Enterprise IP Solutions

OfficeServ 7400

GPLIMT/GPLIM User Manual

Every effort has been made to eliminate errors and ambiguities in the information contained in this guide. Any questions concerning information presented here should be directed to SAMSUNG TELECOMMUNICATIONS AMERICA, 1301 E. Lookout Dr. Richardson, TX. 75082 telephone (972) 761-7300. SAMSUNG TELECOMMUNICATIONS AMERICA disclaims all liabilities for damages arising from the erroneous interpretation or use of information presented in this guide.

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 GPLIMT/GPLIM Data Switch and describes the procedures for installing and using the module.

Document Content and Organization

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

CHAPTER 1. Overview of OfficeServ 7400 GPLIMT/GPLIM

This chapter briefly introduces the OfficeServ 7400 GPLIMT/GPLIM.

CHAPTER 2. Installing OfficeServ 7400 GPLIMT/GPLIM

This chapter describes the installation procedure and login procedure.

CHAPTER 3. Using OfficeServ 7400 GPLIMT/GPLIM

This chapter describes how to use the menus of the OfficeServ 7400 GPLIMT/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

The OfficeServ 7400 General Description introduces the OfficeServ 7400 platform and presents the system information necessary to understand the hardware configuration, specification, and system functionality.

OfficeServ 7400 Installation Manual

The 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 how to program the system using the Man Machine Communication (MMC) entries (using digital telephone).

Revision History

EDITION	DATE OF ISSUE	REMARKS
00	11. 2005.	Original Draft
01	02. 2006.	Second Edition
02	11. 2006.	- 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.

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

TABLE OF CONTENTS

INTRODUCTION III

Purpose III
Document Content and Organization III
Conventions IV
Console Screen Output IV
References V
Revision History V

SAFETY CONCERNS VI

Symbols VI
Caution VII

CHAPTER 1. Overview of OfficeServ 7400 GPLIMT/GPLIM 10

Introduction to OfficeServ 7400 10
Introduction to OfficeServ 7400 GPLIMT/GPLIM Data Switch 11

CHAPTER 2. Installation of OfficeServ 7400 GPLIMT/GPLIM 13

Installing 13
Getting Started 15
Port 17
Port 18
Port 19
VLAN 24
MAC 30
Layer2 32
RSTP 33
Port Aggregation 37
GVRP 39
IGMP Snooping 42
Authentication 45
Application 48
VoIP Service 48
PoE 49

System **56**
Network 57
DB Config 58
Admin Config 59
Log 60
Time Configuration 62
Upgrade 64
Appl Server 64
Reboot 65
Utility 65
Management Menu **67**
SNMP 68
RMON 71
My Info Menu **74**

ABBREVIATION **75**

A~L 75
M~V 76

CHAPTER 1. Overview of OfficeServ 7400 GPLIMT/GPLIM

This chapter introduces the OfficeServ 7400 system and OfficeServ 7400 GPLIMT/GPLIM Data Switch.

Introduction to OfficeServ 7400

The OfficeServ 7400 platform delivers the convergence of voice, data, wired and wireless communications for small and medium sized businesses. This ‘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 GWIMT/GWIM, GPLIMT/GPLIM, and GSIMT/GSIM Data 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 switching capabilities of the OfficeServ 7400 GPLIMT/GPLIM Data Switch.


NOTE

Structure of OfficeServ 7400

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

Introduction to OfficeServ 7400 GPLIMT/GPLIM Data Switch

GPLIM Module

GPLIMT Module

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 10/100-BASE-TX Fast Ethernet ports: LAN interface between terminal devices
- GPLIM: Two Gigabit Ethernet ports: uplink LAN interface
- GPLIMT: Two 10/100/1000 Base-T 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 GPLIMT/GPLIM functional block via a browser
- Configuration and verification functions for the operations of GPLIMT/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 GPLIMT/GPLIM

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

Installing

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

Package	File	Description
Bootrom Package	GPLIMT/GPLIM-bootldr.img-vx.xx GPLIMT/GPLIM-bootldr.img-vx.xx.sum	Boot ROM program
Main Package	GPLIMT/GPLIM-pkg-vx.xx.tgz	Upgrade package for HTTP
	GPLIMT/GPLIM-os..img-vx.xx	'os' partition upgrade package for TFTP
	GPLIMT/GPLIM-firmware.img-vx.xx	'Firmware' partition upgrade package for TFTP
	GPLIMT/GPLIM-configdb.img-vx.xx	'configdb' partition upgrade package for TFTP
	GPLIMT/GPLIM-logdb.img-vx.xx	'logdb' partition upgrade package for TFTP
	GPLIMT/GPLIM-flash.img-vx.xx GPLIMT/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.

GPLIMT/GPLIM Installation

1. Insert the GPLIMT/GPLIM into an open slot in the OfficeServ 7400 cabinet **(excluding slots 0 or 3 which are reserved for the MP40 and LP40 cards)**.

2. Connect a PC to any port (P1 –P12) of the GPLIMT/GPLIM module with either a straight or cross over cable.. Installers will need to configure the TCP/IP settings of the PC to be on the same subnet as the default Management IP address of the GPLIMT/GPLIM shown in step 3.

3. Using Internet Explorer 6.0 or higher navigate to the default Management IP address of the GPLIMT/GPLIM board (10.0.4.1/24 (https://10.0.4.1).

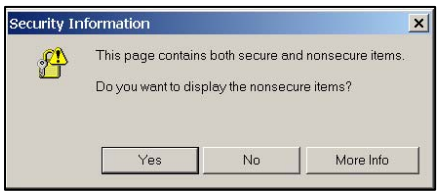
Caution when using a Web Browser

The version of Internet Explorer should be 6.0 or higher when logging in and performing maintenance on the GPLIMT/GPLIM. Other web browsers are not supported.

Getting Started

1. Start Internet Explorer and enter the IP address of the GPLIMT/GPLIM management IP Address into the address bar. The Security Alert window shown below will appear. Click on the Yes button to proceed:

2. A Security Information window will now open. Click on the Yes button to proceed.



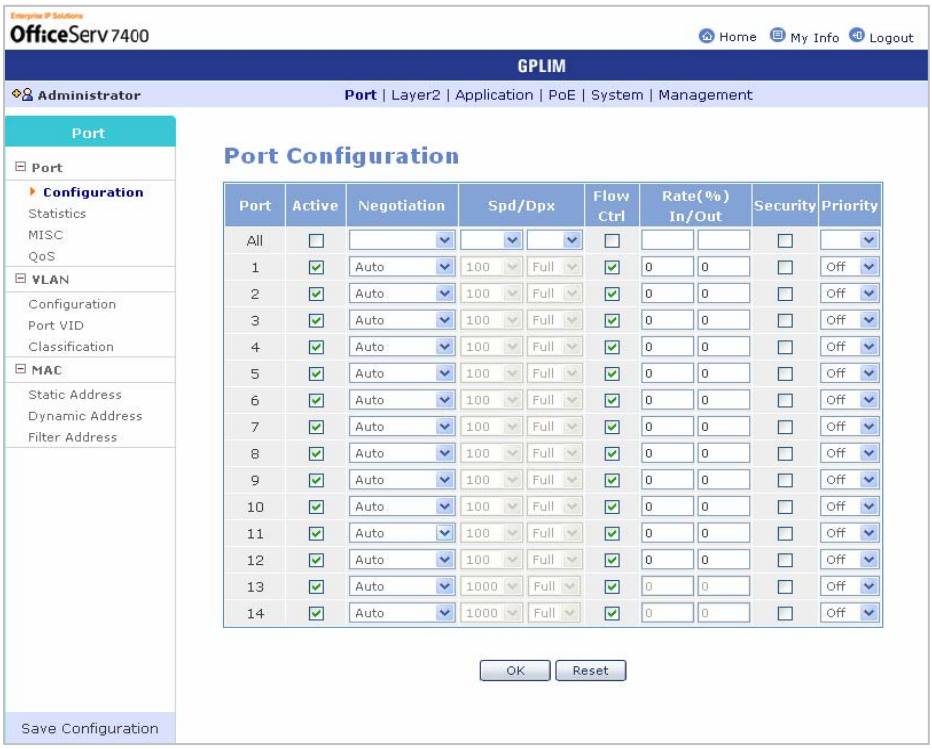
3. The Administrator will now be prompted for a Login ID and Password.

NOTE

The Login ID is “admin” and the default password is “root”

4. Log into the GPLIMT/GPLIM using the administrator ID and password and then click on the OK button. The following Security Information window will appear again. Click on the Yes button to proceed.

5. The GPLIMT/GPLIM menus are displayed in the upper part of the screens. Select each menu to display its submenus on the left section of the screen. For more detailed information for each menu, refer to 'Chapter 3. Using OfficeServ 7400 GWIMT/GWIM' of this document

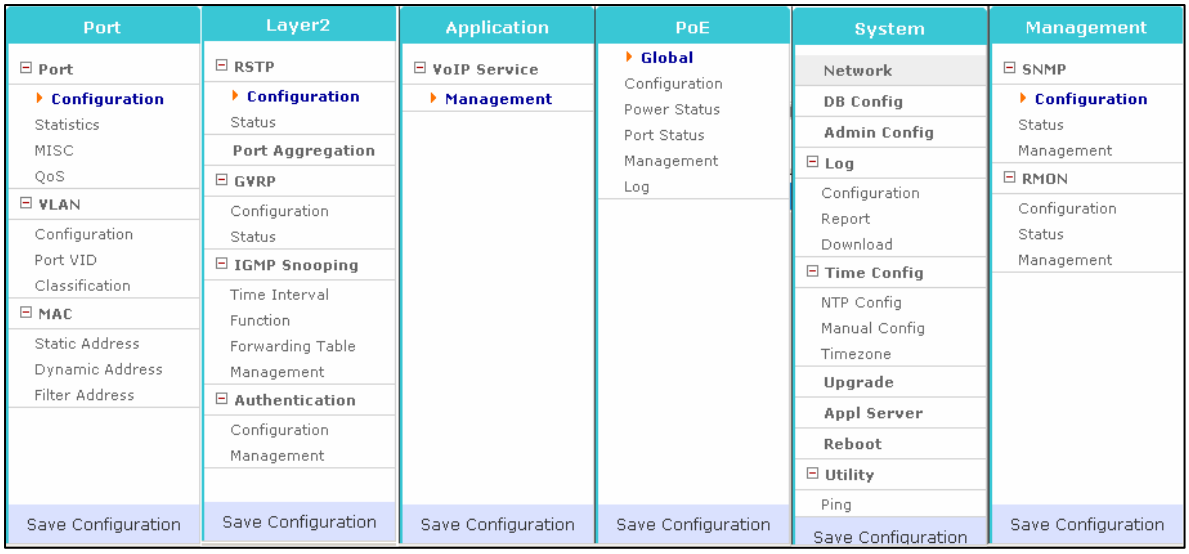


6. Click the Logout button on the upper section of the screen to close the connection to the GPLIMT/GPLIM system.

CHAPTER 3. Use of OfficeServ 7400 GPLIMT/GPLIM

This chapter describes the menus of the OfficeServ 7400 GPLIMT/GPLIM.

The OfficeServ 7400 GPLIMT/GPLIM Data Switch menus are arranged as shown below:



Port

The **[Port]** menu is used by the administrator to configure the individual switch port settings such as speed, duplex, and flow control, to configure VLANs, to statically assign MAC Addresses to switch ports, and to assign MAC Address filtering. Select the **[Port]** menu and the submenus will be displayed in the upper left side of the window as follows:

Port Menu Description

Menu	Submenu	Description
Port	Configuration	Used to set the environment of the switch ports.
	Statistics	Used to display the information and statistics on the transmission method, link status and speed of the switch ports.
	MISC	Used to display the mirroring function and other functions of the switch.
	QoS	Used to set the prioritization of the packets that arrive into the switch to specific ports
VLAN	Configuration	Used to configure Virtual LAN (VLAN).
	Port VID	Use to set the Port VID to set the process method for untagged packets when the VLAN mode is ‘Tag-based VLAN’.
	Classification	Used to set the VLAN based on Protocol type or MAC Address.

Menu	Submenu	Description
MAC	Static Address	Used to store a MAC address to the static address table.
	Dynamic Address	Used to retrieve a floating address table or to delete a MAC address.
	Filter Address	Used to enter 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	-	Used to store the data base.

Port

The **[Port]** → **[Port]** submenu is used to set the functionality of the switch ports, to retrieve configuration information on the switch ports, to set port mirroring, and to configure the Layer 2 QoS.

Configuration

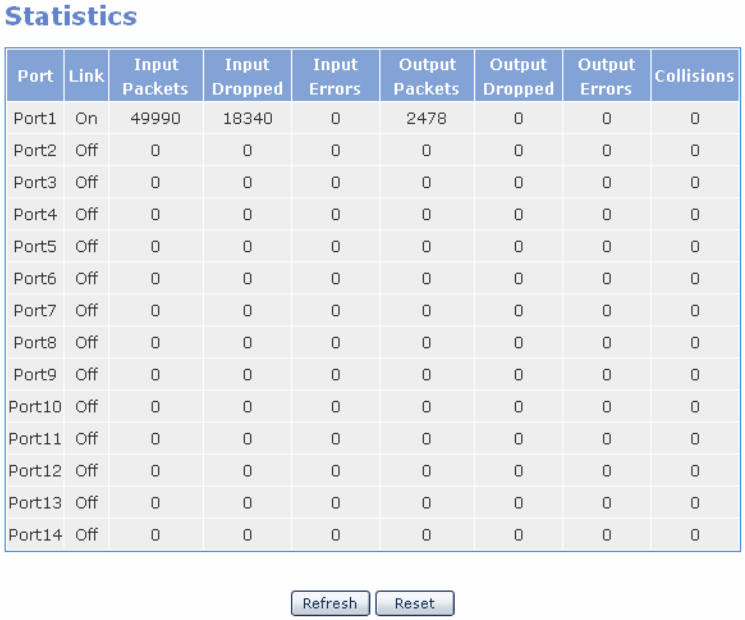
The **[Port]** → **[Port]** → **[Configuration]** submenu is used to set the configuration of the switch ports in the GPLIMT/GPLIM.

Port Configuration Parameter Description

Parameter	Description
Port	Used to display the port number
Active	Used to set 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	Used only if the Negotiation parameter is set to "Force" - Speed: Ports 1-12 can be set to 10/100 Mbps. Ports 13-14 are 10/100/1000 Mbps. - Duplex(Dpx): Select Set Full(two-way service) or Half(one-way service).
Flow Ctl	Used to set whether to use the flow control function. The flow control is processed according to the value set at Rate (%) In/Out (Entry rate/Exit rate).
Rate(%) In/Out	Used to control the flow by setting the entry rate and exit rate. The unit is the Rate (%) of the port speed. If the flow control function is not used then the value is set as '0'.
Security	Used to set a switch port to be secure. If a Static MAC address is to be entered for a specific switch port (**[Port]** → **[MAC]** → **[Static Address]** submenu) then the 'Security' box must be checked. That ensures that the port is secured for that specific MAC address only.
Priority	Used to set the port value as 'Low', 'High', or Off. This parameter works in conjunction with **[Port]** → **[QoS]** submenu.

Statistics

The administrator can retrieve the link status and statistics for each port on the GPLIMT/GPLIM switch using the **[Port] → [Port] → → [Statistics]** submenu. In order to reset the statistics click the Reset button.

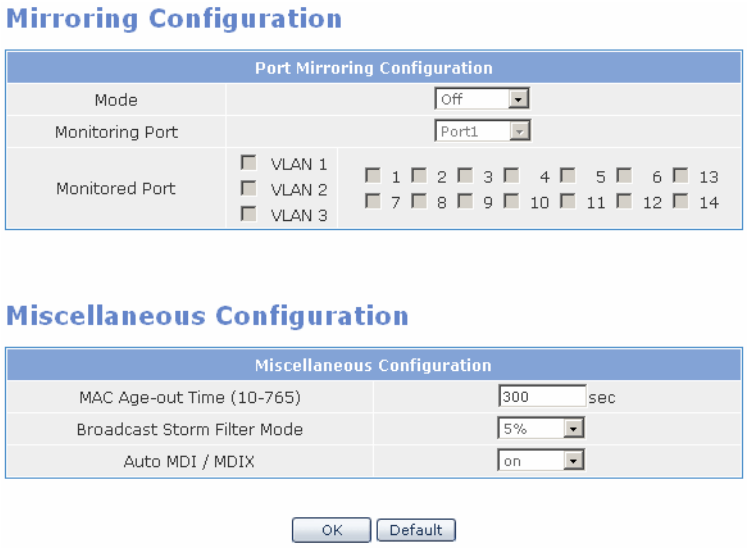


Port Statistics Field Description

Field	Description
Input Packets	Used to display the number of packets received
Input Dropped	Used to display the number of packets that are received but dropped without successfully being switched
Input Errors	Used to display the number of error packets received
Output Packets	Used to display the number of packets that are transmitted
Output Dropped	Used to display the number of packets that are transmitted but dropped
Output Errors	Used to display the number of packets that are transmitted to the port and encounter errors
Collisions	Used to display the number of times that a collision occurs between a packet received and a packet transmitted at a port

MISC

The administrator can set up the port mirroring feature and adjust the MAC Age-out Timer, the Broadcast Storm Filter, and the Auto MDI/MDIX parameters using the **[Port] → [Port] → [MISC]** submenu.

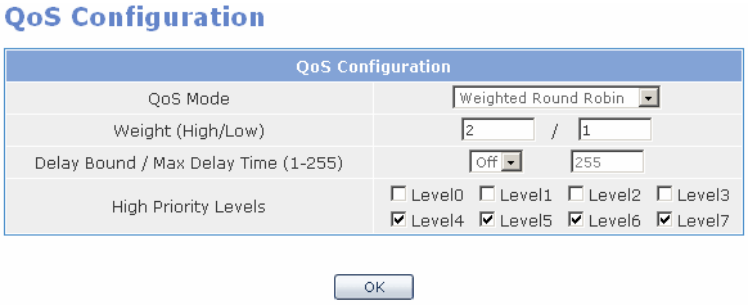


MISC Parameter Description

Parameter	Description
Mode	Used to set up 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	Used to assign a specific port for monitoring. Generally, this means a connection to a PC doing the monitoring.
Monitored Port	Used to assign the port/s or VLAN/s where the monitoring will be performed. The monitoring port and the monitored port cannot be the same port.
MAC Age-Out Delay Bound	Used to set the duration of time that a MAC address remains in the MAC address table. The default value is 300 seconds. If the LAN Port connection is released or disconnected then the MAC address is deleted immediately.
Broadcast Storm Filter Mode	Used to set the switch buffer. This value can be set to 5, 10, 15, 20 or 25 % load. If this value is exceeded then the broadcast packet will be discarded.
Auto MDI/MDIX	Used to set the automatic sensing of the direct/cross cable on or off.

QoS

The GPLIMT/GPLIM Layer 2 QoS configuration is performed using the **[Port] → [Port] → [QoS]** submenu.



QoS Parameter Description

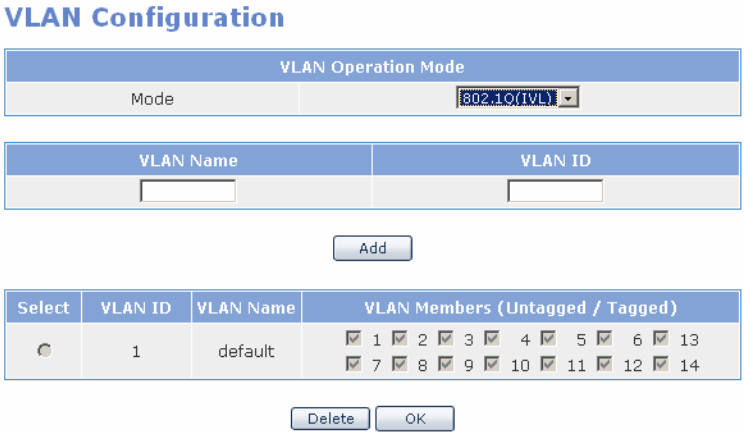
Parameter	Description
QoS Mode	Used to select the QoS mode. - **First Come First Service**: Packets are transmitted according to there incoming order.(QoS function not used) - **All High before Low**: When a packet has a higher priority it is transmitted prior to a packet with a lower priority. All lower priority packets must wait until all the higher priority packets are transmitted. - **Weighted Round Robin**: This method is used to transmit high priority packets and low priority packets at an established rate (Weight). For example if the setting for High Weight is '5' and the Low Weight to '2', then five high priority packets are transmitted before two priority packets are transmitted.
Weight	Used to set the High weight and Low weight ratio when the method of 'Weighted Round Robin' is employed.
Delay Bound/ Max Delay Time	Used to set 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 a High or Low priority. The Level 0~Level 7 boxes do not indicate the actual value of the priority. The GPLIMT/GPLIM processes packets by separating them into two Queues, 'High' and 'Low'.

VLAN

VLANs are used to divide a network into smaller networks to reduce the traffic and for security purposes. The **[Port] → [VLAN]** submenu is used to configure VLANS, Port VIDs, and VLAN Classifications.

Configuration

Using the **[Port] →[VLAN] → [Configuration]** submenu the administrator can configure the VLAN features.



VLAN Operation Mode Description

Mode	Description
802.1 Q(IVL)	Used to set the VLAN type to Independent VLAN Learning – Tag based
MAC	Used to set the VLAN type to MAC based VLAN
Port	Used to set the VLAN type to Port Based VLAN
802.1 Q(SVL)	Used to set the VLAN type to Shared VLAN Learning – Tag based

802.1 Q (IVL)

IVL (Independent VLAN): Each VLAN operates while maintaining an independent MAC address table. Because the security is enhanced, data cannot be exchanged directly among the VLANs.

MAC Based VLAN

The MAC based VLAN is configured with an access list mapping individual MAC addresses to VLAN membership. The VLAN is configured without information on the port and the number of a VLAN members may change. Up to 256 MAC address 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.

Port Based VLAN

The Port based VLAN is configured with an access list specifying membership in a set of VLANs.. A single port can be assigned to multiple VLANs. In such cases the 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.

802.1Q (SVL)

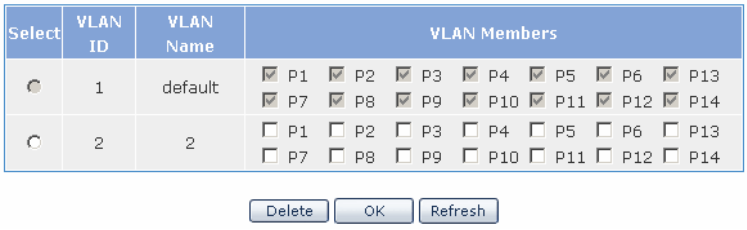
802.1Q(SVL) can be set and operate with the same method as 802.1Q(IVL).

SVL (Shared VLAN): All VLANs operates while maintaining a common MAC address table. Because the security is not tightened and the MAC address table exists for all ports, data can be exchanged among all VLANs.

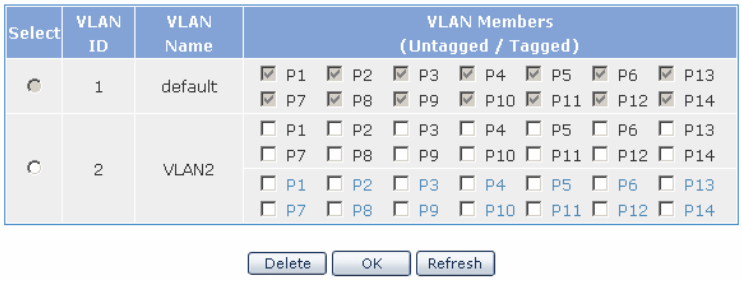
In order to create a new VLAN simply enter the VLAN name and ID and then click the Add button.

Once a VLAN is created then it is then possible to add members to the VLAN

Port and MAC based VLAN



802.1Q IVL and SVL based VLAN

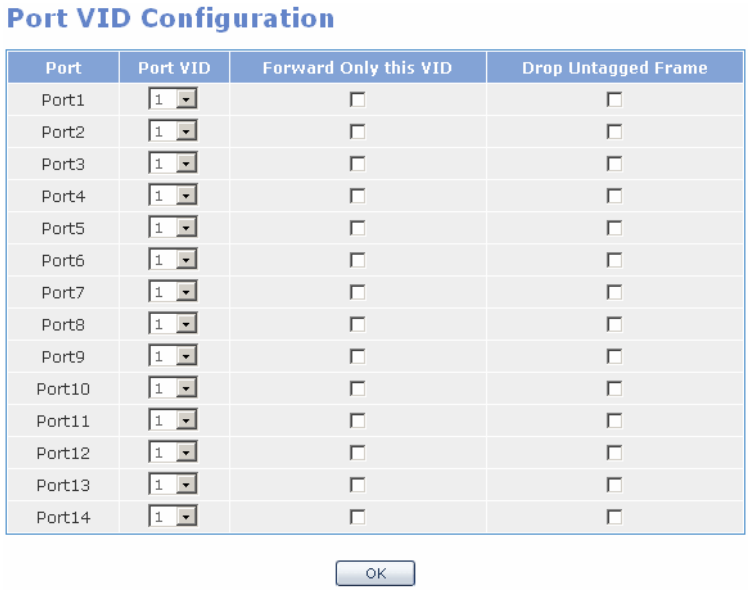


The 802.1q IVL and SVL based VLANs have two groups of boxes. The top grouping (in black) is used to assign untagged ports, and the bottom grouping (in blue) is used to assign tagged ports.

- VLAN Untagged Members: Select the port/s that will send the Ethernet frame that deletes the TCI (Tag Control Information). 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. Connect to another switch port that supports IEEE 802.1Q.

Port VID

For an ethernet packet to have a VLAN ID the tag must be written by an Ethenet adapter or Switch. Using the **[Port] → [VLAN] → [Port VID]** submenu the administrator will assign the VLAN IDs to specific ports.



Port VID Parameter Description

Parameter	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 this box is checked and the received tagged packet tag is different from the Port VID then the packet is discarded. When this box is not checked then the packet is re-sent according to the received tag information.
Drop Untagged Frame	If this box is checked then the port discards the untagged frame. If not, the untagged frame is re-sent to the VLAN corresponding to the setting Port VID.

NOTE

Port VID Input Value

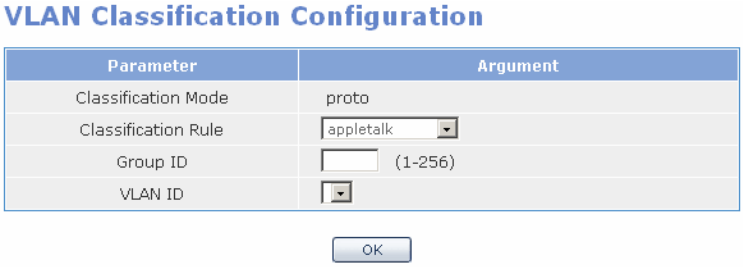
The valid PVID values on the GPLIMT/GPLIM are between 1 and 255.

Classification

Using the **[Port]** → **[VLAN]** →**[Classification]** submenu the administrator can define the VLAN Classification Rules.

802.1Q (IVL and SVL)

If an untagged frame is received it can be classified according to protocol. The rule values are set to decide which VLAN ID is attached to a frame.



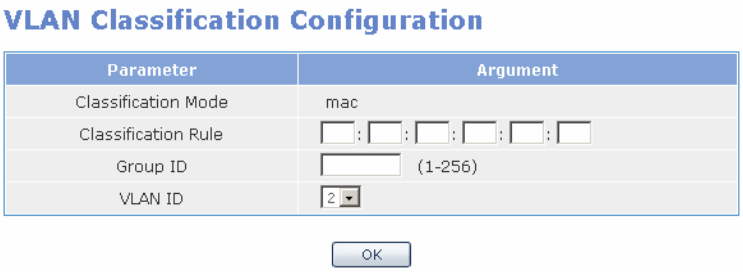
VLAN Configuration Field/Parameter Description

Field/Parameter	Description
Classification Mode	This field is defined automatically according to the VLAN mode. When the mode is 802.1Q 'proto' (for protocol) is selected.
Classification Rule	Based on Appletalk, arp, decnet, ip, ipx, sna, and x25, VLAN is set.
Group ID	Used to enter a Group ID for the selected protocol. Valid groups numbers are 1~256.
VLAN ID	Decides which VLAN ID will be assigned to the frame..

In order to delete a VLAN Classification rule simply click on the radio button to the left of the rule and then click the delete button.

MAC Based VLAN

Frames coming into a switch can be marked for a particular VLAN based on the source MAC Address



VLAN Classification Parameter Description

Field/Parameter	Description
Classification Mode	This field is defined automatically according to the VLAN mode. When the mode is MAC 'mac' is selected
Classification Rule	According to the received packet via a defined MAC address the VLAN can be set.
Group ID	Used to enter a Group ID for the selected mac. Valid groups numbers are 1~256.
VLAN ID	Decides which VLAN ID will be assigned to the frame..

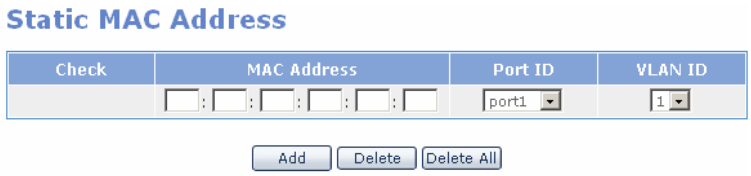
In order to delete a VLAN Classification rule simply click on the radio button to the left of the rule and then click the delete button.

MAC

The **[Port]** → **[MAC]** submenu is used to assign MAC addresses to ports, to view dynamic MAC address tables, and to assign MAC address filtering.

Static Address

The **[Port]** → **[MAC]** → **[Static Address]** submenu is used to enter a specific MAC address in the MAC address table. Even if the device is not connected to the switch and the MAX Aging Time (interval of MAC address table renewal) is passed the corresponding MAC address is left in the address table. Multiple MAC Addresses may be defined on the same port.



Enter the MAC address and Port ID and then click the Add button to add the MAC address. In order to delete an entry select the box to the left of the specific MAC address and thenclick the Delete button

.

If the Security box is checked for a port in the **[Port]** →**[Port]** → **[Config]** submenu then any learning of source MAC addresses will not occur. Only defined MAC addressed can access the port at this point.

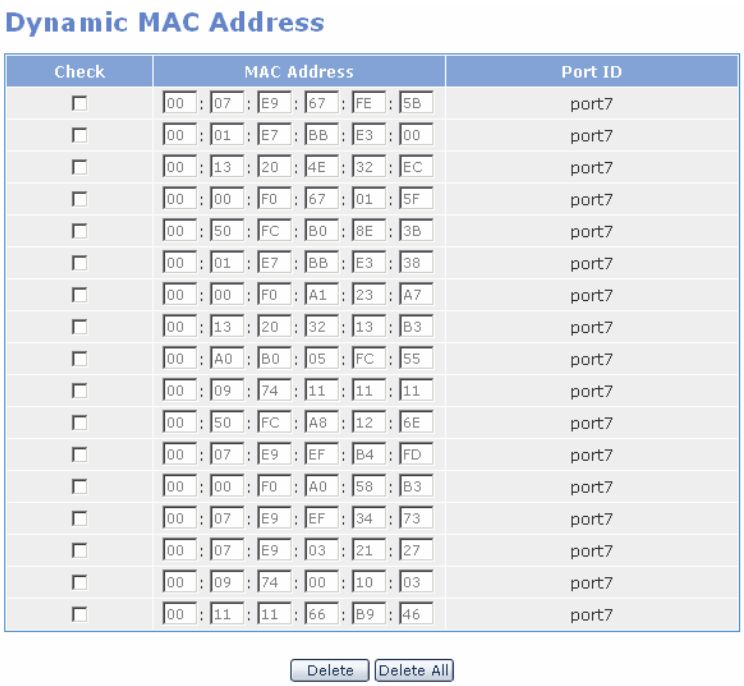
NOTE

Number of Static MAC Addresses Entered

Up to 50 static MAC addresses can be entered into the Static MAC Address table.

Dynamic Address

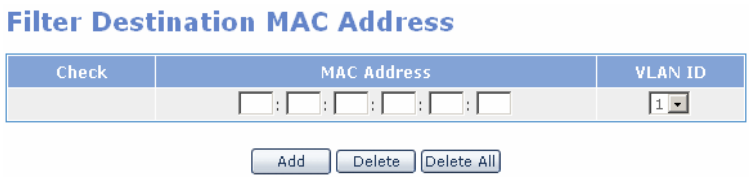
In order to view the dynamically learned MAC addresses use the **[Port] → [MAC] → [Dynamic Address]** submenu.



Filter Address

By using the Mac filtering feature on the GPLIMT/GPLIM it is possible to block unwanted traffic on the network. The **[Port] → [MAC] → [Filter Address]** submenu is used to enter MAC addresses that are to be filtered.

Enter the desired MAC address and VLAN ID and then click the Add button.
If a MAC Address filter needs to be removed check the box to the left of the filter and then click the Delete button.



Layer2

The Layer 2 Menu is used to configure the Spanning Tree Protocol, GVRP, IGMP, and port based authentication. Once the **[Layer2]** menu is selected the submenus will be displayed in the upper left side of the window as follows:

Layer 2 Menu Description

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

RSTP

Configuration

The Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocols (RSTP) provide a loop free topology for any bridged LAN. Use the **[Layer2] → [RSTP] → [Configuration]** submenu to begin configuring the RSTP and STP settings.

Protocol Status

Parameter	Argument
RSTP status	Current Enable

Bridge Parameter

Parameter	Argument
Bridge Priority	8 Default : 8 (0 - 15)
Hello Time	2 sec Default : 2 (1 - 10)
Max Age Time	20 sec Default : 20 (6 - 40)
Forward Time	15 sec Default : 15 (4 - 30)

Port Parameter

Port Name	Priority	Force Version	Path Cost	Port Fast	Link Type
Port 1	8	RSTP	200000	Enable	Point to Point
Port 2	8	RSTP	200000	Enable	Point to Point
Port 3	8	RSTP	200000	Enable	Point to Point
Port 4	8	RSTP	200000	Enable	Point to Point
Port 5	8	RSTP	200000	Enable	Shared
Port 6	8	RSTP	200000	Enable	Shared
Port 7	8	RSTP	200000	Enable	Shared
Port 8	8	RSTP	200000	Enable	Shared
Port 9	8	RSTP	200000	Enable	Shared
Port 10	8	RSTP	200000	Enable	Shared
Port 11	8	RSTP	200000	Enable	Shared
Port 12	8	RSTP	200000	Enable	Shared
Port 13	8	RSTP	200000	Disable	Shared
Port 14	8	RSTP	200000	Disable	Shared

Save Reset

RSTP Protocol Status/Bridge/Port Parameter Description

Parameter	Description
Protocol Status	Used to display the current status of the RSTP protocol.
Bridge Parameter	Used to configure the Bridge parameters of the switch that RSTP uses. - **Bridge Priority**: Used to set the priority of Bridges. - **Hello Time**: Used to set the transmission cycle of BPDU. - **Max Age Time**: Used to set the Message Age time. - **Forward Time**: Used to set the time that the state of each port is changed (Discarding-Learning-Forwarding).
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**: Used to set and display the path cost according to the bandwidth when the connection with the opponent is established. - **Port Fast**: If the port is enabled for Port Fast then the port becomes an Edge port and quickly goes into a forwarding state. If this function is activated then the MAC address learned in the corresponding port is not canceled even when all topologies of Bridges are changed.(If STP is used then the Port Fast function should be disabled.) - **Link Type**: Used to set and display the type of the link connected to the opponent. The link is connected as point-to-point in RSTP.

Status

The **[Layer2] → [RSTP] → [Status]** submenu is used to display the status of the 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

RSTP Bridge Status Field Description

Field	Description
Protocol Status	Used to show the RSTP status
Designated Bridge Identifier	Used to display the GPLIMT/GPLIM's bridge information in hexadecimal numbers. The upper four digits represent the bridge priority and the remaining lower digits is the GPLIMT/GPLIM MAC address.
Root Bridge Identifier	Used to display the network root bridge.
Root Path Cost	Once the root bridge is decided this field displays the calculated cost for the path to the root switch.
Root Port	If the current equipment is not the root switch then this field indicates the ID of the port corresponding to the root port. A switch can have only root port.)

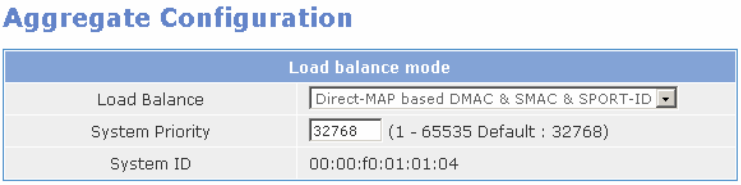
Field	Description
Last Topology Changed	Used to display the most recent time that the RSTP network was reconfigured due to a change in the network configuration.

RSTP Port Status Field Description

Field	Description
Port Name	Used to display the port number
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.
Designated Root	Used to display the designated root

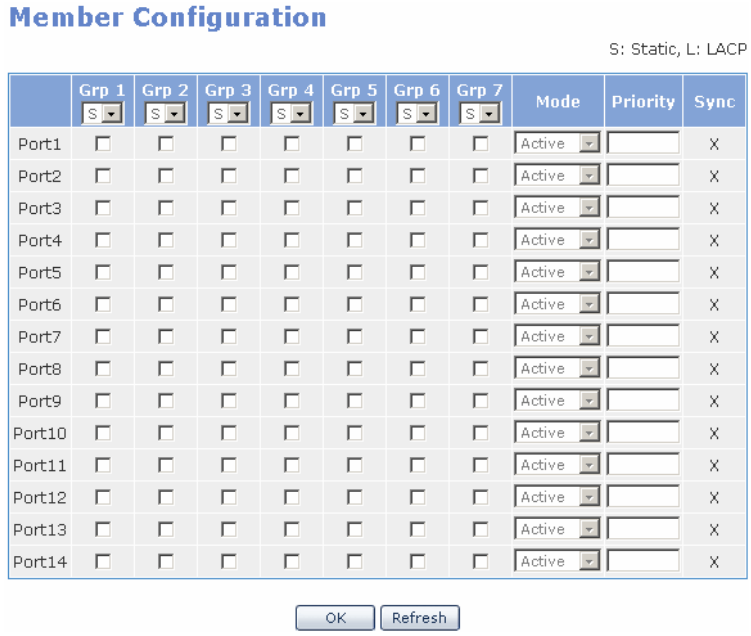
Port Aggregation

In order to use multiple transmission paths between network devices so there can be an increase in transmission speeds then the Port Aggregation feature can be used. Select the **[Layer2] → [Port Aggregation → [Configuration]** submenu to begin configuring Port Aggregation.



Port Aggregate Configuration Parameter Description

Parameter	Description
Load Balance	When transferring a packet to the opposite party through a trunk port then the packet is transferred to a port among members included in 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 Parameter Description

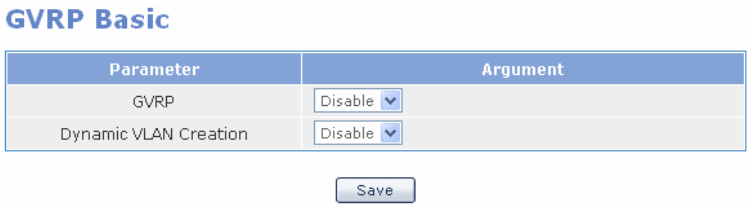
Parameter	Description
Group	'S' represents a static trunk, and 'L' represents a LACP (Link Aggregation Control Protocol) trunk. Up to eight groups can be used and up to four ports can be included in one group as members. In addition, a member included in one group cannot be included another group simultaneously.
Mode	Used to set the mode when LACP is the Group type. Select either **'**Active' or 'Passive'. When a port is set as Active, an LACP packet is transferred to the opposite switch first. When set as Passive it responds only when receiving a packet from the opposite switch. If the user system and opposite system are both set up as Active, then the system that has higher priority is used as a reference.
Priority	Used to setsup the port priority. The default is 32768.
Sync	This field 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

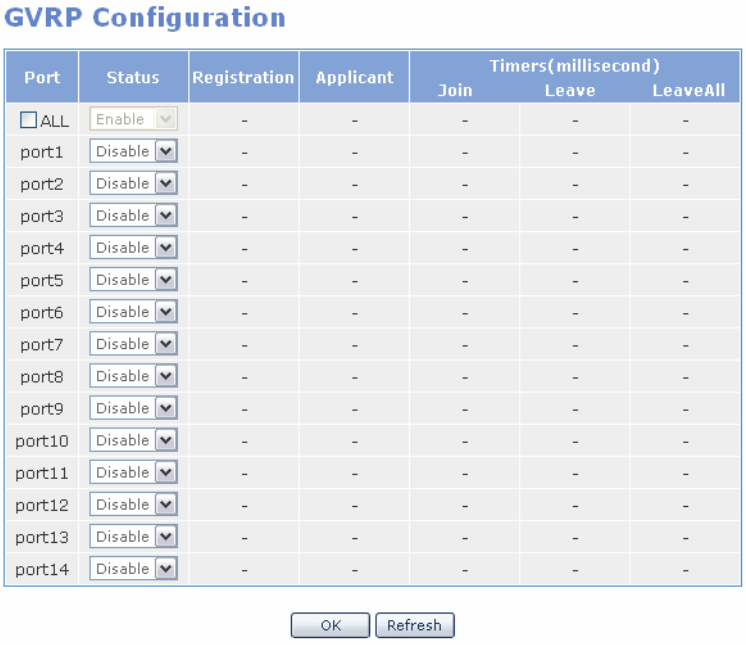
GVRP (GARP VLAN Registration Protocol) is a protocol that facilitates control of virtual local area networks (VLANs) within a network. It defines a method of tagging frames with VLAN configuration data. This allows network devices to dynamically exchange VLAN configuration information with other devices. Select the **[GVRP]** menu to start or stop the GVRP service, to modify the GVRP service for each port, and to view the status of GVRP.

Configuration

Use the **[Layer2] → [GVRP] → [Configuration]** submenu to start or stop the GVRP service and the Dynamic VLAN Creation service.



In the **<GVRP Basic>** window specify the GVRP configuration as Enabled and then click the Save button. Once GVRP is enabled the following configuration window will appear.



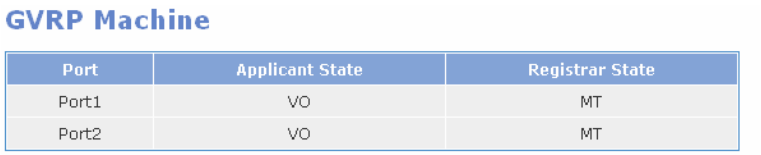
Make changes to the ports and then click the OK button to save the information. Click the Refresh button to display the latest information of the port .

GVRP Configuration Field/Parameter Description

Field/Parameter	Description
Port	Used to display the port Number
Status	Used to enable or disable GVRP per port
Registration	Used to display the Registration mode as Normal, Forbidden or Fixed
Applicant	Used to display the Applicant mode as Normal or Active conditions
Join	Used to display the interval for Join Transfer Time
Leave	Used to ddisplay the value of Leave Delay Time
LeaveAll	Used to display the value of LeaveAll Transfer Time

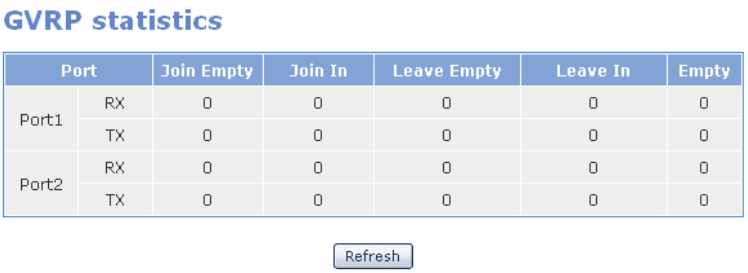
Status

The [Layer2] → **[GVRP]** → **[Status]** submenu is used to display the information on the ports where GVRP is configured.



GVRP Machine Field Description

Field	Description
Port	Used to display the Port Number
Applicant State	Used to display the Current Status of the Applicant State Machine
Register State	Used to display the Current Status of the Register State Machine



GVRP Statistics Field Description

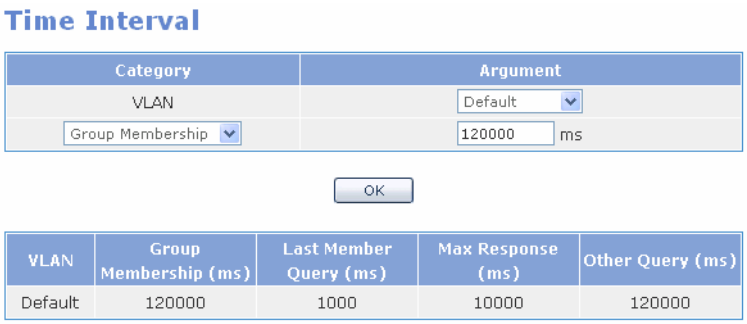
Field	Description
Port	Used to display the Port Number
Join Empty	Used to display the number of Join Empty packets
Join In	Used to display the number of Join In packets
Leave Empty	Used to display the number of Leave Empty packets
Leave In	Used to display the number of Leave In packets
Empty	Used to display the number of Empty packets

IGMP Snooping

The purpose of Internet Group Management Protocol (IGMP) snooping is to restrain multicast traffic in a switched network. The [Layer2] → **[IGMP Snooping]** menu is used for the configuration of IGMP Snooping.

Time Interval

Use the **[Layer2] →[IGMP Snooping] → [Time Interval]** submenu to configure the time related parameters of IGMP Snooping.



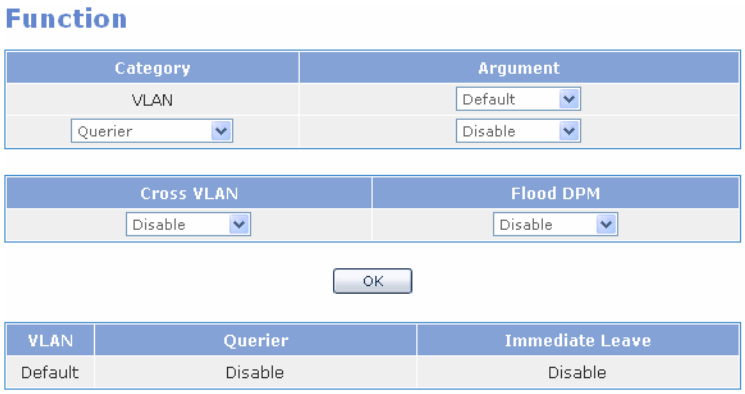
IGMP Time Interval Category Description

Categories	Description
VLAN	Pull down menu used to select the VLAN to be configured.
Group Membership	Used to configure the time to exit from the multicast forwarding database list when new report does not exist.
Last Member Query	Used to configure 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	Used to configure the maximum time until its response when IGMP Snooping query is received.
Other Query	Used to configure 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 timed value, and then click the OK button to store the configuration.

Function

Use the [Layer2] → **[IGMP Snooping]** → **[Function]** submenu to specify the functions related to IGMP Snooping.



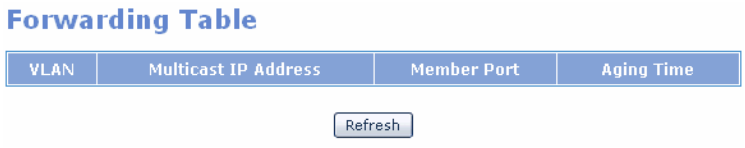
IGMP Snooping Function Category Description

Categories	Description
VLAN	Pull down menu used to select the VLAN to be configured.
Querier	Used to specify the operation as IGMP querier when the multicast router does not exist.
Immediate Leave	Used to delete a host from the group immediately when receiving the Leave Message.
Cross VLAN	Used to Forward multicast packets to all ports regardless of VLAN.
Flood DPM	Used if no member exists in the IGMP group, sets whether to forward multicast packets.

Select the VLAN and the Category to configure, select ‘Enable’ or ‘Disable’, and then click the OK button to store the configuration. The Querier and Immediate Leave values can be set for each VLAN, but the Cross VLAN and Flood DPM values are set on a bridge basis.

Forwarding Table

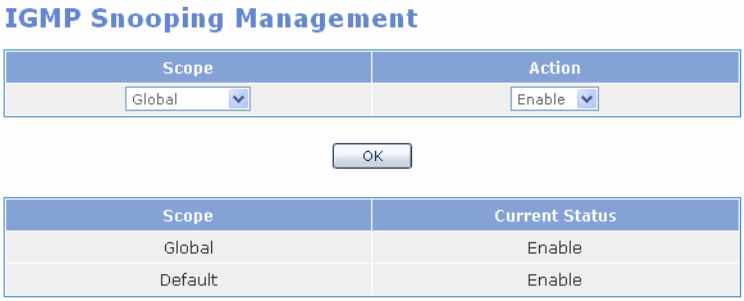
Use the **[Layer2] → [IGMP Snooping] → [Forwarding Table]** submenu to display the information on the members registered in IGMP Group.



Click the Refresh button to update the information displayed on the web screen.

Management

Use the **[Layer2] → [IGMP Snooping] → [Management]** to specify the operation of IGMP Snooping.



In the Scope parameter each VLANs can be turned on or off independantly.
However, if Global is set to Disable then all the VLANs become disabled.

> **NOTE**
>
> **IGMP Snooping Management**
>
> If Global is set to Disable mode then other pages within the **[Layer2] → [IGMP Snooping]** submenu are not be displayed.

Authentication

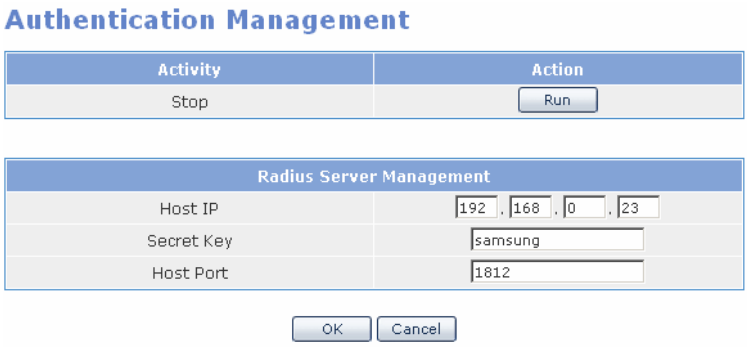
The **[Authentication]** submenu is used to enable or disable remote authentication, to review existing authentication information, and to configure individual ports and their authentication methods.

Management

Use the **[Layer2]** → **[Authentication]** → **[Management]** submenu to turn authentication on or off and to define the Radius server management items.

Click the Run button to start the service and click the Stop button to cease the authentication service.

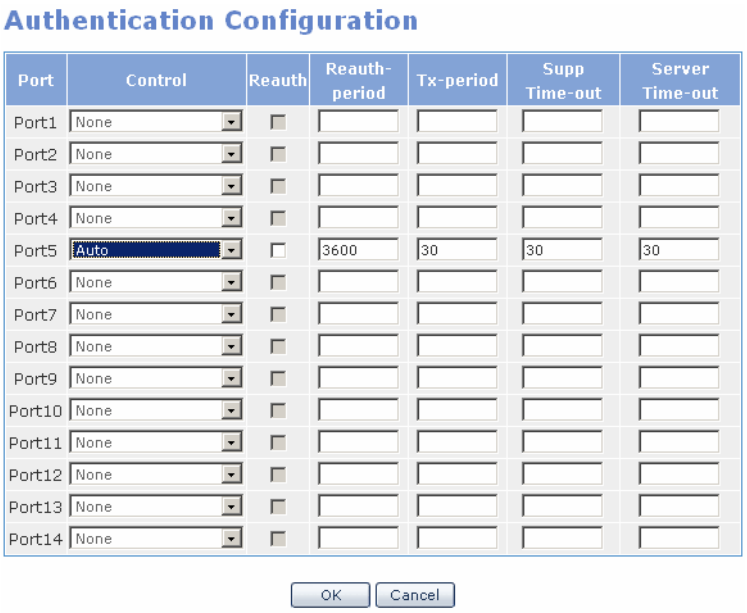
If there is the Radius server performing the 802.1x user authentication then the relevant data must be input here. The host IP address, host, and key should be registered. The default port of the Radius Host Port is 1812 port. Click the OK button to save any changes.



Configuration

Use the **[Layer2] → [Authentication] → [Configuration]** submenu to configure the authentication method on a per port basis. If the authentication service has not been started the following window will appear:

Once the service is started using the **[Layer2] → [Authentication] → [Management]** submenu the following window will appear when using the **[Layer2] → [Authentication] → [Configuration]** submenu



Authentication Configuration Parameter Description

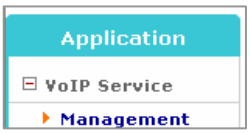
Parameter	Description
Control	Used to set the authentication mode of each port when employing the (802.1x) authentication - **None**: Authentication is not performed for the port. - **Force-authorized**: Admits the port forcibly. - **Force-unauthorized**: Blocks the port forcibly. - **Auto**: Allows the port through authentication from the Radius server and blocks the port.
Reauth	Used to set the port for re-authentication.
Reauth-Period	Used to set the timer for the re-authentication cycle when the Reauth box is checked. (1-4294967295sec) default: 3600 sec

Parameter	Description
Tx-Period	Used to set the cycle that sends Request regularly to supplicant. (1-65535sec) default: 30 sec
Supp-Timeout	Used to set the time before re-sending to the user when EAP is requested.(1-65535sec) default: 30 sec
Sever-Timeout	Used to set the time before re-sending to the device when server authentication of a server is requested.(1-65535sec) default: 30 sec

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

Application

The **[Application]** menu is used to view the status of VoIP Service and to start or stop the VoIP service. The submenus will be displayed in the upper left side of the window as follows:

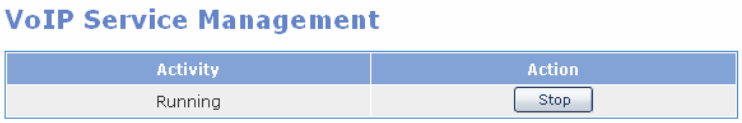


VoIP Service

This **[Application]** → **[VoIP Service]** submenu is used to start or stop the VoIP Service.

Management

From the **[Application]** → **[VoIP Service]** → [Management] submenu start or stop the VoIP service function. Whenever the system is rebooted the status of VoIP Service is restored to the how it was before the reboot..

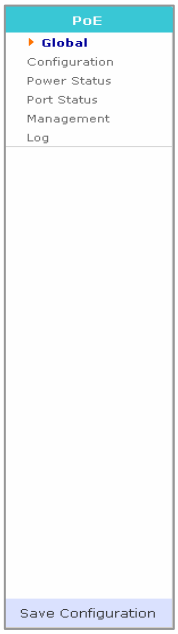


VoIP Service Parameter Description

Parameter	Description
Activity	Used to display the current status of the VoIP Service.
Action	Used to change the current status of VoIP Service.

PoE

The **[PoE]** menu is used to configure, edit, and view the GPLIMT/GPLIM PoE settings. The submenus will be displayed in the upper left side of the window as follows:

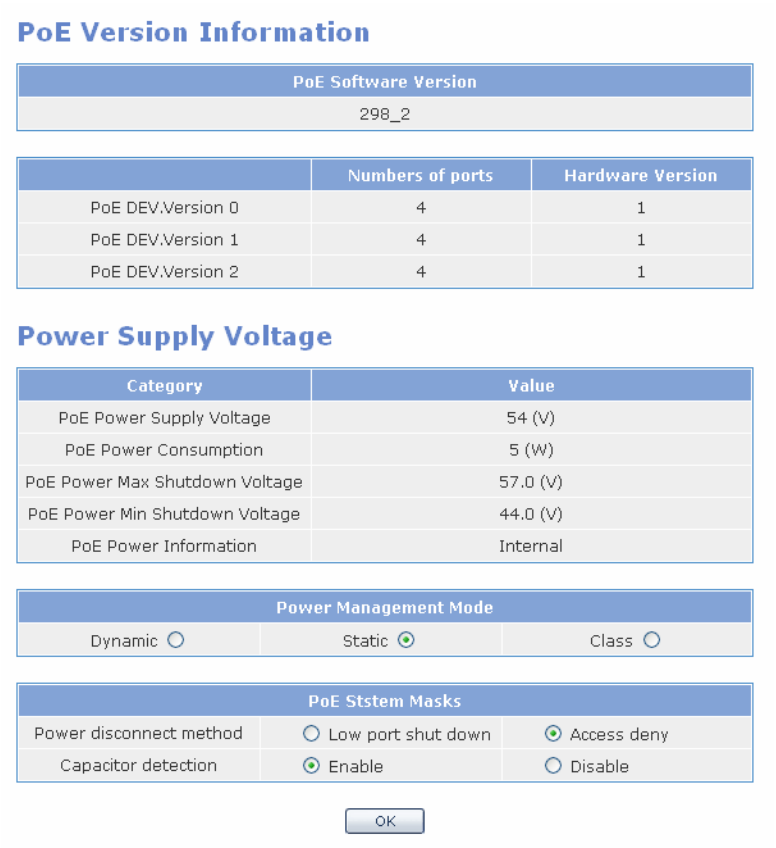


PoE Menu Description

Menu	Submenu	Description
PoE	Global	Used to set or retrieve the PoE version information and power supply information.
	Configuration	Used to set or retrieve the power information of each port.
	Power Status	Used to display the PoE power supply status in real time.
	Port Status	Used to display the PoE port status in real time.
	Management	Used to start and stop the PoE manager.
	Log	Used to set the recording parameters for the PoE log information.

Global

Select the **[PoE]** → **[Global]** submenu to check the PoE version information and power supply information. In addition this menu is used to set the Power Management Mode.



PoE Global Field Description

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

When the administrator sets the Power Management Mode the power supply type is selected depending on the Power Device (PD) terminal power.

Use the ‘Dynamic’ setting to make the maximum power of 18.9 W available for each port. Use the ‘Static’ setting to make the restriction of power definable. Use the ‘Class’ setting to decide upon the restriction of the PoE power depending on the PD terminal PD Classes which are are described as follows:

PoE Power Management Class Power Description

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.

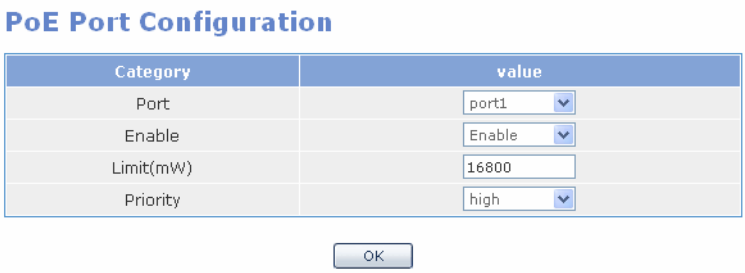
PoE System Mask Parameter Description

Parameter	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

Make the appropriate changes and then click the OK button to apply the settings.

Configuration

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



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

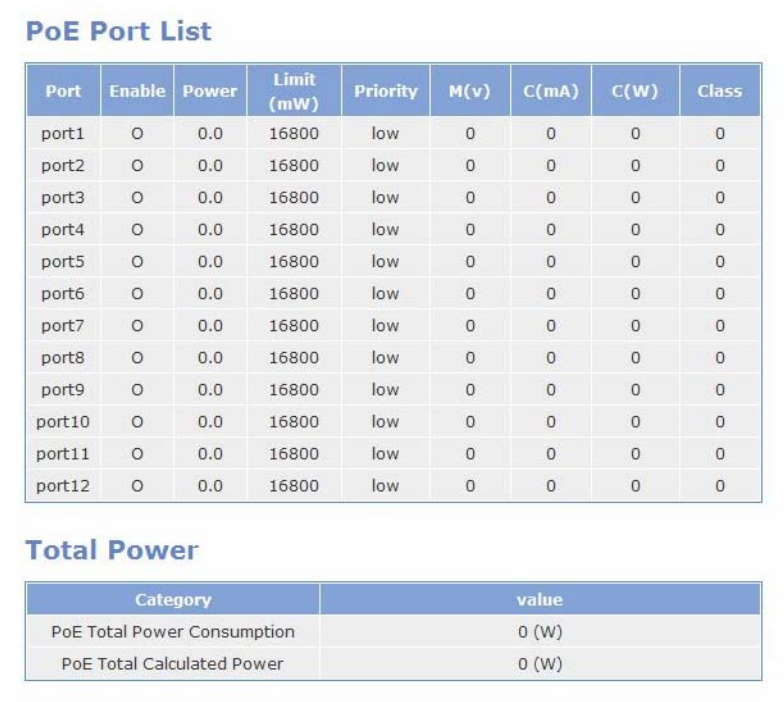
PoE Configuration Parameter Description

Parameter	Description
Port	Used to indicate the Ethernet port 1~12 being configured.
Enable	Used to sets or release the PoE power supply of the target port.
Limit(mW)	If the Power Management Mode is set to Static then the power limit of each port. Up to 1000~18900 mW can be set.
Priority	Used to set 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 then set the four port parameters. Click the OK button to save the changes. The applied changes can be checked by viewing the PoE Port List.

Power Status

Select the **[PoE]** → **[Power Status]** submenu 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

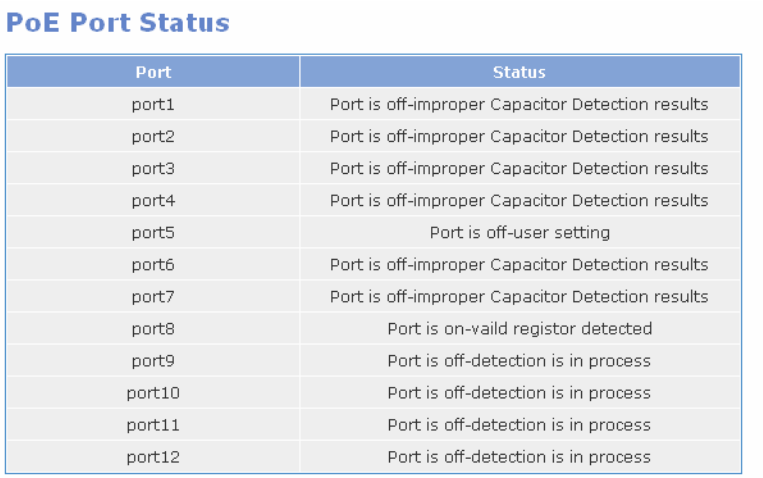
Category	value
PoE Total Power Consumption	0 (W)
PoE Total Calculated Power	0 (W)

PoE Power Status Field Description

Field	Description
Port	Used to display the Ethernet port 1~12.
Enable	Used to display the status of Power management for each port.
Power	Used to display the power allocated to each port.
Limit(mW)	If the Power Management Mode is set to Static this field is used to display the power limit on each port (1000mW to 18900 mW).
Priority	Used to display the power priority for each port.
M(v)	Used to display the total voltage provided.
C(mA)	Used to display the calculated current (Displays the **C(mA)** of the target port.)
C(W)	Used to display the power consumption (Displays the **C(W)** of the target port.)
Class	Used to display the class of the target port.

Port Status

Select the **[PoE]** → **[Port Status]** submenu 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

PoE Port Status Field Description

Field	Description
Port	Used to display the Ethernet port 1~12.
Status	Used to display the current PoE information for each port.

Management

Select the **[PoE]** → **[Management]** submenu to start or stop the PoE Manager. Click on the Run button to start the PoE Management and click on the Stop button to halt the PoE Management.

PoE Management

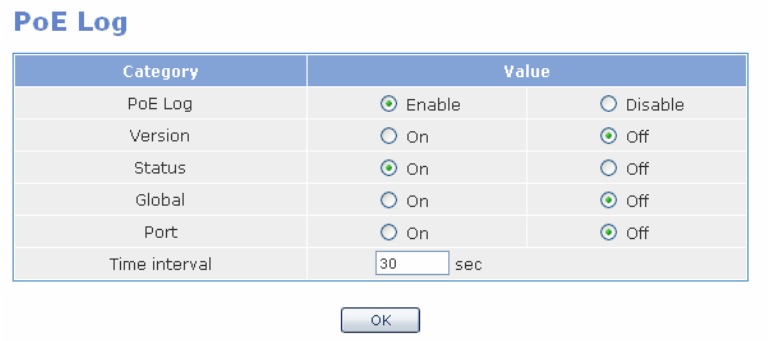
Module Name	Activity	Action
PoE	Running	Stop

PoE Management

Module Name	Activity	Action
PoE	Stop	Run

Log

Select the **[PoE]** → **[Log]** submenu to set the PoE log report attributes.



PoE Log Parameter Description

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

If the PoE Log is not enabled then the following items are not activated.
Change the items and then click the OK button to save.

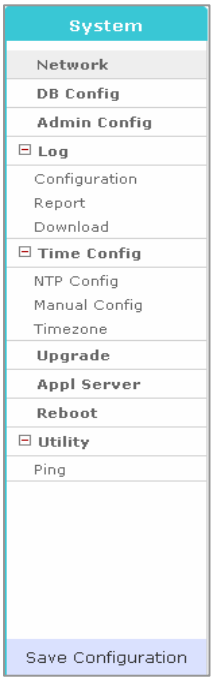
CAUTION

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

The System Menu is used to import or export the GPLIMT/GPLIM database, to view system logs, to set time attributes, to upgrade the software, and to reboot the system. Select the **[System]** menu and the submenus will be displayed in the upper left side of the window as follows:



System Menu Description

Menu	Submenu	Description
Network	-	Used to set the IP and DNS services.
DB Config	-	Used to import, and export the system database and to default the GPLIMT/GPLIM
Admin Config	-	Used to set up the GPLIMT/GPLIM for management authentication.
Log	Configuration	Used to set the system logging parameters
	Report	Used to retrieve the system logs currently stored.
	Download	Used to download the system log in file form to a pc.
Time Config	NTP Config	Used to set the time server to synchronize the time server with date and time information.
	Manual Config	Used to set the date and time of the system.
	Timezone	Used to set the timezone for the GPLIMT/GPLIM.
Upgrade	-	Used to upgrade the GPLIMT/GPLIM software.

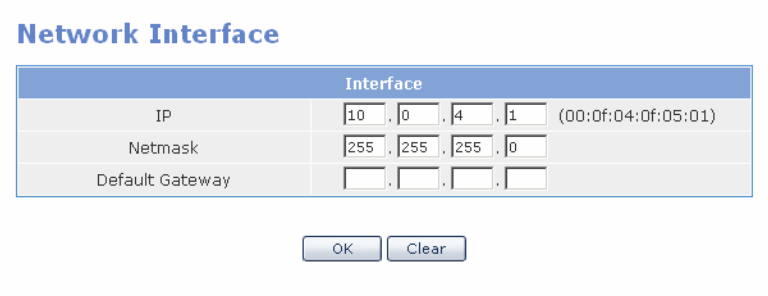
Menu	Submenu	Description
Appl Server	-	Used to allow remote access to the GPLIMT/GPLIM via SSH, FTP, and Telnet.
Reboot	-	Used to reboot the system.
Utility	Ping	Used to execute a Ping test

Network

The **[System] → [Network]** submenu is used to set the Management IP address and DNS information for the GPLIMT/GPLIM.

Network Interface

This section of the submenu is used to set the GPLIMT/GPLIM Management IP address and Netmask information. Enter the new IP address and Netmask information and then click the OK button to save the changes. The default value of the GPLIMT/GPLIM IP Address is 10.0.4.1/24.



Network Parameter Description

Parameter	Description
IP	Used to set the IP address information.
Netmask	Used to set the Netmask information.
Default Gateway	Used to set the default gateway IP information.

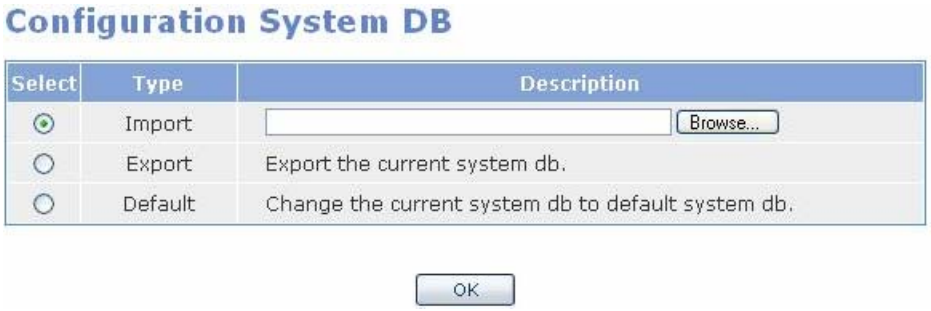
DNS

This section of the submenu is used to enter the Name Server information to be used in the GPLIMT/GPLIM.

Enter the IP address corresponding to the DNS server and then click the Add button.
The new setting is directly applied to the <**Static DNS**> window of the **[Interface] → [DNS]** submenu.

DB Config

Use the **[System]** → **[DB Config]** submenu to export the GPLIMT/GPLIM database, to import the GPLIMT/GPLIM database, or to default the GPLIMT/GPLIM to the factory defaults.



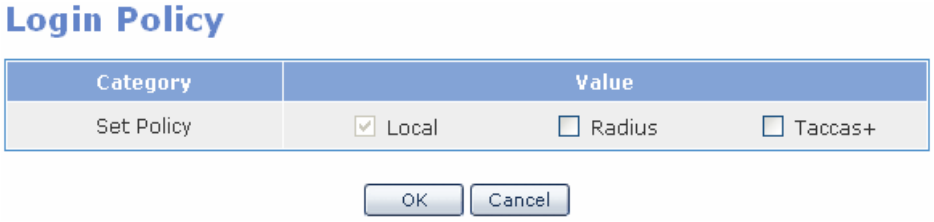
DB Config Parameter Description

Parameter	Description
Import	Used to restore a previously saved database
Export	Used to save the existing DB
Default	Used to restore the DB to factory defaults

After the GPLIMT/GPLIM is defaulted the adminstrator must use the default IP address 10.0.4.1 when using Web Management.

Admin Config

The **[System]** → **[Admin Config]** submenu is used to set up the authentication server for logging into the GPLIMT/GPLIM and for changing the Web Time-out configuration. The choices for authentication server are Local, Radius or Taccas+ . Check the box of the authentication method desired and then click the OK button to save the change. Once the setting is applied then the selected authentication method configuration window will be displayed.



Local

The local password is the Admin password that is used to access the GPLIMT/GPLIM switch using Telnet, SSH, FTP, and Web Management. Enter the new password and then click the OK button to save the change.

Radius

If a Radius server will be used then select the Radius box. Then enter the information for the Radius authentication server. Up to 5 lists can be entered.

Taccas+

If Taccas+ will be used then select the Taccas+ box. Enter the information for the Taccas+ authentication method. Up to 5 lists can be entered. When deleting the list of all the server IPs, the corresponding secret key values are also deleted.

Log

The **[System]** → **[Log]** submenu is used to allow the system log, to run system log reports, and to download a system log report to a file.

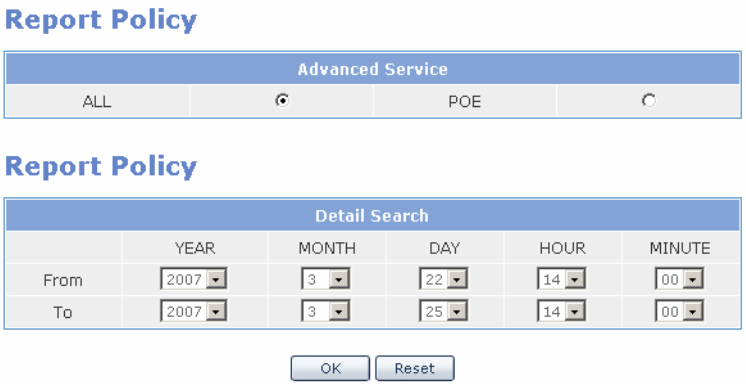
Configuration

The **[System]** → **[Log** → **[Configuration]** submenu is used to turn the logging feature on and off.

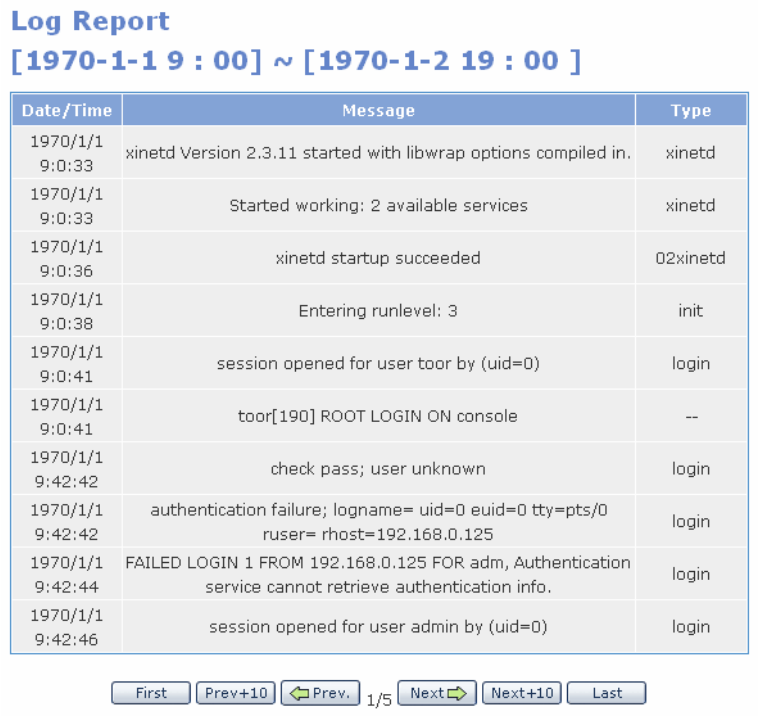
Click the ON or OFF radio button to enable or disable the logging for the GPLIMT/GPLIM and then click the OK button to save the change. Click the Reset button to return the Log Policy to the previous status before applying the change.

Report

Using the **[System] → [Log] → [Report]** submenu the administrator can retrieve the logs stored in the system according to attributes, date, and time.

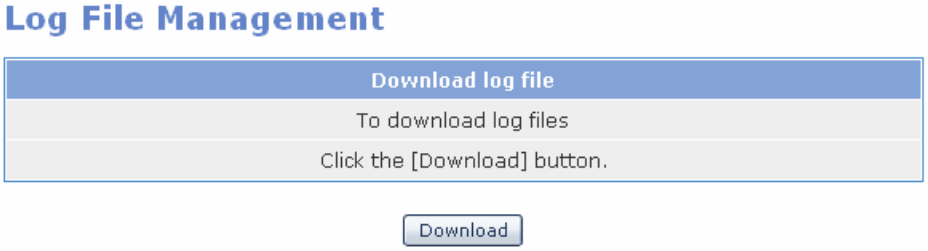


Click the radio button for the desired log type and then select the date and time. Then click the OK button to run the report. Click the Reset button to return the log report settings to default.



Download

Using the **[System] → [Log] → [Download]** submenu the administrator can download a log report to a PC. Simply press the Download button and the system log will be downloaded in the form of a compressed file.



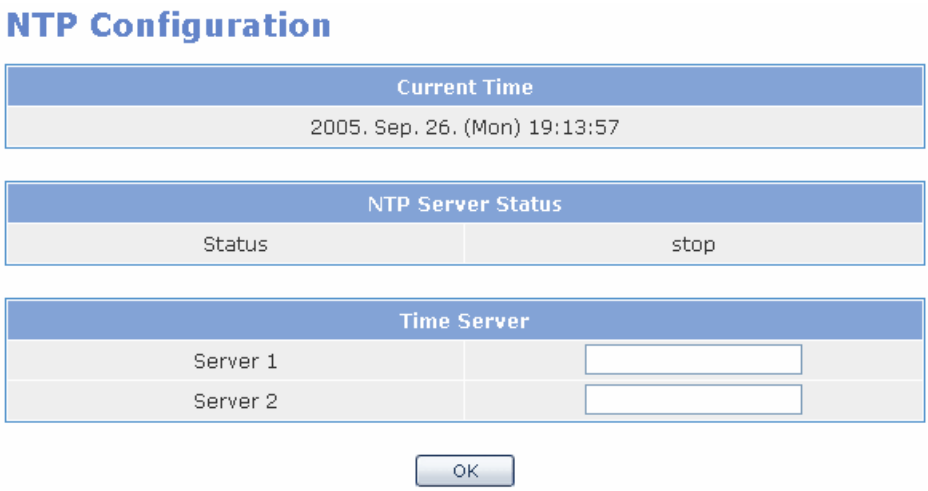
Time Configuration

Using the **[System] → [Time Configuration]** submenu the system administrator can either synchronize the date and time of the GPLIMT/GPLIM with a NTP server or manually set the date and time.

NTP Config

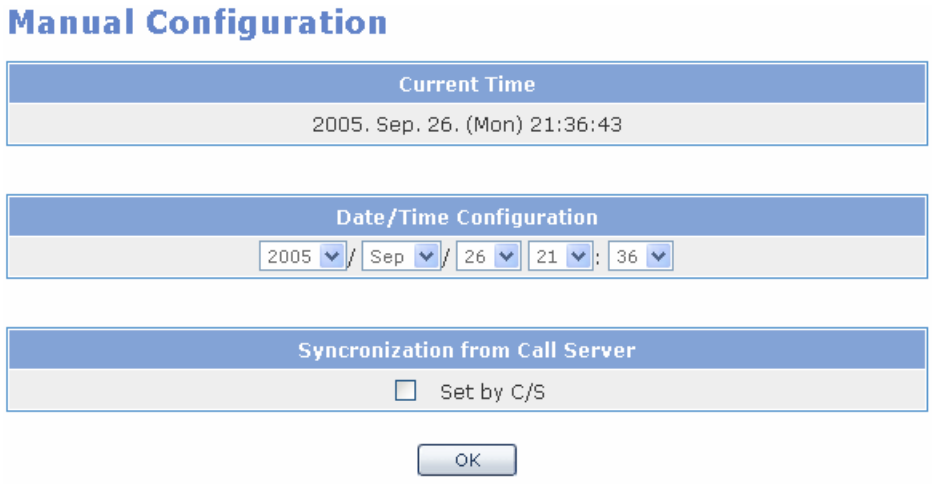
Use the **[System] → [Time Configuration] → [NTP Config]** submenu to set up a NTP Time Server/s to synchronize the date and time with the GPLIMT/GPLIM. The Current Time window indicates the current date and time of the GPLIMT/GPLIM. The NTP Server Status window indicates the status of NTP Server synchronization process.

The Time Server fields are used to enter the NTP Time Server IP Addresses. Click the OK button to start or restart the NTP daemon to register the Time Server.



Manual Config

By using the **[System] → [Time Configuration] → [Manual Config]** submenu the administrator can manually set and modify the date and time of the GPLIMT/GPLIM. In the Date/Time Configuration window enter the desired date and time and then click the OK button to save the changes. The new date and time will be displayed in the Current Time window. In order to synchronize the date and time of the system with the MP40 then check the Set by C/S box and then click the OK button to save the change..

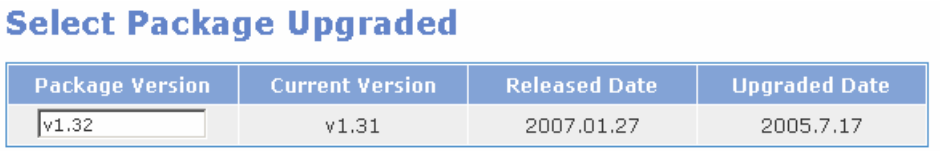


Timezone

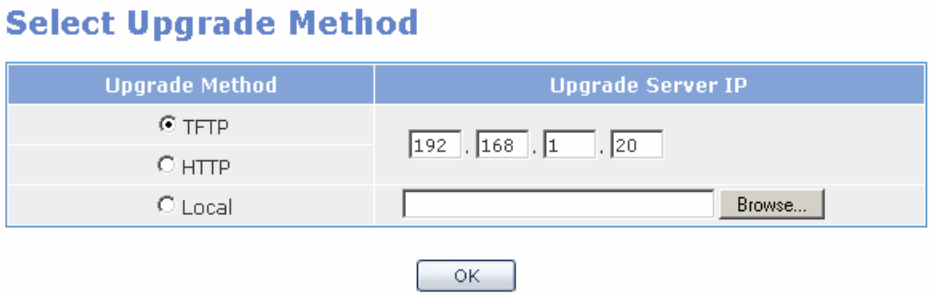
By using the **[System] → [Time Configuration] → [Timezone]** submenu the administrator can change Time Zones by selecting the desired timezone and then by clicking the OK button to save the change.

Upgrade

Upgrading the GPLIMT/GPLIM software is performed using the **[System] → [Upgrade]** submenu. First obtain the appropriate upgrade files . Then enter the new software package version number in the Package Version field.



Then select one of the three types of upgrade methods (TFTP, HTTP, or Local). If the Upgrde method is TFTP or HTTP enter the correct IP address of the server. Then click the OK button to start the upgrade process.



Appl Server

Using the **[System] → [Appl Server]** submenu the administrator can control remote access to the GPLIMT/GWPLIM using SSH, FTP and Telnet. In order to secure the system from hackers Samsung recommends that these are disabled and only turned on when the administrator needs to use them for debugging, and uploading or downloading files.

Check the box of the access method and then click the OK button to save the change.

Reboot

Using the **[System]** → **[Reboot]** submenu the administrator can reboot the GPLIMT/GPLIM.

Simply click the OK button and all the services will be terminated and the system will reboot.

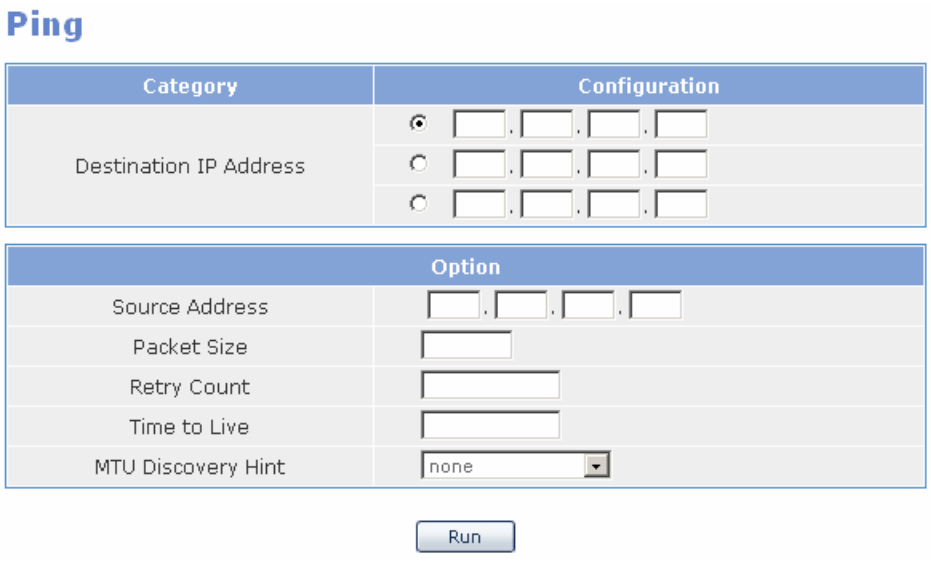
The webscreen will return to the initial login window and the webscreen will not operate until the network and services are all up and running

Utility

The GPLIMT/GPLIM is able to do both basic ping and extended ping tests. Select the **[System]** → [**Utility**] → [**Ping**] submenu to access the Ping function.

Ping

The Ping window is a table which is used to specify and execute the Ping test. When an administrator selects this submenu the following configuration window is displayed.



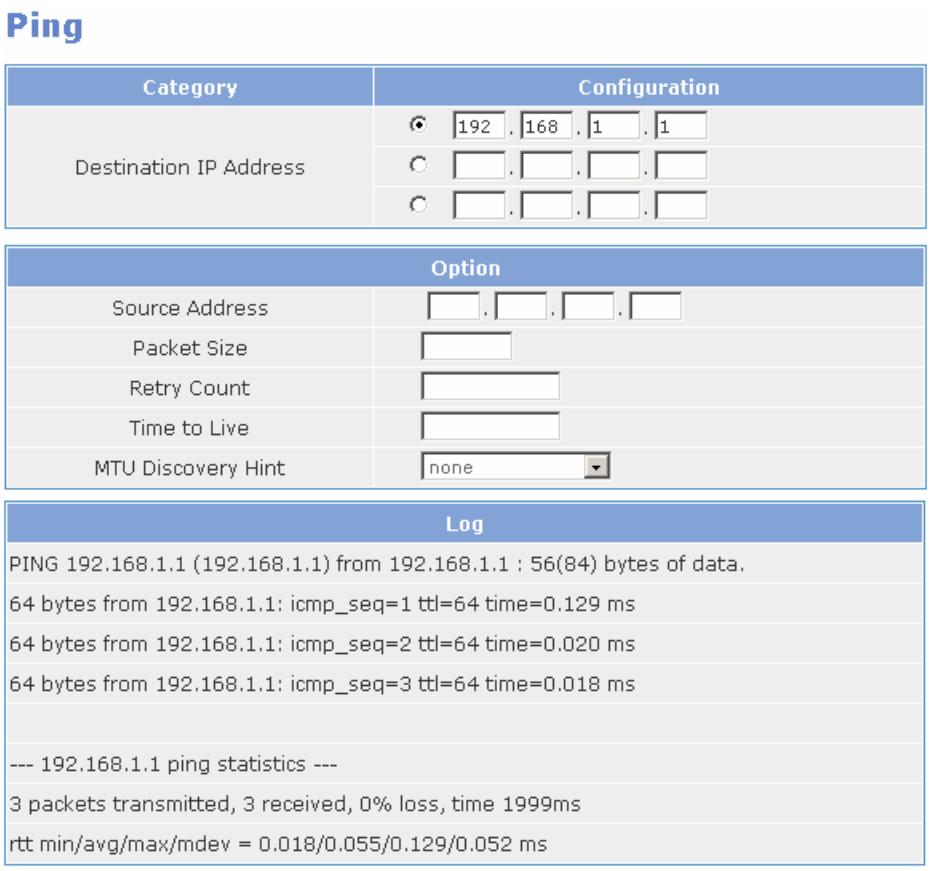
Ping Parameters

Parameter	Description
Destination IP Address	Used to enter the destination IP address for the Ping test

Parameter	Description
Source Address	Used to set the IP address of the interface for the Ping test
Packet Size	Used to set the packet size to be transmitted
Retry Count	Used to set the retry count. If it set to '0', there is no retry. Max is 3
Time to Live	Used to set the TTL value.
MTU Discovery Hint Selects the Path MTU Discovery method	None:
	Do: Uses PMTU but does not treat. In short, packet fragmentation does not occur
	Don't: Does not use PMTU at all. Since it does not set the DF field, the fragmentation may occur in remote site
	Want: Uses PMTU and treats appropriately. In short, if the packet size is longer than MTU, the packet fragmentation occurs

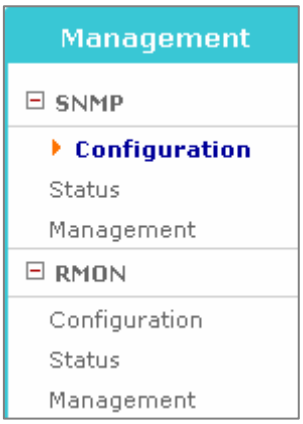
Enter the destination IP (and any exdeted ping parameters if needed) then click the Run button.

Only one destination IP can be tested at a time and the radio button of the IP Address to be tested must be checked. The radio button of the destination IP Address on the top of the list is set by default.



Management Menu

The SNMP and RMON settings are configured and managed using the **[Management]** menu. The submenus will be displayed in the upper left side of the window as follows:



Management Menu Description

Menu	Submenu	Description
SNMP	Configuration	Used to display the configuration items of SNMP.
	Status	Used to display the SNMP configuration currently configured.
	Management	Used to start or stop the SNMP service.
RMON	Configuration	Used to display the configuration items of RMON.
	Status	Used to display the RMON configuration currently configured.
	Management	Used to start or stop the RMON services.

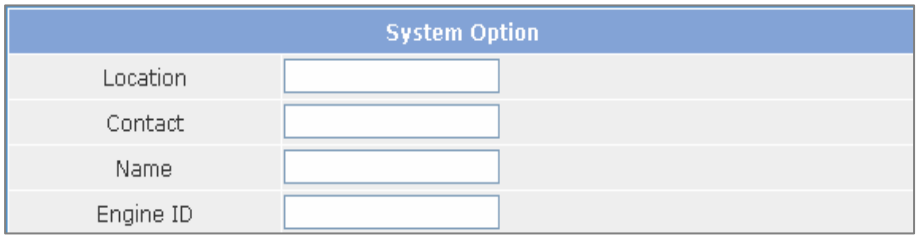
SNMP

Configuration

SNMP is a set of protocols used for managing complex networks. The **[SNMP]→[Configuration]** submenu is used by the administrator to enter SNMP System Options, SNMP Community information, SNMP v3 User information, and Trap Manager information. Once all the changes are entered then click the Save button at the bottom of the window. Click the Reset button to reset the configuration.

System Option

The following window is used to set up the SNMP System Options.



SNMP System Option Parameter Description

Parameter	Description
Location	Used to enter the information for System Location
Contact	Used to enter the information for System Contact
Name	Used to enter the information for System Name
Engine ID	Used to enter the information for System Engine ID

Community

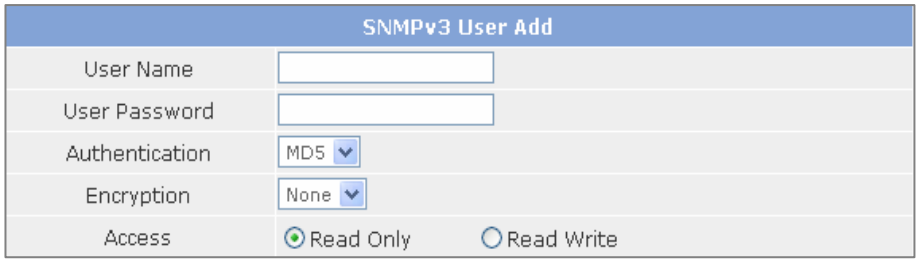
The following window is used to add new community information used in SNMP v1/2c.

Community Parameter Description

Parameter	Description
New Community name	Used to fill in the new community name being added
Community Network	Used to set up new community network
Access	Used to set up the access authority.

SNMPv3 Administrator Add

The following window is used to enter the SNMPv3 Administrator v3 information.



SNMP v3 Parameter Description

Parameter	Description
Administrator Name	Used to enter the new administrator's name
Administrator Password	Used to enter the new administrator's password (8 alphanumeric characters)
Authentication	Used to set up the authentication method.
Encryption	Used to set up the ciphering method.
Access	Set up access authority.

Trap Manager

The following window is used to set up the IP address used to transmit a trap. Up to five IP addresses can be entered.

Trap Manager Parameter Description

Parameter	Description
IP Address	Used to set up a new Trap IP Address
Community Name	Used to set up a community to be used for transmitting to the Trap IP Address added.

Status

The **[Management] → [SNMP] → [Status]** submenu is used to view the SNMP System Configuration information and to delete the SNMP Community, SNMPv3 User and SNMP Trap information. In order to delete the Community, User, and Trap settings select the box to the left of the item that needs to be deleted and then click the Delete button. Click the Reset button to initialize the settings.

SNMP Config Information

System Infomation	
Location	Seoul, Korea
Contact	support@
Name	OS7400-GSIM
Engine ID	GSIM

Select	Community Name	Community Net	Access
	private	local	Read Write
	public	anynet	Read Only

Select	User Name	Access
	root	Read Write

Select	Trap IP	Trap Port
☐	192.168.0.123	162

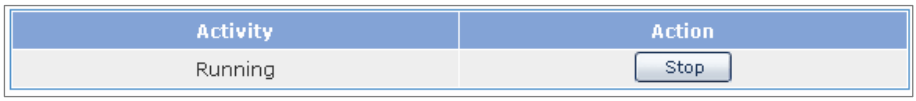
Status Field Description

Field	Description
System Information	This field displays the information set up for the System Options.
Select	Used to select the information to delete.
Community Name	This field display the community name.
Community Net	This field displays the configured name of the Community Network.
Community Access	This field displays the access authority of the configured community.
Administrator Name	This field displays the configured administrator's name.
Access	This field displays the access authority of the configured administrator.
Trap IP	This field displays the configured Trap IP.
Trap Port	This field displays the configured Trap Port.

Management

The **[Management]** → **[SNMP]** → **[Management] sub**menu is used to start and stop the SNMP service. Click the Run button to start the SNMP service and click the Stop button to halt the SNMP service.

SNMP Management



SNMP Management Field Description

Field	Description
Activity	This field displays the operational condition of the SNMPservice.
Action	Used to select whether to start or stop SNMP.

RMON

Configuration

Remote Monitoring *(RMON)* is a standard monitoring specification that enables various network monitors and console systems to exchange network-monitoring data. RMON provides network administrators with more freedom in selecting network-monitoring probes and consoles with features that meet their particular networking needs. Use the **[Management]** → **[RMON]** → **[Configuration]** submenu to begin configuring RMON.

Enter the History and Event Options and then click the Save button to apply the changes. Click the Reset button To initialize the RMON.

History Option

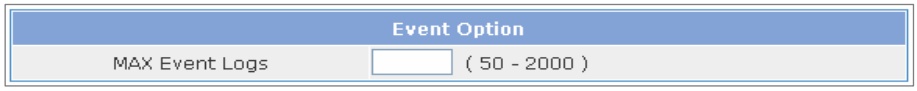
The History Option window is used to set up the RMON history options.

RMON Configuration Parameter Description

Parameter	Description
MAX History Buckets	Used to set up the maximum history storage space.
MIN History Interval	Used to set up the minimum history sample collection cycle.

Event Options

The Event Options window is used to set up the RMON event options.

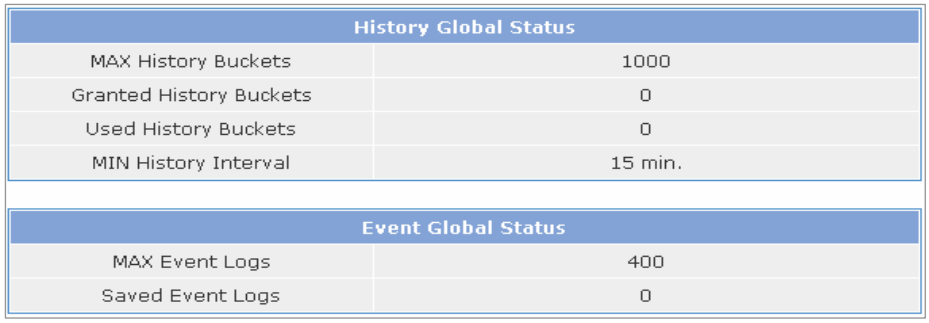


RMON Event Options Parameter Description

Parameter	Description
Max Event Logs	Used to set up the maximum number of Event Logs.

Status

The **[Management]** → **[RMON]** → **[Status]** submenu is used to view the RMON System Configuration.



RMON Global Status Field Description

Field	Description
MAX History Buckets	This field displays the maximum history storage space that has been set up.
Granted History Buckets	This field displays the history storage space that is currently allocated.
Used History Buckets	This field displays the history storage space that is currently used.

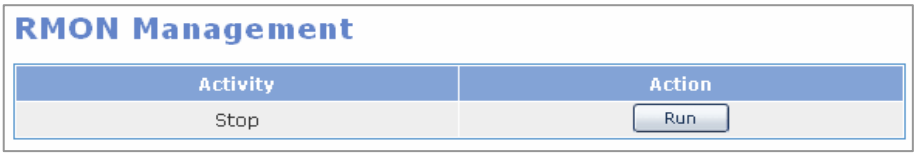
Field	Description
MIN History Interval	This field displays the minimum history sample collection cycle.
Max Event Logs	This field displays the maximum number of logs that are set up.
Saved Event Logs	This field displays the number of logs that is currently stored.

Management

The **[Management] → [RMON] → [Management]** submenu is used to start and stop the SNMP service. Click the Run button to start the RMON service and click the Stop button to halt the RMON service.

RMON Management

The administrator can start/stop the RMON service.

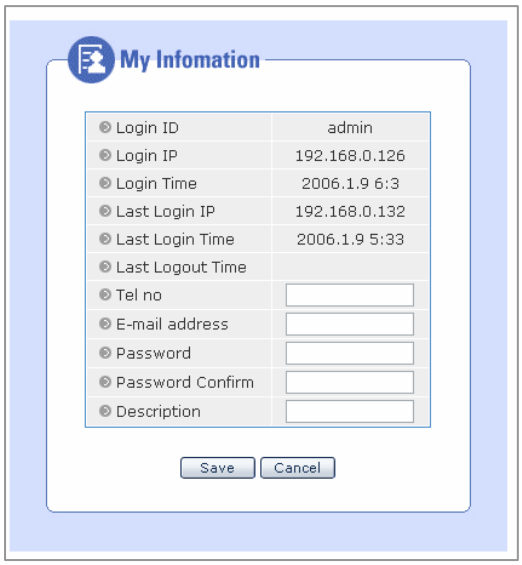


RMON Management Field Description

Item	Description
Activity	This field displays the operational status of the current service.
Action	Used to to start or stop RMON.

My Info Menu

Click the My Info icon on the upper right hand side of the GWIMT/GWIM Web Page to open the My Info window. In this window administrators can enter a telephone number, an E-mail address, and desciption of the router . This window is also used to enter the admin password which is used when logging into the GWIMT/GWIM router. Enter the new admin password into the Password and Password Confirm fields and then click the Save button.



My Info Parameters

Item	Description
Login ID	This field displays the login ID.
Login IP	This field displays the IP address of the PC logged into the GWIMT/GWIM.
Login Time	This field displays time when the login occued.
Last Login IP	This field displays the last login IP address.
Last Login Time	This field displays the last login time.
Last Logout Time	This field displays the last logout time.
Tel no	Used to enter the Telephone No. of the administrator
E-mail address	Used to enter the E-mail address of the administrator
Password	Used to enter the Password to be modified
Password Confirm	Used to enter the Password again to confirm the change
Description	Used to enter a Description of the Router

ABBREVIATION

A

ARP Address Resolution Protocol

B

BPDU Bridge Protocol Data Unit

C

CTI Computer Telephony Integration

D

DNS Domain Name Server

G

GPLIMT/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