Enterprise IP Solutions

OfficeServ 7400

GWIMT/GWIM User Manual

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

Samsung Telecommunications

Publication Information

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

Trademarks

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

PRINTED IN USA

INTRODUCTION

Purpose

This document introduces the OfficeServ 7400 GWIMT/GWIM Data Server, an application module of the OfficeServ 7400, 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 7400 GWIMT/GWIM

This chapter briefly introduces the OfficeServ 7400 GWIMT/GWIM.

CHAPTER 2. Installing OfficeServ 7400 GWIMT/GWIM

This chapter describes the installation procedure and login procedure.

CHAPTER 3. Using OfficeServ 7400 GWIMT/GWIM

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

ABBREVIATIONS

Abbreviations frequently used in this document are described.

Conventions

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

WARNING

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

CAUTION

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

CHECKPOINT

Provides the operator with checkpoints for stable system operation.

NOTE

Indicates additional information as a reference.

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.
- '**`Bold Courier New`**' font will indicate the value entered by the operator on the console screen.

Reference

OfficeServ 7400 General Description

The OfficeServ 7400 General Description introduces the OfficeServ 7400 platform and presents the information necessary to understand the hardware configuration, specification, and system functionality.

OfficeServ 7400 Installation Manual

The OfficeServ 7400 Installation Manual describes the installation of the system and how to inspect and operate the system.

OfficeServ 7400 Programming Manual

The OfficeServ 7400 Call Server Programming Manual describes how to program the system using Man Machine Communication (MMC) entries.

Revision History

EDITION	DATE OF ISSUE	REMARKS
00	10. 2005.	Original Draft
01	02. 2006.	Second Edition
02	03. 2007.	Descriptions of GWIMT/GWIM are added. - Programming Examples are added - 'Ping' utility is modified. - 'Network Link'/'Ping'/'HTB QoS'/'Policy' are modified. - UI of 'IPsec Management' is modified. - 'SIP-ALG'/'Taccas+' are modified. - 'IDS Rule update' is added. - Setting Web Time-out of 'Admin Config' is added. - Method option of WAN-> PPPoE is deleted. - IPSec -> Configuration menu is modified. - Connection Add menu is modified. - Router value configuration is modified. - VoIP Service menu is modified. - Key Chain description added

SAFETY CONCERNS

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

Symbols

Caution

Indication of a general caution.

Restriction

Indication for prohibiting an action for a product.

Instruction

Indication for commanding a specifically required action.

CAUTION

For Security

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

When Setting IP Range

The number of IPs for the ‘Local IP range’ and that for the ‘Remote IP range’ should be identical when setting PPTP VPN.
For example, if the number of IPs for ‘Local IP range’ is 10 and that for ‘Remote IP range’ is 20, only 10 calls will be set.

When Setting PPTP in Windows XP/2000

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

When Changing Network Interface

Note that all IP sessions connected through a GWIMT/GWIM interface are disconnected for a while if the network interface (i.e., IP, Gateway, and Subnet Mask) is changed and saved.

When Using a Web Browser

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

When Using Dynamic IPs of DHCP, PPPoE, and VDSL

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

When Changing DB

If the DB is changed in OfficeServ 7400 GWIMT/GWIM, the system restarts.

When Using a Private Key

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

When Deleting Internet Temporary Files

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

TABLE OF CONTENTS

CHAPTER 1. Overview of OfficeServ 7400 GWIMT/GWIM

This chapter introduces the OfficeServ 7400 system and OfficeServ 7400 GWIMT/GWIM Data Server.

Introduction to the OfficeServ 7400

The OfficeServ 7400 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 GWIMT/GWIM, GPLIMT/GPLIM, and GSIMT/GSIM Data Modules, the OfficeServ 7400 provides network functions such as a gigabit switching, Power Over Ethernet, high speed data routing, and network security in a single converged solution.

This document describes the data and routing capabilities of the OfficeServ 7400 GWIMT/GWIM Data Server.

Structure of OfficeServ 7400

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

Introduction to the OfficeServ 7400 GWIMT/GWIM Data Server

GWIMT Module

GWIM Module

The OfficeServ 7400 GWIMT/GWIM Data Server provides the following functionality:

Router Functions

- Path management and queuing function of data packets for external WAN and internal LAN
- Static and dynamic routing functions
  - Support of Routing Information Protocol version1(RIPv1), RIPv2, (Open Shortest Path First version2) OSPFv2, (Border Gateway Protocol 4) BGP4 routing protocol
- Dynamic Host Configuration Protocol (DHCP)
- Point-to-Point Protocol over Ethernet (PPPoE) client function in Ethernet WAN interface
- Encapsulation function of High-level Data Link Control (HDLC), PPP, and Frame Relay in Serial WAN interface
- Support of IP Multicast
  - Support of IGMPv1(Internet Group Management Protocol version1), IGMPv2 protocols
  - Support of Distance Vector Multicast Routing Protocol (DVMRP), (Protocol Independent Multicast-Sparse Mode) PIM-SM multicast routing protocol
- Access interface function for WAN
  - GWIMT: 3-10/100/1000 Ethernet ports: For WAN or LAN interfaces
  - GWIM: 3-Gigabit Ethernet ports: For WAN or LAN interfaces
  - 2-Serial WAN ports: For hooking up data private lines via a DSU or CSU which supports V.35 1 port or HSSI 1
- Network Load Balance (NLB) function
  - Function that equally distributes the load by setting several gigabit Ethernets or serial interfaces into WAN and increases the availability by automatically sharing the load with other lines when a line is not operated.

Data Network Security Functions

- Outbound and Inbound NAT (Network Address Translation)/PT (Protocol Translation) function
  - Access control for internal resources via the conversion between common IP and public IP
- Firewall function
  - Access control from the outside by Extended Access List
- Intrusion Detection System (IDS) function
  - Detection and report of the access for the access control area by the access list
  - Recognition and notification of illegal packets by applying the basic intrusion rule for packets
  - Detection and block of DoS attack such as SYN Flood
- Virtual Private Network VPN function
  - VPN gateway function based on Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), and Internet Protocol Security Protocol (IPSec)
  - Confidentiality and integrity functions via VPN tunneling and data encryption

Data Network Application Functions

- Data network application functions such as NAT/PT, firewall, VPN, DHCP, and Application Level Gateway (ALG)
- Use of Application Software operating in GWIMT/GWIM board
- ALG function
  - Support to operate the security function and smoothly pass the VoIP packets by implementing the AIG function for signaling and media traffic
- DHCP Server function
  - Auto-configuration of network environment for the IP equipment in another functional block of the OfficeServ 7400 system
- DHCP Relay function
  - Function to connect the IP equipment in another functional block of the OfficeServ 7400 system to external DHCP server for the auto-configuration of network environment

QoS Function

- Priority queuing process for layer 3 packets and priority queuing for a specified IP
- Priority queuing process for layer 4 packets and priority for RTP packets (UDP/TCP port)

Management Function

- Advanced debugging functions via Telnet connection
- Configuration and verification functions for the operations of GWIMT/GWIM functional block via a browser
- Configuration and verification functions for the operations of GWIMT/GWIM functional block via the Simple Network Management Protocol (SNMP)
- 4 Real-time Monitoring (4RMON) function
- Program Upgrade
  - Program upgrade via Trivial File Transfer Protocol (TFTP)
  - Program upgrade via Hypertext Transfer Protocol (HTTP)
  - Program upgrade via local manager’s PC

CHAPTER 2. Installing OfficeServ 7400 GWIMT/GWIM

This chapter describes the installation and the login procedure for OfficeServ 7400 GWIMT/GWIM.

Software Installation

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

Package	File	Description
Bootrom Package	gwim-bootldr.img-vx.xx gwim-bootldr.img-vx.xx.sum	Boot ROM program
Main Package	gwim-pkg-vx.xx.tar.gz	Upgrade package for HTTP
	gwim-os..img-vx.xx	'os' partition upgrade package for TFTP
	gwim-firmware.img-vx.xx	'Firmware' partition upgrade package for TFTP
	gwim-configdb.img-vx.xx	'configdb' partition upgrade package for TFTP
	gwim-logdb.img-vx.xx	'logdb' partition upgrade package for TFTP
	gwim-flash1.img-vx.xx gwim-flash1.img-vx.xx.sum	Fusing file for the first flash memory
	gwim-flash2.img-vx.xx gwim-flash2.img-vx.xx.sum	Fusing file for the second flash memory

GWIMT/GWIM Installation

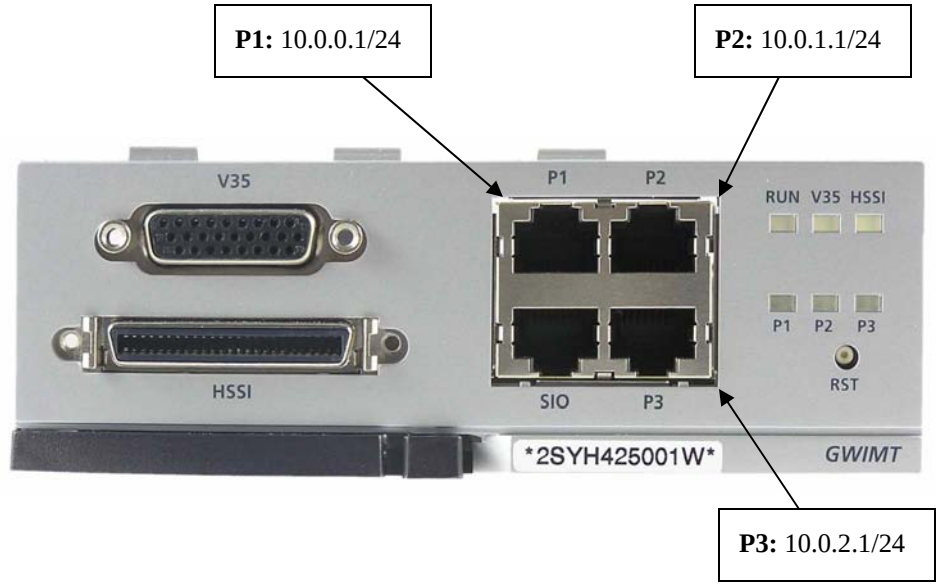
1. Insert the GWIMT/GWIM into an open slot in the OfficeServ 7400 cabinet **(excluding slots 0 or 3 which are reserved for the MP40 and LP40 cards)**.

2. Connect a PC to port #1-3 of the GWIMT/GWIM module with either a straight or 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 GWIMT/GWIM interface 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 GWIMT/GWIM.

   The default IP value of the GWIMT/GWIM 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)



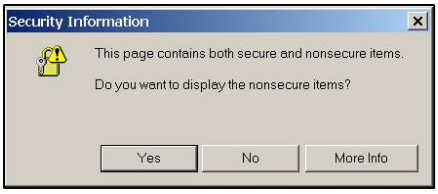
Caution when using a Web Browser

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

Getting Started

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

2. A Security Information window will now open. Click on the Yes button to proceed.

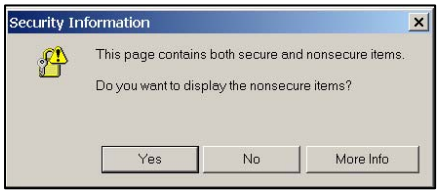


3. The Administrator will now be prompted for a Login ID and Password.

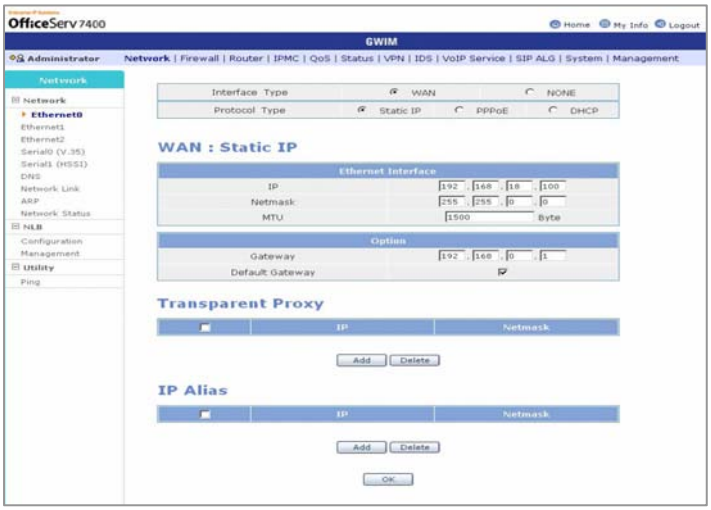
NOTE

The login ID is "**admin**" and the default password is "**root**".

4. Log into the GWIMT/GWIM using the administrator ID and password and then click on the OK button. The following Security Information window will appear again. Click on the Yes button to proceed.



5. The GWIMT/GWIM 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 7400 GWIMT/GWIM’ of this document.



6. Click the Logout button on the upper section of the screen to close the connection to the GWIMT/GWIM system.

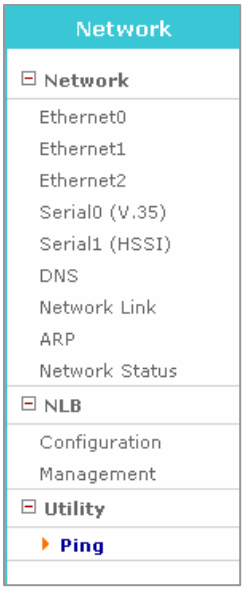
CHAPTER 3. Using OfficeServ 7400 GWIMT/GWIM

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

The menus of the OfficeServ 7400 GWIMT/GWIM Data Server are as follows:

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 7400 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.
	Serial0(V.35)	Used to setup the V.35 Serial port.
	Serial1(HSSI)	Used to setup the HSSI 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

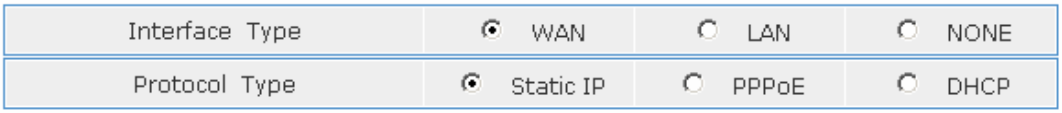
The **[Network]** menu is used to view and configure the five network interfaces that are built-in to the GWIMT/GWIM. This menu is used to set the IP Address information, transfer speed, and transfer mode of each interface. In addition, this menu is used to set the DNS server IP address information and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

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

Ethernet Setup

The **[Network]** → **[EthernetX] (X = 0 through 2)** 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.



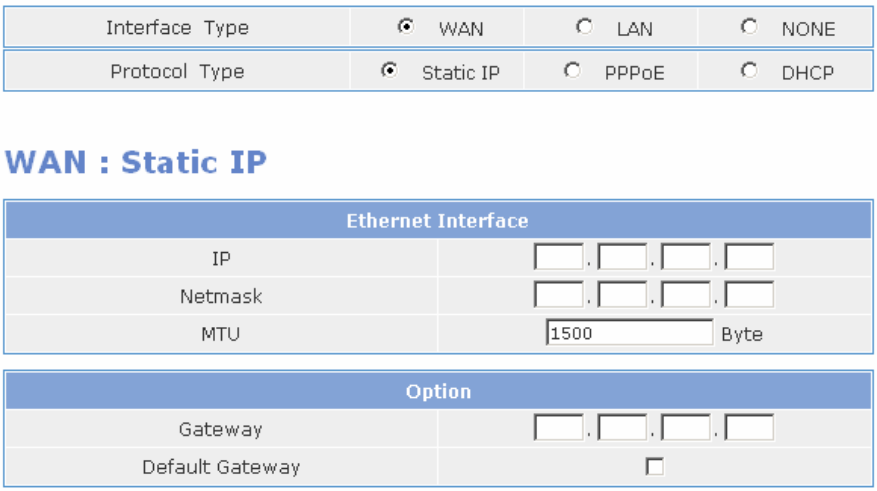
The fields that are displayed will vary depending on the type of interface being defined. The details of each interface type are as follows:

- 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.



Static WAN Parameters

Parameter	Description
IP	Used to enter the public IP address assigned to the WAN interface
Netmask	Used to enter the Subnet Mask information for the WAN interface
MTU	Maximum Transmission Unit: Leave this field at default unless told to change by Samsung Technical Support
Gateway	Used to enter the public IP address received from the Internet Service Provider (ISP) or the IP address of a router
Default Gateway	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 7400 system without the change of the existing network. To add entries, click the Add button and enter the following IP address and netmask . To delete entries, select the entry to be deleted and click the Delete button.
- IP Alias: Is used to add up to 32 IP addresses**.** To add entries, click the Add button and enter the following IP address and netmask. To delete entries, select the entry to be deleted and 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	(•) WAN	( ) LAN	( ) NONE
Protocol Type	(•) Static IP	( ) PPPoE	( ) 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	☑

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 GWIMT/GWIM Routing Table as **0.0.0.0/0 [1/0] via 10.0.0.1, eth1**.

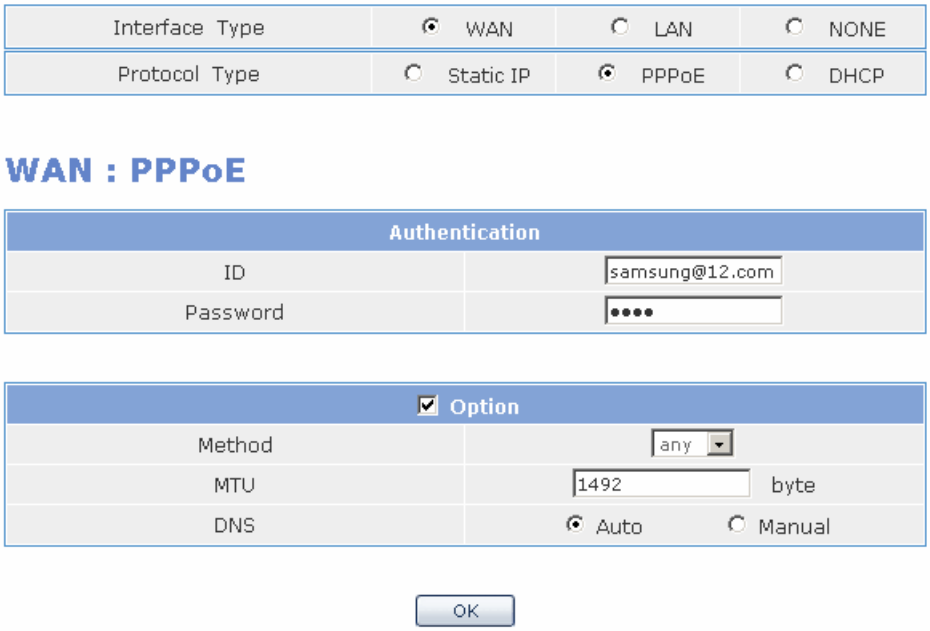
Routes

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.

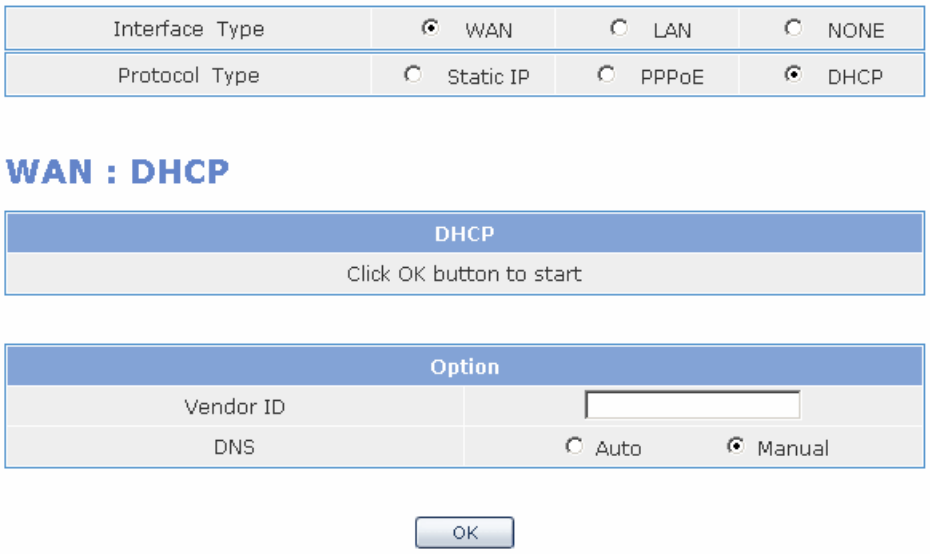


PPPoE WAN Parameters

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 GWIMT/GWIM 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

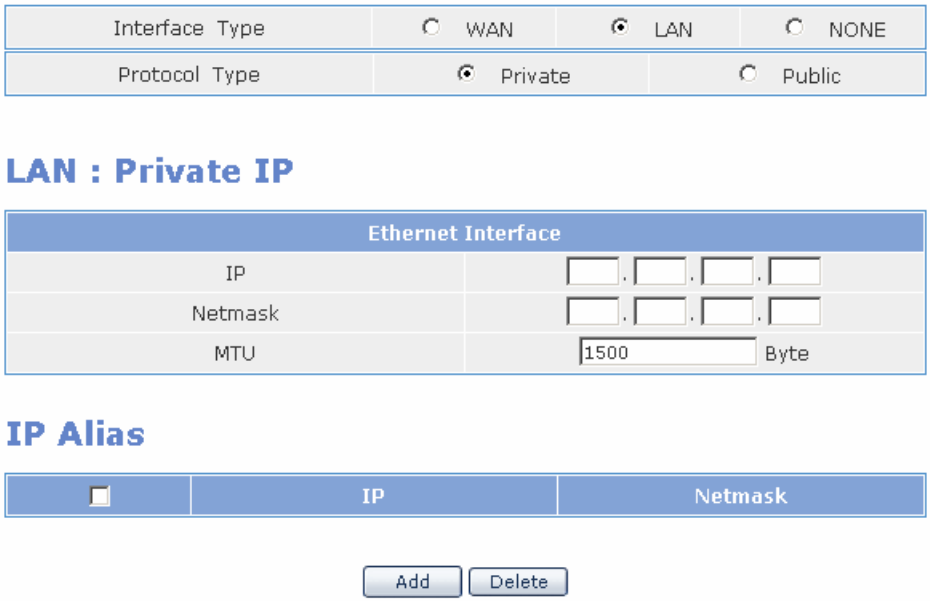
Select the WAN-DHCP category to display the following setup window. The WAN-DHCP information is automatically configured without any special setup fields. The OK button must be clicked in order to complete the setup.



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.



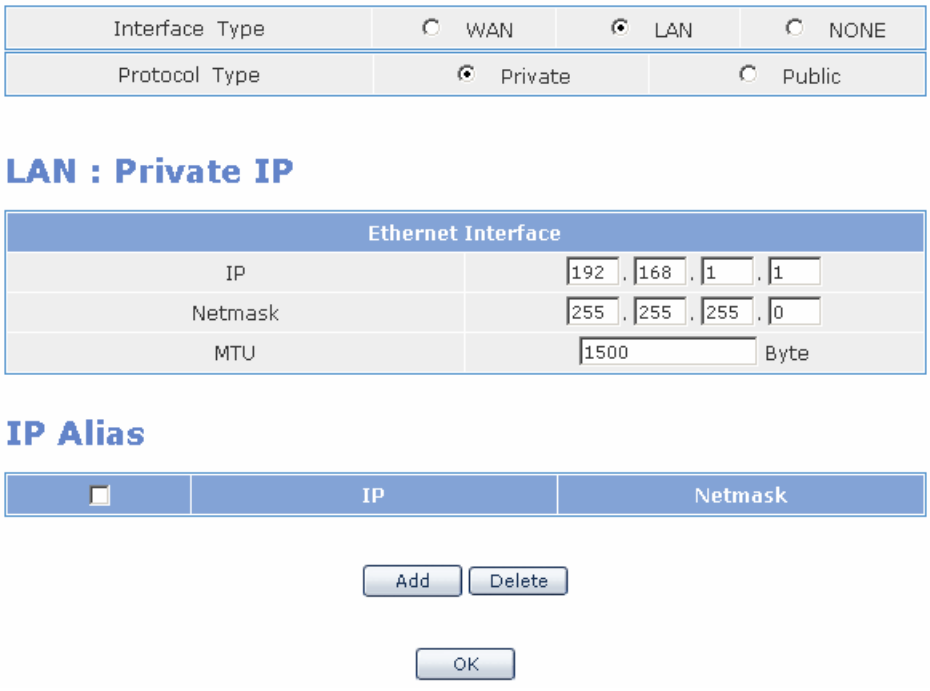
Enter the IP address and the netmask value to be assigned to the Ethernet interface. The IP Alias field is the same as the corresponding input field displayed when selecting WAN → Static IP.

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

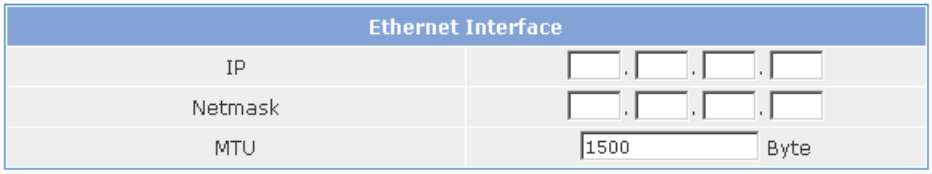
LAN → Private IP Programming Example

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.



LAN → Public IP

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



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

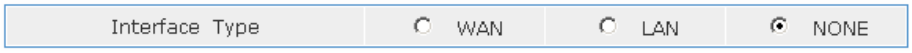
NONE is selected when the corresponding interface is not going to be used.

Setup Details fo the Serial0 (V.35) and Serial1 (HSSI) Connections

Serial Interface Type

The **[Network]** → **[Serial0 (V.35]** and **[Network]** → **[Serial1 (HSSI]** submenus enable the administrator to specify the Serial Interface parameters.

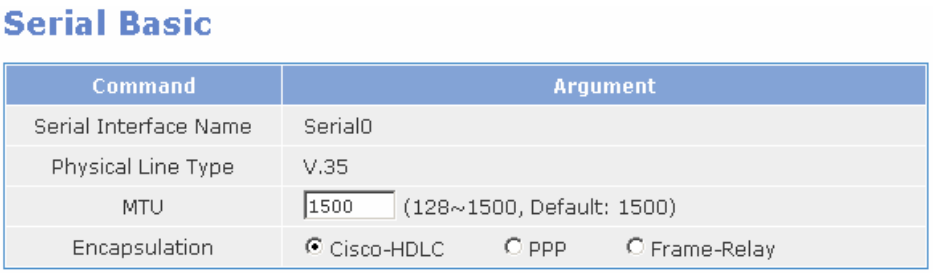
Select one of the two Serial Interfaces to display the setup window shown below.



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.

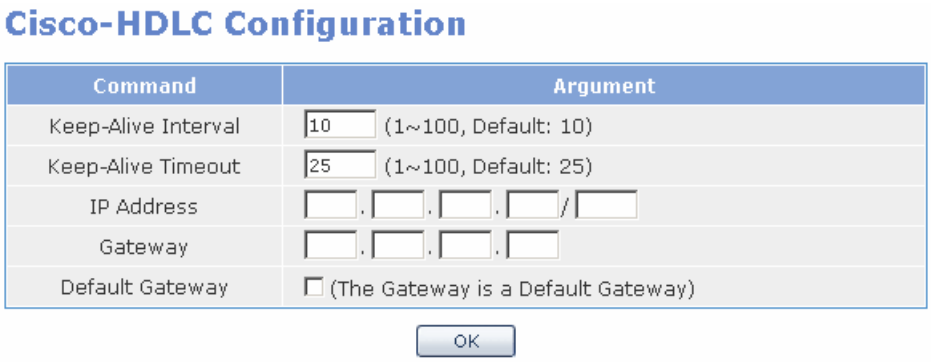


Serial Basic Parameters

Parameter	Description
Serial Interface Name	Name of the current serial port
Physical Line Type	Physical line type of the current serial port
MTU	Maximum Transmission Unit: Leave this field at default unless told to change by Samsung Technical Support
Encapsulation	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.

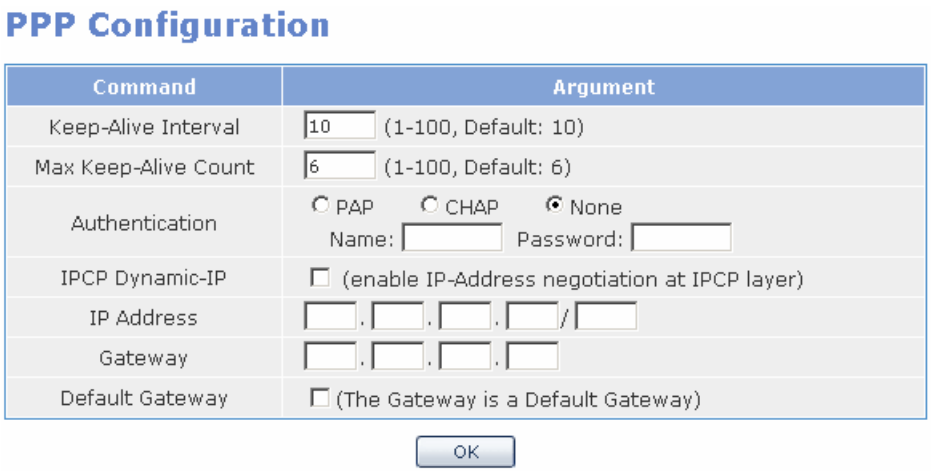


Cisco-HDLC Parameters

Parameter	Description
Keep-Alive Interval	Time interval to check Keep-Alive
Keep-Alive Timeout	Time to estimate the failure of Keep-Alive
IP Address	IP Address of the serial port
Gateway	Gateway IP Address(Peer Address) of the serial port
Default Gateway	Mark the check box to set this gateway to default gateway. (This item is displayed 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 Parameters

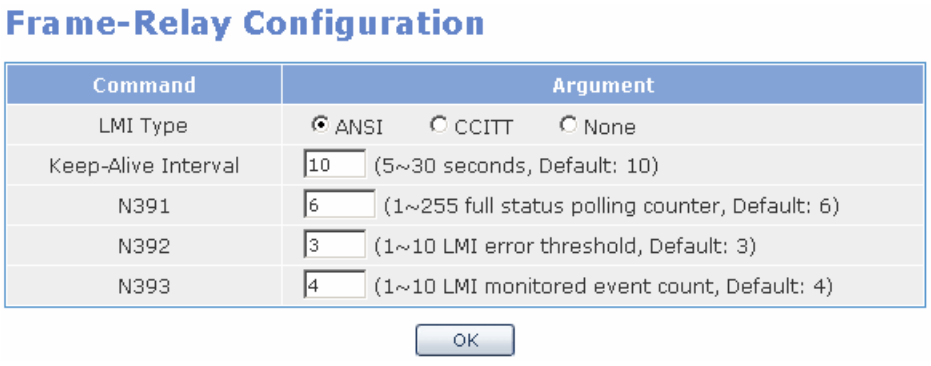
Parameter	Description
Keep-Alive Interval	Time interval to check Keep-Alive
Max Keep-Alive Count	Count of Keep-Alives to estimate as the disconnection
Authentication	Information for PPP authentication
IPCP Dynanmic	Use of Dynamic-IP function to support IPCP
IP Address	IP Address of the serial port
Gateway	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 GWIMT/GWIM 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 GWIMT/GWIM Frame Relay point-to-point with another GWIMT/GWIM without a DCE.



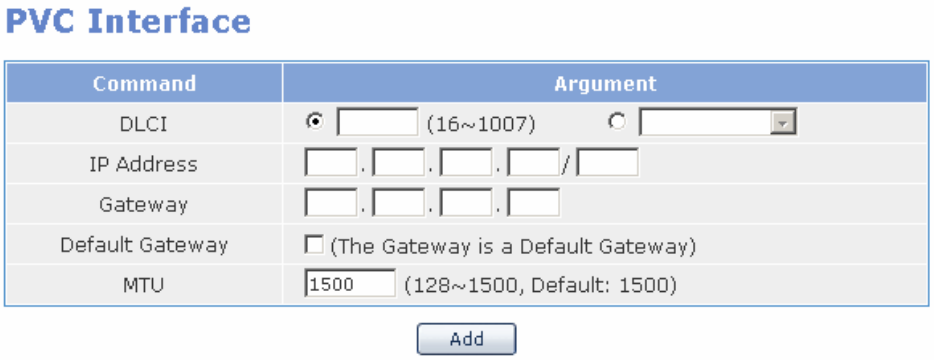
Frame Relay Parameters

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

Parameter	Description
N391	Cycle to request all status information. The information on all status is requested at every cycle specified in the N391 field. As usual, only Keep-Alive is exchanged.
N392	Count of Keep-Alives to estimate as the disconnection
N393	Buffer size to record success/failure of Keep-Alive. The value of N393 should be bigger than that of N392.

PVC Interface

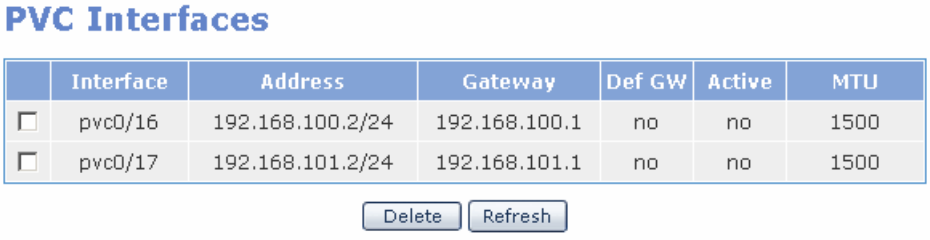
Select the Frame-Relay protocol to display the PVC Interface table. Enter the value of each field and press the Add button to create new PVC.



PVC Interface Parameters

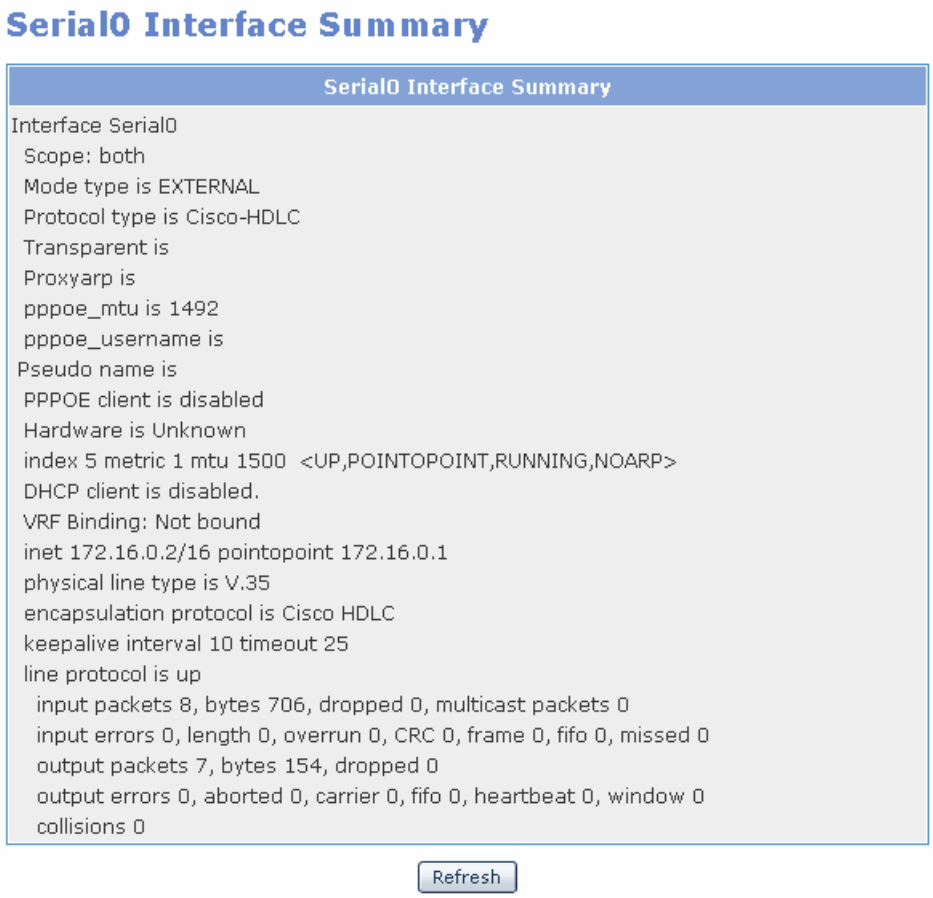
Parameter	Description
DLCI	Number of DLCI(a type of network address)
IP Address	IP Address to be used by PVC
Gateway	Gateway IP Address (Peer Address) of PVC
Default Gateway	Mark the check box to set this gateway to default gateway. (This item is displayed only if the WAN radio button is selected.)
MTU	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.



Serial Interface Summary

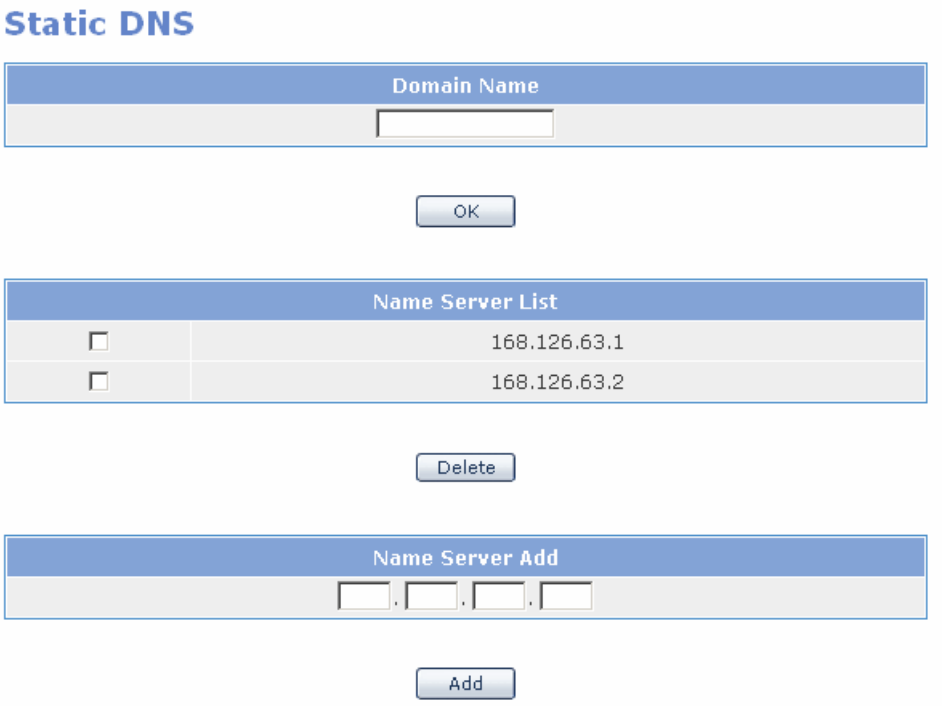
The Serial Interface Summary table briefly displays the current connection information of the serial port. The following is an example when the Serial connection is defined using the Cisco-HDLC protocol with an IP address of 172.16.0.2/16.



DNS

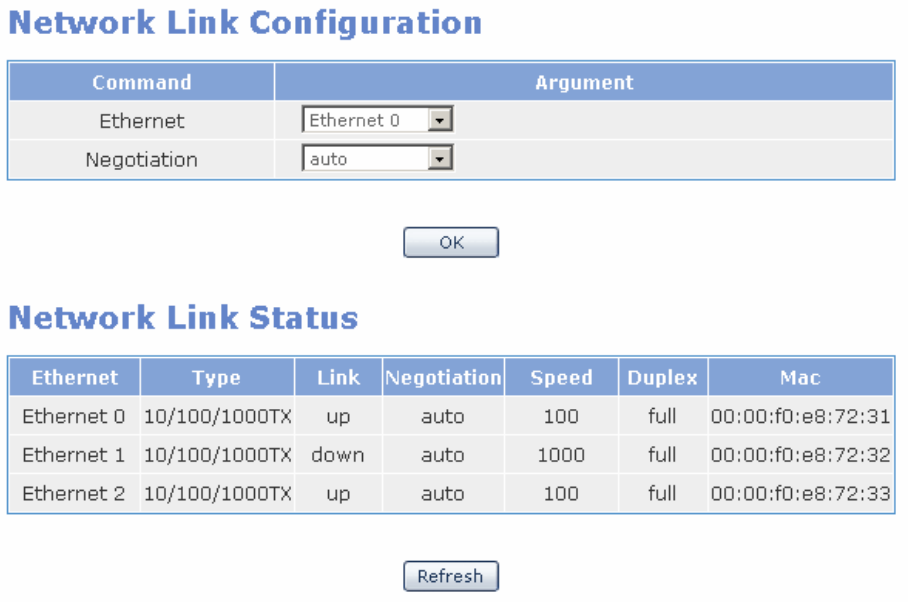
Select the [**Network**] → [**DNS**] submenu in order to display the following configuration window. Enter the domain name and the IP address information for the DNS server /s. Then click the OK button to store the domain name and the IP address information.

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.



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

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

Use the Negotiotion pull down menu to select **auto** or **force**.
If **auto** is selected the Ethenet 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

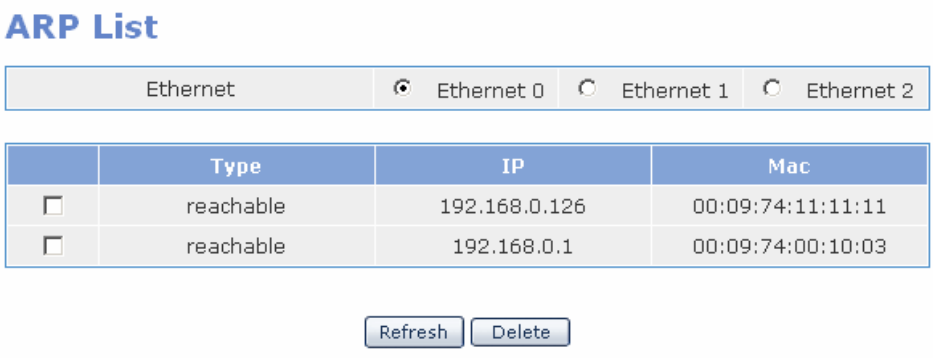
Field	Description
Ethernet	Logical name of each Ethernet Interface
Type	Type of Ethernet Connection
Link	Status is either **up** or **down**
Negotiation	Shows setup as auto or force mode
Speed	Transmission bandwidth of the corresponding Ethernet interface
Duplex	Transfer mode of the corresponding Ethernet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



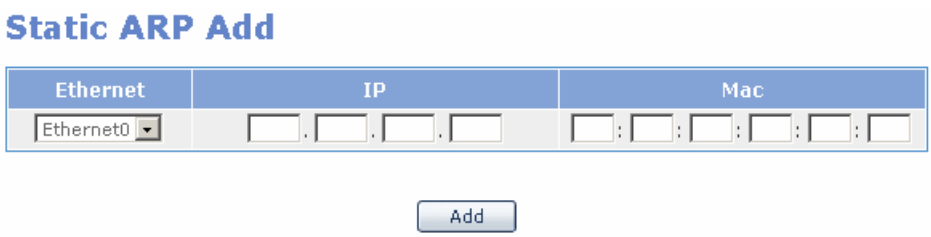
ARP List Fields

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 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 Leaset 600 sec. unit: sec.) to delete the unused ARP entries from the ARP table.

ARP Refresh

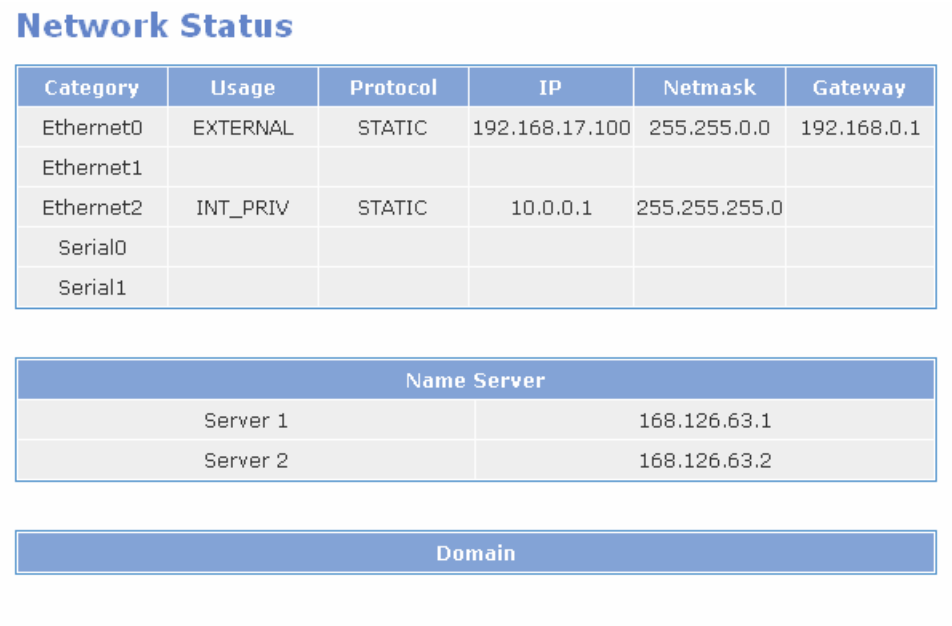
The ARP Refresh window is used to submit changed ARP information in the ARP table after route or a host information on the network has changed. The host or the route with the destination IP, the Mac with the current source IP is updated into the Ethernet Mac of the OfficeServ 7400 system.

ARP Refresh Paramenters

Field	Description
Ethernet	Used to select the Ethernet to be changed
Source IP	Used to select the IP address to be changed
Destination IP	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.

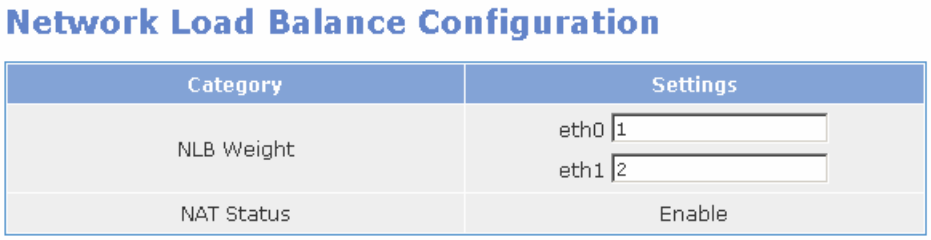


NLB

The GWIMT/GWIM 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

The Network Load Balance Configuration can be used when at leaset two of the GWIMT/GWIM 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 GWIMT/GWIM 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 Parameters

Parameter	Description
Source	Source IP address, netmask and port number of transfer session
Destination	Destination IP address, netmask and port number of transfer session
Traffic Distribution	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

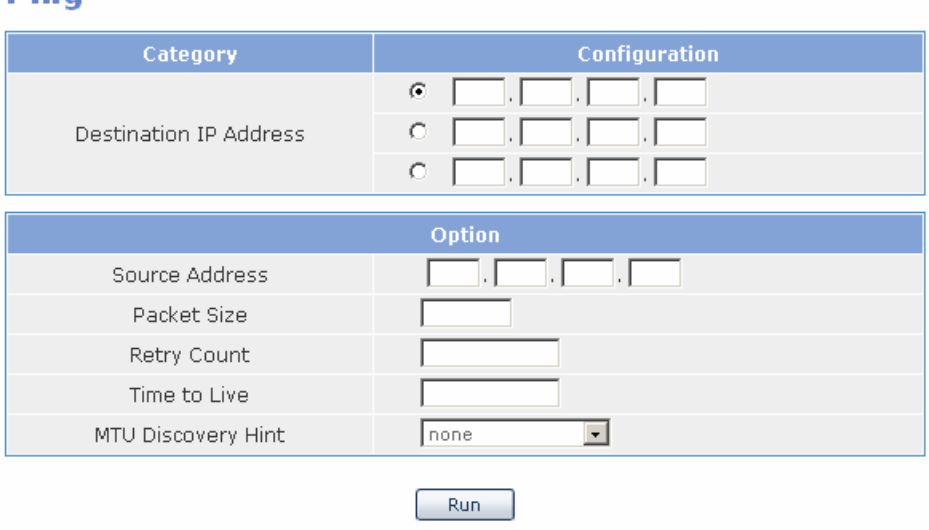
The Network Load Balance Management window is used for starting and stopping the NLB service.

Utility

The GWIMT/GWIM 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.



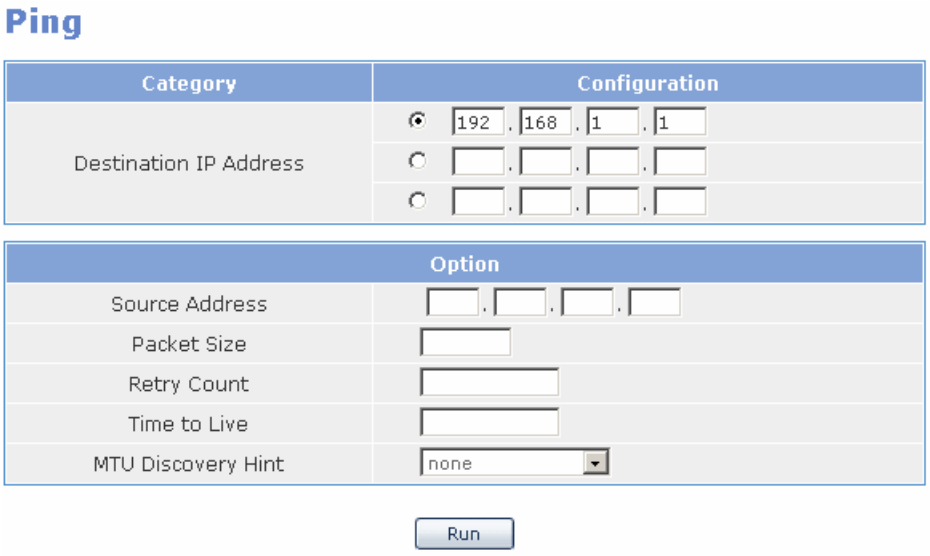
Ping Parameters

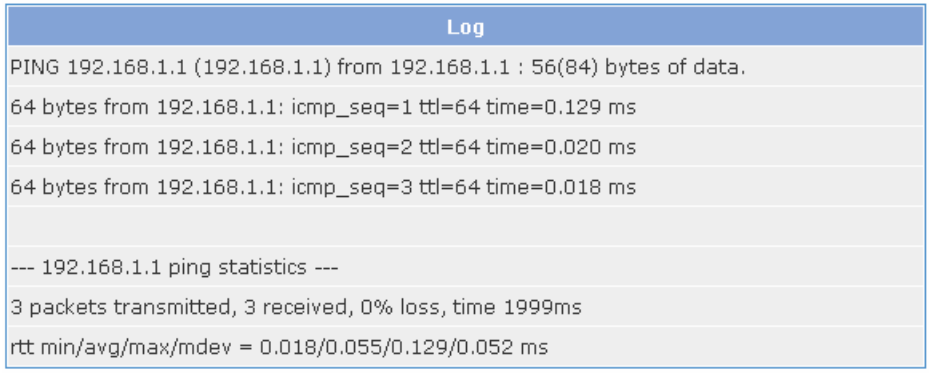
Parameter	Description
Destination IP Address	Used to enter the destination IP address for the Ping test
Source Address	Used to set the IP address of the interface for the Ping test
Packet Size	Used to set the packet size to be transmitted

Parameter	Description
Retry Count	Used to set the retry count. If it set to '0', there is no retry. Max is 3
Time to Live	Used to set the TTL value.
MTU Discovery Hint Selects the Path MTU Discovery method	None:
	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 exdeted 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.





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
NAT	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
Firewall	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
	ICMP Filtering	Used to block ICMP Reply (Ping, Tracert, etc.) of the GWIMT/GWIM Interfaces

NAT

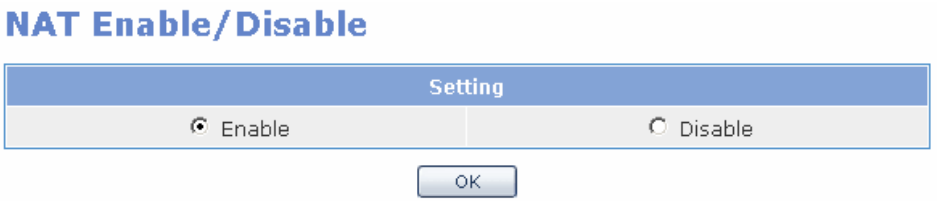
NAT (Network Address Translation) is an Internet standard that enables a local-area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. Select the **[NAT]** → [**Management**] submenu to begin configuring NAT.


NOTE

When a GWIMT/GWIM is initially installed data traffic from a LAN device will not be allowed 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 Parameter Description

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

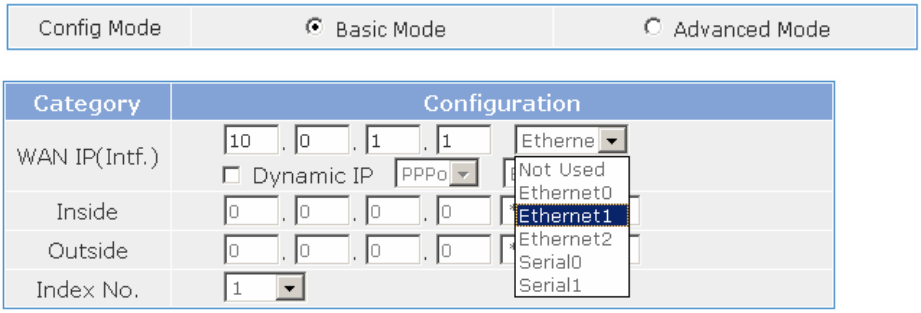
Configuration

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



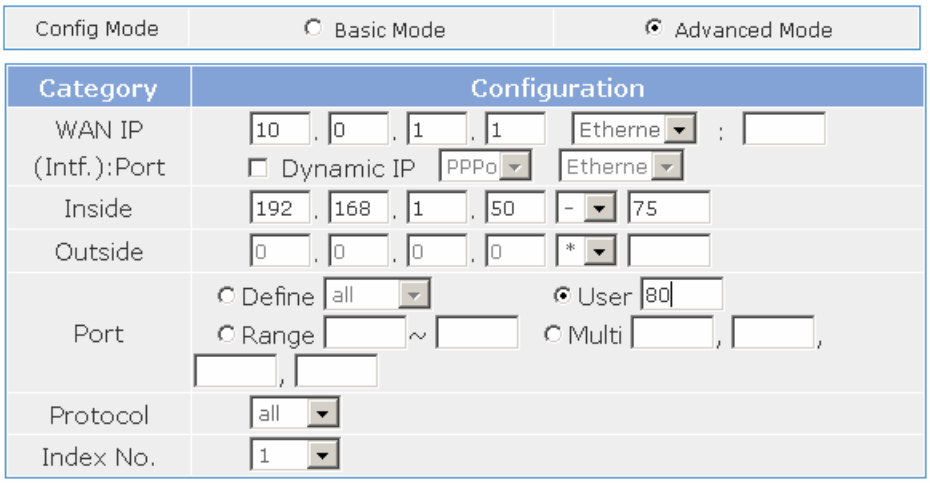
Basic NAT Parameter Description

Category	Description	
WAN IP	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).	
Inside	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 *****
Outside	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 *****
Index No	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.

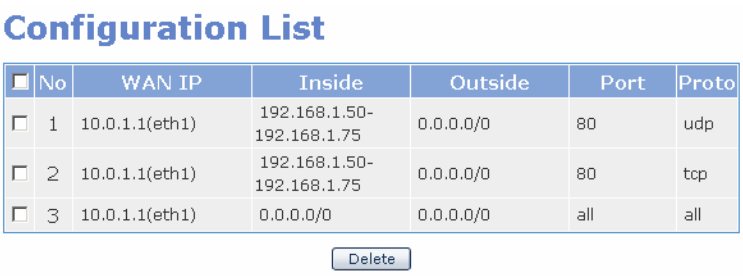
In this Advanced Mode example the WAN Interface field is set with an IP Address of 10.0.1.1, the Interface is being set to Ethernet1, and all Inside private IP Addresses in the defined range (192.168.1.50 thru 192.168.1.75) are being allowed out over the WAN interface to any destination over port 80 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.



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.



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.

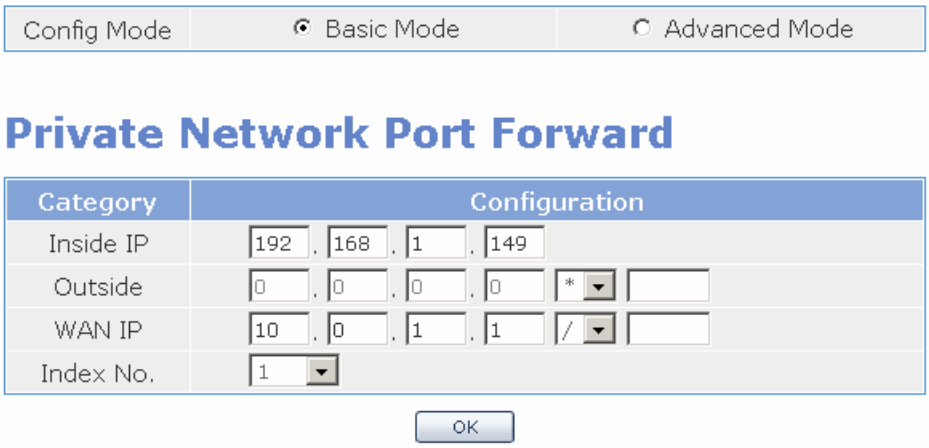
Port forwarding allows remote computers (e.g. public machines on The Internet) to connect to a specific computer within a private LAN.

The administrator can begin to configure the port forwarding feature on the GWIMT/GWIM 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



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.

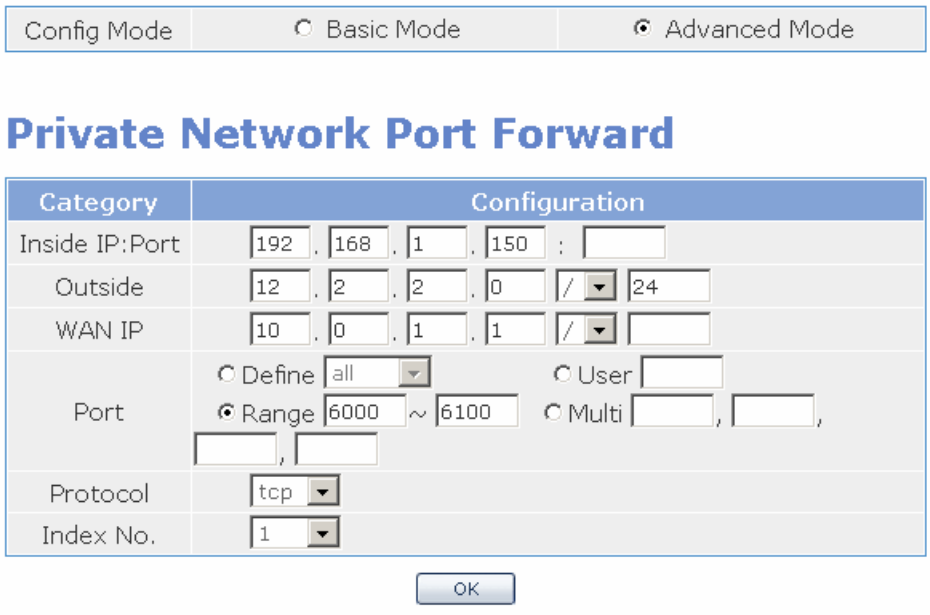
Basic Port Forward Parameter Description

Parameter	Description	
Inside IP	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	
Outside	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 *****
WAN IP	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
Index No	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.



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

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

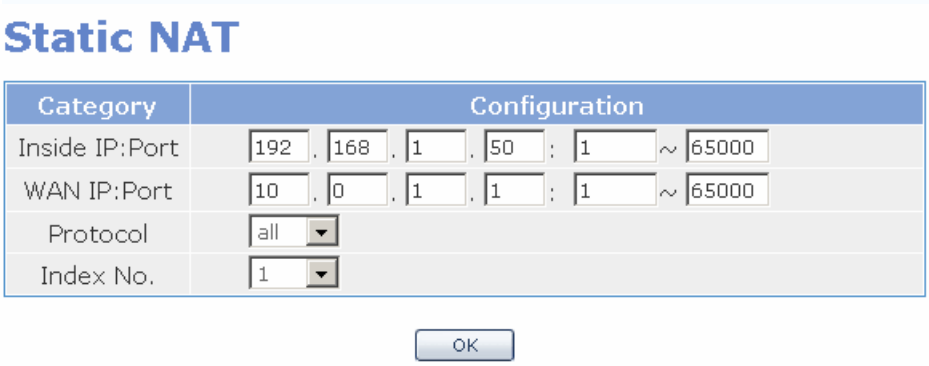
If a Port Forward rule must be deleted then check the box to the left of the rule and then click the delete button. In order to delete all Port Forward rules click on the box on the top left of the Configuration List then click on the delete button.

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 GWIMT/GWIM 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.



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 GWIMT/GWIM 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.

Firewall Parameter Description

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

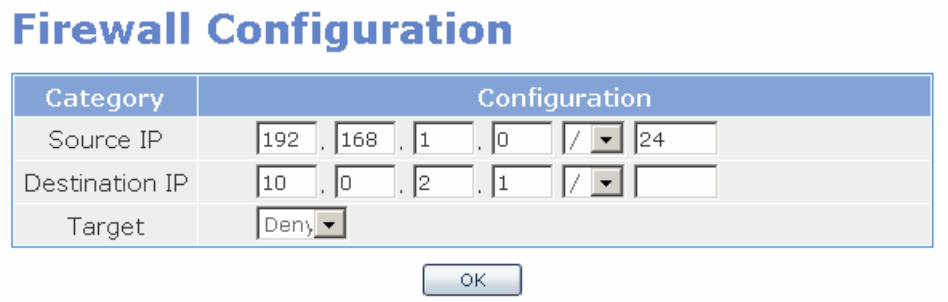
Configuration

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

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.



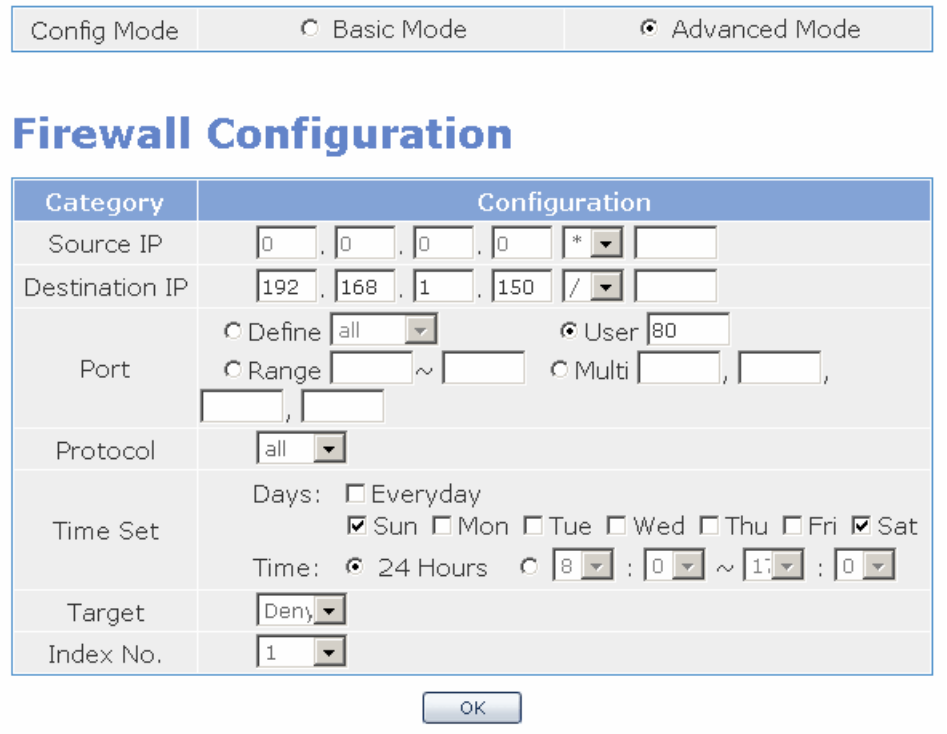
Basic Firewall Rule Parameter Description

Parameter	Description	
Source IP	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 *****
Destination IP	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 *****
Target	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.

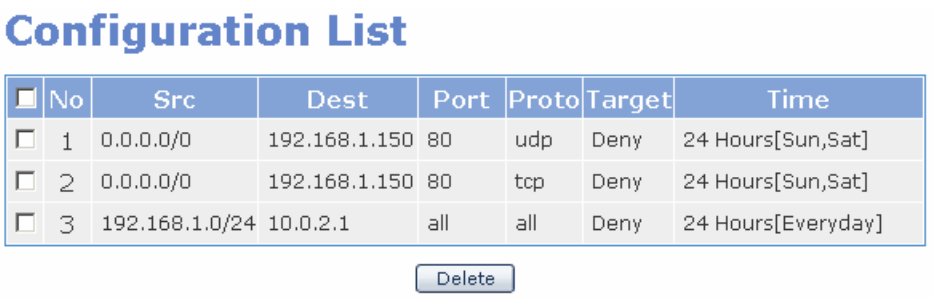
In this Advanced Mode example all Source IP Addresses are being denied access to IP Address 192.168.1.150 on port 80, Saturday and Sunday only.



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.



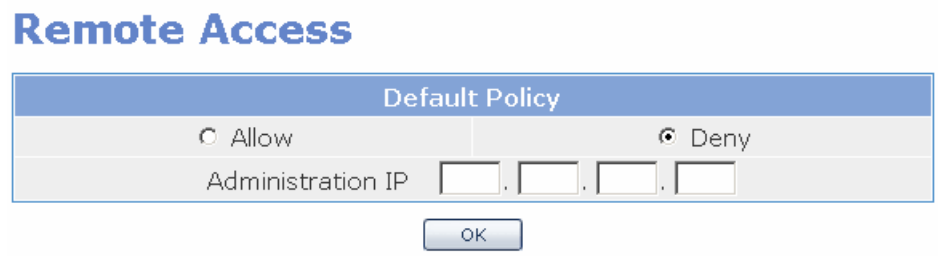
If a Firewall rule must be deleted then check the box to the left of the rule and then click the delete button. In order to delete all Firewall rules click on the box on the top left of the Configuration List then click on the delete button.

Remote Access

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

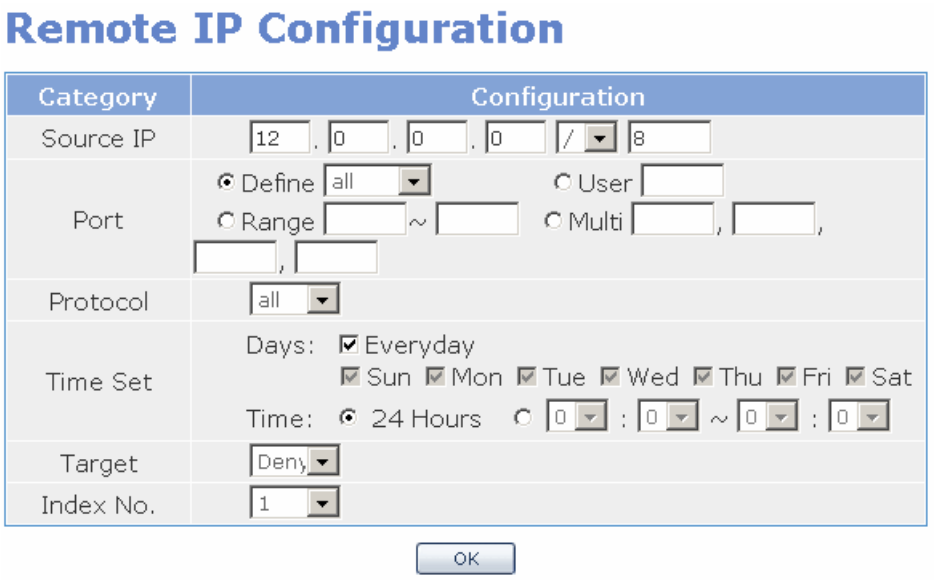
The first parameter is used to either enable or disable the Remote Access feature. Select the "Enable' or 'Disable" radio button and click on the OK button to set.

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 GWIMT/GWIM unless the computer has this IP Address.

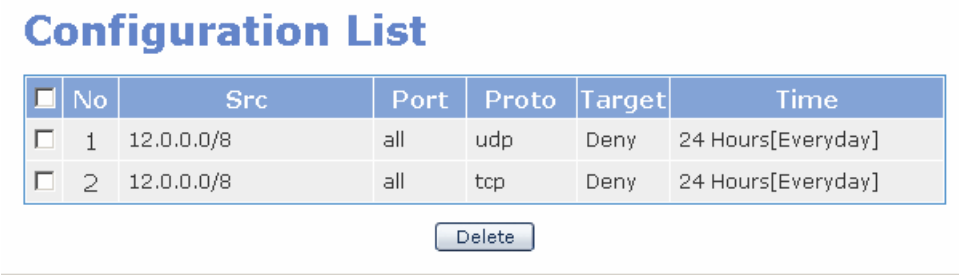


When the Allow radio button is selected then the administrator can set up the Remote Access policy. If Allow is selected and a policy is not defined then everyone will have Remote Access to the GWIMT/GWIM.

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



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.

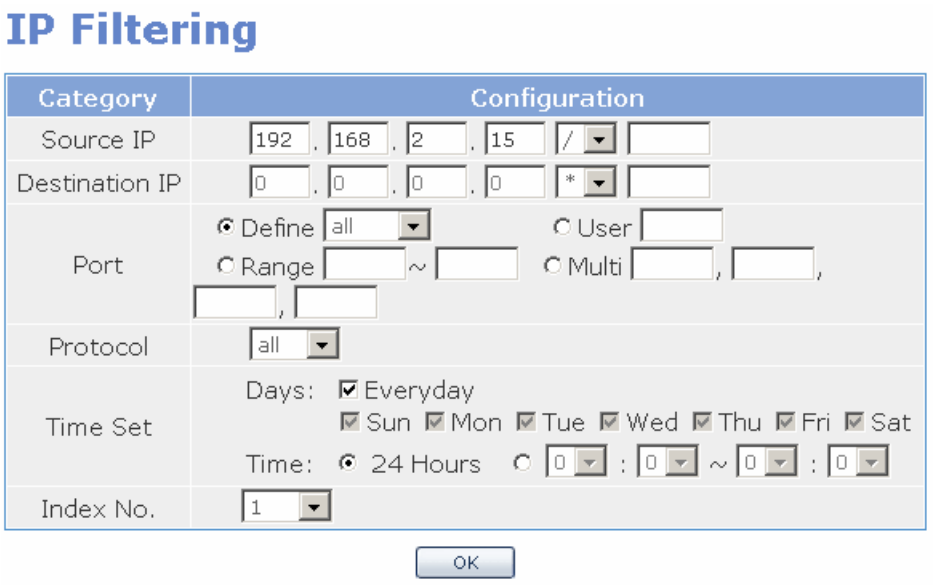


If a Remote Access rule must be deleted then check the box to the left of the rule and then click the delete button. In order to delete all Remote Access rules click on the box on the top left of the Configuration List then click on the delete button.

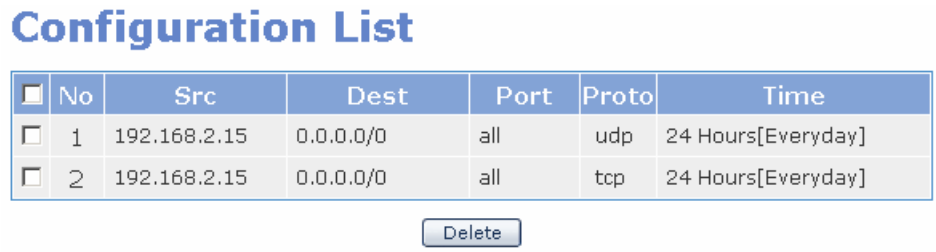
IP Filtering

The GWIMT/GWIM 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.



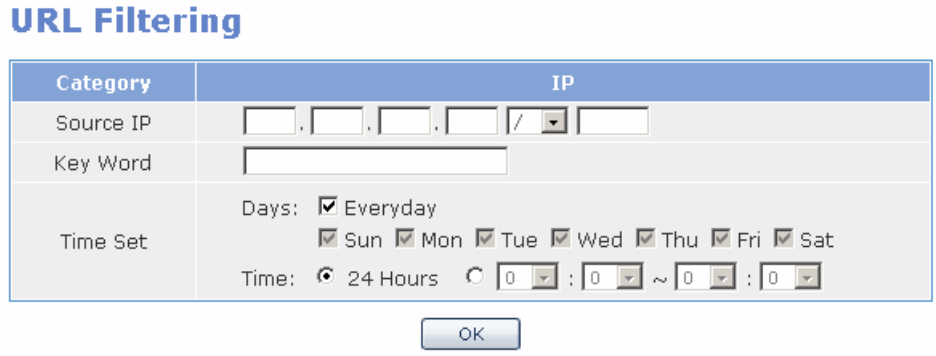
The administrator can view the current status of the IP Filtering rules by using the [**Firewall**] → [**Firewall**] → [**IP Filtering**] submenu. The Configuration List is shown on the bottom of the window.



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

Administrator can deny web access to PCs connected to the system using the [**Firewall**] → [**Firewall**] → [**URL Filtering**] submenu. Once the data is entered click the OK button to save.



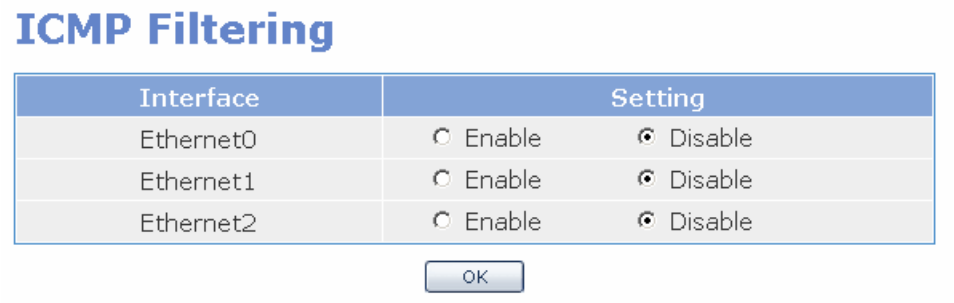
In the example listed below LAN users with an IP Address 192.168.2.15 thru 20 are not allowed to view any website 7 days a week, 24 hours a day with the word myspace in the website name.

URL Filtering Parameter Description

Parameter	Description	
Source IP	To set the originating IP. Address	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
		The **–** is used to specify a range of IP Addresses to be restricted from accessing a web site Example: 192.168.1.50 **-** 60
		The ***** symbol is used to deny all LAN IP Addresses from accessing a web site Example: 0.0.0.0 *****
Keyword	To enter the keyword of the site to deny.	
Time Set	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.



Router

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

Router Menu Submenu Description

Menu	Submenu	Description
General	Routes	Used to display the routing table of GWIMT/GWIM.
	Management	Used to start or stop RIP, OSPF, and BGP.
Configuration	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.
	BGP	Used to set up BGP.

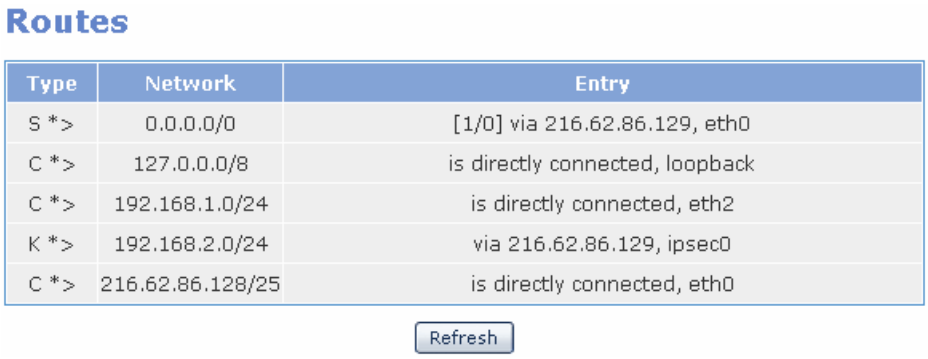
Menu	Submenu	Description
List	Access List	Used to set up Access-lists.
	Prefix List	Used to set up Prefix-lists.
	Route Map	Used to set up Route-maps.
	As Path List	Used to set up BGP AS-path lists.
	Community List	Used to set up BGP Community-lists.
	Key Chain	Used to set up the key used for authentication of RIP v2.
Status	RIP	Used to display RIP network information.
	OSPF	Used to display OSPF Neighbor information.
	BGP	Used to display the Neighbor status connected with the BGP network 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 GWIMT/GWIM.

Routes

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

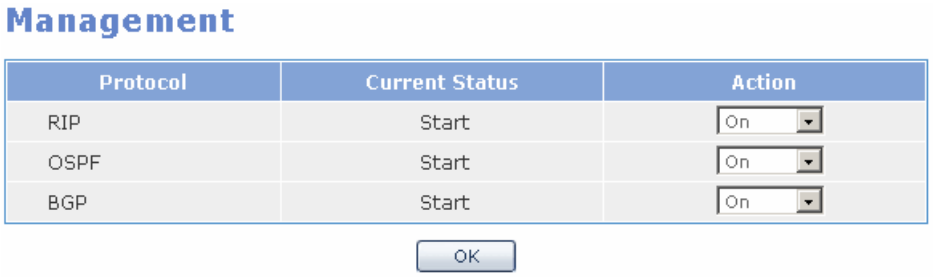


Routes Window Field Description

Item	Description
Type	- C: Network directly connected to GWIMT/GWIM network interface - S: Static network set by a administrator - R: Path information received from another router via RIP - O: Path information received from another router via OSPF protocol - B: Path information received from another router via BGP - K: Path information set by system kernel * >: Whether to have activated routing table
Network	Network/Netmask information of route
Entry	Route information

Management

In order to turn the GWIMT/GWIM routing protocols on or off select the [**Router**] → **[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.



Configuration

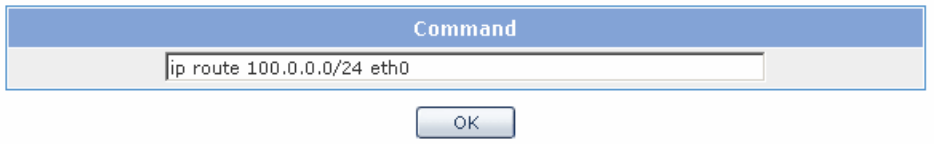
In order to configure static routes, and set up the routing protocols RIP, OSP, and BGP the system administrator will use the **[Router]** → **[Configuration]** submenu.

Static Route

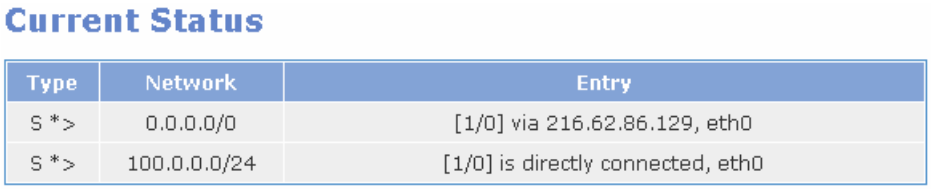
Static routes are entered into the GWIMT/GWIM by the system administrator. An entire network can be configured using static routes but this type of configuration is not fault tolerant. When there is a change in the network or a failure occurs between two statically defined nodes, traffic will not be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

Static routes are set by using the Command line.

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.



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



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

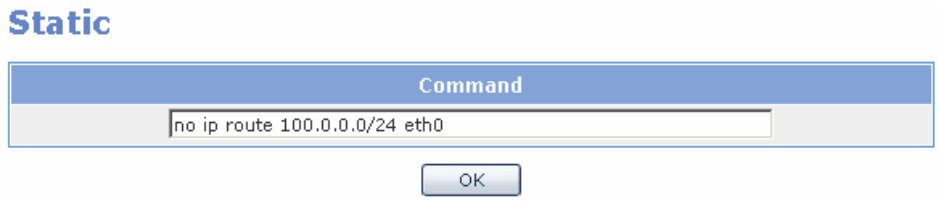
Current Status Parameter Description

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 whet the correct command is to remove the static route that was just entered they would selet “no ip route” and then select the appropriate argument.

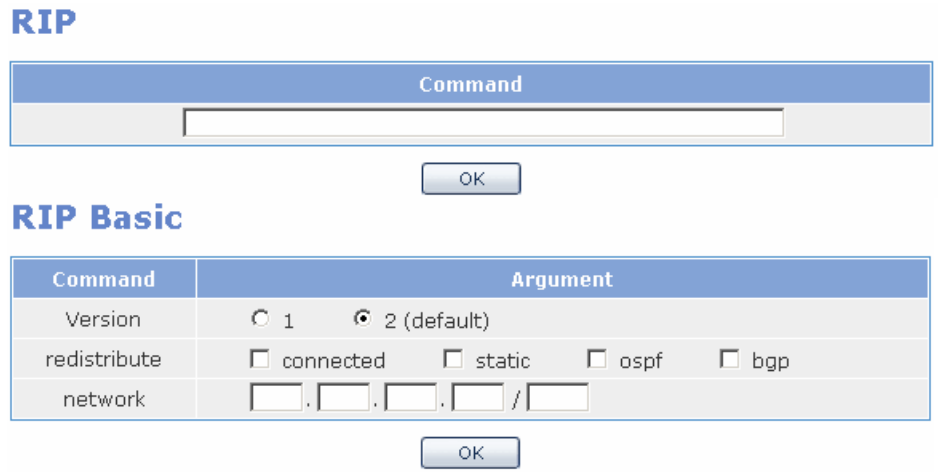
Then at the command line the following command must be typed in. Then click the OK button to submit the change.



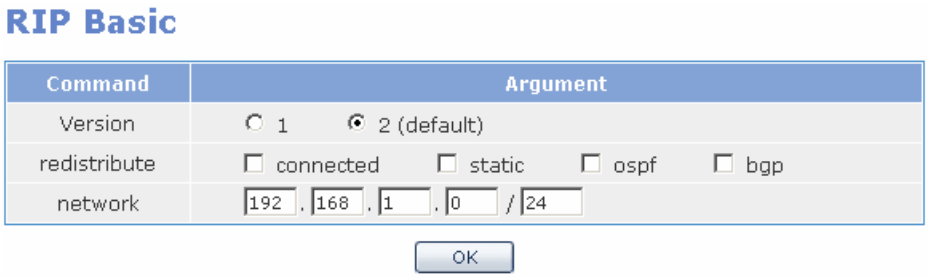
RIP

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 **[Router] →[Configuration] → [RIP]** submenu to begin configuring RIP.

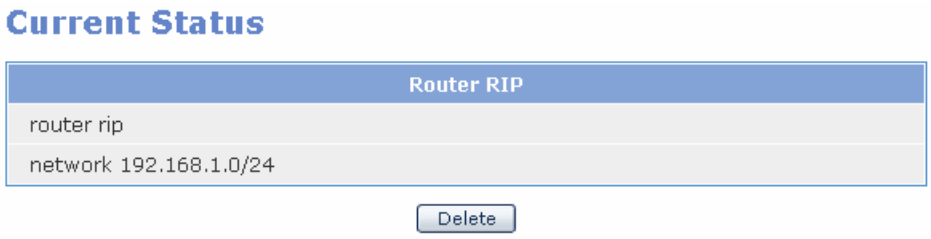
On the GWIMT/GWIM the RIP information (basic and advanced commands)can be entered by using the Command field or by using the RIP Basic fields (basic commands only).



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



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 **[Router] → [Configuration] → [RIP]** submenu.



Help

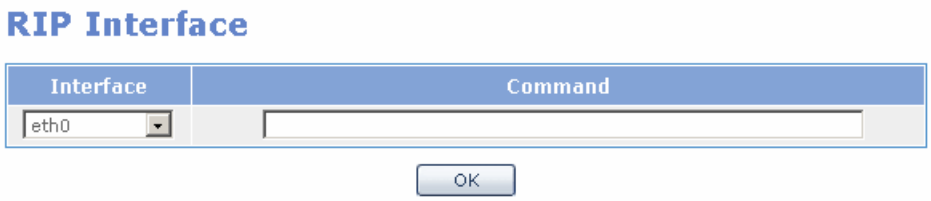
If a system administrator is unsure which RIP commands to use in the Command field then they may use the Help Command pull down menu to see all possible choices. Once a command is selected the Argument pull down menu will be populated with the appropriate choices. Once the correct RIP command is identified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

RIP Interface

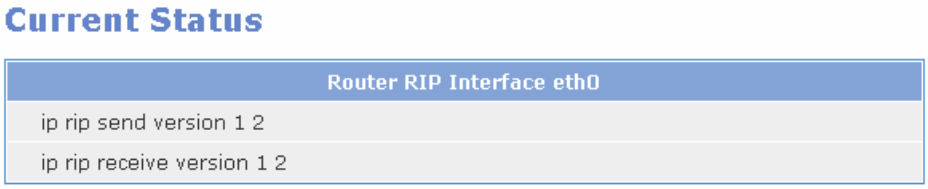
The **[Router] → [Configuration] → [RIP Interface]** submenu is used to select the Interfaces which will use RIP, to apply advanced RIP functionality, and to select the send and receive RIP settings per Interface.

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.



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

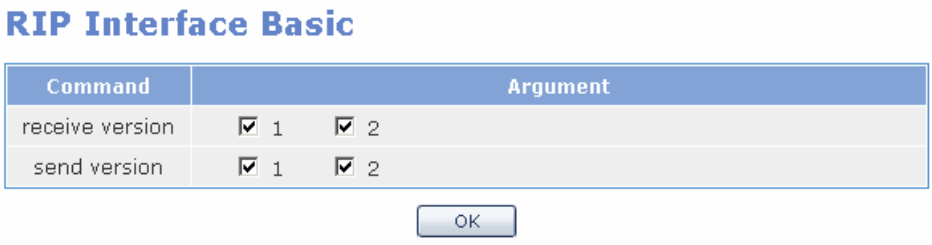


Help

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

RIP Interface Basic

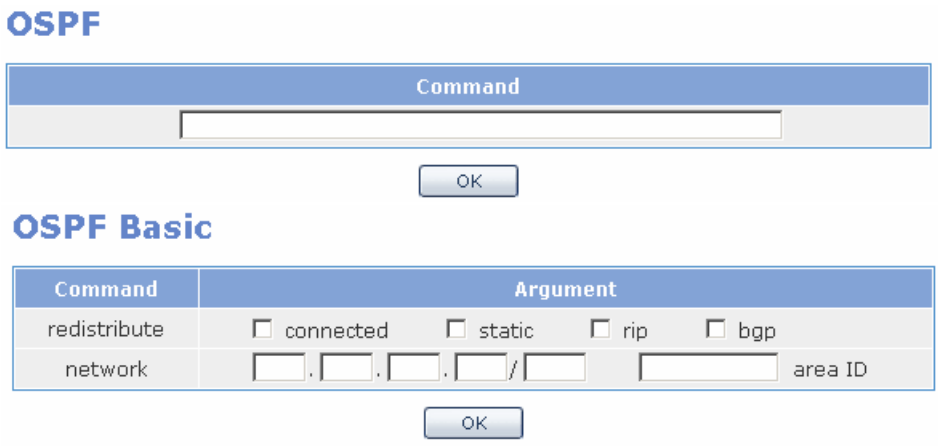
The RIP Interface Basic fields are used to set the Interface to send and/or receive RIP Versions 1 and 2. After selecting each item click the OK button to submit the change. The applied value will be displayed in the <**Current Status**> window.



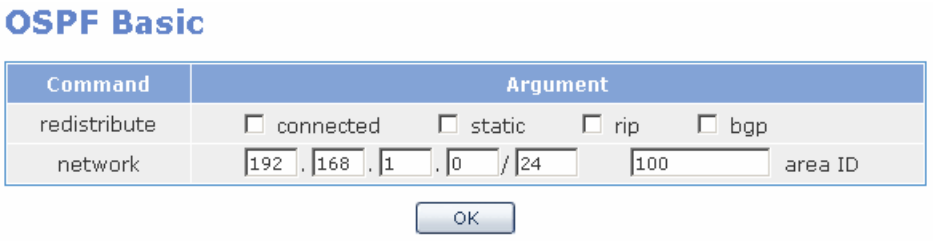
OSPF

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 [**Router**] → [**Configuration**] → [**OSPF**] submenu to begin configuring OSPF.

On the GWIMT/GWIM 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).



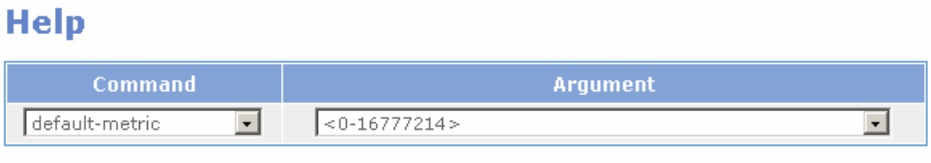
In the Command field and OSPF Basic examples listed below the network administrator is setting the 192.168.1.0 network for OSPF with an area of 100. Click the OK button to apply the change.



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

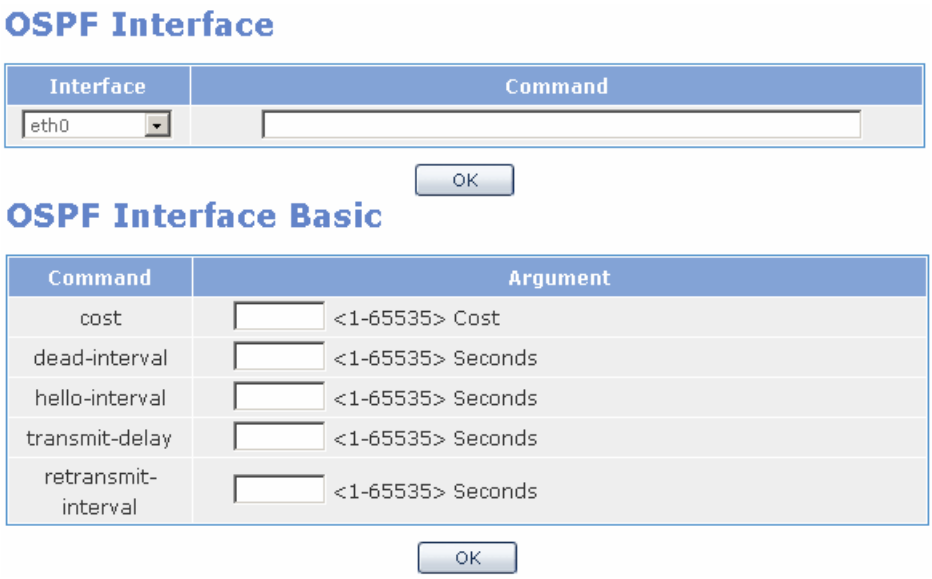
Help

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



OSPF Interface

The **[Router] →[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 advance OSPF configuration commannds and the OSPF Interface Basic fields may be used to enter Basic OSPF configuration commands.



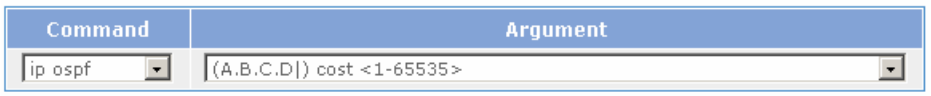
Select the target interface and then enter the OSPF configuration command using the Command field or OSPF Interface Basic fields.


NOTE

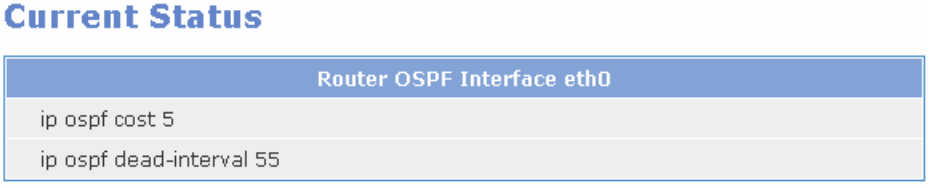
If a WAN Interface is set up to work through a VPN Tunnel then it will not be possible to send routing updates through it. This includes RIP, OSPF and BGP.

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



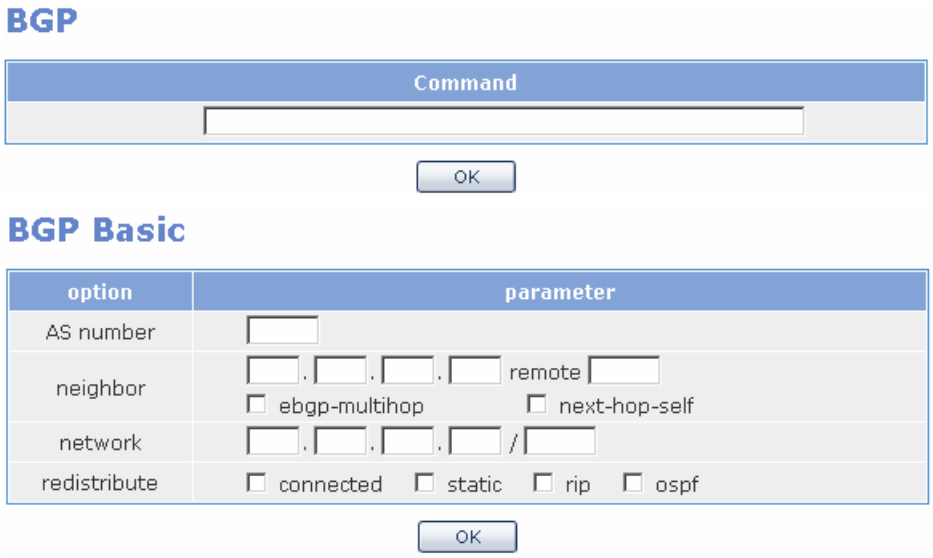
Once an OSPF configuration command is successfully applied the results will be displayed in the **[Router] → [Configuration] → [OSPF Interface] <Current Status>** window



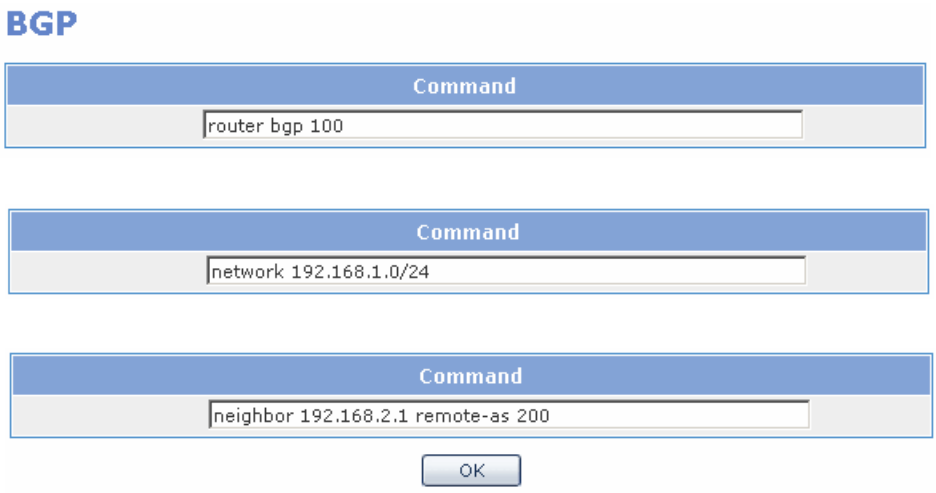
BGP

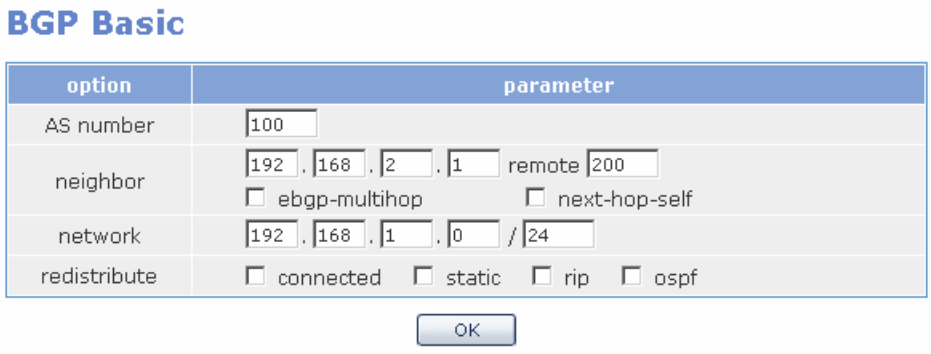
BGP is the core routing protocol of The Internet. It works by maintaining a table of IP networks or 'prefixes' which designate network reachability among autonomous systems (AS). It is a path vector protocol which does not use traditional IGP metrics, but makes routing decisions based on path, network policies and/or rule sets.Select the **[Router]** → **[Configuration]** → **[BGP]** submenu to begin configuring BGP.

On the GWIMT/GWIM the BGP information (basic and advanced commands)can be entered by using the Command field or by using the BGP Basic fields (basic commands only).

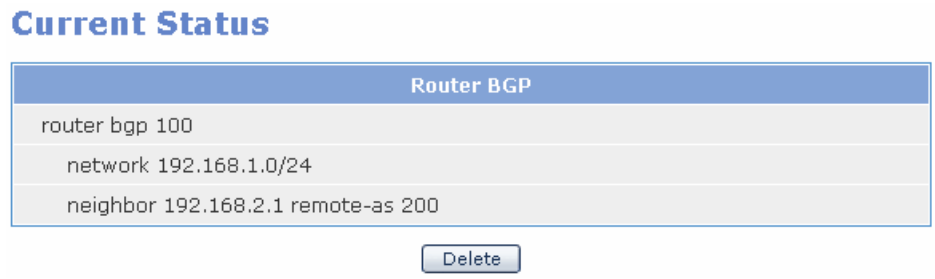


In the Command fields and BGP Basic field examples listed below the network administrator is setting the 192.168.1.0 network for BGP with an area of 100. The neighbor has an IP Address of 192.168.2.1 and has a remote AS of 200. Click the OK button to apply the change. When using the Command field several entries will need to be entered to set up this configuration. Click the OK button after each entry.





Once the entered command/s are successfully executed, the BGP configuration is directly applied to the **[Router] → [Configuration] → [BGP]**. <**Current Status**> window.



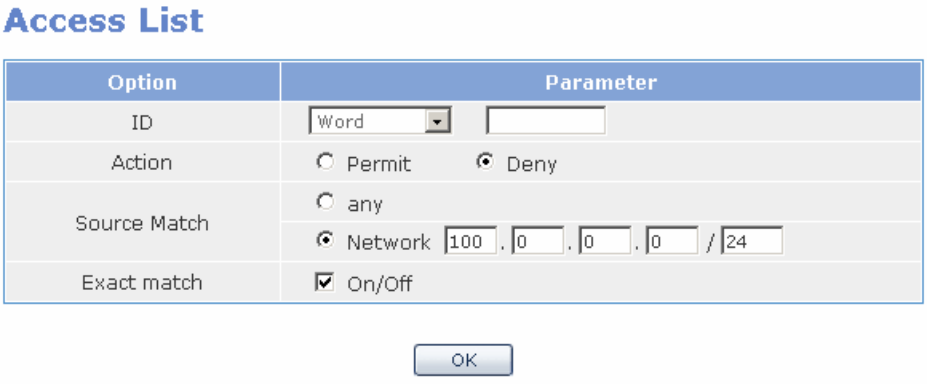
Help

If a system administrator is unsure which BGP commands to use then they may use the Help Command pull down menu to see all possible choices. Select the Command field and select the BGP entry and then the Argument field entry. Once the correct BGP command is identified then type it into the Command field and click on the OK button to submit the change

List

Access List

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



Access List Parameters

Item	Description	
ID	Used to set the Access-list name.	1~99: Standard Access List
		100~199: Extended Access List
		1300~1999: Standard Access List
		2000~2699: Extended Access List
		Word: Named Access List
Action	Used to allow or reject the packet matched.	
Source Match	Sets the match condition. Any - All packets Host - A host Network - Network range	
Destination Match	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	
Exact match	Available when ID is set to word and when match condition is set to Network. Sets only the packets matched correctly with the prefix.	

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

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

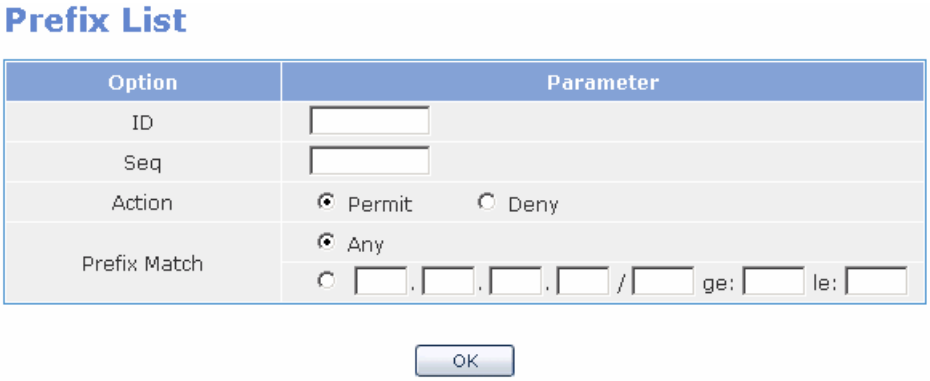
Current Status Fields

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 **[Router] → [List] → [Prefix List]** submenu to configure the Prefix-list.

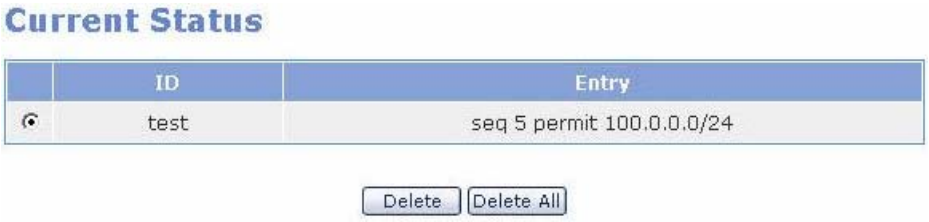
If no Prefix List is specified on the GWIMT/GWIM then it acts as a permit rule. If the Prefix List is defined, and no match is found, then a default rule of deny is applied.



Prefix List 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 **[Router] → [List] → [Prefix List] <Current Status>** window.



Once a Prefix List is set in the GWIMT/GWIM 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

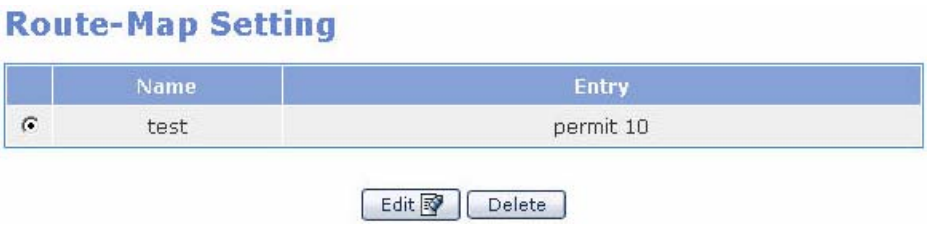
Route maps are similar to access lists as they both have criteria for matching the details of certain packets and an action of permitting or denying those packets. Use the **[Router] → [List] → [Route-Map]** submenu to begin configuring Route-Map.

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

Route-Map Parameter Description

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

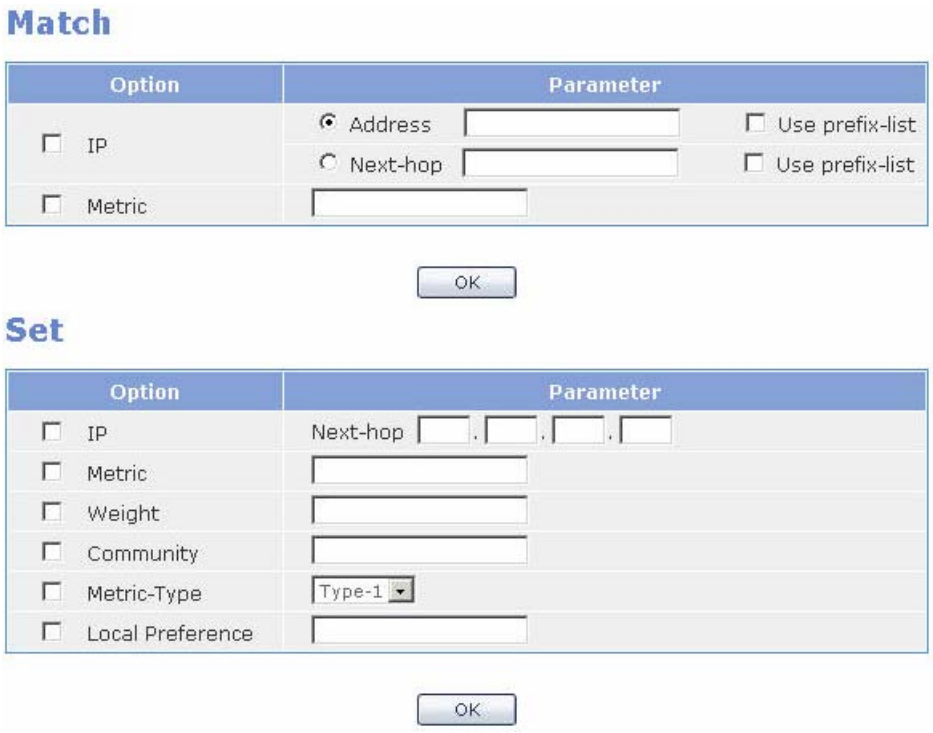
If the Route-Map command is successfully entered and saved then the results will be directly applied to the <**Current Status**> of the **[Router] → [List] → [Route-Map]** submenu.



Route-Map Setting Field Description

Field	Description
Name	Route-map name
Entry	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.



Route-Map Match Parameter Description

Parameter	Description
IP	- 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.
Metric	Used to set the Metric to be matched.

Route-Map Set Parameter Description

Parameter	Description
IP	Used to set the next-hop of the BGP table.
Metric	Used to set the metric of the BGP table.
Weight	Used to set the weight of the BGP table.
Community	Used to set the community of the BGP table.
Metric-Type	Used to set the metric type of the BGP table. - Type 1: External Type 1 - Type 2: External Type 2
Local Preference	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 **[Router] → [List] → [Route-Map]** submenu .

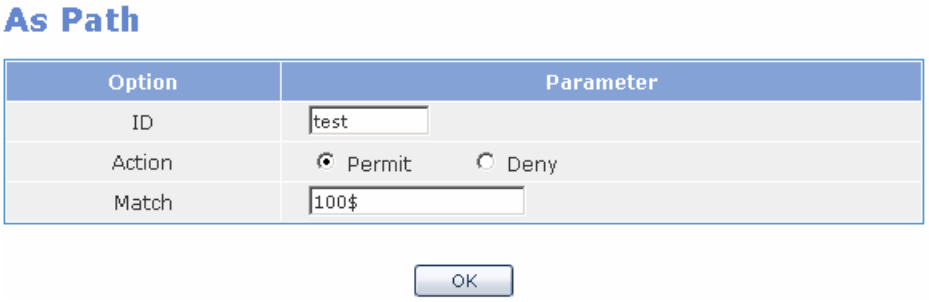
Current Status Field Description

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

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

As Path List

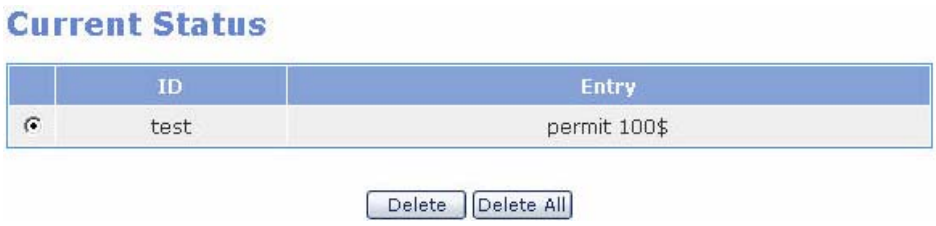
Select the **[Router] → [List] → [As Path List]** submenu to begin configuring the AS Path access-list entries for the GWIMT/GWIM BGP. Enter the target values and then click the Save button.



AS Path List Parameter Description

Parameter	Description
ID	Usd to set the AS Path access-list name.
Action	Used to set the system to allow/reject if a BGP route information exists that meets the match condition.
Match	Used to set the match condition.

Once the AS Path command is successfully entered and saved then the results will be directly applied to the <**Current Status**> of the **[Router] → [List] → [As Path List]** submenu.



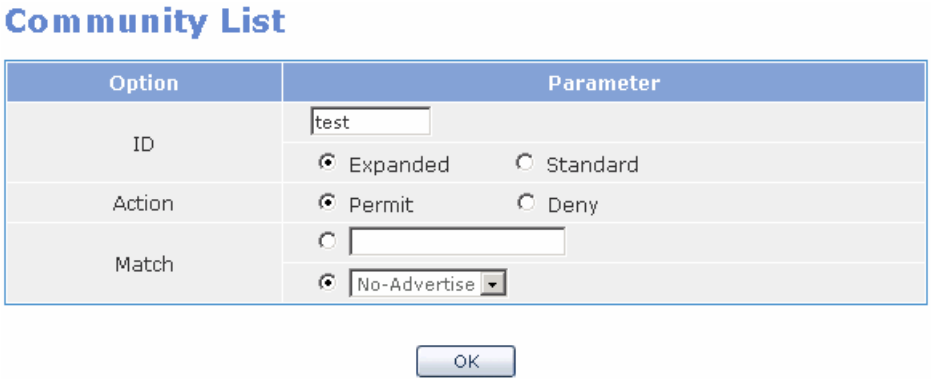
Current Status Field Description

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

In order to delete an AS Path entry click the radio button to the left of the AS Path rule and then click the Delete button. Click the Delete All button to remove all AS Path entries from the GWIMT/GWIM at the same time.

Community List

Select the **[Router] → [List] → [Community List]** submenu to begin configuring the Community List of the GWIMT/GWIM BGP. Set the target values and then click the Save button.



Community List Parameter Description

Parameter	Description
ID	Used to set the Community list name Expanded - When a normal community list is set Standard - When community list with a selected format is set
Action	Used to set whether to allow/reject the community that is matched
Match	No-Advertise - Do not distribute path to the neighbor router No-Export - Do not distribute path to an external neighbor router Local-AS - Do not distribute path to the neighbor router of the lower AS located at BGP combination network. In other cases, set normally to community list.

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

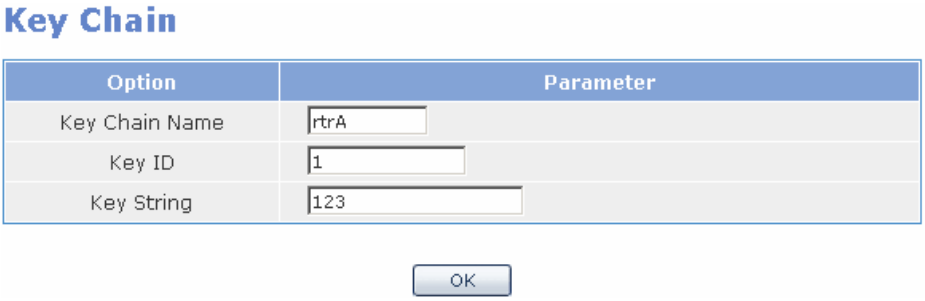
Current Status Field Description

Field	Description
ID	Community list name
Entry	Community list information

In order to remove a Community List entry click the radio button to the left of the Community List rule and then click the Delete button. Click the Delete All button to remove all community-list entries at the same time.

Key Chain

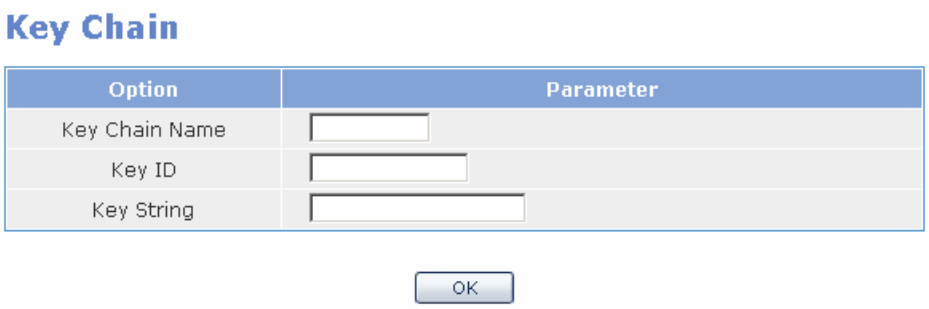
The GWIMT/GWIM uses the Key Chain window for setting up MD5 Authentication for (RIP) Version 2 packets. Select the **[Router] → [List] → [Key Chain]** submenu to begin configuring the Key Chain information. Enter the values and then click the OK button.



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 **[Router] → [List] → [Key Chain]** submenu.

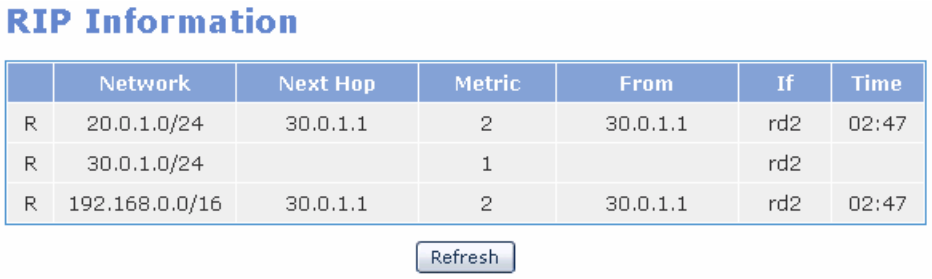


In order to remove a Key Chain entry click the radio button to the left of the Key Chain rule and then click the Delete button. Click the Delete All button to remove all Key Chain entries at the same time.

Status

RIP

The **[Router] → [Status] → [RIP]** submenu is used to display the RIP connection status and information of the GWIMT/GWIM.

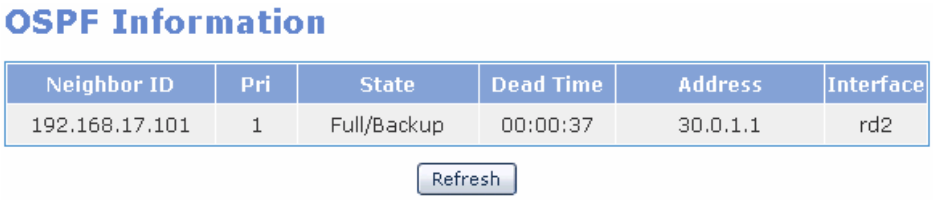


RIP Status Field Description

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 **[Router]** → **[Status]** → **[OSPF]** submenu is used to display the OSPF connection status and information of the GWIMT/GWIM.

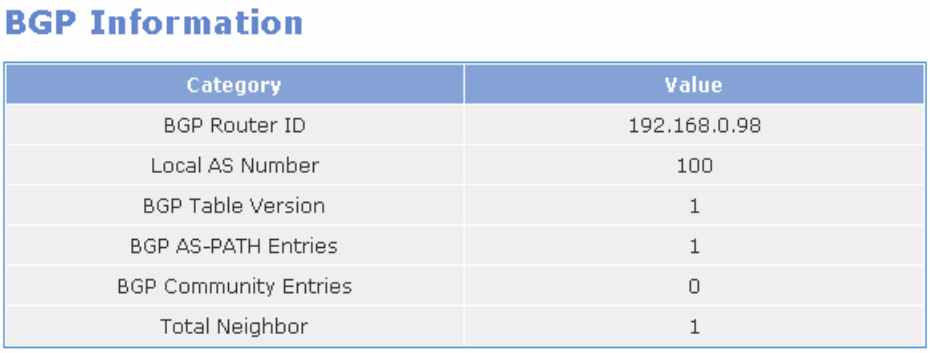


OSPF Status Field Description

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

BGP

The **[Router]** → **[Status]** → **[BGP]** submenu is used to display the BGP connection status and information of the GWIMT/GWIM.



BGP Information Field Description Part 1

Field	Description
BGP Router ID	Current system router-ID Sets to the IP address that is the highest in the IPs set in loopback when an address or a loopback that is the highest from the IP addresses is used.
Local AS Number	Local AS No. set by a administrator

Field	Description
BGP Table Version	BGP table change version information
BGP AS-PATH Entries	Number of AS PATH Hash tables used in BGP
BGP Community Entries	Number of Hash table of community attribute used in BGP
Total Neighbor	Total sum of BGP neighbor

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
192.168.0.1	4	100	0	0	0	0	0	never	Idle

BGP Information Field Description Part 2

Field	Description
Neighbor	IP address of the neighbor router
V	Version No. used by neighbor
AS	AS No. of neighbor
MsgRcvd	Message number received from neighbor
MsgSent	Message number sent from neighbor
TblVer	Latest BGP database version sent from neighbor
InQ	Number of messages that should be received from neighbor and processed
OutQ	Number of messages sent to neighbor
Up/Down	Displays the path time when BGP session is finished. Displays the status when BGP session is not finished.
State/PfxRcd	Number of BGP routes via neighbor or peer group or BGP current status

Network	Nexthop	Metric	LocalPrf	Weight	Path
*> 100.0.0.0/24	0.0.0.0			32768	i

Refresh

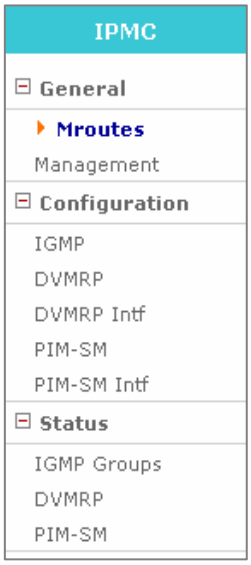
BGP Information Field Description Part 3

Field	Description
Network	Displays network information. Status code information s - Indicates the suppressed network. * - Indicates proper network information.

Field	Description
	h - BGP dampening is activated. > - best route i - Indicates the network entered by IBGP.
Nexthop	Nexthop address of the BGP route sent from neighbor
Metric	MED value of BGP neighbor
LocalPrf	Local Preference. Default is 100.
Weight	Weight allocated in prefix - Local route default is 32768. - The default of the sent route is 0.
Path	Displays the list of AS path that should be passed to go to the network corresponding to the prefix. Origin code information i - Information received by the network command e - Information received via EGP ? - Information received by redistribution

IPMC

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

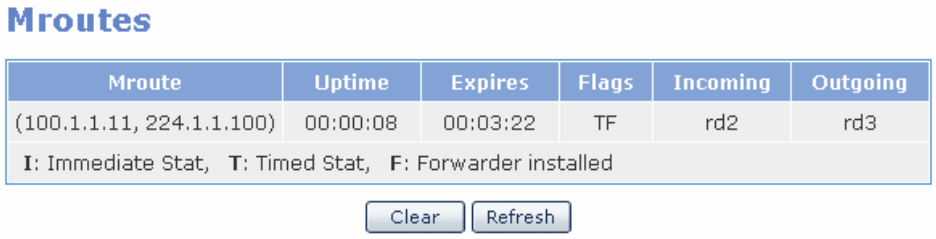
Menu	Submenu	Description
General	Mroutes	Displays the Multicast Routing Entry.
	Management	Used to starts/stop IPMC protocol daemons.
Configuration	IGMP	Used to display or change the IGMP configuration.
	DVMRP	Used to display or change the DVMRP default configuration.
	DVMRP Intf	Used to display or change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

Menu	Submenu	Description
	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.

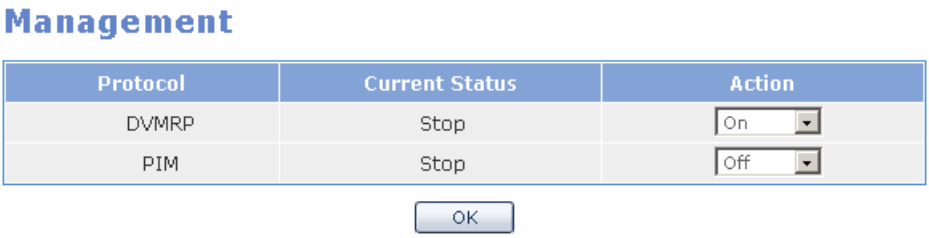


Mroute Field Description

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.



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

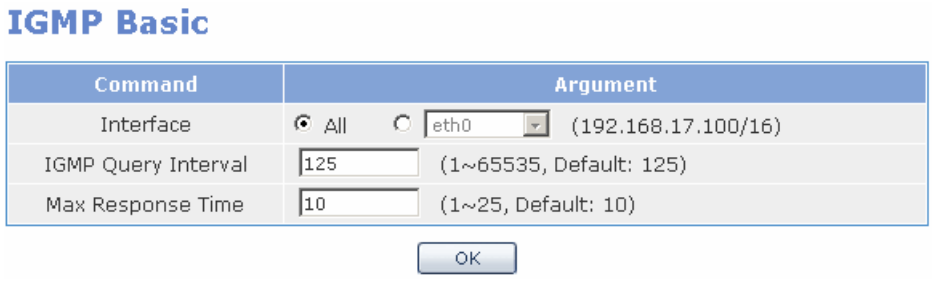
The Internet Group Management Protocol is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. The **[IPMC] → [Configuration]** submenu is used to display and change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

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

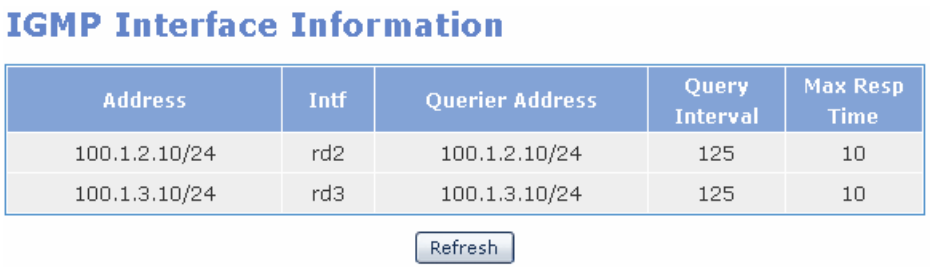


IGMP Basic Parameter Description

Parameter	Description
Interface	Select the target IGMP interface and select All. Then, all interface configuration values are applied
IGMP Query Interval	Cycle of sending IGMP Membership Query
Max Response Time	Maximum time of waiting a response after sending Membership Query

IGMP Interface Information

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



IGMP Interface Field Description

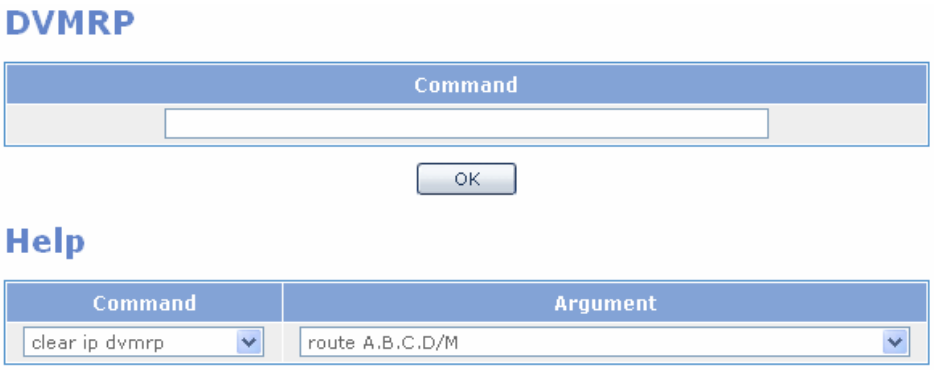
Field	Description
Address	IGMP group address
Intf	IGMP interface name
Querier Address	IP address of IGMP interface that sends membership query. IP address of Designate Router(DR)
Query Interval	Cycle of sending Membership Query
Max Resp Time	Maximum time of waiting a response to Membership Query

Configuration / DVMRP

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 GWIMT/GWIM DVMRP configuration.

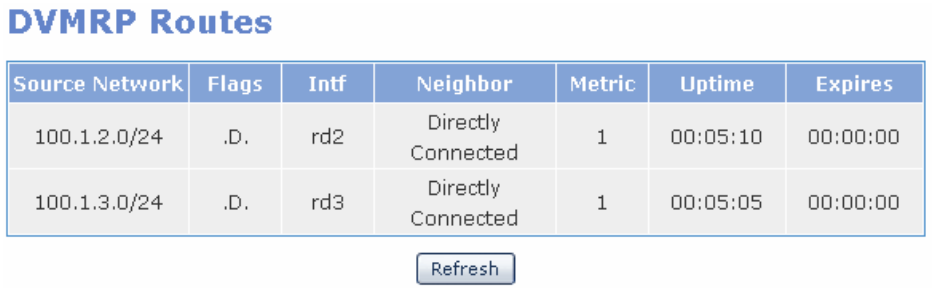
DVMRP & Help

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 Routes

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



DVMRP Routes Field Description

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

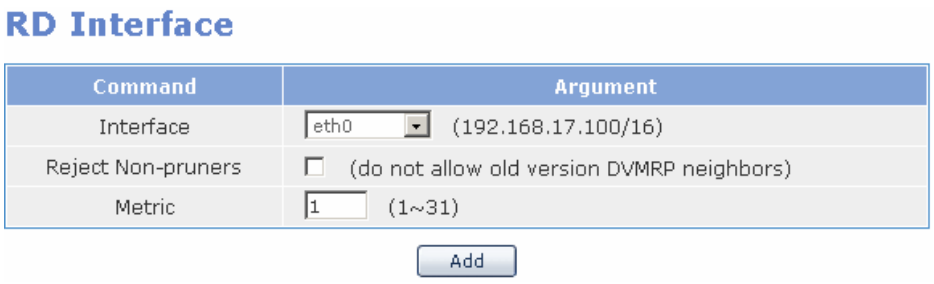
Field	Description
Metric	DVMRP route Metric(=distance) value
Uptime	Time passed after using the DVMRP route item
Expires	Left time until the DVMRP route item is expired

DVMRP Intf

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.

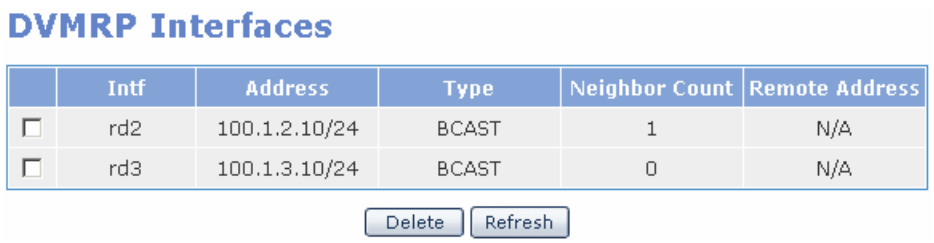


RD Interface Parameter Description

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 Field Description

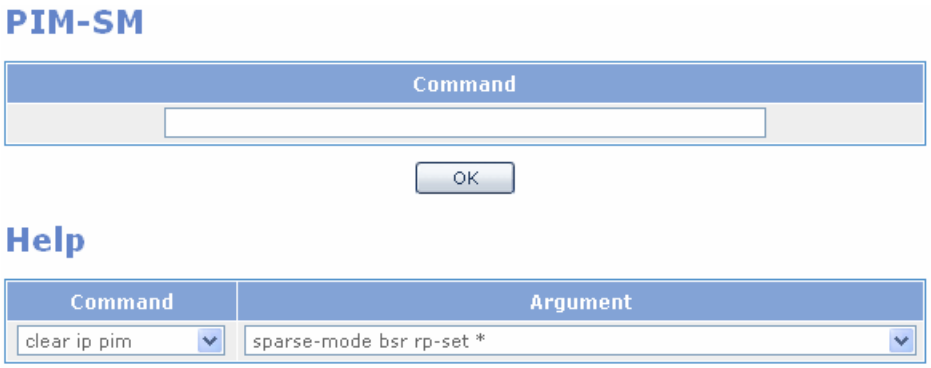
Field	Description
Intf	DVMRP VIF name
Address	IP address of DVMRP VIF
Type	DVMRP VIF type. Tunnel, Point-to-Point, Broadcast
Neighbor Count	Number of neighbors connected to DVMRP VIF
Remote Address	Address of the other party in case of Tunnel or Point-to-Point type.(Peer Address)

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 GWIMT/GWIM.

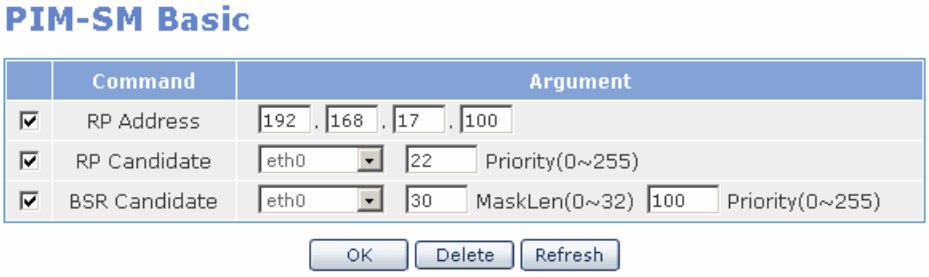
PIM-SM & Help

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 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.

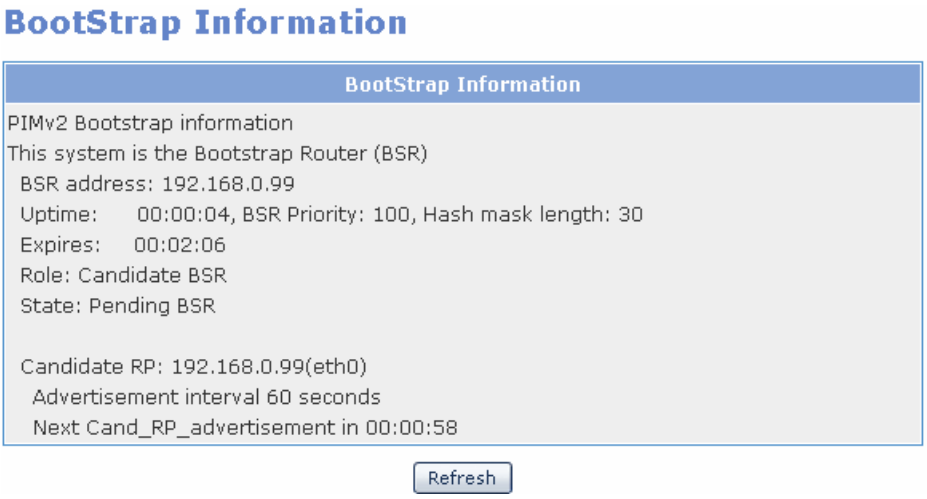


PIM-SM Basic Parameter Description

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

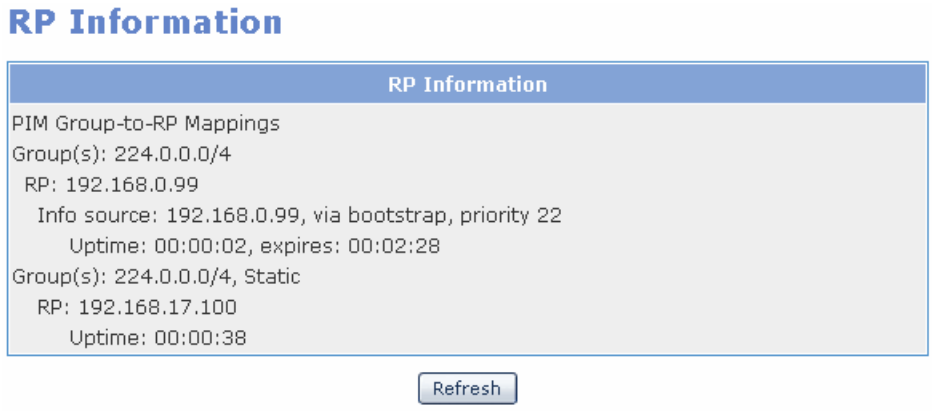
BootStrap Information

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



RP Information

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

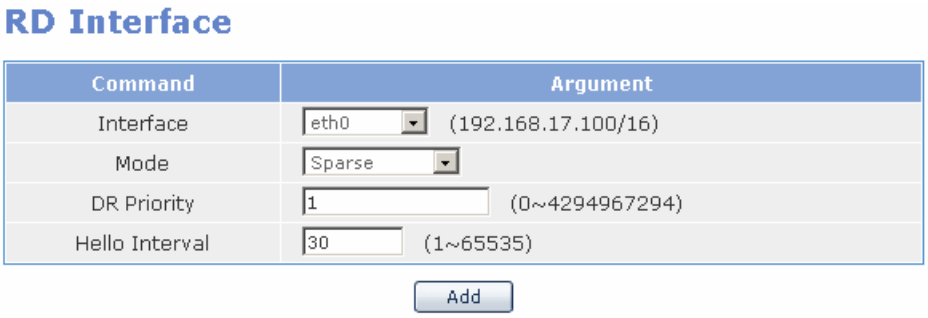


PIM-SM Intf

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.



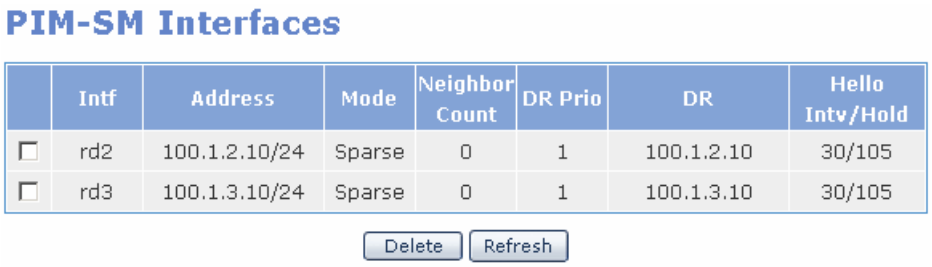
PIM-SM RD Interface Parameter Description

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.)

Parameter	Description
Hello Interval	Cycle of exchanging hello packets with connected PIM-SM neighbors

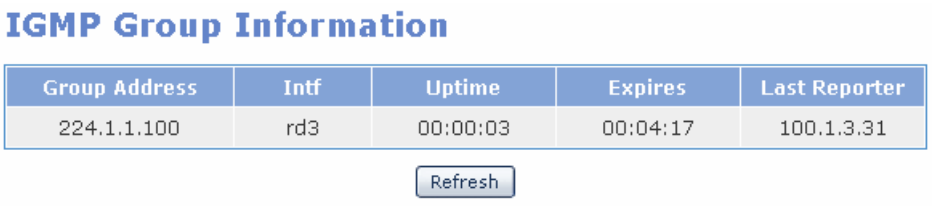
PIM-SM Interfaces

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.



IGMP Groups

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



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

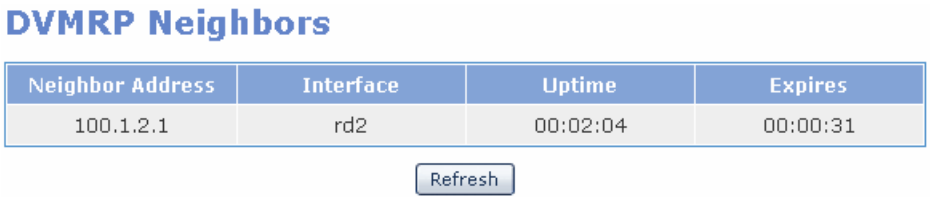
Status

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 GWIMT/GWIM.

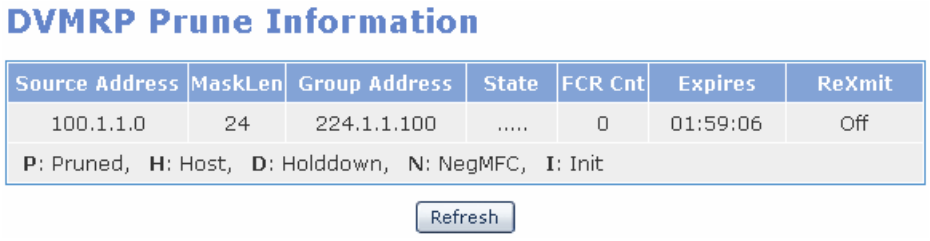


DVMRP Neighbors Field Description

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.



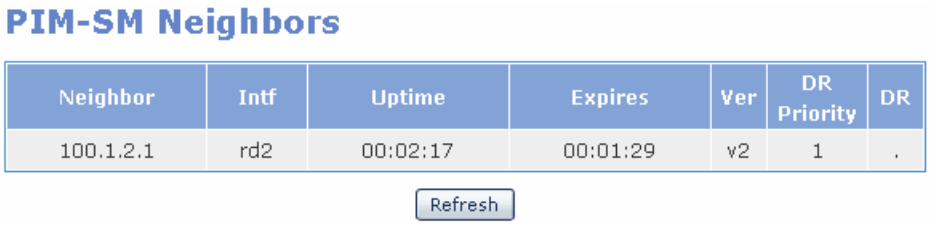
DVMRP Prune Information Field Description

Field	Description
Source Address	Host Ip address that sends multicast packets

Field	Description
MaskLen	Mask length of DVMRP Prune
Group Address	Multicast group address
State	Flags that display the DVMRP Prune status. Refer to the description on the lower side
FCR Cnt	DVMRP Forwarding Cache count
Expires	Time passed after the DVMRP Prune information is created
ReXmit	Left time until retransmission

PIM-SM

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



PIM-SM Neighbors Field Description

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

QoS

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
Group	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
Policy	-	Used to set a class for a port
Management	-	Used to start or stop the QoS service and to set the GWIMT/GWIM to start QoS automatically when the system reboots.

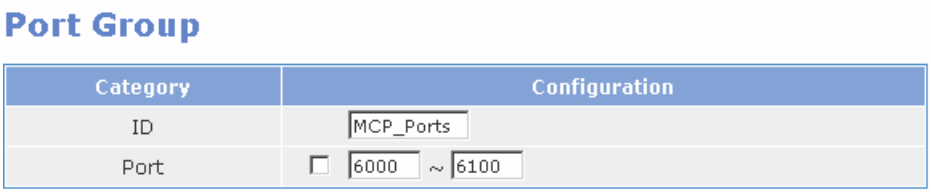
Group

Port Group

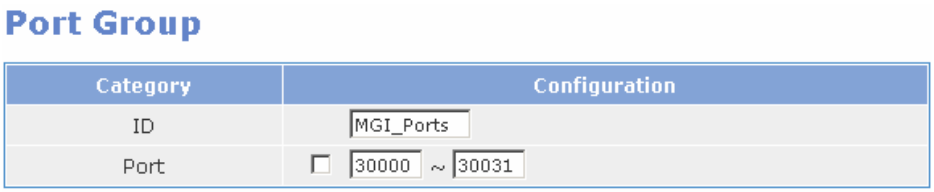
The GWIMT/GWIM uses the Port Group submenu to define specific IP ports or ranges of IP ports for the QoS policies. Select the [QoS] → [Group] → **[Port Group]** submenu to retrieve, set, edit, or delete a port group.

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.

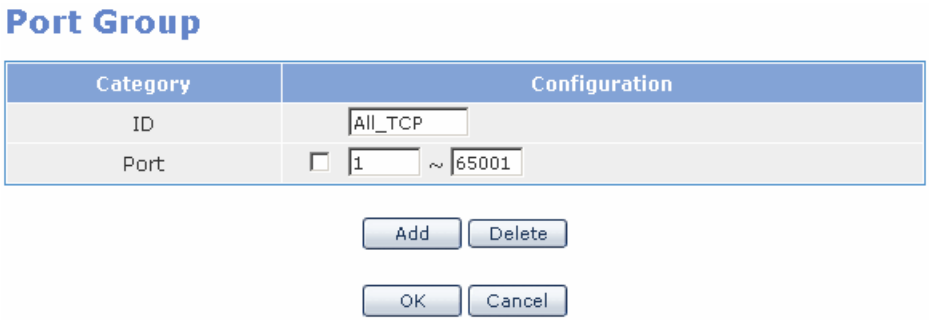
In the examples listed below there are three Port Groups created. One is for ports 6000 through 6100 which will be used for the MP40 card, the second is for ports 30000 through 30031 for the MGI card, and the last is for ports 1 through 65001 for TCP on the entire network.



Click the Add button to create another Port Group

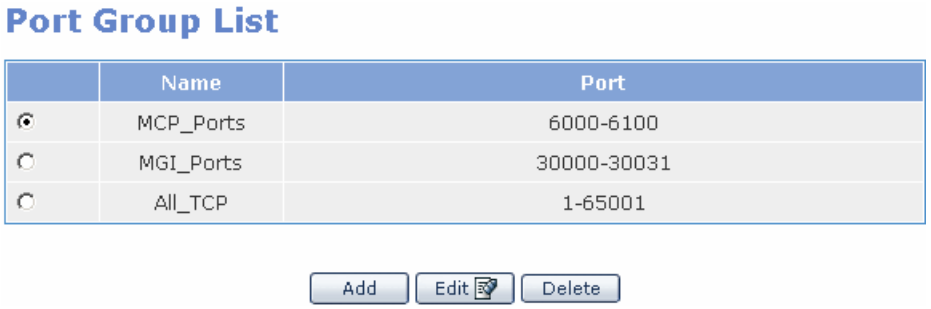


Click the Add button to create another Port Group



Port Group Parameter Description

Parameter	Description
ID	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.
Port	- Port range - Enter '0' to set all ports



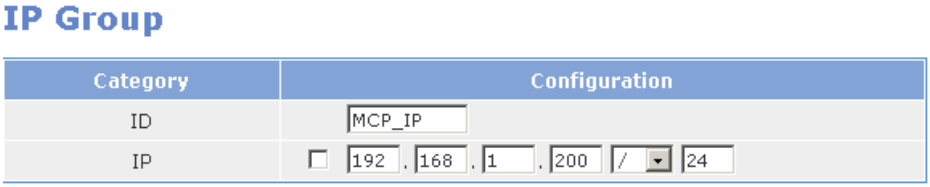
In order to delete a Port Group List highlight the radio button to the left of the Port Group List and then click the delete button.

IP Group

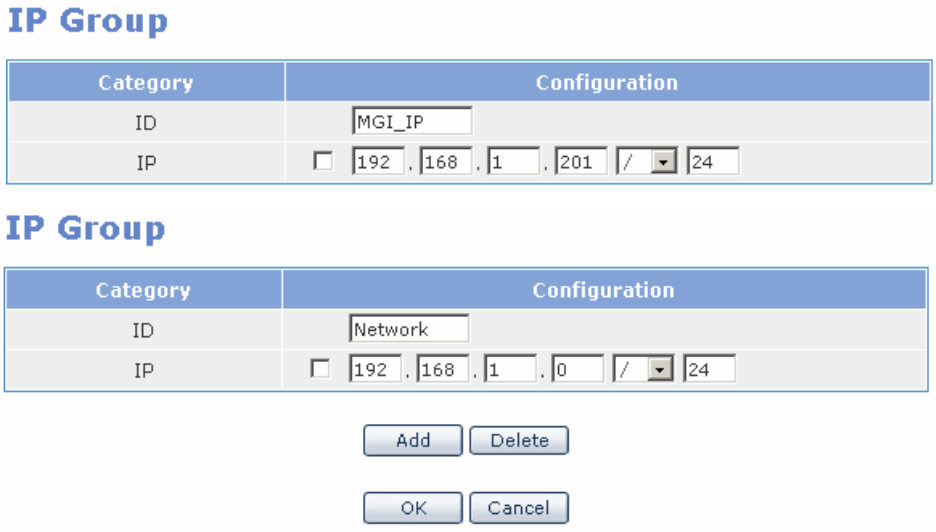
The GWIMT/GWIM uses the IP Group submenu to define specific IP addresses for the QoS policies. Select the **[QoS]** → **[Group]** → **[IP Group]** to retrieve, set, edit, or delete an IP group.

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.

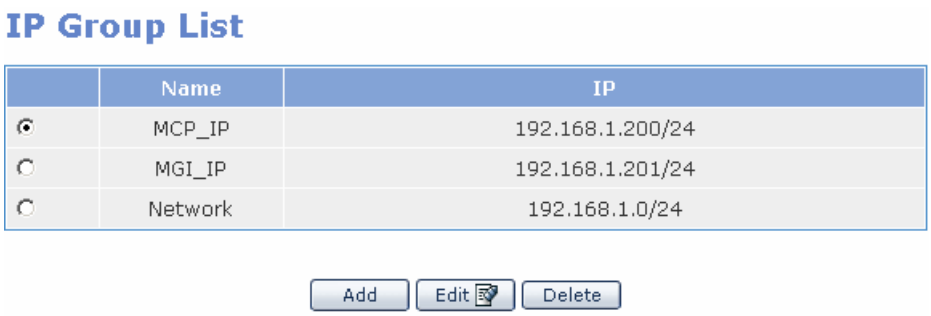


Enter the IP Group ID and then the IP address information. Click the OK button to save the changes Click the Add button to add another IP Group.



IP Group Parameter Description

Parameter	Description
ID	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.
IP	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.



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 GWIMT/GWIM 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

Add | Edit | Delete

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 ans 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 theMP40, 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	DEC HEX 0x
Source IP:Port	any : any
Destination IP:Port	MGI_IP : MGI_Ports

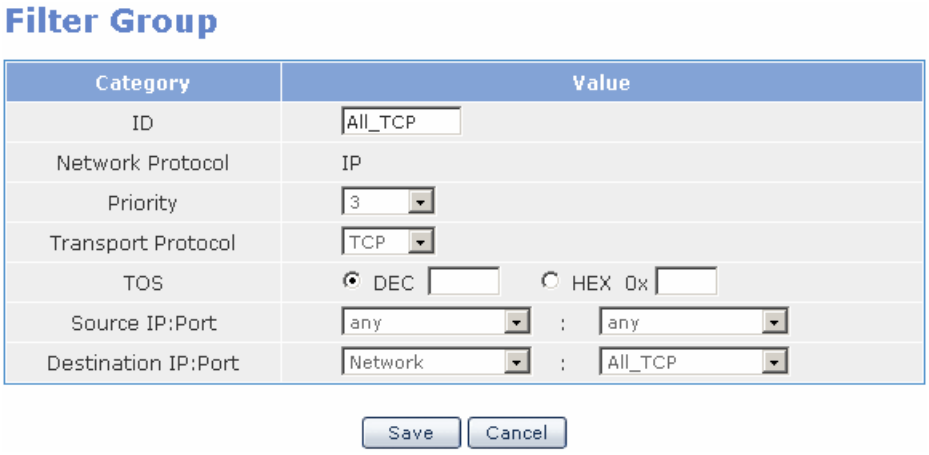
Save | Cancel

Click the Add button to create another Filter Group

Filter Group

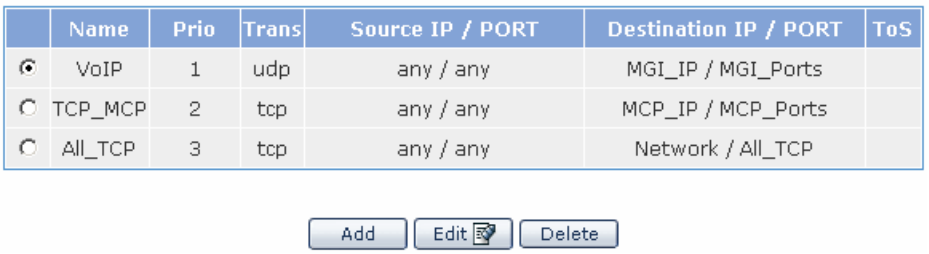
Category	Value
ID	TCP_MCP
Network Protocol	IP
Priority	2
Transport Protocol	TCP
TOS	DEC HEX 0x
Source IP:Port	any : any
Destination IP:Port	MCP_IP : MCP_Ports

Save | Cancel



Filter Group Parameter Description

Parameter	Description
ID	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.
Priority	Queue Priority
Transport Protocol	TCP or UDP Protocol
TOS	TOS entry
Source IP:Port	Source IP Address and Port number/s
Destination IP:Port	Destination IP Address and Port number/s



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.

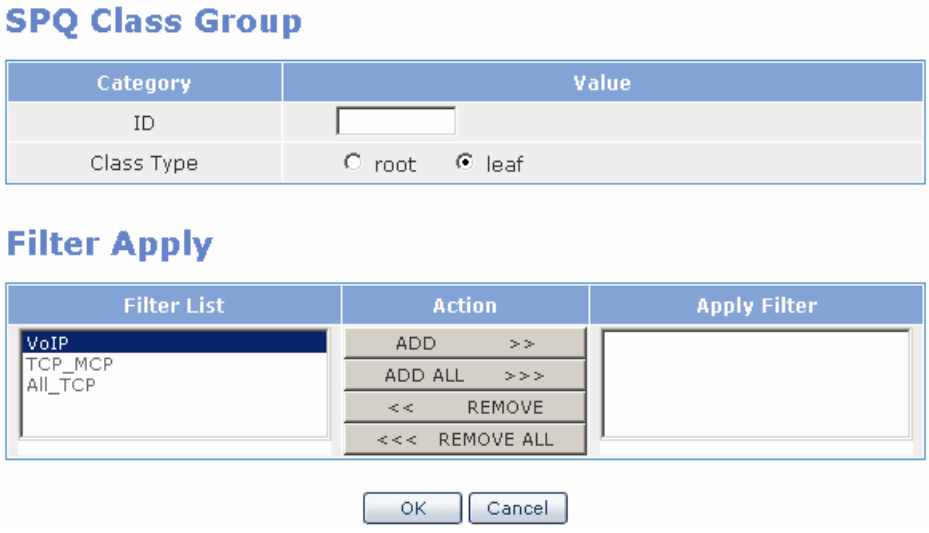
Class Group

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

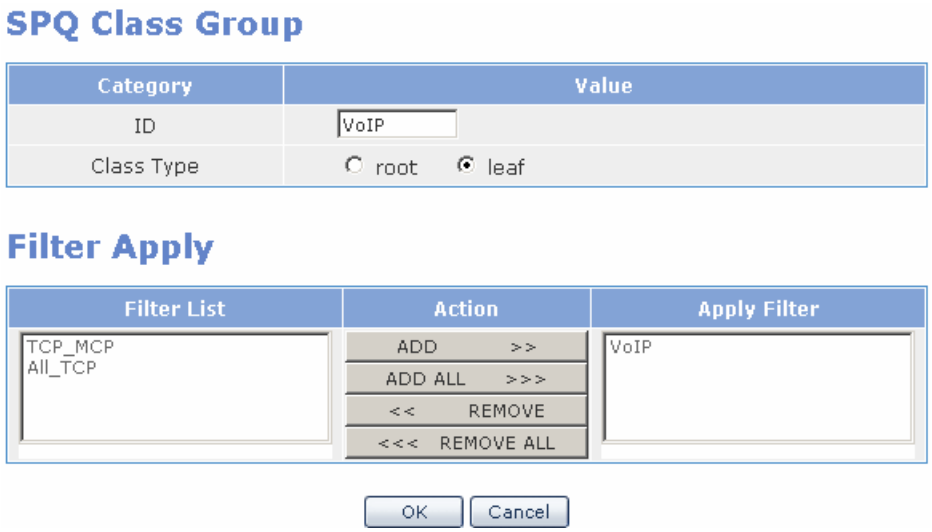
Begin configuring the Strict Policy Queuing by clicking the Add button

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.

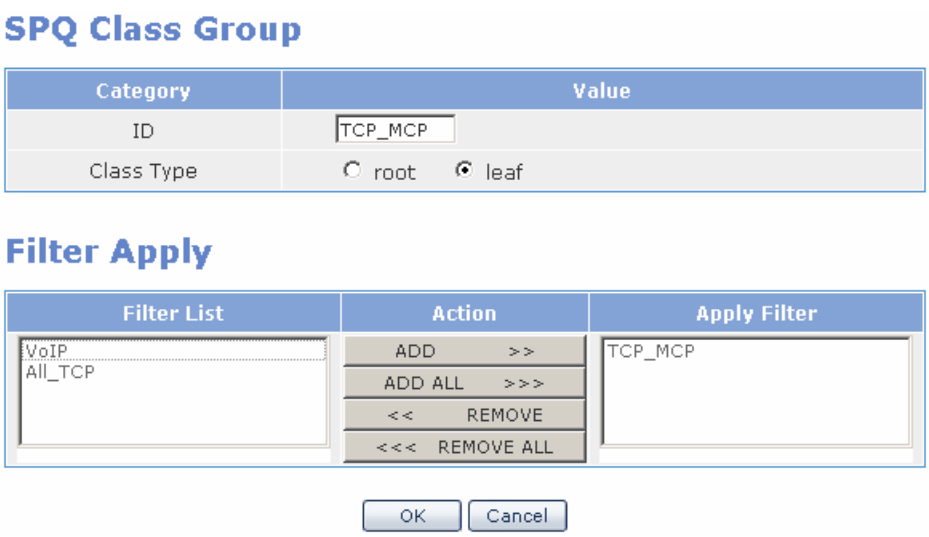


In the examples listed below there are three leaf and one root SPQ Class Groups created. One leaf is for the VoIP Traffic, the second is for the MP40, and the last leaf is for the rest of the TCP traffic on the 192.168.1.0/24 network. The root group prioritizes the leafs into High, Middle, and Low Priority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

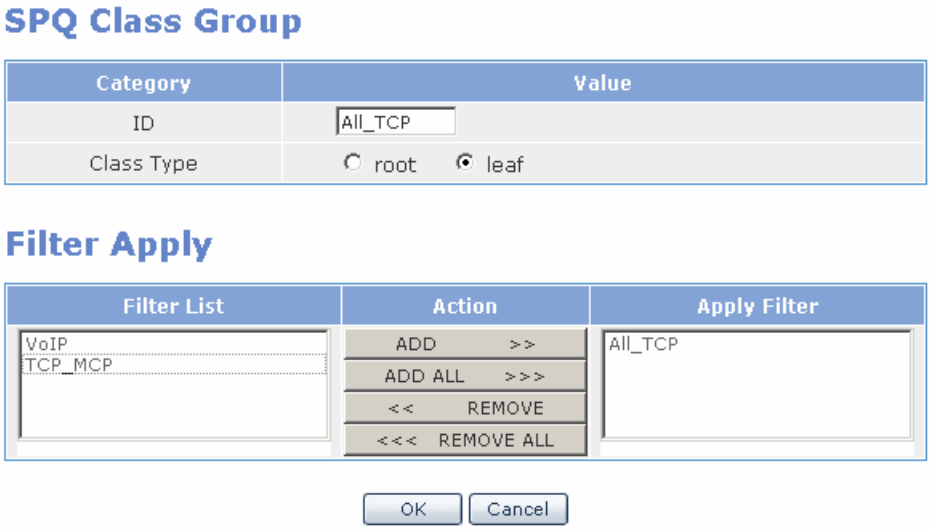
Example 1 shows a SPQ leaf Class Group which was designed for VoIP traffic.



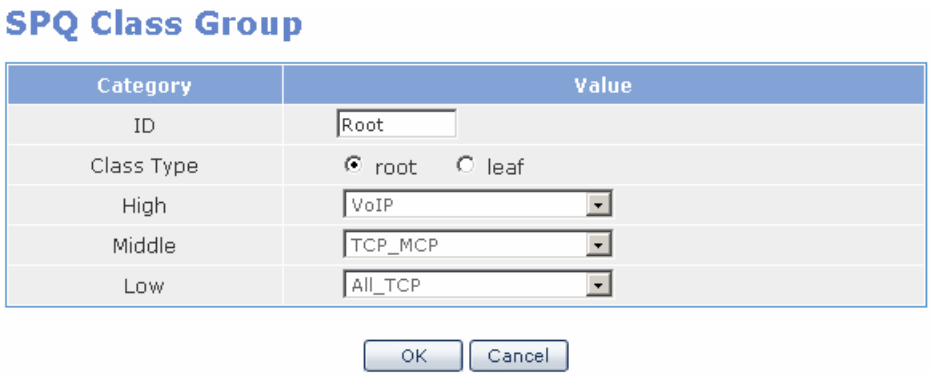
Example 2 shows a SPQ leaf Class Group which was designed for MCP TCP traffic.



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



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 Parameter Description

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

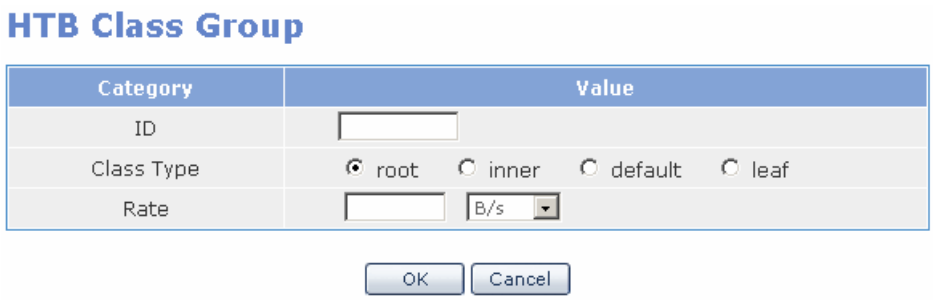
NOTE

SPQ

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

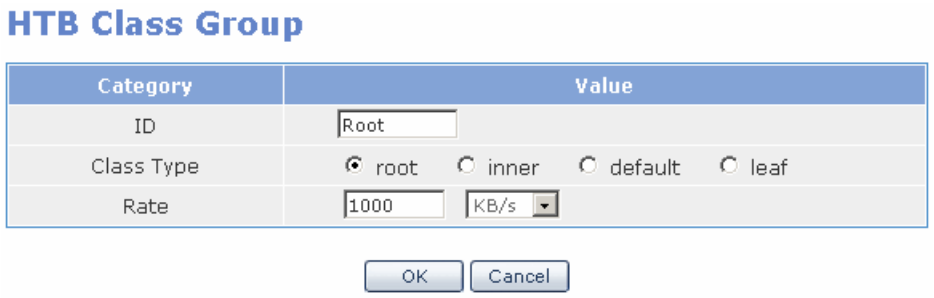
HTB Class Group

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.



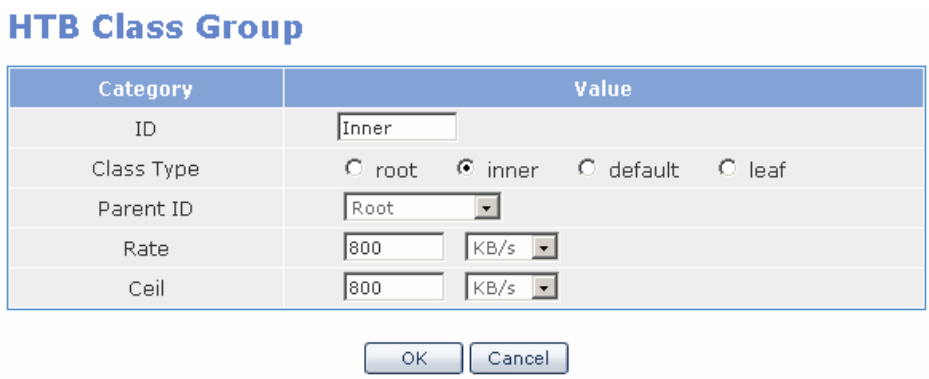
When configuring HTB it is best to begin by creating the root. Assign a Root ID, click the root radio button, and define the bandwidth allocation.

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



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 desised speed) and the Ceil parameter (maximum desired speed).

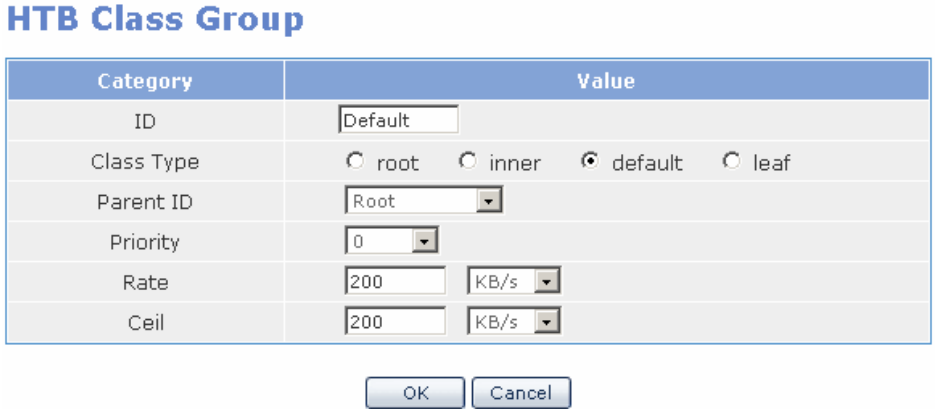
In the example listed below the there will only be one Inner class so 800 KBs will be used. The remaining 200 KBs will be used for the Default class.



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 desised speed) and the Ceil parameter (maximum desired speed).

In the example listed below the 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.



The forth 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 desised speed) and the Ceil parameter (maximum desired speed), and then select the Filter to apply.

In the examples listed below the 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	○ root ○ inner ○ default ● leaf
Parent ID	Inner
Priority	1
Rate	300 KB/s
Ceil	800 KB/s

Filter Apply

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

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	○ root ○ inner ○ default ● leaf
Parent ID	Inner
Priority	2
Rate	200 KB/s
Ceil	600 KB/s

Filter Apply

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

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	root inner default leaf
Parent ID	Inner
Priority	3
Rate	200 KB/s
Ceil	500 KB/s

Filter Apply

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

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
◉	Root	root	-	-	1000 KB/s	-
○	Inner	inner	Root		800 KB/s	800 KB/s
○	Default	default		0	200 KB/s	200 KB/s
○	Voip_Leaf	leaf	Inner	1	300 KB/s	800 KB/s
Filter			VoIP			
○	MCP_TCP	leaf	Inner	2	200 KB/s	600 KB/s
Filter			TCP_MCP			
○	All_TCP	leaf	Inner	3	200 KB/s	500 KB/s
Filter			All_TCP			

Add Edit Delete

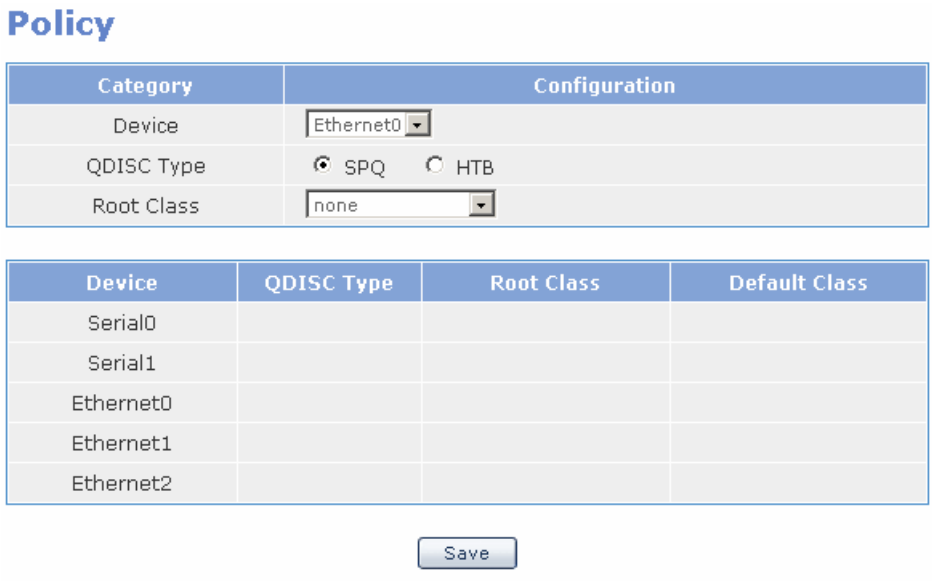
Each class group can either be modified or deleted by clicking the radio button to the left of the class group and then by clicking the Edit or Delete button.

HTB Class Group List Parameter Description

Item	Description
Class Type	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.
Parent ID	If the target class is a child class of another class, set the parent class in the Parent ID item. Do not set the Parent ID if the target class is the root class(highest level class physically connected to the device) or if the default class (class including the bandwidth for traffics that do not belong to a filter).
Priority	If several classes compete to occupy leftover bandwidths or if all classes attempt to occupy excess bandwidth, set the priority so that the class with the highest priority occupies the bandwidth first.
Rate	This is the basic minimal bandwidth needed for setting class for an assigned bandwidth.
Ceil	Maximum value of assigned bandwidth.
Filter List	Used to set the filtering rules for the class.
Scheduling Parameter	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.

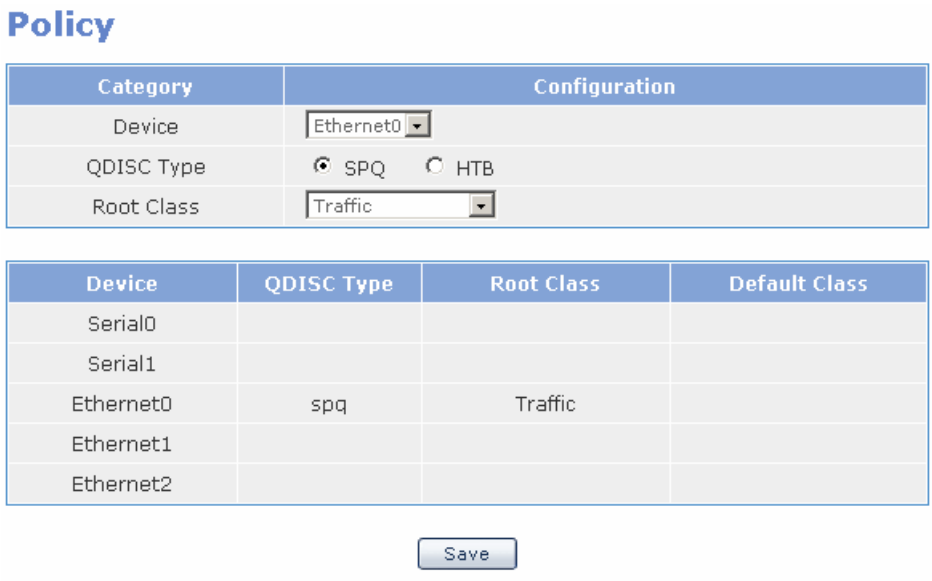


Policy Parameter Description

Parameter	Description
Device	Used to select an interface (eth0, eth1, eth2, V.35, or HSSI)
QDISC Type	Used to select the QDISC to be applied to the interface
Root Class	Used to assign a Class connected to the interface. Select the class group from the class group list.
Default Class (HTB only)	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.

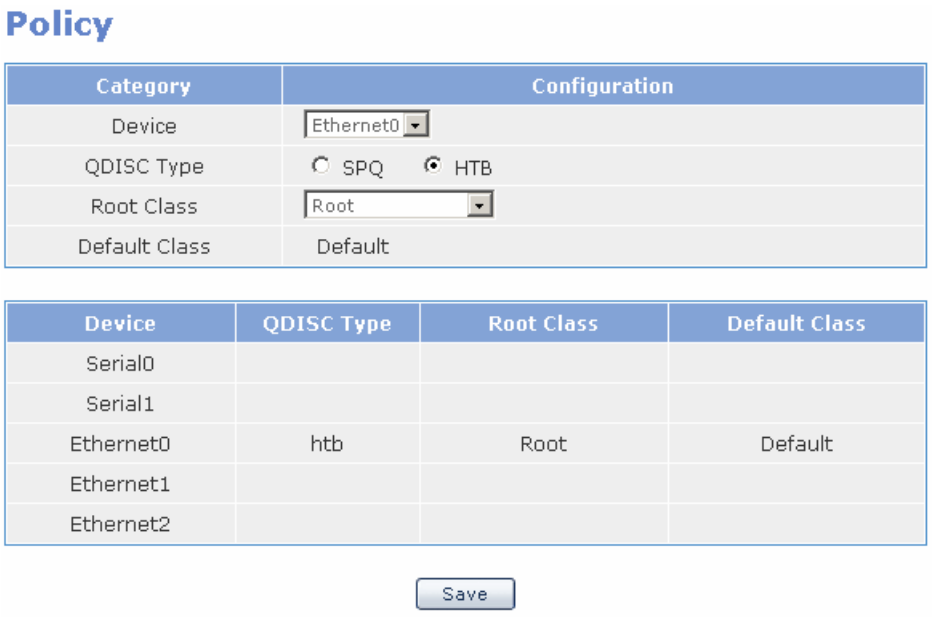
SPQ Policy

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.



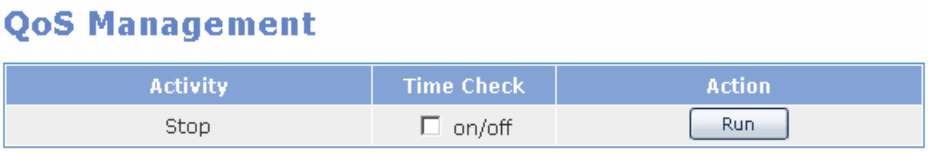
HTB Policy

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.



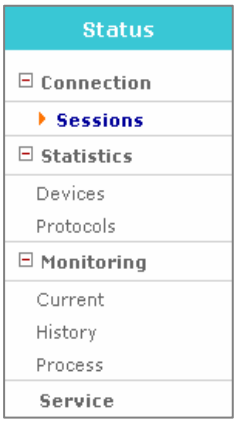
Management

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.



Status

The Status Menu is used to view active IP sessions on the GWIMT/GWIM, 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:



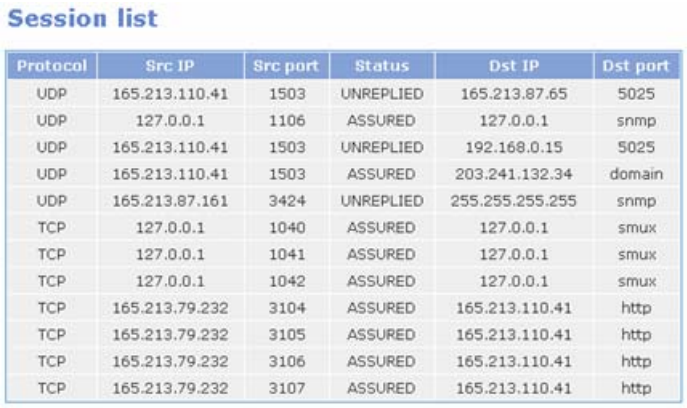
Status Menu Description

Menu	Submenu	Description
Connection	Sessions	Used to display the information on the IP address and IP ports connected to GWIMT/GWIM.
Statistics	Devices	Used to display the GWIMT/GWIM network statistics for the Tx and Rx of each interface.
	Protocols	Used to display the GWIMT/GWIM network statistics of each protocol.
Monitoring	Current	Provides the GWIMT/GWIM network statistics in a table format in real time.
	History	Used to display the GWIMT/GWIM 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 GWIMT/GWIM.
Services	-	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 GWIMT/GWIM.



Session list

Protocol	Src IP	Src port	Status	Dst IP	Dst port
UDP	165.213.110.41	1503	UNREPLIED	165.213.87.65	5025
UDP	127.0.0.1	1106	ASSURED	127.0.0.1	snmp
UDP	165.213.110.41	1503	UNREPLIED	192.168.0.15	5025
UDP	165.213.110.41	1503	ASSURED	203.241.132.34	domain
UDP	165.213.87.161	3424	UNREPLIED	255.255.255.255	snmp
TCP	127.0.0.1	1040	ASSURED	127.0.0.1	smux
TCP	127.0.0.1	1041	ASSURED	127.0.0.1	smux
TCP	127.0.0.1	1042	ASSURED	127.0.0.1	smux
TCP	165.213.79.232	3104	ASSURED	165.213.110.41	http
TCP	165.213.79.232	3105	ASSURED	165.213.110.41	http
TCP	165.213.79.232	3106	ASSURED	165.213.110.41	http
TCP	165.213.79.232	3107	ASSURED	165.213.110.41	http

Session List Field Description

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

Statistics

Devices

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

Received

Devices	Bytes	Packets	Errs	Drop	FIFO	Frame	Compressed	Multicast
Ethernet 0	18314987	162219	0	0	0	0	0	0
Ethernet 1	8351384	67681	0	0	0	0	0	0
Ethernet 2	536234	7771	0	0	0	0	0	0
Serial0	0	0	0	0	0	0	0	0
Serial1	0	0	0	0	0	0	0	0

Transmitted

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

Refresh

Devices Received and Transmittted Field Description

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

Protocols

The **[Status]** → **[Statistics]** → **[Protocols]** is used to display GWIMT/GWIM network statistics of each protocol type (Unit: Byte)

Network statisics by protocols

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

Monitoring

Current

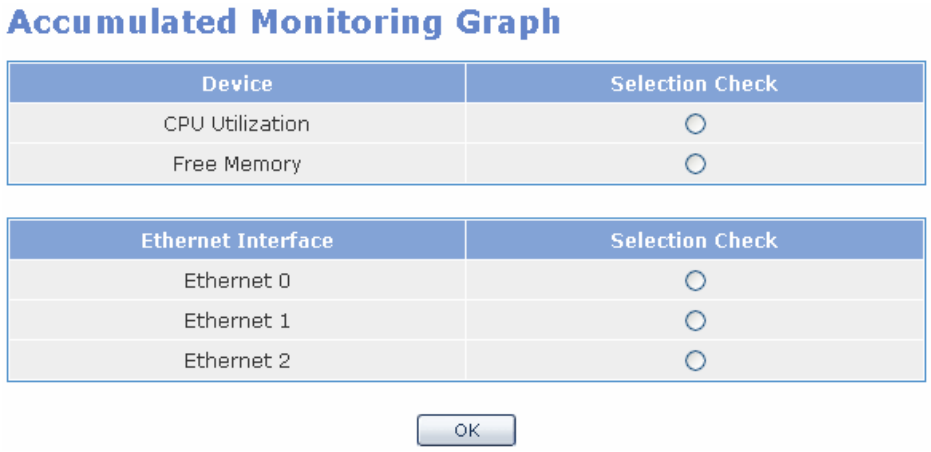
The **[Status]** → **[Monitoring]** → **[Current]** submenu is used to display the GWIMT/GWIM network statistics in real time. The data window is updated every 5 seconds.

Rate(Bytes/Sec)

Devices	Received	Transmitted	Trans/Recv
Ethernet 0	2735	8513	2249
Ethernet 1	0	0	0
Ethernet 2	56	0	11
Serial 0	0	0	0
Serial 1	0	0	0

History

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



Accumulated Monitoring Graph

Device	Selection Check
CPU Utilization	○
Free Memory	○

Ethernet Interface	Selection Check
Ethernet 0	○
Ethernet 1	○
Ethernet 2	○

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 GWIMT/GWIM.

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 GWIMT/GWIM 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 GWIMT/GWIM.

Security

Name	Activity
NAT (Network Address Translation)	Running
Filter	Running
PPTP (Point-to-Point Tunneling Protocol)	Stopped
IDS (Intrusion Detection System)	Stopped
L2TP (Layer 2 Transfer Protocol)	Stopped
IPSEC (IP Security)	Stopped

Router

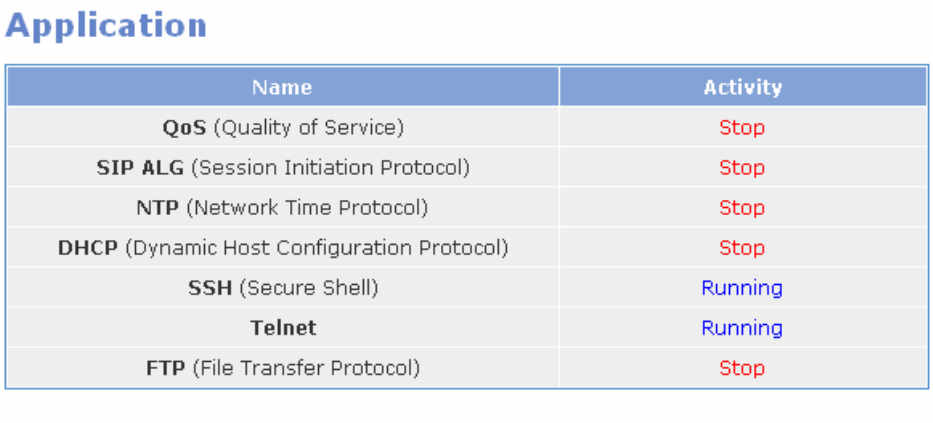
This window is used to display the current status of the Router services being provided by the GWIMT/GWIM.

Router

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

Application

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

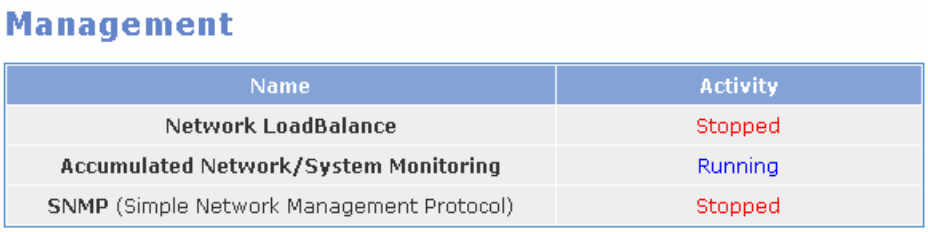


Application

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

Management

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



Management

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

VPN Menu

A VPN is an encryted tunnel which is used to allows 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 GWIMT/GWIM 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 GWIMT/GWIM 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

NOTE

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 7400 Data Server. For detailed information on the configuration settings and method, refer to ‘Appendix A’..

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 GWIMT/GWIM 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.

NOTE

IPSec Tunnel Mode

The OfficeServ 7400 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.

NOTE

VPN Programming

The OfficeServ 7400 Data Server requires a VPN Accelerator daughterboard for VPN functionality.

Config

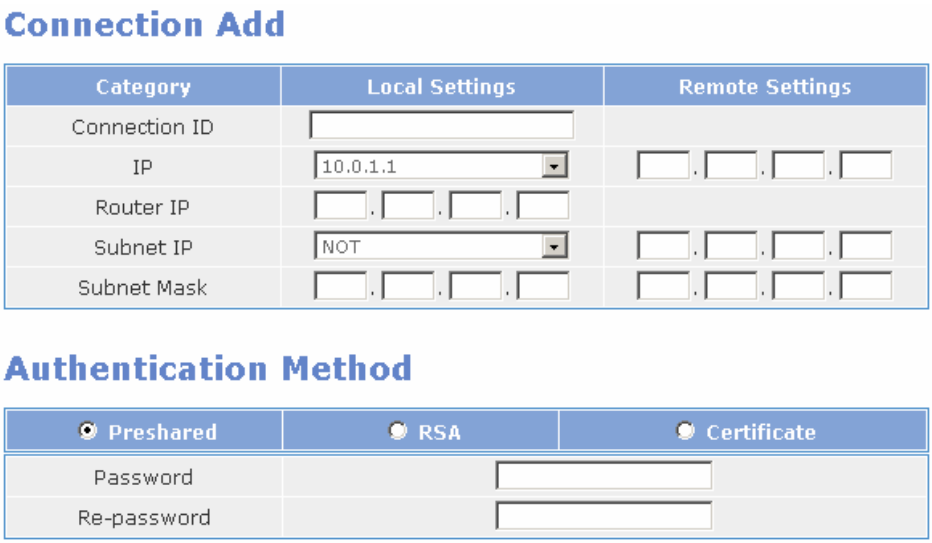
Use the **[VPN]** → **[IPSec]** → **[Configuration]** submenu to begin configuring IPSec.

IPSec Connection Button Description

Item	Description
Add	Used to create an IPSec tunnel
Delete	Used to delete an IPSec tunnel
Edit	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.



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	Router IP address (typically the gateway for WAN Interface)
Subnet IP	Internal IP address range
Subnet Mask	Internal subnet mask

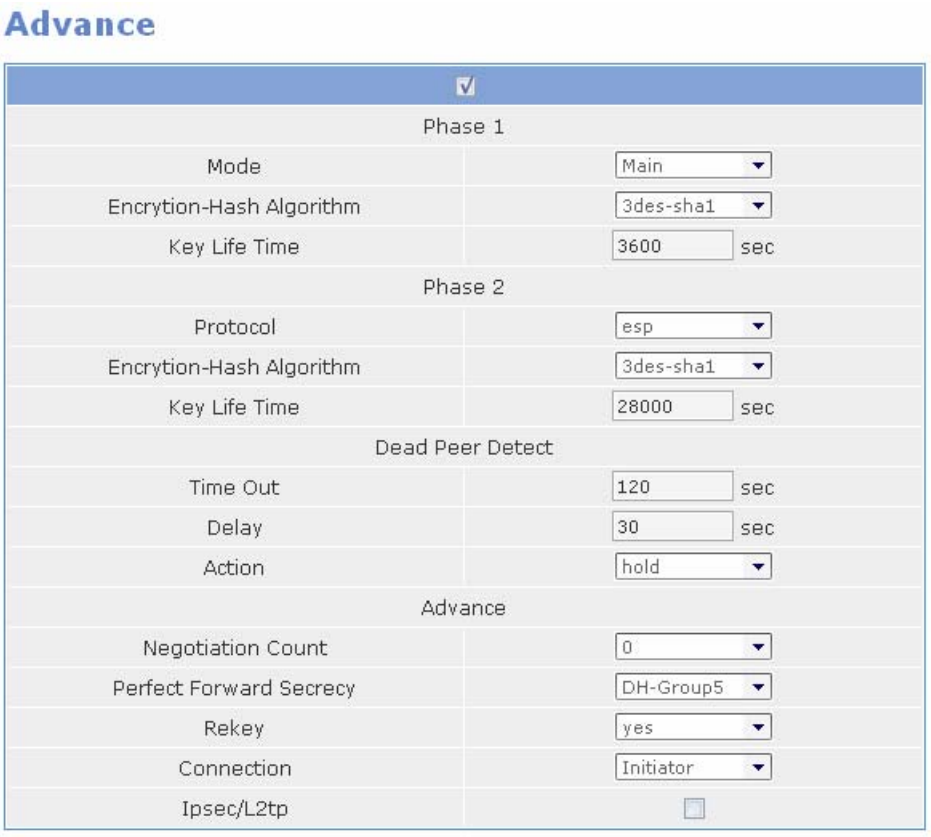
Parameter	Description
RSA Key/ Preshared Key /Certificate	Selects the host authentication method - **RSA Key**: The Public RSA key is already defined.. Click the Browse button to find the Remote Key and then click on the Upload button to store the RSA key into the GWIMT/GWIM - **Preshared Key**: Used to enter an authentication password. - **Certificate**: 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.

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.



IPSec Advanced Parameter Description

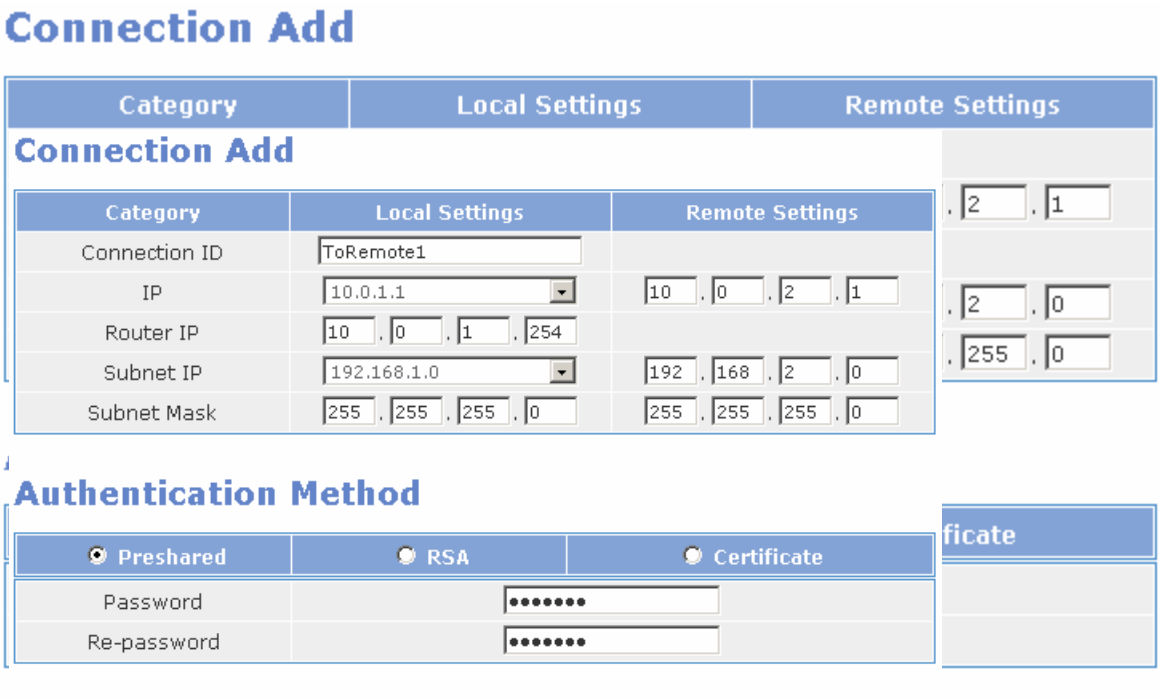
Parameter		Description
Phase1	mode	Used to set the Ike mode - **Main**: Configures a secure channel to perform the ISAKMP exchange of phase one - **Aggressive**: Different type of phase one, which is more simple and faster than the Main mode
	Encryption-Hash Algorithm	Used to set the supporting Algorithm 3DES-MD5, 3DES-SHA1, AES128-MD5, AES128-SHA1, AES192-MD5, AES192-SHA1, AES256-MD5, AES256-SHA1
	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.

Parameter		Description
Phase2	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
	Encryption-Hash Algorithm	Used to set the supporting Algorithm 3DES-MD5, 3DES-SHA1, AES128-MD5, AES128-SHA1, AES192-MD5, AES192-SHA1, AES256-MD5, AES256-SHA1
	Key life time	The cycle of newly added key used for packet encryption by the repeated phase two IKE negotiation
Advance	PFS	Used to select the session key transfer/security
	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
	Connection	IPSec Connection Attempt - initiator: Attempting a connection - response: Attempt to receive a connection
	IPSec/l2tp	Sets when IPSec over l2tpis is used. (Supports Window XP SP 2.)
DPD	Time out	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.

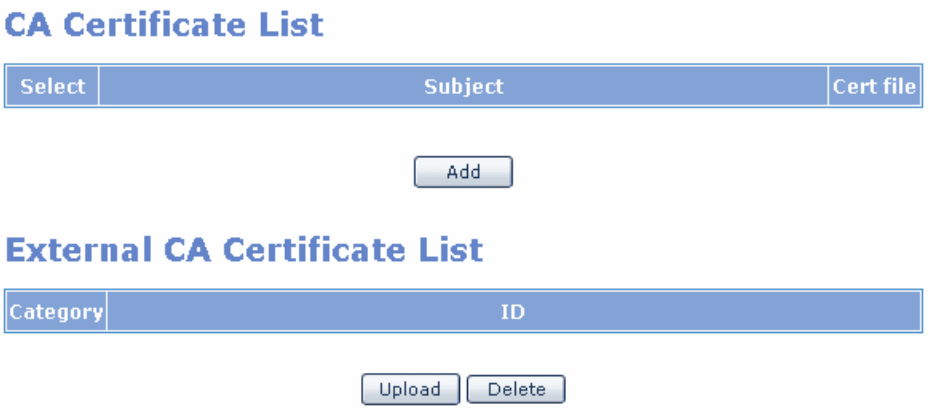
IPSec Tunnel Programming Example

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.



Certificate

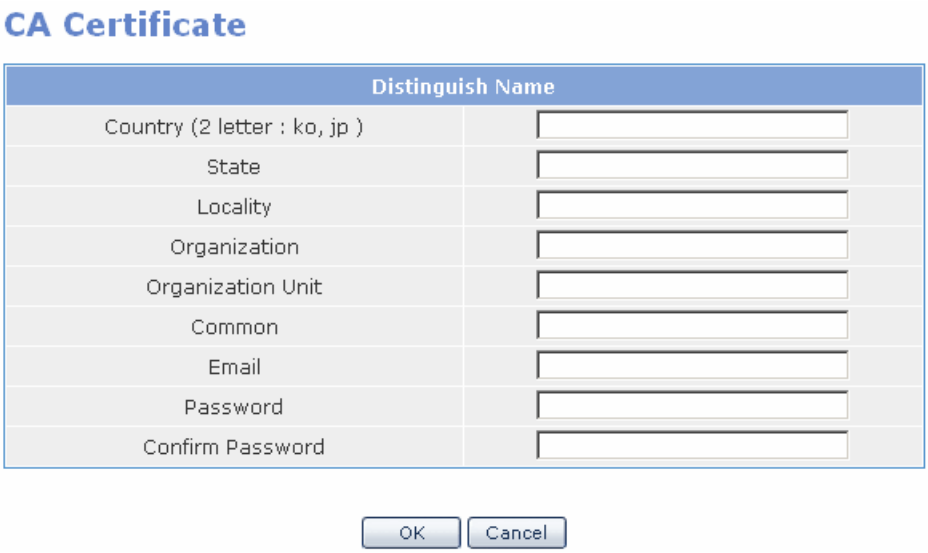
The **[VPN]→ [IPSec] → [Certificate]** submenu is used by the administrator to verify Issue/Delete/Download a CA Certificate and Host certificate. In addition the addition/delete of an external certificate, and the current certificate list is performed here.



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 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 sucessully enter the CA Certificate password. So keep track of any CA Certificates that are created.

External Certificate

External CA Certificate Parameter Description

Item	Description
CA Certificate	External certificate upload

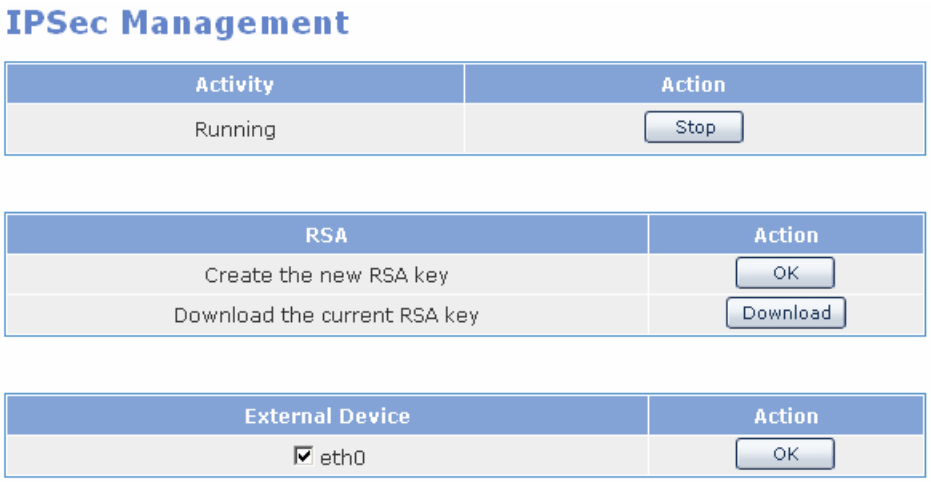
Host Certificate

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 GWIMT/GWIM 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.



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.

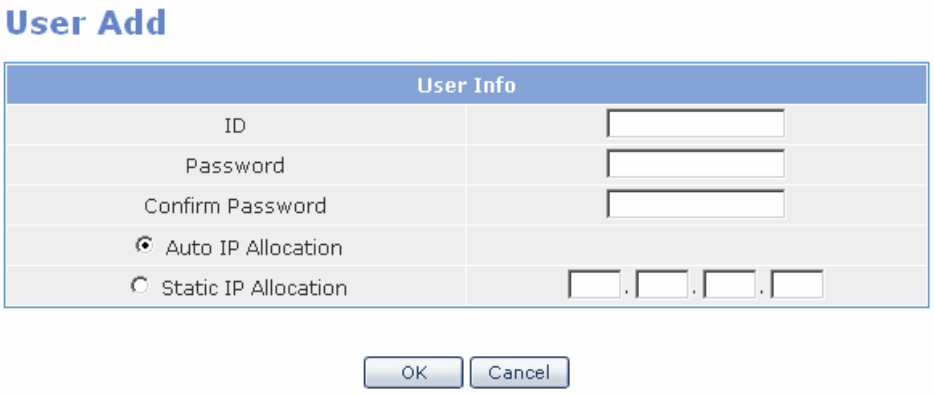
L2TP User List Field Description

Field	Description
Add	Create a PPTP administrator

Field	Description
Delete	Delete a PPTP administrator
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..

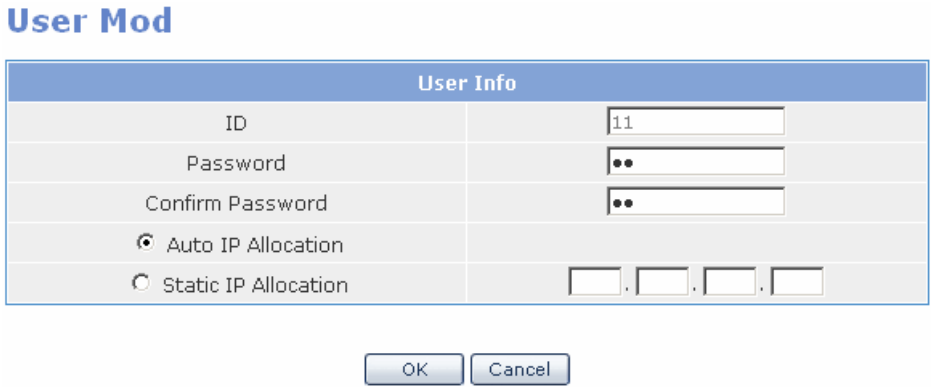


L2TP User Add Parameter Description

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

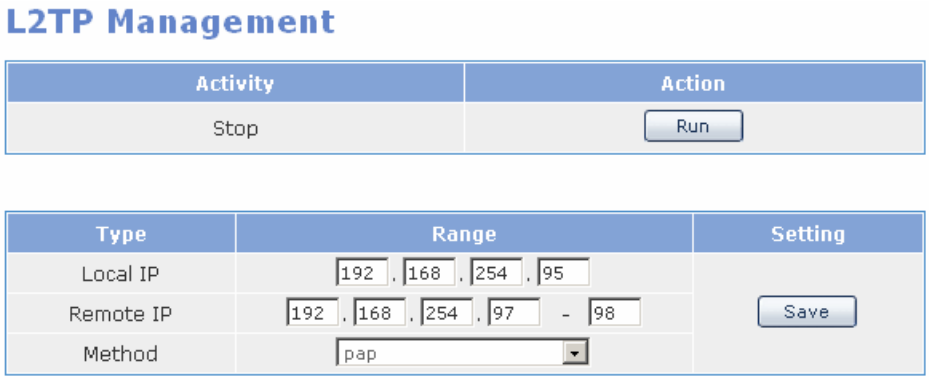
Edit

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.



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.



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’.

> **CAUTION**
>
> **Setting up IP Range**
>
> The number of IPs for the ‘Local IP range’ and that for the ‘Remote IP range’ should be identical.
> For example, if the number of IPs for ‘Local IP range’ is 10 and that for ‘Remote IP range’ is 20, only 10 calls will be set.

PPTP

Configuration

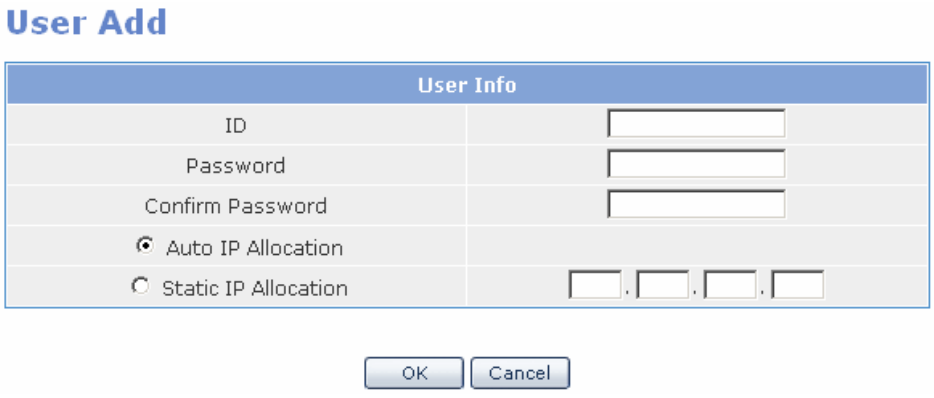
The system administrator can begin setting up the PPTP security between a local subnet and a remote host by using the **[VPN] → [PPTP] → [Configuration]** submenu. The administrator can create, modify, delete, or retrieve the VPN tunnel data from here.

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..



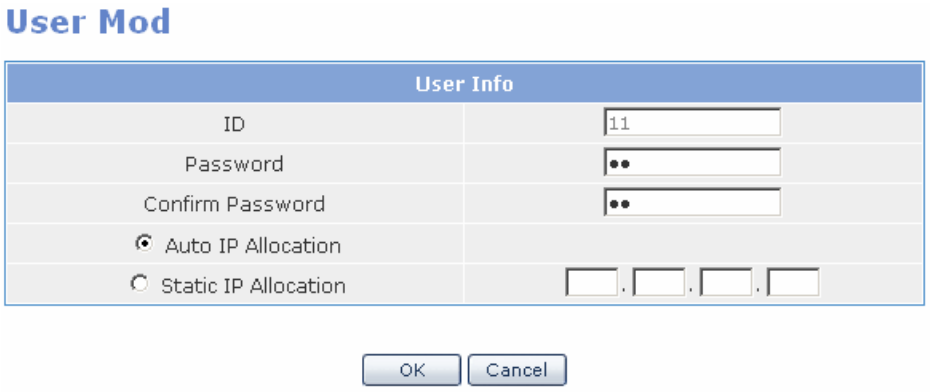
PPTP User Add Paramer Description

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)

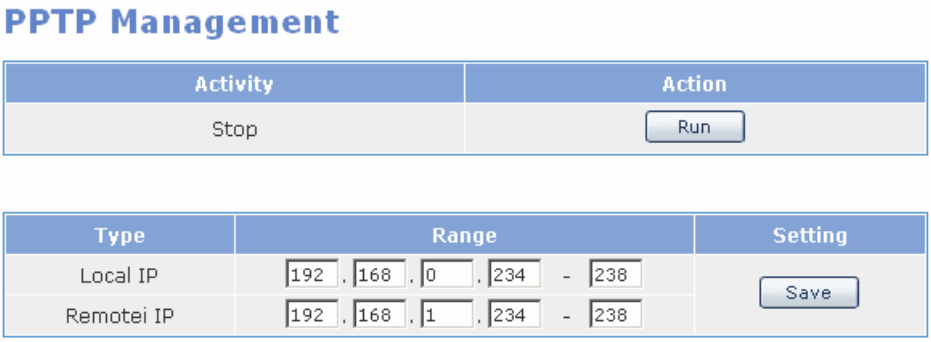
Edit

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.



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.

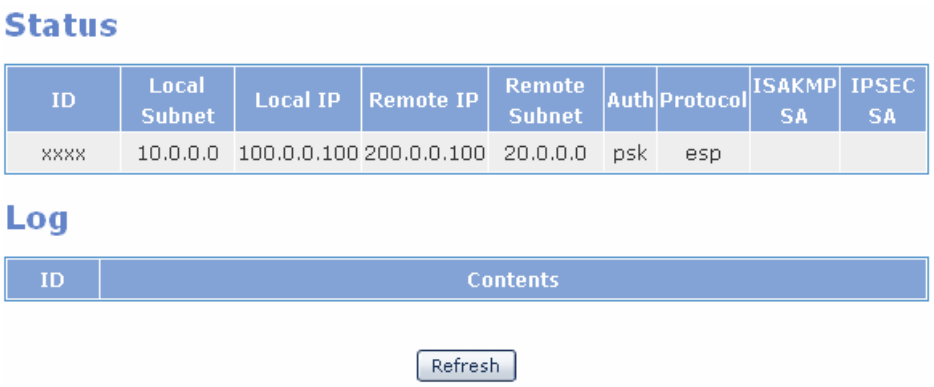


The administrator can also set up the IP range for the remote PPTP clients that use the dynamic IP feature.

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

Status

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.



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.

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 GWIMT/GWIM 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:

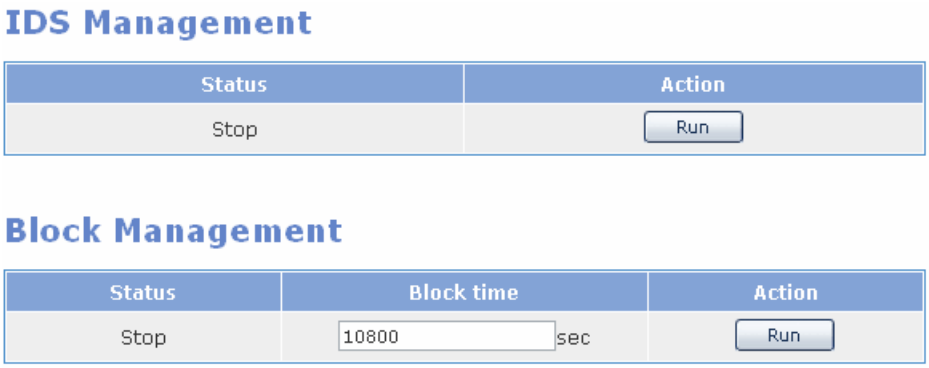
IDS Menu Description

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 IPAddress of the system Manager

IDS Config

Management

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

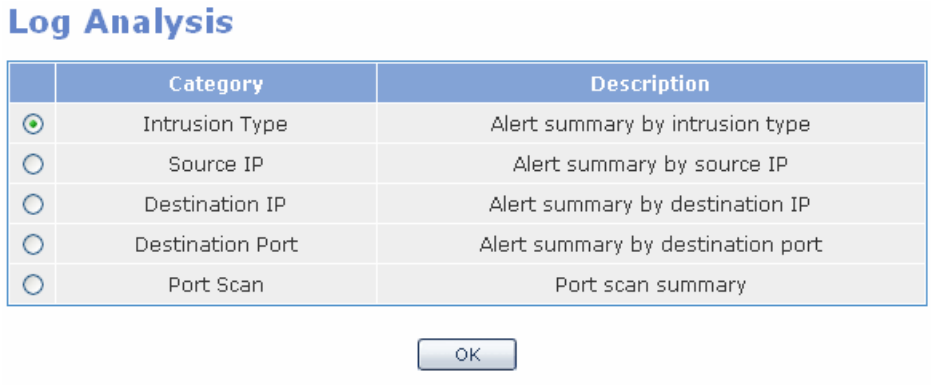


IDS Management Field/Parameter Description

Field/Parameter	Description
Status	- Running: The IDS module is operational - Stop: The IDS module is not in operation
Action	Click\ the **Run** button to start the IDS module. Click the **[Stop]** button to stop the IDS module
Block time	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

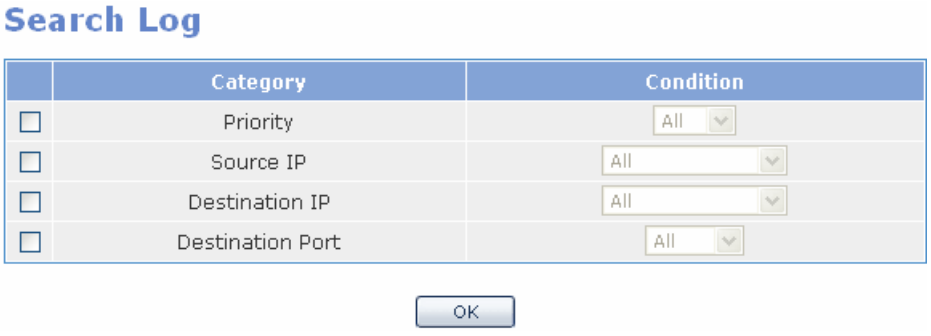
Log Analysis

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 Parameter Description

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

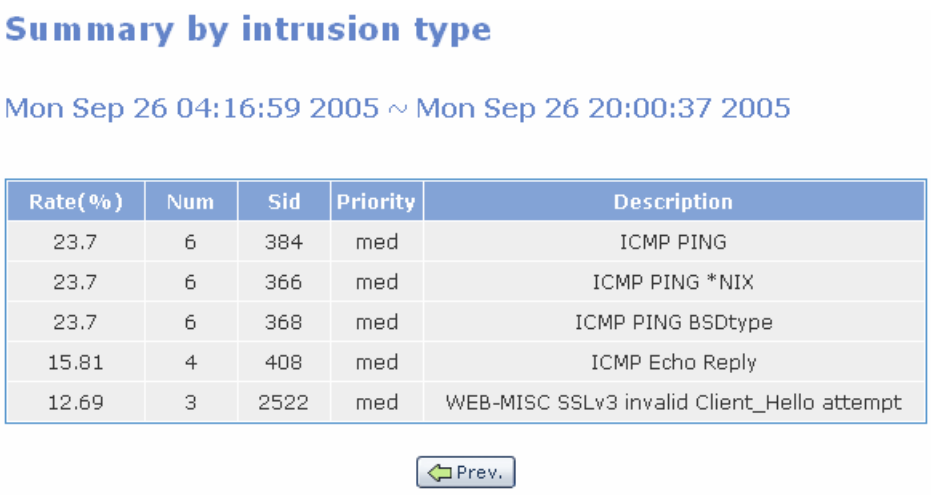


Search Log Parameter Description

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

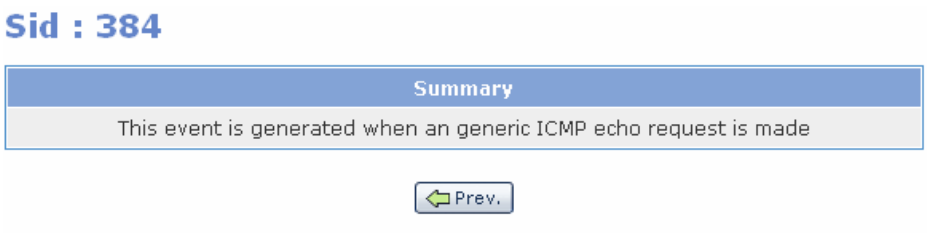
The administrator can summarize the IDS alerts by type. If the alert log is defined by Intrusion Type the following window will appear:



Intrusion Type Field Description

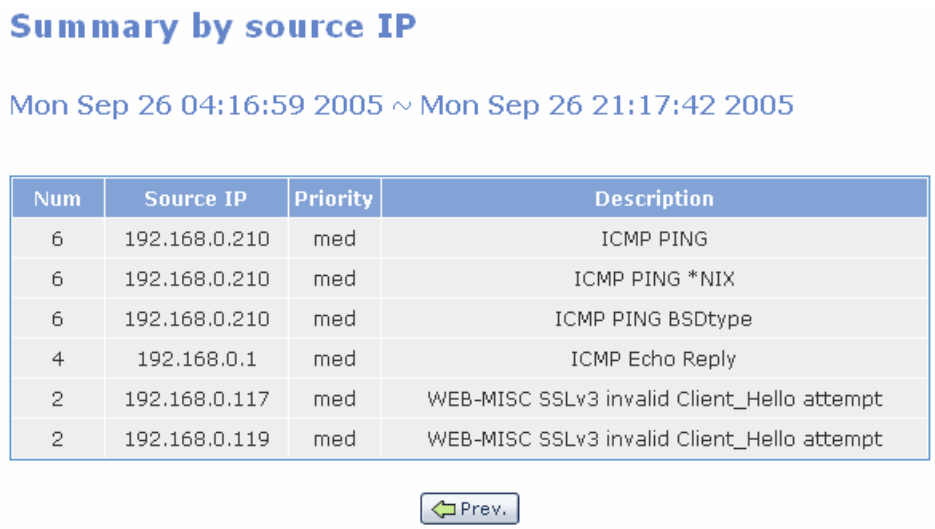
Field	Description
Rate(%)	Monitors logs detected by IDS according to type and displays logs as a percentage(%).
Num	Number of logs detected by IDS according to type.
SID	ID number for an intrusion
Priority	Risk level depending on the rules level of IDS. - high: Rule level is one day(the highest risk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



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:



Source IP Field Description

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

Destination IP Log

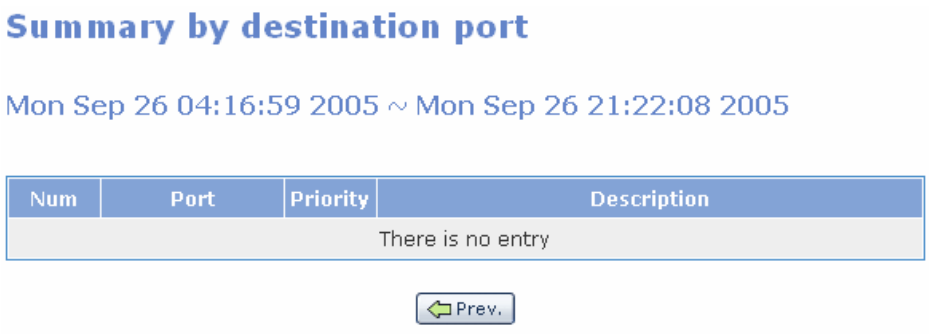
The administrator can summarize the IDS alerts by the Destination IP. If the alert log is defined by Destination IP the following window will appear.

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.

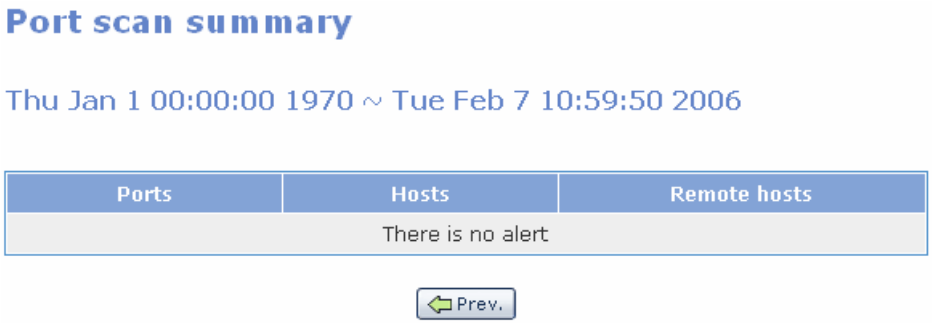


Destination Port Field Description

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.

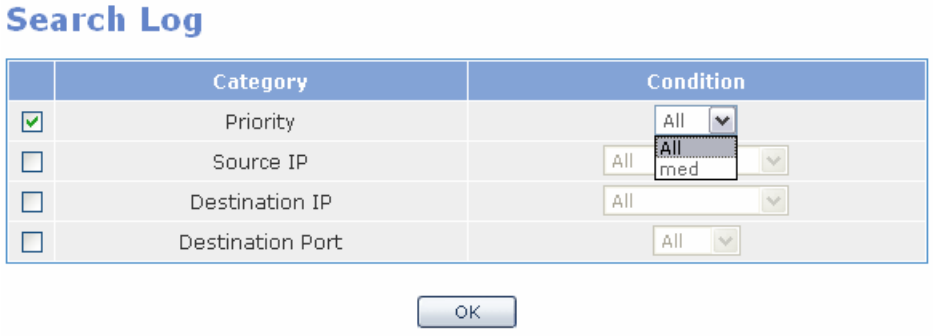


Port Scan Field Description

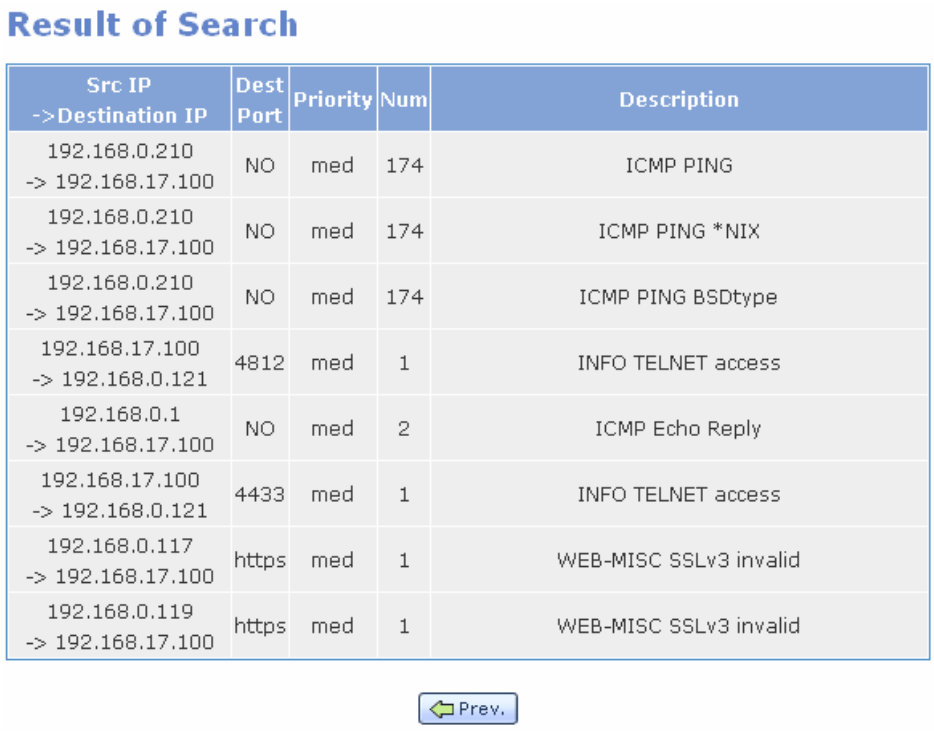
Item	Description
Ports	Number of TCP and UDP ports that are scanned in logs detected by IDS.
Hosts	Number of host that a port scanned in logs detected by IDS
Remote host	IP that attempts port scan

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.



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:



Selecting Search Condition

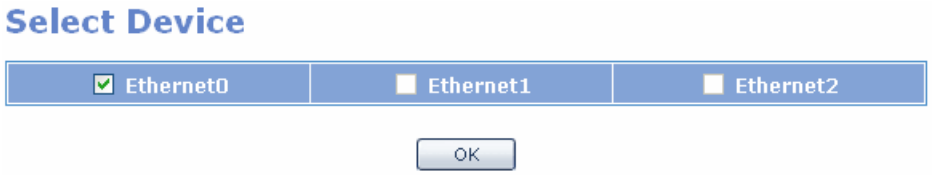
Since the conditions are not displayed dependently, the administrator cannot obtain a result that satisfies all conditions.

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

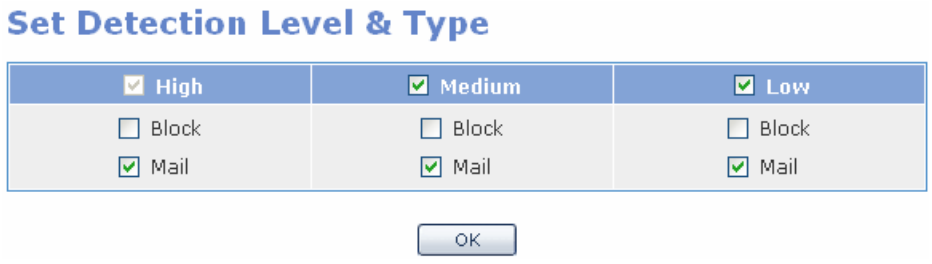
The Select Device window is used by the administrator to set up a network for IDS monitoring. The interfaces which are set up as WAN can be selected here. The administrator simply selects the check box of the Interace needing to be monitored and it is activated.



Set Detection Level & Type

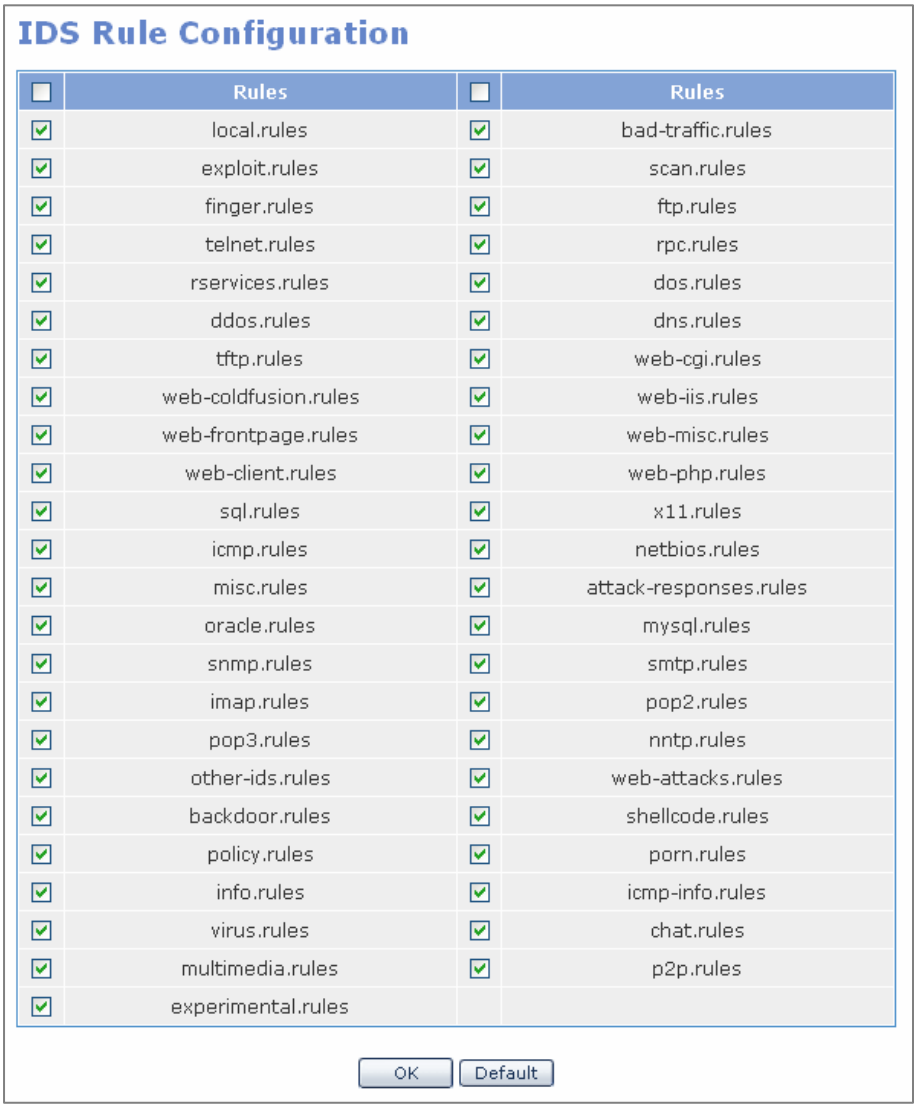
The intrusion types are classified as High, Medium and Low according to the risk level. The administrator can set up the intrusion detection levels so an alert will be generated when an intrusion exceeding the level occurs. In addition, the administrator can set up the associated operations for each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



IDS Rule Configuration

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

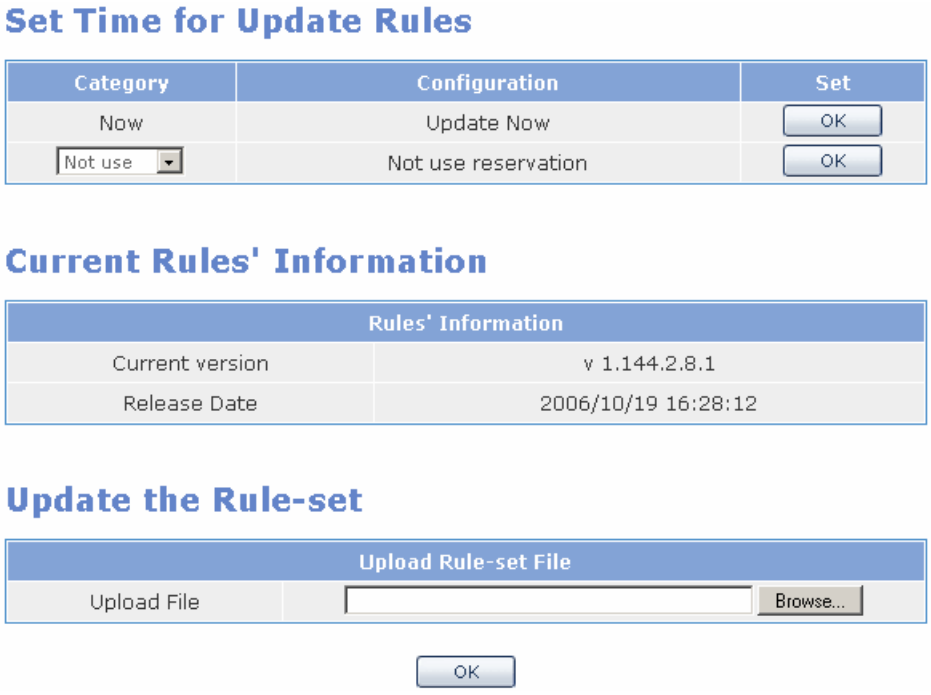


Click the box of each rule set that needs to be functioning and then click on the OK button to activate the selected rule sets.

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.



Rule Config Parameter/Field Description

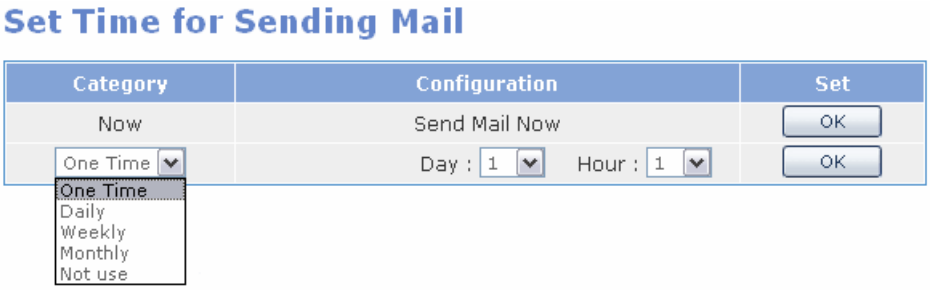
Field/Parameter	Description
Category	**Now**: Updates the IDS Rule Now
	Pull Down Menu: Can select Not use, One Time, Daily, Weekly, or Monthly
Configuration	Will change depending on the Category
Set	OK button used to implement the Category operation
Current version	Shows current IDS File Set version
Release Date	Shows current Release Date of IDS File Set
Update File	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

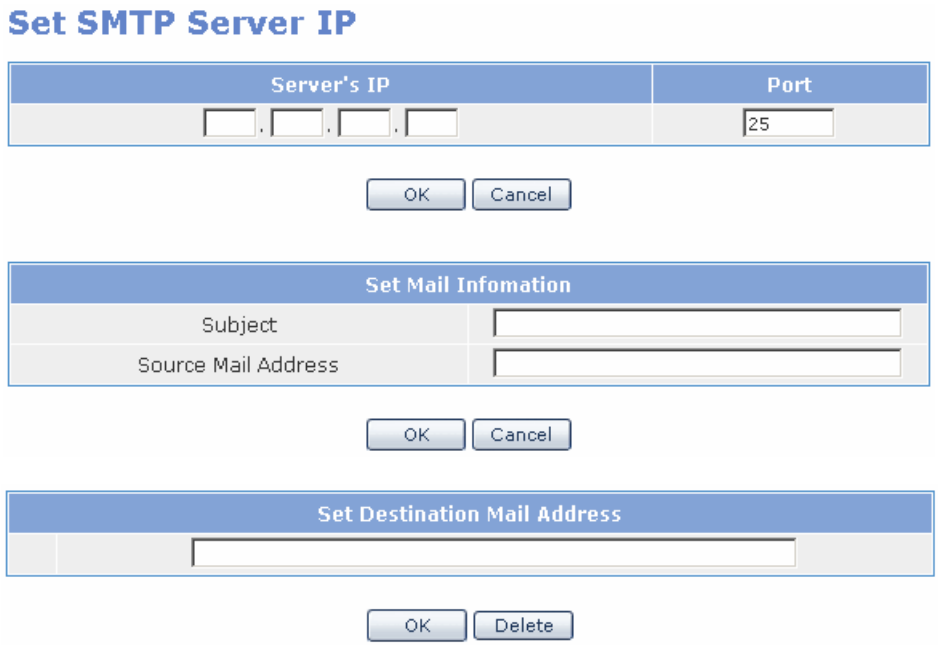
The administrator uses this window to set up when the GWIMT/GWIM will send an email to the defined SMTP server



Either click the OK buton 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.



CAUTION

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

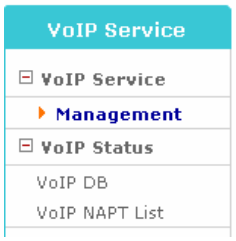
If an IP Address,is flagged as an intruder and it is blocked from accessing the system, then the IP Address will be shown in the Manage Blocked IP List.

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 GWIMT/GWIM uses this specialized feature to automatically configure NAPT, Firewall rules, strong and efficient VoIP packet inspection, and QoS. Select the **[VoIP Service]** menu to display the submenus in the upper left side of the window as follows.



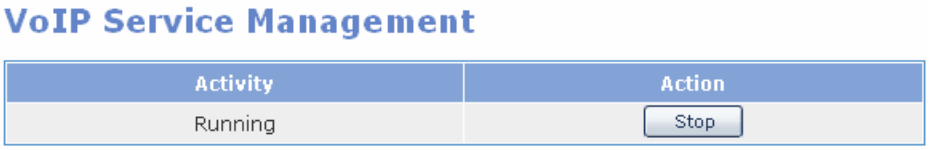
VoIP Service Menu Description

Menu	Submenu	Description
VoIP Service	Management	Used to set up the VoIP Service.
VoIP Status	VoIP Status	Used to display the configuration status of the VoIP Service.
	VoIP NAPT Status	Used to displays the configuration status of the VoIP NAPT.

VoIP Service

Management

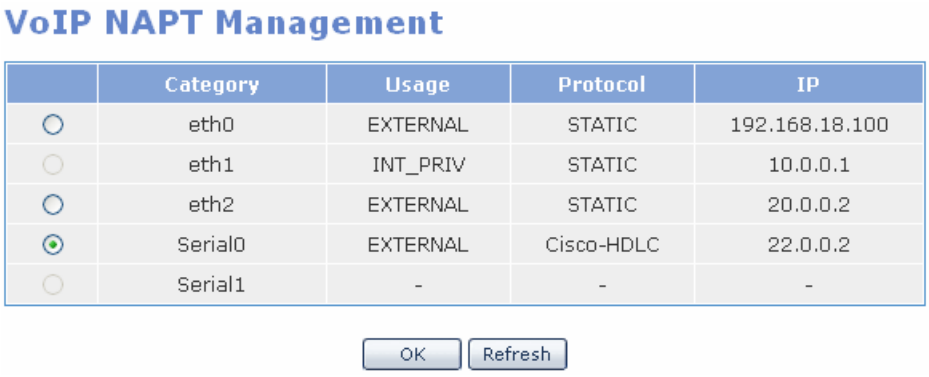
Using the **[VoIP Service]** → **[VoIP Service]** → **[Management]** submenu the system administrator can start or stop the VoIP Service. By default the VoIP Service is running after the GWIMT/GWIM finishes its booting cycle. Click the Stop or Run button to change the status of VoIP Service.



VoIP Sevice Management Field Description

Item	Description
Activity	Current VoIP service status. It is either Running (active) or Stop (inactive)
Action	Command that will change the status of the VoIP Service. Either Stop (to deactivate) or Run (to start)

In the VoIP NAPT window a WAN interface needs to be selected for VoIP Service to function. Select the WAN interface which will utilize VoIP Service and then click the OK button to save the changes. Whatever the last setting is will be restored when the system reboots.



VoIP NAPT Management Field Description

Field	Description
Category	This field displays the Interface name
Usage	This field displays the type of each interface
Protocol	This field displays the protocol type of each interface
IP	This field displays the IP Address of each interface

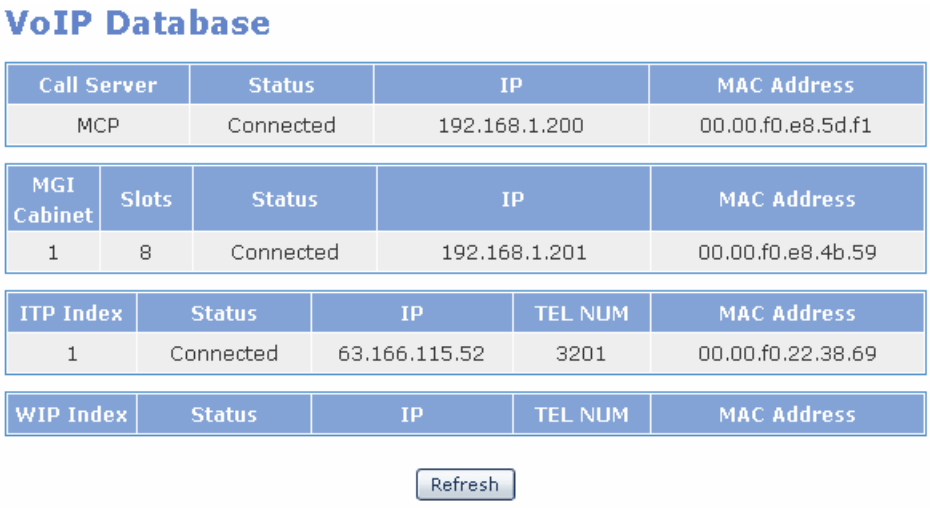
NOTE

NAPT (Network Address Port Translation)

This is a method by which many network addresses and their ports are translated into a single network address and its TCP/UDP ports

VoIP DB

Using the **[VoIP Service]** → **[VoIP Status]** → **[VoIP DB]** submenu the system administrator can display the current VoIP Service information on the OfficeServ 7400 system.



VoIP Database Field Description

Field	Description
Call Server	This field displays the type of call server
Status	This field displays the status of each card and phone
IP	This field dsplays the IP information of each card and phone
MAC Address	This field displays the MAC address information of each card and phone
MGI Slots	This field displays the slot of the MGI card
ITP Index	This field displays the index of ITP Phone
WIP Index	This field displays the index of WIP Phone
Port	This field displays the port of ITP/WIP Phone
TEL NUM	This field displays the phone number of ITP/WIP Phone

VoIP NAPT List

Using the **[VoIP Service]** → **[VoIP Status]** → **[VoIP NAPT List]** submenu the system administrator can display the NAPT items for VoIP Service . The service connects 64 internal ports and external ports to each MGI card through one to one mapping. There are also multiple IP ports forwaded to the MCP card. The following table shows a basic VoIP NAPT list with (1) MGI 64 and an MP40 card.

NAPT List for VoIP

Index	Public IP	Protocol	StartPort	EndPort	Internal IP	StartPort	EndPort
1	216.62.86.140	tcp	6100		192.168.1.200	6100	
2	216.62.86.140	udp	6000		192.168.1.200	6000	
3	216.62.86.140	tcp	6000		192.168.1.200	6000	
4	216.62.86.140	udp	9000		192.168.1.200	9000	
5	216.62.86.140	udp	1719		192.168.1.200	1719	
6	216.62.86.140	tcp	1720		192.168.1.200	1720	
7	216.62.86.140	udp	5060		192.168.1.200	5060	
8	216.62.86.140	tcp	5060		192.168.1.200	5060	
9	216.62.86.140	tcp	5000		192.168.1.200	5000	
10	216.62.86.140	udp	60896	61023	192.168.1.201	30000	30127

NAPT Ports

Please refer to the OS 7400 Special Applications Manual for a listing and description of all IP Ports that the OS 7400 uses.

NAPT List for VoIP Field Description

Field	Description
Public IP	This field displays the external IP Address which communicates with the external environment
Public Start Port	This field displays the port number for the external source IP to communicate with external media
Public End Port	This field displays the last external source port number.
Internal IP	This field displays the Internal IP Address that VoIP Service uses inside the GWIMT/GWIM firewall
Internal Start Port	This field displays the IP port number for the internal IP Address that VoIP Service uses
Internal End Port	This field displays the last IP port number for the Internal IP Address that VoIP Service uses.

SIP ALG Menu

SIP-capable firewalls such as the GWIMT/GWIM use the SIP ALG (Application Level Gateway) architecture, to solve firewall traversal by “taking care of the SIP packets on-the-fly,” making sure that they reach the right destination on the LAN. Select the **[SIP AGP]** menu to begin configuring SIP ALG. The submenus will be displayed in the upper left side of the window as follows:

SIP ALG Menu Description

Menu	Description
Config	Used to set up the SIP environment.
Management	Used to start or stop the SIP AGP service.

NOTE

SIP ALG(SIP aware ALG)

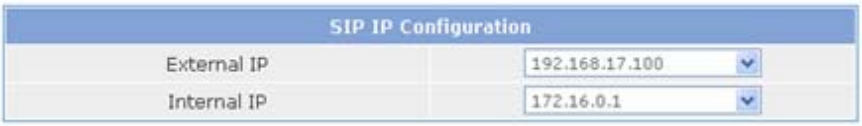
The firewall protects the internal network based on NAT so it is is safe from external attacks and resolves the limits on the services so that SIP devices behind the firewall can communicate with external devices.

Config

Using the **[SIP ALG]** → **[Configuration]** submenu the administrator can set up the SIP environment on the GWIMT/GWIM. Set the following items and then click the OK button to save the changes.

SIP Configuration

This window displays the firewall installation data.



The external IP and internal IP Address choices are displayed using the pull down menus so that the administrator can view and select the usable information from the firewall configuration. Select an External IP and an Internal IP and then click the OK button.

Map LIST

Enter the SIP data for the SIP network devices inside of the firewall.

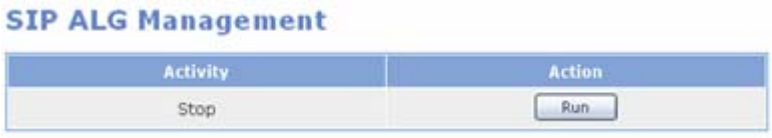
If an IP address or phone number is not entered into the Number(ID) field then the 'default' ID will be used. The IP Address of the Call Server (OS 7400 MP40) should be entered in the 'default' IP field.

Click the Add button to add more Map information.

If a Map entry must be removed then check the check box to the left of the ID and then click the Delete button.

Management

The **[SIG ALG]** → **[Management]** submenu is used to start and stop the SIP ALG. service.



SIP ALG Management Field Description

Field	Description
Activity	Current status of SIP ALG
Action	Command that is available to execute in current status

System Menu

The System Menu is used to import or export the GWIM/GWIMT database, to view system logs, to configure the DHCP server and relay functions, 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:

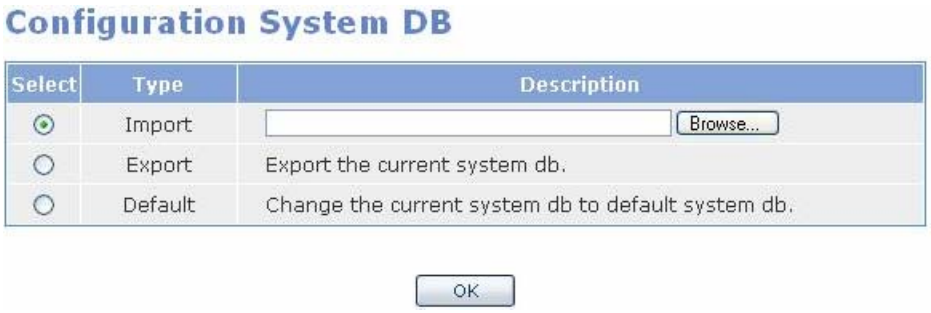
System Menu Description

Menu	Submenu	Description
DB Config		Manages the current configuration DB of GWIMT/GWIM
Admin Config		Sets 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
DHCP Server	Configuration	Used to define and edit the DHCP scope
	Management	Used to start or stop the DHCP server

Menu	Submenu	Description
	Lease Info	Used to display DHCP Lease status
DHCP Relay	Configuration	Used to define the DHCP Relay settings
	Management	Used to start or stop the DHCP Relay
Time Configuration	NTP Config	Used to enter the NTP server info
	Manual Config	Used to manually configure time
	Timezone	Used to set the GWIMT/GWIM timezone
Upgrade		Used to upgrade the GWIMT/GWIM software
Appl Server		Used to allow SSH, FTP, and Telnet access to the GWIMT/GWIM
Reboot		Used to Reboot the GWIMT/GWIM

DB Config

Use the **[System] → [DB Config]** submenu to export the GWIMT/GWIM database, to import the GWIMT/GWIM database, or to default the GWIMT/GWIM to the factory defaults.



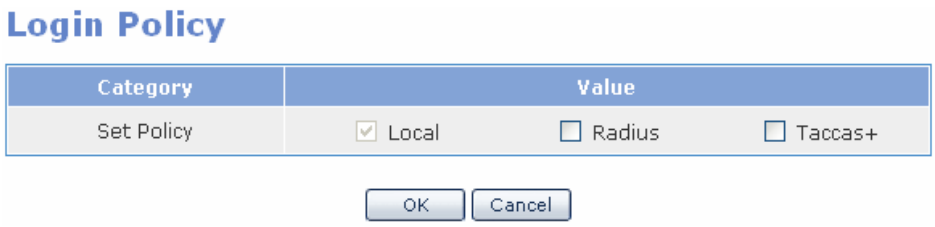
DB Config Parameter Description

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 GWIM is defaulted the adminstrator 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 GWIMT/GWIM 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.



Local

The local password is the Admin password that is used to access the GWIMT/GWIM router using Telnet, SSH, FTP, and Web Management. Enter the new password and then click the OK button to save the change.

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.

Taccas+

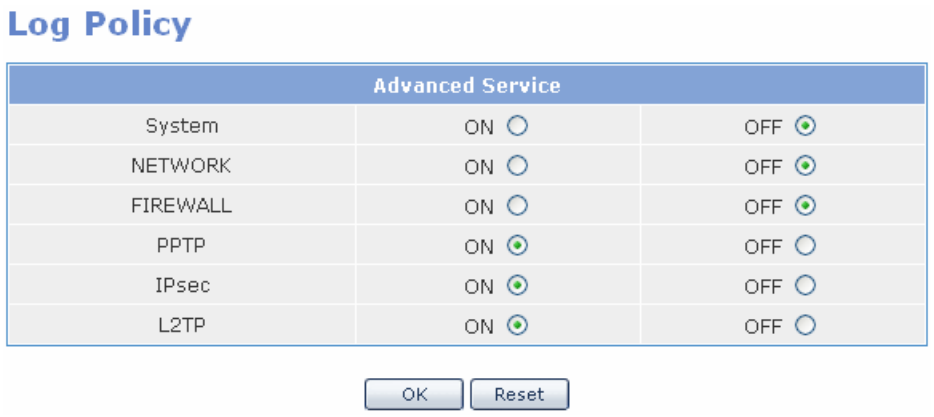
If Taccas+ will be used then select the Taccas+ box. Enter the information for the Taccas+ authentication method. Up to 5 lists can be entered. When deleting the list of all the server IPs, the corresponding secret key values are also deleted.

Log

The **[Log]** submenu is used to configure the system log by selecting specific GWIMT/GWIM attributes, to run system log reports, and to download a system log report to a file.

Configuration

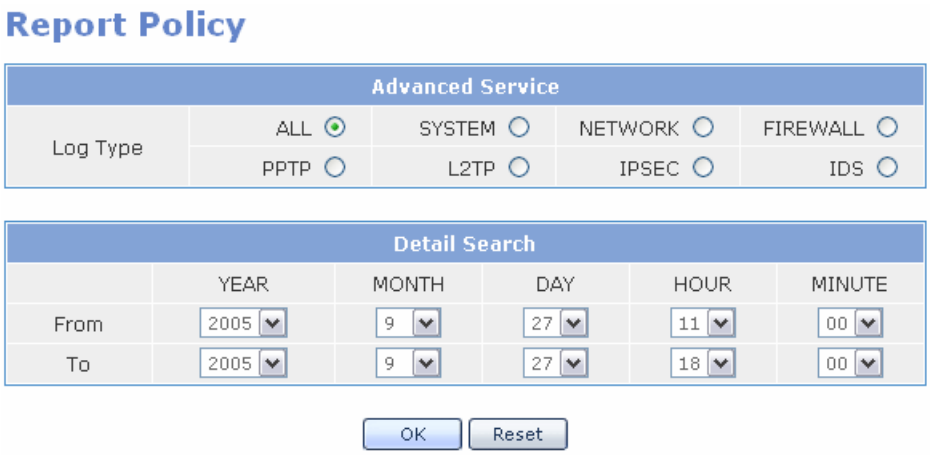
The **[System]** → **[Log** → **[Configuration]** submenu is used to determine which system attributes will be included in the system log.



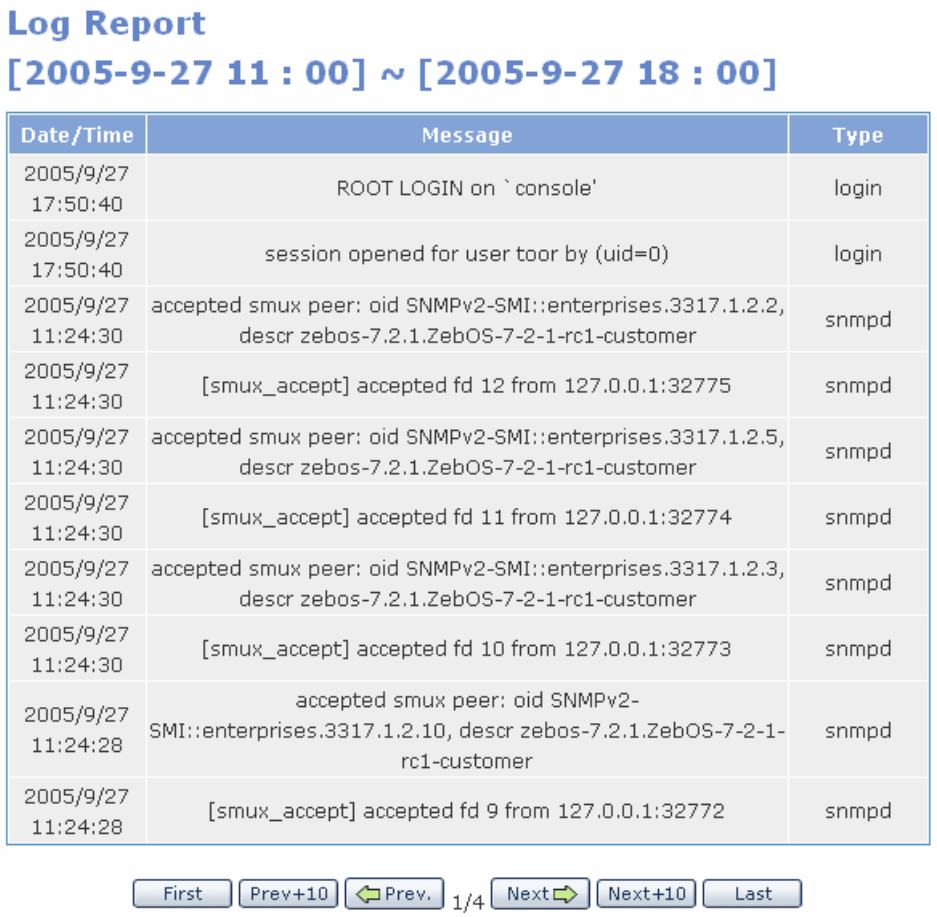
Click the ON or OFF radio button to include or ignore the GWIMT/GWIM attribute. The choices are System , NETWORK, FIREWALL, PPTP, IPSec, and L2TP. Once the radio buttons are selected then click the OK button to apply the changes.. Click the Reset button to return the Log Policy to the previous status 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.

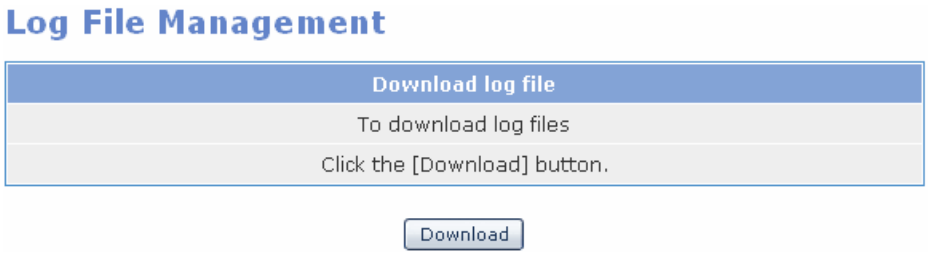


Click the radio button for the desired log type and then select the date and time. Then click the OK button to run the report. Click the Reset button to return the log report settings to default.



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.

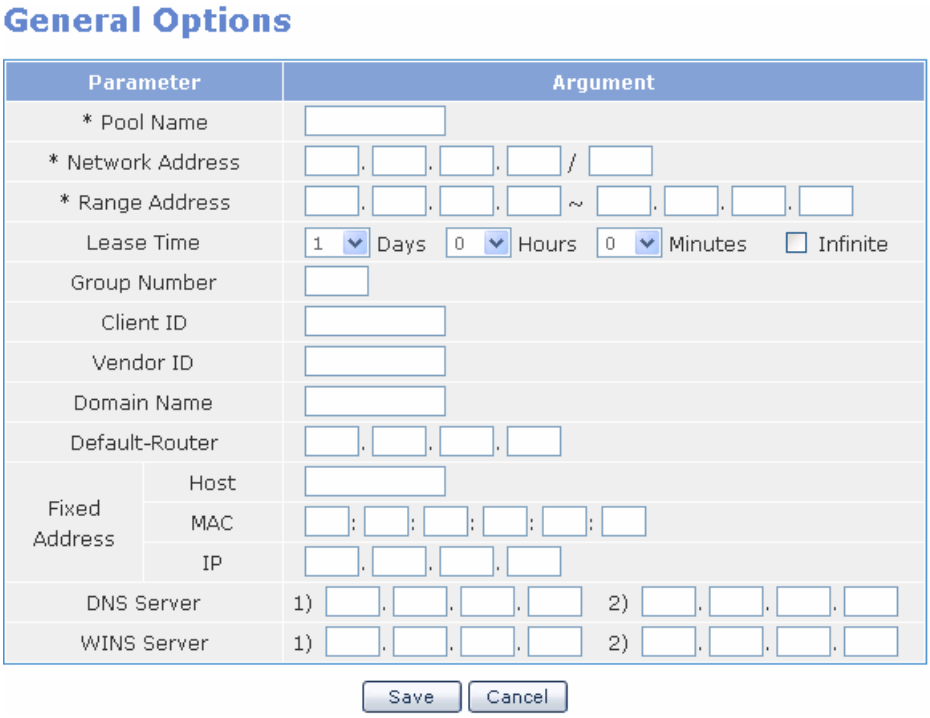


DHCP Server

The **[System] → [DHCP Server]** submenus are used to configure and edit the DHCP scope (Pool), to start and stop the DHCP server, and to track the DHCP Lease status for the network devices which acquire IP addresses using DHCP. .

Configuration

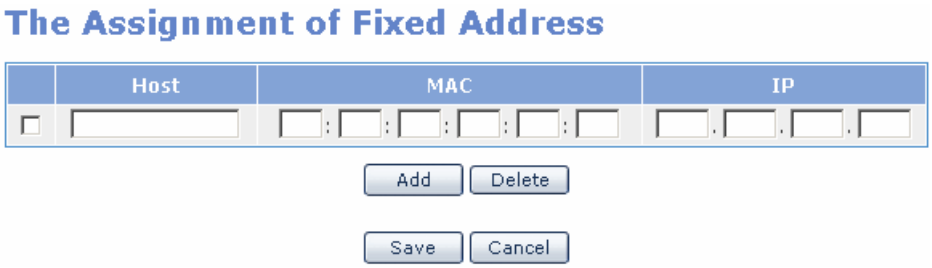
The **[System] → [DHCP Server] →[Configuration]** submenu allows the administrator to set various configuration items for the DHCP Server. The Pool Name, Network Address and Range Address are all required fields in DHCP Server configuration and are designated with an asterisk.



General Options Parameter Description

Parameter	Description
*** Pool Name**	Used to set up the name of Pool to distinguish it from the other Pools.
*** Network Address**	Used to enter the value of a Network number. The value is classified into IP type and Netmask.
*** Range Address**	Used to set up the range of IP addresses that the DHCP Server allocates to DHCP Clients. Enter the first/last IP addresses to be allocated in order to designate the range.
Lease Time	Used to set up the duration of the DHCP Lease. The default lease time is 1 Day.
Client ID	Used to set up a Client Identifier.
Vendor ID	Used to sets up a Vendor Class Identifier.
Domain Name	Used to set up a Domain Name.
Default-Router	Used to set up the IP address of the Default Router.
DNS Server	Used to set up the DNS Server/s.
WINS Server	Used to set up the WINS Server/s.

The Fixed Address assignments are used for allocating a fixed IP address for a specific client.

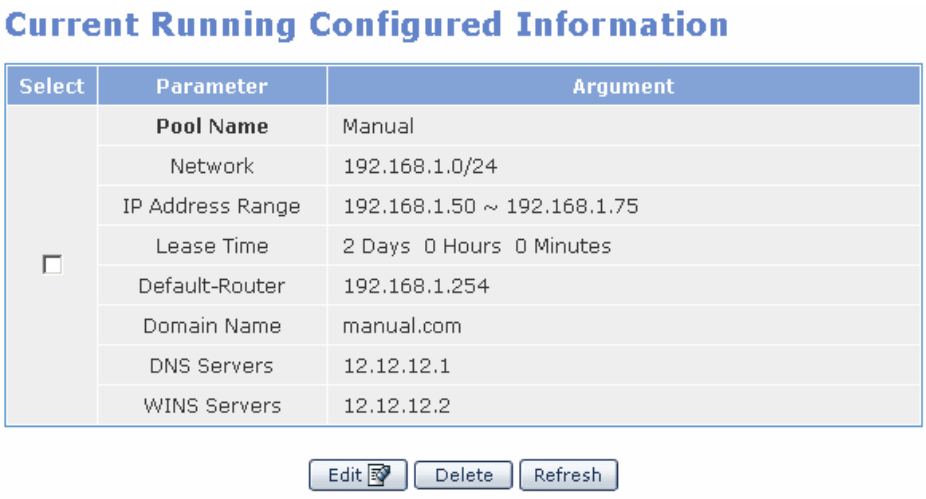


Assignment of Fixed Address Parameter Description

Parameter		Description
Fixed Address	**Host**	Used to set up the Name of Host.
	MAC	Used to set up the MAC address of a specific client.
	IP	Used to set up the IP Address to be allocated.

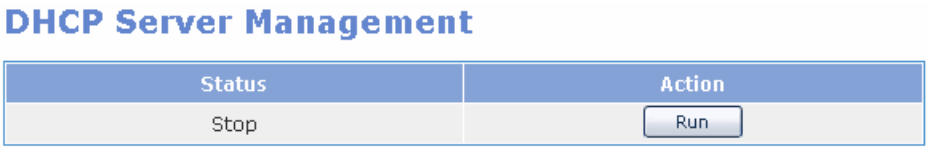
.

The Current Running Configured Information window is used to view, edit, or delete existing DHCP Pools. If a Pool needs to be deleted or modified check the box to the left in the Pool window and then click the Edit or Delete button.



Management

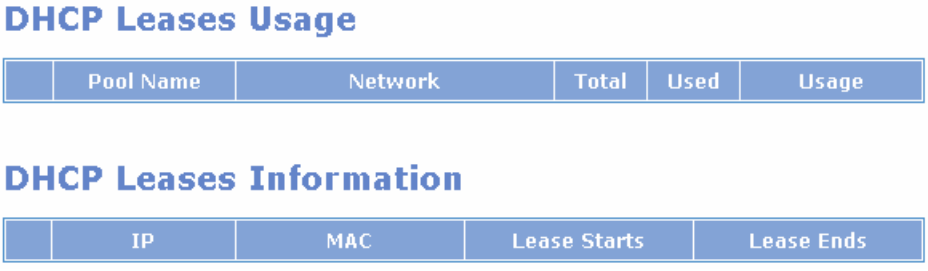
The **[System] → [DHCP Server] → [Management]** submenu is used by the system administrator to start or stop the DHCP server.



Click the Run button to start the DHCP Server and click the Stop button to halt the DHCP server

Lease Info

The **[System] → [DHCP Server] → [Lease Info]** submenu is used to view the active Lease information.



DHCP Relay Agent

The **[System]** → **[DHCP Relay Agent]** submenus are used to configure DHCP Relay feature..

Configuration

By using the **[System]** → **[DHCP Relay Agent]** → **[Configuration]** submenu the administrator can begin to configure the DHCP Relay Agent settings. First designate an interface which will accept DHCP leases from a DHCP Server. Click the add button if more interfaces need to be added to the list. If an interface needs to be removed from the list then check the box for that interface and then click the Delete button.

Then add the DHCP Server/s which will be handing out the DHCP leases into the Server List, If more than one DHCP server is going to be used then click the Add button and enter the IP Address of the additional server/s. If a DHCP server needs to be removed from the server list then check the box for that server and then click the Delete button.

Management

By using the **[System]** → **[DHCP Relay Agent]** → **[Management]** submenu the administrator can start or stop the DHCP Relay Agent service.

Click the Run button to start the DHCP Relay Agent and click the Stop button to halt the DHCP Relay Agent.

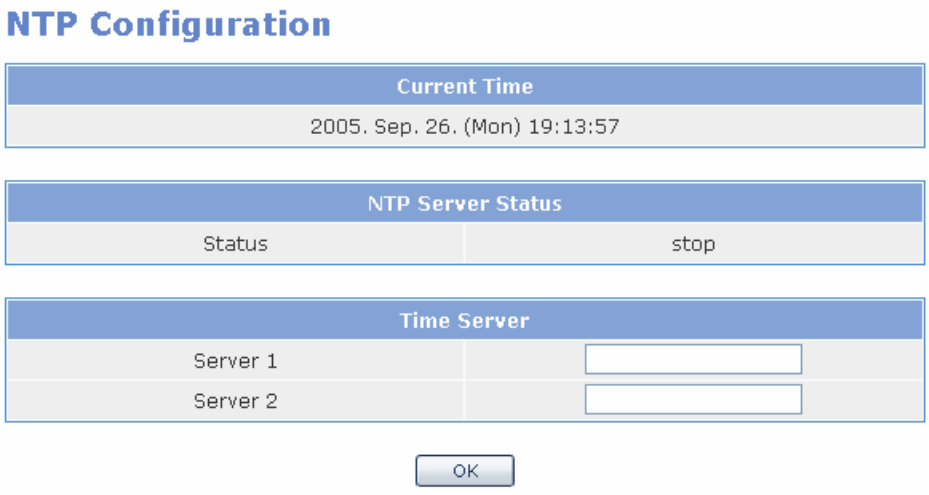
Time Configuration

Using the **[System]** → **[Time Configuration]** submenu the system administrator can either synchronize the date and time of the GWIMT/GWIM with a NTP server or manually set the date and time.

NTP Config

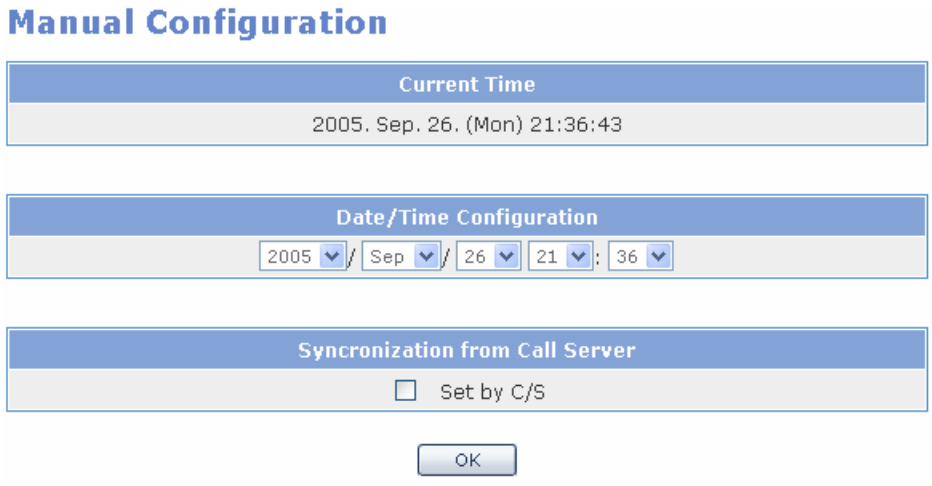
Use the **[System]** → **[Time Configuration]** → **[NTP Config]** submenu to set up a NTP Time Server/s to synchronize the date and time with the GWIMT/GWIM. The Current Time window indicates the current date and time of the GWIMT/GWIM. The NTP Server Status window indicates the status of NTP Server 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.



Manual Config

By using the **[System] → [Time Configuration] → [Manual Config]** submenu the administrator can manually set and modify the date and time of the GWIMT/GWIM. 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..

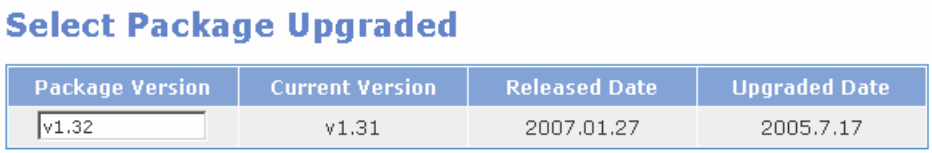


Timezone

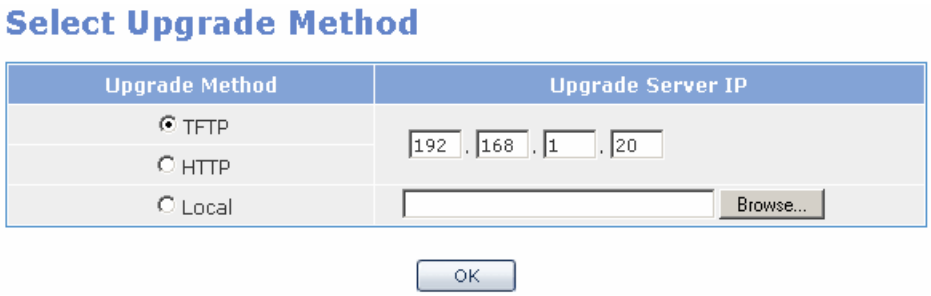
By using the **[System] → [Time Configuration] → [Timezone]** submenu the administrator can change Time Zones by selecting the desired timezone and then by clicking the OK button to save the change.

Upgrade

Upgrading the GWIMT/GWIM 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.



Then select one of the three types of upgrade methods (TFTP, HTTP, or Local). If the Upgrde method is TFTP or HTTP enter the correct IP address of the server. Then click the OK button to start the upgrade process.



Appl Server

Using the **[System] → [Appl Server]** submenu the administrator can control remote access to the GWIMT/GWIM 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.

Check the box of the access method and then click the OK button to save the change.

Reboot

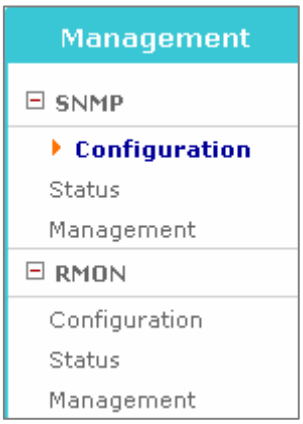
Using the **[System]** → **[Reboot]** submenu the administrator can reboot the GWIMT/GWIM.

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

Management Menu

The SNMP and RMON settings are configured and managed using the **[Management]** menu. The submenus will be displayed in the upper left side of the window as follows:



Management Menu Description

Menu	Submenu	Description
SNMP	Configuration	Used to display the configuration items of SNMP.
	Status	Used to displays the SNMP configuration currently configured.
	Management	Used to starts or stop the SNMP service.
RMON	Configuration	Used to display the configuration items of RMON.
	Status	Used to display the RMON configuration currently configured.
	Management	Used to start or stop the RMON services.

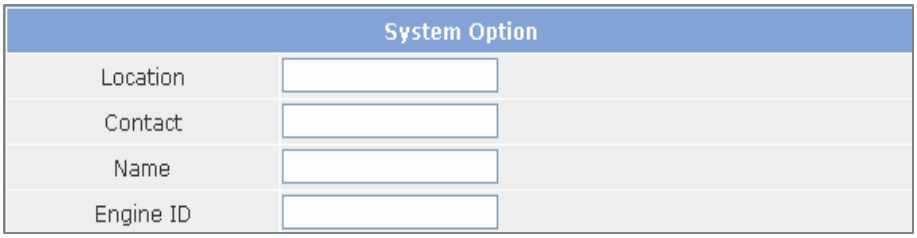
SNMP

Configuration

SNMP is a set of protocols used for managing complex networks. The **[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.



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

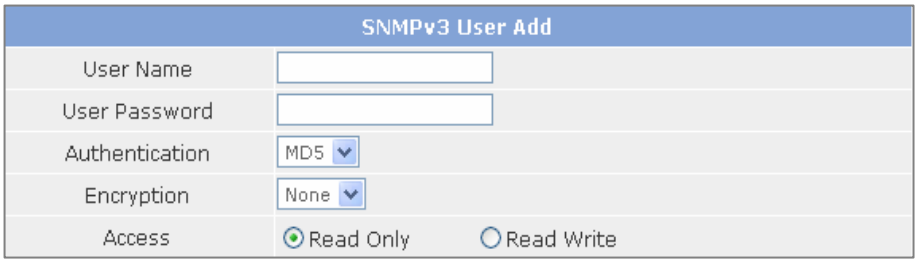
The following window is used to add new community information used in SNMP v1/2c.

Community 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.



SNMP v3 Parameter Description

Parameter	Description
Administrator Name	Used to enter the new administrator's name
Administrator Password	Used to enter the new administrator's password (8 alphanumeric characters)
Authentication	Used to set up the authentication method.
Encryption	Used to set up the ciphering method.
Access	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 Parameter Description

Parameter	Description
IP Address	Used to set up a new Trap IP Address
Community Name	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 Infomation	
Location	Seoul, Korea
Contact	support@
Name	OS7400-GSIM
Engine ID	GSIM

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

Select	User Name	Access
	root	Read Write

Select	Trap IP	Trap Port
☐	192.168.0.123	162

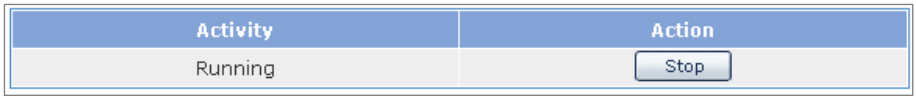
Status Field Description

Field	Description
System Information	This field displays the information set up for the System Options.
Select	Used to select the information to delete.
Community Name	This field display the community name.
Community Net	This field displays the configured name of the Community Network.
Community Access	This field displays the access authority of the configured community.
Administrator Name	This field displays the configured administrator's name.
Access	This field displays the access authority of the configured administrator.
Trap IP	This field displays the configured Trap IP.
Trap Port	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



SNMP Management Field Description

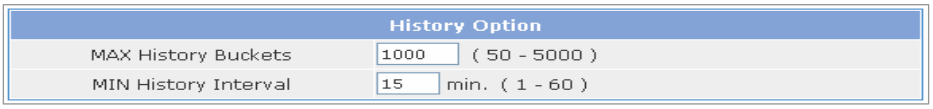
Field	Description
Activity	This field displays the operational condition of the SNMPservice.
Action	Used to select whether to start or stop SNMP.

RMON

Configuration

Remote Monitoring *(RMON)* is a standard monitoring specification that enables various network monitors and console systems to exchange network-monitoring data. RMON provides network administrators with more freedom in selecting network-monitoring probes and consoles with features that meet their particular networking needs. Use the **[Management]** → **[RMON]** → **[Configuration]** submenu to begin configuring RMON.

Enter the History and Event Options and then click the Save button to apply the changes. Click the Reset button To initialize the RMON.



History Option

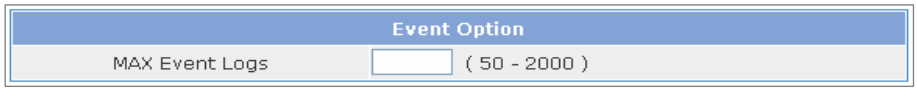
The History Option window is used to set up the RMON history options.

RMON Configuration Parameter Description

Parameter	Description
MAX History Buckets	Used to set up the maximum history storage space.
MIN History Interval	Used to set up the minimum history sample collection cycle.

Event Options

The Event Options window is used to set up the RMON event options.

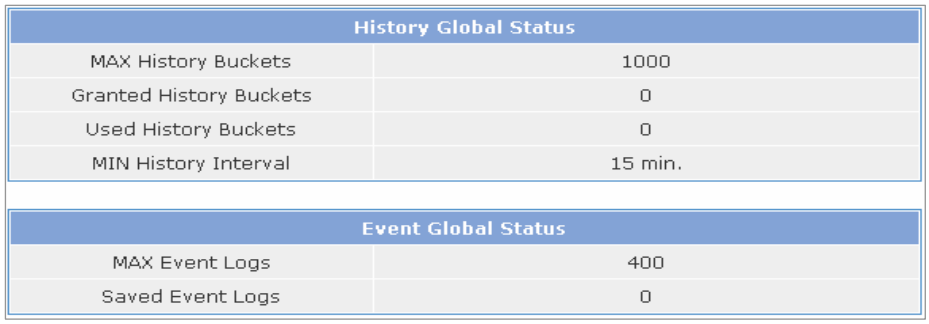


RMON Event Options Parameter Description

Parameter	Description
Max Event Logs	Used to set up the maximum number of Event Logs.

Status

The **[Management]** → **[RMON]** → **[Status]** submenu is used to view the RMON System Configuration.



RMON Global Status Field Description

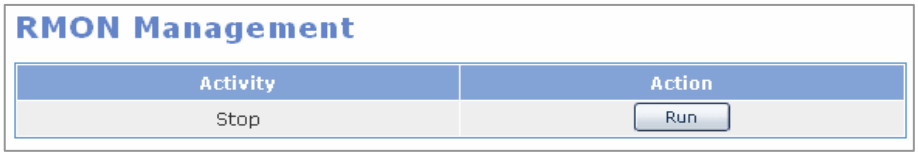
Field	Description
MAX History Buckets	This field displays the maximum history storage space that has been set up.
Granted History Buckets	This field displays the history storage space that is currently allocated.
Used History Buckets	This field displays the history storage space that is currently used.
MIN History Interval	This field displays the minimum history sample collection cycle.
Max Event Logs	This field displays the maximum number of logs that are set up.
Saved Event Logs	This field displays the number of logs that is currently stored.

Management

The **[Management]** → **[RMON]** → **[Management]** submenu is used to start and stop the SNMP service. Click the Run button to start the RMON service and click the Stop button to halt the RMON service.

RMON Management

The administrator can start/stop the RMON service.

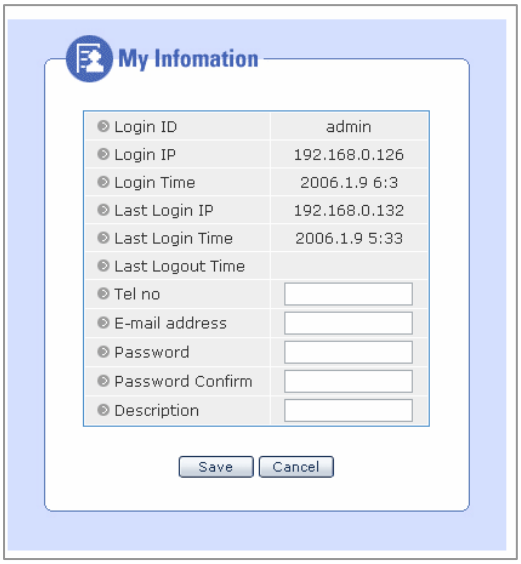


RMON Management Field Description

Item	Description
Activity	This field displays the operational status of the current service.
Action	Used to to start or stop RMON.

My Info Menu

Click the My Info icon on the upper right hand side of the GWIMT/GWIM Web Page to open the My Info window. In this window administrators can enter a telephone number, an E-mail address, and desciption of the router . This window is also used to enter the admin password which is used when logging into the GWIMT/GWIM router. Enter the new admin password into the Password and Password Confirm fields and then click the Save button.



My Info Parameters

Item	Description
Login ID	This field displays the login ID.
Login IP	This field displays the IP address of the PC logged into the GWIMT/GWIM.
Login Time	This field displays time when the login occued.
Last Login IP	This field displays the last login IP address.
Last Login Time	This field displays the last login time.
Last Logout Time	This field displays the last logout time.
Tel no	Used to enter the Telephone No. of the administrator
E-mail address	Used to enter the E-mail address of the administrator
Password	Used to enter the Password to be modified
Password Confirm	Used to enter the Password again to confirm the change
Description	Used to enter a Description of the Router

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

GWIMT/GWIM	Gigabit WAN Interface Module
GVRP	GARP VLAN Registration Protocol

H

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

I

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

L

LAN	Local Area Network
L2TP	Layer 2 Tunneling Protocol

N

NAT	Network Address Translation
NTP	Network Time Protocol

R

RMON	Realtime Monitoring
RP	Rendezvous Pointv
RSTP	Rapid Spanning Tree Protocol

P

PAP	Password Authentication Protocol
PIM-SM	Protocol Independent Multicast-Sparse Mode
PD	Power Device
PoE	Power Of Etnernet
PPTP	Point to Point Tunneling Protocol
PT	Protocol Translation
PVC	Permanent Virtual Circuit
PVID	Port VLAN Identification

S

STP	Spanning Tree Protocol
SMTP	Simple Mail Transfer Protocol
SNAT	Source Network Address Translation
SNMP	Simple Network Management Protocol
SPQ	Strict Priority Queuing

T

TFTP	Trivial File Transfer Protocol

V

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