FBR-4000

Multi-WAN VPN Router

User Manual

V1.0

TABLE OF CONTENTS

1: INTRODUCTION 1

INTERNET FEATURES 1
OTHER FEATURES 3
PACKAGE CONTENTS 4
PHYSICAL DETAILS 4
Front Panel 4
Rear Panel 6

2: BASIC SETUP 8

OVERVIEW 8
PROCEDURE 8
1. Configuring the Router for your LAN 8
2. Installing the Router in your LAN 12
3. Configuring the Router for Internet Access 13
4. Enable Dedicated DMZ Port 15
5. Configure PCs on your LAN 16
Macintosh Clients 18
Linux Clients 18

3: ADVANCED PORT 19

OVERVIEW 19
PORT OPTIONS 19
LOAD BALANCE 21
ADVANCED PPPOE 23
ADVANCED PPTP 25

4: ADVANCED SETUP 27

OVERVIEW 27
HOST IP 28
ROUTING 30
VIRTUAL SERVER 33
SPECIAL APPLICATION 36
DYNAMIC DNS 38
MULTI DMZ 40
UPNP SETUP 41
NAT SETUP 42
ADVANCED FEATURE 44

5: SECURITY MANAGEMENT 47

OVERVIEW 47
BLOCK URL 47
ACCESS FILTER 49
SESSION LIMIT 51
SYSFILTER EXCEPTION 52

6: VPN CONFIGURATION 53

OVERVIEW 53
IKE GLOBAL SETUP 53
IPSEC POLICY SETUP 56
MESH GROUP SETUP 63
VPN LOG 65

7: QOS CONFIGURATION 66

OVERVIEW 66
QOS SETUP 66

POLICY CONFIGURATION 67
8: MANAGEMENT ASSISTANT 70
OVERVIEW 70
ADMIN. SETUP 71
SETTINGS ï ADMIN. SETUP 71
EMAIL ALERT 73
SNMP 74
SYSLOG 75
UPGRADE FIRMWARE 77
9: NETWORK INFO 78
OPERATION 78
SYSTEM STATUS 78
Restore Factory Defaults 80
WAN STATUS 81
APPENDIX A - SPECIFICATION 82
APPENDIX B - WINDOWS TCP/IP SETUP 83
APPENDIX C - TROUBLESHOOTING 89

1: Introduction

Congratulations on the purchase of your new Multi-WAN VPN Router. The Multi-WAN VPN Router not only provides a selection of 1~4 WAN ports ï it also provides ***Shared Broadband Internet Access*** for all LAN users.

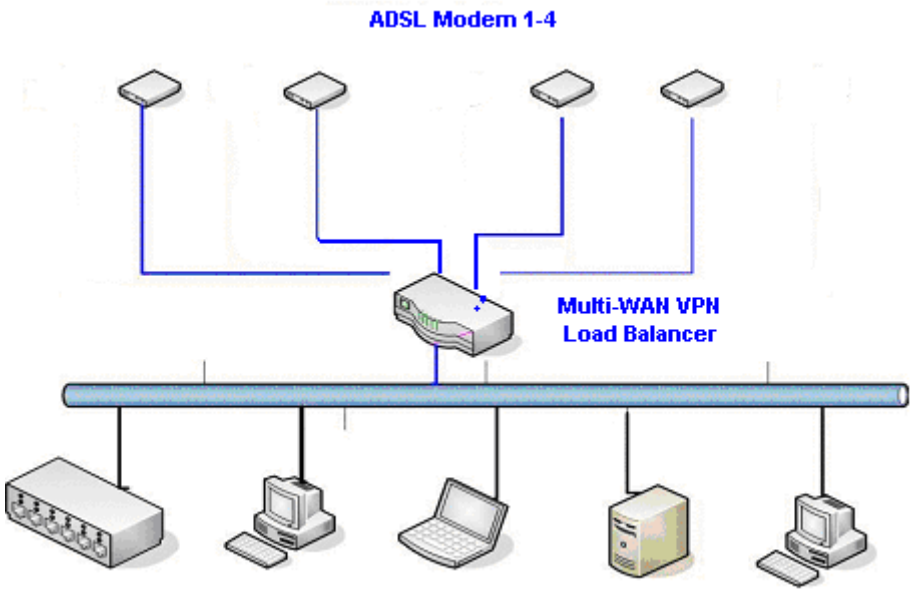


Figure 1-1: Multi-WAN VPN Router

Internet Features

¶ ***Flexible use of WAN ports***

There are 4 WAN ports available for use on Multi-WAN Link Balancer. The user can decide how many WAN ports to use by setting the web page on setup area.

¶ ***Shared Broadband Internet Access***

All LAN users can access the Internet through the Multi-WAN VPN Router by sharing from one (1) up to four (4) Broadband modems and connections.

¶ ***High-Performance multi ADSL Modem Support***

The Multi-WAN VPN Router has four (4) WAN ports, allowing the connection of up to four (4) Broadband modems at the same time.

This can provide a greater increase in bandwidth than is allowed by a single modem. This flexible configuration allows each port to use a different type of modem and connection method. Also, the Internet traffic that is shared between the 4 modems can be pre-determined.

¶ ***Support for all common Connection Methods***

All popular DSL, Cable Modems and connection methods are supported. These include - Fixed IP, Dynamic IP, PPPoE and PPTP.

¶ ***Outbound Traffic Load Balancing and Failover***

There are a variety of load balancing methods that allow administrators to manage the traffic from LAN or WAN in order to maximize bandwidth - as well as smart health check methods to protect against connection failure for failover.

¶ ***PPPoE Session Management***

Multiple PPPoE sessions are supported and PCs can if desired.

¶ ***Multiple IP Address Support***

If your ISP allocates you multiple IP addresses, these are also supported and you can map IP addresses to selected PCs if desired.

¶ ***Special Application***

This feature allows you to use some non-standard applications; for example, where the port number used for the response is different to the port number used by the sender.

¶ ***Virtual Server***

This feature allows Internet users to access Internet servers on your LAN. For standard servers such as Web, FTP or E-Mail servers, only the IP address of the server PC is required. You can also define your own Server types if required.

¶ ***Multiple DMZ***

A "DMZ" PC will receive incoming connection requests which would otherwise be blocked. For each IP address allocated by your ISP, a separate "DMZ" PC can be specified. So if your ISP has given you multiple IP addresses, yeMulti-WAN VPN have mul Router, each DMZ PC -way Internet access, providing the ability to run programs that are otherwise normally incompatible with NAT routers.

¶ ***Access Filter***

The network Administrator can use the Access Filter to gain fine control over the Internet access and applications available to LAN users. Five (5) user groups are available and each group can be assigned unique access rights.

¶ ***Block URL***

This feature can be used by the Administrator to block access to undesirable Web sites by LAN users. You can even assign different settings for different groups of PCs.

¶ ***Session Limit***

With the Session Limit feature, if the number of new sessions for the system exceeds the maximum allowance set by the Administrator in the sampling time, any new session in the system will be dropped.

¶ ***System Filter Exception***

This feature ensures that every packet with an unrecognized port will be rejected so as to prevent access to port scanning programs from hackers. However, in some situations this may incur problems with some servers (e.g. SMTP server port 113) or WAN clients which require a response packet to verify the availability of their communication peers.

¶ ***VPN (Virtual Private Network)***

Support is provided for up to 50 VPN tunnels with a failover and back-up mechanism.

Other Features

- ***12-Port Switching Hub***

  The Multi-WAN VPN Router incorporates a 12-port 10 /100BaseT switching hub, making it easy to create or extend your LAN as needed.

- ***DHCP Server Support***

  Dynamic **H**ost **C**onfiguration **P**rotocol provides a dynamic IP address to PCs and other devices upon request. The Multi-WAN VPN Router can act as a **DHCP Server** for devices on your local LAN.

- ***Multi Segment LAN Support***

  LANs comprising of one or more segments or additional IPs are supported via the Multi-WAN VPN Router's built-in static routing table.

- ***Easy Setup***

  Setup and configuration is easily accomplished through your favorite WEB browser.

- ***Remote Management***

  The Multi-WAN VPN Router can be managed from any PC on your LAN. Also, if an Internet connection exists, it can (optionally) be configured via the Internet.

- ***Password - protected Configuration***

  Optional password protection is provided to prevent unauthorized users from modifying the configuration data and settings.

- ***HTTP Firmware Upgrade and backup***

  The web management feature allows you to use HTTP upgrade for new firmware and backup system configuration from a local or even remote web-based setupò is enabled in the Advanced featur

- ***Email Alert***

  The Email Alert will send a warning email message to the system administrator if any of the WAN ports become disconnected when more than two WAN ports are enabled or if there is excessive ping notification.

- ***Syslog***

  This is a very useful feature for monitoring the device in that it can generate real time system information on the web page or on a particular machine.

- ***QoS Configuration.***

  This function will allow higher priority pass-through for specified packets such as real-time applications like Internet phone, video conference, etc.

- ***UPnP***

  When UPnP (Universal Plug-and-Play) is enabled, the Multi-WAN VPN Router becomes a network device. This feature is useful for detecting and controlling network devices such as Internet gateways.

Package Contents

The following items are included in the Multi-WAN VPN Router package:

¶ Multi-WAN VPN Router Unit

¶ Power Cord

¶ Quick Installation Guide

¶ CD with Manual

If any of the above items are damaged or missing, please contact your dealer immediately.

Physical Details

Front Panel

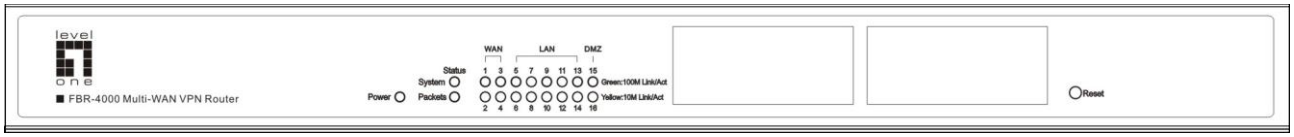


Figure 1-2: Front Panel

Front Panel LED indication is as follows:

Power	OFF ï No Power ON ï Normal Operation
Status	
System	Blinking ï Normal Operation. ON/OFF ï Error
Packets	Blinking ï Packets Active ON/OFF ï No Packet
Ethernet	Green ON ï 100M Linked Yellow ON ï 10M Linked Blinking ï Data Transmit / Receive. OFF ï No Linked

Ethernet Ports and Reset Button

Ethernet Ports	WAN ports: Using Port 1 to Port 4 for connecting to Modem(s). DMZ ports: Using Port 15 and Port 16 LAN ports: The remaining ports which are connected to PCs or a Hub. Note: Any port will automatically operate normal LAN cable to connect to a normal port on another hub.
Reset Button	When pressed and released, the Multi-WAN VPN Router will reboot (restart) within 1 second. It will reset to default when pushed and held for more than 3 seconds.

Some Status and Error conditions are indicated by the combinations of LEDs, as shown below:

LED Action	Condition
Status ï System & Packets flash alternatively.	Firmware Download in progress.
Status ï System & Packets flash concurrently.	MAC address not assigned.
Status ï System (Solid Off) & Packets (Solid On)	SDRAM error
Status ï System (Solid On) & Packets (Solid On)	Timer/Interrupt error

Rear Panel

Figure 1-3: Rear Panel

100 ~ 240VAC	Connects to AC100~240V / 50~60Hz with supplied AC power cord.

Default Settings

When the Multi-WAN VPN Router has finished booting, all configuration settings will be set to the factory defaults, including:

- *IP Address* set to its default value of 192.168.1.1, with a *Network Mask* of 255.255.255.0
- *DHCP Server* is enabled
- *User Name: admin*
- Password cleared (no password)

TFTP Download

This setting should be used only if your Multi-WAN VPN Router becomes unusable and you are attempting to restore it by upgrading the firmware. Follow this procedure:

1. Power-On the Multi-WAN VPN Router.
2. Use the supplied Windows utility or a TFTP client program to apply the new firmware. If using the supplied Windows TFTP program, the screen will look like the following example:

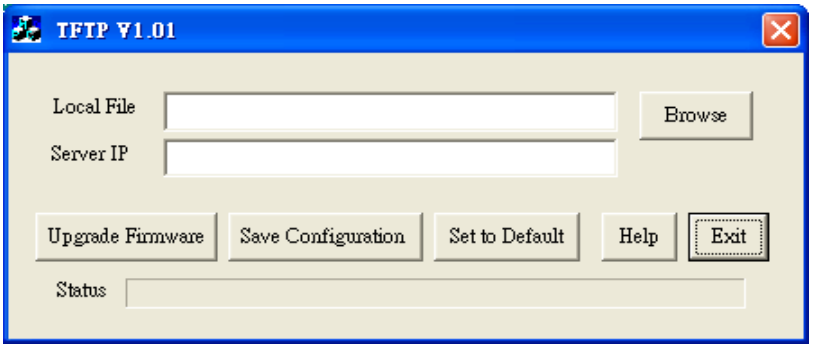


Figure 1-4: Windows TFTP utility

- ¶ Enter the name of the firmware upgrade file located on your PC, or click the "Browse" button to locate the file.
- ¶ Enter the LAN IP address of the Multi-WAN VPN Router in the "Server IP" field.
- ¶ Click "Upgrade Firmware" to send the file to the Multi-WAN VPN Router.

3. When the upgrade is finished, the Multi-WAN VPN Router should work normally. The factory default settings will be applied.

Note:

The supplied Windows TFTP utility also allows you to perform three (3) additional operations:

- ¶ Save the current configuration settings to your PC (use the "Save Configuration" button).
- ¶ Restore a previously saved configuration file to the Multi-WAN VPN Router (use the "Upgrade Firmware" button).
- ¶ Set the Multi-WAN VPN Router to its default values (use the "Set to Default" button).

2: Basic Setup

Overview

Basic Setup of your Multi-WAN VPN Router involves the following steps:

1. Attach the Multi-WAN VPN Router to a PC using any LAN port (5 to14) and configure it for your LAN.
2. Install your Multi-WAN VPN Router in your LAN and connect the Broadband Modem(s).
3. Configure your Multi-WAN VPN Router for Internet Access.
4. Configure PCs on your LAN to use the Multi-WAN VPN Router.

Requirements

¶ One (1) up to four (4) DSL or Cable modems, each with an ISP Internet Access account.

¶ Network cables. Use standard 10/100BaseT network (UTP) cables with RJ45 connectors

¶ TCP/IP network protocol must be installed on all PCs.

Procedure

1. Configuring the Router for your LAN

1. Use a standard LAN cable to connect your PC to any LAN port (5 -16) on the Multi-WAN VPN Router. (WAN ports from Port 1 ~ 4)
2. Connect the power cord into the power outlet on the rear panel of the Multi-WAN VPN Router.
3. Power-on your PC. If your PC is already running, restart it. It will then obtain an IP address from the Multi-WAN VPN Router.
4. Open your WEB browser.
5. In the *Address* or *Location* box enter:

   HTTP://192.168.1.1

6. You will be prompted for the User Name and password, as shown below:

Figure 2-1: Password Dialog

7. Enter *admin* for the "User Name" and leave the "Password" field blank.
   - ¶ The "User Name" is always set as *admin*
   - ¶ For security, it is highly recommended that you set a password. You may do this using the ***Admin Setup*** screen.
8. After logging in, you will see the ***Administrator Password*** setup in the ***Admin Setup*** screen, as shown below.
   Assign a password by entering it in the "Password" and "Verify P a s s w o r d" fields.

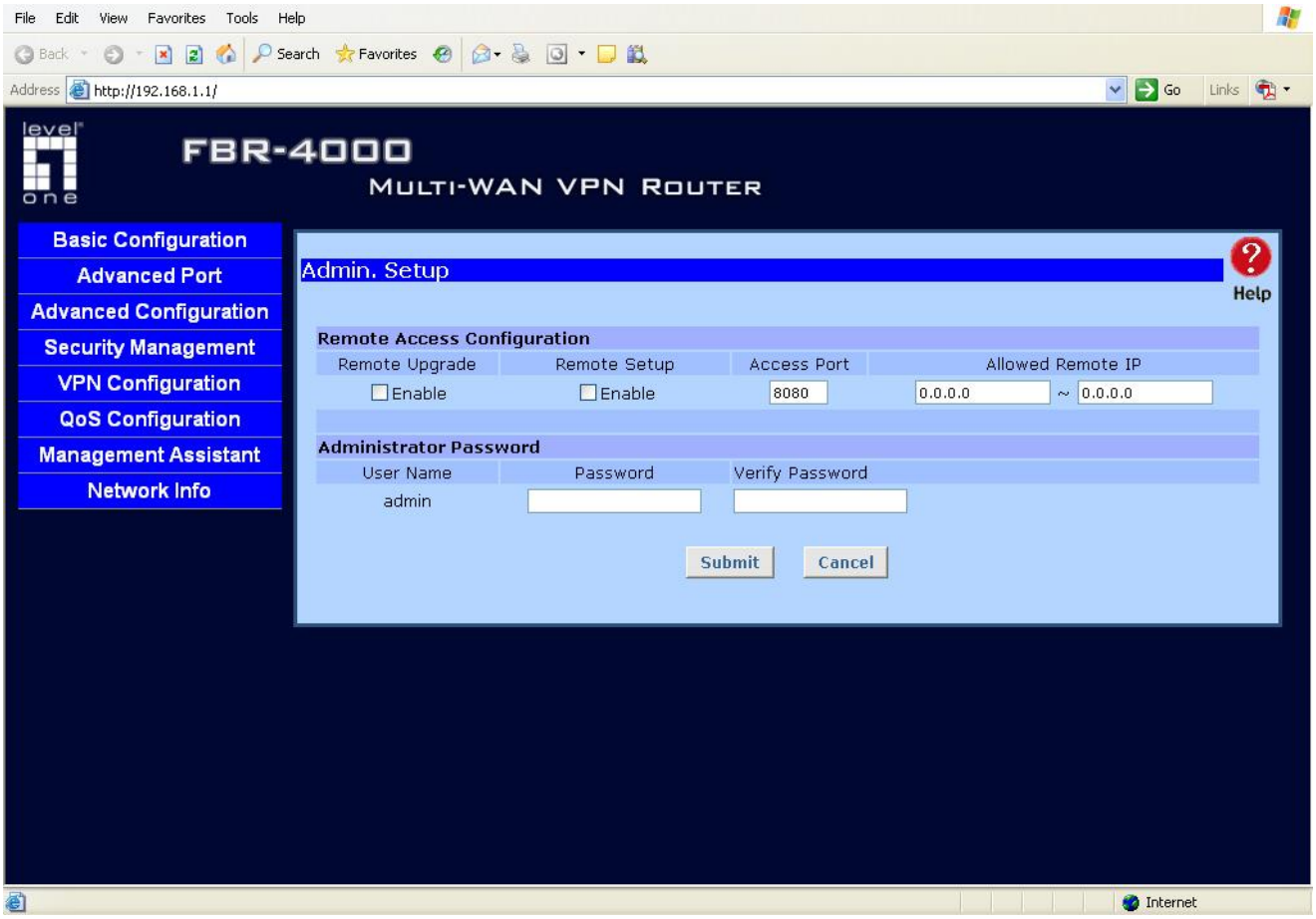


Figure 2-2: Home Screen (Admin. Setup)

9. Select ***LAN & DHCP*** from the menu. You will see a screen like in the example below.

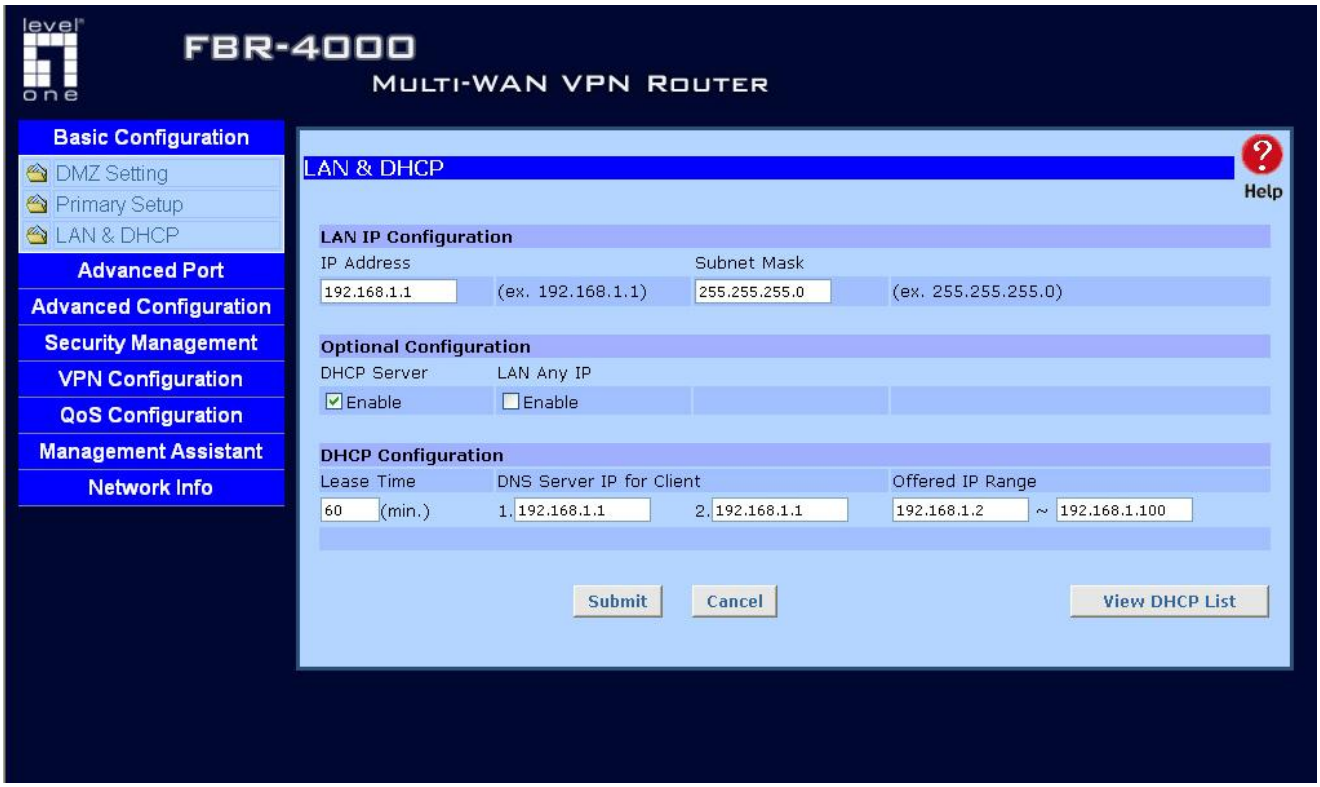


Figure 2-3: LAN & DHCP Setup

10. If your LAN already has a DHCP Server and you wish to continue using it, the following configuration is required:

    ¶ The DHCP Server function in the Multi-WAN VPN Router must be **disabled**. You will find this setting in the ***LAN & DHCP*** screen.

    ¶ Your DHCP Server must be configured to provide the Multi-WAN VPN Router's LAN IP Address as the "Default Gateway".

    ¶ Your DHCP Server must provide correct DNS addresses to any connected PCs.

11. Ensure these settings are suitable for your LAN:

    ¶ See the following table for details of each setting. For most situations, the default settings will be suitable.

Settings ï LAN & DHCP

LAN IP Configuration	¶ **IP Address** ï IP address for the Multi-WAN VPN Router, as seen from the Local LAN. Use the default value unless the address is already in use or your LAN is using a different IP Address range. ¶ **Subnet Mask** ï The default value 255.255.255.0 is standard for small (class "C") networks. For other networks, use the Subnet Mask for the LAN segment to which the Multi-WAN VPN Router is attached. (The same value as the PCs on that LAN segment.)
Optional Configuration	¶ **DHCP Server Setup** ï I f s *Enable* ò p Multi-W will assign IP Addresses to the PCs (DHCP clients) on your LAN when they start up. The default and recommended value is "**Enable**". (Windows systems, by default, act as DHCP clients. This setting in the Windows Internet Protocol (TCP/IP) Properties is: *Obtain an IP address automatically*.) ¶ **LAN Any IP** ï By default this option is disabled. I f y o u e n A n y I P ò , t h e n n o m a t t e r w h a t , t h client (your PC). The client does not need to change the IP address, even though it has a different IP segment than the LAN segment. It can still access the Internet through NAT.
DHCP Configuration	¶ **Lease Time** ï This is a finite period of time for a DHCP server to lease an IP address to a client. ¶ **DNS Server IP for Client** ï An IP address of the default DNS server for the client requesting DNS service. ¶ **Offered IP Range** ï The fields set the values used by the DHCP server when allocating IP addresses to DHCP clients. This range also determines the number of DHCP clients supported.
View DHCP List	This table shows the IP addresses which have been allocated by the DHCP Server. For each address which has been allocated, the following information is shown: ¶ **Free Entry** ï Indicates how many IP addresses the DHCP server can allocate to DHCP clients. ¶ **Name** ï The "hostname" of the PC. In some cases, this may not be known. ¶ **MAC Address** ï The physical address (network adapter address) of the PC. ¶ **IP Address** ï The IP address that is allocated to this PC. ¶ **Type** ï Indicates whether the IP address is to be dynamic or static. ¶ **Status** ï If *Dynamic*, the IP address was allocated by this DHCP Server. If *Sniffed*, the IP address was detected by examining the LAN rather than allocated by the DHCP Server. In this case, the *Name* is usually not known. ¶ **Time Left** ï The time expired since the IP address was leased.

12. Save your data, then go to *Step 2, Installing the Multi-WAN VPN Router in your LAN*.

2. Installing the Router in your LAN

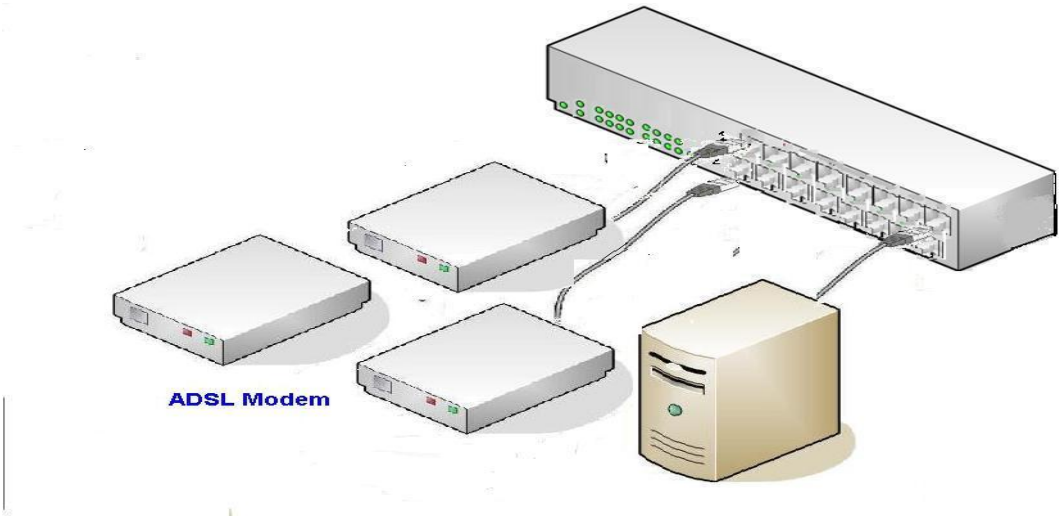


Figure 2-4: Installation Diagram

1. Ensure that the Multi-WAN VPN Router and any DSL/Cable modem(s) are powered-OFF. Leave the modem or modems connected to their data lines.
2. Connect the Broadband modem(s) to the Multi-WAN VPN Router.
   - ¶ If using only one (1) Broadband modem, connect it to port 1.
   - ¶ Use the cable supplied with your DSL/Cable modem. If no cable was supplied, use a standard cable.
3. Use standard LAN cables to connect PCs to the LAN ports on the Multi-WAN VPN Router.
   - ¶ Both 10BaseT and 100BaseT connections can be used simultaneously.
   - ¶ If you need to connect the Multi-WAN VPN Router to another Hub, just use a standard LAN cable to connect any LAN port on the Multi-WAN VPN Router to a standard port on another hub. Any LAN port on the Multi-WAN VPN Router will automatically act as an "Uplink" port when required.
   - ¶ If devices are connected to the 4 WAN ports (1,2,3 & 4), the remaining ports (5 ~ 16), are LAN ports. (You can enable Port 15 and Port 16 as dedicated DMZ ports)
4. Power-Up
   - ¶ Power-on the Cable or DSL modem(s).
   - ¶ Connect the supplied power cord to the Multi-WAN VPN Router and power-up.
5. Check the LEDs
   - ¶ The ***Power*** LED should be ON.
   - ¶ The ***Link/ACT*** LED should be ON if the corresponding WAN port is connected to a broadband modem.
   - ¶ For each PC connected to the LAN ports, the corresponding ***LAN*** LED (either ***10/Yellow*** or ***100/Green***) should be ON.

3. Configuring the Router for Internet Access

Select ***Primary Setup*** from the menu. You will see a screen like in the example below.

- Configure each WAN one by one through the **Interface** column pull-down menu.
- For any of the following situations, refer to ***Chapter 3: Advanced Port Setup,*** for any further configuration which may be required:
  - Using multiple WAN ports
  - Enabling multiple IP addresses on each WAN port
  - Enabling multiple PPPoE sessions
  - PPTP connection method

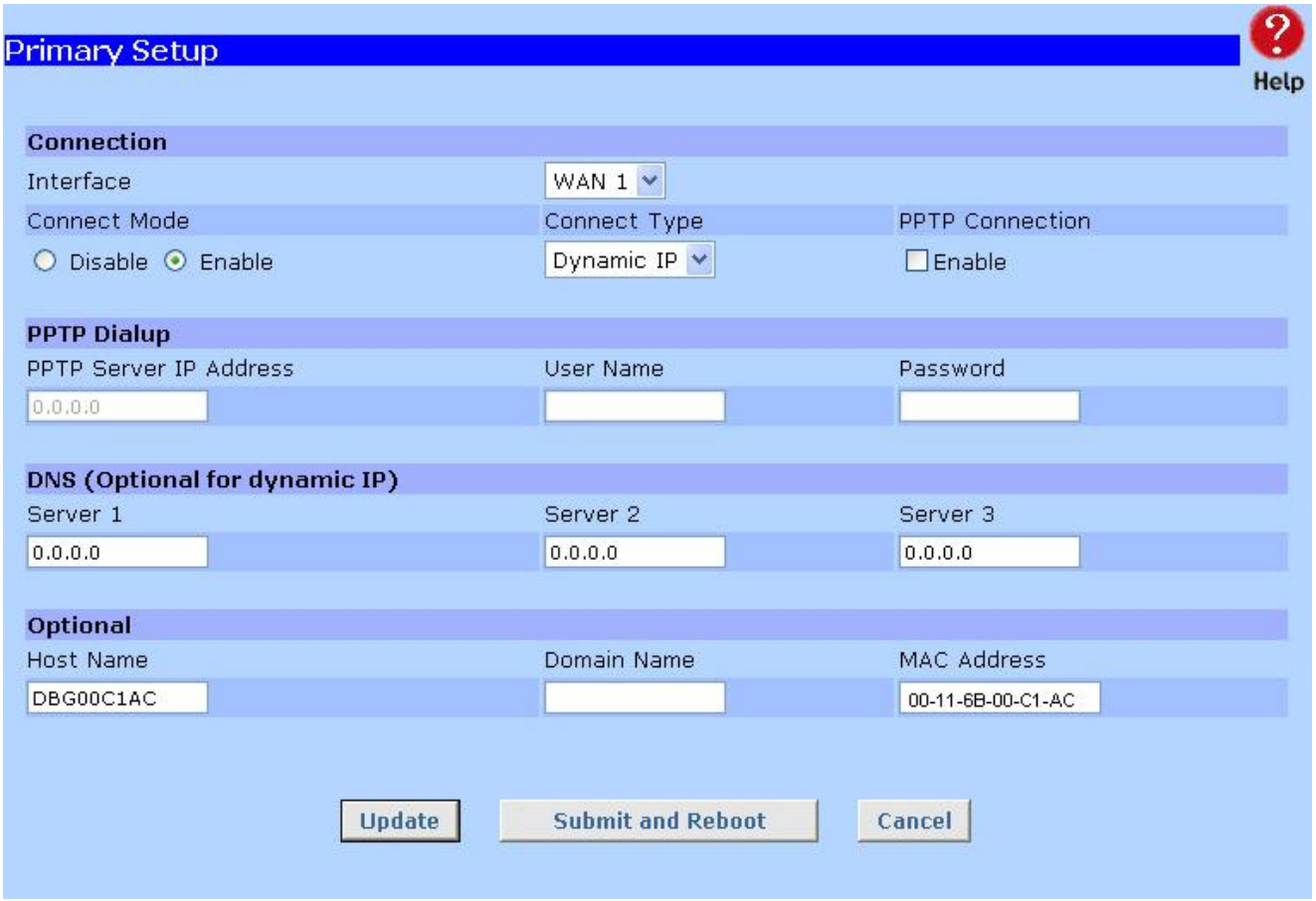


Figure 2-5: Primary Setup

Settings ï Primary Setup

Connection Mode	¶ **Interface** ï A pull down menu for each WAN port that you are going to connect to the Internet. ¶ **Connect Mode** ï **Enable** ï Select this if you have connected a broadband modem to this port. **Disable** ï Select this if there is no broadband modem connected to this port.
Connection Type	Check the data supplied by your ISP and select the appropriate option. ¶ **Static IP** ï Select this if your ISP has provided a Fixed or Static IP address. Enter the data into the *Address Info* fields. ¶ **Dynamic IP** ï Select this if your ISP provides an IP address automatically when you connect. You can ignore the *Address Info* fields. ¶ **PPPoE** ï Select this if your ISP uses this method. (Usually, your ISP will provide some PPPoE software; however, this software is not required and should not be used.) If this method is selected, you must complete the *PPPoE dialup* fields. **Note:** If using the PPTP connection method (enable **PPTP Connection**), select *Static IP* or *Dynamic IP* as appropriate, according to the IP Address method used by your ISP.
Address Information	This is for *Static IP* users only. Enter the address information (IP Address, Subnet Mask, Gateway) provided by your ISP. If your ISP provides multiple IP address, you can use the ***Multi-DMZ*** screen to assign any additional IP addresses.
PPPoE / PPTP Dialup	This is for ***PPPoE*** or ***PPTP*** users only. ¶ Enter the ***Username*** and ***Password*** provided by your ISP. ¶ If using PPTP, enable the ***PPTP Connection*** checkbox and enter the IP address of the PPTP server. ¶ **PPPoE Host name** (Optional) ï This field is used by a Host to uniquely associate an access concentrator with a particular Host request. **Note:** There are additional PPPoE/PPTP options on the ***Port Options*** screen. To use multiple PPPoE sessions on either port, configure settings in the ***Advanced PPPoE*** screen.
DNS	If using a *Fixed IP* address, you MUST enter at least 1 DNS address. If using a *Dynamic IP*, *PPPoE or PPTP*; DNS information is optional.

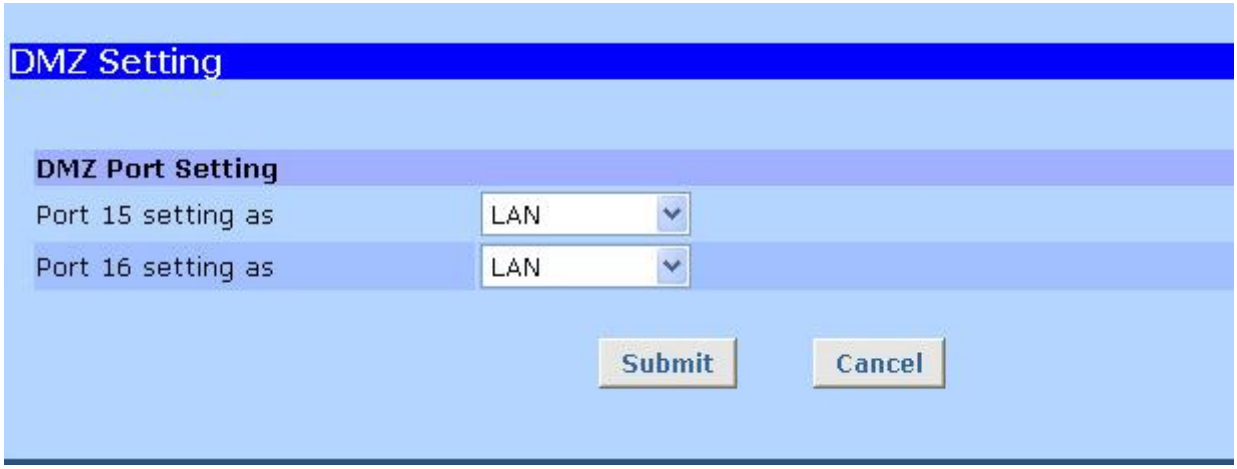
Optional	¶ **Host name** ï This is required by some ISPs. If your ISP provided a Host Name, enter it here. Otherwise, you can use the default value. ¶ **Domain name** ï This is required by some ISPs. If your ISP provided a Domain Name, enter it here. Otherwise, you can use the default value. ¶ **MAC address** ï Some ISP records your MAC address (also called "Physical address" or "Network Adapter address"). If so, you can enter the MAC address expected by your ISP in this field. Otherwise, this should be left at the default value.

Setup of the Multi-WAN VPN Router is now complete. PCs on your LAN must now be configured. See the following section for details.

4. Enable Dedicated DMZ Port

DMZs allow computers behind the firewall to initiate requests outbound to the DMZ. Computers in the DMZ in turn respond, forward or re-issue requests out to the Internet or other public network, as proxy servers do

Select ***DMZ Setting*** from the **Basic Configuration** menu. You will see a screen like in the example below.



¶ Set Port15 or Port16 as dedicated DMZ port by select corresponding WAN Ports

Note:

Select **LAN** for Port15 and Port16, these ports will be the same as other LAN ports on the Router

5. Configure PCs on your LAN

Overview

For each PC, the following settings may need to be configured:

¶ TCP/IP network settings

¶ Internet Access configuration

TCP/IP Settings

If using the default Multi-WAN VPN Router settings and the default Windows 95/98/ME/2000/XP TCP/IP settings, no changes need to be made. Just start (or restart) your PC.

¶ By default, the Multi-WAN VPN Router will act as a DHCP Server, automatically providing a suitable IP Address (and related information) to each PC when the PC boots.

¶ For all non-Server versions of Windows, the default TCP/IP setting is to act as a DHCP client. In Windows, this setting is: *Obtain an IP address automatically*.
Just start (or restart) your PC and it will automatically obtain an IP address from the Multi-WAN VPN Router.

¶ If using fixed IP addresses on your LAN, or if you wish to check your TCP/IP settings, refer to ***Appendix B ï Windows TCP/IP Setup***.

Internet Access

To configure your PCs to use the Multi-WAN VPN Router for Internet access, follow this procedure:

For Windows 9x/2000

1. Select *Start Menu - Settings - Control Panel - Internet Options*.
2. Select the *Connection* tab and then click the *Setup* button.
3. Select "I want to set up my Internet connection r
area network (LAN)" and click *Next*.
4. Select "I connect through a lNœcxatlò area network (L
5. Ensure that all of the boxes on the following *Local area network Internet Configuration* screen are **unchecked**.
6. Check the "No" option when prompted "Do you want to set up an Internet mail account now?"
7. Click *Finish* to close the Internet Connection Wizard.
Setup is now completed.

For Windows XP

1. Select *Start Menu - Control Panel - Network Connections.*
2. Select *Create a new connection*.
3. Click *Next* on the "New Connection Wizard" screen.
4. Select "*Connect to the Internet*" and *Nœlxitòk* ñ
5. Select "*Set up my connection manually*" and *Nœlxitòk* ñ
6. Check "**Connect using a broadband connection that is always on**" and click *Next*.

7. Click *Finish* to close the *New Connection Wizard.*
   Setup is now completed.

Accessing AOL

To access AOL (America On Line) through the Multi-WAN VPN Router, the *AOL for Windows* software must be configured to use TCP/IP network access rather than a dial-up connection. The configuration process is as follows:

- Start the *AOL for Windows* communication software. Ensure that it is Version 2.5, 3.0 or later. This procedure will not work with earlier versions.
- Click the *Setup* button.
- Select *Create Location* and change the location name from "New Locality" to " Multi-WAN VPN Router".
- Click *Edit Location*. Select *TCP/IP* for the *Network* field. (Leave the *Phone Number* field blank.)
- Click *Save*, then *OK*.
  Configuration is now complete.
- Before clicking "Sign On", always ensure that you are using the "Multi-WAN VPN Router" location.

Macintosh Clients

For Macintosh users, the procedure for accessing the Internet via the Multi-WAN VPN Router is as follows.

1. Open the TCP/IP Control Panel.
2. Select *Ethernet* from the *Connect via* pop-up menu.
3. Select *Using DHCP Server* from the *Configure* pop-up menu. The DHCP Client ID field can be left blank.
4. Close the TCP/IP panel, saving your settings.

Note:

If using manually assigned IP addresses instead of DHCP, the required changes are:

¶ Set the *Router Address* field to the Multi-WAN VPN Routerô IP Address.

¶ Ensure your *DNS* settings are correct.

Linux Clients

To access the Internet via the Multi-WAN VPN Router using Linux, it is only necessary to set the Multi-WAN VPN Router as the "Gateway" and ensure your *Name Server* settings are correct.

Ensure you are logged in as "root" before attempting any changes.

Fixed IP Address

By default, most Unix installations use a fixed IP Address. If you wish to continue using a fixed IP Address, make the following changes to your configuration.

¶ Set your *Default Gateway* to the IP Address of the Multi-WAN VPN Router.

¶ Ensure your *DNS* (Name server) settings are correct.

To act as a DHCP Client (recommended)

The procedure below may vary depending on your version of Linux and X -windows shell.

1. Start your X Windows client.
2. Select *Control Panel - Network*
3. Select the "Interface" entry for your Network card. Normally this will be called "eth0".
4. Click the *Edit* button, set the "protocol" to "DHCP" and save this data.
5. To apply your changes, use the "Deactivate" and "Activate" buttons if available. Otherwise, restart your system.

3: Advanced Port

Overview

- ***Port Options*** contains some options which can be set on any WAN port. For most situations, the default values are satisfactory.
- ***Load Balance*** is only functional if you are using multiple WAN ports. It allows you to determine the proportion of WAN traffic sent through each port.
- ***Advanced PPPoE*** setup is required if you wish to use multiple sessions on each WAN port. It can also be used to manually connect or disconnect a PPPoE session. Otherwise, this screen can be ignored.
- ***Advanced PPTP*** setup is required if using the PPTP connection method.

Port Options

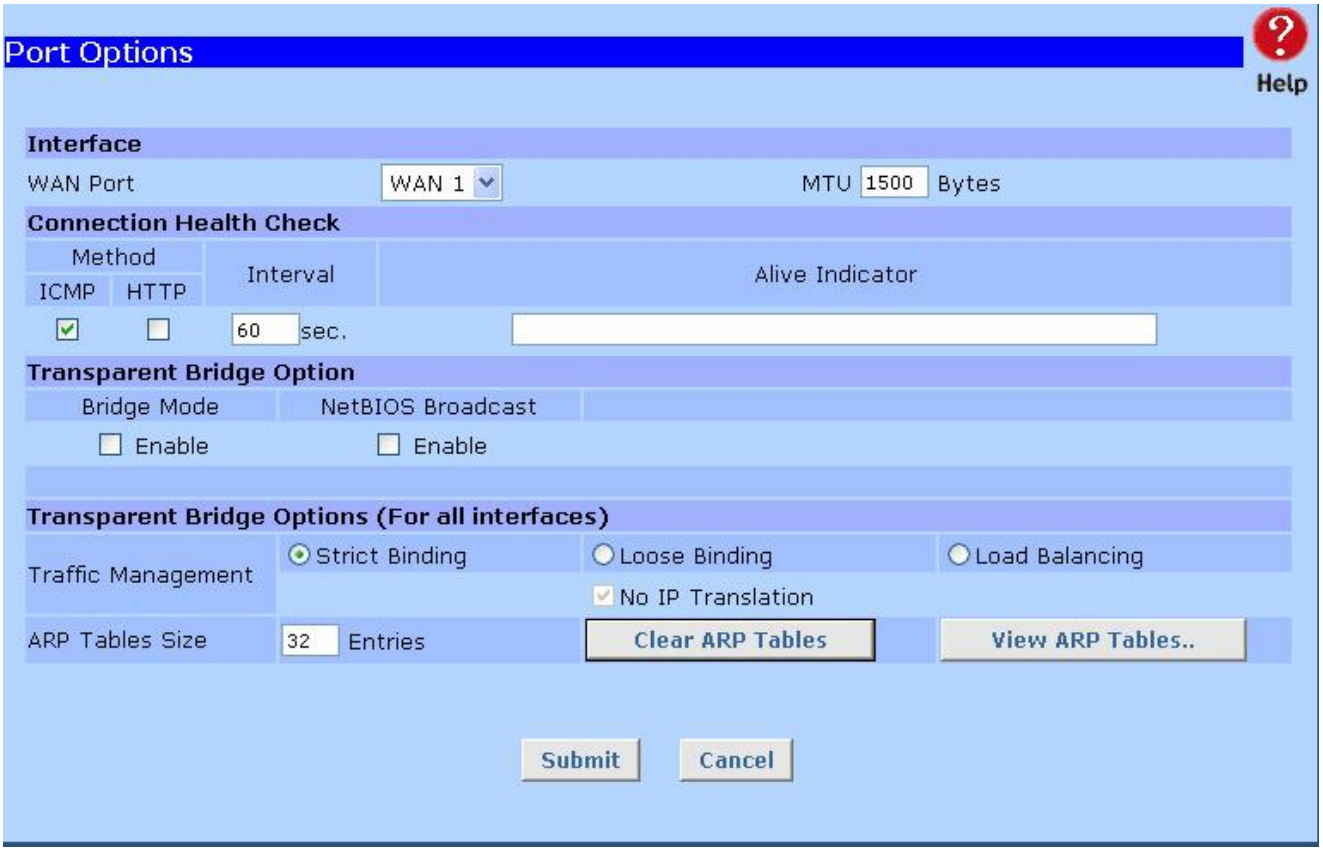


Figure 3-1: Port Options

Settings ï Port Options

Interface	¶ **WAN Port** ï Select a particular WAN port from the pull-down menu to setup WAN port configuration. ¶ **MTU** ï The Maximum Transmission Unit for the Ethernet data. This is used to determine the packet size to be used on the WAN interface. Normally, this does not need to be changed but if your ISP advises you to use a particular MTU, enter it here. The default MTU value is 1500 Bytes.
Connection Health Check	¶ **Method** ï There are three methods available for checking if a WAN port is alive or not**.** Multiple choices can be selected when using it. ¶ *Disable* will not perform an Alive Indicator Check. By default, Health Check is set to *Enable*. If the ñAlive Indic Health Check performs an ICMP echo packet request to the specific destination. This could be either a URL or an IP Address specified by users inndtihceatñoArlòi vien put box gateway. ¶ **Interval** ï The interval time for device health check. The default interval time is 60 seconds. ¶ **Alive Indicator** ï This is the IP address used to check if the WAN connection is operating. The Multi-WAN VPN Router will contact this system to check if the WAN connection is working or not. You may change this address if you wish. Default is the gateway IP. **Note**: This is not used for PPPoE connections.
Transparent Bridge Option	¶ **Bridge Mode** ï If set to *Enable*, this WAN port doesnô Load Balance function when the LAN/WAN IP have the real IP addresses on the same network segment. ¶ **NetBIOS Broadcast** ï If you enable the NetBIOS Broadcast, this will allow you to access files through the Microsoft network neighborhood.
Transparent Bridge Options (For all interfaces)	¶ **Traffic Management** ï **Strict Binding:** Traffic from bridge hosts (eg. transparent to WAN1) can only go through the specified WAN interface (eg. WAN1). **Loose Binding:** This acts as a failover mechanism for transparent bridge mode. Traffic from bridge hosts (eg. transparent to WAN1) can go through any WAN interface (eg. WAN2 or other) when bind interface (eg. WAN1) is down. **Load Balancing:** This acts as a load balancing mechanism for transparent bridge mode. Traffic from bridge hosts (eg. transparent to WAN1) can go through any WAN interface (eg. WAN1, 2 or other) based on the loading mechanism specified in the load balance section. ¶ **ARP Table** ï The ARP Table is used by the device to determine the bridge hosts ô location (e.g. insi WAN). Its size can be adjusted if needed. **View ARP Tables** displays ON/OFF selection of bridge mode on each WAN port. **Clear ARP Tables** disables bridge mode on all WAN ports.

Load Balance

This screen is only operational if using Internet connections on multiple WAN ports

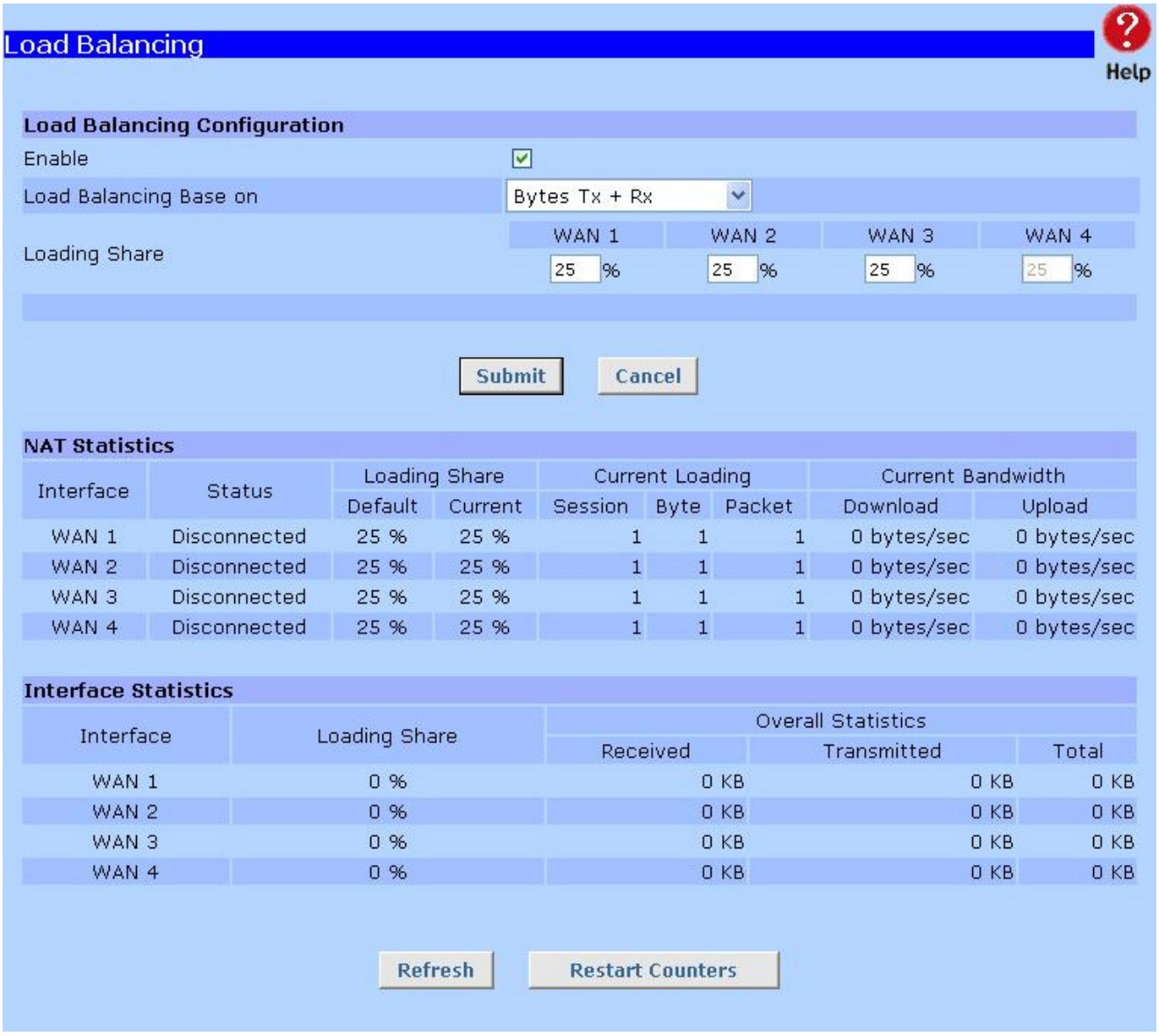


Figure 3-2: Load Balance

Only functional when using two (2) or more WAN ports - these settings determine the proportion of traffic sent over each port.

Settings ï Load Balance

Load Balance Configuration	¶ **Enable** ï This enables your Load Balance setting options and must be checked for other settings on this screen to be effective. ¶ **Balance Type** ï You can select the Balance types based on: ¶ Bytes Tx + Rx ï Traffic is measured by Bytes. (Least load) ¶ Packets Tx + Rx ï Traffic is measured by Packets. (Least load) ¶ Sessions established ï Traffic is measured by Sessions. (Least load) ¶ IP Address ï Traffic is measured by IP address. (Least load) ¶ Auto Learning ï The largest unused upload/outgoing bandwidth. ¶ Fastest ï The largest upload bandwidth. ¶ Priority ï The highest priority**.** ¶ Round Robin ï Continuously repeating sequence. ¶ Weight Round Robin ï In sequence with weight placed accordingly. ¶ **Loading Share** ï Enter the percentage (%) of traffic to be sent over each WAN port. If one WAN port connection has a greater bandwidth than another, the one with the greater bandwidth is given a higher percentage of traffic than the other. Click the "submit" button to save your changes.
NAT Statistics	This section displays the current data about any WAN port. You can use this information to help you "fine-tune" the settings above.
Interface Statistics	This section displays cumulative statistics. Use the "Restart Counters" button to restart the counters when required.
Buttons	¶ **Refresh** ï Update the data entered on the screen. ¶ **Restart Counters** ï Restart the counters used in the "Interface Statistics" section.

Advanced PPPoE

The Advanced PPPoE screen is required in order to use multiple PPPoE sessions on the same WAN port.

It can also be used to manually connect or disconnect a PPPoE session.

Figure 3-3: Advanced PPPoE

Settings ï Advanced PPPoE

Select WAN Port & Session	**WAN Port** ï Selected WAN port only using PPPoE connection **PPPoE Session** ï ISPs can usually provide multiple floating real IPs for PPPoE. Each WAN port can have up to eight (8) PPPoE sessions, each with a different IP address if your WAN port is using PPPoE connectivity. **PPPoE Session MTU** ï The Maximum Transfer Unit for PPPoE packet data. Leave it as default unless the ISP provides a different PPPoE packet data size. The default MTU value is 1492 bytes.
WAN IP Account	¶ **User Name** ï Enter the PPPoE user name assigned by your ISP. ¶ **Password** ï Enter the PPPoE password assigned by your ISP. ¶ **Verify Password** ï Re-enter the PPPoE password assigned by your ISP.
Options	¶ **Specified Fix IP Address** ï If you have a fixed IP address, enter if here. Otherwise, this field should be left at 0.0.0.0. ¶ **Assigned Host Name** ï This field is used by a Host to uniquely associate an access concentrator with a particular Host request.
PPPoE Auto Dialup	¶ **Auto Dialup** (connect-on-demand) ï If set to *Enable,* a connection will be established whenever outgoing WAN traffic is detected. If not enabled, you must establish a connection manually. ¶ **Disconnect after Idle** ï This determines when an idle connection will be terminated. Enter the required time period. (-1**:** Always on) ¶ **Echo Time** ï This determines how often an Echo request is sent to the PPPoE server. The Echo request is used to determine if the connection is still alive. Normally, there is no need to change the default value. ¶ **Echo Retry** ï The number of times the Echo request will be sent, if there is no response to the first request. Normally, there is no need to change the default value.
Connection Status	This displays the current connection status for each session.

Advanced PPTP

This Advanced PPTP screen is only useful if using the PPTP connection method.

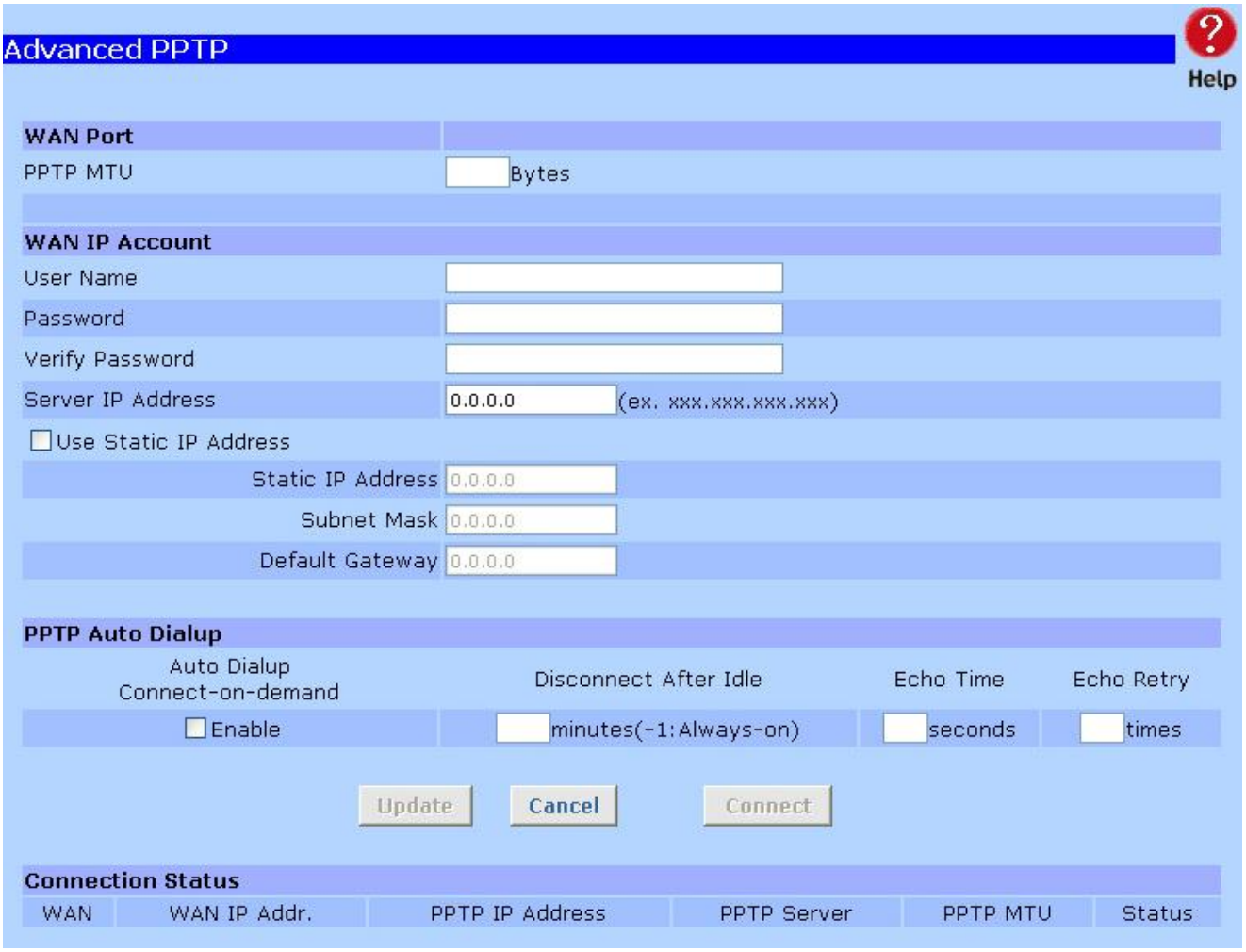


Figure 3-4: Advanced PPTP

Settings ï Advanced PPTP

WAN Port	Select the desired WAN port (click desired WAN on Connection Status). The data of the selected port will then be displayed in the *WAN IP Account* section. **PPTP MTU** ï Maximum transfer unit for PPTP. The default value is 1460
WAN IP Account	¶ **User Name** ï The PPTP user name (login name) assigned by your ISP. ¶ **Password** ï The PPTP password associated with the *User Name* above. This is assigned by your ISP, and used to login to the PPTP Server. ¶ **Verify Password** ï Re-enter the PPTP password assigned by your ISP. ¶ **Server IP Address** ï Enter the IP address of the PPTP Server, as provided by your ISP. ¶ **Static IP Address** ï If you have a fixed IP address, enter if here. Otherwise, this field should be left at 0.0.0.0.
PPTP Auto Dialup	¶ **Auto Dialup** (connect-on-demand**)** ï If set to *Enable,* a connection will be established whenever outgoing WAN traffic is detected. If not enabled, you must establish a connection manually. ¶ **Disconnect after Idle** ï This determines when an idle connection will be terminated. Enter the required time period. (-1**:** Always on) ¶ **Echo Time** ï This determines how often an Echo request is sent to the PPTP server. The Echo request is used to determine if the connection is still alive. Normally, there is no need to change the default value. ¶ **Echo Retry** ï The number of times the Echo request will be sent, if there is no response to the first request. Normally, there is no need to change the default value.
Connection Status	This displays the current PPTP connection status.

4: Advanced Setup

Overview

The following features are provided in Advanced Setup:

- Host IP
- Routing
- Virtual Server
- Special Application
- Dynamic DNS
- Multi DMZ
- UPnP Setup
- NAT Setup
- Advanced Feature

This chapter contains details on the configuration and use of each of these features.

Host IP

This feature is used in the following situations:

¶ You have Multi-Session PPPoE and wish to bind each session to a particular PC on your LAN.

¶ You wish to use the ***Access Filter*** feature. This requires that each PC is identified by using the ***Host IP*** screen.

¶ You wish to have different ***Block URL*** settings for different PCs. This requires that each PC is identified by using the ***Host IP*** screen. (You do not have to use the Host IP feature to apply the same ***Block URL*** settings to all PCs.)

¶ You wish to reserve a particular (LAN) IP address for a particular PC on your LAN. This allows the PC to use DHCP (In Windows this setting is configured as: "*Obtain an IP address automatically*") while gaining the benefits of a fixed IP address. The PC's IP address will never change, allowing it to be provided to other users and applications.

Figure 4-1: Host IP

Settings ï Host IP

Host Network Identity	This section identifies each Host (PC) ¶ **Host name** ï Enter a suitable name. Generally, you should use the "Hostname" (computer name) as defined on the Host itself. ¶ **MAC Address** ï Also called *Physical Address* or *Network Adapter Address*. Enter the MAC address of this Host. ¶ **Select Group** ï Select the group you wish this Host to be included in. ¶ **Reserve in DHCP** ï Select *Enable* to reserve a particular (LAN) IP address for a particular PC on your LAN. This allows the PC to use DHCP (In Windows this setting is configured as: "Obtain an IP address automatically") while retaining an IP address that never changes. ¶ **Reserved IP Address** ï Enter the IP address you wish to reserve, if the setting above (Reserve in DHCP) is set to *Enable*. Otherwise, ignore this field.
Host Network Binding	¶ **Binding WAN Port / Session** ï Select *Enable* if you wish to associate this PC with a particular PPPoE session. All traffic for that PC will then use the selected PPPoE port and session. ¶ **Binding Method** ï Suppose your PC is bound to WAN1 port and you select ñStrict Binding.ò If WAN1 port is through another WAN port, if it is still alive. If you select ñLoose Bindingò if WAN1 port becomes disconnected, your packets will automatically go to another WAN port, if it is alive. ¶ **Select WAN Port / Select PPPoE session** ï If the Binding Method setting above is set to *Enable*, select the desired Port and Session. Otherwise, ignore these settings. **Note**: Multiple PPPoE sessions are defined on the ***Advanced PPPoE*** screen.
Buttons	¶ **Add** ï Use this to add a new entry to the database, using the data shown on screen. ¶ **Delete** ï Click this to delete the selected entry. ¶ **Update** ï After making the desired changes, use this to update the selected entry ¶ **Reset** ï Reverse any changes you have made since loading the data from the Multi-WAN VPN Router.
Host & Group List	This table shows the current bindings.

Routing

This section is only relevant if your LAN has other Routers or Gateways.

- If you don't have other Routers or Gateways on your LAN, you can ignore the ***Static Routing*** page completely.
- If your LAN has other Gateways and Routers, you must configure the Static Routing screen as described below. You also need to configure the other Routers.

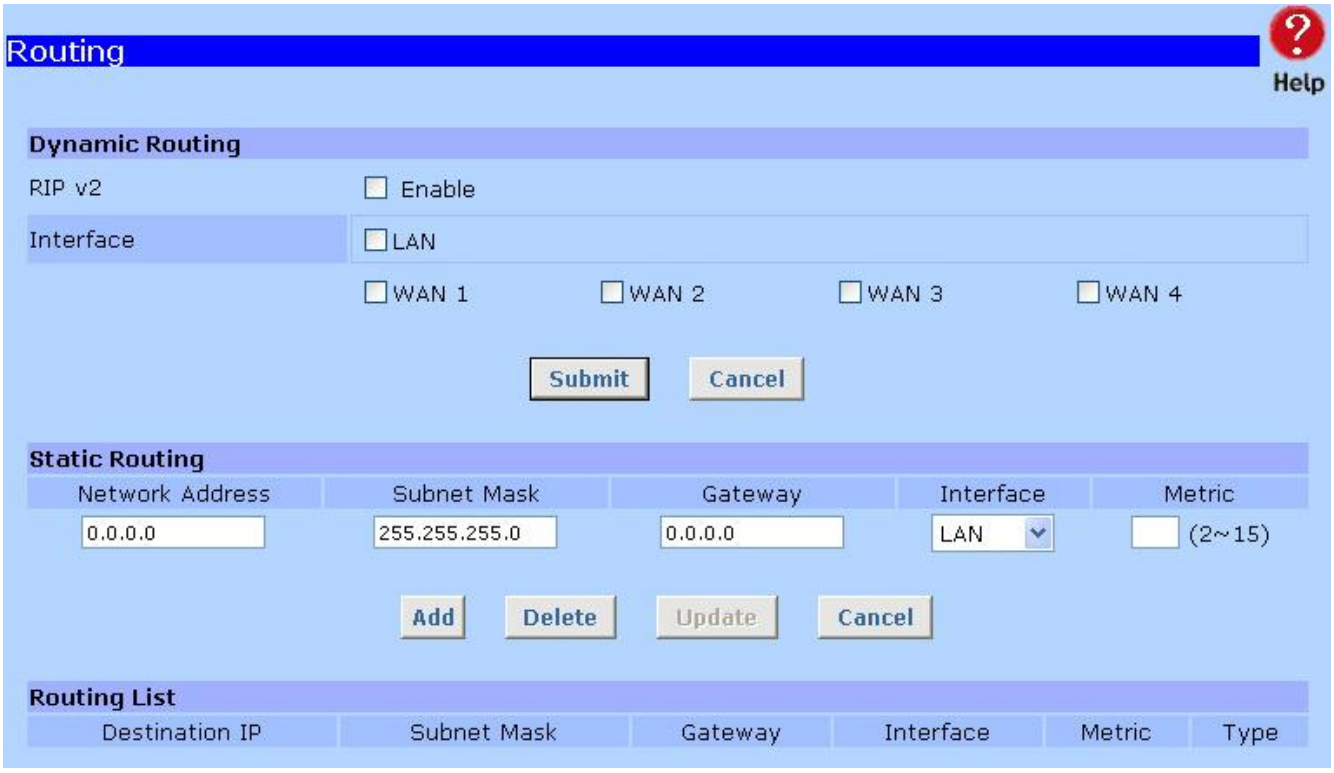


Figure 4-2: Routing

Note:

If there is an entry or entries in the Routing table with an Index of zero (0), these are System entries. You cannot modify or delete these entries.

Settings ï Routing

Dynamic Routing	¶ **RIP v2** ï This acts as a If enabled, the selected WAN or LAN. will run RIPv1/v2, otherwise RIP function will not be available. ¶ **Interface** ï If LAN or other WAN are enabled, the specified WAN or LAN can execute RIP function.

Static Routing	¶ **Network Address** ï The network address of the remote LAN segment. For standard class "C" LANs, the network address is the first 3 fields of the Destination IP Address. The 4th (last) field can be left at 0. ¶ **Netmask** ï The Network Mask for the remote LAN segment. For class "C" networks, the default mask is 255.255.255.0 ¶ **Gateway** ï The IP Address of the Gateway or Router that the Multi-WAN VPN Router must use to communicate with the destination IP address entered above. (NOT the router attached to the remote segment.) ¶ **Interface** ï Select the correct interface - usually "LAN". The "WAN" interface is only available if NAT (Network Address Translation) is disabled. ¶ **Metric** ï The number of "hops" (routers) to pass through to reach the remote LAN segment. The shortest path will be used.
Routing List	This shows the current routing table set by the user.

Configuring Other Routers on your LAN

All traffic for devices not on the local LAN must be forwarded to the Multi-WAN VPN Router so that it can be forwarded to the Internet. This is done by configuring other Routers to use the Multi-WAN VPN Router as the *Default Route* or *Default Gateway*, as illustrated by the example below.

Static Routing - Example

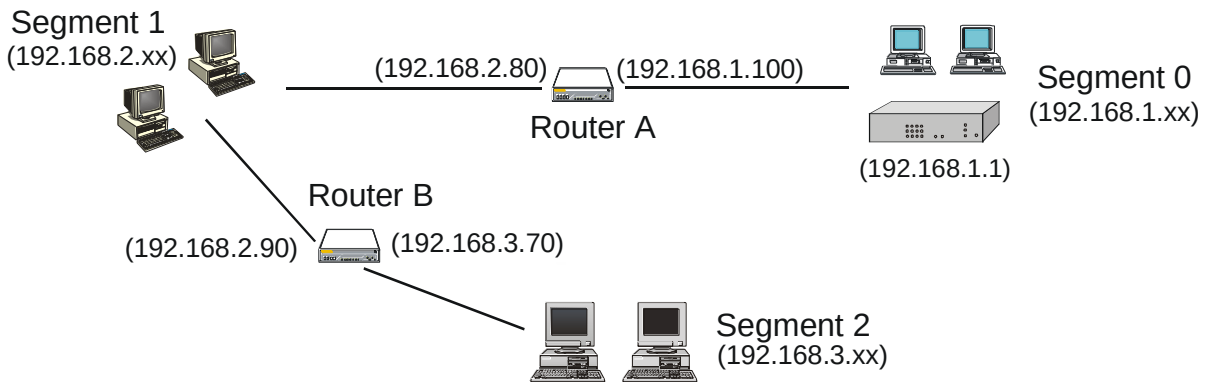


Figure 4-3: Routing Example

For the Multi-WAN VPN Router Gateway's Routing Table

For the LAN shown above, with 2 routers and 3 LAN segments - the Multi-WAN VPN Router requires 2 entries as follows:

Entry 1 (Segment 1)	
Destination IP Address	192.168.2.0
Network Mask	255.255.255.0
Gateway IP Address	192.168.1.100
Interface	LAN
Metric	2
Entry 2 (Segment 2)	
Destination IP Address	192.168.3.0
Network Mask	255.255.255.0 (Standard Class C)
Gateway IP Address	192.168.1.100
Interface	LAN
Metric	3

For Router A's Default Route

Destination IP Address	0.0.0.0
Network Mask	0.0.0.0
Gateway IP Address	192.168.1.1
Metric	2

For Router B's Default Route

Destination IP Address	0.0.0.0
Network Mask	0.0.0.0
Gateway IP Address	192.168.2.80
Interface	LAN
Metric	3

Virtual Server

This feature allows you to make Servers on your LAN accessible to Internet users. Normally, Internet users would not be able to access a server on your LAN because:

¶ Your Server's IP address is only valid on your LAN, not on the Internet.

¶ Attempts to connect to devices on your LAN are blocked by the firewall in the Multi-WAN VPN Router.

The "Virtual Server" feature solves these problems and allows Internet users to connect to your servers, as illustrated below.

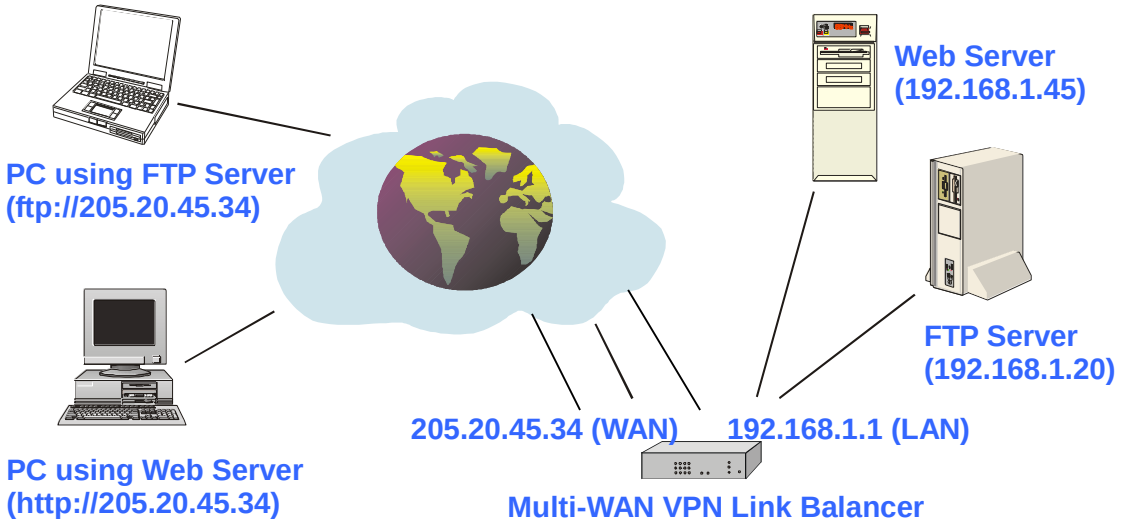


Figure 4-4: Virtual Server

Note that, in this illustration, both Internet users are connecting to the same IP Address but using different protocols.

Connecting to the Virtual Server

Once configured, anyone on the Internet can connect to your Virtual Servers. They must use the Multi-WAN VPN Router's Internet IP Address (the IP Address allocated by your ISP).
e.g.

http://205.20.45.34

ftp://205.20.45.34

¶ To Internet users, all virtual Servers on your LAN have the same IP Address. This IP Address is allocated by your ISP.

¶ This address should be static, rather than dynamic, to make it easier for Internet users to connect to your Servers. However, you can use the *Dynamic DNS* feature (explained later in this chapter) to allow users to connect to your Virtual Servers using a URL, instead of an IP Address.
e.g.

http://my_domain_name.dyndns.org
ftp://my_domain_name.dyndns.org

This screen allows you to define your own Server types.

Figure 4-5: Virtual Server

Settings ï Virtual Server

Virtual Server Configuration	¶ **Enable** ï The enable checkbox is to Enable or Disable each Virtual server as required. ¶ **Server Name** ï Enter a suitable name for this server. (By default, 12 well-known virtual servers have been listed on the Custom Virtual Server List) ¶ **Protocol** ï Select the network protocol (TCP/UDP) used by this sever. ¶ **IP Address** ï **LAN**, Enter the IP address of the server on your LAN which is running the required Server software. Each Host (server) should have a fixed IP address, or have a reserved IP address. (See the ***Host IP*** section earlier in this Chapter for details on reserving an IP address.) Each Host (server) must be running the appropriate Server software **WAN** ï This selection allows this server to bind to any WAN port (1-4), or even bind to all WAN ports together. ¶ **LAN Port Range** ï Enter the range of port number used for outgoing traffic from this Server. If only a single port is required, enter it in both fields. ¶ **WAN Port Range** -ï Enter the range of port numbers used for incoming traffic to this Server. If only a single port is required, enter it in both fields ¶ **Allowed Remote IP** ï It allows only a range of remote side IP addresses to access the virtual servers. The default entry 0.0.0.0 ~ 0.0.0.0, means all remote side IP address can access it.
Buttons	¶ **Add** ï Create a new Virtual Server entry. ¶ **Delete** ï Delete the selected entry. ¶ **Update** ï Save any changes you have made to the current entry. ¶ **Cancel** ï Cancel any changes you have made since the last saved operation.
Virtual Server List	This table shows the details of all Custom Virtual Servers configuration data which have been defined. You can modify their configuration data by selecting and clicking on a row.

Special Application

If you use Internet applications which have non-standard connections or port numbers, you may find that they do not function correctly because they are blocked by the firewall in the Multi-WAN VPN Router. In this case, you can define the application as a "Special Application" in order to make it work.

Note that the terms "Incoming" and "Outgoing" on this screen refer to traffic from the client (PC) viewpoint

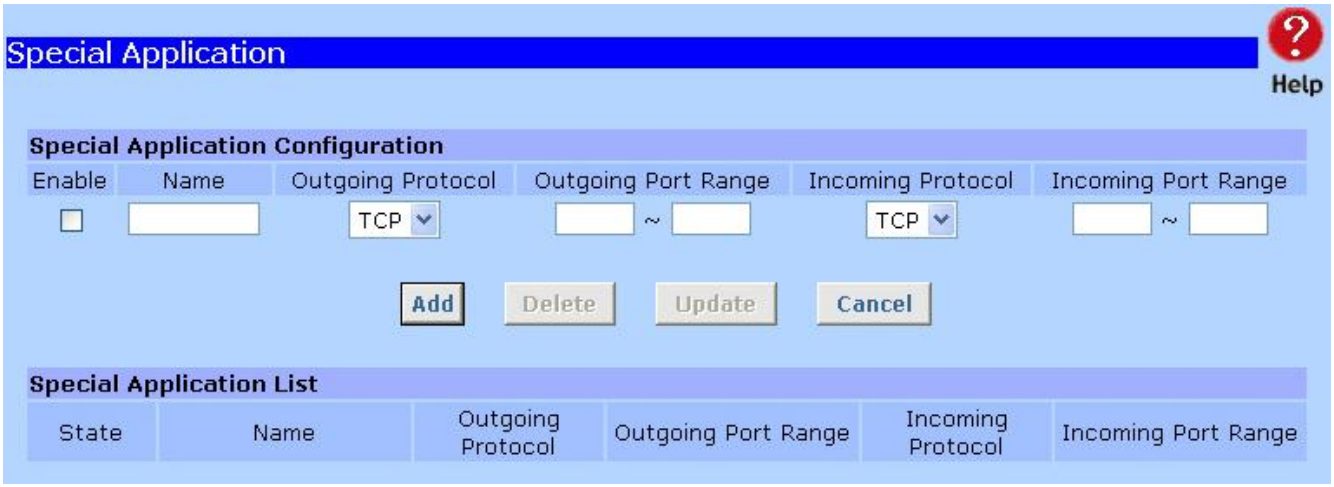


Figure 4-6: Special Application

Settings ï Special Application

Special Application Configuration	¶ **Enable** ï Use this to Enable or Disable the Special Application as required ¶ **Name** ï Enter a descriptive name to identify the Special Application. ¶ **Outgoing Protocol** ï Select the protocol used by the application when sending data to the remote server or PC. ¶ **Outgoing Port Range** ï Enter the beginning and end of the range of port numbers used by the application server for data you send. If the application uses a single port number, enter it in both fields. ¶ **Incoming Protocol** ï Select the protocol used by the application when receiving data from the remote server or PC. ¶ **Incoming Port Range** ï Enter the beginning and end of the range of port numbers used by the application server for data you receive. If the application uses a single port number, enter it in both fields.

Buttons	¶ **Add** ï Create a new Special Application entry. ¶ **Delete** ï Delete the selected entry. ¶ **Update** ï Save any changes you have made to the current entry. ¶ **Cancel** ï Cancel any changes you have made since the last saved operation.
Special Application List	This shows the details of all Special Applications which are currently defined. You can modify its configuration data by selecting and clicking on a row.

Using a Special Application on your PC

¶ Once the *Special Applications* screen is configured correctly, you can use the application on your PC normally. Remember that only one (1) PC can use each Special application at any time.

¶ Also, when 1 PC is finished using a particular Special Application, there may need to be a "Time-out" period before another PC can use the same Special Application.

¶ If an application still cannot function correctly, try using the "DMZ" feature, if possible.

Dynamic DNS

Dynamic DNS is very useful when combined with the *Virtual Server* feature. It allows Internet users to connect to your Virtual Servers using a URL, rather than an IP Address.

This also solves the problem of having a dynamic IP address. With a dynamic IP address, your IP address may change each time you connect to your ISP, making it difficult to connect to you.

You must register for the Dynamic DNS service. The Multi-WAN VPN Router supports 3 types of service providers:

¶ Standard client, available at http://www.dyndns.org
(Other sites may offer the same service, but can not be guaranteed to work)

¶ TZO at http://www.tzo.com

¶ 3322 is available in China at http://www.3322.org

To use the Dynamic DNS feature

1. Register for the service from your preferred service provider.
2. Follow the service provider's procedure to have a Domain Name (Host name) allocated to you.
3. Configure the ***Dynamic DNS*** screen, as described below.
4. The Multi-WAN VPN Router will then automatically update your IP Address recorded by the Dynamic DNS service provider.
5. From the Internet, users will now be able to connect to your Virtual Servers (or DMZ PC) using your Domain name.

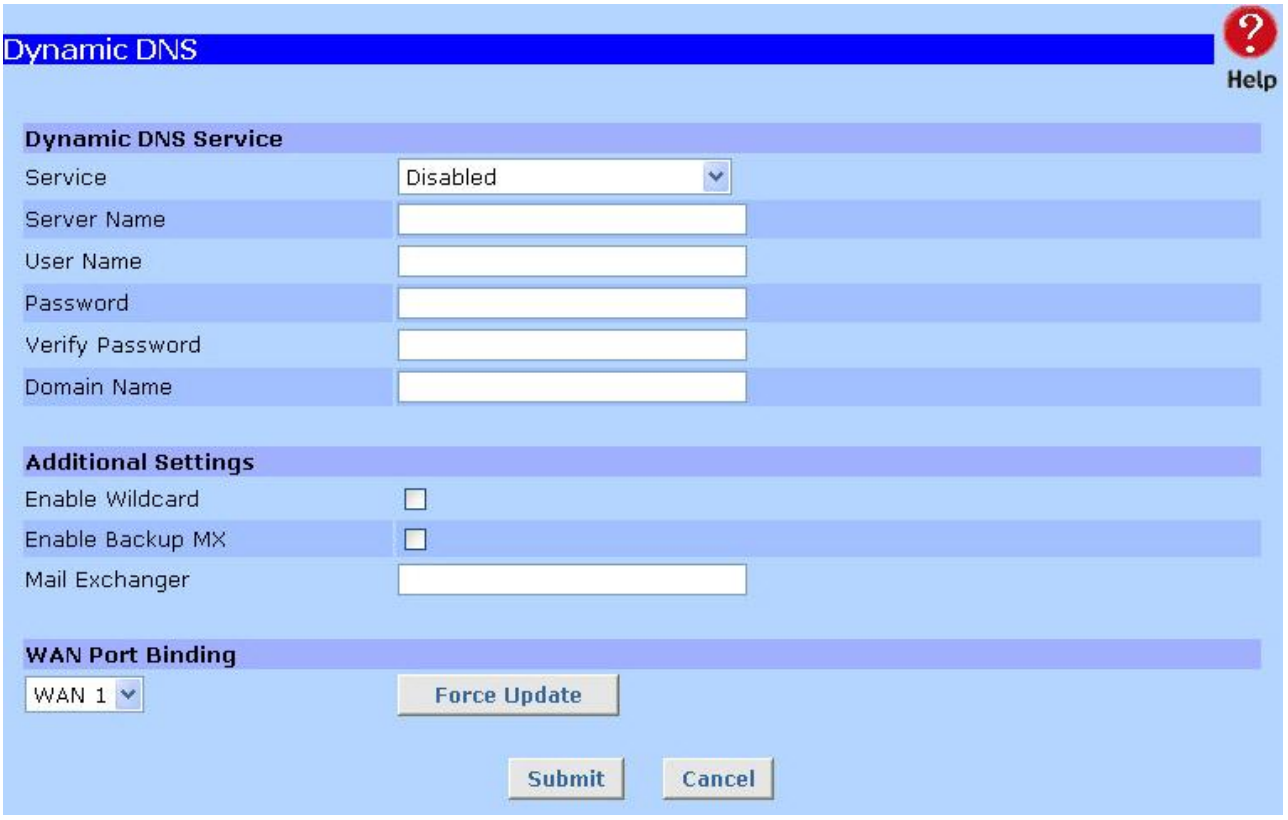


Figure 4-7: Dynamic DNS

Settings ï Dynamic DNS

Dynamic DNS Service	This pull-down menu can Enable/Disable the Dynamic DNS feature and select the required service provider. ¶ **Disable** ï Dynamic DNS is not used. ¶ **TZO** ï Select this to use the TZO service (www.tzo.com). You must configure the *TZO* section of this screen. ¶ **DynDNS** ï Select this to use the standard service (from www.dyndns.org or other provider). You must configure the *Standard Client* section of this screen. ¶ **3322(in China)** ï This is available in China ¶ **User Defined DDNS Server** ï This is the user defined DDNS server. If the DDNS provider is other than TZO, dyndns.org or 3322.
Additional Settings	These options are available if using the standard client. ¶ **Enable Wildcard** ï If selected, traffic sent to sub-domains (of your Domain name) will also be forwarded to you. ¶ **Enable backup MX** ï If enabled, you must enter the *Mail Exchanger* address below. ¶ **Mail Exchanger** ï If the setting above is enabled, enter the address of the backup Mail Exchanger.
WAN Port Binding	¶ Select the WAN port used by the Dynamic DNS. ¶ The "Force Update" button will update your record on the Dynamic DNS Server immediately.

Multi DMZ

This feature allows each WAN port IP address to be associated with one (1) computer on your LAN. All outgoing traffic from that PC will be associated with that WAN port IP address. Any traffic sent to that IP address will be forwarded to the specified PC, allowing unrestricted 2-way communication between the "DMZ PC" and other Internet users or Servers.

Note:

The "DMZ PC" is effectively outside the Firewall, making it more vulnerable to hacker attacks or other intrusions. For this reason, you should only enable the DMZ feature when required.

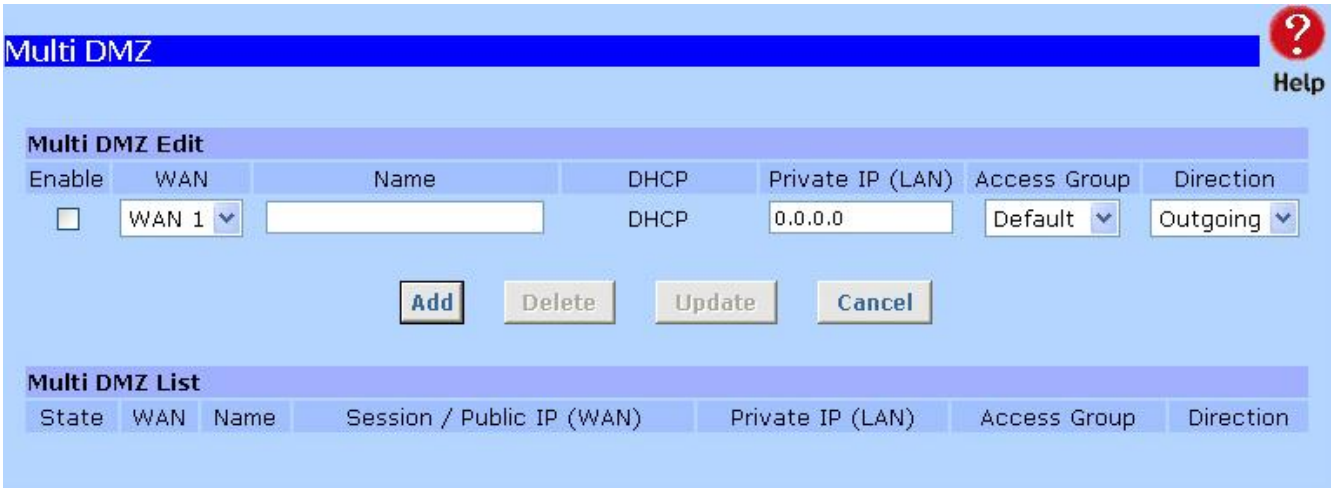


Figure 4-8: Multi DMZ

Settings ï Multi DMZ

Multi DMZ Edit	¶ **Enable** ï Use this to enable or disable the DMZ setting, as required. ¶ **WAN** ï Select the desired WAN port binding with a particular LAN host. (There are a maximum 4 WAN ports which can be available.) Its connection type may change based on your WAN connection type (Static/DHCP/PPPoE/PPTP). ¶ **Name** ï Enter a name to assist you to remember this setting. This name can be anything you choose and will have no effect on the operation. ¶ **Private IP Address (LAN)** ï Enter the IP address of the PC you wish to associate with this WAN port IP address. This IP address should be fixed, or reserved. (See the ***Host IP*** section for details on reserving an IP address.) ¶ **Access Group** ï You can decide which users will have authorization to use DMZ by defining the groups (Host IP web page) ¶ **Direction** ï For DMZ, you can allow inbound only, outbound only, or both inbound and outbound traffic.
Multi DMZ List	Multi DMZ List shows the details of all DMZ configuration data which are currently defined. You can modify its configuration data by selecting and clicking on a row.

UPnP Setup

With the UPnP (Universal Plug & Play) function, you can easily setup and configure an entire network as well as enable detection and control of networked devices and services.

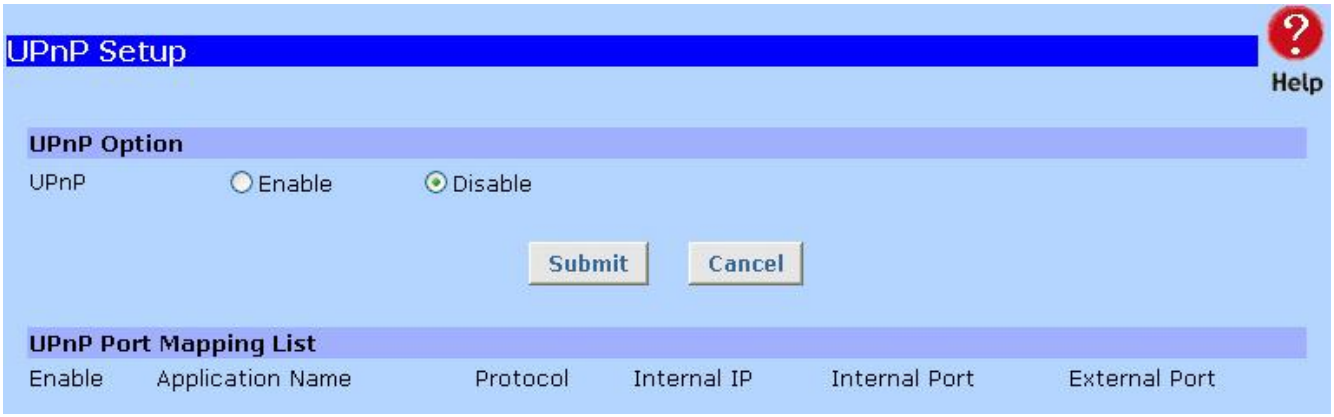


Figure 4-9: UPnP Setup

Settings ï UPnP Setup

UPnP Option	If set to *Enable UPnP*, this device will register on the local network. You will find that there is an icon showing on the *My Network Places* in Window XP. Each time you add a new service with port mapping, the new service will appear on the mapping list.
UPnP Port Mapping List	If UPnP is set to *Enable*, this table shows the details of all Custom Virtual Servers configuration data which have been defined.

NAT Setup

NAT (Network Address Translation) is the technology which allows one (1) WAN (Internet) IP address to be used by multiple LAN users.

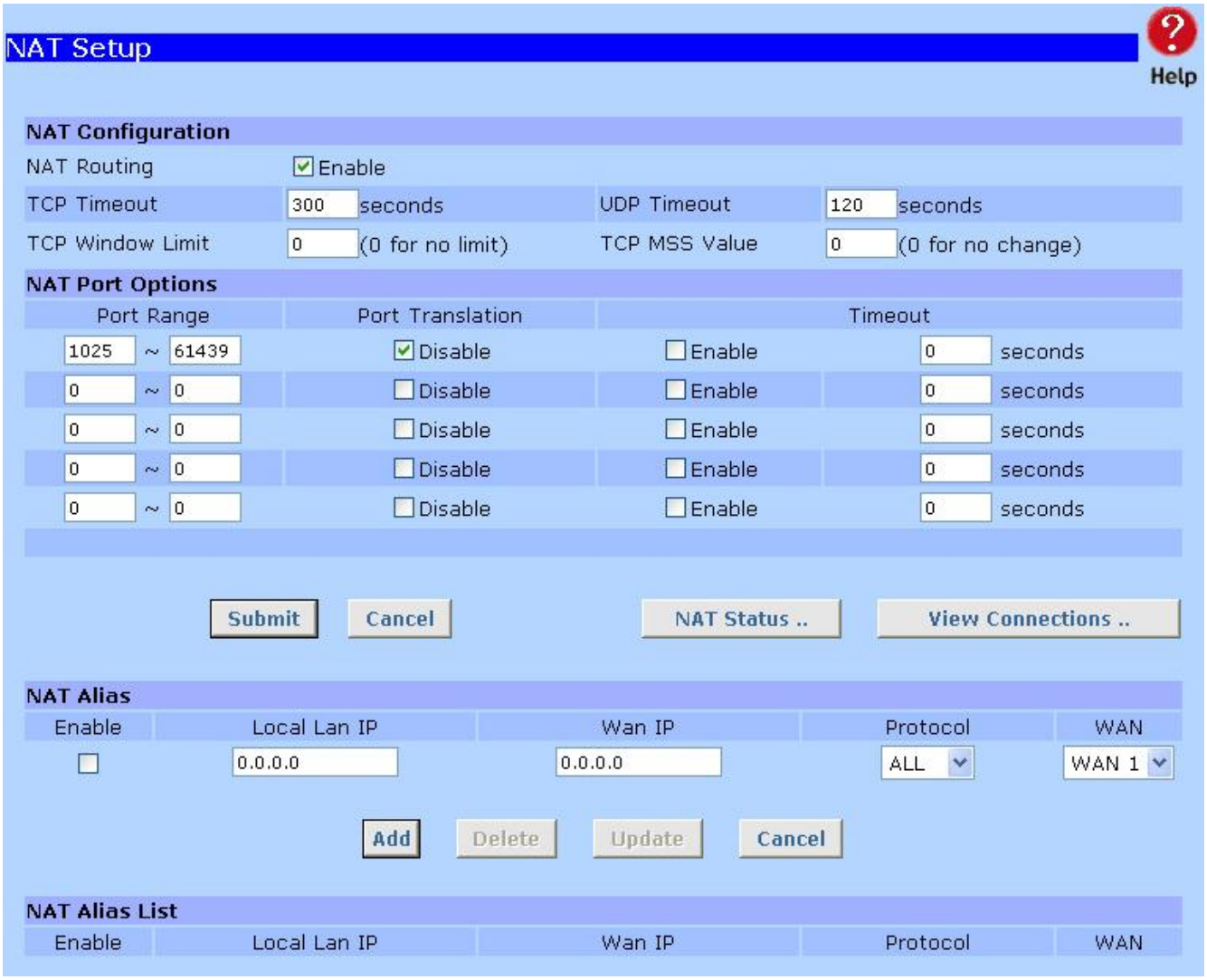


Figure 4-10: NAT Setup

Settings ï NAT Setup

NAT Configuration	¶ **NAT Routing** ï You can enable or disable NAT through the check box. If you disable the NAT checkbox, it will act as a bridge or Static Router. Most features will be unavailable. ¶ **TCP Timeout** ï Enter the desired value to use on each WAN port. The default is 300 ¶ **UDP Timeout** ï Enter the desired value to use on each WAN port. The default is 120 ¶ **TCP Window Limit** ï Enter the desired value to use on each WAN port. The default is 0 (no limit). ¶ **TCP MSS Limit** ï Enter the required MSS (Maximum Segment Size) to use on each WAN port. The default is 0 (no limit).
NAT Port Options	If some packets whose port number cannot be translated for special applications, you must set state t oEn ãa b l e ò a n d i n p u t v a Alternatively, if its port cannot be translated in the specified time period, you must set Enable and enter a seconds value in Timeout.
NAT Alias	For each alias entry, the WAN IP acts as an alias of the host with Local LAN IP accessing the Internet via the specified WAN port for the specified protocol packets, i.e. 1-1 NAT.
NAT Alias List	NAT Alias List shows the list of all NAT alias configuration data which are currently defined. You can modify its configuration data by selecting and clicking on a row.
Check NAT Detail	Shows all detailed NAT configuration data.
NAT Connection List	This shows the current details of all NAT entries which include interface, protocol, state, destination IP, WAN IP, local IP, idle time and in/out packets.

Advanced Feature

- **External Filters Configuration** ï These settings determine whether the Multi-WAN VPN Router should respond to ICMP (ping) requests received from the WAN port or not.
- **Interface Binding** ï Use these settings to ensure that certain traffic is sent by a particular WAN port and thereby a particular ISP account. These settings are only useful on some WAN ports.
- **Protocol & Port Binding** ï This allows you to bind any WAN port by selecting the protocol type you want.

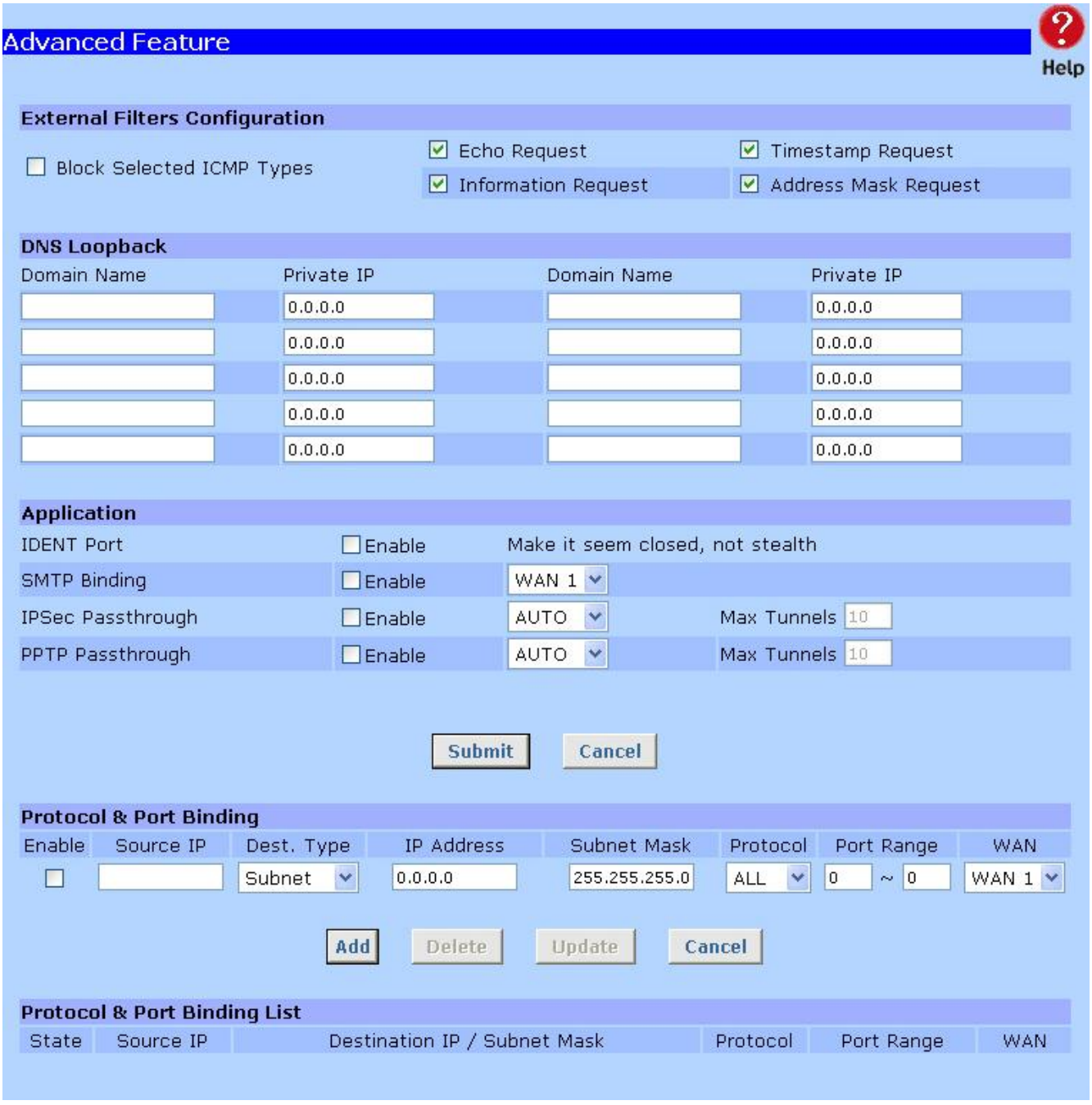


Figure 4-11: Advanced Feature

Settings ï Advanced Feature

External Filters Configuration	¶ **Block Selected ICMP Types** ï These settings determine whether or not this device should respond to ICMP requests received from the WAN port. If checked, the selected packet types are blocked. Otherwise, the packets are accepted. ¶ **Echo Request / Information Request / Timestamp / Address Mask Request :** The ICMP standard (RFC 792) also specifies timestamp request, information request, and address mask request packets as codes 13, 15, and 17, respectively. While the ostensible purpose for these queries is to learn information such as address masks and current times, they can easily be used for host discovery. A system that replies is up and available. A timestamp reply (ICMP code 14) or address mask (code 18) discloses that the host is available
DNS Loopback	Used when you have some servers on the LAN and their domain names have already been registered on public DNS. To avoid DNS loop back problems, please enter the following fields: ¶ **Domain Name** ï Enter the domain name specified by you for the local server. ¶ **Private IP** ï Enter the private IP address of your local server.
Application	¶ **IDENT Port** ï Port 113 is associated with the Internet's (Identification / Authentication) service. When a client program in your computer contacts a remote server for services such as POP, IMAP, SMTP, that remote server sends back a query to the "Ident" server running in many systems listening for these queries on port 113. This means that hackers can probe port 113 as a rich source of your personal information. The default value of this check box is ñDisableò ¶ **SMTP Binding** ï Unless you are using E-mail accounts from different ISPs on each port, you can ignore these settings. Some ISPs configure their E-mail Servers so they will not accept E-mail from IP addresses not allocated by them. If you are using accounts from different ISPs, sending E-mail over the wrong WAN port may result in the mail not being accepted. In this case, you can use these settings to correct the problem: **-Enable** ï If enabled, the WAN port you specify below will be used for all outgoing SMTP traffic. If not enabled, either WAN ports will be used. **-WAN** ï Select the desired WAN port to be bound. ¶ **IPSec Passthrough** ï Enable/Disable IPSec passthrough, and designate it to a WAN port. By default IPSec passthrough is ñEnable ¶ **PPTP Passthrough** ï Enable/Disable PPTP passthrough, and designate it to a WAN port. By default PPTP passthrough is ñEnable

Protocol & Port Binding	**Protocol and Port Binding** Use these settings if you wish to ensure that particular traffic is sent by a specific WAN port, and thereby a particular ISP account. ¶ **Enable** - Enable or disable each item as required. ¶ **Source IP** - IP address of source from which packets are sent. ¶ **Destination IP** ï IP address of destination to which packets are sent. ¶ **Subnet Mask** ï With a subnet mask other than 255.255.255.255, you can make an IP sub-network as your destination. ¶ **Protocol** ï Select protocol type used by the traffic you wish to configure. ¶ **Port Range** - Enter the beginning and end of the port range used by the traffic you wish to configure. If only a single port is used, enter the port number in both fields. ¶ **WAN** - Select the WAN port you wish this traffic to use.
Protocol & Port Binding List	This list shows the details of all protocol and port configuration data which are currently defined. You can modify them by clicking on a selected row.

5: Security Management

Overview

¶ ***Block URL*** ï Ability to block a specific website by configuring IP address, URL or Keywords.

¶ ***Access Filter*** ï Ability to block all Internet access, a known port or user defined ports by group access.

¶ ***Session Limit*** ï Ability to limit users Internet access when the device detects new sessions that exceed the maximum value in the sampling time, for example, virus, syn flood, etc.

¶ ***SysFilter Exception*** ï This feature allows you to configure an unrecognized port, allowing those packets to be processed, enabling some programs to run more smoothly. This is also applicable for some future applications that may need this mechanism in order to work well.

Block URL

This feature allows you to block access to undesirable Web sites. You can block by URL, IP address, or Keyword. You can also have different blocking settings for different groups of PCs.

¶ In operation, every URL is searched to see if it matches or contains any of the URLs or keywords entered here. Then, after a DNS lookup, it determines the IP address of the requested site and checks it against IP address entries on this screen.

¶ Note that a single IP address may host many Web sites (shared IP). Entering an IP address on this screen will block all Web sites that may be hosted on that IP address.

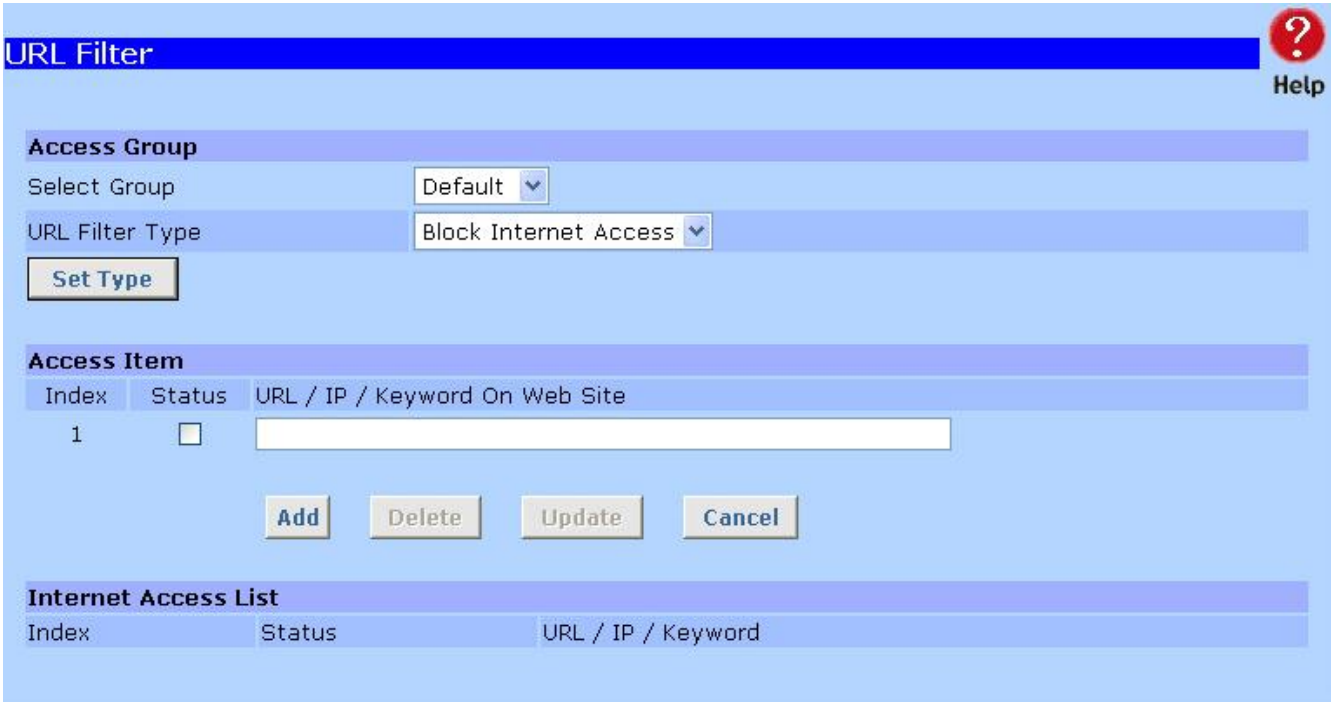


Figure 5-1: Block URL

Settings ï Block URL

Access Group	This allows you to have different blocking rules for different Groups of PCs. ¶ All PCs (users) are in the *Default* Group unless moved to another specified group on the ***Host IP*** screen. ¶ If you want the same restrictions to apply to everyone, select *Default* for the Group. In this case, there is no need to enter any Hosts in the ***Host IP*** screen. ¶ If you wish to apply different restrictions on different Groups, select the desired Group, and click the "Select" button. The screen will update the data for the selected Group. ¶ URL List Type ï **Block Internet Access**: If you select Black List, It will block the URL that you keep it on Access Item. **Allow Internet Access:** If you are select White List type, it will block the entire URL except you keep it on the Access Item. ¶ **Set Type** Button ï Button to submit Black List or White List.
Access Item	¶ **Enable/Disable** ï Use this to Enable or Disable each setting as required. ¶ **Block URL/IP/Keyword** ï Enter the URL, IP address or Keyword you wish to block.
Internet Access List	The list will display all block rules that you have setup. You can modify it by clicking on a selected row.

Access Filter

The network Administrator can use the Access Filter to gain fine control over the Internet access and applications available to LAN users.

¶ Five (5) user groups are available and each group can have different access rights assigned to them.

¶ All PCs (users) are in the *Default* group, unless assigned to another group on the ***Host IP*** screen.

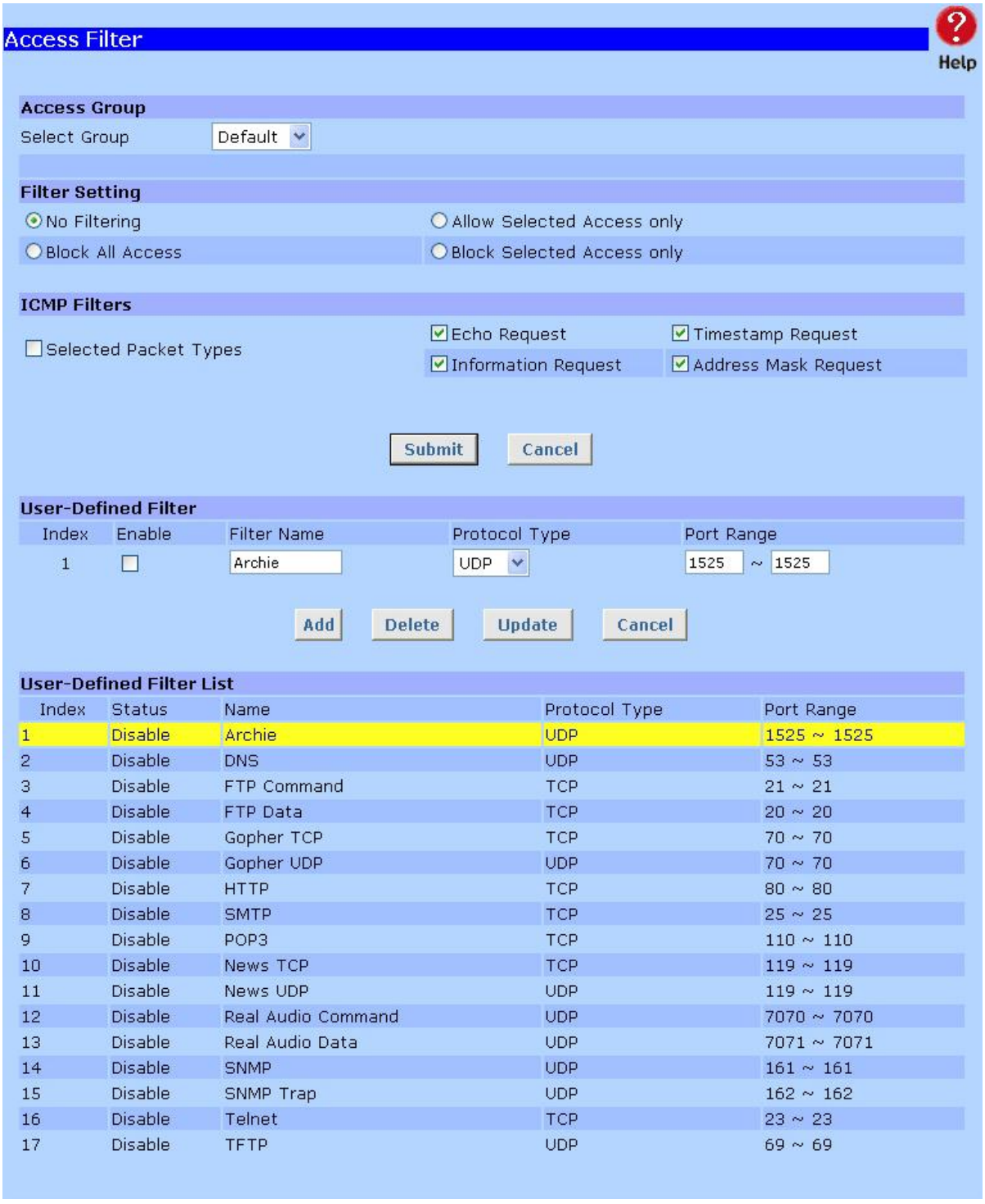


Figure 5-2: Access Filter

Settings ï Access Filter

Access Group	This allows you have different access rights for different Groups of PCs. ¶ If you want the same restrictions to apply to everyone, select *Default* for the Group. In this case, there is no need to enter any Hosts on the ***Host IP*** screen. ¶ If you wish to apply different restrictions to different Groups, select the desired Group. The screen will update data for the selected Group.
Filter Setting	Select the desired option for this Group: ¶ **No filtering** ï Nothing is blocked, Internet access is not restricted. ¶ **Block All Access** ï Everything is blocked, Internet access is not available. ¶ **Block selected items** ï Items selected on this screen are blocked. You can block known services by using the checkboxes, or you may define your own filters.
ICMP Filters	If you enable ICMP Filter that means it will block ICMP request packet types specified by users from local host to remote side.
User-Defined Filter	This section is optional. It allows you to define your own filters as required. For each filter, the following information is required: ¶ **Filter Name** ï Enter a name for this filter. ¶ **Protocol Type** ï Select a protocol type you wish to block. ¶ **Port No. Range** ï Enter the range of port numbers used that you wish to block. If only a single port is required, enter it in both fields.
User-Defined Filter List	This List shows the details of all User-Defined Filter configurations which are currently defined. You can modify its configuration data by clicking on a selected row.

Session Limit

This new feature allows to drop the new sessions from both WAN and LAN side, if the number of new sessions exceeds the maximum value set by you in the Sampling Time field.

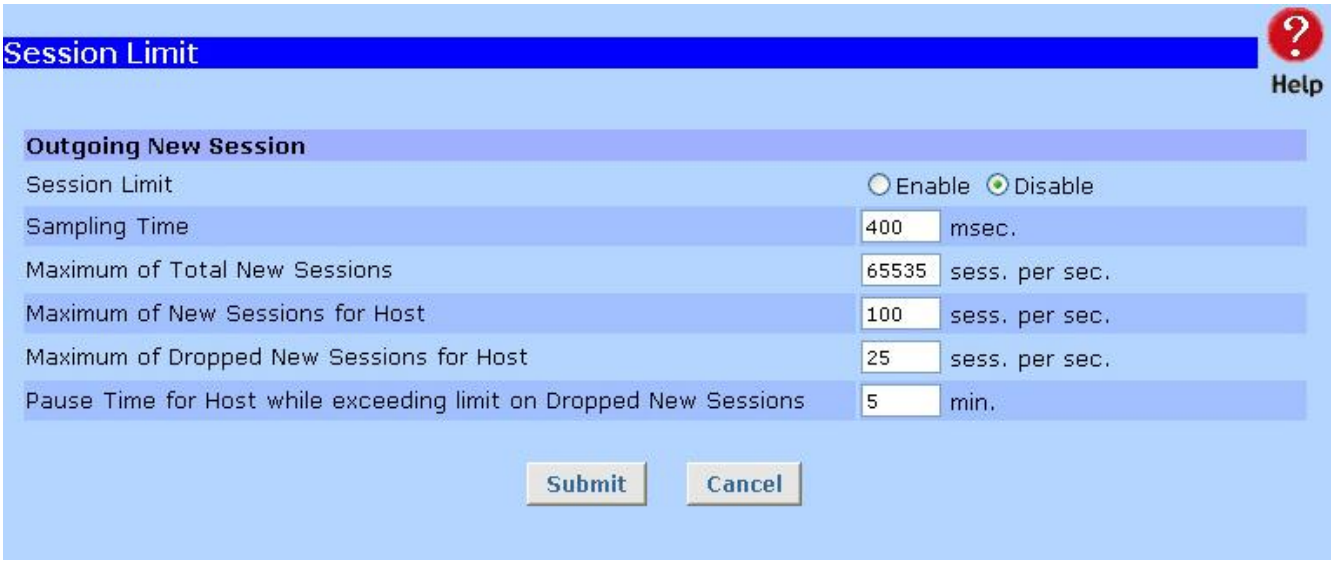


Figure 5-3: Session Limit

Settings ï Session Limit

Sampling Time	The time interval specified by you for new sessions. Only the new sessions that have recently occurred are counted according to the sampling time entered. (Default is 400 mil-sec)
Maximum of Total New session	The maximum total number of new sessions in the system which is acceptable in the sampling time. Any new incoming sessions will be dropped after the number of new sessions has been exceeded. (Default: 65535 session/sec)
Maximum of New Sessions for Host	The maximum number of new sessions from the host which is acceptable in the sampling time. Any new incoming sessions will be dropped from this host after the number of new sessions has been exceeded. (Default: 100 session/sec)
Maximum of Dropped New Sessions for Host	If the number of dropped new sessions from the host exceeds the Maximum in the sampling time, any new session from the host will be dropped in the pause time period. (Default: 25 session/sec)
Pause Time for Host while exceeding limit on Dropped New Sessions	Within the pause time period, new session from the suspended host will not be served by the system when the number of dropped new sessions exceeds the defined Maximum. (Default is 5 minutes)

SysFilter Exception

System Filter Exception - This will reject every packet with an unrecognized port to block port scan programs from hackers. This, however, also incurs problems in some situations where servers (e.g. SMTP server port 113) or WAN clients need to send a response packet to verify the activity of their communication peers.

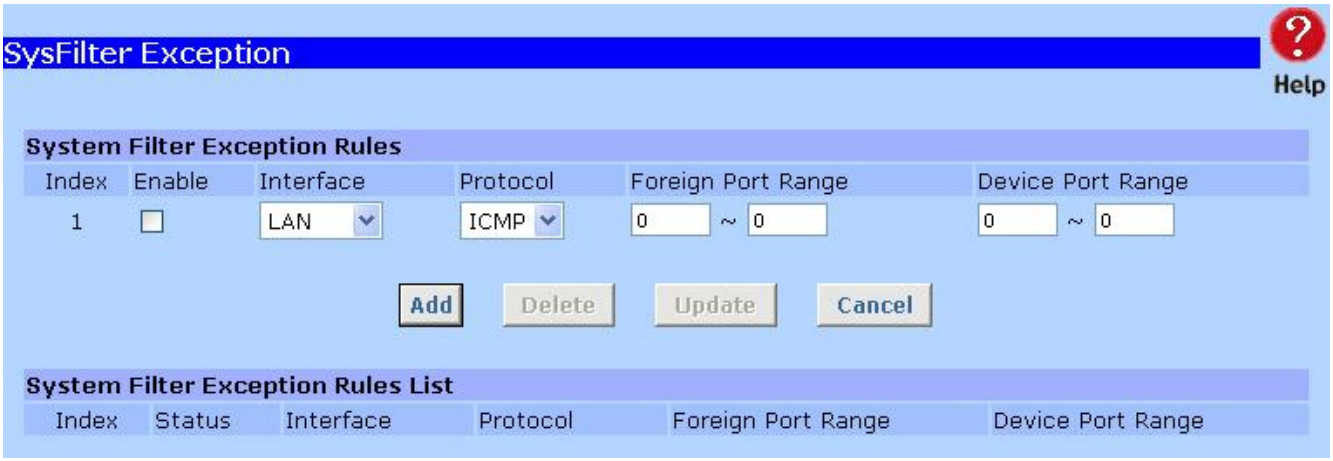


Figure 5-4: SysFilter Exception

Settings ï SysFilter Exception

System Filter Exception Rules	¶ **Enable** ï If check box is marked, it will enable System Filter Exception ¶ **Interface** ï You can select LAN, any WAN port or ALL interfaces from which a packet originates. ¶ **Protocol** ï The packet type (selected in the above Interface) which will be directly processed by this device. ¶ **Foreign Port Range** ï Enter the beginning and end of the foreign port range used by the traffic you wish to configure. If only a single port is used, enter the port number in both fields. ¶ **Device Port Range** ï Enter the beginning and end of the device port range used by the traffic you wish to configure. If only a single port is used, enter the port number in both fields.
System Filter Exception Rules List	The list will display the details of all System Filter Exception Rules that you have setup. You can modify data by clicking on a selected row.

6: VPN Configuration

Overview

Virtual Private Network (VPN) uses encryption to create the connection between two end points (computers or networks). It allows private data to be sent securely over a public network or the Internet without the risk of outside intruders gaining unauthorized access. VPN establishes a private network that can send data securely between two networks. We call this by creating a ñ t u n n e l ò . A tunnel connects the two PCs or networks

Note: The VPN Router uses industry standard IPSec encryption. However, due to the variations in how manufactures interpret these standards, many VPN products are not interoperable. Although the Multi-WAN VPN Router can interoperate with many other VPN products, it is not possible for the Multi-WAN VPN Router to provide specific technical support for every other product.

IKE Global Setup

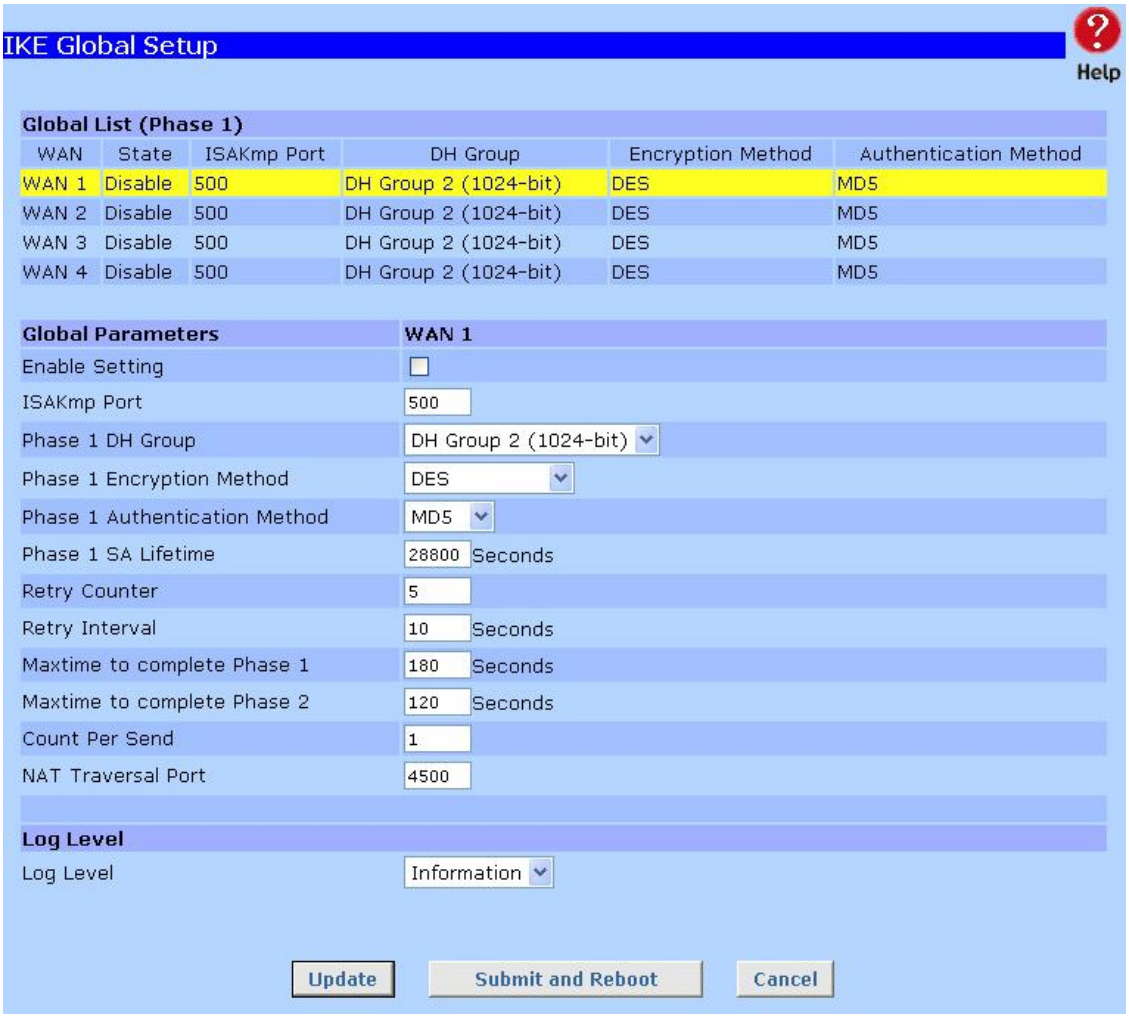


Figure 6-1: IKE Global Setup

Settings ï IKE Global Setup

Global List (Phase 1)	The list will only show the approximate information of all Global Settings on each WAN port. You can modify it by clicking on a selected row.
Global Parameters	¶ **Enable Setting** ï If set to Enable, it enables the VPN function to work. ¶ **ISAkmp Port** ï Internet Security Association and Key Protocol Management (ISAkmp) is designed to negotiate, establish, modify and delete security associations and their attributes. By default, it is assigned UDP port 500 by the IANA. You can set it to use a port other than port 500. The remote IPsec site will attempt to connect on it. ¶ **Phase 1 DH Group** ï There are three levels of cryptography from the Diffie-Hellman group. The DH method illustrates key generation using public key cryptography. It uses the public and secret key information held by both users to generate a key. ¶ **Phase 1 Encryption Method** ï There are three data encryption methods available: DES, 3DES and AES. ¶ **Phase 1 Authentication Method** ï There are two authentication methods available: MD5 and SHA1 (Secure Hash Algorithm) ¶ **Phase 1 SA Life Time** ï By default the Security Association lifetime is 28800 seconds. When it is expired, a new key is re-negotiated. During the negotiation period, ¶ **Retry Counter** ï This indicates how many times the process of Phase 1 will be restarted will be an error message in the VPN log once it is expired. ¶ **Retry Interval** ï This indicates the time period between two consecutive retries. ¶ **Maxtime to complete Phase 1** ï This indicates the maximum time allowed for negotiation in Phase 1. If it expires, it is recommended to increase the Maxtime period or reduce the DH group level. Default value is 30 sec. ¶ **Maxtime to complete Phase 2** ï It indicates the maximum time allowed for negotiation in Phase 2. If it expires, it is recommended to increase the Maxtime period or reduce the DH group level. Default value is 30 sec. ¶ **Count Per Send** ï This indicates the maximum amount of duplicate packets to be resent if the remote side does not respond to the first packet. ¶ **Force Deletion after Expiry** ï When set to *Enable,* once SA has expired, the tunnel session will be removed and all related resources will be cleared.
Log Level	This function allows you to select which information you want to see on the VPN log. It has six different message levels: None, Critical, Error, Warning, Information and Debug.

Planning the VPN

When planning your VPN, you must make the following choices first:

1. If the remote site is a LAN network, the two end-point networks must have different LAN IP address ranges. If the remote end-point is a single PC running a VPN client, its destination address must be a single IP address with subnet mask of 255.255.255.255
2. Will you be using the Internet Key Exchange (IKE) setup, or Manual Keying? Whichever method is used, you must specify each phase of the connection.
3. At least one side must have a fixed IP address. The other side with a dynamic IP address must always be the initiator of the connection.
4. What encryption level will you use (DES, 3DES or AES)?
5. What authentication method will you use (MD5, SHA1 or SHA2)?

IPSec Policy Setup

The VPN Policy Setup is to define the VPN phase 2 policy including the encryption and authentication method. Once you have finished the configuration, you can press the Connect button to initiate the VPN connection. You can also press Set Options button for advanced setting of the policy.

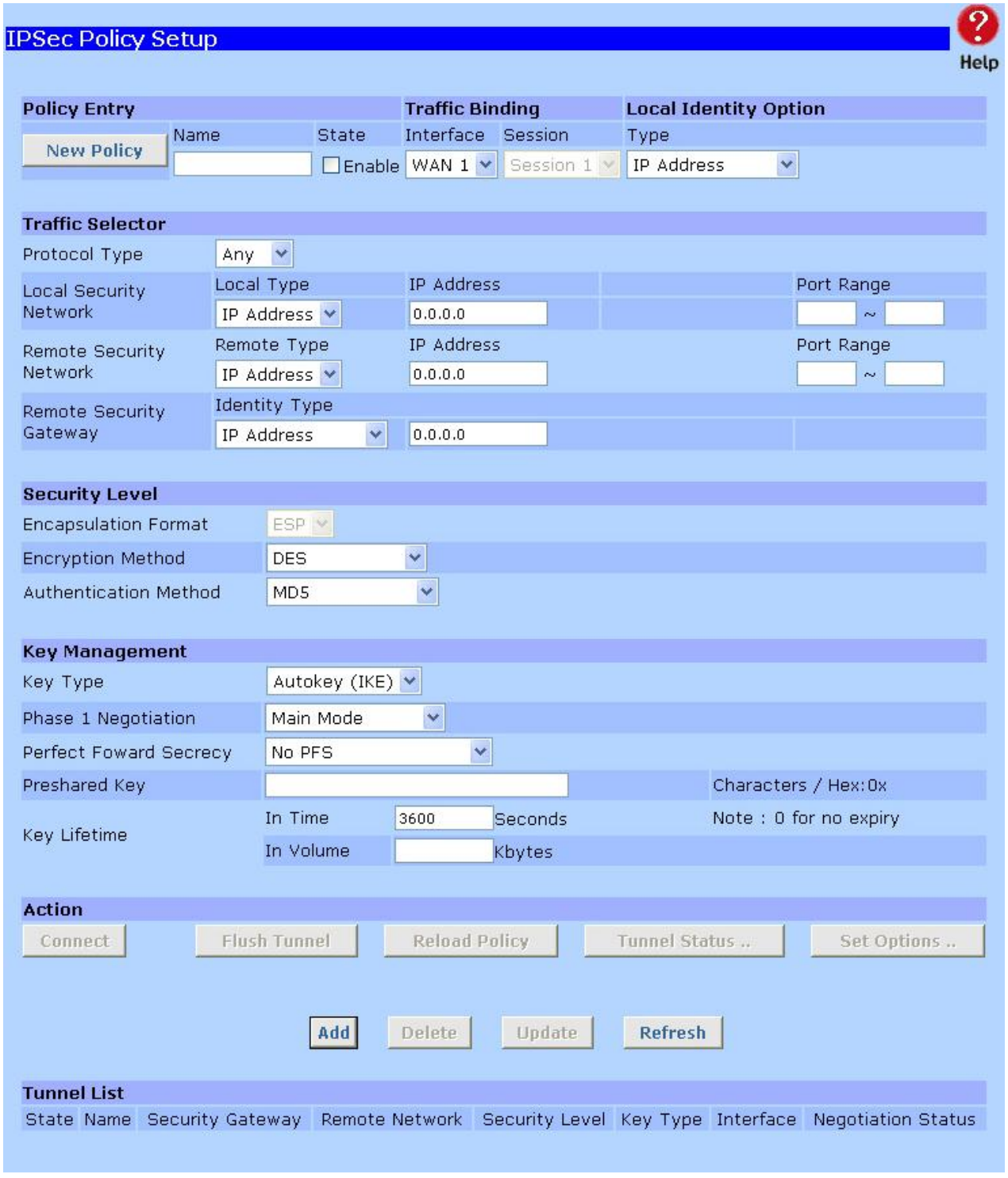


Figure 6-2: IPSec Policy Setup

Settings ï IPSec Policy Setup

Policy Entry	¶ **Name** ï In order to distinguish the tunnel, you have to give ñTunnelò a name. ¶ **State Enable** ï If set to *Enable*, this will allow the tunnel to connect. ¶ **Traffic Binding** **WAN port** ï You can choose any WAN port to make the VPN connection. **Session** ï If you are using a multi-session PPPoE connection, you can select which PPPoE session will create a VPN tunnel between two sites. ¶ **Local Identity Type** ï You can select how the router will identify itself to the destination VPN site. There are three options to select from: ¶ **IP address** ï This allows the authentication by using its public IP address. ¶ **Domain Name** ï This allows the authentication by using a domain name. ¶ **Distinguished Name** ï This allows the authentication by using a distinguished name such as an email address or alpha-numeric characters.
Traffic Selector	¶ **Service** ï **Protocol Type:** You can choose TCP, UDP, ICMP or GRE protocol as your connection protocol. By default the protocol type is ñAnyò. ¶ **Local Security Network** ï These entries identify the private network on this VPN gateway - the hosts of which can use the LAN-to-LAN connection. You can choose a single IP address, the subnet, or a selected IP range to make VPN LAN-to-LAN connection. ¶ **Remote Security Network** ï These entries identify the private network on the remote peer VPN gateway whose hosts can use the LAN-to-LAN connection. You can choose a single IP address, the subnet, or a selected IP range to make VPN connection ¶ **Remote Security Gateway** ï You can select either the remote side by a domain name, a remote side IP address (WAN IP address) or a distinguished name as your remote side security gateway.

Security Level	¶ **Encryption Method** ï Specifies the encryption mechanism to use. Data encryption makes the data unreadable if intercepted. There are three encryption methods available: DES, 3DES and AES. The default setting is *null*. ¶ **Authentication Method** ï Specifies the packets authentication mechanism to use. Packets authentication confirms if the dataô s source is correct or not. There are three authentication methods available - MD5, SHA1 and SHA2. ¶ **ESP Mode** ï Only *Tunnel Mode* is available. It offers the most protection against an intruder trying to intercept VPN packets.
Key Management	**Key Type** ï Two key types are available for the key exchange management - Manual Key and Auto Key: ¶ **Manual Key** ï If manual key is selected, no key negotiation is needed. The following fields to be set are: 1. **Encryption Key** ï This field specifies a key to encrypt and decrypt IP traffic. 2. **Authentication Key** ï This field specifies a key to use to authenticate IP traffic. 3. **Inbound/out bound SPI (Security Parameter Index)** ï This information is carried on the ESP header. Each tunnel must have a unique inbound and outbound SPI and no two tunnels share the same SPI. Note that the Inbound SPI must match the other routerôs outbound SPI. ¶ **AutoKey (IKE)** ï There are two types of operation modes which can be used in Phase 1 Negotiation: 1. **Main mode** ï Accomplishes a Phase 1 IKE exchange by establishing a secure channel. 2. **Aggressive Mode** ï This is another way of accomplishing a phase one exchange. It is faster and simpler than Main Mode but does not provide identity protection for the negotiating nodes. ¶ **Perfect Forward Secrecy (PFS)** ï If PFS is enabled, Phase 2 IKE negotiation will generate new key data for IP traffic encryption & authentication. If set to *Enable*, a hacker using brute force in an attempt to break encryption keys is not able to obtain other or future IPSec keys. ¶ **Preshared Key** ï This field is used to authenticate the remote IKE peer. It is a ñpass codeò or ñpasswo used between both the local site and remote site. Otherwise the VPN tunnel will not be established. ¶ **Key Lifetime** ï This specifies the lifetime of the IKE generated Key. If the time expires or passed data exceeds the allowed volume, a new key will be renegotiated. By default, 0 is set for *No Limit*.

Security Association List	The list will display the details of all Policy Setup configuration data that you have entered. Modification can be made by clicking on a selected row.
Action	¶ **Connect** ï Manually trigger the tunnel negotiation with selected IKE/IPSec proposals ¶ **Disconnect** ï Manually shut down the established tunnel and clear all the SA in use, inform peer by sending Delete payload. ¶ **Flush** ï Manually clear the established, unfinished or in progressing tunnel disregarding current negotiation state. ¶ **Reload Policy** ï Bring current policy configuration into effect, use this when policy has been updated ¶ **Tunnel Status** ï Display the current tunnel Runtime attributes and Traffic Statistics. ¶ **Set Option** ï Option set provided for setting advanced tunnel attributes eg: DPD(health checking), NATT, triggering, filtering.. etc.

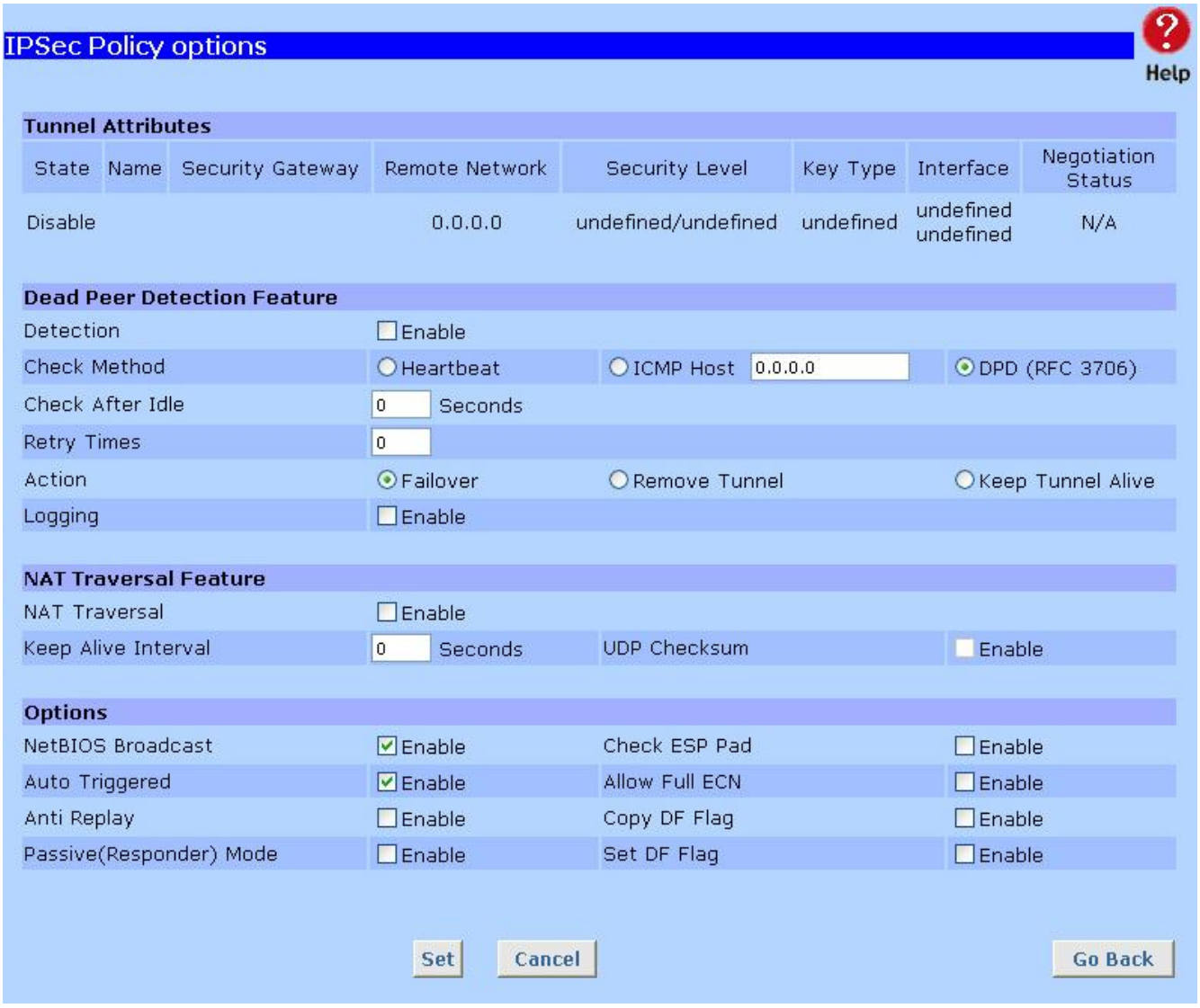


Figure 6-3: IPSec Policy Options

Settings ï IPSec Policy Options

Dead Peer Detection Feature	¶ **Dead Peer Detection (DPD)** ï If set to *Enable*, a device will periodically send HELLO/ACK messages to check if the tunnel is alive when both peers of a VPN tunnel provide DPD mechanism. Once a dead peer is detected, a device will end the connection so it can be re-established. This is the primary method of VPN failover or backup. ¶ **Detection** ï If set to *Enable***,** this will enable the following Check Method which you have selected to work: ¶ **Check Method**: 1. **Heartbeat** ï Sends a u n i d i r *HELLO* message to determine connection aliveness. 2. **ICMP Host** ï It uses **ICMP** packets to determine connection

	aliveness 3. **DPD (RFC 3706)** ï Uses a bi-directional (*ó H E L L O ì* message, ACK) message to determine connection aliveness. ¶ **Check After Idle** ï Indicates the time period in which no traffic passes - a *Detection* packet is sent to the peer. ¶ **Retry Times** ï The number of times a device will attempt to send the Detection packet before the *Check After Idle* time expires. ¶ **Action** ï This will execute one of the following actions after the Detection is determined: *Failover* - ignores the dead tunnel. *Remove Tunnel* - disconnects the dead tunnel. *Keep Tunnel Alive* - attempts to keep the tunnel alive. ¶ **Logging** ï If set to Enable, all DPD activity of will show up in the VPN log.
NAT Traversal Feature	¶ **NAT Traversal (NAT-T)** ï NAT Traversal is a VPN Gateway feature that circumvents IPSec NATing problems. It is a more effective solution than IPSec Passthrough. If you enable the checkbox it will turn on NAT-T mechanism. By default is ñDisableò ¶ **Keep Alive Interval** ï It is usually necessary for the IPSec to send periodic keep-alive packets, so that the NAT mapping does not change until the phase1 and phase2 SAs expire. By default is ñ0ò second mean always keep alive. ¶ **UDP Checksum** ï All UDP packets contain a UDP checksum, a calculated value that ensures UDP packets are free of transmission errors. The device (Multi-WAN router) does not require use of UDP checksum for NAT-T. Therefore, the checkbox keep it always ñDisableò

Options	¶ **NetBIOS Broadcast** ï This option is used to forward NetBIOS packets across the Internet from remote side to local side and vice versa. When enabled, the remote side computer can be reached by a host name. ¶ **Auto Triggered** ï If set to *Enable*, a device will automatically attempt to connect the remote VPN gateway without any user input. ¶ **Anti Replay** ï This ensures that IP packet-level security is kept track of in order. ¶ **Passive (Responder) Mode** ï When enabled, the tunnel state will remain idle until an attempt is made to connect to the remote side. This setting will override the *Auto Triggered* option. ¶ **Check ESP Pad** ï If set to *Enable*, a device will check the ESP (Encapsulating Security Payload) padding of each packet. ESP is a key protocol in the IPSec architecture which is designed to provide a mix of security services in IPv4 and IPv6. ¶ **Allow Full ECN** ï If set to *Enable*, it will allow full Explicit Congestion Notification (ECN). ECN is a standard proposed by the IETF that will minimizes congestion on a network and prevent the gateway from dropping data packets. ¶ **Copy DF Flag** ï When an IP packet is encapsulated as payload inside another IP packet, some of the outer header fields can be newly written while others are determined by the inner header. Among these fields is the IP DF (Do not Fragment) flag. When the inner packet DF flag is clear, the outer packet may copy it or set it. However, when the inner DF flag is set, the outer header MUST copy it. ¶ **Set DF Flag-** If the DF (Do not Fragment) flag is set; it means that the fragmentation of this packet at the IP level is not permitted.

Mesh Group Setup

The Multi-WAN VPN Link Balancer not only provides VPN failover and backup but is also capable of offering VPN load balance.

If you have setup IPSec policy on the IPSec Policy Setup web page, then you don't have to enter IPSec policy setup again here. You can press the **Scan Policies** button to copy the IPSec Policy into the Mesh Group Setup web page. You also can configure your IPSec Policy on the Mesh Group web page by pressing the **Create** button. To use the VPN load balance option, it is necessary to use a static IP.

For configuring Mesh Group Setup you can refer to the IPSec Policy Setup:

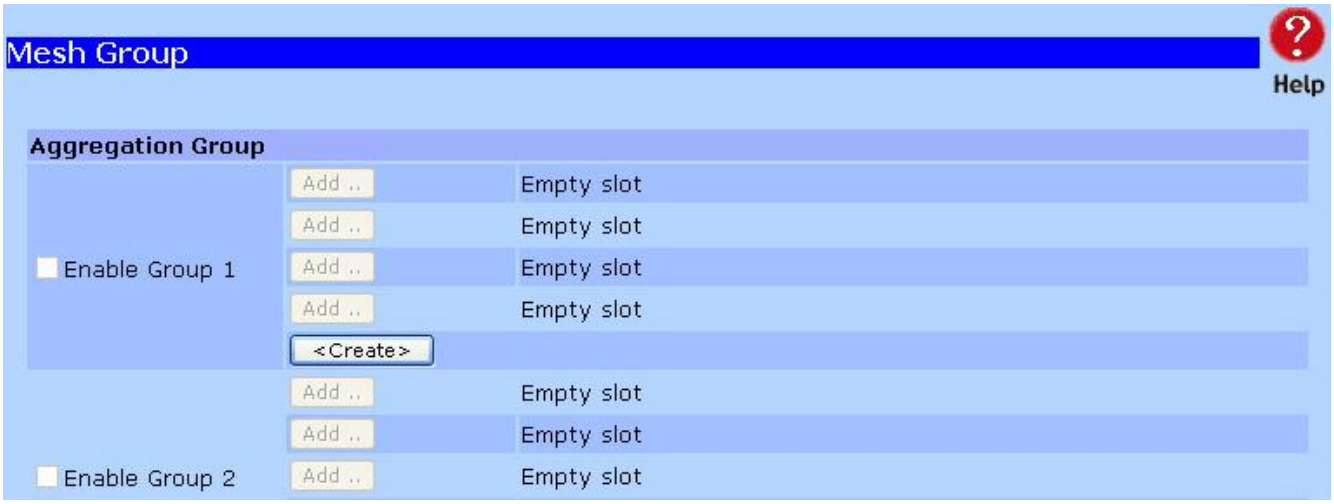


Figure 6-4: Mesh Group Setup

Once you have added your VPN Policy to the Mesh Group, you can set up your Mesh Group through the VPN Mesh Group Configuration.

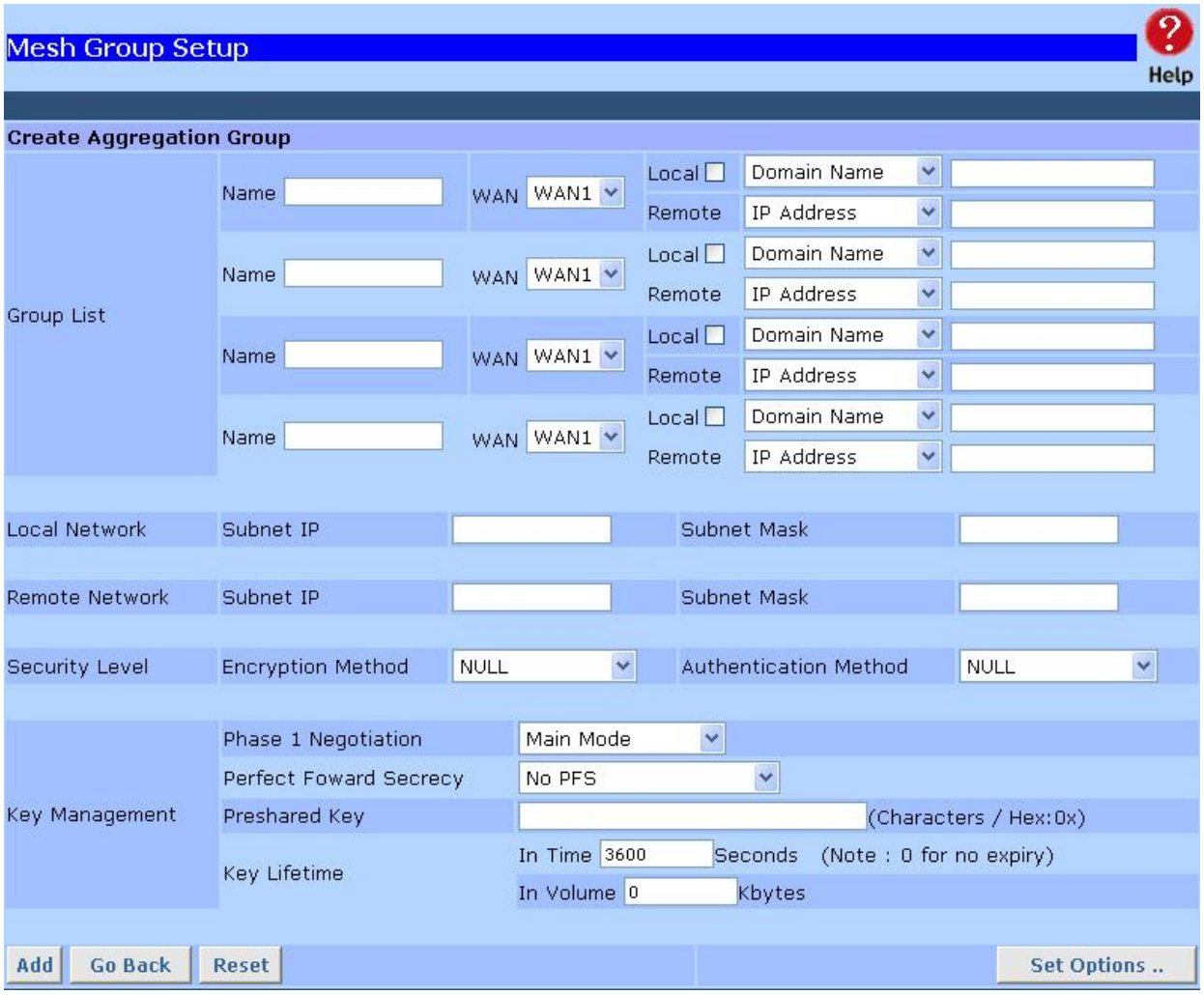


Figure 6-5: Mesh Group Configuration

Settings ï Mesh Group Configuration

Aggregation Group	This will display all the VPN connections that are using for VPN load balancing. You should enable the check box before you make a VPN load balance connection. ¶ **Delete Button** ï This button can delete one or all IPSec Policies. ¶ **Set Button** ï Once you have enabled/disabled the check box, you have to press the *Set* button to submit it. ¶ **Edit Button** ï The *Edit* button will let you edit the IPSec policy. ¶ **View Button** ï This will let you monitor the connection status. ¶ **Connection Button** ï Allows you connect or disconnect the VPN manually,

VPN Log

You can monitor the VPN status through the VPN Logs web page. The log level (priority) can be chosen from the VPN IKE Global Settings web page.

Figure 6-6: VPN Logs

Data ï VPN Logs

Message Status	¶ **Time** ï Indicates when the message was created according to system time. ¶ **Priority** ï Indicates the priority level of a message for analysis.
Undefined Messages	¶ **Module ï** Denotes the module responsible for the message sent in the IPSec architecture. ¶ **Messages ï** Displays some information describing the event that happened.

7: QoS Configuration

Overview

The Multi-WAN VPN Router incorporates a QoS (Quality of Service) utility to provide high quality network support service.

Because it classifies outgoing packets based on policies defined by users, real-time applications should respond or perform better.

QoS Setup

The following web page instructs you on setting up and enabling QoS.

Figure 7-1: QoS Setup

Settings ï QoS Setup.

QoS Feature	È **Enable QoS** ï Checkbox allows users enable QoS mechanism. If set to "enable" QoS. QoS will allocate Inbound/Outbound bandwidth to pass through the device. ¶ **WAN Inbound / Outbound Bandwidth** ï This allows you to set the maximum inbound or outbound bandwidth, maximizing your network's performance. This information can be obtained from your ISP ¶ **Set Policy Button** ï Setting the policy can allocate Inbound/Outbound bandwidth (based on your configuration) to pass through this device.

Policy Configuration

Setting the **QoS** policy can allocate Inbound/Outbound bandwidth (based on your configuration) to pass through this device. You can define some policies which classify received packets based on Local/Remote IP, MAC, port and protocol type. This feature is useful when the WAN link is very busy or congested or when using special applications that need real time services such as Internet phone, video conference...etc.

Figure 7-2: Policy Configuration

Settings ï QoS Policy

WAN Inbound Policy	¶ **Policy Name** ï The name of a policy which is used to classify the received packets based on the following types for your memory ¶ **Local / Remote Address, Port** ï Specify a packet based on Local/Remote address or port. Address has two types: IP address and MAC address. By default, the IP address is 0.0.0.0 for all IP Addresses but the MAC address is 00-00-00-00-00-00 which cannot be used to classify. Port and Protocol Type define all packets for special applications ¶ **Protocol Type** ï The field defines traffic packet type, i.e. IP, TCP and UDP. ¶ **Maximum Guaranteed Bandwidth** ï This device supports Bandwidth queues. When a packet meets a policy rule requirement, it will be put into the responding queue. The queue will send them use the guaranteed bandwidth. If the rest bandwidth is enough it will try to arrive the maximum bandwidth.