OfficeServ 7200

Data Server User Guide

Every effort has been made to eliminate errors and ambiguities in the information contained in this booklet. Any questions concerning information presented here should be directed to SAMSUNG TELECOMMUNICATIONS AMERICA. SAMSUNG TELECOMMUNICATIONS AMERICA disclaims all liabilities for damages arising from erroneous interpretation or use of information presented in this manual.

PUBLICATION INFORMATION

SAMSUNG TELECOMMUNICATIONS AMERICA reserves the right without prior notice to revise information in this publication for any reason.

SAMSUNG TELECOMMUNICATIONS AMERICA also reserves the right without prior notice to make changes in design or components of equipment as engineering and manufacturing may warrant.

COPYRIGHT 2006

TRADEMARKS

INTRODUCTION

Purpose

This document introduces the OfficeServ 7200 Data Server, an application module of OfficeServ 7200, and describes procedures on installing and using the software.

Document Content and Organization

This document contains three chapters one annex and an abbreviation as follows:

CHAPTER 1. OfficeServ 7200 Data Server Overview

This chapter briefly introduces the OfficeServ 7200 Data Server Data Server.

CHAPTER 2. OfficeServ 7200 Data Server Installation

This chapter describes the installation procedure and login procedure.

CHAPTER 3. Using the OfficeServ 7200 Data Server

This chapter describes how to use the menus of the OfficeServ 7200 Data Server Data Server.

ANNEX A. VPN Setting in Windows XP/2000

This chapter describes how to set up a VPN on Windows XP/2000.

ABBREVIATION

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 is 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 7200 General Description

The OfficeServ 7200 General Description Guide introduces OfficeServ 7200 and describes the system information necessary for the understanding of this system, such as hardware configuration, specification, and function.

OfficeServ 7200 Installation Manual

The OfficeServ 7200 Installation Manual describes the condition necessary for the installation,of the system and how to inspect and operate the system.

OfficeServ 7200 Call Server Programming Manual

The OfficeServ 7200 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
01	10.2006	First Version

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.

DB Change

When the DB is changed in the OfficeServ 7200 GPLIM, the system will restart.

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

Cautions before operating the IDS Module

The alert of the IDS Module is remained in the system log. Therefore, the IDS Item should be set to **[On]** in the **[System]** → **[Log]** → **[Configuration]**. If not so, the alert is not remained, and whether the intrusion that is detected cannot be confirmed.

. **When Deleting Internet Temporary Files**

If the Data server 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 Data Server may not be displayed correctly.

When Using a Web Browser

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

TABLE OF CONTENTS

CHAPTER 1. Overview of OfficeServ 7200 Data Server

This chapter introduces the OfficeServ 7200 system and OfficeServ 7200 Data Server.

Introduction to the OfficeServ 7200

The OfficeServ 7200 is a single platform that delivers the convergence of voice, data, wired and wireless communications for small offices. This ‘office in a box’ solution offers TDM voice processing, voice over IP integration, wireless communications, voice mail, computer telephony integration, data router and switching functions, all in one powerful platform.

The OfficeServ 7200 Data Server provides the network functions of a switch, router, and network security.. This document describes the data and routing capabilities of OfficeServ 7200 Data Server.

OfficeServ 7200 Configuration

For information on the configuration, features, or specifications of the OfficeServ 7200, refer to the ‘OfficeServ 7200 General Description ’.

Introduction to the OfficeServ 7200 Data Server

The OfficeServ 7200 Data Server provides the following functions:

Unmanaged Switch

- The switch performs the function of a layer 2 Internet switch as well as the Learning Bridge function based on the MAC address filtering and forwarding algorithm.
- The LIM module provides 16 LAN ports per module. Each port is 10/100 Base T, auto sending, full duplex. OS 7200 can support up to 8 unmanaged LIM.

Managed Switch

When the LIM is installed in slot 2 with a Data Server in slot 1, it can function as a managed switch by using an access interface LAN on the Data Server. OfficeServ 7200 supports 1 managed LIM.

As a managed switch, the following features are support:

- 802.1D Spanning Tree – The switch configures and processes the forwarding tree based on the spanning tree algorithm to prevent a packet forwarding loop in the switch.
- Layer 2 802.1p Packet Priority QoS – The switch extracts the priority field from the Ethernet frame configured according to the 802.1p specification standard, and discriminatively processes the frame according to the priority of the specified operation. The switch then maps packets to a designated queue. Up to 2 output queues, Low and High, are supported per egress port with queuing type of Weighted Round Robin or All High before Low. For devices that do not support 802.1p, OS 7200 LIM can be configured to create an enforceable priority.
- Supports Virtual LAN (VLAN) – The Virtual Local Area Network (VLAN) groups the related equipment by the work group according to the LAN operational policy regardless of the location of the user equipment. VLAN removes the effects of unnecessary broadcasting packets and configures a stable switching subnet only for the corresponding group by separating and processing the group in the virtual LAN. The VLAN can be configured based on the switch port, MAC address, and 802.1Q tag.
- IGMP Snooping – IGMP Snooping provides a method for intelligent forwarding of multicast packets within a layer 2 broadcast domains. By snooping IGMP registration information, a distribution list of work stations is formed that determines which end-stations will receive packets with a specific multicast address.
- 802.3x Layer 2 Flow Control – Flow control is performed according to the value set for incoming rate and/or outgoing rate. Limiting the rate at which a port can receive or send traffic is used to ease congestion on bottlenecks in the network and provide simple prioritization when the network is busy.

Router Functions

- Manages paths and performs queuing for data packets on both external WAN and internal LAN
- Performs static or dynamic routing.
- Supports RIPv1(Routing Information Protocol version1), RIPv2, and OSPFv2(Open Shortest Path First version2),
- Functions as a client such as Dynamic Host Configuration Protocol(DHCP), Point-to-Point Protocol(PPP), and Point-to-Point Protocol over Ethernet (PPPoE) over the Ethernet WAN interface.
- Performs High-level Data Link Control(HDLC), PPP, or frame relay encapsulation over the Serial WAN interface.
- Supports IP multi-casting
  - Supports IGMPv1(Internet Group Management Protocol version1), IGMPv2 protocol
  - Supports DVMRP(Distance Vector Multicast Routing Protocol), PIM-SM(Protocol Independent Multicast-Sparse Mode) multicast routing protocol
- Performs functions by using an access interface for WAN.
  - 3-10/100 Ethernet Ports: Used for WAN or LAN interfaces
  - 1-10-Base T Ethernet Port Used for WAN or LAN Interface
  - 1-Serial WAN Port: Used for a private data line by connecting a data circuit unit such as DSU and CSU(supports V.35)
- Network Load Balance(NLB) Function
  - Enables to distribute the load equally by specifying multiple Gigabit Ethernet lines or Serial interfaces as WAN and raise the availability by automatically sharing the load to the other lines when a line does not work.

Data Network Security

- Outbound and Inbound NAT(Network Address Translation)/PT(Protocol Translation)
  - Controls an access to internal resources through conversion between the Global IP and Private IP
- Firewall
  - Controls an access from outside by the extended access list.
  - Intrusion Detection System(IDS)
  - Detects and notifies an access to unauthorized areas by the access list
  - Recognizes and notifies unauthorized packets by applying the basic intrusion rule for packets.
  - Detects and blocks DoS attacks such as SYN flood.
- Virtual Private Network(VPN)
  - Function as a VPN gateway based on PPTP(Point-to-Point Tunneling Protocol), L2TP(Layer 2 Tunneling Protocol), IPSec(Internet Protocol Security protocol)
  - Performs privacy and integrity through VPN tunneling and data encryption.

Data Network Application

- Functions as data network applications such as NAT/PT, Firewall, VPN, DHCP, and Application Level Gateway(ALG)
- Executed as application software that operates in the Data Server board
- Application Level Gateway(ALG)
  - Supports ALG for VoIP signaling and media traffic, allowing flawless VoIP packets to be transferred while the security function is active.
- DHCP Server
  - Automatically sets network environment for IP equipment on other functional blocks of the OfficeServ 7200 system.
- DHCP Relay Function
  - Enables to connect to external DHCP server for automatic network environment setup of IP units in the other function block of the OfficeServ 7200 system.

QoS Function

- Performs the treatment of the priority for the second layer frame under 802.1p standards(Switch function)
- Treats the priority queue for the third layer packet and performs the priority queue for a specified IP.
- Treats the priority queue for the fourth layer packet and performs the priority queue for RTP packet.(UDP/TCP Port)

Management Function

- Supports a specialist level debugging function through Telnet connection
- Supports configuring and verifying the functional block operations of the data server through a browser
- Exchanges IDS data and alarm data with the system manager
- Execute program upgrade through local administrator PC
- Program upgrade
  - Upgrades program through TFTP
  - Upgrades program through HTTP

CHAPTER 2. Installing the OfficeServ 7200 Data Server

This chapter describes the installation and login procedures for the OfficeServ 7200 Data Server.

Software Installation

OfficeServ 7200 Data Server software is pre-installed. The software package is composed of the following items described below:

Package	File	Description
Bootrom Package	Data Server-bootldr.img-vx.xx Data Server-bootldr.img-vx.xx.sum	Boot ROM program
Main Package	Data Server-pkg-vx.xx.tar.gz	Upgrade package for HTTP
	Data Server-os..img-vx.xx	Upgrade package of 'OS' partition for TFTP
	Data Server-firmware.img-vx.xx	Upgrade package of 'firmware' partition for TFTP
	Data Server-configdb.img-vx.xx	Upgrade package of 'configdb' partition for TFTP
	Data Server-logdb.img-vx.xx	Upgrade package of 'longdb' partition for TFTP
	Data Server-flash1.img-vx.xx Data Server-flash1.img-vx.xx.sum	File to copy to the first flash memory(fusing)
	Data Server-flash2.img-vx.xx Data Server-flash2.img-vx.xx.sum	File to copy to the second flash memory(fusing)

Software Package Configuration

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

Data Server Installation

Setup the environment as follows to access the Data Server.

1. Insert the Data Server board into slot 1 and the LIM board on slot 2 of the OS 7200 cabinet.

   - When installing the Data Server board set the connections of shunt pin #1, 2, 3 and 4 to the direction of the back panel to connect the Data Server board and the LIM board via the back panel. In this case, the LAN port is de-activated if the UTP cable is connected to the port.
   - If the shunt pins of JP1, 2, 3 and 4 are towards the front direction of the Data Server board connect the LAN port of the Data Server board and a certain port of the LIM board to the LAN cable.

2. With a Cross Over cable connect a PC to port #1, 2, or 4 of the Data Server module or with a straight cable connect a PC to a port of the LIM board (Tied to Port 3). The programmer will need to configure the TCP/IP settings to match the corresponding default IP address of the Data Server shown in step 3.

3. Using Internet Explorer navigate to one of the folling IP addresses to access the management interface of the Data Server.

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

   - P1 - (Ethernet 0) 10.0.0.1/24 (https://10.0.0.1)
   - P2 - (Ethernet 1) 10.0.1.1/24 (https://10.0.1.1)
   - P3 (LIM) - (Ethernet 2) 10.0.2.1/24 (https://10.0.2.1)
   - P4 – (Ethernet 3) 10.0.3.1/24 (https://10.0.3.1)

CAUTION

Caution for the Use of a Web Browser

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

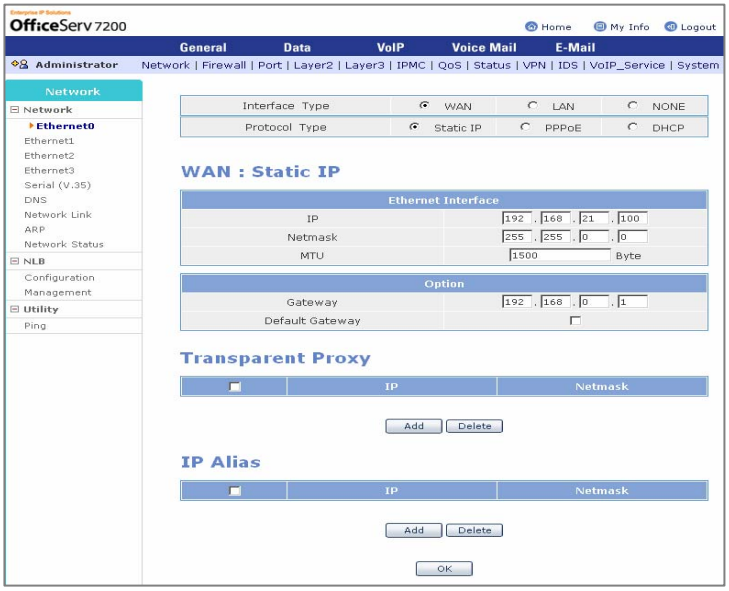
Getting Starting

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

2. Login using the administrator ID and password. The following window will appear: (The default administrator name is “admin” and the default password is “admin”.)

Click the **[Logout]** button on the upper right section of the window to close the connection to the Data Server .

3. Click on the **[Data]** button to use the menus for the Data Server shown in the following window:

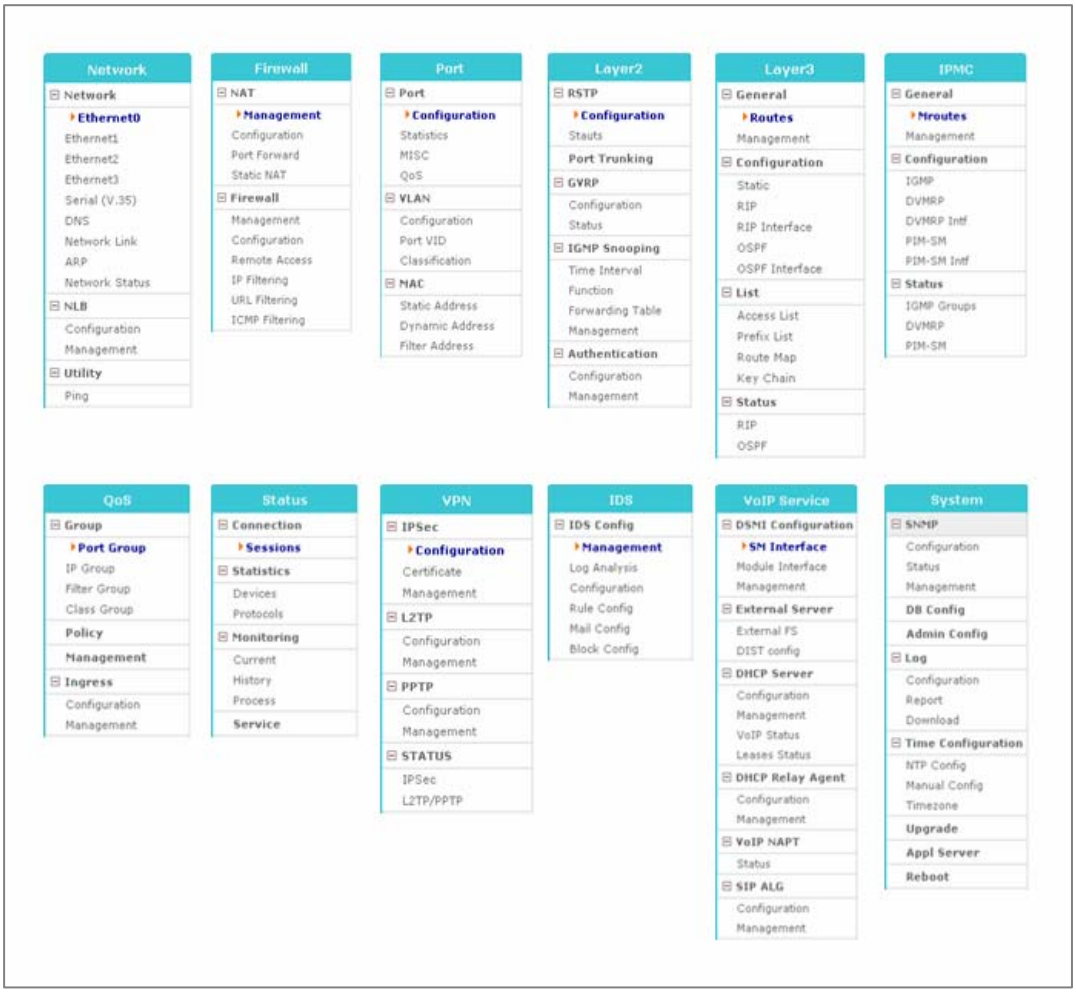


When the 'Data' button is clicked the Network menu is automatically selected and the submenus of the Network Menu appear on the left section of the window. Descriptions on each submenu is provided in 'Chapter 3. Using the OfficeServ 7200 Data Server.

CHAPTER 3. Using the OfficeServ 7200 Data Server

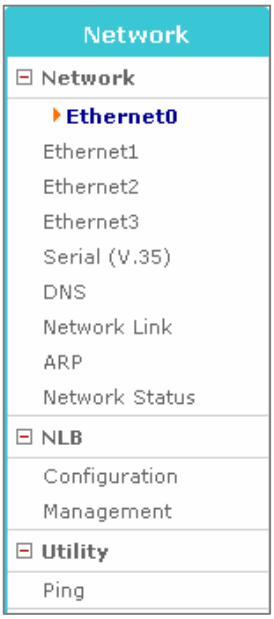
This chapter describes how to use the menus of the OfficeServ 7200 Data Server.

The menus of the OfficeServ 7200 Data Server are as follows:



Network Menu

When the **[Network]** menu of the OfficeServ 7200 Data Server is selected the submenu of the **[Network]** menu is displayed on the left top of the screen.



Menu	Submenu	Description
Network	Ethernet 0	User configuration for Ethernet port, P1
	Ethernet 1	User configuration for Ethernet port, P2
	Ethernet 2	User configuration for Ethernet port, P3
	Ethernet 3	User configuration for Ethernet port, P4
	Serial(V.35)	Configuration of V.35 Serial port
	DNS	Configuration of a Domain name server
	Network Link	Configuration of Ethernet port speed and transfer method
	ARP	Management of additional ARP deletion
	Network status	Brief description of all port configuration information
NLB	Configuration	User configuration for NLB function organization
	Management	Operation of NLB function
Utility	Ping	Connection test of the communication with another system via Ping

Network

The **[Network]** menu displays the five network interfaces built-in to the Data Server. This menu sets IP information, transfer speed, and transfer mode of each interface. In addition, this menu sets DNS, ARP, Network Load Balancing, and has a ping utility.

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

Ethernet Setup

[Network] → [Ethernet]

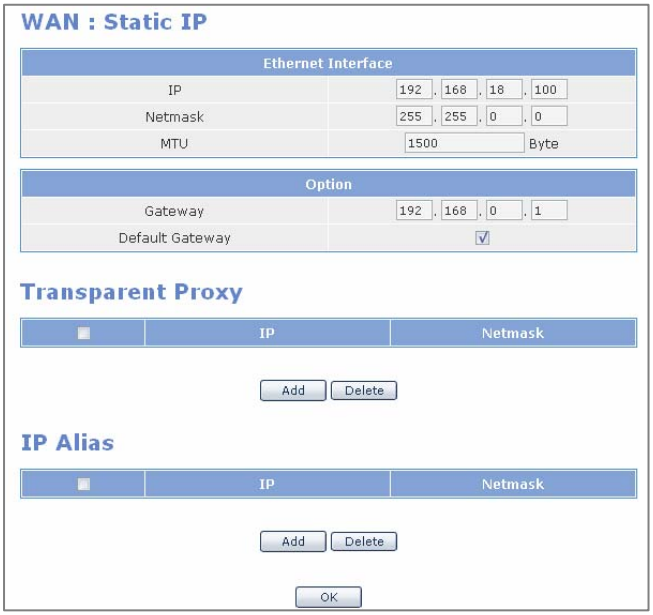
Select one of four Ethernet categories to display the setup window below. The selection fields are displayed depending on the method used for the corresponding interface. According to the selection of fields, different sub-setup window is displayed on the lower section of the window. The details by fields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

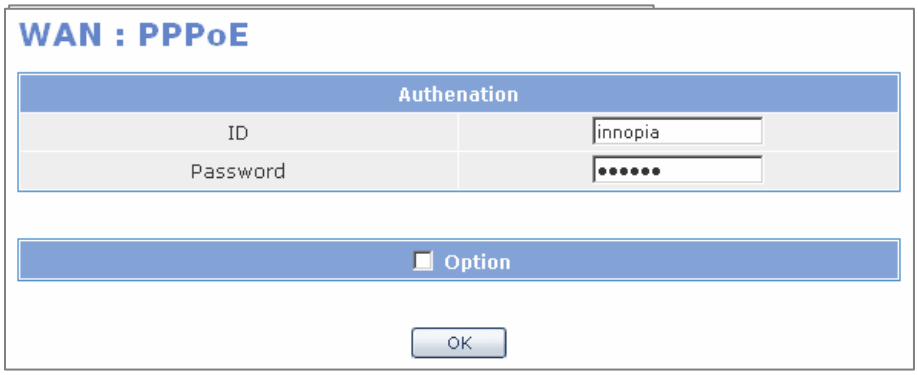
Select the WAN-Static IP category to display the following configuration window: The details by fields are as follows:



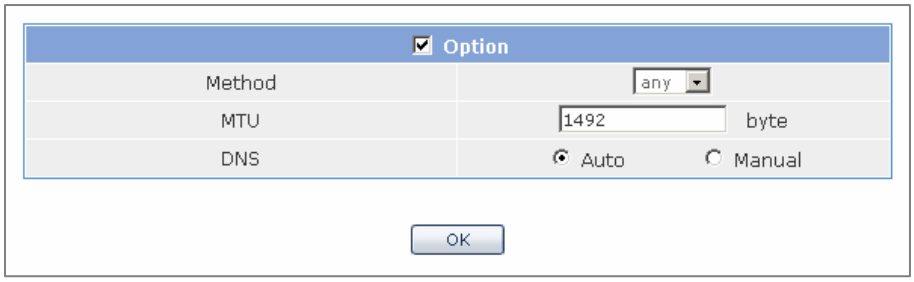
- WAN: Static IP
  - IP: Enter the public IP address assigned to the current network interface.
  - Netmask: Enter the netmask address of the current network interface.
  - MTU: Enter the maximum transmission frame size.
  - Gateway: Enter the public IP address received from Internet Service Provider 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 7200 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 the 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 .



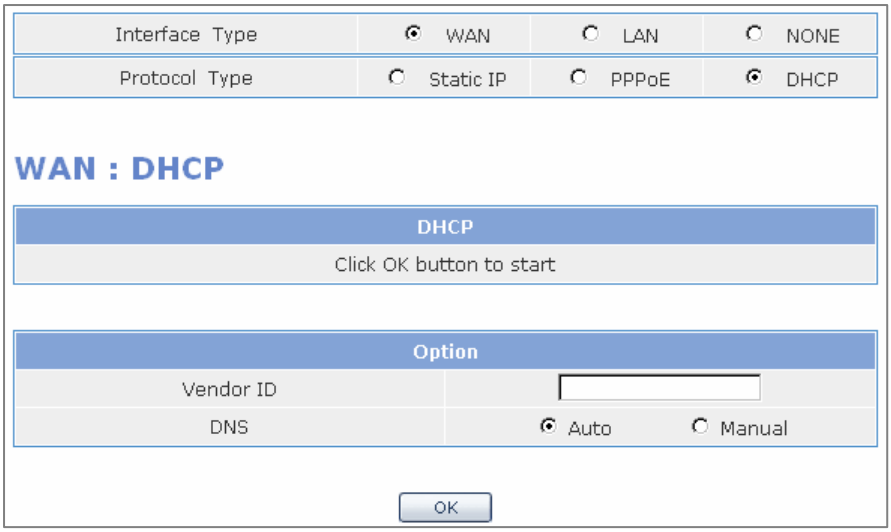
The details by fields are as follows:

- Method: Authentication Method
- MTU: Input of the maximum transmission frame size(default: 1492)
- DNS
  - Auto: Automatically receives DNS information from ISP
  - manual: Does not receive DNS information.

WAN → DHCP

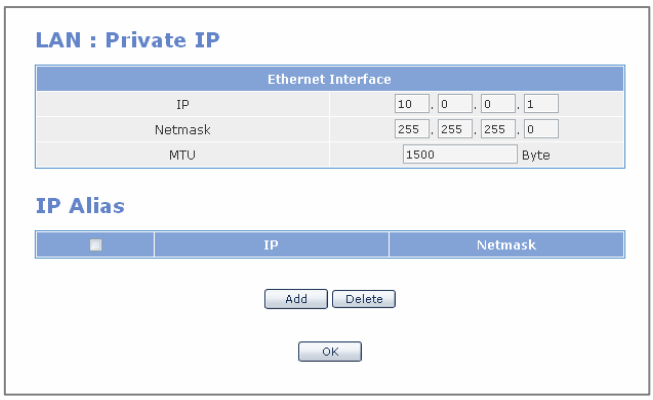
Since the **[WAN]** → **[DHCP]** item is automatically set without any additional configuration steps just click the **[OK]** button to complete the setup.

Input the Vendor ID if it is required. For the auto-assignment of DNS information just check the **[Auto]** radio button. If DNS information must be entered manually check the **[Manual]** radio button.



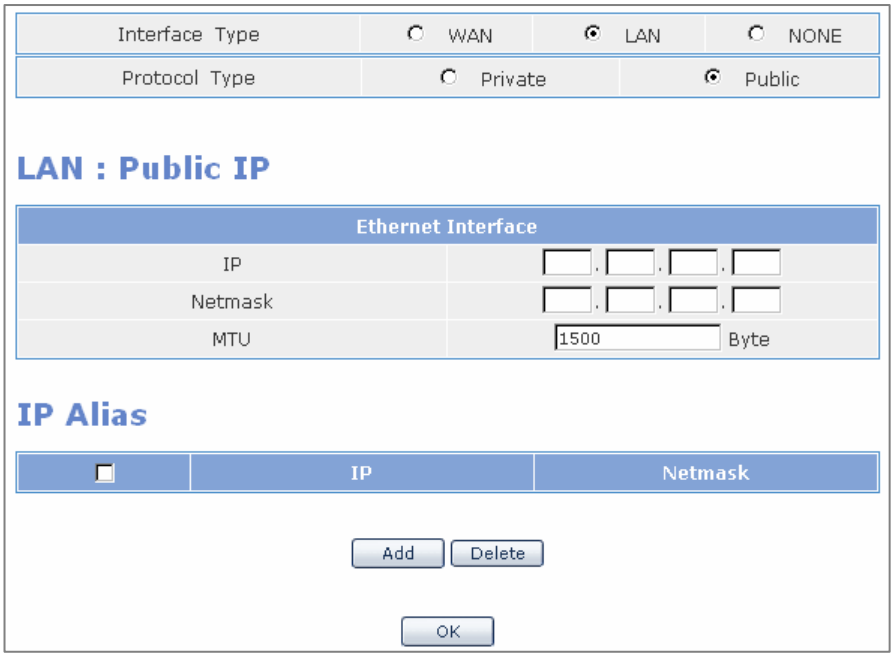
LAN → Private IP

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 the ISP. 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.



NONE

NONE is selected when any interface is not selected.

Serial (V.35) Setup

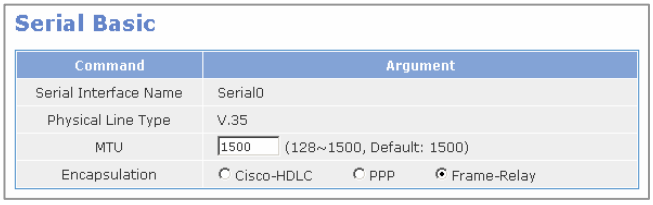
This is a submenu to specify V.35 Serial port.

Interface Type

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

Serial Basic

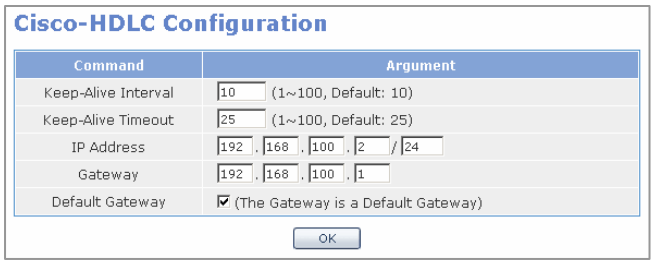
The Serial Basic table sets the basic information of the Serial Interface. Select one of the Serial Protocols in the Encapsulation field of this table to display the configuration window.



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

Cisco-HDLC Configuration

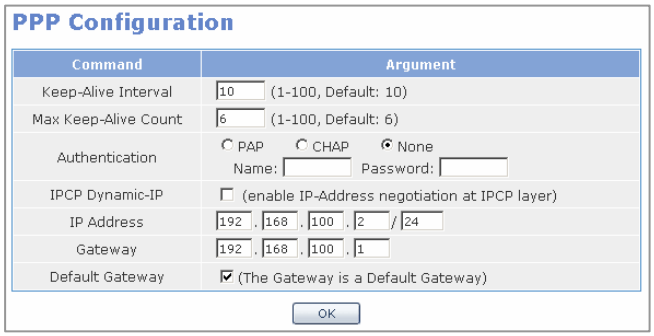
Set the Encapsulation type as Cisco-HDLC to display the Cisco-HDLC Configuration window. Specify the value for each field, and click the **[OK]** button to store the configuration.



- **Keep-Alive Interval**: Keep-Alive inspection time interval
- **Keep-Alive Timeout**: Time to decide the failure of Keep-Alive
- **IP Address**: IP address of the serial port
- **Gateway**: IP Address (Peer Address) of the serial port
- **Default Gateway**: Mark the check box to set this gateway as the default gateway. (This item is displayed if WAN is set.)

PPP Configuration

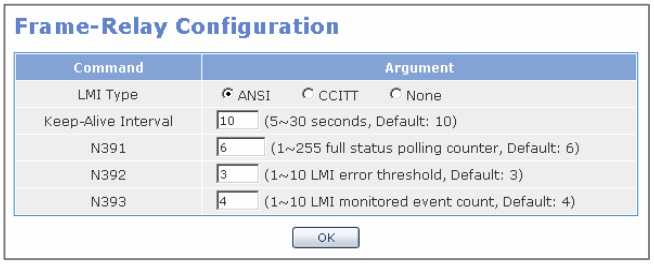
Set the Encapsulation type as PPP Protocol in the Encapsulation field to display the PPP Configuration table. Specify the value for each field, and click the **[OK]** button to store the configuration.



- **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 as the 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.

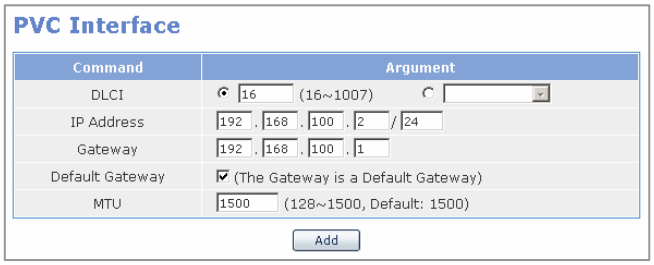


- LMI Type: LMI type of Frame-Relay
- Keep-Alive Interval: Time interval to check Keep-Alive
- N391: Cycle to request all status information. The information on all status is requested at every cycle specified in the N391 field. As usual, only Keep-Alive is exchanged.

- 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.

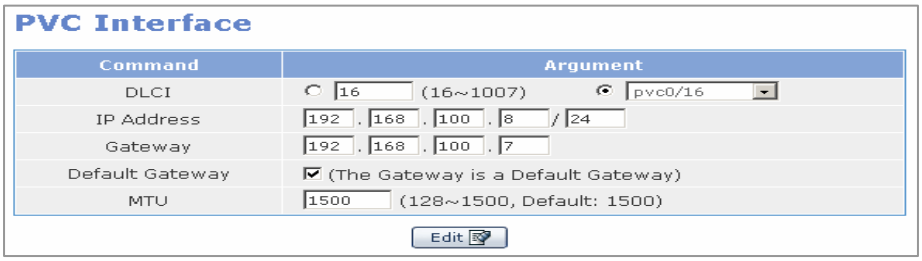
PVC Interface

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

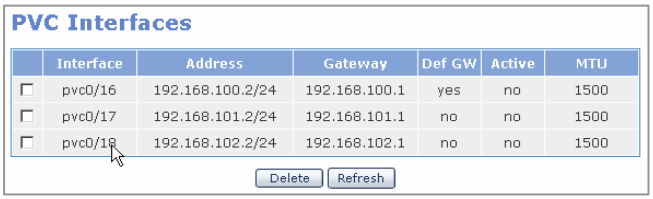


- DLCI: Number of DLCI(a type of network address)
- IP Address: IP Address to be used by PVC
- Gateway: Gateway IP Address(Peer Address) of PVC
- Default Gateway: Mark the check box to set this gateway to default gateway. (This item is displayed if WAN is set.)
- MTU: Maximum size of the packet to transfer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

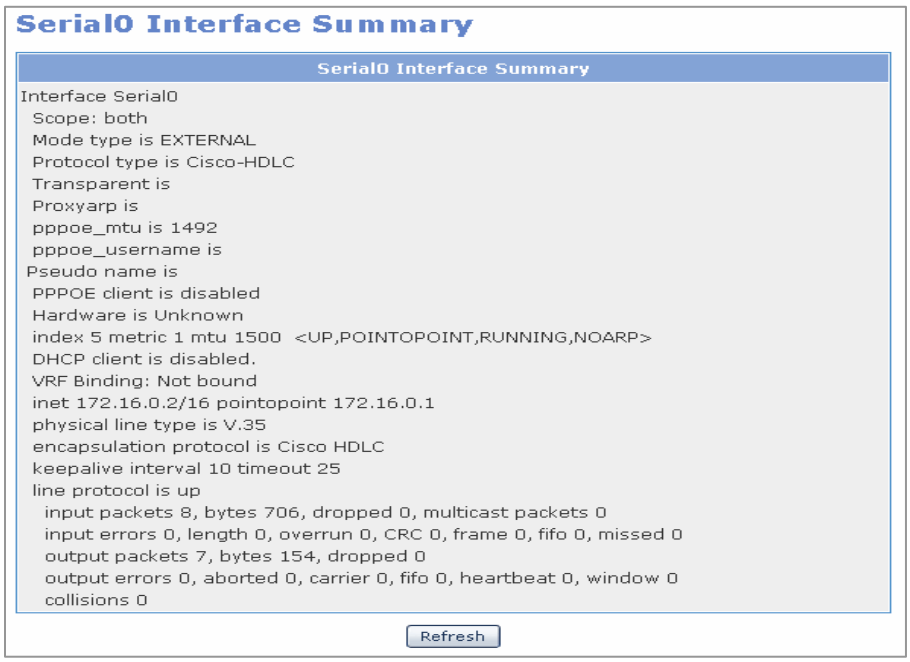


To delete a specific PVC, mark the check box of the corresponding PVC and click the **[Delete]** button.



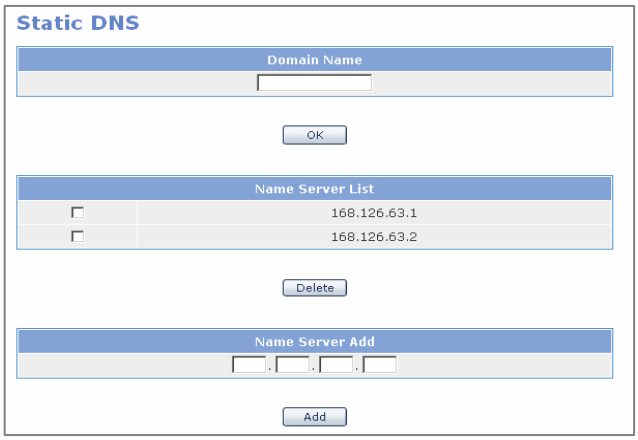
Serial Interface Summary

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

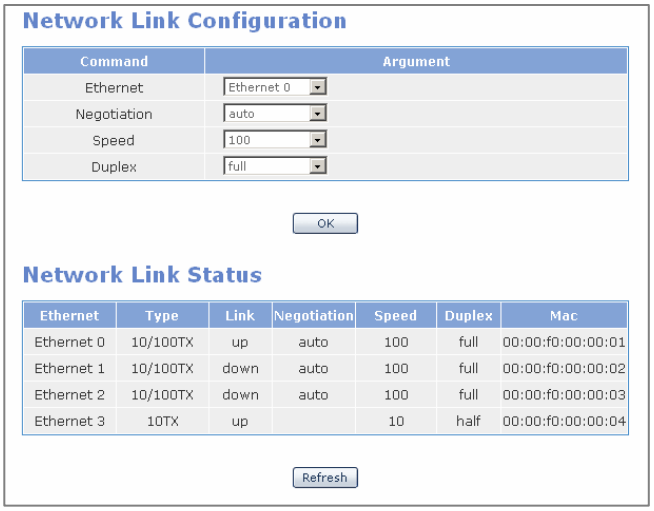
Click this menu to display the following configuration window. Enter the domain name and the IP address of the DNS server to the Domain name field and the DNS server field. Then click the **[OK]** button to store the domain name and the IP address.



Network Link

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

Note: Ethernet 3 can only change Duplex type.

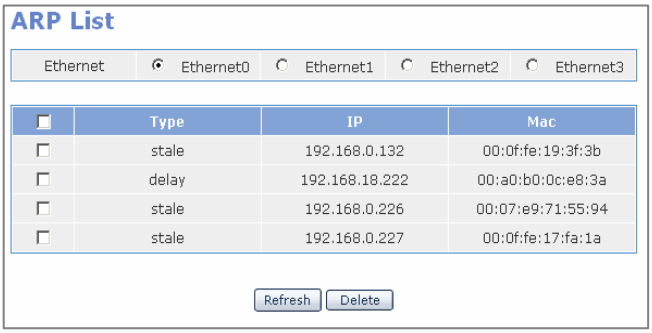


- Ethernet: Logical name of each Ethernet port
- Type: Type of Ethernet Cables/SFP GBIC Adapters
- **Link: Ethernet connection status**
- Negotiation: Setup of auto and force modes
- Speed(Mbps): Transmission bandwidth of the corresponding Ethernet interface
- Duplex: Transfer mode of the corresponding Ethernet interface
- MAC: MAC addresses by Ethernet interfaces

ARP

ARP list

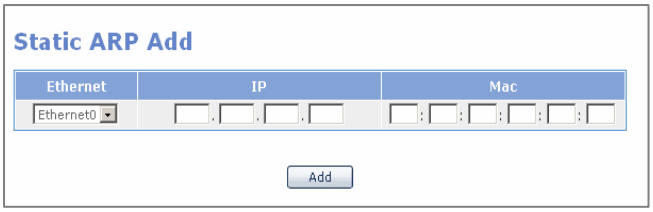
The ARP menu is used for the addition/deletion/management of the ARP information in each Ethernet interface.



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

Static ARP add

The Static ARP add window is used to add Static ARP to the ARP table.



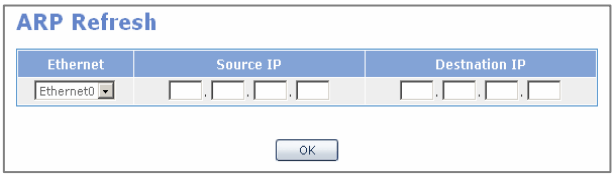
- **Ethernet**: Ethernet to add a static MAC Address
- **IP**: IP address to be added
- **Mac**: MAC Address to be added.

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

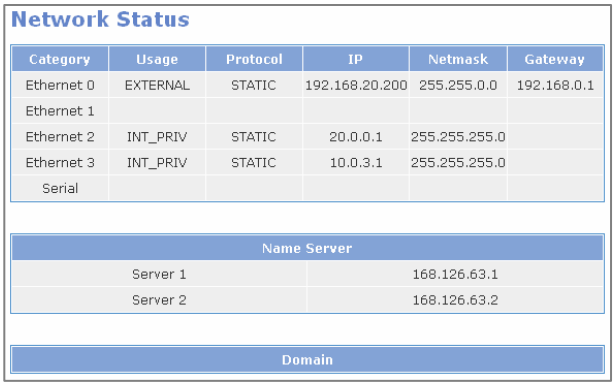
The ARP Refresh window is used for the modification of the changed ARP information in the ARP table of a route or a host when the network is changed. In the host or the route with the destination IP, the Mac with the current source IP is updated into the Ethernet Mac of the OfficeServ 7200 system.



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

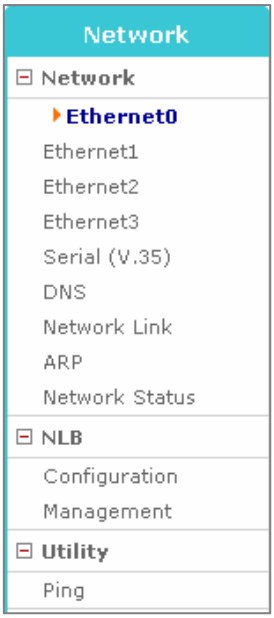
Network Status

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:

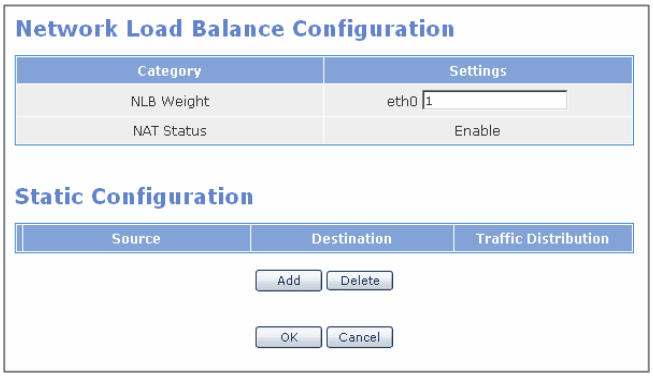


The Data Server can support up to 5 external WAN interfaces. The system can distribute the Internet access traffic to each external interfaces by using the NLB function. For effective access traffic balancing, the system uses the 'Weighted Round Robin' method. The NLB menu is used for the setup of the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

Configuration

[Network] → [NLB] → [Configuration]

This menu sets the network load balancing function. If you select this menu, the following configuration window is displayed. The details for each item is as follows:



Network Load Balance Configuration

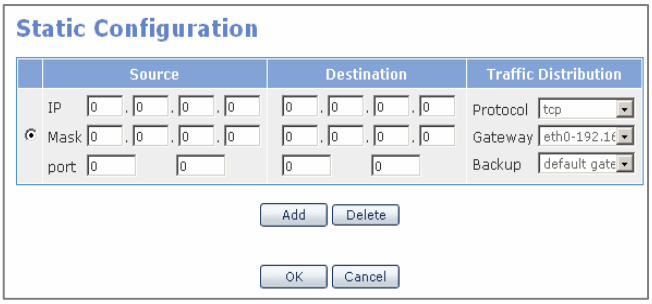
The Network Load Balance Configuration is valid when at Leaset two network interfaces are specified as the external network interface. For example, if T1 private line and ADSL line are selectively connected to Ethernet 0 Interface (eth 0) and Ethernet 1 Interface (eth 1), the higher weighted value is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



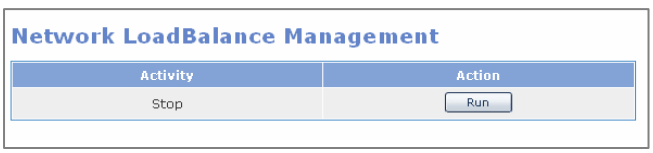
.

- 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 LoadBalance Management

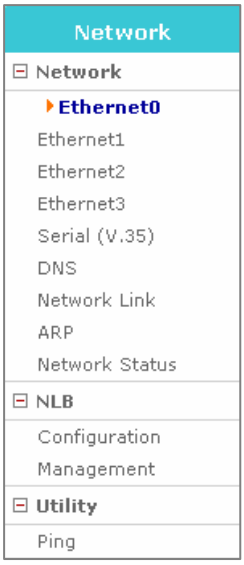
This item enable to execute/close the NLB function. If you select this item, the following window is displayed. The details for each item are as follows:



- Activity: Current activity
- Action: Click the **[Run]** button to start the NLB service.
- If the OfficeServ 7200 system is restarted the NLB service will automatically return to its last state.

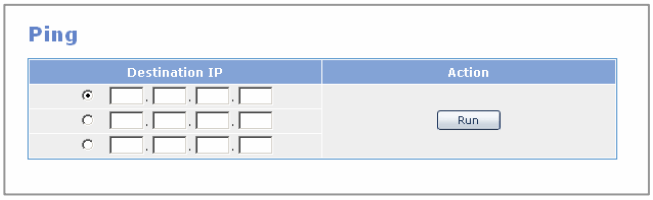
Utility

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



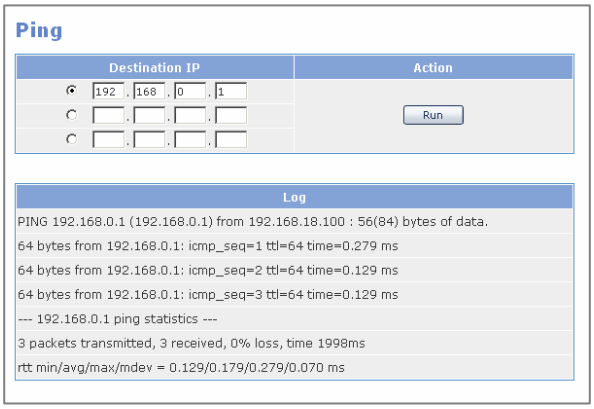
Ping

The Ping menu is used to initiate a ping test.



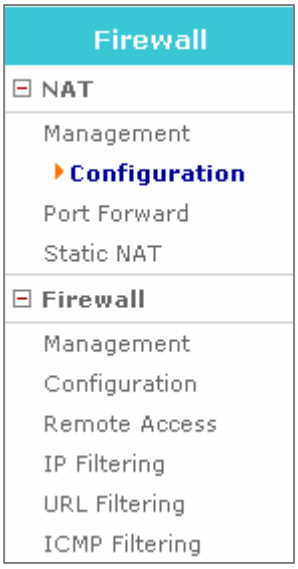
The **[Destination IP]** item is used to enter the destination address of a remote host to check if communication is being established. Enter the target information into the **[Destination IP]** item and click the **[Run]** button. Then, a ping test is executed.

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
Firewall	Management	To select the Firewall (Filter) function
	Configuration	To set the Firewall (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 to “Enable” by default.

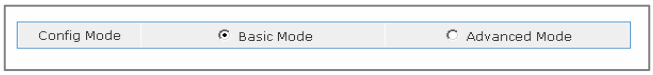
Setting	Description
Enable	Activates the NAT function.
Disable	Inactivates the NAT function.

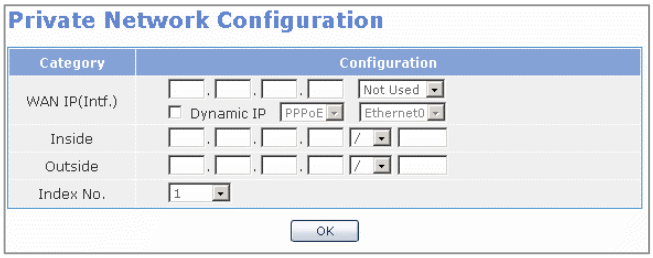
Configuration

The administrator can set up a network configured with private IPs. A private IP can then 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.

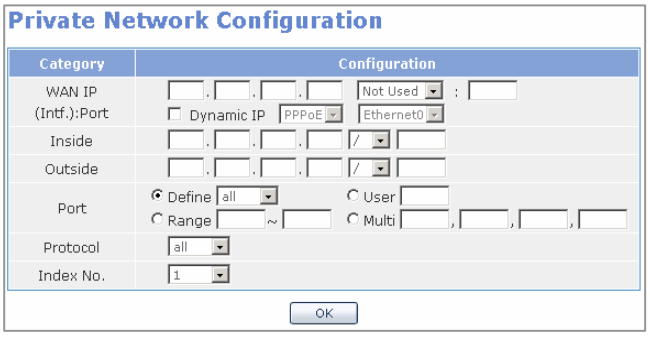




Category	Description
WAN IP	To set a general IP. Set up the connected port after selecting a dynamic IP for ADSL or Cable modem.
Inside	To enter a network address to configure a private network or select the range of netmask.(/: netmask, -: range, *; all)
Outside	To enter the network address connected to WAN or select the range of netmask.(/: netmask, -: range, *; all)
Index No.	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’.

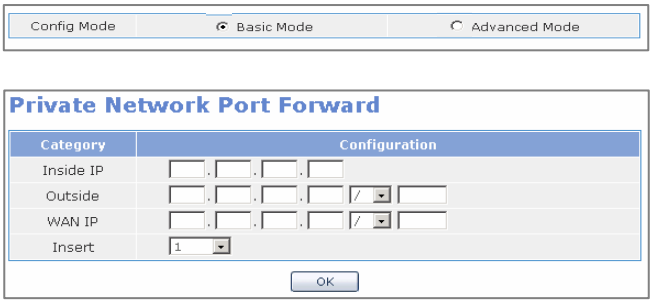
The administrator can view the current status of the configuration on Configuration List.

Port Forward

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

Basic Mode

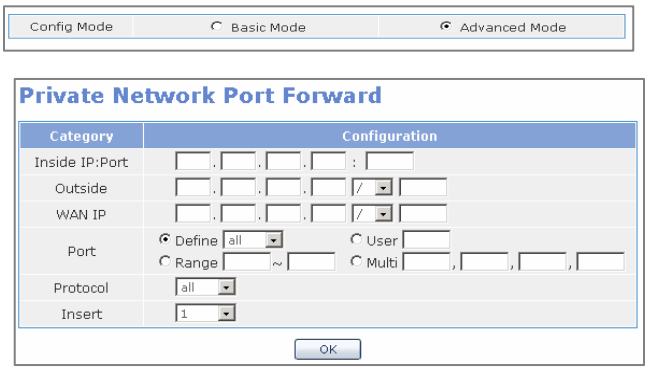
The basic mode is set up by using the minimum value of the options for port forwarding.



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.

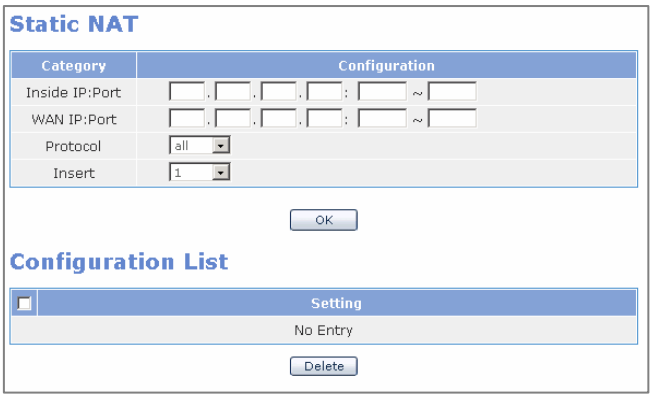


Category	Description
Port	It is available to set up as only some specific ports are allowed to transfer to the outside.
Protocol	Select a TCP and UDP protocol. For 'All', both TCP and UDP should be set up.

Configuration List displays the current setup status.

Static NAT

This window allows the administrator to connect a 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.

Firewall

The administrator can set up the filtering for the traffic forwarding through the system using this menu.

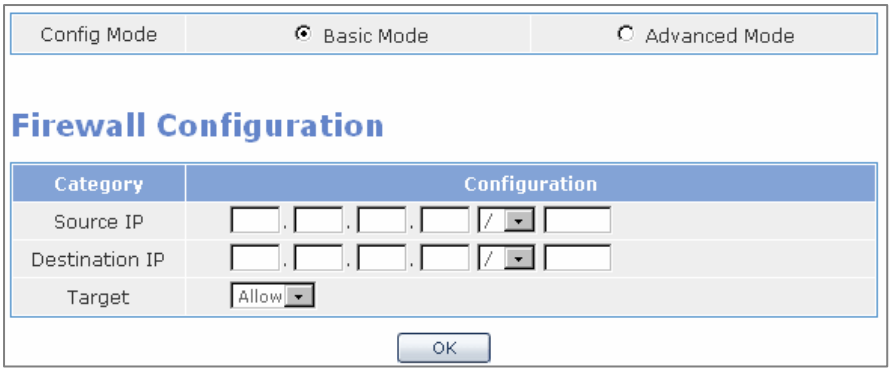
Management

The Management submenu activates/inactivates the Firewall filter function.

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

Configuration

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



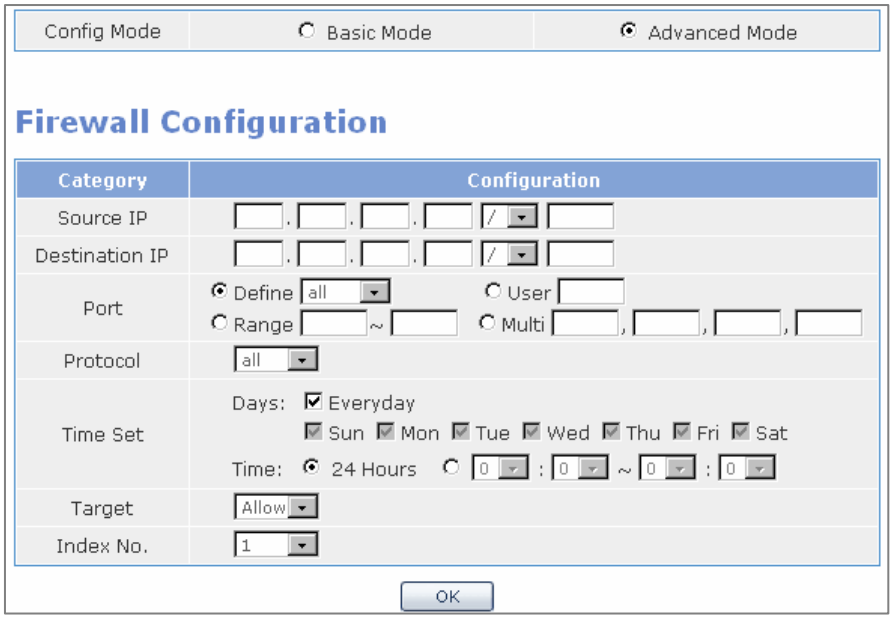
Basic Mode

Enter the minimum options required for packet filtering.

Category	Description
Source IP	To set the origination IP. . (/: netmask, -: range, *; all)
Destination IP	To set the destination IP. .(/: netmask, -: range, *; all)
Target	To select Allow or Deny.

Advanced Mode

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

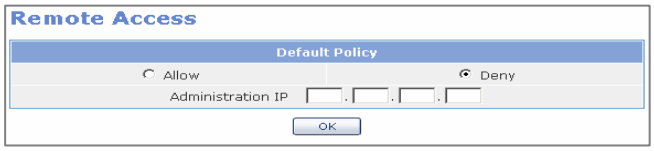


Category	Description
Source IP	To set the origination IP. .(/: netmask, -: range, *; all)
Destination IP	To set the destination IP. .(/: netmask, -: range, *; all)
Port	To set the port.
Protocol	To set the protocol.
Time Set	To set the time to apply the filtering rule.
Target	To set the permission of target.
Insert	To select a location to insert the entered rule.

This table displays the current setup status.

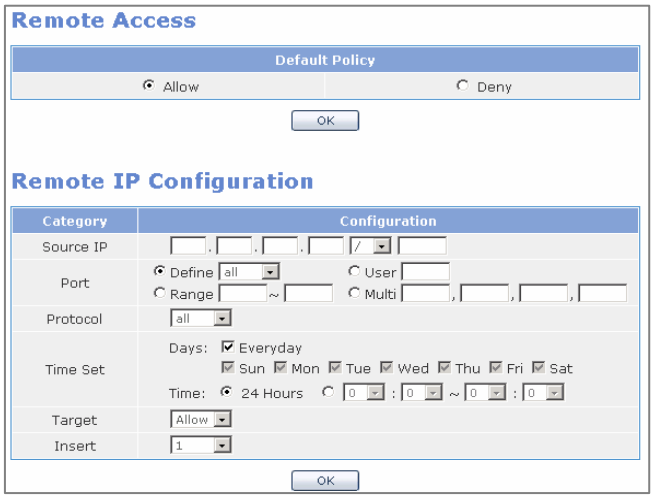
Remote Access

The Remote Access menu is used to allow or deny access to the Data Server from inside or outside the LAN.



Default Policy

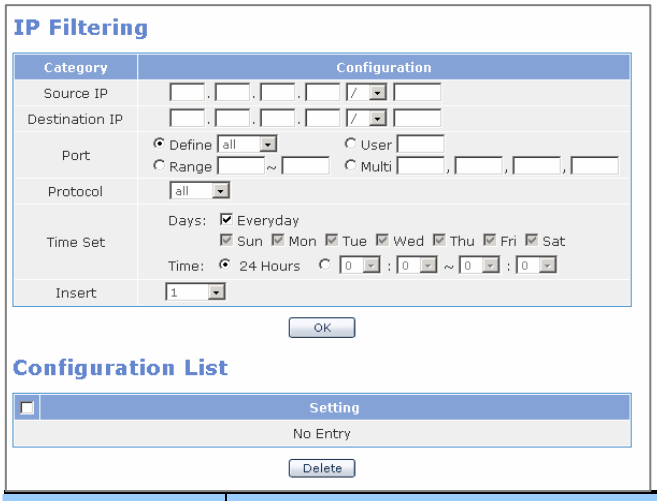
- Allow: The basic policy is set to ‘Allow’ and the administrator can set up the policy by using ‘Target’ information.
- Deny: Blocks all accesses from the inside and outside except the PC that is set up as the manager IP.
- Administration IP: Enter the manager IP. Pay attention on entering this IP because all access for other IP Addresses will be denied.



Category	Description
Source IP	To set the origination IP. .(/: netmask, -: range, *; all)
Port	To set the port.
Protocol	To set the protocol.
Time Set	To set the time to apply the remote access rule
Target	To set the permission of target.
Insert	To select a location to insert the entered rule

IP Filtering

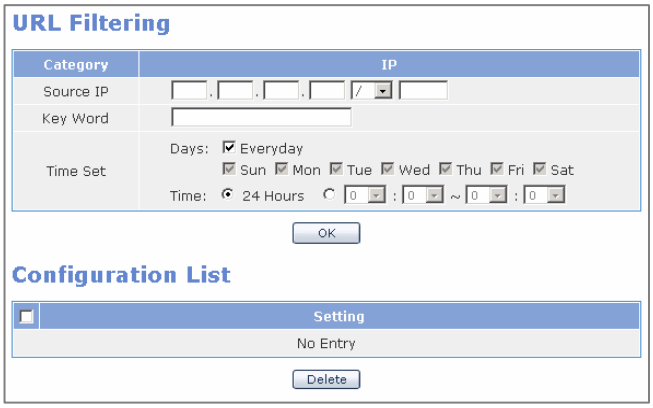
The Administrator can perform IP Filtering via this menu .



Category	Description
Source IP	To set the origination IP. .(/: netmask, -: range, *; all)
Destination IP	To set the Destination IP .(/: netmask, -: range, *; all)
Port	To set the port.
Protocol	To set the protocol.
Time Set	To set the time to apply the remote access rule
Insert	To select a location to insert the entered rule

URL Filtering

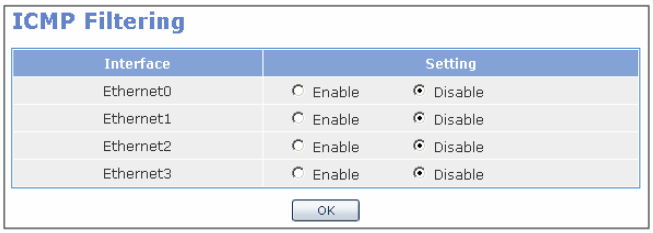
The Administrator can deny web access to PCs connected to the system.



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.

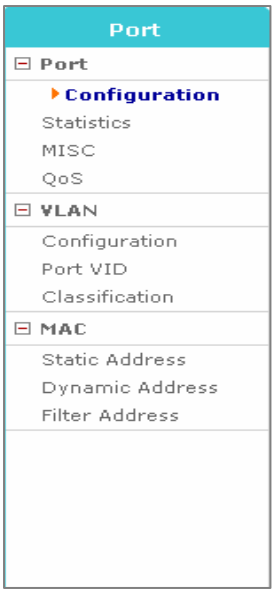
ICMP Filtering

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



Port Menu

The Port Menu is used for the management of the Switch Ports (when LIM card is installed in slot 2). Select the **[Port]** menu. The submenus will be displayed in the upper left side of the window as follows:



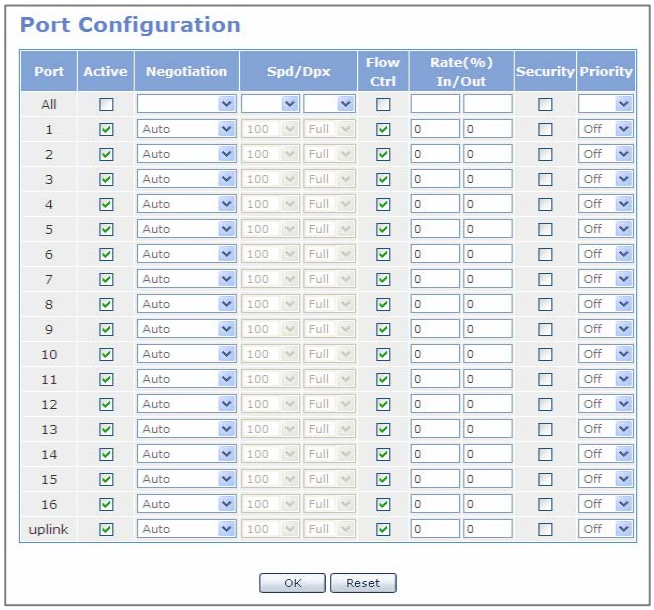
Menu	Submenu	Description
Port	Configuration	To set the switch port environment.
	Statistics	To display the information and statistics on the transmission method, link status and speed.
	MISC	To set the mirroring function and other switching functions.
	QoS	To set layer 2 QoS by giving priority compulsorily to specific ports.
VLAN	Configuration	To configures Virtual LAN (VLAN).
	Port VID	To set the Port VID: the process method for untagged packets when the VLAN mode is 'Tag-based VLAN'.
	Classification	To set VLAN based on protocol or MAC.
MAC	Static Address	To set MAC address to a static address table of the switch.
	Dynamic Address	To retrieve the dynamic address table or delete a MAC address.
	Filter Address	To enter a MAC address and set to filter the frame data that has the same MAC address information with the entered value in the switch.

Port

The administrator can set the functions for the ports and retrieve information on the ports in the **[Port]** menu.

Configuration

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

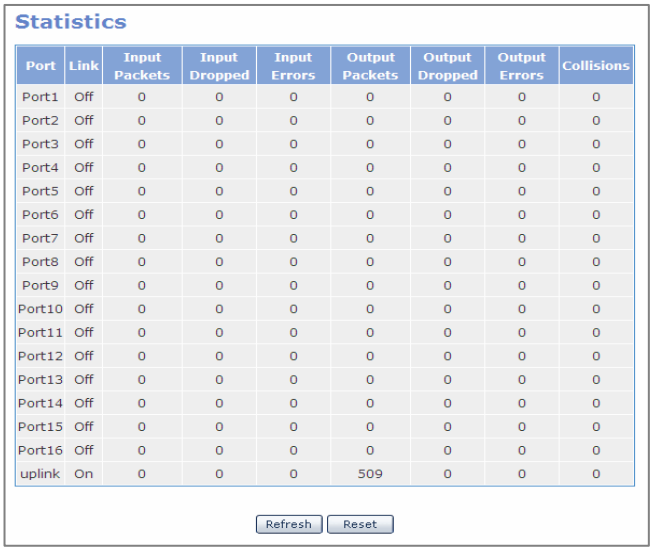


Item	Description
Port	There are16-switch ports. All ports can be processed at once through the 'All' item.
Active	Sets whether to use a port or not.
Negotiation	- Auto: Adjusts the speed through a negotiation with the counterpart. - Force: Sets the speed without a negotiation with the counterpart. Set the negotiation item as 'Force' If setting the Duplex item as 'Full'. -Nway Force: Sets the Flow Control after negotiation
Speed/Dpx	- Speed: Ports 1-12 can be set to 10/100 Mbps. Ports 13-14 are 1000 Mbps only. - Duplex(Dpx): Select Set Full(two-way service) or Half(one-way service). Ports 13-14 are Full Duplex Only.
Flow Ctl	Sets whether to use the function for flow control. The flow control is processed according to the value set at Rate (%) In/Out (Entry rate/Exit rate).
Rate(%) In/Out	Controls the flow by setting the entry rate and exit rate by ports. The unit is the Rate (%) of the port speed. If the function of flow control is not used (The item of Flow Ctl is not checked), the value is set as '0'.

Item	Description
Security	Sets whether to allow updating the MAC address table. The source MAC address is not updated at the switch port where the 'Security' item is not checked. Therefore, no terminal connects to the port. If entering the Static MAC address of a specific value to the switch port where 'Security' is checked, normal service is provided to the terminal having the entered MAC address. Therefore, the security service is provided by the method that a terminal, which is not allowed,(a terminal having a MAC address not entered to the Static MAC address) is not used.
Priority	If set as 'Low' or 'High', the priority is set as 'Low' or 'High' regardless of the configuration value of QoS bit for the packet entered to the relevant port. It is available to set Priority when the QoS mode is not First Come First Service (FCFS) in the **[Port]** → **[QoS]** menu.

Statistics

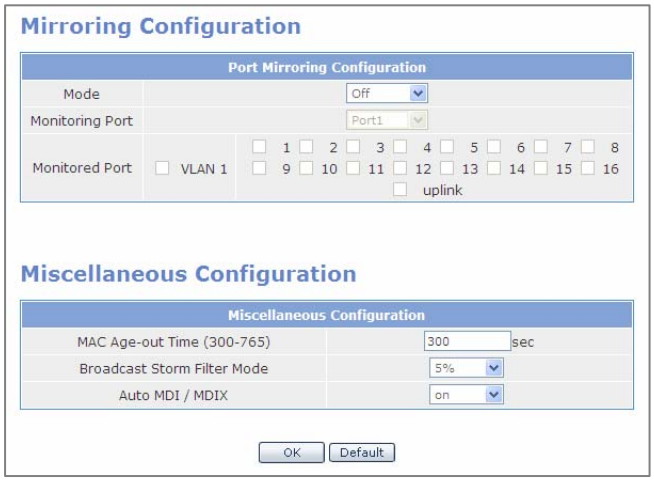
The user can retrieve the link status and statistics for each port on the switch in the **[Port]** → **[Statistics]** menu. Clicking the **[Reset]** button, will reset all statistics to '0'.



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

MISC

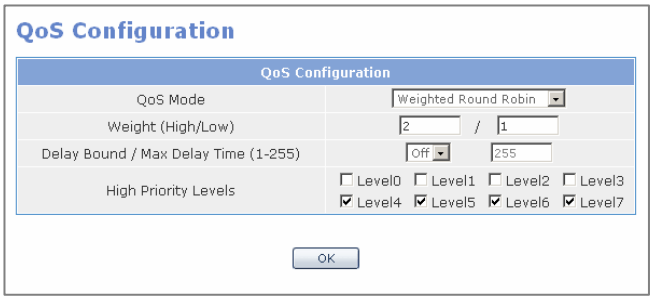
Select **[Port]** → **[MISC]** to set the mirroring function and other switch functions.



Item	Description
Mode	Sets the use of the mirroring function. - Off: Mirroring function not used - Receive: Mirroring for incoming packets - Transmit: Mirroring for outgoing packets - Both: Mirroring for incoming/outgoing packets
Monitoring Port	Assigns a port for monitoring. Generally, this means a connection to a PC for monitoring.
Monitored Port	Assigns a port where the monitoring wil be performed. The monitoring port and the monitored port cannot be the same port.
MAC Age-Out Delay Bound	Sets the duration that a MAC address remains in the address table. The default is 300 seconds. If the LAN Port connection is released, the MAC address is deleted immediately.
Broadcast Storm Filter Mode	The switch buffer can be set to 5, 10, 15, 20 and 25 % load. If this value is exceeded, the broadcast packet will be discarded.

QoS Configuration

Select **[Port]** → **[QoS Configuration]** to give set priorities according to the packets sent to the switch or process QoS by giving priority compulsorily to a specific port.



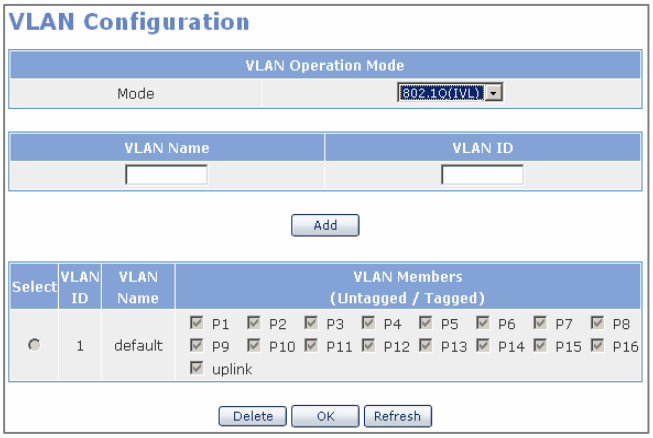
Item	Description
QoS Mode	Select the QoS mode. - First Come First Service: Packets are transmitted according to there incoming order.(QoS function not used) - All High before Low: Method that a packet that has higher priority is transmitted prior to a packet that has lower priority than that packet. A packet is not transferred until the packets that are higher priorities than the packet are all transmitted. - Weighted Round Robin: Method to transmit packets in the rate that high priority packets and low priority packets are configured at an established rate (Weight). For example, if setting High Weight to '5' and Low Weight to '2', the five high priority packets are transmitted before the two priority packets are transmitted.
Weight	Sets the rate of High weight and Low weight when the method of 'Weighted Round Robin' is used.
Delay Bound/ Max Delay Time	Sets the time limit to prevent the low priority packets from being delayed too much when the QoS mode is selected as 'All High before Low' or 'Weighted Round Robin'. The unit of 'Max Delay Time' is ms (1/1000 second) and the default is 255 ms. If a low priority packet is not switched even though the established time is exceeded, the packet will be processed preferentially.
High Priority Levels	There are 8 tags to indicate priority. Level 0~Level 7 does not indicate the actual value of the priority and it is set as a level having higher value has the priority against a level of a lower value. The GPLIM processes priority by separating the two Queues, 'High' and 'Low'.

VLAN

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

Configuration

Select **[VLAN]** → **[Configuration]** to display the VLAN configuration window.



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

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

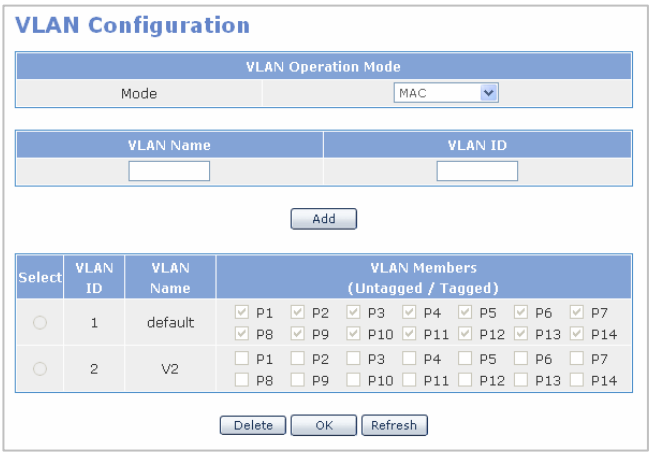
Enter the VLAN name and ID, then click the **[Add]** button. Check the target VLAN and click the **[Delete]** button to delete the VLAN.

- VLAN Untagged Members: Select the port that will send Ethernet frame that deletes TCI information if one of 1 to 17 ports is set to be sent by being switched.
  Tagged VLAN configuration is available by connecting a terminal that IEEE 802.1Q is not supported to the selected port.
- VLAN Tagged Members: Select the port that will keep, and send TCI information if one of 1 to 17 ports is set to be sent by being switched. Connect a terminal that IEEE 802.1Q is supported.

MAC Based VLAN

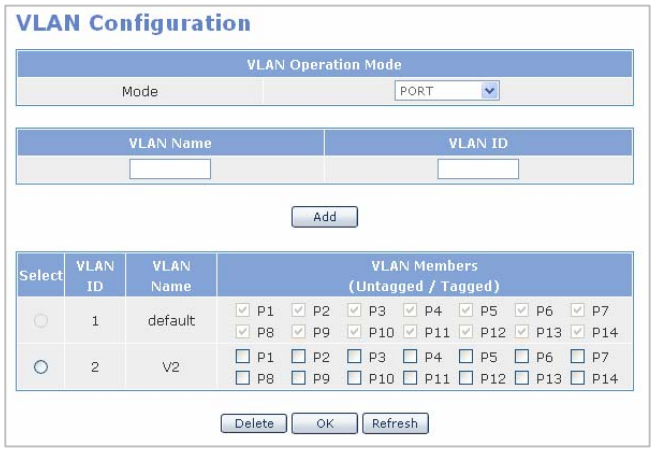
VLAN is configured for each MAC address. VLAN is configured without information on port and the number of a VLAN member may change. Up to 256 MAC members can be saved either in a single VLAN or in multiple VLANs.
Since a MAC Based VLAN does not basically contain port information, the port serves as a VLAN member by receiving packets. Thus, the ARP packet must be transmitted to the switch to enable members of a VLAN to exchange packets.

Select 'MAC' from VLAN Operation Mode of the **<VLAN Configuration>** screen. Select the corresponding VLAN and enter VLAN Name and VLAN ID and click the **[Add]** button to display the following screen. Enter the MAC address into **[Classification]** menu.



Port Based VLAN

This option is used to configure the VLAN on a port basis. A single port can be assigned to multiple VLANs. In such cases, broadcast packets transmitted by the port is transmitted to all VLANs containing the port. Ports not assigned to any VLANs serve as a single VLAN.
Select 'Port' from VLAN Operation Mode of the **<VLAN Configuration>** screen. Select the corresponding VLAN and enter VLAN Name and VLAN ID and click the **[Add]** button to display the following screen. Select the corresponding port from VLAN Members and click the **[OK]** button.

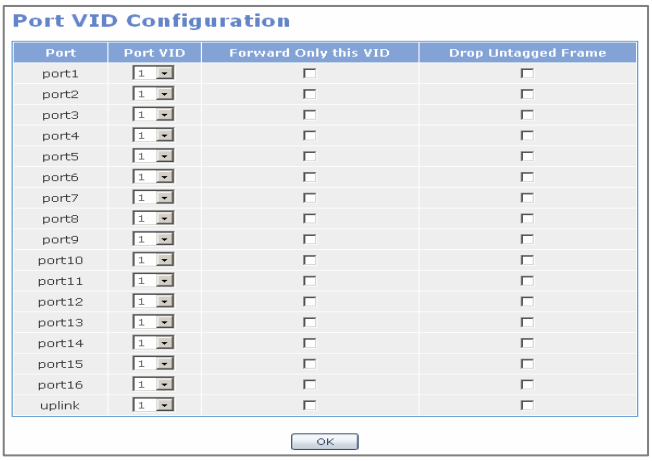


802.1Q (SVL)

- 802.1Q(SVL) can be set and operate with the same method as 802.1Q(IVL).
- IVL (Independent VLAN): Each VLAN operates while maintaining each MAC address table. Because the security is enhanced, data cannot be exchanged directly among VLANs.
- SVL (Shared VLAN): All VLANs operates while maintaining a MAC address table. Because the security is not tightened and the MAC address table exists for all ports, data can be exchanged among VLANs.

Port VID

If the VLAN mode is set for 'Tag-based VLAN', then the Port VID is set at the **[VLAN]** → **[Port VID]** menu to determine the processing system for untagged packets.



Item	Description
Port VID	- VLAN ID for an untagged packet. - When an untagged packet is sent to the corresponding port, the packet is switched to the VLAN corresponding to the Port VID.
Forward Only this VLAN	If the received tagged packet tag is different from Port VID when this item is marked, discard the packet. When this item is not marked, the packet is re-sent according to the received tag information.
Drop Untagged Frame	If this item is marked, discard the untagged frame. If not, the untagged frame re-sends the packet to the VLAN corresponding to the setting Port VID.

NOTE

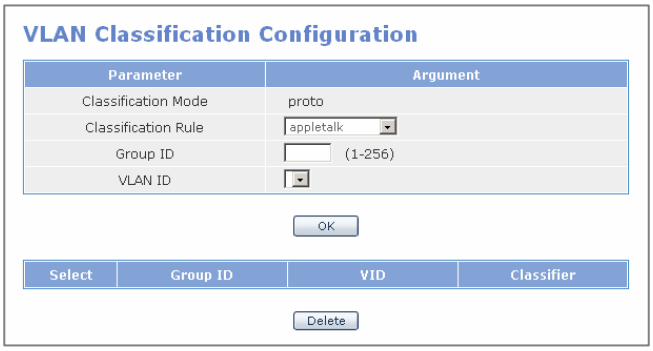
Port VID Input Value

Below 255 can be entered for Port VID.

Classification

In the **[Classification]** menu, set the values to decide VLAN ID. If the VLAN mode is '802.1Q' in **[VLAN]** → **[Configuration]**, VLAN ID is decided depending on the protocol of the packet received.

Select the member protocol from **[Classification Rule]** and click the **[OK]** button.

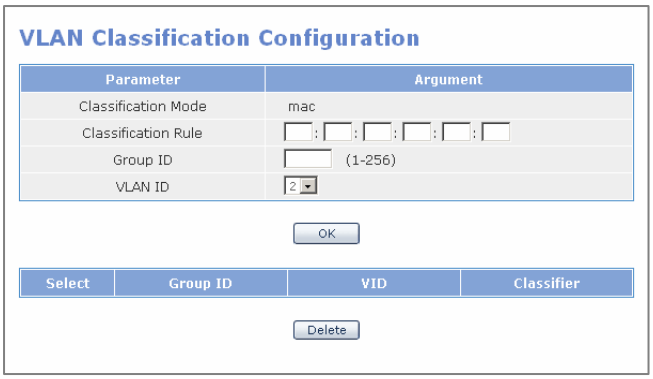


Item	Description
Classification Mode	Selected automatically according to the VLAN mode. In case of 802.1Q VLAN, 'proto' is selected. In case of MAC Based VLAN, 'MAC' is selected.
Classification Rule	Based on Appletalk, arp, decnet, ip, ipx, sna, and x25, VLAN is set.
Group ID	Group the selected protocol. Up to 1~256 can be registered.
VLAN ID	Decides which VLAN ID is proper for the current group.

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

In the **[Configuration]** menu, if the VLAN mode is set to 'MAC', VLAN ID is decided according to the received packet MAC address.

Enter the member MAC address into **[Classification Rule]** and click the **[OK]** button.



Item	Description
Classification Mode	Selected automatically according to the VLAN mode. In case of 802.1Q VLAN, 'proto' is selected. In case of MAC Based VLAN, 'MAC' is selected.
Classification Rule	According to the received packet MAC address, VLAN can be set.
Group ID	Group the selected MAC address. Group ID can be registered ranging from 1 to 256.
VLAN ID	Decides which VLAN ID is proper for the current group.

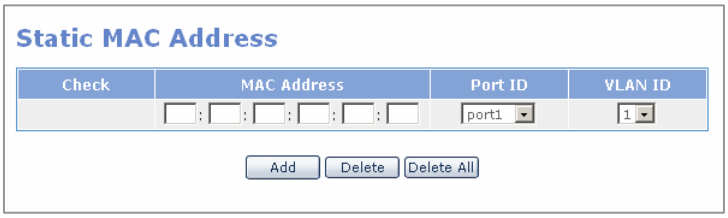
Select a Group ID from **[Select]** and click the **[Delete]** button to delete the group ID.

MAC

This menu is used to retrieve the address table of the switch and set filtering MAC.

Static Address

Select **[MAC]** → **[Static Address]** and save a specific MAC address in the address table of the switch regardless of the connection between the device and switch physically.
That is, without using learning(MAC address table renewal), a specific MAC address can be saved in the address table. Even if the device is not connected with the switch and MAX Aging Time(interval of MAC address table renewal) is passed, the corresponding MAC address is left in the address table of the switch.



Enter the target MAC address and port No. and click the **[Add]** button to add the MAC address. Select a specific MAC address and click the **[Delete]** button to delete the MAC address.
Select **[Port]** → **[Config]** and set the security of the port. Then, Learning of the source MAC address to the port is not established. In this case, a user can access the port only through the static MAC address set in the port. Thus, by using this access condition, security function can be configured.

NOTE

Number of Static MAC Addresses Entered

Up to 50 static MAC addresses can be entered without a port.

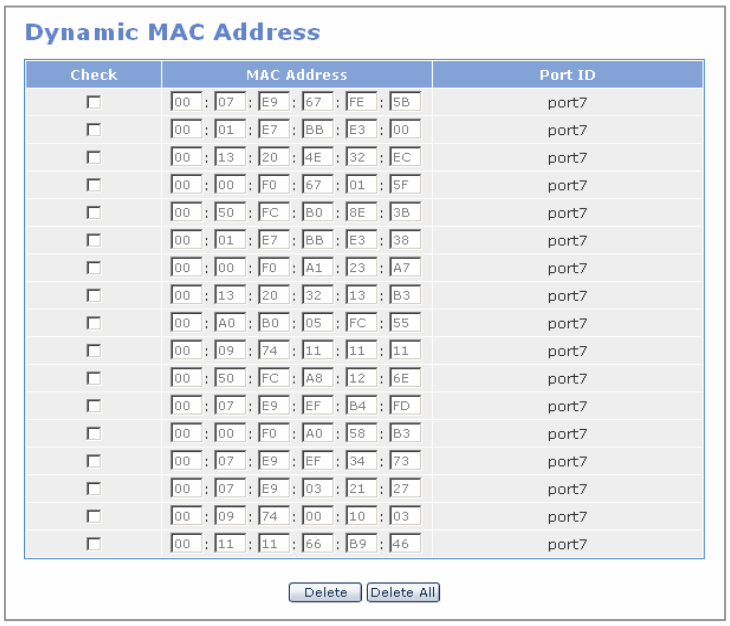
NOTE

VID Setting

In the mode where 802.1Q VLAN is set, if a setting value is entered in the **[Static Address]** and **[Filter Address]** menus, enter **[VLAN ID]**.
If not, '0' is entered.

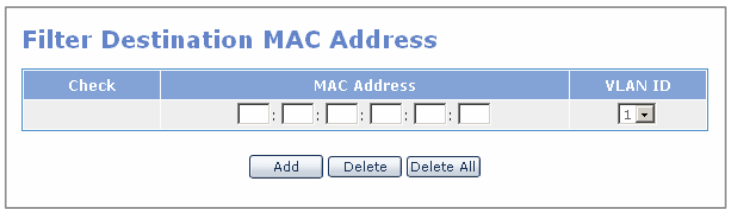
Dynamic Address

Select **[MAC]** → **[Dynamic Address]** to retrieve the dynamic address table.



Filter Address

Use Mac filtering to block unwanted traffics. Enter the target MAC address in the **[Filter Address]** menu to block the target packet in the switch. Note that MAC is the destination address of the packet sent to the switch port.
Enter the target MAC address and port No. and click the **[Add]** button.
After selecting a specific MAC address, click the **[Delete]** button.



Layer2 Menu

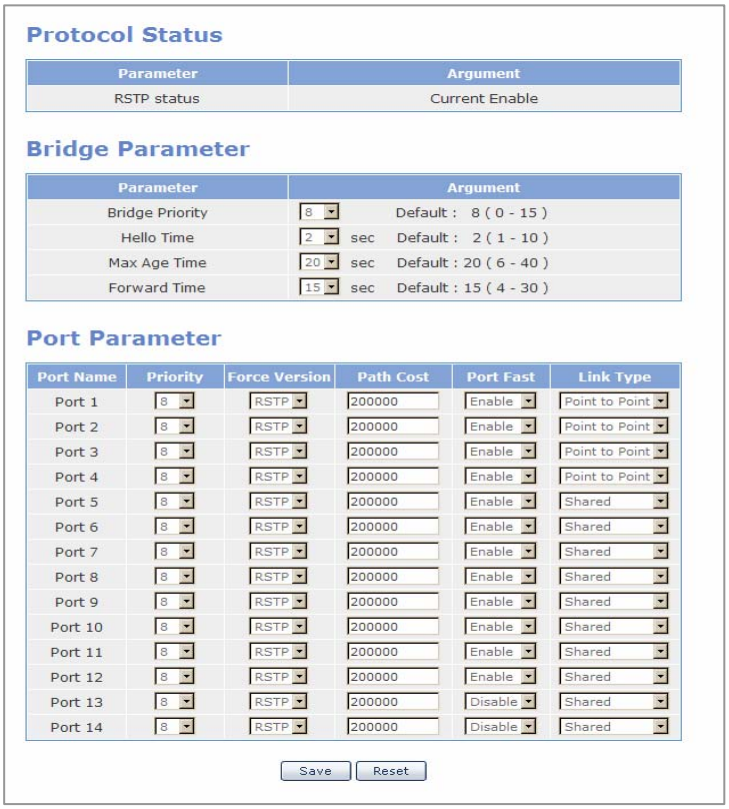
Select the **[Layer2]** menu. The submenus will be displayed in the upper left side of the window as follows:

Menu	Submenu	Description
RSTP	Configuration	Sets bridge and port environment used in RSTP.
	Status	Retrieves the RSTP operation status of the switch.
Port Trunking	-	Sets Port Trunking related value in menu.
GVRP	Configuration	Sets GVRP and Dynamic VLAN Creation services.
	Status	Retrieves the status of each port where GVRP is set.
IGMP Snooping	Time Interval	Sets the time related with IGMP Snooping.
	Function	Sets the function related with IGMP Snooping.
	Forwarding Table	Retrieves the information of the members registered in IGMP Group.
	Management	Sets whether to operate IGMP Snooping.
Authentication	Configuration	Sets the Authentication service.
	Management	Retrieves the setting information of Authentication.

RSTP

Configuration

[RSTP] → [Configuration]

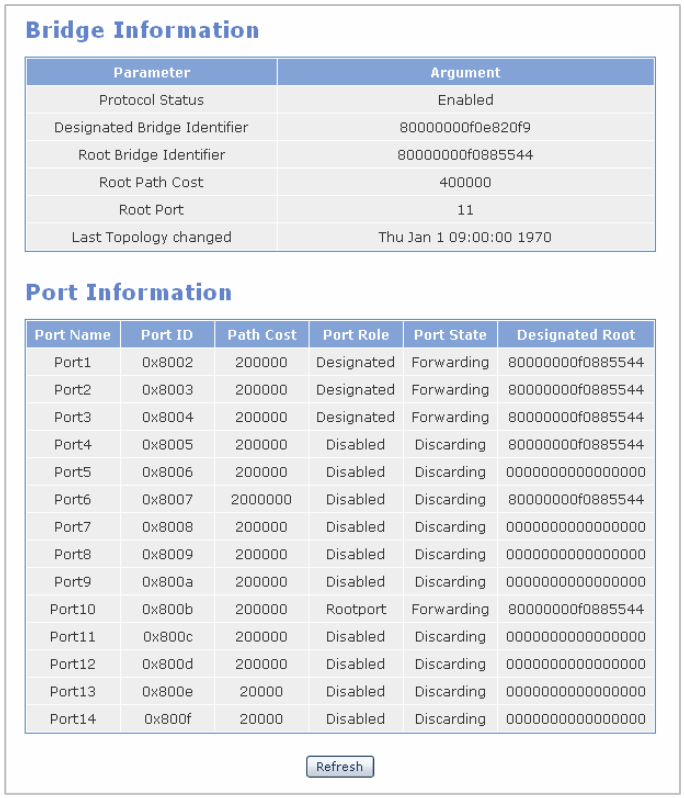


Item	Description
Protocol Status	Displays the current status of the RSTP protocol.
Bridge Parameter	Configures the Bridge parameter of the switch that RSTP operates. - Bridge Priority: Decides the priority of Bridges. - Hello Time: Sets the transmission cycle of BPDU. - Max Age Time: Sets the Message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

Item	Description
Port Parameter	- Priority: Standard to select the port to be blocked when the switch loop is established. - Force Version: Communication is progressed via the switch connected to the corresponding port and the BPDU that a user specifies. For '0', STP BPDU is transmitted. For '1', RSTP BPDU is transmitted. - Path Cost: Displays the path cost according to the bandwidth when the connection with the opponent is established. - portfast: If this value is activated, the corresponding port becomes Edge port and quickly converted into forwarding state by considering the port is connected to a terminal device, not a switch device. In addition, if this function is activated, the MAC address learned in the corresponding port is not canceled even when all topologies of Bridges are changed.(To connect the port to the STP device, the portfast function should be canceled.) - linktype: Displays the type of the link connected to the opponent. The link is connected as point-to-point in RSTP.

Status

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



Bridge Information

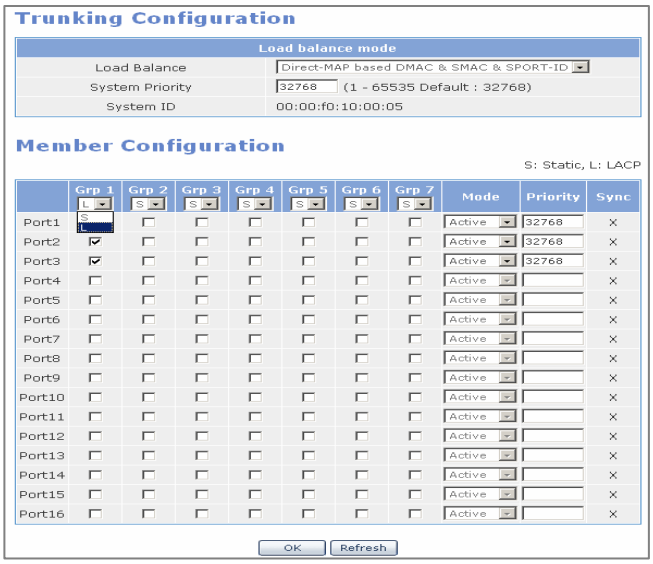
- Designated Bridge Identifier
  Its own bridge information is displayed in hexadecimal numbers.
  The upper four digits represent the bridge priority and the remaining lower digits are expressed as the system MAC address.
- Root Bridge Identifier
  Among the connected switches, it indicates the identifier of the switch equipment selected as the root bridge. Therefore, if there is no connection between switches, the Root Bridge Identifier displays the same information as the Designed Bridge Identifier.
- Root Path Cost
  When the root bridge is decided, it displays the calculated cost for the path to the root switch.
- Root Port
  If the current equipment is not the root switch, it indicates the ID of the port corresponding to the root port.(The figure above indicates 0x8003 of port2. A switch can have only root port.)
- Last Topology Changed
  It indicates the recent time that the RSTP network is reconfigured by the change of the network configuration between switches.

Port Information

- Port ID
  The value is combined with the value of the port priority and the ID value of the port specified in the system. The highest two digits represents the value of the port priority and the lowest two digits consist of port index.
- Path Cost
  The value indicates the path cost of the corresponding path.
- Port Role
  The value indicates the role of the port that selected via the BDPU exchange between switches. The RSTP Port Role is divided into Disable, Alternate, Backup, Designated, Root roles.
- Port State
  The Port State shows the status of the corresponding port. If a loop is detected via the BDPU communication, the Port State looks for the port to be blocked in accordance with Port ID and Path Cost and blocks data communication to prevent the loop from being constructed in the whole switch. The port state is divided into Discarding, Learning, Forwarding and Blocking states. In blocking, learning, discarding states, data communication is not performed. The data communication is performed only in forwarding state. In addition, the blocking state represents the state that blocks the data communication by force by detecting a loop via RSTP.
- Designated Root
  If a switch connected to the corresponding port is more close to the root switch, the Designated Root shows the Bridge identifier of the connected switch. Otherwise, Designated Root shows its own Bridge identifier.

Port Trunking

Select **[Port Trunking]** → **[Configuration]** to set the port trunking. Click the **[OK]** button to apply the setup to the system. Click the **[Refresh]** button to display the updated status.



Trunking Configuration

Item	Description
Load Balance	When transferring a packet to the opposite party through a trunk port, the packet is transferred to a port among members included to the trunk group. Select an algorithm to select a port for transfer at this time. The default is Direct-MAP based DMAC & SMAC & SPORT-ID. - CRC based DMAC & SMAC - Direct-MAP based DMAC & SMAC - CRC based DMAC & SMAC & SPORT-ID - Direct-MAP based DMAC & SMAC & SPORT-ID
System Priority	A protocol setup value used in a LACP. The default is 32768.
System ID	An identification value used in LACP. This value is the same as the value of the MAC address in the system.

Member Configuration

Item	Description
Group	'S' means a static trunk, and 'L' means a LACP. It is used for setting up the trunk type of the group. Up to eight groups can be generated as shown on the screen, and up to four ports can be included to a group as members. In addition, a member included to a group cannot be included anther group simultaneously.

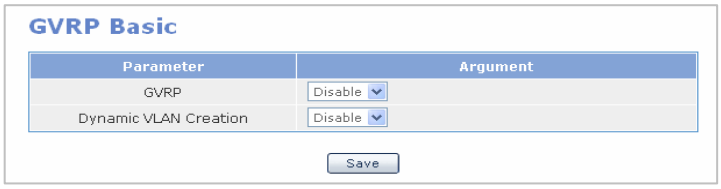
Item	Description
Mode	Displayed when selecting the trunk configuration as 'LACP'. It is available to select one of 'Active/Passive'. For the Active, a LACP packet is transferred to the opposite party first, based on the system. For the Passive, it is responded only when receiving a packet from the opposite system. If the user system and opposite system are all set up as Active, a system that has higher priority is used as a reference.
Priority	Sets up the port priority. The default is 32768.
Sync	Indicates information connected to the opposite system in ports that are configured with LACP ports. If configured as a LACP member but the LACP connection is abnormal for the opposite system, it is displayed as **'X'**. **'O'** means that a port is properly operated as a LACP port.

GVRP

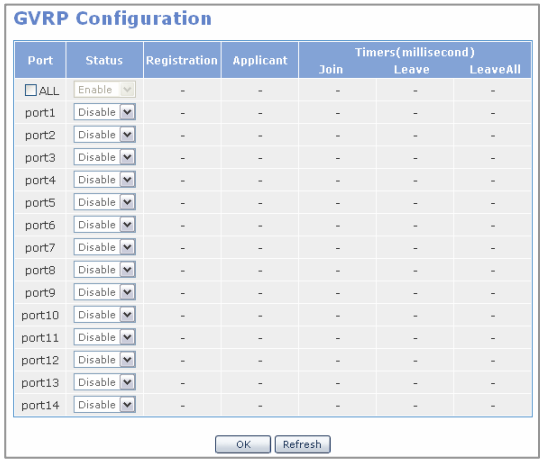
The **[GVRP]** menu is used to start or stop the GVRP service, or to modify the GVRP service for each port.

Configuration

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



On the <**GVRP Basic**> window, specify the GVRP configuration as Enable and click the **[Save]** button to display the following window and modify the GVRP configuration for each port.

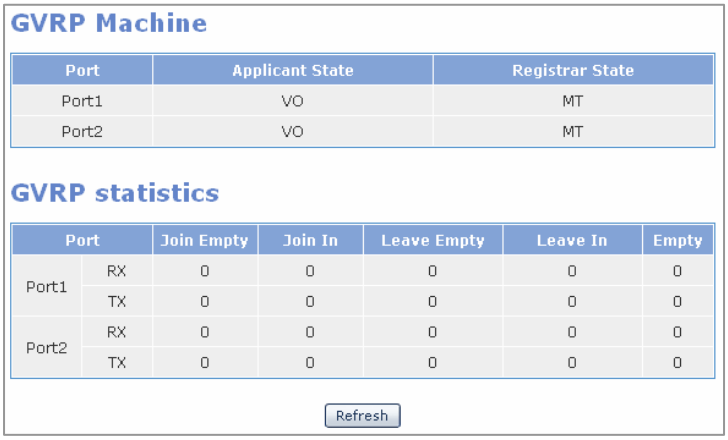


Click the **[OK]** button to save the information of each port and click the **[Refresh]** button. Then, the latest information of the port is displayed.

Item	Description
Port	Port Number
Status	GVRP configuration Information
Registration	Registration mode with Normal, Forbidden and Fixed conditions
Applicant	Applicant mode with Normal and Active conditions
Join	Interval for Join Transfer Time
Leave	Value of Leave Delay Time
LeaveAll	Value of LeaveAll Transfer Time

Status

Select **[GVRP]** → **[Status]** to display the information of the port that GVRP is configured.



GVRP Machine

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

GVRP Statistics

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

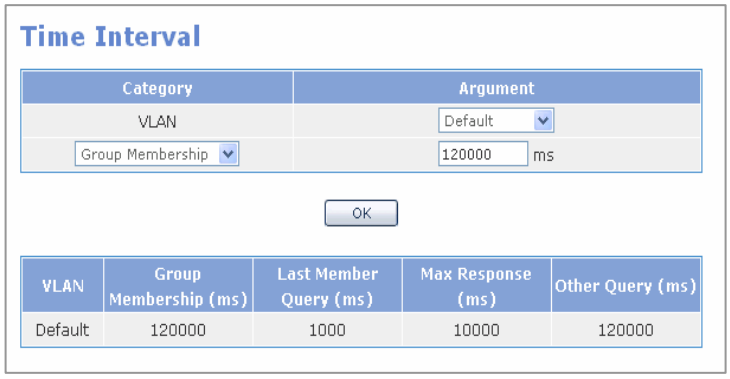
Item	Description
Join In	Number of Join In packets
Leave Empty	Number of Leave Empty packets
Leave In	Number of Leave In packets
Empty	Number of Empty packets

IGMP Snooping

The **[IGMP Snooping]** menu is used for the configuration of IGMP Snooping functions and the query of the configured information.

Time Interval

Select **[IGMP Snooping]** → **[Time Interval]** to configure the time related to IGMP Snooping.

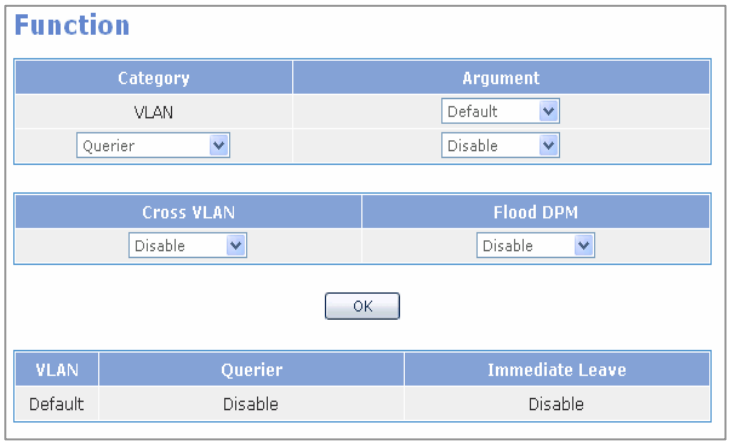


Categories	Description
VLAN	Selects the VLAN to be configured.
Group Membership	Configures the time to exit from the multicast forwarding database list when new report does not exist.
Last Member Query	Indicates the time to wait a response report after sending a query to check if the host is the last host when multicast router receives a leave message from a host. If the report is not replied until the time is elapsed, the host is deleted from the group.
Max Response	Configures the maximum time until its response when IGMP Snooping query is received.
Other Query	Configures the time until the operation as a querier starts when a query from the multicast router doest not exist.

Select the VLAN and the Category to configure, enter the time and click the **[OK]** button to store the configuration.

Function

Select **[IGMP Snooping]** → **[Function]** to specify the functions related to IGMP Snooping.



Categories	Description
VLAN	Selects the VLAN to be configured.
Querier	Specifies the operation as IGMP querier when the multicast router does not exist.
Immediate Leave	Deletes a host from the group immediately when receiving the Leave Message.
Cross VLAN	Forwards multicast packets to all ports regardless of VLAN.
Flood DPM	If no member exists in the IGMP group, sets whether to forward multicast packets.

Querier and Immediate Leave can be set of each VLAN, but Cross VLAN and Flood DPM can be set on a bridge basis.

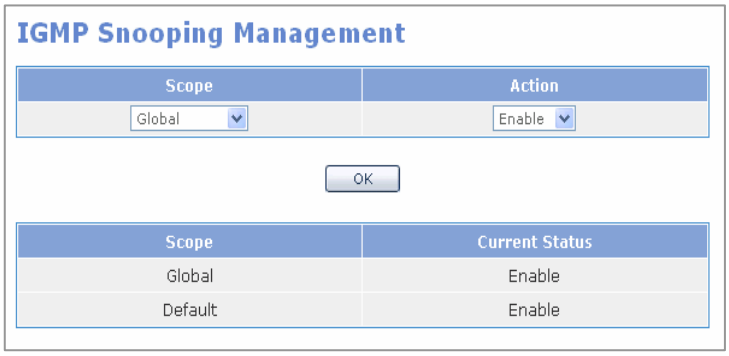
Forwarding Table

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

Click the **[Refresh]** button to update the information displayed on the web screen into the latest information.

Management

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



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

NOTE

IGMP Snooping Management

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

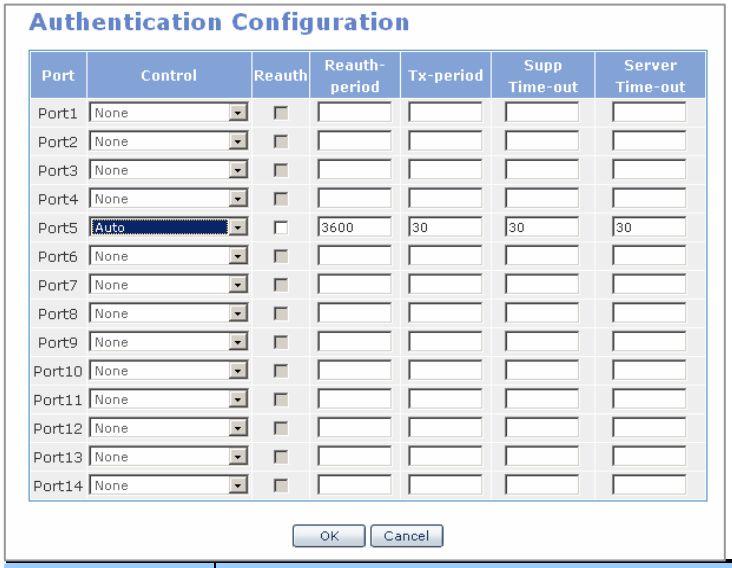
Authentication

This menu is used to retrieve the setting information or set the authentication.

Configuration

When selecting **[Authentication]** → **[Configuration]** if the activity status of **[Authentication]** → **[Management]** is 'Stop', the following window appears:

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



Item	Description
Control	Indicates the authentication mode of each port of user authentication.(802.1x). - None: Authentication is not performed for the port. - Force-authorized: Admits the port forcibly. - Force-unauthorized: Block the port forcibly. - Auto: Allows the port through authentication from the Radius server and blocks the port.
Reauth	Used for re-authentication.
Reauth-Period	Indicates re-authentication cycle when Reauth is set. (1-4294967295sec) default: 3600 sec
Tx-Period	Indicates the cycle that sends Request regularly to supplicant. (1-65535sec) default: 30 sec

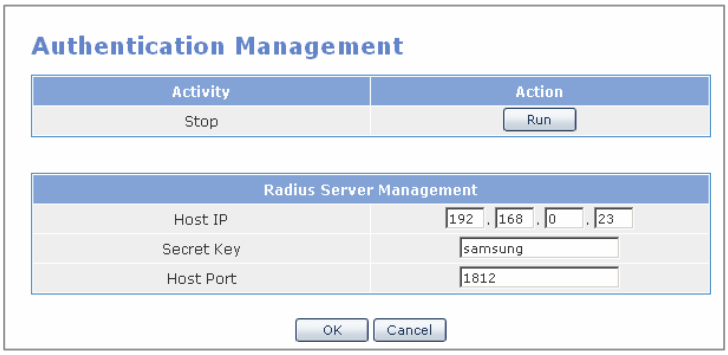
Item	Description
Supp-Timeout	Indicates the time before re-sending to the user when EAP is requested.(1-65535sec) default: 30 sec
Sever-Timeout	Indicates the time before re-sending to the device when server authentication of a server is requested.(1-65535sec) default: 30 sec

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

Management

Select **[Authentication]** → **[Management]** to activate/deactivate the authentication of system. When executing **[Run]** of Action if Activity is set to Stop, items of **[Authentication]** → **[Configuration]** can be set. When executing **[Stop]** of Action if Activity is set to Running, user authentication is deactivated.

Setting 802.1x user authentication indicates that there is the Radius server that has the user information. The host IP address, host, and key should be registered of the Radius server to be used. The default of the Radius Host Port is 1812 port. Click the **[OK]** button after the setting. Then, the setting is applied.



Layer3 Menu

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

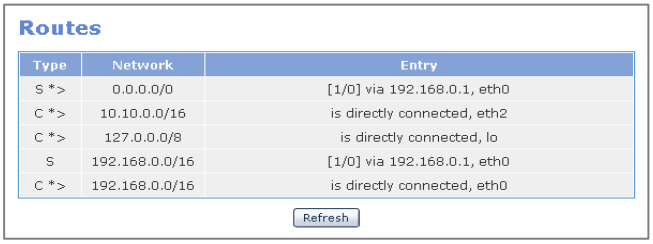
Menu	Submenu	Description
General	Routes	Displays the routing table of the Data Server.
	Management	Starts or Stops RIP and OSPF.
Configuration	Static	Sets a static route.
	RIP	Sets RIP.
	RIP Interface	Sets RIP Interface
	OSPF	Sets OSPF protocol.
	OSPF Interface	Sets OSPF interface..
List	Access List	Sets access-list.
	Prefix List	Sets prefix-list.
	Route Map	Sets route-map.
	Key Chain	Sets the key used for the authentication of RIP v2.
Status	RIP	Displays the RIP network information.
	OSPF	Displays the OSPF neighbor information.

General

This menu is used to start/stop RIP and OSPF services or to retrieve the routing table of the Data Server.

Routes

Select **[General]** → **[Routes]** to retrieve the routing table of the OfficeServ 7200 Data Server.

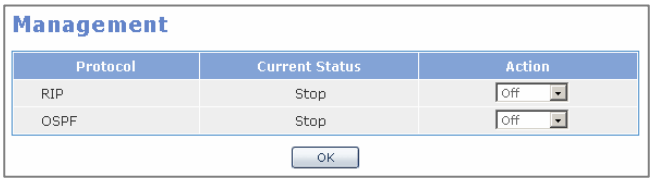


Item	Description
Type	- C: Network directly connected to the Data Server network interface - S: Static network set by a administrator

Item	Description
	- R: Path information received from another router via RIP - O: Path information received from another router via OSPF protocol * >: Whether to have activated routing table
Network	Network/Netmask information of route
Entry	Route Information.

Management

Select **[General]** → **[Management]** to start/stop the RIP or OSPF services.



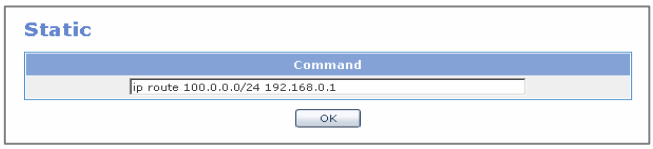
Configuration

This menu is used to set static routes, RIP, and OSPF protocols.

Static Route

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

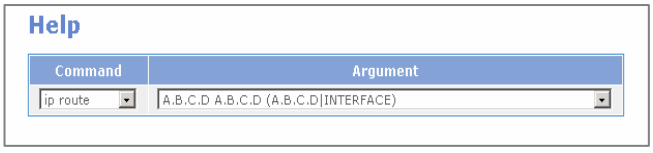
Enter the Static Route command.



When the entered command is successfully executed the configuration is directly applied to <**Current Status**> of **[Router]** → **[Configuration]** → **[Static]**.

Help

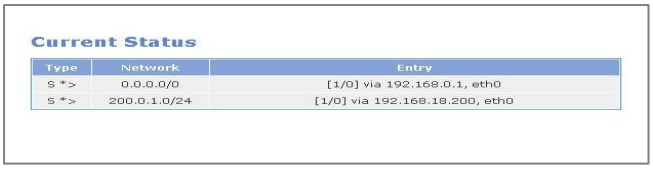
.Select the argument corresponding to the ‘ip route’ or ‘no ip route’ command.
Click **[Argument]** to display all arguments corresponding to the command..



Current Status

Displays the current static table from the Data Server.

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



Item	Description
Type	- S: Network statically set by an administrator - *>: Whether to include activated routing table.
Network	The Network/Netmask information of the route
Entry	Description of the route

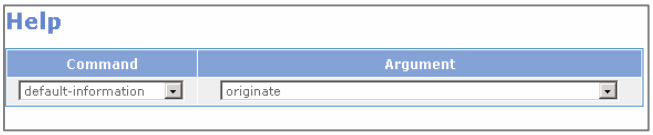
RIP

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

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

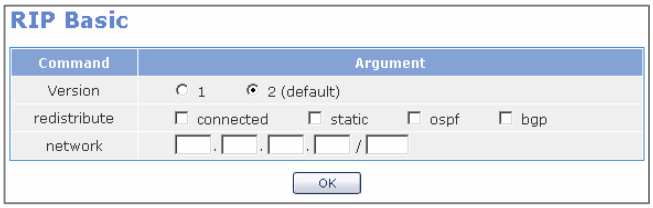
Help

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



RIP Basic

After entering the data of 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

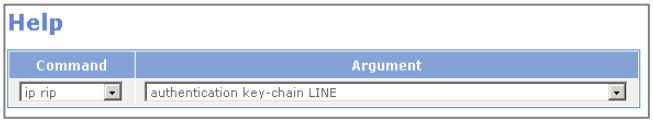
Select **[Configuration]** → **[RIP Interface]** to set RIP.

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]**.

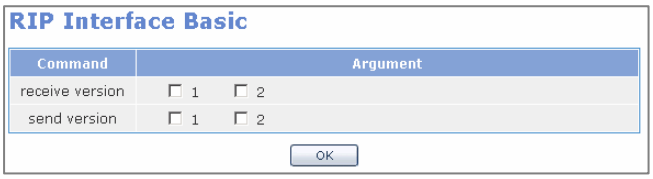
Help

Select an argument corresponding to the RIP interface command.
Select the **[Argument]** item to display all arguments corresponding to the command. Select one from all arguments.

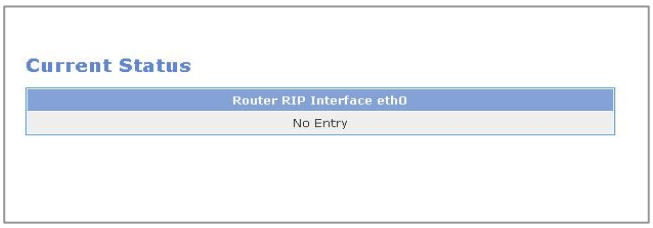


RIP Interface Basic

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

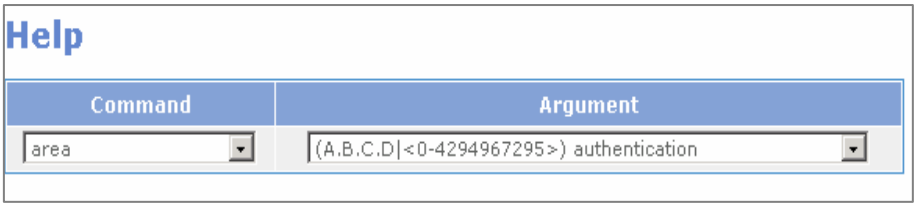
Select **[Configuration]** → **[OSPF]** to set OSPF protocol.

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]**.

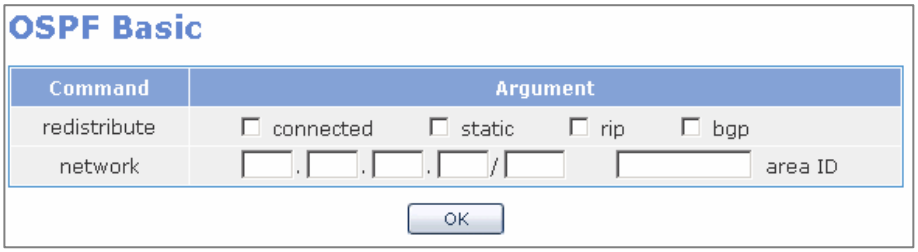
Help

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

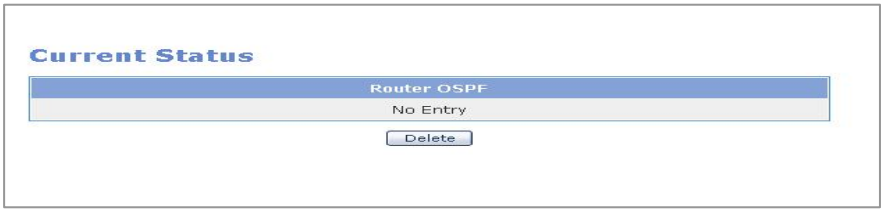


OSPF Basic

After entering all data 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]

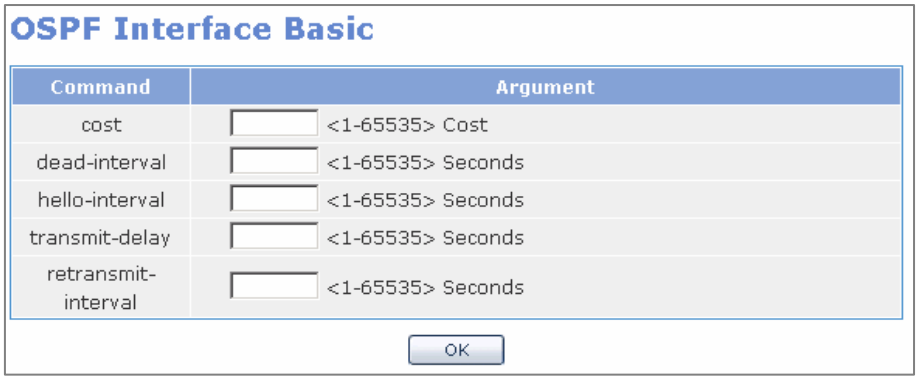
Select the target interface and enter the protocol configuration command directly.
If the entered command is successfully executed, the execution result is directly applied to **<Current Status>** of **[Router] → [Configuration] → [OSPF Interface]**.

Help

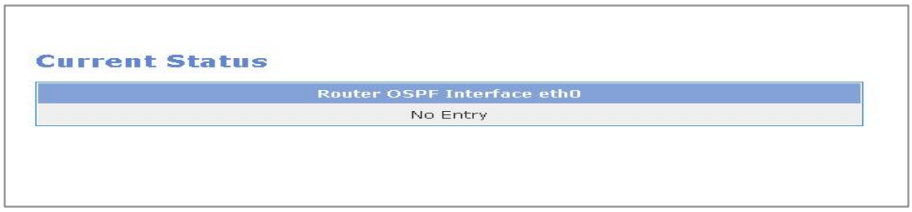
Select the argument corresponding to the OSPF interface.
Clicking the **[Argument]** item displays all arguments corresponding to the command.

OSPF Interface Basic

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



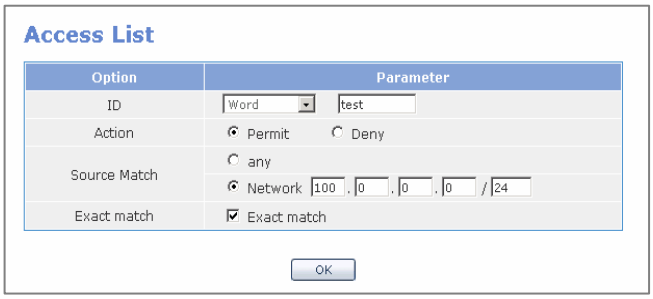
Display the command configuration currently entered.



List

Access List

Select **[List]** → **[Access List]** to set access list. Enter all data and then click the **[OK]** button.



Item	Description
ID	Sets the access list name
Action	Allows or prohibits the packet that matches the condition.
Source Match	Sets the match conditions. - 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.
Destination Match	If theAccess List 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

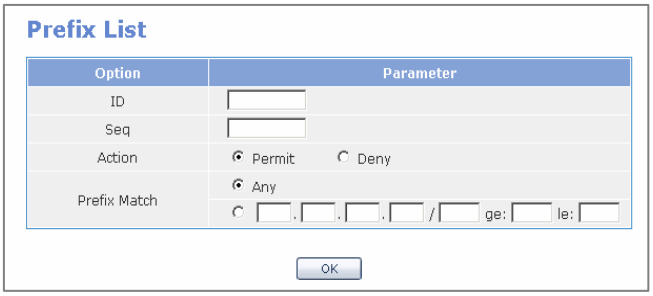
If the entered command is successfully executed, the execution results are directly applied to <**Current Status**> of **[Router]** → **[List]** → **[Access List]**. For example, when Access-list is entered, the <**Current Status**> window is displayed as follows.

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 or rejects the packets matched
Prefix Match	Sets the match condition - Any: All packets - Network: Network range
ge	The ge parameter specifies the prefix length. The prefix list will be applied if the prefix length is greater than or equal to the ge prefix length.
le	The le parameter specifies the prefix length. The prefix list will be applied if the prefix length is less than or equal to the le prefix length

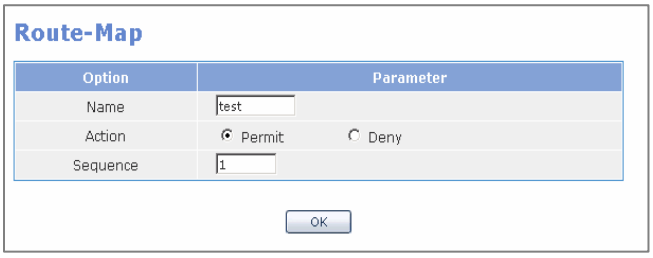
If the entered command is successfully executed the execution results are directly applied to **<Current Status>** of **[Router]** → **[List]** → **[Prefix List]**. For example, when a prefix is entered, the **<Current Status>** window is displayed as follows:

The prefix-list information being set in the Data Server 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

Select **[List]** → **[Route-Map]** to set the route map of OfficeServ 7200 Data Server. Set the following item and then click the **[OK]** button.

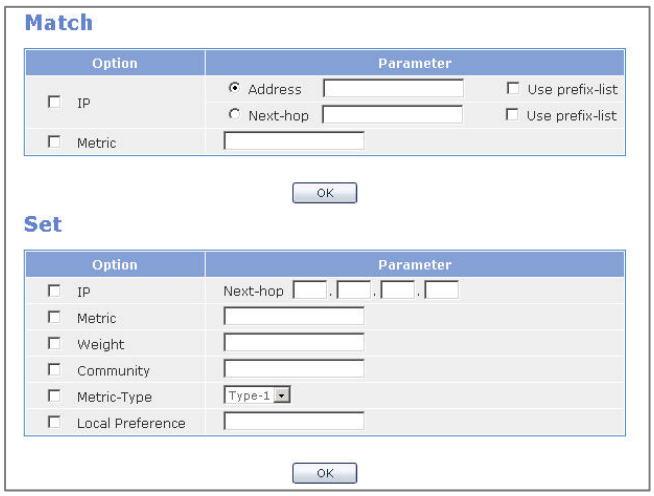


Item	Description
Name	Route-map name
Action	Sets whether to apply set operation.
Sequence	Sets the sequence No. to additionally add a route-map.

If the entered command is successfully executed, the command execution is immediately applied to the **<Current Status>** from **[Router]** → **[List]** → **[Route-Map]**. Enter the target route-map as shown in the figure above.
Then, the <Current Status> is displayed as follows.

The information of the route-map set in OfficeServ 7200 Data Server can be checked. Click the **[Delete]** button to delete the target route-map. Click the **[Edit]** button to display the following window. Through the window, the Set/Match operation of the corresponding route-map can be set.

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



Items related with Match operation are described as follows:

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 value to be matched.

Items related with Set operation are described as follows:

Item	Description
IP	Sets the next-hop of the BGP table.
Metric	Sets the metric of the BGP table.
Weight	Sets the weight of the BGP table.
Community	Sets the community of the BGP table.
Metric-Type	Sets the metric type of the BGP table. - Type 1: External Type 1 - Type 2: External Type 2
Local Preference	Sets the local preference among BGP attributes.

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>**.

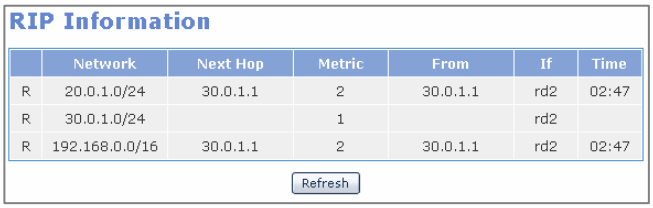
Item	Description
Sequence	Match/Set operation Sequence No. of route-map
Entry	Match/Set operation information of route-map

Click the **[Prev]** button to move to the route-map window mentioned above. Click the **[Delete]** button to delete the target Match/Set operation.

Status

RIP

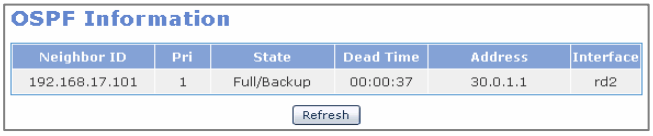
This menu is used to display the RIP connection status and information.



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

OSPF

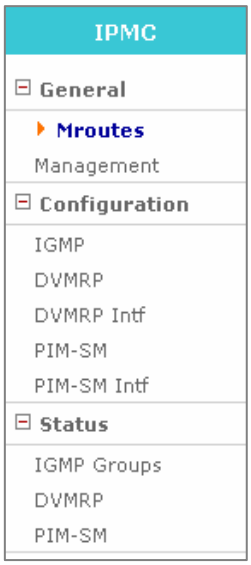
This menu is used to check the OSPF connection status and information with the other party's router.



Item	Description
Neighbor ID	Neighbor ID of the router of the counterpart
Pri	Priority
Status	Connection progress status
Dead Time	End time
Address	Address of the counterpart
Interface	Connected interface

IPMC Menu

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

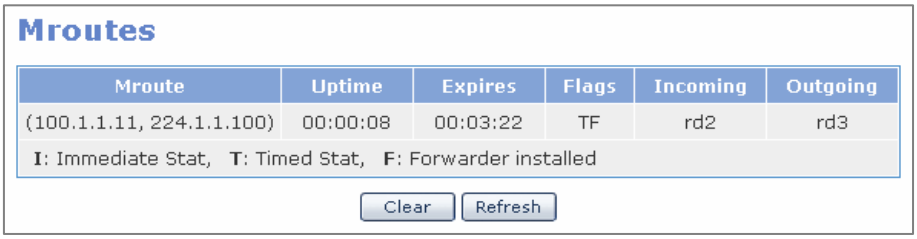


Menu	Submenu	Description
General	Mroutes	Displays Multicast Routing Entry.
	Management	Starts/Stops IPMC protocol demons.
Configuration	IGMP	Displays or changes IGMP configuration.
	DVMRP	Displays or changes DVMRP default configuration.
	DVMRP Intf	Displays or changes VIF of DVMRP.
	PIM-SM	Displays or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

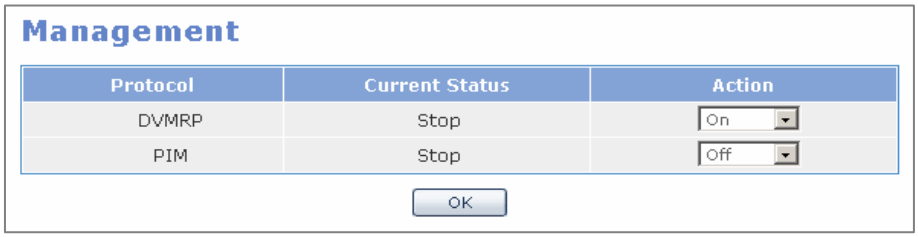
This menu is used to display multicast routing entries being shown in this window.



- 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

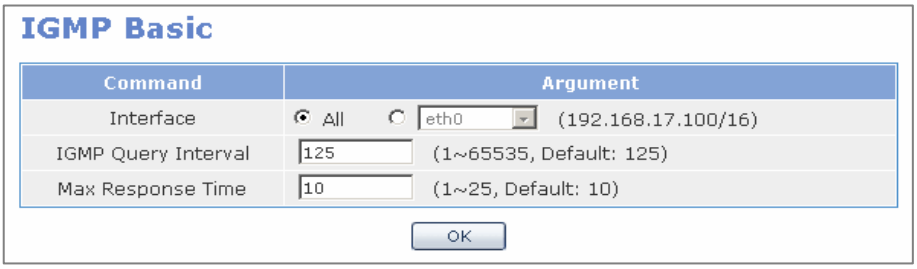
This menu is used to display and change IGMP configuration.

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

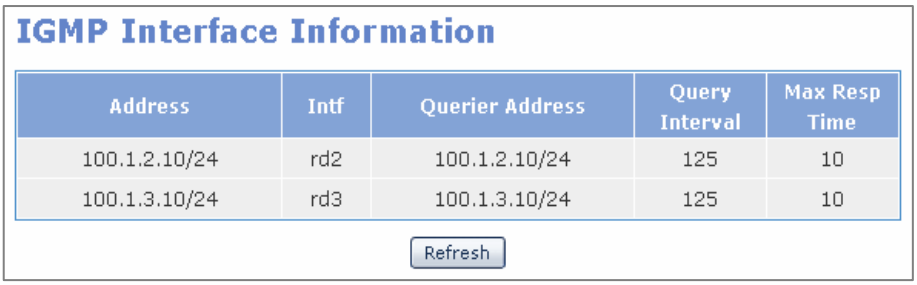
Enter new information and click the **[OK]** button to change the default configuration of IGMP.



- 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.



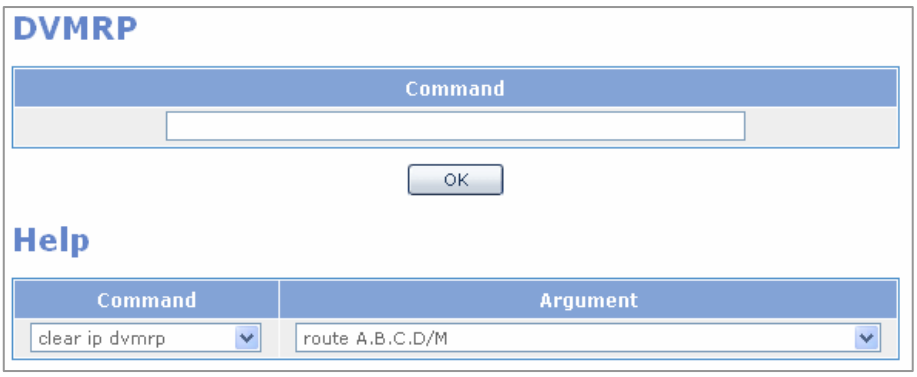
- Address: IGMP group address
- Intf: IGMP interface name
- Querier Address: IP address of IGMP interface that sends membership query. IP address of Designate Router(DR)
- Query Interval: Cycle of sending Membership Query
- Max Resp Time: Maximum time of waiting a response to Membership Query

Configuration / DVMRP

This menu is used to set DVMRP.

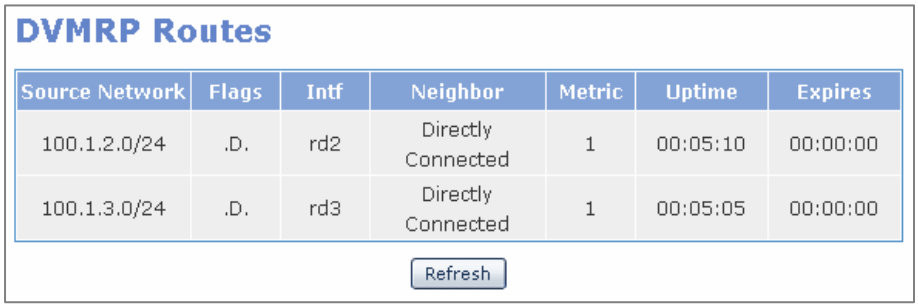
DVMRP & Help

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.



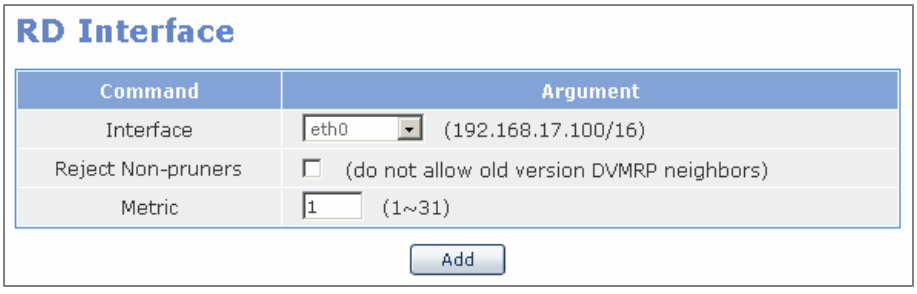
- Source Network: VIF network address to which multicast packets flow
- Flags: DVMRP route feature flag. N=New, D=Direct Connected, H=Hold down
- Intf: VIF name to which multicast packets flow
- Neighbor: DVMRP neighbor IP address that provides information on DVMRP route
- Metric: DVMRP route Metric(=distance)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

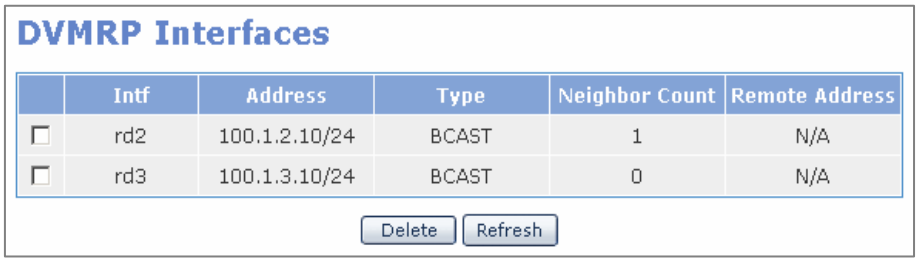
This menu is used to add L3 interface where an IP address is set to DVMRP VIF. Select the target interface to be added to VIF from the Interface item, enter the target value, and click the **[Add]** button.



- 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.



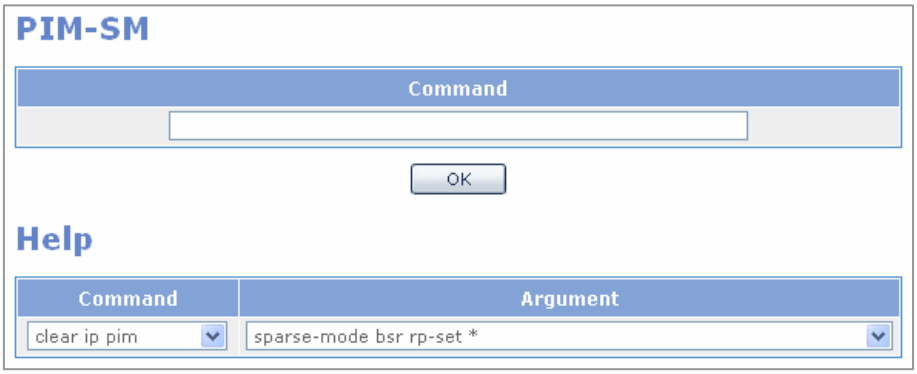
- Intf: DVMRP VIF name
- Address: IP address of DVMRP VIF
- Type: DVMRP VIF type. Tunnel, Point-to-Point, Broadcast
- Neighbor Count: Number of neighbors connected to DVMRP VIF
- Remote Address: Address of the other party in case of Tunnel or Point-to-Point type.(Peer Address)

PIM-SM

This menu is used to set PIM-SM.

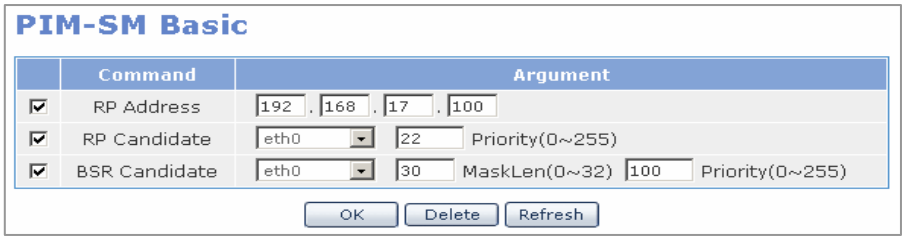
PIM-SM & Help

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



PIM-SM Basic

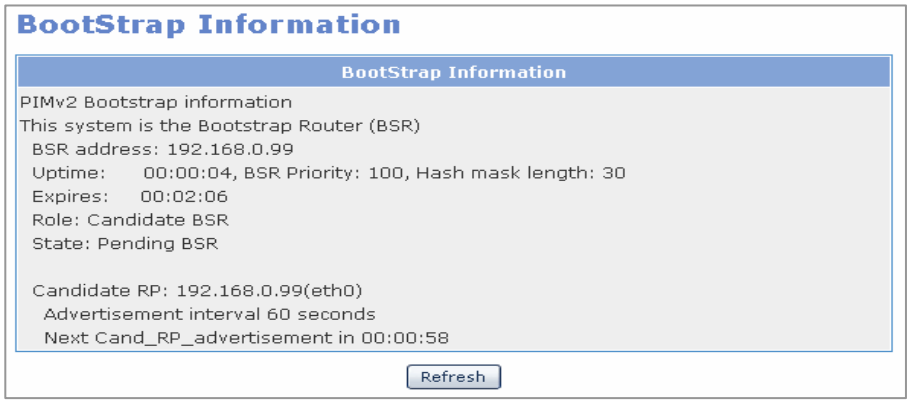
This menu is used to set BSR and RP of PIM-SM protocol. Mark the check box on the right and enter the configuration values. Click the **[OK]** button to apply the values. Mark the check box of the target item and click the [**Delete**] button.



- 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.)

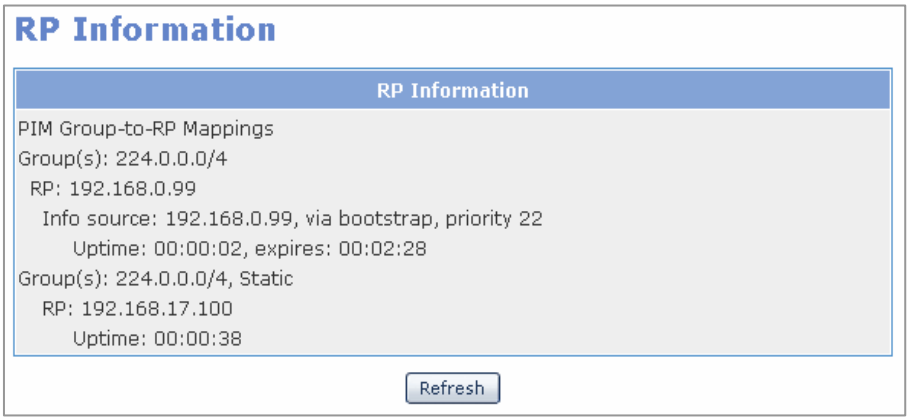
BootStrap Information

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.

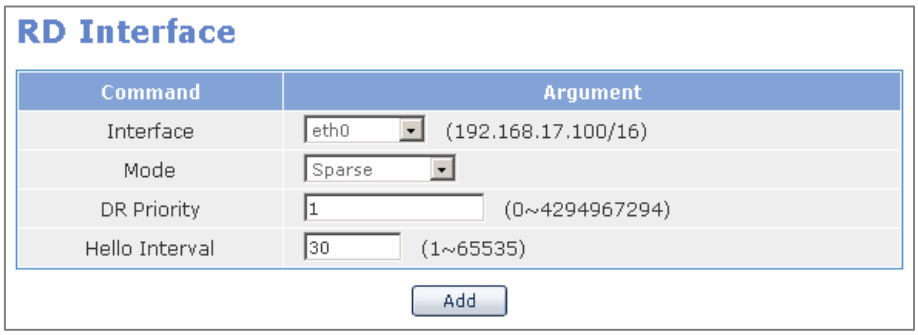


PIM-SM Intf

This menu is used to set PIM-SM VIF.

RD Interface

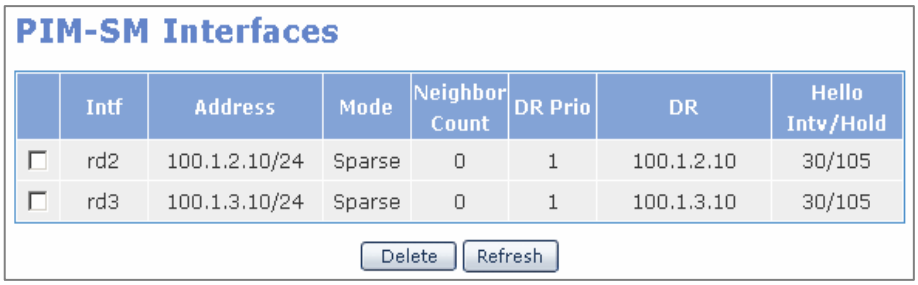
This menu is used to add PIM-SM VIF. Select the target L3 interface from the Interface item, enter the target values, and click the **[Add]** button to add PIM-SM VIF.



- 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

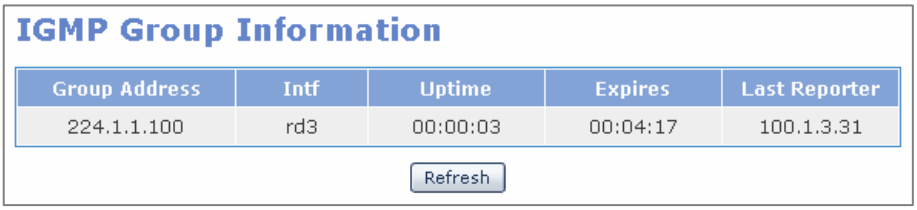
PIM-SM Interfaces

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

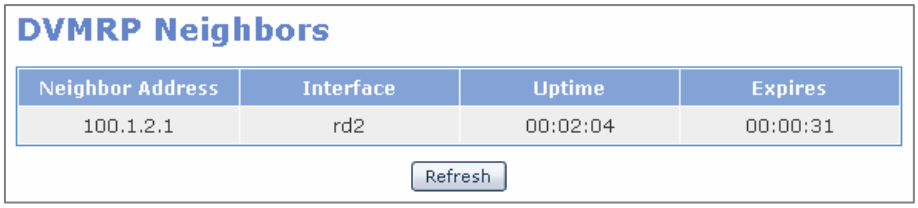
Status

DVMRP

This menu is used to display the DVMRP protocol status.

DVMRP Neighbors

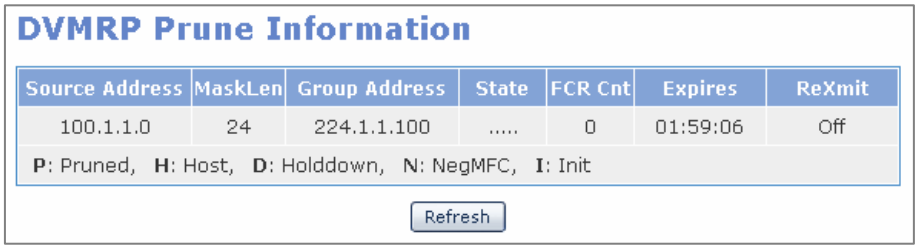
This menu is used to display the information on the DVMRP neighbor whose information is exchanged.



- 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

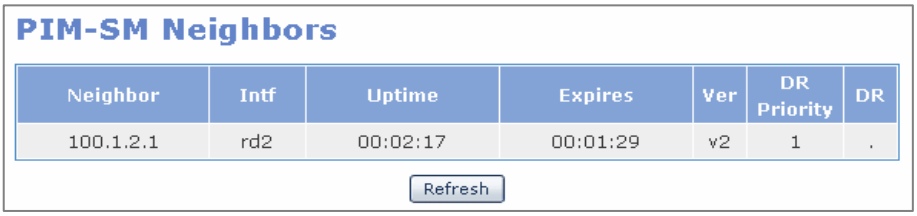
This menu is used to display DVMRP Prune items.



- 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 Menu

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

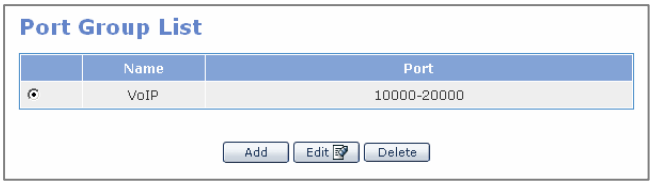
Menu	Submenu	Description
Group	**Port Group**	Retrieves, sets, edits, or deletes a port group
	IP Group	Retrieves, sets, edits, or deletes an IP group
	Filter Group	Retrieves, sets, edits, or deletes a filter group.
	Class Group	Retrieves, sets, edits, or deletes a class group.
Policy	**-**	Set up the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

Group

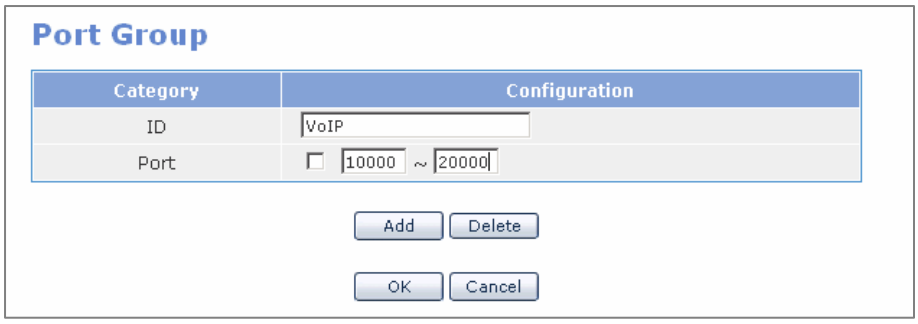
The **[Group]** menu is used to retrieve, set, edit, or delete a port group, an IP group, a filter group, or a class group.

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.



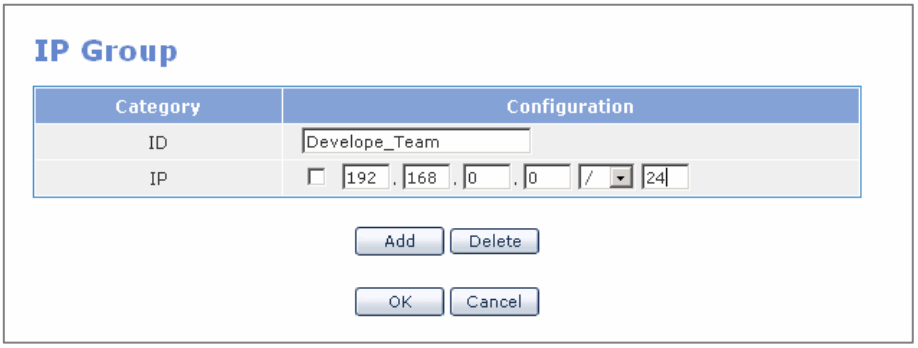
Enter the target ID and port No. and click the **[Save]** button.
Click the **[Add]** button to add a port, and click the **[Delete]** button after marking the checkbox to delete the target port.

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.

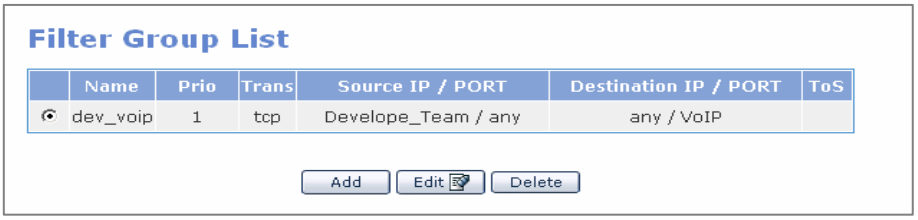


Enter the target ID and port No. and click the **[Save]** button.
Click the **[Add]** button to add an IP, and click the **[Delete]** button to delete the target IP.

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

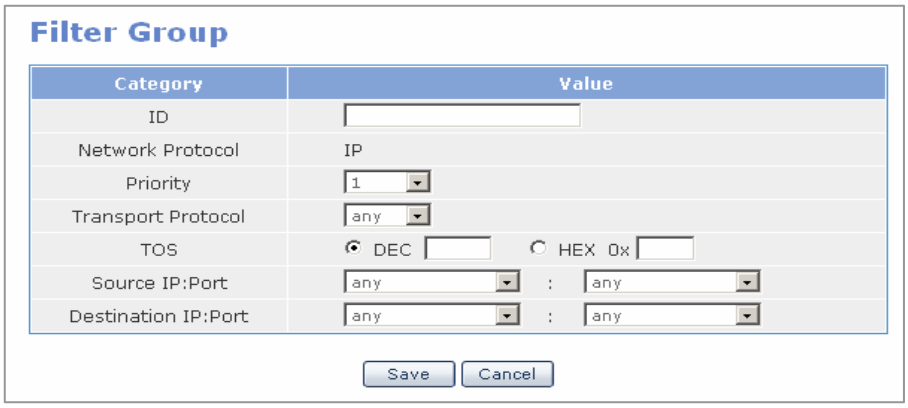
Select **[Filter Group]** to retrieve, set, edit, or delete a filter group.



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.

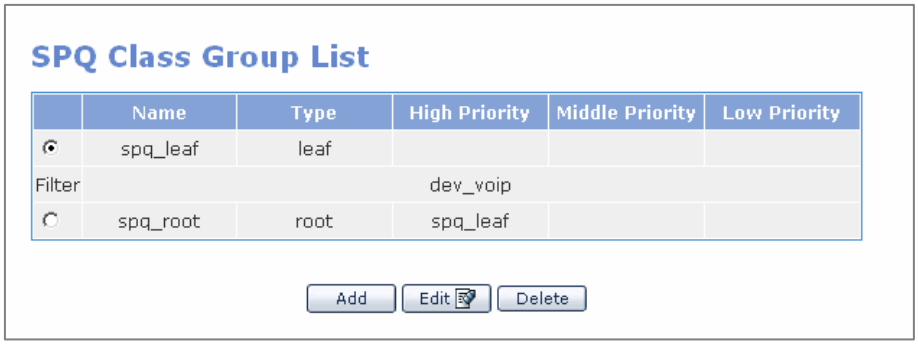


Filter means a configuration filtering for the values in the packet header. Values set in **[QoS]** → **[Group]** → **[Port Group]** and **[IP Group]** are used. Protocols and TOS fields can also be filtered. In addition, priority can be set for each filter and apply the filtering rule according to the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

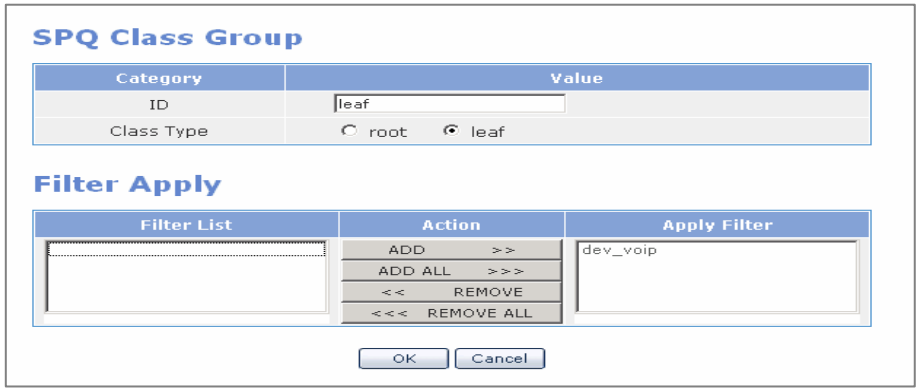
Class Group

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.

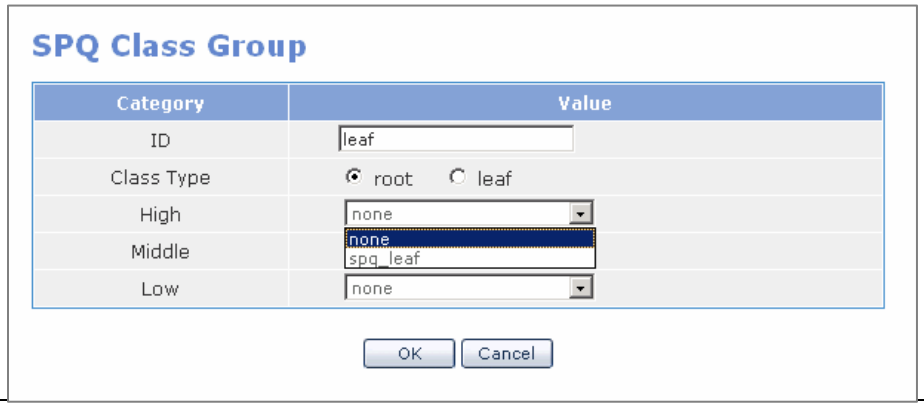
SPQ Class Group



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.



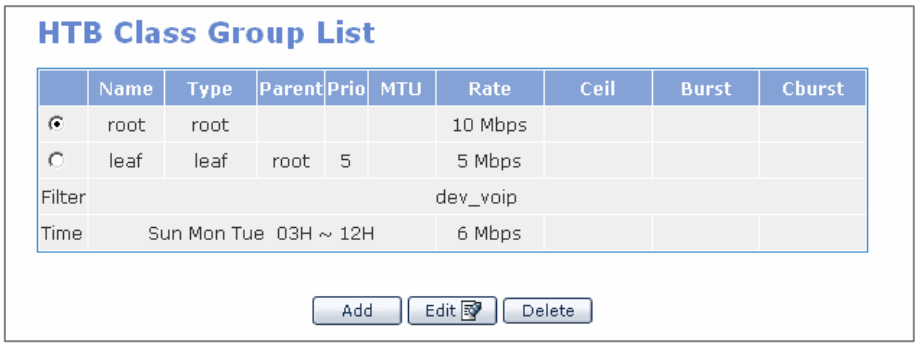
Item	Description
Class Type	Configuration window depends on the type of the class to be set. - root: Sets the root class. - Leaf: Sets the leaf class.
High	Sets the leaf class whose priority will be set to high.
Middle	Sets the leaf class whose priority will be set to middle.
low	Sets the leaf class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

NOTE

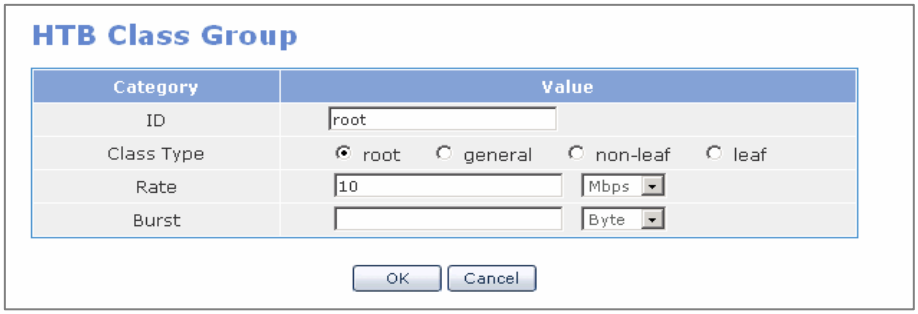
SPQ

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.

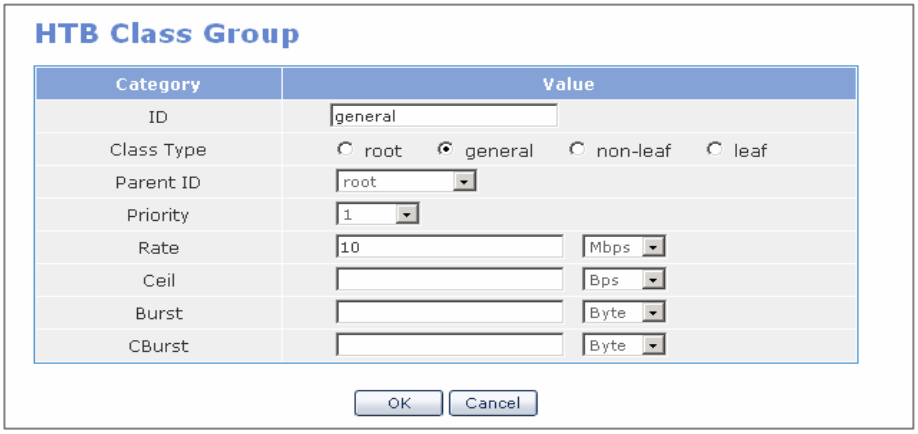
HTB Class Group



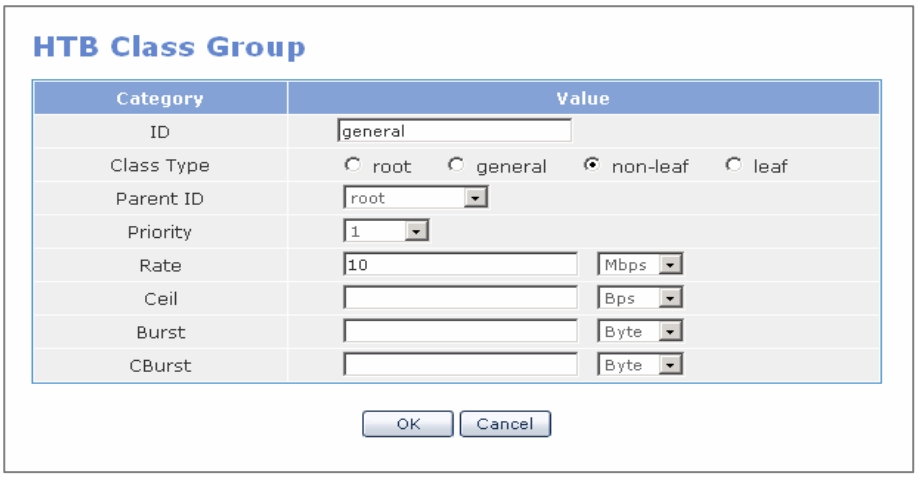
Click the **[Add]** button of HTB Class Group List in the <**HTB Class Group**> window to display the window where HTB class group can be set. If the class type is root, the window is displayed as follows. Set each item and click the **[OK]** button.



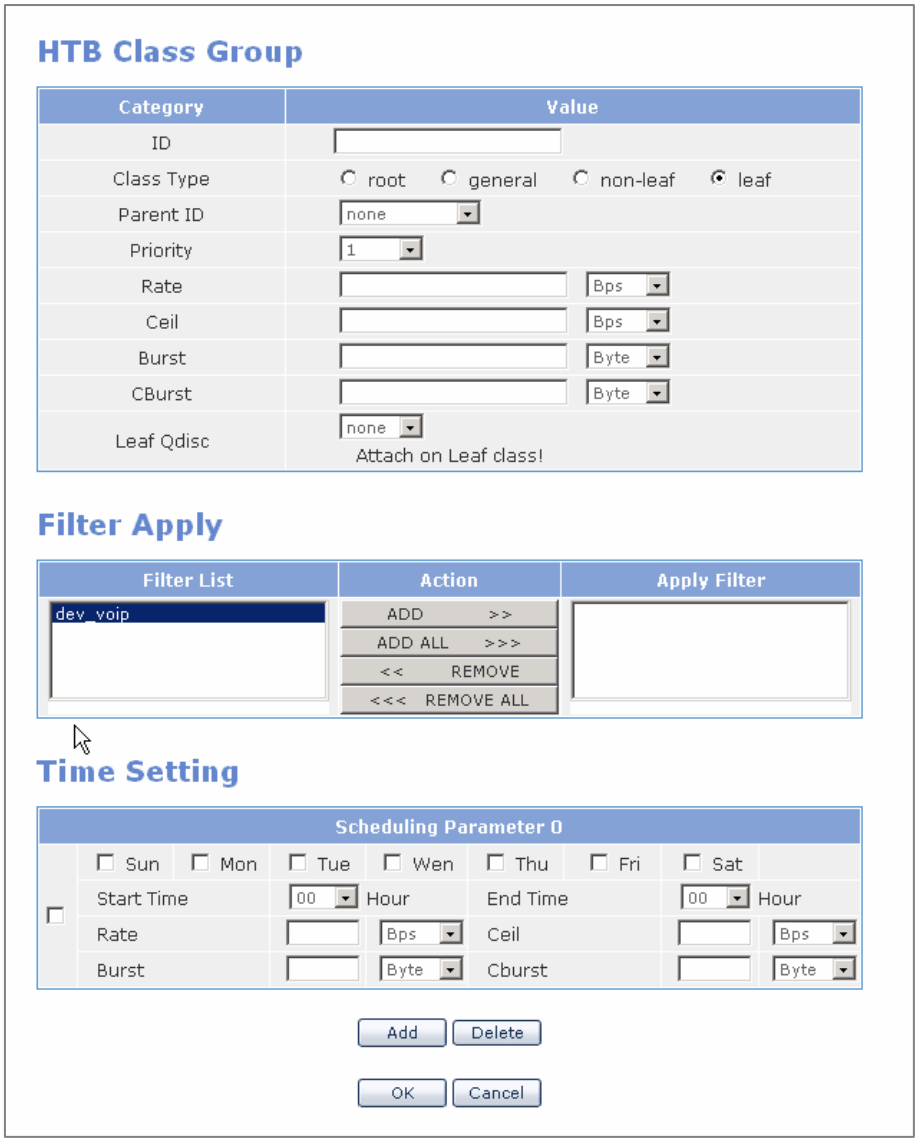
If the class type is general, the window is displayed as follows. Set each item and click the **[OK]** button.



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.



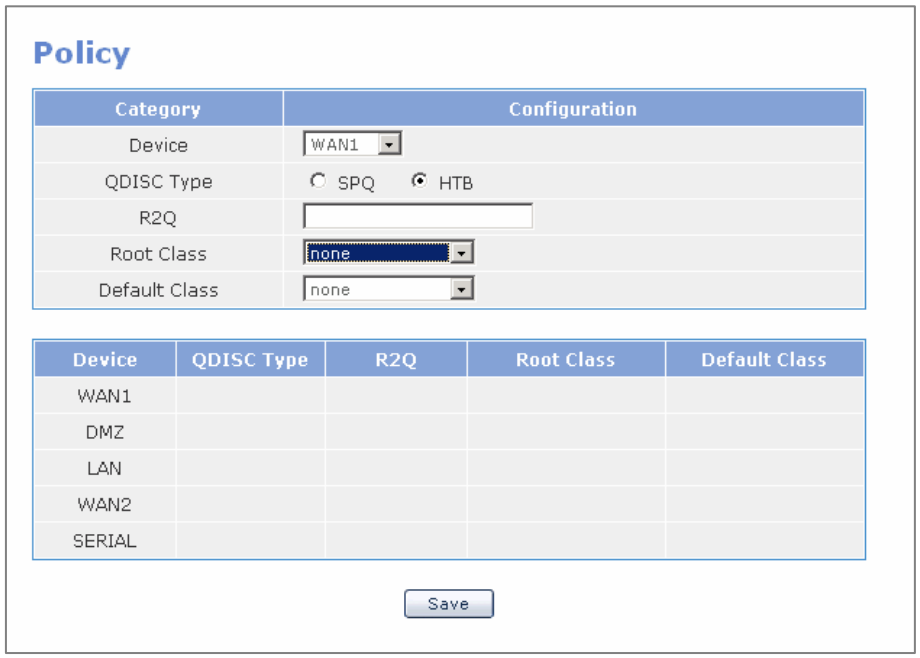
Item	Description
Class Type	Configuration window depends on the type of the class to be set. - root: Sets the root class. - general: Sets the class that connects the root with the leaf classes. - non-leaf: Sets the default class. - Leaf: Sets the leaf class.
Parent ID	If the target class is a child class 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).

Item	Description
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

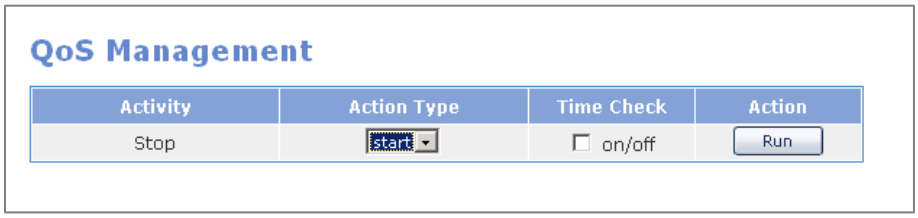
The **[Policy]** menu is used for setting a class for a port. Enter the following items and click the **[Save]** button to select a class for a port.



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.

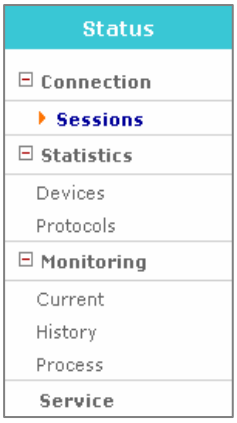
Management

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 Menu

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



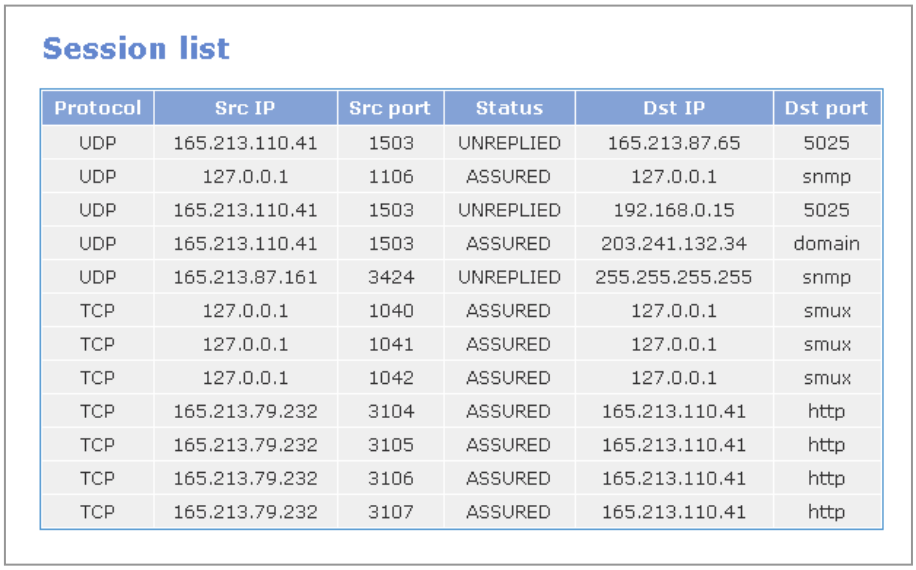
Menu	Submenu	Description
Connection	Sessions	Displays the information on the IP and port connected to the Data Server.
Statistics	Devices	Displays the Data Server network statistics by classifying Tx and Rx of each device.
	Protocols	Displays Data Server network statistics of each protocol.
Monitoring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

Connection

The **[Connection]** menu is used to display the Data Server session connection status.

Sessions

This menu is used to display the information connected to Data Server.



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

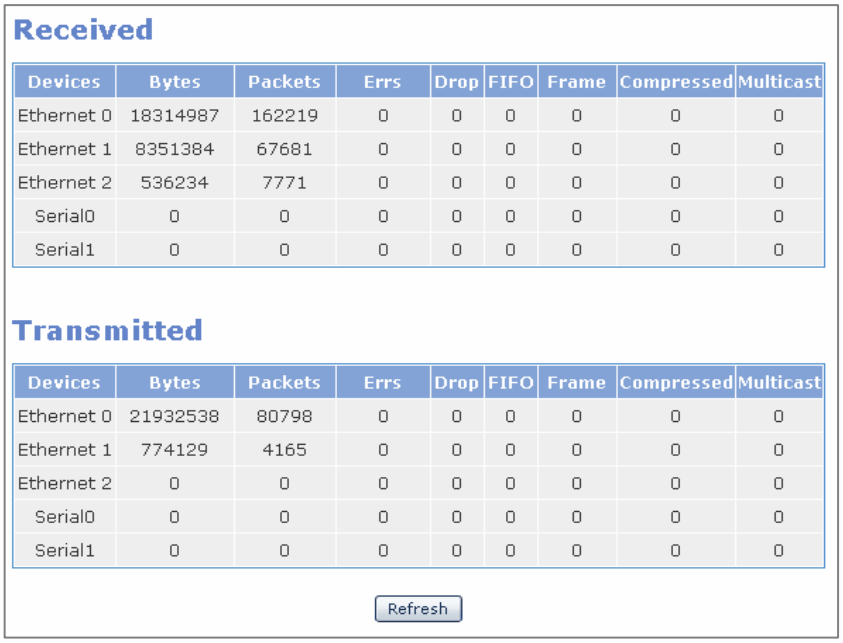
Item	Description
Protocol	Type of the protocol connected with session(UDP, TCP)
Src IP	Source IP
Src Port	Source port
Status	- UNREPLIED: Packets that are expected to be answered are received, but there is no response packet. - ASSURED: There is no response packet. (‘UNREPLIED’ is changed to ‘ASSURED’.)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

Statistics

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

Devices

Select **[Statistics]** → **[Devices]** and display the Data Server 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

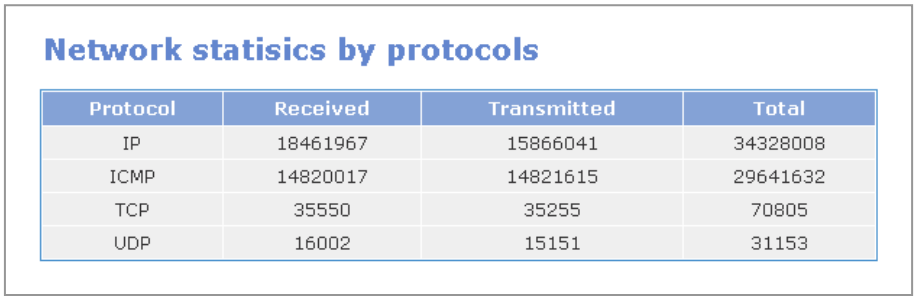
Devices	Bytes	Packets	Errs	Drop	FIFO	Frame	Compressed	Multicast
Ethernet 0	21932538	80798	0	0	0	0	0	0
Ethernet 1	774129	4165	0	0	0	0	0	0
Ethernet 2	0	0	0	0	0	0	0	0
Serial0	0	0	0	0	0	0	0	0
Serial1	0	0	0	0	0	0	0	0

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 the Data Server network statistics of each protocol(Unit: Byte)



Network statisics by protocols

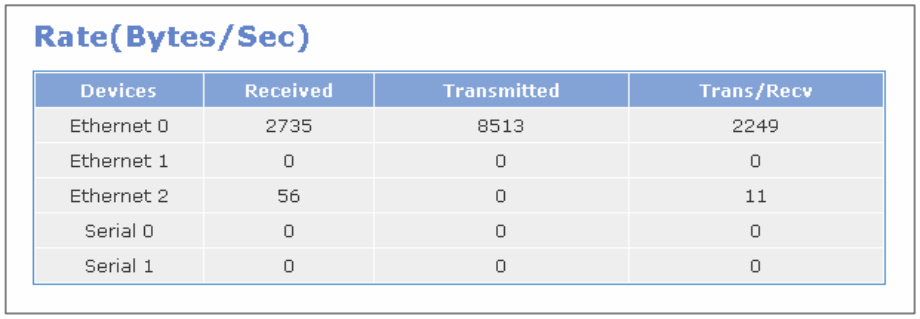
Protocol	Received	Transmitted	Total
IP	18461967	15866041	34328008
ICMP	14820017	14821615	29641632
TCP	35550	35255	70805
UDP	16002	15151	31153

Monitoring

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

Current

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

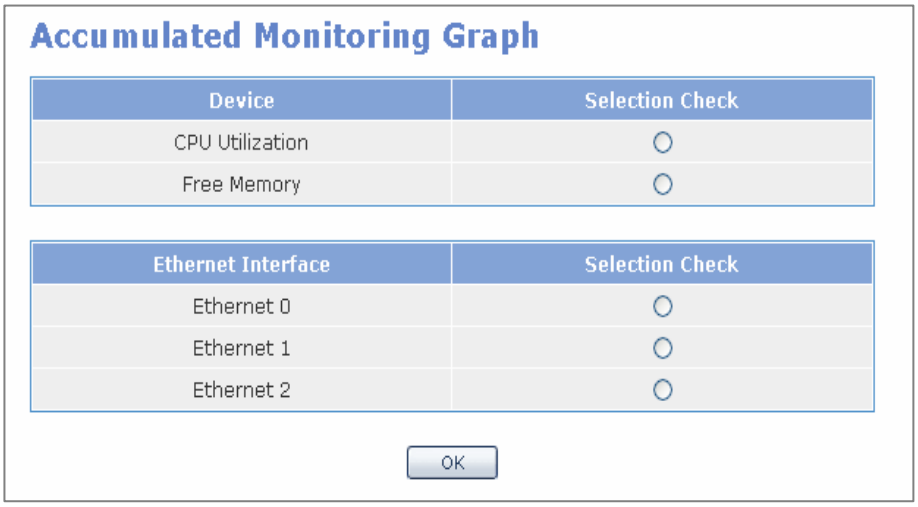


Rate(Bytes/Sec)

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 the Data Server as the accumulation value on an hourly, weekly, monthly, and yearly.

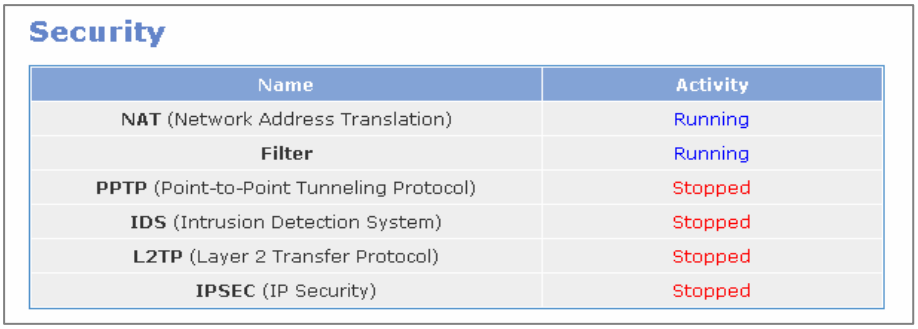


Service

This menu is used to display the status of the Security, Router, and Management services provided by the Data Server 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.

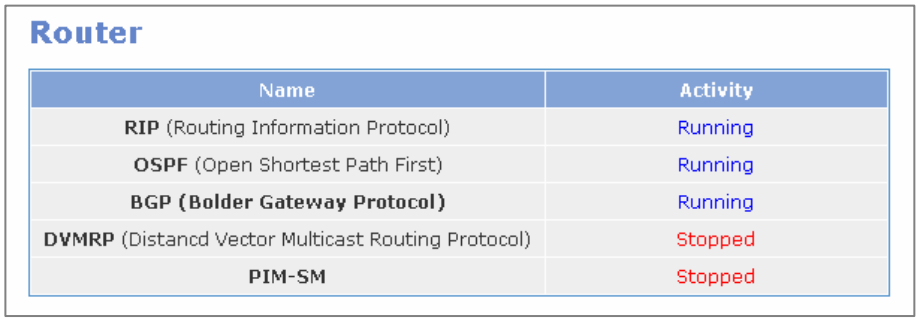
Security

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



Router

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

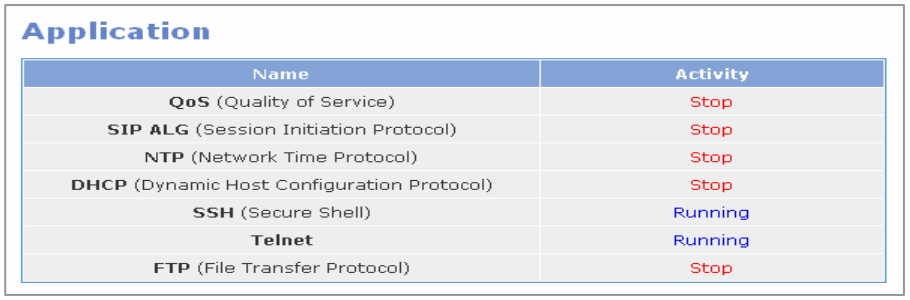


Router

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

Application

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

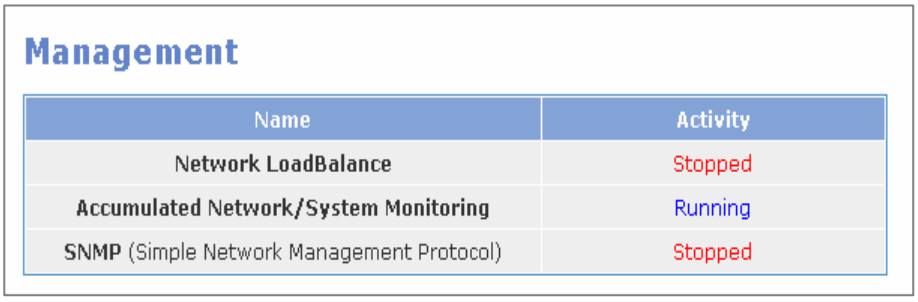


Application

Name	Activity
QoS (Quality of Service)	Stop
SIP ALG (Session Initiation Protocol)	Stop
NTP (Network Time Protocol)	Stop
DHCP (Dynamic Host Configuration Protocol)	Stop
SSH (Secure Shell)	Running
Telnet	Running
FTP (File Transfer Protocol)	Stop

Management

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



Management

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

VPN Menu

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

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

NOTE

Setting up VPN Client in Windows XP/2000

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

IPSec

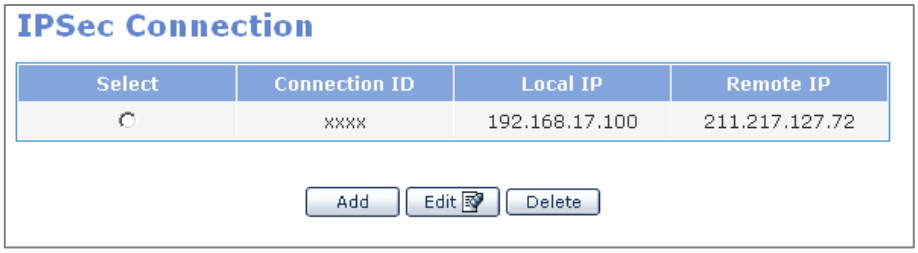
IP Security Protocol(IPSec) provides security services in the IP layer through implementing Internet Key Exchange(IKE). The security service is categorized into two services depending on remote equipment: the services providing security tunnels between local subnet and remote subnet, and between local subnet and remote host.
Even if IPSec can be set up to provide a security tunnel between local host and remote host the Data Server 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 7200 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.

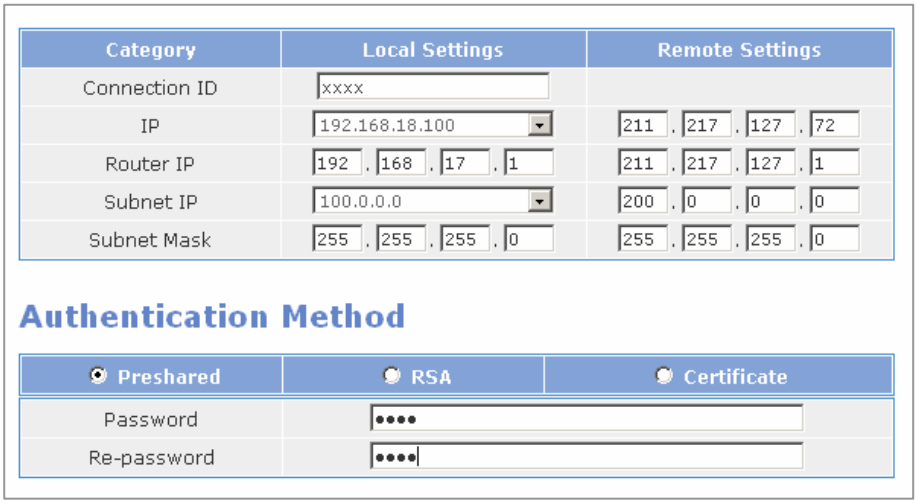


The menu buttons are defined as shown below:

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'.

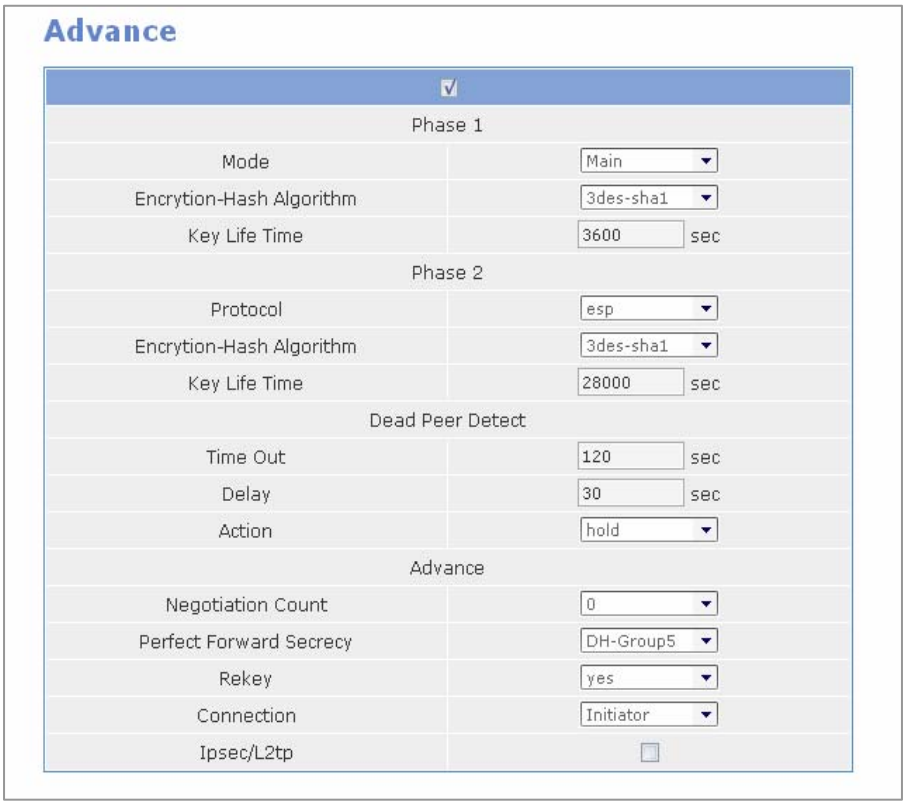
NOTE

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.

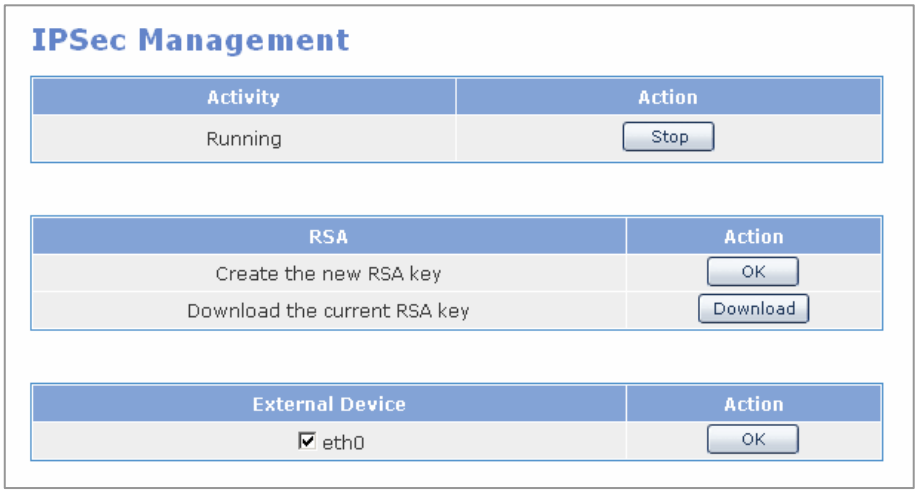


Item		Description
Phase1	mode	Ike mode - main: Configures a secure channel to perform the ISAKMP exchange of phase one - aggressive: Different type of phase one, which is more simple and faster than the main mode
	Encryption-Hash Algorithm	Supporting Algorithm 3DES-MD5, 3DES-SHA1, AES128-MD5, AES128-SHA1,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

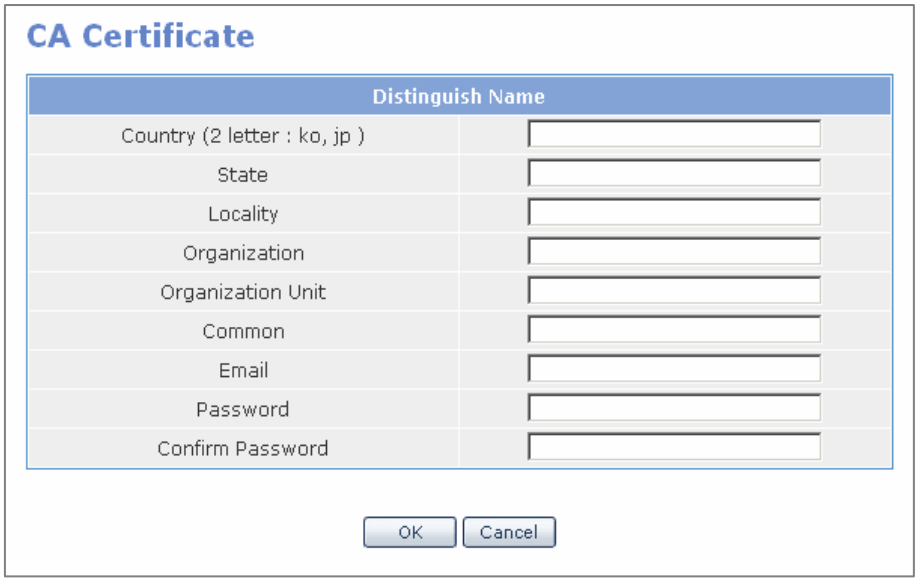
Certificate

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:

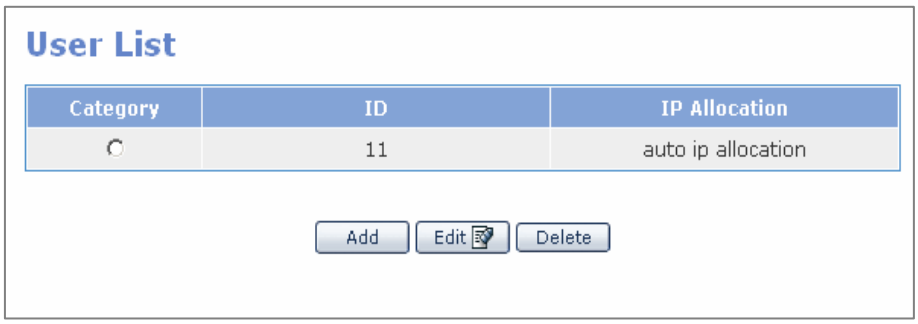
Item	Description
Common name	Name
Email address	Email address
Password	Certificate password
Confirm Password	Confirming certificate password

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.

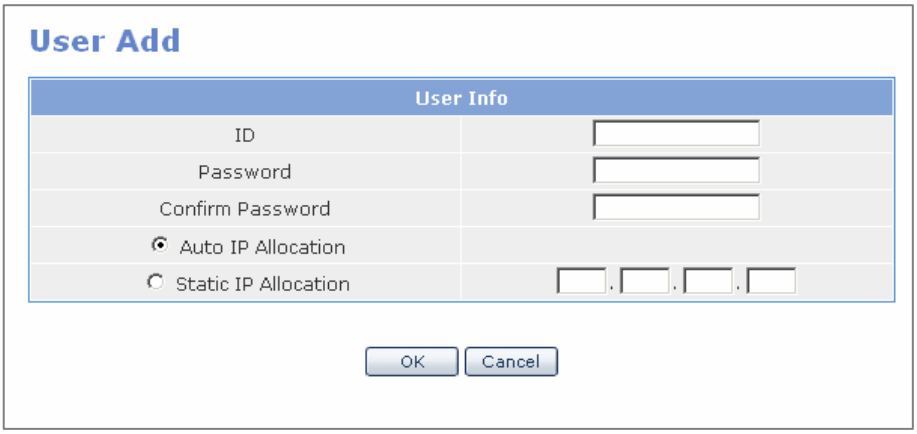


The menu buttons are defined as follows:

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

Add

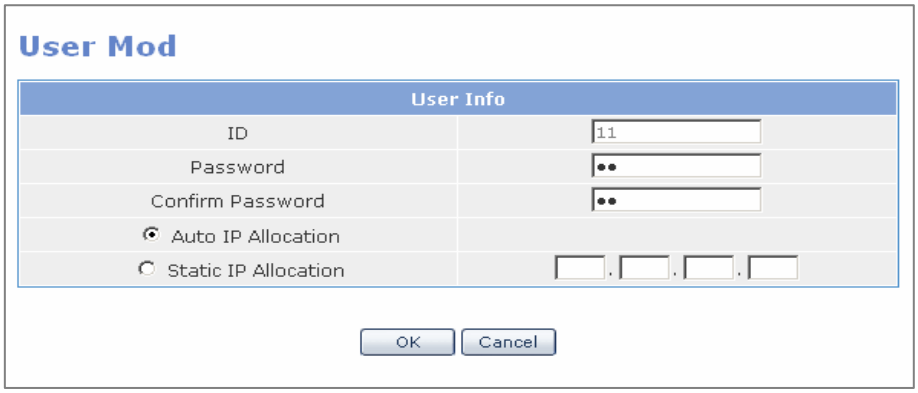
If clicking the **[Add]** button on the **<L2TP administrator list>** window, the following window appears. Enter each item and click the **[OK]** button to create a L2TP administrator.



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)

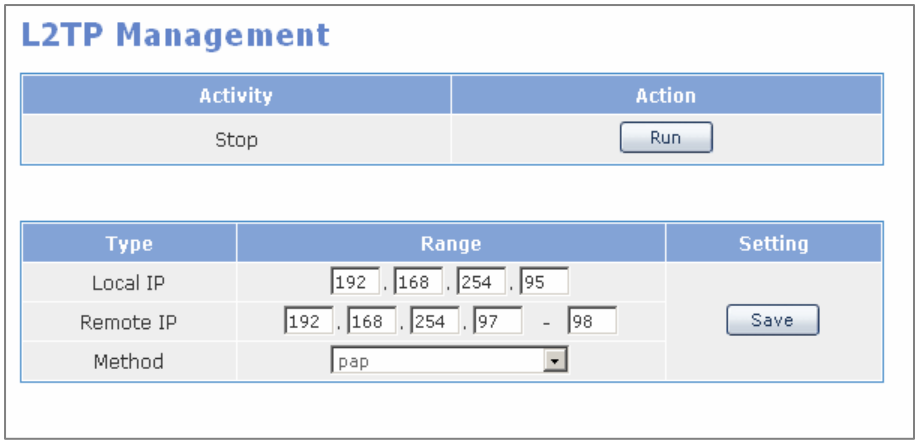
Edit

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.

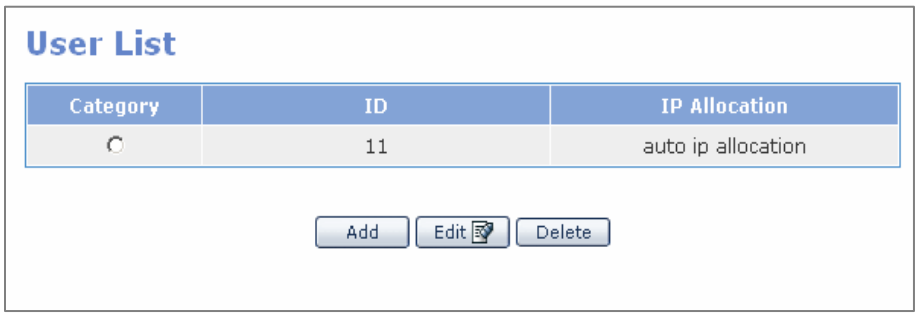
For example, if the number of IPs for 'Local IP range' is 10 and that for 'Remote IP range' is 20, only 10 calls will be set.

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

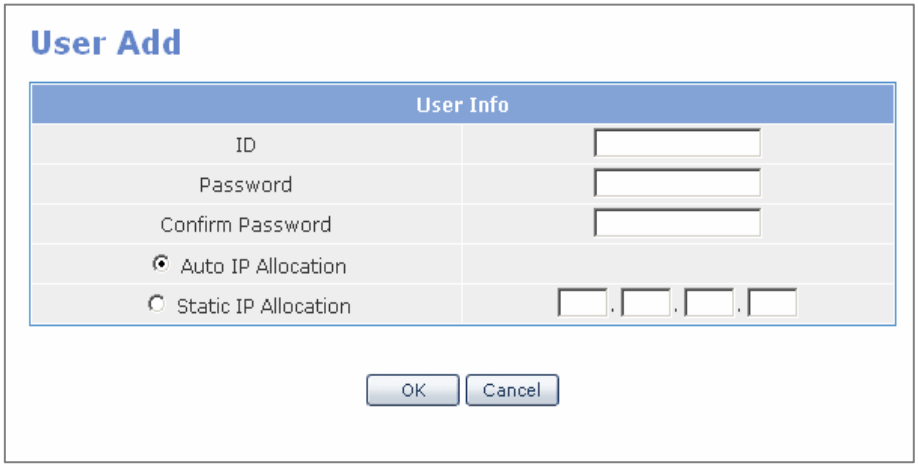
On the **[PPTP]** → **[Configuration]** menu, the administrator can create, modify, delete, and retrieve VPN tunnel data.
The menu buttons are defined as follows:



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

Add

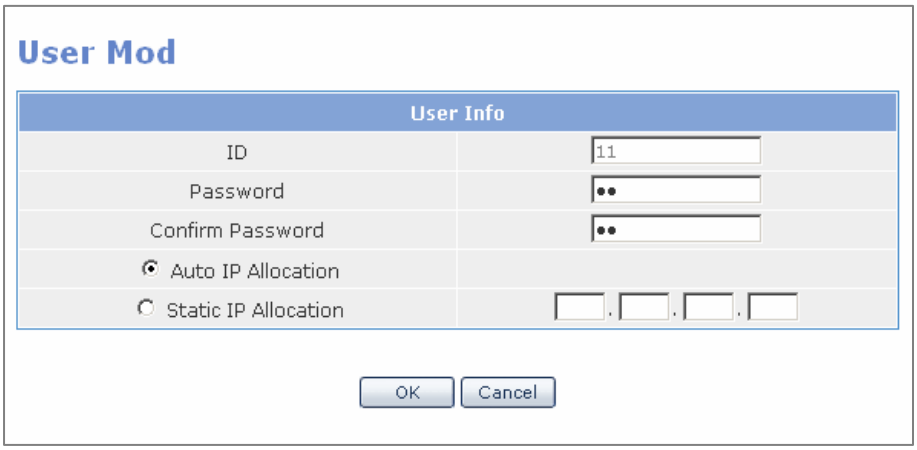
[Add] → **<PPTP administrator list>**



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)

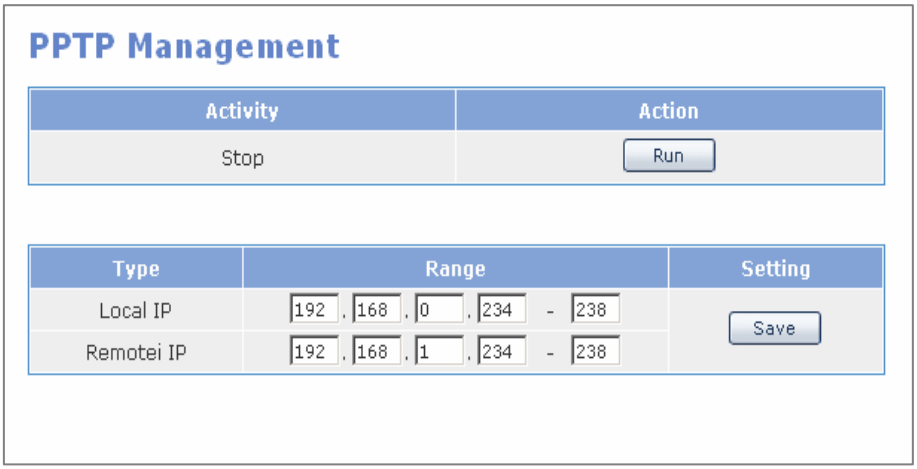
Edit

[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.



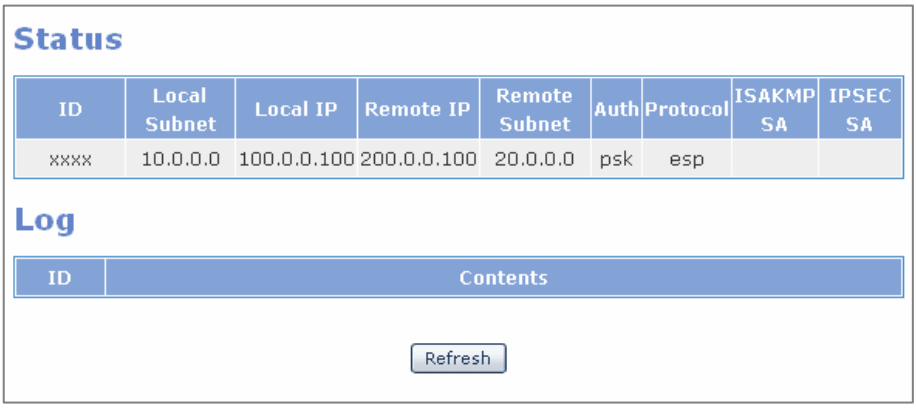
The administrator can set up the IP range of the remote client that uses dynamic IP in the 'Local IP range' item, and set up the IP range of PPP demon responsible for remote client in the 'Remote IP range' item. The encryption method supports 'pap' and 'chap'.

CAUTION

Setting up IP Range

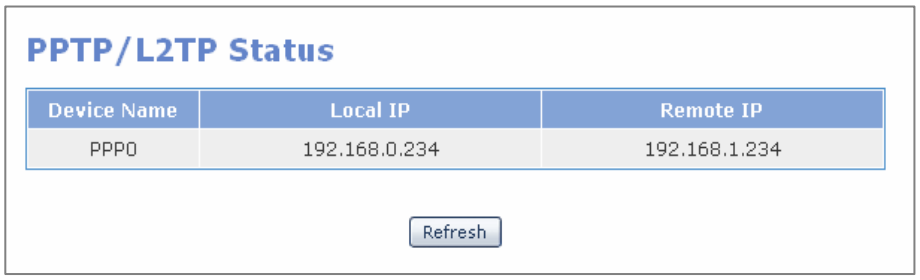
The number of IPs for the 'Local IP range' and that for the 'Remote IP range' should be identical.
For example, if the number of IPs for 'Local IP range' is 10 and that for 'Remote IP range' is 20, only 10 calls will be set.

Status



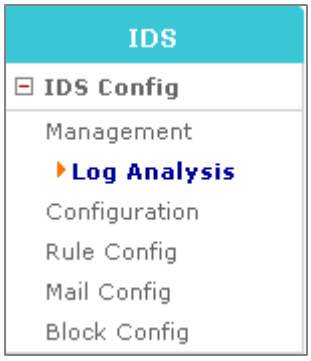
Check the IPSec tunnel set up in **[STATUS] → [IPsec]** to insure it is properly connected.

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:

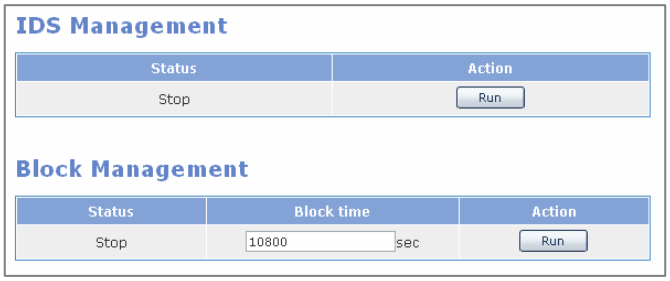


Menu	Submenu	Description
IDS Config	Management	Start or stop the IDS application
	Log Analysis	Classifies the IDS logs that are currently stored in the WIM Data Server
	Configuration	Sets up the rules and detection levels for the IDS application.
	Rule Config	Updates the IDS rule files.
	Mail Config	Registers the mail server and email address of the IDS manager.
	Block Config	Registers the trusted IP Address (IP Addresses that are not set to be blocked)

IDS Config

Management

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



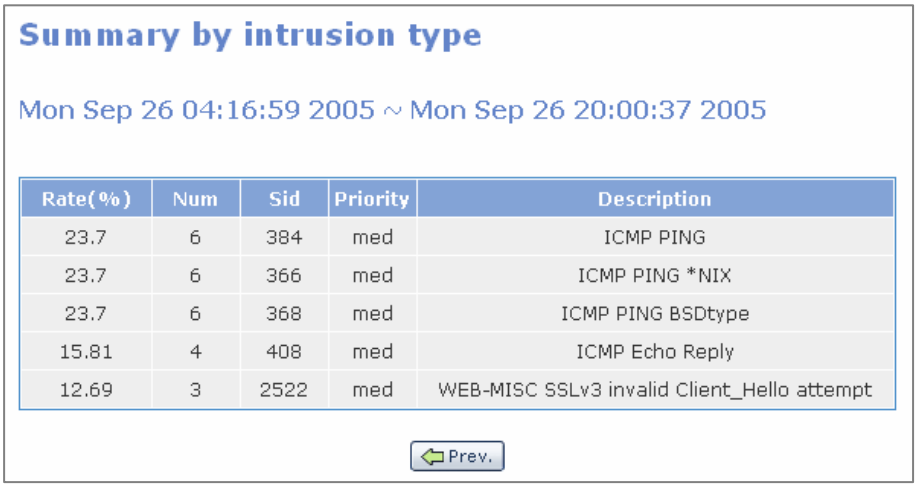
Item	Description
Status	- Running: Status that the module is in operation - Stopped: Status that the module is not in operation
Action	Click the **[Run]** button to begin the IDS application. Click the **[Stop]** button to stop the IDS application.
Block time	When the Data Server detects an intrusion from an IP Address then that IP Address is blocked until this timer is reached.

Log Analysis

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

Intrusion Type

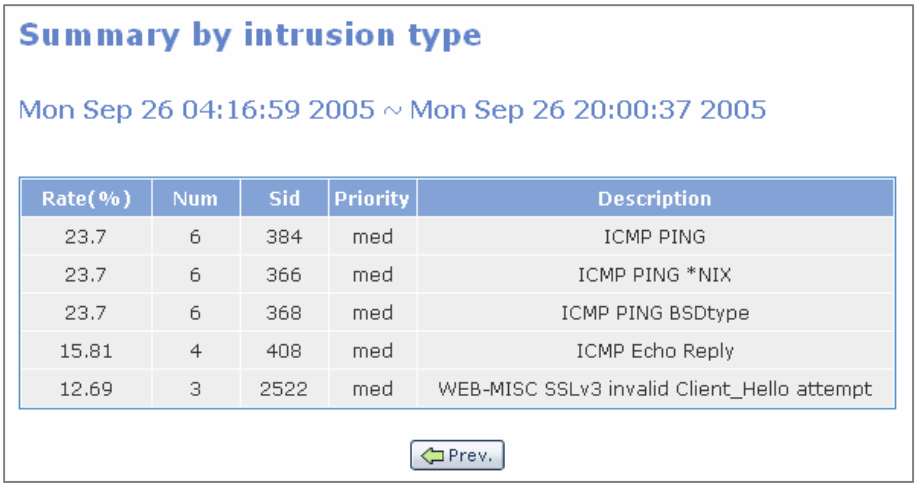
The administrator can summarize alerts by type. If selecting the category of Intrusion Type, the following window appears:



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 7200 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

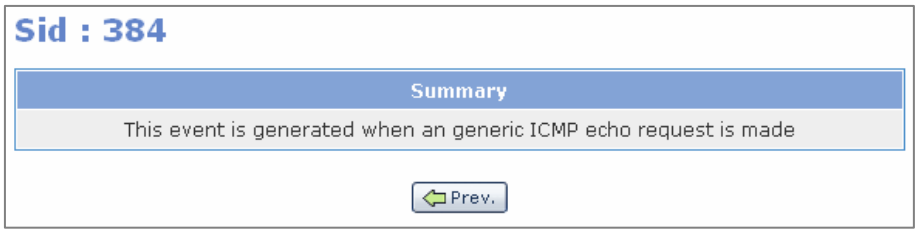
Intrusion Type

The administrator can summarize alerts by type. Select the category of Intrusion Type then following window appears:



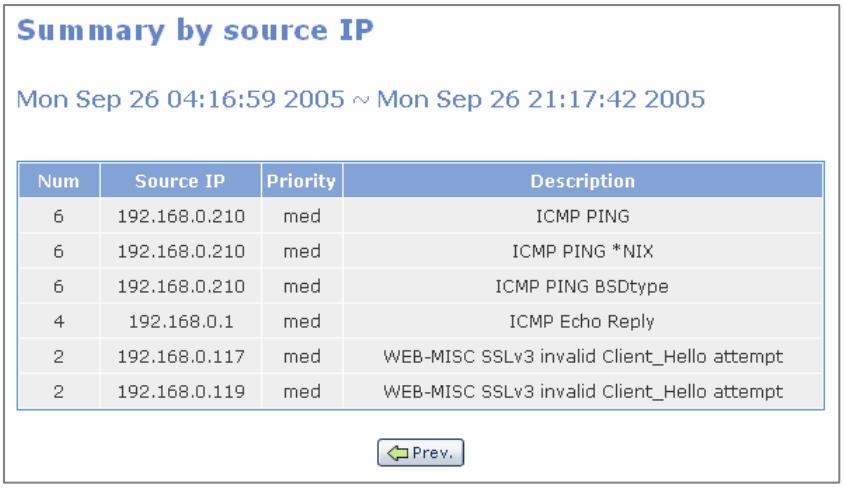
Item	Description
Rate(%)	Monitors logs detected by IDS according to type and displays logs as a percentage(%).
Num	Number of logs detected by IDS according to type.
Priority	Risk level depending on the rules level of IDS. - high: Rule level is one day(the highest risk level) - med: Rule level is 2 or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

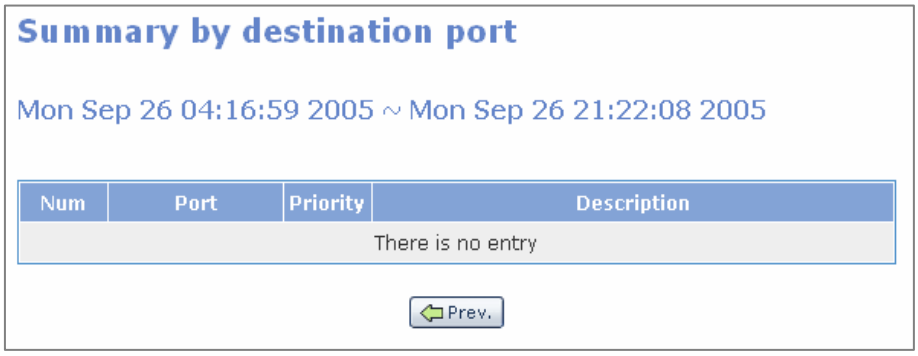
Destination IP

The administrator can summarize alerts by the destination IP. Select this category and 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. Select this category and then the following category appears:

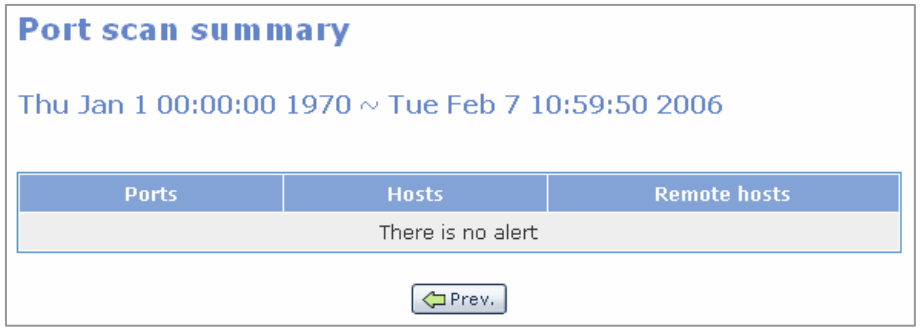


Item	Description
Num	Numbers of detected by IDS according to port when attacked Destination IP is a network (e.g., LAN).
Port	Attacked host IP of logs detected by IDS.

Item	Description
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

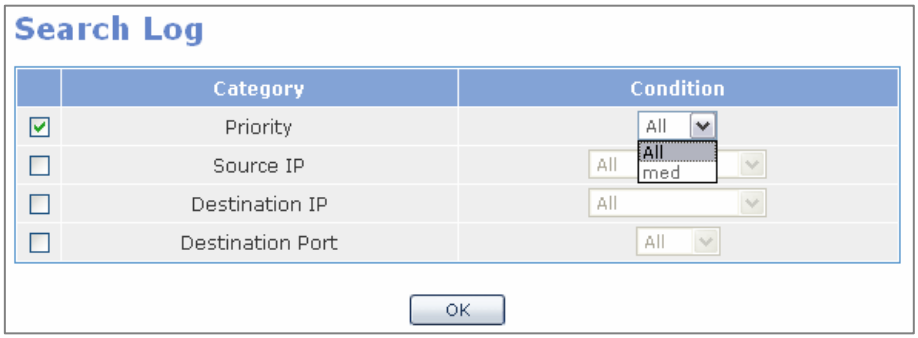
The administrator can summarize alerts for Port Scan. Select this category and the following window appears:



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



Select the category including the desired condition and the selected box will be 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:

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

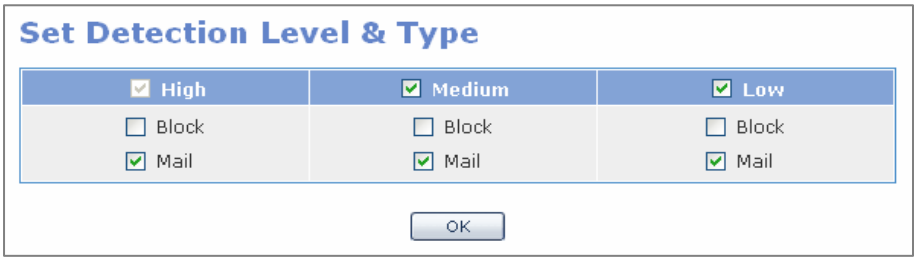
The administrator can set up a the network which needs to be monitored. The interface needs to be set as WAN and must be a static network.

Set Detection Level & Type

The Data Server intrusion type is classified as High, Medium or Low according to the risk level. The administrator can set up an intrusion alert when an intrusion exceeding the level occurs. In addition the administrator can set up the associated operations for each level.

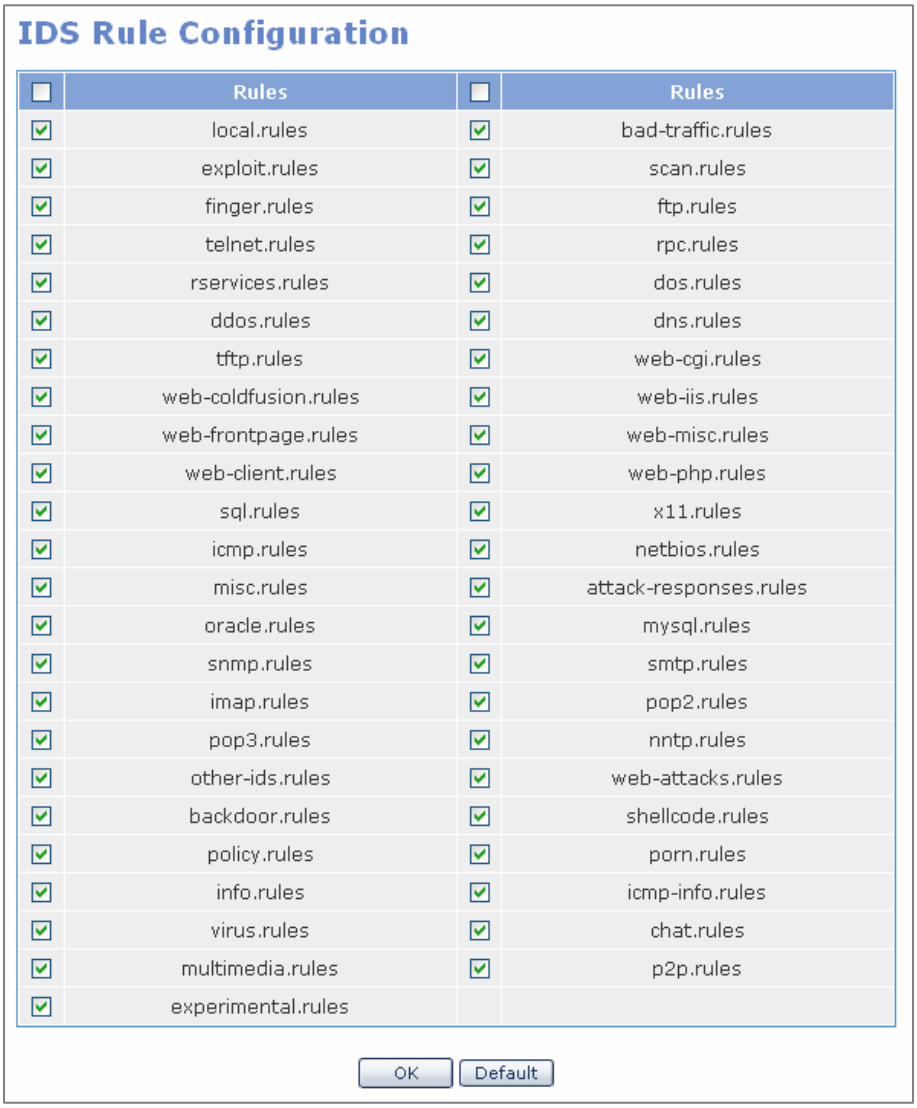
When setting up a block, the block is associated with the block module. If an intrusion corresponding to the relevant level is detected, the relevant IP Address is blocked and prevents access to the system for a configured time.
(Refer to 'Block Config')

When setting up Mail, the IDS mail is transmitted when the alert occurs.
(Refer to 'Mail Config')



IDS Rule Configuration

This page is used to set up the rule file for the IDS application.



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

When an administrator checks 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 application to the latest version. The following window shows the version of the current rule-set file and the released date:

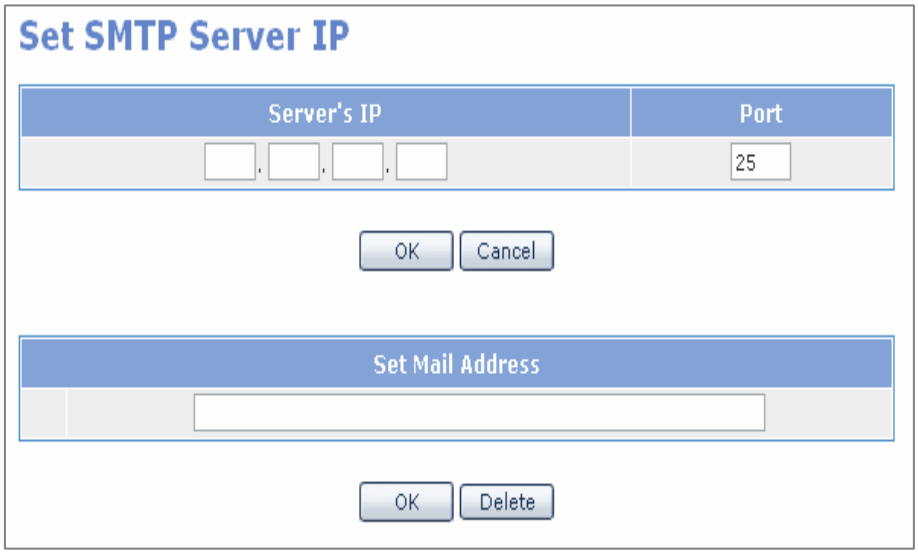
NOTE

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

Mail Config

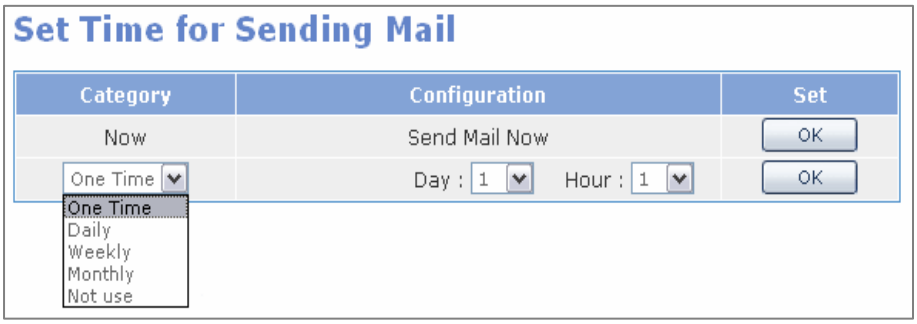
Set SMTP Server IP

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.

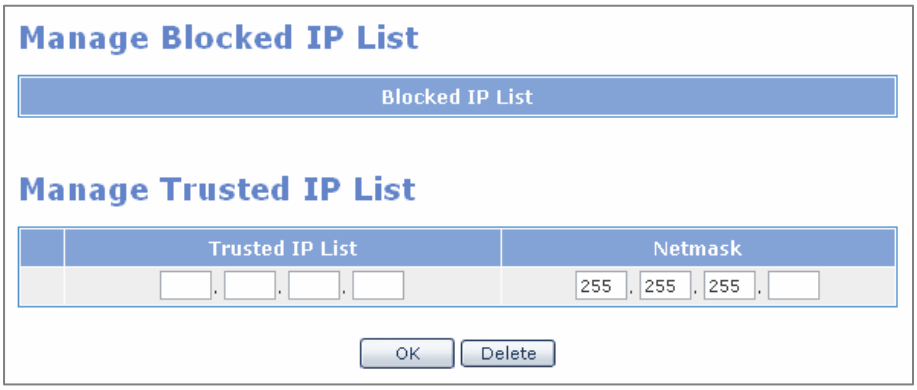


If clicking the button in the Now category, an email is sent to the e-mail address stored above the recorded alert. Select One Time to send a mail at the relevant time. The other items are used to check if there is an alert and send to Mail at the configured time daily, weekly or monthly.

> **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

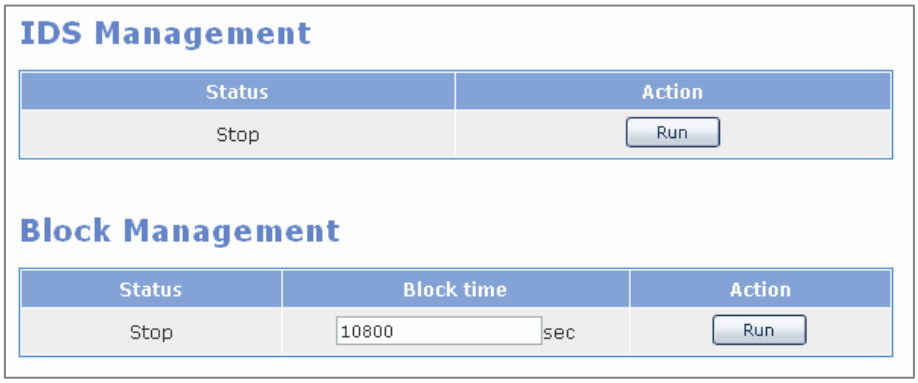
If an intrusion is detected when the IDS module and block module are all in operation, the IP of the block that is set up at Configuration Menu according to the intrusion risk, is blocked to access to the system for an amount of time. Manage Blocked IP List shows the list of IP that the access is blocked.

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 Services]** Menu. The submenus for VoIP Services will be displayed on the left top as follows:

Menu	Submenu	Description
DSMI Configuration	SM Interface (future release)	Enable or disable items related to the Message Data transmission for the communication with the system manager (SM).
	Module Interface	Select the WAN VoIP interface and set the environment for the communication with Call Server and Feature Server.
	Management	Start or stop the programs for the communication with the SM Interface, Call Server, and Feature Server. Set the Data Server so that the execution of these programs is automatic on reboot.
External Server	External FS (future release)	Sets or deletes the IP Address of the Feature Server existing on the external network (A public network when the NAT is used).
	DIST Config (future release)	Transmits the message received via the externally designated port into the terminal designated at the internal network.

Menu	Submenu	Description
DHCP Server	Configuration	Set the internal network that operates the DHCP Server. In addition set the IP addresses for the DHCP scope. The IP pool for Call Server, Feature Server, MGI, IP Phone, SIP Phone, and general data terminal are set here as well.
	Management	Start or stop the DHCP Server, and configure the system so that the DHCP Server runs automatically when the Data Server reboots.
	VoIP Status	Displays the IP terminal information of the OfficeServ 7200 system receives from Call Server or Feature Server when the program for the communication with Call Server or Feature Server is executed.
	Leases Status	Displays the DHCP lease status.
DHCP Relay Agent	Configuration	Set the Interface and DHCP Server to be relayed,
	Management	Start or stop the DHCP Relay Agent.
VoIP NAPT	Status	Displays the information on the Static NAPT for the OfficeServ 7200 VoIP service. This information is automatically set when the program for the communication with Call Server and Feature Server is executed. The information is displayed when the setup is completed.
SIP ALG	Configuration	Set up the SIP environment.
	Management	Start or stop the execution of the SIP ALG. Configure the Data Server so that the execution of this service is made when rebooting the system.

Configuration

Set the environment of the Data Server Module Interface(DSMI) using the VoIP Service **[Configuration]** Menu.

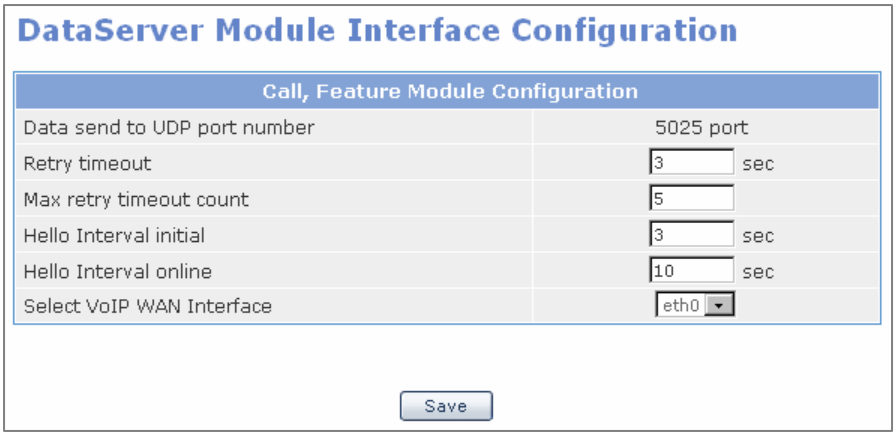
SM Interface

SM Interface: The System Manager Interface is a network management tool that is not available at this time. In a future release of the OS 7200 Data Server the The NMS (Network Management System) will become available

.

Module Interface

Set the VoIP WAN Interface using the **[Module Interface]** Menu. Other environmental settings used for communication between the Data Server and the Call and Feature Servers are set here as well.



Item	Description
Data send to UDP port number	This view only field shows the information on the UDP port used for the communication with Call Server and Feature Server.
Retry timeout (Sec)	The Call Server, Feature Server, and the Data Server communicate using the UDP protocol. If the Data Server does not receive the requested UDP data it requests a retransmission. If this field is set to '3', when a packet is lost and another is not received after its retransmission is requested, the retransmission is requested three seconds afterward. When that requested packet is not received for three seconds a time out occurs.
Max retry timeout count	This parameter sets the number of the retransmission requests. when the packets continue to be lost while sending and receiving the information to and from the Call Server and Feature Server. For example, the Retry timeout item is set as '3', and this item is set as '5', the retransmission is requested five times for three seconds. If the requested packet is not received the request of the retransmission stops.
Hello Interval initial	This parameter sets the cycle of sending the Hello message. The Hello is a message that is sent and received periodically in order to recognize the status of the Call Server and Feature Server.
Hello Interval online	This parameter sets the cycle of sending the Hello message After the initial Hello message.. The value of this item should be set larger than that of the 'Hello Interval initial' item.
Select VoIP WAN Interface	In order for VoIP Services to work this parameter must be selected and saved.

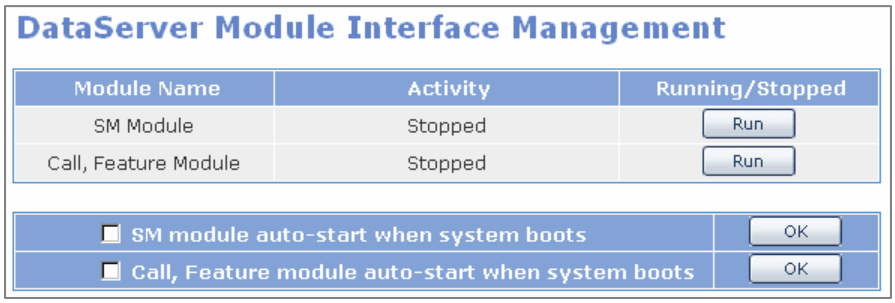
CAUTION

Select VoIP WAN Interface

Although it appears as if this parameter is already set it still must be selected and saved in order for VoIP services to run properly.

Management

The Call and Feature Servers can be started or stopped by selecting the **[Management]** menu. If an automatic restart of the Call, Feature Module service is needed upon a reboot of the OS 7200 Data Server then the 'Auto Start', box must be checked.



CAUTION

SM Module: The System Manager Module is a network management tool that is not available at this time. In a future release of the OS 7200 Data Server the The NMS (Network Management System) will become available

External Server

This feature will become available in a future release of the OS 7200 Data Server.

External FS

Not available until future release

> NOTE
>
> **Feature Server in the internal network**
>
> The Feature Server feature will become available in a future release of the OS 7200 Data Server

DIST Config

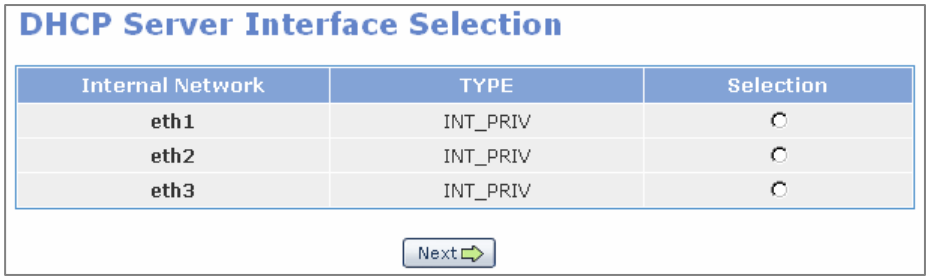
Not available until future release

DHCP Server

This Menu is used to start or stop the DHCP Server.

Configuration

Select the Internal Network that is to receive DHCP addresses from the Data Server using the **[Configuration]** Menu.

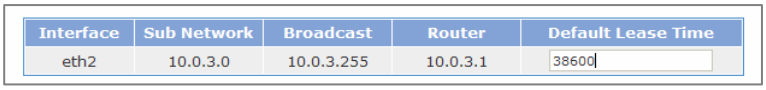


To begin the DHCP Server configuration select the radio button of the Internal network and then click the **[Next]** button.

The <DHCP Server Configuration> screen displays the basic information on the device selected on the <DHCP Server Interface Selection> screen.
In addition the administrator can program the IP Addresses of the OfficeServ 7200 Call Server, IP phones, SIP phones, and data terminals, These devices must be on the same subnet which is defined in the DHCP scope.

DHCP Server Configuration

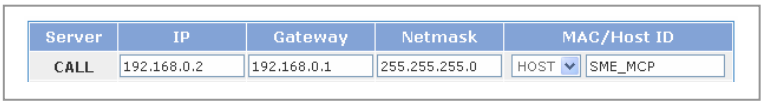
This displays the general information for allocating DHCP to clients.



Item	Description
Sub Network	Subnetwork information. This value is set in the **[/Network]** Menu. It selects the Sub Network based on the IP Address of the Ethernet Interface
Broadcast Address	Broadcast address. This value is set in the **[Network]** Menu. It selects the Broadcast Address based on the IP Address of the Ethernet Interface
Router Address	Router address. This value is set in the **[Network]** Menu. It selects the Router Address based on the IP Address of the Ethernet Interface
Default Lease Time	Basic release allocation time of the IP address. The IP Address release time for the overall IPs that are to be provided via DHCP Server can be set in increments of seconds.

CALL Server

This field sets the Call Server's IP. This is the IP Address of the MCP of the OS 7200 system. When authenticated as host, the 'Host ID' is designated as 'SME_MCP' as its default value.



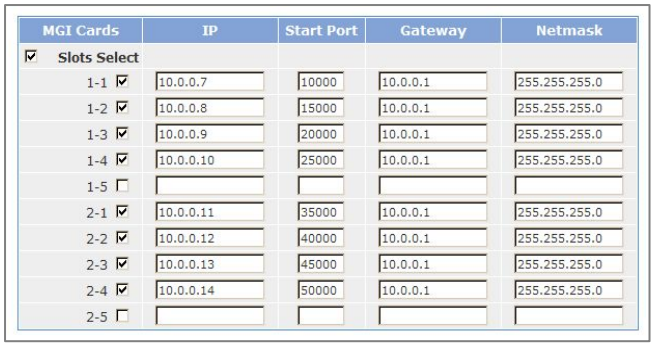
Item	Description
IP	Call Server's IP address
Gateway	Gateway Information
Netmask	Sub Netmask information
MAC/Host ID	Types of the client authentication - NONE: Execute the DHCP IP request without the authentication - MAC: Authenticates with MAC. - HOST: Authenticates with HOST ID(Default value: SME_MCP)

Feature Server

This feature will be supported in a future release of the OS 7200 Data Server.

MGI Cards

This window sets the IP Addresses of the MGI card/s mounted in the system.
First check at the 'Slot Select' check box. Second check at the checkbox on the left side of each item. Last enter the IP Address, External IP Port, Gateway, and Sub Netmask of the MGI card/s.



Up to ten MGI cards can be entered into this table. The figures on the left side indicate the locations of the cabinet-slots. The 'Start Port' means the number of the first port among the 32 external ports where the services are to be provided in the MGI card. If there is no entered number, the setup is autumatically made as the values increasing by 5000 from no. 1000 as the orders of the cabinets or slots.

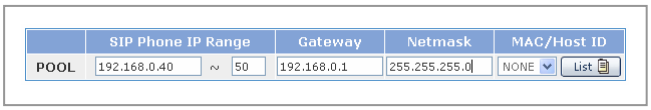
IP Phone

This defines the IP range of the IP phones that are to use the DHCP scope of the Data Server. The DHCP IP pool allocated in this menu sets the authentication of the ITP-5000 series IP phone and the allocation of the IP.

Item	Description
IP Range	The IP range of the IP phone(the maximum range:120 pieces). When entering an IP, enter '192.168.0.20~20'.
Gateway	The gateway information entered at the CALL Server Item.
Netmask	The netmask information entered at the CALL Server Item.
MAC/Host-ID	The client authentication type - NONE: Executes the DHCP IP request without the authentication. - MAC: Click the **[List]** Button to enter the MAC address for the authentication. - HOST: Uses the HOST ID internally specialized. Authenticates the ITP-5000 series phones.

SIP Phone

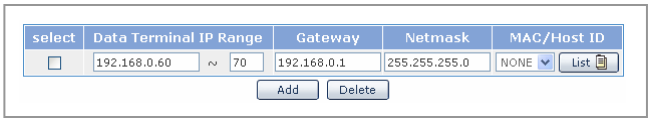
This defines the IP range of the standard SIP phones that are to use the DHCP scope of the Data Server.



Item	Description
IP Range	The IP range of the SIP phone (Maximum range:120 pieces). When entering one IP, enter '192.168.0.40~40'.
Gateway	The gateway information entered at the CALL Server Item.
Netmask	The subnet mask information entered at the CALL Server Item.
MAC/Host-ID	The client authentication type - NONE: Executes the DHCP IP request without the authentication. - MAC: Click the **[List]** Button, and enter the MAC address of the SIOP phone for the authentication. - HOST: Click the **[List]** button and enter the HOST ID because the internally specialized HOST ID is not used.

Terminal

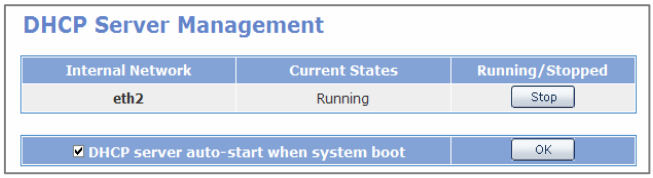
This defines the IP range of the standard data terminals (PCs, printers, etc) that are to use the DHCP scope of the Data Server.



Item	Description
IP Range	The IP range of the Data terminal(Maximum range: 120 pieces) When entering a IP, enter '192.168.0.60~60'.
Gateway	The gateway information entered at the CALL Server Item.
Netmask	The subnet mask information entered at the CALL Server tem.
MAC/Host-ID	The client authentication type - NONE: Executes the DHCP IP request without the authentication. - HOST: Click the **[List]** Button, and enter the HOST ID. - MAC: Click the **[List]** Button, and enter the MAC address.

Management

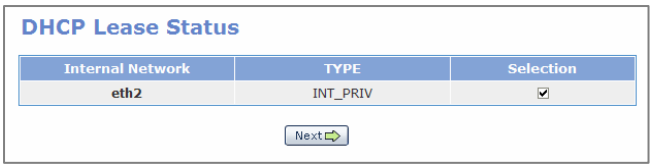
The DHCP Server can be started or stopped by selecting the **[DHCP Server]** → **[Management]** Menu. Check the 'Auto Start' Item, to automatically start DHCP when the system is rebooted.



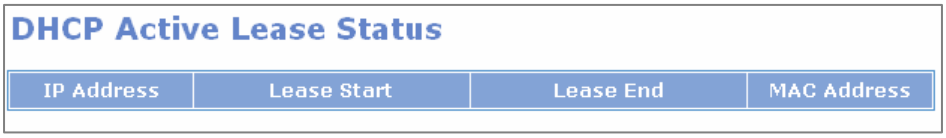
VoIP Status

The **[DHCP Server]** → **[VoIP Status]** Menu displays active information on the OfficeServ 7200 system. When the Call Server receives the IP allocations, the information is notified via the Module interface demon of the Data Server, and this information can be confirmed on the screen below:

Leases Status



On the **[DHCP Server]** → **[Leases Status]** Menu, the IP address lease information can be accessed. Select the desired Interface then click the [**Next**] button to see the lease information.

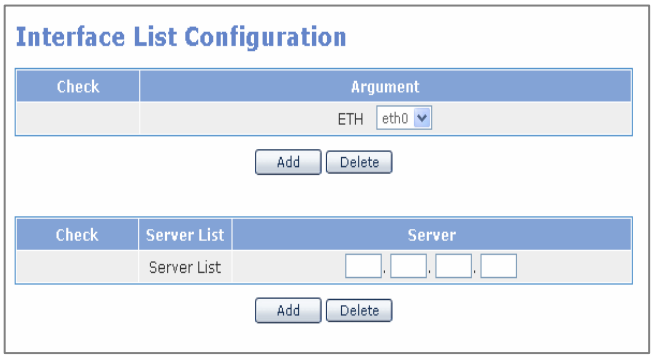


DHCP Relay Agent

This function is needed when one DHCP server is used on several subnets. This function enables the DHCP Client to receive the IP allocation when the DHCP Server and the DHCP Client are in mutually different networks.

Configuration

The DHCP Relay is configured by designating the interface to perform the relay and registering from the DHCP Server. Designate the Interface where the relay is performed among the activated interface list by using the **[Add]** button. For the designated interface, its list is made, the set interface can be deleted in the list by using the **[Delete]** button.
In the DHCP Server list enter the IP Address of the DHCP and click the **[Add]** button.. To delete a DHCP Server, check the box to the left of the IP Address, and then press the **[Delete]** button.



Management

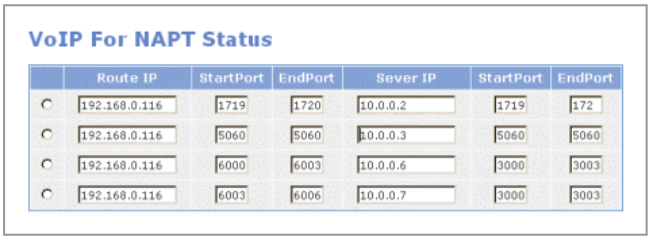
In this Menu the DHCP Relay is started and stopped.Click on the [**Run**] button to start the DHCP Relay and click on the [**Stop**] button to stop the DHCP Relay..

VoIP NAPT

On the **[VoIP NAPT]** Menu, the NAPT item for the VoIP communication is displayed.

Status

32 units of the internal and external ports per MGI card are connected by one to one mapping. Whenever the item of the DHCP Server is newly set, the program for connecting the Call Server and Feature Server sends/receives the new information to/from the Call Server. On this occasion, the NAPT item is automatically configured at the Data Server for the VoIP commuication of the H.323 phone. On the **[Status]** menu, the related information is displayed.



The MGI card set in the **[DHCP Server]** → **[Configuration]** menu and the VoIP NAPT for the Call Server and Feature Server are made. The screen above displays this information on the VoIP NAPT table.

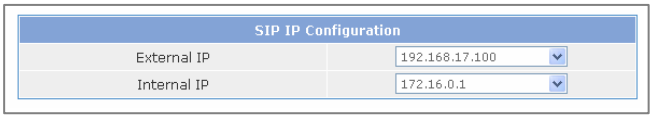
SIP ALG

Config

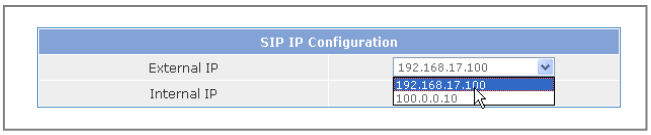
On the **[Config]** menu, the SIP environment can be set. Set the following item, and click the **[Save]** button.

SIP Configuration

The information on the firewall setup is displayed.

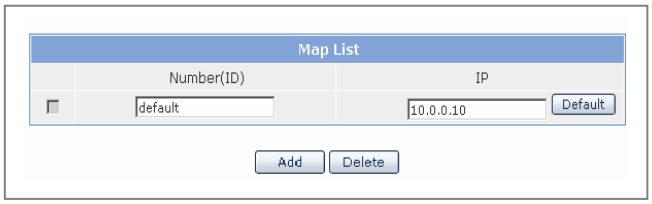


The External IP item and the Internal IP item are displayed on the list box so that the web manager can combine the usable information to select it.
If there are two external or internal networks or more, the network that is to be used in the list box can be selected.

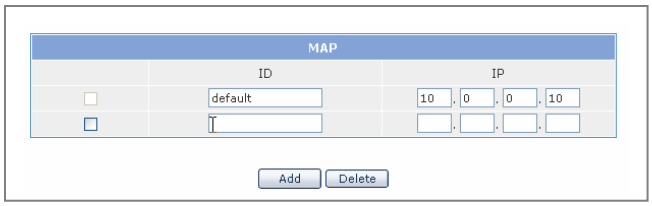


Map LIST

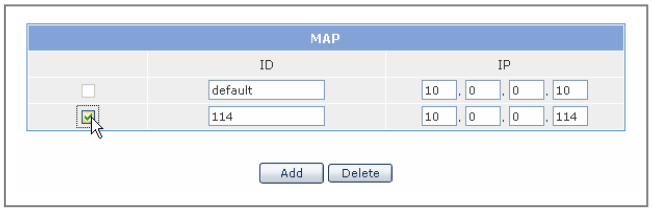
Enter the information on the SIP devices located inside the firewall.



When there is no information on the IP or the phone on the SIP message entered outside the firewall, the SIP message is converged to be sent into the IP terminal set in the ‘default’ item. Therefore, this item should be surely entered. The setup can be coventiently made when all traffic are considered as the calls of the digital phone by the Call Server. Therefore, on the ‘default’ item, in general enter the IP of the Call Server.

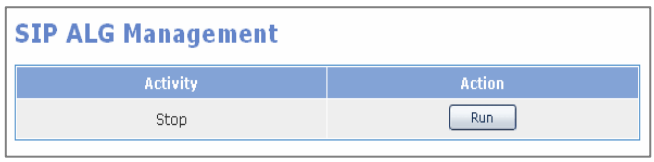


When adding the Map information, press the **[Add]** btton to add the entry window and insert the information.
When deleting the Map information, check the checkbox of the deleted information, and press the **[Delete]** button. All setups can be reflected on the system when the **[OK]** button on the lower side of the setup SIP configuration is pressed.



Management

The SIP ALG can be executed or its execution can stop by selecting the **[Management]** menu. The following figure shows that the activity is in the stop status and the SIP ALG stops in the present. On the contrary, when the Activity running and the SIP ALG is under execution, the stop that stops the SIP ALG is activated. Although the system is rebooted, the setup returns into the last set status.



The Management is classified into the Activity displaying the current status information and the Action displaying the execution commands.

Item	Description
Activity	The current SIP ALG status
Action	The commands that can be executed in the present status.

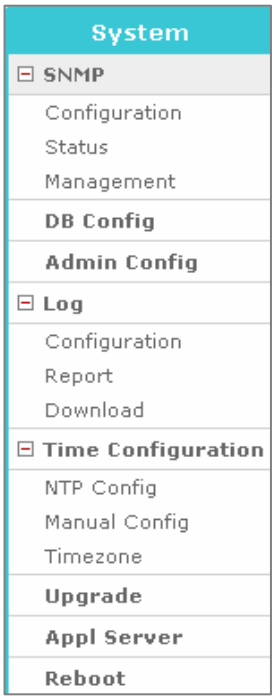
NOTE

SIP ALG(SIP aware ALG)

If the firewall based on NAT like the Data Server board of OfficeServ 720 protects the internal network, the system is safe against the external attack, but is limited in the service. For settling this trouble, SIP aware ALG(SIP ALG) enables the SIP devices inside the firewall to communicate with the external equipments.

System Menu

Select the **[System]** menu of the OfficeServ 7200 Data Server. The submenu is displayed on the left top of the screen as follows:



Menu	Submenu	Description
SNMP	Configuration	Displays the configuration items of SNMP.
	Status	Displays the SNMP configuration currently configured
	Management	Starts or Stops the SNMP service.
DB Config		Manage the DB currently set in the Data Server
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
Time Configuration	NTP Config	Registers a Time Server where the information on the date and the time is taken and synchronizes the time with the time Server by using the NTP.

(Continued)

Menu	Submenu	Description
Time Configuration	Manual Config	These settings set the date and the time of the system or synchronizes the time with the Call Server.
	Timezone	Selects the areas categorized by GMT and sets the local time.
Upgrade		Upgrades the Data Server with newest package version.
ApplServer		These settings control telnet, ftp, and ssh access to the Data Server
Reboot		Reboots the system.

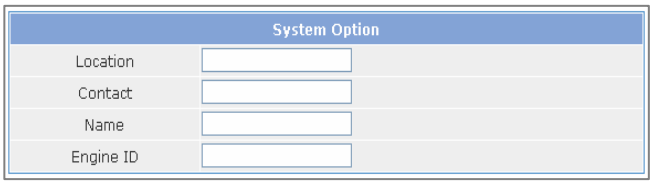
SNMP

Configuration

Set up the SNMP using 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

Sets the SNMP System Option.



Item	Description
Location	Sets up the information on System Location
Access	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

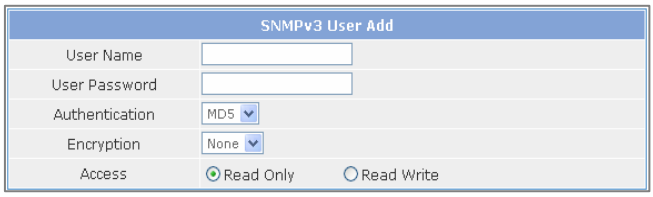
Community

Adds the new community used in the 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

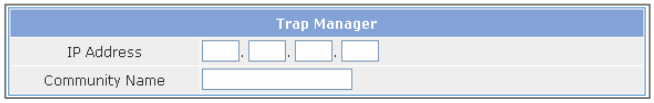
SNMPv3 Administrator Add allows adding a administrator to be used at SNMP v3.



Item	Description
User Name	Fill in new administrator's name to add.
User 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

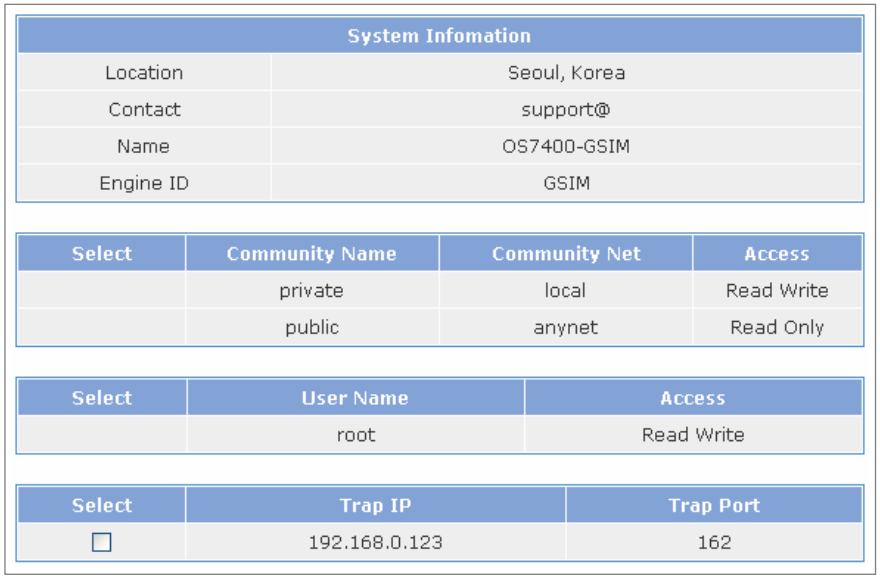
Sets the IP address that is to transmit the trap. Up to five ones can be designated.



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.



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

SNMP Config Information

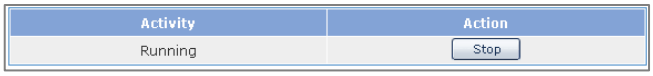
The administrator can retrieve the SNMP configuration.

Item	Description
System Information	Displays the information set up at System Options.
Select	Selects information to delete.
Community Name	Displays the community name.
Community Net	Displays the configured name of the Community Network.
Community Access	Displays the access authority of the configured community.
User Name	Displays the configured 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. By clicking the **[Run]** button, the SNMP service starts. If clicking the **[Stop]** button, the SNMP service stops.

SNMP Management

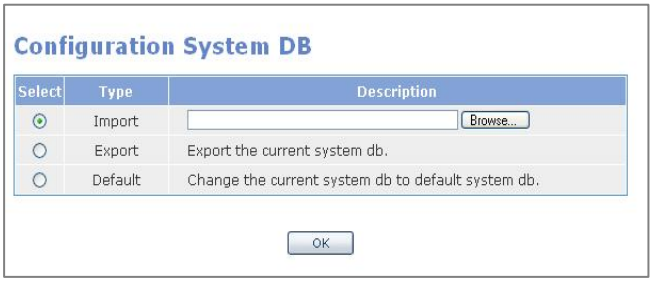


SNMP Management allows the administrator to start/stop the SNMP service.

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

DB Config

Manage the Data Server database using the **[System]** → **[DB Config]** menu. From this menu the DB can be Imported, Exported or Defaulted.



Item	Description
Import	Uploads a saved DB into the Data Server from a user's PC.
Export	Saves the current Data Server DB onto a user's PC.
Default	Changes the Data Server DB to factory defaults.

In order to change the DB by using the DB Import function the DB backup file should be saved on a PC. The DB Default function changes the Data Server DB to factory defaults. In order to access the web manager after a default use 10.0.0.1 via the LAN port of the internal network after restarting the system.

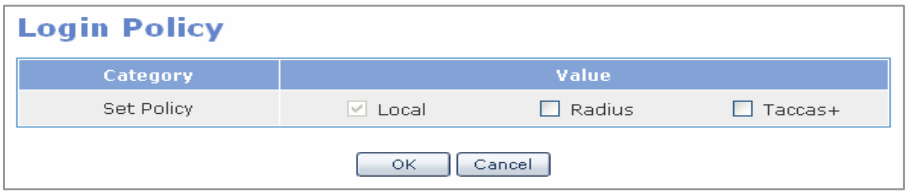
CAUTION

DB Change

When the DB is changed in the OfficeServ 7200 Data Server the system restarts.

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.

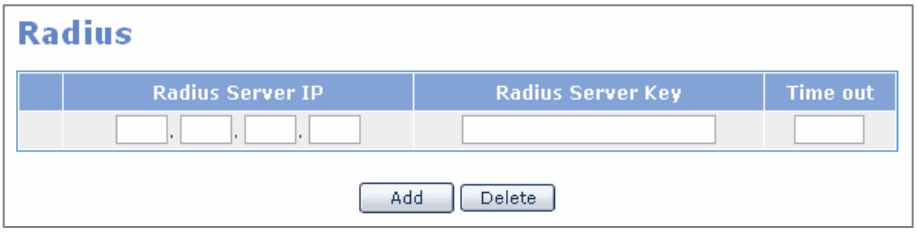


Local

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+

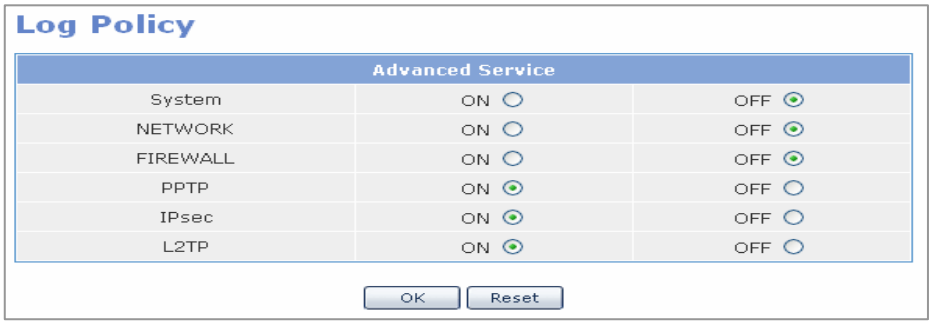
Enter the information on the Taccas+ authentication. Up to 5 lists can be entered or deleted. When deleting the list of all server IPs, the corresponding secret key values are also deleted.

Log

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

Configuration

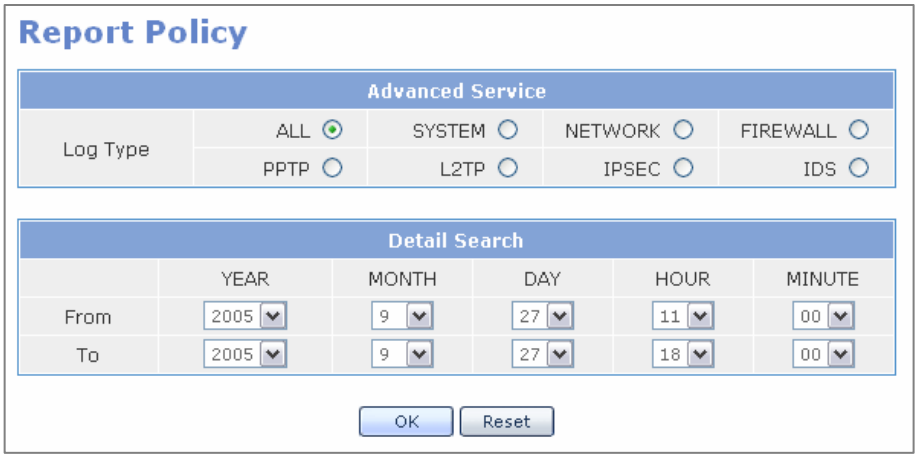
This page allows setting up the log to determine whether to add a log to the system.



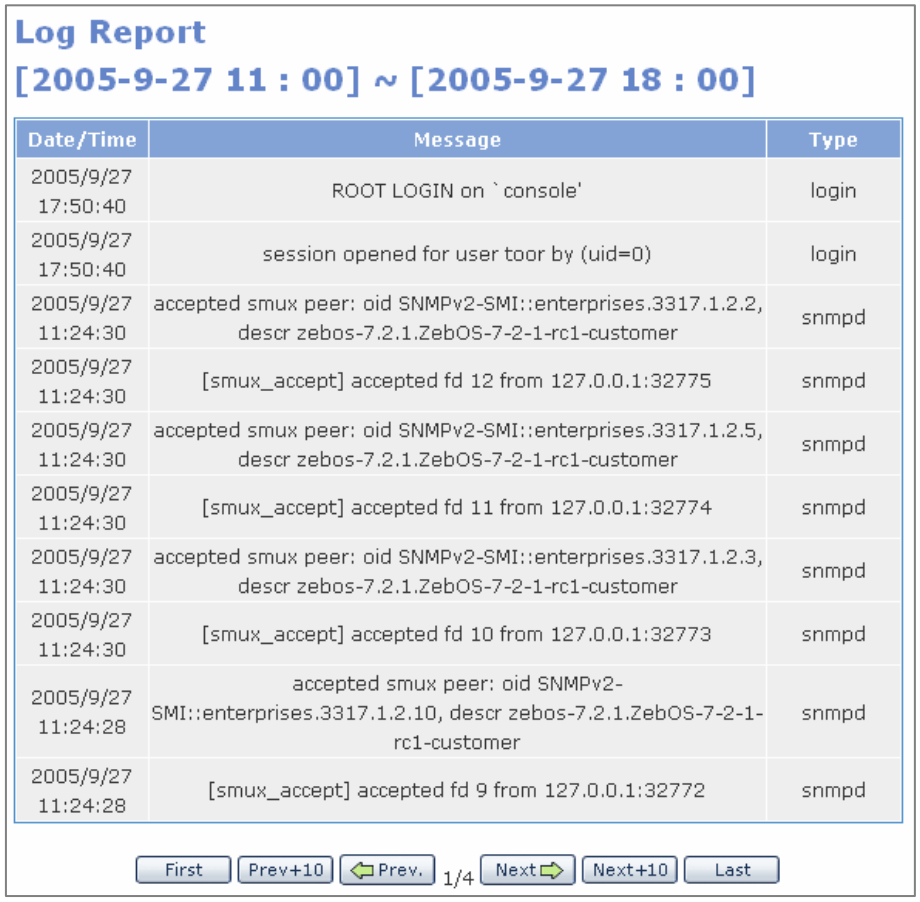
Select added logs from the logs for system log, network, firewall, VPN, and click the **[OK]** button to add logs to the system log. Click the **[Reset]** button to return to the previous status before applying the configuration.

Report

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

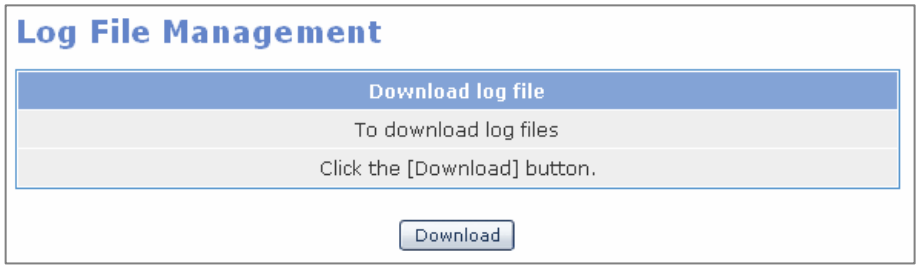


Set up the desired log type and time and click the **[OK]** button to verify the log. Click the **[Reset]** button to return to the previous status.



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.



Time Configuration

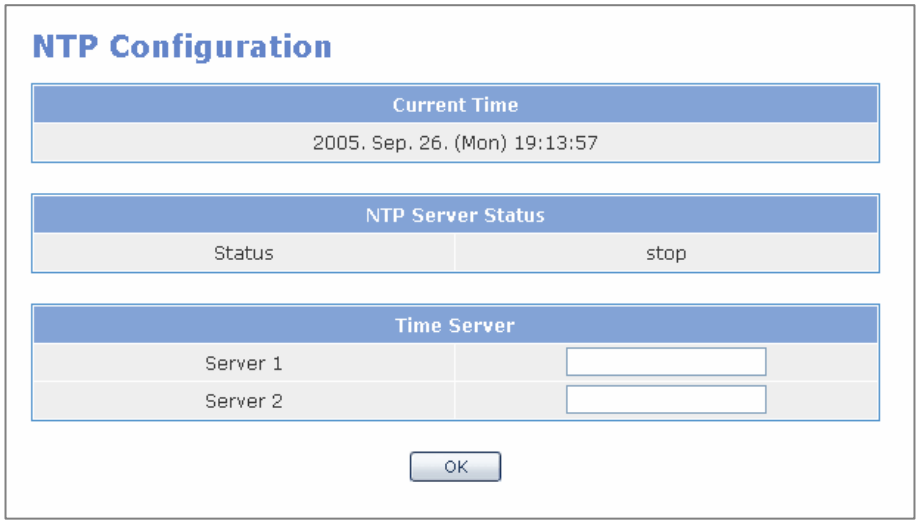
Synchronize the date and time of the system on the **[Time Configuration]** menu of the **[System]** through a network or manual configuration.

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.)

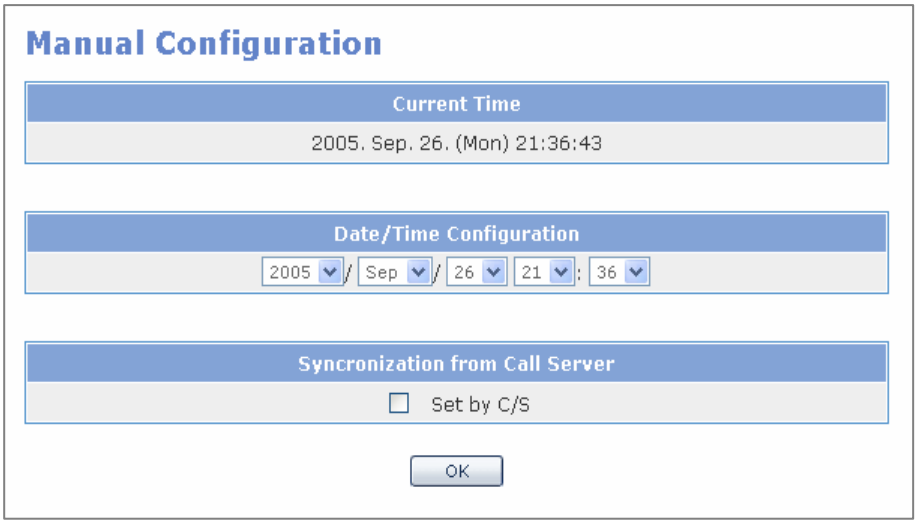
Click the **[OK]** button to start or restart NTP demon to register Time Server.



- 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.

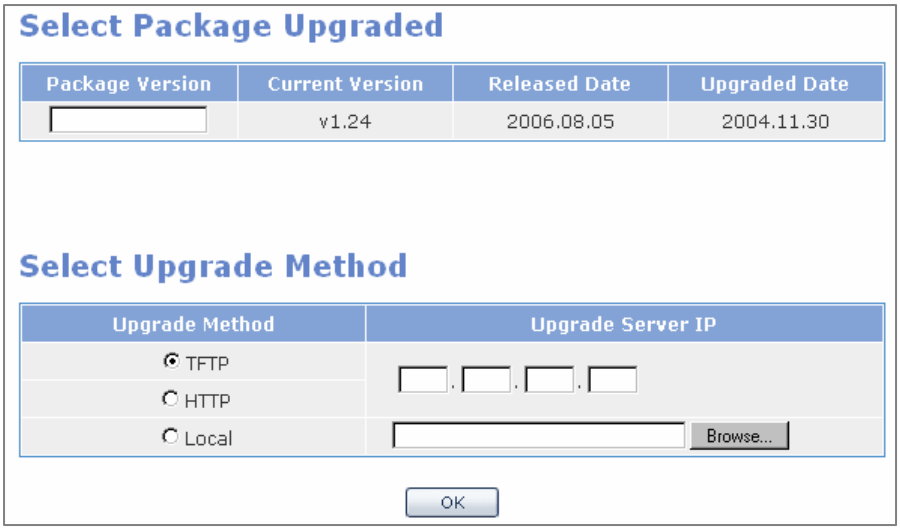
NOTE

Information on the System Time

The Data Server system has no internal Real-Time Clock(RTC). Therefore, the time information is not saved after the system restarts, but is internally saved by one hour unit. Therefore, when restarting the system, the time information previously set can be changed.(In case of the normal restarts, the setup is made on the basis of the time before the termination.)

Upgrade

Upgrade the Kernel and Ramdisk using the PC **[Upgrade]** menu.
The types of upgrade methods are 'TFTP Method', 'File Transmission Method through HTTP', and Local Method that uploads the upgrade from the administrator's PC.



When upgrading the Data Server package the version number should be entered into the the **[Package Version]** field (i.e v1.24).

For the TFTP and HTTP methods enter the address of the TFTP/HTTP server and then click the **[OK]** button. For the Local method the upgrade package file should exist on the administrator's PC. Click the **[OK]** button after selecting the file. In the TFTP/HTTP method the files of the upgrade version are searched automatically and downloaded, but for the Local method the entered version name and file name to upload should be identical. If the upgrade Package Version is 'v124', the file name is 'gData Server-pkg-v1.24.tgz'.

CAUTION

Deleting Temporary Internet Files

Be sure to delete temporary Internet files after upgrading the **DATA SERVER** package. Select the **[Internet Explorer]** → **[Tools]** → **[Internet Options]** menu, and click the **[Deleting Cookies]** and **[Deleting Files]** buttons on the **[Temporary Internet Files]**. If these files are not deleted the web screen may not be properly displayed..

Appl Server

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

Reboot

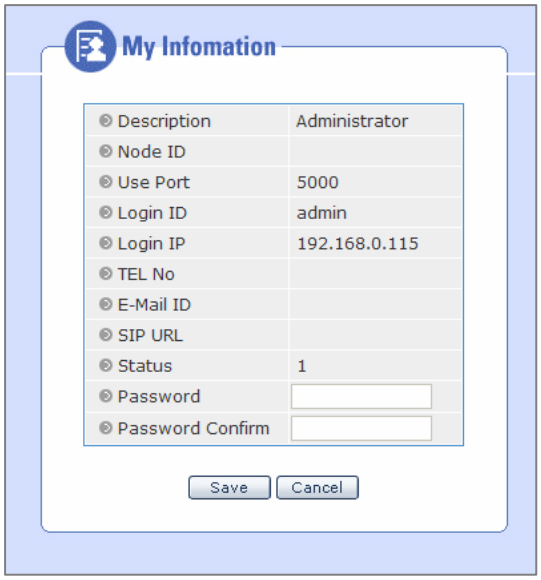
The administrator can reboot the system in the **[Reboot]** menu.

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.

My Info Menu

If you click the My Info on the right upper side of the Web, you can check your information can be confirmed.
If you enter the information into the Telephone number, E-mail address and Description entry window, clicking the **[Save]** button, the information is saved. Only one piece of information can be saved.
If you enter on the password entry window the password that is to be changed, clicking the **[Save]** button, the login password is changed. Although the system is rebooted, the setup status is recovered into the last setup one.



Item	Description
Description	Login user authority.
Node ID	Information on the node logged in
Use Port	Port information.
Login ID	Login user ID
TEL No	TEL No. of the login user
E-Mail ID	E-Mail ID of the login user
SIP URL	Displays the connection URL information of the SIP Server.
Status	-
Password	Enters the password to be changed.
Password Confirm	Confirms the password to be changed.

ANNEX A. VPN Setting for Windows XP/2000

If IPSec and PPTP should be set on the **[VPN]** menu of the OfficeServ 7200 Data Server, VPN client should be also set on the MS Windows. This section describes how to set VPN on the Windows XP. The Windows 2000 case is similar with the Windows XP case.

Under the following network environment, the setting procedures of IPSec and PPTP are as follows:

- External IP address of the OfficeServ: 211.217.127.40
- Internal IP address of the OfficeServ: 192.168.0.1
- Internal network IP address: 192.168.0.0
- Internal network Netmask: 255.255.255.0
- IP address of a Windows XP/2000-installed client PC: 211.217.127.73

IPSec Setting

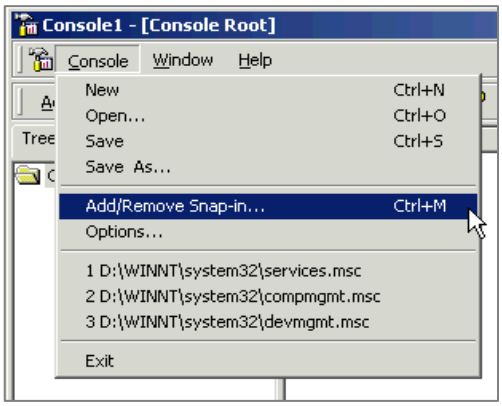
IPSec and various encryption/authentication algorithm can be used through the installation CD and Windows update in Windows XP/2000. Additionally, LAN to VPN client can be configured through the IPSec.

IPSec Setting in Windows XP/2000

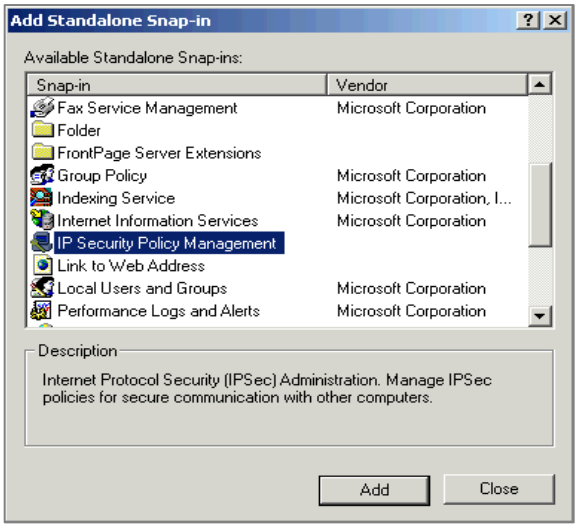
- Windows XP: Executes ‘IPSeccmd.exe’in the Support/Tools setup folder of the Windows XP installation CD.

- Windows 2000: Download and install ‘Windows 2000 Service pack 2’in the Windows update site. Or, execute ‘IPSecpol.exe’in the Support/Tools setup in the Windows 2000 installation CD.

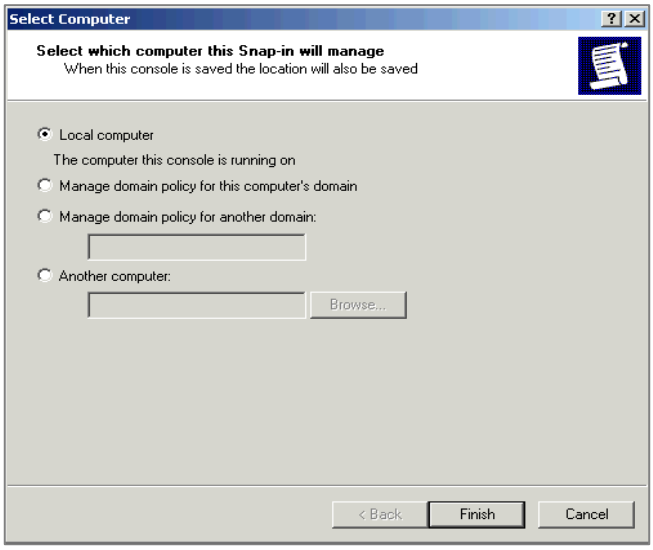
1. Select the **[Start]** → **[Run]** in the task bar and execute 'mmc' to display the window below: In the console window, select the **[File]** → **[Add/Remove Snap-in…]**.



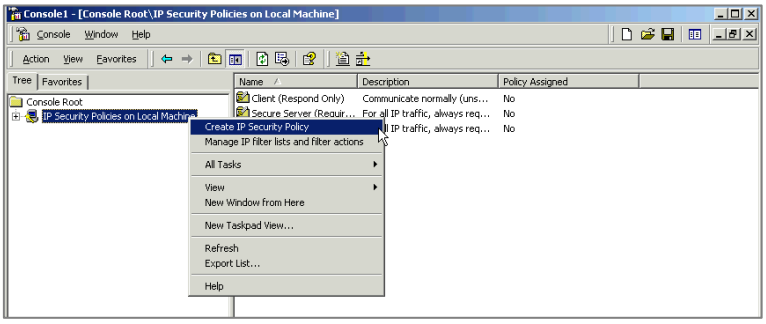
2. In the <Add/Remove Snap-in…>, click **[Add]** to display the following window: Select 'IP security policy management' in the Add/Remove Snap-in… menu and click **[Add]**.



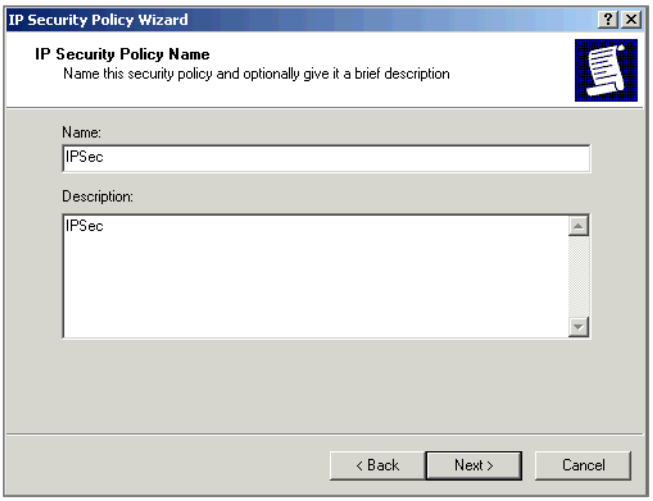
3. Select ‘Local computer(T)’in the window below and click **[Finish]**.



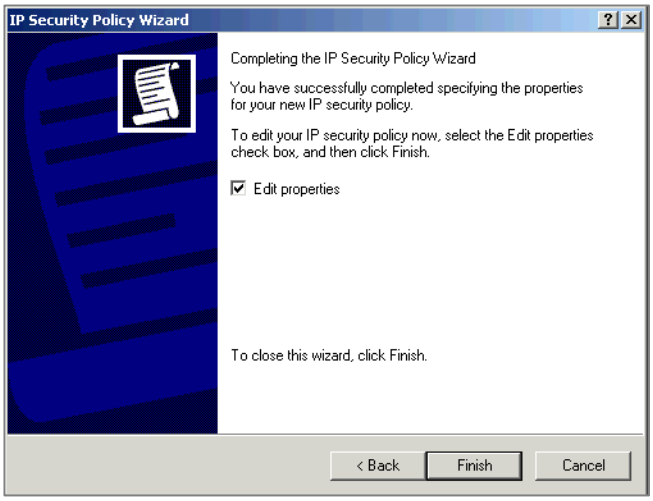
4. Move to the <Console> window. Then, ‘IP Security Policies on Local Machine’ of the ‘Console Root’ is created. Select the item and right click the **[Create IP Security Policy]** menu.



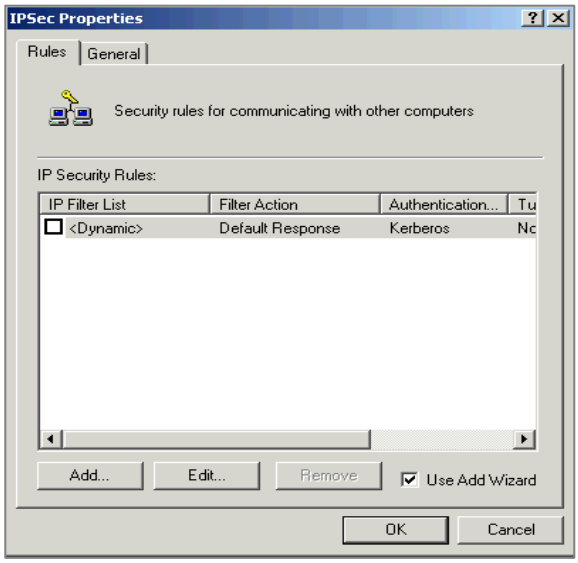
5. Click **[Next]** on the <IP Security Policy Wizard> window to display the window below: Enter the Name and Description and click **[Next]**.



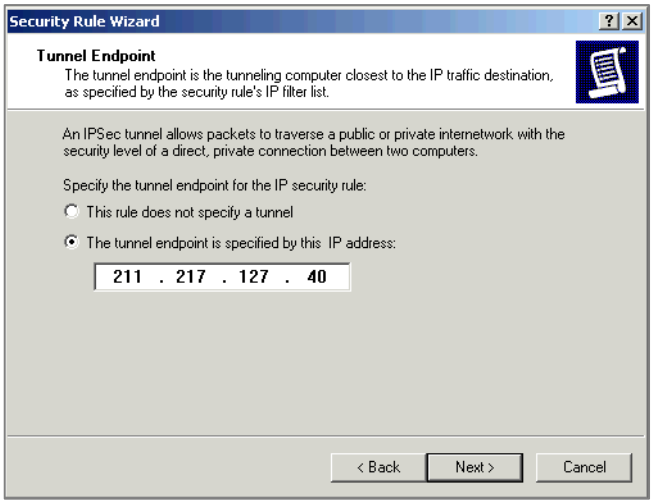
6. If 'Activate the default response rule(R)' is checked, release the check and click **[Add]** to display the window below: Check 'Edit Properties(P)' and click **[Finish]**.



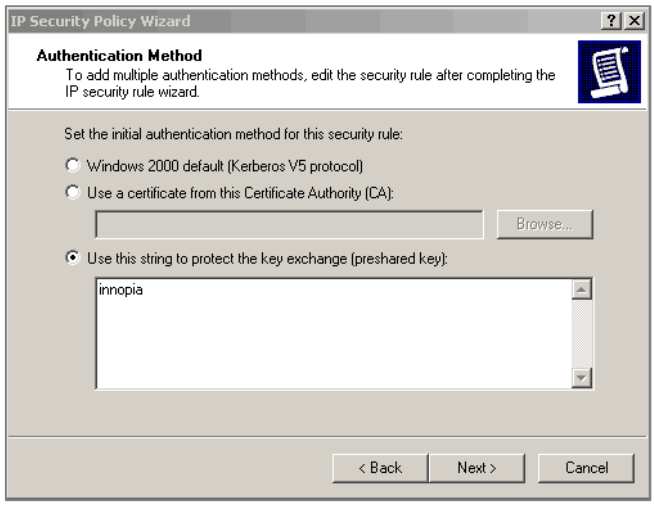
7. When the <XP_OPSec Registration Information> window is displayed, the created items are displayed. If the corresponding item is checked, release the check and click **[Add]**.



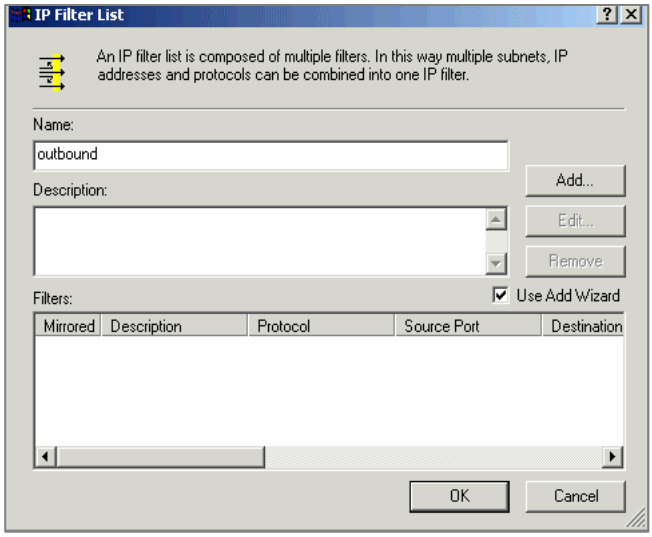
8. Click **[Add]** on the <Security Rule Wizard> window to display the window below: Select 'The funnel endpoint is specified by this IP address' and enter the fire wall external IP address(211.217.127.40). Click **[Next]**.



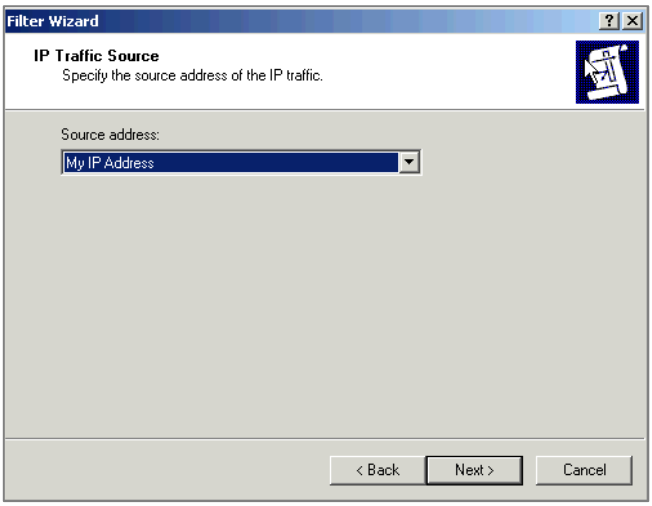
9. Select the Local Area Network(LAN) on the <Network Type> window and click **[Add]** to display the window below: Select 'Use this string to protect the key exchange **[preshared key]**' and enter the password registered with the firewall. Click **[Next]**.



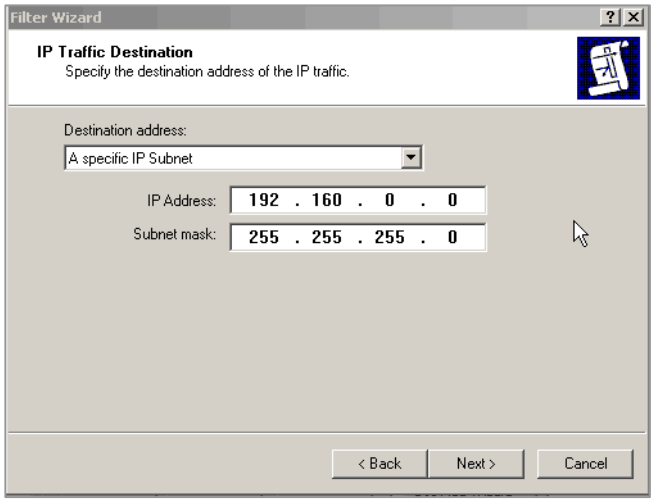
10. Click **[Add]** on the <Security Rule Wizard> window to display the window below: Enter 'outbound' in the Name field and click **[Add]**.



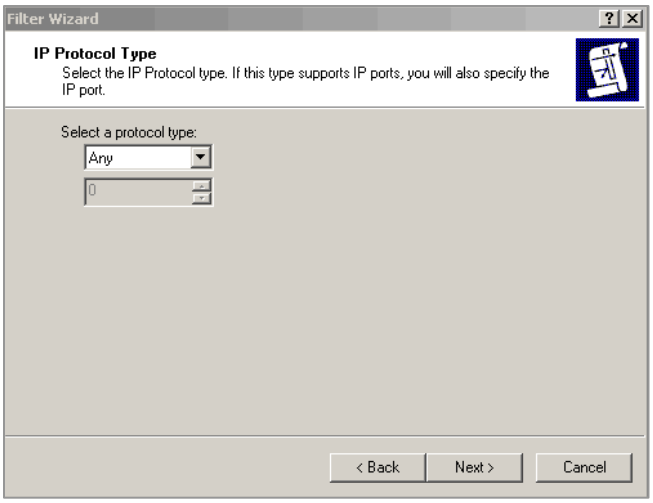
11. Click **[Add]** on the <IP Filer Wizard> window to display the window below: Select 'My IP address' in the Source address field and click **[Add]**.



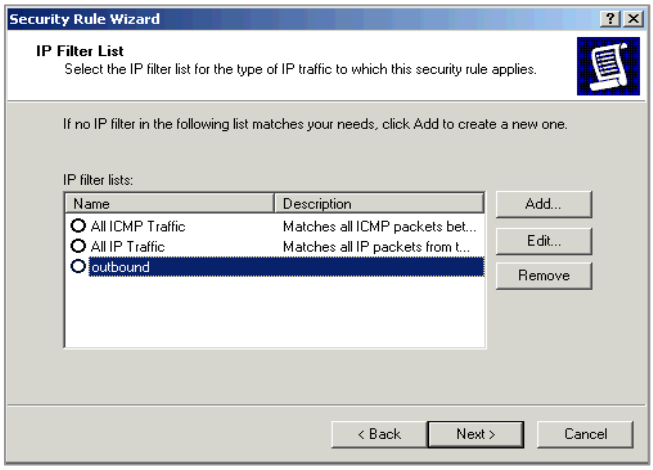
12. Select 'Specific IP Subnet' in the target address and enter the internal network address(192.168.0.0) and subnet mask(255.255.255.0).
Click **[Next]**.



13. Select ‘All’ from the protocol type selection and click **[Add]**.
Check ‘Edit Properties(P)’ on the <IP Filter Wizard> window and click **[Finish]**.

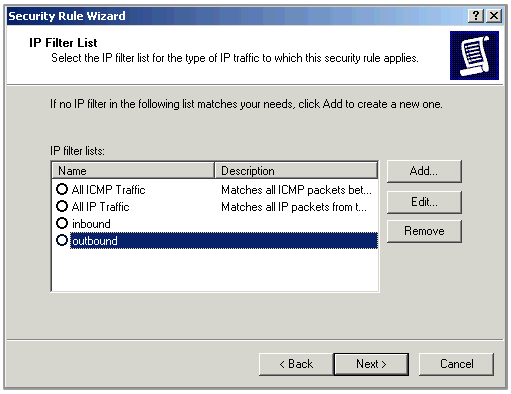


14. Click **[OK]**. Then, the outbound item is created. Click **[Add]** to create the inbound item.

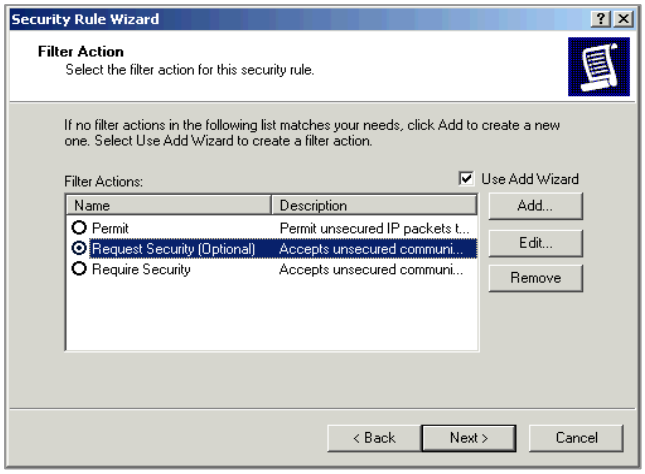


15. Enter the ‘inbound’ in the Name field and click **[Add]** like step **10**.
The above steps **11** through **13** also apply to this procedure.

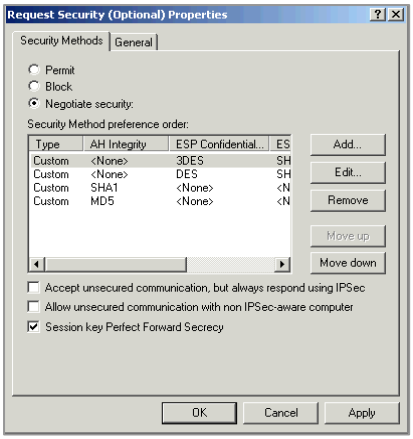
16. Click **[Add]** to display the window below: Then, select the 'outbound' item and click **[Next]**.



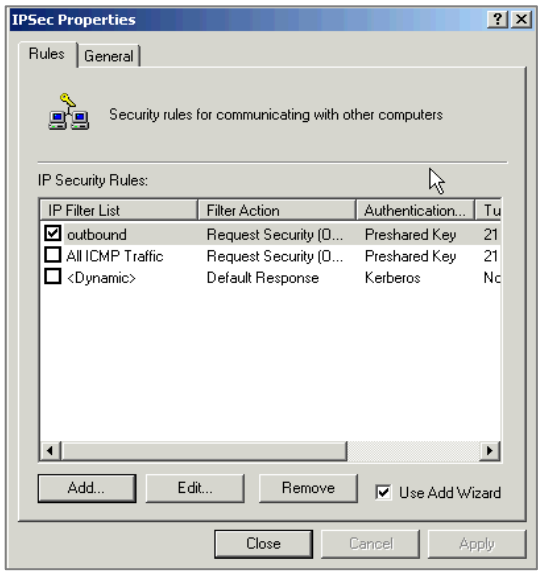
17. Select the 'Request Security **[Optional]**' item and click **[Edit]**.



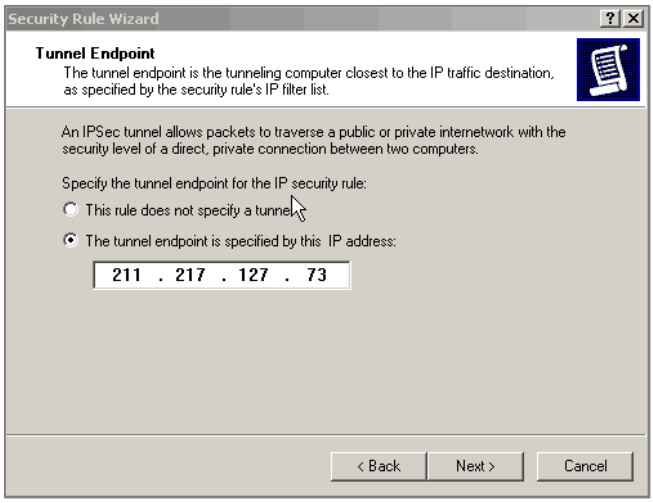
18. Select 'Negotiate security' and select 'AH Integrity(None), ESP Confidential(3DES), ESP Integrity(MD5)' in the Security Method preference order. Click **[Move up]** to move to the first row of the corresponding item. Check 'Session key Perfect Forward Secrecy(PFS)' and click **[OK]**.



19. Check 'Edit Properties' and click **[Finish]** to display the window creating the outbound item. Click **[Add]** to create the inbound item.



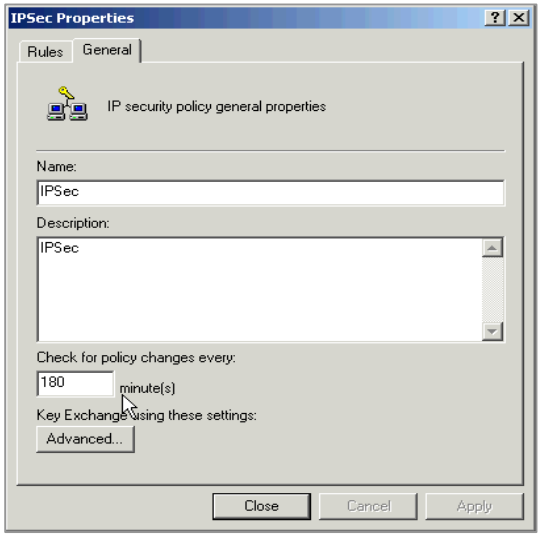
20. Click **[Next]** on the <Security Rule Wizard> window to display the window below: Check 'The tunnel endpoint is specified by this IP address' and enter the IP address of a client PC. Click **[Next]**.



21. Select Local Area Network(LAN) on the <Network type> window and click **[Next]**. Select 'Use this string to protect the key exchange **[preshared key]**' and enter the password registered with the firewall. Click **[Next]**.(Refer to step **9.**)

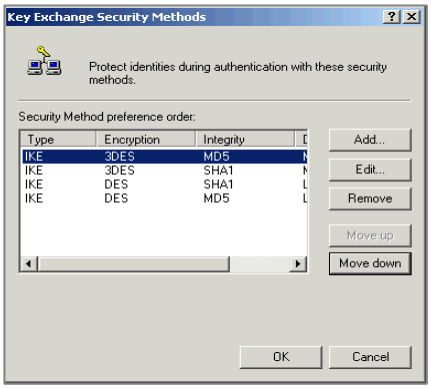
22. Select the 'inbound' item in the step **16** window and click **[Next]**. Follow the step **17** and **18**.

23. Check 'Edit Properties' and click **[Finish]** to display the window below: Select the **[General]** tab and click **[Advanced]**.

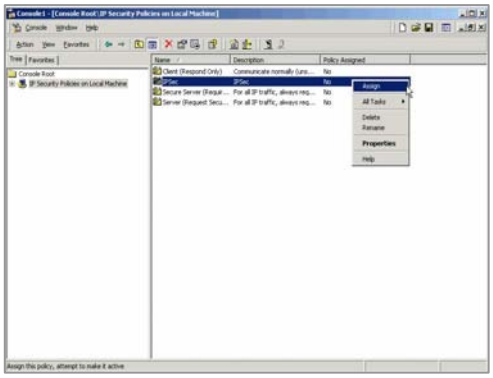


24. Check 'Master key Perfect Forward Secrecy(PFS)' and click **[Methods…]** in the window below:

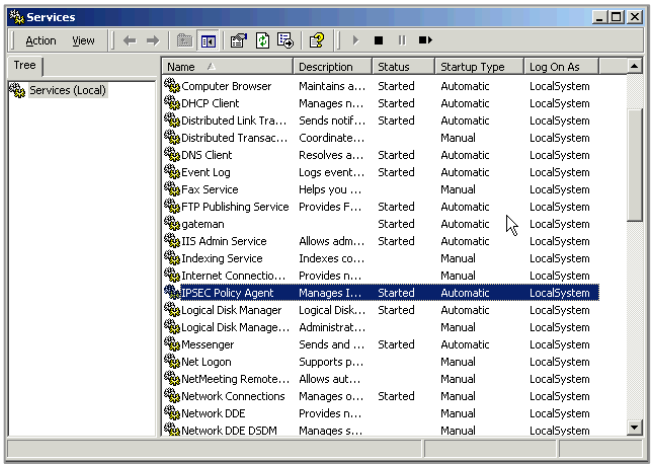
25. Select ‘Encryption(3DES), Integrity(MD5), Diffie-Hellman(Med)’ in the window below and click **[Move up]** to move the first row of the corresponding item. Click **[OK]**.



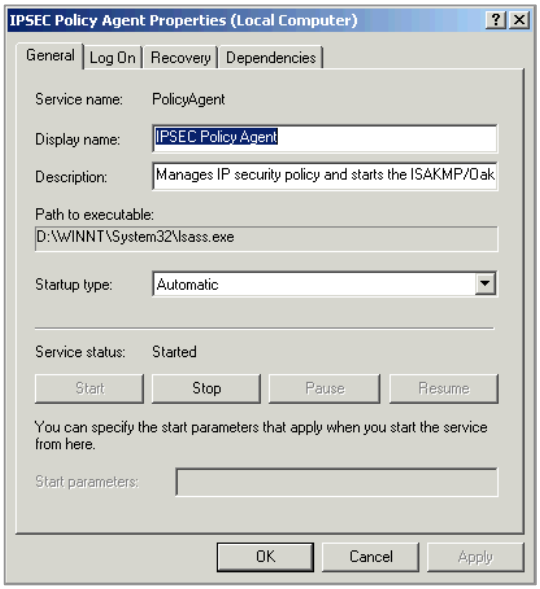
26. Select IP Security Policies on Local Machine’ on the <Console> window. Select the item newly created on the right corner of the window and right-click the **[Assign]** menu. Then, policy assignment is changed into ‘Yes’.



27. Select **[Start] → [Program] → [Administrative Tools] → [Services]** in the Window task bar and double click the ‘IPSec Services’ item.



28. Click **[Stop]** and click **[Start]** to restart the service in the window below:



29. Verify the connection status of the firewall internal IP address through the ping command at a command prompt. If responses like the window below are displayed, the IP address is properly connected.

```
C:\>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Negotiating IP Security.
Reply from 192.168.0.1: bytes=32 time=5 ms TTL=255
Reply from 192.168.0.1: bytes=32 time=6 ms TTL=255
Reply from 192.168.0.1: bytes=32 time=4 ms TTL=255

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 3, Lost = 1 <25% loss>.
Approximate round trip times in milli-seconds:
    Minimum = 4 ms, Maximum = 6 ms, Average = 5 ms
```

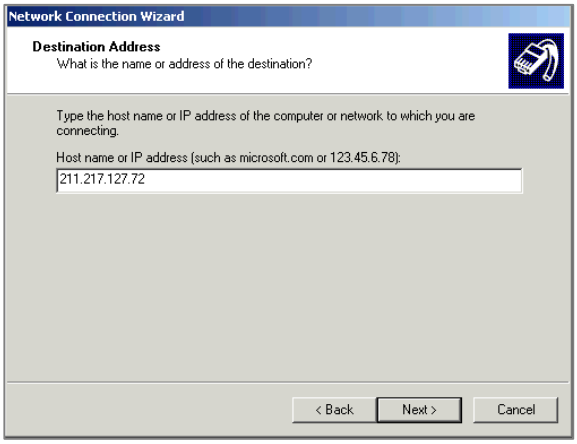
PPTP Setting

Users are allowed to configure VPN with PPTP by using the installation CD and through Windows update in Windows XP/2000.

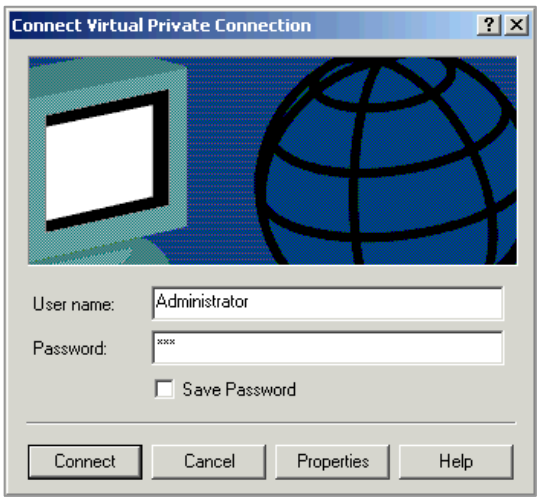
> CAUTION
>
> **PPTP Setting in Windows XP/2000**
>
> In Windows XP/2000, This item enables to use DHCP client. If VPN PPTP client is connected while the DHCP client is operating, errors will be found. To prevent this problem, close the DHCP client operation on the **[Start]** → **[Program]** → **[Administrative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

1. Double click the **[My Network Environment]** icon and select the **[Property]** item from the Windows desktop. Double **click [Create New Connection]** on the upper right corner of the screen to display the window below: Click **[Next]**.

2. Select ‘Connect to the network at my workplace’ and click **[Next]** button to select ‘Virtual Private Connection’. Click **[Next]** to display the window below: Enter the Host name or IP address and click **[Next]**. Enter the firewall external IP address and click **[Finish]** button.



3. Select **[Start]** → **[Set]** → **[Network Connections]** in the Windows task bar and select the host name entered in the window above to display the login window below: Enter the User name and Password to check if the VPN in a client is properly connected. Or, use the ping command like the **step 29** of 'IPSec Setting' to check the connection status.



After checking the VPN connection status, check if the shared directory of the internal computer connected to VPN can be accessed.

ABBREVIATION

A

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

B

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

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

M

MAC	Media Access Control

R

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