Micronet
Faster and Easier Networks

User's Manual

Broadband VPN Router

Model No.: SP880B

http://www.micronet.info

Table of Content

1. Introduction

Micronet SP880B Broadband VPN Router is an ideal broadband router for establishing VPN connection. It supports up to 20 IPSec VPN tunnels which helps users to setup widely private network application for small and medium office. SP880B's highly configurable built-in network firewall provides you with the power to choose the specific services allowed through your network, while keeping all malicious Internet attackers out. Its QoS function will prioritize traffic allowing specified packets to pass-through. This feature is especially important if you use real-time applications like Internet phone, video conference... etc. SP880B also provides simple Web-based interface, which will help network administrators to set up the router just in few minutes.

1.1 Package Contents

Verify the package contains the following items:

- SP880B Broadband VPN Router
- Quick Installation Guide
- Manual CD
- Power Adapter
- RJ-45 cable

1.2 Features

Micronet SP880B provides the following features:

- Support IPSec VPN for remote resource sharing by secure tunneling technology
- Provide 4 ports of 10/100M Ethernet for connecting to a home or office network
- Support Priority QoS by source and destination IP, MAC address and QoS-ToS service types for best resource allocation
- Provide firewall protection based on DoS, SPI, Ping to Death, Port scan and Access Control
- Support URL filter, Access filter and session limit for restricting inappropriate transmission
- Support multi-DMZ, Virtual Server and Special Application functions for Internet Service hosting
- Support IPsec and PPTP VPN Pass Through
- Support DDNS for dynamic IP environment
- Support Universal Plug and Play (UPnP) for peer-to-peer network connectivity
- Support NAT function to share single account with multiple workstations
- Support easy management via Web UI, SNMP, Email alert and Syslog
- Firmware upgradeable for further function enhancement

1.3 System Requirement

- One External xDSL (ADSL) or Cable modem with an Ethernet port (RJ-45)
- Network Interface Card (NIC) for each Personal Computer (PC)
- PCs with a Web-Browser (Internet Explorer 4.0 or higher, or Netscape Navigator 4.7 or higher)

1.4 Physical Description

1.4.1 Front Panel

SP880B Front Panel

POWER LED

This LED comes on when the router is properly connected to power.

Port LEDs

Every RJ-45 port on the front panel has two relevant LEDs (10/100M; LINK/ACT) for indicating the connection speed and activity status.

LEDs Status

Please refer to the following table for LED definition

LED	Status	Operation
Power	Steady Green	Power is on
	Off	Power is off
System	Steady Green	Firmware unloaded or Hardware error
	Off	Normal operation
	Blinking	Transmitting or receiving data
LINK/ACT	Steady Green	Network connection established
	Off	No connection established
	Blinking	Transmitting or receiving data
LAN 10/100M	Steady Green	100M network connection established
	Off	10M network connection established
WAN 10/100M	Steady Green	Network connection established
	Off	No connection established

1.4.2 Rear Panel

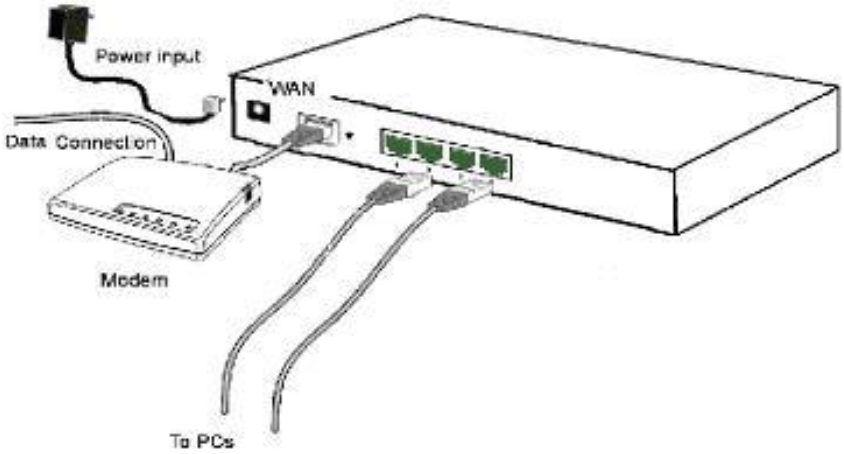
SP880B Rear Panel

DC 5V	Connect the supplied power adapter here.
Reset	After pressing and releasing the reset button, the router will reboot (restart) within 1 second and resets to default if button is pressed for over 3 seconds. *(Please refer to **default setting** below)*
LAN Ports	Connect the PCs to these ports. Both 10BaseT and 100BaseT connections can be used simultaneously. **Note:** Every port can 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 router has finished booting, all configuration settings will be set to the factory defaults as follows:
  IP Address: **192.168.1.1**
  Network Mask: **255.255.255.0**
  DHCP Server: enabled
  User Name: admin
  Password cleared (no password)

2. Installation

2.1 Hardware Installation



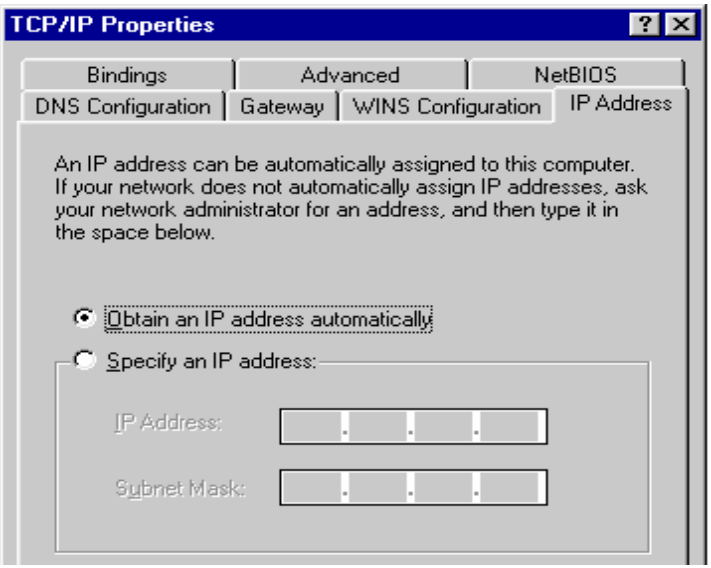
1. Shut off the power on all devices, including PCs, your DSL/Cable modem and SP880B.
2. Connect a network cable from one of your PC's Ethernet port to one of LAN port on the back of the SP880B.
3. Connect the network cable from your DSL/Cable modem to the WAN port of the SP880B.
4. Connect the power adapter to the power jack on the rear of SP880B, and then plug the power adapter into the power outlet.
5. Turn on the power of the DSL/Cable modem.

2.2 Access Router

Below is a step-by-step instruction on how to access the SP880B from your PCs and get connection to the Internet.

1. Set your LAN PC clients to "**Obtain an IP Address automatically"** so that it can obtain an IP address from DHCP server. (If you have already configured your PC to obtain an IP automatically then proceed to step 3).
   For all non-Server versions of Windows, the default TCP/IP setting is to act as a DHCP client. Just start (or restart) your PC, and it will obtain an IP address from the Router. By default, the SP880B will act as a **DHCP Server**, automatically providing a suitable IP Address (and related information) to each PC when the PC boots. This section will instruct you on how to configure your PC's for either Windows 95/98/Me, 2000, NT operating systems, Macintosh or Linux. For other operating systems (Macintosh, Sun, etc.), please refer to system manufacturer's instructions.

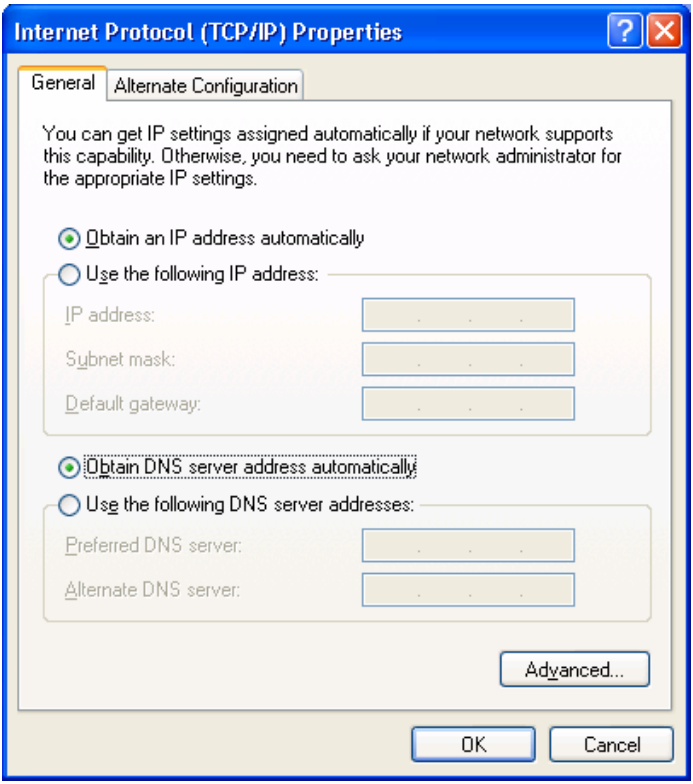
- **Windows 95/98/Me**
  a. Click the ***Start*** button and select ***Settings***, then click ***Control Panel***. The ***Control Panel*** window will appear.
  b. Double-click the ***Network*** icon. The ***Network*** window will appear.
  c. Check your list of Network Components. If TCP/IP is not installed, click the ***Add*** button to install it now. If TCP/IP is installed, go to **step 6**.
  d. In the ***Network Component Type*** dialog box, select ***Protocol*** and click the ***Add*** button.
  e. In the ***Select Network Protocol*** dialog box, select ***Microsoft*** and ***TCP/IP*** and then click the ***OK*** button to start installing the TCP/IP protocol. You may need your Windows CD to complete the installation.
  f. After installing TCP/IP, go back to the ***Network*** dialog box. Select ***TCP/IP*** from the list of ***Network Components*** and then click the ***Properties*** button.
  g. Check each of the tabs and verify the following settings:
     - **Bindings**: Check *Client for Microsoft Networks* and *File and printer sharing for Microsoft Networks*.
     - **Gateway**: All fields are blank.
     - **DNS Configuration**: Select *Disable DNS.*
     - **WINS Configuration**: Select *Disable WINS Resolution.*
     - **IP Address**: Select *Obtain IP address automatically*.



  h. Reboot the PC. Your PC will now obtain an IP address automatically from your Broadband Router's DHCP server. Once you've configured your PC to obtain an IP address automatically, please proceed to Step 3.

Note: Make sure that the Broadband router's DHCP server is the only DHCP server available on your LAN.

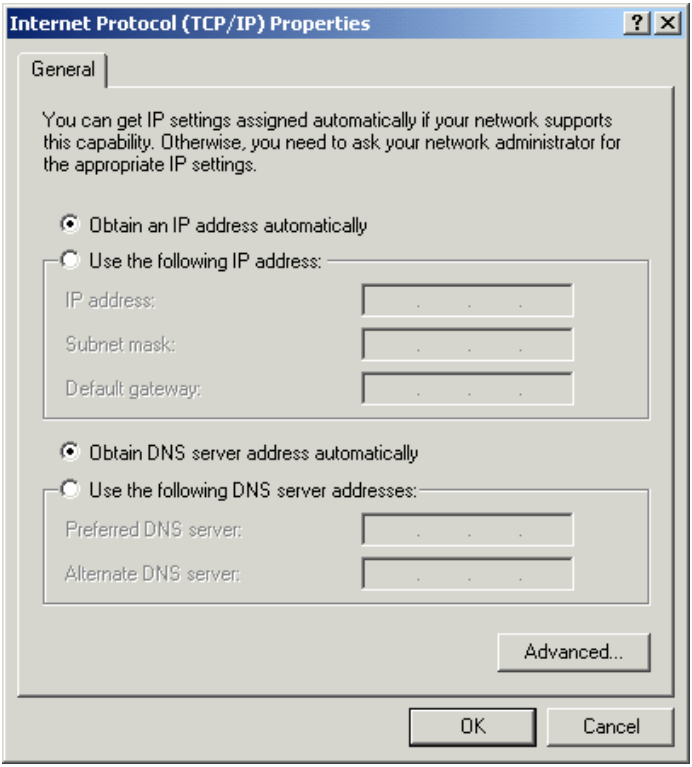
- **Windows XP**
  a. Click the *Start* button and select ***Settings***, then click *Network Connections.* The *Network Connections* window will appear.
  b. Double-click *Local Area Connection* icon. The ***Local Area Connection*** window will appear.
  c. Check your list of Network Components. You should see ***Internet Protocol [TCP/IP]*** on your list. Select it and click the ***Properties*** button.
  d. In the Internet Protocol (TCP/IP) Properties window, select ***Obtain an IP address automatically*** and ***Obtain DNS server address automatically*** as shown on the following screen.



  e. Click ***OK*** to confirm the setting. Your PC will now obtain an IP address automatically from your Broadband Router's DHCP server. Once you've configured your PC to obtain an IP address automatically, please proceed to Step 3.

Note: Make sure that the Broadband router's DHCP server is the only DHCP server available on your LAN.

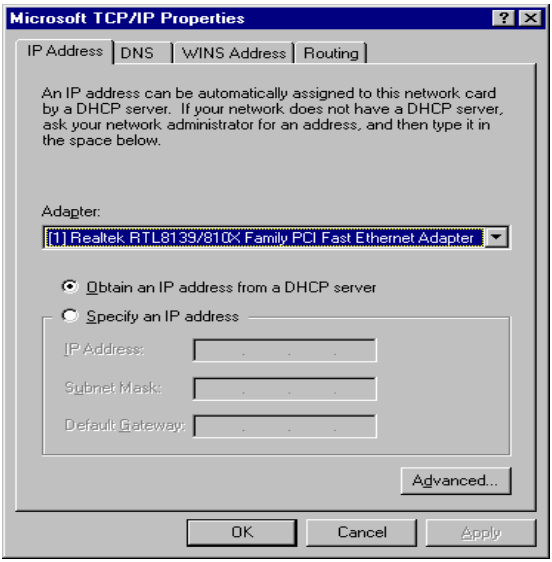
- **Windows 2000**
  a. Click the *Start* button and select ***Settings***, then click ***Control Panel***. The ***Control Panel*** window will appear.
  b. Double-click *Network and Dial-up Connections* icon. In the *Network and* ***Dial-up Connection*** window, double-click *Local Area Connection* icon. The *Local Area Connection* window will appear.
  c. In the ***Local Area Connection*** window, click the ***Properties*** button.
  d. Check your list of Network Components. You should see ***Internet Protocol [TCP/IP]*** on your list. Select it and click the *Properties* button.
  e. In the Internet Protocol (TCP/IP) Properties window, select ***Obtain an IP address automatically*** and ***Obtain DNS server address automatically*** as shown on the following screen.



  f. Click *OK* to confirm the setting. Your PC will now obtain an IP address automatically from your Broadband Router's DHCP server. Once you've configured your PC to obtain an IP address automatically, please proceed to Step 3.

Note: Make sure that the Broadband router's DHCP server is the only DHCP server available on your LAN.

- **Windows NT**
  a. Click the *Start* button and select *Settings*, then click *Control Panel*. The ***Control Panel*** window will appear.
  b. Double-click *Network* icon. The ***Network*** window will appear. Select the ***Protocol*** tab from the ***Network*** window.
  c. Check if the *TCP/IP Protocol* is on your list of ***Network Protocols***. If TCP/IP is not installed, click the ***Add*** button to install it now. If TCP/IP is installed, go to **step 5**.
  d. In the ***Select Network Protocol*** window, select the ***TCP/IP Protocol*** and click the ***Ok*** button to start installing the TCP/IP protocol. You may need your Windows CD to complete the installation.
  e. After installing TCP/IP, go back to the ***Network*** window. Select ***TCP/IP*** from the list of ***Network Protocols*** and then click the ***Properties*** button.
  f. Check each of the tabs and verify the following settings:
     - **IP Address**: Select *Obtain an IP address from a DHCP server*.
     - **DNS:** All fields are blank.
     - **WINS:** All fields are blank.
     - **Routing:** All fields are blank.



  g. Click *OK* to confirm the setting. Your PC will now obtain an IP address automatically from your Broadband Router's DHCP server. Once you've configured your PC to obtain an IP address automatically, please proceed to Step 3.

Note: Make sure that the Broadband router's DHCP server is the only DHCP server available on your LAN.

- **Macintosh Clients**
  From your Macintosh, you can access the Internet via the Router by the following procedure:
  a. Open the TCP/IP Control Panel.
  b. Select *Ethernet* from the *Connect via* pop-up menu.
  c. Select *Using DHCP Server* from the *Configure* pop-up menu. The DHCP Client ID field can be left blank.
  d. 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 Router's IP Address.
  - Ensure your *DNS* settings are correct.

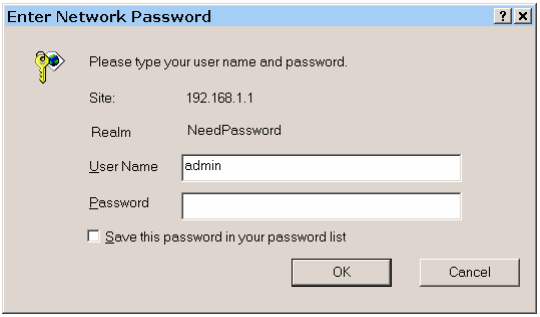
- **Linux Clients**
  To access the Internet via the Router, simply set the Router as the "Gateway", and ensure your *Name Server* settings are correct.
  Ensure you are logged in as "root" before attempting any changes.
  - Fixed IP Address
    By default, most UNIX installations use a fixed IP Address. If you wish to continue using a fixed IP Address, make the following changes to your configuration.
    1. Set your *Default Gateway* to the IP Address of the Router.
    2. 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 is 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.

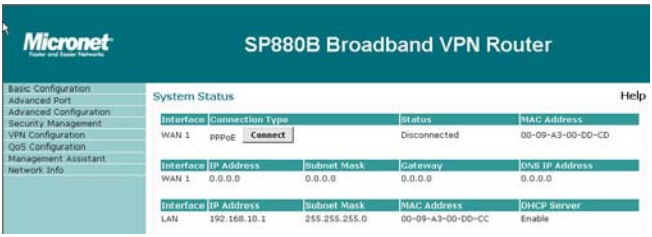
2. Restart your computer if necessary.
3. Open the Internet Explorer and type **http://192.168.1.1** (broadband router's IP address) into the browser address window to access the SP880B.
4. Login information request page will pop up as shown below. Key in the **user name** field

as “**admin**” and leave the **password** field **blank**.

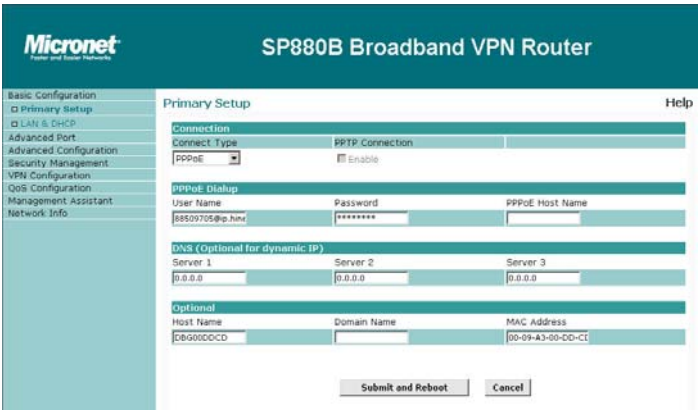


Note: By default there is no password. For security reasons it is recommended that you change the password as soon as possible.

5. The home page will show up after login in process as shown below.



6. In the “Basic Configure” field, select “**Primary Setup**” from the menu and configure WAN 1 as required. Fill in the information necessary to access the Internet.



3. Basic Configuration

SP880B provides a web-based interface, allowing users to configure and manage the router remotely from web browser.

3.1 Primary Setup

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

- Configure WAN as required.
- For any of the following situations, which may be required further configuration refer to ***Chapter 3.2: Advanced Port Setup***.
  - Multiple PPPoE sessions
  - PPTP connection method

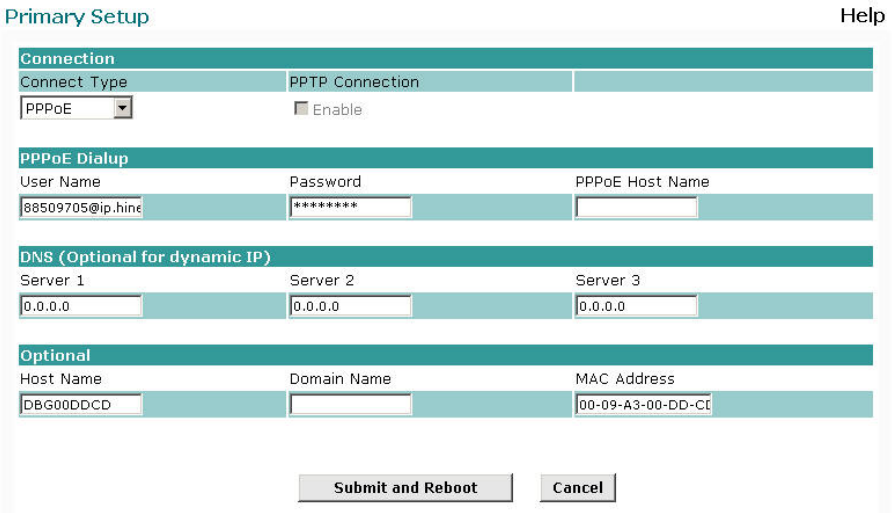


Figure: Primary Setup

Settings – Primary Setup

Connection	• **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. 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*, whichever is 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 addresses, 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 has 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 has provided a Domain Name, enter it here. Otherwise, you can use the default value. • **MAC address** – Some ISPs 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 Router is now completed. You must proceed to configure the PCs on your LAN. See the following section for details.

3.2 LAN & DHCP

Select LAN & DHCP from the menu. You will see a screen like the example below. These screens and settings are provided to deal with non-standard situations, or to provide additional options for advanced users.

Existing DHCP Server

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 Router must be disabled.
- Your DHCP Server must be configured to provide the Router's LAN IP address as the "Default Gateway".
- Your DHCP Server must provide correct DNS addresses to the PCs.

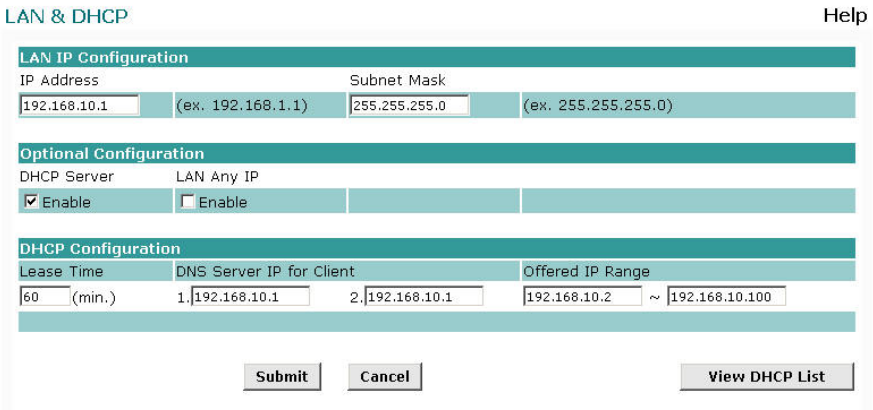


Figure: LAN & DHCP

Settings – LAN & DHCP

LAN IP Configuration	• **IP address –** This is the Router IP address to 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 Router is attached (the same value as the PCs on that LAN segment).
Optional Configuration	• **DHCP Server Setup** - If **Enabled**, the Router will allocate IP Addresses to PCs (DHCP clients) on your LAN when they start up. The default and recommended value is "Enabled". (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 Router as the *Default Gateway*. • **LAN Any IP** –By default, it is disabled. If you enable "LAN

	Any IP", it means no matter what static IP address the client (your PC) has. It does not need to change the IP address, even though it has a 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.
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 related information is shown. **Free Entry** indicates how many DHCP entries are not currently allocated, and still available. • **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 leftover time after the IP address is leased.

4. Advanced Port Setup

Overview

- Port Options contains some options for the WAN port. For most situations, the default values are satisfactory.
- 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.

4.1 Port Options

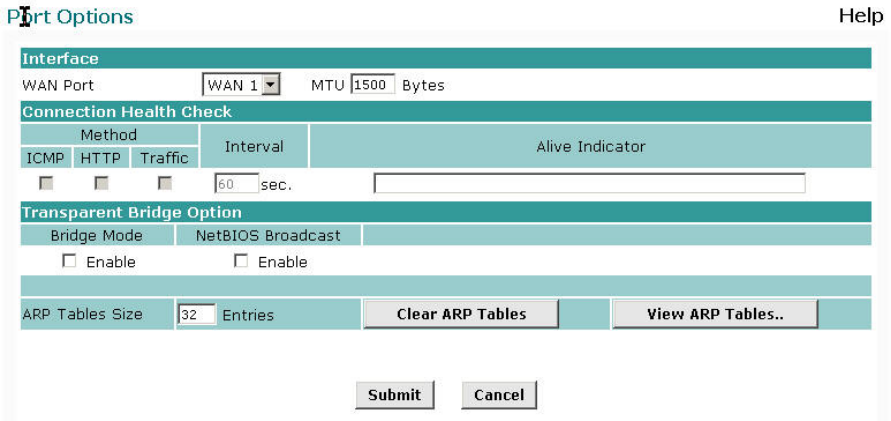


Figure: Port Options

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.
Connection Health Check	• **Method** – ▪ **ICMP:** The health checkup 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 responses 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. • **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.

4.2 Advanced PPPoE

In order to use multiple PPPoE sessions on the same WAN port, configuring the following screen is required.
This can also be used to manually connect or disconnect a PPPoE session.

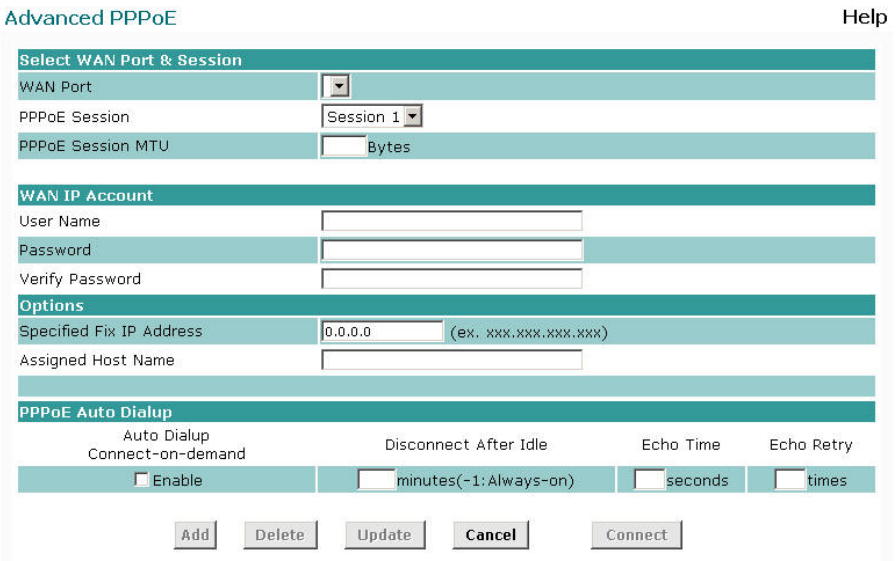


Figure: Advanced PPPoE

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 it here. Otherwise, this field should be left as 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, 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.

4.3 Advanced PPTP

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

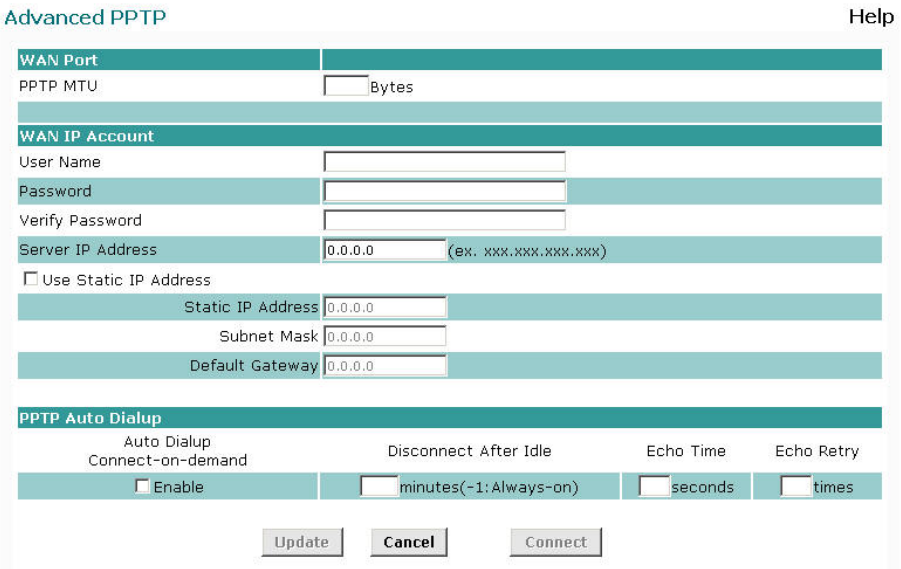


Figure: Advanced PPTP

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 it here. Otherwise, this field should be left as 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

5. Advanced Configuration

Overview

The following advanced features are provided.

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

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

5.1 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 enjoying 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.

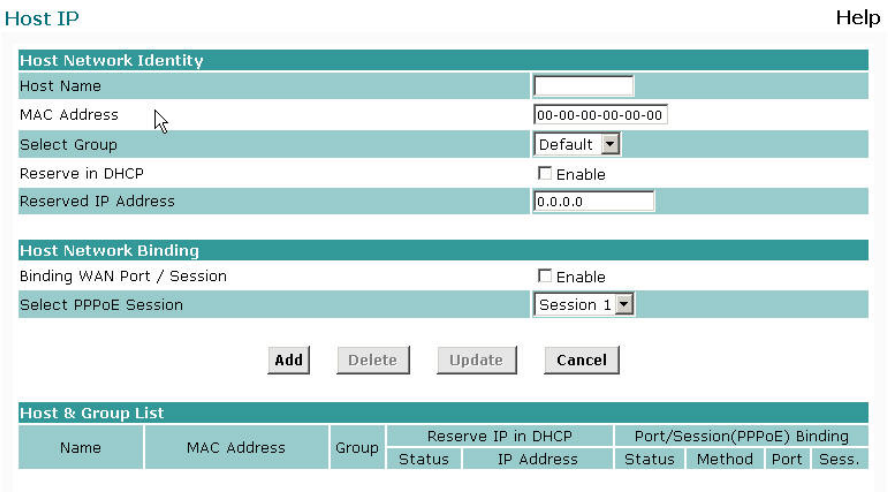


Figure: Host IP Setup

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. • **Select PPPoE session** – If the setting above is *Enable*, select the desired 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.

5.2 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.

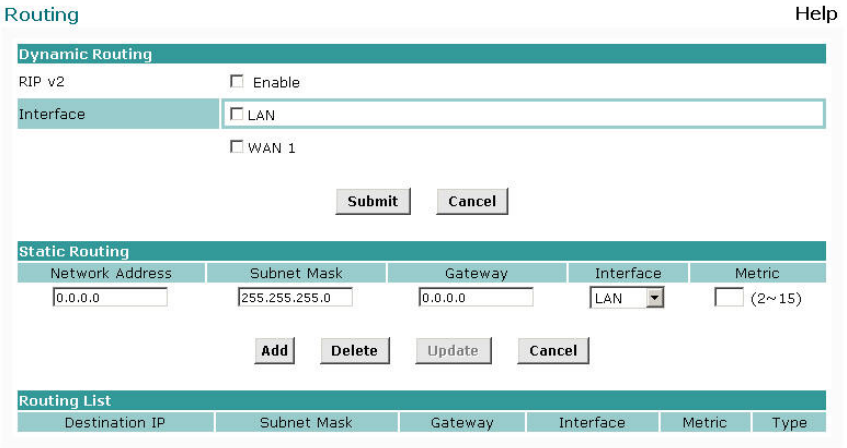


Figure: Routing

Note:
If there is an 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 and WAN1** – 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** – 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 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 Router, so that they can be forwarded to the Internet. This is done by configuring other Routers to use the Router as the Default Route or Default Gateway, as illustrated by the example below.

Static Routing – Example

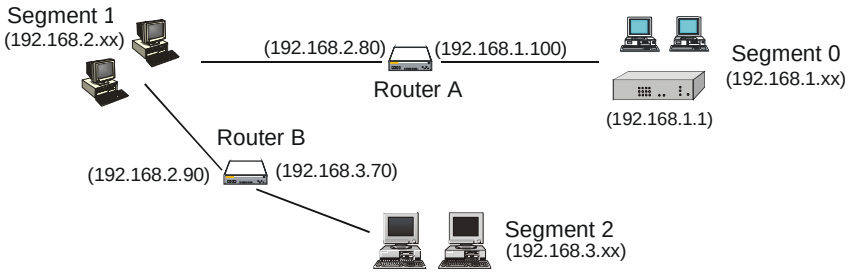


Figure: Routing Example

- For the Router Gateway's Routing Table

  For the LAN shown above, with 2 routers and 3 LAN segments, the 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

5.3 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 Router.

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

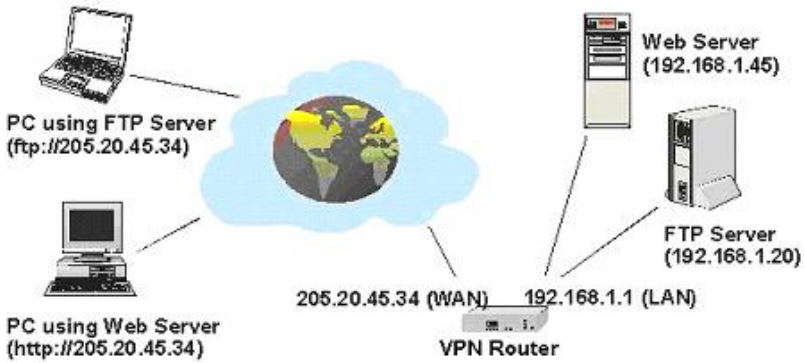


Figure: Virtual Servers

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 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

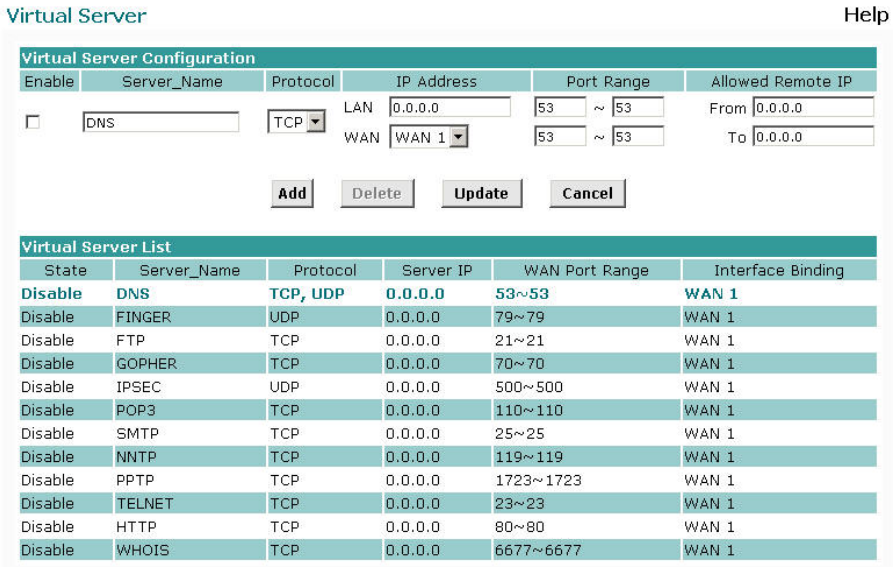


Figure: Virtual Server

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.

5.4 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 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

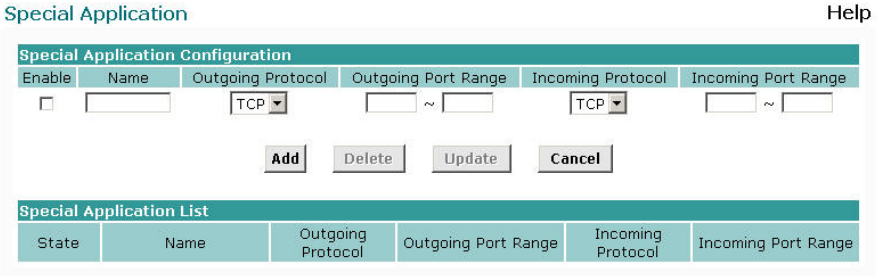


Figure: Special Applications

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 one 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.

5.5 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 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 get a Domain Name (Host name) allocated to you.
3. Configure the **Dynamic DNS** screen, as shown below.
4. The 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.

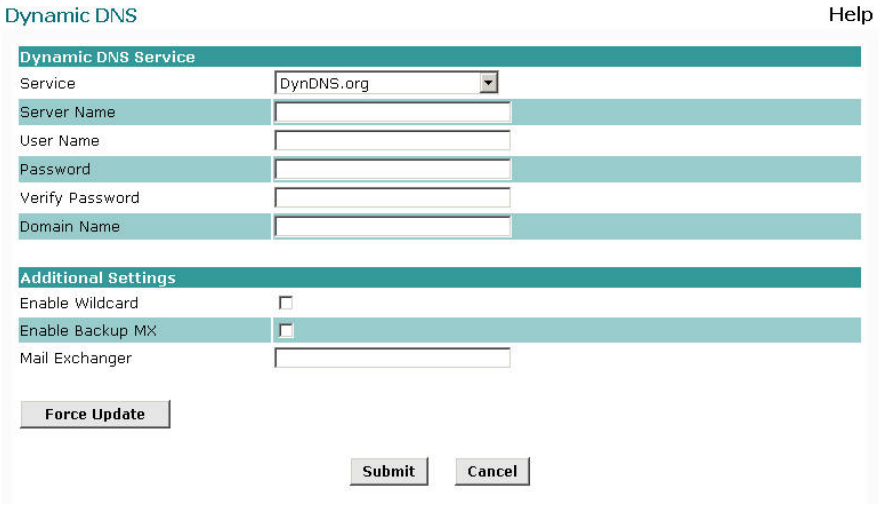


Figure: Dynamic DNS

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. • **DynDNS** – Select this to use the DynDNS service (from www.dyndns.org). You must configure the DynDNS section of this screen. • **3322(in China)** – This is available in China. It is similar to

	"DynDNS" • **User Defined DDNS Server** – This is the user defined DDNS server. If the DDNS other than TZO, dyndns.org and 3322.
Additional Settings	These options are available to 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.

5.6 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

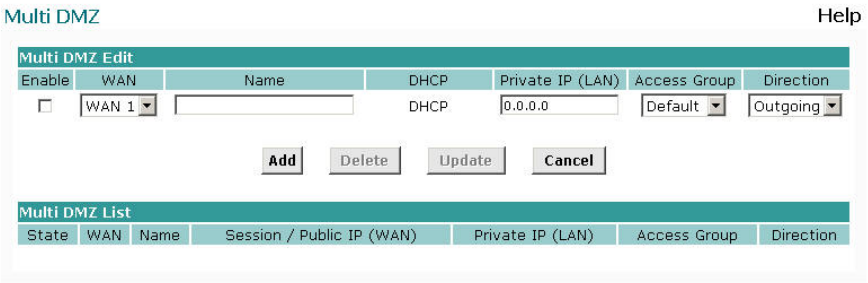


Figure: Multi DMZ

Settings – Multi DMZ

Multi DMZ Edit	• **Enable** – To activate or deactivate the current DMZ entry. • **WAN** – The WAN 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.

5.7 UPnP

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

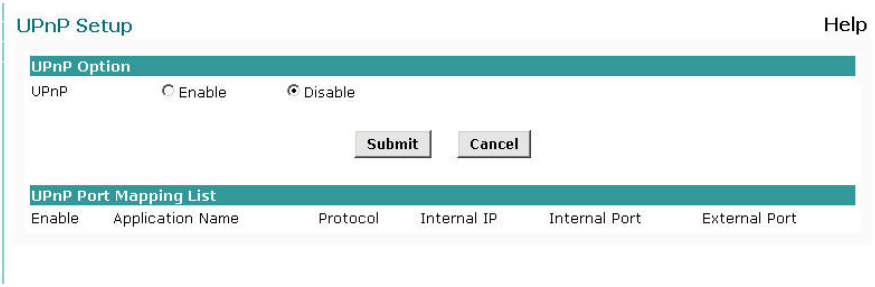


Figure: UPnP

Settings – UPnP

UPnP Option	UPnP (Universal Plug & Play) function makes it easy to set up and configure an entire network, enable discovery and control of the network devices and services
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

5.8 NAT Setup

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

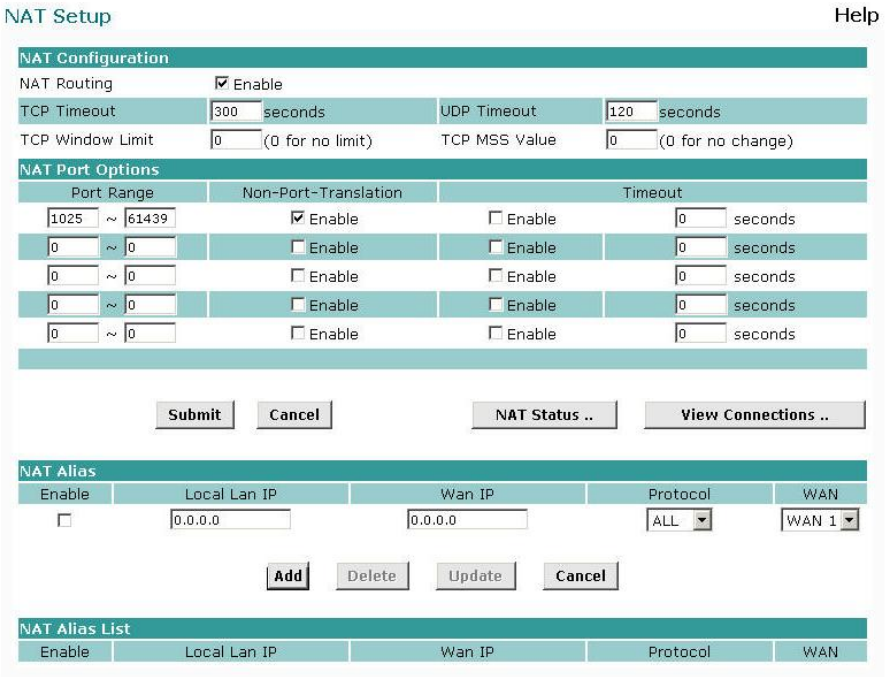


Figure: NAT

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.

5.9 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 meets all the checked items, the packet will be bound on the specified WAN port.

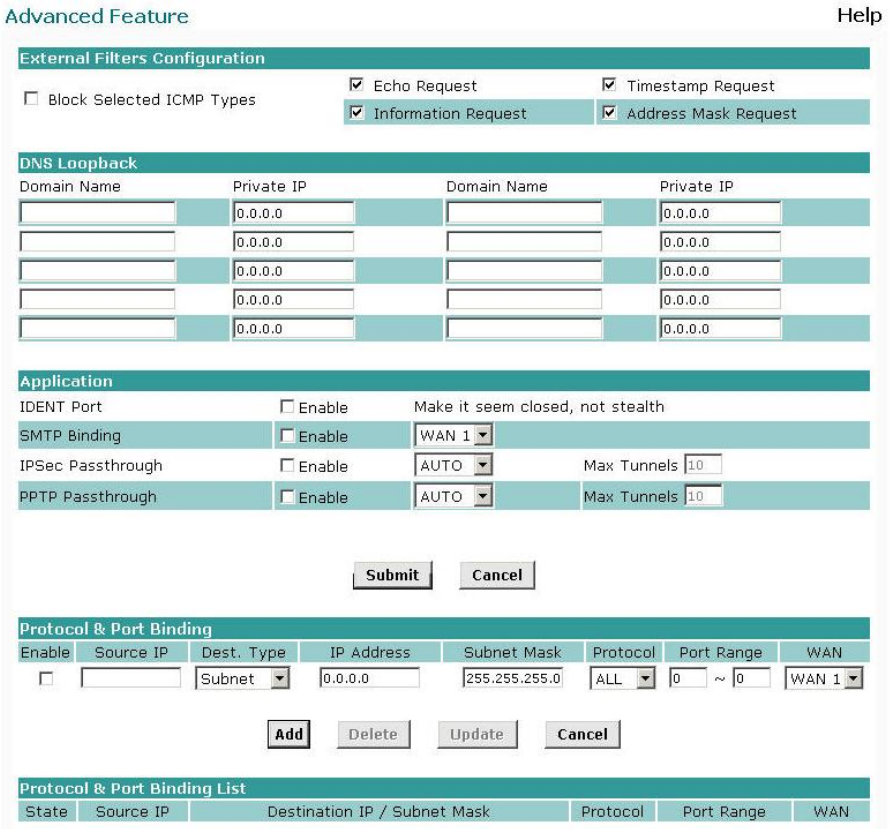


Figure: Advanced Features

Settings – Advanced Features

External Filters Configuration	• **Block Selected ICMP Types** –This acts as "master" switch. If checked, the selected packet types will be blocked. Otherwise, they will be 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 will close the port, 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 established a tunnel 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 all protocols and port binding that are currently defined.

6. Security Management

Overview

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

6.1 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.

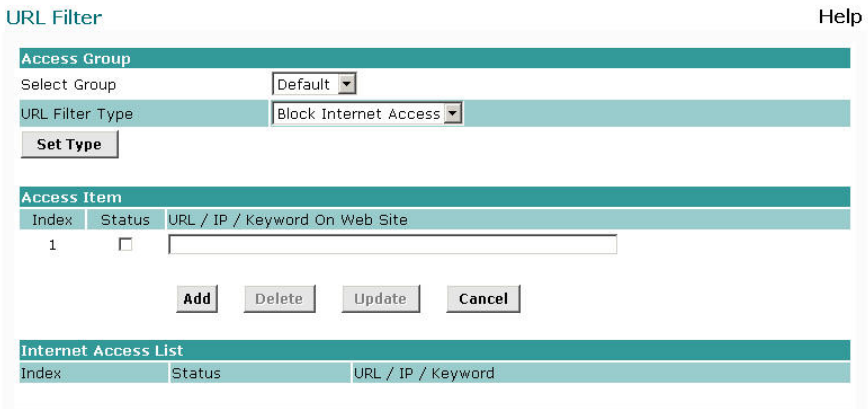


Figure: URL Filter

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 Interne Access:** All the web page accesses will be permitted if the targe 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.

6.2 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.

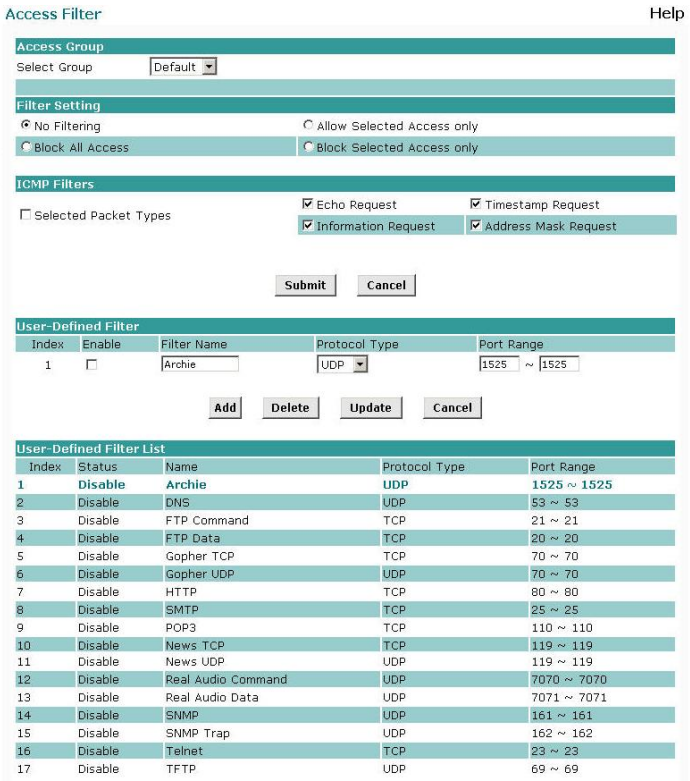


Figure: Access Filter

Settings – Access Filter

Access Group	The Group that the current rule is applied to. To apply the 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 filters which have been defined.

6.3 Session Limit

This new feature allows to dropping the new sessions from both WAN and LAN side, if the new session numbers are exceed the maximum sessions in a sampling time.

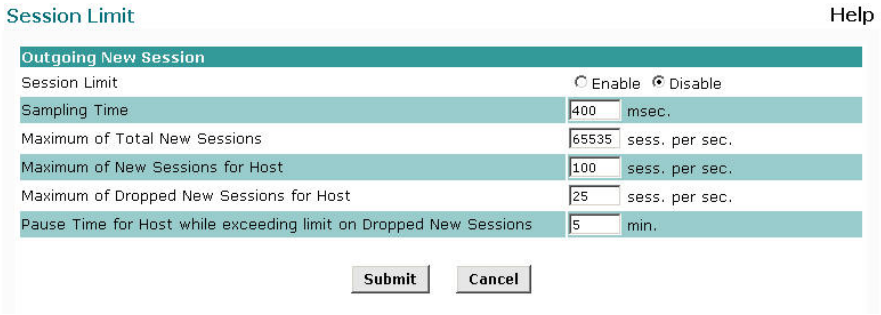


Figure: Session Limit

Settings – 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.)

6.4 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.

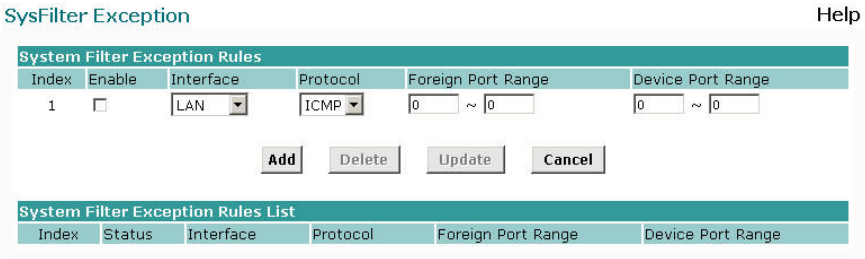


Figure: SysFilter Exception

Settings – SysFilter 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.

7. VPN Configuration

Overview

Virtual Private Network (VPN) is a connection between two end points. It allows private data to be sent securely over a public network, such as Internet. VPN establishes a private network that can send data securely between two networks by creating a “tunnel”. A VPN tunnel connects the two PCs or networks

Note: The SP880B VPN Router uses industry standard VPN protocol. However, due to variations in how manufactures interpret these standards, many VPN products are not interoperable. Although the SP880B VPN Router can interoperate with many other VPN products, it is not possible for SP880B VPN Router to provide specific technical support for every other product.

Planning the VPN:

When planning your VPN, you must make sure of the following items first.

1. If the remote end was a network, the two-endpoint network must have different LAN IP address ranges. If the remote endpoint 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. If you will be using the Internet Key Exchange (IKE) setup, or Manual Key, in which 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. The encryption level you are planning to use (DES or 3DES)?

7.1 IKE Global Setup

The following web page management will guide you on how to setup IKE (Internet Key Exchange) and make VPN work.

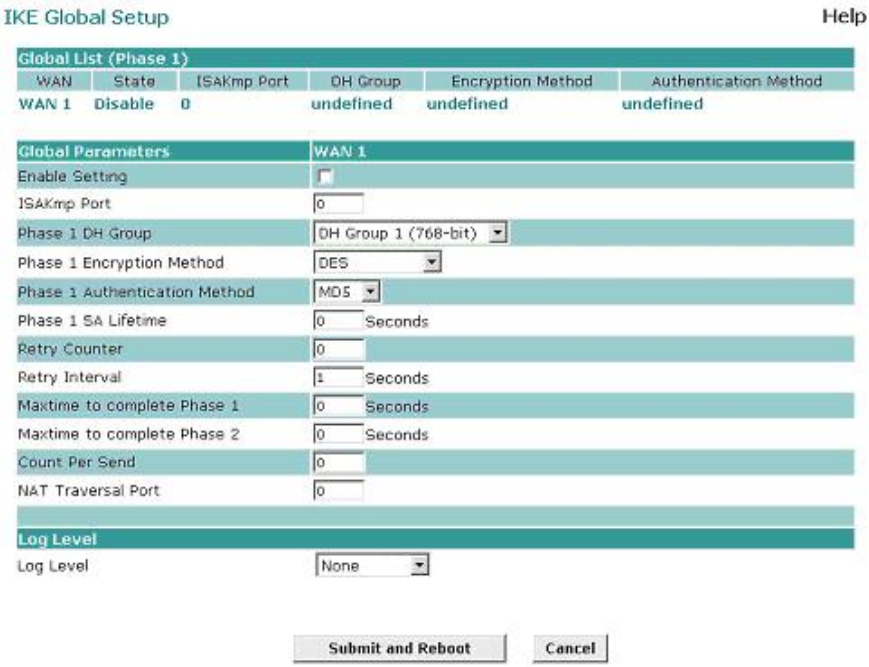


Figure: IKE Global Setup

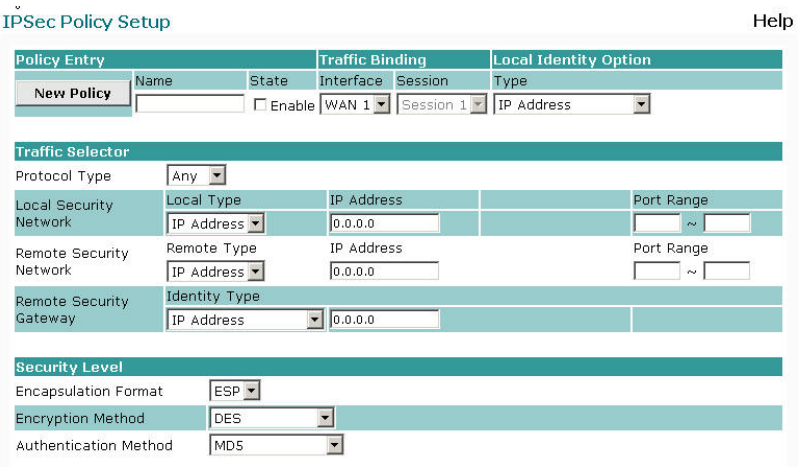
Settings – IKE Global Setup.

IP Global Setting	• **Enable Setting** – If you checked the box, this will start VPN global setting. • **ISAkmp Port** – Internet Security Association and Key Protocol Management (ISAkmp) is designed to negotiate, establish, modify and delete security associations and their attributes. In particular, it was assigned UDP port 500 by the IANA. • **Phase 1 DH Group** – Use DH Group 1(768-bits), DH Group 2(1024-bits), Group 5 (1536-bits) to generate IPSec SA keys. • **Phase 1 Encryption Method** – There are three data encryption methods available, DES, 3DES and AES. • **Phase 1 Authentication Method** – There are two authentication available. MD5 and SHA1 (Secure Hash Algorithm) • **Phase 1 SA Life Time** – By default the Security Association lifetime is 28800 Sec**.**

	• **Maxtime to complete phase 1** – The aim of phase 1 is to authenticate and establish a secure tunnel, which will protect further IKE negotiation. The maximum time default is 300 sec. • **Maxtime to complete phase 2** – Really establish the IPSec SAs. By default the maximum time is 300 sec. • **Count Per Send** – Number of duplicated packets for resend. • **NAT Traversal Port** – If there is other router on the network and didn't support VPN pass through, when you connect the SP880B to the router and want to make a VPN connection, this function will allow the VPN packets to pass through the router and make a VPN connection without any problem.
Log Level	It is a VPN Log Level. Select a VPN log level that you like to display on VPN log.

7.2 IPSec Policy Setup

VPN Policy Setup is to define the VPN phase 2 policy, including encryption and authentication methods. Once you have made the configuration you can press the "connection" button to make the VPN connection. You can also press "set option" button to do more detail of VPN policy.



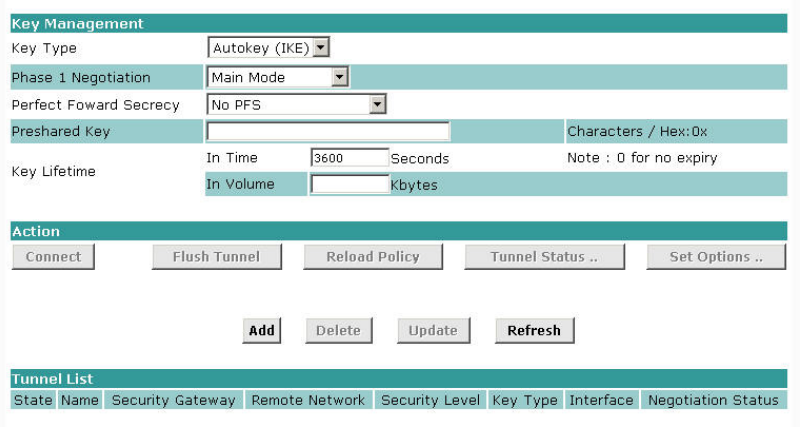


Figure: IPSec Policy Setup

Settings – IPSec Policy Setup

Policy Entry	• **Tunnel Name** – Given a name for this tunnel. • **State** – Enable/Disable VPN policy state.
Traffic Binding	• **Interface** – Select WAN1 for binding VPN tunnel.
Local Identity Option	• **Type** – There are three local WAN identity types to choose from: IP address, domain name and distinguished name.
Traffic Selector	• **Protocol Type** – You can choose either TCP/UDP/ICMP/GRE protocol as your connection protocol. By default the protocol type is “Any”. • **Local Security Network** – These entries identify the private network on this VPN router, 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** – These entries identify the private network on the remote peer VPN router 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** – You can either select remote side domain name or remote side IP address (WAN IP

	address) as your remote side security gateway.
Security Level	• **Encryption Method** – It specifies the encryption mechanism to use. Data encryption makes the data unreadable if intercepted. There are three encryption method available; DES/3DES and AES. The default is null. • **Authentication** – It specifies the packets authentication mechanism to use. Packets authentication confirms that data comes from the source you think it comes from. There are three authentications available. MD5, SHA1 and SHA2.
Key Management	• **Key Type** – There are two key types (manual key and auto key) available for the key exchange management. • **Manual Key** – If manual key is selected, no key negotiation is needed. Encryption Key- This field specifies a key to encrypt and decrypt IP traffic. Authentication Key – This field specifies a key use to authentication IP traffic. Inbound/outbound SPI (Security Parameter Index) – is carried on the ESP header. Each tunnel must have a unique inbound and outbound SPI, and no two tunnels share the same SPI. Notice that Inbound SPI must match the other router's outbound SPI. • **AutoKey (IKE)** – There are two types of operation modes can be used. 1. **Main mode** accomplishes a phase one IKE exchange establishing a secure channel. 2. **Aggressive Mode** 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) – If PFS is enabled, IKE phase 2 negotiation will generate a new key material for IP traffic encryption & authentication. Preshared Key – This field is to authenticate the remote IKE peer. • **Key Lifetime**- This is specified the lifetime of the IKE generated Key. If the time expires or data is passed over this volume, a new key will be renegotiated. By default, 0 is for no

	limit.
Tunnel List	• List all VPN tunnel that you have configured, so you can modify, update, and delete each VPN record.

8. QoS Configuration

Overview

The Router supports QoS, providing high quality of network service.
It will classify outgoing packets based on policies defined by users and provide better response or performance to various real-time applications.

8.1 QoS Setup

The following web page management will guide you on how to setup QoS and make QoS work.

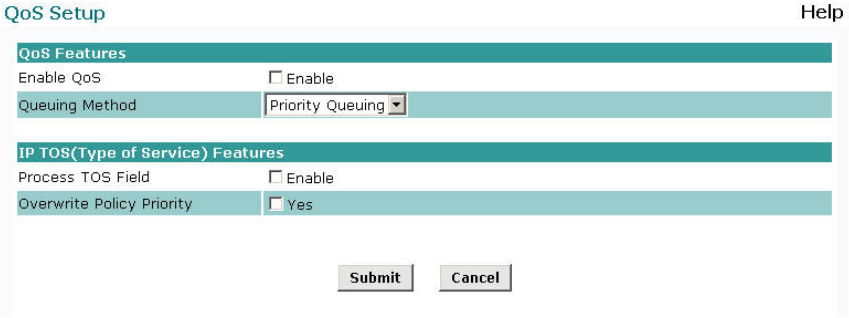


Figure: QoS Setup

Settings – 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 first. • **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 are always transmitted ahead of others.
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 this function will process the IP Type of Service field. • **Overwrite policy priority** – Choose “yes” to set the priority of TOS field in IP packet and overwrite the priority defined in policy configuration

8.2 QoS Policy

By setting the **QoS** policy, you can assign a higher/lower priority (based on your configuration) to received packets 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.

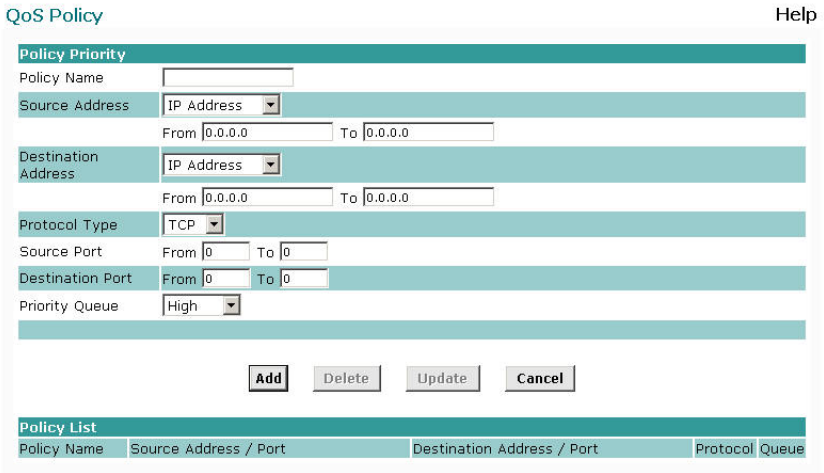


Figure: QoS Policy

Settings – QoS Policy

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. There are two types of address: 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 defines 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

9. Management Assistant

Overview

The following advanced features are offered.

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

9.1 Administration Setup

This chapter contains details on the configuration and use of each of these features. The password screen allows you to assign a password to the Router and enable /disable the remote access mechanism.

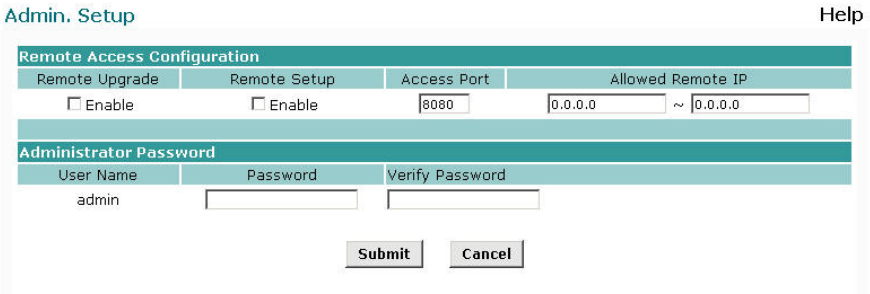


Figure: Admin Password

Enter the desired password, re-enter it in the Verify Password field, then save it.
When you connect to the Router with your Browser, you will be prompted for the password as shown below.

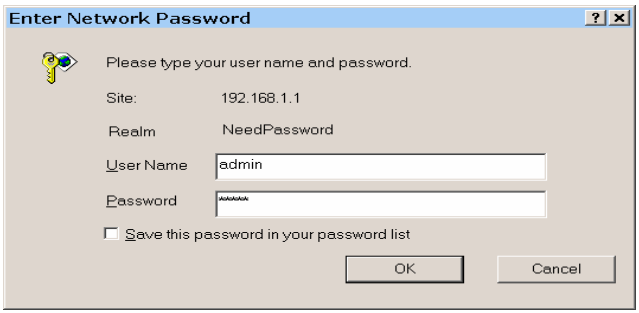


Figure: Password Dialog

- Enter "Admin" for the User Name.
- Enter the password for the Router, as set on the Admin Password screen above.

9.2 Email Alert

This feature will send a warning Email to inform system administrator that one of the WAN ports is 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.

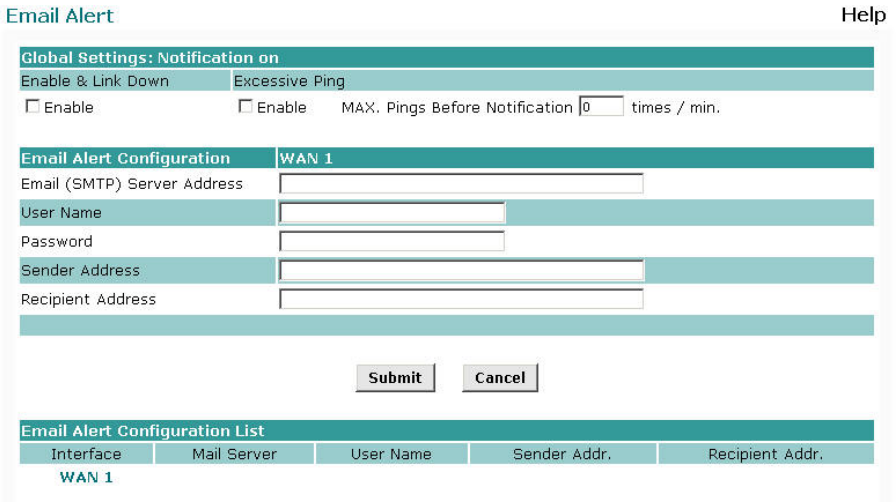


Figure: Email Alert

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 on 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 message that you have configured previously.

9.3 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 Router.

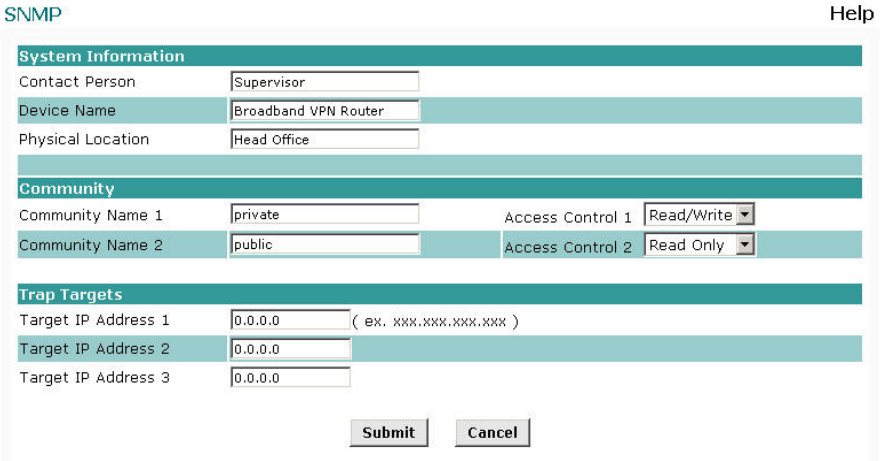


Figure: SNMP

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.

9.4 Syslog

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

- **Syslog Configuration** – Syslog Configuration allows you to choose whether 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 sent are only kept when “keep sent message” enable check box is checked. Currently we keep the last 100 messages in the RAM area; they will clear when reboot or power off.

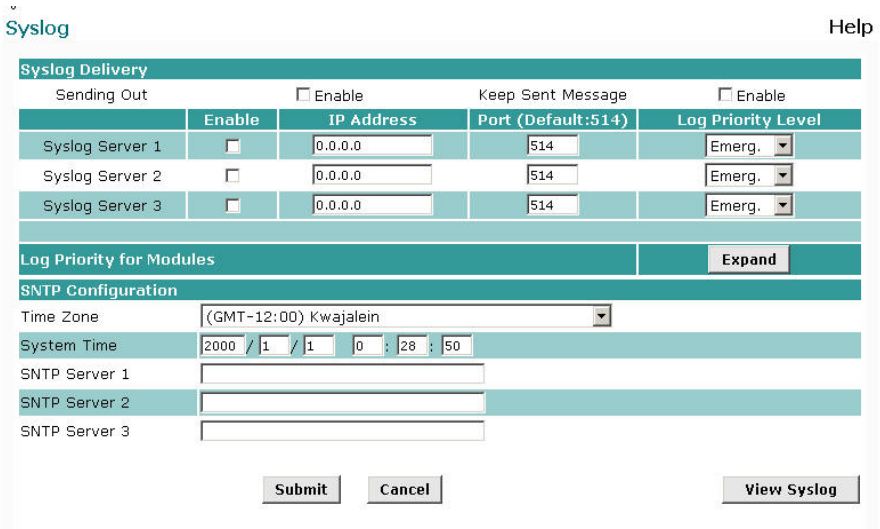


Figure: Syslog

Settings – 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 at the highest priority to Debug being the lowest priority. The lower the level, the greater the messages generated, with Debug sending 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, the greater the messages 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.

9.5 Upgrade Firmware

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

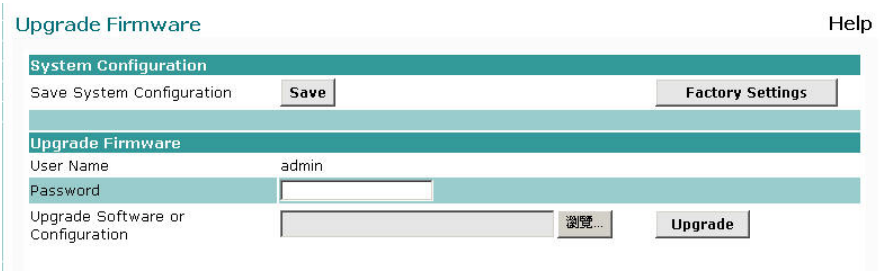


Figure: Firmware Upgrade Screen

- 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)
- 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 updating new firmware, because it may cause system to crash.

TFTP Download

This setting should be used only if your router is unusable, and you wish to restore it by downloading new firmware. Follow this procedure:

1. Power on the router.
2. Use a TFTP client program applies the new firmware. The screen will look like the following figure.

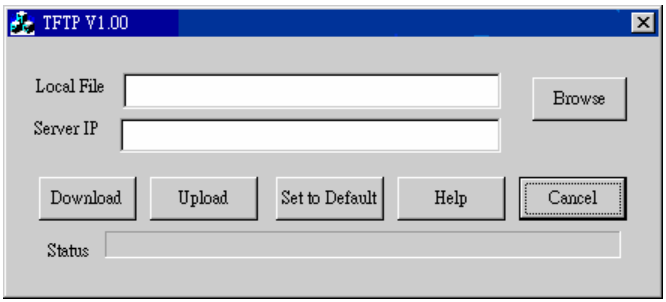


Figure: Windows TFTP utility

- 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 router in the "Server IP" field.
- Click "Download" to send the file to the router.

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

10. System information

10.1 System Status

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

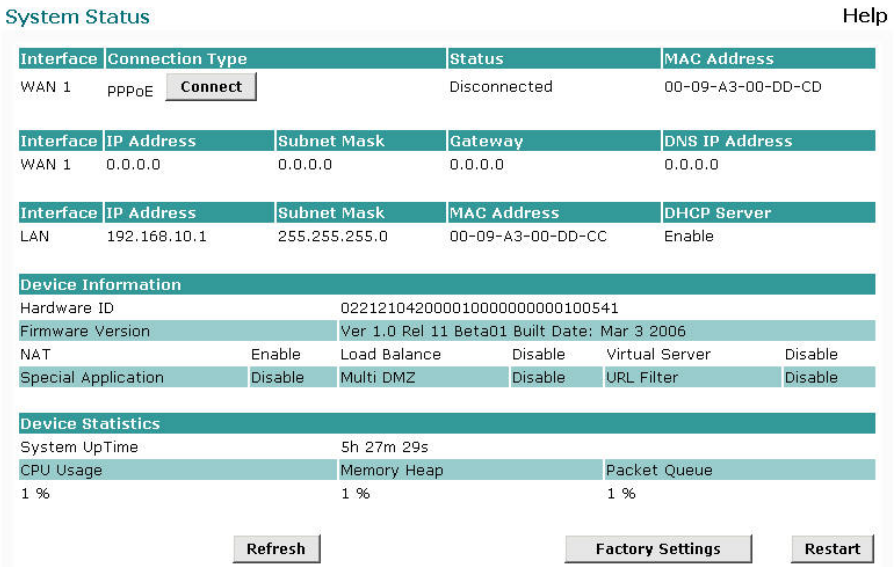


Figure 9-1: System Status

Data – System Status

Interface Information	• **Connection Status** – Current status – either "Connected" or "Not connected". • **Connection Type** – The type of connection used – DHCP, Fixed IP, PPPoE, or PPTP. • **"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. • **IP Address** – The IP address of the Router, 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. • **Domain Name IP Address** – The address of the current DNS

	(Domain Name Server. • **MAC Address** – The MAC (physical) address of the Router, as seen from the Internet.
LAN Information	• **IP Address** – The LAN IP Address of the Router. • **Subnet Mask** – The Network Mask (Subnet Mask) for the IP Address above. • **MAC Address** – The MAC (physical) address of the Router, as seen from the local LAN. • **DHCP Server** – The status of the DHCP Server function - either "Enabled" or "Disabled".
Device Information	• **Hardware ID** – The manufacturer 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 Usage** – The current usage percentage of Memory (Heap & Queue).
Buttons	• **Refresh** – Update the data on screen. • **Restart** – Restart (reboot) the Router. • **Restore Factory Defaults** – This will delete all existing settings, and restore the factory default settings. See below for details.

- **Restore Factory Defaults**

  When the "Restore Factory Defaults" button on the Status screen above is clicked, the following screen will be displayed.

Figure: 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 mean that the current connection is invalid, and you will have to re-connect to the Router using its default IP address (192.168.1.1).

10.2 WAN Status

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

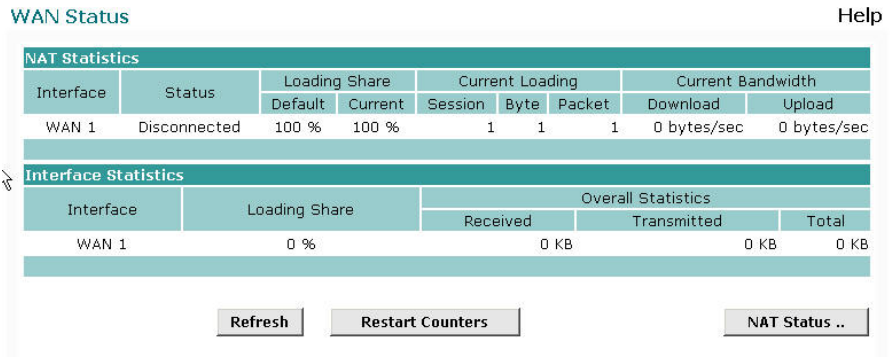


Figure: WAN Status

Data – System Status

NAT Statistics	This section displays data for each WAN port. • **Connection status** – The current connection status, 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.

- **NAT Status**

  This screen is displayed when you click the "Check NAT Detail" button on the WAN Status screen.

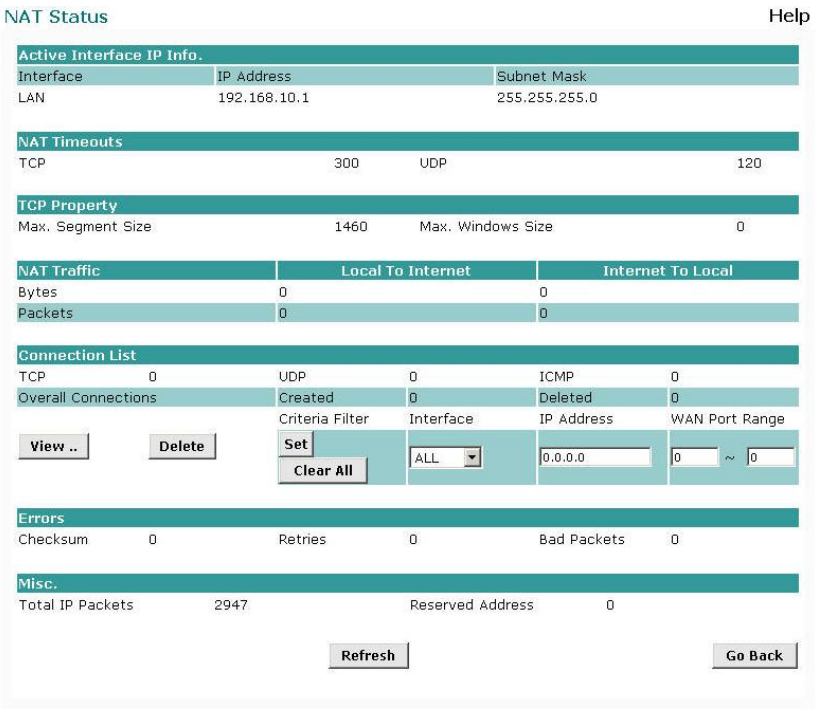


Figure: NAT Status

Data – NAT Status

Active Interface IP Info	• **Interface** – LAN and WAN interface of the Routerr. • **IP Address** – The WAN (Internet) & LAN IP Address of the Router. • **Subnet Mask** – The Network Mask (Subnet Mask) for the IP Address above
NAT Timeouts	This displays the current timeout values for TCP and UDP connections.
TCP Prosperity	This displays the MSS (Maximum Segment Size) and Maximum Windows size for TCP packets.
NAT Traffic	This section displays statistics for both outgoing (LAN to Internet) and Incoming (Internet to Local) traffic.
Connections List	This displays the current number of active connections. For further details, click the "View Connection" list button.
Errors	Statistics are displayed for Checksum errors, number of retries, and number of bad packets.
Misc.	This displays the total IP packets and reserved address.

11. Specifications

Standard	IEEE802.3, IEEE802.3u
Interface	1 10/100M RJ-45 WAN port 4 10/100M RJ-45 LAN ports
Cable Connections	10BASE-T: Category 3, 4, 5 UTP/STP 100BASE-TX: Category 5 UTP/STP
Uplink	Auto Uplink (Auto MDI / MDI-X)
Protocol	Security: NAT, UPAP, CHAP Network: TCP/IP, HTTP, DHCP, PPP, UPAP, PPPoE, Multi-session PPPoE, ICMP, APR proxy Routing: Static route for WAN & LAN, RIPv1, RIPv2 Connection: Static IP, dynamic IP, PPPoE, PPTP
Feature	Virtual server, Multi-DMZ, Special Application, NAT, UPnP, DHCP server, DDNS, Transparent bridge mode, MTU change for WAN, MAC address clone
Firewall	DoS, SPI, Ping to Death, Port scan, ICMP filter, URL filter and Access Control
VPN	IPSec VPN up to 20 tunnels, IPSec & PPTP VPN pass through
QoS	Policy Priority QoS, ToS-QoS
Security	Admin passwords Authentication with UPAP and CHAP for PPPoE
System Memory	1MB Flash, 16MB RAM
Management	Web-based, Email alert, SNMP, Syslog
Firmware update	HTTP web based download TFTP download
Operating Temperature	0 ^{o} C - 40 ^{o} C (32 ^{o} - 104^{o} F)
Storage Temperature	-10 ^{o} - 70 ^{o} C (-4 ^{o} - 158^{o} F)
Operating Humidity	10% - 90% (Non-condensing)
Dimension	245mm (W) x 137mm (D) x 30mm (H)
Weight	890 (g)
Power Supply	DC 5V 1.5A
Emission	CE, FCC

Appendix C

Troubleshooting

Overview

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

General Problems

Problem 1:	**Can't connect to the Router to configure it.**
Solution 1:	Check the following: • The Router is properly installed, LAN connections are OK, and it is powered ON. • Ensure that your PC and the Router are on the same network segment. (If you don't have a router, this must be the cause.) • 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 Router's default IP Address of 192.168.1.1. Also, the Network Mask should be set to 255.255.255.0 to match the Router. 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 does not working, check the Router. Ensure that it is connected and powered ON. Connect to it and check its settings. (If you can't connect to it, check the LAN and power connections.) • If the Router is configured correctly, check your Internet connection

	(DSL/Cable modem etc) to see if it is working correctly.
Problem 2:	**Some applications do not run properly when using the Router.**
Solution 2:	The Router 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.

2006/03/09