



# **Multi-Homing Security Gateway MH-1000**

## **User's Manual**

## Copyright

Copyright (C) 2006 PLANET Technology Corp. All rights reserved.

The products and programs described in this User's Manual are licensed products of PLANET Technology, This User's Manual contains proprietary information protected by copyright, and this User's Manual and all accompanying hardware, software, and documentation are copyrighted.

No part of this User's Manual may be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form by any means by electronic or mechanical. Including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's personal use, and without the prior express written permission of PLANET Technology.

## 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.

## 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.



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.

## 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.

## 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-1000

Rev: 1.0 (February, 2006)

## Table of Contents

<b>CHAPTER 1: INTRODUCTION</b> .....	<b>1</b>
1.1 FEATURES .....	1
1.2 PACKAGE CONTENTS .....	2
1.3 MH-1000 FRONT VIEW .....	2
1.4 MH-1000 REAR PANEL .....	2
1.5 SPECIFICATION.....	3
<b>CHAPTER 2: ROUTER APPLICATION</b> .....	<b>4</b>
2.1 OVERVIEW .....	4
2.2 BANDWIDTH MANAGEMENT WITH QoS .....	4
2.2.1 <i>Transparent Mode Connection Example</i> .....	4
2.2.2 <i>QoS Policies for Different Applications</i> .....	5
2.2.3 <i>Guaranteed / Maximum Bandwidth</i> .....	6
2.2.4 <i>Policy Based Traffic Shaping</i> .....	6
2.2.5 <i>Priority Bandwidth Utilization</i> .....	7
2.2.6 <i>Management by IP or MAC address</i> .....	8
2.2.7 <i>DiffServ (DSCP Marking)</i> .....	8
2.3 OUTBOUND TRAFFIC .....	9
2.3.1 <i>Outbound Fail Over</i> .....	9
2.3.2 <i>Outbound Load Balancing</i> .....	9
2.4 INBOUND TRAFFIC .....	10
2.4.1 <i>Inbound Fail Over</i> .....	10
2.4.2 <i>Inbound Load Balancing</i> .....	11
2.5 DNS INBOUND .....	12
2.5.1 <i>DNS Inbound Fail Over</i> .....	13
2.5.2 <i>DNS Inbound Load Balancing</i> .....	14
2.6 VIRTUAL PRIVATE NETWORKING .....	16
2.6.1 <i>General VPN Setup</i> .....	16
2.6.2 <i>VPN Planning - Fail Over</i> .....	17
2.6.3 <i>Concentrator</i> .....	18
<b>CHAPTER 3: GETTING STARTED</b> .....	<b>19</b>
3.1 OVERVIEW .....	19
3.2 BEFORE YOU BEGIN .....	19
3.3 CONFIGURING PCs FOR TCP/IP NETWORKING.....	19
3.3.1 <i>Overview</i> .....	20

---

3.3.2	<i>Windows XP</i>	20
3.3.3	<i>Windows 2000</i>	22
3.3.4	<i>Windows 95/98/ME</i>	23
3.3.5	<i>Windows NT 4.0</i>	24
3.4	FACTORY DEFAULT SETTINGS	25
3.4.1	<i>User name and password</i>	25
3.4.2	<i>LAN and WAN Port Addresses</i>	25
3.5	INFORMATION FROM YOUR ISP	25
3.5.1	<i>Protocols</i>	25
3.5.2	<i>Web Configuration Interface</i>	26
<b>CHAPTER 4:</b>	<b>ROUTER CONFIGURATION</b>	<b>27</b>
4.1	OVERVIEW	27
4.2	STATUS	28
4.2.1	<i>ARP Table</i>	29
4.2.2	<i>Routing Table</i>	29
4.2.3	<i>Session Table</i>	30
4.2.4	<i>DHCP Table</i>	30
4.2.5	<i>IPSec Status</i>	31
4.2.6	<i>PPTP Status</i>	31
4.2.7	<i>Traffic Statistic</i>	32
4.2.8	<i>System Log</i>	33
4.2.9	<i>IPSec Log</i>	33
4.3	QUICK START	34
4.3.1	<i>DHCP</i>	34
4.3.2	<i>Static IP</i>	34
4.3.3	<i>PPPoE</i>	35
4.3.4	<i>PPTP</i>	35
4.3.5	<i>Big Pond</i>	36
4.4	CONFIGURATION	37
4.4.1	LAN	37
4.4.1.1	Ethernet	37
4.4.1.2	DHCP Server	38
4.4.2	WAN	39
4.4.2.1	ISP Settings	39
4.4.2.1.1	DHCP	40
4.4.2.1.2	Static IP	41
4.4.2.1.3	PPPoE	41
4.4.2.1.4	PPTP Settings	43
4.4.2.1.5	Big Pond Settings	44

---

4.4.2.2 Bandwidth settings .....	45
<b>4.4.3 Dual WAN.....</b>	<b>45</b>
4.4.3.1 General Settings.....	45
4.4.3.2 Outbound Load Balance .....	46
4.4.3.3 Inbound Load Balance.....	47
4.4.3.4 Protocol Binding .....	50
<b>4.4.4 System.....</b>	<b>51</b>
4.4.4.1 Time Zone.....	51
4.4.4.2 Remote Access .....	52
4.4.4.3 Firmware Upgrade.....	52
4.4.4.4 Backup / Restore.....	53
4.4.4.5 Restart.....	53
4.4.4.6 Password.....	54
4.4.4.7 System Log Server.....	55
4.4.4.8 E-mail Alert .....	55
<b>4.4.5 Firewall.....</b>	<b>56</b>
4.4.5.1 Packet Filter .....	57
4.4.5.2 URL Filter.....	58
4.4.5.3 LAN MAC Filter .....	60
4.4.5.4 Block WAN Request .....	61
4.4.5.5 Intrusion Detection .....	62
<b>4.4.6 VPN.....</b>	<b>62</b>
4.4.6.1 IPSec.....	62
4.4.6.1.1 IPSec Wizard.....	62
4.4.6.1.2 IPSec Policy .....	66
4.4.6.2 PPTP.....	70
<b>4.4.7 QoS.....</b>	<b>71</b>
<b>4.4.8 Virtual Server.....</b>	<b>74</b>
4.4.8.1 DMZ.....	75
4.4.8.2 Port Forwarding Table.....	76
<b>4.4.9 Advanced.....</b>	<b>77</b>
4.4.9.1 Static Route.....	77
4.4.9.2 Dynamic DNS.....	79
4.4.9.3 Device Management.....	80
<b>4.5 SAVE CONFIGURATION TO FLASH .....</b>	<b>80</b>
<b>4.6 LOGOUT .....</b>	<b>81</b>
<b>CHAPTER 5: TROUBLESHOOTING .....</b>	<b>82</b>
<b>5.1 BASIC FUNCTIONALITY .....</b>	<b>82</b>
5.1.1 Router Won't Turn On.....	82

---

5.1.2 LEDs Never Turn Off.....	82
5.1.3 LAN or Internet Port Not On.....	82
5.1.4 Forgot My Password.....	82
5.2 LAN INTERFACE.....	83
5.2.1 Can't Access MH-1000 from the LAN.....	83
5.2.2 Can't Ping Any PC on the LAN.....	83
5.2.3 Can't Access Web Configuration Interface.....	83
5.2.3.1 Pop-up Windows.....	84
5.2.3.2 Java Scripts.....	85
5.2.3.3 Java Permissions.....	86
5.3 WAN INTERFACE.....	87
5.3.1 Can't Get WAN IP Address from the ISP.....	87
5.4 ISP CONNECTION.....	87
5.5 PROBLEMS WITH DATE AND TIME.....	89
5.6 RESTORING FACTORY DEFAULTS.....	89
<b>APPENDIX A: VIRTUAL PRIVATE NETWORKING.....</b>	<b>90</b>
A.1 WHAT IS THE VPN?.....	90
A.1.1 VPN Applications.....	90
A.2 WHAT IS THE IPSEC?.....	90
A.2.1 IPSec Security Components.....	91
A.2.1.1 Authentication Header (AH).....	91
A.2.1.2 Encapsulating Security Payload (ESP).....	91
A.2.1.3 Security Associations (SA).....	92
A.2.2 IPSec Modes.....	92
A.2.3 Tunnel Mode AH.....	93
A.2.4 Tunnel Mode ESP.....	93
A.2.5 Internet Key Exchange (IKE).....	94
<b>APPENDIX B: IPSEC LOGS AND EVENTS.....</b>	<b>96</b>
B.1 IPSEC LOG EVENT CATEGORIES.....	96
B.2 IPSEC LOG EVENT TABLE.....	96
<b>APPENDIX C: BANDWIDTH MANAGEMENT WITH QOS.....</b>	<b>99</b>
C.1 OVERVIEW.....	99
C.2 WHAT IS QUALITY OF SERVICE?.....	99
C.3 WHAT IS QUALITY OF SERVICE?.....	99
C.4 WHO NEEDS QoS?.....	99
C.4.1 Home Users.....	100
C.4.2 Office Users.....	100

---

<b>APPENDIX D: ROUTER SETUP EXAMPLES.....</b>	<b>102</b>
D.1 OUTBOUND FAIL OVER .....	102
D.2 OUTBOUND LOAD BALANCING .....	103
D.3 INBOUND FAIL OVER .....	106
D.4 DNS INBOUND FAIL OVER .....	108
D.5 DNS INBOUND LOAD BALANCING .....	111
D.6 DYNAMIC DNS INBOUND LOAD BALANCING.....	113
D.7 VPN CONFIGURATION .....	117
<i>D.7.1 LAN to LAN</i> .....	117
<i>D.7.2 Host to LAN</i> .....	118
D.8 IP SEC FAIL OVER (GATEWAY TO GATEWAY).....	120
D.9 IP VPN CONCENTRATOR .....	123
D.10 PROTOCOL BINDING .....	128
D.11 INTRUSION DETECTION .....	129
D.12 PPTP REMOTE ACCESS BY WINDOWS XP .....	130
D.13 PPTP REMOTE ACCESS .....	136

## Chapter 1: Introduction

PLANET's Multi-Homing Security Gateway, MH-1000 integrated with cutting-edge technology including Load Balancing, VPN and Firewall for central sites to establish office network and connect with branch offices, remote dial up and tele-workers. It is designed for business requiring application-based network solution at low-capital investment and is perfectly catering to the needs of small and medium sized business.

Built-in multiple WAN interfaces can prevent your Internet connection from failure, and also reduces the risks of potential shutdown if one of the Internet connections fails. Moreover, it allows you to perform load-balancing by distributing the traffic through two WAN connections.

In addition to a multi-homing device, PLANET's Multi-Homing Security Gateway provides a complete security solution in a box. The policy-based firewall, content filtering function and VPN connectivity with 3DES and AES encryption make it a perfect product for your network security. Bandwidth management function is also supported to offers network administrators an easy yet powerful means to allocate network resources based on business priorities, and to shape and control bandwidth usage.

### 1.1 Features

- ◆ **WAN Fail-over:** Auto failover feature can be configured for a second connection to ensure redundant connectivity when the primary line fails.
- ◆ **Load Balancing:** MH-1000 provides the ability to balance the workload by distributing incoming traffic across the two connections.
- ◆ **DNS inbound load balance:** The MH-1000 can be configured to reply the WAN2 IP address for the DNS domain name request if WAN1 fails.
- ◆ **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.
- ◆ **PPTP Server:** The MH-1000 also provides PPTP server feature, the remote user can connect to MH-1000 PPTP server without too many complex setting and to access the LAN resource.
- ◆ **Content Filtering:** The security gateway can block network connection based on URLs, Scripts (The Pop-up, Java Applet, cookies and Active X).
- ◆ **SPI Firewall:** Built-in Stateful Packet Inspection (SPI) can determine if a data packet is allowed through the firewall to the private LAN.
- ◆ **Denial of Service (DoS):** The MH-1000 protects against hackers attack by DoS, it can allow private LAN securely connected to the Internet.
- ◆ **Quality of Service (QoS):** Network packets can be classified based on IP address and TCP/UDP port number and give guarantee and maximum bandwidth with three levels of priority.
- ◆ **Dynamic Domain Name Service (DDNS):** The Dynamic DNS service allows users to alias a dynamic IP address to a static hostname.



## 1.2 Package Contents

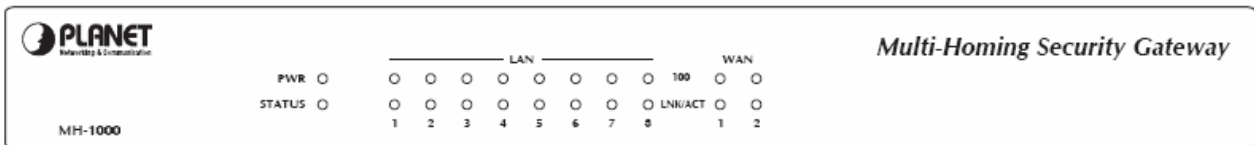
The following items should be included:

- MH-1000
  - n Multi-Homing Security Gateway
  - n User's Manual CD-ROM
  - n This Quick Installation Guide
  - n Power Adapter
  - n Bracket x 2 (For rack-mounted)
  - n Screw x 4 (For rack-mounted)

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

## 1.3 MH-1000 Front View

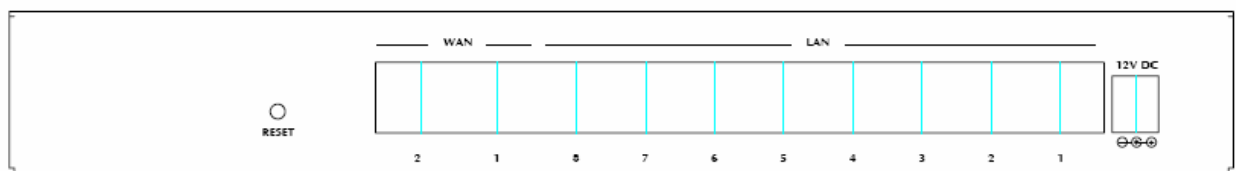
MH-1000 Front Panel



LED	Description
PWR	A solid light indicates a steady connection to a power source
STATUS	A blinking light indicates the device is writing to flash memory
LAN 1 - 8	Lit when connected to an Ethernet device 10/100: Lit green when connected at 100Mbps Not lit when connected at 10Mbps LNK/ACT: Lit when device is connected. Blinking when data is transmitting /receiving
WAN1, WAN2	Lit when connected to an Ethernet device 10/100: Lit green when connected at 100Mbps Not lit when connected at 10Mbps LNK/ACT: Lit when device is connected. Blinking when data is transmitting /receiving

## 1.4 MH-1000 Rear Panel

MH-1000 Rear Panel



Port or button	Description
RESET	To reset device and restore factory default settings, after the device is fully booted, press and hold RESET until the Status LED begins to blink.
WAN 1, WAN2	Connect to your xDSL/Cable modem or other Internet connection devices
LAN 1- 8	Connect to your local PC, switch or other local network device
DC 12V	Connect DC Power Adapter here (12VDC)

## 1.5 Specification

Product	Multi-homing Security Gateway	
Model	MH-1000	
Hardware		
Ethernet	LAN	8 x 10/100 Based-TX RJ-45
	WAN	2 x 10/100 Based-TX RJ-45
Performance		
Firewall throughput	90Mbps	
IPSec VPN throughput	30Mbps	
PPTP VPN throughput	10Mbps	
Maximum Concurrent sessions	10,000	
Software		
Management	Web	
Network Protocol and features	Static IP, PPPoE, PPTP, Big Pond and DHCP client connection to ISP NAT, Static Route, RIP-2 Dynamic Domain Name System (DDNS) Virtual Server and DMZ DHCP server NTP	
Load Balancing	Increased bandwidth of outbound and inbound traffic DNS inbound load balance	
Firewall	Stateful Packet Inspection (SPI) and Denial of Service (DoS) prevention Packet Filter (by IP, port number and packet type) E-mail alert and logs of attack MAC Address Filtering	
Content Filtering	URL Filtering Java Applet/Active X/Web Proxy/Surfing of IP Address/Cookie Blocking	
VPN Tunnels	IPSec: 100, PPTP: 4	
VPN Functions	PPTP, IPSec VPN support DES, 3DES and AES encrypting SHA-1 / MD5 authentication algorithm Remote access VPN (Client-to-Site) and Site to Site VPN IPSec, PPTP, L2TP pass through	
QoS	Support DiffServ approach Prioritization and bandwidth managed by IP, Port number and MAC address	
Log and Alert	Syslog support E-mail Alert	

## Chapter 2: Router Application

### 2.1 Overview

MH-1000 is a versatile device that can be configured to not only protect your network from malicious attackers, but also ensure optimal usage of available bandwidth with Quality of Service (QoS) and both Inbound and Outbound Load Balancing. Alternatively, MH-1000 can also be set to redirect incoming and outgoing network traffic with the Fail Over capability, ensuring minimal downtime and increased reliability.

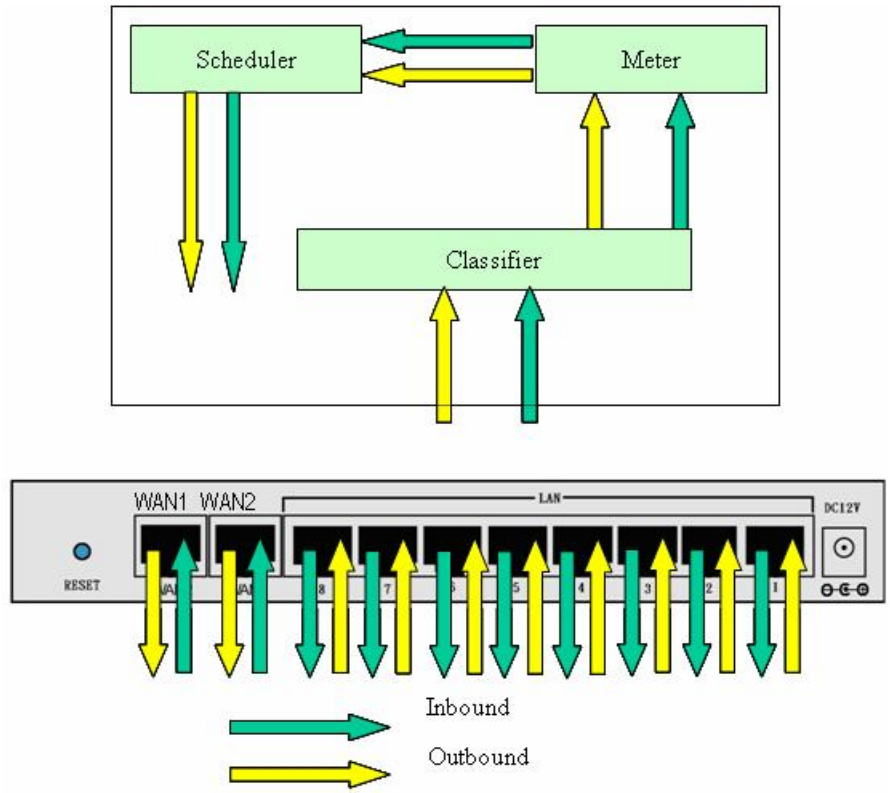
### 2.2 Bandwidth Management with QoS

Quality of Service (QoS) gives you full control over which types of outgoing data traffic should be given priority by the router. By doing so, the router can ensure that latency-sensitive applications like voice, bandwidth-consuming data like gaming packets, or even mission critical files efficiently move through the router even under a heavy load. You can throttle the speed at which different types of outgoing data pass through the router. In addition, you can simply change the priority of different types of upload data and let the router sort out the actual speeds.

#### 2.2.1 Transparent Mode Connection Example

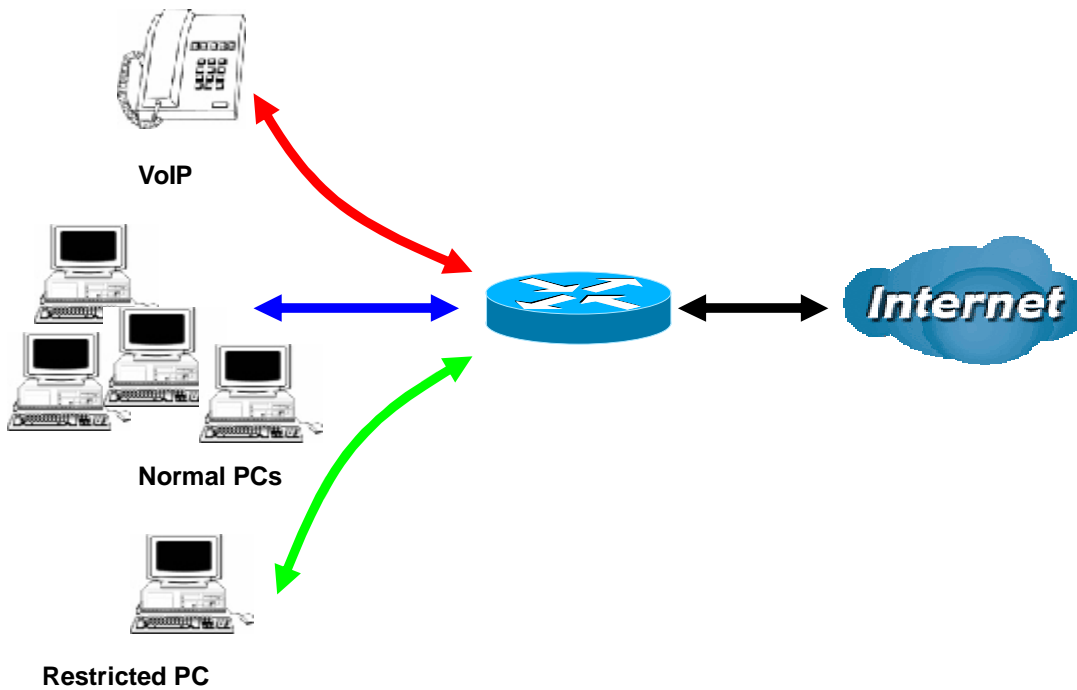
QoS generally involves the prioritization of network traffic. QoS is comprised of three major components: Classifier, Meter, and Scheduler. Each of these components has a distinct role in ensuring that incoming and outgoing data is managed according to user specifications.

The Classifier analyses incoming packets and marks each one according to configured parameters. The Meter communicates the drop priority to the Scheduler and measures the temporal priorities of the output stream against configured parameters. Finally, the Scheduler schedules each packet for transmission based on information from both the Classifier and the Meter.



### 2.2.2 QoS Policies for Different Applications

By setting different QoS policies according to the applications you are running, you can use MH-1000 to optimize the bandwidth that is being used on your network.



As illustrated in the diagram above, applications such as Voice over IP (VoIP) require low network latencies to function properly. If bandwidth is being used by other applications such as an FTP server, users using VoIP will experience network lag and/or service interruptions during use. To avoid this scenario, this

network has assigned VoIP with a guaranteed bandwidth and higher priority to ensure smooth communications. The FTP server, on the other hand, has been given a maximum bandwidth cap to make sure that regular service to both VoIP and normal Internet applications is uninterrupted.

### 2.2.3 Guaranteed / Maximum Bandwidth

Setting a Guaranteed Bandwidth ensures that a particular service receives a minimum percentage of bandwidth. For example, you can configure MH-1000 to reserve 10% of the available bandwidth for a particular computer on the network to transfer files.

Alternatively you can set a Maximum Bandwidth to restrict a particular application to a fixed percentage of the total throughput. Setting a Maximum Bandwidth of 20% for a file sharing program will ensure that no more than 20% of the available bandwidth will be used for file sharing.

Quality of Service	
Add QoS Rule	
Interface	WAN1 Outbound
Application	FTP
Guaranteed	10 %
Maximum	20 %
Priority	6 (Lowest)
DSCP Marking	Disable
Address Type	<input checked="" type="radio"/> IP Address <input type="radio"/> MAC Address
Source IP Address Range	From 192.168.1.1 To 255.255.255.255
Destination IP Address Range	From 0.0.0.0 To 255.255.255.255
Protocol	TCP
Source Port Range <a href="#">Helper</a>	From 1 To 65535
Destination Port Range <a href="#">Helper</a>	From 20 To 21
<input type="button" value="Apply"/>	

### 2.2.4 Policy Based Traffic Shaping

Policy Based Traffic Shaping allows you to apply specific traffic policies across a range of IP addresses or **[D1]** ports. This is particularly useful for assigning different policies for different PCs on the network.

Policy based traffic shaping lets you better manage your bandwidth, providing reliable Internet and network service to your organization.

Quality of Service	
Add QoS Rule	
Interface	WAN1 Outbound
Application	FTP
Guaranteed	10 %
Maximum	20 %
Priority	6 (Lowest)
DSCP Marking	Disable
Address Type	<input checked="" type="radio"/> IP Address <input type="radio"/> MAC Address
Source IP Address Range	From 192.168.1.1 To 255.255.255.255
Destination IP Address Range	From 0.0.0.0 To 255.255.255.255
Protocol	TCP
Source Port Range <a href="#">Helper</a>	From 1 To 65535
Destination Port Range <a href="#">Helper</a>	From 20 To 21
<input type="button" value="Apply"/>	

## 2.2.5 Priority Bandwidth Utilization

Assigning priority to a certain service allows MH-1000 to give either a higher or lower priority to traffic from this particular service. Assigning a higher priority to an application ensures that it is processed ahead of applications with a lower priority and vice versa.

Quality of Service	
Add QoS Rule	
Interface	WAN1 Outbound
Application	FTP
Guaranteed	10 %
Maximum	20 %
Priority	6 (Lowest)
DSCP Marking	0 (Highest)
Address Type	<input type="radio"/> IP Address <input checked="" type="radio"/> MAC Address
Source IP Address Range	From .1 To 255.255.255.255
Destination IP Address Range	From To 255.255.255.255
Protocol	TCP
Source Port Range <a href="#">Helper</a>	From 1 To 65535
Destination Port Range <a href="#">Helper</a>	From 20 To 21
<input type="button" value="Apply"/>	

## 2.2.6 Management by IP or MAC address

MH-1000 can also be configured to apply traffic policies based on a particular IP or MAC address. This allows you to quickly assign different traffic policies to a specific computer on the network.

Quality of Service	
Add QoS Rule	
Interface	WAN1 Outbound
Application	FTP
Guaranteed	10 %
Maximum	20 %
Priority	6 (Lowest)
DSCP Marking	Disable
Address Type	<input checked="" type="radio"/> IP Address <input type="radio"/> MAC Address
Source IP Address Range	From 192.168.1.1 To 255.255.255.255
Destination IP Address Range	From 0.0.0.0 To 255.255.255.255
Protocol	TCP
Source Port Range <a href="#">Helper</a>	From 1 To 65535
Destination Port Range <a href="#">Helper</a>	From 20 To 21
<input type="button" value="Apply"/>	

## 2.2.7 DiffServ (DSCP Marking)

DiffServ (a.k.a. DSCP Marking) allows you to classify traffic based on IP DSCP values. These markings can be used to identify traffic within the network. Other interfaces can match traffic based on the DSCP markings. DSCP markings are used to decide how packets should be treated, and is a useful tool to give precedence to varying types of data.

Quality of Service	
Add QoS Rule	
Interface	WAN1 Outbound
Application	FTP
Guaranteed	10 %
Maximum	20 %
Priority	6 (Lowest)
DSCP Marking	Disable
Address Type	<input checked="" type="radio"/> IP Address <input type="radio"/> MAC Address
Source IP Address Range	From [ ] To 255.255.255.255
Destination IP Address Range	From [ ] To 255.255.255.255
Protocol	[ ]
Source Port Range <a href="#">Helper</a>	From [ ] To 65535
Destination Port Range <a href="#">Helper</a>	From [ ] To 21
<input type="button" value="Apply"/>	

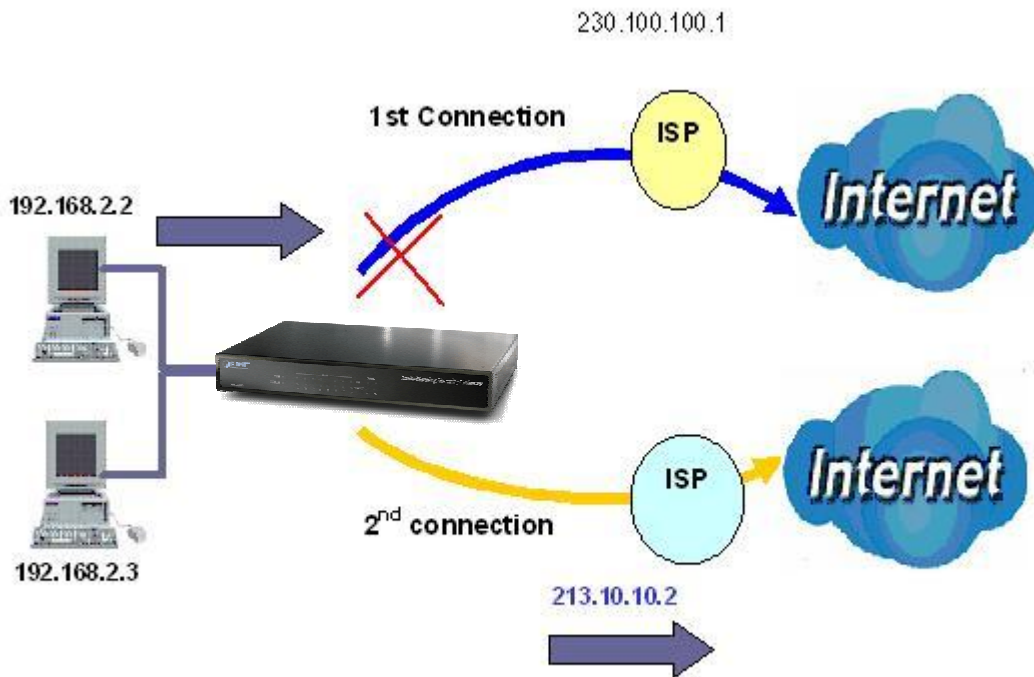
Disable  
 Best Effort  
 Premium  
 Gold service(L)  
 Gold service(M)  
 Gold service(H)  
 Silver service(L)  
 Silver service(M)  
 Silver service(H)  
 Bronze service(L)  
 Bronze service(M)  
 Bronze service(H)

## 2.3 Outbound Traffic

This section outlines some of the ways you can use MH-1000 to manage outbound traffic.

### 2.3.1 Outbound Fail Over

Configuring MH-1000 for Outbound Fail Over allows you to ensure that outgoing traffic is uninterrupted.



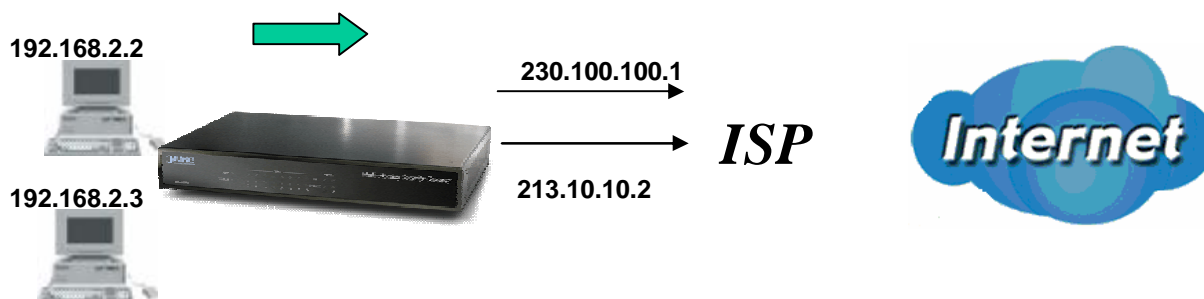
In the above example, PC 1 (IP\_192.168.2.2) and PC 2 (IP\_192.168.2.3) are connected to the Internet via WAN1 (IP\_230.100.100.1) on MH-1000. Should WAN1 fail, Outbound Fail Over tells MH-1000 to reroute outgoing traffic to WAN2 (IP\_213.10.10.2). Configuring your MH-1000 for Outbound Fail Over provides a more reliable connection for your outgoing traffic.

Please refer to appendix D for example settings.

### 2.3.2 Outbound Load Balancing

Outbound Load Balancing allows MH-1000 to intelligently manage outbound traffic based on the amount of load of each WAN connection.





In the above example, PC 1 (IP\_192.168.2.2) and PC 2 (IP\_192.168.2.3) are connected to the Internet via WAN1 (IP\_230.100.100.1) and WAN2 (IP\_213.10.10.2) on MH-1000. You can configure MH-1000 to balance the load of each WAN port with one of two mechanisms:

1. Session (by session/by traffic/weight of link capability)
2. IP Hash (by traffic/weight of link capability)

The IP Hash mechanism will ensure that the traffic from the same source IP address and destination IP address will go through the same WAN port. This is useful for some server applications that need to identify the source IP address of the client.

By balancing the load between WAN1 and WAN2, your MH-1000 can ensure that outbound traffic is efficiently handled by making sure that both ports are equally sharing the load, preventing situations where one port is completely saturated by outbound traffic.

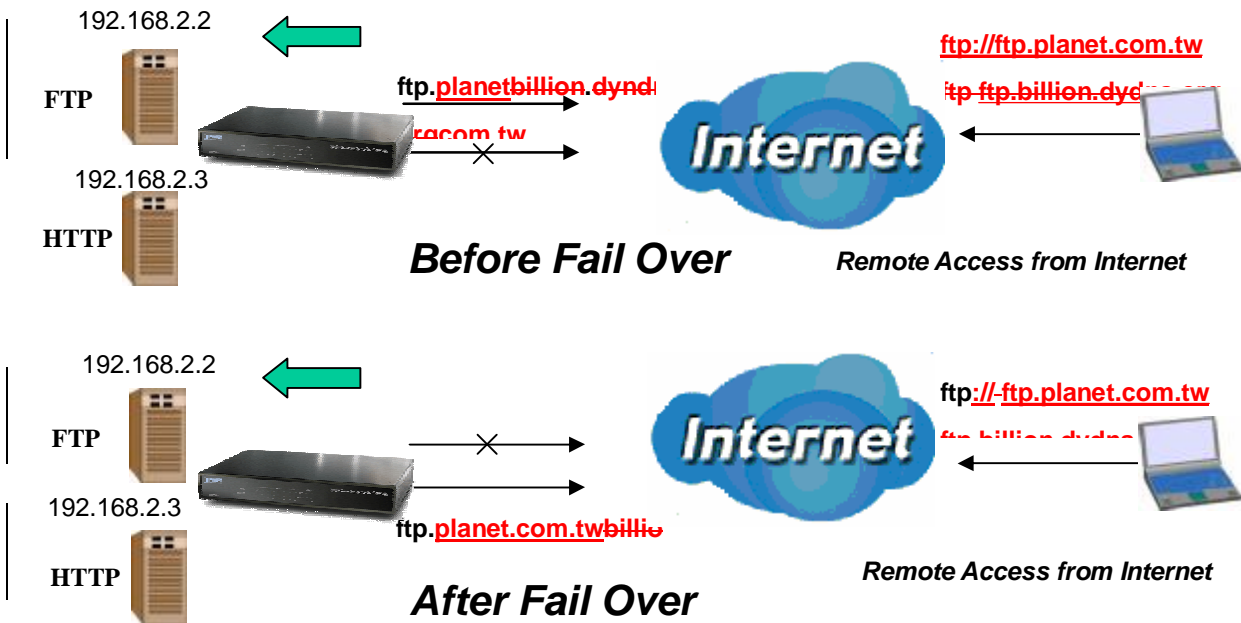
Please refer to appendix D for example settings.

## 2.4 Inbound Traffic

Learn how MH-1000 can handle inbound traffic in the following section.

### 2.4.1 Inbound Fail Over

Configuring MH-1000 for Inbound Fail Over allows you to ensure that incoming traffic is uninterrupted by having MH-1000 default to WAN2 should WAN1 fail.

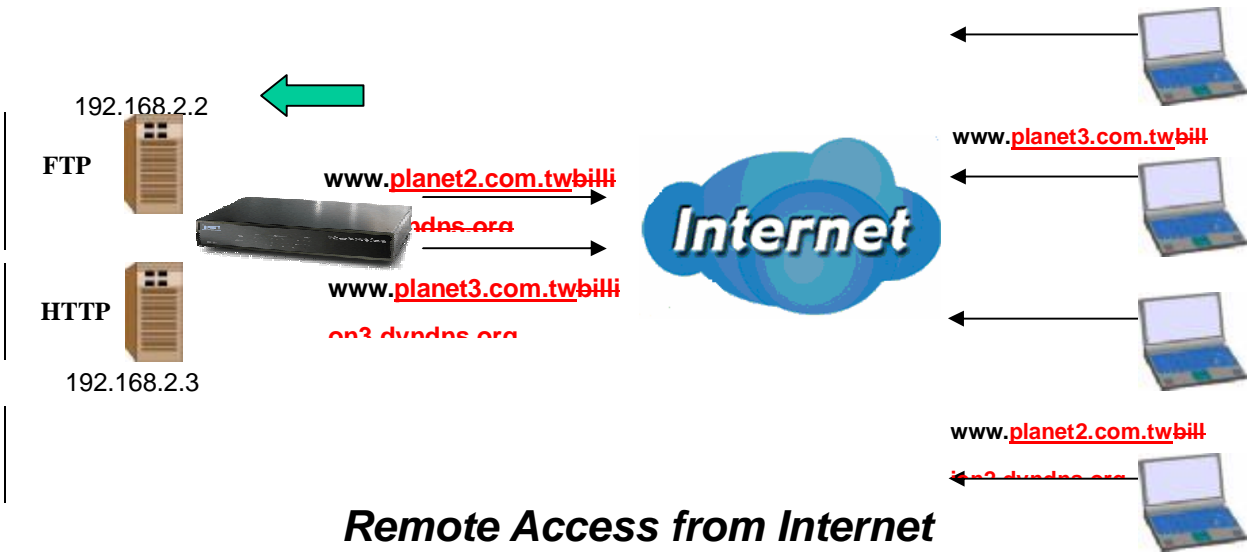


In the above example, an FTP Server (IP\_192.168.2.2) and an HTTP Server (IP\_192.168.2.3) are connected to the Internet via WAN1 ([ftp.planet.com.tw](http://ftp.planet.com.tw)) on MH-1000. A remote computer is trying to access these servers via the Internet. Under normal circumstances, the remote computer will gain access to the network via WAN1. Should WAN1 fail, Inbound Fail Over tells MH-1000 to reroute incoming traffic to WAN2 by using the Dynamic DNS mechanism. Configuring your MH-1000 for Inbound Fail Over provides a more reliable connection for your incoming traffic.

Please refer to appendix D for example settings.

## 2.4.2 Inbound Load Balancing

Inbound Load Balancing allows MH-1000 to intelligently manage inbound traffic based on the amount of load of each WAN connection.



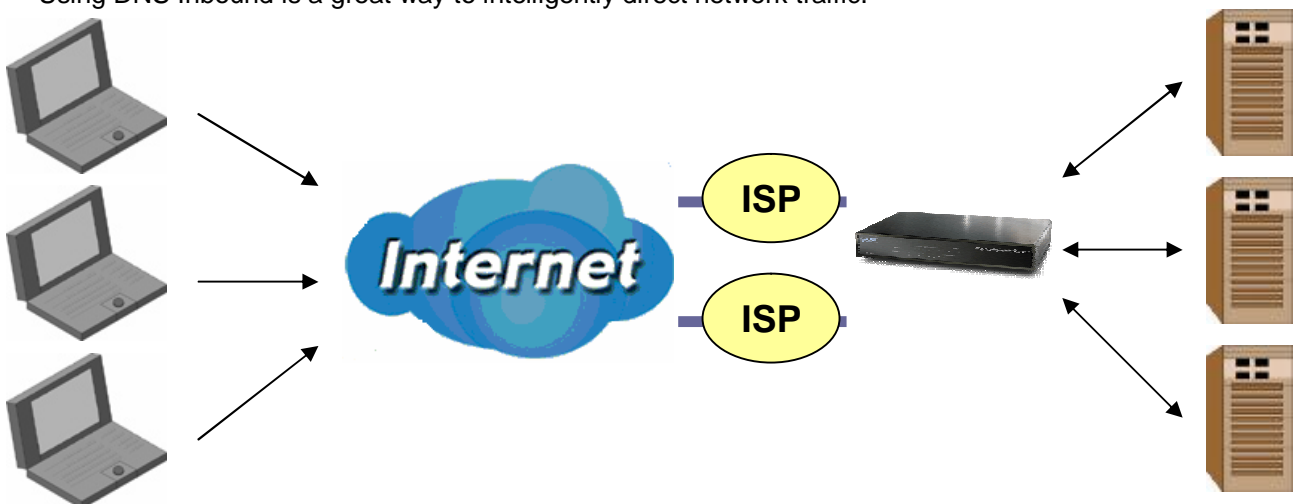
### Remote Access from Internet

In the above example, an FTP server (IP\_192.168.2.2) and an HTTP server (IP\_192.168.2.3) are connected to the Internet via WAN1 ([www.planet2.com.tw](http://www.planet2.com.tw)) and WAN2 ([www.planet3.com.tw](http://www.planet3.com.tw)) on MH-1000. Remote PCs are attempting to access the servers via the Internet. Using Inbound Load Balancing, MH-1000 can direct incoming requests to the correct WAN port based on group assignment. For example, a sales force can be directed to [www.planet2.com.tw](http://www.planet2.com.tw) while the R&D group can access [www.planet3.com.tw](http://www.planet3.com.tw). By balancing the load between WAN1 and WAN2, your MH-1000 can ensure that inbound traffic is efficiently handled with both ports equally sharing the load, preventing situations where service is slow because one port is completely saturated by inbound traffic.

Please refer to appendix D for example settings.

### 2.5 DNS Inbound

Using DNS Inbound is a great way to intelligently direct network traffic.



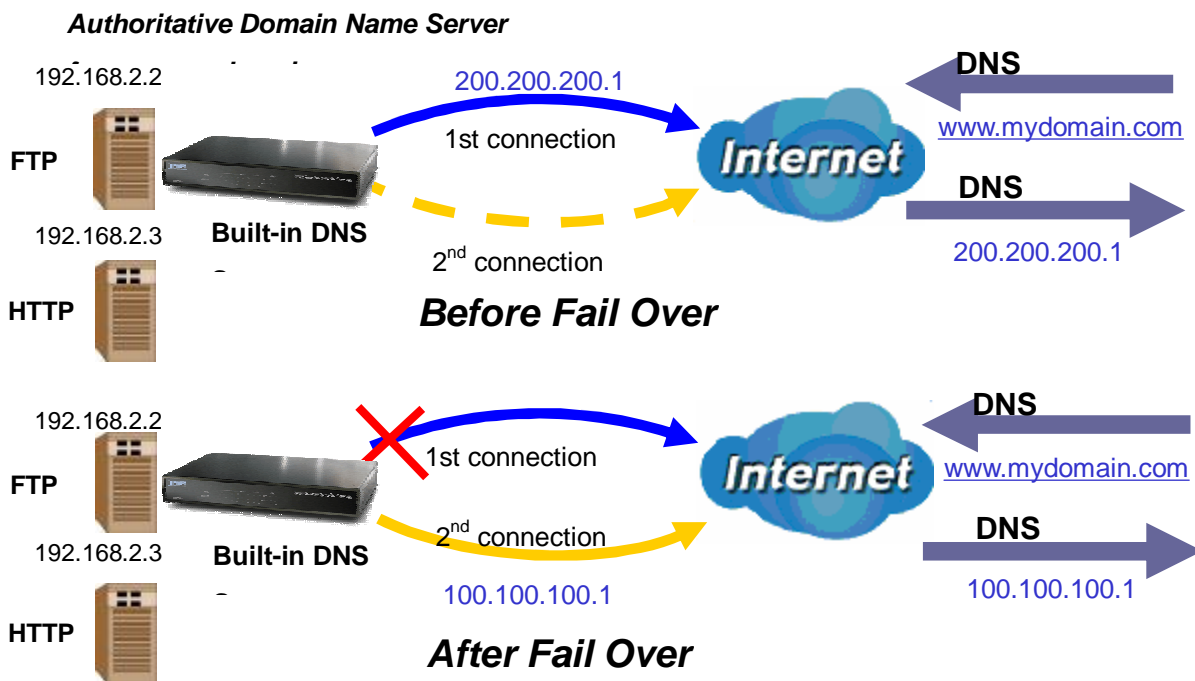
DNS Inbound is a three step process. First, a DNS request is made to the router via a remote PC. MH-1000, based on settings specified by the user, will direct the requesting PC to the correct WAN

port by replying the selected WAN IP address through the built-in DNS server. The remote PC then accesses the network via the specified WAN port. How MH-1000 directs this traffic through the built-in DNS server depends on whether it is configured for Fail Over or Load Balancing.

Learn how to make DNS Inbound on MH-1000 work for you in the following section.

### 2.5.1 DNS Inbound Fail Over

MH-1000 can be configured to reply the WAN2 IP address for the DNS domain name request should WAN1 fail.

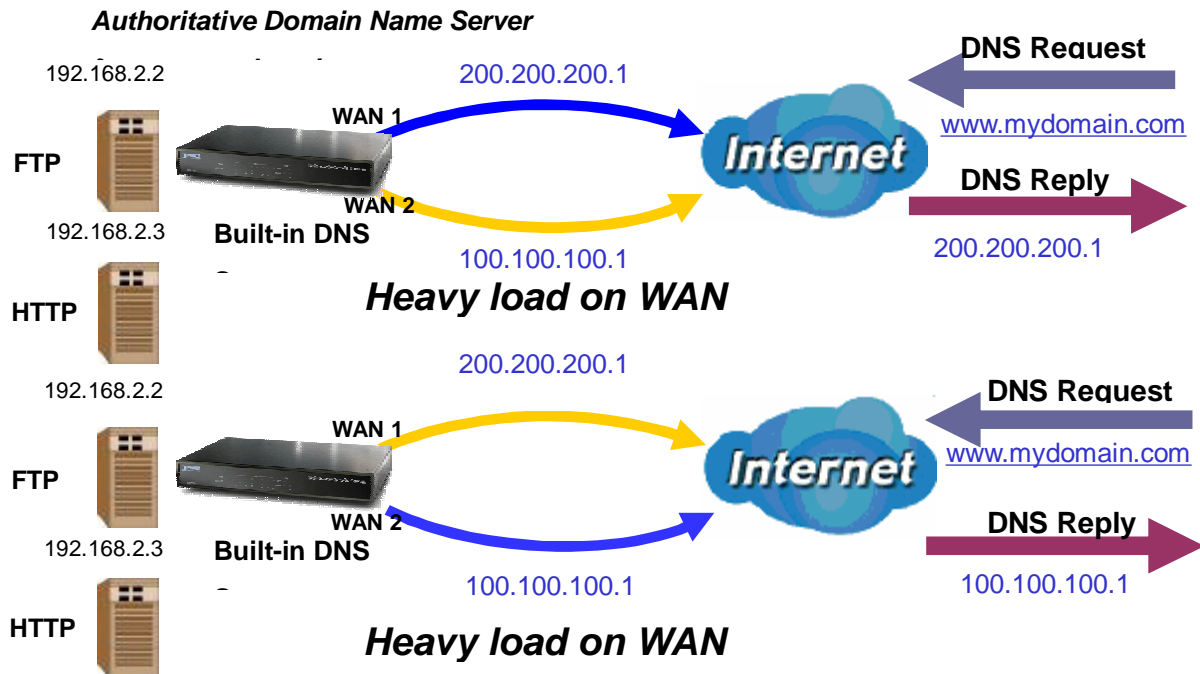


In the above example, an FTP Server (IP\_192.168.2.2) and an HTTP Server (IP\_192.168.2.3) are connected to the Internet via WAN1 (IP\_200.200.200.1) on MH-1000. A remote computer is trying to access these servers via the Internet, and makes a DNS request. The DNS request ([www.mydomain.com](http://www.mydomain.com)) will be sent through WAN1 (200.200.200.1) to the built-in DNS server. The DNS server will reply 200.200.200.1 because this is the only active WAN port. Should WAN1 fail, MH-1000 will instead reply with WAN2's IP address (100.100.100.1), and the remote PC will gain access to the network via WAN2. By configuring MH-1000 for DNS Inbound Fail Over, incoming requests will enjoy increased reliability when accessing your network.

Please refer to appendix D for example settings.

## 2.5.2 DNS Inbound Load Balancing

DNS Inbound Load Balancing allows MH-1000 to intelligently manage inbound traffic based on the amount of load of each WAN connection by assigning the IP address with the lowest traffic load to incoming requests.



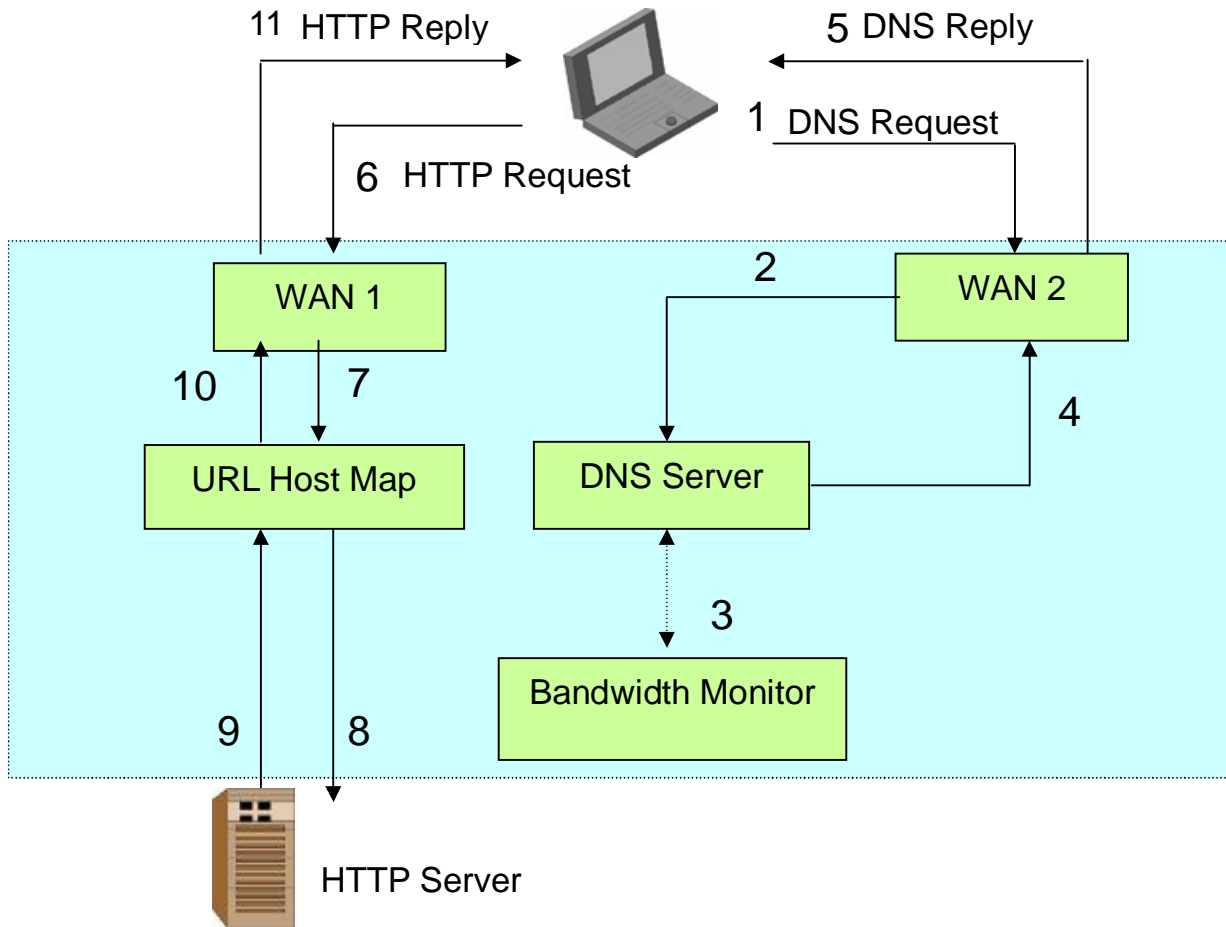
In the above example, an FTP server (IP\_192.168.2.2) and an HTTP server (IP\_192.168.2.3) are connected to the Internet via WAN1 (IP\_200.200.200.1) and WAN2 (IP\_100.100.100.1) on MH-1000. Remote PCs are attempting to access the servers via the Internet by making a DNS request, entering a URL ([www.mydomain.com](http://www.mydomain.com)).

Using a load balancing algorithm, MH-1000 can direct incoming requests to either WAN port based on the amount of load each WAN port is currently experiencing. If WAN2 is experiencing a heavy load, MH-1000 responds to incoming DNS requests with WAN1.

By balancing the load between WAN1 and WAN2, your MH-1000 can ensure that inbound traffic is efficiently handled, making sure that both ports are equally sharing the load and preventing situations where service is slow because one port is completely saturated by inbound traffic.

Please refer to appendix D for example settings.

A typical scenario of how traffic is directed with DNS Inbound Load Balancing is illustrated below:



In the example above, the client is making a DNS request.

- (1). The request is sent to the DNS server of MH-1000 through WAN2.
- (2). WAN2 will route this request to the embedded DNS server of MH-1000.
- (3). MH-1000 will analyze the bandwidth of both WAN1 and WAN2 and decide which WAN IP to reply to the request.
- (4). After the decision is made, MH-1000 will route the DNS reply to the user through WAN2.
- (5). The user will receive the DNS reply with the IP address of WAN1.
- (6). The browser will initiate an HTTP request to the WAN1 IP address.
- (7). The HTTP request will be send to MH-1000's URL Host Map.
- (8). The Host Map will then redirect the HTTP request to the HTTP server.
- (9). The HTTP server will reply.
- (10). The URL Host Map will route the packet through WAN1 to the user.
- (11). Finally, the client will receive an HTTP reply packet.

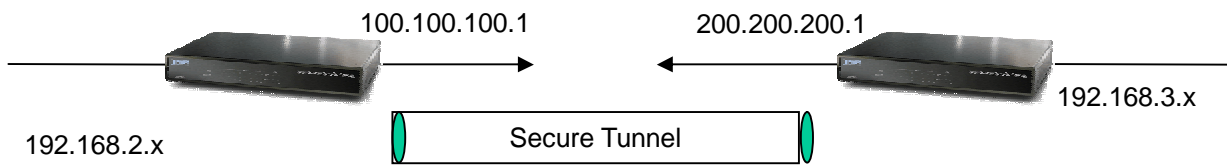
## 2.6 Virtual Private Networking

A Virtual Private Network (VPN) enables you to send data between two computers across a shared or public network in a manner that emulates the properties of a point-to-point private link. As such, it is perfect for connecting branch offices to headquarters across the Internet in a secure fashion.

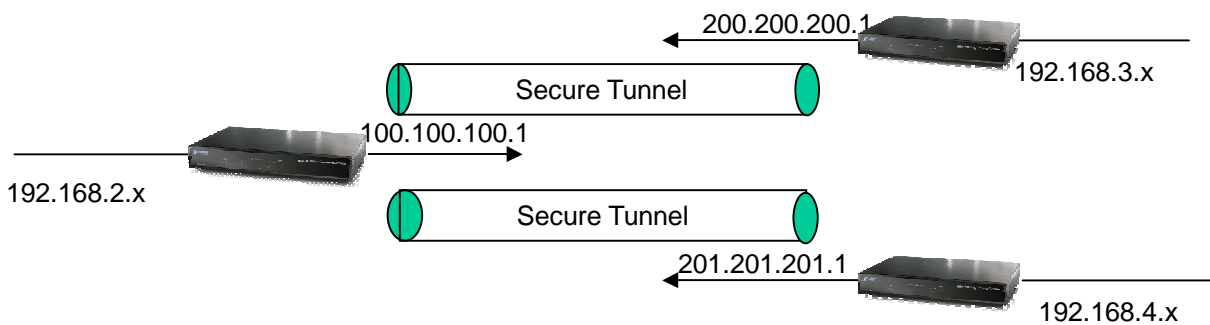
The following section discusses Virtual Private Networking with MH-1000.

### 2.6.1 General VPN Setup

There are typically three different VPN scenarios. The first is a **Gateway to Gateway** setup, where two remote gateways communicate over the Internet via a secure tunnel.



The next type of VPN setup is the **Gateway to Multiple Gateway** setup, where one gateway (Headquarters) is communicating with multiple gateways (Branch Offices) over the Internet. As with all VPNs, data is kept secure with secure tunnels.



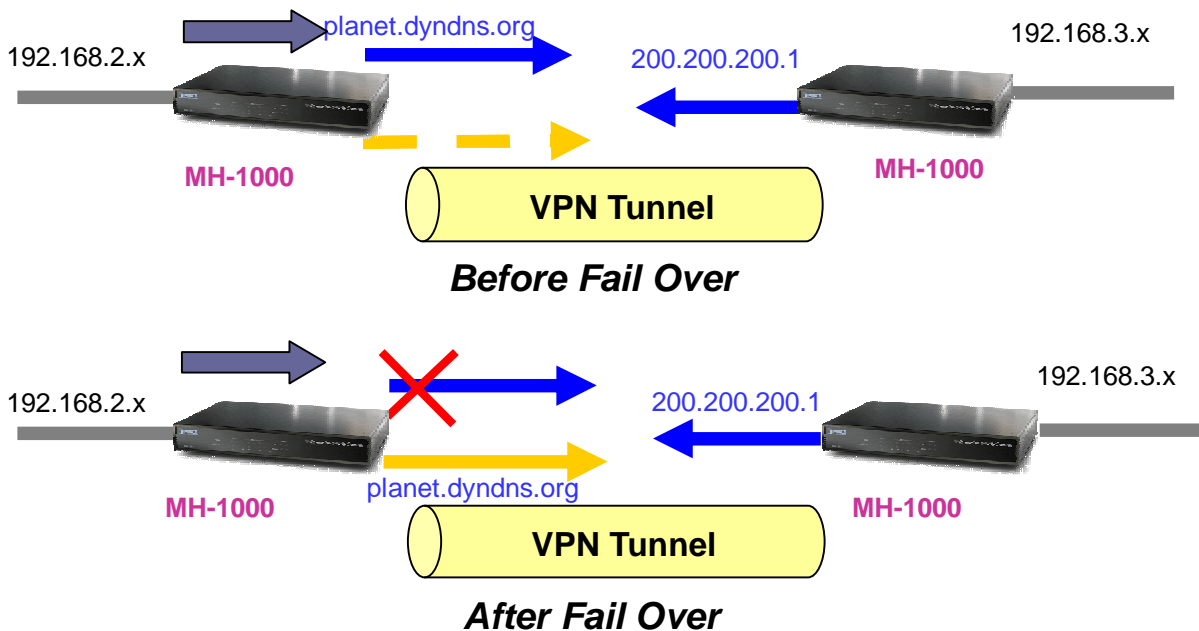
The final type of VPN setup is the **Client to Gateway**. A good example of where this can be applied is when a remote sales person accesses the corporate network over a secure VPN tunnel.



VPN[D2] provides a flexible, cost-efficient, and reliable way for companies of all sizes to stay connected. One of the most important steps in setting up a VPN is proper planning. The following sections demonstrate the various ways of using MH-1000 to setup your VPN.

## 2.6.2 VPN Planning - Fail Over

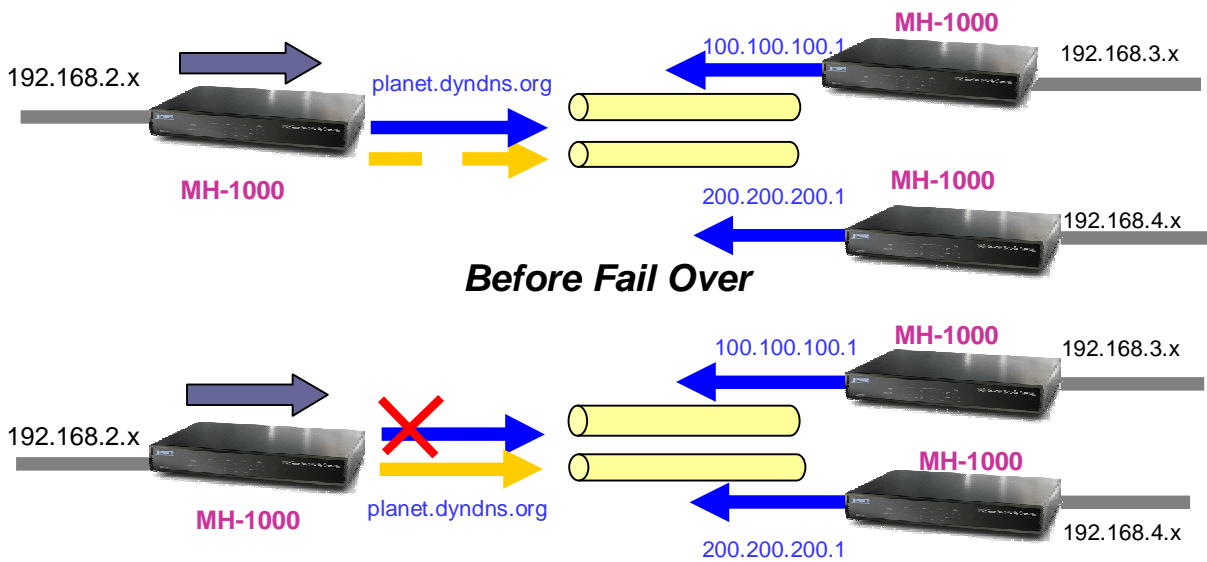
Configuring your VPN with Fail Over allows MH-1000 to automatically default to WAN2 should WAN1 fail.



Because the dynamic domain name planet.dyndns.org is configured for both WAN1 and WAN2, the active WAN port will announce the domain name through the WAN IP address. The remote gateway will then be able to connect to the VPN through the domain name.

In this Gateway to Gateway example, MH-1000 is communicating to a remote gateway using WAN1 through a secure VPN tunnel. Should WAN1 fail, outbound traffic from MH-1000 will automatically be redirected to WAN2. This process is completely transparent to the remote gateway, as MH-1000 will automatically update the domain name (planet.dyndns.org) with the WAN2 IP address. Configuring a Gateway to Multiple Gateway setup with Fail Over is similar, as shown below:



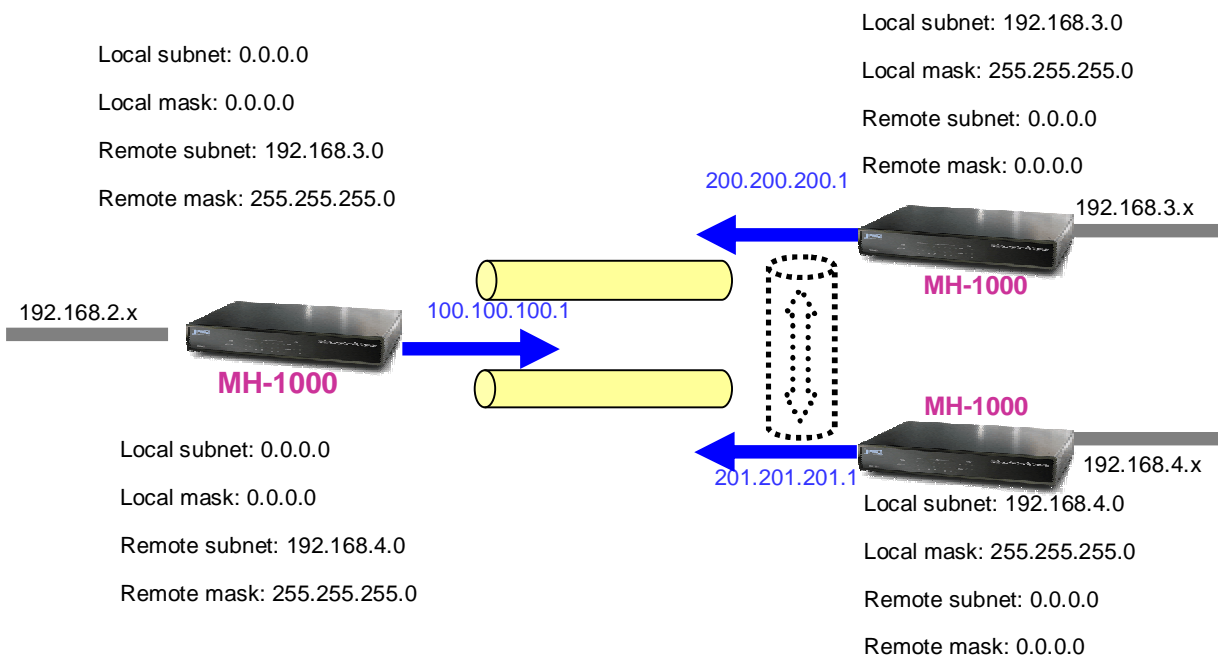


Configuring MH-1000 for Fail Over provides added reliability to your VPN.

### 2.6.3 Concentrator

The VPN Concentrator provides an easy way for branch offices to connect to headquarter through a VPN tunnel. All branch office traffic will be redirected to the VPN tunnel to headquarter with the exception of LAN-side traffic. This way, all branch offices can connect to each other through headquarter via the headquarter's firewall management. You can also configure MH-1000 to function as a VPN Concentrator:

Please refer to appendix D for example settings.



## Chapter 3: Getting Started

### 3.1 Overview

MH-1000 is designed to be a powerful and flexible network device that is also easy to use. With an intuitive web-based configuration, MH-1000 allows you to administer your network via virtually any Java-enabled web browser and is fully compatible with Linux, Mac OS, and Windows 98/ME/NT/2000/XP operating systems.

The following chapter takes you through the very first steps to configuring your network for MH-1000. Take a look and see how easy it is to get your network up and running.

### 3.2 Before You Begin

In order to simplify the configuration process and increase the efficiency of your network, you should consider the following items before setting up your network for the first time:

#### 1. Plan your network

Decide whether you are going to use one or both WAN ports. For one WAN port, you may need a fully qualified domain name either for convenience or if you have a dynamic IP address. If you are going to use both WAN ports, determine whether you are going to use them in fail over mode for increased network reliability or load balancing mode for maximum bandwidth efficiency. See Chapter 2: Router Applications for more information.

#### 2. Set up your accounts

Have access to the Internet and locate the Internet Service Provider (ISP) configuration information. Each MH-1000 WAN port must be configured separately, whether you are using a separate ISP for each WAN port or are having the traffic of both WAN ports routed through the same ISP.

#### 3. Determine your network management approach

MH-1000 is capable of remote management. However, this feature is not active by default. If you reset the device, remote administration must be enabled again. If you decide to manage your network remotely, be sure to change the default password for security reason.

#### 4. Prepare to physically connect MH-1000 to Cable or DSL modems and a computer.

### 3.3 Configuring PCs for TCP/IP Networking

In order for your networked PCs to communicate with your router, they must have the following characteristics:

1. Have a properly installed and functioning Ethernet Network Interface Card (NIC).
2. Be connected to MH-1000, either directly or through an external repeater hub via an Ethernet cable.

3. Have TCP/IP installed and configured with an IP address.

The IP address for each PC may be a fixed IP address or one that is obtained from a DHCP server. If using a fixed IP address, it is important to remember that it must be in the same subnet as the router. **The default IP address of MH-1000 is 192.168.1.1** with a subnet mask of 255.255.255.0. Using the default configuration, networked PCs must reside in the same subnet, and have an IP address in the range of 192.168.1.2 to 192.168.1.254. However, you'll find that the quickest and easiest way to configure the IP addresses for your PCs is to obtain the IP addresses automatically by using the router as a DHCP server.

If you are unable to access the web configuration interface, check to see if you have any software-based firewalls installed on your PCs, as they can cause problems accessing the 192.168.1.1 IP address of MH-1000.

The following sections outline how to set up your PCs for TCP/IP networking. Refer to the applicable section for your PC's operating system.

### 3.3.1 Overview

Before you begin, make sure that the TCP/IP protocol and a functioning Ethernet network adapter is installed on each of your PCs.

The following operating systems already include the necessary software components you need to install TCP/IP on your PCs:

- Windows 95/98/Me/NT/2000/XP
- Mac OS 7 and later

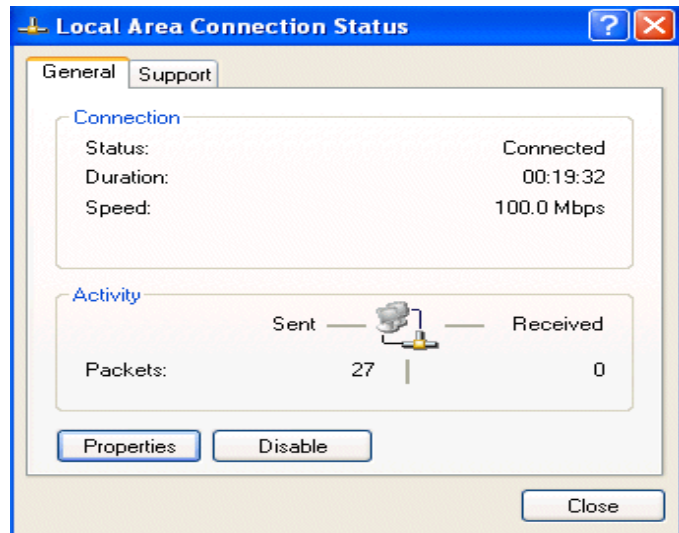
Any TCP/IP capable workstation can be used to communicate with or through MH-1000. To configure other types of workstations, please consult the manufacturer's documentation.

### 3.3.2 Windows XP

1. Go to Start / Control Panel (in Classic View). In the Control Panel, double-click on Network Connections.
2. Double-click Local Area Connection.



3. In the Local Area Connection Status window, click Properties.

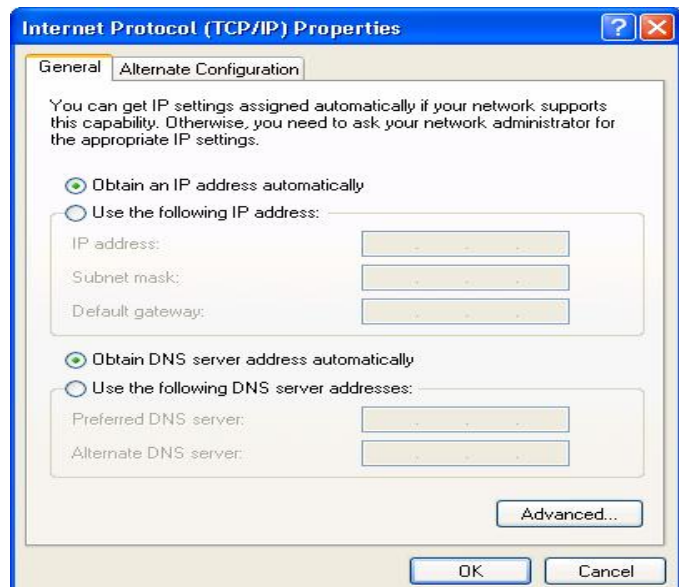


4. Select **Internet Protocol (TCP/IP)** and click **Properties**.



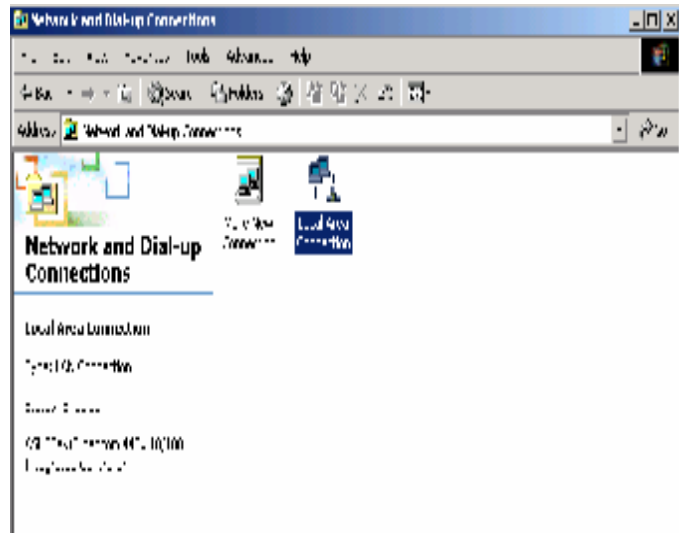
5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** radio buttons.

6. Click **OK** to finish the configuration.

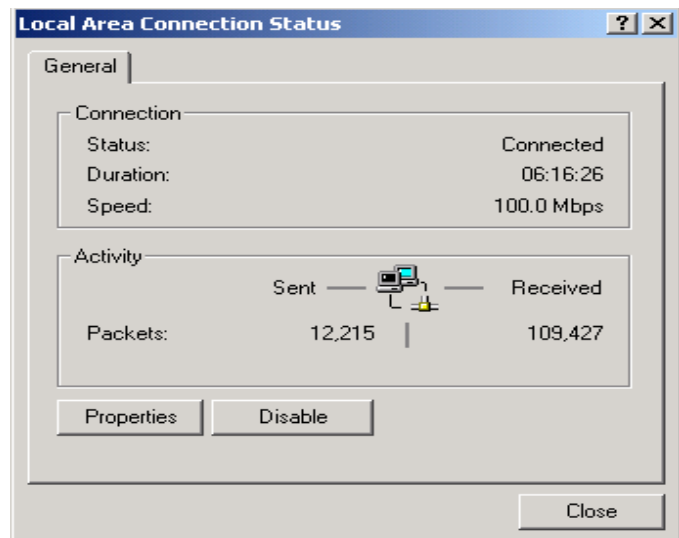


### 3.3.3 Windows 2000

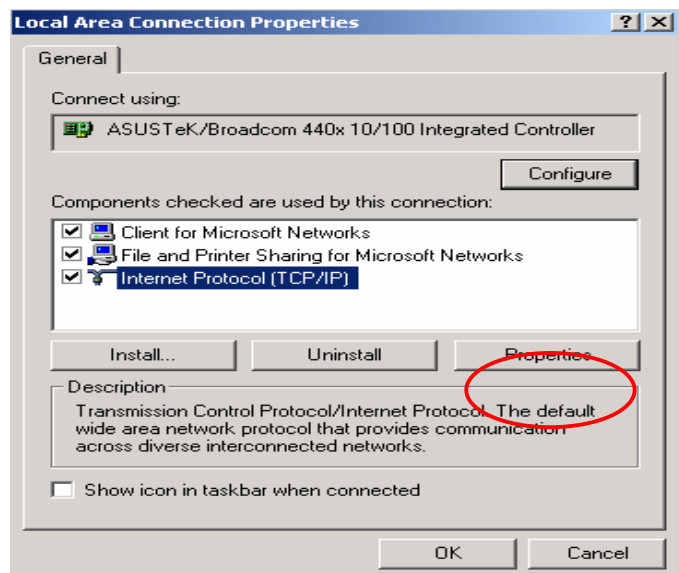
1. Go to Start / Settings / Control Panel. In the Control Panel, double-click on Network and Dial-up Connections.
2. Double-click Local Area Connection.



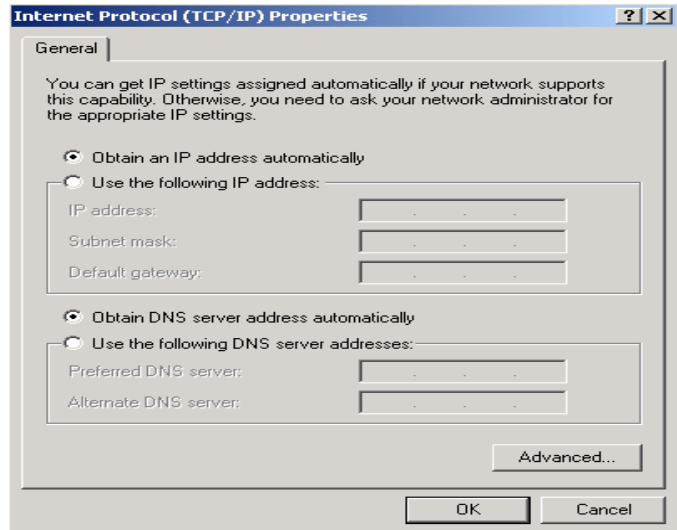
3. In the **Local Area Connection Status** window click **Properties**.



4. Select **Internet Protocol (TCP/IP)** and click **Properties**.

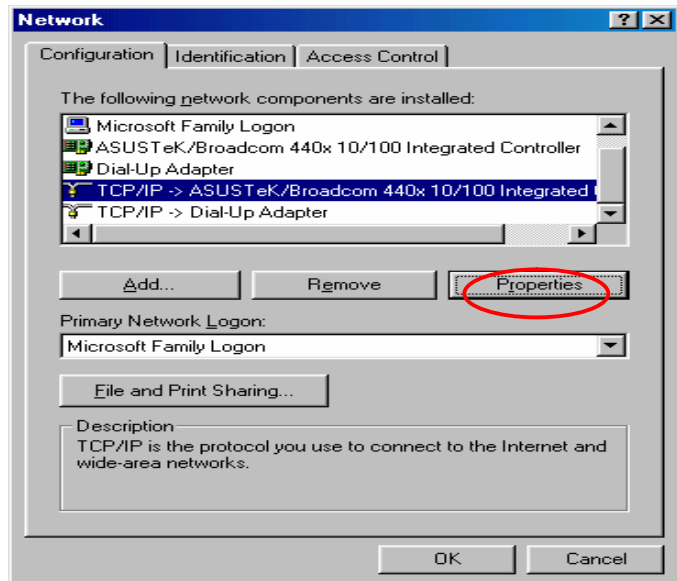


5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** radio buttons.
6. Click **OK** to finish the configuration.

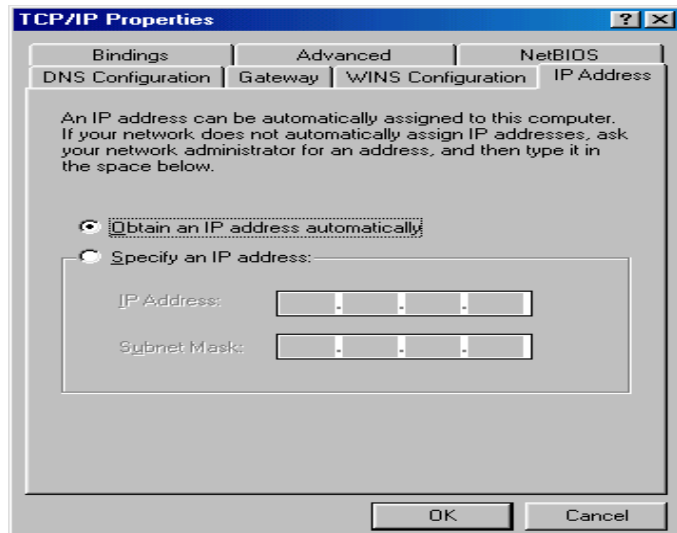


### 3.3.4 Windows 95/98/ME

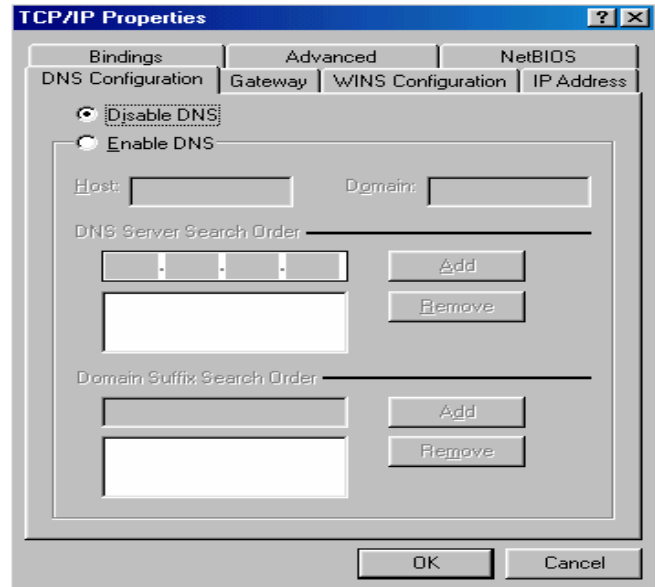
1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network** and choose the **Configuration** tab.
2. Select **TCP/IP ->NE2000 Compatible**, or the name of your Network Interface Card (NIC) in your PC.



3. Select the **Obtain an IP address automatically** radio button.

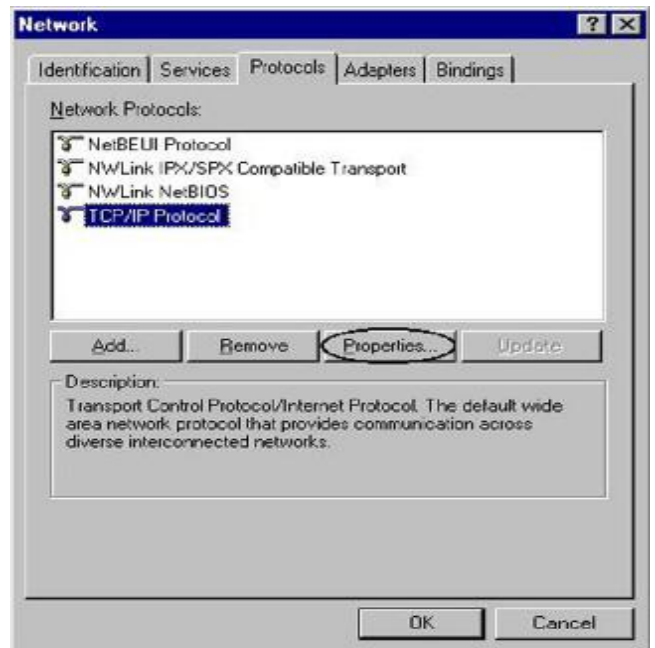


4. Then select the **DNS Configuration** tab.
5. Select the **Disable DNS** radio button and click **OK** to finish the configuration.

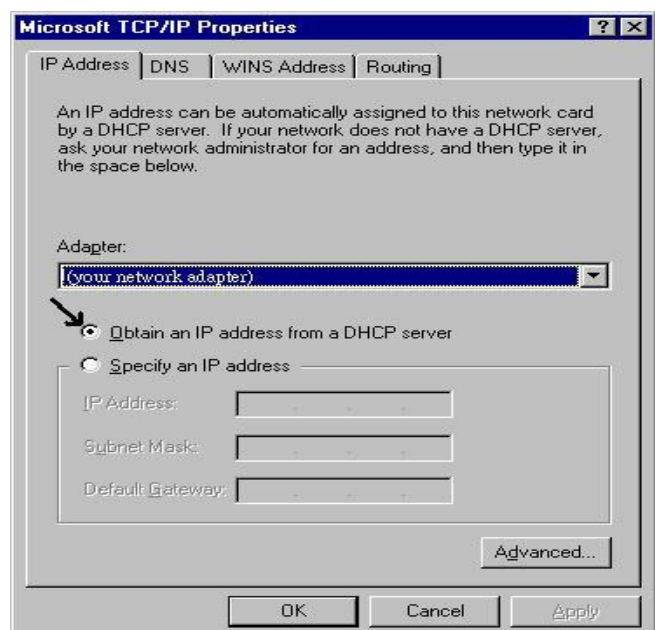


### 3.3.5 Windows NT 4.0

1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network** and choose the **Protocols** tab.
2. Select **TCP/IP Protocol** and click **Properties**.



3. Select the **Obtain an IP address from a DHCP server** radio button and click **OK**.



## 3.4 Factory Default Settings

### 3.4.1 User name and password

The default user name and password are "**admin**" and "**admin**" respectively.

If you ever forget your user name and/or password, you can restore your MH-1000 to its factory settings by holding the Reset button on the back of your router until the Status LED begins to blink. Please note that doing this will also erase any previous router settings that you have made. The Status LED will remain solid as the device boots. Once the boot sequence is complete, the LED will shut off, indicating that MH-1000 is ready.

### 3.4.2 LAN and WAN Port Addresses

The default values for LAN and WAN ports are shown below:

LAN Port		WAN Port
IP address	192.168.1.1	The DHCP Client is <b>enabled</b> to automatically get the WAN port configuration from the ISP.
Subnet Mask	255.255.255.0	
DHCP server function	Enabled	
IP addresses for distribution to PCs	100 IP addresses continuing from 192.168.1.100 through 192.168.1.199	

## 3.5 Information from Your ISP

### 3.5.1 Protocols

Before configuring this device, you have to check with your ISP (Internet Service Provider) to find out what kind of service is provided such as DHCP, Static IP, PPPoE, or PPTP. The following table outlines each of these protocols:

<b>DHCP</b>	Configure this WAN interface to use DHCP client protocol to get an IP address from your ISP automatically. Your ISP provides an IP address to the router dynamically when logging in.
<b>Static IP</b>	Configure this WAN interface with a specific IP address. This IP address should be provided by your ISP.
<b>PPPoE</b>	PPPoE (PPP over Ethernet) is known as a dial-up DSL or cable service. It is designed to integrate the broadband services into the current widely deployed, easy-to-use, and low-cost dial-up-access networking infrastructure.



<b>PPTP</b>	If your ISP provides a PPTP connection, you can use the PPTP protocol to establish a connection to your ISP.
<b>Big Pond</b>	The Big [D3]Pond login for Telstra cable in Australia.

If your account uses PPP over Ethernet (PPPoE), you will need to enter your login name and password when configuring your MH-1000. After the network and firewall are configured, MH-1000 will login automatically, and you will no longer need to run the login program from your PC.

### 3.5.2 Web Configuration Interface

MH-1000 includes a Web Configuration Interface for easy administration via virtually any browser on your network. To access this interface, open your web browser, enter the IP address of your router, which by default is **192.168.1.1**, and click **Go**. A user name and password window prompt will appear. Enter your user name and password (the default user name and password are "admin" and "admin") to access the Web Configuration Interface.



If the Web Configuration Interface appears, congratulations! You are now ready to configure your MH-1000. If you are having trouble accessing the interface, please refer to **Chapter 5: Troubleshooting** for possible resolutions.

## Chapter 4: Router Configuration

### 4.1 Overview

The Web Configuration Interface makes it easy for you to manage your network via any PC connected to it. On the Web Configuration homepage, you will see the navigation pane located on the left hand side. From it, you will be able to select various options used to configure your router.



1. Click **Apply** if you would like to apply the settings on the current screen to the device. The settings will be effective immediately, however the configuration is not saved yet and the settings will be erased if you power off or restart the device.
2. Click **SAVE CONFIG** to save the current settings permanently to the device.
3. Click **RESTART** to restart the device. There are two options to restart the device.
  - Select **Current Settings** if you would like to restart using the current configuration.
  - Select **Factory Default Settings** if you would like to restart using the factory default configuration.
4. To exit the router's web interface, click **LOGOUT**. Please ensure that you have saved your configuration settings before you logout. Be aware that the router is restricted to only one PC accessing the web configuration interface at a time. Once a PC has logged into the web interface, other PCs cannot gain access until the current PC has logged out. If the previous PC forgets to logout, the second PC can access the page after a user-defined period (5 minutes by default).

The following sections will show you how to configure your router using the Web Configuration Interface.

## 4.2 Status

The Status menu displays the various options that have been selected and a number of statistics about your MH-1000. In this menu, you will find the following sections:

- ARP Table
- Routing Table
- Session Table
- DHCP Table
- IPsec Status
- PPTP Status
- Traffic Statistics
- System Log
- IPsec Log

**PLANET** Multi-Homing Security Gateway MH-1000

**Status** Refresh

**Device Information**

Device Name	MH-1000
System Up Time	0: 3:20:50 (day:hour:min:sec)
Current Time	Mon Aug 1 08:20:38 2005 <span style="float: right;">Sync Now</span>
Private LAN MAC Address	00:04:ed:46:02:5b
Public WAN1 MAC Address	00:04:ed:46:02:5c
Public WAN2 MAC Address	00:04:ed:46:02:5d
Firmware Version	1.04c
Home URL	<a href="#">PLANET Technology Corporation</a>

**LAN**

IP Address	192.168.1.1
Netmask	255.255.255.0
DHCP Server	Enabled

**WAN1**

Connection Method	Connect by Static IP Settings
IP Address	192.168.99.96
Netmask	255.255.255.0
Gateway	192.168.99.253
DNS	168.95.1.1
Up Time	0: 2:22:44 (day:hour:min:sec)

**WAN2**

Connection Method	No Link
IP Address	
Netmask	
Gateway	
DNS	
Up Time	

SAVE CONFIG RESTART LOGOUT

## 4.2.1 ARP Table

The Address Resolution Protocol (ARP) Table shows the mapping of Internet (IP) addresses to Ethernet (MAC) addresses. This is a quick way to determine the MAC address of your PC's network interface to use with the router's Firewall – MAC Address Filter function. See the **Firewall** section of this chapter for more information on this feature.

No.	IP Address	MAC Address	Interface	Static
1	192.168.1.2	00:00:09:09:79:2D	LAN	no
2	192.168.1.101	00:00:09:09:79:2D	LAN	no
3	192.168.03.253	00:30:4F:3E:0F:5C	WAN1	no

**No.:** Number of the list.

**IP Address:** A list of IP addresses of devices on your LAN.

**MAC Address:** The Media Access Control (MAC) addresses for each device on your LAN.

**Interface:** The interface name (on the router) that this IP address connects to.

**Static:** Static status of the ARP table entry.

- **NO** indicates dynamically generated ARP table entries.
- **YES** indicates static ARP table entries added by the user.

## 4.2.2 Routing Table

The Routing Table displays the current path for transmitted packets. Both static and dynamic routes are displayed.

No.	Destination	Netmask	Gateway/Interface	Cost
1	192.168.1.0	255.255.255.0	0.0.0.0/LAN	0
2	192.168.0.0	255.255.0.0	0.0.0.0/WAN1	1
3	0.0.0.0	0.0.0.0	192.168.03.253/WAN1	0

**No.:** Number of the list.

**Destination:** The IP address of the destination network.

**Netmask:** The destination netmask address.

**Gateway/Interface:** The IP address of the gateway or existing interface that this route will use.

**Cost:** The number of hops counted as the cost of the route.

### 4.2.3 Session Table

The NAT Session Table displays a list of current sessions for both incoming and outgoing traffic with protocol type, source IP, source port, destination IP and destination port, each page shows 10 sessions.

**Session Table**

No.	Protocol	From IP	From Port	To IP	To Port
1	TCP	192.168.1.100	2710	192.168.1.1	80
2	TCP	192.168.1.101	2711	192.168.1.1	80
3	UDP	192.168.1.100	33043	70.176.231.190	5080
4	TCP	192.168.1.100	2712	192.168.1.1	80
5	TCP	192.168.1.101	2713	192.168.1.1	80
6	UDP	192.168.1.100	33043	84.201.56.3	5025
7	TCP	192.168.1.100	2710	192.168.1.1	80
8	TCP	192.168.1.101	2711	192.168.1.1	80
9	TCP	192.168.1.100	2714	192.168.1.1	80

Session 1 9 of 9, 1/1.

Filter From IP From Port To IP To Port

First Previous Next Last Jump to session GO

**No.:** Number of the list.

**Protocol:** Protocol type of the Session.

**From IP:** Source IP of the session.

**From port:** source port of the session.

**To IP:** Destination IP of the session.

**To port:** Destination port of the session.

#### Sessions:

**Filter:** when the presented field is filled, please click Filter button.

**From IP:** please input the source IP you would like to filter.

**From port:** please input the source port you would like to filter.

**To IP:** please input the destination IP you would like to filter.

**To port:** please input the destination port you would like to filter.

**First:** To the first page.

**Previous:** To the previous page.

**Next:** To the next page.

**Last:** To the last page.

**Jump to the session:** please input the session number you would like to see and press "GO"

### 4.2.4 DHCP Table

The DHCP Table displays a list of IP addresses that have been assigned to PCs on your network via Dynamic Host Configuration Protocol (DHCP).

**DHCP Table**  
DHCP IP Assignment Table

No.	IP Address	Device Name	MAC Address	Lease Time
1	192.168.1.100	752D3C-D12	00:0e:a3:0f:8e:52	243690

Refresh

**No.:** Number of the list.

**IP Address:** A list of IP addresses of devices on your LAN.

**Device Name:** The host name (computer name) of the client.

**MAC Address:** The MAC address of client.

**Lease Time:** The expired time for the IP address.

#### 4.2.5 IPsec Status

The IPsec Status window displays the status of the IPsec Tunnels that are currently configured on your MH-1000.

**IPsec Status**  
IPsec Tunnels

Name	Enable	Status	Local Network	Remote Network	Remote Gateway	SA	Action
------	--------	--------	---------------	----------------	----------------	----	--------

**Name:** The name you assigned to the particular IPsec entry.

**Enable:** Whether the IPsec connection is currently Enable or Disable.

**Status:** Whether the IPsec is Active, Inactive or Disable.

**Local Subnet:** The local IP address or subnet used.

**Remote Subnet:** The subnet of the remote site.

**Remote Gateway:** The remote gateway IP address.

**SA:** The Security Association for this IPsec entry.

**Action:** Manually connect or drop the tunnel.

#### 4.2.6 PPTP Status

The PPTP Status window displays the status of the PPTP Tunnels that are currently configured on your MH-1000.

PPTP Status						
PPTP Accounts						
Name	Enable	Status	Type	Peer Network	Connect By	Action

**Name:** The name you assigned to the particular PPTP entry.

**Enable:** Whether the PPTP connection is currently Enable or Disable.

**Status:** Whether the PPTP is Active, Inactive or Disable.

**Type:** Whether the Connection type is Remote Access or LAN to LAN

**Peer Network:** The Remote subnet for LAN to LAN as connection type.

**Connect by:** The remote address when connected.

**Action:** Manually drop the tunnel.

#### 4.2.7 Traffic Statistic

The Traffic Statistics window displays both sent and received sent data (in Bytes/sec) over one hour duration. The line in red represents WAN1, while the line in blue represents WAN2.

Traffic Statistics		
Statistics		
WAN1	Rx Bytes: 345094 Tx Bytes: 1201751	Tx Packets: 4185 Tx Packets: 1120
WAN2	Rx Bytes: 1 Tx Bytes: 80010	Rx Packets: 1 Tx Packets: 210

Diagram

Display:

Legend: ■ WAN1 Traffic, ■ WAN2 Traffic

**WAN1:** Transmitted (Tx) and Received (Rx) bytes and packets for WAN1.

**WAN2:** Transmitted (Tx) and Received (Rx) bytes and packets for WAN2.

**Display:** Allows you to change the units of measurement for the traffic graph.

## 4.2.8 System Log

This window displays MH-1000's System Log entries. Major events are logged on this window.

The screenshot shows the 'System Log' window of the Planet Multi-Homing Security Gateway (MH-1000). The sidebar menu on the left includes options like Status, ARP Table, Routing Table, Session Table, DHCP Table, IPsec Status, PPTP Status, Traffic Statistics, System Log (highlighted with red checkmarks), IPsec Log, Quick Start, Configuration, and Save Config to Flash. The main content area displays a list of log entries with the following text:

Timestamp	Event Description
Aug 1 05:00:26	Initialize WAN for failover mode.
Aug 1 05:00:26	Switch active gateway to WAN1
Aug 1 05:00:26	Connecting to ISP for WAN1.
Aug 1 05:00:28	DHCP client - send discover
Aug 1 05:00:30	DHCP client - send discover
Aug 1 05:00:32	DHCP client - send discover
Aug 1 05:00:37	DHCP fail to obtain lease.
Aug 1 05:01:26	Fail to synchronize with time server.
Aug 1 05:01:37	DHCP client - send discover
Aug 1 05:01:39	DHCP client - send discover
Aug 1 05:01:41	DHCP client - send discover
Aug 1 05:01:45	DHCP fail to obtain lease.

At the bottom of the log window, there are four buttons: Refresh, Clear Log, Send Log, and Save Log.

**Refresh:** Refresh the System Log.

**Clear Log:** Clear the System Log.

**Send Log:** Send the System Log to your email account. You can set the email address in **Configuration >**

**System > Email Alert.** See the **Email Alert** section for more details.

## 4.2.9 IPsec Log

This page displays the router's IPsec Log entries. Major events are logged to this window.

The screenshot shows the 'IPsec Log' window of the Planet Multi-Homing Security Gateway (MH-1000). The sidebar menu on the left includes options like Status, ARP Table, Routing Table, Session Table, DHCP Table, IPsec Status, PPTP Status, Traffic Statistics, System Log, IPsec Log (highlighted with red checkmarks), Quick Start, Configuration, and Save Config to Flash. The main content area displays the 'IPsec Log' header and a large empty box for log entries. At the bottom of the log window, there are four buttons: Refresh, Clear Log, Send Log, and Save Log.

**Refresh:** Refresh the IPsec Log.

**Clear Log:** Clear the IPsec Log.

**Send Log:** Send IPsec Log to your email account. You can set the email address in **Configuration >**



**System > Email Alert.** See the **Email Alert** section for more details.

Please refer to **Appendix F: IPSec Log Events** for more information on log events.

## 4.3 Quick Start

The Quick Start menu allows you to quickly configure your network for Internet access using the most basic settings.

Connection Method: Select your router's connection to the Internet. Selections include **Obtain an IP Address Automatically**, **Static IP Settings**, **PPPoE Settings**, **PPTP Settings**, and **Big Pond Settings**.

### 4.3.1 DHCP

The following is information regarding your ISP that you will need to enter in order to properly configure your Internet connection. If you select to **Obtain an IP Address Automatically**, these will be automatically set for you, provided that your ISP dynamically assigns an IP address.

The screenshot shows the Planet Multi-Homing Security Gateway web interface. The left sidebar contains navigation options: Status, Quick Start (highlighted with a red double-checkmark), Quick Start WAN1, Quick Start WAN2, Configuration, and Save Config to Flash. The main content area is titled 'Quick Start WAN1' and shows the 'DHCP' configuration section. The 'Connection Method' is set to 'Obtain an IP Address Automatically' via a dropdown menu. Below it is a text input field for 'Host Name'. At the bottom of the section are 'Apply' and 'Reset' buttons.

### 4.3.2 Static IP

The screenshot shows the Planet Multi-Homing Security Gateway web interface. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Quick Start WAN1' and shows the 'Static IP' configuration section. The 'Connection Method' is set to 'Static IP Settings' via a dropdown menu. Below it is a table for entering IP settings:

IP assigned by your ISP	192	168	99	94
IP Subnet Mask	255	255	255	0
ISP Gateway Address	192	168	99	253
Primary DNS	168	95	1	1
Secondary DNS	0	0	0	0

At the bottom of the section are 'Apply' and 'Reset' buttons.

**IP assigned by your ISP:** Enter the assigned IP address from your IP.

**IP Subnet Mask:** Enter your IP subnet mask.

**ISP Gateway Address:** Enter your ISP gateway address.

**Primary DNS:** Enter your primary DNS.

**Secondary DNS:** Enter your secondary DNS.

Click **Apply** to save your changes. To reset to defaults, click **Reset**.

### 4.3.3 PPPoE

The screenshot shows the 'Quick Start WAN1' configuration page for PPPoE. The interface includes a left-hand navigation menu with options: Status, Quick Start, Quick Start WAN1 (highlighted), Quick Start WAN2, Configuration, and Save Config to Flash. The main configuration area is titled 'Quick Start WAN1' and 'PPPoE'. It contains the following fields and options:

- Connection Method: PPPoE Settings (dropdown)
- Username: [text input]
- Password: [text input]
- Retype Password: [text input]
- Connection: Always Connect (dropdown)
- Idle Time: 10 minutes (dropdown)

At the bottom of the configuration area are 'Apply' and 'Reset' buttons.

**Username:** Enter your user name.

**Password:** Enter your password.

**Retype Password:** Retype your password.

**Connection:** Select whether the connection should **Always Connect** or **Trigger on Demand**.

- **Always Connect:** If you want the router to establish a PPPoE session when starting up and to automatically re-establish the PPPoE session when disconnected by the ISP.

- **Trigger on Demand:** If you want to establish a PPPoE session only when there is a packet requesting access to the Internet (i.e. when a program on your computer attempts to access the Internet).

**Idle Time:** Auto-disconnect the router when there is no activity on the line for a predetermined period of time. Select the idle time from the drop down menu. Active if **Trigger on Demand** is selected.

Click **Apply** to save your changes. To reset to defaults, click **Reset**.

### 4.3.4 PPTP

The screenshot shows the 'Quick Start WAN1' configuration page for PPTP. The interface includes a left-hand navigation menu with options: Status, Quick Start, Quick Start WAN1 (highlighted), Quick Start WAN2, Configuration, and Save Config to Flash. The main configuration area is titled 'Quick Start WAN1' and 'PPTP'. It contains the following fields and options:

- Connection Method: PPTP Settings (dropdown)
- Username: [text input]
- Password: [text input]
- Retype Password: [text input]
- PPTP Client IP: [0] [0] [0] [0] (four separate input boxes)
- PPTP Client IP Netmask: [0] [0] [0] [0] (four separate input boxes)
- PPTP Client IP Gateway: [0] [0] [0] [0] (four separate input boxes)
- PPTP Server IP: [0] [0] [0] [0] (four separate input boxes)
- Connection: Always Connect (dropdown)
- Idle Time: 10 minutes (dropdown)

At the bottom of the configuration area are 'Apply' and 'Reset' buttons.

**Username:** Enter your user name.

**Password:** Enter your password.

**Retype Password:** Retype your password.

**PPTP Client IP:** Enter the PPTP Client IP provided by your ISP.

**PPTP Client IP Netmask:** Enter the PPTP Client IP Netmask provided by your ISP.

**PPTP Client IP Gateway:** Enter the PPTP Client IP Gateway provided by your ISP.

**PPTP Server IP:** Enter the PPTP Server IP provided by your ISP.

**Connection:** Select whether the connection should **Always Connect** or **Trigger on Demand**.

- **Always Connect:** If you want the router to establish a PPTP session when starting up and to automatically re-establish the PPTP session when disconnected by the ISP.

- **Trigger on Demand:** If you want to establish a PPTP session only when there is a packet requesting access to the Internet (i.e. when a program on your computer attempts to access the Internet).

**Idle Time:** Auto-disconnect the router when there is no activity on the line for a predetermined period of time. Select the idle time from the drop down menu. Active if **Trigger on Demand** is selected.

Click **Apply** to save your changes. To reset to defaults, click **Reset**.

### 4.3.5 Big Pond

The screenshot shows the configuration interface for a Multi-Homing Security Gateway (MH-1000). The main title is 'Multi-Homing Security Gateway' and the model number 'MH-1000' is displayed in the top right. The interface includes a navigation menu on the left with options: Status, Quick Start, Quick Start WAN1 (highlighted), Quick Start WAN2, Configuration, and Save Config to Flash. The main content area is titled 'Quick Start WAN1' and contains a 'Big Pond' section. This section includes a 'Connection Method' dropdown menu set to 'Big Pond Settings', and input fields for 'Username', 'Password', and 'Retype Password'. Below these fields is a 'Login server' field with four separate input boxes for IP address digits. At the bottom of the form are 'Apply' and 'Reset' buttons.

**Username:** Enter your user name.

**Password:** Enter your password.

**Retype Password:** Retype your password.

**Login Server:** Enter the IP of the Login server provided by your ISP.

Click **Apply** to save your changes. To reset to defaults, click **Reset**.

For detailed instructions on configuring WAN settings, please refer to the **WAN** section of this chapter.

## 4.4 Configuration

The **Configuration** menu allows you to set many of the operating parameters of MH-1000. In this menu, you will find the following sections:

- LAN
- WAN
- Dual WAN
- System
- Firewall
- VPN
- QoS
- Virtual Server
- Advanced

These items are described below in the following sections.

### 4.4.1 LAN

There are two items within this section: **Ethernet** and **DHCP Server**.

The screenshot shows the Planet Multi-Homing Security Gateway (MH-1000) configuration interface. The left sidebar contains a navigation menu with the following items: Status, Quick Start, Configuration, LAN (highlighted), Ethernet, DHCP Server, and WAN. The main content area displays the 'Ethernet' configuration form. The form has a title 'Ethernet' and a section 'Parameters'. The 'IP Address' field is set to 192.168.1.1. The 'Subnet Mask' field is set to 255.255.255.0. The 'RIP' section has a dropdown menu set to 'Disable', and two radio buttons: 'RIP-2B' (selected) and 'RIP-2M'. There are 'Apply' and 'Reset' buttons at the bottom of the form.

#### 4.4.1.1 Ethernet

The screenshot shows the Planet Multi-Homing Security Gateway (MH-1000) configuration interface. The left sidebar contains a navigation menu with the following items: Status, Quick Start, Configuration, LAN, Ethernet (highlighted), DHCP Server, and WAN. The main content area displays the 'Ethernet' configuration form. The form has a title 'Ethernet' and a section 'Parameters'. The 'IP Address' field is set to 192.168.1.1. The 'Subnet Mask' field is set to 255.255.255.0. The 'RIP' section has a dropdown menu set to 'Disable', and two radio buttons: 'RIP-2B' (selected) and 'RIP-2M'. There are 'Apply' and 'Reset' buttons at the bottom of the form.

**IP Address:** Enter the internal LAN IP address for MH-1000 (192.168.1.1 by default).

**Subnet Mask:** Enter the subnet mask (255.255.255.0 by default).

**RIP:** RIP v2 Broadcast and RIP v2 Multicast. Check to enable RIP.

### 4.4.1.2 DHCP Server

In this menu, you can disable or enable the Dynamic Host Configuration Protocol (DHCP) server. The DHCP protocol allows your MH-1000 to dynamically assign IP addresses to PCs on your network if they are configured to automatically obtain IP addresses.

The screenshot shows the DHCP Server configuration interface. The 'DHCP Server Functions' section has the 'Enable' radio button selected. The 'IP Pool Range From' is 192.168.1.100 and 'IP Pool Range to' is 192.168.1.199. The 'Primary DNS Server', 'Secondary DNS Server', 'Primary WINS Server', and 'Secondary WINS Server' are all set to 0.0.0.0. The 'Domain Name' field is empty. At the bottom, there are 'Apply', 'Reset', and 'Fixed Host' buttons.

To disable the router's DHCP Server, select the **Disable** radio button, and then click **Apply**. When the DHCP Server is disabled, you will need to manually assign a fixed IP address to each PC on your network, and set the default gateway for each PC to the IP address of the router (192.168.1.1 by default).

To configure the router's DHCP Server, select the **Enable** radio button, and then configure parameters of the DHCP Server including the IP Pool (starting IP address and ending IP address to be allocated to the PCs on your network), DNS Server, WINS Server, and Domain Name. These details are sent to each DHCP client when they request an IP address from the DHCP server. Click **Apply** to enable this function.

Fixed Host allows specific computer/network clients to have a reserved IP address.

This screenshot is identical to the one above, showing the DHCP Server configuration page. The 'Fixed Host' button at the bottom is circled in red.

**IP Address:** Enter the IP address that you want to reserve for the above MAC address.

**MAC Address:** Enter the MAC address of the PC or server you wish to be assigned a reserved IP.

**Candidates:** You can also select the Candidates which are referred from the ARP table for automatic input.

Click the **Apply** button to add the configuration into the Host Table. Press the **Delete** button to delete a configuration from the Host Table.

#### 4.4.2 WAN

WAN refers to your Wide Area Network connection. In most cases, this means your router's connection to the Internet through your ISP. MH-1000 features Dual WAN capability.

The WAN menu contains two items: ISP Settings and Bandwidth Settings.

##### 4.4.2.1 ISP Settings

This WAN Service Table displays the different WAN connections that are configured on MH-1000. To edit any of these connections, click **Edit**. You will be taken to the following menu.

**PLANET** Multi-Homing Security Gateway MH-1000

**WAN1**

**Static IP**

Connection Method: Static IP Settings (dropdown menu open showing: Obtain an IP Address Automatically, Static IP Settings, PPPoE Settings, PPTP Settings, Big Pond Settings)

IP assigned by your ISP: Obtain an IP Address Automatically

IP Subnet Mask: [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ]

ISP Gateway Address: [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ]

MAC Address: [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ]

Primary DNS: 168 95 1 1

Secondary DNS: 0 0 0 0

RIP: Disable (dropdown menu)  RIP-2B  RIP-2M

MTU: 1500

Apply Reset

**Connection Method:** Select how your router will connect to the Internet. Selections include **Obtain an IP Address Automatically**, **Static IP Settings**, **PPPoE Settings**, **PPTP Settings**, and **Big Pond Settings**. For each WAN port, the factory default is DHCP. If your ISP does not use DHCP, select the correct connection method and configure the connection accordingly. Configurable items will vary depending on the connection method selected.

#### 4.4.2.1.1 DHCP

**PLANET** Multi-Homing Security Gateway MH-1000

**WAN1**

**DHCP**

Connection Method: Obtain an IP Address Automatically

Host Name: [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ]

MAC Address: [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ]

DNS:  Your ISP requires you to manually setup DNS settings

Primary DNS: 168 95 1 1

Secondary DNS: 0 0 0 0

RIP: Disable (dropdown menu)  RIP-2B  RIP-2M

MTU: 1500

Apply Reset

**Host Name:** Some ISPs authenticate logins using this field.

**MAC Address:** If your ISP requires you to input a WAN Ethernet MAC, check the checkbox and enter your MAC address in the blanks below.

**DNS:** If your ISP requires you to manually setup DNS settings, check the checkbox and enter your primary and secondary DNS.

**RIP:** To activate RIP, select **Send**, **Receive**, or **Both** from the drop down menu. To disable RIP, select **Disable** from the drop down menu.

**MTU:** Enter the Maximum Transmission Unit (MTU) for your network.

Click **Apply** to save your changes. To reset to defaults, click **Reset**.

#### 4.4.2.1.2 Static IP

The screenshot shows the configuration page for WAN1 Static IP. The interface includes a left-hand navigation menu with options like Status, Quick Start, Configuration, LAN, WAN, ISP Settings, Bandwidth Settings, Dual WAN, System, Firewall, VPN, DoS, Virtual Server, and Advanced. The main content area is titled 'WAN1 Static IP' and contains the following fields:

Connection Method	Static IP Settings			
IP assigned by your ISP	192	168	99	94
IP Subnet Mask	255	255	255	0
ISP Gateway Address	192	168	99	253
MAC Address	<input type="checkbox"/> Your ISP requires you to input Ethernet MAC			
	MAC Address	00	00	00
Primary DNS	168	95	1	1
Secondary DNS	0	0	0	0
RIP	Disable <input checked="" type="radio"/> RIP-2B <input type="radio"/> RIP-2M			
MTU	1500			

At the bottom of the configuration area are 'Apply' and 'Reset' buttons.

**IP assigned by your ISP:** Enter the static IP assigned by your ISP.

**IP Subnet Mask:** Enter the IP subnet mask provided by your ISP.

**ISP Gateway Address:** Enter the ISP gateway address provided by your ISP.

**MAC Address:** If your ISP requires you to input a WAN Ethernet MAC, check the checkbox and enter your MAC address in the blanks below.

**Primary DNS:** Enter the primary DNS provided by your ISP.

**Secondary DNS:** Enter the secondary DNS provided by your ISP.

**RIP:** To activate RIP, select **Send**, **Receive**, or **Both** from the drop down menu. To disable RIP, select **Disable** from the drop down menu.

**MTU:** Enter the Maximum Transmission Unit (MTU) for your network.

Click **Apply** to save your changes. To reset to defaults, click **Reset**.

#### 4.4.2.1.3 PPPoE



The screenshot shows the configuration page for WAN1 PPPoE. The left sidebar contains a navigation menu with options: Status, Quick Start, Configuration, LAN, WAN, ISP Settings, Bandwidth Settings, Dual WAN, System, Firewall, VPN, QoS, Virtual Server, Advanced, and Save Config to Flash. The main configuration area is titled 'WAN1' and 'PPPoE'. It includes the following fields and options:

- Connection Method:** A dropdown menu set to 'PPPoE Settings'.
- Username:** An empty text input field.
- Password:** An empty text input field.
- Retype Password:** An empty text input field.
- Connection:** A dropdown menu set to 'Always Connect'.
- Idle Time:** A dropdown menu set to '10 minutes'.
- IP assigned by your ISP:** Two radio buttons: 'Dynamic (IP automatically assigned by your ISP)' (selected) and 'Fixed (Your ISP requires you to input IP address)'. Below the 'Fixed' option are four empty input fields for IP address digits.
- MAC Address:** A checkbox 'Your ISP requires you to input WAN Ethernet MAC' (unchecked). Below it are six empty input fields for MAC address digits.
- DNS:** A checkbox 'Your ISP requires you to manually setup DNS settings' (checked). Below it are two rows of four input fields each: 'Primary DNS' (168, 95, 1, 1) and 'Secondary DNS' (0, 0, 0, 0).
- RIP:** A dropdown menu set to 'Disable' and two radio buttons: 'RIP-2B' (selected) and 'RIP-2M'.
- MTU:** An input field containing '1492'.

At the bottom of the configuration area are 'Apply' and 'Reset' buttons.

**Username:** Enter your user name.

**Password:** Enter your password.

**Retype Password:** Retype your password.

**Connection:** Select whether the connection should **Always Connect** or **Trigger on Demand**.

- **Always Connect:** If you want the router to establish a PPPoE session when starting up and to automatically re-establish the PPPoE session when disconnected by the ISP.
- **Trigger on Demand:** If you want to establish a PPPoE session only when there is a packet requesting access to the Internet (i.e. when a program on your computer attempts to access the Internet).

**Idle Time:** Auto-disconnect the router when there is no activity on the line for a predetermined period of time. Select the idle time from the drop down menu. Active if **Trigger on Demand** is selected.

**IP Assigned by your ISP:** If your IP is dynamically assigned by your ISP, select the **Dynamic** radio button. If your IP assigns a static IP address, select the **Static** radio button, and input your IP address in the blank provided.

**MAC Address:** If your ISP requires you to input a WAN Ethernet MAC, check the checkbox and enter your MAC address in the blanks below.

**DNS:** If your ISP requires you to manually setup DNS settings, check the checkbox and enter your primary and secondary DNS.

**RIP:** To activate RIP, select **Send**, **Receive**, or **Both** from the drop down menu. To disable RIP, select **Disable** from the drop down menu.

**MTU:** Enter the Maximum Transmission Unit (MTU) for your network.

Click **Apply** to save your changes. To reset to defaults, click **Reset**.

#### 4.4.2.1.4 PPTP Settings

The screenshot displays the configuration page for WAN1 PPTP settings. The left sidebar contains navigation options: Status, Quick Start, Configuration, LAN, WAN, ISP Settings, Bandwidth Settings, Dual WAN, System, Firewall, VPN, QoS, Virtual Server, Advanced, and Save Config to Flash. The main configuration area is titled 'WAN1 PPTP' and includes the following fields:

- Connection Method:** PPTP Settings (dropdown)
- Username:** [Text input]
- Password:** [Text input]
- Retype Password:** [Text input]
- PPTP Client IP:** [0][0][0][0] (IP address)
- PPTP Client IP Netmask:** [0][0][0][0] (Netmask)
- PPTP Client IP Gateway:** [0][0][0][0] (Gateway)
- PPTP Server IP:** [0][0][0][0] (Server IP)
- Connection:** Always Connect (dropdown)
- Idle Time:** 10 minutes (dropdown)
- IP assigned by your ISP:**
  - Dynamic (IP automatically assigned by your ISP)
  - Fixed (Your ISP requires you to input IP address)
- MAC Address:**
  - Your ISP requires you to input WAN Ethernet MAC
  - MAC Address: [00][00][00][00][00][00]
- DNS:**
  - Your ISP requires you to manually setup DNS settings
  - Primary DNS: [168][95][1][1]
  - Secondary DNS: [0][0][0][0]
- RIP:** Disable (dropdown),  RIP-2B,  RIP-2M
- MTU:** 1432

Buttons for 'Apply' and 'Reset' are located at the bottom of the configuration area.

**Username:** Enter your user name.

**Password:** Enter your password.

**Retype Password:** Retype your password.

**PPTP Client IP:** Enter the PPTP Client IP provided by your ISP.

**PPTP Client IP Netmask:** Enter the PPTP Client IP Netmask provided by your ISP.

**PPTP Client IP Gateway:** Enter the PPTP Client IP Gateway provided by your ISP.

**PPTP Server IP:** Enter the PPTP Server IP provided by your ISP.

**Connection:** Select whether the connection should **Always Connect** or **Trigger on Demand**.

- **Always Connect:** If you want the router to establish a PPTP session when starting up and to automatically re-establish the PPTP session when disconnected by the ISP.
- **Trigger on Demand:** If you want to establish a PPTP session only when there is a packet requesting access to the Internet (i.e. when a program on your computer attempts to access the Internet).

**Idle Time:** Auto-disconnect the router when there is no activity on the line for a predetermined period of time. Select the idle time from the drop down menu. Active if **Trigger on Demand** is selected.

**IP Assigned by your ISP:** If your IP is dynamically assigned by your ISP, select the **Dynamic** radio button. If your IP assigns a static IP address, select the **Static** radio button. This will take you to another page for inputting the IP address information.

**MAC Address:** If your ISP requires you to input a WAN Ethernet MAC, check the checkbox and enter your

MAC address in the blanks below.

**DNS:** If your ISP requires you to manually setup DNS settings, check the checkbox and enter your primary and secondary DNS.

**RIP:** To activate RIP, select **Send**, **Receive**, or **Both** from the drop down menu. To disable RIP, select **Disable** from the drop down menu.

**MTU:** Enter the Maximum Transmission Unit (MTU) for your network.

Click **Apply** to save your changes. To reset to defaults, click **Reset**.

#### 4.4.2.1.5 Big Pond Settings

The screenshot shows the configuration page for WAN1 Big Pond. The interface includes a left-hand navigation menu with options like Status, Quick Start, Configuration, LAN, WAN, ISP Settings, Bandwidth Settings, Dual WAN, System, Firewall, VPN, QoS, Virtual Server, Advanced, and Save Config to Flash. The main content area is titled 'WAN1 Big Pond' and contains the following fields:

- Connection Method:** A dropdown menu set to 'Big Pond Settings'.
- Username:** A text input field.
- Password:** A text input field.
- Retype Password:** A text input field.
- Login server:** Four numeric input fields for IP address.
- MAC Address:** A checkbox labeled 'Your ISP requires you to input WAN Ethernet MAC' and a field with six numeric input boxes for the MAC address.
- DNS:** A checkbox labeled 'Your ISP requires you to manually setup DNS settings'. Below it are fields for 'Primary DNS' (four numeric boxes: 168, 95, 1, 1) and 'Secondary DNS' (four numeric boxes: 0, 0, 0, 0).
- RIP:** A dropdown menu set to 'Disable' and two radio buttons for 'RIP-2B' (selected) and 'RIP-2M'.
- MTU:** A text input field containing '1500'.

At the bottom of the form are 'Apply' and 'Reset' buttons.

**Username:** Enter your user name.

**Password:** Enter your password.

**Retype Password:** Retype your password.

**Login Server:** Enter the IP of the Login server provided by your ISP.

**MAC Address:** If your ISP requires you to input a WAN Ethernet MAC, check the checkbox and enter your MAC address in the blanks below.

**DNS:** If your ISP requires you to manually setup DNS settings, check the checkbox and enter your primary and secondary DNS.

**RIP:** To activate RIP, select **Send**, **Receive**, or **Both** from the drop down menu. To disable RIP, select **Disable** from the drop down menu.

**MTU:** Enter the Maximum Transmission Unit (MTU) for your network.

Click **Apply** to save your changes. To reset to defaults, click **Reset**.

A simpler alternative is to select **Quick Start** from the main menu. Please see the **Quick Start** section of this chapter for more information.

### 4.4.2.2 Bandwidth settings

Under Bandwidth Settings, you can easily configure both inbound and outbound bandwidth for each WAN port.

**Bandwidth Settings**

Max Bandwidth Provided by ISP

WAN 1	Outbound Bandwidth	102400	kbps
	Inbound Bandwidth	102400	kbps
WAN 2	Outbound Bandwidth	102400	kbps
	Inbound Bandwidth	102400	kbps

(⚠ These bandwidth settings will be referenced by QoS and Loadbalance functions.)

Apply

**WAN1:** Enter your ISP inbound and outbound bandwidth for WAN1.

**WAN2:** Enter your ISP inbound and outbound bandwidth for WAN2.

**NOTE:** These values entered here are referenced by both QoS and Load Balancing functions.

### 4.4.3 Dual WAN

In this section, you can setup the fail over or load balance function, outbound load balance or inbound load balance function, or setup specific protocol to bind with specific WAN port. In this menu are the following sections: **General Settings**, **Outbound Load Balance**, **Inbound Load Balance**, and **Protocol Binding**.

#### 4.4.3.1 General Settings

**General Setting**

Dual WAN Mode

Mode  Load Balance  Fail Over

WAN Port Service Detection Policy

Service Detection (for load balance.)  Enable  Disable

Connectivity Decision Not in service when probing failed after 3 consecutive times.

Probe Cycle Every 30 seconds.

Probe WAN1  Gateway  Host 0 0 0 0

Probe WAN2  Gateway  Host 0 0 0 0

Failback to WAN1 when possible (for failover.)  Enable  Disable

Apply

**Mode:** You can select Load Balance or Fail Over.

**Service Detection:** Enables or disables the service detection feature. For fail over, the service detection function is enabled. For load balance, user is able to enable or disable it.

**Connectivity Decision:** Establishes the number of times probing the connection has to fail before the connection is judged as failed.

**Probe Cycle:** The number of seconds between each probe.

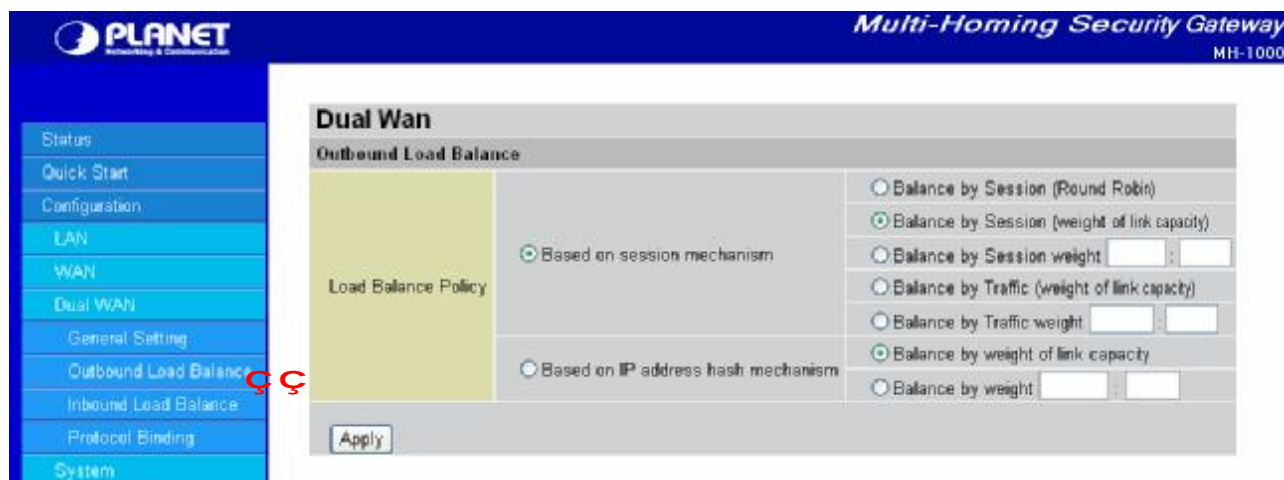
**Probe WAN1:** Determines if WAN1 is a gateway or host. If host is selected, please enter the IP address.

**Probe WAN2:** Determines if WAN2 is a gateway or host. If host is selected, please enter the IP address.

**Fail back to WAN1 when possible:** Enables or disables fail back to WAN1. This function only applies to fail over.

Click **Apply** to save your changes.

#### 4.4.3.2 Outbound Load Balance



Outbound Load Balancing on MH-1000 can be based on one of two methods:

1. Based on session mechanism
2. Based on IP address hash mechanism

Choose one by clicking the corresponding radio button.

**Based on session mechanism:** The source IP address and destination IP address might go through WAN1 or WAN2 according to policy settings in this mechanism. You can choose this mechanism if the applications the users use will not tell the difference of the WAN IP addresses. (some applications in the Internet need to identify the source IP address, e.g. Back, Forum, ...)

- **Balance by Session (Round Robin):** Balances session traffic based on a round robin method.
- **Balance by Session (weight of length capacity):** Balances session traffic based on weight of length capacity.
- **Balance by Session weight:** Balances session traffic based on a weight ratio. Enter the desired ratio in the blanks provided.
- **Balance by Traffic (weight of length capacity):** Balances traffic based on weight of link capacity.

- **Balance by Traffic weight:** Balances traffic based on a traffic weight ratio. Enter the desired ratio into the blanks provided.

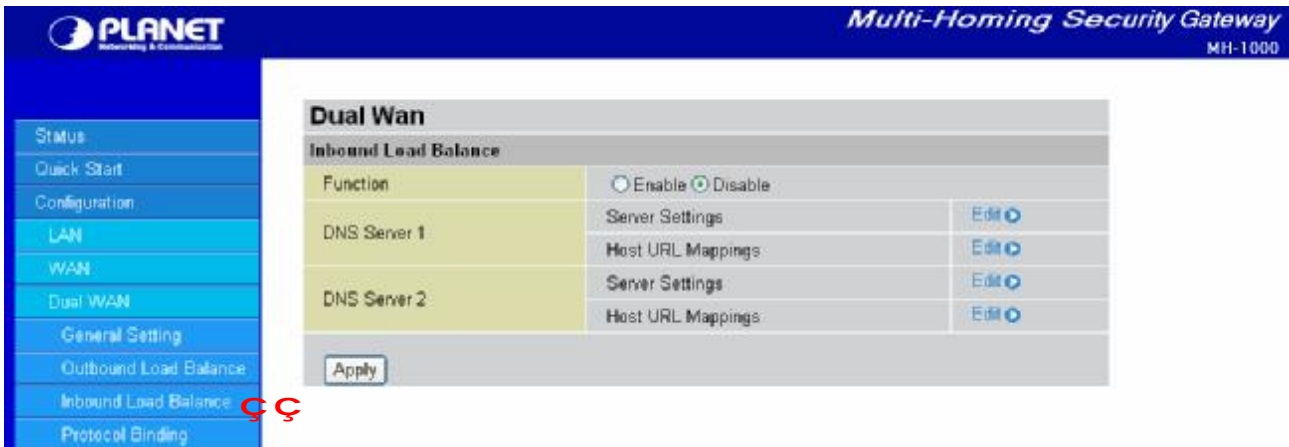
**Based on IP hash mechanism:** The source IP address and destination IP address will go through specific WAN port (WAN1 or WAN2) according to policy settings in this mechanism. This will assure that some applications will work when it would like to authenticate the source IP address.

- **Balance by weight of link capacity:** Uses an IP hash to balance traffic based on weight of link bandwidth capacity.

- **Balance by weight:** Uses an IP hash to balance traffic based on a ratio. Enter the desired ratio into the blanks provided.

Click **Apply** to save your changes.

#### 4.4.3.3 Inbound Load Balance



**Function:** Used to enable or disable inbound load balancing.

**DNS Server 1:** DNS Server 1 settings including Host URL mappings.

**DNS Server 2:** DNS Server 2 settings including Host URL mappings.

To edit server settings, click Edit. The following example illustrates DNS Server 1 settings. DNS Server 2 settings follow a similar procedure.

**SOA:**

**Domain Name:** The domain name of DNS Server 1. It is the name that you register on DNS organization. You have to fill-out the Fully Qualified Domain Name (FQDN) with an ending character (a dot) for this text field (ex:abc.com.). When you enter the following domain name, you can only input different chars without an ending dot, its name is then added with domain name, and it becomes FQDN.

**Primary Name Server:** The name assigned to the primary Name Server. (e.g: aaa, its FQDN is aaa.abc.com.).

**Admin. Mail Box:** The administrator's email account (e.g:admin@abc.com.)

**Serial Number:** It is the version number that keeps in the SOA record.

**Refresh Interval:** The interval refreshes are done. Denoted in seconds.

**Retry Interval:** The interval retries are done. Denoted in seconds.

**Expiration Time:** The length of time that can elapse before the zone is no longer authoritative. Denoted in seconds.

**Minimum TTL:** The minimum time to live. Denoted in seconds.

**NS Record:**

**Name Server:** The name of the Primary Name Server.

**MX Record:**

**Mail Exchanger:** The name of the mail server.

**IP Address:** The mail server IP address.

Click **Apply** to save your changes.

To edit the Host Mapping URL list, click **Edit**. This will open the Host Mapping URL table, which lists the current Host Mapping URLs.

The screenshot shows the 'Host URL Mapping List' table in the Multi-Homing Security Gateway web interface. The table has the following columns: Host URL, Domain Name, Local IP Address, Protocol, and Port Range. A 'Create' button is visible below the table header.

Host URL	Domain Name	Local IP Address	Protocol	Port Range
Create				

To add a host mapping URL to the list, click **Create**.

The screenshot shows the 'Host URL Mappings' configuration form. It includes fields for Domain Name (abc.com), Host URL, Private IP Address (with a Candidates dropdown), Protocol (Any), and Port Range (1-65535). There are also fields for Name1 and Name2, and an Apply button.

A Record	
Domain Name	abc.com
* Host URL	<input type="text"/>
Private IP Address <small>Candidates </small>	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
Protocol	Any
Port Range <small>Helper </small>	<input type="text"/> - <input type="text"/>
CNAME	
* Name1	<input type="text"/>
* Name2	<input type="text"/>
<small>* : Domain will be appended automatically in these fields.</small>	
Apply	

**Domain Name:** The domain name of the local host.

**Host URL:** The URL to be mapped.

**Private IP Address:** The IP address of the local host.

**Protocol:** You could also select the application type you would like to apply for automatic input.

**Port Range:** The port range of all incoming packets are accepted and processed by a local host with the specified private IP address.

- **Candidates:** You can also select the Candidates which are referred from the ARP table for automatic input.

- **Helper:** You could also select the application type you would like to apply for automatic input.

**Name1:** The Alias Host URL

**Name2:** The Alias Host URL

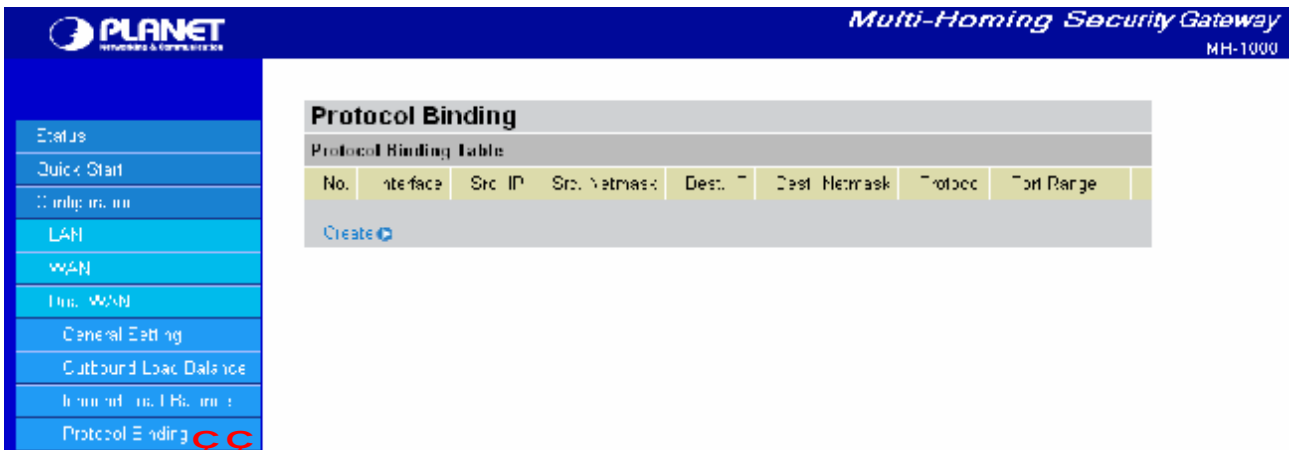
Click **Apply** to save your changes.



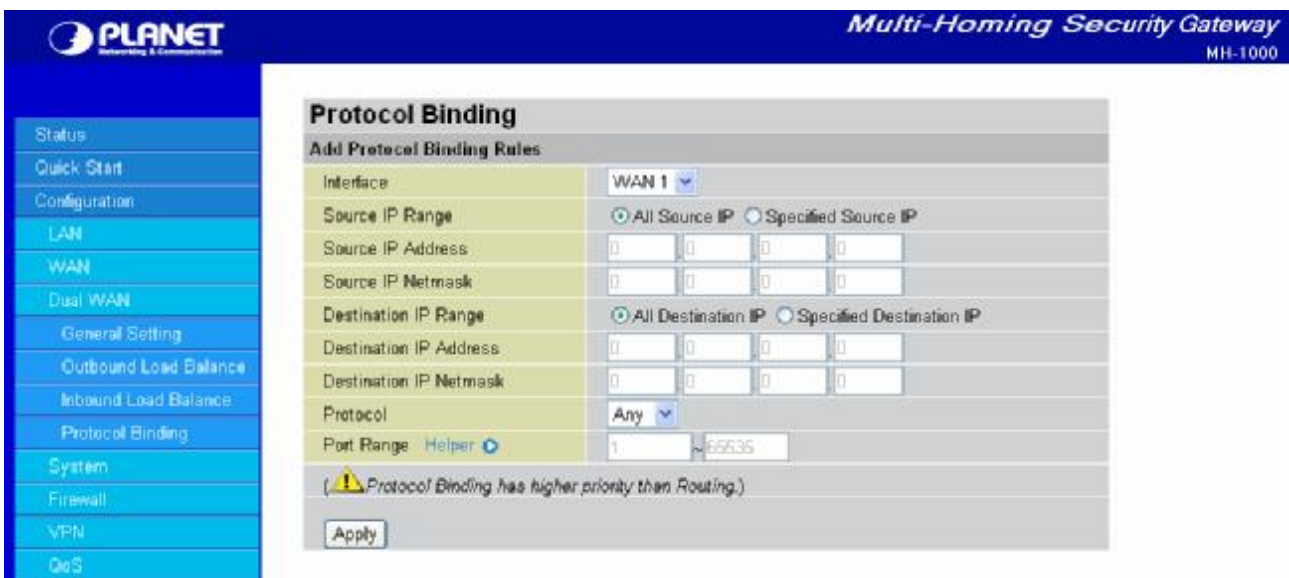
#### 4.4.3.4 Protocol Binding

Protocol Binding lets you direct specific traffic to go out from a specific WAN port. Click the **Create** button to create a new policy entry. Policies entered would tell specific types of Internet traffic from a particular range of IPs to go to a particular range of IPs with ONE WAN port, rather than using both of the WAN ports with load balancing.

(**NOTE:** If any policies are added in the Protocol Binding section, please note that it would take precedence over the settings that are already configured in the Load Balance Setting section.)



The Protocol Binding Table lists any protocol binding that has been configured. To add a new binding, click **Create**.



**Interface:** Choose which WAN port to use: WAN1, WAN2

**Source IP Range:**

- **All Source IP:** Click it to specify all source IPs.
- **Specified Source IP:** Click to specify a specific source IP address and source IP netmask.

**Source IP Address:** If Specified Source IP was chosen, here's where the IP can be entered.

**Source IP Netmask:** If Specified Source IP was chosen, here's where the subnet mask can be entered.

**Destination IP Range:**

- **All Destination IP:** Click it to specify all source IPs.
- **Specified Destination IP:** Click to specify a specific destination IP address and Destination IP Netmask.

**Destination IP Address:** If Specified Destination IP was chosen, here's where the IP can be entered.

**Destination IP Netmask:** If Specified Destination IP was chosen, here's where the subnet mask can be entered.

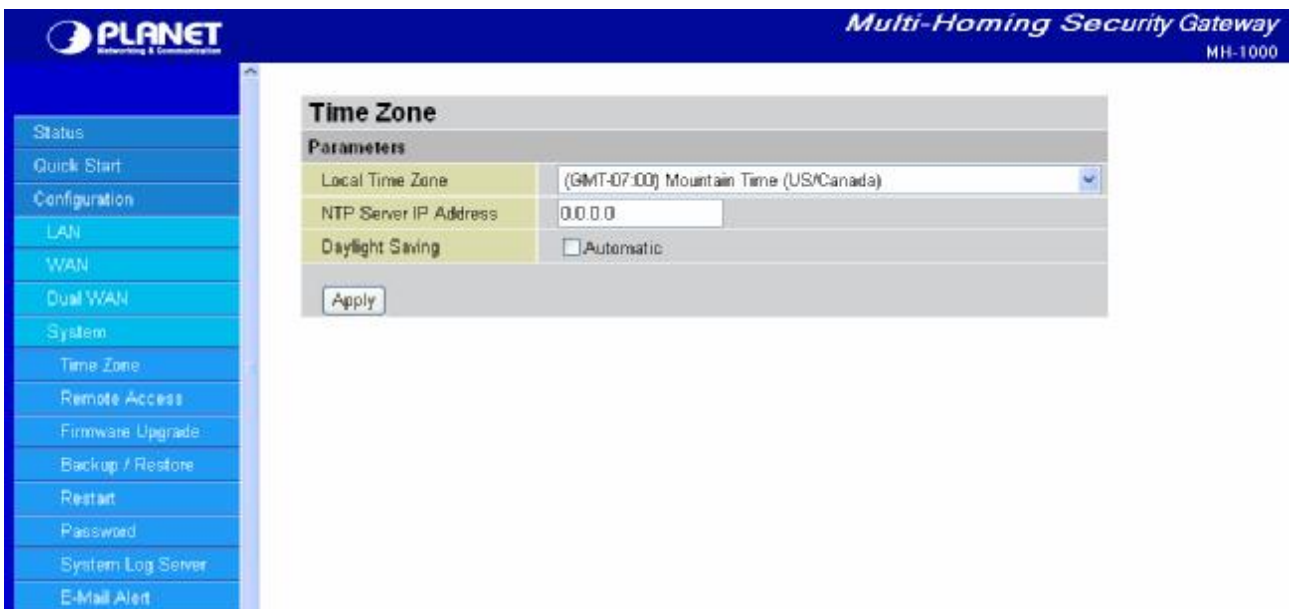
**Protocol:** The particular protocol of Internet traffic for the specified policy. Choose from **TCP**, **UDP**, or **Any**.

**Port Range:** The range of ports for the specified policy (if you only want to use one port, enter the same value in both boxes).

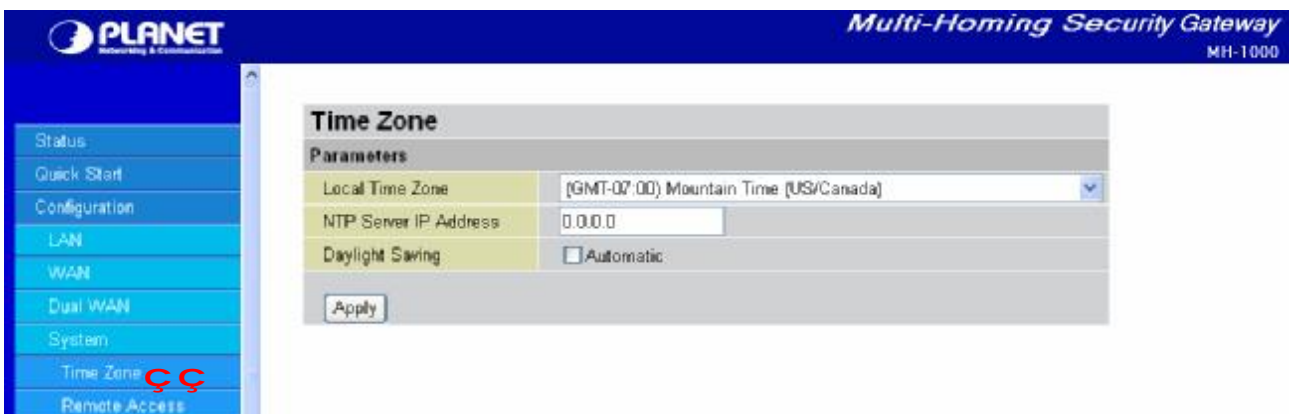
Click **Apply** to save your changes.

#### 4.4.4 System

The System menu allows you to adjust a variety of basic router settings, upgrade firmware, set up remote access, and more. In this menu are the following sections: **Time Zone**, **Remote Access**, **Firmware Upgrade**, **Backup/Restore**, **Restart**, **Password**, **System Log** and **Email Alert**.



##### 4.4.4.1 Time Zone

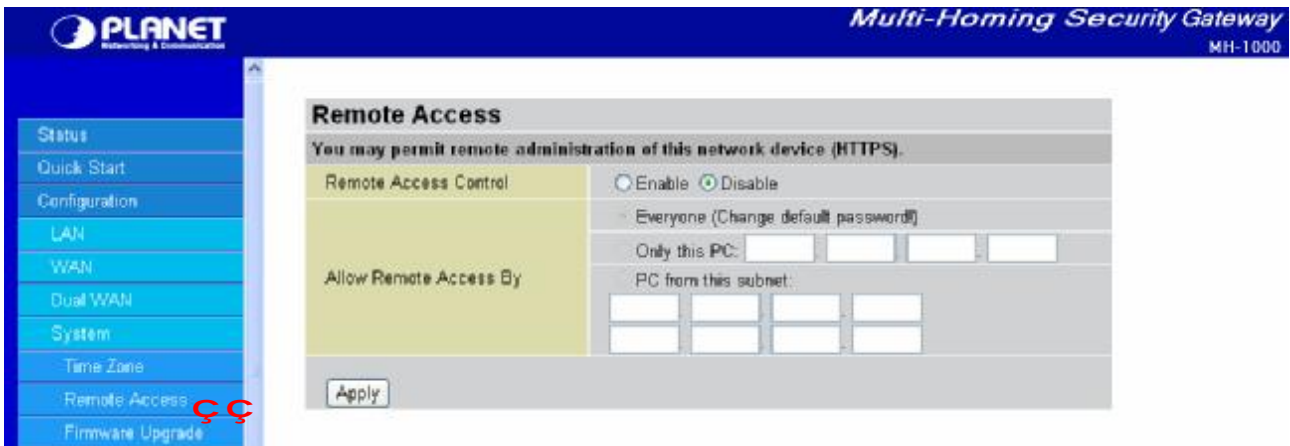


MH-1000 does not use an onboard real time clock; instead, it uses the Network Time Protocol (NTP) to

acquire the current time from an NTP server outside your network. Simply choose your local time zone, enter NTP Server IP Address, and click **Apply**. After connecting to the Internet, MH-1000 will retrieve the correct local time from the NTP server you have specified. Your ISP may provide an NTP server for you to use.

To have MH-1000 automatically adjust for Daylight Savings Time, check the **Automatic** checkbox.

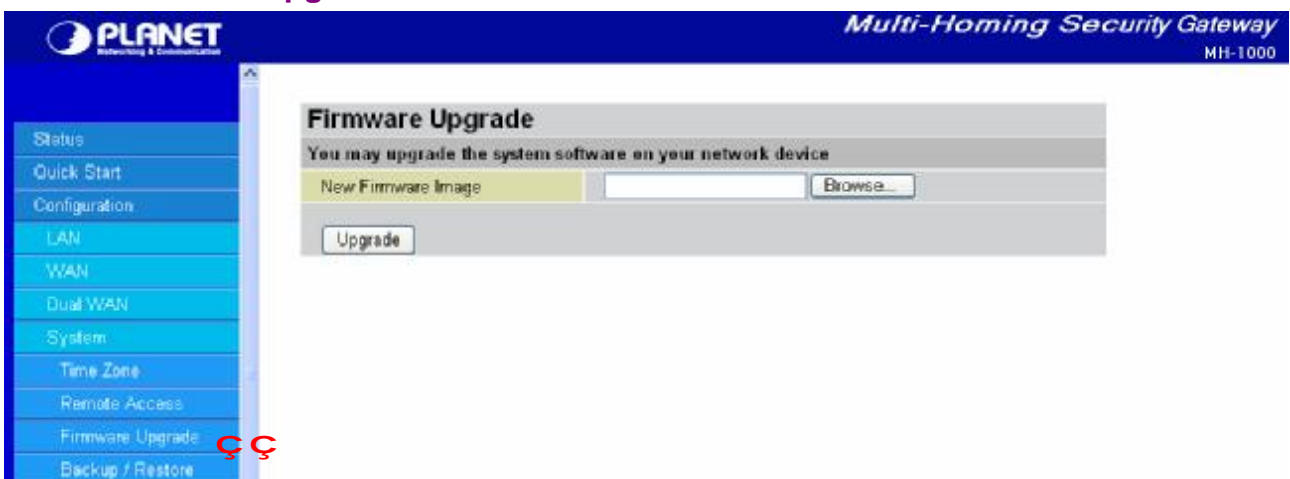
#### 4.4.4.2 Remote Access



To allow remote users to configure and manage MH-1000 through the Internet, select the **Enable** radio button. To deactivate remote access, select the **Disable** radio button. This function also enables you grant access from any PC or from a specific IP address. Click **Apply** to save your settings.

**NOTE:** When enabling remote access, be sure to change the default administration password for security reason.

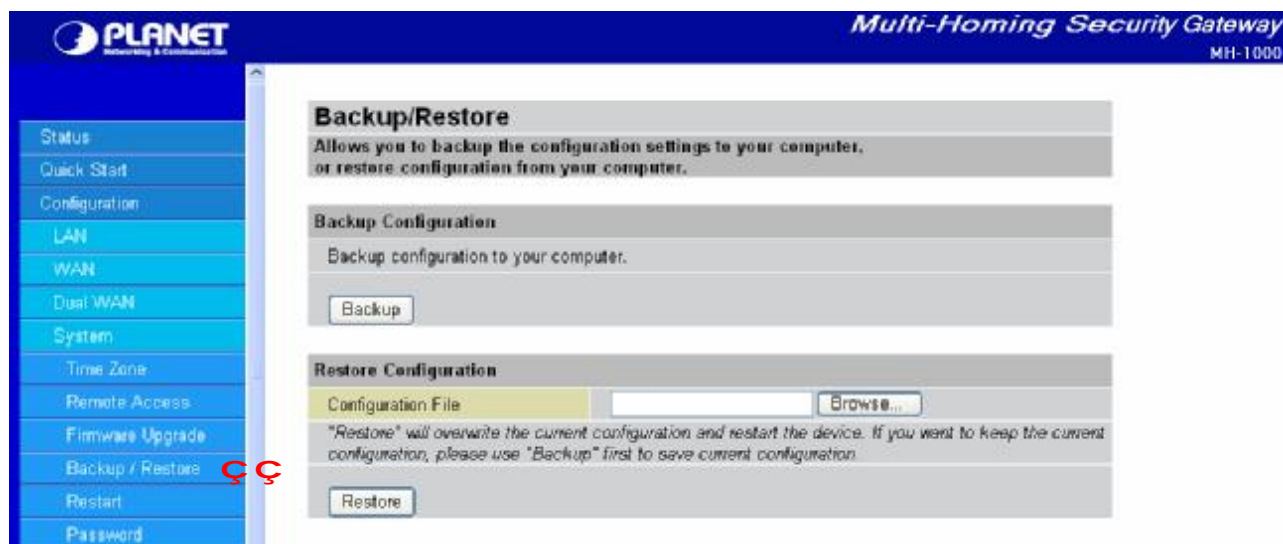
#### 4.4.4.3 Firmware Upgrade



Upgrading your MH-1000's firmware is a quick and easy way to enjoy increased functionality, better reliability, and ensure trouble-free operation. To upgrade your firmware, simply visit PLANET's website (<http://www.planet.com.tw>) and download the latest firmware image file for MH-1000. Next, click **Browse** and select the newly downloaded firmware file. Click **Upgrade** to complete the update.

**NOTE:** DO NOT power down the router or interrupt the firmware upgrade while it is still in process. Interrupting the firmware upgrade process could damage the router.

#### 4.4.4.4 Backup / Restore



This feature allows you to save and backup your router's current settings, or restore a previously saved backup. This is useful if you wish to experiment with different settings, knowing that you have a backup handy. It is advisable to backup your router's settings before making any significant changes to your router's configuration.

To backup your router's settings, click **Backup** and select where to save the settings backup file. You may also change the name of the file when saving if you wish to keep multiple backups. Click **OK** to save the file.

To restore a previously saved backup file, click **Browse**. You will be prompted to select a file from your PC to restore. Be sure to only restore setting files that have been generated by the Backup function, and that were created when using the same firmware version. Settings files saved to your PC should not be manually edited in any way. After selecting the settings file you wish to use, clicking **Restore** will load those settings into the router.

#### 4.4.4.5 Restart



The Restart feature allows you to easily restart MH-1000. To restart with your last saved configuration, select the **Current Settings** radio button and click **Restart**.

If you wish to restart the router using the factory default settings, select **Factory Default Settings** and click **Restart** to reboot MH-1000 with factory default settings.

You may also reset your router to factory default settings by holding the Reset button on the router until the Status LED begins to blink. Once MH-1000 completes the boot sequence, the Status LED will stop blinking.

#### 4.4.4.6 Password



In order to prevent unauthorized access to your router's configuration interface, it requires the administrator to login with a password. You can change your password by entering your new password in both fields. Click **Apply** to save your changes. Click **Reset** to reset to the default administration password (admin).

#### 4.4.4.7 System Log Server

This function allows MH-1000 to send system logs to an external Syslog Server. Syslog is an industry-standard protocol used to capture information about network activity. To enable this function, select the **Enable** radio button and enter your Syslog server IP address in the **Log Server IP Address** field. Click **Apply** to save your changes.

To disable this feature, simply select the **Disable** radio button and click **Apply**.

#### 4.4.4.8 E-mail Alert

The Email Alert function allows a log of security-related events (such as System Log and IPSec Log) to be sent to a specified email address.

**Email Alert:** You may enable or disable this function by selecting the appropriate radio button.

**Recipient's Email Address:** Enter the email address where you wish the alert logs to be sent.

**Sender's Email Address:** Enter the email address where you wish the alert logs to be sent by which address.

**SMTP Mail Server:** Enter your email account's outgoing mail server. It may be an IP address or a domain name.

**Mail Server Login:** Some SMTP servers may request users to login before serving. Select **Enable** to activate SMTP server login function, **Disable** to deactivate.

**Username:** Input the SMTP server's username.

**Password:** Input the SMTP server's password.

**Alert via Email when:** Select the frequency of each email update. Choose one of the five options:

- **Immediately:** The router will send an alert immediately.
- **Hourly:** The router will send an alert once every hour.
- **Daily:** The router will send an alert once a day. The exact time can be specified using the pull down menu.
- **Weekly:** The router will send an alert once a week.
- **When log is full:** The router will send an alert only when the log is full.

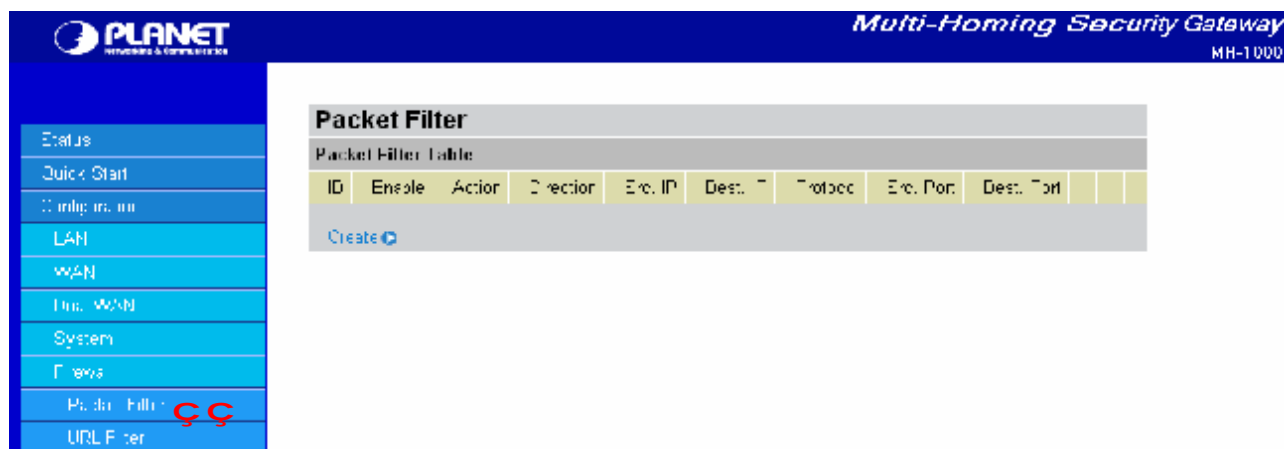
#### 4.4.5 Firewall

MH-1000 includes a full Stateful Packet Inspection (SPI) firewall for controlling Internet access from your LAN, and preventing attacks from hackers. Your router also acts as a "natural" Internet firewall when using Network Address Translation (NAT), as all PCs on your LAN will use private IP addresses that cannot be directly accessed from the Internet. Please see the WAN configuration section for more details.

The screenshot shows the Planet Multi-Homing Security Gateway (MH-1000) web interface. The top navigation bar includes the Planet logo and the text "Multi-Homing Security Gateway MH-1000". The left sidebar contains a menu with the following items: Status, Quick Start, Configuration, LAN, WAN, Dns, WAN, System, Filter, Packet Filter, URL Filter, LAN MAC Filter, Block WAN Request, and Intrusion Detection. The main content area is titled "Packet Filter" and contains a "Packet Filter Table" with the following columns: ID, Enable, Action, Direction, Src. IP, Dest. IP, Protocol, Src. Port, and Dest. Port. Below the table is a "Create" button.

You can find three items under the Firewall section: **Packet Filter**, **URL Filter**, and **Block WAN Request**.

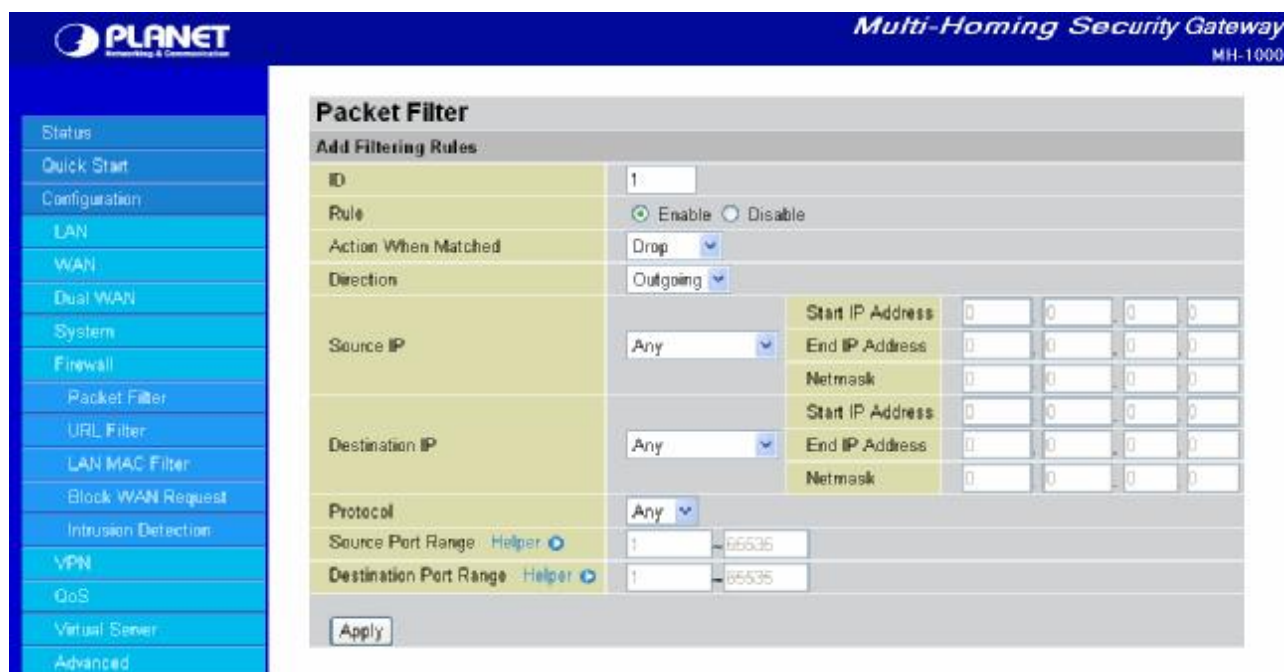
### 4.4.5.1 Packet Filter



The Packet Filter function is used to limit user access to certain sites on the Internet or LAN. The Filter Table displays all current filter rules. If there is an entry in the Filter Table, you can click **Edit** to modify the setting of this entry, click **Delete** to remove this entry, or click **Move** to change this entry's priority.

When the entry is upper, the priority is higher.

To create a new filter rule, click **Create**.



**ID:** This is an identify that allows you to move the rule by before or after an ID.

**Rule:** Enable or Disable this entry.

**Action When Matched:** Select to **Drop** or **Forward** the packet specified in this filter entry.

**Direction:** Incoming Packet Filter rules prevent unauthorized computers or applications accessing your local network from the Internet. Outgoing Packet Filter rules prevent unauthorized computers or applications accessing the Internet. Select if the new filter rule is incoming or outgoing.

**Source IP:** Select **Any**, **Subnet**, **IP Range** or **Single Address**.

- **Starting IP Address:** Enter the source IP or starting source IP address this filter rule is to be applied.



- **End IP Address:** Enter the End source IP Address this filter rule is to be applied. (for IP Range only)
- **Netmask:** Enter the subnet mask of the above IP address.

**Destination IP:** Select **Any**, **Subnet**, **IP Range** or **Single Address**.

- **Starting IP Address:** Enter the destination IP or starting destination IP address this filter rule is to be applied.

- **End IP Address:** Enter the End destination IP Address this filter rule is to be applied. (for IP Range only)
- **Netmask:** Enter the subnet mask of the above IP address.

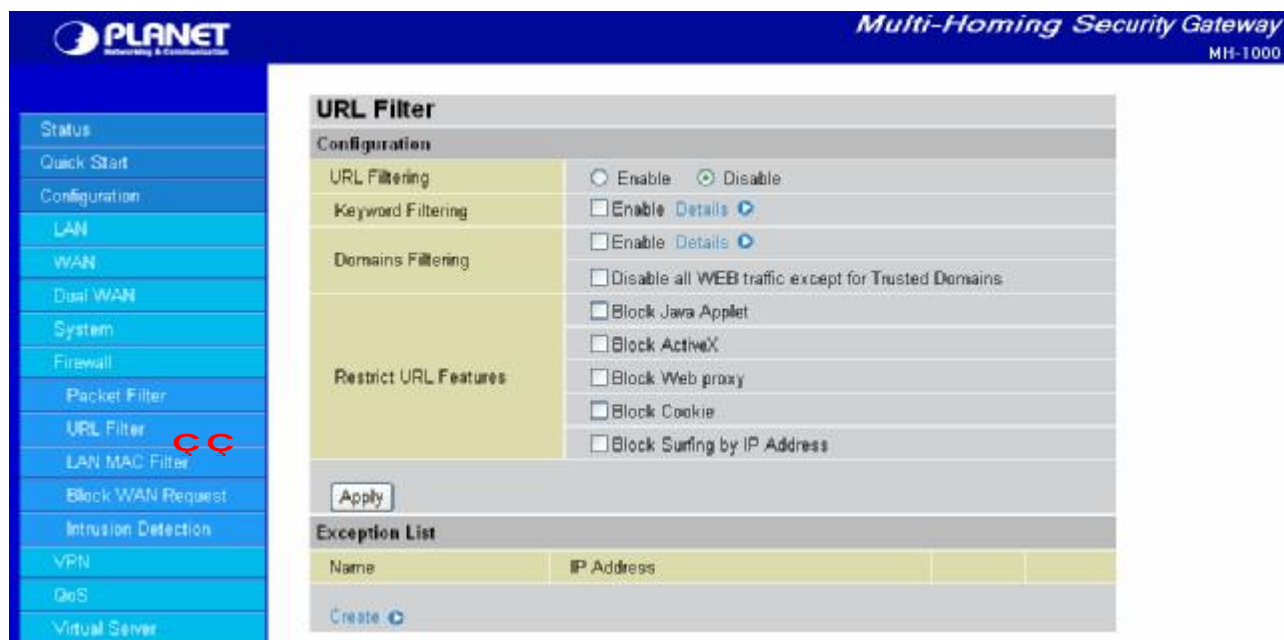
**Protocol:** Select the Transport protocol type (Any, TCP, UDP).

**Source Port Range:** Enter the source port number range. If you only want to specify one service port, then enter the same port number in both boxes.

**Destination Port Range:** Enter the destination port number range. If you only want to specify one service port, then enter the same port number in both boxes.

**Helper:** You could also select the application type you would like to apply for automatic input.

#### 4.4.5.2 URL Filter



The URL Filter is a powerful tool that can be used to limit access to certain URLs on the Internet. You can block web sites based on keywords or even block out an entire domain. Certain web features can also be blocked to grant added security to your network.

**URL Filtering:** You can choose to Enable or Disable this feature.

**Keyword Filtering:** Click the checkbox to enable this feature. To edit the list of filtered keywords, click Details.

**Domain Filtering:** Click the "enable" checkbox to enable filtering by Domain Name. Click the "Disable all WEB traffic except for trusted domains" check box to allow web access only for trusted domains.

**Restrict URL Features:** Click **Block Java Applet** to filter web access with Java Applet components. Click

**Block ActiveX** to filter web access with ActiveX components. Click **Block Web proxy** to filter web proxy access. Click **Block Cookie** to filter web access with Cookie components. Click **Block Surfing by IP Address** to filter web access with an IP address as the domain name.

**Exception List:** You can input a list of IP addresses as the exception list for URL filtering.

**Keyword Filtering:** Click the top checkbox to enable this feature. You can also choose to disable all web traffic except for trusted sites by clicking the bottom checkbox. To edit the list of filtered domains, click **Details**.

The screenshot shows the 'Keywords Filtering' configuration page. On the left is a navigation menu with options: Status, Quick Start, Configuration, LAN, WAN, Dual WAN, System, Firewall, Packet Filter, URL Filter, and LAN MAC Filter. The main content area has a title bar 'Multi-Homing Security Gateway MH-1000'. Below the title is the 'Keywords Filtering' section. It includes a 'Create' form with a 'Keyword' input field and an 'Apply' button. Below the form is a section titled 'Block WEB URLs which contain these keywords' with a table:

No.	Keyword

Enter a keyword to be filtered and click **Apply**. Your new keyword will be added to the filtered keyword listing.

**Domains Filtering:** Click the top checkbox to enable this feature. You can also choose to disable all web traffic except for trusted sites by clicking the bottom checkbox. To edit the list of filtered domains, click **Details**.

The screenshot shows the 'Domains Filtering' configuration page. On the left is a navigation menu with options: Status, Quick Start, Configuration, LAN, WAN, Dual WAN, System, Firewall, Packet Filter, URL Filter, and LAN MAC Filter. The main content area has a title bar 'Multi-Homing Security Gateway MH-1000'. Below the title is the 'Domains Filtering' section. It includes a 'Create' form with a 'Domain Name' input field, a 'Type' dropdown menu (set to 'Forbidden Domain'), and an 'Apply' button. Below the form are two tables:

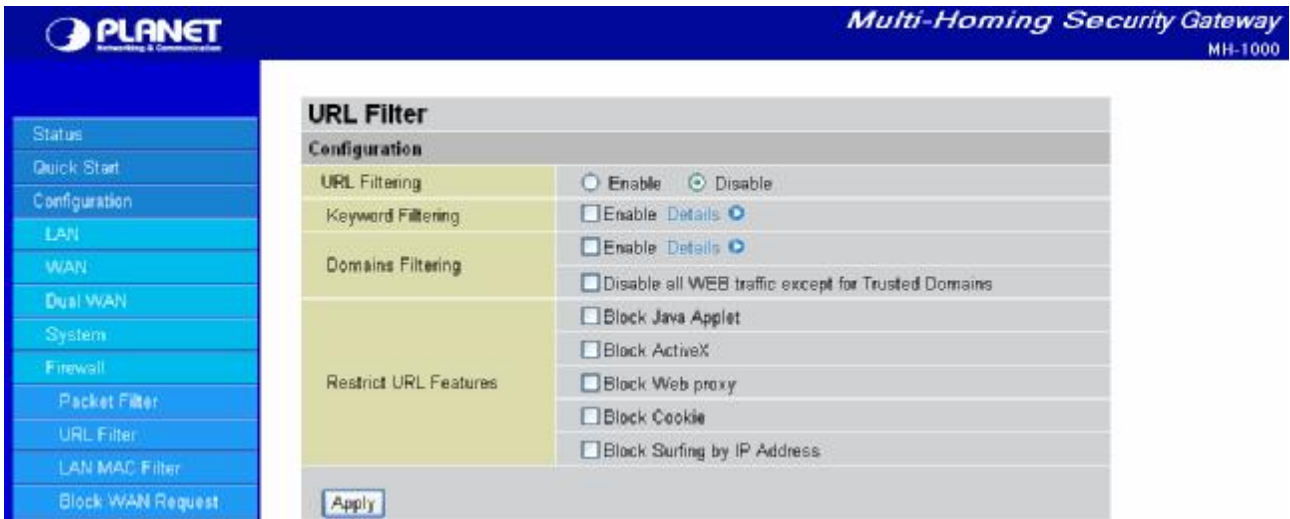
Trusted Domain Table	
No.	Domain

Forbidden Domain Table	
No.	Domain

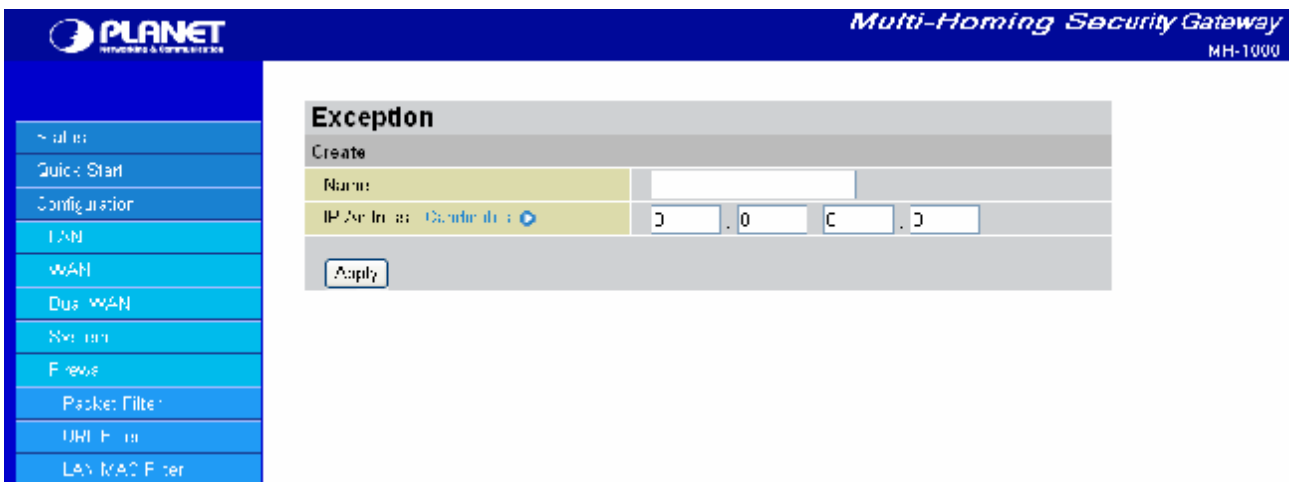
Enter a domain and select whether this domain is trusted or forbidden with the pull-down menu. Next, click **Apply**. Your new domain will be added to either the Trusted Domain or Forbidden Domain listing, depending on which you selected previously.

**Restrict URL Features:** Use this to disable certain web features. Select the options you want (Block Java

Applet, Block ActiveX, Block Web proxy, Block Cookie, Block Surfing by IP Address) and click **Apply** to save your changes.

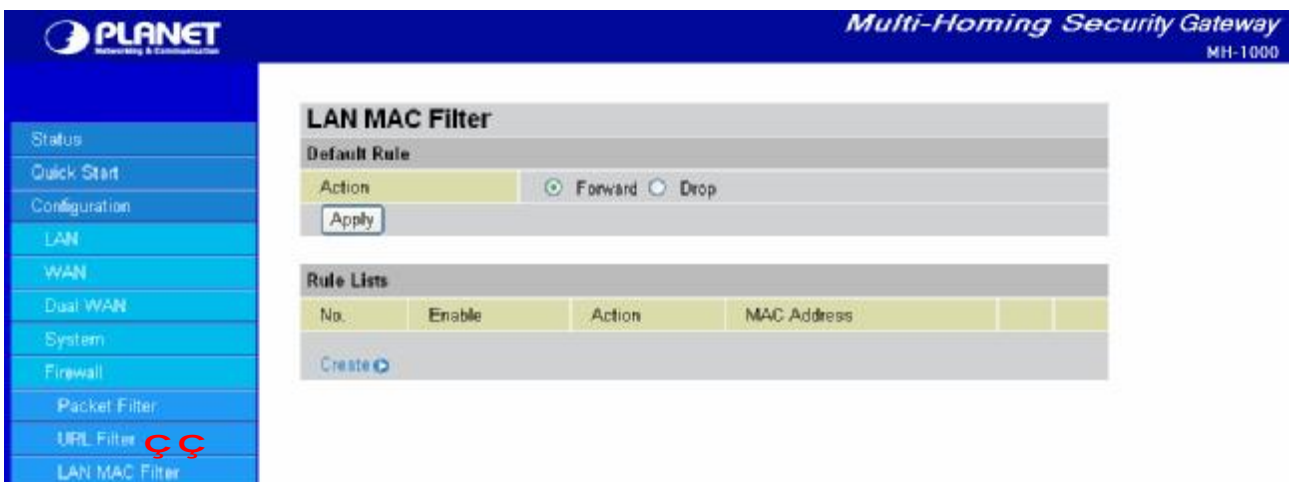


You may also designate which IP addresses are to be excluded from these filters by adding them to the Exception List. To do so, click **Add**.



Enter a name for the IP Address and then enter the IP address itself. Click **Apply** to save your changes. The IP address will be entered into the Exception List, and excluded from the URL filtering rules in effect.

#### 4.4.5.3 LAN MAC Filter



**LAN MAC Filter** can decide that MH-1000 will serve those devices at LAN side or not by MAC Address.

**Default Rule:** Forward or Drop all LAN request. (Forward by default)

**Create:** You can also input a specified MAC Address to be dropped or Forward without depending on the default rule.



**Rule:** Enable or disable this entry.

**Action When Matched:** Select to **Drop** or **Forward** the packet specified in this filter entry.

**MAC Address:** The MAC Address you would like to apply.

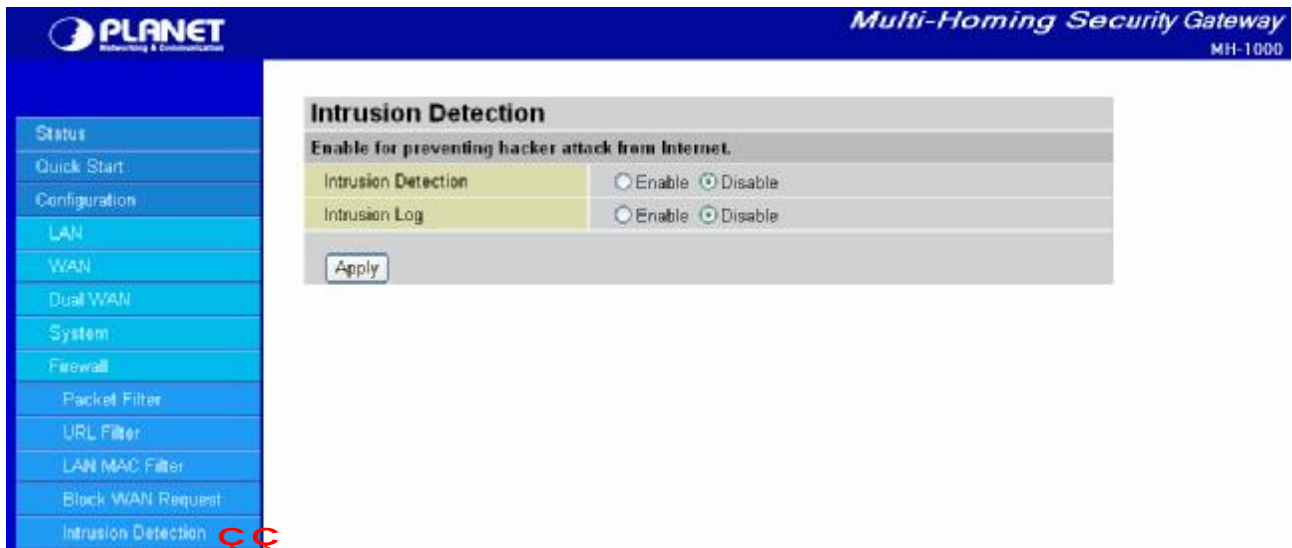
**Candidates:** You can also select the **Candidates** which are referred from the ARP table for automatic input.

#### 4.4.5.4 Block WAN Request



Blocking WAN requests is one way to prevent DDOS attacks by preventing ping requests from the Internet. Use this menu to enable or disable function.

### 4.4.5.5 Intrusion Detection



Intrusion Detection can prevent most common DoS attacks from the Internet or from LAN users.

**Intrusion Detection:** Enable or disable this function.

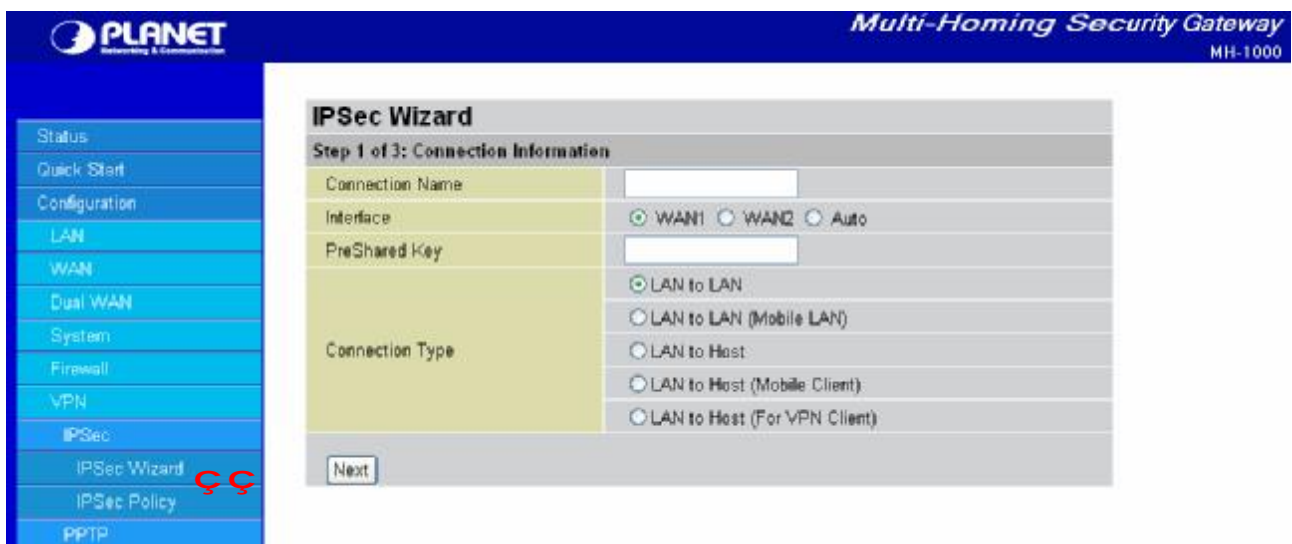
**Intrusion Log:** All the detected and dropped attacks will be shown in the system log.

## 4.4.6 VPN

### 4.4.6.1 IPSec

IPSec is a set of protocols that enable Virtual Private Networks (VPN). VPN is a way to establish secured communication tunnels to an organization's network via the Internet.

#### 4.4.6.1.1 IPSec Wizard



**Connection Name:** A user-defined name for the connection.

**Interface:** Select the interface the IPSec tunnel will apply to.

**WAN1:** Select interface WAN1

**WAN2:** Select interface WAN2

**Auto:** The device will automatically apply the tunnel to WAN1 or WAN2 depending on which WAN interface is active when the IPSec tunnel is being established. (**Note:** Auto only applies to Fail Over mode. For Load Balance mode, please do not select "Auto". In Load Balance mode, Auto will be forced to WAN1 interface if Auto is selected.)

**Pre-shared Key:** This is for the Internet Key Exchange (IKE) protocol. IKE is used to establish a shared security policy and authenticated keys for services (such as IPSec) that require a key. Before any IPSec traffic can be passed, each router must be able to verify the identity of its peer. This can be done by manually entering the pre-shared key into both sides (router or hosts).

### Connection Type:

There are 5 connection types:

**(1) LAN to LAN:** MH-1000 would like to establish an IPSec VPN tunnel with remote router using Fixed Internet IP or domain name by using main mode.

The screenshot shows the 'IPSec Wizard' configuration page for a Planet Multi-Homing Security Gateway (MH-1000). The page is titled 'Step 2 of 3: Remote Information'. It contains the following fields and controls:

- Remote Secure Gateway Address (or hostname):** A text input field.
- Remote Network:** A table with two rows:
 

IP Address	Net mask
0 . 0 . 0 . 0	0 . 0 . 0 . 0
- Buttons:** 'Back' and 'Next' buttons are located at the bottom of the form.

**Secure Gateway Address (or Domain Name):** The IP address or hostname of the remote VPN gateway.

**Remote Network:** The subnet of the remote network. Allow you to enter an IP address and netmask.

**Back:** Back to the Previous page.

**Next:** Go to the next page.

**(2) LAN to Mobile LAN:** MH-1000 would like to establish an IPSec VPN tunnel with remote router using Dynamic Internet IP by using aggressive mode.

The screenshot shows the IPsec Wizard configuration page for a Planet Multi-Homing Security Gateway (MH-1000). The page is titled "IPsec Wizard" and is at "Step 2 of 3: Remote Information". On the left is a navigation menu with options: Status, Quick Start, Configuration, LAN, WAN, Dual WAN, System, Firewall, VPN, IPsec, IPsec Wizard (selected), IPsec Policy, and NAT. The main content area has the following fields:

- Remote Identifier:** A text input field.
- Remote Network:** A section containing two sub-fields:
  - IP Address:** Four numeric input boxes for octets, with values 0, 0, 0, 0.
  - Netmask:** Four numeric input boxes for octets, with values 11, 1, 1, 1.
- Navigation:** "Back" and "Next" buttons.

**Remote Identifier:** The Identifier of the remote gateway. According to the input value, the ID type will be auto-defined as IP Address, FQDN (DNS) or FQUN (E-mail).

**Remote Network:** The subnet of the remote network. Allow you to enter an IP address and netmask.

**Back:** Back to the Previous page.

**Next:** Go to the next page.

**(3) LAN to Host:** MH-1000 would like to establish an IPsec VPN tunnel with remote client software using Fixed Internet IP or domain name by using main mode.

The screenshot shows the IPsec Wizard configuration page for a Planet Multi-Homing Security Gateway (MH-1000). The page is titled "IPsec Wizard" and is at "Step 2 of 3: Remote Information". On the left is a navigation menu with options: Status, Quick Start, Configuration, LAN, WAN, Dual WAN, System, Firewall, VPN, IPsec, IPsec Wizard (selected), IPsec Policy, and NAT. The main content area has the following fields:

- Remote Secure Gateway Address (or Hostname):** A text input field.
- Navigation:** "Back" and "Next" buttons.

**Secure Gateway Address (or Domain Name):** The IP address or hostname of the remote VPN device that is connected and establishes a VPN tunnel.

**Back:** Back to the Previous page.

**Next:** Go to the next page.

(4)LAN to Mobile Host: MH-1000 would like to establish an IPSec VPN tunnel with remote client software using Dynamic Internet IP by using aggressive mode.

The screenshot shows the Planet Multi-Homing Security Gateway (MH-1000) IPsec Wizard interface. The sidebar on the left contains the following menu items: Status, Quick Start, Configuration, LAN, WAN, Dual WAN, System, Firewall, VPN, IPsec, IPsec Wizard (highlighted), IPsec Policy, and PPTP. The main content area is titled 'IPsec Wizard' and 'Step 1 of 3: Remote Information'. It features a 'Remote Identifier' input field and 'Back' and 'Next' buttons.

**Remote Identifier:** The Identifier of the remote gateway. According to the input value, the ID type will be auto-defined as IP Address, FQDN (DNS) or FQUN (E-mail).

**Back:** Back to the Previous page.

**Next:** Go to the next page.

(5)LAN to Host (for VPN Client only): MH-1000 would like to establish an IPSec VPN tunnel with MH-1000 VPN Client by using aggressive mode.

The screenshot shows the Planet Multi-Homing Security Gateway (MH-1000) IPsec Wizard interface. The sidebar on the left contains the following menu items: Status, Quick Start, Configuration, LAN, WAN, Dual WAN, System, Firewall, VPN, IPsec, IPsec Wizard (highlighted), IPsec Policy, and PPTP. The main content area is titled 'IPsec Wizard' and 'Step 2 of 3: Remote Information'. It features a 'VPN Client IP Address' input field with the value '192.168.100.1', a warning message, and 'Back' and 'Next' buttons.

**VPN Client IP Address:** The VPN Client Address for MH-1000 VPN Client, this value will be applied on both **remote ID** and **Remote Network** as single address.

**Back:** Back to the Previous page.

**Next:** Go to the next page.



The screenshot shows the 'IPsec Wizard' configuration summary. The interface includes a left-hand navigation menu with options like Status, Quick Start, Configuration, LAN, WAN, Dual WAN, System, Firewall, VPN, IPsec, and PPTP. The main area displays the 'Configuration Summary' for a connection named 'M'.

Connection Name		M	
Tunnel		Encapsulate	
Interface		WAN1	
Local	ID	WAN = Address	Type: IP Address
	Network	192.168.1.0/24 (Subnet)	Type: Subnet
Remote	Secure Gateway	210.66.155.0	Type: IP Address/ Hostname
	ID	Remote Secure Gateway = Address	Type: IP Address
	Network	192.168.1.0/24 (Subnet)	Type: Subnet
	Secure Association	Main Mode	
Proposal	Method	ESP	
	Encryption Method	3DES	
	Authentication Protocol	MD5	
	Perfect Forward Secure	Enabled	
	Key Group	Group 1	
	PreShared Key	1345678	
	Life Time	3600 seconds	
	Rekey Interval	28800 seconds	

Buttons for 'Back' and 'Done' are located at the bottom of the configuration summary.

After your configuration is done, you will see a **Configuration Summary**.

**Back:** Back to the Previous page.

**Done:** Click **Done** to apply the rule.

#### 4.4.6.1.2 IPsec Policy

The screenshot shows the 'IPsec Policy' configuration screen. The left-hand navigation menu is similar to the previous screen, but 'IPsec Policy' is highlighted. The main area displays the 'IPsec Policy' configuration, which includes a table for 'IPsec Tunnels'.

Name	Enable	Local Network	Remote Network	Remote Gateway	IPsec Proposal
Create					

Click **Create** to create a new IPsec VPN connection account.

## Configuring a New VPN Connection

The screenshot shows the configuration page for creating a new IPsec connection. The left sidebar contains the following menu items: Status, Quick Start, Configuration, LAN, WAN, Dual WAN, System, Firewall, VPN, IPsec, IPsec Wizard, IPsec Policy, PPTP, CoS, Virtual Server, Advanced, and Save Config to Flash. The main configuration area is titled 'IPSec Create' and includes the following sections:

- Connection Name:** A text input field.
- Tunnel:** Radio buttons for  Enabled and  Disabled.
- Interface:** Radio buttons for  WAN1,  WAN2, and  Auto.
- Local:**
  - ID:** A dropdown menu with 'IP Address' selected.
  - Network:** A dropdown menu with 'Any Local Address' selected.
  - IP Address:** Four input fields for octets (0, 0, 0, 0).
  - End IP Address:** Four input fields for octets (0, 0, 0, 0).
  - Netmask:** Four input fields for octets (0, 0, 0, 0).
- Remote:**
  - Secure Gateway:** A dropdown menu with 'IP Address/Hostname' selected.
  - ID:** A dropdown menu with 'IP Address' selected.
  - Network:** A dropdown menu with 'Subnet' selected.
  - IP Address:** Four input fields for octets (0, 0, 0, 0).
  - End IP Address:** Four input fields for octets (0, 0, 0, 0).
  - Netmask:** Four input fields for octets (0, 0, 0, 0).
- Proposal:**
  - Secure Association:** Radio buttons for  Main Mode,  Aggressive Mode, and  Manual Key.
  - Method:** Radio buttons for  ESP and  AH.
  - Encryption Protocol:** A dropdown menu with '3DES' selected.
  - Authentication Protocol:** A dropdown menu with 'MD5' selected.
  - Perfect Forward Secure:** Radio buttons for  Enabled and  Disabled.
  - PreShared Key:** A text input field.
  - IKE Life Time:** A text input field with '28800' and a 'Seconds' label.
  - Key Life Time:** A text input field with '3600' and a 'Seconds' label.
  - Netbios Broadcast:** Radio buttons for  Enabled and  Disabled.
  - DPD Setting:**
    - DPD Function:** Radio buttons for  Enabled and  Disabled.
    - Detection Interval:** A text input field with '30' and a 'seconds' label.
    - Idle Timeout:** A text input field with '4' and a 'consecutive times' label.

An 'Apply' button is located at the bottom of the configuration area.

**Connection Name:** A user-defined name for the connection.

**Tunnel:** Select **Enable** to activate this tunnel. Select **Disable** to deactivate this tunnel.

**Interface:** Select the interface the IPsec tunnel will apply to.

**WAN1:** Select interface WAN1

**WAN2:** Select interface WAN2

**Auto:** The device will automatically apply the tunnel to WAN1 or WAN2 depending on which WAN interface is active when the IPsec tunnel is being established. (**Note:** Auto only applies to Fail Over mode. For Load Balance mode, please do not select "Auto". In Load Balance mode, Auto will be forced to WAN1 interface if Auto is selected.)

**Local:** This section configures the local host.

**ID:** This is the identity type of the local router or host. Choose from the following four options:

- **WAN IP Address:** Automatically use the current WAN Address as ID.
- **IP Address:** Use an IP address format.

- **FQDN DNS (Fully Qualified Domain Name):** Consists of a hostname and domain name. For example, WWW.VPN.COM is a FQDN. WWW is the host name, VPN.COM is the domain name. When you enter the FQDN of the local host, the router will automatically seek the IP address of the FQDN.

- **FQUN E-Mail (Fully Qualified User Name):** Consists of a username and its domain name. For example, user@vpn.com is a FQUN. "user" is the username and "vpn.com" is the domain name.

- **Data:** Enter the ID data using the specific ID type.

**Network:** Set the IP address, IP range, subnet, or address range of the local network.

- **Any Local Address:** Will enable any local address on the network.

- **Subnet:** The subnet of the local network. Selecting this option enables you to enter an IP address and netmask.

- **IP Range:** The IP Range of the local network.

- **Single Address:** The IP address of the local host.

**Remote:** This section configures the remote host.

**Secure Gateway Address (or Domain Name):** The IP address or hostname of the remote VPN device that is connected and establishes a VPN tunnel.

**ID:** The identity type of the local host. Choose from the following three options:

- **Remote IP Address:** Automatically use the remote gateway Address as ID.

- **IP Address:** Use an IP address format.

- **FQDN DNS (Fully Qualified Domain Name):** Consists of a hostname and domain name. For example, WWW.VPN.COM is a FQDN. WWW is the host name, VPN.COM is the domain name. When you enter the FQDN of the local host, the router will automatically seek the IP address of the FQDN.

- **FQUN E-Mail (Fully Qualified User Name):** Consists of a username and its domain name. For example, user@vpn.com is a FQUN. "user" is the username and "vpn.com" is the domain name.

- **Data:** Enter the ID data using the specific ID type.

**Network:** Set the subnet, IP Range, single address, or gateway address of the remote network.

- **Any Local Address:** Will enable any local address on the network.

- **Subnet:** The subnet of the remote network. Selecting this option allows you to enter an IP address and netmask.

- **IP Range:** The IP Range of the remote network.

- **Single Address:** The IP address of the remote host.

- **Gateway Address:** The gateway address of the remote host.

#### **Proposal:**

**Secure Association (SA):** SA is a method of establishing a security policy between two points. There are three methods of creating SA, each varying in degrees of security and speed of negotiation:

- **Main Mode:** Uses the automated Internet Key Exchange (IKE) setup; most secure method with the highest level of security.

- **Aggressive Mode:** Uses the automated Internet Key Exchange (IKE) setup; mid-level security. Speed is faster than Main mode.

- **Manual Key:** Standard level of security. It is the fastest of the three methods.

**Method:** There are two methods of checking the authentication information, AH (Authentication Header) and ESP (Encapsulating Security Payload). Use ESP for greater security so that data will be encrypted and authenticated. AH data will be authenticated but not encrypted.

**Encryption Protocol:** Select the encryption method from the pull-down menu. There are several options: DES, 3DES, and AES (128, 192 and 256). 3DES and AES are more powerful but increase latency.

- **DES:** Stands for Data Encryption Standard. It uses a 56-bit encryption method.
- **3DES:** Stands for Triple Data Encryption Standard. It uses a 168-bit encryption method.
- **AES:** Stands for Advanced Encryption Standard. You can use 128, 192 or 256 bits as encryption method.

**Authentication Protocol:** Authentication establishes data integrity and ensures it is not tampered with while in transit. There are two options: Message Digest 5 (MD5), and Secure Hash Algorithm (SHA1). While slower, SHA1 is more resistant to brute-force attacks than MD5.

- **MD5:** A one-way hashing algorithm that produces a 128-bit hash.
- **SHA1:** A one-way hashing algorithm that produces a 160-bit hash.

**Perfect Forward Secure:** Choose whether to enable PFS using Diffie-Hellman public-key cryptography to change encryption keys during the second phase of VPN negotiation. This function will provide better security, but extends the VPN negotiation time. Diffie-Hellman is a public-key cryptography protocol that allows two parties to establish a shared secret over the Internet.

**Pre-shared Key:** This is for the Internet Key Exchange (IKE) protocol. IKE is used to establish a shared security policy and authenticated keys for services (such as IPSec) that require a key. Before any IPSec traffic can be passed, each router must be able to verify the identity of its peer. This can be done by manually entering the pre-shared key into both sides (router or hosts).

**IKE Life Time:** Allows you to specify the timer interval for renegotiation of the IKE security association. The value is in seconds, eg. 28800 seconds = 8 hours.

**Key Life Time:** Allows you to specify the timer interval for renegotiation of another key. The value is in seconds eg. 3600 seconds = 1 hour.

**Netbios Broadcast:** Allows MH-1000 to send local Netbios Broadcast packet through the IPSec Tunnel, please select **Enable** or **Disable**.

#### **DPD Setting:**

**DPD function:** Select **Enable**, MH-1000 will send out informational packet to see if remote VPN device responds the packets, the function is used to detect the tunnel is alive or not. Check **Disable** to stop the feature.

**Detection Interval:** The interval time to check the remote IPSec device. By default is 30 seconds.

**Idle Timeout:** If the remote VPN device does not respond, MH-1000 will retry to send out the packets. When the frequency reaches to the **Idle Timeout** setting, MH-1000 will disconnect the VPN connection automatically. The range of **Idle Timeout** can be set within 1 to 10.

Click the **Apply** button to save your changes.

After you have created the IPSec connection, the account information will be displayed.

Name	Enable	Local Network	Remote Network	Remote Gateway	IPsec Proposal
MH1	<input checked="" type="checkbox"/>	192.168.1.0/24	192.168.100.0/24	210.65.100.90	MAIN Mode ESP (DES MD5)

**Name:** This is the user-defined name of the connection.

**Enable:** This function activates or deactivates the IPSec connection.

**Local Subnet:** Displays IP address and subnet of the local network.

**Remote Subnet:** Displays IP address and subnet of the remote network.

**Remote Gateway:** This is the IP address or Domain Name of the remote VPN device that is connected and has an established IPSec tunnel.

**IPSec Proposal:** This is the selected IPSec security method.

#### 4.4.6.2 PPTP

PPTP is a set of protocols that enable Virtual Private Networks (VPN). VPN is a way to establish secured communication tunnels to an organization's network via the Internet.

**PPTP function:** Select **Enable** to activate PPTP Server. **Disable** to deactivate PPTP Server function.

**Auth. Type:** The authentication type, **Pap or Chap, PaP, Chap.**

**Data Encryption:** Select **Enable** or **Disable** the Data Encryption.

**Encryption Key Length:** **Auto, 40 bits** or **128 bits.**

**Peer Encryption Mode:** **Only Stateless** or **Allow Stateless and Stateful.**

**IP Addresses Assigned to Peer Start from:** 192.168.1.x: please input the IP assigned range from **1 ~ 254** (except MH-1000's LAN IP address with **192.168.1.1** as MH-1000's default LAN IP address and IP pool range of DHCP server settings with **100~199** as MH-1000's default DHCP IP pool range.)

**Idle Timeout “ ” Min:** Specify the time for remote peer to be disconnected without any activities, from **0~120.**

Click **Create** to create a new PPTP VPN connection account.

**Connection Name:** A user-defined name for the connection.

**Tunnel:** Select **Enable** to activate this tunnel. Select **Disable** to deactivate this tunnel.

**Username:** Please input the username for this account.

**Password:** Please input the password for this account.

**Retype Password:** Please repeat the same password as previous field.

**Connection Type:** Select **Remote Access** for single user, Select **LAN to LAN** for remote gateway.

**Peer Network IP:** Please input the IP for remote network.

**Peer Netmask:** Please input the Netmask for remote network.

**Netbios Broadcast:** Allows MH-1000 to send local Netbios Broadcast packets through the PPTP Tunnel, please select **Enable** or **Disable**.

#### 4.4.7 QoS

MH-1000 can optimize your bandwidth by assigning priority to both inbound and outbound data with QoS. This menu allows you to configure QoS for both inbound and outbound traffic.



The first menu screen gives you an overview of which WAN ports currently have QoS active, and the bandwidth settings for each.

#### WAN1 Outbound:

- **QoS Function:** QoS status for WAN1 outbound. Select **Enable** to activate QoS for WAN1's outgoing traffic. Select **Disable** to deactivate.
- **Max ISP Bandwidth:** The maximum bandwidth afforded by the ISP for WAN1's outbound traffic.

#### WAN1 Inbound:

- **QoS Function:** QoS status for WAN1 inbound. Select **Enable** to activate QoS for WAN1's incoming traffic. Select **Disable** to deactivate.
- **Max ISP Bandwidth:** The maximum bandwidth afforded by the ISP for WAN1's inbound traffic.

#### WAN2 Outbound:

- **QoS Function:** QoS Status for WAN2 outbound. Select **Enable** to activate QoS for WAN2's outgoing traffic. Select **Disable** to deactivate.
- **Max ISP Bandwidth:** The maximum bandwidth afforded by the ISP for WAN2's outbound traffic.

#### WAN2 Inbound:

- **QoS Function:** QoS Status for WAN2 inbound. Select **Enable** to activate QoS for WAN2's incoming traffic. Select **Disable** to deactivate.
- **Max ISP Bandwidth:** The maximum bandwidth afforded by the ISP for WAN2's inbound traffic.

### Creating a New QoS Rule

To get started using QoS, you will need to establish QoS rules. These rules tell MH-1000 how to handle both incoming and outgoing traffic. The following example shows you how to configure WAN1 Outbound

QoS. Configuring the other traffic types follows the same process.

To make a new rule, click Rule Table. This will bring you to the Rule Table which displays the rules currently in effect.

Next, click **Create** to open the QoS Rule Configuration window.

**Interface:** The current traffic type. This can be WAN1 (outbound, inbound) and WAN2 (outbound, inbound).

**Application:** User defined application name for the current rule.

**Guaranteed:** The guaranteed amount of bandwidth for this rule as a percentage.

**Maximum:** The maximum amount of bandwidth for this rule as a percentage.

**Priority:** The priority assigned to this service. Select a value from 0 to 6, 0 being highest.

**DSCP Marking:** Used to classify traffic. Select from **Best Effort**, **Premium**, **Gold Service (High Medium, Low)**, **Silver (H,M,L)**, and **Bronze (H,M,L)**.

**Address Type:** The type of address this rule applies to. Select **IP Address** or **MAC Address**.



**For IP Address:**

- **Source IP Address Range:** The range of source IP Addresses this rule applies to.
- **Destination IP Address Range:** The range of destination IP Addresses this rule applies to.
- **Protocol:** The type of packet this rule applies to. Choose from **Any**, **TCP**, **UDP**, or **ICMP**.
- **Source Port Range:** The range of source ports this rule applies to.
- **Destination Port Range:** The range of destination ports this rule applies to.
- **Helper:** You could also select the application type you would like to apply for automatic input.

Click **Apply** to save your changes.

**For MAC Address:**

- **Source MAC Address:** The source MAC Address of the device this rule applies to.
- **Candidates:** You can also select the Candidates which are referred from the ARP table for automatic input.
- **Protocol:** The type of packet this rule applies to. Choose from **Any**, **TCP**, **UDP**, or **ICMP**.
- **Source Port Range:** The range of source ports this rule applies to.
- **Destination Port Range:** The range of destination ports this rule applies to.
- **Helper:** You could also select the application type you would like to apply for automatic input.

#### 4.4.8 Virtual Server

In TCP/IP and UDP networks, a port is a 16-bit number used to identify which application program (usually a server) incoming connections should be delivered to. Some ports have numbers that are pre-assigned to them by the Internet Assigned Numbers Authority (IANA), and these are referred to as "well-known ports". Servers follow the well-known port assignments so clients can locate them.

If you wish to run a server on your network that can be accessed from the WAN (i.e. from other machines

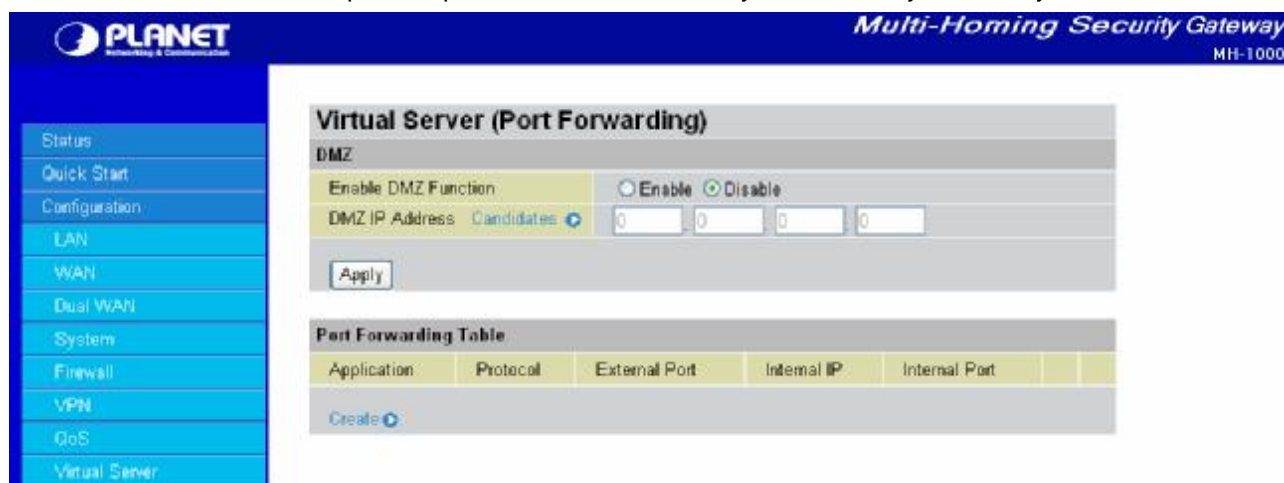
on the Internet that are outside your local network), or any application that can accept incoming connections (e.g. peer-to-peer applications) and are using NAT (Network Address Translation), then you will usually need to configure your router to forward these incoming connection attempts using specific ports to the PC on your network running the application. You will also need to use port forwarding if you want to host an online game server. The reason for this is that when using NAT, your publicly accessible IP address will be used by and point to your router, which then needs to deliver all traffic to the private IP addresses used by your PCs. Please see the **WAN Configuration** section of this manual for more information on NAT.

MH-1000 can also be configured as a virtual server so that remote users accessing services such as Web or FTP services via the public (WAN) IP address can be automatically redirected to local servers in the LAN network. Depending on the requested service (TCP/UDP port number), the device redirects the external service request to the appropriate server within the LAN network.

#### 4.4.8.1 DMZ

The DMZ Host is a local computer exposed to the Internet. When setting a particular internal IP address as the DMZ Host, all incoming packets will be checked by the Firewall and NAT algorithms then passed to the DMZ host, when a packet received does not use a port number used by any other Virtual Server entries.

**Caution:** Such Local computer exposure to the Internet may face a variety of security risks.



#### Enable DMZ function:

- **Enable:** Activates your router's DMZ function.
- **Disable:** Default setting. Disables the DMZ function.

**DMZ IP Address:** Give a static IP address to the DMZ Host when the **Enable** radio button is selected. Be aware this IP will be exposed to the WAN/Internet.

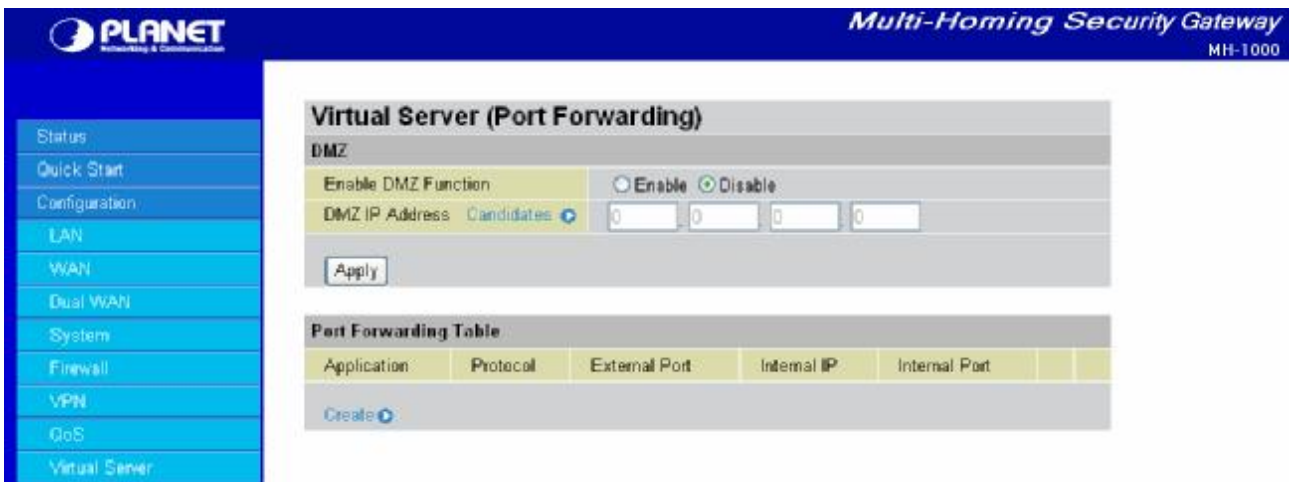
**Candidates:** You can also select the Candidates which are referred from the ARP table for automatic input.

Select the **Apply** button to apply your changes.

#### 4.4.8.2 Port Forwarding Table

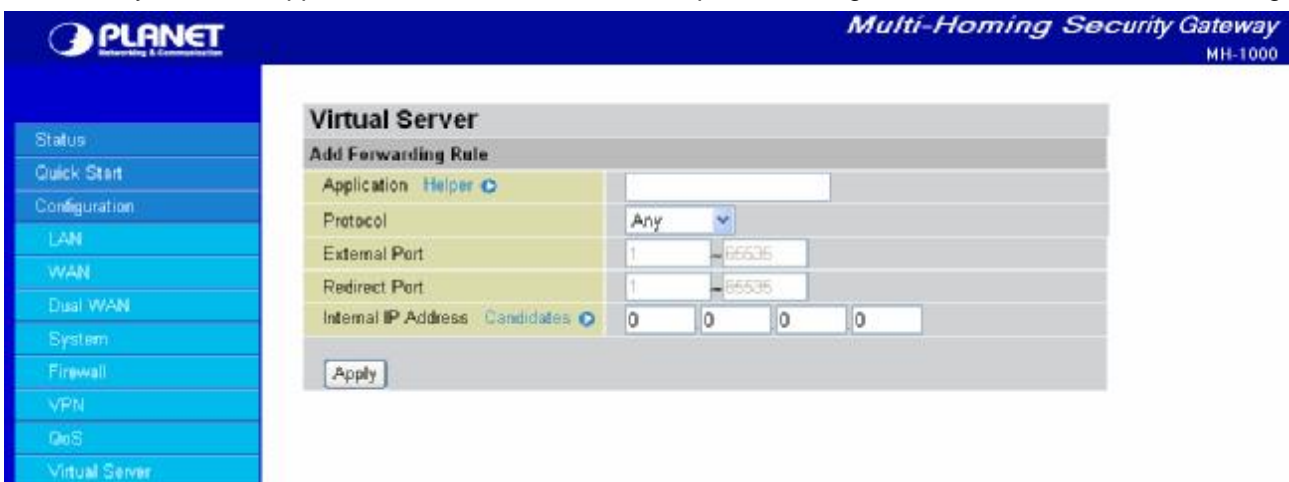
Because NAT can act as a "natural" Internet firewall, your router protects your network from being accessed by outside users, as all incoming connection attempts will point to your router unless you specifically create Virtual Server entries to forward those ports to a PC on your network.

When your router needs to allow outside users to access internal servers, e.g. a web server, FTP server, Email server or game server, the router can act as a "virtual server". You can set up a local server with a specific port number for the service to use, e.g. web/HTTP (port 80), FTP (port 21), Telnet (port 23), SMTP (port 25), or POP3 (port 110). When an incoming access request is received, it will be forwarded to the corresponding internal server.



Click **Create** to add a new port forwarding rule.

This function allows any incoming data addressed to a range of service port numbers (from the Internet/WAN Port) to be re-directed to a particular LAN private/internal IP address. This option gives you the ability to handle applications that use more than one port such as games and audio/video conferencing.



**Application:** User defined application name for the current rule.

**Helper:** You could also select the application type you would like to apply for automatic input.

**Protocol:** please select protocol type

**External Port:** Enter the port number of the service that will be sent to the Internal IP address.

**Redirect Port:** Enter a new port number for the service that will be sent to the Internal IP address.

**Internal IP Address:** Enter the LAN server/host IP address that the service request from the Internet will be sent to.

**Candidates:** You can also select the Candidates which are referred from the ARP table for automatic input.

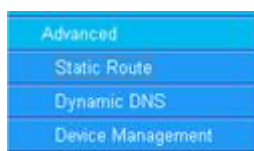
**NOTE:** You need to give your LAN server/host a static IP address for the Virtual Server to work properly.

Click **Apply** to save your changes.

Using port forwarding does have security implications, as outside users will be able to connect to PCs on your network. For this reason, using specific Virtual Server entries just for the ports your application requires, instead of using DMZ is recommended.

#### 4.4.9 Advanced

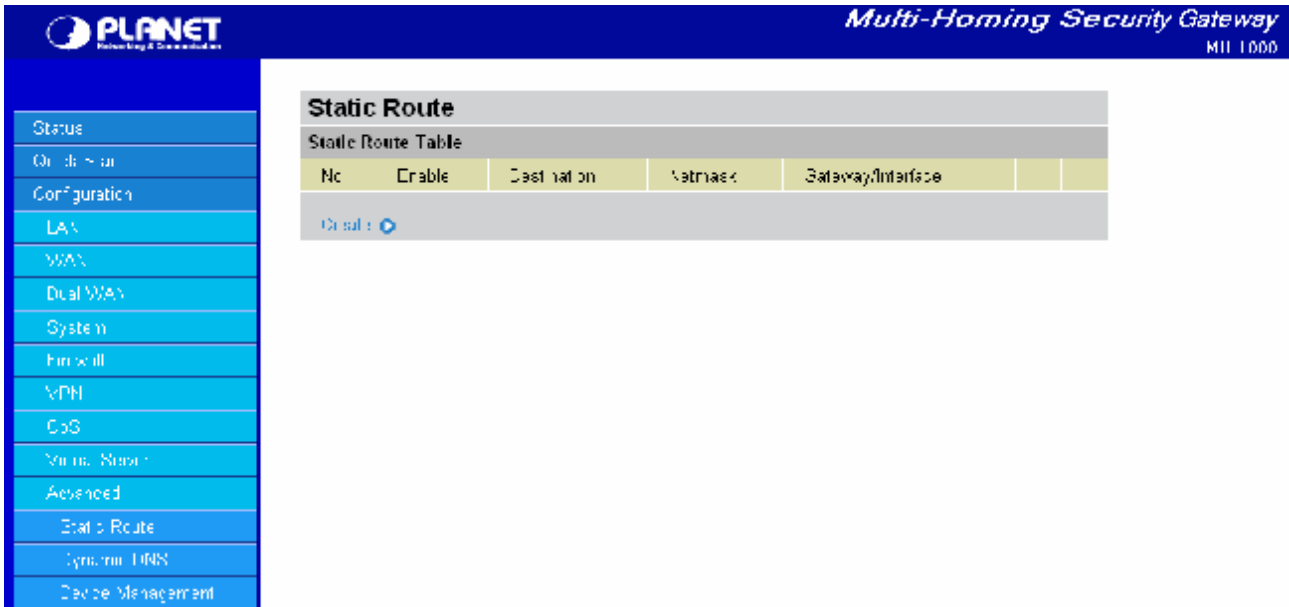
Configuration options within the Advanced section are for users who wish to take advantage of the more advanced features of MH-1000. Users who do not understand the features should not attempt to reconfigure their router, unless advised to do so by support staff.



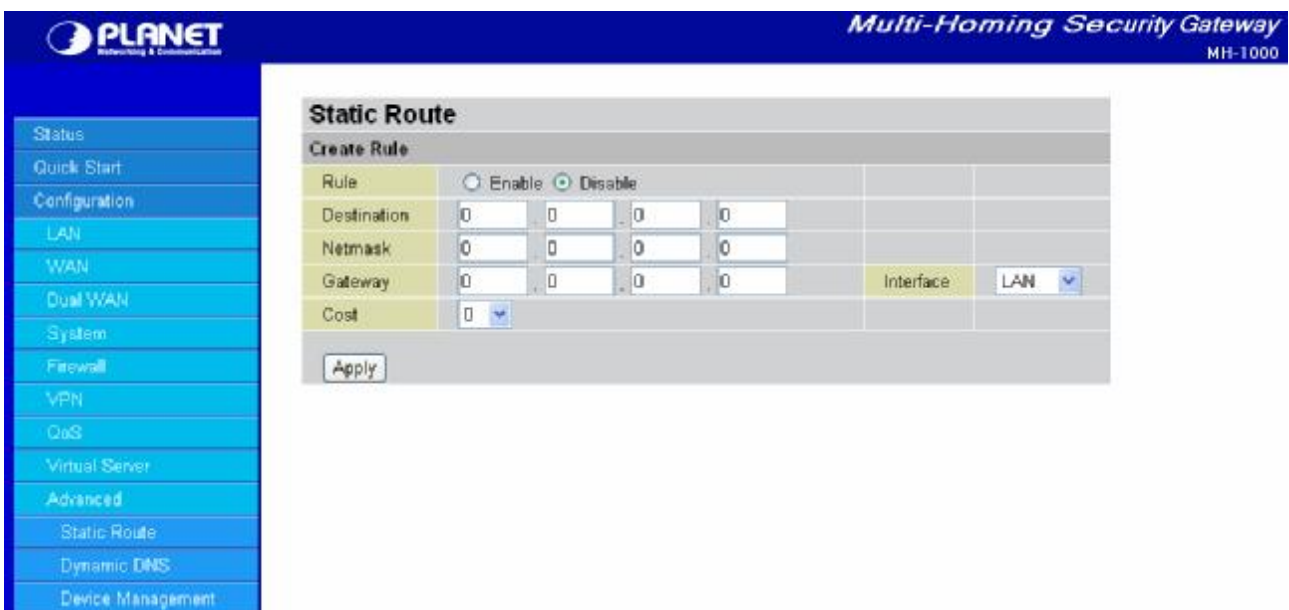
There are three items within the Advanced section: **Static Route**, **Dynamic DNS** and **Device Management**.

##### 4.4.9.1 Static Route

The static route settings enable the router to route IP packets to another network (subnet). The routing table stores the routing information so the router knows where to redirect the IP packets.



Click on **Static Route** and then click **Create** to add a routing table.



**Rule:** Select **Enable** to activate this rule, **Disable** to deactivate this rule.

**Destination:** This is the destination subnet IP address.

**Netmask:** This is the subnet mask of the destination IP addresses based on above destination subnet IP.

**Gateway:** This is the gateway IP address to which packets are to be forwarded.

**Interface:** Select the interface through which packets are to be forwarded.

**Cost:** This is the same meaning as Hop.

Click **Apply** to save your changes.

### 4.4.9.2 Dynamic DNS

The Dynamic DNS function allows you to alias a dynamic IP address to a static hostname, allowing users whose ISP does not assign them a static IP address to use a domain name. This is especially useful when hosting servers via your WAN connection, so that anyone wishing to connect to you may use your domain name, rather than having to use a dynamic IP address that changes periodically. This dynamic IP address is the WAN1/WAN2 IP address of the router, which is assigned to you by your ISP. Click **Edit** in the Dynamic DNS Settings Table to set related parameters for a specific interface.

You will first need to register and establish an account with the Dynamic DNS provider using their website,

Example: DYNDNS

<http://www.dyndns.org/>

(MH-1000 supports several Dynamic DNS providers , such as [www.dyndns.org](http://www.dyndns.org) , [www.orgdns.org](http://www.orgdns.org) , [www.dhs.org](http://www.dhs.org), [www.dyns.cx](http://www.dyns.cx), [www.3domain.hk](http://www.3domain.hk), [www.zoneedit.com](http://www.zoneedit.com), [www.3322.org](http://www.3322.org), [www.no-ip.com](http://www.no-ip.com) )**[D4]**

#### Dynamic DNS:

- **Disable:** Check to disable the Dynamic DNS function.
- **Enable:** Check to enable the Dynamic DNS function. The following fields will be activated and required:

**Dynamic DNS Server:** Select the DDNS service you have established an account with.

**Wildcard:** Select this check box to enable the DYNDNS Wildcard.

**Domain Name:** Enter your registered domain name for this service.

**Username:** Enter your registered user name for this service.

**Password:** Enter your registered password for this service.

Click **Apply** to save your changes.

### 4.4.9.3 Device Management

The Device Management Advanced Configuration settings allow you to control your router's security options and device monitoring features.

The screenshot shows the Planet Multi-Homing Security Gateway web interface. The top header includes the Planet logo and the text 'Multi-Homing Security Gateway M11 1000'. A sidebar menu on the left lists various configuration options, with 'Device Management' selected. The main content area is titled 'Device Management' and contains the following settings:

Device Management		
Device Name		
Name	MI1-1000	
Web Server Settings		
HTTP Port	80	(80 is default HTTP port)
Management IP Address	0 . 0 . 0 . 0	(0.0.0.0 means Any)
Expire to auto-logout	300	seconds
*: This setting will become effective after you save to flash and restart the router.		
Apply		

#### Device Name

**Name:** Enter a name for this device.

#### Web Server Settings

**HTTP Port:** This is the port number the router's embedded web server (for web-based configuration) will use. The default value is the standard HTTP port, 80. Users may specify an alternative if, for example, they are running a web server on a PC within their LAN.

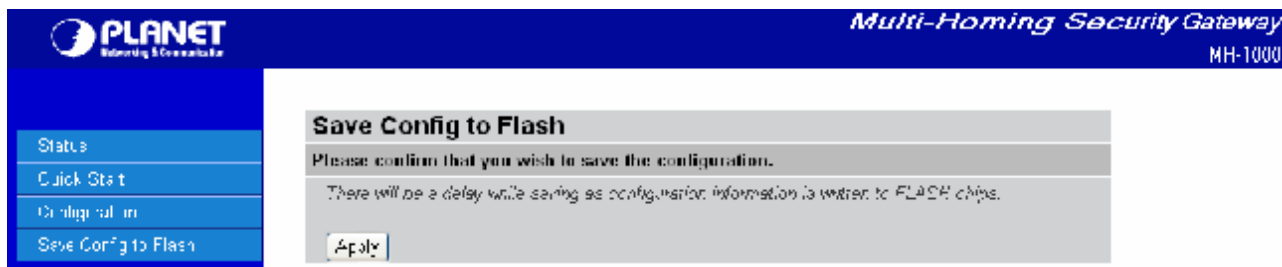
**Management IP Address:** You may specify an IP address allowed to logon and access the router's web server. Setting the IP address to 0.0.0.0 will disable IP address restrictions, allowing users to login from any IP address.

**Expire to auto-logout:** Specify a time frame for the system to auto-logout the user's configuration session.

**Example:** User A changes HTTP port number to 100, specifies their own IP address of 192.168.1.100 and sets the logout time to be 100 seconds. The router will only allow User A access from the IP address 192.168.1.100 to logon to the Web GUI by typing: <http://192.168.1.1:100> in their web browser. After 100 seconds, the device will automatically logout User A.

### 4.5 Save Configuration To Flash

After changing the router's configuration settings, you must save all of the configuration parameters to flash memory to avoid them being lost after turning off or resetting your router. Click **Apply** to write your new configuration to flash memory.



## 4.6 Logout

To exit the router's web interface, click **Logout**. Please ensure that you have saved your configuration settings before you logout.



Be aware that the router is restricted to only one PC accessing the web configuration interface at a time. Once a PC has logged into the web interface, other PCs cannot gain access until the current PC has logged out. If the previous PC forgets to logout, the second PC can access the page after a user-defined period (5 minutes by default). You can modify this value using the **Advanced > Device Management** section of the Web Configuration Interface. Please see the **Advanced** section of this manual for more information.



## Chapter 5: Troubleshooting

### 5.1 Basic Functionality

This section deals with issues regarding your MH-1000's basic functions.

#### 5.1.1 Router Won't Turn On

If the Power and other LEDs fail to light when your MH-1000 is turned on:

- Make sure that the power cord is properly connected to your firewall and that the power supply adapter is properly connected to a functioning power outlet.
- Check that you are using the 12VDC power adapter supplied by Planet for this product.

If the error persists, you may have a hardware problem, and should contact technical support.

#### 5.1.2 LEDs Never Turn Off

When your MH-1000 is turned on, the LEDs turn on for about 10 seconds and then turn off. If all the LEDs stay on, there may be a hardware problem.

If all LEDs are still on one minute after powering up:

- Cycle the power to see if the router recovers.
- Clear the configuration to factory defaults.

If the error persists, you may have a hardware problem, and should contact technical support.

#### 5.1.3 LAN or Internet Port Not On

If either the LAN LEDs or Internet LED does not light when the Ethernet connection is made, check the following:

- Make sure each Ethernet cable connection is secure at the firewall and at the hub or workstation.
- Make sure that power is turned on to the connected hub or workstation.
- Be sure you are using the correct cable. When connecting the firewall's Internet port to a cable or DSL modem, use the cable that was supplied with the cable or DSL modem. This cable could be a standard straight-through Ethernet cable or an Ethernet crossover cable.

#### 5.1.4 Forgot My Password

Try entering the default User Name and Password:

User Name: admin

Password: admin

Please note that both the User Name and Password are case-sensitive.

If this fails, you can restore your MH-1000 to its factory default settings by holding the Reset button on the back of your router until the Status LED begins to blink. Then enter the default User Name and Password to access your router.

## 5.2 LAN Interface

Refer to this section for issues relating to MH-1000's LAN Interface.

### 5.2.1 Can't Access MH-1000 from the LAN

If there is no response from MH-1000 from the LAN:

- Check your Ethernet cable types and each connection.
- Make sure the computer's Ethernet adapter is installed and functioning properly.

If the error persists, you may have a hardware problem, and should contact technical support.

### 5.2.2 Can't Ping Any PC on the LAN

If PCs connected to the LAN cannot be pinged:

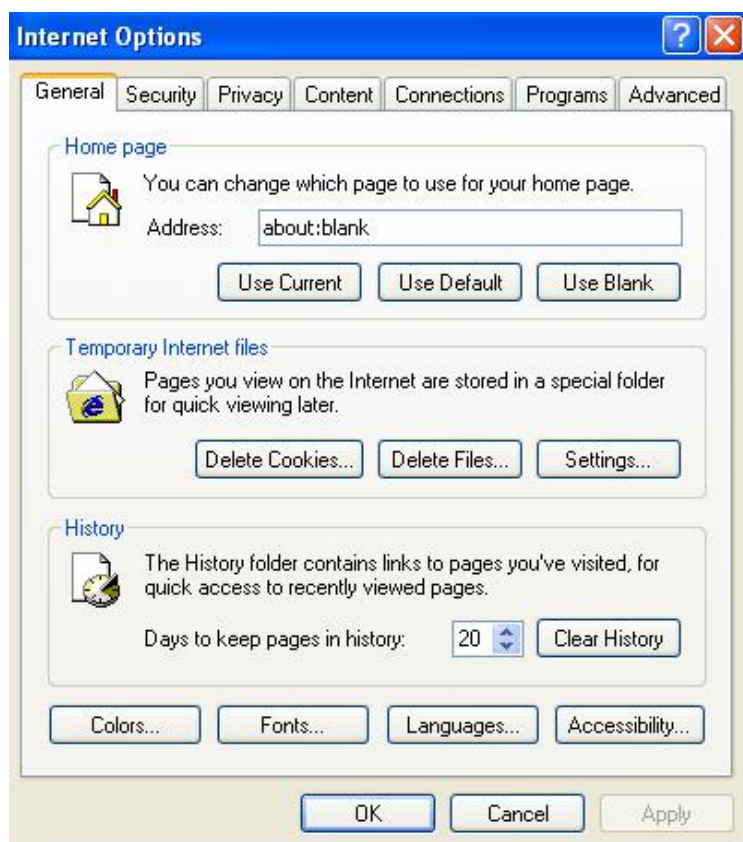
- Check the 10/100 LAN LEDs on MH-1000's front panel. One of these LEDs should be on. If they are both off, check the cables between MH-1000 and the hub or PC.
- Check the corresponding LAN LEDs on your PC's Ethernet device are on.
- Make sure that driver software for your PC's Ethernet adapter and TCP/IP software is correctly installed and configured on your PC.
- Verify the IP address and the subnet mask of MH-1000 and the computers are on the same subnet.

### 5.2.3 Can't Access Web Configuration Interface

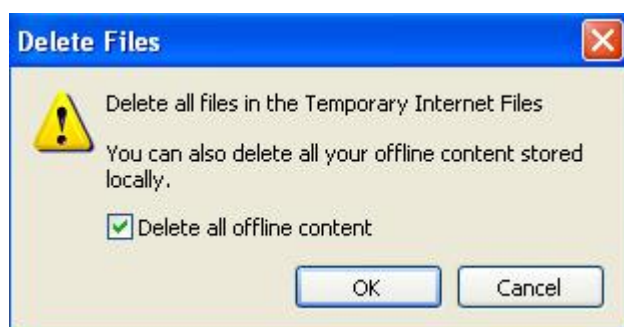
If you are having trouble accessing MH-1000's Web Configuration Interface from a PC connected to the network:

- Check the connection between the PC and the router.
- Make sure your PC's IP address is on the same subnet as the router.
- If your MH-1000's IP address has changed and you don't know the current IP address, reset the router to factory defaults by holding the Reset button on the back of your router for 6 seconds. This will reset the router's IP address to 192.168.1.
- Check to see if your browser had Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click **Refresh** to ensure that the Java applet is loaded.
- Try closing the browser and re-launching it.
- Make sure you are using the correct User Name and Password. User Names and Passwords are case-sensitive, so make sure that **CAPS LOCK** is not on when entering this information.

- Try clearing your browser's cache.
  1. With Internet Explorer, click **Tools > Internet Options**.
  2. Under the **General** tab, click **Delete Files**.



3. Make sure that the **Delete All Offline Content** checkbox is checked, and click **OK**.



4. Click **OK** under **Internet Options** to close the dialogue.
- In Windows, type **arp -d** at the command prompt to clear you computer's ARP table.

### 5.2.3.1 Pop-up Windows

To use the Web Configuration Interface, you need to disable pop-up blocking. You can either disable pop-up blocking, which is enabled by default in Windows XP Service Pack 2, or create an exception for your MH-1000's IP address.

### Disabling All Pop-ups

In Internet Explorer, select **Tools > Pop-up Blocker** and select **Turn Off Pop-up Blocker**.

[D6]

You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab of the **Internet Options** dialogue.

1. In Internet Explorer, select **Tools > Internet Options**.
2. Under the **Privacy** tab, clear the **Block pop-ups** checkbox and click **Apply** to save your changes.

### Enabling Pop-up Blockers with Exceptions

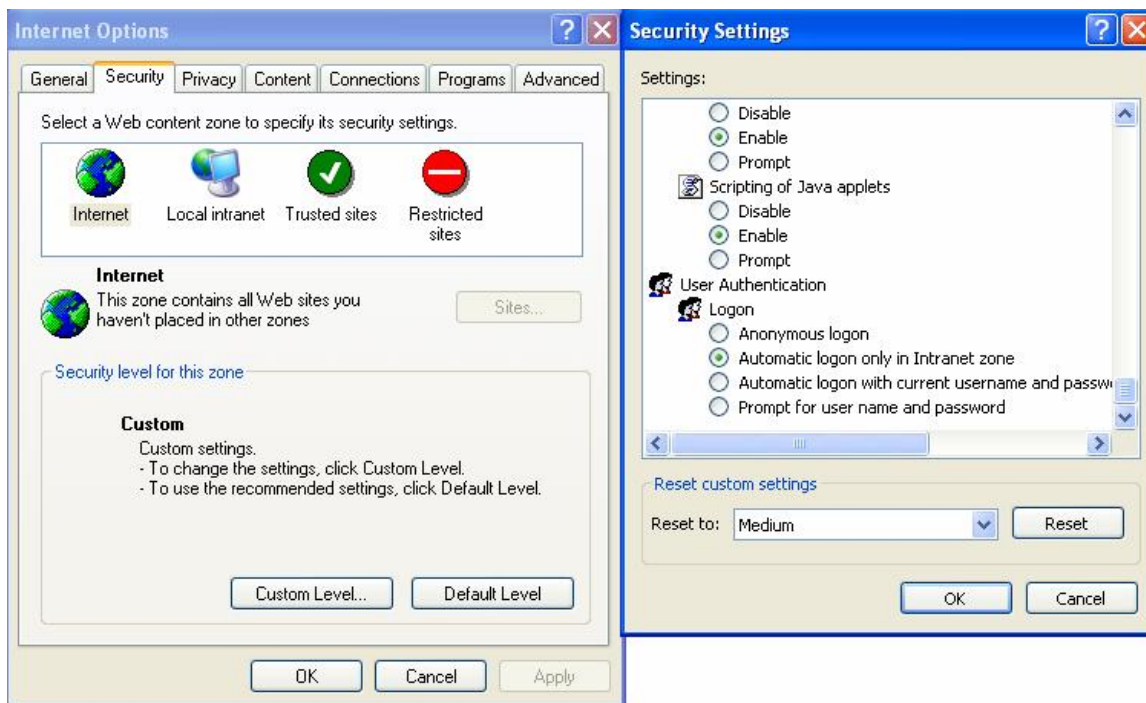
If you only want to allow pop-up windows with your MH-1000:

1. In Internet Explorer, select **Tools > Internet Options**.
2. Under the **Privacy** tab, click **Settings** to open the **Pop-up Blocker Settings** dialogue. [D7]
3. Enter the IP address of your router.
4. Click **Add** to add the IP address to the list of **Allowed sites**.
5. Click **Close** to return to the **Privacy** tab of the **Internet Options** dialogue.
6. Click **Apply** to save your changes.

### 5.2.3.2 Java Scripts

If the Web Configuration Interface is not displaying properly in your browser, check to make sure that Java Scripts are allowed.

1. In Internet Explorer, click **Tools > Internet Options**.
2. Under the **Security** tab, click **Custom Level**.

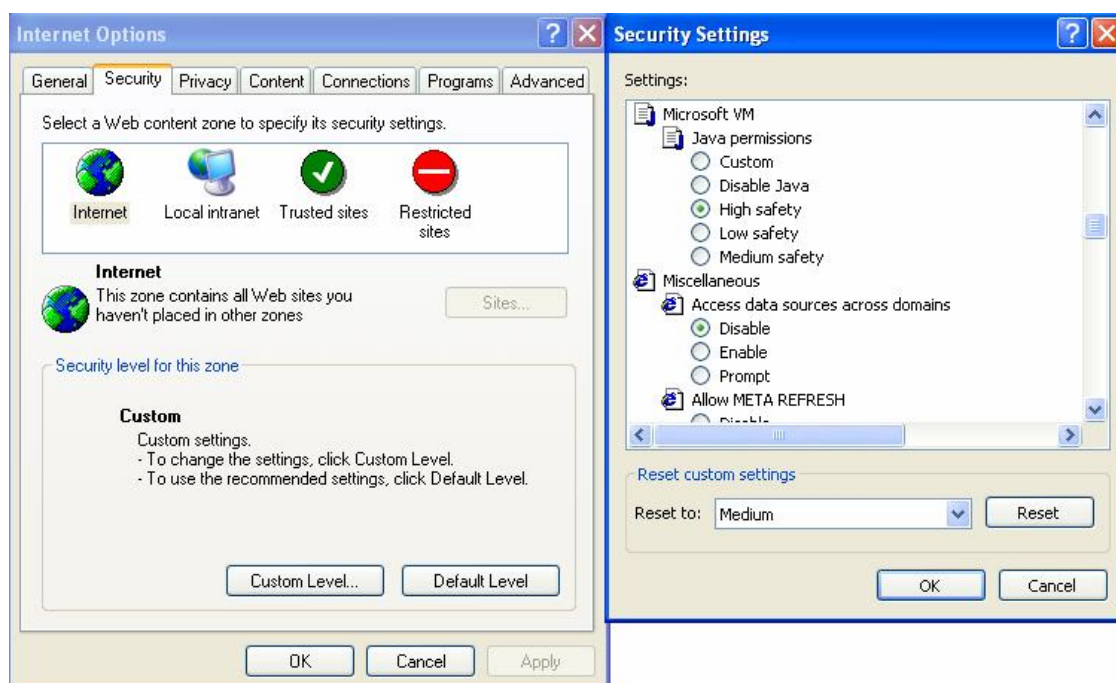


3. Under **Scripting**, check to see if **Active scripting** is set to **Enable**.
4. Ensure that **Scripting of Java applets** is set to **Enabled**.
5. Click **OK** to close the dialogue.

### 5.2.3.3 Java Permissions

The following Java Permissions should also be given for the Web Configuration Interface to display properly:

1. In Internet Explorer, click **Tools > Internet Options**.
2. Under the **Security** tab, click **Custom Level**.



3. Under **Microsoft VM\***, make sure that a safety level for **Java permissions** is selected.
4. Click **OK** to close the dialogue.

**NOTE:** If Java from Sun Microsystems is installed, scroll down to **Java (Sun)** and ensure that the checkbox is filled.

## 5.3 WAN Interface

If you are having problems with the WAN Interface, refer to the tips below.

### 5.3.1 Can't Get WAN IP Address from the ISP

If the WAN IP address cannot be obtained from the ISP:

- If you are using PPPoE or **[S8]** PPTP encapsulation, you will need a user name and password. Ensure that you have entered the correct **Service Type**, **User Name**, and **Password**. Note that user names and passwords are case-sensitive.
- If your ISP requires MAC address authentication, clone the MAC address from your PC on the LAN as MH-1000's WAN MAC address.
- If your ISP requires host name authentication, configure your PC's name as MH-1000's system name.

## 5.4 ISP Connection

Unless you have been assigned a static IP address by your ISP, your MH-1000 will need to request an IP address from the ISP in order to access the Internet. If your MH-1000 is unable to access the Internet, first determine if your router is able to obtain a WAN IP address from the ISP.

To check the WAN IP address:

1. Open your browser and choose an external site (i.e. [www.planet.com.tw](http://www.planet.com.tw)).
2. Access the Web Configuration Interface by entering your router's IP address (default is 192.168.1.1).
3. The WAN IP Status is displayed on the first page.

The screenshot displays the status page of a PLANET Multi-Homing Security Gateway (MH-1000). The page is divided into several sections:

- Status:** Includes a 'Refresh' button.
- Device Information:**
  - Device Name: MH-1000
  - System Up Time: 0: 6:53:53 (day:hour:min:sec)
  - Current Time: Mon Aug 1 11:53:41 2005 (with a 'Sync Now' button)
  - Private LAN MAC Address: 00:04:ed:46:02:5b
  - Public WAN1 MAC Address: 00:04:ed:46:02:5c
  - Public WAN2 MAC Address: 00:04:ed:46:02:5d
  - Firmware Version: 1.04c
  - Home URL: PLANET Technology Corporation
- LAN:**
  - IP Address: 192.168.1.1
  - Netmask: 255.255.255.0
  - DHCP Server: Enabled
- WAN1:**
  - Connection Method: Connect by Static IP Settings
  - IP Address: 192.168.99.94
  - Netmask: 255.255.255.0
  - Gateway: 192.168.99.253
  - DNS: 168.95.1.1
  - Up Time: 0: 5:35:19 (day:hour:min:sec)
- WAN2:**
  - Connection Method: No Link
  - IP Address: (empty)
  - Netmask: (empty)
  - Gateway: (empty)
  - DNS: (empty)
  - Up Time: (empty)

4. Check to see that the WAN port is properly connected to the ISP. If a **Connected by (x)** where **(x)** is your connection method is not shown, your router has not successfully obtained an IP address from your ISP.

If an IP address cannot be obtained:

1. Turn off the power to your cable or DSL modem.
2. Turn off the power to your MH-1000.
3. Wait five minutes and power on your cable or DSL modem.
4. When the modem has finished synchronizing with the ISP (generally shown by LEDs on the modem), turn on the power to your router.

If an IP address still cannot be obtained:

- Your ISP may require a login program. Consult your ISP whether they require PPPoE or some other type of login.
- If your ISP requires a login, check to see that your User Name and Password are entered correctly.
- Your ISP may check for your PC's host name. Assign the PC Host Name of your ISP account as your PC's host name on the router.
- Your ISP may check for your PC's MAC address. Either inform your ISP that you have purchased a new

network device or ask them to use your router's MAC address, or configure your router to spoof your PC's MAC address.

If an IP address can be obtained, but your PC cannot load any web pages from the Internet:

- Your PC may not recognize DNS server addresses. Configure your PC manually with DNS addresses.
- Your PC may not have the router correctly configured as its TCP/IP gateway.

## 5.5 Problems with Date and Time

If the date and time is not being displayed correctly, be sure to set it for your MH-1000 via the Web Configuration Interface. Both date and time can be found under **Configuration > System > Time Zone**.

## 5.6 Restoring Factory Defaults

You can restore your MH-1000 to its factory settings by holding the Reset button on the back of your router until the Status LED begins to blink. This will reset your router to its default settings.



## Appendix A: Virtual Private Networking

### A.1 What is the VPN?

A Virtual Private Network (VPN) is a shared network where private data is segmented from other traffic so that only the intended recipient has access. It allows organizations to securely transmit data over a public medium like the Internet. VPNs utilize tunnels, which allow data to be safely delivered to the intended recipient.

Because private networks lack data security, IPSec-based VPNs employ encryption technologies that protect a private network from data theft or tampering. These private networks can be implemented over any type of IP network, which allows for excellent flexibility.

#### A.1.1 VPN Applications

VPNs are traditionally used three ways:

- Extranets: Extranets are secure connections between two or more organizations. IPSec-based VPNs are ideal for extranet connections, as they can be quickly and inexpensively installed. Extranets are often used to securely share a company's information with suppliers, vendors, customers, or other businesses.
- Intranets: Intranets are private networks that connect an organization's locations together. These locations range from a headquarters, to branch offices, to a remote employee's home. Intranets are often used for email and for sharing applications and files. A firewall protects Intranets from unauthorized access.
- Remote Access: Remote access enables mobile workers to access email and business applications. Remote access VPNs greatly reduce expenses by enabling mobile workers to dial a local Internet connection and then set up a secure IPSec-based VPN communications to their organization.

### A.2 What is the IPSec?

Internet Protocol Security (IPSec) is a set of protocols and algorithms that provide data authentication, integrity, and confidentiality as data is transferred across IP networks. IPSec provides data security at the IP packet level, and protects against possible security risks by protecting data. IPSec is widely used to establish VPNs.

There are three major functions of IPSec:

- Confidentiality: Conceals data through encryption.
- Integrity: Ensures that contents did not change in transit.
- Authentication: Verifies that packets received are actually from the claimed sender.

## A.2.1 IPSec Security Components

IPSec contains three major components:

- Authentication Header (AH): Provides authentication and integrity.
- Encapsulating Security Payload (ESP): Provides confidentiality, authentication, and integrity.
- Internet Key Exchange (IKE): Provides key management and Security Association (SA) management.

These components are discussed below.

### A.2.1.1 Authentication Header (AH)

The Authentication Header (AH) is a protocol that provides authentication and integrity, protecting data from tampering. It provides authentication of either all or part of the contents of a datagram through the addition of a header that is calculated based on the values in the datagram.

The AH can also protect packets from unauthorized re-transmission with anti-replay functionality. The presence of the AH header allows us to verify the integrity of the message, but doesn't encrypt it. Thus, AH provides authentication but not privacy. ESP protects data confidentiality. Both AH and ESP can be used together for added protection.

A typical AH packet looks like this:

Next Header	Payload Length	Reserved
SPI		
Sequence Number		
Authentication Data		

### A.2.1.2 Encapsulating Security Payload (ESP)

Encapsulating Security Payload (ESP) provides privacy for data through encryption. An encryption algorithm combines the data with a key to encrypt it. It then repackages the data using a special format, and transmits it to the destination. The receiver then decrypts the data using the same algorithm. ESP is usually used with AH to provide added data security.

ESP divides its fields into three components...

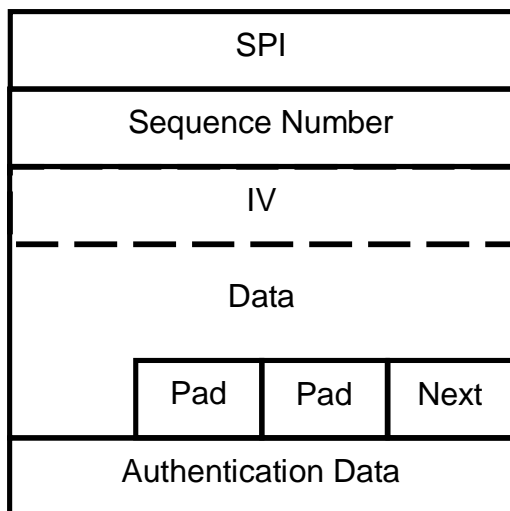
ESP Header: Placed before encrypted data, the ESP Header contains the SPI and Sequence Number. Its

placement depends on whether ESP is used in transport mode or tunnel mode.

**ESP Trailer:** Placed after the encrypted data, the ESP Trailer contains padding that is used to align the encrypted data.

**ESP Authentication Data:** This contains an Integrity Check Value (ICV) for when ESP's optional authentication feature is used.

ESP provides authentication, integrity, and confidentiality, which provides data content protection, and protects against data tampering. A typical ESP packet looks like this:



### A.2.1.3 Security Associations (SA)

Security Associations are a one-way relationships between sender and receiver that specify IPSec-related parameters. They provide data protection by using the defined IPSec protocols, and allow organizations to control according to the security policy in effect, which resources may communicate securely.

SA is identified by 3 parameters:

- Security Parameters Index (SPI), a locally unique value
- Destination IP Address
- Security Protocol: (AH or ESP, but not both)

There are several other parameters associated with an SA that are stored in a Security Association database.

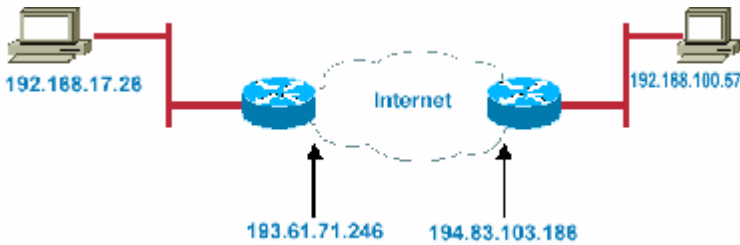
### A.2.2 IPSec Modes

To exchange data between different types of VPNs, IPSec provides two major modes:

- Tunnel Mode

This mode is used for host-to-host security. Protection extends to the payload of IP data, and the IP

addresses of the hosts must be public IP addresses.



Transport Mode

- This mode is used to provide data security between two networks. It provides protection for the entire IP packet and is sent by adding an outer IP header corresponding to the two tunnel end-points. Since tunnel mode hides the original IP header, it provides security of the networks with private IP address space.



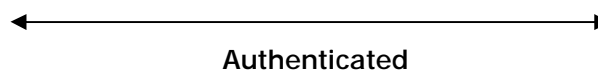
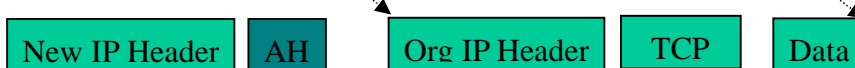
**A.2.3 Tunnel Mode AH**

AH is typically applied to a data packet in the following manner:

Original Packet

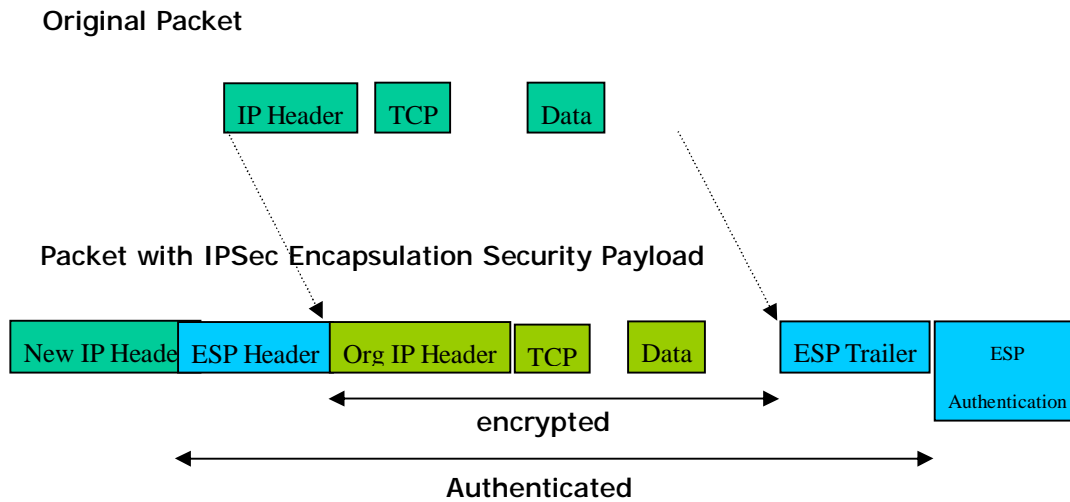


Packet with IPSec Authentication Header



**A.2.4 Tunnel Mode ESP**

Here is an example of a packet with ESP applied:



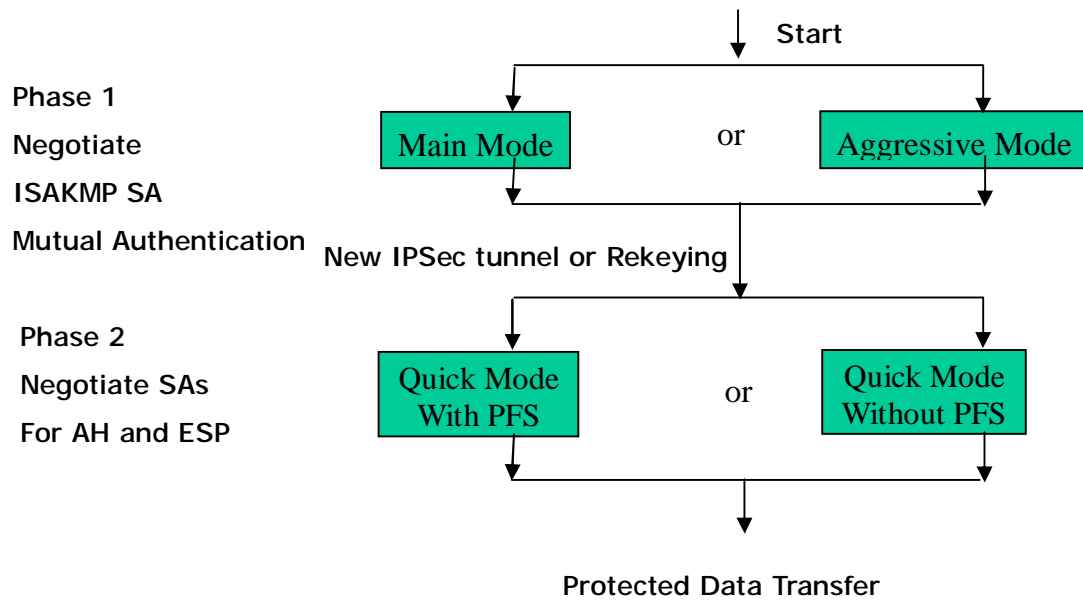
### A.2.5 Internet Key Exchange (IKE)

Before either AH or ESP can be used, it is necessary for the two communication devices to exchange a secret key that the security protocols themselves will use. To do this, IPSec uses Internet Key Exchange (IKE) as a primary support protocol. IKE facilitates and automates the SA setup, and exchanges keys between parties transferring data. Using keys ensures that only the sender and receiver of a message can access it. These keys need to be re-created or refreshed frequently so that the parties can communicate securely with each other. Refreshing keys on a regular basis ensures data confidentiality.

There are two phases to this process. Phase I deals with the negotiation and management of IKE and IPSec parameters. This phase can be carried out in either one of two modes: Main Mode or Aggressive Mode. Main mode utilizes three message pairs that negotiate IKE parameters, establish a shared secret and derive session keys, and exchange and provide identities, retroactively authenticating the information sent. This method is very secure, but when using the pre-shared key method for authentication, it is possible to use IDs other than the packets's IP addresses. Aggressive mode reduces this process to three messages, but parameter negotiation is limited, identity protection is lacking except when using public key encryption, and is more vulnerable to Denial of Service attacks.

Phase II, known as Quick Mode, establishes symmetrical IPSec Security Associations for both AH and ESP. It does this by negotiating IPSec parameters, exchange nonces to derive session keys from the IKE shared secret, exchange DH values to generate a new key, and identify which traffic this SA bundle will protect using selectors (IDi and IDr payloads).

The following is an illustration on how data is handled with IKE:



## Appendix B: IPsec Logs and Events

### B.1 IPsec Log Event Categories

There are three major categories of IPsec Log Events for your MH-1000. These include:

1. IKE Negotiate Packet Messages
2. Rejected IKE Messages
3. IKE Negotiated Status Messages

The table in the following section lists the different events of each category, and provides a detailed explanation of each.

### B.2 IPsec Log Event Table

IKE Negotiate Packet Messages	
Log Event	Explanation
Send Main mode initial message of ISAKMP	Sending the first initial message of main mode (phase I). Done to exchange encryption algorithm, hash algorithm, and authentication method.
Send Aggressive mode initial message of ISAKMP	Sending the first message of aggressive mode (phase I).
Received Main mode initial message of ISAKMP	Received the first message of main mode.
Send Main mode first response message of ISAKMP	Sending the first response message of main mode. Done to exchange encryption algorithm, hash algorithm, and authentication method.
Received Main mode first response message of ISAKMP	Received the first response message of main mode. Done to exchange encryption algorithm, hash algorithm, and authentication method.
Send Main mode second message of ISAKMP	Sending the second message of main mode. Done to exchange key values.
Received Main mode second message of ISAKMP	Received the second message of main mode. Done to exchange key values.
Send Main mode second response message of ISAKMP	Sending the main mode second response message. Done to exchange key values.
Received Main mode second response message of ISAKMP	Received the main mode second response message. Done to exchange key values.
Send Main mode third message of ISAKMP	Sending the third message of main mode. Done for authentication.
Received Main mode third message of ISAKMP	Received the third message of main mode. Done for authentication.

Send Main mode third response message of ISAKMP	Sending the third response message of main mode. Done for authentication.
Received Main mode third response message of ISAKMP	Received the third response message of main mode. Done for authentication.
Received Aggressive mode initial ISAKMP Message	Received the first message of aggressive mode.
Send Aggressive mode first response message of ISAKMP	Sending the first response message of aggressive mode. Done to exchange proposal and key values.
Received Aggressive mode first response message of ISAKMP	Received the first response message of aggressive mode. Done to exchange proposal and key values.
Send Aggressive mode second message of ISAKMP	Sending the second message of aggressive mode. Done to exchange proposal and key values.
Received Aggressive mode second ISAKP Message	Received the second message of aggressive mode. Done to exchange proposal and key values.
Send Quick mode initial message	Sending the first message of quick mode (Phase II). Done to exchange proposal and key values (IPSec).
Received Quick mode initial message	Received the first message of quick mode (Phase II). Done to exchange proposal and key values (IPSec).
Send Quick mode first response message	Sending the first response message of quick mode (Phase II). Done to exchange proposal and key values (IPSec).
Received Quick mode first response message	Received the first response message of quick mode (Phase II). Done to exchange proposal and key values (IPSec).
Send Quick mode second message	Sending the second message of quick mode (Phase II).
Received Quick mode second message	Received the second message of quick mode (Phase II).
ISAKMP IKE Packet	Indicates IKE packet.
ISAKMP Information	Indicates Information packet.
ISAKMP Quick Mode	Indicates quick mode packet.
<b>Rejected IKE Messages</b>	
NO PROPOSAL CHOSEN: No acceptable Oakley Transform	
NO PROPOSAL CHOSEN: No acceptable Proposal in IPsec SA	
NO PROPOSAL CHOSEN: PFS is required in Quick Initial SA.	
NO PROPOSAL CHOSEN: PFS is not required in Quick Initial SA.	
NO PROPOSAL CHOSEN: Initial Aggressive Mode message from %s but no connection has been configured	
NO PROPOSAL CHOSEN: Initial Main Mode message received on %s:%u but no connection has been authorized	
INVALID ID: Require peer to have ID %s, but peer declares %s	



---

INVALID ID INFORMATION: Initial Aggressive Mode packet claiming to be from %s on %s but no connection has been authorized
INVALID ID: Require peer to have ID %s, but peer declares %s
INVALID ID INFORMATION: Initial Aggressive Mode packet claiming to be from %s on %s but no connection has been authorized
<b>IKE Negotiated Status Messages</b>
Received Delete SA payload and deleting IPSEC State ( <i>integer</i> )
Received Delete SA payload: Deleting ISAKMP State ( <i>integer</i> )
(Main/Aggressive) mode peer ID is (identifier string)
ISAKMP SA Established
IPsec SA Established

## Appendix C: Bandwidth Management with QoS

### C.1 Overview

In a home or office environment, users constantly have to transmit data to and from the Internet. When too many are accessing the Internet at the same time, service can slow to a crawl, causing service interruptions and general frustration. Quality of Service (QoS) is one of the ways MH-1000 can optimize the use of bandwidth, ensuring a smooth and responsive Internet connection for all users.

### C.2 What is Quality of Service?

QoS is a feature that prioritizes and guarantees bandwidth to achieve optimal service performance. QoS can maximize the use of available network bandwidth by prioritizing time-sensitive traffic to avoid latencies and delays. By ensuring that time-sensitive applications such as VoIP and streaming video get priority access to bandwidth, users in both home and office environments can enjoy smooth and responsive data transmission no matter which applications they are running.

If you've ever experienced slow Internet speeds due to other network users using bandwidth-consuming applications like P2P, you'll understand why QoS is such a breakthrough for home users and office users. PLANET makes itself unique by integrating QoS in its routers for both inbound and outbound traffic.

QoS helps users manage bandwidth and effectively prioritize data traffic. It gives you full control over the traffic of any type of data. Employed on DiffServ (Differentiated Services) architecture, data traffic is given priority by the router; ensuring latency-sensitive applications like voice and mission-critical data such as VPN move through the router at lightning speeds, even under heavy load. You can throttle the speed of different types of data passing through the router, limit the speed of unimportant or bandwidth-consuming applications, and even distribute the bandwidth for different groups of users at home or in the office. QoS keeps your Internet connection smooth and responsive.

### C.3 What is Quality of Service?

QoS employs three different methods for optimizing bandwidth:

- Prioritization: Assigns different priority levels for different applications, prioritizing traffic. High, Normal and Low priority settings.
- Outbound and Inbound IP Throttling: Controls network traffic and allows you to limit the speed of each application.
- DiffServ Technology: Manages priority queues and DSCP tagging through the Internet backbone. Manages traffic among Ethernet, wireless, and ADSL interfaces.

### C.4 Who Needs QoS?

QoS is ideal for home and office users who need to use a variety of real-time applications like VoIP, on-line games, P2P, video streaming, and FTP simultaneously. With QoS, you can optimize your bandwidth to accommodate several of these applications without experiencing latency or service interruptions.

### C.4.1 Home Users

Low latency is everything for gamers. Most home users feel frustrated when trying to play an online game over a shared ADSL connection. Unfortunately, most routers have no way of determining the importance of the packet at any given time. All the traffic is treated equally, so a packet containing an "urgent" command may be delayed. QoS gives you the ability to control the bandwidth. Using IP Throttling, bandwidth limits can be enforced on a particular application or any system within the LAN. Prioritization specifies which packets have priority and should not be delayed, and which packets have lower priority and should be moved to the end of the upload queue.

Suppose there are four students sharing a three-floor house with one single broadband connection. Robert, a college freshman, is playing the online game with his group members, while Mary, a sophomore student, is talking to her net pal via Skype. Meanwhile, Jerome is downloading a movie file by using the P2P application program. Sophia, however, is just trying to log on to the website to send her photos to her family. As a result, the net speed slows to a crawl and affects everyone sharing the Internet connection. QoS is designed for managing traffic flow and bandwidth to solve this problem. You can first classify different applications (online games, FTP, Skype, email) as shown in the table below. Then, you can manage and prioritize the flow of bandwidth at different levels (e.g. 30% for games, 20% for downloads, 10% for email, 20% for FTP, and 35% for others). QoS can be used to identify different applications and assign priority to enable a smooth and responsive broadband connection.

Application	Data Ratio (%)	Priority
On-line games	30%	High
Skype	5%	High
Email	10%	High
FTP	20%	Upload (High), Download (Normal)
Other	35%	

### C.4.2 Office Users

QoS is also ideal for small businesses using an office server as a web server. With QoS control, web pages served to your customers can be given top priority and delivered first so that it will not be impeded by email and office web browsing.

Here is a good example of how QoS can work in an office environment. A CEO is holding a videoconference with international clients in the meeting room. However, the streaming video and voice frequently lag. Sales people are talking to international agencies via VoIP phone, while sending orders via email to vendors for production. However, some staff are downloading MP3 music files, large-size photos and watching video streaming online. Consequently, the Internet connection slows down. This is why business users need QoS to manage data traffic. With QoS, the network administrator can define and classify important packets; specify a minimum guaranteed rate for each application, and ensure that

important packets have priority to ensure a good quality of broadband connection for the entire organization.

<b>Application</b>	<b>Data Ratio (%)</b>	<b>Priority</b>
Videoconferencing	30%	High
VoIP	20%	High
Email	10%	High
FTP	10%	Upload (High), Download (Normal)
Other	30%	MP3 (Low), MSN (Normal)

## Appendix D: Router Setup Examples

### D.1 Outbound Fail Over

Step 1: Go to **Configuration > WAN > ISP Settings**. Select **WAN1** and **WAN2[S9]** and click **Edit**.

**ISP Settings**

WAN Service Table	
Name	Description
WAN1	Static IP <a href="#">Edit</a>
WAN2	Static IP <a href="#">Edit</a>

Step 2: Configure WAN1 and WAN2 according to the information given by your ISP.

**WAN1**

**Static IP**

Connection Method: Static IP Settings

IP assigned by your ISP: 192 . 168 . 99 . 94

IP Subnet Mask: 255 . 255 . 255 . 0

ISP Gateway Address: 192 . 168 . 99 . 253

MAC Address:  Your ISP requires you to input Ethernet MAC  
 MAC Address: 00 . 00 . 00 . 00 . 00 . 00

Primary DNS: 188 . 95 . 1 . 1

Secondary DNS: 0 . 0 . 0 . 0

RIP: Disable |  RIP-2B |  RIP-2M

MTU: 1500

[Apply](#) [Reset](#)

**WAN2**

**Static IP**

Connection Method: Static IP Settings

IP assigned by your ISP: 210 . 66 . 155 . 90

IP Subnet Mask: 255 . 255 . 255 . 224

ISP Gateway Address: 210 . 66 . 155 . 94

MAC Address:  Your ISP requires you to input Ethernet MAC  
 MAC Address: 00 . 00 . 00 . 00 . 00 . 00

Primary DNS: 188 . 95 . 1 . 1

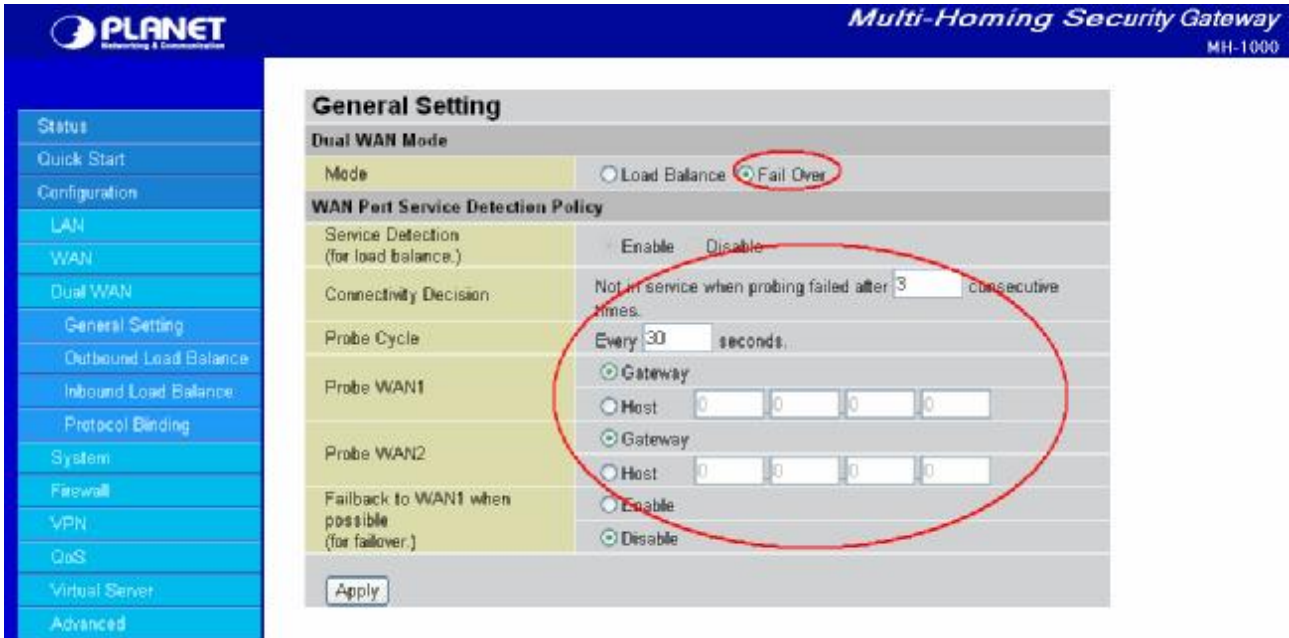
Secondary DNS: 0 . 0 . 0 . 0

RIP: Disable |  RIP-2B |  RIP-2M

MTU: 1500

[Apply](#) [Reset](#)

Step 3: Go to Configuration > Dual WAN > General Settings. Select the **Fail Over** radio button. Under Connectivity Decision, input the number of times MH-1000 should probe the WAN before deciding that the ISP is in service or not (3 by default). Next, input the duration of the probe cycle (30 sec. by default) and choose the way WAN ports are probed.

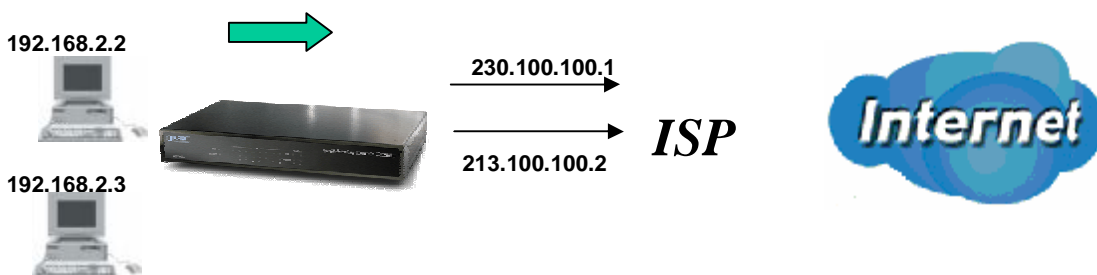


[D10]

Please ensure the WAN ports are functioning by performing a ping operation on each before proceeding. Finally, choose whether or not MH-1000 should fail back to WAN1.

Step 4: Click **Save Config** to save all changes to flash memory.

## D.2 Outbound Load Balancing



With Outbound Load Balancing, you can improve upload performance by optimizing your connection via Dual WAN. To do this, follow these steps:

Step 1: Go to **Configuration > WAN > ISP Settings**. Configure your WAN1 ISP settings and click **Apply**.

WAN1	
<b>Static IP</b>	
Connection Method	Static IP Settings
IP assigned by your ISP	192 168 99 94
IP Subnet Mask	255 255 255 0
ISP Gateway Address	192 168 99 253
MAC Address	<input type="checkbox"/> Your ISP requires you to input Ethernet MAC MAC Address 00 00 00 00 00 00
Primary DNS	188 95 1 1
Secondary DNS	0 0 0 0
RIP	Disable <input checked="" type="radio"/> RIP-2B <input type="radio"/> RIP-2M
MTU	1500
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

Step 2: Configure your WAN2 ISP settings and click **Apply**.

WAN2	
<b>Static IP</b>	
Connection Method	Static IP Settings
IP assigned by your ISP	210 66 155 90
IP Subnet Mask	255 255 255 224
ISP Gateway Address	210 66 155 94
MAC Address	<input type="checkbox"/> Your ISP requires you to input Ethernet MAC MAC Address 00 00 00 00 00 00
Primary DNS	188 95 1 1
Secondary DNS	0 0 0 0
RIP	Disable <input checked="" type="radio"/> RIP-2B <input type="radio"/> RIP-2M
MTU	1500
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

Step 3: Go to **Configuration > Dual WAN > General Settings**. Select the **Load Balance** radio button.

General Setting	
<b>Dual WAN Mode</b>	
Mode	<input checked="" type="radio"/> Load Balance <input type="radio"/> Fail Over
<b>WAN Port Service Detection Policy</b>	
Service Detection (for load balance.)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Connectivity Decision	Not in service when probing failed after 3 consecutive times.
Probe Cycle	Every 30 seconds.
Probe WAN1	<input checked="" type="radio"/> Gateway <input type="radio"/> Host 0 0 0 0
Probe WAN2	<input checked="" type="radio"/> Gateway <input type="radio"/> Host 0 0 0 0
Failback to WAN1 when possible (for failover.)	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
<input type="button" value="Apply"/>	

Step 4: Go to **Configuration > Dual WAN > Outbound Load Balance**. Choose the Load Balance mechanism you want and click **Apply**.

The screenshot shows the 'Dual Wan' configuration page for 'Outbound Load Balance'. The left sidebar contains navigation options: Status, Quick Start, Configuration, LAN, WAN, Dual WAN, General Setting, Outbound Load Balance, Inbound Load Balance, Protocol Binding, and System. The main content area has a 'Load Balance Policy' section with two radio buttons: 'Based on session mechanism' (selected) and 'Based on IP address hash mechanism'. To the right, there are several radio button options for balancing: 'Balance by Session (Round Robin)', 'Balance by Session (weight of link capacity)' (selected), 'Balance by Session weight' (with input fields), 'Balance by Traffic (weight of link capacity)', 'Balance by Traffic weight' (with input fields), 'Balance by weight of link capacity' (selected), and 'Balance by weight' (with input fields). An 'Apply' button is at the bottom left.

Step 5: Complete. To check traffic statistics, go to **Status > Traffic Statistics**.

The screenshot shows the 'Traffic Statistics' page. The left sidebar includes: Status, ACT Table, Routing Table, Session Table, D-CT Table, E-DC Status, --IP Statistics, Traffic Statistics (selected), System Log, --Routing, Quick Start, Configuration, and Show Configuration. The main content area has a 'Statistics' table:

Statistics		
WAN 1	Pk Pkts: 14311231	Tx Packets: 52950
	Tx Bytes: 4061143	Rx Packets: 0
WAN 2	Rx Bytes: 0	Tx Packets: 0
	Pk Pkts: 4111	Rx Bytes: 0

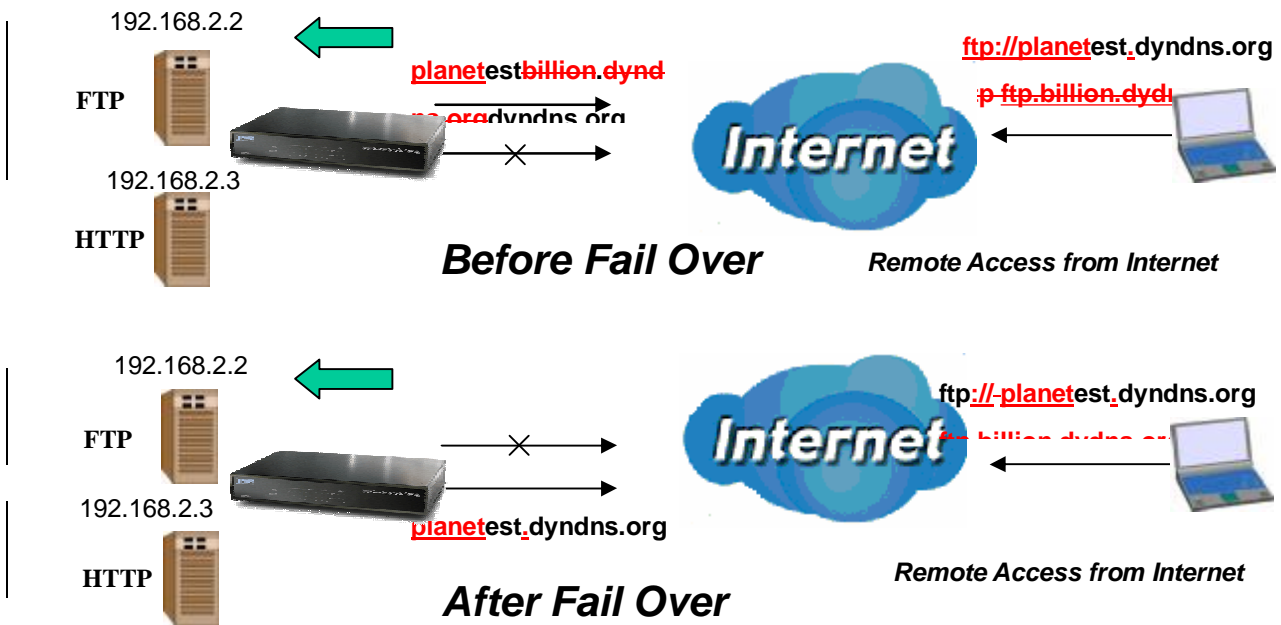
Below the table is a 'Diagram' section with a 'Display' dropdown set to 'Rx Bytes'. A line graph shows 'Rx Bytes' on the y-axis (0 to 1000) and 'Time (min)' on the x-axis (0 to 60). A red vertical bar at approximately 28 minutes indicates a spike in traffic. A legend at the bottom identifies 'WAN1 Traffic' (red) and 'WAN2 Traffic' (blue).

[D11]

Step 6: Click **Save Config** to save all changes to flash memory.



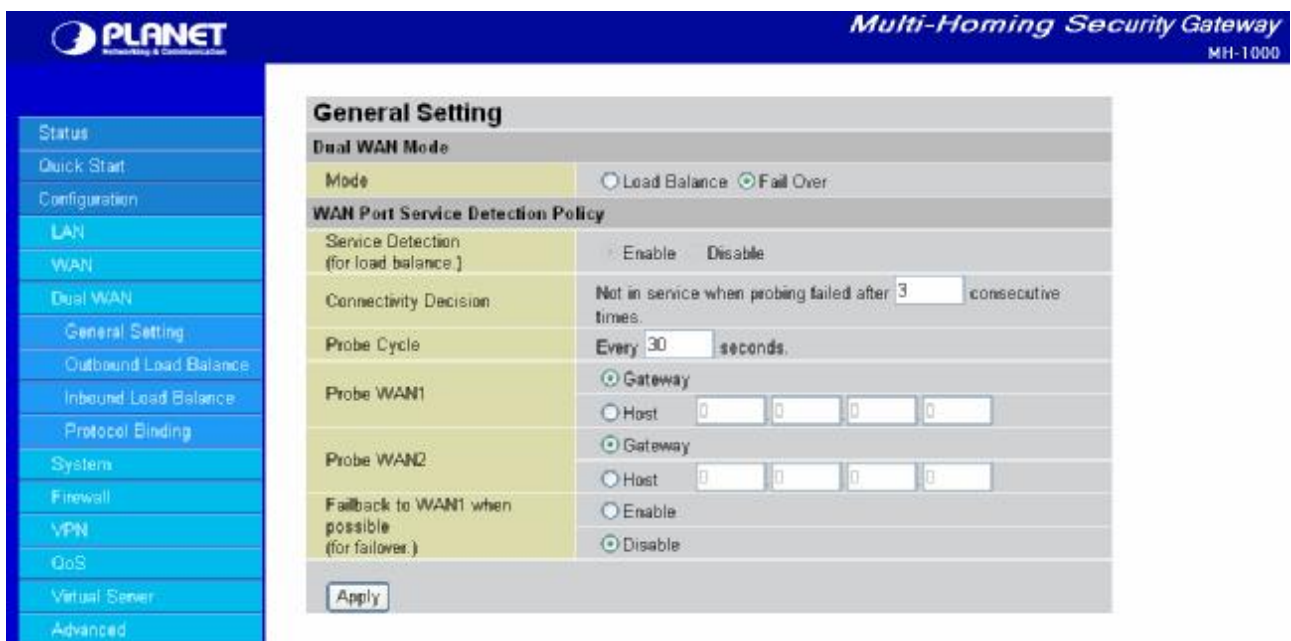
### D.3 Inbound Fail Over



Configuring your MH-1000 for Inbound Fail Over is a great way to ensure a more reliable connection for incoming requests. To do so, follow these steps:

NOTE: Before you begin, ensure that both WAN1 and WAN2 have been properly configured. See **Chapter 4: Router Configuration** for more details.

Step 1: From the Web Configuration Interface, go to **Configuration > Dual WAN > General Settings**. Select the **Fail Over** radio button.



Step 2: Configure Fail Over options if necessary.

**PLANET** Networking & Communication *Multi-Homing Security Gateway* MH-1000

Status  
Quick Start  
Configuration  
LAN  
WAN  
Dual WAN  
General Setting  
Outbound Load Balance  
Inbound Load Balance  
Protocol Binding  
System  
Firewall  
VPN  
QoS  
Virtual Server  
Advanced

### General Setting

**Dual WAN Mode**

Mode  Load Balance  Fail Over

**WAN Port Service Detection Policy**

Service Detection (for load balance.)  Enable  Disable

Connectivity Decision Not in service when probing failed after  consecutive times.

Probe Cycle Every  seconds.

Probe WAN1  Gateway  Host

Probe WAN2  Gateway  Host

Fallback to WAN1 when possible (for failover.)  Enable  Disable

Apply

Step 3: Go to **Configuration > Advanced > Dynamic DNS**. Set the **WAN1 DDNS** settings.

**PLANET** Networking & Communication *Multi-Homing Security Gateway* MH-1000

Status  
Quick Start  
Configuration  
LAN  
WAN  
Dual WAN  
System  
Firewall  
VPN  
QoS  
Virtual Server  
Advanced  
Static Route  
Dynamic DNS

### Dynamic DNS Settings

**Parameters**

Dynamic DNS  Enable  Disable

Dynamic DNS Server

Wildcard  Enable  Disable

Domain Name

Username

Password

Apply

Step 4: From the same menu, set the **WAN2 DDNS** settings.

The screenshot shows the Planet Multi-Homing Security Gateway web interface. The left sidebar contains a navigation menu with the following items: Status, Quick Start, Configuration, LAN, WAN, Dual WAN, System, Firewall, VPN, QoS, Virtual Server, Advanced, Static Route, Dynamic DNS, and Device Management. The main content area is titled "Dynamic DNS Settings" and contains the following parameters:

- Dynamic DNS:**  Enable  Disable
- Dynamic DNS Server:** www.dyndns.org (dynamic)
- Wildcard:**  Enable  Disable
- Domain Name:** planetest.dyndns.org
- Username:** jackyko
- Password:** [masked]

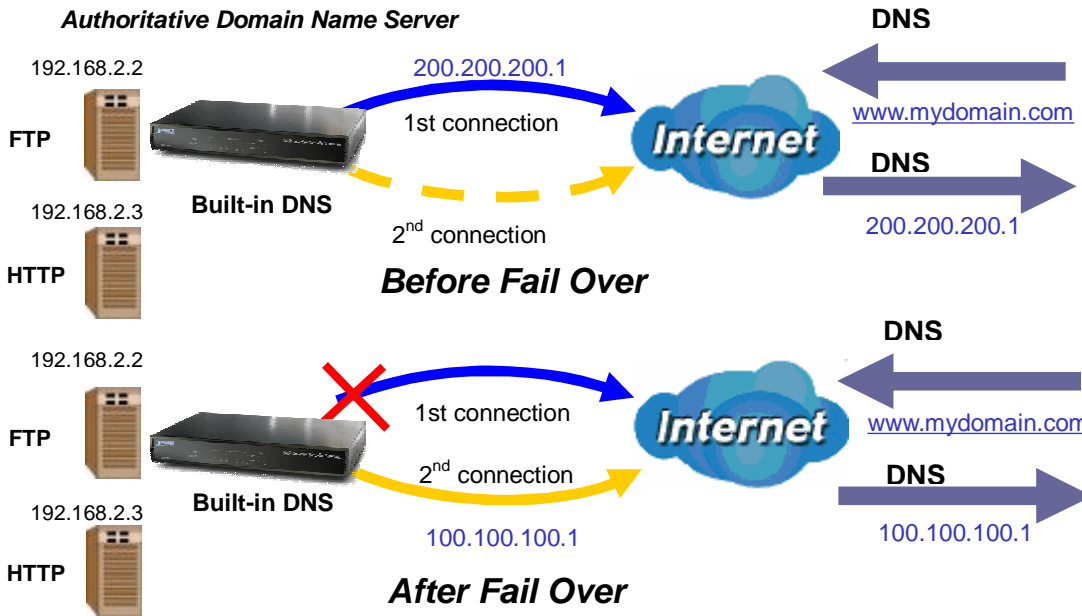
An "Apply" button is located at the bottom of the configuration form.

Step 5: Click **Save Config** to save all changes to flash memory.

The screenshot shows the Planet Multi-Homing Security Gateway web interface. The left sidebar contains a navigation menu with the following items: Status, Quick Start, Configuration, LAN, WAN, Dual WAN, System, Firewall, VPN, QoS, Virtual Server, Advanced, Static Route, Dynamic DNS, and Device Management. The main content area is titled "Dynamic DNS" and contains a "Dynamic DNS Table" with the following data:

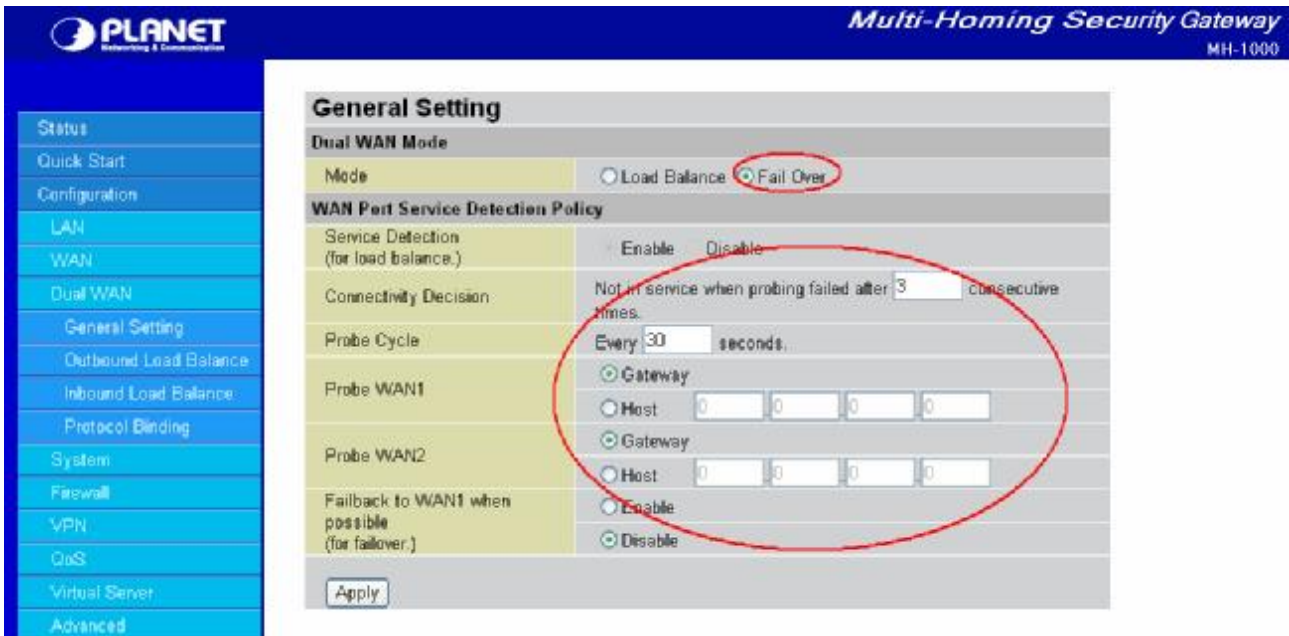
Interface	Enabled	Dynamic DNS Server	
WAN1	✓	www.dyndns.org (dynamic)	<a href="#">Edit</a>
WAN2	✓	www.dyndns.org (dynamic)	<a href="#">Edit</a>

## D.4 DNS Inbound Fail Over

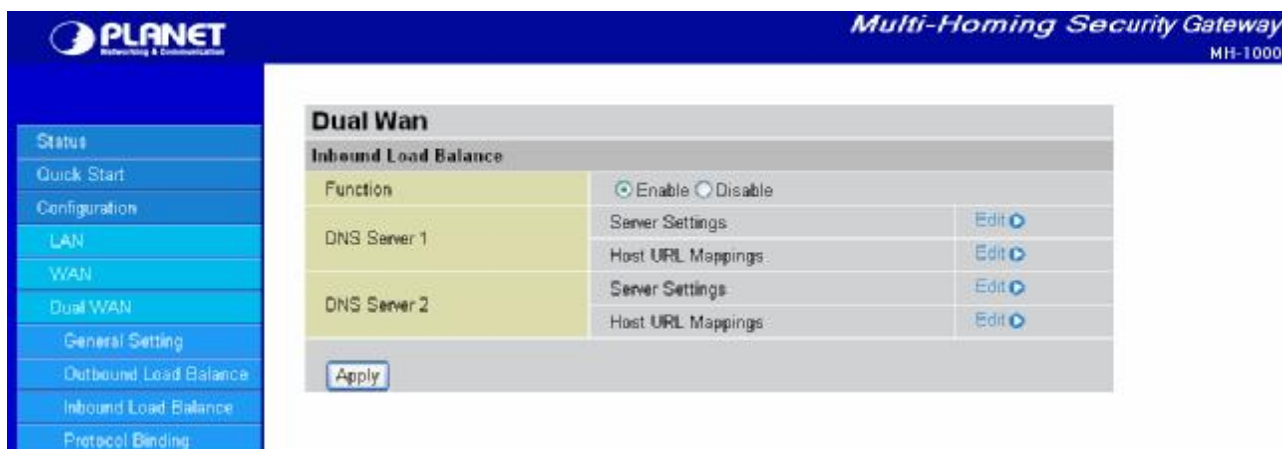


NOTE: Before proceeding, please ensure that both WAN1 and WAN2 are properly configured according to the settings provided by your ISP. If not, please refer to Chapter 4.2.2.1 ISP Settings for details on how to configure your WAN ports.

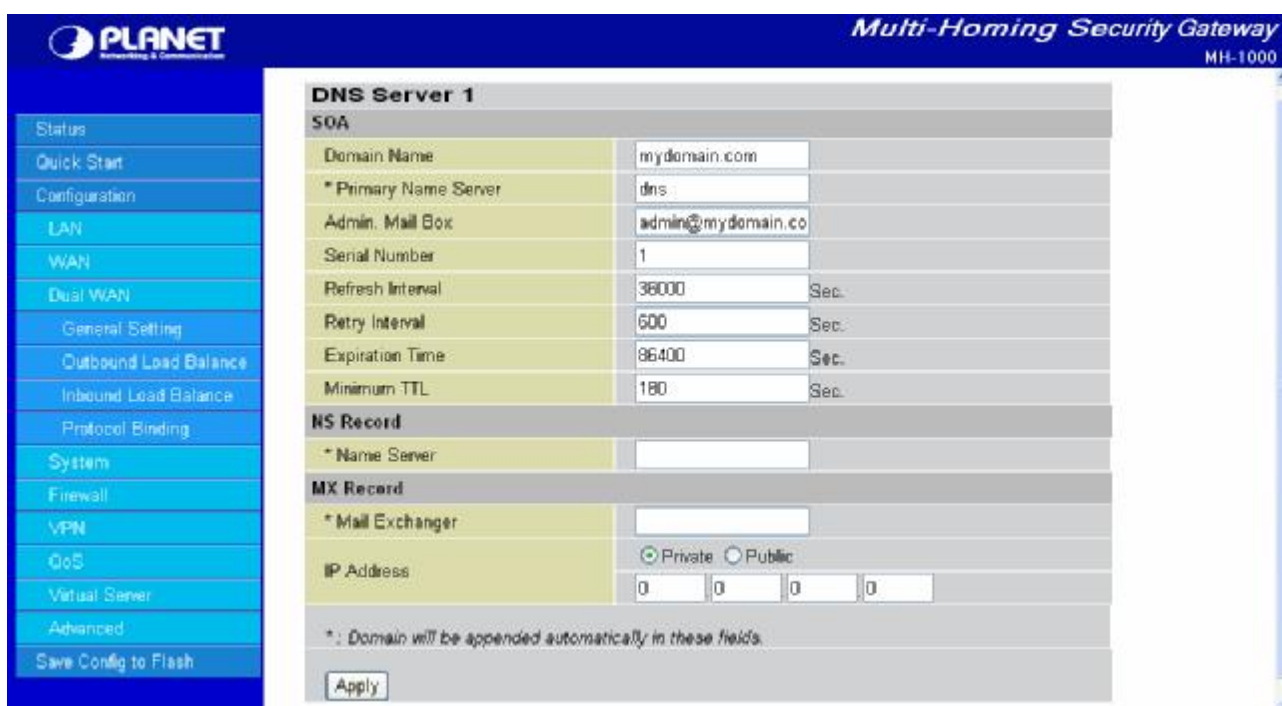
Step 1: Go to **Configuration > Dual WAN > General Settings**. Select the **Fail Over** radio button and configure your fail over policy.



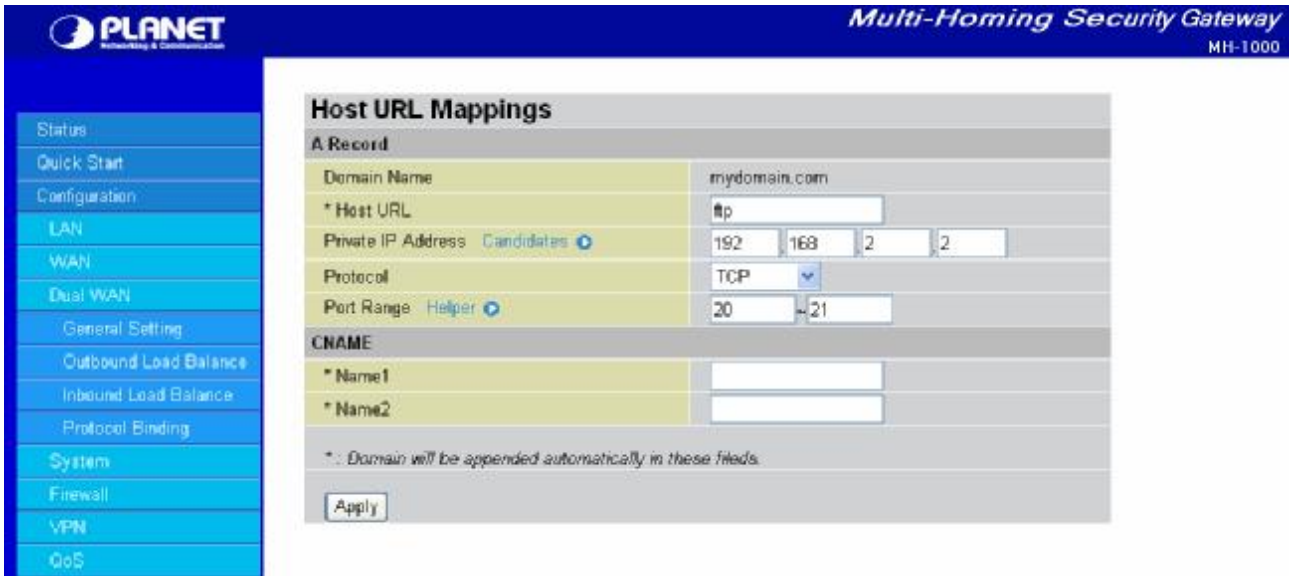
Step 2: Go to **Configuration > Dual WAN > Inbound Load Balance**. Select the **Enable** radio button and configure DNS Server 1 by clicking **Edit**.



Step 3: Input DNS Server 1 settings and click **Apply**.

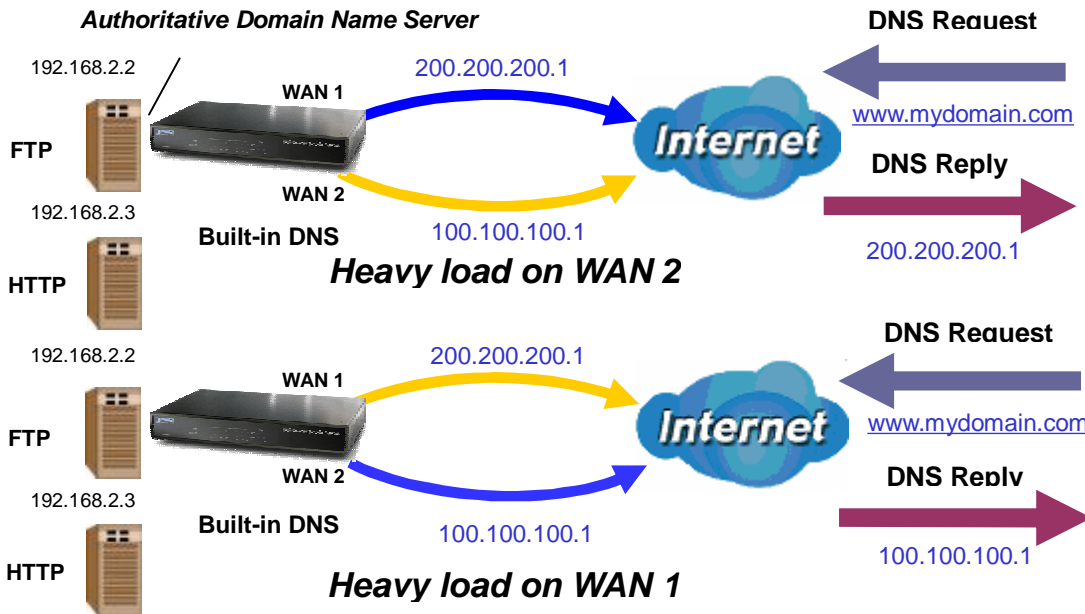


Step 4: Configure your Host URL Mapping for DNS Server 1 by clicking **Edit** to enter the Host URL Mappings List. Click **Create** and input the settings for Host URL Mappings and click **New**.



Step 5: Click **Save Config** to save all changes to flash memory.

### D.5 DNS Inbound Load Balancing



Step 1: Go to **Configuration > Dual WAN > General Settings**. Select the **Load Balance** radio button.

**PLANET** Multi-Homing Security Gateway MH-1000

**General Setting**

**Dual WAN Mode**

Mode  Load Balance  Fail Over

**WAN Port Service Detection Policy**

Service Detection (for load balance.)  Enable  Disable

Connectivity Decision Not in service when probing failed after  consecutive times.

Probe Cycle Every  seconds.

Probe WAN1  Gateway  Host

Probe WAN2  Gateway  Host

Failback to WAN1 when possible (for failover.)  Enable  Disable

Step 2: Go to **Configuration > Dual WAN > Inbound Load Balance > Server Settings** and configure DNS Server 1.

**PLANET** Multi-Homing Security Gateway MH-1000

**DNS Server 1**

**SOA**

Domain Name

\* Primary Name Server

Admin. Mail Box

Serial Number

Refresh Interval  Sec.

Retry Interval  Sec.

Expiration Time  Sec.

Minimum TTL  Sec.

**NS Record**

\* Name Server

**MX Record**

\* Mail Exchanger

Private  Public

IP Address

\*: Domain will be appended automatically in these fields.

Step 3: Go to **Configuration > Dual WAN > Inbound Load Balance > Host URL Mapping** and configure your FTP mapping.

**Host URL Mappings**

**A Record**

Domain Name	mydomain.com
* Host URL	ftp
Private IP Address <small>Candidates</small>	192 168 2 2
Protocol	TCP
Port Range <small>Helper</small>	20 ~ 21

**CNAME**

* Name1	
* Name2	

\* : Domain will be appended automatically in these fields.

Apply

Step 4: Next configure your HTTP mapping.

**Host URL Mappings**

**A Record**

Domain Name	mydomain.com
* Host URL	www
Private IP Address <small>Candidates</small>	192 168 2 3
Protocol	TCP
Port Range <small>Helper</small>	80 ~ 80

**CNAME**

* Name1	
* Name2	

\* : Domain will be appended automatically in these fields.

Apply

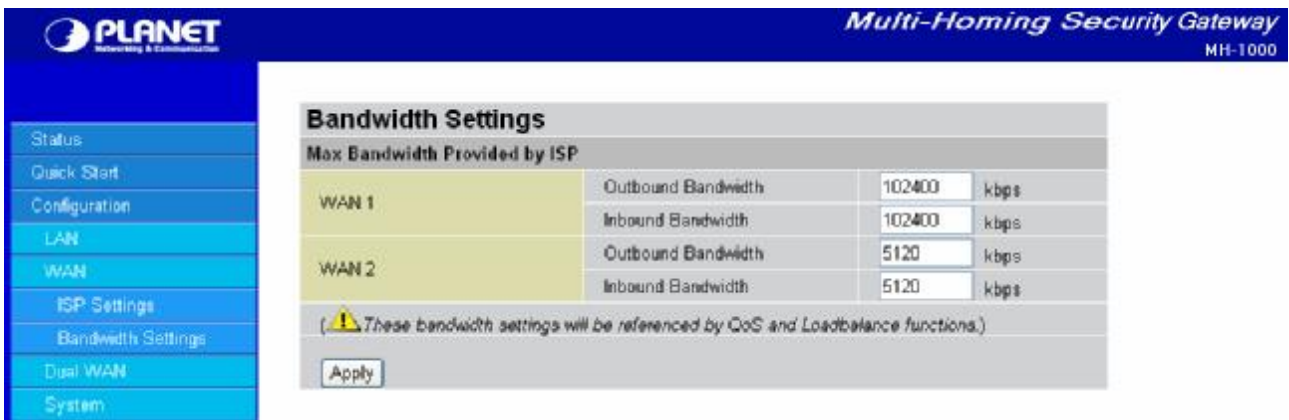
Step 5: Click **Save Config** to save all changes to flash memory.

## D.6 Dynamic DNS Inbound Load Balancing

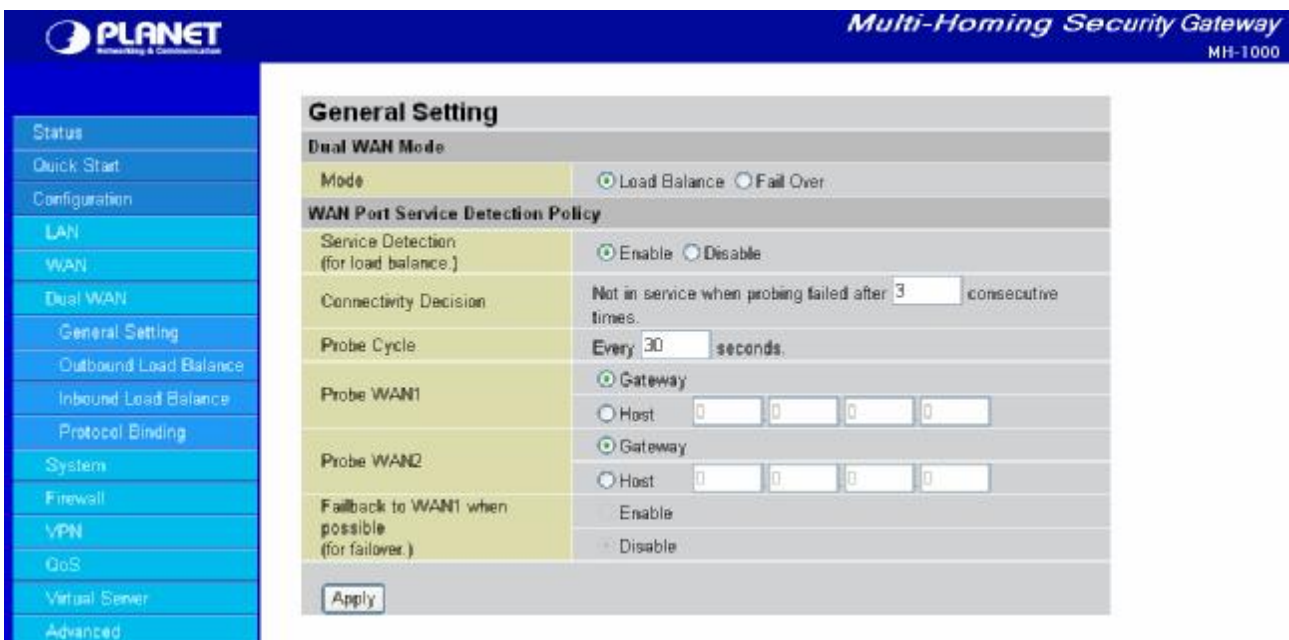




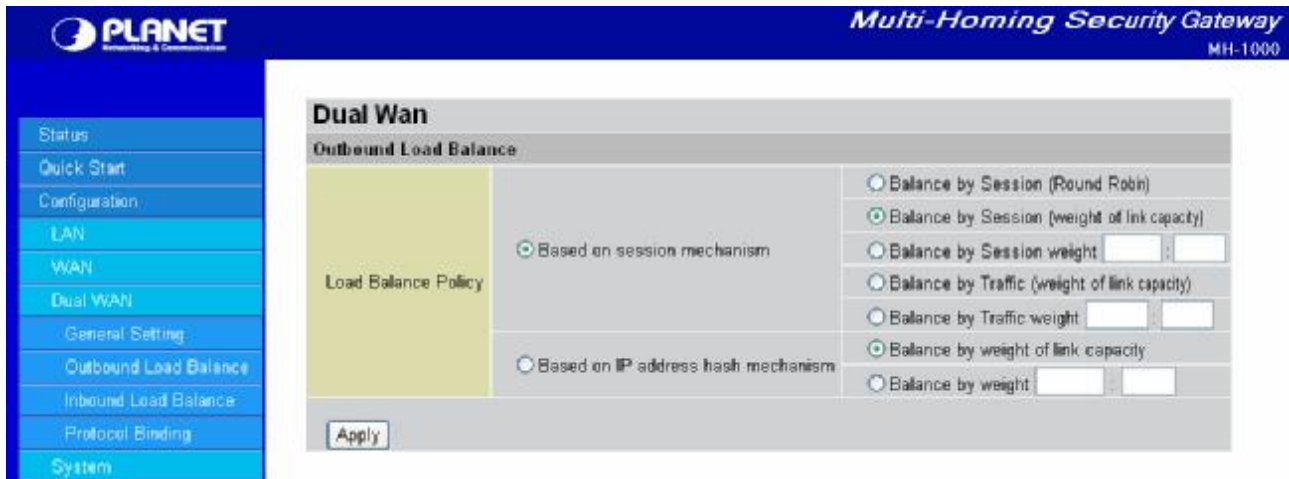
Step 1: Go to **Configuration > WAN > Bandwidth Settings**. Configure your WAN inbound and outbound bandwidth.



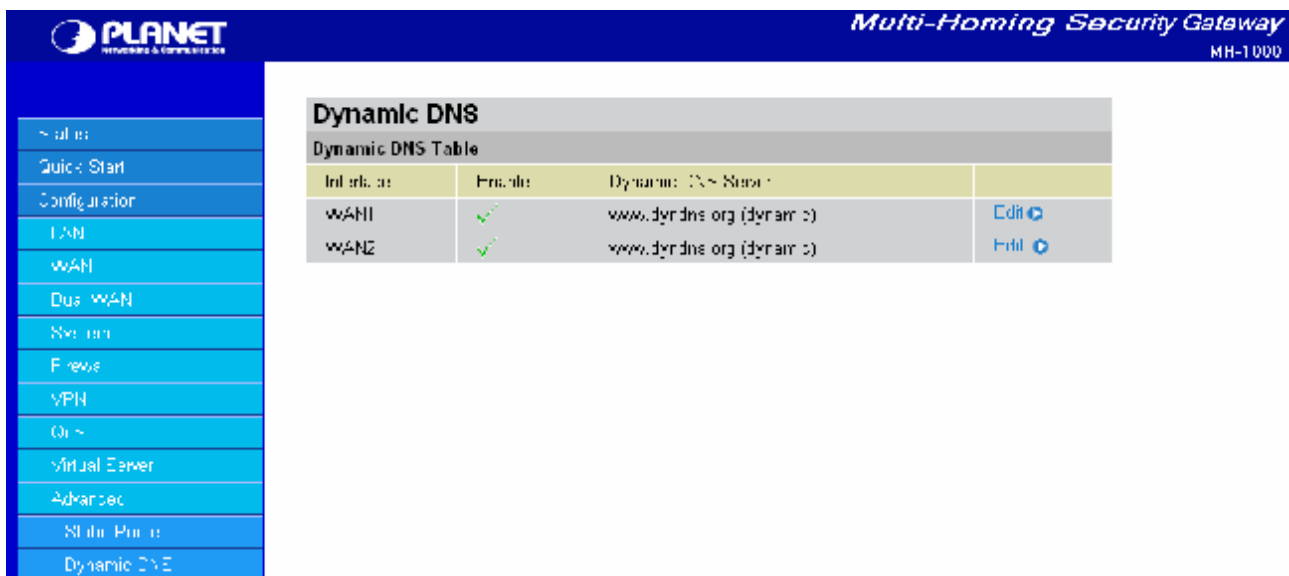
Step 2: Go to **Configuration > Dual WAN > General Settings** and enable **Load Balance** mode. You may then decide whether to enable Service Detection or not.



Step 3: Go to **Configuration > Dual WAN > Outbound Load Balance**. Choose your load balance policy and click **Apply** to apply your changes. If you selected Based on session mechanism as your policy, the source IP address and destination IP address may go through WAN1 or WAN2 depending on policy settings. If you selected Based on IP hash mechanism as your policy, the source IP address and destination IP address will go through a specific WAN port according to the IP hash algorithm.



Step 4: Go to **Configuration > Advanced > Dynamic DNS** and input the dynamic DNS settings for WAN1 and WAN2.



WAN1:

The screenshot shows the configuration page for WAN1 Dynamic DNS Settings. The interface includes a left-hand navigation menu with options like Status, Quick Start, Configuration, LAN, WAN, Dual WAN, System, Firewall, VPN, QoS, Virtual Server, Advanced, Static Route, and Dynamic DNS. The main content area is titled "Dynamic DNS Settings" and contains a "Parameters" section with the following fields:

Parameters	
Dynamic DNS	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Dynamic DNS Server	www.dyndns.org (dynamic) ▼
Wildcard	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Domain Name	www.planet2.dyndns.org
Username	username
Password	*****

An "Apply" button is located at the bottom of the parameters section.

WAN 2:

The screenshot shows the configuration page for WAN 2 Dynamic DNS Settings. The interface is identical to the WAN1 page, with the same navigation menu and "Dynamic DNS Settings" section. The "Parameters" section for WAN 2 has the following values:

Parameters	
Dynamic DNS	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Dynamic DNS Server	www.dyndns.org (dynamic) ▼
Wildcard	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Domain Name	www.planet3.dyndns.org
Username	username
Password	*****

An "Apply" button is located at the bottom of the parameters section.

Step 5: Go to **Configuration > Virtual Server** and set up a virtual server for both FTP and HTTP.

[D12]

The screenshot shows the configuration page for a Virtual Server on a Planet Multi-Homing Security Gateway (MH-1000). The left sidebar contains navigation options: Status, Quick Start, Configuration, LAN, WAN, Dual WAN, System, Firewall, VPN, QoS, and Virtual Server. The main content area is titled "Virtual Server" and "Add Forwarding Rule".

Application <small>Helper</small>	FTP
Protocol	TCP
External Port	20 ~ 21
Redirect Port	20 ~ 21
Internal IP Address <small>Candidates</small>	192 168 2 2

An "Apply" button is located at the bottom of the configuration form.

The screenshot shows the configuration page for a Virtual Server on a Planet Multi-Homing Security Gateway (MH-1000). The left sidebar contains navigation options: Status, Quick Start, Configuration, LAN, WAN, Dual WAN, System, Firewall, VPN, QoS, and Virtual Server. The main content area is titled "Virtual Server" and "Add Forwarding Rule".

Application <small>Helper</small>	HTTP
Protocol	TCP
External Port	80 ~ 80
Redirect Port	80 ~ 80
Internal IP Address <small>Candidates</small>	192 168 2 3

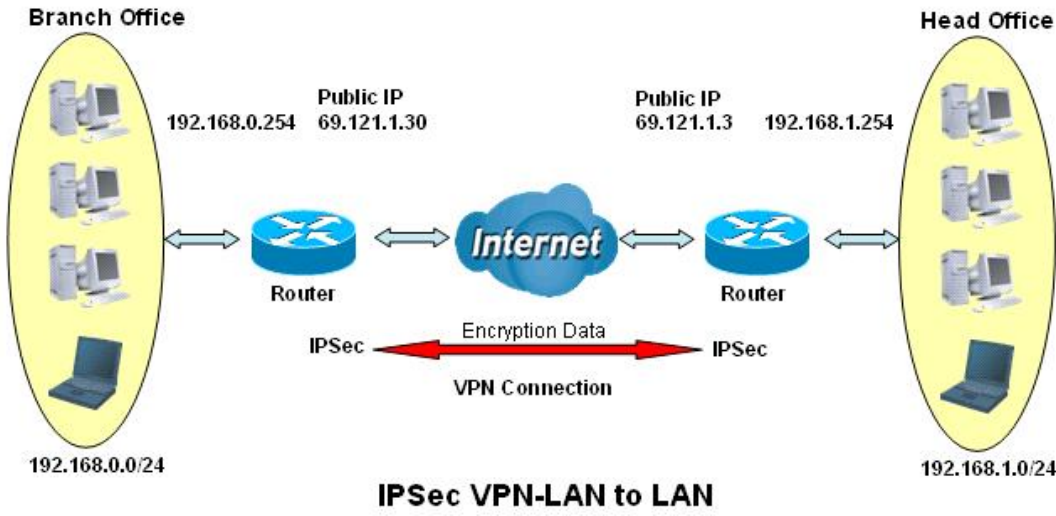
An "Apply" button is located at the bottom of the configuration form.

Step 6: Click **Save Config** to save all changes to flash memory.

## D.7 VPN Configuration

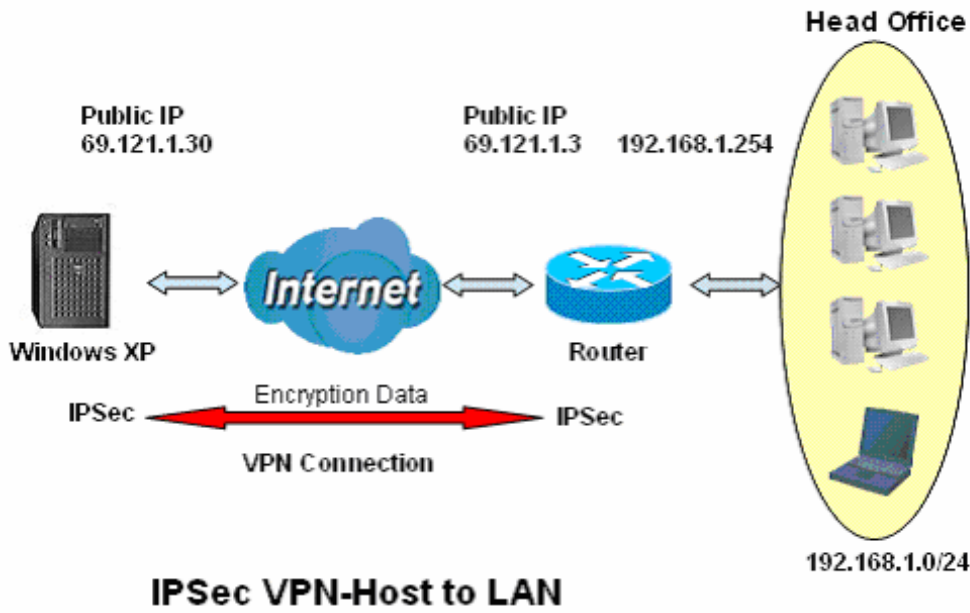
This section outlines some concrete examples on how you can configure MH-1000 for your VPN.

### D.7.1 LAN to LAN



	Branch Office	Head Office
<b>Local</b>		
ID	IP Address	IP Address
Data	69.121.1.30	69.121.1.3
Network	Any Local Address	Any Local Address
IP Address	192.168.0.0	192.168.1.0
Netmask	255.255.255.0	255.255.255.0
<b>Remote</b>		
Secure Gateway Address(or Hostname)	69.121.1.3	69.121.1.30
ID	IP Address	IP Address
Data	69.121.1.3	69.121.1.30
Network	Subnet	Subnet
IP Address	192.168.1.0	192.168.0.0
Netmask	255.255.255.0	255.255.255.0
<b>Proposal</b>		
IKE Pre-shared Key	12345678	12345678
Security Algorithm	Main Mode; ESP: MD5 3DES PFS	Main ESP MD5 3DES PFS

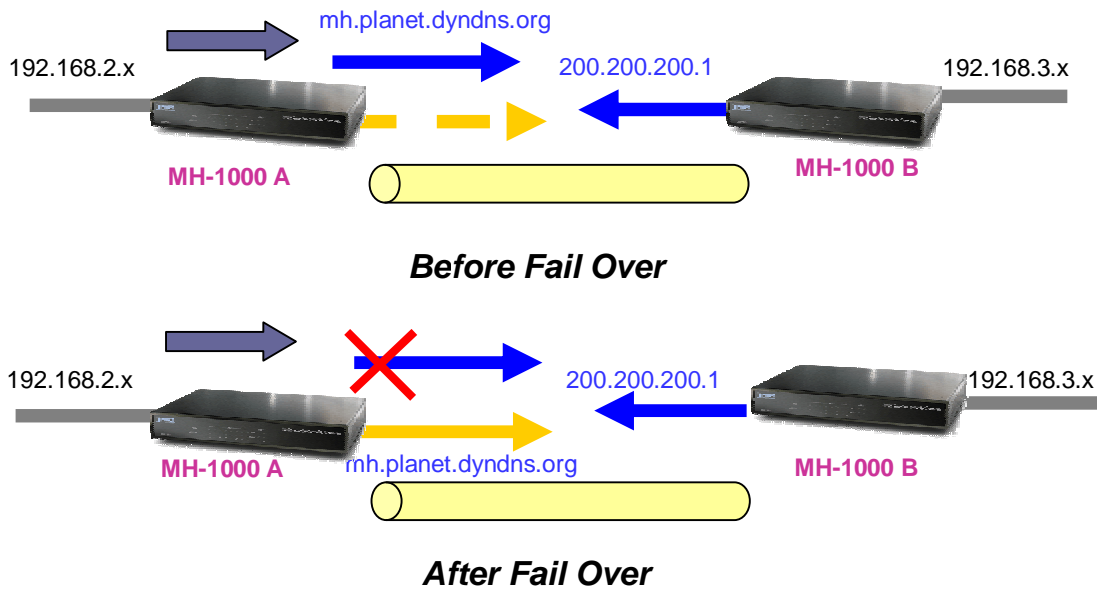
### D.7.2 Host to LAN



	Single client	Head Office
<b>Local</b>		
ID	IP Address	IP Address
Data	69.121.1.30	69.121.1.3
Network	Any Local Address	Any Local Address
IP Address	0.0.0.0	192.168.1.0
Netmask	0.0.0.0	255.255.255.0
<b>Remote</b>		
Secure Gateway Address(or Hostname)	69.121.1.3	69.121.1.30
ID	IP Address	IP Address
Data	69.121.1.3	69.121.1.30
Network	Subnet	Single Address
IP Address	192.168.1.0	69.121.1.30
Netmask	255.255.255.0	255.255.255.255
<b>Proposal</b>		
IKE Pre-shared Key	12345678	12345678
Security Algorithm	Main Mode; ESP: MD5 3DES	Main ESP MD5 3DES

	PFS	PFS
--	-----	-----

### D.8 IP Sec Fail Over (Gateway to Gateway)



Step 1: Go to **Configuration > Dual WAN > General Settings**. Enable Fail Over by selecting the **Fail Over** radio button. Then, configure your Fail Over policy.

The screenshot shows the configuration page for the Multi-Homing Security Gateway (MH-1000). The left sidebar contains a navigation menu with the following items: Status, Quick Start, Configuration, LAN, WAN, Dual WAN, General Setting (selected), Outbound Load Balance, Inbound Load Balance, Protocol Binding, System, Firewall, VPN, QoS, Virtual Server, and Advanced. The main content area is titled "General Setting" and contains the following sections:

- Dual WAN Mode**: Mode is set to  Fail Over.
- WAN Port Service Detection Policy**:
  - Service Detection (for load balance.):  Enable  Disable
  - Connectivity Decision: Not in service when probing failed after 3 consecutive times.
  - Probe Cycle: Every 30 seconds.
  - Probe WAN1:  Gateway,  Host (IP: 0.0.0.0)
  - Probe WAN2:  Gateway,  Host (IP: 0.0.0.0)
  - Failback to WAN1 when possible (for failover.):  Enable,  Disable

An "Apply" button is located at the bottom of the configuration area.

Step 2: Go to **Configuration > Advanced > Dynamic DNS** and configure your dynamic DNS settings (Both WAN1 and WAN2).


The screenshot shows the configuration page for Dynamic DNS Settings. The left sidebar contains a navigation menu with the following items: Status, Quick Start, Configuration, LAN, WAN, Dual WAN, System, Firewall, VPN, QoS, Virtual Server, Advanced, Static Route, and Dynamic DNS (selected). The main content area is titled "Dynamic DNS Settings" and contains the following sections:

- Parameters**:
  - Dynamic DNS:  Enable  Disable
  - Dynamic DNS Server: www.dyndns.org (dynamic)
  - Wildcard:  Enable  Disable
  - Domain Name: mih.planet.dyndns.org
  - Username: username
  - Password: \*\*\*\*\*

An "Apply" button is located at the bottom of the configuration area.

Step 3: Go to **Configuration > VPN > IPSec > IPSec Policy**. Click **Create** to configure VPN settings.





PLANET  
Networking & Communication

*Multi-Homing Security Gateway*

MH-1000

Status

Quick Start

Configuration

LAN

WAN

Dual WAN

System

Firewall

VPN

IPSec

IPSec Wizard

IPSec Policy

PPTP

QoS

Virtual Server

Advanced

Save Config to Flash


### IPSec

**Create**

Connection Name	<input type="text" value="MH1000A"/>		
Tunnel	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled		
Interface	<input type="radio"/> WAN1 <input type="radio"/> WAN2 <input checked="" type="radio"/> Auto		
<b>Local</b>			
ID	<input type="text" value="FQDN (DNS)"/> ▼	Data	<input type="text" value="mh.planet.dyndns.org"/>
Network	<input type="text" value="Subnet"/> ▼	IP Address	<input type="text" value="192"/> <input type="text" value="168"/> <input type="text" value="2"/> <input type="text" value="0"/>
		End IP Address	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
		Netmask	<input type="text" value="255"/> <input type="text" value="255"/> <input type="text" value="255"/> <input type="text" value="0"/>
<b>Remote</b>			
Secure Gateway	<input type="text" value="IP Address/ Hostname"/> ▼	Data	<input type="text" value="200.200.200.1"/>
ID	<input type="text" value="Remote WAN IP"/> ▼	Data	<input type="text"/>
Network	<input type="text" value="Subnet"/> ▼	IP Address	<input type="text" value="192"/> <input type="text" value="168"/> <input type="text" value="3"/> <input type="text" value="0"/>
		End IP Address	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
		Netmask	<input type="text" value="255"/> <input type="text" value="255"/> <input type="text" value="255"/> <input type="text" value="0"/>
<b>Proposal</b>			
Secure Association	<input checked="" type="radio"/> Main Mode <input type="radio"/> Aggressive Mode <input type="radio"/> Manual Key		
Method	<input checked="" type="radio"/> ESP <input type="radio"/> AH		
Encryption Protocol	<input type="text" value="3DES"/> ▼		
Authentication Protocol	<input type="text" value="MD5"/> ▼		
Perfect Forward Secure	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled		
PreShared Key	<input type="text" value="12345678"/>		
IKE Life Time	<input type="text" value="28800"/>	Seconds	
Key Life Time	<input type="text" value="3600"/>	Seconds	
Netbios Broadcast	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled		
<b>DPD Setting</b>			
DPD Function	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled		
Detection Interval	<input type="text" value="30"/>	seconds	
Idle Timeout	<input type="text" value="4"/>	consecutive times	
<input type="button" value="Apply"/>			

Step 4: Click **Save Config** to save all changes to flash memory.

To configure another MH-1000 gateway, refer to the screenshot below.



**Multi-Homing Security Gateway**  
 MH-1000

- Status
- Quick Start
- Configuration
- LAN
- WAN
- Dual WAN
- System
- Firewall
- VPN
- IPSec
- IPSec Wizard
- IPSec Policy
- PPTP
- QoS
- Virtual Server
- Advanced
- Save Config to Flash

### IPSec

**Create**

Connection Name: MH1000B

Tunnel:  Enabled  Disabled

Interface:  WAN1  WAN2  Auto

**Local**

ID: IP Address | Data: 200.200.200.1

Network: Subnet | IP Address: 192.168.3.0 | End IP Address: 0.0.0.0 | Netmask: 255.255.255.0

**Remote**

Secure Gateway: IP Address/Hostname | Data: mh.planet.dyndns.org

ID: FQDN (DNS) | Data: mh.planet.dyndns.org

Network: Subnet | IP Address: 192.168.2.0 | End IP Address: 0.0.0.0 | Netmask: 255.255.255.0

**Proposal**

Secure Association:  Main Mode  Aggressive Mode  Manual Key

Method:  ESP  AH

Encryption Protocol: 3DES

Authentication Protocol: MD5

Perfect Forward Secure:  Enabled  Disabled

PreShared Key: 12345678

IKE Life Time: 28800 Seconds

Key Life Time: 3600 Seconds

Netbios Broadcast:  Enabled  Disabled

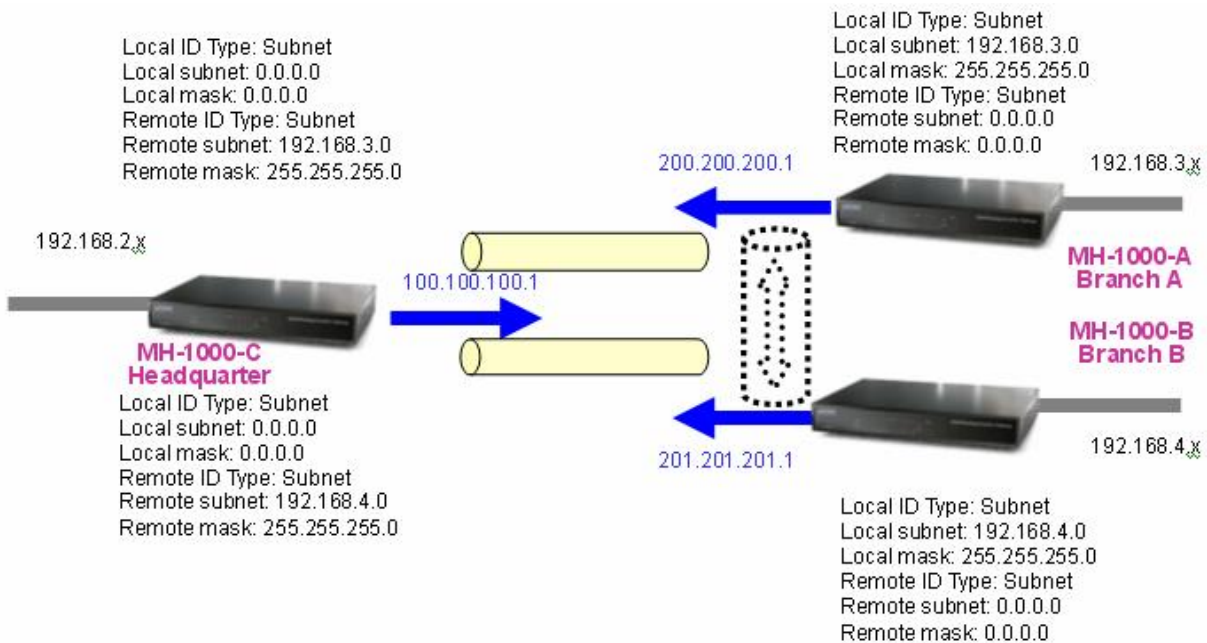
**DPD Setting**

DPD Function:  Enabled  Disabled

Detection Interval: 30 seconds

Idle Timeout: 4 consecutive times

## D.9 IP VPN Concentrator



Step 1: Go to **Configuration > VPN > IPSec > IPSec Policy** and configure the link from MH-1000-C to MH-1000-A Branch A.

The screenshot shows the configuration page for an IPSec policy on a Planet Multi-Homing Security Gateway. The interface includes a left-hand navigation menu and a main configuration area.

**Navigation Menu:**

- Status
- Quick Start
- Configuration
- LAN
- WAN
- Dual WAN
- System
- Firewall
- VPN
- IPSec
- IPSec Wizard
- IPSec Policy
- PPTP
- QoS
- Virtual Server
- Advanced
- Save Config to Flash

**IPSec Configuration Form:**

**Create**

Connection Name: CtoA

Tunnel:  Enabled  Disabled

Interface:  WAN1  WAN2  Auto

**Local:**

ID: IP Address [v] Data: 100.100.100.1

IP Address: 0 0 0 0

Network: Subnet [v] End IP Address: 0 0 0 0

Netmask: 0 0 0 0

**Remote:**

Secure Gateway: IP Address/Hostname [v] Data: 200.200.200.1

ID: Remote WAN IP [v] Data:

IP Address: 192 168 3 0

Network: Subnet [v] End IP Address: 0 0 0 0

Netmask: 255 255 255 0

**Proposal:**

Secure Association:  Main Mode  Aggressive Mode  Manual Key

Method:  ESP  AH

Encryption Protocol: 3DES [v]

Authentication Protocol: MD5 [v]

Perfect Forward Secure:  Enabled  Disabled

PreShared Key: 12345678

IKE Life Time: 28800 Seconds

Key Life Time: 3600 Seconds

Netbios Broadcast:  Enabled  Disabled

DPD Setting

DPD Function:  Enabled  Disabled

Detection Interval: 30 seconds

Idle Timeout: 4 consecutive times

[Apply]

Step 2: Go to **Configuration > VPN > IPSec > IPSec Policy** and configure the link from MH-1000-C to MH-1000-B Branch B.

**PLANET** Multi-Homing Security Gateway MH-1000

**IPSec**

Create

Connection Name: CtoB

Tunnel:  Enabled  Disabled

Interface:  WAN1  WAN2  Auto

Local

ID: IP Address Data: 100.100.100.1

IP Address: 0 0 0 0

Network: Subnet

End IP Address: 0 0 0 0

Netmask: 0 0 0 0

Remote

Secure Gateway: IP Address/ Hostname Data: 201.201.201.1

ID: Remote WAN IP Data:

IP Address: 192 168 4 0

Network: Subnet

End IP Address: 0 0 0 0

Netmask: 255 255 255 0

Proposal

Secure Association:  Main Mode  Aggressive Mode  Manual Key

Method:  ESP  AH

Encryption Protocol: 3DES

Authentication Protocol: MD5

Perfect Forward Secure:  Enabled  Disabled

PreShared Key: 12345678

IKE Life Time: 28800 Seconds

Key Life Time: 3600 Seconds

Netbios Broadcast:  Enabled  Disabled

DPD Setting

DPD Function:  Enabled  Disabled

Detection Interval: 30 seconds

Idle Timeout: 4 consecutive times

Apply

Step 3: Go to **Configuration > VPN > IPSec > IPSec Policy** and configure the connection from MH-1000-A Branch A to MH-1000-C.

**PLANET** Multi-Homing Security Gateway MH-1000

**IPSec**

Create

Connection Name: AtoC

Tunnel:  Enabled  Disabled

Interface:  WAN1  WAN2  Auto

Local

ID: IP Address [v] Data: 200.200.200.1

Network: Subnet [v]

IP Address: 192 168 3 0

End IP Address: 0 0 0 0

Netmask: 255 255 255 0

Remote

Secure Gateway: IP Address/Hostname [v] Data: 100.100.100.1

ID: Remote WAN IP [v] Data:

IP Address: 0 0 0 0

End IP Address: 0 0 0 0

Netmask: 0 0 0 0

Proposal

Secure Association:  Main Mode  Aggressive Mode  Manual Key

Method:  ESP  AH

Encryption Protocol: 3DES [v]

Authentication Protocol: MD5 [v]

Perfect Forward Secure:  Enabled  Disabled

PreShared Key: 12345678

IKE Life Time: 28800 Seconds

Key Life Time: 3600 Seconds

Netbios Broadcast:  Enabled  Disabled

DPD Setting

DPD Function:  Enabled  Disabled

Detection Interval: 30 seconds

Idle Timeout: 4 consecutive times

Apply

Step 4: Go to **Configuration > VPN > IPSec > IPSec Policy** and configure the connection from MH-1000-B Branch B to MH-1000-C.

**PLANET** Multi-Homing Security Gateway MH-1000

**IPSec**

Create

Connection Name: AtoC

Tunnel:  Enabled  Disabled

Interface:  WAN1  WAN2  Auto

Local

ID: IP Address: 201.201.201.1

Network: Subnet: 192.168.4.0

End IP Address: 0.0.0.0

Netmask: 255.255.255.0

Remote

Secure Gateway: IP Address/ Hostname: 100.100.100.1

ID: Remote WAN IP

Network: Subnet: 0.0.0.0

End IP Address: 0.0.0.0

Netmask: 0.0.0.0

Proposal

Secure Association:  Main Mode  Aggressive Mode  Manual Key

Method:  ESP  AH

Encryption Protocol: 3DES

Authentication Protocol: MD5

Perfect Forward Secure:  Enabled  Disabled

PreShared Key: 12345678

IKE Life Time: 28800 Seconds

Key Life Time: 3600 Seconds

Netbios Broadcast:  Enabled  Disabled

DPD Setting

DPD Function:  Enabled  Disabled

Detection Interval: 30 seconds

Idle Timeout: 4 consecutive times

Apply

Step 5: Click **Save Config** to save all changes to flash memory.

## D.10 Protocol Binding

Step 1: Go to **Configuration > Dual WAN > General Settings**. Select the **Load Balancing** radio button.

The screenshot shows the configuration interface for a Multi-Homing Security Gateway (MH-1000). The left sidebar contains a navigation menu with options: Status, Quick Start, Configuration, LAN, WAN, Dual WAN, General Setting, Outbound Load Balance, Inbound Load Balance, Protocol Binding, System, Firewall, VPN, QoS, Virtual Server, and Advanced. The main content area is titled "General Setting" and is divided into two sections:

- Dual WAN Mode:** The "Mode" is set to "Load Balance" (selected) and "Fail Over".
- WAN Port Service Detection Policy:**
  - Service Detection (for load balance.):** "Enable" (selected) and "Disable".
  - Connectivity Decision:** "Not in service when probing failed after 3 consecutive times." (The number 3 is in a text input field).
  - Probe Cycle:** "Every 30 seconds." (The number 30 is in a text input field).
  - Probe WAN1:** "Gateway" (selected) and "Host" (with IP address input fields: 0, 0, 0, 0).
  - Probe WAN2:** "Gateway" (selected) and "Host" (with IP address input fields: 0, 0, 0, 0).
  - Failback to WAN1 when possible (for failover.):** "Enable" and "Disable".

An "Apply" button is located at the bottom of the configuration area.

Step 2: Go to **Configuration > Dual WAN > Protocol Binding** and configure settings for WAN1.

The screenshot shows the configuration interface for a Multi-Homing Security Gateway (MH-1000). The left sidebar contains a navigation menu with options: Status, Quick Start, Configuration, LAN, WAN, Dual WAN, General Setting, Outbound Load Balance, Inbound Load Balance, Protocol Binding, System, Firewall, VPN, QoS, Virtual Server, and Advanced. The main content area is titled "Protocol Binding" and is divided into two sections:

- Add Protocol Binding Rules:**
  - Interface:** "WAN 1" (selected in a dropdown menu).
  - Source IP Range:** "All Source IP" and "Specified Source IP" (selected).
  - Source IP Address:** 192, 168, 2, 2 (input fields).
  - Source IP Netmask:** 255, 255, 255, 255 (input fields).
  - Destination IP Range:** "All Destination IP" and "Specified Destination IP" (selected).
  - Destination IP Address:** 200, 200, 200, 1 (input fields).
  - Destination IP Netmask:** 255, 255, 255, 255 (input fields).
  - Protocol:** "TCP" (selected in a dropdown menu).
  - Port Range:** 20 - 21 (input fields).

A warning message is displayed: "(⚠ Protocol Binding has higher priority than Routing.)". An "Apply" button is located at the bottom of the configuration area.

Step 3: Go to **Configuration > Dual WAN > Protocol Binding** and configure settings for WAN2.

**PLANET** Multi-Homing Security Gateway MH-1000

**Protocol Binding**

Add Protocol Binding Rules

Interface: WAN 2

Source IP Range:  All Source IP  Specified Source IP

Source IP Address: 192 168 2 3

Source IP Netmask: 255 255 255 255

Destination IP Range:  All Destination IP  Specified Destination IP

Destination IP Address: 0 0 0 0

Destination IP Netmask: 0 0 0 0

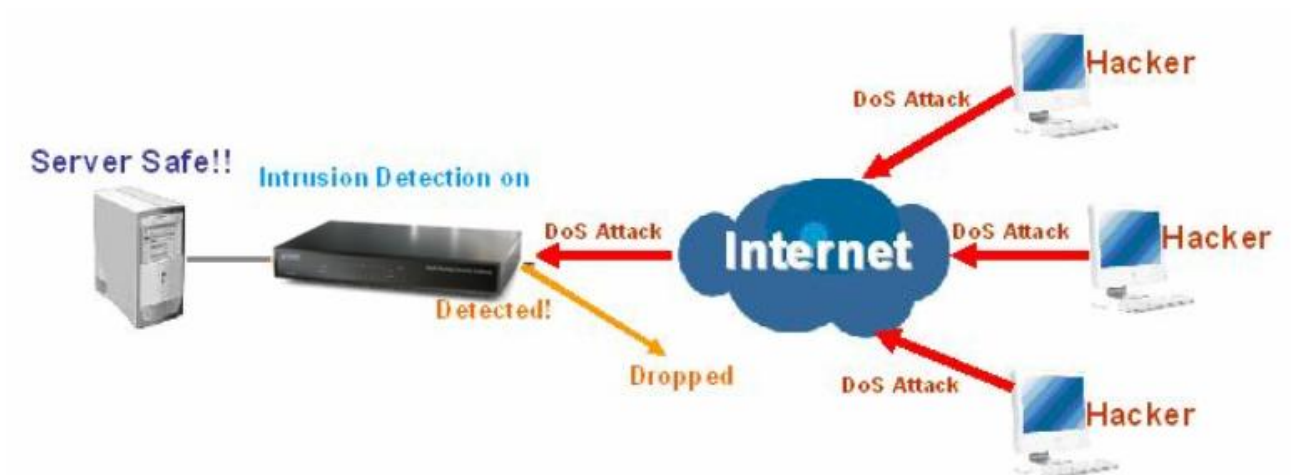
Protocol: TCP

Port Range:  20  21

( Protocol Binding has higher priority than Routing )

Step 4: Click **Save Config** to save all changes to flash memory.

## D.11 Intrusion Detection



Step 1: Go to **Configuration > Firewall > Intrusion Detection** and Enable the settings.

**PLANET** Multi-Homing Security Gateway MH-1000

**Intrusion Detection**

Enable for preventing hacker attack from Internet.

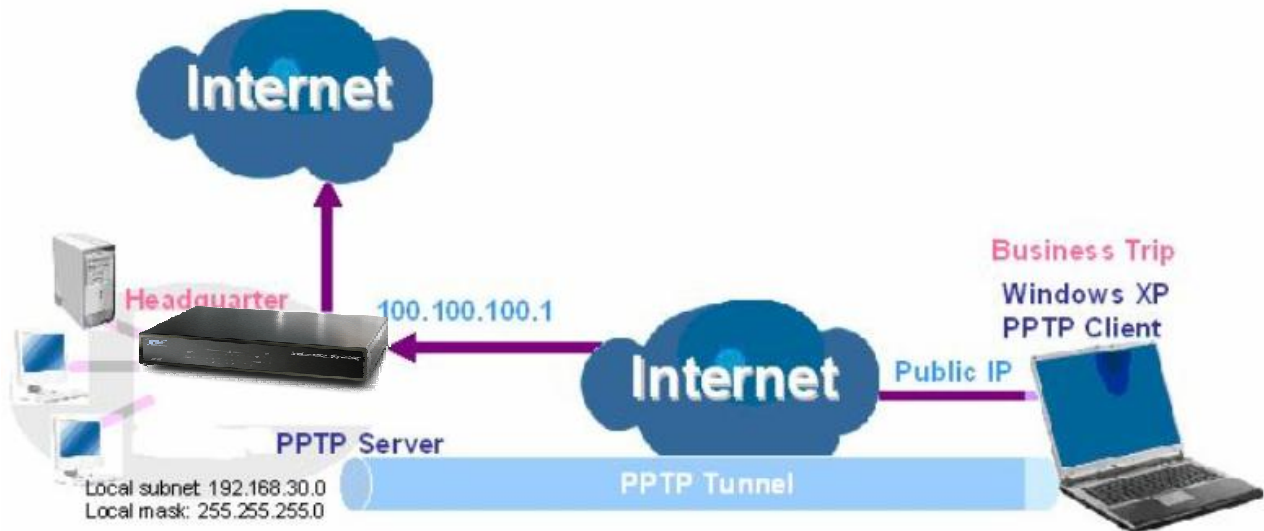
Intrusion Detection:  Enable  Disable

Intrusion Log:  Enable  Disable

Step 2: Click **Apply** and then **Save Config** to save all changes to flash memory.



## D.12 PPTP Remote Access by Windows XP



Step1: Go to **Configuration > VPN > PPTP** and Enable the PPTP function, Click **Apply**.

The screenshot shows the configuration interface for the Multi-Homing Security Gateway (MH-1000). The left sidebar contains a navigation menu with options: Status, Quick Start, Configuration, LAN, WAN, Dual WAN, System, Firewall, VPN, IPsec, PPTP, QoS, Virtual Server, Advanced, and Save Config to Flash. The main content area is titled 'PPTP' and is divided into two sections: 'General Setting' and 'Account Setting'.

**General Setting**

PPTP function	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Auth. Type	Pap or Chap
Data Encryption	Enable
Encryption Key Length	Auto
Peer Encryption Mode	Only Stateless
IP Addresses Assigned to Peer	Start from: 192.168.30 200
Idle Timeout	0 Min.

( ! Enable data encryption will use MS-CHAPv2 to authenticate the peer. )

**Account Setting**

Name	Enable	Type	Peer Network
<input type="button" value="Create"/>			

Step2: Click **Create** to create a PPTP Account.

**PLANET** Multi-Homing Security Gateway MH-1000

**PPTP**

**Add PPTP Account**

Connection Name	WinXP
Tunnel	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Username	test
Password	••••
Retype Password	••••
Connection Type	<input checked="" type="radio"/> Remote Access <input type="radio"/> LAN to LAN
Peer Network IP	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
Peer Netmask	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
Netbios Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

Apply

Step3: Click **Apply**, you can see the account is successfully created.

**PLANET** Multi-Homing Security Gateway MH-1000

**PPTP**

**General Setting**

PPTP function	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Auth. Type	Pap or Chap
Data Encryption	Enable
Encryption Key Length	Auto
Peer Encryption Mode	Only Stateless
IP Addresses Assigned to Peer	Start from: 192.168.30.200
Idle Timeout	0 Min.

(⚠ Enable data encryption will use MS-CHAPv2 to authenticate the peer.)

Apply

**Account Setting**

Name	Enable	Type	Peer Network		
WinXP	✓	Remote Access	-----	Edit	Delete

Create

Step4: Click **Save Config** to save all changes to flash memory.

Step5: In Windows XP, go **Start > Settings > Network Connections**.



Step6: In **Network Tasks**, Click **Create a new connection**, and press **Next**.



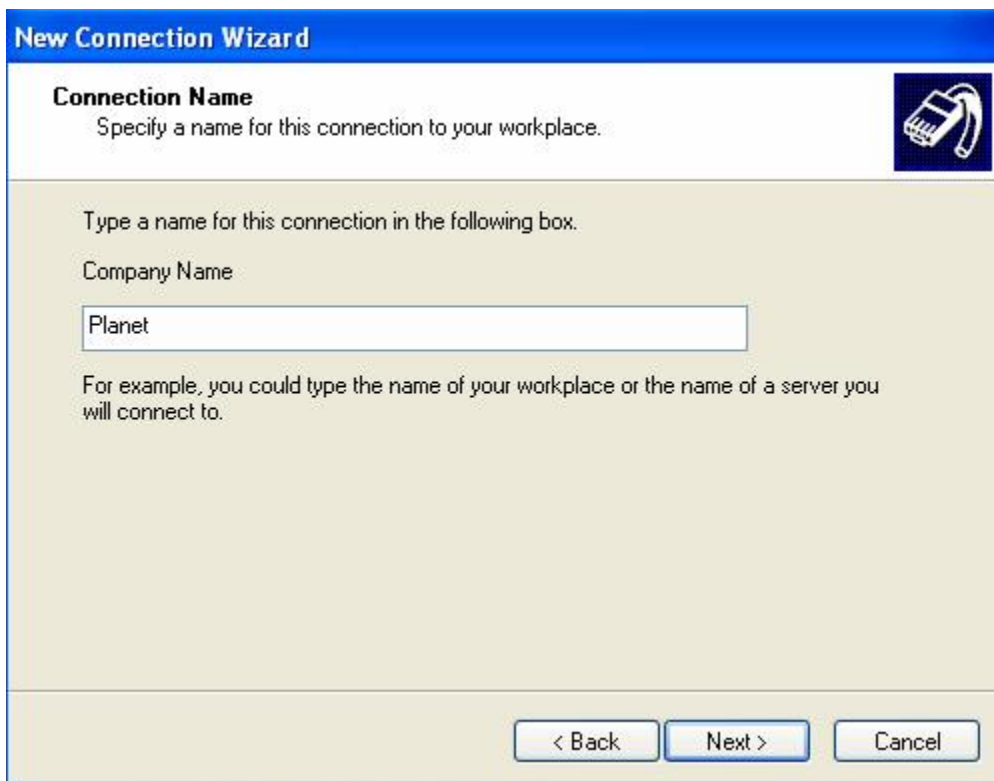
Step7: Select **Connect to the network at my workplace** and press **Next**.



Step8: Select **Virtual Private Network connection** and press **Next**.



Step9: Input the user-defined name for this connection and press **Next**.



**New Connection Wizard**

**Connection Name**  
Specify a name for this connection to your workplace.

Type a name for this connection in the following box.

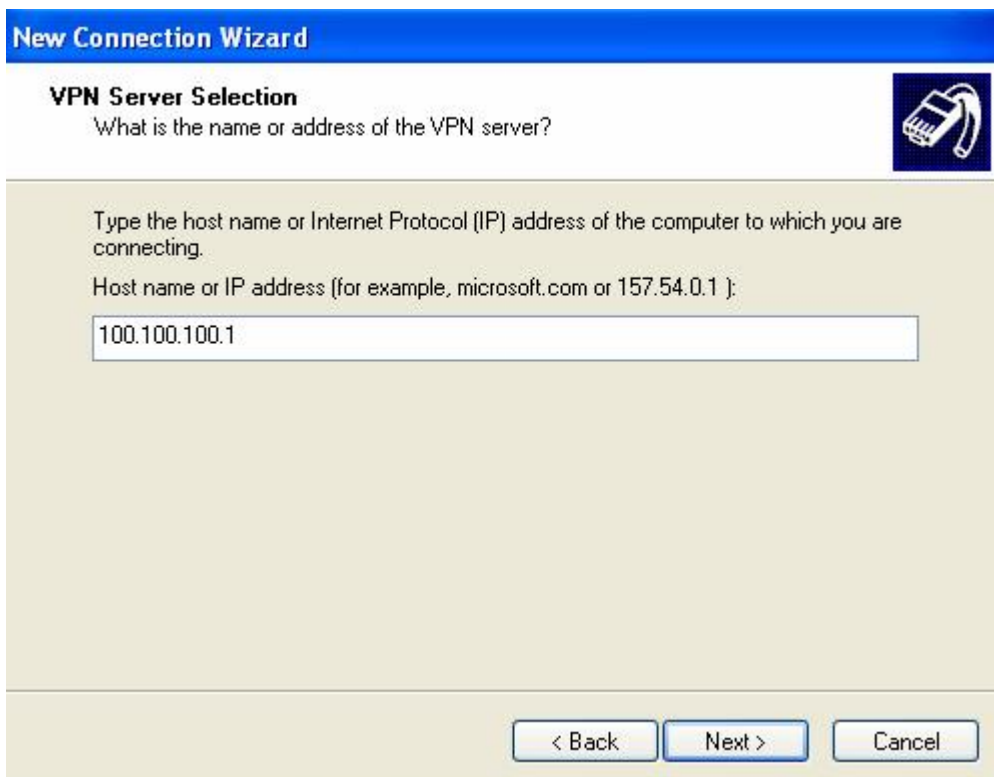
Company Name

Planet

For example, you could type the name of your workplace or the name of a server you will connect to.

< Back   Next >   Cancel

Step10: Input PPTP Server Address and press **Next**.



**New Connection Wizard**

**VPN Server Selection**  
What is the name or address of the VPN server?

Type the host name or Internet Protocol (IP) address of the computer to which you are connecting.

Host name or IP address (for example, microsoft.com or 157.54.0.1):

100.100.100.1

< Back   Next >   Cancel

Step11: Please press **Finish**.



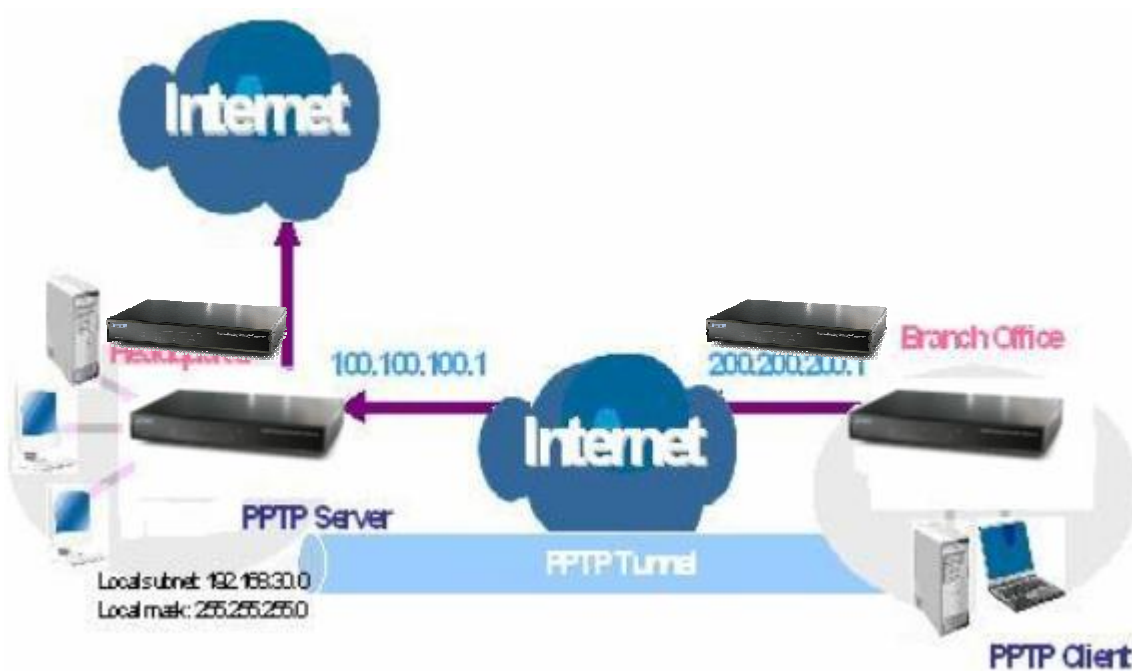
Step12: Double click the connection, and input **Username** and **Password** that defined in Planet PPTP **Account Settings**.



PS. You can also refer the **Properties > Security** page as below, by default.



### D.13 PPTP Remote Access



Step1: Go to **Configuration > VPN > PPTP** and Enable the PPTP function, **Disable** the **Encryption**, then Click **Apply**.

The screenshot shows the PPTP configuration page. The left sidebar contains a navigation menu with options: Status, Quick Start, Configuration, LAN, WAN, Dual WAN, System, Firewall, VPN, IPsec, PPTP, QoS, Virtual Server, Advanced, and Save Config to Flash. The main content area is titled 'PPTP' and has a sub-section 'General Setting'. The settings are as follows:

- PPTP function:  Enable  Disable
- Auth. Type: Pap or Chap
- Data Encryption: Enable
- Encryption Key Length: Auto
- Peer Encryption Mode: Only Stateless
- IP Addresses Assigned to Peer: Start from: 192.168.30 200
- Idle Timeout: 0 Min.

Below the settings is a warning icon and text: "( Enable data encryption will use MS-CHAPv2 to authenticate the peer.)". An 'Apply' button is located at the bottom of the General Setting section. Below this is the 'Account Setting' section, which contains a table with columns: Name, Enable, Type, Peer Network, and an empty cell. A 'Create' button with a plus icon is at the bottom left of the Account Setting section.

Step2: Click **Create** to create a PPTP Account.

The screenshot shows the 'Add PPTP Account' page. The left sidebar is the same as in the previous screenshot. The main content area is titled 'PPTP' and has a sub-section 'Add PPTP Account'. The settings are as follows:

- Connection Name: PPTPClient
- Tunnel:  Enable  Disable
- Username: test
- Password: \*\*\*\*
- Retype Password: \*\*\*\*
- Connection Type:  Remote Access  LAN to LAN
- Peer Network IP: [ ][ ][ ][ ]
- Peer Netmask: [ ][ ][ ][ ]
- Netbios Broadcast:  Enable  Disable

An 'Apply' button is located at the bottom left of the form.

Step3: Click **Apply**, you can see the account is successfully created.



**PLANET** Multi-Homing Security Gateway MH-1000

**PPTP**

**General Setting**

PPTP function	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Auth. Type	Pap or Chap
Data Encryption	Enable
Encryption Key Length	Auto
Peer Encryption Mode	Only Stateless
IP Addresses Assigned to Peer	Start from: 192.168.30.200
Idle Timeout	0 Min.

(! Enable data encryption will use MS-CHAPv2 to authenticate the peer.)

Apply

**Account Setting**

Name	Enable	Type	Peer Network	Edit	Delete
PPTPClient	<input checked="" type="checkbox"/>	Remote Access	-----	<a href="#">Edit</a>	<a href="#">Delete</a>

Create

Step4: Click **Save Config** to save all changes to flash memory.

Step5: In another MH-1000 as Client, Go to **Configuration > WAN > ISP Settings**.

**PLANET** Multi-Homing Security Gateway MH-1000

**WAN1**

**PPTP**

Connection Method	PPTP Settings
Username	test
Password	****
Retype Password	****
PPTP Client IP	200 200 200 1
PPTP Client IP Netmask	255 255 255 0
PPTP Client IP Gateway	200 200 200 254
PPTP Server IP	100 100 100 1
Connection	Always Connect
Idle Time	10 minutes
IP assigned by your ISP	<input checked="" type="radio"/> Dynamic (IP automatically assigned by your ISP) <input type="radio"/> Fixed (Your ISP requires you to input IP address)
MAC Address	<input type="checkbox"/> Your ISP requires you to input WAN Ethernet MAC MAC Address 00 00 00 00 00 00
DNS	<input checked="" type="checkbox"/> Your ISP requires you to manually setup DNS settings Primary DNS 168 95 1 1 Secondary DNS 0 0 0 0
RIP	Disable <input checked="" type="radio"/> RIP-2B <input type="radio"/> RIP-2M
MTU	1432

Apply Reset

Step6: Click **Apply**, and **Save CONFIG**.