur Manager 192	D	PoE Configuration, 151	
Backup Manager, 182		Preamble, 112	
Bandwidth, 148	<u> </u>	Properties, 114	
	С		Q
CoS Mapping, 145			¥.
	D	QoS Configuration, 129, 140	_
Dashboard, 22, 23			S
Diagnostics, 189		Security, 94	
DoS, 114		SNMP, 167	
DoS Port Setting, 116		SNMP Community, 171, 172, 174	
DoS Protection, 116		Storm Control, 113	
	D	Storm Control, 95, 97, 98, 100, 103,	109, 111, 112
	Ε	Storm Control, 117	
Egress Shaping Per Queue, 150		Storm Control, 120	
Egress Shaping Rate, 149		Storm Control, 125	
	F	Stric Priority Queue, 144	
Factory Default, 187		System Configuration, 25	
	G	System Maintenance, 157	
	G		U
General, 130, 133, 139, 141		Unanda Managan 192	U
General Setup, 26		Upgrade Manager, 183	
	Ι		W
Ingress Rate Limit, 148		Weight, 144	
Installation for VigorAPM, 6		WRR Bandwidth, 144	
	L		
License Agreement, 29			