BR-6624

Load Balancing Router

Manual

TABLE OF CONTENTS

Document Version: 2.0

1: Introduction

Congratulations on the purchase of your new Load Balancer. The Load Balancer provides ***Shared Broadband Internet Access*** for all LAN users.

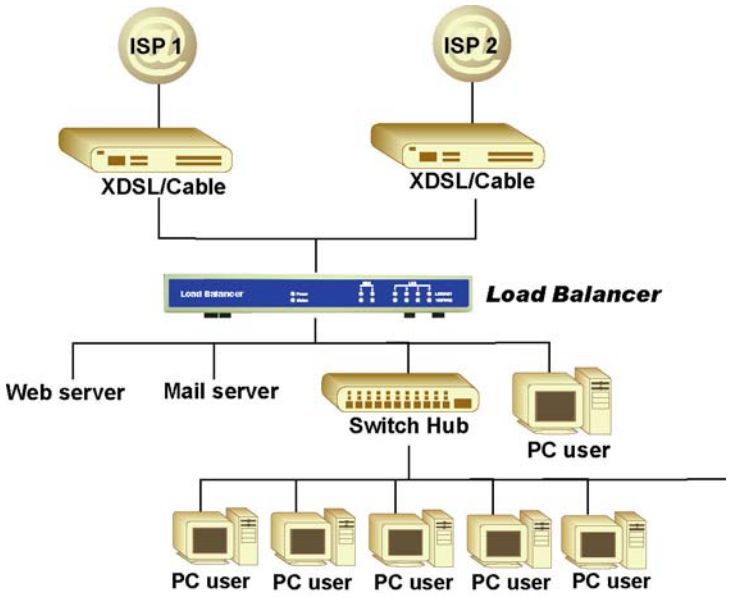

Figure 1-1: Load Balancer

Internet Features

- ***Shared Broadband Internet Access***

  All LAN users can access the Internet through the Load Balancer, by sharing one (1) or two (2) Broadband modems and connections.

- ***High-Performance Dual Modem Support***

  The Load Balancer has two (2) WAN ports, allowing connection of two (2) Broadband modems. **This gives twice the bandwidth of a single modem**.
  Flexible configuration allows each port to use a different type of modem and connection method. Also, you can determine how the Internet traffic is shared between the 2 modems.

- ***Supports all common Connection Methods***

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

- ***PPPoE Session Management***

  Multiple PPPoE sessions are supported and you can choose to “map” sessions to individual PCs 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 individual PCs if desired.

- ***Special Applications***

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

- ***Virtual Servers***

  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 you 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, you can have multiple “DMZ” PCs. Each “DMZ” PC has unrestricted 2-way Internet access, providing the ability to run programs that are otherwise incompatible with NAT routers like the Load Balancer.

- ***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.

  URL Filter

  Use this feature to block access to undesirable Web sites by LAN users. You can even have different settings for different groups of PCs.

- ***Session Limit***

  With Session Limit feature, if the numbers of new sessions for system exceed the maximum in the sampling time, any new session in the system will be drop.

- ***System Filter Exception***

  With firewall exception, the packets will not be processed by firewall or NAT module, but be processed directly by system protocol stack.

Other Features

- ***4-Port Switching Hub***

  The Load Balancer incorporates a 4-port 10 /100BaseT switching hub, making it easy to create or extend your LAN.

- ***DHCP Server Support***

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

- ***Multi Segment LAN Support***

  LANs containing one or more segments are supported, via The Load Balancer's built-in static routing table.

- ***ARP proxy***

  The ARP proxy feature allows you to assign an external (Internet) IP address to The Load Balancer's LAN port. This allows Servers on your LAN to have external (Internet) IP addresses.

- ***Easy Setup***

  Use your favorite WEB browser for configuration.

- ***Remote Management***

  The Load Balancer can be managed from any PC on your LAN. And, if the Internet connection exists, it can also (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 new firmware and backup system configuration from local or even from remote site. As long as you enable “Remote upgrade” and “Remote web-based setup” from Advanced feature web page.

- ***Email Alert***

  It will send a warning email to the system administrator, if one of the WAN ports was disconnected when both WAN ports are enabled.

- ***Syslog***

  It can generate real time system information on the web page or a particular machine. It is useful to monitor the device.

- ***QoS Configuration.***

  This function will make some specified packets with higher priority for pass-through. Especially you use real-time applications like Internet phone, video conference,. etc.

- ***UPnP***

  To “Enable” UpnP (Universal Plug & Play), the load balancer will become one of the network devices. It is useful to discovery and control network devices, such as Internet gateway.

Package Contents

The following items should be included:

- The Load Balancer Unit
- Power Adapter
- Quick Installation Guide
- CD-ROM containing the on-line manual.

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

Physical Details

Front Panel

Figure 1-2: Load Balancer Front Penal

Operation of the Front Panel LEDs is as follows:

LAN	
LINK/ACT	ON – Physical connection or data in/out.
	OFF – No physical connection.
10M/100M	ON – The corresponding LAN port is using 100BaseT.
	OFF – 10BaseT connection on the corresponding LAN port or no connection.
WAN	
LINK/ACT	ON – Physical connection to the Broadband modem on WAN port 1/2 established.
	OFF – No physical connection on WAN port 1/2.
10M/100M	ON – Physical connection using 100BaseT on WAN port 1/2 established.
	OFF – 10BaseT connection or no connection on WAN port 1/2.
System	
Power	OFF – No power.
	ON – Normal Operation
Status	OFF – Normal operation.
	ON – Firmware not loaded or Hardware error.
	Blinking – Data in/out

Also, some Status and Error conditions are indicated by combinations of LEDs, as shown below

LED Action	Condition
WAN1 LINK/ACT & 10M/100M LEDs flash alternatively.	Firmware Download in progress.
WAN1 LINK/ACT & 10M/100M LEDs flash concurrently.	MAC address not assigned.
WAN1 LINK/ACT & 10M/100M LEDs solid On	SDRAM error
WAN2 LINK/ACT & 10M/100M LEDs solid On	Timer/Interrupt error
LAN1 LINK/ACT & 10M/100M LEDs solid On	LAN/WAN error

Rear Panel

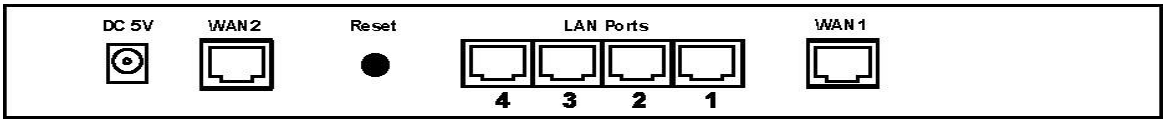

Figure 1-2: Rear Panel

DC 5V	Connect the supplied power adapter here.
WAN 2	Connect the 2nd Broadband Modem here, if available.
Reset Button	When pressed and released, The Load Balancer will reboot (restart) within 1 second. It resets to default over 3 seconds.
LAN Ports	Connect the PCs to these ports. Both 10BaseT and 100BaseT connections can be used simultaneously. **Note:** Any port will automatically operate as an "Uplink" port if required. Just use a normal LAN cable to connect to a normal port on another hub.
WAN 1	Connect the primary Broadband Modem here.

Default Settings

When The Load Balancer 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 Load Balancer is unusable, and you wish to restore it by downloading new firmware. Follow this procedure:

1. Power On The Load Balancer.
2. Use the supplied Windows utility or a TFTP client program applies the new firmware. If using the supplied Windows TFTP program, the screen will look like the following example.

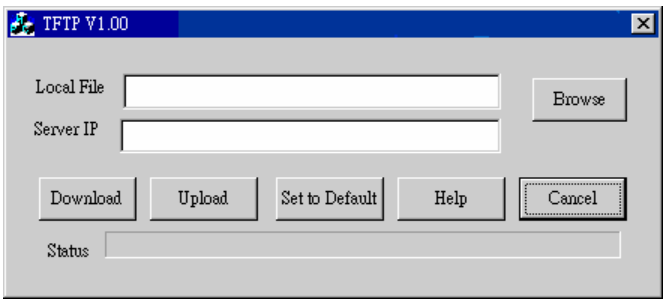

Figure 1-3: Windows TFTP utility

- Enter the name of the firmware upgrade file on your PC, or click the "Browse" button to locate the file.
- Enter the LAN IP address of The Load Balancer in the "Server IP" field.
- Click "Download" to send the file to The Load Balancer.

3. When downloading is finished. It should then work normally, using the default settings.

Note:

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

- Save the current configuration settings to your PC (use the "Upload" button).
- Restore a previously-saved configuration file to The Load Balancer (use the "Download" button).
- Set The Load Balancer to its default values (use the "Set to Default" button).

2: Basic Setup

Overview

Basic Setup of your Load Balancer involves the following steps:

1. Attach The Load Balancer to one (1) PC, and configure it for your LAN.
2. Install your Load Balancer in your LAN, and connect the Broadband Modem or Modems.
3. Configure your Load Balancer for Internet Access.
4. Configure PCs on your LAN to use The Load Balancer.

Requirements

- One (1) or two (2) DSL or Cable modems, each with an Internet Access account with an ISP.
- 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 Load Balancer for your LAN

1. Use a standard LAN cable to connect your PC to any Hub port on The Load Balancer.
2. Connect the power adapter and power up The Load Balancer. Only use the power adapter provided; using a different one may cause hardware damage.
3. Start your PC. If your PC is already running, restart it. It will then obtain an IP address from The Load Balancer.
4. Start 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.

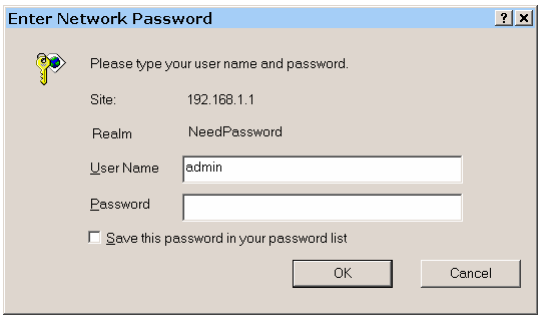

Figure 2-1: Password Dialog

7. Enter *admin* for the "User Name" and leave the "Password" blank.
   - The "User Name" is always *admin*

- You can and should set a password, using the following ***Admin Password*** screen.

No Response ?

- Is your PC using a Fixed IP address ?

  If so, you must configure your PC to use an IP address within the range 192.168.1.2 to 192.168.1.254, with a *Network Mask* of 255.255.255.0. See *Appendix B – Windows TCP/IP Setup* for details.

- Check that The Load Balancer is properly installed, LAN connection is OK, and it is powered ON.

8. After the login, you will then see the ***Admin Password*** screen, as shown below. Assign a password by entering it in the "Password" and "Verify Fields.

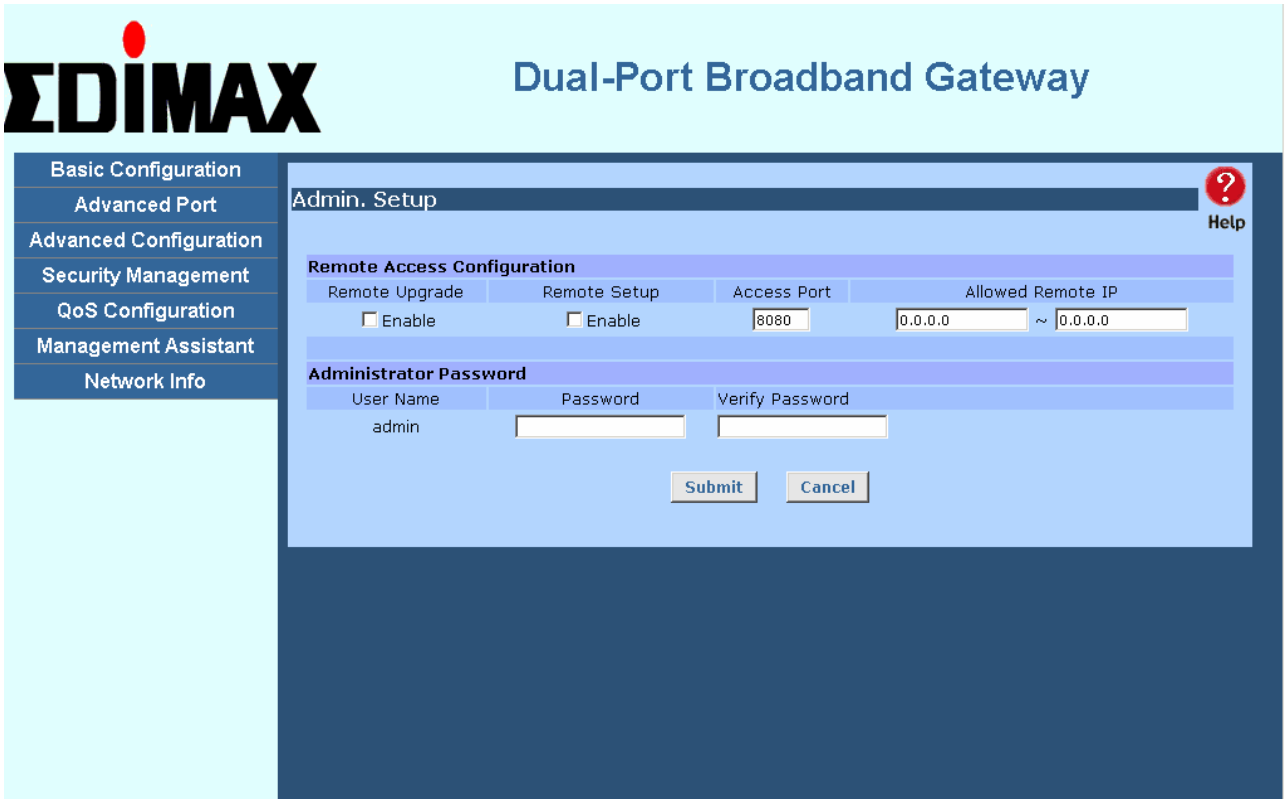

Figure 2-2: Home Screen (Admin Password)

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

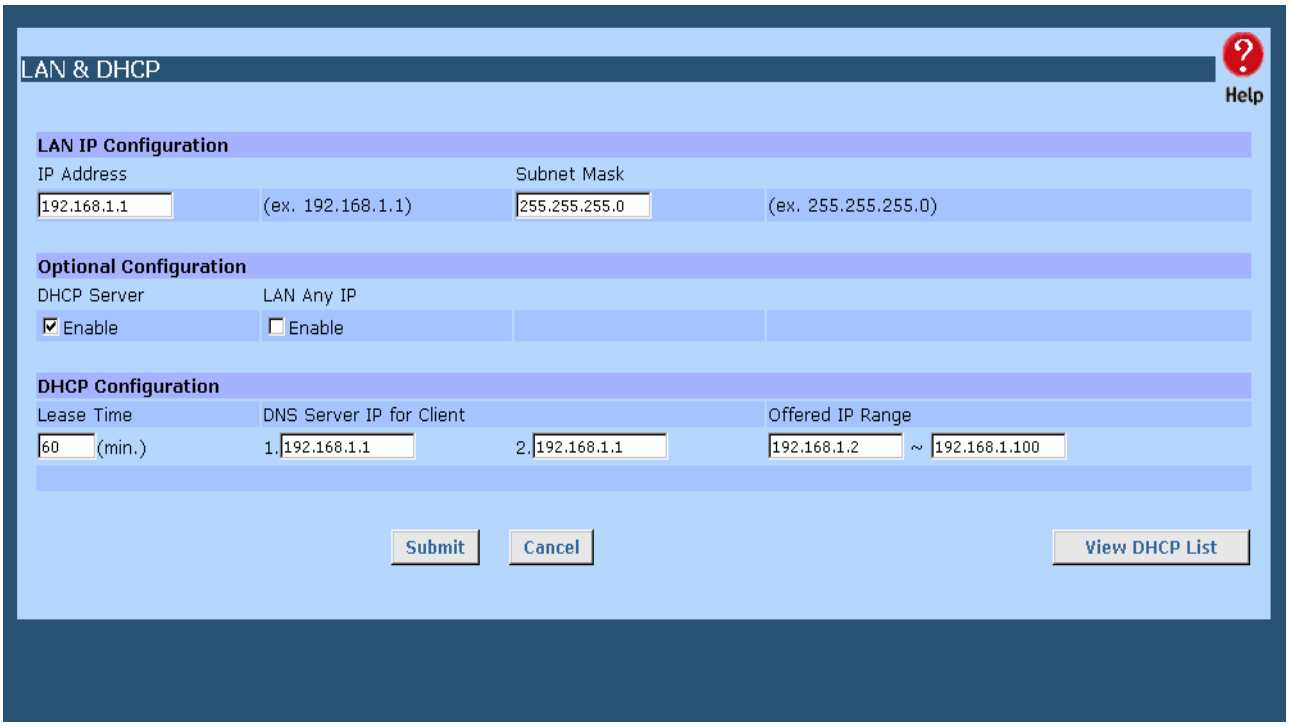

Figure 2-3: LAN & DHCP

10. Ensure these settings are suitable for your LAN:
    - The default settings are suitable for many situations.
    - See the following table for details of each setting.
11. Save your data, then go to *Step 2, Installing The Load Balancer in your LAN*.

Settings – LAN & DHCP

LAN IP Configuration	• **IP address -** for the Load Balancer, 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. In the latter case, enter an unused IP Address from within the range used by your LAN. • **Subnet Mask -** 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 Load Balancer is attached (the same value as the PCs on that LAN segment).
Optional Configuration	• **DHCP Server Setup** - If **Enabled**, the Load Balancer will allocate IP Addresses to 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 is called *Obtain an IP address automatically*.) If you are already using a DHCP Server, the DHCP

	Server setting must be **Disabled**, and the existing DHCP server must be set to provide the IP address of the Load Balancer as the *Default Gateway*. • **LAN Any IP** –By default is disabled. If you enable “LAN Any IP”, that means no matter what static IP address hold on the client (your PC). The client has do not need to change the IP address, even though it has different IP segment than LAN segment. It still can access Internet through NAT.
DHCP Configuration	• **Lease Time** – It is a finite period of time for a DHCP server lease an IP address to a client.. • **DNS Server IP for Client** – An IP address of the default DNS server for the client requesting DHCP service. • **Offered IP Range** 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.
DHCP Free List	• **Free Entry** indicates how many DHCP entries are not currently allocated, and still available. This table shows the IP addresses which have been allocated by the DHCP Server function. For each address which has been allocated, the following information is shown. • **Name** – The "hostname" of the PC. In some cases, this may not be known. • **MAC Address** – The physical address (network adapter address) of the PC. • **IP Address** – The IP address allocated to this PC. • **Type** – Indicates IP address to be dynamic or static. • **Status** – 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** – The time expired since which IP address is leased.

2. Installing The Load Balancer in your LAN

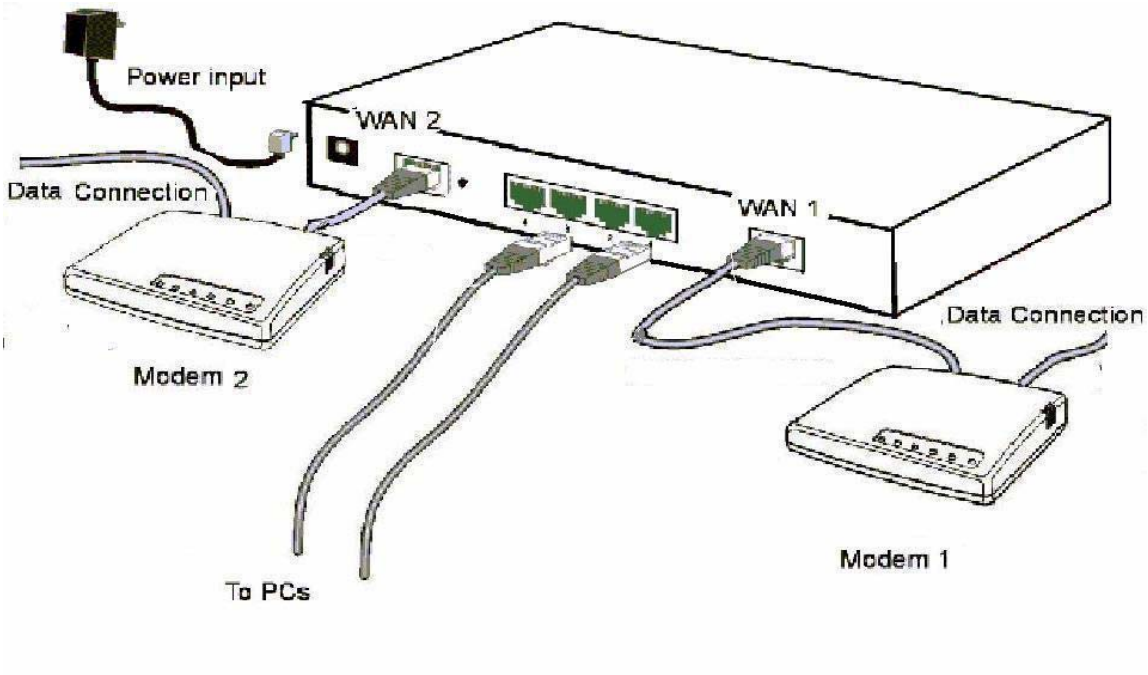

Figure 2-4: Installation Diagram

1. Ensure The Load Balancer and the DSL/Cable modem are powered OFF.
   Leave the modem or modems connected to their data line.
2. Connect the Broadband modem or modems to The Load Balancer.
   - If using only one (1) Broadband modem, connect it to the "WAN 1" port.
   - 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 Switching Hub ports on The Load Balancer.
   - Both 10BaseT and 100BaseT connections can be used simultaneously.
   - If you need to connect The Load Balancer to another Hub, just use a standard LAN cable to connect any port on The Load Balancer to a standard port on another hub. Any LAN port on The Load Balancer will automatically act as an "Uplink" port when required.
4. Power Up
   - Power on the Cable or DSL modem or modems.
   - Connect the supplied power adapter to The Load Balancer and power up.
5. Check the LEDs
   - The ***Power*** LED should be ON.
   - The ***WAN – Link*** LED should be ON, if the corresponding WAN port is connected to a broadband modem.
   - The ***Error*** LED will flash during start up, but will then turn Off. If it stays On, there is an error condition.

- For each PC connected to the LAN ports, the corresponding ***LAN*** LED (either ***10*** or ***100***) should be ON.

3. Configuring The Load Balancer for Internet Access

Select *Primary Setup* from the menu, to see a screen like the example below.

- Configure WAN 1 and/or WAN 2 as required.
- For any of the following situations, refer to ***Chapter 3: Advanced Port Setup*** for any further configuration, which may be required.
  - Using both ports
  - Multiple IP addresses on either port
  - Multiple PPPoE sessions
  - PPTP connection method

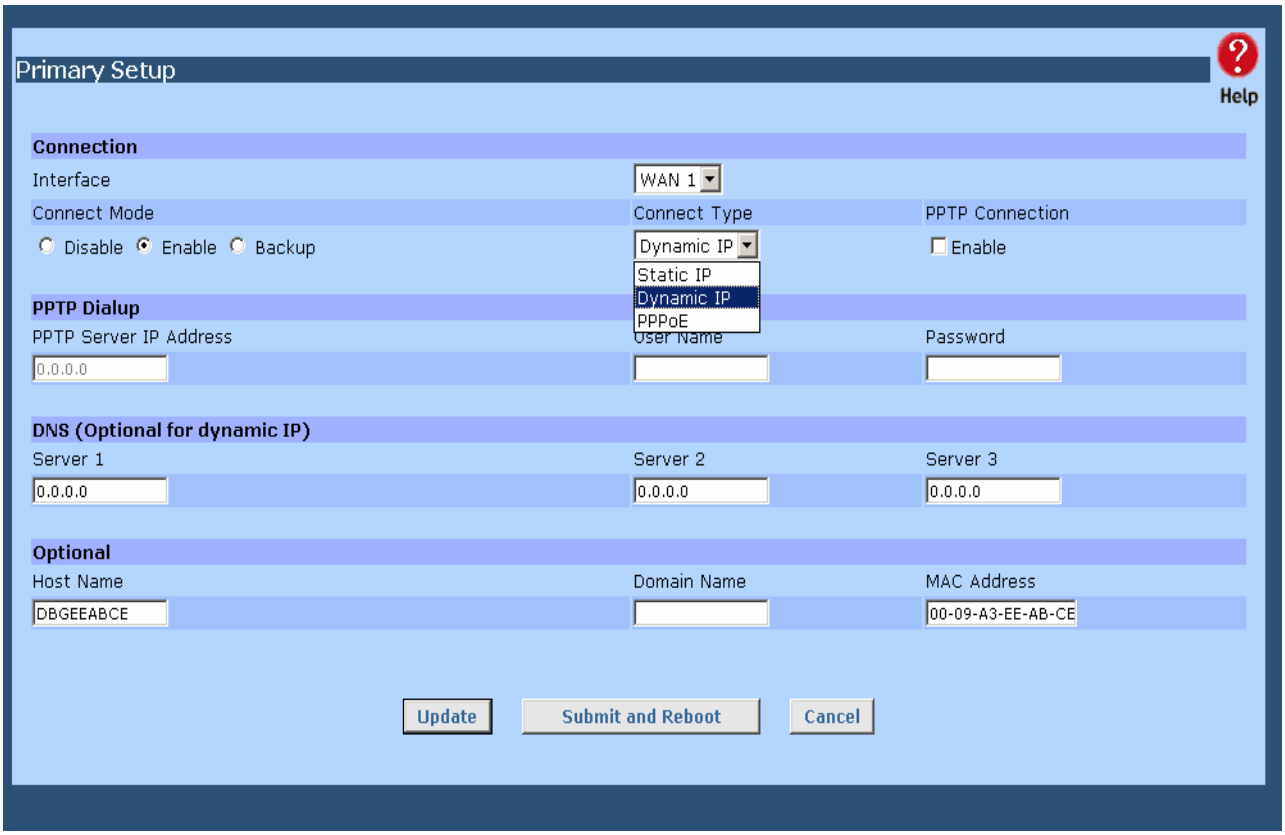

Figure 2-5: Primary Setup

Settings – Primary Setup

Connection	• **Interface** – Select which WAN (WAN1 or WAN2) to be setup. • **Connection Mode** Select the appropriate setting: • **Enable** – Select this if you have connected a broadband modem to this port. • **Disable** – Select this if there is no broadband modem connected to this port. • **Backup** – Use this if you have a broadband modem on each port, and wish to normally use only one. Select *Enable* for the primary port, and *Backup* for the secondary port. The *Backup* port will only be used if the primary port fails. • **Connection Type** Check the data supplied by your ISP, and select the appropriate option. • **Static IP** – Select this if your ISP has provided a Fixed or Static IP address. Then enter the data into the *Address Info* fields. • **Dynamic IP** – Select this if your ISP provides an IP address automatically, when you connect. You can ignore the *Address Info* fields. • **PPPoE** – Select this if your ISP uses this method. (Usually, your ISP will provide some PPPoE software. This software is no longer required, and should not be used.) If this method is selected, you must complete the *PPPoE dialup* fields. • **PPTP Connection** – This is for *PPTP* users only. • **1.** Enter the *Username* and *Password* provided by your ISP. • **2.** If using PPTP, enable the *PPTP Connection* checkbox, and enter the IP address of the PPTP server. **Note:** If using the PPTP connection method, 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 provided by your ISP. If your ISP provided multiple IP address, you can use the ***Multi-DMZ*** screen to assign the additional IP addresses.
DNS (Optional for dynamic IP)	If using a *Fixed IP* address, you MUST enter at least 1 DNS address. If using *Dynamic IP* or *PPPoE*, DNS information is optional.

Optional	• **Host name** – 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** – 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** – Some ISP's record 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 Load Balancer is now complete. PCs on your LAN must now be configured. See the following section for details.

4: Configure PCs on your LAN

Overview

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

- TCP/IP network settings
- Internet Access configuration

TCP/IP Settings

If using the default Load Balancer 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 Load Balancer 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 is called *Obtain an IP address automatically*.
  Just start (or restart) your PC, and it will obtain an IP address from The Load Balancer.
- If using fixed IP addresses on your LAN, or you wish to check your TCP/IP settings, refer to ***Appendix B – Windows TCP/IP Setup***.

Internet Access

To configure your PCs to use The Load Balancer 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 click the *Setup* button.
3. Select "I want to set up my Internet connection manually, or I want to connect through a local area network (LAN)" and click *Next*.
4. Select "I connect through a local area network (LAN)" and click "*Next"*.
5. Ensure 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 and Internet Connections.
2. Select *Set up or change your Internet Connection*.
3. Select the *Connection* tab, and click the *Setup* button.
4. Cancel the pop-up "Location Information" screen.
5. Click *Next* on the "New Connection Wizard" screen.
6. Select "Connect to the Internet" and click "*Next"*.

7. Select "Set up my connection manually" and click “*Next”*.
8. Check "Connect using a broadband connection that is always on" and click *Next*.
9. Click *Finish* to close the New Connection Wizard.
   Setup is now completed.

Accessing AOL

To access AOL (America On Line) through The Load Balancer, 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 "Load Balancer".
- Click *Edit Location*. Select *TCP/IP* for the *Network* field. (Leave the *Phone Number* blank.)
- Click *Save*, then *OK*.
  Configuration is now complete.
- Before clicking "Sign On", always ensure that you are using the "Load Balancer" location.

Macintosh Clients

From your Macintosh, you can access the Internet via The Load Balancer. The procedure 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 Load Balancer’s IP Address.
- Ensure your *DNS* settings are correct.

Linux Clients

To access the Internet via The Load Balancer, it is only necessary to set The Load Balancer 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 Load Balancer.
- Ensure your *DNS* (Name server) settings are correct.

To act as a DHCP Client (recommended)

The procedure below may vary according to 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.

   OR, restart your system.

3: Advanced Port Setup

Overview

- ***Port Options*** contains some options, which can be set on either or both WAN ports. For most situations, the default values are satisfactory.
- ***Load Balance*** screen is only functional if you are using both 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 one or both of the WAN ports. 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

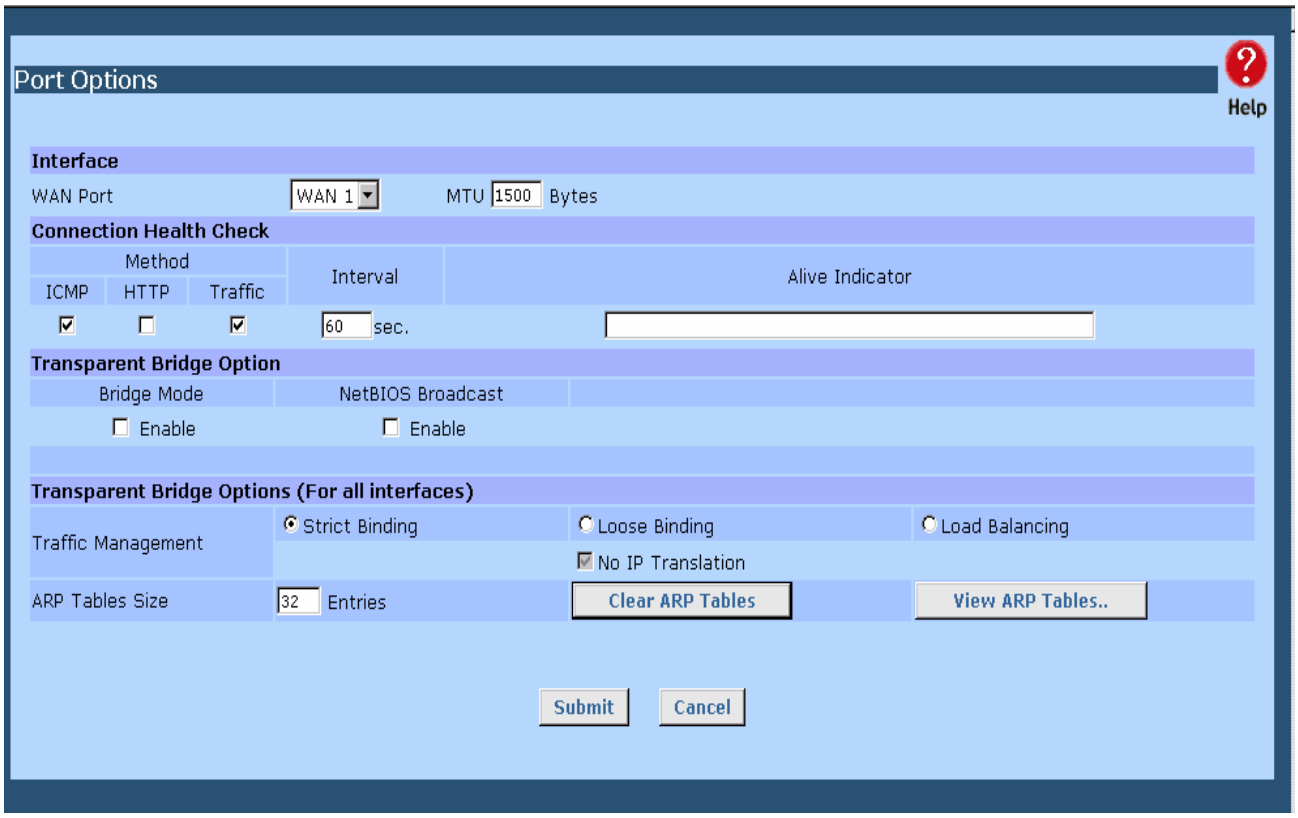

Figure 3-1: Port Options

Settings – Port Options

Interface	• **WAN Ports** – To select the WAN port for option settings • **MTU** –The largest amount of data that can be transferred across a given physical network. Ethernet limits transfers to **1500** octets of data. Normally, you should leave this value at its default value. Change it only if the ISP is providing a MTU that is not optimal
Connection Health Check	• Method – **ICMP:** The health check is performed by sending an ICMP echo request packet to the specific destination. The specific destination ("Alive Indicator") could be either: 1. If the input box is filled (NAME or IP address): the host is used. 2. If the input box is left blank: gateway of WAN interface will be used. Then if one ICMP echo reply packet from Alive Indicator or gateway is received, the connection is considered OK. If there is no response received after 4 tries, the connection is considered as failed. **HTTP:** The device gets TCP connection with the Alive Indicator first. Then the device sends HTTP HEAD packet to the Alive Indicator. If any HTTP DATA from the Alive Indicator is received, the connection is considered OK. If there are no response received after 5 tries, the connection is considered as failed. **Traffic:** If there is no traffic on the WAN port in the Interval time, the connection is considered as failed • **Interval** – The period to check if the WAN port is alive or not. • **Alive Indicator** – This is used for the ICMP or HTTP Method to determine if your Internet connection is active or not. (You can enter either the IP address or host name
Transparent Bridge Option	• **Bridge Mode** – If Set to Enable, traffic from Lan hosts with real IPs can go through the specific WAN port without NAT translation. This device works like a bridge switch for that specific WAN port. • **NetBIOS Broadcast** – If enabled, NetBIOS Broadcast packets are allowed to pass through the device

Transparent Bridge Option (for all interface)	• **Traffic Management** – **Strict binding:** Traffic from bridge hosts (eg. transparent to WAN1) can only go through that a specified WAN (eg. WAN1) interface. **Loose binding:** Traffic from bridge hosts (eg. transparent to WAN1) can go through an alternative WAN (eg. WAN2) interface when binded interface (eg. WAN1) is down. It acts like a failover mechanism for Transparent Bridge mode. **Load Balancing:** Traffic from bridge hosts (eg. transparent to WAN1) can go through either WAN (eg. WAN1 or WAN2) interface based on the loading mechanism specified in the Load Balance section. It acts like a load balancing mechanism for Transparent Bridge mode. **No IP Translation:** When Bridge mode is set to Loose binding or Load Balancing, traffic from bridge hosts (eg. transparent to WAN1) can go through an alternative WAN (eg. WAN2) interface with its original IP (if checked) or with an alternative WAN IP (if unchecked). That is, NAT is performed. • **ARP Table** – ARP Table is used by the device to determine the bridge hosts location (eg. inside/outside WAN and which WAN). Its size can be adjusted if needed.

Load Balance

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

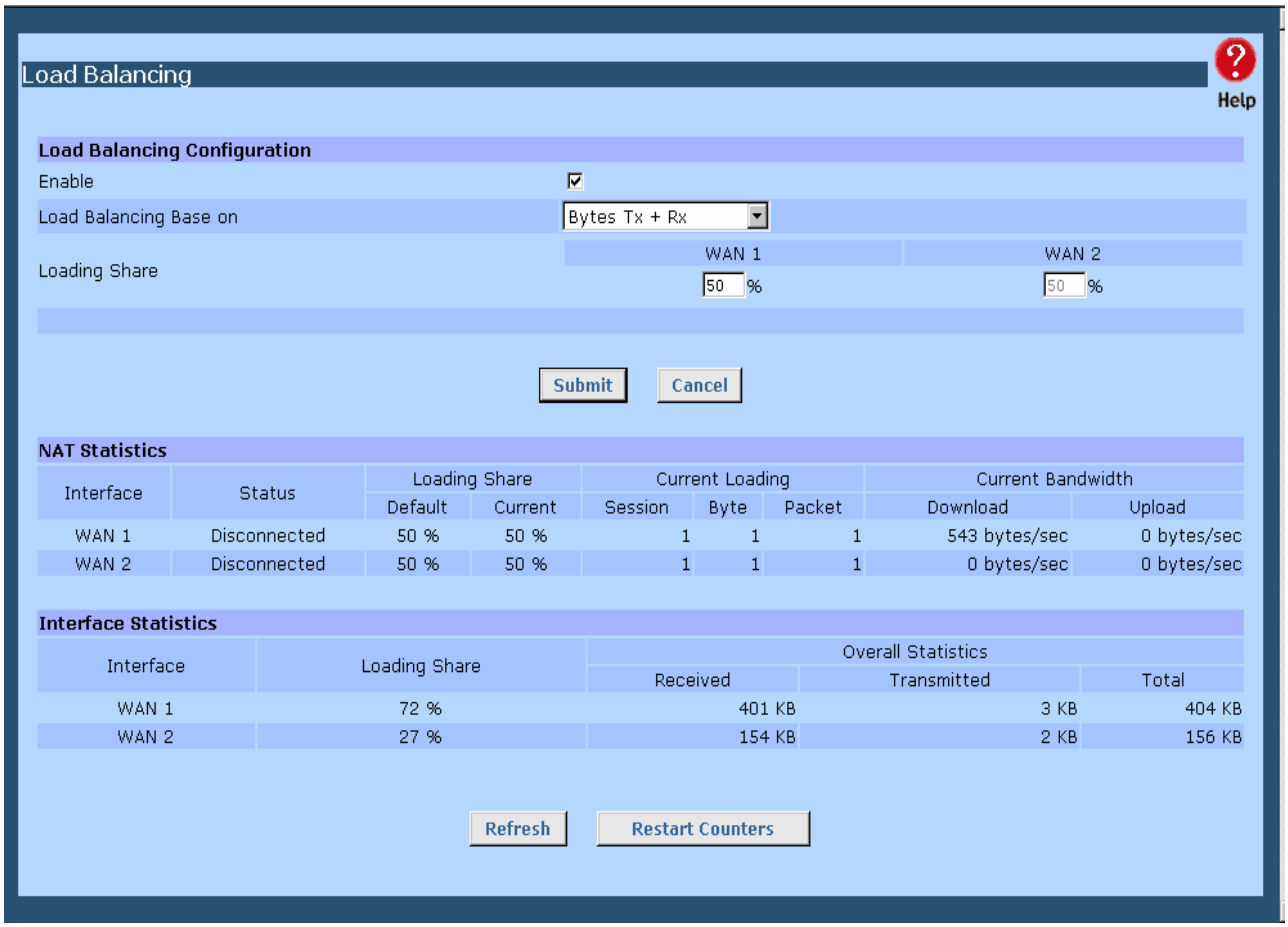

Figure 3-2: Load Balance

These settings are only functional if using both WAN ports. If using both WAN ports, these settings determine the proportion of traffic sent over each port.

Settings – Load Balance

Load Balance Configuration	• **Enable** – This will allow you enable or disable the load-balancing feature. • **Load Balancing Base On** – Select the desired option to measure the traffic load. **1. Bytes Tx + Rx**: The link with the least number of bytes transmitted through the WAN port. **2. Packets Tx + Rx**: The link with the least number of packets transmitted through the WAN port. **3. Sessions Established**: The link with the least number of sessions built on the WAN port. **4. IP Addresses**: The link with the least number of Host IP addresses built on the WAN port. • **Loading Share** –Enter the desired percent of traffic load for each WAN port
NAT Statistics	This section displays the current data about WAN 1 and WAN 2. 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 these counters when required.

Advanced PPPoE

The 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.

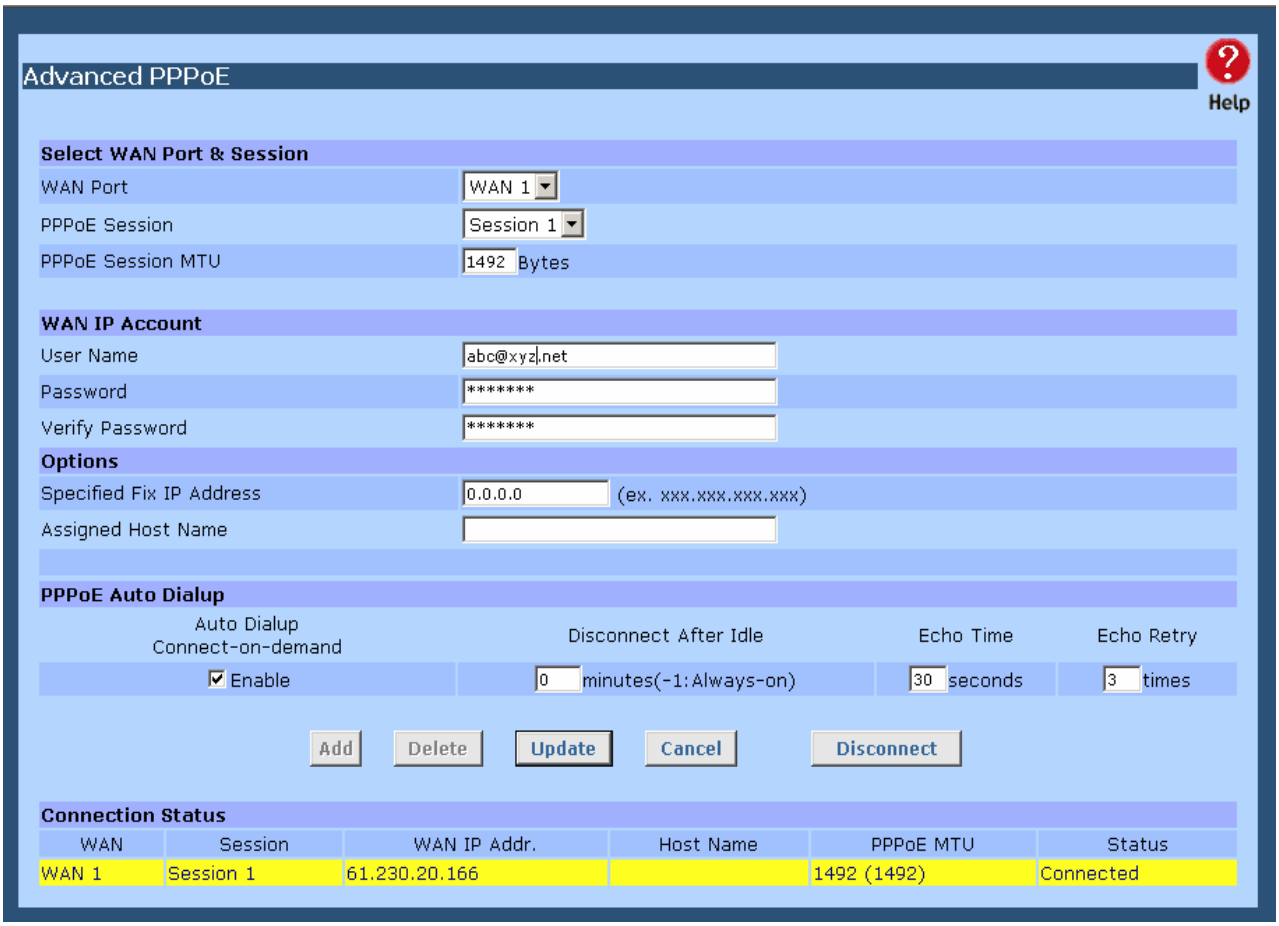

Figure 3-3: Advanced PPPoE

Settings – Advanced PPPoE

Select WAN Port & Session	• **Select WAN Port & PPPoE Session** – Select the desired WAN port and PPPoE session from the pull-down menu and click the **Select** button. The screen will then show the data for the selected Port/Session. Input the required data and click **Update** to save your changes • **PPPoE Session MTU** –The Maximum Transmission Unit for the PPPoE session. The default value is 1492 bytes.
WAN IP Account	• **User Name** – Enter the PPPoE user name assigned by your ISP. • **Password** – Enter the PPPoE password assigned by your ISP. • **Verify Password** – Re-enter the PPPoE password assigned by your ISP.
Options	• **Specified Fix IP Address** – If you have a fixed IP address, enter if here. Otherwise, this field should be left at 0.0.0.0. • **Assigned Host Name** – This field is used by a Host to uniquely associate an access concentrator to a particular Host request.
PPPoE Auto Dialup	• **Auto Dialup Connect-on-demand** – To enable or disable auto dialup for a PPPoE connection. If you decide not to use auto dialup or auto disconnect, then you have to connect/disconnect manually. • **Disconnect After Idle** – To decide the timeout for disconnecting when there is no traffic on the connection. Enter **-1** to keep the connection always **alive**. Enter **0** to enable 'dial on demand by trigger'. • **Echo Time** –To determine how often an Echo request is sent to the PPPoE server. Normally, leave this setting at its default value. • **Echo Retry** –To determine the maximum number times that the Echo request is allowed to be sent to the PPPoE server until a response is received. Normally, leave this setting at its default value.
Connection Status	This displays the current connection status for each session.

Advanced PPTP

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

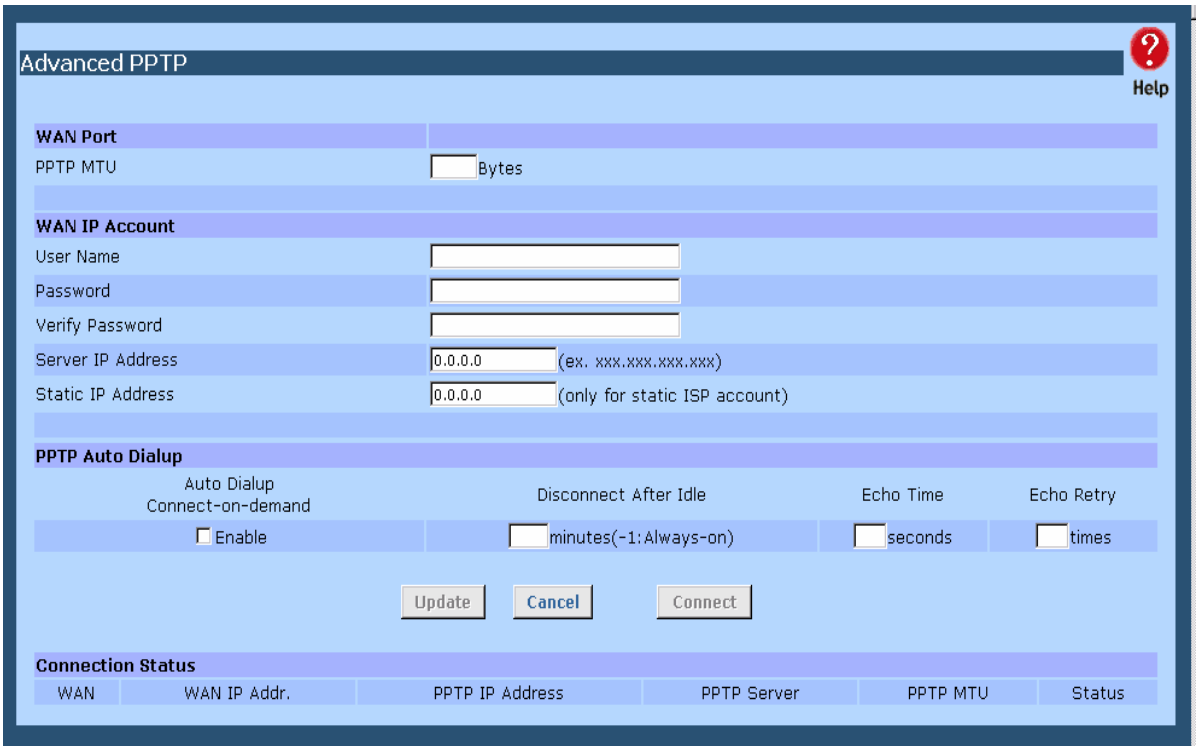

Figure 3-4: Advanced PPTP

Settings – Advanced PPTP

WAN Port	Used if you choose PPTP on Static/Dynamic IP as your connection setup from primary setup. You may use PPTP manual dialup in this page or use Port Options for auto dialup on demand or always connected • **PPTP MTU** –The default value is 1460 (bytes), the same as the maximum PPTP MTU for this device
WAN IP Account	• **User Name** – The PPTP user name (login name) assigned by your ISP. • **Password** – 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** – Re-enter the PPTP password assigned by your ISP. • **Server IP Address** – Enter the IP address of the PPTP Server, as provided by your ISP. • **Static IP Address** – 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** –To enable or disable auto dialup for a PPTP connection. If you decide not to use auto dialup or auto disconnect, then you have to connect/disconnect manually. • **Disconnect After Idle** –To decide the timeout for disconnecting when there is no traffic on the connection. Enter **-1** to keep the connection always **alive**. Enter **0** to enable 'dial on demand by trigger'. • **Echo Time** –To determine how often an Echo request is sent to the PPTP server. Normally, leave this setting at its default value. • **Echo Retry** –To determine the maximum number times that the Echo request is allowed to be sent to the PPTP server until a response is received. Normally, leave this setting at its default value.
Connection Status	This displays the current connection status for PPTP

4: Advanced Configuration

Overview

The following advanced features are provided.

- Host IP Setup
- Routing
- Virtual Servers
- Special Applications
- Dynamic DNS
- Multi DMZ
- UpnP
- NAT Setup
- ARP Statp
- Advanced Features

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

Host IP Setup

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 be identified by using the ***Host IP Setup*** screen.
- You wish to have different ***URL Filter*** settings for different PCs. This requires that each PC be identified by using the ***Host IP Setup*** screen. (You do not have to use the Host IP feature to apply the same ***URL Filter*** 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 (Windows calls this "Obtain an IP address automatically") while gaining the benefits of a fixed IP address. The PC's IP address will never change, so it can be provided to other people and applications.

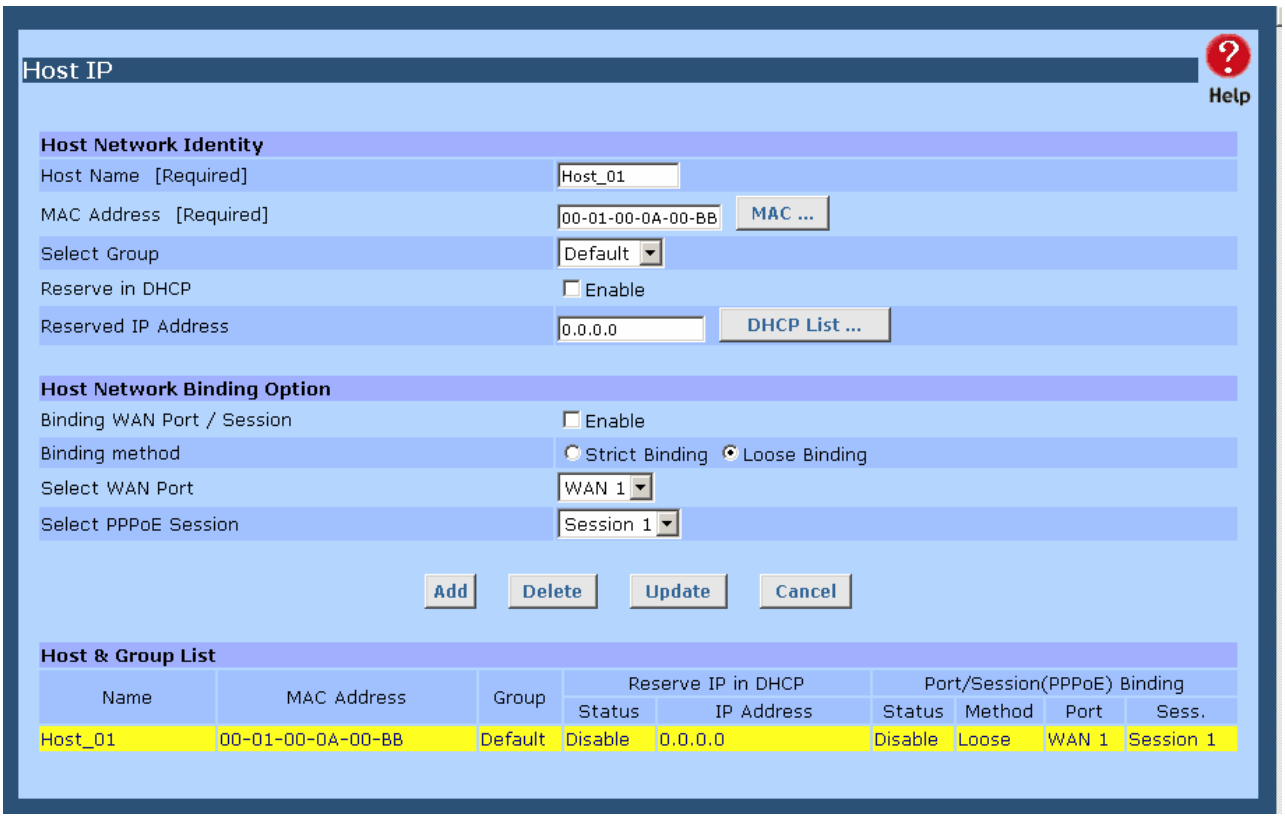

Figure 4-1: Host IP Setup

Settings – Host IP Setup

Host Network Identity	This section identifies each Host (PC) • **Host name** – Enter a suitable name. Generally, you should use the "Hostname" (computer name) defined on the Host itself. • **MAC Address** – Also called *Physical Address* or *Network Adapter Address*. Enter the MAC address of this host. • **Select Group** – Select the group you wish to put this host into. • **Reserve in DHCP** – Select *Enable* to reserve a particular (LAN) IP address for a particular PC on your LAN. This allows the PC to use DHCP (Windows calls this "obtain an IP address automatically") while having an IP address which never changes. • **Reserved IP** – Enter the IP address you wish to reserve, if the setting above is *Enable*. Otherwise, ignore this field.

Host Network Binding	• **Bind WAN port/Session** – 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** – Suppose your PC is bound to WAN1 port, now you are selecting “Strict Binding”. If WAN1 port is disconnected, your packets cannot go out through WAN2 port, if WAN2 port is still alive. If you are selecting “Loose Binding” then when WAN1 port is disconnected, your packets will automatically go to WAN2, if WAN2 is alive. • **Select WAN Port/Select PPPoE session** – If the setting above is *Enable*, select the desired Port and Session. Otherwise, ignore these settings. **Note**: Multiple PPPoE sessions are defined on the ***Advanced PPPoE*** screen.
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.

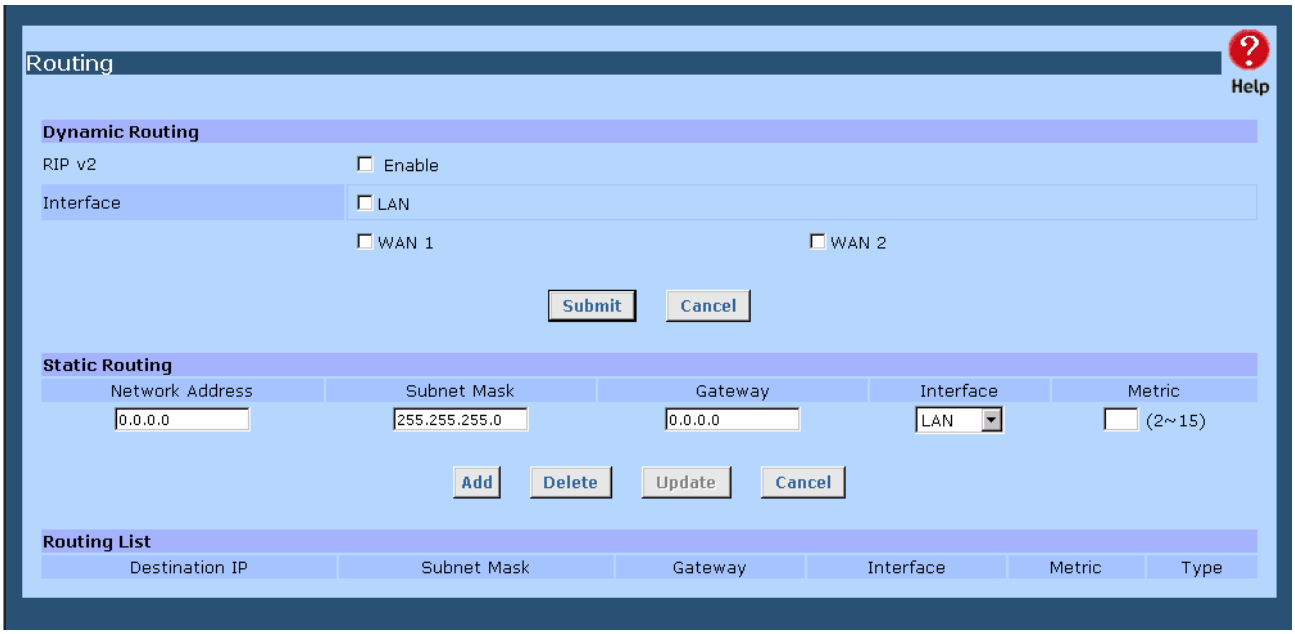

Figure 4-2: Routing

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 – Routing

Dynamic Routing	• **RIP v2** – RIP is a dynamic routing protocol which is used to direct traffic over the network. Disable it if you don't need to use it. • **LAN, WAN1, WAN2** – If enabled, any WAN or LAN can execute RIP function.
Static Routing	If there is more than one router on a network, this Routing table must be configured because the router needs to know what packet goes to which router. A routing table entry is required for each LAN segment on the network • **Network Address** – Network Address is the address of the destination network segment. • **Netmask** –The subnet mask used to select the bits from an IP Address that corresponds to the subnet. • Gateway –The IP router that the packets destined for the subnet with **Network Address** will be forwarded to. • **Interface** – The device's port that the packets destined for the subnet with Network Address will be passed through. • **Metric** – The number of routers that must be traversed to reach the destination network segment
Routing List	List of static route that you configured previously.

Configuring Other Routers on your LAN

All traffic for devices not on the local LAN must be forwarded to The Load Balancer, so that they can be forwarded to the Internet. This is done by configuring other Routers to use The Load Balancer as the *Default Route* or *Default Gateway*, as illustrated by the example below.

Static Routing - Example

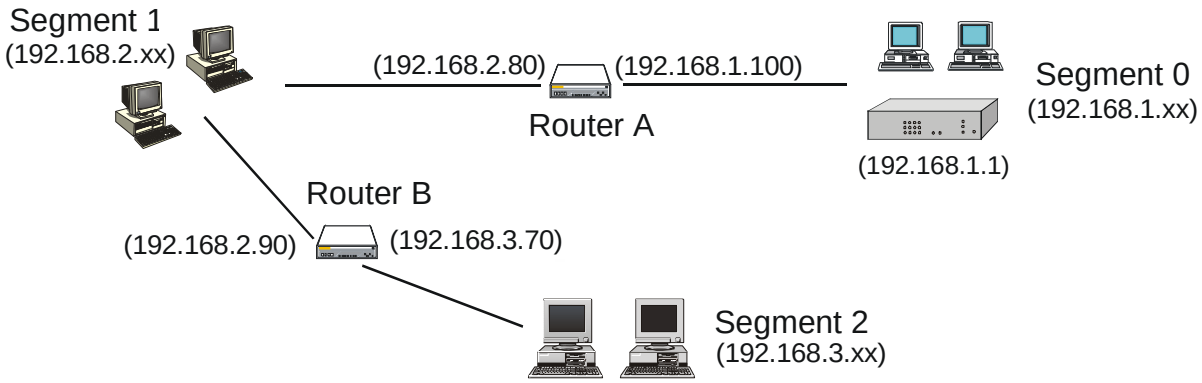

Figure 4-3: Routing Example

For The Load Balancer Gateway's Routing Table

For the LAN shown above, with 2 routers and 3 LAN segments, The Load Balancer 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 Servers

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 Load Balancer.

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

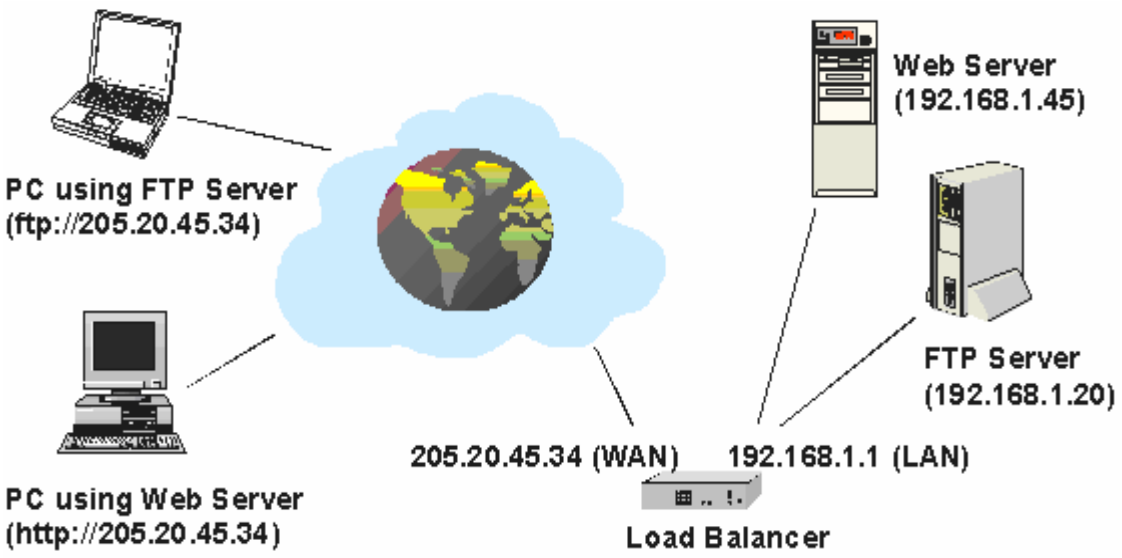

Figure 4-4: Virtual Servers

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

Connecting to the Virtual Servers

Once configured, anyone on the Internet can connect to your Virtual Servers. They must use The Load Balancer'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`

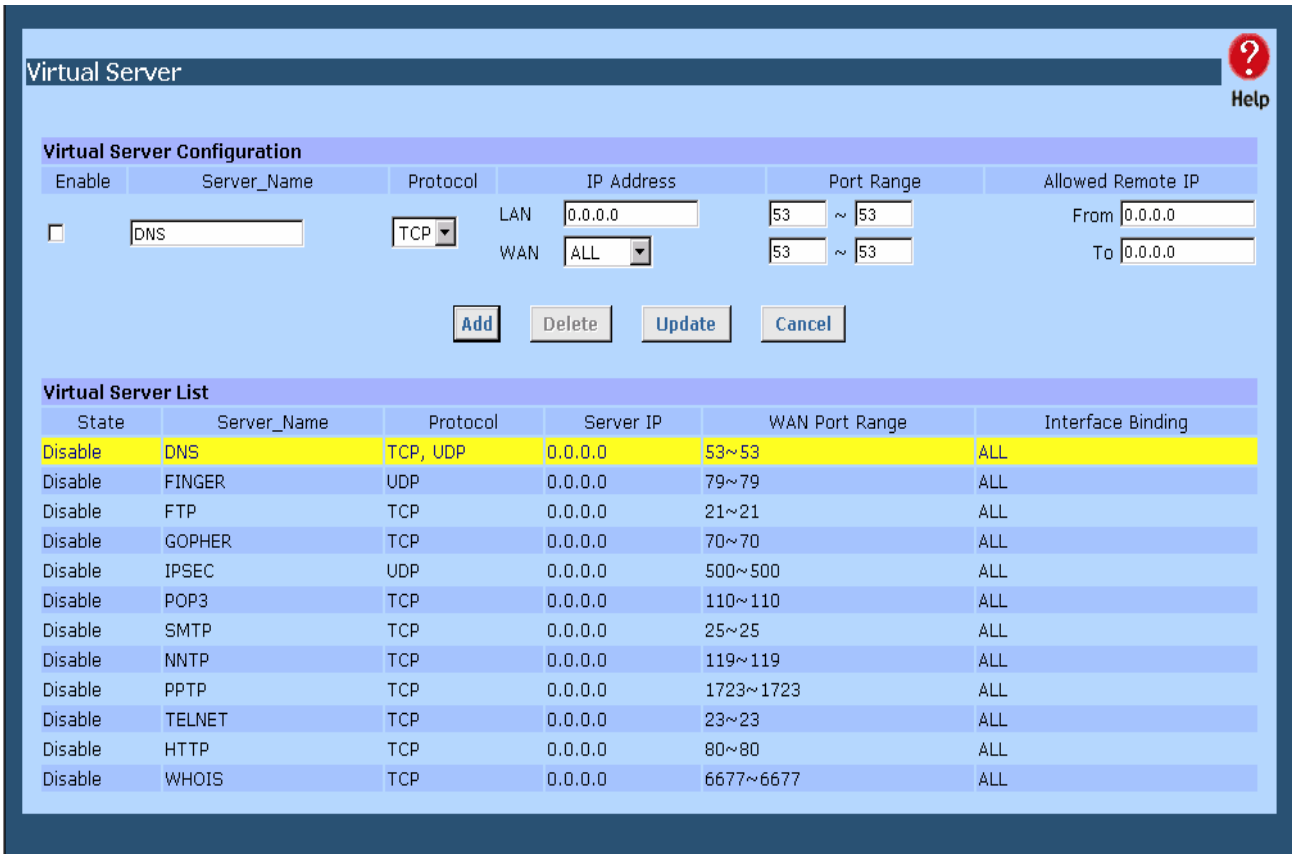

Figure 4-5: Virtual Server

Settings – Virtual Server

Virtual Server Configuration	• **Enable** – To activate or deactivate the current entry. • **Server Name** – A unique name for identifying the virtual server. • **Protocol** – Select the protocol (either TCP or UDP) used by the server software. • **IP Address** – **LAN:** Enter the IP address of the server on the device's LAN side. The hosts used as Virtual Servers need static IP addresses or reserved IP addresses. **WAN:** The WAN port that the virtual server is bound on. • **Port Range** – **LAN:** The range of port numbers used by the server. If only one port number is used, fill the same number in both starting and ending fields. **WAN:** The range of port numbers for users in public to access the virtual server. If only one port number is used, fill the same number in both starting and ending fields. • **Allowed Remote IP** –The range of IP addresses that are allowed to access the virtual server.
Virtual Server List	The Virtual Server List shows details of all Virtual Servers which have been defined.

Special Applications

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 Load Balancer. 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

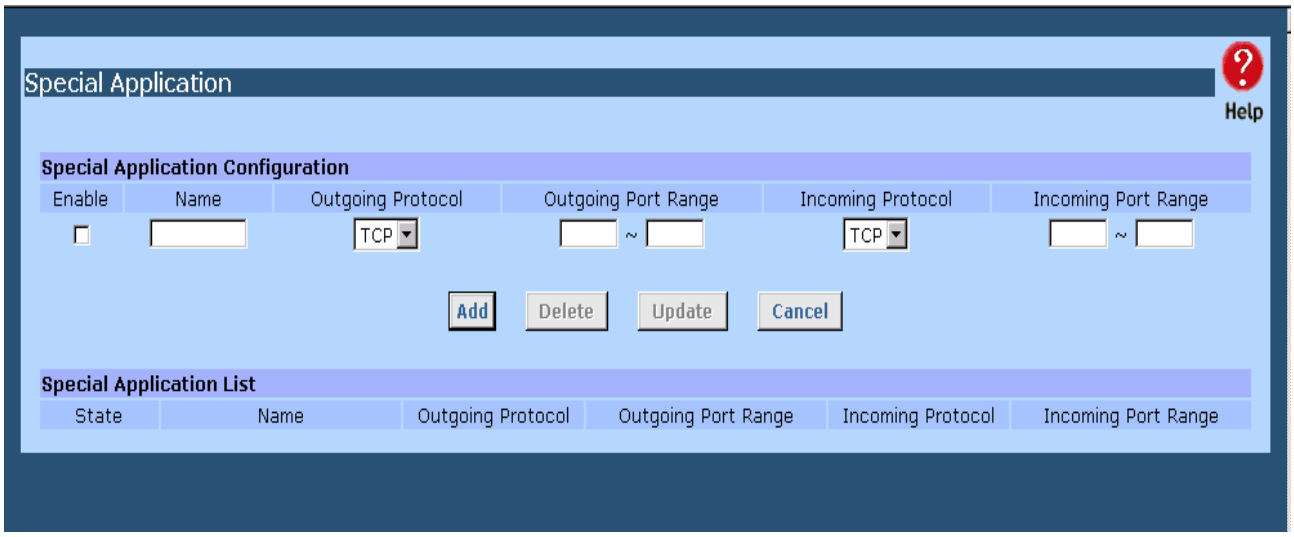

Figure 4-6: Special Applications

Settings – Special Applications

Special Application Configuration	• **Enable** – Use this to Enable or Disable this Special Application as required. • **Name** – Enter a descriptive name to identify this Special Application. • **Outgoing Protocol** –Select the protocol used by this application, when sending data to the remote server or PC. • **Outgoing Port Range** – 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** – Select the protocol used by this application, when receiving data from the remote server or PC. • **Incoming Port Range** – 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.
Special Application List	This shows details of all Special Applications which are currently defined.

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 whenever you connect to your ISP, which makes it difficult to connect to you.

You must register for the Dynamic DNS service. The Load Balancer supports 2 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 Load Balancer 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.

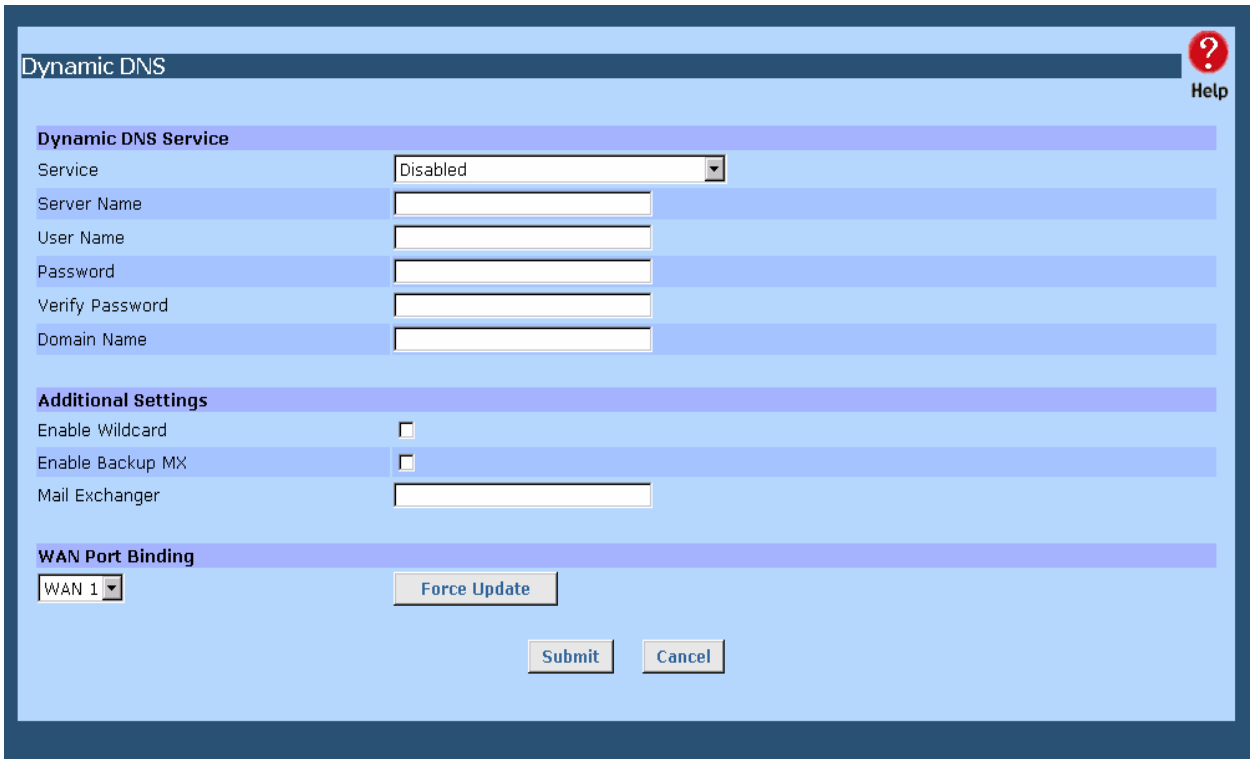

Figure 4-7: Dynamic DNS

Settings – Dynamic DNS

Dynamic DNS Service	Use this to Enable/Disable the Dynamic DNS feature, and select the required service provider. • **Disable** – Dynamic DNS is not used. • **TZO** – Select this to use the TZO service (www.tzo.com). You must configure the *TZO* section of this screen. • **Standard Client** – 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)** – This is available in China. It is similar to “Standard client” • **User Defined DDNS Server** – This is the user define DDNS server. If the DDNS other than TZO, dyndns.org and 3322.
Additional Settings	These options are available if using the standard client. • **Enable Wildcard** – If selected, traffic sent to sub-domains (of your Domain name) will also be forwarded to you. • **Enable backup MX** – If enabled, you must enter the *Mail Exchanger* address below. • **Mail Exchanger** – If the setting above is enabled, enter the address of the backup Mail Exchanger.
WAN Port Binding	Select the WAN port on which the Dynamic DNS is used. 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 attacks. For this reason, you should only enable the DMZ feature when required

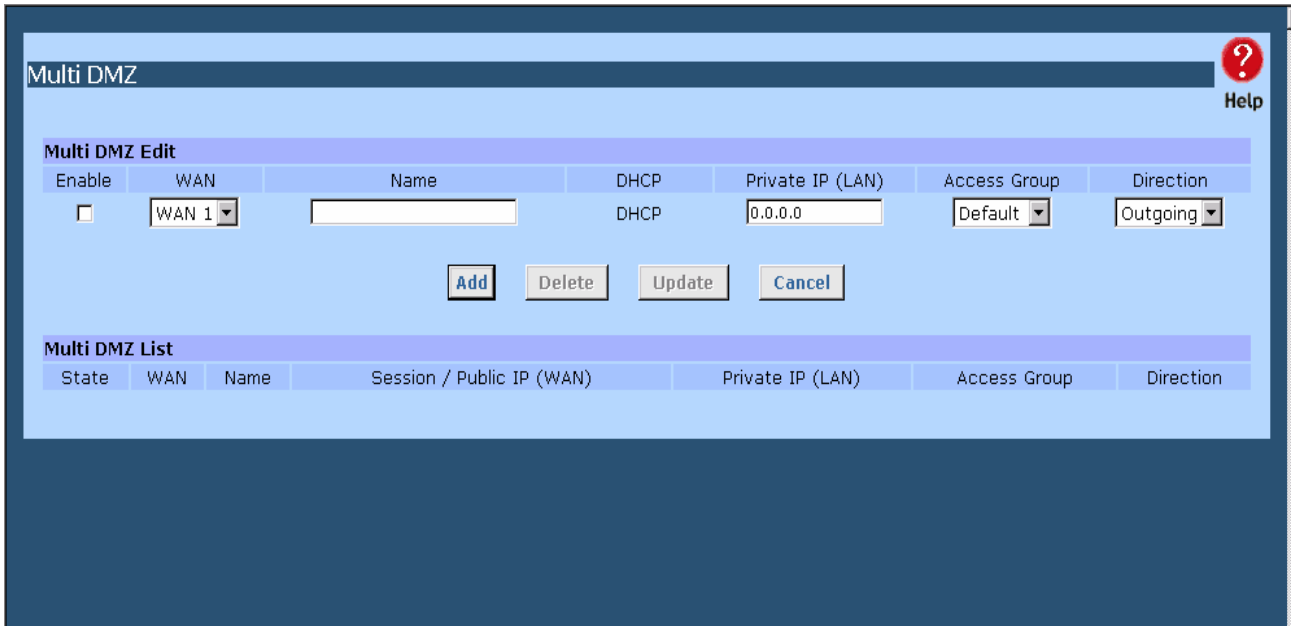

Figure 4-8: Multi DMZ

Settings – Multi DMZ

Multi DMZ Edit	• **Enable** – To activate or deactivate the current DMZ entry.
	• **WAN** – The WAN (WAN1, WAN2) port applied to the current DMZ entry.
	• **Name** – To identify the current DMZ entry.
	• **Public IP** –The public IP (or PPPoE session) that the current DMZ entry is bound on.
	• **Private IP (LAN)** –The IP address of the server in the DMZ
	• **Access Group** –To specify which Access Group will be applied. Each Access Group has its own access rules.
	  • **Default :** Applies the access rules for the Default Group.
	  • **Group1** ~ **Group4 :** Applies the access rules for Group1~Group4, respectively
	• **Direction** –To specify in which direction the Access Group will be applied: Outgoing, Incoming, Both.

Multi DMZ List	The List shows details of all DMZ that are currently defined.

UPnP

With UPNP (Universal Plug & Play) function, it can easily setup and configure an entire network, enable discovery and control of networked devices and services.

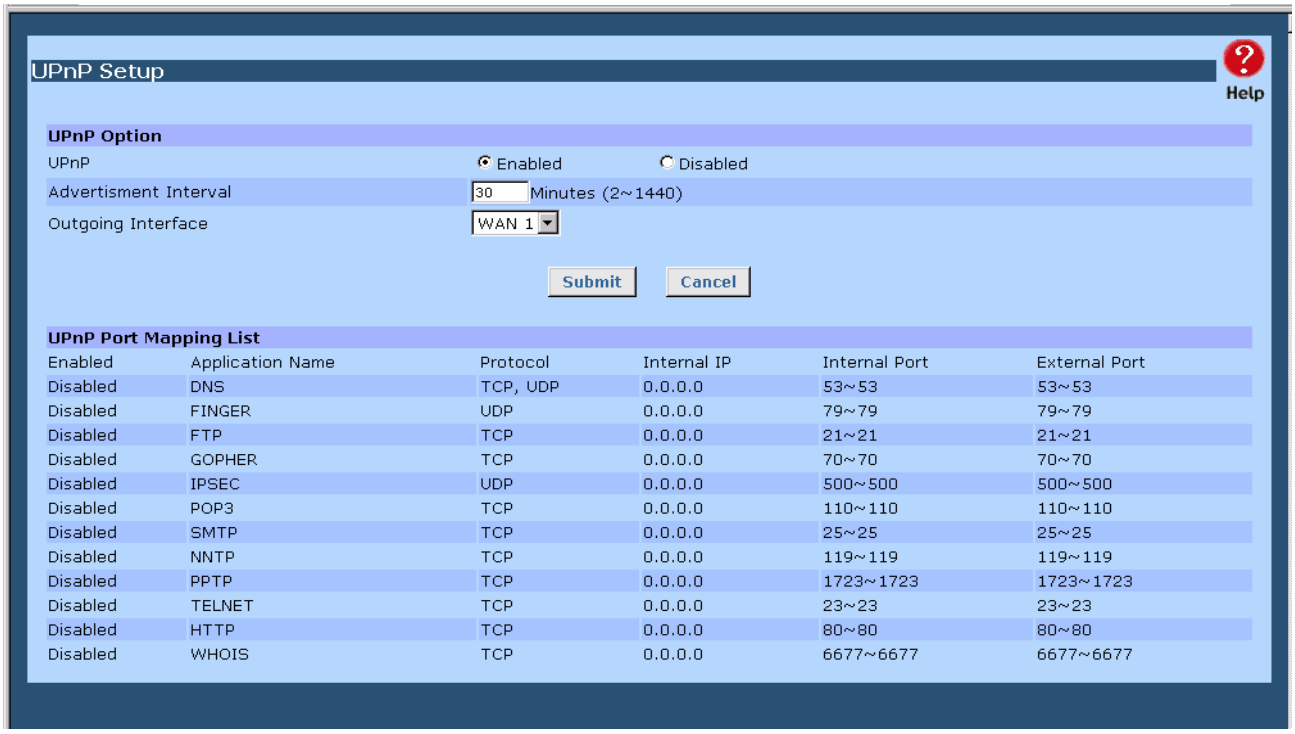

Figure 4-9: UPnP

Settings – UPnP

UPnP Option	• UpnP (Univeral Plug & Play) can be enabled or disabled for automatic device configuration. If disabled (Default), the router will not allow any device to automatically control the resources. • **Advertisement Interval** –The Advertisement Interval is how often the router will broadcast its UPnP information. This value can range from 2 to 1440 minutes. The default interval is for 30 minutes. Shorter time interval will ensure that control points have current device status at the expense of additional network traffic. Longer time interval may compromise the freshness of the device status but can significantly reduce network traffic. • **Outgoing Interface** – Select though which WAN or LAN port you want to send out traffic from UPNP. If the WAN port you select loses its connection, the router attempts to use the other WAN port. If the other WAN port also does no work, the router drop outgoing packets from UPNP.

UpnP Port Mapping List	You can set the dynamic port mappings to Internet gateway via UPnP on Windows XP. This will allow you make a connection between applications and the defined device

NAT

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

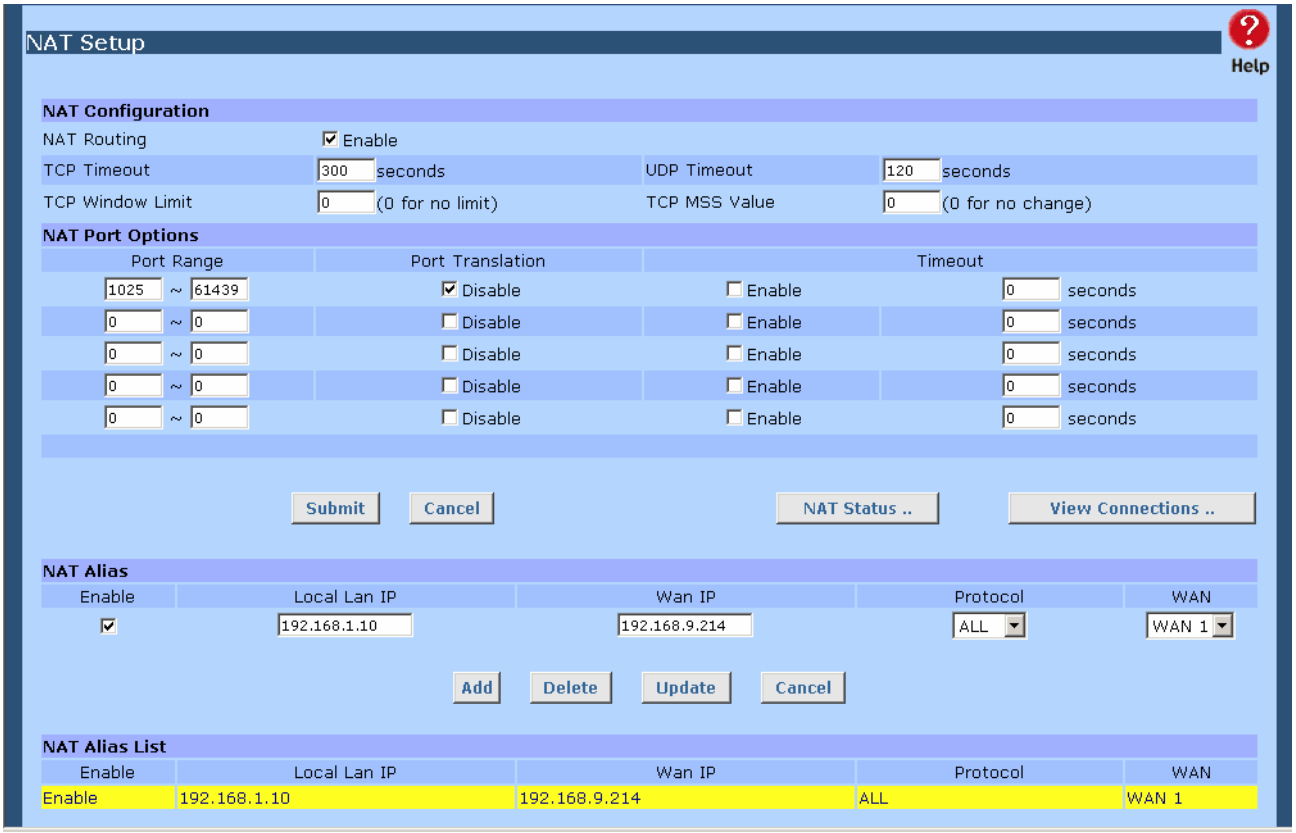

Figure 4-10: NAT

Settings – NAT

NAT Configuration	• **NAT Routing** –Enables or disables NAT routing by checking or un-checking the checkbox. If you disable NAT routing, this device will act as a Bridge or Static Router. Most features, including Load Balance, will be unavailable. If some packets have port numbers which cannot be translated for special applications, you must input value in port range for **Disable Port Translation**. • **TCP Timeout** –The time during which TCP expects to receive the acknowledgement from the destination. The default is 300 seconds. • **UDP Timeout** –The time during which UDP expects to receive the acknowledgement from the destination. The default is 120 seconds. • **TCP Window Limit** –The maximum number of outstanding packets prior to TCP receiving an acknowledgement. The default is 0 (no limit). • **TCP MSS Limit** –The largest amount of data that can be transmitted in one TCP packet. The default is 0 (no change).

NAT Port Option	• **Non-Port-Translation** –To keep the source port number unchanged for TCP/UDP sessions on the specified Port Range. Some special applications do not allow the source port number to be translated. • **Port Range** – The Source Port Number Range for TCP and UDP protocol. • **Specific TCP / UDP Timeout** –To define specific Timeout for TCP/UDP sessions on the specified Port Range.
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. • **Enable** – To activate or deactivate current entry. • **Local LAN IP** –The IP address of the host in LAN that wants to use the specific WAN IP as its source IP. • **WAN IP** – The IP address used as the source IP of the packets sent out from the specified host. • **Protocol** –The protocol that the current rule is applied to. • **WAN** – The WAN port that the current rule is applied to.
NAT Alias List	• The List shows NAT Alias that is currently defined.

ARP Status

ARP (Address Resolution Protocol) – This is web page is regarding LAN & WAN ARP statistics and information,

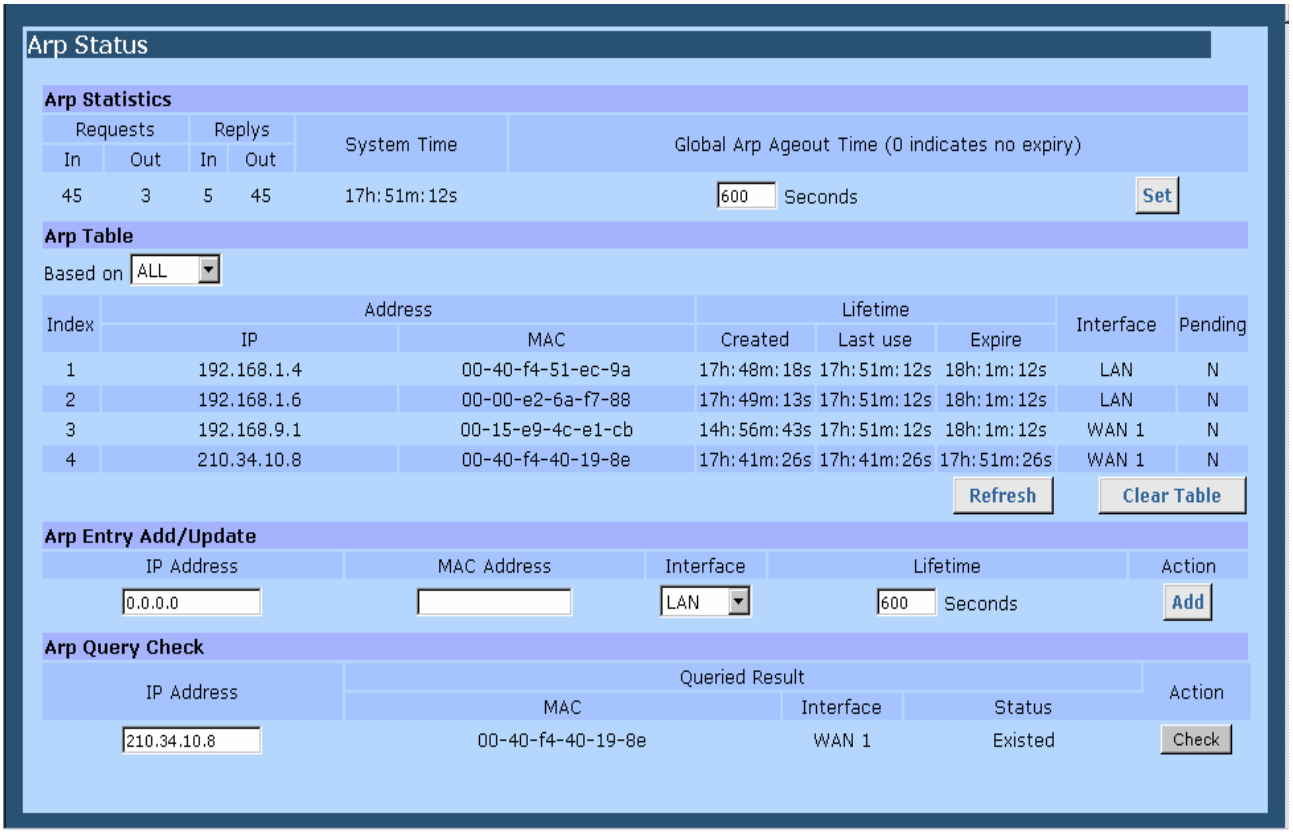

Figure 4-11: ARP Table

Arp Statistics	• **Requests (In / Out)** – The numbers of system ARP sent to requests. • **Reply (In / Out)** –The numbers of system ARP reply to. • **System Time** – System starting time. • **Global Arp Ageout Time** – Arp time out. By default is 600 seconds. If set to “0” means no expire.
Arp Table	• List all LAN, WAN address resolution and its related info.
Arp Entry Add / Update	• According to IP and MAC address, add or update a record to a ARP table
Arp Query Check	• Input LAN or WAN IP address to query ARP.

Advanced Features

- **External Filters Configuration** –To limit the packets passing through the device from WAN side to LAN side
- **DNS Loopback** – If there is any domain in your private network you can setup the Domain Name & Private IP mapping table for DNS query.
- **Protocol & Port Binding** – It is similar to SMTP binding but you must setup additional data such as Protocol & Port Range. If all the checking items are met, the packet will be bound on the specified WAN port.

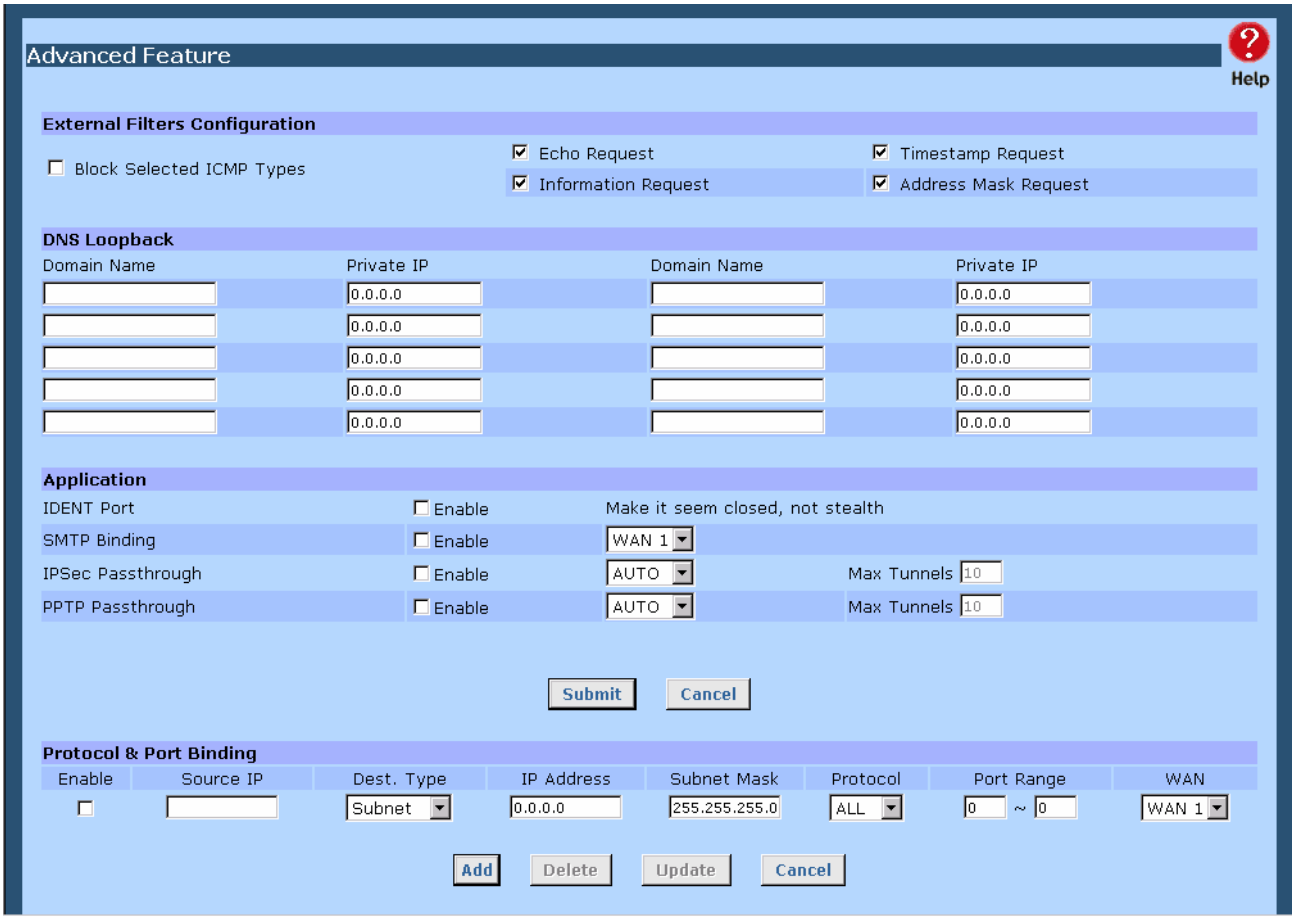

Figure 4-12: Advanced Features

Settings – Advanced Features

External Filters Configuration	• **Block Selected ICMP Types** –This acts as "master" switch. If checked, the selected packet types are blocked. Otherwise, they are accepted.
DNS Loopback	When you have some servers on LAN and their domain names have already registered on public DNS. To avoid DNS loopback problem, please enter the following fields. • **Domain Name** – Enter the domain name specified by you for local host/server. • **Private IP** – Enter the private IP address of your local host/server.
Application	• **IDENT Port** – Port 113 is associated with the Internet's (Identification / Authentication) service. This port (port 113) provides a means of determining the identity of a user on a particular TCP connection. By default the device is stealth for this port. Enable to make this port closed, not stealth. • **SMTP Binding** –To determine if the SMTP packets are bound on the WAN port. • **IPSec Passthrough** – To determine if the VPN client can make a tunnel established with remote side VPN host. • **PPTP Passthrough** – To determine if PPTP client can connect to remote side PPTP server via the device.
Protocol & Port Binding	• **Enable** – To activate or deactivate the current rule. • **Source IP** –The IP address that the packet's source IP will be checked against. • **Destination IP / IP Address** –The specific IP range that the packet's destination IP will be checked against. There are two forms of Destination IP: If Subnet is selected, the IP Address and Subnet Mask fields need to be filled. If IP Range is selected, the From and To fields need to be filled. • **Protocol** –The protocol that the packet's protocol will be checked against. • **Port Range** –The specific port number range that the packet's destination port number will be checked against. • **WAN** –The specific WAN port that the packet will be bound on if all the checked items are met.
Protocol & Port Binding List	The List shows NAT Alias that is currently defined.

5: Security Management

Overview

- ***URL Filter*** It can block specific website by configure IP address, URL or Key words
- ***Access filter*** You can block all Internet access or select block well-known port or block user define ports by groups.
- ***Session Limit*** It can eliminate users access Internet, and send email alert to the administrator. If the device detect new sessions that is exceed the maximum sampling time.
- ***Firewall Exception*** It can eliminate users access Internet, and send email alert to the administrator. If the device detect new sessions that is exceed the maximum sampling time.

URL Filter

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

- In operation, every URL is searched to see if it matches or contains any of the URL or keywords entered here. Then, after a DNS lookup determines the IP address of the requested site, the site's IP address is checked against IP address entries on this screen.
- Note that a single IP address may host many Web sites. Entering the IP address on this screen will block all Web sites hosted on that IP address.

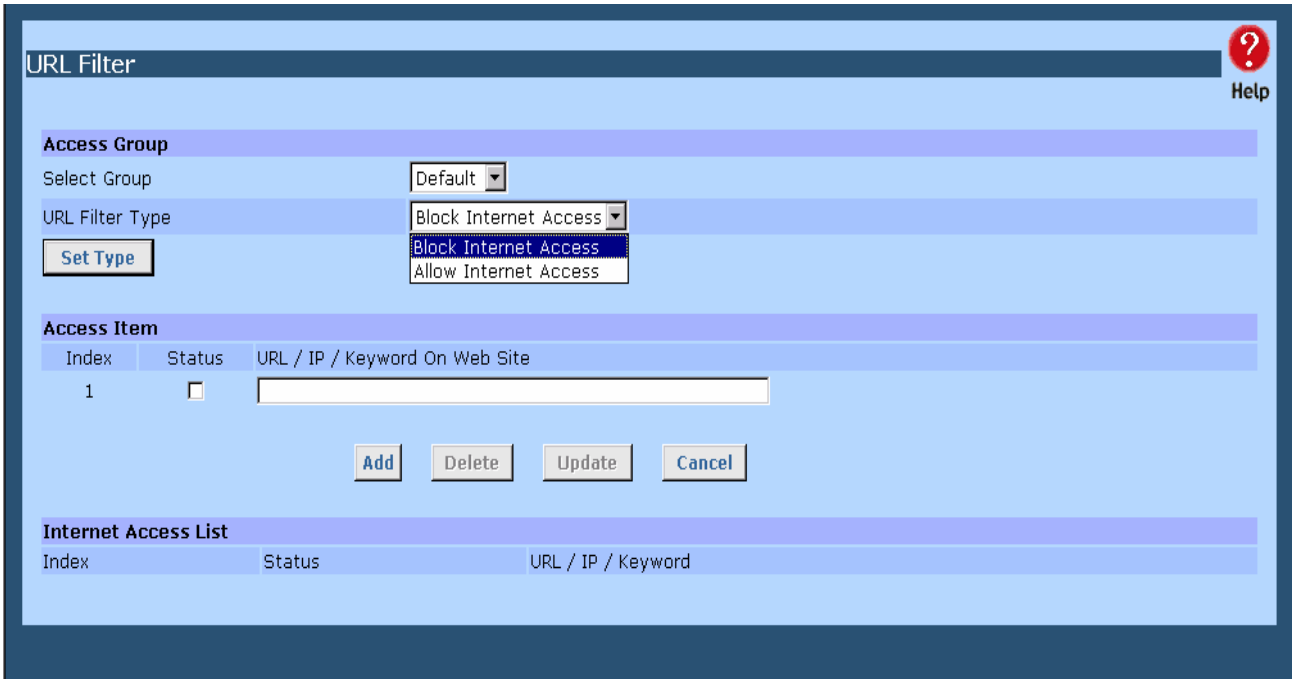

Figure 5-1: URL Filter

Settings – URL Filter

Access Group	• **Select Group** – A group that current rule is applied for • **URL Filter Type** –The Filter type (Block/Allow) that current group is set to use. **Block Internet Access:** All the web page accesses will be blocked if the target is found in the packets. **Allow Internet Access:** All the web page accesses will be permitted if the target is found in the packets.
Access Item	This text field is to enable/disable the URL Filter function, and input URL keyword phrase.
Internet Access List	List of current input items.

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

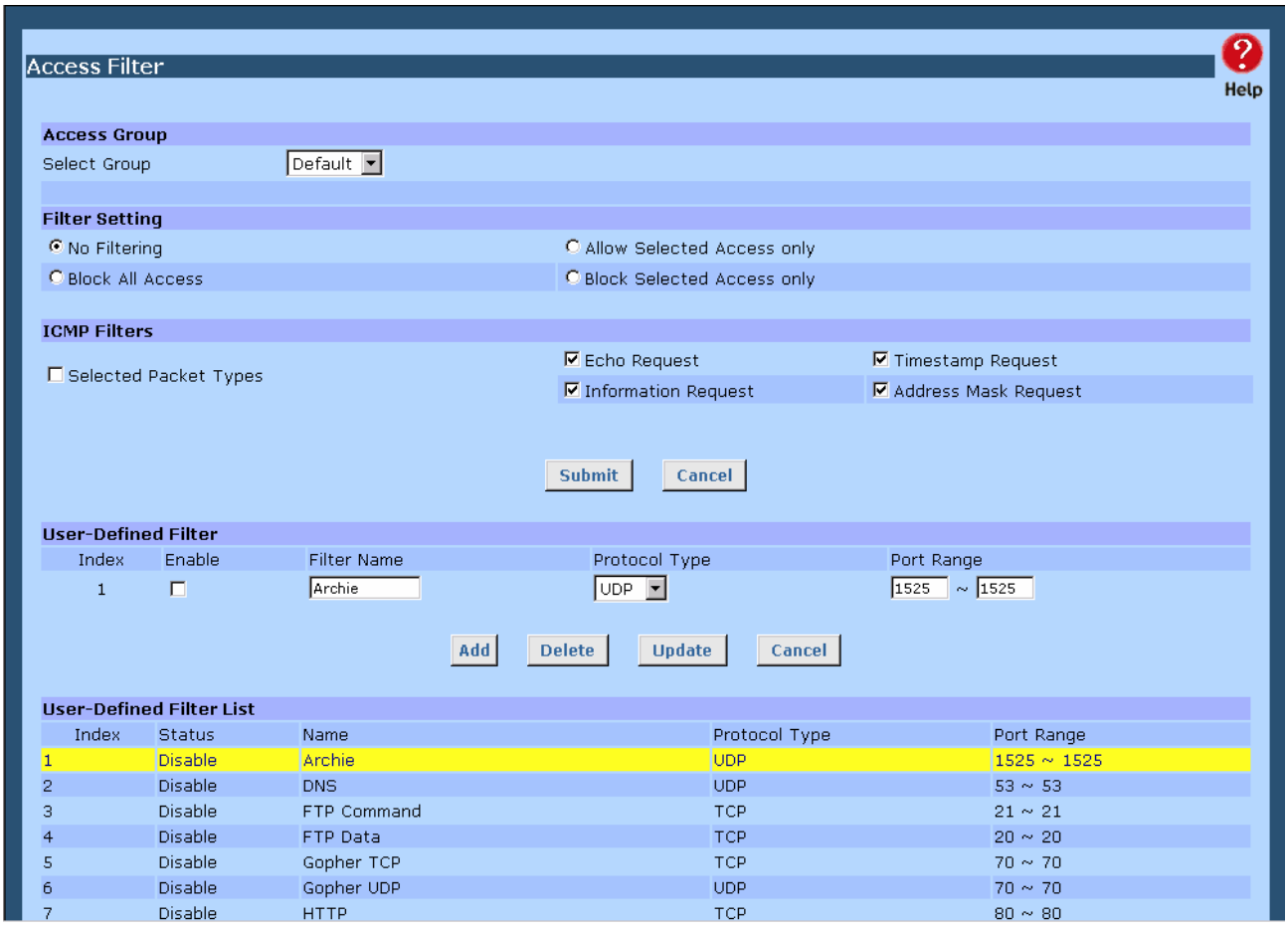

Figure 5-2: Access Filter

Settings – Access Filter

Access Group	The Group that the current rule is applied for. To apply restrictions to everyone, select the Default group. All users (Hosts) are in the default group unless moved to another group on the Host IP screen
Filter Setting	• **No Filtering** –To allow all Internet access by LAN users. • **Block All Access** –To prohibit all Internet access by LAN users. • **Allow Selected Items** – To apply the rules for permitting Internet access defined in User-Defined Filter**.** • **Block Selected Items** – To apply the rules for blocking Internet access defined in User-Defined Filter.
ICMP Filter	To limit the ICMP activities initialized from the LAN. • **Selected Packet Types** –To prohibit the selected types of ICMP packets from the LAN to be passed through the device. • **Packet Types** –The types of ICMP packets that could be blocked
User-defined Filter	This lets you define custom ports to be blocked. • **Enable** – To activate or deactivate the current rule. • **Name** – A unique name to identify the current rule. • **Protocol Type** – The protocol to be blocked. • **Port No. Range** – The port number range to be blocked. (For TCP and UDP only) If only one port number is used, enter the same port number in both fields.
User- Defined Filter List	List all enabled and disabled filter and have been defined.

Session Limit

This new feature allows to drop the new sessions from both WAN and LAN side. If the new sessions number are exceed the maximum sessions in a sampling time.

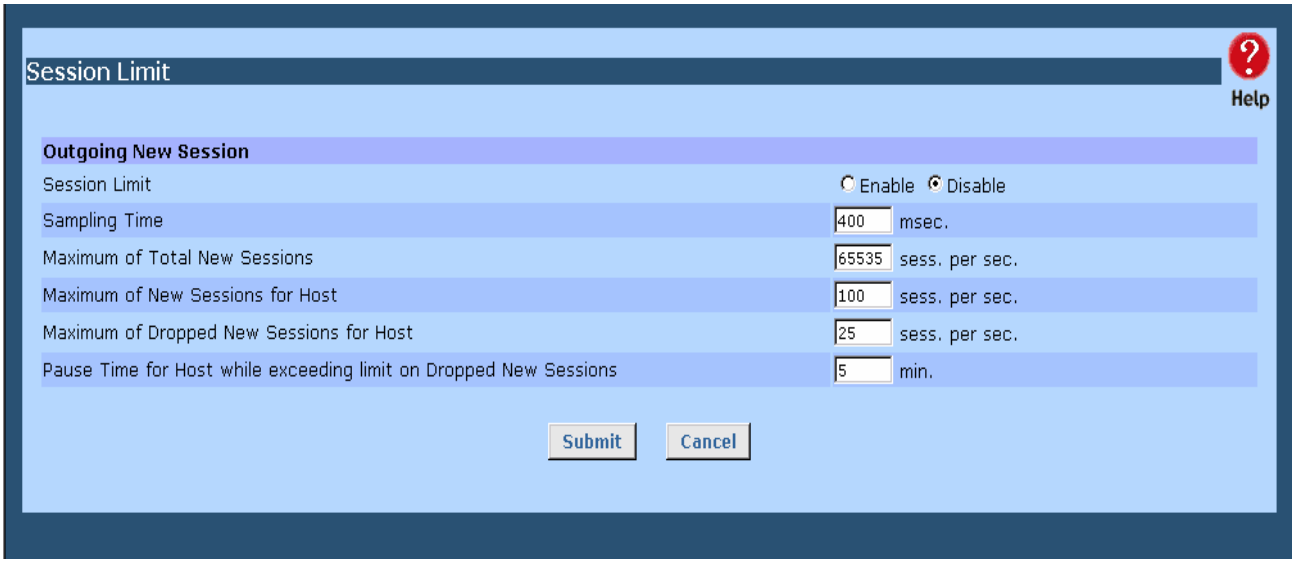

Figure 5-3: Session Limit

Session Limit

Outgoing New Session	• **Session Limit** – Check this to enable limiting sessions. • **Sampling Time** – The period to count the new sessions. Only those new sessions which occurred in the most recently Sampling Time are counted for limit checking. (default: 400 mili-sec., maximum: 500 mili-sec., step: 50 mili-sec.) • **Maximum of Total New session** – If the number of new sessions for the system exceeds the Maximum in the Sampling Time, any new session in the system will be dropped. (Default: 65535 sess./sec., maximum: 65535 sess./sec.) • **Maximum of New Sessions for Host** – If the number of new sessions for the host exceeds the Maximum in the Sampling Time, any new session of the host will be dropped. (Default: 100 sess./sec., maximum: 999 sess./sec.) • **Maximum of Dropped New Sessions for Host** –If the number of dropped new sessions for the host exceeds the Maximum in the Sampling Time, any new session of the host will be dropped for the Pause Time. (default: 25 sess./sec., maximum: 999 sess./sec.) • **Pause Time for Host while exceeding limits on dropped new sessions** – Within the Pause Time, no new session of the suspended host will be served by the system. (Default: 5 min., maximum: 65535 min.)

SysFilter Exception

System Filter Exception Rules: Any unrecognized packet to the device itself will be rejected. If you want the device to accept the specific packets, you should build the corresponding exception rules here.

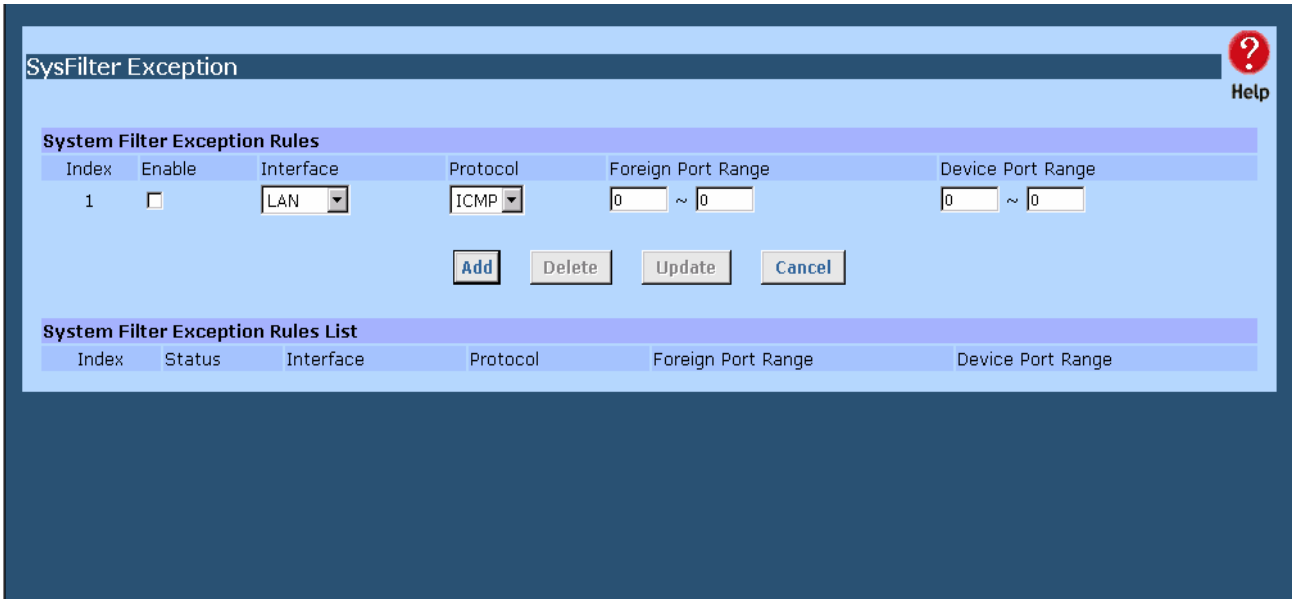

Figure 5-4: SysFilter Exception

Firewall Exception

System Filter Exception Rules	• **Enable** –To activate or deactivate this rule. • **Interface** – The port that the packets enter the device on. • **Protocol** – The protocol of the packets to be accepted. • **Foreign Port Range** –The source port range of the packets to be accepted. • **Device Port Range** – The destination port range of the packets to be accepted.
System Filter Exception Rule List	List all system rules that have been defined.

6: QoS Configuration

Overview

The Load Balancer provides QoS, which supports the high quality of network service.
Because it will classify outgoing packets based on some policies defined by users, make some real-time applications to get better response or performance.

QoS Setup

The following web page management are guiding you how to setup QoS and make QoS work.

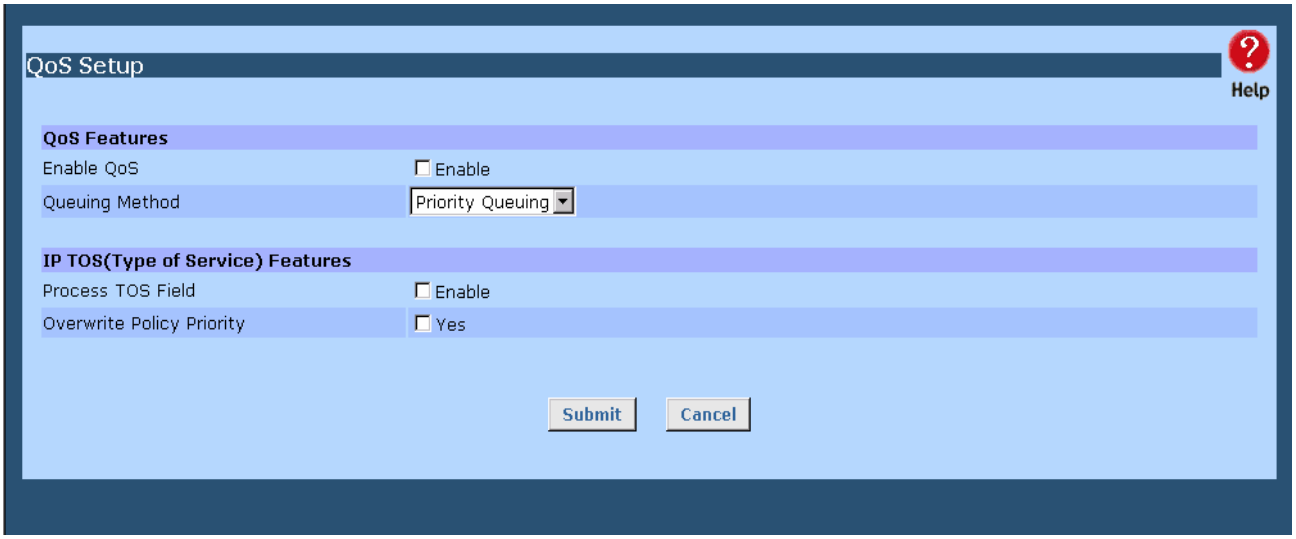

Figure 6-1:QoS Setup

Data – QoS Setup.

QoS Feature	• **Enable QoS** – Users can choose to Enable QoS (Quality of Service). If set to "enable" QoS, the QoS will allow higher priority packets to pass through the device • **Queuing Method** –The methods for managing your queue. "Priority Queuing" is one of the first queuing variations to be widely implemented. This is based on the concept that certain types of traffic can be identified and shuffled to the front of the output queue so that some traffic is always transmitted ahead of other types of traffic.

IP TOS (Type of Service) Feature	• **Process TOS Field** –An 8 bits field in the IP packet header designed to contain values indicating how each packet should be handled in the network. If you choose "enable" then it will enable this function to process IP Type of Service field. • **Overwrite policy priority** – Choose “yes” to set the priority of TOS field in IP packet overwrite the priority defined in policy configuration

Policy Configuration

Setting the **QoS** policy can assign received packets a higher/lower priority (based on your configuration) to pass through this device. You can define some policies which classify received packets based on source/destination 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.

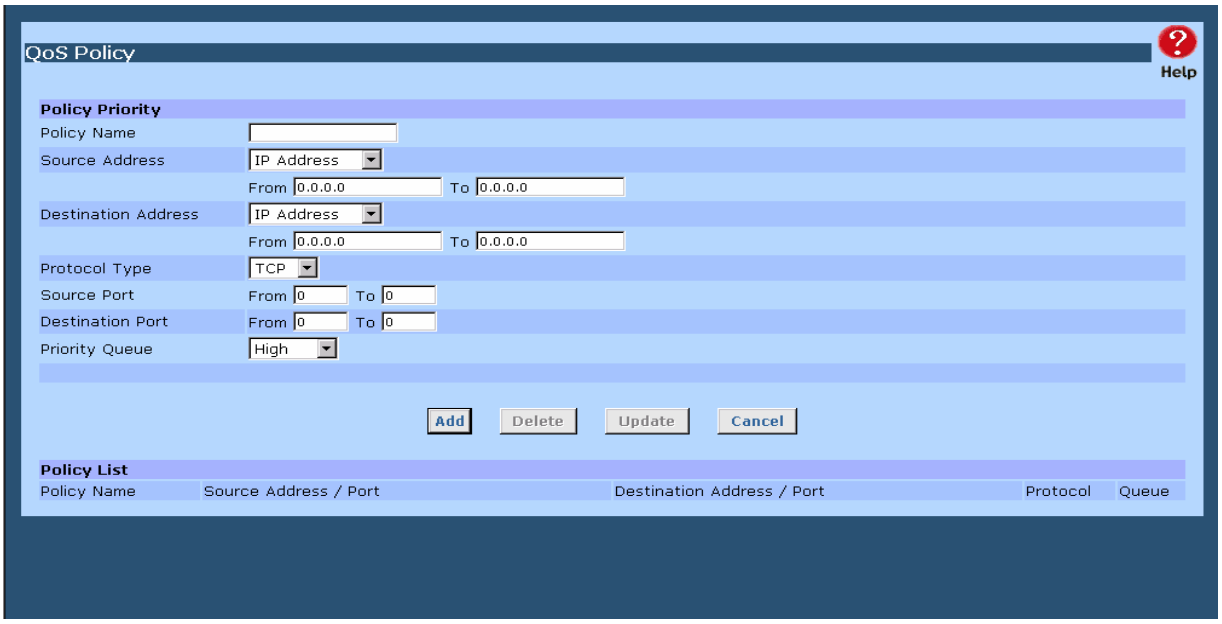

Figure 6-2: Policy Configuration

Data – Policy Configuration.

Policy Priority	• **Policy Name** –The name of a policy which is used to classify the received packets based on the following types for your memory. • **Source/Destination Address, Port** – Specify a packet based on source/destination 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** – The field defines traffic packet type, i.e. IP,TCP and UDP. • **Priority Queue** –This device supports four queues. When a packet meets a policy rule requirement, it will be put into the responding queue. Otherwise it is assigned the lowest priority to pass through

7: Management Assistant

Overview

The following advanced features are provided.

- Admin Setup
- Email Alert
- SNMP
- Syslog
- Upgrade Firmware

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

Admin Setup

The password screen allows you to assign a password to The Load Balancer, and enable /disable the remote access mechanism.

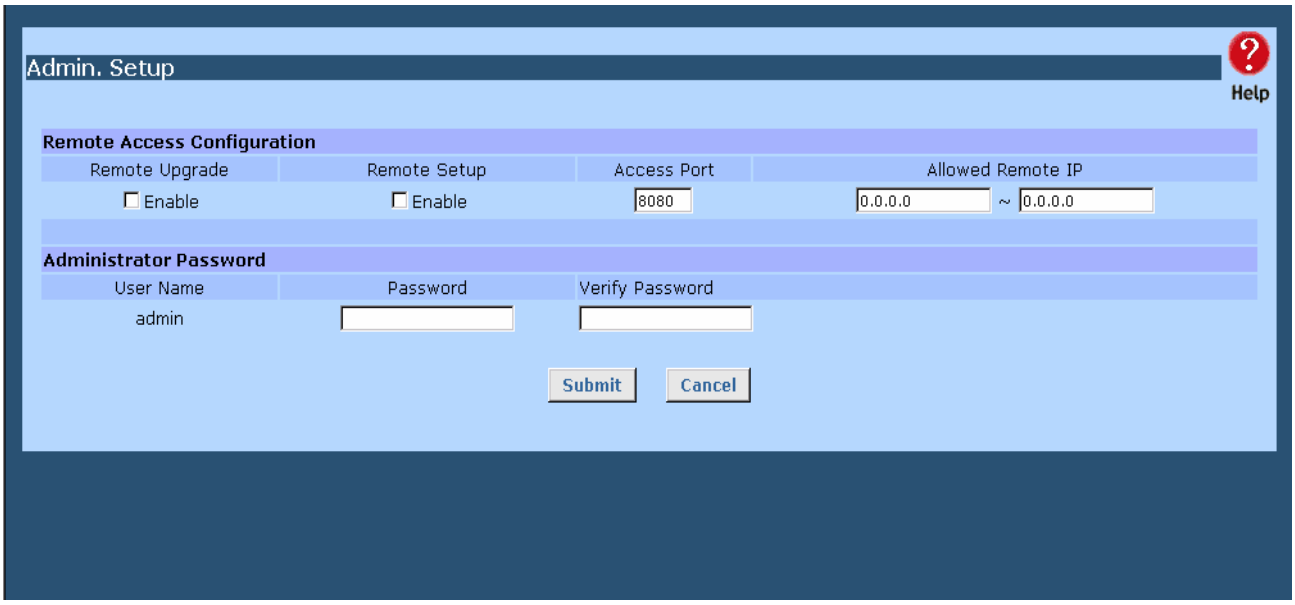

Figure 7-1: Admin Password

Enter the desired password, re-enter it in the *Verify Password* field, then save it.

When you connect to The Load Balancer with your Browser, you will be prompted for the password when you connect, as shown below.

Figure 7-2: Password Dialog

- Enter "Admin" for the *User Name*.
- Enter the password for The Load Balancer, as set on the *Admin Password* screen above.

Admin. Setup

Remote Access Configuration	• **Remote Upgrade** – If enabled, you can use the supplied Windows utility to remotely upgrade the firmware. If not enabled, the upgrade must be performed by a PC on the LAN. • **Remote Setup** – If enabled, access to the web-based interface is available via the Internet (See below for details). If not enabled, access is only available by a PC on the LAN. • **Access port** – The port number used when connecting remotely. The default port number is 8080. • **Allowed Remote IP** – Remote access is only available to the IP address entered here. 1. Leaving these fields blank (0.0.0.0 ~ 0.0.0.0), will allow access by all PCs. 2. These addresses must be Internet IP addresses; not addresses on the local LAN. 3. To specify a single address, enter it in both fields.
Administrator Password	You can modify the device password in this field. The default entry is “ “ (no password).

Email Alert

This feature will send an warning Email, inform system administrator that one of the WAN ports was disconnected.

Email Alert – You can choose to enable or disable it to send a warning email.

Email Sender Address – It is an email address, which will send the warning email.

Email (SMTP) Server Address – It is an email server address the warning email will be sent to.

Email Recipient Address – It is an email address of system administrator the email will be sent to.

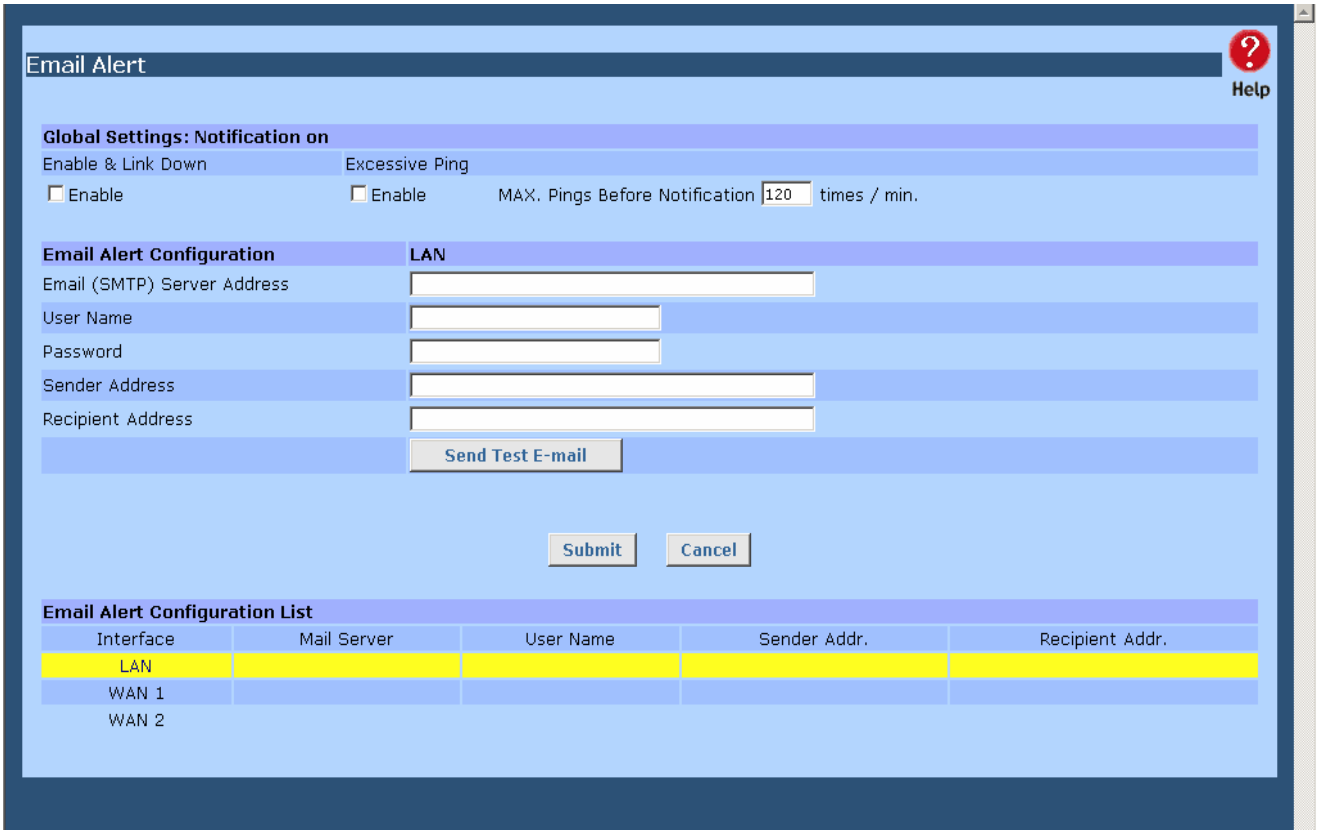

Figure 7-3: Email Alert

Settings – Email Alert

Global Setting	• **Enable & Link down** – To enable or disable the Alert Mail sending in the event one of the WAN ports is disconnected. • **Excessive ping** –This function is useful to prevent ICMP packets attacks from WAN or LAN onk the device. It will drop the packets if the ping times exceed the threshold value

Email Alert Configuration	The purpose of email alert is in the event a WAN port is disconnected or mal-functions, it will send an email message to inform the recipient. • **Email (SMTP) Server Address** – The e-mail server address. (ex: mail.yourdomain.com) • **User Name** –The user name of an e-mail sender address for authentication. (ex: abc) • **Password** –The password of an e-mail sender address for authentication. (ex:12345) • **Sender Address** – The email address of the sender. • **Recipient Address** –The email address of the receiver. (ex: .admin@yourdomain.com)
Email Alert Configuration list	List Email Alert messge that you have configured previously.

SNMP

This section is only useful if you have SNMP (Simple Network Management Protocol) software on your PC. If you have SNMP software, you can use a standard MIB II file with The Load Balancer.

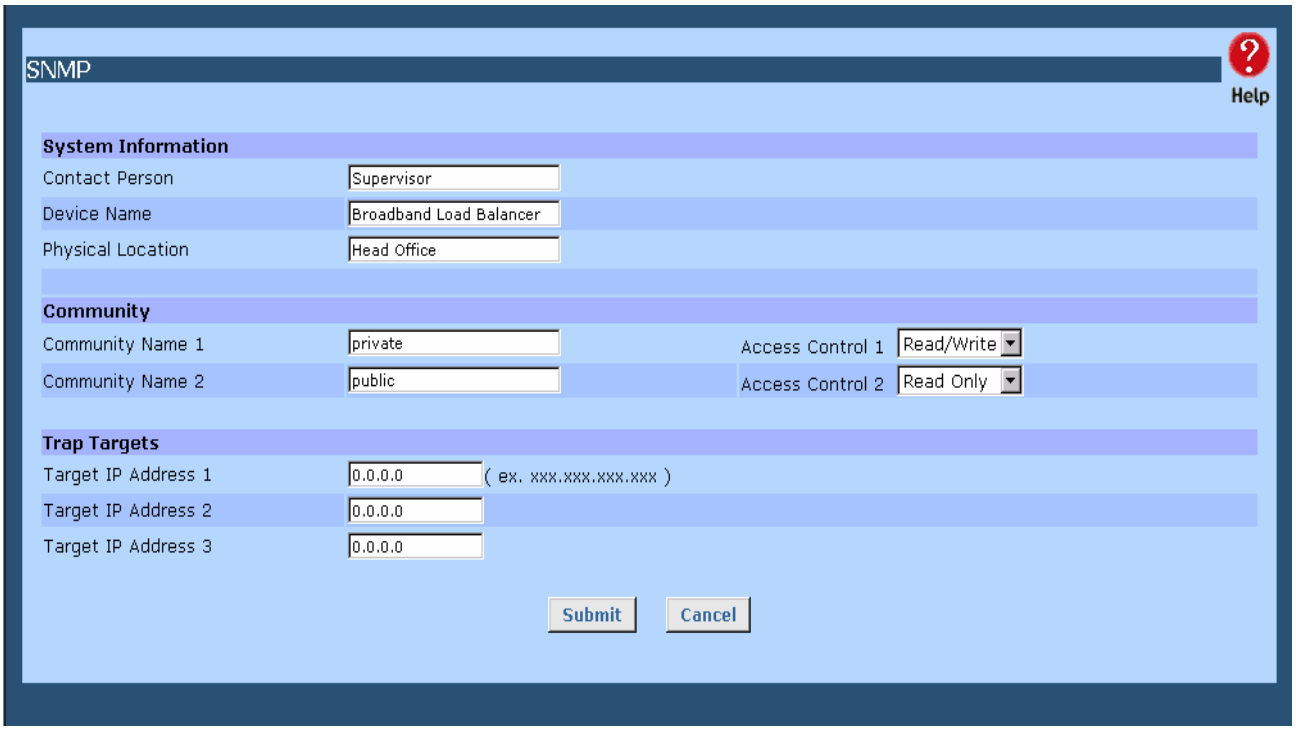

Figure 7-4: SNMP

Settings – SNMP

System Information	This is the system information which will identify this device.
Community	A relationship between a SNMP agent and a set of SNMP managers that defines authentication, access control and proxy characteristics.
Trap Targets	Up to three IP addresses can be entered. Trap information will be sent to these addresses

Syslog

This feature can send real time system information on the web page or to the specified PC.

Syslog Configuration – Syslog Configuration allow you where to send system information to other machine or not. There are up to three machines you can choose to send your system log.

Message Status– Messages send only keep when “keep send message” checked. Currently we keep last 100 messages in the RAM area, they will clear when reboot or power off.

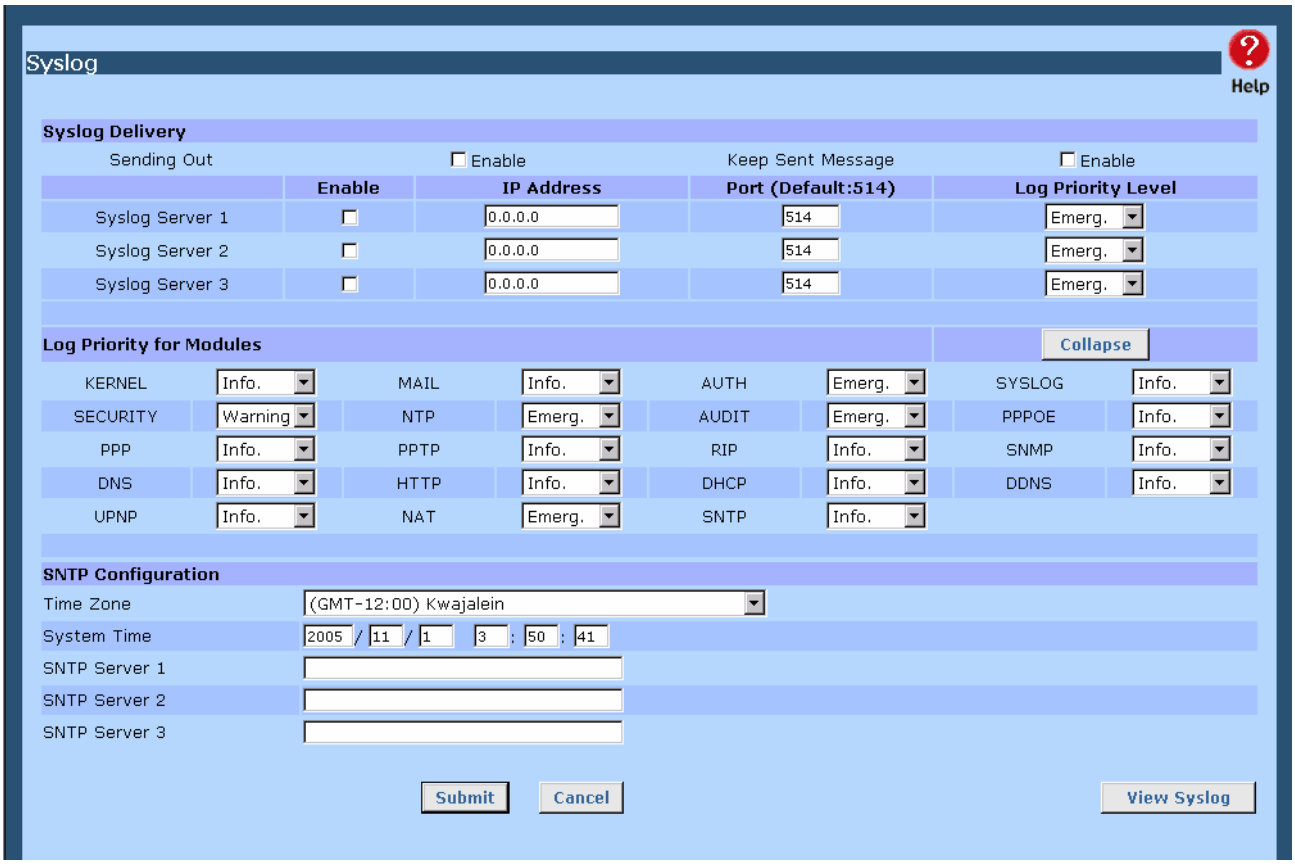

Figure 7-5:Syslog

Syslog Configuration

Syslog Delivery	• **Sending Out** – If checked, the device will send syslog messages to other machines (log servers).
	• **Keep Sent Message** – If checked, the sent messages will be kept on the device, otherwise they will be deleted
	• **Syslog Servers** –
	  • **IP Address:** Up to **3** syslog servers can be used.
	  • **Enable:** If checked, the log message will be sent to the server. You can disable or enable each server temporarily.
	  • **Port:** If your syslog server does not use the default port (514), change it.
	  • **Log Priority Level:** The messages are grouped into **8** priority levels, from Emergency to Debug. The lower level it is, the more messages it will generate. Emergency is the highest priority level, and Debug is the lowest.Setting priority to Debug will send all generated messages

Log Priority Modules	This feature displays and controls the current log priority for each module. For a module with different priorities, the different level of messages will be generated in Syslog. The lower the level of log priority for a module, a more messages will be generated. DEBUG is the lowest level of log priority
SNTP Configuration	• **SNTP Servers** – Up to 3 SNTP servers can be used for GMT. You can enter its IP or Domain address here. You can use some servers such as time-a.nist.gov**,** time.nist.gov**,** time-nw.nist.gov, etc. • **Time Zone** –This lists all time differences between GMT and the local time selected by you.

Upgrade Firmware

This Upgrade Firmware Screen allows you to upgrade firmware or backup system configuration by using HTTP upgrade.

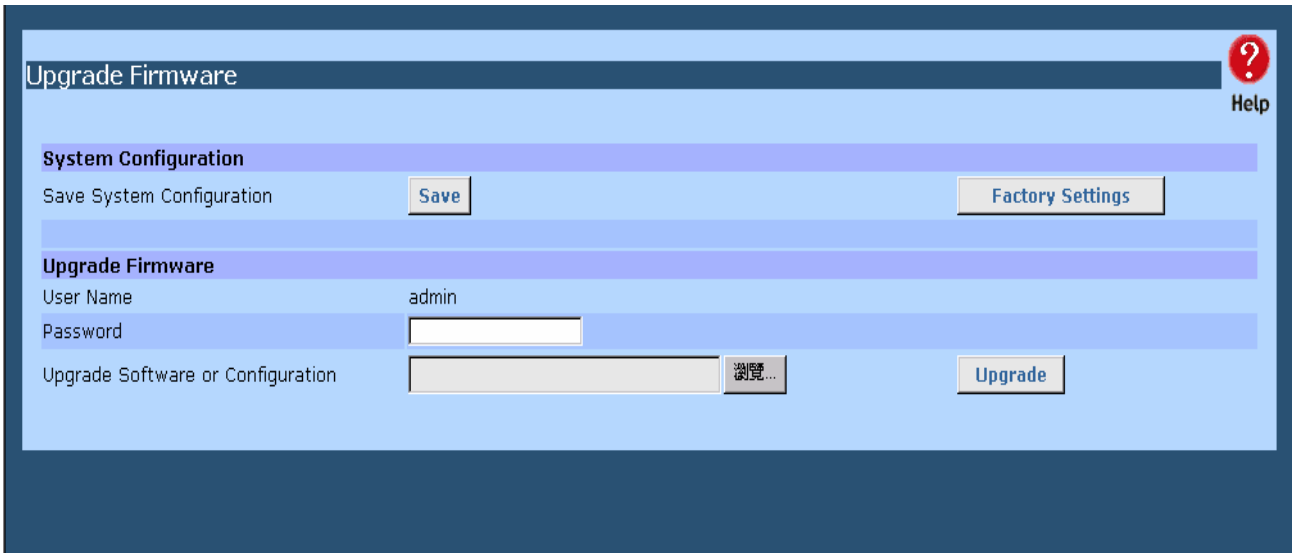

Figure 7-6: Firmware Upgrade Screen

System configuration	◆ You can backup your system configuration by press “save” button of Save System Configuration. It will save the system configuration for you. (Notice: You have to refresh the browser after you saved the system configuration file)
Upgrade Firmware	◆ You also can do firmware upgrade by input the correct password and the file name of your firmware. Remember do not Reset or Restart the device while update new firmware, because it may cause system to crash.

Restore Factory Defaults

When the "Restore Factory Defaults" button on the ***upgrade Firmware*** screen above is clicked, the following screen is displayed.

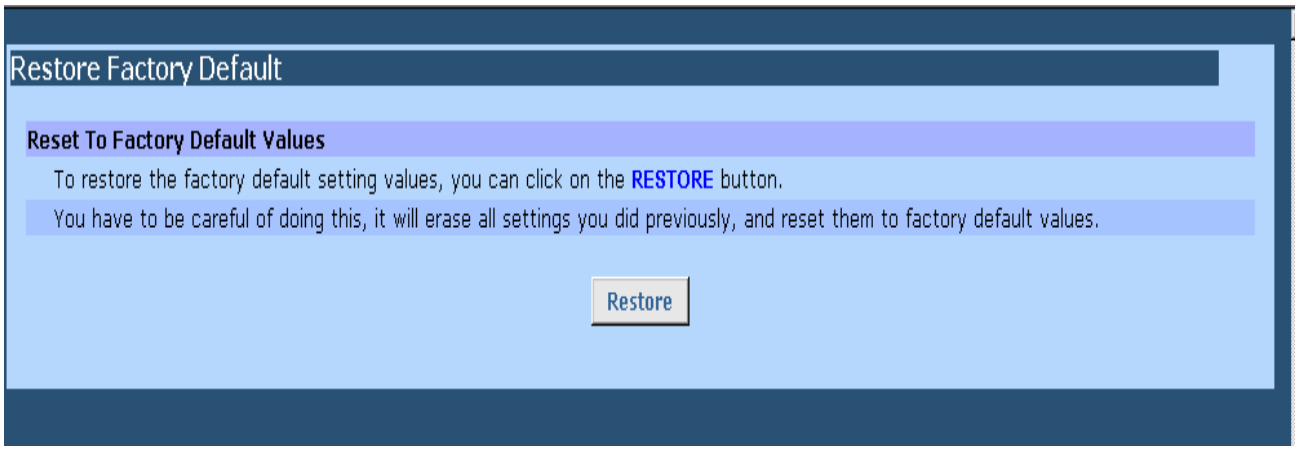

Figure 7-7: Restore Factory Defaults

If the "Restore Default Value" button on this screen is clicked:

- ALL of your settings will be erased.
- The default IP address, password and ALL other settings will be restored to the factory default values.
- The DCHP server function will be enabled.

These changes may mean that the current connection is invalid, and you will have to re-connect to The Load Balancer using its default IP address (192.168.1.1).

8: Operation and Status

Operation

Once both The Load Balancer and the PCs are configured, operation is automatic.

However, there are some situations where additional Internet configuration may be required:

Refer to *Chapter 4 - Advanced Features* for further details.

System Status

Use the ***System Status*** link on the main menu to view this screen.

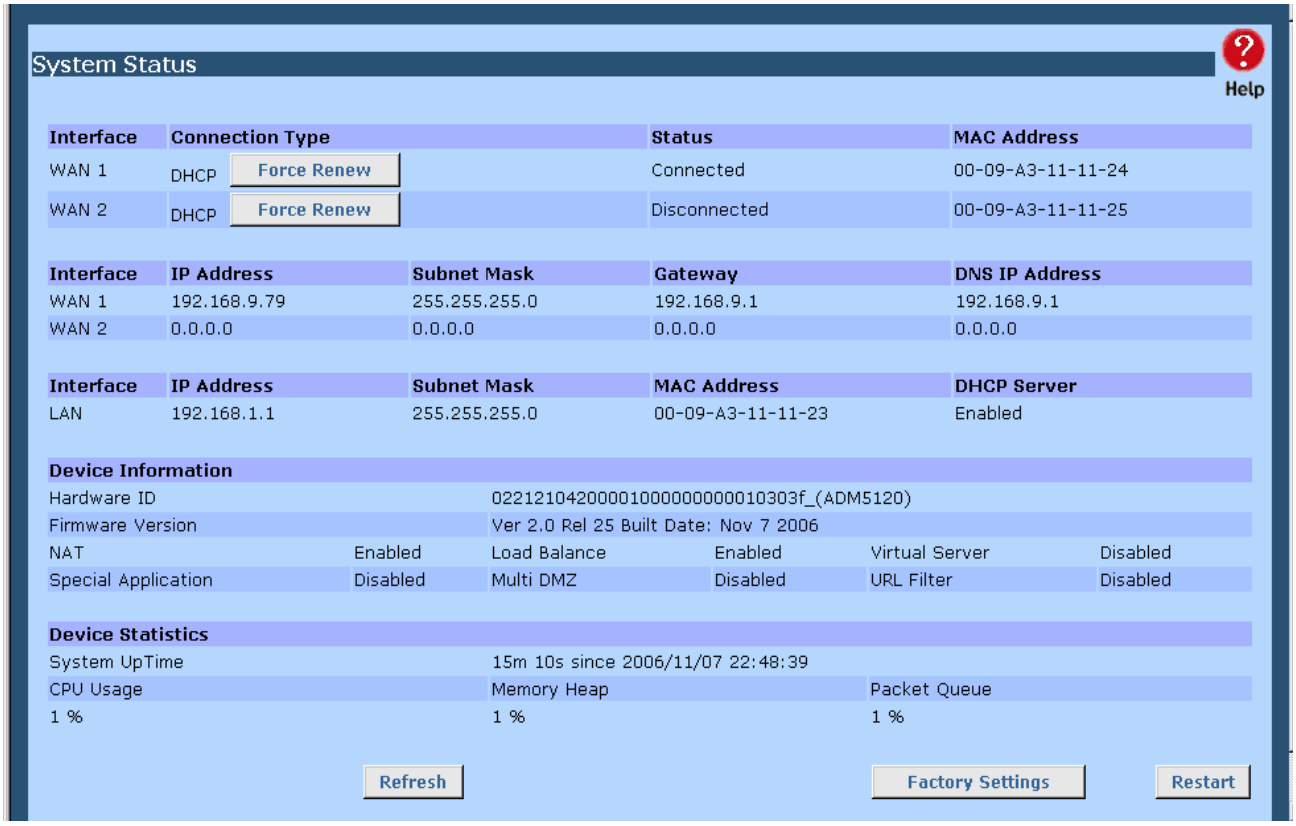

Figure 8-1: System Status

Data – System Status

Interface Information	• **Connection Type** – The type of connection used – DHCP, Fixed IP, PPPoE, or PPTP. • **Connection Status** – Current status – either "Connected" or "Not connected". • **"Force Renew"** button– Only available if using a dynamic IP address (DHCP). Clicking this button will perform a DHCP "Renew" transaction with the ISP's DHCP server. This will extend the period for which the current WAN IP address is allocated to you. • **MAC Address** – The WAN port MAC (physical) address of the Load Balancer,
Interface (WAN)	• **IP Address** – The IP address of the Load Balancer, as seen from the Internet. This IP Address is allocated by the ISP (Internet Service Provider) • **Subnet Mask** – The Network Mask (Subnet Mask) for the IP Address above. • **Gateway** – An IP address that act as entrance to another network. • **DNS IP Address** – The address of the current DNS (Domain Name Server.)
Interface (LAN)	• **IP Address** – The LAN IP Address of the Load Balancer. • **Subnet Mask** – The Network Mask (Subnet Mask) for the IP Address above. • **MAC Address** – The MAC (physical) address of the Load Balancer, as seen from the local LAN. • **DHCP Server** – The status of the DHCP Server function - either "Enabled" or "Disabled".
Device Information	• **Hardware ID** – The manufacturers ID for this particular device. • **Firmware Version** – Version of the Firmware currently installed. • **NAT** – Status of the *NAT* feature – either “Enable” or “Disable”. • **Load Balance** – Status of the *Load Balance* feature – either “Enable” or “Disable”. • **Virtual Server** – Status of the *Virtual Server* feature – either "Enabled" or "Disabled". • **Special Applications** – Status of the *Special Applications* feature – either "Enabled" or "Disabled". • **Multi DMZ** – Status of the *DMZ* feature – either "Enabled" or "Disabled". • **URL Filter** – Status of the *Block URL* feature – either “Enable” or “Disable”.
Device Statistics	• **System UpTime** – The time since the system of a device was last reinitialized. • **CPU Usage** – The current usage percentage of CPU. • **Memory Heap** – The current memory usage percentage in memory heap. • **Packet Queue** – The current packets usage percentage in queue,

Buttons	• **Refresh** – Update the data on screen. • **Restart** – Restart (reboot) the Load Balancer. • **Restore Factory Defaults** – This will delete all existing settings, and restore the factory default settings. See below for details.

WAN Status

Use the ***WAN Status*** link on the main menu to view this screen.

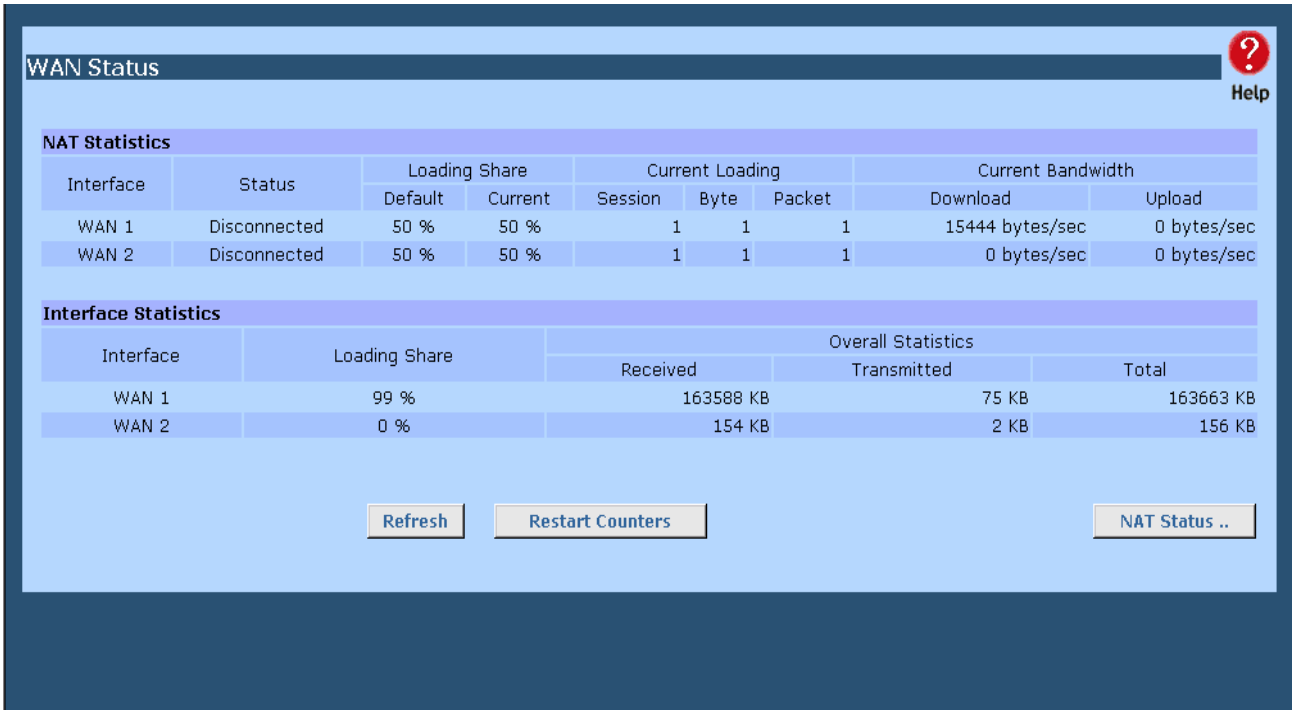

Figure 8-2: WAN Status

Data – System Status

NAT Statistics	This section displays data for each WAN port. • **Connection status** – This will display either *Connected* or *Not Connected*. • **Default Loading Share** - The default traffic loading between the WAN ports. • **Current Loading Share** – The current traffic loading between the WAN ports. • **Current Loading** – The number of sessions, Bytes and Packets currently being processed on each port. • **Current Bandwidth** – The current Download and Upload speeds on each WAN port. • "Check NAT Detail" will display the ***NAT Status*** screen, described below.
Interface Statistics	This section displays cumulative statistics. Use the "Restart Counter" button to restart these counters when required.

Appendix A

Specifications

Model	Load Balancer
Dimensions	245mm (W) x 137mm (D) x 30mm (H)
Operating Temperature	0° C to 40° C
Storage Temperature	-10° C to 70° C
Network Protocol:	TCP/IP
Network Interface:	6 Ethernet: 4 * 10/100BaseT (RJ45) auto-Switching Hub ports for LAN devices 2 * 10/100BaseT (RJ45) for WAN
LEDs	8 LAN 4 WAN 1 Status 1 Power
External Power Adapter	5 V 1.5A DC

FCC Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference.

(2) This device must accept any interference received, including interference that may cause undesired operation.

CE Marking Warning

This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Appendix B
Windows TCP/IP Setup

Overview

TCP/IP Settings

If using the default Load Balancer settings, and the default Windows 95/98/ME/2000 TCP/IP settings, no changes need to be made.

- By default, The Load Balancer 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.
- If you wish to check your TCP/IP settings, the procedure is described in the following sections.
- If your LAN has a Router, the LAN Administrator must re-configure the Router itself.

Checking TCP/IP Settings - Windows 9x/ME:

1. Select *Control Panel - Network*. You should see a screen like the following:

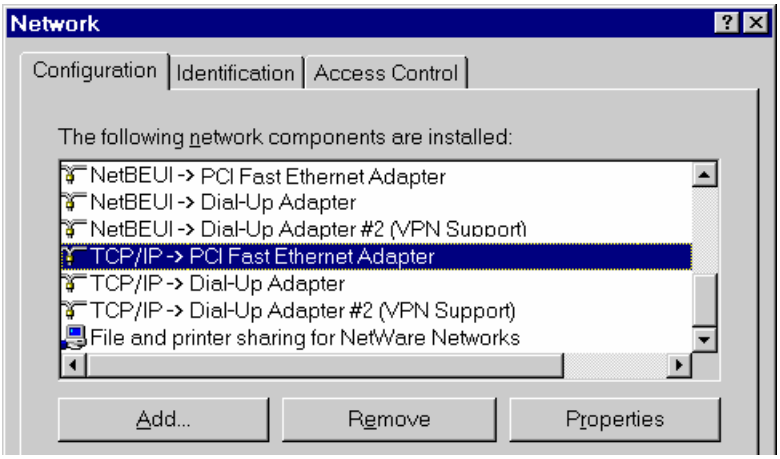

Figure B-1: Network Configuration

2. Select the *TCP/IP* protocol for your network card.
3. Click on the *Properties* button. You should then see a screen like the following.

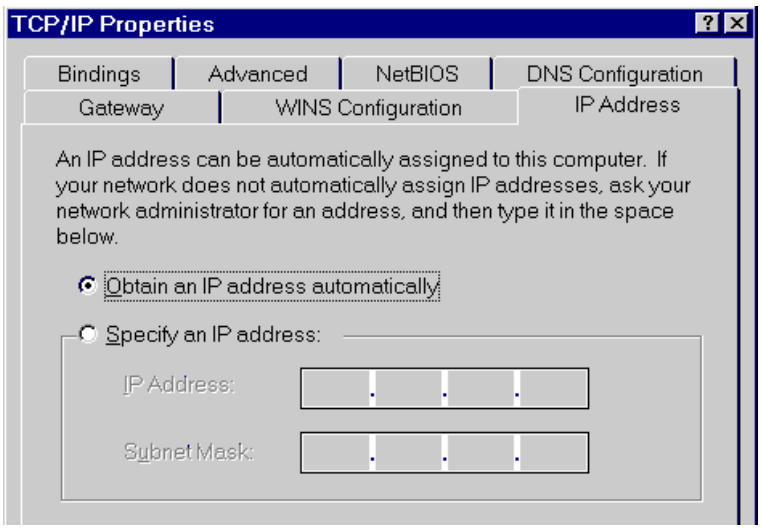

Figure B-2: IP Address (Win 95)

Ensure your TCP/IP settings are correct, as follows:

Using DHCP

To use DHCP, select the radio button *Obtain an IP Address automatically*. This is the default Windows settings.

Restart your PC to ensure it obtains an IP Address from The Load Balancer.

Using "Specify an IP Address"

If your PC is already configured, check with your network administrator before making the following changes:

- If the *DNS Server* fields are empty, select *Use the following DNS server addresses*, and enter the DNS address or addresses provided by your ISP, then click *OK*.
- On the *Gateway* tab, enter The Load Balancer's IP address in the *New Gateway* field and click *Add*, as shown below. (Your LAN administrator can advise you of the IP Address they assigned to The Load Balancer.)

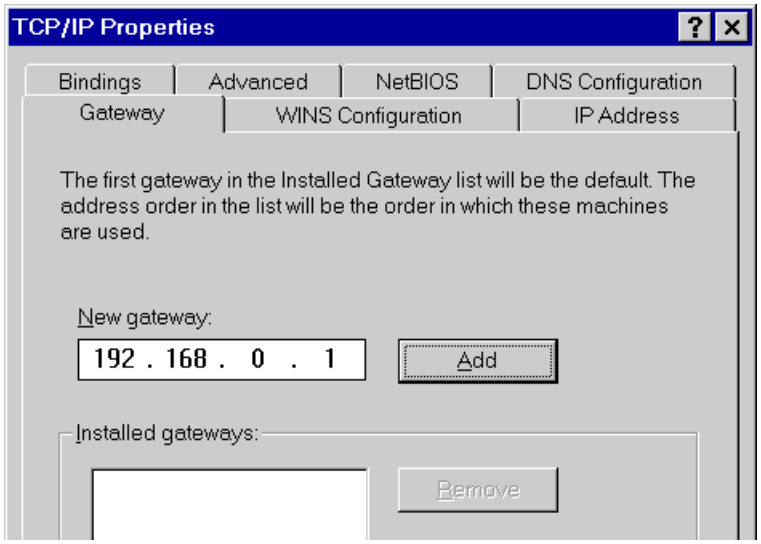

Figure B-3: Gateway Tab (Win 95/98)

- On the *DNS Configuration* tab, ensure *Enable DNS* is selected. If the *DNS Server Search Order* list is empty, enter the DNS address provided by your ISP in the fields beside the *Add* button, then click *Add*.

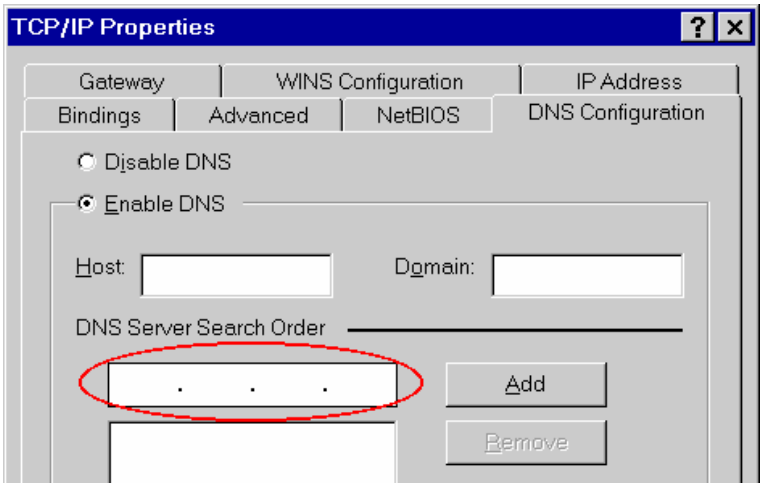

Figure B-4: DNS Tab (Win 95/98)

Checking TCP/IP Settings - Windows 2000:

1. Select *Control Panel - Network and Dial-up Connection*.
2. Right click the *Local Area Connection* icon and select *Properties*. You should see a screen like the following:

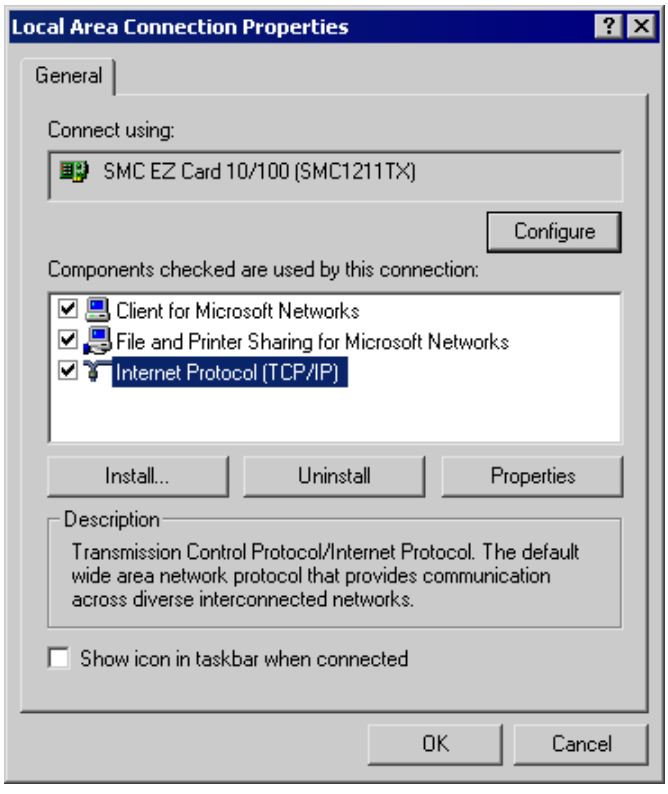

Figure B-5: Network Configuration (Win 2000)

3. Select the *TCP/IP* protocol for your network card.
4. Click on the *Properties* button. You should then see a screen like the following.

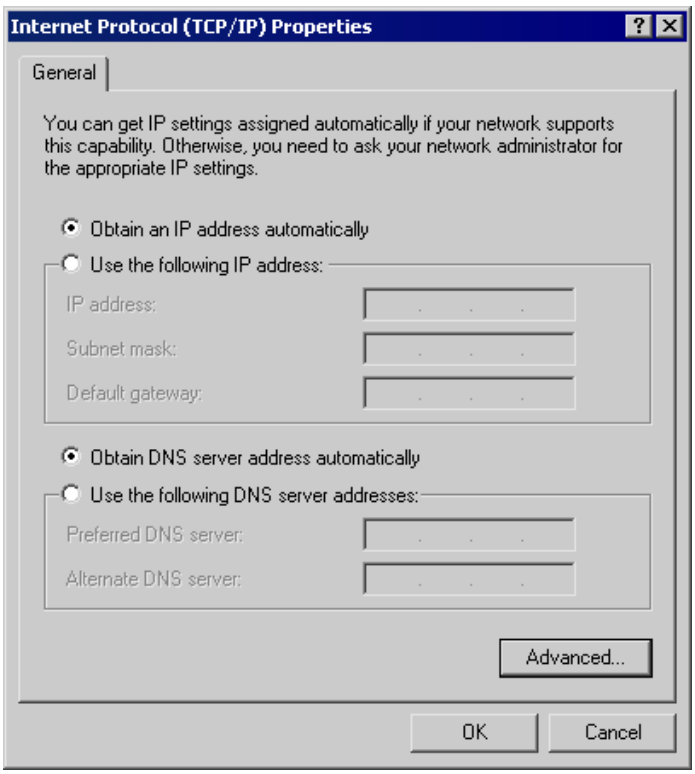

Figure B-6: TCP/IP Properties (Win 2000)

5. Ensure your TCP/IP settings are correct:

Using DHCP

To use DHCP, select the radio button *Obtain an IP Address automatically*. This is the default Windows settings.

Restart your PC to ensure it obtains an IP Address from The Load Balancer.

Using a fixed IP Address ("Use the following IP Address")

If your PC is already configured, check with your network administrator before making the following changes:

- Enter The Load Balancer's IP address in the *Default gateway* field and click *OK*. (Your LAN administrator can advise you of the IP Address they assigned to The Load Balancer.)
- If the *DNS Server* fields are empty, select *Use the following DNS server addresses*, and enter the DNS address or addresses provided by your ISP, then click *OK*.

Checking TCP/IP Settings - Windows XP:

1. Select Control Panel - Network Connection.
2. Right click the *Local Area Connection* and choose *Properties*. You should see a screen like the following:

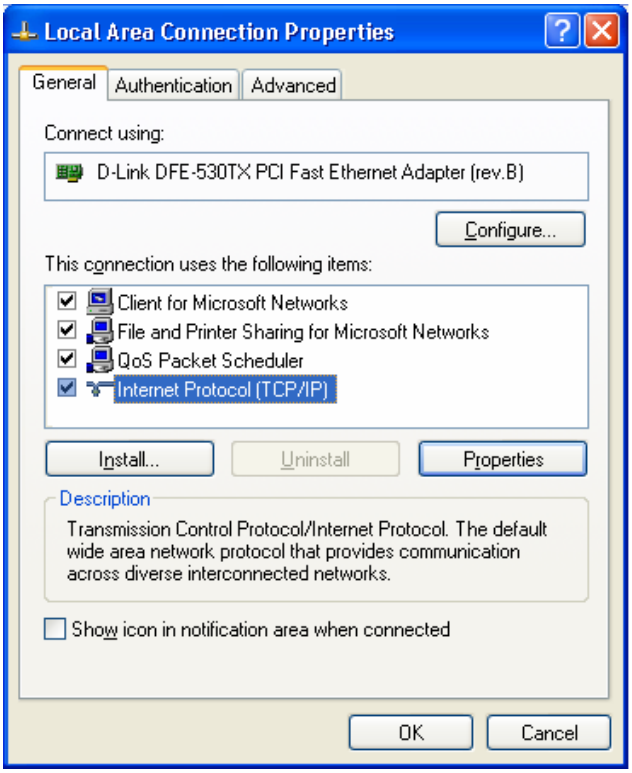

Figure B-7: Network Configuration (Windows XP)

3. Select the *TCP/IP* protocol for your network card.
4. Click on the *Properties* button. You should then see a screen like the following.

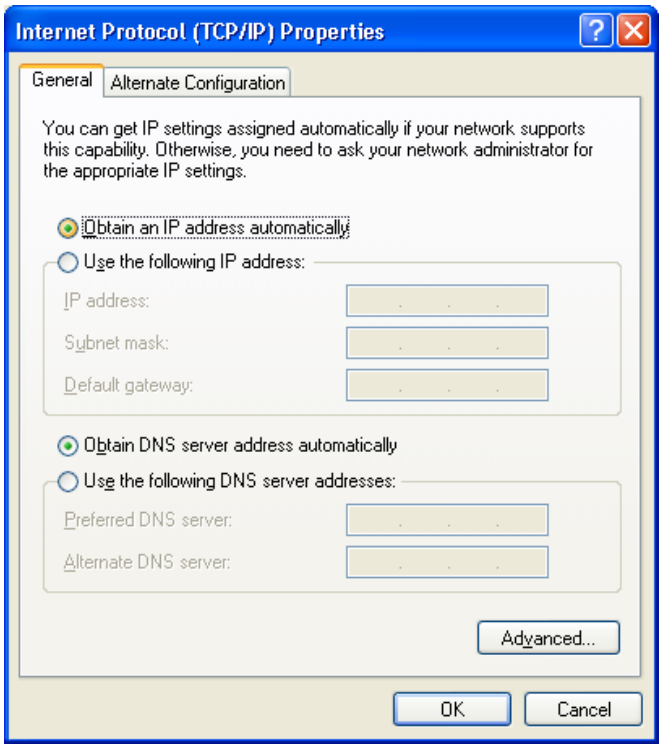

Figure B-8: TCP/IP Properties (Windows XP)

5. Ensure your TCP/IP settings are correct.

Using DHCP

To use DHCP, select the radio button *obtain an IP Address automatically*. This is the default Windows settings.

Restart your PC to ensure it obtains an IP Address from The Load Balancer.

Using a fixed IP Address ("Use the following IP Address")

If your PC is already configured, check with your network administrator before making the following changes.

- Enter The Load Balancer's IP address in the *Default gateway* field and click *OK*. (Your LAN administrator can advise you of the IP Address they assigned to The Load Balancer.)
- If the *DNS Server* fields are empty, select *Use the following DNS server addresses*, and enter the DNS address or addresses provided by your ISP, then click *OK*.

Appendix C

Troubleshooting

Overview

This chapter covers some common problems that may be encountered while using The Load Balancer and some possible solutions to them. If you follow the suggested steps and The Load Balancer still does not function properly, contact your dealer for further advice.

General Problems

Problem 1:	**Can't connect to The Load Balancer to configure it.**
Solution 1:	Check the following: • The Load Balancer is properly installed, LAN connections are OK, and it is powered ON. • Ensure that your PC and The Load Balancer are on the same network segment. (If you don't have a router, this must be the case.) • If your PC is set to "Obtain an IP Address automatically" (DHCP client), restart it. • If your PC uses a Fixed (Static) IP address, ensure that it is using an IP Address within the range 192.168.1.2 to 192.168.1.254 and thus compatible with The Load Balancer's default IP Address of 192.168.1.1. Also, the Network Mask should be set to 255.255.255.0 to match The Load Balancer. In Windows, you can check these settings by using *Control Panel-Network* to check the *Properties* for the TCP/IP protocol.

Internet Access

Problem 1:	**When I enter a URL or IP address I get a time out error.**
Solution 1:	A number of things could be causing this. Try the following troubleshooting steps. • Check if other PCs work. If they do, ensure that your PCs IP settings are correct. If using a Fixed (Static) IP Address, check the Network Mask, Default gateway and DNS as well as the IP Address. • If the PCs are configured correctly, but still not working, check The Load Balancer. Ensure that it is connected and ON. Connect to it and check its settings. (If you can't connect to it, check the LAN and power connections.) • If The Load Balancer is configured correctly, check your Internet connection (DSL/Cable modem etc) to see that it is working correctly.
Problem 2:	**Some applications do not run properly when using The Load Balancer.**

Solution 2:	The Load Balancer processes the data passing through it, so it is not transparent. Use the *Special Applications* feature to allow the use of Internet applications which do not function correctly. If this does solve the problem you can use the *DMZ* function. This should work with most applications, but: • It is a security risk, since the firewall is disabled for the *DMZ* PC. • Only one (1) PC can use this feature.