SAMSUNG

Enterprise IP Solutions

OfficeServ 7400

GWIM User Manual

Samsung Telecommunications

Publication Information

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

Trademarks

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

PRINTED IN USA

INTRODUCTION

Purpose

This document introduces the OfficeServ 7400 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

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 folling 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

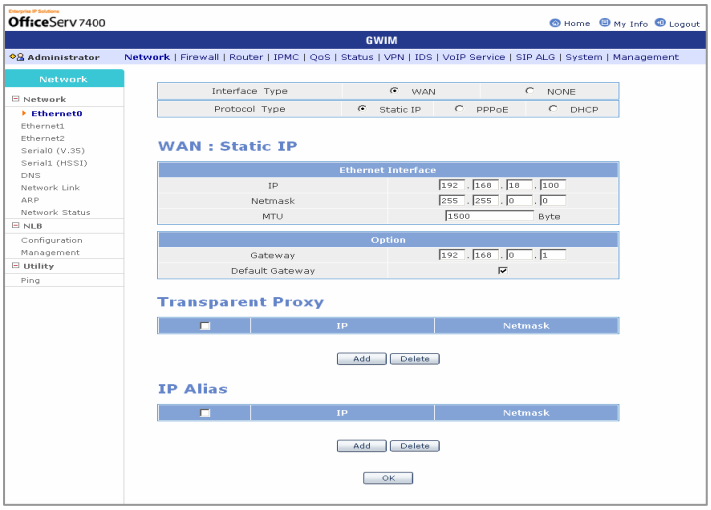
The version of the Internet Explorer should be 6.0 or higher for the maintenance of GWIM. Other web browsers are not supported.

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:

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**".)*



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

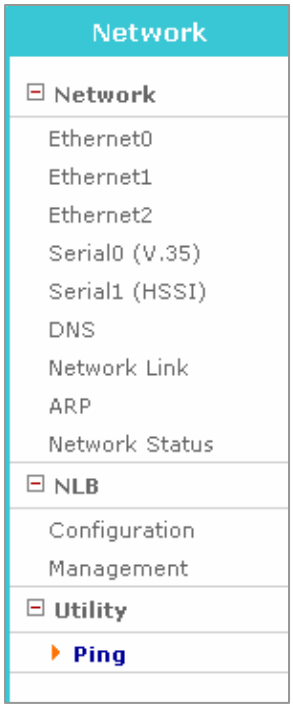
CHAPTER 3. Using OfficeServ 7400 GWIM

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

The configuration of OfficeServ 7400 GWIM menus are as follows:

Network 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

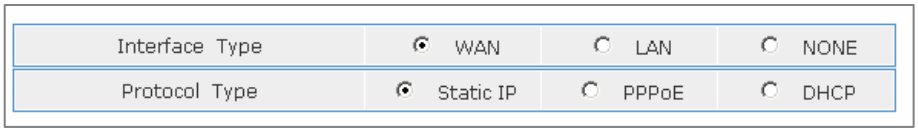
The **[Network]** menu displays the five network interfaces built-in to the GWIM. This menu sets IP information, transfer speed, and transfer mode of each interface. In addition, this menu sets DNS and ARP.

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:

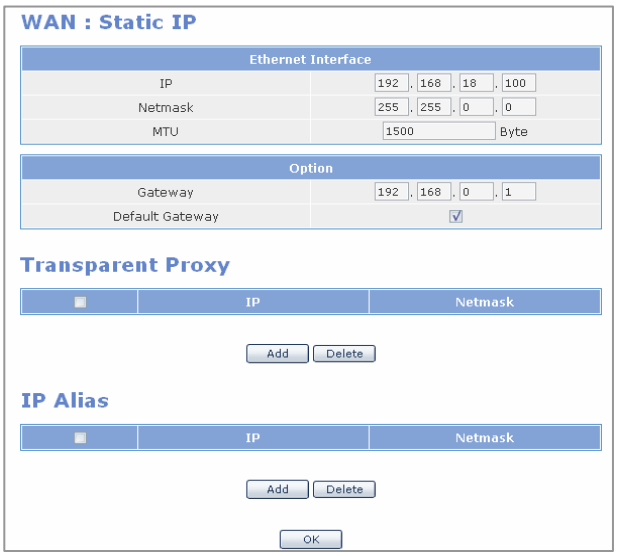


- WAN: The following protocol types can be selected in WAN:
  - Static IP: Select Static IP if your Internet service account uses Fixed IP (Static) IP assignment.
  - PPPoE: Select PPPoE if your Internet service account uses PPP over Ethernet login protocol, such as in ADSL account.
  - DHCP: Select 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

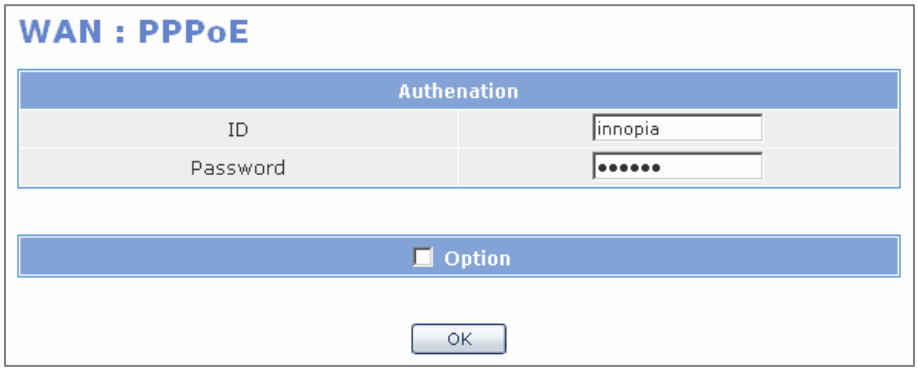
Select the WAN-Static IP category to display the following configuration window: The details by fields are as follows:



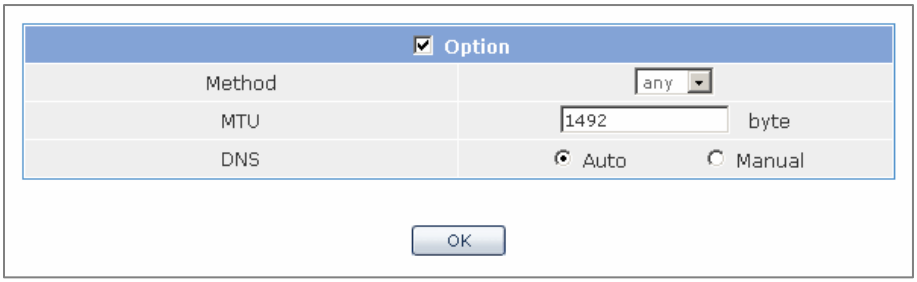
- WAN: Static IP
  - IP: Enter the public IP address assigned to the current network interface.
  - Network: Enter the netmask address of the current network interface.
  - Gateway: Enter the public IP address received from Internet Service Provider or the IP address of a router.
  - Default Gateway: 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.



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



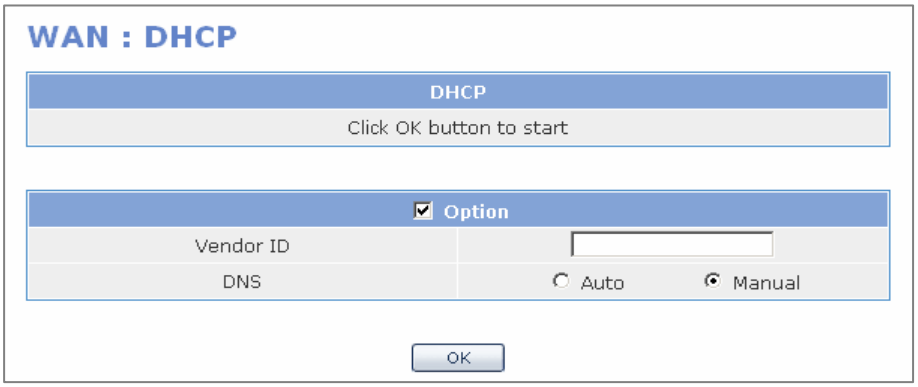
The details by fields are as follows:

- 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

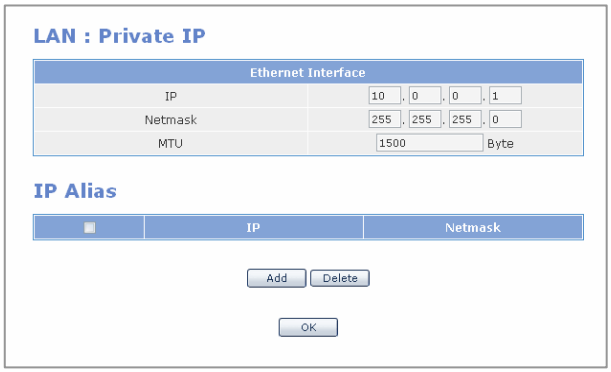
WAN → DHCP field is automatically set without a special setup field. Therefore, press the **[OK]** button to complete the setup.

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]**.



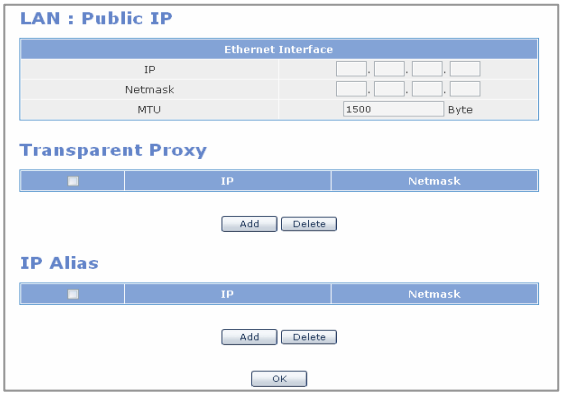
LAN → Private IP

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.



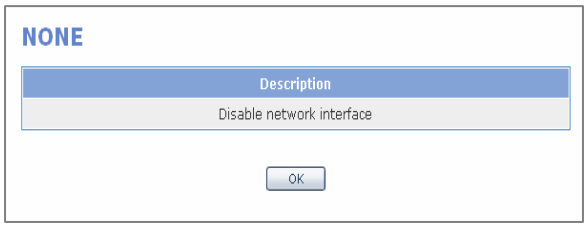
LAN → Public IP

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.



NONE

NONE is selected when the corresponding interface is not used.



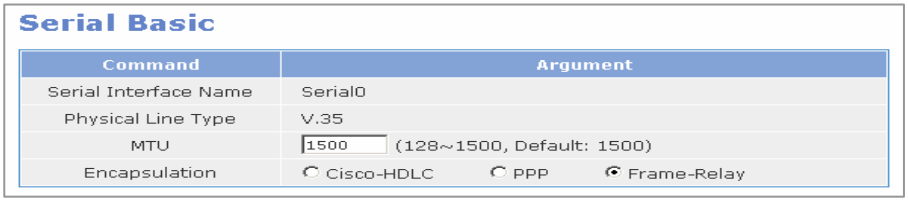
Setup for Serial0 (V.35) and Serial1 (HSSI)

Interface Type

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

Serial Basic

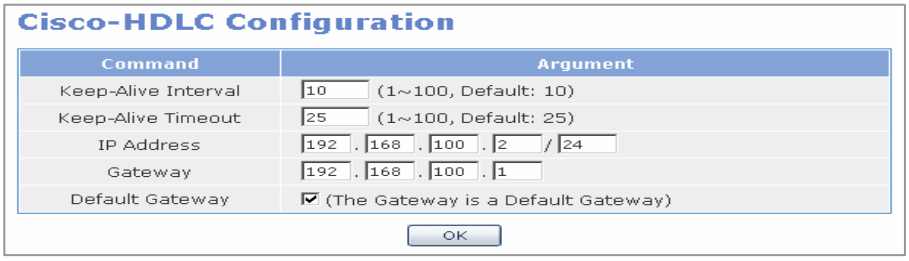
The Serial Basic table sets the basic information of Serial Interface. Select one of the Serial Protocols in the Encapsulation field of this table to display the configuration window.



- Serial 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

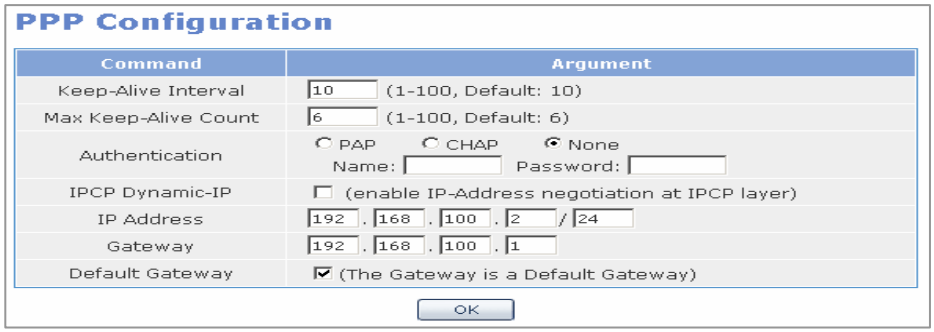
Set the Encapsulation type as Cisco-HDLC to display the Cisco-HDLC Configuration window. Specify the value for each field, and click the **[OK]** button to store the configuration.



- 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

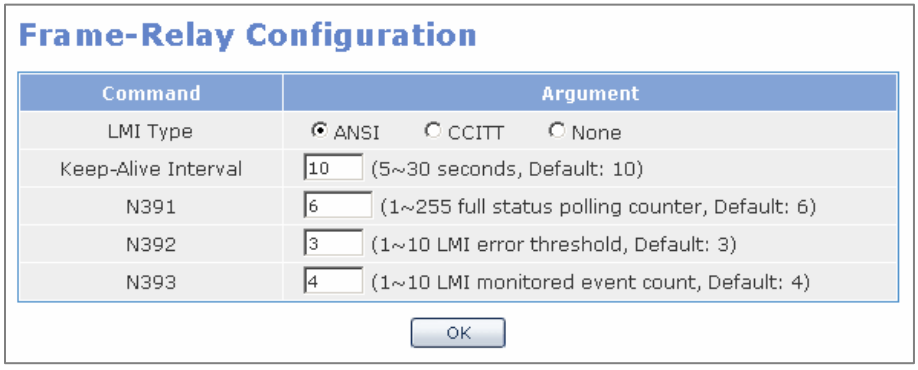
Set the Encapsulation type as PPP Protocol in the Encapsulation field to display the PPP Configuration table. Specify the value for each field, and click the **[OK]** button to store the configuration.



- 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.

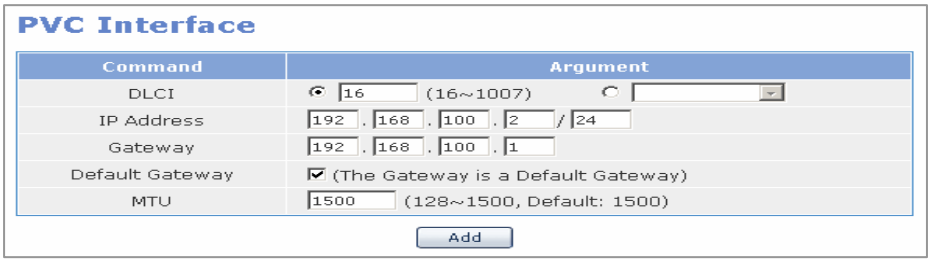


- LMI Type: LMI type of Frame-Relay
- Keep-Alive Interval: Time interval to check Keep-Alive

- 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.

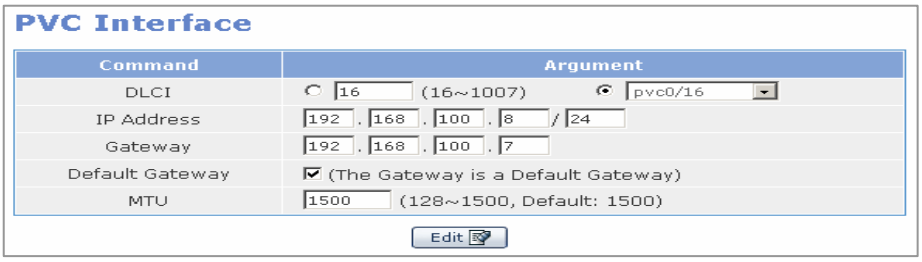
PVC Interface

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.

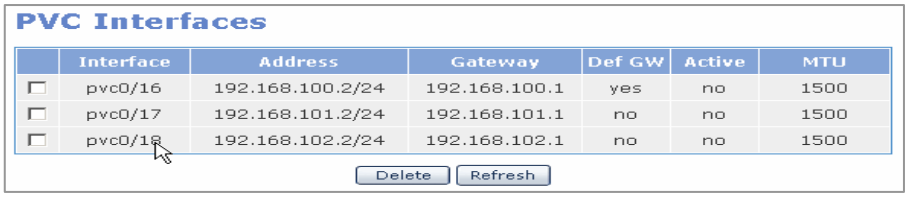


- DLCI: Number of DLCI(a type of network address)
- IP Address: IP Address to be used by PVC
- Gateway: Gateway IP Address(Peer Address) of PVC
- Default Gateway: Mark the check box to set this gateway to default gateway. (This item is displayed if WAN is set.)
- MTU: Maximum size of the packet to transfer 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.

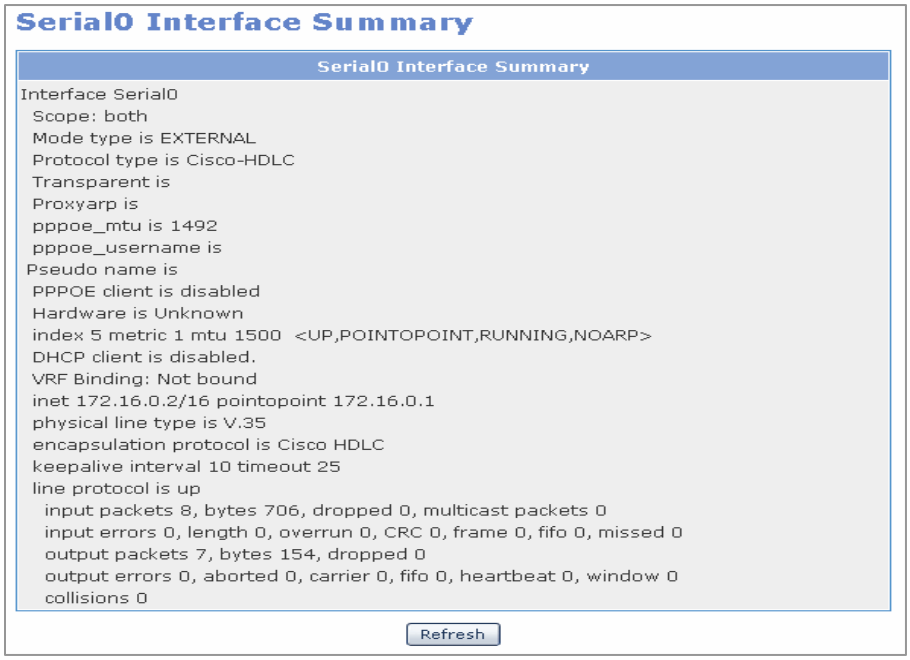


To delete a specific PVC, mark the check box of the corresponding PVC and click the **[Delete]** button.



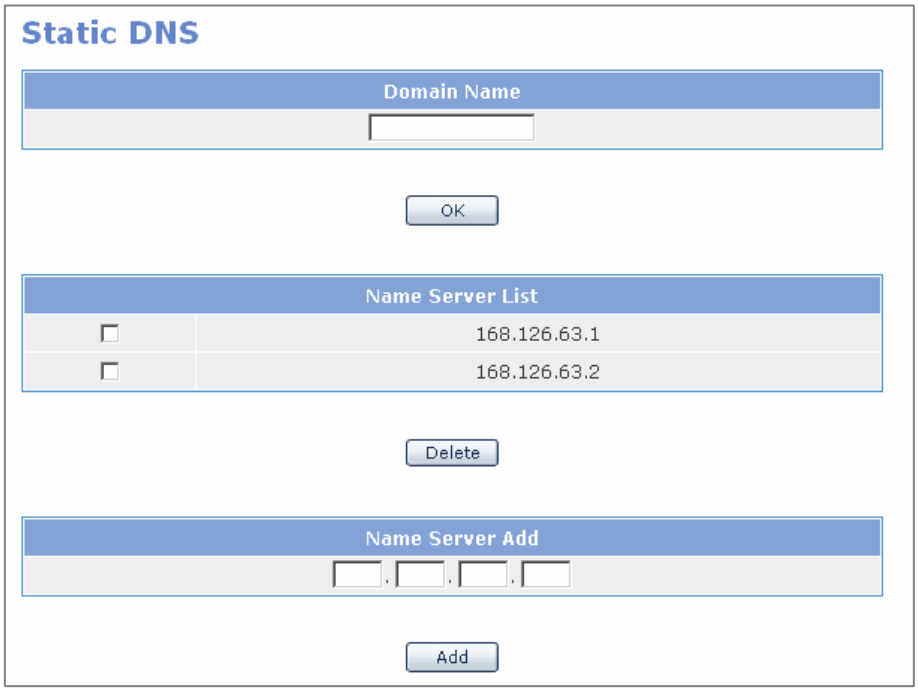
Serial Interface Summary

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.



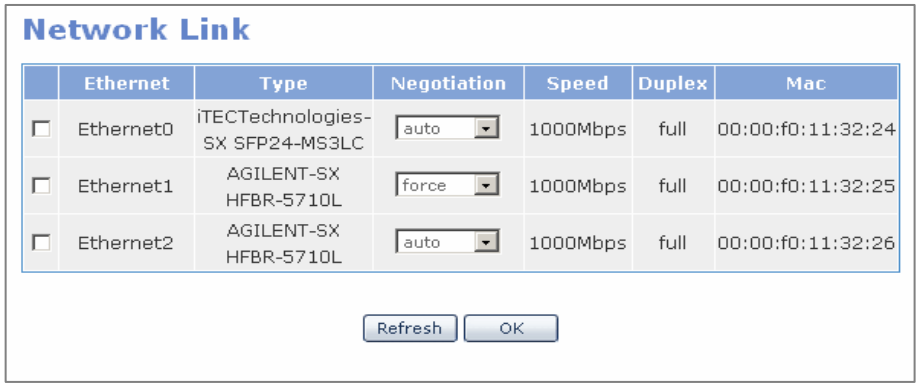
DNS

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.



Network Link

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



- Ethernet: Logical name of each Ethernet port
- Type: Type of Ethernet Cables/SFP GBIC Adapters
- Negotiation: Setup of auto and force modes

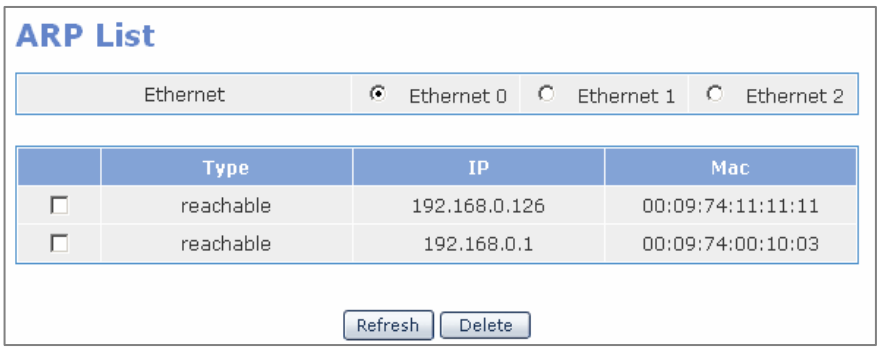
- Speed(Mbps): Transmission bandwidth of the corresponding Ethernet interface
- Duplex: Transfer mode of the corresponding Ethernet interface
- MAC: MAC addresses by Ethernet interfaces

ARP

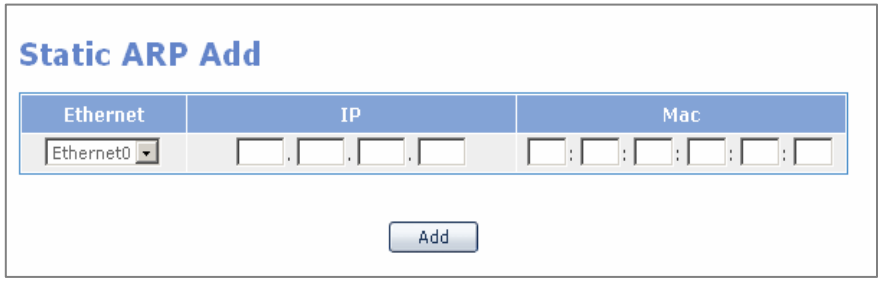
The ARP menu is used for the addition/deletion/management of the ARP information in each Ethernet interface.

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.



- Type: ARP status
- IP: IP address sent ARP
- Mac: Mac address sent ARP



static ARP add

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

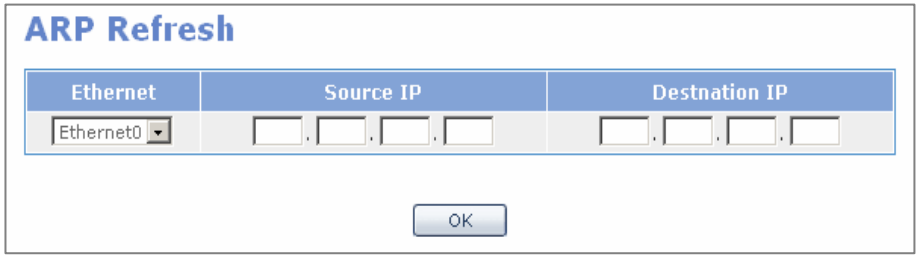
- Ethernet: Ethernet to add static Mac
- IP: IP address to be added
- Mac: Mac to be added

ARP Age Time

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

ARP refresh

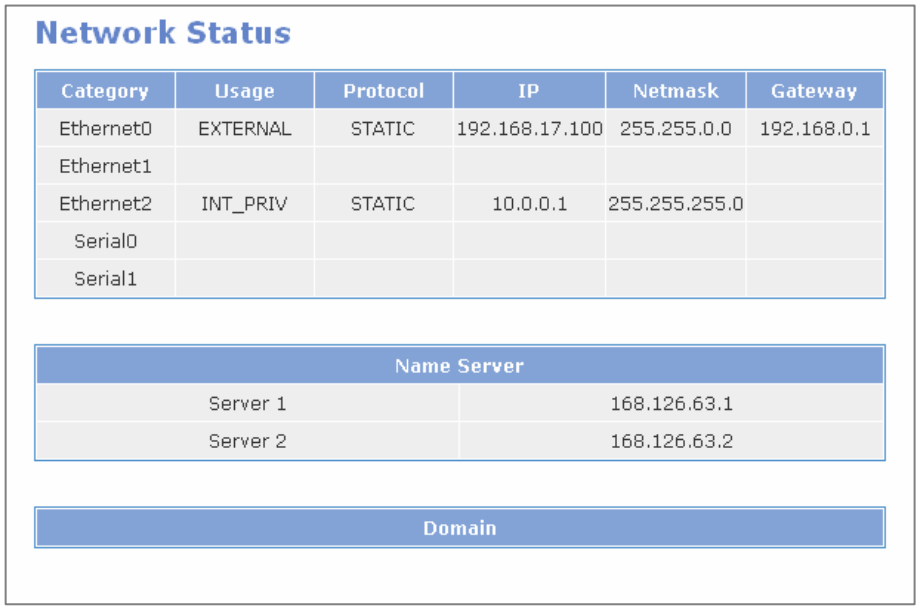
The ARP Refresh window is used for the modification of the changed ARP information in the ARP table of a route or a host when the network is changed. In the host or the route with the destination IP, the Mac with the current source IP is updated into the Ethernet Mac of the OfficeServ 7400 system.



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

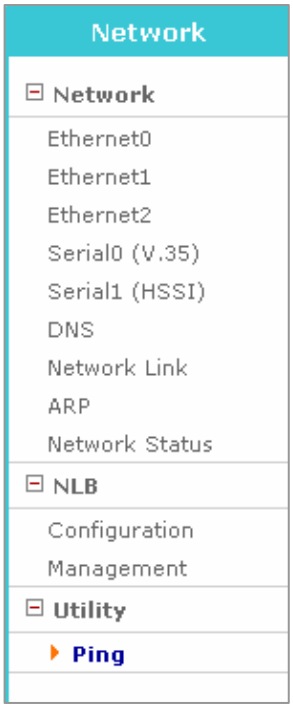
Network Status

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



NLB

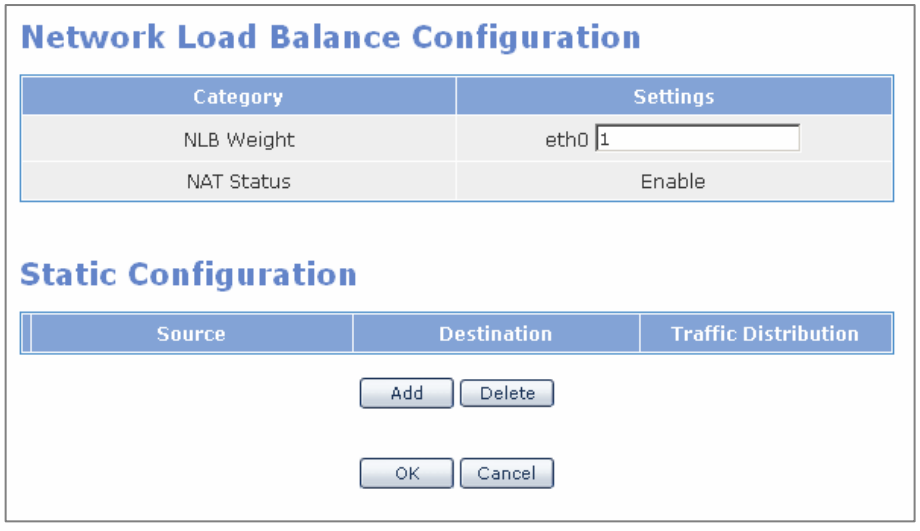
Select the **[Network]** menu. The submenus will be displayed in the upper left side of the window as follows:



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

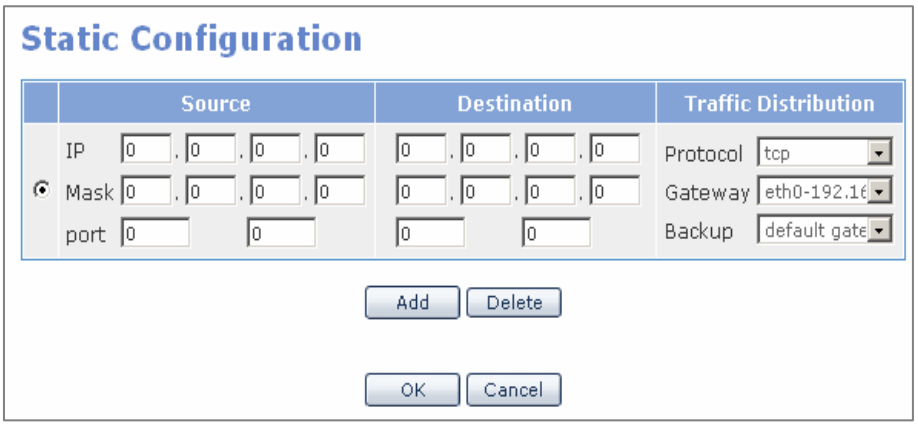
The Network Load Balance Configuration is valid when at Leaset two network interfaces are specified as the external network interface. For example, if T1 private line and ADSL line are selectively connected to Ethernet 0 Interface (eth 0) and Ethernet 1 Interface (eth 1), the higher weighted value is 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.



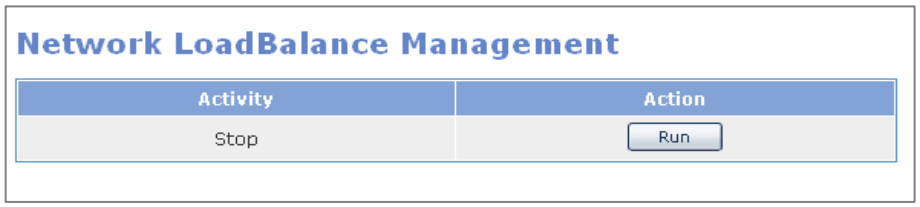
- Source: Source IP address, netmask and port number of transfer session
- Destination: Destination IP address, netmask and port number of transfer session
- Traffic distribution: Interface and protocol that transfer session passes through

- 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.



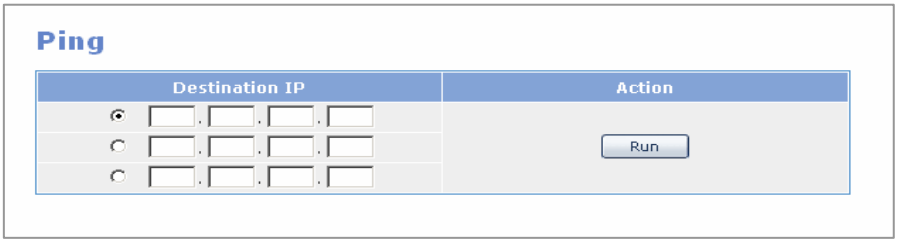
- Activity: Current activity
- Action: Click the **[Run]** button to start the NLB service.
- If the OfficeServ 7400 system is restarted the NLB service will automatically return to its last state.

Utility

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

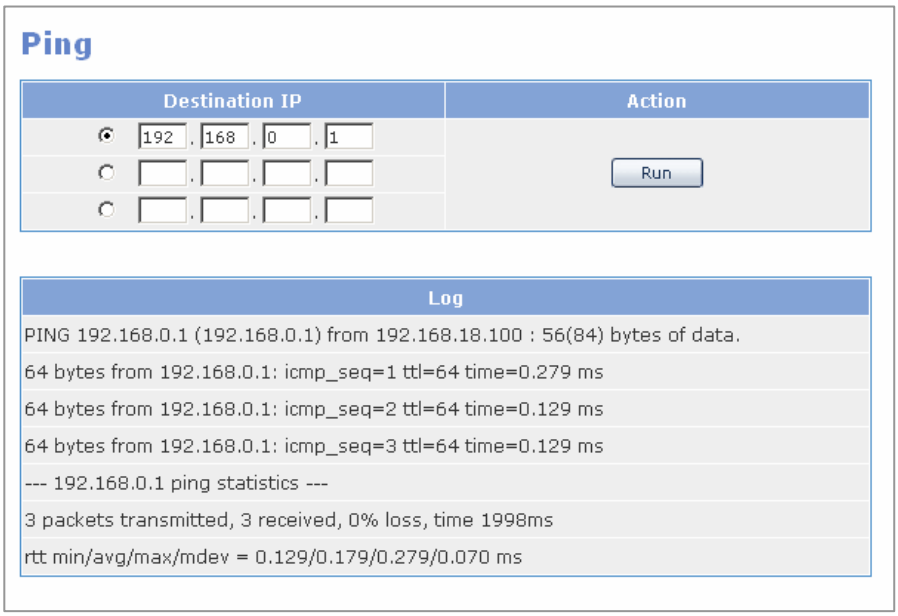
Ping

The Ping menu is used to initiate a ping test.



The **[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.



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.

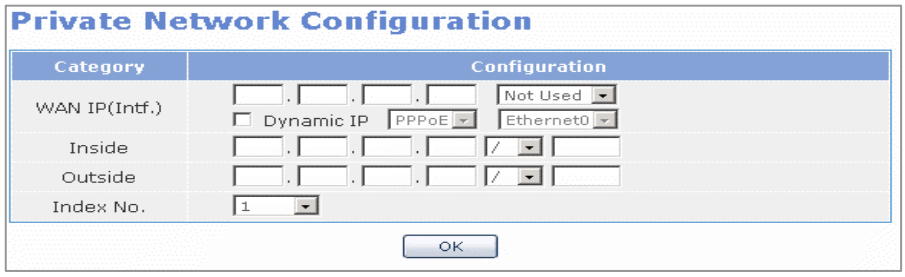
Setting	Description
Enable	To enable the NAT function
Disable	To disable the NAT function

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

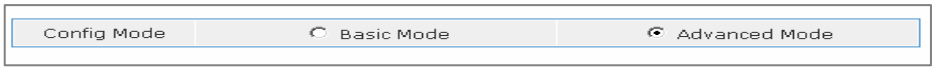
This table configures a network by using the minimum value of the options required for the configuration of a private network.

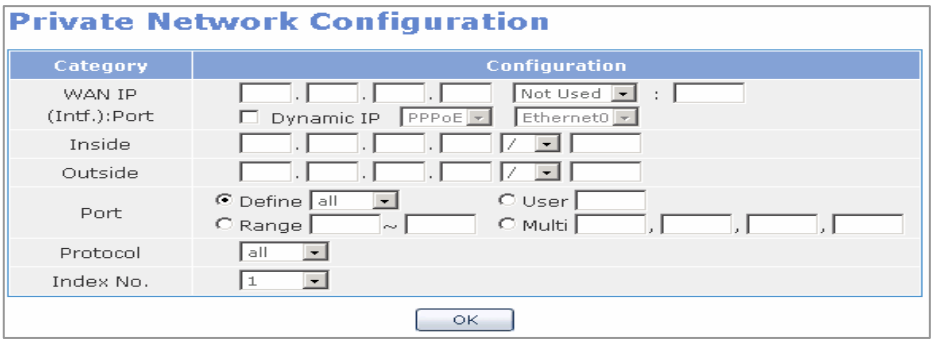


Category	Description
WAN IP	To set a general IP. Set up the connected port after selecting a dynamic IP for ADSL or Cable modem.
Inside	To enter a network address to configure a private network or select the range of netmask.(/: netmask, -: range, *; all)
Outside	To enter the network address connected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





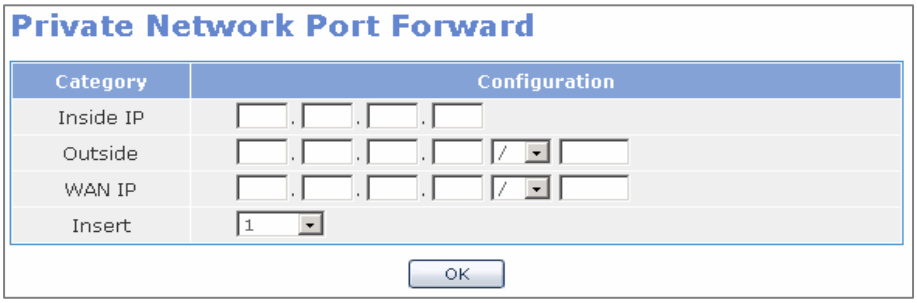
Category	Description
Port	For only some specific ports, It is allowed to set up for the outside.
Protocol	Select TCP and UDP protocols. Both TCP and UDP are set up for ‘All’.

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

Port Forward

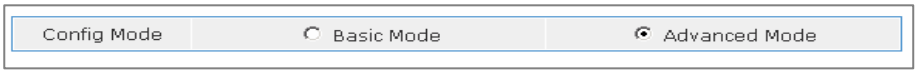
This table allows connecting to PC, which has a private IP inside the system, from outside environment.

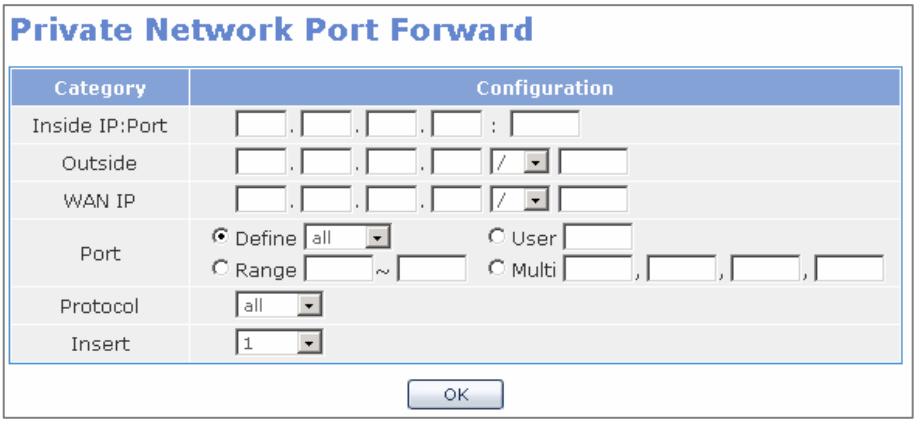
Basic Mode: The basic mode is set up by using the minimum value of the options for port forwarding.



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.

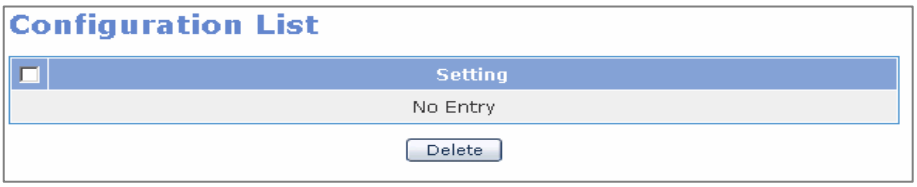
Advanced Mode: The administrator can select and set up ports or protocols that are not included in the basic configuration additionally.





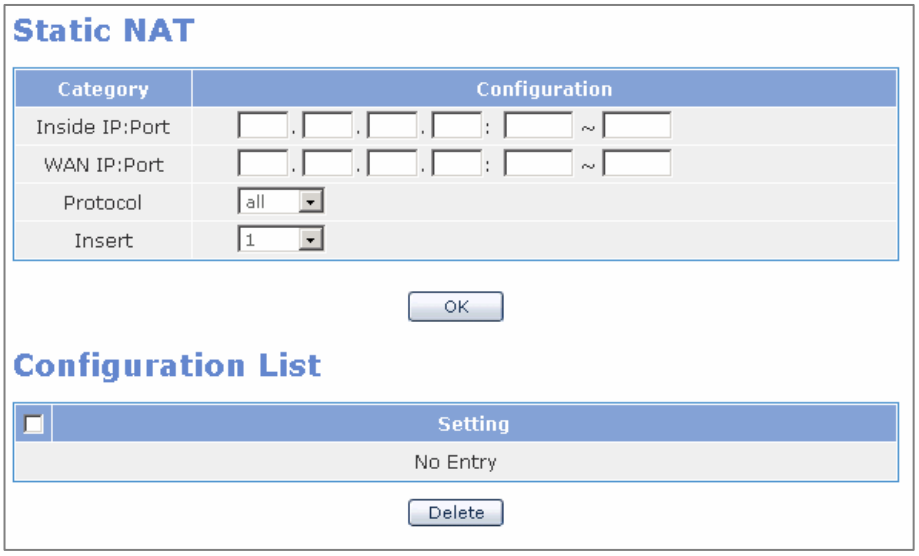
Category	Description
Port	It is available to set up as only some specific ports are allowed to transfer to the outside.
Protocol	Select a TCP and UDP protocol. For 'All', both TCP and UDP should be set up.

Configuration List displays the current setup status.



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.



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

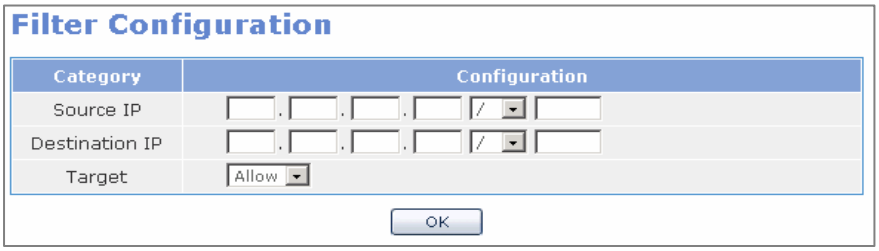
Setting	Description
Enable	To enable the Filter function
Disable	To disable the Filter function

Configuration

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

Basic Mode

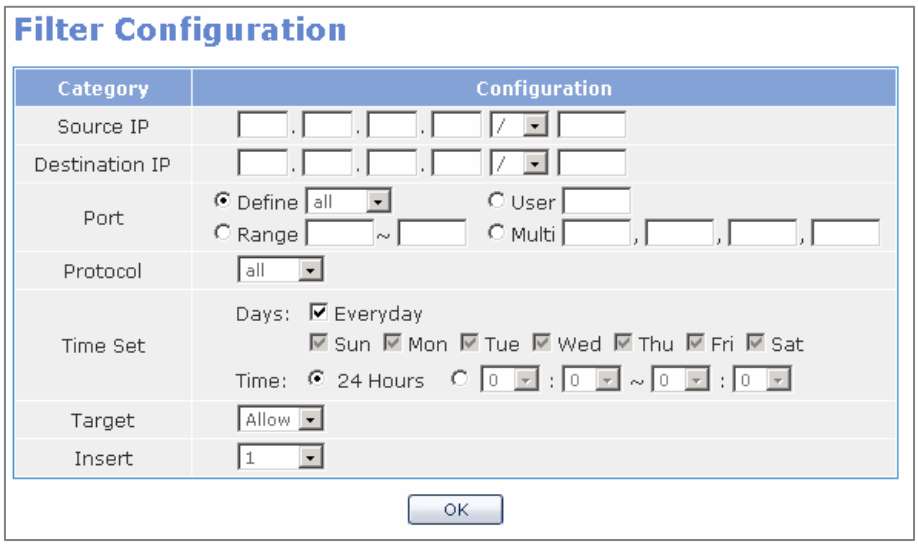
Enter the minimum options required for packet filtering.



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

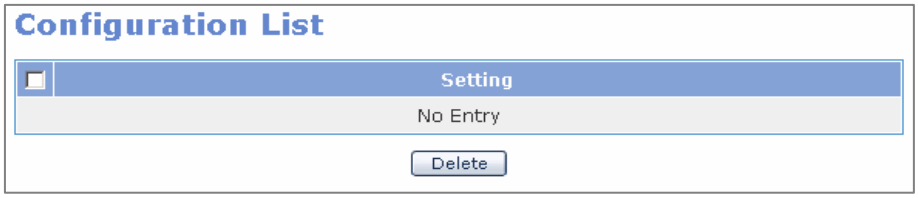
Advanced Mode

This window allows the administrator to assign additional options for packet filtering.



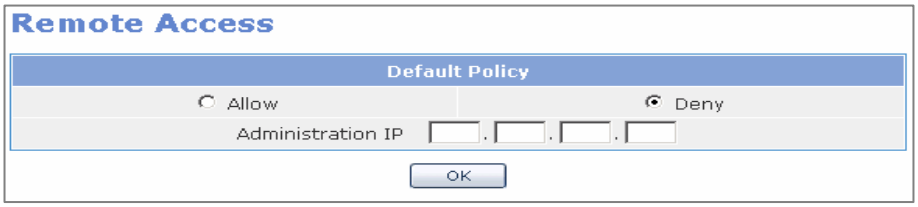
Category	Description
Source IP	To set the origination IP.
Destination IP	To set the destination IP.
Port	To set the port.
Protocol	To set the protocol.
Time Set	To set the time to apply the filtering rule.
Insert	To select a location to insert the entered rule.

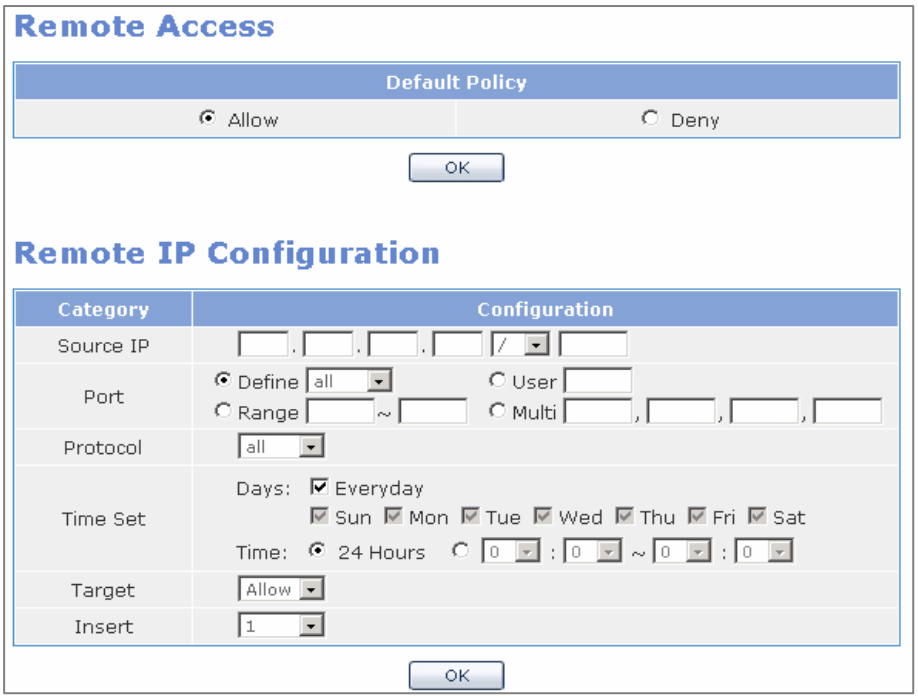
This table displays the current setup status.



Remote Access

Allow or Deny remote access.

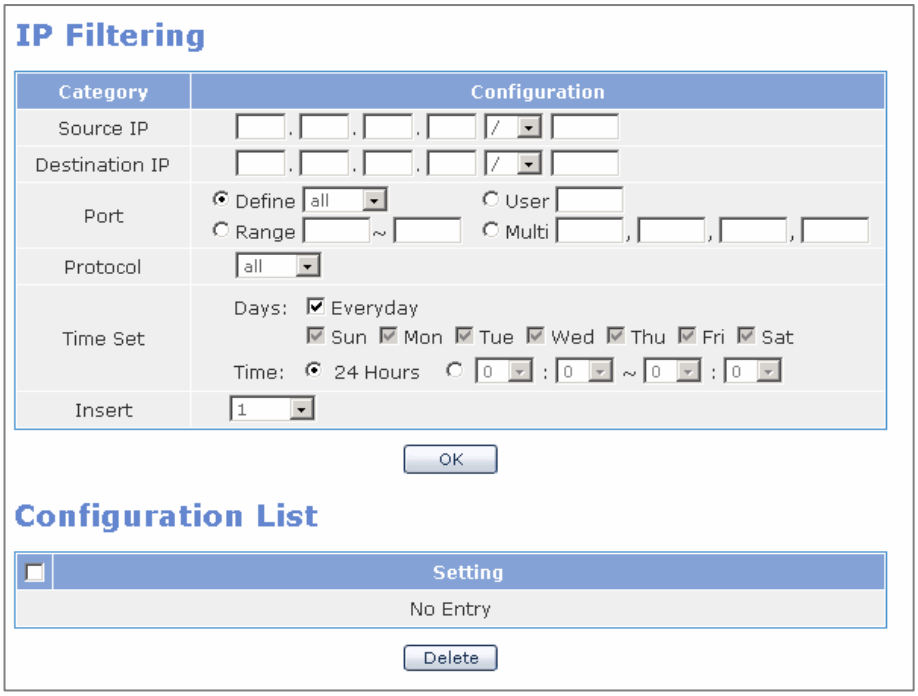




Default Policy

- 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



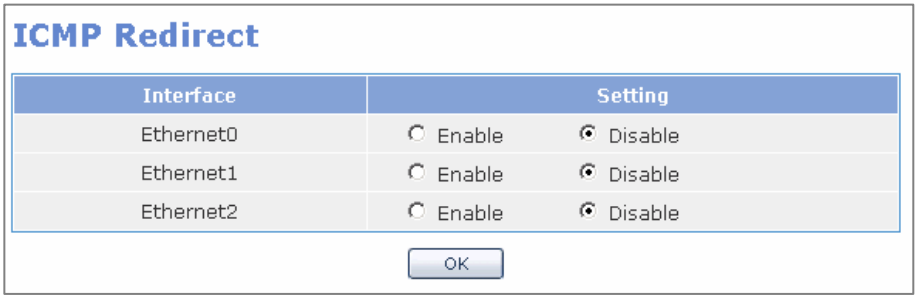
URL Filtering

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

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.



Router

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

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.

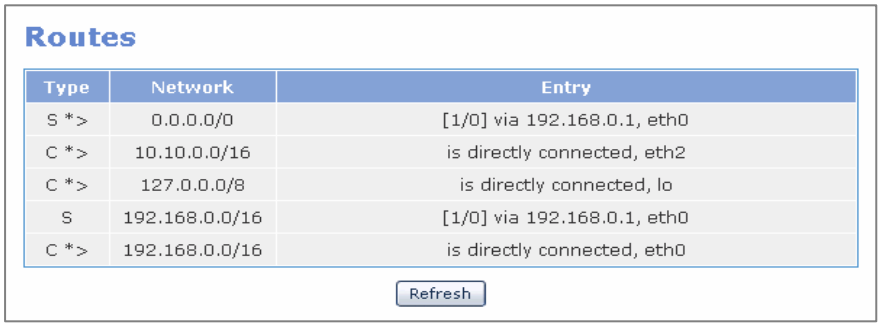
Menu	Submenu	Description
List	Access List	Sets Access-list.
	Prefix List	Sets Prefix-list.
	Route Map	Sets Route-map.
	As Path List	Sets BGP AS-path list.
	Community List	Sets BGP Community-list.
	Key Chain	Sets the key used for authentication of RIP v2.
Status	RIP	Displays RIP network information.
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

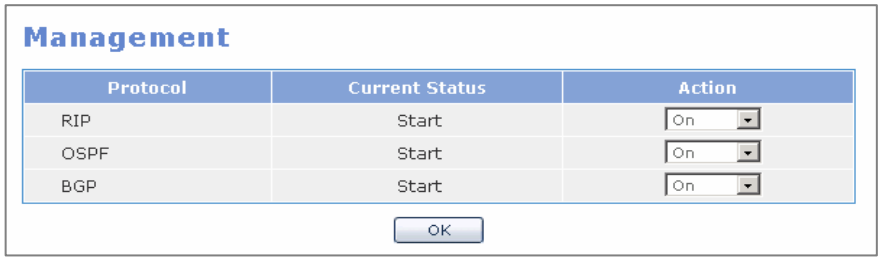
Select **[General]** → **[Routes]** to retrieve the routing table of GWIM.



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.



Configuration

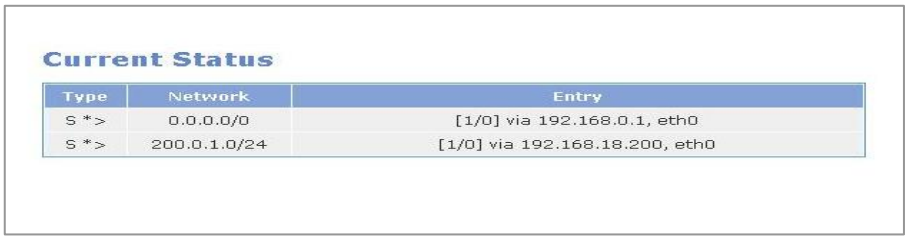
This menu is used to set static route, RIP, OSPF protocol, and BGP.

Static Route

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

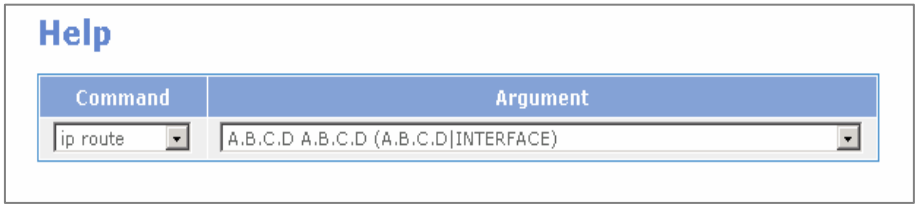
Enter the Static Route command.

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:



Help

Select the argument corresponding to the ‘ip route’ or ‘no ip route’ command.
Click **[Argument]** to display all arguments corresponding to the command..



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

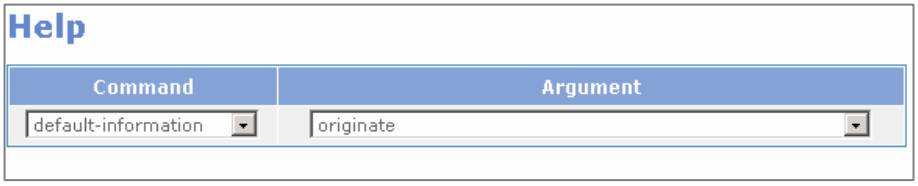
RIP

[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]**.

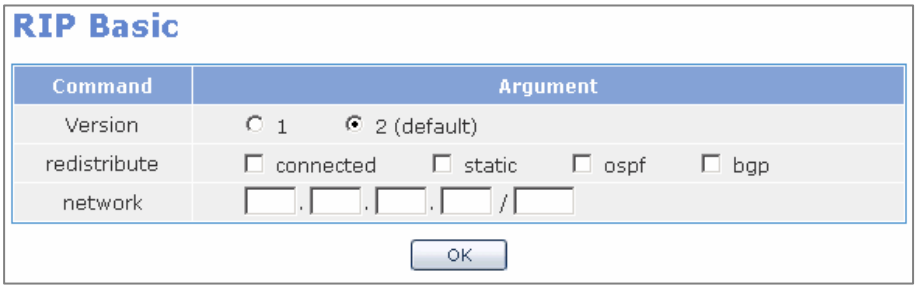
Help

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

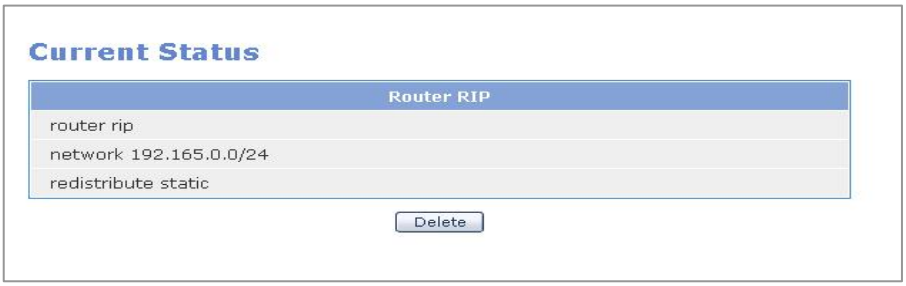


RIP Basic

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



Displays the command configuration currently entered.



RIP Interface

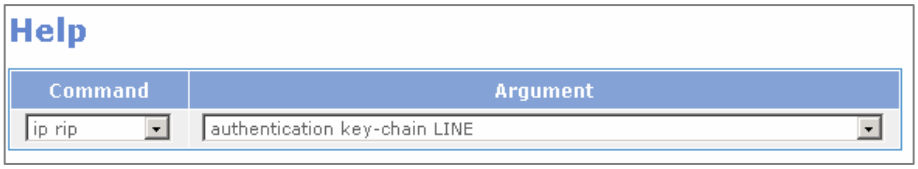
[Configuration] → [RIP Interface]

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] → [RIP Interface]**.

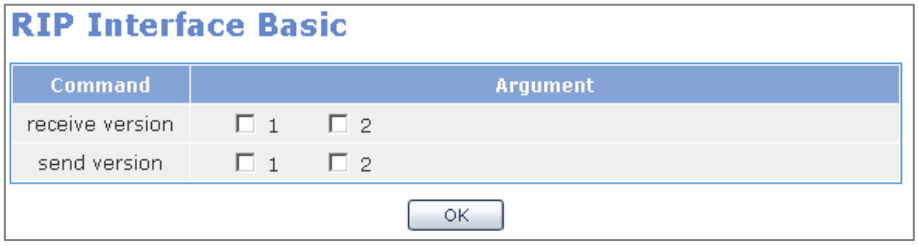
Help

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

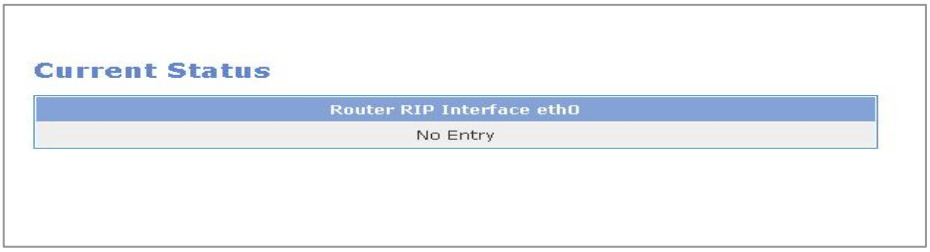


RIP Interface Basic

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



Displays the command configuration currently entered.



OSPF

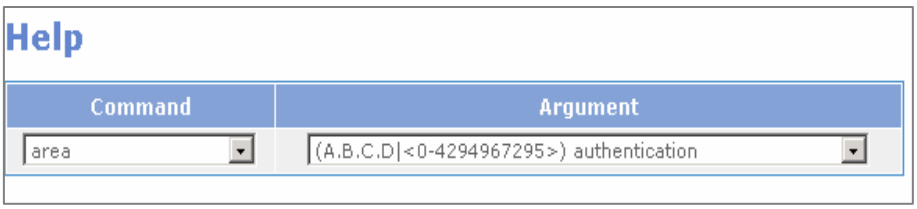
[Configuration] → [OSPF]

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]**.

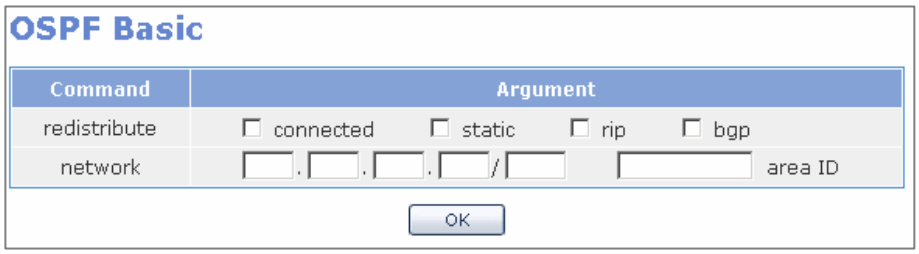
Help

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

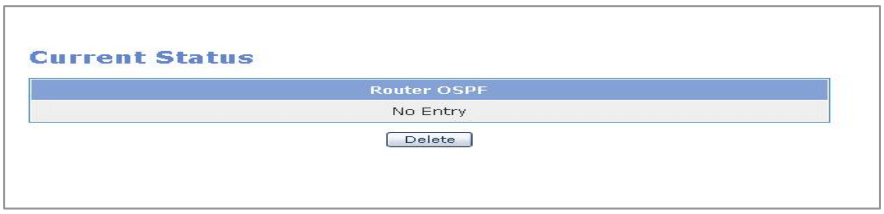


OSPF Basic

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



Displays the command configuration currently entered.



OSPF Interface

[Configuration] → [OSPF Interface]

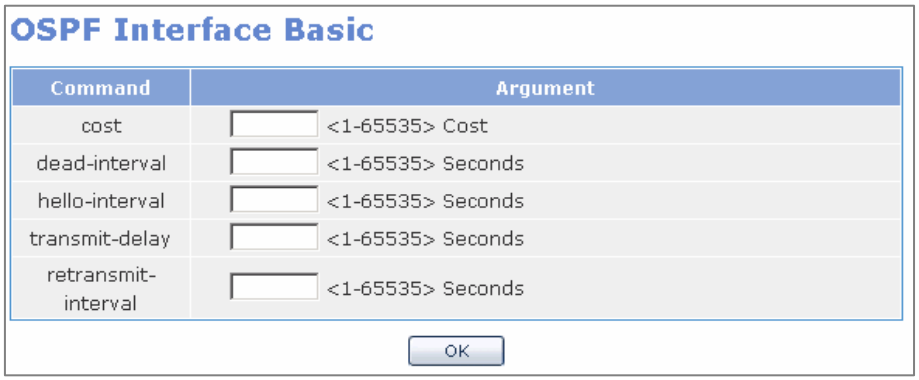
Select the target interface and enter the protocol configuration command directly.
If the entered command is successfully executed, the execution result is directly applied to **<Current Status>** of **[Router] → [Configuration] → [OSPF Interface]**.

Help

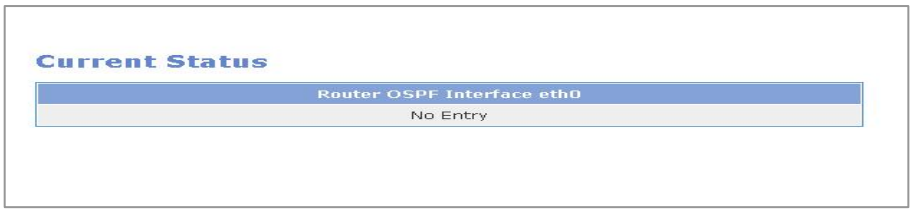
Select the argument corresponding to the OSPF interface.
Clicking the **[Argument]** item displays all arguments corresponding to the command.

OSPF Interface Basic

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



Display the command configuration currently entered.



BGP

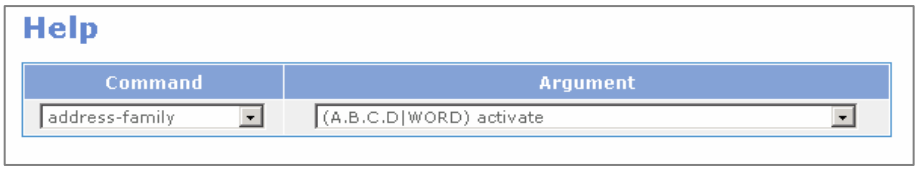
Select **[Configuration]** → **[BGP]** and set BGP. After setting the target item and click the **[Save]** button.

Enter the BGP configuration command directly.

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:

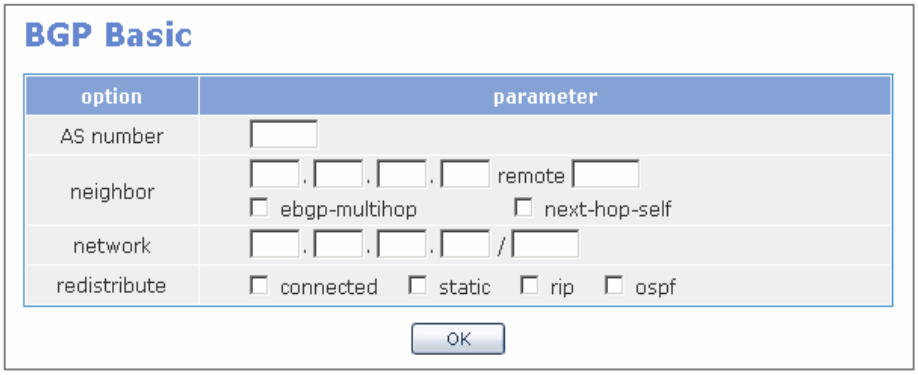
Help

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



BGP Basic

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



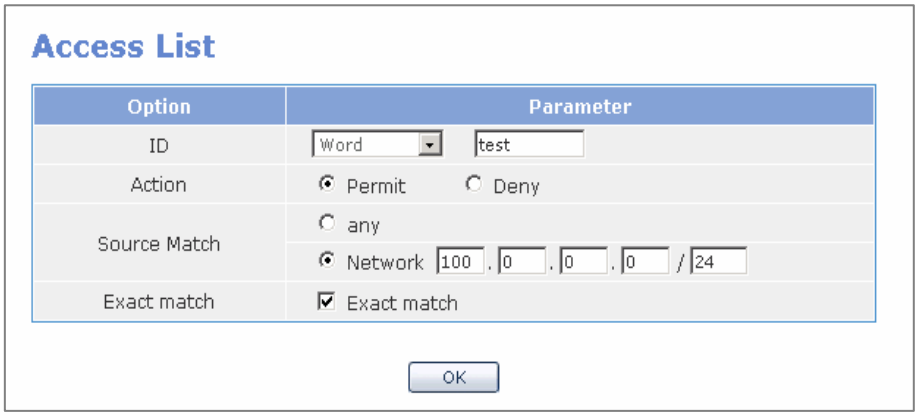
Current Status

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

List

Access List

[List] → [Access List]



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.

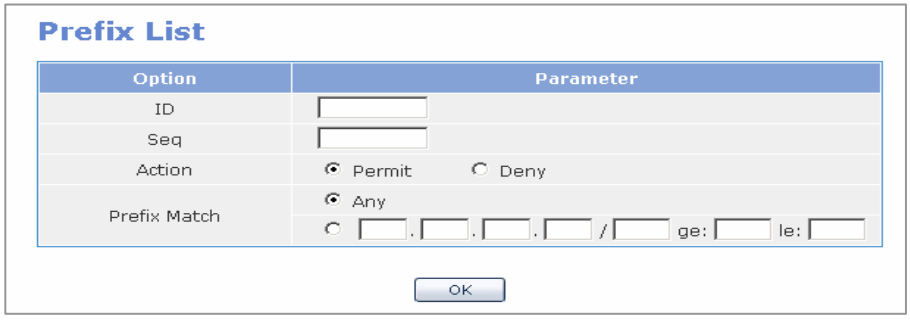
If the entered command is successfully executed, the execution results are directly applied to <**Current Status**> of **[Router] → [List] → [Access List]**. For example, when Access-list is entered, the <**Current Status**> window is displayed as follows.

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.



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:

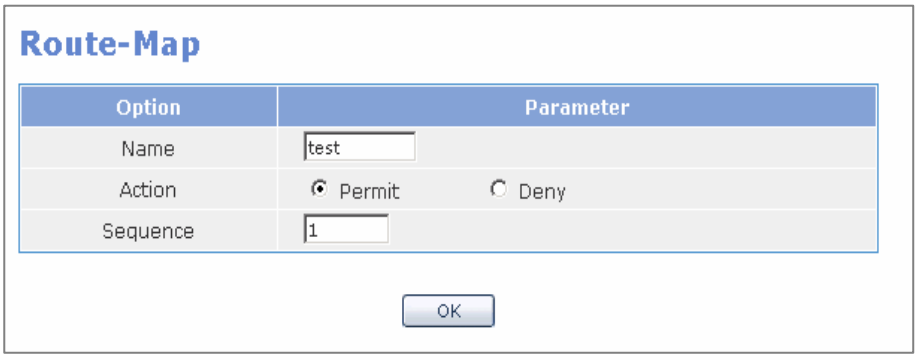
Prefix-list information being set in GWIM can be displayed. Click the **[Delete]** button to delete the entry of the selected prefix list. Click the **[Delete All]** button to delete all entries of the prefix list.

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.



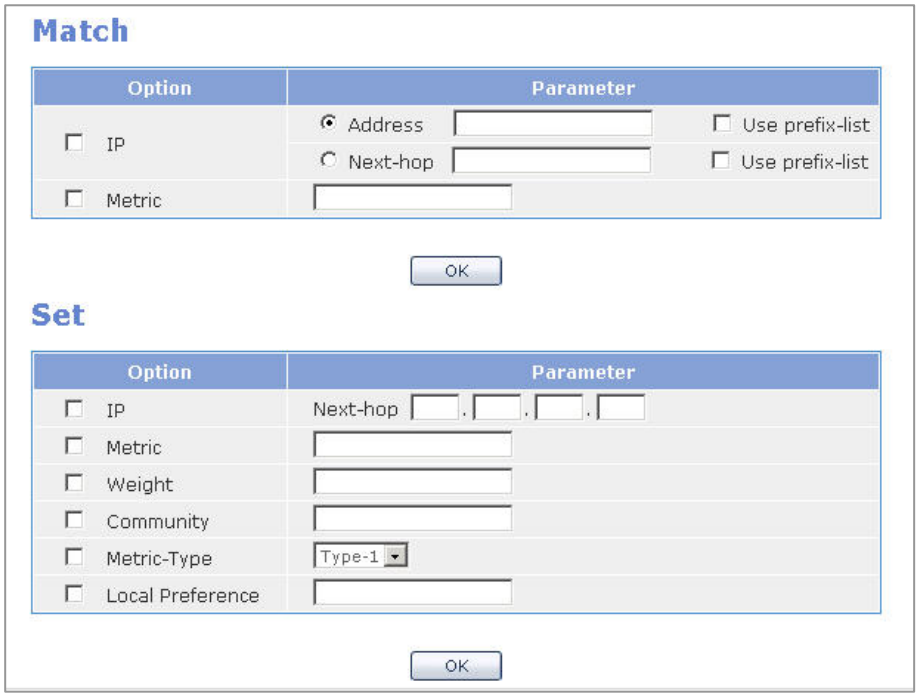
Item	Description
Name	Route-map name
Action	Sets whether to apply set operation.
Sequence	Sets the sequence No. to additionally delete a route-map

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:

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.



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.

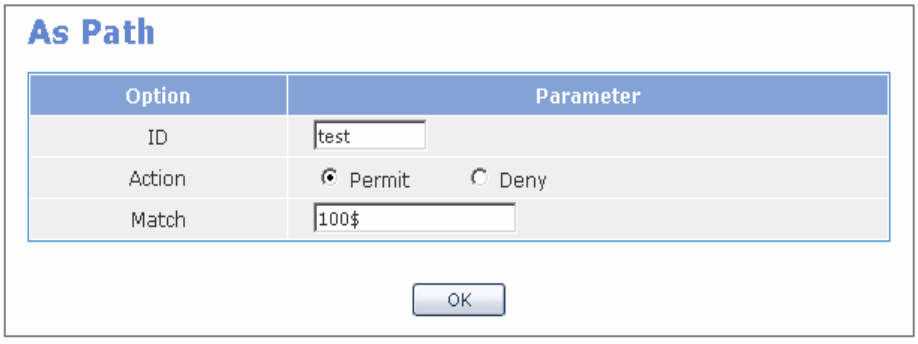
When the match condition is met and Action is set to Permit, the job corresponding to Set operation is performed. If the command is successfully executed, the execution result is directly applied to **<Current Status>**.

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

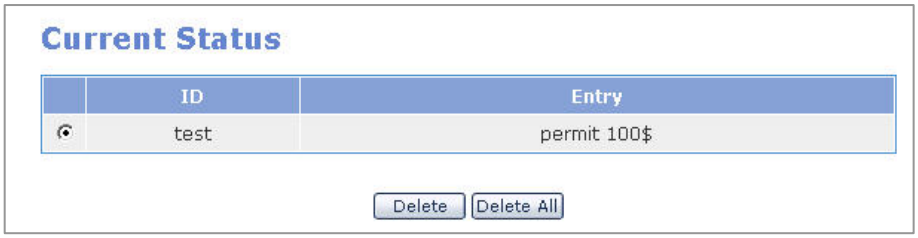
Select **[List]** → **[As Path List]** and set AS Path access-list of GWIM BGP. Enter the target value and click the **[Save]** button.



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:



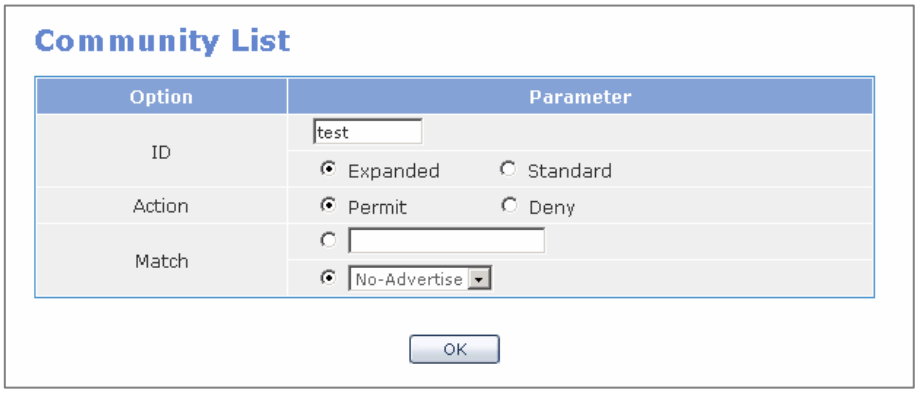
This menu is used to display the information on the as path access-list set in GWIM.

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.



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:

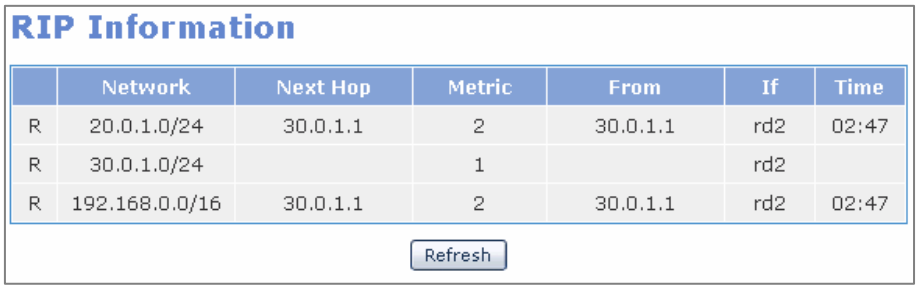
Item	Description
ID	Community list name
Entry	Community list information

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

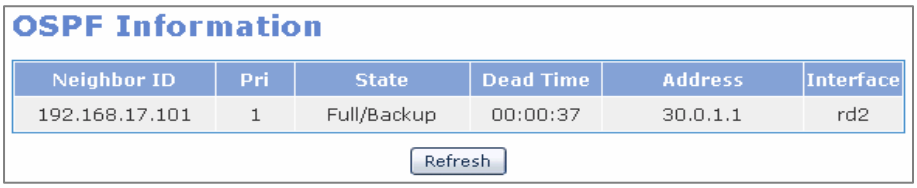
This menu is used to display the RIP connection status and information.



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

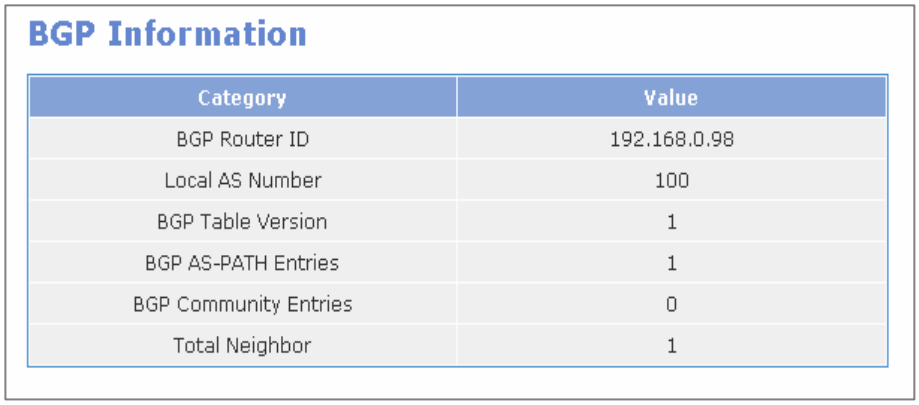
This menu is used to check the OSPF connection status and information with the other party's router.



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

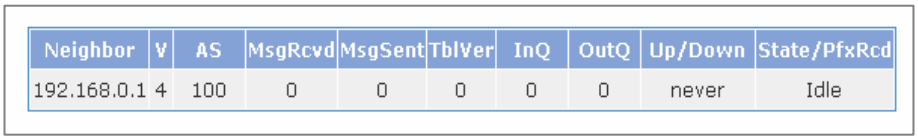
This menu is used to check the BGP connection status information and BGP routing table information.



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

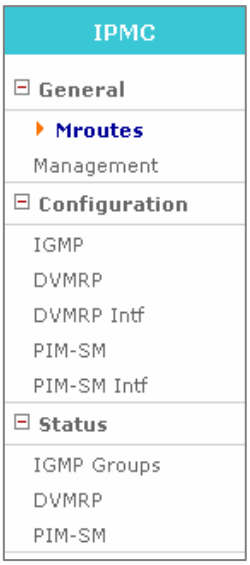
Item	Description
Neighbor	IP address of the neighbor router
V	Version No. used by neighbor
AS	AS No. of neighbor
MsgRcvd	Message number received from neighbor
MsgSent	Message number sent from neighbor
TblVer	Latest BGP database version sent from neighbor
InQ	Number of messages that should be received 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

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:

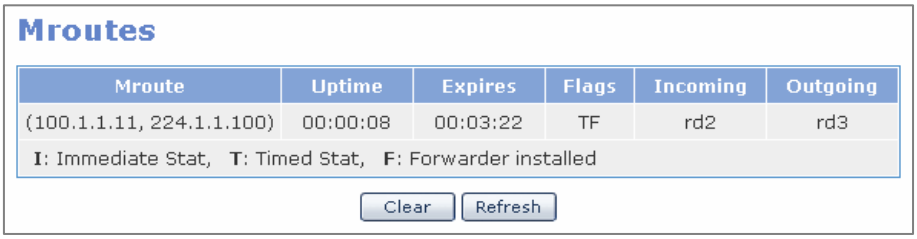


Menu	Submenu	Description
General	Mroutes	Displays Multicast Routing Entry.
	Management	Starts/Stops IPMC protocol demons.
Configuration	IGMP	Displays or changes IGMP configuration.
	DVMRP	Displays or changes DVMRP default configuration.
	DVMRP Intf	Displays or changes VIF of DVMRP.
	PIM-SM	Displays or 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

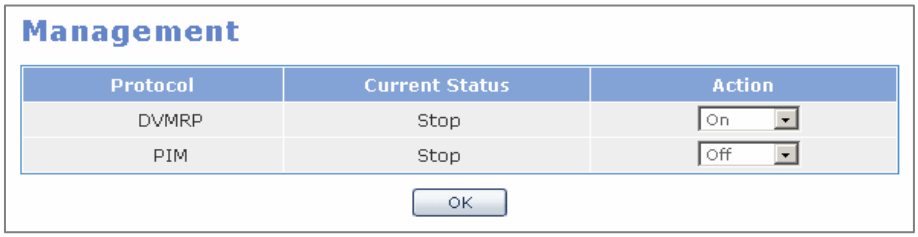
This menu is used to display multicast routing entries being shown in this window.



- 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.



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

Configuration

IGMP

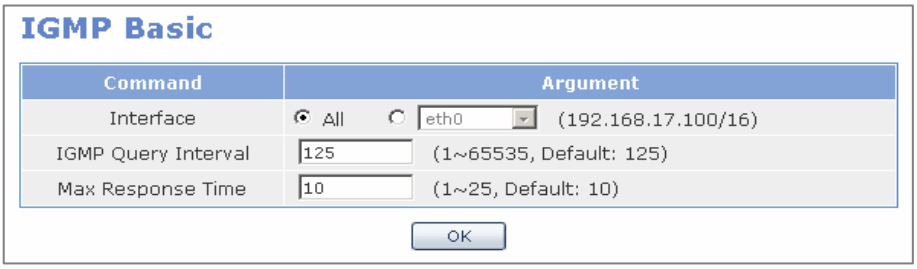
This menu is used to display and change IGMP configuration.

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 Basic

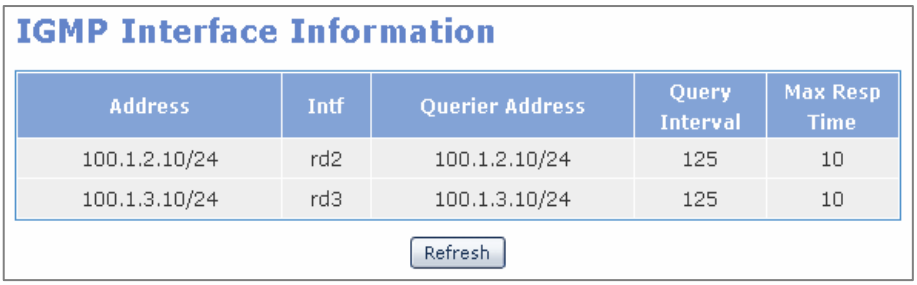
Enter new information and click the **[OK]** button to change the default configuration of IGMP.



- 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.



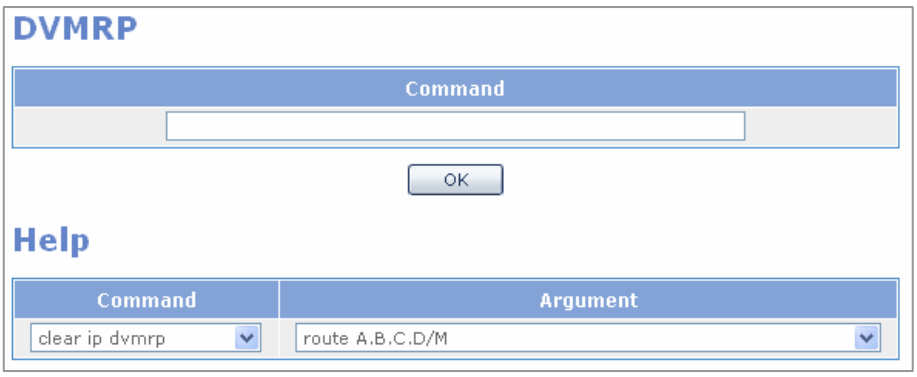
- Address: IGMP group address
- Intf: IGMP interface name
- Querier Address: IP address of IGMP interface that sends membership query. IP address of Designate Router(DR)
- Query Interval: Cycle of sending Membership Query
- Max Resp Time: Maximum time of waiting a response to Membership Query

Configuration / DVMRP

This menu is used to set DVMRP.

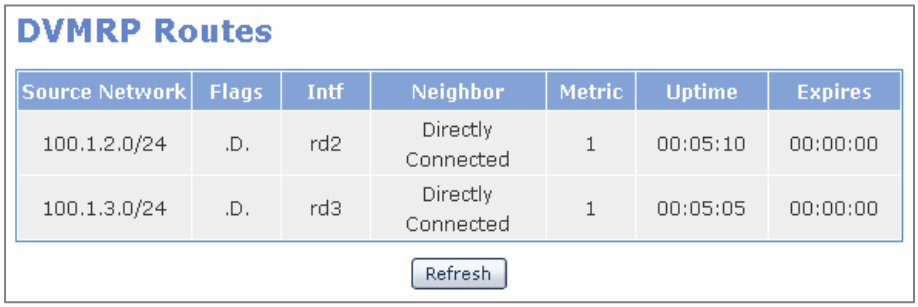
DVMRP & Help

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



DVMRP Routes

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



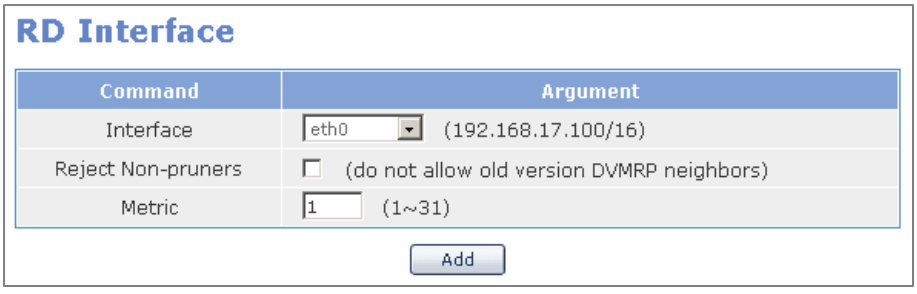
- Source Network: VIF network address to which multicast packets flow
- Flags: DVMRP route feature flag. N=New, D=Direct Connected, H=Hold down
- Intf: VIF name to which multicast packets flow
- Neighbor: DVMRP neighbor IP address that provides information on DVMRP route
- Metric: DVMRP route Metric(=distance) 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

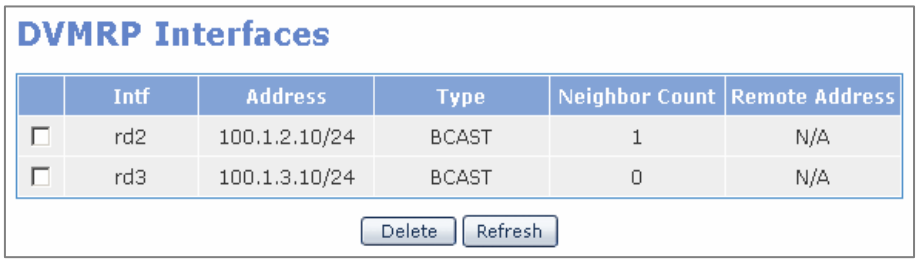
This menu is used to add L3 interface where an IP address is set to DVMRP VIF. Select the target interface to be added to VIF from the Interface item, enter the target value, and click the **[Add]** button.



- 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.



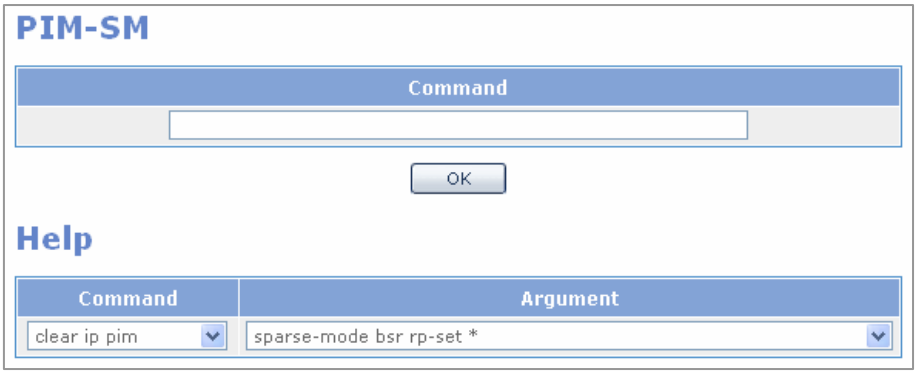
- Intf: DVMRP VIF name
- Address: IP address of DVMRP VIF
- Type: DVMRP VIF type. Tunnel, Point-to-Point, Broadcast
- Neighbor Count: Number of neighbors connected to DVMRP VIF
- Remote Address: Address of the other party in case of Tunnel or Point-to-Point type.(Peer Address)

PIM-SM

This menu is used to set PIM-SM.

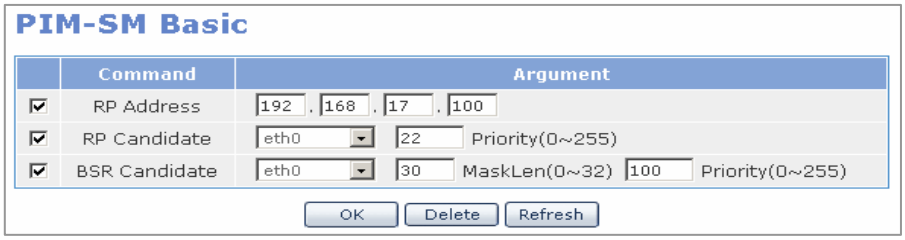
PIM-SM & Help

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



PIM-SM Basic

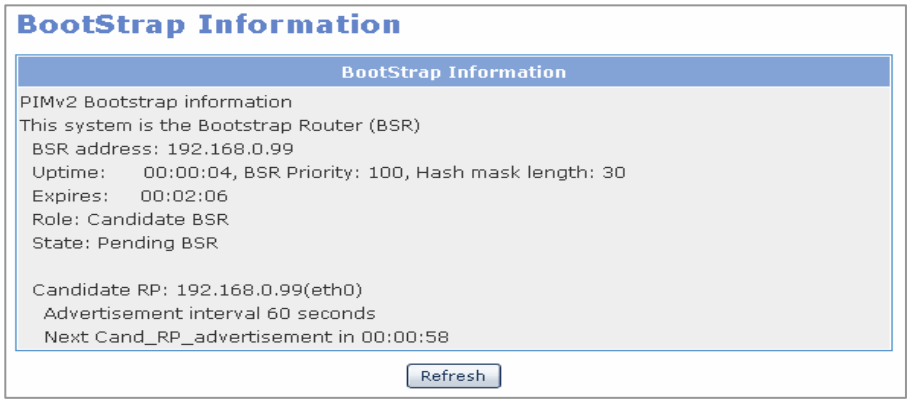
This menu is used to set BSR and RP of PIM-SM protocol. Mark the check box on the right and enter the configuration values. Click the **[OK]** button to apply the values. Mark the check box of the target item and click the [**Delete**] button.



- 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.)

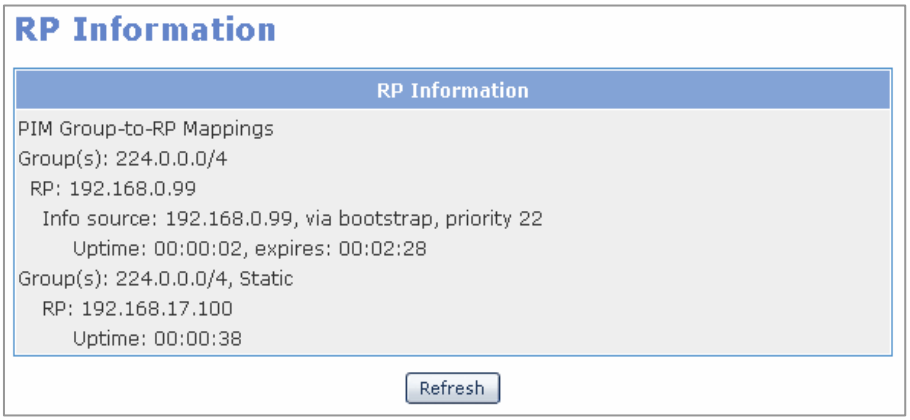
BootStrap Information

This menu is used to display the information on BootStrap router.



RP Information

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

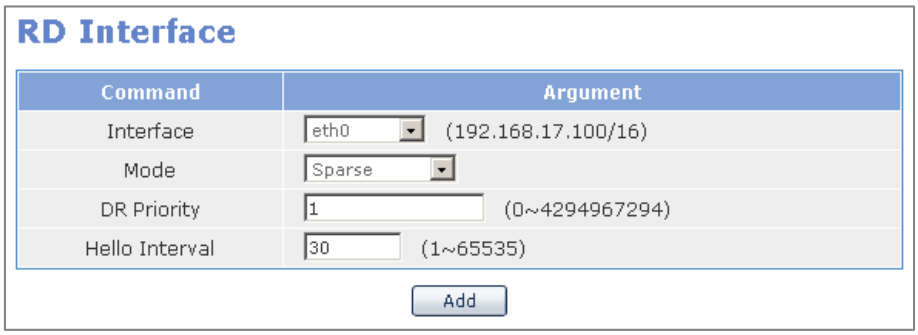


PIM-SM Intf

This menu is used to set PIM-SM VIF.

RD Interface

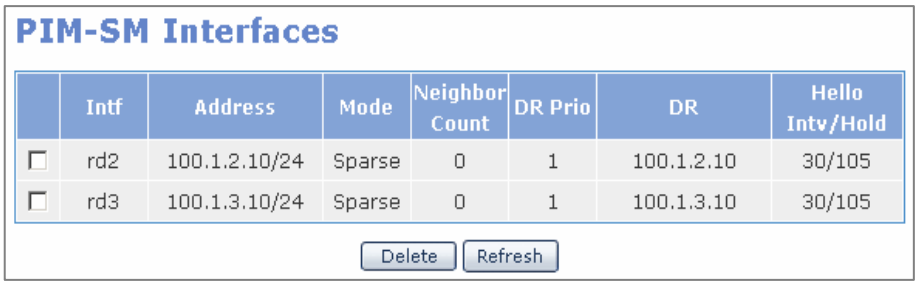
This menu is used to add PIM-SM VIF. Select the target L3 interface from the Interface item, enter the target values, and click the **[Add]** button to add PIM-SM VIF.



- 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

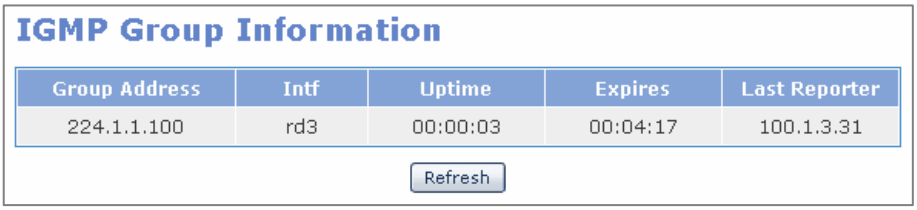
PIM-SM Interfaces

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.



IGMP Groups

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



- 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

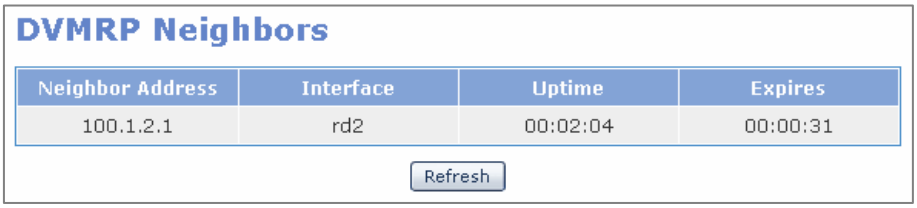
Status

DVMRP

This menu is used to display the DVMRP protocol status.

DVMRP Neighbors

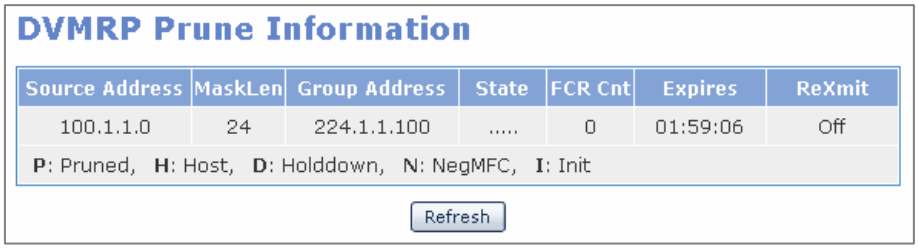
This menu is used to display the information on the DVMRP neighbor whose information is exchanged.



- 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

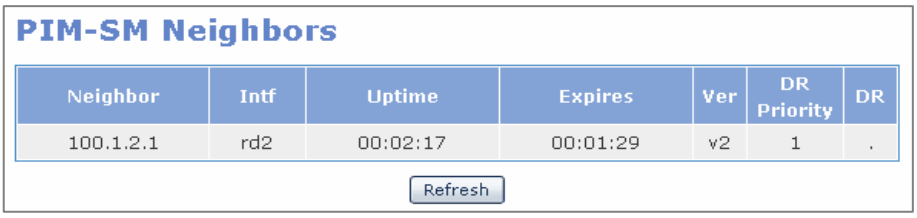
This menu is used to display DVMRP Prune items.



- 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.



- 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:

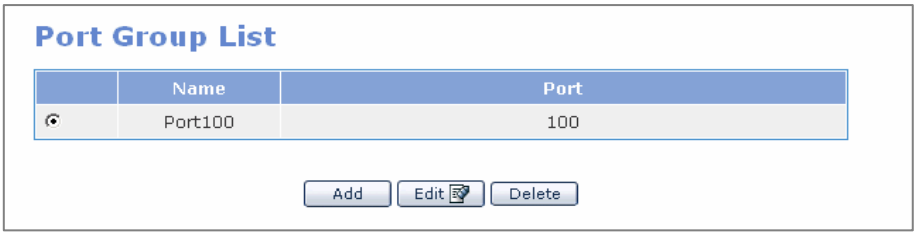
Menu	Submenu	Description
Group	Port Group	Retrieves, sets, edits, or deletes a port group
	IP Group	Retrieves, sets, edits, or deletes an IP group
	Filter Group	Retrieves, sets, edits, or deletes a filter group
	Class Group	Retrieves, sets, edits, or deletes a class group
Policy	-	Sets a class for a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

Group

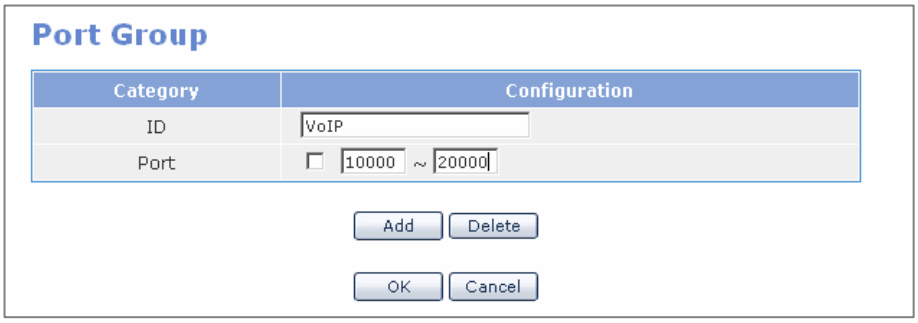
The **[Group]** menu is used to retrieve, set, edit, or delete a port group, an IP group, a filter group, or a class group.

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.

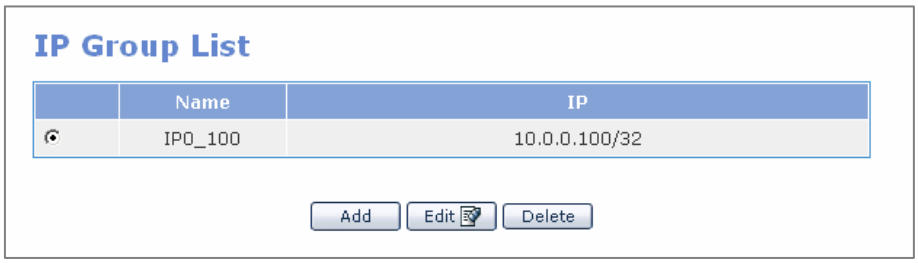


Enter the target ID and port No. and click the **[Save]** button.
Click the **[Add]** button to add a port, and click the **[Delete]** button after marking the checkbox to delete the target port.

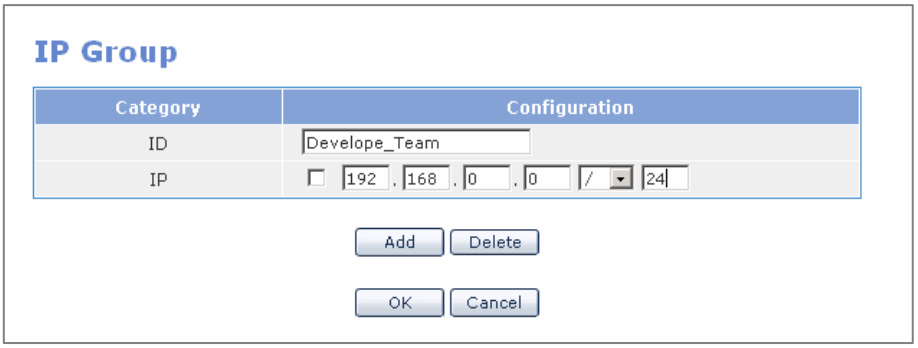
Item	Description
ID	Name of the port group - Should include both letters and numbers. - Group ID shall start only with letters, not numbers. - No blanks should be left in between characters.
Port	- Port range - Enter '0' to set all ports

IP Group

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



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

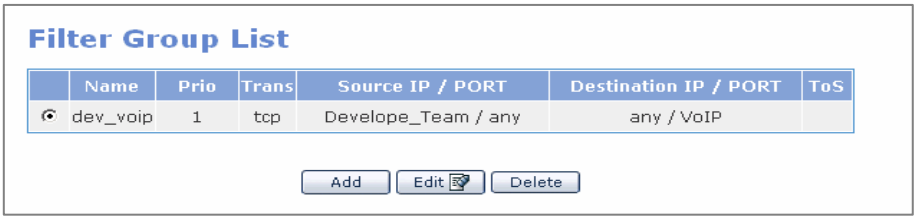


Enter the target ID and port No. and click the **[Save]** button.
Click the **[Add]** button to add an IP, and click the **[Delete]** button to delete the target IP.

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

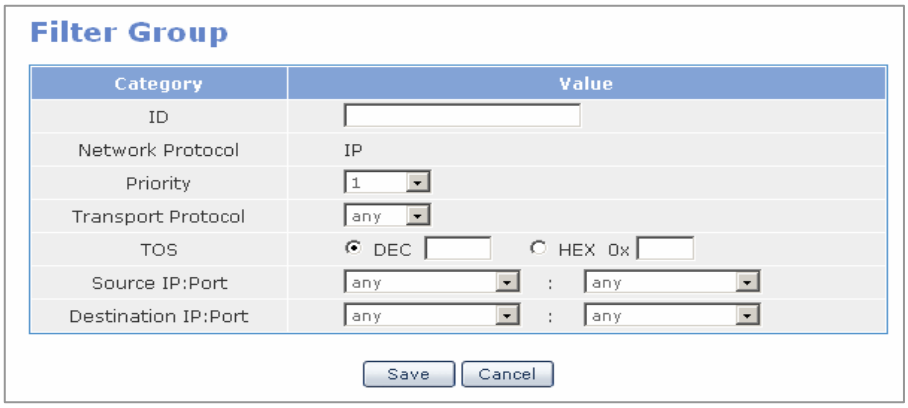
Select **[Filter Group]** to retrieve, set, edit, or delete a filter group.



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.

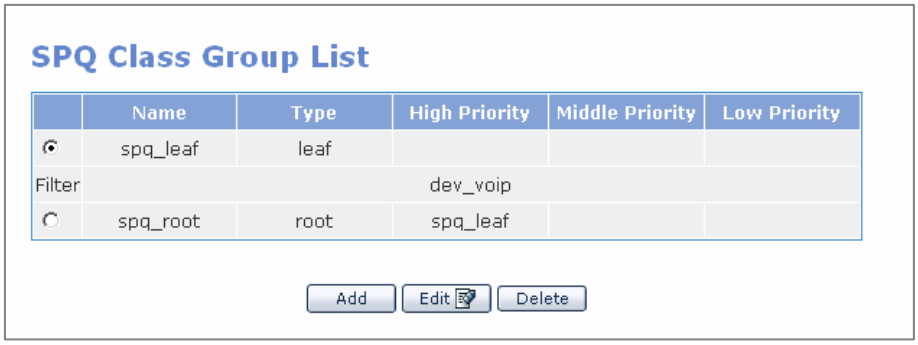


Filter means a configuration filtering for the values in the packet header. Values set in **[QoS]** → **[Group]** → **[Port Group]** and **[IP Group]** are used. Protocols and TOS fields can also be filtered. In addition, priority can be set for each filter and apply the filtering rule according to the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

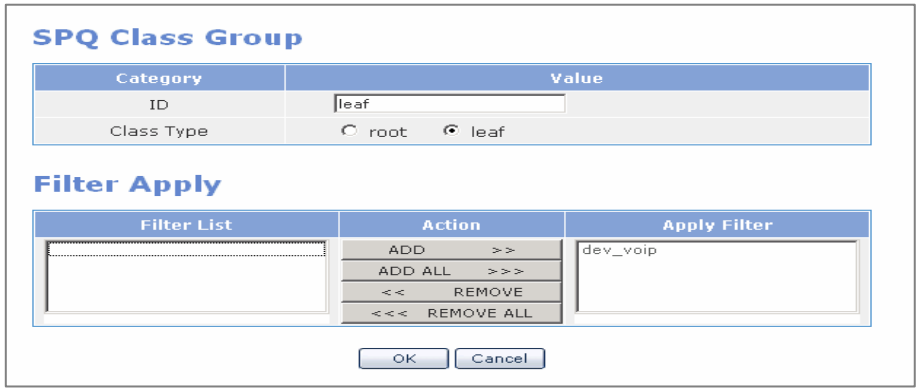
Class Group

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.

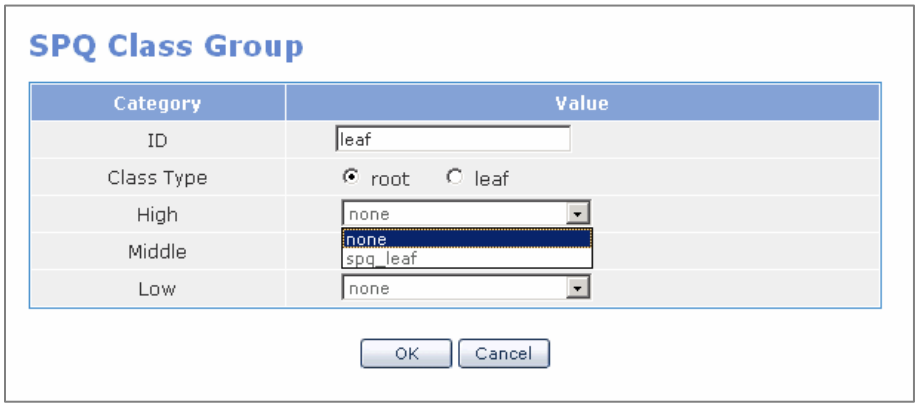
SPQ Class Group



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.



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.



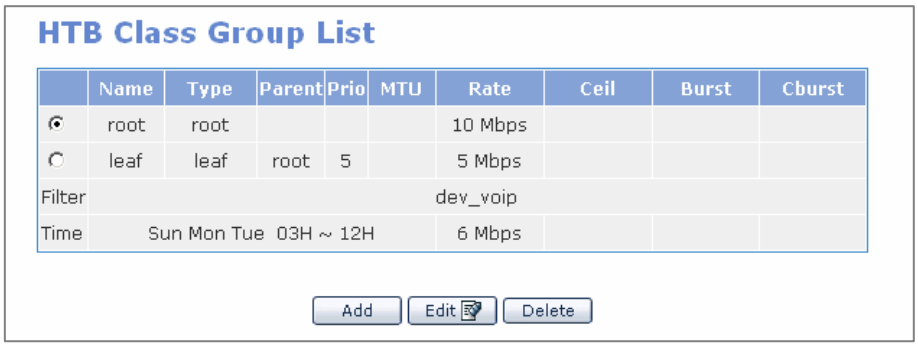
Item	Description
Class Type	Configuration window depends on the type of the class to be set. - root: Sets the root class. - Leaf: Sets the leaf class.
High	Sets the leaf class whose priority will be set to high.
Middle	Sets the leaf class whose priority will be set to middle.
low	Sets the leaf class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

NOTE

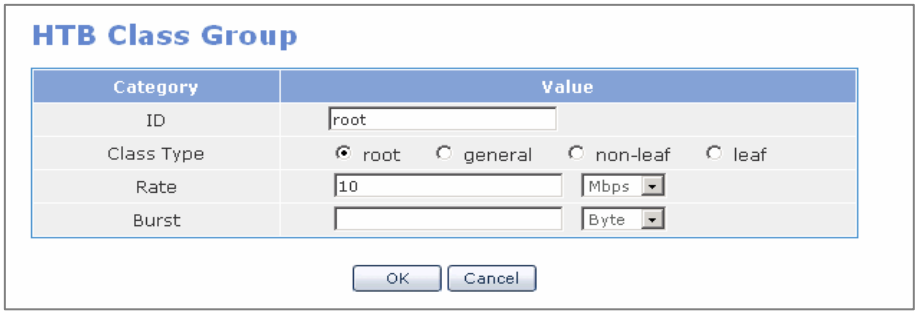
SPQ

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

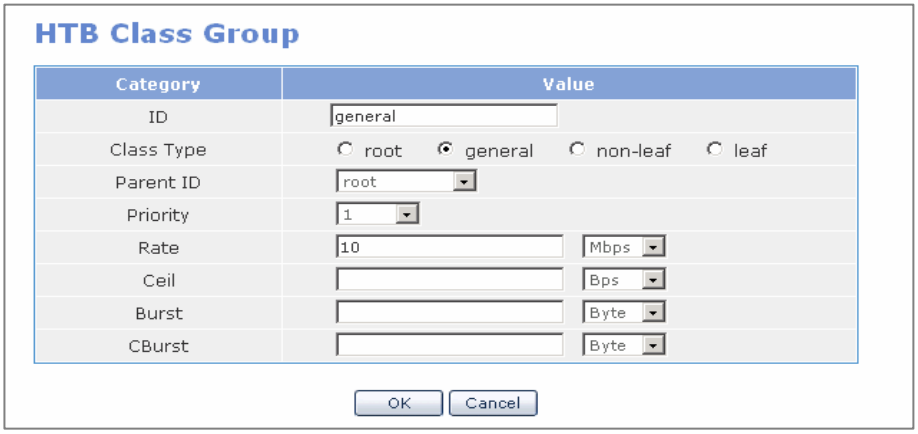
HTB Class Group



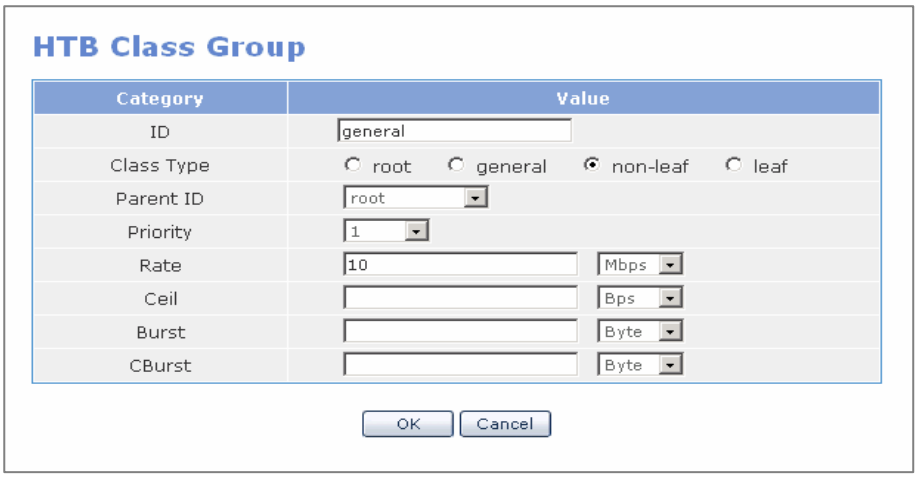
Click the **[Add]** button of HTB Class Group List in the **<HTB Class Group>** window to display the window where HTB class group can be set. If the class type is root, the window is displayed as follows. Set each item and click the **[OK]** button.



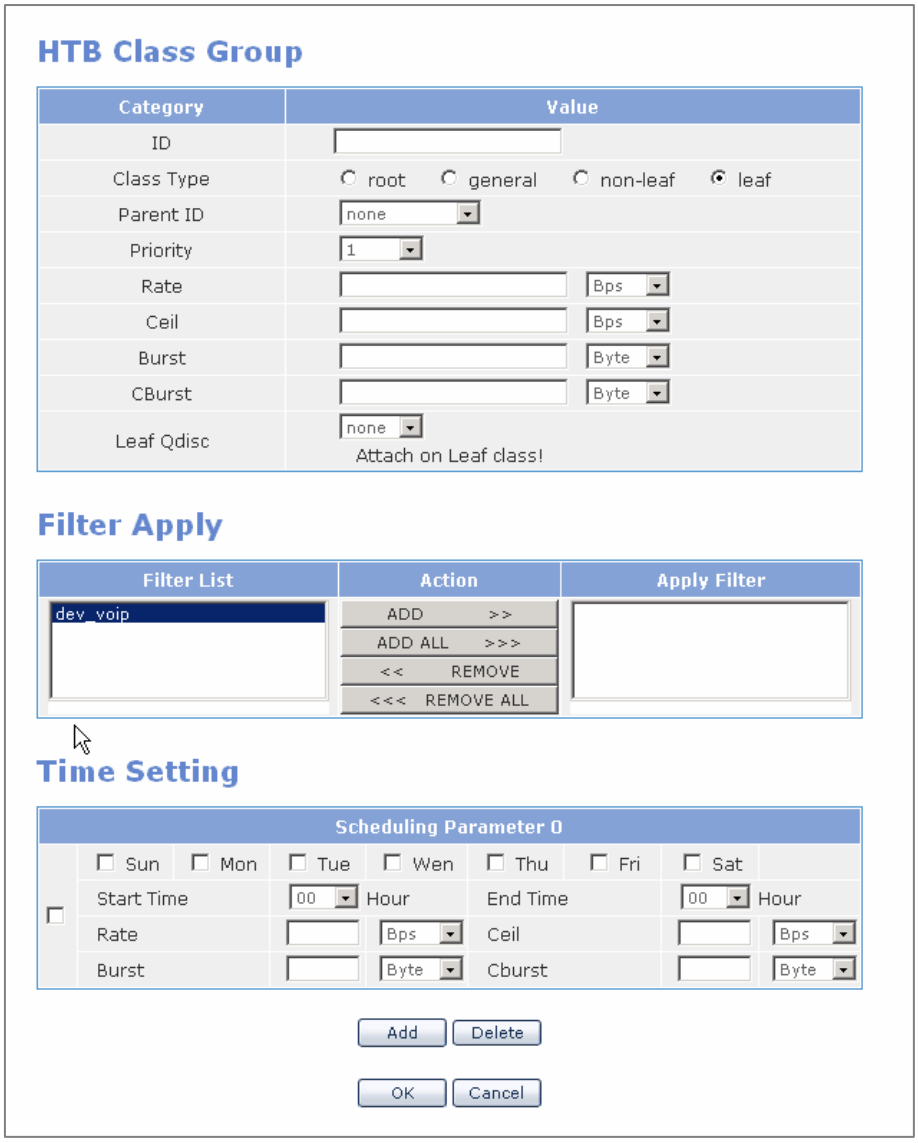
If the class type is general, the window is displayed as follows. Set each item and click the **[OK]** button.



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



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



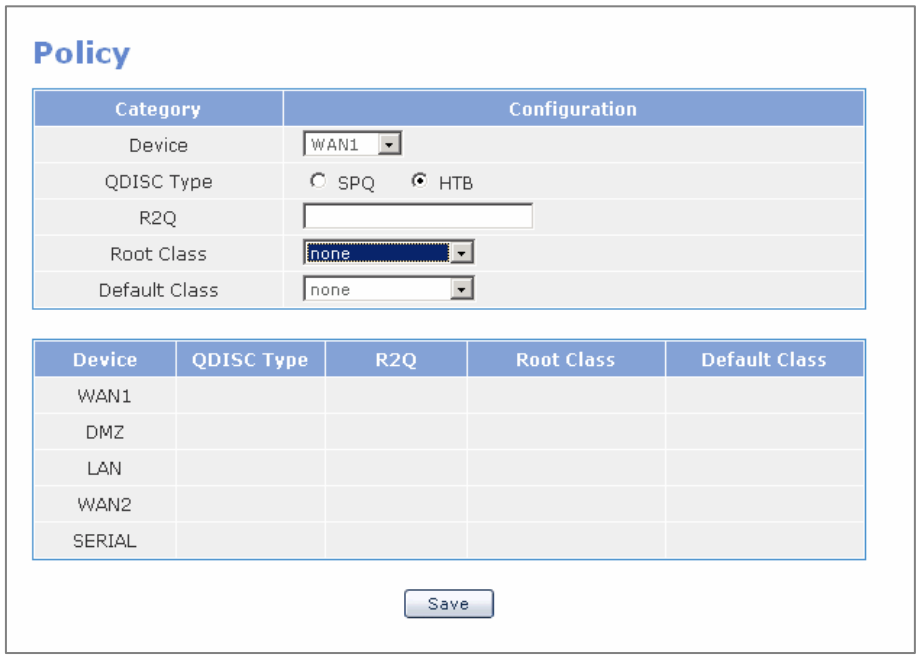
Item	Description
Class Type	Configuration window depends on the type of the class to be set. - root: Sets the root class. - general: Sets the class that connects the root with the leaf classes. - non-leaf: Sets the default class. - Leaf: Sets the leaf class.

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]** ort **[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

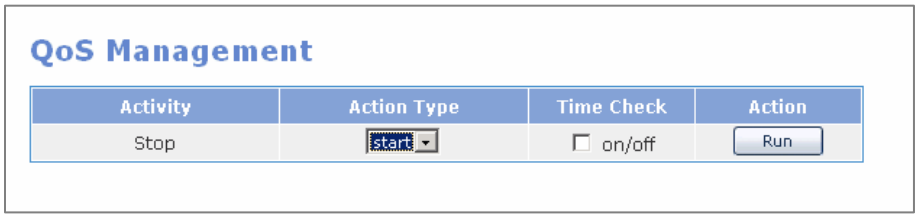
The **[Policy]** menu is used for setting a class for a port. Enter the following items and click the **[Save]** button to select a class for a port.



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.

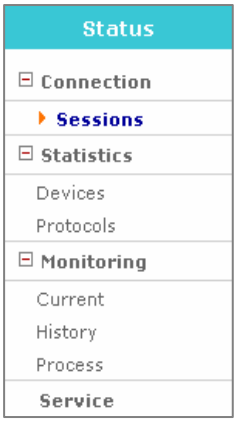
Management

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]**.



Status

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



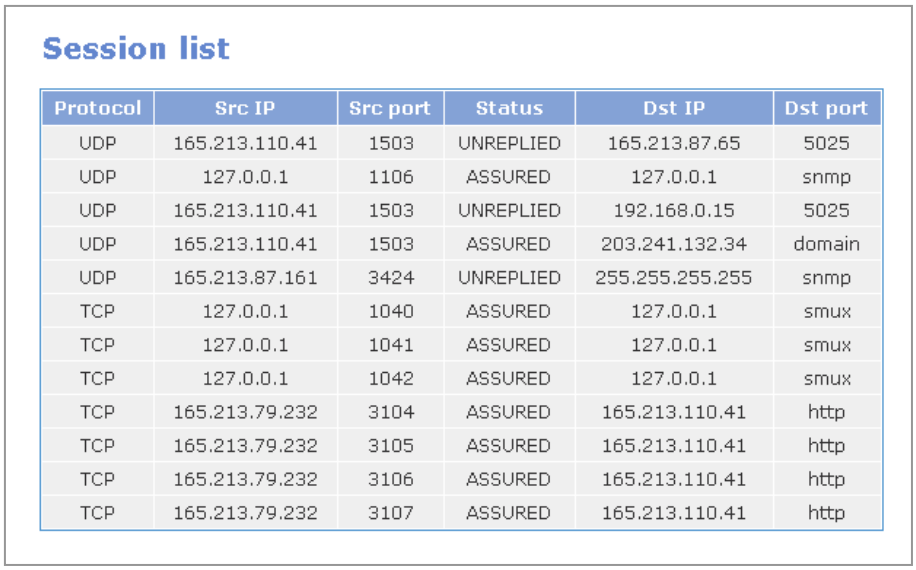
Menu	Submenu	Description
Connection	Sessions	Displays the information on the IP and port connected to GWIM.
Statistics	Devices	Displays GWIM network statistics by classifying Tx and Rx of each device.
	Protocols	Displays GWIM network statistics of each protocol.
Monitoring	Current	Provides the GWIM network 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

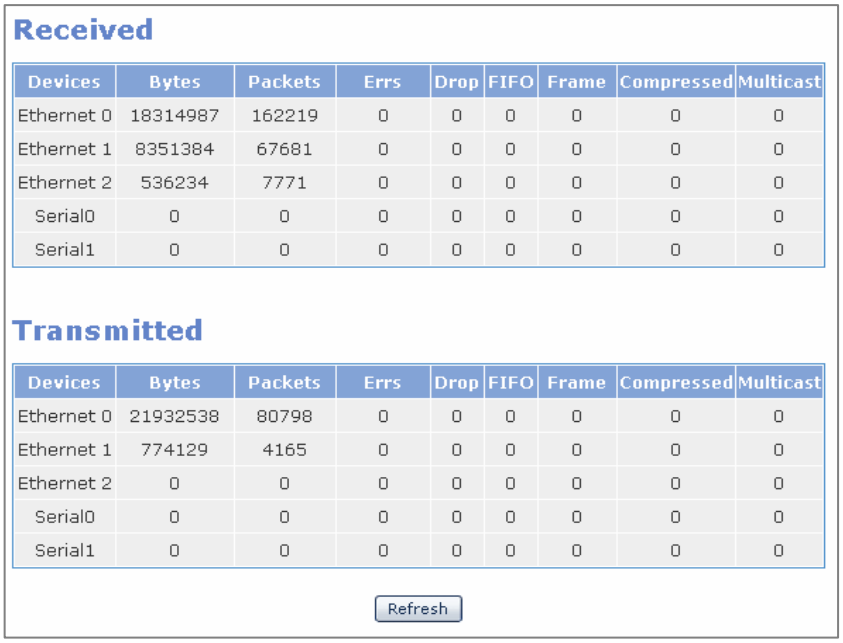
Item	Description
Protocol	Type of the protocol connected with session(UDP, TCP)
Src IP	Source IP
Src Port	Source port
Status	- UNREPLIED: Packets that are expected to be answered are received, but there is no response packet. - ASSURED: There is no response packet. (‘UNREPLIED’ is changed to ‘ASSURED’.)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

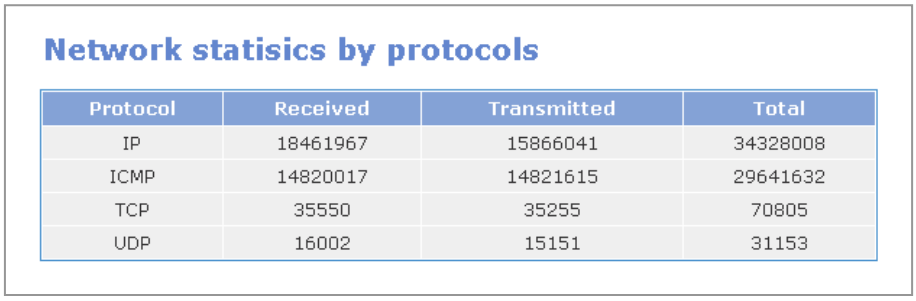
Devices	Bytes	Packets	Errs	Drop	FIFO	Frame	Compressed	Multicast
Ethernet 0	21932538	80798	0	0	0	0	0	0
Ethernet 1	774129	4165	0	0	0	0	0	0
Ethernet 2	0	0	0	0	0	0	0	0
Serial0	0	0	0	0	0	0	0	0
Serial1	0	0	0	0	0	0	0	0

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 statisics by protocols

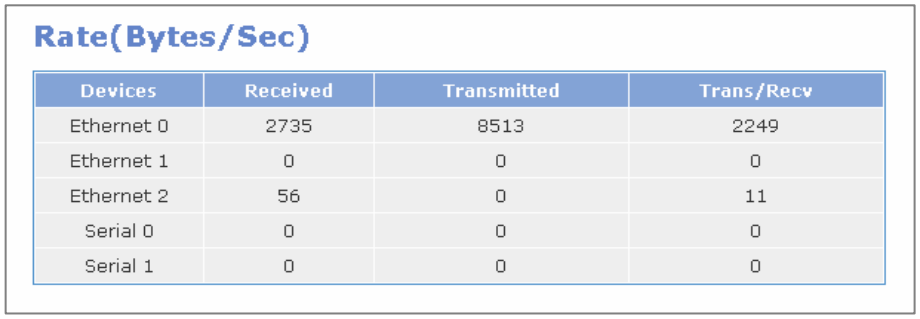
Protocol	Received	Transmitted	Total
IP	18461967	15866041	34328008
ICMP	14820017	14821615	29641632
TCP	35550	35255	70805
UDP	16002	15151	31153

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.

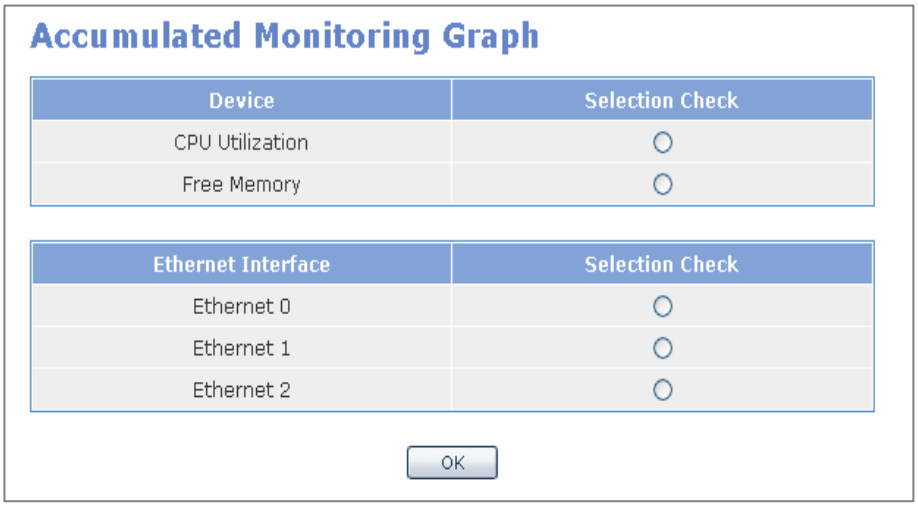


Rate(Bytes/Sec)

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.

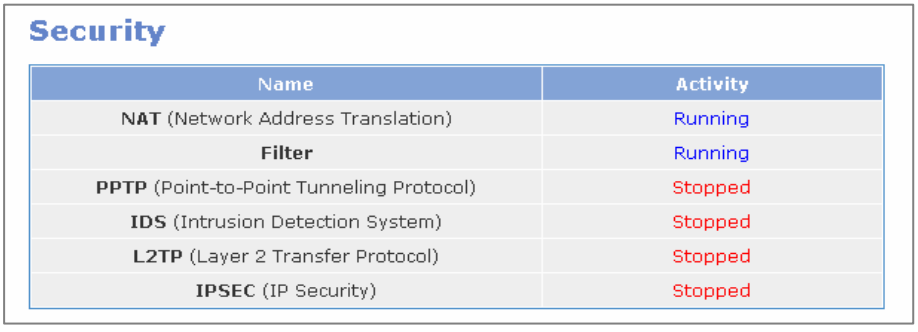


Services

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.

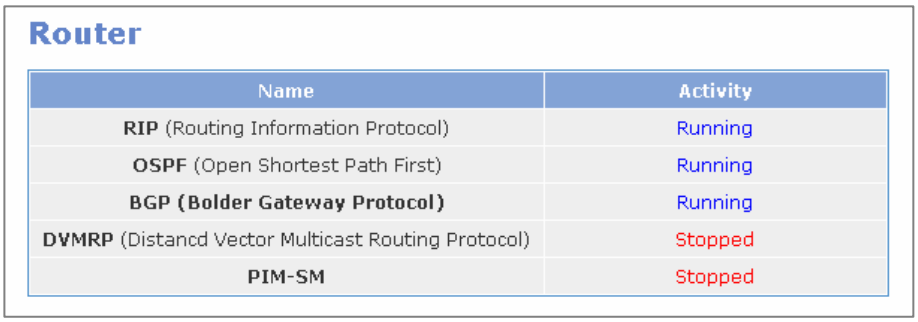
Security

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



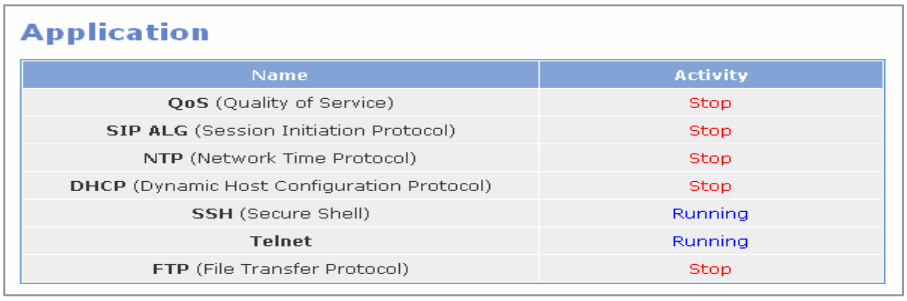
Router

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



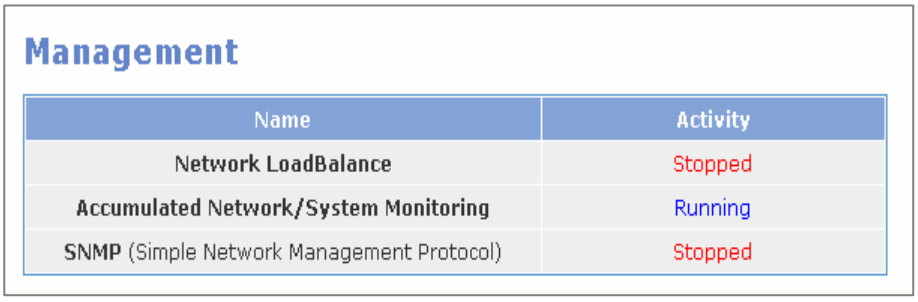
Application

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



Management

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



VPN Menu

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

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

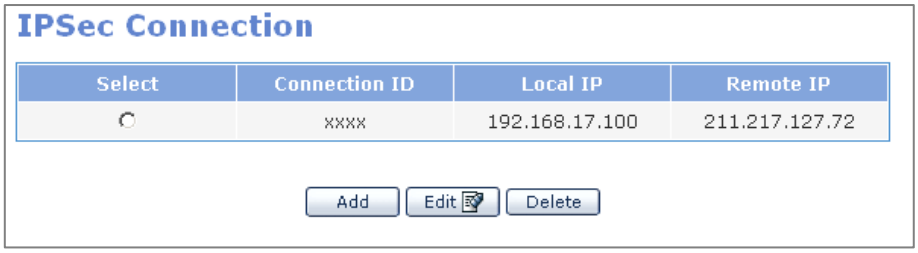
IP Security Protocol(IPSec) provides security services in the IP layer through implementing Internet Key Exchange(IKE). The security service is categorized into two services depending on remote equipment: the services providing security tunnels between local subnet and remote subnet, and between local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

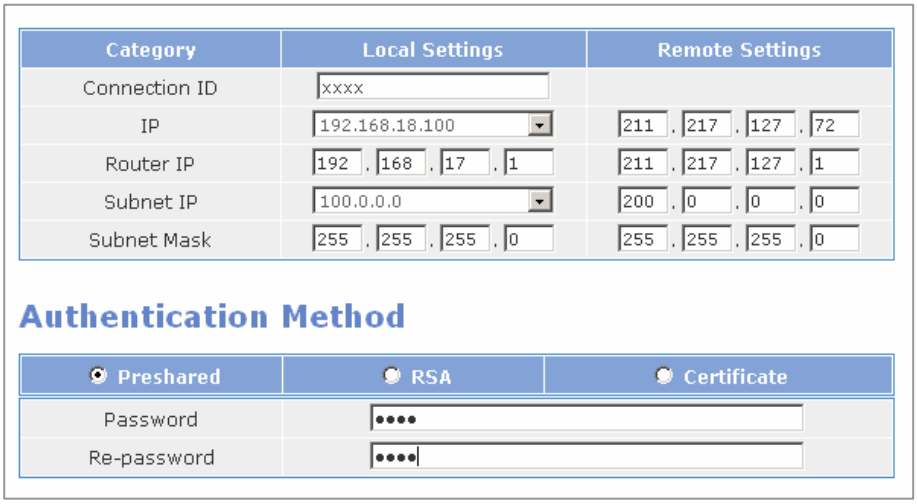


The menu buttons are defined as shown below:

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.



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’.

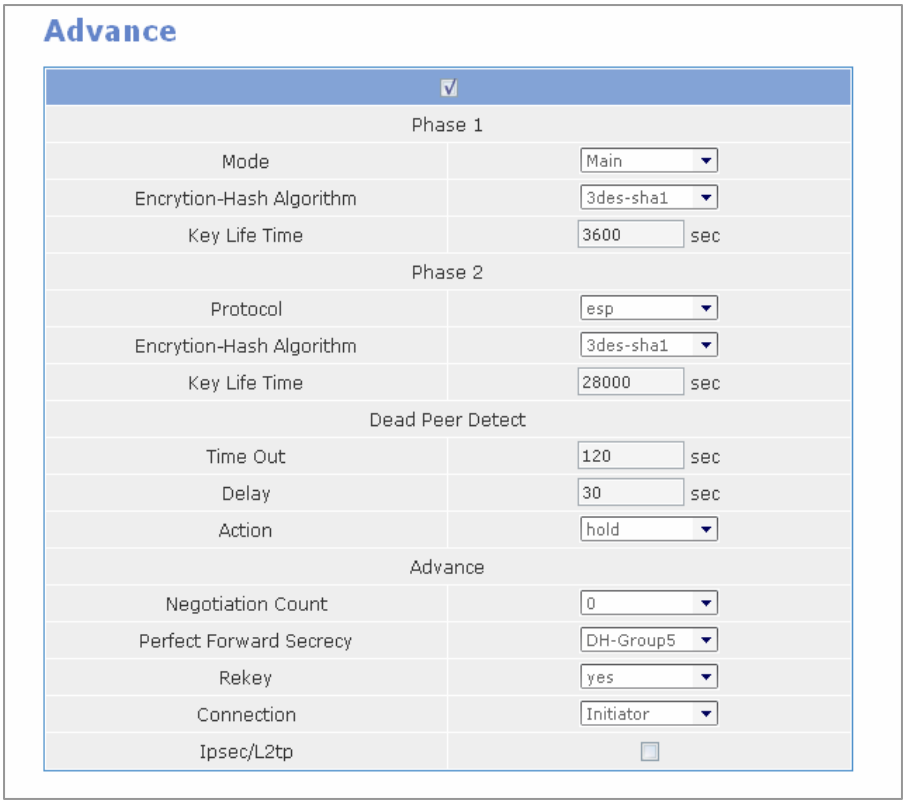
NOTE

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.

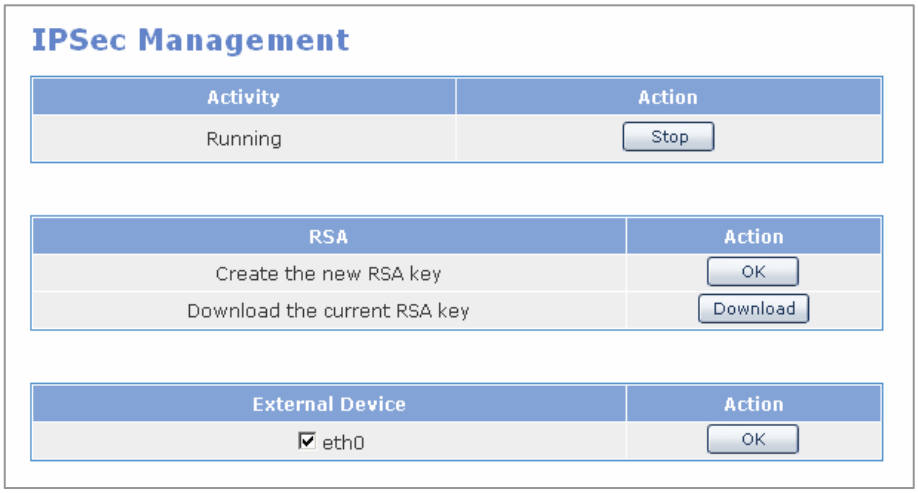


Item		Description
Phase1	mode	Ike mode - main: Configures a secure channel to perform the ISAKMP exchange of phase one - aggressive: Different type of phase one, which is more simple and faster than the main mode
	Encryption-Hash Algorithm	Supporting Algorithm 3DES-MD5, 3DES-SHA1, AES128-MD5, AES128-SHA1, 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/l2tp	Sets when IPSec over l2tpis 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.



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.

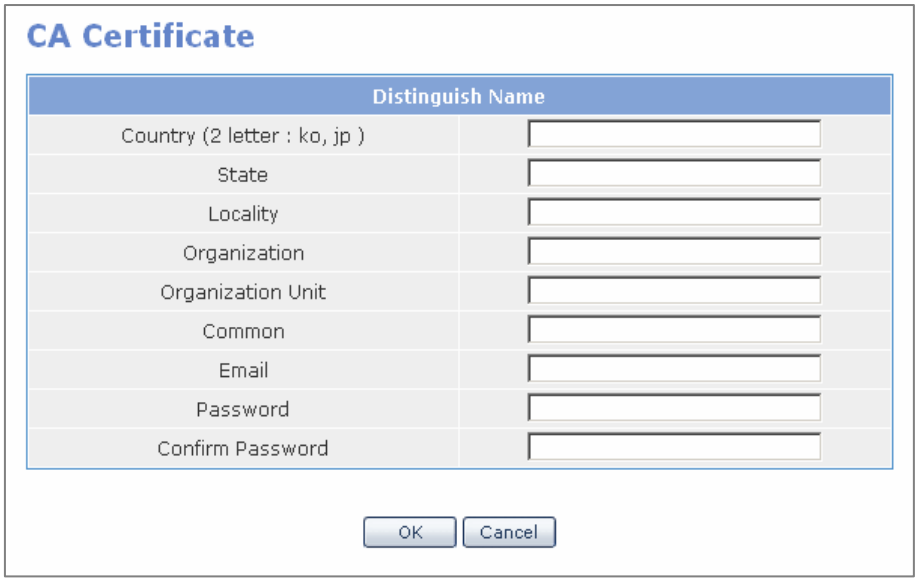
Certificate

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

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



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 uploaded items of an external certificate are defined as follows:

Item	Description
CA Certificate	External certificate upload

Host Certificate

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

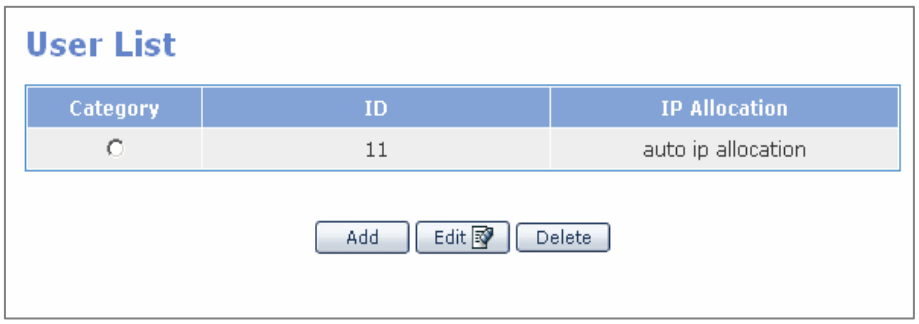
Item	Description
Common name	Name
Email address	Email address
Password	Certificate password
Confirm Password	Confirming certificate password

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.

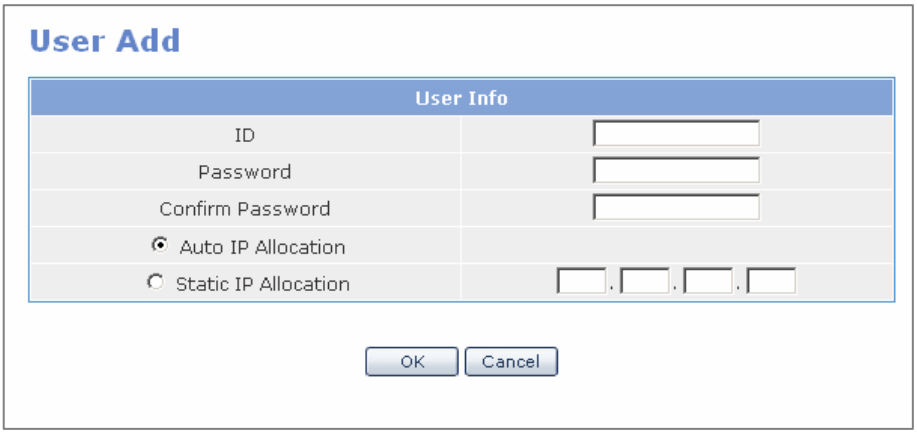


The menu buttons are defined as follows:

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

Add

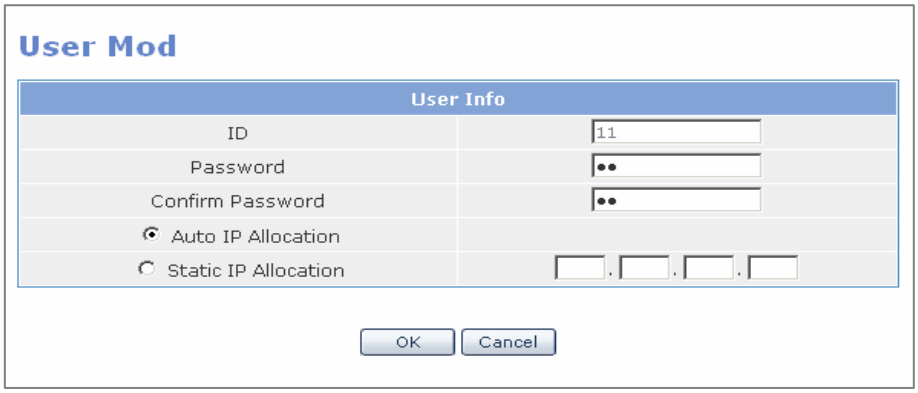
If clicking the **[Add]** button on the **<L2TP administrator list>** window, the following window appears. Enter each item and click the **[OK]** button to create a L2TP administrator.



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)

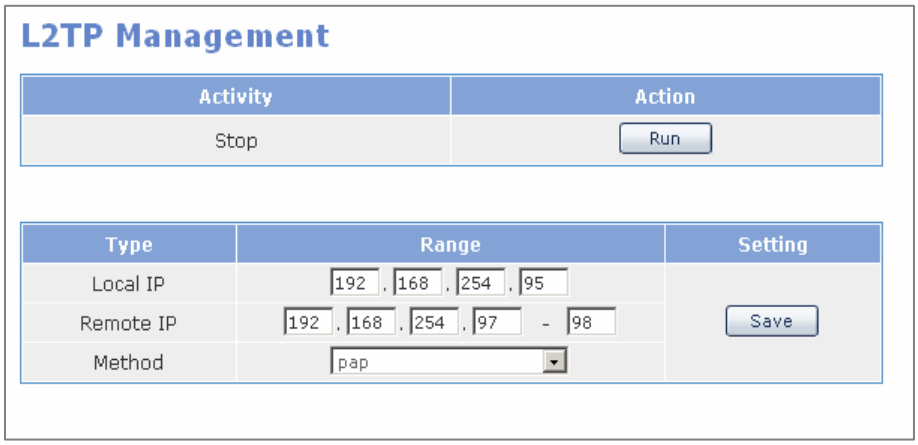
Edit

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.



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.



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.

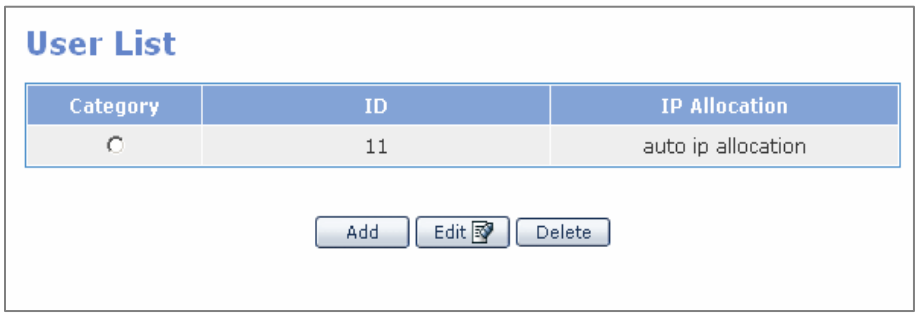
For example, if the number of IPs for 'Local IP range' is 10 and that for 'Remote IP range' is 20, only 10 calls will be set.

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.

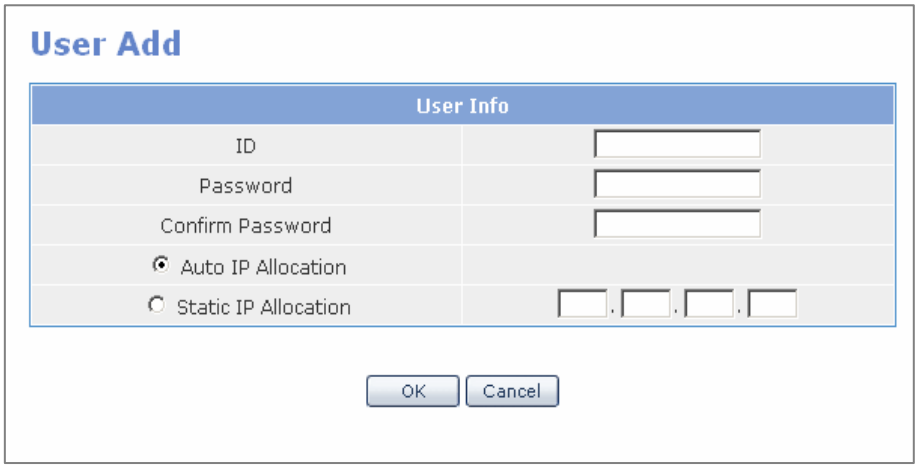


The menu buttons are defined as follows:

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

Add

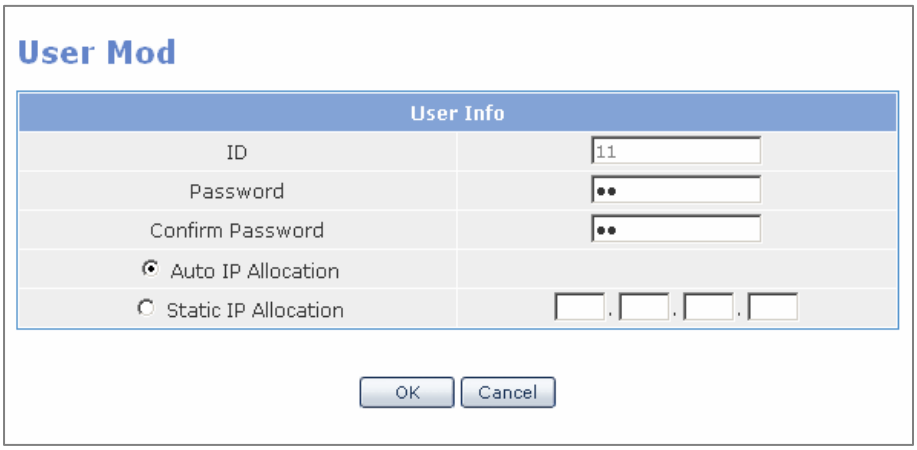
[Add] → **<PPTP administrator list>**



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)

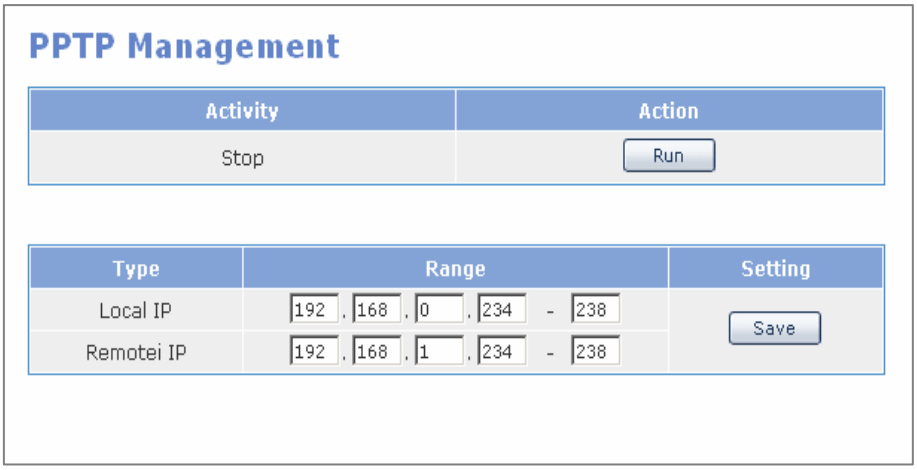
Edit

[Edit] → <Administrator List>



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.



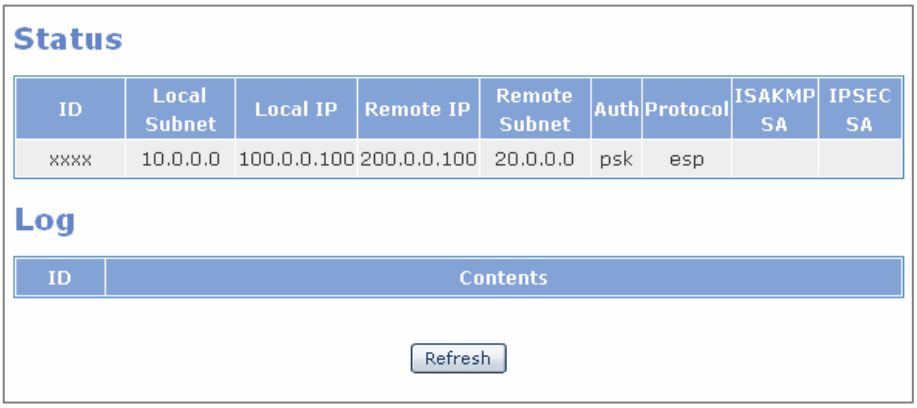
The administrator can set up the IP range of the remote client that uses dynamic IP in the 'Local IP range' item, and set up the IP range of PPP demon responsible for remote client in the 'Remote IP range' item. The encryption method supports 'pap' and 'chap'.

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.

Status

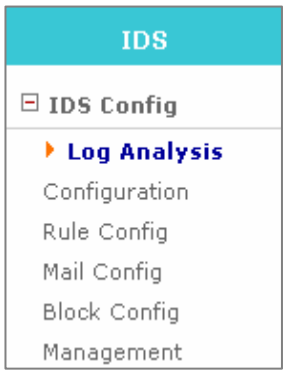


Check the IPSec tunnel set up in **[STATUS] → [IPsec]** to insure it is properly connected.

Check the L2TP/PPTP tunnel set up in **[STATUS] → [L2TP/PPTP]** to insure it is properly connected.

IDS Menu

If selecting the **[IDS** menu. The submenus will be displayed in the upper left side of the window as follows:

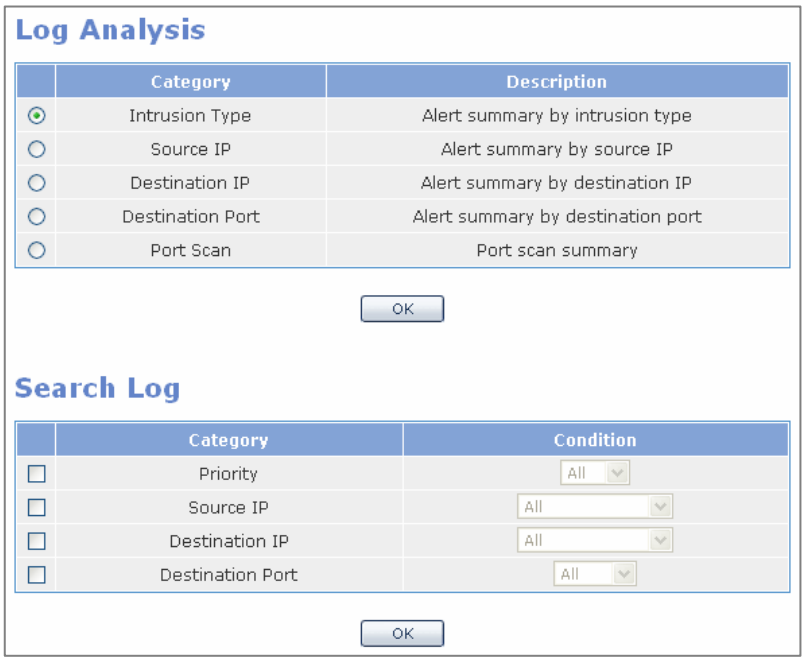


Menu	Submenu	Description
IDS Config	Log Analysis	Classifies the logs currently stored in types to verify and search the logs
	Configuration	Sets up the rule and detection level of IDS.
	Rule Config	Updates to new rule files.
	Mail Config	Registers the mail server and email address of the manager.
	Block 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

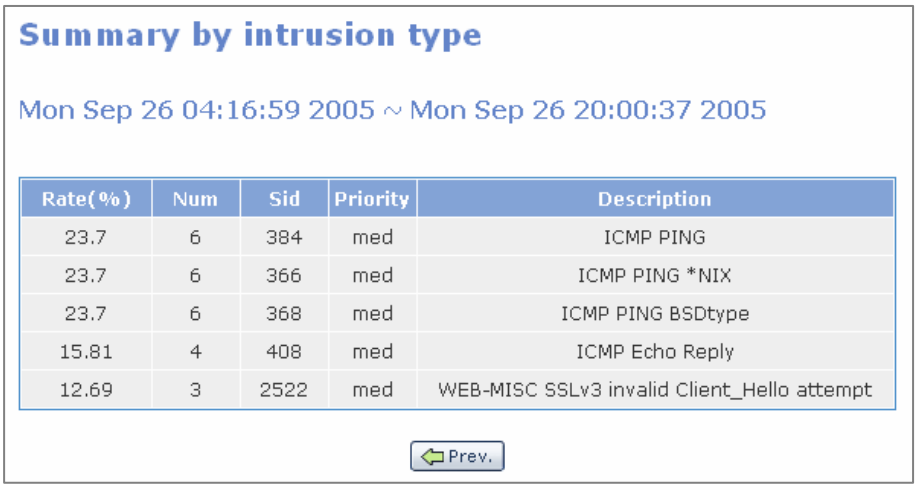
The administrator can view alerts detected in the IDS module by category. Select the desired category and click the **[OK]** button. Then, the following page appears.



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

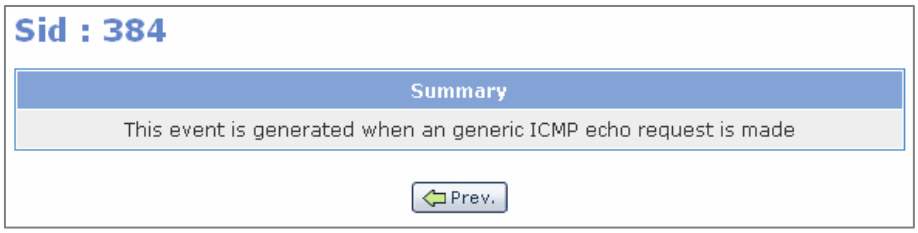
Intrusion Type

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



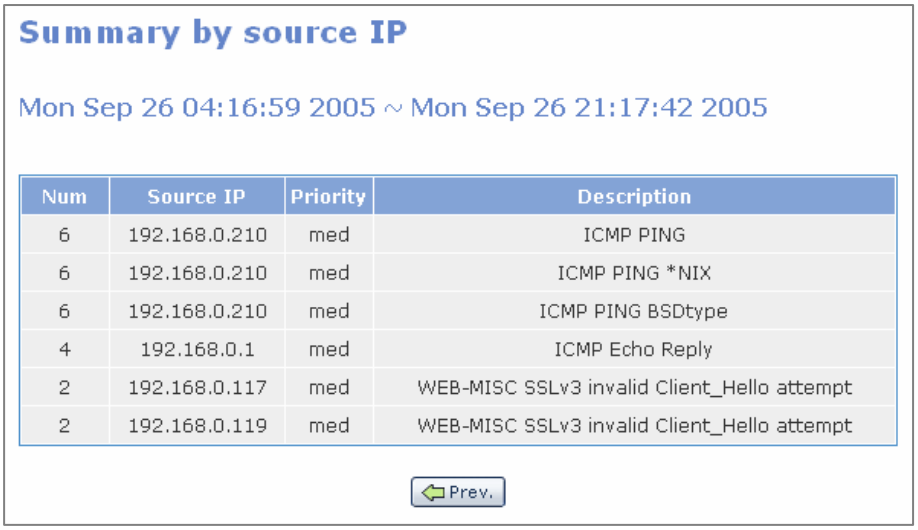
Item	Description
Rate(%)	Monitors logs detected by IDS according to type and displays logs as a percentage(%).
Num	Number of logs detected by IDS according to type.
Priority	Risk level depending on the rules level of IDS. - high: Rule level is one day(the highest risk level) - med: Rule level is 2 or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



Source IP

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



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

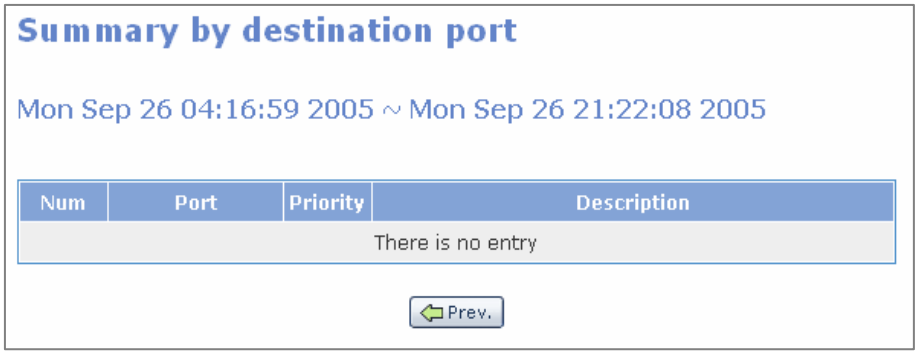
Destination IP

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

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

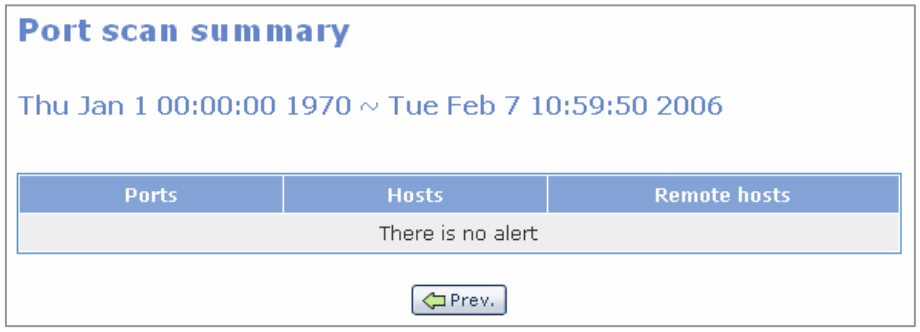
The administrator can summarize alerts by destination port. If selecting this category, the following category appears:



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

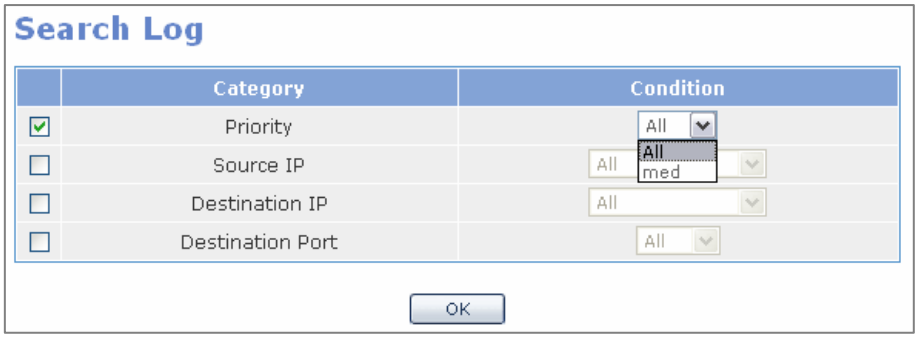
The administrator can summarize alerts for Port Scan. If selecting this category, the following window appears:



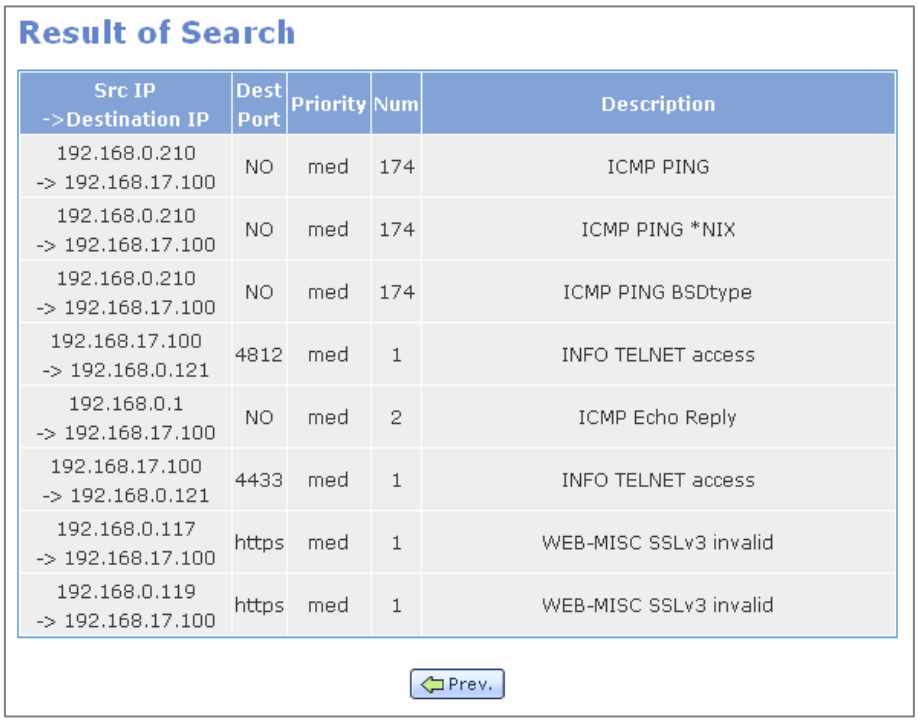
Item	Description
Ports	Number of TCP and UDP ports that are scanned in logs detected by IDS.
Hosts	Number of host that a port scanned in logs detected by IDS
Remote host	IP that attempts port scan

Search

The administrator can search by condition



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:



CHECK

Selecting Search Condition

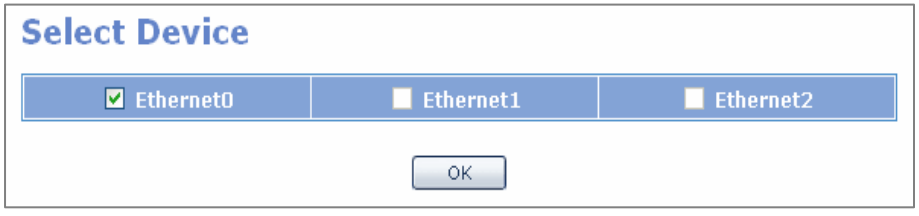
Since the conditions are not displayed dependently, the administrator cannot obtain a result that satisfies all conditions.

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.



Set Detection Level & Type

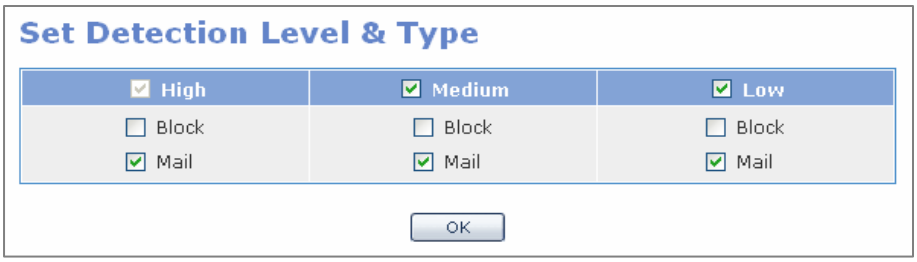
The intrusion type is classified into High, Medium and Low according to the risk level. The administrator can set up the intrusion detection level as alert is generated when an intrusion exceeding the level occurs. In addition, the administrator can set up the associated operation for each level.

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')

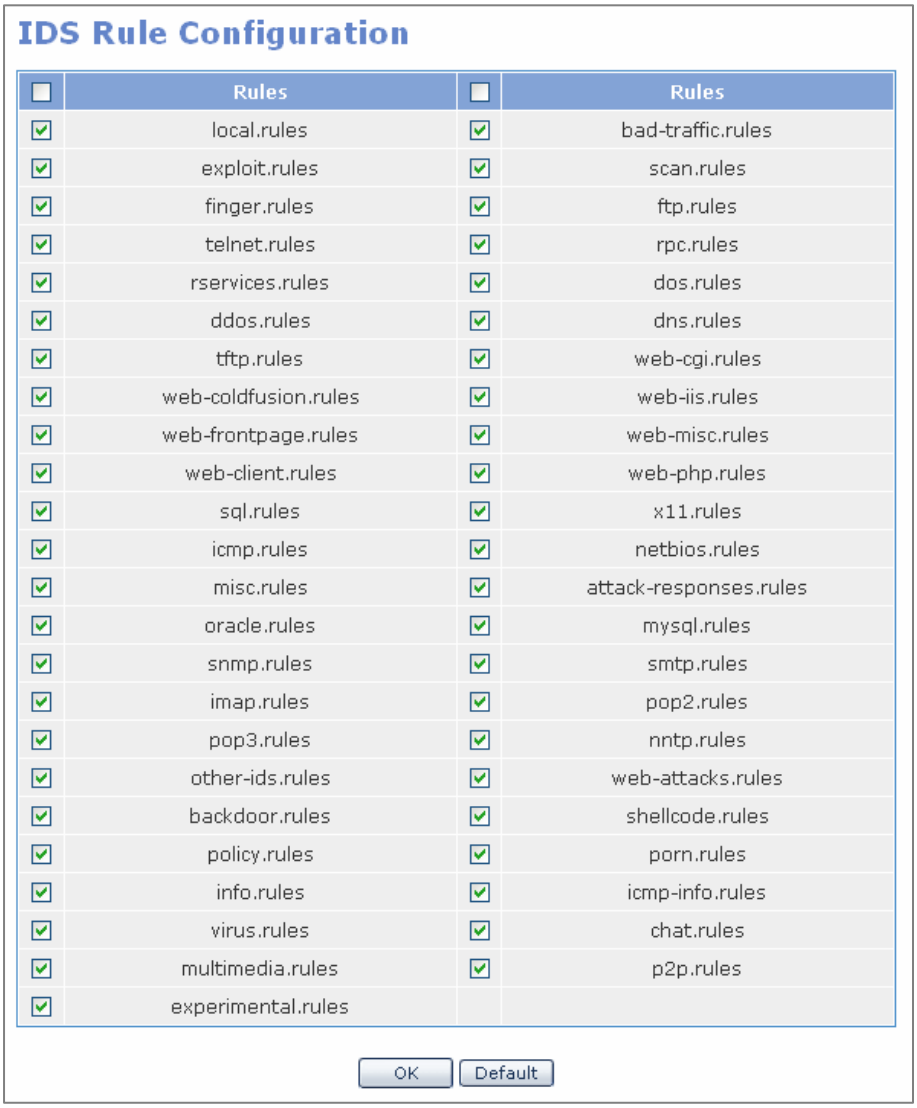
If setting up Mail, alerts are transferred when a mail is transmitted.

(Refer to 'Mail Config')



IDS Rule Configuration

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



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:

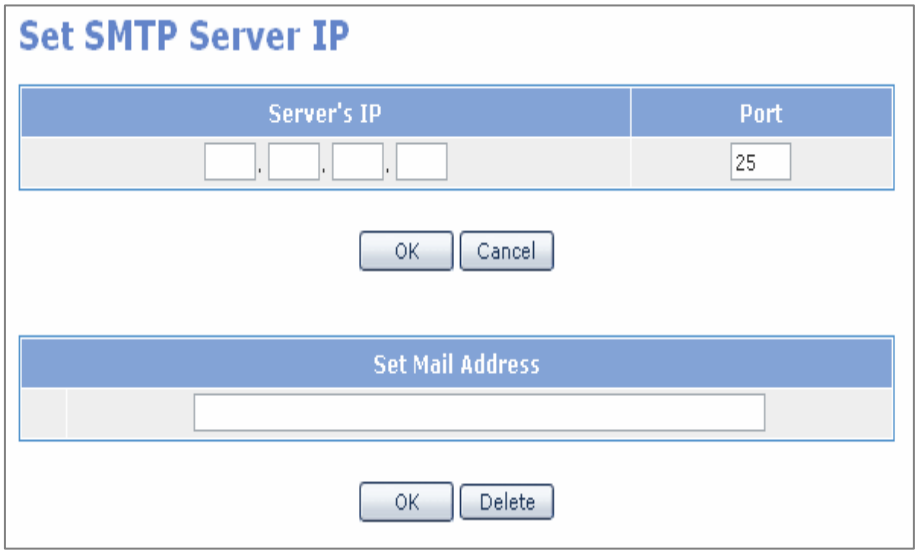
NOTE

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

Mail Config

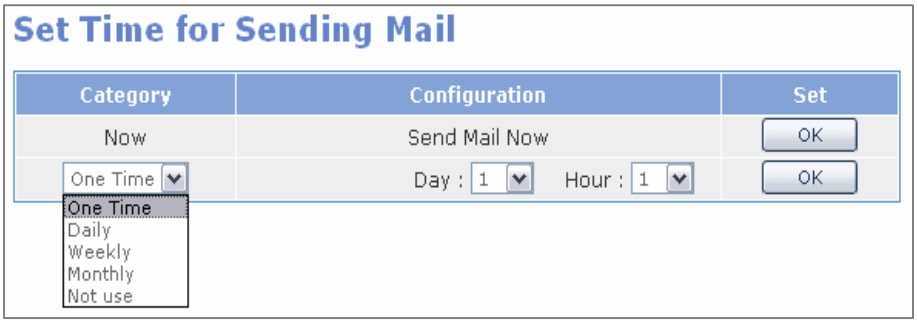
Set SMTP Server IP

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 Time for Sending Mail

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

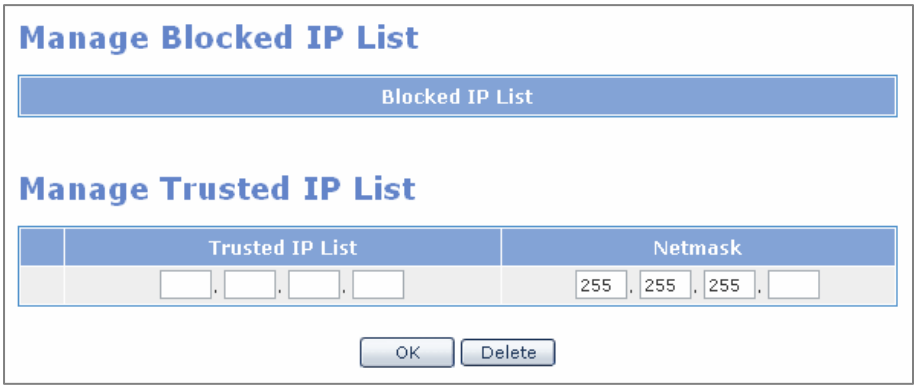


If clicking the button in the Now category, an email is sent to the e-mail address stored above the recorded alert. Select One Time to send a mail at the relevant time. The other items are used to check if there is an alert and send to Mail at the configured time daily, weekly or monthly.

> **CAUTION**
>
> **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

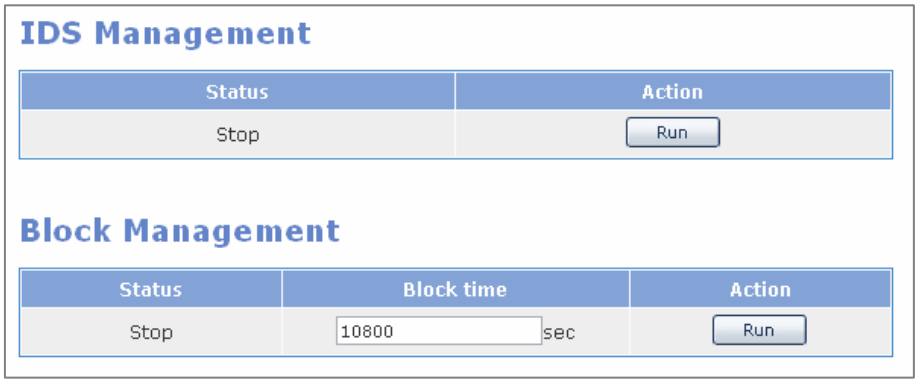
If an intrusion is detected when the IDS module and block module are all in operation, the IP of the block that is set up at Configuration Menu according to the intrusion risk, is blocked to access to the system for an amount of time. Manage Blocked IP List shows the list of IP that the access is blocked.

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

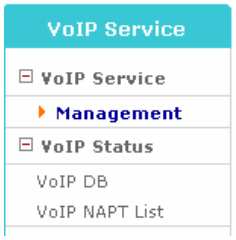
In this page, the administrator can set up the operation of the IDS module and block module.



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.

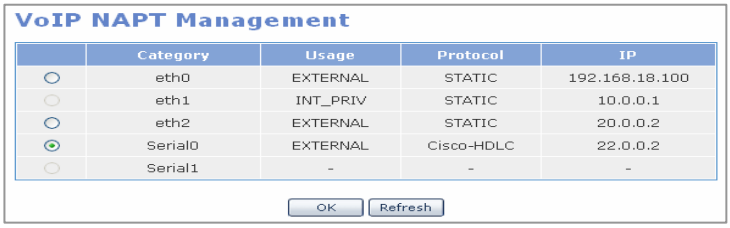
VoIP Service

Management

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

Item	Description
Activity	Current VoIP service status
Action	Command that currently can be executed

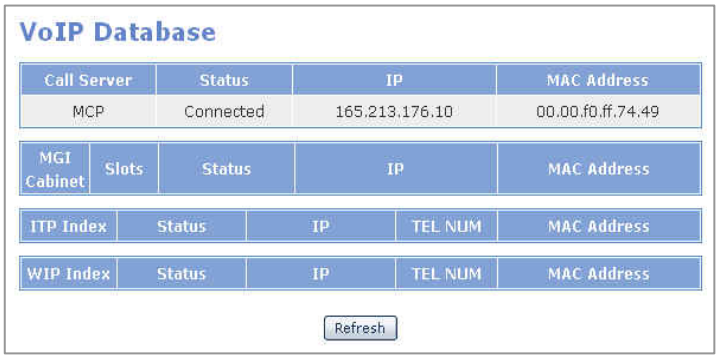
WAN interface can be selected. Last setting is restored even if the system reboots. When the information on the selected WAN interface is changed, WAN interface is automatically set.



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.



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.

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:

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)

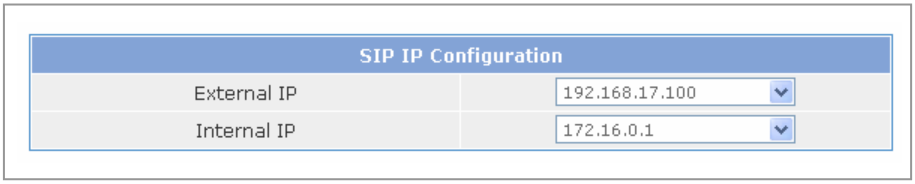
Typically, if a firewall protects internal network based on NAT such as the GWIM module of OfficeServ 7400, SIP AGP(SIP aware ALG) is safe from external attacks and resolves the limits on the services so that SIP devices of a firewall can communicate with external devices.

Config

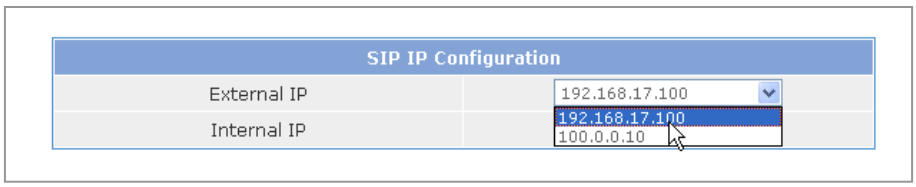
In this page, the administrator can set up the SIP environment on the **[Config]** menu. Set up the following items and click the **[Save]** button.

SIP Configuration

This page displays firewall installation data.

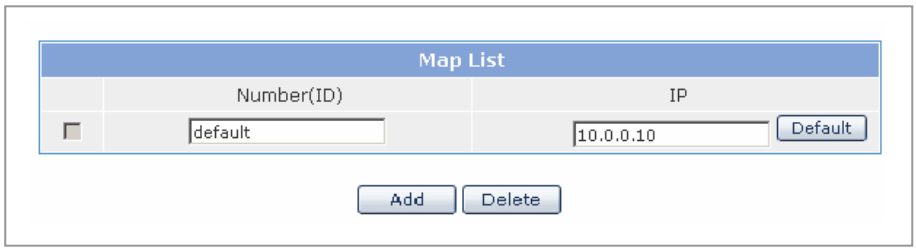


The external IP and internal IP items are displayed on the list box so that the web manager collects and selects the usable information from the firewall configuration.
If the external or internal network is two or more, it is available to select the desired network to be the list box as follows:

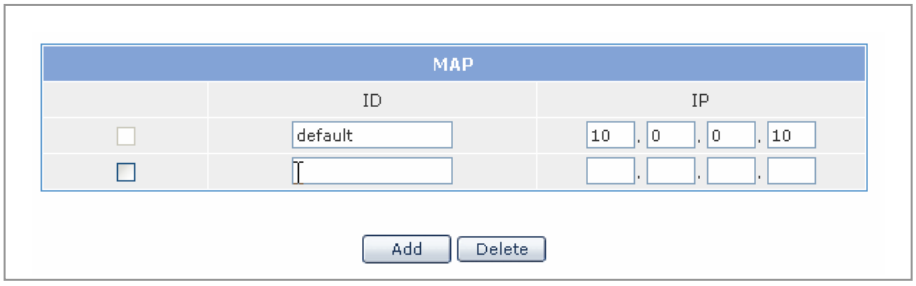


Map LIST

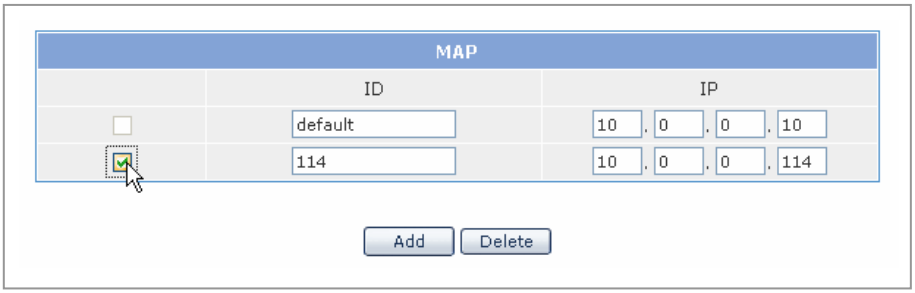
Enter SIP devices data inside of the firewall.



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.



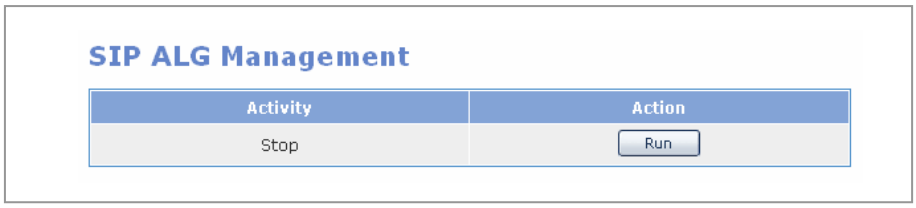
Clicking the **[Add]** button will allow you to add additional Map information.



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.



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

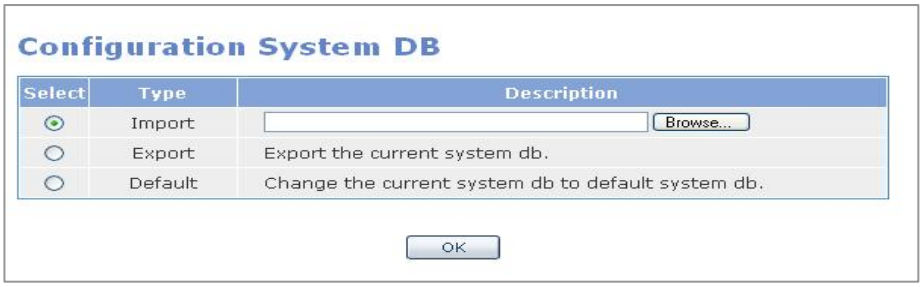
System Menu

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

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]

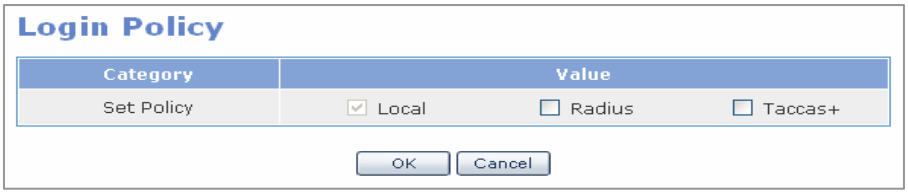


Item	Description
Import	Restore a previously saved database
Export	Saves the existing DB
Default	Restore the DB to factory defaults

After defaulting the DB the adminstrator 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.

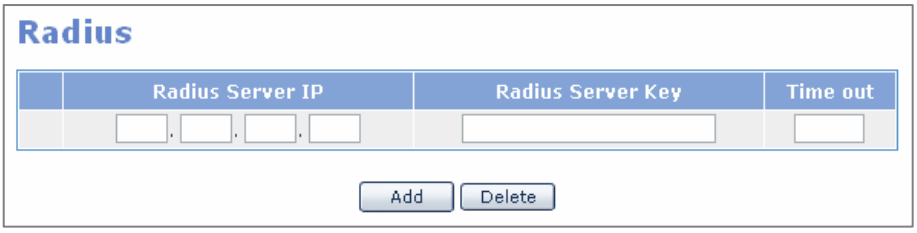


Local

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

Radius

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



Taccas+

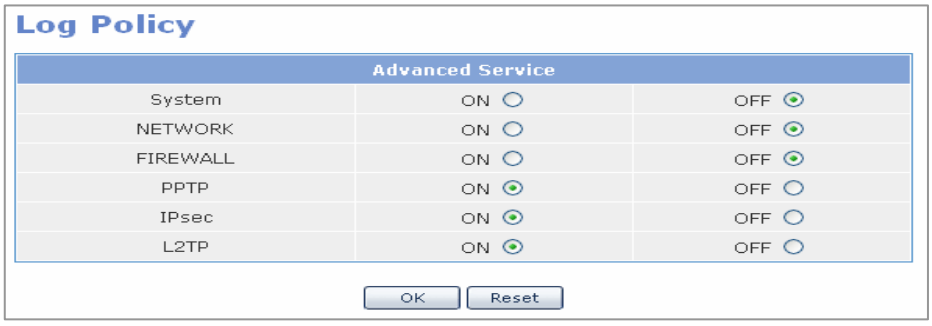
Enter the information on the Taccas+ authentication. Up to 5 lists can be entered or deleted. When deleting the list of all server IPs, the corresponding secret key values are also deleted.

Log

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

Configuration

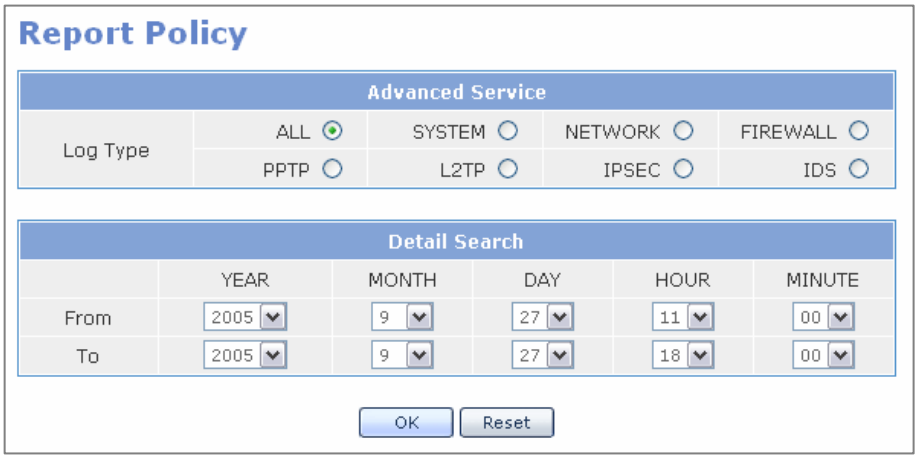
This page allows setting up the log to determine whether to add a log to the system.



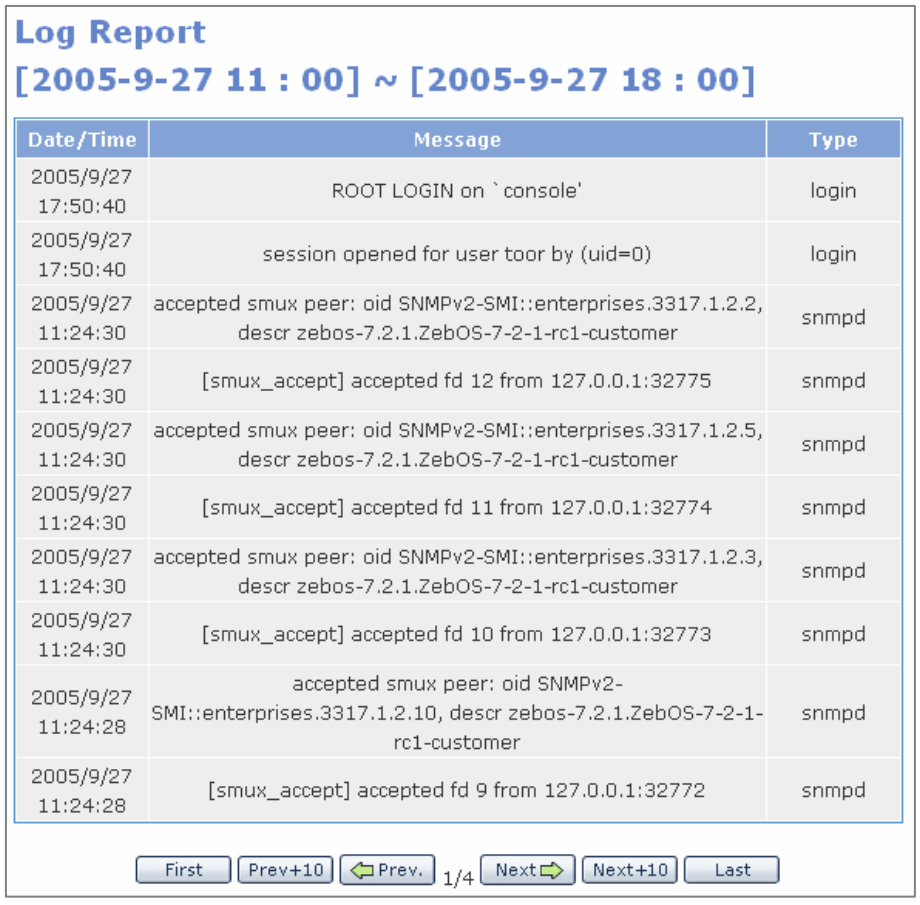
Select added logs from the logs for system log, network, firewall, VPN, and click the **[OK]** button to add logs to the system log. Click the **[Reset]** button to return to the previous status before applying the configuration.

Report

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

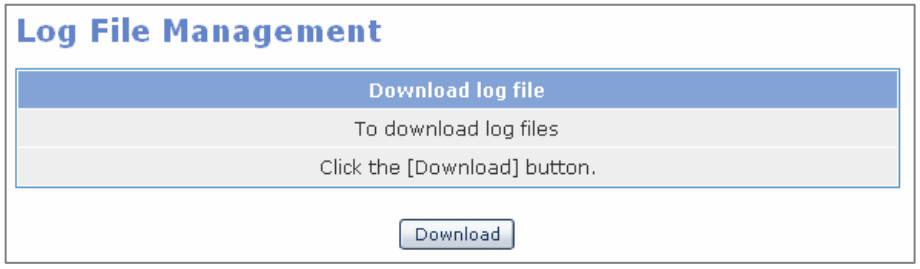


Set up the desired log type and time and click the **[OK]** button to verify the log. Click the **[Reset]** button to return to the previous status.



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.

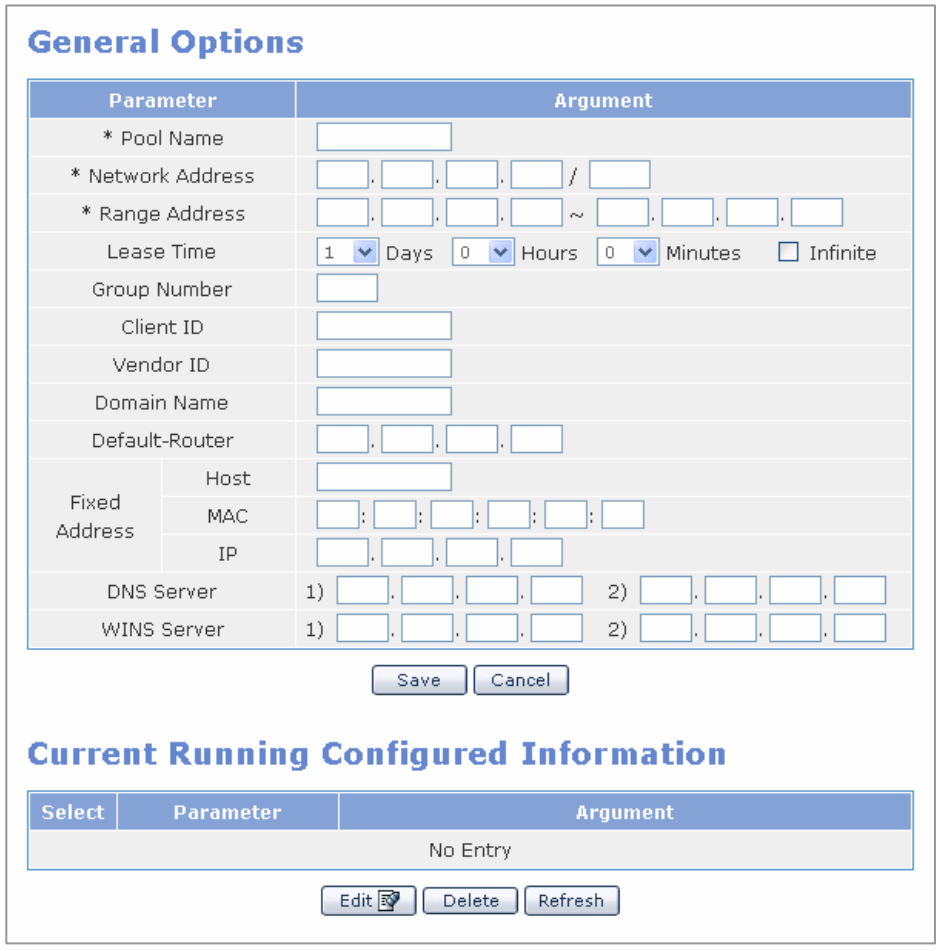


DHCP Server

[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.



The configuration options are as follows:

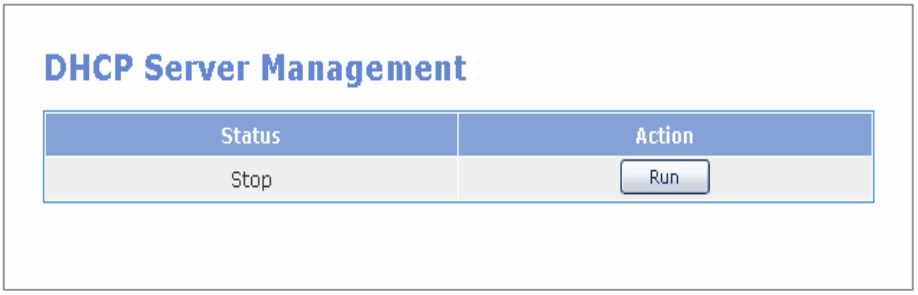
Item		Description
*** Pool Name**		Sets up the name of Pool to distinguish from the other Pools.
*** Network Address**		The value of a Network to be set up. The value is classified into IP type and Netmask.
*** Range Address**		Sets up the range of IP addresses that DHCP Server allocates to DHCP Client. 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.

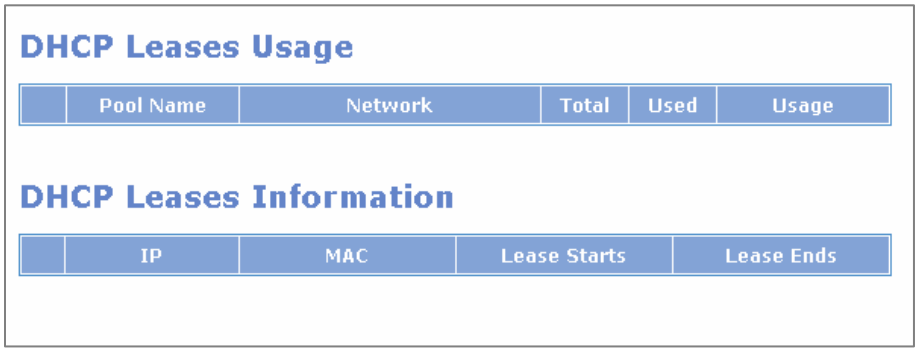
Management

This page allows managing the operation of DHCP Server.



Lease Info

The Lease Info window shows the active Lease information.



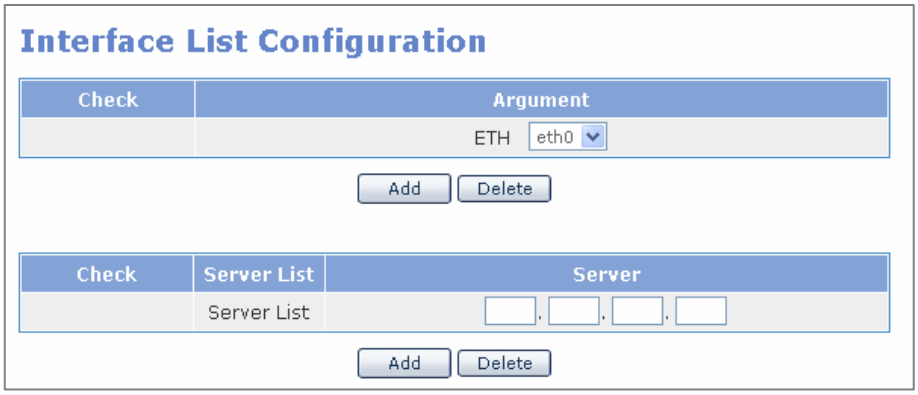
DHCP Relay Agent

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.



Management

This page starts/stops the DHCP daemon.

Time Configuration

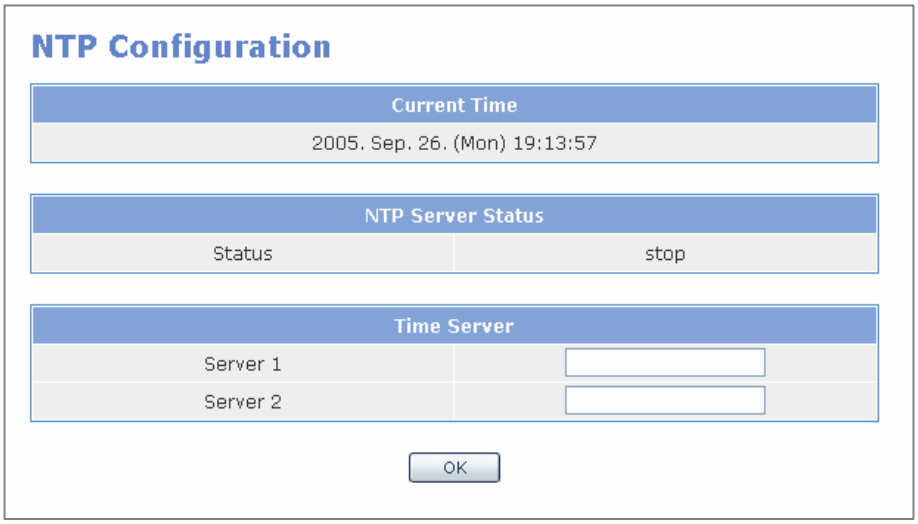
Synchronize the date and time of the system on the **[Time Configuration]** menu of the **[System]** through a network or manual configuration.

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.

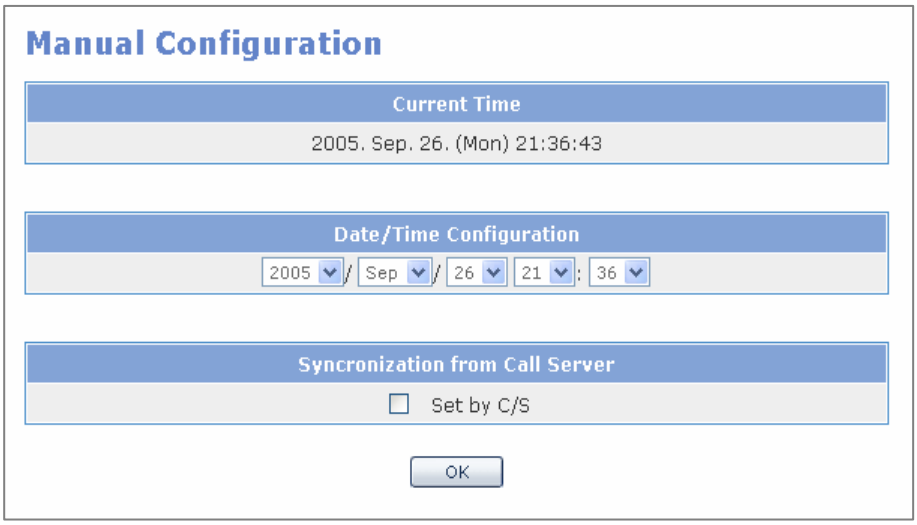


- Current Time indicates the current time of the system.
- NTP Server Status indicates the execution status of NTP Demon.

- 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.

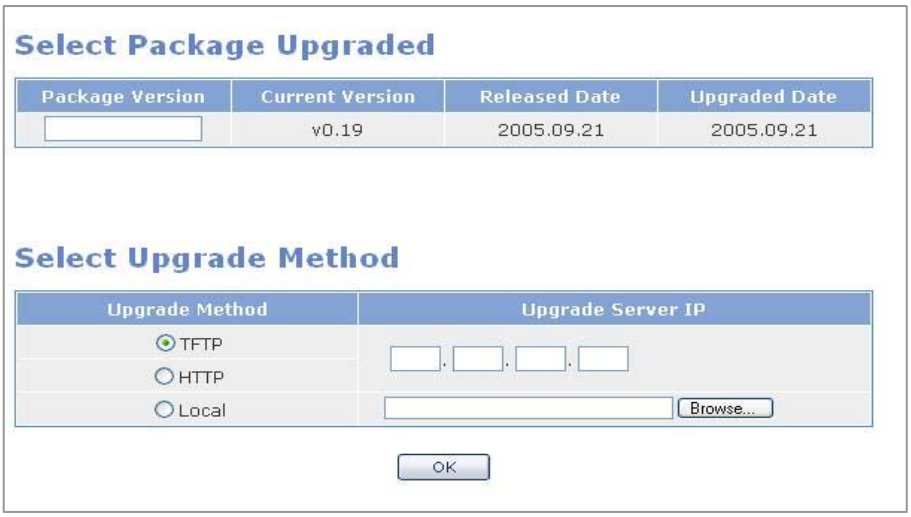


Timezone

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.

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.

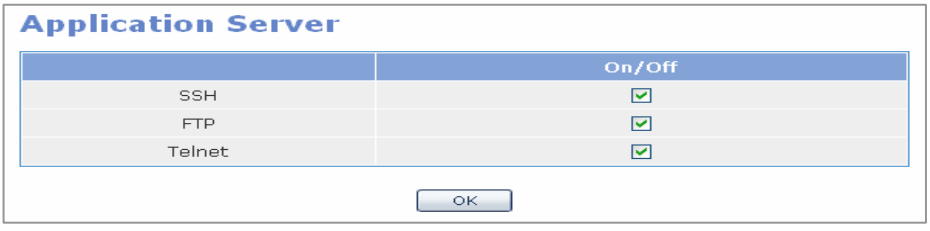


When upgrading a package, the package version should be entered in the type such as 'v0.19' in the **[Package Version]** field.

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.



Reboot

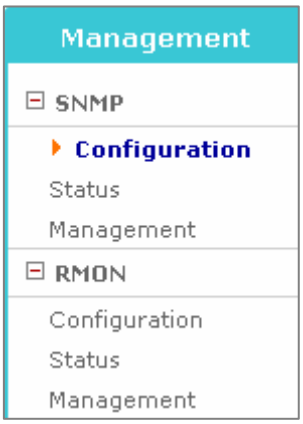
The administrator can reboot the system in the **[Reboot]** menu.

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.

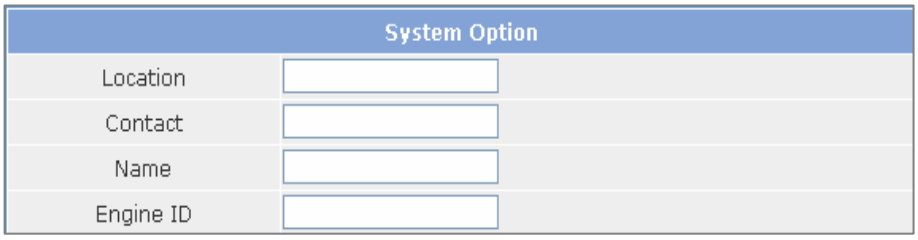
SNMP

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.



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

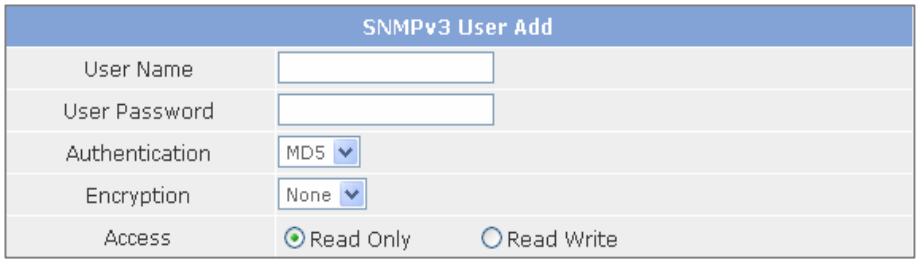
Community

Add new community used in SNMP v1/2c.

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 a administrator to be used at SNMP v3.



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.

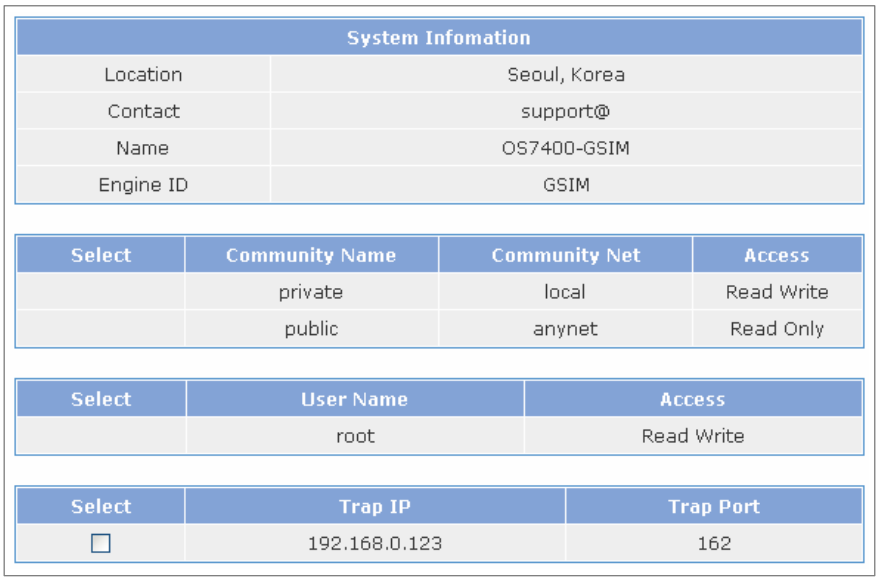
Item	Description
IP Address	Set up new Trap IP Address to add.
Community Name	Set up a community to be used for transmitting to the Trap IP Address added.

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

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

Select	User Name	Access
	root	Read Write

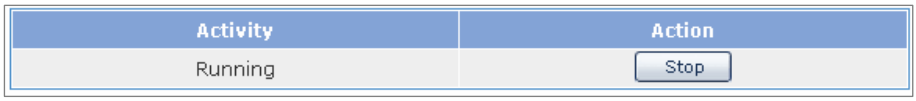
Select	Trap IP	Trap Port
☐	192.168.0.123	162

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



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.

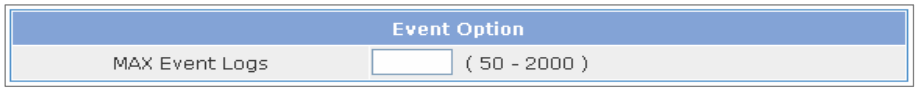
History Option

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.

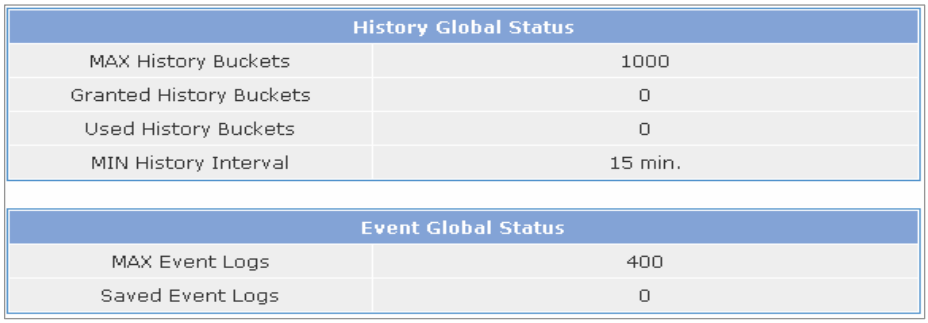


Item	Description
Max Event Logs	Sets up the maximum number of Event Logs.

Status

[RMON] → [Status]

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



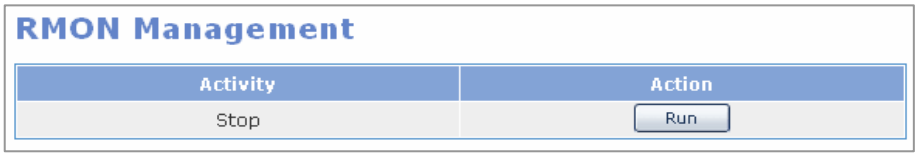
Item	Description
MAX History Buckets	Displays the maximum history storage space that has been set up.
Granted History Buckets	Displays the history storage space that is currently allocated.
Used History Buckets	Displays the history storage space that is currently used.
MIN History Interval	Sets up the 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

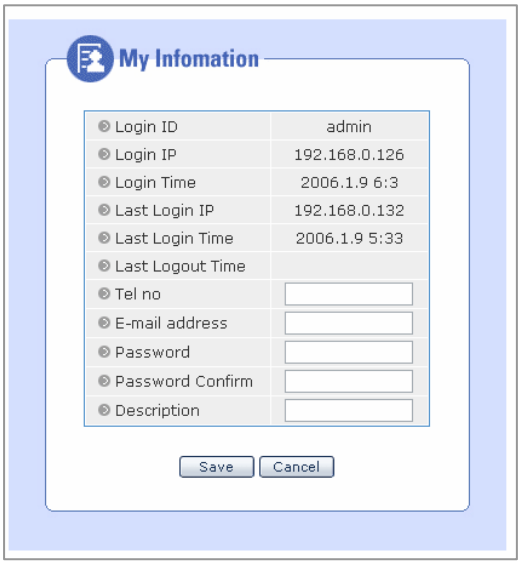
The administrator can start/stop the RMON service.



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 desciption 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.



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 Pointv
RSTP	Rapid Spanning Tree Protocol

P

PAP	Password Authentication Protocol
PIM-SM	Protocol Independent Multicast-Sparse Mode
PD	Power Device
PoE	Power Of Etnernet
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