

OfficeServ 7400 GWIM User Manual



COPYRIGHT

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

TRADEMARKS

Enterprise IP Solutions

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

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

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

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

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

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

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



INTRODUCTION

Purpose

This document introduces the OfficeServ 7400 GWIM, an application software of OfficeServ 7400, and describes procedures on installing and using the software.

Document Content and Organization

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

CHAPTER 1. Overview of OfficeServ 7400 GWIM

This chapter briefly introduces the OfficeServ 7400 GWIM.

CHAPTER 2. Installing OfficeServ 7400 GWIM

This chapter describes the installation procedure and login procedure.

CHAPTER 3. Using OfficeServ 7400 GWIM

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

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.

Reference

OfficeServ 7400 System Manual

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

OfficeServ 7400 Installation Manual

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

OfficeServ 7400 Service Manual

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

OfficeServ 7400 Programming Manual

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

OfficeServ 7400 GLIMP User Manual

OfficeServ 7400 GLIMP User Manual describes the configuration procedure and method of GLIMP, which is OfficeServ 7400 Application Software, depending on the functions of OfficeServ 7400.

Revision History

EDITION	DATE OF ISSUE	REMARKS
00	10. 2005.	Original Draft



This page is intentionally left blank.



SAFETY CONCERNS

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

Symbols



Caution

Indication of a general caution.



Restriction

Indication for prohibiting an action for a product.



Instruction

Indication for commanding a specifically required action.



CAUTION



For Security

Note that all external users are allowed to access the firewall when the Remote IP is set to '0.0.0.0' and Port is set to '0:'.



When Setting IP Range

The number of IPs for the 'Local IP range' and that for the 'Remote IP range' should be identical when setting PPTP VPN.

For example, if the number of IPs for 'Local IP range' is 10 and that for 'Remote IP range' is 20, only 10 calls will be set.



When Setting PPTP in Windows XP/2000

In Windows XP/2000, the user can use DHCP client. If VPN PPTP client is connected while the DHCP client is operating, errors will be found. To prevent this problem, close the DHCP client operation on the **[Start] → [Program] → [Administrative Tools] → [Services]** menu of the Windows PPTP client installed.



When Changing Network Interface

Note that all IP sessions in working are disconnected for a while if network interface(IP, Gateway, and Subnet Mask) is changed and finally applied during the router operation.



When Using a Web Browser

Use Microsoft Internet Explorer(version 6.0 or higher) as the web browser for the maintenance of GWIM. Other web browsers are not supported.

**When Using Dynamic IPs of DHCP, PPPoE, and VDSL**

When a dynamic IP is used, the public information of 'Port Forward' and 'Static NAT' is not automatically changed. Therefore, 'Fixed IPs' should be used for the VoIP related services that the setups of 'Port Forward' and 'Static NAT' menus are required. In addition, the 'Fixed IP' are used for the VPN services that the setups of WAN IP addresses are needed.

When Changing DB

If DB is changed in OfficeServ 7400 GWIM, the system restarts.

**When Using a Private Key**

The private key is provided with the package. The private key allows accessing SSH from the outside. Thus, only trusted administrator should use the key.

**When Deleting Internet Temporary Files**

If GWIM 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 GWIM may not be normally displayed.



This page is intentionally left blank.



TABLE OF CONTENTS

INTRODUCTION	I
Purpose	I
Document Content and Organization	I
Conventions.....	II
Console Screen Output	II
Reference	III
Revision History.....	III
SAFETY CONCERNS	V
Symbols.....	V
Caution	VI
CHAPTER 1. Overview of OfficeServ 7400 GWIM	1
Introduction to OfficeServ 7400	1
Introduction to OfficeServ 7400 GWIM	2
CHAPTER 2. Installing OfficeServ 7400 GWIM	5
Installing.....	5
Getting Started.....	7
CHAPTER 3. Using OfficeServ 7400 GWIM	9
Network Menu	10
Network	11
NLB	27
Firewall Menu	31
NAT.....	32

TABLE OF CONTENTS

Filter.....	37
Router.....	42
General.....	44
Configuration.....	45
List.....	54
Status.....	63
IPMC.....	67
General.....	68
Configuration.....	69
Status.....	77
QoS.....	79
Group.....	80
Policy.....	89
Management.....	90
Status.....	91
Connection.....	92
Statistics.....	93
Monitoring.....	94
Services.....	95
VPN Menu.....	97
IPSec.....	98
L2TP.....	107
PPTP.....	110
Status.....	113
IDS Menu.....	114
IDS Config.....	115
VoIP Service Menu.....	128
VoIP Service.....	128
SIP ALG Menu.....	131
Config.....	131
Management.....	133
System Menu.....	134
DB Config.....	135
Admin Config.....	136
Log.....	138
DHCP Server.....	141
DHCP Relay Agent.....	144

NTP Server.....	Ошибка! Закладка не определена.
Upgrade.....	148
Appl Server.....	149
Reboot.....	149
Management Menu	150
SNMP	151
RMON.....	154
ABBREVIATION	158
A ~ I	158
L ~ V	159



This page is intentionally left blank.



CHAPTER 1. Overview of OfficeServ 7400 GWIM

This chapter introduces OfficeServ 7400 system and OfficeServ 7400 GWIM.

Introduction to OfficeServ 7400

As an key phone system for small offices using less than 500 subscriber lines, OfficeServ 7400 supports not only voice calls but data transfer over a data network. Users on various platforms, such as a digital phone, IP phone, mobile phone, PC, and server, can conveniently use various telephony features and applications.

The OfficeServ 7400 is configured with a cabinet mounted on a 19-inch rack, internal station, wireless LAN device, and application software. Having a conventional server on a Linux platform outside of the cabinet, the OfficeServ 7400 provides the following application software:

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

Gigabit WAN Interface Module(GWIM) provides network functions such as a router and network security by inter-working with a call server or OfficeServ IP-UMS. This document describes the functions and the using method of OfficeServ 7400 GWIM Server.



NOTE

Structure of OfficeServ 7400

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

Introduction to OfficeServ 7400 GWIM

OfficeServ 7400 provides the following functions via GWIM based on IP:

Router Functions

- Path management and queuing function of data packets for external WAN and internal LAN
- Static and dynamic routing functions
 - Support of Routing Information Protocol version1(RIPv1), RIPv2, (Open Shortest Path First version2) OSPFv2, (Border Gateway Protocol 4) BGP4 routing protocol
- Dynamic Host Configuration Protocol(DHCP) Point-to-Point Protocol over Ethernet(PPPoE) client function in Ethernet WAN interface
- Encapsulation function of High-level Data Link Control(HDLC), PPP, and Frame Relay in Serial WAN interface
- Support of IP multicast
 - Support of IGMPv1(Internet Group Management Protocol version1), IGMPv2 protocols
 - Support of Distance Vector Multicast Routing Protocol(DVMRP), (Protocol Independent Multicast-Sparse Mode) PIM-SM multicast routing protocol
- Access interface function for WAN
 - 3-Gigabit Ethernet port: For WAN or LAN interface
 - 2-Serial WAN port: For data private line service by connecting to DSU or CSU, which is data line equipment(support of V.35 1 port and HSSI 1 port)
- Network Load Balance(NLB) function
 - Function that equally distributes the load by setting several gigabit Ethernets or serial interfaces into WAN and increases the availability by automatically sharing the load with other lines when a line is not operated.

Data Network Security Functions

- Outbound and Inbound NAT(Network Address Translation)/PT(Protocol Translation) function
 - Access control for internal resources via the conversion between common IP and public IP
- Firewall function
 - Access control from the outside by Extended Access List

- Intrusion Detection System(IDS) function
 - Detection and report of the access for the access control area by the access list
 - Recognition and notification of illegal packets by applying the basic intrusion rule for packets
 - Detection and block of DoS attack such as SYN Flood
- Virtual Private Network VPN function
 - VPN gateway function based on Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol(L2TP), and Internet Protocol Security protocol(IPSec)
 - Confidentiality and integrity functions via VPN tunneling and data encryption

Data Network Application Functions

- Data network application functions such as NAT/PT, firewall, VPN, DHCP, and Application Level Gateway(ALG)
- Use of Application Software operating in GWIM board
- ALG function
 - Support to operate the security function and smoothly pass the VoIP packets by implementing the AIG function for signaling and media traffic
- DHCP Server function
 - Auto-configuration of network environment for the IP equipment in another functional block of the OfficeServ 7400 system
- DHCP Relay function
 - Function to connect the IP equipment in another functional block of the OfficeServ 7400 system to external DHCP server for the auto-configuration of network environment

QoS Function

- Priority queuing process for layer 3 packets and priority queuing for a specified IP
- Priority queuing process for layer 4 packets and priority for RTP packets (UDP/TCP port)

Management Function

- Advanced debugging function via Telnet connection
- Configuration and verification functions for the operations of GWIM functional block via a browser
- Configuration and verification functions for the operations of GWIM functional block via the Simple Network Management Protocol(SNMP)
- 4 Real-time Monitoring(4RMON) function
- Program Upgrade
 - Program upgrade via Trivial File Transfer Protocol(TFTP)
 - Program upgrade via Hypertext Transfer Protocol(HTTP)
 - Program upgrade via local manager's PC



CHAPTER 2. Installing OfficeServ 7400 GWIM

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

Installing

Since software package is included in the OfficeServ 7400 GWIM system, additional installation of software is not required. The GWIM software package is composed of items described below:

Package	File	Description
Bootrom Package	gwim-bootldr.img-vx.xx	Boot ROM program
	gwim-bootldr.img-vx.xx.sum	
Main Package	gwim-pkg-vx.xx.tar.gz	Upgrade package for HTTP
	gwim-os..img-vx.xx	'os' partition upgrade package for TFTP
	gwim-firmware.img-vx.xx	'Firmware' partition upgrade package for TFTP
	gwim-configdb.img-vx.xx	'configdb' partition upgrade package for TFTP
	gwim-logdb.img-vx.xx	'logdb' partition upgrade package for TFTP
	gwim-flash1.img-vx.xx gwim-flash1.img-vx.xx.sum	Fusing file for the first flash memory
	gwim-flash2.img-vx.xx gwim-flash2.img-vx.xx.sum	Fusing file for the second flash memory



NOTE

Software Package Configuration

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

Configure the environment as follows to access GWIM.

1. Mount the GWM board on a slot of OfficeServ 7400.
2. Connect a PC to port #3 of the GWIM board.
3. Run the Internet Explorer from the PC and access the IP(10.0.2.1) of GWIM of Port #3. The IP initial value of the GWIM board is set as follows:
 - Port 1 - 10.0.0.1/24
 - Port 2 - 10.0.1.1/24
 - Port 3 - 10.0.2.1/24



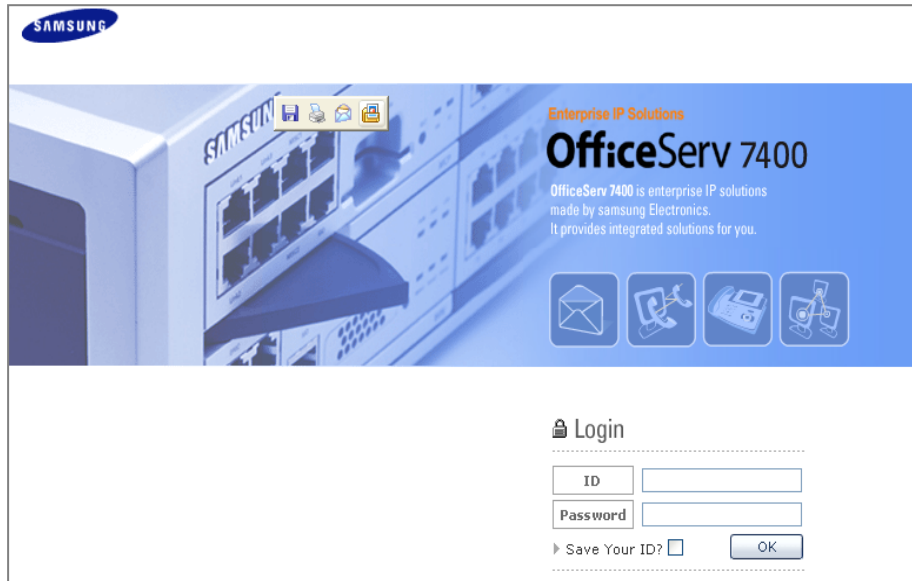
CAUTION

Caution for the Use of a Web Browser

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

Getting Started

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



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

The screenshot displays the OfficeServ 7400 GWIM configuration interface. At the top, the title 'OfficeServ 7400' is visible, followed by a navigation bar with 'Administrator' selected and other options like 'Network', 'Firewall', 'Router', etc. A left sidebar shows a tree view with 'Network' expanded and 'Ethernet0' selected. The main content area shows configuration options for the selected interface:

- Interface Type:** WAN (selected), LAN, NONE
- Protocol Type:** Static IP (selected), PPPoE, DHCP

Below this, the 'WAN : Static IP' section is active, showing the following configuration:

Ethernet Interface				
IP	192	168	17	100
Netmask	255	255	0	0
MTU	1500			Byte

The 'Option' section below shows:

Option				
Gateway	192	168	0	1
Default Gateway				<input checked="" type="checkbox"/>

At the bottom, the 'Transparent Proxy' section is partially visible, showing fields for 'IP' and 'Netmask'.

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



CHAPTER 3. Using OfficeServ 7400 GWIM

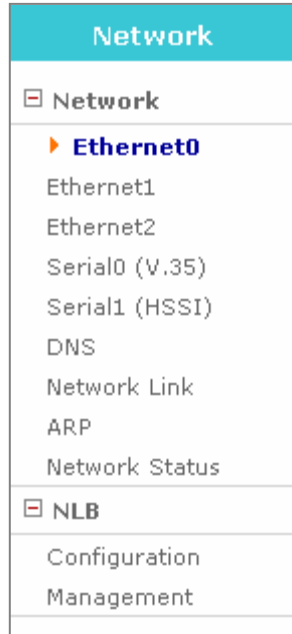
This chapter describes how to use the menus of OfficeServ 7400 GWIM.

The configuration of OfficeServ 7400 GWIM menus is as follows:

Network	Firewall	Router	IPMC	QoS	Status
<ul style="list-style-type: none"> [-] Network ▶ Ethernet0 <ul style="list-style-type: none"> Ethernet1 Ethernet2 Serial0 (V.35) Serial1 (HSSI) DNS Network Link ARP Network Status NLB <ul style="list-style-type: none"> Configuration Management 	<ul style="list-style-type: none"> [-] NAT <ul style="list-style-type: none"> ▶ Management <ul style="list-style-type: none"> Configuration Port Forward Static NAT [-] Filter <ul style="list-style-type: none"> Management Configuration Remote Access IP Filtering URL Filtering ICMP Redirect 	<ul style="list-style-type: none"> [-] General <ul style="list-style-type: none"> ▶ Routes <ul style="list-style-type: none"> Management [-] Configuration <ul style="list-style-type: none"> Static RIP RIP Interface OSPF OSPF Interface BGP [-] List <ul style="list-style-type: none"> Access List Prefix List 	<ul style="list-style-type: none"> [-] General <ul style="list-style-type: none"> ▶ Mroutes <ul style="list-style-type: none"> Management [-] Configuration <ul style="list-style-type: none"> IGMP DVMRP DVMRP Intf PIM-SM PIM-SM Intf [-] Status <ul style="list-style-type: none"> IGMP Groups DVMRP PIM-SM 	<ul style="list-style-type: none"> [-] Group <ul style="list-style-type: none"> ▶ Port Group <ul style="list-style-type: none"> IP Group Filter Group Class Group Policy <ul style="list-style-type: none"> Management 	<ul style="list-style-type: none"> [-] Connection <ul style="list-style-type: none"> ▶ Sessions <ul style="list-style-type: none"> IP Group Filter Group Devices Protocols [-] Monitoring <ul style="list-style-type: none"> Current History Process Service
VPN	IDS	DSMI	SIP ALG	System	Management
<ul style="list-style-type: none"> [-] IPSEC <ul style="list-style-type: none"> ▶ Configuration <ul style="list-style-type: none"> Certificate Management L2TP <ul style="list-style-type: none"> Configuration Management PPTP <ul style="list-style-type: none"> Configuration Management STATUS <ul style="list-style-type: none"> Ipssec L2tp/pptp 	<ul style="list-style-type: none"> [-] IDS Config <ul style="list-style-type: none"> ▶ Log Analysis <ul style="list-style-type: none"> Configuration Rule Config Mail Config Block Config Management 	<ul style="list-style-type: none"> [-] VoIP Service <ul style="list-style-type: none"> ▶ Configuration <ul style="list-style-type: none"> management [-] VoIP Status <ul style="list-style-type: none"> VoIP Status VoIP NAPT Status 	<ul style="list-style-type: none"> Configuration Management 	<ul style="list-style-type: none"> DB Config Admin Config <ul style="list-style-type: none"> [-] Log <ul style="list-style-type: none"> Configuration Report Download [-] DHCP Server <ul style="list-style-type: none"> Configuration Management Lease Info [-] DHCP Relay Agent <ul style="list-style-type: none"> Configuration Management Time Configuration 	<ul style="list-style-type: none"> [-] SNMP <ul style="list-style-type: none"> ▶ Configuration <ul style="list-style-type: none"> Status Management [-] RMON <ul style="list-style-type: none"> Configuration Status Management

Network Menu

Select the [**Network**] menu of GWIM to display its submenus on the top left of the screen.



Menu	Submenu	Description
Network	Ethernet0	User setup for Ethernet port P1.
	Ethernet1	User setup for Ethernet port P2.
	Ethernet2	User setup for Ethernet port P3.
	Serial0(V.35)	Sets V.35 Serial ports.
	Serial1(HSSI)	Sets HSSI Serial ports.
	DNS	Sets domain name servers.
	Network Link	Sets the speed and transfer method of Ethernet port.
	ARP	Manages the addition/deletion of ARP.
	Network status	Briefly displays the setup information on all ports.

Network

The **[Network]** menu is a menu that basically sets five network interfaces built-in the OfficeServ 7400 system. The menu sets IP address, transfer speed, and transfer mode in accordance with each interface and selects the connection of each interface with the Internet line or the internal line. In addition, this menu sets DNS and ARP.

On the feature of network equipment. The **[Network]** menu is the basic menu that should be set before the setup of other functions.

Ethernet Setup

Select **[Network]** → **[Ethernet]** menu to configure the Ethernet port.

Select one of three Ethernet categories to display the setup window below. The selection fields are displayed depending on the method used for the corresponding interface. According to the selection of fields, different sub-setup window is displayed on the lower section of the window. The details by fields are as follows:

Interface Type	<input checked="" type="radio"/> WAN	<input type="radio"/> LAN	<input type="radio"/> NONE
Protocol Type	<input checked="" type="radio"/> Static IP	<input type="radio"/> PPPoE	<input type="radio"/> DHCP

- **WAN:** Select to set as the interface for the connection with the external network link Internet line. The following protocol types can be selected in WAN:
 - **Static IP:** Select to connect dedicated lines and ADSL lines on the basis of fixed IP.
 - **PPPoE:** Select to connect general ADSL lines on the basis of dynamic IP.
 - **DHCP:** Select to connect cable lines.
- **LAN:** Select to set as the interface to connect internal network. The following protocol types can be selected in LAN:
 - **Private:** Select to construct the internal network based on private IP address.
 - **Public:** Select to construct the internal network based on public IP address.
- **NONE:** Select when the corresponding interface is not used.

The detailed setup in accordance with the selection of each field is as follows:

WAN → Static IP

Select the WAN-Static IP category to display the following configuration window: The details by fields are as follows:

WAN : Static IP

Ethernet Interface	
IP	192 . 168 . 17 . 100
Netmask	255 . 255 . 0 . 0
MTU	1500 Byte

Option	
Gateway	192 . 168 . 0 . 1
Default Gateway	<input checked="" type="checkbox"/>

Transparent Proxy

IP	Netmask
----	---------

Add Delete

IP Alias

IP	Netmask
----	---------

Add Delete

OK

- WAN: Static IP
 - IP: Enter the public IP address assigned to the current network interface.
 - Network: Enter the netmask address of the current network interface.
 - Gateway: Enter the public IP address received from Internet Service Provider or the IP address of a router.
 - Default Gateway: Mark the check box in the Default Gateway field to select the default gateway interface when two interfaces are used for the external network.

- **Transparent Proxy:** Proxy-ARP is used when hosts or networks are added in the Transparent Proxy field. Up to 128 Proxy-ARPs can be set in the OfficeServ 7400 system without the change of the existing network. To add entries, click the **[Add]** button and enter the following IP address and netmask . To delete entries, select the entry to be deleted and click the **[Delete]** button.
- **IP Alias:** Is used to add up to 32 IP addresses. To add entries, click the **[Add]** button and enter the following IP address and netmask . To delete entries, select the entry to be deleted and click the **[Delete]** button.

WAN → PPPoE

Select the WAN-PPPoE field to display the following setup window: Enter ID and Password of the ADSL account that is assigned from the ISP providing ADSL service based on dynamic IP.

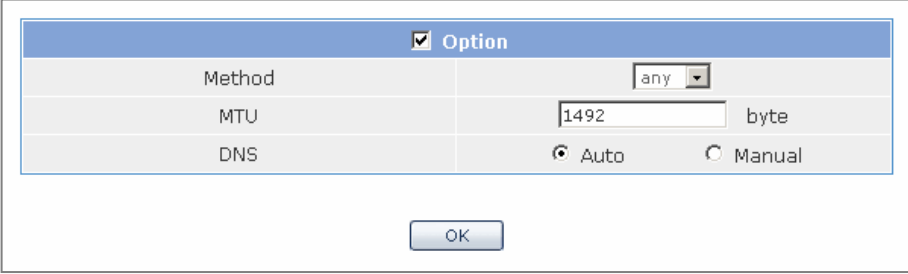
Authentication	
ID	innopia
Password	••••••

Option
<input type="checkbox"/>

OK

Mark the check box of the Option field in the lower section to display Method, MTU, and DNS setup window. This field displays the additional configuration window for the more detailed service.

The details by fields are as follows:



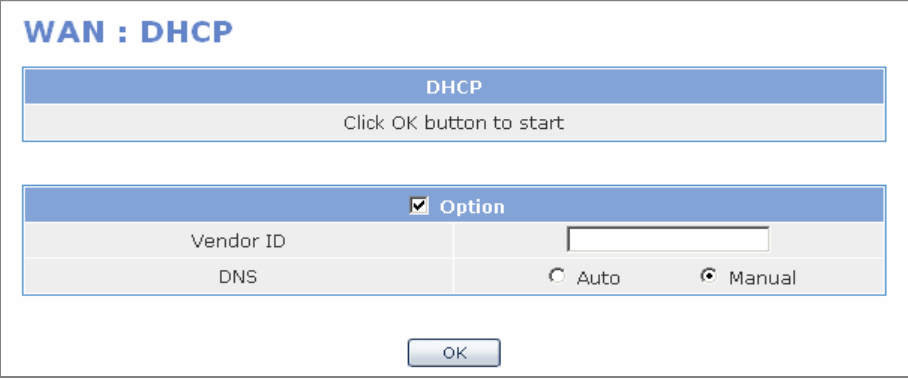
The screenshot shows a configuration dialog box with a blue header bar containing a checked checkbox and the text "Option". Below the header is a table with three rows: "Method" with a dropdown menu showing "any", "MTU" with a text input field containing "1492" and the unit "byte", and "DNS" with two radio buttons, "Auto" (selected) and "Manual". At the bottom center of the dialog is an "OK" button.

- Method: Authentication Method
- MTU: Input of the maximum transmission frame size(default: 1412)
- DNS
 - Auto: Automatically receives DNS information from ISP
 - manual: Does not receive DNS information.

WAN → DHCP

WAN → DHCP field is automatically set without a special setup field. Therefore, press the [OK] button to complete the setup.

For cable modem service that requires detailed setup, mark the check box in the Option field to display the detailed setup field. To enter a vendor ID or fetch the DNS information, check [Auto].



The screenshot shows a configuration dialog box with a blue header bar containing the text "WAN : DHCP". Below the header is a section titled "DHCP" with the instruction "Click OK button to start". Below this is another configuration dialog box with a blue header bar containing a checked checkbox and the text "Option". Below the header is a table with two rows: "Vendor ID" with a text input field, and "DNS" with two radio buttons, "Auto" (selected) and "Manual". At the bottom center of the dialog is an "OK" button.

LAN → Private IP

For the construction of the internal network on the basis of private IP address, select LAN-Private IP.

Enter the IP address and the netmask value to be assigned to the network interface connected to the internal network in the IP field and the netmask field of the 'LAN: Private IP' table below. The IP Alias field is the same as the corresponding input field displayed when selecting WAN → Static IP. After the completion of the setup, click the [OK] button.

LAN : Private IP

Ethernet Interface	
IP	<input type="text" value="10"/> , <input type="text" value="100"/> , <input type="text" value="100"/> , <input type="text" value="1"/>
Netmask	<input type="text" value="255"/> , <input type="text" value="255"/> , <input type="text" value="255"/> , <input type="text" value="0"/>
MTU	<input type="text" value="1500"/> Byte

IP Alias

IP	Netmask
----	---------

LAN → public IP

For the construction of the internal network on the basis of public IP address, select LAN-public IP field. For this case, enter the IP address and the netmask provided by ISP. The IP Alias and the Transparent proxy field is the same as the corresponding input field displayed when selecting WAN → Static IP. After the completion of the setup, click the [OK] button.

LAN : Public IP

Ethernet Interface	
IP	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Netmask	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
MTU	<input type="text" value="1500"/> Byte

Transparent Proxy

IP	Netmask
----	---------

IP Alias

IP	Netmask
----	---------

NONE

NONE is selected when the corresponding interface is not used.

NONE

Description
Disable network interface

Setup of Serial0 (V.35) and Serial1 (HSSI)

These menus are used for the setup of V.35 Serial port and HSSI Serial port. The procedure to set up the V.35 Serial port and the HSSI Serial port is equal.

Interface Type

The Interface Type table is configured in the same way as that of Ethernet. Refer to the Interface Type setup of Ethernet setup.

Interface Type	<input type="radio"/> WAN	<input type="radio"/> LAN	<input checked="" type="radio"/> NONE
----------------	---------------------------	---------------------------	---------------------------------------

Serial Basic

The Serial Basic table sets the basic information of Serial Interface. Select one of Serial Protocols in the Encapsulation field of this table to display the window to set each protocol.

Serial Basic	
Command	Argument
Serial Interface Name	Serial0
Physical Line Type	V.35
MTU	<input type="text" value="1500"/> (128~1500, Default: 1500)
Encapsulation	<input checked="" type="radio"/> Cisco-HDLC <input type="radio"/> PPP <input type="radio"/> Frame-Relay <input type="radio"/> None

- Serial Interface Name: Name of the current serial port
- Physical Line Type: Physical line type of the current serial port
- MTU: Maximum size of the packet to transfer at once
- Encapsulation: Serial protocol to be used

Cisco-HDLC Configuration

Set the Encapsulation of the Serial Basic table as Cisco-HDLC to display the Cisco-HDLC Configuration window. Specify the value for each field, and click the [OK] button to store the configuration.

Cisco-HDLC Configuration	
Command	Argument
Keep-Alive Interval	<input type="text" value="10"/> (1~100, Default: 10)
Keep-Alive Timeout	<input type="text" value="25"/> (1~100, Default: 25)
IP Address	<input type="text" value="172"/> . <input type="text" value="16"/> . <input type="text" value="0"/> . <input type="text" value="2"/> / <input type="text" value="16"/>
Gateway	<input type="text" value="172"/> . <input type="text" value="16"/> . <input type="text" value="0"/> . <input type="text" value="1"/>

- Keep-Alive Interval: Time interval to check Keep-Alive
- Keep-Alive Timeout: Time to estimate the failure of Keep-Alive
- IP Address: IP Address of the serial port
- Gateway: Gateway IP Address(Peer Address) of the serial port

PPP Configuration

Select PPP Protocol in the Encapsulation field of the Serial Basic table to display the PPP Configuration table. Specify the value for each field, and click the [OK] button to store the configuration.

PPP Configuration	
Command	Argument
Keep-Alive Interval	<input type="text" value="10"/> (1-100, Default: 10)
Max Keep-Alive Count	<input type="text" value="6"/> (1-100, Default: 6)
Authentication	<input type="radio"/> PAP <input type="radio"/> CHAP <input checked="" type="radio"/> None Name: <input type="text"/> Password: <input type="text"/>
IPCP Dynamic-IP	<input type="checkbox"/> (enable IP-Address negotiation at IPCP layer)
IP Address	<input type="text" value="172"/> . <input type="text" value="16"/> . <input type="text" value="0"/> . <input type="text" value="2"/> / <input type="text" value="16"/>
Gateway	<input type="text" value="172"/> . <input type="text" value="16"/> . <input type="text" value="0"/> . <input type="text" value="1"/>

- Keep-Alive Interval: Time interval to check Keep-Alive
- Max Keep-Alive Count: Count of Keep-Alives to estimate as the disconnection
- Authentication: Information for PPP authentication
PAP, CHAP and None: Authentication method
Name and Password: User ID and Password
- IPCP Dynamic-IP: Use of Dynamic-IP function to support IPCP
- IP Address: IP Address of the serial port
- Gateway: Gateway IP Address(Peer Address) of the serial port

Frame-Relay Configuration

Select Frame-Relay protocol to display the Frame-Relay Configuration table. Specify the value of each field, and click the **[OK]** button to store the configuration.

Frame-Relay Configuration	
Command	Argument
LMI Type	<input checked="" type="radio"/> ANSI <input type="radio"/> CCITT <input type="radio"/> None
Keep-Alive Interval	<input type="text" value="10"/> (5~30 seconds, Default: 10)
N391	<input type="text" value="6"/> (1~255 full status polling counter, Default: 6)
N392	<input type="text" value="3"/> (1~10 LMI error threshold, Default: 3)
N393	<input type="text" value="4"/> (1~10 LMI monitored event count, Default: 4)

- LMI Type: LMI type of Frame-Relay
- Keep-Alive Interval: Time interval to check Keep-Alive
- N391: Cycle to request all status information. The information on all status is requested at every cycle specified in the N391 field. As usual, only Keep-Alive is exchanged.
- N392: Count of Keep-Alives to estimate as the disconnection
- N393: Buffer size to record success/failure of Keep-Alive. The value of N393 should be bigger than that of N393.

PVC Interface

Select the Frame-Relay protocol to display the PVC Interface table. Enter the value of each field and press the **[Add]** button to create new PVC.

PVC Interface

Command	Argument
DLCI	<input type="text" value="16"/> (16~1007)
IP Address	<input type="text" value="172"/> . <input type="text" value="16"/> . <input type="text" value="0"/> . <input type="text" value="2"/> / <input type="text" value="16"/>
Gateway	<input type="text" value="172"/> . <input type="text" value="16"/> . <input type="text" value="0"/> . <input type="text" value="1"/>
MTU	<input type="text" value="1500"/> (128~1500, Default: 1500)

- DLCI: Number of DLCI(a type of network address)
- IP Address: IP Address to be used by PVC
- Gateway: Gateway IP Address(Peer Address) of PVC
- MTU: Maximum size of the packet to transfer at once

To delete a specific PVC, mark the check box of the corresponding PVC and click the **[Delete]** button.

PVC Interfaces

	Interface	Address	Gateway	Active	MTU
<input type="checkbox"/>	pvc0/16	172.16.0.2/16	172.16.0.1	yes	1500
<input type="checkbox"/>	pvc0/17	172.17.0.2/16	172.17.0.1	no	1500
<input type="checkbox"/>	pvc0/18	172.18.0.2/16	172.18.0.1	no	1500

Serial Interface Summary

The Serial Interface Summary table briefly displays the current information of the serial port. The following figure is an example that uses Cisco-HDLC protocol and specifies the IP address as 172.16.0.2/16.

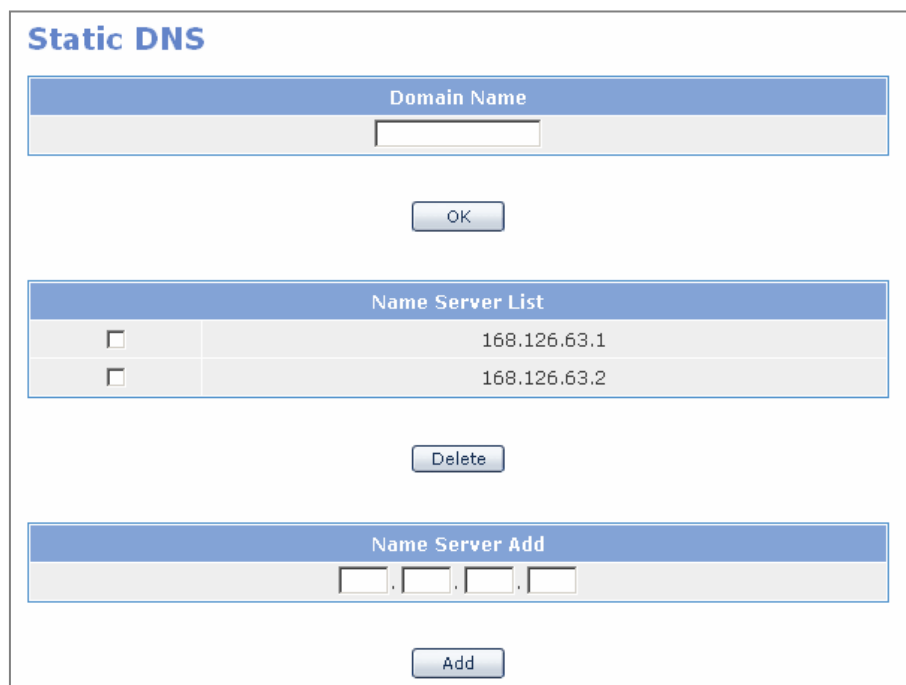
Serial0 Interface Summary

```
Serial0 Interface Summary
Interface Serial0
Scope: both
Mode type is
Protocol type is Cisco-HDLC
Transparent is
pppoe_mtu is 1492
pppoe_username is
Pseudo name is
PPPOE client is disabled
Hardware is Unknown
index 5 metric 1 mtu 1500 <UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>
VRF Binding: Not bound
DHCP client is disabled.
inet 172.16.0.2/16 pointopoint 172.16.0.1
physical line type is V.35
encapsulation protocol is Cisco HDLC
keepalive interval 10 timeout 25
input packets 122, bytes 8808, dropped 0, multicast packets 0
input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
output packets 103, bytes 4804, dropped 0
output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
collisions 0
```

Refresh

DNS

DNS menu is used for the setup of DNS server. Click this menu to display the following configuration window. Enter the domain name and the IP address of DNS server to the Domain name field and the DNS server field. After then, click the [OK] button to store the domain name and the IP address.



The image shows a 'Static DNS' configuration window with three main sections:

- Domain Name:** A text input field for entering the domain name, with an 'OK' button below it.
- Name Server List:** A table with two rows, each containing a checkbox and an IP address.

Name Server List	
<input type="checkbox"/>	168.126.63.1
<input type="checkbox"/>	168.126.63.2

A 'Delete' button is located below the table.
- Name Server Add:** A text input field for entering a new IP address in dotted decimal format (four boxes separated by dots), with an 'Add' button below it.

Network Link

The Network Link menu is used for the setup of connections, transmission speeds and transmission modes by network interfaces. Click this menu to display the following configuration window. The details by fields are as follows:

Network Link

	Ethernet	Type	Negotiation	Speed	Duplex	Mac
<input type="checkbox"/>	Ethernet0	iTECTechnologies-SX SFP24-MS3LC	auto	1000Mbps	full	00:00:f0:11:32:24
<input type="checkbox"/>	Ethernet1	AGILENT-SX HFBR-5710L	force	1000Mbps	full	00:00:f0:11:32:25
<input type="checkbox"/>	Ethernet2	AGILENT-SX HFBR-5710L	auto	1000Mbps	full	00:00:f0:11:32:26

- Ethernet: Name of each Ethernet
- Type: Type of Ethernet Cables
- Negotiation: Setup of auto and force modes
- Speed(Mbps): Transmission bandwidth of the corresponding Ethernet interface
- Duplex: Transfer mode of the corresponding Ethernet interface
- MAC: MAC addresses by Ethernet interfaces

ARP

The ARP menu is used for the addition/deletion/management of the ARP information in each Ether interface.

Arp list

According to each interface, the ARP table is displayed on the ARP List window. Use the **[Refresh]** button and the **[Delete]** button to update and delete the current arp table, respectively.

ARP List

Ethernet
 Ethernet 0
 Ethernet 1
 Ethernet 2

	Type	IP	Mac
<input type="checkbox"/>	reachable	192.168.0.126	00:09:74:11:11:11
<input type="checkbox"/>	reachable	192.168.0.1	00:09:74:00:10:03

- type: arp status
- ip: ip address sent arp
- mac: mac address sent arp

static arp add

The Static ARP Add window is used for the addition of static arp, which is a permanent type.

Static ARP Add

Ethernet	IP	Mac
Ethernet0 ▾	<input style="width: 20px;" type="text"/> . <input style="width: 20px;" type="text"/> . <input style="width: 20px;" type="text"/> . <input style="width: 20px;" type="text"/>	<input style="width: 20px;" type="text"/> : <input style="width: 20px;" type="text"/> : <input style="width: 20px;" type="text"/> : <input style="width: 20px;" type="text"/> : <input style="width: 20px;" type="text"/> : <input style="width: 20px;" type="text"/>

- Ethernet: Ethernet to add static Mac
- Ip: ip to be added
- Mac: mac to be added

ARP Age Time

The ARP Age Time window is used for the setup of the cycle(at least 600 sec. unit: sec.) to delete the unused ARP in the ARP table.

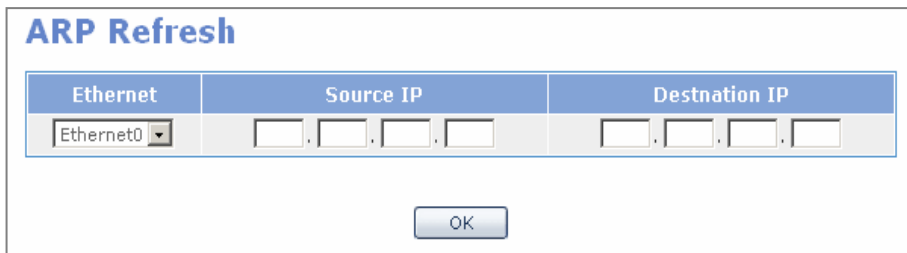


Time
600 sec

OK

Arp refresh

The ARP Refresh window is used for the modification of the changed ARP information in the ARP table of a route or a host when the network is changed. In the host or the route with the destination IP, the Mac with the current source IP is updated into the Ethernet Mac of the OfficeServ 7400 system.



Ethernet	Source IP	Destination IP
Ethernet0

OK

- Ethernet: Ethernet to be changed
- Source IP: IP to be changed
- Destination IP: host or Mac to be changed

Network status

Select the Network Status submenu to display the Network Status window. The window displays the access network of each Ethernet interface and its information.

Network Status					
Category	Usage	Protocol	IP	Netmask	Gateway
Ethernet0	EXTERNAL	STATIC	192.168.17.100	255.255.0.0	192.168.0.1
Ethernet1					
Ethernet2	INT_PRIV	STATIC	10.0.0.1	255.255.255.0	
Serial0					
Serial1					

Name Server	
Server 1	168.126.63.1
Server 2	168.126.63.2

Domain

NLB

Select the **[Network]** menu of GWIM to display NLB submenu on the top left of the screen.

The OfficeServ 7400 system supports the Multi-WAN function to access external lines up to five. The system can distribute the Internet access traffic to each external interfaces by using this function. For the effective access traffic balancing, the system uses the 'Weighted Round Robin' method considering the throughout that may vary depending on the types of external lines. The NLB menu is used for the setup of the network load balancing function.

Configuration

Select **[Network]** → **[NLB]** → **[Configuration]** to set the network load balancing function, then the following configuration window will appear. The details by items are as follows:

Network Load Balance Configuration

Category	Settings
NLB Weight	eth0 <input style="width: 100px;" type="text" value="1"/>
NAT Status	Enable

Static Configuration

Source	Destination	Traffic Distribution
<input type="button" value="Add"/> <input type="button" value="Delete"/>		
<input type="button" value="OK"/> <input type="button" value="Cancel"/>		

Network Load Balance Configuration

The Network Load Balance Configuration is valid when at least two network interfaces are specified as the external network interface. For example, if T1 private line and ADSL line are connected to Ethernet 0 Interface(eth 0) and Ethernet 1 Interface(eth 1) selectively, the higher weighted value is given to the eth 1 with ADSL line that the bandwidth is relatively big and the lower weighted value is given to the eth 0. In this way, the load balancing according to the performance of the external network line is performed. The system has the Failover function that a different internal network interface line automatically backs up when any failure occurs in some of multiple external interfaces.

The details by fields are as follows:

NLB Weight: Relatively higher load is distributed in the line of the external interface side that higher numerical value is assigned. The weighted value for each external interface should be the greatest common divisor(minimum irreducible unit).

Static Configuration

The Static Configuration window is used to pass a line in the specific external network interface side by separately specifying the traffic session to satisfy a specific condition different from Network Load Balance Configuration. In this window, entries can be added or deleted by clicking the **[Add]** or the **[Delete]** button in the bottom of the window. 0.0.0.0 of the IP address field and all '0s' of the port field indicates all IP addresses all port numbers, respectively.

Static Configuration

	Source	Destination	Traffic Distribution
IP	0 . 0 . 0 . 0	0 . 0 . 0 . 0	Protocol tcp
<input checked="" type="radio"/> Mask	0 . 0 . 0 . 0	0 . 0 . 0 . 0	Gateway eth0-192.168.1.1
port	0 0	0 0	Backup default gate

- Source: Source IP address, netmask and port number of transfer session
- Destination: Destination IP address, netmask and port number of transfer session
- Traffic distribution: Interface and protocol that transfer session passes through
 - Protocol: Protocol to be applied
 - Gateway: External network interface that the corresponding traffic session passes through(if the default gateway is selected, the load balancing by Network Load Balance Configuration is applied.)
 - Backup: Backup interface to perform the failover function when any failure occurs in the external network interface line selected in the Gateway field.(For the application of load balancing, select default gateway.)

The input of 0.0.0.0 in the IP address and netmask input field represents that any IP addresses are allowed as the source and the destination IP addresses. In addition, all '0s' of the source port number means that any port number is allowed as the source port number.

Network Load balance Management

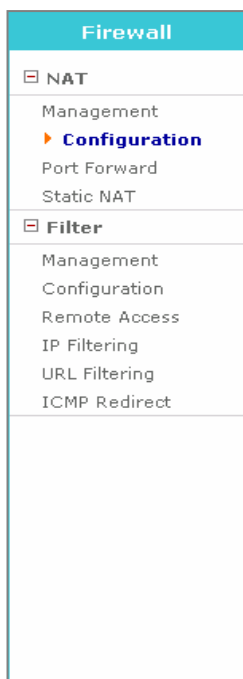
The Network Load Balance Management window is used for the execution and the stop of the NLB function. Click this menu to display the following configuration window. The details by fields are as follows:

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

- Activity: Current activity
- Action: Click the **[Run]** button to execute the NLB function in Stop mode or to stop in Running mode. If the OfficeServ 7400 system is restarted in the running mode, the NLB function is automatically executed.

Firewall Menu

Select the **[Firewall]** menu of GWIM to display the Firewall submenu on the top left of the screen.



Menu	Submenu	Description
NAT	Management	To select the use of NAT function
	Configuration	To set the private IP sharing function
	Port Forward	To set the port forwarding function
	Static NAT	To set the static forwarding function
Filter	Management	To select the Filter function
	Configuration	To set the Filtering policy
	Remote Access	To permit or block the remote access to the system
	IP Filtering	To block a specific IP access
	URL Filtering	To block the web access to the specified site
	ICMP Redirect	To block ICMP Replay of the system

NAT

The Network Address Translation(NAT) menu is used for the construction of a network by using private IPs.

Management

The use of NAT is set.

NAT Enable/Disable

Setting	
<input checked="" type="radio"/> Enable	<input type="radio"/> Disable

Setting	Description
Enable	To enable the NAT function
Disable	To disable the NAT function

Configuration

The user can configure a network configured with private IPs. A private IP can be transferred to the Internet through an authenticated IP.

Basic Mode

This table configures a network by using the minimum value of the options required for the configuration of a private network.

<input type="radio"/> Config Mode	<input checked="" type="radio"/> Basic Mode	<input type="radio"/> Advanced Mode
-----------------------------------	---	-------------------------------------

Private Network Configuration

Category	Configuration	
WAN IP	<input style="width: 20px; height: 20px; border: 1px solid #ccc;" type="text"/> <input style="width: 20px; height: 20px; border: 1px solid #ccc;" type="text"/> <input style="width: 20px; height: 20px; border: 1px solid #ccc;" type="text"/> <input style="width: 20px; height: 20px; border: 1px solid #ccc;" type="text"/>	<input type="checkbox"/> Dynamic IP <input style="width: 40px; height: 20px; border: 1px solid #ccc;" type="text"/>
Inside	<input style="width: 20px; height: 20px; border: 1px solid #ccc;" type="text"/> <input style="width: 20px; height: 20px; border: 1px solid #ccc;" type="text"/> <input style="width: 20px; height: 20px; border: 1px solid #ccc;" type="text"/> <input style="width: 20px; height: 20px; border: 1px solid #ccc;" type="text"/> / <input style="width: 20px; height: 20px; border: 1px solid #ccc;" type="text"/>	
Outside	<input style="width: 20px; height: 20px; border: 1px solid #ccc;" type="text"/> <input style="width: 20px; height: 20px; border: 1px solid #ccc;" type="text"/> <input style="width: 20px; height: 20px; border: 1px solid #ccc;" type="text"/> <input style="width: 20px; height: 20px; border: 1px solid #ccc;" type="text"/> / <input style="width: 20px; height: 20px; border: 1px solid #ccc;" type="text"/>	
Insert	<input style="width: 40px; height: 20px; border: 1px solid #ccc;" type="text"/>	

Category	Description
WAN IP	To set a general IP. Set up the connected port after selecting a dynamic IP for ADSL or Cable modem.
Inside	To enter a network address to configure a private network or select the range of netmask.(/: netmask, -: range, *; all)
Outside	To enter the network address connected to WAN or select the range of netmask.(/: netmask, -: range, *; all)
Insert	To select the location to insert the entered rule.

Advanced Mode

This table allows the user to select and set up a port or protocol that is not included to the basic configuration additionally.

Config Mode	<input type="radio"/> Basic Mode	<input checked="" type="radio"/> Advanced Mode
-------------	----------------------------------	--

Private Network Configuration

Category	Configuration
WAN IP:Port	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> : <input type="text"/> <input type="checkbox"/> Dynamic IP <input type="text"/> Port1 <input type="text"/>
Inside	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> / <input type="text"/>
Outside	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> / <input type="text"/>
Port	<input checked="" type="radio"/> Define <input type="text"/> all <input type="text"/> <input type="radio"/> User <input type="text"/> <input type="radio"/> Range <input type="text"/> ~ <input type="text"/> <input type="radio"/> Multi <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>
Protocol	<input type="text"/> all <input type="text"/>
Insert	<input type="text"/> 1 <input type="text"/>

Category	Description
Port	For only some specific ports, It is allowed to set up for the outside.
Protocol	Select TCP and UDP protocols. Both TCP and UDP are set up for 'All'.

The user can view the current status of configuration on Configuration List.

Configuration List

<input type="checkbox"/>	Setting
No Entry	

Port Forward

This table allows connecting to PC, which has a private IP inside the system, from outside environment.

Basic Mode: The basic mode is set up by using the minimum value of the options for port forwarding.

Basic Mode
 Advanced Mode

Private Network Port Forward

Category	Configuration
Inside IP	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Outside	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> / <input type="text"/> <input type="button" value="v"/>
WAN IP	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> / <input type="text"/> <input type="button" value="v"/>
Insert	<input type="text" value="1"/> <input type="button" value="v"/>

Category	Description
Inside IP	To set the IP to be connected from the outside.
Outside	To enter the network address connected to WAN or select the range of netmask.(/: netmask, -: range, *; all)
WAN IP	To set an authenticated IP.(/: netmask, -: range, *; all)
Insert	To select the location to insert the entered rule.

Advanced Mode: The user can select and set up ports or protocols that are not included in the basic configuration additionally.

Config Mode	<input type="radio"/> Basic Mode	<input checked="" type="radio"/> Advanced Mode
-------------	----------------------------------	--

Private Network Port Forward

Category	Configuration
Inside IP:Port	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> : <input type="text"/>
Outside	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> / <input type="text"/>
WAN IP	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> / <input type="text"/>
Port	<input checked="" type="radio"/> Define <input type="text"/> all <input type="text"/> <input type="radio"/> User <input type="text"/> <input type="radio"/> Range <input type="text"/> ~ <input type="text"/> <input type="radio"/> Multi <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>
Protocol	<input type="text"/> all <input type="text"/>
Insert	<input type="text"/> 1 <input type="text"/>

Category	Description
Port	It is available to set up as only some specific ports is allowed to transfer to the outside.
Protocol	Select a TCP and UDP protocol. For 'All', both TCP and UDP should be set up.

Configuration List displays the current setup status.

Configuration List	
<input type="checkbox"/>	Setting
	No Entry

Static NAT

This window allows the user to connect the PC, which has a private IP of the internal system, to the outside. The user can designate the port range and the port is mapped by 1:1.

Static NAT

Category	Configuration
Inside IP:Port	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> : <input type="text"/> ~ <input type="text"/>
WAN IP:Port	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> : <input type="text"/> ~ <input type="text"/>
Protocol	<input type="text" value="all"/> ▾
Insert	<input type="text" value="1"/> ▾

Configuration List

	Setting
<input type="checkbox"/>	No Entry

Category	Description
Inside IP: Port	To set an IP connected to the outside and a port.
WAN IP: Port	To set a port to be connected to the configured WAN IP.
Protocol	To select a protocol.
Insert	To select a location to insert the entered rule.

Filter

The user can set up the filtering for the traffic forwarded through the system.

Management

This table allows the user to set up whether to use the filter function.

Filter Enable/Disable

Setting	
<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
<input type="button" value="OK"/>	

Setting	Description
Enable	To enable the Filter function
Disable	To disable the Filter function

Configuration

The user can set up the filtering policy for the packets passing the system.

Basic Mode

Enter the minimum options required for packet filtering.

Config Mode	<input checked="" type="radio"/> Basic Mode	<input type="radio"/> Advanced Mode
-------------	---	-------------------------------------

Filter Configuration

Category	Configuration
Source IP	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> / <input type="text"/> <input type="text"/>
Destination IP	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> / <input type="text"/> <input type="text"/>
Target	<input type="text" value="Allow"/> <input type="button" value="OK"/>

Category	Description
Source IP	To set the origination IP.
Destination IP	To set the destination IP.
Target	To select Allow or Deny.

Advanced Mode

This window allows the user to use additional options for packet filtering.

Config Mode Basic Mode Advanced Mode

Filter Configuration

Category	Configuration
Source IP	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> / <input type="text"/>
Destination IP	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> / <input type="text"/>
Port	<input checked="" type="radio"/> Define <input type="text"/> all <input type="text"/> <input type="radio"/> User <input type="text"/> <input type="radio"/> Range <input type="text"/> ~ <input type="text"/> <input type="radio"/> Multi <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>
Protocol	<input type="text"/> all <input type="text"/>
Time Set	Days: <input checked="" type="checkbox"/> Everyday <input checked="" type="checkbox"/> Sun <input checked="" type="checkbox"/> Mon <input checked="" type="checkbox"/> Tue <input checked="" type="checkbox"/> Wed <input checked="" type="checkbox"/> Thu <input checked="" type="checkbox"/> Fri <input checked="" type="checkbox"/> Sat Time: <input checked="" type="radio"/> 24 Hours <input type="radio"/> 0 <input type="text"/> : 0 <input type="text"/> ~ 0 <input type="text"/> : 0 <input type="text"/>
Target	<input type="text"/> Allow <input type="text"/>
Insert	<input type="text"/> 1 <input type="text"/>

Category	Description
Source IP	To set the origination IP.
Destination IP	To set the destination IP.
Port	To set the port.
Protocol	To set the protocol.
Time Set	To set the time to apply the filtering rule.
Insert	To select a location to insert the entered rule.

This table displays the current setup status.

Configuration List

	Setting
<input type="checkbox"/>	No Entry

Remote Access

The user can allow or deny that the system connects to the outside.

Remote Access

Default Policy

Allow Deny

Administration IP . . .

OK

Remote Access

Default Policy

Allow Deny

OK

Remote IP Configuration

Category	Configuration
Source IP	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> / <input type="text"/>
Port	<input checked="" type="radio"/> Define <input type="text"/> all <input type="text"/> <input type="radio"/> User <input type="text"/> <input type="radio"/> Range <input type="text"/> ~ <input type="text"/> <input type="radio"/> Multi <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>
Protocol	<input type="text"/> all <input type="text"/>
Time Set	Days: <input checked="" type="checkbox"/> Everyday <input checked="" type="checkbox"/> Sun <input checked="" type="checkbox"/> Mon <input checked="" type="checkbox"/> Tue <input checked="" type="checkbox"/> Wed <input checked="" type="checkbox"/> Thu <input checked="" type="checkbox"/> Fri <input checked="" type="checkbox"/> Sat Time: <input checked="" type="radio"/> 24 Hours <input type="radio"/> 0 <input type="text"/> : 0 <input type="text"/> ~ 0 <input type="text"/> : 0 <input type="text"/>
Target	<input type="text"/> Allow <input type="text"/>
Insert	<input type="text"/> 1 <input type="text"/>

OK

Default Policy

- Allow: The basic policy is 'Allow' and the user can set up the policy by using 'Target'.
- Deny: Blocks all accesses from the outside except the PC that is set up as the manager IP.
- Administration IP: Enter the manager IP. Pay attention on entering the IP because all accesses may be denied.

IP Filtering

This window allows the user to deny the packet IPs of PCs connected to the system.

IP Filtering

Category	Configuration
Source IP	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> / <input type="text"/>
Destination IP	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> / <input type="text"/>
Port	<input checked="" type="radio"/> Define <input type="text"/> all <input type="text"/> <input type="radio"/> User <input type="text"/> <input type="radio"/> Range <input type="text"/> ~ <input type="text"/> <input type="radio"/> Multi <input type="text"/> , <input type="text"/> , <input type="text"/> , <input type="text"/>
Protocol	<input type="text"/> all
Time Set	Days: <input checked="" type="checkbox"/> Everyday <input checked="" type="checkbox"/> Sun <input checked="" type="checkbox"/> Mon <input checked="" type="checkbox"/> Tue <input checked="" type="checkbox"/> Wed <input checked="" type="checkbox"/> Thu <input checked="" type="checkbox"/> Fri <input checked="" type="checkbox"/> Sat Time: <input checked="" type="radio"/> 24 Hours <input type="radio"/> <input type="text"/> : <input type="text"/> : <input type="text"/> ~ <input type="text"/> : <input type="text"/> : <input type="text"/>
Insert	<input type="text"/> 1

OK

Configuration List

Setting
No Entry

Delete

URL Filtering

The user can deny the web access of PCs connected to the system.

URL Filtering

Category	IP
Source IP	<input type="text" value="."/> <input type="text" value="."/> <input type="text" value="."/> <input type="text" value="."/> / <input type="text" value=""/>
Key Word	<input type="text"/>
Time Set	Days: <input checked="" type="checkbox"/> Everyday <input checked="" type="checkbox"/> Sun <input checked="" type="checkbox"/> Mon <input checked="" type="checkbox"/> Tue <input checked="" type="checkbox"/> Wed <input checked="" type="checkbox"/> Thu <input checked="" type="checkbox"/> Fri <input checked="" type="checkbox"/> Sat Time: <input checked="" type="radio"/> 24 Hours <input type="radio"/> <input type="text" value="0"/> : <input type="text" value="0"/> ~ <input type="text" value="0"/> : <input type="text" value="0"/>

Configuration List

Setting
No Entry

Category	Description
Source IP	To set the origination IP.
Keyword	To enter the keyword of the site to deny.
Time Set	To set the time to apply the filtering rule.

ICMP Redirect

The user can deny the INTERNET CONTROL MESSAGE PROTOCOL (ICMP) Replay packet. Select the target interface and enable the interface to apply to this table.

ICMP Redirect

Interface	Setting	
Ethernet0	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
Ethernet1	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
Ethernet2	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable

Router

Select the [**Router**] menu of GWIM. Then, the submenus of IPMC are displayed in the upper left side of the window as follows:

Router	
[-] General	
▶ Routes	Management
[-] Configuration	
	Static
	RIP
	RIP Interface
	OSPF
	OSPF Interface
	BGP
[-] List	
	Access List
	Prefix List
	Route Map
	As Path List
	Community List
	Key Chain
[-] Status	
	RIP
	OSPF
	BGP

Menu	Submenu	Description
General	Routes	Displays the routing table of GWIM.
	Management	Starts or stops RIP, OSPF, and BGP.
Configuration	Static	Sets a static route.
	RIP	Sets RIP.
	RIP Interface	Sets RIP interface.
	OSPF	Sets OSPF protocol.
	OSPF Interface	Sets OSPF interface.
	BGP	Sets BGP.

(Continued)

Menu	Submenu	Description
List	Access List	Sets Access-list.
	Prefix List	Sets Prefix-list.
	Route Map	Sets Route-map.
	As Path List	Sets BGP AS-path list.
	Community List	Sets BGP Community-list.
	Key Chain	Sets the key used for authentication of RIP v2.
Status	RIP	Displays RIP network information.
	OSPF	Displays OSPF neighbor information.
	BGP	Displays the Neighbor status connected with the BGP network information.

General

This menu is used to start/stop RIP, OSPF, and BGP services or to retrieve the routing table of GWIM.

Routes

Select **[General]** → **[Routes]** to retrieve the routing table of GWIM.

Routes		
Type	Network	Entry
S *>	0.0.0.0/0	[1/0] via 192.168.0.1, eth0
C *>	10.10.0.0/16	is directly connected, eth2
C *>	127.0.0.0/8	is directly connected, lo
S	192.168.0.0/16	[1/0] via 192.168.0.1, eth0
C *>	192.168.0.0/16	is directly connected, eth0

Item	Description
Type	<ul style="list-style-type: none"> - C: Network directly connected to GWIM network interface - S: Static network set by a user - R: Path information received from another router via RIP - O: Path information received from another router via OSPF protocol - B: Path information received from another router via BGP * >: Whether to have activated routing table
Network	Network/Netmask information of route
Entry	Route information

Management

Select **[General]** → **[Management]** to start/stop RIP, OSPF, and BGP services.

Management		
Protocol	Current Status	Action
RIP	Start	<input type="button" value="On"/> ▾
OSPF	Start	<input type="button" value="On"/> ▾
BGP	Start	<input type="button" value="On"/> ▾

Configuration

This menu is used to set static route, RIP, OSPF protocol, and BGP.

Static Route

Select **[Configuration]** → **[Static]** and set a static route. After setting the target item, click the **[Save]** button.

Enter the Static Route command.

Static

Command

When the entered command is successfully executed, the configuration is directly applied to <Current Status> of **[Router]** → **[Configuration]** → **[Static]**. For example, when entering the static route command, the <Current Status> window is displayed as follows:

Current Status

Type	Network	Entry
S *>	0.0.0.0/0	[1/0] via 192.168.0.1, eth0
S *>	100.0.0.0/24	[1/0] via 192.168.0.1, eth0
S	192.168.0.0/16	[1/0] via 192.168.0.1, eth0

Help

Select the argument corresponding to the 'ip route' or 'no ip route' command. Click **[Argument]** to display all arguments corresponding to the command. Select an argument from them.

Help

Command	Argument
ip route	A.B.C.D A.B.C.D (A.B.C.D INTERFACE)

Current Status

Displays the static table from the routing tables of GWIM.

Displayed information is identical with the window description of **[Router]** → **[General]** → **[Routes]**.

Item	Description
Type	- S: Static network ser by a user - **: Whether to include activated routing table
Network	Network/Netmask information of route
Entry	Route information

RIP

Select **[Configuration]** → **[RIP]** and set RIP.

Enter the RIP command. If the entered command is successfully executed, the execution result is directly applied to <Current Status> of **[Router]** → **[Configuration]** → **[RIP]**.

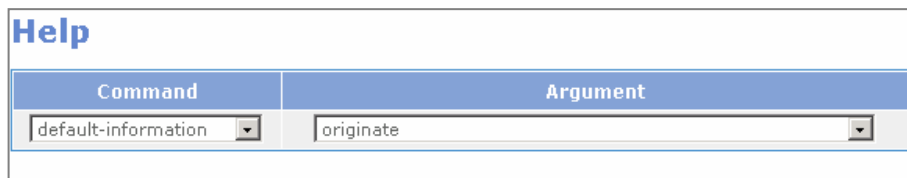


The screenshot shows a dialog box titled "RIP". It features a blue header bar with the text "Command". Below the header is a text input field. At the bottom center of the dialog is an "OK" button.

Help

Select the argument corresponding to the RIP command.

Clicking the **[Argument]** item displays all arguments corresponding to the command. Select an argument from them.



The screenshot shows a dialog box titled "Help". It has a blue header bar with two columns: "Command" and "Argument". Below the header, there are two dropdown menus. The "Command" dropdown is set to "default-information" and the "Argument" dropdown is set to "originate".

RIP Basic

After selecting each item, click the [OK] button. Then, the applied value is displayed in the <Current Status> window.

RIP Basic	
Command	Argument
Version	<input type="radio"/> 1 <input checked="" type="radio"/> 2 (default)
redistribute	<input type="checkbox"/> connected <input type="checkbox"/> static <input type="checkbox"/> ospf <input type="checkbox"/> bgp
network	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> / <input type="text"/>

[OK]

Displays the command configuration currently entered.

Current Status	
Router RIP	
No Entry	

[Save] [Delete]

RIP Interface

Select [Configuration] → [RIP Interface] and set RIP.

Select the target interface and enter the protocol configuration command directly.

RIP Interface	
Interface	Command
<input type="text" value="eth0"/>	<input type="text"/>

[OK]

If the entered command is successfully executed, the execution result is directly applied to <Current Status> of [Router] → [Configuration] → [RIP Interface].

Help

Select the argument corresponding to the RIP interface.

Clicking the [**Argument**] item displays all arguments corresponding to the command. Select an argument from them.

Command	Argument
ip rip	authentication key-chain LINE

RIP Interface Basic

After selecting each item, click the [**OK**] button. Then, the applied value is displayed in the <**Current Status**> window.

Command	Argument	
receive version	<input type="checkbox"/> 1	<input type="checkbox"/> 2
send version	<input type="checkbox"/> 1	<input type="checkbox"/> 2

OK

Displays the command configuration currently entered.

Router RIP Interface eth0
No Entry

Save

OSPF

Select [**Configuration**] → [**OSPF**] and set OSPF protocol.

Select the target interface and enter the protocol configuration command directly.



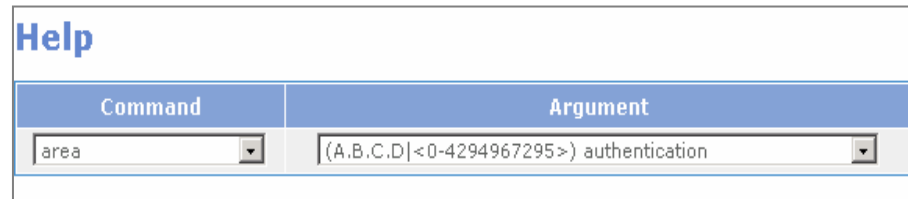
The dialog box is titled "OSPF" in blue. It features a blue header bar with the word "Command" in white. Below the header is a white text input field. At the bottom center of the dialog is a blue "OK" button.

If the entered command is successfully executed, the execution result is directly applied to <Current Status> of [**Router**] → [**Configuration**] → [**OSPF**].

Help

Select the argument corresponding to the OSPF command.

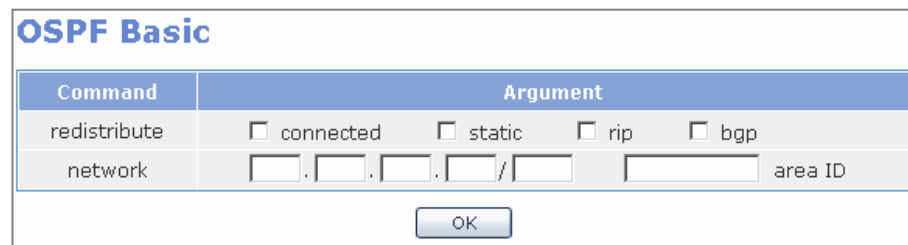
Clicking the [**Argument**] item displays all arguments corresponding to the command. Select an argument from them.



The dialog box is titled "Help" in blue. It has a blue header bar with "Command" and "Argument" in white. Below the header, there are two dropdown menus. The first dropdown menu is labeled "area" and the second is labeled "(A.B.C.D|<0-4294967295>) authentication".

OSPF Basic

After selecting each item, click the [**OK**] button. Then, the applied value is displayed in the <Current Status> window.



The dialog box is titled "OSPF Basic" in blue. It has a blue header bar with "Command" and "Argument" in white. Below the header, there are two rows of options. The first row is for the "redistribute" command, with four checkboxes: "connected", "static", "rip", and "bgp". The second row is for the "network" command, with four input boxes for IP address, a slash, and an input box for "area ID". At the bottom center is a blue "OK" button.

Displays the command configuration currently entered.

Current Status

Router OSPF
No Entry

Save Delete

OSPF Interface

Select [**Configuration**] → [**OSPF Interface**] to set OSPF protocol.

Select the target interface and enter the protocol configuration command directly.

If the entered command is successfully executed, the execution result is directly applied to <**Current Status**> of [**Router**] → [**Configuration**] → [**OSPF Interface**].

OSPF Interface

Interface	Command
eth0	

OK

Help

Select the argument corresponding to the OSPF interface.

Clicking the [**Argument**] item displays all arguments corresponding to the command. Select an argument from them.

Help

Command	Argument
ip ospf	A.B.C.D authentication (null message-digest)

OSPF Interface Basic

After selecting each item, click the [OK] button. Then, the applied value is displayed in the <Current Status> window.

OSPF Interface Basic	
Command	Argument
cost	<input type="text"/> <1-65535> Cost
dead-interval	<input type="text"/> <1-65535> Seconds
hello-interval	<input type="text"/> <1-65535> Seconds
transmit-delay	<input type="text"/> <1-65535> Seconds
retransmit-interval	<input type="text"/> <1-65535> Seconds

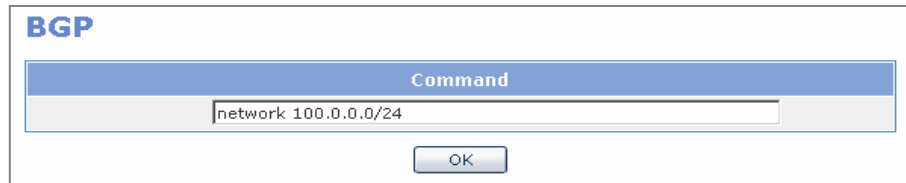
Display the command configuration currently entered.

Current Status	
Router OSPF Interface eth0	
No Entry	

BGP

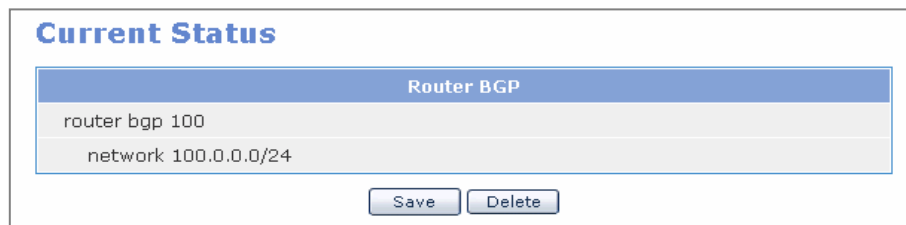
Select [**Configuration**] → [**BGP**] and set BGP. After setting the target item and click the [**Save**] button.

Enter the BGP configuration command directly.



The screenshot shows a dialog box titled "BGP". It has a header bar with the word "Command" in the center. Below the header is a text input field containing the command "network 100.0.0.0/24". At the bottom center of the dialog is an "OK" button.

If the entered command is successfully executed, the execution result is directly applied to <Current Status> of [**Router**] → [**Configuration**] → [**BGP**]. For example, when the BGP command is entered, the <Current Status> window is displayed as follows:

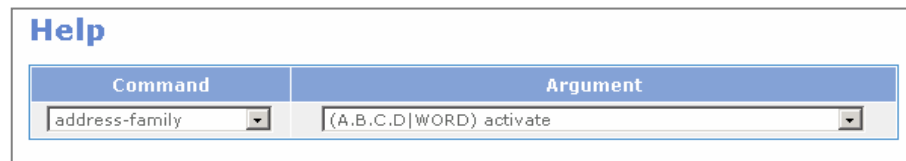


The screenshot shows a window titled "Current Status". It has a header bar with "Router BGP" in the center. Below the header, there are two lines of text: "router bgp 100" and "network 100.0.0.0/24". At the bottom of the window are two buttons: "Save" and "Delete".

Help

Select the argument corresponding to the BGP command.

Clicking the [**Argument**] item displays all arguments corresponding to the command. Select an argument from them.



The screenshot shows a dialog box titled "Help". It has two columns: "Command" and "Argument". Under "Command", there is a dropdown menu with "address-family" selected. Under "Argument", there is a dropdown menu with "(A.B.C.D|WORD) activate" selected.

BGP Basic

After entering each item and clicking the [OK] button, the configuration values are displayed in the <Current Status> window.

BGP Basic

option	parameter
AS number	<input style="width: 50px;" type="text"/>
neighbor	<input style="width: 20px;" type="text"/> . <input style="width: 20px;" type="text"/> . <input style="width: 20px;" type="text"/> . <input style="width: 20px;" type="text"/> remote <input style="width: 50px;" type="text"/> <input type="checkbox"/> ebgp-multihop <input type="checkbox"/> next-hop-self
network	<input style="width: 20px;" type="text"/> . <input style="width: 20px;" type="text"/> . <input style="width: 20px;" type="text"/> . <input style="width: 20px;" type="text"/> / <input style="width: 20px;" type="text"/>
redistribute	<input type="checkbox"/> connected <input type="checkbox"/> static <input type="checkbox"/> rip <input type="checkbox"/> ospf

Current Status

Display the configuration information related with BGP of GWIM. Click the [Save] button to save the current configuration information in the system. Click the [Delete] button to delete all configuration information.

Current Status

Router BGP

```
router bgp 100
network 100.0.0.0/24
```

List

Access List

Select **[List]** → **[Access List]** and set Access-list. After setting the target item, click the **[Save]** button.

Access List

Option	Parameter
ID	Word <input type="text" value="test"/>
Action	<input checked="" type="radio"/> Permit <input type="radio"/> Deny
Source Match	<input type="radio"/> any
	<input checked="" type="radio"/> Network <input type="text" value="100"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> / <input type="text" value="24"/>
Exact match	<input checked="" type="checkbox"/> Exact match

Item	Description
ID	Sets the Access-list name.
Action	Allows/Rejects the packet matched.
Source Match	Sets the match condition. Any - All packets Host - A host Network - Network range
Destination Match	If ID ranges from 100 to 199 or from 2000 to 2699, Destination Match can be set as well as the Source Match condition Any - All packets Host - A host Network - Network range
Exac-match	Available when ID is set to word and when match condition is set to Network. Sets only the packets matched correctly with the prefix.

If the entered command is successfully executed, the execution result is directly applied to <Current Status> of [Router] → [List] → [Access List]. For example, when Access-list is entered, the <Current Status> window is displayed as follows. The Access list being set in GWIM can be retrieved.

Current Status

	ID	Entry
<input checked="" type="radio"/>	test	permit 100.0.0.0/24 exact-match

Click the [Save] button to save the current configuration information in the system. Click the [Delete] button to delete the corresponding access-list.

Item	Description
ID	Access-list name information
Entry	Access-list description

Prefix List

Select [List] → [Prefix List] and set Prefix-list. After setting the target item, click the [Save] button.

Prefix List

Option	Parameter
ID	<input type="text" value="test"/>
Seq	<input type="text" value="5"/>
Action	<input checked="" type="radio"/> Permit <input type="radio"/> Deny
Prefix Match	<input type="radio"/> any <input checked="" type="radio"/> <input type="text" value="100"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> / <input type="text" value="24"/> <input type="text"/> ~ <input type="text"/>

Item	Description
ID	Sets the prefix-list name.
Seq	Sets the sequence No. of the prefix-list.
Action	Allows/Rejects the packets matched.

(Continued)

Item	Description
Prefix Match	Sets the match condition. Any - All packets Network - network range. Minimum and maximum prefix length can be set.

If the entered command is successfully executed, the execution result is directly applied to <Current Status> of [Router] → [List] → [Prefix List]. For example, when a prefix is entered, the <Current Status> window is displayed as follows:

Current Status

	ID	Entry
⦿	test	seq 5 permit 100.0.0.0/24

Click the [Save] button to save the current configuration information in the system. Click the [Delete] button to delete the entry of the selected prefix list. Click the [Delete All] button to delete all entries of the prefix list.

Prefix-list information being set in GWIM can be displayed.

Current Status

	ID	Entry
⦿	test	seq 5 permit 100.0.0.0/24

Item	Description
ID	Prefix-list name information
Entry	Prefix-list information

Route-Map

Select [List] → [Route-Map] and set the route-map of GWIM. Enter the target value and click the [Save] button.

Route-Map

Option	Parameter
Name	<input style="width: 80%;" type="text" value="test"/>
Action	<input checked="" type="radio"/> Permit <input type="radio"/> Deny
Sequence	<input style="width: 80%;" type="text" value="1"/>

Item	Description
Name	Route-map name
Action	Sets whether to apply set operation.
Sequence	Sets the sequence No. to additionally delete a route-map

If the entered command is successfully executed, the execution result is directly applied to <Current Status> of [Router] → [List] → [Route-Map].
For example, when a route-map is entered, the <Current Status> window is displayed as follows:

Route-Map Setting

	Name	Entry
<input checked="" type="radio"/>	test	permit 1

This menu is used to view the information on the route-map set in GWIM.

Item	Description
Name	Route-map name
Entry	Route-map information

Click the **[Save]** button to save the current configuration information in the system. Click the **[Delete]** button to delete the target route-map. Click the **[Edit]** button to display the window as follows. Through this window, the target Set/Match operation of the route-map can be set.

Match

Option	Parameter
<input type="checkbox"/> IP	<input checked="" type="radio"/> Address <input style="width: 100px;" type="text"/> <input type="checkbox"/> Use prefix-list
	<input type="radio"/> Nexthop <input style="width: 100px;" type="text"/> <input type="checkbox"/> Use prefix-list
<input type="checkbox"/> Metric	<input style="width: 100px;" type="text"/>

Set

Option	Parameter
<input type="checkbox"/> IP	Nexthop <input style="width: 20px;" type="text"/> . <input style="width: 20px;" type="text"/> . <input style="width: 20px;" type="text"/> . <input style="width: 20px;" type="text"/>
<input type="checkbox"/> Metric	<input style="width: 100px;" type="text"/>
<input type="checkbox"/> Weight	<input style="width: 100px;" type="text"/>
<input type="checkbox"/> Metric-Type	Type-1 <input type="button" value="v"/>
<input type="checkbox"/> Local Preference	<input style="width: 100px;" type="text"/>

The items of Match Operation is as follows:

Item	Description
IP	- Address - Sets access-list or prefix-list for an IP to be matched. - Nexthop - Sets the Nexthop IP to be matched.
Metric	Sets the Metric to be matched.

The items of Set Operation is as follows:

Item	Description
IP	Sets nexthop of the route table.
Metric	Sets metric of the route table.
Weight	Sets weight of the route table.

(Continued)

Item	Description
Metric-Type	Sets metric type of the route table. - Type 1: External Type 1 - Type 2: External Type 2
Local Preference	Sets local preference from BGP attribute.

When the match condition is met and Action is set to Permit, the job corresponding to Set operation is performed. If the command is successfully executed, the execution result is directly applied to <Current Status>.

Current Status

	Sequence	Entry
<input checked="" type="radio"/>	1	match ip address test
<input type="radio"/>	1	set ip next-hop 1.1.1.1

Item	Description
Sequence	Matches/Sets operation Sequence No. of route-map.
Entry	Matches/Sets operation information of route-map.

Click the [**Prev.**] button to return to the route-map window mentioned above. Click the [**Delete**] button to delete the selected Match/Set operation. Click the [**Save**] button to save the current configuration information in the system.

As Path List

Select **[List]** → **[As Path List]** and set AS Path access-list of GWIM BGP.
Enter the target value and click the **[Save]** button.

As Path

Option	Parameter
ID	<input style="width: 80%;" type="text" value="test"/>
Action	<input checked="" type="radio"/> Permit <input type="radio"/> Deny
Match	<input style="width: 80%;" type="text" value="100\$"/>

Item	Description
ID	Sets AS Path access-list name.
Action	Decides whether to allow/reject if the BGP route information exists that meets the match condition.
Match	Sets normally match condition.

If the entered command is successfully executed, the execution result is directly applied to **<Current Status>** of **[Router]** → **[List]** → **[As Path List]**.
For example, when as path access-list is entered, the **<Current Status>** window is as follows:

Current Status

	ID	Entry
<input checked="" type="radio"/>	test	permit 100\$

This menu is used to display the information on the as path access-list set in GWIM.

Current Status

	ID	Entry
<input checked="" type="radio"/>	test	permit 100\$

Item	Description
ID	As path access-list name
Entry	As path access-list information

Click the **[Save]** button to save the current configuration information in the system. Click the **[Delete]** button to delete the entry of the selected as path access-list. Click the **[Delete All]** button to delete all as path access-list entries of the corresponding name.

Community List

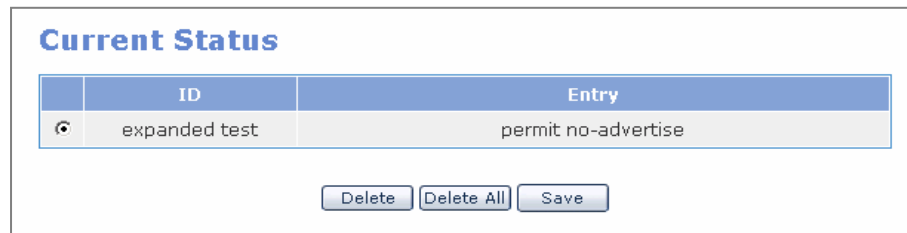
Select **[List]** → **[Community List]** and set Community List of GWIM BGP. Set the target value and click the **[Save]** button.

Community List

Option	Parameter
ID	<input type="text" value="test"/>
Action	<input checked="" type="radio"/> Expanded <input type="radio"/> Standard
Match	<input checked="" type="radio"/> Permit <input type="radio"/> Deny
	<input type="radio"/> <input type="text"/>
	<input checked="" type="radio"/> No-Advertise

Item	Description
ID	Sets Community list name Expanded - When normally community list is set Standard - When community list with selected format is set
Action	Sets whether to allow/reject the community to be matched
Match	No-Advertise - Do not distribute path to the neighbor router No-Export - Do not distribute path to an external neighbor router Local-AS - Do not distribute path to the neighbor router of the lower AS located at BGP combination network. In other cases, set normally to community list.

If the entered command is successfully executed, the execution result is directly applied to <Current Status> of [Router] → [List] → [Community List]. For example, when as path access-list is entered, the <Current Status> window is displayed as follows:



Item	Description
ID	Community list name
Entry	Community list information

Click the [Save] button to save the current configuration information in the system. Click the [Delete] button to delete the target community-list entry. Click the [Delete All] button to delete all community-list entries of the name.

Status

RIP

This menu is used to display the RIP connection status and information.

RIP Information						
	Network	Next Hop	Metric	From	If	Time
R	20.0.1.0/24	30.0.1.1	2	30.0.1.1	rd2	02:47
R	30.0.1.0/24		1		rd2	
R	192.168.0.0/16	30.0.1.1	2	30.0.1.1	rd2	02:47

Item	Description
Network	Displays network information
Next Hop	Next hop address of the RIP route that sends neighbor.
Metric	Metric information.
From	Displays the address being connected.
If	Displays interface information.
Time	Update time.

OSPF

This menu is used to check the OSPF connection status and information with the other party's router.

OSPF Information					
Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.17.101	1	Full/Backup	00:00:37	30.0.1.1	rd2

Item	Description
Neighbor ID	Neighbor ID of the other party's router
Pri	Priority
Status	Displays the connection process.
Dead Time	Displays the dead time.

(continued)

Item	Description
Address	Address of the other party
Interface	Interface connected

BGP

This menu is used to check the BGP connection status information and BGP routing table information.

BGP Information	
Category	Value
BGP Router ID	192.168.0.98
Local AS Number	100
BGP Table Version	1
BGP AS-PATH Entries	1
BGP Community Entries	0
Total Neighbor	1

Item	Description
BGP Router ID	Current system router-ID Sets to the IP address that is the highest in the IPs set in loopback when an address or a loopback that is the highest from the IP addresses is used.
Local AS Number	Local AS No. set by a user
BGP Table Version	BGP table change version information
BGP AS-PATH Entries	Number of AS PATH Hash tables used in BGP
BGP Community Entries	Number of Hash table of community attribute used in BGP
Total Neighbor	Total sum of BGP neighbor

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
192.168.0.1	4	100	0	0	0	0	0	never	Idle

Item	Description
Neighbor	IP address of the neighbor router
V	Version No. used by neighbor
AS	AS No. of neighbor
MsgRcvd	Message number received from neighbor
MsgSent	Message number sent from neighbor
TblVer	Latest BGP database version sent from neighbor
InQ	Number of messages that should be received from neighbor and processed
OutQ	Number of messages sent to neighbor
Up/Down	Displays the path time when BGP session is finished. Displays thee status when BGP session is not finished.
State/PfxRcd	Number of BGP routes via neighbor or peer group or BGP current status

Network	Nexthop	Metric	LocalPrf	Weight	Path
* > 100.0.0.0/24	0.0.0.0			32768	i

Item	Description
Network	Displays network information. Status code information s - Indicates the suppressed network. * - Indicates proper network information. h - BGP dampening is activated. > - best route i - Indicates the network entered by IBGP.
Nexthop	Nexthop address of the BGP route sent from neighbor
Metric	MED value of BGP neighbor
LocalPrf	Local Preference. Default is 100.

(Continued)

Item	Description
Weight	Weight allocated in prefix - Local route default is 32768. - The default of the sent route is 0.
Path	Displays the list of AS path that should be passed to go to the network corresponding to the prefix. Origin code information i - Information received by the network command e - Information received via EGP ? - Information received by redistribution

IPMC

Select the [IPMC] menu of GWIM. Then, the submenus of IPMC are displayed in the upper left side of the window as follows:

IPMC	
[-] General	
▶ Mroutes	Management
[-] Configuration	
	IGMP
	DVMRP
	DVMRP Intf
	PIM-SM
	PIM-SM Intf
[-] Status	
	IGMP Groups
	DVMRP
	PIM-SM

Menu	Submenu	Description
General	Mroutes	Displays Multicast Routing Entry.
	Management	Starts/Stops IPMC protocol demons.
Configuration	IGMP	Displays or changes IGMP configuration.
	DVMRP	Displays or changes DVMRP default configuration.
	DVMRP Intf	Displays or changes VIF of DVMRP.
	PIM-SM	Displays or changes PIM-SM default configuration.
	PIM-SM Intf	Displays or changes VIF PIM-SM.
Status	IGMP Groups	Displays IGMP Group information.
	DVMRP	Displays DVMRP neighbor and Prune information.
	PIM-SM	Displays PIM-SM Neighbor information.

General

Mroutes

This menu is used to display multicast routing entries being operated in this window.

Mroutes					
Mroute	Uptime	Expires	Flags	Incoming	Outgoing
(100.1.1.11, 224.1.1.100)	00:00:08	00:03:22	TF	rd2	rd3
I: Immediate Stat, T: Timed Stat, F: Forwarder installed					
<input type="button" value="Clear"/> <input type="button" value="Refresh"/>					

- Mroute: Multicast Routing identifier
- Uptime: Time passed after starting the operation of multicast routing entry
- Expires: Rest time until multicast routing entry is expired
- Flags: Multicast routing feature flag. Refer to the description on the lower side
- Incoming: Name of VIF to which multicast is sent
- Outgoing: List of VIF where multicast is sent

Management

This menu is used to execute or stop dvmrpd and pimd, IPMC protocol demons. <Current Status> of Management shows the current status of each demon. To change the demon status, select another status from [Action] and click the [OK] button.

Management		
Protocol	Current Status	Action
DVMRP	Stop	On
PIM	Stop	Off
<input type="button" value="OK"/>		

- Protocol: IPMC protocol
- Current Status: Current IPMC protocol demon status
- Action: New status of IPMC protocol demon status

Configuration

IGMP

This menu is used to display and change IGMP configuration.

IGMP & Help

IGMP command can be entered and executed. Command that can be executed can be retrieved in the following Help table. Enter the target command into the input field of IGMP and click the [OK] button. Then, the command is executed.

IGMP

Command
<input style="width: 90%; border: none; border-bottom: 1px solid gray;" type="text" value="clear ip igmp group"/>

Help

Command	Argument
<input style="width: 95%; border: none; border-bottom: 1px solid gray;" type="text" value="clear ip igmp"/>	<input style="width: 95%; border: none; border-bottom: 1px solid gray;" type="text" value="group"/>

IGMP Basic

Enter new information and click the [OK] button to change the default configuration of IGMP.

IGMP Basic

Command	Argument
Interface	<input checked="" type="radio"/> All <input type="radio"/> <input style="width: 80px; border: none; border-bottom: 1px solid gray;" type="text" value="eth0"/> (192.168.17.100/16)
IGMP Query Interval	<input style="width: 60px; border: none; border-bottom: 1px solid gray;" type="text" value="125"/> (1~65535, Default: 125)
Max Response Time	<input style="width: 60px; border: none; border-bottom: 1px solid gray;" type="text" value="10"/> (1~25, Default: 10)

- Interface: Select the target IGMP interface and select All. Then, all interface configuration values are applied.
- IGMP Query Interval: Cycle of sending IGMP Membership Query
- Max Response Time: Maximum time of waiting a response after sending Membership Query

IGMP Interface Information

This menu is used to display the configuration values of IGMP interfaces.

IGMP Interface Information				
Address	Intf	Querier Address	Query Interval	Max Resp Time
100.1.2.10/24	rd2	100.1.2.10/24	125	10
100.1.3.10/24	rd3	100.1.3.10/24	125	10

- Address: IGMP group address
- Intf: IGMP interface name
- Querier Address: IP address of IGMP interface that sends membership query. IP address of Designate Router(DR)
- Query Interval: Cycle of sending Membership Query
- Max Resp Time: Maximum time of waiting a response to Membership Query

Configuration / DVMRP

This menu is used to set DVMRP, an IPMC protocol. In addition, the Route items of DVMRP being operated can be displayed.

DVMRP & Help

Commands can be executed to set DVMRP. The commands that can be executed in Help can be searched. Enter a command into DVMRP and click the [OK] button to execute the command.

DVMRP

Command	
<input type="text" value="clear ip dvmrp route 240.0.0.0/4"/>	

Help

Command	Arguement
<input type="text" value="clear ip dvmrp"/>	<input type="text" value="route A.B.C.D/M"/>

DVMRP Routes

This menu is used to display DVMRP Route items being operated.

DVMRP Routes						
Source Network	Flags	Intf	Neighbor	Metric	Uptime	Expires
100.1.2.0/24	.D.	rd2	Directly Connected	1	00:05:10	00:00:00
100.1.3.0/24	.D.	rd3	Directly Connected	1	00:05:05	00:00:00

- Source Network: VIF network address to which multicast packets flow
- Flags: DVMRP route feature flag. N=New, D=Direct Connected, H=Holddown
- Intf: VIF name to which multicast packets flow
- Neighbor: DVMRP neighbor IP address that provides information on DVMRP route
- Metric: DVMRP route Metric(=distance) value
- Uptime: Time passed after using the DVMRP route item
- Expires: Left time until the DVMRP route item is expired

DVMRP Intf

This menu is used to add or set DVMRP VIF.

RD Interface

This menu is used to add L3 interface where an IP address is set to DVMRP VIF. Select the target interface to be added to VIF from the Interface item, enter the target value, and click the **[Add]** button.

RD Interface	
Command	Argument
Interface	<input type="text" value="eth0"/> (192.168.17.100/16)
Reject Non-pruners	<input type="checkbox"/> (do not allow old version DVMRP neighbors)
Metric	<input type="text" value="1"/> (1~31)

- Interface: Select the target L3 interface
- Reject Non-pruners: Non-pruners indicate the neighbors that only support DVMRP with the previous version. Mark if this is not communicated with the DVMRP with the previous version.
- Metric: Metric(=distance) value to be used for multicasting routing by VIF

DVMRP Interfaces

This menu is used to display the configuration DVMRP VIF. To delete a specific VIF, check the check box on the left and click the **[Delete]** button.

DVMRP Interfaces					
	Intf	Address	Type	Neighbor Count	Remote Address
<input type="checkbox"/>	rd2	100.1.2.10/24	BCAST	1	N/A
<input type="checkbox"/>	rd3	100.1.3.10/24	BCAST	0	N/A

- Intf: DVMRP VIF name
- Address: IP address of DVMRP VIF
- Type: DVMRP VIF type. Tunnel, Point-to-Point, Broadcast
- Neighbor Count: Number of neighbors connected to DVMRP VIF
- Remote Address: Address of the other party in case of Tunnel or Point-to-Point type.(Peer Address)

PIM-SM

This menu is used to set PIM-SM.

PIM-SM & Help

Command can be executed to set PIM-SM. Commands that can be executed can be retrieved in Help. Enter the target command into the input field of PIM-SM and click the [OK] button.

PIM-SM

Command
<input style="width: 95%; border: 1px solid gray;" type="text" value="clear ip pim sparse-mode bsr rp-set *"/>

Help

Command	Argument
<div style="border: 1px solid gray; padding: 2px;"> clear ip pim ▼ </div>	<div style="border: 1px solid gray; padding: 2px;"> sparse-mode bsr rp-set * ▼ </div>

PIM-SM Basic

This menu is used to set BSR and RP of PIM-SM protocol. Mark the check box on the right and enter the configuration values. Click the [OK] button to apply the values.

PIM-SM Basic

	Command	Argument
<input checked="" type="checkbox"/>	RP Address	<input style="width: 20px;" type="text" value="192"/> <input style="width: 20px;" type="text" value="."/> <input style="width: 20px;" type="text" value="168"/> <input style="width: 20px;" type="text" value="."/> <input style="width: 20px;" type="text" value="17"/> <input style="width: 20px;" type="text" value="."/> <input style="width: 20px;" type="text" value="100"/>
<input checked="" type="checkbox"/>	RP Candidate	<input style="width: 40px;" type="text" value="eth0"/> ▼ <input style="width: 20px;" type="text" value="24"/> Priority(0~255)
<input checked="" type="checkbox"/>	BSR Candidate	<input style="width: 40px;" type="text" value="eth0"/> ▼ <input style="width: 20px;" type="text" value="30"/> MaskLen(0~32) <input style="width: 20px;" type="text" value="100"/> Priority(0~255)

- RP Address: When setting static RP, enter the IP address of RP
- RP Candidate: When setting RP Candidate, select VIF and enter the target priority.(Small value has high priority.)
- BSR Candidate: When setting BSR Candidate, select VIF and enter the target Mask Length and Priority.(High value has high priority.)

BootStrap Information

This menu is used to display the information on BootStrap router. Click the **[Delete]** button to delete all BSR candidates.

BootStrap Information

BootStrap Information

PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
BSR address: 100.1.2.10
Uptime: 00:01:15, BSR Priority: 44, Hash mask length: 30
Expires: 00:00:55
Role: Candidate BSR
State: Pending BSR

Candidate RP: 100.1.2.10(rd2)
Advertisement interval 60 seconds
Next Cand_RP_advertisement in 00:00:47

RP Information

This menu is used to display the information on RP router. Click the **[Delete]** button to delete all RP configurations.

RP Information

RP Information

PIM Group-to-RP Mappings
Group(s): 224.0.0.0/4
RP: 100.1.2.10
Info source: 100.1.2.10, via bootstrap, priority 0
Uptime: 00:01:14, expires: 00:02:16
Group(s): 224.0.0.0/4, Static
RP: 100.1.2.1
Uptime: 00:04:05

PIM-SM Intf

This menu is used to set PIM-SM VIF.

RD Interface

This menu is used to add PIM-SM VIF. Select the target L3 interface from the Interface item, enter the target values, and click the **[Add]** button to add PIM-SM VIF.

RD Interface

Command	Argument
Interface	<input type="text" value="eth0"/> (192.168.17.100/16)
Mode	<input type="text" value="Sparse"/>
DR Priority	<input type="text" value="1"/> (0~4294967294)
Hello Interval	<input type="text" value="30"/> (1~65535)

- Interface: Select the target L3 interface to be added to PIM-SM VIF
- Mode: Select the target PIM-SM protocol mode. Sparse, Passive
- DR Priority: Enter the priority value used when selecting Designate Router (DR). (High value has high priority.)
- Hello Interval: Cycle of exchanging hello packets with connected PIM-SM neighbors

PIM-SM Interfaces

This menu is used to display the VIFs added to PIM-SM. To delete a VIF, click the check box on the left and click the **[Delete]** button.

PIM-SM Interfaces

	Intf	Address	Mode	Neighbor Count	DR Prio	DR	Hello Intv/Hold
<input type="checkbox"/>	rd2	100.1.2.10/24	Sparse	0	1	100.1.2.10	30/105
<input type="checkbox"/>	rd3	100.1.3.10/24	Sparse	0	1	100.1.3.10	30/105

IGMP Groups

This menu is used to display the information on registered IGMP group.

IGMP Group Information				
Group Address	Intf	Uptime	Expires	Last Reporter
224.1.1.100	rd3	00:00:03	00:04:17	100.1.3.31

- Group Address: IGMP group address
- Intf: IGMP interface name
- Uptime: Time passed after IGMP group is created
- Expires: Left time until the IGMP Group information is expired
- Last Reporter: Client IP address that sends the last membership report

Status

DVMRP

This menu is used to display the DVMRP protocol status.

DVMRP Neighbors

This menu is used to display the information on the DVMRP neighbor whose information is exchanged.

DVMRP Neighbors			
Neighbor Address	Interface	Uptime	Expires
100.1.2.1	rd2	00:02:04	00:00:31

- Neighbor Address: IP address of DVMRP Neighbor
- Interface: VMRP VIF name
- Uptime: Time passed after being connected
- Expires: Left time until the Neighbor connection information is expired

DVMRP Prune Information

This menu is used to display DVMRP Prune items.

DVMRP Prune Information						
Source Address	MaskLen	Group Address	State	FCR Cnt	Expires	ReXmit
100.1.1.0	24	224.1.1.100	0	01:59:06	Off

P: Pruned, H: Host, D: Holddown, N: NegMFC, I: Init

- Source Address: Host Ip address that sends multicast packets
- MaskLen: Mask length of DVMRP Prune
- Group Address: Multicast group address
- State: Flags that display the DVMRP Prune status. Refer to the description on the lower side

- FCR Cnt: DVMRP Forwarding Cache count
- Expires: Time passed after the DVMRP Prune information is created
- ReXmit: Left time until retransmission

PIM-SM

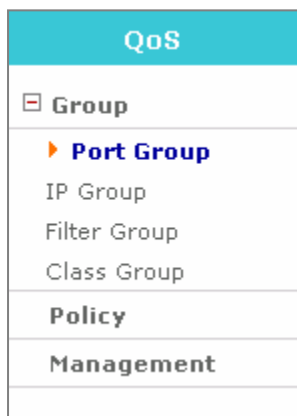
This menu is used to display the neighbor list of PIM-SM protocol.

PIM-SM Neighbors						
Neighbor	Intf	Uptime	Expires	Ver	DR Priority	DR
100.1.2.1	rd2	00:02:17	00:01:29	v2	1	.

- Neighbor: Neighbor IP address
- Intf: IP address of VIF connected with neighbor
- Uptime: Time passed after being connected with neighbor
- Expires: Left time until the Neighbor connection information is expired
- Ver: Version of the PIM-SM protocol used for the connection
- DR Priority: Designate Router(DR) priority of neighbor
- DR: Displays whether the neighbor is Designate Router(DR)

QoS

Select the [QoS] menu of GWIM to display the submenus of QoS on the upper left section of the window.



Menu	Submenu	Description
Group	Port Group	Retrieves, sets, edits, or deletes a port group
	IP Group	Retrieves, sets, edits, or deletes an IP group
	Filter Group	Retrieves, sets, edits, or deletes a filter group
	Class Group	Retrieves, sets, edits, or deletes a class group
Policy	-	Sets a class for a port
Management	-	Starts or stops the execution of a QoS and sets to execute when the system reboots.

Group

The **[Group]** menu is used to retrieve, set, edit, or delete a port group, an IP group, a filter group, or a class group.

Port Group

Select **[Port Group]** to retrieve, set, edit, or delete a port group.

Port Group List

	Name	Port
🔍	Port100	100

Click the **[Add]** button in the above window to display a window from which a port group can be set.

Port Group

Category	Configuration
ID	<input type="text" value="VoIP"/>
Port	<input type="checkbox"/> <input type="text" value="10000"/> ~ <input type="text" value="20000"/>

Enter the target ID and port No. and click the **[Save]** button.

Click the **[Add]** button to add a port, and click the **[Delete]** button after marking the checkbox to delete the target port.

Item	Description
ID	Name of the port group - Should include both letters and numbers. - Group ID shall start only with letters, not numbers. - No blanks should be left in between characters.
Port	- Port range - Enter '0' to set all ports

IP Group

Select **[IP Group]** to retrieve, set, edit, or delete an IP group.

IP Group List

	Name	IP
☉	IP0_100	10.0.0.100/32

Click the **[Add]** button in the above window to display a window from which an IP group can be set.

IP Group

Category	Configuration
ID	<input style="width: 90%;" type="text" value="Develope_Team"/>
IP	<input type="checkbox"/> <input style="width: 20px;" type="text" value="192"/> <input style="width: 20px;" type="text" value="168"/> <input style="width: 20px;" type="text" value="0"/> <input style="width: 20px;" type="text" value="0"/> <input style="width: 20px;" type="text" value=" /"/> <input style="width: 20px;" type="text" value=" 24"/>

Enter the target ID and port No. and click the **[Save]** button.

Click the **[Add]** button to add an IP, and click the **[Delete]** button to delete the target IP.

Item	Description
ID	Name of the IP group - Should include both letters and numbers. - Group ID shall start only with letters, not numbers. - No blanks should be left in between characters.
IP	IP address /: Used for entering subnet -: Used for entering the range of IPs Enter '0.0.0.0/0' to set all ports.

Filter Group

Select **[Filter Group]** to retrieve, set, edit, or delete a filter group.

Filter Group List						
	Name	Prio	Trans	Source IP / PORT	Destination IP / PORT	ToS
<input checked="" type="checkbox"/>	dev_voip	1	tcp	Develope_Team / any	any / VoIP	

If 'dev_voip' is registered as the filter group as shown above, the filtering rule is as follows:

- 'Source' and 'Destination' items are the information set in the **[Port Group]** and **[IP Group]** menus.
- All TCP packet traffics of which the internal IP is Develop_Team (192.168.0.0/24) and the connection port is VoIP(10000~20000) are filtered with a priority of '1'.
- The filter is then associated with the class group set at the **[QoS] → [Group] → [Class Group]** menu.

Click the **[Add]** button in the above window to display a window from which a filter group can be set. Set the items and select the target IP and port from the list and click the **[Save]** button.

Category	Value
ID	<input type="text" value="dev_voip"/>
Network Protocol	IP
Priority	<input type="text" value="1"/>
Transport Protocol	<input type="text" value="TCP"/>
TOS	<input type="text"/>
Source IP:Port	<input type="text" value="Develope_Team"/> : <input type="text" value="any"/>
Destination IP:Port	<input type="text" value="any"/> : <input type="text" value="VoIP"/>

Filter means a configuration filtering for the values in the packet header. Values set in **[QoS] → [Group] → [Port Group]** and **[IP Group]** used, and protocols and TOS fields can also be filtered. In addition, priority can be set for each filter and apply the filtering rule according to the priority.

Class Group

Select [**Class Group**] to retrieve, set, edit, or delete SPQ class group and HTB class group. A class includes information on the defined filtering rule and the bandwidth that should be assigned to the filtered traffic.

SPQ Class Group

SPQ Class Group List

	Name	Type	High Priority	Middle Priority	Low Priority
<input checked="" type="radio"/>	spq_leaf	leaf			
Filter	dev_voip				
<input type="radio"/>	spq_root	root	spq_leaf		

Click the [**Add**] button of the SPQ Class Group list in the <**Class Group**> window. Then, the window that can set SPQ class group appears. If Class Type is set to leaf, the window displayed is as follows. Set the ID and filter of leaf class and click the [**OK**] button.

SPQ Class Group

Category	Value
ID	leaf
Class Type	<input type="radio"/> root <input checked="" type="radio"/> leaf

Filter Apply

Filter List	Action	Apply Filter
	ADD >>	dev_voip
	ADD ALL >>>	
	<< REMOVE	
	<<< REMOVE ALL	

When the Class type is set to root, the window is as follows. Set the root class ID and child class and click the [OK] button.

SPQ Class Group

Category	Value
ID	<input type="text" value="leaf"/>
Class Type	<input checked="" type="radio"/> root <input type="radio"/> leaf
High	<input type="text" value="none"/>
Middle	<input type="text" value="none"/> <input type="text" value="spq_leaf"/>
Low	<input type="text" value="none"/>

Item	Description
Class Type	Configuration window depends on the type of the class to be set. - root: Sets the root class. - Leaf: Sets the leaf class.
High	Sets the leaf class whose priority will be set to high.
Middle	Sets the leaf class whose priority will be set to middle.
low	Sets the leaf class whose priority will be set to low.
Filter List	Sets the filtering rule for the target traffic in the target class.



NOTE

SPQ

SPQ queue is the simplest queuing method. The priority of the leaf class can be set to high, middle, or low. From the highest priority, service is provided.

HTB Class Group

HTB Class Group List

	Name	Type	Parent	Prio	MTU	Rate	Ceil	Burst	Cburst
<input checked="" type="radio"/>	root	root				10 Mbps			
<input type="radio"/>	leaf	leaf	root	5		5 Mbps			
Filter						dev_voip			
Time	Sun Mon Tue	03H ~ 12H				6 Mbps			

Click the **[Add]** button of HTB Class Group List in the **<HTB Class Group>** window to display the window where HTB class group can be set. If the class type is root, the window is displayed as follows. Set each item and click the **[OK]** button.

HTB Class Group

Category	Value
ID	<input type="text" value="root"/>
Class Type	<input checked="" type="radio"/> root <input type="radio"/> general <input type="radio"/> non-leaf <input type="radio"/> leaf
Rate	<input type="text" value="10"/> <input type="text" value="Mbps"/>
Burst	<input type="text"/> <input type="text" value="Byte"/>

If the class type is general, the window is displayed as follows. Set each item and click the **[OK]** button.

HTB Class Group

Category	Value
ID	<input type="text" value="general"/>
Class Type	<input type="radio"/> root <input checked="" type="radio"/> general <input type="radio"/> non-leaf <input type="radio"/> leaf
Parent ID	<input type="text" value="root"/>
Priority	<input type="text" value="1"/>
Rate	<input type="text" value="10"/> <input type="text" value="Mbps"/>
Ceil	<input type="text"/> <input type="text" value="Bps"/>
Burst	<input type="text"/> <input type="text" value="Byte"/>
CBurst	<input type="text"/> <input type="text" value="Byte"/>

If the class type is non-leaf, the window is displayed as follows. Set each item and click the **[OK]** button.

HTB Class Group

Category	Value
ID	<input type="text" value="general"/>
Class Type	<input type="radio"/> root <input type="radio"/> general <input checked="" type="radio"/> non-leaf <input type="radio"/> leaf
Parent ID	<input type="text" value="root"/>
Priority	<input type="text" value="1"/>
Rate	<input type="text" value="10"/> <input type="text" value="Mbps"/>
Ceil	<input type="text"/> <input type="text" value="Bps"/>
Burst	<input type="text"/> <input type="text" value="Byte"/>
CBurst	<input type="text"/> <input type="text" value="Byte"/>

If the class type is leaf, the window is displayed as follows. Set each item and click the [OK] button.

HTB Class Group

Category	Value
ID	<input type="text"/>
Class Type	<input type="radio"/> root <input type="radio"/> general <input type="radio"/> non-leaf <input checked="" type="radio"/> leaf
Parent ID	<input type="text" value="none"/>
Priority	<input type="text" value="1"/>
Rate	<input type="text"/> Bps
Ceil	<input type="text"/> Bps
Burst	<input type="text"/> Byte
CBurst	<input type="text"/> Byte
Leaf Qdisc	<input type="text" value="none"/> Attach on Leaf class!

Filter Apply

Filter List	Action	Apply Filter
dev voip	ADD >>	<input type="text"/>
	ADD ALL >>>	
	<< REMOVE	
	<<< REMOVE ALL	

Time Setting

Scheduling Parameter 0							
<input type="checkbox"/>	<input type="checkbox"/> Sun	<input type="checkbox"/> Mon	<input type="checkbox"/> Tue	<input type="checkbox"/> Wen	<input type="checkbox"/> Thu	<input type="checkbox"/> Fri	<input type="checkbox"/> Sat
<input type="checkbox"/>	Start Time	<input type="text" value="00"/> Hour	End Time	<input type="text" value="00"/> Hour			
	Rate	<input type="text"/> Bps	Ceil	<input type="text"/> Bps			
	Burst	<input type="text"/> Byte	Cburst	<input type="text"/> Byte			

Item	Description
Class Type	Configuration window depends on the type of the class to be set. - root: Sets the root class. - general: Sets the class that connects the root with the leaf classes. - non-leaf: Sets the default class. - Leaf: Sets the leaf class.
Parent ID	If the target class is a child class of another class, set the parent class in the Parent ID item. Do not set the Parent ID if the target class is the root class(highest level class physically connected to the device) or if the default class(class including the bandwidth for traffics that do not belong to a filter).
Priority	If several classes compete to occupy leftover bandwidths or if all classes attempt to occupy excess bandwidth, set the priority so that the class with the highest priority occupies the bandwidth first.
MTU	The Maximum Transmit Unit(MTU) represents the maximum amount of packets that can be transmitted at a time. It is recommended that this configuration does not exceed the maximum packet size (1504 Byte) of Ethernet. If this item is not entered, the default value, '1500' Byte, will be applied.
Rate	This is the basic bandwidth needed for setting class for an assigned bandwidth.
Ceil	Maximum value of assigned bandwidth.
Burst	Size of data that can be sent by the class.
Cburst	Maximum data size that can be sent at a time.
Filter List	Sets filtering rules for the class.
Leaf Qdisc Parameter	Set a desired Qdisc for the Leaf Qdisc parameter when setting the lowest level class.
Scheduling Parameter	Changes the bandwidth of the class based on day and hour. Click the [Add] or [Delete] button to add or delete.

Because of the attribute of QoS layer, the class to be set may be the highest class(Root Class) or the lowest class(Leaf Class). In addition the class to be set is classified into Parent class and Child class.

Policy

The **[Policy]** menu is used for setting a class for a port. Enter the following items and click the **[Save]** button to select a class for a port.

Policy

Category	Configuration
Device	<input type="text" value="WAN1"/>
QDISC Type	<input type="radio"/> SPQ <input checked="" type="radio"/> HTB
R2Q	<input type="text"/>
Root Class	<input type="text" value="none"/>
Default Class	<input type="text" value="none"/>

Device	QDISC Type	R2Q	Root Class	Default Class
WAN1				
DMZ				
LAN				
WAN2				
SERIAL				

Item	Description
Device	Selects a port(eth0, eth1, eth2, V.35, or HSSI)
QDISC Type	Selects QDISC to be applied to the port.
R2Q	R2Q is used as a variable for calculating the amount of Deficit Round Robin(DRR).(Bps/r2q)
Root Class	Class connected to the port. Select the class group from the class group list.
Default Class	This class defines the bandwidth for incoming traffics that are not applicable to all filtering rules. Select the class group from the class group list.

Management

This menu is used to execute, stop, and re-execute QoS. In addition, this menu is used to execute or stops the execution of 'Scheduling Parameter' set in [QoS] → [Group] → [Class Group].

QoS Management

Activity	Action Type	Time Check	Action
Stop	start	<input type="checkbox"/> on/off	Run

Status

Select the **[Status]** menu of GWIM to display the submenus of Status on the upper left section of the window.

Status
[-] Connection
▶ Sessions
[-] Statistics
Devices
Protocols
[-] Monitoring
Current
History
Process
Service

Menu	Submenu	Description
Connection	Sessions	Displays the information on the IP and port connected to GWIM.
Statistics	Devices	Displays GWIM network statistics by classifying Tx and Rx of each device.
	Protocols	Displays GWIM network statistics of each protocol.
Monitoring	Current	Provides the GWIM network statistics in the table format in real time.
	History	Displays the GWIM network statistics on a hourly, weekly, monthly, yearly basis.
	Process	Displays the information on processes being operated in GWIM.
Services	-	Displays service status in a table format by classifying various functions provided by GWIM into Security, Router, and Management.

Connection

The [Connection] menu is used to display the GWIM session connection status.

Sessions

This menu is used to display the information connected to GWIM.

Session list

Protocol	Src IP	Src port	Status	Dst IP	Dst port
UDP	165.213.110.41	1503	UNREPLIED	165.213.87.65	5025
UDP	127.0.0.1	1106	ASSURED	127.0.0.1	snmp
UDP	165.213.110.41	1503	UNREPLIED	192.168.0.15	5025
UDP	165.213.110.41	1503	ASSURED	203.241.132.34	domain
UDP	165.213.87.161	3424	UNREPLIED	255.255.255.255	snmp
TCP	127.0.0.1	1040	ASSURED	127.0.0.1	smux
TCP	127.0.0.1	1041	ASSURED	127.0.0.1	smux
TCP	127.0.0.1	1042	ASSURED	127.0.0.1	smux
TCP	165.213.79.232	3104	ASSURED	165.213.110.41	http
TCP	165.213.79.232	3105	ASSURED	165.213.110.41	http
TCP	165.213.79.232	3106	ASSURED	165.213.110.41	http
TCP	165.213.79.232	3107	ASSURED	165.213.110.41	http

Item	Description
Protocol	Type of the protocol connected with session(UDP, TCP)
Src IP	Source IP
Src Port	Source port
Status	- UNREPLIED: Packets that are expected to be answered are received, but there is no response packet. - ASSURED: There is no response packet. (‘UNREPLIED’ is changed to ‘ASSURED’.)
Dst IP	Destination IP
Dst Port	Destination port

Statistics

This menu is used to display GWIM network statistics of each device and protocol.

Devices

Select [**Statistics**] → [**Devices**] and display GWIM network statistics by classifying received part and transmitted part of each device.

Received								
Devices	Bytes	Packets	Errs	Drop	FIFO	Frame	Compressed	Multicast
Ethernet 0	18314987	162219	0	0	0	0	0	0
Ethernet 1	8351384	67681	0	0	0	0	0	0
Ethernet 2	536234	7771	0	0	0	0	0	0
Serial0	0	0	0	0	0	0	0	0
Serial1	0	0	0	0	0	0	0	0

Transmitted								
Devices	Bytes	Packets	Errs	Drop	FIFO	Frame	Compressed	Multicast
Ethernet 0	21932538	80798	0	0	0	0	0	0
Ethernet 1	774129	4165	0	0	0	0	0	0
Ethernet 2	0	0	0	0	0	0	0	0
Serial0	0	0	0	0	0	0	0	0
Serial1	0	0	0	0	0	0	0	0

Item	Description
Devices	Port type
Bytes	Total number of bytes received or transmitted
Packets	Total number of packets received or transmitted
Errs	Number of packets where an error occurs
Drop	Number of packets lost
Fifo	FIFO queue is full(FIFO Overrun)
Frame	Ethernet header is not met the format(Frame Alignment Error)
Compressed	Number of compressed packets
Multicast	Number of multicast packets

Protocols

Select **[Statistics]** → **[Protocols]** and display GWIM network statistics of each protocol(Unit: Byte)

Network statistics by protocols

Protocol	Received	Transmitted	Total
IP	18461967	15866041	34328008
ICMP	14820017	14821615	29641632
TCP	35550	35255	70805
UDP	16002	15151	31153

Monitoring

This menu is used to display GWIM network statistics in real time or display as accumulation value of a certain period.

Current

This menu is used to display GWIM network statistics in real time, and the data is updated every 5 seconds.

Rate(Bytes/Sec)

Devices	Received	Transmitted	Trans/Recv
Ethernet 0	2735	8513	2249
Ethernet 1	0	0	0
Ethernet 2	56	0	11
Serial 0	0	0	0
Serial 1	0	0	0

History

This menu is used to display CPU use, available memory capacity, and network statistics of GWIM as the accumulation value on an hourly, weekly, monthly, and yearly.

Accumulated Monitoring Graph

Device	Selection Check
CPU Utilization	<input type="radio"/>
Free Memory	<input type="radio"/>

Ethernet Interface	Selection Check
Ethernet 0	<input type="radio"/>
Ethernet 1	<input type="radio"/>
Ethernet 2	<input type="radio"/>

Services

This menu is used to display the statuses of the Security, Router, and Management services provided by GWIM in a table format.

If 'Auto Start' is set to 'On', the services are provided automatically while the system reboots. If 'Activity' is set to 'Running', the service is being performed. If 'Activity' is set to 'Stopped', the service stops.

Security

This menu is used to display the current status of the Security service provided by GWIM.

Security

Name	Activity
NAT (Network Address Translation)	Running
Filter	Running
PPTP (Point-to-Point Tunneling Protocol)	Stopped
IDS (Intrusion Detection System)	Stopped
L2TP (Layer 2 Transfer Protocol)	Stopped
IPSEC (IP Security)	Stopped

Router

This menu is used to display the current status of the Router service provided by GWIM.

Router	
Name	Activity
RIP (Routing Information Protocol)	Running
OSPF (Open Shortest Path First)	Running
BGP (Bolder Gateway Protocol)	Running
DVMRP (Distanced Vector Multicast Routing Protocol)	Stopped
PIM-SM	Stopped

Application

This menu is used to display the current status of the Application service provided by GWIM.

Application	
Name	Activity
QoS (Quality of Service)	Stopped
SIP ALG (Session Initiation Protocol)	Stopped
NTP (Network Time Protocol)	Stopped
DHCP (Dynamic Host Configuration Protocol)	Stopped
SSH (Secure Shell)	Stopped
Telnet / Ftp	Running

Management

This menu is used to display the current status of the Management service provided by GWIM.

Management	
Name	Activity
Network LoadBalance	Stopped
Accumulated Network/System Monitoring	Running
SNMP (Simple Network Management Protocol)	Stopped

VPN Menu

Select the [VPN] menu of the Data Server to display the submenus of [VPN] on the upper left corner of the window as follows:

VPN
<input type="checkbox"/> IPSEC
<input checked="" type="checkbox"/> Configuration
Certificate
Management
<input type="checkbox"/> L2TP
Configuration
Management
<input type="checkbox"/> PPTP
Configuration
Management
<input type="checkbox"/> STATUS
Ipsec
L2tp/pptp

Menu	Submenu	Description
IPSec	Configuration	Sets up IPSec.
	Management	Allows/Inhibits execution of IPSec. Sets whether to execute IPSec when the system reboots.
	Certificate	Generates or deletes a certificate.
L2TP	Configuration	Sets up L2TP.
	Management	Allows/Inhibits execution of L2TP. Sets whether to execute L2TP when the system reboots.
PPTP	Configuration	Sets up PPTP.
	Management	Allows/Inhibits execution of PPTP. Sets whether to execute PPTP when the system reboots.
STATUS	Ipsec	Checks if IPSec tunnel is properly connected.
	L2tp/pptp	Checks if L2tp/PPTP is properly connected.



NOTE

Setting up VPN Client in Windows XP/2000

Setting up VPN client in MS Windows is required when IPSec and PPTP are set in the [VPN] menu in the OfficeServ 7200 Data Server. For detailed information on setting method, refer to 'Appendix A'..

IPSec

IP Security Protocol(IPSec) provides security services in the IP layer through implementing Internet Key Exchange(IKE). The security service is categorized into two services depending on remote equipment: the services providing security tunnels between local subnet and remote subnet, and between local subnet and remote host.

Even if IPSec can be set up to provide a security tunnel between local host and remote host, the GWIM board is used for a gateway, not a host. Thus, this service is not used.

Since IPSec setting requires two gateways for a security tunnel, local configuration and remote configuration have the same items.



NOTE

IPSec Tunnel Mode

OfficeServ 7400 Data Server only supports the IPSec Tunnel mode. The transport mode is not supported. In addition, if the WAN interface is used for SERIAL, IPSec is not supported. Since a SERIAL line is used for a dedicated line, IPSec is not required for the security.

Config

On the [IPSec] → [Configuration] menu, the user can add, delete, and search an IPSEC tunnel.

IPSec Connection

Select	Connection ID	Local IP	Remote IP
○	xxxx	192.168.17.100	211.217.127.72

Add
Edit
Delete

The menu buttons are defined as shown below:

Item	Description
Add	Creates IPSec tunnel
Delete	Deletes IPSec tunnel
Edit	Modifies IPSec tunnel data

Add

Click the **[Add]** button from the <**IPSec Connection**> window to display the window below. Enter the value of each item and click the **[Add]** button to add an IPSEC tunnel.

Category	Local Settings	Remote Settings
ID	<input type="text" value="xxxx"/>	
ID	<input type="text" value="192.168.17.100"/>	<input type="text" value="211"/> <input type="text" value="217"/> <input type="text" value="127"/> <input type="text" value="72"/>
Route	<input type="text" value="192"/> <input type="text" value="168"/> <input type="text" value="17"/> <input type="text" value="1"/>	<input type="text" value="211"/> <input type="text" value="217"/> <input type="text" value="127"/> <input type="text" value="1"/>
Subnet IP	<input type="text" value="100.0.0.0"/>	<input type="text" value="200"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
Subnet Mask	<input type="text" value="255"/> <input type="text" value="255"/> <input type="text" value="255"/> <input type="text" value="0"/>	<input type="text" value="255"/> <input type="text" value="255"/> <input type="text" value="255"/> <input type="text" value="0"/>

Authentication Method

<input checked="" type="radio"/> Preshared	<input type="radio"/> RSA	<input type="radio"/> Certificate
Password	<input type="text" value="...."/>	
Re-password	<input type="text" value="...."/>	

Item	Description
Connection ID	ID composed of certain letters(Required)
IP Address	External IP address(Required)
Router	Router IP address
Subnet IP	Internal IP address
Subnet Mask	Internal subnet mask
RSA Key/ Preshared Key /Certificate	<p>Selects host authentication method</p> <ul style="list-style-type: none"> - RSA Key: Public key is RSA key of Local settings. Click the [Download] button to store RSA key to your PC, and send it to other PC through a path. After RSA key of Remote settings receives file in the target PC through a path, click the [Upload] button to enter a key value. - Preshared Key: Authentication method entering password. - Certificate: its own certificate and the CA certificate that authenticates the previous certificate are used for the authentication. For Local settings, select a certificate from the certificate list.(If selecting a certificate, the Local ID of Advanced is entered automatically) For Remote settings, enter Remote ID. It is available to check the integrity of the host certificate registered to Local.

If the value of the 'Router' item is not entered, the 'IP address' item of the Local settings and Remote settings will be used as the 'Router' item.
If the 'Subnet IP' item value and the 'Subnetmask' item value are not entered in the Remote settings, the security tunnel between local subnet and remote host will be added. Then, remote IPSEC client can operate as a part of local subnet.



NOTE

Router Value Configuration

If 'IP Address' of 'Local settings' and the network address of 'IP Address' of 'Remote settings' (the result of Netmask for IP Address) are identical, enter the value of 'IP Address' of 'Remote settings' as the value for the 'Router' of 'Local settings' and enter the value of 'IP Address' of 'Local settings' as the value for 'IP Address' of 'Remote settings'.



NOTE

Connection ID Value Configuration

The value of Connection ID should be configured of alphanumerical characters and the first character should be an alphabet.
(The value cannot be composed of only numbers.)

Advance

Click the [Advanced] button from the <IPsec Add> or <IPsec Mod> window to display the following window and it is available to set up detailed items of IPSEC.

Advance

Phase 1

Mode: sec

Encryption-Hash Algorithm: sec

Key Life Time: sec

Phase 2

Protocol: sec

Encryption-Hash Algorithm: sec

Key Life Time: sec

Dead Peer Detect

Time Out: sec

Delay: sec

Action: sec

Advance

Negotiation Count: sec

Perfect Forward Secrecy: sec

Rekey: sec

Connection: sec

Local Protocol/Port Select: /

Remote Protocol/Port Select: /

Item		Description
Phase1	mode	Ike mode - main: Configures a secure channel to perform the ISAKMP exchange of phase one - aggressive: Different type of phase one, which is more simple and faster than the main mode
	Encryption-Hash Algorithm	Supporting Algorithm 3DES-MD5, 3DES-SHA1, AES-MD5, AES-SHA1
	Key life time	IKE Duration If Key life time is passed, the host authentication (the phase one IKE) is performed again.

(Continued)

Item		Description
Phase2	Protocol	Selects a packet authentication protocol - Authentication Header(AH): Allows the authentication of data transmitter - Encapsulating Security Payload(ESP): Allows the authentication and data encryption
	Encryption-Hash Algorithm	Supporting Algorithm 3DES-MD5, 3DES-SHA1, AES-MD5, AES-SHA1
	Key life time	The cycle of newly added key used for packet encryption by the repeated phase two IKE negotiation
Advance	PFS	Selects whether to use a session key transfer/security
	Re-Key	Sets whether to add a new key(whether to add a new key and negotiate again in the phase 1, 2 IKE).
	Negotiation count	Reattempt count of key exchange when key exchange is failed on the phase 1 IKE
	Connection	Ipssec Connection Attempt - initiator: Attempting a connection - response: Attempt to receive a connection
	Left port/protocol select	Local Protocol and port limit
	Right port/protocol select	Remote Protocol and port limit
DPD	Time out	Effective time when the counterparty receives a DPD packet and receive packet
	Delay	Alive check time of the counter party
	Action	Action after Dead Peer Detect - hold: Waiting for connection - clear: No more connection

The aggressive mode only supports the authentication methods of Pre-shared key and Encryption Algorithm 3DES. The items use defaults and it is available to modify the value of PFS or Key lifetime for the interaction with other equipments.

Management

The user allows/inhibits executing IPSEC services on the [IPSEC] → [Management] menu. When the system is rebooted in the execution of IPSEC, the IPsec service is automatically performed.

IPSEC Management

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

RSA	Action
Create the new RSA key	<input type="button" value="OK"/>
Download the current RSA key	<input type="button" value="Download"/>

External Device	Action
<input checked="" type="checkbox"/> eth1	<input type="button" value="OK"/>

Click the [OK] button of the [Create the new RSA key] item to add a new RSA (public key password method) key. Use this menu to add a new RSA key if the host authentication method of RSA key used.

Click the [OK] button after selecting a device of the [External Device] items to apply the IPsec connection to the device.

Certificate

The user can verify Issue/delete/download of CA Certificate and Host certificate, addition/delete of an external certificate and the current certificate list.

CA Certificate List

Select	Subject	Cert file
<input type="checkbox"/>	Country : ko State : 1 Locality : 1 Organization : 1 Organization unit : 1 Common name : 1 Email : 1 date : Sep 22 12:49:10 2005 GMT - Sep 21 12:49:10 2009 GMT	<input type="button" value="Download"/>

External CA Certificate List

Category	ID

Host Certificate List

Select	Subject	Cert file

The menu buttons are defined as shown below:

Item	Description
(CA) Download	CA Certificate download
(CA) Delete	CA Certificate delete
(Ex) upload	External CA Certificate upload
(Ex) Delete	External CA Certificate delete
(Host) Add	Host Certificate add
(Host) Delete	Host Certificate delete

CA Certificate

CA Certificate

Distinguish Name	
Country (2 letter : ko, jp)	<input type="text"/>
State	<input type="text"/>
Locality	<input type="text"/>
Organization	<input type="text"/>
Organization Unit	<input type="text"/>
Common	<input type="text"/>
Email	<input type="text"/>
Password	<input type="text"/>
Confirm Password	<input type="text"/>

Each item of CA Certificate is defined as follows:

Item	Description
Country name	Country name(Two characters: ex. kr, cn)
State name	State name
Locality name	Local name
Organization name	Company name
Organization unit name	Organization(division) name
Common name	Name
Email address	Email
Password	Certificate password
Confirm Password	Confirming the password of certificate

* Verify the certificate password when deleting CA Certificate.

External Certificate

The upload items of an external certificate are defines as follows:

Item	Description
CA Certificate	External certificate upload

Host Certificate

The upload items of an external certificate are defines as follows:

Item	Description
Common name	Name
Email address	Email address
Password	Certificate password
Confirm Password	Confirming certificate password

L2TP

The user can set up the security tunnel between a local subnet and remote host simply by using Layer2 Tunneling Protocol(L2TP). Since it is simpler to set up than IPsec and software is provided from the Windows operating system, the user can apply the VPN function easily.

Configuration

In the [L2TP] → [Configuration] menu, the user can create/modify/delete/retrieve the VPN tunnel data.

User List

Category	ID	IP Allocation
○	11	auto ip allocation

The menu buttons are defined as follows:

Item	Description
Add	Create a PPTP user
Delete	Delete a PPTP user
Edit	Modify a PPTP user information

Add

If clicking the **[Add]** button on the <L2TP user list> window, the following window appears. Enter each item and click the **[OK]** button to create a L2TP user.

User Add

User Info	
ID	<input style="width: 100%;" type="text"/>
Password	<input style="width: 100%;" type="password"/>
Confirm Password	<input style="width: 100%;" type="password"/>
<input checked="" type="radio"/> Auto IP Allocation	
<input type="radio"/> Static IP Allocation	<input style="width: 20px;" type="text"/> . <input style="width: 20px;" type="text"/> . <input style="width: 20px;" type="text"/> . <input style="width: 20px;" type="text"/>

Item	Description
User ID	ID composed of certain letters
Password	Shared password
Dynamic IP	Enter dynamic IP to remote client
Static IP	Enter static IP to remote client(Enter IP address)

Edit

Click the **[Edit]** button from the <User List> window. Then, the window below appears. Enter each item value and click the **[OK]** button to edit VPN tunnel data.

User Mod

User Info	
ID	<input style="width: 100%;" type="text" value="11"/>
Password	<input style="width: 100%;" type="password" value="••"/>
Confirm Password	<input style="width: 100%;" type="password" value="••"/>
<input checked="" type="radio"/> Auto IP Allocation	
<input type="radio"/> Static IP Allocation	<input style="width: 20px;" type="text"/> . <input style="width: 20px;" type="text"/> . <input style="width: 20px;" type="text"/> . <input style="width: 20px;" type="text"/>

Management

In the [L2TP] → [Management] menu, the user can allow/inhibit executing PPTP services. When the system is rebooted in the execution of L2TP, the L2TP service is automatically performed.

L2TP Management

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

Type	Range	Setting
Local IP	<input type="text" value="192"/> , <input type="text" value="168"/> , <input type="text" value="254"/> , <input type="text" value="95"/>	<input type="button" value="Save"/>
Remote IP	<input type="text" value="192"/> , <input type="text" value="168"/> , <input type="text" value="254"/> , <input type="text" value="97"/> - <input type="text" value="98"/>	
Method	<input type="text" value="pap"/>	

The user can set up the IP range of the remote client that uses dynamic IP in the 'Local IP range' item, and set up the IP range of PPP daemon responsible for remote client in the 'Remote IP range' item. The encryption method supports 'pap' and 'chap'.



CAUTION

Setting up IP Range

The number of IPs for the 'Local IP range' and that for the 'Remote IP range' should be identical.

For example, if the number of IPs for 'Local IP range' is 10 and that for 'Remote IP range' is 20, only 10 calls will be set.

PPTP

The user can set up the security tunnel between a local subnet and remote host simply by using Point to Point Tunneling Protocol(PPTP). Since it is simpler to set up than IPSec and software is provided from the Windows operating system, the user can apply the VPN function easily.

Configuration

On the [PPTP] → [Configuration] menu, the user can create/modify/delete/retrieve the VPN tunnel data.

User List

Category	ID	IP Allocation
○	11	auto ip allocation

The menu buttons are defined as follows:

Item	Description
Add	Create a PPTP user
Delete	Delete a PPTP user
Edit	Modify PPTP user information

Add

If clicking the **[Add]** button on the <PPTP user list> window, the following window appears. Enter each item and click the **[OK]** button to create a PPTP user.

User Add

User Info	
ID	<input style="width: 100%;" type="text"/>
Password	<input style="width: 100%;" type="password"/>
Confirm Password	<input style="width: 100%;" type="password"/>
<input checked="" type="radio"/> Auto IP Allocation	
<input type="radio"/> Static IP Allocation	<input style="width: 20px;" type="text"/> . <input style="width: 20px;" type="text"/> . <input style="width: 20px;" type="text"/> . <input style="width: 20px;" type="text"/>

Item	Description
User ID	ID composed of certain letters
Password	Shared password
Dynamic IP	Enter dynamic IP to remote client
Static IP	Enter static IP to remote client(Enter IP address)

Edit

Click the **[Edit]** button from the **<User List>** window. Then, the window below appears. Enter each item value and click the **[OK]** button to edit VPN tunnel data.

User Mod

User Info	
ID	<input type="text" value="11"/>
Password	<input type="password" value="••"/>
Confirm Password	<input type="password" value="••"/>
<input checked="" type="radio"/> Auto IP Allocation	
<input type="radio"/> Static IP Allocation	<input type="text" value=""/> . <input type="text" value=""/> . <input type="text" value=""/> . <input type="text" value=""/>

Management

In the **[PPTP] → [Management]** menu, the user can allow/inhibit executing PPTP services. When the system is rebooted in the execution of PPTP, the PPTP service is automatically performed.

PPTP Management

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

Type	Range	Setting
Local IP	<input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="0"/> . <input type="text" value="234"/> - <input type="text" value="238"/>	<input type="button" value="Save"/>
Remote IP	<input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="1"/> . <input type="text" value="234"/> - <input type="text" value="238"/>	

The user can set up the IP range of the remote client that uses dynamic IP in the 'Local IP range' item, and set up the IP range of PPP daemon responsible for remote client in the 'Remote IP range' item. The encryption method supports 'pap' and 'chap'.



CAUTION

Setting up IP Range

The number of IPs for the 'Local IP range' and that for the 'Remote IP range' should be identical.

For example, if the number of IPs for 'Local IP range' is 10 and that for 'Remote IP range' is 20, only 10 calls will be set.

Status

Check if the IPsec tunnel set up in the [STATUS] → [IPsec] menu is properly connected.

Status

ID	Local Subnet	Local IP	Remote IP	Remote Subnet	Auth	Protocol	ISAKMP SA	IPSEC SA
xxxx	10.0.0.0	100.0.0.100	200.0.0.100	20.0.0.0	psk	esp		

Log

ID	Contents

Refresh

Check if the L2tp/pptp tunnel set up in the [STATUS] → [L2tp/pptp] menu is properly connected.

PPTP/L2TP Status

Device Name	Local IP	Remote IP
PPP0	192.168.0.234	192.168.1.234

Refresh

IDS Menu

If selecting the [IDS] menu of GWIM, the submenu of IDS appears on the top left corner of the window.



Menu	Submenu	Description
IDS Config	Log Analysis	Classifies the logs currently stored in types to verify and search the logs
	Configuration	Sets up the rule and detection level of IDS.
	Rule Config	Updates to new rule files.
	Mail Config	Registers the mail server and email address of the manager.
	Block Config	Registers IP(IP that is not checked to block module) confirming and trusting the block list registered to a block module.
	Management	Allows or inhibits executing IDS module and block module.

IDS Config

Log Analysis

The user can view alerts detected in the IDS module by category. Select the desired category and click the **[OK]** button. Then, the following page appears.

Log Analysis

	Category	Description
<input checked="" type="radio"/>	Intrusion Type	Alert summary by intrusion type
<input type="radio"/>	Source IP	Alert summary by source IP
<input type="radio"/>	Destination IP	Alert summary by destination IP
<input type="radio"/>	Destination Port	Alert summary by destination port
<input type="radio"/>	Port Scan	Port scan summary

Search Log

	Category	Condition
<input type="checkbox"/>	Priority	All <input type="button" value="v"/>
<input type="checkbox"/>	Source IP	All <input type="button" value="v"/>
<input type="checkbox"/>	Destination IP	All <input type="button" value="v"/>
<input type="checkbox"/>	Destination Port	All <input type="button" value="v"/>

Type	Item	Description
Category	Intrusion type	Analyzes logs detected by IDS rule
	Source IP	Analyzes logs by Source IP detected at IDS
	Destination IP	Analyzes logs of the OfficeServ 7400 external IP (eth0, eth1, eth2) detected at IDS
	Destination Port	Analyzes logs when the destination IP of a log detected at IDS is the port of an external IP (eth0, eth1, eth2)
	Port Scan	Analyzes the logs when the logs detected at IDS have port scan type
Date	-	Time that log is recorded
Search Log	-	Analyzes and retrieves logs


Intrusion Type

The user can summarize alerts by type. If selecting the category of Intrusion Type, the following window appears:

Summary by intrusion type

Mon Sep 26 04:16:59 2005 ~ Mon Sep 26 20:00:37 2005

Rate(%)	Num	Sid	Priority	Description
23.7	6	384	med	ICMP PING
23.7	6	366	med	ICMP PING *NIX
23.7	6	368	med	ICMP PING BSDtype
15.81	4	408	med	ICMP Echo Reply
12.69	3	2522	med	WEB-MISC SSLv3 invalid Client_Hello attempt




Item	Description
Rate(%)	Monitors logs detected by IDS according to type and displays logs as a percentage(%).
Num	Number of logs detected by IDS according to type.
Prio	Risk level depending on the rules level of IDS. - high: Rule level is one day(the highest risk level) - med: Rule level is 2 or 3 days(mid level) - low: Rule level is 4 days(low level)
Description	Type of logs detected by IDS

If clicking the unique ID of an alert, Sid displays the information on the alert.

Sid : 384


Summary
This event is generated when an generic ICMP echo request is made



Source IP

The user can summarize alerts by the Source IP. If selecting this category, the following window appears:

Summary by source IP			
Mon Sep 26 04:16:59 2005 ~ Mon Sep 26 21:17:42 2005			
Num	Source IP	Priority	Description
6	192.168.0.210	med	ICMP PING
6	192.168.0.210	med	ICMP PING *NIX
6	192.168.0.210	med	ICMP PING BSDtype
4	192.168.0.1	med	ICMP Echo Reply
2	192.168.0.117	med	WEB-MISC SSLv3 invalid Client_Hello attempt
2	192.168.0.119	med	WEB-MISC SSLv3 invalid Client_Hello attempt



Item	Description
Num	Number of logs detected by IDS according to the host(source) IP that attacks the logs
Remote host	Host IP that attacks logs detected at IDS
Prio	Risk level depending on the rules level of IDS - high: Rule level is one day(the highest risk level) - med: Rule level is 2 or 3 days(mid level) - low: Rule level is 4 days(low level)
Description	Type of logs detected at IDS

Destination IP

The user can summarize alerts by the destination IP. If selecting this category, the following window appears:

Summary by destination IP

Mon Sep 26 04:16:59 2005 ~ Mon Sep 26 21:21:08 2005

Num	Destination IP	Priority	Description
6	192.168.17.100	med	ICMP PING
6	192.168.17.100	med	ICMP PING *NIX
6	192.168.17.100	med	ICMP PING BSDtype
4	192.168.17.100	med	ICMP Echo Reply
4	192.168.17.100	med	WEB-MISC SSLv3 invalid Client_Hello attempt



Item	Description
Num	Number of logs detected by IDS according to attacked Destination IP
Local host	Attacked host IP of logs detected by IDS
Prio	Risk level depending on the rules level of IDS - High: Rule level is one day(the highest risk level) - Med: Rule level is 2 or 3 days(mid level) - Low: Rule level is 4 days(low level)
Description	Type of logs detected by IDS

Destination Port

The user can summarize alerts by destination port. If selecting this category, the following category appears:

Summary by destination port

Mon Sep 26 04:16:59 2005 ~ Mon Sep 26 21:22:08 2005

Num	Port	Priority	Description
There is no entry			

Item	Description
Num	Numbers of detected by IDS according to port when attacked Destination IP is a network (e.g., LAN).
Port	Attacked host IP of logs detected by IDS.
Prio	Risk level depending on the rules level of IDS - High: Rule level is one day(the highest risk level) - Med: Rule level is 2 or 3 days(mid level) - Low: Rule level is 4 days(low level)
Description	Type of logs detected by IDS

Port Scan

The user can summarize alerts for Port Scan. If selecting this category, the following window appears:

Summary by portscan

Mon Sep 26 04:16:59 2005 ~ Mon Sep 26 21:22:49 2005

Ports	Hosts	Remote hosts
There is no alert		

Item	Description
Ports	Number of TCP and UDP ports that are scanned in logs detected by IDS.
Hosts	Number of host that a port scanned in logs detected by IDS
Remote host	IP that attempts port scan

Search

The user can search by condition

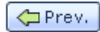
Search Log

	Category	Condition
<input checked="" type="checkbox"/>	Priority	All <input type="button" value="v"/>
<input type="checkbox"/>	Source IP	All <input type="button" value="v"/> med <input type="button" value="v"/>
<input type="checkbox"/>	Destination IP	All <input type="button" value="v"/>
<input type="checkbox"/>	Destination Port	All <input type="button" value="v"/>

If selecting the category including the desired condition, the selection box is activated. Then the user can select the desired condition. Set up the condition and click the [OK] button to display the desired information on the window as follows:

Result of Search

Src IP ->Destination IP	Dest Port	Priority	Num	Description
192.168.0.210 -> 192.168.17.100	NO	med	174	ICMP PING
192.168.0.210 -> 192.168.17.100	NO	med	174	ICMP PING *NIX
192.168.0.210 -> 192.168.17.100	NO	med	174	ICMP PING BSDtype
192.168.17.100 -> 192.168.0.121	4812	med	1	INFO TELNET access
192.168.0.1 -> 192.168.17.100	NO	med	2	ICMP Echo Reply
192.168.17.100 -> 192.168.0.121	4433	med	1	INFO TELNET access
192.168.0.117 -> 192.168.17.100	https	med	1	WEB-MISC SSLv3 invalid
192.168.0.119 -> 192.168.17.100	https	med	1	WEB-MISC SSLv3 invalid





CAUTION

Selecting Search Condition

Since the conditions are not displayed dependently, the user cannot obtain a result that satisfies all conditions.

Configuration

This page allows the configuration required for the IDS module. The user can set up the network monitored by IDS, detection level, rule file to be used at the IDS module, etc.

Select Device

The user can set up a network to monitor. For IDS module, the interface is WAN and the protocol monitors only for a static network. Therefore, if the network status is in UP, the user can select a check box as the check box is activated.

Select Device

<input checked="" type="checkbox"/> Ethernet0	<input type="checkbox"/> Ethernet1	<input type="checkbox"/> Ethernet2
---	------------------------------------	------------------------------------

OK

Set Detectiv Level & Type

The intrusion type is classified into High, Medium and Low according to the risk level. The user can set up the intrusion detection level as alert is generated when an intrusion exceeding the level occurs. In addition, the user can set up the associated operation for each level.

If setting up a block, this block is associated with the block module. So, if an intrusion corresponding to the relevant level is detected, the relevant IP is blocked not to prevent to access to the system for an configured time.

(Refer to 'Block Config')

If setting up Mail, alerts are transferred when a mail is transmitted.

(Refer to 'Mail Config')

Set Detection Level & Type

<input checked="" type="checkbox"/> High	<input checked="" type="checkbox"/> Medium	<input checked="" type="checkbox"/> Low
<input type="checkbox"/> Block	<input type="checkbox"/> Block	<input type="checkbox"/> Block
<input checked="" type="checkbox"/> Mail	<input checked="" type="checkbox"/> Mail	<input checked="" type="checkbox"/> Mail

OK

IDS Rule Configuration

This page allows setting up the rule file to be used in the IDS module.

IDS Rule Configuration

<input type="checkbox"/>	Rules	<input type="checkbox"/>	Rules
<input checked="" type="checkbox"/>	local.rules	<input checked="" type="checkbox"/>	bad-traffic.rules
<input checked="" type="checkbox"/>	exploit.rules	<input checked="" type="checkbox"/>	scan.rules
<input checked="" type="checkbox"/>	finger.rules	<input checked="" type="checkbox"/>	ftp.rules
<input checked="" type="checkbox"/>	telnet.rules	<input checked="" type="checkbox"/>	rpc.rules
<input checked="" type="checkbox"/>	rservices.rules	<input checked="" type="checkbox"/>	dos.rules
<input checked="" type="checkbox"/>	ddos.rules	<input checked="" type="checkbox"/>	dns.rules
<input checked="" type="checkbox"/>	tftp.rules	<input checked="" type="checkbox"/>	web-cgi.rules
<input checked="" type="checkbox"/>	web-coldfusion.rules	<input checked="" type="checkbox"/>	web-iis.rules
<input checked="" type="checkbox"/>	web-frontpage.rules	<input checked="" type="checkbox"/>	web-misc.rules
<input checked="" type="checkbox"/>	web-client.rules	<input checked="" type="checkbox"/>	web-php.rules
<input checked="" type="checkbox"/>	sql.rules	<input checked="" type="checkbox"/>	x11.rules
<input checked="" type="checkbox"/>	icmp.rules	<input checked="" type="checkbox"/>	netbios.rules
<input checked="" type="checkbox"/>	misc.rules	<input checked="" type="checkbox"/>	attack-responses.rules
<input checked="" type="checkbox"/>	oracle.rules	<input checked="" type="checkbox"/>	mysql.rules
<input checked="" type="checkbox"/>	snmp.rules	<input checked="" type="checkbox"/>	smtp.rules
<input checked="" type="checkbox"/>	imap.rules	<input checked="" type="checkbox"/>	pop2.rules
<input checked="" type="checkbox"/>	pop3.rules	<input checked="" type="checkbox"/>	nntp.rules
<input checked="" type="checkbox"/>	other-ids.rules	<input checked="" type="checkbox"/>	web-attacks.rules
<input checked="" type="checkbox"/>	backdoor.rules	<input checked="" type="checkbox"/>	shellcode.rules
<input checked="" type="checkbox"/>	policy.rules	<input checked="" type="checkbox"/>	porn.rules
<input checked="" type="checkbox"/>	info.rules	<input checked="" type="checkbox"/>	icmp-info.rules
<input checked="" type="checkbox"/>	virus.rules	<input checked="" type="checkbox"/>	chat.rules
<input checked="" type="checkbox"/>	multimedia.rules	<input checked="" type="checkbox"/>	p2p.rules
<input checked="" type="checkbox"/>	experimental.rules	<input type="checkbox"/>	

If pressing the **[OK]** button after selecting the desired rule file, the IDS module performs intrusion detection by using the selected rule file.
 If checking the check box on the top of each column, all rule files in the relevant column are selected. Click the **[Default]** button to select a default.

Rule Config

The user can update the rule-set file used in the IDS module to the latest version. The following window shows the version of the current rule-set file and the released date:

Current Rules' Information	
Rules' Information	
Current version	v 1.151
Release Date	2005/03/02 15:45:04

The user can set up the time to update on the following window. Click the **[OK]** button in the category of Now to update directly. Select One Time to check if there is a new file at the relevant time. The other items are used to check if there is a new file and update the file at the configured time daily, weekly or monthly.

Category	Configuration	Set
Now	Update Now	<input type="button" value="OK"/>
One Time <input type="button" value="v"/>	Day : <input type="button" value="1"/> Hour : <input type="button" value="1"/>	<input type="button" value="OK"/>
<input type="button" value="One Time"/> <input type="button" value="Daily"/> <input type="button" value="Weekly"/> <input type="button" value="Monthly"/> <input type="button" value="Not use"/>		

Mail Config

In this page, the user can set up the condition to transfer an alert recorded in the system to Mail.

Set SMTP Server IP

The user can enter an E-Mail address to receive the SMTP Server IP and alert record. Up to 10 E-Mail addresses can be entered.

Set SMTP Server IP

Server's IP	Port
<input style="width: 20px; height: 20px;" type="text"/> . <input style="width: 20px; height: 20px;" type="text"/> . <input style="width: 20px; height: 20px;" type="text"/> . <input style="width: 20px; height: 20px;" type="text"/>	<input style="width: 40px; height: 20px;" type="text" value="25"/>

Set Mail Address

Set Time for Sending Mail

The user can set up the time to send a mail, and send a mail directly or set up the desired time to receive a mail.

Set Time for Sending Mail

Category	Configuration	Set
Now	Send Mail Now	<input type="button" value="OK"/>
<input style="width: 50px; height: 20px;" type="text" value="One Time"/>	Day : <input style="width: 20px; height: 20px;" type="text" value="1"/> Hour : <input style="width: 20px; height: 20px;" type="text" value="1"/>	<input type="button" value="OK"/>

One Time

Daily

Weekly

Monthly

Not use

If clicking the button in the Now category, a mail is transferred to the e-mail address stored above the recorded alert. Select One Time to send a mail at the relevant time. The other items are used to check if there is an alert and send to Mail at the configured time daily, weekly or monthly.



SMTP Server IP Configuration

Even though a fail message or success message occurs, if a mail is not transferred to the relevant e-mail address, verify the SMTP Server IP or retrieve the IDS log in System → Log. If there is no recorded alert, a mail is not transferred.

Block Config

In this page, the user can view the block list applied to the block module or enter a trusted IP.

The screenshot shows a web interface with two main sections. The top section is titled 'Manage Blocked IP List' and contains a blue bar labeled 'Blocked IP List'. The bottom section is titled 'Manage Trusted IP List' and contains a table with two columns: 'Trusted IP List' and 'Netmask'. The 'Trusted IP List' column has four input fields for IP address digits. The 'Netmask' column has four input fields, with the first three containing the value '255' and the last one empty. Below the table are two buttons: 'OK' and 'Delete'.

Manage Blocked IP List

If an intrusion is detected when the IDS module and block module are all in operation, the IP of the block that is set up at Configuration Menu according to the intrusion risk, is blocked to access to the system for an amount of time. Manage Blocked IP List shows the list of IP that the access is blocked.

Manage Trusted IP List

The user can register a trusted IP. Enter the IP and netmask and click the [OK] button to register. Check the IP list that is already registered and click the [Delete] button to delete the list. The IP registered in this page is not blocked even in the abnormal status defined at IDS.

Management

In this page, the user can set up the operation of the IDS module and block module.

IDS Management

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

Block Management

Status	Block time	Action
Stop	<input type="text" value="10800"/> sec	<input type="button" value="Run"/>

Item	Description
Status	<ul style="list-style-type: none"> - Running: Status that the module is in operation - Stopped: Status that the module is not in operation
Action	If clicking the [Run] button, the module operates. If clicking the [Stop] button, the module stops operating.
Block time	When detecting an intrusion in the block module, the relevant IP is listed on the block list and the system access is blocked for an configured time. After the configured time, the IP is released from the block list and can access to the system.



NOTE

The block module operates depending on the IDS module and firewall. So, the IDS module and firewall should be operated to operate the block module. If the firewall is operated in advance, the block module is automatically operated when operating the IDS module.



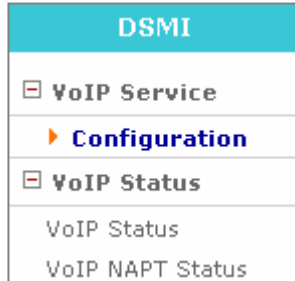
CAUTION

Check Point Before Operating IDS Module

Since the alert of the IDS module is left on System Log, the user should set up the IDS item to [ON] in System → Log → Configuration. Otherwise, it is not available to verify the intrusion detection even though the IDS module is in operation as there is no alert left.

VoIP Service Menu

Select the [DSMI] menu of GWIM to display the submenu of VoIP Service on the top left corner of the window.



Menu	Submenu	Description
VoIP Service	Configuration	Sets up VoIP Service.
VoIP Status	VoIP Status	Displays the configuration status of VoIP service.
	VoIP NAPT Status	Displays the configuration status of VoIP NAPT.

VoIP Service

Configuration

This page allows the user to set up the configuration of the VoIP service.

DataServer Module Interface Configuration

DSMI Module Configuration	
Retry Time Out	<input type="text"/> sec
Time Configuration Interval	<input type="text"/> hour

Item	Description
Retry Time out	Duration configuration of Card Alive message transferred to the call server.
Time Configuration Interval	Duration configuration of time information received from the call server.

VoIP Status

The **[VoIP Status]** menu allows displaying the current information on the OfficeServ 7400 system.

Item	Description
Call Server	Displays the type of call server(7200/7400)
Status	Displays the status of each card and phone
IP	Displays IPs of each card and phone
MAC Address	Displays MAC addresses of each card and phone
MGI Slots	Displays the slot of the MGI card
IPT Index	Displays the index of IPT Phone
WIP Index	Displays the index of WIP Phone
Port	Displays the port of IPT/WIP Phone
TEL NUM	Displays the phone number of IPT/WIP Phone

VoIP NAPT Status

VoIP NAPT Status displays NAPT items for VoIP communication on the **[VoIP NAPT]** menu. It connects 64 internal ports and external ports to each MGI card through one to one mapping.

The external ports for the VoIP service in GWIM provide UDP port 60000~61343(total 1344) and the internal ports using VoIP are assigned in MCP. So, the following information on the following window shows the current status that the VoIP terminals connect to the external environment through the firewall of GWIM.

VoIP For NAPT Status					
Public IP	StartPort	EndPort	Internal IP	StartPort	EndPort

Item	Description
Public IP	External IP to communicate with the external environment GWIM instead of the internal VoIP terminal in the system (WAN Interface IP of GWIM)
Public Start Port	Port number for external IP to communicate with external media instead of VoIP terminal in GWIM.(WAN Interface IP ports of GWIM: Configured with total 64 ports. 1:1 mapping with Internal Port)
Public End Port	Last external source port number. Configured with 64 external ports for each MGI.
Internal IP	Internal IP that VoIP terminals uses inside firewall of Data Server(IPs of VoIP terminals)
Internal Start Port	Port number for internal IP that VoIP terminals existed in internal LAN network of GWIM have(Ports for Private IP of VoIP Terminal: Configured with total 64 ports. 1:1 mapping with public port number of GWIM.)
Internal End Port	Last external source port number. Configured with 64 external ports for each MGI.

SIP ALG Menu

Select the **[SIP AGP]** menu of the GWIM to display the submenus of SIP AGP on the lower left corner of the window.

SIP ALG
Config
Management

Item	Description
Config	Sets up SIP environment.
Management	Allows/Inhibits SIP AGP implementation. Set SIP AGP to be executed when the system reboots.



NOTE

SIP ALG(SIP aware ALG)

Typically, if a firewall protects internal network based on the NAT such as the GWIM board of OfficeServ 7400, SIP AGP(SIP aware ALG) is safe from external attacks and resolves the limits on the services so that SIP devices of a firewall can communicate with external devices.

Config

In this page, the user can set up the SIP environment on the **[Config]** menu. Set up the following items and click the **[Save]** button.

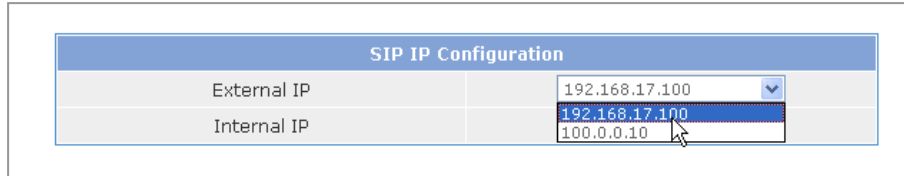
SIP Configuration

This page displays firewall installation data.

SIP IP Configuration	
External IP	192.168.17.100
Internal IP	172.16.0.1

The external IP and internal IP items are displayed on the list box so that the web manager collects and selects the usable information from the firewall configuration.

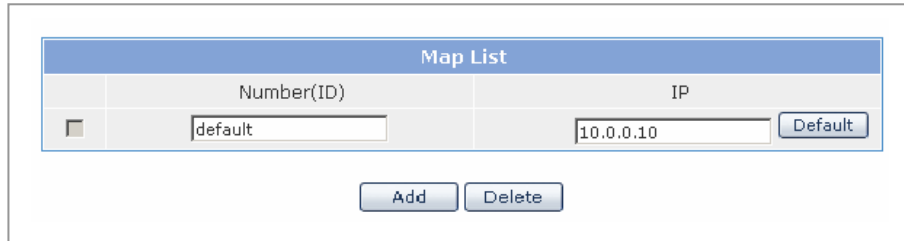
If the external or internal network is two or more, it is available to select the desired network to be the list box as follows:



The screenshot shows a form titled "SIP IP Configuration". It has two rows: "External IP" and "Internal IP". Each row has a dropdown menu. The "External IP" dropdown is currently set to "192.168.17.100". The "Internal IP" dropdown is open, showing a list of options: "192.168.17.100" (highlighted in blue), "100.0.0.10", and "100.0.0.10". A mouse cursor is pointing at the bottom option.

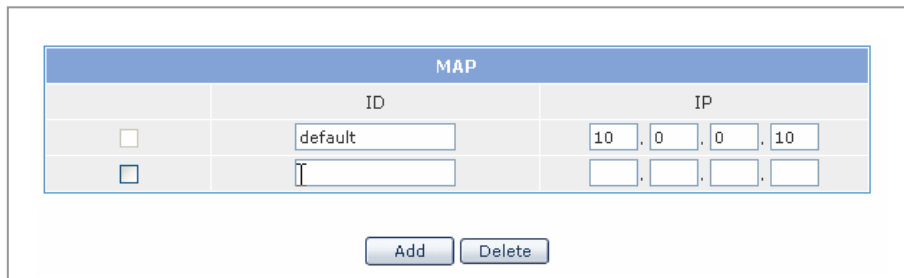
Map LIST

Enter SIP devices data inside of the firewall.



The screenshot shows a form titled "Map List". It contains a table with two columns: "Number(ID)" and "IP". The first row has a checkbox, the text "default" in a text box, the IP "10.0.0.10" in a text box, and a "Default" button. Below the table are "Add" and "Delete" buttons.

If IP or phone number is not entered on the SIP message, the IP set in the 'default' item will be used. Therefore, this item should be entered. Since configuration is convenient if all traffic is regarded as the calls of a digital phone through the Call Server, the IP of the Call Server should be entered in the 'default' item.



The screenshot shows a form titled "MAP". It contains a table with two columns: "ID" and "IP". The first row has a checkbox, the text "default" in a text box, and the IP "10.0.0.10" in a text box. The second row has a checkbox, an empty text box, and four empty text boxes for IP digits. Below the table are "Add" and "Delete" buttons.

Add the input window by clicking the **[Add]** button to add the Map information.

MAP					
	ID	IP			
<input type="checkbox"/>	default	10	0	0	10
<input checked="" type="checkbox"/>	114	10	0	0	114

Check the check box of the deletion information and click the **[Delete]** button to delete the Map information. All configurations are reflected to the system when clicking the **[OK]** button on the bottom of the SIP Configuration.

Management

Select the **[Management]** menu to allow/inhibit operating SIP ALG.

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

Management is composed of Activity that shows the current status and Action that the executable commands are displayed.

Item	Description
Activity	Current status of SIP ALG
Action	Command that is available to execute in current status

The above figure shows that SIP ALG stops operating at the current time as Activity is in Stop status. As SIP ALG is in stop status, the user can execute Action to operate SIP ALG.

If SIP ALG is in operation as Activity is running, the stop function of Action is activated.

Even though the user reboots the system, the system is restored to the last configuration status.

System Menu

Select the **[System]** menu of GWIM to display the submenu on the top left corner of the window.

System
DB Config
Admin Config
<input type="checkbox"/> Log
Configuration
Report
Download
<input type="checkbox"/> DHCP Server
Configuration
Management
Lease Info
<input type="checkbox"/> DHCP Relay Agent
Configuration
Management
<input type="checkbox"/> Time Configuration
NTP Config
Manual Config
Timezone
Upgrade
Appl Server
Reboot

Menu	Submenu	Description
DB Config		Manages the current configuration DB of GWIM
Admin Config		Sets up the authentication of the manager
Log	Configuration	Sets up whether to generate a log for each item
	Report	Searches the system logs stored currently
	Download	Downloads the system logs

DB Config

The user can save or delete DB or change the operating DB to other DB on the **[DB Config]** menu.

Configuration System DB

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

Item	Description
Import	Modifies to DB existing in the user's PC
Export	Stores the current DB to the user's PC
Default	Modifies DB to the initial configuration

To modify DB by using the DB Import function, the relevant DB file should be stored in the PC.

Since the DB Default is modified to the initial DB, the user should access the web manager at 10.0.4.1 through the LAN port of the internal network after system restart.

Admin Config

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

Login Policy

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

If checking the desired authentication method and clicking the **[OK]** button, the authentication method is applied.

If selecting two or more authentication servers, it is available to establish the priority for the authentication servers. Basically, the authentication servers are processed in the order of Local → Radius → Taccas+.

Local

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

Local

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

Radius

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

Radius			
Radius Server IP	Radius Server Key	Time out	
<input type="text"/>	<input type="text"/>	<input type="text"/>	
<input type="button" value="Add"/> <input type="button" value="Delete"/>			

Taccas+

Enter the information on the Taccas+ authentication. Up to 5 lists are entered or deleted the same as the Radius input page.

Taccas+	
Taccas+ Server	Taccas+ Secret Key
<input type="text"/>	<input type="text"/>
<input type="button" value="Add"/> <input type="button" value="Delete"/>	



CAUTION

Configuration Application

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 page allows setting up the system log and retrieving the information.

Configuration

This page allows setting up the log to determine whether to add a log to the system.

Log Policy

Advanced Service		
System	ON <input checked="" type="radio"/>	OFF <input type="radio"/>
NETWORK	ON <input type="radio"/>	OFF <input checked="" type="radio"/>
FIREWALL	ON <input type="radio"/>	OFF <input checked="" type="radio"/>
PPTP	ON <input type="radio"/>	OFF <input checked="" type="radio"/>
IPsec	ON <input type="radio"/>	OFF <input checked="" type="radio"/>
L2TP	ON <input type="radio"/>	OFF <input checked="" type="radio"/>
IDS	ON <input type="radio"/>	OFF <input checked="" type="radio"/>

OK Reset

Select added logs from the logs for system log, network, firewall, VPN and IDS, and click the **[OK]** button to add logs to the system log. Click the **[Reset]** button to return to the previous status before applying the configuration.

Report

The user can retrieve the logs stored in the system according to an item and time.

Report Policy

Advanced Service				
Log Type	ALL <input checked="" type="radio"/>	SYSTEM <input type="radio"/>	NETWORK <input type="radio"/>	FIREWALL <input type="radio"/>
	PPTP <input type="radio"/>	L2TP <input type="radio"/>	IPSEC <input type="radio"/>	IDS <input type="radio"/>

Detail Search					
	YEAR	MONTH	DAY	HOUR	MINUTE
From	2005	9	27	11	00
To	2005	9	27	18	00

OK Reset

Set up the desired log type and time and click the **[OK]** button to verify the log as shown to the following figure. Click the **[Reset]** button to return to the previous status.

Log Report
[2005-9-27 11 : 00] ~ [2005-9-27 18 : 00]

Date/Time	Message	Type
2005/9/27 17:50:40	ROOT LOGIN on `console`	login
2005/9/27 17:50:40	session opened for user toor by (uid=0)	login
2005/9/27 11:24:30	accepted smux peer: oid SNMPv2-SMI::enterprises.3317.1.2.2, descr zebos-7.2.1.ZebOS-7-2-1-rc1-customer	snmpd
2005/9/27 11:24:30	[smux_accept] accepted fd 12 from 127.0.0.1:32775	snmpd
2005/9/27 11:24:30	accepted smux peer: oid SNMPv2-SMI::enterprises.3317.1.2.5, descr zebos-7.2.1.ZebOS-7-2-1-rc1-customer	snmpd
2005/9/27 11:24:30	[smux_accept] accepted fd 11 from 127.0.0.1:32774	snmpd
2005/9/27 11:24:30	accepted smux peer: oid SNMPv2-SMI::enterprises.3317.1.2.3, descr zebos-7.2.1.ZebOS-7-2-1-rc1-customer	snmpd
2005/9/27 11:24:30	[smux_accept] accepted fd 10 from 127.0.0.1:32773	snmpd
2005/9/27 11:24:28	accepted smux peer: oid SNMPv2- SMI::enterprises.3317.1.2.10, descr zebos-7.2.1.ZebOS-7-2-1- rc1-customer	snmpd
2005/9/27 11:24:28	[smux_accept] accepted fd 9 from 127.0.0.1:32772	snmpd

1/4

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

Download

This page allows 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.

Log File Management

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

DHCP Server

The user can configure a DHCP server to execute the DHCP server or stop the operation of the server in the [DHCP Server] menu of [System].

Configuration

The [Configuration] menu allows setting various configuration items of DHCP Server.

Basically, Pool Name, Network Address and Range Address are the required fields in DHCP Server configuration.

General Options

Parameter	Argument
* Pool Name	<input type="text"/>
* Network Address	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> / <input type="text"/>
* Range Address	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> ~ <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Lease Time	1 <input type="text"/> Days 0 <input type="text"/> Hours 0 <input type="text"/> Minutes <input type="checkbox"/> Infinite
Group Number	<input type="text"/>
Client ID	<input type="text"/>
Vendor ID	<input type="text"/>
Domain Name	<input type="text"/>
Default-Router	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Fixed Address	Host <input type="text"/>
	MAC <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>
	IP <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
DNS Server	1) <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> 2) <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
WINS Server	1) <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> 2) <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>

Current Running Configured Information

Select	Parameter	Argument
It is empty that saved dhcp server configuration entry		

The configuration of DHCP Server is configured by Pool. Each items is described as follows:

Item		Description
* Pool Name		Sets up the name of Pool to distinguish from the other Pools.
* Network Address		The value of a Network to be set up. The value is classified into IP type and Netmask.
* Range Address		Sets up the range of IP addresses that DHCP Server allocates to DHCP Client. Enter the first/last IP addresses to be allocated in order to designate the range.
Lease Time		Sets up the duration to lease an IP address to DHCP Client. The default is 1Days.
Client ID		Sets up Client Identifier.
Vendor ID		Sets up Vendor Class Identifier.
Domain Name		Sets up Domain Name.
Default-Router		Sets up IP address of Default Router.
Fixed Address	Host	Sets up Name of Host.
	MAC	Sets up MAC address of a specific client.
	IP	Sets up IP Address to be allocated.
DNS Server		Sets up DNS Server.
WINS Server		Sets up WINS Server.

Fixed Address is used for allocating a fixed IP address for a specific client. If pressing the Save button after the configuration, the configuration is saved. It is available to verify and delete the saved information in the table below. Press the Delete button after checking the target Pool in order to delete.

Management

This page allows managing the operation of DHCP Server.

It is available to verify the status of DHCP Server and operate/stop DHCP Server Daemon using the **[Run]/[Stop]** button.

DHCP Server Management

Status	Action
Stoped	<input type="button" value="Run"/>

Lease Info

Leas Info is a window that allows verifying the status of DHCP Server.

DHCPD Daemon operates according to the configuration after reading the configuration from the configuration file, and records the information on allocation or returned IP Address to a specific file. Leas Info extracts the information on such file to display on the window.

Lease Info displays the information on the allocated IP Address and information used for the configuration of the window and DHCP Server.

DHCP Leases Usage

	Pool Name	Network	Total	Used	Usage
--	-----------	---------	-------	------	-------

DHCP Leases Information

	IP	MAC	Lease Starts	Lease Ends
--	----	-----	--------------	------------

DHCP Relay Agent

DHCP Relay Agent is used for applying one DHCP server to multiple Subnets. Therefore, when DHCP Server and DHCP Client are in different networks each other, the DHCP Client allows allocating an IP from IP.

Configuration

DHCP Relay is configured by assigning the interface to be relayed and registering DHCP Server.

Designate an interface, which is relayed, from the list of the activated interfaces by using the **[Add]** button. Then, the list for the designated interface is configured. If pressing the **[Delete]** button on the list, the interface is deleted. To save the list of DHCP Server, enter the IP address that DHCP Server is using and adds the address. To delete the list, select a DHCP server to be deleted and press the **[Delete]** button.

Interface List Configuration

Check	Argument
<input type="checkbox"/>	ETH eth0 ▼

Check	Server List	Server
<input type="checkbox"/>	Server List	<input style="width: 15px;" type="text"/> . <input style="width: 15px;" type="text"/> . <input style="width: 15px;" type="text"/> . <input style="width: 15px;" type="text"/>

Management

This page allows operating and stopping the DHCP Relay.

It is composed of the status display of DHCP Relay Daemon and the **[Action]** button.

DHCP Relay Agent Management

Status	Action
Stoped	<input type="button" value="Run"/>

Time Configuration

Synchronize the timezone, date and time of the system on the **[Time Configuration]** menu of the **[System]** through a network or sets up the values by itself.

NTP Config

Select **[Time Configuration]** → **[NTP Config]** and set up 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 DNS Server should be set up to use Domain Name and, a network should be connected to synchronize with Time Server by configuring such NTP.)

Click the **[OK]** button to start or restart NTP daemon to register Time Server.

NTP Configuration

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

NTP Server Status	
Status	stop

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

- 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 DNS Server should be set up to use Domain Name and, a network should be connected to synchronize with Time Server by configuring such NTP.)

Ошибка! Стил ь не определен.

Manual Config

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

Check the check box and click the **[OK]** button to synchronize the date and time of the system with Call Server.

Manual Configuration

Current Time
2005. Sep. 26. (Mon) 21:36:43

Date/Time Configuration
2005 / Sep / 26 21 : 36

Synchronization from Call Server
 Set by C/S

OK

Timezone

The user can change Time Zone by selecting the timezone corresponding to the user from the **[Time Configuration] → [Timezone]** menu. Select the desired area(city or GMT) in the areas separated by GMT and click the OK button to modify the timezone information of the system.

Time Configuration

Time Zone
(GMT+09:00) Seoul, Tokyo

OK

Upgrade

Upgrade the Kernel and Ramdisk in the PC **[Upgrade]** menu.
 For the types of upgrade, there are 'TFTP Method' and 'File Transmission Method through HTTP' as well as Local Method that uploads the user's PC.

Select Package Upgraded

Package Version	Current Version	Released Date	Upgraded Date
<input style="width: 80%;" type="text"/>	v0.19	2005.09.21	2005.09.21

Select Upgrade Method

Upgrade Method	Upgrade Server IP
<input checked="" type="radio"/> TFTP	<input style="width: 40px;" type="text"/> . <input style="width: 40px;" type="text"/> . <input style="width: 40px;" type="text"/> . <input style="width: 40px;" type="text"/>
<input type="radio"/> HTTP	
<input type="radio"/> Local	<input style="width: 150px;" type="text"/> <input type="button" value="Browse..."/>

When upgrading a package, the package version should be entered in the type such as '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 exist 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 'gwim-pkg-v0.19.tgz'.

Appl Server

The **[Appl Server]** menu manages the services of SSH, FTP and Telnet and it is available to connect to the GWIM board by using these service.

Application Server

	On/Off
SSHD	<input type="checkbox"/>
FTP	<input checked="" type="checkbox"/>
Telnet	<input checked="" type="checkbox"/>

Reboot

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

System Reboot

Warning

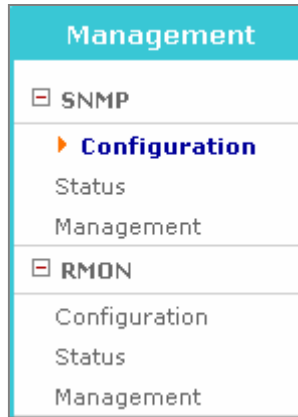
Network will be disconnected!

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 until the network and service are all executed after rebooting.

Management Menu

If selecting the [**Management**] menu of GWIM, the submenu of the Management is displayed on the top left corner of the window as follows:



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

SNMP

Configuration

Set up SNMP in the [SNMP]→[Configuration] menu.

Click the [Save] button to apply the configuration to the system.

Click the [Reset] button to reset the configuration currently set up by the user.

System Option

Set up SNMP System Option.

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

item	Description
Location	Sets up the information on System Location
Contact	Sets up the information on System Contact
Name	Sets up the information on System Name
Engine ID	Sets up the information on System Engine ID

Community

Add new community used in SNMP v1/2c.

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

Item	Description
New Community name	Fill in new community name to add.
Community Network	Set up new community network to add.
Access	Set up the access authority.

SNMPv3 User Add

SNMPv3 User Add allows adding a user to be used at SNMP v3.

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

Item	Description
User Name	Fill in new user's name to add.
User Password	Fill in new user's password. 8 alphanumeric characters
Authentication	Set up authentication method.
Encryption	Set up ciphering method.
Access	Set up access authority.

Trap Manager

This window is used to set up IP address to transmit a trap. Up to five addresses can be designated.

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

Item	Description
IP Address	Set up new Trap IP Address to add.
Community Name	Set up a community to be used for transmitting to the Trap IP Address added.

Status

The function is used for retrieving the SNMP configuration in the [SNMP] → [Status] menu.

If clicking the [Delete] button, the item that the user has selected by marking on the check box is deleted.

If clicking the [Reset] button, all check boxes are initialized.

SNMP Config Information

The user can retrieve the SNMP configuration.

System Information			
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
<input type="checkbox"/>	192.168.0.123	162

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

Management

The user can start/stop the SNMP service on the [SNMP] → [Management] menu.

If clicking the [Run] button, the SNMP service starts.

If clicking the [Stop] button, the SNMP service stops.

SNMP Management

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

SNMP Management allows the user to start/stop the SNMP service.

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

RMON

Configuration

In the [RMON] → [Configuration] menu, the user can set up RMON Global.

If clicking the [Save] button, the information that is set up by the user is applied to the system.

If clicking the [Reset] button, the information that the user is to set up is reset.

History Option

History Option allows setting up the RMON history option.

History Option	
MAX History Buckets	<input type="text"/> (50 - 5000)

Item	Description
MAX History Buckets	Sets up the maximum history storage space.

Event Options

Event Options allows the user to set up the RMON event option.

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

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

Status

The user can retrieve the configuration for RMON Global on the **[RMON]** → **[Status]** menu.

If clicking the **[Refresh]** button, the displayed information is synchronized.

RMON Global Status

RMON Global Status allows the user to retrieve the SNMP configuration.

History Global Status	
MAX History Buckets	1000
Granted History Buckets	0
Used History Buckets	0

Event Global Status	
MAX Event Logs	400
Saved Event Logs	0

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

Management

The user can start/terminate the RMON service on the **[RMON]** → **[Management]** menu.

If clicking the **[Run]** button, the RMON service starts.

If clicking the **[Stop]** button, the RMON service stops.

RMON Management

The user can start/stop the RMON service.

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

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



This page is intentionally left blank.



ABBREVIATION

A

ALG	Application Level Gateway
AH	Authentication Header
ARP	Address Resolution Protocol

C

CTI	Computer Telephony Integration
-----	--------------------------------

D

DHCP	Dynamic Host Configuration Protocol
DNAT	Destination Network Address Translation
DNS	Domain Name Server
DRR	Deficit Round Robin
DVMRP	Distance Vector Multicast Routing Protocol

E

ESP	Encapsulating Security Payload
-----	--------------------------------

H

HDLC	High-level Data Link Control
HTTP	Hypertext Transfer Protocol

I

IDS	Intrusion Detection System
IGMP	Internet Group Management Protocol
IKE	Internet Key Exchange
IPSEC	IP Security Protocol

L

LAN	Local Area Network
L2TP	Layer 2 Tunneling Protocol

N

NAT	Network Address Translation
NLB	Network Load Balance
NMS	Network Management System

R

RMON	Realtime Monitoring
------	---------------------

P

PIM-SM	Protocol Independent Multicast-Sparse Mode
PD	Power Device
PPP	Point-to-Point Protocol
PPPoE	Point-to-Point Protocol over Ethernet
PPTP	Point to Point Tunneling Protocol
PT	Protocol Translation
PVC	Permanent Virtual Circuit
PVID	Port VLAN Identification

S

STP	Spanning Tree Protocol
SMTP	Simple Mail Transfer Protocol
SNAT	Source Network Address Translation
SNMP	Simple Network Management Protocol

T

TFTP	Trivial File Transfer Protocol
------	--------------------------------

V

VLAN	Virtual Local Area Network
VPN	Virtual Private Network

OfficeServ 7400 GWIM User Manual

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

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

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

Information in this manual is subject to change without notice.

