



Enterprise IP Solutions

OfficeServ 7400

GWIM User Manual

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

Samsung Telecommunications

Publication Information

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

Copyright 2006

Samsung Telecommunications America

All rights reserved. No part of this manual may be reproduced in any form or by any means—graphic, electronic or mechanical, including recording, taping, photocopying or information retrieval systems—without express written permission of the publisher of this material.

Trademarks

Enterprise IP Solutions

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

PRINTED IN USA

INTRODUCTION

Purpose

This document introduces the OfficeServ 7400 Data Server, an application module of the OfficeServ 7400, and describes procedures for 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 General Description

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

OfficeServ 7400 Installation Manual

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

OfficeServ 7400 Programming Manual

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

Revision History

EDITION	DATE OF ISSUE	REMARKS
00	05 2006	Initial Release

SAFETY CONCERNS

For product safety and correct operation, the following information must be given to the operator/administrator 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 administrators 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 administrator 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 (i.e., IP, Gateway, and Subnet Mask) is changed and finally applied while operating a router.



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 NAPT' is not automatically changed. Therefore, 'Fixed IPs should be used for the VoIP related services that the setups of 'Port Forward' and 'Static NAPT' 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 the 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 administrators 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 are not deleted, the webscreen of GWIM may not be normally displayed.

TABLE OF CONTENTS

INTRODUCTION	1
Purpose	I
Document Content and Organization.....	I
Conventions.....	II
Console Screen Output	II
Reference	III
Revision History.....	III
SAFETY CONCERNS	IV
Symbols.....	IV
Caution	V
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	8
Network Menu	9
Network	10
NLB.....	23
Utility.....	26
Firewall Menu	28
NAT	29
Filter.....	33
Router	38
General	39
Configuration	40
List	47

Status.....	54
IPMC	57
General.....	58
Configuration	59
Status.....	65
QoS	67
Group.....	67
Policy	76
Management.....	77
Status.....	78
Connection.....	79
Statistics.....	80
Monitoring	81
Services.....	82
VPN Menu.....	84
IPSec	85
L2TP	93
PPTP	96
Status.....	98
IDS Menu	99
IDS Config	100
VoIP Service Menu.....	111
VoIP Service	111
SIP ALG Menu	114
Config	114
Management.....	116
System Menu	117
DB Config	118
Admin Config	118
Log.....	119
DHCP Server	121
DHCP Relay Agent	123
Time Configuration.....	124
Upgrade.....	126
Appl Server	126
Reboot	127
Management Menu	128
SNMP	129
RMON.....	132
My Info Menu.....	135

ABBREVIATION	136
A ~ H.....	136
I ~ T	137
U ~ Z.....	138

CHAPTER 1. Overview of OfficeServ 7400 GWIM

This chapter introduces OfficeServ 7400 system and OfficeServ 7400 GWIM.

Introduction to OfficeServ 7400

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

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

This document describes the data and routing capabilities of OfficeServ 7400 GWIM.



NOTE

Structure of OfficeServ 7400

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

Introduction to OfficeServ 7400 GWIM

OfficeServ 7400 provides the following functions:

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 functions 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.

Software Installation

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

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

GWIM Installation

1. Insert the GWIM into an open slot in the OfficeServ 7400 cabinet.
2. Connect a PC to port #1-3 of the GWIM module. You will need to configure your TCP/IP settings to match the corresponding default IP address of the GWIM shown in step 3.
3. Using Internet Explorer navigate to one of the following IP addresses to access the management interface of the GWIM.

The IP initial value of the GWIM board is set as follows:

- Port 1 - 10.0.0.1/24 (<https://10.0.0.1>)
- Port 2 - 10.0.1.1/24 (<https://10.0.1.1>)
- Port 3 - 10.0.2.1/24 (<https://10.0.2.1>)

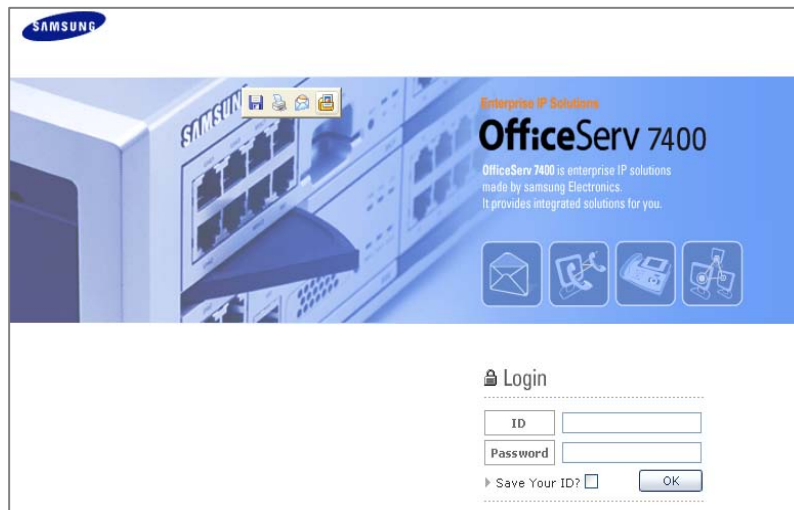


Caution for the Use of a Web Browser

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

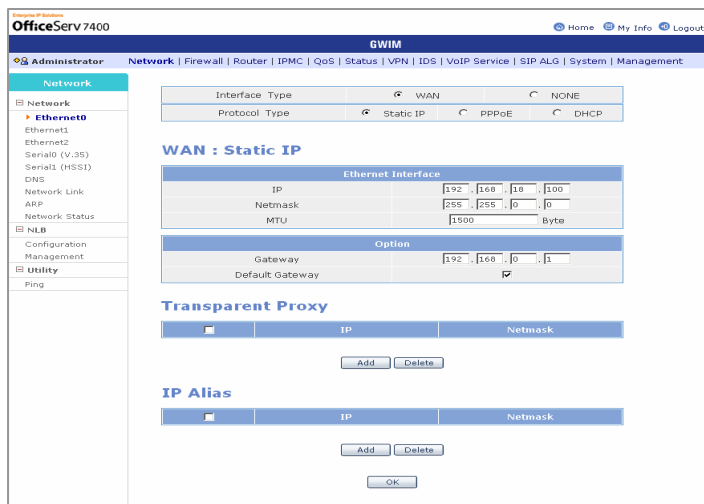
1. Start Internet Explorer and enter the IP address of the GWIM into the address bar. The login window shown below will appear:



The login window features the Samsung logo at the top left. The main header area has a blue background with the text 'Enterprise IP Solutions' and 'OfficeServ 7400'. Below this, a description states: 'OfficeServ 7400 is enterprise IP solutions made by Samsung Electronics. It provides integrated solutions for you.' There are four icons representing different services: email, VoIP, network, and security. The login section is titled 'Login' and contains two input fields: 'ID' and 'Password'. Below these fields are two checkboxes: 'Save Your ID?' and 'OK'.

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

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



The configuration window shows the 'OfficeServ 7400' title bar and a navigation menu on the left. The main content area is titled 'GWIM' and contains several sections: 'Network' (with submenus like Ethernet, Serial, and Network Link), 'WAN : Static IP' (with fields for IP, Netmask, and MTU), 'Transparent Proxy' (with fields for IP and Netmask), and 'IP Alias' (with fields for IP and Netmask). The 'WAN : Static IP' section is currently selected and shows the following values: IP: 192.168.1.100, Netmask: 255.255.0.0, MTU: 1500. The 'Transparent Proxy' section shows IP: 192.168.1.1 and Netmask: 255.255.0.0. The 'IP Alias' section shows IP: 192.168.1.1 and Netmask: 255.255.0.0. There are 'Add' and 'Delete' buttons for each section, and an 'OK' button at the bottom.

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

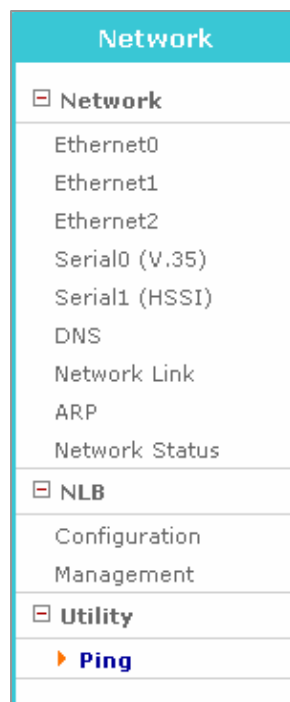
This chapter describes how to use the menus of OfficeServ 7400 GWIM.

The configuration of OfficeServ 7400 GWIM menus are as follows:

Network	Firewall	Router	IPMC	QoS	Status
- Network - Ethernet0 - Ethernet1 - Ethernet2 - Serial0 (V.35) - Serial1 (HSSI) - DNS - Network Link - ARP - Network Status - NLB - Configuration - Management - Utility - Ping	- NAT - Management - Configuration - Port Forward - Static NAT - Firewall - Management - Configuration - Remote Access - IP Filtering - URL Filtering - ICMP Filtering	- 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	- General - Mroutes - Management - Configuration - IGMP - DVMRP - DVMRP Intf - PIM-SM - PIM-SM Intf - Status - IGMP Groups - DVMRP - PIM-SM	- Group - Port Group - IP Group - Filter Group - Class Group - Policy - Management	- Connection - Sessions - Statistics - Devices - Protocols - Monitoring - Current - History - Process - Service
VPN	IDS	VoIP Service	SIP ALG	System	Management
- IPSEC - Configuration - Certificate - Management - L2TP - Configuration - Management - PPTP - Configuration - Management - STATUS - Ipsec - L2tp/ppp	- IDS Config - Log Analysis - Configuration - Rule Config - Mail Config - Block Config - Management	- VoIP Service - Management - VoIP Status - VoIP DB - VoIP NAPT List	- Configuration - Management	- DB Config - Admin Config - Log - Configuration - Report - Download - DHCP Server - Configuration - Management - Lease Info - DHCP Relay Agent - Configuration - Management - Time Configuration - NTP Config - Manual Config - Timezone - Upgrade - Appl Server - Reboot	- SNMP - Configuration - Status - Management - RMON - Configuration - Status - Management

Network Menu

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



Menu	Submenu	Description
Network	Ethernet0	setup for Ethernet port P1.
	Ethernet1	setup for Ethernet port P2.
	Ethernet2	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 displays the five network interfaces built-in to the GWIM. This menu sets IP information, transfer speed, and transfer mode of each interface. In addition, this menu sets DNS and ARP.

Note: It is recommended that your network interfaces be programmed before any other options in the GWIM.

Ethernet Setup

[Network] → [Ethernet]

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	☒ WAN	☐ LAN	☐ NONE
Protocol Type	☒ Static IP	☐ PPPoE	☐ DHCP

- WAN: The following protocol types can be selected in WAN:
 - Static IP: Select Static IP if your Internet service account uses Fixed IP (Static) IP assignment.
 - PPPoE: Select PPPoE if your Internet service account uses PPP over Ethernet login protocol, such as in ADSL account.
 - DHCP: Select DHCP if your Internet service account uses Dynamic IP assignment, such as a Cable Modem account.
- LAN: The following protocol types can be selected in LAN:
 - Private: Select to assign the internal network numbers based on private IP address.
 - Public: Select to assign the internal network numbers 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	18	100
Netmask	255	255	0	0
MTU	1500			Byte

Option	
Gateway	192 . 168 . 0 . 1
Default Gateway	☒

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.

WAN : PPPoE

Authentication	
ID	innopia
Password	

☐ Option

OK

Check the “Option” check box in the lower section to display Method, MTU, and DNS setup window.

☒ Option

Method	any
MTU	1492 byte
DNS	☒ Auto ☐ Manual

OK

The details by fields are as follows:

- 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]**.

WAN : DHCP

DHCP

Click OK button to start

☒ Option

Vendor ID

DNS

☐ Auto ☒ Manual

OK

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	10	0	0	1
Netmask	255	255	255	0
MTU	1500	Byte		

IP Alias

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

Add

Delete

OK

LAN → Public IP

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	
Netmask	
MTU	1500 Byte

Transparent Proxy

☐	IP	Netmask
Add Delete		

IP Alias

☐	IP	Netmask
Add Delete		

NONE

NONE is selected when the corresponding interface is not used.

NONE

Description
Disable network interface

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

Interface Type

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

Interface Type	☐ WAN	☐ LAN	☒ NONE
----------------	---------------------------	---------------------------	---------------------------------------

Serial Basic

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

Serial Basic	
Command	Argument
Serial Interface Name	Serial0
Physical Line Type	V.35
MTU	1500 (128~1500, Default: 1500)
Encapsulation	☐ Cisco-HDLC ☐ PPP ☒ Frame-Relay

- 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 type 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	10 (1~100, Default: 10)
Keep-Alive Timeout	25 (1~100, Default: 25)
IP Address	192 . 168 . 100 . 2 / 24
Gateway	192 . 168 . 100 . 1
Default Gateway	☒ (The Gateway is a Default Gateway)

- 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
- Default Gateway: Mark the check box to set this gateway to default gateway. (This item is displayed if WAN is set.)

PPP Configuration

Set the Encapsulation type as PPP Protocol in the Encapsulation field 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	10 (1-100, Default: 10)
Max Keep-Alive Count	6 (1-100, Default: 6)
Authentication	☐ PAP ☐ CHAP ☒ None Name: Password:
IPCP Dynamic-IP	☐ (enable IP-Address negotiation at IPCP layer)
IP Address	192 . 168 . 100 . 2 / 24
Gateway	192 . 168 . 100 . 1
Default Gateway	☒ (The Gateway is a Default Gateway)

- 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: Administrator 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
- Default Gateway: Mark the check box to set this gateway to default gateway. (This item is displayed if WAN is set.)

Frame-Relay Configuration

Set the Encapsulation type as 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	☒ ANSI ☐ CCITT ☐ None
Keep-Alive Interval	10 (5~30 seconds, Default: 10)
N391	6 (1~255 full status polling counter, Default: 6)
N392	3 (1~10 LMI error threshold, Default: 3)
N393	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 N392.

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	☐ 16 (16~1007) ☐
IP Address	192 . 168 . 100 . 2 / 24
Gateway	192 . 168 . 100 . 1
Default Gateway	☒ (The Gateway is a Default Gateway)
MTU	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
- **Default Gateway:** Mark the check box to set this gateway to default gateway. (This item is displayed if WAN is set.)
- MTU: Maximum size of the packet to transfer at once

To edit the setting of a specific PVC, select the target PVC from the list and enter the target information into each item. Click the **[Edit]** button.

PVC Interface	
Command	Argument
DLCI	☐ 16 (16~1007) ☒ pvc0/16
IP Address	192 . 168 . 100 . 8 / 24
Gateway	192 . 168 . 100 . 7
Default Gateway	☒ (The Gateway is a Default Gateway)
MTU	1500 (128~1500, Default: 1500)

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

PVC Interfaces						
	Interface	Address	Gateway	Def GW	Active	MTU
☐	pvc0/16	192.168.100.2/24	192.168.100.1	yes	no	1500
☐	pvc0/17	192.168.101.2/24	192.168.101.1	no	no	1500
☐	pvc0/18	192.168.102.2/24	192.168.102.1	no	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
Interface Serial0 Scope: both Mode type is EXTERNAL Protocol type is Cisco-HDLC Transparent is Proxyarp 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> DHCP client is disabled. VRF Binding: Not bound 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 line protocol is up input packets 8, bytes 706, dropped 0, multicast packets 0 input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0 output packets 7, bytes 154, dropped 0 output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0 collisions 0

DNS

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.

Static DNS

Domain Name

OK

Name Server List

☐	168.126.63.1
☐	168.126.63.2

Delete

Name Server Add

Add

Network Link

The Network Link menu is used for the setup of connections, transmission speeds and transmission modes by network interfaces.

Network Link

	Ethernet	Type	Negotiation	Speed	Duplex	Mac
☐	Ethernet0	ITECTechnologies-SX SFP24-MS3LC	auto	1000Mbps	full	00:00:f0:11:32:24
☐	Ethernet1	AGILENT-SX HFBR-5710L	force	1000Mbps	full	00:00:f0:11:32:25
☐	Ethernet2	AGILENT-SX HFBR-5710L	auto	1000Mbps	full	00:00:f0:11:32:26

RefreshOK

- Ethernet: Logical name of each Ethernet port
- Type: Type of Ethernet Cables/SFP GBIC Adapters
- 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 Ethernet 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
☐	reachable	192.168.0.126	00:09:74:11:11:11
☐	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

Ethernet	IP	Mac
Ethernet0		

static ARP add

The Static ARP Add window is used for the addition of static ARP.

- Ethernet: Ethernet to add static Mac
- IP: IP address 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.

ARP Age Time

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.

ARP Refresh

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.

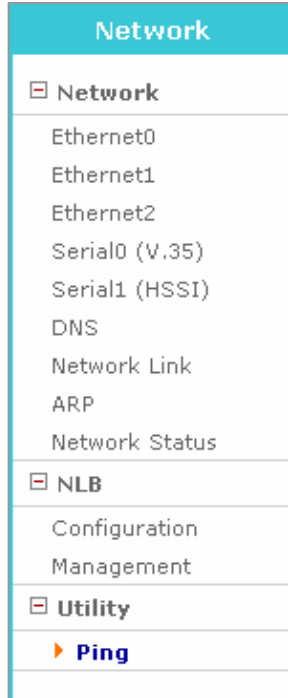
Network Status					
Category	Usage	Protocol	IP	Netmask	Gateway
Ethernet0	EXTERNAL	STATIC	192.168.17.100	255.255.0.0	192.168.0.1
Ethernet1					
Ethernet2	INT_PRIV	STATIC	10.0.0.1	255.255.255.0	
Serial0					
Serial1					

Name Server	
Server 1	168.126.63.1
Server 2	168.126.63.2

Domain

NLB

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



The GWIM supports 5 external WAN interfaces. The system can distribute the Internet access traffic to each external interfaces by using the NLB function. For effective access traffic balancing, the system uses the 'Weighted Round Robin' method. The NLB menu is used for the setup of the Network Load Balancing function.

Configuration

[Network] → [NLB] → [Configuration]

Network Load Balance Configuration

Category	Settings
NLB Weight	eth0 1
NAT Status	Enable

Static Configuration

Source	Destination	Traffic Distribution
--------	-------------	----------------------

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 selectively connected to Ethernet 0 Interface (eth 0) and Ethernet 1 Interface (eth 1), the higher weighted value is given to the eth 1 connected with ADSL line that its bandwidth is relatively bigger 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

Along with the Network Load Balance Configuration, the Static Configuration window is used to pass a specific external network interface line by separately specifying the traffic session to satisfy a specific condition. 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
☒ Mask	0 0 0 0	0 0 0 0	Gateway eth0-192.168.1.1
port	0 0	0 0	Backup default gateway

- **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 starting and stopping the NLB service.

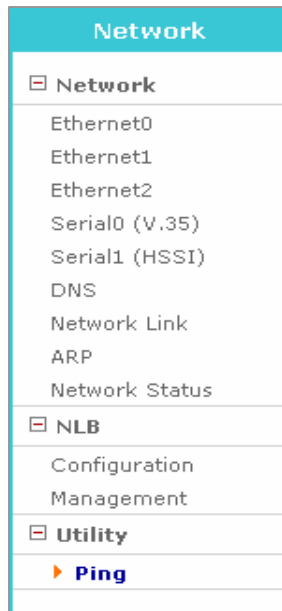
Network LoadBalance Management

Activity	Action
Stop	Run

- Activity: Current activity
- Action: Click the **[Run]** button to start the NLB service.
- If the OfficeServ 7400 system is restarted the NLB service will automatically return to its last state.

Utility

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



Ping

The Ping menu is used to initiate a ping test.

The screenshot shows the 'Ping' configuration window. It has a title bar 'Ping' and a table with two columns: 'Destination IP' and 'Action'. The 'Destination IP' column has three rows, each with a radio button and a text input field for IP address (format:). The 'Action' column has a 'Run' button.

Destination IP	Action
☒	Run
☐	
☐	

The **[Destination IP]** item is used to enter the destination address of a remote host to check if communication is being established. Enter the target information into the **[Destination IP]** item and click the **[Run]** button. Then, a ping test is executed.

Only one destination IP can be tested of each time and the radio button of the IP to be tested is checked. The radil button of the destination IP on the top is default.

Ping

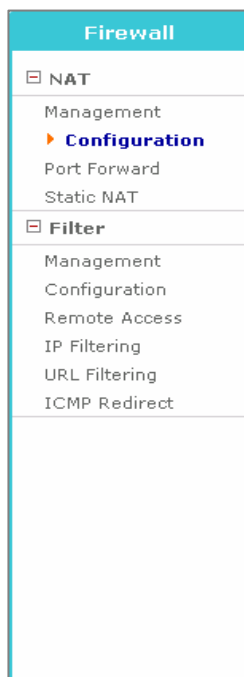
Destination IP					Action
☒	192	168	0	1	Run
☐					
☐					

Log

PING 192.168.0.1 (192.168.0.1) from 192.168.18.100 : 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_seq=1 ttl=64 time=0.279 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=64 time=0.129 ms
64 bytes from 192.168.0.1: icmp_seq=3 ttl=64 time=0.129 ms
--- 192.168.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% loss, time 1998ms
rtt min/avg/max/mdev = 0.129/0.179/0.279/0.070 ms

Firewall Menu

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



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 assignment of a network using private IPs.

Management

The use of NAT is set.

NAT Enable/Disable

Setting
☒ Enable
☐ Disable

OK

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

Configuration

The administrator 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.

Config Mode

☒ Basic Mode

☐ Advanced Mode

Private Network Configuration

Category	Configuration
WAN IP(Intf.)	Not Used
	☐ Dynamic IP PPPoE Ethernet0
Inside	/
Outside	/
Index No.	1

OK

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 administrator to select and set up a port or protocol that is not included to the basic configuration additionally.

Config Mode
Basic Mode
Advanced Mode

Private Network Configuration

Category	Configuration
WAN IP (Intf.):Port	. . . Not Used : ☐ Dynamic IP PPPoE Ethernet0
Inside	. . . /
Outside	. . . /
Port	☒ Define all ☐ User ☒ Range ~ ☐ Multi , , ,
Protocol	all
Index No.	1

OK

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 administrator can view the current status of configuration on Configuration List.

Configuration List

	Setting
☐	No Entry

Delete

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.

Config Mode
☒ Basic Mode
☐ Advanced Mode

Private Network Port Forward

Category	Configuration
Inside IP	. . .
Outside	. . . /
WAN IP	. . . /
Insert	1

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 administrator can select and set up ports or protocols that are not included in the basic configuration additionally.

Config Mode
☐ Basic Mode
☒ Advanced Mode

Private Network Port Forward

Category	Configuration
Inside IP:Port	. . . :
Outside	. . . /
WAN IP	. . . /
Port	☒ Define ☐ User
	☐ Range ~ ☐ Multi , , ,
Protocol	
Insert	1

Category	Description
Port	It is available to set up as only some specific ports are 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

☐

Setting
No Entry

Delete

Static NAT

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

Static NAT

Category	Configuration
Inside IP:Port	, , , : ~
WAN IP:Port	, , , : ~
Protocol	all
Insert	1

OK

Configuration List

☐

Setting
No Entry

Delete

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 administrator can set up the filtering for the traffic forwarding through the system.

Management

Filter Enable/Disable

Setting
☒ Enable
☐ Disable

OK

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

Configuration

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

Basic Mode

Enter the minimum options required for packet filtering.

Config Mode ☒ Basic Mode ☐ Advanced Mode

Filter Configuration

Category	Configuration
Source IP	. . . /
Destination IP	. . . /
Target	Allow

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 administrator to assign additional options for packet filtering.

Config Mode

Basic Mode

Advanced Mode

Filter Configuration

Category	Configuration
Source IP	. . . /
Destination IP	. . . /
Port	☒ Define all ☐ User ☐ Range ~ ☐ Multi , , ,
Protocol	all
Time Set	Days: ☒ Everyday ☒ Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☒ Sat Time: ☒ 24 Hours ☐ : ~ :
Target	Allow
Insert	1

OK

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
No Entry

Delete

Remote Access

Allow or Deny remote access.

Remote Access

Default Policy	
☐ Allow	☒ Deny
Administration IP . . .	
OK	

Remote Access

Default Policy	
☒ Allow	☐ Deny
OK	

Remote IP Configuration

Category	Configuration
Source IP	. . . /
Port	☒ Define all v ☐ User ☐ Range ~ ☐ Multi , , ,
Protocol	all v
Time Set	Days: ☒ Everyday ☒ Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☒ Sat Time: ☒ 24 Hours ☐ 0 v : 0 v ~ 0 v : 0 v
Target	Allow v
Insert	1 v
OK	

Default Policy

- Allow: The basic policy is 'Allow' and the administrator 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

IP Filtering

Category	Configuration
Source IP	. . . /
Destination IP	. . . /
Port	☒ Define all ☐ User ☐ Range ~ ☐ Multi , , ,
Protocol	all
Time Set	Days: ☒ Everyday ☒ Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☒ Sat Time: ☒ 24 Hours ☐ : : ~ : :
Insert	1

OK

Configuration List

Setting
No Entry

Delete

URL Filtering

Administrator can deny web access to PCs connected to the system.

URL Filtering

Category	IP
Source IP	. . . /
Key Word	
Time Set	Days: ☒ Everyday ☒ Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☒ Sat Time: ☒ 24 Hours ☐ : : ~ : :

OK

Configuration List

Setting
No Entry

Delete

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

Administrators 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	☐ Enable	☒ Disable
Ethernet1	☐ Enable	☒ Disable
Ethernet2	☐ Enable	☒ Disable

OK

Router

Select the **[Router]** menu. The submenus will be 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.

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 neighbour 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
Refresh		

Item	Description
Type	- C: Network directly connected to GWIM network interface - S: Static network set by a administrator - 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	On
OSPF	Start	On
BGP	Start	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

ip route 100.0.0.0/24 192.168.0.1

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 *>	200.0.1.0/24	[1/0] via 192.168.18.200, 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..

Help

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

Current Status

Displays the current static table from the GWIM.

Displayed information is identical to **[Router] → [General] → [Routes]**.

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

RIP

[Configuration] → [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]**.

RIP

Command

OK

Help

Select the Argument corresponding to the RIP command.
Clicking the **[Argument]** item displays all arguments corresponding to the command.

Help

Command	Argument
default-information	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	☐ 1 ☒ 2 (default)
redistribute	☐ connected ☐ static ☐ ospf ☐ bgp
network	. . . /

OK

Displays the command configuration currently entered.

Current Status

Router RIP

router rip
network 192.165.0.0/24
redistribute static

Delete

RIP Interface

[Configuration] → [RIP Interface]

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

RIP Interface

Interface	Command
eth0	

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.

Help

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.

RIP Interface Basic

Command	Argument
receive version	☐ 1 ☐ 2
send version	☐ 1 ☐ 2

OK

Displays the command configuration currently entered.

Current Status

Router RIP Interface eth0
No Entry

OSPF

[Configuration] → [OSPF]

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

OSPF

Command

OK

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.

Help

Command	Argument
area	(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.

OSPF Basic

Command	Argument
redistribute	☐ connected ☐ static ☐ rip ☐ bgp
network	. . . / area ID

OK

Displays the command configuration currently entered.

Current Status

Router OSPF

No Entry

Delete

OSPF Interface

[Configuration] → [OSPF Interface]

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.

Help

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

OSPF Interface Basic

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

OSPF Interface Basic

Command	Argument
cost	<1-65535> Cost
dead-interval	<1-65535> Seconds
hello-interval	<1-65535> Seconds
transmit-delay	<1-65535> Seconds
retransmit-interval	<1-65535> Seconds

OK

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.

BGP

Command
network 100.0.0.0/24

OK

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:

Current Status

Router BGP

router bgp 100

network 100.0.0.0/24

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.

Help

Command	Argument
address-family	{A,B,C,D WORD} activate

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	
neighbor	. . . remote ☐ ebgp-multihop ☐ next-hop-self
network	. . . /
redistribute	☐ connected ☐ static ☐ rip ☐ ospf

OK

Current Status

Display the configuration information related with BGP of GWIM. Click the **[Delete]** button to delete all configuration information.

Current Status

Router BGP

router bgp 100
network 100.0.0.0/24

Delete

List

Access List

[List] → [Access List]

Access List

Option	Parameter
ID	Word test
Action	☒ Permit ☐ Deny
Source Match	☐ any ☒ Network 100 0 0 0 / 24
Exact match	☒ Exact match

OK

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
Exact 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 results are 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.

Current Status

	ID	Entry
☒	test	permit 100.0.0.0/24 exact-match

Delete

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 **[OK]** button.

Prefix List

Option	Parameter
ID	
Seq	
Action	☒ Permit ☐ Deny
Prefix Match	☒ Any ☐ . . . / ge: le:

OK

Item	Description
ID	Sets the prefix-list name.
Seq	Sets the sequence No. of the prefix-list.
Action	Allows/Rejects the packets matched.
Prefix Match	Sets the match condition. - Any: All packets - Network: network range. .

If the entered command is successfully executed, the execution results are 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

Delete

Delete All

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

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

Route-Map

[List] → [Route-Map]

Enter the target value and click the **[OK]** button.

Route-Map

Option	Parameter
Name	test
Action	☒ Permit ☐ Deny
Sequence	1

OK

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 results are 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
☒	test	permit 10

Edit

Delete

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 **[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
☐ IP	☒ Address ☐ Use prefix-list ☐ Next-hop ☐ Use prefix-list
☐ Metric	

OK

Set

Option	Parameter
☐ IP	Next-hop . . .
☐ Metric	
☐ Weight	
☐ Community	
☐ Metric-Type	Type-1
☐ Local Preference	

OK

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

Set options are as follows:

Item	Description
IP	Sets next-hop of the BGP table.
Metric	Sets metric of the BGP table.
Weight	Sets weight of the BGP table.
Community	Sets community of the BGP table.

Item	Description
Metric-Type	Sets metric type of the BGP 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
☐	10	match ip address test
☐	10	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.

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	test
Action	☒ Permit ☐ Deny
Match	100\$

OK

Item	Description
ID	Sets AS Path access-list name.

Item	Description
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 results are 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
☒	test	permit 100\$

Delete
Delete All

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

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

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	test
Action	☒ Expanded ☐ Standard
Match	☒ Permit ☐ Deny
	☐
	☒ No-Advertise

OK

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 results are 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:

Current Status

	ID	Entry
☒	expanded test	permit no-advertise

Delete
Delete All

Item	Description
ID	Community list name
Entry	Community list information

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
<button>Refresh</button>						

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
<button>Refresh</button>					

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.
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 administrator
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

Item	Description
OutQ	Number of messages sent to neighbor
Up/Down	Displays the path time when BGP session is finished. Displays the 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

Refresh

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.
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. The submenus will be 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 shown 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					
Clear 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 run 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
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 commands can be entered and executed. Enter the target command into the input field and click the **[OK]** button. Then, the command is executed.

IGMP

Command

OK

Help

Command	Argument
clear ip igmp	group

IGMP Basic

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

IGMP Basic

Command	Argument
Interface	☒ All ☐ eth0 (192.168.17.100/16)
IGMP Query Interval	125 (1~65535, Default: 125)
Max Response Time	10 (1~25, Default: 10)

OK

- 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 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

Refresh

- 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.

DVMRP & Help

Enter a command into DVMRP field and click the **[OK]** button to execute the command.

DVMRP

Command

OK

Help

Command	Argument
clear ip dvmrp	route A.B.C.D/M

DVMRP Routes

This menu is used to display DVMRP Route items in use.

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
Refresh						

- Source Network: VIF network address to which multicast packets flow
- Flags: DVMRP route feature flag. N=New, D=Direct Connected, H=Hold down
- 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	eth0 (192.168.17.100/16)
Reject Non-pruners	☐ (do not allow old version DVMRP neighbors)
Metric	1 (1~31)
Add	

- 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
☐	rd2	100.1.2.10/24	BCAST	1	N/A
☐	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

Enter the target command into the input field of PIM-SM and click the **[OK]** button.

PIM-SM

Command

Help

Command	Argument
clear ip pim	sparse-mode bsr rp-set *

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. Mark the check box of the target item and click the **[Delete]** button.

PIM-SM Basic

	Command	Argument
☒	RP Address	192 168 17 100
☒	RP Candidate	eth0 22 Priority(0~255)
☒	BSR Candidate	eth0 30 MaskLen(0~32) 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.(Low 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.

BootStrap Information

BootStrap Information

PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
BSR address: 192.168.0.99
Uptime: 00:00:04, BSR Priority: 100, Hash mask length: 30
Expires: 00:02:06
Role: Candidate BSR
State: Pending BSR

Candidate RP: 192.168.0.99(eth0)
Advertisement interval 60 seconds
Next Cand_RP_advertisement in 00:00:58

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: 192.168.0.99

Info source: 192.168.0.99, via bootstrap, priority 22

Uptime: 00:00:02, expires: 00:02:28

Group(s): 224.0.0.0/4, Static

RP: 192.168.17.100

Uptime: 00:00:38

Refresh

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	eth0 (192.168.17.100/16)
Mode	Sparse
DR Priority	1 (0~4294967294)
Hello Interval	30 (1~65535)

Add

- 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
☐	rd2	100.1.2.10/24	Sparse	0	1	100.1.2.10	30/105
☐	rd3	100.1.3.10/24	Sparse	0	1	100.1.3.10	30/105
<button>Delete</button><button>Refresh</button>							

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
<button>Refresh</button>				

- 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
<button>Refresh</button>			

- 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						
Refresh						

- 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

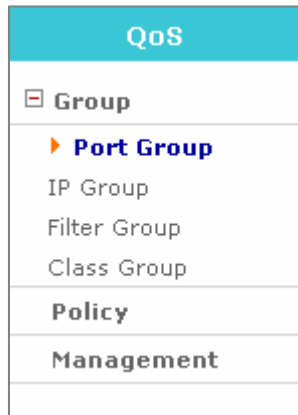
This menu is used to display the neighbor list of PIM-SM protocol.

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

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



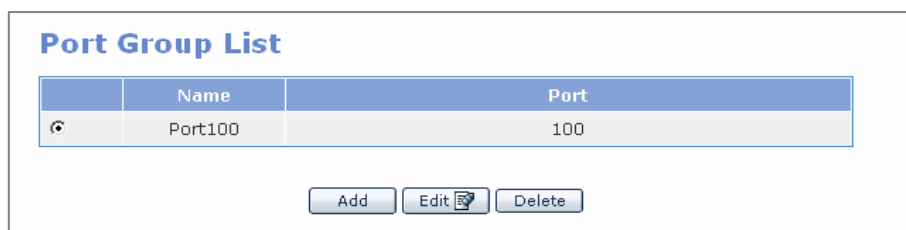
Menu	Submenu	Description
Group	Port Group	Retrieves, sets, edits, or deletes a port group
	IP Group	Retrieves, sets, edits, or deletes an IP group
	Filter Group	Retrieves, sets, edits, or deletes a filter group
	Class Group	Retrieves, sets, edits, or deletes a class group
Policy	-	Sets a class for a 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.



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	VoIP
Port	☐ 10000 ~ 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	Develope_Team
IP	☐ 192 . 168 . 0 . 0 / 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
☒	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.

Filter Group

Category	Value
ID	
Network Protocol	IP
Priority	1
Transport Protocol	any
TOS	☒ DEC ☐ HEX 0x
Source IP:Port	any : any
Destination IP:Port	any : any

Filter means a configuration filtering for the values in the packet header. Values set in **[QoS] → [Group] → [Port Group]** and **[IP Group]** are used. 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
☒	spq_leaf	leaf			
Filter	dev_voip				
☐	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	☐ root ☒ 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	leaf
Class Type	☒ root ☐ leaf
High	none
Middle	none spq_leaf
Low	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.



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	Cell	Burst	Cburst
☒	root	root				10 Mbps			
☐	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	root
Class Type	☒ root ☐ general ☐ non-leaf ☐ leaf
Rate	10 Mbps
Burst	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	general
Class Type	☐ root ☒ general ☐ non-leaf ☐ leaf
Parent ID	root
Priority	1
Rate	10 Mbps
Ceil	Bps
Burst	Byte
CBurst	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	general
Class Type	☐ root ☐ general ☒ non-leaf ☐ leaf
Parent ID	root
Priority	1
Rate	10 Mbps
Ceil	Bps
Burst	Byte
CBurst	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	
Class Type	☐ root ☐ general ☐ non-leaf ☒ leaf
Parent ID	none
Priority	1
Rate	Bps
Ceil	Bps
Burst	Byte
CBurst	Byte
Leaf Qdisc	none Attach on Leaf class!

Filter Apply

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

Time Setting

Scheduling Parameter 0							
☐	☐ Sun	☐ Mon	☐ Tue	☐ Wen	☐ Thu	☐ Fri	☐ Sat
	Start Time 00 Hour		End Time 00 Hour				
	Rate Bps		Ceil Bps				
	Burst Byte		Cburst Byte				
Add Delete OK Cancel							

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.

Item	Description
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	WAN1
QDISC Type	☐ SPQ ☒ HTB
R2Q	
Root Class	none
Default Class	none

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

Save

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 stop the execution of the 'Scheduling Parameter' set in **[QoS] → [Group] → [Class Group]**.

QoS Management

Activity	Action Type	Time Check	Action
Stop	start	☐ on/off	Run

Status

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

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 an 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

Refresh

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	☐
Free Memory	☐

Ethernet Interface	Selection Check
Ethernet 0	☐
Ethernet 1	☐
Ethernet 2	☐

OK

Services

This menu is used to display the status 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)	Stop
SIP ALG (Session Initiation Protocol)	Stop
NTP (Network Time Protocol)	Stop
DHCP (Dynamic Host Configuration Protocol)	Stop
SSH (Secure Shell)	Running
Telnet	Running
FTP (File Transfer Protocol)	Stop

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

VPN
IPSec Configuration Certificate Management
L2TP Configuration Management
PPTP Configuration Management
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 7400 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.



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 administrator 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

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
Connection ID	xxxx	
IP	192.168.18.100	211 217 127 72
Router IP	192 168 17 1	211 217 127 1
Subnet IP	100.0.0.0	200 0 0 0
Subnet Mask	255 255 255 0	255 255 255 0

Authentication Method

☒ Preshared	☐ RSA	☐ Certificate
Password 		
Re-password 		

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	Selects host authentication method - 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	Main
Encryption-Hash Algorithm	3des-sha1
Key Life Time	3600 sec
Phase 2	
Protocol	esp
Encryption-Hash Algorithm	3des-sha1
Key Life Time	28000 sec
Dead Peer Detect	
Time Out	120 sec
Delay	30 sec
Action	hold
Advance	
Negotiation Count	0
Perfect Forward Secrecy	DH-Group5
Rekey	yes
Connection	Initiator
Ipssec/L2tp	☐

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, AES128-MD5, AES128-SHA1, AES192-MD5, AES192-SHA1, AES256-MD5, AES256-SHA1
	Key life time	IKE Duration If Key life time is passed, the host authentication (the phase one IKE) is performed again.
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, AES128-MD5, AES128-SHA1, AES192-MD5, AES192-SHA1, AES256-MD5, AES256-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	IPSec Connection Attempt - initiator: Attempting a connection - response: Attempt to receive a connection
	IPSec/I2tp	Sets when IPSec over I2tpis is used. (Supports Window XP SP 2.)
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 administrator 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
Running	Stop

RSA	Action
Create the new RSA key	OK
Download the current RSA key	Download

External Device	Action
☒ eth0	OK

Click the **[OK]** button on 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 in the **[External Device]** items to apply the IPsec connection to the device.

Certificate

The administrator 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
☐	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	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)	
State	
Locality	
Organization	
Organization Unit	
Common	
Email	
Password	
Confirm Password	

Each item of the 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

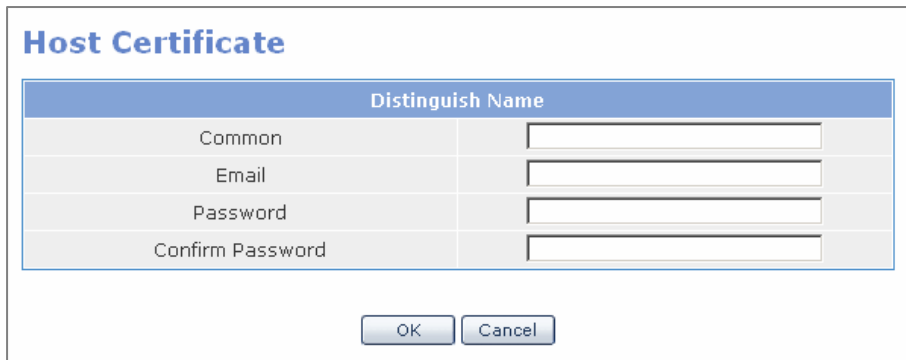


The dialog box titled "External CA Certificate" contains a section labeled "Upload". Inside this section, there is a label "CA Certificate" followed by a text input field and a "Browse..." button. Below the "Upload" section, there are two buttons: "OK" and "Cancel".

The uploaded items of an external certificate are defined as follows:

Item	Description
CA Certificate	External certificate upload

Host Certificate



The dialog box titled "Host Certificate" contains a table with the heading "Distinguish Name". The table has four rows: "Common", "Email", "Password", and "Confirm Password". Each row has a corresponding text input field. Below the table, there are two buttons: "OK" and "Cancel".

The uploaded items of the external certificate are defined as follows:

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

L2TP

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

Configuration

In the **[L2TP] → [Configuration]** menu, the administrator 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 administrator
Delete	Delete a PPTP administrator
Edit	Modify a PPTP administrator information

Add

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

User Add

User Info	
ID	
Password	
Confirm Password	
☒ Auto IP Allocation	
☐ Static IP Allocation	. . .

Item	Description
Administrator 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 <**Administrator 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	11
Password	••
Confirm Password	••
☒ Auto IP Allocation	
☐ Static IP Allocation	. . .

Management

In the **[L2TP] → [Management]** menu, the administrator 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	Run

Type	Range	Setting
Local IP	192 . 168 . 254 . 95	Save
Remote IP	192 . 168 . 254 . 97 - 98	
Method	pap	

The administrator 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 demon 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 administrator 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 administrator can apply the VPN function easily.

Configuration

On the **[PPTP] → [Configuration]** menu, the administrator can create, modify, delete, and retrieve 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 administrator
Delete	Delete a PPTP administrator
Edit	Modify PPTP administrator information

Add

[Add] → <PPTP administrator list>

User Add

User Info	
ID	
Password	
Confirm Password	
☒ Auto IP Allocation	
☐ Static IP Allocation	. . .

Item	Description
Administrator 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

[Edit] → <Administrator List>

User Mod

User Info	
ID	11
Password	••
Confirm Password	••
☒ Auto IP Allocation	
☐ Static IP Allocation	

Management

In the [PPTP] → [Management] menu, the administrator 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	Run

Type	Range	Setting
Local IP	192 168 0 234 - 238	Save
Remote IP	192 168 1 234 - 238	

The administrator 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 demon responsible for remote client in the 'Remote IP range' item. The encryption method supports 'pap' and 'chap'.



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

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 the IPsec tunnel set up in **[STATUS] → [IPsec]** to insure it is properly connected.

Check the L2TP/PPTP tunnel set up in **[STATUS] → [L2TP/PPTP]** to insure it 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. The submenus will be displayed in the upper left side of the window as follows:

IDS
 IDS Config
 Log Analysis
Configuration
Rule Config
Mail Config
Block Config
Management

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 administrator 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
☒	Intrusion Type	Alert summary by intrusion type
☐	Source IP	Alert summary by source IP
☐	Destination IP	Alert summary by destination IP
☐	Destination Port	Alert summary by destination port
☐	Port Scan	Port scan summary

OK

Search Log

	Category	Condition
☐	Priority	All
☐	Source IP	All
☐	Destination IP	All
☐	Destination Port	All

OK

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

Port scan summary
Thu Jan 1 00:00:00 1970 ~ Tue Feb 7 10:59:50 2006

Ports	Hosts	Remote hosts
There is no alert		

Prev.

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 administrator can search by condition

Search Log

	Category	Condition
☒	Priority	All
☐	Source IP	All
☐	Destination IP	All
☐	Destination Port	All

OK

If selecting the category including the desired condition, the selection box is activated. Then the administrator 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





CHECK

Selecting Search Condition

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

Configuration

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

Select Device

The administrator 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 administrator can select a check box as the check box is activated.

Select Device		
☒ Ethernet0	☐ Ethernet1	☐ Ethernet2
OK		

Set Detection Level & Type

The intrusion type is classified into High, Medium and Low according to the risk level. The administrator can set up the intrusion detection level as alert is generated when an intrusion exceeding the level occurs. In addition, the administrator 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 a configured time.

(Refer to 'Block Config')

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

(Refer to 'Mail Config')

☒ High	☒ Medium	☒ Low
☐ Block	☐ Block	☐ Block
☒ Mail	☒ Mail	☒ Mail

OK

IDS Rule Configuration

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

IDS Rule Configuration

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

Pressing the **[OK]** button after selecting the desired rule activates all of the selected rule sets.

By checking the check box on the top of each column, all rules in the relevant column will be selected. Click the **[Default]** button to select the default rules.

Rule Config

The administrator 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



NOTE

Th administrator can manully update the rule set by clicking the "Browse" button and selecting a new "Rule-Set" to upload.

Mail Config

Set SMTP Server IP

The administrator 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
. . .	25

Set Mail Address

Set Time for Sending Mail

The administrator can set up the time to send an email.

Set Time for Sending Mail

Category	Configuration	Set
Now	Send Mail Now	OK
One Time	Day : 1 Hour : 1	OK
One Time		
Daily		
Weekly		
Monthly		
Not use		

If clicking the button in the Now category, an email is sent 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

If you are not receiving an email verify the SMTP Server IP or retrieve the IDS log in System → Log. If there is no recorded alert, an email was not sent.

Block Config

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

Manage Blocked IP List

Blocked IP List

Manage Trusted IP List

Trusted IP List	Netmask
. . .	255 . 255 . 255 .

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 administrator 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 administrator can set up the operation of the IDS module and block module.

IDS Management

Status	Action
Stop	Run

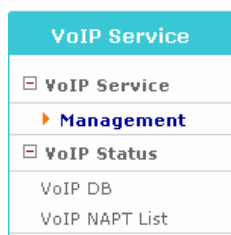
Block Management

Status	Block time	Action
Stop	10800 sec	Run

Item	Description
Status	- 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 a configured time. After the configured time, the IP is released from the block list and can access to the system.

VoIP Service Menu

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



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

Management

The **[Management]** menu is used to enable or disable the VoIP service.

VoIP Service Management	
Activity	Action
Running	<button>Stop</button>
Item	Description
Activity	Current VoIP service status
Action	Command that currently can be executed

WAN interface can be selected. Last setting is restored even if the system reboots. When the information on the selected WAN interface is changed, WAN interface is automatically set.

VoIP NAPT Management				
	Category	Usage	Protocol	IP
☐	eth0	EXTERNAL	STATIC	192.168.18.100
☐	eth1	INT_PRIV	STATIC	10.0.0.1
☐	eth2	EXTERNAL	STATIC	20.0.0.2
☒	Serial0	EXTERNAL	Cisco-HDLC	22.0.0.2
☐	Serial1	-	-	-
<button>OK</button><button>Refresh</button>				

Item	Description
Category	Interface
Usage	Type of each interface
Protocol	Protocol type of each interface
IP	IP of each interface

VoIP DB

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

VoIP Database

Call Server	Status	IP	MAC Address
MCP	Connected	165.213.176.10	00.00.f0.ff.74.49

MGI Cabinet	Slots	Status	IP	MAC Address
-------------	-------	--------	----	-------------

ITP Index	Status	IP	TEL NUM	MAC Address
-----------	--------	----	---------	-------------

WIP Index	Status	IP	TEL NUM	MAC Address
-----------	--------	----	---------	-------------

Refresh

Item	Description
Call Server	Displays the type of call server(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
ITP Index	Displays the index of ITP Phone
WIP Index	Displays the index of WIP Phone
Port	Displays the port of ITP/WIP Phone
TEL NUM	Displays the phone number of ITP/WIP Phone

VoIP NAPT List

VoIP NAPT Status displays NAPT items for VoIP communication on the **[VoIP NAPT List]** 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. The submenus will be displayed in the upper left side of the window as follows:

SIP ALG
Config
Management

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



NOTE

SIP ALG(SIP aware ALG)

Typically, if a firewall protects internal network based on NAT such as the GWIM module 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 administrator 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:

SIP IP Configuration	
External IP	192.168.17.100
Internal IP	192.168.17.100 100.0.0.10

Map LIST

Enter SIP devices data inside of the firewall.

Map List		
☐	Number(ID)	IP
	default	10.0.0.10
		Default
Add Delete		

If a IP address or phone number is not entered, 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.

MAP		
	ID	IP
☐	default	10 . 0 . 0 . 10
☐		. . .
Add Delete		

Clicking the **[Add]** button will allow you to add additional Map information.

MAP					
	ID	IP			
☐	default	10	0	0	10
☒	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.

SIP ALG Management	
Activity	Action
Stop	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

System Menu

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

System
DB Config
Admin Config
Log
Configuration
Report
Download
DHCP Server
Configuration
Management
Lease Info
DHCP Relay Agent
Configuration
Management
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

[DB Config]

Configuration System DB

Select	Type	Description
☒	Import	Browse...
☐	Export	Export the current system db.
☐	Default	Change the current system db to default system db.

OK

Item	Description
Import	Restore a previously saved database
Export	Saves the existing DB
Default	Restore the DB to factory defaults

After defaulting the DB the administrator should access the web manager using one of the default IP addresses such as 10.0.4.1 through the LAN port.

Admin Config

This function sets up the authentication server of the system login. It sets up the Local, Radius and Taccas+ authentication server. Select the target authentication method and click the **[OK]** button. Then, the setting is applied and the setting page for the selected authentication method is displayed.

Login Policy

Category	Value
Set Policy	☒ Local ☐ Radius ☐ Taccas+

OK Cancel

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	
Confirm New Password	

OK

Radius

Enter the information on the Radius authentication server. Up to 5 lists can be entered.

Radius

Radius Server IP	Radius Server Key	Time out

Taccas+

Enter the information on the Taccas+ authentication. Up to 5 lists can be entered or deleted. When deleting the list of all server IPs, the corresponding secret key values are also deleted.

Taccas+

Taccas+ Server

Taccas+ Secret Key

Log

This page allows setting up the system log and retrieving the log 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 ☐	OFF ☒
NETWORK	ON ☐	OFF ☒
FIREWALL	ON ☐	OFF ☒
PPTP	ON ☒	OFF ☐
IPsec	ON ☒	OFF ☐
L2TP	ON ☒	OFF ☐

Select added logs from the logs for system log, network, firewall, VPN, 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 administrator can retrieve the logs stored in the system according to an item and time.

Report Policy

Advanced Service					
Log Type	ALL ☒	SYSTEM ☐	NETWORK ☐	FIREWALL ☐	
	PPTP ☐	L2TP ☐	IPSEC ☐	IDS ☐	

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

Set up the desired log type and time and click the **[OK]** button to verify the log. 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

Download

This page allows downloading the system log 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.

Download

DHCP Server

[System] → [DHCP Server].

Configuration

The **[Configuration]** menu allows setting of various configuration items in the DHCP Server.
Pool Name, Network Address and Range Address are all required fields in DHCP Server configuration.

General Options

Parameter	Argument
* Pool Name	
* Network Address	. . . /
* Range Address	. . . ~ . . .
Lease Time	▼ Days ▼ Hours ▼ Minutes ☐ Infinite
Group Number	
Client ID	
Vendor ID	
Domain Name	
Default-Router	. . .
Fixed Address	Host
	MAC : : : : :
	IP . . .
DNS Server	1) . . . 2) . . .
WINS Server	1) . . . 2) . . .

Save Cancel

Current Running Configured Information

Select	Parameter	Argument
No Entry		

Edit Delete Refresh

The configuration options are 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 are used for allocating a fixed IP address for a specific client.

Press the Delete button after checking the target Pool in order to delete. Check the target pool and click the **[Edit]** button for modification.

Management

This page allows managing the operation of DHCP Server.

DHCP Server Management

Status	Action
Stop	<button>Run</button>

Lease Info

The Lease Info window shows the active Lease information.

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. If pressing the **[Delete]** button on the list, the interface is deleted.

To save the list of DHCP Server, enter the IP address that the DHCP Server is using and click the **[Add]** button.

Interface List Configuration

Check	Argument
	ETH eth0

Check	Server List	Server
	Server List	

Management

This page starts/stops the DHCP daemon.

DHCP Relay Agent Management

Status	Action
Stop	Run

Time Configuration

Synchronize the date and time of the system on the **[Time Configuration]** menu of the **[System]** through a network or manual configuration.

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.

The 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 demon to register Time Server.

NTP Configuration

Current Time

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

NTP Server Status

Status
stop

Time Server

Server 1	
Server 2	

- 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.)

Manual Config

The administrator can set and modify the date and time of the system to the time that the administrator 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 administrator can change Time Zone by selecting the timezone corresponding to the administrator 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 administrator's PC.

The image shows two stacked dialog boxes. The top one is titled 'Select Package Upgraded' and contains a table with four columns: 'Package Version', 'Current Version', 'Released Date', and 'Upgraded Date'. The 'Current Version' is 'v0.19', 'Released Date' is '2005.09.21', and 'Upgraded Date' is '2005.09.21'. There is an empty input field under 'Package Version'. The bottom dialog box is titled 'Select Upgrade Method' and contains a table with two columns: 'Upgrade Method' and 'Upgrade Server IP'. Under 'Upgrade Method', there are three radio buttons: 'TFTP' (selected), 'HTTP', and 'Local'. Under 'Upgrade Server IP', there are four input fields for IP address segments, a 'Browse...' button, and an 'OK' button at the bottom.

Package Version	Current Version	Released Date	Upgraded Date
	v0.19	2005.09.21	2005.09.21

Upgrade Method	Upgrade Server IP
☒ TFTP	. . .
☐ HTTP	
☐ Local	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 administrator'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.

The image shows a dialog box titled 'Application Server' containing a table with two columns: the service name and its 'On/Off' status. The services listed are SSH, FTP, and Telnet, all of which have a checked checkbox indicating they are turned on. There is an 'OK' button at the bottom.

	On/Off
SSH	☒
FTP	☒
Telnet	☒

Reboot

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

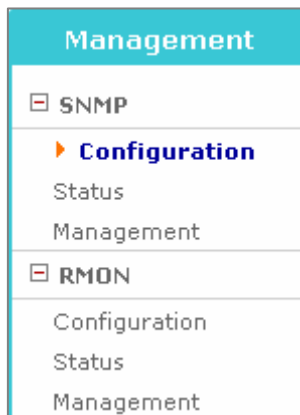


If clicking the **[OK]** button, all services are terminated and the system is rebooted.

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

Management Menu

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



Menu	Submenu	Description
SNMP	Configuration	Displays 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 administrator.

System Option

Set up SNMP System Option.

System Option	
Location	
Contact	
Name	
Engine ID	

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	
Community Network	. . . /
Access	☒ Read Only ☐ 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 Administrator Add

SNMPv3 Administrator Add allows adding an administrator to be used at SNMP v3.

SNMPv3 User Add	
User Name	
User Password	
Authentication	MD5 v
Encryption	None v
Access	☒ Read Only ☐ Read Write

Item	Description
Administrator Name	Fill in new administrator's name to add.
Administrator Password	Fill in new administrator'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	. . .
Community Name	

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 administrator has selected by marking on the check box is deleted. If clicking the **[Reset]** button, all check boxes are initialized.

SNMP Config Information

The administrator 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
☐	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.
Administrator Name	Displays the configured administrator's name.
Access	Displays the access authority of the configured administrator.
Trap IP	Displays the configured Trap IP.
Trap Port	Displays the configured Trap Port.

Management

The administrator 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	Stop

SNMP Management allows the administrator 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

[RMON] → [Configuration]

If clicking the **[Save]** button, the information that is set up by the administrator is applied to the system. If clicking the **[Reset]** button, the information that the administrator is to set up is reset.

History Option		
MAX History Buckets	1000	(50 - 5000)
MIN History Interval	15 min.	(1 - 60)

History Option

History Option allows setting up the RMON history option.

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

Event Options

Even Options allows the administrator to set up the RMON event option.

Event Option	
MAX Event Logs	(50 - 2000)

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

Status

[RMON] → [Status]

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

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

Event Global Status	
MAX Event Logs	400
Saved Event Logs	0

Item	Description
MAX History Buckets	Displays the maximum history storage space that has been set 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.
MIN History Interval	Sets up the minimum history sample collection cycle.
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 administrator 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

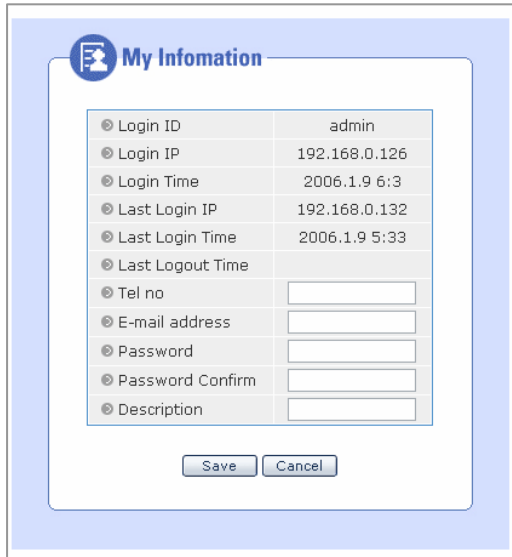
The administrator can start/stop the RMON service.

RMON Management	
Activity	Action
Stop	Run

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

My Info Menu

Click  **My Info** on the upper right of Web to identify the administrator information. Enter the target Tel no, E-mail address, and description into the input fields and click the **[Save]** button. Enter the target password into the Password field and click the **[Save]** button. Then, the login password is modified. Last setting is restored even if the system reboots.



The screenshot shows a web interface titled "My Information" with a user icon. It contains a table of login details and several input fields for user information. At the bottom are "Save" and "Cancel" buttons.

Item	Description
Login ID	admin
Login IP	192.168.0.126
Login Time	2006.1.9 6:3
Last Login IP	192.168.0.132
Last Login Time	2006.1.9 5:33
Last Logout Time	
Tel no	
E-mail address	
Password	
Password Confirm	
Description	

Save Cancel

Item	Description
Login ID	Displays login ID.
Login IP	Displays login IP.
Login Time	Displays time when login occurs.
Last Login IP	Displays last login IP.
Last Login Time	Displays last login time.
Last Logout Time	Displays last logout time.
Tel no	Telephone No.
E-mail address	E-mail address
Password	Password to be modified
Password Confirm	Confirms the password to be modified
Description	Description

ABBREVIATION

A

ALG	Application Level Gateway
AH	Authentication Header
ARP	Address Resolution Protocol
AS	Autonomous System

B

BGP	Border Gateway Protocol
BPDU	Bridge Protocol Data Unit
BSR	Bootstrap Router

C

CHAP	Challenge-Handshake Authentication Protocol
CTI	Computer Telephony Integration

D

DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
DRR	Deficit Round Robin
DSMI	Data Server Module Interface
DVMRP	Distance Vector Multicast Routing Protocol

E

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

G

GWIM	Gigabit WAN Interface Module
GVRP	GARP VLAN Registration Protocol

H

HDLC	High-level Data Link Control
HTTP	Hypertext Transfer Protocol
HTB	Hierarchical Token Bucket

I

IDS	Intrusion Detection System
IGMP	Internet Group Management Protocol
IKE	Internet Key Exchange
IPMC	IP Multicast
IPSec	IP Security Protocol
ISAKMP	Internet Security Association Key Management Protocol

L

LAN	Local Area Network
L2TP	Layer 2 Tunneling Protocol

N

NAT	Network Address Translation
NTP	Network Time Protocol

R

RMON	Realtime Monitoring
RP	Rendezvous Point
RSTP	Rapid Spanning Tree Protocol

P

PAP	Password Authentication Protocol
PIM-SM	Protocol Independent Multicast-Sparse Mode
PD	Power Device
PoE	Power Of 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
SPQ	Strict Priority Queuing

T

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

V

VLAN	Virtual Local Area Network
VoIP	Voice Over IP
VPN	Virtual Private Network