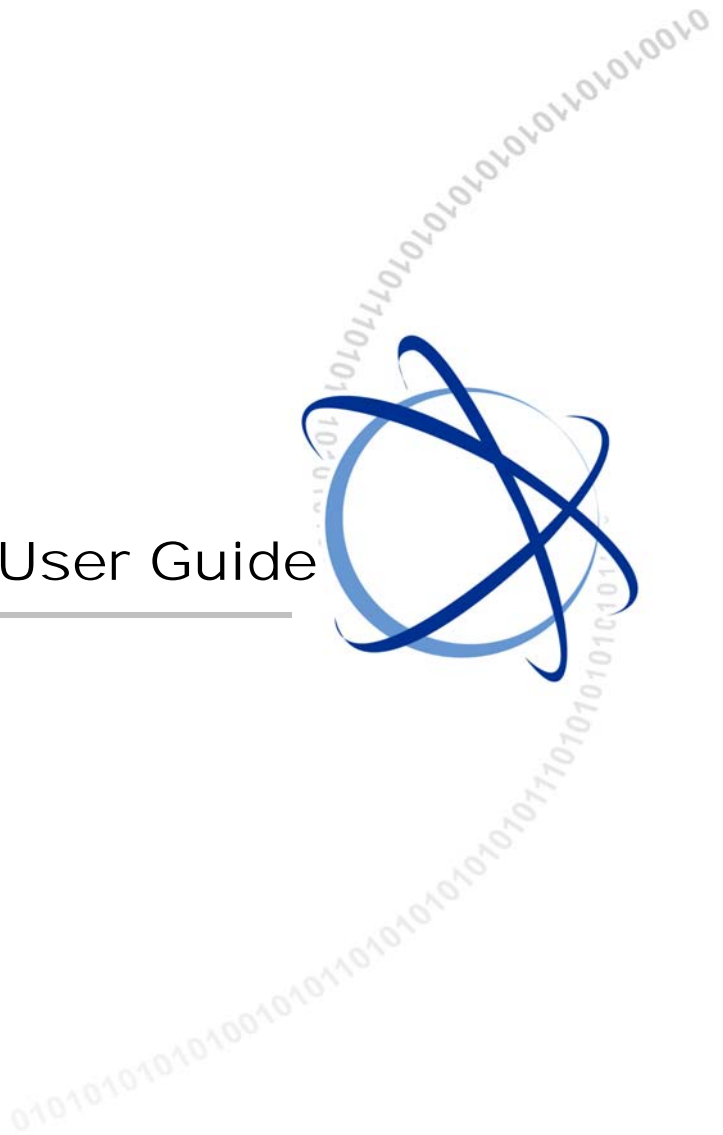


OfficeServ 7400
GPLIM(GPLIMT) User Guide



COPYRIGHT

This manual is proprietary to SAMSUNG Electronics Co., Ltd. and is protected by copyright. No information contained herein may be copied, translated, transcribed or duplicated for any commercial purposes or disclosed to third parties in any form without the prior written consent of SAMSUNG Electronics Co., Ltd.

TRADEMARKS

Enterprise IP Solutions

OfficeServ™ is a trademark of SAMSUNG Electronics Co., Ltd.

WINDOWS 95/98/XP/2000 are trademarks of Microsoft Corporation.

This manual should be read before the installation and operation, and the operator should correctly install and operate the product by using this manual.

This manual may be changed for the system improvement, standardization and other technical reasons without prior notice.

For further information on the updated manual or have a question for the content of manual, contact the address or homepage below.

**Address: Document Center 2nd Floor IT Center. Dong-Suwon P.O. Box 105, 416, Maetan-3dong
Yeongtong-gu, Suwon-si, Gyeonggi-do, Korea 442-600**

Homepage: <http://www.samsungdocs.com>

© 2005~2007 SAMSUNG Electronics Co., Ltd. All rights reserved.



INTRODUCTION

Purpose

This document introduces the OfficeServ 7400 GPLIM(GPLIMT), an application software of OfficeServ 7400, and describes procedures on installing and using the software.

Document Content and Organization

This document consists of three chapters and abbreviation, which are summarized as follows:

CHAPTER 1. Overview of OfficeServ 7400 GPLIM(GPLIMT)

This chapter briefly introduces the OfficeServ 7400 GPLIM(GPLIMT).

CHAPTER 2. Installing OfficeServ 7400 GPLIM(GPLIMT)

This chapter describes the installation procedure and login procedure.

CHAPTER 3. Using OfficeServ 7400 GPLIM(GPLIMT)

This chapter describes how to use the menus of the OfficeServ 7400 GPLIM(GPLIMT).

ABBREVIATIONS

Abbreviations frequently used in this document are described.

Conventions

The following types of paragraphs contain special information that must be carefully read and thoroughly understood. Such information may or may not be enclosed in a rectangular box, separating it from the main text, but is always preceded by an icon and/or a bold title.



WARNING

Provides information or instructions that the reader should follow in order to avoid personal injury or fatality.



CAUTION

Provides information or instructions that the reader should follow in order to avoid a service failure or damage to the system.



CHECKPOINT

Provides the operator with checkpoints for stable system operation.



NOTE

Indicates additional information as a reference.

Console Screen Output

- The lined box with 'Courier New' font will be used to distinguish between the main content and console output screen text.
- '**Bold Courier New**' font will indicate the value entered by the operator on the console screen.

References

OfficeServ 7400 System Description

OfficeServ 7400 System Description introduces OfficeServ 7400 and describes the system information necessary for the understanding of this system, such as hardware configuration, specification, and functions.

OfficeServ 7400 Installation Manual

OfficeServ 7400 Installation Manual describes the conditions necessary for the installation of the system and how to inspect and operate the system.

OfficeServ 7400 Service Manual

OfficeServ 7400 Service Manual describes the instruction and specification of the system, the configuration and features of each hardware circuit, troubleshooting for the system, and the programming method for the system maintenance.

OfficeServ 7400 Programming Manual

OfficeServ 7400 Programming Manual describes how to use Man Machine Communication(MMC) for the modification of system setup.

Revision History

EDITION	DATE OF ISSUE	REMARKS
00	11. 2005.	Original Draft
01	02. 2006.	Second Edition
02	11. 2006.	<ul style="list-style-type: none"> - Descriptions of GPLIMT are added. - 'Ping' utility is modified. - 'Nway Force' field of 'Port Configuration' is added. - Setting Web Time-out of 'Admin Config' is added.
03	04. 2007	<ul style="list-style-type: none"> - Port is changed into MISC UI. - Description about the port VID input value is changed. - The figure and description of the Layer2 menu are changed. - Port Aggregation UI and its description are changed. - GVRP UI and its description are changed. - IGMP Snooping UI and its description are changed. - Authentication figure and its description are changed. - PoE figure and its description are changed. - Admin Config UI is changed. - Time Config UI is changed. - Upgrade UI is changed. - The descriptions about the SNMP functions are changed. - The description about the RMON functions is changed.



This page is intentionally left blank.



SAFETY CONCERNS

For product safety and correct operation, the following information must be given to the operator/user and shall be read before the installation and operation.

Symbols



Caution

Indication of a general caution.



Restriction

Indication for prohibiting an action for a product.



Instruction

Indication for commanding a specifically required action.



CAUTION



When Protecting Overload Caused by PoE Log Activation

When all items are set to On or Enable, system overload may occur. Use the setting only when logs are left. If not, set to Disable.



When Changing DB

If DB is changed in OfficeServ 7400 GPLIM(GPLIMT), the system restarts.



When Activating Server Authentication

Login Policy should be applied first to activate the server authentication to the system. If entering the authentication information in the status that the Logging Policy is only selected without application, the information is not applied to the server authentication information.



When Deleting Internet Temporary Files

If GPLIM(GPLIMT) package is upgraded, Internet temporary files should be deleted. Select **[Internet Explorer] → [Tools] → [Internet Options]** menu and click the **[Delete Cookies]** and the **[Delete Files]** buttons in **[Internet Temporary Files]** area. If these files is not deleted, the webscreen of GPLIM(GPLIMT) may not be normally displayed.



TABLE OF CONTENTS

INTRODUCTION	I
Purpose	I
Document Content and Organization.....	I
Conventions	II
Console Screen Output.....	II
References	III
Revision History	IV
SAFETY CONCERNS	VI
Symbols	VI
Caution	VII
CHAPTER 1. Overview of OfficeServ 7400 GPLIM(GPLIMT)	1
Introduction to OfficeServ 7400	1
Introduction to OfficeServ 7400 GPLIM(GPLIMT)	1
CHAPTER 2. Installation of OfficeServ 7400 GPLIM(GPLIMT)	1
Installing.....	1
Getting Started.....	1
CHAPTER 3. Use of OfficeServ 7400 GPLIM(GPLIMT)	1
Port	1
Port	1
VLAN	1
MAC.....	1
Layer2.....	1

RSTP	1
Port Aggregation	1
GVRP	1
IGMP Snooping	1
Authentication	1
Application	1
VoIP Service	1
PoE	1
PoE	1
System	1
Network	1
DB Config	1
Admin Config	1
Log	1
Time Config	1
Upgrade	1
Appl Server	1
Reboot	1
Utility	1
Management	1
SNMP	1
RMON	1
ABBREVIATION	1
A ~ L	1
M ~ V	1



CHAPTER 1. Overview of OfficeServ 7400 GPLIM(GPLIMT)

This chapter introduces OfficeServ 7400 system and OfficeServ 7400 GPLIM(GPLIMT).

Introduction to OfficeServ 7400

OfficeServ 7400 is the most proper communication product for mid/large-sized offices and provides the complex function including voice, data and internet functions. OfficeServ 7400, also, provides the data exchange function using data network as well as the voice call function. Users can enjoy various phone functions and applications at the various platforms such as digital phones, IP phones, mobile phones, PCs and servers.

OfficeServ 7400 is configured with a chassis mounted on a 19-inch rack, extension terminal, wireless LAN device, and application software. With a commercial server with a Linux platform outside the chassis, the OfficeServ 7400 system provides the following application software:

- OfficeServ IP-UMS
- OfficeServ Admin(OfficeServ Operator and CTI)
- OfficeServ Solution(System Manager, Web Management, PCMMC and OfficeServ EasySet)

Gigabit PoE LAN Interface Module(GPLIM) provides the ethernet related functions by interworking with a call server or a OfficeServ IP-UMS. This document describes the functions and the method of OfficeServ 7400 GPLIM(GPLIMT)



NOTE

Structure of OfficeServ 7400

For the information on the structure, features, or specifications of the OfficeServ 7400, refer to 'OfficeServ 7400 System Description'.

Introduction to OfficeServ 7400 GPLIM(GPLIMT)

OfficeServ 7400 provides the following functions via GPLIM(GPLIMT) based on IP:

Ethernet Switch Function

- Fast Ethernet L2 switch module(compatible with IEEE 802.3)
- Managed switch function by using an access interface for LAN
- Twelve 10-BASE-T/100-BASE-TX Ethernet ports: LAN interface between terminal devices
- Two Gigabit Ethernet ports: uplink LAN interface
- Support of multicasting relay(IGMP snooping function)
- Learning bridge function by the spanning-tree algorithm
- Virtual LAN(VLAN) function
 - VLAN based on ports
 - VLAN based on tags
 - VLAN based on protocols
 - VLAN based on MAC addresses
- Uplink fail over function by 4-port/3-group port trunk
- Layer 2 frame priority function by 802.1p
- 802.3x layer 2 flow control
- Network Access Control function based on ports by 802.1x

Power Of Ethernet (PoE) Function

- Power supply function via ethernet cable without additional power source.
- Managed function in accordance with ports.
- Function to confirm the status of the current and to restrict the supply of the current.
- Enable/disable function for supplying power.

Management Function

- Advanced debugging function via telnet connection
- Configuration and verification functions for the operations of GPLIM(GPLIMT) functional block via a browser
- Configuration and verification functions for the operations of GPLIM(GPLIMT) functional block via the Simple Network Management Protocol(SNMP)
- 4-Real-time Monitoring(4RMON) function
- Program upgrade
 - Program upgrade via TFTP
 - Program upgrade via HTTP
 - Program upgrade via Local manager's PC



This page is intentionally left blank.



CHAPTER 2. Installation of OfficeServ 7400 GPLIM(GPLIMT)

This chapter describes the installation and the login procedure for OfficeServ 7400 GPLIM(GPLIMT).

Installing

Since software package is included in the OfficeServ 7400 GPLIM(GPLIMT), additional installation of software is not required. The GPLIM(GPLIMT) software package is composed of items described below:

Package	File	Description
Bootrom Package	gplim-bootldr.img-vx.xx	Boot ROM program
	gplim-bootldr.img-vx.xx.sum	
Main Package	gplim-pkg-vx.xx.tgz	Upgrade package for HTTP
	gplim-os..img-vx.xx	'os' partition upgrade package for TFTP
	gplim-firmware.img-vx.xx	'Firmware' partition upgrade package for TFTP
	gplim-configdb.img-vx.xx	'configdb' partition upgrade package for TFTP
	gplim-logdb.img-vx.xx	'logdb' partition upgrade package for TFTP
	gplim-flash.img-vx.xx gplim-flash.img-vx.xx.sum	Fusing file for the flash memory



NOTE

Software Package Configuration

Each package has a separate file for checking checksum, and x.xx represents the version.

Configure the environment as follows to access GPLIM(GPLIMT).

- 1.** Mount the GPLIM(GPLIMT) board on a slot of OfficeServ 7400.
- 2.** Connect a PC to a certain port in the GPLIM(GPLIMT) board.
- 3.** Run the Internet Explorer from the PC and access the initial IP(10.0.4.1) of GPLIM(GPLIMT). The IP initial value of the GPLIM(GPLIMT) board is set to 10.0.4.1/24.



Caution for the Use of a Web Browser

The version of the Internet Explorer should be 6.0 or higher for the maintenance of GPLIM(GPLIMT). Other web browsers are not supported.

Getting Started

The start procedure of OfficeServ 7400 GPLIM(GPLIMT) is as follows:

1. Run the Internet Explorer and enter the GPLIM(GPLIMT) IP address in the address input field to connect to GPLIM(GPLIMT). The login window shown below will appear.

SAMSUNG

Enterprise IP Solutions

OfficeServ 7400

OfficeServ 7400 is enterprise IP solutions made by Samsung Electronics. It provides integrated solutions for you.

✉️ 🖨️ 📞 📱

🔒 Login

ID

Password

Save Your ID?

[Forget Your ID & Password?](#)

Copyright © 2003 Samsung Electronics Co., Ltd. V1.0

- Log in using the administrator ID and password. The following window will appear. GPLIM(GPLIMT) menus are displayed on the upper part of the screens. Select each menu to display its submenus on the left section of the screen. For more detailed method for each menu, refer to ‘Chapter 3. Using OfficeServ 7400 GPLIM(GPLIMT)’ of this manual.

Port Configuration

Port	Active	Negotiation	Spd/Dplx	Flow Ctrl	Rate(%) In/Out	Security	Priority
All	<input type="checkbox"/>						
1	<input checked="" type="checkbox"/>	Auto	100	Full	0 0	<input type="checkbox"/>	Off
2	<input checked="" type="checkbox"/>	Auto	100	Full	0 0	<input type="checkbox"/>	Off
3	<input checked="" type="checkbox"/>	Auto	100	Full	0 0	<input type="checkbox"/>	Off
4	<input checked="" type="checkbox"/>	Auto	100	Full	0 0	<input type="checkbox"/>	Off
5	<input checked="" type="checkbox"/>	Auto	100	Full	0 0	<input type="checkbox"/>	Off
6	<input checked="" type="checkbox"/>	Auto	100	Full	0 0	<input type="checkbox"/>	Off
7	<input checked="" type="checkbox"/>	Auto	100	Full	0 0	<input type="checkbox"/>	Off
8	<input checked="" type="checkbox"/>	Auto	100	Full	0 0	<input type="checkbox"/>	Off
9	<input checked="" type="checkbox"/>	Auto	100	Full	0 0	<input type="checkbox"/>	Off
10	<input checked="" type="checkbox"/>	Auto	100	Full	0 0	<input type="checkbox"/>	Off
11	<input checked="" type="checkbox"/>	Auto	100	Full	0 0	<input type="checkbox"/>	Off
12	<input checked="" type="checkbox"/>	Auto	100	Full	0 0	<input type="checkbox"/>	Off
13	<input checked="" type="checkbox"/>	Auto	1000	Full	0 0	<input type="checkbox"/>	Off
14	<input checked="" type="checkbox"/>	Auto	1000	Full	0 0	<input type="checkbox"/>	Off

OK Reset

Save Configuration

- Click the **[Logout]** button on the upper section of the screen to close the connection to the GPLIM(GPLIMT).



This page is intentionally left blank.



CHAPTER 3. Use of OfficeServ 7400 GPLIM(GPLIMT)

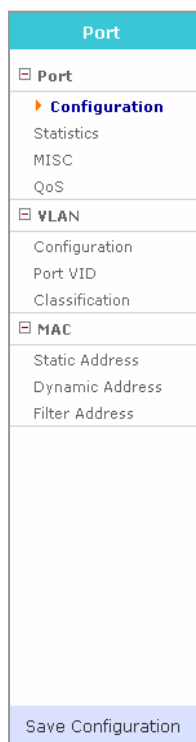
This chapter describes the menus of OfficeServ 7400 GPLIM(GPLIMT).

The menus of OfficeServ 7400 GPLIM(GPLIMT) are configured as shown to below:

Port	Layer2	Application	PoE	System	Management
<ul style="list-style-type: none"> ▣ Port <ul style="list-style-type: none"> ▸ Configuration Statistics MISC QoS ▣ VLAN <ul style="list-style-type: none"> Configuration Port VID Classification ▣ MAC <ul style="list-style-type: none"> Static Address Dynamic Address Filter Address 	<ul style="list-style-type: none"> ▣ RSTP <ul style="list-style-type: none"> ▸ Configuration Status Port Trunking ▣ GVRP <ul style="list-style-type: none"> Configuration Status ▣ IGMP Snooping <ul style="list-style-type: none"> Time Interval Function Forwarding Table Management ▣ Authentication <ul style="list-style-type: none"> Configuration Management 	<ul style="list-style-type: none"> ▣ VoIP Service <ul style="list-style-type: none"> ▸ Configuration 	<ul style="list-style-type: none"> ▸ Global <ul style="list-style-type: none"> Configuration Power Status Port Status Management Log 	<ul style="list-style-type: none"> Network DB Config Admin Config ▣ Log <ul style="list-style-type: none"> Configuration Report Download ▣ Time Config <ul style="list-style-type: none"> NTP Config Manual Config Timezone Upgrade Appl Server Reboot ▣ Utility <ul style="list-style-type: none"> Ping 	<ul style="list-style-type: none"> ▣ SNMP ▸ Configuration <ul style="list-style-type: none"> Status Management ▣ RMON <ul style="list-style-type: none"> Configuration Status Management
Save Configuration	Save Configuration	Save Configuration	Save Configuration	Save Configuration	Save Configuration

Port

Select the **[Port]** menu of GPLIM(GPLIMT) to display the submenus of Port on the left of the window as follows:



Menu	Submenu	Description
Port	Configuration	Sets the environment of switch port.
	Statistics	Displays the information and statistics on the transmission method, link status and speed.
	MISC	Displays the mirroring function and other functions for switch.
	QoS	Prioritizes by packets led into switch, or prioritizes to a specific port by force to process QoS.
VLAN	Configuration	Configures Virtual LAN (VLAN).
	Port VID	Sets the Port VID to set the process method for untagged packets when the VLAN mode is 'Tag-based VLAN'.
	Classification	Sets the VLAN based on Protocol or MAC.

(Continued)

Menu	Submenu	Description
MAC	Static Address	Stores a MAC address to the static address table.
	Dynamic Address	Retrieves a floating address table or deletes a MAC address arbitrarily.
	Filter Address	Enters a MAC address and sets to filter the frame data that has the same MAC address information with the entered value in the switch.
Save Config	-	Stores the configured information to operate in the value currently entered, or modifies all configuration values to the initial values.

Port

The user can set the functions for the ports and retrieves the information on the ports in the **[Port]** menu.

Configuration

This table allows the user to set the configuration of the switch ports in the **[Port] → [Configuration]** menu.

Port Configuration									
Port	Active	Negotiation	Spd/Dpx		Flow Ctrl	Rate(%) In/Out		Security	Priority
All	<input type="checkbox"/>				<input type="checkbox"/>			<input type="checkbox"/>	
1	<input checked="" type="checkbox"/>	Auto	100	Full	<input checked="" type="checkbox"/>	0	0	<input type="checkbox"/>	Off
2	<input checked="" type="checkbox"/>	Auto	100	Full	<input checked="" type="checkbox"/>	0	0	<input type="checkbox"/>	Off
3	<input checked="" type="checkbox"/>	Auto	100	Full	<input checked="" type="checkbox"/>	0	0	<input type="checkbox"/>	Off
4	<input checked="" type="checkbox"/>	Auto	100	Full	<input checked="" type="checkbox"/>	0	0	<input type="checkbox"/>	Off
5	<input checked="" type="checkbox"/>	Auto	100	Full	<input checked="" type="checkbox"/>	0	0	<input type="checkbox"/>	Off
6	<input checked="" type="checkbox"/>	Auto	100	Full	<input checked="" type="checkbox"/>	0	0	<input type="checkbox"/>	Off
7	<input checked="" type="checkbox"/>	Auto	100	Full	<input checked="" type="checkbox"/>	0	0	<input type="checkbox"/>	Off
8	<input checked="" type="checkbox"/>	Auto	100	Full	<input checked="" type="checkbox"/>	0	0	<input type="checkbox"/>	Off
9	<input checked="" type="checkbox"/>	Auto	100	Full	<input checked="" type="checkbox"/>	0	0	<input type="checkbox"/>	Off
10	<input checked="" type="checkbox"/>	Auto	100	Full	<input checked="" type="checkbox"/>	0	0	<input type="checkbox"/>	Off
11	<input checked="" type="checkbox"/>	Auto	100	Full	<input checked="" type="checkbox"/>	0	0	<input type="checkbox"/>	Off
12	<input checked="" type="checkbox"/>	Auto	100	Full	<input checked="" type="checkbox"/>	0	0	<input type="checkbox"/>	Off
13	<input checked="" type="checkbox"/>	Auto	1000	Full	<input checked="" type="checkbox"/>	0	0	<input type="checkbox"/>	Off
14	<input checked="" type="checkbox"/>	Auto	1000	Full	<input checked="" type="checkbox"/>	0	0	<input type="checkbox"/>	Off

Item	Description
Port	There are 14 switch ports. All ports can be processed at once through the 'All' item.
Active	Sets whether to use a port or not.
Negotiation	<ul style="list-style-type: none"> - Auto: Adjusts the speed through a negotiation with the counterparty. - Force: Sets the speed without a negotiation with the counterparty. Set the negotiation item as 'Force' If setting the Duplex item as 'Full'.
Speed/Dpx	<ul style="list-style-type: none"> - Speed: Select the speed as 10/100 Mbps. For Port 13 and 14, it is available to set as 1000 Mbps. - Duplex(Dpx): Select Set Full(two-way service) or Half(one-way service). For 1000bps, it is only available to select 'FULL'.
Flow Ctl	Sets whether to use the function for flow control. The flow control is processed according to the value set at Rate(%) In/Out(Entry rate/Exit rate).
Rate(%) In/Out	Controls the flow by setting the entry rate and exit rate by ports. The unit is the rate(%) of the port speed. If the function of flow control is not used(The item of Flow Ctl is not checked), the value is set as '0'.
Security	Sets whether to allow updating the MAC address table. The source MAC address is not updated at the switch port where the 'Security' item is not checked. Therefore, no terminal connects to the port. If entering the Static MAC address of a specific value to the switch port where 'Security' is checked, normal service is provided to the terminal having the entered MAC address. Therefore, the security service is provided by the method that a terminal, which is not allowed,(a terminal having a MAC address not entered to the Static MAC address) is not used.
Priority	<p>If set as 'Low' or 'High', the priority is set as 'Low' or 'High' regardless of the configuration value of QoS bit for the packet entered to the relevant port.</p> <p>It is available to set Priority when the QoS mode is not First Come First Service (FCFS) in the [Port] → [QoS] menu.</p>

Statistics

The user can retrieve the link status and statistics for each port of the switch in the [Port] → [Statistics] menu. The number of the statistics item is the cumulative value from the start of the system to the current status. Click the [Refresh] button to update this window. If clicking the [Reset] button, all the values of the statistics is initialized to '0'.

Statistics								
Port	Link	Input Packets	Input Dropped	Input Errors	Output Packets	Output Dropped	Output Errors	Collisions
Port1	On	49990	18340	0	2478	0	0	0
Port2	Off	0	0	0	0	0	0	0
Port3	Off	0	0	0	0	0	0	0
Port4	Off	0	0	0	0	0	0	0
Port5	Off	0	0	0	0	0	0	0
Port6	Off	0	0	0	0	0	0	0
Port7	Off	0	0	0	0	0	0	0
Port8	Off	0	0	0	0	0	0	0
Port9	Off	0	0	0	0	0	0	0
Port10	Off	0	0	0	0	0	0	0
Port11	Off	0	0	0	0	0	0	0
Port12	Off	0	0	0	0	0	0	0
Port13	Off	0	0	0	0	0	0	0
Port14	Off	0	0	0	0	0	0	0

- Input Packets: Number of packets received to the port
- Input Dropped: Number of packets that are received to the port but dropped without successfully being switched
- Input Errors: Number of packets that are received to the port but an error occurs
- Output Packets: Number of packets are transmitted to the port
- Output Dropped: Number of packets that are transmitted to the port but dropped as it is not switched successfully
- Output Errors: Number of packets that are transmitted to the port but an error occurs
- Collisions: Number of times that a collision occurs between a packet received to the port and a packet transmitted with being switched

MISC

The user can set the mirroring function and other functions for switch in the [Port] → [MISC] menu.

Mirroring Configuration

Port Mirroring Configuration	
Mode	Off
Monitoring Port	Port1
Monitored Port	<input type="checkbox"/> VLAN 1 <input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 13 <input type="checkbox"/> VLAN 2 <input type="checkbox"/> 7 <input type="checkbox"/> 8 <input type="checkbox"/> 9 <input type="checkbox"/> 10 <input type="checkbox"/> 11 <input type="checkbox"/> 12 <input type="checkbox"/> 14

Miscellaneous Configuration

Miscellaneous Configuration	
MAC Age-out Time (300-765)	300 sec
Broadcast Storm Filter Mode	5%
Auto MDI / MDIX	on

Item	Description
Mode	Sets whether to use the mirroring function. - Off: Mirroring function not used - Receive: Mirroring for incoming packets - Transmit: Mirroring for outgoing packets - Both: Mirroring for incoming/outgoing packets
Monitoring Port	Assigns a port for monitoring. Generally, it means a connection port of a PC for monitoring.
Monitored Port	Assigns a port where the monitoring is performed. It means to assign a port where the port to be monitored connects. It is not available to set the same port with the monitoring port.
MAC Age-Out Time	Sets the duration that the MAC address where 'Learning' (MAC address is updated) is performed remains in the address table of a switch. The default is 300 seconds. If the connection for the LAN port is released, the MAC address where the learning function is performed is deleted immediately. If connecting the LAN port again, the learning function is performed for new MAC address and the MAC address is renewed immediately.

(Continued)

Item	Description
Broadcast Storm Filter Mode	The overall buffer volume of a switch is set among 5, 10, 15, 20 and 25 %. If this value is exceeded, the broadcast packet is to be lost.
Auto MDI/MDIX	Operated by sensing the direct/cross cable automatically. The user can stop this function by setting to 'Off', if necessary.

QoS

In the [Port] → [QoS] menu, the user can process by prioritizing according to packets incoming to the switch, or prioritizing a specific port by force.

QoS Configuration

QoS Configuration	
QoS Mode	Weighted Round Robin
Weight (High/Low)	2 / 1
Delay Bound / Max Delay Time (1-255)	Off / 255
High Priority Levels	<input type="checkbox"/> Level0 <input type="checkbox"/> Level1 <input type="checkbox"/> Level2 <input type="checkbox"/> Level3 <input checked="" type="checkbox"/> Level4 <input checked="" type="checkbox"/> Level5 <input checked="" type="checkbox"/> Level6 <input checked="" type="checkbox"/> Level7

OK

Item	Description
QoS Mode	<p>Select the QoS mode.</p> <ul style="list-style-type: none"> - First Come First Service: Packet is transmitted according to the incoming order.(QoS function not used) - All High before Low: Method that a packet that has higher priority is transmitted prior to a packet that has lower priority than that packet. A packet is not transferred until the packets that are higher priorities than the packet are all transmitted. - Weighted Round Robin: Method to transmit packets in the rate that high priority packets and low priority packets are configured at an established rate(Weight). For example, if setting High Weight to '5' and Low Weight to '2', the five high priority packets are transmitted before the two priority packets are transmitted.
Weight	Sets the rate of High weight and Low weight when the method of 'Weighted Round Robin' is used.

(Continued)

Item	Description
Delay Bound/ Max Delay Time	Sets the time limit to prevent the low priority packets from being delayed too much when the QoS mode is selected as 'All High before Low' or 'Weighted Round Robin'. The unit of 'Max Delay Time' is ms(1/1000 second) and the default is 255 ms. If a low priority packet is not switched even though the established time is exceeded, the packet is processed preferentially.
High Priority Levels	There are 8 tags to indicate the priority. So, Level 0~Level 7 does not indicate the actual value of the priority and it is set as a level having higher value has the priority against a level of a lower value. As GPLIM(GPLIMT) processes the priority by separating only by two Queues, 'High' and 'Low'.

VLAN

This menu is used to configure Virtual Local Area Network(VLAN).

Configuration

Select [VLAN] → [Configuration] to display the window that can configure VLAN.

VLAN Configuration

VLAN Operation Mode

Mode 802.1Q(1VL) ▾

VLAN Name	VLAN ID

Select	VLAN ID	VLAN Name	VLAN Members (Untagged / Tagged)
<input type="checkbox"/>	1	default	<input checked="" type="checkbox"/> 1 <input checked="" type="checkbox"/> 2 <input checked="" type="checkbox"/> 3 <input checked="" type="checkbox"/> 4 <input checked="" type="checkbox"/> 5 <input checked="" type="checkbox"/> 6 <input checked="" type="checkbox"/> 13 <input checked="" type="checkbox"/> 7 <input checked="" type="checkbox"/> 8 <input checked="" type="checkbox"/> 9 <input checked="" type="checkbox"/> 10 <input checked="" type="checkbox"/> 11 <input checked="" type="checkbox"/> 12 <input checked="" type="checkbox"/> 14

Select VLAN from 'Mode'. VLAN mode is classified into four types as follows and VLAN configuration method depends on a VLAN mode.

- 802.1Q (IVL) Tag Base VLAN
- MAC Based VLAN
- Port Based VLAN
- 802.1Q(SVL) Tag Base VLAN

Enter VLAN name and ID to add a VLAN and click the [**Add**] button. Check the target VLAN and click the [**Delete**] button to delete the VLAN.

802.1Q (IVL)

If a packet includes tag information when VLAN is decided for the packet sent via a specific port(the corresponding port belongs to various VLANs), VLAN can be decided by using the tag information. If a packet does not include tag information, a VLAN is decided by using the Port VLAN ID(PVID) information, and the packet is sent to only the corresponding VLAN. In case of a packet that includes tag information, VLAN is decided by using the Tag Control Information(TCI) of the 2 layer protocol.

Tag Based VLAN is composed of tagged member and untagged member and the members are processed according to the case. When a tagged packet is received from a specific port of the switch, a network device that can process 802.1Q standard may not be connected. Thus, convert the received tagged packet to a normal packet and sent the packet.

Select '802.1Q(IVL)' from VLAN Operation Mode of the <VLAN Configuration> window and select the corresponding VLAN. Enter VLAN Name and VLAN ID and click the [Add] button to display the window below. Select the corresponding ports from VLAN Untagged Members and VLAN Tagged Members and click the [OK] button.

VLAN Configuration

VLAN Operation Mode

Mode 802.1Q(IVL) ▾

VLAN Name	VLAN ID

Select	VLAN ID	VLAN Name	VLAN Members (Untagged / Tagged)																									
			P1		P2		P3		P4		P5		P6		P7		P8		P9		P10		P11		P12		P13	
<input type="radio"/>	1	default	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="radio"/>	2	VLAN0002	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="radio"/>	3	v3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

- VLAN Untagged Members: Select a port that will send the Ethernet frame that deletes TCI information when a port is switched and data is sent ranging from 1 to 14 ports. Connect to a terminal that does not support IEEE 802.1Q to configure tagged VLAN.
- VLAN Tagged Members: Select a port that will send the TCI information by saving the information when a port is switched and data is sent ranging from 1 to 14 ports. Connect to the port that selects a terminal that supports IEEE 802.1Q.

MAC Based VLAN

VLAN is configured for each MAC address. VLAN is configured without information on port and the number of a VLAN member may change. Up to 256 MAC members can be saved either in a single VLAN or in multiple VLANs.

Since a MAC Based VLAN does not basically contain port information, the port serves as a VLAN member by receiving packets. Thus, the ARP packet must be transmitted to the switch to enable members of a VLAN to exchange packets.

Select 'MAC' from VLAN Operation Mode of the <**VLAN Configuration**> screen. Select the corresponding VLAN and enter VLAN Name and VLAN ID and click the [Add] button to display the following screen. Enter the MAC address into [Classification] menu.

VLAN Configuration

VLAN Operation Mode

Mode MAC ▼

VLAN Name	VLAN ID

Select	VLAN ID	VLAN Name	VLAN Members (Untagged / Tagged)													
<input type="radio"/>	1	default	<input checked="" type="checkbox"/> P1	<input checked="" type="checkbox"/> P2	<input checked="" type="checkbox"/> P3	<input checked="" type="checkbox"/> P4	<input checked="" type="checkbox"/> P5	<input checked="" type="checkbox"/> P6	<input checked="" type="checkbox"/> P7	<input checked="" type="checkbox"/> P8	<input checked="" type="checkbox"/> P9	<input checked="" type="checkbox"/> P10	<input checked="" type="checkbox"/> P11	<input checked="" type="checkbox"/> P12	<input checked="" type="checkbox"/> P13	<input checked="" type="checkbox"/> P14
<input type="radio"/>	2	V2	<input type="checkbox"/> P1	<input type="checkbox"/> P2	<input type="checkbox"/> P3	<input type="checkbox"/> P4	<input type="checkbox"/> P5	<input type="checkbox"/> P6	<input type="checkbox"/> P7	<input type="checkbox"/> P8	<input type="checkbox"/> P9	<input type="checkbox"/> P10	<input type="checkbox"/> P11	<input type="checkbox"/> P12	<input type="checkbox"/> P13	<input type="checkbox"/> P14

Port Based VLAN

This option is used to configure VLAN on port basis. A single port can be assigned to multiple VLANs. In such cases, broadcast packets transmitted by the port is transmitted to all VLANs containing the port. Ports not assigned to any VLANs serve as a single VLAN.

Select 'Port' from VLAN Operation Mode of the <VLAN Configuration> screen. Select the corresponding VLAN and enter VLAN Name and VLAN ID and click the [Add] button to display the following screen. Select the corresponding port from VLAN Members and click the [OK] button.

VLAN Configuration

VLAN Operation Mode

Mode: PORT

VLAN Name:

VLAN ID:

Select	VLAN ID	VLAN Name	VLAN Members (Untagged / Tagged)													
<input type="radio"/>	1	default	<input checked="" type="checkbox"/> P1	<input checked="" type="checkbox"/> P2	<input checked="" type="checkbox"/> P3	<input checked="" type="checkbox"/> P4	<input checked="" type="checkbox"/> P5	<input checked="" type="checkbox"/> P6	<input checked="" type="checkbox"/> P7	<input checked="" type="checkbox"/> P8	<input checked="" type="checkbox"/> P9	<input checked="" type="checkbox"/> P10	<input checked="" type="checkbox"/> P11	<input checked="" type="checkbox"/> P12	<input checked="" type="checkbox"/> P13	<input checked="" type="checkbox"/> P14
<input type="radio"/>	2	V2	<input type="checkbox"/> P1	<input type="checkbox"/> P2	<input type="checkbox"/> P3	<input type="checkbox"/> P4	<input type="checkbox"/> P5	<input type="checkbox"/> P6	<input type="checkbox"/> P7	<input type="checkbox"/> P8	<input type="checkbox"/> P9	<input type="checkbox"/> P10	<input type="checkbox"/> P11	<input type="checkbox"/> P12	<input type="checkbox"/> P13	<input type="checkbox"/> P14

802.1Q (SVL)

802.1Q(SVL) can be set and operate with the same method as 802.1Q(IVL).

- IVL(Independent VLAN): Each VLAN operates while maintaining each MAC address table. Because the security is enhanced, data cannot be exchanged directly among VLANs.
- SVL(Shared VLAN): All VLANs operates while maintaining a MAC address table. Because the security is not tightened and the MAC address table exists for all ports, data can be exchanged among VLANs.

Port VID

In the [Port VID] menu, if the VLAN mode is set to 'Tag-based VLAN', set Port VID to specify how to process untagged packets.

Port VID Configuration			
Port	Port VID	Forward Only this VID	Drop Untagged Frame
Port1	1	<input type="checkbox"/>	<input type="checkbox"/>
Port2	1	<input type="checkbox"/>	<input type="checkbox"/>
Port3	1	<input type="checkbox"/>	<input type="checkbox"/>
Port4	1	<input type="checkbox"/>	<input type="checkbox"/>
Port5	1	<input type="checkbox"/>	<input type="checkbox"/>
Port6	1	<input type="checkbox"/>	<input type="checkbox"/>
Port7	1	<input type="checkbox"/>	<input type="checkbox"/>
Port8	1	<input type="checkbox"/>	<input type="checkbox"/>
Port9	1	<input type="checkbox"/>	<input type="checkbox"/>
Port10	1	<input type="checkbox"/>	<input type="checkbox"/>
Port11	1	<input type="checkbox"/>	<input type="checkbox"/>
Port12	1	<input type="checkbox"/>	<input type="checkbox"/>
Port13	1	<input type="checkbox"/>	<input type="checkbox"/>
Port14	1	<input type="checkbox"/>	<input type="checkbox"/>

OK

Item	Description
Port VID	<ul style="list-style-type: none"> - VLAN ID for an untagged packet. - When an untagged packet is sent to the corresponding port, the packet is switched to the VLAN corresponding to the Port VID.
Forward Only this VID	If the received tagged packet tag is different from Port VID when this item is marked, discard the packet. When this item is not marked, the packet is re-sent according to the received tag information.
Drop Untagged Frame	If this item is marked, discard the untagged frame. If not, the untagged frame re-sends the packet to the VLAN corresponding to the setting Port VID.



NOTE

Port VID Input Value

Port VID value is possible only when the value is 255 or less.

Classification

In the [**Classification**] menu, set values to decide VLAN ID. If the VLAN mode is '802.1Q' in [**VLAN**] → [**Configuration**], VLAN ID is decided depending on the protocol of the packet received.

Select the member protocol from [**Classification Rule**] and click the [**OK**] button.

VLAN Classification Configuration

Parameter	Argument
Classification Mode	proto
Classification Rule	appletalk ▾
Group ID	<input type="text"/> (1-256)
VLAN ID	▾

Select	Group ID	VID	Classifier
<input type="button" value="Delete"/>			

Item	Description
Classification Mode	Selected automatically according to the VLAN mode. In case of 802.1Q VLAN, 'proto' is selected. In case of MAC Based VLAN, 'MAC' is selected.
Classification Rule	Based on Appletalk, arp, decnet, ip, ipx, sna, and x25, VLAN is set.
Group ID	Group the selected protocol. Up to 1~256 can be registered.
VLAN ID	Decides which VLAN ID is proper for the current group.

Select the group ID from [**Select**] and click the [**Delete**] button to delete the group ID.

In the [**Configuration**] menu, if the VLAN mode is set to 'MAC', VLAN ID is decided according to the received packet MAC address.

Enter the member MAC address into [**Classification Rule**] and click the [**OK**] button.

VLAN Classification Configuration

Parameter	Argument
Classification Mode	mac
Classification Rule	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>
Group ID	<input type="text"/> (1-256)
VLAN ID	<input type="text" value="2"/>

Select	Group ID	VID	Classifier

Item	Description
Classification Mode	Selected automatically according to the VLAN mode. In case of 802.1Q VLAN, 'proto' is selected. In case of MAC Based VLAN, 'MAC' is selected.
Classification Rule	According to the received packet MAC address, VLAN can be set.
Group ID	Group the selected MAC address. Group ID can be registered ranging from 1 to 256.
VLAN ID	Decides which VLAN ID is proper for the current group.

Select a Group ID from [**Select**] and click the [**Delete**] button to delete the group ID.

MAC

The menu is used to retrieve the address table of the switch and set filtering MAC.

Static Address

Select **[MAC] → [Static Address]** and save a specific MAC address in the address table of the switch regardless of the connection between the device and switch physically.

That is, without using learning(MAC address table renewal), a specific MAC address can be saved in the address table. Even if the device is not connected with the switch and MAX Aging Time(interval of MAC address table renewal) is passed, the corresponding MAC address is left in the address table of the switch.

Static MAC Address

Check	MAC Address	Port ID	VLAN ID
<input type="checkbox"/>	: : : : :	port1	1

Enter the target MAC address and port No. and click the **[Add]** button to add the MAC address. Select a specific MAC address and click the **[Delete]** button to delete the MAC address.

Select **[Port] → [Config]** and set the security of the port. Then, Learning of the source MAC address to the port is not established. In this case, a user can access the port only through the static MAC address set in the port. Thus, by using this access condition, security function can be configured.



NOTE

Number of Static MAC Addresses Entered

Up to 50 static MAC addresses can be entered without a port.



NOTE

VID Setting

In the mode where 802.1Q VLAN is set, if a setting value is entered in the **[Static Address]** and **[Filter Address]** menus, enter **[VLAN ID]**. If not, '0' is entered.

Dynamic Address

Select [MAC] → [Dynamic Address] to retrieve the dynamic address table.

Select a specific MAC address and click the [Delete] button.

Dynamic MAC Address

Check	MAC Address	Port ID
<input type="checkbox"/>	00 : 07 : E9 : 67 : FE : 5B	port7
<input type="checkbox"/>	00 : 01 : E7 : BB : E3 : 00	port7
<input type="checkbox"/>	00 : 13 : 20 : 4E : 32 : EC	port7
<input type="checkbox"/>	00 : 00 : F0 : 67 : 01 : 5F	port7
<input type="checkbox"/>	00 : 50 : FC : B0 : 8E : 3B	port7
<input type="checkbox"/>	00 : 01 : E7 : BB : E3 : 38	port7
<input type="checkbox"/>	00 : 00 : F0 : A1 : 23 : A7	port7
<input type="checkbox"/>	00 : 13 : 20 : 32 : 13 : B3	port7
<input type="checkbox"/>	00 : A0 : B0 : 05 : FC : 55	port7
<input type="checkbox"/>	00 : 09 : 74 : 11 : 11 : 11	port7
<input type="checkbox"/>	00 : 50 : FC : A8 : 12 : 6E	port7
<input type="checkbox"/>	00 : 07 : E9 : EF : B4 : FD	port7
<input type="checkbox"/>	00 : 00 : F0 : A0 : 58 : B3	port7
<input type="checkbox"/>	00 : 07 : E9 : EF : 34 : 73	port7
<input type="checkbox"/>	00 : 07 : E9 : 03 : 21 : 27	port7
<input type="checkbox"/>	00 : 09 : 74 : 00 : 10 : 03	port7
<input type="checkbox"/>	00 : 11 : 11 : 66 : B9 : 46	port7

Filter Address

Use Mac filtering to block unwanted traffics. Enter the target MAC address in the [Filter Address] menu to block the target packet in the switch. Note that MAC is the destination address of the packet sent to the switch port.

Enter the target MAC address and port No. and click the [Add] button.

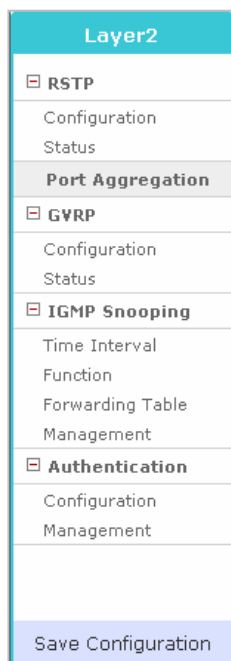
After selecting a specific MAC address, click the [Delete] button.

Filter Destination MAC Address

Check	MAC Address	VLAN ID
<input type="checkbox"/>	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>	<input type="text" value="1"/>

Layer2

Select the **[Layer2]** menu of GPLIM(GPLIMT) to display the submenu of the Layer2 menu on the top left of the window:



Menu	Submenu	Description
RSTP	Configuration	Sets bridge and port environment used in RSTP.
	Status	Retrieves the RSTP operation status of the switch.
Port Aggregation	-	Sets the Port Aggregation related information.
GVRP	Configuration	Sets GVRP and Dynamic VLAN Creation services.
	Status	Retrieves the status of each port where GVRP is set.
IGMP Snooping	Time Interval	Sets the time related with IGMP Snooping.
	Function	Sets the function related with IGMP Snooping.
	Forwarding Table	Retrieves the information of the members registered in IGMP Group.
	Management	Sets whether to operate IGMP Snooping.
Authentication	Configuration	Sets the Authentication service.
	Management	Retrieves the setting information of Authentication.

RSTP

The [RSTP] menu is used to detect a loop from several switches or a single switch link via the environment configuration for Port or the RSTP protocol for Bridge and provides data communication by blocking and forwarding the corresponding port.

Configuration

Select [RSTP] → [Configuration] to configure the Bridge or the Port environment used in the RSTP protocol.

Protocol Status

Parameter	Argument
RSTP status	Current Enable

Bridge Parameter

Parameter	Argument
Bridge Priority	<input type="text" value="8"/> Default : 8 (0 - 15)
Hello Time	<input type="text" value="2"/> sec Default : 2 (1 - 10)
Max Age Time	<input type="text" value="20"/> sec Default : 20 (6 - 40)
Forward Time	<input type="text" value="15"/> sec Default : 15 (4 - 30)

Port Parameter

Port Name	Priority	Force Version	Path Cost	Port Fast	Link Type
Port 1	<input type="text" value="8"/>	<input type="text" value="RSTP"/>	<input type="text" value="200000"/>	<input type="text" value="Enable"/>	<input type="text" value="Point to Point"/>
Port 2	<input type="text" value="8"/>	<input type="text" value="RSTP"/>	<input type="text" value="200000"/>	<input type="text" value="Enable"/>	<input type="text" value="Point to Point"/>
Port 3	<input type="text" value="8"/>	<input type="text" value="RSTP"/>	<input type="text" value="200000"/>	<input type="text" value="Enable"/>	<input type="text" value="Point to Point"/>
Port 4	<input type="text" value="8"/>	<input type="text" value="RSTP"/>	<input type="text" value="200000"/>	<input type="text" value="Enable"/>	<input type="text" value="Point to Point"/>
Port 5	<input type="text" value="8"/>	<input type="text" value="RSTP"/>	<input type="text" value="200000"/>	<input type="text" value="Enable"/>	<input type="text" value="Shared"/>
Port 6	<input type="text" value="8"/>	<input type="text" value="RSTP"/>	<input type="text" value="200000"/>	<input type="text" value="Enable"/>	<input type="text" value="Shared"/>
Port 7	<input type="text" value="8"/>	<input type="text" value="RSTP"/>	<input type="text" value="200000"/>	<input type="text" value="Enable"/>	<input type="text" value="Shared"/>
Port 8	<input type="text" value="8"/>	<input type="text" value="RSTP"/>	<input type="text" value="200000"/>	<input type="text" value="Enable"/>	<input type="text" value="Shared"/>
Port 9	<input type="text" value="8"/>	<input type="text" value="RSTP"/>	<input type="text" value="200000"/>	<input type="text" value="Enable"/>	<input type="text" value="Shared"/>
Port 10	<input type="text" value="8"/>	<input type="text" value="RSTP"/>	<input type="text" value="200000"/>	<input type="text" value="Enable"/>	<input type="text" value="Shared"/>
Port 11	<input type="text" value="8"/>	<input type="text" value="RSTP"/>	<input type="text" value="200000"/>	<input type="text" value="Enable"/>	<input type="text" value="Shared"/>
Port 12	<input type="text" value="8"/>	<input type="text" value="RSTP"/>	<input type="text" value="200000"/>	<input type="text" value="Enable"/>	<input type="text" value="Shared"/>
Port 13	<input type="text" value="8"/>	<input type="text" value="RSTP"/>	<input type="text" value="200000"/>	<input type="text" value="Disable"/>	<input type="text" value="Shared"/>
Port 14	<input type="text" value="8"/>	<input type="text" value="RSTP"/>	<input type="text" value="200000"/>	<input type="text" value="Disable"/>	<input type="text" value="Shared"/>

Item	Description
Protocol Status	Displays the current status of the RSTP protocol.
Bridge Parameter	<p>Configures the Bridge parameter of the switch that RSTP operates.</p> <ul style="list-style-type: none"> - Bridge Priority: Decides the priority of Bridges. - Hello Time: Sets the transmission cycle of BPDU. - Max Age Time: Sets the Message Age time. - Forward Time: Displays the time that the state of each port is changed by level.(Discarding-Learning-Forwarding)
Port Parameter	<ul style="list-style-type: none"> - Priority: Standard to select the port to be blocked when the switch loop is established. - Force Version: Communication is progressed via the switch connected to the corresponding port and the BPDU that a user specifies. For '0', STP BPDU is transmitted. For '1', RSTP BPDU is transmitted. - Path Cost: Displays the path cost according to the bandwidth when the connection with the opponent is established. - portfast: If this value is activated, the corresponding port becomes Edge port and quickly converted into forwarding state by considering the port is connected to a terminal device, not a switch device. In addition, if this function is activated, the MAC address learned in the corresponding port is not canceled even when all topologies of Bridges are changed.(To connect the port to the STP device, the portfast function should be canceled.) - linktype: Displays the type of the link connected to the opponent. The link is connected as point-to-point in RSTP.

Status

Select [RSTP] → [Status] to display the status of switch RSTP operation. The status is roughly divided into Bridge Information and Port Information. The Bridge Information Category in the upper section displays the RSTP parameter configured in the system and the Port Information item in the lower section displays the detailed information by ports.

Bridge Information	
Parameter	Argument
Protocol Status	Enabled
Designated Bridge Identifier	80000000f0e820f9
Root Bridge Identifier	80000000f0885544
Root Path Cost	400000
Root Port	11
Last Topology changed	Thu Jan 1 09:00:00 1970

Port Information					
Port Name	Port ID	Path Cost	Port Role	Port State	Designated Root
Port1	0x8002	200000	Designated	Forwarding	80000000f0885544
Port2	0x8003	200000	Designated	Forwarding	80000000f0885544
Port3	0x8004	200000	Designated	Forwarding	80000000f0885544
Port4	0x8005	200000	Disabled	Discarding	80000000f0885544
Port5	0x8006	200000	Disabled	Discarding	0000000000000000
Port6	0x8007	2000000	Disabled	Discarding	80000000f0885544
Port7	0x8008	200000	Disabled	Discarding	0000000000000000
Port8	0x8009	200000	Disabled	Discarding	0000000000000000
Port9	0x800a	200000	Disabled	Discarding	0000000000000000
Port10	0x800b	200000	Rootport	Forwarding	80000000f0885544
Port11	0x800c	200000	Disabled	Discarding	0000000000000000
Port12	0x800d	200000	Disabled	Discarding	0000000000000000
Port13	0x800e	20000	Disabled	Discarding	0000000000000000
Port14	0x800f	20000	Disabled	Discarding	0000000000000000

- Bridge Information
 - Designated Bridge Identifier
 - Its own bridge information is displayed in hexadecimal numbers.
 - The upper four digits represent the bridge priority and the remaining lower digits are expressed as the system MAC address.

- Root Bridge Identifier
Among the connected switches, it indicates the identifier of the switch equipment selected as the root bridge. Therefore, if there is no connection between switches, the Root Bridge Identifier displays the same information as the Designed Bridge Identifier.
- Root Path Cost
When the root bridge is decided, it displays the calculated cost for the path to the root switch.
- Root Port
If the current equipment is not the root switch, it indicates the ID of the port corresponding to the root port. (The figure above indicates 0x8003 of port2. A switch can have only root port.)
- Last Topology Changed
It indicates the recent time that the RSTP network is reconfigured by the change of the network configuration between switches.
- Port Information
 - Port ID
The value is combined with the value of the port priority and the ID value of the port specified in the system. The highest two digits represents the value of the port priority and the lowest two digits consist of port index.
 - Path Cost
The value indicates the path cost of the corresponding path.
 - Port Role
The value indicates the role of the port that selected via the BDPU exchange between switches. The RSTP Port Role is divided into Disable, Alternate, Backup, Designated, Root roles.
 - Port State
The Port State shows the status of the corresponding port. If a loop is detected via the BDPU communication, the Port State looks for the port to be blocked in accordance with Port ID and Path Cost and blocks data communication to prevent the loop from being constructed in the whole switch. The port state is divided into Discarding, Learning, Forwarding and Blocking states. In blocking, learning, discarding states, data communication is not performed. The data communication is performed only in forwarding state. In addition, the blocking state represents the state that blocks the data communication by force by detecting a loop via RSTP.
 - Designated Root
If a switch connected to the corresponding port is more close to the root switch, the Designated Root shows the Bridge identifier of the connected switch. Otherwise, Designated Root shows its own Bridge identifier.

Port Aggregation

Select **[Port Trunking]** → **[Configuration]** to specify the configuration related to Port Trunking. Click the **[OK]** button to apply the setting to the system. Click the **[Refresh]** button to update and display the current status.

Aggregate Configuration

Load balance mode	
Load Balance	Direct-MAP based DMAC & SMAC & SPORT-ID
System Priority	32768 (1 - 65535 Default : 32768)
System ID	00:00:f0:d5:c9:ea

Member Configuration

S: Static, L: LACP

	Grp 1	Grp 2	Grp 3	Grp 4	Grp 5	Grp 6	Grp 7	Mode	Priority	Sync
Port1	S							Active		X
Port2	✓							Active		X
Port3	✓							Active		X
Port4								Active		X
Port5								Active		X
Port6								Active		X
Port7								Active		X
Port8								Active		X
Port9								Active		X
Port10								Active		X
Port11								Active		X
Port12								Active		X
Port13								Active		X
Port14								Active		X

Port Aggregation

Item	Description
Load Balance	<p>When transferring a packet to the opposite party through a trunk port, the packet is transferred to a port among members included to the trunk group. Select an algorithm to select a port for transfer at this time.</p> <p>The default is Direct-MAP based DMAC & SMAC & SPORT-ID.</p> <ul style="list-style-type: none"> - CRC based DMAC & SMAC - Direct-MAP based DMAC & SMAC - CRC based DMAC & SMAC & SPORT-ID - Direct-MAP based DMAC & SMAC & SPORT-ID
System Priority	A protocol setup value used in a LACP. The default is 32768.
System ID	An identification value used in LACP. This value is the same as the value of the MAC address in the system.

Member Configuration

Item	Description
Group	'S' means a static trunk, and 'L' means a LACP. It is used for setting up the trunk type of the group. Up to eight groups can be generated as shown on the screen, and up to four ports can be included to a group as members. In addition, a member included to a group cannot be included another group simultaneously.
Mode	Displayed when selecting the trunk configuration as 'LACP'. It is available to select one of 'Active/Passive'. For the Active, a LACP packet is transferred to the opposite party first, based on the system. For the Passive, it is responded only when receiving a packet from the opposite system. If the user system and opposite system are all set up as Active, a system that has higher priority is used as a reference.
Priority	Sets up the port priority. The default is 32768.
Sync	Indicates information connected to the opposite system in ports that are configured with LACP ports. If configured as a LACP member but the LACP connection is abnormal for the opposite system, it is displayed as 'X'. 'O' means that a port is properly operated as a LACP port.

GVRP

The **[GVRP]** menu is used to start or stop the GVRP service, or modify the GVRP service of each port.

Configuration

Select **[GVRP]** → **[Configuration]** to start/stop the GVRP and the Dynamic VLAN Creation services.

Parameter	Argument
GVRP	Disable ▼
Dynamic VLAN Creation	Disable ▼

Save

On the **<GVRP Basic>** window, specify the GVRP configuration as Enable and click the **[Save]** button to display the following window and modify the GVRP configuration for each port.

Port	Status	Registration	Applicant	Timers(millisecond)		
				Join	Leave	LeaveAll
<input type="checkbox"/> ALL	Enable ▼	-	-	-	-	-
port1	Disable ▼	-	-	-	-	-
port2	Disable ▼	-	-	-	-	-
port3	Disable ▼	-	-	-	-	-
port4	Disable ▼	-	-	-	-	-
port5	Disable ▼	-	-	-	-	-
port6	Disable ▼	-	-	-	-	-
port7	Disable ▼	-	-	-	-	-
port8	Disable ▼	-	-	-	-	-
port9	Disable ▼	-	-	-	-	-
port10	Disable ▼	-	-	-	-	-
port11	Disable ▼	-	-	-	-	-
port12	Disable ▼	-	-	-	-	-
port13	Disable ▼	-	-	-	-	-
port14	Disable ▼	-	-	-	-	-

OK Refresh

Click the **[OK]** button to save the information of each port and click the **[Refresh]** button. Then, the latest information of the port is displayed.

Item	Description
Port	Port Number
Status	GVRP configuration Information
Registration	Registration mode with Normal, Forbidden and Fixed conditions
Applicant	Applicant mode with Normal and Active conditions
Join	Interval for Join Transfer Time
Leave	Value of Leave Delay Time
LeaveAll	Value of LeaveAll Transfer Time

Status

Select [GVRP] → [Status] to display the information of the port that GVRP is configured.

GVRP Machine			
Port	GID	Applicant State	Registrar State
Port1	0	VP	INR
Port2	0	VP	INR

GVRP Statistics						
Port		Join Empty	Join In	Leave Empty	Leave In	Empty
Port1	RX	0	0	0	0	0
	TX	0	0	0	0	0
Port2	RX	0	0	0	0	0
	TX	0	0	0	0	0

GVRP Machine

Item	Description
Port	Port Number
GID	Index showing the information of GARP.
Applicant State	Current status of Applicant State Machine
Register State	Current Status of Register State Machine

GVRP Statistics

Item	Description
Port	Port Number
Join Empty	Number of Join Empty packets
Join In	Number of Join In packets
Leave Empty	Number of Leave Empty packets
Leave In	Number of Leave In packets
Empty	Number of Empty packets

IGMP Snooping

The **[IGMP Snooping]** menu is used for the configuration of IGMP Snooping functions and the query of the configured information.

Time Interval

Select **[IGMP Snooping]** → **[Time Interval]** to configure the time related to IGMP Snooping.

Time Interval

Category	Argument
VLAN	Default
Group Membership	120000 ms

OK

VLAN	Group Membership (ms)	Last Member Query Timeout (ms)	Max Response (ms)	Other Query (ms)
Default	120000	1000	10000	120000

Categories	Description
VLAN	Selects the VLAN to be configured.
Group Membership	Configures the time to exit from the multicast forwarding database list when new report does not exist.
Last Member Query Timeout	Indicates the time to wait a response report after sending a query to check if the host is the last host when multicast router receives a leave message from a host. If the report is not replied until the time is elapsed, the host is deleted from the group.
Max Response	Configures the maximum time until its response when IGMP Snooping query is received.
Other Query	Configures the time until the operation as a querier starts when a query from the multicast router does not exist.

Select the VLAN and the Category to configure, enter the time and click the **[OK]** button to store the configuration.

Function

Select **[IGMP Snooping]** → **[Function]** to specify the functions related to IGMP Snooping.

Function

Category	Argument
VLAN	Default <input type="button" value="v"/>
<input type="button" value="v"/> Querier	Disable <input type="button" value="v"/>

Cross VLAN	Flood DPM
Disable <input type="button" value="v"/>	Disable <input type="button" value="v"/>

VLAN	Querier	Immediate Leave
Default	Disable	Disable

Categories	Description
VLAN	Selects the VLAN to be configured.
Querier	Specifies the operation as IGMP querier when the multicast router does not exist.
Immediate Leave	Deletes a host from the group immediately when receiving the Leave Message.
Cross VLAN	Forwards multicast packets to all ports regardless of VLAN.
Flood DPM	If no member exists in the IGMP group, sets whether to forward multicast packets.

Querier and Immediate Leave can be set of each VLAN, but Cross VLAN and Flood DPM can be set on a bridge basis.

Forwarding Table

Select **[IGMP Snooping]** → **[Forwarding Table]** to display the information on the members registered in IGMP Group.

Forwarding Table			
VLAN	Multicast IP Address	Member Port	Aging Time
<input type="button" value="Refresh"/>			

Click the **[Refresh]** button to update the information displayed on the web screen into the latest information.

Management


Select [IGMP Snooping] → [Management] to specify the operation of IGMP Snooping.

IGMP Snooping Management

Scope	Action
Global ▼	Enable ▼

Scope	Current Status
Global	Enable
Default	Enable

According to VLANs, the IGMP Snooping can be operated respectively. If, however, Global is set to Disable, all VLANs become in Disable mode.



IGMP Snooping Management

In Global Disable mode, other pages except the Management page are not be displayed.

NOTE

Authentication

This menu is used to retrieve the setting information or set the authentication.

Configuration

When selecting [Authentication] → [Configuration] if the activity status of [Authentication] → [Management] is 'Stop', the following window appears:

Authentication Configuration

802.1X Port-Based Authentication Disabled

If the activity status of [Authentication] → [Management] is 'Running', the following window appears:

Authentication Configuration

Port	Control	Reauth	Reauth-period	Tx-period	Supp Time-out	Server Time-out
Port1	None	<input type="checkbox"/>				
Port2	None	<input type="checkbox"/>				
Port3	None	<input type="checkbox"/>				
Port4	None	<input type="checkbox"/>				
Port5	Auto	<input type="checkbox"/>	3600	30	30	30
Port6	None	<input type="checkbox"/>				
Port7	None	<input type="checkbox"/>				
Port8	None	<input type="checkbox"/>				
Port9	None	<input type="checkbox"/>				
Port10	None	<input type="checkbox"/>				
Port11	None	<input type="checkbox"/>				
Port12	None	<input type="checkbox"/>				
Port13	None	<input type="checkbox"/>				
Port14	None	<input type="checkbox"/>				

OK Cancel

Item	Description
Control	Indicates the authentication mode of each port of user authentication.(802.1x). - None: Authentication is not performed for the port. - Force-authorized: Admits the port forcibly. - Force-unauthorized: Block the port forcibly. - Auto: Allows the port through authentication from the Radius server and blocks the port.
Reauth	Used for re-authentication.
Reauth-Period	Indicates re-authentication cycle when Reauth is set. (1-4294967295sec) default: 3600 sec
Tx-Period	Indicates the period that sends Request regularly to supplicant. (1-65535sec) default: 30 sec
Supp-Timeout	Indicates the time before re-sending to the user when EAP is requested.(1-65535sec) default: 30 sec
Sever-Timeout	Indicates the time before re-sending to the device when server authentication of a server is requested.(1-65535sec) default: 30 sec

The settings of re-authentication and period are applied only when the defaults exist and the settings are changed. For server authentication, the Control field should be set as Auto. The corresponding port is permitted only when the information received from Supplicant is transmitted to the Radius server and the authentication is approved. If Reauth is marked after the authentication is approved, the re-authentication is periodically requested to the server at the interval of Reauth-Period.

Management

Select [**Authentication**] → [**Management**] to activate/deactivate the authentication of system. When executing [**Run**] of Action if Activity is set to Stop, items of [**Authentication**] → [**Configuration**] can be set. When executing [**Stop**] of Action if Activity is set to Running, user authentication is deactivated.

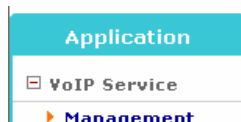
Setting 802.1x user authentication indicates that there is the Radius server that has the user information. The host IP address, host, and key should be registered of the Radius server to be used. The default of the Radius Host Port is 1812 port. Click the [**OK**] button after the setting. Then, the setting is applied.

Activity	Action
Stop	<input type="button" value="Run"/>

Radius Server Management	
Host IP	192 . 168 . 0 . 23
Secret Key	samsung
Host Port	1812

Application

Select the [**Application**] menu of GPLIM(GPLIMT) to display the submenu of the interface on the top left window.

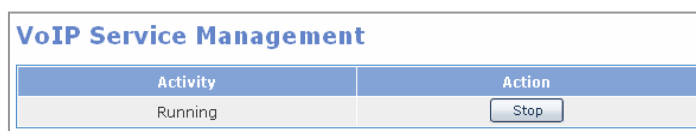


VoIP Service

This menu is used to set VoIP service environment.

Management

The [Management] menu enables to start or stop the VoIP service function. Although the system is rebooted, the setup is restored to the last status.



Item	Description
Activity	Current VoIP Service Status.
Action	A command that is available to be executed in the current status.

PoE

Select the [**PoE**] menu of GPLIM(GPLIMT) to display the submenu of the port on the top left window.



Menu	Submenu	Description
PoE	Global	Sets or retrieves the PoE version information and power supply information.
	Configuration	Sets or retrieves the power information of each port.
	Power Status	Displays the PoE power supply status in real time.
	Port Status	Displays the PoE port status in real time.
	Management	Activates and deactivates the PoE manager.
	Log	Records the PoE information as logs in real time.
Save Config	-	Saves the setting information to apply the information for the operation. Or, sets all setting information to the default value.

PoE

This menu is used to retrieve the PoE status or the PoE function status.

Global

Select [**PoE**] → [**Global**] to check the PoE version information and power supply information. In addition, this menu enables retrieving and setting the Power Management Mode.

PoE Version Information

PoE Software Version	
501.4	

	Numbers of ports	Hardware Version
PoE DEV.Version 0	4	1
PoE DEV.Version 1	4	1
PoE DEV.Version 2	4	1

Power Supply Voltage

Category	Value
PoE Power Supply Voltage	54 (V)
PoE Power Consumption	0 (W)
PoE Power Max Shutdown Voltage	57.0 (V)
PoE Power Min Shutdown Voltage	44.0 (V)
PoE Power Information	Internal

Power Management Mode

Dynamic <input type="radio"/>	Static <input checked="" type="radio"/>	Class <input type="radio"/>
-------------------------------	---	-----------------------------

PoE System Masks

Power disconnect method	<input type="radio"/> Low port shut down	<input checked="" type="radio"/> Access deny
Capacitor detection	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable

Item	Description
PoE Software Version	Indicates the PoE Software version.
PoE DEV.Version(0, 1, 2)	Indicates the number of ports of each PoE chip and the hardware version.
PoE Power Supply Voltage	Indicates total voltage of PoE power supply.
PoE Power Consumption	Indicates the total usage of the PoE power.
PoE Power Max Shutdown Voltage	Indicates the maximum voltage of the power.
PoE Power Min Shutdown Voltage	Indicates the minimum voltage of the power.
PoE Power Information	Indicates whether the power source comes from external power or internal power.

When setting the Power Management Mode, power supply type can be selected depending on Power Device(PD), terminal power.

'Dynamic' is based on the power being used and the maximum power is 18.9 W. 'Static' indicates a user defines the restriction of the power. According to the defined power, items related with the restriction of the power are decided. 'Class' decides the restriction of the power depending on the PD terminal PD Classes are described as follows:

Class	Power
0	15.4 W
1	4 W
2	7 W
3	15.4 W
4	15.4 W

PoE System Masks decides the disconnection method of the power and whether to execute Capacitor Detection.

Item	Description
Power Disconnect Method	<ul style="list-style-type: none"> - Low port shut down: If the power of the next port supplied after exceeding the power budget, the low priority port is shut down for the port with high priority. - Access deny: Denied if the power of the next port supplied after exceeding the power budget.
Capacitor Detection	<ul style="list-style-type: none"> - Enable: Capacitor enable - Disable: Capacitor disable

Set the target item and click the **[OK]** button to apply the setting.

Configuration

Select [PoE] → [Configuration] to retrieve and set the power information of each port.

PoE Port Configuration

Category	value
Port	port1
Enable	Enable
Limit(mW)	16800
Priority	high

OK

PoE Port List

Port	Enable	Power	Limit (mW)	Priority	M(v)	C(mA)	C(W)	Class
port1	0	0.0	16800	low	0	0	0	0
port2	0	0.0	16800	low	0	0	0	0
port3	0	0.0	16800	low	0	0	0	0
port4	0	0.0	16800	low	0	0	0	0
port5	0	0.0	16800	low	0	0	0	0
port6	0	0.0	16800	low	0	0	0	0
port7	0	0.0	16800	low	0	0	0	0
port8	0	0.0	16800	low	0	0	0	0
port9	0	0.0	16800	low	0	0	0	0
port10	0	0.0	16800	low	0	0	0	0
port11	0	0.0	16800	low	0	0	0	0
port12	0	0.0	16800	low	0	0	0	0

Item	Description
Port	Indicates the Ethernet port 1~12 of a device.
Enable	Sets or releases the PoE power supply of the target port.
Limit(mW)	If the Power Management Mode is set to Static, the power limit of each port. Up to 1000~18900 mW can be set.
Priority	Indicates the priority setting of the power. When the power is supplied excessively, the power supply for the port is blocked according to the priority.

Select the target port and set whether to enable/disable PoE and the power limit and priority, and click the [OK] button. Then, the setting is applied. The applied information can be checked by viewing the PoE Port List item. The items and descriptions of PoE Port List as same as the items and descriptions of the Power Status below.

Power Status

Select [PoE] → [Power Status] to display the PoE power supply status of all ports in real time.

PoE Port List								
Port	Enable	Power	Limit (mW)	Priority	M(v)	C(mA)	C(W)	Class
port1	○	0.0	16800	low	0	0	0	0
port2	○	0.0	16800	low	0	0	0	0
port3	○	0.0	16800	low	0	0	0	0
port4	○	0.0	16800	low	0	0	0	0
port5	○	0.0	16800	low	0	0	0	0
port6	○	0.0	16800	low	0	0	0	0
port7	○	0.0	16800	low	0	0	0	0
port8	○	0.0	16800	low	0	0	0	0
port9	○	0.0	16800	low	0	0	0	0
port10	○	0.0	16800	low	0	0	0	0
port11	○	0.0	16800	low	0	0	0	0
port12	○	0.0	16800	low	0	0	0	0

Total Power	
Category	value
PoE Total Power Consumption	0 (W)
PoE Total Calculated Power	0 (W)

Item	Description
Port	Indicates the Ethernet port 1~12 of a device.
Enable	Sets or releases the PoE power supply of the target port.
Power	Indicates the power allocated to the port.
Limit(mW)	If the Power Management Mode is set to Static, the power limit of each port. Up to 1000~18900 mW can be set.
Priority	Sets the priority of the port. - Low: Priority is low when the power is supplied excessively. - High: Priority is high when the power is supplied excessively.
M(v)	Vmain voltage–Total voltage of the power.
C(mA)	Calculated current(Displays the current of the target port.)
C(W)	Power consumption(Displays the voltage of the target port.)
Class	Displays the class of the target port.

Port Status

Select [PoE] → [Port Status] to display the current status of all ports in real time.

PoE Port Status	
Port	Status
port1	Port is off-improper Capacitor Detection results
port2	Port is off-improper Capacitor Detection results
port3	Port is off-improper Capacitor Detection results
port4	Port is off-improper Capacitor Detection results
port5	Port is off-user setting
port6	Port is off-improper Capacitor Detection results
port7	Port is off-improper Capacitor Detection results
port8	Port is on-vaild registor detected
port9	Port is off-detection is in process
port10	Port is off-detection is in process
port11	Port is off-detection is in process
port12	Port is off-detection is in process

Item	Description
Port	Indicates the Ethernet port 1~12 of a device.
Status	Indicates the current PoE information of the port.

Management

Select [PoE] → [Management] to activate/deactivate PoE Manager.

If Activity is set to 'Stoped' and [Run] of Action is executed, the items of [PoE] → [Global], [PoE] → [Configuration], and [PoE] → [Power status], [PoE] → [Port status] can be set and retrieve. If Activity is set to 'Running' and [Stop] of Action is executed, PoE Manager is deactivated.

PoE Management		
Module Name	Activity	Action
PoE	Running	<input type="button" value="Stop"/>

PoE Management		
Module Name	Activity	Action
PoE	Stop	<input type="button" value="Run"/>

Log

Select [**PoE**] → [**Log**] to record the PoE information as logs regularly.

PoE Log

Category	Value	
PoE Log	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
Version	<input type="radio"/> On	<input checked="" type="radio"/> Off
Status	<input checked="" type="radio"/> On	<input type="radio"/> Off
Global	<input type="radio"/> On	<input checked="" type="radio"/> Off
Port	<input type="radio"/> On	<input checked="" type="radio"/> Off
Time interval	30 sec	

Item	Description
PoE Log	- Enable: Enables PoE Log Manager. - Disable: Disables PoE Log Manager.
Version	Set the version information to On in the PoE Global menu.
Status	Sets this value to On when PoE System masks information and PoE fault occur.
Global	Sets the power supplies information to On in the PoE Global menu.
Port	Sets the power status and port status of the port to On.
Time interval	Sets the time for displaying logs regularly.

If PoE Log is not enabled, the following items are not activated.
Set the items and click the [**OK**] button. Then, the setting is applied.



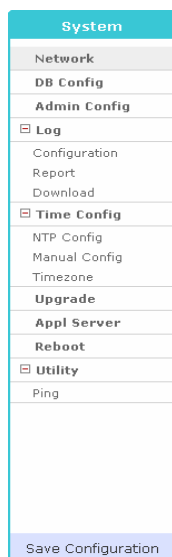
CAUTION

When Protecting Overload Caused by PoE Log Activation

When all items are set to On or Enable, system overload may occur.
Use the setting only when logs are left. If not, set to Disable.

System

Select the **[System]** menu of GPLIM(GPLIMT) to display the submenu of the system on the top left window.



Menu	Submenu	Description
Network	-	Sets IP and DNS services.
DB Config	-	Saves DB and change to the basic DB or user DB.
Admin Config	-	Sets for the management authentication.
Log	Configuration	Sets to determine whether to leave the log for each item.
	Report	Retrieves the system log currently stored.
	Download	Downloads System Log.
Time Config	NTP Config	Sets the time server to synchronize the time server with date and time information.
	Manual Config	Sets the date and time of the system.
	Timezone	Sets the timezone of the user.

(continued)

Menu	Submenu	Description
Upgrade	-	Upgrades the GPLIM(GPLIMT) operation software.
Appl Server	-	Sets SSH, FTP, and Telnet services.
Reboot	-	Reboots the system.
Utility	Ping	Executes a Ping command and verifies the result.

Network

Select [System] → [Network] and set IP and DNS.

Network Interface

This menu is used to set GPLIM(GPLIMT) IP address and Netmask and set whether to use interface. Select the target item and click the [OK] button. IP default value of the GPLIM(GPLIMT) board is set to 10.0.4.1/24.

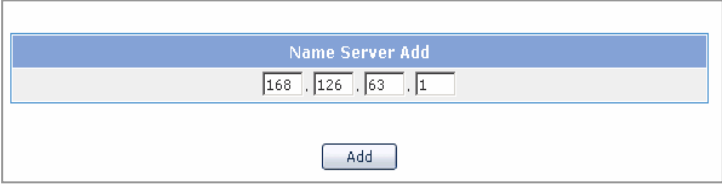
Network Interface

Interface	
IP	<input type="text" value="10"/> . <input type="text" value="0"/> . <input type="text" value="4"/> . <input type="text" value="1"/> (00:0f:04:0f:05:01)
Netmask	<input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="0"/>
Default Gateway	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>

Item	Description
IP	Sets network IP.
Netmask	Sets Netmask.
Default Gateway	Sets default gateway IP.


DNS

The Name Server to be used in GPLIM(GPLIMT) can be set in STATIC DNS.



Name Server Add			
168	.126	.63	.1
<input type="button" value="Add"/>			

Set the IP corresponding to the DNS server and click the [**Add**] button. Then, the setting is directly applied to the <**Static DNS**> window of [**Interface**] → [**DNS**]. For example, when DNS is entered as shown in the figure above, the <**Static DNS**> window is displayed as follows:



Name Server List	
<input type="checkbox"/>	168.126.63.1
<input type="button" value="Delete"/>	

DB Config

[DB Config] menu is used to save DB and change to the basic DB or user DB.

Select	Type	Description
<input checked="" type="radio"/>	Import	<input type="text"/> <input type="button" value="Browse..."/>
<input type="radio"/>	Export	Export the current system db.
<input type="radio"/>	Default	Change the current system db to default system db.

item	Description
Import	Modifies to DB that exists on the user's PC.
Export	Saves the DB in use to the user's PC.
Default	Modifies DB to initial setting.

To modify DB using the DB Import function, the DB file should be stored on PC in advance. As the DB default is changed to the initial DB, the web manager should be connected to 10.0.4.1 through the LAN port of the internal network after the restart of the system.



DB Change

If the database of OfficeServ 7400 GPLIM(GPLIMT) is changed, the system is rebooted.

Admin Config

This menu sets the authentication server of the system login. It sets the Local, Radius and Taccas+ authentication server. If selecting an authentication method, the setting page for the selected method is displayed.

Category	Value
Set Policy	<input checked="" type="checkbox"/> Local <input checked="" type="checkbox"/> Radius <input checked="" type="checkbox"/> Taccas+

If checking the desired authentication method and clicking the [OK] button, the authentication method is applied. If selecting two or more authentication

servers, it is available to establish the priority for the authentication servers. Basically, the authentication servers are processed in the order of **[Local]** → **[Radius]** → **[Taccas+]**.

Local

Change the Local Password. Enter new password and click the **[OK]** button to change the Local Password of the system.

Local	
Category	Configuration
New Password	<input type="text"/>
Confirm New Password	<input type="text"/>

Radius

Enter the information on the Radius authentication server. If entering Server IP, key defined on Server and timeout time and clicking the **[Add]** button, the entered values are applied to the system. Up to 5 lists can be entered. If checking the entered lists and pressing the **[Delete]** button, the selected lists are deleted.

Radius			
	Radius Server IP	Radius Server Key	Time out
	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	<input type="text"/>	<input type="text"/>

Taccas+

Enter the information on the [Taccas+] authentication. Up to 5 server IP lists are entered or deleted the same as the Radius input page. All of the server IP and secret key should be entered initially. If values are added, it is possible to update secret keys. If all server IP lists are deleted, the values of the secret keys are, also, deleted.

Taccas+

Taccas+ Server

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

Taccas+ Secret Key

<input type="text"/>

In the following screen, Web Time-out can be set. If setting as 'Enable', Web Time-out operates using the set value. If setting as 'Disable', Web Time-out doesn't operate. Default value is 10 minutes(minimum 1 minute/maximum 1440 minutes). After changing the time, surely log-out and log-in, then Web Time-out operates regularly using the set value.

Web Time-out Configuration

Category	Value
Time	<input type="text" value="Enable"/> <input type="text" value="10"/> Min (1 ~ 1440)



CAUTION

When Activating Server Authentication

Login Policy should be applied first to activate the server authentication to the system. If entering the authentication information in the status that the Logging Policy is only selected without application, the information is not applied to the server authentication information.

Log

This menu allows setting up the system log and retrieve the information.

Configuration

Allow setting up the log to determine whether to add a log to the system.

Log Policy		
Advanced Service		
Log	ON <input checked="" type="radio"/>	OFF <input type="radio"/>
<input type="button" value="OK"/> <input type="button" value="Reset"/>		

Determine to add a log to the system and click the **[OK]** button to add the log to the system log. Click the **[Reset]** button to return to the previous status before applying the setting.

Log Report

Allow retrieving a log saved in the system according to the desired time.

Report Policy					
Advanced Service					
ALL	<input checked="" type="radio"/>	POE	<input type="radio"/>		
Report Policy					
Detail Search					
	YEAR	MONTH	DAY	HOUR	MINUTE
From	2005	9	23	8	00
To	2005	9	28	21	00
<input type="button" value="OK"/> <input type="button" value="Reset"/>					

Click the **[OK]** button after setting the desired time to verify the following log below. Click the **[Reset]** button to return to the default value.

- ALL: All logs including POE
- POE: Log related with POE

Log Report
[1970-1-1 9 : 00] ~ [1970-1-2 19 : 00]

Date/Time	Message	Type
1970/1/1 9:0:33	xinetd Version 2.3.11 started with libwrap options compiled in.	xinetd
1970/1/1 9:0:33	Started working: 2 available services	xinetd
1970/1/1 9:0:36	xinetd startup succeeded	02xinetd
1970/1/1 9:0:38	Entering runlevel: 3	init
1970/1/1 9:0:41	session opened for user toor by (uid=0)	login
1970/1/1 9:0:41	toor[190] ROOT LOGIN ON console	--
1970/1/1 9:42:42	check pass; user unknown	login
1970/1/1 9:42:42	authentication failure; logname= uid=0 euid=0 tty=pts/0 ruser= rhost=192.168.0.125	login
1970/1/1 9:42:44	FAILED LOGIN 1 FROM 192.168.0.125 FOR adm, Authentication service cannot retrieve authentication info.	login
1970/1/1 9:42:46	session opened for user admin by (uid=0)	login

1/5

Click one of the buttons on the bottom of the window above to move the desired page. Click the **[First]** or **[Last]** button to move to the first page or last page. Click the **[Next]** or **[Prev]** button to move the previous or next page. Click the **[Next+10]** or **[Prev+10]** button to move the 10 pages backward or forward.

Download

Allow downloading the log of the system that is currently saved.

Log File Management

Download log file
To download log files
Click the [Download] button.

Press the **[Download]** button to download the system log in the form of a compressed file.

Time Config

Synchronize the timezone, date and time of the system through a network or sets the values by itself.

NTP Config

Select [**Time Configuration**] → [**NTP Config**] and set Time Server to synchronize the information on the time server, date and time. Current Time indicates the current time of the system. NTP Server Status indicates the execution status of NTP Demon.

Time Server is registered in the Time Server table. For the registration method, both IP and Domain Name methods are available. (But, to use Domain Name, DNS Server should be set. To synchronize with Time Server by configuring such NTP, a network should be connected.)

If registering Time Server, click the [**OK**] button to start or restart NTP demon.

Current Time	
2005. Sep. 26. (Mon) 19:13:57	

NTP Server Status	
Status	stop

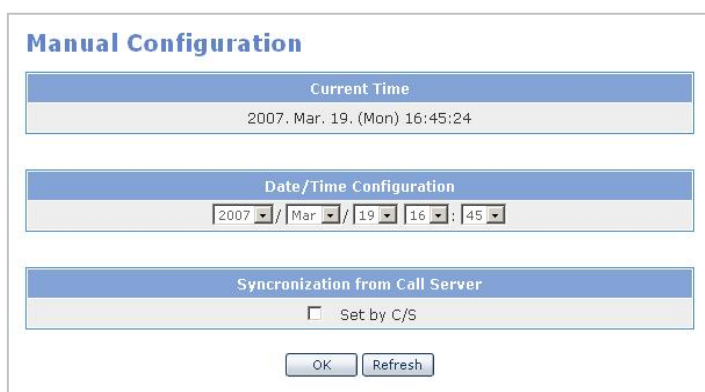
Time Server	
Server 1	<input type="text"/>
Server 2	<input type="text"/>

OK

Manual Config

[Time Configuration] → [Manual Config] menu is used to set and modify the date and time of the system to the time that the user wants. If clicking the [OK] button after selecting date and time that the user wants in the table of Date/Time Configuration, the date and time of the system is changed to the selected time.

Check and click the [OK] button to synchronize the date and time of the user from Call Server table with Call Server.



The screenshot shows a dialog box titled "Manual Configuration". It contains three main sections:

- Current Time:** A blue header bar with the text "Current Time" and a light gray bar below it displaying "2007. Mar. 19. (Mon) 16:45:24".
- Date/Time Configuration:** A blue header bar with the text "Date/Time Configuration" and a light gray bar below it containing five dropdown menus for date and time selection, showing "2007", "Mar", "19", "16", and "45".
- Synchronization from Call Server:** A blue header bar with the text "Synchronization from Call Server" and a light gray bar below it containing a checkbox labeled "Set by C/S".

At the bottom of the dialog box are two buttons: "OK" and "Refresh".

Timezone

[Time Configuration] → [Timezone] menu is used to change the timezone by selecting the timezone related to the user.

Select the desired area(city or GMT) in the areas by GMT and click the [OK] button to modify the timezone information of the system.



The screenshot shows a dialog box titled "Time Configuration". It contains one main section:

- Time Zone:** A blue header bar with the text "Time Zone" and a light gray bar below it containing a dropdown menu with the selected option "[GMT+09:00] Seoul, Tokyo".

At the bottom of the dialog box is one button: "OK".

Upgrade

Upgrade the Kernel and Ramdisk in the [**Upgrade**] menu.

For the types of upgrade, there are 'TFTP method' and 'File Transmission method through HTTP' as well as Local method that uploads the user's PC.

Select Package Upgraded

Package Version	Current Version	Released Date	Upgraded Date
<input style="width: 80%;" type="text"/>	v1.32	2007.03.16	2007.03.16

Select Upgrade Method

Upgrade Method	Upgrade Server IP
<input checked="" type="radio"/> TFTP	<input style="width: 15%;" type="text"/> . <input style="width: 15%;" type="text"/> . <input style="width: 15%;" type="text"/> . <input style="width: 15%;" type="text"/>
<input type="radio"/> HTTP	<input style="width: 80%;" type="text"/>
<input type="radio"/> Local	<input style="width: 80%;" type="text"/> <input type="button" value="Browse..."/>

Upgrade Image

OS + Firmware
 Config DB
 Log DB

When upgrading a package, the package version to upgrade should be entered like 'v0.19' in the [**Package Version**] field.

For TFTP/HTTP, enter the address of the TFTP/HTTP server and click the [**OK**] button. For Local method, the relevant package file should be existed in the user's PC. Click the [**OK**] button after selecting the file.

In the TFTP/HTTP method, the files of the relevant version are searched automatically and downloaded, but for Local method, the entered version name and file name to upload should be identical.

If Package Version is 'v0.19', the file name is 'gplim-pkg-v0.19.tgz'.



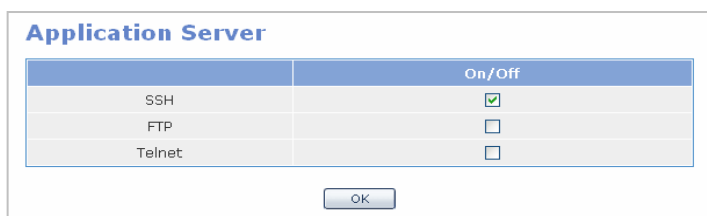
CAUTION

When Deleting Internet Temporary Files

If GSIM package is upgraded, Internet temporary files should be deleted. Select [**Internet Explorer**] → [**Tools**] → [**Internet Options**] menu and click the [**Delete Cookies**] and the [**Delete Files**] buttons in [**Internet Temporary Files**] area. If these files is not deleted, the webscreen of GSIM may not be normally displayed.

Appl Server

The [**Appl Server**] menu is used to manage the services of SSH, FTP and Telnet and it is available to connect to the GPLIM(GPLIMT) board by using these service.



Reboot

The user can reboot the system in the [**Reboot**] menu.



If clicking the [**OK**] button, all services are terminated and the system is rebooted.

The webscreen returns to the initial login window and the webscreen does not operate before the network and service are all executed after rebooting.

Utility

[System] → [Utility] enables to start a ping command and verify the result. The ping is an application program using TCP/IP protocols and inspects whether an IP datagram is received to another host. A program executing the ping transfers an ICMP echo request message to a remote host and waits the response. If the host that receives the ICMP echo request is in operation, it responds to the message. Otherwise, it does not respond to the message. Therefore, by verifying whether an ICMP echo reply is returned, it is available to verify whether a remote host is in use.

Ping

In this page, it is available to set up a ping test. If selecting this item, the following setup window appears. The details by items are as follows:

Category	Configuration
Destination IP Address	<input checked="" type="radio"/> [] . [] . [] . []
	<input type="radio"/> [] . [] . [] . []
	<input type="radio"/> [] . [] . [] . []
Option	
Source Address	[] . [] . [] . []
Packet Size	[]
Retry Count	[]
Time to Live	[]
MTU Discovery Hint	none

Run

- Destination IP Address: Enter the destination IP address for the Ping test. The input of multiple IP addresses requires the test for the IP addresses whose checkboxes are checked. Options are as follows:
 - Source Address: Sets the IP address of the interface for the Ping test.
 - Packet Size: Sets the packet size to be transmitted.
 - Retry Count: Sets the retry count. If it set to '0', there is no retry.
 - Time to Live: Set the TTL value.
 - MTU Discovery Hint: Selects the Path MTU Discovery method.
 - do: Uses PMTU but does not treat. In short, packet fragmentation does not occur.
 - want: Uses PMTU and treats appropriately. In short, if the packet size is

- longer than MTU, the packet fragmentation occurs.
- dont: Does not use PMTU at all. Since it does not set the DF field, the fragmentation may occur in remote site.

If you enter the destination IP and click the **[Run]** button, the Ping test is progressed.

The test is available for only one IP at a time. Select the target IP from the check box. In the default, the IP on the top is marked. The result of the ping test is as follows:

Ping

Category	Configuration
Destination IP Address	<input checked="" type="radio"/> 192 . 168 . 0 . 1
	<input type="radio"/>
	<input type="radio"/>

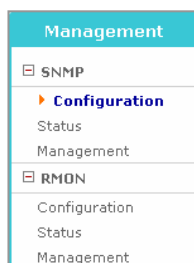
Option	
Source Address	192 . 168 . 22 . 21
Packet Size	128
Retry Count	6
Time to Live	64
MTU Discovery Hint	none

Log
PING 192.168.0.1 (192.168.0.1) from 192.168.22.21 : 128(156) bytes of data.
136 bytes from 192.168.0.1: icmp_seq=1 ttl=64 time=1.85 ms
136 bytes from 192.168.0.1: icmp_seq=2 ttl=64 time=0.657 ms
136 bytes from 192.168.0.1: icmp_seq=3 ttl=64 time=0.653 ms

--- 192.168.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% loss, time 2007ms
rtt min/avg/max/mdev = 0.653/1.055/1.856/0.566 ms

Management

If selecting the [Management] menu of GPLIM(GPLIMT), the submenu of the Management on the top left is displayed as follows:



Menu	Submenu	Description
SNMP	Configuration	Displays the setting items of SNMP.
	Status	Displays the SNMP setting currently configured.
	Management	Starts/Stops the SNMP service.
RMON	Configuration	Displays the setting items of RMON.
	Status	Displays the RMON set currently configured.
	Management	Starts/Stops the RMON services.

SNMP

Configuration

Set SNMP by selecting [SNMP] → [Configuration]. The [SNMP] menu is used to set or monitor the system at a remote site by using the standard SNMP protocol. It enables to interwork with the management system such as NMS. Click the [Save] button to apply the setting to the system. Click the [Reset] button to reset the setting currently set by the user.

System Option

Set SNMP System Option. The [System Option] menu is used for the setting of the basic information to identify each system in the management system. All items of the [System Option] should be filled in with values.

System Option	
Location	<input type="text"/>
Contact	<input type="text"/>
Name	<input type="text"/>
Engine ID	<input type="text"/>

Item	Description
Location	Sets the information on System Location. Ex) Seoul,Korea
Contact	Sets the information on System Contact. Ex) manager@samsung.com
Name	Sets the information on System Name. Ex) ServiceSwitch
Engine ID	Sets the information on System Engine ID. The Engine ID information is used as the information to authenticate the system in SNMPv3.

Community

Add the community used in SNMP v1/2c newly. The community is used to limit the Access authority for the system information in SNMP v1/2c. A user can restrict the network to be accessed depending on community names and assign the access authority for the system management information as Read Only or Read/Write.

Community	
New Community name	<input type="text"/>
Community Network	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> / <input type="text"/>
Access	<input checked="" type="radio"/> Read Only <input type="radio"/> Read Write

Item	Description
New Community name	Sets the target community name.
Community Network	Sets the accessible network for newly added community. A specific IP address, also, can be set.
Access	Sets the access authority as Read Only or Read/Write.

SNMPv3 User Add

Add a user to be used at SNMP v3. The SNMP v3 supports User-based Security Model (USM) and enables to set the access authority for each user as Read Only or Read/Write.

SNMPv3 User Add	
User Name	<input type="text"/>
User Password	<input type="text"/>
Authentication	MD5 ▾
Encryption	None ▾
Access	<input checked="" type="radio"/> Read Only <input type="radio"/> Read Write

Item	Description
User Name	Fills in new user's name to add.
User Password	Fills in new user's password. (More than 8 alphanumeric characters)
Authentication	Sets an authentication method. Both authentication methods, MD5 and SHA, are supported.
Encryption	Sets an encryption method. A user can set the support of DES in the Encryption field.
Access	Sets the access authority as Read Only or Read Write.

Trap Manager

Set IP address to transmit a trap. Up to five addresses can be designated.

Trap Manager	
IP Address	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Community Name	<input type="text"/>

Item	Description
IP Address	Sets new Trap IP Address to add.
Community Name	Sets a community used to transmit to the Trap IP Address to be added.

Status

The menu is used for retrieving the SNMP setting in [SNMP] → [Status]. If clicking the [Delete] button, the item that the user has selected by marking on the check box is deleted. If clicking the [Reset] button, all check boxes are initialized.

SNMP Config Information

Retrieve the SNMP setting. A user can display the information specified in the SNMP Configuration page.

System Information			
Location	Seoul, Korea		
Contact	support@		
Name	GPLIM		
Engine ID	GPLIM		

Select	Community Name	Community Net	Access
<input type="checkbox"/>	private	localhost	Read Write
<input type="checkbox"/>	public	0.0.0.0/0	Read Only

Select	User Name	Access
<input type="checkbox"/>	root	Read Write

Select	Trap IP	Trap Port
<input type="checkbox"/>	192.168.0.123	162

Item	Description
System Information	Displays the information set at System Options.
Select	Selects information to delete.
Community Name	Displays the community name.
Community Net	Displays the established name of the Community Network.
Community Access	Displays the access authority of the established community.
User Name	Displays the established user's name.
Access	Displays the access authority of the established user.
Trap IP	Displays the established Trap IP.
Trap Port	Displays the established Trap Port.

Management

In [SNMP] → [Management], the user can start/stop the SNMP service.
If clicking the [Run] button, the SNMP service starts. If clicking the [Stop] button, the SNMP service stops.

SNMP Management

Start/stop the SNMP service.

Activity	Action
Running	<input type="button" value="Stop"/>

Item	Description
Activity	Displays the operational condition of the current service.
Action	Selects whether to start/stop.

RMON

Configuration

The [RMON] menu is used to display various statistics information putting emphasis on the system monitoring. The information is only managed via NMS. The limited RMON Global setting is possible via Web. In [RMON] → [Configuration], the user can set RMON Global. If clicking the [Save] button, the information that is set by the user is applied to the system. If clicking the [Reset] button, the information that the user is to set is reset.

History Option

Set RMON History Option.

History Option	
MAX History Buckets	<input type="text" value="1000"/> (50 - 5000)
MIN History Interval	<input type="text" value="15"/> min. (1 - 60)

Item	Description
MAX History Buckets	Sets the maximum history storage space.
MIN History Interval	Sets the minimum period of history sample collection.

Event Options

Set RMON Event Option.

Event Option	
MAX Event Logs	<input type="text"/> (50 - 2000)

Item	Description
Max Event Logs	Sets the maximum number of Event Logs.

Status

In [RMON] → [Status], the user can retrieve the setting for RMON Global. If clicking the [Refresh] button, the displayed information is synchronized.

RMON Global Status

Retrieve the SNMP setting.

History Global Status	
MAX History Buckets	1000
Granted History Buckets	0
Used History Buckets	0
MIN History Interval	15 min.

Event Global Status	
MAX Event Logs	400
Saved Event Logs	0

Item	Description
MAX History Buckets	Displays the maximum history storage space that has been set.
Granted History Buckets	Displays the history storage space that is currently allocated.
Used History Buckets	Displays the history storage space that is currently used.
MIN History Interval	Displays the minimum period of history sample collection.
Max Event Logs	Displays the maximum number of logs that are set.
Saved Event Logs	Displays the number of logs that is currently stored.

Management

In [RMON] → [Management], the user can start/terminate the RMON service. If clicking the [Run] button, the RMON service starts. If clicking the [Stop] button, the RMON service stops.

RMON Management

Start/stop the RMON service.

Activity	Action
Stop	<input type="button" value="Run"/>

Item	Description
Activity	Displays the operational status of the current service.
Action	Selects whether to start/stop.



ABBREVIATION

A

ARP Address Resolution Protocol

B

BPDU Bridge Protocol Data Unit

C

CTI Computer Telephony Integration

D

DNS Domain Name Server

G

GPLIM Gigabit PoE LAN Interface Module

GVRP GARP VLAN Registration Protocol

H

HTTP Hypertext Transfer Protocol

I

IGMP Internet Group Management Protocol

L

LAN Local Area Network

M

MAC Media Access Control

N

NAT Network Address Translation

NTP Network Time Protocol

P

PD Powered Device

PoE Power Of Ethernet

PVC Permanent Virtual Circuit

PVID Port VLAN Identification

Q

QoS Quality of Service

R

RMON Realtime Monitoring

RSTP Rapid Spanning Tree Protocol

S

STP Spanning Tree Protocol

SNMP Simple Network Management Protocol

T

TFTP Trivial File Transfer Protocol

V

VLAN Virtual Local Area Network

VoIP Voice Over IP

OfficeServ 7400
GPLIM(GPLIMT) User Guide

© 2005~2007 Samsung Electronics Co., Ltd.
All rights reserved.

Information in this Manual is proprietary to SAMSUNG
Electronics Co., Ltd.

No information contained here may be copied, translated,
transcribed or duplicated by any form without the prior written
consent of SAMSUNG.

Information in this Manual is subject to change without notice.

