SAMSUNG

Enterprise IP Solutions

OfficeServ 7400

GPLIM User Manual

Samsung Telecommunications

Publication Information

SAMSUNG TELECOMMUNICATIONS AMERICA reserves the right without prior notice to revise information in this publication for any reason. SAMSUNG TELECOMMUNICATIONS AMERICA also reserves the right without prior notice to make changes in design or components of equipment as engineering and manufacturing may warrant.

Trademarks

Enterprise IP Solutions
OfficeServ™ is a trademark of SAMSUNG Telecommunications America, L.P.
WINDOWS 95/98/XP/2000 are trademarks of Microsoft Corporation.

PRINTED IN USA

INTRODUCTION

Purpose

This document introduces the OfficeServ 7400 GPLIM and describes the procedures for installing and using this module.

Document Content and Organization

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

CHAPTER 1. Overview of OfficeServ 7400 GPLIM

This chapter briefly introduces the OfficeServ 7400 GPLIM.

CHAPTER 2. Installing OfficeServ 7400 GPLIM

This chapter describes the installation procedure and login procedure.

CHAPTER 3. Using OfficeServ 7400 GPLIM

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

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 General 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 Programming Manual

The OfficeServ 7400 Call Server Programming Manual describes the method of using the Man Machine Communication (MMC) program that changes system settings by using phones.

Revision History

EDITION	DATE OF ISSUE	REMARKS
00	05. 2006	Initial Release

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, 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 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 may not be normally displayed.

TABLE OF CONTENTS

CHAPTER 1. Overview of OfficeServ 7400 GPLIM

This chapter introduces OfficeServ 7400 system and OfficeServ 7400 GPLIM.

Introduction to OfficeServ 7400

The OfficeServ 7400 is a single platform that delivers the convergence of voice, data, wired and wireless communications for small and medium offices. The 'office in a box' solution offers TDM voice processing, voice over IP integration, wireless communications, voice mail, computer telephony integration, data router and switching functions, all in one powerful platform.

With the GWIM, GPLIM and GSIM modules, the OfficeServ 7400 provides network functions such as a gigabit switching, Power Over Ethernet, high speed data routing, and network security in a single converged solution.

This document describes the data and switching capabilities of OfficeServ 7400 GPLIM.

Structure of OfficeServ 7400

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

Introduction to OfficeServ 7400 GPLIM

OfficeServ 7400 provides the following functions:

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.

Management Function

- Configuration and verification functions for the operations of GPLIM functional block via a browser
- Configuration and verification functions for the operations of GPLIM 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

CHAPTER 2. Installation of OfficeServ 7400 GPLIM

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

Installing

OfficeServ 7400 GPLIM software is pre-installed. The software package is composed of the following items described below:

Package	File	Description
Bootrom Package	gplim-bootldr.img-vx.xx gplim-bootldr.img-vx.xx.sum	Boot ROM program
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.

GPLIM Installation

1. Insert the GWIM into an open slot in the OfficeServ 7400 cabinet.

2. Connect a PC to port #1 of the GWIM module. You will need to configure your TCP/IP settings to match the corresponding default IP address of the GPLIM shown in step 3.

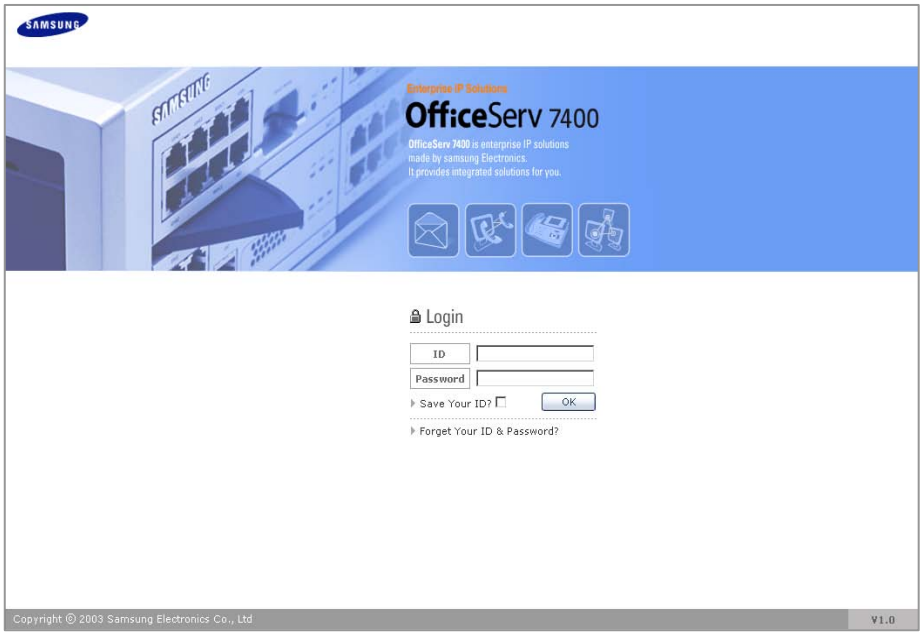
3. Using Internet Explorer navigate to one of the folling IP addresses to access the management interface of the GPLIM. The default IP address of the GPLIM board is 10.0.4.1/24.

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. Other web browsers are not supported.

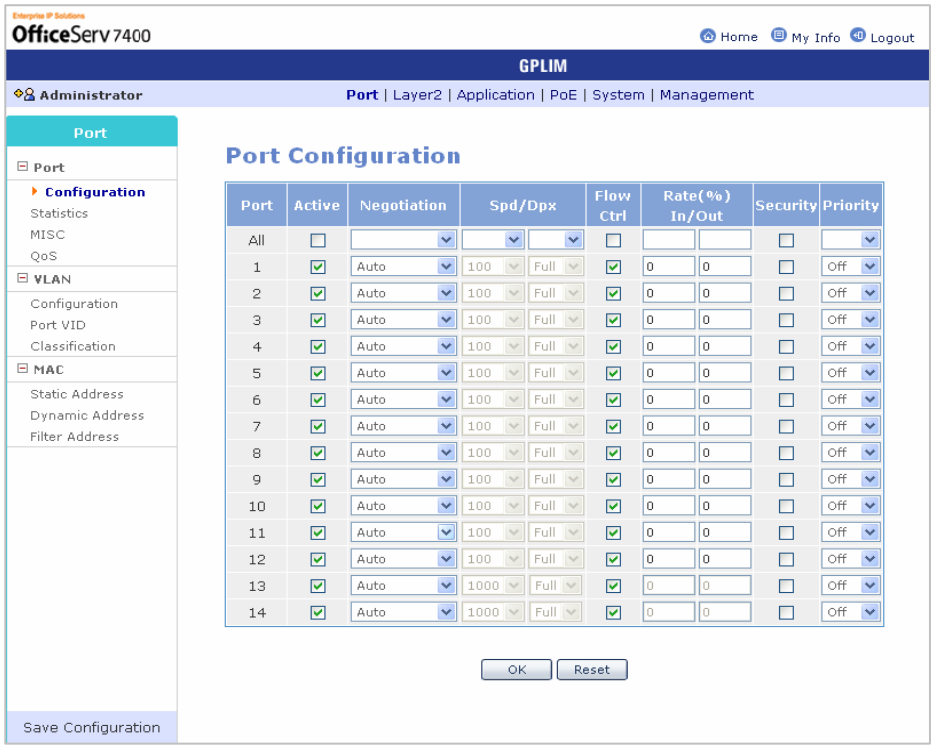
Getting Started

1. Start Internet Explorer and enter the IP address of the GPLIM into the address bar. The login window shown below will appear.



2. Log in using the administrator ID and password. The following window will appear. The GPLIM 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 a more detailed method of each menu, refer to 'Chapter 3. Using OfficeServ 7400 GPLIM'.

*(The default administrator name is "**admin**" and the default password is "**root**".)*

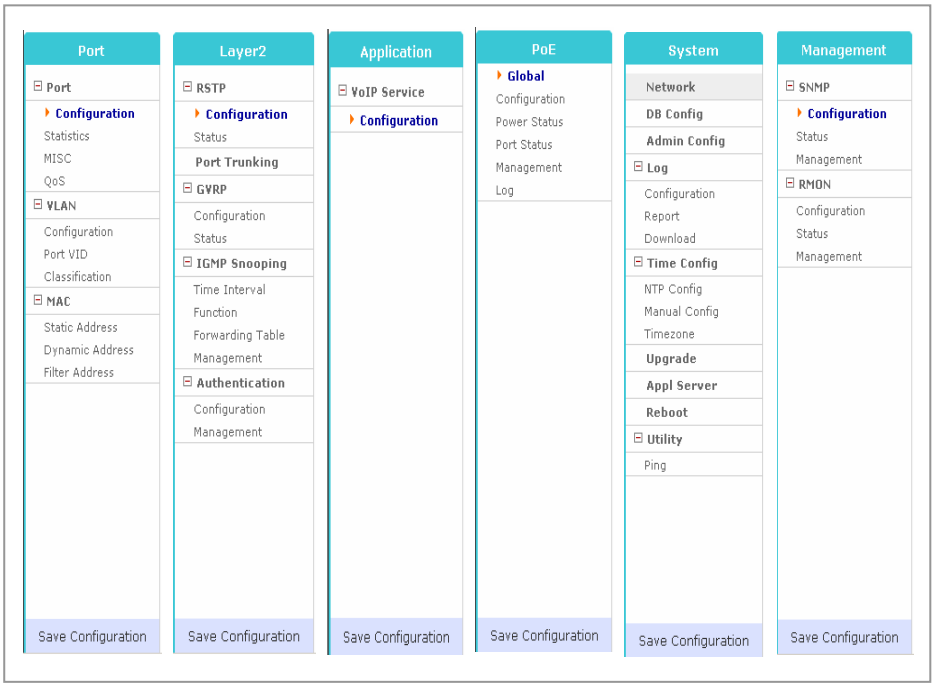


3. Click the **[Logout]** button on the upper section of the screen to close the connection to the GPLIM.

CHAPTER 3. Use of OfficeServ 7400 GPLIM

This chapter describes the menus of OfficeServ 7400 GPLIM.

The OfficeServ 7400 GPLIM menus are arranged as shown to below:



Port

Select the **[Port]** menu. The submenus will be displayed in the upper left side 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.

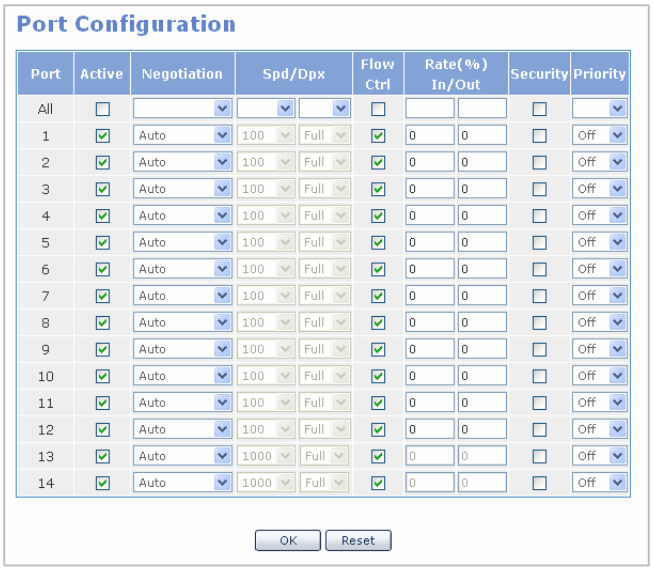
Menu	Submenu	Description
MAC	Static Address	Stores a MAC address to the static address table.
	Dynamic Address	Retrieves a floating address table or deletes a MAC address.
	Filter Address	Enters a MAC address and sets to filter the frame data that has the same MAC address information with the entered 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 retrieve information on the ports in the **[Port]** menu.

Configuration

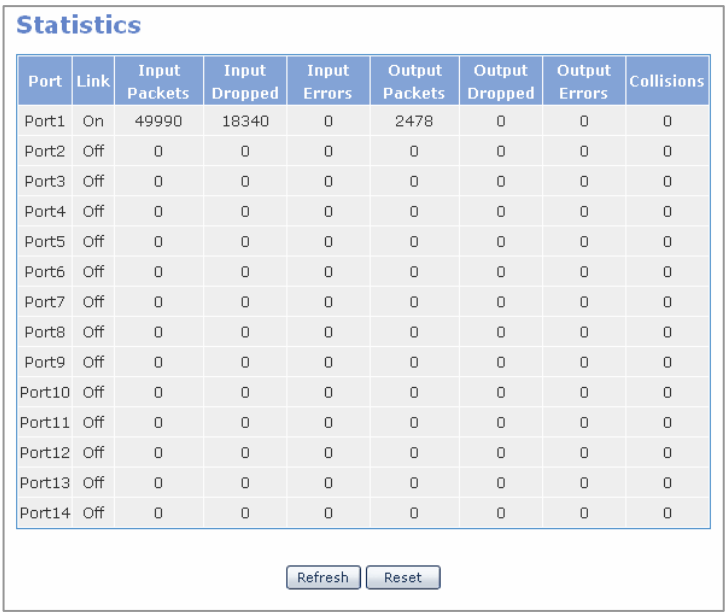
This table allows the user to set the configuration of the switch ports in the **[Port]** → **[Configuration]** menu.



Item	Description
Port	There are14-switch ports. All ports can be processed at once through the ‘All’ item.
Active	Sets whether to use a port or not.
Negotiation	- Auto: Adjusts the speed through a negotiation with the counterpart. - Force: Sets the speed without a negotiation with the counterpart. Set the negotiation item as ‘Force’ If setting the Duplex item as ‘Full’.
Speed/Dpx	- Speed: Ports 1-12 can be set to 10/100 Mbps. Ports 13-14 are 1000 Mbps only. - Duplex(Dpx): Select Set Full(two-way service) or Half(one-way service). Ports 13-14 are Full Duplex Only.
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	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. It is available to set Priority when the QoS mode is not First Come First Service (FCFS) in the **[Port]** → **[QoS]** menu.

Statistics

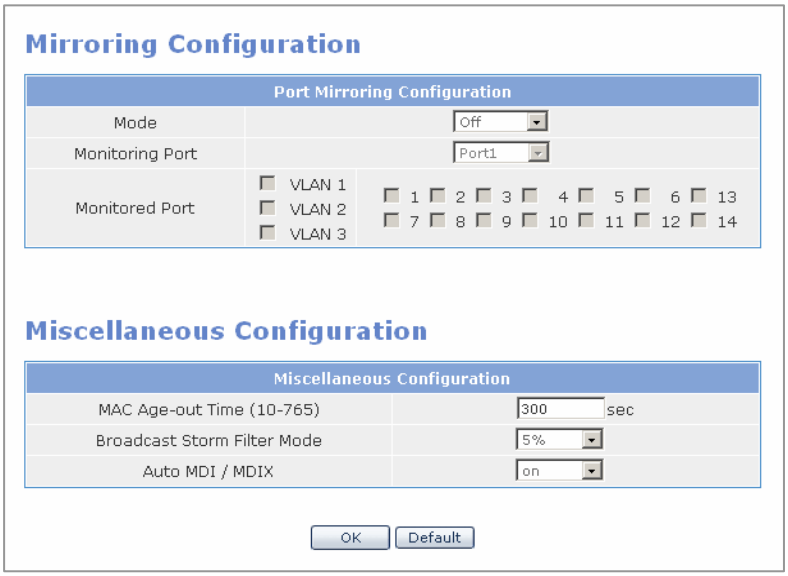
The user can retrieve the link status and statistics for each port on the switch in the **[Port]** → **[Statistics]** menu. Clicking the **[Reset]** button, will reset all statistics to '0'.



- Input Packets: Number of packets received
- Input Dropped: Number of packets that are received but dropped without successfully being switched
- Input Errors: Number of errored packets received
- Output Packets: Number of packets are transmitted
- Output Dropped: Number of packets that are transmitted but dropped
- Output Errors: Number of packets that are transmitted to the port that encountered errors
- Collisions: Number of times that a collision occurs between a packet received to the port and a packet transmitted with being switched

MISC

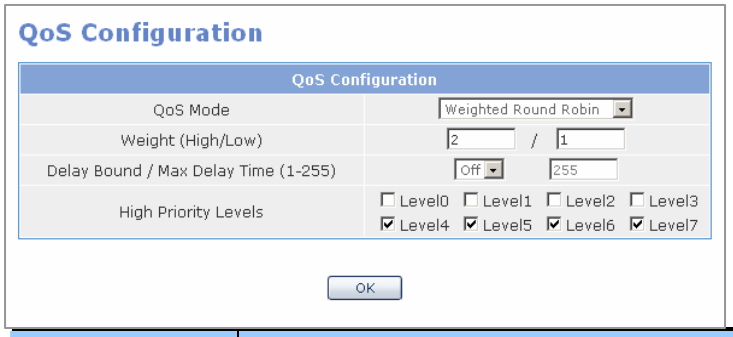
[Port] → **[MISC]** menu.



Item	Description
Mode	Sets the use of 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, this means a connection to a PC for monitoring.
Monitored Port	Assigns a port where the monitoring wil be performed. The monitoring port and the monitored port cannot be the same port.
MAC Age-Out Delay Bound	Sets the duration that a MAC address remains in the address table. The default is 300 seconds. If the LAN Port connection is released, the MAC address is deleted immediately.
Broadcast Storm Filter Mode	The switch buffer can be set to 5, 10, 15, 20 and 25 % load. If this value is exceeded, the broadcast packet will be discarded.
Auto MDI/MDIX	Automatic sensing of the direct/cross cable. This feature can be disabled by setting it to ‘Off”.

QoS

[Port] → **[QoS]** menu.



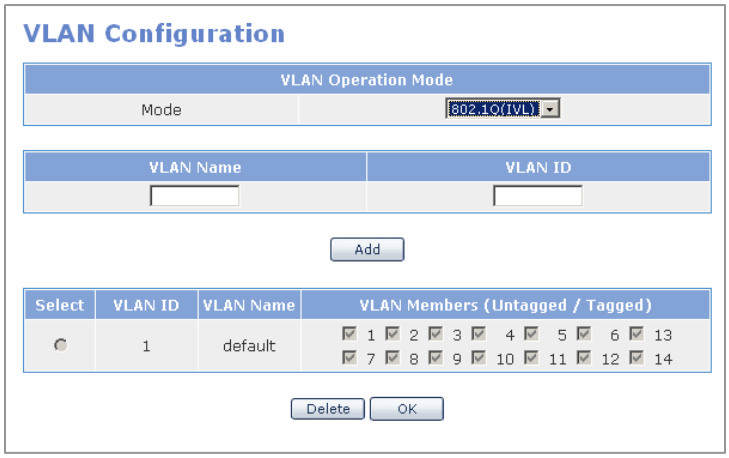
Item	Description
QoS Mode	Select the QoS mode. - First Come First Service: Packets are transmitted according to there incoming order.(QoS function not used) - All High before Low: Method that a packet that has higher priority is transmitted prior to a packet that has lower priority than that packet. 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.
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 will be processed preferentially.
High Priority Levels	There are 8 tags to indicate priority. 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. The GPLIM processes priority by separating the two Queues, 'High' and 'Low'.

VLAN

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

Configuration

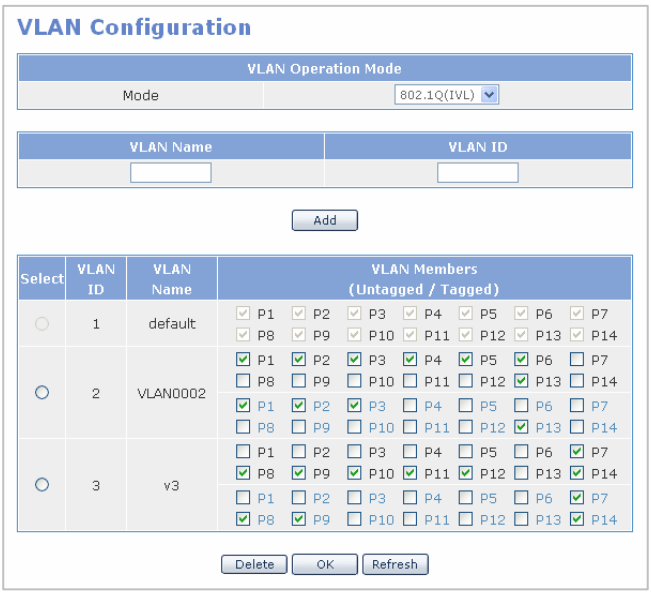
[VLAN] → [Configuration]



VLAN mode is classified using four VLAN configuration methods depending on the selected mode.

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

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

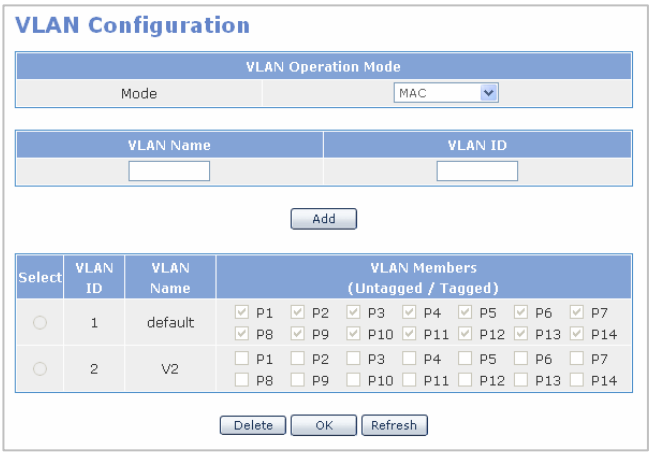


- VLAN Untagged Members: Select a port that will send the Ethernet frame that deletes TCI information when a port is switched and data is sent ranging from 1 to 14 ports. Connect to a terminal that does not support IEEE 802.1Q to configure tagged VLAN.
- VLAN Tagged Members: Select a port that will send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

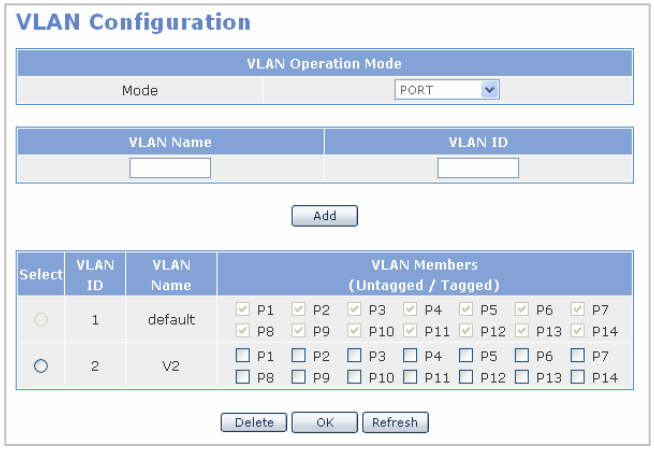
VLAN is configured for each MAC address. VLAN is configured without information on port and the number of a VLAN member may change. Up to 256 MAC members can be saved either in a single VLAN or in multiple VLANs.
Since a MAC Based VLAN does not basically contain port information, the port serves as a 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.



Port Based VLAN

This option is used to configure the VLAN on a 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.



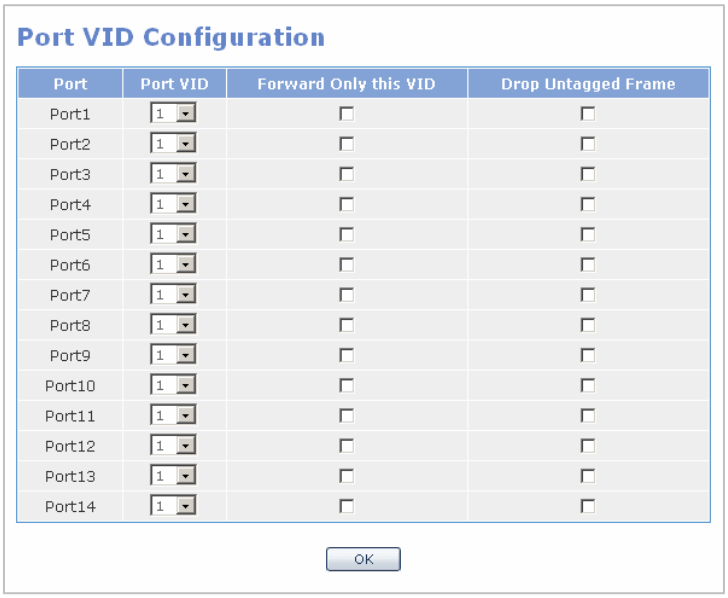
802.1Q (SVL)

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

[Port VID]



Item	Description
Port VID	- 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

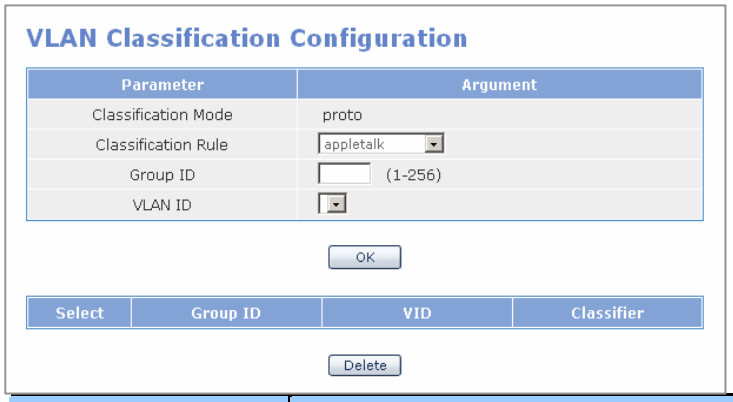
Port VID Input Value

Below 255 can be entered for Port VID.

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.

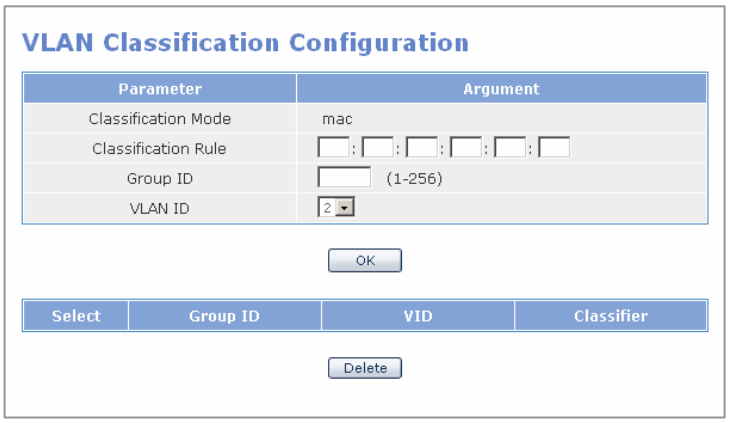


Item	Description
Classification Mode	Selected automatically according to the VLAN mode. In case of 802.1Q VLAN, 'proto' is selected. In case of MAC Based VLAN, 'MAC' is selected.
Classification Rule	Based on Appletalk, arp, decnet, ip, ipx, sna, and x25, VLAN is set.
Group ID	Group the selected protocol. 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.



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.

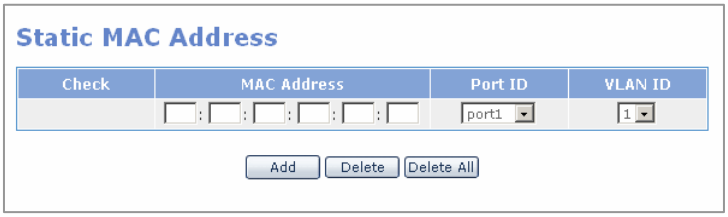
Select a Group ID from **[Select]** and click the **[Delete]** button to delete the group ID.

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.



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.

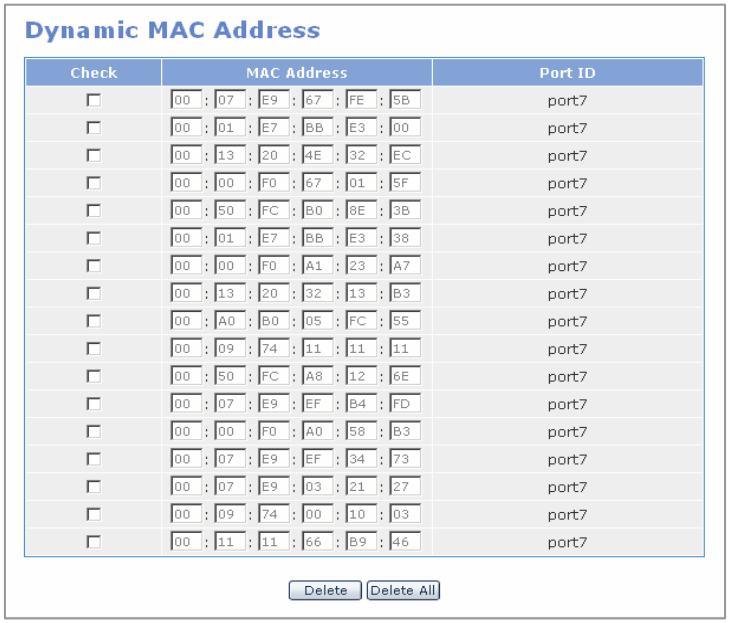
NOTE

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.

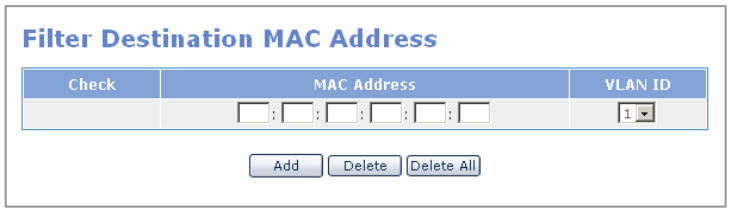


Filter Address

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.



Layer2

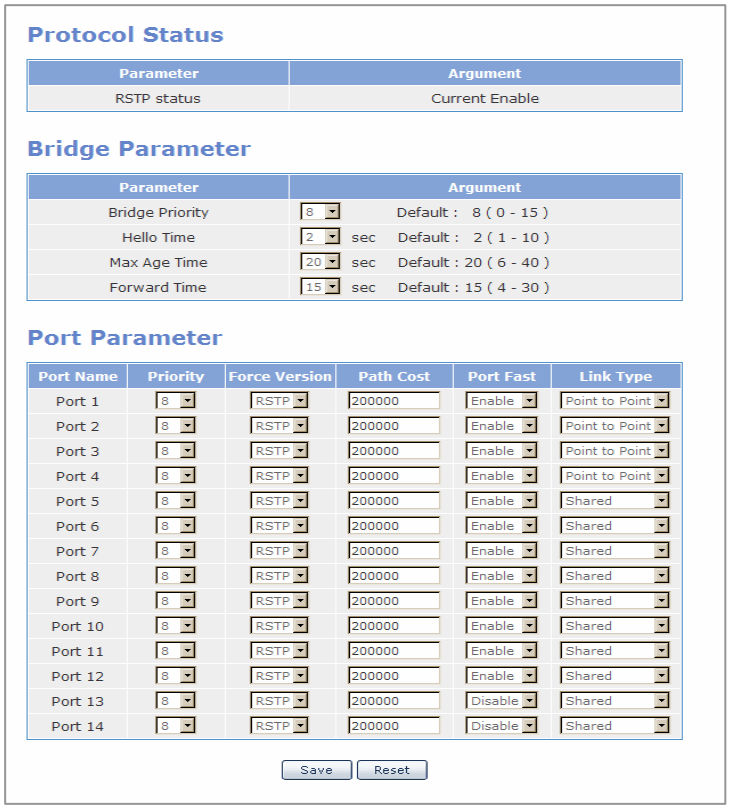
Select the **[Layer2]** menu. The submenus will be displayed in the upper left side of the window as follows:

Menu	Submenu	Description
RSTP	Configuration	Sets bridge and port environment used in RSTP.
	Status	Retrieves the RSTP operation status of the switch.
Port Trunking	-	Sets Port Trunking related value in menu.
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

Configuration

[RSTP] → [Configuration]

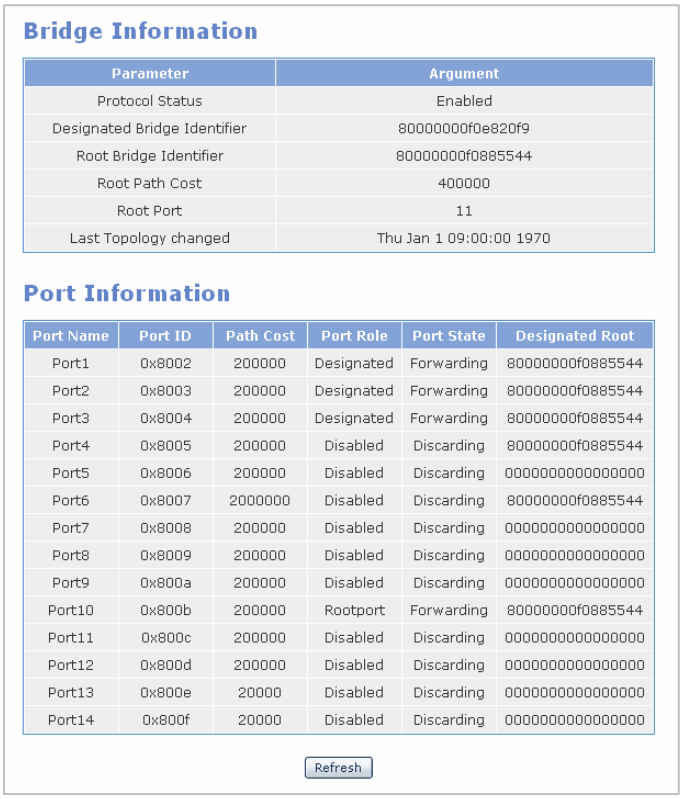


Item	Description
Protocol Status	Displays the current status of the RSTP protocol.
Bridge Parameter	Configures the Bridge parameter of the switch that RSTP operates. - Bridge Priority: Decides the priority of Bridges. - Hello Time: Sets the transmission cycle of BPDU. - Max Age Time: Sets the Message Age time. - Forward Time: Displays the time that the state of each port is changed by level.(Discarding-Learning-Forwarding)

Item	Description
Port Parameter	- 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

[RSTP] → **[Status]** to display the status of switch RSTP operation.



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

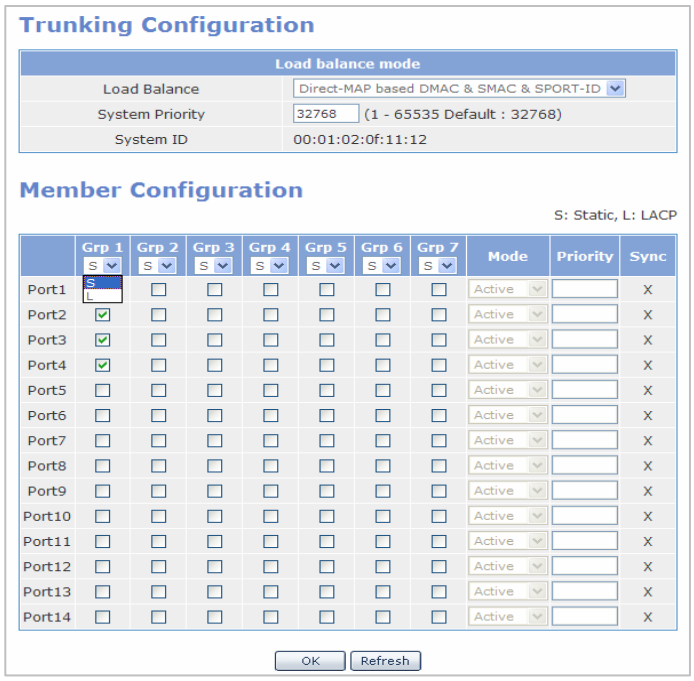
Refresh

- 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 Trunking

[Port Trunking] → [Configuration]



Trunking Configuration

Item	Description
Load Balance	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. The default is Direct-MAP based DMAC & SMAC & SPORT-ID. - 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 anther group simultaneously.

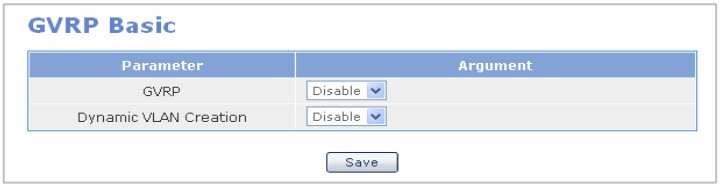
Item	Description
Mode	Displayed when selecting the trunk configuration as 'LACP'. It is available to select one of 'Active/Passive'. For the Active, a LACP packet is transferred to the opposite party first, based on the system. For the Passive, it is responded only when receiving a packet from the opposite 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

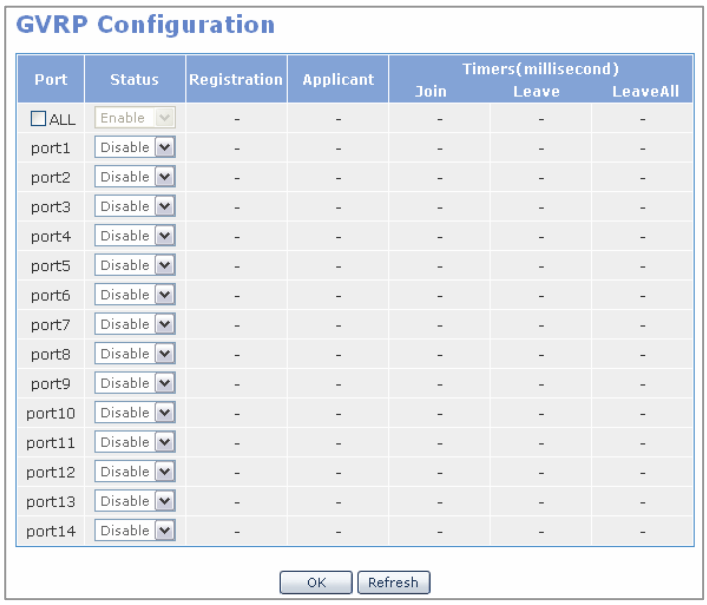
The **[GVRP]** menu is used to start or stop the GVRP service, or modify the GVRP service for each port.

Configuration

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



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.

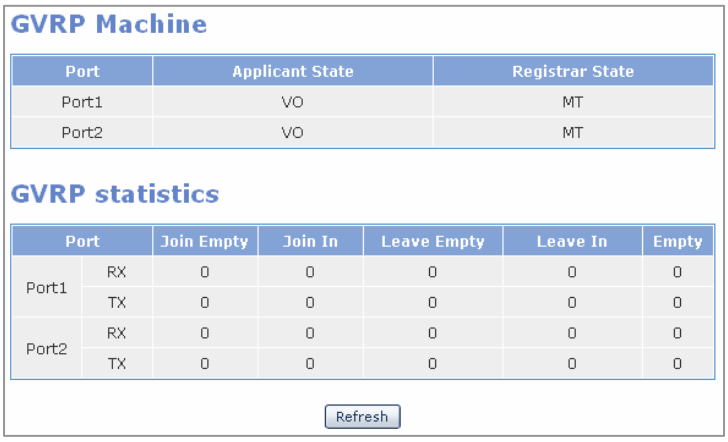


Click the **[OK]** button to save the information of each port and click the **[Refresh]** button. Then, the latest information of the port is displayed.

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

Item	Description
Port	Port Number
Applicant State	Current Status of Applicant State Machine
Register State	Current Status of Register State Machine

GVRP Statistics

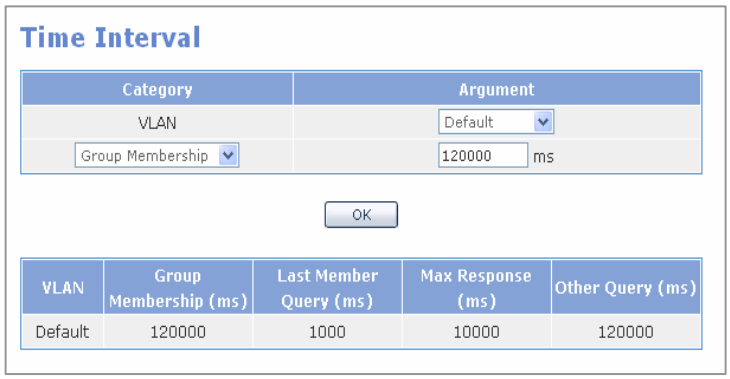
Item	Description
Port	Port Number
Join Empty	Number of Join Empty packets
Join In	Number of Join In packets
Leave Empty	Number of Leave Empty packets
Leave In	Number of Leave In packets
Empty	Number of Empty packets

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.

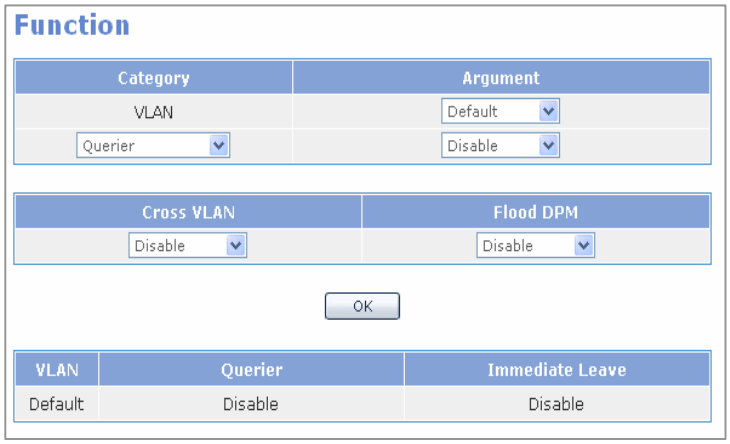


Categories	Description
VLAN	Selects the VLAN to be configured.
Group Membership	Configures the time to exit from the multicast forwarding database list when new report does not exist.
Last Member Query	Indicates the time to wait a response report after sending a query to check if the host is the last 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 doest 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.



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.

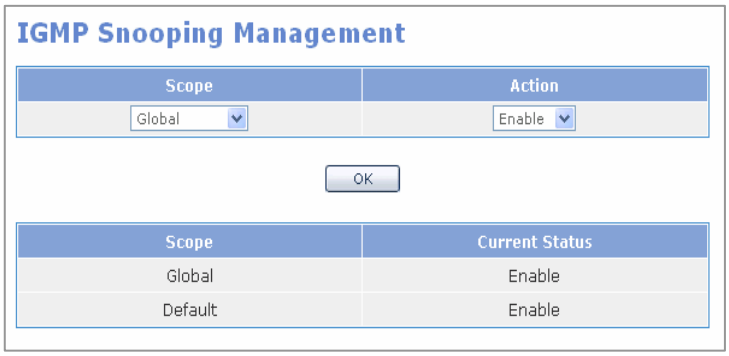
Forwarding Table

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

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.



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

NOTE

IGMP Snooping Management

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

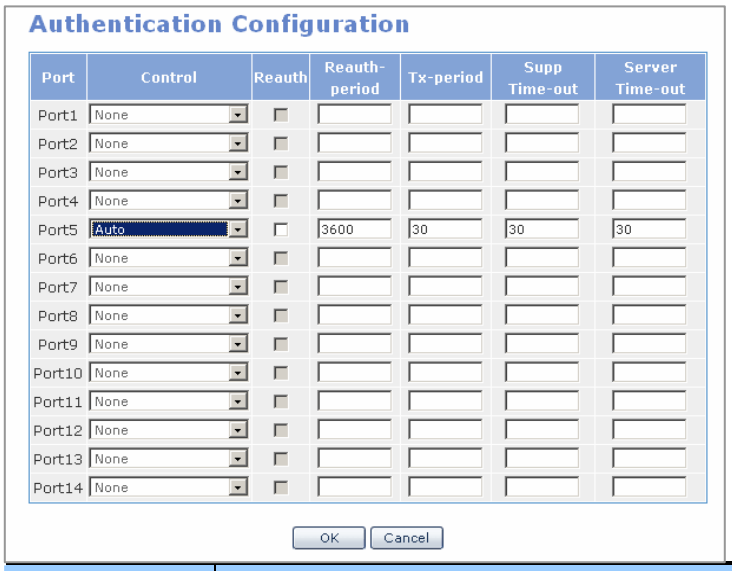
Authentication

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:

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



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 cycle that sends Request regularly to supplicant. (1-65535sec) default: 30 sec

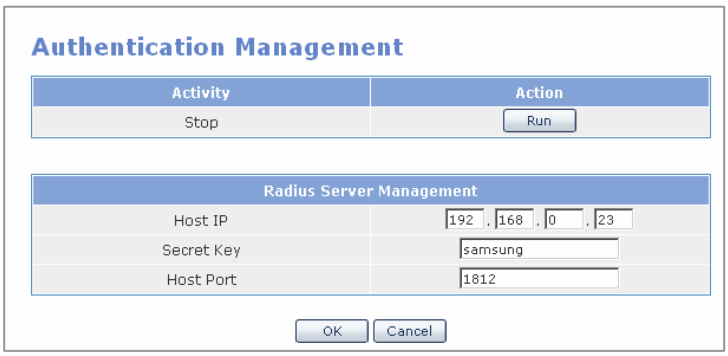
Item	Description
Supp-Timeout	Indicates the time before re-sending to the user when EAP is requested.(1-65535sec) default: 30 sec
Sever-Timeout	Indicates the time before re-sending to the device when server authentication of a server is requested.(1-65535sec) default: 30 sec

Re-authentication setting and the cycle setting are applied only when setting is changed because there is default value.

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.



Application

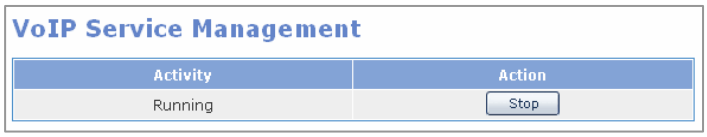
Select the **[Application]** menu. The submenus will be displayed in the upper left side of the window as follows:

VoIP Service

This menu is used to set VoIP service environment.

Management

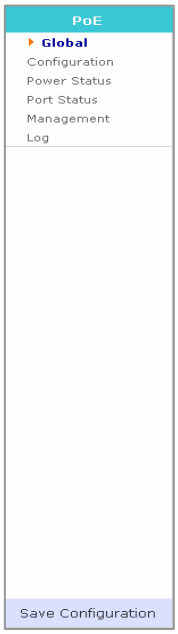
The [Management] menu enables to start or stop the VoIP service function. Although the system is rebooted, the setup is restored to the last status.



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. The submenus will be displayed in the upper left side of the window as follows:



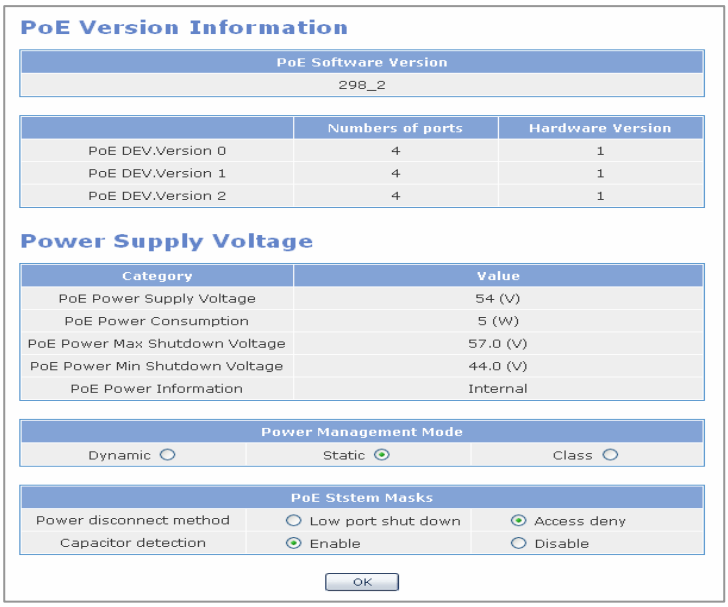
Menu	Submenu	Description
PoE	Global	Sets or retrieves the PoE version information and power supply information.
	Configuration	Sets or retrieves the power information of each port.
	Power Status	Displays the PoE power supply status in real time.
	Port Status	Displays the PoE port status in real time.
	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.



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

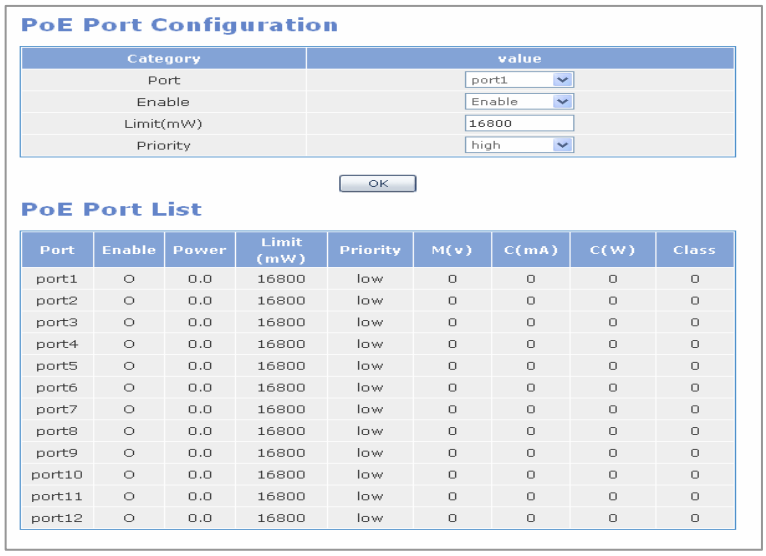
PoE System Masks decides the disconnection method of the power and whether to execute Capacitor Detection.

Item	Description
Power Disconnect Method	- 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	- 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.

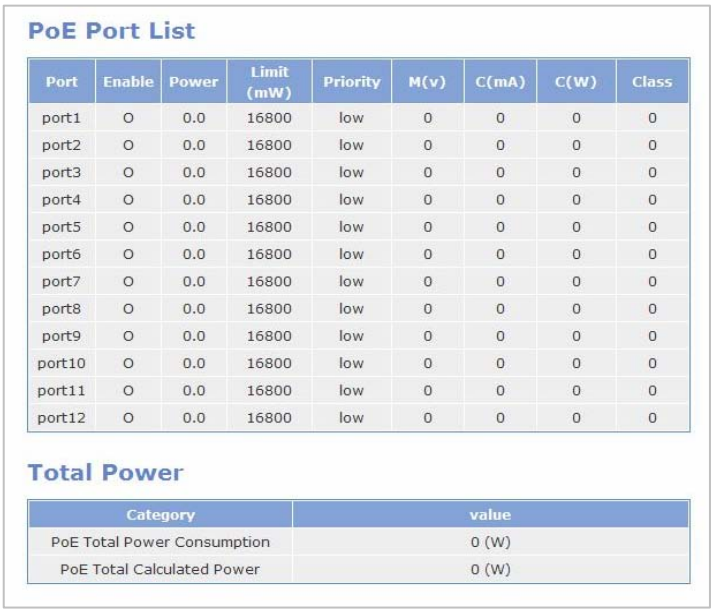


Item	Description
Port	Indicates the Ethernet port 1~12 of a device.
Enable	Sets or releases the PoE power supply of the target port.
Limit(mW)	If the Power Management Mode is set to Static, the power limit of each port. Up to 1000~18900 mW can be set.
Priority	Indicates the priority setting of the power.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

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	O	0.0	16800	low	0	0	0	0
port2	O	0.0	16800	low	0	0	0	0
port3	O	0.0	16800	low	0	0	0	0
port4	O	0.0	16800	low	0	0	0	0
port5	O	0.0	16800	low	0	0	0	0
port6	O	0.0	16800	low	0	0	0	0
port7	O	0.0	16800	low	0	0	0	0
port8	O	0.0	16800	low	0	0	0	0
port9	O	0.0	16800	low	0	0	0	0
port10	O	0.0	16800	low	0	0	0	0
port11	O	0.0	16800	low	0	0	0	0
port12	O	0.0	16800	low	0	0	0	0

Total Power

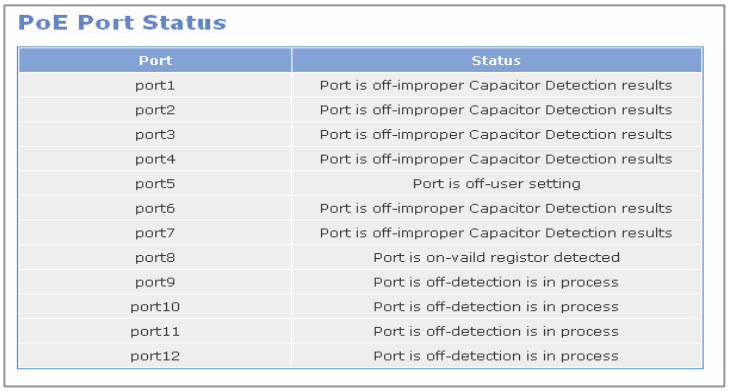
Category	value
PoE Total Power Consumption	0 (W)
PoE Total Calculated Power	0 (W)

Item	Description
Port	Indicates the Ethernet port 1~12.
Enable	Sets or releases the PoE power supply to 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 on each port can be set from 1000mW to 18900 mW.
Priority	Sets the power priority of the port.
M(v)	Total voltage provided.

Item	Description
C(mA)	Calculated current (Displays the **C(mA)** of the target port.)
C(W)	Power consumption (Displays the **C(W)** 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.

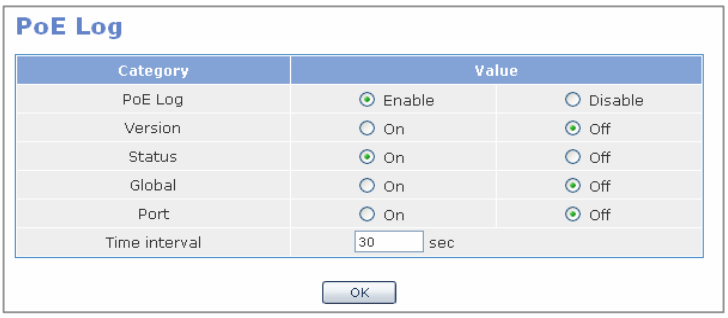


Item	Description
Port	Indicates the Ethernet port 1~12 of a device.
Status	Indicates the current PoE information of that port.

Management

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

Log
[PoE] → [Log]



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. The submenus will be displayed in the upper left side of the window as follows:

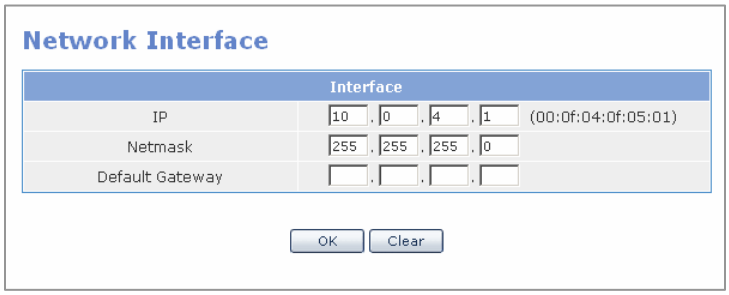
Menu	Submenu	Description
Network	-	Sets IP and DNS services.
DB Config	-	Saves DB and change to the basic DB or user DB.
Admin Config	-	Sets for the management authentication.
Log	Configuration	Sets to determine whether to leave the log for each item.
	Report	Retrieves the system log currently stored.
	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.
Upgrade	-	Upgrades the GPLIM 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

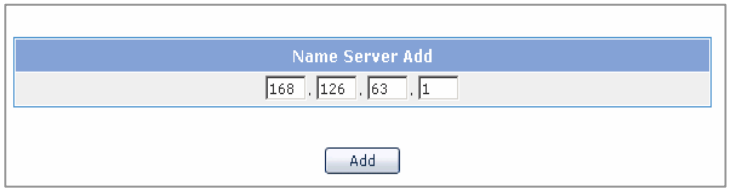
This menu is used to set GPLIM IP address and Netmask and set whether to use interface.
Select the target item and click the **[OK]** button.
IP default value of the GPLIM board is set to 10.0.4.1/24.



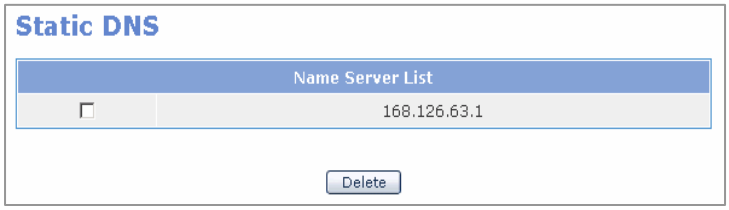
Item	Description
IP	Sets network IP.
Netmask	Sets Netmask.
Default Gateway	Sets default gateway IP.

DNS

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

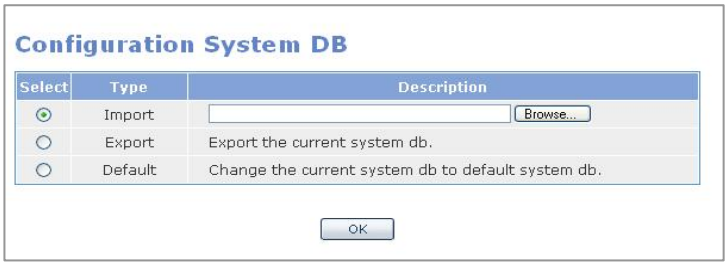


Set the IP corresponding to the DNS server and click the **[Add]** button.
Then, the setting is directly applied to the <**Static DNS**> window of **[Interface]** → **[DNS]**.
For example, when DNS is entered as shown in the figure above, the <**Static DNS**> window is displayed as follows:



DB Config

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

CAUTION

DB Change

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

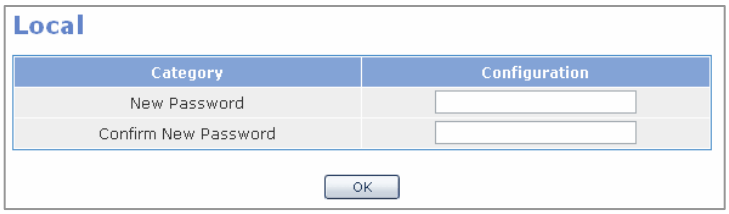
Admin Config

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.

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+]**.

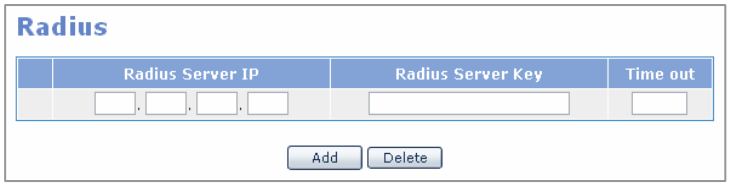
Local

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



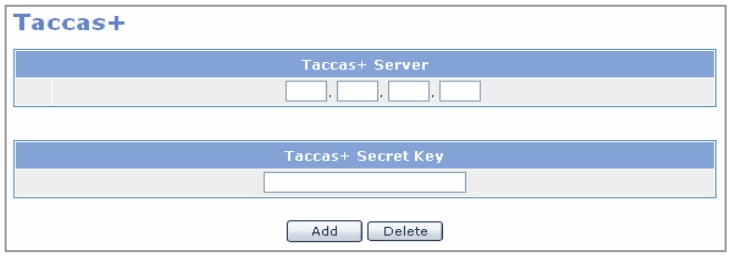
Radius

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.



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.



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.

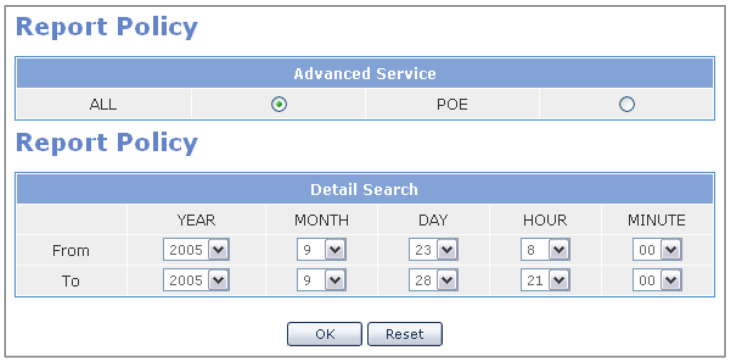
Configuration

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

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.

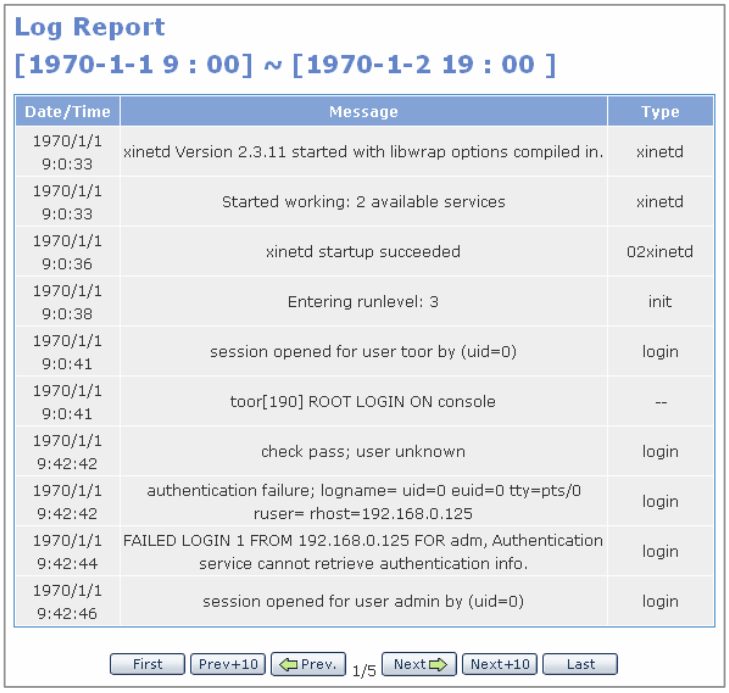
Log Report

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



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.

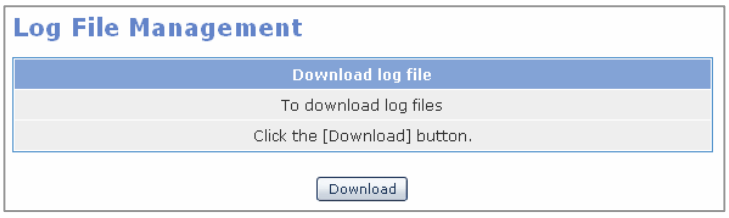
- ALL: All logs including POE
- POE: Log related with POE



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.



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

Time Config

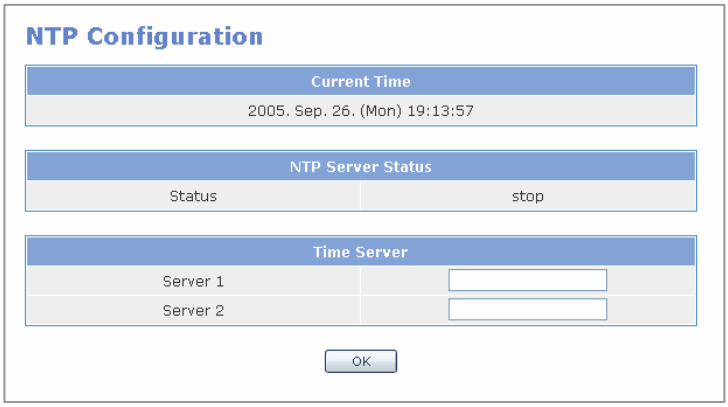
Synchronize the timezone, date and time of the system through a network or sets the values by itself.

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.)

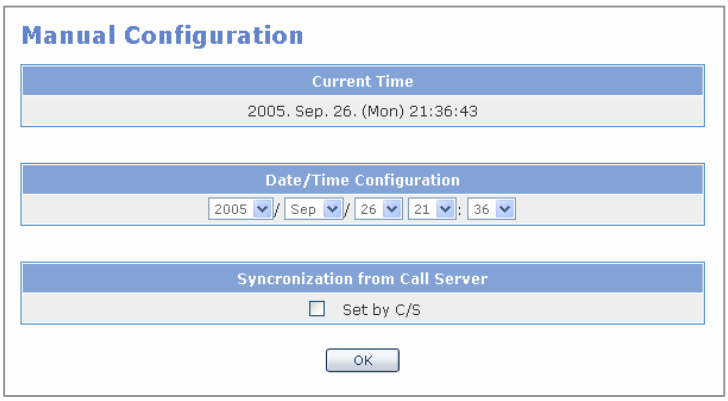
If registering Time Server, click the **[OK]** button to start or restart NTP demon.



Manual Config

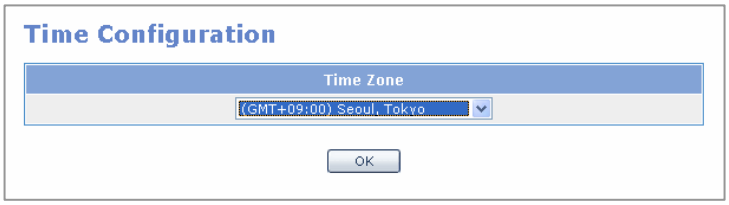
[Time Configuration] → **[Manual Config]** menu is used to set and modify the date and time of the system to the time that the user wants. If clicking the **[OK]** button after selecting date and time that the user wants in the table of Date/Time Configuration, the date and time of the system is changed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



Timezone

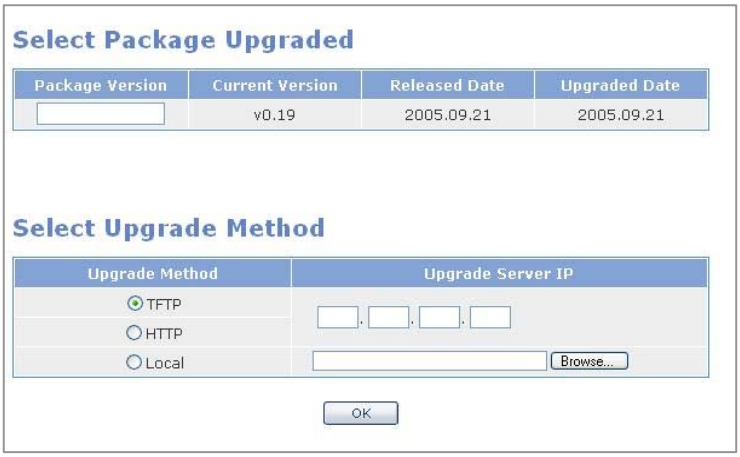
[Time Configuration] → **[Timezone]** menu is used to change the timezone by selecting the timezone related to the user.
Select the desired area(city or GMT) in the areas by GMT and click the **[OK]** button to modify the timezone information of the system.



Upgrade

[Upgrade] Upgrade the Kernel and Ramdisk in the 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.



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

[Appl Server] menu is used to manage the SSH, FTP and Telnet services.

Reboot

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

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

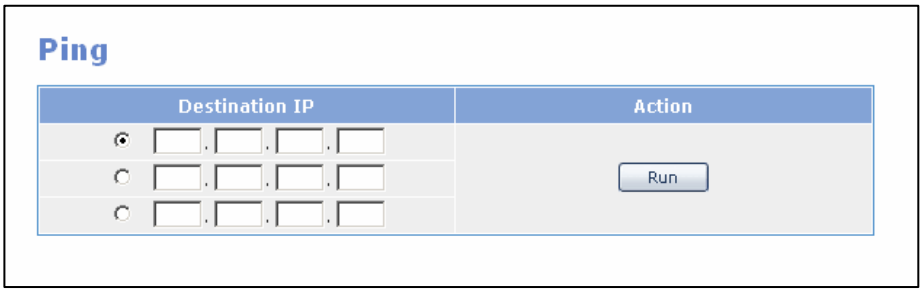
The webscreen returns to the initial login window and the webscreen does not operate before the network and service are all executed after rebooting.

Utility

[System] → [Utility]

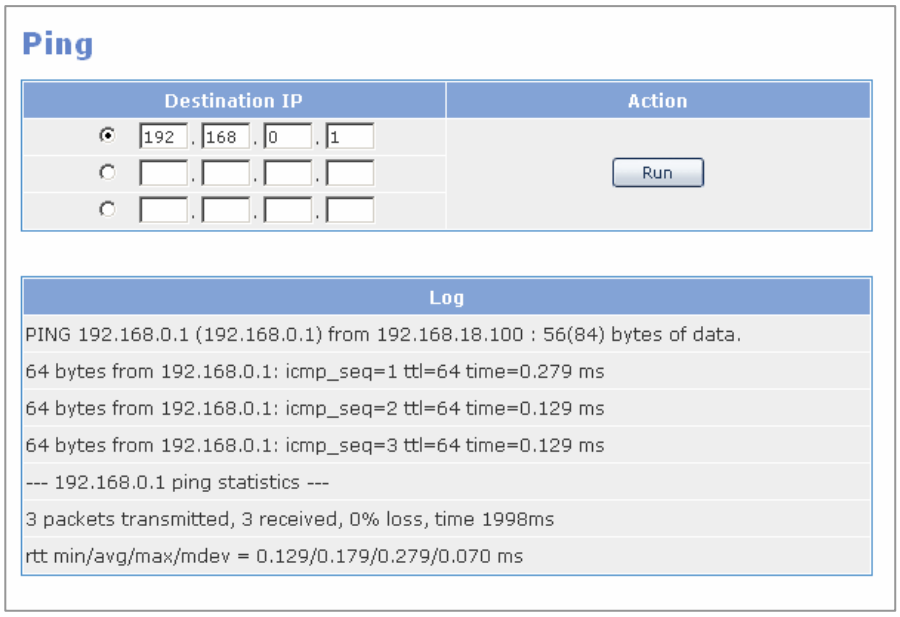
Ping

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:



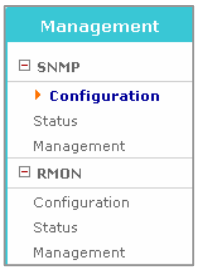
For **[Destination IP]**, the destination address of a remote host is entered to verify the communication. If entering the **[Destination IP]** and clicking the **[Run]** button, the ping test is operated.

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:



Management

Select the **[Management]** menu. The submenus will be displayed in the upper left side of the window as follows



Menu	Submenu	Description
SNMP	Configuration	Displays of the SNMP global information.
	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.

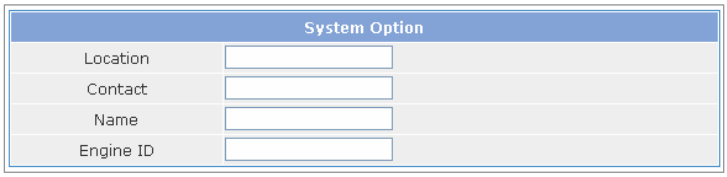
SNMP

Configuration

[SNMP] → [Configuration]

System Option

Set SNMP System Information.



Item	Description
Location	Sets the System Location information.
Contact	Sets the System Contact.
Name	Sets the System Name.
Engine ID	Sets the System Engine ID.

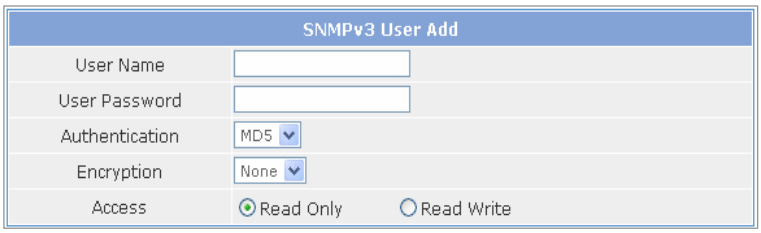
Community

Add the community used in SNMP v1/2c.

Item	Description
New Community name	Sets the target community name.
Community Network	Sets the target community network.
Access	Sets the target access authority.

SNMPv35 User

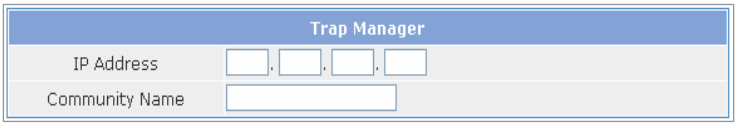
Add a SNMP v3 user.



Item	Description
User Name	New user's name to add.
User Password	New user's password.
Authentication	Sets authentication method.
Encryption	Sets encryption method.
Access	Sets access authority.

Trap Manager

Set Trap Manager IP address. Up to five addresses can be assigned.



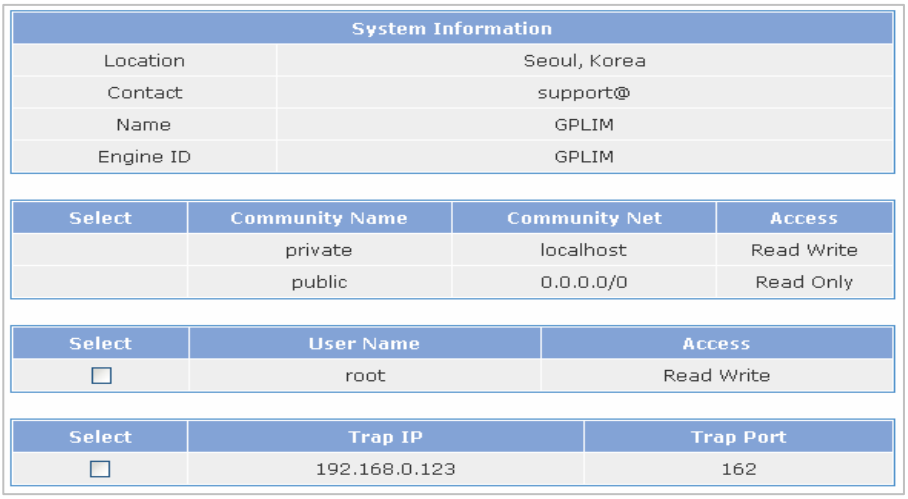
Item	Description
IP Address	Sets new IP Address for the Trap
Community Name	Sets a community used to transmit to the Trap IP Address.

Status

[SNMP] → [Status]

SNMP Config Information

Retrieve the SNMP setting.



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

Select	Community Name	Community Net	Access
	private	localhost	Read Write
	public	0.0.0.0/0	Read Only

Select	User Name	Access
☐	root	Read Write

Select	Trap IP	Trap Port
☐	192.168.0.123	162

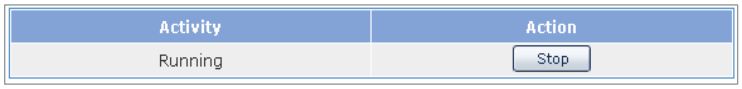
Item	Description
System Information	Displays the information set in System Options.
Select	Selects information to delete.
Community Name	Displays the community name.
Community Net	Displays the established name of the Community Network.
Community Access	Displays the access authority of the established 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

[SNMP] → [Management]

SNMP Management

Start/stop the SNMP service.



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

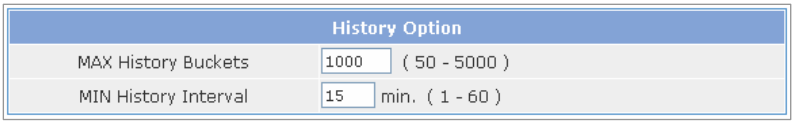
RMON

Configuration

[RMON] → [Configuration

History Option

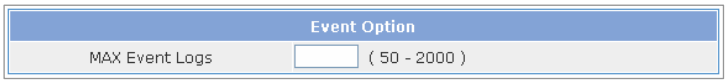
Set RMON History Option.



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

Event Options

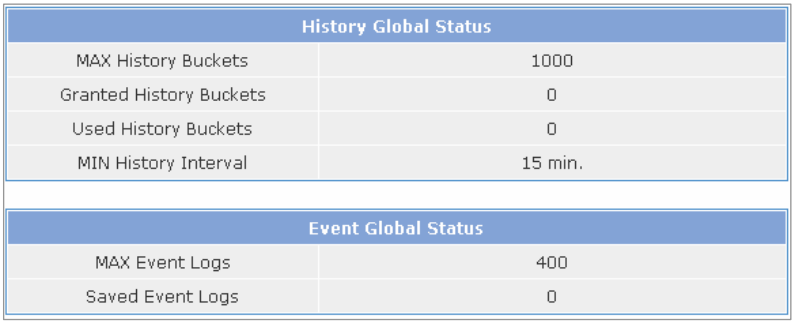
Set RMON Event Option.



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

Status

[RMON] → [Status]



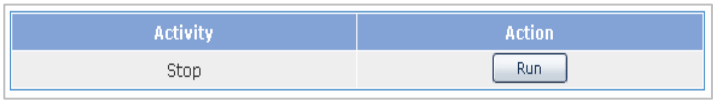
Item	Description
MAX History Buckets	Displays the maximum history storage space.
Granted History Buckets	Displays the allocated history storage space.
Used History Buckets	Displays the history storage space that is currently used.
MIN History Interval	Displays the minimum history interval time.
Max Event 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.

RMON Management

Start/stop the RMON service.



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 Etnernet
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