



Enterprise IP Solutions

# OfficeServ 7200

## WIM v1.28 User Manual

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

## **Samsung Telecommunications**

### **Publication Information**

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

### **Copyright 2006-2007**

#### **Samsung Telecommunications America**

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

### **Trademarks**

Enterprise IP Solutions

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

PRINTED IN USA

# INTRODUCTION

---

## Purpose

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

## Document Content and Organization

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

### **CHAPTER 1. Overview of OfficeServ 7200 WIM**

This chapter briefly introduces the OfficeServ 7200 WIM.

### **CHAPTER 2. Installing OfficeServ 7200 WIM**

This chapter describes the installation procedure and login procedure.

### **CHAPTER 3. Using OfficeServ 7200 WIM**

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

### **ANNEX A. VPN Setting in Windows XP/2000**

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

### **ABBREVIATIONS**

Abbreviations frequently used in this document are described.

## Conventions

The following types of paragraphs contain special information that must be carefully read and thoroughly understood. Such information may or may not be enclosed in a rectangular box, separating it from the main text, but is always preceded by an icon and/or a bold title.



### **WARNING**

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



### **CAUTION**

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



### **CHECKPOINT**

Provides the operator with checkpoints for stable system operation.



### **NOTE**

Indicates additional information as a reference.



### **Examples**

Indication that there is a programming example which should be remembered.

## Console Screen Output

- The lined box with ‘Courier New’ font will be used to distinguish between the main content and console output screen text.
- ‘**Courier New**’ font will indicate the value entered by the operator on the console screen.

## Reference

### OfficeServ 7200 General Description

The OfficeServ 7200 General Description introduces the OfficeServ 7200 platform and presents the information necessary to understand the hardware configuration, specification, and system functionality.

### OfficeServ 7200 Installation Manual

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

### OfficeServ 7200 Programming Manual

The OfficeServ 7200 Call Server Programming Manual describes how to program the system using Man Machine Communication (MMC) entries.

## Revision History

EDITION	DATE OF ISSUE	REMARKS
00	04. 2004.	First draft
01	04. 2005.	- Cautions are added, Port Forward, Static NAT, Network DB list, Filtering Service items are added. - Some Function names and Descriptions are modified.
02	04. 2006	Whole contents modification and repletion
03	11. 2006	- 'DB Change'/'supporting BGP' are deleted. - 'Ping utility'/'IDS config'/'SIP ALG config' are modified. - 'Nway Force' field is added. - 'Web Time-out' field of 'Admin Config' is added.
04	06. 2007	Expanded the documentation to include comprehensive Programming examples throughout

# SAFETY CONCERNS

For product safety and correct operation, the following information must be given to the operator/administrator and shall be read before the installation and operation of the OS 7200 WIM Data Server.

## Symbols



### Caution

Indication of a general caution.



### Restriction

Indication for prohibiting an action for a product.



### Instruction

Indication for commanding a specifically required action.



## CAUTION



### **For Security**

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



### **When Setting an IP Range for VPN**

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

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



### **When Setting PPTP in Windows XP/2000**

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



### **When Changing Network Interfaces**

If a network interface (i.e. IP Address, gateway, and subnet mask) is changed while the router is operating, all the IP sessions that are being used through that interface are disconnected.



### **When Using a Web Browser**

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



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

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



#### **Caution Before Operating the IDS Module**

Intrusion alerts of the IDS Module remain in the system log as long as IDS items are set to **[On]** in the **[System] → [Log] → [Configuration]**. If not, the alert will not remain in the log, and if an intrusion occurs and is detected by the Data Server it cannot be confirmed.



#### **When Changing the DB**

If the DB is changed (imported) the OfficeServ 7200 WIM will restart.



#### **When Using a Private Key**

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



#### **When Deleting Internet Temporary Files**

If the WIM software package is upgraded, then The Internet temporary files should be deleted. Select **[Internet Explorer] → [Tools] → [Internet Options]** menu and click the **[Delete Cookies]** and the **[Delete Files]** buttons in **[Internet Temporary Files]** area. If these files are not deleted, the webscreen of Data Server may not be displayed correctly.



# TABLE OF CONTENTS

---

<b>INTRODUCTION</b>	<b>1</b>
Purpose .....	1
Document Content and Organization.....	1
Conventions.....	2
Console Screen Output .....	2
Reference .....	3
Revision History .....	3
<b>SAFETY CONCERNS</b>	<b>4</b>
Symbols.....	4
Caution .....	5
<b>TABLE OF CONTENTS</b>	<b>7</b>
<b>CHAPTER 1. OfficeServ 7200 WIM Overview</b>	<b>10</b>
Introduction to the OfficeServ 7200 .....	10
Introduction to the OfficeServ 7200 Data Modules .....	11
<b>CHAPTER 2. Installing OfficeServ 7200 WIM</b>	<b>15</b>
Software Installation.....	15
WIM Installation .....	16
Getting Started.....	18
<b>CHAPTER 3. Using the OfficeServ 7200 WIM Data Server</b>	<b>20</b>
<b>Network Menu</b> .....	<b>21</b>
Network .....	22
NLB.....	38
Utility.....	40
<b>Firewall Menu</b> .....	<b>42</b>
NAT .....	43
Firewall .....	50

<b>Port Menu</b> .....	<b>59</b>
Port .....	60
VLAN .....	65
MAC .....	71
<b>Layer2 Menu</b> .....	<b>73</b>
RSTP .....	74
Port Aggregation .....	78
GVRP .....	80
IGMP Snooping .....	83
Authentication .....	86
<b>Layer3 Menu</b> .....	<b>89</b>
General .....	90
Configuration .....	91
List .....	100
Status .....	106
<b>IPMC Menu</b> .....	<b>107</b>
General .....	108
Configuration .....	109
Status .....	117
<b>QoS Menu</b> .....	<b>119</b>
Group .....	120
Policy .....	133
Management .....	135
Ingress .....	136
<b>Status Menu</b> .....	<b>137</b>
Connection .....	138
Statistics .....	139
Monitoring .....	140
Services .....	142
<b>VPN Menu</b> .....	<b>144</b>
IPSec .....	145
L2TP .....	153
PPTP .....	156
Status .....	158
<b>IDS Menu</b> .....	<b>159</b>
IDS Config .....	160
<b>VoIP Service Menu</b> .....	<b>172</b>
VoIP Service Configuration .....	174
External Server .....	177
DHCP Server .....	177
DHCP Relay Agent .....	184

VoIP NAPT.....	185
SIP ALG.....	187
<b>System Menu .....</b>	<b>190</b>
SNMP .....	191
DB Config.....	194
Admin Config.....	195
Log.....	197
Time Configuration.....	199
Upgrade.....	201
Appl Server.....	201
Reboot.....	202
<b>My Info Menu.....</b>	<b>203</b>
<hr/>	
<b>ANNEX A. VPN Setting for Windows XP/2000</b>	<b>204</b>
IPSec Setting.....	204
PPTP Setting.....	217
<hr/>	
<b>ABBREVIATION</b>	<b>219</b>

# CHAPTER 1. OfficeServ 7200 WIM Overview

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

## Introduction to the OfficeServ 7200

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

With the WIM and PLIM Data Modules, the OfficeServ 7200 provides network functions such as routing, switching, Power Over Ethernet, Quality of Service, and network security in a single converged solution.

This document describes the data and routing capabilities of the OfficeServ 7200 WIM Data Server.



NOTE

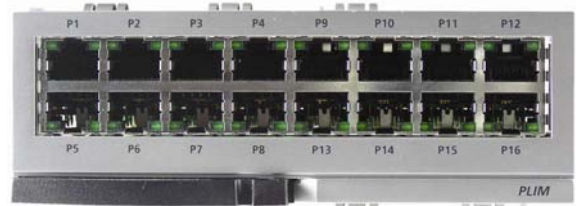
### Structure of OfficeServ 7200

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

# Introduction to the OfficeServ 7200 Data Modules



*WIM Module*



*PLIM Module*

The OfficeServ 7200 WIM Data Server provides the following functionality:

## Unmanaged Switch

- The PLIM/LIM switch performs the function of a layer 2 Internet switch as well as the Learning Bridge function based on the MAC address filtering and forwarding algorithm.
- The PLIM/LIM module provides 16 LAN ports per module. Each port is 10/100 Base T, auto sending, full duplex. OS 7200 can support up to 8 unmanaged LIM/PLIMs.
- The PLIM also offers Power over Ethernet (PoE) to all IEEE 801.3af compliant devices

## Managed Switch

When the PLIM/LIM is installed in slot 2 with a WIM in slot 1, it can function as a managed switch by using the LAN interface on the WIM. The OfficeServ 7200 supports 1 managed PLIM/LIM.



NOTE

### Managed Switch in OfficeServ 7200

There can only be one managed PLIM/LIM switch in the OfficeServ 7200 system.

As a managed switch, the following features are supported:

- 802.1D Spanning Tree – The switch configures and processes the forwarding tree based on the spanning tree algorithm to prevent a packet forwarding loop in the switch.
- Layer 2 802.1p Packet Priority QoS – The switch extracts the priority field from the Ethernet frame configured according to the 802.1p specification standard, and discriminatively processes the frame according to the priority of the specified operation. The switch then maps packets to a designated queue. Up to 2 output queues, Low and High, are supported per egress port with queuing type of Weighted Round Robin or All High before Low. For devices that do not support 802.1p, OS 7200 LIM can be configured to create an enforceable priority.

- Supports Virtual LAN (VLAN) – The Virtual Local Area Network (VLAN) groups the related equipment by the work group according to the LAN operational policy regardless of the location of the user equipment. VLAN removes the effects of unnecessary broadcasting packets and configures a stable switching subnet only for the corresponding group by separating and processing the group in the virtual LAN. The VLAN can be configured based on the switch port, MAC address, and 802.1Q tag.
- IGMP Snooping – IGMP Snooping provides a method for intelligent forwarding of multicast packets within a layer 2 broadcast domains. By snooping IGMP registration information, a distribution list of work stations is formed that determines which end-stations will receive packets with a specific multicast address.
- 802.3x Layer 2 Flow Control – Flow control is performed according to the value set for incoming rate and/or outgoing rate. Limiting the rate at which a port can receive or send traffic is used to ease congestion on bottlenecks in the network and provide simple prioritization when the network is busy.

### Router Functions

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

## Data Network Security

- Outbound and Inbound NAT (Network Address Translation)/PT (Protocol Translation)
  - Controls access to the 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) with automatic updating.
  - Detects and notifies an access to unauthorized areas by the access list.
  - Recognizes and notifies unauthorized packets by applying the basic intrusion rule for packets.
  - Detects and blocks DoS attacks such as SYN flood.
- Virtual Private Network (VPN)
  - Function as a VPN gateway based on PPTP (Point-to-Point Tunneling Protocol), L2TP (Layer 2 Tunneling Protocol), IPSec (Internet Protocol Security protocol)
  - Performs privacy and integrity through VPN tunneling and data encryption.

## Data Network Application

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

## QoS Function

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

## Management Function

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



## CHAPTER 2. Installing OfficeServ 7200 WIM

This chapter describes the installation and the login procedure for OfficeServ 7200 WIM.

### Software Installation

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

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

# WIM Installation

1. Insert the WIM into slot 1 of the OfficeServ 7200 cabinet. If a PLIM/LIM card is to be used as a managed switch then install the PLIM/LIM into slot 2.

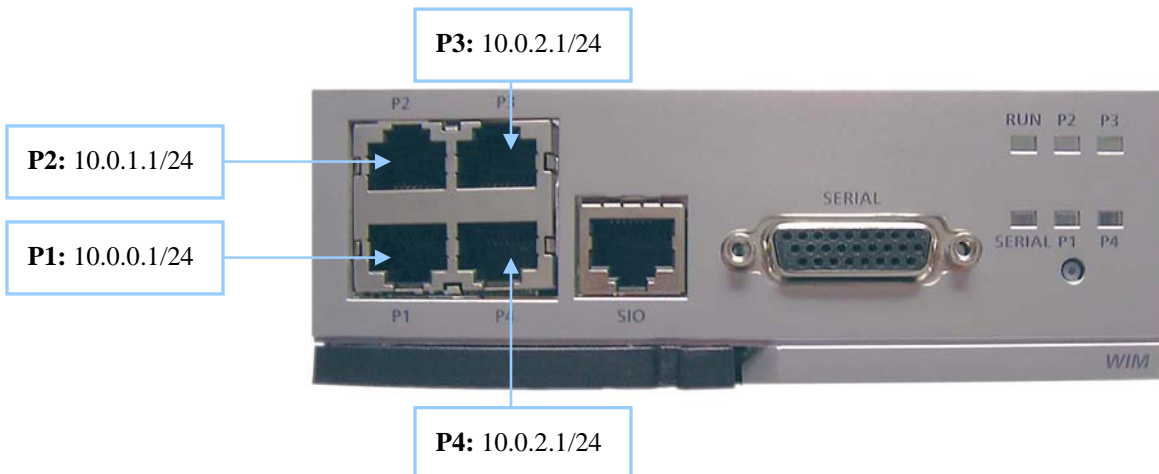
To connect the WIM and PLIM/LIM via the backplane: On the WIM set the connections of the shunt pins #1, 2, 3 and 4 in the direction of the back of the OS 7200 cabinet. Refer to the OfficeServ Installation Manual for more information. Once this is done the P3 Ethernet port is de-activated. If this method is used then do not insert a cable into P3.

To connect the WIM and PLIM/LIM via an Ethernet cable: On the WIM set the connections of the shunt pins #1, 2, 3 and 4 towards the front direction of the WIM then connect the P3 interface of the WIM and a port of the PLIM/LIM together with an Ethernet cable.

2. If a PLIM/LIM is not used then connect a PC to port #1-4 of the WIM module with a cross over cable. Installers will need to configure the TCP/IP settings of the PC to be on the same subnet as the default IP address of the WIM interface being used. The IP address information of each interface is shown in step 3. If a PLIM/LIM is used then connect a PC to any open PLIM/LIM port. Installers will need to configure the TCP/IP settings of the PC to be on the same subnet as the default IP address of the WIM interface P3 shown in step 3.
3. Using Internet Explorer 6.0 or higher navigate to one of the following IP addresses to access the management interface of the WIM.

The default IP value of the WIM interfaces are set as follows:

- Port 1 - 10.0.0.1/24 (<https://10.0.0.1>)
- Port 2 - 10.0.1.1/24 (<https://10.0.1.1>)
- Port 3 - 10.0.2.1/24 (<https://10.0.2.1>)
- Port 4 – 10.0.3.1/24 (<https://10.0.3.1>)





**Caution when using a Web Browser**


The version of Internet Explorer should be 6.0 or higher when logging in and performing maintenance on the WIM. Other web browsers are not supported.

# Getting Started

1. Start Internet Explorer and enter the IP address of the WIM Data Server interface into the address bar. The Security Alert window shown below will appear. Click on the Yes button to proceed:



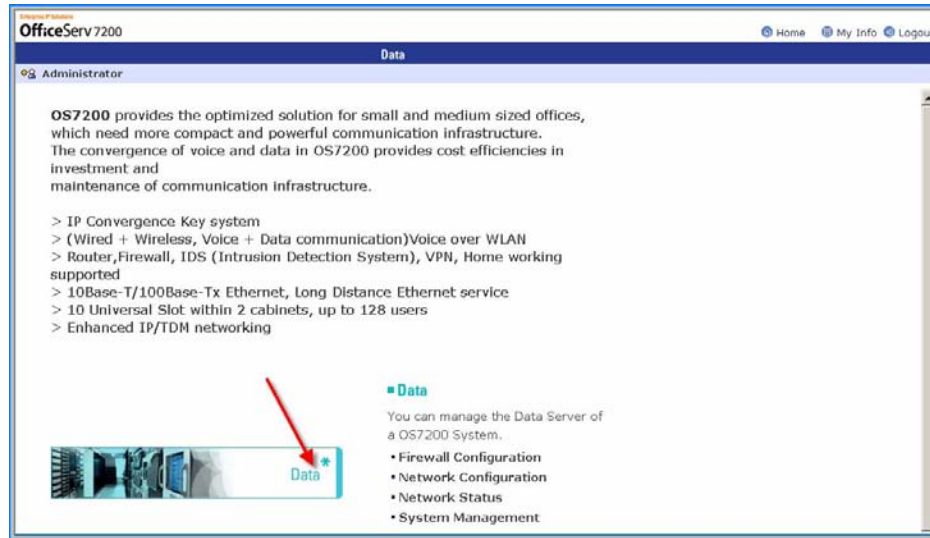
2. The Administrator will now be prompted for a Login ID and Password. Enter the Login ID and Password and then click on the OK button to proceed.

 The WIM login ID is **admin** and the default password is **admin**.

**NOTE**



3. After logging into the WIM Data Module the administrator must click on the Data box to proceed.



4. Once the Data box has been clicked then the WIM menus are displayed in the upper part of the screen. Select each menu to display its submenus on the left section of the screen. For more detailed information for each menu, refer to 'Chapter 3. Using OfficeServ 7200 WIM' of this document.



5. Click the Logout button on the upper right section of the screen to close the connection to the WIM Data Module.

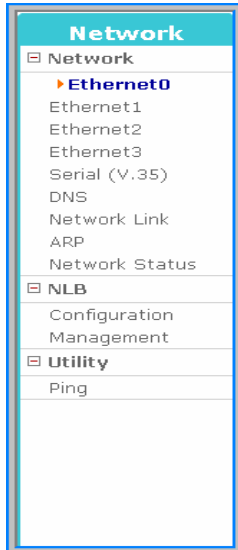
# CHAPTER 3. Using the OfficeServ 7200 WIM Data Server

This chapter describes how to use the menus of the OfficeServ 7200 WIM Data Server. The menu structure of the WIM Data Server is as follows.

<p><b>Network</b></p> <ul style="list-style-type: none"> <li>[-] Network           <ul style="list-style-type: none"> <li>▶ <b>Ethernet0</b> <ul style="list-style-type: none"> <li>Ethernet1</li> <li>Ethernet2</li> <li>Ethernet3</li> <li>Serial (V.35)</li> <li>DNS</li> <li>Network Link</li> <li>ARP</li> <li>Network Status</li> </ul> </li> <li>[-] <b>NLB</b> <ul style="list-style-type: none"> <li>Configuration</li> <li>Management</li> </ul> </li> <li>[-] <b>Utility</b> <ul style="list-style-type: none"> <li>Ping</li> </ul> </li> </ul> </li> </ul>	<p><b>Firewall</b></p> <ul style="list-style-type: none"> <li>[-] <b>NAT</b> <ul style="list-style-type: none"> <li>▶ <b>Management</b> <ul style="list-style-type: none"> <li>Configuration</li> <li>Port Forward</li> <li>Static NAT</li> </ul> </li> <li>[-] <b>Firewall</b> <ul style="list-style-type: none"> <li>Management</li> <li>Configuration</li> <li>Remote Access</li> <li>IP Filtering</li> <li>URL Filtering</li> <li>ICMP Filtering</li> </ul> </li> </ul> </li> </ul>	<p><b>Port</b></p> <ul style="list-style-type: none"> <li>[-] <b>Port</b> <ul style="list-style-type: none"> <li>▶ <b>Configuration</b> <ul style="list-style-type: none"> <li>Statistics</li> <li>MISC</li> <li>QoS</li> </ul> </li> <li>[-] <b>VLAN</b> <ul style="list-style-type: none"> <li>Configuration</li> <li>Port VID</li> <li>Classification</li> </ul> </li> <li>[-] <b>MAC</b> <ul style="list-style-type: none"> <li>Static Address</li> <li>Dynamic Address</li> <li>Filter Address</li> </ul> </li> </ul> </li> </ul>	<p><b>Layer2</b></p> <ul style="list-style-type: none"> <li>[-] <b>RSTP</b> <ul style="list-style-type: none"> <li>▶ <b>Configuration</b> <ul style="list-style-type: none"> <li>Status</li> </ul> </li> <li><b>Port Aggregation</b></li> <li>[-] <b>GVRP</b> <ul style="list-style-type: none"> <li>Configuration</li> <li>Status</li> </ul> </li> <li>[-] <b>IGMP Snooping</b> <ul style="list-style-type: none"> <li>Time Interval</li> <li>Function</li> <li>Forwarding Table</li> <li>Management</li> </ul> </li> <li>[-] <b>Authentication</b> <ul style="list-style-type: none"> <li>Configuration</li> <li>Management</li> </ul> </li> </ul> </li> </ul>	<p><b>Layer3</b></p> <ul style="list-style-type: none"> <li>[-] <b>General</b> <ul style="list-style-type: none"> <li>▶ <b>Routes</b> <ul style="list-style-type: none"> <li>Management</li> </ul> </li> <li>[-] <b>Configuration</b> <ul style="list-style-type: none"> <li>Static</li> <li>RIP</li> <li>RIP Interface</li> <li>OSPF</li> <li>OSPF Interface</li> </ul> </li> <li>[-] <b>List</b> <ul style="list-style-type: none"> <li>Access List</li> <li>Prefix List</li> <li>Route Map</li> <li>Key Chain</li> </ul> </li> <li>[-] <b>Status</b> <ul style="list-style-type: none"> <li>RIP</li> <li>OSPF</li> </ul> </li> </ul> </li> </ul>	<p><b>IPMC</b></p> <ul style="list-style-type: none"> <li>[-] <b>General</b> <ul style="list-style-type: none"> <li>▶ <b>Mroutes</b> <ul style="list-style-type: none"> <li>Management</li> </ul> </li> <li>[-] <b>Configuration</b> <ul style="list-style-type: none"> <li>IGMP</li> <li>DVMRP</li> <li>DVMRP Intf</li> <li>PIM-SM</li> <li>PIM-SM Intf</li> </ul> </li> <li>[-] <b>Status</b> <ul style="list-style-type: none"> <li>IGMP Groups</li> <li>DVMRP</li> <li>PIM-SM</li> </ul> </li> </ul> </li> </ul>
<p><b>QoS</b></p> <ul style="list-style-type: none"> <li>[-] <b>Group</b> <ul style="list-style-type: none"> <li>▶ <b>Port Group</b> <ul style="list-style-type: none"> <li>IP Group</li> <li>Filter Group</li> <li>Class Group</li> </ul> </li> <li><b>Policy</b></li> <li><b>Management</b></li> </ul> </li> <li>[-] <b>Ingress</b> <ul style="list-style-type: none"> <li>Configuration</li> <li>Management</li> </ul> </li> </ul>	<p><b>Status</b></p> <ul style="list-style-type: none"> <li>[-] <b>Connection</b> <ul style="list-style-type: none"> <li>▶ <b>Sessions</b></li> </ul> </li> <li>[-] <b>Statistics</b> <ul style="list-style-type: none"> <li>Devices</li> <li>Protocols</li> </ul> </li> <li>[-] <b>Monitoring</b> <ul style="list-style-type: none"> <li>Current</li> <li>History</li> <li>Process</li> </ul> </li> <li><b>Service</b></li> </ul>	<p><b>VPN</b></p> <ul style="list-style-type: none"> <li>[-] <b>IPSec</b> <ul style="list-style-type: none"> <li>▶ <b>Configuration</b> <ul style="list-style-type: none"> <li>Certificate</li> <li>Management</li> </ul> </li> <li>[-] <b>L2TP</b> <ul style="list-style-type: none"> <li>Configuration</li> <li>Management</li> </ul> </li> <li>[-] <b>PPTP</b> <ul style="list-style-type: none"> <li>Configuration</li> <li>Management</li> </ul> </li> <li>[-] <b>STATUS</b> <ul style="list-style-type: none"> <li>IPSec</li> <li>L2TP/PPTP</li> </ul> </li> </ul> </li> </ul>	<p><b>IDS</b></p> <ul style="list-style-type: none"> <li>[-] <b>IDS Config</b> <ul style="list-style-type: none"> <li>▶ <b>Management</b> <ul style="list-style-type: none"> <li>Log Analysis</li> <li>Configuration</li> <li>Rule Config</li> <li>Mail Config</li> <li>Block Config</li> </ul> </li> </ul> </li> </ul>	<p><b>VoIP Service</b></p> <ul style="list-style-type: none"> <li>[-] <b>Configuration</b> <ul style="list-style-type: none"> <li>▶ <b>SM Interface</b> <ul style="list-style-type: none"> <li>Module Interface</li> <li>Management</li> </ul> </li> <li>[-] <b>External Server</b> <ul style="list-style-type: none"> <li>External FS</li> <li>DIST config</li> </ul> </li> <li>[-] <b>DHCP Server</b> <ul style="list-style-type: none"> <li>Configuration</li> <li>Management</li> <li>VoIP Status</li> <li>Leases Status</li> </ul> </li> <li>[-] <b>DHCP Relay Agent</b> <ul style="list-style-type: none"> <li>Configuration</li> <li>Management</li> </ul> </li> <li>[-] <b>VoIP NAPT</b> <ul style="list-style-type: none"> <li>Status</li> </ul> </li> <li>[-] <b>SIP ALG</b> <ul style="list-style-type: none"> <li>Configuration</li> <li>Management</li> </ul> </li> </ul> </li> </ul>	<p><b>System</b></p> <ul style="list-style-type: none"> <li>[-] <b>SNMP</b> <ul style="list-style-type: none"> <li>Configuration</li> <li>Status</li> <li>Management</li> </ul> </li> <li><b>DB Config</b></li> <li><b>Admin Config</b></li> <li>[-] <b>Log</b> <ul style="list-style-type: none"> <li>Configuration</li> <li>Report</li> <li>Download</li> </ul> </li> <li>[-] <b>Time Configuration</b> <ul style="list-style-type: none"> <li>NTP Config</li> <li>Manual Config</li> <li>Timezone</li> </ul> </li> <li><b>Upgrade</b></li> <li><b>Appl Server</b></li> <li><b>Reboot</b></li> </ul>

# Network Menu

The Network Menu is used to configure the WAN, LAN, and Serial Interfaces, define the DNS server IP Address information, define and modify the ARP list, configure the Network Load balancing function, perform ping tests, and view the Network Status. Simply select the [Network] menu of the OfficeServ 7200 Data Server. The submenus will be displayed in the upper left side of the window as follows:



## Network Menu Description

Menu	Submenu	Description
Network	Ethernet0	Used to setup the Ethernet port P1.
	Ethernet1	Used to setup the Ethernet port P2.
	Ethernet2	Used to setup the Ethernet port P3.
	Ethernet3	Used to setup the Ethernet port P4.
	Serial1(V.35)	Used to setup the V.35 Serial port.
	DNS	Used to setup the domain name servers.
	Network Link	Used to set the speed and transfer method for the Ethernet ports.
	ARP	Used to manage the addition/deletion of ARP.
	Network status	Briefly displays the setup information on all ports.
NLB	Configuration	Used to configure the Network Load Balance function
	Management	Starts and stops the NLB function
Utility	Ping	Used to perform ping tests

## Network

The [Network] menu is used to view and configure the five network interfaces that are built-in to the WIM. This menu is used to set the IP Address information, transfer speed, and transfer mode of each interface. In addition, this menu is used to set the DNS server IP address information and ARP tables.



NOTE

It is recommended that the network interfaces are programmed before any of the other features or options in the WIM Data Server.

## Ethernet Setup

The [Network] → [EthernetX] ( X = 0 through 3) submenus enable the administrator to specify the Ethernet Interface parameters.

Select one of the three Ethernet Interface submenus to display the setup window shown below.

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

The fields that are displayed will vary depending on the type of interface being defined. The details of each interface type are as follows:

- WAN: The following types can be selected for a WAN interface:
  - Static IP: Select Static IP if your Internet service account uses a Fixed IP (Static) IP address assignment.
  - PPPoE: Select PPPoE if your Internet service account uses a PPP over Ethernet login protocol, such as in ADSL account.
  - DHCP: Select DHCP if your Internet service account uses a Dynamic IP address assignment, such as a Cable Modem account.
- LAN: The following types can be selected for a LAN interface:
  - Private: Select to assign the internal network numbers based on private IP address.
  - Public: Select to assign the internal network numbers based on public IP address.
- NONE: Select when the corresponding interface is not used.



Detailed setup information for each interface type are as follows:

### WAN → Static IP

Select the WAN-Static IP category to display the following configuration window.

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

### WAN : Static IP

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

Option	
Gateway	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Default Gateway	<input type="checkbox"/>

### Static WAN Parameters

Parameter	Description
<b>IP</b>	Used to enter the public IP address assigned to the WAN interface
<b>Netmask</b>	Used to enter the Subnet Mask information for the WAN interface
<b>MTU</b>	Maximum Transmission Unit: Leave this field at default unless told to change by Samsung Technical Support
<b>Gateway</b>	Used to enter the public IP address received from the Internet Service Provider (ISP) or the IP address of a router
<b>Default Gateway</b>	Mark the check box in the Default Gateway field to create an entry in the routing table which specifies this address as the default gateway

- **Transparent Proxy:** Proxy-ARP is used when hosts or networks are added in the Transparent Proxy field. Up to 128 Proxy-ARPs can be set in the OfficeServ 7200 system without the change of the existing network. To add entries, click the Add button and enter the following IP address and netmask . To delete entries, select the entry to be deleted and click the Delete button.
- **IP Alias:** Is used to add up to 32 IP addresses. To add entries, click the Add button and enter the following IP address and netmask. To delete entries, select the entry to be deleted and then click the Delete button.

## WAN → Static IP Programming Example



In the example listed below the following information is assigned to the Ethernet1 Interface. The Interface type is set to Static WAN, the IP Address is entered as 10.1.1.2, the Subnet Mask is 255.0.0.0, the Gateway is 10.0.0.1, and the Default Gateway box is checked. Click the OK button on the bottom of the window to save the information.

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

### WAN : Static IP

Ethernet Interface	
IP	10 . 1 . 1 . 2
Netmask	255 . 0 . 0 . 0
MTU	1500 Byte
Option	
Gateway	10 . 0 . 0 . 1
Default Gateway	<input checked="" type="checkbox"/>

By checking the Default Gateway box a default route is entered into the routing table specifying this Gateway as the default route. It is displayed in the WIM Routing Table as **0.0.0.0 [1/0] via 10.0.0.1, eth1**.

### Routes

Type	Network	Entry
S *>	0.0.0.0/0	[1/0] via 10.0.0.1, eth1
C *>	10.0.0.0/8	is directly connected, eth1
C *>	127.0.0.0/8	is directly connected, loopback
C *>	192.168.1.0/24	is directly connected, eth2

## WAN → PPPoE

Select the WAN-PPPoE category to display the following setup window. Enter the ID and Password for the account that is assigned from the ISP .

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

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

## WAN : PPPoE

Authentication	
ID	<input type="text" value="samsung@12.com"/>
Password	<input type="password" value="••••"/>

<input checked="" type="checkbox"/> Option	
Method	<input type="text" value="any"/> ▾
MTU	<input type="text" value="1492"/> byte
DNS	<input checked="" type="radio"/> Auto <input type="radio"/> Manual

OK

## PPPoE WAN Parameters

Parameter	Description
ID	Used to enter the User ID which is supplied by the ISP
Password	Used to enter the Password supplied by the ISP
MTU	Maximum Transmission Unit: Leave this field at default unless told to change by Samsung Technical Support
DNS	Auto: The WIM will automatically receive DNS information from ISP Manual: This connection will use the manually entered DNS server IP addresses configured using the [Network] → [DNS] submenu

## WAN → DHCP

Select the WAN-DHCP category to display the following setup window. The WAN-DHCP information is automatically configured without any special setup fields. The OK button must be clicked in order to complete the setup.

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

## WAN : DHCP

DHCP
Click OK button to start

Option	
Vendor ID	<input type="text"/>
DNS	<input type="radio"/> Auto <input checked="" type="radio"/> Manual

OK

For cable modem service that requires a more detailed setup enter a vendor ID.

## LAN → Private IP

Select the LAN-Private IP category to display the following setup window.

Interface Type	<input type="radio"/> WAN	<input checked="" type="radio"/> LAN	<input type="radio"/> NONE
Protocol Type	<input checked="" type="radio"/> Private	<input type="radio"/> Public	

## LAN : Private IP

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

## IP Alias

<input type="checkbox"/>	IP	Netmask
--------------------------	----	---------

Add Delete

Enter the IP address and the netmask value to be assigned to the Ethernet interface. The IP Alias field is the same as the corresponding input field displayed when selecting WAN → Static IP.

### Private LAN Parameters

Parameter	Description
IP	Used to enter the private IP address assigned to the LAN interface
Netmask	Used to enter the Subnet Mask information for the LAN interface
MTU	Maximum Transmission Unit: Leave this field at default unless told to change by Samsung Technical Support

### LAN → Private IP Programming Example



In the example listed below the following information is applied to the Ethernet2 Interface. The Interface type is set to Private LAN, the IP Address is entered as 192.168.1.1, and the Subnet Mask is 255.255.255.0. Click the OK button on the bottom of the window to save the information.

Interface Type	<input type="radio"/> WAN	<input checked="" type="radio"/> LAN	<input type="radio"/> NONE
Protocol Type	<input checked="" type="radio"/> Private	<input type="radio"/> Public	

### LAN : Private IP

Ethernet Interface	
IP	<input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="1"/> . <input type="text" value="1"/>
Netmask	<input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="0"/>
MTU	<input type="text" value="1500"/> Byte

### IP Alias

<input type="checkbox"/>	IP	Netmask

## LAN → Public IP

Select the LAN-Public IP category to display the following setup window.

Interface Type	<input type="radio"/> WAN	<input checked="" type="radio"/> LAN	<input type="radio"/> NONE
Protocol Type	<input type="radio"/> Private	<input checked="" type="radio"/> Public	

## LAN : Public IP

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

Enter the IP address and the netmask information provided by the ISP. The IP Alias and the Transparent proxy fields are the same as the corresponding input field displayed when selecting WAN → Static IP. After the completion of the setup, click the OK button to save the information.

## NONE

NONE is selected when the corresponding interface is not going to be used.

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

## NONE

Description
Disable network interface

OK

## Setup Details for the Serial0 (V.35) Connection

### Serial Interface Type

The [Network] → [Serial0 (V.35)] submenu enables the administrator to specify the Serial Interface parameters.

Select the V.35 Serial Interface submenu to display the setup window shown below.

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

Select WAN or LAN to begin configuring the Serial Interface, or select NONE if the Serial Interface will not be used.

### Serial Basic

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

### Serial Basic

Command	Argument
Serial Interface Name	Serial0
Physical Line Type	V.35
MTU	<input type="text" value="1500"/> (128~1500, Default: 1500)
Encapsulation	<input checked="" type="radio"/> Cisco-HDLC <input type="radio"/> PPP <input type="radio"/> Frame-Relay

### Serial Basic Parameters

Parameter	Description
<b>Serial Interface Name</b>	Name of the current serial port
<b>Physical Line Type</b>	Physical line type of the current serial port
<b>MTU</b>	Maximum Transmission Unit: Leave this field at default unless told to change by Samsung Technical Support
<b>Encapsulation</b>	Cisco HDLC:
	PPP:
	Frame Relay:

## Cisco-HDLC Configuration

Set the Encapsulation radio button to Cisco-HDLC in order to display the Cisco-HDLC Configuration window. Specify the value for each field, and then click the OK button to store the information.

## Cisco-HDLC Configuration

Command	Argument
Keep-Alive Interval	<input type="text" value="10"/> (1~100, Default: 10)
Keep-Alive Timeout	<input type="text" value="25"/> (1~100, Default: 25)
IP Address	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> / <input type="text"/>
Gateway	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Default Gateway	<input type="checkbox"/> (The Gateway is a Default Gateway)

OK

## Cisco-HDLC Parameters

Parameter	Description
<b>Keep-Alive Interval</b>	Time interval to check Keep-Alive
<b>Keep-Alive Timeout</b>	Time to estimate the failure of Keep-Alive
<b>IP Address</b>	IP Address of the serial port
<b>Gateway</b>	Gateway IP Address(Peer Address) of the serial port
<b>Default Gateway</b>	Mark the check box to set this gateway to default gateway. (This item is displayed only if the WAN radio button is selected.)

## PPP Configuration

Set the Encapsulation radio button to the PPP Protocol in order to display the PPP Configuration table. Specify the value for each field, and then click the OK button to store the configuration.

## PPP Configuration

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

OK



## PPP Configuration Parameters

Parameter	Description
Keep-Alive Interval	Time interval to check Keep-Alive
Max Keep-Alive Count	Count of Keep-Alives to estimate as the disconnection
Authentication	Information for PPP authentication
IPCP Dynamic	Use of Dynamic-IP function to support IPCP
IP Address	IP Address of the serial port
Gateway	Gateway IP Address (Peer Address) of the serial port
Default Gateway	Mark the check box to set this gateway to default gateway. (This item is displayed only if the WAN radio button is selected.)

## Frame-Relay Configuration

Set the Encapsulation radio button to the Frame-Relay protocol in order to display the Frame-Relay Configuration table. Specify the value of each field, and then click the OK button to store the configuration.



NOTE

When a Serial Interface is set up as Frame Relay on the WIM it is a DTE device only. A DCE device is needed on the other end of the connection in order for it to function. It is not possible to do a WIM Frame Relay point-to-point with another WIM without a DCE.

## Frame-Relay Configuration

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

OK

## Frame Relay Parameters

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

Parameter	Description
N392	Count of Keep-Alives to estimate as the disconnection
N393	Buffer size to record success/failure of Keep-Alive. The value of N393 should be bigger than that of N392.

## PVC Interface

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

## PVC Interface

Command	Argument
DLCI	<input checked="" type="radio"/> <input type="text"/> (16~1007) <input type="radio"/> <input type="text"/>
IP Address	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> / <input type="text"/>
Gateway	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Default Gateway	<input type="checkbox"/> (The Gateway is a Default Gateway)
MTU	<input type="text"/> 1500 (128~1500, Default: 1500)

Add

## PVC Interface Parameters

Parameter	Description
DLCI	Number of DLCI (a type of network address)
IP Address	IP Address to be used by PVC
Gateway	Gateway IP Address (Peer Address) of PVC
Default Gateway	Mark the check box to set this gateway to default gateway. (This item is displayed only if the WAN radio button is selected.)
MTU	Maximum Transmission Unit: Leave this field at default unless told to change by Samsung Technical Support

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

## PVC Interfaces

	Interface	Address	Gateway	Def GW	Active	MTU
<input type="checkbox"/>	pvc0/16	192.168.100.2/24	192.168.100.1	no	no	1500
<input type="checkbox"/>	pvc0/17	192.168.101.2/24	192.168.101.1	no	no	1500

Delete

Refresh

## Serial Interface Summary

The Serial Interface Summary table briefly displays the current connection information of the serial port. The following is an example when the Serial connection is defined using the Cisco-HDLC protocol with an IP address of 172.16.0.2/16.

## Serial0 Interface Summary

Serial0 Interface Summary
Interface Serial0
Scope: both
Mode type is EXTERNAL
Protocol type is Cisco-HDLC
Transparent is
Proxyarp is
pppoe_mtu is 1492
pppoe_username is
Pseudo name is
PPPOE client is disabled
Hardware is Unknown
index 5 metric 1 mtu 1500 <UP,POINTOPOINT,RUNNING,NOARP>
DHCP client is disabled.
VRF Binding: Not bound
inet 172.16.0.2/16 pointopoint 172.16.0.1
physical line type is V.35
encapsulation protocol is Cisco HDLC
keepalive interval 10 timeout 25
line protocol is up
input packets 8, bytes 706, dropped 0, multicast packets 0
input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
output packets 7, bytes 154, dropped 0
output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
collisions 0

Refresh

## DNS

Select the [Network] → [DNS] submenu in order to display the following configuration window. Enter the domain name and the IP address information for the DNS server /s. Then click the OK button to store the domain name and the IP address information.

The default DNS information should be deleted. In order to delete a DNS entry select the check box directly to the left of the DNS Server IP Address and then click on the Delete button.

### Static DNS

Domain Name
<input type="text"/>

OK

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

Delete

Name Server Add
<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>

Add

## Network Link

Select the [Network] → [Network Link] submenu to view and set up the transmission speeds and transmission modes for the Ethernet interfaces.

### Network Link Configuration

Command	Argument
Ethernet	Ethernet 0
Negotiation	auto
Speed	100
Duplex	full

OK

### Network Link Status

Ethernet	Type	Link	Negotiation	Speed	Duplex	Mac
Ethernet 0	10/100TX	up	auto	100	full	00:00:f0:12:13:14
Ethernet 1	10/100TX	down	auto	100	full	00:00:f0:12:13:15
Ethernet 2	10/100TX	up	auto	100	full	00:00:f0:12:13:16
Ethernet 3	10TX	up	force	10	half	00:00:f0:12:13:17

Refresh

## Network Link Configuration

Use the Ethernet pull down menu to select the correct Ethernet connection.

Use the Negotiation pull down menu to select **auto** or **force**.

If **auto** is selected the Ethernet Interface speed and duplex type will be automatically selected.

If **force** is selected the administrator can manually define the speed and duplex type.

## Network Link Status Fields

Field	Description
<b>Ethernet</b>	Logical name of each Ethernet Interface
<b>Type</b>	Type of Ethernet Connection
<b>Link</b>	Status is either <b>up</b> or <b>down</b>
<b>Negotiation</b>	Shows setup as auto or force mode
<b>Speed</b>	Transmission bandwidth of the corresponding Ethernet interface
<b>Duplex</b>	Transfer mode of the corresponding Ethernet interface
<b>MAC</b>	MAC addresses of the Ethernet interface

## ARP

The [Network] → [ARP] submenu is used to manage the ARP information for each Ethernet Interface. Within this submenu the administrator can view the current ARP List, delete and add ARP entries, and set the ARP Age Time.

### ARP List

Select the radio button of the Ethernet Interface whose ARP table needs to be managed. The ARP table will be displayed in the ARP List window. Use the Refresh button and the Delete button to update and delete the current ARP table.

### ARP List

Ethernet	<input checked="" type="radio"/> Ethernet0	<input type="radio"/> Ethernet1	<input type="radio"/> Ethernet2	<input type="radio"/> Ethernet3
----------	--	---------------------------------	---------------------------------	---------------------------------

<input type="checkbox"/>	Type	IP	Mac
<input type="checkbox"/>	reachable	216.62.86.129	00:a0:c8:0c:04:bf
<input type="checkbox"/>	reachable	216.62.86.140	00:00:f0:00:00:00

## ARP List Fields

Field	Description
Type	ARP status
IP	IP address of device in ARP table
MAC	Mac address of device in ARP table

## Static ARP Add

Use the Static ARP Add window to manually add ARP entries into the ARP table.

### Static ARP Add

Ethernet	IP	Mac
Ethernet0	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>

Add

## Static ARP Parameters

Parameter	Description
Ethernet	Used to select the Ethernet Interface
IP	Used to enter the IP address of device for ARP table
MAC	Used to enter the Mac address of device for ARP table

## ARP Age Time

The ARP Age Time window is used to setup the ARP Table cycle (at Least 600 sec. unit: sec.) to delete the unused ARP entries from the ARP table.

### ARP Age Time

Time
<input type="text" value="600"/> sec

OK

## ARP Refresh

The ARP Refresh window is used to submit changed ARP information in the ARP table after route or a host information on the network has changed. The host or the route with the destination IP, the Mac with the current source IP is updated into the Ethernet Mac of the OfficeServ 7200 system.

## ARP Refresh

Ethernet	Source IP	Destination IP
Ethernet0	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>

OK

## ARP Refresh Parameters

Field	Description
<b>Ethernet</b>	Used to select the Ethernet to be changed
<b>Source IP</b>	Used to select the IP address to be changed
<b>Destination IP</b>	Used to select the Host or Mac to be changed

## Network Status

Select the [Network] → [Network Status] submenu to display the Network Status window. The window displays the network information of each Ethernet interface.

## Network Status

Category	Usage	Protocol	IP	Netmask	Gateway
Ethernet 0	EXTERNAL	STATIC	216.62.86.142	255.255.255.128	216.62.86.1
Ethernet 1	INT_PRIV	STATIC	10.0.1.1	255.255.255.0	
Ethernet 2	INT_PRIV	STATIC	192.168.2.1	255.255.255.0	
Ethernet 3	INT_PRIV	STATIC	10.0.3.1	255.255.255.0	
Serial	INT_PRIV	SyncPPP	10.1.1.2	255.255.255.252	10.1.1.1

Name Server	
Server 1	168.126.63.1
Server 2	168.126.63.2

Domain

## NLB

The WIM supports 5 external WAN interfaces. It can distribute network or Internet access traffic through each WAN interface by using the NLB function. For effective access and traffic balancing the system uses the 'Weighted Round Robin' method. The NLB submenu is used for the setup of the Network Load Balancing function and Failover function.

### Configuration

In order to begin configuring the NLB function select the [Network] → [NLB] → [Configuration] submenu.

#### Network Load Balance Configuration

Category	Settings
NLB Weight	eth0 <input type="text" value="1"/> eth1 <input type="text" value="2"/>
NAT Status	Enable

#### Network Load Balance Configuration

The Network Load Balance Configuration can be used when at least two of the WIM interfaces are configured as WAN. For example, if a T1 private line and ADSL line are selectively connected to the Ethernet 0 Interface (eth0) and the Ethernet 1 Interface (eth1), the higher weighted value should be given to the ADSL line because its bandwidth is relatively bigger. In this way, the load balancing feature is optimized according to the performance of the external network medium. The WIM also utilizes a Failover function. This means if there are multiple WAN interfaces set up and using NLB, if one of the interfaces go down the other WAN interface will automatically be used as the back up path.

- **NLB Weight:** A relatively higher load will be distributed on the line of the external interface that has a higher numerical value. The weighted value for each external interface should be the greatest common divisor (minimum irreducible unit).



## Static Configuration

Along with the Network Load Balance Configuration, the Static Configuration window is used to pass data through a specific WAN interface by separately specifying the traffic session to satisfy a specific condition. The auto failover feature is also set here. In the following window the entries can be added or deleted by clicking the Add or the Delete button. If an entry of 0.0.0.0 is entered for the IP address field and all '0s' in the port field then it will indicate all IP addresses all port numbers.

## Static Configuration

	Source	Destination	Traffic Distribution
IP	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	Protocol <input type="text" value="all"/>
Mask	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	Gateway <input type="text" value="default gate"/>
port	<input type="text"/> - <input type="text"/>	<input type="text"/> - <input type="text"/>	Backup <input type="text" value="default gate"/>

## Static Configuration Parameters

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

If 0.0.0.0 is input as the IP address and netmask then any IP address is allowed as the source and the destination IP address. In addition, a value of '0s' as the source port number means that any port number is allowed as the source port number.

## Network Load Balance Management

The Network Load Balance Management window is used for starting and stopping the NLB service.

### Network LoadBalance Management

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

## Utility

The WIM is able to do both basic ping and extended ping tests. Select the [Network] → [Utility] → [Ping] submenu to access the Ping function.

## Ping

The Ping window is a table which is used to specify and execute the Ping test. When an administrator selects this submenu the following configuration window is displayed.

### Ping

Category	Configuration
Destination IP Address	<input checked="" type="radio"/> <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
	<input type="radio"/> <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
	<input type="radio"/> <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Option	
Source Address	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Packet Size	<input type="text"/>
Retry Count	<input type="text"/>
Time to Live	<input type="text"/>
MTU Discovery Hint	none <input type="button" value="v"/>

### Ping Parameters

Parameter	Description
<b>Destination IP Address</b>	Used to enter the destination IP address for the Ping test
<b>Source Address</b>	Used to set the IP address of the interface for the Ping test
<b>Packet Size</b>	Used to set the packet size to be transmitted
<b>Retry Count</b>	Used to set the retry count. If it set to '0', there is no retry. Max is 3

Parameter	Description
Time to Live	Used to set the TTL value.
MTU Discovery Hint	None:
Selects the Path MTU Discovery method	Do: Uses PMTU but does not treat. In short, packet fragmentation does not occur
	Don't: Does not use PMTU at all. Since it does not set the DF field, the fragmentation may occur in remote site
	Want: Uses PMTU and treats appropriately. In short, if the packet size is longer than MTU, the packet fragmentation occurs

Enter the destination IP (and any excluded ping parameters if needed) then click the Run button.

Only one destination IP can be tested at a time and the radio button of the IP Address to be tested must be checked. The radio button of the destination IP Address on the top of the list is set by default.

## Ping

Category	Configuration
Destination IP Address	<input checked="" type="radio"/> 192 . 168 . 1 . 1
	<input type="radio"/> . . . .
	<input type="radio"/> . . . .

Option	
Source Address	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Packet Size	<input type="text"/>
Retry Count	<input type="text"/>
Time to Live	<input type="text"/>
MTU Discovery Hint	none <input type="button" value="v"/>

Log
PING 192.168.1.1 (192.168.1.1) from 192.168.1.1 : 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=0.129 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=0.020 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=0.018 ms
---
--- 192.168.1.1 ping statistics ---
3 packets transmitted, 3 received, 0% loss, time 1999ms
rtt min/avg/max/mdev = 0.018/0.055/0.129/0.052 ms

# Firewall Menu

The Firewall menu is used to configure port forwarding, static NAT rules, and all firewall functions. Select the **[Firewall]** menu and the submenus will be displayed in the upper left side of the window as follows:



## Firewall Menus Description

Menu	Submenu	Description
<b>NAT</b>	Management	Used to enable or disable the NAT function
	Configuration	Used to set up the private IP sharing function
	Port Forward	Used to set up the port forwarding function
	Static NAT	Used to set up the static forwarding function
<b>Firewall</b>	Management	Used to enable or disable the Firewall function
	Configuration	Used to set up the Filtering policies
	Remote Access	Used to permit or block the remote access to the system
	IP Filtering	Used to block specific IP Address access
	URL Filtering	Used to block web access to specified web sites using key words
	ICMP Filtering	Used to block ICMP Reply (Ping, Tracert, etc.) of the WIM Interfaces

# NAT

NAT (Network Address Translation) is an Internet standard that enables a local-area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. Select the [NAT] → [Management] submenu to begin configuring NAT.



NOTE

When a WIM is initially installed data traffic from a LAN device will not be allowed out over a WAN Interface. The Private Network Configuration or Static NAT must be set up to allow this functionality.

## Management

This submenu is used to either enable or disable the NAT feature. Select the “Enable” or “Disable” radio button and then click on the OK button to set.

### NAT Enable/Disable

Setting

Enable  Disable

OK

### NAT Parameter Description

Setting	Description
Enable	Used to enable the NAT function
Disable	Used to disable the NAT function

## Configuration

This submenu is used by the administrator to allow a network configured with private IPs to send data through a WAN interface. A private IP Address must be transferred to The Internet through an authenticated IP Address.

### Basic Mode

This window is used to configure a network by using the minimum number of options.



In the following Basic Mode example the WAN Interface is being set with an IP Address of 10.0.1.1, the Interface is being set to Ethernet1, and all Inside private IP Addresses are being allowed out over the WAN interface to any destination. Once the information is entered click on the OK button to apply. Every user on the LAN is now allowed to go out on WAN 10.0.1.1

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

## Private Network Configuration

Category	Configuration				
WAN IP(Intf.)	10	0	1	1	Not Use
	<input type="checkbox"/> Dynamic IP	PPPoE			
Inside	0	0	0	0	Not Used
Outside	0	0	0	0	Ethernet0
Index No.	1				Ethernet1
					Ethernet2
					Ethernet3
					Serial0

OK

### Basic NAT Parameter Description

Category	Description	
<b>WAN IP</b>	Used to set a general IP Address. Select the dynamic IP box and then use the pull down menu to select PPPoE or DHCP if the interface is acquiring a dynamic IP from an Internet Service Provider (ISP).	
<b>Inside</b>	Used to enter the NAT LAN (internal network) information.	The / symbol is used to specify an entire network or subnet exiting a WAN Interface Example: 192.168.1.0/24 This allows every device within the 192.168.1.0 network to go out over the WAN interface
		The – is used to specify a range of IP Addresses exiting a WAN Interface Example: 192.168.1.50 - 60
		The * symbol is used to allow all possible LAN IP Addresses to go out over the WAN Interface Example: 0.0.0.0 *
<b>Outside</b>	Used to enter the NAT WAN (external network) information	The / symbol is used to specify a public Subnet as a valid destination Example: 12.168.1.0/24 This allows the destination to be any device within the 12.168.1.0 network
		The – is used to specify a range of IP Address destinations Example: 12.168.1.50 - 60
		The * symbol is used to allow all destination IP Addresses Example: 0.0.0.0 *
<b>Index No</b>	Location of the NAT rule.	

## Advanced Mode

This window is used by the administrator to select and set up the port/s or protocol/s that are not included in the Basic Mode configuration.



In this Advanced Mode example the WAN Interface field is set with an IP Address of 10.0.1.1, the Interface is being set to Ethernet1, and all Inside private IP Addresses in the defined range (192.168.1.50 thru 192.168.1.75) are being allowed out over the WAN interface to any destination over port 80 on all protocols. Once the information is entered click on the OK button to apply. Now users within the IP Address range of 192.168.1.50-75 are allowed out on WAN 10.0.1.1 using port 80 only.

Config Mode	<input type="radio"/> Basic Mode	<input checked="" type="radio"/> Advanced Mode
Category	Configuration	
WAN IP (Intf.):Port	10 . 0 . 1 . 1	Etherne [ ] ; [ ]
Inside	<input type="checkbox"/> Dynamic IP	PPPo [ ] Etherne [ ]
Outside	192 . 168 . 1 . 50	- [ ] 75
Port	<input type="radio"/> Define	all [ ] <input checked="" type="radio"/> User [ 80 ]
Protocol	<input type="radio"/> Range	[ ] ~ [ ] <input type="radio"/> Multi [ ] , [ ]
Index No.	all [ ]	
	1 [ ]	

## Advanced NAT Parameter Description

Parameter	Description
Port	Used to define the specific IP port/s for the outside destination.
Protocol	Select TCP, UDP, or all (both tcp and upd) protocol.

The administrator can view the current status of the NAT rules by using the **[Firewall] → [NAT] → [Configuration]** submenu. The Configuration List is shown on the bottom of the window.

## Configuration List

<input type="checkbox"/>	No	WAN IP	Inside	Outside	Port	Proto
<input type="checkbox"/>	1	10.0.1.1(eth1)	192.168.1.50-192.168.1.75	0.0.0.0/0	80	udp
<input type="checkbox"/>	2	10.0.1.1(eth1)	192.168.1.50-192.168.1.75	0.0.0.0/0	80	tcp
<input type="checkbox"/>	3	10.0.1.1(eth1)	0.0.0.0/0	0.0.0.0/0	all	all

Delete

If a NAT rule must be deleted then check the box to the left of the NAT rule and then click the delete button. In order to delete all NAT rules click on the box on the top left of the Configuration List then click on the delete button.

## Port Forward

Port Forwarding is the act of forwarding a network port from one network to another. This technique can allow an external user to reach a port on a private IP address (inside a LAN) from the outside via a NAT-enabled router.

Port forwarding allows remote computers (e.g. public machines on The Internet) to connect to a specific computer within a private LAN.

The administrator can begin to configure the port forwarding feature on the WIM by using the [Firewall] → [NAT] → [Port Forward] submenu.

### Basic Mode



This window is used to configure port forwarding by using the minimum number of options.

In the Basic Mode example listed below the Inside IP Address is 192.168.1.149, the Outside IP is set to any, and the WAN IP is set to 10.0.1.1

Config Mode     Basic Mode     Advanced Mode

### Private Network Port Forward

Category	Configuration
Inside IP	192 . 168 . 1 . 149
Outside	0 . 0 . 0 . 0 * ▾
WAN IP	10 . 0 . 1 . 1 / ▾
Index No.	1 ▾

OK

This means when any external IP device tries to connect to the WAN IP 10.0.1.1 it will be redirected to 192.168.1.149. When using the Basic Mode all network or IP ports and protocols are forwarded. If a specific network port or protocol needs to be defined then the Advanced Mode must be used.



NOTE

If only one WAN IP is being defined use the / symbol without anything in the field to the right of the entry.



## Basic Port Forward Parameter Description

Parameter	Description	
<b>Inside IP</b>	Used to set the Internal IP Address which will be connected to from the outside. The field to the right of this entry is used to specify a different destination network or IP port	
<b>Outside</b>	Used to define the external IP addresses that will be allowed to connect to the Inside IP	The / symbol is used to specify a public IP Address, Public network, or subnet as a valid source Example: 12.168.1.0/24 This allows the source to be any device within the 12.168.1.0 network
		The – is used to specify a range of IP Address sources Example: 12.168.1.50 - 60
		The * symbol is used to allow all possible external IP Addresses as the source IP Example: 0.0.0.0 *
<b>WAN IP</b>	Used to define the WAN IP Address	The / symbol is used to specify a WAN IP Address or Addresses as a valid IP to perform the port forwarding Example: 10.0.1.0/24 This allows the forwarding source to be all WAN Interfaces within the 10.0.1.0 network
		The – is used to specify a range of WAN P Address port forward sources Example: 10.0.1.1 - 2
<b>Index No</b>	Used to set the location of the Port Forward rule.	

## Advanced Mode

This window is used by the administrator to select and set up Port Forwarding for a port or protocol that is not included in the Basic Mode configuration.



In the Advanced Mode example listed below the internal or inside IP Address destination is 192.168.1.150, the external or Outside device must come from an IP Address on the 12.2.2.0 network, the WAN IP is set to 10.0.1.1, ports 6000 through 6100 are defined, and protocol tcp is used.

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

## Private Network Port Forward

Category	Configuration
Inside IP:Port	192 . 168 . 1 . 150 : <input type="text"/>
Outside	12 . 2 . 2 . 0 / <input type="text"/> 24
WAN IP	10 . 0 . 1 . 1 / <input type="text"/>
Port	<input type="radio"/> Define <input type="text"/> all <input type="radio"/> User <input type="text"/> <input checked="" type="radio"/> Range <input type="text"/> 6000 ~ <input type="text"/> 6100 <input type="radio"/> Multi <input type="text"/> , <input type="text"/> <input type="text"/> , <input type="text"/>
Protocol	tcp <input type="text"/>
Index No.	1 <input type="text"/>

OK

This means when an external IP device from the 12.2.2.0 network tries to connect to the WAN IP Address 10.0.1.1 on network ports 6000 through 6100 and protocol tcp, it will be redirected to 192.168.1.150 on network ports 6000 through 6100 and protocol tcp.

## Advanced Port Forward Parameter Description

Parameter	Description
<b>Port</b>	Used to define the specific IP port/s for the destination.
<b>Protocol</b>	Select TCP, UDP, or all (both tcp and upd) protocol.

The administrator can view the current status of the Port Forwarding Rules using the **[Firewall] → [NAT] → [Port Forwarding]** submenu. The Configuration List is shown on the bottom of the window.

## Configuration List

<input type="checkbox"/>	No	Inside IP	Outside	WAN IP	Port	Proto
<input type="checkbox"/>	1	192.168.1.150	12.2.2.0/24	10.0.1.1	6000~6100	tcp
<input type="checkbox"/>	2	192.168.1.149	0.0.0.0/0	10.0.1.1	all	all

Delete

If a Port Forward rule must be deleted then check the box to the left of the rule and then click the delete button. In order to delete all Port Forward rules click on the box on the top left of the Configuration List then click on the delete button.

## Static NAT

This is a type of NAT in which a private IP address is mapped directly to a public IP address, where the public address is always the same IP address (i.e., it has a static address). This allows an internal host, such as a Web server, to have an unregistered (private) IP address and still be reachable over The Internet. This is also referred to as 1-to-1 NAT.

The administrator can begin configuring the static NAT feature on the WIM by using the [Firewall] → [NAT] → [Static NAT] submenu.



In this example the inside (internal network) IP Address is 192.168.1.50, the WAN (external network) IP Address is 10.0.0.1, network ports 1 thru 65000 are selected for both the inside and WAN IPs, and all protocols are selected. Click the OK button to save the change.

## Static NAT

Category	Configuration
Inside IP:Port	192 . 168 . 1 . 50 : 1 ~ 65000
WAN IP:Port	10 . 0 . 1 . 1 : 1 ~ 65000
Protocol	all
Index No.	1

OK

This means that when an external IP device tries to connect to the WAN IP Address 10.0.1.1 on network ports 1 through 65000 and any protocol, it will be redirected to 192.168.1.50 on network ports 1 through 65000 and any protocol.

## Static NAT Parameter Description

Parameter	Description
Inside IP: Port	Used to set an inside IP Address and network ports

Parameter	Description
WAN IP: Port	Used to set the WAN IP Address and network ports
Protocol	Used to select the protocol type.
Index No	Used to set the location of the Static NAT rule

## Firewall

The WIM firewall is software based and configured to permit or deny connections from The Internet or other networks depending of the organization's security policies. Select the [Firewall] → [Firewall] → [Management] submenu to begin configuring the firewall.

### Management

This submenu is used to either enable or disable the firewall feature. Select the “Enable” or “Disable” radio button and click on the OK button to set.

#### Filter Enable/Disable

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

#### Firewall Parameter Description

Parameter	Description
Enable	Radio button used to enable the Firewall function
Disable	Radio button used to disable the Firewall function

### Configuration

This submenu is used by the administrator to set firewall rules which are used to allow or deny access to and from the WIM .

#### Basic Mode

This window is used to configure firewall rules by using the minimum number of options.



This Basic Mode example shows how to block traffic from the 192.168.1.0 network to the destination IP Address 10.0.2.1 In the Basic Mode all ports and protocols follow the allow or deny setting by default. If the rule needs to be either port or protocol specific use the Advanced Mode.

## Firewall Configuration

Category	Configuration
Source IP	192 . 168 . 1 . 0 / ▾ 24
Destination IP	10 . 0 . 2 . 1 / ▾
Target	Deny ▾

OK

### Basic Firewall Rule Parameter Description

Parameter	Description	
<b>Source IP</b>	Used to set the source IP Address	The / symbol is used to specify an entire network or subnet Example: 192.168.1.0/24 This defines every device within the 192.168.1.0 network to be allowed or not allowed to reach the destination IP
		The – is used to specify a range of IP Addresses to be allowed or not allowed to reach the destination IP Example: 192.168.1.50 - 60
		The * symbol is used to allow all Source IP Addresses to be allowed or not allowed to reach the destination IP Example: 0.0.0.0 *
<b>Destination IP</b>	Used to set the destination IP Address.	The / symbol is used to specify an entire network or subnet Example: 192.168.1.0/24 This defines every device within the 192.168.1.0 network to be an allowed or denied destination
		The – is used to specify a range of IP Addresses to be an allowed or denied destination Example: 192.168.1.50 - 60
		The * symbol is used to allow or deny all possible IP Addresses as the destination Example: 0.0.0.0 *
<b>Target</b>	Allow or Deny.	Allow = Sets the rule to allow access
		Deny = Sets the rule to deny access

## Advanced Mode

This window is used by the administrator to select and set up port, protocol, and time rules that are not included in the Basic Mode configuration.



In this Advanced Mode example all Source IP Addresses are being denied access to IP Address 192.168.1.150 on port 80, Saturday and Sunday only.

Config Mode  Basic Mode  Advanced Mode

## Firewall Configuration

Category	Configuration
Source IP	<input type="text" value="0"/> , <input type="text" value="0"/> , <input type="text" value="0"/> , <input type="text" value="0"/> * <input type="text" value=""/>
Destination IP	<input type="text" value="192"/> , <input type="text" value="168"/> , <input type="text" value="1"/> , <input type="text" value="150"/> / <input type="text" value=""/>
Port	<input type="radio"/> Define <input type="text" value="all"/> <input checked="" type="radio"/> User <input type="text" value="80"/> <input type="radio"/> Range <input type="text" value=""/> ~ <input type="text" value=""/> <input type="radio"/> Multi <input type="text" value=""/> , <input type="text" value=""/> , <input type="text" value=""/>
Protocol	<input type="text" value="all"/>
Time Set	Days: <input type="checkbox"/> Everyday <input checked="" type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input checked="" type="checkbox"/> Sat Time: <input checked="" type="radio"/> 24 Hours <input type="radio"/> <input type="text" value="8"/> : <input type="text" value="0"/> ~ <input type="text" value="17"/> : <input type="text" value="0"/>
Target	<input type="text" value="Deny"/>
Index No.	<input type="text" value="1"/>

OK

## Advanced Firewall Rule Parameter Description

Parameter	Description
Port	Used to set the network port./s
Protocol	Used to set the protocol.
Time Set	Used to set the time to apply the firewall rule.
Index No	Used to set the location of the firewall rule

The administrator can view the current status of the Firewall rules by using the [Firewall] → [Firewall] → [Configuration] submenu. The Configuration List is shown on the bottom of the window.

## Configuration List

<input type="checkbox"/>	No	Src	Dest	Port	Proto	Target	Time
<input type="checkbox"/>	1	0.0.0.0/0	192.168.1.150	80	udp	Deny	24 Hours[Sun,Sat]
<input type="checkbox"/>	2	0.0.0.0/0	192.168.1.150	80	tcp	Deny	24 Hours[Sun,Sat]
<input type="checkbox"/>	3	192.168.1.0/24	10.0.2.1	all	all	Deny	24 Hours[Everyday]

Delete

If a Firewall rule must be deleted then check the box to the left of the rule and then click the delete button. In order to delete all Firewall rules click on the box on the top left of the Configuration List then click on the delete button.

## Remote Access

The WIM Remote Access feature is used to permit or deny remote access. Select the [Firewall] → [Firewall] → [Remote Access] submenu to begin configuring the rule.

The first parameter is used to either enable or disable the Remote Access feature. Select the “Enable” or “Disable” radio button and click on the OK button to set.

## Remote Access

Default Policy	
<input checked="" type="radio"/> Allow	<input type="radio"/> Deny

OK

If Deny is selected then a new parameter will be displayed. Enter the Administration IP information. Please pay close attention when entering this IP Address because all access will be denied to the WIM unless the computer has this IP Address.

## Remote Access

Default Policy	
<input type="radio"/> Allow	<input checked="" type="radio"/> Deny
Administration IP	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>

OK

When the Allow radio button is selected then the administrator can set up the Remote Access policy. If Allow is selected and a policy is not defined then everyone will have Remote Access to the WIM.



In this example Remote Access to the WIM from any IP Address on the 12.0.0.0/8 network is denied 24 hours a day, 7 days a week.

## Remote IP Configuration

Category	Configuration
Source IP	12 . 0 . 0 . 0 / 8
Port	<input checked="" type="radio"/> Define all <input type="radio"/> User <input type="text"/> <input type="radio"/> Range <input type="text"/> ~ <input type="text"/> <input type="radio"/> Multi <input type="text"/> , <input type="text"/>
Protocol	all
Time Set	Days: <input checked="" type="checkbox"/> Everyday <input checked="" type="checkbox"/> Sun <input checked="" type="checkbox"/> Mon <input checked="" type="checkbox"/> Tue <input checked="" type="checkbox"/> Wed <input checked="" type="checkbox"/> Thu <input checked="" type="checkbox"/> Fri <input checked="" type="checkbox"/> Sat Time: <input checked="" type="radio"/> 24 Hours <input type="radio"/> 0 : 0 ~ 0 : 0
Target	Deny
Index No.	1

OK

The administrator can view the current status of the Remote Access rules by using the [Firewall] → [Firewall] → [Remote Access] submenu. The Configuration List is shown on the bottom of the window.

## Configuration List

<input type="checkbox"/>	No	Src	Port	Proto	Target	Time
<input type="checkbox"/>	1	12.0.0.0/8	all	udp	Deny	24 Hours[Everyday]
<input type="checkbox"/>	2	12.0.0.0/8	all	tcp	Deny	24 Hours[Everyday]

Delete

If a Remote Access rule must be deleted then check the box to the left of the rule and then click the delete button. In order to delete all Remote Access rules click on the box on the top left of the Configuration List then click on the delete button.



## IP Filtering

The WIM IP Filtering feature is very similar to the Advanced Firewall Rules. The biggest difference is the rule default is set to deny. These IP Filter rules are used to deny access only. Select the **[Firewall] → [Firewall] → [IP Filtering]** submenu to begin configuring the rule.



In the example listed below IP Address 192.168.2.15 is not allowed to exit any interface 7 days a week, 24 hours a day.

### IP Filtering

Category	Configuration
Source IP	192 . 168 . 2 . 15 / ▾
Destination IP	0 . 0 . 0 . 0 * ▾
Port	<input checked="" type="radio"/> Define all ▾ <input type="radio"/> User <input type="text"/> <input type="radio"/> Range <input type="text"/> ~ <input type="text"/> <input type="radio"/> Multi <input type="text"/> , <input type="text"/> <input type="text"/> , <input type="text"/>
Protocol	all ▾
Time Set	Days: <input checked="" type="checkbox"/> Everyday <input checked="" type="checkbox"/> Sun <input checked="" type="checkbox"/> Mon <input checked="" type="checkbox"/> Tue <input checked="" type="checkbox"/> Wed <input checked="" type="checkbox"/> Thu <input checked="" type="checkbox"/> Fri <input checked="" type="checkbox"/> Sat Time: <input checked="" type="radio"/> 24 Hours <input type="radio"/> 0 ▾ : 0 ▾ ~ 0 ▾ : 0 ▾
Index No.	1 ▾

OK

The administrator can view the current status of the IP Filtering rules by using the **[Firewall] → [Firewall] → [IP Filtering]** submenu. The Configuration List is shown on the bottom of the window.

### Configuration List

<input type="checkbox"/>	No	Src	Dest	Port	Proto	Time
<input type="checkbox"/>	1	192.168.2.15	0.0.0.0/0	all	udp	24 Hours[Everyday]
<input type="checkbox"/>	2	192.168.2.15	0.0.0.0/0	all	tcp	24 Hours[Everyday]

Delete

If an IP Filtering rule must be deleted then check the box to the left of the rule and then click the delete button. In order to delete all IP Filtering rules click on the box on the top left of the Configuration List then click on the Delete button.

## URL Filtering

Administrators can deny web access to PCs connected to the system using the [Firewall] → [Firewall] → [URL Filtering] submenu. Once the Source IP and Key Word data is entered click the OK button to save.

### URL Filtering

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

OK



In the example listed below LAN users with an IP Address 192.168.2.15 thru 20 are not allowed to view any website 7 days a week, 24 hours a day with the word myspace in the website name.

### URL Filtering

Category	IP
Source IP	<input type="text" value="192"/> <input type="text" value="."/> <input type="text" value="168"/> <input type="text" value="."/> <input type="text" value="2"/> <input type="text" value="."/> <input type="text" value="15"/> - <input type="text" value="20"/>
Key Word	<input type="text" value="myspace"/>
Time Set	Days: <input checked="" type="checkbox"/> Everyday <input checked="" type="checkbox"/> Sun <input checked="" type="checkbox"/> Mon <input checked="" type="checkbox"/> Tue <input checked="" type="checkbox"/> Wed <input checked="" type="checkbox"/> Thu <input checked="" type="checkbox"/> Fri <input checked="" type="checkbox"/> Sat Time: <input checked="" type="radio"/> 24 Hours <input type="radio"/> <input type="text" value="0"/> : <input type="text" value="0"/> ~ <input type="text" value="0"/> : <input type="text" value="0"/>

OK

### Configuration List

<input type="checkbox"/>	No	Src	Key Word	Time
<input type="checkbox"/>	1	192.168.2.15-192.168.2.20	myspace	24 Hours[Everyday]

Delete

## URL Filtering Parameter Description

Parameter	Description	
<b>Source IP</b>	To set the originating IP. Address	<p>The / symbol is used to specify an entire network or subnet. Example: 192.168.1.0/24 This denies access to any website with a defined word from any users on the 192.168.1.0 network</p> <hr/> <p>The – is used to specify a range of IP Addresses to be restricted from accessing a web site Example: 192.168.1.50 - 60</p> <hr/> <p>The * symbol is used to deny all LAN IP Addresses from accessing a web site Example: 0.0.0.0 *</p>
<b>Keyword</b>	To enter the keyword of the site to deny.	
<b>Time Set</b>	To set the time to apply the filtering rule.	

## ICMP Filtering

Administrators can deny the Internet Control Message Protocol (ICMP) Reply packets. Select the [Firewall] → [Firewall] → [ICMP Filtering] submenu. Then select the “Enable” or “Disable” radio button for the interface and click on the OK button to apply the change. If the Interface is set to Enable then it will not respond to ping requests or trace route.

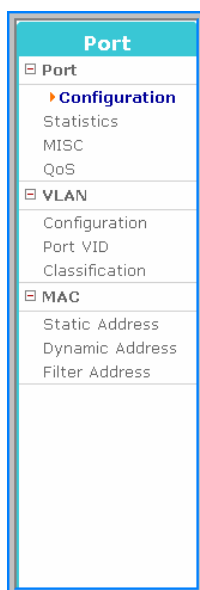
### ICMP Filtering

Interface	Setting	
Ethernet0	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
Ethernet1	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
Ethernet2	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
Ethernet3	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable

OK

## Port Menu

One PLIM/LIM can be managed on the OS 7200 system through the WIM Data Module using the **[Port]** → and **[Layer2]** menus. If you select the **[Port]** menu from OfficeServ 7200 WIM Data Server, the following submenus will be displayed on the left side of the window.



### Port Menu Description

Menu	Submenu	Description
Port	Configuration	Used to set the switch port environment.
	Statistics	Used to display the link status, speed, transmission system, and statistics of each switch port.
	MISC	Used to set the mirroring function, to set the MAC Age-out time, and Broadcast Storm Filter percentage.
	QoS	Used to set the Layer 2 QoS Mode which gives priority to specific ports based on priority levels.
VLAN	Configuration	Used to configure the Virtual LAN (VLAN) settings.
	Port VID	Used to set the processing method for untagged packets when VLAN mode is set to 'Tag-based VLAN'.
	Classification	Used to set the VLAN based on the protocol or MAC.
MAC	Static Address	Used to save MAC addresses to the static address table of the switch.
	Dynamic Address	Used to retrieve the dynamic address table or to delete a MAC address.
	Filter Address	Used to enter the MAC address to block the frame data with the MAC address information identical with the entered value from the switch.

# Port

The administrator uses the **[Port]** menu to set the port related functions and retrieve information on each port.

## Configuration

Select the **[Port]** → **[Configuration]** submenu to set or view the parameters of each switch port.

**Port Configuration**

Port	Active	Negotiation	Spd/Dpx		Flow Ctrl	Rate(%) In/Out		Security	Priority
All	<input type="checkbox"/>				<input type="checkbox"/>			<input type="checkbox"/>	
1	<input checked="" type="checkbox"/>	Auto	100	Full	<input checked="" type="checkbox"/>	0	0	<input type="checkbox"/>	Off
2	<input checked="" type="checkbox"/>	Auto	100	Full	<input checked="" type="checkbox"/>	0	0	<input type="checkbox"/>	Off
3	<input checked="" type="checkbox"/>	Auto	100	Full	<input checked="" type="checkbox"/>	0	0	<input type="checkbox"/>	Off
4	<input checked="" type="checkbox"/>	Auto	100	Full	<input checked="" type="checkbox"/>	0	0	<input type="checkbox"/>	Off
5	<input checked="" type="checkbox"/>	Auto	100	Full	<input checked="" type="checkbox"/>	0	0	<input type="checkbox"/>	Off
6	<input checked="" type="checkbox"/>	Auto	100	Full	<input checked="" type="checkbox"/>	0	0	<input type="checkbox"/>	Off
7	<input checked="" type="checkbox"/>	Auto	100	Full	<input checked="" type="checkbox"/>	0	0	<input type="checkbox"/>	Off
8	<input checked="" type="checkbox"/>	Auto	100	Full	<input checked="" type="checkbox"/>	0	0	<input type="checkbox"/>	Off
9	<input checked="" type="checkbox"/>	Auto	100	Full	<input checked="" type="checkbox"/>	0	0	<input type="checkbox"/>	Off
10	<input checked="" type="checkbox"/>	Auto	100	Full	<input checked="" type="checkbox"/>	0	0	<input type="checkbox"/>	Off
11	<input checked="" type="checkbox"/>	Auto	100	Full	<input checked="" type="checkbox"/>	0	0	<input type="checkbox"/>	Off
12	<input checked="" type="checkbox"/>	Auto	100	Full	<input checked="" type="checkbox"/>	0	0	<input type="checkbox"/>	Off
13	<input checked="" type="checkbox"/>	Auto	100	Full	<input checked="" type="checkbox"/>	0	0	<input type="checkbox"/>	Off
14	<input checked="" type="checkbox"/>	Auto	100	Full	<input checked="" type="checkbox"/>	0	0	<input type="checkbox"/>	Off
15	<input checked="" type="checkbox"/>	Auto	100	Full	<input checked="" type="checkbox"/>	0	0	<input type="checkbox"/>	Off
16	<input checked="" type="checkbox"/>	Auto	100	Full	<input checked="" type="checkbox"/>	0	0	<input type="checkbox"/>	Off
uplink	<input checked="" type="checkbox"/>	Auto	100	Full	<input checked="" type="checkbox"/>	0	0	<input type="checkbox"/>	Off

## Port Configuration Parameter Description

Parameter	Description
Port	Column is used to lists the 16 switch ports and 1 uplink port.
Active	Used to turn a switch port on or off.
Negotiation	Used to set the negotiation type - Auto: Controls speed through negotiation. - Force: Controls speed through enforcement. Sets this item to 'force' when setting the Duplex item to 'Full'. - Nway Force: It enables the port to perform link partner and auto negotiation by specifying own capability in auto negotiation.
Speed/Dpx	Used to set the speed and duplex type - Speed: Set 10/100 Mbps. - Dpx(Duplex): Select Full(bidirectional service) or Half (unidirectional service).

Parameter	Description
Flow Ctl	Used to 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	On ports using Flow Control these fields set the 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	Used to allow or deny the MAC address table from being updated on a per port basis. If the 'Security' box is checked, then the source MAC address table will not update when a device is connected to the port. For ports using Security the MAC address information of the connecting terminal device must be entered into the Static MAC Address field in the <b>[Port] → [MAC] → [Static Address]</b> submenu otherwise the connecting terminal will not function at the Layer 2. If the Security' box is not checked then the Static MAC address table is updated with the connecting terminal's MAC address information automatically.
Priority	Used to set the port priority to 'Low' or 'High'. Once the priority is set to 'Low' or 'High', then the QoS Mode can be defined as First Come First Service (FCFS), Weighted Round Robin (WRR), or All High Before Low using the <b>[Port] → [QoS]</b> submenu.

## Statistics

Select the **[Port]** → **[Statistics]** submenu to retrieve the link status, speed, transmission system, and statistics of each port. The numbers show the accumulated values for the period from the system boot up to date. The window is automatically updated by clicking the Refresh button. Click the Reset button to initialize all values to '0'.

### Statistics

Port	Link	Input Packets	Input Dropped	Input Errors	Output Packets	Output Dropped	Output Errors	Collisions
Port1	Off	0	0	0	0	0	0	0
Port2	Off	0	0	0	0	0	0	0
Port3	Off	0	0	0	0	0	0	0
Port4	Off	0	0	0	0	0	0	0
Port5	Off	0	0	0	0	0	0	0
Port6	Off	0	0	0	0	0	0	0
Port7	Off	0	0	0	0	0	0	0
Port8	Off	0	0	0	0	0	0	0
Port9	Off	0	0	0	0	0	0	0
Port10	Off	0	0	0	0	0	0	0
Port11	Off	0	0	0	0	0	0	0
Port12	Off	0	0	0	0	0	0	0
Port13	Off	0	0	0	0	0	0	0
Port14	Off	0	0	0	0	0	0	0
Port15	Off	0	0	0	0	0	0	0
Port16	Off	0	0	0	0	0	0	0
uplink	On	0	0	0	509	0	0	0

Refresh Reset

### Statistic Field Description

Field	Description
Port	This column is used to lists the 16 switch ports and 1 uplink port.
Link	This column is used to show the link status of the switch port
Input Packets	This column is used to show the number of packets which are successfully sent to the port
Input Dropped	This column is used to show the number of packets which are successfully sent to the port, but not switched and dropped
Input Errors	This column is used to show the number of packets which are sent to the port but an error occurs
Output Packets	This column is used to show the number of packets which are sent out through the port
Output Dropped	This column is used to show the number of packets which are successfully sent out through the port, but are not switched and dropped
Output Errors	This column is used to show the number of packets which are sent out through the port, but an error occurs
Collisions	This column is used to show the number of cases that a collision occurs between packets received in the port and switched



## MISC

Select the **[Port]** → **[MISC]** submenu to set the mirroring function, the MAC Age-out timer, and the Broadcast Storm Filter.

### Mirroring Configuration

Port Mirroring Configuration	
Mode	Off
Monitoring Port	Port1
Monitored Port	<input type="checkbox"/> VLAN 1 <input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7 <input type="checkbox"/> 8 <input type="checkbox"/> 9 <input type="checkbox"/> 10 <input type="checkbox"/> 11 <input type="checkbox"/> 12 <input type="checkbox"/> 13 <input type="checkbox"/> 14 <input type="checkbox"/> 15 <input type="checkbox"/> 16 <input type="checkbox"/> uplink

### Miscellaneous Configuration

Miscellaneous Configuration	
MAC Age-out Time (300-765)	300 sec
Broadcast Storm Filter Mode	5%
Auto MDI / MDIX	on

OK Default

### Mirroring and Miscellaneous Parameter Description

Parameter	Description
Mode	Used to turn the mirroring function On or Off. <b>Off:</b> The mirroring function is not used. <b>Receive:</b> The monitoring port will be sent all received packets of the mirrored port/s <b>Transmit:</b> The monitoring port will be sent all transmitted packets from the mirrored port/s <b>Both:</b> The monitoring port will be sent all packets that are sent or received to/from the mirrored port/s
Monitoring Port	Used to sets the port that performs the monitoring. Generally, this is a connection port of a PC doing the monitoring.
Monitored Port	Used to set the port/s that will be monitored..
MAC Age-Out Delay Bound	Used to set the time when the MAC address learned (MAC address updated) can be left in the address table of the switch. Default is 300 seconds. When the LAN port connection is released, the MAC address which was previously learned is automatically deleted. When the LAN port is re-connected, a new MAC address is learned and MAC address table is rapidly updated.
Broadcast Storm Filter Mode	Used to set the value from 5, 10, 15, 20% of the entire buffer size of the switch. If a value exceeds the value above, broadcast packet is lost.

## QoS Configuration

Select the [Port] → [QoS Configuration] submenu to assign Layer 2 QoS priority according to the packets sent to the switch or process QoS by giving priority compulsorily to a specific port.

### QoS Configuration

QoS Configuration	
QoS Mode	Weighted Round Robin
Weight (High/Low)	2 / 1
Delay Bound / Max Delay Time (1-255)	Off 255
High Priority Levels	<input type="checkbox"/> Level0 <input type="checkbox"/> Level1 <input type="checkbox"/> Level2 <input type="checkbox"/> Level3 <input checked="" type="checkbox"/> Level4 <input checked="" type="checkbox"/> Level5 <input checked="" type="checkbox"/> Level6 <input checked="" type="checkbox"/> Level7

OK

### QoS Parameter Description

Item	Description
QoS Mode	<p>Used to set the QoS mode type.</p> <p><b>First Come First Service:</b> Packets are sent according to the arrival order.(The QoS function is not used.)</p> <p><b>All High before Low:</b> Packets with higher priority are sent prior to the packets with lower priority.</p> <p><b>Weighted Round Robin:</b> Packets with higher priority and lower priority are sent with a certain ratio (weight). For example, if high weight is set to '5', and low weight is set to '2', 5 packets with higher priority are sent before the 2 packets with lower priority.</p>
Weight	When using the 'Weighted Rounded Robin' type, these fields are used to set the ratio of high weight and low weight.
Delay Bound/ Max Delay Time	When using 'All High before Low' or 'Weighted Round Robin', this field is used to set a time limit to prevent the continuous delay of packets with lower priority. The unit of 'Max Delay Time' is ms (1/1000 sec), and default is 255ms. Processes preferentially when packets with lower priority are not switched to exceed the time set in this item.
High Priority Levels	These check boxes are used to determine which levels are considered High Priority.

# VLAN

VLANs are used to divide a network into smaller networks to reduce the traffic and for security purposes. The **[Port] → [VLAN]** submenu is used to configure VLANs, Port VLANs, and VLAN Classifications.

## Configuration

Using the **[Port] → [VLAN] → [Configuration]** submenu the administrator can configure the VLAN features.

### VLAN Configuration

VLAN Operation Mode

Mode	802.1Q(IVL)
------	-------------

VLAN Name	VLAN ID

Select	VLAN ID	VLAN Name	VLAN Members (Untagged / Tagged)
<input type="radio"/>	1	default	<input checked="" type="checkbox"/> P1 <input checked="" type="checkbox"/> P2 <input checked="" type="checkbox"/> P3 <input checked="" type="checkbox"/> P4 <input checked="" type="checkbox"/> P9 <input checked="" type="checkbox"/> P10 <input checked="" type="checkbox"/> P11 <input checked="" type="checkbox"/> P12 <input checked="" type="checkbox"/> P5 <input checked="" type="checkbox"/> P6 <input checked="" type="checkbox"/> P7 <input checked="" type="checkbox"/> P8 <input checked="" type="checkbox"/> P13 <input checked="" type="checkbox"/> P14 <input checked="" type="checkbox"/> P15 <input checked="" type="checkbox"/> P16 <input checked="" type="checkbox"/> uplink

## VLAN Operation Mode Description

Mode	Description
802.1 Q(IVL)	Used to set the VLAN type to Independent VLAN Learning – Tag based
MAC	Used to set the VLAN type to MAC based VLAN
Port	Used to set the VLAN type to Port Based VLAN
802.1 Q(SVL)	Used to set the VLAN type to Shared VLAN Learning – Tag based

### 802.1 Q (IVL)

IVL (Independent VLAN): Each VLAN operates while maintaining an independent MAC address table. Because the security is enhanced, data cannot be exchanged directly among the VLANs.

### MAC Based VLAN

The MAC based VLAN is configured with an access list mapping individual MAC addresses to VLAN membership. The VLAN is configured without information on the port and the

number of a VLAN members may change. Up to 256 MAC address members can be saved either in a single VLAN or in multiple VLANs. Since a MAC Based VLAN does not basically contain port information, the port serves as a VLAN member by receiving packets. Thus, the ARP packet must be transmitted to the switch to enable members of a VLAN to exchange packets.

### Port Based VLAN

The Port based VLAN is configured with an access list specifying membership in a set of VLANs.. A single port can be assigned to multiple VLANs. In such cases the 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.

### 802.1Q (SVL)

802.1Q(SVL) can be set and operate with the same method as 802.1Q(IVL).

SVL (Shared VLAN): All VLANs operates while maintaining a common MAC address table. Because the security is not tightened and the MAC address table exists for all ports, data can be exchanged among all VLANs.

In order to create a new VLAN simply enter the VLAN name and ID and then click the Add button.

VLAN Name	VLAN ID
VLAN2	2

Once a VLAN is created then it is then possible to add members to the VLAN

### Port and MAC based VLAN

Select	VLAN ID	VLAN Name	VLAN Members (Untagged / Tagged)
<input checked="" type="radio"/>	1	default	<input checked="" type="checkbox"/> P1 <input checked="" type="checkbox"/> P2 <input checked="" type="checkbox"/> P3 <input checked="" type="checkbox"/> P4 <input checked="" type="checkbox"/> P9 <input checked="" type="checkbox"/> P10 <input checked="" type="checkbox"/> P11 <input checked="" type="checkbox"/> P12 <input checked="" type="checkbox"/> P5 <input checked="" type="checkbox"/> P6 <input checked="" type="checkbox"/> P7 <input checked="" type="checkbox"/> P8 <input checked="" type="checkbox"/> P13 <input checked="" type="checkbox"/> P14 <input checked="" type="checkbox"/> P15 <input checked="" type="checkbox"/> P16 <input checked="" type="checkbox"/> uplink
<input type="radio"/>	2	VLAN2	<input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4 <input type="checkbox"/> P9 <input type="checkbox"/> P10 <input type="checkbox"/> P11 <input type="checkbox"/> P12 <input type="checkbox"/> P5 <input type="checkbox"/> P6 <input type="checkbox"/> P7 <input type="checkbox"/> P8 <input type="checkbox"/> P13 <input type="checkbox"/> P14 <input type="checkbox"/> P15 <input type="checkbox"/> P16 <input type="checkbox"/> uplink

## 802.1Q IVL and SVL based VLAN

Select	VLAN ID	VLAN Name	VLAN Members (Untagged / Tagged)
<input checked="" type="radio"/>	1	default	<input checked="" type="checkbox"/> P1 <input checked="" type="checkbox"/> P2 <input checked="" type="checkbox"/> P3 <input checked="" type="checkbox"/> P4 <input checked="" type="checkbox"/> P9 <input checked="" type="checkbox"/> P10 <input checked="" type="checkbox"/> P11 <input checked="" type="checkbox"/> P12 <input checked="" type="checkbox"/> P5 <input checked="" type="checkbox"/> P6 <input checked="" type="checkbox"/> P7 <input checked="" type="checkbox"/> P8 <input checked="" type="checkbox"/> P13 <input checked="" type="checkbox"/> P14 <input checked="" type="checkbox"/> P15 <input checked="" type="checkbox"/> P16 <input checked="" type="checkbox"/> uplink
<input type="radio"/>	2	VLAN2	<input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4 <input type="checkbox"/> P9 <input type="checkbox"/> P10 <input type="checkbox"/> P11 <input type="checkbox"/> P12 <input type="checkbox"/> P5 <input type="checkbox"/> P6 <input type="checkbox"/> P7 <input type="checkbox"/> P8 <input type="checkbox"/> P13 <input type="checkbox"/> P14 <input type="checkbox"/> P15 <input type="checkbox"/> P16 <input type="checkbox"/> uplink <input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4 <input type="checkbox"/> P9 <input type="checkbox"/> P10 <input type="checkbox"/> P11 <input type="checkbox"/> P12 <input type="checkbox"/> P5 <input type="checkbox"/> P6 <input type="checkbox"/> P7 <input type="checkbox"/> P8 <input type="checkbox"/> P13 <input type="checkbox"/> P14 <input type="checkbox"/> P15 <input type="checkbox"/> P16 <input type="checkbox"/> uplink

The 802.1q IVL and SVL based VLANs have two groups of boxes. The top grouping (in black) is used to assign untagged ports, and the bottom grouping (in blue) is used to assign tagged ports.

- VLAN Untagged Members: Select the port/s that will send the Ethernet frame that deletes the TCI (Tag Control Information). Connect to a terminal that does not support IEEE 802.1Q to configure tagged VLAN.
- VLAN Tagged Members: Select a port that will send the TCI. Connect to another switch port that supports IEEE 802.1Q.

## Port VID

For an ethernet packet to have a VLAN ID the tag must be written by an Ethernet adapter or Switch. Using the **[Port] → [VLAN] → [Port VID]** submenu the administrator will assign the VLAN IDs to specific ports.

### Port VID Configuration

Port	Port VID	Forward Only this VID	Drop Untagged Frame
port1	1	<input type="checkbox"/>	<input type="checkbox"/>
port2	1	<input type="checkbox"/>	<input type="checkbox"/>
port3	1	<input type="checkbox"/>	<input type="checkbox"/>
port4	1	<input type="checkbox"/>	<input type="checkbox"/>
port5	1	<input type="checkbox"/>	<input type="checkbox"/>
port6	1	<input type="checkbox"/>	<input type="checkbox"/>
port7	1	<input type="checkbox"/>	<input type="checkbox"/>
port8	1	<input type="checkbox"/>	<input type="checkbox"/>
port9	1	<input type="checkbox"/>	<input type="checkbox"/>
port10	1	<input type="checkbox"/>	<input type="checkbox"/>
port11	1	<input type="checkbox"/>	<input type="checkbox"/>
port12	1	<input type="checkbox"/>	<input type="checkbox"/>
port13	1	<input type="checkbox"/>	<input type="checkbox"/>
port14	1	<input type="checkbox"/>	<input type="checkbox"/>
port15	1	<input type="checkbox"/>	<input type="checkbox"/>
port16	1	<input type="checkbox"/>	<input type="checkbox"/>
uplink	1	<input type="checkbox"/>	<input type="checkbox"/>

OK

### Port VID Parameter Description

Parameter	Description
<b>Port VID</b>	<ul style="list-style-type: none"> <li>- VLAN ID for an untagged packet.</li> <li>- When an untagged packet is sent to the corresponding port, the packet is switched to the VLAN corresponding to the Port VID.</li> </ul>
<b>Forward Only this VID</b>	<p>If this box is checked and the received tagged packet tag is different from the Port VID then the packet is discarded. When this box is not checked then the packet is re-sent according to the received tag information.</p>
<b>Drop Untagged Frame</b>	<p>If this box is checked then the port discards the untagged frame. If not, the untagged frame is re-sent to the VLAN corresponding to the setting Port VID.</p>



NOTE

#### Port VID Input Value

The valid PVID values on the GPLIMIT/GPLIM are between 1 and 255.

## Classification

Using the [Port] → [VLAN] → [Classification] submenu the administrator can define the VLAN Classification Rules.

### 802.1Q (IVL and SVL)

If an untagged frame is received it can be classified according to protocol. The rule values are set to decide which VLAN ID is attached to a frame.

#### VLAN Classification Configuration

Parameter	Argument
Classification Mode	proto
Classification Rule	appletalk
Group ID	<input type="text"/> (1-256)
VLAN ID	<input type="text"/>

#### VLAN Configuration Field/Parameter Description

Field/Parameter	Description
<b>Classification Mode</b>	This field is defined automatically according to the VLAN mode. When the mode is 802.1Q 'proto' (for protocol) is selected.
<b>Classification Rule</b>	Based on Appletalk, arp, decnet, ip, ipx, sna, and x25, VLAN is set.
<b>Group ID</b>	Used to enter a Group ID for the selected protocol. Valid groups numbers are 1~256.
<b>VLAN ID</b>	Decides which VLAN ID will be assigned to the frame.

In order to delete a VLAN Classification rule simply click on the radio button to the left of the rule and then click the delete button.

## MAC Based VLAN

Frames coming into a switch can be marked for a particular VLAN based on the source MAC Address

### VLAN Classification Configuration

Parameter	Argument
Classification Mode	mac
Classification Rule	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>
Group ID	<input type="text"/> (1-256)
VLAN ID	<input type="text" value="2"/>

OK

### VLAN Classification Parameter Description

Field/Parameter	Description
<b>Classification Mode</b>	This field is defined automatically according to the VLAN mode. When the mode is MAC 'mac' is selected
<b>Classification Rule</b>	According to the received packet via a defined MAC address the VLAN can be set.
<b>Group ID</b>	Used to enter a Group ID for the selected mac. Valid groups numbers are 1~256.
<b>VLAN ID</b>	Decides which VLAN ID will be assigned to the frame..

In order to delete a VLAN Classification rule simply click on the radio button to the left of the rule and then click the delete button.



## MAC

The **[Port] → [MAC]** submenu is used to assign MAC addresses to ports, to view dynamic MAC address tables, and to assign MAC address filtering.

### Static Address

The **[Port] → [MAC] → [Static Address]** submenu is used to enter a specific MAC address in the MAC address table. Even if the device is not connected to the switch and the MAX Aging Time (interval of MAC address table renewal) is passed the corresponding MAC address is left in the address table. Multiple MAC Addresses may be defined on the same port.

#### Static MAC Address

Check	MAC Address	Port ID
<input type="checkbox"/>	<input type="text" value=""/> <input type="text" value=""/> <input type="text" value=""/> <input type="text" value=""/> <input type="text" value=""/> <input type="text" value=""/>	<input type="text" value="port1"/>
<input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Delete All"/>		

Enter the MAC address and Port ID and then click the Add button to add the MAC address. In order to delete an entry select the box to the left of the specific MAC address and then click the Delete button

If the Security box is checked for a port in the **[Port] → [Port] → [Config]** submenu then any learning of source MAC addresses will not occur. Only defined MAC addresses can access the port at this point.



#### Number of Static MAC Addresses Entered

Up to 50 static MAC addresses can be entered into the Static MAC Address table.

## Dynamic Address

In order to view the dynamically learned MAC addresses use the [Port] → [MAC] → [Dynamic Address] submenu.

### Dynamic MAC Address

Check	MAC Address	Port ID
<input type="checkbox"/>	00 : 07 : E9 : 67 : FE : 5B	port7
<input type="checkbox"/>	00 : 01 : E7 : BB : E3 : 00	port7
<input type="checkbox"/>	00 : 13 : 20 : 4E : 32 : EC	port7
<input type="checkbox"/>	00 : 00 : F0 : 67 : 01 : 5F	port7
<input type="checkbox"/>	00 : 50 : FC : B0 : 8E : 3B	port7
<input type="checkbox"/>	00 : 01 : E7 : BB : E3 : 38	port7
<input type="checkbox"/>	00 : 00 : F0 : A1 : 23 : A7	port7
<input type="checkbox"/>	00 : 13 : 20 : 32 : 13 : B3	port7
<input type="checkbox"/>	00 : A0 : B0 : 05 : FC : 55	port7
<input type="checkbox"/>	00 : 09 : 74 : 11 : 11 : 11	port7
<input type="checkbox"/>	00 : 50 : FC : A8 : 12 : 6E	port7
<input type="checkbox"/>	00 : 07 : E9 : EF : B4 : FD	port7
<input type="checkbox"/>	00 : 00 : F0 : A0 : 58 : B3	port7
<input type="checkbox"/>	00 : 07 : E9 : EF : 34 : 73	port7
<input type="checkbox"/>	00 : 07 : E9 : 03 : 21 : 27	port7
<input type="checkbox"/>	00 : 09 : 74 : 00 : 10 : 03	port7
<input type="checkbox"/>	00 : 11 : 11 : 66 : B9 : 46	port7

## Filter Address

By using the Mac filtering feature on the GPLIMIT/GPLIM it is possible to block unwanted traffic on the network. The [Port] → [MAC] → [Filter Address] submenu is used to enter MAC addresses that are to be filtered.

Enter the desired MAC address and VLAN ID and then click the Add button.

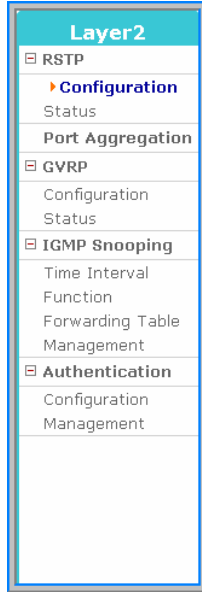
If a MAC Address filter needs to be removed check the box to the left of the filter and then click the Delete button.

### Filter Destination MAC Address

Check	MAC Address
<input type="checkbox"/>	: : : : :

# Layer2 Menu

One PLIM/LIM can be managed on the OS 7200 system through the WIM using the [Port] → and [Layer2] menus. If you select the [Layer2] menu the following submenus will be displayed on the upper left side of the window.



## Layer 2 Menu Description

Menu	Submenu	Description
<b>RSTP</b>	Configuration	Used to set the bridge and port environment used in RSTP.
	Status	Used to display the RSTP operation status of the switch.
<b>Port Aggregation</b>	-	Used to set Port Aggregation related values
<b>GVRP</b>	Configuration	Used to set up the GVRP and Dynamic VLAN Creation services.
	Status	Used to display the status of each port where GVRP is set.
<b>IGMP Snooping</b>	Time Interval	Used to set the time interval for IGMP Snooping.
	Function	Used to set the function related with IGMP Snooping.
	Forwarding Table	Used to display the information for the members registered in IGMP Group.
	Management	Used to set whether to operate IGMP Snooping.
<b>Authentication</b>	Configuration	Used to set the Authentication service.
	Management	Used to start or stop the Authentication service.

# RSTP

## Configuration

The Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocols (RSTP) provide a loop free topology for any bridged LAN. Use the [Layer2] → [RSTP] → [Configuration] submenu to begin configuring the RSTP and STP settings.

### Protocol Status

Parameter	Argument
RSTP status	Current Enable

### Bridge Parameter

Parameter	Argument
Bridge Priority	8 ( 0 - 15 )
Hello Time	2 sec ( 1 - 10 )
Max Age Time	20 sec ( 6 - 40 )
Forward Time	15 sec ( 4 - 30 )

### Port Parameter

Port Name	Priority	Force Version	Path Cost	Port Fast	Link Type
port1	8	RSTP	200000	Disable	Shared
port2	8	RSTP	200000	Disable	Shared
port3	8	RSTP	200000	Disable	Shared
port4	8	RSTP	200000	Disable	Shared
port5	8	RSTP	200000	Disable	Point to Point
port6	8	RSTP	200000	Disable	Shared
port7	8	RSTP	200000	Disable	Point to Point
port8	8	RSTP	200000	Disable	Shared
port9	8	RSTP	200000	Disable	Shared
port10	8	RSTP	200000	Disable	Shared
port11	8	RSTP	200000	Disable	Shared
port12	8	RSTP	200000	Disable	Shared
port13	8	RSTP	200000	Disable	Shared
port14	8	RSTP	200000	Disable	Shared
port15	8	RSTP	200000	Disable	Shared
port16	8	RSTP	200000	Disable	Shared
uplink	8	RSTP	200000	Disable	Point to Point

Save Reset

## RSTP Protocol Status/Bridge/Port Parameter Description

Parameter	Description
<b>Protocol Status</b>	Used to display the current status of the RSTP protocol.
<b>Bridge Parameter</b>	<p>Used to configure the Bridge parameters of the switch that RSTP uses.</p> <ul style="list-style-type: none"> <li>- <b>Bridge Priority:</b> Used to set the priority of Bridges.</li> <li>- <b>Hello Time:</b> Used to set the transmission cycle of BPDU.</li> <li>- <b>Max Age Time:</b> Used to set the Message Age time.</li> <li>- <b>Forward Time:</b> Used to set the time that the state of each port is changed (Discarding-Learning-Forwarding).</li> </ul>
<b>Port Parameter</b>	<ul style="list-style-type: none"> <li>- <b>Priority:</b> Standard to select the port to be blocked when the switch loop is established.</li> <li>- <b>Force Version:</b> Communication is progressed via the switch connected to the corresponding port and the BPDU that a user specifies. For '0', STP BPDU is transmitted. For '1', RSTP BPDU is transmitted.</li> <li>- <b>Path Cost:</b> Used to set and display the path cost according to the bandwidth when the connection with the opponent is established.</li> <li>- <b>Port Fast:</b> If the port is enabled for Port Fast then the port becomes an Edge port and quickly goes into a forwarding state. If this function is activated then the MAC address learned in the corresponding port is not canceled even when all topologies of Bridges are changed.(If STP is used then the Port Fast function should be disabled.)</li> <li>- <b>Link Type:</b> Used to set and display the type of the link connected to the opponent. The link is connected as point-to-point in RSTP.</li> </ul>

## Status

The [Layer2] → [RSTP] → [Status] submenu is used to display the status of the switch RSTP operation.

### Bridge Information

Parameter	Argument
Protocol Status	Enabled
Designated Bridge Identifier	80000000f0121318
Root Bridge Identifier	80000000f0121318
Root Path Cost	0
Root Port	0
Last Topology changed	Fri Sep 29 12:43:58 2006

### Port Information

Port Name	Port ID	Path Cost	Port Role	Port State	Designated Root
port1	0x8002	200000	Disabled	Discarding	00000000f0121318
port2	0x8003	200000	Disabled	Discarding	0000000000000000
port3	0x8004	200000	Disabled	Discarding	0000000000000000
port4	0x8005	200000	Disabled	Discarding	0000000000000000
port5	0x8006	200000	Designated	Forwarding	80000000f0121318
port6	0x8007	200000	Disabled	Discarding	0000000000000000
port7	0x8008	200000	Designated	Forwarding	80000000f0121318
port8	0x8009	200000	Disabled	Discarding	0000000000000000
port9	0x800a	200000	Disabled	Discarding	0000000000000000
port10	0x800b	200000	Disabled	Discarding	0000000000000000
port11	0x800c	200000	Disabled	Discarding	0000000000000000
port12	0x800d	200000	Disabled	Discarding	0000000000000000
port13	0x800e	200000	Disabled	Discarding	0000000000000000
port14	0x800f	200000	Disabled	Discarding	0000000000000000
port15	0x8010	200000	Disabled	Discarding	0000000000000000
port16	0x8011	200000	Disabled	Discarding	0000000000000000
uplink	0x8012	200000	Designated	Forwarding	80000000f0121318

Refresh

### RSTP Bridge Status Field Description

Field	Description
<b>Protocol Status</b>	Used to show the RSTP status
<b>Designated Bridge Identifier</b>	Used to display the GPLIMIT/GPLIM's bridge information in hexadecimal numbers. The upper four digits represent the bridge priority and the remaining lower digits is the GPLIMIT/GPLIM MAC address.
<b>Root Bridge Identifier</b>	Used to display the network root bridge.
<b>Root Path Cost</b>	Once the root bridge is decided this field displays the calculated cost for the path to the root switch.

Field	Description
<b>Root Port</b>	If the current equipment is not the root switch then this field indicates the ID of the port corresponding to the root port. A switch can have only root port.)
<b>Last Topology Changed</b>	Used to display the most recent time that the RSTP network was reconfigured due to a change in the network configuration.

### RSTP Port Status Field Description

Field	Description
<b>Port Name</b>	Used to display the port number
<b>Port ID</b>	The value is combined with the value of the port priority and the ID value of the port specified in the system. The highest two digits represents the value of the port priority and the lowest two digits consist of port index.
<b>Path Cost</b>	The value indicates the path cost of the corresponding path.
<b>Port Role</b>	The value indicates the role of the port that selected via the BDPUs exchange between switches. The RSTP Port Role is divided into Disable, Alternate, Backup, Designated, Root roles.
<b>Port State</b>	The Port State shows the status of the corresponding port.
<b>Designated Root</b>	Used to display the designated root

# Port Aggregation

In order to use multiple transmission paths between network devices so there can be an increase in transmission speeds then the Port Aggregation feature can be used. Select the [Layer2] → [Port Aggregation] → [Configuration] submenu to begin configuring Port Aggregation.

## Aggregate Configuration

Load balance mode	
Load Balance	Direct-MAP based DMAC & SMAC & SPORT-ID
System Priority	32768 (1 - 65535 Default : 32768)
System ID	00:00:f0:01:01:04

## Port Aggregate Configuration Parameter Description

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

## Member Configuration

S: Static, L: LACP

	Grp 1	Grp 2	Grp 3	Grp 4	Grp 5	Grp 6	Grp 7	Mode	Priority	Sync
Port1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Active		X
Port2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Active		X
Port3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Active		X
Port4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Active		X
Port5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Active		X
Port6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Active		X
Port7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Active		X
Port8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Active		X
Port9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Active		X
Port10	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Active		X
Port11	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Active		X
Port12	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Active		X
Port13	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Active		X
Port14	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Active		X
Port15	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Active		X
Port16	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Active		X

OK Refresh



Parameter	Description
<b>Group</b>	'S' represents a static trunk, and 'L' represents a LACP (Link Aggregation Control Protocol) trunk. Up to eight groups can be used and up to four ports can be included in one group as members. In addition, a member included in one group cannot be included another group simultaneously.
<b>Mode</b>	Used to set the mode when LACP is the Group type. Select either 'Active' or 'Passive'. When a port is set as Active, an LACP packet is transferred to the opposite switch first. When set as Passive it responds only when receiving a packet from the opposite switch. If the user system and opposite system are both set up as Active, then the system that has higher priority is used as a reference.
<b>Priority</b>	Used to setup the port priority. The default is 32768.
<b>Sync</b>	This field indicates information connected to the opposite system in ports that are configured with LACP ports. If configured as a LACP member but the LACP connection is abnormal for the opposite system, it is displayed as 'X'. 'O' means that a port is properly operated as a LACP port.

# GVRP

GVRP (GARP VLAN Registration Protocol) is a protocol that facilitates control of virtual local area networks (VLANs) within a network. It defines a method of tagging frames with VLAN configuration data. This allows network devices to dynamically exchange VLAN configuration information with other devices. Select the **[GVRP]** menu to start or stop the GVRP service, to modify the GVRP service for each port, and to view the status of GVRP.

## Configuration

Use the **[Layer2] → [GVRP] → [Configuration]** submenu to start or stop the GVRP service and the Dynamic VLAN Creation service.

### GVRP Basic

Parameter	Argument
GVRP	Disable ▼
Dynamic VLAN Creation	Disable ▼

In the **<GVRP Basic>** window specify the GVRP configuration as Enabled and then click the Save button. Once GVRP is enabled the following configuration window will appear.

### GVRP Configuration

Port	Status	Registration	Applicant	Timers(millisecond)		
				Join	Leave	LeaveAll
<input type="checkbox"/> ALL	Enable ▼	-	-	-	-	-
port1	Disable ▼	-	-	-	-	-
port2	Disable ▼	-	-	-	-	-
port3	Disable ▼	-	-	-	-	-
port4	Disable ▼	-	-	-	-	-
port5	Disable ▼	-	-	-	-	-
port6	Disable ▼	-	-	-	-	-
port7	Disable ▼	-	-	-	-	-
port8	Disable ▼	-	-	-	-	-
port9	Disable ▼	-	-	-	-	-
port10	Disable ▼	-	-	-	-	-
port11	Disable ▼	-	-	-	-	-
port12	Disable ▼	-	-	-	-	-
port13	Disable ▼	-	-	-	-	-
port14	Disable ▼	-	-	-	-	-

Make changes to the ports and then click the OK button to save the information. Click the Refresh button to display the latest information of the port .

## GVRP Configuration Field/Parameter Description

Field/Parameter	Description
Port	Used to display the port Number
Status	Used to enable or disable GVRP per port
Registration	Used to display the Registration mode as Normal, Forbidden or Fixed
Applicant	Used to display the Applicant mode as Normal or Active conditions
Join	Used to display the interval for Join Transfer Time
Leave	Used to display the value of Leave Delay Time
LeaveAll	Used to display the value of LeaveAll Transfer Time

## Status

The [Layer2] → [GVRP] → [Status] submenu is used to display the information on the ports where GVRP is configured.

### GVRP Machine

Port	Applicant State	Registrar State
Port1	VO	MT
Port2	VO	MT

### GVRP Machine Field Description

Field	Description
Port	Used to display the Port Number
Applicant State	Used to display the Current Status of the Applicant State Machine
Register State	Used to display the Current Status of the Register State Machine

### GVRP statistics

Port		Join Empty	Join In	Leave Empty	Leave In	Empty
Port1	RX	0	0	0	0	0
	TX	0	0	0	0	0
Port2	RX	0	0	0	0	0
	TX	0	0	0	0	0

Refresh

### GVRP Statistics Field Description

Field	Description
Port	Used to display the Port Number

<b>Field</b>	<b>Description</b>
<b>Join Empty</b>	Used to display the number of Join Empty packets
<b>Join In</b>	Used to display the number of Join In packets
<b>Leave Empty</b>	Used to display the number of Leave Empty packets
<b>Leave In</b>	Used to display the number of Leave In packets
<b>Empty</b>	Used to display the number of Empty packets

# IGMP Snooping

The purpose of Internet Group Management Protocol (IGMP) snooping is to restrain multicast traffic in a switched network. The [Layer2] → [IGMP Snooping] menu is used for the configuration of IGMP Snooping.

## Time Interval

Use the [Layer2] → [IGMP Snooping] → [Time Interval] submenu to configure the time related parameters of IGMP Snooping.

**Time Interval**

Category	Argument
VLAN	Default
Group Membership	120000 ms

OK

VLAN	Group Membership (ms)	Last Member Query (ms)	Max Response (ms)	Other Query (ms)
Default	120000	1000	10000	120000

## IGMP Time Interval Category Description

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

Select the VLAN and the Category to configure, enter the timed value, and then click the OK button to store the configuration.

## Function

Use the [Layer2] → [IGMP Snooping] → [Function] submenu to specify the functions related to IGMP Snooping.

### Function

Category		Argument	
VLAN		Default	
Querier		Disable	

Cross VLAN		Flood DPM	
Disable		Disable	

OK

VLAN	Querier	Immediate Leave
Default	Disable	Disable

### IGMP Snooping Function Category Description

Categories	Description
<b>VLAN</b>	Pull down menu used to select the VLAN to be configured.
<b>Querier</b>	Used to specify the operation as IGMP querier when the multicast router does not exist.
<b>Immediate Leave</b>	Used to delete a host from the group immediately when receiving the Leave Message.
<b>Cross VLAN</b>	Used to Forward multicast packets to all ports regardless of VLAN.
<b>Flood DPM</b>	Used if no member exists in the IGMP group, sets whether to forward multicast packets.

Select the VLAN and the Category to configure, select 'Enable' or 'Disable', and then click the OK button to store the configuration. The Querier and Immediate Leave values can be set for each VLAN, but the Cross VLAN and Flood DPM values are set on a bridge basis.

## Forwarding Table

Use the [Layer2] → [IGMP Snooping] → [Forwarding Table] submenu to display the information on the members registered in IGMP Group.

### Forwarding Table

VLAN	Multicast IP Address	Member Port	Aging Time
<input type="button" value="Refresh"/>			

Click the Refresh button to update the information displayed on the web screen.

## Management

Use the [Layer2] → [IGMP Snooping] → [Management] to specify the operation of IGMP Snooping.

### IGMP Snooping Management

Scope	Action
Global <input type="button" value="v"/>	Enable <input type="button" value="v"/>
<input type="button" value="OK"/>	

Scope	Current Status
Global	Enable
Default	Enable

In the Scope parameter each VLANs can be turned on or off independantly. However, if Global is set to Disable then all the VLANs become disabled.



NOTE

#### IGMP Snooping Management

If Global is set to Disable mode then other pages within the [Layer2] → [IGMP Snooping] submenu are not be displayed.

## Authentication

The [Authentication] submenu is used to enable or disable remote authentication, to review existing authentication information, and to configure individual ports and their authentication methods.

## Management

Use the [Layer2] → [Authentication] → [Management] submenu to turn authentication on or off and to define the Radius server management items.

Click the Run button to start the service and click the Stop button to cease the authentication service.

If there is the Radius server performing the 802.1x user authentication then the relevant data must be input here. The host IP address, host, and key should be registered. The default port of the Radius Host Port is 1812 port. Click the OK button to save any changes.

### Authentication Management

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

Radius Server Management	
Host IP	<input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="0"/> . <input type="text" value="23"/>
Secret Key	<input type="text" value="samsung"/>
Host Port	<input type="text" value="1812"/>



## Configuration

Use the [Layer2] → [Authentication] → [Configuration] submenu to configure the authentication method on a per port basis. If the authentication service has not been started the following window will appear:

### Authentication Configuration

802.1X Port-Based Authentication Disabled

Once the service is started using the [Layer2] → [Authentication] → [Management] submenu the following window will appear when using the [Layer2] → [Authentication] → [Configuration] submenu

### Authentication Configuration

Port	Control	Reauth	Reauth-period	Tx-period	Supp Time-out	Server Time-out
Port1	None	<input type="checkbox"/>				
Port2	None	<input type="checkbox"/>				
Port3	None	<input type="checkbox"/>				
Port4	None	<input type="checkbox"/>				
Port5	Auto	<input type="checkbox"/>	3600	30	30	30
Port6	None	<input type="checkbox"/>				
Port7	None	<input type="checkbox"/>				
Port8	None	<input type="checkbox"/>				
Port9	None	<input type="checkbox"/>				
Port10	None	<input type="checkbox"/>				
Port11	None	<input type="checkbox"/>				
Port12	None	<input type="checkbox"/>				
Port13	None	<input type="checkbox"/>				
Port14	None	<input type="checkbox"/>				

OK Cancel

### Authentication Configuration Parameter Description

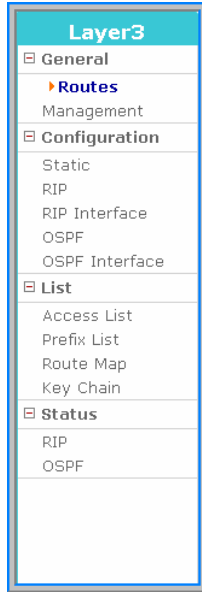
Parameter	Description
<b>Control</b>	Used to set the authentication mode of each port when employing the (802.1x) authentication - <b>None</b> : Authentication is not performed for the port. - <b>Force-authorized</b> : Admits the port forcibly. - <b>Force-unauthorized</b> : Blocks the port forcibly. - <b>Auto</b> : Allows the port through authentication from the Radius server and blocks the port.
<b>Reauth</b>	Used to set the port for re-authentication.
<b>Reauth-Period</b>	Used to set the timer for the re-authentication cycle when the Reauth box is checked. (1-4294967295sec) default: 3600 sec

Parameter	Description
<b>Tx-Period</b>	Used to set the cycle that sends Request regularly to supplicant. (1-65535sec) default: 30 sec
<b>Supp-Timeout</b>	Used to set the time before re-sending to the user when EAP is requested.(1-65535sec) default: 30 sec
<b>Sever-Timeout</b>	Used to set the time before re-sending to the device when server authentication of a server is requested.(1-65535sec) default: 30 sec

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

# Layer3 Menu

The Layer3 Menu is used to manage static and dynamic routing for the WIM. Select the [Layer3] Menu to begin configuring the routing statements and routing protocols. The [Layer3] submenus will be displayed in the upper left side of the window as follows:



## Layer3 Menu Submenu Description

Menu	Submenu	Description
<b>General</b>	Routes	Used to display the routing table of WIM.
	Management	Used to start or stop RIP, OSPF, and BGP.
<b>Configuration</b>	Static	Used to set up a static route.
	RIP	Used to set up RIP.
	RIP Interface	Used to sets the RIP interface.
	OSPF	Used to set up OSPF.
	OSPF Interface	Used to set up the OSPF interface.
<b>List</b>	Access List	Used to set up Access-lists.
	Prefix List	Used to set up Prefix-lists.
	Route Map	Used to set up Route-maps.
	Key Chain	Used to set up the key used for authentication of RIP v2.
<b>Status</b>	RIP	Used to display RIP network information.
	OSPF	Used to display OSPF Neighbor information.

## General

This submenu is used to start and stop the routing protocols RIP, OSPF, and BGP and to view the routing table of the WIM.

## Routes

In order to view all static and dynamic routes select the [Layer3] → [General] → [Routes] submenu. Click the refresh button to refresh the routing table.

### Routes

Type	Network	Entry
S *>	0.0.0.0/0	[1/0] via 216.62.86.129, eth0
C *>	127.0.0.0/8	is directly connected, loopback
C *>	192.168.1.0/24	is directly connected, eth2
K *>	192.168.2.0/24	via 216.62.86.129, ipsec0
C *>	216.62.86.128/25	is directly connected, eth0

Refresh

### Routes Window Field Description

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

## Management

In order to turn the WIM routing protocols on or off select the **[Layer3] → [General] → [Management]** submenu. Go to the Action pull down menu and select On or Off for each of the routing protocols. Click the OK button to submit the change.

### Management

Protocol	Current Status	Action
RIP	Start	On
OSPF	Start	On
BGP	Start	On

OK

## Configuration

In order to configure static routes, and set up the routing protocols RIP, OSP, and BGP the system administrator will use the **[Layer3] → [Configuration]** submenu.

### Static Route

Static routes are entered into the WIM by the system administrator. An entire network can be configured using static routes but this type of configuration is not fault tolerant. When there is a change in the network or a failure occurs between two statically defined nodes, traffic will not be rerouted. Select the **[Layer3] → [Configuration] → [Static]** submenu to set the static routes.

Static routes are set by using the Command line.

### Static

Command
<input type="text"/>

OK



In the example listed below the network administrator enters a static route of 100.0.0.0/24 going out through eth0. Click the OK button to submit the command.

### Static

Command
<input type="text" value="ip route 100.0.0.0/24 eth0"/>

OK

When the entered command is successfully executed, the configuration is directly applied to the <Current Status> section of the [Layer3] → [Configuration] → [Static] submenu.

## Current Status

Type	Network	Entry
S *>	0.0.0.0/0	[1/0] via 216.62.86.129, eth0
S *>	100.0.0.0/24	[1/0] is directly connected, eth0

The static route that was entered is redundant because the default route was already sending 100.0.0.0/24 traffic out of eth0.

## Current Status Parameter Description

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

## Help

If the system administrator is unsure which static route command to use then they may use the <Help> section to see all possible commands. Select the Command choice (either 'ip route' or 'no ip route' then use the Argument pull down menu to see the possible choices. For example if the administrator wants to see what the correct command is to remove the static route that was just entered they would select "no ip route" and then select the appropriate argument.

## Help

Command	Argument
no ip route	A.B.C.D/M (A.B.C.D INTERFACE )

Then at the command line the following command must be typed in. Then click the OK button to submit the change.

## Static

Command
no ip route 100.0.0.0/24 eth0

OK

## RIP

The Routing Information Protocol (RIP) is one of the most commonly used routing protocols on internal networks (and to a lesser extent, networks connected to The Internet). RIP helps routers dynamically adapt to routing changes on a network by communicating information about which networks each router within a network can reach and how far away those networks are. Select the **[Layer3] → [Configuration] → [RIP]** submenu to begin configuring RIP.

On the WIM the RIP information (basic and advanced commands) can be entered by using the Command field or by using the RIP Basic fields (basic commands only).

### RIP

Command
<input type="text"/>

OK

### RIP Basic

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

OK



In the Command field and RIP Basic examples listed below the network administrator is setting the 192.168.1.0 network for RIP version 2

### RIP

Command
network 192.168.1.0/24

OK

### RIP Basic

Command	Argument
Version	<input type="radio"/> 1 <input checked="" type="radio"/> 2 (default)
redistribute	<input type="checkbox"/> connected <input type="checkbox"/> static <input type="checkbox"/> ospf <input type="checkbox"/> bgp
network	192 . 168 . 1 . 0 / 24

OK

Enter the RIP command or enter the RIP Basic information. If the entered command or RIP Basic information is correct then click on the OK button to submit the change. The new RIP configuration is directly applied to <Current Status> of [Layer3] → [Configuration] → [RIP] submenu.

## Current Status

Router RIP
router rip
network 192.168.1.0/24

Delete

## Help

If a system administrator is unsure which RIP commands to use in the Command field then they may use the Help Command pull down menu to see all possible choices. Once a command is selected the Argument pull down menu will be populated with the appropriate choices. Once the correct RIP command is identified then type it into the Command field and click on the OK button to submit the change

## Help

Command	Argument
redistribute	(kernel connected static ospf isis bgp) metric <0-16> rout



## RIP Interface

The [Layer3] → [Configuration] → [RIP Interface] submenu is used to select the Interfaces which will use RIP, to apply advanced RIP functionality, and to select the send and receive RIP settings per Interface.



NOTE

If a WAN Interface is set up to work through a VPN Tunnel then it will not be possible to send routing updates through it. This includes RIP, OSPF and BGP.

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

### RIP Interface

Interface	Command
eth0	

OK

If the RIP command is successfully executed then the execution result is directly applied to the <Current Status> of [Layer3] → [Configuration] → [RIP Interface] submenu.

### Current Status

Router RIP Interface eth0
ip rip send version 1 2
ip rip receive version 1 2

### Help

If a system administrator is unsure which RIP commands to use then they may use the Help Command pull down menu to see all possible choices. Select the Command field (either “ip rip” or “no ip rip” and then the Argument field. Once the correct RIP command is identified then type it into the Command field and click on the OK button to submit the change

### Help

Command	Argument
ip rip	receive version 1 2

## RIP Interface Basic

The RIP Interface Basic fields are used to set the Interface to send and/or receive RIP Versions 1 and 2. After selecting each item click the OK button to submit the change. The applied value will be displayed in the <Current Status> window.

### RIP Interface Basic

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

OK

### Current Status

Router RIP Interface eth0	
ip rip send version	1 2
ip rip receive version	1 2

## OSPF

The Open Shortest Path First (OSPF) protocol is a link-state, hierarchical routing protocol. Dijkstra's algorithm which is used to calculate the shortest path tree. It uses cost as its routing metric. A link state database is constructed of the network topology which is identical with all routers in the OSPF area. OSPF is perhaps the most widely used Routing Protocol in large networks. Select the [Layer3] → [Configuration] → [OSPF] submenu to begin configuring OSPF.

On the WIM the OSPF information (basic and advanced commands) can be entered by using the Command field or by using the OSPF Basic fields (basic commands only).

### OSPF

Command
<input type="text"/>

OK

### OSPF Basic

Command	Argument			
redistribute	<input type="checkbox"/> connected	<input type="checkbox"/> static	<input type="checkbox"/> rip	<input type="checkbox"/> bgp
network	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> / <input type="text"/>	<input type="text"/>	area ID	

OK



In the Command field and OSPF Basic examples listed below the network administrator is setting the 192.168.1.0 network for OSPF with an area of 100. Click the OK button to apply the change.

## OSPF

Command
network 192.168.1.0/24 area 100

OK

## OSPF Basic

Command	Argument
redistribute	<input type="checkbox"/> connected <input type="checkbox"/> static <input type="checkbox"/> rip <input type="checkbox"/> bgp
network	192 . 168 . 1 . 0 / 24 100 area ID

OK

Both the Command field and OSPF Basic field entries listed above produce the same configuration and will be displayed under the current status.

## Current Status

Router OSPF
router ospf
network 192.168.1.0/24 area 100

Delete

## Help

If a system administrator is unsure which OSPF command to use in the Command field then they may use the Help Command pull down menu to see all possible choices. Once a command is selected the Argument pull down menu will be populated with the appropriate choices. Once the correct OSPF command is identified then type it into the Command field and click on the OK button to submit the change

## Help

Command	Argument
default-metric	<0-16777214>

## OSPF Interface

The [Layer3] → [Configuration] → [OSPF Interface] submenu is used to select the Interfaces which will use OSPF and to apply advanced OSPF functionality. The Command field may be used to enter both basic and advanced OSPF configuration commands and the OSPF Interface Basic fields may be used to enter Basic OSPF configuration commands.

### OSPF Interface

Interface	Command
eth0	

OK

### OSPF Interface Basic

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

OK

Select the target interface and then enter the OSPF configuration command using the Command field or OSPF Interface Basic fields.



NOTE

If a WAN Interface is set up to work through a VPN Tunnel then it will not be possible to send routing updates through it. This includes RIP, OSPF and BGP.

## Help

If a system administrator is unsure which OSPF commands to use then they may use the Help Command pull down menu to see all possible choices. Select the Command field (either “ip ospf” or “no ip ospf” and then the Argument field. Once the correct OSPF command is identified then type it into the Command field and click on the OK button to submit the change.

## Help

Command	Argument
ip ospf	{A.B.C.D} cost <1-65535>

Once an OSPF configuration command is successfully applied the results will be displayed in the [Layer3] → [Configuration] → [OSPF Interface] <Current Status> window.

## Current Status

Router OSPF Interface eth0
ip ospf cost 5
ip ospf dead-interval 55

# List

## Access List

Access Lists are used on the WIM to control access to the network. Access lists can prevent certain traffic from entering or exiting the router. Select the **[Layer3] → [List] → [Access List]** submenu to begin configuring the Access-list. After setting the target items, click the OK button.

### Access List

Option	Parameter
ID	Word <input type="text"/>
Action	<input type="radio"/> Permit <input checked="" type="radio"/> Deny
Source Match	<input type="radio"/> any <input checked="" type="radio"/> Network <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> / <input type="text"/>
Exact match	<input checked="" type="checkbox"/> On/Off

OK

### Access List Parameters

Item	Description					
<b>ID</b>	Used to set the Access-list name. <table border="1"> <tr> <td>1~99: Standard Access List</td> </tr> <tr> <td>100~199: Extended Access List</td> </tr> <tr> <td>1300~1999: Standard Access List</td> </tr> <tr> <td>2000~2699: Extended Access List</td> </tr> <tr> <td>Word: Named Access List</td> </tr> </table>	1~99: Standard Access List	100~199: Extended Access List	1300~1999: Standard Access List	2000~2699: Extended Access List	Word: Named Access List
1~99: Standard Access List						
100~199: Extended Access List						
1300~1999: Standard Access List						
2000~2699: Extended Access List						
Word: Named Access List						
<b>Action</b>	Used to allow or reject the packet matched.					
<b>Source Match</b>	Sets the match condition. Any - All packets Host - A host Network - Network range					
<b>Destination Match</b>	If the ID ranges from 100 to 199 or from 2000 to 2699, then the Destination Match can be set as well as the Source Match condition Any - All packets Host - A host Network - Network range					
<b>Exact match</b>	Available when ID is set to word and when match condition is set to Network. Sets only the packets matched correctly with the prefix.					

Once the Access List command is successfully executed then the results are directly applied to the **[Layer3] → [List] → [Access List] <Current Status>** window.

### Current Status

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

In order to delete an Access List select the radio button to the left of the Access List and then click the Delete button.

### Current Status Fields

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

## Prefix List

The Prefix List provides the most powerful prefix based filtering mechanism. In addition to access-list functionality the Prefix List has prefix length range specification and sequential number specification. You can add or delete prefix based filters to arbitrary points of Prefix List using sequential number specification. Select the **[Layer3] → [List] → [Prefix List]** submenu to configure the Prefix-list.

If no Prefix List is specified on the WIM then it acts as a permit rule. If the Prefix List is defined, and no match is found, then a default rule of deny is applied.

### Prefix List

Option	Parameter
ID	<input type="text"/>
Seq	<input type="text"/>
Action	<input checked="" type="radio"/> Permit <input type="radio"/> Deny
Prefix Match	<input checked="" type="radio"/> Any
	<input type="radio"/> <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> / <input type="text"/> ge: <input type="text"/> le: <input type="text"/>

## Prefix List Parameters

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

Once the Prefix List information is entered and saved then the results are directly applied to the [Layer3] → [List] → [Prefix List] <Current Status> window.

## Current Status

	ID	Entry
<input checked="" type="radio"/>	test	seq 5 permit 100.0.0.0/24

Once a Prefix List is set in the WIM it can be removed by selecting the radio button of the Prefix List and then click the Delete button.

## Prefix List Current Status Fields

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

## Route-Map

Route maps are similar to access lists as they both have criteria for matching the details of certain packets and an action of permitting or denying those packets. Use the [Layer3] → [List] → [Route-Map] submenu to begin configuring Route-Map.

Enter the target value and then click the OK button to save the change.

## Route-Map

Option	Parameter
Name	<input type="text" value="test"/>
Action	<input checked="" type="radio"/> Permit <input type="radio"/> Deny
Sequence	<input type="text" value="1"/>



Parameter	Description
<b>Name</b>	Route-map name
<b>Action</b>	Sets whether to apply set operation.
<b>Sequence</b>	Sets the sequence No. to additionally delete a route-map

If the Route-Map command is successfully entered and saved then the results will be directly applied to the <Current Status> of the [Layer3] → [List] → [Route-Map] submenu.

## Route-Map Setting

	Name	Entry
<input checked="" type="radio"/>	test	permit 10

## Route-Map Setting Field Description

Field	Description
<b>Name</b>	Route-map name
<b>Entry</b>	Route-map information

Once a Route-Map is created it can be defined. Highlight the radio button to the left of the Route –Map and click the edit button.

## Match

Option	Parameter
<input type="checkbox"/> IP	<input checked="" type="radio"/> Address <input type="text"/> <input type="checkbox"/> Use prefix-list <input type="radio"/> Next-hop <input type="text"/> <input type="checkbox"/> Use prefix-list
<input type="checkbox"/> Metric	<input type="text"/>

## Set

Option	Parameter
<input type="checkbox"/> IP	Next-hop <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
<input type="checkbox"/> Metric	<input type="text"/>
<input type="checkbox"/> Weight	<input type="text"/>
<input type="checkbox"/> Community	<input type="text"/>
<input type="checkbox"/> Metric-Type	Type-1 <input type="button" value="v"/>
<input type="checkbox"/> Local Preference	<input type="text"/>

Parameter	Description
<b>IP</b>	- Address: Used to set the access-list or prefix-list for an IP to be matched. - Next-hop: Used to set the Next-hop IP to be matched.
<b>Metric</b>	Used to set the Metric to be matched.

### Route-Map Set Parameter Description

Parameter	Description
<b>IP</b>	Used to set the next-hop of the BGP table.
<b>Metric</b>	Used to set the metric of the BGP table.
<b>Weight</b>	Used to set the weight of the BGP table.
<b>Community</b>	Used to set the community of the BGP table.
<b>Metric-Type</b>	Used to set the metric type of the BGP table. - Type 1: External Type 1 - Type 2: External Type 2
<b>Local Preference</b>	Used to set the local preference from BGP attribute.

If a Route-Map entry needs to be deleted then click the radio button to the left of the Route-Map and then click the Delete button. When the match condition is met and the Action is set to Permit then the job corresponding to Set operation is carried out. If the command is successfully entered and saved then the Route-Map result is directly applied to <Current Status> of the [Layer3] → [List] → [Route-Map] submenu.

### Current Status

	Sequence	Entry
<input type="radio"/>	10	match ip address test
<input type="radio"/>	10	set ip next-hop 1.1.1.1

### Current Status Field Description

Field	Description
<b>Sequence</b>	Matches/Sets operation Sequence No. of route-map.
<b>Entry</b>	Matches/Sets operation information of route-map.

Click the Prev button to return to the route-map window or click the Delete button to delete the selected Match/Set operation.

## Key Chain

The WIM uses the Key Chain window for setting up MD5 Authentication for (RIP) Version 2 packets. Select the [Layer3] → [List] → [Key Chain] submenu to begin configuring the Key Chain information. Enter the values and then click the OK button.

### Key Chain

Option	Parameter
Key Chain Name	<input type="text" value="rtrA"/>
Key ID	<input type="text" value="1"/>
Key String	<input type="text" value="123"/>

### Key Chain Parameter Description

Parameter	Description
Key Chain Name	Used to name the Key Chain rule
Key ID	ID number of the Key
Key String	Password to be used in authentication process

Once the Key Chain command is successfully entered and saved then the results are directly applied to the <Current Status> of the [Layer3] → [List] → [Key Chain] submenu.

### Key Chain

Option	Parameter
Key Chain Name	<input type="text"/>
Key ID	<input type="text"/>
Key String	<input type="text"/>

In order to remove a Key Chain entry click the radio button to the left of the Key Chain rule and then click the Delete button. Click the Delete All button to remove all Key Chain entries at the same time.

# Status

## RIP

The [Layer3] → [Status] → [RIP] submenu is used to display the RIP connection status and information of the WIM.

### RIP Information

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

Refresh

### RIP Status Field Description

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

## OSPF

The [Layer3] → [Status] → [OSPF] submenu is used to display the OSPF connection status and information of the WIM.

### OSPF Information

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

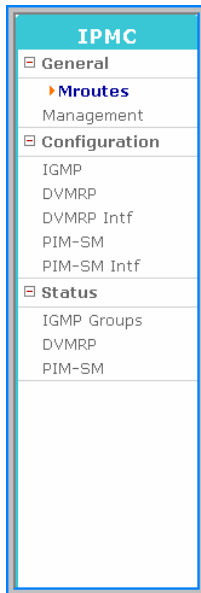
Refresh

### OSPF Status Field Description

Field	Description
Neighbor ID	Neighbor ID of the other routers using OSPF
Pri	Priority
State	Displays the state of the router.
Dead Time	Displays the dead time.
Address	Address of the other party
Interface	Interface connected

# IPMC Menu

For large amounts of data, IP Multicast is more efficient than normal Internet transmissions because the same data is broadcast to many recipients simultaneously. Unlike traditional Internet traffic that requires separate connections for each source-destination pair, IP Multicasting allows many recipients to share the same source. This means that just one set of packets is transmitted for all the destinations. Select the [IPMC] menu to begin configuring IPMC. The submenus will be displayed in the upper left side of the window as follows:



## IPMC Menu Description

Menu	Submenu	Description
<b>General</b>	Mroutes	Used to display the Multicast Routing Entry.
	Management	Used to starts/stop IPMC protocol daemons.
<b>Configuration</b>	IGMP	Used to display or change the IGMP configuration.
	DVMRP	Used to display or change the DVMRP default configuration.
	DVMRP Intf	Used to display or change the VIF of the DVMRP.
	PIM-SM	Used to display or change the PIM-SM default configuration.
	PIM-SM Intf	Used to display or change the VIF PIM-SM.
<b>Status</b>	IGMP Groups	Used to displays the IGMP Group information.
	DVMRP	Used to display the DVMRP neighbor and Prune information.
	PIM-SM	Used to display the PIM-SM Neighbor information.

## General

### Mroutes

The [IPMC] → [General] → [Mroutes] submenu is used to display the multicast routing entries.

#### Mroutes

Mroute	Uptime	Expires	Flags	Incoming	Outgoing
(100.1.1.11, 224.1.1.100)	00:00:08	00:03:22	TF	rd2	rd3

I: Immediate Stat, T: Timed Stat, F: Forwarder installed

#### Mroute Field Description

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

### Management

The [IPMC] → [General] → [Management] submenu is used to start or stop dvmrpd and pimd, IPMC protocol daemons. The <Current Status> field of Management window shows the current status of each daemon. To change the daemon status use the [Action] pull down menu and then click the OK button.

#### Management

Protocol	Current Status	Action
DVMRP	Stop	On
PIM	Stop	Off

#### IPMC Management Field Description

Field	Description
Protocol	IPMC protocol
Current Status	Current IPMC protocol demon status
Action	New status of IPMC protocol demon status

# Configuration

## IGMP

The Internet Group Management Protocol is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. The **[IPMC] → [Configuration]** submenu is used to display and change the WIM IGMP configuration.

### IGMP & Help

IGMP commands can be entered into the Command field and saved by clicking the OK button.. Use the Help field to find an IGMP command.

### IGMP

Command	
<input type="text"/>	
<input type="button" value="OK"/>	

### Help

Command	Argument
<input type="text" value="clear ip igmp"/>	<input type="text" value="group"/>

### IGMP Basic

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

### IGMP Basic

Command	Argument
Interface	<input checked="" type="radio"/> All <input type="radio"/> <input type="text" value="eth0"/> (192.168.17.100/16)
IGMP Query Interval	<input type="text" value="125"/> (1~65535, Default: 125)
Max Response Time	<input type="text" value="10"/> (1~25, Default: 10)

### IGMP Basic Parameter Description

Parameter	Description
<b>Interface</b>	Select the target IGMP interface and select All. Then, all interface configuration values are applied
<b>IGMP Query Interval</b>	Cycle of sending IGMP Membership Query

Parameter	Description
<b>Max Response Time</b>	Maximum time of waiting a response after sending Membership Query

### IGMP Interface Information

This section of the [IPMC] → [Configuration] → [IGMP] window is used to display the IGMP interfaces.

### IGMP Interface Information

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

Refresh

### IGMP Interface Field Description

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



## Configuration / DVMRP

The Distance Vector Multicast Routing Protocol (DVMRP) is an Internet routing protocol that provides an efficient mechanism for connectionless message multicast to a group of hosts across an internetwork. The [IPMC] → [Configuration] → [DVMRP] submenu is used to display and change the WIM DVMRP configuration.

### DVMRP & Help

DVMRP commands can be entered into the Command field and saved by clicking the OK button. Use the Help field to find a DVMRP command.

### DVMRP

Command
<input type="text"/>
OK

### Help

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

### DVMRP Routes

This submenu is used to display the DVMRP Route items in use.

### DVMRP Routes

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

Refresh

### DVMRP Routes Field Description

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

Field	Description
Uptime	Time passed after using the DVMRP route item
Expires	Left time until the DVMRP route item is expired

## DVMRP Intf

The [IPMC] → [Configuration] → [DVMRP Intf] submenu is used to add or set the DVMRP VIF (Virtual Interface).

### RD Interface

This window is used to add L3 interfaces where an IP address is set to DVMRP VIF. Select the target interface to be added to the VIF from the Interface and then enter the target value, and click the Add button.

### RD Interface

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

Add

### RD Interface Parameter Description

Parameter	Description
Interface	Used to select the target L3 interface
Reject Non-pruners	Select the Non-pruners box to indicate that the neighbors only support DVMRP with an older version.
Metric	Metric(=distance) value to be used for multicasting routing by VIF

### DVMRP Interfaces

This section of the submenu is used to display the configuration of the DVMRP VIF. To delete a specific VIF, check the check box on the left of the entry and then click the Delete button.

### DVMRP Interfaces

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

Delete

Refresh

## DVMRP Interfaces Field Description

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

## PIM-SM

PIM-SM or Protocol Independent Multicast - Sparse-Mode (PIM-SM) is a protocol for efficiently routing to multicast groups that may span wide-area (and inter-domain) internets. Use the [IPMC] → [Configuration] → [PIM-SM] submenu to begin configuring the PIM-SM on the WIM.

### PIM-SM & Help

PIM-SM commands can be entered into the Command field and saved by clicking the OK button. Use the Help field to find a PIM-SM command.

### PIM-SM

Command
<input type="text"/>
<input type="button" value="OK"/>

### Help

Command	Argument
clear ip pim <input type="button" value="v"/>	sparse-mode bsr rp-set * <input type="button" value="v"/>

## PIM-SM Basic

These fields are used to set the BSR and RP of the PIM-SM protocol. Mark the check box to the left of each item and then enter the configuration values. Click the OK button to apply the values. To delete the values mark the check box to the left of the item and then click the **Delete** button.

## PIM-SM Basic

	Command	Argument
<input checked="" type="checkbox"/>	RP Address	192 . 168 . 17 . 100
<input checked="" type="checkbox"/>	RP Candidate	eth0 [vif] 22 Priority(0~255)
<input checked="" type="checkbox"/>	BSR Candidate	eth0 [vif] 30 MaskLen(0~32) 100 Priority(0~255)

## PIM-SM Basic Parameter Description

Parameter	Description
<b>RP Address</b>	When setting static RP, enter the IP address of RP
<b>RP Candidate</b>	When setting RP Candidate, select VIF and enter the target priority.(Low value has high priority.)
<b>BSR Candidate</b>	When setting BSR Candidate, select VIF and enter the target Mask Length and Priority.(High value has high priority.)

## BootStrap Information

This section of the [IPMC] → [Configuration] → [PIM-SM] submenu is used to display the information on the BootStrap router.

## BootStrap Information

BootStrap Information
PIMv2 Bootstrap information This system is the Bootstrap Router (BSR) BSR address: 192.168.0.99 Uptime: 00:00:04, BSR Priority: 100, Hash mask length: 30 Expires: 00:02:06 Role: Candidate BSR State: Pending BSR  Candidate RP: 192.168.0.99(eth0) Advertisement interval 60 seconds Next Cand_RP_advertisement in 00:00:58

## RP Information

This section of the [IPMC] → [Configuration] → [PIM-SM] submenu is used to display the information on the RP router.

## RP Information

RP Information	
PIM Group-to-RP Mappings	
Group(s): 224.0.0.0/4	
RP: 192.168.0.99	
Info source: 192.168.0.99, via bootstrap, priority 22	
Uptime: 00:00:02, expires: 00:02:28	
Group(s): 224.0.0.0/4, Static	
RP: 192.168.17.100	
Uptime: 00:00:38	

## PIM-SM Intf

The [IPMC] → [Configuration] → [PIM-SM Intf] submenu is used to add or modify the PIM-SM VIF (Virtual Interface).

## RD Interface

This section of the [IPMC] → [Configuration] → [PIM-SM Intf] submenu is used to add PIM-SM VIF. Select the target L3 interface from the Interface pull down menu and then enter the target values. Once done click the Add button to add the PIM-SM VIF.

## RD Interface

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

## PIM-SM RD Interface Parameter Description

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

## PIM-SM Interfaces

This section of the [IPMC] → [Configuration] → [PIM-SM Intf] submenu is used to display the VIFs added to the PIM-SM. To delete a VIF, click the check box on the left of the entry and then click the Delete button.

## PIM-SM Interfaces

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

Delete

Refresh

## IGMP Groups

The [IPMC] → [Status] → [IGMP Groups] submenu is used to display the information on registered IGMP groups.

## IGMP Group Information

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

Refresh

## IGMP Groups Field Description

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

# Status

## DVMRP

The [IPMC] → [Status] → [DVMRP] submenu is used to display the information on DVMRP Neighbors.

### DVMRP Neighbors

This section of the [IPMC] → [Status] → [DVMRP] submenu is used to display the information on the DVMRP neighbor whose information is exchanged with the WIM.

### DVMRP Neighbors

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

Refresh

### DVMRP Neighbors Field Description

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

### DVMRP Prune Information

This section of the [IPMC] → [Status] → [DVMRP] submenu is used to display the DVMRP Prune items.

### DVMRP Prune Information

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

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

Refresh

### DVMRP Prune Information Field Description

Field	Description
Source Address	Host Ip address that sends multicast packets
MaskLen	Mask length of DVMRP Prune
Group Address	Multicast group address

Field	Description
<b>State</b>	Flags that display the DVMRP Prune status. Refer to the description on the lower side
<b>FCR Cnt</b>	DVMRP Forwarding Cache count
<b>Expires</b>	Time passed after the DVMRP Prune information is created
<b>ReXmit</b>	Left time until retransmission

## PIM-SM

The [IPMC] → [Status] → [PIM-SM] submenu is used to display the neighbor list of the PIM-SM protocol.

### PIM-SM Neighbors

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

Refresh

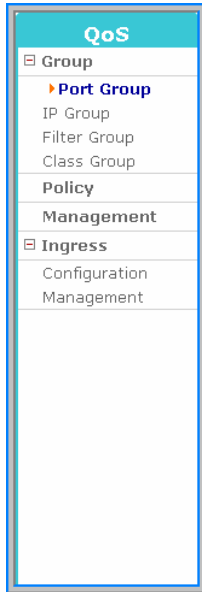
### PIM-SM Neighbors Field Description

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



# QoS Menu

Quality of Service (QoS) refers to the capability of a network to provide better service to selected network traffic over various IP technologies. Select the **[QoS]** menu to begin configuring QoS. The QoS submenus will be displayed in the upper left side of the window as follows:



## QoS Menu Description

Menu	Submenu	Description
<b>Group</b>	Port Group	Used to retrieve, set, edit, or delete a Port Group
	IP Group	Used to retrieve, set, edit, or delete an IP Group
	Filter Group	Used to retrieve, set, edit, or delete a Filter Group
	Class Group	Used to retrieve, set, edit, or delete a Class Group
<b>Policy</b>	-	Used to set a class for a port
<b>Management</b>	-	Used to start or stop the QoS service and to set the WIM to start QoS automatically when the system reboots.
<b>Ingress</b>	Configuration	Used to retrieve/Set up/Edit/Delete QoS setting values of an Ingress
	Management	Used to execute an Ingress QoS or to stop the operation.

# Group

## Port Group

The WIM uses the Port Group submenu to define specific IP ports or ranges of IP ports for the QoS policies. Select the [QoS] → [Group] → [Port Group] submenu to retrieve, set, edit, or delete a port group.

### Port Group List

Name	Port
------	------

In order to add a Port Group List click the Add button and a new Port Group window will be displayed. Enter the Port Group information and then click the OK button to save the changes.



In the examples listed below there are three Port Groups created. One is for ports 6000 through 6100 which will be used for the MP40 card, the second is for ports 30000 through 30031 for the MGI card, and the last is for ports 1 through 65001 for TCP on the entire network.

### Port Group

Category	Configuration
ID	<input type="text" value="MCP_Ports"/>
Port	<input type="checkbox"/> <input type="text" value="6000"/> ~ <input type="text" value="6100"/>

Click the Add button to create another Port Group

### Port Group

Category	Configuration
ID	<input type="text" value="MGI_Ports"/>
Port	<input type="checkbox"/> <input type="text" value="30000"/> ~ <input type="text" value="30031"/>

Click the Add button to create another Port Group

### Port Group

Category	Configuration
ID	<input type="text" value="All_TCP"/>
Port	<input type="checkbox"/> <input type="text" value="1"/> ~ <input type="text" value="65001"/>

## Port Group Parameter Description

Parameter	Description
<b>ID</b>	Name of the port group - Should include both letters and numbers. - Group ID must start only with letters. - No blanks should be left in between characters.
<b>Port</b>	- Port range - Enter '0' to set all ports

## Port Group List

	Name	Port
<input checked="" type="radio"/>	MCP_Ports	6000-6100
<input type="radio"/>	MGI_Ports	30000-30031
<input type="radio"/>	All_TCP	1-65001

In order to delete a Port Group List highlight the radio button to the left of the Port Group List and then click the delete button.

## IP Group

The WIM uses the IP Group submenu to define specific IP addresses for the QoS policies. Select the [QoS] → [Group] → [IP Group] to retrieve, set, edit, or delete an IP group.

## IP Group List

Name	IP
------	----

Click the Add button in the above window to open another window from which the IP group information can be entered.



In the examples listed below there are three IP Groups created. One is for the MP40 at IP Address 192.168.1.200, the second is for the MGI card at IP Address 192.168.1.201, and the last is for the entire 192.168.1.0/24 network.

## IP Group

Category	Configuration
ID	<input type="text" value="MCP_IP"/>
IP	<input type="checkbox"/> <input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="1"/> . <input type="text" value="200"/> / <input type="text" value="24"/>

Enter the IP Group ID and then the IP address information. Click the OK button to save the changes Click the Add button to add another IP Group.

## IP Group

Category	Configuration
ID	<input type="text" value="MGI_IP"/>
IP	<input type="checkbox"/> <input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="1"/> . <input type="text" value="201"/> / <input type="text" value="24"/>

## IP Group

Category	Configuration
ID	<input type="text" value="Network"/>
IP	<input type="checkbox"/> <input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="1"/> . <input type="text" value="0"/> / <input type="text" value="24"/>

Click the OK button and then click the Add button to create another IP Group.

## IP Group Parameter Description

Parameter	Description
<b>ID</b>	Used to enter the 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.
<b>IP</b>	Used to enter the IP address information of the IP Group /: Used for entering subnet -: Used for entering the range of IPs Enter '0.0.0.0/0' to set all ports.

## IP Group List

	Name	IP
<input checked="" type="radio"/>	MCP_IP	192.168.1.200/24
<input type="radio"/>	MGI_IP	192.168.1.201/24
<input type="radio"/>	Network	192.168.1.0/24

In order to delete a IP Group List highlight the radio button to the left of the IP Group List and then click the delete button.

## Filter Group

The WIM uses the Filter Group submenu to define specific filtering rules for the QoS policies. Select the [QoS] → [Group] → [Filter Group] submenu to retrieve, set, edit, or delete a filter group. The Filter group can be filtered by Transport Protocol, TOS, IP Group, and Port Group.

### Filter Group List

Name	Prio	Trans	Source IP / PORT	Destination IP / PORT	ToS
------	------	-------	------------------	-----------------------	-----

Click the Add button in the above window to open another window from which the Filter Group List information can be entered. Enter a Filter ID, select a priority number, select a Transport Protocol, define the TOS bits, define the Source and Destination IP Group and Port Group, and then click the save button.



In the examples listed below there are three Filter Groups created. One is for the VoIP Traffic, the second is for the MP40, and the last is for the rest of the TCP traffic on the 192.168.1.0/24 network.

### Filter Group

Category	Value
ID	VoIP
Network Protocol	IP
Priority	1
Transport Protocol	UDP
TOS	<input checked="" type="radio"/> DEC <input type="text"/> <input type="radio"/> HEX 0x <input type="text"/>
Source IP:Port	any : any
Destination IP:Port	MGI_IP : MGI_Ports

Click the Add button to create another Filter Group.

### Filter Group

Category	Value
ID	TCP_MCP
Network Protocol	IP
Priority	2
Transport Protocol	TCP
TOS	<input checked="" type="radio"/> DEC <input type="text"/> <input type="radio"/> HEX 0x <input type="text"/>
Source IP:Port	any : any
Destination IP:Port	MCP_IP : MCP_Ports

## Filter Group

Category	Value
ID	<input type="text" value="All_TCP"/>
Network Protocol	IP
Priority	<input type="text" value="3"/>
Transport Protocol	<input type="text" value="TCP"/>
TOS	<input checked="" type="radio"/> DEC <input type="text"/> <input type="radio"/> HEX 0x <input type="text"/>
Source IP:Port	<input type="text" value="any"/> : <input type="text" value="any"/>
Destination IP:Port	<input type="text" value="Network"/> : <input type="text" value="All_TCP"/>

### Filter Group Parameter Description

Parameter	Description
<b>ID</b>	Used to enter the 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.
<b>Priority</b>	Queue Priority
<b>Transport Protocol</b>	TCP or UDP Protocol
<b>TOS</b>	TOS entry
<b>Source IP:Port</b>	Source IP Address and Port number/s
<b>Destination IP:Port</b>	Destination IP Address and Port number/s

### Filter Group List

	Name	Prio	Trans	Source IP / PORT	Destination IP / PORT	ToS
<input checked="" type="radio"/>	VoIP	1	udp	any / any	MGI_IP / MGI_Ports	
<input type="radio"/>	TCP_MCP	2	tcp	any / any	MCP_IP / MCP_Ports	
<input type="radio"/>	All_TCP	3	tcp	any / any	Network / All_TCP	

In order to delete a Filter Group List highlight the radio button to the left of the Filter Group List and then click the delete button.

## Class Group

The [QoS] → [Group] → [Class Group] submenu is used by the administrator to retrieve, set, edit, or delete SPQ Class Group and HTB Class Group configurations.

### SPQ Class Group

Begin configuring the Strict Policy Queuing by clicking the Add button.

### SPQ Class Group List

Name	Type	High Priority	Middle Priority	Low Priority
------	------	---------------	-----------------	--------------

After the Add button is clicked the SPQ Class Group configuration window will open. By default the Class Type is set to leaf. Set the ID and filter of the leaf classes and then click the OK button to save the changes.

### SPQ Class Group

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

### Filter Apply

Filter List	Action	Apply Filter
VoIP	ADD >>	<input type="text"/>
TCP_MCP	ADD ALL >>>	
All_TCP	<< REMOVE	
	<<< REMOVE ALL	



In the examples listed below there are three leaf and one root SPQ Class Groups created. One leaf is for the VoIP Traffic, the second is for the MP40, and the last leaf is for the rest of the TCP traffic on the 192.168.1.0/24 network. The root group prioritizes the leaves into High, Middle, and Low Priority Groups.

Example 1 shows a SPQ leaf Class Group which was designed for VoIP traffic.

### SPQ Class Group

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

### Filter Apply

Filter List	Action	Apply Filter
TCP_MCP All_TCP	ADD >> ADD ALL >>> << REMOVE <<< REMOVE ALL	VoIP

OK Cancel

Example 2 shows a SPQ leaf Class Group which was designed for MCP TCP traffic.

### SPQ Class Group

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

### Filter Apply

Filter List	Action	Apply Filter
VoIP All_TCP	ADD >> ADD ALL >>> << REMOVE <<< REMOVE ALL	TCP_MCP

OK Cancel



Example 3 shows a SPQ leaf Class Group which was designed for all other TCP traffic.

### SPQ Class Group

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

### Filter Apply

Filter List	Action	Apply Filter
VoIP	ADD >>	All_TCP
TCP_MCP	ADD ALL >>>	
	<< REMOVE	
	<<< REMOVE ALL	

Once the SPQ Class leaf Groups are created then it is time to define the SPQ root. Select the root radio button in the Class Type row to open the following window. Assign the Class Group ID, and then use the pull down menus to assign the High, Middle, and Low priorities for the leaf classes previously defined.

### SPQ Class Group

Category	Value
ID	Root
Class Type	<input checked="" type="radio"/> root <input type="radio"/> leaf
High	VoIP
Middle	TCP_MCP
Low	All_TCP

### SPQ Class Group Parameter Description

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



### SPQ

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

## HTB Class Group

HTB uses the concept of tokens and buckets along with the class-based system and filters to allow for complex and granular control over traffic. With a complex borrowing model, HTB can perform a variety of sophisticated traffic control techniques. One of the easiest ways to use HTB immediately is that of shaping. Begin configuring the Hierchical Token Bucket by clicking the Add button in the <HTB Class Group> window.

## HTB Class Group

Category	Value
ID	<input type="text"/>
Class Type	<input checked="" type="radio"/> root <input type="radio"/> inner <input type="radio"/> default <input type="radio"/> leaf
Rate	<input type="text"/> B/s

When configuring HTB it is best to begin by creating the root. Assign a Root ID, click the root radio button, and define the bandwidth allocation.



In the example listed below the root is defined with an allocated bandwidth of 1000 KBs.

## HTB Class Group

Category	Value
ID	Root
Class Type	<input checked="" type="radio"/> root <input type="radio"/> inner <input type="radio"/> default <input type="radio"/> leaf
Rate	1000 KB/s

The second step in the HTB configuration is creating the Inner rule. From the <HTB Class Group List> window click the Add button. Assign an Inner ID, click the inner radio button, define the Parent (root), define the Rate parameter (minimal desired speed) and the Ceil parameter (maximum desired speed).



In the example listed below there will only be one Inner class so 800 KBs will be used. The remaining 200 KBs will be used for the Default class.

### HTB Class Group

Category	Value
ID	Inner
Class Type	<input type="radio"/> root <input checked="" type="radio"/> inner <input type="radio"/> default <input type="radio"/> leaf
Parent ID	Root
Rate	800 KB/s
Ceil	800 KB/s

OK Cancel

The third step in the HTB configuration is creating the Default class. A default class is used with every HTB Queue. The default Priority is 0, which causes any unclassified traffic to be dequeued at hardware speed, completely bypassing any of the classes attached to the root Queue.

From the <HTB Class Group List> window click the Add button. Assign a Default ID, click the default radio button, set the Parent ID (root), select a priority, and define the Rate parameter (minimal desired speed) and the Ceil parameter (maximum desired speed).



In the example listed below there will only be one Default class. The default Priority will be set to 0 so all unclassified traffic will bypass any of the classes attached to the root Queue. The Parent ID will be set to Root, and the rate will be set to 200 KBs and the Ceil will be set to 200 KBs as well.

### HTB Class Group

Category	Value
ID	Default
Class Type	<input type="radio"/> root <input type="radio"/> inner <input checked="" type="radio"/> default <input type="radio"/> leaf
Parent ID	Root
Priority	0
Rate	200 KB/s
Ceil	200 KB/s

OK Cancel

The fourth step in the HTB configuration is to create the Leaf rules. From the <HTB Class Group List> window click the Add button. Assign a Leaf ID, click the leaf radio button, set the Parent ID (inner), select a priority, define the Rate parameter (minimal desired speed) and the Ceil parameter (maximum desired speed), and then select the Filter to apply.



In the examples listed below there will be three Leaf configurations (One for VoIP traffic, one for TCP MP40 traffic, and one for all other TCP traffic). The Voip Group will have a priority of 1, and will have a minimum speed of 300 KBs and a maximum speed of 800KBs, the TCP for the MP40 group will have a priority of 2, and will have a minimum speed of 300 KBs and a maximum speed of 600KBs, and the All TCP droup will have a priority of 3, and will have a minimum speed of 200 KBs and a maximum speed of 500KBs,

### HTB Class Group

Category	Value	
ID	Voip_Leaf	
Class Type	<input type="radio"/> root <input type="radio"/> inner <input type="radio"/> default <input checked="" type="radio"/> leaf	
Parent ID	Inner	
Priority	1	
Rate	300	KB/s
Ceil	800	KB/s

### Filter Apply

Filter List	Action	Apply Filter
TCP_MCP	ADD >>	VoIP
All_TCP	ADD ALL >>>	
	<< REMOVE	
	<<< REMOVE ALL	

Enter the information for the VoIP\_Leaf class and then click the OK button to save the changes.

### HTB Class Group

Category	Value	
ID	MCP_TCP	
Class Type	<input type="radio"/> root <input type="radio"/> inner <input type="radio"/> default <input checked="" type="radio"/> leaf	
Parent ID	Inner	
Priority	2	
Rate	200	KB/s
Ceil	600	KB/s

### Filter Apply

Filter List	Action	Apply Filter
VoIP	ADD >>	TCP_MCP
All_TCP	ADD ALL >>>	
	<< REMOVE	
	<<< REMOVE ALL	

Enter the information for the MCP\_MP40\_Leaf class and then click the OK button to save the changes.

## HTB Class Group

Category	Value
ID	All_TCP
Class Type	<input type="radio"/> root <input type="radio"/> inner <input type="radio"/> default <input checked="" type="radio"/> leaf
Parent ID	Inner
Priority	3
Rate	200 KB/s
Ceil	500 KB/s

## Filter Apply

Filter List	Action	Apply Filter
VoIP	ADD >>	All_TCP
TCP_MCP	ADD ALL >>>	
	<< REMOVE	
	<<< REMOVE ALL	

Enter the information for the All\_TCP\_Leaf class and then click the OK button to save the changes.

## HTB Class Group List

	Name	Type	Parent	Prio	Rate	Ceil
<input checked="" type="radio"/>	Root	root	-	-	1000 KB/s	-
<input type="radio"/>	Inner	inner	Root		800 KB/s	800 KB/s
<input type="radio"/>	Default	default		0	200 KB/s	200 KB/s
<input type="radio"/>	Voip_Leaf	leaf	Inner	1	300 KB/s	800 KB/s
Filter	VoIP					
<input type="radio"/>	MCP_TCP	leaf	Inner	2	200 KB/s	600 KB/s
Filter	TCP_MCP					
<input type="radio"/>	All_TCP	leaf	Inner	3	200 KB/s	500 KB/s
Filter	All_TCP					

Each class group can either be modified or deleted by clicking the radio button to the left of the class group and then by clicking the Edit or Delete button.

## HTB Class Group List Parameter Description

Item	Description
<b>Class Type</b>	Configuration window depends on the type of the class to be set. - root: Sets the root class. - inner: Sets the class that connects the root with the leaf classes. - default: Sets the default class. - leaf: Sets the leaf class.
<b>Parent ID</b>	If the target class is a child class of another class, set the parent class in the Parent ID item. Do not set the Parent ID if the target class is the root class(highest level class physically connected to the device) or if the default class (class including the bandwidth for traffics that do not belong to a filter).
<b>Priority</b>	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.
<b>Rate</b>	This is the basic minimal bandwidth needed for setting class for an assigned bandwidth.
<b>Ceil</b>	Maximum value of assigned bandwidth.
<b>Filter List</b>	Used to set the filtering rules for the class.
<b>Scheduling Parameter</b>	Used to set the bandwidth of the class based on day of the week and hour.

## Policy

The [QoS] → [Group] → [Policy] submenu is used for setting the QDISC type and root class class for an interface.

### Policy

Category	Configuration
Device	<input type="text" value="Ethernet0"/>
QDISC Type	<input checked="" type="radio"/> SPQ <input type="radio"/> HTB
Root Class	<input type="text" value="none"/>

Device	QDISC Type	Root Class	Default Class
Serial0			
Serial1			
Ethernet0			
Ethernet1			
Ethernet2			

Save

### Policy Parameter Description

Parameter	Description
<b>Device</b>	Used to select an interface (eth0, eth1, eth2, V.35, or HSSI)
<b>QDISC Type</b>	Used to select the QDISC to be applied to the interface
<b>Root Class</b>	Used to assign a Class connected to the interface. Select the class group from the class group list.
<b>Default Class (HTB only)</b>	This class defines the bandwidth for incoming traffic that is not applicable to any filtering rules. Select the class group from the class group list.

## SPQ Policy

In order to set up the Interface for SPQ use the Device pull down menu and select the Interface, then select the radio button for SPQ, select the Root Class, and then click the Save button to apply the change.

### Policy

Category	Configuration
Device	Ethernet0
QDISC Type	<input checked="" type="radio"/> SPQ <input type="radio"/> HTB
Root Class	Traffic

Device	QDISC Type	Root Class	Default Class
Serial0			
Serial1			
Ethernet0	spq	Traffic	
Ethernet1			
Ethernet2			

Save

## HTB Policy

In order to set up the Interface for HTB use the Device pull down menu and select the Interface, then select the radio button for HTB, select the Root Class, and then click the Save button to apply the change.

### Policy

Category	Configuration
Device	Ethernet0
QDISC Type	<input type="radio"/> SPQ <input checked="" type="radio"/> HTB
Root Class	Root
Default Class	Default

Device	QDISC Type	Root Class	Default Class
Serial0			
Serial1			
Ethernet0	htb	Root	Default
Ethernet1			
Ethernet2			

Save



## Management

The [QoS] → [Group] → [Management] submenu is used to start and stop the QoS service. In addition, this submenu is used to start or stop the execution of the 'Scheduling Parameter' set in the [QoS] → [Group] → [Class Group] submenu.

### QoS Management

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

## Ingress

The [QoS] → [Ingress] → [Configuration] submenu is used by the administrator to set up, retrieve, edit or delete the class group from the [Ingress] menu.

### Ingress Configuration

This page is used to retrieve, set up, edit, or delete the TOS value for each device in the [Ingress Configuration] menu.

**Ingress Configuration**

Category	Configuration
Device	Etherne
TOS	<input checked="" type="radio"/> DEC <input type="text"/> <input type="radio"/> HEX 0x <input type="text"/>

Device	TOS
Ethernet0	
Ethernet1	
Ethernet2	

Using the Device pull down menu select the target interface and then select DEC (10 digits) or HEX (16 digits). Then enter the Tos value and click the Save button.

### Ingress Parameter Description

Parameter	Description
Device	Used to select a port to set up Ingress QoS (Ethernet0, Ethernet1, or Ethernet2)
TOS	When a packet is Ingress and the TOS is set up then that packet is preferentially transmitted.

### Ingress Management

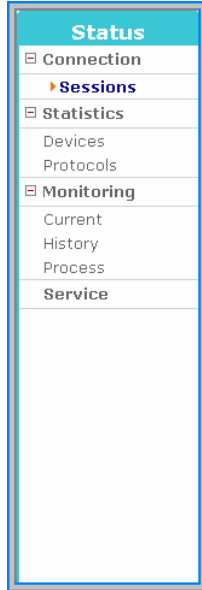
The [QoS] → [Ingress] → [Management] submenu is used to start or stop the Ingress service.

#### Ingress Management

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

# Status Menu

The Status Menu is used to view active IP sessions on the WIM, to display statistics on interfaces and protocols, and to view CPU utilization. Select the [**Status**] menu to begin viewing the system information . The submenus will be displayed in the upper left side of the window as follows:



## Status Menu Description

Menu	Submenu	Description
<b>Connection</b>	Sessions	Used to display the information on the IP address and IP ports connected to WIM.
<b>Statistics</b>	Devices	Used to display the WIM network statistics for the Tx and Rx of each interface.
	Protocols	Used to display the WIM network statistics of each protocol.
<b>Monitoring</b>	Current	Provides the WIM network statistics in a table format in real time.
	History	Used to display the WIM network statistics on an hourly, weekly, monthly, yearly basis.
	Process	Used to display the information (such as CPU utilization and memory usage) on processes being run in WIM.
<b>Services</b>	-	Used to display the service status in a table format. The services are categorized into Security, Router, Application, and Management tables.

# Connection

## Sessions

The [Status] → [Connection] → [Sessions] submenu is used to display the IP Address and IP Port information for devices connected to WIM.

### 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

### Session List Field Description

Field	Description
<b>Protocol</b>	This field displays the type of protocol connected with session (UDP, TCP)
<b>Src IP</b>	This field displays the source IP Address
<b>Src Port</b>	This field displays the source IP port
<b>Status</b>	- UNREPLIED: Packets that are expected to be answered are received, but there is no response packet. - ASSURED: There is no response packet. (‘UNREPLIED’ is changed to ‘ASSURED’.)
<b>Dst IP</b>	This field displays the destination IP Address
<b>Dst Port</b>	This field displays the destination IP port

# Statistics

## Devices

The [Status] → [Statistics] → [Devices] submenu is used to display WIM network statistics by classifying the received and transmitted part of each device.

### Received

Devices	Bytes	Packets	Errs	Drop	FIFO	Frame	Compressed	Multicast
Ethernet 0	18451009	271173	0	0	0	0	0	0
Ethernet 1	0	0	0	0	0	0	0	0
Ethernet 2	24840	414	0	0	0	0	0	0
Ethernet 3	0	0	0	0	0	0	0	0
Serial0	1256078	89713	2	0	0	2	0	0

### Transmitted

Devices	Bytes	Packets	Errs	Drop	FIFO	Frame	Compressed	Multicast
Ethernet 0	7555122	15840	0	0	0	0	0	0
Ethernet 1	0	0	0	0	0	0	0	0
Ethernet 2	126	3	0	0	0	0	0	0
Ethernet 3	0	0	0	0	0	0	0	0
Serial0	1076652	89713	0	0	0	0	0	0

Refresh

### Devices Received and Transmitted Field Description

Field	Description
<b>Devices</b>	Interface type
<b>Bytes</b>	Displays the total number of bytes received or transmitted
<b>Packets</b>	Displays the total number of packets received or transmitted
<b>Errs</b>	Displays the number of packets when an error occurs
<b>Drop</b>	Displays the number of packets lost
<b>FIFO</b>	Displays the FIFO queue is full(FIFO Overrun)
<b>Frame</b>	Displays the ethernet header count when a frame does not meet the format (Frame Alignment Error)
<b>Compressed</b>	Displays the number of compressed packets
<b>Multicast</b>	Displays the number of multicast packets

## Protocols

The [Status] → [Statistics] → [Protocols] is used to display WIM network statistics of each protocol type (Unit: Byte).

### Network statistics by protocols

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

## Monitoring

### Current

The [Status] → [Monitoring] → [Current] submenu is used to display the WIM network statistics in real time. The data window is updated every 5 seconds.

### Rate(Bytes/Sec)

Devices	Received	Transmitted	Trans/Recv
Ethernet 0	319	1175	298
Ethernet 1	0	0	0
Ethernet 2	0	0	0
Ethernet 3	0	0	0
Serial 0	2	2	0

## History

The [Status] → [Monitoring] → [History] submenu is used to display the CPU utilization, available memory capacity, and network statistics of the WIM router with an accumulation value on an hourly, weekly, monthly, and yearly basis.

### Accumulated Monitoring Graph

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

Ethernet Interface	Selection Check
Ethernet 0	<input type="radio"/>
Ethernet 1	<input type="radio"/>
Ethernet 2	<input type="radio"/>
Ethernet 3	<input type="radio"/>

OK

## Process

The [Status] → [Monitoring] → [Process] submenu is used to display the CPU utilization %, memory usage, and start time of the processes running on the WIM.

### Process

PID	%CPU	%MEM	RSS	STAT	START	COMMAND
1	0.0	0.1	556	S	12:19	init
2	0.0	0.0	0	SW	12:19	keventd
3	0.0	0.0	0	SWN	12:19	ksoftirqd_CPU0
4	0.0	0.0	0	SW	12:19	kswapd
5	0.0	0.0	0	SW	12:19	bdflush
6	0.0	0.0	0	SW	12:19	kupdated
8	0.0	0.0	0	SW	12:19	swapper
9	0.0	0.0	0	SW	12:19	mtdblockd
7	0.0	0.0	0	SW	12:19	kdpram
19	0.0	0.0	0	SWN	12:19	jffs2_gcd_mtd4
21	0.0	0.0	0	SWN	12:19	jffs2_gcd_mtd5
69	0.0	0.0	0	SW	12:19	cavium
81	0.0	0.4	2196	S	12:19	nsm
87	0.0	0.4	2344	S	12:19	imi
105	0.0	0.3	1808	S	12:19	ripd
121	0.0	0.3	1908	S	12:19	ospfd
133	0.0	0.4	2112	S	12:19	bgpd

## Services

This submenu is used to display the status of the Security, Router, and Management services provided by the WIM in a table format. If a service is set to 'Auto Start' then the service is started automatically when the system reboots. If the 'Activity' field shows that a service is 'Running', then the service's function is being performed. If the 'Activity' field of the service shows 'Stop', then the service is not functioning.

### Security

This window is used to display the current status of the Security services being provided by the WIM.

### Security

Name	Activity
NAT (Network Address Translation)	Running
<b>Firewall</b>	Running
PPTP (Point-to-Point Tunneling Protocol)	Stop
IDS (Intrusion Detection System)	Stop
L2TP (Layer 2 Tunneling Protocol)	Stop
IPSEC (IP Security)	Stop

### Router

This window is used to display the current status of the Router services being provided by the WIM.

### Router

Name	Activity
RIP (Routing Information Protocol)	Running
OSPF (Open Shortest Path First)	Running
DVMRP (Distance Vector Multicast Routing Protocol)	Stop
<b>PIM-SM</b> (Protocol Independent Multicast - Sparse Mode)	Stop



## Application

This window is used to display the current status of the Application services being provided by the WIM.

### Application

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

## Management

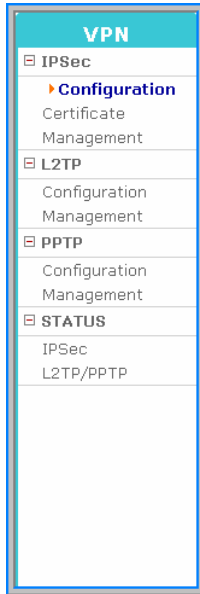
This window is used to display the current status of the Management services being provided by the WIM.

### Management

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

# VPN Menu

A VPN is an encrypted tunnel which is used to allow remote users and other private networks to connect to other networks using secure methods. VPNs are widely utilized by enterprises to create wide area networks (WANs) that span large geographic areas, to offer site-to-site connections to branch offices, and to allow mobile users to dial into their company LANs. Select the [VPN] menu to begin configuring the VPNs feature. The VPN submenus will be displayed in the upper left side of the window as follows:



## VPN Menu Description

Menu	Submenu	Description
IPSec	Configuration	Used to set up IPsec.
	Certificate	Used to generate or delete an IPsec certificate
	Management	Used to Start or Stop the IPsec feature, to generate an RSA Key, and to assign the WAN Interface for the IPsec Tunnel.
L2TP	Configuration	Used to set up L2TP.
	Management	Used to Start or Stop the L2TP feature and to set the IP Address range for clients when they connect to the WIM with L2TP
PPTP	Configuration	Used to set up PPTP.
	Management	Used to Start or Stop the PPTP feature and to set the IP Address range for client s when they connect to the WIM with PPTP
STATUS	IPSec	Used to display the status of the IPsec tunnel
	L2TP/PPTP	Used to display the status of the L2TP and PPTP connections



#### **Setting up VPN Client in Windows XP/2000**

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



#### **VPN Tunnels**

The OfficeServ 7200 WIM Data Server can support up to 100 Tunnels.

## **IPSec**

The IP Security Protocol (IPSec) provides security services in the IP layer through implementing an Internet Key Exchange (IKE). The IPSec security service is categorized into two services depending the remote equipment. The security tunnel can be between a local subnet and a remote subnet or between a local subnet and a remote host.

Even if IPSec can be set up to provide a security tunnel between a local host and a remote host the WIM board is used as a gateway not as a host. Thus, this service is not supported. Since the IPSec setting requires two gateways for a security tunnel the local configuration and remote configurations have the same items.



#### **IPSec Tunnel Mode**

The OfficeServ 7200 Data Server only supports the IPSec Tunnel mode. The transport mode is not supported. In addition, if the WAN interface is SERIAL then IPSec is not supported. Since a SERIAL line is a dedicated line IPSec is not required for the security.



#### **VPN Programming**

The OfficeServ 7200 WIM Data Server comes with a built-on VPN Accelerator daughterboard for VPN functionality.

## Config

Use the [VPN] → [IPSec] → [Configuration] submenu to begin configuring IPSec.

### IPSec Connection

Select	Connection ID	Local IP	Remote IP
--------	---------------	----------	-----------

### IPSec Connection Button Description

Item	Description
<b>Add</b>	Used to create an IPSec tunnel
<b>Delete</b>	Used to delete an IPSec tunnel
<b>Edit</b>	Used to modify the IPSec tunnel data

### Add

Click the Add button from the <IPSec Connection> window to display the window shown below. Enter the value of each item and then click the OK button to save the IPSec tunnel configuration.

### Connection Add

Category	Local Settings	Remote Settings
Connection ID	<input type="text"/>	
IP	<input type="text" value="10.0.1.1"/>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Router IP	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	
Subnet IP	<input type="text" value="NOT"/>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Subnet Mask	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>

### Authentication Method

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

## IPSec Connection Parameter Description

Parameter	Description
Connection ID	Used to enter the Tunnel ID which is composed of letters and numbers (Required). First character must be a letter
IP	External IP address (Required)
Router IP	Router IP address (typically the gateway for WAN Interface)
Subnet IP	Internal IP address range
Subnet Mask	Internal subnet mask
RSA Key/ Preshared Key /Certificate	<p>Selects the host authentication method</p> <ul style="list-style-type: none"> <li>- <b>RSA Key:</b> The Public RSA key is already defined.. Click the Browse button to find the Remote Key and then click on the Upload button to store the RSA key into the WIM</li> <li>- <b>Preshared Key:</b> Used to enter an authentication password.</li> <li>- <b>Certificate:</b> Used to define the local authentication certificate and the CA certificate. For Local settings select a certificate from the certificate list.(If selecting a certificate from the Local ID of Advanced is entered automatically) For Remote settings, enter the Remote ID. It is available to check the integrity of the host certificate registered to Local.</li> </ul>



NOTE

### Router Value Configuration

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

## Advance

Click the IPsec Advanced button from the <IPsec Add> or <IPsec Mod> window to display the following window.

## Advance

<input checked="" type="checkbox"/>	
Phase 1	
Key Life Time	<input type="text" value="3600"/> sec
Phase 2	
Protocol	<input type="text" value="esp"/>
Key Life Time	<input type="text" value="28800"/> sec
Dead Peer Detect	
Time Out	<input type="text" value="120"/> sec
Delay	<input type="text" value="30"/> sec
Action	<input type="text" value="hold"/>
Advance	
Negotiation Count	<input type="text" value="0"/>
Perfect Forward Secrecy	<input type="text" value="yes"/>
Rekey	<input type="text" value="yes"/>
Connection	<input type="text" value="Initiator"/>

## IPSec Advanced Parameter Description

Parameter		Description
Phase 1	Key life time	Used to set the IKE Duration If Key life time expires then the host authentication (the phase one IKE) is performed again.
	Protocol	Used to select the packet authentication protocol - Authentication Header (AH): Allows the authentication of data transmitter - Encapsulating Security Payload (ESP): Allows the authentication and data encryption
Phase 2	Key life time	The cycle of newly added key used for packet encryption by the repeated phase two IKE negotiation
	PFS	Used to select the session key transfer/security
Advance	Re-Key	Used to set whether to add a new key (whether to add a new key and negotiate again in the phase 1, 2 IKE).
	Negotiation count	Reattempt count of key exchange when key exchange is failed on the phase 1 IKE

Parameter		Description
	Connection	IPSec Connection Attempt - initiator: Attempting a connection - response: Attempt to receive a connection
DPD	Time out	Used to set the effective time when the counter party receives a DPD packet and receive packet
	Delay	Used to set the alive check time of the counter party
	Action	Used to set the action after the Dead Peer Detect - hold: Waiting for connection - clear: No more connection

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

### IPSec Tunnel Programming Example



In the example listed below the following information is applied to an IPSec Tunnel. The Connection ID is set to ToRemote1, the WAN Interface being used for the tunnel is 10.0.1.1, the Router IP is the Gateway for 10.0.1.1 is 10.0.1.254, the Local Subnet is 192.168.1.0 and the local subnet is 255.255.255.0. The remote end of the tunnel is 10.0.2.1, the local subnet is 192.168.2.0, and the remote Subnet Mask is 255.255.0. This tunnel uses a Preshared key.

### Connection Add

Category	Local Settings	Remote Settings
Connection ID	ToRemote1	
IP	10.0.1.1	10 . 0 . 2 . 1
Router IP	10 . 0 . 1 . 254	
Subnet IP	192.168.1.0	192 . 168 . 2 . 0
Subnet Mask	255 . 255 . 255 . 0	255 . 255 . 255 . 0

### Authentication Method

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

## Certificate

The [VPN]→ [IPSec] → [Certificate] submenu is used by the administrator to verify Issue/Delete/Download a CA Certificate and Host certificate. In addition the addition/delete of an external certificate, and the current certificate list is performed here.

### CA Certificate List

Select	Subject	Cert file
--------	---------	-----------

Add

### External CA Certificate List

Category	ID
----------	----

Upload

Delete

### Certificate Parameter Description

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

### CA Certificate List

#### CA Certificate

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

OK

Cancel



## CA Certificate List Parameter Description

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



NOTE

### CA Certificate deletion

When a CA Certificate must be deleted the administrator must successfully enter the CA Certificate password. So keep track of any CA Certificates that are created.

## External Certificate

### External CA Certificate

Upload	
CA Certificate	<input type="text"/> <input type="button" value="Browse..."/>

## Host Certificate

Distinguish Name	
Common	<input type="text"/>
Email	<input type="text"/>
Password	<input type="text"/>
Confirm Password	<input type="text"/>

## External CA Certificate Parameter Description

Item	Description
CA Certificate	External certificate upload

## Host Certificate

### Host Certificate Parameter Description

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

## Management

The [VPN] → [IPSec] → [Management] submenu is used by the administrator to start and stop the IPSec service.. When the WIM is rebooted the IPSec service will be returned to the state it was in before the reboot was performed. RSA keys may be generated or downloaded from this window and the External Interface is also selected here.

### IPSec Management

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

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

External Device	Action
<input checked="" type="checkbox"/> eth0	<input type="button" value="OK"/>

In the RSA window click the OK button for the [Create the new RSA key] item to add a new RSA (public key password method) key. Use this submenu to add a new RSA key if the host authentication method of RSA key used.

After setting an External Device in the External Device window click the OK button to save the configuration.

## L2TP

### Configuration

The system administrator can begin setting up the L2TP security between a local subnet and a remote host by using the [VPN] → [L2TP] → [Configuration] submenu. The administrator can create, modify, delete, or retrieve the VPN tunnel data from here.

### User List

Category	ID	IP Allocation
----------	----	---------------

### L2TP User List Field Description

Field	Description
Add	Create a PPTP administrator
Delete	Delete a PPTP administrator

Field	Description
Edit	Modify a PPTP administrator information

## Add

Click the Add button on the <**L2TP administrator list**> window to add a L2TP Tunnel ID and password., Enter each parameter and then click the OK button to save the changes..

## User Add

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

## L2TP User Add Parameter Description

Parameter	Description
<b>ID</b>	Used to enter the L2TP Tunnel ID composed of letters and numbers
<b>Password</b>	Shared tunnel password
<b>Confirm Password</b>	Re-enter shared tunnel password
<b>Auto IP Allocation</b>	Used to assign dynamic IP to remote client
<b>Static IP Allocation</b>	Used to assign static IP to remote client (Enter IP address)

## Edit

If a L2TP Tunnel parameter needs to be modified highlight the radio button to the left of the User List needing to be changed and then click the Edit button. Modify each parameter value and then click the OK button to save the VPN tunnel data changes.

## User Mod

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

## Management

Using the [VPN] → [L2TP] → [Management] submenu, the system administrator can start or stop the L2TP services. When the system is rebooted the L2TP service will be automatically initiated if the L2TP service is running.

## L2TP Management

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

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

The administrator can also set up the IP range for the remote L2TP clients that use the dynamic IP feature. The encryption method supports 'pap' and 'chap'.



### Setting up IP Range

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

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

# PPTP

## Configuration

The system administrator can begin setting up the PPTP security between a local subnet and a remote host by using the [VPN] → [PPTP] → [Configuration] submenu. The administrator can create, modify, delete, or retrieve the VPN tunnel data from here.

### User List

Category	ID	IP Allocation
----------	----	---------------

### PPTP User List Parameter Description

Parameter	Description
Add	Used to create a PPTP administrator
Delete	Used to delete a PPTP administrator
Edit	Used to modify PPTP administrator information

### Add

Click the Add button on the <PPTP administrator list> window to add a PPTP Tunnel ID and password., Enter each parameter and then click the OK button to save the changes.

### User Add

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

### PPTP User Add Parameter Description

Parameter	Description
ID	Used to enter the ID composed of letters and numbers
Password	Used to enter the shared password
Confirm Password	Used to re-enter shared password

Parameter	Description
Dynamic IP	Used to assign dynamic IP for remote clients
Static IP	Used to assign static IP for remote clients (Enter IP address)

### Edit

If a PPTP Tunnel parameter needs to be modified highlight the radio button to the left of the User List needing to be changed and then click the Edit button. Modify each parameter value and then click the OK button to save the VPN tunnel data changes.

### User Mod

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

## Management

Using the [VPN] → [PPTP] → [Management] submenu, the system administrator can start or stop the PPTP services. When the system is rebooted the PPTP service will be automatically initiated if the PPTP service is running.

### PPTP Management

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

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

The administrator can also set up the IP range for the remote PPTP clients that use the dynamic IP feature.



**Setting up IP Range**

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

## Status

In order to check the status of an IPSec tunnel go to the [VPN] → [STATUS] → [IPsec] submenu. All IPSec Tunnels and their status will be displayed.

### Status

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

### Log

ID	Contents

Refresh

In order to check the status of L2TP or PPTP tunnels go to the [VPN] → [STATUS] → [L2TP/PPTP] submenu. All L2TP and PPTP Tunnels and their status will be displayed.

### PPTP/L2TP Status

Device Name	Local IP	Remote IP
PPP0	192.168.0.234	192.168.1.234

Refresh

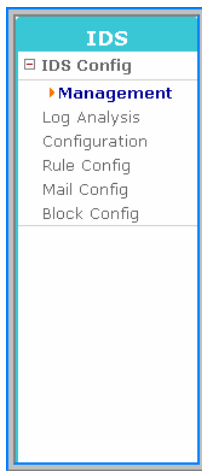


# IDS Menu

An intrusion detection system (**IDS**) generally detects unwanted attacks to computer systems mainly through The Internet. The attacks may come from skilled malicious hackers, or by others using automated tools.

The WIM intrusion detection system is used to detect all types of malicious network traffic and computer usage that can not be detected by a conventional firewall. This includes network attacks against vulnerable services, data driven attacks on applications, unauthorized logins and access to sensitive files, and malware (viruses, trojan horses, and worms).

Select the **[IDS]** menu to begin configuring the IDS feature. The IDS submenus will be displayed in the upper left side of the window as follows:



## IDS Menu Description

Menu	Submenu	Description
IDS Config	Management	Used to start or stop the IDS module and block module.
	Log Analysis	Used to classify how the IDS logs will be searched
	Configuration	Used to set up the rule and detection level of the IDS.
	Rule Config	Used to update the IDS rule files.
	Mail Config	Used to register the email server and email address of the system manager.
	Block Config	Used to register the Trusted IP Address of the system Manager

# IDS Config

## Management

Using the [IDS] → [IDS Config] → [Management] submenu the system administrator can start or stop the IDS module.

### IDS Management

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

### Block Management

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

### IDS Management Field/Parameter Description

Field/Parameter	Description
<b>Status</b>	- Running: The IDS module is operational - Stop: The IDS module is not in operation
<b>Action</b>	Click the <b>Run</b> button to start the IDS module. Click the <b>[Stop]</b> button to stop the IDS module
<b>Block time</b>	When an intrusion is detected this timer determines how long the IP address is blocked from the system. The max block time is 999999999 seconds

## Log Analysis

Using the [IDS] → [IDS Config] → [Log Analysis] submenu the system administrator can view alerts detected by the IDS module. In this window select the desired IDS category and then click the OK button. The IDS search can be narrowed down and pin pointed by defining the Search Log Parameters. IDS Logs can be filtered by Priority, Source IP, Destination IP, and Destination port.

### Log Analysis

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

OK

### Log Analysis Parameter Description

Parameter	Item	Description
Category	Intrusion type	Used to set the WIM to show IDS log by intrusion type
	Source IP	Used to set the WIM to show IDS log by intrusion type
	Destination IP	Used to set the WIM to show IDS log by Destination IP
	Destination Port	Used to set the WIM to show IDS log by Destination Port
	Port Scan	Used to set the WIM to show IDS log if information is the port scan type

### Search Log

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

OK

## Search Log Parameter Description

Parameter	Item	Description
Category	Priority	Used to filter the IDS log by Priority of the Intrusion. Choices are all, high, med, or low
	Source IP	Used to filter the IDS log by Source IP Address
	Destination IP	Used to filter the IDS log by Destination IP Address
	Destination Port	Used to filter the IDS log by Destination IP Port

## Intrusion Type Log

The administrator can summarize the IDS alerts by type. If the alert log is defined by Intrusion Type the following window will appear:

### Summary by intrusion type

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

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



## Intrusion Type Field Description

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

If the Sid number is clicked then more information on the alert will be displayed.

## Sid : 384

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

 Prev.

## Source IP Log

The administrator can summarize the IDS alerts by the Source IP. If the alert log is defined by Source IP the following window will appear:

## Summary by source IP

Mon Sep 26 04:16:59 2005 ~ Mon Sep 26 21:17:42 2005

Num	Source IP	Priority	Description
6	192.168.0.210	med	ICMP PING
6	192.168.0.210	med	ICMP PING *NIX
6	192.168.0.210	med	ICMP PING BSDtype
4	192.168.0.1	med	ICMP Echo Reply
2	192.168.0.117	med	WEB-MISC SSLv3 invalid Client_Hello attempt
2	192.168.0.119	med	WEB-MISC SSLv3 invalid Client_Hello attempt

 Prev.

## Source IP Field Description

Field	Description
<b>Num</b>	Number of logs detected by IDS according to the host (source) IP that attacks the logs
<b>Source IP</b>	Host IP that performed the attack
<b>Priority</b>	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)
<b>Description</b>	Type of log detected in IDS

## Destination IP Log

The administrator can summarize the IDS alerts by the Destination IP. If the alert log is defined by Destination IP the following window will appear.

### Summary by destination IP

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

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

 Prev.

### Destination IP Field Description

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

## Destination Port

The administrator can summarize the IDS alerts by the Destination Port. If the alert log is defined by Destination Port the following window will appear.

### Summary by destination port

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

Num	Port	Priority	Description
There is no entry			

 Prev.

## Destination Port Field Description

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

## Port Scan

The administrator can summarize the IDS alerts by the Port Scan. If the alert log is defined by Port Scan the following window will appear.

### Port scan summary

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

Ports	Hosts	Remote hosts
There is no alert		



## Port Scan Field Description

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

## Search

The IDS search can be narrowed down and pin pointed by the administrator by defining the Search Log Parameters. IDS Logs can be filtered by Priority, Source IP, Destination IP, and Destination port.

## Search Log

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

OK

Once the Search Log Category is selected the administrator can select the desired condition. Set the condition and then click the OK button to display the desired information in the window as follows:

## Result of Search

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

← Prev.



CHECK

### Selecting Search Condition

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



## Configuration

Using the [IDS] → [IDS Config] → [Configuration] submenu the system administrator can configure the Interface/s which will use IDS, set the Detection Level and Type for IDS, and choose which IDS rules to use.

### Select Device

The Select Device window is used by the administrator to set up a network for IDS monitoring. The interfaces which are set up as WAN can be selected here. The administrator simply selects the check box of the Interface needing to be monitored and it is activated.

### Select Device

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

### Set Detection Level & Type

The intrusion types are classified as High, Medium and Low according to the risk level. The administrator can set up the intrusion detection levels so an alert will be generated when an intrusion exceeding the level occurs. In addition, the administrator can set up the associated operations for each intrusion level.

For example if the Block box is checked for High then the relevant IP Address is blocked from accessing the system for a configured time. If the Mail box is checked then alerts are sent to the system administrator via email.

### Set Detection Level & Type

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

## IDS Rule Configuration

This window is used by the administrator to select the IDS rule sets to be used by the system.

### IDS Rule Configuration

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

Click the box of each rule set that needs to be functioning and then click on the OK button to activate the selected rule sets.

Click the Default button to select the default rules.

## Rule Config

Using the [IDS] → [IDS Config] → [Rule Config] submenu the system administrator can set the IDS rules to be update automatically or they can manually update the IDS rules. The version of the current rule-set file and the released date is displayed as well.

### Set Time for Update Rules

Category	Configuration	Set
Now	Update Now	<input type="button" value="OK"/>
<input type="text" value="Not use"/>	Not use reservation	<input type="button" value="OK"/>

### Current Rules' Information

Rules' Information	
Current version	v 1.144.2.8.1
Release Date	2006/10/19 16:28:12

### Update the Rule-set

Upload Rule-set File	
Upload File	<input type="text"/> <input type="button" value="Browse..."/>

### Rule Config Parameter/Field Description

Field/Parameter	Description
<b>Category</b>	<b>Now:</b> Updates the IDS Rule Now
	<b>Pull Down Menu:</b> Can select Not use, One Time, Daily, Weekly, or Monthly
<b>Configuration</b>	Will change depending on the Category
<b>Set</b>	OK button used to implement the Category operation
<b>Current version</b>	Shows current IDS File Set version
<b>Release Date</b>	Shows current Release Date of IDS File Set
<b>Update File</b>	Used to Manually browse to an IDS rule set file to update the system.

## Mail Config

Using the [IDS] → [IDS Config] → [Mail Config] submenu the system administrator can set up the SMTP attributes.

### Set Time for Sending Mail

The administrator uses this window to set up when the WIM will send an email to the defined SMTP server

### Set Time for Sending Mail

Category	Configuration	Set
Now	Send Mail Now	<input type="button" value="OK"/>
One Time <input type="button" value="v"/>	Day : <input type="button" value="1"/> <input type="button" value="v"/> Hour : <input type="button" value="1"/> <input type="button" value="v"/>	<input type="button" value="OK"/>

One Time

Daily

Weekly

Monthly

Not use

Either click the OK button to the right of the Now category to send an email immediately or use the pull down menu to select when the email should be sent. The choices are One Time, Daily, Weekly, Monthly, or Not use. Define the configuration of the send category and then click the OK button to save the changes.

### Set SMTP Server IP

The administrator enters the IP Address of the SMTP server, enters the subject and Source Mail Address, and can enter up to 10 email addresses to receive email notifications here. Click the OK button to save the changes.

### Set SMTP Server IP

Server's IP	Port
<input type="text" value="."/> <input type="text" value="."/> <input type="text" value="."/> <input type="text" value="."/>	<input type="text" value="25"/>

Set Mail Information	
Subject	<input type="text"/>
Source Mail Address	<input type="text"/>

Set Destination Mail Address
<input type="text"/>



### SMTP Server IP Configuration

If there is not a recorded alert in the IDS alert log then an email was not sent.

## Block Config

Using the [IDS] → [IDS Config] → [Block Config] submenu the system administrator can view the IP Block List applied to the block module or enter a trusted IP.

### Manage Blocked IP List

Blocked IP List

### Manage Trusted IP List

Trusted IP List				Netmask			
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="255"/>	<input type="text" value="255"/>	<input type="text" value="255"/>	<input type="text"/>

OK

Delete

### Manage Blocked IP List

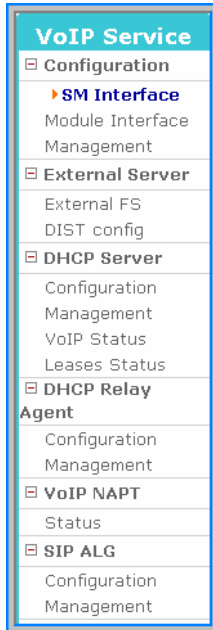
If an IP Address, is flagged as an intruder and it is blocked from accessing the system, then the IP Address will be shown in the Manage Blocked IP List.

### Manage Trusted IP List

The administrator can register a trusted IP Address here. Simply enter the IP and netmask and click the OK button to register. Check the IP list that is already registered and click the Delete button to delete the list.

# VoIP Service Menu

The [VoIP Service] Menu of the WIM Data Server is used for setting up the Auto-QoS, DHCP, and SIP-ALG. Once the [VoIP Service] Menu is selected the submenus will be displayed on the left top of the window as follows:



## VoIP Service Menu Description

Menu	Submenu	Description
Configuration	SM Interface (future Release)	Used to enable or disable items related to the Message Data transmission for the communication with the system manager (SM).
	Module Interface	Used to set the environment for the communication with Call Server and Feature Server. *Although the Select VoIP WAN Interface field seems to be set the system administrator <b>must</b> select the correct WAN Interface and then click the save button in order for VoIP Service to work.
	Management	Start or stop the programs for the communication with SM Interface, Call Server, and Feature Server. Set the OS 7200 WIM Data Server to automatically restart these programs when the WIM is rebooted.

Menu	Submenu	Description
External Server	External FS (future release)	Used to set or delete the IP of the Feature Server existing on the external network (A public network when the NAT is used).
	DIST Config (future release)	Transmits the message received via the externally designated port into the terminal designated at the internal network.
DHCP Server	Configuration	Used to set the internal network that operates the DHCP Server. In addition, used to set the IP pool for the DHCP terminals, the IP pool for Call Server, the Feature Server, MGI information, IP Phones, SIP Phones, and general data terminals can be set, respectively.
	Management	Used to start or stop the DHCP Server. There is also a check box which needs to be checked in order to start the DHCP server in the event of a system reboot.
	VoIP Status	Used to display the IP terminal information of the OfficeServ 7200 system received from Call Server or Feature Server when the program for the communication with Call Server or Feature Server is running.
	Leases Status	Used to display the IP Address lease information for the DHCP clients.
DHCP Relay Agent	Configuration	Used to set the Interface and DHCP Server to be relayed, connected for connecting mutually when DHCP Server and the client are in the mutually different network.
	Management	Used to start or stop the DHCP Relay Agent.
VoIP NAPT	Status	Used to display the information on the Static NAPT for the OfficeServ 7200 VoIP service. This information is automatically set when the program for the communication with Call Server and Feature Server is executed. The information is displayed when the setup is completed.
SIP ALG	Configuration	Used to set the SIP environment.
	Management	Used to start or stop the SIP ALG. Also sets so that the execution is made when rebooting the system.

## VoIP Service Configuration

The [VoIP Service] → [Configuration] submenu is used to set all the environmental parameters of the Data Server Module Interface (DSMI).

### SM Interface

Not available until future release



NOTE

#### SM Interface

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

### Module Interface

Using the [VoIP Service] → [Configuration] → [Module Interface] submenu the system administrator sets the VoIP WAN Interface. Other environmental settings used for communication between the WIM Data Server and the Call Server are set here as well.

### DataServer Module Interface Configuration

Call, Feature Module Configuration	
Data send to UDP port number	5025 port
Retry timeout	<input type="text" value="3"/> sec
Max retry timeout count	<input type="text" value="5"/>
Hello Interval initial	<input type="text" value="3"/> sec
Hello Interval online	<input type="text" value="10"/> sec
Select VoIP WAN Interface	<input type="text" value="eth0"/> ▼

Save



NOTE

#### Select VoIP WAN Interface Field

Although this field appears to be set automatically the system administrator must use the pull down menu to select the correct WAN interface. Once the WAN interface is selected click on the Save button.



## Module Interface Parameter Description

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

## Management

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

### DataServer Module Interface

#### Management

Module Name	Activity	Running/Stopped
SM Module	Stopped	<input type="button" value="Run"/>
Call, Feature Module	Stopped	<input type="button" value="Run"/>

<input type="checkbox"/> SM module auto-start when system boots	<input type="button" value="OK"/>
<input type="checkbox"/> Call, Feature module auto-start when system boots	<input type="button" value="OK"/>



NOTE

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

## External Server

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

## External FS

Not available until future release



### Feature Server in the internal network

The Feature Server feature will become available in a future release of the OS 7200 Data Server

## DIST Config

Not available until future release

## DHCP Server

The [VoIP Service] → [DHCP Server] submenu is used to configure the DHCP Scope, to start and stop the DHCP Server, to view the VoIP Status, and to view the DHCP Lease status.

## Configuration

Using the [VoIP Service] → [DHCP Server] → [Configuration] submenu the system administrator must first select the Internal Network that is to receive DHCP addresses from the WIM Data Server. Select the radio button of the correct LAN Interface and then click on the Next button.

### DHCP Server Interface Selection

Internal Network	TYPE	Selection
eth1	INT_PRIV	<input type="radio"/>
eth2	INT_PRIV	<input type="radio"/>
eth3	INT_PRIV	<input type="radio"/>

Next

The <DHCP Server Configuration> screen will then display the basic information on the device selected on the <DHCP Server Interface Selection> screen.

In addition the administrator can program the IP Addresses of the OfficeServ 7200 Call Server, IP phones, SIP phones, and data terminals, These devices must be on the same subnet which is defined in the DHCP scope.

## DHCP Server Configuration

This field displays the general information for allocating DHCP to clients.

### DHCP Server Configuration

Interface	Sub Network	Broadcast	Router	Default Lease Time
eth2	192.168.2.0	192.168.2.255	192.168.2.1	0

### DHCP Server Field and Parameter Description

Field/Parameter	Description
<b>Sub Network</b>	Subnetwork information. This value is set in the <b>[Network]</b> Menu. It shows the Sub Network based on the IP Address of the Ethernet Interface
<b>Broadcast Address</b>	Broadcast address. This value is set in the <b>[Network]</b> Menu. It shows the Broadcast Address based on the IP Address of the Ethernet Interface
<b>Router Address</b>	Router address. This value is set in the <b>[Network]</b> Menu. It shows the Router Address based on the IP Address of the Ethernet Interface
<b>Default Lease Time</b>	Basic release allocation time of the IP address. The IP Address release time for the overall IPs that are to be provided via DHCP Server can be set in increments of seconds. An entry of "0" equals an infinite lease and the default lease time is 30 days.

## CALL Server

This field is used to set the Call Server's IP Address. This is the IP Address of the MCP of the OS 7200 system. When authenticated as host, the 'Host ID' is designated as 'SME\_MCP' as its default value.

Server	IP	Gateway	Netmask	MAC/Host ID
CALL	192.168.1.200	192.168.1.1	255.255.255.0	HOST SME_MCP

### Call Server Parameter Description

Item	Description
<b>IP</b>	Call Server's IP address
<b>Gateway</b>	Gateway Information
<b>Netmask</b>	Netmask information

Item	Description
<b>MAC/Host ID</b>	Types of the client authentication - NONE: Execute the DHCP IP request without the authentication - MAC: Authenticates with MAC. - HOST: Authenticates with HOST ID(Default value: SME_MCP)

### Feature Server

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

### MGI Cards

This window sets the IP Addresses of the MGI card/s mounted in the system.

First check at the 'Slot Select' check box. Second check at the checkbox on the left side of each item. Then enter the IP Address, External IP Port, Gateway, and Sub Netmask of the MGI card/s.

Cards	IP	Start Port	Gateway	Netmask
<input checked="" type="checkbox"/> Slots Select				
1-1 <input type="checkbox"/>				
1-2 <input type="checkbox"/>				
1-3 <input type="checkbox"/>				
1-4 <input checked="" type="checkbox"/>	192.168.1.201	25000	192.168.2.1	255.255.255.0
1-5 <input type="checkbox"/>				
2-1 <input type="checkbox"/>				
2-2 <input type="checkbox"/>				
2-3 <input type="checkbox"/>				
2-4 <input type="checkbox"/>				
2-5 <input type="checkbox"/>				

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

## IP Phone

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

select	IP Phone IP Range	Gateway	Netmask	MAC/Host ID
<input type="checkbox"/>	192.168.1.50 ~ 75	192.168.1.1	255.255.255.255	NONE List
		Add	Delete	

## IP Phone Parameter Description

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

## SIP Phone

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

	SIP Phone IP Range	Gateway	Netmask	MAC/Host ID
POOL	192.168.80 ~ 90	192.168.1.1	255.255.255.0	NONE List

## SIP Phone Parameter Description

Parameter	Description
<b>IP Range</b>	The IP range of the SIP phone (Maximum range:120 terminals). When entering one IP, enter '192.168.0.40~40'.
<b>Gateway</b>	The gateway information entered at the CALL Server Item.
<b>Netmask</b>	The netmask information entered at the CALL Server Item.
<b>MAC/Host-ID</b>	The client authentication type <ul style="list-style-type: none"> <li>- NONE: Executes the DHCP IP request without the authentication.</li> <li>- MAC: Click the <b>[List]</b> Button, and enter the MAC address of the SIOIP phone for the authentication.</li> <li>- HOST: Click the <b>[List]</b> button and enter the HOST ID because the internally specialized HOST ID is not used.</li> </ul>

## Terminal

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

select	Data Terminal IP Range	Gateway	Netmask	MAC/Host ID
<input type="checkbox"/>	192.168.1.150 ~ 200	192.168.1.1	255.255.255.0	NONE List

## Terminal Parameter Description

Parameter	Description
<b>IP Range</b>	The IP range of the Data terminals (Maximum range: 120 terminals) When entering one IP, enter '192.168.0.60~60'.
<b>Gateway</b>	The gateway information entered at the CALL Server Item.
<b>Netmask</b>	The netmask information entered at the CALL Server tem.

Parameter	Description
MAC/Host-ID	The client authentication type - NONE: Executes the DHCP IP request without the authentication. - HOST: Click the <b>[List]</b> Button, and enter the HOST ID. - MAC: Click the <b>[List]</b> Button, and enter the MAC address.

## Management

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

### DHCP Server Management

Internal Network	Current States	Running/Stopped
eth2	Running	<input type="button" value="Stop"/>
<input checked="" type="checkbox"/> DHCP server auto-start when system boot		<input type="button" value="OK"/>



## VoIP Status

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

DHCP Server Current States
RUNNING

Server	Status	IP	MAC Address
CALL	Connected	192.168.2.100	00:00:f0:e8:00:57
FEATURE			

MGI Slots	Status	IP	MAC Address
1			
2			
3			
4	Connected	192.168.2.101	00:00:f0:01:02:03
5			
6			
7			
8			
9			
10			

## Leases Status

The system administrator can view the DHCP lease status on all DHCP IP devices using the [VoIP Service] → [DHCP Server] → [Leases Status] submenu. Select the LAN that is using the DHCP server and then click the Next button.

### DHCP Lease Status

Internal Network	TYPE	Selection
eth2	INT_PRIV	<input checked="" type="checkbox"/>

Next 

Once the Next button has been clicked the Lease Status window will open.

### DHCP Active Lease Status

IP Address	Lease Start	Lease End	MAC Address
192.168.2.200	01/02/2007 23:56:50	02/02/2007 11:56:50	00:0b:cd:98:d2:ad

## DHCP Relay Agent

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

### Configuration

The DHCP Relay Agent is configured by designating the interface to perform the relay and registering from the DHCP Server. Designate the Interface where the relay is performed among the activated interface list by using the Add button. For the designated interface, its list is made, the set interface can be deleted in the list by using the Delete button.

In the DHCP Server list enter the IP Address of the DHCP and click the Add button.. To delete a DHCP Server, check the box to the left of the IP Address, and then press the Delete button.

### Interface List Configuration

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

Add Delete

Check	Server List	Server
<input type="checkbox"/>	Server List	<input type="text" value="."/> <input type="text" value="."/> <input type="text" value="."/> <input type="text" value="."/>

Add Delete

## Management

Using the [VoIP Service] → [DHCP Relay Agent] → [Management] submenu the administrator can start or stop the DHCP Relay Agent Service. Click on the Run button to start the DHCP Relay Agent and click on the Stop button to stop the DHCP Relay Agent.

### DHCP Relay Agent Management

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

## VoIP NAPT

Using the [VoIP Service] → [VoIP NAPT] → [Status] submenu the system administrator can display the NAPT items for VoIP Service.

### Status

The service connects 32 internal ports and external ports to each MGI card through one to one mapping. There are also multiple IP ports forwarded to the MCP card. The following table shows a basic VoIP NAPT list with (1) MGI 16 and an MCP card.

#### NAPT List for VoIP

Index	Public IP	Protocol	StartPort	EndPort	Internal IP	StartPort
1	216.62.86.142	udp	1719	1719	192.168.2.100	1719
2	216.62.86.142	tcp	1720	1720	192.168.2.100	1720
3	216.62.86.142	tcp	5000	5000	192.168.2.100	5000
4	216.62.86.142	udp	5003	5003	192.168.2.100	5003
5	216.62.86.142	tcp	5003	5003	192.168.2.100	5003
6	216.62.86.142	tcp	5060	5060	192.168.2.100	5060
7	216.62.86.142	udp	5060	5060	192.168.2.100	5060
8	216.62.86.142	tcp	6000	6000	192.168.2.100	6000
9	216.62.86.142	udp	6000	6000	192.168.2.100	6000
10	216.62.86.142	tcp	6100	6100	192.168.2.100	6100
11	216.62.86.142	udp	9000	9000	192.168.2.100	9000
12	216.62.86.142	udp	25000	25031	192.168.2.101	30000



NOTE

#### NAPT Ports

Please refer to the OS 7200 Special Applications Manual for a listing and description of all IP Ports that the OS 7200 uses.

## NAPT List for VoIP Field Description

Field	Description
<b>Public IP</b>	This field displays the external IP Address which communicates with the external environment
<b>Public Start Port</b>	This field displays the port number for the external source IP to communicate with external media
<b>Public End Port</b>	This field displays the last external source port number.
<b>Internal IP</b>	This field displays the Internal IP Address that VoIP Service uses inside the WIM firewall
<b>Internal Start Port</b>	This field displays the IP port number for the internal IP Address that VoIP Service uses
<b>Internal End Port</b>	This field displays the last IP port number for the Internal IP Address that VoIP Service uses.



NOTE

### **VoIP Service and SIP ALG**

VoIP Service and SIP-ALG cannot run at the same time

# SIP ALG

## Config

Using the [VoIP Service] → [SIP-ALG] → [Configuration] submenu, the SIP environment can be set up by the system administrator. Set the following items, and then click the Save button.

### SIP Configuration

SIP IP Configuration	
External IP	192.168.22.21
Internal IP	10.0.0.1
Dynamic Learning	<input type="radio"/> on <input checked="" type="radio"/> off

The information on the firewall setup is displayed.

The External IP item and the Internal IP item are displayed on the list box so that the web manager can combine the usable information to select it.

If there are two external or internal networks or more, the network that is to be used in the list box can be selected.

SIP IP Configuration	
External IP	192.168.22.21
Internal IP	192.168.22.21 100.0.0.10
Dynamic Learning	<input type="radio"/> on <input checked="" type="radio"/> off

If the Dynamic Learning function is set to 'On', then the Map information of a SIP phone transmitting the REGISTER message to an external SIP proxy server is learned automatically.

## Map LIST

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

MAP						
	ID	IP				
<input type="checkbox"/>	default	10	0	0	10	5060

When there is no information on the IP or the phone on the SIP message entered outside the firewall, the SIP message is converged to be sent into the IP terminal set in the 'default' item. Therefore, this item should be entered. The setup can be conveniently made when all traffic is considered as the calls of the digital phone by the Call Server. Therefore, on the 'default' item, in enter the IP Address of the Call Server (MCP).

The input box, which is placed in the back of four input boxes receiving IP addresses, is used for the input of the port information. In general, it inputs the standard SIP port number, 5060. When the Map information is added, 5060 is input as the default input to this input box.

MAP						
	ID	IP				
<input type="checkbox"/>	default	10	0	0	10	5060
<input type="checkbox"/>						5060

When adding the Map information, press the Add button to insert the information. When an entry needs to be deleted check the box to the left of the entry and then press the Delete button. All new or deleted information will be reflected on the system after the OK button on the lower side of the setup SIP configuration is clicked.

MAP						
	ID	IP				
<input type="checkbox"/>	default	10	0	0	10	5060
<input checked="" type="checkbox"/>	2003	10	0	0	20	5060

## Management

The SIP ALG service can be started or stopped using the [VoIP Service] → [SIP-ALG] → [Management] submenu.

### SIP ALG Management

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

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

### SIP –ALG Management Parameter Description

Parameter	Description
Activity	Shows the current SIP ALG status
Action	Used to change the status of the SIP-ALG server



NOTE

#### SIP ALG(SIP aware ALG)

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



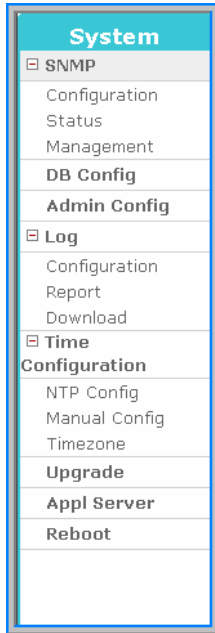
NOTE

#### SIP ALG and VoIP Service

VoIP Service and SIP-ALG cannot run at the same time

# System Menu

The System Menu is used to configure the SNMP settings, import or export the WIM database, to view system logs, to set time attributes, to upgrade the software, and to reboot the system. Select the **[System]** menu and the submenus will be displayed in the upper left side of the window as follows:



## System Menu Description

Menu	Submenu	Description
SNMP	Configuration	Used to display the configuration items of SNMP.
	Status	Used to display the SNMP configuration currently configured
	Management	Used to start or stop the SNMP service.
DB Config		Used to manage the current configuration DB of the WIM
Admin Config		Used to set up the authentication of the manager
Log	Configuration	Used to set up logging policies
	Report	Used to search the current system logs
	Download	Used to download the system logs
Time Configuration	NTP Config	Used to enter the NTP server info
	Manual Config	Used to manually configure time
	Timezone	Used to set the WIM timezone
Upgrade		Used to upgrade the WIM software
Appl Server		Used to allow SSH, FTP, and Telnet access to the WIM
Reboot		Used to Reboot the WIM



# SNMP

## Configuration

SNMP is a set of protocols used for managing complex networks. The [System] → [SNMP]→[Configuration] submenu is used by the administrator to enter SNMP System Options, SNMP Community information, SNMP v3 User information, and Trap Manager information. Once all the changes are entered then click the Save button at the bottom of the window. Click the Reset button to reset the configuration.

### System Option

The following window is used to set up the SNMP System Options.

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

### SNMP System Option Parameter Description

Parameter	Description
Location	Used to enter the information for System Location
Contact	Used to enter the information for System Contact
Name	Used to enter the information for System Name
Engine ID	Used to enter the information for System Engine ID

### Community

The following window is used to add new community information used in SNMP v1/2c.

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

### Community Parameter Description

Parameter	Description
New Community name	Used to fill in the new community name being added
Community Network	Used to set up new community network
Access	Used to set up the access authority.

## SNMPv3 Administrator Add

The following window is used to enter the SNMPv3 Administrator v3 information.

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

## SNMP v3 Parameter Description

Parameter	Description
<b>Administrator Name</b>	Used to enter the new administrator's name
<b>Administrator Password</b>	Used to enter the new administrator's password (8 alphanumeric characters)
<b>Authentication</b>	Used to set up the authentication method.
<b>Encryption</b>	Used to set up the ciphering method.
<b>Access</b>	Set up access authority.

## Trap Manager

The following window is used to set up the IP address used to transmit a trap. Up to five IP addresses can be entered.

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

## Trap Manager Parameter Description

Parameter	Description
<b>IP Address</b>	Used to set up a new Trap IP Address
<b>Community Name</b>	Used to set up a community to be used for transmitting to the Trap IP Address added.

## Status

The [Management] → [SNMP] → [Status] submenu is used to view the SNMP System Configuration information and to delete the SNMP Community, SNMPv3 User and SNMP Trap information. In order to delete the Community, User, and Trap settings select the box to the left of the item that needs to be deleted and then click the Delete button. Click the Reset button to initialize the settings.

### SNMP Config Information

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

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

Select	User Name	Access
	root	Read Write

Select	Trap IP	Trap Port
<input type="checkbox"/>	192.168.0.123	162

### Status Field Description

Field	Description
<b>System Information</b>	This field displays the information set up for the System Options.
<b>Select</b>	Used to select the information to delete.
<b>Community Name</b>	This field display the community name.
<b>Community Net</b>	This field displays the configured name of the Community Network.
<b>Community Access</b>	This field displays the access authority of the configured community.
<b>Administrator Name</b>	This field displays the configured administrator's name.
<b>Access</b>	This field displays the access authority of the configured administrator.
<b>Trap IP</b>	This field displays the configured Trap IP.
<b>Trap Port</b>	This field displays the configured Trap Port.

## Management

The [Management] → [SNMP] → [Management] submenu is used to start and stop the SNMP service. Click the Run button to start the SNMP service and click the Stop button to halt the SNMP service.

### SNMP Management

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

### SNMP Management Field Description

Field	Description
Activity	This field displays the operational condition of the SNMP service.
Action	Used to select whether to start or stop SNMP.

## DB Config

Use the [System] → [DB Config] submenu to export the WIM database, to import the WIM database, or to default the WIM to the factory defaults.

### Configuration System DB

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

### DB Config Parameter Description

Parameter	Description
Import	Used to restore a previously saved database
Export	Used to save the existing DB
Default	Used to restore the DB to factory defaults

After the WIM is defaulted the administrator must use one of the default IP addresses such as 10.0.2.1 through the LAN port when using Web Management.

## Admin Config

The [System] → [Admin Config] submenu is used to set up the authentication server for logging into the WIM and for changing the Web Time-out configuration. The choices for authentication server are Local, Radius or Taccas+ . Check the box of the authentication method desired and then click the OK button to save the change. Once the setting is applied then the selected authentication method configuration window will be displayed.

### Login Policy

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

### Local

The local password is the Admin password that is used to access the WIM router using Telnet, SSH, FTP, and Web Management. Enter the new password and then click the OK button to save the change.

### Local

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

### Radius

If a Radius server will be used then select the Radius box. Then enter the information for the Radius authentication server. Up to 5 lists can be entered.

### Radius

Radius Server IP	Radius Server Key	Time out
<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	<input type="text"/>	<input type="text"/>

## Taccas+

If Taccas+ will be used then select the Taccas+ box. Enter the information for the Taccas+ authentication method. Up to 5 lists can be entered. When deleting the list of all the server IPs, the corresponding secret key values are also deleted.

## Taccas+

Taccas+ Server			
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Taccas+ Secret Key
<input type="text"/>

## Web Time-out Configuration

This setting is used to lengthen or shorten the amount of time before the Web Management of the WIM Data Server Times out. When a change is made to this parameter the system administrator will be logged out of the WIM.

## Web Time-out Configuration

Category	Value	
Time	<input type="text" value="Enable"/> <input type="button" value="v"/>	<input type="text" value="60"/> Min ( 1 ~ 1440)

## Log

The **[Log]** submenu is used to configure the system log by selecting specific WIM attributes, to run system log reports, and to download a system log report to a file.

### Configuration

The **[System] → [Log] → [Configuration]** submenu is used to determine which system attributes will be included in the system log.

#### Log Policy

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

Click the ON or OFF radio button to include or ignore the WIM attribute. The choices are System , NETWORK, FIREWALL, PPTP, IPsec, and L2TP. Once the radio buttons are selected then click the OK button to apply the changes.. Click the Reset button to return the Log Policy to the previous status before applying the change.

### Report

Using the **[System] → [Log] → [Report]** submenu the administrator can retrieve the logs stored in the system according to attributes, date, and time.

#### Report Policy

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

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

Click the radio button for the desired log type and then select the date and time. Then click the OK button to run the report. Click the Reset button to return the log report settings to default.

## Log Report

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

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

1/4



## Download

Using the [System] → [Log] → [Download] submenu the administrator can download a log report to a PC. Simply press the Download button and the system log will be downloaded in the form of a compressed file.

### Log File Management

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

Download

## Time Configuration

Using the [System] → [Time Configuration] submenu the system administrator can either synchronize the date and time of the WIM with a NTP server or manually set the date and time.

### NTP Config

Use the [System] → [Time Configuration] → [NTP Config] submenu to set up a NTP Time Server/s to synchronize the date and time with the WIM. The Current Time window indicates the current date and time of the WIM. The NTP Server Status window indicates the status of NTP Server synchronization process.

The Time Server fields are used to enter the NTP Time Server IP Addresses. Click the OK button to start or restart the NTP daemon to register the Time Server.

### NTP Configuration

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

NTP Server Status	
Status	stop

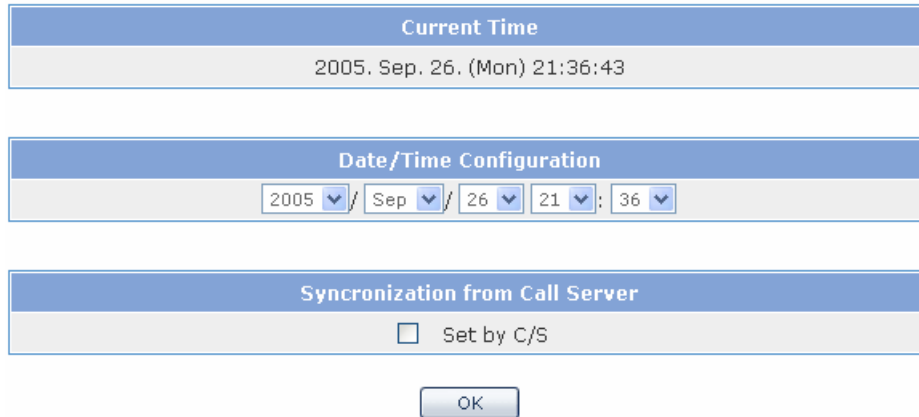
Time Server	
Server 1	<input type="text"/>
Server 2	<input type="text"/>

OK

## Manual Config

By using the [System] → [Time Configuration] → [Manual Config] submenu the administrator can manually set and modify the date and time of the WIM. In the Date/Time Configuration window enter the desired date and time and then click the OK button to save the changes. The new date and time will be displayed in the Current Time window. In order to synchronize the date and time of the system with the MP40 then check the Set by C/S box and then click the OK button to save the change..

### Manual Configuration

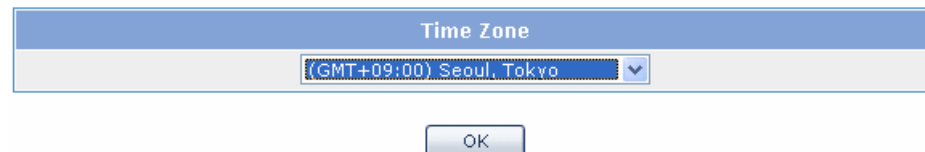


The Manual Configuration dialog box consists of three main sections. The first section, titled "Current Time", displays the current date and time as "2005. Sep. 26. (Mon) 21:36:43". The second section, titled "Date/Time Configuration", contains five dropdown menus for selecting the year (2005), month (Sep), day (26), hour (21), and minute (36). The third section, titled "Synchronization from Call Server", includes a checkbox labeled "Set by C/S" which is currently unchecked. An "OK" button is located at the bottom center of the dialog.

## Timezone

By using the [System] → [Time Configuration] → [Timezone] submenu the administrator can change Time Zones by selecting the desired timezone and then by clicking the OK button to save the change.

### Time Configuration



The Time Configuration dialog box features a single dropdown menu titled "Time Zone" with the selected option "(GMT+09:00) Seoul, Tokyo". An "OK" button is positioned at the bottom center of the dialog.

## Upgrade

Upgrading the WIM software is performed using the **[System] → [Upgrade]** submenu. First obtain the appropriate upgrade files . Then enter the new software package version number in the Package Version field.

### Select Package Upgraded

Package Version	Current Version	Released Date	Upgraded Date
<input type="text" value="v.1.29"/>	v1.28	2007.03.16	2004.11.30

Then select one of the three types of upgrade methods (TFTP, HTTP, or Local). If the Upgrade method is TFTP or HTTP enter the correct IP address of the server. Then click the OK button to start the upgrade process.

### Select Upgrade Method

Upgrade Method	Upgrade Server IP
<input checked="" type="radio"/> TFTP	<input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="1"/> . <input type="text" value="20"/>
<input type="radio"/> HTTP	
<input type="radio"/> Local	<input type="text"/> <input type="button" value="Browse..."/>

## Appl Server

Using the **[System] → [Appl Server]** submenu the administrator can control remote access to the WIM using SSH, FTP and Telnet. In order to secure the system from hackers Samsung recommends that these are disabled and only turned on when the administrator needs to use them for debugging, and uploading or downloading files.

### Application Server

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

Check the box of the access method and then click the OK button to save the change.

## Reboot

Using the [System] → [Reboot] submenu the administrator can reboot the WIM.


### System Reboot

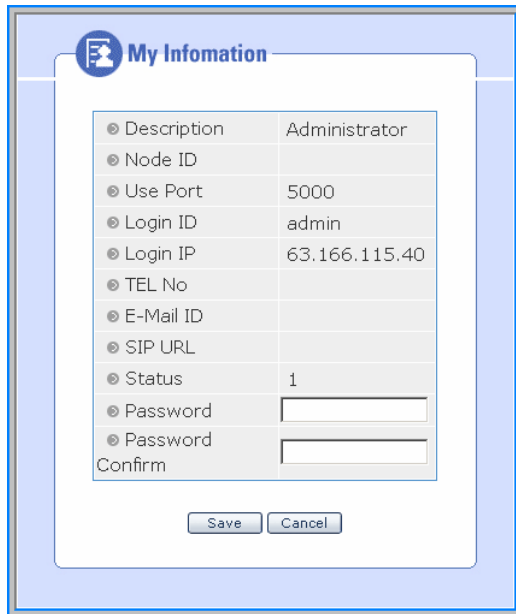


Simply click the OK button and all the services will be terminated and the system will reboot.

The webscreen will return to the initial login window and the webscreen will not operate until the network and services are all up and running

## My Info Menu

Click the  My Info icon on the upper right hand side of the WIM Web Page to open the My Info window. In this window administrators can enter the admin password which is used when logging into the WIM router. Enter the new admin password into the Password and Password Confirm fields and then click the Save button. The password must be alpha and/or numeric characters.



The image shows a web-based form titled "My Information" with a blue header and a light blue border. The form contains a table of configuration fields, each with a radio button icon. The fields are:

Description	Administrator
Node ID	
Use Port	5000
Login ID	admin
Login IP	63.166.115.40
TEL No	
E-Mail ID	
SIP URL	
Status	1
Password	<input type="text"/>
Password Confirm	<input type="text"/>

At the bottom of the form are two buttons: "Save" and "Cancel".

# ANNEX A. VPN Setting for Windows XP/2000

If IPsec or PPTP tunneling is used on a Microsoft server or PCs in order to connect to the OfficeServ 7200 WIM Data Server, then the VPN needs to be configured on MS Windows. This section describes how to set up the VPN on Windows XP. The Windows 2000 OS is done in a similar fashion.

For this example we will use the following information:

- External IP address of the OfficeServ WIM: 211.217.127.40
- Internal IP address of the OfficeServ WIM: 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 algorithms 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.

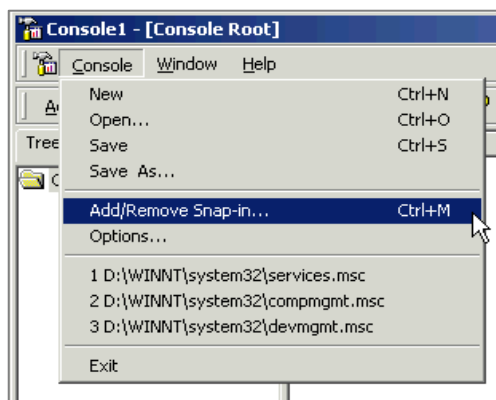


NOTE

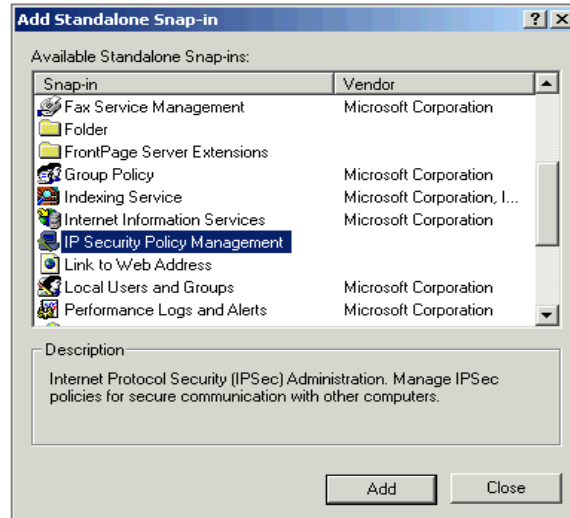
### IPsec Setting in Windows XP/2000

- 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.

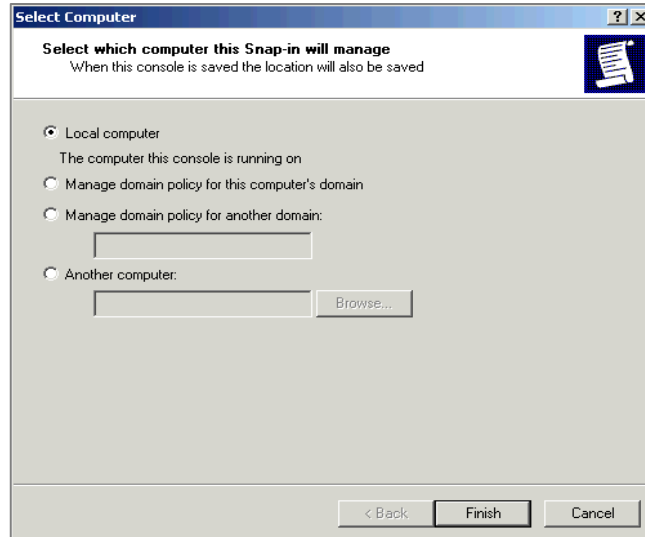
1. Select [Start] → [Run] and in the task bar type in 'mmc' <enter> to display the window below: In the console window, select the [File] → [Add/Remove Snap-in...].



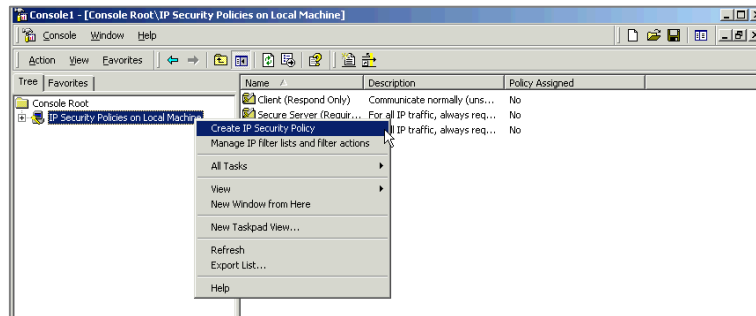
2. In the <Add/Remove Snap-in...>, click the **[Add]** button to display the following window: Select 'IP security policy management' in the Add/Remove Snap-in... menu and then click the **[Add]** button.



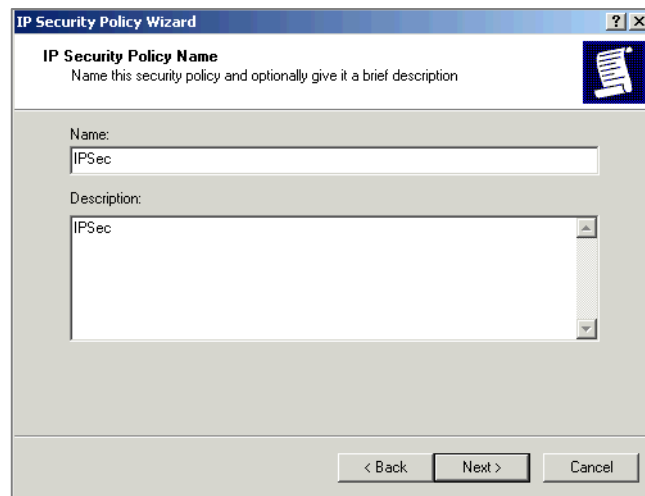
3. Select 'Local computer' in the window below and then click the **[Finish]** button.



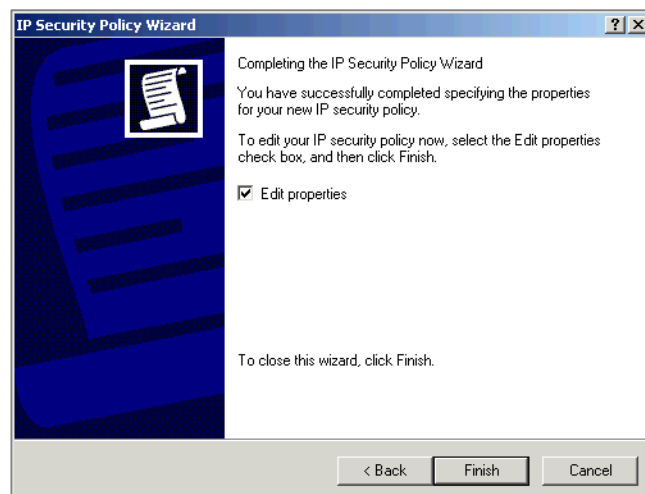
4. Move to the <Console> window. Then, 'IP Security Policies on Local Machine' of the 'Console Root' is created. Select the item and then right click the [Create IP Security Policy] menu.



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

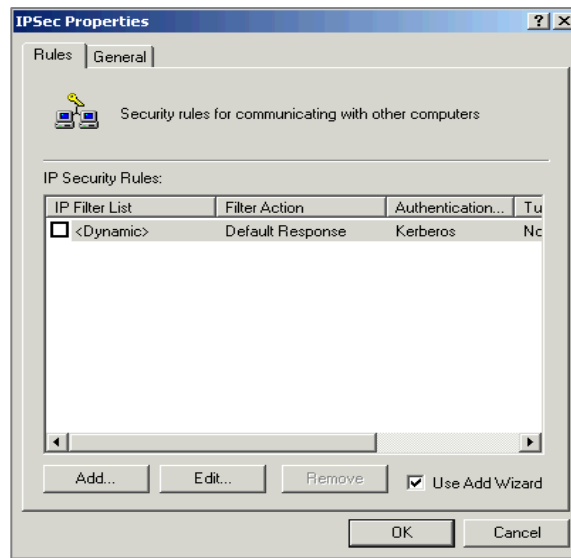


6. If 'Activate the default response rule' is checked, release the check and then click the [Add] button to display the window below: Check 'Edit Properties' and then click the [Finish] button.

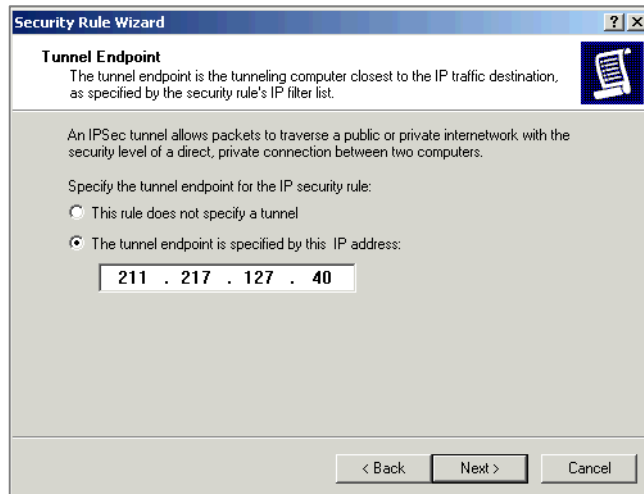




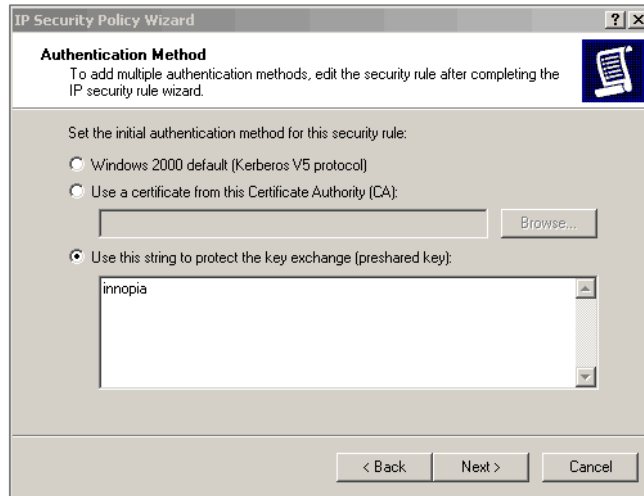
7. When the <XP\_OPsec Registration Information> window is displayed, the created items are displayed. If the corresponding item is checked, release the check and then click the [Add] button.



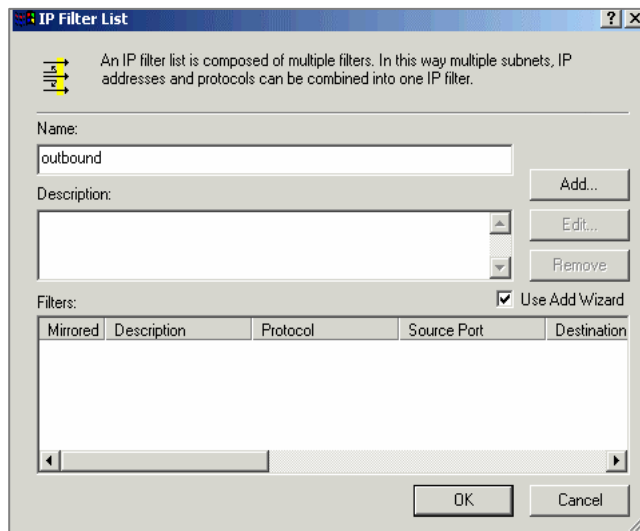
8. Click the [Add] button on the <Security Rule Wizard> window to display the window below: Select 'The tunnel endpoint is specified by this IP address' and enter the firewall external IP address (211.217.127.40). Then click the [Next] button.



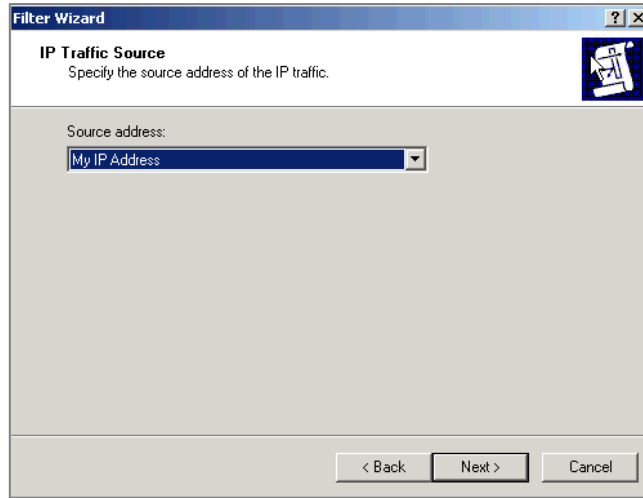
9. Select the Local Area Network (LAN) on the <Network Type> window and then click the [Add] button to display the window below: Select ‘Use this string to protect the key exchange [preshared key]’ and enter the password registered with the firewall. Then click the [Next] button.



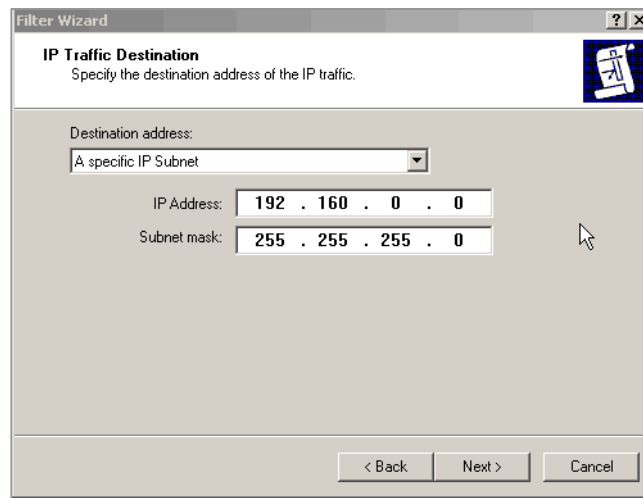
10. Click the [Add] button on the <Security Rule Wizard> window to display the window below: Enter ‘outbound’ in the Name field and then click the [Add] button.



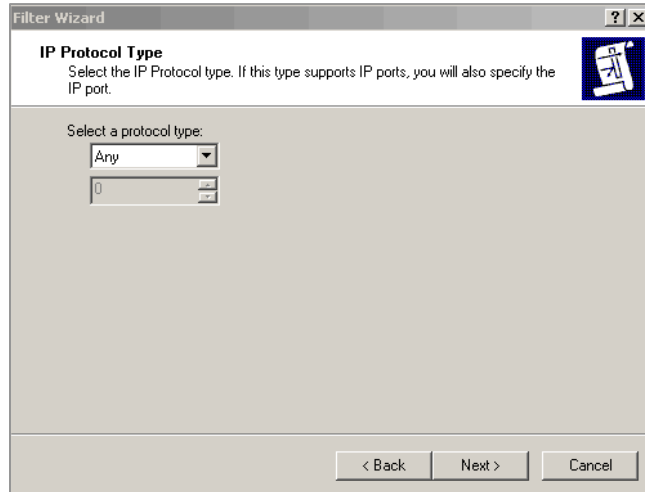
11. Click the **[Add]** button on the <IP Filer Wizard> window to display the window below:  
Select 'My IP address' in the Source address field and then click the **[Add]** button.



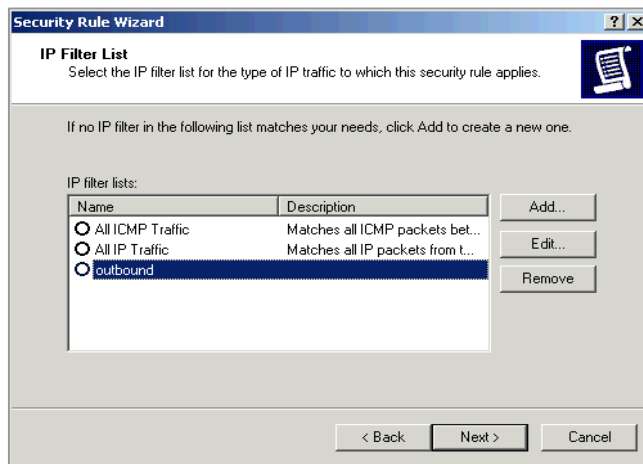
12. Select 'Specific IP Subnet' in the target address and enter the internal network address (192.168.0.0) and subnet mask (255.255.255.0).  
Then click the **[Next]** button.



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

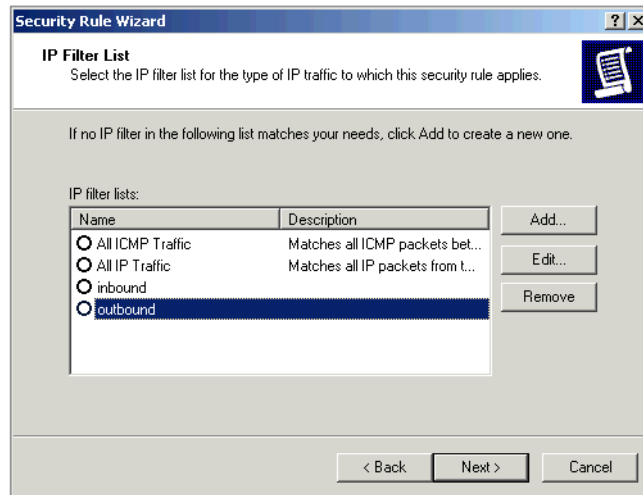


14. Then click the **[OK]** button. Then, the outbound item is created. Click the **[Add]** button to create the inbound item.

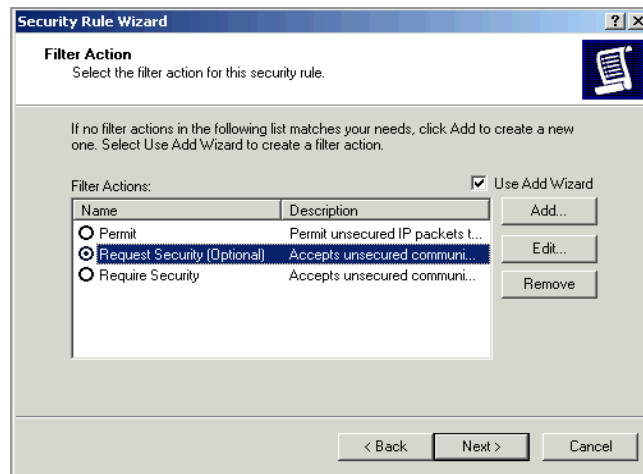


15. Enter the 'inbound' in the Name field and click **[Add]** like step 10. The above steps 11 through 13 also apply to this procedure.

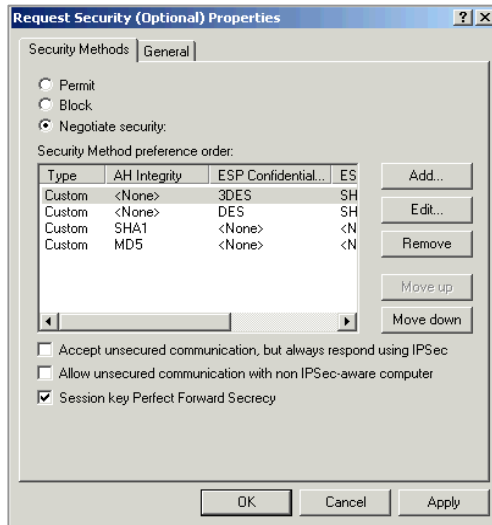
16. Click the **[Add]** button to display the window below: Then, select the 'outbound' item and click the **[Next]** button.



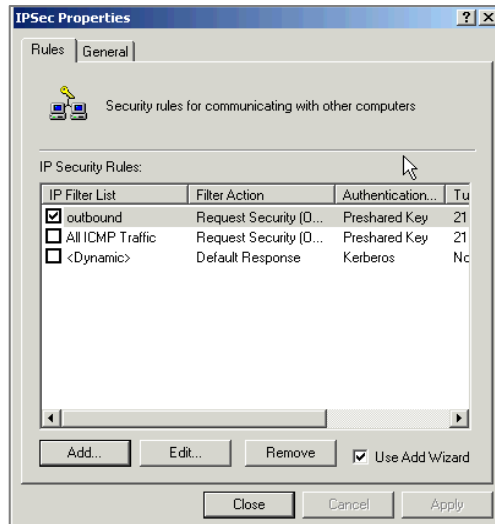
17. Select the 'Request Security [Optional]' item and then click the **[Edit]** button.



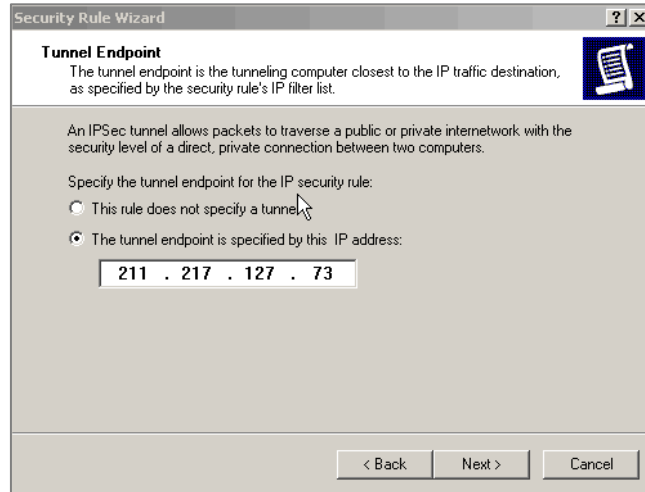
18. Select 'Negotiate security' and select 'AH Integrity(None), ESP Confidential(3DES), ESP Integrity(MD5)' in the Security Method preference order. Click the **[Move up]** button to move to the first row of the corresponding item. Check 'Session key Perfect Forward Secrecy(PFS)' and then click the **[OK]**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



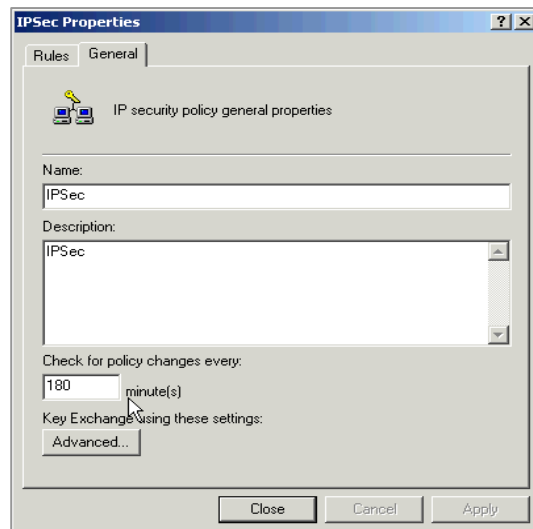
19. Check 'Edit Properties' and then click the **[Finish]** button to display the window creating the outbound item. Click the **[Add]** button to create the inbound item.



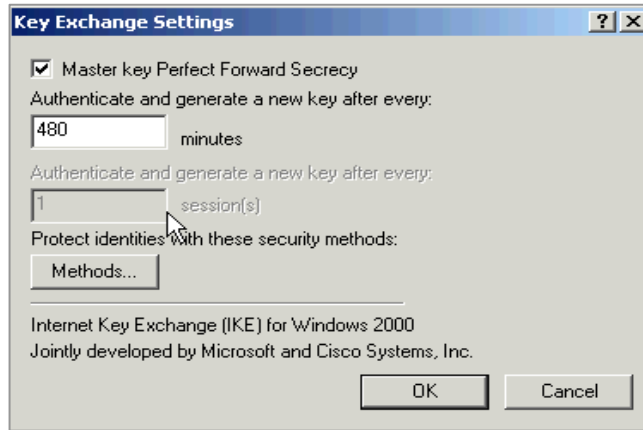
20. Click the **[Next]** button on the <Security Rule Wizard> window to display the window below: Check ‘The tunnel endpoint is specified by this IP address’ and enter the IP address of a client PC. Then click the **[Next]** button.



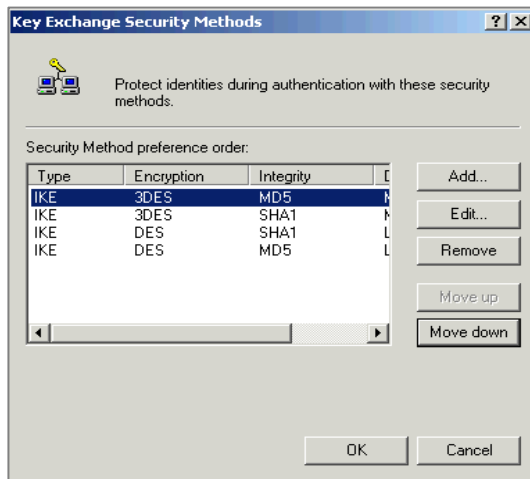
21. Select Local Area Network (LAN) on the <Network type> window and then click the **[Next]** button. Select ‘Use this string to protect the key exchange **[preshared key]**’ and enter the password registered with the firewall. Click the **[Next]** button. (Refer to step 9.)
22. Select the ‘inbound’ item in the step 16 window and then click the **[Next]** button. Follow the step 17 and 18.
23. Check ‘Edit Properties’ and then click the **[Finish]** button to display the window below: Select the **[General]** tab and then click the **[Advanced]** button.



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

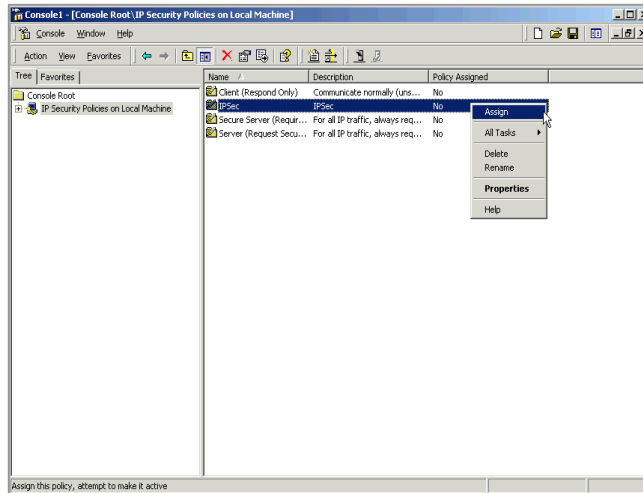


25. Select 'Encryption (3DES), Integrity (MD5), Diffie-Hellman (Med)' in the window below and then click the [Move up] button to move the first row of the corresponding item. Click [OK].

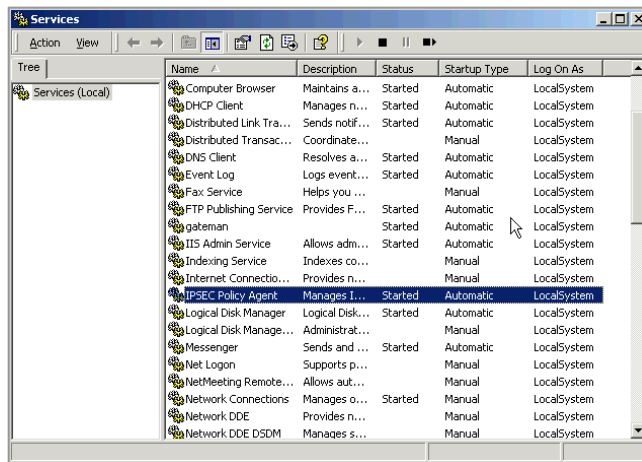




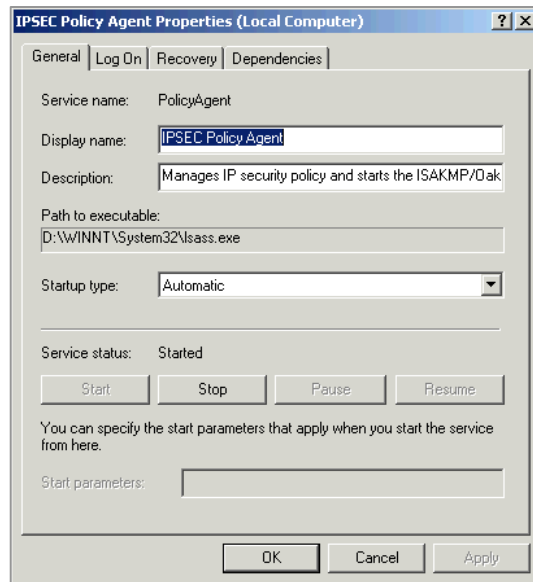
26. Select 'IP Security Policies on Local Machine' on the <Console> window. Select the item newly created on the right corner of the window and right-click the [Assign] menu. Then, policy assignment is changed into 'Yes'.



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



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



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

```
C:\>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Negotiating IP Security.
Reply from 192.168.0.1: bytes=32 time=5 ms TTL=255
Reply from 192.168.0.1: bytes=32 time=6 ms TTL=55
Rply rom 92.1.0.1 yte=32 tme=4 s TTL=55

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

## PPTP Setting

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



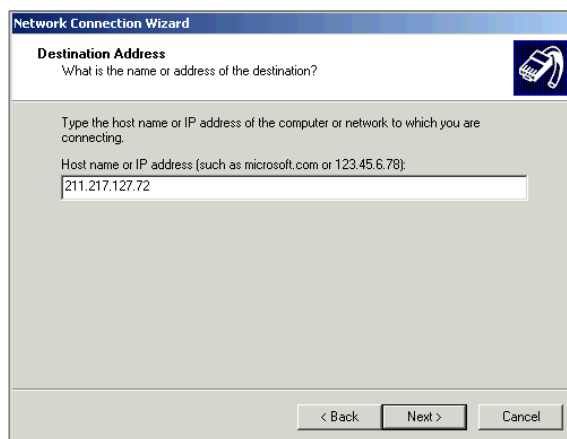
### PPTP Setting in Windows XP/2000

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

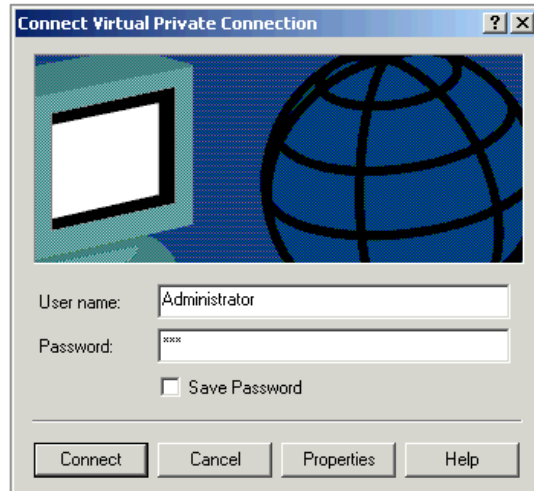
1. Double click the **[My Network Environment]** icon and select the **[Property]** item from the Windows desktop. Double click **[Create New Connection]** on the upper right corner of the screen to display the window below: Click **[Next]**.



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



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



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

# ABBREVIATION

---

## A

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

## B

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

## C

CHAP	Challenge-Handshake Authentication Protocol
CTI	Computer Telephony Integration

## D

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

## E

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

## G

WIM	Gigabit WAN Interface Module
GVRP	GARP VLAN Registration Protocol

## H

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

## I

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

## L

LAN	Local Area Network
L2TP	Layer 2 Tunneling Protocol

## N

NAT	Network Address Translation
NTP	Network Time Protocol

## R

RMON	Realtime Monitoring
RP	Rendezvous Point
RSTP	Rapid Spanning Tree Protocol

## P

PAP	Password Authentication Protocol
PIM-SM	Protocol Independent Multicast-Sparse Mode
PD	Power Device
PoE	Power Of Ethernet
PPTP	Point to Point Tunneling Protocol
PT	Protocol Translation
PVC	Permanent Virtual Circuit
PVID	Port VLAN Identification

## S

STP	Spanning Tree Protocol
SMTP	Simple Mail Transfer Protocol
SNAT	Source Network Address Translation
SNMP	Simple Network Management Protocol
SPQ	Strict Priority Queuing

## T

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

# V

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