



# **Multi-Homing Security Gateway MH-2001**

## **User's Manual**

## Copyright

Copyright© 2007 by PLANET Technology Corp. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written permission of PLANET.

PLANET makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not this company, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, this company reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.

## Disclaimer

PLANET Technology does not warrant that the hardware will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose.

PLANET has made every effort to ensure that this User's Manual is accurate; PLANET disclaims liability for any inaccuracies or omissions that may have occurred.

Information in this User's Manual is subject to change without notice and does not represent a commitment on the part of PLANET. PLANET assumes no responsibility for any inaccuracies that may be contained in this User's Manual. PLANET makes no commitment to update or keep current the information in this User's Manual, and reserves the right to make improvements to this User's Manual and/or to the products described in this User's Manual, at any time without notice.

If you find information in this manual that is incorrect, misleading, or incomplete, we would appreciate your comments and suggestions.

## Trademarks

The PLANET logo is a trademark of PLANET Technology.

This documentation may refer to numerous hardware and software products by their trade names. In most, if not all cases, these designations are claimed as trademarks or registered trademarks by their respective companies.

## CE mark Warning

This is a class B device, in a domestic environment; this product may cause radio interference, in which case the user may be required to take adequate measures.

## Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio technician for help.

## FCC Caution:

To assure continued compliance (example-use only shielded interface cables when connecting to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the Following two conditions: (1) This device may not cause harmful interference, and (2) this Device must accept any interference received, including interference that may cause undesired operation.

## R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/EC OF THE EUROPEAN PARLIAMENT AND THE COUNCIL OF 9 March 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE)

The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

## WEEE Caution



To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

## Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

## Customer Service

For information on customer service and support for the Multi-Homing Security Gateway, please refer to the following Website URL:

<http://www.planet.com.tw>

Before contacting customer service, please take a moment to gather the following information:

- ◆ Multi-Homing Security Gateway serial number and MAC address
- ◆ Any error messages that displayed when the problem occurred
- ◆ Any software running when the problem occurred
- ◆ Steps you took to resolve the problem on your own

## Revision

User's Manual for PLANET Multi-Homing Security Gateway

Model: MH-2001

Rev: 1.0 (April, 2007)

## Table of Contents

<b>CHAPTER 1: INTRODUCTION .....</b>	<b>1</b>
1.1 FEATURES .....	1
1.2 PACKAGE CONTENTS .....	2
1.3 MH-2001 FRONT VIEW .....	2
1.4 MH-2001 REAR PANEL .....	3
1.5 SPECIFICATION .....	4
<b>CHAPTER 2: HARDWARE INSTALLATION.....</b>	<b>5</b>
2.1 INSTALLATION REQUIREMENTS .....	5
2.2 OPERATION MODE .....	6
2.2.1 <i>Transparent Mode Connection Example</i> .....	6
2.2.2 <i>NAT Mode Connecting Example</i> .....	7
<b>CHAPTER 3: GETTING STARTED .....</b>	<b>8</b>
3.1 WEB CONFIGURATION .....	8
3.2 CONFIGURE WAN 1 INTERFACE .....	9
3.3 CONFIGURE WAN 2 INTERFACE .....	11
3.4 CONFIGURE DMZ INTERFACE .....	11
3.5 CONFIGURE POLICY .....	11
<b>CHAPTER 4: SYSTEM .....</b>	<b>13</b>
4.1 ADMINISTRATION.....	13
4.1.1 <i>Admin</i> .....	13
4.1.2 <i>Permitted IPs</i> .....	16
4.1.3 <i>Software Update</i> .....	17
4.2 CONFIGURE .....	18
4.2.1 <i>Setting</i> .....	18
4.2.2 <i>Date/Time</i> .....	24
4.2.3 <i>Multiple Subnet</i> .....	25
4.2.4 <i>Route Table</i> .....	28
4.2.5 <i>DHCP</i> .....	29
4.2.6 <i>Dynamic DNS</i> .....	30
4.2.7 <i>Host Table</i> .....	32
4.2.8 <i>Language</i> .....	32
4.3 LOGOUT .....	33
<b>CHAPTER 5: INTERFACE.....</b>	<b>34</b>



---

5.1 LAN .....	34
5.2 WAN.....	35
5.3 DMZ .....	40
<b>CHAPTER 6: POLICY OBJECT .....</b>	<b>42</b>
6.1 ADDRESS .....	42
6.1.1 LAN.....	42
6.1.2 LAN Group.....	44
6.1.3 WAN .....	45
6.1.4 WAN Group.....	46
6.1.5 DMZ.....	47
6.1.6 DMZ Group.....	49
6.1.7 Example1.....	51
6.1.8 Example2.....	53
6.2 SERVICE .....	56
6.2.1 Pre-defined.....	56
6.2.2 Custom.....	57
6.2.3 Group.....	58
6.3 SCHEDULE .....	60
6.4 QoS.....	61
6.5 AUTHENTICATION .....	63
6.5.1 Auth Setting.....	63
6.5.2 Auth User.....	64
6.5.3 Auth User Group.....	67
6.5.4 Radius Server.....	70
6.5.5 POP3.....	90
6.6 CONTENT BLOCKING .....	92
6.6.1 URL Blocking.....	92
6.6.2 Script Blocking.....	94
6.6.3 Download Blocking.....	95
6.6.4 Upload Blocking.....	96
6.7 IM/P2P BLOCKING .....	97
6.8 VIRTUAL SERVER.....	98
6.8.1 Mapped IP .....	99
6.8.2 Virtual Server 1- 4.....	102
6.9 VPN.....	104
6.9.1 Example.1.....	111
6.9.2 Example.2.....	124
6.9.3 Example.3.....	182
6.9.4 Example.4.....	195

6.9.5 Example.5.....	208
6.9.6 Example.6.....	218
<b>CHAPTER 7: POLICY .....</b>	<b>235</b>
7.1 OUTGOING .....	238
7.2 INCOMING .....	242
7.3 WAN To DMZ & LAN To DMZ .....	244
7.4 DMZ To WAN & DMZ To LAN .....	247
<b>CHAPTER 8: ANOMALY FLOW IP .....</b>	<b>253</b>
<b>CHAPTER 9: MONITOR .....</b>	<b>261</b>
9.1 LOG.....	261
9.1.1 Traffic Log.....	262
9.1.2 Event.....	264
9.1.3 Connection Log.....	266
9.1.4 Log Backup.....	268
9.2 ACCOUNTING REPORT.....	270
9.2.1 Setting.....	270
9.2.2 Outbound.....	273
9.2.3 Inbound .....	277
9.3 STATISTICS .....	280
9.3.1 WAN Statistics.....	281
9.3.2 Policy Statistics.....	284
9.4 WAKE ON LAN.....	286
9.5 STATUS .....	287
9.5.1 Interface Status.....	287
9.5.2 Authentication.....	289
9.5.3 ARP Table.....	290
9.5.4 DHCP Clients .....	291

## Chapter 1: Introduction

As Internet become essential for your business, the only way to prevent your Internet connection from failure is to have more than one connection. PLANET's Multi-Homing Security Gateway MH-2001 reduces the risk of potential shutdown if one of the Internet connections should fail. In addition, they allow you to perform load-balancing by distributing the traffic through two WAN connections.

Not only is a multi-homing device, PLANET's MH-2001 also provides a complete security solution in a box. The policy-based firewall, Intrusion detection and prevention, content filtering function and VPN connectivity with 3DES and AES encryption make it become a perfect product for your network security. No more complex connection and settings for integrating different security products on the network is required.

Bandwidth management function is also supported on MH-2001 to offers network administrators an easy and powerful means to allocate network resources based on business priorities, and to shape and control bandwidth usage.

### 1.1 Features

- ◆ **WAN Backup:** The MH-2001 can monitor each WAN link status and automatically activate backup links when a failure is detected. The detection is based on the configurable target Internet addresses.
- ◆ **Outbound Load Balancing:** The network sessions are assigned based on the user configurable load balancing mode, including "Auto", "Round-Robin", "By Traffic", "By Session", "By Packet", "By Source IP" and "By Destination IP". User can also configure which IP or TCP/UDP type of traffic use which WAN port to connect.
- ◆ **Policy-based Firewall:** The built-in policy-based firewall prevent many known hacker attack including SYN attack, ICMP flood, UDP flood, Ping of Death, etc. The access control function allowed only specified WAN or LAN users to use only allowed network services on specified time.
- ◆ **VPN Connectivity:** The security gateway support PPTP and IPSec VPN. With DES, 3DES and AES encryption and SHA-1 / MD5 authentication, the network traffic over public Internet is secured.
- ◆ **Content Filtering:** The security gateway can block network connection based on URLs, Scripts (The Pop-up, Java Applet, cookies and Active X), P2P (eDonkey, Bit Torrent and WinMX), Instant Messaging (MSN, Yahoo Messenger, ICQ, QQ and Skype) and Download/Upload blocking.
- ◆ **Dynamic Host Control Protocol (DHCP) server:** DHCP server can allocate up to 253 client IP addresses and distribute them including IP address, subnet mask as well as DNS IP address to local computers. It provides an easy way to manage the local IP network.
- ◆ **Web based GUI:** MH-2001 supports web based GUI for configuration and management. It also supports multiple language including English, Traditional Chinese and Simplified Chinese.
- ◆ **User Authentication:** User database can be configured on the devices, MH-2001 also supports the authenticated database through external RADIUS and POP3 server.
- ◆ **Bandwidth Management:** Network packets can be classified based on IP address, IP subnet and

TCP/UDP port number and give guarantee and burst bandwidth with three levels of priority

- ◆ **Dynamic Domain Name System (DDNS):** The Dynamic DNS service allows users to alias a dynamic IP address to a static hostname.
- ◆ **Multiple NAT:** Multiple NAT allows local port to set multiple subnet and connect to the Internet through different WAN IP addresses.
- ◆ **Server Load Balancing:** Up to 4 group virtual servers support server load balancing
- ◆ **Accounting Report:** Accounting report function can monitor the information about the Intranet and External network traffic via MH-2001.

## 1.2 Package Contents

The following items should be included:

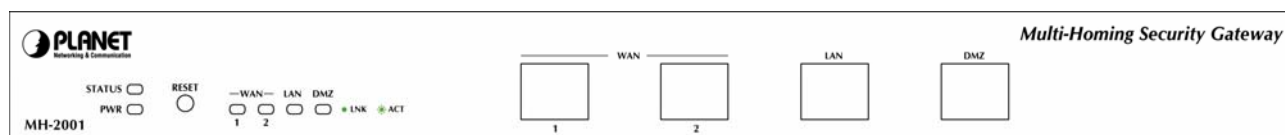
MH-2001

- Multi-Homing Security Gateway x 1
- User's Manual CD-ROM x 1
- Quick Installation Guide x 1
- Power Adapter x 1
- Cat5 Cable x 1
- Mat x 4

If any of the contents are missing or damaged, please contact your dealer or distributor immediately.

## 1.3 MH-2001 Front View

MH-2001 Front Panel



### LED / Button Definition

LED / Button	Description
<b>Reset Button</b>	Press this button to restore factory default setting.
<b>PWR</b>	Power is supplied to this device.
<b>STATUS</b>	Blinks to indicate this device is being turned on and booting. After four minutes, this LED indicator will stop blinking, it means this device is now ready to use.
<b>WAN1, WAN2, LAN, DMZ</b>	Steady on indicates the port is connected to other network device.  Blink to indicates there is traffic on the port

**- Port definition**

Port	Description
<b>WAN1, WAN2</b>	Connect to your xDSL/Cable modem or other Internet connection devices
<b>LAN</b>	Connect to your local PC, switch or other local network device
<b>DMZ</b>	Connect to your server or other network device

**1.4 MH-2001 Rear Panel**

MH-2001 Rear Panel



**DC Power:** connect one end of the power supply to this port, the other end to the electrical wall outlet.

## 1.5 Specification

Product		Multi-Homing Security Gateway
Model		MH-2001
Hardware		
Ethernet	LAN	1 x 10/100Mbps RJ-45
	WAN	2 x 10/100Mbps RJ-45
	DMZ	1 x 10/100Mbps RJ-45
Button		Reset button for reset to factory default setting
Software		
Management		Web
Network Connection		DMZ_NAT, DMZ_Transparent, NAT
Routing Protocol		Static Route, RIPv2
Outbound Load Balancing		Policy-based routing Load-balancing by Round-Robin, traffic, session, packet, Source IP and Destination IP
Firewall		Policy-based firewall rule with schedule NAT/ NATP SPI firewall Prevention of SYN attack, ICMP Flood, UDP flood, Ping of Death, Tear Drop, IP Spoofing, IP route, Port Scan and Land attack
VPN Tunnels (Configure/Connection)		200/100
VPN Functions		PPTP, IPSec DES, 3DES and AES encrypting SHA-1 / MD5 authentication algorithm Remote access VPN (Client-to-Site) and Site to Site VPN
Content Filtering		URL blocking, Script blocking (Popup, Java Applet, cookies and Active X) IM blocking (MSN, Yahoo Messenger, ICQ, QQ and Skype) P2P blocking (eDonkey, Bit Torrent and WinMX) Download and Upload blocking
Bandwidth Management		Policy-based bandwidth management Guarantee and maximum bandwidth with 3 priority levels Classify traffics based on IP, IP subnet, TCP/UDP port
User authentication		Built-in user database with up to 200 entries Radius, POP3 authentication support
Accounting Report		Outbound/Inbound accounting report statistics by Source IP, Destination IP and Service
Log and Alarm		Log and alarm for event and traffic Log can be saved from web, sent by e-mail or sent to syslog server
Statistics		Traffic statistic for interface (WAN 1/2) and policies Graphic display Record up to 30 days
Others		Firmware Upgradeable through Web Configuration Backup and Restore through Web Dynamic DNS NTP support DHCP server Multiple NAT and multiple DMZ (mapped IP) support Server load balancing

## Chapter 2: Hardware Installation

### 2.1 Installation Requirements

Before installing MH-2001, make sure your network meets the following requirements.

#### **- Mechanical Requirements**

MH-2001 is installed between your Internet connection and local area network. You can place it on the table or rack, and locate the unit near the power outlet.

#### **- Electrical Requirements**

MH-2001 is a power-required device, which means, it will not work until it is powered. If your network PCs will need to transmit data all the time, please consider use an UPS (Uninterrupted Power Supply) for your MH-2001. It will prevent you from network data loss. In some area, installing a surge suppression device may also help to protect your device from being damaged by unregulated surge or current to the MH-2001.

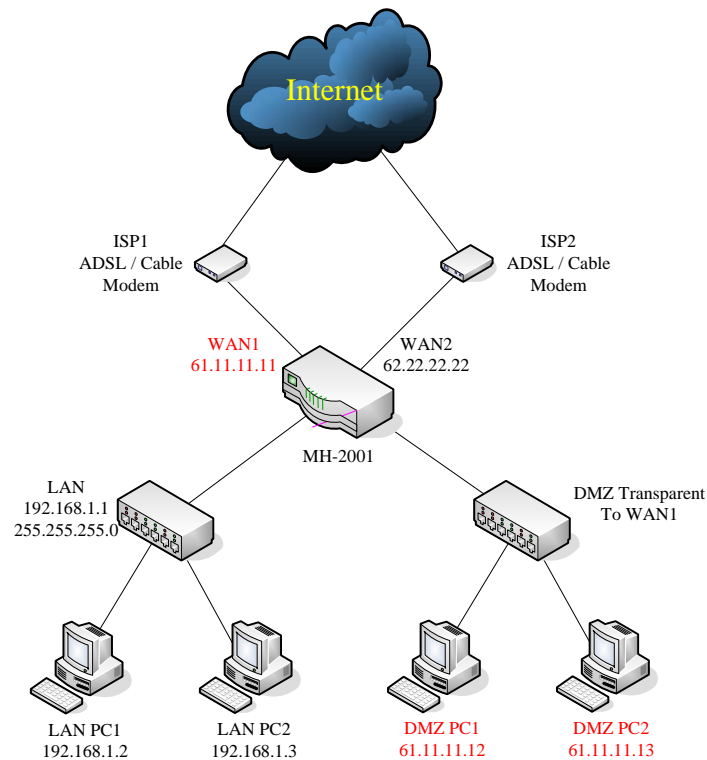
#### **- Network Requirements**

In order for MH-2001 to secure your network traffic, the traffic must pass through the device at a useful point in a network. In most situations, MH-2001 should be placed behind the Internet connection device.

## 2.2 Operation Mode

MH-2001 DMZ port supports three operation modes, Disable, NAT and Transparent. In Disable mode, the DMZ port is not active. In transparent mode, MH-2001 works as proxy with forward DMZ packet to WAN and forward WAN packet to DMZ. The DMZ and WAN side IP addresses are in the same subnet. In NAT mode, DMZ side user will share one public IP address of WAN port to make Internet connection. Please find the following two pictures for example.

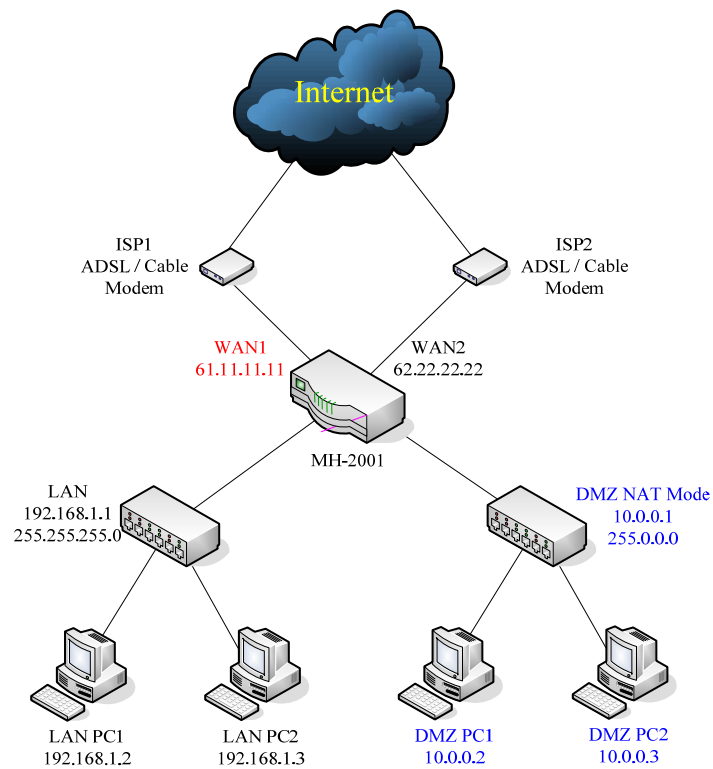
### 2.2.1 Transparent Mode Connection Example



The WAN1 and DMZ side IP addresses are on the same subnet. This application is suitable if you have a subnet of IP addresses and you do not want to change any IP configuration on the subnet.



## 2.2.2 NAT Mode Connecting Example



DMZ and WAN1 IP addresses are on the different subnet. This provides higher security level than transparent mode.

## Chapter 3: Getting Started

### 3.1 Web Configuration

#### STEP 1:

Connect the Administrator's PC and the LAN port of MH-2001 to a hub or switch. Make sure there is a link light on the hub/switch for both connections. MH-2001 has an embedded web server used for management and configuration. Use a web browser to display the configurations of MH-2001 (such as Internet Explorer 4(or above) or Netscape 4.0(or above) with full java script support). The default IP address of MH-2001 is **192.168.1.1** with a subnet mask of 255.255.255.0. Therefore, the IP address of the Administrator PC must be in the range between 192.168.1.2– 192.168.1.254

If the company's LAN IP Address is not subnet of 192.168.1.0, (i.e. LAN IP Address is 172.16.0.1), then the Administrator must change his/her PC IP address to be within the same range of the LAN subnet. Reboot the PC if necessary.

By default, MH-2001 is shipped with its DHCP Server function enabled. This means the client computers on the LAN network including the Administrator PC can set their TCP/IP settings to automatically obtain an IP address from the device.

The following table is a list of private IP addresses. These addresses may not be used as a WAN IP address.

10.0.0.0 ~ 10.255.255.255
172.16.0.0 ~ 172.31.255.255
192.168.0.0 ~ 192.168.255.255

#### STEP 2:

Once the Administrator PC has an IP address on the same network as the Multi-Homing Security Gateway, open up an Internet web browser and type in <http://192.168.1.1> in the address bar.

A pop-up screen will appear and prompt for a username and password. A username and password is required to connect to MH-2001. Enter the default login username and password of Administrator (see below).

**Username:** admin

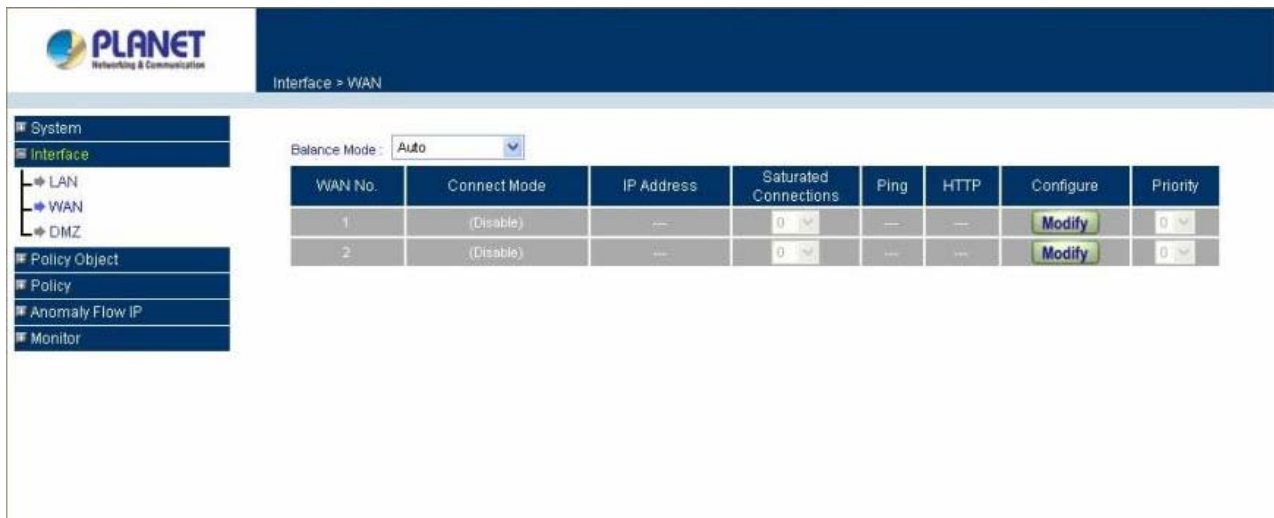
**Password:** admin

Click **OK**.



### 3.2 Configure WAN 1 interface

After entering the username and password, MH-2001 WebUI screen will display. Select the **Interface** tab on the left menu. Click on **WAN** from the sub-function list, and a sub-function list will be displayed.



Click **Modify** button to configure **WAN NO. 1** and the following page will be displayed.

WAN1 Interface

Service : DNS      DNS Server IP Address :  [Assist](#)

Domain name :  [Assist](#) (Max. 55 characters)

Wait 3 seconds between sending alive packet. ( Range: 0 - 99, 0: means not checking )

☐ PPPoE (ADSL User)  
☐ Dynamic IP Address (Cable Modem User)  
☒ Static IP Address

IP Address

Netmask

MAC Address 00:30:4f:ee:dd:09

Default Gateway

DNS Server 1

DNS Server 2

Max. Downstream Bandwidth  Kbps ( Range: 1 - 51200 )

Max. Upstream Bandwidth  Kbps ( Range: 1 - 51200 )

Enable System Management      ☐ Ping      ☒ HTTP

OK
Cancel

**Alive Indicator Site IP:** This feature is used to ping an address for detecting WAN connection status.

**Service: ICMP** You can select an IP address by **Assist**, or type an IP address manually.

**Service: DNS** You can select a DNS IP and Domain name by **Assist**, or type the related data manually.

**PPPoE (ADSL User):** This option is for PPPoE users who are required to enter a username and password in order to connect.

**Username:** Enter the PPPoE username provided by the ISP.

**Password:** Enter the PPPoE password provided by the ISP.

**IP Address provided by ISP:**

**Dynamic:** Select this if the IP address is automatically assigned by the ISP.

**Fixed:** Select this if you were given a static IP address. Enter the IP address that is given to you by your ISP.

**Max. Upstream/Downstream Bandwidth:** The bandwidth provided by ISP.

**Service-On-Demand:**

The PPPoE connection will automatically disconnect after a length of idle time (no activities). Enter in the amount of idle minutes before disconnection. Enter '0' if you do not want the PPPoE connection to disconnect at all.

**For Dynamic IP Address (Cable Modem User):** This option is for users who are automatically assigned an IP address by their ISP, such as cable modem users. The following fields apply:

**MAC Address:** This is the MAC Address of the device. Some ISPs require specified MAC address. If the required MAC address is your PC's, click **Clone MAC Address**.

**Hostname:** This will be the name assign to the device. Some cable modem ISP assigns a specific hostname in order to connect to their network, please enter the hostname here. If not required by your ISP, you do not have to enter a hostname.

**Domain Name:** You can specify your own domain name or leave it blank.

**User Name:** The user name is provided by ISP.

**Password:** The password is provided by ISP.

**Max. Upstream/Downstream Bandwidth:** The bandwidth provided by ISP.

**For Static IP Address:** This option is for users who are assigned a static IP Address from their ISP. Your ISP will provide all the information needed for this section such as IP Address, Netmask, Gateway, and DNS.

**IP Address:** Enter the static IP address assigned to you by your ISP. This will be the public IP address of the WAN 1 port of the device.

**Netmask:** This will be the Netmask of the WAN 1 network. (i.e. 255.255.255.0)

**Default Gateway:** This will be the Gateway IP address.

**Domain Name Server (DNS):** This is the IP Address of the DNS server.

**Max. Upstream/Downstream Bandwidth:** The bandwidth provided by ISP.

**Ping:** Select this to allow the WAN network to ping the IP Address of MH-2001 This will allow people from the Internet to be able to ping MH-2001 WAN IP. If set to enable, the device will respond to echo request packets from the WAN network.

**HTTP:** Select this to allow the device WebUI to be accessed from the WAN network. This will allow the WebUI to be configured from a user on the Internet. Keep in mind that the device always requires a username and password to enter the WebUI.

### 3.3 Configure WAN 2 interface

If you want to connect WAN 2 to another ISP connection, click **Modify** button of **WAN No. 2** then repeat above procedures to setup.

### 3.4 Configure DMZ interface

Depends on your network requirement, you can disable the DMZ port, make DMZ port transparent to WAN 1 or enable NAT function on it.

To configure the DMZ port, select the **Interface** tab on the left menu, then click on DMZ, the following page is shown.

DMZ Interface NAT

IP Address Disable 0.0.0.1

Netmask NAT 5.0.0.0

MAC Address DMZ\_TRANSPARENT 00:30:4f:ee:dd:04

Enable System Management ☒ Ping ☒ HTTP

OK Cancel

Please refer to **Section 2.2** for select the mode you need and configure relative IP parameters.

### 3.5 Configure Policy

#### STEP 1:

Click on the **Policy** tab from the main function menu, and then click on **Outgoing** (LAN to WAN) from the sub-function list.

#### STEP 2:

Click on **New Entry** button.

#### STEP 3:

When the **New Entry** option appears, enter the following configuration:

**Source Address** – select “**Inside\_Any**”

**Destination Address** – select “**Outside\_Any**”

**Service** - select “**ANY**”

**Action** - select “**Permit, ALL**”

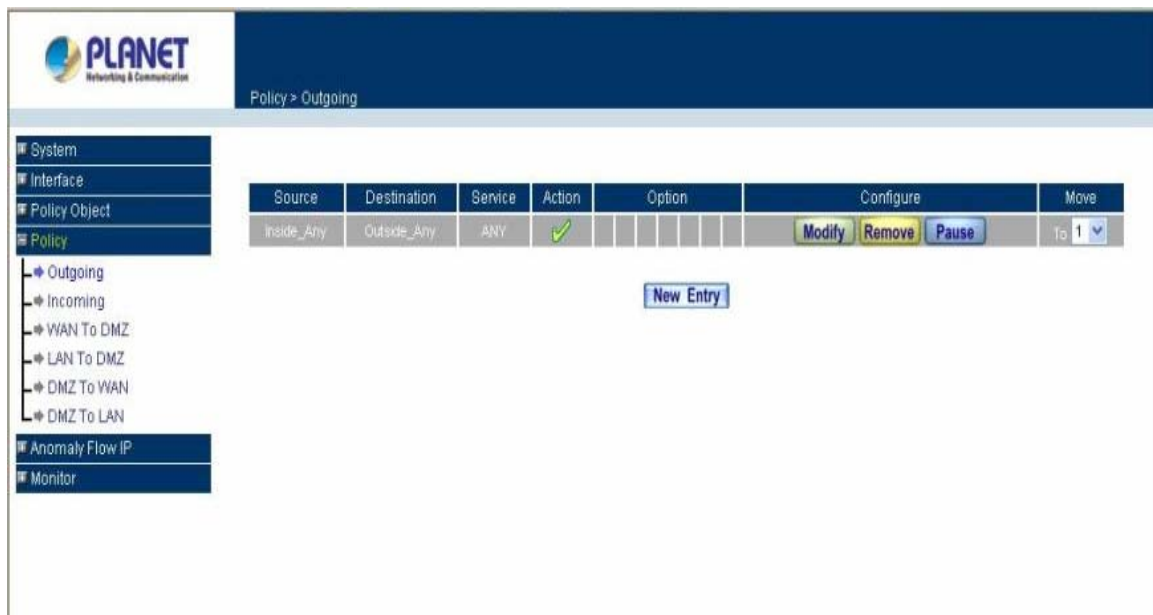
Click on **OK** to apply the changes.

Comment :  (Max. 32 characters)

Add New Policy	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
Tunnel	None
Action, WAN Port	PERMIT ALL
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> Enable
IM / P2P Blocking	None
QoS	None
MAX. Bandwidth Per Source IP	Downstream <input type="text"/> 0 Kbps Upstream <input type="text"/> 0 Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	<input type="text"/> 0 ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	<input type="text"/> 0 ( Range: 1 - 99999, 0: means unlimited )

**STEP 4:**

The configuration is successful when the screen below is displayed.



Please make sure that all the computers that are connected to the LAN port have their Default Gateway IP Address set to MH-2001's LAN IP Address (i.e. 192.168.1.1). At this point, all the computers on the LAN network should gain access to the Internet immediately. If MH-2001 filter function is required, please refer to the Policy section in chapter 7.

## Chapter 4: System

MH-2001 Administration and monitoring configuration is set by the System Administrator. The System Administrator can add or modify System settings and monitoring mode. The sub Administrators can only read System settings but not modify them. In **System**, the System Administrator can:

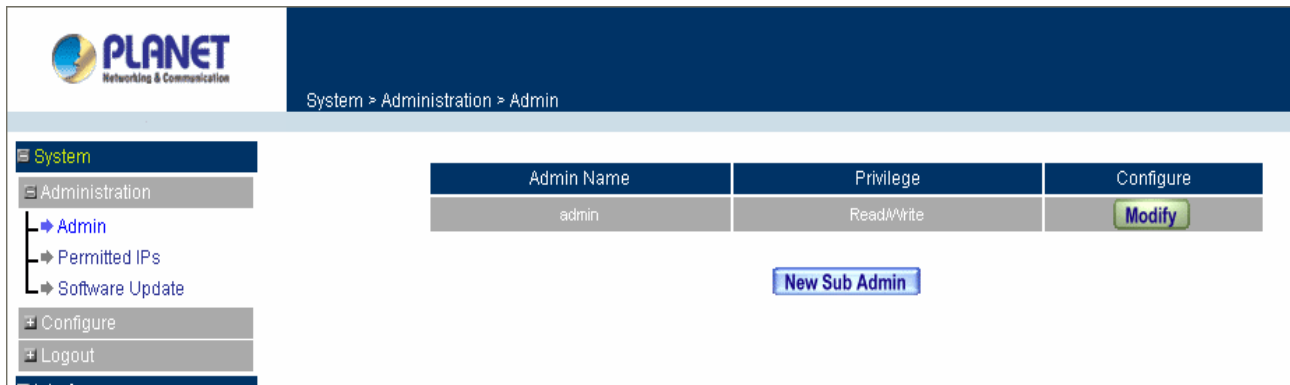
1. Add and change the sub Administrator's names and passwords;
2. Back up all MH-2001 settings into local files;
3. Set up alerts for Hackers invasion.

"System" is the managing of settings such as the privileges of packets that pass through MH-2001 and monitoring controls. Administrators may manage, monitor, and configure MH-2001 settings. All configurations are "read-only" for all users other than the Administrator; those users are not able to change any settings for MH-2001.

### 4.1 Administration

#### 4.1.1 Admin

Click the **System/Administration/Admin** on the left menu, and the list of Administrators will display as below.



The screenshot shows the Planet Network Administration web interface. The breadcrumb path is "System > Administration > Admin". The left sidebar menu includes "System", "Administration", "Admin", "Permitted IPs", "Software Update", "Configure", "Logout", and "Interface". The main content area displays a table of administrators:

Admin Name	Privilege	Configure
admin	Read/Write	<a href="#">Modify</a>

Below the table is a button labeled "New Sub Admin".

#### Define the required fields of Administrator

##### Admin Name:

- The username of Administrators and Sub Administrator for the MH-2001. The **admin** user name cannot be removed; and the sub-admin user can be removed or configure.



The default Account: **admin**; Password: **admin**

##### Privilege:

- The privileges of Administrators (Admin or Sub Admin). The username of the main Administrator is **Administrator** with **reading / writing** privilege. Administrator also can change the system setting, log system status, and to increase or delete sub-administrator. Sub-Admin may be created by the **Admin** by

clicking **New Sub Admin**. Sub Admin have **only** read and monitor privilege and cannot change any system setting value.

**Configure:**

- Click **Modify** to change the “Sub-Administrator’s” password or click **Remove** to delete a “Sub Administrator.”

**Changing the Main/Sub-Administrator’s Password**

Step 1. The **Modify Administrator Password** window will appear. Enter in the required information:

- **Password:** enter original password.
- **New Password:** enter new password
- **Confirm Password:** enter the new password again.

Step 2. Click **OK** to confirm password change or click **Cancel** to cancel it.

The screenshot shows the PLANET web interface. The top navigation bar includes the PLANET logo and the breadcrumb 'System > Administration > Admin'. A left sidebar contains a tree view with 'System' expanded, showing 'Administration' (with 'Admin' selected), 'Permitted IPs', 'Software Update', 'Configure', 'Logout', 'Interface', and 'Policy Object'. The main content area displays the 'Modify Admin Password' window. This window has a table with the following fields: 'Admin Name' (value: admin), 'Password' (masked with dots, note: (Max. 16 characters)), 'New Password' (masked with dots, note: (Max. 16 characters)), and 'Confirm Password' (masked with dots, note: (Max. 16 characters)). At the bottom right of the window are 'OK' and 'Cancel' buttons.


**Adding a new Sub Administrator**

Step 1. In the **Add New Sub Administrator** window:

- **Sub Admin Name:** enter the username of new **Sub Admin**.
- **Password:** enter a password for the new **Sub Admin**.
- **Confirm Password:** enter the password again.

Step 2. Click **OK** to add the user or click **Cancel** to cancel the addition.





System > Administration > Admin

**System**

- Administration
  - Admin**
  - Permitted IPs
  - Software Update
- Configure
- Logout
- Interface


**Add New Sub Admin**

Sub Admin name	planet	(Max. 16 characters)
Password	*****	(Max. 16 characters)
Confirm Password	*****	(Max. 16 characters)

OK Cancel

## Removing a Sub Administrator

- Step 1. In the Administration table, locate the Administrator name you want to edit, and click on the **Remove** option in the Configure field.
- Step 2. The Remove confirmation pop-up box will appear. Click **OK** to remove that Sub Admin or click **Cancel** to cancel.



System > Administration > Admin

**System**

- Administration
  - Admin**
  - Permitted IPs
  - Software Update
- Configure
- Logout
- Interface
- Policy Object
- Policy
- Anomaly Flow IP
- Monitor

Admin Name	Privilege	Configure
admin	Read/Write	Modify
planet	Read	Modify Remove

New Sub Admin

Microsoft Internet Explorer

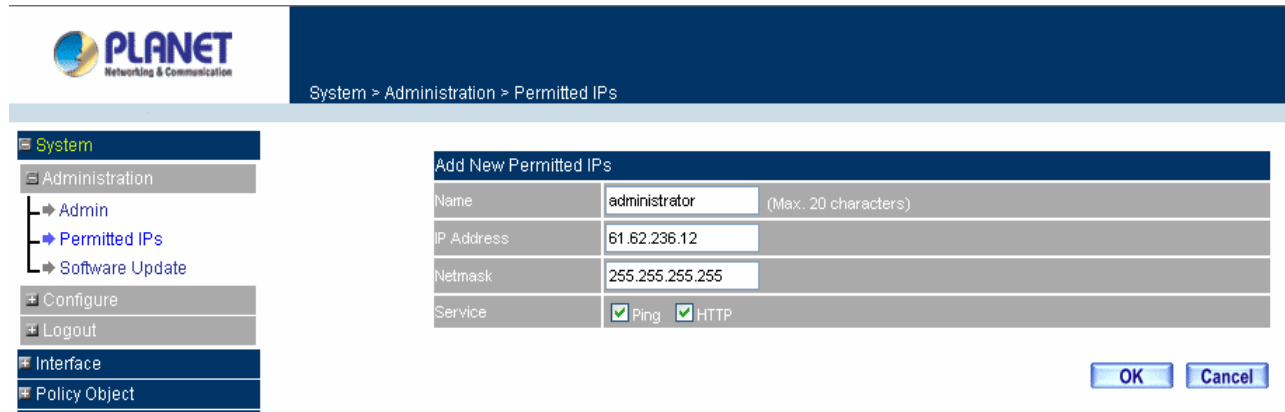
Are you sure you want to remove ?

確定 取消

## 4.1.2 Permitted IPs

### Add Permitted IPs

**STEP 1** . Add the following setting in **Permitted IPs** of **Administration**:



- **Name:** Enter a new name
- **IP Address:** Enter a IP address you want to permitted
- **Netmask:** Enter the Netmask( 255.255.255.255 means a host)
- **Service:** Select Ping and HTTP
- Click **OK**
- Complete add new permitted IPs

Name	IP Address / Netmask	Ping	HTTP	Configure
administrator	61.62.236.12 / 255.255.255.255	✓	✓	Modify Remove

**New Entry**



To make Permitted IPs be effective, it must cancel the **Ping** and **HTTP** selection in the WebUI of MH-2001 that Administrator enter. (LAN, WAN, or DMZ Interface)

Before canceling the **HTTP** selection of Interface, must set up the Permitted IPs first, otherwise, it would cause the situation of cannot enter WebUI by appointed Interface.

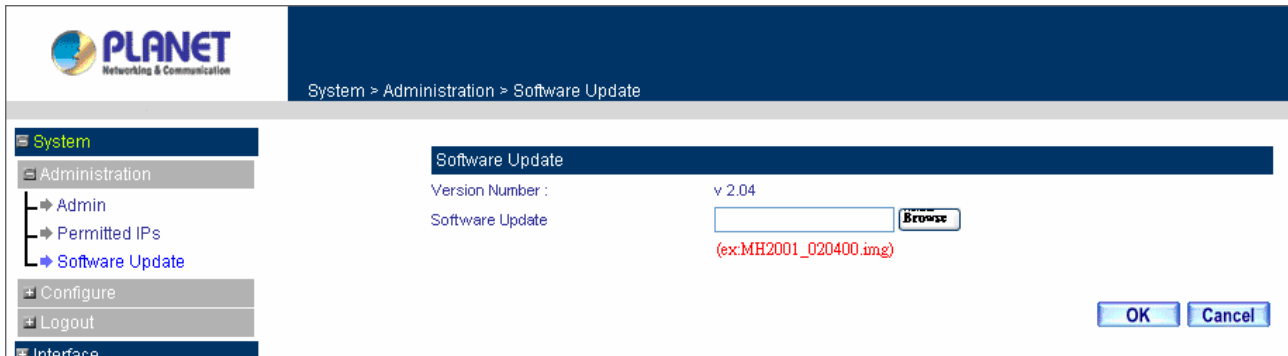
### 4.1.3 Software Update

Under **Software Update**, the admin may update the device's software with newer software.

You may acquire the current version number of software in **Version Number**. Administrators may visit distributor's web site to download the latest version and save it in server's hard disc.

Step 1. Click **Browse** to select the latest version of Software.

Step 2. Click **OK** to update software.



The screenshot shows the Planet Security Gateway web interface. The top header features the Planet logo and the text 'System > Administration > Software Update'. On the left is a navigation menu with 'System' (selected), 'Administration' (containing 'Admin', 'Permitted IPs', and 'Software Update'), 'Configure', 'Logout', and 'Interface'. The main content area is titled 'Software Update' and displays 'Version Number : v 2.04'. Below this, there is a 'Software Update' label, an empty text input field, and a 'Browse' button. A red text example '(ex:MH2001\_020400.img)' is shown below the input field. At the bottom right of the main area are 'OK' and 'Cancel' buttons.

**NOTE:** It takes three minutes to update the software. The system will restart automatically after updating the software.

## 4.2 Configure

The Configure is according to the basic setting of the MH-2001. In this chapter the definition is Setting, Date/Time, Multiple Subnet, Route Table, DHCP, Dynamic DNS, Hosts Table, and Language settings.

### 4.2.1 Setting

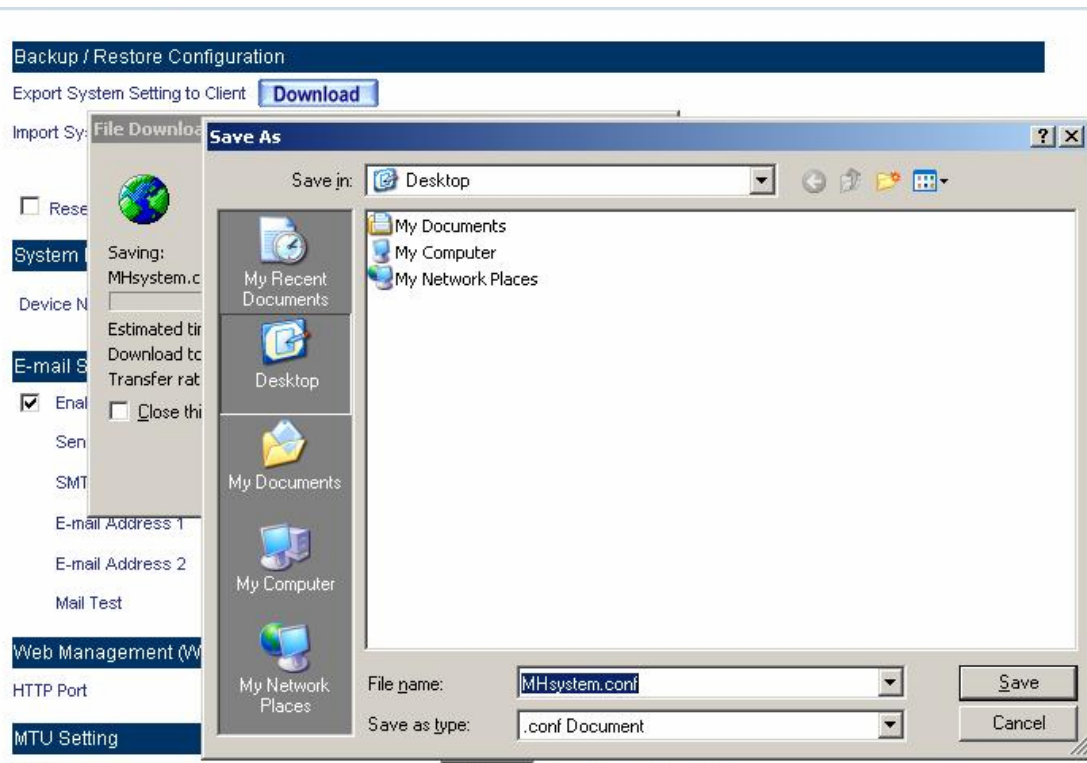
The Administrator may use this function to backup, restore MH-2001 configurations or restore MH-2001 back to default factory settings. You can also set general setting like device's name, E-mail setting and HTTP port on it.

#### Entering the Settings window

Click **Setting** in the **System/configure** menu to enter the **Settings** window. **MH-2001 Configuration settings** will be shown on the screen.

#### Exporting MH-2001 settings

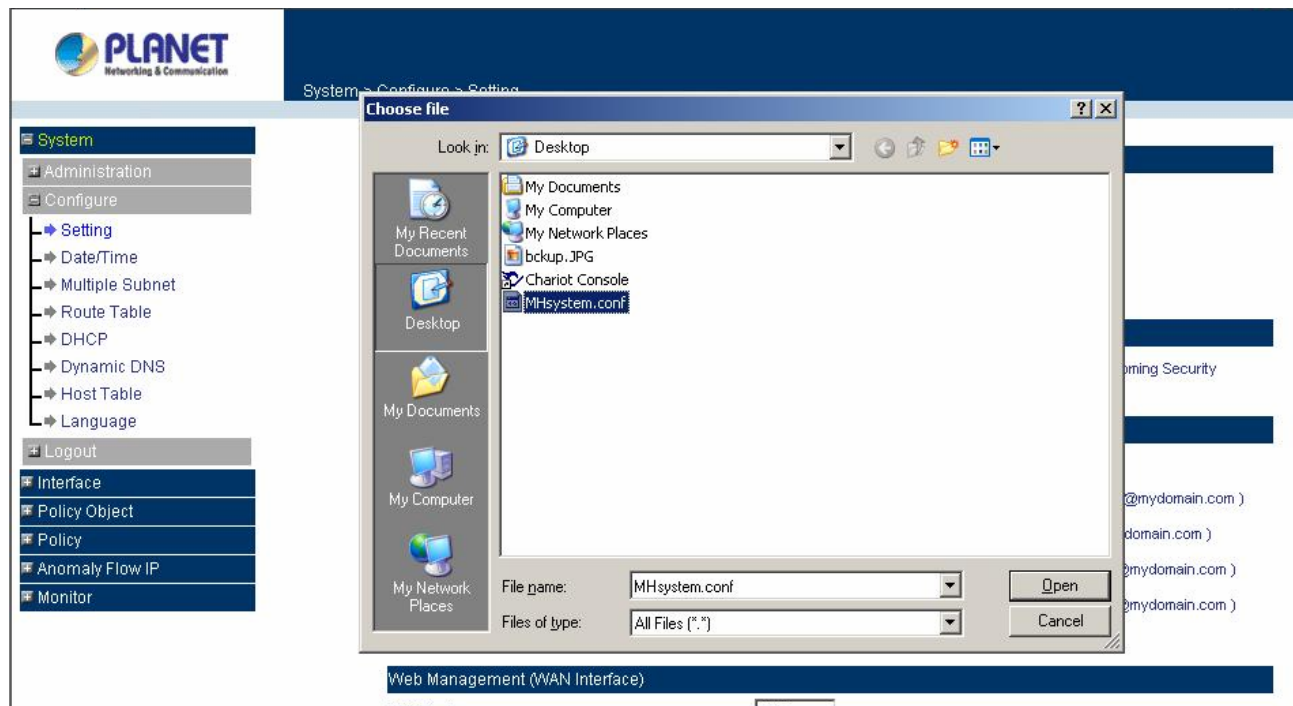
- Step 1. Under **Backup/Restore Configuration**, click on the **Download** button next to **Export System Settings to Client**.
- Step 2. When the **File Download** pop-up window appears, choose the destination place to save the exported file.



## Importing MH-2001 settings

Under **Backup/Restore Configuration**, click on the **Browse** button next to **Import System Settings**. When the **Choose File** pop-up window appears, select the file which contains the saved MH-2001 Settings, then click **OK**.

Click **OK** to import the file into MH-2001 or click **Cancel** to cancel importing.



## Restoring Factory Default Settings

Step 1. Select **Reset Factory Settings**.

Click **OK** at the bottom-right of the screen to restore the factory settings.

The screenshot shows the Planet Networking & Communication web interface. The breadcrumb trail at the top reads 'System > Configure > Setting'. On the left sidebar, the 'Configure' menu is expanded, showing options like 'Setting', 'Date/Time', 'Multiple Subnet', 'Route Table', and 'DHCP'. The 'Setting' option is selected. The main content area is titled 'Backup / Restore Configuration'. It contains two sections: 'Export System Setting to Client' with a 'Download' button, and 'Import System Setting from Client' with a text input field and a 'Browse...' button. Below these, there is a checkbox labeled 'Reset Factory Setting', which is circled in red. At the bottom, there is a section titled 'System Name Setting'.

## System Name Setting

Step 1. You can modify your device name. Enter the new name in the field.

Step 2. Click **OK** at the bottom-right of the screen.

The screenshot shows the 'System Name Setting' form. It has a title bar 'System Name Setting'. Below it, there is a 'Device Name' label followed by a text input field containing 'MH-2001'. To the right of the input field, there is a note: '( Max. 30 characters, ex: Multi-Homing Security Gateway )'.

## Enabling E-mail Alert Notification

Step 1. Select **Enable E-mail Alert Notification** under **E-Mail Settings**. This function will enable the MH-2001 to send e-mail alerts to the System Administrator when the network is being attacked by hackers or when emergency conditions occur.

Step 2. **SMTP Server IP:** Enter SMTP server's IP address.

Step 3. **E-Mail Address 1:** Enter the first e-mail address to receive the alarm notification.

Step 4. **E-Mail Address 2:** Enter the second e-mail address to receive the alarm notification. (Optional)

Step 5. Click **OK** on the bottom-right of the screen to enable E-mail alert notification.



Click on **Mail Test** to test if E-mail Address 1 and E-mail Address 2 can receive the Alert Notification correctly.

## Web Management (WAN Interface)

The administrator can change the port number used by HTTP port anytime. (Remote WebUI management)



After HTTP port has changed, if the administrator want to enter WebUI from WAN, will have to change the port number of browser. (For example: <http://61.62.108.172:8080>)

Step 1. **Set Web Management (WAN Interface).** Enter the new port number used by HTTP port.  
( Range 1 – 65535 )

Step 2. Click **OK** at the bottom-right of the screen.

## MTU (set networking packet length)

The administrator can modify the networking packet length.

Step 1. **MTU Setting.** Modify the networking packet length. ( Range 40 – 1500 )

Step 2. Click **OK** at the bottom-right of the screen.

The screenshot shows the Planet Network Configuration web interface. The left sidebar contains a tree view with 'System' expanded, and 'Setting' selected. The main content area is titled 'System > Configure > Setting'. It includes fields for 'E-mail Address 1' (alex\_tien@so-net.net), 'E-mail Address 2' (empty), and a 'Mail Test' button. Below these are sections for 'Web Management (WAN Interface)' with an 'HTTP Port' of 8080, 'MTU Setting' with an 'MTU' value of 1500 Bytes (circled in red), and 'Dynamic Routing (RIPv2)'.

## Dynamic Routing (RIPv2)

Enable Dynamic Routing (RIPv2), MH-2001 will switch the routing information of RIP. The routers which support RIP can connect automatically. You can choose to enable LAN, WAN1, WAN2 or DMZ interface to allow RIP protocol supporting.

**Routing information update timer:** MH-2001 will send out the RIP protocol in a period of time to update the routing table, the default timer is 30 seconds.

**Routing information timeout:** If MH-2001 does not receive the RIP protocol from the other router in a period of time, MH-2001 will cut off the routing automatically until it receives RIP protocol again. The default timer is 180 seconds.

The screenshot shows the Planet Network Configuration web interface, specifically the 'Dynamic Routing (RIPv2)' section. The left sidebar is the same as the previous screenshot. The main content area shows the 'Dynamic Routing (RIPv2)' section with 'Enable' checked for LAN, WAN1, WAN2, and DMZ. It also includes 'Routing information update timer' set to 30 seconds and 'Routing information timeout' set to 180 seconds. The 'SIP protocol pass-through' section is visible at the bottom.



## SIP protocol pass-through

Select this option to the device's **SIP protocol pass-through**. Once this function is enabled, the SIP packets will be allowed to pass-through via MH-2001.

The screenshot shows the Planet Security Gateway configuration interface. The left sidebar contains a tree view with the following items: System, Administration, Configure, Setting (selected), Date/Time, Multiple Subnet, Route Table, DHCP, Dynamic DNS, Host Table, Language, Logout, Interface, Policy Object, Policy, Anomaly Flow IP, and Monitor. The main content area is titled 'System > Configure > Setting'. It contains several sections: 'E-mail Address 1' (alex\_tien@so-net.net), 'E-mail Address 2' (empty), 'Mail Test' button, 'Web Management (WAN Interface)' with 'HTTP Port' set to 8080, 'MTU Setting' with 'MTU' set to 1500, and 'Dynamic Routing (RIPv2)' with 'Enable' checked for LAN, WAN1, WAN2, and DMZ. The 'SIP protocol pass-through' section is highlighted with a red circle, showing the 'Enable SIP protocol pass-through' checkbox checked.

## To-Appliance Packets Log

Select this option to the device's **To-Appliance Packets Log**. Once this function is enabled, every packet to this appliance will be recorded for system administrator to trace.

The screenshot shows the Planet Security Gateway configuration interface, similar to the previous one. The left sidebar is the same. The main content area is titled 'System > Configure > Setting'. It contains the same sections as before, but the 'To-Appliance Packets Log' section is highlighted with a red circle, showing the 'Enable To-Appliance Packets Log' checkbox checked. The 'SIP protocol pass-through' section is also visible and checked.

## System Reboot

Once this function is enabled, MH-2001 will be rebooted.

Click **Reboot**. The confirmation pop-up box will appear. Click **OK** to restart MH-2001 or click **Cancel** to discard changes

The screenshot shows the Planet Networking & Communication web interface. The left sidebar contains a navigation menu with options: System, Administration, Configure, Setting, Date/Time, Multiple Subnet, Route Table, DHCP, Dynamic DNS, Host Table, Language, Logout, Interface, Policy Object, Policy, Anomaly Flow IP, and Monitor. The main content area is titled 'System > Configure > Setting'. It contains several configuration sections: 'Sender Address' (alex\_tien@so-net.ne), 'SMTP Server' (211.23.80.85), 'E-mail Address 1' (alex\_tien@so-net.ne), 'E-mail Address 2' (empty), and a 'Mail Test' button. Below these are sections for 'Web Management (WAN Interface)' (HTTP Port), 'MTU Setting' (MTU), 'Dynamic Routing (RIPv2)' (Enable, LAN, WAN1, WAN2, DMZ, Routing information update timer, Routing information timeout), 'SIP protocol pass-through' (Enable SIP protocol pass-through), 'To-Appliance Packets Log' (Enable To-Appliance Packets Log), and 'System Reboot' (Reboot Multi-Homing Security Gateway Appliance, Reboot button). A 'Microsoft Internet Explorer' dialog box is overlaid in the center, asking 'Are you sure to Reboot?' with 'OK' and 'Cancel' buttons.

### 4.2.2 Date/Time

#### Synchronizing the MH-2001 with the System Clock

Administrator can configure MH-2001's date and time by either syncing to an Internet Network Time Server (NTP) or by syncing to your computer's clock.

##### Follow these steps to sync to an Internet Time Server

- Step 1.** Enable synchronization by checking the box.
- Step 2.** Click the down arrow to select the offset time from GMT.
- Step 3.** Enter the Server IP Address or Server name with which you want to synchronize.
- Step 4.** **Update system clock every 120 minutes** You can set the interval time to synchronize with outside servers. If you set it to 0, it means the device will not synchronize automatically.

##### Follow this step to sync to your computer's clock.

- Step 1.** Click on the **Sync** button. Click **OK** to apply the setting or click **Cancel** to discard changes.



The value of **Set Offset From GMT** and **Server IP / Name** can be looking for from **Assist**.

## 4.2.3 Multiple Subnet

### NAT mode

Multiple Subnet allows local port to set multiple subnet works and connect with the internet through different WAN 1 IP Addresses.

For instance: The lease line of a company applies several real IP Addresses 168.85.88.0/24, and the company is divided into R&D department, service, sales department, procurement department, accounting department, the company can distinguish each department by different subnet works for the purpose of convenient management. The settings are as the following:

1. **R&D department** sub-network: **192.168.1.11/24**(LAN )  $\leftrightarrow$  168.85.88.253(WAN 1)
2. **Service department** sub-network: **192.168.2.11/24**(LAN )  $\leftrightarrow$  168.85.88.252(WAN 1)
3. **Sales department** sub-network: **192.168.3.11/24**(LAN )  $\leftrightarrow$  168.85.88.251(WAN 1)
4. **Procurement department** sub-network: **192.168.4.11/24**(LAN )  $\leftrightarrow$  168.85.88.250(WAN 1)
5. **Accounting department** sub-network: **192.168.5.11/24**(LAN )  $\leftrightarrow$  168.85.88.249(WAN 1)

The first department(R&D department) was set while setting interface IP, the other four ones have to be added in Multiple Subnet, after completing the settings, each department use the different WAN IP Address to connect to the internet. The settings of LAN computers on **Service department** are as the following

Service IP Address: 192.168.2.1

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.2.11

The other departments are also set by groups, this is the function of Multiple Subnet.

## Multiple Subnet settings

Click **Multiple Subnet** under the **System/Configure** menu to enter Multiple Subnet window.

WAN Interface IP / Forwarding Mode	Interface	Alias IP of Interface / Netmask	Configure
WAN 1 : 210.66.155.77 / NAT	LAN	192.168.2.11 / 255.255.255.0	<a href="#">Modify</a> <a href="#">Remove</a>
WAN 2 : 211.74.64.177 / NAT	LAN	192.168.2.11 / 255.255.255.0	<a href="#">Modify</a> <a href="#">Remove</a>

[New Entry](#)

### Multiple Subnet functions:

**WAN Interface IP / Forwarding Mode:** Display WAN Port IP Address and Forwarding Mode.

**Alias IP of Interface / Netmask:** Local Interface IP Address and subnet Mask.

**Configure:** Modify the settings of Multiple Subnet. Click **Modify** to modify the parameters of Multiple Subnet or click **Remove** to delete settings.

### Add a Multiple Subnet with NAT Mode:

**Step 1:** Click the **New Entry** button below to add Multiple Subnet.

**Step 2:** Interface: Select LAN or DMZ Interface which you want to add a Subnet.

Alias IP of LAN Interface: Enter Subnet Interface IP Address.

Netmask: Enter Subnet Interface Netmask.

WAN Interface IP: Add WAN 1 or WAN 2 IP.

Forwarding Mode: Select the NAT button to enable NAT mode.

**Step 3:** Click OK to add Multiple Subnet or click Cancel to discard changes.

Modify Multiple Subnet IP

Interface: ☒ LAN ☐ DMZ

Alias IP of Interface: 192.168.2.11

Netmask: 255.255.255.0

WAN Interface IP		Forwarding Mode
WAN1	210.66.155.77 <a href="#">Assist</a>	<input checked="" type="radio"/> NAT <input type="radio"/> Routing
WAN2	211.74.64.177 <a href="#">Assist</a>	<input checked="" type="radio"/> NAT <input type="radio"/> Routing

[OK](#) [Cancel](#)

### Add a Multiple Subnet with Routing Mode:

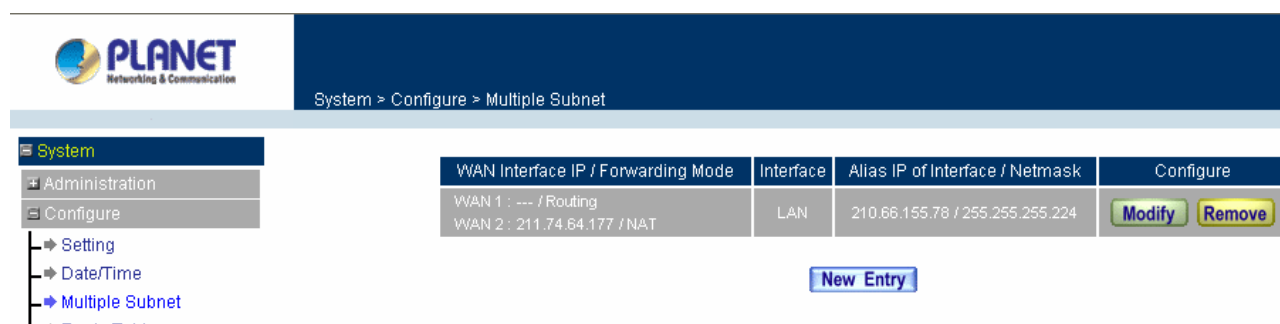
Multiple Subnet allows local Interface to set Multiple Subnet Routing Mode and connect with the internet through different WAN IP Addresses.

For example, the leased line of a company applies several real IP Addresses 168.85.88.0/24 and the company is divided into R&D, Customer Service, Sales, Procurement, and Accounting Department. The company can distinguish each department by different sub-network for the purpose of convenient management.

The settings are as the following:

1. **R&D department:** Alias IP of LAN interface - 168.85.88.1, Netmask: 255.255.255.192
2. **Sales department:** Alias IP of LAN interface - 168.85.88.65, Netmask: 255.255.255.192
3. **Procurement department:** Alias IP of LAN interface - 168.85.88.129, Netmask: 255.255.255.192
4. **Accounting department:** Alias IP of LAN interface - 168.85.88.193, Netmask: 255.255.255.192

Click **Multiple Subnet** under the **System/Configure** menu to enter Multiple Subnet window.



### Multiple Subnet functions

**WAN Interface IP / Forwarding Mode:** Display WAN Port IP Address and Forwarding Mode which is NAT Mode or Routing Mode.

**Alias IP of Int. Interface / Subnet Mask:** Local Interface IP Address and subnet Mask.

**Modify:** Modify the settings of Multiple Subnet. Click **Modify** to modify the parameters of Multiple Subnet or click **Remove** to delete settings.

### Adding a Multiple Subnet with Routing Mode

**Step 1:** Click the Add button below to add Multiple Subnet.

**Step 2:** Interface: Select LAN or DMZ Interface which you want to add a Subnet.

Alias IP of LAN Interface: Enter Subnet Interface IP Address.

Netmask: Enter Subnet Interface Netmask.

WAN Interface IP: Add WAN 1 or WAN 2 IP.

Forwarding Mode: Select the Routing button to enable Routing mode.

**Step 3:** Click OK to add Multiple Subnet or click Cancel to discard changes.

PLANET Networking & Communication

System > Configure > Multiple Subnet

**System**

- Administration
- Configure
  - Setting
  - Date/Time
  - Multiple Subnet**
  - Route Table
  - DHCP
  - Dynamic DNS
  - Host Table
  - Language
- Logout

**Modify Multiple Subnet IP**

Interface: ☒ LAN ☐ DMZ

Alias IP of Interface: 210.66.155.78

Netmask: 255.255.255.224

WAN Interface IP		Forwarding Mode
WAN1	0.0.0.0 <a href="#">Assist</a>	<input type="radio"/> NAT <input checked="" type="radio"/> Routing
WAN2	211.74.64.177 <a href="#">Assist</a>	<input checked="" type="radio"/> NAT <input type="radio"/> Routing

[OK](#) [Cancel](#)

#### 4.2.4 Route Table

In this section, the Administrator can add static routes for the networks.

##### Entering the Route Table screen

Click Route Table under the System/Configure menu and the Route Table window will appear, in which current route settings are shown.

PLANET Networking & Communication

System > Configure > Route Table

**System**

- Administration
- Configure
  - Setting
  - Date/Time
  - Multiple Subnet
  - Route Table**

Interface	Destination IP / Netmask	Gateway	Configure
LAN	192.168.4.0 / 255.255.255.0	192.168.1.254	<a href="#">Modify</a> <a href="#">Remove</a>

[New Entry](#)

##### Route Table functions

- **Interface:** Destination network through the Interface, LAN, DMZ or WAN 1.
- **Destination IP:** IP address of destination network.
- **NetMask:** Netmask of destination network.
- **Gateway:** Gateway IP address for connecting to destination network.
- **Configure:** Modify or remove the settings in the route table.

##### Adding a new Static Route

- Step 1. In the Route Table window, click the **New Entry** button.
- Step 2. In the Add New Static Route window, enter new static route information.
- Step 3. In the Interface pull-down menu, choose the Interface to connect (LAN, WAN1, DMZ).
- Step 4. Click **OK** to add the new static route or click **Cancel** to cancel.

The screenshot shows the PLANET Networking & Communication configuration interface. The breadcrumb path is 'System > Configure > Route Table'. On the left, a sidebar menu shows 'System' expanded with 'Configure' selected, and 'Route Table' highlighted. The main area is titled 'Modify Static Route' and contains the following fields:

Destination IP	192.168.4.0
Netmask	255.255.255.0
Gateway	192.168.1.254
Interface	LAN

At the bottom right, there are 'OK' and 'Cancel' buttons.

#### 4.2.5 DHCP

In this section, the Administrator can configure DHCP (Dynamic Host Configuration Protocol) settings for the LAN and DMZ network.

##### Entering the DHCP window

Click **DHCP** under the **System/Configure** menu. The DHCP window appears in which current DHCP settings are shown on the screen.

The screenshot shows the PLANET Networking & Communication configuration interface. The breadcrumb path is 'System > Configure > DHCP'. On the left, a sidebar menu shows 'System' expanded with 'Configure' selected, and 'DHCP' highlighted. The main area contains the following settings:

- ☒ Enable DHCP Support
- Domain Name:  (Max. 40 characters, ex: dhcp.domain\_name)
- ☐ Automatically Get DNS
- DNS Server 1:  192.168.1.1
- DNS Server 2:
- WINS Server 1:
- WINS Server 2:
- LAN Interface :
  - Client IP Range 1:  192.168.1.2 To  192.168.1.50
  - Client IP Range 2:  To
- DMZ Interface :
  - Client IP Range 1:  10.0.0.10 To  10.0.0.50
  - Client IP Range 2:  To
- Leased Time:  12 hours (Range: 0 - 99999)

At the bottom right, there are 'OK' and 'Cancel' buttons.

##### Dynamic IP Address functions

- **Subnet:** LAN network's subnet
- **NetMask:** LAN network's netmask
- **Gateway:** LAN network's gateway IP address
- **Broadcast:** LAN network's broadcast IP address

## Enabling DHCP Support

Step 1. In the DHCP window, click **Enable DHCP Support**.

**Domain Name:** The Administrator may enter the name of the LAN network domain if preferred.

**Automatically Get DNS:** Check this box to automatically detect DNS server.

**DNS Server 1 :** Enter the distributed IP address of DNS Server 1.

**DNS Server 2 :** Enter the distributed IP address of DNS Server 2.

**WINS Server 1 :** Enter the distributed IP address of WINS Server 1.

**WINS Server 2 :** Enter the distributed IP address of WINS Server 2.

**LAN interface:**

**Client IP Address Range 1:** Enter the starting and the ending IP address dynamically assigning to DHCP clients.

**Client IP Address Range 2:** Enter the starting and the ending IP address dynamically assigning to DHCP clients. (Optional)

**DMZ interface:**

**Client IP Address Range 1:** Enter the starting and the ending IP address dynamically assigning to DHCP clients.

**Client IP Address Range 2:** Enter the starting and the ending IP address dynamically assigning to DHCP clients. (Optional)

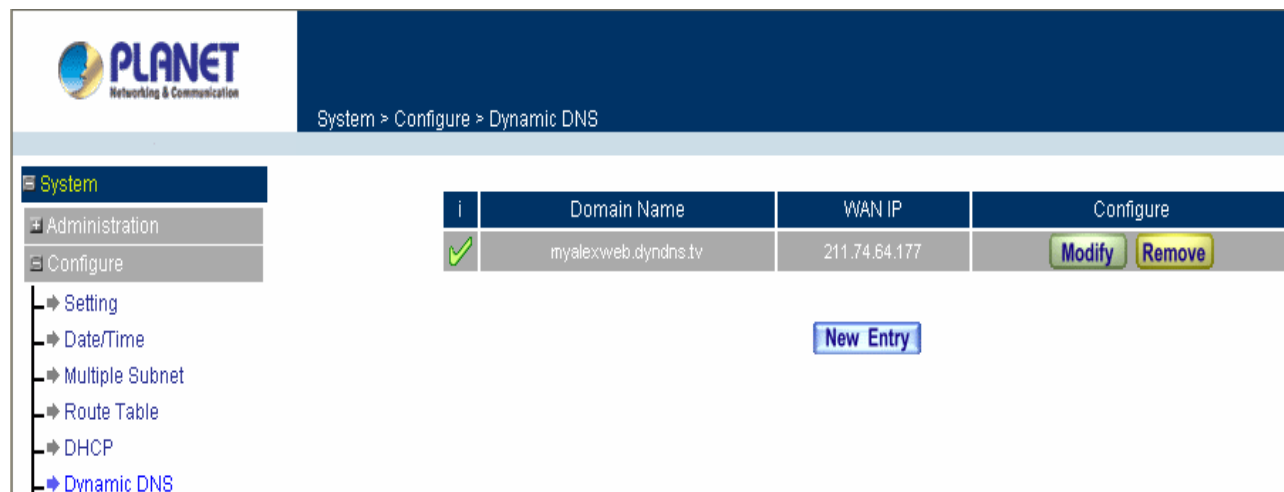
**Leased Time:** Enter the leased time for DHCP. The default time is 24 hours.

Step 2. Click **OK** to enable DHCP support.

### 4.2.6 Dynamic DNS

The **Dynamic DNS** (require Dynamic DNS Service) allows you to assign a dynamic IP address to a static hostname, allowing your device to be more easily accessed by specific name. When this function is enabled, the IP address in Dynamic DNS Server will be automatically updated with the new IP address provided by ISP.

Click **Dynamic DNS** under **System/Configure** menu to enter Dynamic DNS window.



System > Configure > Dynamic DNS





i	Domain Name	WAN IP	Configure
✓	myalexweb.dyndns.tv	211.74.64.177	Modify Remove

New Entry



The icons in Dynamic DNS window:

**! : Update Status**

Chart				
Meaning	Update successfully	Incorrect username or password	Connecting to server	Unknown error

**Domain name:** Your host domain name.

**WAN IP Address:** IP Address of the WAN port.

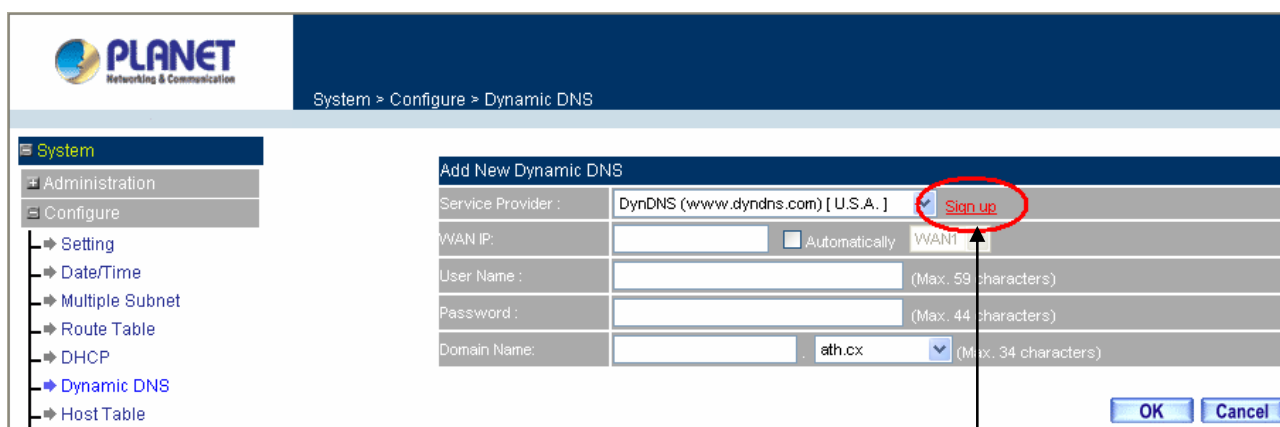
**Configure:** Modify dynamic DNS settings. Click **Modify** to change the DNS parameters; click **Remove** to delete the settings.

**How to use dynamic DNS:**

MH-2001 provides many service providers, users have to register prior to use this function. For the usage regulations, see the providers' websites.

**How to register:**

Firstly, Click **Dynamic DNS** under the **System/Configure** menu to enter Dynamic DNS window, then click **Add** button , on the right side of the service providers, click **Sign up**, the service providers` website will appear, please refer to the website for the way of registration.



The screenshot shows the 'Planet' logo and the 'System > Configure > Dynamic DNS' breadcrumb. On the left is a navigation tree with 'Dynamic DNS' selected. The main area contains the 'Add New Dynamic DNS' form. The 'Service Provider' dropdown is set to 'DynDNS (www.dyndns.com) [ U.S.A. ]'. The 'Sign up' button next to it is circled in red. Below the form are 'OK' and 'Cancel' buttons.

Click on **Sign up** then can enter the website of the provider

**Add Dynamic DNS settings**

Step 1. Click **Add** button.

Step 2. Click the information in the column of the Dynamic DNS window.

**Service providers:** Select service providers.

**Sign up:** to the service providers' website.

**WAN IP Address:** IP Address of the WAN port.

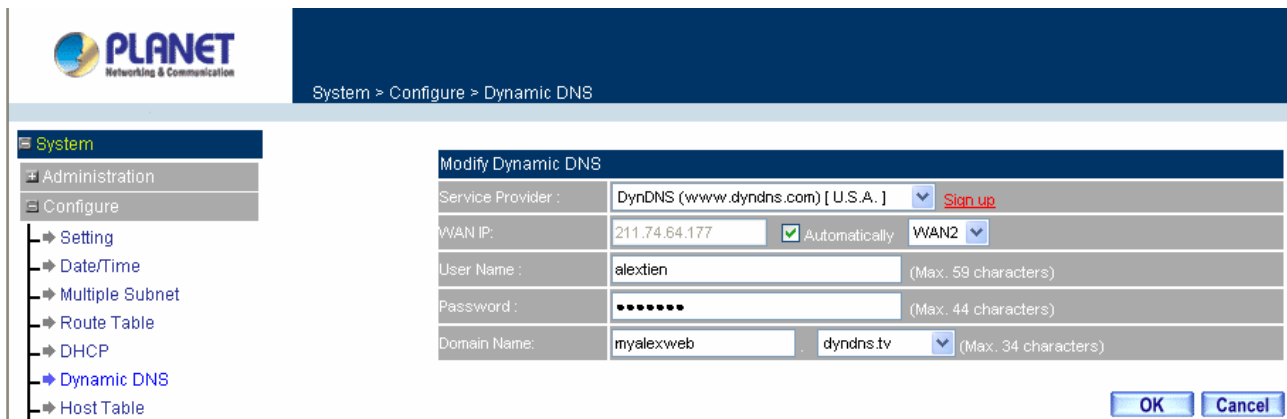
☐ **Automatically** : Check to automatically fill in the WAN IP. °

**User Name:** Enter the registered user name.

**Password:** Enter the user password.

**Domain name:** Your host domain name provided by service provider

Step 3. Click **OK** to add dynamic DNS or click **Cancel** to discard changes.



System > Configure > Dynamic DNS

**Modify Dynamic DNS**

Service Provider : DynDNS (www.dyndns.com) [ U.S.A. ] [Sign up](#)

WAN IP: 211.74.64.177 ☒ Automatically WAN2

User Name : alexten (Max. 59 characters)

Password : ..... (Max. 44 characters)

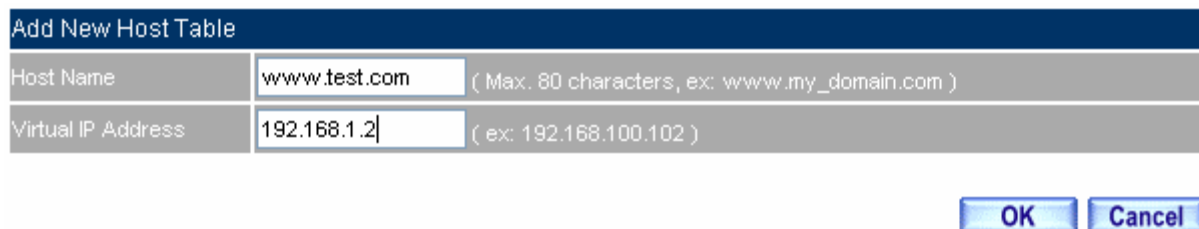
Domain Name: myalexweb dyndns.tv (Max. 34 characters)

**OK** **Cancel**

## 4.2.7 Host Table

**STEP 1** . Select **Host Table** under **System/Configure** menu and click on **New Entry**

- **Domain Name:** The domain name of the server
- **Virtual IP Address:** The virtual IP address respective to Host Table
- Click **OK** to add Host Table.



**Add New Host Table**

Host Name: www.test.com ( Max. 80 characters, ex: www.my\_domain.com )

Virtual IP Address: 192.168.1.2 ( ex: 192.168.100.102 )

**OK** **Cancel**



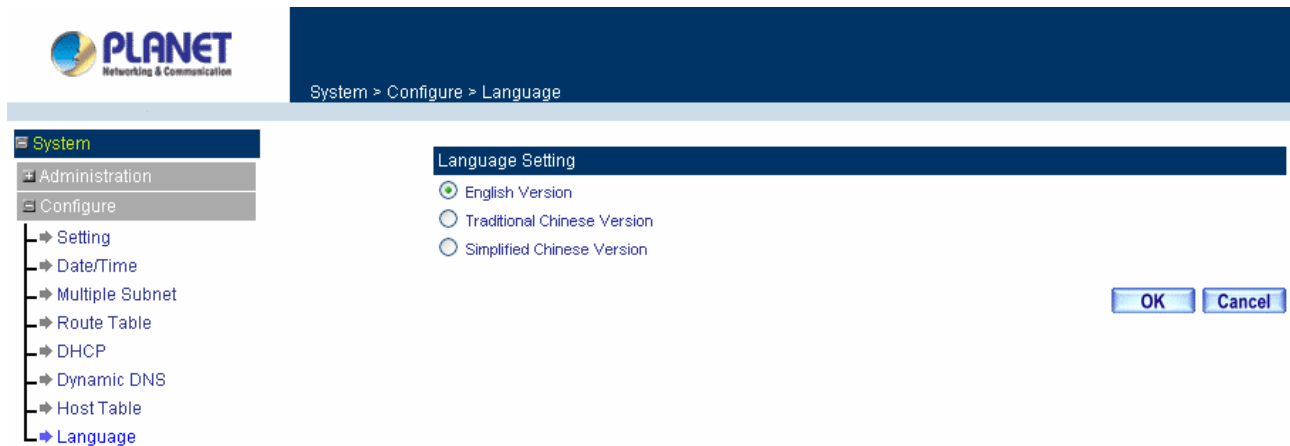
To use Host Table, the user PC's first DNS Server must be the same as the LAN Port or DMZ Port IP of MH-2001. That is, the default gateway.

## 4.2.8 Language

Administrator can configure MH-2001 to select the Language version

Step 1. Select the Language version (**English Version**, **Traditional Chinese Version** or **Simplified Chinese Version**).

Step 2. Click **OK** to set the Language version or click **Cancel** to discard changes.



### 4.3 Logout

**STEP 1** . Click **Logout** in **System** to protect the system while Administrator is away.



Confirm Logout WebUI

**STEP 2** . Click **OK** and the logout message will appear in WebUI.

#### Multi-Homing Security Gateway Web Server Information

Your current connection has expired, you have now been logged out.  
If you want to login, please restart your browser.

Logout WebUI Message

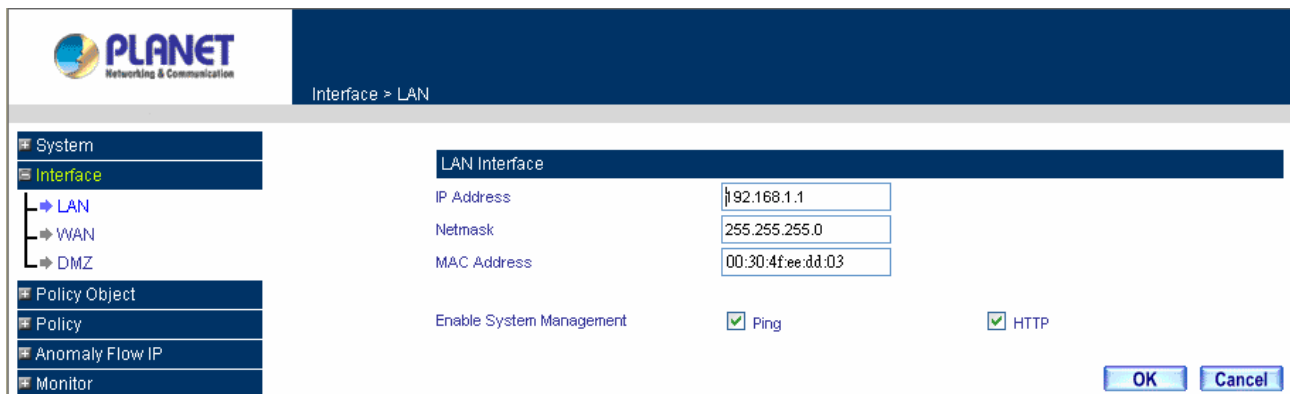
## Chapter 5: Interface

In this section, the **Administrator** can set up the IP addresses for the office network. The Administrator may configure the IP addresses of the LAN network, the WAN 1/2 network, and the DMZ network. The netmask and gateway IP addresses are also configured in this section.

### 5.1 LAN

#### Entering the Interface menu:

Click on **Interface** in the left menu bar. Then click on **LAN** below it. The current settings of the interface addresses will appear on the screen.



The screenshot shows the PLANET web interface. The left sidebar contains a menu with 'System', 'Interface', 'Policy Object', 'Policy', 'Anomaly Flow IP', and 'Monitor'. Under 'Interface', 'LAN' is selected. The main content area is titled 'Interface > LAN' and 'LAN Interface'. It contains the following fields and options:

IP Address	192.168.1.1
Netmask	255.255.255.0
MAC Address	00:30:4f:ee:dd:03

Below these fields, there are three checkboxes: 'Enable System Management' (unchecked), 'Ping' (checked), and 'HTTP' (checked). At the bottom right, there are 'OK' and 'Cancel' buttons.

#### Modify the Interface Settings

Using the LAN **Interface**, the Administrator sets up the LAN network. The LAN network will use a private IP scheme. The private IP network will not be routable on the Internet.

**IP Address:** The private IP address of MH-2001 LAN network is the IP address of the LAN port of the device. The default IP address is 192.168.1.1. If the new LAN IP Address is not 192.168.1.1, the Administrator needs to set the IP Address on the computer to be on the same subnet as MH-2001 and restart the System to make the new IP address effective. For example, if MH-2001's new LAN IP Address is 172.16.0.1, then enter the new LAN IP Address 172.16.0.1 in the URL field of browser to connect to MH-2001.

**NetMask:** This is the subnet mask of the LAN network. The default netmask of the device is 255.255.255.0.

**Ping:** Select this to allow the LAN network to ping the IP Address of MH-2001. If set to enable, the device will respond to ping packets from the LAN network.

**HTTP:** Select this to allow the device WEBUI to be accessed from the LAN network.



Do not cancel WebUI selection before not setting Permitted IPs yet. It will cause the Administrator cannot be allowed to enter the MH-2001's WebUI from LAN.

## 5.2 WAN

### Entering the Interface menu

Click on **Interface** in the left menu bar. Then click on **WAN** below it. The current settings of the Interface will appear on the screen.

WAN No.	Connect Mode	IP Address	Saturated Connections	Ping	HTTP	Configure	Priority
1	Static IP	210.66.155.77	2	✓	✓	Modify	1
2	PPPoE	211.74.64.177	1	✓	✓	Modify	2

### Balance Mode:

- **Auto:** The MH-2001 will adjust the WAN 1/2 utility rate automatically according to the downstream/upstream of WAN. (For users who are using various download bandwidth)
- **Round-Robin:** The MH-2001 distributes the WAN 1/2 download bandwidth 1:1, in other words, it selects the agent by order. (For users who are using same download bandwidths)
- **By Traffic:** The MH-2001 distributes the WAN 1/2 download bandwidth by accumulative traffic.
- **By Session:** The MH-2001 distributes the WAN 1/2 download bandwidth by saturated connections.
- **By Packet:** The MH-2001 distributes the WAN 1/2 download bandwidth by accumulated packets and saturated connection.
- **By Source IP:** The MH-2001 distributes the WAN 1/2 download bandwidth by Source IP.
- **By Destination IP:** The MH-2001 distributes the WAN 1/2 download bandwidth by Destination IP

**WAN No:** WAN port 1 or 2.

**Connect Mode:** Display the current connection mode: PPPoE, Dynamic IP Address (Cable Modem User) or Static IP Address.

**IP Address:** Display the current WAN IP Address.

**Saturated Connections:** Set the number for saturation whenever session numbers reach it, the MH-2001 switches to the next WAN port on the list. This function is only applicable for **By Traffic**, **By Session** and **By Packet** mode.

**Ping / HTTP:** Display Ping/HTTP functions of WAN 1/2 to show if they are enabled or disabled.

**Configure:** Click **Modify** to modify WAN 1/2 settings.

**Priority:** Set priority of WAN 1/2 for Internet Access.

## Setting WAN Interface Address

**STEP 1** . Select **WAN** in **Interface** and click **Modify** in **WAN1 Interface**.



The setting of WAN2 Interface is almost the same as WAN1. The difference is that WAN2 has a selection of **Disable**. The System Administrator can close WAN2 Interface by this selection.

Interface > WAN

System

Interface

- LAN
- WAN
- DMZ

Policy Object

WAN2 Interface **Disable**

Service: **DNS** **Disable** **Enable** Server IP Address: 139.175.55.244 [Assist](#)

Domain name: www.google.com.tw [Assist](#) (Max. 55 characters)

Wait 3 seconds between sending alive packet. ( Range: 0 - 99, 0: means not checking )

### Disable WAN2 Interface

**STEP 2** . Setting the Connection Service (ICMP or DNS way) :

- **ICMP** : Enter an Alive Indicator Site IP (can select from **Assist**)
- **DNS** : Enter DNS Server IP Address and Domain Name (can select from **Assist**)
- Setting time of seconds between sending alive packet.

WAN1 Interface

Service: **ICMP** Alive Indicator Site IP: 206.228.179.10 [Assist](#)

Wait 1 seconds between sending alive packet.

### ICMP Connection

WAN1 Interface

Service: **DNS** DNS Server IP Address: 168.95.1.1 [Assist](#)

Domain name: tw.yahoo.com [Assist](#) (Max. 55 characters)

Wait 3 seconds between sending alive packet. ( Range: 0 - 99, 0: means not checking )

### DNS Service



Connection test is used for MH-2001 to detect if the WAN can connect or not. So the **Alive Indicator Site IP**, **DNS Server IP Address**, or **Domain Name** must be able to use permanently. Or it will cause judgmental mistakes of the device.

**STEP 3 . Select the Connecting way:****■ PPPoE (ADSL User):**

1. Select **PPPoE**
2. Enter **User Name** as an account
3. Enter **Password** as the password
4. Select **Dynamic** or **Fixed** in **IP Address provided by ISP**. If you select Fixed, please enter IP Address, Netmask, and Default Gateway.
5. Enter **Max. Downstream Bandwidth** and **Max. Upstream Bandwidth**. (According to the flow that user apply)
6. Enter **Auto Disconnect** idle time. Default is 0 minute, it means always connected.
7. Select **Ping** and **HTTP**
8. Click **OK**

☒ PPPoE (ADSL User)  
☐ Dynamic IP Address (Cable Modem User)  
☐ Static IP Address

Current Status: Disconnected Connecting Disconnect

IP Address: 0.0.0.0

User Name:  (Max. 60 characters)

Password:  (Max. 60 characters)

IP Address provided by ISP: ☒ Dynamic ☐ Fixed

IP Address:

Netmask:

Default Gateway:

Max. Downstream Bandwidth:  Kbps ( Range: 1 - 51200 )

Max. Upstream Bandwidth:  Kbps ( Range: 1 - 51200 )

Auto Disconnect if idle:  minutes ( Range: 1 - 99999, 0: means always connected )

Enable System Management: ☐ Ping ☐ HTTP

**PPPoE Connection**

If the connection is PPPoE, you can set up **Auto Disconnect if idle** (not recommend)

### ■ Dynamic IP Address (Cable Modem User) :

1. Select **Dynamic IP Address (Cable Modem User)**
2. Click **Renew** in the right side of IP Address and then can obtain IP automatically.
3. If the MAC Address is required for ISP then click on **Clone MAC Address** to obtain MAC IP automatically.
4. **Hostname**: Enter the hostname provided by ISP.
5. **Domain Name**: Enter the domain name provided by ISP.
6. **User Name** and **Password** are the IP distribution method according to Authentication way of DHCP+ protocol (like ISP in China)
7. Enter **Max. Downstream Bandwidth** and **Max. Upstream Bandwidth** (According to the flow that user apply)
8. Select **Ping** and **HTTP**
9. Click **OK**

WAN1 Interface			
Service :	<span>DNS</span>	DNS Server IP Address :	<input type="text" value="168.95.1.1"/> <a href="#">Assist</a>
		Domain name :	<input type="text" value="tw.yahoo.com"/> <a href="#">Assist</a> (Max. 55 characters)
Wait	<input type="text" value="3"/>	seconds between sending alive packet. ( Range: 0 - 99, 0: means not checking )	
<input type="radio"/> PPPoE (ADSL User) <input checked="" type="radio"/> Dynamic IP Address (Cable Modem User) <input type="radio"/> Static IP Address			
IP Address	<input type="text" value="0.0.0.0"/>	<a href="#">Renew</a>	<a href="#">Release</a>
MAC Address	<input type="text" value="00:30:4F:EE:DD:09"/>	<a href="#">Clone MAC Address</a>	
Hostname	<input type="text"/>	(Max. 50 characters)	
Domain Name	<input type="text"/>	(Max. 80 characters)	
User Name (Required by DHCP+ protocol)	<input type="text"/>	(Max. 127 characters)	
Password (Required by DHCP+ protocol)	<input type="text"/>	(Max. 127 characters)	
Max. Downstream Bandwidth	<input type="text" value="2000"/>	Kbps ( Range: 1 - 51200 )	
Max. Upstream Bandwidth	<input type="text" value="2000"/>	Kbps ( Range: 1 - 51200 )	
Enable System Management	<input type="checkbox"/> Ping	<input type="checkbox"/> HTTP	
		<a href="#">OK</a>	<a href="#">Cancel</a>

### Dynamic IP Address Connection



### ■ Static IP Address

1. Select **Static IP Address**
2. Enter **IP Address**, **Netmask**, and **Default Gateway** that provided by ISP
3. Enter **DNS Server1** and **DNS Server2 (option)**



In WAN2, the connecting of Static IP Address does not need to set DNS Server

4. Enter **Max. Downstream Bandwidth** and **Max. Upstream Bandwidth** (According to the flow that user apply)
5. Select **Ping** and **HTTP**
6. Click **OK**

WAN1 Interface	
Service :	DNS <input type="button" value="v"/> DNS Server IP Address : 168.95.1.1 <a href="#">Assist</a>
	Domain name : tw.yahoo.com <a href="#">Assist</a> (Max. 55 characters)
Wait <input type="text" value="3"/>	seconds between sending alive packet. ( Range: 0 - 99, 0: means not checking )
<input type="radio"/> PPPoE (ADSL User) <input type="radio"/> Dynamic IP Address (Cable Modem User) <input checked="" type="radio"/> Static IP Address	
IP Address	<input type="text" value="210.66.155.77"/>
Netmask	<input type="text" value="255.255.255.224"/>
MAC Address	<input type="text" value="00:30:4f:ee:dd:09"/>
Default Gateway	<input type="text" value="210.66.155.94"/>
DNS Server 1	<input type="text" value="168.95.1.1"/>
DNS Server 2	<input type="text"/>
Max. Downstream Bandwidth	<input type="text" value="2000"/> Kbps ( Range: 1 - 51200 )
Max. Upstream Bandwidth	<input type="text" value="2000"/> Kbps ( Range: 1 - 51200 )
Enable System Management	<input checked="" type="checkbox"/> Ping <input checked="" type="checkbox"/> HTTP
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

### Static IP Address Connection



When selecting **Ping** and **HTTP** on **WAN** network Interface, users will be able to ping the MH-2001 and enter the WebUI WAN network. It may influence network security. The suggestion is to **Cancel Ping** and **HTTP** after all the settings have finished. And if the System Administrator needs to enter UI from WAN, he/she can use **Permitted IPs** to enter.

## 5.3 DMZ

The Administrator uses the **DMZ Interface** to set up the DMZ network. The DMZ network consists of server computers such as FTP, SMTP, and HTTP (web). These Servers are put in the DMZ network so they can be isolated from the LAN network traffic. Broadcast messages from the LAN network will not cross over to the DMZ network to cause congestions and slow down these Servers. This allows the Servers to work efficiently without any slowdowns.

**DMZ Interface:** There are three options that you can select, Disable, NAT and Transparent.

**IP Address:** The private IP address of MH-2001's DMZ interface. This will be the IP address of the DMZ port. If it is in NAT mode, the IP address cannot use the same network with the WAN or LAN network.

**Netmask:** This will be the subnet mask of the DMZ network.

**Ping:** Select this to allow the DMZ network to ping the IP Address of MH-2001. If set to enable, the device will respond to echo request packets from the DMZ network.

**HTTP:** Select this to allow the device WEBUI to be accessed from the DMZ network. Keep in mind that the device always requires a username and password to enter the WebUI.

### Setting DMZ Interface Address (NAT Mode)

**STEP 1 .** Click **DMZ Interface**

**STEP 2 .** Select NAT Mode in DMZ Interface

- Select **NAT** in **DMZ Interface**
- Enter **IP Address** and **Netmask**

**STEP 3 .** Select **Ping** and **HTTP**

**STEP 4 .** Click **OK**

### Setting DMZ Interface Address (NAT Mode) WebUI

## Setting DMZ Interface Address (Transparent Mode)

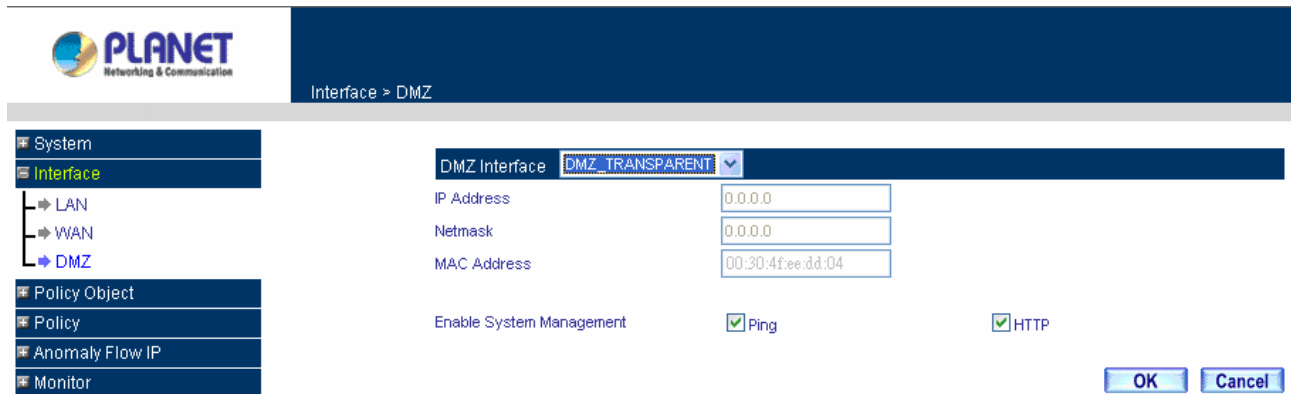
**STEP 1** . Select **DMZ** Interface

**STEP 2** . Select Transparent Mode in DMZ Interface

- Select **DMZ\_Transparent** in **DMZ Interface**

**STEP 3** . Select **Ping** and **HTTP**

**STEP 4** . Click **OK**



PLANET  
Networking & Communication

Interface > DMZ

System

Interface

- LAN
- WAN
- DMZ

Policy Object

Policy

Anomaly Flow IP

Monitor

DMZ Interface: DMZ\_TRANSPARENT

IP Address: 0.0.0.0

Netmask: 0.0.0.0

MAC Address: 00:30:4fee:dd:04

Enable System Management: ☒ Ping ☒ HTTP

OK Cancel

### Setting DMZ Interface Address (Transparent Mode) WebUI



In WAN, the connecting way must be **Static IP Address** and can choose **Transparent Mode** in **DMZ**.

## Chapter 6: Policy Object

### 6.1 Address

MH-2001 allows the Administrator to set addresses of the LAN network, LAN network group, WAN network, WAN group, DMZ network and DMZ group. These settings are to be used for policy editing.

#### What is the Address Table?

An IP address in the Address Table can be an address of a computer or a sub network. The Administrator can assign an easily recognized name to an IP address. Based on the network it belongs to, an IP address can be LAN IP address, WAN IP address and DMZ IP address. If the Administrator needs to create a control policy for packets of different IP addresses, he can first add a new group in the LAN **Network Group** or the **WAN Network Group** and assign those IP addresses into the newly created group. Using group addresses can greatly simplify the process of building control policies.

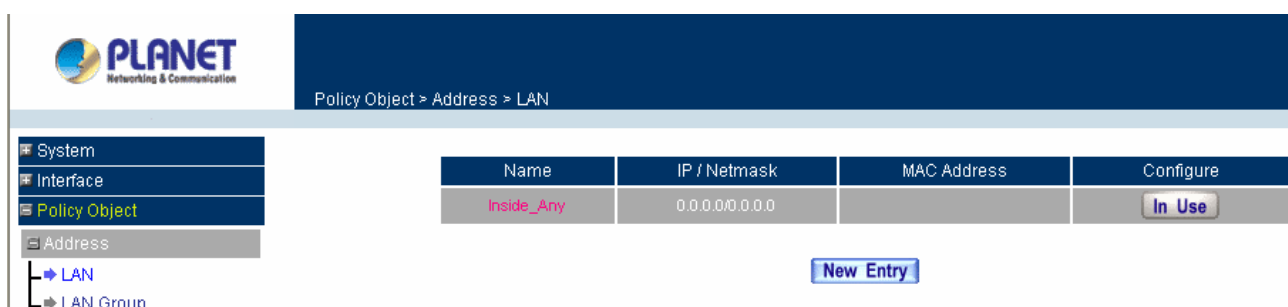
#### How to use Address Table

With easily recognized names of IP addresses and names of address groups shown in the address table, the Administrator can use these names as the source address or destination address of control policies. The address table should be built before creating control policies, so that the Administrator can pick the names of correct IP addresses from the address table when setting up control policies.

#### 6.1.1 LAN

##### Entering the LAN window

Step 1. Click LAN under the **Address** menu to enter the LAN window. The current setting information such as the name of the LAN network, IP and Netmask addresses will show on the screen.



#### Definition

**Name:** Name of LAN network address.

**IP:** IP address of LAN network

**Netmask:** subnet mask of LAN network.

**MAC Address:** MAC address corresponded with LAN IP address.

**Configure:** You can configure the settings in LAN network. Click **Modify** to change the parameters in LAN

network. Click **Remove** to delete the settings.



If one of the members has been added to **Policy** or **LAN Group**, the **Configure** column will show the message – **In Use**. In this case, you are not allowed to modify or remove the setting.

### Adding a new LAN Address

- Step 1. In the LAN window, click the **New Entry** button.
- Step 2. In the **Add New Address** window, enter the settings of a new LAN network address.
- Step 3. If you want to enable **Get Static IP address from DHCP Server** function, enter the MAC Address then check the **Get Static IP address from DHCP Server**.
- Step 4. Click **OK** to add the specified LAN network or click **Cancel** to cancel the changes.

The screenshot shows the PLANET Networking & Communication software interface. On the left is a tree view with categories: System, Interface, Policy Object, Address, and Service. Under 'Address', there are sub-items: LAN, LAN Group, WAN, WAN Group, DMZ, and DMZ Group. The 'Policy Object > Address > LAN' path is selected. The main area displays the 'Add New Address' dialog box with the following fields and options:

- Name:** Alex (Max. 16 characters)
- IP Address:** 192.168.1.10
- Netmask:** 255.255.255.255 (255.255.255.255 means the specified PC; 255.255.255.0 means class C subnet)
- MAC Address:** (empty field) with a **Clone MAC Address** button
- ☐ Get static IP address from DHCP Server.

At the bottom right of the dialog are **OK** and **Cancel** buttons.



When the System Administrator setting the **Address Book**, he/she can choose the way of clicking on **Clone MAC Address** to make the MH-2001 to fill out the user's MAC Address automatically.



In **LAN** of **Address** function, the MH-2001 has an default **Inside Any** address setting represents the whole LAN network automatically. Others like **WAN**, **DMZ** also have the **Outside Any** and **DMZ Any** default address setting to represent the whole subnet.

## 6.1.2 LAN Group

### Entering the LAN Group window

The LAN Addresses may be combined together to become a group.

- Step 1. Click **LAN Group** under the **Address** menu to enter the LAN Group window. The current setting information for the LAN network group appears on the screen.

The screenshot shows the PLANET configuration interface. On the left is a navigation tree with 'System', 'Interface', 'Policy Object', 'Address', 'LAN', 'LAN Group', and 'WAN'. The 'LAN Group' item is selected. The main area has a breadcrumb 'Policy Object > Address > LAN Group'. Below this is a table with three columns: 'Name', 'Member', and 'Configure'. The 'Name' column contains 'User'. The 'Member' column contains 'alex, joe, james'. The 'Configure' column contains 'Modify', 'Remove', and 'Pause' buttons. A 'New Entry' button is located below the table.

Name	Member	Configure
User	alex, joe, james	Modify Remove Pause

New Entry

### Definitions (LAN group):

**Name:** Name of the LAN group.

**Member:** Members of the group.

**Configure:** Configure the settings of LAN group. Click **Modify** to change the settings of LAN group. Click **Remove** to delete the group.



If one of the LAN Group has been added to **Policy**, the **Configure** column will show the message – **In Use**. In this case, you are not allowed to modify or remove the LAN group. You have to delete the Group in **Policy** window, and then you are allowed to configure the LAN Group.

### Adding a LAN Group

- Step 1. In the LAN **Group** window, click the **New Entry** button to enter the **Add New Address Group** window.
- Step 2. In the Add New Address Group window:
- **Name:** enter the name of the new group in the open field.
  - **Available Address:** list the names of all the members of the LAN network.
  - **Selected Address:** list the names to be assigned to the new group.
- Step 3. **Add members:** Select names to be added in Available Address list, and click the **Add>>** button to add them to the Selected Address list.
- Step 4. **Remove members:** Select names to be removed in the Selected Address list, and click the **<<Remove** button to remove these members from Selected Address list.
- Step 5. Click **OK** to add the new group or click **Cancel** to discard changes.

### 6.1.3 WAN

#### Entering the WAN window

- Step 1. Click **WAN** under the **Address** menu to enter the WAN window. The current setting information, such as the name of the WAN network, IP and Netmask addresses will show on the screen.

Name	IP / Netmask	Configure
Outside_Any	0.0.0.0/0.0.0.0	In Use
remote_admin	61.62.236.12/255.255.255.255	Modify Remove

#### Definitions

**Name:** Name of WAN network address.

**IP/Netmask:** IP address/Netmask of WAN network.

**Configure:** Configure the settings of WAN network. Click **Modify** to change the settings of WAN network.

Click **Remove** to delete the setting of WAN network.

**NOTE:** In the **WAN** Network window, if one of the members has been added to **Policy** or **LAN Group**, the **Configure** column will show the message – **In Use**. In this case you are not allowed to modify or remove the settings.



If one of the members has been added to **Policy** or **WAN Group**, the **Configure** column will show the

message – **In Use**. In this case, you are not allowed to modify or remove the setting. You have to remove the setting in **Policy** or **WAN Group**, and then you are allowed to configure the WAN address.

### Adding a new WAN Address

- Step 1. In the WAN window, click the **New Entry** button.
- Step 2. In the **Add New Address** window, enter the settings for a new WAN network address.
- Step 3. Click **OK** to add the specified WAN network or click **Cancel** to discard changes.

The screenshot shows the PLANET configuration interface. The breadcrumb path is 'Policy Object > Address > WAN'. On the left, a tree view shows 'System', 'Interface', 'Policy Object', 'Address', 'LAN', 'LAN Group', 'WAN', 'WAN Group', and 'NM7'. The 'Modify Address' window is open with the following fields:

Modify Address	
Name	remote_admin (Max. 16 characters)
IP Address	61.62.236.12
Netmask	255.255.255.255 ( 255.255.255.255 means the specified PC )
	( 255.255.255.0 means class C subnet )

At the bottom right of the window are 'OK' and 'Cancel' buttons.

### 6.1.4 WAN Group

#### Entering the WAN Group window

- Step 1. Click the **WAN Group** under the **Address** menu bar to enter the WAN window. The current settings for the WAN network group(s) will appear on the screen.

The screenshot shows the PLANET configuration interface. The breadcrumb path is 'Policy Object > Address > WAN Group'. On the left, the tree view is the same as in the previous screenshot, but 'WAN Group' is selected. The main area displays a table with the following data:

Name	Member	Configure
WAN_user	remote_admin, remote_user	<div>Modify Remove</div> <div>Pause</div>

Below the table is a 'New Entry' button.

#### Definitions:

**Name:** Name of the WAN group.

**Member:** Members of the group.

**Configure:** Configure the settings of WAN group. Click **Modify** to change the parameters of WAN group. Click **Remove** to delete the selected group.



If one of the WAN Group has been added to **Policy**, the **Configure** column will show the message – **In Use**. In this case, you are not allowed to modify or remove the WAN group. You have to remove the Group in **Policy** window, and then you are allowed to configure the WAN Group.



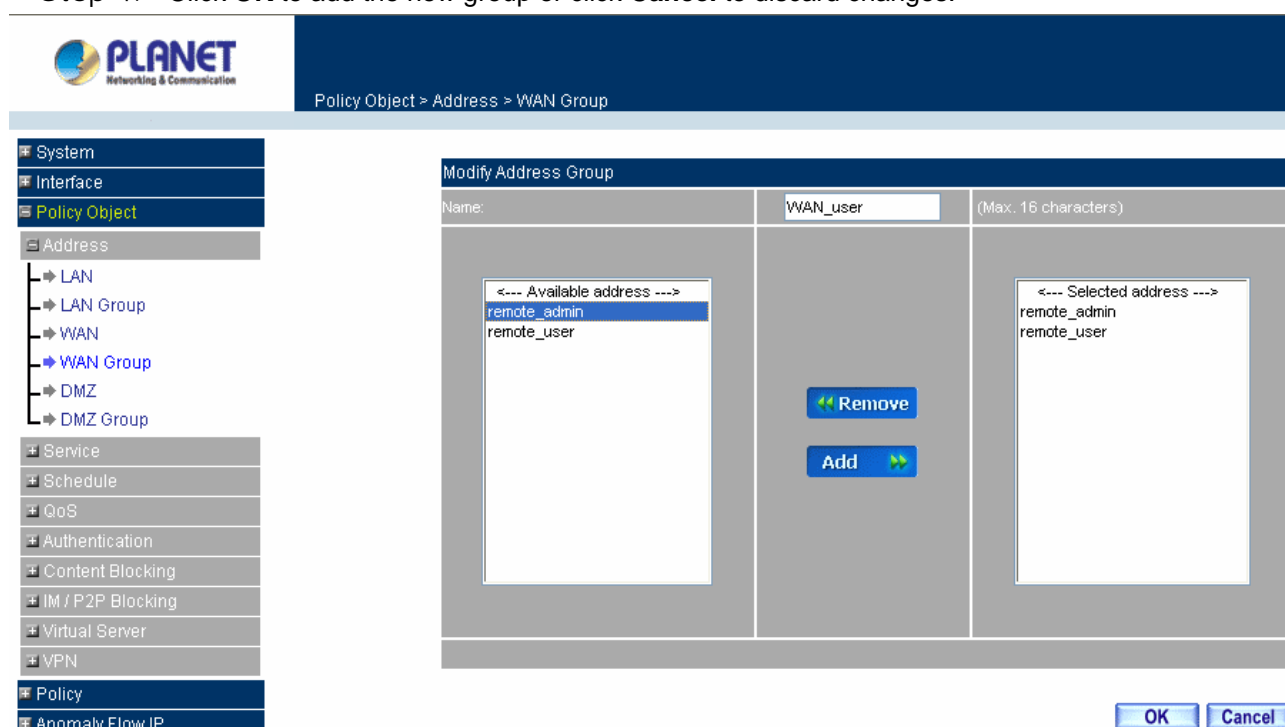
## Adding an WAN Group

Step 2. In the **WAN Group** window, click the **New Entry** button and the **Add New Address Group** window will appear.

Step 3. In the **Add New Address Group** window the following fields will appear:

- **Name:** Enter the name of the new group.
- **Available Address:** List the names of all the members of the WAN network.
- **Selected Address:** List the names to assign to the new group.
- **Add members:** Select the names to be added in the **Available Address** list, and click the **Add>>** button to add them to the **Selected Address** list.
- **Remove members:** Select the names to be removed in the **Selected Address** list, and click the **<<Remove** button to remove them from the **Selected Address** list.


Step 4. Click **OK** to add the new group or click **Cancel** to discard changes.



## 6.1.5 DMZ

### Entering the DMZ window:

Click **DMZ** under the **Address** menu to enter the **DMZ** window. The current setting information such as the name of the DMZ network, IP, and Netmask addresses will show on the screen.



Policy Object > Address > DMZ

Name	IP / Netmask	MAC Address	Configure
DMZ_Any	0.0.0.0/0.0.0.0		In Use
DMZ_user1	10.0.0.10/255.255.255.255		Modify Remove
DMZ_user2	10.0.0.11/255.255.255.255		Modify Remove
DMZ_user3	10.0.0.12/255.255.255.255		Modify Remove

New Entry

## Definition

**Name:** Name of DMZ network address.

**IP:** IP address of DMZ network

**Netmask:** subnet mask of DMZ network.

**MAC Address:** MAC address corresponded with DMZ IP address.

**Configure:** You can configure the settings in DMZ network. Click **Modify** to change the parameters in DMZ network. Click **Remove** to delete the settings.




If one of the members has been added to **Policy** or **DMZ Group**, the **Configure** column will show the message – **In Use**. In this case, you are not allowed to modify or remove the setting. You have to remove the setting in **Policy** or **DMZ Group**, and then you are allowed to configure the DMZ address.

## Adding a new DMZ Address:

**Step 1.** In the DMZ window, click the **New Entry** button.

**Step 2.** In the **Add New Address** window, enter the settings for a new DMZ address.

**Step 3.** Click **OK** to add the specified DMZ or click **Cancel** to discard changes.



Policy Object > Address > DMZ

Add New Address

Name: DMZ\_user1 (Max. 16 characters)

IP Address: 10.0.0.10

Netmask: 255.255.255.255 ( 255.255.255.255 means the specified PC )  
( 255.255.255.0 means class C subnet )

MAC Address:  Clone MAC Address

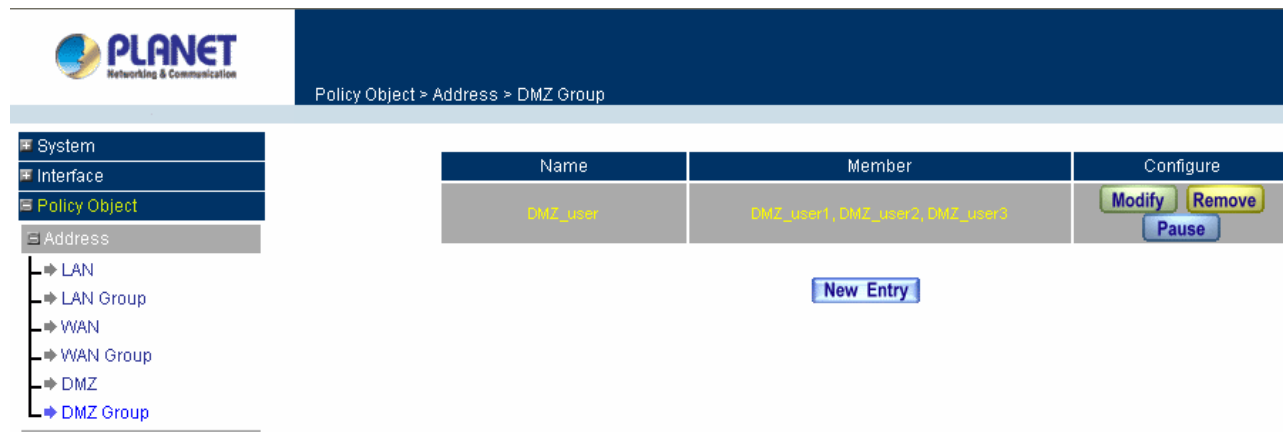
☐ Get static IP address from DHCP Server.

OK Cancel

## 6.1.6 DMZ Group

### Entering the DMZ Group window

Click **DMZ Group** under the **Address** menu to enter the **DMZ** window. The current settings information for the DMZ group appears on the screen.



The screenshot shows the PLANET web interface. The breadcrumb trail is "Policy Object > Address > DMZ Group". On the left, a tree view shows the navigation structure: System, Interface, Policy Object, Address (expanded), LAN, LAN Group, WAN, WAN Group, DMZ, and DMZ Group (selected). The main content area displays a table with three columns: Name, Member, and Configure. The table contains one entry: "DMZ\_user" in the Name column, "DMZ\_user1, DMZ\_user2, DMZ\_user3" in the Member column, and "Modify", "Remove", and "Pause" buttons in the Configure column. A "New Entry" button is located below the table.

Name	Member	Configure
DMZ_user	DMZ_user1, DMZ_user2, DMZ_user3	Modify Remove Pause

New Entry

### Definitions:

**Name:** Name of the DMZ group.

**Member:** Members of the group.


**Configure:** Configure the settings of DMZ group. Click **Modify** to change the parameters of DMZ group. Click **Remove** to delete the selected group.



If one of the DMZ Group has been added to **Policy**, the **Configure** column will show the message – **In Use**. In this case, you are not allowed to modify or remove the DMZ group. You have to remove the Group in **Policy** window, and then you are allowed to configure the DMZ Group.

### Adding a DMZ Group:

- Step 1. In the **DMZ Group** window, click the **New Entry** button and the **Add New Address Group** window will appear.
- Step 2. In the **Add New Address Group** window the following fields will appear:
  - **Name:** Enter the name of the new group.
  - **Available Address:** List the names of all the members of the DMZ network.
  - **Selected Address:** List the names to assign to the new group.
  - **Add members:** Select the names to be added in the **Available Address** list, and click the **Add>>** button to add them to the **Selected Address** list.
  - **Remove members:** Select the names to be removed in the **Selected Address** list, and click the **<<Remove** button to remove them from the **Selected Address** list.
- Step 3. Click **OK** to add the new group or click **Cancel** to discard changes.



Policy Object > Address > DMZ Group

System

Interface

Policy Object

Address

LAN

LAN Group

WAN

WAN Group

DMZ

DMZ Group

Service

Schedule

QoS

Authentication

Content Blocking

IM / P2P Blocking

Virtual Server

VPN

Policy

Anomaly Flow IP

Monitor

Add New Address Group

Name:DMZ\_user(Max. 16 characters)

<--- Available address --->  
DMZ\_user1  
DMZ\_user2  
DMZ\_user3

Remove

Add

<--- Selected address --->  
DMZ\_user1  
DMZ\_user2

OK

Cancel

- 50 -

### 6.1.7 Example1

**Under DHCP situation, assign the specific IP to static users and restrict them to access FTP net service only through policy**

**STEP 1** . Select **LAN** in **Address** and enter the following settings:

- Click **New Entry** button
- **Name:** Enter Rayearth
- **IP Address:** Enter 192.168.3.2
- **Netmask:** Enter 255.255.255.255
- **MAC Address :** Enter the user's MAC Address ( 00:B0:18:25:F5:89 )
- Select **Get static IP address from DHCP Server**
- Click **OK**

Add New Address	
Name	Rayearth (Max. 16 characters)
IP Address	192.168.3.2
Netmask	255.255.255.255 ( 255.255.255.255 means the specified PC ) ( 255.255.255.0 means class C subnet )
MAC Address	00:B0:18:25:F5:89 <a href="#">Clone MAC Address</a>
<input checked="" type="checkbox"/> Get static IP address from DHCP Server.	

[OK](#) [Cancel](#)

#### Setting LAN Address Book WebUI

Name	IP / Netmask	MAC Address	Configure
Inside_Any	0.0.0.0/0.0.0.0		<a href="#">In Use</a>
Rayearth	192.168.3.2/255.255.255.255	00:B0:18:25:F5:89	<a href="#">Modify</a> <a href="#">Remove</a>

[New Entry](#)

#### Complete the Setting of LAN

**STEP 2 . Adding the following setting in **Outgoing Policy**:**

Comment :  (Max. 32 characters)

Modify Policy	
Source Address	Rayearth <input type="button" value="v"/>
Destination Address	Outside_Any <input type="button" value="v"/>
Service	FTP <input type="button" value="v"/>
Schedule	None <input type="button" value="v"/>
Authentication User	None <input type="button" value="v"/>
Tunnel	None <input type="button" value="v"/>
Action, WAN Port	PERMIT ALL <input type="button" value="v"/>
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> Enable
IM / P2P Blocking	None <input type="button" value="v"/>
QoS	None <input type="button" value="v"/>
MAX. Bandwidth Per Source IP	Downstream <input type="text" value="0"/> Kbps Upstream <input type="text" value="0"/> Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )

**Add a Policy of Restricting the Specific IP to Access to Internet****STEP 3 . Complete assigning the specific IP to static users in **Outgoing Policy** and restrict them to access FTP net service only through policy:**

Source	Destination	Service	Action	Option					Configure			Move
Rayearth	Outside_Any	FTP	✓						<input type="button" value="Modify"/>	<input type="button" value="Remove"/>	<input type="button" value="Pause"/>	To 1 <input type="button" value="v"/>

**Complete the Policy of Restricting the Specific IP to Access to Internet**

### 6.1.8 Example2

#### Setup a policy that only allows partial users to connect with specific IP (External Specific IP)

**STEP 1 .** Setting several LAN network Address.

Name	IP / Netmask	MAC Address	Configure
Inside_Any	0.0.0.0/0.0.0.0		In Use
Rayearth	192.168.1.2/255.255.255.255	00:B0:18:25:F5:89	Modify Remove
Josh	192.168.1.4/255.255.255.255		Modify Remove
SinSan	192.168.1.5/255.255.255.255	00:B0:18:25:F5:87	Modify Remove
Daniel	192.168.1.7/255.255.255.255	00:B0:18:25:F5:45	Modify Remove
Luke	192.168.1.10/255.255.255.255		Modify Remove

New Entry

#### Setting Several LAN Network Address

**STEP 2 .** Enter the following settings in **LAN Group of Address**:

- Click **New Entry**
- Enter the **Name** of the group
- Select the users in the **Available Address** column and click **Add**
- Click **OK**

Add New Address Group

Name:
TestTeam
(Max. 16 characters)

<--- Available address --->

Rayearth
Josh
SinSan
Daniel
Luke

Remove
Add

<--- Selected address --->

Rayearth
Josh
SinSan

OK
Cancel

#### Add New LAN Address Group

Name	Member	Configure
TestTeam	Rayearth, Josh, SinSan	<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>

### Complete Adding LAN Address Group



The setting mode of **WAN Group** and **DMZ Group** of **Address** are the same as **LAN Group**.

**STEP 3 .** Enter the following settings in **WAN** of **Address** function:

- Click **New Entry**
- Enter the following data (**Name**, **IP Address**, **Netmask**)
- Click **OK**

Add New Address	
Name	<input type="text" value="Yahoo"/> (Max. 16 characters)
IP Address	<input type="text" value="202.1.237.21"/>
Netmask	<input type="text" value="255.255.255.255"/> ( 255.255.255.255 means the specified PC )
( 255.255.255.0 means class C subnet )	

### Add New WAN Address

Name	IP / Netmask	Configure
Outside_Any	0.0.0.0/0.0.0.0	<input type="button" value="In Use"/>
Yahoo	202.1.237.21/255.255.255.255	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

### Complete the Setting of WAN Address



**STEP 4 . To exercise STEP1~3 in Policy**

Comment :  (Max. 32 characters)

Modify Policy	
Source Address	TestTeam ▼
Destination Address	Yahoo ▼
Service	ANY ▼
Schedule	None ▼
Authentication User	None ▼
Tunnel	None ▼
Action, WAN Port	PERMIT ALL ▼
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> Enable
IM / P2P Blocking	None ▼
QoS	None ▼
MAX. Bandwidth Per Source IP	Downstream <input type="text" value="0"/> Kbps Upstream <input type="text" value="0"/> Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )

**To Exercise Address Setting in Policy**

Source	Destination	Service	Action	Option					Configure			Move
TestTeam	Yahoo	ANY	✓						<input type="button" value="Modify"/>	<input type="button" value="Remove"/>	<input type="button" value="Pause"/>	To 1 ▼

**Complete the Policy Setting**

The **Address** function really take effect only if use with **Policy**.

## 6.2 Service

In this section, network services are defined and new network services can be added. There are three sub menus under Service which are: **Pre-defined, Custom, and Group**. The Administrator can simply follow the instructions below to define the protocols and port numbers for network communication applications. Users then can connect to servers and other computers through these available network services.

### What is Service?

TCP and UDP protocols support varieties of services, and each service consists of a TCP Port or UDP port number, such as TELNET(23), SMTP(21), POP3(110),etc. MH-2001 defines two services: pre-defined service and custom service. The common-use services like TCP and UDP are defined in the pre-defined service and cannot be modified or removed. In the custom menu, users can define other TCP port and UDP port numbers that are not in the pre-defined menu according to their needs. When defining custom services, the client port ranges from 0 to 65535 and the server port ranges from 0 to 65535.

### How do I use Service?

The Administrator can add new service group names in the Group option under Service menu, and assign desired services into that new group. Using service group the Administrator can simplify the processes of setting up control policies. For example, there are 10 different computers that want to access 5 different services on a server, such as HTTP, FTP, SMTP, POP3, and TELNET. Without the help of service groups, the Administrator needs to set up 50 (10x5) control policies, but by applying all 5 services to a single group name in the service field, it takes only one control policy to achieve the same effect as the 50 control policies.

### 6.2.1 Pre-defined

#### Entering a Pre-defined window





- Step 1. Click **Pre-defined** under it. A window will appear with a list of services and their associated IP addresses. This list cannot be modified.



The screenshot shows the Planet Network & Communication software interface. On the left is a navigation tree with the following items: System, Interface, Policy Object (selected), Address, Service, Pre-defined (selected), Custom, Group, Schedule, QoS, Authentication, Content Blocking, IM / P2P Blocking, Virtual Server, and VPN. The main window title is 'Policy Object > Service > Pre-defined'. It displays a grid of 20 services, each with a protocol icon, protocol name, and port number. The services are arranged in four columns and five rows.

ANY ANY (Any)	TCP IMAP (143)	TCP POP3 (110)	TCP TELNET (23)
TCP AFPoverTCP (548)	TCP InterLocator (389)	TCP PPTP (1723)	UDP FTP (89)
TCP AOL (5190-5194)	TCP IRC (6660-6669)	TCP Real-Media (7070)	ICMP Traceroute (3,11)
TCP BGP (179)	TCP L2TP (1701)	UDP RP (520)	UDP TCP-ANY (Any)
UDP DNS (53)	TCP LDAP (389)	TCP RLOGIN (513)	UDP RUP (540)
TCP FINGER (79)	TCP NetMeeting (389&1503&1720)	TCP SMTP (25)	TCP VDO-Live (7000-7010)
TCP FTP (20-21)	UDP NFS (111)	UDP Ssh (161)	TCP WAIS (210)
TCP GOPHER (70)	TCP NNTP (119)	TCP SSH (22)	TCP WINFRAME (1494)
TCP HTTP (80)	UDP NTP (123)	UDP SYSLOG (514)	TCP X-Windows (6000-6063)
TCP HTTPS (443)	UDP PC-Anywhere (5631-5632)	UDP TALK (517-518)	TCP MSN (1863)
UDP NSE (500)	ICMP PING (Any)	TCP TCP-ANY (Any)	

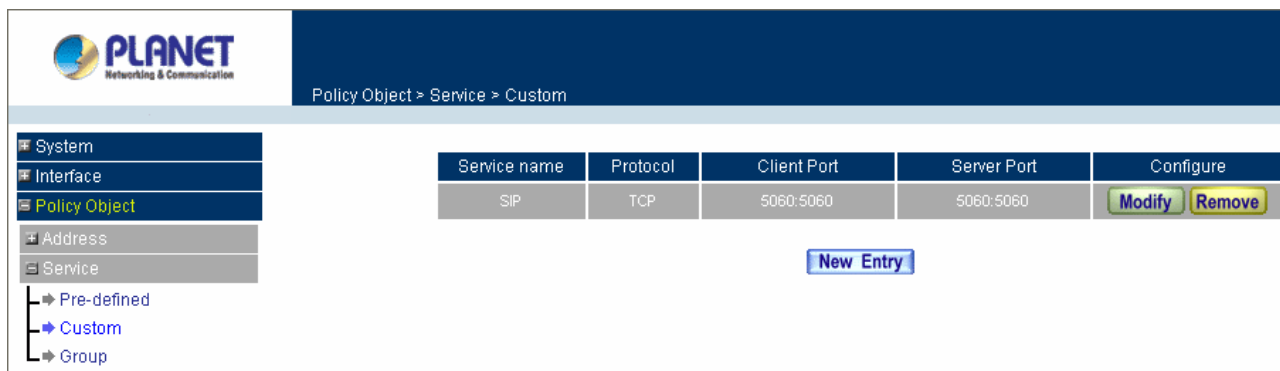
## Icons and Descriptions

Figure	Description
	Any Service
	TCP services, e.g. TCP, FTP, FINGER, HTTP, HTTPS, IMAP, SMTP, POP3, ANY, AOL, BGP, GOPHER, Inter Locator, IRC, L2TP, LDAP, NetMeeting, NNTP, PPTP, Real Media, RLOGIN, SSH, TCP ANY, TELNET, VDO Live, WAIS, WINFRAME, X-WINDOWS, MSN, etc.
	UDP services, e.g. IKE, DNS, NTP, RIP, SNMP, SYSLOG, TALK, TFTP, UDP-ANY, UUCP, NFS, PC Anywhere, etc.
	ICMP services, e.g. PING, TRACEROUTE, etc.

### 6.2.2 Custom

#### Entering the Custom window

Step 1. Click **Custom** under Service menu. A window will appear with a table showing all services currently defined by the Administrator.



#### Definitions:

**Service name:** The defined service name.

**Protocol:** Network protocol used in the basic setting. Such as TCP 、UDP or others.

**Client port:** The range of Client port in defined service. If the number of ports entered in the two fields of Client port is different, it means that the port numbers between these two numbers are opened. If the number of ports entered in the two fields of Client port is identical, it means that the entered port number is opened.

**Server port:** The range of Serer port in defined service.

If the number of ports entered in the two fields of Server port is different, it means that the port numbers between these two numbers are opened. If the number of ports entered in the two fields of Server port is identical, it means that the entered port number is opened.

**Configure:** Configure the settings in Service table. Click **Modify** to change the parameters in Service table. Click **Remove** to delete the selected setting.



If one of the Services has been added to **Policy or Group**, **Configure** column will show the message – **In Use**. In this case, you are not allowed to modify or remove the settings. You have to remove the setting in **Policy or Group** window, and then you are allowed to configure the settings.

## Adding a new Service

Step 1. In the **Custom** window, click the **New Entry** button and a new service table appears.

- **New Service Name:** This will be the name referencing the new service.
- **Protocol:** Enter the network protocol type to be used, such as TCP, UDP, or Other (please enter the number for the protocol type).
- **Client Port:** enter the range of port number of new clients.
- **Server Port:** enter the range of port number of new servers.

Step 2. Click **OK** to add new services, or click **Cancel** to cancel.

The screenshot shows the PLANET Network & Communication web interface. The breadcrumb navigation is 'Policy Object > Service > Custom'. On the left, a sidebar menu shows 'Policy Object' selected, with sub-items 'Pre-defined', 'Custom', and 'Group'. The main area is titled 'Add User Defined Service'. It contains a 'Service NAME' field with 'P2P' entered (Max. 16 characters). Below this is a table with 8 rows. Each row has columns for '#', 'Protocol (Range: 1 - 255)', 'Client Port (Range: 0 - 65535)', and 'Server Port (Range: 0 - 65535)'. The first row is pre-filled with '1', 'TCP', '22128', and '22500'. The other rows are empty. At the bottom right, there are 'OK' and 'Cancel' buttons.

#	Protocol (Range: 1 - 255)	Client Port (Range: 0 - 65535)	Server Port (Range: 0 - 65535)
1	TCP	22128	22500
2	TCP	0	0
3	TCP	0	0
4	TCP	0	0
5	TCP	0	0
6	TCP	0	0
7	TCP	0	0
8	TCP	0	0

## 6.2.3 Group

### Entering the Group window

Click **Group** under Service menu. A window will appear with a table displaying current service group settings.

The screenshot shows the PLANET Network & Communication web interface. The breadcrumb navigation is 'Policy Object > Service > Group'. On the left, a sidebar menu shows 'Policy Object' selected, with sub-items 'Pre-defined', 'Custom', and 'Group'. The main area displays a table with 3 columns: 'Group name', 'Service', and 'Configure'. The first row shows 'Internet' under 'Group name' and 'DNS,FTP,HTTP...' under 'Service'. The 'Configure' column has 'Modify' and 'Remove' buttons. Below the table, there is a 'New Entry' button.

Group name	Service	Configure
Internet	DNS,FTP,HTTP...	Modify Remove

**Definitions:**

**Group name:** The Group name of the defined Service.

**Service:** The Service item of the Group.

**Configure:** Configure the settings of Group. Click **Modify** to change the parameters of the Group.  
Click **Remove** to delete the Group.



If one of the Services has been added to **Policy**, **Configure** column will show the message – **In Use**.

In this case, you are not allowed to modify or remove the settings. You have to remove the setting in **Policy** window, and then you are allowed to configure the settings.

**Adding Service Groups**

Step 1. In the **Group** window, click the **New Entry** button.

Step 2. In the **Add Service Group** window, the following fields will appear:

- **Available Services:** list all the available services.
- **Selected Services:** list services to be assigned to the new group.

Step 3. Enter the new group name in the group **Name** field. This will be the name referencing the created group.

Step 4. **To add new services:** Select the services desired to be added in the **Available Services** list and then click the **Add>>** button to add them to the group.

Step 5. **To remove services:** Select services desired to be removed in the **Selected Services**, and then click the **<<Remove** button to remove them from the group.

Step 6. Click **OK** to add the new group.

The screenshot displays the PLANET Networking & Communication configuration interface. The left sidebar shows a tree view with categories: System, Interface, Policy Object, Address, Service, Schedule, QoS, Authentication, Content Blocking, IM / P2P Blocking, Virtual Server, VPN, Policy, Anomaly Flow IP, and Monitor. The 'Policy Object' category is expanded, showing 'Pre-defined' and 'Custom' sub-items. The 'Group' item under 'Custom' is selected. The main window is titled 'Add Service Group' and contains the following elements:

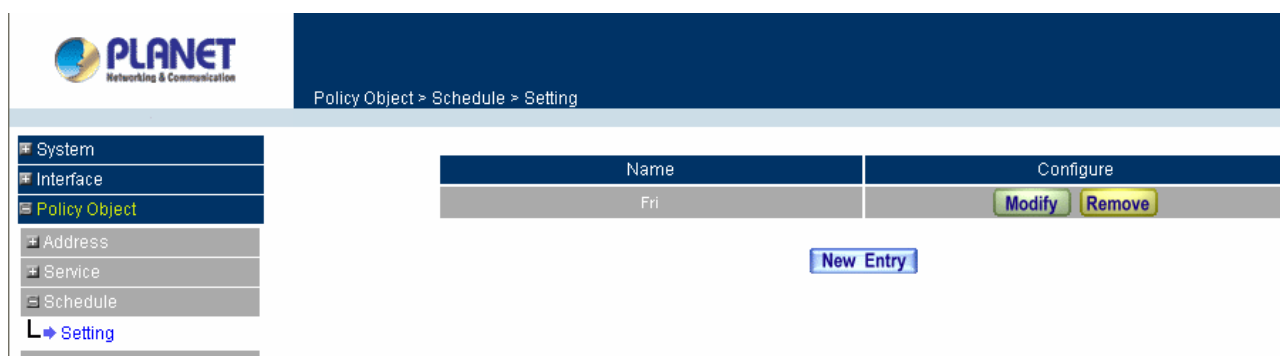
- Name:** A text field containing 'Internet' with a note '(Max. 16 characters)'.
- Available service list:** A list box containing the following services: ANY, AFPOverTCP, AOL, BGP, DNS, FINGER, FTP, GOPHER, HTTP, HTTPS, IKE, IMAP, InterLocator, and IRC. The 'DNS' service is currently selected.
- Selected service list:** A list box containing the services: DNS, FTP, HTTP, and HTTPS.
- Buttons:** A 'Remove' button (with a left-pointing arrow) and an 'Add' button (with a right-pointing arrow) are positioned between the two lists.
- Footer:** 'OK' and 'Cancel' buttons are located at the bottom right of the window.

## 6.3 Schedule

MH-2001 allows the Administrator to configure a schedule for policies to take affect. By creating a schedule, the Administrator is allowing MH-2001 policies to be used at those designated times only. Any activities outside of the scheduled time slot will not follow MH-2001 policies therefore will likely not be permitted to pass through MH-2001. The Administrator can configure the start time and stop time, as well as creating 2 different time periods in a day. For example, an organization may only want MH-2001 to allow the LAN network users to access the Internet during work hours. Therefore, the Administrator may create a schedule to allow MH-2001 to work Monday-Friday, 8AM - 5PM only. During the non-work hours, MH-2001 will not allow Internet access.

### Entering the Schedule window

Step 1. Click on **Setting** under **Schedule** menu and the schedule window will appear displaying the active schedules.



### Definitions:

**Name:** The name assigned to the schedule

**Configure:** Configure the settings of Schedule. Click **Modify** to change the parameters of the Schedule. Click Remove to delete the Schedule.




If one of the Schedule has been added to **Policy**, **Configure** column will show the message – **In Use**. In this case, you are not allowed to modify or remove the settings. You have to remove the setting in **Policy** window, and then you are allowed to configure the settings.

### Adding a new Schedule

Step 1. Click on the **New Entry** button and the **Add New Schedule** window will appear.

- **Schedule Name:** Fill in a name for the new schedule.
- **Period:** Configure the start and stop time for the days of the week that the schedule will be active.

Step 2. Click **OK** to save the new schedule or click **Cancel** to cancel adding the new schedule.



Policy Object > Schedule > Setting

- System
- Interface
- Policy Object
- Address
- Service
- Schedule
- Setting**
- QoS
- Authentication
- Content Blocking
- IM / P2P Blocking
- Virtual Server
- VPN
- Policy
- Anomaly Flow IP
- Monitor

### Add New Schedule

Schedule Name  (Max. 16 characters)

Week Day	Period	
	Start Time	Stop Time
Monday	Disable	Disable
Tuesday	Disable	Disable
Wednesday	Disable	Disable
Thursday	Disable	Disable
Friday	09:00	18:00
Saturday	Disable	Disable
Sunday	Disable	Disable



In setting a Schedule, the value in **Start time** must be less than the value in **Stop Time**, or you cannot add or configure the setting.

## 6.4 QoS

By configuring the QoS, you can control the outbound Upstream/downstream Bandwidth.

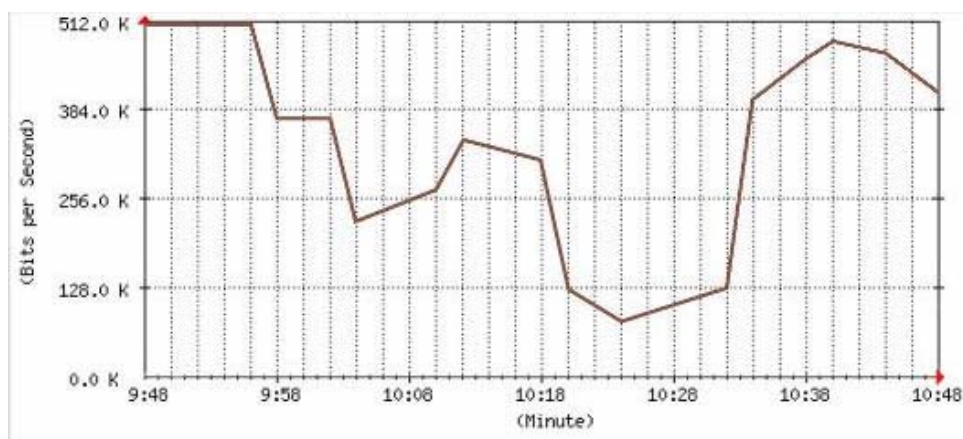
The administrator can configure the bandwidth according to the WAN bandwidth.

**Downstream Bandwidth:** To configure the Guaranteed Bandwidth and Maximum Bandwidth.

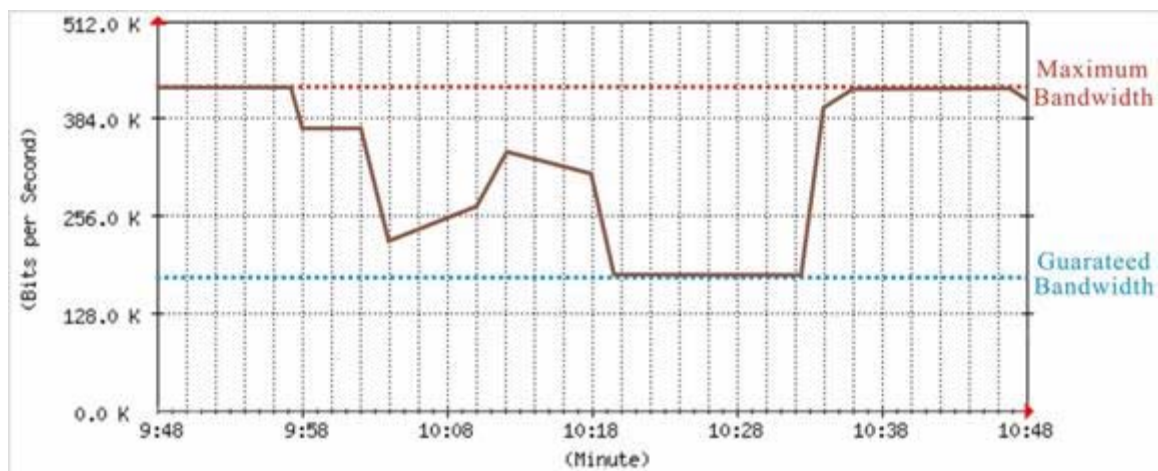
**Upstream Bandwidth:** To configure the Guaranteed Bandwidth and Maximum Bandwidth.

**QoS Priority:** To configure the priority of distributing Upstream/Downstream and unused bandwidth.

MH-2001 configures the bandwidth by different QoS, and selects the suitable QoS through Policy to control and efficiently distribute bandwidth. MH-2001 also makes it convenient for the administrator to make the Bandwidth reach the best Utility.




**The Flow Before Using QoS**



The Flow After Using QoS (Max. Bandwidth: 400Kbps, Guaranteed Bandwidth: 200Kbps)

## Configuration of QoS

Click on **Setting** under QoS menu and the QoS window will appear.



Policy Object > QoS > Setting

Name	WAN	Downstream Bandwidth	Upstream Bandwidth	Priority	Configure
HTTP	1	G.Bandwidth = 400 Kbps M.Bandwidth = 800 Kbps	G.Bandwidth = 400 Kbps M.Bandwidth = 800 Kbps	Middle	<div style="text-align: center;"> <div style="border: 1px solid black; padding: 2px 5px; background-color: #e0e0e0;">Modify</div> <div style="border: 1px solid black; padding: 2px 5px; background-color: #e0e0e0;">Remove</div> </div>
	2	G.Bandwidth = 0 Kbps M.Bandwidth = 0 Kbps	G.Bandwidth = 0 Kbps M.Bandwidth = 0 Kbps		

New Entry

## Definitions:

**Name:** The name of the QoS you want to configure.

**WAN:** Display WAN 1 or WAN 2.

**Downstream Bandwidth:** To configure the Guaranteed Bandwidth and Maximum Bandwidth.

**Upstream Bandwidth:** To configure the Guaranteed Bandwidth and Maximum Bandwidth.

**Priority:** To configure the priority of distributing Upstream/Downstream and unused bandwidth.

## Add New QoS

Step 1. Click on the **New Entry** button and the **Add New QoS** window will appear.

- **Name:** The name of the QoS you want to define.
- **Downstream Bandwidth:** To configure the Guaranteed Bandwidth and Maximum Bandwidth.
- **Upstream Bandwidth:** To configure the Guaranteed Bandwidth and Maximum Bandwidth.
- **QoS Priority:** To configure the priority of distributing Upstream/Downstream and unused bandwidth.



Step 2. Click the **OK** button to add new QoS.

The screenshot shows the PLANET web interface with the 'Policy Object > QoS > Setting' breadcrumb. On the left is a navigation menu with options: System, Interface, Policy Object (selected), Address, Service, Schedule, QoS, Setting (highlighted), Authentication, Content Blocking, IM / P2P Blocking, Virtual Server, and VPN. The main area is titled 'Add New QoS' and contains a 'Name' field with 'HTTP' and a '(Max. 16 characters)' hint. Below this is a table for configuring QoS for two WAN connections:

WAN	Downstream Bandwidth	Upstream Bandwidth	QoS Priority
1	G.Bandwidth = 400 Kbps ( Range: 1 - 1600 ) M.Bandwidth = 800 Kbps ( Range: 1 - 2000 )	G.Bandwidth = 400 Kbps ( Range: 1 - 1600 ) M.Bandwidth = 800 Kbps ( Range: 1 - 2000 )	<div>Middle ▼</div> <div>High</div> <div>Middle</div> <div>Low</div>
2	G.Bandwidth = 0 Kbps ( Range: 1 - 1000 ) M.Bandwidth = 0 Kbps ( Range: 1 - 1000 )	G.Bandwidth = 0 Kbps ( Range: 1 - 64 ) M.Bandwidth = 0 Kbps ( Range: 1 - 64 )	

At the bottom right of the configuration area are 'OK' and 'Cancel' buttons.

## 6.5 Authentication

By configuring the Authentication, you can control the user's connection authority. The user has to pass the authentication to access to Internet.

The MH-2001 appliance provided 3 authentication modes. The **User** and **User Group** built in; others are **RADIUS** and **POP3** self-built Authentication Server. The MIS engineer can use the 4 modes, to manage the authentication.

### 6.5.1 Auth Setting

The administrator can specify the port number and authentication time of authentication management system for LAN user to access WAN network.

#### Configuration of Authentication

Click **Authentication** in the menu bar on the left hand side and click **Auth Setting**. The **Authentication Management** window will appear as below.

The screenshot shows the PLANET web interface with the 'Policy Object > Authentication > Auth Setting' breadcrumb. On the left is a navigation menu with options: System, Interface, Policy Object (selected), Address, Service, Schedule, QoS, Authentication (selected), Auth Setting (highlighted), Auth User, Auth Group, RADIUS, POP3, Content Blocking, IM / P2P Blocking, Virtual Server, VPN, and Policy. The main area is titled 'Authentication Management' and contains the following configuration fields:

- Authentication Port: 82 (Range: 1 - 65535)
- Re-Login if Idle: 30 Minutes (Range: 1 - 1000)
- Re-Login after user login successfully: 0 Hours (Range: 0 - 24, 0 means unlimited)
- ☐ Disallow Re-Login if the auth user has login
- URL to redirect when authentication succeed: (Max. 60 characters)
- Messages to display when user login: (Text area)

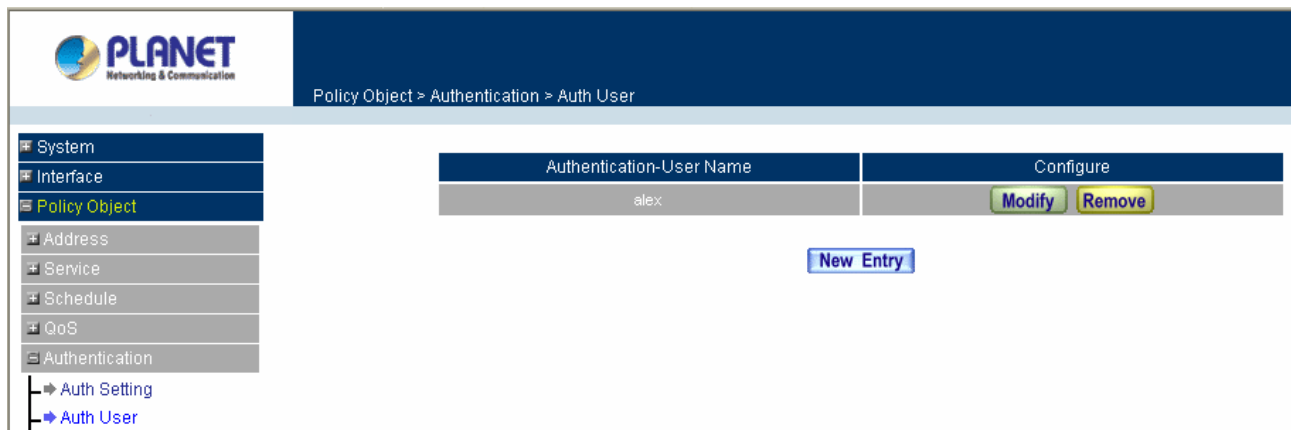
At the bottom right of the configuration area are 'OK' and 'Cancel' buttons.

**Definitions:**

- **Authentication Port:** The internal users have to pass the authentication to access to the Internet when enable MH-2001.
- **Re-Login if Idle:** When the internal user access to Internet, can setup the idle time after passing authentication. If idle time exceeds the time you setup, the authentication will be invalid. The default value is 30 minutes.
- **Re-Login after user login successfully :** When the LAN user connect to the WAN through the authentication. The available authentication time depends on the time limit, if over the default time setting, the authentication will be invalid.
- **Disallow Re-Login if the auth user has login :** When enable this function through **User, User Group, RADIUS** or **POP3** to access the authentication, the authorized account can not be used by other people.
- **URL to redirect when authentication succeed:** The user who had passes Authentication have to connect to the specific website. (It will connect to the website directly which the user want to login) The default value is blank.
- **Messages to display when user login:** It will display the login message in the authentication WebUI. (Support HTML) The default value is blank (display no message in authentication WebUI).

**6.5.2 Auth User**

Click **Authentication** in the menu bar on the left hand side and click **Auth User**.

**Definitions:**

**Name :** The name of the Authentication you want to configure.

**Configure:** modify settings or remove users.

**Adding a new Auth User**

**Step 1.** In the **Authentication** window, click the **New User** button to create a new **Auth User**.

**Step 2.** In the **Auth-User** window:

- **Auth-User Name:** enter the username of new **Authentication**.
- **Password:** enter a password for the new **Authentication**.
- **Confirm Password:** enter the password again.

**Step 3.** Click **OK** to add the user or click **Cancel** to cancel the setting

PLANET Networking & Communication

Policy Object > Authentication > Auth User

**Add New Authentication-User**

Authentication-User Name	alex	(Max. 16 characters)
Password	••••	(Max. 16 characters)
Confirm Password	••••	(Max. 16 characters)

OK Cancel

**Step 4.** In the form of controlling the [Outgoing] Policy, enable the Authentication-User Function.

PLANET Networking & Communication

Policy > Outgoing

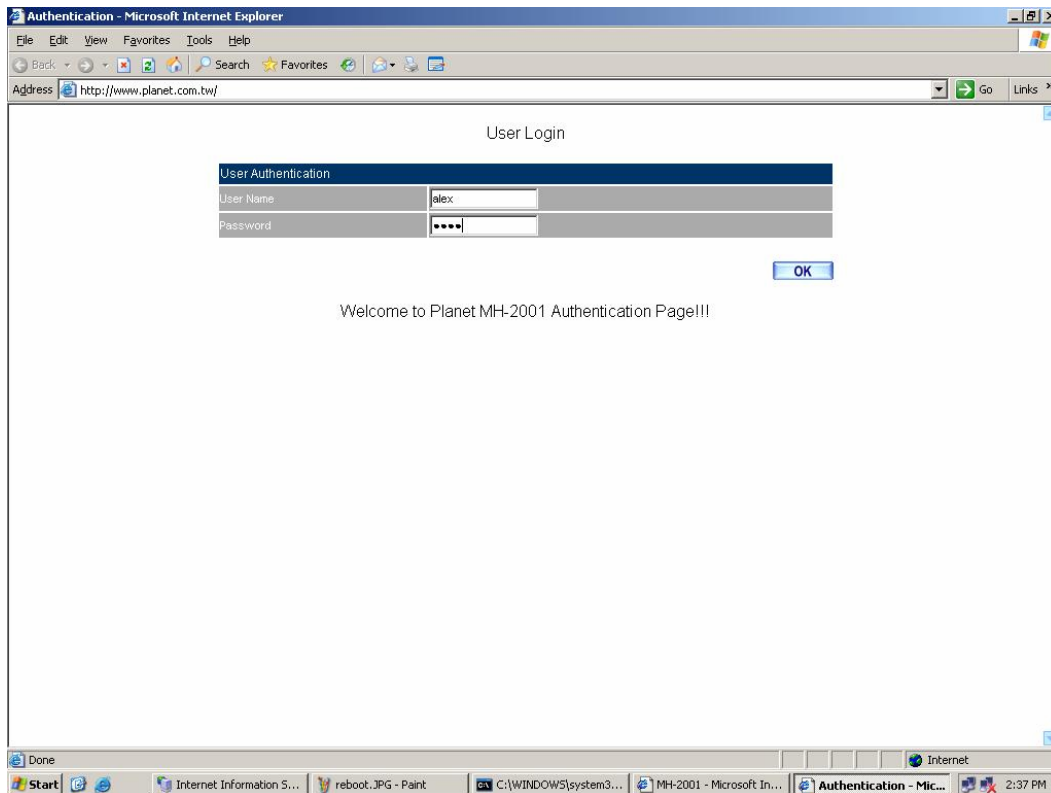
Comment : (Max. 32 characters)

**Modify Policy**

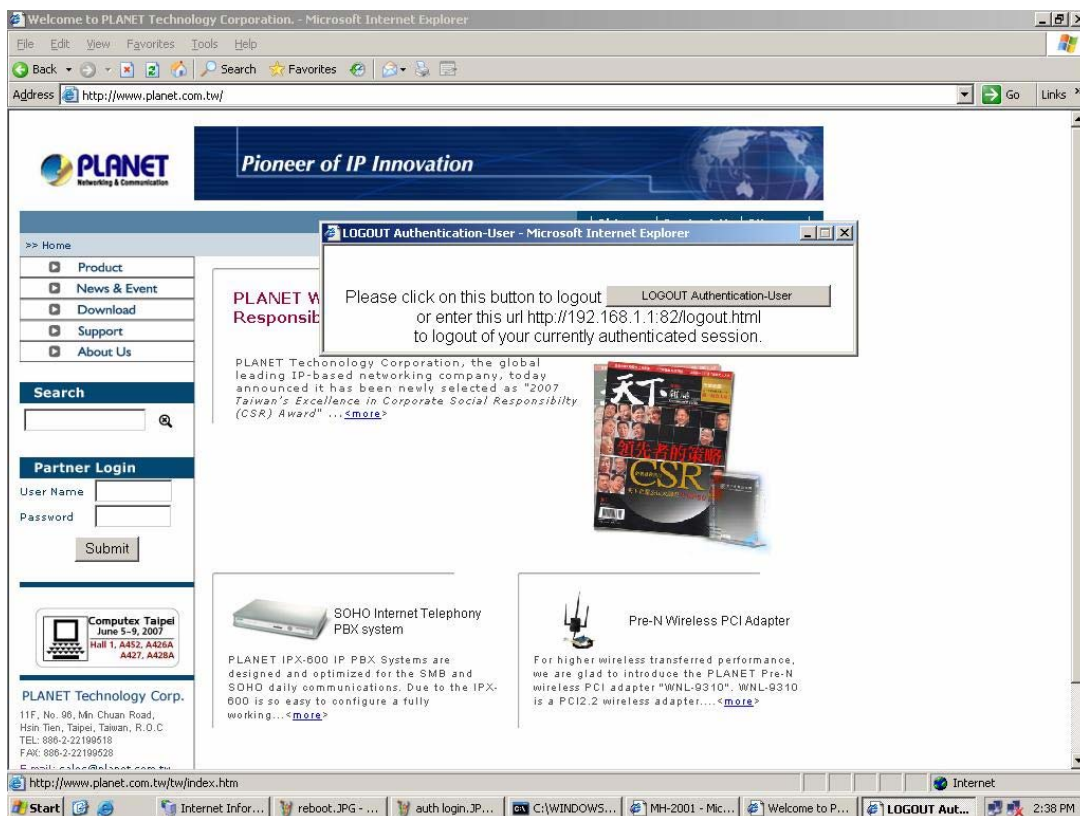
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	alex
Tunnel	None
Action, WAN Port	PERMIT ALL
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> Enable
IM / P2P Blocking	None
QoS	None
MAX. Bandwidth Per Source IP	Downstream 0 Kbps Upstream 0 Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	0 ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )

OK Cancel

- Step 5.** When the user connect to external network by Authentication, the following page will be displayed.  
Enter the User Name and Password for authentication.



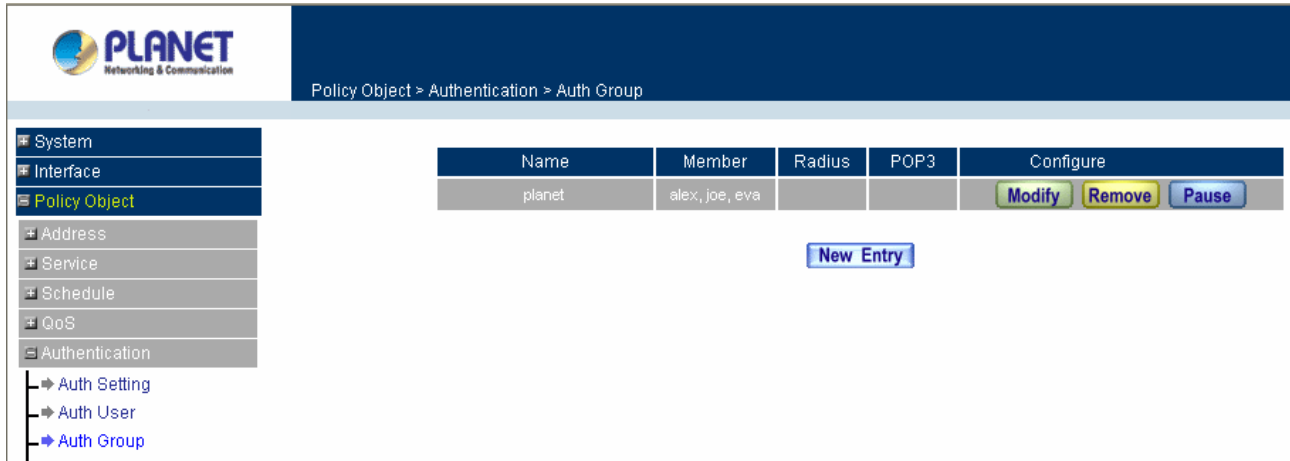
- Step 6.** Authentication success, it will pop-up a window that you can logout and you can access to internet.



### 6.5.3 Auth User Group

#### Entering the Auth User Group window

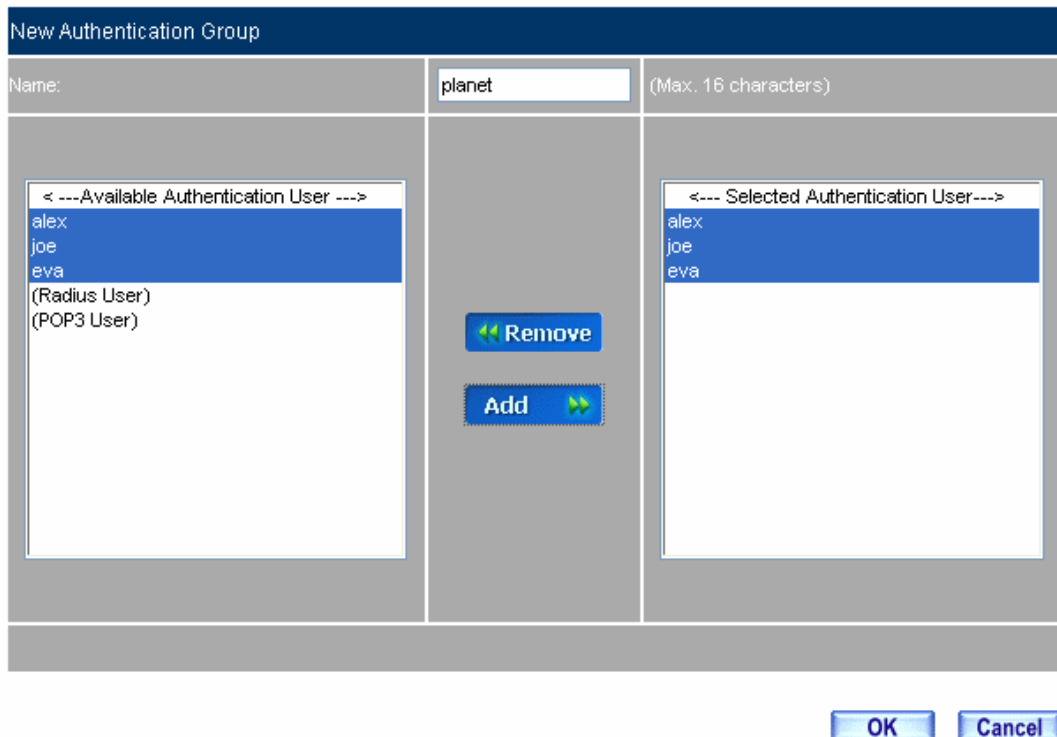
Click **Authentication** in the menu bar on the left hand side of the window and click **Auth Group** under it. A window will appear with a table displaying current Auth User Group settings by the Administrator.



#### Adding Auth Group

**STEP 1 .** Add **Auth Group** Setting in **Authentication** function and enter the following settings:

- Click **New Entry**
- **Name:** Enter laboratory
- Select the Auth User you want and **Add** to Selected Auth User
- Click **OK**
- Complete the setting of Auth User Group




#### Setting Auth Group WebUI

**STEP 2 . Add a policy in *Outgoing Policy* and input the Address and Authentication of STEP 1**

Comment :  (Max. 32 characters)

Modify Policy	
Source Address	Inside_Any ▾
Destination Address	Outside_Any ▾
Service	ANY ▾
Schedule	None ▾
Authentication User	planet ▾
Tunnel	None ▾
Action, WAN Port	PERMIT ALL ▾
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> Enable
IM / P2P Blocking	None ▾
QoS	None ▾
MAX. Bandwidth Per Source IP	Downstream <input type="text" value="0"/> Kbps Upstream <input type="text" value="0"/> Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )

**Auth-User Policy Setting**

Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY	✓		<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To 1 ▾

**Authentication User : planet**

Authentication User
alex
joe
eva

**Complete the Policy Setting of Auth-User**

**STEP 3 .** When user is going to access to Internet through browser, the authentication UI will appear in Browser. After entering the correct user name and password, click **OK** to access to Internet.

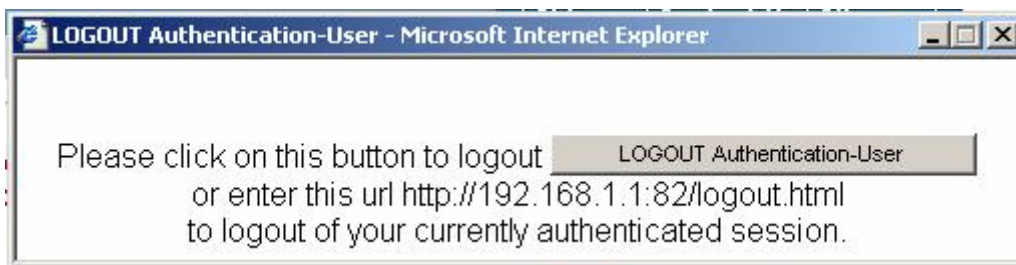
### User Login

User Authentication	
User Name	<input type="text" value="alex"/>
Password	<input type="password" value="...."/>
<input type="button" value="OK"/>	

Welcome to Planet MH-2001 Authentication Page!!!

### Access to Internet through Authentication WebUI

**STEP 4 .** If the user does not need to access to Internet anymore and is going to logout, he/she can click **LOGOUT Auth-User** to logout the system. Or enter the Logout Authentication WebUI ([http:// LAN Interface: Authentication port number/ logout.html](http://LAN Interface: Authentication port number/ logout.html)) to logout.



### Logout Auth-User WebUI

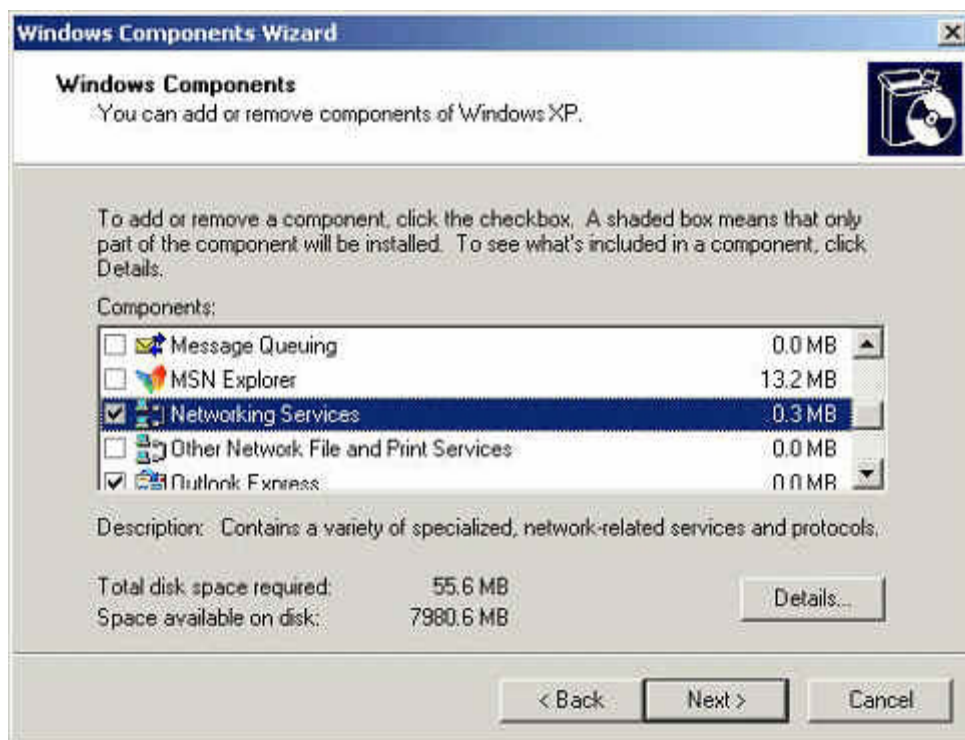
## 6.5.4 Radius Server

To plan the users connect to the WAN through the authentication in policy .To use the WAN RADIUS server (Windows 2003 Server built-in authentication).

### ※ Windows 2003 RADIUS Server Deployment

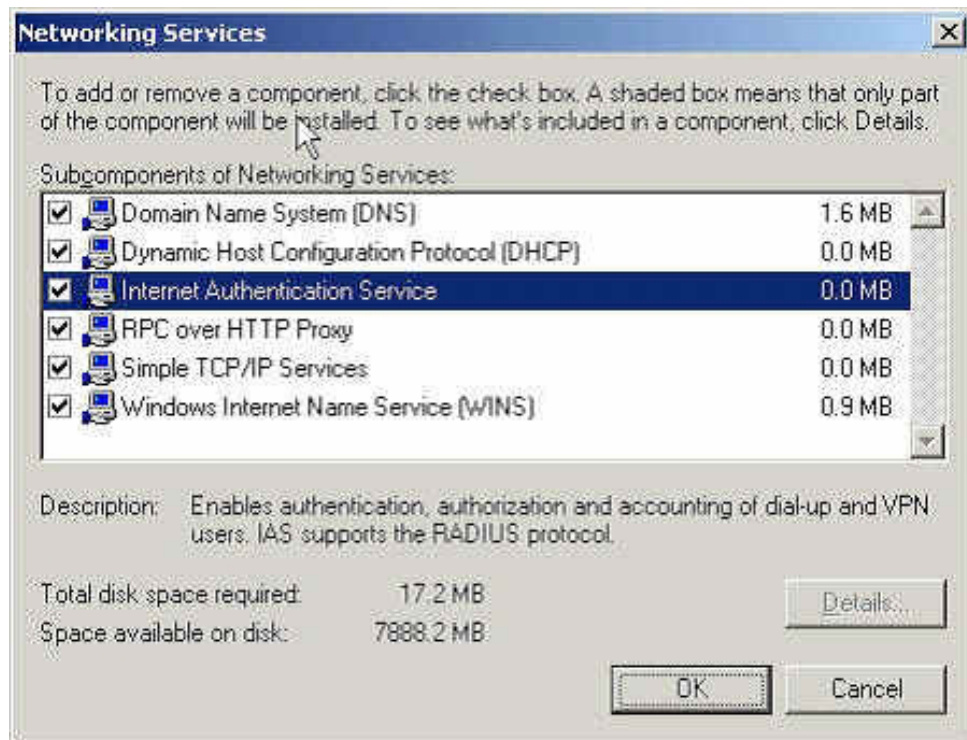
**STEP 1 .** Click **Start** → **Control Panel** → **Add / Remove Programs** select **Add / Remove Windows Components**, and then it shows the **Windows Components Wizard**.

**STEP 2 .** Select **Networking Services**, and then click **Details**.



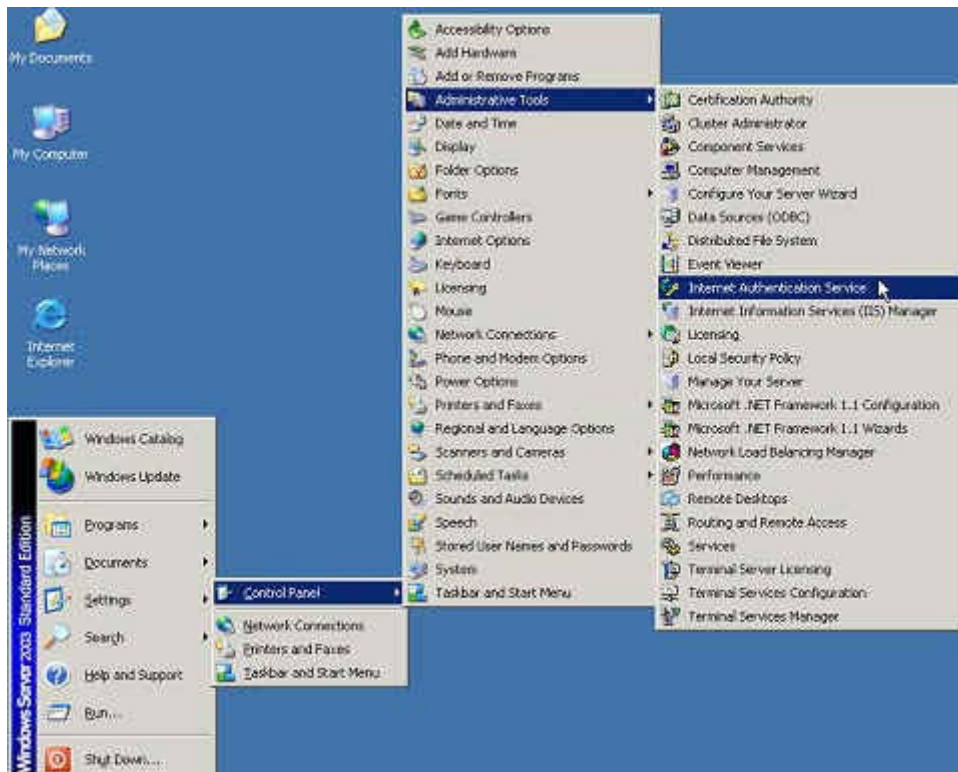
Windows components wizard



**STEP 3 . Select Internet Authentication Service.**

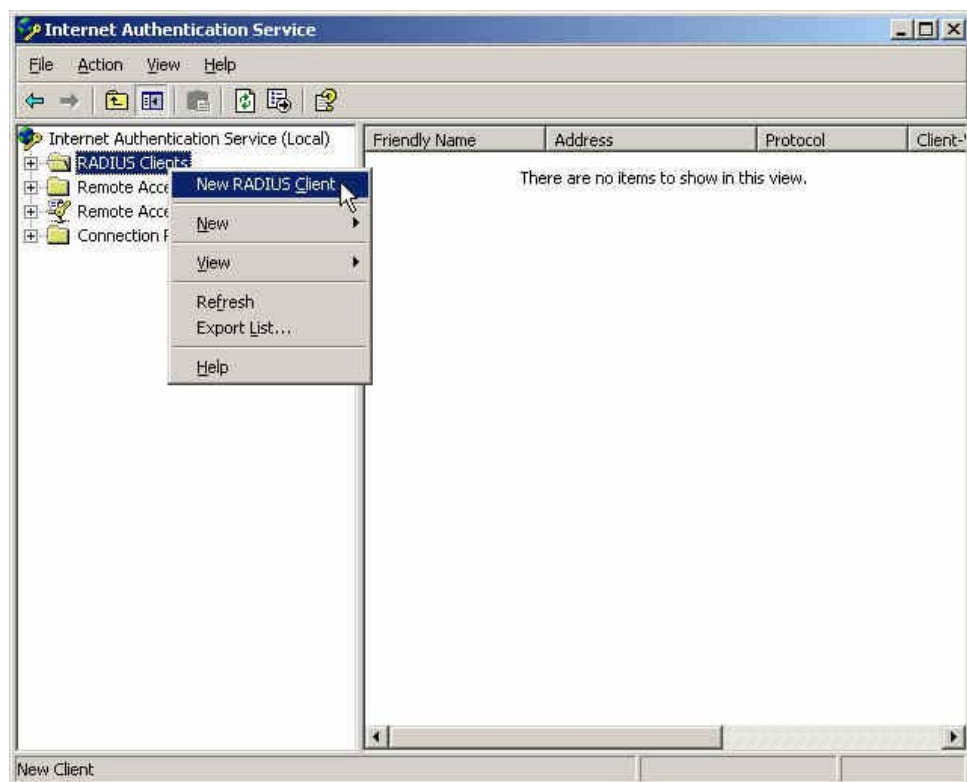
**Add new network authentication service components**

**STEP 4 .** Click **Start** → **Control Panel** → **Administrative Tools**, select **Network Authentication Service**.



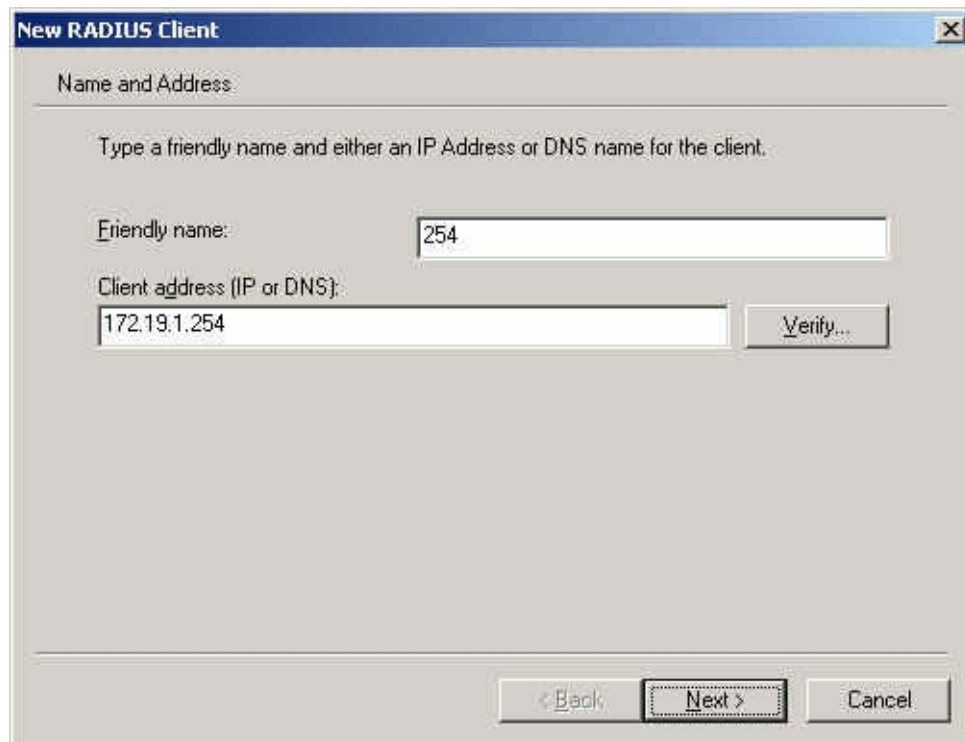
Select network authentication service

**STEP 5 .** Right click **RADIUS Clients** → **New RADIUS Client**.



**Add new RADIUS client**

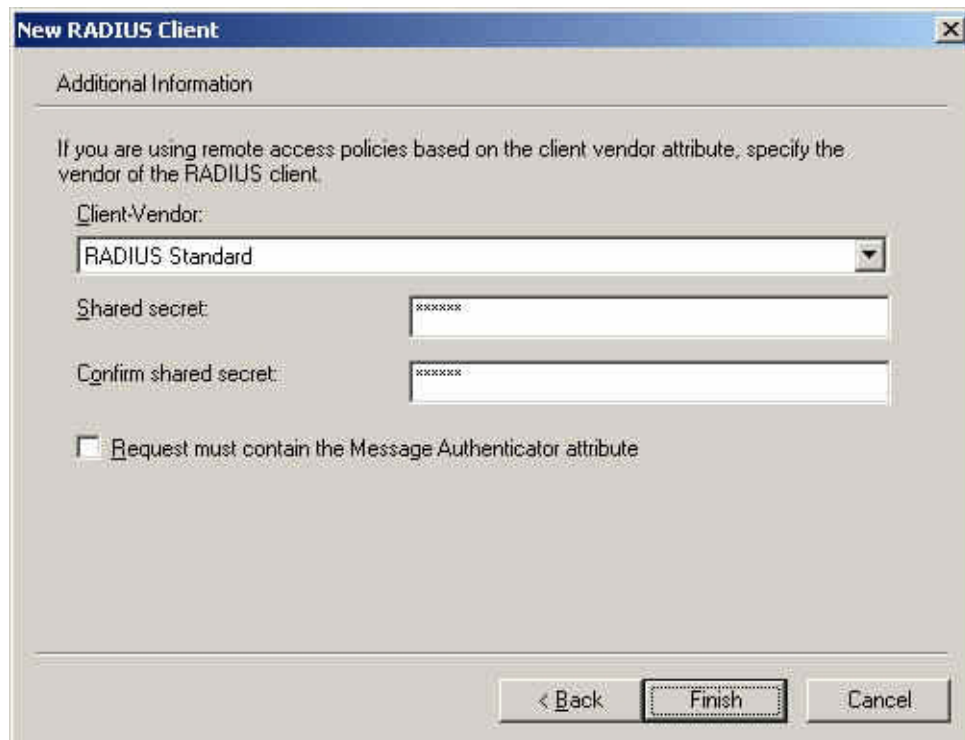
**STEP 6 .** Enter the **Name and Client Address** (It is the same as MH-2001 IP Address).



The image shows a Windows-style dialog box titled "New RADIUS Client". It has a blue title bar with a close button (X) in the top right corner. The main area is light gray. At the top, it says "Name and Address:" followed by a horizontal line. Below this, it says "Type a friendly name and either an IP Address or DNS name for the client." There are two text input fields. The first is labeled "Friendly name:" and contains the text "254". The second is labeled "Client address (IP or DNS):" and contains the text "172.19.1.254". To the right of the second field is a button labeled "Verify...". At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel". The "Next >" button is highlighted with a dashed border.

**Add New RADIUS client name and IP address setting**

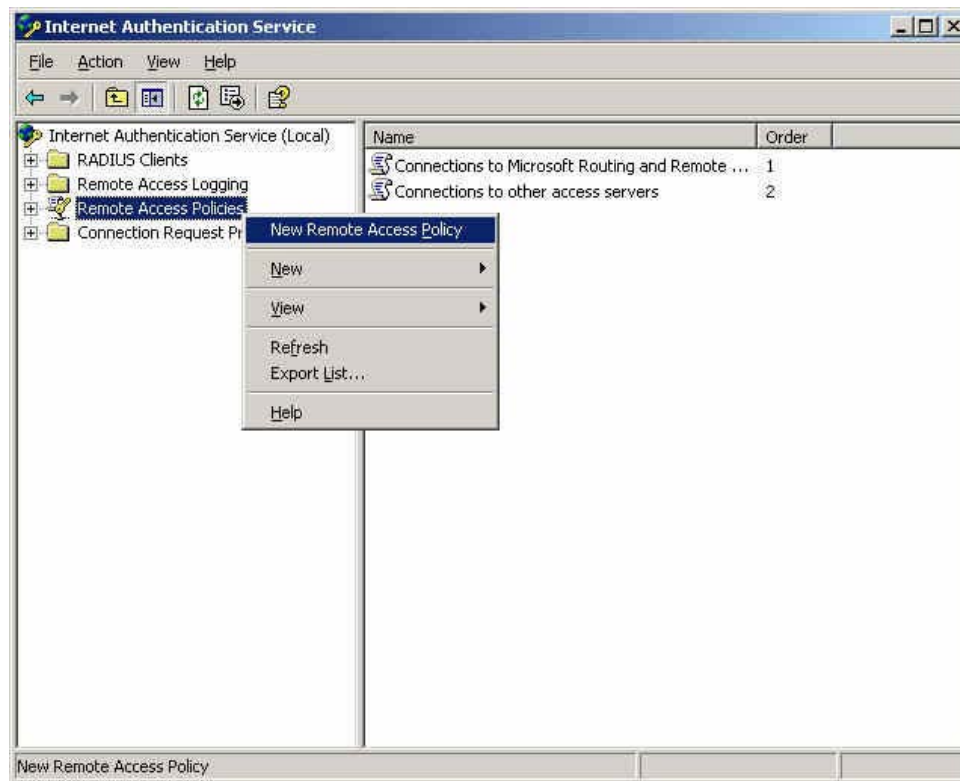
**STEP 7 .** Select **RADIUS Standard**; enter the Shared secret and Confirm Shared secret. (It must be the same setting as RADIUS in MH-2001.



The image shows a Windows-style dialog box titled "New RADIUS Client". It has a tab labeled "Additional Information". Below the tab, there is a text instruction: "If you are using remote access policies based on the client vendor attribute, specify the vendor of the RADIUS client." Below this, there is a label "Client-Vendor:" followed by a dropdown menu currently showing "RADIUS Standard". Below that are two text input fields: "Shared secret:" and "Confirm shared secret:", both containing masked text (asterisks). At the bottom left, there is a checkbox labeled "Request must contain the Message Authenticator attribute" which is currently unchecked. At the bottom right, there are three buttons: "< Back", "Finish", and "Cancel". The "Finish" button is highlighted with a dashed border.

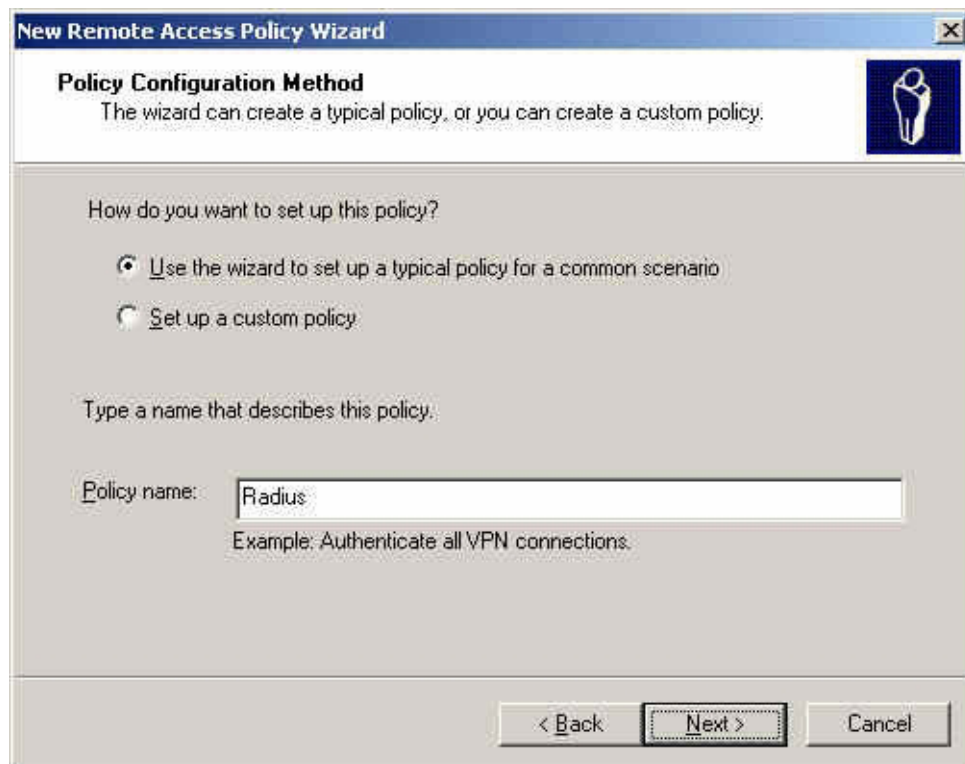
**Add new RADIUS client-vendor and shared secret**

**STEP 8 .** Right click on **Remote Access Policies**→ **New Remote Access Policy**.



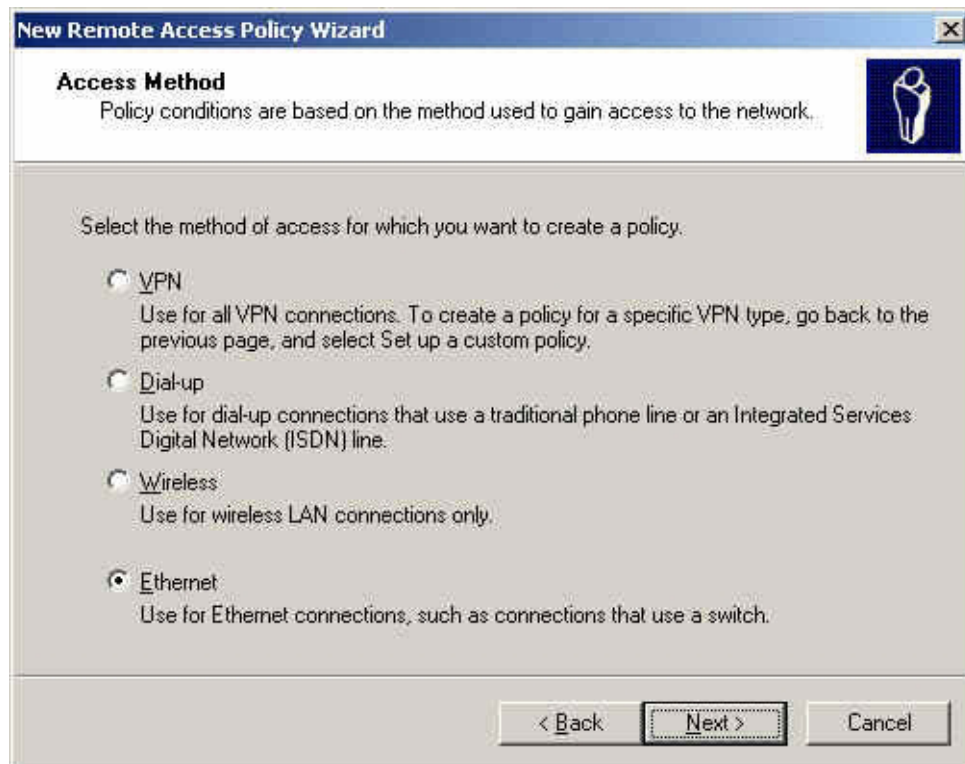
**Add new remote access policies**

**STEP 9 .** Select **Use the wizard to set up a typical policy for a common scenario**, and enter the **Policy name**.



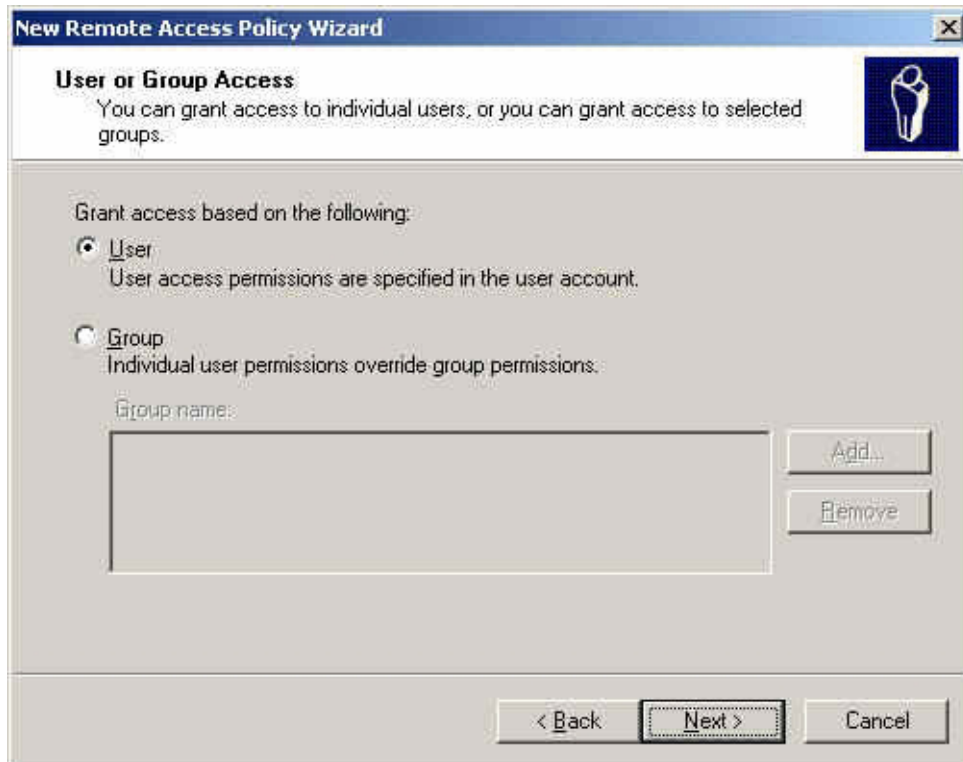
The image shows a Windows-style dialog box titled "New Remote Access Policy Wizard". It has a blue header bar with the title and a close button. Below the header, there's a section titled "Policy Configuration Method" with a small icon of a person. The text says "The wizard can create a typical policy, or you can create a custom policy." Below this, there's a question "How do you want to set up this policy?" with two radio button options: "Use the wizard to set up a typical policy for a common scenario" (which is selected) and "Set up a custom policy." Below the options, there's a text prompt "Type a name that describes this policy:" followed by a text input field containing the word "Radius". Below the input field, there's an example text "Example: Authenticate all VPN connections." At the bottom of the dialog, there are three buttons: "< Back", "Next >" (which is highlighted with a dashed border), and "Cancel".

**Add new remote access policies and policy name**

**STEP 10 . Select Ethernet.**

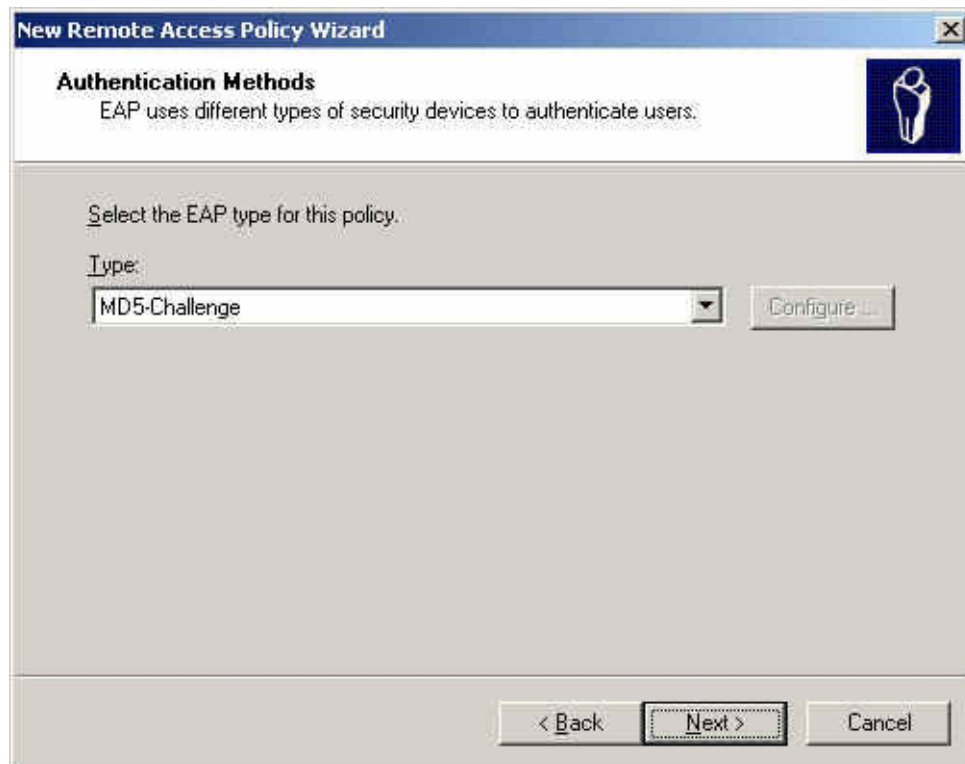
The way to add new remote access policy



**STEP 11 . Select User.**

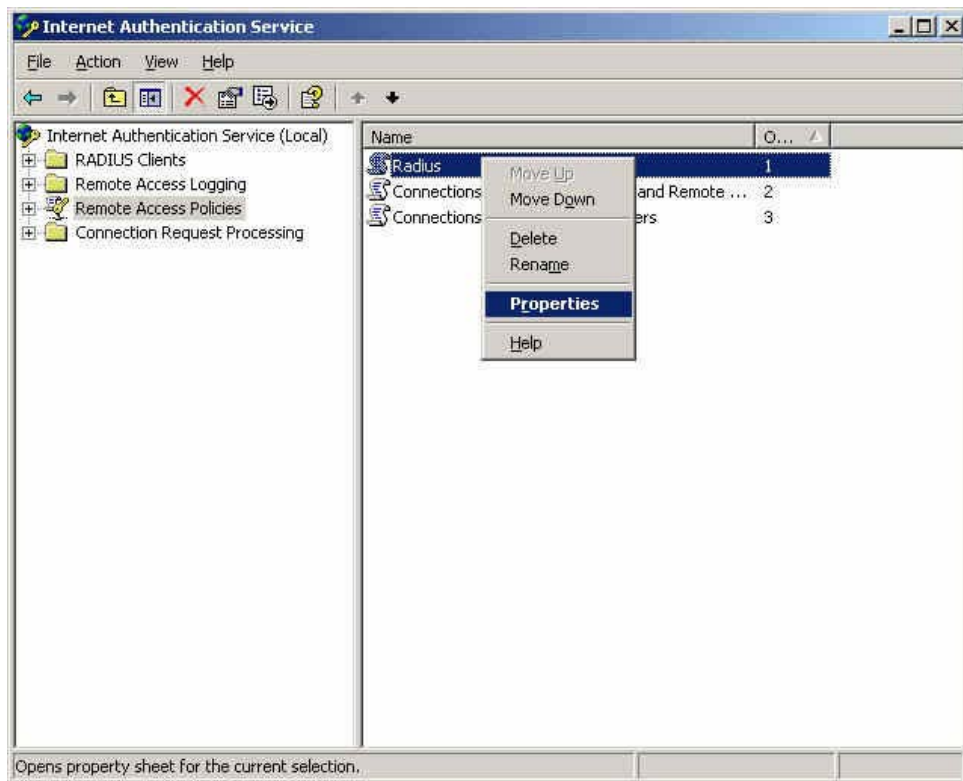
The image shows a Windows-style dialog box titled "New Remote Access Policy Wizard". The main heading is "User or Group Access", followed by the instruction: "You can grant access to individual users, or you can grant access to selected groups." There are two radio button options: "User" (selected) with the description "User access permissions are specified in the user account.", and "Group" with the description "Individual user permissions override group permissions:". Below the "Group" option is a text field labeled "Group name:" and two buttons, "Add..." and "Remove". At the bottom of the dialog are three buttons: "< Back", "Next >" (which is highlighted with a dashed border), and "Cancel".

**Add new remote access policy user and group**

**STEP 12 . Select MD5-Challenge.**

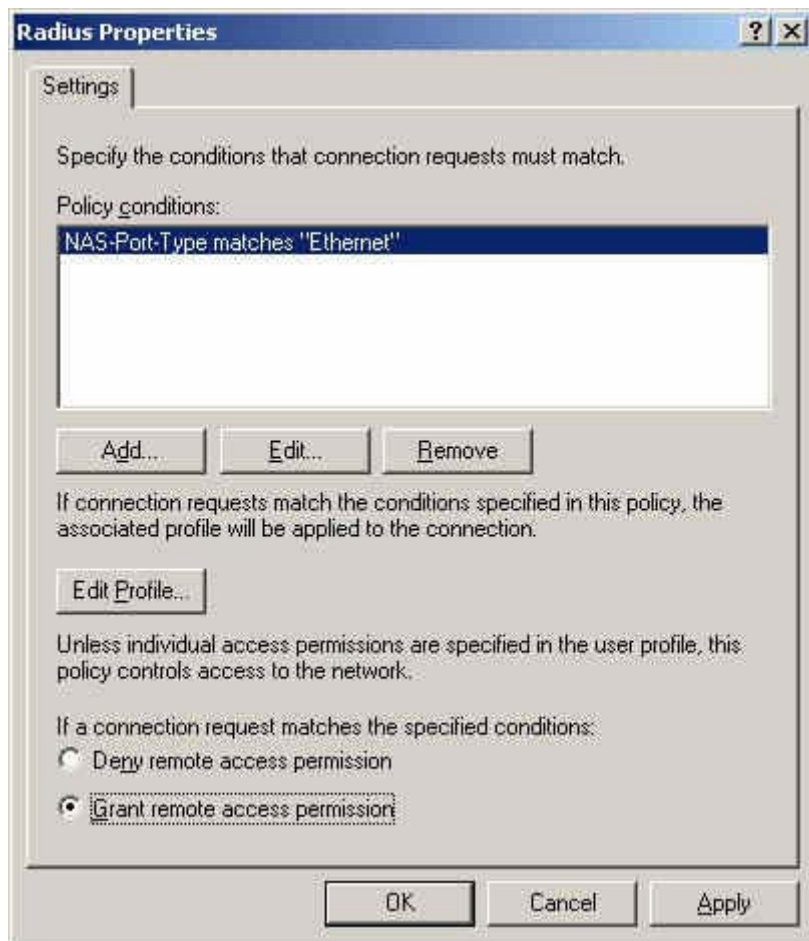
The authentication of add new remote access policy

**STEP 13 .** Right click on the **Radius** → **Properties**.

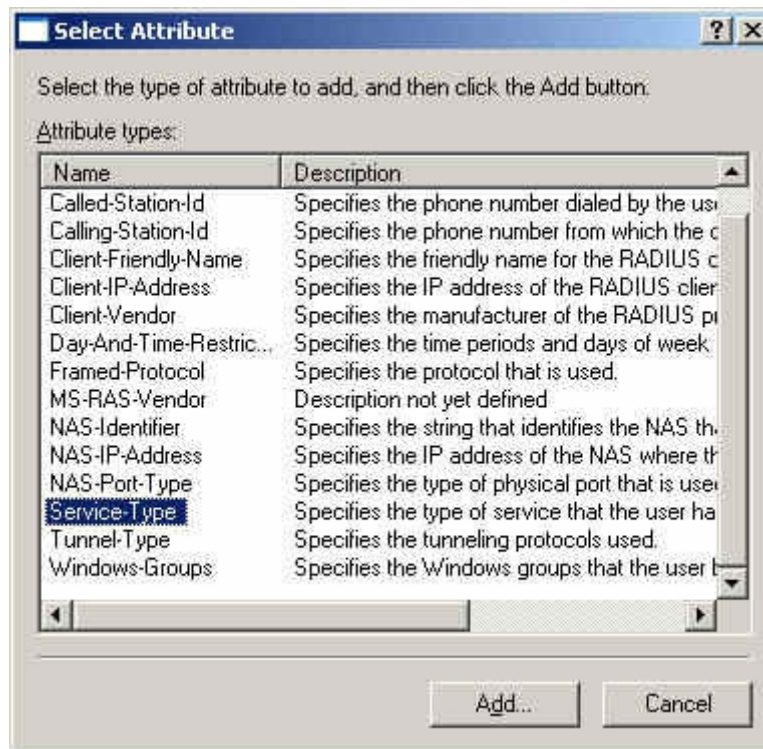


**The network authentication service setting**

**STEP 14 .** Select **Grant remote access permission**, and **Remove** the original setting, then click **Add**.

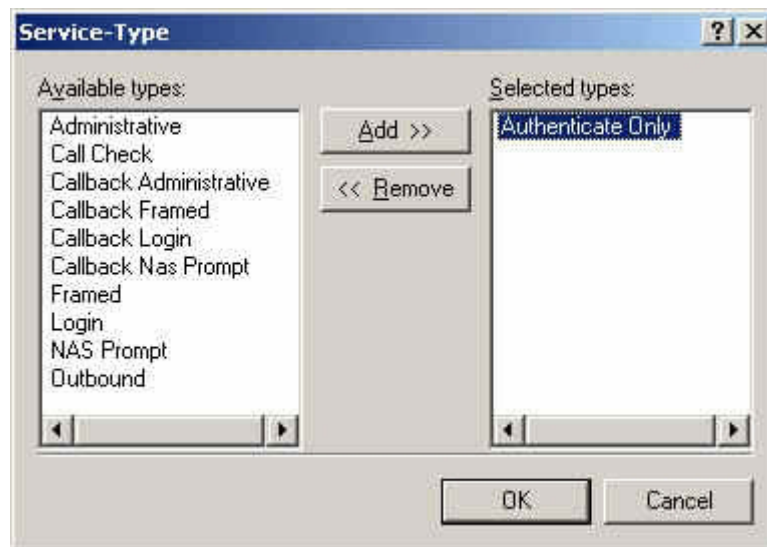


**The RADIUS properties settings**

**STEP 15 . Add Service-Type.**

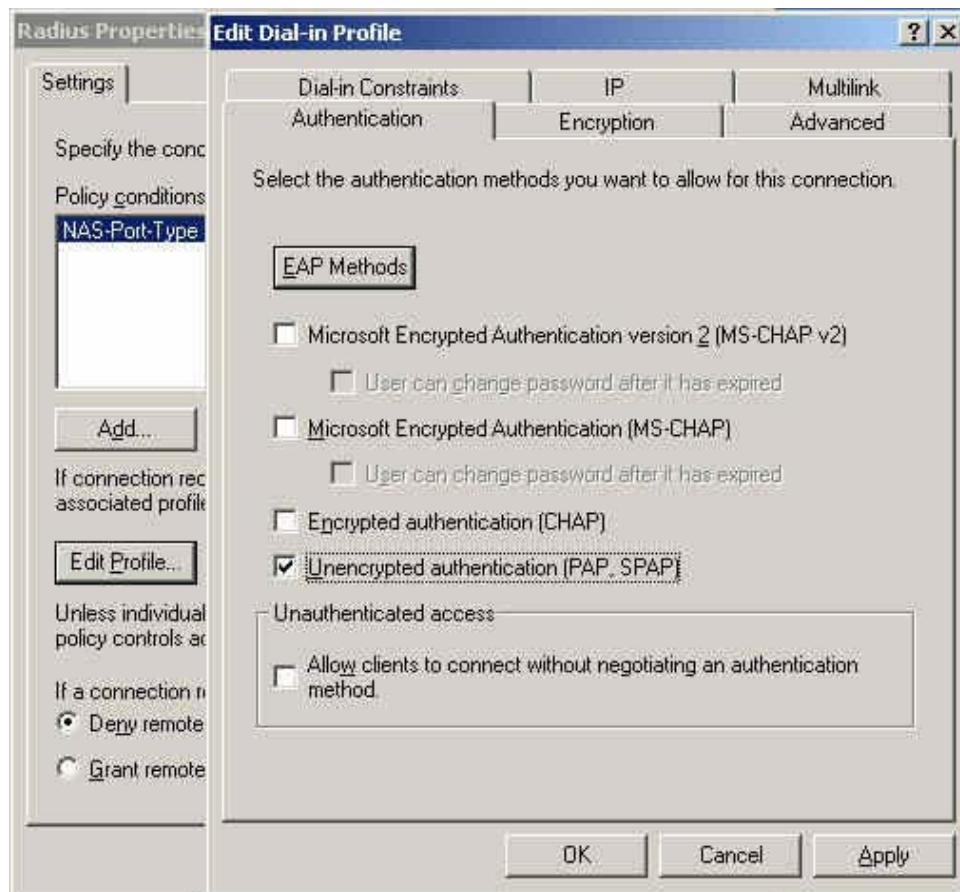
**Add new RADIUS properties attribute**

**STEP 16 . Add Authenticate Only** from the left side.



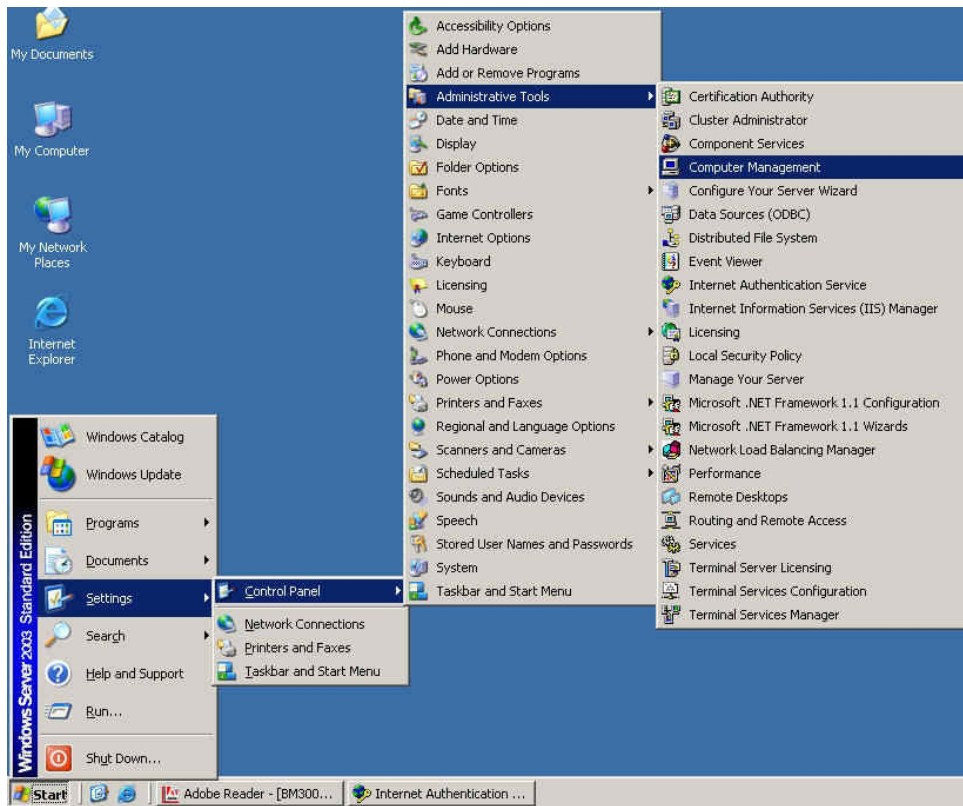
**Add RADIUS properties service-type**

**STEP 17** . Click **Edit Profile**, select **Authentication**, and check **Unencrypted authentication (PAP, SPAP)**.



**Edit RADIUS service-type dial-in property**

**STEP 18 . Add Auth User, click **Start** → **Setting** → **Control Panel**→**Administrative Tools**, select **Computer Management**.**



**Enter computer management**



**STEP 19 .** Right click on **Users**, select **New User**.



**Add new user**

**STEP 20 .** Complete the Windows 2003 RADIUS Server Settings.

**STEP 21 .** In **Authentication** → **RADIUS** function, enter **IP**, **Port** and **Shared Secret**. (The setting must be the same as RADIUS server).

**RADIUS Server**

☒ Enable RADIUS Server Authentication

RADIUS Server IP:  (Max. 60 characters)

RADIUS Server Port:  ( Range: 1025 - 65535 )

Shared Secret:  (Max. 80 characters)

☐ Enable 802.1x RADIUS Server Authentication

**OK** **Cancel**

### The RADIUS server setting

**STEP 22 .** In **Authentication** → **User Group**, add new **Radius User**.

**New Authentication Group**

Name:  (Max. 16 characters)

< ---Available Authentication User --->

alex  
joe  
eva  
(Radius User)  
(POP3 User)

**Remove** **Add**

<--- Selected Authentication User --->

(Radius User)

**OK** **Cancel**

### Add new RADIUS user

Name	Member	Radius	POP3	Configure
planet	alex, joe, eva			<b>In Use</b>
Radius	---	✓		<b>Modify</b> <b>Remove</b> <b>Pause</b>

**New Entry**

### Complete adding a RADIUS Authentication

**STEP 23 .** In **Policy → Outgoing**, apply the **Authentication Group** (RADIUS included) in **STEP22**. To add the new policy.

Comment :  (Max. 32 characters)

Modify Policy	
Source Address	Inside_Any ▾
Destination Address	Outside_Any ▾
Service	ANY ▾
Schedule	None ▾
Authentication User	Radius ▾
Tunnel	None ▾
Action, WAN Port	PERMIT ALL ▾
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> Enable
IM / P2P Blocking	None ▾
QoS	None ▾
MAX. Bandwidth Per Source IP	Downstream <input type="text"/> 0 Kbps Upstream <input type="text"/> 0 Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	<input type="text"/> 0 ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	<input type="text"/> 0 ( Range: 1 - 99999, 0: means unlimited )

To add the RADIUS authentication policy

Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY	✓		<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To 1 ▾

Authentication User : Radius	
Authentication User	
RADIUS_USER	

Complete the RADIUS authentication policy setting

**STEP 24 .** When the users connect to the network via the browser, it will show the authentication window.  
Enter the user name and password, click **OK**, and then link to the network through the MH-2001.

User Login

User Authentication	
User Name	<input type="text" value="alex"/>
Password	<input type="password" value="...."/>

Welcome to Planet MH-2001 Authentication Page!!!

Link to the network through the authentication window

### 6.5.5 POP3

To plan the users connect to the WAN through the authentication by policy. (To use the WAN POP3 server authentication)

**STEP 1 . In Authentication → POP3, add the new setting as following.**

**POP3 Server**

☒ Enable POP3 Server Authentication

POP3 Server ( IP or Domain Name )  (Max. 80 characters)

POP3 Server Port  ( Range: 110 or 1025 - 65535 )

#### The POP3 server setting

**STEP 2 . In Authentication → User Group, add new POP3 User.**

**New Authentication Group**

Name:  (Max. 16 characters)

< ---Available Authentication User --->

alex  
joe  
eva  
(Radius User)  
(POP3 User)

<--- Selected Authentication User --->

(POP3 User)

#### Add new POP3 user

Name	Member	Radius	POP3	Configure
planet	alex, joe, eva			<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>
Radius	---	✓		<input type="button" value="In Use"/>
POP3	---		✓	<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>

#### Complete adding a new POP3 Authentication

**STEP 3 . In Policy → Outgoing, apply the Step2 (The authentication group) in to the policy.**

Comment :  (Max. 32 characters)

Modify Policy	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	POP3
Tunnel	None
Action, WAN Port	PERMIT ALL
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> Enable
IM / P2P Blocking	None
QoS	None
MAX. Bandwidth Per Source IP	Downstream 0 Kbps Upstream 0 Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	0 ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )

### The POP3 server authentication in policy setting

Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Outside_Any	ANY			<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To 1

**Authentication User : POP3**  
 Authentication User  
 POP3\_USER

### Complete the POP3 server authentication in policy setting

**STEP 4 .** When the users want to connect to the network via browser, it will show the authentication window.

Enter the user name and password, click **OK** then link to the network through the MH-2001 appliance.

### User Login

User Authentication	
User Name	<input type="text" value="alex"/>
Password	<input type="password" value="...."/>

Welcome to Planet MH-2001 Authentication Page!!!

**Link to the network through the authentication window**

## 6.6 Content Blocking

Content Filtering includes “**URL Blocking**”, “**Script Blocking**”, “**Download Blocking**” and “**Upload Blocking**”.

**URL Blocking:** The administrator can use a complete domain name or key word to make rules for specific websites.

**Script Blocking:** To let Popup 、ActiveX 、Java 、Cookie in or keep them out.

**Download Blocking:** Block download connection, audio and video transferring from web page. You can select to block which type of extension name or all type of the file.

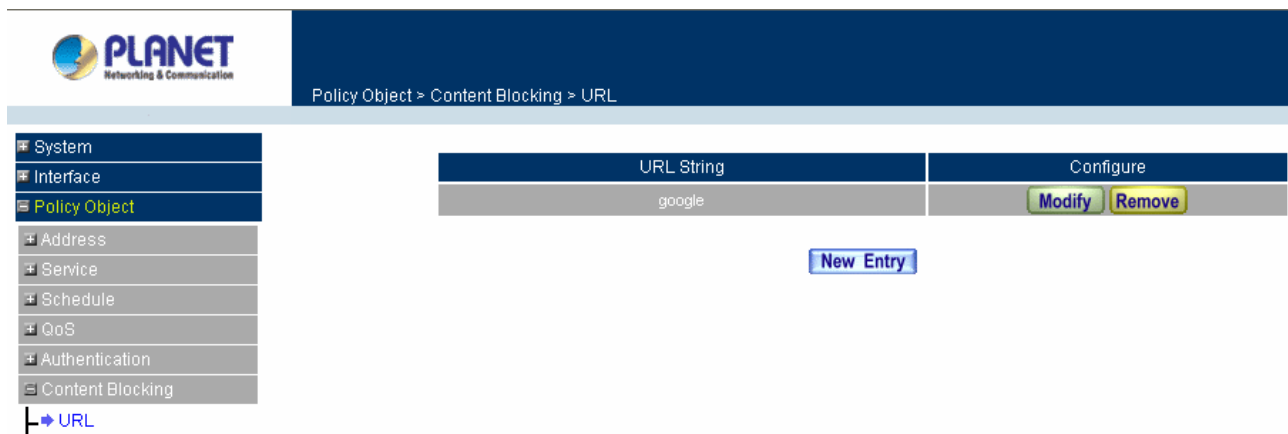
**Upload Blocking:** Block upload connection, audio and video transferring to Internet. You can select to block which type of extension name or all type of the file.

### 6.6.1 URL Blocking

The Administrator may setup URL Blocking to prevent LAN network users from accessing a specific website on the Internet. Any web request coming from an LAN network computer to a blocked website will receive a blocked message instead of the website.

#### Entering the URL blocking window

Step 1. Click on **URL** under the **Content Blocking** menu bar and the screen will display as below..



#### Definition:

**URL String:** The domain name that is blocked to enter by MH-2001.

**Configure:** To change the settings of URL Blocking, click **Modify** to change the parameters; click **Remove** to delete the settings.

#### Adding a URL Blocking policy

Step 1. After clicking **New Entry**, the **Add New Block String** window will appear.

Step 2. Enter the URL String of the website to be blocked.

Step 3. Click **OK** to add the policy. Click **Cancel** to discard changes.

Step 4. After finishing Content Filtering setting, you must enable it at Outgoing Policy, or Content Filtering will not be workable.



You can use the symbol to help you configure the URL Blocking.

**Symbol:** ~ means **open up**; \* means **metacharacter**

**Restrict not to enter specific website:** Enter the 「complete domain name」 or 「key word」 of the website you want to restrict in **URL String**. For example: www.kcg.gov.tw or gov.

**Only open specific website to enter:**

1. Add the website you want to **open up** in URL String. While adding, you must enter the symbol “~” in front of the 「complete domain name」 or 「key word」 that represents to open these website to enter. For Example: ~www.kcg.gov.tw or ~gov.
2. After setting up the website you want to open up, enter an order to “forbid all” in the last URL String; means only enter \* in URL String.



**Warning!** The order to forbid all must be placed at last forever. If you want to open a new website, you must delete the order of forbidding all and then enter the new domain name. At last, re-enter the “forbid all” order again.

## 6.6.2 Script Blocking

To let Popup, ActiveX, Java, or Cookies in or keep them out.

Step 1. Click **Content Blocking** in the menu.

Step 2. **Script Blocking** detective functions.

- **Popup:** Prevent pop-up boxes from appearing.
- **ActiveX:** Prevent ActiveX packets.
- **Java:** Prevent Java packets.
- **Cookie:** Prevent Cookie packets.

Step 3. After selecting each function, click the **OK** button below.

Step 4. After finishing Script Blocking setting, you must enable it at Outgoing Policy, or Content Filtering will not be workable.

Modify Policy	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
Tunnel	None
Action, WAN Port	PERMIT ALL
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input checked="" type="checkbox"/> Enable
IM / P2P Blocking	None
QoS	None
MAX. Bandwidth Per Source IP	Downstream 0 Kbps Upstream 0 Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	0 ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )



The users may not use the specific function (like JAVA, cookie...etc.) to browse the website through this policy. It can forbid the user browsing stock exchange website...etc.



### 6.6.3 Download Blocking

Step 1. Click **Content Blocking** in the menu.

Step 2. Select **Download Blocking** and configure the setting.

- **All Types Blocking:** To block all types of the files downloading from web page.
- **Audio and Video Types blocking:** To block audio and video downloading from web page..
- **Extensions Blocking:** To block specific extensions name of the files from web page.

Step 3. After selecting each function, click the **OK** button below.

Step 4. After finishing Content Filtering setting, you must enable it at Outgoing Policy, or Content Filtering will not be workable.

## 6.6.4 Upload Blocking

Step 1. Click **Content Blocking** in the menu.

Step 2. Select **Upload Blocking** and configure the setting.

- **All Types Blocking:** To block all types of the files uploading to Internet.
- **Extensions Blocking:** To block specific extensions name of the files to Internet.

Step 3. After selecting each function, click the **OK** button below.

The screenshot shows the PLANET Security Gateway configuration interface. The left sidebar contains a tree view with the following items: System, Interface, Policy Object, Address, Service, Schedule, QoS, Authentication, Content Blocking, URL, Script, Download, Upload, IM / P2P Blocking, and Virtual Server. The 'Content Blocking' item is expanded, and 'Upload' is selected. The main panel displays the 'Upload Blocking' configuration. At the top, there is a checkbox for 'All Types Blocking'. Below it, there is a section for 'Extension Blocking' with a grid of checkboxes for various file extensions. The extensions and their status are as follows:

Extension	Status
.exe	<input type="checkbox"/>
.iso	<input checked="" type="checkbox"/>
.doc	<input checked="" type="checkbox"/>
.pdf	<input type="checkbox"/>
.bat	<input type="checkbox"/>
.scr	<input type="checkbox"/>
.pif	<input type="checkbox"/>
.reg	<input type="checkbox"/>
.mpg	<input type="checkbox"/>
.zip	<input type="checkbox"/>
.bin	<input checked="" type="checkbox"/>
.xl?	<input checked="" type="checkbox"/>
.tgz	<input type="checkbox"/>
.dll	<input type="checkbox"/>
.vb?	<input type="checkbox"/>
.msi	<input type="checkbox"/>
.mp3	<input type="checkbox"/>
.rar	<input type="checkbox"/>
.rpm	<input type="checkbox"/>
.ppt	<input type="checkbox"/>
.gz	<input checked="" type="checkbox"/>
.hta	<input checked="" type="checkbox"/>
.wps	<input checked="" type="checkbox"/>
.com	<input checked="" type="checkbox"/>
.mpeg	<input checked="" type="checkbox"/>

At the bottom right of the main panel, there are 'OK' and 'Cancel' buttons.

Step 4. After finishing Content Filtering setting, you must enable it at Outgoing Policy, or Content Filtering will not be workable.

The screenshot shows the PLANET Security Gateway configuration interface. The left sidebar contains a tree view with the following items: System, Interface, Policy Object, Policy, Outgoing, Incoming, WAN To DMZ, LAN To DMZ, DMZ To WAN, DMZ To LAN, Anomaly Flow IP, and Monitor. The 'Policy' item is expanded, and 'Outgoing' is selected. The main panel displays the 'Modify Policy' configuration for the 'Outgoing' policy. At the top, there is a 'Comment' field. Below it, there is a table with various policy settings. The 'Content Blocking' setting is highlighted with a red box and is set to 'Enable'.

Setting	Value
Source Address	Inside_Any
Destination Address	Outside_Any
Service	ANY
Schedule	None
Authentication User	None
Tunnel	None
Action, WAN Port	PERMIT ALL
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input checked="" type="checkbox"/> Enable
IM / P2P Blocking	None
QoS	None
MAX. Bandwidth Per Source IP	Downstream: 0 Kbps Upstream: 0 Kbps (0: means unlimited)
MAX. Concurrent Sessions Per IP	0 (Range: 1 - 99999, 0: means unlimited)
MAX. Concurrent Sessions	0 (Range: 1 - 99999, 0: means unlimited)

At the bottom right of the main panel, there are 'OK' and 'Cancel' buttons.

## 6.7 IM/P2P Blocking

Restrict the Internal Users to access to the file on Internet by IM and P2P software.

Step 1. Click **IM/P2P Blocking** in the menu.

Step 2. Select **Setting** and configure the setting.

Step 3. Click **New Entry** Button and the **IM/P2P Blocking Configure** screen will appear.

- **Name:** Enter the name of the IM/P2P Blocking.
- **Instant Messaging:** Select the IM software which you want to block.
- **Peer-to-Peer Application:** Select the P2P software which you want to block.

Step 4. After selecting each function, click the **OK** button below.

Step 5. After finishing IM/P2P Blocking setting, you must enable it at Outgoing Policy, or IM/P2PBlocking will not be workable

## 6.8 Virtual Server

MH-2001 separates an enterprise's Intranet and Internet into LAN networks and WAN networks respectively. Generally speaking, in order to allocate enough IP addresses for all computers, an enterprise assigns each computer a private IP address, and converts it into a real IP address through MH-2001's NAT (Network Address Translation) function. If a server providing service to the WAN networks is located in the LAN networks, outside users can't directly connect to the server by using the server's private IP address.

MH-2001's Virtual Server can solve this problem. A virtual server has set the real IP address of MH-2001's WAN network interface to be the Virtual Server IP. Through the virtual server feature, MH-2001 translates the virtual server's IP address into the private IP address of physical server in the LAN network. When outside users on the Internet request connections to the virtual server, the request will be forwarded to the private LAN server.

Virtual Server owns another feature known as one-to-many mapping. This is when one virtual server IP address on the WAN interface can be mapped into 4 LAN network server private IP addresses. This option is useful for Load Balancing, which causes the virtual server to distribute data packets to each private IP addresses (which are the real servers). By sending all data packets to all similar servers, this increases the server's efficiency, reduces risks of server crashes, and enhances servers' stability.

### How to use Virtual Server and mapped IP

Virtual Server and Mapped IP are part of the IP mapping (also called DMZ, De-Militarization Zone) scheme. By applying the incoming policies, Virtual Server and IP mapping work similarly. They map real IP addresses to the physical servers' private IP addresses (which is opposite to NAT), but there are still some differences:

- Virtual Server can map one real IP to several LAN physical servers while Mapped IP can only map one real IP to one LAN physical server (1-to-1 Mapping). The Virtual Servers' load balance feature can map a specific service request to different physical servers running the same services.
- Virtual Server can only map one real IP to one service/port of the LAN physical servers while Mapped IP maps one real IP to all the services offered by the physical server.
- IP mapping and Virtual Server work by binding the IP address of the WAN virtual server to the private LAN IP address of the physical server that supports the services. Therefore users from the WAN network can access servers of the LAN network by requesting the service from the IP address provided by Virtual Server.

In this chapter, we will have detailed introduction and instruction of **Mapped IP** and **Server 1/2/3/4**:

## 6.8.1 Mapped IP

Internal private IP addresses are translated through NAT (Network Address Translation). If a server is located in the LAN network, it has a private IP address, and outside users cannot connect directly to LAN servers' private IP address. To connect to a LAN network server, outside users have to first connect to a real IP address of the WAN network, and the real IP is translated to a private IP of the LAN network. Mapped IP and Virtual Server are the two methods to translate the real IP into private IP. **Mapped IP** maps IP in one-to-one way; that means all services of one real WAN IP address is mapped to one private LAN IP address.

### Make a single server that provides several services such as FTP, Web, and Mail, to provide service by policy

Step 1. Setting a server that provide several services in LAN, and set up the network card's IP as 192.168.1.100. DNS is External DNS Server.

Step 2. Enter the following setting in **LAN** of **Address** function.

Add New Address	
Name	Main_server (Max. 16 characters)
IP Address	192.168.1.100
Netmask	255.255.255.255 ( 255.255.255.255 means the specified PC )
	( 255.255.255.0 means class C subnet )
MAC Address	<input type="text"/> <a href="#">Clone MAC Address</a>
<input type="checkbox"/> Get static IP address from DHCP Server.	

[OK](#)
[Cancel](#)

### Mapped IP Settings of Server in Address

Step 3. Enter the following data in **Mapped IP** of **Virtual Server** function:

- Click **New Entry**
- **WAN IP:** Enter 210.66.155.78 (click **Assist** for assistance)
- **Map to Virtual IP:** Enter 192.168.1.100
- Click **OK**
- Complete the setting of adding new mapped IP

Add New Mapped IP	
WAN IP	210.66.155.78 WAN1 <a href="#">Assist</a>
Map To Virtual IP	192.168.1.100

[OK](#)
[Cancel](#)

### Mapped IP Setting WebUI

Step 4. Group the services (DNS, FTP, HTTP, POP3, SMTP...) that provided and used by server in **Service** function. And add a new service group for server to send mails at the same time.

Group name	Service	Configure
Main_service	DNS,FTP,HTTP...	<a href="#">Modify</a> <a href="#">Remove</a>
Mail_service	DNS,POP3,SMTP	<a href="#">Modify</a> <a href="#">Remove</a>

[New Entry](#)

### Service Setting

Step 5. Add a policy that includes settings of STEP3, 4 in **Incoming Policy**.

Comment :  (Max. 32 characters)

**Add New Policy**

Source Address	Outside_Any
Destination Address	Mapped IP(210.66.155.78)
Service	Main_service
Schedule	None
Tunnel	None
Action	PERMIT
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
QoS	None
MAX. Bandwidth Per Source IP	Downstream <input type="text"/> Kbps Upstream <input type="text"/> Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	<input type="text"/> ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	<input type="text"/> ( Range: 1 - 99999, 0: means unlimited )
NAT	<input type="checkbox"/> Enable

[OK](#) [Cancel](#)

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Mapped IP(210.66.155.78)	Main_service	✓		<a href="#">Modify</a> <a href="#">Remove</a> <a href="#">Pause</a>	To 1

[New Entry](#)

### Complete the Incoming Policy

Step 6. Add a policy that includes STEP2 and 4 in **Outgoing Policy**. It makes the server to send e-mail to external mail server by mail service.

Comment :  (Max. 32 characters)

Modify Policy	
Source Address	Main_server
Destination Address	Outside_Any
Service	Mail_service
Schedule	None
Authentication User	None
Tunnel	None
Action, WAN Port	PERMIT ALL
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> Enable
IM / P2P Blocking	None
QoS	None
MAX. Bandwidth Per Source IP	Downstream <input type="text" value="0"/> Kbps Upstream <input type="text" value="0"/> Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )

Source	Destination	Service	Action	Option					Configure			Move
Main_server	Outside_Any	Mail_service	✓						Modify	Remove	Pause	To 1

### Complete the Outgoing Policy

Step 7. Complete the setting of providing several services by mapped IP.



Strong suggests **not** to choose **ANY** when setting Mapped IP and choosing service. Otherwise the Mapped IP will be exposed to Internet easily and may be attacked by Hacker.

## 6.8.2 Virtual Server 1- 4

Virtual server is a one-to-many mapping technique, which maps a real IP address from the WAN interface to private IP addresses of the LAN network. This function provides services or applications defined in the Service menu to enter into the LAN network. Unlike a mapped IP which binds a WAN IP to a LAN IP, virtual server binds WAN IP ports to LAN IP ports.

### Make several servers that provide a single service, to provide service through policy by Virtual Server (Take Web service for example)

Step 1. Setting several servers that provide Web service in LAN network, which IP Address is 192.168.1.101, 192.168.1.102, 192.168.1.103, and 192.168.1.104

Step 2. Enter the following data in **Server 1** of **Virtual Server** function:

- Click the “**click here to configure**” button to configure **Virtual Server Real IP** in **Server 1**
- **Virtual Server Real IP:** Enter 210.66.155.79 (click **Assist** for assistance)
- Click **OK**

OK Cancel

#### Virtual Server Real IP Setting

Virtual Server Real IP 210.66.155.79

Service	WAN Port	Server Virtual IP	Configure
---------	----------	-------------------	-----------

New Entry

#### Complete Virtual Server Real IP Setting

Step 3. Click the **New Entry** to set Virtual Server Configuration.

- **Service:** Select HTTP (80)
- **External Service Port:** Change to 8080
- **Load Balance Server1:** Enter 192.168.1.101
- **Load Balance Server2:** Enter 192.168.1.102
- **Load Balance Server3:** Enter 192.168.1.103
- **Load Balance Server4:** Enter 192.168.1.104
- Click **OK**
- Complete the setting of Virtual Server



Virtual Server Configuration	
Virtual Server Real IP	210.66.155.79
Service	HTTP (80) ▼
External Service Port	8080 ( Range: 0 - 65535 )
Load Balance Server	Server Virtual IP
1	192.168.1.101
2	192.168.1.102
3	192.168.1.103
4	192.168.1.104

OK Cancel

### Virtual Server Configuration WebUI

Step 4. Add a new policy in **Incoming Policy**, which includes the virtual server, set by STEP2 and 3.

Comment :  (Max. 32 characters)

Modify Policy	
Source Address	Outside_Any ▼
Destination Address	Virtual Server 1(210.66.155.79) ▼
Service	HTTP(8080) ▼
Schedule	None ▼
Tunnel	None ▼
Action	PERMIT ▼
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
QoS	None ▼
MAX. Bandwidth Per Source IP	Downstream <input type="text"/> Kbps Upstream <input type="text"/> Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	<input type="text"/> ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	<input type="text"/> ( Range: 1 - 99999, 0: means unlimited )
NAT	<input type="checkbox"/> Enable

OK Cancel

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Virtual Server 1(210.66.155.79)	HTTP(8080)	✓		<a href="#">Modify</a> <a href="#">Remove</a> <a href="#">Pause</a>	To 1 ▼

New Entry

### Virtual Server Configuration WebUI



In this example, the external users must change its port number to 8080 before entering the Website that set by the Web server.

Step 5. Complete the setting of providing a single service by virtual server.

## 6.9 VPN

The MH-2001 adopts VPN to set up safe and private network service. And combine the remote Authentication system in order to integrate the remote network and PC of the enterprise. Also provide the enterprise and remote users a safe encryption way to have best efficiency and encryption when delivering data. Therefore, it can save lots of problem for manager.

**【IPSec Autokey】**: The system manager can create a VPN connection using Autokey IKE. Autokey IKE (Internet Key Exchange) provides a standard method to negotiate keys between two security gateways. Also set up IPSec Lifetime and Preshared Key of the MH-2001.

**【PPTP Server】**: The System Manager can set up VPN-PPTP Server functions in this chapter.

**【PPTP Client】**: The System Manager can set up VPN-PPTP Client functions in this chapter.

### How to use the VPN?

To set up a Virtual Private Network (VPN), you need to configure an Access Policy include IPSec Autokey, PPTP Server, or PPTP Client settings of Tunnel to make a VPN connection.

### Define the required fields of VPN:

#### RSA:

- A public-key cryptosystem for encryption and authentication.

#### Preshared Key:

- The IKE VPN must be defined with a Preshared Key. The Key may be up to 128 bytes long.

#### ISAKMP (Internet Security Association Key Management Protocol):

- An extensible protocol-encoding scheme that complies to the Internet Key Exchange (IKE) framework for establishment of Security Associations (SAs).

#### Main Mode:

- This is another first phase of the Oakley protocol in establishing a security association, but instead of using three packets like in aggressive mode, it uses six packets.

#### Aggressive mode:

- This is the first phase of the Oakley protocol in establishing a security association using three data packets.

#### AH (Authentication Header):

- One of the IPSec standards that allows for data integrity of data packets.

**ESP (Encapsulating Security Payload):**

- One of the IPSec standards that provides for the confidentiality of data packets.

**DES (Data Encryption Standard):**

- The Data Encryption Standard developed by IBM in 1977 is a 64-bit block encryption block cipher using a 56-bit key.

**Triple-DES (3DES):**

- The DES function performed three times with either two or three cryptographic keys.

**AES (Advanced Encryption Standard):**

- An encryption algorithm yet to be decided that will be used to replace the aging DES encryption algorithm and that the NIST hopes will last for the next 20 to 30 years.

**NULL Algorithm:**

- It is a fast and convenient connecting mode to make sure its privacy and authentication without encryption. NULL Algorithm doesn't provide any other safety services but a way to substitute ESP Encryption

**SHA-1 (Secure Hash Algorithm-1):**

- A message-digest hash algorithm that takes a message less than 264 bits and produces a 160-bit digest.

**MD5:**

- MD5 is a common message digests algorithm that produces a 128-bit message digest from an arbitrary length input, developed by Ron Rivest.



**GRE/IPSec:**

- The device Select GRE/IPSec (Generic Routing Encapsulation) packet seal technology.

**Define the required fields of IPSec Function**

i:

- To display the VPN connection status via icon ◦

Chart	--		
Meaning	Not be applied	Disconnect	Connecting

**Name:**

- The VPN name to identify the IPSec Autokey definition. The name must be the only one and cannot be repeated.

**Gateway IP:**

- The WAN interface IP address of the remote Gateway.

**IPSec Algorithm:**

- To display the Algorithm way.

**Configure:**

- Click **Modify** to change the argument of IPSec; click **Remove** to remote the setting.

i	Name	WAN	Gateway IP	IPSec Algorithm	Configure
---	------	-----	------------	-----------------	-----------

New Entry

IPSec Autokey WebUI

**Define the required fields of PPTP Server Function****PPTP Server:**



- To select Enable or Disable

**Client IP Range:**

- Setting the IP addresses range for PPTP Client connection

i:

- To display the VPN connection status via icon ◦

Chart	--		
Meaning	Not be applied	Disconnect	Connecting

**User Name:**

- Display the PPTP Client user's name when connecting to PPTP Server.

**Client IP:**

- Display the PPTP Client's IP address when connecting to PPTP Server.

**Uptime:**

- Display the connection time between PPTP Server and Client.

**Configure:**

- Click **Modify** to modify the PPTP Server Settings or click **Remove** to remove the setting

PPTP Server ( Disable ) :

Client IP Range : 192.144.209.1-254

**Modify**



i	User Name	Client IP	Uptime	Configure
---	-----------	-----------	--------	-----------

**New Entry****PPTP Server WebUI**

**Define the required fields of PPTP Client Function**

i:

- To display the VPN connection status via icon ◦

Chart	--		
Meaning	Not be applied	Disconnect	Connecting

**User Name:**

- Displays the PPTP Client user's name when connecting to PPTP Server.

**Server IP or Domain Name:**

- Display the PPTP Server IP addresses or Domain Name when connecting to PPTP Server.

**Encryption:**

- Display PPTP Client and PPTP Server transmission, whether opens the encryption authentication mechanism.

**Uptime:**

- Displays the connection time between PPTP Server and Client.

**Configure:**

- Click **Modify** to change the argument of PPTP Client; click **Remove** to remote the setting.

PPTP Client :

i	User Name	Server IP or Domain Name	Encryption	Uptime	Configure
---	-----------	--------------------------	------------	--------	-----------



[New Entry](#)

PPTP Client WebUI

**Define the required fields of Tunnel Function**

i:

- To display the VPN connection status via icon ◦

Chart	--		
Meaning	Not be applied	Disconnect	Connecting

**Name:**

- The VPN name to identify the VPN tunnel definition. The name must be the only one and cannot be repeated.

**Source Subnet:**

- Displays the Source Subnet.

**Destination Subnet:**

- Displays the Destination Subnet.

**IPSec / PPTP:**

- Displays the Virtual Private Network's (IPSec Autokey, PPTP Server and PPTP Client) settings of Tunnel function.

**Configure:**

- Click **Modify** to change the argument of VPN Tunnel; click **Remove** to remote the setting.

i	Name	Source Subnet	Destination Subnet	IPSec / PPTP	Configure
---	------	---------------	--------------------	--------------	-----------

[New Entry](#)

VPN Tunnel Web UI

We set up two VPN examples in this chapter:

No.	Range	The Application Environments	Pages
Example.1	<b>IPSec Autokey</b>	To access the static subnet resources via the IPSec VPN connection between two MH-2001 appliances.	<b>112</b>
Example.2	<b>IPSec Autokey</b>	The way to set the MH-2001 appliance IPSec VPN connection in Windows 2000.	<b>125</b>
Example.3	<b>IPSec Autokey</b>	The way to set the IPSec VPN connection between two MH-2001 appliances. ( aggressive mode) (The IPSec algorithm, 3DES encryption.MD5 authentication.)	<b>183</b>
Example.4	<b>IPSec Autokey</b>	The way to set the IPSec VPN connection between two MH-2001 appliances. (The GRE packets.) (The IPSec algorithm, 3DES encryption, MD5 authentication).	<b>196</b>
Example.5	<b>PPTP</b>	The way to set the PPTP outbound load balance via VPN between two MH-2001 appliance.	<b>209</b>
Example.6	<b>PPTP</b>	The way to set the MH-2001 appliance PPTP VPN connection in Windows 2000.	<b>219</b>



### 6.9.1 Example.1

To access the static subnet resources via the IPSec VPN connection between two MH-2001 appliances.

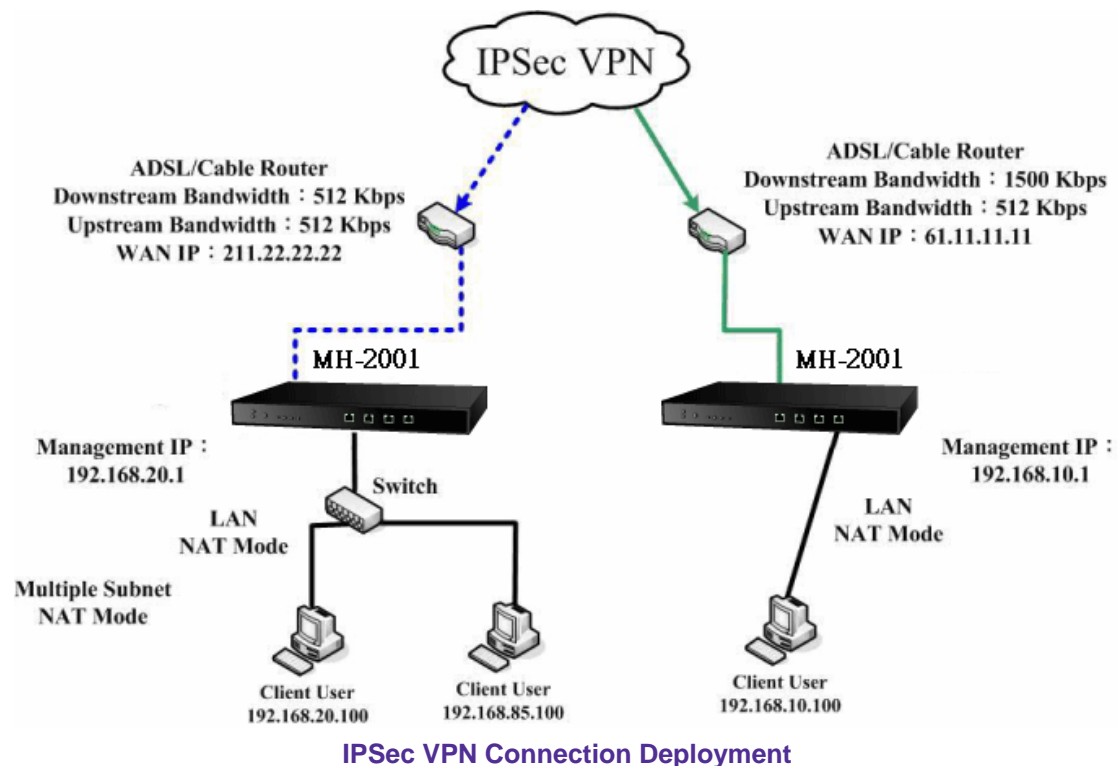
#### Preparation

Company A    **WAN IP: 61.11.11.11**  
                   **LAN IP: 192.168.10.X**

Company B    **WAN IP: 211.22.22.22**  
                   **LAN IP: 192.168.20.X**  
                   **Multiple Subnet: 192.168.85.X**

This example takes two MH-2001 as work platform. Suppose Company A 192.168.10.100 create a VPN connection with Company B 192.168.85.100 for downloading the sharing file.

#### VPN TEST Environment



**The Default Gateway of Company A is the MH-2001 LAN IP 192.168.10.1. Follow the steps below:**

**STEP 1 .** Enter the default IP of Gateway of Company A's MH-2001, 192.168.10.1 and select **IPSec Autokey** in **VPN**. Click **New Entry**.

i	Name	WAN	Gateway IP	IPSec Algorithm	Configure
<div>New Entry</div>					

### IPSec Autokey WebUI

**STEP 2 .** In the list of **IPSec Autokey**, fill in Name with **VPN\_A**.

Necessary Item	
Name	<input type="text" value="VPN_A"/> (Max. 12 characters)
WAN interface	<input checked="" type="radio"/> WAN 1 <input type="radio"/> WAN 2

### IPSec Autokey Name Setting

**STEP 3 .** Select **Remote Gateway-Fixed IP or Domain Name** In **To Destination** list and enter the IP Address.

To Destination	
<input checked="" type="radio"/> Remote Gateway -- Fixed IP or Domain Name	<input type="text" value="211.22.22.22"/> (Max. 99 characters)
<input type="radio"/> Remote Gateway or Client -- Dynamic IP	

#### IPSec To Destination Setting

**STEP 4 .** Select Preshare in **Authentication Method** and enter the **Preshared Key** (max: 100 bits)

Authentication Method	<input type="text" value="Preshare"/>
Preshared Key	<input type="text" value="123456789"/> (Max. 103 characters)

#### IPSec Authentication Method Setting

**STEP 5 .** Select **ISAKMP Algorithm** in **Encapsulation** list. Choose the Algorithm when setup connection. Please select ENC Algorithm (**3DES/DES/AES**), AUTH Algorithm (**MD5/SHA1**), and Group (**GROUP1, 2,5**). Both sides have to choose the same group. Here we select 3DES for ENC Algorithm, MD5 for AUTH Algorithm, and GROUP1 for group.

Encapsulation	
ISAKMP Algorithm	
ENC Algorithm	<input type="text" value="3DES"/>
AUTH Algorithm	<input type="text" value="MD5"/>
Group	<input type="text" value="GROUP 1"/>

#### IPSec Encapsulation Setting

**STEP 6 .** You can choose Data Encryption + Authentication or Authentication Only to communicate in **IPSec**

**Algorithm** list:

ENC Algorithm: **3DES/DES/AES/NULL**

AUTH Algorithm: **MD5/SHA1**

Here we select 3DES for ENC Algorithm and MD5 for AUTH Algorithm to make sure the encapsulation way for data transmission

IPSec Algorithm	
<input checked="" type="radio"/> Data Encryption + Authentication	
ENC Algorithm	3DES ▼
AUTH Algorithm	MD5 ▼
<input type="radio"/> Authentication Only	

#### IPSec Algorithm Setting

**STEP 7 .** After selecting GROUP1 in **Perfect Forward Secrecy**, enter 3600 seconds in **ISAKMP Lifetime**, enter 28800 seconds in **IPSec Lifetime**, and selecting **Main mode** in Mode.

Perfect Forward Secrecy	GROUP 1 ▼
ISAKMP Lifetime	3600 Seconds ( Range: 1200 - 86400 )
IPSec Lifetime	28800 Seconds ( Range: 1200 - 86400 )
Mode	<input checked="" type="radio"/> Main mode <input type="radio"/> Aggressive mode

#### IPSec Perfect Forward Secrecy Setting

**STEP 8 .** Complete the IPSec Autokey setting.

i	Name	WAN	Gateway IP	IPSec Algorithm	Configure
--	VPN_A	WAN1	211.22.22.22	3DES / MD5	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

#### Complete Company A IPSec Autokey Setting


**STEP 9 .** Enter the following setting in **Tunnel** of **VPN** function:

- Enter a specific Tunnel **Name**.
- **From Source:** Select LAN
- **From Source Subnet / Mask:** Enter 192.168.10.0 / 255.255.255.0.
- **To Destination:** Select To Destination Subnet / Mask.
- **To Destination Subnet / Mask:** Enter 192.168.85.0 / 255.255.255.0.
- **IPSec / PPTP Setting:** Select VPN\_A.
- Select **Show remote Network Neighborhood**.
- Click **OK**.

New Entry Tunnel	
Name	IPsec_VPN_Tunnel (Max. 16 characters)
From Source	<input checked="" type="radio"/> LAN <input type="radio"/> DMZ
From Source Subnet / Mask	192.168.10.0 / 255.255.255.0
To Destination	<input checked="" type="radio"/> To Destination Subnet / Mask 192.168.85.0 / 255.255.255.0 <input type="radio"/> Remote Client
IPSec / PPTP Setting	VPN_A ▼
Keep alive IP :	
<input checked="" type="checkbox"/> Show remote Network Neighborhood	

OK Cancel

### New Entry Tunnel Setting

i	Name	Source Subnet	Destination Subnet	IPSec / PPTP	Configure
	IPsec_VPN_Tu...	192.168.10.0	192.168.85.0	VPN_A	Modify Remove Pause

New Entry

### Complete New Entry Tunnel Setting

**STEP 10 .** Enter the following setting in **Outgoing Policy**:

- **Tunnel:** Select IPsec\_VPN\_Tunnel.
- Click **OK**.

Comment :  (Max. 32 characters)

Modify Policy	
Source Address	Inside_Any ▾
Destination Address	Outside_Any ▾
Service	Mail_service ▾
Schedule	None ▾
Authentication User	None ▾
<b>Tunnel</b>	<b>IPsec_VPN_Tunnel ▾</b>
Action, WAN Port	PERMIT ALL ▾
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> Enable
IM / P2P Blocking	None ▾
QoS	None ▾
MAX. Bandwidth Per Source IP	Downstream <input type="text" value="0"/> Kbps Upstream <input type="text" value="0"/> Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )

**Setting the VPN Tunnel Outgoing Policy**

Source	Destination	Service	Action	Option					Configure			Move
Inside_Any	Outside_Any	Mail_service	VPN						<input type="button" value="Modify"/>	<input type="button" value="Remove"/>	<input type="button" value="Pause"/>	To 1 ▾

**Complete the VPN Tunnel Outgoing Policy Setting**

**STEP 11 . Enter the following setting in Incoming Policy:**

- **Tunnel:** Select IPsec\_VPN\_Tunnel.
- Click **OK**.

Comment :  (Max. 32 characters)

Modify Policy	
Source Address	Outside_Any
Destination Address	Inside_Any
Service	ANY
Schedule	None
Tunnel	IPsec_VPN_Tunnel
Action	PERMIT
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
QoS	None
MAX. Bandwidth Per Source IP	Downstream <input type="text"/> Kbps Upstream <input type="text"/> Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	<input type="text"/> ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	<input type="text"/> ( Range: 1 - 99999, 0: means unlimited )
NAT	<input type="checkbox"/> Enable

**Setting the VPN Tunnel Incoming Policy**

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Inside_Any(Routing)	ANY	VPN		<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To 1

**Complete the VPN Tunnel Incoming Policy Setting**

The Default Gateway of Company B is the LAN IP of the MH-2001 192.168.20.1. Follow the steps below:

**STEP 12 .** Enter the following setting in **Multiple Subnet** of **System Configure** function:

WAN Interface IP / Forwarding Mode	Interface	Alias IP of Interface / Netmask	Configure
WAN 1 : 211.22.22.22 / NAT WAN 2 : Disable	LAN	192.168.85.1 / 255.255.255.0	<a href="#">Modify</a> <a href="#">Remove</a>

[New Entry](#)

#### Multiple Subnet Setting

**STEP 13 .** Enter the default IP of Gateway of Company B's MH-2001, 192.168.20.1 and select **IPSec Autokey** in **VPN**. Click **New Entry**.

i	Name	WAN	Gateway IP	IPSec Algorithm	Configure
---	------	-----	------------	-----------------	-----------

[New Entry](#)

Figure11-20 IPSec Autokey Web UI

**STEP 14 .** In the list of **IPSec Autokey**, fill in Name with **VPN\_B**.

Necessary Item	
Name	<input type="text" value="VPN_B"/> (Max. 12 characters)
WAN interface	<input checked="" type="radio"/> WAN 1 <input type="radio"/> WAN 2

#### IPSec Autokey Name Setting



**STEP 15 .** Select **Remote Gateway-Fixed IP or Domain Name** In **To Destination** list and enter the IP Address.

To Destination	
<input checked="" type="radio"/> Remote Gateway -- Fixed IP or Domain Name	<input type="text" value="61.11.11.11"/> (Max. 99 characters)
<input type="radio"/> Remote Gateway or Client -- Dynamic IP	

#### IPSec To Destination Setting

**STEP 16 .** Select Preshare in **Authentication Method** and enter the **Preshared Key**. (The maximum Preshared Key is 100 bytes).

Authentication Method	<input type="text" value="Preshare"/>
Preshared Key	<input type="text" value="123456789"/> (Max. 103 characters)

#### IPSec Authentication Method Setting

**STEP 17 .** Select **ISAKMP Algorithm** in **Encapsulation** list. Choose the Algorithm when setup connection. Please select ENC Algorithm (**3DES/DES/AES**), AUTH Algorithm (**MD5/SHA1**), and Group (**GROUP1, 2,5**). Both sides have to choose the same group. Here we select 3DES for ENC Algorithm, MD5 for AUTH Algorithm, and GROUP1 for group.

Encapsulation	
ISAKMP Algorithm	
ENC Algorithm	<input type="text" value="3DES"/>
AUTH Algorithm	<input type="text" value="MD5"/>
Group	<input type="text" value="GROUP 1"/>

#### IPSec Encapsulation Setting

**STEP 18 .** You can choose Data Encryption + Authentication or Authentication Only to communicate in **IPSec**

**Algorithm** list:

ENC Algorithm: **3DES/DES/AES/NULL**

AUTH Algorithm: **MD5/SHA1**

Here we select 3DES for ENC Algorithm and MD5 for AUTH Algorithm to make sure the encapsulation way for data transmission.

IPSec Algorithm	
<input checked="" type="radio"/> Data Encryption + Authentication	
ENC Algorithm	3DES ▼
AUTH Algorithm	MD5 ▼
<input type="radio"/> Authentication Only	

**IPSec Algorithm Setting**

**STEP 19 .** After selecting GROUP1 in **Perfect Forward Secrecy**, enter 3600 seconds in **ISAKMP Lifetime**, enter 28800 seconds in **IPSec Lifetime**, and selecting Main mode in **Mode**.

Perfect Forward Secrecy	GROUP 1 ▼
ISAKMP Lifetime	3600 Seconds ( Range: 1200 - 86400 )
IPSec Lifetime	28800 Seconds ( Range: 1200 - 86400 )
Mode	<input checked="" type="radio"/> Main mode <input type="radio"/> Aggressive mode

**Figure11-26 IPSec Perfect Forward Secrecy Setting**

**STEP 20 .** Complete the IPSec Autokey setting.

i	Name	WAN	Gateway IP	IPSec Algorithm	Configure
--	VPN_B	WAN1	61.11.11.11	3DES / MD5	<a href="#">Modify</a> <a href="#">Remove</a>

[New Entry](#)

**Complete Company B IPSec Autokey Setting**

**STEP 21** . Enter the following setting in **Tunnel** of **VPN** function:

- Enter a specific Tunnel **Name**.
- **From Source**: Select LAN
- **From Source Subnet / Mask**: Enter 192.168.85.0 / 255.255.255.0.
- **To Destination**: Select To Destination Subnet / Mask.
- **To Destination Subnet / Mask**: Enter 192.168.10.0 / 255.255.255.0.
- **IPSec / PPTP Setting**: Select VPN\_B.
- Select **Show remote Network Neighborhood**.
- Click **OK**.

New Entry Tunnel	
Name	IPsec_VPN_Tunnel (Max. 16 characters)
From Source	<input checked="" type="radio"/> LAN <input type="radio"/> DMZ
From Source Subnet / Mask	192.168.85.0 / 255.255.255.0
To Destination	<input checked="" type="radio"/> To Destination Subnet / Mask <input type="radio"/> Remote Client
	192.168.10.0 / 255.255.255.0
IPSec / PPTP Setting	VPN_B ▼
Keep alive IP :	
<input checked="" type="checkbox"/> Show remote Network Neighborhood	

OK Cancel

### New Entry Tunnel Setting

i	Name	Source Subnet	Destination Subnet	IPSec / PPTP	Configure
	IPsec_VPN_Tu...	192.168.85.0	192.168.10.0	VPN_B	<div>Modify</div> <div>Remove</div> <div>Pause</div>

New Entry

### Complete New Entry Tunnel Setting

**STEP 22 . Enter the following setting in Outgoing Policy:**

- **Tunnel:** Select IPSec\_VPN\_Tunnel.
- Click **OK**.

Comment :  (Max. 32 characters)

Modify Policy	
Source Address	Inside_Any ▾
Destination Address	Outside_Any ▾
Service	ANY ▾
Schedule	None ▾
Authentication User	None ▾
<b>Tunnel</b>	<b>IPsec_VPN_Tunnel ▾</b>
Action, WAN Port	PERMIT ALL ▾
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> Enable
IM / P2P Blocking	None ▾
QoS	None ▾
MAX. Bandwidth Per Source IP	Downstream <input type="text" value="0"/> Kbps Upstream <input type="text" value="0"/> Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )

**Setting the VPN Tunnel Outgoing Policy**

Source	Destination	Service	Action	Option					Configure			Move
Inside_Any	Outside_Any	ANY	VPN						<input type="button" value="Modify"/>	<input type="button" value="Remove"/>	<input type="button" value="Pause"/>	To 1 ▾

**Complete the VPN Tunnel Outgoing Policy Setting**

**STEP 23 . Enter the following setting in Incoming Policy:**

- **Tunnel:** Select IPSec\_VPN\_Tunnel.
- Click **OK**.

Comment :  (Max. 32 characters)

Modify Policy	
Source Address	Outside_Any ▾
Destination Address	Inside_Any ▾
Service	ANY ▾
Schedule	None ▾
Tunnel	IPsec_VPN_Tunnel ▾
Action	PERMIT ▾
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
QoS	None ▾
MAX. Bandwidth Per Source IP	Downstream <input type="text" value="0"/> Kbps Upstream <input type="text" value="0"/> Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
NAT	<input type="checkbox"/> Enable

**Setting the VPN Tunnel Incoming Policy**

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Inside_Any(Routing)	ANY	VPN		<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To 1 ▾

**Complete the VPN Tunnel Incoming Policy Setting****STEP 24 . Complete IPSec VPN Connection.****IPSec VPN Connection Deployment**

## 6.9.2 Example.2

### The way to set the MH-2001 appliance IPSec VPN connection in Windows 2000.

#### The Deployment

Company A : Use the MH-2001

**WAN IP: 61.11.11.11**

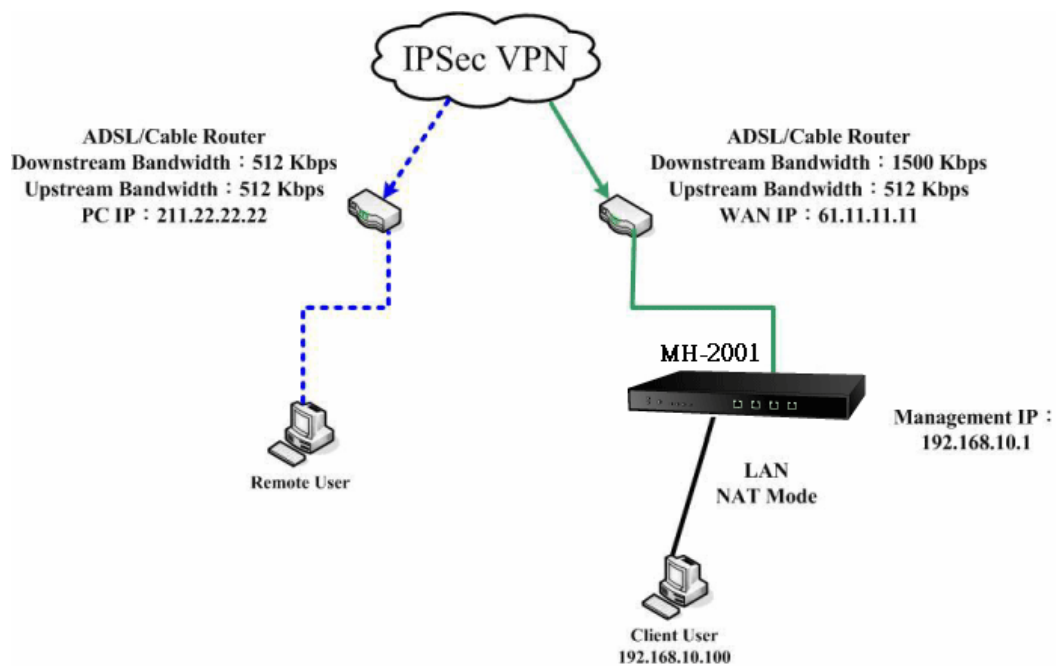
**LAN IP: 192.168.10.X**

Company B : The PC with Windows 2000 inside.

**WAN IP: 211.22.22.22**

We use the MH-2001 and Windows 2000 VPN-IPsec to be the platform. On the other hand, we assume that B Company 211.22.22.22 want to build the VPN to A Company 192.168.10.100, in order to download the shared document.

#### TEST Environment



The MH-2001 and Windows 2000 IPSec VPN deployment

The A Company's default gateway is the LAN IP 192.168.10.1 in the MH-2001. Add the following settings :

**STEP 1** . Enter the A Company's MH-2001 default IP 192.168.10.1. Click **VPN → IPsec Autokey → New Entry**.

i	Name	WAN	Gateway IP	IPsec Algorithm	Configure
---	------	-----	------------	-----------------	-----------

New Entry

### IPsec Autokey

**STEP 2** . In **IPsec Autokey**, enter VPN\_A in **Name**. In **WAN interface**, select WAN 1, in order to build up the A Company's VPN connection.

Necessary Item	
Name	VPN_A (Max. 12 characters)
WAN interface	<input checked="" type="radio"/> WAN 1 <input type="radio"/> WAN 2

### The IPsec VPN name and WAN interface setting

**STEP 3** . In **To Destination**, select **Remote Gateway or Client—Dynamic IP**

To Destination	
<input type="radio"/> Remote Gateway -- Fixed IP or Domain Name	(Max. 99 characters)
<input checked="" type="radio"/> Remote Gateway or Client -- Dynamic IP	

### The IPsec To Destination setting

**STEP 4** . In **Authentication Method**, select **Preshare**, enter the **Preshared Key**. (The maximum Preshared Key is 100 bytes)

Authentication Method	Preshare
Preshared Key	123456789 (Max. 103 characters)

### The IPsec Authentication Method setting

**STEP 5 . In Encapsulation** → select **ISAKMP Algorithm**. Select the needed algorithm as both sides start the connection. In **ENC Algorithm** (3DES/DES/AES), select 3DES. In **AUTH Algorithm** (MD5/SHA1), select MD5. In **Group** (GROUP 1, 2, 5), select GROUP 2. The both sides need to select the same group.

Encapsulation	
ISAKMP Algorithm	
ENC Algorithm	3DES ▼
AUTH Algorithm	MD5 ▼
Group	GROUP 2 ▼

**The IPSec Encapsulation setting**

**STEP 6 . In IPSec Algorithm**, select **Data Encryption + Authentication** or **Authentication Only: ENC Algorithm** (3DES/DES/AES/NULL), select 3DES. **AUTH Algorithm** (MD5/SHA1), select MD5. To assure the Data Encryption + Authentication Method.

IPSec Algorithm	
<input checked="" type="radio"/> Data Encryption + Authentication	
ENC Algorithm	3DES ▼
AUTH Algorithm	MD5 ▼
<input type="radio"/> Authentication Only	

**The IPSec algorithm setting**



**STEP 7 .** In **Perfect Forward Secrecy** (NO-PFS/ GROUP 1, 2, 5), select GROUP 1. In **ISAKMP Lifetime**, enter 3600 seconds. In **IPSec Lifetime**, enter 28800 seconds. In **Mode**, select main mode.

Perfect Forward Secrecy	GROUP 1 ▾	
ISAKMP Lifetime	3600	Seconds ( Range: 1200 - 86400 )
IPSec Lifetime	28800	Seconds ( Range: 1200 - 86400 )
Mode	<input checked="" type="radio"/> Main mode <input type="radio"/> Aggressive mode	

#### The IPSec Perfect Forward Secrecy setting

**STEP 8 .** Complete the IPSec Autokey setting.

i	Name	WAN	Gateway IP	IPSec Algorithm	Configure
--	VPN_A	WAN1	Dynamic IP	3DES / MD5	<a href="#">Modify</a> <a href="#">Remove</a>

[New Entry](#)

#### Complete the IPSec Autokey setting

**STEP 9 . In VPN → Tunnel , add the following settings :**

- **Name**, enter the Tunnel Name.
- **From Source**, select LAN.
- **From Source Subnet / Mask**, enter Source LAN IP 192.168.10.0 (A Company), and Mask 255.255.255.0.
- **To Destination**, select Remote Client.
- **IPSec / PPTP Setting**, select VPN\_A.
- Select **Show remote Network Neighborhood**.
- Click **OK**.

New Entry Tunnel	
Name	IPsec_VPN_Tunnel (Max. 16 characters)
From Source	<input checked="" type="radio"/> LAN <input type="radio"/> DMZ
From Source Subnet / Mask	192.168.10.0 / 255.255.255.0
To Destination	<input type="radio"/> To Destination Subnet / Mask <input checked="" type="radio"/> Remote Client
IPSec / PPTP Setting	VPN_A ▼
Keep alive IP :	
<input checked="" type="checkbox"/> Show remote Network Neighborhood	

**Add the VPN Tunnel setting**

i	Name	Source Subnet	Destination Subnet	IPSec / PPTP	Configure
	IPsec_VPN_Tu...	192.168.10.0	Remote Client	VPN_A	<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>

**Complete to add the VPN Tunnel setting**

**STEP 10 . In Policy → Outgoing, add the following settings :**

■ **Tunnel**, select IPsec\_VPN\_Tunnel.

■ Click **OK**.

Comment :  (Max. 32 characters)

Add New Policy	
Source Address	Inside_Any ▾
Destination Address	Outside_Any ▾
Service	ANY ▾
Schedule	None ▾
Authentication User	None ▾
Tunnel	IPsec_VPN_Tunnel ▾
Action, WAN Port	PERMIT ALL ▾
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> Enable
IM / P2P Blocking	None ▾
QoS	None ▾
MAX. Bandwidth Per Source IP	Downstream <input type="text" value="0"/> Kbps Upstream <input type="text" value="0"/> Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )

**Set the outgoing policy setting included the VPN Tunnel**

Source	Destination	Service	Action	Option					Configure			Move
Inside_Any	Outside_Any	ANY	VPN						<input type="button" value="Modify"/>	<input type="button" value="Remove"/>	<input type="button" value="Pause"/>	To 1 ▾

**Complete the outgoing policy setting included the VPN Tunnel**

**STEP 11 . In Policy → Incoming, add the following settings :**

■ **Tunnel**, select IPsec\_VPN\_Tunnel.

■ Click **OK**.

Comment :  (Max. 32 characters)

Add New Policy	
Source Address	Outside_Any ▾
Destination Address	Inside_Any ▾
Service	ANY ▾
Schedule	None ▾
<b>Tunnel</b>	<b>IPsec_VPN_Tunnel ▾</b>
Action	PERMIT ▾
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
QoS	None ▾
MAX. Bandwidth Per Source IP	Downstream <input type="text" value="0"/> Kbps Upstream <input type="text" value="0"/> Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
NAT	<input type="checkbox"/> Enable

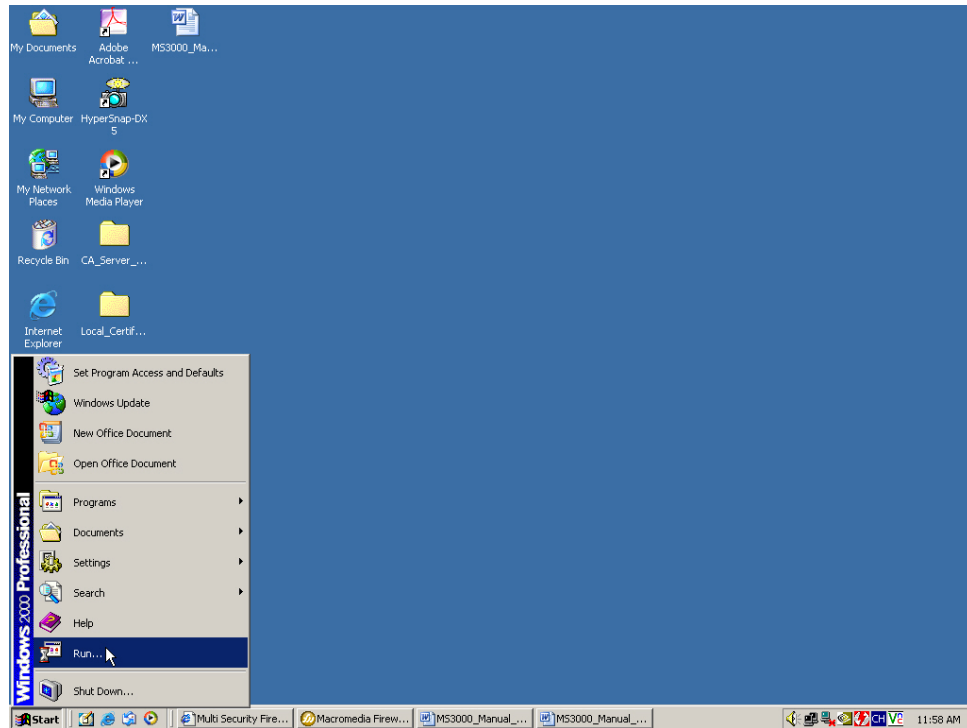
**Set the incoming policy setting included the VPN Tunnel**

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Inside_Any(Routing)	ANY	VPN		<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To 1 ▾

**Complete the incoming policy setting included the VPN Tunnel**

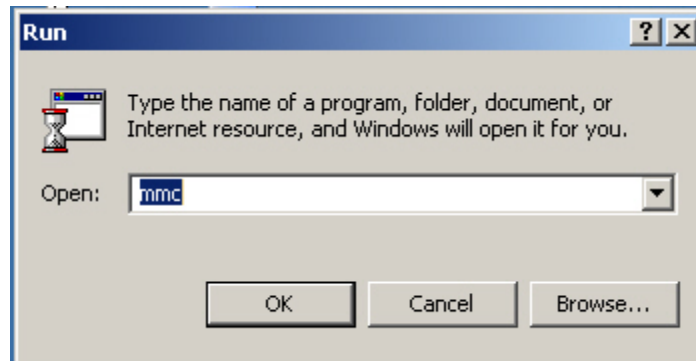
**The B Company's real IP is 211.22.22.22, add the following settings :**

**STEP 12 . Click **Start** → **Run** in Windows 2000**



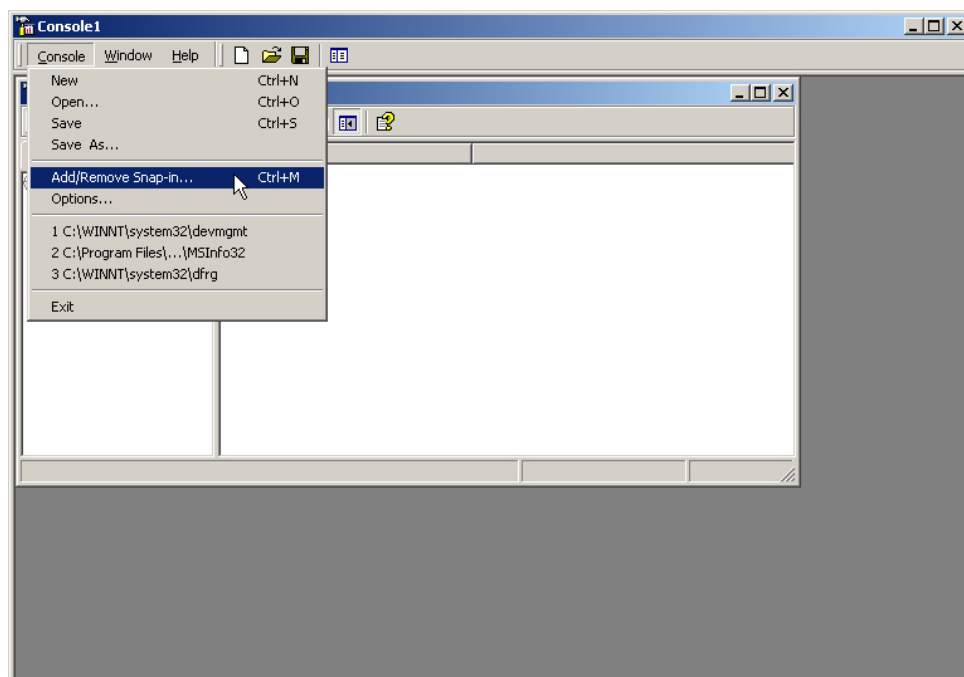
**Start the IPSec VPN setting in Windows 2000**

**STEP 13 .** In **Run** → **Open** column, enter mmc.



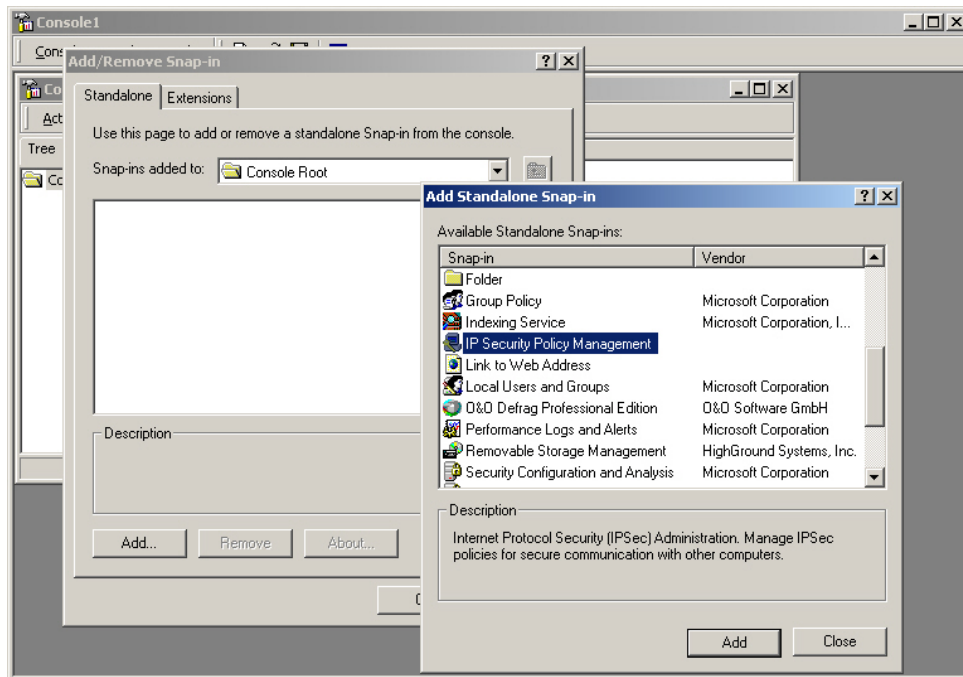
**To startup the Windows 2000 IPsec VPN setting**

**STEP 14 .** In **Console 1** → **Console** → **Add/Remove Snap-in**.



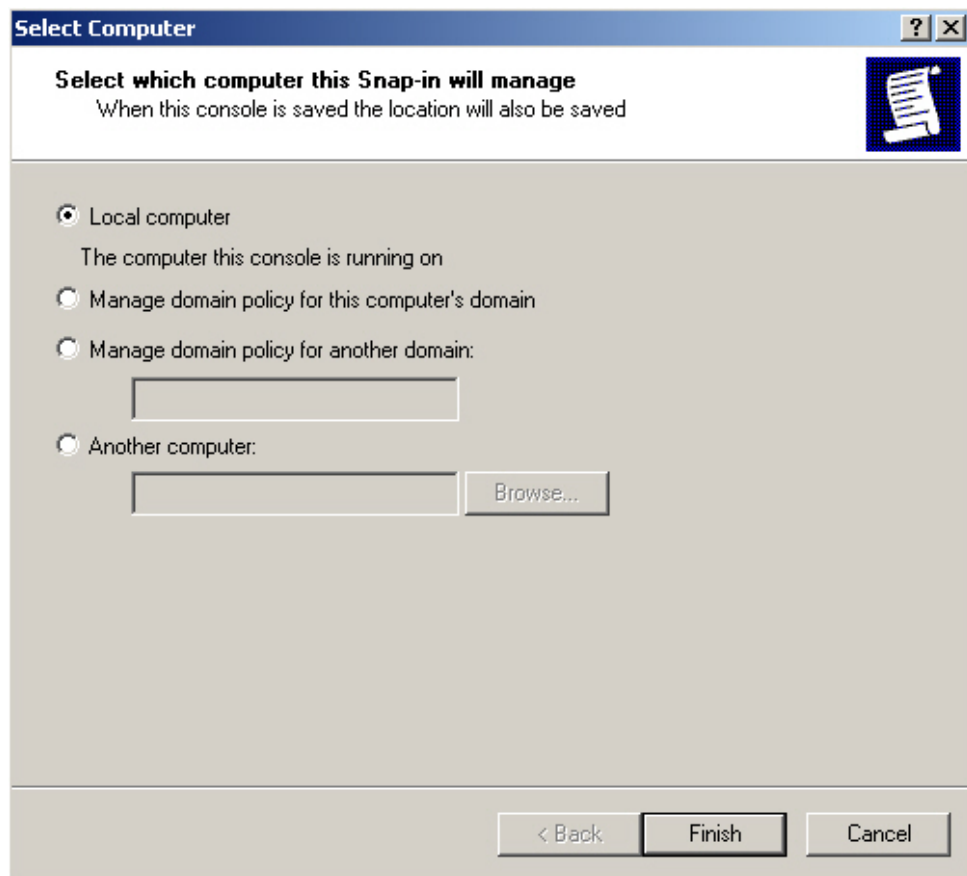
**Add / Remove Snap-in .**

**STEP 15 .** In **Add / Remove Snap-in**, click **Add**. In **Add Standalone Snap-in**, add **IP Security Policy Management**.



**Add IP Security Policy Management**

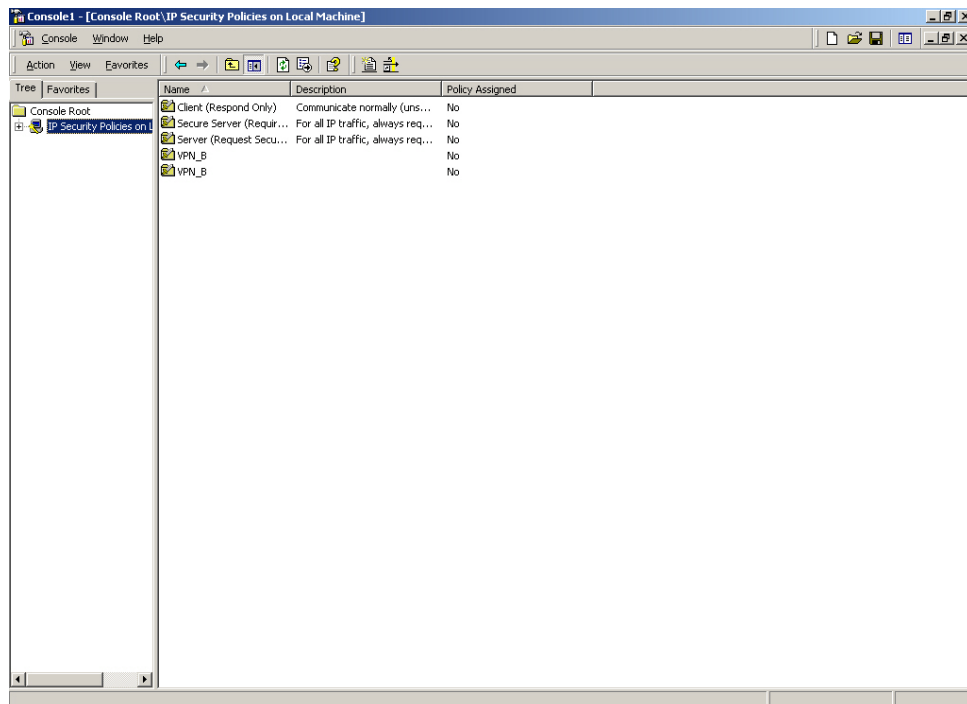
**STEP 16 .** Select **Local Computer**, click **Finish**.



**Select the type of IP Security Policy Management**

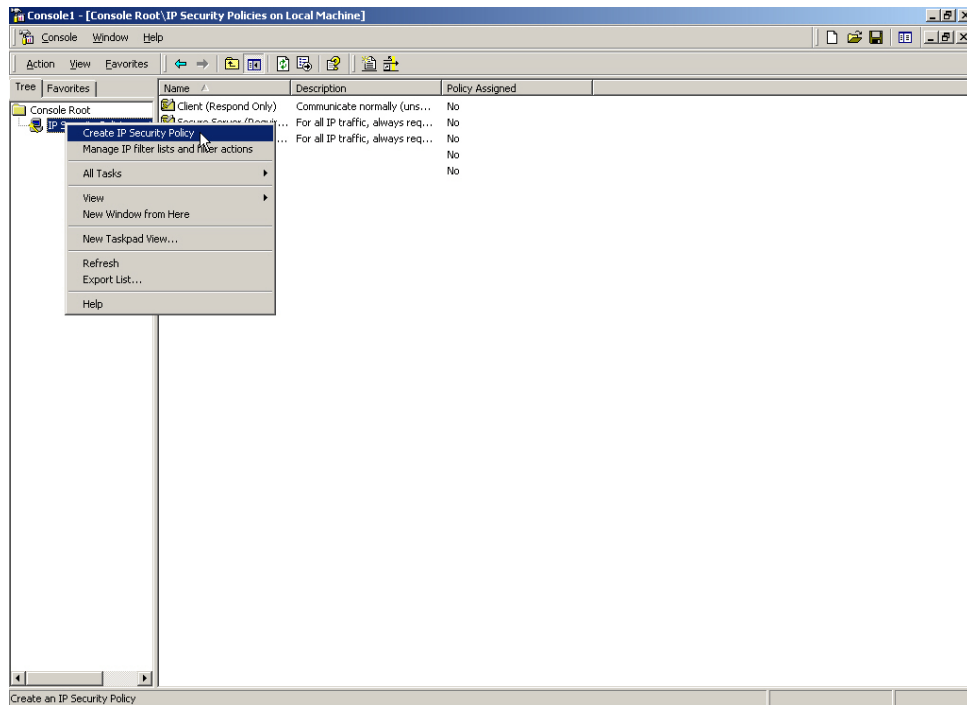


**STEP 17 .** Complete to set the IP Security Policy Management.



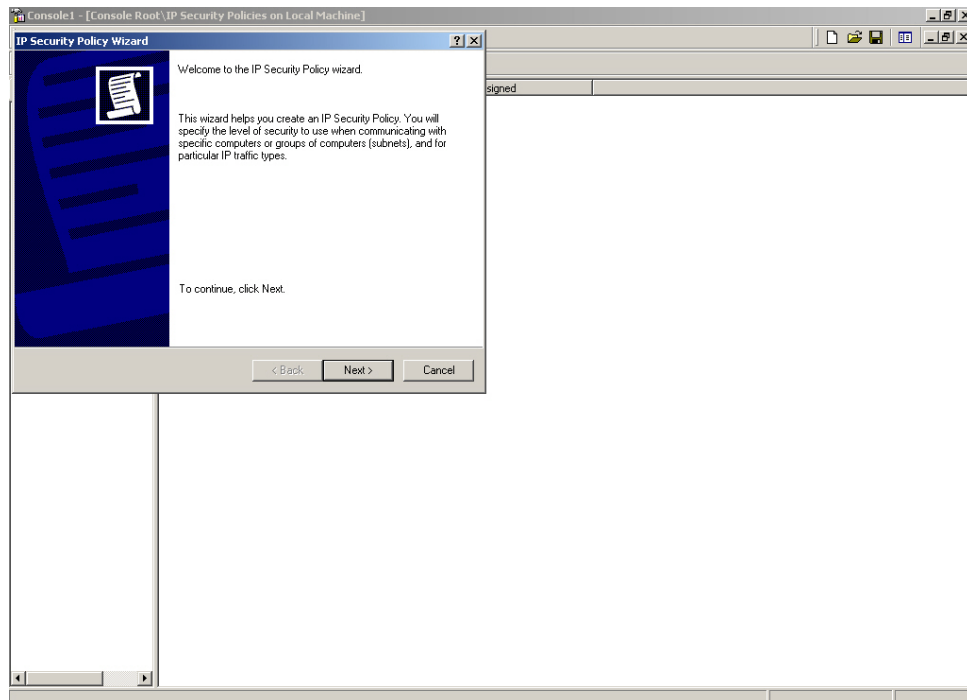
**Complete to set the IP Security Policy Management**

**STEP 18 .** Right click on the **IP Security Policies on Local Machine**, and select **Create IP Security Policy**.



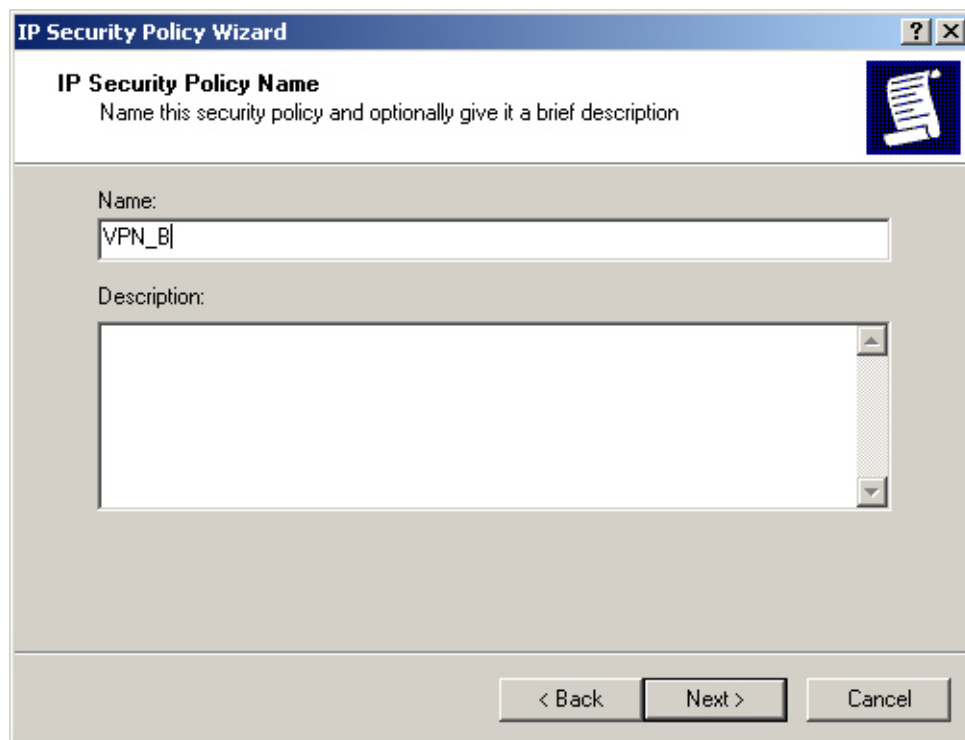
**Create IP Security Policy**

**STEP 19 . Click Next.**



**Open IP Security Policy Wizard**

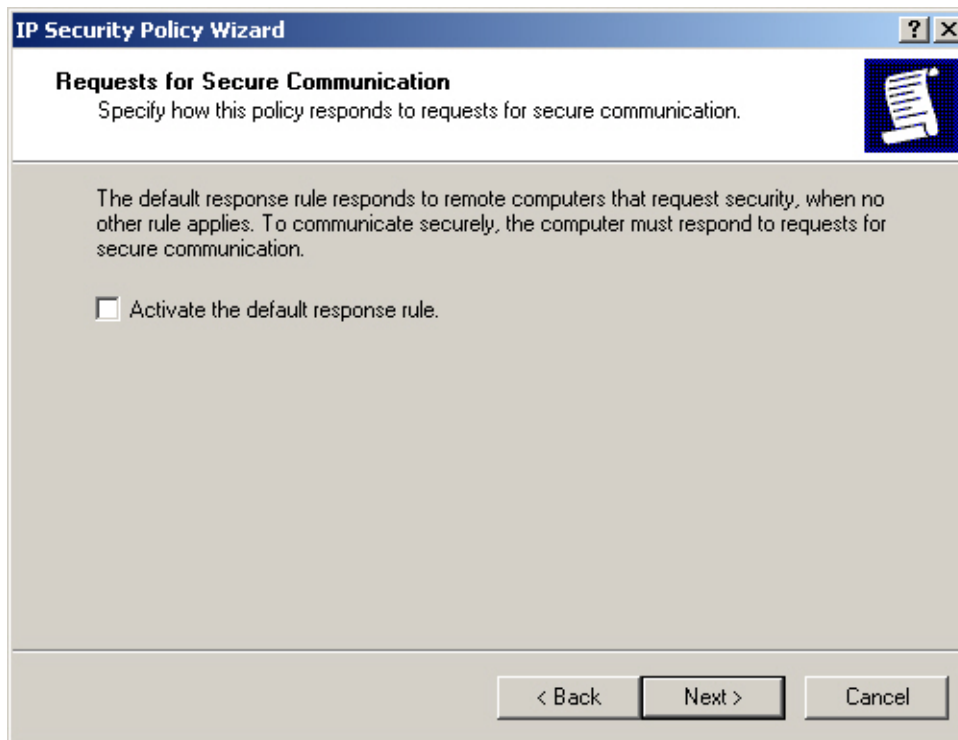
**STEP 20** . Enter the VPN **Name** and **Description**, and click **Next**.



The image shows a Windows-style dialog box titled "IP Security Policy Wizard". The title bar includes a question mark icon and a close button. The main content area has a header section with the title "IP Security Policy Name" and a subtitle "Name this security policy and optionally give it a brief description". To the right of this header is a small icon of a document with a pencil. Below the header, there are two input fields: a "Name:" field containing the text "VPN\_B" and a "Description:" field which is a larger text area. At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel".

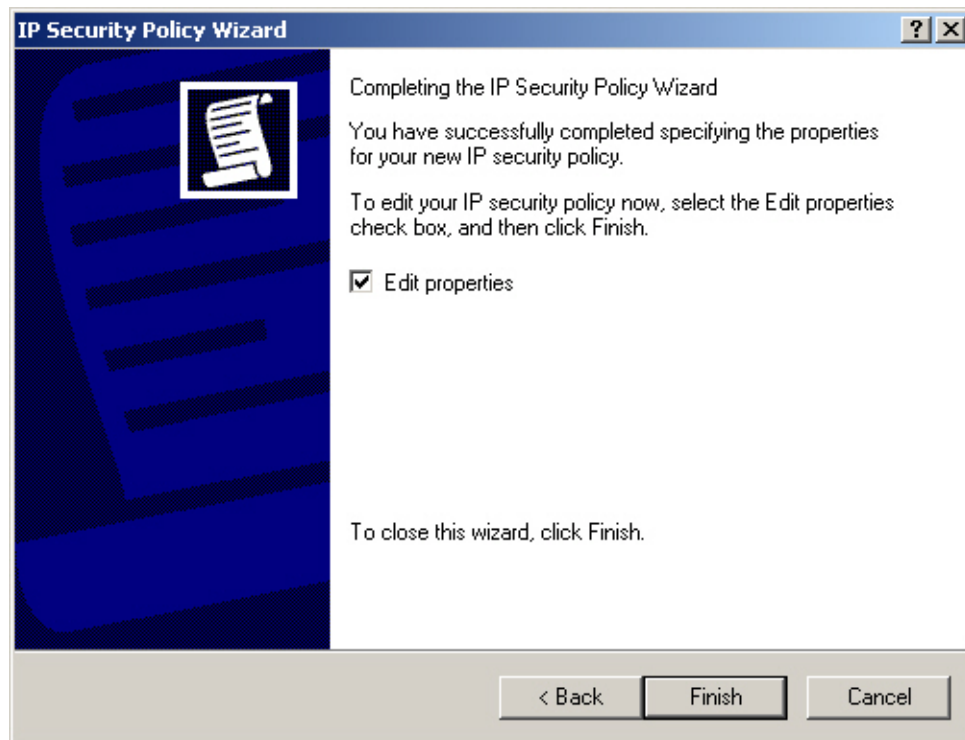
**Set the VPN name and description**

**STEP 21** . Disable to **Activate the default response rule**, and click **Next**.



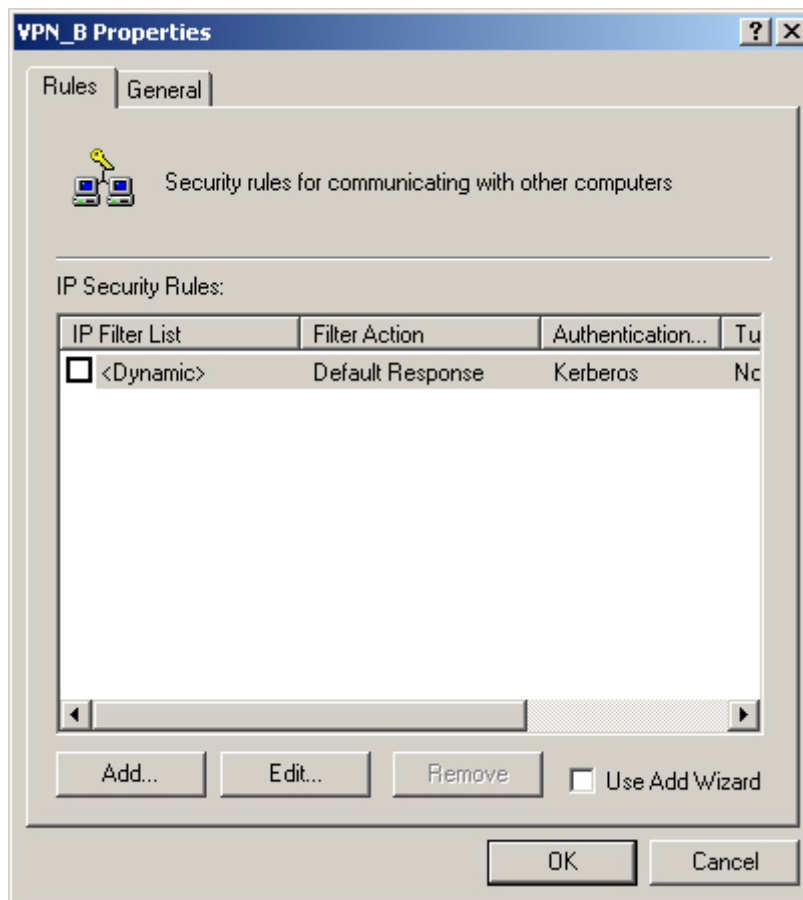
**Disable to activate the default response rule**

**STEP 22 .** In **IP Security Policy Wizard**, select **Edit properties**, click **Finish**.



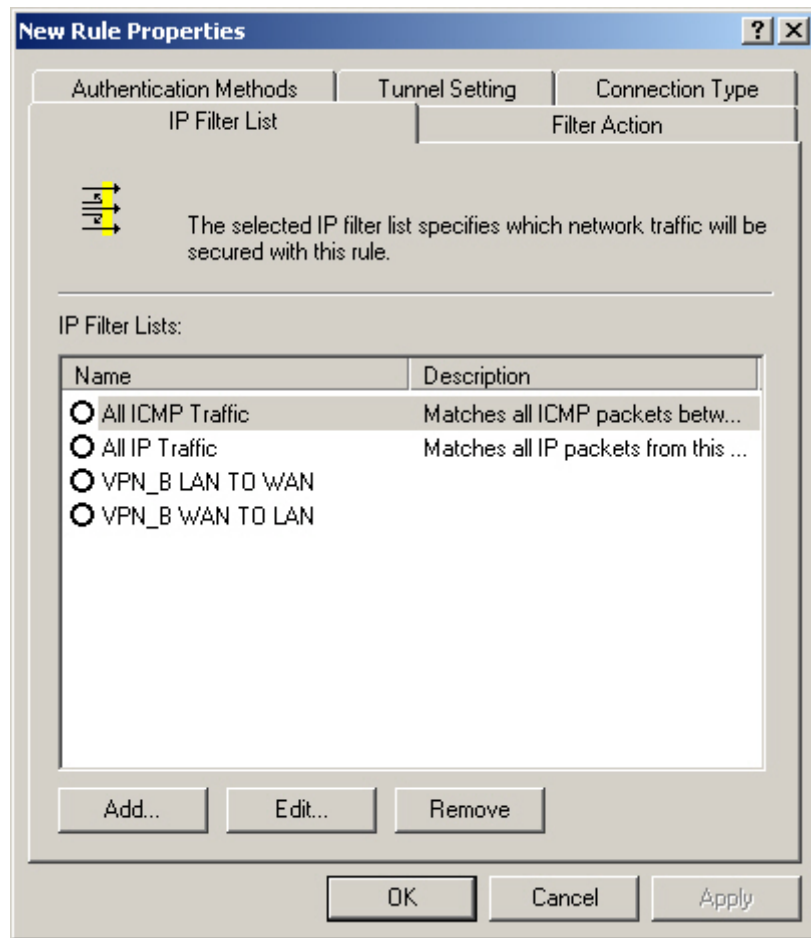
**Complete the IP Security Policy Wizard settings**

**STEP 23 .** In **VPN\_B Properties**, do not select **Use Add Wizard**, and click **Add**.



**VPN\_B Properties**

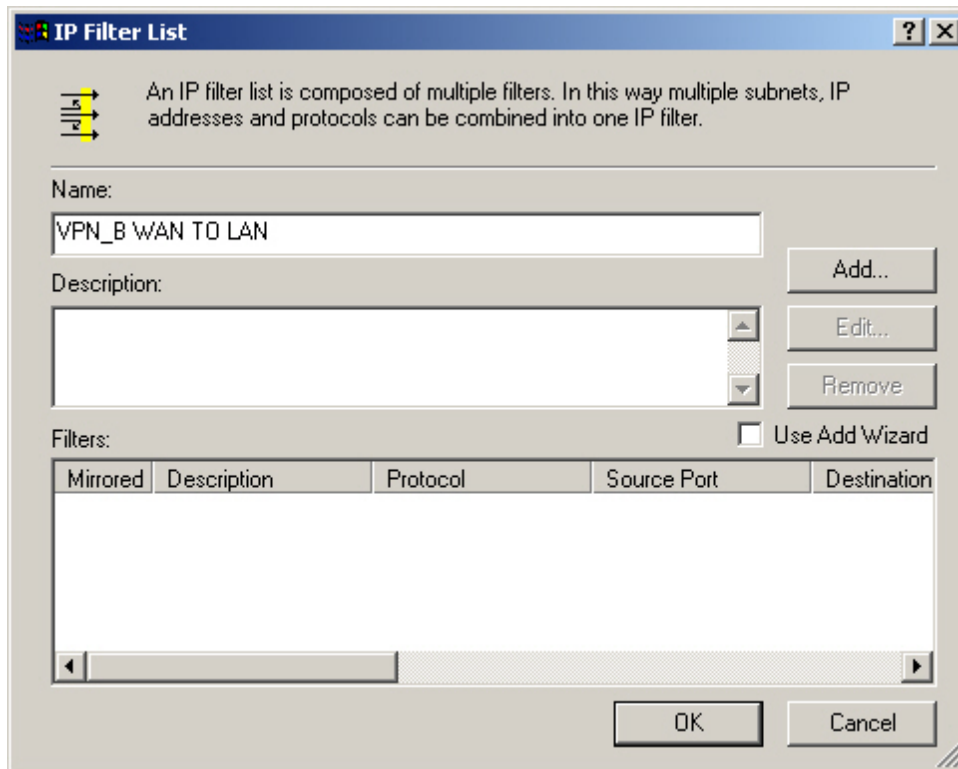
**STEP 24 . In New Rule Properties, Click Add.**



**New Rule Properties**



**STEP 25 .** In **IP Filter List**, do not select **Use Add Wizard**. Modify the **Name** into VPN\_B WAN TO LAN, click **Add**.



The **IP Filter List** dialog box contains the following elements:

- Title Bar:** "IP Filter List" with help and close buttons.
- Help Text:** "An IP filter list is composed of multiple filters. In this way multiple subnets, IP addresses and protocols can be combined into one IP filter."
- Name:** A text box containing "VPN\_B WAN TO LAN".
- Description:** An empty text box with up and down arrow buttons.
- Buttons:** "Add...", "Edit...", and "Remove" buttons.
- Filters:** A checkbox labeled "Use Add Wizard" (unchecked).
- Table:** A table with 5 columns: "Mirrored", "Description", "Protocol", "Source Port", and "Destination". The table is currently empty.
- Bottom:** "OK" and "Cancel" buttons.

**IP Filter List**

**STEP 26 .** In **Filter Properties** → **Source address** → **A specific IP Address**, enter B Company's WAN IP address 211.22.22.22 , Subnet mask 255.255.255.255 . In **Destination address** → **A specific IP Subnet**, enter A Company's LAN IP address 192.168.10.0, subnet mask 255.255.255.0. Do not select **Mirrored**. Also match packets with the exact opposite source and destination addresses.

The screenshot shows the 'Filter Properties' dialog box with the 'Addressing' tab selected. The 'Source address' section has a dropdown menu set to 'A specific IP Address', with the IP Address field containing '211 . 22 . 22 . 22' and the Subnet mask field containing '255 . 255 . 255 . 255'. The 'Destination address' section has a dropdown menu set to 'A specific IP Subnet', with the IP Address field containing '192 . 168 . 10 . 0' and the Subnet mask field containing '255 . 255 . 255 . 0'. At the bottom, the 'Mirrored' checkbox is unchecked, with the text 'Mirrored. Also match packets with the exact opposite source and destination addresses.' below it. The 'OK', 'Cancel', and 'Apply' buttons are at the bottom right.

Source address:	
IP Address:	211 . 22 . 22 . 22
Subnet mask:	255 . 255 . 255 . 255

Destination address:	
IP Address:	192 . 168 . 10 . 0
Subnet mask:	255 . 255 . 255 . 0

☐ Mirrored. Also match packets with the exact opposite source and destination addresses.

**Filter Properties**

**STEP 27** . Complete the setting, and close the **IP Filter List**.

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

Name: VPN\_B WAN TO LAN

Description:

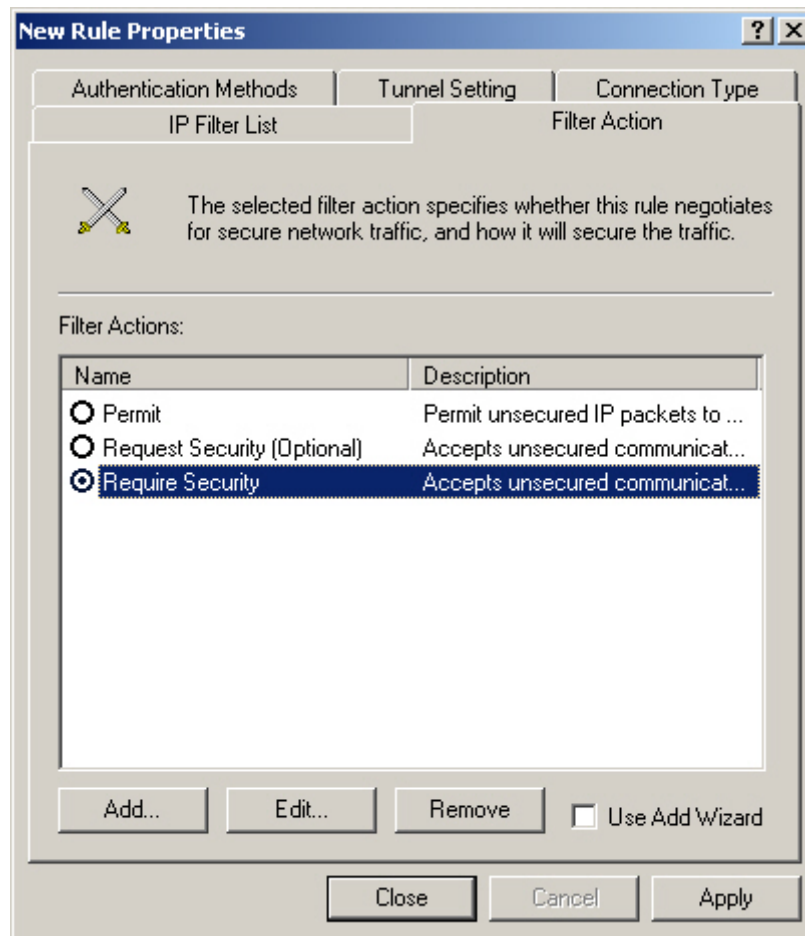
Filters: ☐ Use Add Wizard

Mirrored	Description	Protocol	Source Port	Destination
No		ANY	ANY	ANY

Close Cancel

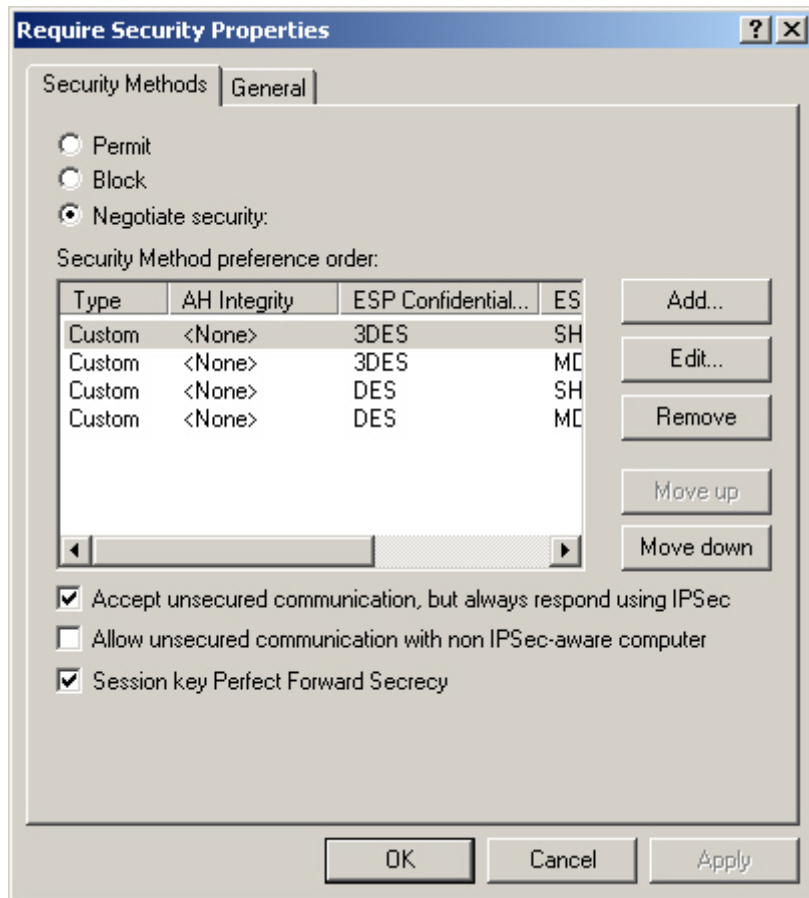
**Complete the IP Filter List setting**

**STEP 28 .** In **New Rule Properties** → **Filter Action** → **Require Security**. Click **Edit**.



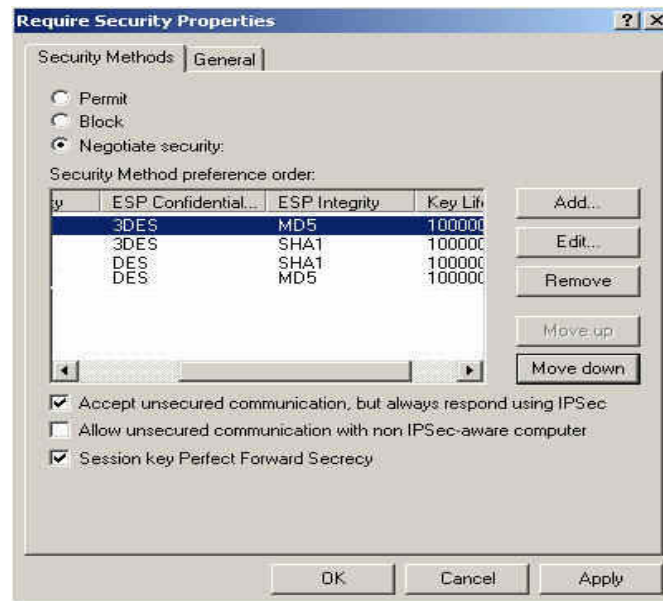
**Filter Action setting**

**STEP 29 .** In **Require Security Properties**, select **Session Key Perfect Forward Secrecy**.



**Select Session Key Perfect Forward Secrecy**

**STEP 30 .** Select **Custom / None / 3DES / MD5** Security Method, click **Edit**.



**Edit the Security Method**

**STEP 31** . Click **Custom (for expert users)**, and click **Settings**.



### Custom Security Method

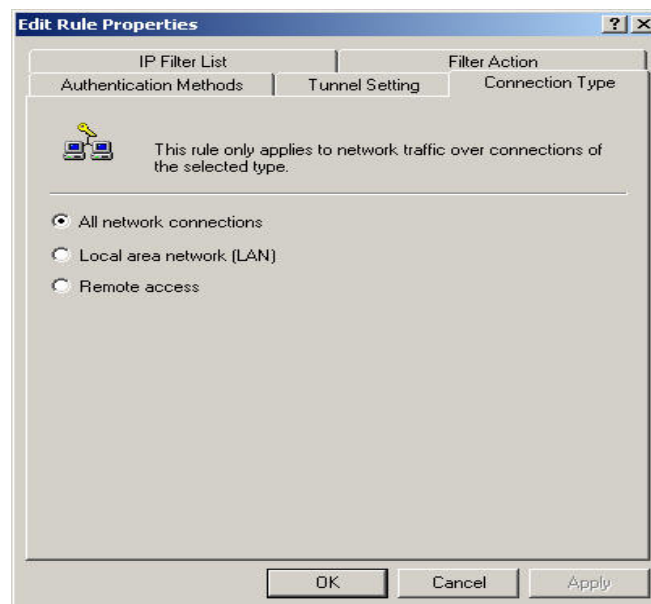
**STEP 32 .** Select **Data integrity and encryption**, choose **Integrity algorithm → MD5. Encryption algorithm → 3DES**. Select **Generate a new key every**, enter 28800 seconds, then click **OK** to back to **New Rule Properties**.



**Custom Security Method settings**



**STEP 33 .** In **New Rule Properties → Connection Type**, select **All network connections**.



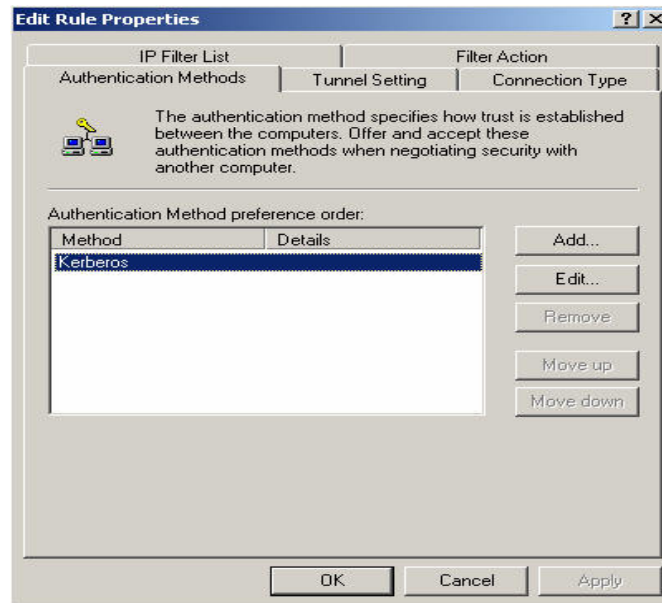
**Connection Type setting**

**STEP 34 .** In **New Rule Properties → Tunnel Setting**, select **The tunnel endpoint is specified by this IP Address**. Enter A Company's WAN IP address 61.11.11.11.



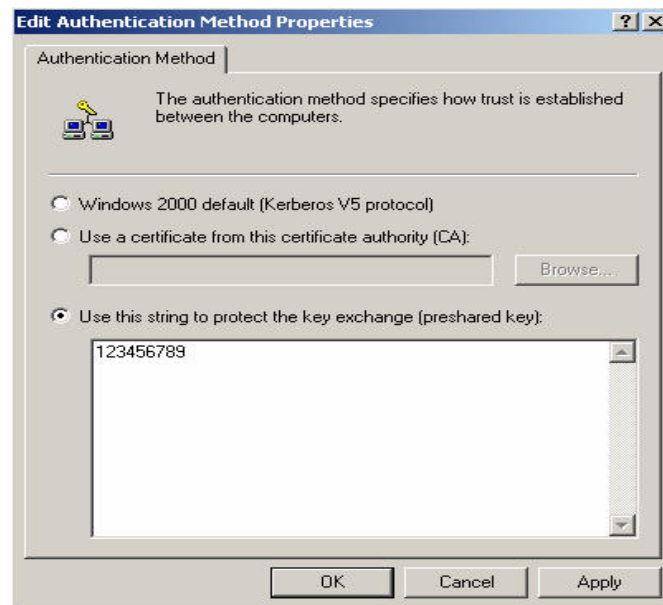
**Tunnel setting**

**STEP 35 .** In **New Rule Properties → Authentication Methods**, click **Edit**.



**Authentication Methods setting**

**STEP 36 .** Select **Use this string to protect the key exchange (Preshared key)**, enter the Preshared Key, 123456789.



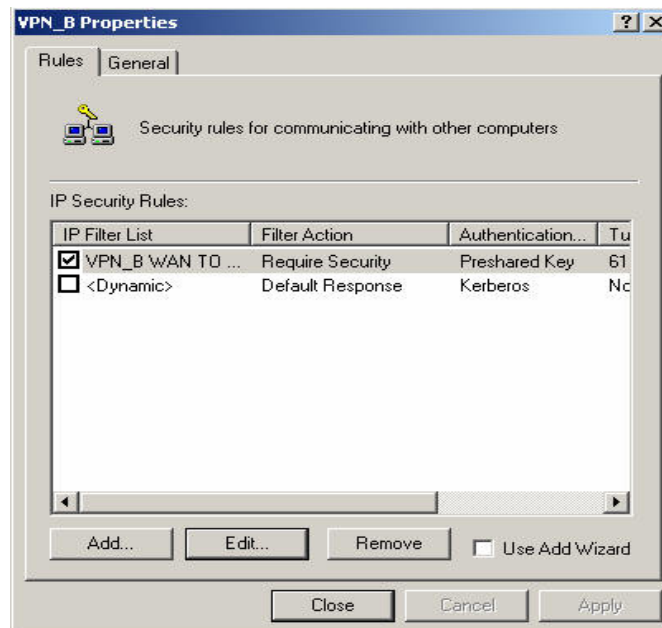
**Set the VPN Preshared Key**

**STEP 37** . Click **Apply** → **OK** → **Close**.



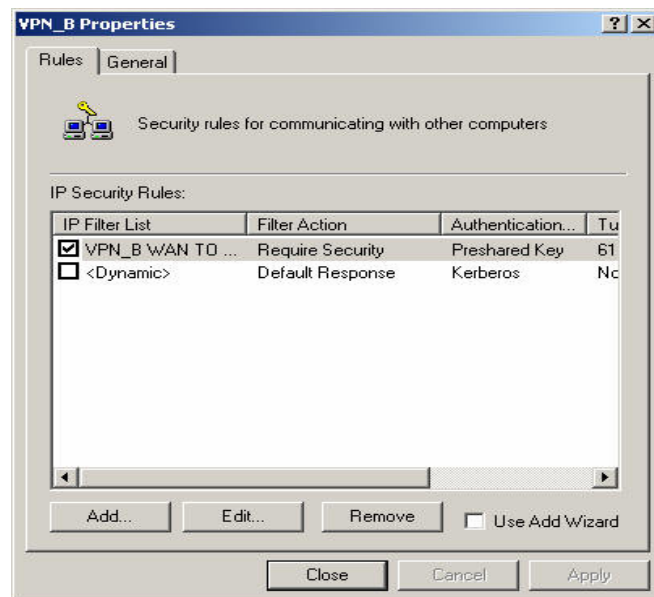
**Complete the Authentication Methods setting**

**STEP 38** . Complete the VPN\_B WAN TO LAN settings.



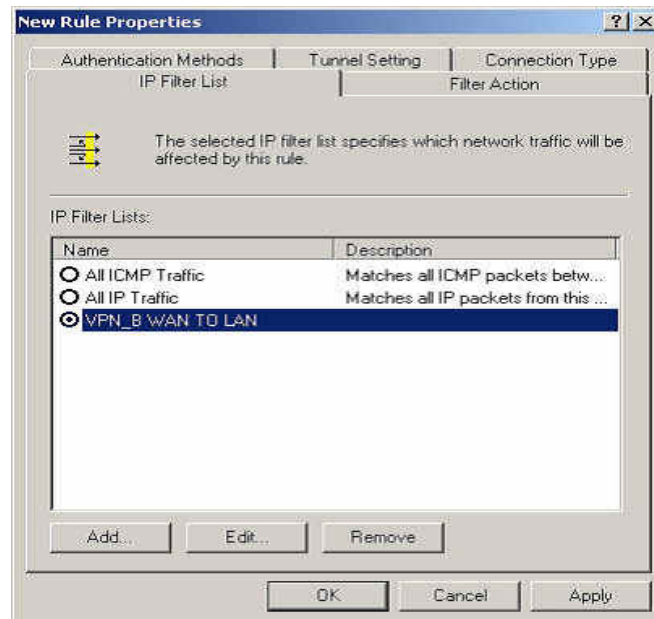
**Complete the VPN\_B WAN TO LAN policy setting**

**STEP 39 .** In **VPN\_B Properties**, do not select **Use Add Wizard**. Click **Add**, to add the second IP security policy.



**The VPN\_B Properties**

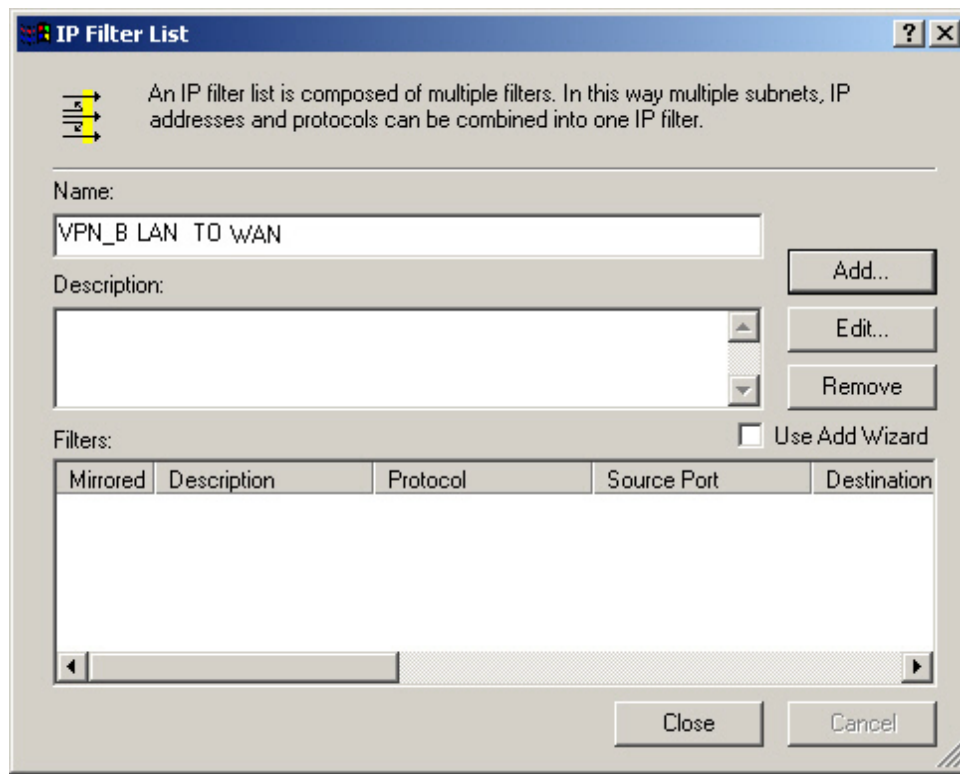
**STEP 40 . In New Rule Properties, click Add.**



**New Rule Properties**



**STEP 41** . In **IP Filter List**, do not select **Use Add Wizard**. Modify the **Name** into VPN\_B LAN TO WAN, click **Add**.



**IP Filter List**

**STEP 42 .** In **Filter Properties**→ **Source address**, select **A specific IP Subnet**, enter A Company's LAN IP Address 192.168.10.0, subnet mask 255.255.255.0. In **Destination address**, select **A specific IP Address**, enter B Company's WAN IP Address 211.22.22.22, subnet mask 255.255.255.255. Do not select **Mirrored, Also match packets with the exact opposite source and destination addresses.**

The screenshot shows the 'Filter Properties' dialog box with the 'Addressing' tab active. It contains two main sections: 'Source address' and 'Destination address'. In the 'Source address' section, a dropdown menu shows 'A specific IP Subnet', and below it, the IP Address is '192 . 168 . 10 . 0' and the Subnet mask is '255 . 255 . 255 . 0'. In the 'Destination address' section, a dropdown menu shows 'A specific IP Address', and below it, the IP Address is '211 . 22 . 22 . 22' and the Subnet mask is '255 . 255 . 255 . 255'. At the bottom, there is an unchecked checkbox labeled 'Mirrored. Also match packets with the exact opposite source and destination addresses.' and three buttons: 'OK', 'Cancel', and 'Apply'.

**Filter Properties**

**STEP 43 .** Complete the settings, close the **IP Filter List**.

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

Name: VPN\_B LAN TO WAN

Description:

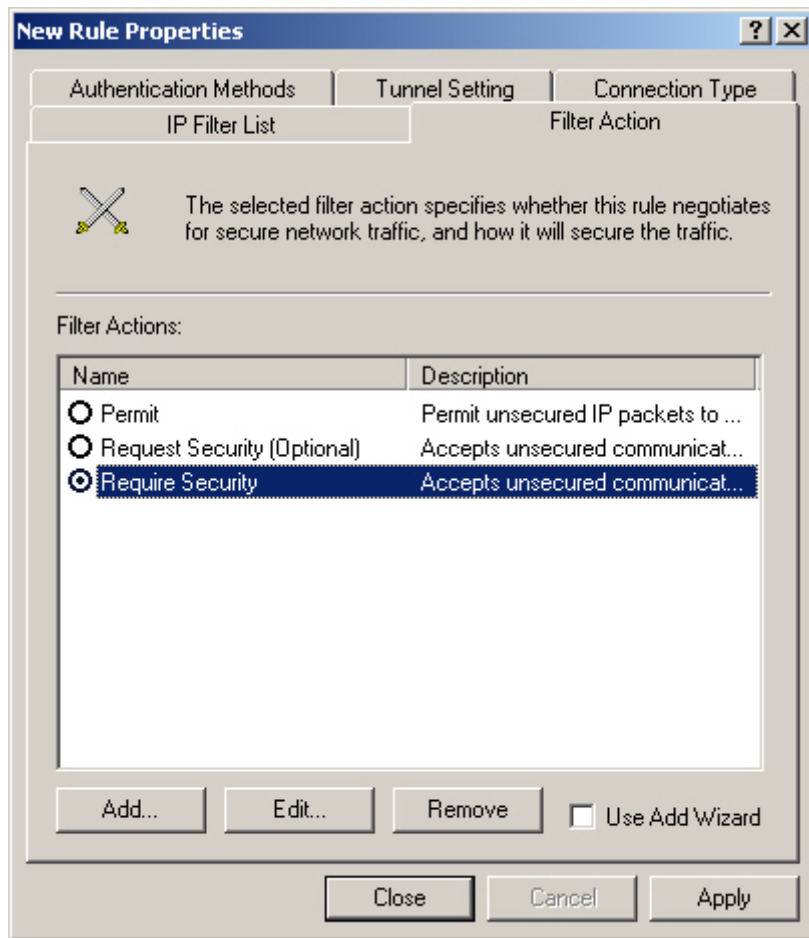
Filters: ☐ Use Add Wizard

Mirrored	Description	Protocol	Source Port	Destination
No		ANY	ANY	ANY

Close Cancel

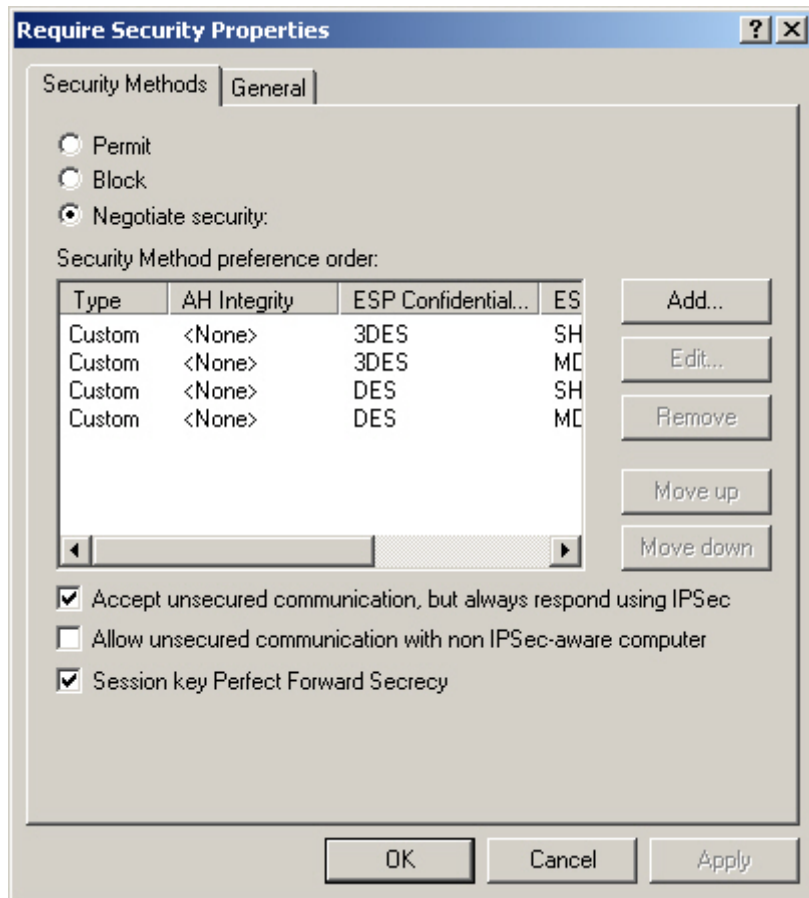
**Complete the IP Filter List setting**

**STEP 44 .** In **New Rule Properties** → **Filter Action**, select **Required Security**, then click **Edit**.



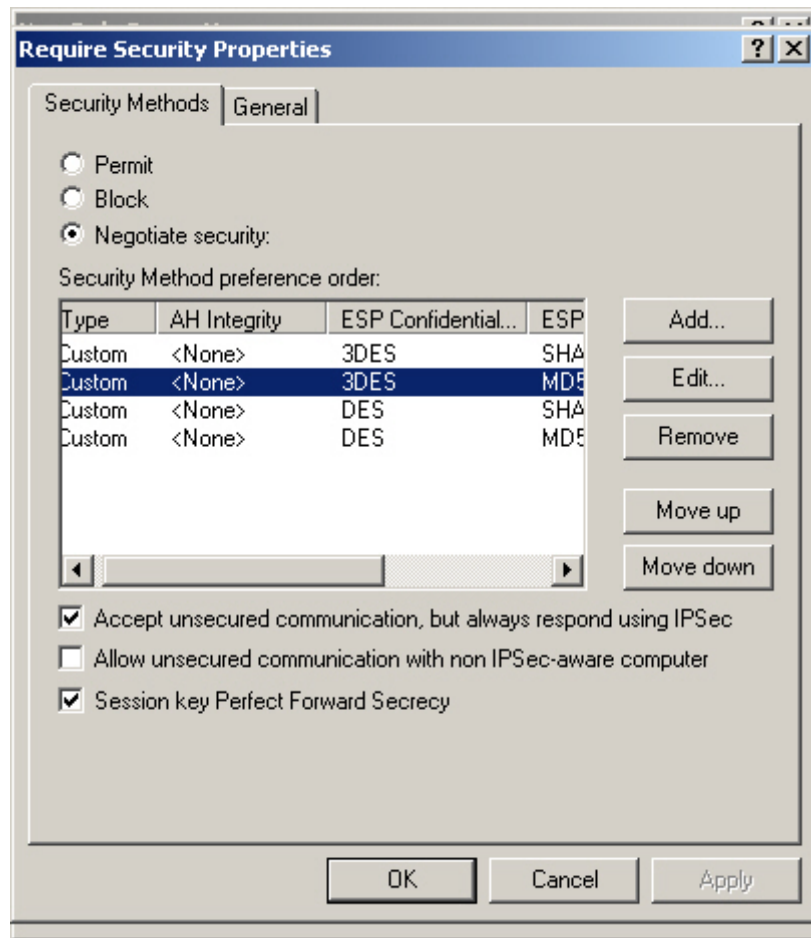
**Filter Action**

**STEP 45 .** In **Require Security Properties**, select **Session key Perfect Forward Secrecy**.



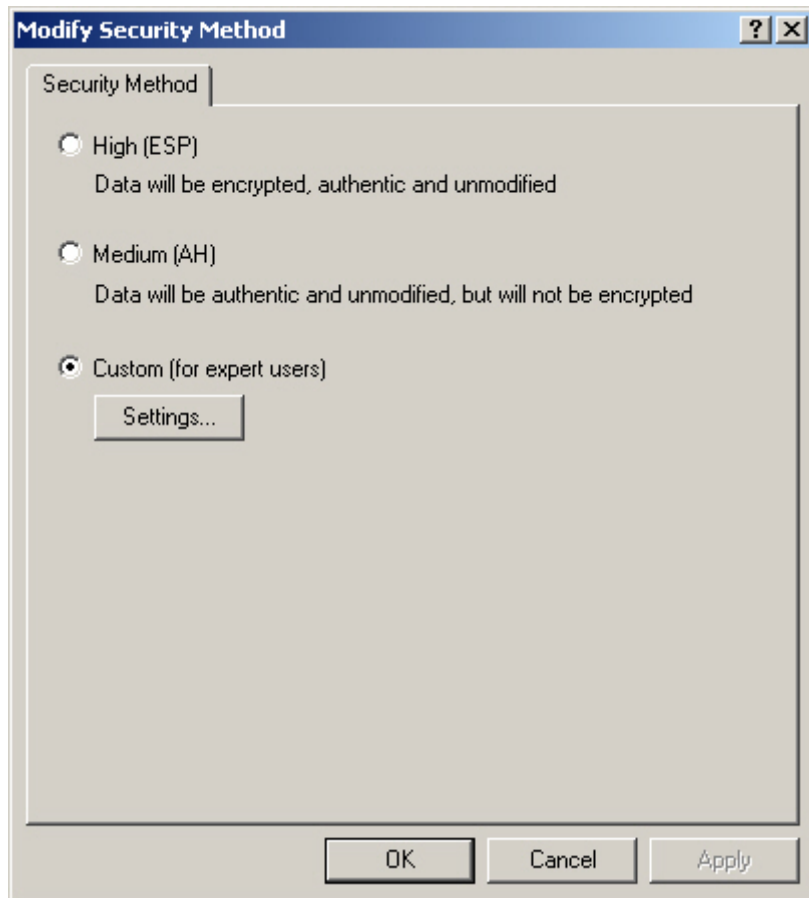
Select Session key Perfect Forward Secrecy

**STEP 46 .** Select **Custom / None / 3DES / MD5** Security Method. Click **Edit**.



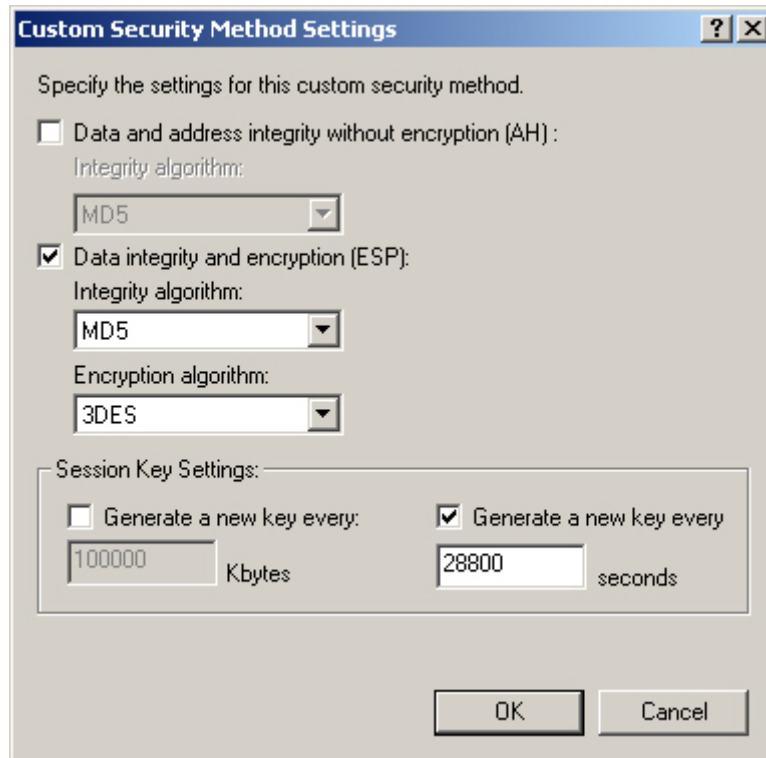
**Set the Security Method**

**STEP 47 .** Select **Custom (for expert users)**, click **Settings**.



**Custom Security Method settings**

**STEP 48 .** Select **Data integrity and encryption (ESP)**. Integrity algorithm, select MD5. **Encryption algorithm**, select 3DES. Also select **Generate a new key every**, enter 28800 seconds. Click **OK** to back to **New Rule Properties**.



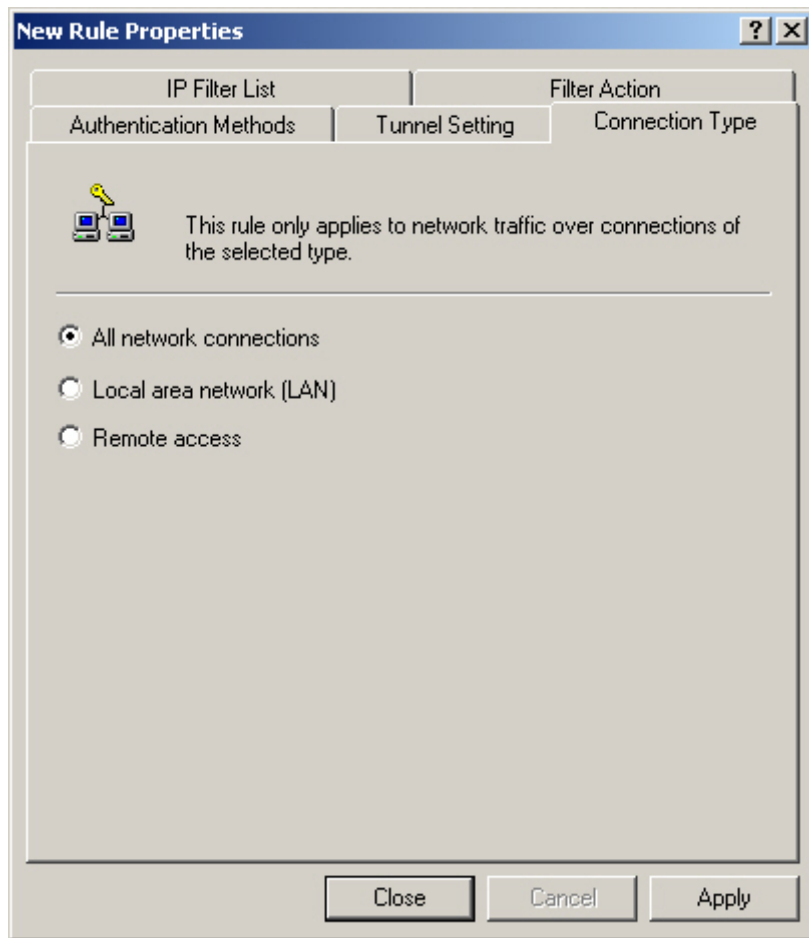
The image shows a Windows-style dialog box titled "Custom Security Method Settings". It contains the following elements:

- A title bar with a question mark icon and a close button (X).
- Text: "Specify the settings for this custom security method."
- Two radio buttons for selecting a security method:
  - ☐ Data and address integrity without encryption (AH) :
  - ☒ Data integrity and encryption (ESP):
- For the selected ESP method:
  - "Integrity algorithm:" with a dropdown menu showing "MD5".
  - "Encryption algorithm:" with a dropdown menu showing "3DES".
- A "Session Key Settings:" section containing:
  - Two checkboxes for "Generate a new key every":
    - ☐ Generate a new key every: (with a text box containing "100000" and the label "Kbytes")
    - ☒ Generate a new key every (with a text box containing "28800" and the label "seconds")
- At the bottom right, "OK" and "Cancel" buttons.

**Complete the Custom Security Methods setting**

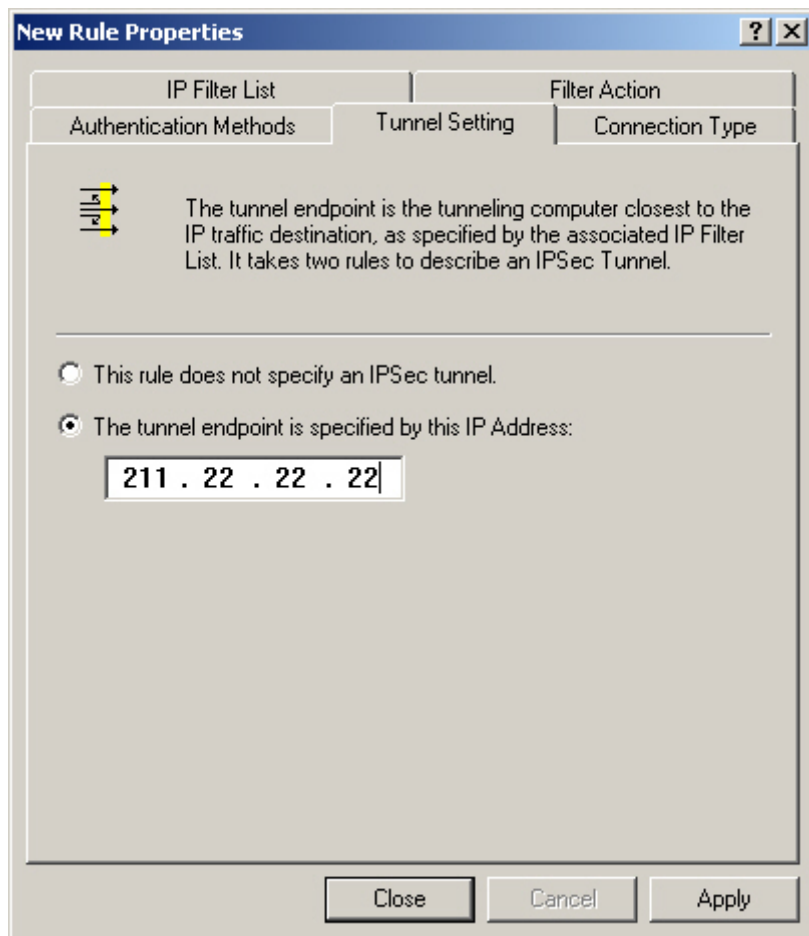


**STEP 49 . In New Rule Properties → Connection Type, select All network connections.**



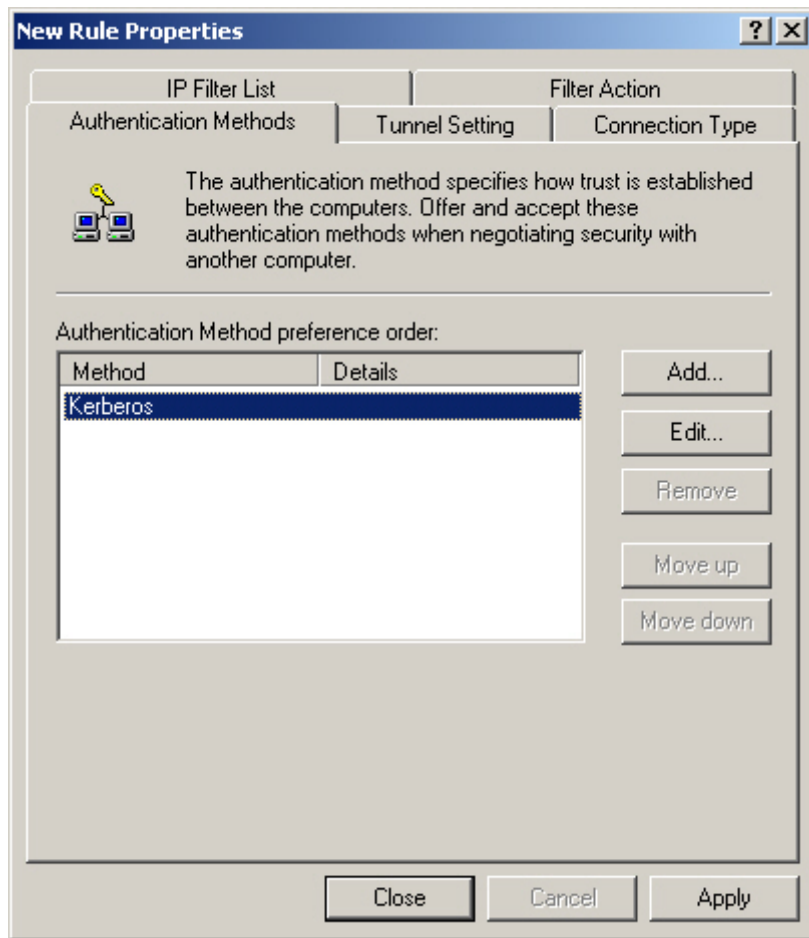
**Connection Type setting**

**STEP 50 .** In **New Rule Properties → Tunnel Setting**, select **The tunnel endpoint is specified by this IP Address**. Enter B Company's WAN IP address **211.22.22.22**.



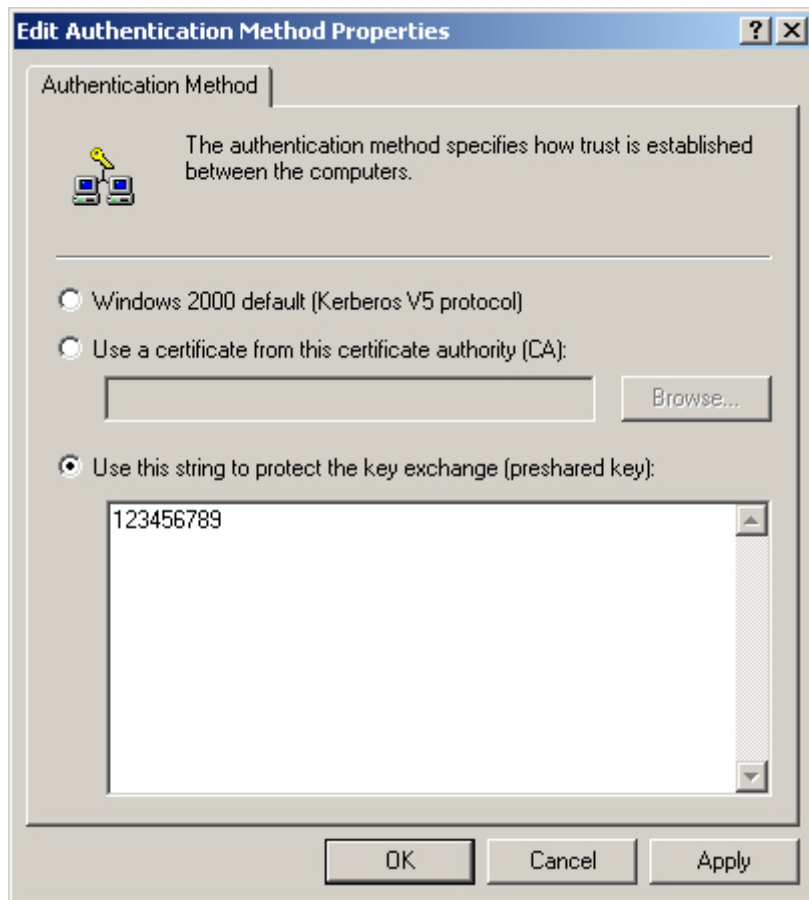
**Tunnel setting**

**STEP 51** . In **New Rule Properties → Authentication Methods**, click **Edit**.



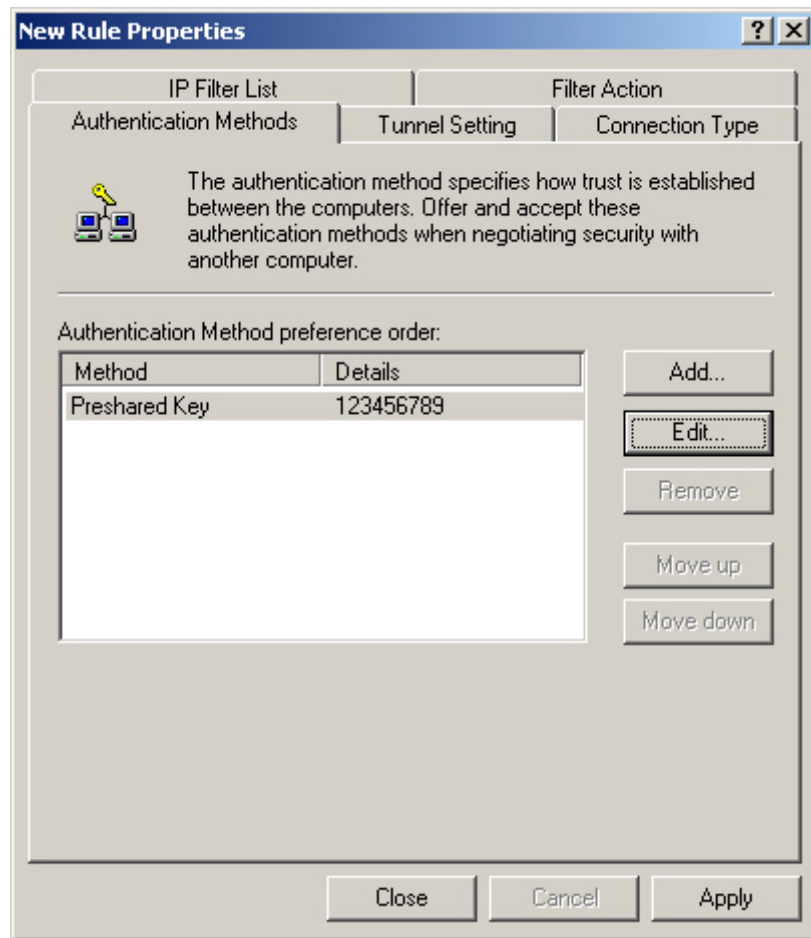
**Authentication Methods**

**STEP 52 .** Select **Use this string to protect the key exchange (Preshared key)**. Enter the Preshared Key, 123456789.



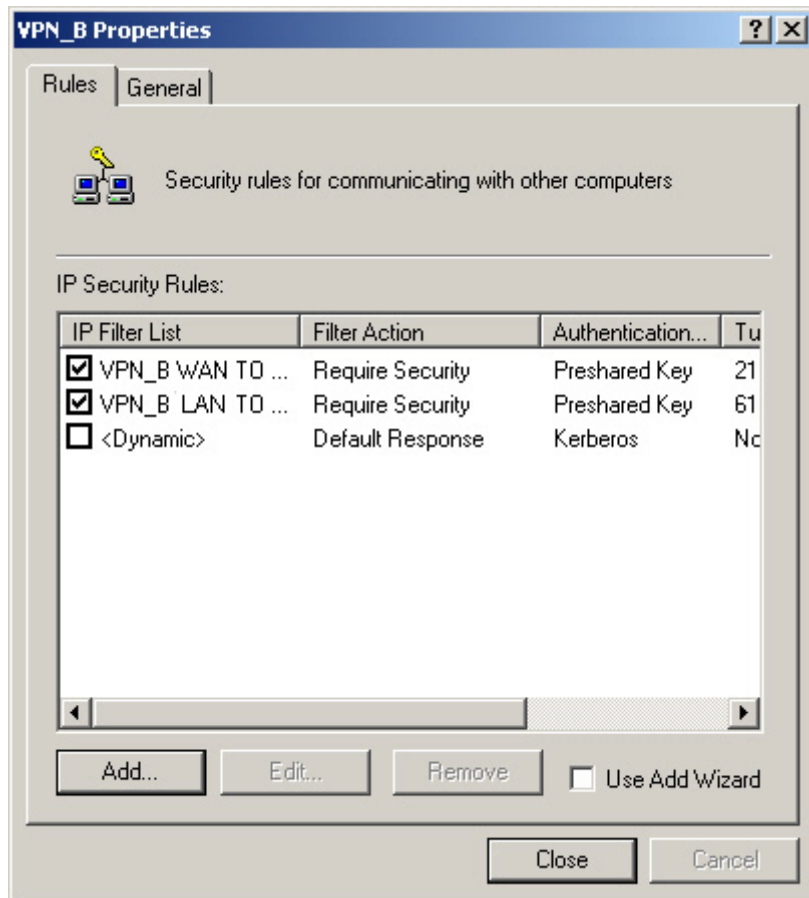
**VPN Preshared key setting**

**STEP 53** . Click **Apply** and **close** the setting window.



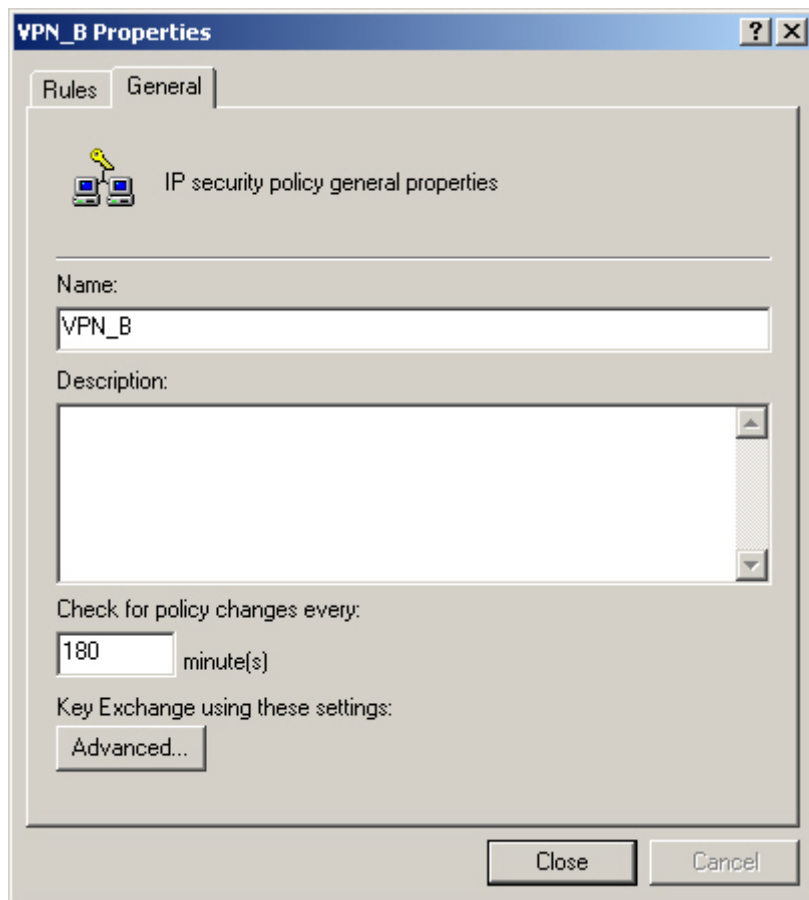
**Complete the New Rule setting**

**STEP 54** . Complete the VPN\_B LAN TO WAN setting.



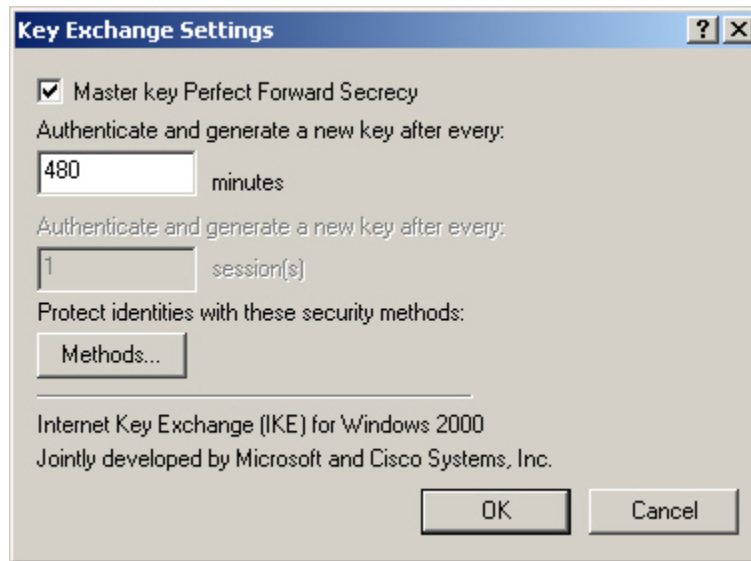
**Complete the VPN\_B LAN TO WAN Rule setting**

**STEP 55 .** In **VPN\_B Properties** → **General**, click **Advanced**.



**The VPN\_B General setting**

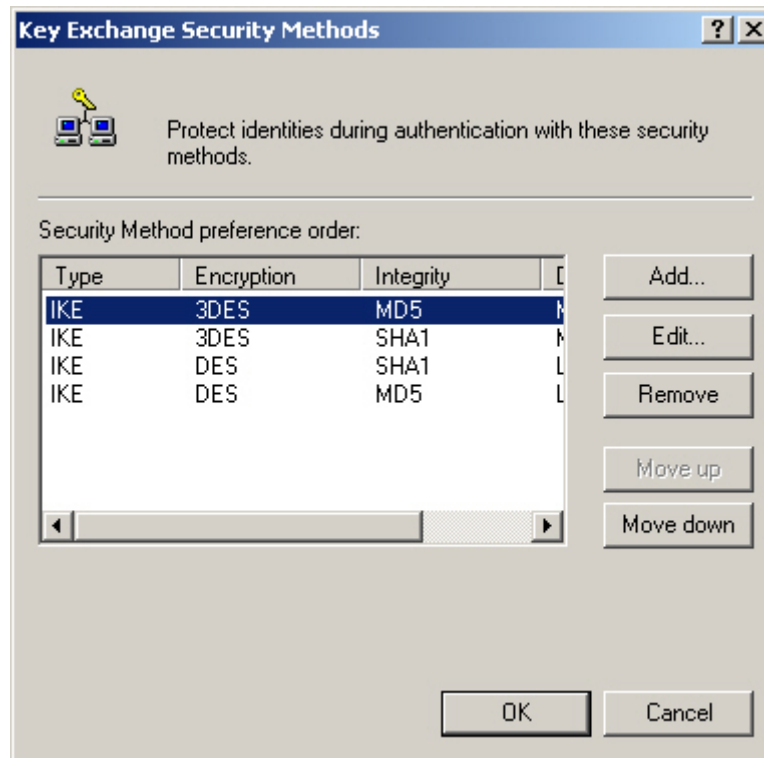
**STEP 56 .** Select **Master Key Perfect Forward Secrecy**, click **Methods**.



**Key Exchange settings**

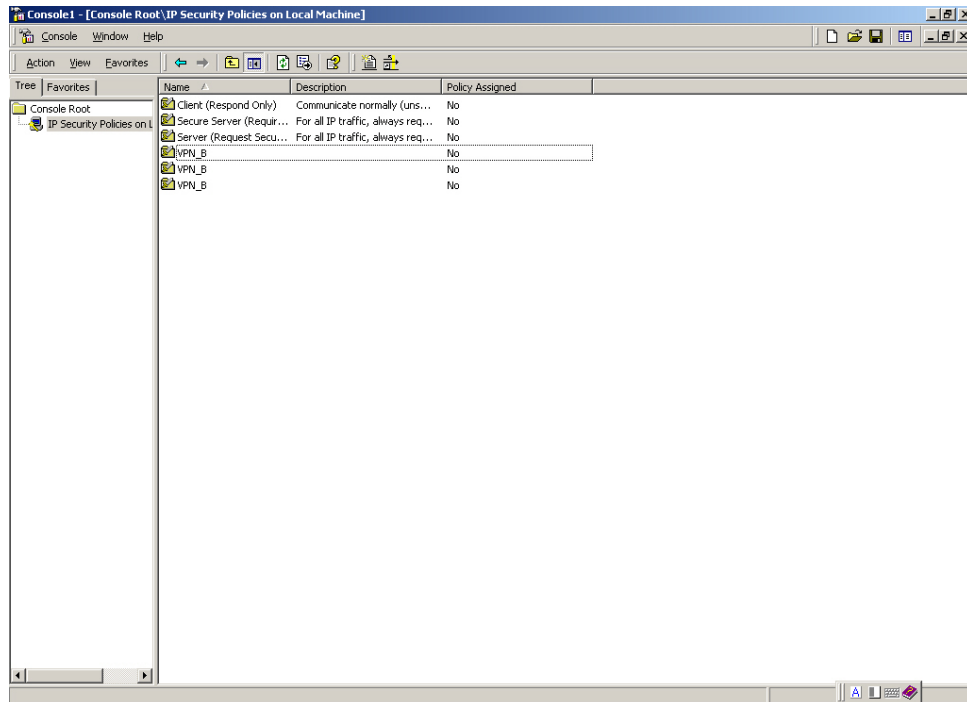


**STEP 57** . Click **Move up** or **Move down** to arrange IKE / 3DES / MD5 / to the Top, and click **OK**.



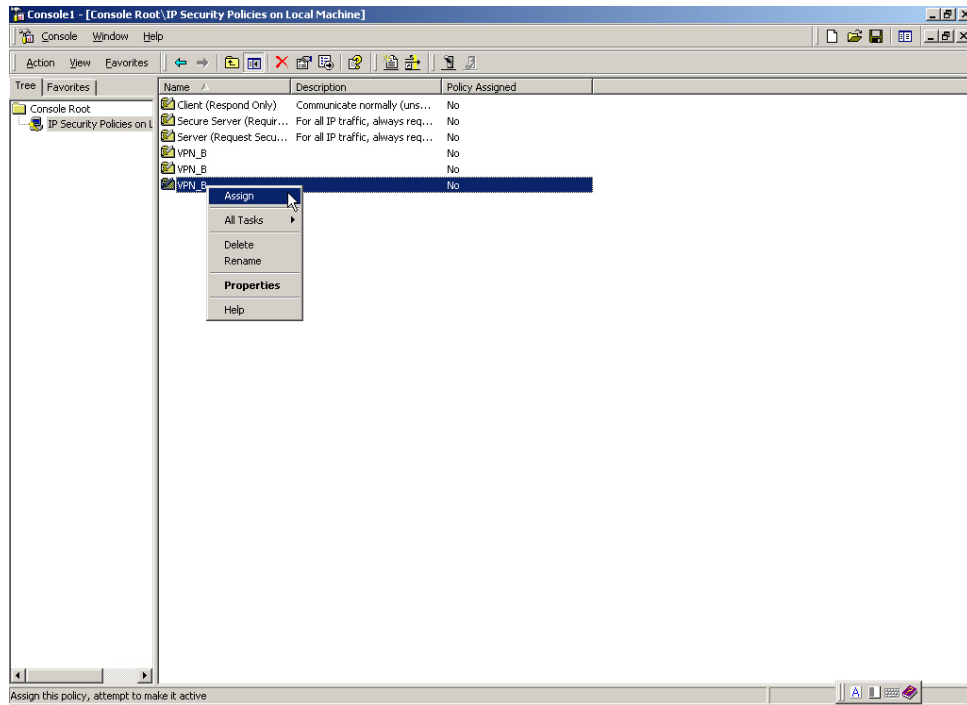
**To arrange the Security Methods**

**STEP 58 .** Complete all the Windows 2000 VPN settings.



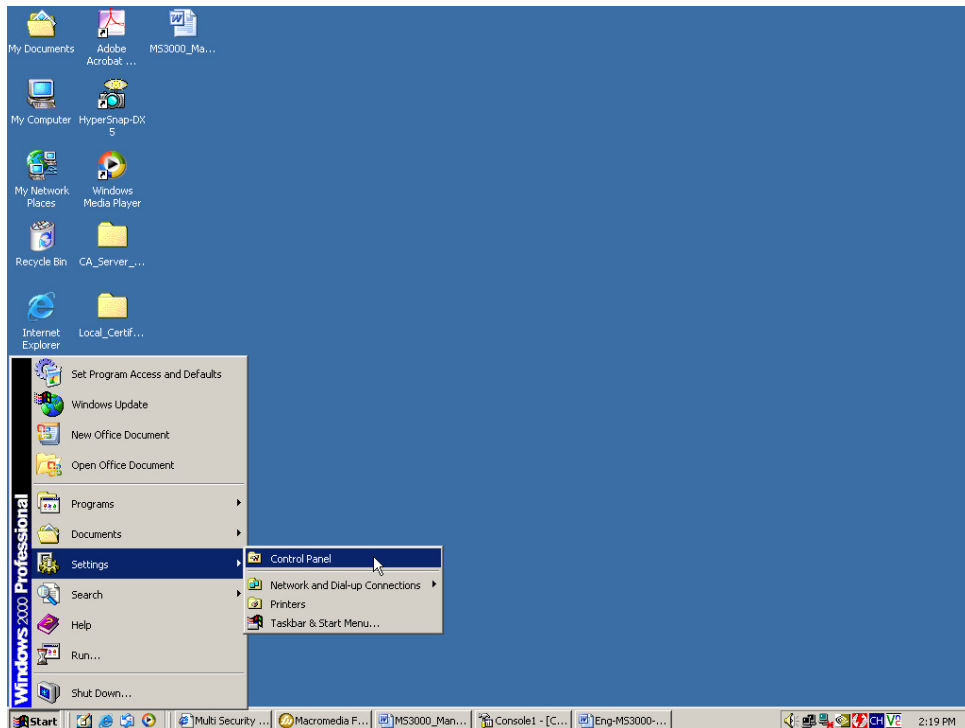
**Complete all the Windows 2000 IPsec VPN settings**

**STEP 59 .** Right click on VPN\_B, select **Assign**.



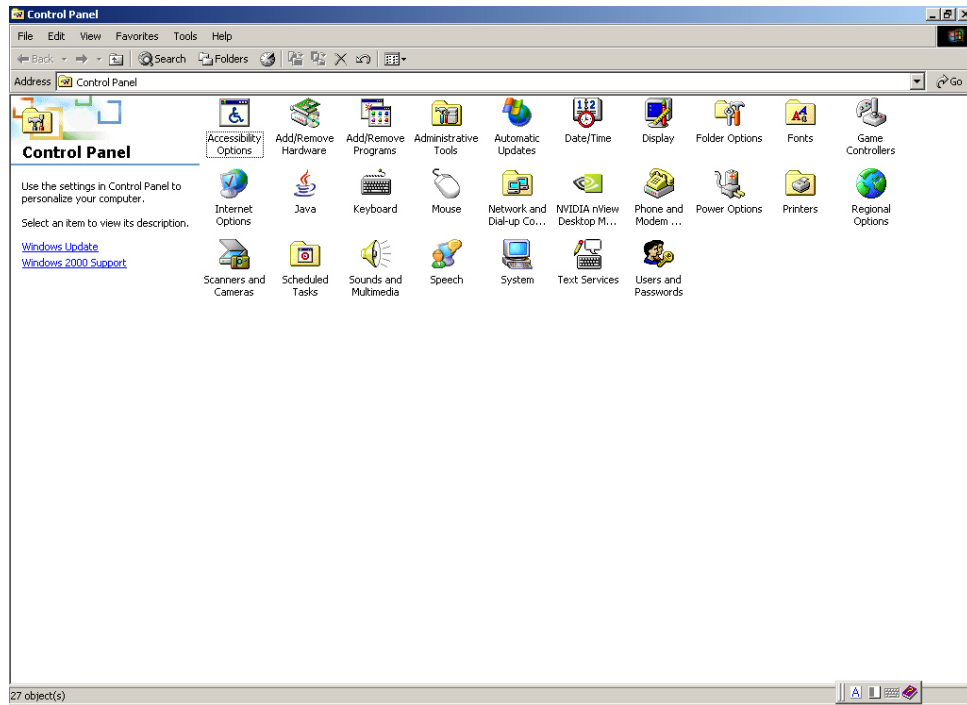
**To assign the VPN\_B Security Rules**

**STEP 60 .** We need to restart the IPsec Service. Click **Start → Setting → Control Panel**.



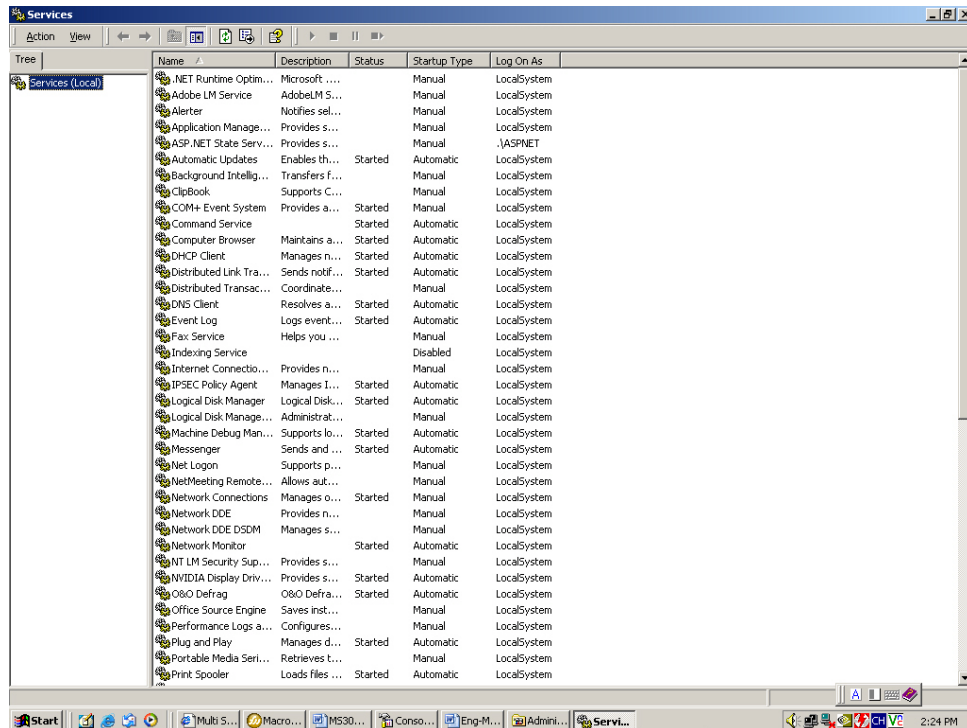
**Enter the Control Panel**

**STEP 61 .** In **Control Panel**, double click **Administrative Tools** icon.



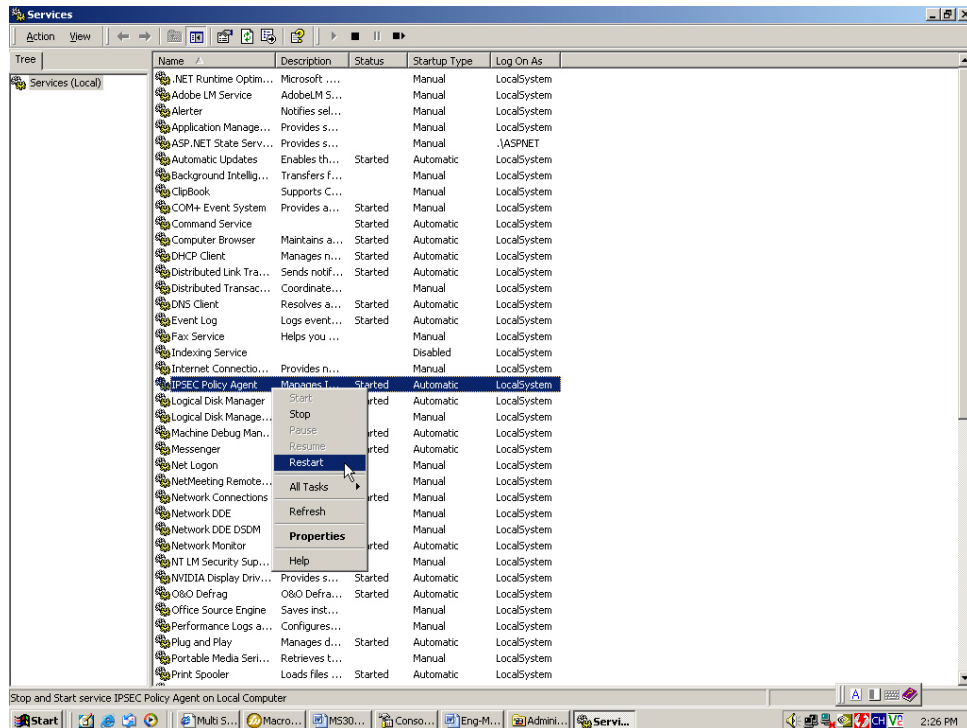
**Enter the Administrative Tools**

**STEP 62 . In Administrative Tools, double click Services icon.**



**Enter the Services**

**STEP 63 .** In **Services**, right click on **IPsec Policy Agent**, select **Restart**.



### Restart IPsec Policy Agent

**STEP 64 .** Complete all the settings.

### 6.9.3 Example.3

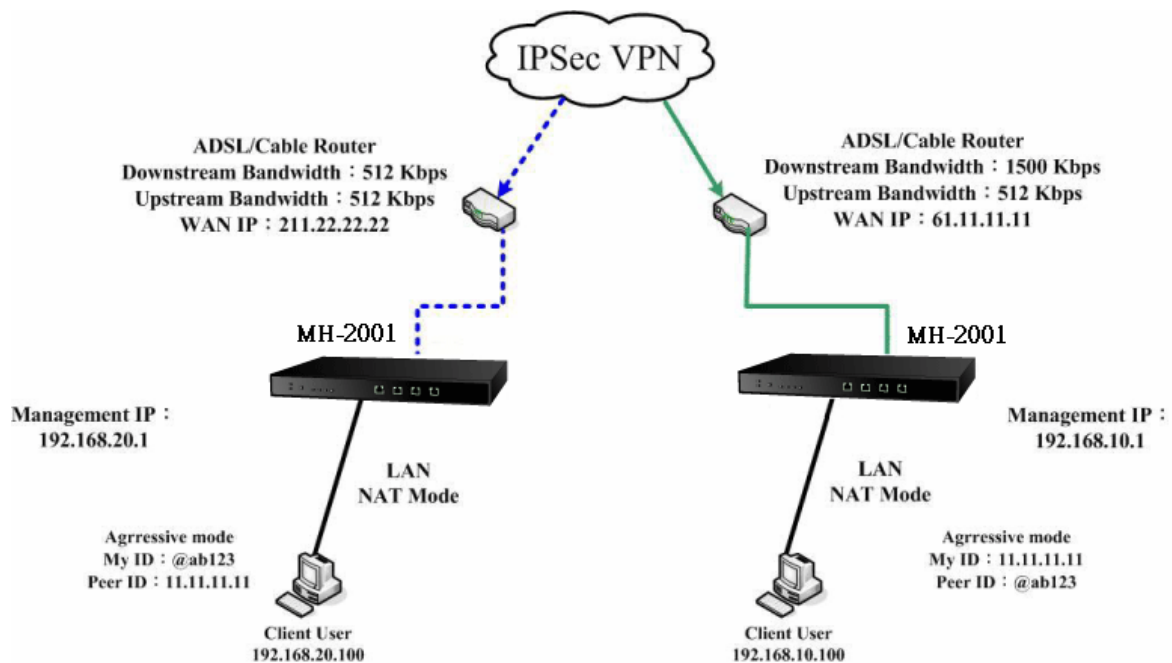
The way to set the IPSec VPN connection between two MH-2001 appliances.  
(Aggressive mode) (The IPSec algorithm, 3DES encryption, MD5 authentication).

#### The Deployment

Company A : **WAN IP** 61.11.11.11  
**LAN IP** 192.168.10.X  
 Company B : **WAN IP** 211.22.22.22  
**LAN IP** 192.168.20.X

We use two MH-2001 devices to be the platform. Assume that A Company 192.168.10.100 want to build the **VPN** to B Company 192.168.20.100, in order to download the shared documents. (Aggressive mode)

#### TEST Environment



The IPSec VPN aggressive mode deployment



The A Company's default gateway is the MH-2001 LAN IP 192.168.10.1. Make the following settings:

**STEP 1** . Enter A Company's MH-2001 default IP Address 192.168.10.1. In **Policy Object → VPN → IP Sec Autokey → New Entry**.

i	Name	WAN	Gateway IP	IPSec Algorithm	Configure
---	------	-----	------------	-----------------	-----------

[New Entry](#)

### IPSec Autokey

**STEP 2** . In **IPSec Autokey**, enter VPN\_A in the VPN **Name**. In **WAN interface**, select **WAN 1**, which the A Company use it to build the VPN.

Necessary Item	
Name	VPN_A (Max. 12 characters)
WAN interface	<input checked="" type="radio"/> WAN 1 <input type="radio"/> WAN 2

### The IPSec VPN name and WAN interface setting

**STEP 3** . In To Destination, select Remote Gateway – Fixed IP or Domain Name. Enter the Remote IP address to link to B Company.

To Destination	
<input checked="" type="radio"/> Remote Gateway -- Fixed IP or Domain Name	211.22.22.22 (Max. 99 characters)
<input type="radio"/> Remote Gateway or Client -- Dynamic IP	

### The IPSec To Destination setting

**STEP 4** . In **Authentication Method**, select **Preshare**, enter the **Preshared Key**. (the maximum Preshared Key is 100 bytes).

Authentication Method	Preshare ▼
Preshared Key	123456789 (Max. 103 characters)

### The IPSec Authentication Method setting

**STEP 5 .** In **Encapsulation**, select **ISAKMP Algorithm**, to select the needed algorithm. In **ENC Algorithm** (3DES/DES/AES), select **3DES**. In **AUTH Algorithm** (MD5/SHA1), select **SHA1**. In **Group** (GROUP 1, 2, 5), select **Group 2**, the both sides need to choose the same group.

Encapsulation	
ISAKMP Algorithm	
ENC Algorithm	3DES ▼
AUTH Algorithm	SHA1 ▼
Group	GROUP 2 ▼

**The IPSec Encapsulation setting**

**STEP 6 .** In **IPSec Algorithm**, select **Data Encryption + Authentication** or **Authentication Only**. In **ENC Algorithm** (3DES/DES/AES/NULL) select 3DES. In **AUTH Algorithm** (MD5/SHA1), select MD5. To assure the Authentication Method.

IPSec Algorithm	
<input checked="" type="radio"/> Data Encryption + Authentication	
ENC Algorithm	3DES ▼
AUTH Algorithm	MD5 ▼
<input type="radio"/> Authentication Only	

**The IPSec Algorithm setting**

**STEP 7 . In Perfect Forward Secrecy** ( NO-PFS/ GROUP 1, 2, 5 ) , select GROUP 1. In **ISAKMP Lifetime**, enter 3600 seconds, and the **IPSec Lifetime**, enter 28800 seconds.

Perfect Forward Secrecy	GROUP 1 ▼	
ISAKMP Lifetime	3600	Seconds ( Range: 1200 - 86400 )
IPSec Lifetime	28800	Seconds ( Range: 1200 - 86400 )

#### The IPSec Perfect Forward Secrecy setting

**STEP 8 . In Mode**, select Aggressive mode.

In **My ID**, select not to enter.

If the both sides need to enter the My ID / Peer ID, then the MIS engineer must enter the different IP address. For example, 11.11.11.11 or 22.22.22.22. If the MIS engineer want to enter the Authentication number or alphabet, then he must add the @ in front of the number or alphabet. For example, @123a 、 @abcd1.

Mode	<input type="radio"/> Main mode <input checked="" type="radio"/> Aggressive mode	
My ID	11.11.11.11	(Max. 39 characters)
Peer ID	@abc123	(Max. 39 characters)

#### The IPSec Aggressive mode setting

**STEP 9 . Complete the IPSec Autokey Setting.**

i	Name	WAN	Gateway IP	IPSec Algorithm	Configure
--	VPN_A	WAN1	211.22.22.22	3DES / MD5	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

#### Complete the IPSec Autokey setting

**STEP 10 . In VPN → Tunnel add the following settings :**

- **Name**, enter the Tunnel name.
- **From Source**, select LAN.
- **From Source Subnet / Mask**, enter the LAN address (A Company) 192.168.10.0 and Mask 255.255.255.0.
- **To Destination**, select To Destination Subnet / Mask.
- Enter the destination LAN IP address (B Company) 192.168.20.0 and mask 255.255.255.0.
- **IPSec / PPTP Setting**, select VPN\_A.
- Select **show remote Network Neighborhood**.
- Click **OK**.

New Entry Tunnel	
Name	IPsec_VPN_Tunnel (Max. 16 characters)
From Source	<input checked="" type="radio"/> LAN <input type="radio"/> DMZ
From Source Subnet / Mask	192.168.10.0 / 255.255.255.0
To Destination	<input checked="" type="radio"/> To Destination Subnet / Mask <input type="radio"/> Remote Client
	192.168.20.0 / 255.255.255.0
IPSec / PPTP Setting	VPN_A
Keep alive IP :	
<input checked="" type="checkbox"/> Show remote Network Neighborhood	

### Add the VPN Tunnel setting

i	Name	Source Subnet	Destination Subnet	IPSec / PPTP	Configure
	IPsec_VPN_Tu...	192.168.10.0	192.168.20.0	VPN_A	<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>

### Complete the VPN Tunnel setting

**STEP 11 . In Policy → Outgoing , add the following settings :**

■**Tunnel**, select IPsec\_VPN\_Tunnel.

■Click **OK**.

Comment :  (Max. 32 characters)

Add New Policy	
Source Address	Inside_Any ▾
Destination Address	Outside_Any ▾
Service	ANY ▾
Schedule	None ▾
Authentication User	None ▾
<b>Tunnel</b>	<b>IPsec_VPN_Tunnel ▾</b>
Action, WAN Port	PERMIT ALL ▾
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> Enable
IM / P2P Blocking	None ▾
QoS	None ▾
MAX. Bandwidth Per Source IP	Downstream <input type="text" value="0"/> Kbps Upstream <input type="text" value="0"/> Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )

**Set the outgoing policy included the VPN Tunnel**

Source	Destination	Service	Action	Option					Configure			Move
Inside_Any	Outside_Any	ANY	VPN						Modify	Remove	Pause	To 1 ▾

**Complete the outgoing policy setting included the VPN Tunnel**

**STEP 12 . In Policy → Incoming , add the following settings :**

■ **Tunnel**, select IPsec\_VPN\_Tunnel.

■ Click **OK**.

Comment :  (Max. 32 characters)

Add New Policy	
Source Address	Outside_Any ▾
Destination Address	Inside_Any ▾
Service	ANY ▾
Schedule	None ▾
Tunnel	IPsec_VPN_Tunnel ▾
Action	PERMIT ▾
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
QoS	None ▾
MAX. Bandwidth Per Source IP	Downstream <input type="text" value="0"/> Kbps Upstream <input type="text" value="0"/> Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
NAT	<input type="checkbox"/> Enable

**Set the incoming policy included the VPN Tunnel**

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Inside_Any(Routing)	ANY	VPN		<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To <input type="text" value="1"/> ▾

**Complete the incoming policy setting included the VPN Tunnel**

The B Company's default gateway is the MH-2001's LAN IP 192.168.20.1. Add the following settings :

**STEP 13 .** Enter B Company's default IP address 192.168.20.1. Click **VPN → IPsec Autokey**, click **New Entry**.

i	Name	WAN	Gateway IP	IPsec Algorithm	Configure
---	------	-----	------------	-----------------	-----------

[New Entry](#)

### IPsec Autokey

**STEP 14 .** In **IPsec Autokey**, enter VPN\_B in **Name**. In **WAN interface**, select WAN 1, in order to build the B Company's VPN.

Necessary Item	
Name	<input type="text" value="VPN_B"/> (Max. 12 characters)
WAN interface	<input checked="" type="radio"/> WAN 1 <input type="radio"/> WAN 2

### Set the IPsec VPN name and WAN interface setting

**STEP 15 .** In **To Destination**, select **Remote Gateway --Fixed IP or Domain Name**, enter the Remote IP address to link to A Company.

To Destination	
<input checked="" type="radio"/> Remote Gateway -- Fixed IP or Domain Name	<input type="text" value="61.11.11.11"/> (Max. 99 characters)
<input type="radio"/> Remote Gateway or Client -- Dynamic IP	

### The IPsec To Destination IP setting

**STEP 16 .** In **Authentication Method**, select **Preshare**, enter the Preshared Key. (The maximum Preshared Key is 100 bytes).

Authentication Method	Preshare ▼
Preshared Key	123456789 (Max. 103 characters)

### The IPSec Authentication Setting

**STEP 17 .** In **Encapsulation**, select ISAKMP Algorithm, choose the needed algorithm. In **ENC Algorithm** (3DES/DES/AES), select **3DES**. In **AUTH Algorithm** (MD5/SHA1), select **SHA1**. In **Group** (GROUP 1, 2, 5), select **GROUP 2**. The both sides need to select the same group.

Encapsulation	
ISAKMP Algorithm	
ENC Algorithm	3DES ▼
AUTH Algorithm	SHA1 ▼
Group	GROUP 2 ▼

### The IPSec Encapsulation setting

**STEP 18 .** In **IPSec Algorithm**, select **Data Encryption + Authentication** or **Authentication Only**. In **ENC Algorithm** (3DES/DES/AES/NULL), select **3DES**. In **AUTH Algorithm** (MD5/SHA1), select **MD5**, to assure the authentication methods.

IPSec Algorithm	
<input checked="" type="radio"/> Data Encryption + Authentication	
ENC Algorithm	3DES ▼
AUTH Algorithm	MD5 ▼
<input type="radio"/> Authentication Only	

### The IPSec Algorithm setting



**STEP 19 .** In **Perfect Forward Secrecy** ( NO-PFS/ GROUP 1,2,5 ) , select **GROUP 1**. In **ISAKMP Lifetime**, enter **3600** seconds. In **IPSec Lifetime**, enter **28800** seconds.

Perfect Forward Secrecy	GROUP 1 ▼	
ISAKMP Lifetime	3600	Seconds ( Range: 1200 - 86400 )
IPSec Lifetime	28800	Seconds ( Range: 1200 - 86400 )

### The IPSec Perfect Forward Secrecy setting

**STEP 20 .** In **My ID**, select Aggressive mode.

In **My ID / Peer ID**, the MIS engineer can select not to enter.

In **My ID / Peer ID**, if the MIS engineers want to enter the IP, then it must be the two different IP address. For example, 11.11.11.11, 22.22.22.22. If the MIS engineers want to add the number or alphabet to access the authentication, then he must add the @ in front of the alphabet or the numbers . For example, @123a, @abcd1.

Mode	<input type="radio"/> Main mode <input checked="" type="radio"/> Aggressive mode	
My ID	@abc123	(Max. 39 characters)
Peer ID	11.11.11.11	(Max. 39 characters)

### The IPSec Aggressive mode setting

**STEP 21 .** Complete the IPSec Autokey settings

i	Name	WAN	Gateway IP	IPSec Algorithm	Configure
--	VPN_B	WAN1	61.11.11.11	3DES / MD5	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

### Complete the IPSec Autokey setting

**STEP 22 . In VPN → Tunnel→ New Entry, add the following settings :**

- **Name**, enter the Tunnel Name.
- **From Source**, select LAN.
- **From Source Subnet / Mask**, enter the LAN IP address (B Company) 192.168.20.0 and mask 255.255.255.0.
- **To Destination**, select To Destination Subnet / Mask.
- Enter To Destination LAN IP (A Company) 192.168.10.0 and mask 255.255.255.0.
- **IPSec / PPTP Setting**, select VPN\_B.
- Select **Show remote Network Neighborhood**.
- Click **OK**.

New Entry Tunnel	
Name	IPsec_VPN_Tunnel (Max. 16 characters)
From Source	<input checked="" type="radio"/> LAN <input type="radio"/> DMZ
From Source Subnet / Mask	192.168.20.0 / 255.255.255.0
To Destination	<input checked="" type="radio"/> To Destination Subnet / Mask <input type="radio"/> Remote Client
	192.168.10.0 / 255.255.255.0
IPSec / PPTP Setting	VPN_B ▼
Keep alive IP :	
<input checked="" type="checkbox"/> Show remote Network Neighborhood	

#### Add the VPN Tunnel setting

i	Name	Source Subnet	Destination Subnet	IPSec / PPTP	Configure
	IPsec_VPN_Tu...	192.168.20.0	192.168.10.0	VPN_B	<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>

Complete to add the VPN Tunnel setting

**STEP 23 . In Policy → Outgoing , add the following settings :**

■**Tunnel**, select IPsec\_VPN\_Tunnel.

■Click **OK**.

Comment :  (Max. 32 characters)

Add New Policy	
Source Address	Inside_Any ▾
Destination Address	Outside_Any ▾
Service	ANY ▾
Schedule	None ▾
Authentication User	None ▾
<b>Tunnel</b>	<b>IPsec_VPN_Tunnel ▾</b>
Action, WAN Port	PERMIT ALL ▾
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> Enable
IM / P2P Blocking	None ▾
QoS	None ▾
MAX. Bandwidth Per Source IP	Downstream <input type="text" value="0"/> Kbps Upstream <input type="text" value="0"/> Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )

**Set the outgoing policy included the VPN Tunnel**

Source	Destination	Service	Action	Option					Configure			Move
Inside_Any	Outside_Any	ANY	VPN						<input type="button" value="Modify"/>	<input type="button" value="Remove"/>	<input type="button" value="Pause"/>	To 1 ▾

**Complete the outgoing policy setting included the VPN Tunnel**

**STEP 24 . In Policy → Incoming, add the following settings :**

■ **Tunnel**, select IPsec\_VPN\_Tunnel.

■ Click **OK**.

Comment :  (Max. 32 characters)

Add New Policy	
Source Address	Outside_Any ▾
Destination Address	Inside_Any ▾
Service	ANY ▾
Schedule	None ▾
Tunnel	IPsec_VPN_Tunnel ▾
Action	PERMIT ▾
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
QoS	None ▾
MAX. Bandwidth Per Source IP	Downstream <input type="text" value="0"/> Kbps Upstream <input type="text" value="0"/> Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
NAT	<input type="checkbox"/> Enable

**Set the incoming policy included the VPN Tunnel**

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Inside_Any(Routing)	ANY	VPN		<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To <input type="text" value="1"/> ▾

**Complete the incoming policy setting included the VPN Tunnel**

**STEP 25 . Complete the IPsec VPN aggressive mode settings.**

### 6.9.4 Example.4

The way to set the IPSec VPN connection between two MH-2001 appliances. (The GRE packets) (The IPSec algorithm, 3DES encryption, MD5 authentication)

#### The Deployment

Company A :

**WAN1 IP :** 61.11.11.11

**WAN2 IP :** 61.22.22.22

**LAN IP :** 192.168.10.X

Company B :

**WAN1 IP :** 211.22.22.22

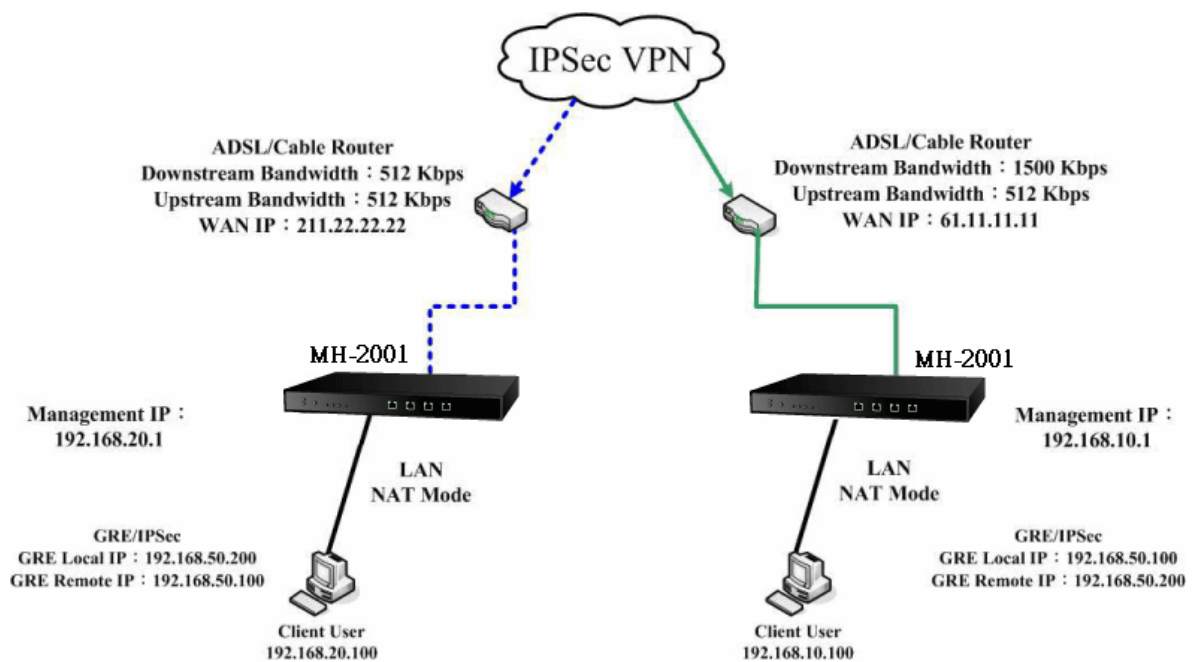
**WAN2 IP :** 211.33.33.33

**LAN IP :** 192.168.20.X

The A and B Company applied two local certificates from different CA Server.

We use two MH-2001 devices to be the platform. Assume that the A Company 192.168.10.100 want to build up the VPN to B Company 192.168.20.100 , in order to download the shared documents. (Use the GRE/IPSec packets algorithm)

#### TEST Environment



The IPSec VPN GRE/IPSec deployment

The A Company's default gateway is the LAN IP 192.168.10.1 in MH-2001.

**STEP 1** . Enter the A Company's default IP address 192.168.10.1. In **VPN → IPsec Autokey**, click **New Entry**.

i	Name	WAN	Gateway IP	IPsec Algorithm	Configure
<div>New Entry</div> <div>IPsec Autokey</div>					

**STEP 2** . In **IPsec Autokey → Name**, enter VPN\_A. In **WAN interface**, select WAN 1.

Necessary Item	
Name	VPN_A (Max. 12 characters)
WAN interface	<input checked="" type="radio"/> WAN 1 <input type="radio"/> WAN 2

#### The IPsec VPN name and WAN interface setting

**STEP 3** . In **To Destination**, select **Remote Gateway—Fixed IP or Domain Name**, enter the remote (WAN 1) IP address to link to B Company.

To Destination	
<input checked="" type="radio"/> Remote Gateway -- Fixed IP or Domain Name	211.22.22.22 (Max. 99 characters)
<input type="radio"/> Remote Gateway or Client -- Dynamic IP	

#### The IPsec To destination setting

**STEP 4** . In **Authentication Method**, select **Preshare**, enter the Preshared Key. (The maximum Preshared Key is 100 bytes).

Authentication Method	Preshare ▼
Preshared Key	123456789 (Max. 103 characters)

#### The IPsec Authentication Method setting

**STEP 5** . In **Encapsulation**, select ISAKMP algorithm, to select the needed algorithm. In **ENC Algorithm** (3DES/DES/AES), select **3DES**. In **AUTH Algorithm** (MD5/SHA1), select **MD5**. In **Group** (GROUP 1, 2, 5), select **GROUP 1**. The both sides need to select the same group.

Encapsulation	
ISAKMP Algorithm	
ENC Algorithm	3DES ▼
AUTH Algorithm	MD5 ▼
Group	GROUP 1 ▼

#### The IPSec Encapsulation setting

**STEP 6 . In IPSec Algorithm**, select Data Encryption + Authentication or Authentication Only. In **ENC Algorithm** (3DES/DES/AES/NULL), select **3DES**. In **AUTH Algorithm** (MD5/SHA1), select **MD5**, to assure the data authentication method.

IPSec Algorithm	
<input checked="" type="radio"/> Data Encryption + Authentication	
ENC Algorithm	3DES ▼
AUTH Algorithm	MD5 ▼
<input type="radio"/> Authentication Only	

#### The IPSec Algorithm setting

**STEP 7 .** In **Perfect Forward Secrecy** (NO-PFS/ GROUP 1, 2, 5), select **GROUP 1**. In **ISKMP Lifetime**, enter **3600** seconds. In **IPSec Lifetime**, enter **28800** seconds. In **Mode**, select main mode.

Perfect Forward Secrecy	GROUP 1 ▼	
ISAKMP Lifetime	3600	Seconds ( Range: 1200 - 86400 )
IPSec Lifetime	28800	Seconds ( Range: 1200 - 86400 )
Mode	<input checked="" type="radio"/> Main mode <input type="radio"/> Aggressive mode	

#### The IPSec Perfect Forward Secrecy setting

**STEP 8 .** In **GRE/IPSec → GRE Local IP**, enter 192.168.50.100. In **GRE Remote IP**, enter 192.168.50.200  
(The local IP and remote IP must be in the same subnet of C class).

GRE/IPSec			
GRE Local IP	192.168.50.100		
GRE Remote IP	192.168.50.200		
<input type="checkbox"/> Manual Connect			
Dead Peer Detection	delay	5	Second
	Timeout	5	Second (delay Range: 0 - 10, 0: means disable; Timeout Range: 1 - 100)

#### The GRE/IPSec setting

**STEP 9 .** Complete the VPN\_A setting in IPSec Autokey.

i	Name	WAN	Gateway IP	IPSec Algorithm	Configure
--	VPN_A	WAN1	211.22.22.22	3DES / MD5	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

#### Complete the IPSec Autokey setting



**STEP 10 . In VPN → Tunnel , add the following settings :**

- **Name**, enter the Tunnel Name.
- **From Source**, select LAN.
- In **From Source Subnet / Mask**, enter the LAN source IP (A Company) 192.168.10.0 and mask 255.255.255.0.
- In **To Destination**, select To Destination Subnet / Mask.
- In **To Destination Subnet / Mask**, enter the LAN IP address 192.168.20.0 (B Company) and mask 255.255.255.0.
- In **IPSec / PPTP Setting**, select VPN\_A.
- Select **Show remote Network Neighborhood**.
- Click **OK**.

New Entry Tunnel	
Name	IPsec_VPN_Tunnel (Max. 16 characters)
From Source	<input checked="" type="radio"/> LAN <input type="radio"/> DMZ
From Source Subnet / Mask	192.168.10.0 / 255.255.255.0
To Destination	<input checked="" type="radio"/> To Destination Subnet / Mask <input type="radio"/> Remote Client
	192.168.20.0 / 255.255.255.0
IPSec / PPTP Setting	VPN_A ▼
Keep alive IP :	
<input checked="" type="checkbox"/> Show remote Network Neighborhood	

**To add the VPN Tunnel setting**

i	Name	Source Subnet	Destination Subnet	IPSec / PPTP	Configure
	IPsec_VPN_Tu...	192.168.10.0	192.168.20.0	VPN_A	<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>

**Complete to add the VPN Tunnel setting**

**STEP 11 . In Policy → Outgoing, add the following settings :**

- **Tunnel**, select IPsec\_VPN\_Tunnel.
- Click **OK**.

Comment :  (Max. 32 characters)

Add New Policy	
Source Address	Inside_Any ▾
Destination Address	Outside_Any ▾
Service	ANY ▾
Schedule	None ▾
Authentication User	None ▾
<b>Tunnel</b>	<b>IPsec_VPN_Tunnel ▾</b>
Action, WAN Port	PERMIT ALL ▾
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> Enable
IM / P2P Blocking	None ▾
QoS	None ▾
MAX. Bandwidth Per Source IP	Downstream <input type="text" value="0"/> Kbps Upstream <input type="text" value="0"/> Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )

**Set the outgoing policy setting included the VPN Tunnel**

Source	Destination	Service	Action	Option					Configure			Move
Inside_Any	Outside_Any	ANY	VPN						<input type="button" value="Modify"/>	<input type="button" value="Remove"/>	<input type="button" value="Pause"/>	To 1 ▾

**Complete the outgoing policy setting included the VPN Tunnel**

**STEP 12 . In Policy → Incoming , add the following settings :**

- **Tunnel**, select IPsec\_VPN\_Tunnel.
- Click **OK**.

Comment :  (Max. 32 characters)

Add New Policy	
Source Address	Outside_Any ▾
Destination Address	Inside_Any ▾
Service	ANY ▾
Schedule	None ▾
Tunnel	IPsec_VPN_Tunnel ▾
Action	PERMIT ▾
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
QoS	None ▾
MAX. Bandwidth Per Source IP	Downstream <input type="text" value="0"/> Kbps Upstream <input type="text" value="0"/> Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
NAT	<input type="checkbox"/> Enable

**Set the incoming policy setting included the VPN Tunnel**

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Inside_Any(Routing)	ANY	VPN		<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To <input type="text" value="1"/> ▾

**Complete the incoming policy setting included the VPN Tunnel**

The B Company's default gateway is the LAN IP 192.168.20.1 of MH-2001. Add the following settings :

**STEP 13 .** Enter the B Company's default IP address 192.168.20.1. In **VPN → IPsec Autokey → New Entry**.

i	Name	WAN	Gateway IP	IPsec Algorithm	Configure
<div>New Entry</div> <div>IPsec Autokey</div>					

**STEP 14 .** In **IPsec Autokey → Name**, enter VPN\_B. In **WAN interface**, select WAN 1, which the B Company use it to build the VPN.

Necessary Item	
Name	<input type="text" value="VPN_B"/> (Max. 12 characters)
WAN interface	<input checked="" type="radio"/> WAN 1 <input type="radio"/> WAN 2

To set the IPsec VPN name and WAN interface setting

**STEP 15 .** In **To Destination**, select **Remote Gateway – Fixed IP or Domain Name**, enter the remote (WAN 1) IP address, to link to A Company.

To Destination	
<input checked="" type="radio"/> Remote Gateway -- Fixed IP or Domain Name	<input type="text" value="61.11.11.11"/> (Max. 99 characters)
<input type="radio"/> Remote Gateway or Client -- Dynamic IP	

The IPsec to Destination setting

**STEP 16 .** In **Authentication Method**, select **Preshare**, enter the Preshared Key. (The maximum Preshared Key is 100 bytes).

Authentication Method	Preshare ▼
Preshared Key	123456789 (Max. 103 characters)

#### The IPSec Authentication Method setting

**STEP 17 .** In **Encapsulation**, select ISAKMP algorithm, to choose the needed algorithm. In **ENC Algorithm** (3DES/DES/AES), select **3DES**. In **AUTH Algorithm** (MD5/SHA1), select **MD5**. In **Group** (GROUP 1, 2, 5), select **GROUP 1**. The both sides need to choose the same group.

Encapsulation	
ISAKMP Algorithm	
ENC Algorithm	3DES ▼
AUTH Algorithm	MD5 ▼
Group	GROUP 1 ▼

#### The IPSec Encapsulation setting

**STEP 18 .** In **IPSec Algorithm**, select **Data Encryption + Authentication** or **Authentication Only**. In **ENC Algorithm** (3DES/DES/AES/NULL), select **3DES**. In **AUTH Algorithm** (MD5/SHA1), select **MD5**, to assure the data authentication method.

IPSec Algorithm	
<input checked="" type="radio"/> Data Encryption + Authentication	
ENC Algorithm	3DES ▼
AUTH Algorithm	MD5 ▼
<input type="radio"/> Authentication Only	

#### The IPSec Algorithm setting

**STEP 19 .** In **Perfect Forward Secrecy** (NO-PFS/ GROUP 1, 2, 5), select **GROUP 1**. In **ISAKMP Lifetime**, enter **3600** seconds. In **IPSec Lifetime**, enter **28800** seconds. In **Mode**, select main mode.

Perfect Forward Secrecy	GROUP 1 ▼	
ISAKMP Lifetime	3600	Seconds ( Range: 1200 - 86400 )
IPSec Lifetime	28800	Seconds ( Range: 1200 - 86400 )
Mode	<input checked="" type="radio"/> Main mode <input type="radio"/> Aggressive mode	

#### The IPSec Perfect Forward Secrecy setting

**STEP 20 .** In **GRE/IPSec → GRE Local IP**, enter 192.168.50.200. In **GRE Remote IP**, enter 192.168.50.100.  
(The local IP and remote IP must be in the same C class segment).

GRE/IPSec			
GRE Local IP	192.168.50.200		
GRE Remote IP	192.168.50.100		
<input type="checkbox"/> Manual Connect			
Dead Peer Detection	delay	5	Second
	Timeout	5	Second (delay Range: 0 - 10, 0: means disable; Timeout Range: 1 - 100)

#### The GRE/IPSec setting

**STEP 21 .** Complete the IPSec Autokey VPN\_B setting.

i	Name	WAN	Gateway IP	IPSec Algorithm	Configure
--	VPN_B	WAN1	61.11.11.11	3DES / MD5	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

#### Complete to set the IPSec Autokey setting

**STEP 22 . In VPN → Tunnel , add the following settings :**

- In **Name**, enter the Tunnel name.
- **From Source**, select LAN.
- In **From Source Subnet/ Mask**, enter B Company's LAN source IP 192.168.20.0 and mask 255.255.255.0.
- In **To Destination**, select To Destination Subnet / Mask.
- In **To Destination Subnet / Mask**, enter A Company's LAN IP 192.168.10.0 and mask 255.255.255.0.
- In **IPSec / PPTP Setting**, select VPN\_B.
- Select **Show remote Network Neighborhood**.
- Click **OK**.

**New Entry Tunnel**

Name	IPsec_VPN_Tunnel (Max. 16 characters)
From Source	<input checked="" type="radio"/> LAN <input type="radio"/> DMZ
From Source Subnet / Mask	192.168.20.0 / 255.255.255.0
To Destination	<input checked="" type="radio"/> To Destination Subnet / Mask <input type="radio"/> Remote Client
	192.168.10.0 / 255.255.255.0
IPSec / PPTP Setting	VPN_B
Keep alive IP :	
<input checked="" type="checkbox"/> Show remote Network Neighborhood	

OK Cancel

**To add the VPN Tunnel setting**

i	Name	Source Subnet	Destination Subnet	IPSec / PPTP	Configure
	IPsec_VPN_Tu...	192.168.20.0	192.168.10.0	VPN_B	<div>Modify</div> <div>Remove</div> <div>Pause</div>

**New Entry**

**Complete to add the VPN Tunnel setting**

**STEP 23 . In Policy →Outgoing , add the following settings :**

- **Tunnel**, select IPsec\_VPN\_Tunnel.
- Click **OK**.

Comment :  (Max. 32 characters)

Add New Policy	
Source Address	Inside_Any ▾
Destination Address	Outside_Any ▾
Service	ANY ▾
Schedule	None ▾
Authentication User	None ▾
<b>Tunnel</b>	<b>IPsec_VPN_Tunnel ▾</b>
Action, WAN Port	PERMIT ALL ▾
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> Enable
IM / P2P Blocking	None ▾
QoS	None ▾
MAX. Bandwidth Per Source IP	Downstream <input type="text" value="0"/> Kbps Upstream <input type="text" value="0"/> Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )

**To set the outgoing policy included the VPN Tunnel**

Source	Destination	Service	Action	Option					Configure			Move
Inside_Any	Outside_Any	ANY	VPN						<input type="button" value="Modify"/>	<input type="button" value="Remove"/>	<input type="button" value="Pause"/>	To 1 ▾

**Complete to set the outgoing policy included the VPN Tunnel**



**STEP 24 .** In **Policy → Incoming**, add the following settings :

- **Tunnel**, select IPsec\_VPN\_Tunnel.
- Click **OK**.

Comment :  (Max. 32 characters)

Add New Policy	
Source Address	Outside_Any ▾
Destination Address	Inside_Any ▾
Service	ANY ▾
Schedule	None ▾
Tunnel	IPsec_VPN_Tunnel ▾
Action	PERMIT ▾
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
QoS	None ▾
MAX. Bandwidth Per Source IP	Downstream <input type="text" value="0"/> Kbps Upstream <input type="text" value="0"/> Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
NAT	<input type="checkbox"/> Enable

**To set the incoming policy included the VPN Tunnel**

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Inside_Any(Routing)	ANY	VPN		<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To <input type="text" value="1"/> ▾

**Complete to set the incoming policy included the VPN Tunnel**

**STEP 25 .** Complete the IPsec VPN GRE/IPsec settings.

### 6.9.5 Example.5

#### Setting PPTP VPN connection between two MH-2001

##### The Deployment

Company A :

**WAN1 IP :** 61.11.11.11

**LAN IP :** 192.168.10.X

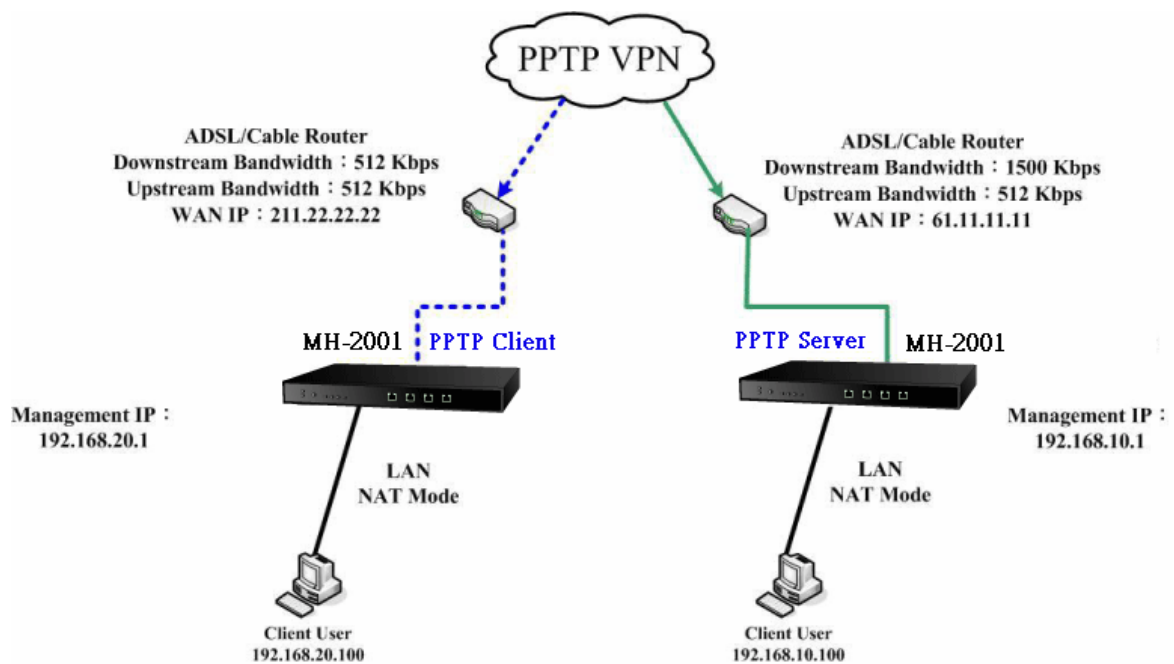
Company B :

**WAN1 IP :** 211.22.22.22

**LAN IP :** 192.168.20.X

This example takes two MH-2001 as flattop. Suppose Company B 192.168.20.100 is going to have VPN connection with Company A 192.168.10.100 and download the resource.

##### TEST Environment



**PPTP VPN Connection Deployment**

**The Default Gateway of Company A is the LAN IP of the MH-2001 192.168.10.1. Follow the steps below:**

**STEP 1 .** Enter **PPTP Server** of **VPN** function in the MH-2001 of Company A. Select **Modify** and enable PPTP Server:

- Select **Encryption**.
- **Client IP Range:** Enter 192.44.75.1-254.
- **Idle Time:** Enter 0.

Modify PPTP Server Setting	
<input type="radio"/> Disable PPTP	
<input checked="" type="radio"/> Enable PPTP	
<input checked="" type="checkbox"/> Encryption	
Client IP Range :	192.144.75.1 .. 254
DNS Server 1	
DNS Server 2	
WINS Server 1	
WINS Server 2	
<input checked="" type="checkbox"/> Allow PPTP client to connect the Internet.	
Auto-Disconnect if idle <input type="text" value="0"/> minutes ( Range: 0 - 999999, 0: means always connected )	
Echo-Request	Retry <input type="text" value="4"/> times Timeout <input type="text" value="30"/> Second ( Retry: 0 - 9, 0: means disable; Timeout: 1 - 60 )
<div>OK Cancel</div>	

### Enable PPTP VPN Server Settings



**Idle Time:** the setting time that the VPN Connection will auto-disconnect under unused situation.

**STEP 2 .** Add the following settings in **PPTP Server** of **VPN** function in the MH-2001 of Company A:

- Select **New Entry**.
- **User Name**: Enter PPTP\_Connection.
- **Password**: Enter 123456789.
- **Client IP assigned by**: Select **IP Range**.
- Click **OK**.

Add New PPTP Server

User Name :

PPTP\_Connection

(Max. 16 characters)

Password :

.....

(Max. 19 characters)

Client IP assigned by

☒ IP Range

☐ Fixed IP :

☐ Manual Disconnect

OK

Cancel

### PPTP VPN Server Setting

PPTP Server ( **Enable**, Encryption:ON ) :

Client IP Range : 192.144.75.1-254

**Modify**

i	User Name	Client IP	Uptime	Configure
--	PPTP_Connection	0.0.0.0	---	<b>Modify</b> <b>Remove</b>

**New Entry**

### Complete PPTP VPN Server Setting

**STEP 3 .** Enter the following setting in **Tunnel** of **VPN** function:

- Enter a specific Tunnel **Name**.
- **From Source:** Select LAN
- **From Source Subnet / Mask:** Enter 192.168.10.0 / 255.255.255.0.
- **To Destination:** Select To Destination Subnet / Mask.
- **To Destination Subnet / Mask:** Enter 192.168.20.0 / 255.255.255.0.
- **IPSec / PPTP Setting:** Select PPTP\_Server\_PPTP\_Connection.
- Select **Show remote Network Neighborhood**.
- Click **OK**.

**Figure11-167 New Entry Tunnel Setting**

i	Name	Source Subnet	Destination Subnet	IPSec / PPTP	Configure
	PPTP_VPN_Tun..	192.168.10.0	192.168.20.0	PPTP_Ser...	<div>Modify</div> <div>Remove</div> <div>Pause</div>

**New Entry**

**Complete New Entry Tunnel Setting**

**STEP 4 .** Enter the following setting in **Outgoing Policy**:

- **Tunnel:** Select PPTP\_VPN\_Tunnel.
- Click **OK**.

Comment :  (Max. 32 characters)

Modify Policy	
Source Address	Inside_Any ▾
Destination Address	Outside_Any ▾
Service	ANY ▾
Schedule	None ▾
Authentication User	None ▾
Tunnel	PPTP_VPN_Tunnel ▾
Action, WAN Port	PERMIT ALL ▾
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> Enable
IM / P2P Blocking	None ▾
QoS	None ▾
MAX. Bandwidth Per Source IP	Downstream <input type="text" value="0"/> Kbps Upstream <input type="text" value="0"/> Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )

**Setting the VPN Tunnel Outgoing Policy**

Source	Destination	Service	Action	Option					Configure			Move
Inside_Any	Outside_Any	ANY	VPN						<input type="button" value="Modify"/>	<input type="button" value="Remove"/>	<input type="button" value="Pause"/>	To 1 ▾

**Complete the VPN Tunnel Outgoing Policy Setting**




**STEP 5 . Enter the following setting in Incoming Policy:**

- **Tunnel:** Select PPTP\_VPN\_Tunnel.
- Click **OK**.

Comment :  (Max. 32 characters)

Add New Policy	
Source Address	Outside_Any
Destination Address	Inside_Any
Service	ANY
Schedule	None
Tunnel	PPTP_VPN_Tunnel
Action	PERMIT
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
QoS	None
MAX. Bandwidth Per Source IP	Downstream <input type="text" value="0"/> Kbps Upstream <input type="text" value="0"/> Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
NAT	<input type="checkbox"/> Enable

**Setting the VPN Tunnel Incoming Policy**

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Inside_Any(Routing)	ANY	VPN	  	<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To <input type="text" value="1"/>

**Complete the VPN Tunnel Incoming Policy Setting**

**The Default Gateway of Company B is the LAN IP of the MH-2001 192.168.20.1. Follow the steps below:**

**STEP 6 .** Add the following settings in **PPTP Client** of **VPN** function in the MH-2001 of Company B:

- Click **New Entry** Button.
- **User Name:** Enter PPTP\_Connection.
- **Password:** Enter 123456789.
- **Server IP or Domain Name:** Enter 61.11.11.11.
- Select **Encryption**.
- Click **OK**.

Add New PPTP Client

User Name : PPTP\_Connection (Max. 16 characters)

Password : ..... (Max. 19 characters)

Server IP or Domain Name : 61.11.11.11 (Max. 39 characters) ☒ Encryption

WAN interface : ☒ WAN 1 ☐ WAN 2

☐ NAT(Connect to Windows PPTP Server)

☐ Manual Connect

OK Cancel

#### PPTP VPN Client Setting

PPTP Client :

i	User Name	Server IP or Domain Name	Encryption	Uptime	Configure
--	PPTP_Connection	61.11.11.11	OFF	---	<a href="#">Modify</a> <a href="#">Remove</a>

[New Entry](#)

#### Complete PPTP VPN Client Setting



**STEP 7 .** Enter the following setting in **Tunnel** of **VPN** function:

- Enter a specific Tunnel **Name**.
- **From Source:** Select LAN
- **From Source Subnet / Mask:** Enter 192.168.20.0 / 255.255.255.0.
- **To Destination:** Select To Destination Subnet / Mask.
- **To Destination Subnet / Mask:** Enter 192.168.10.0 / 255.255.255.0.
- **IPSec / PPTP Setting:** Select PPTP\_Client\_PPTP\_Connection.
- Select **Show remote Network Neighborhood**.
- Click **OK**.

New Entry Tunnel	
Name	PPTP_VPN_Tunnel (Max. 16 characters)
From Source	<input checked="" type="radio"/> LAN <input type="radio"/> DMZ
From Source Subnet / Mask	192.168.20.0 / 255.255.255.0
To Destination	<input checked="" type="radio"/> To Destination Subnet / Mask <input type="radio"/> Remote Client
	192.168.10.0 / 255.255.255.0
IPSec / PPTP Setting	PPTP_Client_PPTP_Connection(61.11.11.11) ▼
Keep alive IP :	
<input checked="" type="checkbox"/> Show remote Network Neighborhood	

OK Cancel

### New Entry Tunnel Setting

i	Name	Source Subnet	Destination Subnet	IPSec / PPTP	Configure
	PPTP_VPN_Tun..	192.168.20.0	192.168.10.0	PPTP_Cli...	<div>Modify</div> <div>Remove</div> <div>Pause</div>

New Entry

### Complete New Entry Tunnel Setting

**STEP 8 .** Enter the following setting in **Outgoing Policy**:

- **Tunnel:** Select PPTP\_VPN\_Tunnel.
- Click **OK**.

Comment :  (Max. 32 characters)

Modify Policy	
Source Address	Inside_Any ▾
Destination Address	Outside_Any ▾
Service	ANY ▾
Schedule	None ▾
Authentication User	None ▾
Tunnel	PPTP_VPN_Tunnel ▾
Action, WAN Port	PERMIT ALL ▾
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> Enable
IM / P2P Blocking	None ▾
QoS	None ▾
MAX. Bandwidth Per Source IP	Downstream <input type="text" value="0"/> Kbps Upstream <input type="text" value="0"/> Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )

**Setting the VPN Tunnel Outgoing Policy**

Source	Destination	Service	Action	Option					Configure			Move
Inside_Any	Outside_Any	ANY	VPN						<input type="button" value="Modify"/>	<input type="button" value="Remove"/>	<input type="button" value="Pause"/>	To 1 ▾

**Complete the VPN Tunnel Outgoing Policy Setting**

**STEP 9 .** Enter the following setting in **Incoming Policy**:

- **Tunnel:** Select PPTP\_VPN\_Tunnel.
- Click **OK**.

Comment :  (Max. 32 characters)

Add New Policy	
Source Address	Outside_Any ▾
Destination Address	Inside_Any ▾
Service	ANY ▾
Schedule	None ▾
Tunnel	PPTP_VPN_Tunnel ▾
Action	PERMIT ▾
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
QoS	None ▾
MAX. Bandwidth Per Source IP	Downstream <input type="text" value="0"/> Kbps Upstream <input type="text" value="0"/> Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
NAT	<input type="checkbox"/> Enable

**Setting the VPN Tunnel Incoming Policy**

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Inside_Any(Routing)	ANY	VPN		<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To 1 ▾

**Complete the VPN Tunnel Incoming Policy Setting****STEP 10 .** Complete PPTP VPN Connection.

### 6.9.6 Example.6

The way to set the MH-2001 appliance PPTP VPN connection in Windows 2000.

#### The Deployment

Company A : Use with MH-2001

**WAN1 IP :** 61.11.11.11

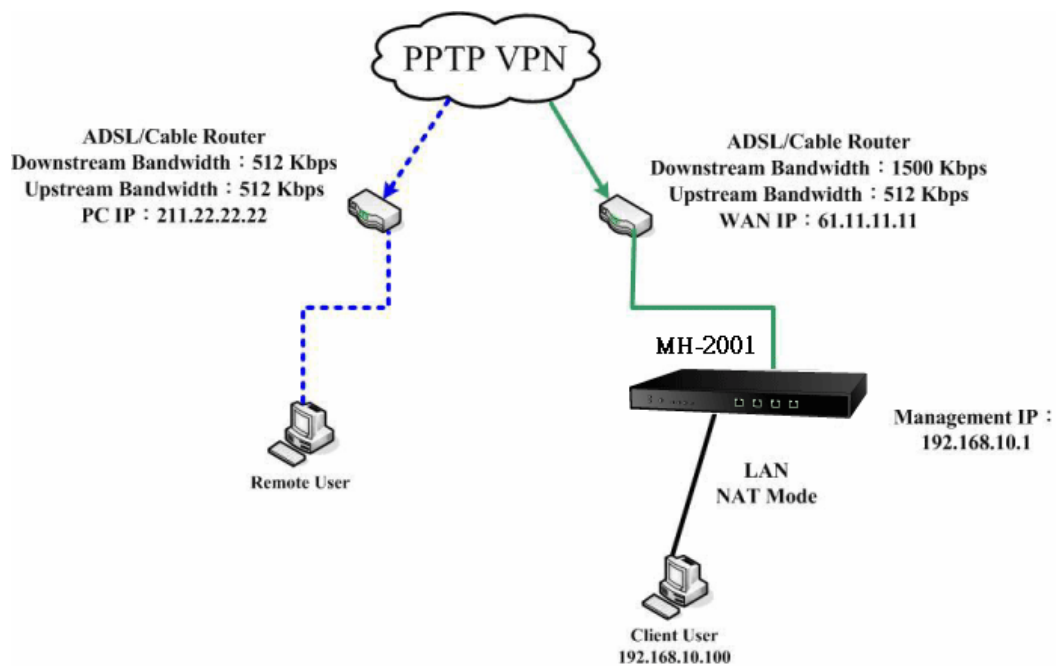
**LAN IP :** 192.168.10.X

Company B : Use with Windows 2000 PC

**WAN1 IP :** 211.22.22.22

We use the MH-2001 and Windows 2000 VPN-PPTP client to be the platform. Assume the B Company 211.22.22.22 link to A Company 192.168.10.100 via the VPN, in order to download the shared files.

#### TEST Environment



The PPTP VPN deployment

The A Company's default gateway is the LAN IP 192.168.10.1 in MH-2001, add the following settings :

**STEP 1 .** In A Company's MH-2001, **VPN → PPTP Server**, click **Modify**, select **Enable PPTP** :

- Select **Encryption**.
- **Client IP Range**, enter 192.44.75.1 – 254.
- Select **Allow remote client to connect to Network**.
- **Auto-Disconnect if idle**, enter 0.

Modify PPTP Server Setting	
<input type="radio"/> Disable PPTP	
<input checked="" type="radio"/> Enable PPTP	
<input checked="" type="checkbox"/> Encryption	
Client IP Range :	192.144.75.1 .. 254
DNS Server 1	
DNS Server 2	
WINS Server 1	
WINS Server 2	
<input checked="" type="checkbox"/> Allow PPTP client to connect the Internet.	
Auto-Disconnect if idle <input type="text" value="0"/> minutes ( Range: 0 - 999999, 0: means always connected )	
Echo-Request Retry	<input type="text" value="4"/> times Timeout <input type="text" value="30"/> Second ( Retry: 0 - 9, 0: means disable; Timeout: 1 - 60 )
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

**To enable PPTP VPN setting**



As create the MH-2001 PPTP server VPN, the MIS engineer can allow or limit the external user to link to network via the MH-2001.



**Auto-Disconnect if idle** : When the VPN is not in use, it will automatically disconnect. (Time unit : minute).

**STEP 2 .** In A Company's MH-2001, **VPN → PPTP Server**, add the following settings :

- Click **New Entry**.
- **User Name**, enter PPTP\_Connection.
- **Password**, enter 123456789.
- **Client IP assigned by**, select IP Range.

- Click **OK**.

**Add New PPTP Server**

User Name :	<input type="text" value="PPTP_Connection"/>	(Max. 16 characters)
Password :	<input type="password" value="....."/>	(Max. 19 characters)
Client IP assigned by		
<input checked="" type="radio"/> IP Range		
<input type="radio"/> Fixed IP :	<input type="text"/>	
<input type="checkbox"/> Manual Disconnect		

**OK** **Cancel**

### The PPTP VPN setting

PPTP Server ( **Enable**, **Encryption:ON** ) :

Client IP Range : 192.144.75.1-254 **Modify**

i	User Name	Client IP	Uptime	Configure
--	PPTP_Connection	0.0.0.0	---	<b>Modify</b> <b>Remove</b>

**New Entry**

**Complete to set the PPTP VPN setting**

**STEP 3 . In VPN → Tunnel, add the following settings :**

- **Name**, enter the Tunnel name.
- **From Source**, select LAN.
- **From Source Subnet / Mask**, enter the A Company's LAN IP address 192.168.10.0 and mask 255.255.255.0.
- **To Destination**, select Remote Client.
- **IPSec / PPTP Setting**, select **PPTP\_Server\_PPTP\_Connection**.
- Select **Show remote Network Neighborhood**.
- Click **OK**.

Modify PPTP\_VPN\_Tunnel Tunnel

Name: PPTP\_VPN\_Tunnel (Max. 16 characters)

From Source: ☒ LAN ☐ DMZ

From Source Subnet / Mask: 192.168.10.0 / 255.255.255.0

To Destination: ☐ To Destination Subnet / Mask ☒ Remote Client

IPSec / PPTP Setting: PPTP\_Server\_PPTP\_Connection

Keep alive IP:

☒ Show remote Network Neighborhood

OK Cancel

**To add the VPN Tunnel setting**

i	Name	Source Subnet	Destination Subnet	IPSec / PPTP	Configure
	PPTP_VPN_Tun..	192.168.10.0	Remote Client	PPTP_Ser...	<div>Modify</div> <div>Remove</div> <div>Pause</div>

**New Entry**

**Complete to set the VPN Tunnel setting**

**STEP 4 . In Policy → Outgoing, add the following settings :**

■**Tunnel**, select PPTP\_VPN\_Tunnel.

■Click **OK**.

Comment :  (Max. 32 characters)

Modify Policy	
Source Address	Inside_Any ▾
Destination Address	Outside_Any ▾
Service	ANY ▾
Schedule	None ▾
Authentication User	None ▾
<b>Tunnel</b>	<b>PPTP_VPN_Tunnel ▾</b>
Action, WAN Port	PERMIT ALL ▾
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> Enable
IM / P2P Blocking	None ▾
QoS	None ▾
MAX. Bandwidth Per Source IP	Downstream <input type="text" value="0"/> Kbps Upstream <input type="text" value="0"/> Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )

**To set the outgoing policy included the VPN Tunnel**

Source	Destination	Service	Action	Option					Configure			Move
Inside_Any	Outside_Any	ANY	VPN						Modify	Remove	Pause	To 1 ▾

**Complete to set the outgoing policy included the VPN Tunnel**



**STEP 5 . In Policy → Incoming,** add the following settings :

■**Tunnel**, select PPTP\_VPN\_Tunnel.

■Click **OK**.

Comment :  (Max. 32 characters)

Add New Policy	
Source Address	Outside_Any ▾
Destination Address	Inside_Any ▾
Service	ANY ▾
Schedule	None ▾
Tunnel	PPTP_VPN_Tunnel ▾
Action	PERMIT ▾
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
QoS	None ▾
MAX. Bandwidth Per Source IP	Downstream <input type="text" value="0"/> Kbps Upstream <input type="text" value="0"/> Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
NAT	<input type="checkbox"/> Enable

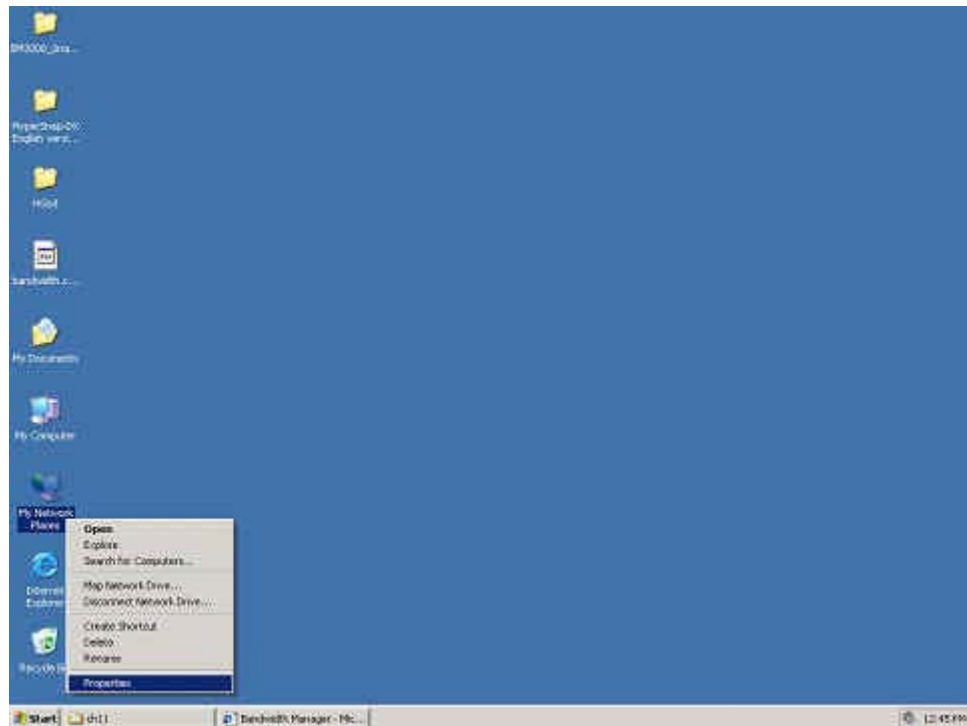
**To set the incoming policy included the VPN Tunnel**

Source	Destination	Service	Action	Option	Configure			Move
Outside_Any	Inside_Any(Routing)	ANY	VPN				<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To 1 ▾

**Complete to set the incoming policy included the VPN Tunnel**

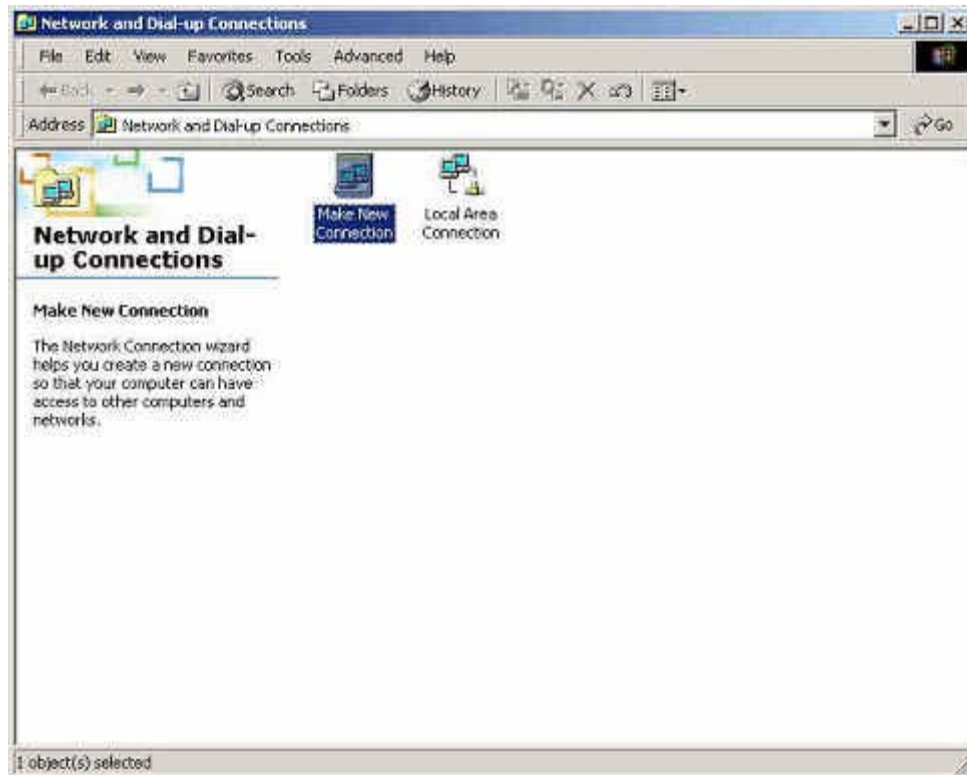
**The B Company's PC use the Real IP (211.22.22.22). Add the following settings :**

**STEP 6 .** Right click on **My Network Places**, and select **Properties**.



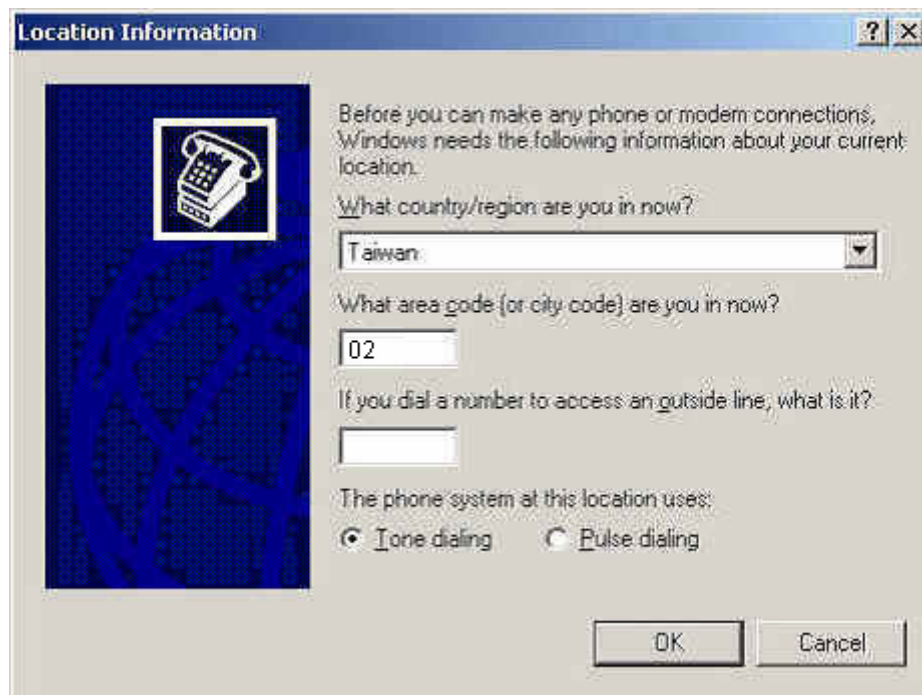
## To start the Windows 2000 PPTP VPN setting

**STEP 7 . In Network and Dial-up Connection, click **Make New Connection**.**



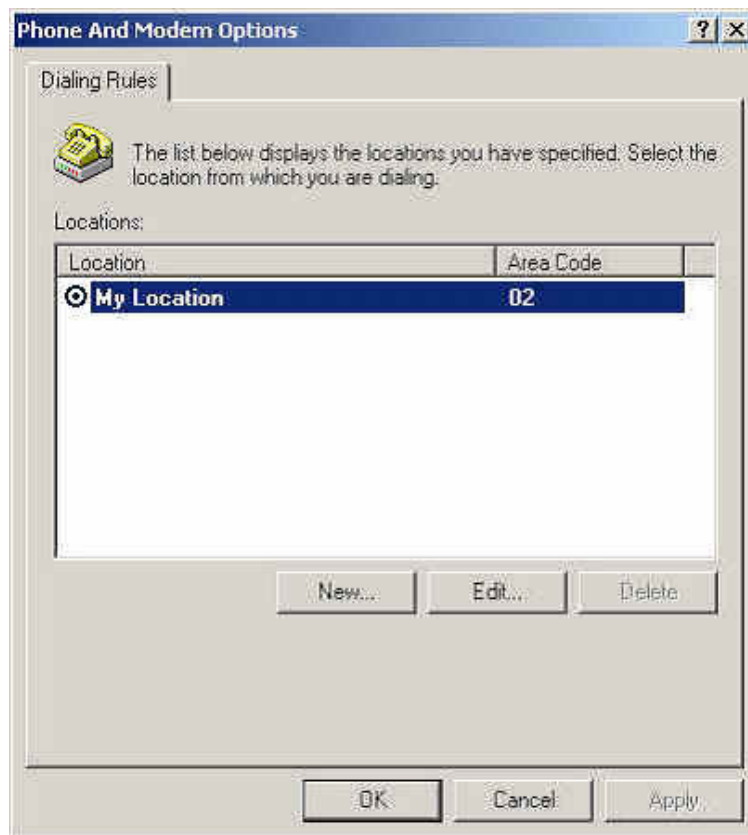
**Network and Dial-up Connection**

**STEP 8 .** In **Location Information**, enter the **Country /Region**, **Area code** and select the **phone system**, then click **OK**.



**The Local Information setting**

**STEP 9 .** In **Phone and Modem Options**, click **OK**.



**Phone and Modem Options**

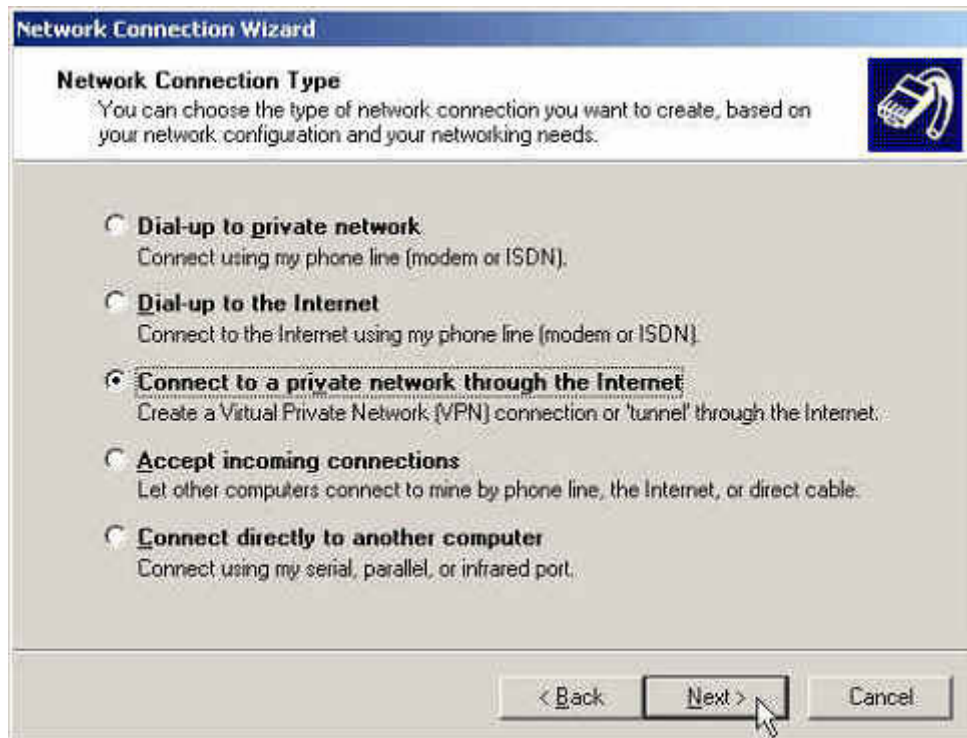
**STEP 10 .** In **Network Connection Wizard**, click **Next**.



**Network Connection Wizard**


**STEP 11 .** In **Network Connection Wizard**, select **Connect to a private network through the Network**.

Click **Next**.



**To Connect to a private network through the Internet**

**STEP 12 .** In **New Connection Wizard**, enter the **IP Address**, then click **Next**.



The screenshot shows a Windows-style dialog box titled "New Connection Wizard". Inside, the "VPN Server Selection" section asks "What is the name or address of the VPN server?". Below this, it instructs the user to "Type the host name or Internet Protocol (IP) address of the computer to which you are connecting." and provides an example: "Host name or IP address (for example, microsoft.com or 157.54.0.1 ):". A text input field contains the IP address "61.11.11.11". At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel". A small icon of a computer with a network cable is in the top right corner of the dialog.

**Setup the Host name or IP address**



**STEP 13 .** In **Network Connection Wizard** → **Connection Availability**, select **For all users**. Click **Next**.



**Setup the Connection Availability**

**STEP 14 .** In **New Connection Wizard**, enter the **Connection Name**, click **Finish**.



**Complete the New Connection Wizard**

**STEP 15 .** In **Connect Virtual Private Connection**, add the following settings :

- **User Name**, enter PPTP\_Connection.
- **Password**, enter 123456789.
- Select **Save Password**.
- Click **Connect**.
- It shows **Connecting to Virtual Private Connection** window.
- **Connection Complete**.



**Connect Virtual Private Connection**



**Creating the PPTP VPN Connection**



**Complete to setup the PPTP VPN connection**

**STEP 16 .** Complete to setup the PPTP VPN connection.

## Chapter 7: Policy

This section provides the Administrator with facilities to set control policies for packets with different source IP addresses, source ports, destination IP addresses, and destination ports. Control policies decide whether packets from different network objects, network services, and applications are able to pass through MH-2001.

### What is Policy?

The device uses policies to filter packets. The policy settings are: source address, destination address, services, permission, packet log, packet statistics, and flow alarm. Based on its source addresses, a packet can be categorized into:

- (1) **Outgoing:** The source IP is in LAN network; the destination is in WAN network. The system manager can set all the policy rules of Outgoing packets in this function.
- (2) **Incoming:** The source IP is in WAN network; the destination is in LAN network. (For example: Mapped IP, Virtual Server) The system manager can set all the policy rules of Incoming packets in this function.
- (3) **WAN to DMZ:** The source IP is in WAN network; the destination is in DMZ network. (For example: Mapped IP, Virtual Server) The system manager can set all the policy rules of WAN to DMZ packets in this function.
- (4) **LAN to DMZ:** The source IP is in LAN network; the destination is in DMZ network. The system manager can set all the policy rules of LAN to DMZ packets in this function.
- (5) **DMZ to LAN:** The source IP is in DMZ network; the destination is in LAN network. The system manager can set all the policy rules of DMZ to LAN packets in this function.
- (6) **DMZ to WAN:** The source IP is in DMZ network; the destination is in WAN network. The system manager can set all the policy rules of DMZ to WAN packets in this function.



All the packets that go through MH-2001 must pass the policy permission (except VPN). Therefore, the LAN, WAN, and DMZ network have to set the applicable policy when establish network connection.

### How do I use Policy?

The policy settings are source addresses, destination addresses, services, permission, log, statistics, and flow alarm. Among them, source addresses, destination addresses and IP mapping addresses have to be defined in the **Address** menu in advance. Services can be used directly in setting up policies, if they are in the Pre-defined Service menu. Custom services need to be defined in the **Custom** menu before they can be used in the policy settings.

If the destination address of an incoming policy is a Mapped IP address or a Virtual Server address, then the address has to be defined in the **Virtual Server** section instead of the **Address** section.

### Define the required fields of Policy

**Source and Destination:**





- Source IP and Destination IP is according to the MH-2001's point of view. The active side is the source; passive side is destination.

**Service:**

- It is the service item that controlled by Policy. The user can choose default value or the custom services that the system manager set in **Service** function.








**Action, WAN Port:**

- Control actions to permit or reject packets that delivered between LAN network and WAN network when pass through MH-2001 (See the chart and illustration below)

Chart	Name	Illustration
	Permit all WAN network Interface	Allow the packets that correspond with policy to be transferred by WAN1/2 Port
	Permit WAN1	Allow the packets that correspond with policy to be transferred by WAN1 Port
	Permit WAN2	Allow the packets that correspond with policy to be transferred by WAN2 Port
	DENY	Reject the packets that correspond with policy to be transferred by WAN Port

**Option:**

- To display if every function of Policy is enabled or not. If the function is enabled and then the chart of the function will appear (See the chart and illustration below)

Chart	Name	Illustration
	Traffic Log	Enable traffic log
	Statistics	Enable traffic statistics
	Authentication User	Enable Authentication User
	Schedule	Enable the policy to automatically execute the function in a certain time
	Content Blocking	Enable Content Blocking
	IM/P2P Blocking	Enable IM/P2P Blocking
	QoS	Enable QoS

**Move:**

- Every packet that passes the MH-2001 is detected from the front policy to the last one. So it can modify the priority of the policy from the selection.

**Traffic Log:**

- Record all the packets that go through policy.

**Statistics:**

- Chart of the traffic that go through policy

**Content Blocking:**

- To restrict the packets that passes through the policy

**Authentication-User:**

- The user have to pass the authentication to connect by Policy

**Schedule:**

- Setting the policy to automatically execute the function in a certain time

**QoS:**

- Setting the Guarantee Bandwidth and Maximum Bandwidth of the Policy (the bandwidth is shared by the users who correspond to the Policy)

**MAX. Bandwidth Per Source IP:**

- Set the Max. Bandwidth of Downstream/Upstream that permitted by source IP.

**MAX. Concurrent Sessions:**

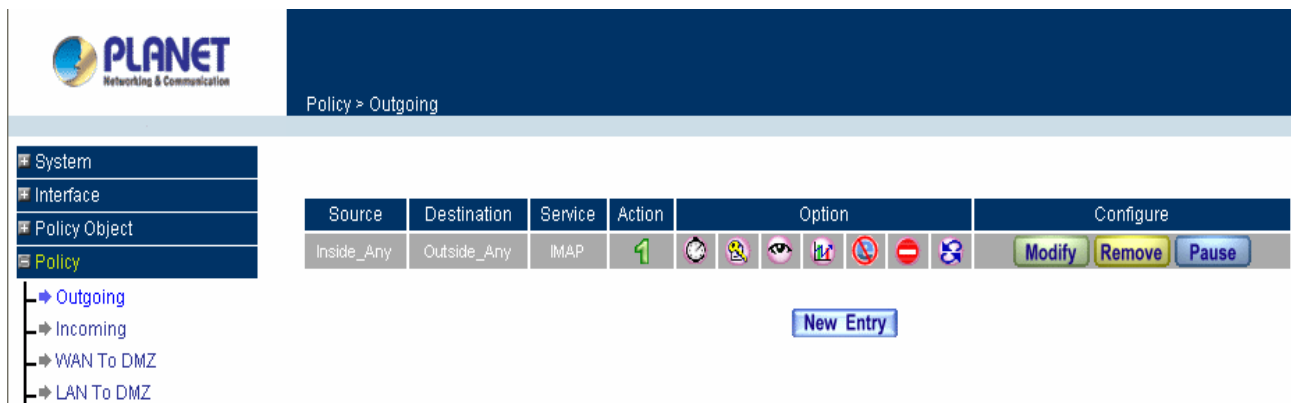
- Set the concurrent sessions that permitted by policy. And if the sessions exceed the setting value, the surplus connection cannot be set successfully.

## 7.1 Outgoing

This section describes steps to create policies for packets and services from the LAN network to the WAN 1/2 network.

**Entering the Outgoing window:**

Click **Policy** on the left hand side menu bar, then click **Outgoing** under it. A window will appear with a table displaying currently defined Outgoing policies.

**Adding a new Outgoing Policy**

**Step 1:** Click on the New Entry button and the Add New Policy window will appear.

Comment :  (Max. 32 characters)

Modify Policy	
Source Address	Inside_Any
Destination Address	Outside_Any
Service	IMAP
Schedule	Fri
Authentication User	alex
Tunnel	None
Action, WAN Port	PERMIT, WAN 1
Traffic Log	<input checked="" type="checkbox"/> Enable
Statistics	<input checked="" type="checkbox"/> Enable
Content Blocking	<input checked="" type="checkbox"/> Enable
IM / P2P Blocking	IM_P2P
QoS	HTTP
MAX. Bandwidth Per Source IP	Downstream <input type="text"/> Kbps Upstream <input type="text"/> Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	<input type="text"/> ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	<input type="text"/> ( Range: 1 - 99999, 0: means unlimited )



**Step 2:** Configure all the parameters.

**Source Address:** Select the name of the LAN network from the drop down list. The drop down list contains the names of all LAN networks defined in the LAN section of the **Address** menu. To create a new source address, please go to the LAN section under the **Address** menu.

**Destination Address:** Select the name of the WAN 1/2 network from the drop down list. The drop down list contains the names of all WAN 1/2 networks defined in the WAN 1/2 section of the **Address** window. To create a new destination address, please go to the WAN 1/2 section under the **Address** menu.

**Service:** Specified services provided by WAN 1/2 network servers. These are services/application that are allowed to pass from the LAN network to the WAN 1/2 network. Choose ANY for all services.

**Schedule:** Select the item listed in the schedule to enable the policy to automatically execute the function in a certain time and range.

**Authentication User:** Select the item listed in the Authentication User to enable the policy to automatically execute the function in a certain time and range.

**Tunnel:** Select the VPN Tunnel which you want to establish a connection.

**Action:** Select Permit ALL, Permit WAN 1, Permit WAN 2 or Deny ALL to allow or reject the packets travelling between the source network and the destination network.

**Traffic Log:** Select **Enable** to enable flow monitoring.

**Statistics:** Select **Enable** to enable flow statistics.

**Content Blocking:** Select **Enable** to enable Content Filtering.

**IM/P2P Blocking:** Select the listed item to enable the IM/P2P Blocking.

**QoS:** Select the item listed in the QoS to enable the policy to automatically execute the function in a certain time and range.

**MAX. Bandwidth Per Source IP:** The maximum Bandwidth that allows passing through MH-2001 which by source IP. 0 means it is unlimited.

**MAX. Concurrent Sessions Per IP:** The maximum concurrent sessions that allows passing through MH-2001 which by source IP. 0 means it is unlimited.

**MAX. Concurrent Sessions:** The maximum concurrent sessions that allows passing through MH-2001. 0 means it is unlimited.

**Step 3:** Click **OK** to add a new outgoing policy; or click **Cancel** to cancel adding a new outgoing policy.

### Enabled Monitoring function:

**Set up the policy that can monitor the internal users. (Take Logging, Statistics, and Alarm Threshold for example)**

**STEP 1 .** Enter the following setting in **Outgoing Policy**:


- Click **New Entry**
- Select **Logging**

■ **Select Statistics**■ **Click OK**Comment :  (Max. 32 characters)

Modify Policy	
Source Address	Inside_Any ▾
Destination Address	Outside_Any ▾
Service	ANY ▾
Schedule	None ▾
Authentication User	None ▾
Tunnel	None ▾
Action, WAN Port	PERMIT ALL ▾
Traffic Log	<input checked="" type="checkbox"/> Enable
Statistics	<input checked="" type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> Enable
IM / P2P Blocking	None ▾
QoS	None ▾
MAX. Bandwidth Per Source IP	Downstream <input type="text" value="0"/> Kbps Upstream <input type="text" value="0"/> Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )

 **Setting the Outgoing Policy**

**STEP 2 .** Go to **Monitor / Log / Traffic** menu, you can obtain the information of Traffic if you want to monitor all the packets of the MH-2001.



Monitor > Log > Traffic

System

Interface

Policy Object

Policy

Anomaly Flow IP

Monitor

Log

Traffic

Event

Connection

Log Backup

Accounting Report

Statistics

Wake on Lan

Status

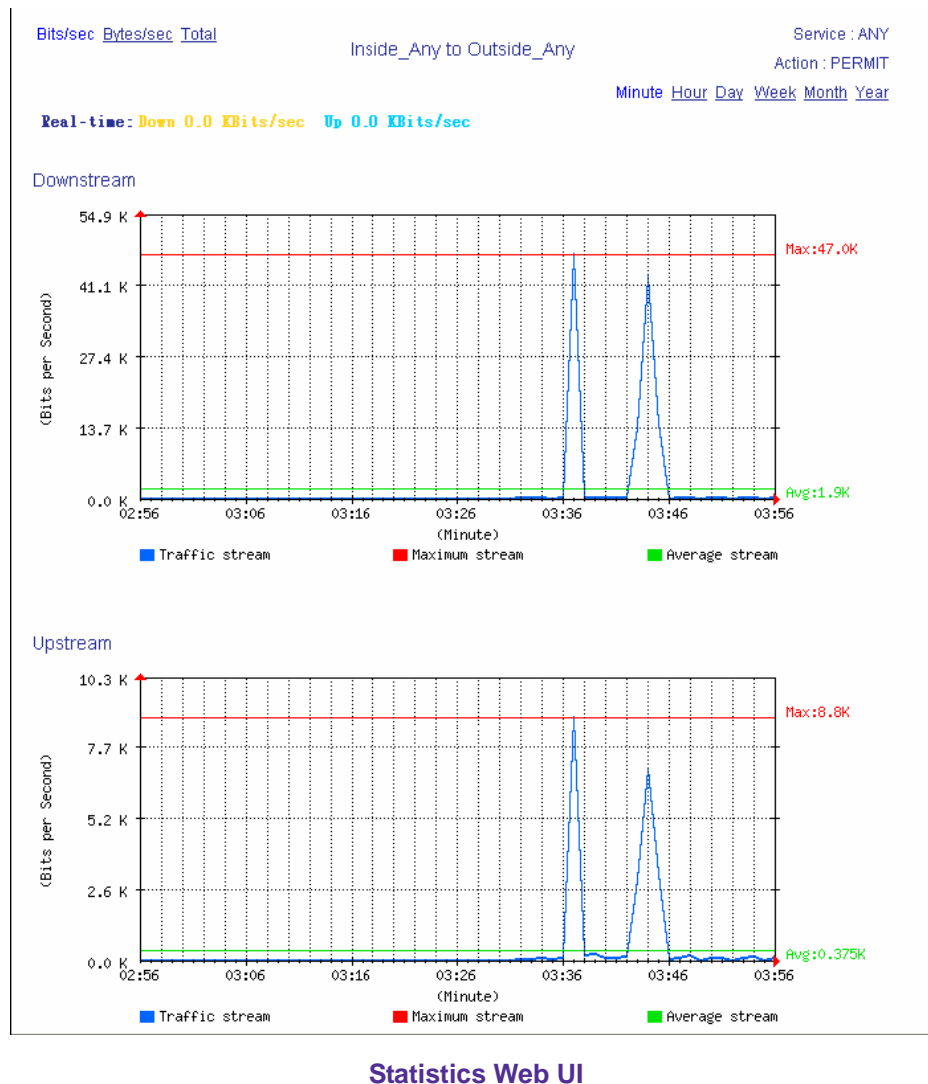
Apr 13 19:16:43

Next

Time	Source	Destination	Protocol	Port	Disposition
Apr 13 19:16:43	211.75.117.114	210.66.155.77	TCP	1374 ==> 8080	✓
Apr 13 19:16:42	211.75.117.114	210.66.155.77	TCP	1373 ==> 8080	✓
Apr 13 19:16:40	211.75.117.114	210.66.155.77	TCP	1372 ==> 8080	✓
Apr 13 19:16:40	211.75.117.114	210.66.155.77	TCP	1371 ==> 8080	✓
Apr 13 19:16:39	211.75.117.114	210.66.155.77	TCP	1370 ==> 8080	✓
Apr 13 19:16:01	210.66.155.77	211.75.117.114	TCP	8080 ==> 1347	✓
Apr 13 19:14:48	211.75.117.114	210.66.155.77	TCP	1367 ==> 8080	✓
Apr 13 19:14:30	211.75.117.114	210.66.155.77	TCP	1366 ==> 8080	✓
Apr 13 19:13:59	211.75.117.114	210.66.155.77	TCP	1365 ==> 8080	✓
Apr 13 19:13:57	211.75.117.114	210.66.155.77	TCP	1364 ==> 8080	✓
Apr 13 19:13:55	211.75.117.114	210.66.155.77	TCP	1363 ==> 8080	✓
Apr 13 19:13:54	211.75.117.114	210.66.155.77	TCP	1362 ==> 8080	✓
Apr 13 19:13:53	211.75.117.114	210.66.155.77	TCP	1361 ==> 8080	✓
Apr 13 19:13:52	211.75.117.114	210.66.155.77	TCP	1360 ==> 8080	✓
Apr 13 19:13:52	211.75.117.114	210.66.155.77	TCP	1359 ==> 8080	✓
Apr 13 19:13:49	211.75.117.114	210.66.155.77	TCP	1358 ==> 8080	✓
Apr 13 19:13:47	211.75.117.114	210.66.155.77	TCP	1357 ==> 8080	✓
Apr 13 19:13:38	211.75.117.114	210.66.155.77	TCP	1356 ==> 8080	✓

**Traffic Log Monitor Web UI**

**STEP 3** . To display the traffic statistics that through Policy to access to Internet in **Policy Statistics** of **Statistics** function.



## 7.2 Incoming

This section describes steps to create policies for packets and services from the WAN 1/2 network to the LAN network including Mapped IP and Virtual Server.

**The external user control the internal PC through remote control software (Take pcAnywhere for example)**

**STEP 1** . Set up a Internal PC controlled by external user, and Internal PC's IP Address is 192.168.1.2

**STEP 2 .** Enter the following setting in **Virtual Server1** of **Virtual Server** function:

Virtual Server Real IP

Service	WAN Port	Server Virtual IP	Configure
PC-Anywhere (5631-5632)	5631-5632	192.168.1.2	<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>

**Setting Virtual Server**

**STEP 3 .** Enter the following in **Incoming Policy**:

- Click **New Entry**
- **Destination Address:** Select Virtual Server1
- **Service:** Select PC-Anywhere (5631-5632)
- Click **OK**

Comment :  (Max. 32 characters)

Add New Policy	
Source Address	Outside_Any
Destination Address	Virtual Server 1(61.11.11.12)
Service	PC-Anywhere(5631-5632)
Schedule	None
Tunnel	None
Action	PERMIT
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
QoS	None
MAX. Bandwidth Per Source IP	Downstream <input type="text" value="0"/> Kbps Upstream <input type="text" value="0"/> Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
NAT	<input type="checkbox"/> Enable

### Setting the External User Control the Internal PC Policy

**STEP 4 .** Complete the policy for the external user to control the internal PC through remote control software.

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Virtual Server 1(61.11.11.12)	PC-Anywhere(5631-5632)	✓		<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To <input type="text" value="1"/>

### Complete Policy Setting

## 7.3 WAN To DMZ & LAN To DMZ

This section describes steps to create policies for packets and services from the WAN networks to the DMZ networks. Please follow the same procedures for LAN networks to DMZ networks.

Enter [WAN To DMZ] or [LAN To DMZ] window:

Click **WAN To DMZ** under **Policy** menu to enter the **WAN To DMZ** window. The WAN To DMZ table will show up displaying currently defined policies.



The fields in WAN To DMZ window:

- **Source:** source networks, which are addresses specified in the **WAN** section of the **Address** menu, or all the WAN network addresses.
- **Destination:** destination networks, which are addresses specified in **DMZ** section of the **Address** menu and **Mapped IP** addresses of the **Virtual Server** menu.
- **Service:** services supported by servers in DMZ network.
- **Action:** control actions, to permit or deny packets from WAN networks to DMZ travelling through MH-2001.
- **Option:** specify the monitoring functions of packets from WAN network to DMZ network travelling through MH-2001.
- **Configure:** modify settings or remove policies.
- **Move:** this sets the priority of the policies, number 1 being the highest priority.

**Adding a new WAN To DMZ Policy:**

**Example :** Set a FTP Server under DMZ NAT Mode and restrict the download bandwidth from external and MAX. Concurrent Sessions.

**STEP 1 .** Set a FTP Server under **DMZ**, which IP is 192.168.3.2 (The DMZ Interface Address is 192.168.3.1/24)

**STEP 2 .** Enter the following setting in **Virtual Server1** of **Virtual Server** function:

Virtual Server Real IP

Service	WAN Port	Server Virtual IP	Configure
FTP (21)	21	10.0.0.10	<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>

### Setting up Virtual Server Corresponds to FTP Server



When using the function of **Incoming** or **WAN to DMZ** in **Policy**, strong suggests that cannot select **ANY** in **Service**. It may be attacked by Hacker easily.

**STEP 3 .** Enter the following in **QoS**:

Name	WAN	Downstream Bandwidth	Upstream Bandwidth	Priority	Configure
FTP_QoS	1	G.Bandwidth = 100 Kbps M.Bandwidth = 500 Kbps	G.Bandwidth = 50 Kbps M.Bandwidth = 200 Kbps	Middle	<input type="button" value="Modify"/> <input type="button" value="Remove"/>
	2	G.Bandwidth = 500 Kbps M.Bandwidth = 512 Kbps	G.Bandwidth = 50 Kbps M.Bandwidth = 60 Kbps		

### QoS Setting

**STEP 4 . Enter the following in WAN to DMZ Policy:**

- Click **New Entry**
- **Destination Address:** Select Virtual Server1 (61.11.11.12)
- **Service:** Select FTP (21)
- **QoS:** Select FTP\_QoS
- **MAX. Concurrent Sessions:** Enter 100
- Click **OK**

Comment :  (Max. 32 characters)

Add New Policy	
Source Address	Outside_Any ▾
Destination Address	Virtual Server 1(61.11.11.12) ▾
Service	FTP(21) ▾
Schedule	None ▾
Tunnel	None ▾
Action	PERMIT ▾
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
QoS	FTP_QoS ▾
MAX. Bandwidth Per Source IP	Downstream <input type="text" value="0"/> Kbps Upstream <input type="text" value="0"/> Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	<input type="text" value="100"/> ( Range: 1 - 99999, 0: means unlimited )
NAT	<input type="checkbox"/> Enable

**Add New Policy****STEP 5 . Complete the policy of restricting the external users to access to internal network server (which may occupy the resource of network)**

Source	Destination	Service	Action	Option	Configure	Move
Outside_Any	Virtual Server 1(61.11.11.12)	FTP(21)	✓		<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To 1 ▾

**Complete the Policy Setting**



## 7.4 DMZ To WAN & DMZ To LAN

This section describes steps to create policies for packets and services from DMZ networks to WAN networks.

**Please follow the same procedures for DMZ networks to LAN networks.**

**Entering the DMZ To WAN window:**

Click **DMZ To WAN** under **Policy** menu and the **DMZ To WAN** table appears displaying currently defined **DMZ To WAN** policies.

The screenshot shows the PLANET web interface. On the left is a navigation menu with options: System, Interface, Policy Object, Policy, Outgoing, Incoming, WAN To DMZ, LAN To DMZ, DMZ To WAN (highlighted), DMZ To LAN, Anomaly Flow IP, and Monitor. The main area has a header 'Policy > DMZ To WAN'. Below this is a table with columns: Source, Destination, Service, Action, Option, Configure, and Move. The table contains one entry: Source 'DMZ\_Any', Destination 'Outside\_Any', Service 'ANY', Action with a green checkmark, and Move set to '1'. Action buttons 'Modify', 'Remove', and 'Pause' are visible. A 'New Entry' button is located below the table.

Source	Destination	Service	Action	Option	Configure	Move
DMZ_Any	Outside_Any	ANY	✓		Modify Remove Pause	To 1

**The fields in the DMZ To WAN window are:**

- **Source:** source network addresses which are specified in the **DMZ** section of the **Address** window.
- **Destination:** destination networks, which is the WAN network address
- **Service:** services supported by Servers of WAN networks.
- **Action:** control actions, to permit or deny packets from the DMZ network to WAN networks travelling through MH-2001.
- **Option:** specify the monitoring functions on packets from the DMZ network to WAN networks travelling through MH-2001..
- **Configure:** modify settings or remove policies
- **Move:** this sets the sequence of the policies, number 1 being the first policy to proceed.

**Adding a DMZ To WAN and DMZ To LAN Policy:**

**Example : Set a Mail Server to allow the internal and external users to receive and send e-mail under DMZ Transparent Mode.**

**STEP 1** . Set a Mail Server in **DMZ** and set its network card's IP Address as 61.11.11.12. The DNS setting is external DNS Server.

**STEP 2** . Add the following setting in **DMZ** of **Address** function:

Name	IP / Netmask	MAC Address	Configure
DMZ_Any	0.0.0.0/0.0.0.0		<a href="#">In Use</a>
Mail_Server	61.11.11.12/255.255.255.255		<a href="#">Modify</a> <a href="#">Remove</a>

[New Entry](#)

The Mail Server's IP Address Corresponds to Name Setting in Address Book of Mail Server

**STEP 3** . Add the following setting in **Group** of **Service** function:

Group name	Service	Configure
Mail_service	DNS,POP3,SMTP	<a href="#">Modify</a> <a href="#">Remove</a>

[New Entry](#)

Setting up a Service Group that has POP3, SMTP, and DNS

**STEP 4 .** Enter the following setting in **WAN to DMZ Policy**:

- Click **New Entry**
- **Destination Address:** Select Mail\_Server
- **Service:** Select Mail\_service
- Click **OK**

Comment :  (Max. 32 characters)

Modify Policy	
Source Address	Outside_Any ▾
Destination Address	Mail_Server ▾
Service	Mail_service ▾
Schedule	None ▾
Tunnel	None ▾
Action	PERMIT ▾
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
QoS	None ▾
MAX. Bandwidth Per Source IP	Downstream <input type="text" value="0"/> Kbps Upstream <input type="text" value="0"/> Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	<input type="text" value="100"/> ( Range: 1 - 99999, 0: means unlimited )
NAT	<input type="checkbox"/> Enable

### Setting a Policy to access Mail Service by WAN to DMZ

**STEP 5 .** Complete the policy to access mail service by **WAN to DMZ**.

Source	Destination	Service	Action	Option			Configure			Move
Outside_Any	Mail_Server(Routing)	Mail_service	✓				Modify	Remove	Pause	To 1 ▾

### Complete the Policy to access Mail Service by WAN to DMZ

**STEP 6 . Add the following setting in LAN to DMZ Policy:**

- Click **New Entry**
- **Destination Address:** Select Mail\_Server
- **Service:** Select Mail\_service
- Click **OK**

Comment :  (Max. 32 characters)

Modify Policy	
Source Address	Inside_Any ▾
Destination Address	Mail_Server ▾
Service	Mail_service ▾
Schedule	None ▾
Action	PERMIT ▾
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
MAX. Concurrent Sessions Per IP	0 ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )
NAT	<input type="checkbox"/> Enable

**Setting a Policy to access Mail Service by LAN to DMZ****STEP 7 . Complete the policy to access mail service by LAN to DMZ**

Source	Destination	Service	Action	Option	Configure	Move
Inside_Any	Mail_Server	Mail_service	✓		<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To 1 ▾

**Complete the Policy to access Mail Service by LAN to DMZ**

**STEP 8 . Add the following setting in DMZ to WAN Policy:**

- Click **New Entry**
- **Source Address:** Select Mail\_Server
- **Service:** Select Mail\_service
- Click **OK**

Comment :  (Max. 32 characters)

Modify Policy	
Source Address	Mail_Server ▼
Destination Address	Outside_Any ▼
Service	Mail_service ▼
Schedule	None ▼
Authentication User	None ▼
Tunnel	None ▼
Action, WAN Port	PERMIT ALL ▼
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> Enable
IM / P2P Blocking	None ▼
QoS	None ▼
MAX. Bandwidth Per Source IP	Downstream <input type="text" value="0"/> Kbps Upstream <input type="text" value="0"/> Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )

**Setting the Policy of Mail Service by DMZ to WAN****STEP 9 . Complete the policy access to mail service by DMZ to WAN.**

Source	Destination	Service	Action	Option					Configure			Move
Mail_Server	Outside_Any	Mail_service	✓						<input type="button" value="Modify"/>	<input type="button" value="Remove"/>	<input type="button" value="Pause"/>	To 1 ▼

**Complete the Policy access to Mail Service by DMZ to WAN**

**STEP 10 . Add the following setting in DMZ to LAN Policy:**

- Click **New Entry**
- **Source Address:** Select Mail\_Server
- **Service:** Select Mail\_service
- Click **OK**

Comment :  (Max. 32 characters)

Modify Policy	
Source Address	Mail_Server ▾
Destination Address	Inside_Any ▾
Service	Mail_service ▾
Schedule	None ▾
Action	PERMIT ▾
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
MAX. Concurrent Sessions Per IP	0 ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	0 ( Range: 1 - 99999, 0: means unlimited )
NAT	<input type="checkbox"/> Enable

**Setting the Policy of Mail Service by DMZ to LAN****STEP 11 . Complete the policy access to mail service by DMZ to LAN.**

Source	Destination	Service	Action	Option	Configure	Move
Mail_Server	Inside_Any	Mail_service	✓		<input type="button" value="Modify"/> <input type="button" value="Remove"/> <input type="button" value="Pause"/>	To 1 ▾

**Complete the Policy access to Mail Service by DMZ to LAN**

## Chapter 8: Anomaly Flow IP

When the MH-2001 received the intrusion packets from hackers, the internal PC will block this abnormal packets in it, to prevent the Company's network be paralyzed.

**In this chapter, we will make the introduction and settings of Anomaly Flow IP.**

### Settings

#### Sasser Block

- Can block the external Sasser virus attack.

#### MSBlaster Block

- Can block the external MSBlaster virus attack.

#### Code Red Block

- Can block the external Code Red virus attack.

#### Nimda Block

- Can block the external Nimda virus attack.

#### Detect SYN Attack

- Can detect the disconnection situation as the hacker keeps sending the TCP SYN data packets to paralyze the server connection.
  - ◆ **SYN Flood Threshold (Total)** : Define all the IP and the total SYN packets (Pkts/Sec) pass through the MH-2001. If over the setting value, then MH-2001 will define it to be attacked.
  - ◆ **SYN Flood Threshold ( Per Source IP )** : Define every source IP and the total SYN packets (Pkts/Sec) pass through the MH-2001. If over the setting value, then MH-2001 will define it to be attacked.
  - ◆ **SYN Flood Threshold Blocking Time (Per Source IP)** : The MH-2001 will block the packets from the attack source IP according to the time setting. After the blocking time, the MH-2001 will re-calculate the total SYN flow from every source IP, if over the setting value, then MH-2001 will keep blocking.

### Detect ICMP Flood

- Can detect the data packets sent from hacker and use the Broadcast to send to ever internal PC.
  - ◆ **ICMP Flood Threshold** : Define all the IP and the total ICMP packets( Pkts/Sec ) pass through the MH-2001. If over the setting value, then MH-2001 will define it to be attacked.
  - ◆ **ICMP Flood Threshold (Per Source IP )** : Define every source IP and the total ICMP packets ( Pkts/Sec ) pass through the MH-2001. If over the setting value, then MH-2001 will define it to be attacked.
  - ◆ **ICMP Flood Threshold Blocking Time ( Per Source IP )** : The MH-2001 will block the packets from the attack source IP according to the time setting. After the blocking time, the MH-2001 will re-calculate the total ICMP flow from every source IP, if over the setting value, then MH-2001 will keep blocking.

### Detect UDP Flood

- Can detect the UDP data packets sent from hacker and use the Broadcast to send to ever internal PC.
  - ◆ **UDP Flood Threshold (Total)** : Define all the IP and the total UDP packets ( Pkts/Sec ) pass through the MH-2001. If over the setting value, then MH-2001 will define it to be attacked.
  - ◆ **UDP Flood Threshold (Per Source IP )** : Define every source IP and the total UDP packets ( Pkts/Sec ) pass through the MH-2001. If over the setting value, then MH-2001 will define it to be attacked.
  - ◆ **Udp Flood Threshold Blocking Time ( Per Source IP )** : The MH-2001 will block the packets from the attack source IP according to the time setting. After the blocking time, the MH-2001 will re-calculate the total UDP flow from every source IP, if over the setting value, then MH-2001 will keep blocking.

### Detect Ping of Death Attack

- Can detect the status of PING data packets sent from the hackers, in order to paralyze the network.

### Detect IP Spoofing Attack

- Can detect the hackers which prevent the illegal user to pass through the MH-2001.

### Detect Port Scan Attack

- Can detect the Port ID which the hacker use it to detect the port and attack them.

### Detect Tear Drop Attack

- Can detect the IP data packets which pretend the normal data packets, but actually this kind of packets contain the mount of data packets, which can let the system crash, hold on or reboot.



### Filter IP Route Option

- Select the function can prevent some IP packets which the hacker use it to enter the domain.

### Detect Land Attack

- Select this function can prevent the data packets which includes the source port as the same as destination port. Or this kind of packets has the SYN characters in TCP packets header.



When the MIS engineer enable the **Anomaly Flow IP** function, the MH-2001 will instantly show the message in **Virus-infected IP** and **Attack Events**. If the MIS engineers enable the function in **System → E-mail alert notification**, then the MH-2001 will automatically send the notification to the MIS engineer.

## To alert and block the external or internal anomalous data packets.

### STEP 1 . In Anomaly IP → Setting :

- The threshold sessions of virus-infected is (default is 30 sessions/sec)
- Select **Enable Virus-infected IP Blocking** (Blocking Time 600 seconds)
- Select **Enable E-Mail Alert Notification**.
- Select **Enable NetBIOS Alert Notification**.
- Enter 192.168.89.30 in IP Address of Administrator.
- Enable all the function in DoS / Anti-Attack Setting.
- Click OK.

Virus-infected IP Setting	
The threshold sessions of virus-infected (per source IP) is <input type="text" value="30"/> Sessions / Sec ( Range: 1 - 9999 )	
<input checked="" type="checkbox"/> Enable Virus-infected IP Blocking	Blocking Time <input type="text" value="600"/> seconds ( Range: 1 - 999 )
<input checked="" type="checkbox"/> Enable E-Mail Alert Notification	
<input checked="" type="checkbox"/> Enable NetBIOS Alert Notification	IP Address of Administrator <input type="text" value="192.168.189.30"/>

DoS / Anti-Attack Setting	
<input checked="" type="checkbox"/> Sasser Block	<input checked="" type="checkbox"/> MSBlaster Block
<input checked="" type="checkbox"/> Code Red Block	<input checked="" type="checkbox"/> Nimda Block
<input checked="" type="checkbox"/> Detect SYN Attack	SYN Flood Threshold (Total) <input type="text" value="200"/> Pkts/Sec ( Range: 0 - 9999 )
	SYN Flood Threshold (Per Source IP) <input type="text" value="50"/> Pkts/Sec ( Range: 0 - 9999 )
	SYN Flood Threshold Blocking Time (Per Source IP) <input type="text" value="60"/> Seconds ( Range: 0 - 9999 )
<input checked="" type="checkbox"/> Detect ICMP Flood	ICMP Flood Threshold (Total) <input type="text" value="1000"/> Pkts/Sec ( Range: 0 - 9999 )
	ICMP Flood Threshold (Per Source IP) <input type="text" value="300"/> Pkts/Sec ( Range: 0 - 9999 )
	ICMP Flood Threshold Blocking Time (Per Source IP) <input type="text" value="60"/> Seconds ( Range: 0 - 9999 )
<input checked="" type="checkbox"/> Detect UDP Flood	UDP Flood Threshold (Total) <input type="text" value="1000"/> Pkts/Sec ( Range: 0 - 9999 )
	UDP Flood Threshold (Per Source IP) <input type="text" value="300"/> Pkts/Sec ( Range: 0 - 9999 )
	UDP Flood Threshold Blocking Time (Per Source IP) <input type="text" value="60"/> Seconds ( Range: 0 - 9999 )
<input checked="" type="checkbox"/> Detect Ping of Death Attack	<input checked="" type="checkbox"/> Detect Tear Drop Attack
<input checked="" type="checkbox"/> Detect IP Spoofing Attack	<input checked="" type="checkbox"/> Filter IP Route Option
<input checked="" type="checkbox"/> Detect Port Scan Attack	<input checked="" type="checkbox"/> Detect Land Attack

Non-detected IP		
Interface	IP Address / Netmask	Configure
LAN	192.168.1.2 / 255.255.255.255	<input type="button" value="Modify"/> <input type="button" value="Remove"/>

### The setting of anomaly flow IP and Dos / Anti-Attack

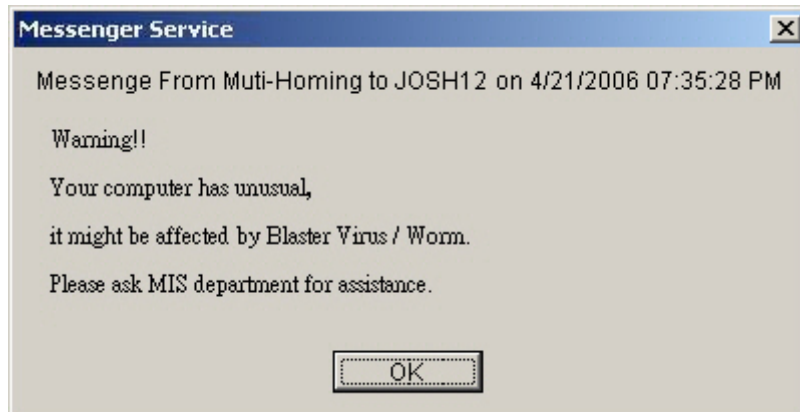


You can add **Non-detected IP**, and these IP will not controlled by this function.

**STEP 2 .** When the system detects the DDoS attack packets, it will show the message in **Anomaly Flow IP → Virus-infected IP**. Or send the Net BIOS Notification to the MIS and virus-infected PC.

Threshold Sessions / Sec : 30		
Interface	Virus-infected IP	Alarm Time
LAN	192.168.1.2	08/17 23:37:08

**Anomaly flow IP and Virus-infected IP**

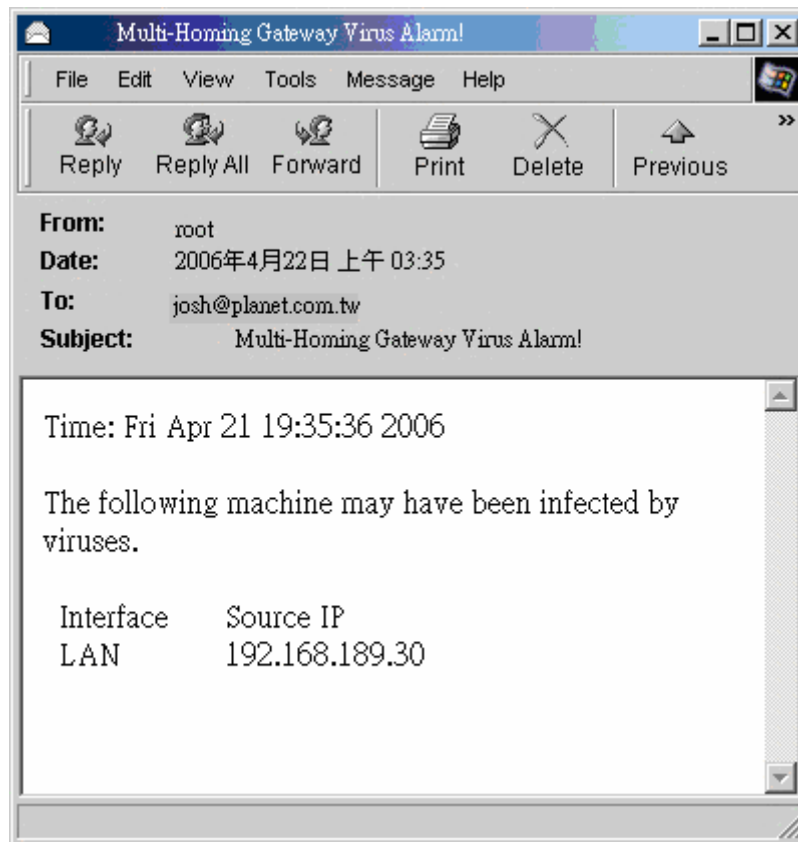


**Send the NetBIOS Alert notification to the virus-infected PC**



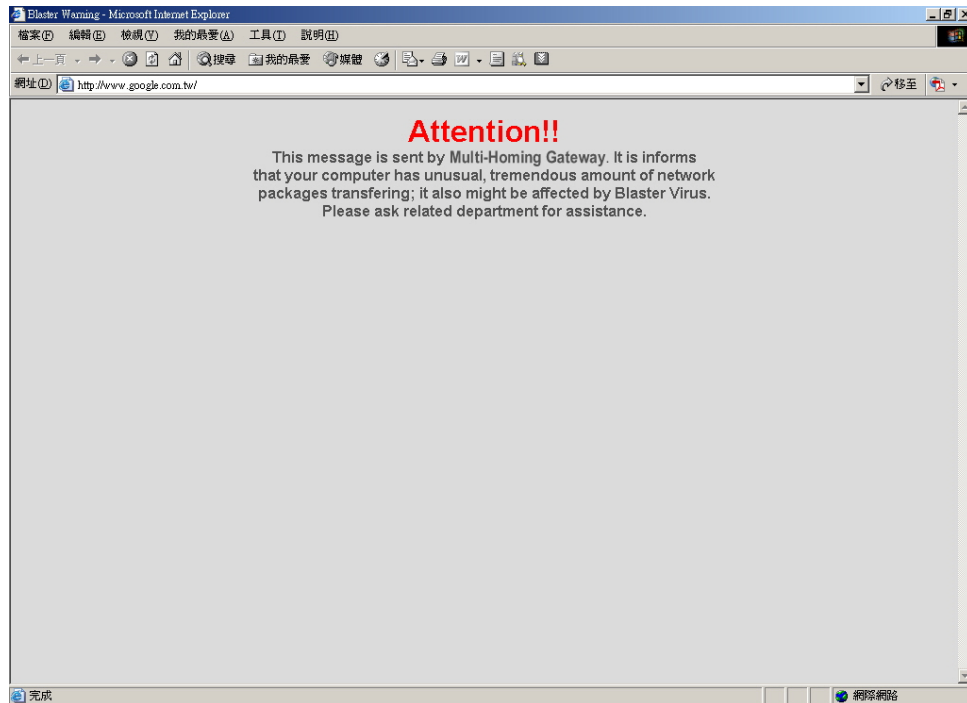
**Send the NetBIOS Alert Notification to the MIS engineer**

**STEP 3 .** Enable the **System → E-Mail alert notification**, and then the MH-2001 will send the mail notice to the MIS engineer.



**Send the e-mail alert notification**

**STEP 4 .** When internal user PC got virus – infected, the MH-2001 will show the alert message at first time (If the virus-infected user can not solve the problem then the MH-2001 will restrict the virus-infected user and it will make the link speed slow and will not show any alert message again).



**Show the alert message**

**STEP 5 .** Enable the **Anomaly Flow IP→Attack Event**, then the MH-2001 shows the attack information in detail.

Apr 13 18:15:49 ▼

Time	Event
Apr 13 18:15:49	The system has detected the attack of TCP port scan , suspected to be 58.24.126.97
Apr 13 18:15:40	The system has detected the attack of TCP port scan , suspected to be 58.24.126.97

Clear Alarm

Download Alarm

**Anomaly Flow IP attack event**

## Chapter 9: Monitor

### 9.1 Log

MH-2001 supports traffic logging and event logging to monitor and record services, connection times, and the source and destination network address. The Administrator may also download the log files for backup purposes. The Administrator mainly uses the Log menu to monitor the traffic passing through MH-2001.

#### What is Log?

Log records all connections that pass through MH-2001's control policies.

- **Traffic** : Traffic log's parameters are setup when setting up control policies. Traffic logs record the details of packets such as the start and stop time of connection, the duration of connection, the source address, the destination address and services requested, for each control policy.
- **Event** : Event logs record the contents of System Configuration changes made by the Administrator such as the time of change, settings that change, the IP address used to log on, etc.
- **Connection** : Record all the MH-2001 connecting information. MIS engineer can easily to know the status depends on the connecting information when the problems happened.

#### How to use the Monitor

- **Traffic**, MIS engineer can view the connection status includes time, source IP, destination IP and disposition. MH-2001 can backup the traffic log and refresh the online record on specific time period.
- **Event**, if MH-2001 detected some events happened, MIS engineer can know the events description and backup it.
- **Connection**, can record the connection status by this function.
- **Log Backup**, MIS engineer can set the MH-2001 to automatically send the email alarm of traffic and events or instantly send the log to syslog server.

The Administrator can use the log data to monitor and manage the device and the networks. The Administrator can view the logged data to evaluate and troubleshoot the network, such as pinpointing the source of traffic congestions.

### 9.1.1 Traffic Log

The Administrator queries MH-2001 for information, such as source address, destination address, start time, and Protocol port of all connections.

#### Enter to the Traffic Log window

Step 1. Click the **Traffic Log** option under **Log** menu to enter the Traffic Log window.

Monitor > Log > Traffic

Next

Time	Source	Destination	Protocol	Port	Disposition
Apr 14 10:55:05	211.75.117.114	210.66.155.77	TCP	1633 => 8080	✓
Apr 14 10:55:05	211.75.117.114	210.66.155.77	TCP	1632 => 8080	✓
Apr 14 10:55:05	211.75.117.114	210.66.155.77	TCP	1631 => 8080	✓
Apr 14 10:50:41	211.75.117.114	210.66.155.77	TCP	1614 => 8080	✓
Apr 14 10:50:41	211.75.117.114	210.66.155.77	TCP	1613 => 8080	✓
Apr 14 10:50:40	211.75.117.114	210.66.155.77	TCP	1612 => 8080	✓
Apr 14 10:50:18	219.132.138.237	210.66.155.77	TCP	1724 => 8080	✓
Apr 14 10:50:17	219.132.138.237	210.66.155.77	TCP	1716 => 8080	✓
Apr 14 10:50:15	219.132.138.237	210.66.155.77	TCP	1548 => 8080	✓
Apr 14 10:50:15	219.132.138.237	210.66.155.77	TCP	1521 => 8080	✓
Apr 14 10:50:05	219.132.138.237	210.66.155.77	TCP	4301 => 8080	✓
Apr 14 10:50:05	219.132.138.237	210.66.155.77	TCP	4223 => 8080	✓
Apr 14 10:50:04	219.132.138.237	210.66.155.77	TCP	4103 => 8080	✓
Apr 14 10:50:04	219.132.138.237	210.66.155.77	TCP	4046 => 8080	✓
Apr 14 10:50:00	219.132.138.237	210.66.155.77	TCP	3462 => 8080	✓
Apr 14 10:50:00	219.132.138.237	210.66.155.77	TCP	2901 => 8080	✓
Apr 14 10:49:59	219.132.138.237	210.66.155.77	TCP	3236 => 8080	✓
Apr 14 10:49:59	219.132.138.237	210.66.155.77	TCP	3148 => 8080	✓

Clear Logs Download Logs

#### Traffic Log Table

The table in the Traffic Log window displays current System statuses:

##### Definition:

- **Time:** The start time of the connection.
- **Source:** IP address of the source network of the specific connection.
- **Destination:** IP address of the destination network of the specific connection.
- **Protocol:** Protocol type of the specific connection.
- **Port:** Port number of the specific connection.
- **Disposition:** Accept or Deny.

#### Download the Traffic Logs

The Administrator can backup the traffic logs regularly by downloading it to the computer.

Step 1. In the Traffic Log window, click the **Download Logs** button at the bottom of the screen.



Step 2. Follow the File Download pop-up window to save the traffic logs into a specified directory on the hard drive.

Monitor > Log > Traffic

System

traffic[1].log - 記事本

檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)

Time	Source	Destination	Protocol	Port	Disposition
Jan 31 16:03:23 2006	211.75.117.114	210.66.155.77	TCP	1740 8080	✓
Jan 31 16:03:26 2006	211.75.117.114	210.66.155.77	TCP	1741 8080	✓
Jan 31 16:03:28 2006	211.75.117.114	210.66.155.77	TCP	1742 8080	✓
Jan 31 16:03:41 2006	192.168.1.3	192.168.1.1	TCP	1583 80	✓
Jan 31 16:03:42 2006	192.168.1.3	192.168.1.1	TCP	1584 80	✓
Jan 31 16:03:42 2006	192.168.1.3	192.168.1.1	TCP	1585 80	✓
Jan 31 16:03:42 2006	192.168.1.3	192.168.1.1	TCP	1584 80	✓
Jan 31 16:03:42 2006	192.168.1.3	192.168.1.1	TCP	1585 80	✓
Jan 31 16:03:43 2006	192.168.1.3	192.168.1.1	TCP	1584 80	✓
Jan 31 16:03:43 2006	192.168.1.3	192.168.1.1	TCP	1585 80	✓
Jan 31 16:03:44 2006	192.168.1.3	192.168.1.1	TCP	1586 80	✓
Jan 31 16:03:45 2006	192.168.1.3	192.168.1.1	TCP	1587 80	✓
Jan 31 16:03:45 2006	192.168.1.3	192.168.1.1	TCP	1588 80	✓
Jan 31 16:03:46 2006	192.168.1.3	192.168.1.1	TCP	1587 80	✓
Jan 31 16:03:46 2006	192.168.1.3	192.168.1.1	TCP	1588 80	✓
Jan 31 16:03:46 2006	192.168.1.3	192.168.1.1	TCP	1588 80	✓
Jan 31 16:03:46 2006	192.168.1.3	192.168.1.1	TCP	1589 80	✓
Apr 14 10:49:59	219.132.138.237	210.66.155.77	TCP	1633 => 8080	✓
Apr 14 10:49:59	219.132.138.237	210.66.155.77	TCP	1632 => 8080	✓
Apr 14 10:49:59	219.132.138.237	210.66.155.77	TCP	1631 => 8080	✓
Apr 14 10:49:59	219.132.138.237	210.66.155.77	TCP	1614 => 8080	✓
Apr 14 10:49:59	219.132.138.237	210.66.155.77	TCP	1613 => 8080	✓
Apr 14 10:49:59	219.132.138.237	210.66.155.77	TCP	1612 => 8080	✓
Apr 14 10:49:59	219.132.138.237	210.66.155.77	TCP	1724 => 8080	✓
Apr 14 10:49:59	219.132.138.237	210.66.155.77	TCP	1716 => 8080	✓
Apr 14 10:49:59	219.132.138.237	210.66.155.77	TCP	1548 => 8080	✓
Apr 14 10:49:59	219.132.138.237	210.66.155.77	TCP	1521 => 8080	✓
Apr 14 10:49:59	219.132.138.237	210.66.155.77	TCP	4301 => 8080	✓
Apr 14 10:49:59	219.132.138.237	210.66.155.77	TCP	4223 => 8080	✓
Apr 14 10:49:59	219.132.138.237	210.66.155.77	TCP	4103 => 8080	✓
Apr 14 10:49:59	219.132.138.237	210.66.155.77	TCP	4046 => 8080	✓
Apr 14 10:49:59	219.132.138.237	210.66.155.77	TCP	3462 => 8080	✓
Apr 14 10:49:59	219.132.138.237	210.66.155.77	TCP	2901 => 8080	✓
Apr 14 10:49:59	219.132.138.237	210.66.155.77	TCP	3236 => 8080	✓
Apr 14 10:49:59	219.132.138.237	210.66.155.77	TCP	3148 => 8080	✓

Clear Logs Download Logs

### Clear the Traffic Logs

The Administrator may clear on-line logs to keep just the most updated logs on the screen.

Step 1. In the Traffic Log window, click the **Clear Logs** button at the bottom of the screen.

Step 2. In the Clear Logs pop-up box, click **Ok** to clear the logs or click **Cancel** to cancel it.

Monitor > Log > Traffic

System

Interface

Policy Object

Policy

Anomaly Flow IP

Monitor

Log

Traffic

Event

Connection

Log Backup

Accounting Report

Statistics

Wake on Lan

Status

Time	Source	Destination	Protocol	Port	Disposition
Apr 14 10:55:05	211.75.117.114	210.66.155.77	TCP	1633 => 8080	✓
Apr 14 10:55:05	211.75.117.114	210.66.155.77	TCP	1632 => 8080	✓
Apr 14 10:55:05	211.75.117.114	210.66.155.77	TCP	1631 => 8080	✓
Apr 14 10:50:41	211.75.117.114	210.66.155.77	TCP	1614 => 8080	✓
Apr 14 10:50:41	211.75.117.114	210.66.155.77	TCP	1613 => 8080	✓
Apr 14 10:50:40	211.75.117.114	210.66.155.77	TCP	1612 => 8080	✓
Apr 14 10:50:18	219.132.138.237	210.66.155.77	TCP	1724 => 8080	✓
Apr 14 10:50:17	219.132.138.237	210.66.155.77	TCP	1716 => 8080	✓
Apr 14 10:50:15	219.132.138.237	210.66.155.77	TCP	1548 => 8080	✓
Apr 14 10:50:15	219.132.138.237	210.66.155.77	TCP	1521 => 8080	✓
Apr 14 10:50:05	219.132.138.237	210.66.155.77	TCP	4301 => 8080	✓
Apr 14 10:50:05	219.132.138.237	210.66.155.77	TCP	4223 => 8080	✓
Apr 14 10:50:04	219.132.138.237	210.66.155.77	TCP	4103 => 8080	✓
Apr 14 10:50:04	219.132.138.237	210.66.155.77	TCP	4046 => 8080	✓
Apr 14 10:50:00	219.132.138.237	210.66.155.77	TCP	3462 => 8080	✓
Apr 14 10:50:00	219.132.138.237	210.66.155.77	TCP	2901 => 8080	✓
Apr 14 10:49:59	219.132.138.237	210.66.155.77	TCP	3236 => 8080	✓
Apr 14 10:49:59	219.132.138.237	210.66.155.77	TCP	3148 => 8080	✓

Clear Logs Download Logs

Microsoft Internet Explorer

Do you really want to delete?

OK Cancel

## 9.1.2 Event

When MH-2001 WAN detects events, the Administrator can get the details, such as time and description of the events from the Event Logs.

### Enter to the Event Log window

Step 1. Click the **Event Log** option under the **Log** menu and the Event Log window will appear.

Time	Event
Apr 14 11:25:35	user admin [Login success] from 211.75.117.114
Apr 14 11:00:01	user admin [Login success] from 211.75.117.114
Apr 14 10:57:29	user admin [Login success] from 211.75.117.114
Apr 14 10:55:05	user admin [Login success] from 211.75.117.114
Apr 14 10:50:40	user admin [Login success] from 211.75.117.114
Apr 14 10:47:11	user admin [Login success] from 211.75.117.114
Apr 14 10:45:47	user admin [Login success] from 211.75.117.114
Apr 14 10:45:43	user admin [Login success] from 211.75.117.114
Apr 14 10:44:13	user admin [Login success] from 211.75.117.114
Apr 14 10:32:38	(null) Modify [Setting] from 211.75.117.114
Apr 14 10:06:21	(null) Modify [Policy](DMZ to Internal,Mail_Server=>Inside_Any,Mail_service,permit) from 211.75.117.114
Apr 14 10:04:37	(null) Modify [Policy](DMZ to External,Mail_Server=>Outside_Any,Mail_service,permit) from 211.75.117.114
Apr 14 09:59:42	(null) Modify [Policy](Internal to DMZ,Inside_Any=>Mail_Server,Mail_service,permit) from 211.75.117.114
Apr 14 09:57:18	(null) Modify [Policy](External to DMZ,Outside_Any=>Mail_Server(Routing),Mail_service,permit) from 211.75.117.114
Apr 14 09:54:20	(null) Delete [Service Group] Main_service from 211.75.117.114
Apr 14 09:53:15	(null) Add [Address] Mail_Server from 211.75.117.114
Apr 14 09:52:30	(null) Delete [Address] DMZ_user2 from 211.75.117.114
Apr 14 09:52:23	(null) Delete [Address] DMZ_user3 from 211.75.117.114

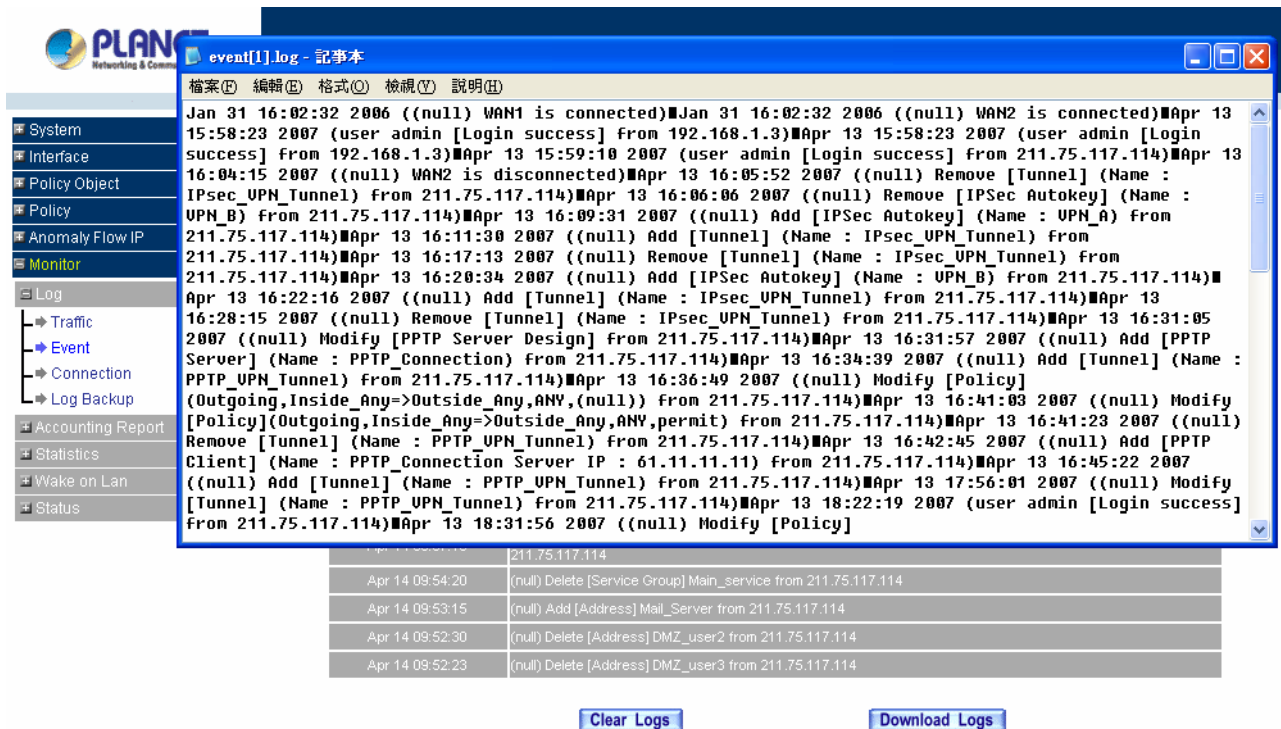
Step 2. The table in the Event Log window displays the time and description of the events.

- **Time:** time when the event occurred.
- **Event:** description of the event.

### Download the Event Logs

Step 1. In the Event Log window, click the Download Logs button at the bottom of the screen.

Step 2. Follow the File Download pop-up window to save the event logs into a specific directory on the hard drive.



event[1].log - 記事本

檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)

Jan 31 16:02:32 2006 ((null) WAN1 is connected)■Jan 31 16:02:32 2006 ((null) WAN2 is connected)■Apr 13 15:58:23 2007 (user admin [Login success] from 192.168.1.3)■Apr 13 15:58:23 2007 (user admin [Login success] from 192.168.1.3)■Apr 13 15:59:10 2007 (user admin [Login success] from 211.75.117.114)■Apr 13 16:04:15 2007 ((null) WAN2 is disconnected)■Apr 13 16:05:52 2007 ((null) Remove [Tunnel] (Name : IPsec\_UPN\_Tunnel) from 211.75.117.114)■Apr 13 16:06:06 2007 ((null) Remove [IPSec Autokey] (Name : UPN\_B) from 211.75.117.114)■Apr 13 16:09:31 2007 ((null) Add [IPSec Autokey] (Name : UPN\_A) from 211.75.117.114)■Apr 13 16:11:30 2007 ((null) Add [Tunnel] (Name : IPsec\_UPN\_Tunnel) from 211.75.117.114)■Apr 13 16:17:13 2007 ((null) Remove [Tunnel] (Name : IPsec\_UPN\_Tunnel) from 211.75.117.114)■Apr 13 16:20:34 2007 ((null) Add [IPSec Autokey] (Name : UPN\_B) from 211.75.117.114)■Apr 13 16:22:16 2007 ((null) Add [Tunnel] (Name : IPsec\_UPN\_Tunnel) from 211.75.117.114)■Apr 13 16:28:15 2007 ((null) Remove [Tunnel] (Name : IPsec\_UPN\_Tunnel) from 211.75.117.114)■Apr 13 16:31:05 2007 ((null) Modify [PPTP Server Design] from 211.75.117.114)■Apr 13 16:31:57 2007 ((null) Add [PPTP Server] (Name : PPTP\_Connection) from 211.75.117.114)■Apr 13 16:34:39 2007 ((null) Add [Tunnel] (Name : PPTP\_UPN\_Tunnel) from 211.75.117.114)■Apr 13 16:36:49 2007 ((null) Modify [Policy] (Outgoing,Inside\_Any=>Outside\_Any,ANY,(null)) from 211.75.117.114)■Apr 13 16:41:03 2007 ((null) Modify [Policy](Outgoing,Inside\_Any=>Outside\_Any,ANY,permit) from 211.75.117.114)■Apr 13 16:41:23 2007 ((null) Remove [Tunnel] (Name : PPTP\_UPN\_Tunnel) from 211.75.117.114)■Apr 13 16:42:45 2007 ((null) Add [PPTP Client] (Name : PPTP\_Connection Server IP : 61.11.11.11) from 211.75.117.114)■Apr 13 16:45:22 2007 ((null) Add [Tunnel] (Name : PPTP\_UPN\_Tunnel) from 211.75.117.114)■Apr 13 17:56:01 2007 ((null) Modify [Tunnel] (Name : PPTP\_UPN\_Tunnel) from 211.75.117.114)■Apr 13 18:22:19 2007 (user admin [Login success] from 211.75.117.114)■Apr 13 18:31:56 2007 ((null) Modify [Policy]

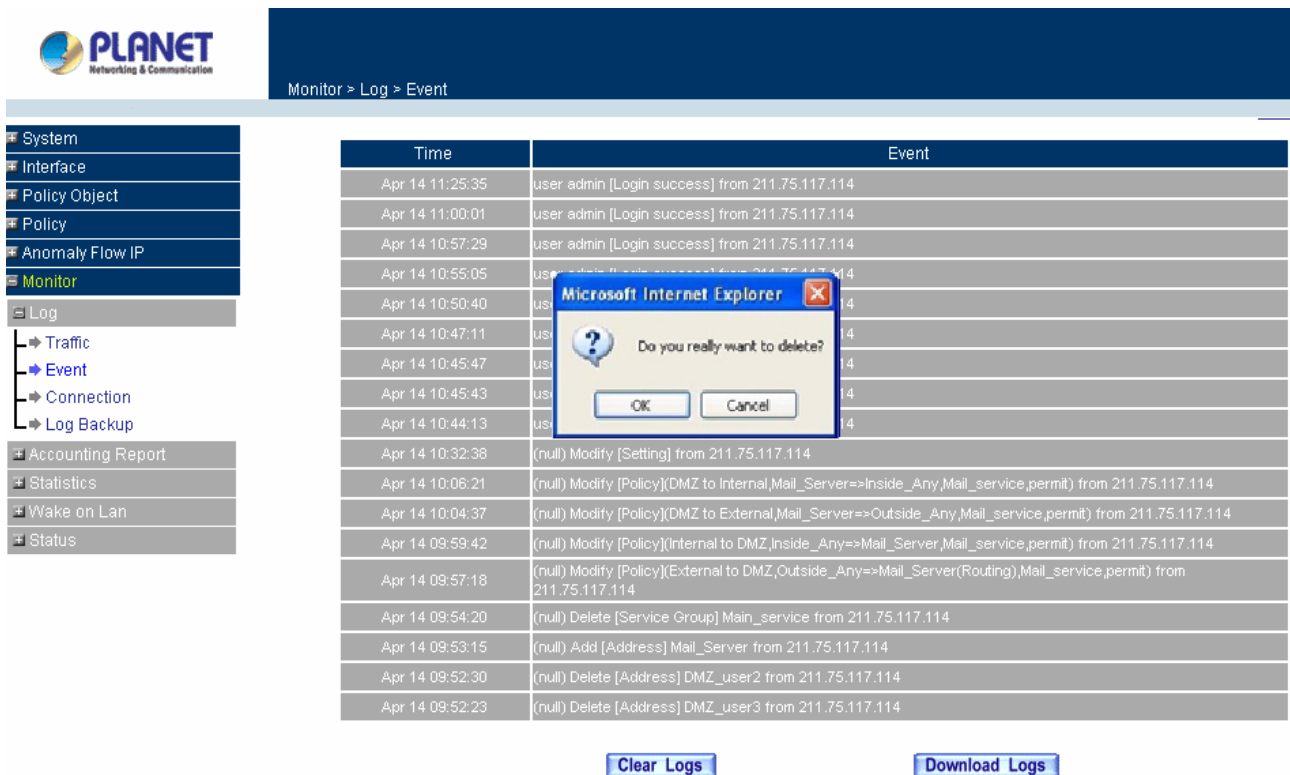
Time	Event
Apr 14 09:54:20	((null) Delete [Service Group] Main_service from 211.75.117.114
Apr 14 09:53:15	((null) Add [Address] Mail_Server from 211.75.117.114
Apr 14 09:52:30	((null) Delete [Address] DMZ_user2 from 211.75.117.114
Apr 14 09:52:23	((null) Delete [Address] DMZ_user3 from 211.75.117.114

Clear Logs Download Logs

### Clear the Event Logs

The Administrator may clear on-line event logs to keep just the most updated logs on the screen.

- Step 1. In the Event Log window, click the Clear Logs button at the bottom of the screen.
- Step 2. In the Clear Logs pop-up box, click **OK** to clear the logs or click **Cancel** to cancel it.



Monitor > Log > Event

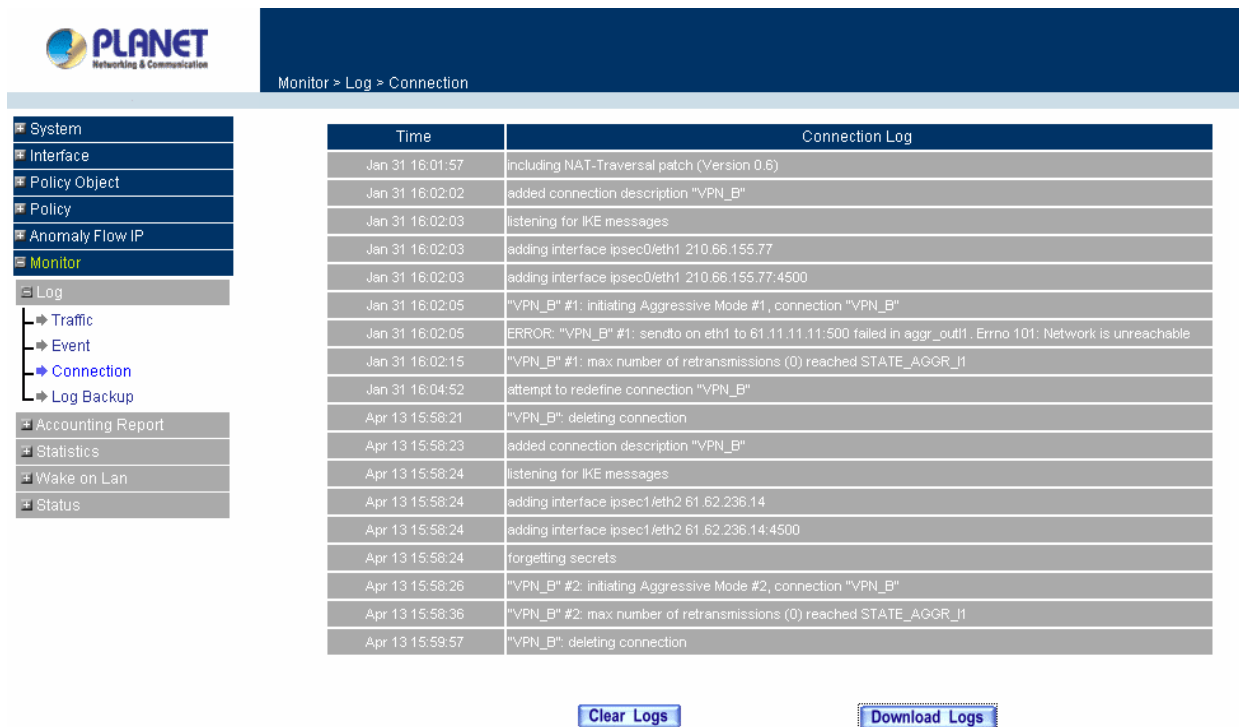
Time	Event
Apr 14 11:25:35	user admin [Login success] from 211.75.117.114
Apr 14 11:00:01	user admin [Login success] from 211.75.117.114
Apr 14 10:57:29	user admin [Login success] from 211.75.117.114
Apr 14 10:55:05	user admin [Login success] from 211.75.117.114
Apr 14 10:50:40	user admin [Login success] from 211.75.117.114
Apr 14 10:47:11	user admin [Login success] from 211.75.117.114
Apr 14 10:45:47	user admin [Login success] from 211.75.117.114
Apr 14 10:45:43	user admin [Login success] from 211.75.117.114
Apr 14 10:44:13	user admin [Login success] from 211.75.117.114
Apr 14 10:32:38	((null) Modify [Setting] from 211.75.117.114
Apr 14 10:06:21	((null) Modify [Policy](DMZ to Internal,Mail_Server=>Inside_Any,Mail_service,permit) from 211.75.117.114
Apr 14 10:04:37	((null) Modify [Policy](DMZ to External,Mail_Server=>Outside_Any,Mail_service,permit) from 211.75.117.114
Apr 14 09:59:42	((null) Modify [Policy](Internal to DMZ,Inside_Any=>Mail_Server,Mail_service,permit) from 211.75.117.114
Apr 14 09:57:18	((null) Modify [Policy](External to DMZ,Outside_Any=>Mail_Server(Routing),Mail_service,permit) from 211.75.117.114
Apr 14 09:54:20	((null) Delete [Service Group] Main_service from 211.75.117.114
Apr 14 09:53:15	((null) Add [Address] Mail_Server from 211.75.117.114
Apr 14 09:52:30	((null) Delete [Address] DMZ_user2 from 211.75.117.114
Apr 14 09:52:23	((null) Delete [Address] DMZ_user3 from 211.75.117.114

Clear Logs Download Logs

### 9.1.3 Connection Log

#### Enter to the Connection Log window

Step 1. Click the **Connection** option under the **Log** menu and the Connection Log window will appear.



Monitor > Log > Connection

Time	Connection Log
Jan 31 16:01:57	including NAT-Traversal patch (Version 0.6)
Jan 31 16:02:02	added connection description "VPN_B"
Jan 31 16:02:03	listening for IKE messages
Jan 31 16:02:03	adding interface ipsec0/eth1 210.66.155.77
Jan 31 16:02:03	adding interface ipsec0/eth1 210.66.155.77:4500
Jan 31 16:02:05	"VPN_B" #1: Initiating Aggressive Mode #1, connection "VPN_B"
Jan 31 16:02:05	ERROR: "VPN_B" #1: sendto on eth1 to 61.11.11.11:500 failed in aggr_out1. Errno 101: Network is unreachable
Jan 31 16:02:15	"VPN_B" #1: max number of retransmissions (0) reached STATE_AGGR_I1
Jan 31 16:04:52	attempt to redefine connection "VPN_B"
Apr 13 15:58:21	"VPN_B": deleting connection
Apr 13 15:58:23	added connection description "VPN_B"
Apr 13 15:58:24	listening for IKE messages
Apr 13 15:58:24	adding interface ipsec1/eth2 61.62.236.14
Apr 13 15:58:24	adding interface ipsec1/eth2 61.62.236.14:4500
Apr 13 15:58:24	forgetting secrets
Apr 13 15:58:26	"VPN_B" #2: Initiating Aggressive Mode #2, connection "VPN_B"
Apr 13 15:58:36	"VPN_B" #2: max number of retransmissions (0) reached STATE_AGGR_I1
Apr 13 15:59:57	"VPN_B": deleting connection

Clear Logs Download Logs

#### Definition:

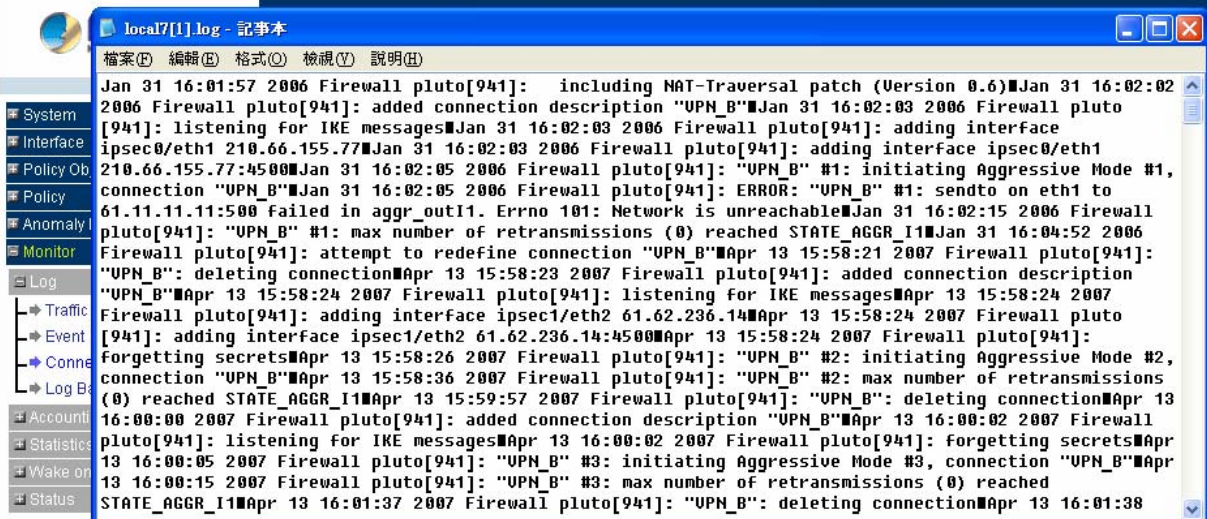
**Time:** The start and end time of connection.

**Connection Log:** Event description during connection.

#### Download Connection Logs

Step 1. In Connection Log window, click the **Download Logs** button.

Step 2. In the Download Logs window, save the logs to the specified location.

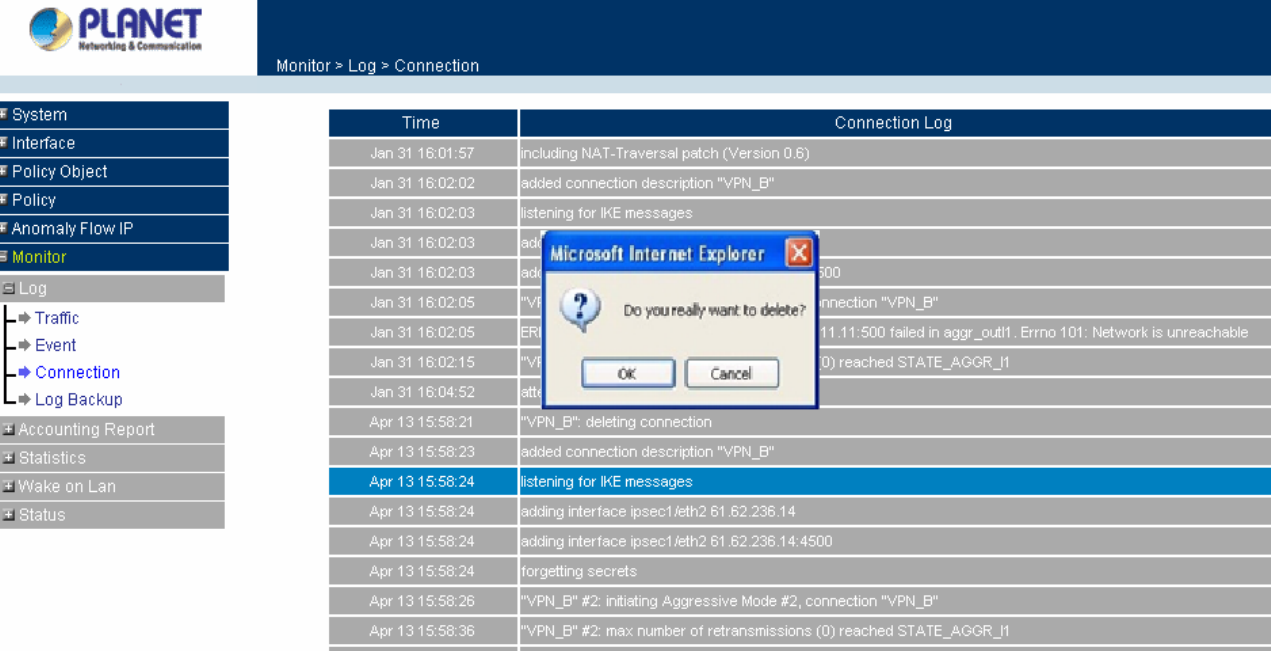


Apr 13 15:58:24	forgetting secrets
Apr 13 15:58:26	"VPN_B" #2: initiating Aggressive Mode #2, connection "VPN_B"
Apr 13 15:58:36	"VPN_B" #2: max number of retransmissions (0) reached STATE_AGGR_I1
Apr 13 15:59:57	"VPN_B": deleting connection

[Clear Logs](#)
[Download Logs](#)

## Clear Connection Logs

- Step 1. In Connection Log window, click the **Clear Logs** button.
- Step 2. In Clear Logs window, click **OK** to clear the logs or click **Cancel** to discard changes.

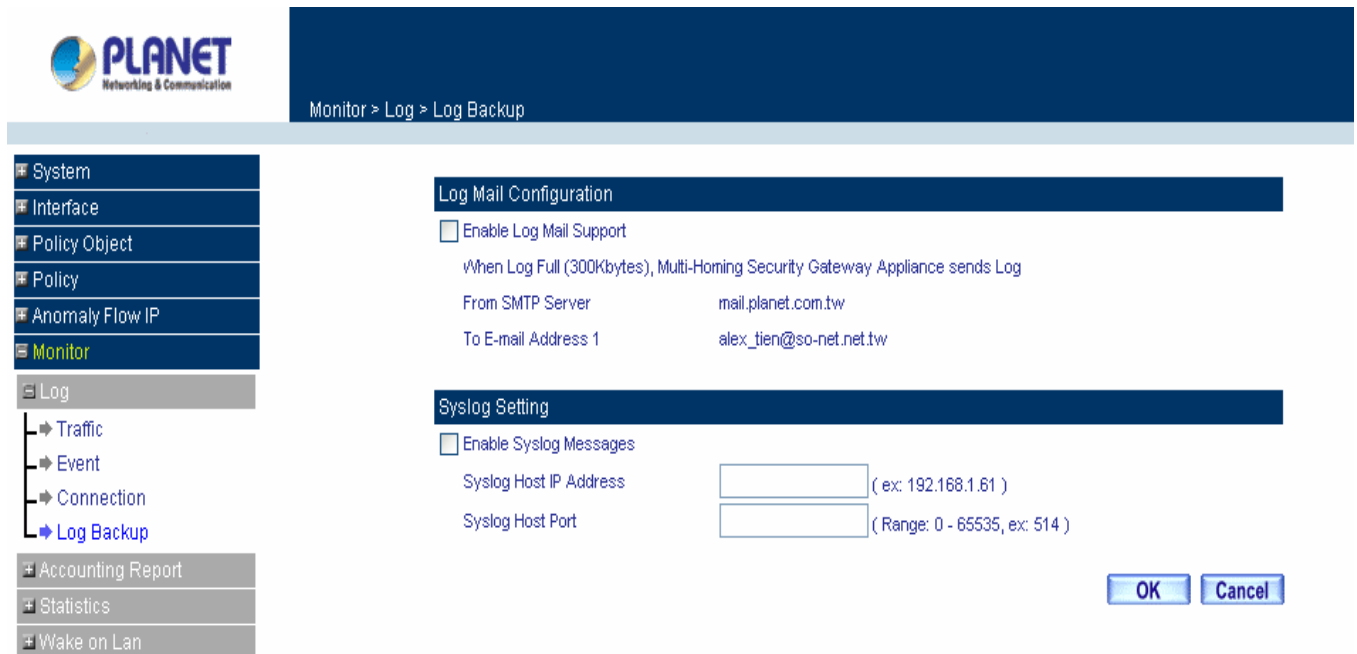


Time	Connection Log
Jan 31 16:01:57	including NAT-Traversal patch (Version 0.6)
Jan 31 16:02:02	added connection description "VPN_B"
Jan 31 16:02:03	listening for IKE messages
Jan 31 16:02:03	ad
Jan 31 16:02:03	ad
Jan 31 16:02:05	"V
Jan 31 16:02:05	ER
Jan 31 16:02:15	"V
Jan 31 16:04:52	att
Apr 13 15:58:21	"VPN_B": deleting connection
Apr 13 15:58:23	added connection description "VPN_B"
Apr 13 15:58:24	listening for IKE messages
Apr 13 15:58:24	adding interface ipsec1/eth2 61.62.236.14
Apr 13 15:58:24	adding interface ipsec1/eth2 61.62.236.14:4500
Apr 13 15:58:24	forgetting secrets
Apr 13 15:58:26	"VPN_B" #2: initiating Aggressive Mode #2, connection "VPN_B"
Apr 13 15:58:36	"VPN_B" #2: max number of retransmissions (0) reached STATE_AGGR_I1
Apr 13 15:59:57	"VPN_B": deleting connection

### 9.1.4 Log Backup

#### Enter to the Log Backup window

Click **Log** → **Log Backup**.



The screenshot shows the Planet Multi-Homing Security Gateway web interface. The left sidebar contains a menu with options: System, Interface, Policy Object, Policy, Anomaly Flow IP, Monitor, Log, Accounting Report, Statistics, and Wake on Lan. The 'Log' menu is expanded, showing sub-options: Traffic, Event, Connection, and Log Backup. The 'Log Backup' option is selected. The main content area displays the 'Log Mail Configuration' and 'Syslog Setting' sections.

**Log Mail Configuration**

☐ Enable Log Mail Support

When Log Full (300Kbytes), Multi-Homing Security Gateway Appliance sends Log

From SMTP Server: mail.planet.com.tw

To E-mail Address 1: alex\_tien@so-net.net.tw

**Syslog Setting**

☐ Enable Syslog Messages

Syslog Host IP Address: ( ex: 192.168.1.61 )

Syslog Host Port: ( Range: 0 - 65535, ex: 514 )

OK Cancel

- **Log Mail Configuration:** When the Log Mail files accumulated up to 300Kbytes, router will notify administrator by email with the traffic log and event log.

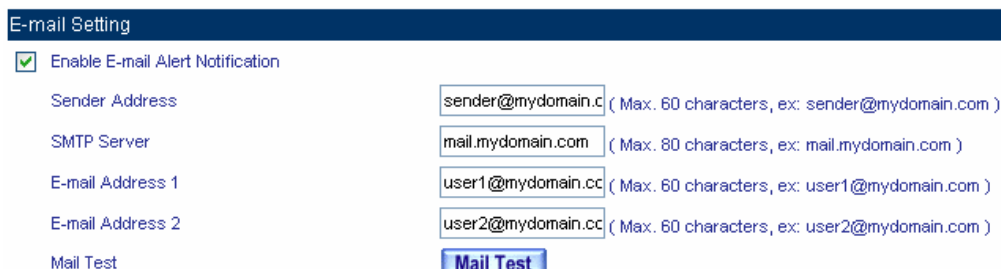


Before enabling this function, you have to configure E-mail Settings in **System -> Configure -> Settings**.

- **Syslog Settings:** If you enable this function, system will transmit the Traffic Log and the Event Log simultaneously to the server which supports Syslog function.

#### Enable Log Mail Support & Syslog Setting

**STEP 1 . System → Configure→Setting**, enable **E-mail Alert Notification** and enter the e-mail settings.



The screenshot shows the 'E-mail Setting' configuration window. It includes a checkbox for 'Enable E-mail Alert Notification' which is checked. Below this are fields for 'Sender Address', 'SMTP Server', 'E-mail Address 1', and 'E-mail Address 2'. Each field has a text input and a character limit note. At the bottom, there is a 'Mail Test' button.

**E-mail Setting**

☒ Enable E-mail Alert Notification

Sender Address: sender@mydomain.cc ( Max. 60 characters, ex: sender@mydomain.com )

SMTP Server: mail.mydomain.com ( Max. 80 characters, ex: mail.mydomain.com )

E-mail Address 1: user1@mydomain.cc ( Max. 60 characters, ex: user1@mydomain.com )

E-mail Address 2: user2@mydomain.cc ( Max. 60 characters, ex: user2@mydomain.com )

Mail Test

#### E-mail setting

**STEP 2 . Monitor → Backup → enable Log mail Configuration. Click OK.**



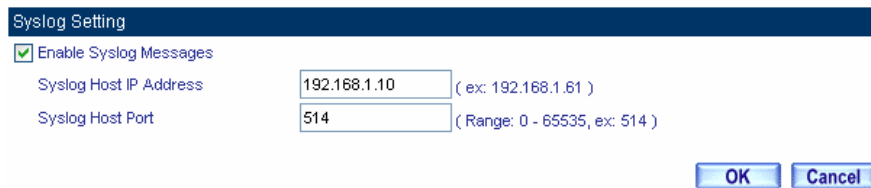
The 'Log Mail Configuration' dialog box has a title bar 'Log Mail Configuration'. It contains a checked checkbox 'Enable Log Mail Support'. Below it is a note: 'When Log Full (300Kbytes), Multi-Homing Security Gateway Appliance sends Log'. There are three rows of configuration fields: 'From SMTP Server' with value 'mail.mydomain.com', 'To E-mail Address 1' with value 'user1@mydomain.com', and 'E-mail Address 2' with value 'user2@mydomain.com'.

From SMTP Server	mail.mydomain.com
To E-mail Address 1	user1@mydomain.com
E-mail Address 2	user2@mydomain.com

### Log mail configuration

**STEP 3 . Monitor→ Backup → Syslog setting :**

- Select **Enable Syslog Messages**.
- Enter the IP in **Syslog host IP address**.
- Enter the Syslog receive Port number in **Syslog host Port**.
- Click OK.
- Complete the setting.



The 'Syslog Setting' dialog box has a title bar 'Syslog Setting'. It contains a checked checkbox 'Enable Syslog Messages'. Below it are two input fields: 'Syslog Host IP Address' with value '192.168.1.10' and a hint '( ex: 192.168.1.61 )', and 'Syslog Host Port' with value '514' and a hint '( Range: 0 - 65535, ex: 514 )'. At the bottom right are 'OK' and 'Cancel' buttons.

Syslog Host IP Address	192.168.1.10	( ex: 192.168.1.61 )
Syslog Host Port	514	( Range: 0 - 65535, ex: 514 )

### Syslog setting

## 9.2 Accounting Report

Administrator can use this Accounting Report to inquire the LAN IP users and WAN IP users, and to gather the statistics of **Downstream/Upstream**, **First packet/Last packet/Duration** and the **Service** of all the user's IP that passes the MH-2001.

Accounting Report can be divided into three parts, **Setting**, **Outbound Accounting Report**, and the **Inbound Accounting Report**.

### 9.2.1 Setting

#### Accounting Report Setting:

By accounting report function can record the sending information about Intranet and the external PC via MH-2001.

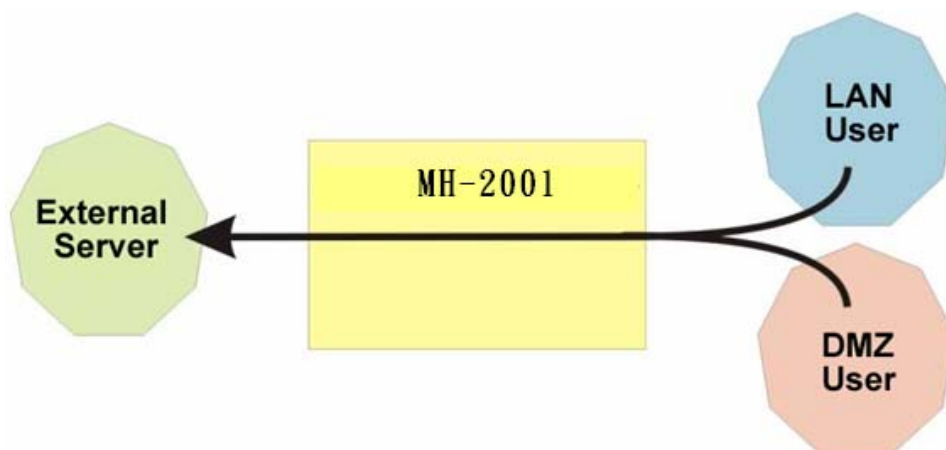
#### Enable Accounting Report Setting

**STEP 1** . In the **Monitor → Accounting Report → Setting**, the screen will show as below.



#### Define the required fields of Accounting Report

##### Outbound Accounting Report



It is the statistics of the downstream and upstream of the LAN, WAN and all kinds of communication network services



**Source IP :**

- The IP address used by LAN users who use MH-2001

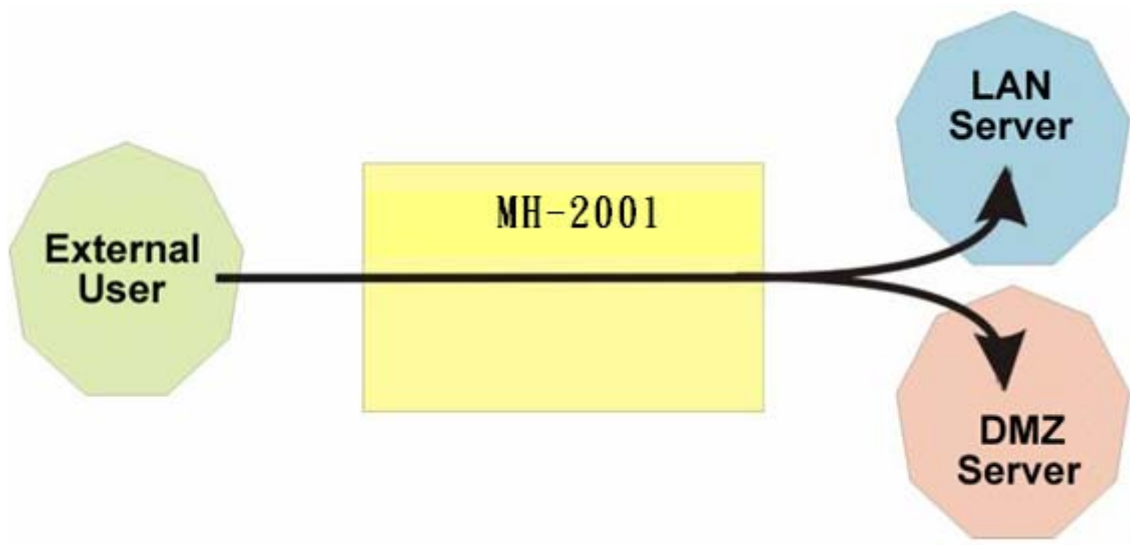
**Destination IP :**

- The IP address used by WAN service server which uses MH-2001.

**Service :**

- The communication service which listed in the menu when LAN users use MH-2001 to connect to WAN service server.

## Inbound Accounting Report



It is the statistics of downstream / upstream for all kinds of communication services; the Inbound Accounting report will be shown when WAN user uses MH-2001 to connect to LAN Service Server.

**Source IP :**

- The IP address used by WAN users who use MH-2001

**Destination IP :**

- The IP address used by LAN service server who use MH-2001

**Service :**

- The communication service which listed in the menu when WAN users use MH-2001 to connect to LAN Service server.

## 9.2.2 Outbound

**STEP 1** . Enter **Outbound** in **Accounting Report** and select **Top Users** to inquire the statistics of Send / Receive packets, **Downstream / Upstream, First packet/Last packet/Duration** and the service from the LAN or DMZ user's IP that pass the MH-2001.

- **TOP**: Select the data you want to view, it presents 10 results in one page.

### Pull-down menu selection

- **Source IP** : The IP address used by LAN users who use MH-2001 to connect to WAN service server.
- **Downstream** : The percentage of downstream and the value of each WAN service server which uses MH-2001 to LAN user.
- **Upstream** : The percentage of upstream and the value of each LAN user who uses MH-2001 to WAN service server.
- **First Packet** : When the first packet is sent to WAN service server from LAN user, the sent time will be recorded by the MH-2001.
- **Last Packet** : When the last packet sent from WAN service server is received by the LAN user, the sent time will be recorded by the MH-2001.
- **Duration** : The period of time which starts from the first packet to the last packet to be recorded.
- **Total Traffic** : The MH-2001 will record the sum of packet sent/receive time and show the percentage of each LAN user's upstream/downstream to WAN service server.
- **Reset Counter** : Click Reset Counter button to refresh Accounting Report.

Top: 1 - 2 ▼

Starting Time : Mon Jun 23 15:51:48 2008

No.	Source IP ▼	Downstream ▼		Upstream ▼		First Packet ▼	Last Packet ▼	Duration ▼	Action
1	10.0.0.10	3.2 MB	97.7 %	1.7 MB	99.4 %	06/23 15:52:37	06/24 09:59:19	18:06:42	<a href="#">Remove</a>
2	192.168.1.3	75.8 KB	2.3 %	10.0 KB	0.6 %	06/23 15:50:07	06/23 16:29:02	00:38:55	<a href="#">Remove</a>
Total Traffic		3.3 MB		1.7 MB		Reporting time Sat Apr 14 13:16:14 2007			

[Reset Counters](#)

### Outbound Source IP Statistics Report

**STEP 2 .** Enter **Outbound** in **Accounting Report** and select **Top Sites** to inquire the statistics website of Send/Receive packets, **Downstream/Upstream, First packet/Last packet/Duration** and the service from the WAN Server to pass the MH-2001.

- **TOP** : Select the data you want to view; it presents 10 results in one page.

**Pull-down menu selection**

- **Destination IP** : The IP address used by WAN service server which uses MH-2001.
- **Downstream** : The percentage of downstream and the value of each WAN service server which uses MH-2001 to LAN user.
- **Upstream** : The percentage of upstream and the value of each LAN user who uses MH-2001 to WAN service server.
- **First Packet** : When the first packet is sent from WAN service server to LAN users, the sent time will be recorded by the MH-2001.
- **Last Packet** : When the last packet from LAN user is sent to WAN service server, the sent time will be recorded by the MH-2001.
- **Duration** : The period of time which starts from the first packet to the last packet to be recorded.
- **Total Traffic** : The MH-2001 will record the sum of time and show the percentage of each WAN service server's upstream/downstream to LAN user.
- **Reset Counter Button** : Click Reset Counter button to refresh Accounting Report.

Top: 1 - 7 ▼

Starting Time : Mon Jun 23 15:51:48 2008


No.	Destination IP ▼	Downstream ▼		Upstream ▼		First Packet ▼	Last Packet ▼	Duration ▼	Action
1	210.66.155.70	3.2 MB	97.5%	1.7 MB	98.3%	06/23 15:52:37	06/24 09:59:19	18:06:42	<a href="#">Remove</a>
2	211.75.117.120	75.1 KB	2.2%	8.3 KB	0.5%	06/23 15:50:07	06/23 15:50:07	00:00:00	<a href="#">Remove</a>
3	192.43.244.18	7.6 KB	0.2%	19.4 KB	1.1%	06/23 16:01:00	06/24 09:57:27	17:56:27	<a href="#">Remove</a>
4	64.233.189.104	696.0 B	0.0%	1.2 KB	0.1%	06/23 15:52:25	06/23 15:52:25	00:00:00	<a href="#">Remove</a>
5	61.62.236.13	0.0 B	0.0%	240.0 B	0.0%	06/23 16:27:26	06/23 16:28:43	00:01:17	<a href="#">Remove</a>
6	209.85.139.104	0.0 B	0.0%	40.0 B	0.0%	06/23 16:27:48	06/23 16:27:48	00:00:00	<a href="#">Remove</a>
7	210.66.155.79	0.0 B	0.0%	240.0 B	0.0%	06/23 16:27:48	06/23 16:29:02	00:01:14	<a href="#">Remove</a>
Total Traffic		3.3 MB		1.7 MB		Reporting time Sat Apr 14 13:18:30 2007			

[Reset Counters](#)

### Outbound Destination IP Statistics Report

**STEP 3 .** Enter **Outbound** in **Accounting Report** and select **Top Services** to inquire the statistics website of **Send / Receive packets, Downstream/Upstream, First packet/Last packet/Duration** and the service from the WAN Server to pass the MH-2001.

- **TOP** : Select the data you want to view. It presents 10 results in one page.

-  : According to the downstream / upstream report of the selected TOP numbering to draw the Protocol Distribution chart.

#### Pull-down menu selection

- **Service** : The report of Communication Service when LAN users use the MH-2001 to connect to WAN service server.
- **Downstream** : The percentage of downstream and the value of each WAN service server who uses MH-2001 to connect to LAN user.
- **Upstream** : The percentage of upstream and the value of each LAN user who uses MH-2001 to WAN service server.
- **First Packet** : When the first packet is sent to the WAN Service Server, the sent time will be recorded by the MH-2001.
- **Last Packet** : When the last packet is sent from the WAN Service Server, the sent time will be recorded by the MH-2001.
- **Duration** : The period of time starts from the first packet to the last packet to be recorded.
- **Total Traffic** : The MH-2001 will record the sum of time and show the percentage of each Communication Service's upstream/downstream to WAN service server.
- **Reset Counter Button** : Click the Reset Counter button to refresh the Accounting Report.

Top:



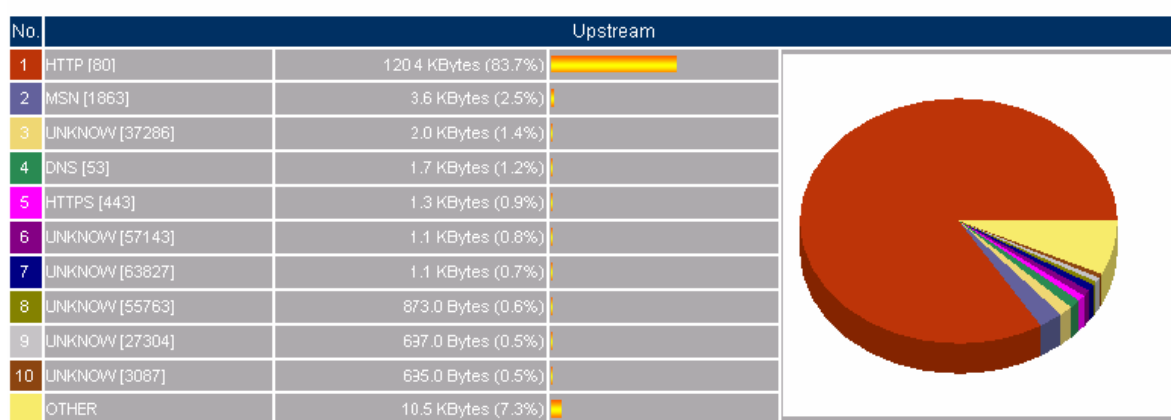
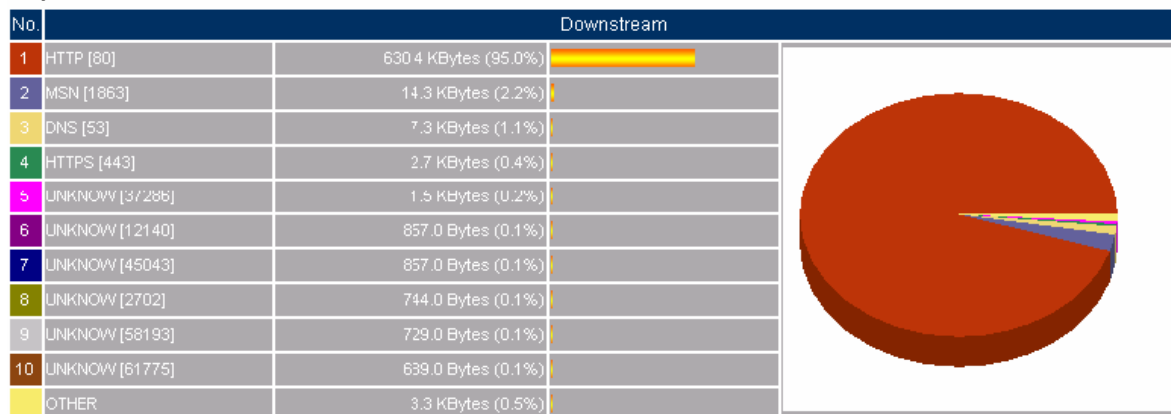
Starting Time : Mon Jun 23 15:51:48 2008

No.	Service	Downstream		Upstream		First Packet	Last Packet	Duration	Action
1	UNKNOWN [5060]	3.2 MB	97.5%	1.7 MB	98.3%	06/23 15:52:37	06/24 09:59:19	18:06:42	<a href="#">Remove</a>
2	HTTP [80]	75.8 KB	2.3%	10.0 KB	0.6%	06/23 15:50:07	06/23 16:29:02	00:38:55	<a href="#">Remove</a>
3	NTP [123]	7.6 KB	0.2%	19.4 KB	1.1%	06/23 16:01:00	06/24 09:57:27	17:56:27	<a href="#">Remove</a>
Total Traffic		3.3 MB		1.7 MB		Reporting time Sat Apr 14 13:22:08 2007			

[Reset Counters](#)

#### Outbound Services Statistics Report

## Service Distribution



According to the downstream / upstream report of the selected TOP numbering to draw the Protocol Distribution chart



Press



to return to **Accounting Report** window.

### 9.2.3 Inbound

**STEP 1** . Enter **Inbound** in **Accounting Report** and select **Top Users** to inquire the statistics website of **Send / Receive packets, Downstream / Upstream, First packet/Last packet / Duration** and the service from the WAN user to pass the MH-2001.

- **TOP** : Select the data you want to view. It presents 10 pages in one page.

#### Select from the Pull-down menu

- **Source IP** : The IP address used by WAN users who use MH-2001.
- **Downstream** : The percentage of Downstream and the value of each WAN user who uses MH-2001 to LAN service server.
- **Upstream** : The percentage of Upstream and the value of each LAN service server who uses MH-2001 to WAN users.
- **First Packet** : When the first packet is sent from WAN users to LAN service server, the sent time will be recorded by the MH-2001.
- **Last Packet** : When the last packet is sent from LAN service server to WAN users, the sent time will be recorded by the MH-2001.
- **Duration** : The period of time starts from the first packet to the last packet to be recorded.
- **Total Traffic** : The MH-2001 will record the sum of time and show the percentage of each WAN user's upstream / downstream to LAN service server.
- **Reset Counter Button** : Click the Reset Counter button to refresh the Accounting Report.

Top: 1 - 4

Starting Time : Fri Aug 18 15:02:11 2006

No.	Source IP	Upstream		Downstream		First Packet	Last Packet	Duration	Action
1	172.19.1.106	382.9 KB	34.7%	22.8 KB	25.5%	08/18 15:12:46	08/18 15:12:49	00:00:03	<a href="#">Remove</a>
2	172.19.50.26	361.2 KB	32.7%	48.1 KB	53.8%	08/18 15:13:34	08/18 15:14:53	00:01:19	<a href="#">Remove</a>
3	172.19.20.1	360.1 KB	32.6%	18.3 KB	20.5%	08/18 15:14:56	08/18 15:15:00	00:00:04	<a href="#">Remove</a>
4	172.19.50.11	0.0 B	0.0%	180.0 B	0.2%	08/18 15:13:54	08/18 15:13:56	00:00:02	<a href="#">Remove</a>
Total Traffic		1.1 MD		09.3 KD		Reporting time Fri Aug 18 15:15:06 2006			

[Reset Counters](#)

### Inbound Top Users Statistics Report

**STEP 2 .** Enter **Inbound** in **Accounting Report** and select **Top Sites** to inquire the statistics website of **Send / Receive packets, Downstream / Upstream, First packet/Last packet / Duration** and the service from the WAN user to pass the MH-2001.

- **TOP** : Select the data you want to view. It presents 10 pages in one page.

Pull-down menu selection

- **Destination IP** : The IP address used by WAN users who uses MH-2001.
- **Downstream** : The percentage of Downstream and the value of each WAN user who uses MH-2001 to LAN service server.
- **Upstream** : The percentage of Upstream and the value of each LAN service server who uses MH-2001 to WAN users.
- **First Packet** : When the first packet is sent from WAN users to LAN service server, the sent time will be recorded by the MH-2001.
- **Last Packet** : When the last packet is sent from LAN service server to WAN users, the sent time will be recorded by the MH-2001.
- **Duration** : The period of time starts from the first packet to the last packet to be recorded.
- **Total Traffic** : The MH-2001 will record the sum of time and show the percentage of each WAN user's upstream / downstream to LAN service server.
- **Reset Counter Button** : Click the Reset Counter button to refresh the Accounting Report.

Top: 1 - 1

Starting Time : Fri Aug 18 15:02:11 2006

No.	Destination IP	Upstream	Downstream	First Packet	Last Packet	Duration	Action
1	192.168.1.2	1.4 MB 100.0%	108.8 KB 100.0%	08/18 15:12:46	08/18 15:13:57	00:01:11	<a href="#">Remove</a>
Total Traffic		1.4 MB	108.8 KB	Reporting time Fri Aug 18 15:16:15 2006			


[Reset Counters](#)

### Inbound Destination IP Statistics Report



**STEP 3 .** Enter **Inbound** in **Accounting Report** and select **Top Services** to inquire the statistics website of Send/Receive packets, **Downstream/Upstream, First packet/Last packet/Duration** and the service from the WAN Server to pass the MH-2001.

- **TOP** : Select the data you want to view. It presents 10 results in one page.

-  : According to the downstream / upstream report of the selected TOP numbering to draw the Protocol Distribution chart.

Pull-down menu selection

- **Service** : The report of Communication Service when WAN users use the MH-2001 to connect to LAN service server.
- **Downstream** : The percentage of downstream and the value of each WAN user who uses MH-2001 to LAN service server.
- **Upstream** : The percentage of upstream and the value of each LAN service server who uses MH-2001 to WAN user.
- **First Packet** : When the first packet is sent to the LAN Service Server, the sent time will be recorded by the MH-2001.
- **Last Packet** : When the last packet is sent from the LAN Service Server, the sent time will be recorded by the MH-2001.
- **Duration** : The period of time starts from the first packet to the last packet to be recorded.
- **Total Traffic** : The MH-2001 will record the sum of time and show the percentage of each Communication Service's upstream / downstream to LAN service server.
- **Reset Counter** : Click the Reset Counter button to refresh the Accounting Report.

Top: 1 - 1

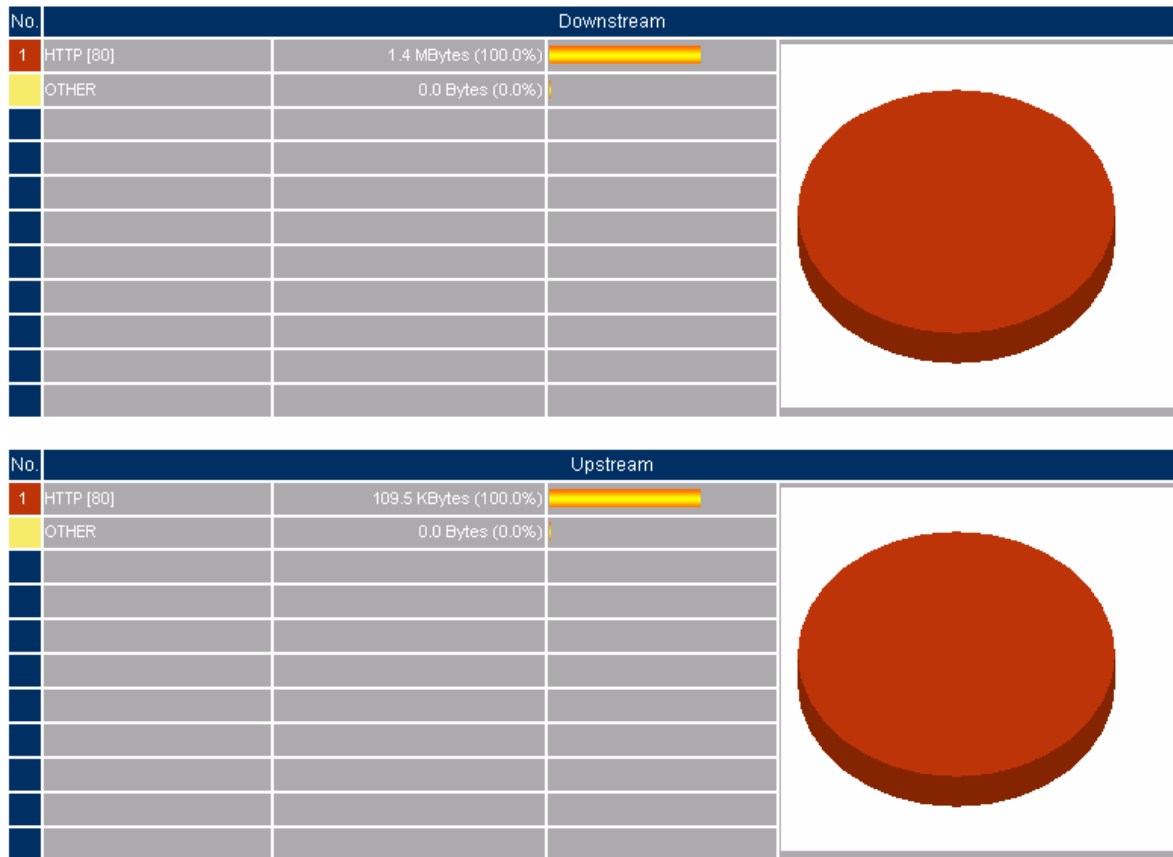
Starting Time : Fri Aug 18 15:02:11 2006

No.	Service	Upstream	Downstream	First Packet	Last Packet	Duration	Action
1	HTTP [80]	1.4 MB 100.0%	109.5 KB 100.0%	08/18 15:12:46	08/18 15:14:56	00:02:10	<a href="#">Remove</a>
Total Traffic		1.4 MB	109.5 KB	Reporting time Fri Aug 18 15:17:09 2006			

[Reset Counters](#)

### Inbound Services Statistics Report

## Service Distribution



According to the downstream / upstream report of the selected TOP numbering to draw the Protocol Distribution chart

### 9.3 Statistics

In this chapter, the Administrator queries MH-2001 for statistics of packets and data which passes across the Multi-Homing Security Gateway. The statistics provides the Administrator with information about network traffics and network loads.

#### What is Statistics

Statistics are the statistics of packets that pass through MH-2001 by control policies setup by the Administrator.

There two part in this section, WAN Statistics and Policy Statistics.

- **WAN Statistics:** The statistics of Downstream / Upstream packets and Downstream/Upstream traffic record that pass WAN Interface
- **Policy Statistics:** The statistics of Downstream / Upstream packets and Downstream/Upstream traffic record that pass Policy

## How to use Statistics

The Administrator can get the current network status from statistics, and use the information provided by statistics as a basis to manage networks.

### Define the required fields of Statistics:

#### Statistics Chart:

- **Y-Coordinate** : Network Traffic ( Kbytes/Sec )
- **X-Coordinate** : Time ( Hour/Minute )

#### Source IP, Destination IP, Service, and Action:

- These fields record the original data of Policy. From the information above, the Administrator can know which Policy is the Policy Statistics belonged to.

#### Time:

- To detect the statistics by minutes, hours, days, months, or years.

#### Bits/sec, Bytes/sec, Utilization, Total:

- The unit that used by Y-Coordinate, which the Administrator can change the unit of the Statistics Chart here.
  - ◆ **Utilization** : The percentage of the traffic of the Max. Bandwidth that System Manager set in Interface function.
  - ◆ **Total**: To consider the accumulative total traffic during a unit time as Y-Coordinate.

## 9.3.1 WAN Statistics

**STEP 1** . Enter **WAN** in **Statistics** function, it will display all the statistics of Downstream/Upstream packets and Downstream/Upstream record that pass **WAN** Interface.

WAN	Time
WAN 1	<a href="#">Minute</a> <a href="#">Hour</a> <a href="#">Day</a> <a href="#">Week</a> <a href="#">Month</a> <a href="#">Year</a>
WAN 2	<a href="#">Minute</a> <a href="#">Hour</a> <a href="#">Day</a> <a href="#">Week</a> <a href="#">Month</a> <a href="#">Year</a>
All WAN Interface	<a href="#">Minute</a> <a href="#">Hour</a> <a href="#">Day</a> <a href="#">Week</a> <a href="#">Month</a> <a href="#">Year</a>

### WAN Statistics function

- **WAN**: Select the WAN1, WAN2 or ALL WAN Interface which you want to monitor.
- **Time**: To detect the statistics by minutes, hours, days, months, or years.

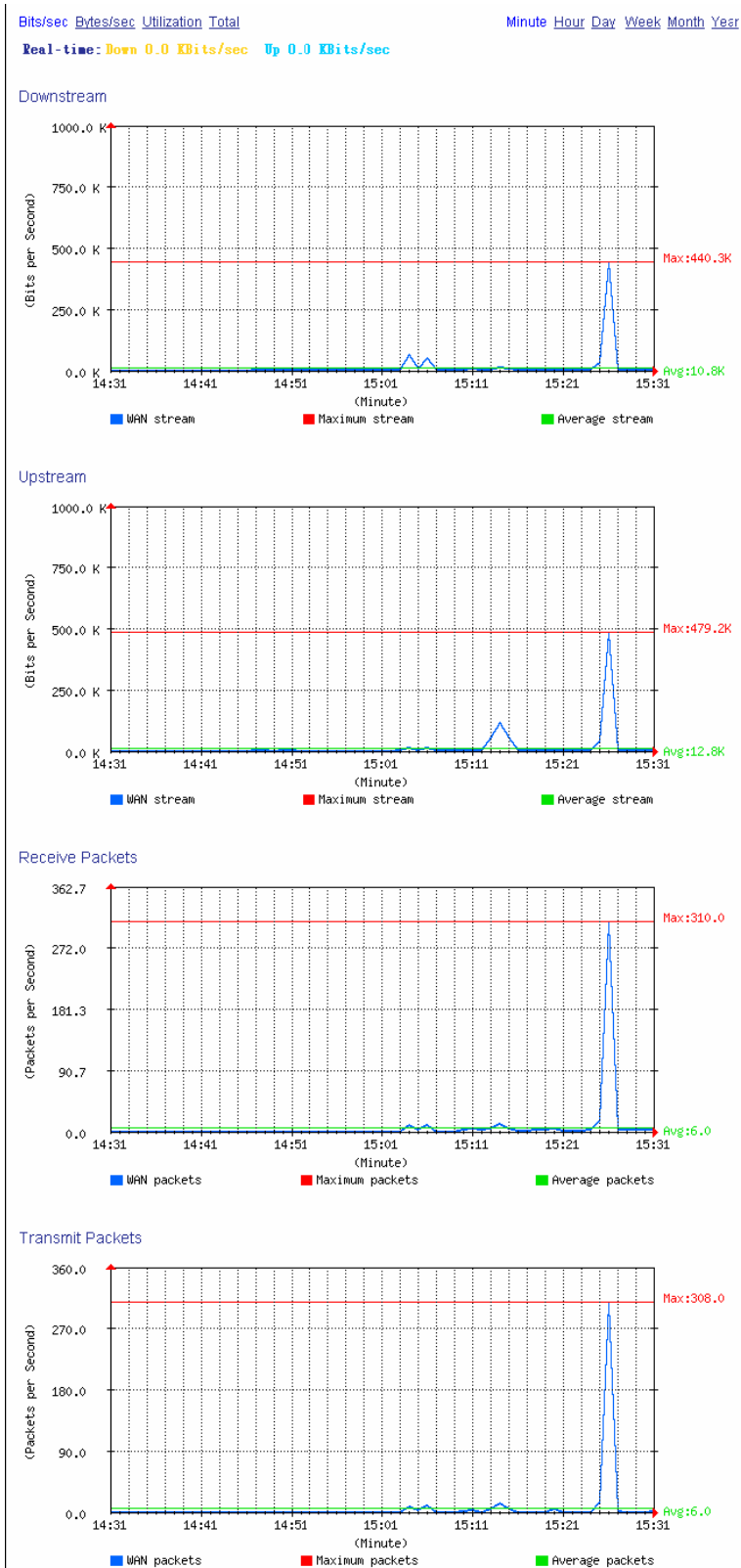


**WAN Statistics** is the additional function of **WAN** Interface. When enable **WAN** Interface, it will enable **WAN Statistics** too.

**STEP 2 .** In the Statistics window, find the network you want to check and click **Minute** on the right side, and then you will be able to check the Statistics figure every minute; click **Hour** to check the Statistics figure every hour; click **Day** to check the Statistics figure every day; click **Week** to check the Statistics figure every week; click **Month** to check the Statistics figure every month; click **Year** to check the Statistics figure every year.

**STEP 3 . Statistics Chart**

- **Y-Coordinate** : Network Traffic ( Kbytes/Sec )
- **X-Coordinate** : Time ( Hour/Minute )



**To Detect WAN Statistics**

### 9.3.2 Policy Statistics

**STEP 1** . If you had select **Statistics** in **Policy**, it will start to record the chart of that policy in **Policy Statistics**.

Source	Destination	Service	Action	Time					
Inside_Any	Outside_Any	ANY	✓	<a href="#">Minute</a>	<a href="#">Hour</a>	<a href="#">Day</a>	<a href="#">Week</a>	<a href="#">Month</a>	<a href="#">Year</a>
Outside_Any	Mail_Server(Routing)	Mail_service	✓	<a href="#">Minute</a>	<a href="#">Hour</a>	<a href="#">Day</a>	<a href="#">Week</a>	<a href="#">Month</a>	<a href="#">Year</a>

#### Policy Statistics Function



If you are going to use **Policy Statistics** function, the System Manager has to enable the **Statistics** in **Policy** first.

**STEP 2** . In the **Statistics** WebUI, find the network you want to check and click **Minute** on the right side, and then you will be able to check the Statistics chart every minute; click **Hour** to check the Statistics chart every hour; click **Day** to check the Statistics chart every day; click **Week** to check the Statistics figure every week; click **Month** to check the Statistics figure every month; click **Year** to check the Statistics figure every year.

**STEP 3 . Statistics Chart****■Y-Coordinate** : Network Traffic (Kbytes/Sec)**■X-Coordinate** : Time (Hour/Minute/Day)[Bits/sec](#) [Bytes/sec](#) [Total](#)

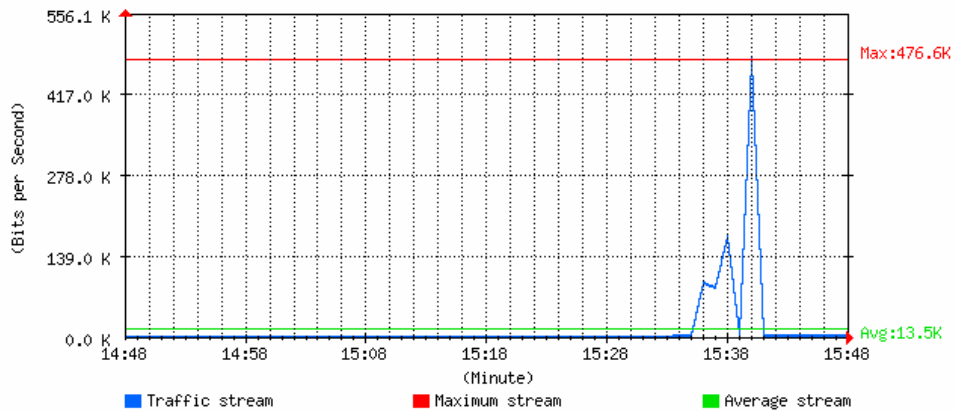
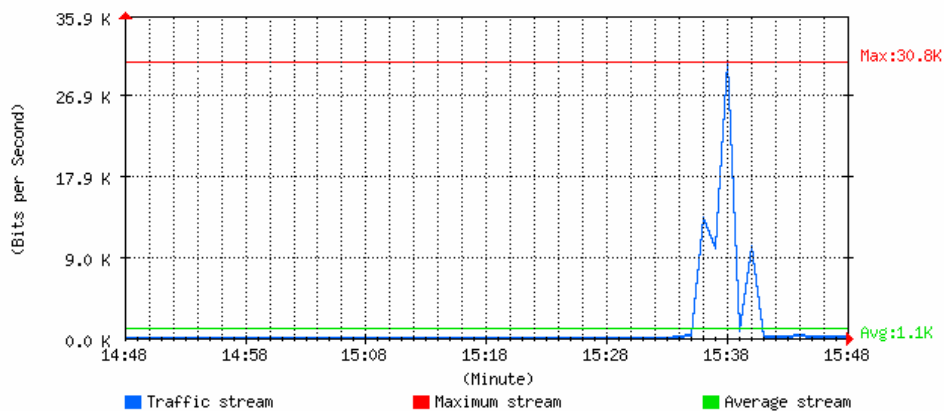
Inside\_Any to Outside\_Any

Service : ANY

Action : PERMIT

[Minute](#) [Hour](#) [Day](#) [Week](#) [Month](#) [Year](#)

Real-time: Down 0.0 KBits/sec Up 0.0 KBits/sec

**Downstream****Upstream****To Detect Policy Statistics**

## 9.4 Wake on Lan

The MIS engineer can use the MH-2001 appliance to start up the internal PCs (by sending packets) which included the network bootable network adapter and can additionally use the remote monitor software such as VNC, Terminal Service and PC Anywhere.

In this chapter, we will make the introduction of Wake on Lan.

### Remote monitor the internal PC

**STEP 1** . The internal PC to be remote monitored, and its MAC is 00:0C:76:B7:96:3B.

**STEP 2** . In **Wake on Lan** → **Setting**, add the following settings :

- Click **New Entry**.
- **Name**, enter josh.
- **MAC Address**, enter 00:0C:76:B7:96:3B.
  - Click **OK**.

Add Wake on Lan setting						
Name	josh					(Max. 20 characters) <a href="#">Assist</a>
MAC Address	00	:	0C	:	76	:
	B7	:	96	:	3B	

Set the internal PC to be monitored

**STEP 3** . Click **Wake Up**, to start up the internal PC.

Name	MAC Address	Configure		
josh	00:0C:76:B7:96:3B	<input type="button" value="Wake Up"/>	<input type="button" value="Modify"/>	<input type="button" value="Remove"/>

Start up the PC



## 9.5 Status

In this section, the device displays the status information about MH-2001. Status will display the network information from the Configuration menu. The Administrator may also use Status to check the DHCP lease time and MAC addresses for computers connected to MH-2001.

The users can know the connection status in Status. For example: LAN IP, WAN IP, Subnet Netmask, Default Gateway, DNS Server Connection, and its IP...etc.

- **Interface:** Display all of the current Interface status of the MH-2001
- **Authentication:** The Authentication information of MH-2001
- **ARP Table:** Record all the ARP that connect to the MH-2001
- **DHCP Clients:** Display the table of DHCP clients that are connected to the MH-2001.

### 9.5.1 Interface Status

**STEP 1** . Enter **Interface** in **Status** function; it will list the setting for each Interface:

- **PPPoE Con. Time:** The last time of the MH-2001 to be enabled
- **MAC Address:** The MAC Address of the Interface
- **IP Address/ Netmask:** The IP Address and its Netmask of the Interface
- **Rx Pkts, Err. Pkts:** To display the received packets and error packets of the Interface
- **Tx Pkts, Err. Pkts:** To display the sending packets and error packets of the Interface
- **Ping, WebUI:** To display whether the users can Ping to the MH-2001 from the Interface or not; or enter its WebUI
- **Forwarding Mode:** The connection mode of the Interface
- **Connection Status:** To display the connection status of WAN
- **DnS/ UpS Kbps:** To display the Maximum DownStream/UpStream Bandwidth of that WAN (set from Interface)
- **DnStream Alloca.:** The distribution percentage of DownStream according to WAN traffic
- **UpStream Alloca.:** The distribution percentage of UpStream according to WAN traffic
- **Default Gateway:** To display the Gateway of WAN
- **DNS1:** The DNS1 Server Address provided by ISP
- **DNS2:** The DNS2 Server Address provided by ISP



Monitor &gt; Status &gt; Interface

- System
- Interface
- Policy Object
- Policy
- Anomaly Flow IP
- Monitor**
  - Log
  - Accounting Report
  - Statistics
  - Wake on Lan
  - Status
    - Interface**
    - Authentication
    - ARP Table
    - DHCP Clients

Active Sessions Number : 45

System Uptime : 0 Day 22 Hour 38 Min 50 Sec

	LAN	WAN1	WAN2	DMZ
Forwarding Mode	NAT	Static IP	Static IP	NAT
WAN Connection	---			---
Max. Downstream / Upstream	---	2000 / 2000 Kbps	2000 / 512 Kbps	---
Downstream Alloca.	---	100%	0%	---
Upstream Alloca.	---	95%	4%	---
PPPoE Con. Time	---	---	---	---
MAC Address	00:30:4f:ee:dd:03	00:30:4f:ee:dd:09	00:30:4f:ee:dd:08	00:30:4f:ee:dd:04
IP Address	192.168.1.1	210.66.155.77	61.62.236.14	10.0.0.1
Netmask	255.255.255.0	255.255.255.224	255.255.255.0	255.0.0.0
Default Gateway	---	210.66.155.94	61.62.236.254	---
DNS1	---	168.95.1.1	168.95.1.1	---
DNS2	---	0.0.0.0	0.0.0.0	---
Rx Pkts, Error Pkts	653, 0	1398060, 0	715, 0	8666, 0
Tx Pkts, Error Pkts	603, 0	209612, 0	46799, 0	6982, 0
Ping				
HTTP				

## Interface Status

## 9.5.2 Authentication

**STEP 1** . Enter **Authentication** in **Status** function, it will display the record of login status:

- **IP Address:** The authentication user IP
- **Auth-User Name:** The account of the auth-user to login
- **Login Time:** The login time of the user (Year/Month/Day Hour/Minute/Second)

IP Address	Authentication-User Name	Login Time	Configure
192.168.1.2	Rayearth	2006/8/18 16:0:51	<a href="#">Remove</a>

### Authentication Status WebUI

### 9.5.3 ARP Table

**STEP 1** . Enter **ARP Table** in **Status** function; it will display a table about IP Address, MAC Address, and the Interface information which is connecting to the MH-2001:

- **IP Address:** The IP Address of the network
- **MAC Address:** The identified number of the network card
- **Interface:** The Interface of the computer

Anti-ARP virus software [Download](#) [Comment](#)

Total MACs : 3

Static <input type="checkbox"/>	IP Address	MAC Address	Interface	Configure
<input type="checkbox"/>	210.66.155.70	00:01:02:03:04:05	WAN1	<a href="#">Remove</a>
<input type="checkbox"/>	192.168.1.3	00:16:E6:8C:F8:F3	LAN	<a href="#">Remove</a>
<input type="checkbox"/>	210.66.155.94	00:A0:C5:11:89:C9	WAN1	<a href="#">Remove</a>

[New Entry](#)

[OK](#)

[Cancel](#)

ARP Table WebUI

## 9.5.4 DHCP Clients

**STEP 1** . In **DHCP Clients** of **Status** function, it will display the table of DHCP Clients that are connected to the MH-2001:

- **IP Address:** The dynamic IP that provided by DHCP Server
- **MAC Address:** The IP that corresponds to the dynamic IP
- **Leased Time:** The valid time of the dynamic IP (Start/End) (Year/Month/Day/Hour/Minute/Second)

IP Address	MAC Address	Leased Time	
		Start	End
192.168.1.2	00:B0:18:25:F5:89	---	---
192.168.1.3	00:16:e6:8c:f8:f3	2007/4/14 14:37:16	2007/4/15 2:37:16
192.168.1.2	00:16:e6:8c:f8:f3	2007/4/14 14:37:13	2007/4/14 14:39:13

### DHCP Clients WebUI