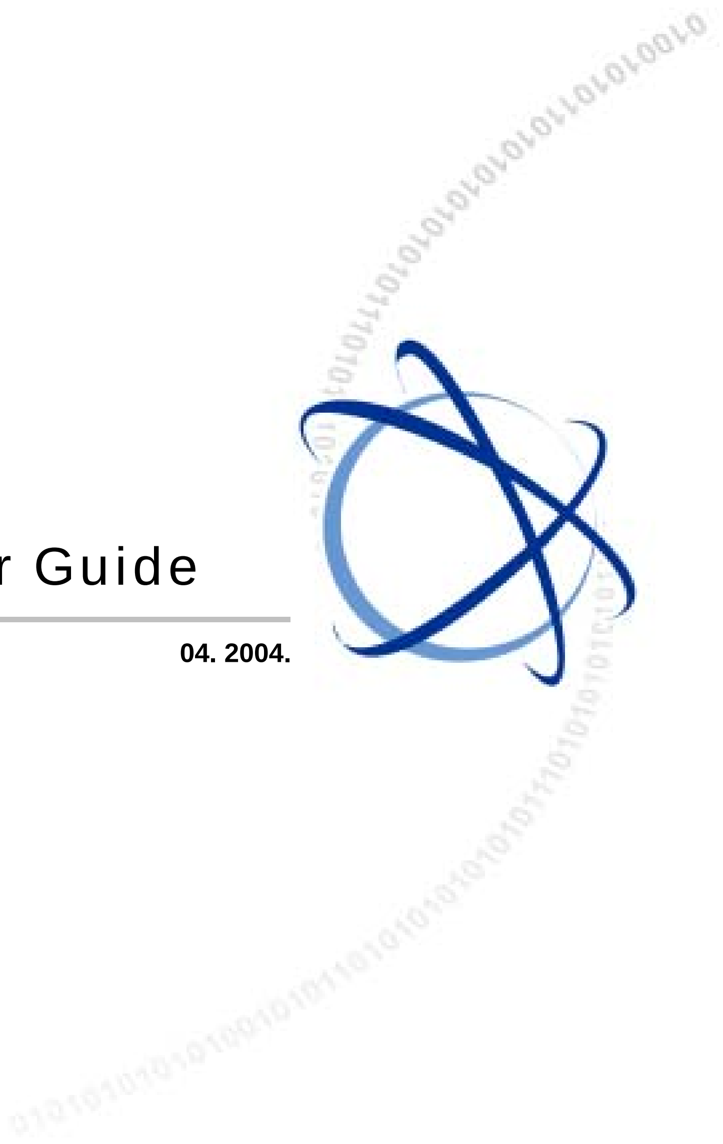
Ed.



OfficeServ 7200

Data Server User Guide

04. 2004.

SAMSUNG
ELECTRONICS

COPYRIGHT

TRADEMARKS

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

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

For further information on the updated manual or have a question the content of manual, contact **Document Center** at the address below.

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

e-mail : manual@samsung.com

http://www.samsungdocs.com

INTRODUCTION

Purpose

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

Document Content and Organization

This document contains 3 chapters and 2 annexes, which are summarized as follows:

Chapter 1. OfficeServ 7200 Data Server Overview

This chapter briefly introduces the OfficeServ 7200 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.

Annex A. VPN Setting in Windows XP/2000

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

Annex B. ABBREVIATION

Acronyms frequently used in this document are described.

Conventions

The following special paragraphs are used in this document to point out information that must be read. This information may be set-off from the surrounding text, but is always preceded by a bold title in capital letters.

⚠ WARNING	**WARNING** Provides information or instructions that the reader should follow in order to avoid personal injury or fatality.

⚠ CAUTION	**CAUTION** Provides information or instructions that the reader should follow in order to avoid a service failure or damage to the system.

☑ CHECK	**CHECKPOINT** Provides the operator with checkpoints for stable system operation.

✎ NOTE	**NOTE** Indicates additional information as a reference.

Console Window Output

- The lined box with '`Courier New`' font will be used to distinguish between the main content and console output window text.
- Shaded font(`Courier New`) will indicate the value entered by the operator on the console window.

References

OfficeServ 7200 General Description Guide

The OfficeServ 7200 General Description Guide introduces the OfficeServ 7200 and provides system information including the hardware configuration, specification, and function.

OfficeServ 7200 Installation Guide

The OfficeServ 7200 Installation Guide describes the condition required for installation, the procedure of installation, and procedures on inspecting and starting the system.

OfficeServ 7200 Service Manual

The OfficeServ 7200 Service Manual provides an overview of the system and describes the specification, configurations and characteristics of each H/W circuit, troubleshooting for error that may occur during operation, and the programming procedure for maintenance.

OfficeServ 7200 Feature Server User Guide

The OfficeServ 7200 Feature Server User Guide introduces the Feature Server, an application software of OfficeServ 7200, and describes the procedures for installing and using the Feature Server.

Revision History

Edition No.	Date of Issue	Remarks
00	04. 2004.	First draft

This page is intentionally left blank.

SAFETY CONCERNS

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

Symbols

⚠ **Caution**

Indication of a general caution

🚫 **Restriction**

Indication for prohibiting an action for a product

❗ **Instruction**

Indication for commanding a specifically required action

⚠ WARNING

⚠ **Security Warning**

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

Setting 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 Setting in Windows XP/2000

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

Caution Against Changing Network Interfaces

If a network interface(e.g. IP, gateway, and subnet mask) is changed during router operation, all the IP sessions that are being used in the router are disconnected for a while.

Private Key

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

Delete Temporary Internet Files

Delete Temporary Internet Files after upgrading Data Server package. After selecting the [Internet Explorer] → [Tools] → [Internet Options] menu, click the [Delete Cookies] and the [Delete Files] button in the [Temporary Internet files].
When Temporary Internet Files are not deleted, Data Server Web Management is not showed properly.

TABLE OF CONTENTS

This page is intentionally left blank.

CHAPTER 1. OfficeServ 7200 Data Server Overview

This chapter provides an overview of OfficeServ 7200 system and OfficeServ 7200 Data Server.

OfficeServ 7200 Introduction

As an ideal phone system for small offices using less than 50 subscriber lines, OfficeServ 7200 supports not only voice calls but data transfer over a data network. Users on various platforms, such as a digital phone, IP phone, mobile phone, PC, and server, can conveniently use various telephony features and applications.

The OfficeServ 7200 is configured with a cabinet mounted on a 19-inch rack, internal station, wireless LAN device, and application software.
Having a conventional server on a Linux platform outside of the cabinet, the OfficeServ 7200 provides the following application software:

- OfficeServ 7200 Feature Server(UMS, Mail Server, SIP Server)
- OfficeServ Admin(OfficeServ Operator, CTI)
- OfficeServ Solution(System Manager, Web Management, PCMMC, OfficeServ EasySet)

The OfficeServ 7200 provides network functions such as a switch, router, and network security over the data server, which operates by inter-working with a call server or feature server. This document describes OfficeServ 7200 Data Server.

NOTE

OfficeServ 7200 Configuration

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

Introduction to the OfficeServ 7200 Data Server

The OfficeServ 7200 system operates by inter-working with OfficeServ 7200 Call Server or Feature Server. The OfficeServ 7200 provides the functions below on the IP-based data server:

Switch

- Functions as Dummy L2 Switch.
- Performs a managed switch by using an access interface for LAN.
- Functions as a switch when a board is mounted by being connected with the WIM board(Basic Unit Slot 2).
- Functions as a learning bridge by spanning tree algorithm.
- Functions as Layer 2 Frame Priority by 802.1p.
- Controls 802.3x Layer 2 flow.
- Functions as Virtual LAN(VLAN), which is configured with a port, MAC address, and 802.1 Q tag.
- Supports IP multicasting relay(IGMP snooping).

Router

- Manages paths and performs queuing for data packets on both external WAN and internal LAN.
- Performs static or dynamic routing.
- Supports RIPv1, RIPv2, OSPFv2 routing protocol.
- Performs inter-VLAN routing.
- 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 the IGMPv1 or IGMPv2 protocol.
- Performs functions by using an access interface for WAN.
- Functions as an interface for ports in the WIM board.
  - 2 WAN Ethernet port: One of the ports is used for backup(10 Mbps).

  - 1 LAN Ethernet port: Enables a connection with a switch that configures LAN.
  - 1 Serial WAN port: Enables dedicated data line service by being connected with DSU or CSU, which is a data line device.
  - 1 DMZ Ethernet port: Enables DMZ configuration.

- LAN interface(LIM) support
  - The LAN interface exists in the LIM board and enables 16-port layer 2 switch.
  - The LAN interface is connected with the WIM board through the uplink port while operating by the managed switch.
- DMZ interface support
  - To protect an internal network from external hazards, the DMZ is a separate LAN port for configuring the device, which requires a free access from outside such as a mail server and web server, while separating the device from internal devices(one Ethernet port used).

Data Network Security

- Outbound and Inbound NAT/PT
  - 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)
  - Functions as a VPN gateway based on PPTP and IPSEC.
  - 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 WIM 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.

QoS

- Processes priority for layer 2 frames based on the 802.1p standard(Switch function)
- Processes priority queuing for layer 3 packets and for selected IPs
- Processes priority queuing for layer 4 packets and for RTP packets(UDP/TCP port)

Management

- 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
- Program upgrade
  - Upgrades program through TFTP
  - Upgrades program through HTTP

CHAPTER 2. OfficeServ 7200 Data Server Installation

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

Installation Procedure

Since a software package is included in the OfficeServ 7200 Data Server, additional installation of software is not required. The software package is composed of items described below:

Package	File	Description
Bootrom Package	bootldr.img-vx.xx bootldr.img-vx.xx.sum	Boot ROM program
Main Package	ds-pkg-vx.xx.tar.gz	Upgrade package for HTTP on the WEB Management
	app.img-vx.xx app.img-vx.xx.sum	'app' partition upgrade package for TFTP
	config.img-vx.xx config.img-vx.xx.sum	'config' partition upgrade package for TFTP
	kernel.img-vx.xx kernel.img-vx.xx.sum	'kernel' partition upgrade package for TFTP
	log.img-vx.xx log.img-vx.xx.sum	'log' partition upgrade package for TFTP
	ramdisk.img-vx.xx ramdisk.img-vx.xx.sum	'ramdisk' partition upgrade package for TFTP
	flash1.img-vx.xx flash1.img-vx.xx.sum	The first flash fusing file
	flash2.img-vx.xx flash2.img-vx.xx.sum	The second flash fusing file

NOTE

Software Package Configuration

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

Setup the environment as follows to access the Data Server.

1. Mount the WIM board on slot 1 and the LIM board on slot 2.
   - In order to connect the WIM board to the LIM board through the back panel, after checking the shunt pin of JP1, 2, 3, 4, then mount the WIM board to the back panel direction . In this case, connecting the UTP-cable to the LAN port will deactivate the port.
   - If the shunt pin of JP1, 2, 3, 4 is directed to the front of the WIM board, connect the LAN port of the WIM board to a port of the LIM board through a LAN cable.

2. Connect a PC to a port of the LIM board.

3. Execute the Internet Explorer from the PC and connect to the IP(10.0.0.1) of LAN. Then, the initial IP of the LAN of the WIM board is set to '10.0.0.1' and the Data Server function is set.

NOTE

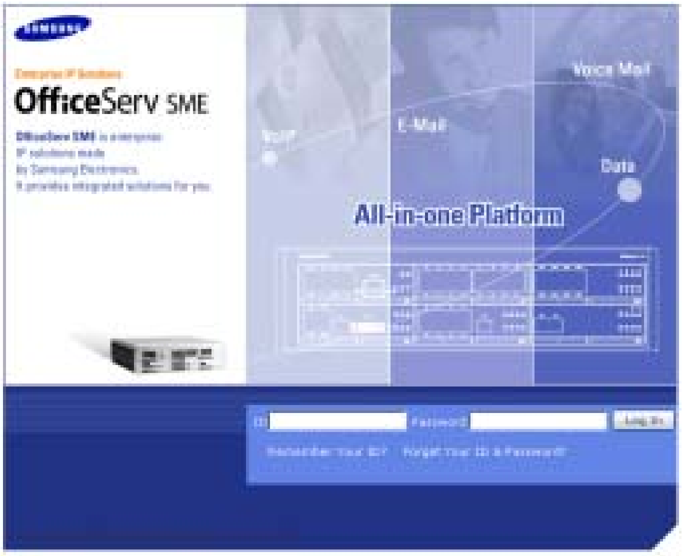
Use Internet Explorer 6.0 or higher

The version of the Internet Explorer should be 6.0 or higher to use the OfficeServ 7200 Data Server.

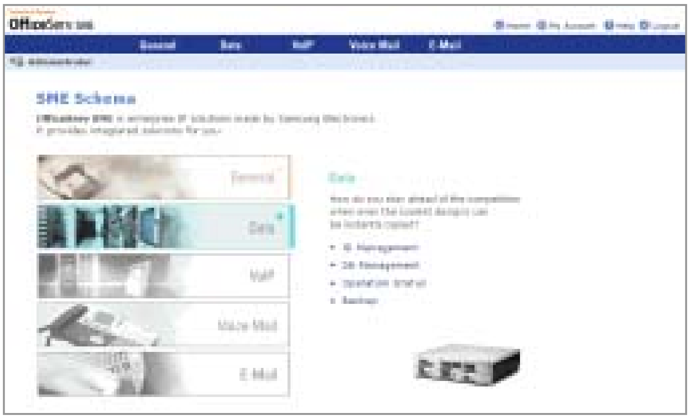
Usage Guide

The procedure for starting up the OfficeServ 7200 Data Server is as follows:

1. Start the 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:



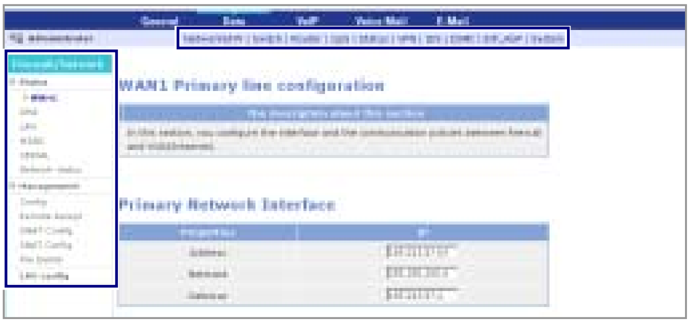
Click the [Logout] button on the upper section of the window to close the connection to the Data Server.

NOTE

OfficeServ 7200 Feature Server

The VoIP, Voice Mail, and E-Mail menus are related to the OfficeServ 7200 Feature Server. Refer to the ‘OfficeServ 7200 Feature Server User Guide’ for details on the menus.

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

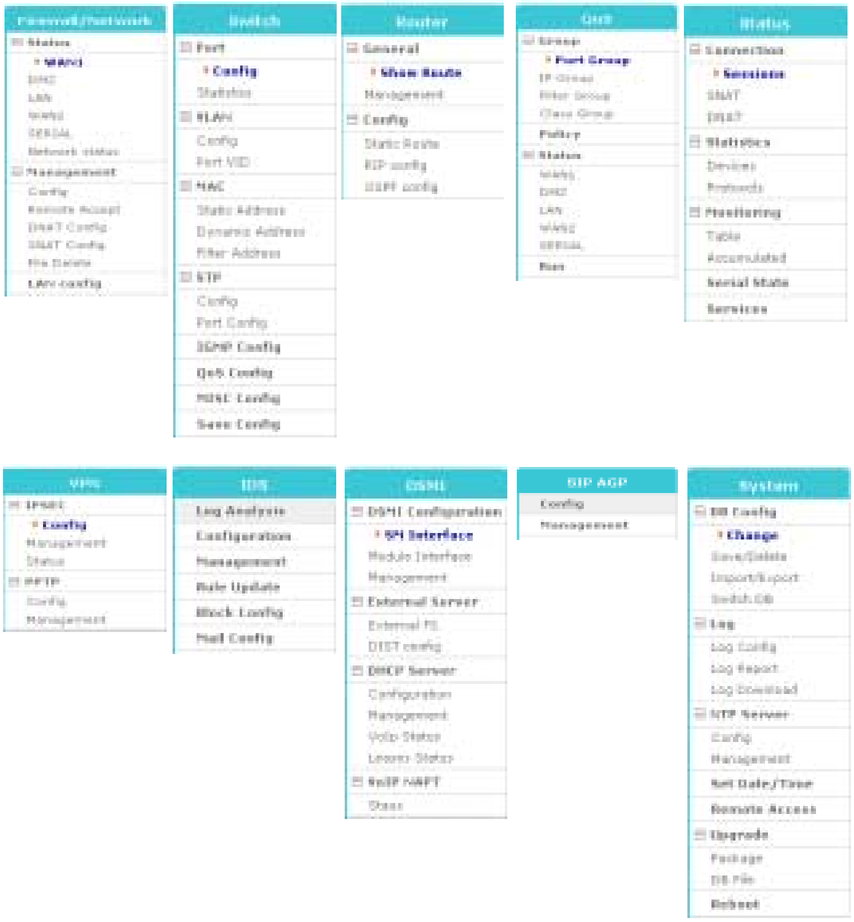


When a Data Server menu is selected, the submenus of the Data Server menu appear on the left section of the window. Descriptions on each submenu are provided in ‘Chapter 3. Using OfficeServ 7200 Data Server’.

CHAPTER 3. Using the OfficeServ 7200 Data Server

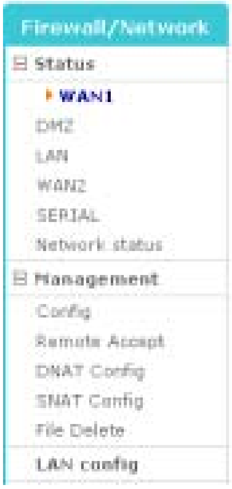
This chapter describes how to use the menus of the OfficeServ 7200 Data Server.

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



Firewall/Network Menus

Select [Network & FW] to display the submenus of Firewall/Network on the upper left section of the window.



Menu	Submenu	Description
Status	WAN1	Displays status of WAN1, an external port.
	DMZ	Displays status of DMZ, an internal port.
	LAN	Displays status of LAN, an internal port.
	WAN2	Displays status of WAN2, an external port.
	SERIAL	Displays status of SERIAL, an external port.
	Network status	Displays a summary of statuses of all ports.
Management	Config	Sets firewall and network.
	Remote Accept	Allows access to firewall.
	DNAT Config	Sets Destination NAT for incoming packets.
	SNAT Config	Sets Source NAT for outgoing packets.
	File Delete	Deletes setup file.
LAN config	-	Sets the transfer rate and transmission system of Ethernet port.

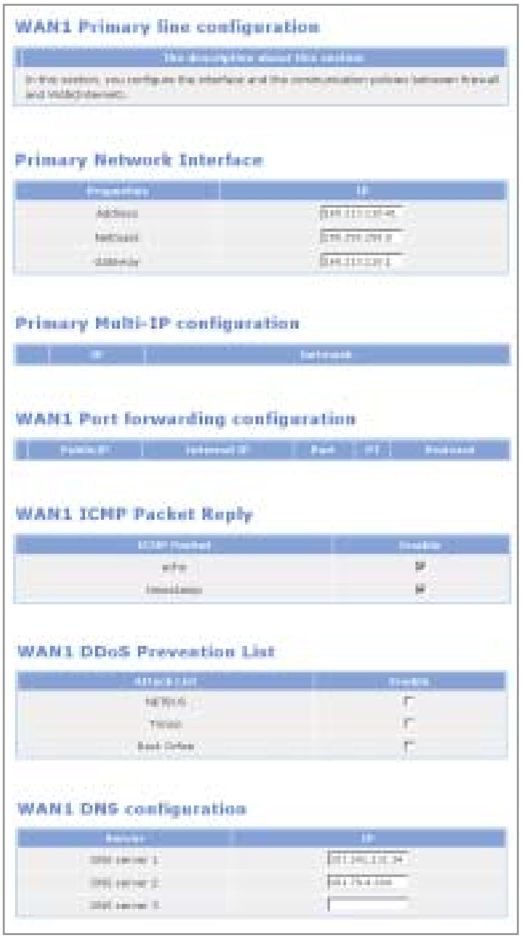
Status

The [Status] menu displays the setting of the WAN1, DMZ, LAN, WAN2, or SERIAL.

> NOTE
>
> **Port Setup Procedure**
>
> The WAN1, LAN, DMZ, WAN2, and SERIAL ports are set at the [Network & FW] → [Management] → [Config] menu. Refer to the description on the menu for the setup procedures.

WAN1

The [Status] → [WAN1] menu shows the setting of WAN1, which is an external port using a public IP.



WAN1 Primary line configuration

The description about this section
In this section, you configure the interface and the communication policies between firewall and WAN(Internet).

Primary Network Interface

Properties	IP
Address	[illegible]
NetMask	[illegible]
Gateway	[illegible]

Primary Multi-IP configuration

	IP	Netmask

WAN1 Port forwarding configuration

	Public IP	Internal IP	Port	PT	Protocol

WAN1 ICMP Packet Reply

ICMP Packet	Enable
echo	☑
timestamp	☑

WAN1 DDoS Prevention List

Attack List	Enable
NETBIOS	□
Trinoo	□
Back Orifice	□

WAN1 DNS configuration

Server	IP
DNS server 1	[illegible]
DNS server 2	[illegible]
DNS server 3	

NOTE

Port Settings

Refer to descriptions on the [Network & FW] → [Management] → [Config] menu for details on the items of the setting.

DMZ

The [Status] → [DMZ] menu shows the setting of DMZ, which is an internal port using a private IP.

LAN

The [Status] → [LAN] menu shows the setting of LAN, which is an internal port using a private IP.

WAN2

The [Status] → [WAN2] menu shows the setting of WAN2, which is an external port using a public IP.

SERIAL

The [Status] → [SERIAL] menu shows the setting of SERIAL, which is an external port using a public IP.

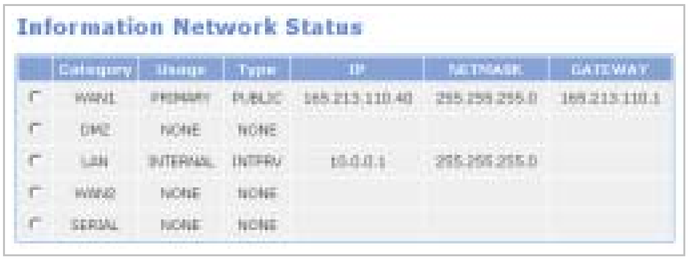
NOTE

DMZ, LAN, WAN2, and SERIAL ports' settings

- The settings of DMZ, LAN, WAN2, and SERIAL ports are shown on a window as shown for the [Status] → [WAN1] menu.
- Settings of ports that have no lines connected(When the port is set to 'No line' at the [Management] → [Config] menu) are displayed as 'No line's connected to this DMZ port'.

Network Status

The [Status] → [Network Status] menu displays settings of WAN1, DMZ, LAN, WAN2, and SERIAL.



Information Network Status

	Category	Usage	Type	IP	NETMASK	GATEWAY
○	WAN1	PRIMARY	PUBLIC	165.213.110.40	255.255.255.0	165.213.110.1
○	DMZ	NONE	NONE			
○	LAN	INTERNAL	INTPRV	10.0.0.1	255.255.255.0	
○	WAN2	NONE	NONE			
○	SERIAL	NONE	NONE			

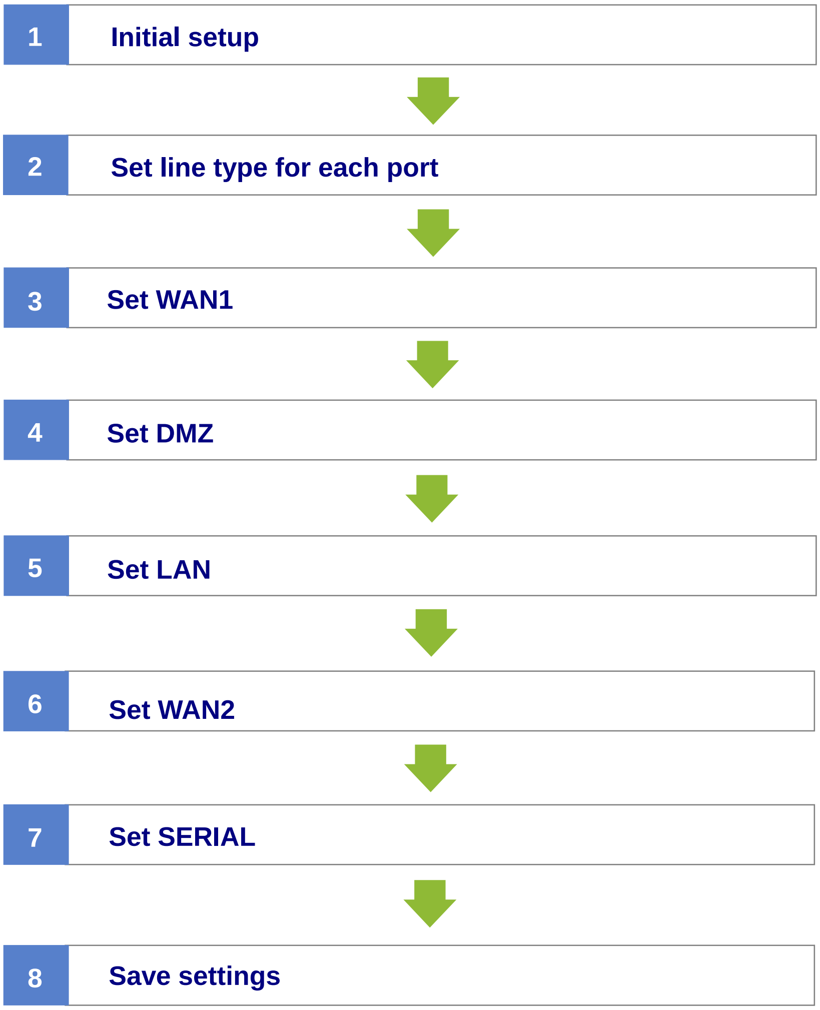
Item	Description
Category	WAN1, DMZ, LAN, WAN2, and SERIAL ports
Usage	- NONE: Unused line - PRIMARY: Mainly used line - INTERNAL: Line used for internal port
Type	- NONE: Unused line - PUBLIC: Port using public IP - INTPRV: Internal port using private IP

Management

The [Management] menu sets ports related to firewall and network.

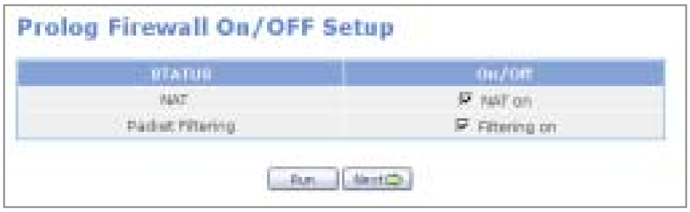
Config

The [Config] menu sets the WAN1, LAN, DMZ, WAN2, and SERIAL ports. Select [Management] → [Config] and set the items of each window. Click the [Next] button and set the firewall and network according to the following procedure:



Initial Setup

1. Select [Management] → [Config] and display the window shown below. The 'NAT' and 'Packet Filtering' items are originally disabled. Check the checkboxes to set the statuses to 'On' and click the [Run] button. If these items are checked, Click the [Next] button.



Prolog Firewall On/OFF Setup

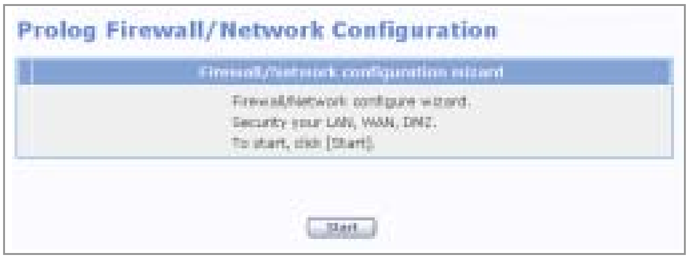
STATUS	On/Off
NAT	☑ NAT on
Packet Filtering	☑ Filtering on

NOTE

Network Address Translation(NAT)

NAT is used for forwarding packets destined for a server having a private IP of an internal network being protected, or when a packet is transmitted to an external network via firewall.

2. Click the [Start] button to start setting the firewall and network.

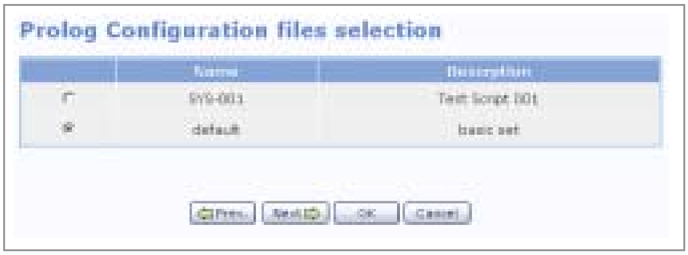


Prolog Firewall/Network Configuration

Firewall/Network configuration wizard

Firewall/Network configure wizard.
Security your LAN, WAN, DMZ.
To start, click [Start].

3. New settings can be set or previously set setup files can be changed or executed from the following window. The IP of the LAN port is initially set to '10.0.0.1'. Check the 'default' item and click the [Next] button.



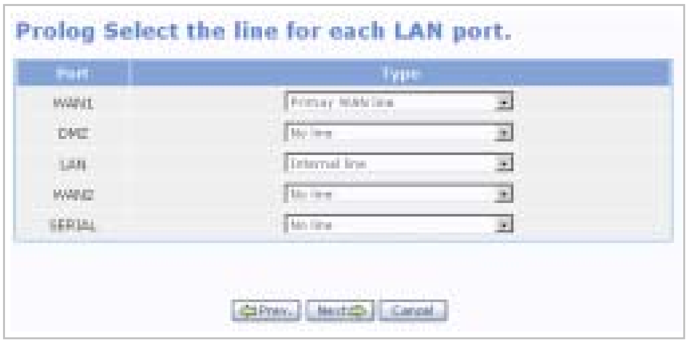
Prolog Configuration files selection

	Name	Description
○	SYS-001	Test Script 001
●	default	basic set

‘SYS-00x’ is displayed when firewall setup is complete and is not shown in the initial status of firewall. Select the setup file and click the [OK] button to edit or execute the file.

Set Line Type for Each Port

External ports(e.g. WAN1, WAN2, SERIAL) use public IPs while internal ports(e.g. DMZ, LAN) use private IPs. Select the line type for each port as shown below:



Prolog Select the line for each LAN port.

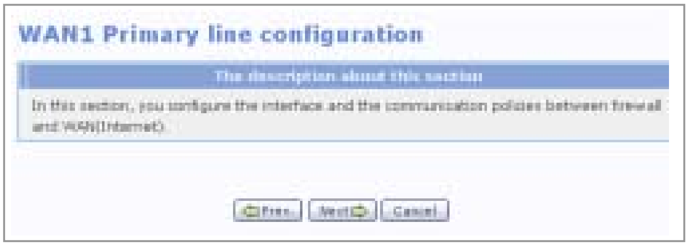
Port	Type
WAN1	Primary WAN line
DMZ	No line
LAN	Internal line
WAN2	No line
SERIAL	No line

- External port(WAN1,WAN2, SERIAL)
  - Primary WAN line: Primarily used line
  - Secondary WAN line: Secondarily used(supplementary line)
  - Third WAN line: Thirdly used(supplementary line)
  - No line: No WAN line is used
- Internal port(DMZ, LAN)
  - Internal line: Internal line is used
  - No line: Internal line is not used

Set the network as described below when setting WAN1 port as the primary line(Primary WAN line), LAN port as the internal line(Internal line), and the WAN2, SERIAL, and DMZ ports as lines not used(No line):

WAN1 Setup

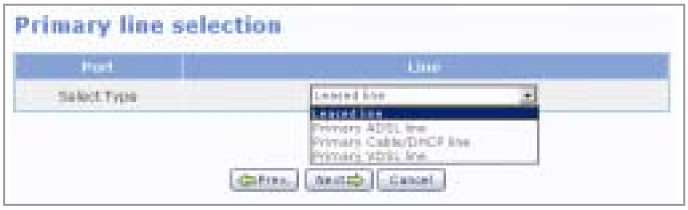
1. The starting window for setting WAN1 as ‘Primary WAN line’ is shown below. Click the [Next] button to start setting the WAN1 port.



WAN1 Primary line configuration

The description about this section
In this section, you configure the interface and the communication policies between firewall and WAN(Internet)

2. Select the line type for Primary WAN line. Select one of the four applications shown below for the external network:

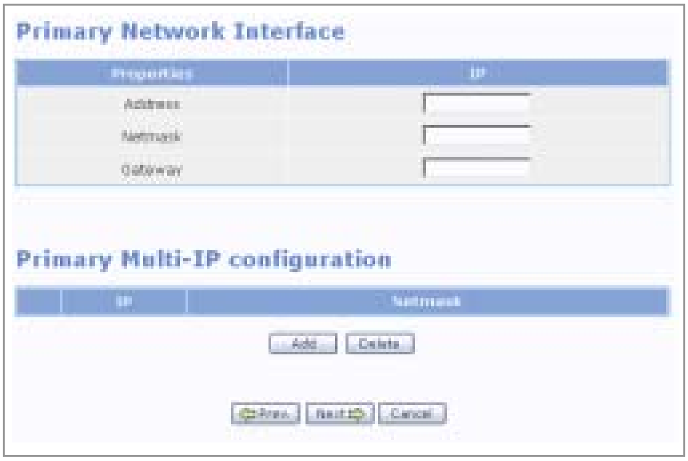


Primary line selection

Port	Line
Select Type	Leased line

The four applications of Primary WAN line are described below:

- Leased line: External network using a fixed IP
  Enter the IP address, netmask, and gateway, and click the [Next] button. To add another IP, apart from the IP of the external line currently being used, click the [Add] button and add the item.



Primary Network Interface

Properties	IP
Address	
Netmask	
Gateway	

Primary Multi-IP configuration

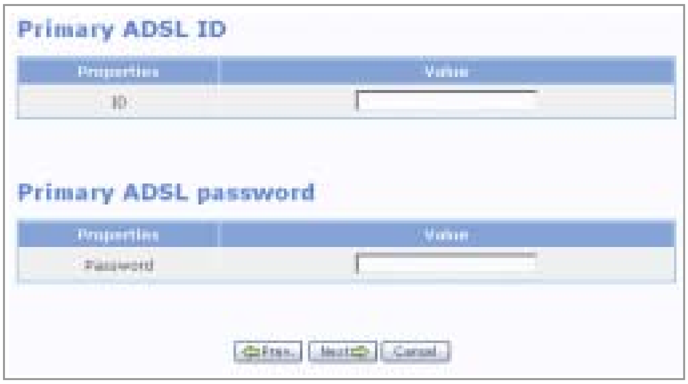
	IP	Netmask

WARNING

Caution Against Changing Network Interfaces

If a network interface(e.g. IP, gateway, and subnet mask) is changed during router operation, all the IP sessions that are being used in the router are disconnected for a while.

- Primary ADSL line: External network using a flexible ADSL IP
  Enter the ADSL account ID and password, and click the [Next] button.



Primary ADSL ID

Properties	Value
ID	

Primary ADSL password

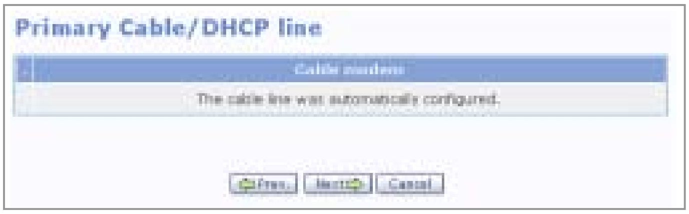
Properties	Value
Password	

CAUTION

Delete Temporary Internet Files

Delete Temporary Internet Files after upgrading Data Server package. After selecting the [Internet Explorer] → [Tools] → [Internet Options] menu, click the [Delete Cookies] and the [Delete Files] button in the [Temporary Internet files]. When Temporary Internet Files are not deleted, Data Server Web Management is not showed properly.

- Primary Cable line: External network using a cable modem
  Since cable modems are set automatically, click the [Next] button and proceed to the next window.

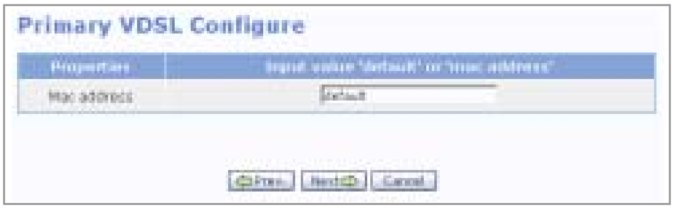


Primary Cable/DHCP line

Cable modem

The cable line was automatically configured.

- Primary VDSL line: External network using a VDSL modem
  Enter 'default' into the 'Mac address' field to disable MAC authentication, and click the [Next] button. Enter a MAC address into the 'Mac address' field to use the MAC copy function.



Primary VDSL Configure

Properties	Input value 'default' or 'mac address'
Mac address	default

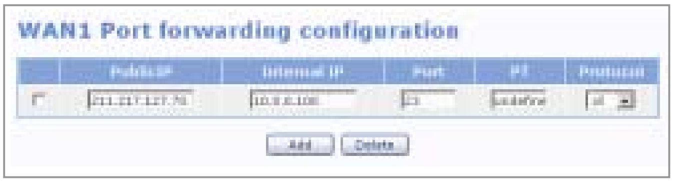
NOTE

MAC Copy Function

When performing authentication through PC MAC of LIM board, MAC of outgoing packets are copied to PC MAC instead of using MAC of outgoing packets as MAC of WAN1.

3. Set the items below and click the [Next] button.

- WAN1 Port forwarding configuration
  This setting is used for enabling external servers to use the services of an internal server connected to the firewall.



WAN1 Port forwarding configuration

	PublicIP	Internal IP	Port	PT	Protocol
□	211.217.127.70	10.0.0.100	23	[illegible]	all

Let's assume that the public IP of the firewall is '211.217.127.70' and the private IP of the internal server is '10.0.0.100'. An external server outside the firewall can use the Telnet service of the internal server through the port forwarding setup.
Click the [Add] button and enter the items below. When entered as shown in the above window, an external network can connect to '211.217.127.70' through Telnet to use the Telnet service of the internal network(10.0.0.100).

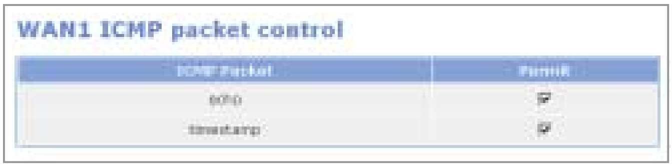
- PublicIP: Public IP of firewall
- InternalIP: Private IP of the internal server connected to the firewall
- Port: Firewall port(ex: port of the Telnet server)
- Protocol: Protocol(select among all, tcp, and udp)

NOTE

Port Range Setting

- When using ports from 0 to 100, enter ‘0:100’.
- ‘0:’ indicates all ports.

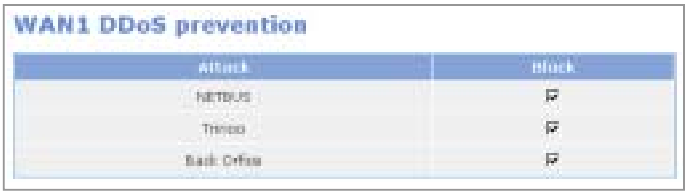
- WAN1 ICMP packet control
  The firewall does not respond to ICMP echo and ICMP timestamp by default. However, if the ‘echo’ and ‘timestamp’ items are checked, response to external ping commands are displayed. If these items are not checked, Request timed out occurs.



WAN1 ICMP packet control

ICMP Packet	Permit
echo	☑
timestamp	☑

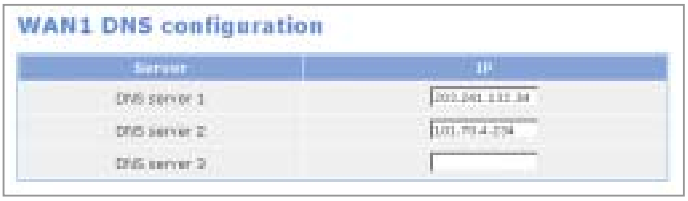
- WAN1 DDoS prevention
  Check the items shown below to prevent DDoS attacks by blocking attacks using the corresponding hacking programs.



WAN1 DDoS prevention

Attack	Block
NETBUS	☑
Trinoo	☑
Back Orifice	☑

- WAN1 DNS configuration
  Enter the IP address of the DNS server.

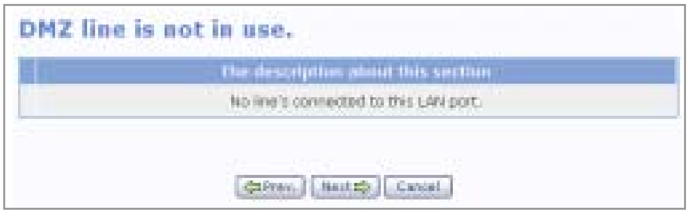


WAN1 DNS configuration

Server	IP
DNS server 1	203.241.132.34
DNS server 2	101.79.4.234
DNS server 3	

DMZ Setup

The below window shows that DMZ was set to ‘No line’ at the <Prolog Select the line for each LAN port> window(Refer to ‘Set Line Type for Each Port’). Click the [Next] button and proceed to the next window.



DMZ line is not in use.

The description about this section

No line's connected to this LAN port.

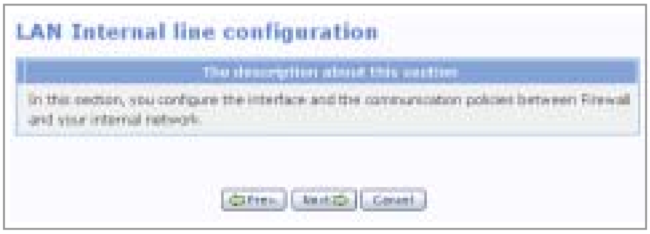
NOTE

When set to ‘Internal line’

If DMZ was set to ‘Internal line’ at the <Prolog Select the line for each LAN port> window(Refer to ‘Set Line Type for Each Port’), follow the setup procedure of ‘LAN Setup’.

LAN Setup

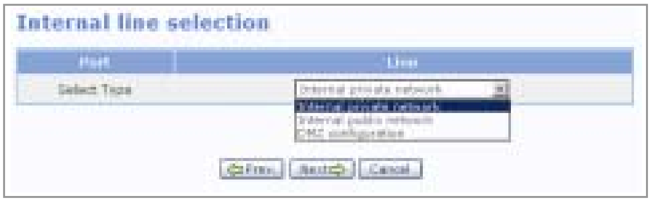
1. The below window shows the LAN was set to ‘Internal line’ at the <Prolog Select the line for each LAN port> window(Refer to ‘Set Line Type for Each Port’). Click the [Next] button to start LAN port setup.



LAN Internal line configuration

The description about this section
In this section, you configure the interface and the communication policies between Firewall and your internal network.

2. Select the internal line type.



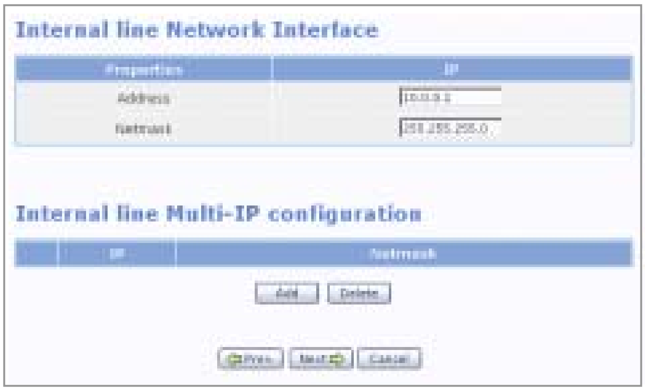
Internal line selection

Port	Line
Select Type	Internal private network

Types of internal lines are described below:

- Internal private network: Select this option to configure an internal network using a private IP.

  Enter the IP address, netmask, and gateway to use LAN as an internal private network, and click the [Next] button. To add another IP, apart from the IP of the internal line currently being used, click the [Add] button and add the item.



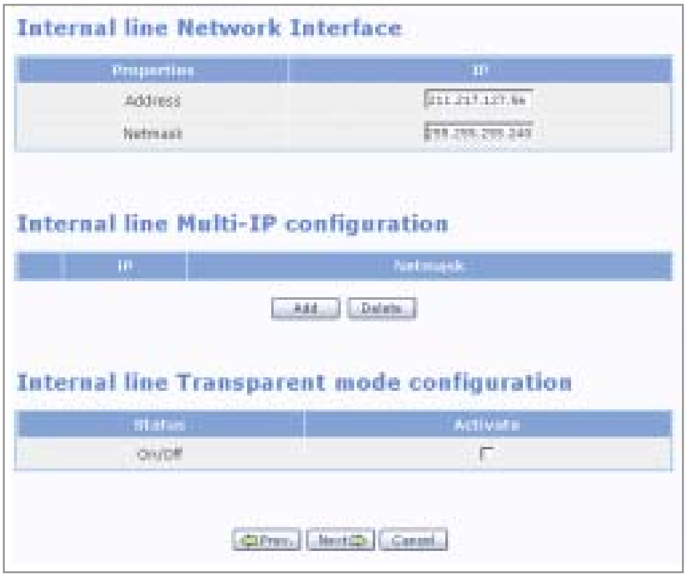
Internal line Network Interface

Properties	IP
Address	10.0.0.1
Netmask	255.255.255.0

Internal line Multi-IP configuration

	IP	Netmask

- Internal public network: Select this option to configure an internal network using a public IP.



Internal line Network Interface

Properties	IP
Address	211.217.127.56
Netmask	255.255.255.240

Internal line Multi-IP configuration

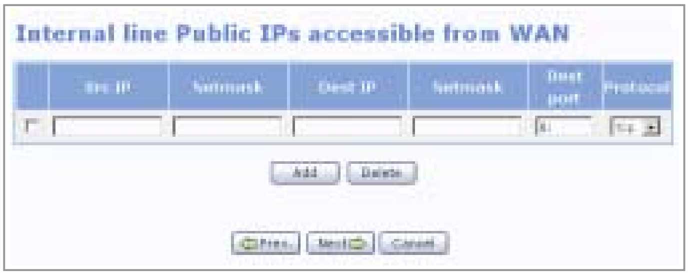
	IP	Netmask

Internal line Transparent mode configuration

Status	Activate
On/Off	□

Click [Add] to add an IP in addition to the IPs of the internal line being used.
If the checkbox of 'Internal line Transparent mode configuration' is selected, the Proxy ARP function is enabled. If not, the function is disabled.

Enter the IP address and netmask to use LAN as an internal public network, and click the [Next] button.



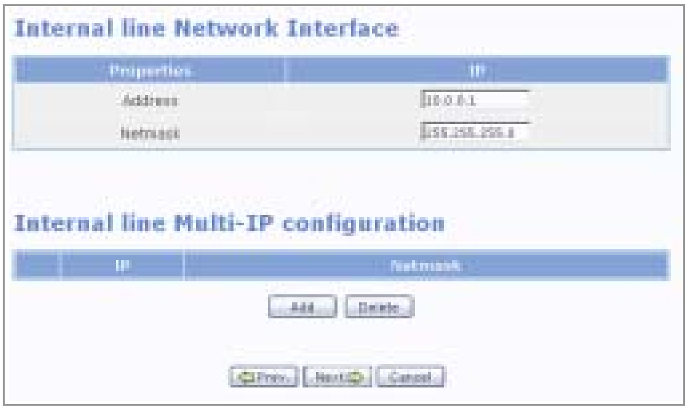
Internal line Public IPs accessible from WAN

	Src IP	Netmask	Dest IP	Netmask	Dest port	Protocol
□					0	TCP

To add another IP, apart from the IP of the external line currently being used, click the [Add] button and add the item.
Check the 'Internal line Transparent mode configuration' item to use the Proxy ARP function.

Set ‘Src IP’ and ‘Netmask’ to allow external networks to access a specific server having a public IP inside the firewall. Set ‘Src IP’ and ‘Netmask’ to ‘0.0.0.0’ to allow access from all external networks.

- DMZ configuration: Select this option to set the DMZ server.



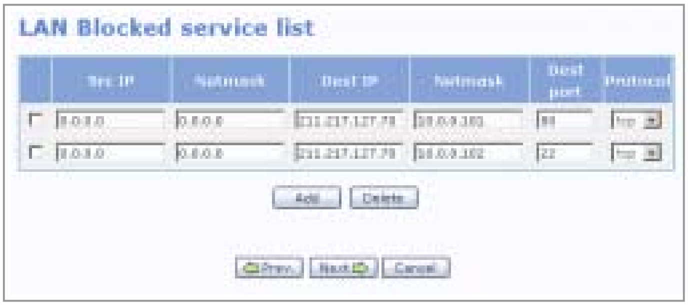
Internal line Network Interface

Properties	IP
Address	10.0.0.1
Netmask	255.255.255.0

Internal line Multi-IP configuration

	IP	Netmask

Enter the IP address, netmask, and gateway to use LAN as a DMZ network, and click the [Next] button. To add another IP, apart from the IP of the internal line currently being used, click the [Add] button and add the item.

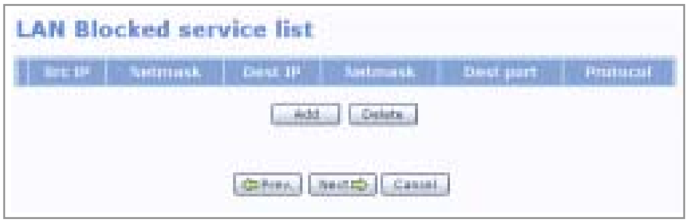


LAN Blocked service list

	Src IP	Netmask	Dest IP	Netmask	Dest port	Protocol
□	0.0.0.0	0.0.0.0	211.217.127.78	10.0.0.103	80	tcp
□	0.0.0.0	0.0.0.0	211.217.127.78	10.0.0.102	22	tcp

Set ‘Src IP’ and ‘Netmask’ to allow external networks to access a specific server having a public IP inside the firewall. Set ‘Src IP’ and ‘Netmask’ to ‘0.0.0.0’ to allow access from all external networks.

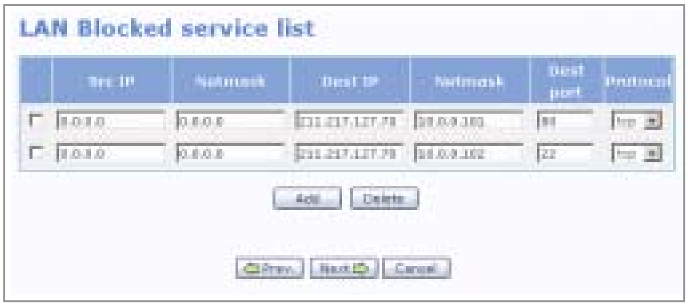
3. Set an IP from this window to restrict an internal PC and ‘Src IP’ from accessing ‘Dest IP’. The entire network or a specific network can be selected.



LAN Blocked service list

Src IP	Netmask	Dest IP	Netmask	Dest port	Protocol

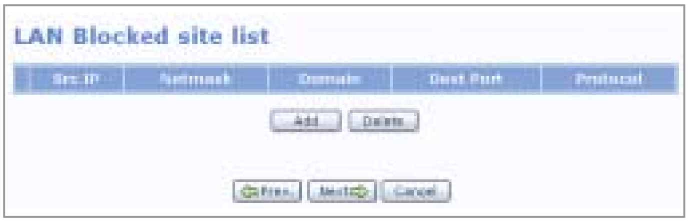
Click [Add] and fill out the fields as shown below. Then, any terminals cannot connect to Ports 80 and 22 whose destination address is ‘211.17.127.70’.



LAN Blocked service list

	Src IP	Netmask	Dest IP	Netmask	Dest port	Protocol
☐	0.0.0.0	0.0.0.0	211.217.127.78	10.0.0.101	80	tcp
☐	0.0.0.0	0.0.0.0	211.217.127.78	10.0.0.102	22	tcp

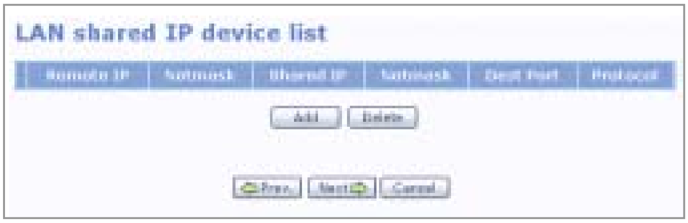
Click the [Next] button to display the window below. Enter a domain in this window to prevent an internal PC and ‘Src IP’ from accessing the site. Click the [Add] button to set the domain, and click the [Next] button.



LAN Blocked site list

Src IP	Netmask	Domain	Dest Port	Protocol

4. Assuming that the LAN port and DMZ port are configured as Internet private lines, this window enables an internal server of the DMZ port to access an internal server of the LAN port. Click the [Add] button to set the IP, and click the [Next] button.

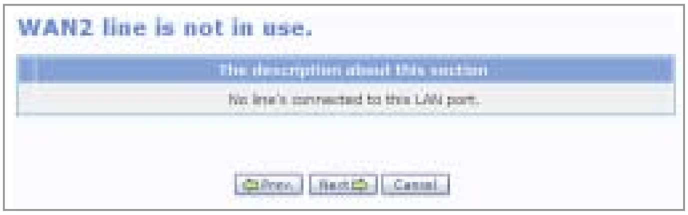


LAN shared IP device list

Remote IP	Subnetmask	Shared IP	Subnetmask	Dest Port	Protocol

WAN2 Setup

The below window shows that WAN2 was set to ‘No line’ at the <Prolog Select the line for each LAN port> window(Refer to ‘Set Line Type for Each Port’). Click the [Next] button and proceed to the next window.



WAN2 line is not in use.

The description about this section
No line's connected to this LAN port.

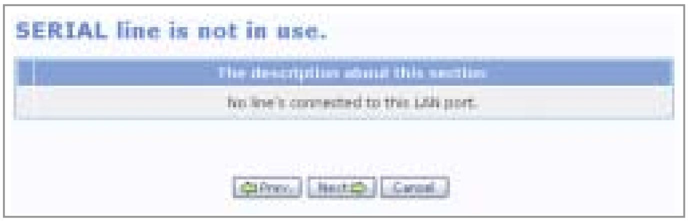
NOTE

WAN2 Setup

If WAN2 was set to Primary WAN line, Secondary WAN line, or Third WAN line at the <Prolog Select the line for each LAN port> window(Refer to ‘Set Line Type for Each Port’), follow the setup procedure of ‘WAN1 Setup’.

SERIAL Setup

The below window shows that SERIAL was set to ‘No line’ at the <Prolog Select the line for each LAN port> window(Refer to ‘Set Line Type for Each Port’). Click the [Next] button and proceed to the next window.



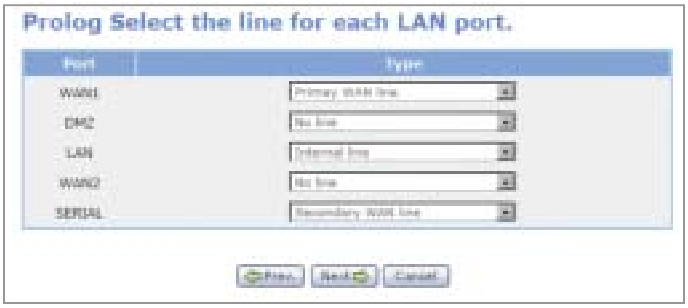
SERIAL line is not in use.

The description about this section

No line's connected to this LAN port.

Follow the procedure below to use SERIAL as the Secondary WAN line:

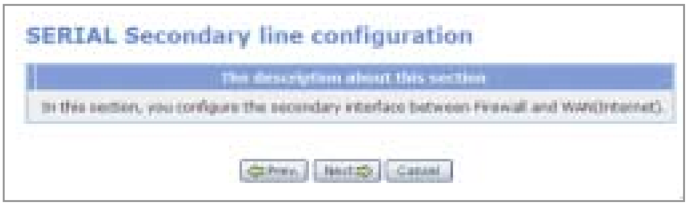
1. Set the SERIAL to ‘Secondary WAN line’ at the <Prolog Select the line for each LAN port> window(Refer to ‘Set Line Type for Each Port’), and click the [Next] button.



Prolog Select the line for each LAN port.

Port	Type
WAN1	Primary WAN line
DMZ	No line
LAN	Internal line
WAN2	No line
SERIAL	Secondary WAN line

2. Click the [Next] button to start the SERIAL port setup.

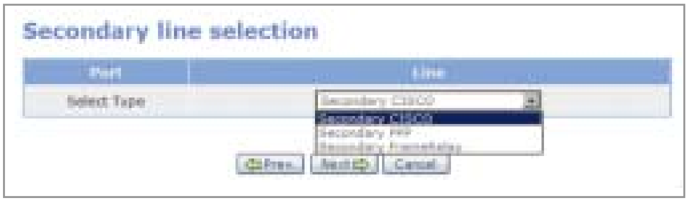


SERIAL Secondary line configuration

The description about this section

In this section, you configure the secondary interface between Firewall and WAN(Internet).

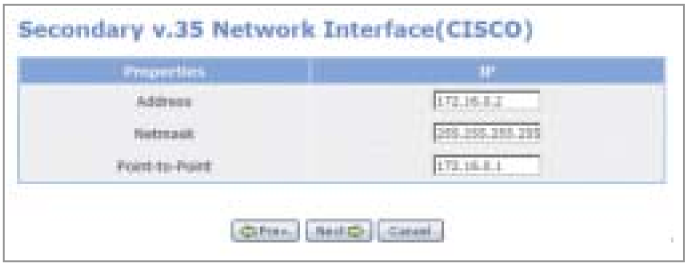
3. Select the type of the secondary line.



Secondary line selection

Port	Line
Select Type	Secondary CISCO

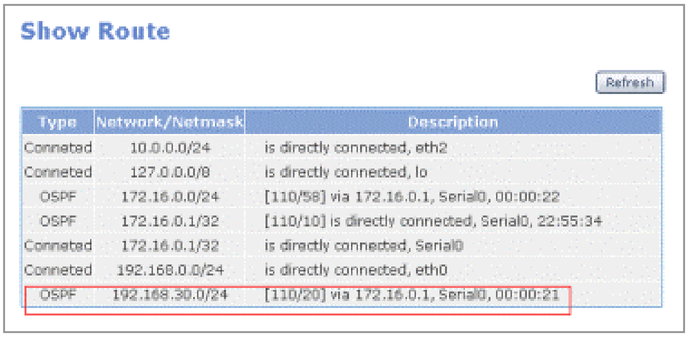
- Secondary CISCO
  Select ‘Secondary CISCO’ from the <Secondary line selection> window and click the [Next] button to display the window shown below. Enter the items and click the [Next] button.



Secondary v.35 Network Interface(CISCO)

Properties	IP
Address	172.16.0.2
Netmask	255.255.255.255
Point-to-Point	172.16.0.1

After setting the SERIAL port as Secondary CISCO line, check the [Router] → [Show Route] menu. The row inside the red box should be displayed if the setting was successful.



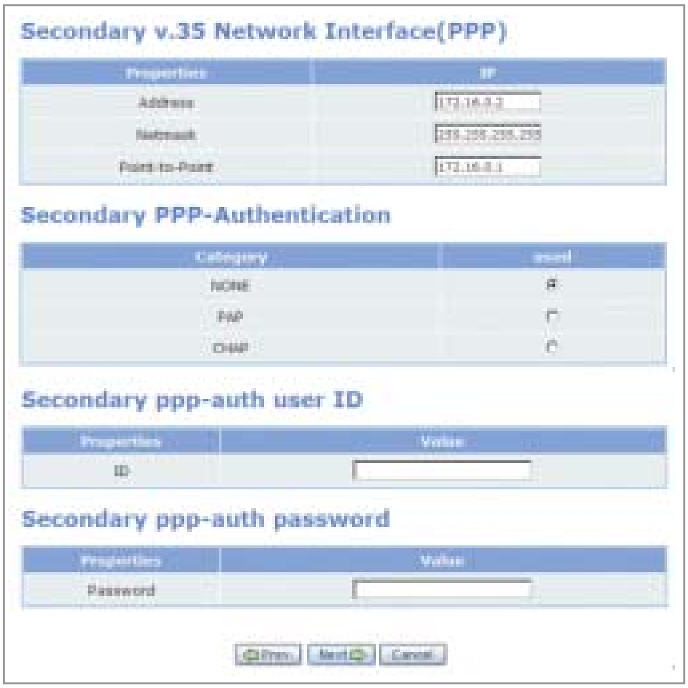
Show Route

Type	Network/Netmask	Description
Conneted	10.0.0.0/24	is directly connected, eth2
Conneted	127.0.0.0/8	is directly connected, lo
OSPF	172.16.0.0/24	[110/58] via 172.16.0.1, Serial0, 00:00:22
OSPF	172.16.0.1/32	[110/10] is directly connected, Serial0, 22:55:34
Conneted	172.16.0.1/32	is directly connected, Serial0
Conneted	192.168.0.0/24	is directly connected, eth0
OSPF	192.168.30.0/24	[110/20] via 172.16.0.1, Serial0, 00:00:21

Use the ping command from the client server to check if the network was normally connected. If not, check the firewall and router settings and check whether the cables are properly connected.

- Secondary PPP

  Select 'Secondary PPP' from the <Secondary line selection> window and click the [Next] button to display the window shown below. Enter the address, netmask, and point-to-point items and click the [Next] button.



Secondary v.35 Network Interface(PPP)

Properties	IP
Address	172.16.0.2
Netmask	255.255.255.255
Point-to-Point	172.16.0.1

Secondary PPP-Authentication

Category	used
NONE	●
PAP	○
CHAP	○

Secondary ppp-auth user ID

Properties	Value
ID	

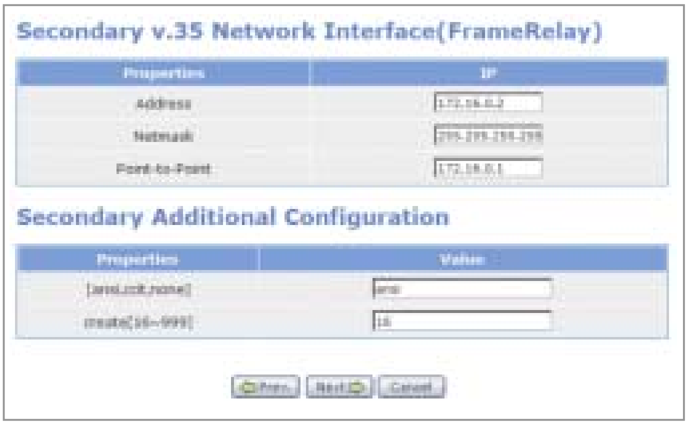
Secondary ppp-auth password

Properties	Value
Password	

If the Secondary PPP-Authentication item is set to 'NONE', do not enter the ID and password.

- Secondary FrameRelay

  Select ‘Secondary FrameRelay’ from the <Secondary line selection> window and click the [Next] button to display the window shown below. Enter the following items and click the [Next] button:



Secondary v.35 Network Interface(FrameRelay)

Properties	IP
Address	172.16.0.2
Netmask	255.255.255.255
Point-to-Point	172.16.0.1

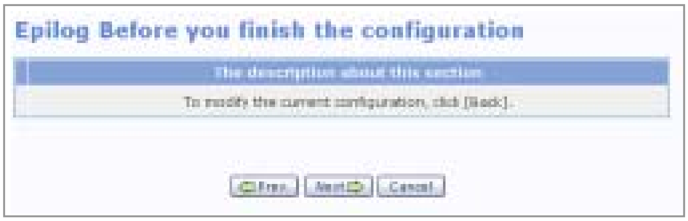
Secondary Additional Configuration

Properties	Value
[ansi,ccitt,none]	ansi
create[16~999]	16

Item	Description
[ansi, ccitt, none]	Signaling type
create[16~999]	Signaling channel No. Permanent Virtual Circuit(PVC).

Saving Settings

1. The below window shows the firewall and network setup is complete. Click the [Next] button and proceed to the next window.

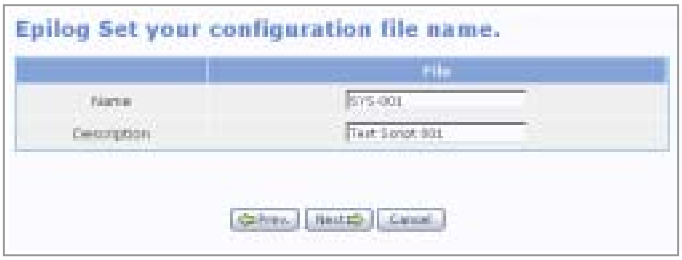


Epilog Before you finish the configuration

The description about this section

To modify the current configuration, click [Back].

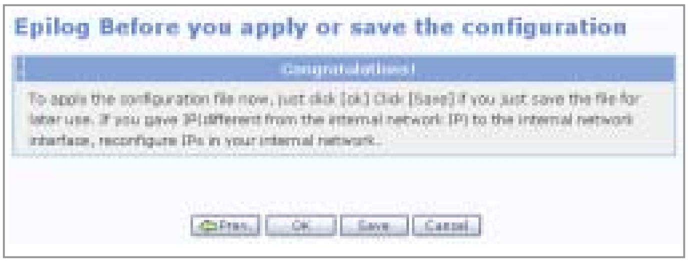
2. To save the setting as a file, enter the file name and description and click the [Next] button.



Epilog Set your configuration file name.

	File
Name	SYS-001
Description	Test Script 001

3. Click the [Save] button to save the setting as a file having the file name set above. Click [OK] to execute the setting or click the [Cancel] button the cancel the setting.



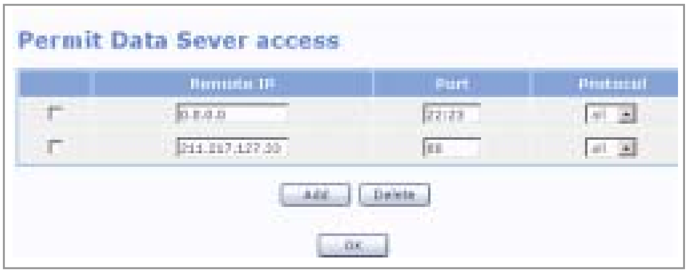
Epilog Before you apply or save the configuration

Congratulations!

To apply the configuration file now, just click [ok]. Click [Save] if you just save the file for later use. If you gave IP(different from the internal network IP) to the internal network interface, reconfigure IPs in your internal network.

Remote Accept

The [Remote Accept] menu is used to allow a specific IP to access the firewall. Although external networks are restricted from accessing the firewall, a specific server can be allowed to access the firewall when necessary.
Select [Management] → [Remote Accept] and set the IP address, port, and protocol, as shown below, and click the [OK] button:



Permit Data Sever access

	Remote IP	Port	Protocol
□	0.0.0.0	22:23	all
□	211.217.127.33	80	all

If the user sets the options as shown above, the server whose IP address is '211.217.127.33' can connect to the system firewall via the web. Also, other external servers can connect to the firewall by using connection programs such as Telnet and SSH.

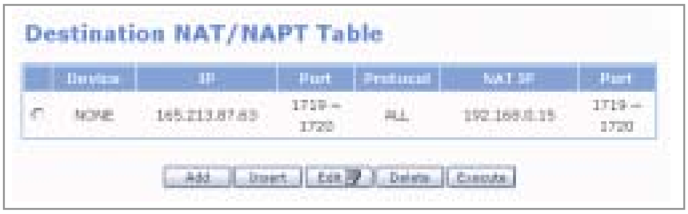
CAUTION

Security Warning

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

DNAT Config

Destination NAT(DNAT) is used to forward packets headed for a server of an internal network protected by a firewall to a specific server having a private IP of the internal network. Select the [Management] → [DNAT Config] menu to set DNAT.

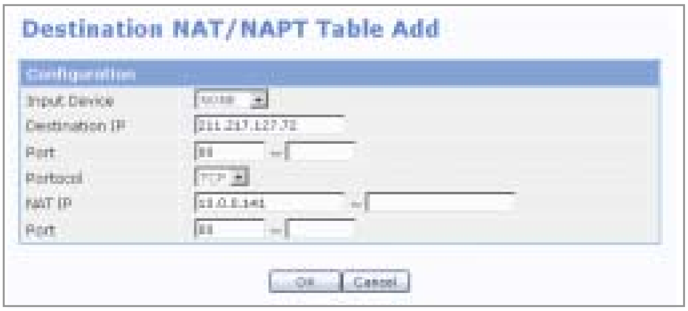


Destination NAT/NAPT Table

	Device	IP	Port	Protocol	NAT IP	Port
○	NONE	165.213.87.63	1719 ~ 1720	ALL	192.168.0.15	1719 ~ 1720

Button	Description
Add	Add a DNAT rule
Insert	Insert a DNAT rule
Edit	Modify a DNAT rule
Delete	Delete a DNAT rule
Execute	Execute a defined rule

Select the menu button from the <Destination NAT/NAPT Table> window to display the DNAT setup window shown below:
When setting values of the Port(destination port), NAT IP, and Port(port No.) options in the type of a range, assign values within the corresponding ranges. When the values are not set in the type of a range, the NAT operates as Static NAT.



Destination NAT/NAPT Table Add

Configuration

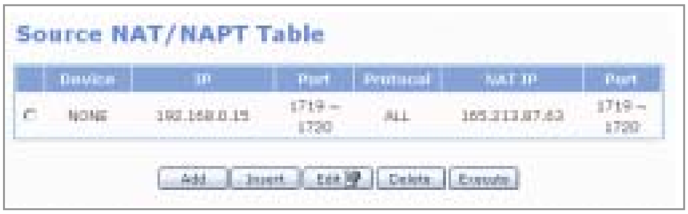
Input Device	NONE
Destination IP	211.217.127.72
Port	80 ~
Protocol	TCP
NAT IP	10.0.0.141 ~
Port	80 ~

When set as above, traffics heading for port #80 of ‘211.217.127.72’ are forwarded to port #80 of ‘10.0.0.141’ inside the firewall.

Item	Description
Input Device	Select port. - NONE: All ports(external ports and internal ports) - External ports: WAN1, WAN2, SERIAL - Internal ports: DMZ, LAN
Destination IP	Destination IP address
Port	Destination port
Protocol	Select protocol(Select TCP, UDP, or ALL)
NAT IP	Range of IP addresses used for NAT
Port	Port No.(1:1 port mapping is disabled when setting a range of ports.)

SNAT Config

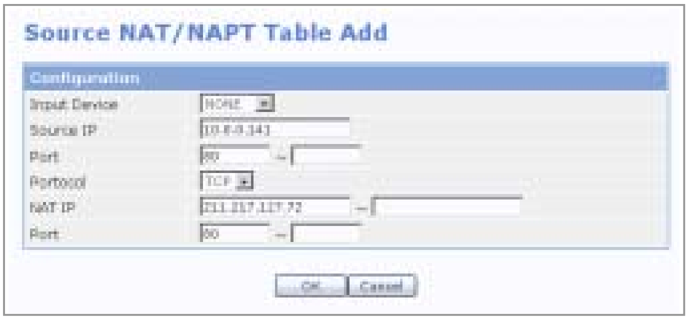
Source NAT(SNAT) is used for packets being transferred from a server of an internal network inside a firewall to an external network via the firewall. Select the [Management] → [SNAT Config] menu to set SNAT.



Source NAT/NAPT Table

	Device	IP	Port	Protocol	NAT IP	Port
○	NONE	192.168.0.15	1719 ~ 1720	ALL	165.213.87.63	1719 ~ 1720

Select the menu button in the above window to display the SNAT setup window shown below:



Source NAT/NAPT Table Add

Configuration

Input Device	NONE
Source IP	10.8.0.141
Port	80 ~
Portocol	TCP
NAT IP	211.217.127.72 ~
Port	80 ~

When set as above, the private IP(10.0.0.141) of an outgoing packet is changed to a public IP(211.217.127.72). That is, packets generated by the internal network will seem as if generated by the public IP set at the firewall.

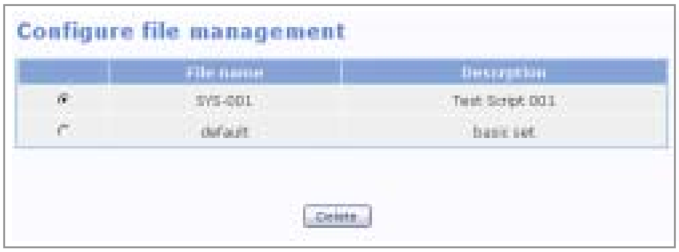
NOTE

Menu Buttons and Item Descriptions

Refer to descriptions on the [DNAT Config] menu for details on menu buttons and item descriptions.

File Delete

The setting data file saved by the [Management] → [Config] menu can be deleted using the [File Delete].



Configure file management

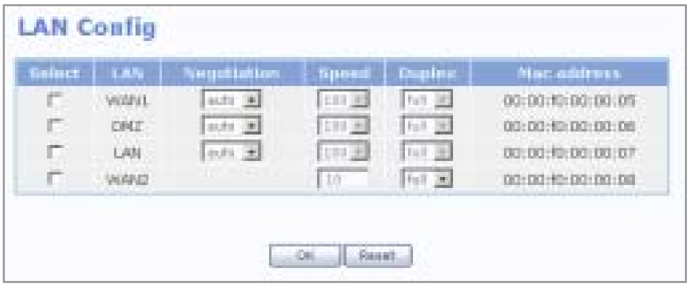
	File name	Description
●	SYS-001	Test Script 001
○	default	basic set

LAN Config

The [LAN Config] menu sets the negotiation, speed, and transfer system for each port.

Select the checkbox of the port to set and click [OK].

Click [Reset] to reset to the default value.



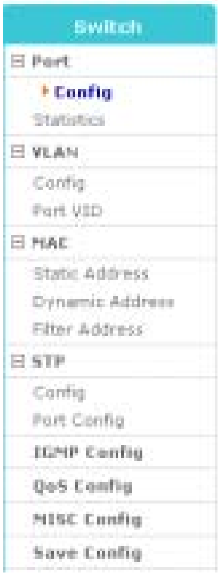
LAN Config

Select	LAN	Negotiation	Speed	Duplex	Mac address
□	WAN1	auto	100	full	00:00:f0:00:00:05
□	DMZ	auto	100	full	00:00:f0:00:00:06
□	LAN	auto	100	full	00:00:f0:00:00:07
□	WAN2		10	full	00:00:f0:00:00:08

Item	Description
Negotiation	- auto: Controls speed through negotiation. - force: Controls speed through enforcement. Set this item to ‘force’ when setting the Duplex item to ‘full’.
Speed(Mbps)	Transfer rate of port
Duplex	- full: Bidirectional service(full-duplex system) - half: Unidirectional service(half-duplex system) Setting for the WAN2 10M interface depends on the counterpart modem.

Switch Menus

Select [Switch] to display the submenus of Switch on the upper left section of the window.



Menu	Submenu	Description
Port	Config	Sets the switch port environment.
	Statistics	Displays the link status, speed, transmission system, and statistics of the switch port.
VLAN	Config	Configures Virtual LAN(VLAN).
	Port VID	Sets processing method for untagged packets when VLAN mode is set to ‘Tag-based VLAN’.
MAC	Static Address	Saves MAC address to the static address table of the switch.
	Dynamic Address	Retrieves the dynamic address table or deletes a MAC address.
	Filter Address	Enter a MAC address to block corresponding packets at the switch.
STP	Config	Prevents switch loop-back through STP.
	Port Config	Sets STP status.
IGMP Config	-	Efficiently processes multicast packets through IGMP snooping.

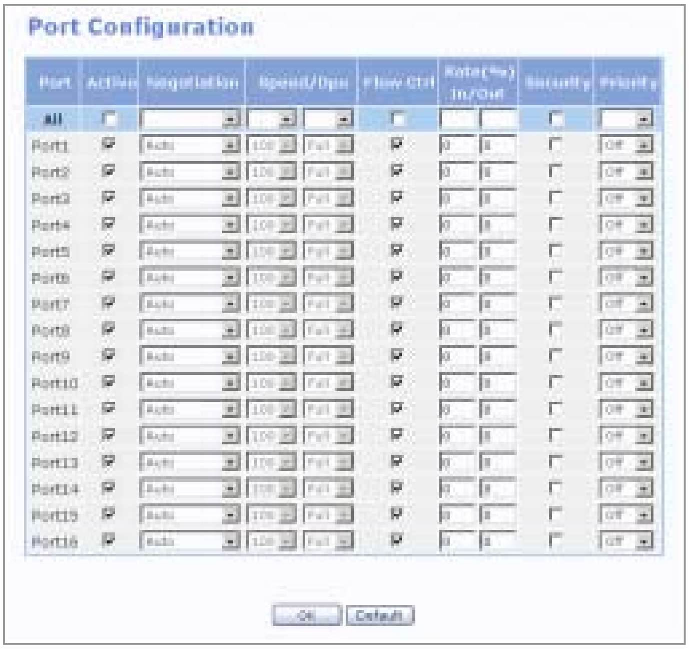
Menu	Submenu	Description
QoS Config	-	Processes QoS by sequentially assigning priority to packets entering the switch or by enforcing priority on a specific port.
MISC Config	-	Sets mirroring and other switching functions.
Save Config	-	Saves setting to flash disk or initializes all setting values.

Port

The [Port] menu is used for setting port related functions and retrieving information on a port.

Config

Select [Port] → [Config] to set the environment of a switch port.



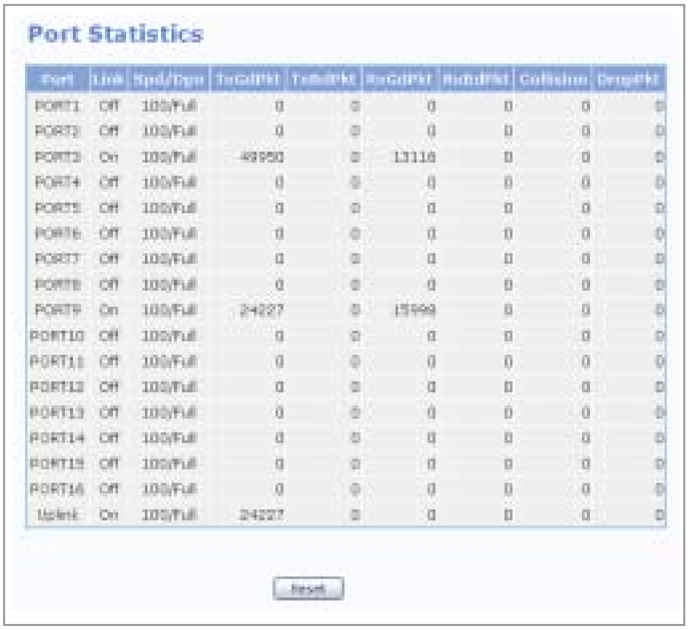
Port Configuration

Port	Active	Negotiation	Speed/Dpx		Flow Ctrl	Rate(%) In/Out		Security	Priority
All	□				□			□	
Port1	☑	Auto	100	Full	☑	0	0	□	Off
Port2	☑	Auto	100	Full	☑	0	0	□	Off
Port3	☑	Auto	100	Full	☑	0	0	□	Off
Port4	☑	Auto	100	Full	☑	0	0	□	Off
Port5	☑	Auto	100	Full	☑	0	0	□	Off
Port6	☑	Auto	100	Full	☑	0	0	□	Off
Port7	☑	Auto	100	Full	☑	0	0	□	Off
Port8	☑	Auto	100	Full	☑	0	0	□	Off
Port9	☑	Auto	100	Full	☑	0	0	□	Off
Port10	☑	Auto	100	Full	☑	0	0	□	Off
Port11	☑	Auto	100	Full	☑	0	0	□	Off
Port12	☑	Auto	100	Full	☑	0	0	□	Off
Port13	☑	Auto	100	Full	☑	0	0	□	Off
Port14	☑	Auto	100	Full	☑	0	0	□	Off
Port15	☑	Auto	100	Full	☑	0	0	□	Off
Port16	☑	Auto	100	Full	☑	0	0	□	Off

Item	Description
Port	16 switch ports are equipped in all. Select All to process all ports simultaneously.
Active	Set whether to use the port.
Negotiation	- Auto: Controls speed through negotiation. - Force: Controls speed through enforcement. Set this item to ‘force’ when setting the Duplex item to ‘Full’.
Speed/Dpx	- Speed: Automatically set according to the value set for ‘Path Cost’ of the [Switch] → [STP] → [Port Config] menu.(10 Mb/s when ‘Path Cost’ is set to ‘100’, and 100 Mb/s when set to ‘19’.) - Dpx(Duplex): Select Full(bidirectional service) or Half(unidirectional service).
Flow Ctl	Set whether to use flow control. Flow control is performed according to the value set for Rate(%) In/Out(incoming rate/outgoing rate).
Rate(%) In/Out	Flow can be controlled by setting Rate(%) In/Out for each port. The unit is the ratio against port speed, and should be set to ‘0’ when not using flow control(when flow control item is not checked).
Security	Set whether to allow MAC address table update. Security can be maintained by checking this item and setting the MAC address as a static address, which allows only hosts corresponding to the MAC address to access the port.
Priority	If set to ‘Low’ or ‘High’, priority is set regardless of the QoS bit setting of the incoming packet.

Statistics

The [Port] → [Statistics] menu is used for retrieving the link status, speed, transmission system, and statistics. The numbers show the accumulated values for the period from the system boot up to date. The window is automatically updated every five seconds. Click the [Reset] button to initialize all values to '0'.



Port Statistics

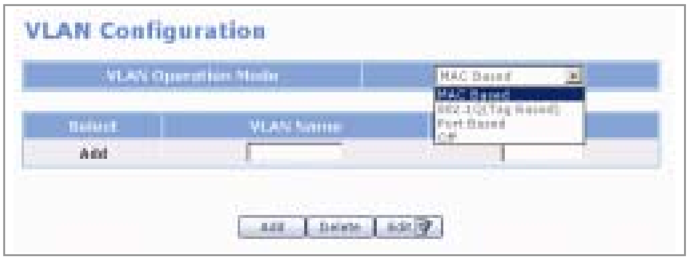
Port	Link	Spd/Dpx	TxGdPkt	TxBdPkt	RxGdPkt	RxBdPkt	Collision	DropPkt
PORT1	Off	100/Full	0	0	0	0	0	0
PORT2	Off	100/Full	0	0	0	0	0	0
PORT3	On	100/Full	49950	0	13116	0	0	0
PORT4	Off	100/Full	0	0	0	0	0	0
PORT5	Off	100/Full	0	0	0	0	0	0
PORT6	Off	100/Full	0	0	0	0	0	0
PORT7	Off	100/Full	0	0	0	0	0	0
PORT8	Off	100/Full	0	0	0	0	0	0
PORT9	On	100/Full	24227	0	15998	0	0	0
PORT10	Off	100/Full	0	0	0	0	0	0
PORT11	Off	100/Full	0	0	0	0	0	0
PORT12	Off	100/Full	0	0	0	0	0	0
PORT13	Off	100/Full	0	0	0	0	0	0
PORT14	Off	100/Full	0	0	0	0	0	0
PORT15	Off	100/Full	0	0	0	0	0	0
PORT16	Off	100/Full	0	0	0	0	0	0
Uplink	On	100/Full	24227	0	0	0	0	0

VLAN

The [VLAN] menu is used for configuring Virtual LAN(VLAN).

Config

Select [VLAN] → [Config] to display the VLAN configuration window.



Select a VLAN mode from the ‘VLAN Operation Mode’ and click the [OK] button. Then, enter a VLAN name and ID and click the [Add] button to add the VLAN.
Check a VLAN and click the [Delete] button to delete the VLAN.

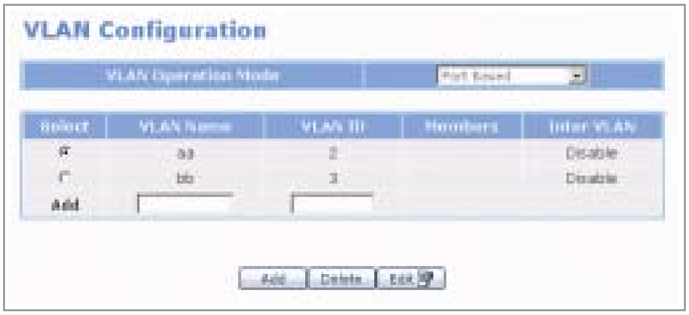
VLAN configuration is determined according to the three VLAN modes below:

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

Port Based VLAN

This option is used to configure VLAN on 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 Based’ as the VLAN Operation Mode from the <VLAN Configuration> window.

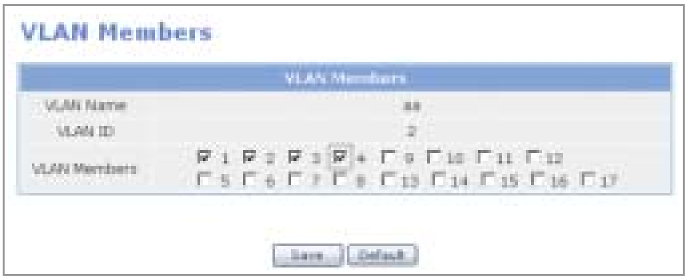


VLAN Configuration

VLAN Operation Mode	Port Based

Select	VLAN Name	VLAN ID	Members	Inter VLAN
●	aa	2		Disable
○	bb	3		Disable
Add				

Select a VLAN and click the [Edit] button to display the window shown below. Select the target port at VLAN Members and click the [Save] button.



VLAN Members

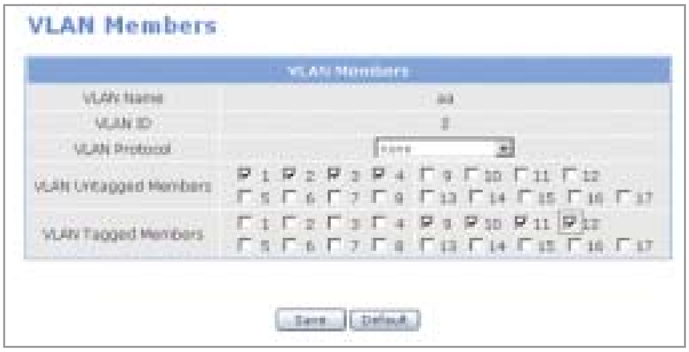
VLAN Members	
VLAN Name	aa
VLAN ID	2
VLAN Members	☑ 1 ☑ 2 ☑ 3 ☑ 4 ☐ 9 ☐ 10 ☐ 11 ☐ 12 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 13 ☐ 14 ☐ 15 ☐ 16 ☐ 17

Tag Based VLAN(802.1 Q)

If VLAN needs to be decided for a packet entering a specific port(When the port is assigned to multiple VLANs), the decision can be made based on the tag information included in the packet.
Packets not including tags are delivered to a single VLAN and only to the VLAN according to the PVID[Port VID(VLAN ID)].
However, since a layer 2 protocol is used for determining the VLAN, even packets forwarded to a single VLAN using PVID will eventually be lost if the protocol does not match that of the VLAN.

Tag Based VLAN is composed of tagged members and untagged members, and is processed accordingly. Since a network equipment that can process the 802.1 Q standard is not connected in most cases to process tagged packets entering a switch port, it is recommended to convert the received tagged packets before transferring them.

Select 'Tag Based' as the VLAN Operation Mode from the <VLAN Configuration> window and click the [Edit] button to display the window shown below. Select the ports for VLAN Untagged Members and for VLAN Tagged Members, and click the [Save].



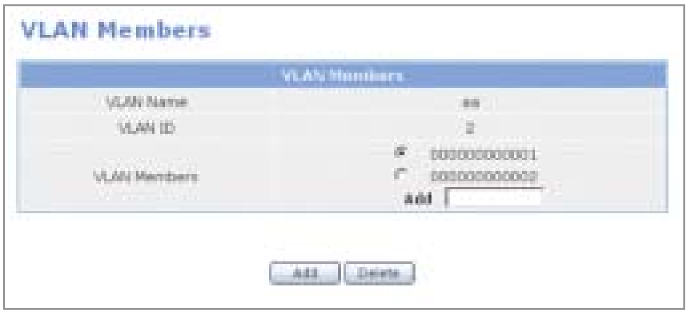
VLAN Members

VLAN Members	
VLAN Name	aa
VLAN ID	2
VLAN Protocol	None
VLAN Untagged Members	☑ 1 ☑ 2 ☑ 3 ☑ 4 □ 9 □ 10 □ 11 □ 12 □ 5 □ 6 □ 7 □ 8 □ 13 □ 14 □ 15 □ 16 □ 17
VLAN Tagged Members	□ 1 □ 2 □ 3 □ 4 ☑ 9 ☑ 10 ☑ 11 ☑ 12 □ 5 □ 6 □ 7 □ 8 □ 13 □ 14 □ 15 □ 16 □ 17

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 1024 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 Address Resolution Protocol(ARP). Thus, the ARP packet must be transmitted to the switch to enable members of a VLAN to exchange packets.

Select 'MAC Based VLAN' as the VLAN Operation Mode from the <VLAN Configuration> window and click the target VLAN, and click the [Edit] button to display the window shown below. Enter the MAC address of a member into the 'Add' field and click the [Add] button to add the member or click the [Delete] button to delete the member.

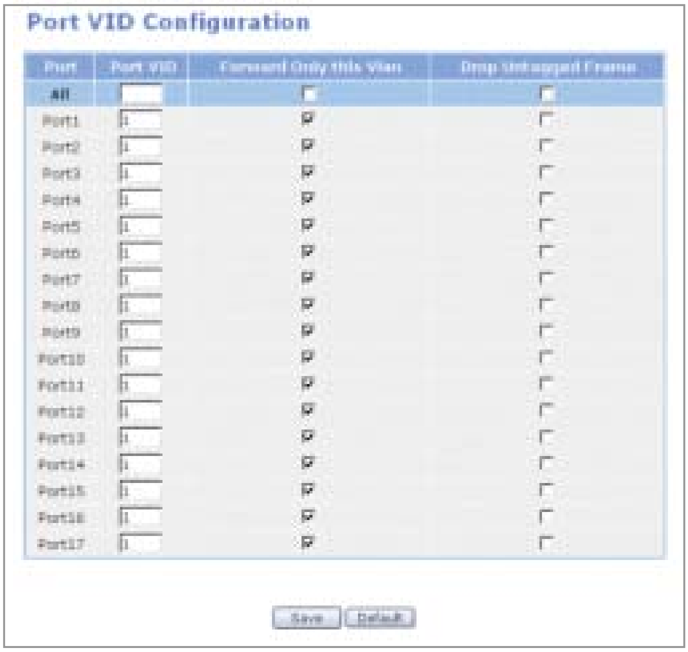


VLAN Members

VLAN Members	
VLAN Name	aa
VLAN ID	2
VLAN Members	● 000000000001 ○ 000000000002 Add

Port VID

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



Port VID Configuration

Port	Port VID	Forward Only this Vlan	Drop Untagged Frame
All		□	□
Port1	1	☑	□
Port2	1	☑	□
Port3	1	☑	□
Port4	1	☑	□
Port5	1	☑	□
Port6	1	☑	□
Port7	1	☑	□
Port8	1	☑	□
Port9	1	☑	□
Port10	1	☑	□
Port11	1	☑	□
Port12	1	☑	□
Port13	1	☑	□
Port14	1	☑	□
Port15	1	☑	□
Port16	1	☑	□
Port17	1	☑	□

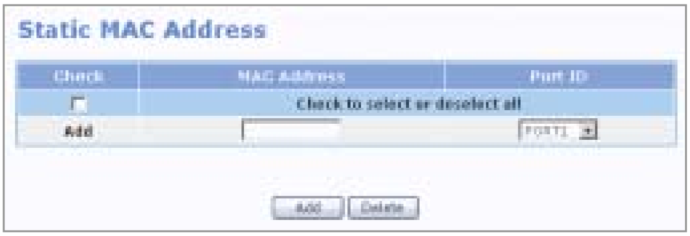
Item	Description
Port VID	VLAN ID for untagged packets.
Forward Only this Vlan	Check this item to drop incoming tagged packets that are not members of VLAN. If the checkboxes are not selected, packets are forwarded to only the VLAN corresponding to the set Port VID.
Drop Untagged Frame	Check this item to drop untagged packets or uncheck this item to retransmit packets only to VLAN corresponding to the designated Port VID.

MAC

The [MAC] menu is used for retrieving the address table of the switch or for setting Filtering MAC.

Static Address

Select [MAC] → [Static Address] to save a MAC address to the address table of a switch regardless of whether the device and switch is physically connected.
That is, a MAC address can be saved in the address table without using learning(MAC address table update), and the MAC address remains in the address table of the switch even if the device is not actually connected to the switch and even after the MAX Aging Time(MAC address table update interval).



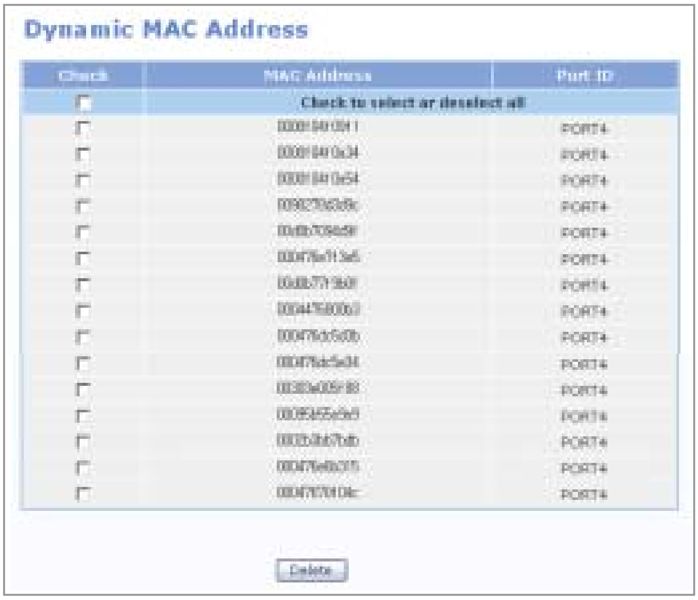
Static MAC Address

Check	MAC Address	Port ID
□	Check to select or deselect all	
Add		PORT1

Enter the MAC address and port No., and click the [Add] button.
Select a MAC address and click the [Delete] button to delete the address.

Dynamic Address

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



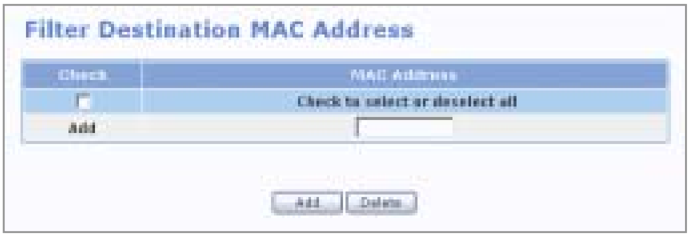
Dynamic MAC Address

Check	MAC Address	Port ID
□	Check to select or deselect all	
□	0009184f0911	PORT4
□	0009184f0a34	PORT4
□	0009184f0e54	PORT4
□	0090275d3d9c	PORT4
□	00d0b7094d9f	PORT4
□	000476e713e6	PORT4
□	00d0b77f3b0f	PORT4
□	000447680063	PORT4
□	000476dc5d0b	PORT4
□	000476dc5e34	PORT4
□	00303a005f08	PORT4
□	00095465e9e9	PORT4
□	0002b3b67bdb	PORT4
□	000476e4b315	PORT4
□	00047670104c	PORT4

Select a MAC address and click the [Delete] button to delete the address.

Filter Address

MAC filtering is used to block unwanted traffic. Select the [Filter Address] menu and enter a MAC address to block the corresponding packet from the switch. The MAC address is the destination address of a packet entering the switch port.



Filter Destination MAC Address

Check	MAC Address
□	Check to select or deselect all
Add	

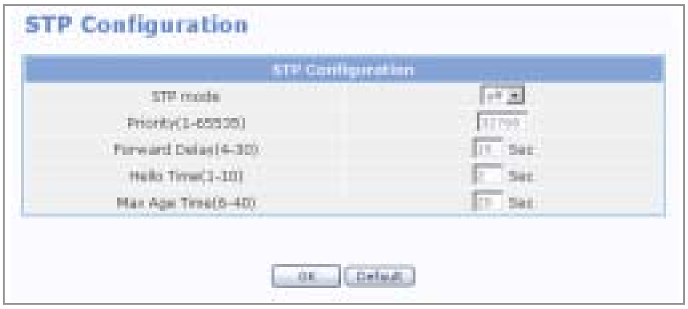
Enter the MAC address and port No. and click the [Add] button.
Select a MAC address and click the [Delete] button to delete the address.

STP

The [STP] menu is used to set the Spanning Tree Protocol(STP) function or to retrieve STP status.

Config

Select [STP] → [Config] to set STP and to prevent switch loop-back.



STP Configuration

STP Configuration

STP mode

Priority(1-65535)

Forward Delay(4-30) Sec

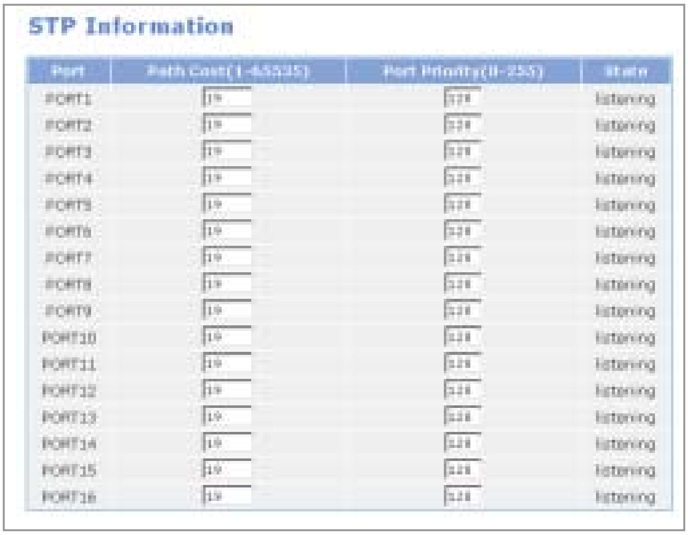
Hello Time(1-10) Sec

Max Age Time(6-40) Sec

Item	Description
STP Mode	Set whether to use STP.
Priority	Set priority for deactivating ports in case switch loop-back occurs.
Forward Delay	In the learning status or in listening status of STP, the status changes to forwarding after waiting for as much time length as set here. (Refer to the [STP] → [Port Config] menu)
Hello Time	Set the transmission interval for STP set messages.
Max Age Time	Set the waiting time for attempting new setup when STP set message is not received.

Port Config

Select [STP] → [Port Config] to set or retrieve STP status.



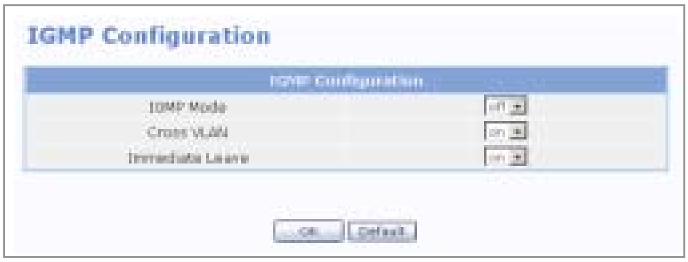
STP Information

Port	Path Cost(1-65535)	Port Priority(0-255)	State
PORT1	19	128	listening
PORT2	19	128	listening
PORT3	19	128	listening
PORT4	19	128	listening
PORT5	19	128	listening
PORT6	19	128	listening
PORT7	19	128	listening
PORT8	19	128	listening
PORT9	19	128	listening
PORT10	19	128	listening
PORT11	19	128	listening
PORT12	19	128	listening
PORT13	19	128	listening
PORT14	19	128	listening
PORT15	19	128	listening
PORT16	19	128	listening

Item	Description
Port	16 switch ports are equipped in all. Select All to process all ports simultaneously.
Path Cost	Set speed according to the speed of each switch port. Set to ‘100’ for 10 Mb/s, and to ‘19’ for 100 Mb/s. The ‘Speed’ value of the ‘Speed/Dpx’ item at the [Switch] → [Port] → [Config] menu is automatically set according to the setting of this item.
Port Priority	Set priority for deactivating ports in case switch loop-back occurs.
State	Indicates the status of each port. - blocking: If a loop occurs on the switch, the corresponding port is blocked and data is no longer sent to the port. - listening: The port is learning the path to the Root Bridge, and can transmit/receive BPDU(frame data for exchanging data between switches). However, the port cannot send data nor update the MAC address table. This status continues for the time length set in the ‘Forward Delay’ item of the <STP Configuration> window. - learning: Similar to ‘listening’, but can exchange BPDU and update the MAC address table. However, data cannot be sent. This status continues for the time length set in the ‘Forward Delay’ item of the <STP Configuration> window. - forwarding: Normal communication is enabled.

IGMP Config

The [IGMP Config] menu is used to efficiently process multicast packets through Internet Group Management Protocol(IGMP) snooping.



IGMP Configuration

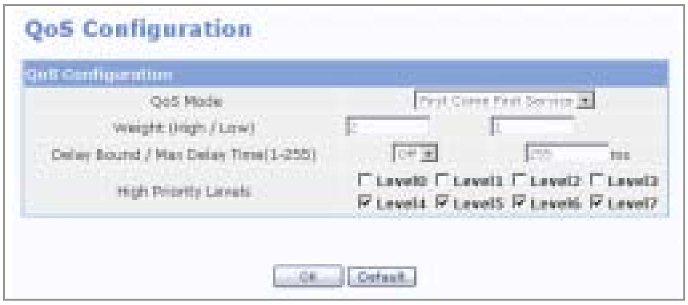
IGMP Configuration

IGMP Mode: off
Cross VLAN: on
Immediate Leave: on

Item	Description
IGMP Mode	Set whether to perform multicasting through IGMP.
Cross VLAN	Set this item to form a multicast group from separate VLANs.
Immediate Leave	Set this item to delete a member from the multicast table upon receiving the IGMPv2 Leave message. This also enables information to be quickly applied to the multicast table when the hosts are directly connected to the switch ports.

QoS Config

The [QoS Config] menu is used for processing QoS by sequentially assigning priority to packets entering the switch or by enforcing priority on a specific port.



QoS Configuration

QoS Configuration

QoS Mode: First Come First Service

Weight (High / Low): 2 / 1

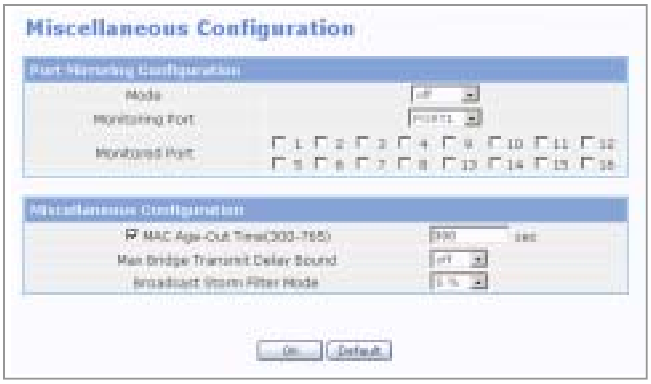
Delay Bound / Max Delay Time(1-255): Off 255 ms

High Priority Levels: □ Level0 □ Level1 □ Level2 □ Level3 ☑ Level4 ☑ Level5 ☑ Level6 ☑ Level7

Item	Description
QoS Mode	Select the QoS mode. - First Come First Service: Packets are sent in the order they arrived.(QoS is not used.) - All High before Low: packets with higher priority are sent ahead of those with lower priority. - Weighted Round Robin: Number of packets are limited to prevent lower priority packets from being over-delayed. For example, setting High weight to ‘5’ and Low weight to ‘2’ will send five higher priority packets before sending two lower priority packets.
Weight	If the user wants to use a ‘Weighted Round Robin’ method, set the ratio of high weight to low weight.
Delay Bound/ Max Delay Time	Time is limited to prevent lower priority packets from being over-delayed when the QoS mode is ‘All High before Low’ or ‘Weighted Round Robin’. The unit of ‘Max Delay Time’ is ms(1/1000 sec) and the initial value is 255 ms. If the waiting time of a lower priority packet exceeds this value, the packet is processed first.
High Priority Levels	There are eight priority levels from Level 0 to Level 7. Level 0 is the lowest priority and Level 7 is the highest. LIM processes priorities by using the two queues: High and Low. The figure above shows the case where high priorities are selected.

MISC Config

The [MISC Config] menu is used for setting the mirroring function and other switching functions.



Miscellaneous Configuration

Port Mirroring Configuration

Mode: off

Monitoring Port: PORT1

Monitored Port: □ 1 □ 2 □ 3 □ 4 □ 9 □ 10 □ 11 □ 12 □ 5 □ 6 □ 7 □ 8 □ 13 □ 14 □ 15 □ 16

Miscellaneous Configuration

☑ MAC Age-Out Time(300-765): 300 sec

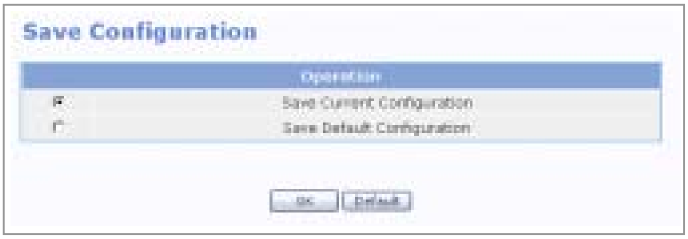
Max Bridge Transmit Delay Bound: off

Broadcast Storm Filter Mode: 5 %

Item	Description
Mode	Set whether to use mirroring. - Off: Do not use mirroring - Tx: Use mirroring for Tx packets - Rx: Use mirroring for Rx packets - Both: Use mirroring for Tx and Rx packets
Monitoring Port	Set the port performing monitoring.
Monitored Port	Set the target port of monitoring. The Monitoring Port may not be designated.
MAC Age-Out Delay Bound	Set the time during which an updated MAC address(Learning) may remain in the address table. Default value is 300 sec. In case of the unmanaged LIM that is not controlled by WIM, if the LAN port is disconnected, the updated MAC address is automatically deleted in 300 seconds. Therefore, the new MAC address is not updated immediately when the LAN port is connected again. In case of the managed LIM(installed into Slot 2) controlled by WIM, if the LAN port is disconnected, the updated MAC address is deleted automatically and immediately. The new MAC address and MAC address table are updated at a fast speed when the LAN port is connected again.
Max Bridge Transmit Delay Bound	Set packet waiting time to Off, 1 sec, 2 sec , or 4 sec.
Broadcast Storm Filter Mode	Select from 5 %, 10 %, 15 %, 20 %, and 25 %. Broadcast packets exceeding this value are lost.

Save Config

The [Save Config] menu is used to save settings to the flash disk. Since settings are basically saved in RAM, the settings will be lost when system is turned off. The settings are saved in the flash disk to prevent the data from being erased during rebooting.



Item	Description
Save Current Configuration	Saves current setting to flash disk. If the system is rebooted without saving the setting, the setting will be lost and will not be applied to the system.
Save Default Configuration	Changes settings in the flash disk to default values. Default values are applied after system rebooting.

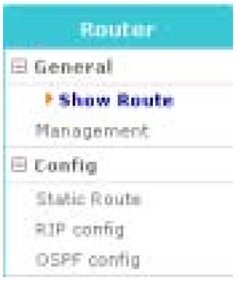
NOTE

Saving or Importing the Switch DB

Click [System] → [DB Config] → [Save/Delete] to save the Switch DB. Click [System] → [DB Config] → [Import/Export] to import the saved DB. Reset the WIM system to import the DB.

Router Menus

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



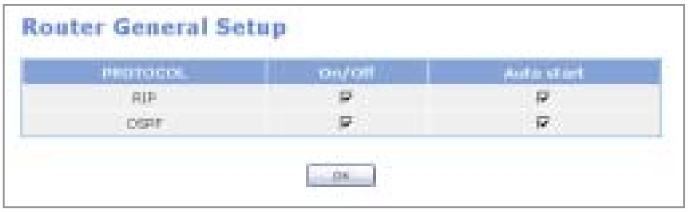
Menu	Submenu	Description
General	Show Route	Displays the routing table of the Data Server.
	Management	Starts or stops RIP and OSPF services, and can set whether to execute the services upon system rebooting.
Config	Static Route	Sets static route.
	RIP config	Sets RIP.
	OSPF config	Sets OSPF.

General

The [General] menu is used for starting or stopping RIP and OSPF services and for retrieving the routing table of the Data Server.

Management

Select [General] → [Management] to start or stop the RIP and OSPF services. Check the ‘Auto Start’ item to start the service automatically when the system is rebooted.

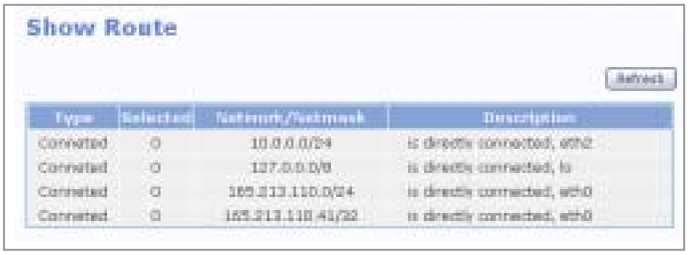


Router General Setup

PROTOCOL	On/Off	Auto start
RIP	☑	☑
OSPF	☑	☑

Show Route

Select [General] → [Show Route] to retrieve the routing table of the Data Server.



Show Route

Type	Selected	Network/Netmask	Description
Connected	O	10.0.0.0/24	is directly connected, eth2
Connected	O	127.0.0.0/8	is directly connected, lo
Connected	O	165.213.110.0/24	is directly connected, eth0
Connected	O	165.213.110.41/32	is directly connected, eth0

Item	Description
Type	- Connected: Network is directly connected to the network interface of the Data Server - RIP: Route data received from other routers through RIP - OSPF: Route data received from other routers through OSPF
Selected	Indicates whether routing is activated
Network/Netmask	Network information on the route
Description	Description on the route

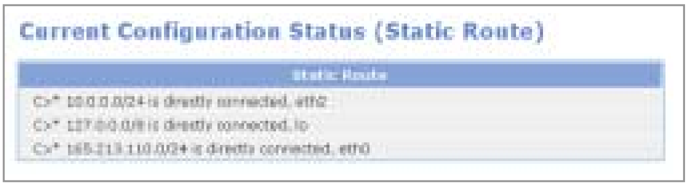
Config

The [Config] menu is used for setting static route, RIP, and OSPF.

Static Route

Select [Config] → [Static Route] to set static route. Set the following items and click the [Save] button:

- Current Configuration Status



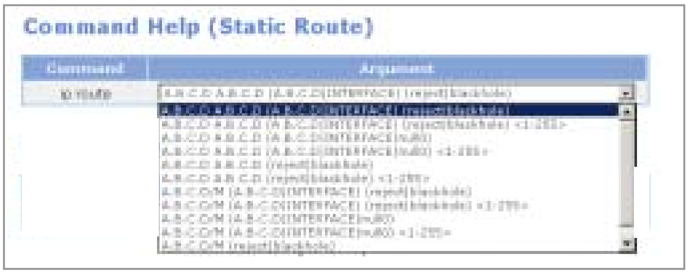
Current Configuration Status (Static Route)

Static Route
C>* 10.0.0.0/24 is directly connected, eth2
C>* 127.0.0.0/8 is directly connected, lo
C>* 165.213.110.0/24 is directly connected, eth0

This window shows the routing table of the Data Server, which is same as that displayed on the window of the [Router] → [General] → [Show Route] menu. However, the above window displays the route type as follows:

Item	Description
C>*	Network route connected to the network interface of the Data Server
O	Route data received from other routers through OSPF
R	Route data received from other routers through RIP
S	Static route set by administrator

- Input Configuration Command
  Select the argument corresponding to the 'ip route' command.
  Clicking the 'Argument' item displays all arguments corresponding to the command. Select an argument from the list.

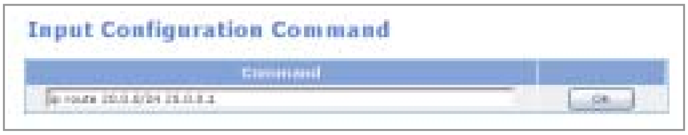


Command Help (Static Route)

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

```
A.B.C.D A.B.C.D (A.B.C.D|INTERFACE) (reject|blackhole)
A.B.C.D A.B.C.D (A.B.C.D|INTERFACE) (reject|blackhole) <1-255>
A.B.C.D A.B.C.D (A.B.C.D|INTERFACE|null0)
A.B.C.D A.B.C.D (A.B.C.D|INTERFACE|null0) <1-255>
A.B.C.D A.B.C.D (reject|blackhole)
A.B.C.D A.B.C.D (reject|blackhole) <1-255>
A.B.C.D/M (A.B.C.D|INTERFACE) (reject|blackhole)
A.B.C.D/M (A.B.C.D|INTERFACE) (reject|blackhole) <1-255>
A.B.C.D/M (A.B.C.D|INTERFACE|null0)
A.B.C.D/M (A.B.C.D|INTERFACE|null0) <1-255>
A.B.C.D/M (reject|blackhole)
```

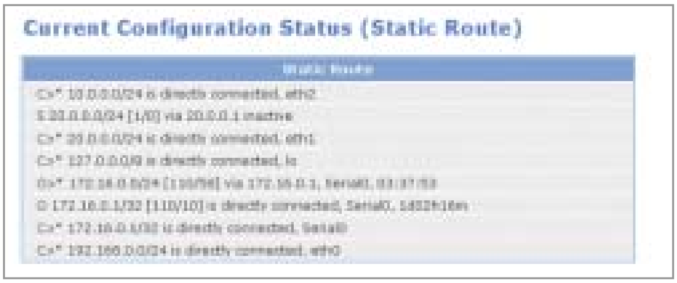
- Input Configuration Command
  Select a command as shown above, or directly enter the static route setup command as shown below:



Input Configuration Command

```
ip route 20.0.0.0/24 20.0.0.1
```

The command execution result is directly applied to the <Current Configuration Status> window of the [Router] → [Config] → [RIP Config] menu. For example, the result of entering the static route command as above is displayed on the <Current Configuration Status> as shown below:



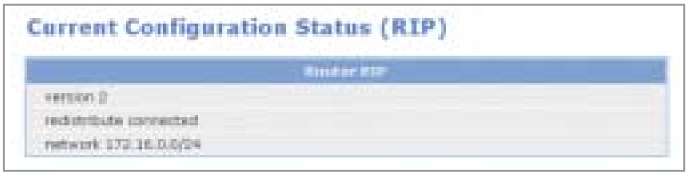
Current Configuration Status (Static Route)

```
C>* 10.0.0.0/24 is directly connected, eth2
S 20.0.0.0/24 [1/0] via 20.0.0.1 inactive
C>* 20.0.0.0/24 is directly connected, eth1
C>* 127.0.0.0/8 is directly connected, lo
O>* 172.16.0.0/24 [110/98] via 172.16.0.1, Serial0, 03:37:53
O 172.16.0.1/32 [110/10] is directly connected, Serial0, 1d02h16m
C>* 172.16.0.1/32 is directly connected, Serial0
C>* 192.168.0.0/24 is directly connected, eth0
```

RIP Config

Select [Config] → [RIP Config] to set RIP. Set the following items and click the [Save] button:

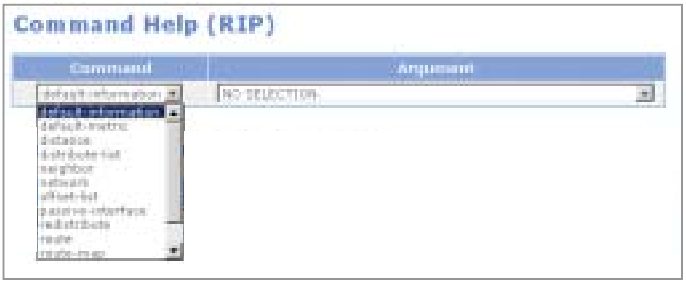
- Current Configuration Status
  This item displays the current RIP status.
  The status is updated when the RIP command entered into the <Input Configuration Command> window of the [Router] → [Config] → [Static Route] menu is executed.



Current Configuration Status (RIP)

```
version 2
redistribute connected
network 172.16.0.0/24
```

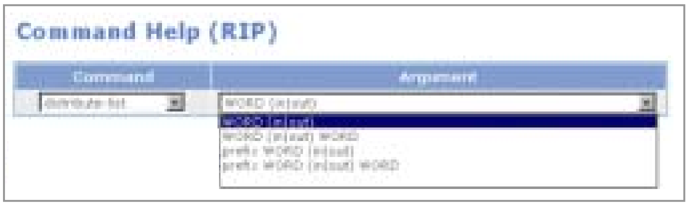
- Command Help
  Select a RIP command from the ‘Command’ item and select an argument for the command from the ‘Argument’ item.



Command Help (RIP)

Command	Argument
default-information	NO SELECTION

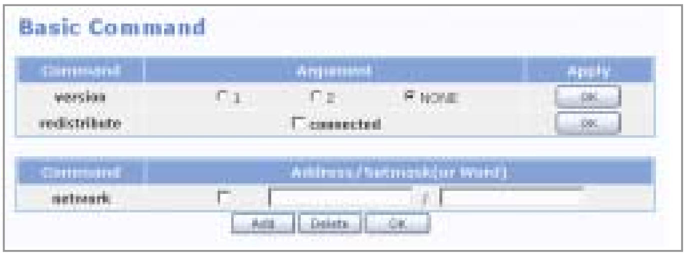
For example, the arguments for the ‘distribute-list’ command are as follows:



Command Help (RIP)

Command	Argument
distribute-list	WORD (in|out)

- Basic Command
  After entering the items, click the [OK] button to display the applied value on the <Current Configuration Status> window.

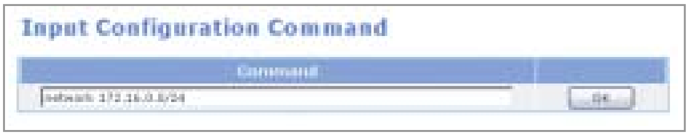


Basic Command

Command	Argument			Apply
version	○ 1	○ 2	● NONE	OK
redistribute		□ connected		OK

Command	Address/Netmask(or Word)
network	□ /

- Input Configuration Command
  Select a command, as if selecting one from the <Command Help(RIP)> window, or directly enter a RIP command and click the [OK] button.



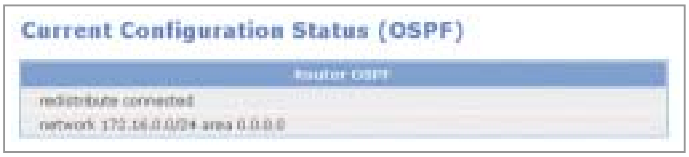
Input Configuration Command

Command	
network 172.16.0.0/24	OK

OSPF Config

Select [Config] → [OSPF Config] to set OSPF. Set the following items and click the [Save] button.

- Current Configuration Status
  This item displays the current OSPF status. The status is updated when the OSPF command entered into the <Input Configuration Command> window of the [Router] → [Config] → [Static Route] menu is executed.

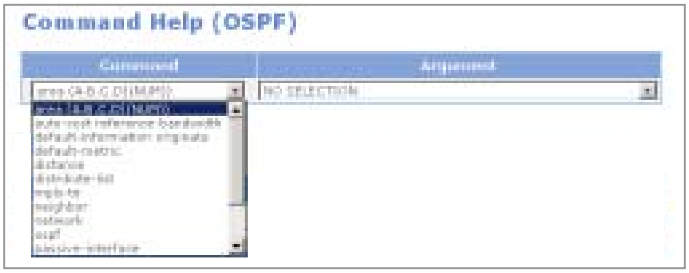


Current Configuration Status (OSPF)

Router OSPF
redistribute connected
network 172.16.0.0/24 area 0.0.0.0

If set as ‘area 0.0.0.0’ as shown above, the information on the route directly connected to the network interface of the Data Server is delivered through ‘network 172.16.0.0’.

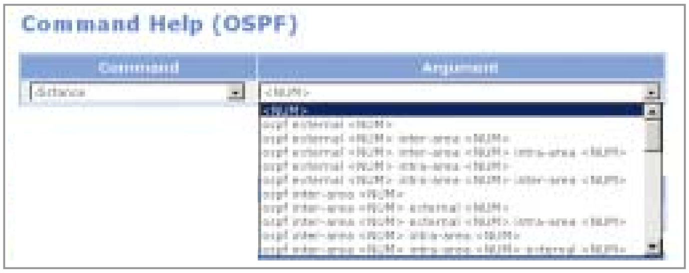
- Command Help
  Select an OSPF command from the ‘Command’ item and select an argument for the command from the ‘Argument’ item.



Command Help (OSPF)

Command	Argument
area (A.B.C.D|<NUM>)	NO SELECTION

For example, the arguments for the ‘distance’ command are as follows:

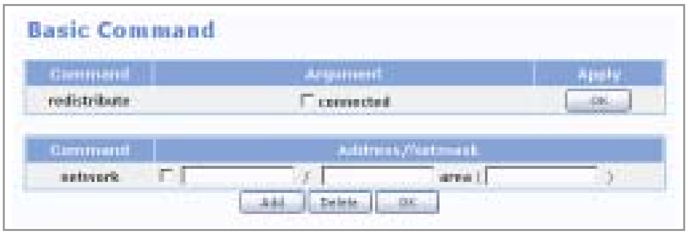


Command Help (OSPF)

Command	Argument
distance	<NUM>

<NUM>
ospf external <NUM>
ospf external <NUM> inter-area <NUM>
ospf external <NUM> inter-area <NUM> intra-area <NUM>
ospf external <NUM> intra-area <NUM>
ospf external <NUM> intra-area <NUM> inter-area <NUM>
ospf inter-area <NUM>
ospf inter-area <NUM> external <NUM>
ospf inter-area <NUM> external <NUM> intra-area <NUM>
ospf inter-area <NUM> intra-area <NUM>
ospf inter-area <NUM> intra-area <NUM> external <NUM>

- Basic Command
  After entering the items, click the [OK] button to display the applied value on the <Current Configuration Status> window.

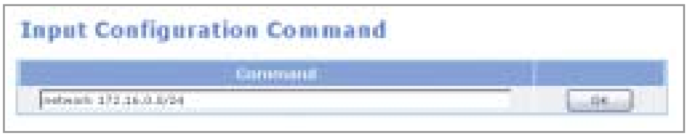


Basic Command

Command	Argument	Apply
redistribute	□ connected	OK

Command	Address/Netmask
network	□ [ ] / [ ] area [ ])

- Input Configuration Command
  Select a command, as if selecting one from the <Command Help(RIP)> window, or directly enter a OSPF command and click the [OK] button.

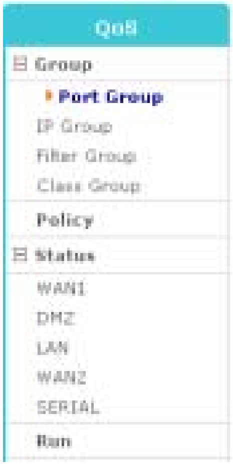


Input Configuration Command

Command	
network 172.16.0.0/24	OK

QoS Menus

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



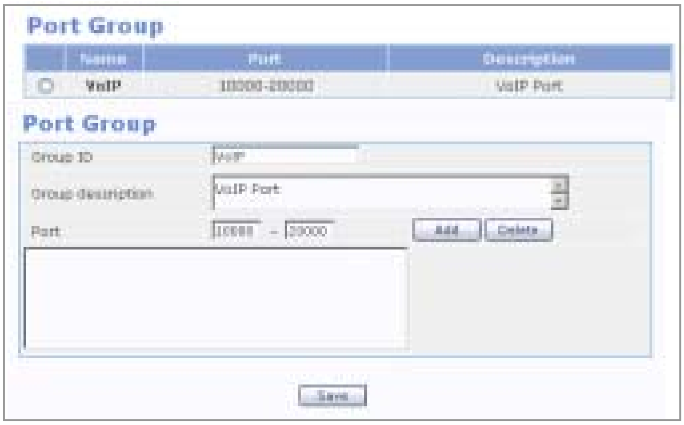
Menu	Submenu	Description
Group	Port Group	Retrieves, sets, edits, or deletes a port group
	IP Group	Retrieves, sets, edits, or deletes an IP group
	Filter Group	Retrieves, sets, edits, or deletes a filter group
	Class Group	Retrieves, sets, edits, or deletes a class group
Policy	-	Sets a class for a port
Status	-	Displays QoS class and filter data of a port in a tree structure
Run	-	Starts or stops the execution of a QoS and can set whether to automatically execute the QoS when the system is rebooted

Group

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

Port Group

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



Port Group

	Name	Port	Description
○	VoIP	10000-20000	VoIP Port

Port Group

Group ID: VoIP

Group description: VoIP Port

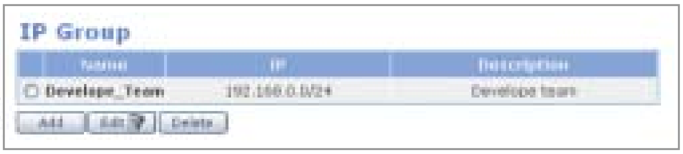
Port: 10000 - 20000

Click the [Add] button in the above window to display a window from which a port group can be set. Enter the group ID, group description, and port number, click the [Add] button, and click the [Save] button.

Item	Description
Group 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.
Group description	Description on the port group
Port	Range of ports Enter ‘0’ to set all ports.

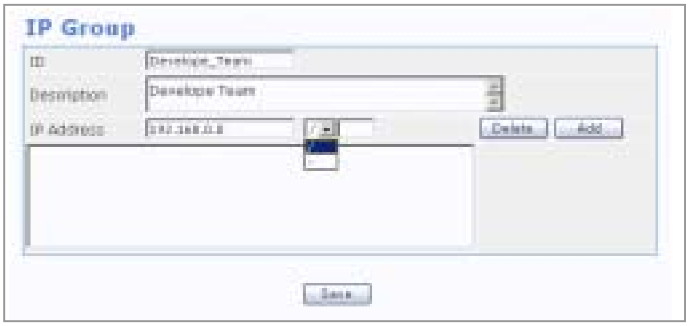
IP Group

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



	Name	IP	Description
○	Develope_Team	192.168.0.0/24	Develope team

Click the [Add] button in the above window to display a window from which an IP group can be set. Enter the group ID, group description, and port number, click the [Add] button, and click the [Save] button.



ID: Develope_Team

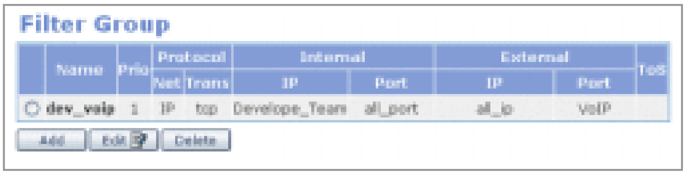
Description: Develope Team

IP Address: 192.168.0.0 /

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.
Group description	Description on the IP group
IP Address	IP address /: Used for entering subnet -: Used for entering the range of IPs Enter ‘0.0.0.0/0’ to set all ports.

Filter Group

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

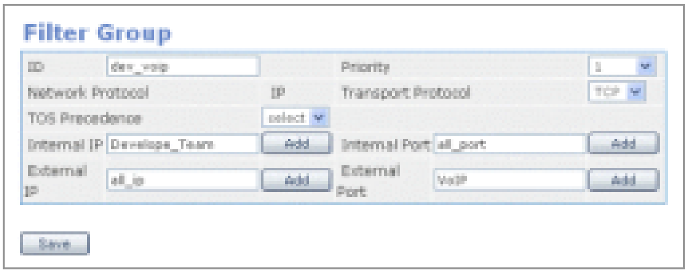


Filter Group

	Name	Prio	Protocol		Internal		External		ToS
			Net	Trans	IP	Port	IP	Port	
○	dev_voip	1	IP	tcp	Develope_Team	all_port	all_ip	VoIP	

If ‘dev_voip’ is registered as the filter group as shown above, the filtering rule is as follows: The Internal and External items represent information set at the [Port Group] menu and the [IP Group] menu. 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 click the [Save] button. Clicking the [Add] button displays a list of port groups and IP groups. Select the IP and port from the list.



Filter Group

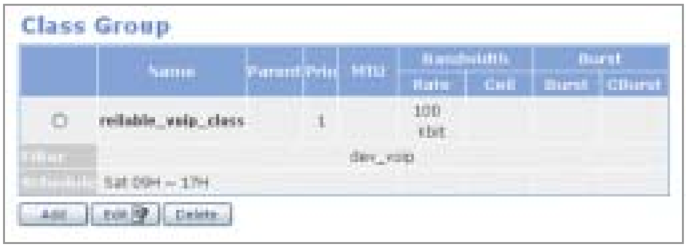
ID: dev_voip
Priority: 1
Network Protocol: IP
Transport Protocol: TCP
TOS Precedence: select
Internal IP: Develope_Team
Internal Port: all_port
External IP: all_ip
External Port: VoIP

Setting a filter means setting a rule for filtering the values in the packet header. Values set at the [QoS] → [Group] → [Port Group] menu and the [IP Group] menu are used, and protocols and TOS fields can also be filtered. In addition, priorities can be set for the filters to apply the filtering rules according to the priority.

The Internal IP, Port and External IP, Port are mandatory items and must be entered. If these items are not entered, an error message will appear.

Class Group

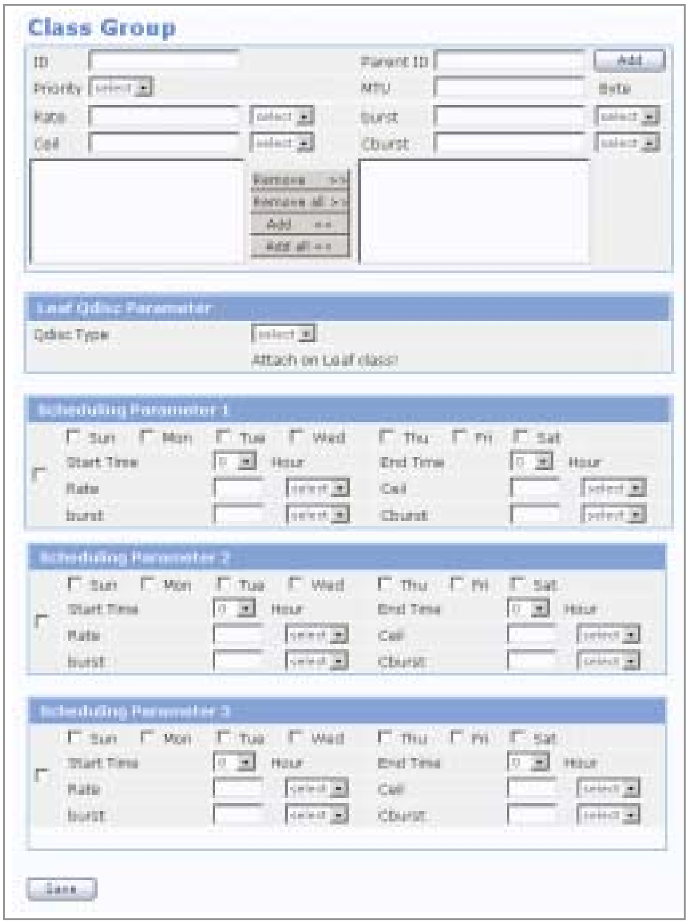
Select [Class Group] to retrieve, set, edit, or delete a class group. A class includes information on the defined filtering rule and the bandwidth that should be assigned to the filtered traffic.



Class Group

	Name	Parent	Prio	MTU	Bandwidth		Burst	
					Rate	Ceil	Burst	Cburst
○	reliable_voip_class		1		100 kbit			
Filter	dev_voip							
Schedule	Sat 09H ~ 17H							

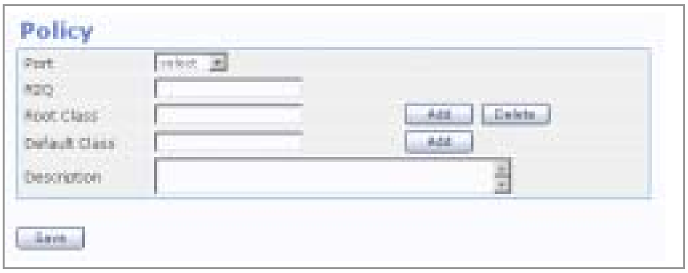
Click the [Add] button in the <Class Group> window to display a window from which a class group can be set. Set the items and click the [Save] button.



Item	Description
Parent ID	Due to the hierarchical characteristic of QoS, classes are classified into the root class(highest level class) and the leaf class(lowest level class) and into the parent class and the child class. 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 the default class(class including the bandwidth for traffics that do not belong to a filter).
Priority	If several classes compete to occupy leftover bandwidths or if all classes attempt to occupy excess bandwidth, set the priority so that the class with the highest priority occupies the bandwidth first.
MTU	The Maximum Transmit Unit(MTU) represents the maximum amount of packets that can be transmitted at a time. It is recommended that this setting 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. Up to three scheduling parameter can be set.

Policy

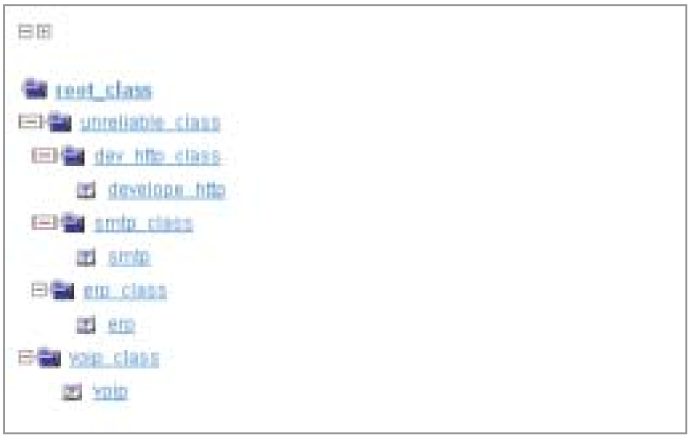
The [Policy] menu is used for setting a class for a port. Enter the following items and click the [Save] button to select a class for a port.



Item	Description
Port	Select a port(select WAN1, DMZ, LAN, WAN2, or SERIAL)
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. Click the [Add] button and 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. Click the [Add] button and select the class group from the class group list.

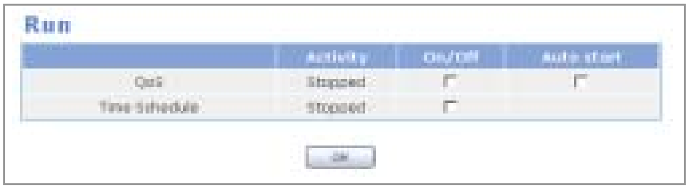
Status

The [Status] menu is used for displaying the class and filters assigned to each port in a tree structure.



Run

The [Run] menu is used to start or stop the execution of a QoS. Execution of the ‘Scheduling Parameter’ set at the [QoS] → [Group] → [Class Group] menu can also be started or stopped. Clicking the ‘Auto start’ item will automatically start the QoS service when the system is rebooted.

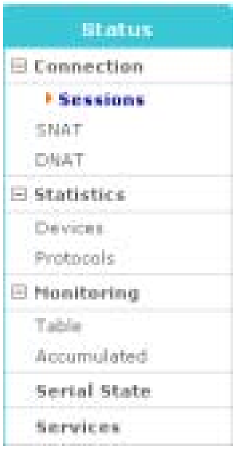


Run

	Activity	On/Off	Auto start
QoS	Stopped	□	□
Time Schedule	Stopped	□	

Status Menus

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



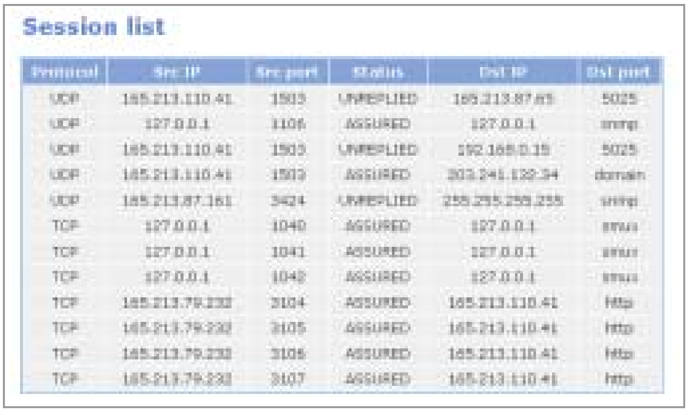
Menu	Submenu	Description
Connection	Sessions	Displays IPs and ports connected to the Data Server.
	SNAT	Displays the connection status of SNAT.
	DNAT	Displays the connection status of DNAT.
Statistics	Devices	Displays the network statistics of the Data Server for each device and for Tx and Rx.
	Protocols	Displays the network statistics of the Data Server for each protocol.
Monitoring	Table	Displays the Data Server network statistics in a table format and in real time.
	Accumulated	Displays the Data Server network statistics in values accumulated yearly, monthly, weekly, and hourly.
Services	-	Various functions of the Data Server are categorized into Security, Router, and Management, and the statuses of services are displayed in a table format.

Connection

The [Connection] menu displays the connection status of the Data Server, SNAT, and DNAT.

Sessions

The [Sessions] menu displays information on IPs and ports connected to the Data Server.



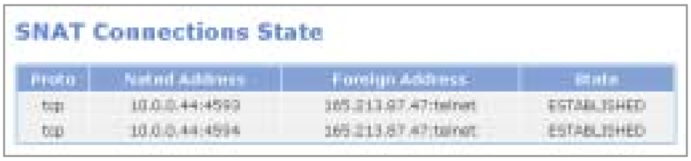
Session list

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 protocol used for session connection(UDP, TCP)
Src IP	Source IP
Src Port	Source port
Status	- UNREPLIED: No response packets found on received packets that should requires response - ASSURED: Response packet has occurred('UNREPLIED' changes to 'ASSURED')
Dst IP	Destination IP
Dst Port	Destination port

SNAT

The [SNAT] menu displays the connection status of SNAT.

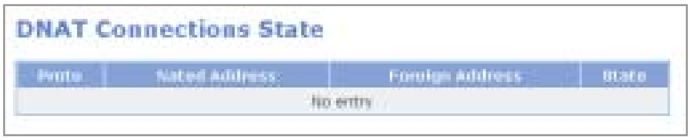


SNAT Connections State

Proto	Nated Address	Foreign Address	State
tcp	10.0.0.44:4593	165.213.87.47:telnet	ESTABLISHED
tcp	10.0.0.44:4594	165.213.87.47:telnet	ESTABLISHED

DNAT

The [DNAT] menu displays the connection status of DNAT.



DNAT Connections State

Proto	Nated Address	Foreign Address	State
No entry			

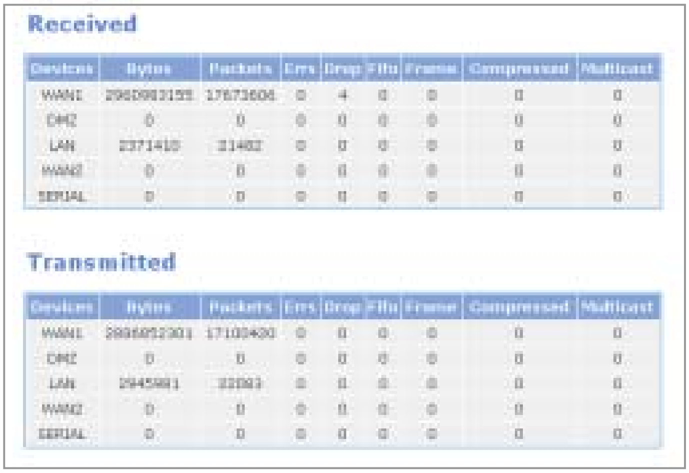
Item	Description
Proto	Protocol type(UDP, TCP)
Nated Address	User IP address
Foreign Address	IP address of the connected user
State	Current status

Statistics

The [Statistics] menu displays the network statistics of the Data Server for each device and for each protocol.

Devices

Select [Statistics] → [Devices] to display the network statistics of Data Server on received data and on transmitted data for each device.



Received

Devices	Bytes	Packets	Errs	Drop	Fifo	Frame	Compressed	Multicast
WAN1	2960983155	17673606	0	4	0	0	0	0
DMZ	0	0	0	0	0	0	0	0
LAN	2371410	21482	0	0	0	0	0	0
WAN2	0	0	0	0	0	0	0	0
SERIAL	0	0	0	0	0	0	0	0

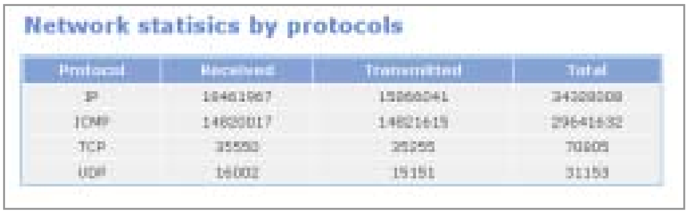
Transmitted

Devices	Bytes	Packets	Errs	Drop	Fifo	Frame	Compressed	Multicast
WAN1	2936852301	17100430	0	0	0	0	0	0
DMZ	0	0	0	0	0	0	0	0
LAN	2945981	22093	0	0	0	0	0	0
WAN2	0	0	0	0	0	0	0	0
SERIAL	0	0	0	0	0	0	0	0

Item	Description
Devices	Port type
Bytes	Total bytes received or transmitted
Packets	Total packets received or transmitted
Errs	Number of errored packets
Drop	Number of dropped packets
Fifo	FIFO queue is full(FIFO overrun)
Frame	Ethernet header type is invalid(Frame Alignment Error)
Compressed	Number of compressed packets
Multicast	Number of multicast packets

Protocols

Select [Statistics] → [Protocols] to display the network statistics of the Data Server for each protocol.(Unit: Byte)



Network statisics by protocols

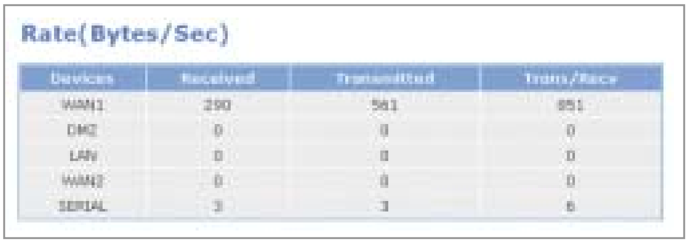
Protocol	Received	Transmitted	Total
IP	16461967	15866041	34328008
ICMP	14820017	14821615	29641632
TCP	35550	35255	70805
UDP	16002	15151	31153

Monitoring

The [Monitoring] menu is used for displaying the network statistics of the Data Server in real time or in values accumulated during a certain period.

Table

Select [Monitoring] → [Table] to display the network statistics of the Data Server in real time. Data is updated every 5 seconds.

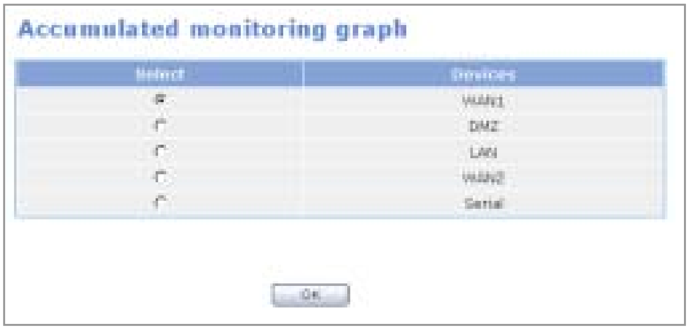


Rate(Bytes/Sec)

Devices	Received	Transmitted	Trans/Recv
WAN1	290	561	851
DMZ	0	0	0
LAN	0	0	0
WAN2	0	0	0
SERIAL	3	3	6

Accumulated

Select [Monitoring] → [Accumulated] to display the Data Server network statistics in values accumulated yearly, monthly, weekly, and hourly.



Accumulated monitoring graph

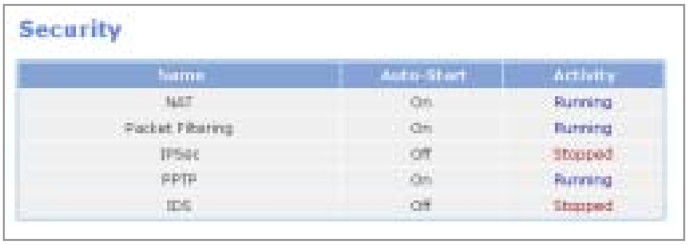
Select	Devices
●	WAN1
○	DMZ
○	LAN
○	WAN2
○	Serial

Services

The [Services] menu is used to display the statuses of security, router, and management services, provided by the Data Server, in a table format.
If the 'Auto Start' item is checked 'On', the service will be started automatically when the system is rebooted. The 'Activity' item is set to 'Running' when the service is being provided, and is set to 'Stopped' when the service is not being provided.

Security

This item displays the current status of security services.

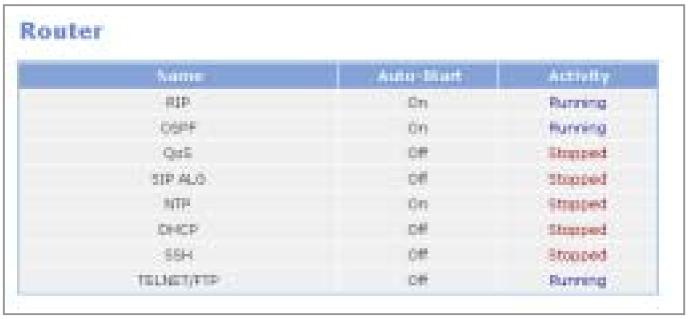


Security

Name	Auto-Start	Activity
NAT	On	Running
Packet Filtering	On	Running
IPSec	Off	Stopped
PPTP	On	Running
IDS	Off	Stopped

Router

This item displays the current status of router services.

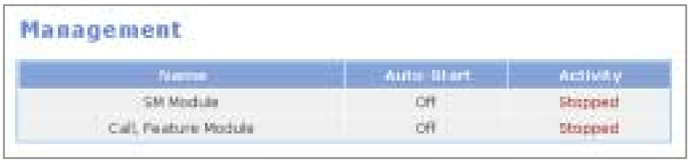


Router

Name	Auto-Start	Activity
RIP	On	Running
OSPF	On	Running
QoS	Off	Stopped
SIP ALG	Off	Stopped
NTP	On	Stopped
DHCP	Off	Stopped
SSH	Off	Stopped
TELNET/FTP	Off	Running

Management

This item displays the current status of management services.

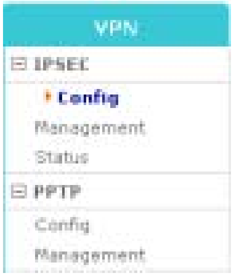


Management

Name	Auto-Start	Activity
SM Module	Off	Stopped
Call, Feature Module	Off	Stopped

VPN Menu

Select [VPN] to display the submenus of VPN on the upper left section of the window.



Menu	Submenu	Description
IPSEC	Config	Sets IPSEC.
	Management	Allows/Inhibits execution of IPSEC. Sets whether to execute IPSEC when the system reboots.
	Status	Checks if IPSEC tunnel is properly connected.
PPTP	Config	Sets PPTP.
	Management	Allows/Inhibits execution of PPTP. Sets whether to execute PPTP when the system reboots.

NOTE

Setting VPN Client in Windows XP/2000

Setting 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 ‘ANNEX A’.

IPSEC

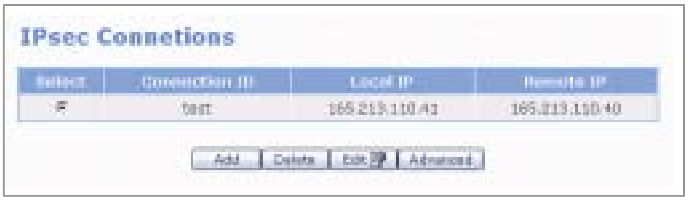
IP Security Protocol(IPSEC) provides security services in the IP layer through implementing Internet Key Exchange(IKE). The security service is categorized into two services depending on remote equipment: the services providing security tunnels between local subnet and remote subnet, and between local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

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

Since IPSEC setting requires a couple of gateways for a security tunnel, local setting and remote setting have the same item.

Config

Users are allowed to add, delete, and search an IPSEC tunnel on the [IPSEC] → [Config] menu, and to set detailed items.



IPsec Connetions

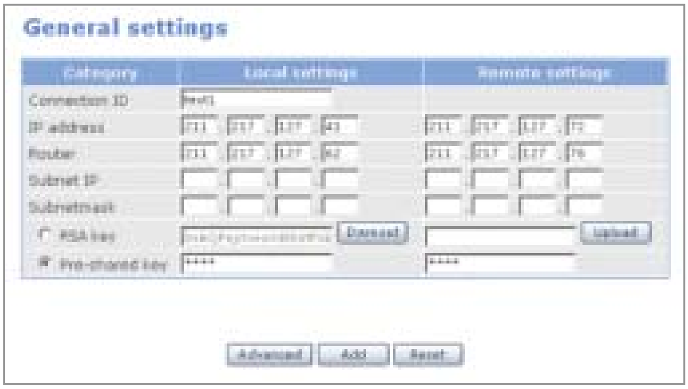
Select	Connection ID	Local IP	Remote IP
☑	test	165.213.110.41	165.213.110.40

The menu buttons are defined as shown below:

Button	Description
Add	Creates IPSEC tunnel
Delete	Deletes IPSEC tunnel
Edit	Modifies IPSEC tunnel data
Advanced	Sets detailed items of IPSEC tunnel

Add

Click the [Add] button from the <Ipsec Connections> window to display the window below: Enter each item value and click the [Add] button to add an IPSEC tunnel.



General settings

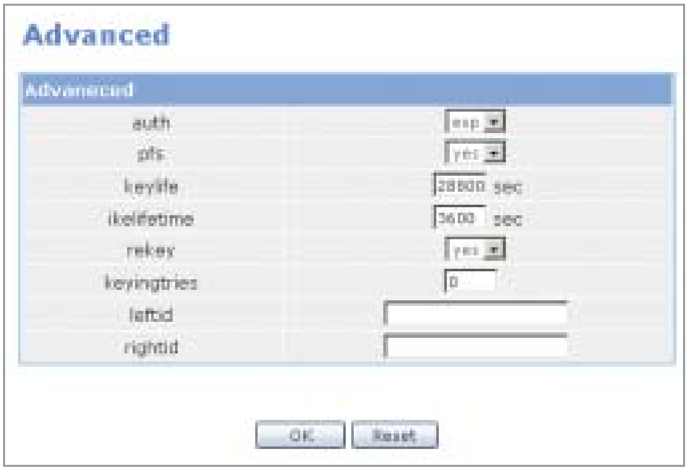
Category	Local settings	Remote settings
Connection ID	[illegible]	
IP address	211 . 217 . 127 . 41	211 . 217 . 127 . 72
Router	211 . 217 . 127 . 62	211 . 217 . 127 . 76
Subnet IP	. . .	. . .
Subnetmask	. . .	. . .
○ RSA key	[illegible] Download	Upload
● Pre-shared key	****	****

Category	Description
Connection ID	ID composed of certain letters(Required)
IP Address	External IP address(Required)
Router	Router IP address
Subnet IP	Internal IP address
Subnetmask	Internal subnetmask
RSA Key/ Preshared Key	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.

If the ‘Router’ item value 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.

Advanced

Click the [Advanced] button from the <Ipsec Connections> window to display the window below: Detailed items of IPSEC can be set.



Advanced

Advanced

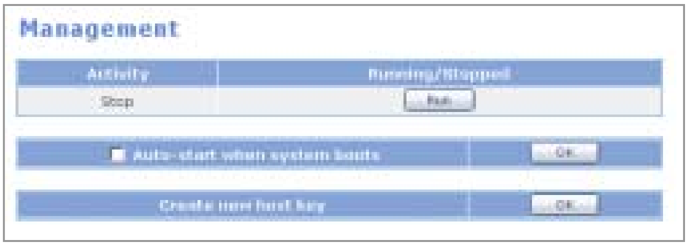
auth	esp
pfs	yes
keylife	28800 sec
ikelifetime	3600 sec
rekey	yes
keyingtries	0
leftid	
rightid	

Item	Description
auth	Select packet authentication protocol. - Authentication Header(AH): Allows data sender authentication. - Encapsulating Security Payload(ESP): Allows sender authentication and data encryption.
pfs	Select whether to use security of completion key.
keylife	Cycle of newly added key used in packet encryption through repeated IKE 2 level
ikelifetime	IKE duration time If duration time passes, host authentication(IKE 1 level) is performed again.
rekey	Set whether to add a new key(whether to add a new key and negotiate again in the IKE 2 level).
keyingtries	Retry count of key exchange when encryption key exchange fails in the IKE 2 level
leftid	Set ID if ID as well as IP address is required. Typically, IP address is used for authenticating other host in the IKE 1 level.
rightid	Set ID if ID as well as IP address is required. Typically, IP address is used for authenticating other host in the IKE 1 level.

Each item uses default value. Users are allowed to edit the value of Pfs or Keylife for mutual operation with other equipment. If ‘Letfid’ and ‘Rightid’ are not set, IP address will be used as the ‘Letfid’ and ‘Rightid’.

Management

The user allows/inhibits executing IPSEC services on the [IPSEC] → [Management] menu. Check the 'Auto-start when system boots' item, and click the [OK] button to execute the IPSEC services automatically while the system reboots.



Management

Activity	Running/Stopped
Stop	Run

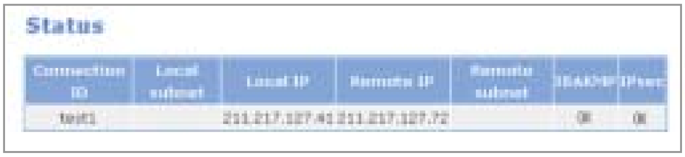
□ Auto-start when system boots | OK

Create new host key | OK

Click the [OK] button of the 'Create new host 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.

Status

Users are allowed to check if the target IPSEC tunnel is connected properly on the [IPSEC] → [Status] menu.



Status

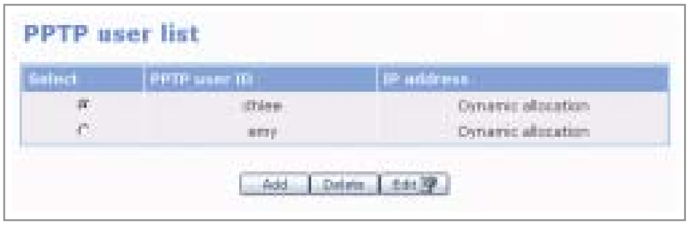
Connection ID	Local subnet	Local IP	Remote IP	Remote subnet	ISAKMP	IPsec
test1		211.217.127.41	211.217.127.72		●	●

PPTP

Users are allowed to set the security tunnel between local subnet and remote host easily through Point to Point Tunneling Protocol(PPTP). Since PPTP setting is convenient compared with IPSEC and the S/W provided by Windows OS exits, the user can use VPN functions easily.

Config

Users are allowed to add, edit, delete, and search VPN tunnel data on the [PPTP] → [Config] menu, and to set detailed items.



PPTP user list

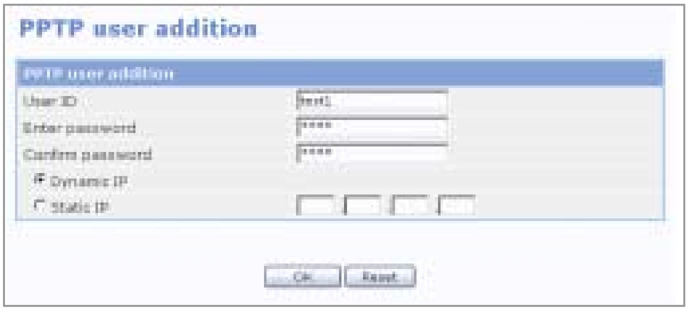
Select	PPTP user ID	IP address
●	chlee	Dynamic allocation
○	amy	Dynamic allocation

The menu buttons are defined as shown below:

Button	Description
Add	Create PPTP tunnel
Delete	Delete PPTP tunnel
Edit	Modify PPTP tunnel data

Add

Click the [Add] button from the <PPTP user list> window. Enter each item value and click the [OK] button to add a VPN tunnel.



PPTP user addition

PPTP user addition

User ID: test1

Enter password: ****

Confirm password: ****

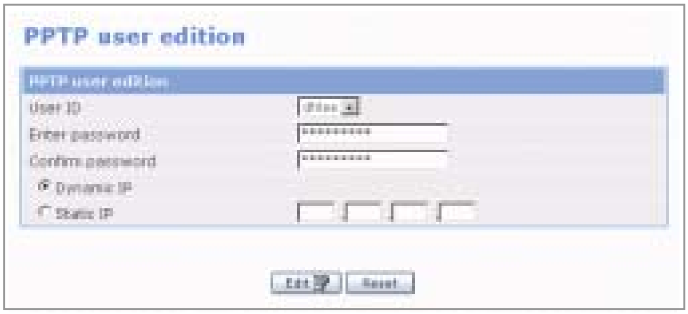
● Dynamic IP

○ Static IP

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

Edit

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



PPTP user edition

PPTP user edition

User ID: [illegible]

Enter password: **********

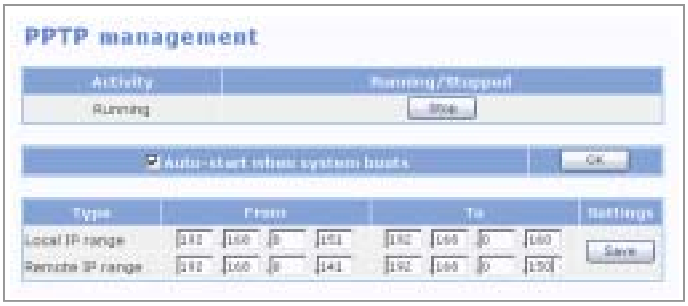
Confirm password: **********

● Dynamic IP

○ Static IP

Management

The user allows/inhibits executing PPTP services on the [PPTP] → [Management] menu. Check the ‘Auto-start when system boots’ item and click the [OK] button to execute the PPTP services automatically while the system reboots.



PPTP management

Activity	Running/Stopped
Running	Stop

☑ Auto-start when system boots OK

Type	From				To				Settings
Local IP range	192	168	0	151	192	168	0	160	Save
Remote IP range	192	168	0	141	192	168	0	150	

Users are allowed to set the IP range of the remote client that uses dynamic IP in the ‘Local IP range’ item, and set the IP range of PPP daemon responsible for remote client in the ‘Remote IP range’ item.

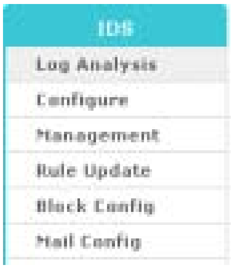
CAUTION

Setting 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.

IDS Menu

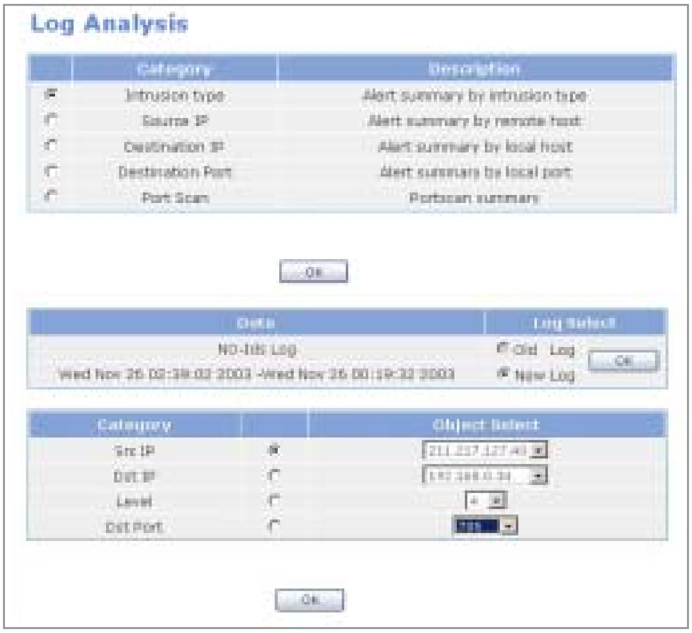
Select [IDS] to display the submenus of IDS on the upper left section of the window.



Menu	Description
Log Analysis	Analyzes logs detected by IDS rule.
Configure	Sets whether to apply Config file and Rule file before executing IDS.
Management	Allows/Inhibits IPSEC implementation. Set IPSEC to be executed when the system reboots.
Rule Update	Updates new rules downloaded from the Web.
Block Config	Sets Source IP detected by IDS to be blocked by a firewall.
Mail Config	Sets to send IDS message when IDS detects.

Log Analysis

Analyze the logs detected by Intrusion Detection System(IDS) rule on the [Log Analysis] menu. Select the target Category to be analyzed, and click the [OK] button to display the corresponding log analysis for the category.



Log Analysis

	Category	Description
●	Intrusion type	Alert summary by intrusion type
○	Source IP	Alert summary by remote host
○	Destination IP	Alert summary by local host
○	Destination Port	Alert summary by local port
○	Port Scan	Portscan summary

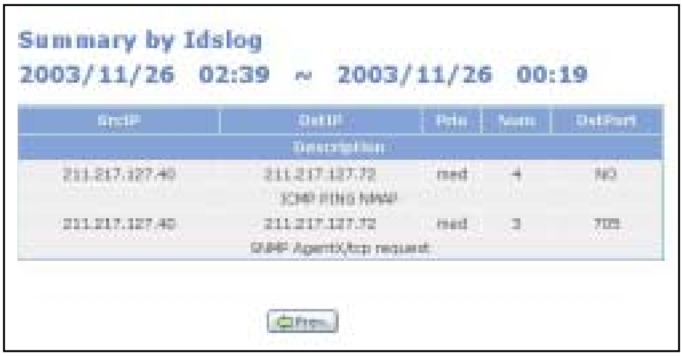
Date	Log Select
NO-Ids Log Wed Nov 26 02:39:02 2003 -Wed Nov 26 00:19:32 2003	○ Old Log ● New Log

Category		Object Select
Src IP	●	211.237.127.4[illegible]
Dst IP	○	192.168.0.34
Level	○	4
Dst Port	○	[illegible]

Category	Item	Description
Category	Intrusion type	Analyzes logs detected for IDS rule types.
	Source IP	Analyzes logs for Source IP detected by IDS.
	Destination IP	Analyzes logs, detected by IDS, of the OfficeServ 7200 external IP(WAN1, WAN2, SERIAL).
	Destination Port	Analyzes logs when the destination IP of a log detected by IDS is the port of an external IP(WAN1, WAN2, SERIAL).
	Port Scan	Analyzes the logs if the logs detected by IDS have port scan type.
Date	-	Time to record a log
Log Select	Old Log	Analyzes old logs.
	New Log	Analyzes the IDS log based on the latest log.

Select ‘Old Log’ and click [OK] to analyze old logs. Then, data on the old logs will be displayed in ‘Object Select’.
Select ‘New Log’ and click [OK] to analyze the latest logs. Then, data on the latest logs will be displayed in ‘Object Select’.
The default is ‘New Log’. If an IDS log does not exist, the ‘NO-Ids Log’ message will be displayed.

Select ‘Old Log’ or ‘New Log’ from the <Log Analysis> window and then, select an option from ‘Object Select’. Then, click [OK] to analyze the log and display the results. The window below shows the results of analyzing the log for Src IP(211.217.127.40).



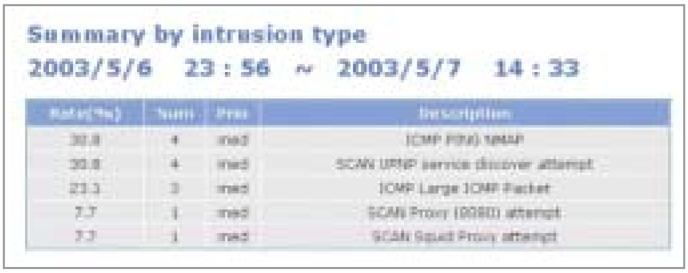
Summary by Idslog
2003/11/26 02:39 ~ 2003/11/26 00:19

<table>
<tr><th>SrcIP</th><th>DstIP</th><th>Prio</th><th>Num</th><th>DstPort</th></tr>
<tr><th colspan="5">Description</th></tr>
<tr><td>211.217.127.40</td><td>211.217.127.72</td><td>med</td><td>4</td><td>NO</td></tr>
<tr><td colspan="5">ICMP PING NMAP</td></tr>
<tr><td>211.217.127.40</td><td>211.217.127.72</td><td>med</td><td>3</td><td>705</td></tr>
<tr><td colspan="5">SNMP AgentX/tcp request</td></tr>
</table>

Item	Description
SrcIP	Displays the source IP of the detected log, which is the attacker IP address.
DstIP	Displays the destination IP of the detected log, which is the attacked IP address.
Prio	Risk level depending on the rules level of IDS - High: Rule level is one day(the highest risk level) - Med: Rule level is 2 or 3 days(mid level) - Low: Rule level is 4 days(low level)
Num	Displays the count of attacks whose types are displayed in ‘Description’.
DstPort	Displays the destination IP.
Description	Displays attack types.

Intrusion type

Check ‘Intrusion type’ from the Category item of the <Log Analysis> window, and click the [OK] button to display the log analysis window below: Date indicates the time from the first detection to the last detection.



Summary by intrusion type

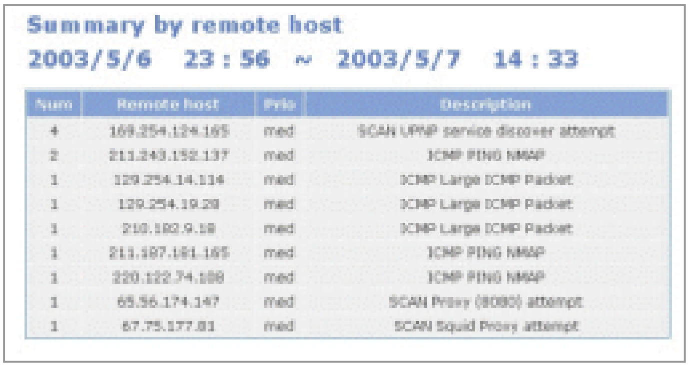
2003/5/6 23 : 56 ~ 2003/5/7 14 : 33

Rate(%)	Num	Prio	Description
30.8	4	med	ICMP PING NMAP
30.8	4	med	SCAN UPNP service discover attempt
23.1	3	med	ICMP Large ICMP Packet
7.7	1	med	SCAN Proxy (8080) attempt
7.7	1	med	SCAN Squid Proxy attempt

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

Source IP

Check ‘Source IP’ from the Category item of the <Log Analysis> window, and click the [OK] button to display the log analysis window below: Date indicates the time from the first detection to the last detection.



Summary by remote host

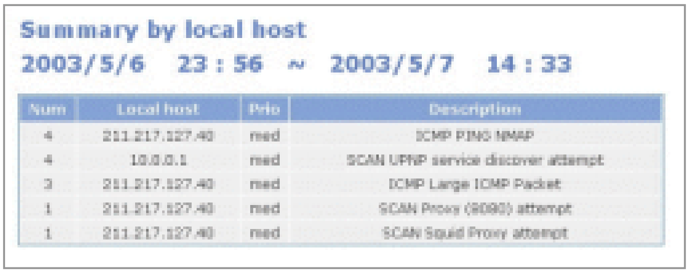
2003/5/6 23 : 56 ~ 2003/5/7 14 : 33

Num	Remote host	Prio	Description
4	169.254.124.165	med	SCAN UPNP service discover attempt
2	211.243.152.137	med	ICMP PING NMAP
1	129.254.14.114	med	ICMP Large ICMP Packet
1	129.254.19.28	med	ICMP Large ICMP Packet
1	210.182.9.18	med	ICMP Large ICMP Packet
1	211.187.181.165	med	ICMP PING NMAP
1	220.122.74.188	med	ICMP PING NMAP
1	65.56.174.147	med	SCAN Proxy (8080) attempt
1	67.75.177.81	med	SCAN Squid Proxy attempt

Item	Description
Num	Number of logs detected by IDS for Source IP attacking the logs
Remote host	Host IP attacking logs detected by IDS
Prio	Risk level depending on the rules level of IDS - High: Rule level is one day(the highest risk level) - Med: Rule level is 2 or 3 days(mid level) - Low: Rule level is 4 days(low level)
Description	Type of logs detected by IDS

Destination IP

Check ‘Destination IP’ from the Category item of the <Log Analysis> window, and click the [OK] button to display the log analysis window below: Date indicates the time from the first detection to the last detection.



Summary by local host

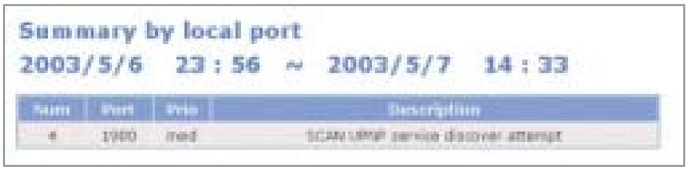
2003/5/6 23 : 56 ~ 2003/5/7 14 : 33

Num	Local host	Prio	Description
4	211.217.127.40	med	ICMP PING NMAP
4	10.0.0.1	med	SCAN UPNP service discover attempt
3	211.217.127.40	med	ICMP Large ICMP Packet
1	211.217.127.40	med	SCAN Proxy (8080) attempt
1	211.217.127.40	med	SCAN Squid Proxy attempt

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

Destination Port

Check ‘Destination Port’ from the Category item of the <Log Analysis> window, and click the [OK] button to display the log analysis window below: Date indicates the time from the first detection to the last detection.



Summary by local port

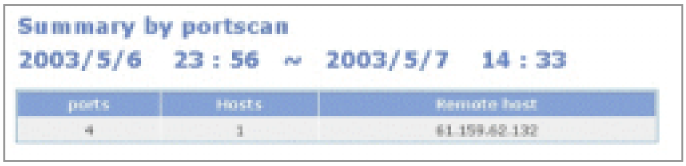
2003/5/6 23 : 56 ~ 2003/5/7 14 : 33

Num	Port	Prio	Description
4	1900	med	SCAN UPNP service discover attempt

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

Port Scan

Check ‘Port Scan’ from the Category item of the <Log Analysis> window and click the [OK] button to display the Log Analysis window below: Date indicates the time from the first detection to the last detection.



Summary by portscan

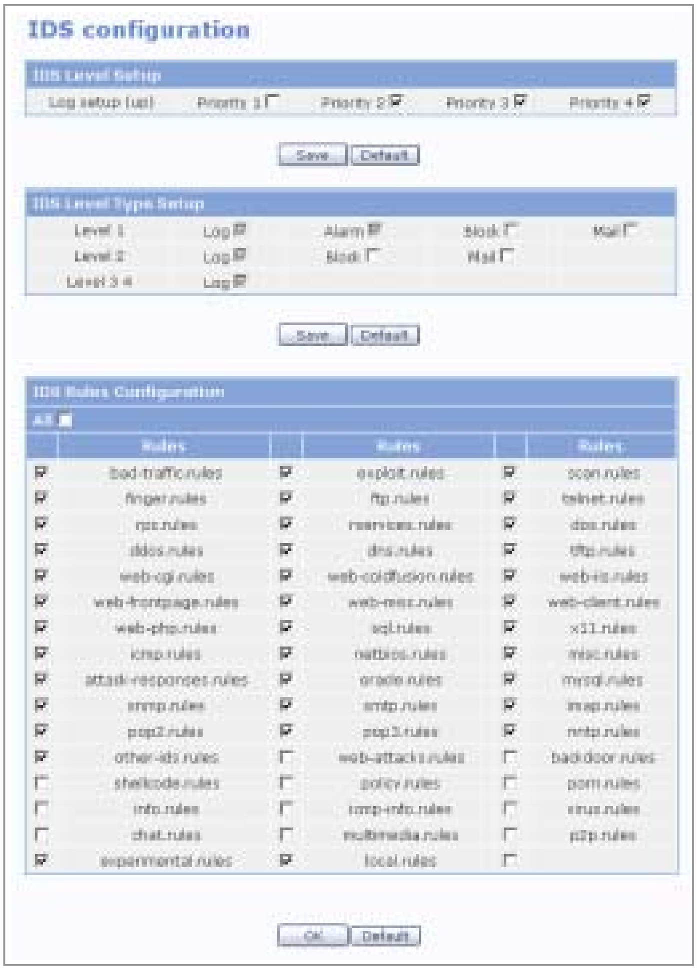
2003/5/6 23 : 56 ~ 2003/5/7 14 : 33

ports	Hosts	Remote host
4	1	61.159.62.132

Item	Description
ports	Number of TCP and UDP ports, which scanned ports in logs detected by IDS.
Hosts	Number of host scanned a port in logs detected by IDS.
Remote host	IP tried port scan.

Configuration

Set whether to apply Config file and Rule file before IDS implementation on the [Configuration] menu. After checking the risk level on the IDS Level Setup, click the [Save] button and select rules. Then, click the [OK] button to apply the rules to IDS Configuration file and to start IDS daemon.



IDS configuration

IDS Level Setup

Log setup (up) Priority 1 □ Priority 2 ☑ Priority 3 ☑ Priority 4 ☑

IDS Level Type Setup

Level 1	Log ☑	Alarm ☑	Block □	Mail □
Level 2	Log ☑	Block □	Mail □	
Level 3 4	Log ☑			

IDS Rules Configuration

All □

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

- IDS Level Setup: Categorized into the following four levels depending on risk level:

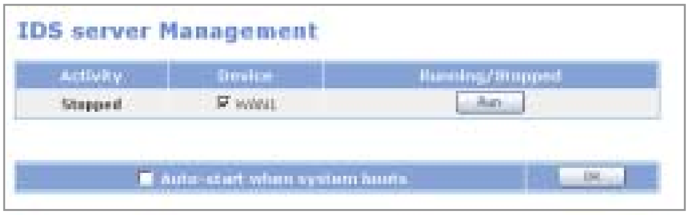
Level setup	Risk	Description
Priority 1	The highest risk(high)	Only Priority 1 is detected by IDS Rules.
Priority 2	Mid risk(med)	Priority 1 and 2 are detected by IDS Rules.
Priority 3	Mid risk(med)	Priority 1, 2 and 3 are detected by IDS Rules.
Priority 4	Low risk(low)	Priority 1, 2, 3 and 4 are detected by IDS Rules.

  – IDS Level Type Setup: Select a function in each level and click [OK].
  – Level1: By default, performs the log and alarm functions. Selects whether to disconnect the detected source IP and to send a mail to the manager.
  – Level2: By default, performs the log function. Selects whether to disconnect the detected source IP and to send a mail to the manager.
  – Level3, 4: By default, performs only the log function.

- IDS Rules Configuration: Sets rules that will detect in IDS. Check the check box of the corresponding rule, and click the [Save] button to set the target site or rule to be detected. If the ‘All’ item is checked, all rules will be selected.

Management

The user allows/inhibits executing IDS on the [Management] menu. Check the ‘Auto-start when system boots’ item and click the [OK] button. Then the IDS service automatically executed when the system reboots.



IDS server Management

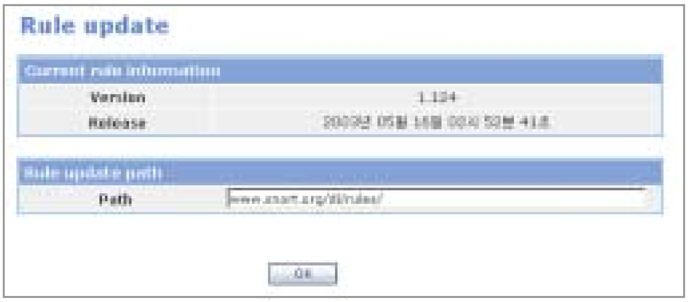
Activity	Device	Running/Stopped
Stopped	☑ WAN1	Run

☐ Auto-start when system boots   OK

Item	Description
Activity	- Running: IDS is operating. - Stopped: IDS is not operating.
Device	Select equipment for applying IDS. Equipment is limited to WAN used for setting firewall, and number of equipment is displayed as much as that of external network, which is set when a firewall is installed.
Running/Stopped	Click the [Run] button. Then, IDS is executed. Click the [Stop] button. Then, IDS is not executed.
Auto-start when system boos	If this item is checked and the [OK] button is clicked, IDS is executed automatically while the system reboots. However, firewall is not executed while the system reboots, the IDS does not operated.

Rule Update

Users are allowed to update new IDS rules on the [Rule Update] menu. Enter the target address in the 'Path' item, and click the [OK] button to download new rules.



Rule update

Current rule information

Version	1.124
Release	2003년 05월 16일 00시 53분 41초

Rule update path

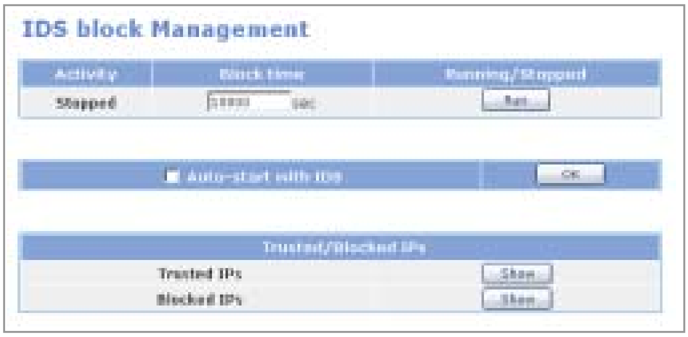
Path: www.snort.org/dl/rules/

- Current rule information: Displays the version of a rule and the time distributed.
- Rule update path: Enter the target address to download new IDS rules. When entering the target URL address, omit 'http://' as shown above. Default address is set to 'www.snort.org/dl/rules/(IDS<snort> official website)'.
  Updating a version is executed when the update is required after the current version is compared with the version to be updated.(The current version is '1.124'.)

> CHECK
>
> **When Rules are not Updated**
>
> If Domain Name Server(DNS) address is not entered when a firewall is installed, update is not executed. Thus, check if the DNS address is entered when the rule is not updated.

Block Config

Set to block the source IP, detected by IDS on the [Block Config] menu, in firewall. This function can be performed when the IDS are operating.


IDS block Management

Activity	Block time	Running/Stopped
Stopped	10800 sec	Run

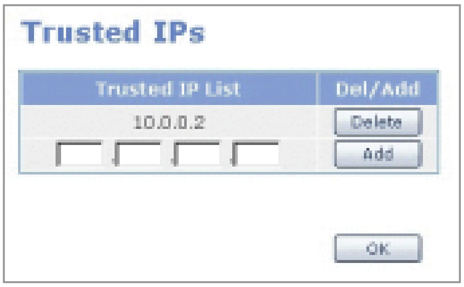
□ Auto-start with IDS — OK

Trusted/Blocked IPs	
Trusted IPs	Show
Blocked IPs	Show

Item	Description
Activity	- Running: IDS Block server is operating. - Stopped: IDS Block server is not operating.
Block time(sec)	Set the time to block source IP detected by IDS. After this item is set and DS Block server is executed, source IP is blocked for a certain period of time set in this item, and deleted from Blocked IP List after timeout. Defaults value of block time is ‘10800’.
Running/ Stopped	Click the [Run] button. Then, IDS Block server operates. Click the [Stop] button. Then, IDS Block server does not operate.
Auto-start when system boos	If this item is checked and the [OK] button is clicked, IDS is executed automatically while the system reboots. However, firewall is not executed while the system reboots, the IDS is not executed.

Trusted IPs

Click the [Show] button from the ‘Trusted IPs’ item of the <IDS block Management> window to display the window below: If the source IP detected by IDS is trusted, enter the target IP and click the [Add] button to register the IP.



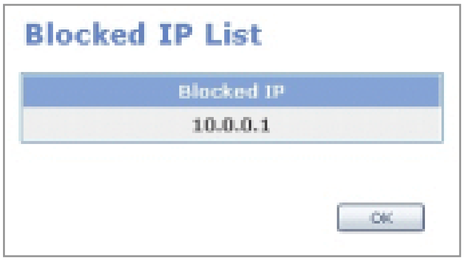
Trusted IPs

Trusted IP List	Del/Add
10.0.0.2	Delete
	Add

Since internal network is registered with Trusted IPs, the internal network or WAN IP does not need to be registered. However, trusted IP from external IPs should be registered.
If IDS detected improperly and people outside can not access, the corresponding IP should be registered. Thus, people outside can access.

Blocked IPs

Select ‘Blocked IPs’ of the <IDS block Management> window to display the window below: The IP blocked by the IDS block server or detected by IDS is displayed.

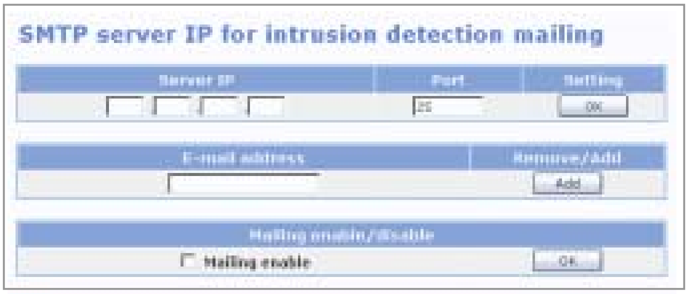


Blocked IP List

Blocked IP
10.0.0.1

Mail Config

Set to send alarm messages(IDS logs) to the administrator when IDS is detected on the [Mail Config] menu.



SMTP server IP for intrusion detection mailing

Server IP	Port	Setting
	25	OK

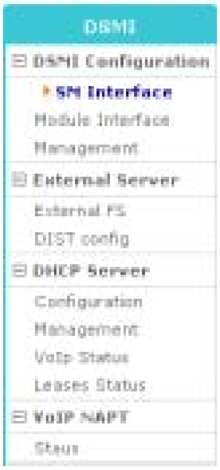
E-mail address	Remove/Add
	Add

Mailing enable/disable	
□ Mailing enable	OK

Item	Description
Server IP	IP address of mail server Install mail server into internal network(e.g. LAN or DMZ) and enter internal IP.
Port	Simple Mail Transfer Protocol(SMTP) service port of mail server Typically, No. 25 port is used.
E-mail address	Administrator’s email address, which will be received alarm messages(e.g. aaa@samsung.com) Click the [Add] button to register the email address. Click the [Delete] button to delete the registered email address.
Mailing enable/disable	Check this item and click the [OK] button to send alarm messages(IDS log) to the target registered email address.

DSMI Menu

Select [DSMI] to display the submenus of DSMI on the upper left section of the window.



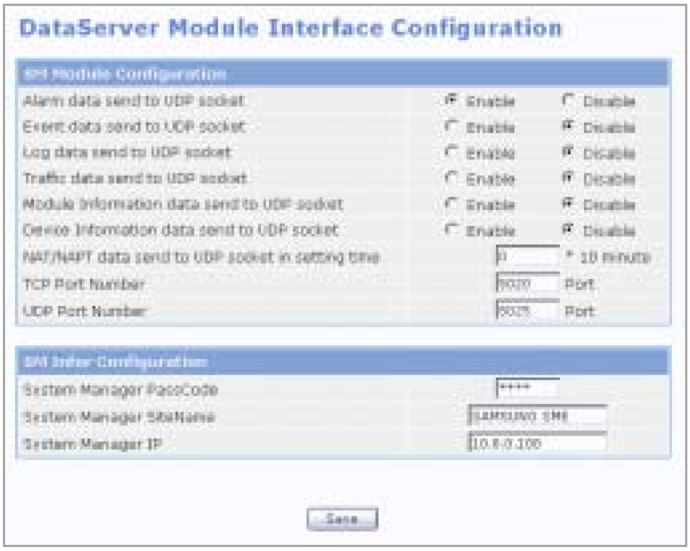
Menu	Submenu	Description
DSMI Configuration	SM Interface	Sets item related with message data.
	Module Interface	Sets DSMI_CF environment.
	Management	Allows/Inhibits executing DSMI_SM program. Set DSMI_SM program to be executed when the system reboots.
External Server	External FS	Sets the external Feature Server IP.
	DIST Config	Sends message sent to the target port from the outside to target terminal of internal network. That is, sets received messages sent to the same port to be sent to several terminals.
DHCP Server	Configuration	Sets equipment to operate DHCP Server.
	Management	Allows/Inhibits executing DHCP Server. Set DHCP Server to be executed when the system reboots.
	VoIP Status	Displays the information on OfficeServ 7200, which has received up to date.
	Leases Status	Displays a list of the IPs leased by the DHCP Server to each client.
VoIP NAPT	Status	Displays 1 to 1 mapping data of both internal port and external port.

DSMI Configuration

Set Data Server Module Interface(DSMI) environment on the [DSMI Configuration] menu.

SM Interface

Users are allowed to set items related with message data transmission on the [SM Interface] menu. Since the network traffic and system are overloads when much message data is transferred, the user should control whether to transfer message data and transmission interval.



DataServer Module Interface Configuration

SM Module Configuration		
Alarm data send to UDP socket	● Enable	○ Disable
Event data send to UDP socket	○ Enable	● Disable
Log data send to UDP socket	○ Enable	● Disable
Traffic data send to UDP socket	○ Enable	● Disable
Module Information data send to UDP socket	○ Enable	● Disable
Device Information data send to UDP socket	○ Enable	● Disable
NAT/NAPT data send to UDP socket in setting time	0	* 10 minute
TCP Port Number	5020	Port
UDP Port Number	5025	Port

SM Infor Configuration	
System Manager PassCode	****
System Manager SiteName	SAMSUNG SME
System Manager IP	10.0.0.100

If message data is sent based on UDP, select whether to send the data as shown above. If message data is sent based on TCP, the user is not required to select whether to send the data because messages data is sent when the system manager requires.

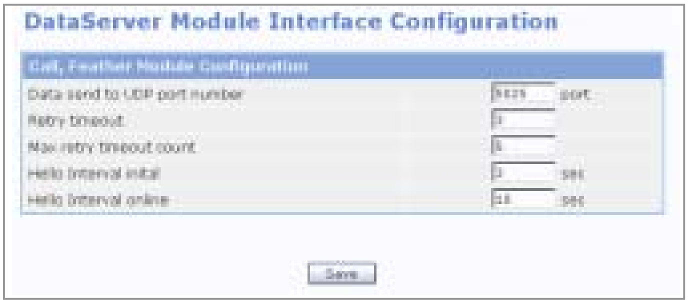
Since the TCP port is set to ‘5020’ and the UDP port is set to ‘5025’, the value should not be changed.

Information on the SM Manager can be entered. This window displays the information received from the Call Server.

Category	Item	Description
SM Module	Alarm data	When 'Enable' is set, alarm message, which occurs when the system is abnormal or a hacker attacked the system, is sent to the system manager through UDP port immediately.
	Event data	When 'Enable' is set, system event message being generated is sent to the system manager through UDP port immediately.
	Log data	When 'Enable' is set, message data is sent to the system manager through UDP port immediately when the user access the system through system connection path.
	Traffic data	When 'Enable' is set, network traffic data generated from system network equipment is sent to the system manager through UDP port on a regular basis(30 minutes).
	Module Information data	When 'Enable' is set, system module data is sent to the system manager through UDP port.
	Device Information data	When 'Enable' is set, system network equipment data is sent to the system manager through UDP port.
	NAT/NAPT data	Sets the time interval for sending IP data and connection data, which use NAT/NAPT from clients being connected to the system manager. For example, '5' is entered, the data is sent every 50 minutes.
	TCP Port Number	Sets the TCP connection port with the system manager. The default is 5020.
	UDP Port Number	Sets the UCP connection port with the system manager. The default is 5025.
SM Infor	System Manager Passcode	Displays the passcode of the system manager received from the Call Server. The passcode may be forced to be set.
	System Manager Sitename	Displays the site name of the system manager received from the Call Server. The name may be forced to be set.
	System Manager IP	Displays the IP of the system manager received from the Call Server. The IP may be forced to be set.

Module Interface

Set DSMI_CF from Data Server Module Interface Daemon(DSMI_SM, DSMI_CF) on the [Module Interface] menu. When the system reboots, default value is set as shown below:



DataServer Module Interface Configuration

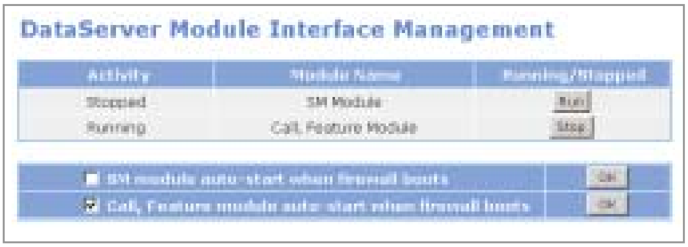
Call, Feather Module Configuration

Data send to UDP port number	5025	port
Retry timeout	3	
Max retry timeout count	5	
Hello Interval initial	3	sec
Hello Interval online	10	sec

Item	Description
Data send to UDP port number	UDP port used when DSMI_CF receives data. Default value is ‘5025’.
Retry timeout (Sec)	DSMI_CF, Call Server, Feature Server, and Data Server communicate based on UDP. Since UDP may lose packet, it requests retry when it does not receive the requested data. Set time interval for retry. For example, the item is set to ‘3’. After a packet is lost, retry is requested, but the requested data is not received. Then, UDP requests retry 3 seconds later. If the requested packet is not received for 3 seconds, timeout occurs.
Max retry timeout count	Sets retry count when packet is lost continuously while DSMI_CF exchanges data with Call Server. For example, Retry timeout is set to ‘3’ and ‘5’, retry is requested five times for three seconds. If requested packet is not received, stop retry request.
Hello Interval initial	Hello massage is the message that DSMI_CF, Call Server, and Feature Server exchanges periodically. Set time interval for sending Hello message.
Hello Interval online	DSMI_CF sends Hello message every certain time set in ‘Hello Interval Initial’ to check other link data and notify its own status when the system reboots. When Hello message is received from Call Server and Feature Server while Hello message is sent, Hello message should be sent every certain time period set in this item. This value should be set to be more than the value of ‘Hello Interval initial’ item.

Management

The user allows/inhibits executing DSMI_SM program on the [Management] menu. Check the ‘Auto Start’ to execute the services automatically while the system reboots.



DataServer Module Interface Management

Activity	Module Name	Running/Stopped
Stopped	SM Module	Run
Running	Call, Feature Module	Stop

□ SM module auto-start when firewall boots	OK
☑ Call, Feature module auto-start when firewall boots	OK

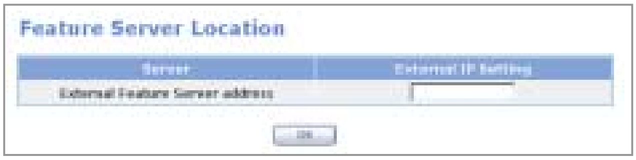
Check the ‘SM module auto-start when firewall boots’ or ‘Call, Feature module auto-start when firewall boots’ item and click the [OK] button. Then, the SM module or the Call, Feature module is automatically executed.

External Server

Set an external Feature Server IP on the [External Server] menu, or an internal network terminal to send received messages from the outside to the target port.

External FS

Set IP of the Feature Server of an external network on the [External FS] menu.



Feature Server Location

Server	External IP Setting
External Feature Server address	

OK

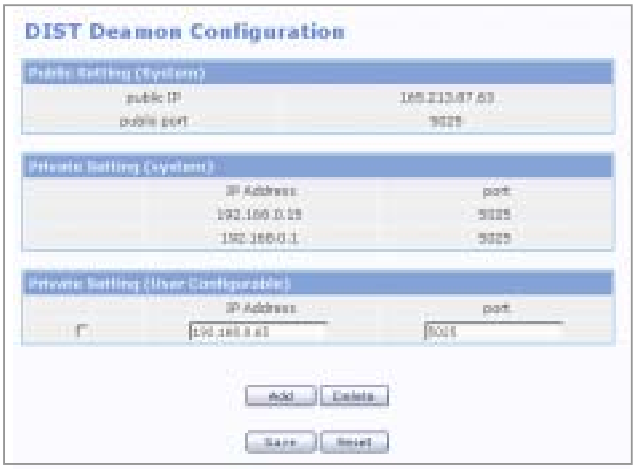
NOTE

Feature Server of Internal Network

- The Feature Server is located in internal network, IP should not be entered in the ‘External Feature Server address’ item, but be entered in the feature Server item of the [DSMI] → [DHCP Server] → [Configuration] menu.
- If the Feature Server is set to both the [DSMI] → [External Server] → [External FS] menu and the [DSMI] → [DHCP Server] → [Configuration] menu, UDP packet will be sent to the Feature Server set to the External Server.

DIST Config

Register an internal network terminal to send messages received to the target port from the outside on the [DIST Config] menu.
The IP addresses of the Feature Server and system manager on the external network, which have been set by DSMI, are automatically registered with 'Private Setting(System)'.
Enter the IP address and port in 'Private Setting(User Configurable)' and click [Add] and [Save] in sequence to register the IP additionally.



DIST Deamon Configuration

Public Setting (System)

public IP	165.213.87.63
public port	5025

Private Setting (System)

IP Address	port
192.168.0.15	5025
192.168.0.1	5025

Private Setting (User Configurable)

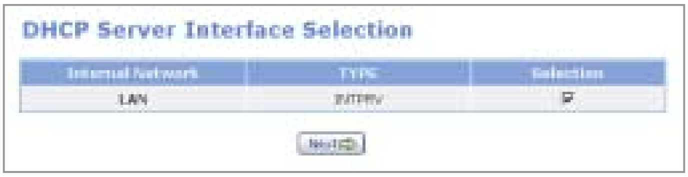
	IP Address	port
□	192.168.0.61	5025

DHCP Server

Set equipment to operate the DHCP Server on the [DHCP Server] menu and allow or inhibit the DHCP Server operation.

Configuration

Select equipment for operating DHCP Server from internal network equipment set on the [Network & FW] menu on the [Configuration] menu. Select the [DHCP Server] → [Configuration] menu to display the internal network set to ‘Internal Private Network’ or ‘Internal Public Network’ on the [Network & FW] → [Management] → [Configuration] menu.



DHCP Server Interface Selection

Internal Network	TYPE	Selection
LAN	INTPRV	☑

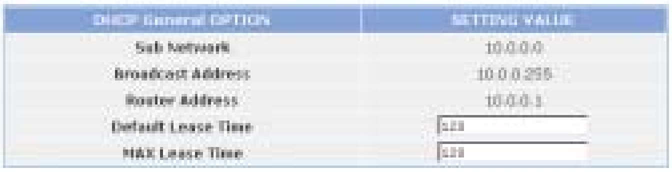
Check the check box to be set and click the [Next] button to display the <DHCP Server Configuration> window to set the environment.

The <DHCP Server Configuration> window displays default value of the equipment selected from the <DHCP Server Interface Selection> window. Allocate the OfficeServ 7200 system IP such as Call Server whose subnet is the same level with that of the selected equipment, Feature Server, IP phone, SIP phone, and data terminal to DHCP.

Set the following items and click the [Save] button.

DHCP Server

Displays normal data to be allocated to DHCP client. Set Lease Time.

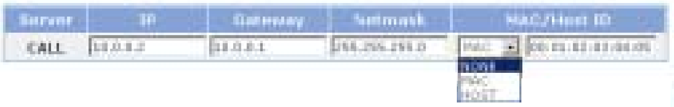


DHCP General OPTION	SETTING VALUE
Sub Network	10.0.0.0
Broadcast Address	10.0.0.255
Router Address	10.0.0.1
Default Lease Time	123
MAX Lease Time	123

Item	Description
Sub Network	Sub network data Value set on the [Network & FW] → [Management] → [Config] menu. This value can be changed on the menu.
Broadcast Address	Broadcast address Value set on the [Network & FW] → [Management] → [Config] menu. This value can be changed on the menu.
Router Address	Router address Value set on the [Network & FW] → [Management] → [Config] menu. This value can be changed on the menu.
Default Lease Time(sec)	If DHCP client does not request expiration time, the value will be allocated to this item.
MAX Lease Time(sec)	If DHCP client requests expiration time, the value is the maximum time to be allocated.

CALL Server

Allocate the Call Server IP to DHCP.

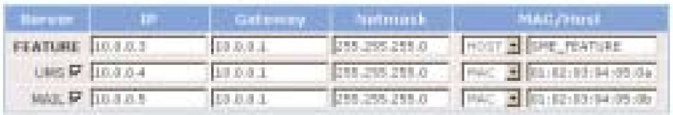


Server	IP	Gateway	Netmask	MAC/Host ID	
CALL	10.0.0.2	10.0.0.1	255.255.255.0	MAC	00:01:02:03:04:05

Item	Description
IP	Call Server IP address
Gateway	Gateway data
Netmask	Netmask data
MAC/Host ID	Client authentication type - NONE: Executes DHCP IP request without authentication. - MAC: Authentication as MAC - HOST: Authentication as HOST ID(Default value: SME_MCP)

Feature Server

Allocate the Feature Server IP to DHCP.

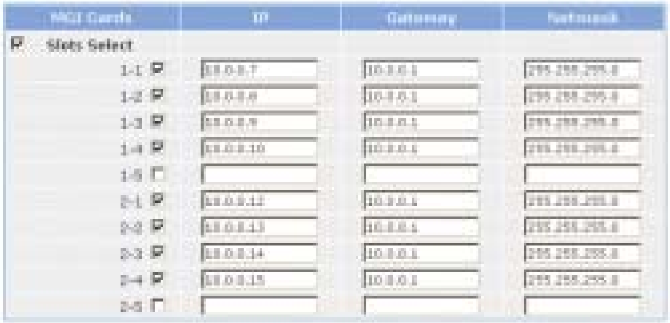


Server	IP	Gateway	Netmask	MAC/Host	
FEATURE	10.0.0.3	10.0.0.1	255.255.255.0	HOST	SME_FEATURE
UMS ☑	10.0.0.4	10.0.0.1	255.255.255.0	MAC	01:02:03:04:05:0a
MAIL ☑	10.0.0.5	10.0.0.1	255.255.255.0	MAC	01:02:03:04:05:0b

If the Feature Server does not contain the UMS and MAIL servers, the IP information on the UMS and MAIL servers should be entered. Since the items of UMS and MAIL servers are inactive, check on the left check box and enter the corresponding values.

MGI Cards

Set the IP of the MGI card mounted on the system.
After checking the 'Slots Select' check box, check the check box on the left for each item and enter the corresponding values.

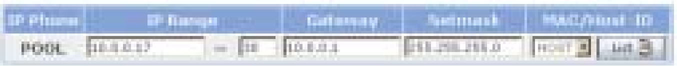


MGI Cards	IP	Gateway	Netmask
☑ Slots Select			
1-1 ☑	10.0.0.7	10.0.0.1	255.255.255.0
1-2 ☑	10.0.0.8	10.0.0.1	255.255.255.0
1-3 ☑	10.0.0.9	10.0.0.1	255.255.255.0
1-4 ☑	10.0.0.10	10.0.0.1	255.255.255.0
1-5 □			
2-1 ☑	10.0.0.12	10.0.0.1	255.255.255.0
2-2 ☑	10.0.0.13	10.0.0.1	255.255.255.0
2-3 ☑	10.0.0.14	10.0.0.1	255.255.255.0
2-4 ☑	10.0.0.15	10.0.0.1	255.255.255.0
2-5 □			

This value should be identical with the network data set on the [Network & FW] → [Management] → [Config] menu. The number of MGI cards can be up to 10, and the number on the left indicates the location of cabinet-slots.

IP Phone

Allocate the IP range of the IP phone on the DHCP mode.

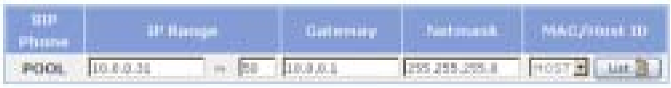


IP Phone	IP Range			Gateway	Netmask	MAC/Host ID	
POOL	10.0.0.17	~	30	10.0.0.1	255.255.255.0	HOST	List

Item	Description
IP Range	IP range of IP phone(Maximum number of IP phone is 120) If one IP is entered, enter like ‘10.0.0.17~17’.
Gateway	Gateway data entered in the CALL Server item
Netmask	Netmask data entered in the CALL Server item
MAC/Host-ID	Client authentication type - NONE: Executes DHCP IP request without authentication. - MAC: Click the [List] button to enter MAC address of IP phone for authentication. - HOST: Uses HOST ID internally specified.

SIP Phone

Allocate the IP range of standard SIP phone on the DHCP mode.

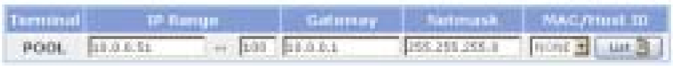


SIP Phone	IP Range			Gateway	Netmask	MAC/Host ID	
POOL	10.0.0.31	~	50	10.0.0.1	255.255.255.0	HOST	List

Item	Description
IP Range	IP range of SIP phone(Maximum number of IP phone is 120) If one IP is entered, enter like ‘10.0.0.17~17’.
Gateway	Gateway data entered in the CALL Server item
Netmask	Netmask data entered in the CALL Server item
MAC/Host-ID	Client authentication type - NONE: Executes DHCP IP request without authentication - MAC: Click the [List] button to enter MAC address of IP phone for authentication. - HOST: Since HOST ID internally specified is not used, click the [List] button to enter HOST ID.

Terminal

Allocate data terminal to DHCP.

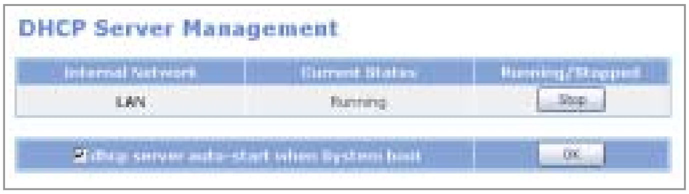


Terminal	IP Range			Gateway	Netmask	MAC/Host ID	
POOL	10.0.0.51	~	100	10.0.0.1	255.255.255.0	NONE	List

Item	Description
IP Range	IP range of data terminal(Maximum number of IP phone is 120) If one IP is entered, enter like ‘10.0.0.17~17’.
Gateway	Gateway data entered in the CALL Server item
Netmask	Netmask data entered in the CALL Server item
MAC/Host-ID	Client authentication type - NONE: Executes DHCP IP request without authentication. - HOST: Click the [List] button to enter HOST ID. - MAC: Click the [List] button to enter MAC address.

Management

Select the [DHCP Server] → [Management] menu to allow/inhibit operating the DHCP Server. Check the ‘Auto Start’ item. Then, the service is provided automatically while the system reboots.



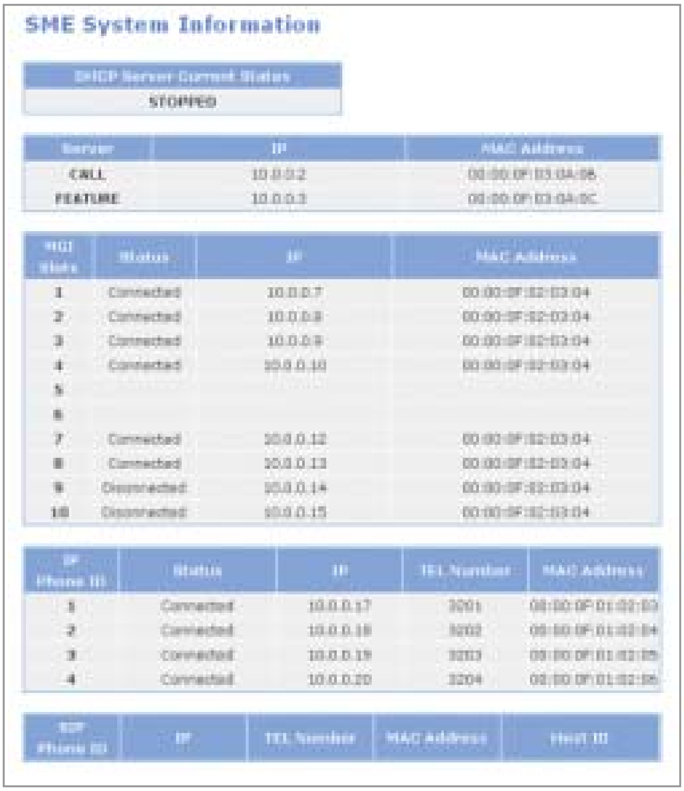
DHCP Server Management

Internal Network	Current Status	Running/Stopped
LAN	Running	Stop

☑ dhcp server auto-start when System boot | OK

VoIP Status

Displays the OfficeServ 7200 systems data, which has been received so far, on the [DHCP Server] → [VoIP Status] menu.
If the DHCP Server data on the [DHCP Server] → [Configuration] menu is set and kept, the DHCP Server operates and the IP is automatically allocated to the Call Server and Feature Server. Then, the data is notified to module interface daemon of the Data Server, and the user can search the data on the following window:



SME System Information

DHCP Server Current Status
STOPPED

Server	IP	MAC Address
CALL	10.0.0.2	00:00:0F:03:04:08
FEATURE	10.0.0.3	00:00:0F:03:04:0C

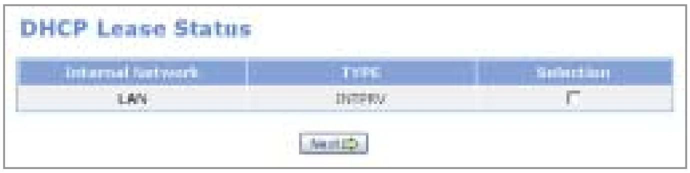
MGI Slots	Status	IP	MAC Address
1	Connected	10.0.0.7	00:00:0F:02:03:04
2	Connected	10.0.0.8	00:00:0F:02:03:04
3	Connected	10.0.0.9	00:00:0F:02:03:04
4	Connected	10.0.0.10	00:00:0F:02:03:04
5			
6			
7	Connected	10.0.0.12	00:00:0F:02:03:04
8	Connected	10.0.0.13	00:00:0F:02:03:04
9	Disconnected	10.0.0.14	00:00:0F:02:03:04
10	Disconnected	10.0.0.15	00:00:0F:02:03:04

IP Phone ID	Status	IP	TEL Number	MAC Address
1	Connected	10.0.0.17	3201	00:00:0F:01:02:03
2	Connected	10.0.0.18	3202	00:00:0F:01:02:04
3	Connected	10.0.0.19	3203	00:00:0F:01:02:05
4	Connected	10.0.0.20	3204	00:00:0F:01:02:06

SIP Phone ID	IP	TEL Number	MAC Address	Host ID

Leases Status

Select [DHCP Server] → [Leases Status] menus. Then, the IP address allocated by the DHCP Server to the data terminal will be displayed.



DHCP Lease Status

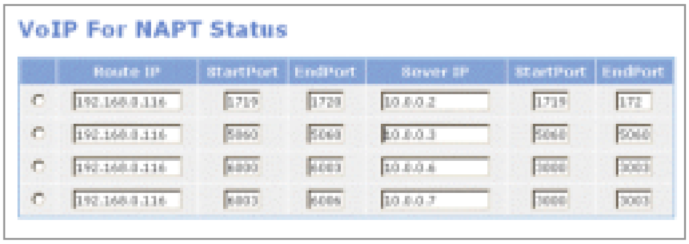
Internal Network	TYPE	Selection
LAN	INTSRV	□

VoIP NAPT

Displays NAPT item for VoIP communication on the [VoIP NAPT] menu.

Status

Connects 32 internet ports and external ports to each MGI card through one to one mapping. Whenever the DHCP Server item is newly set, DSMI_CF Daemon exchanges new data with the Call Server. At this time, the NAPT item is configured on the Data Server for VoIP communication of H.323 phone. The [Status] menu displays the corresponding data.



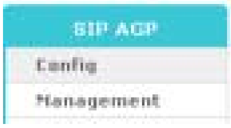
VoIP For NAPT Status

	Route IP	StartPort	EndPort	Server IP	StartPort	EndPort
○	192.168.0.116	1719	1728	10.0.0.2	1719	172
○	192.168.0.116	5060	5060	10.0.0.3	5060	5060
○	192.168.0.116	6000	6003	10.0.0.6	3000	3003
○	192.168.0.116	6003	6006	10.0.0.7	3000	3003

The MGI card item set on the [DHCP Server] → [Configuration] menu and the VoIP NAPT item for Call Server and Feature Server are created. DSMI_CF Daemon sends the internal IP, the external IP of a port, and the port date to the Call Server. The window above displays these data in the VoIP NAPT table format.

SIP AGP Menu

Select [SIP AGP] to display the submenus of SIP AGP on the upper left section of the window.



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

NOTE

SIP AGP(SIP aware ALG)

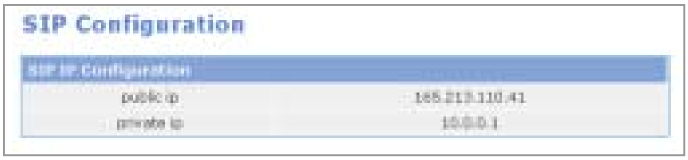
Typically, if a firewall protects internal network, the NAT based SIP AGP(SIP aware ALG) is safe from external attacks, but providing services are limited. The problems are resolved. Thus, SIP devices of a firewall can communicate with external devices.

Config

Users are allowed to set the SIP environment on the [Config] menu. Set the following items and click the [Save] button.

SIP Configuration

Displays firewall installation data.

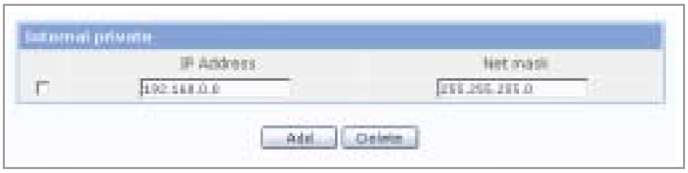


SIP Configuration

SIP IP Configuration	
public ip	165.213.110.41
private ip	10.0.0.1

Internal private

Enter the internal private IP area protected by the Data Server.



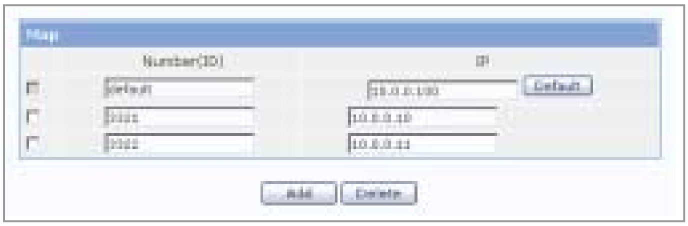
Internal private

	IP Address	Net mask
□	192.168.0.0	255.255.255.0

Click the [Add] button to additionally add private IP area inside of the firewall. The SIP device in the added private IP area provides ALG(SIP AGP) function. Set the target routing data directly or operate the target routing protocol to route to the added private IP area. Refer to Internal IP(LAN, DMZ) Setting on the [Network & FW] → [Management] → [Config] of this document for detailed information.

Map

Enter SIP devices data inside of the firewall.



Map

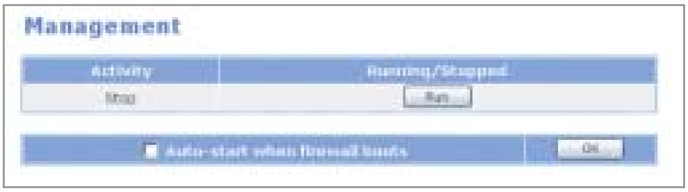
	Number(ID)	IP
□	default	10.0.0.100
□	3321	10.0.0.10
□	3322	10.0.0.11

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

For example, in the window above, all station numbers except 3321 and 3322 is processed by the Call Server(10.0.0.100).

Management

Select the [Management] menu to allow/inhibit operating SIP AGP. Check the ‘Auto Start’ item. Then, the service is provided automatically when the system reboots.

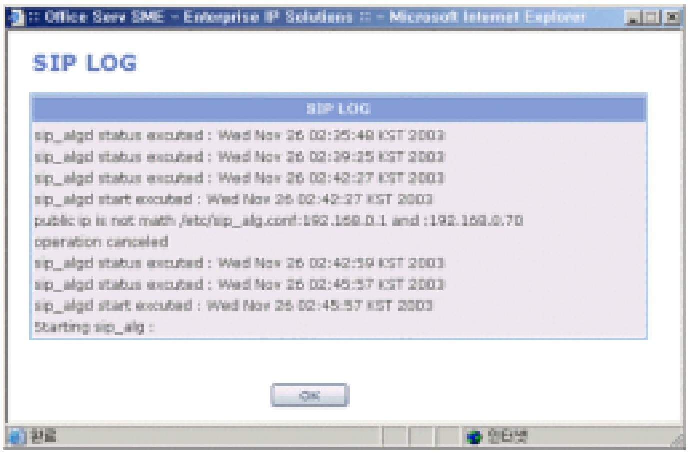


Management

Activity	Running/Stopped
Stop	Run

□ Auto-start when firewall boots

Click the [Run] button to operate the SIP AGP and the following window is displayed:



:: Office Serv SME - Enterprise IP Solutions :: - Microsoft Internet Explorer
OK
완료
인터넷

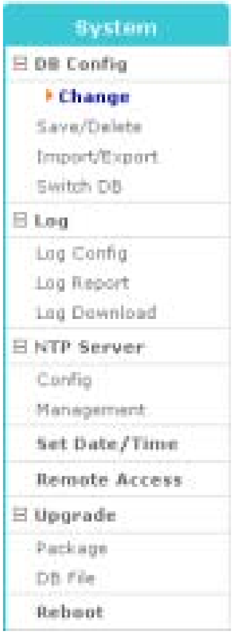
SIP LOG

```
SIP LOG
sip_algd status excuted : Wed Nov 26 02:35:48 KST 2003
sip_algd status excuted : Wed Nov 26 02:39:25 KST 2003
sip_algd status excuted : Wed Nov 26 02:42:27 KST 2003
sip_algd start excuted : Wed Nov 26 02:42:27 KST 2003
public ip is not math /etc/sip_alg.conf:192.168.0.1 and :192.168.0.70
operation canceled
sip_algd status excuted : Wed Nov 26 02:42:59 KST 2003
sip_algd status excuted : Wed Nov 26 02:45:57 KST 2003
sip_algd start excuted : Wed Nov 26 02:45:57 KST 2003
Starting sip_alg :
```

The window above displays when SIP AGP is executed normally. However, errors are found, the ‘operation canceled’ message is displayed.

System Menu

Select [SIP AGP] to display the submenus of SIP AGP on the upper left section of the window.



Menu	Submenu	Description
DB Config	Change	Whether to change the operating DB to other DB or default DB.
	Save/Delete	Whether to save or delete DB.
	Import/Export	Imports the DB to be backed up to operating terminal or exports the DB backed up from terminal.
	Switch DB	Imports the Switch DB to the operating terminal or exports the Switch DB from a termial.
Log	Log Config	Sets type of logs to be recorded.
	Log Search	Searches logs according to type and time.
	Log Download	Downloads all log files saved to a local computer.

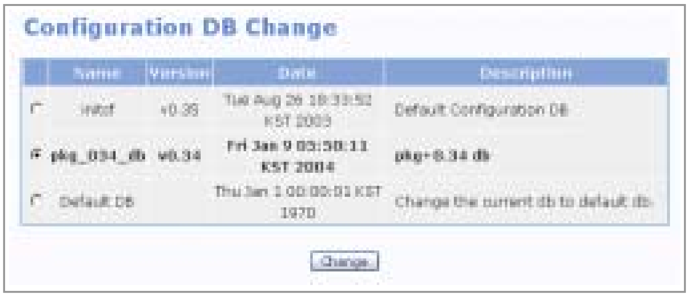
Menu	Submenu	Description
NTP Server	Config	Registers server to search date and hour data.
	Management	Searches date and hour data from the registered server and newly sets date and hour of the system.
Set Date/Time		Changes system date and hour.
Remote Access		Executes Telnet, FTP, and SSH services to connect WIM board from a remote area.
Upgrade	Package	Upgrades DB package, Kernel, Ramdisk, and Application.
	DB File	Upgrades DB to the latest package version.
Reboot		Reboots the system

DB Config

Users are allowed to save or delete DB, or to change the operating DB to other DB on the [DB Config] menu.

Change

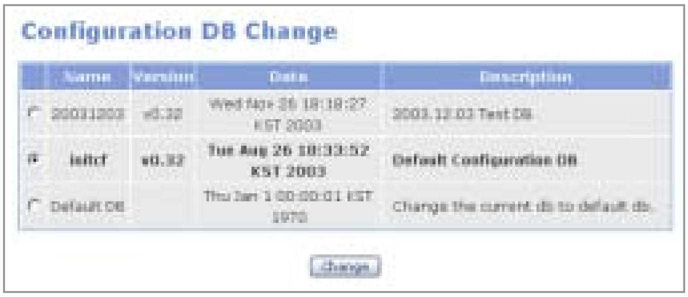
Users are allowed to change the operating DB to other DB or default DB on the [Change] menu. The operating DB below is displayed with bold letters: Select the DB to be changed and click the [Change] button.



Configuration DB Change

	Name	Version	Date	Description
○	initdf	v0.35	Tue Aug 26 18:33:52 KST 2003	Default Configuration DB
●	**pkg_034_db**	**v0.34**	**Fri Jan 9 05:50:11 KST 2004**	**pkg-0.34 db**
○	Default DB		Thu Jan 1 00:00:01 KST 1970	Change the current db to default db

Select ‘Default DB’ and click the [Change] button. Then, initial DB is initialized and changed as shown below: initcf is the initial DB.
When the Default DB is selected, the system is initalized. Thus, connect to the web manager through the LAN port(10.0.0.1) of the internal network.



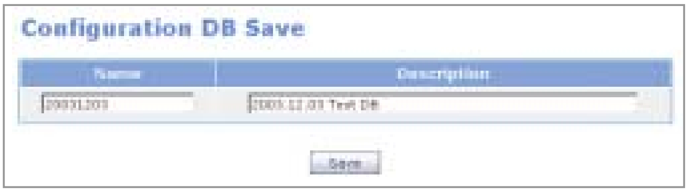
Configuration DB Change

	Name	Version	Date	Description
○	20031203	v0.32	Wed Nov 26 18:18:27 KST 2003	2003.12.03 Test DB
●	**initcf**	**v0.32**	**Tue Aug 26 18:33:52 KST 2003**	**Default Configuration DB**
○	Default DB		Thu Jan 1 00:00:01 KST 1970	Change the current db to default db.

Save/Delete

Users are allowed to change the name of the operating DB, or delete the DB saved on the [Save/Delete] menu.

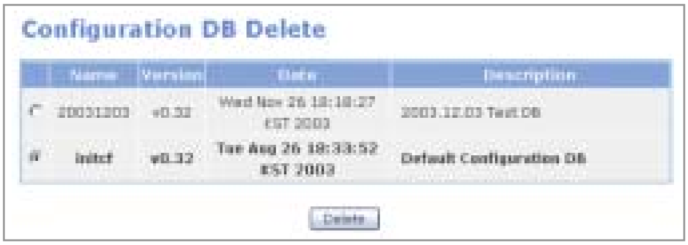
Enter the DB name and description and click the [Save] button to save the DB. Then, the saved DB is registered on the <Configuration DB Delete> window.



Configuration DB Save

Name	Description
20031203	2003.12.03 Test DB

Select the DB to be deleted and click the [Delete] button. The operating DB is displayed with bold letters and can not be deleted.



Configuration DB Delete

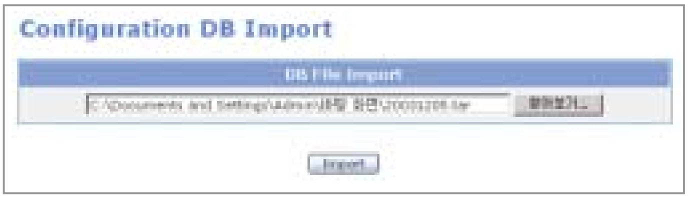
	Name	Version	Date	Description
○	20031203	v0.32	Wed Nov 26 18:18:27 KST 2003	2003.12.03 Test DB
●	**initcf**	**v0.32**	**Tue Aug 26 18:33:52 KST 2003**	**Default Configuration DB**

Import/Export

Users are allowed to import the DB to be backed up to the operating terminal on the [Import/Export] menu, or export the backup DB from a terminal.

Import

DB file should be saved in a terminal to import the DB. Enter the DB file location, or click the [Browse] button to select the target file, and click the [Import] button. Then, the DB is registered on the <Configuration DB Export> window.



Configuration DB Import

DB File Import

C:\Documents and Settings\Admin\바탕 화면\20031205.tar

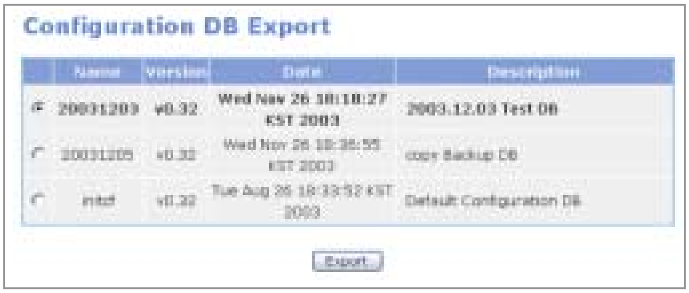
CHECK

If Errors are Found When [Import] is Executed, Check the Following Cases:

- Corresponding file does not exit after file location is entered
- Click the [Import] button without entering anything in the corresponding field.
- DBs whose names are identical
- File name is changed in the existing DB
- The first letter is left blank.

Export

The DB set is displayed with bold letters. Select the target DB and click the [Export] button to save DB to the selected area of a terminal.



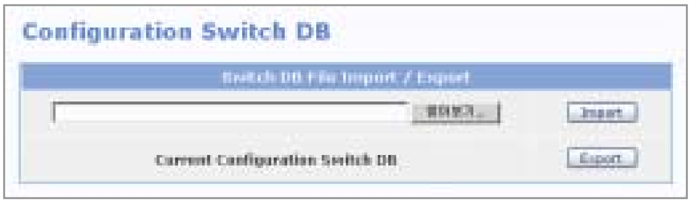
Configuration DB Export

	Name	Version	Date	Description
●	**20031203**	**v0.32**	**Wed Nov 26 18:18:27 KST 2003**	**2003.12.03 Test DB**
○	20031205	v0.32	Wed Nov 26 18:36:55 KST 2003	copy Backup DB
○	initd	v0.32	Tue Aug 26 18:33:52 KST 2003	Default Configuration DB

If the DB is sent to a terminal, click the [Save] button and download the DB: Decompress the downloaded DB with using compressor.

Switch DB

Users are allowed to import the Switch DB to the operating terminal on the [Switch DB] menu, or export the Switch DB from a terminal.



Configuration Switch DB

Switch DB File Import / Export

Current Configuration Switch DB

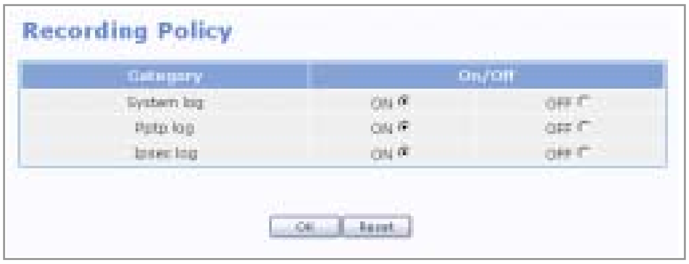
Enter the location of the Switch DB file to import the Switch DB from the terminal. Otherwise, click [Brows…], select the file, and then click [Import]. Click [Export] to export the Switch DB to the terminal.

Log

Users are allowed to search or download logs while logs are set to be recorded on the [Log] menu.

Log Config

Set logs to be recorded on the [Log Config] menu. Set the logs to be recorded to ‘On’, and otherwise, set to ‘Off’.



Recording Policy

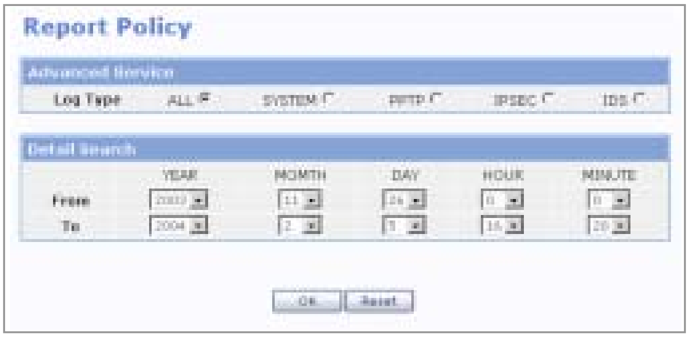
Category	On/Off	
System log	ON ●	OFF ○
Pptp log	ON ●	OFF ○
Ipsec log	ON ●	OFF ○

Log types are as follows:

- System log: System related log
- Pptp log: Log related with PPTP protocol of VPN
- Ipsec log: Log related with IPSEC protocol of VPN

Log Report

Search logs according to type and time on the [Log Report] menu.



Report Policy

Advanced Service

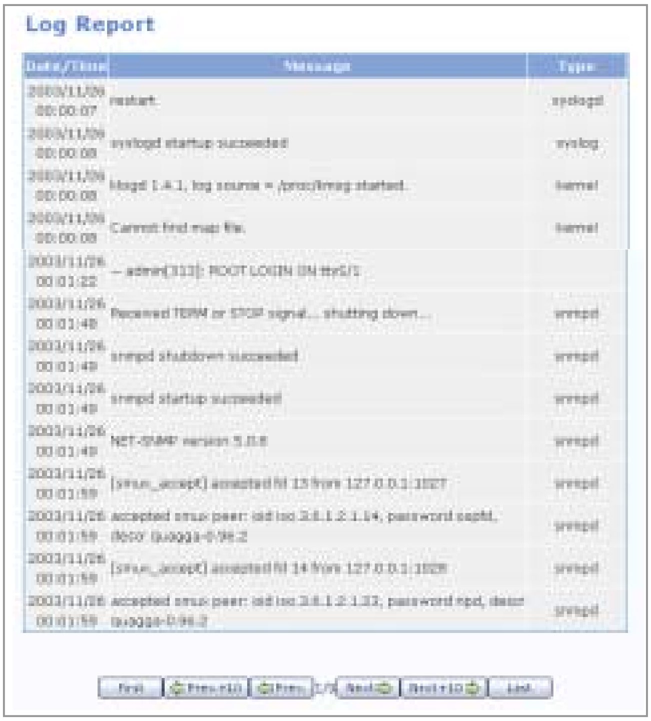
Log Type ALL ● SYSTEM ○ PPTP ○ IPSEC ○ IDS ○

Detail Search

	YEAR	MONTH	DAY	HOUR	MINUTE
From	2003	11	24	0	0
To	2004	2	5	16	20

- Log Type: Select the specific log type and search logs according to the type.
  - ALL: Search all logs
  - SYSTEM: Search all logs except PPTP, IPSEC, and IDS logs
  - PPTP: Search logs of PPTP protocol of VPN
  - IPSEC: Search logs of IPSEC protocol of VPN
  - IDS: Search IDS protocol logs
- Detail Search: Enter the specific time and search logs according to the time.

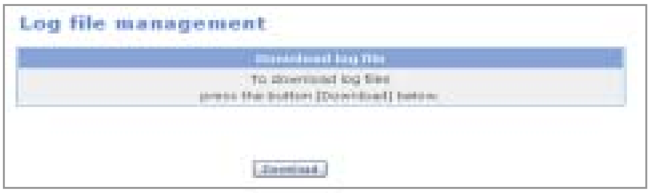
Select the type and time of logs, and click the [OK] button to display the window below:



Date/Time	Message	Type
2003/11/09 00:00:07	restart.	syslogd
2003/11/09 00:00:08	syslogd startup succeeded	syslog
2003/11/09 00:00:08	klogd 1.4.1, log source = /proc/kmsg started.	kernel
2003/11/09 00:00:08	Cannot find map file.	kernel
2003/11/26 00:01:22	-- admin[313]: ROOT LOGIN ON ttyS/1	
2003/11/26 00:01:48	Received TERM or STOP signal... shutting down...	snmpd
2003/11/26 00:01:49	snmpd shutdown succeeded	snmpd
2003/11/26 00:01:49	snmpd startup succeeded	snmpd
2003/11/26 00:01:49	NET-SNMP version 5.0.8	snmpd
2003/11/26 00:01:59	[smux_accept] accepted fd 13 from 127.0.0.1:1027	snmpd
2003/11/26 00:01:59	accepted smux peer: oid iso.3.6.1.2.1.14, password ospfd, descr quagga-0.96.2	snmpd
2003/11/26 00:01:59	[smux_accept] accepted fd 14 from 127.0.0.1:1028	snmpd
2003/11/26 00:01:59	accepted smux peer: oid iso.3.6.1.2.1.23, password ripd, descr quagga-0.96.2	snmpd

Log Download

Users are allowed to download all log files saved to a local computer on the [Log Download] menu.



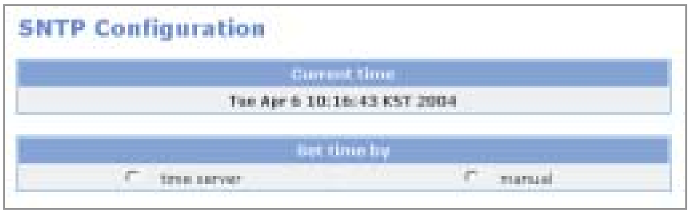
To download log files
press the button [Download] below.

NTP Server

Users are allowed to set the date and hour of the system through network on the [NTP Server] menu.

Config

Click [NTP Server] → [Config] to register a server from which information on date and time will be imported or enter time information manually.



SNTP Configuration

Current time

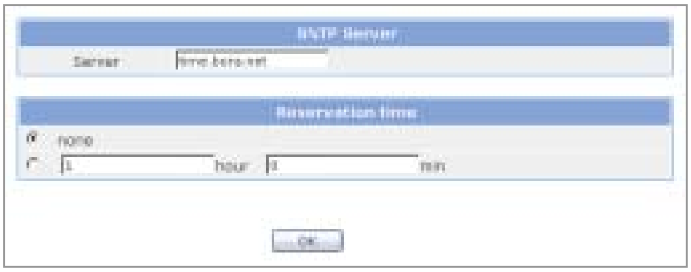
Tue Apr 6 10:16:43 KST 2004

Set time by

○ time server ○ manual

time server

Select the time server option. Then, the window below will appear. Register a server from which information on date and time will be imported and set the cycle of receiving information. Then, click [OK].



SNTP Server

Server: time.bora.net

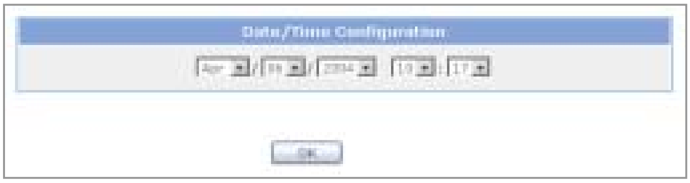
Reservation time

● none

○ 1 hour 0 min

manual

Select the manual option. Then, the window below will appear. Enter date and time manually and click [OK].

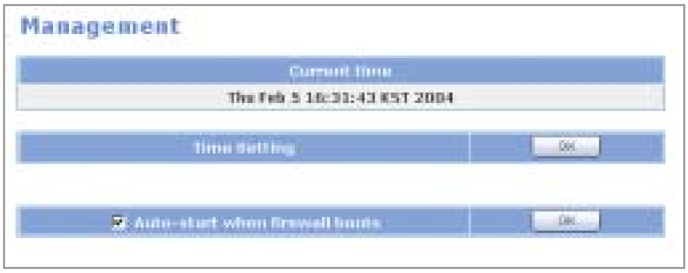


Date/Time Configuration

Apr / 06 / 2004 10 : 17

Management

Select the [NTP Server] → [Management] menu and set the time. Then, set the date and hour of the system received from the saved server on the <NTP Server Configuration> window.



Management

Current time

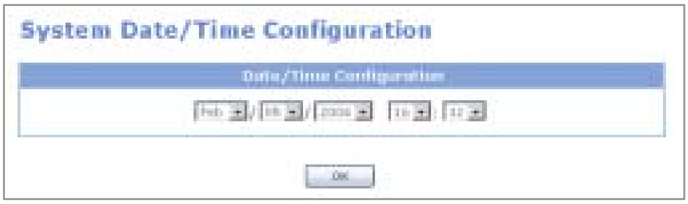
Thu Feb 5 16:31:43 EST 2004

☑ Auto-start when firewall boots

After a server, data and hour are registered with the NTP Server Configuration, set the date and hour of the system received from the registered server.
If the 'Auto Start' item is checked, the service is provided automatically when the system reboots.

Set Data/Time

Users are allowed to change the date and hour of the system on the [Set Data/Time] menu. If the NPT Server is not available to use, the user can change the time manually. After selecting the date and time, click the [OK] button.



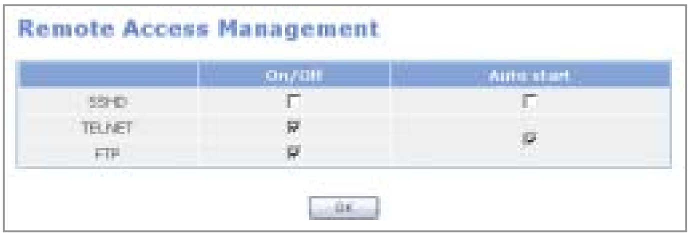
System Date/Time Configuration

Date/Time Configuration

Feb / 05 / 2004 16 : 32

Remote Access

If the SSH, Telnet, and FTP services are executed on the [Remote Access] menu, the user can access the WIM board from a remote area. In addition, If the ‘Auto Start’ item is checked, the service is provided automatically when the system reboots.



Remote Access Management

	On/Off	Auto start
SSHD	□	□
TELNET	☑	☑
FTP	☑	

NOTE

Assigned Active Channel to ‘Response Status’

- SSH can be accessed regardless of external network or internal network.
- If a firewall is strengthened, accessing the system from an external network through Telnet/FTP is not available.
- The default password of root user is ‘samsung’.

The connection methods through WAN and LAN IP by using Telnet, FTP, and SSH applications from the outside and inside are as follows:

Connecting to Telnet

```
[root@localhost package]# telnet 192.168.0.1
Trying 192.168.0.1...
Connected to 192.168.0.1.
Escape character is ‘^]’.

Linux 2.4.19-WIM(localhost.localdomain)(11:36 on Thursday,
01 January 1970)

login: root
Password:samsung
[root@localhost /]# ls
00app     bin       lib        sbin       var
00conf    dev       lost+found tmp
00log     etc       proc       usr
[root@localhost /]# exit
logout
Connection closed by foreign host.
```

Connecting to FTP

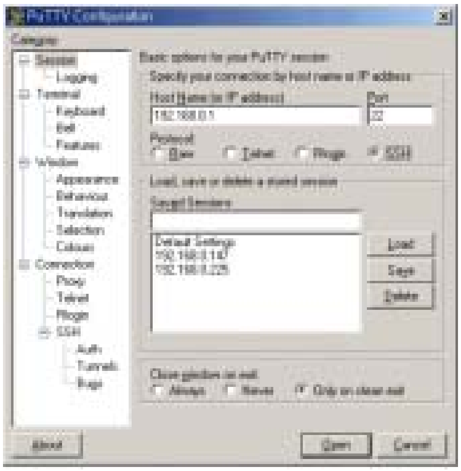
```
[root@localhost package]# ftp 192.168.0.1
Connected to 192.168.0.75(192.168.0.1).
220 localhost.localdomain FTP server(Version wu-2.6.1(1) Sat
Oct 26 13:49:35 MEST 2002) ready.
Name(192.168.0.1:hanpyo): root
331 Password required for root.
Password:samsung
230 User root logged in.Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
227 Entering Passive Mode(192,168,0,1,206,172)
150 Opening ASCII mode data connection for /bin/ls.
drwxr-xr-x   2 root     root       1024 Aug 26   2003 00app
drwxr-xr-x   2 root     root       1024 Aug 26   2003 00conf
drwxr-xr-x   2 root     root       1024 Aug 26   2003 00log
drwxr-xr-x   2 root     root       2048 Aug 26   2003 bin
drwxr-xr-x   1 root     root          0 Jan  1  00:00 dev
drwxr-xr-x   9 root     root       2048 Jan  1  00:31 etc
226 Transfer complete.
ftp> by
221-You have transferred 0 bytes in 0 files.
221-Total traffic for this session was 1261 bytes in 1
transfers.
221-Thank you for using the FTP service on
localhost.localdomain.
221 Goodbye.
```

Connecting to SSH

SSH connection program uses Putty program. The procedure for installing the Putty program and executing the SSH connection program is as follows:

1. Visit the web site below and download the Putty package: ‘http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html’

2. If the ‘putty.exe’ file is executed, the window below is displayed. Enter the firewall address in the Host Name field and select ‘SSH’ from the Protocol.



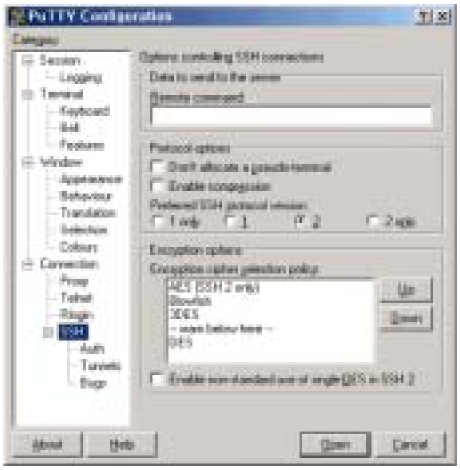
Host Name (or IP address): 192.168.0.1

Port: 22

Protocol: ○ Raw ○ Telnet ○ Rlogin ● SSH

Default Settings
192.168.0.147
192.168.0.225

3. Then, the window below is displayed. Select ‘2’ from the Preferred SSH protocol version.



□ Don't allocate a pseudo-terminal

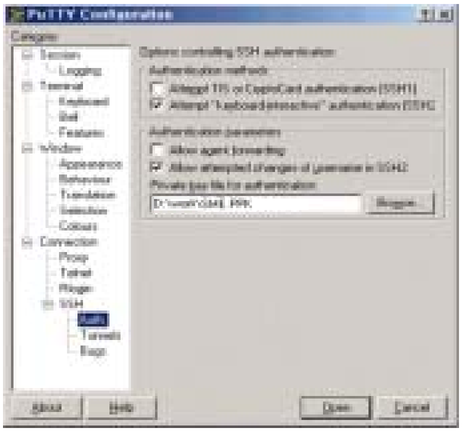
□ Enable compression

Preferred SSH protocol version:
○ 1 only ○ 1 ● 2 ○ 2 only

AES (SSH 2 only)
Blowfish
3DES
-- warn below here --
DES

□ Enable non-standard use of single-DES in SSH 2

4. Select the ‘Auth’ item from the ‘SSH’ item to display the window below: Click the [Browse] button from the ‘Private key file for authentication’ to select Private key file.



Options controlling SSH authentication

Authentication methods

□ Attempt TIS or CryptoCard authentication (SSH1)

☑ Attempt "keyboard-interactive" authentication (SSH2)

Authentication parameters

□ Allow agent forwarding

☑ Allow attempted changes of username in SSH2

Private key file for authentication:

D:\[illegible].PPK

CAUTION

Private Key

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

5. Enter [Open] on the <PuTTY Configuration> window to connect as shown below: Enter the Passphrase used when a private key is encrypted.

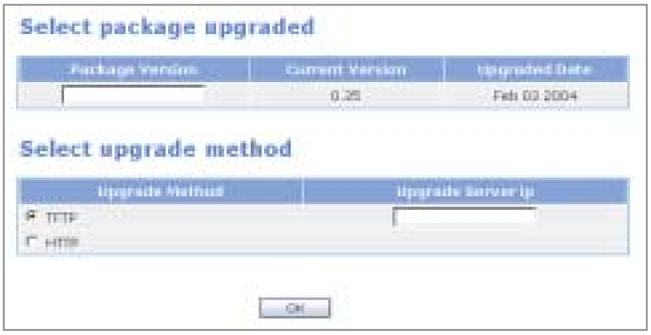
```
Login as: root
Authenticating with public key “rsa-key-20040224”
Passphrase for key “rsa-key-20040224”:
DATASERVER>>
```

Upgrade

Users are allowed to upgrade Kernel, Ramdisk, Application, and DB package on the [Upgrade] menu.

Package

Set the package version and upgrade method on the [Upgrade] → [Package] menu. The upgrade methods are categorized into TFTP type and HTTP type.



Select package upgraded

Package Version	Current Version	Upgraded Date
	0.25	Feb 03 2004

Select upgrade method

Upgrade Method	Upgrade Server Ip
● TFTP ○ HTTP	

NOTE

When setting ADSL/VDSL

The maximum rate of uploading or downloading depends on a feature of ADSL/VDSL MODEM

Upgrade through TFTP

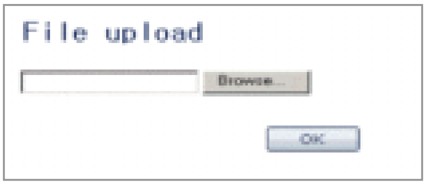
Users are allowed to upgrade the OfficeServ 7200 system with using upgrade file on the TFTP server.

After entering the package version to be updated in the ‘Package Version’ field and select ‘TFTP’ server address, click the [OK] button. If the upgrade is successfully finished, reboot the OfficeServ 7200 system.

Alarm message occurs when the upgrade server is not found or when errors are found during upgrade.

Upgrade Through HTTP

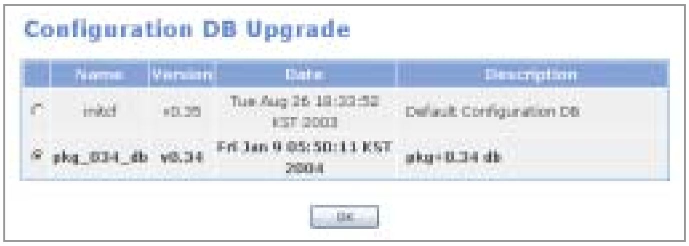
Users are allowed to upgrade the OfficeServ 7200 system by uploading the upgrade file from a terminal where package file to be upgraded exists. Enter the package version to be updated in the ‘Package Version’ field and click the ‘HTTP’ and click the [OK] button to display the window below:



Select the file to be uploaded of a terminal and click the [OK] button to upgrade. After the upgrade ends successfully, the OfficeServ 7200 system reboots.

DB File

Upgrade the DB whose version is not the latest version to the DB whose version is the latest on the [Upgrade] → [DB File] menu.

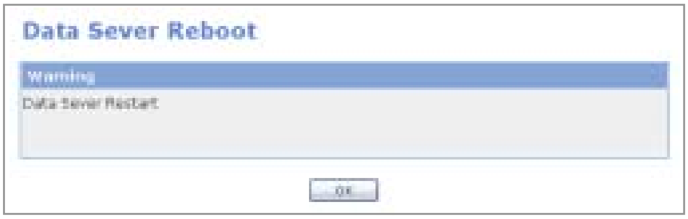

Configuration DB Upgrade

	Name	Version	Date	Description
○	mkd	v0.35	Tue Aug 26 18:33:52 KST 2003	Default Configuration DB
●	pkg_034_db	v0.34	Fri Jan 9 05:50:11 KST 2004	pkg-0.34 db

Select the DB to be upgraded and click the [OK] button to upgrade to the latest version. If the upgrade ends successfully, the Version item is change into the latest version. However, if the upgrade does not end successfully, an alarm message is displayed.

Reboot

Users are allowed to reboot the system on the [Reboot] menu.



Data Sever Reboot

Warning

Data Sever Restart

If the [OK] button is clicked, all services ends and the system reboots. Then, since the Data Server web screen does not operate until the network and services start to be executed, close the web screen and reconnect the system.

ANNEX A. VPN Setting in 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

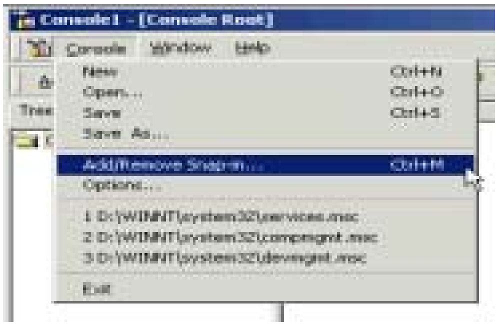
IPSEC and various encryption/authentication algorithm can be used through the installation CD and Windows update in Windows XP/2000. Additionally, LAN to VPN client can be configured through the IPSEC.

NOTE

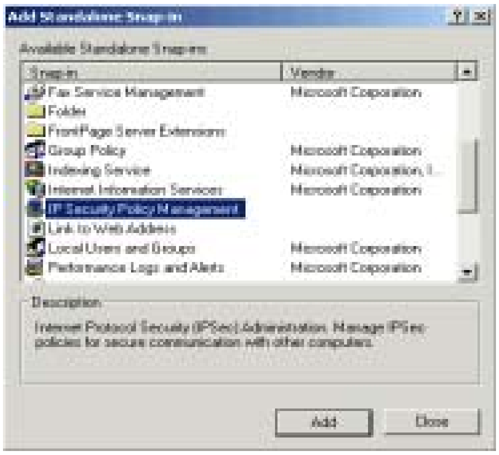
IPSEC Setting in Windows XP/2000

- 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…].


Console1 - [Console Root]
Console
Window
Help
New Ctrl+N
Open... Ctrl+O
Save Ctrl+S
Save As...
Add/Remove Snap-in... Ctrl+M
Options...
1 D:\WINNT\system32\services.msc
2 D:\WINNT\system32\compmgmt.msc
3 D:\WINNT\system32\devmgmt.msc
Exit
Tree

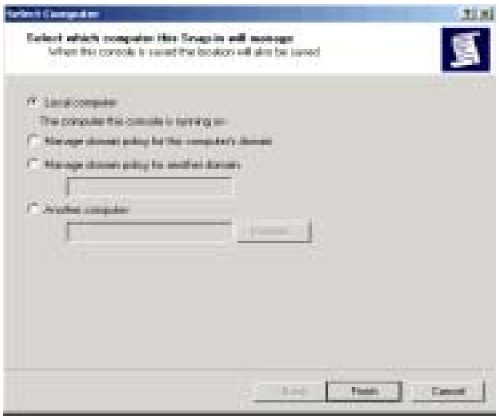
2. In the <Add/Remove Snap-in…>, click [Add] to display the following window: Select 'IP security policy management' in the Add/Remove Snap-in… menu and click [Add].



Snap-in	Vendor
Fax Service Management	Microsoft Corporation
Folder	
FrontPage Server Extensions	
Group Policy	Microsoft Corporation
Indexing Service	Microsoft Corporation, I...
Internet Information Services	Microsoft Corporation
IP Security Policy Management	
Link to Web Address	
Local Users and Groups	Microsoft Corporation
Performance Logs and Alerts	Microsoft Corporation

Internet Protocol Security (IPSec) Administration. Manage IPSec policies for secure communication with other computers.

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

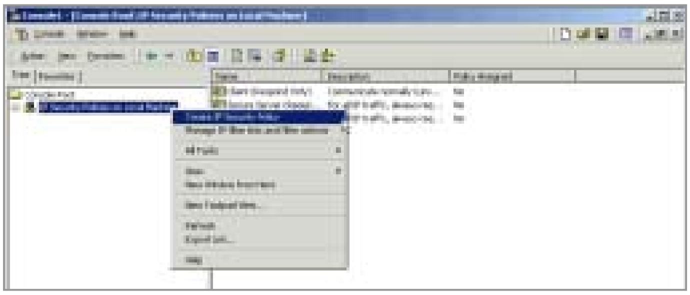


Select Computer

Select which computer this Snap-in will manage
When this console is saved the location will also be saved

● Local computer
The computer this console is running on
○ Manage domain policy for this computer's domain
○ Manage domain policy for another domain:
○ Another computer:

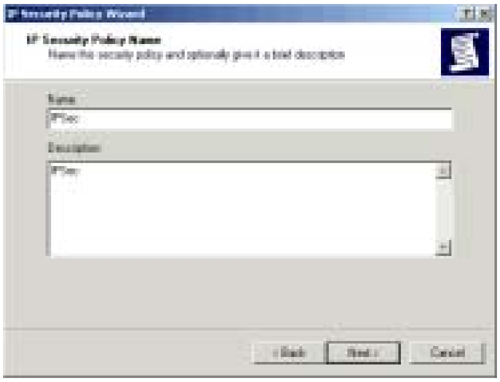
4. Move to the <Console> window. Then, ‘IP Security Policies on Local Machine’ of the ‘Console Root’ is created. Select the item and right click the [Create IP Security Policy] menu.



Console1 - [Console Root\IP Security Policies on Local Machine]

Name	Description	Policy Assigned
Client (Respond Only)	Communicate normally (uns...	No
Secure Server (Require...	For all IP traffic, always req...	No
	For all IP traffic, always req...	No

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



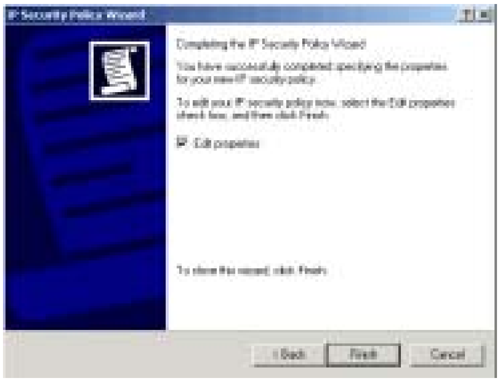
IP Security Policy Wizard

IP Security Policy Name
Name this security policy and optionally give it a brief description

Name:
IPSec

Description:
IPSec

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].



IP Security Policy Wizard

Completing the IP Security Policy Wizard

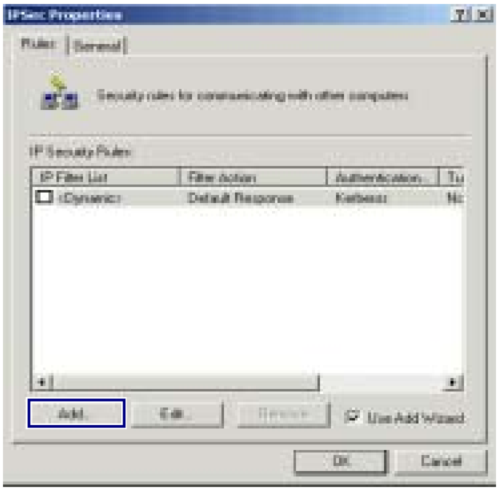
You have successfully completed specifying the properties for your new IP security policy.

To edit your IP security policy now, select the Edit properties check box, and then click Finish.

☑ Edit properties

To close this wizard, 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].



IPSec Properties

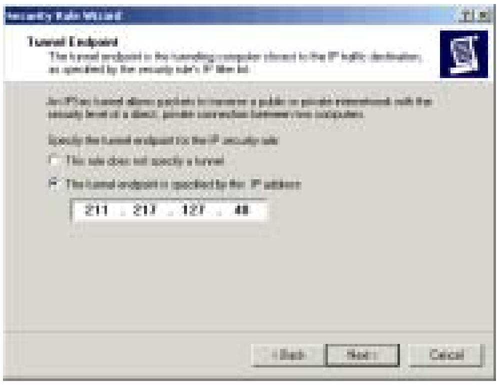
Security rules for communicating with other computers

IP Security Rules:

IP Filter List	Filter Action	Authentication...	Tu
☐ <Dynamic>	Default Response	Kerberos	No

☑ Use Add Wizard

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].



Tunnel Endpoint

The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the security rule's IP filter list.

An IPSec tunnel allows packets to traverse a public or private internetwork with the security level of a direct, private connection between two computers.

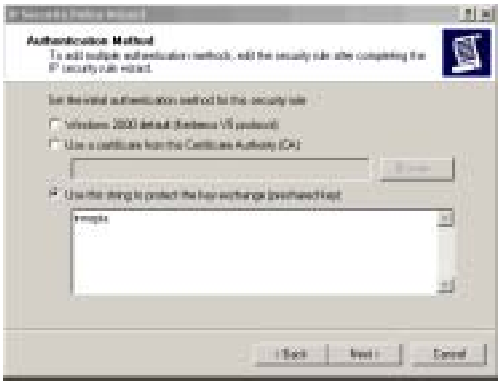
Specify the tunnel endpoint for the IP security rule:

○ This rule does not specify a tunnel

● The tunnel endpoint is specified by this IP address:

211 . 217 . 127 . 48

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].



Authentication Method

To add multiple authentication methods, edit the security rule after completing the IP security rule wizard.

Set the initial authentication method for this security rule:

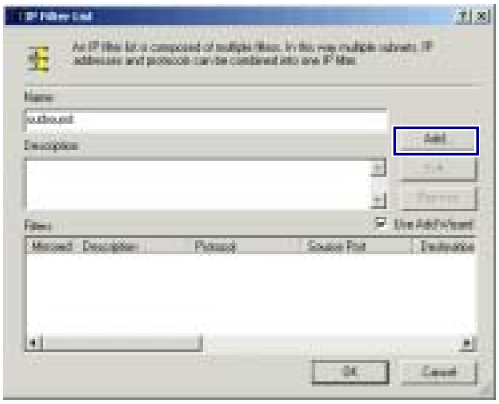
○ Windows 2000 default (Kerberos V5 protocol)

○ Use a certificate from this Certificate Authority (CA):

● Use this string to protect the key exchange (preshared key):

innopia

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



An IP filter list is composed of multiple filters. In this way multiple subnets, IP addresses and protocols can be combined into one IP filter.

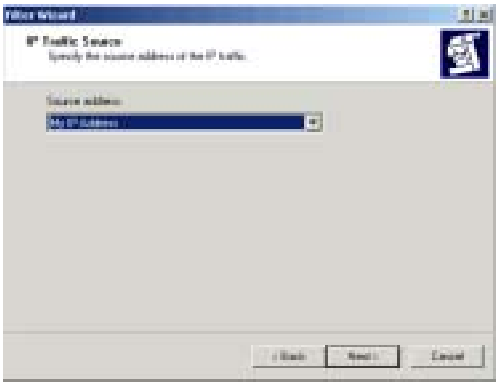
Name:
outbound

Description:

Filters:

☑ Use Add Wizard

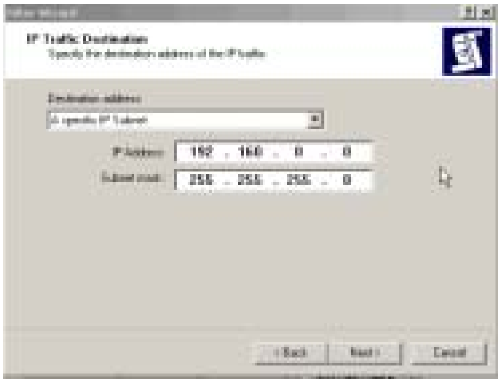
11. Click [Add] on the <IP Filer Wizard> window to display the window below: Select ‘My IP address’ in the Source address field and click [Add].



IP Traffic Source
Specify the source address of the IP traffic.

Source address:
My IP Address

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].



IP Filter Wizard

IP Traffic Destination

Specify the destination address of the IP traffic.

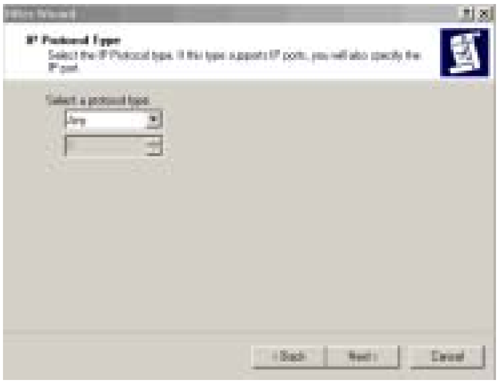
Destination address:

A specific IP Subnet

IP Address: 192 . 168 . 0 . 0

Subnet mask: 255 . 255 . 255 . 0

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



IP Filter Wizard

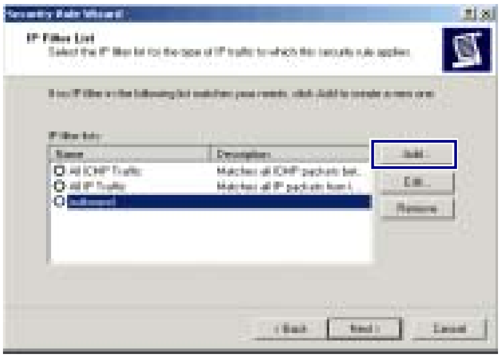
IP Protocol Type

Select the IP Protocol type. If this type supports IP ports, you will also specify the IP port.

Select a protocol type:

Any

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



Security Rule Wizard

IP Filter List

Select the IP filter list for the type of IP traffic to which this security rule applies.

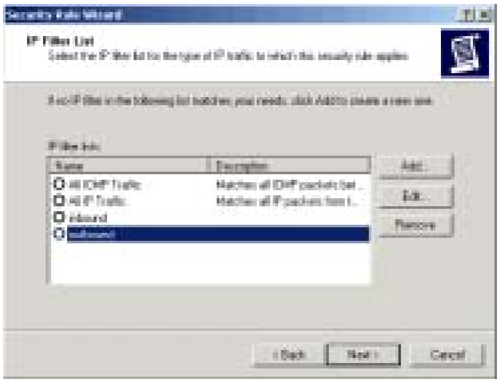
If no IP filter in the following list matches your needs, click Add to create a new one.

IP filter lists:

Name	Description
○ All ICMP Traffic	Matches all ICMP packets bet...
○ All IP Traffic	Matches all IP packets from t...
○ outbound	

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].



Security Rule Wizard

IP Filter List

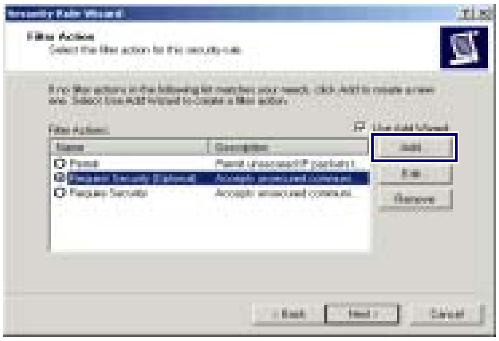
Select the IP filter list for the type of IP traffic to which this security rule applies.

If no IP filter in the following list matches your needs, click Add to create a new one.

IP filter lists:

Name	Description
○ All ICMP Traffic	Matches all ICMP packets bet...
○ All IP Traffic	Matches all IP packets from t...
○ inbound	
○ outbound	

17. Select the ‘Request Security [Optional]’ item and click [Edit].



Security Rule Wizard

Filter Action
Select the filter action for this security rule.

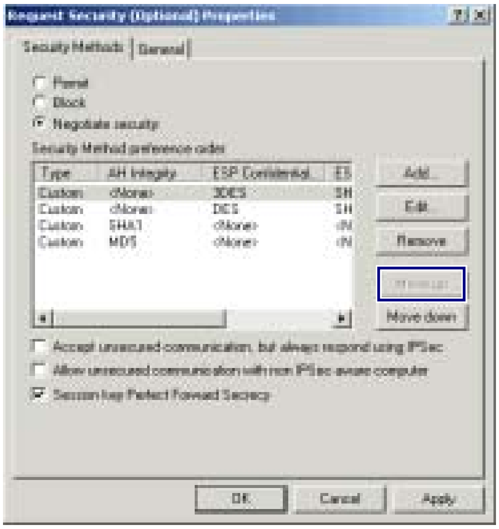
If no filter actions in the following list matches your needs, click Add to create a new one. Select Use Add Wizard to create a filter action.

Filter Actions:

☑ Use Add Wizard

Name	Description
○ Permit	Permit unsecured IP packets t...
● Request Security (Optional)	Accepts unsecured communi...
○ Require Security	Accepts unsecured communi...

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].



Request Security (Optional) Properties

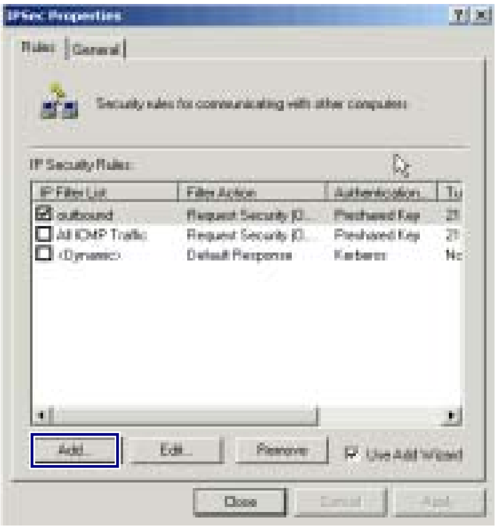
○ Permit
○ Block
● Negotiate security

Security Method preference order:

Type	AH Integrity	ESP Confidential	ES
Custom	<None>	3DES	SH
Custom	<None>	DES	SH
Custom	SHA1	<None>	<N
Custom	MD5	<None>	<N

☐ Accept unsecured communication, but always respond using IPSec
☐ Allow unsecured communication with non IPSec aware computer
☑ Session key Perfect Forward Secrecy

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



IPSec Properties

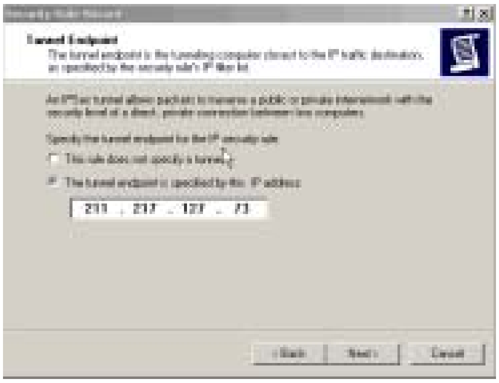
Rules | General

Security rules for communicating with other computers

IP Security Rules:

IP Filter List	Filter Action	Authentication...	Tu
☑ outbound	Request Security (O...	Preshared Key	21
□ All ICMP Traffic	Request Security (O...	Preshared Key	21
□ <Dynamic>	Default Response	Kerberos	Nc

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].



Security Rule Wizard

Tunnel Endpoint

The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the security rule's IP filter list.

An IPSec tunnel allows packets to traverse a public or private internetwork with the security level of a direct, private connection between two computers.

Specify the tunnel endpoint for the IP security rule:

○ This rule does not specify a tunnel

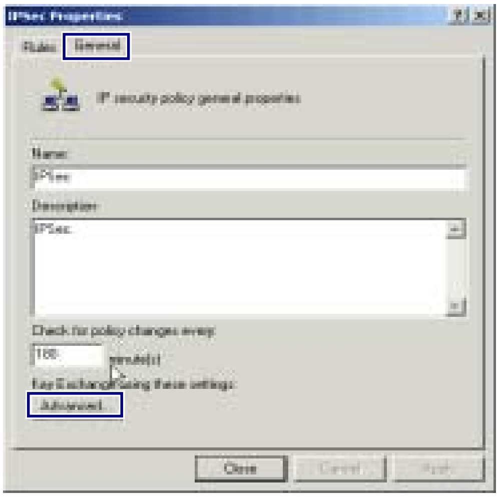
● The tunnel endpoint is specified by this IP address:

211 . 217 . 127 . 73

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].



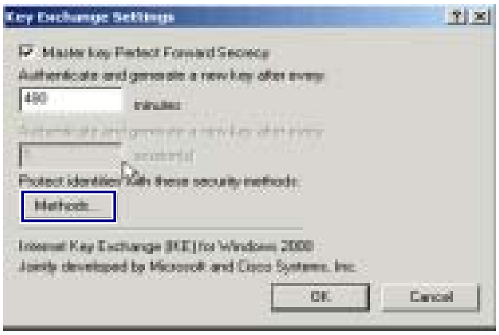
Name:
IPSec

Description:
IPSec

Check for policy changes every:
180 minute(s)

Key Exchange using these settings:

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



☑ Master key Perfect Forward Secrecy

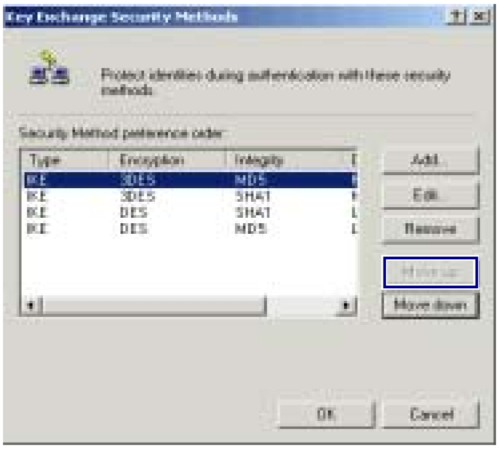
Authenticate and generate a new key after every:
480 minutes

Authenticate and generate a new key after every:
1 session(s)

Protect identities with these security methods:

Internet Key Exchange (IKE) for Windows 2000
Jointly developed by Microsoft and Cisco Systems, Inc.

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].



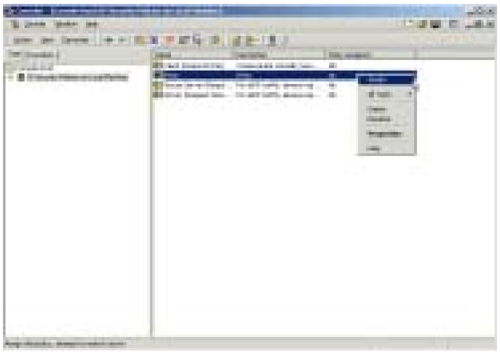
Key Exchange Security Methods

Protect identities during authentication with these security methods.

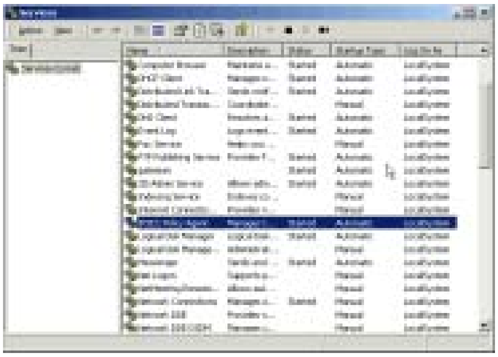
Security Method preference order:

Type	Encryption	Integrity	D
IKE	3DES	MD5	H
IKE	3DES	SHA1	H
IKE	DES	SHA1	L
IKE	DES	MD5	L

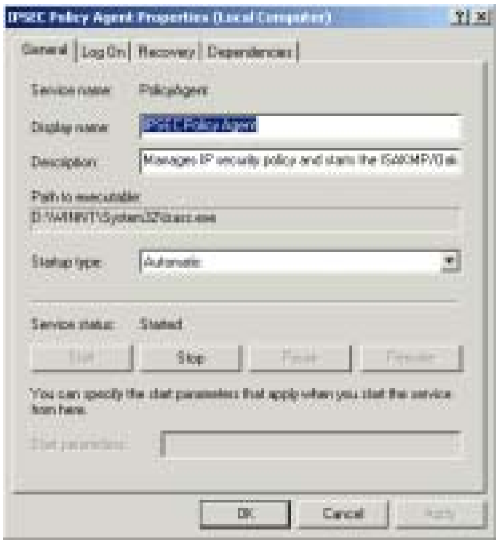
26. Select IP Security Policies on Local Machine’ on the <Console> window. Select the item newly created on the right corner of the window and right-click the [Assign] menu. Then, policy assignment is changed into ‘Yes’.



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:



IPSEC Policy Agent Properties (Local Computer)

General | Log On | Recovery | Dependencies

Service name: PolicyAgent

Display name: IPSEC Policy Agent

Description: Manages IP security policy and starts the ISAKMP/Oak

Path to executable:
D:\WINNT\System32\lsass.exe

Startup type: Automatic

Service status: Started

Start | Stop | Pause | Resume

You can specify the start parameters that apply when you start the service from here.

Start parameters:

OK | Cancel | Apply

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.

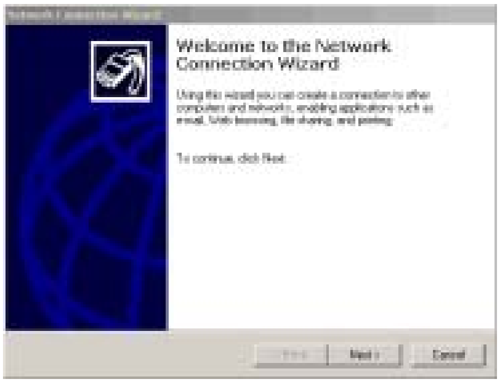
```
C:\>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

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

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

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].



Network Connection Wizard

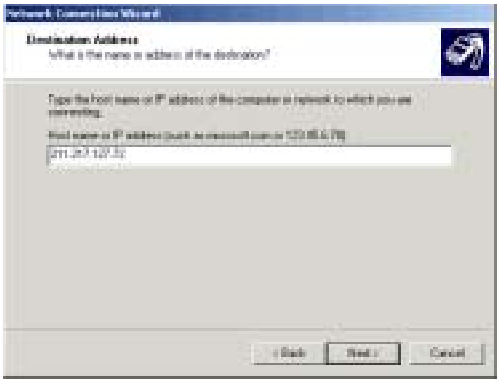
Welcome to the Network Connection Wizard

Using this wizard you can create a connection to other computers and networks, enabling applications such as e-mail, Web browsing, file sharing, and printing.

To continue, click Next.

© SAMSUNG Electronics Co., Ltd.

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.



Network Connection Wizard

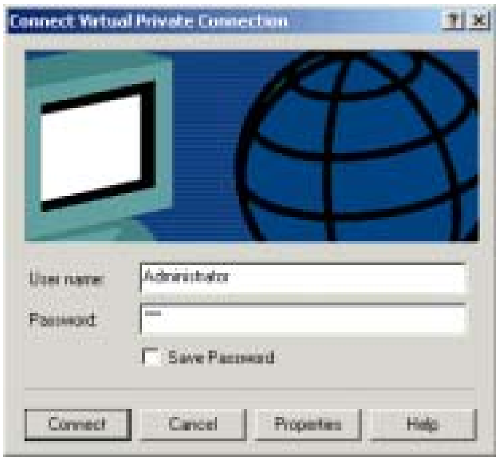
Destination Address

What is the name or address of the destination?

Type the host name or IP address of the computer or network to which you are connecting.

Host name or IP address (such as microsoft.com or 123.45.6.78): 211.207.127.32

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.



Connect Virtual Private Connection

User name: Administrator

Password: ****

□ Save Password

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

ANNEX B. ABBREVIATION

A

ALG	Application Level Gateway
AH	Authentication Header
ARP	Address Resolution Protocol

C

CTI	Computer Telephony Integration

D

DHCP	Dynamic Host Configuration Protocol
DNAT	Destination Network Address Translation
DNS	Domain Name Server
DRR	Deficit Round Robin

E

ESP	Encapsulating Security Payload

H

HDLC	High-level Data Link Control

I

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

L

LAN	Local Area Network

N

NAT	Network Address Translation
NMS	Network Management System

P

PPP	Point-to-Point Protocol
PPPoE	Point-to-Point Protocol over Ethernet
PPTP	Point to Point Tunneling Protocol
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

V

VLAN	Virtual LAN

OfficeServ 7200

Data Server User Guide